



ASDM ブック 1 : Cisco ASA シリーズ ASDM 7.4 コンフィギュレーションガイド (一般的な操作)

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスココンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2005–2015 Cisco Systems, Inc. All rights reserved.



目次

はじめに :

[このマニュアルについて](#) **xlvii**

[本書の目的](#) **xlvii**

[関連資料](#) **xlvii**

[表記法](#) **xlviii**

[通信、サービス、およびその他の情報](#) **xlix**

第 I 部 :

[ASA の開始](#) **51**

第 1 章

[Cisco ASA の概要](#) **1**

[ASDM 要件](#) **2**

[ASDM Java の要件](#) **2**

[ASDM の互換性に関する注意事項](#) **2**

[ハードウェアとソフトウェアの互換性](#) **6**

[VPN の互換性](#) **6**

[新機能](#) **6**

[ASA 9.4\(4.5\)/ASDM 7.6\(2\) の新機能](#) **7**

[ASA 9.4\(3\)/ASDM 7.6\(1\) の新機能](#) **7**

[ASA 9.4\(2.145\)/ASDM 7.5\(1\) の新機能](#) **8**

[ASA 9.4\(2\)/ASDM 7.5\(1\) の新機能](#) **9**

[ASA 9.4\(1.225\)/ASDM 7.5\(1\) の新機能](#) **9**

[ASA 9.4\(1.152\)/ASDM 7.4\(3\) の新機能](#) **10**

[ASAv 9.4\(1.200\)/ASDM 7.4\(2\) の新機能](#) **10**

[ASDM 7.4\(2\) の新機能](#) **11**

[ASA 9.4\(1\)/ASDM 7.4\(1\) の新機能](#) **11**

ファイアウォール機能の概要	19
セキュリティ ポリシーの概要	20
アクセスルールによるトラフィックの許可または拒否	20
NAT の適用	20
IP フラグメントからの保護	20
HTTP、HTTPS、または FTP フィルタリングの適用	21
アプリケーション インспекションの適用	21
サポート対象のハードウェア モジュールまたはソフトウェア モジュールへのトラフィックの送信	21
QoS ポリシーの適用	21
接続制限と TCP 正規化の適用	21
脅威検出のイネーブル化	22
ファイアウォール モードの概要	22
ステートフル インспекションの概要	22
VPN 機能の概要	24
セキュリティ コンテキストの概要	25
ASA クラスタリングの概要	25
特殊なサービス非推奨のサービスおよびレガシー サービス	25

第 2 章**使用する前に 27**

コマンドライン インターフェイス (CLI) のコンソールへのアクセス	27
アプライアンス コンソールへのアクセス	27
Firepower 9300 シャーシ 上の ASA コンソールへのアクセス	29
ASA サービス モジュール コンソールへのアクセス	30
接続方法について	30
ASA サービス モジュールへのログイン	32
コンソール セッションのログアウト	33
アクティブなコンソール接続の終了	34
Telnet セッションのログアウト	35
ソフトウェア モジュール コンソールへのアクセス	35
ASA 5506W-X ワイヤレス アクセス ポイント コンソールへのアクセス	36

ASDM アクセスの設定	36
ASDM アクセス（アプライアンス、ASA v）に対する工場出荷時のデフォルト コンフィ ギュレーションの使用	36
ASDM アクセスのカスタマイズ	37
ASA サービス モジュールの ASDM アクセスの設定	40
ASDM の起動	42
ASDM 動作のカスタマイズ	44
ASDM のアイデンティティ証明書のインストール	44
ASDM コンフィギュレーションメモリの増大	44
Windows での ASDM コンフィギュレーションメモリの増大	45
Mac OS での ASDM コンフィギュレーションメモリの増大	45
工場出荷時のデフォルト設定	46
工場出荷時のデフォルト設定の復元	47
ASA v 導入設定の復元	49
ASA 5506-X、5508-X、および 5516-X のデフォルト設定	50
ASA 5512-X ～ ASA 5585-X デフォルト設定	51
Firepower 9300 シャーシ デフォルト設定	52
ISA 3000 のデフォルト設定	53
ASA v 導入設定	54
設定の開始	56
ASDM でのコマンドライン インターフェイス ツールの使用	57
コマンドライン インターフェイス ツールの使用	57
ASDM によって無視されるコマンドのデバイス上での表示	58
接続の設定変更の適用	59
第 3 章	ASDM グラフィカル ユーザ インターフェイス 61
	ASDM ユーザ インターフェイスについて 61
	ASDM ユーザ インターフェイスのナビゲーション 64
	メニュー 65
	[File] メニュー 65
	[View] メニュー 66

[Tools] メニュー	67
[Wizards] メニュー	70
[Window] メニュー	70
[Help] メニュー	71
ツールバー	72
ASDM Assistant	73
ステータス バー	73
Connection to Device	74
Device List	74
共通ボタン	75
キーボードショートカット	76
ASDM ペインの検索機能	78
ルール リストの検索機能	78
拡張スクリーン リーダ サポートの有効化	79
整理用フォルダー	80
[Home] ペイン (シングル モードとコンテキスト)	80
[Device Dashboard] タブ	80
[Device Information] ペイン	82
[Interface Status] ペイン	83
[VPN Sessions] ペイン	83
[Failover Status] ペイン	83
[System Resources Status] ペイン	83
[Traffic Status] ペイン	84
[Latest ASDM Syslog Messages] ペイン	84
[Firewall Dashboard] タブ	85
[Traffic Overview] ペイン	86
[Top 10 Access Rules] ペイン	87
[Top Usage Status] ペイン	87
[Top Ten Protected Servers Under SYN Attack] ペイン	88
[Top 200 Hosts] ペイン	88
[Top Botnet Traffic Filter Hits] ペイン	88

[Cluster Dashboard] タブ	89
[Cluster Firewall Dashboard] タブ	90
[Content Security] タブ	91
[Intrusion Prevention] タブ	93
[ASA CX Status] タブ	94
[ASA Firepower Status] タブ	95
[Home] ペイン (システム)	95
ASDM 設定の定義	97
ASDM Assistant での検索	99
履歴メトリックの有効化	100
サポートされていないコマンド	100
無視される表示専用コマンド	101
サポートされていないコマンドの影響	102
サポート対象外の連続していないサブネットマスク	102
ASDM CLI ツールでサポートされていないインタラクティブ ユーザ コマンド	102

第 4 章

ライセンス : 製品認証キー ライセンス	105
PAK ライセンスについて	105
事前インストール済みライセンス	105
永続ライセンス	106
時間ベース ライセンス	106
時間ベース ライセンス有効化ガイドライン	106
時間ベース ライセンス タイマーの動作	106
永続ライセンスと時間ベース ライセンスの結合	107
時間ベース ライセンスのスタッキング	108
時間ベース ライセンスの有効期限	109
ライセンスに関する注意事項	109
AnyConnect Plus および Apex ライセンス	109
その他の VPN ライセンス	110
合計 VPN セッション、全タイプ	110
VPN ロード バランシング	110

レガシー VPN ライセンス	110
暗号化ライセンス	110
合計 UC プロキシセッション	111
VLAN、最大	112
ボットネット トラフィック フィルタ ライセンス	112
IPS モジュールのライセンス	112
AnyConnect Premium 共有ライセンス (AnyConnect 3 以前)	112
フェールオーバーまたは ASA クラスタ ライセンス	113
フェールオーバー ライセンスの要件および例外	113
ASA クラスタ ライセンスの要件および例外	115
フェールオーバーまたは ASA クラスタ ライセンスの結合方法	116
フェールオーバーまたは ASA クラスタ ユニット間の通信の途絶	117
フェールオーバー ペアのアップグレード	118
ペイロード暗号化機能のないモデル	118
ライセンスの FAQ	118
PAK ライセンスのガイドライン	120
PAK ライセンスの設定	122
ライセンスの PAK の注文とアクティベーション キーの取得	122
高度暗号化ライセンスの取得	123
キーのアクティブ化または非アクティブ化	125
共有ライセンスの設定 (AnyConnect 3 以前)	127
共有ライセンスについて	127
共有ライセンスのサーバと参加システムについて	127
参加者とサーバ間の通信問題	128
共有ライセンス バックアップ サーバについて	128
フェールオーバーと共有ライセンス	129
参加者の最大数	131
共有ライセンス サーバの設定	131
共有ライセンス パーティシパントとオプションのバックアップ サーバの設定	132
モデルごとにサポートされている機能のライセンス	133
モデルごとのライセンス	133

ASA 5506-X および ASA 5506W-X のライセンス機能	133
ASA 5506H-X ライセンスの各機能	135
ASA 5508-X ライセンスの各機能	136
ASA 5512-X ライセンスの機能	137
ASA 5515-X ライセンスの機能	138
ASA 5516-X ライセンスの機能	140
ASA 5525-X ライセンスの各機能	141
ASA 5545-X ライセンスの機能	143
ASA 5555-X ライセンスの機能	144
ASA 5585-X (SSP-10) ライセンスの各機能	146
ASA 5585-X (SSP-20) ライセンスの機能	148
ASA 5585-X (SSP-40 および -60) ライセンスの機能	149
ASASM ライセンスの機能	151
ISA 3000 ライセンスの各機能	153
PAK ライセンスのモニタリング	154
現在のライセンスの表示	155
共有ライセンスのモニタリング	155
PAK ライセンスの履歴	156

第 5 章

ライセンス : スマート ソフトウェア ライセンス (ASA v、ASA on Firepower)	169
スマート ソフトウェア ライセンスについて	169
Firepower 9300 シャーシの ASA のスマート ソフトウェア ライセンシング	170
Smart Software Manager とアカウント	170
仮想アカウントごとに管理されるライセンスとデバイス	170
評価ライセンス	171
Smart Software Manager 通信	171
デバイスの登録とトークン	171
License Authority との定期通信	172
非適合状態	172
Smart Call Home インフラストラクチャ	172
ライセンスに関する注意事項	173

AnyConnect Plus および Apex ライセンス	173
その他の VPN ライセンス	173
合計 VPN セッション、全タイプ	173
暗号化ライセンス	174
合計 UC プロキシセッション	174
VLAN、最大	175
ボットネットトラフィック フィルタ ライセンス	175
フェールオーバーまたは ASA クラスタ ライセンス	176
ASA のフェールオーバー ライセンス	176
Firepower 9300 シャーシの ASA のフェールオーバー ライセンス	176
Firepower 9300 シャーシ上の ASA の ASA クラスタ ライセンス	177
スマート ソフトウェア ライセンスの前提条件	177
スマート ソフトウェア ライセンスのガイドライン	178
スマート ソフトウェア ライセンスのデフォルト	179
ASA : スマート ソフトウェア ライセンシングの設定	179
ASA : スマート ソフトウェア ライセンシングの設定	179
(オプション) ASA の登録解除	182
(オプション) ASA ID 証明書またはライセンス権限付与の更新	183
Firepower 9300 シャーシ : スマート ソフトウェア ライセンスの設定	183
Firepower 9300 シャーシ : スマート ソフトウェア ライセンシングの設定	183
Firepower 9300 シャーシ : ASDM を使用したスマート ソフトウェア ライセンシングの設定の変更	186
モデルごとのライセンス	187
ASA	187
Firepower 9300 ASA アプリケーション	188
Smart Software Licensing のモニタリング	189
現在のライセンスの表示	189
スマート ライセンス ステータスの表示	189
スマート ソフトウェア ライセンスの履歴	190

Firepower インターフェイスについて	191
シャーシ管理インターフェイス	191
インターフェイス タイプ	192
シャーシとアプリケーションの独立したインターフェイスの状態	192
論理デバイスについて	193
スタンドアロン論理デバイスとクラスタ化論理デバイス	193
ハードウェアとソフトウェアの組み合わせの要件と前提条件	193
論理デバイスに関する注意事項と制約事項	194
Firepower インターフェイスに関する注意事項と制約事項	194
一般的なガイドラインと制限事項	194
インターフェイスの設定	195
インターフェイスの有効化または無効化	195
物理インターフェイスの設定	196
EtherChannel (ポート チャンネル) の追加	197
論理デバイスの設定	198
スタンドアロン ASA の追加	198
ハイ アベイラビリティ ペアの追加	200
ASA のトランスペアレント ファイアウォール モードへの変更	201
ASA 論理デバイスのインターフェイスの変更	203
アプリケーションのコンソールへの接続	204
論理デバイスの履歴	205
<hr/>	
第 7 章	トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード
	207
	ファイアウォール モードについて
	207
	ルーテッド ファイアウォール モードについて
	207
	トランスペアレント ファイアウォール モードについて
	208
	ネットワーク内でトランスペアレント ファイアウォールの使用
	208
	ブリッジグループについて
	209
	ルーテッド モード機能のためのトラフィックの通過
	214
	デフォルト設定
	215
	ファイアウォール モードのガイドライン
	215

ファイアウォールモード（シングルモード）の設定	216
ファイアウォールモードの例	217
ルーテッドファイアウォールモードでASAを通過するデータ	217
内部ユーザがWebサーバにアクセスする	218
外部ユーザがDMZ上のWebサーバにアクセスする	219
内部ユーザがDMZ上のWebサーバにアクセスする	220
外部ユーザが内部ホストにアクセスしようとする	221
DMZユーザによる内部ホストへのアクセスの試み	222
トランスペアレントファイアウォールを通過するデータの動き	222
内部ユーザがWebサーバにアクセスする	223
NATを使用して内部ユーザがWebサーバにアクセスする	225
外部ユーザが内部ネットワーク上のWebサーバにアクセスする	226
外部ユーザが内部ホストにアクセスしようとする	227
ファイアウォールモードの履歴	228

第 8 章

Startup Wizard 231

Startup Wizard へのアクセス	231
Startup Wizard のガイドライン	231
Startup Wizard の画面	231
開始点またはウェルカム	232
基本設定	232
インターフェイスの画面	232
外部インターフェイスの設定（ルーテッドモード）	232
外部インターフェイスの設定 - PPPoE（ルーテッドモード、シングルモード）	232
Management IP Address Configuration（トランスペアレントモード）	232
その他のインターフェイスの設定	233
スタティックルート	233
DHCPサーバ	233
アドレス変換（NAT/PAT）	233
管理アクセス	233
IPSの基本設定	233

ASA CX の基本設定 (ASA 5585-X)	233
ASA FirePOWER の基本設定	234
タイムゾーンおよびクロック コンフィギュレーション	234
Auto Update サーバ (シングル モード)	234
スタートアップ ウィザードの概要	234
Startup Wizard の履歴	235

第 II 部 : ハイ アベイラビリティとスケラビリティ 237

第 9 章	マルチ コンテキスト モード	239
	セキュリティ コンテキストについて	239
	セキュリティ コンテキストの一般的な使用方法	239
	コンテキスト コンフィギュレーション ファイル	240
	コンテキスト コンフィギュレーション	240
	システム設定	240
	管理コンテキストの設定	240
	ASA がパケットを分類する方法	241
	有効な分類子基準	241
	分類例	241
	セキュリティ コンテキストのカスケード接続	244
	セキュリティ コンテキストへの管理アクセス	245
	システム管理者のアクセス	245
	コンテキスト管理者のアクセス	246
	リソース管理の概要	246
	リソース クラス	246
	リソース制限値	246
	デフォルト クラス	246
	オーバーサブスクライブ リソースの使用	248
	無限リソースの使用	248
	MAC アドレスについて	249
	マルチコンテキスト モードでの MAC アドレス	249

自動 MAC アドレス	249
VPN サポート	250
マルチ コンテキスト モードのライセンス	250
マルチ コンテキスト モードの前提条件	252
マルチ コンテキスト モードのガイドライン	252
マルチ コンテキスト モードのデフォルト	253
マルチ コンテキスト の設定	253
マルチ コンテキスト モードの有効化またはディセーブル化	253
マルチ コンテキスト モードの有効化	254
シングルコンテキスト モードの復元	254
リソース管理用のクラスの設定	255
セキュリティ コンテキスト の設定	258
コンテキスト インターフェイスへの MAC アドレスの自動割り当て	261
コンテキスト とシステム実行スペースの切り替え	262
セキュリティ コンテキスト の管理	262
セキュリティ コンテキスト の削除	262
管理コンテキスト の変更	263
セキュリティ コンテキスト URL の変更	264
セキュリティ コンテキスト のリロード	265
コンフィギュレーションのクリアによるリロード	265
コンテキスト の削除および再追加によるリロード	266
セキュリティ コンテキスト のモニタリング	266
コンテキスト リソースの使用状況のモニタリング	266
割り当てられた MAC アドレスの表示	268
システム設定での MAC アドレスの表示	268
コンテキスト内の MAC アドレスの表示	269
マルチ コンテキスト モードの履歴	269
第 10 章	ハイ アベイラビリティのためのフェールオーバー 275
	フェールオーバーについて 275
	フェールオーバー モード 275

フェールオーバーのシステム要件	276
ハードウェア要件	276
ソフトウェア要件	277
ライセンス要件	277
フェールオーバーリンクとステートフルフェールオーバーリンク	277
フェールオーバーリンク	278
ステートフルフェールオーバーリンク	279
フェールオーバーの中断の回避とデータリンク	280
フェールオーバーのMACアドレスとIPアドレス	283
ASAサービスモジュールのシャーシ内およびシャーシ間モジュール配置	285
シャーシ内フェールオーバー	285
シャーシ間フェールオーバー	286
ステートレスフェールオーバーとステートフルフェールオーバー	289
ステートレスフェールオーバー	289
Stateful Failover	290
フェールオーバーのトランスペアレントファイアウォールモードブリッジグループ要件	292
トランスペアレントモードアプライアンス、ASAのブリッジグループ必須要件	292
トランスペアレントモードASAサービスモジュールのブリッジグループ必須要件	293
フェールオーバーのヘルスマニタ	293
ユニットのヘルスマニタリング	294
インターフェイスモニタリング	294
フェールオーバー時間	296
設定の同期	297
コンフィギュレーションの複製の実行	297
File Replication	298
Command Replication	298
アクティブ/スタンバイフェールオーバーについて	299
プライマリ/セカンダリロールとアクティブ/スタンバイステータス	299
起動時のアクティブ装置の判別	300
フェールオーバーイベント	300
アクティブ/アクティブフェールオーバーの概要	302

アクティブ/アクティブ フェールオーバーの概要	302
フェールオーバー グループのプライマリ/セカンダリ ロールとアクティブ/スタンバイステータス	302
起動時のフェールオーバー グループのアクティブ装置の決定	303
フェールオーバー イベント	303
フェールオーバーのライセンス	305
フェールオーバーのガイドライン	307
フェールオーバーのデフォルト	309
アクティブ/スタンバイ フェールオーバーの設定	310
アクティブ/アクティブ フェールオーバーの設定	311
オプションのフェールオーバー パラメータの設定	312
フェールオーバー基準とその他の設定の構成	313
インターフェイス モニタリングの設定およびスタンバイ アドレスの設定	316
非対称にルーティングされたパケットのサポートの設定 (アクティブ/アクティブモード)	317
フェールオーバー の管理	319
フェールオーバーの設定変更	320
フェールオーバーの強制実行	322
フェールオーバーのディセーブル化	323
障害が発生した装置の復元	324
コンフィギュレーションの再同期	325
モニタリング フェールオーバー	325
フェールオーバー メッセージ	325
フェールオーバーの syslog メッセージ	325
フェールオーバー デバッグ メッセージ	326
SNMP のフェールオーバー トラップ	326
フェールオーバー ステータスのモニタリング	326
システム	326
フェールオーバー グループ 1 およびフェールオーバー グループ 2	327
フェールオーバーの履歴	328

第 11 章

ASA クラスタ 331

ASA クラスタリングの概要 331

ASA クラスタをネットワークに適合させる方法 331

パフォーマンス スケーリング係数 332

クラスタ メンバー 332

Bootstrap Configuration 332

マスターおよびスレーブ ユニットの役割 333

マスター ユニット選定 333

クラスタ インターフェイス 334

クラスタ制御リンク 334

ASA クラスタ内のハイ アベイラビリティ 334

ユニットのヘルス モニタリング 334

インターフェイス モニタリング 334

障害後のステータス 335

クラスタへの再参加 335

データ パス接続状態の複製 336

設定の複製 337

ASA クラスタ管理 337

管理ネットワーク 337

管理インターフェイス 337

マスター ユニット管理とスレーブ ユニット管理 338

RSA キー複製 338

ASDM 接続証明書 IP アドレス不一致 339

サイト間クラスタリング 339

ASA クラスタが接続を管理する方法 339

接続のロール 339

新しい接続の所有権 341

サンプル データ フロー 341

新しい TCP 接続のクラスタ全体での再分散 342

ASA の各機能とクラスタリング 342

クラスタリングでサポートされない機能	342
クラスタリングの中央集中型機能	343
個々のユニットに適用される機能	344
ネットワーク アクセス用の AAA とクラスタリング	345
FTP とクラスタリング	345
アイデンティティ ファイアウォールとクラスタリング	345
マルチキャストルーティングとクラスタリング	345
NAT とクラスタリング	346
ダイナミック ルーティングおよびクラスタリング	347
SIP インスペクションとクラスタリング	350
SNMP とクラスタリング	350
syslog および NetFlow とクラスタリング	350
Cisco TrustSec とクラスタリング	350
VPN とクラスタリング	350
ASA クラスタリングのライセンス	351
ASA クラスタリングの要件と前提条件	352
ASA クラスタリングのガイドライン	354
ASA クラスタリングの設定	359
コンフィギュレーションのバックアップ (推奨)	359
ユニットのケーブル接続およびインターフェイスの設定	360
クラスタ インターフェイスについて	360
クラスタ ユニットのケーブル接続とアップストリームおよびダウンストリーム機器の 設定	371
マスターユニットでのクラスタ インターフェイス モードの設定	373
(推奨、マルチ コンテキスト モードでは必須) マスターユニットでのインターフェ イスの設定	376
ASA クラスターの作成または ASA クラスタへの参加	383
高可用性のウィザードの実行	383
クラスタリング動作のカスタマイズ	386
ASA クラスターの基本パラメータの設定	386
インターフェイスのヘルス モニタリングの設定	390

クラスタ メンバの管理	391
マスターユニットからの新しいスレーブの追加	391
非アクティブなメンバーになる	392
マスターユニットからのスレーブメンバーの非アクティブ化	393
クラスタへの再参加	394
クラスタからの脱退	395
マスターユニットの変更	396
クラスタ全体でのコマンドの実行	397
ASA クラスタのモニタリング	398
クラスタ ステータスのモニタリング	398
クラスタ全体のパケットのキャプチャ	398
クラスタ リソースのモニタリング	398
クラスタ トラフィックのモニタリング	399
クラスタ制御リンクのモニタリング	399
クラスタリングのロギングの設定	399
ASA クラスタリングの例	399
ASA およびスイッチのコンフィギュレーションの例	400
ASA の設定	400
Cisco IOS スwitchのコンフィギュレーション	401
スティック上のファイアウォール	403
トラフィックの分離	405
スパンド EtherChannel とバックアップリンク (従来の 8 アクティブ/8 スタンバイ)	408
サイト間クラスタリングの例	413
個別インターフェイスルーテッドモード ノースサウス サイト間の例	414
スパンド EtherChannel トランスペアレントモード ノースサウス サイト間の例	414
スパンド EtherChannel トランスペアレントモード イーストウェスト サイト間の例	416
ASA クラスタリングの履歴	417
<hr/>	
第 12 章	Firepower 9300 シャーシの ASA クラスタ 421
	Firepower 9300 シャーシでのクラスタリングについて 421
	Bootstrap Configuration 422

クラスタ メンバー	422
マスターおよびスレーブ ユニットの役割	423
クラスタ制御リンク	423
クラスタ制御リンク ネットワーク	423
クラスタ インターフェイス	424
VSS または vPC への接続	424
設定の複製	424
ASA クラスタの管理	424
管理インターフェイス	424
マスター ユニット管理とスレーブ ユニット管理	425
RSA キー複製	425
ASDM 接続証明書 IP アドレス不一致	425
ASA の各機能とクラスタリング	425
クラスタリングでサポートされない機能	426
クラスタリングの中央集中型機能	426
個々のユニットに適用される機能	427
ネットワーク アクセス用の AAA とクラスタリング	428
FTP とクラスタリング	428
アイデンティティ ファイアウォールとクラスタリング	428
マルチキャストルーティングとクラスタリング	429
NAT とクラスタリング	429
ダイナミック ルーティングおよびクラスタリング	430
SIP インスペクションとクラスタリング	431
SNMP とクラスタリング	431
syslog および NetFlow とクラスタリング	431
Cisco TrustSec とクラスタリング	431
Firepower 9300 シャーシでのクラスタリングの要件と前提条件	432
上のクラスタリングのライセンス Firepower 9300 シャーシ	432
クラスタリング ガイドラインと制限事項	433
クラスタリングの設定 Firepower 9300 シャーシ	433
FXOS : ASA クラスタの追加	434

ASA クラスタの作成	434
ASA : ファイアウォールモードとコンテキストモードの変更	438
ASA : データ インターフェイスの設定	438
ASA : クラスタ設定のカスタマイズ	441
ASA クラスタの基本パラメータの設定	441
インターフェイスのヘルス モニタリングの設定	443
クラスタ TCP 複製の遅延の設定	444
FXOS : クラスタ メンバの削除	444
ASA : クラスタ メンバの管理	446
非アクティブなメンバーになる	446
マスターユニットからのスレーブ メンバーの非アクティブ化	447
クラスタへの再参加	448
マスターユニットの変更	449
クラスタ全体でのコマンドの実行	449
ASA : での ASA クラスタのモニタリング Firepower 9300 シャーシ	451
クラスタ ステータスのモニタリング	451
クラスタ全体のパケットのキャプチャ	451
クラスタ リソースのモニタリング	451
クラスタ トラフィックのモニタリング	451
クラスタ制御リンクのモニタリング	452
クラスタリングのロギングの設定	452
クラスタリングの参考資料	452
パフォーマンス スケーリング係数	452
マスターユニット選定	453
クラスタ内のハイ アベイラビリティ	453
シャーシアプリケーションのモニタリング	453
ユニットのヘルス モニタリング	453
インターフェイス モニタリング	454
障害後のステータス	454
クラスタへの再参加	454
データ パス接続状態の複製	455

クラスタが接続を管理する方法	456
接続のロール	456
新しい接続の所有権	457
サンプル データ フロー	457
Firepower 9300 シャーシ 上の ASA クラスタリングの履歴	459

第 III 部 :**インターフェイス 461**

第 13 章**基本的なインターフェイス設定 463**

基本的なインターフェイス設定について	463
Auto-MDI/MDIX 機能	464
管理インターフェイス	464
管理インターフェイスの概要	464
管理スロット/ポート インターフェイス	464
管理専用トラフィックに対する任意のインターフェイスの使用	465
トランスペアレント モードの管理インターフェイス	466
冗長管理インターフェイスの非サポート	466
ASA モデルの管理インターフェイスの特性	466
基本インターフェイスの設定のライセンス	467
基本インターフェイスの設定のガイドライン	467
基本インターフェイスのデフォルト設定	468
物理インターフェイスのイネーブル化およびイーサネット パラメータの設定	469
ジャンボ フレーム サポートの有効化	471
基本インターフェイスの例	472
物理インターフェイス パラメータの例	472
マルチ コンテキスト モードの例	472
基本インターフェイスの設定の履歴	473

第 14 章**EtherChannel インターフェイスと冗長インターフェイス 475**

EtherChannel インターフェイスと冗長インターフェイスについて	476
冗長インターフェイスについて	476

冗長インターフェイスの MAC アドレス	476
EtherChannel について	476
チャンネルグループのインターフェイス	477
別のデバイスの EtherChannel への接続	477
リンク集約制御プロトコル	478
ロード バランシング	478
EtherChannel MAC アドレス	479
EtherChannel インターフェイスと冗長インターフェイスのガイドライン	479
EtherChannel インターフェイスと冗長インターフェイスのデフォルト設定	482
冗長インターフェイスの設定	482
冗長インターフェイスの設定	483
アクティブ インターフェイスの変更	484
EtherChannel の設定	485
EtherChannel へのインターフェイスの追加	485
EtherChannelのカスタマイズ	487
EtherChannel インターフェイスと冗長インターフェイスの例	489
EtherChannel インターフェイスと冗長インターフェイスの履歴	490

第 15 章

VLAN サブインターフェイス	493
VLAN サブインターフェイスについて	493
VLAN サブインターフェイスのライセンス	494
VLAN サブインターフェイスのガイドラインと制限事項	495
VLAN サブインターフェイスのデフォルト設定	495
VLAN サブインターフェイスと 802.1Q トランキングの設定	496
VLAN のサブインターフェイスの例	497
VLAN サブインターフェイスの履歴	498

第 16 章

VXLAN インターフェイス	499
VXLAN インターフェイスの概要	499
VXLAN カプセル化	499
VXLAN トンネル エンドポイント	500

VTEP 送信元インターフェイス	500
VNI インターフェイス	501
VXLAN パケット処理	501
ピア VTEP	501
VXLAN 使用例	502
VXLAN ブリッジまたはゲートウェイの概要	502
VXLAN ブリッジ (トランスペアレント モード)	502
VXLAN ゲートウェイ (ルーテッド モード)	503
VXLAN ドメイン間のルータ	503
VXLAN インターフェイスのガイドライン	505
VXLAN インターフェイスのデフォルト設定	505
VXLAN インターフェイスの設定	505
VTEP 送信元インターフェイスの設定	506
VNI インターフェイスの設定	507
VXLAN インターフェイスの例	508
トランスペアレント VXLAN ゲートウェイの例	508
VXLAN ルーティングの例	511
VXLAN インターフェイスの履歴	512
<hr/>	
第 17 章	ルーテッドモード インターフェイスとトランスペアレントモード インターフェイス 513
	ルーテッドモード インターフェイスとトランスペアレントモード インターフェイスについて 514
	セキュリティ レベル 514
	デュアル IP スタック (IPv4 および IPv6) 515
	ルーテッドモードおよびトランスペアレントモードのインターフェイスのガイドラインおよび要件 515
	ルーテッドモードのインターフェイスの設定 517
	ルーテッドモードの一般的なインターフェイス パラメータの設定 517
	PPPoE の設定 520
	トランスペアレントモードのブリッジグループ インターフェイスの設定 521
	ブリッジ仮想インターフェイス (BVI) の設定 521

ブリッジグループメンバーの一般的なインターフェイスパラメータの設定	522
トランスペアレントモードの管理インターフェイスの設定	524
IPv6 アドレスの設定	526
IPv6 について	526
IPv6 アドレス指定	526
Modified EUI-64 インターフェイス ID	527
グローバル IPv6 アドレスの設定	527
(オプション) リンクローカルアドレスの自動設定	529
(オプション) リンクローカルアドレスの手動設定	530
IPv6 ネイバー探索の設定	530
ダイナミックに検出されたネイバーの表示とクリア	534
ルーテッドモードおよびトランスペアレントモードのインターフェイスのモニタリング	535
インターフェイス統計情報	535
スタティック ルート トラッキング	535
PPPoE	535
ダイナミック ACL	535
ルーテッドモードおよびトランスペアレントモードのインターフェイスの例	536
2つのブリッジグループを含むトランスペアレントモードの例	536
ルーテッドモードおよびトランスペアレントモードのインターフェイスの履歴	537

第 18 章

高度なインターフェイス設定	539
高度なインターフェイス設定について	539
MAC アドレスについて	539
デフォルトの MAC アドレス	540
自動 MAC アドレス	540
MTU について	541
『Path MTU Discovery』	541
デフォルト MTU	542
MTU とフラグメンテーション	542
MTU とジャンボフレーム	542

TCP MSS について	543
デフォルト TCP MSS	543
TCP MSS の推奨最大設定	543
インターフェイス間通信	544
インターフェイス内通信 (ルーテッドファイアウォールモード)	544
マルチ コンテキスト モードでの MAC アドレスの自動割り当て	545
手動 MAC アドレス、MTU、および TCP MSS の設定	546
同一のセキュリティ レベル通信の許可	548
ARP および MAC アドレス テーブルのモニタリング	548
インターフェイスの詳細設定の履歴	549

第 19 章

トラフィック ゾーン	551
トラフィック ゾーンの概要	551
ゾーン分割されていない動作	551
ゾーンを使用する理由	552
非対称ルーティング	552
紛失したルート	552
ロード バランシング	553
ゾーンごとの接続テーブルおよびルーティング テーブル	554
ECMP ルーティング	554
ゾーン分割されていない ECMP サポート	554
ゾーン分割された ECMP サポート	555
接続のロード バランス方法	555
別のゾーンのルートへのフォールバック	555
インターフェイススペースのセキュリティ ポリシーの設定	556
トラフィック ゾーンでサポートされるサービス	556
セキュリティ レベル	556
フローのプライマリおよび現在のインターフェイス	557
ゾーンの追加または削除	557
ゾーン内トラフィック	557
To-the-Box および From-the-Box トラフィック	557

ゾーン内の IP アドレスのオーバーラップ	558
トラフィック ゾーンの前提条件	558
トラフィック ゾーンのガイドライン	560
トラフィック ゾーンの設定	561
トラフィック ゾーンのモニタリング	561
ゾーン情報	562
ゾーン接続	562
ゾーンルーティング	563
トラフィック ゾーンの例	564
トラフィック ゾーンの履歴	567

第 IV 部 : **基本設定** **569**

第 20 章 **基本設定** **571**

ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定	571
日時の設定	573
NTP サーバを使用した日付と時刻の設定	573
手動での日時の設定	575
マスター パスフレーズの設定	576
マスター パスフレーズの追加または変更	576
マスター パスフレーズの無効化	577
DNS サーバの設定	578
ハードウェア バイパス (Cisco ISA 3000) の設定	581
ASP (高速セキュリティ パス) のパフォーマンスと動作の調整	582
ルールエンジンのトランザクション コミット モデルの選択	583
ASP ロード バランシングの有効化	584
DNS キャッシュのモニタリング	585
基本設定の履歴	585

第 21 章 **DHCP サービスと DDNS サービス** **587**

DHCP サービスと DDNS サービスについて	587
--------------------------	-----

DHCPv4 サーバについて	587
DHCP オプション	588
DHCP リレー エージェントについて	588
DDNS の概要	589
DDNS アップデート コンフィギュレーション	589
UDP パケット サイズ	589
DHCP サービスと DDNS サービスのガイドライン	590
DHCP サーバの設定	591
DHCPv4 サーバの有効化	591
高度な DHCPv4 オプションの設定	594
DHCP リレー エージェントの設定	595
DDNS の設定	597
DHCP および DDNS サービスのモニタリング	598
DHCP サービスのモニタリング	598
DDNS ステータスのモニタリング	599
DHCP および DDNS サービスの履歴	599

第 22 章

デジタル証明書 603

デジタル証明書の概要	603
公開キー暗号化	604
証明書のスケーラビリティ	605
キーペア	606
トラストポイント	606
認証登録	606
SCEP 要求のプロキシ	607
失効チェック	607
サポート対象の CA サーバ	608
CRL	608
OCSP	609
ローカル CA	610
ローカル CA ファイル用のストレージ	610

ローカル CA サーバ	611
証明書とユーザ ログイン クレデンシャル	611
ユーザ ログイン クレデンシャル	611
証明書	612
デジタル証明書のガイドライン	613
デジタル証明書の設定	615
特定の証明書タイプの設定方法	616
ID 証明書	616
アイデンティティ証明書の追加またはインポート	617
アイデンティティ証明書のエクスポート	620
証明書署名要求の生成	620
アイデンティティ証明書のインストール	621
CA 証明書	623
CA 証明書の追加またはインストール	623
失効に関する CA 証明書の設定	624
CRL 取得ポリシーの設定	625
CRL 取得方式の設定	625
OCSP ルールの設定	626
高度な CRL および OCSP の設定	627
ローカル CA サーバの設定	628
CA サーバ管理	632
コード署名者証明書	633
コード署名者証明書のインポート	633
コード署名者証明書のエクスポート	634
証明書の有効期限アラートの設定 (ID 証明書または CA 証明書用)	634
デジタル証明書のモニタリング	635
証明書管理の履歴	636

第 23 章

トランスパレントファイアウォールモードの ARP インспекションおよび MAC アドレステーブル	639
--	-----

ARP インспекションと MAC アドレス テーブルについて	639
----------------------------------	-----

ブリッジグループのトラフィックの ARP インспекション	639
MAC アドレス テーブル	640
デフォルト設定	641
ARP インспекションと MAC アドレス テーブルのガイドライン	641
ARP インспекションとその他の ARP パラメータの設定	641
スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ	642
ARP インспекションの有効化	643
トランスペアレント モードのブリッジグループにおける MAC アドレス テーブルのカスタマイズ	644
ブリッジグループのスタティック MAC アドレスの追加	644
MAC アドレス ラーニングのディセーブル化	645
ARP インспекションと MAC アドレス テーブルの履歴	645

第 V 部 : **IP ルーティング** 647

第 24 章 **ルーティングの概要** 649

パス判別	649
サポートされるルート タイプ	650
スタティックとダイナミックの比較	650
シングルパスとマルチパスの比較	651
フラットと階層型の比較	651
リンクステートと距離ベクトル型の比較	651
ルーティングにサポートされているインターネットプロトコル	652
ルーティング テーブル	652
ルーティング テーブルへの入力方法	653
ルートのアドミニストレーティブ ディスタンス	653
ダイナミック ルートとフローティング スタティック ルートのバックアップ	655
転送の決定方法	655
ダイナミック ルーティングと フェールオーバー	656
ダイナミック ルーティングおよびクラスタリング	656
スパンド EtherChannel モードでのダイナミック ルーティング	656

個別インターフェイス モードでのダイナミック ルーティング	657
マルチ コンテキスト モードのダイナミック ルーティング	659
ルートのリソース管理	659
等コスト マルチパス (ECMP) ルーティング	660
プロキシ ARP 要求のディセーブル化	660
ルーティング テーブルの表示	661

第 25 章
スタティック ルートとデフォルト ルート 663

スタティック ルートとデフォルト ルートについて	663
デフォルト ルート	663
スタティック ルート	663
不要なトラフィックを「ブラック ホール化」するための null0 インターフェイスへのルート	664
ルートのプライオリティ	664
トランスペアレント ファイアウォール モード ルート	665
スタティック ルート トラッキング	665
スタティック ルートとデフォルト ルートのガイドライン	666
デフォルト ルートおよびスタティック ルートの設定	666
デフォルト ルートの設定	666
スタティック ルートの設定	668
スタティック ルート トラッキングの設定	669
スタティック ルートまたはデフォルト ルートのモニタリング	670
スタティック ルートまたはデフォルト ルートの例	670
スタティック ルートおよびデフォルト ルートの履歴	671

第 26 章
Policy Based Routing : ポリシー ベース ルーティング 673

ポリシーベース ルーティングについて	673
ポリシーベース ルーティングを使用する理由	674
同等アクセスおよび送信元依存ルーティング	674
QoS	674
コスト節約	675

ロードシェアリング 675

PBR の実装 675

ポリシーベース ルーティングのガイドライン 676

ポリシーベース ルーティングの設定 676

ポリシーベース ルーティングの履歴 679

第 27 章

ルートマップ 681

ルートマップについて 681

permit 句と deny 句 682

match 句と set 句の値 682

ルートマップのガイドライン 683

ルートマップの定義 683

ルートマップのカスタマイズ 686

特定の宛先アドレスに一致するルートの定義 686

プレフィックス ルールの設定 688

プレフィックス リストの設定 688

ルートアクションのメトリック値の設定 689

ルートマップの例 689

ルートマップの履歴 690

第 28 章

BGP 693

BGPについて 693

BGP を使用する状況 693

ルーティング テーブルの変更 694

BGP パスの選択 695

BGP マルチパス 696

BGP のガイドライン 697

BGP を設定する 697

BGP の有効化 697

BGP ルーティング プロセスの最適なパスの定義 699

ポリシー リストの設定 700

AS パス フィルタの設定	701
コミュニティ ルールの設定	702
IPv4 アドレス ファミリの設定	703
IPv4 ファミリの一般設定	703
IPv4 ファミリ集約アドレスの設定	704
IPv4 ファミリのフィルタリング設定	705
IPv4 ファミリの BGP ネイバーの設定	706
IPv4 ネットワークの設定	710
IPv4 再配布の設定	710
IPv4 ルート注入の設定	711
IPv6 アドレス ファミリの設定	712
IPv6 ファミリの一般設定	712
IPv6 ファミリ集約アドレスの設定	712
IPv6 ファミリの BGP ネイバーの設定	713
IPv6 ネットワークの設定	717
IPv6 再配布の設定	717
IPv6 ルート注入の設定	718
BGP のモニタリング	719
BGP の履歴	720

第 29 章

OSPF 723

OSPF の概要	723
fast hello パケットに対する OSPF のサポート	725
fast hello パケットに対する OSPF のサポートの前提条件	725
fast hello パケットに対する OSPF のサポートについて	725
OSPFv2 および OSPFv3 間の実装の差異	726
OSPF のガイドライン	727
OSPFv2 の設定	729
OSPFv2 ルータ ID の設定	730
OSPF ルータ ID の手動設定	730
移行中のルータ ID の挙動	731

OSPFv2 のカスタマイズ	731
OSPFv2 へのルートの再配布	732
OSPFv2 にルートを再配布する場合のルート集約の設定	734
ルート サマリー アドレスの追加	734
OSPF サマリー アドレスの追加または編集	735
OSPFv2 エリア間のルート集約の設定	736
OSPFv2 インターフェイス パラメータの設定	736
OSPFv2 エリア パラメータの設定	740
OSPFv2 フィルタ ルール の設定	741
OSPFv2 NSSA の設定	742
クラスタリングの IP アドレス プール の設定 (OSPFv2 および OSPFv3)	743
スタティック OSPFv2 ネイバー の定義	746
ルート計算タイマーの設定	747
ネイバーの起動と停止のロギング	747
OSPF でのフィルタリングの設定	748
OSPF の仮想リンクの設定	749
OSPFv3 の設定	751
OSPFv3 の有効化	751
OSPFv3 インターフェイス パラメータの設定	751
OSPFv3 エリア パラメータの設定	753
仮想リンク ネイバーの設定	754
OSPFv3 受動インターフェイスの設定	756
OSPFv3 アドミニストレーティブ ディスタンスの設定	756
OSPFv3 タイマーの設定	757
スタティック OSPFv3 ネイバーの定義	758
Syslog メッセージの送信	759
Syslog メッセージの抑止	760
集約ルート コストの計算	760
OSPFv3 ルーティング ドメインへのデフォルトの外部ルートの生成	760
IPv6 サマリー プレフィックスの設定	761
IPv6 ルートの再配布	762

グレースフル リスタートの設定	763
OSPFv2 のグレースフル リスタートの設定	764
OSPFv2 の Cisco NSF グレースフル リスタートの設定	764
OSPFv2 の IETF NSF グレースフル リスタートの設定	764
OSPFv3 のグレースフル リスタートの設定	765
OSPFv2 設定の削除	766
OSPFv3 設定の削除	766
OSPFv2 の例	766
OSPFv3 の例	768
OSPF のモニタリング	770
OSPF の履歴	772

 第 30 章
EIGRP 775

EIGRP について	775
EIGRP のガイドライン	777
EIGRP プロセスの設定	777
EIGRP の設定	778
EIGRP のイネーブル化	778
EIGRP スタブルルーティングのイネーブル化	780
EIGRP のカスタマイズ	781
EIGRP ルーティングプロセスのネットワークの定義	781
EIGRP のインターフェイスの設定	782
パッシブ インターフェイスの設定	783
インターフェイスでのサマリー集約アドレスの設定	784
インターフェイス遅延値の変更	785
インターフェイスでの EIGRP 認証のイネーブル化	786
EIGRP ネイバーの定義	787
EIGRP へのルート再配布	788
EIGRP でのネットワークのフィルタリング	790
EIGRP Hello 間隔と保持時間のカスタマイズ	792
自動ルート集約の無効化	793

EIGRP でのデフォルト情報の設定	793
EIGRP スプリット ホライズンのディセーブル化	795
EIGRP プロセスの再始動	796
EIGRP のモニタリング	796
EIGRP の履歴	797

第 31 章

マルチキャスト ルーティング 799

マルチキャスト ルーティングの概要	799
スタブ マルチキャスト ルーティング	800
PIM マルチキャスト ルーティング	800
マルチキャスト グループの概念	800
マルチキャスト アドレス	800
クラスター	801
マルチキャスト ルーティングのガイドライン	801
マルチキャスト ルーティングの有効化	802
マルチキャスト ルーティングのカスタマイズ	803
スタブ マルチキャスト ルーティングの設定と IGMP メッセージの転送	803
スタティック マルチキャスト ルートの設定	804
IGMP 機能の設定	805
インターフェイスでの IGMP の有効化	805
IGMP グループ メンバーシップの設定	805
スタティック加入した IGMP グループの設定	806
マルチキャスト グループへのアクセスの制御	807
インターフェイスにおける IGMP 状態の数の制限	808
マルチキャスト グループに対するクエリー メッセージの変更	808
IGMP バージョンの変更	810
PIM 機能の設定	810
インターフェイスでの PIM の有効化またはディセーブル化	810
スタティック ランデブー ポイントアドレスの設定	811
指定ルータのプライオリティの設定	812
PIM 登録メッセージの設定とフィルタリング	813

PIM メッセージ間隔の設定	813
ルート ツリーの設定	814
マルチキャスト グループの設定	815
PIM ネイバーのフィルタリング	815
双方向ネイバー フィルタの設定	816
マルチキャスト境界の設定	818
マルチキャストルーティングの例	819
マルチキャストルーティングの履歴	820

第 VI 部 :	AAA サーバおよびローカル データベース	823
----------	------------------------------	-----

第 32 章	AAA サーバとローカル データベース	825
	AAA とローカル データベースについて	825
	認証	825
	認証	826
	アカウントिंग	826
	認証、認可、アカウントング間の相互作用	826
	AAA Servers	826
	AAA Server Groups	827
	ローカル データベースについて	827
	フォールバック サポート	828
	グループ内の複数のサーバを使用したフォールバックの仕組み	829
	ローカル データベースのガイドライン	829
	ローカル データベースへのユーザ アカウントの追加	829
	ローカル データベースの認証および認可のテスト	831
	ローカル データベースのモニタリング	831
	ローカル データベースの履歴	832

第 33 章	AAA の RADIUS サーバ	833
--------	-------------------------	-----

	AAA 用の RADIUS サーバについて	833
	サポートされている認証方式	833

VPN 接続のユーザ認証	834
RADIUS 属性のサポートされるセット	834
サポートされる RADIUS 認証属性	835
サポートされる IETF RADIUS 認証属性	851
RADIUS アカウンティング切断の理由コード	853
AAA の RADIUS サーバのガイドライン	854
AAA 用の RADIUS サーバの設定	855
RADIUS サーバグループの設定	855
グループへの RADIUS サーバの追加	858
認証プロンプトの追加	860
RADIUS サーバの認証および認可のテスト	861
AAA 用の RADIUS サーバのモニタリング	861
AAA 用の RADIUS サーバの履歴	862

第 34 章

AAA 用の TACACS+ サーバ	863
AAA 用の TACACS+ サーバについて	863
TACACS+ 属性	863
AAA 用の TACACS+ サーバのガイドライン	865
TACACS+ サーバの設定	865
TACACS+ サーバグループの設定	866
グループへの TACACS+ サーバの追加	867
認証プロンプトの追加	868
TACACS+ サーバの認証および許可のテスト	869
AAA 用の TACACS+ サーバのモニタリング	869
AAA 用の TACACS+ サーバの履歴	870

第 35 章

AAA の LDAP サーバ	871
LDAP および ASA について	871
LDAP での認証方法	871
LDAP 階層	872
LDAP 階層の検索	873

LDAP サーバへのバインド	874
LDAP 属性マップ	874
AAA の LDAP サーバのガイドライン	875
AAA の LDAP サーバの設定	876
LDAP 属性マップの設定	876
LDAP サーバグループの設定	877
LDAP サーバのサーバグループへの追加	878
LDAP サーバによる認証および許可のテスト	880
AAA の LDAP サーバのモニタリング	881
AAA の LDAP サーバの履歴	881

第 VII 部 : システム管理 883

第 36 章 管理アクセス 885

管理リモートアクセスの設定	885
HTTPS (ASDM) 、Telnet、または SSH の ASA アクセス	885
HTTPS (ASDM) アクセスの設定	886
SSH アクセスの設定	887
Telnet アクセスの設定	892
ASDM アクセスまたはクライアントレス SSL VPN のための HTTP リダイレクトの設定	893
VPN トンネルを介した管理アクセスの設定	894
コンソールタイムアウトの変更	894
CLI プロンプトのカスタマイズ	895
ログインバナーの設定	897
管理セッションクォータの設定	898
システム管理者用 AAA の設定	899
管理認証の設定	899
管理認証について	899
CLI、ASDM、および enable コマンドアクセス認証の設定	901
ASDM 証明書認証の設定	902

管理許可による CLI および ASDM アクセスの制限	903
コマンド認可の設定	905
コマンド認可について	906
ローカル コマンド許可の設定	907
TACACS+ サーバでのコマンドの設定	909
TACACS+ コマンド許可の設定	912
ローカル データベース ユーザのパスワード ポリシーの設定	913
パスワードの変更	914
管理アクセス アカウンティングの設定	915
ロックアウトからの回復	916
デバイス アクセスのモニタリング	917
管理アクセスの履歴	918
<hr/>	
第 37 章	ソフトウェアおよびコンフィギュレーション 923
ソフトウェアのアップグレード	923
ROMMON を使用したイメージのロード	923
ROMMON を使用した ASASM のイメージのロード	925
ROMMON イメージのアップグレード (ASA 5506-X、5508-X、および 5516-X)	927
ASA 5506W-X ワイヤレス アクセス ポイントのイメージの回復およびロード	928
ソフトウェアのダウングレード	929
ファイルの管理	930
ファイルアクセスの設定	931
FTP クライアント モードの設定	931
セキュア コピーサーバとしての ASA の設定	931
ASA TFTP クライアントのパス設定	933
マウント ポイントの追加	934
ファイル管理ツールへのアクセス	935
ファイルの転送	936
ローカル PC とフラッシュ間でのファイル転送	936
リモート サーバとフラッシュ間でのファイル転送	937
ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定	939

コンフィギュレーションまたはその他のファイルのバックアップおよび復元	941
完全なシステム バックアップまたは復元の実行	941
バックアップまた復元を開始する前に	941
システムのバックアップ	943
バックアップの復元	944
ローカル CA サーバのバックアップ	945
TFTP サーバへの実行コンフィギュレーションの保存	946
システム再起動のスケジュール	946
Auto Update の設定	947
Auto Update について	947
Auto Update クライアントまたはサーバ	947
Auto Update の利点	948
フェールオーバー設定での Auto Update サーバ サポート	948
Auto Update のガイドライン	950
Auto Update サーバとの通信の設定	951
Auto Update のモニタリング	953
Auto Update プロセスのモニタリング	953
ソフトウェアとコンフィギュレーションの履歴	954

第 38 章

システム イベントに対する応答の自動化	957
EEM について	957
サポートされるイベント	957
イベント マネージャ アプレットのアクション	958
出力先	958
EEM のガイドライン	959
EEM の設定	959
イベント マネージャ アプレットの作成とイベントの設定	960
アクションおよびアクションの出力先の設定	961
イベント マネージャ アプレットの実行	962
トラック メモリ割り当ておよびメモリ使用量	962
EEM のモニタリング	963

EEM の履歴 963

第 39 章

テストとトラブルシューティング 965

イネーブルパスワードと Telnet パスワードの回復 965

ASA のパスワードの回復 965

ASA 5506-X、ASA 5508-X、ASA 5516-X でのパスワードの回復 967

ASAv でのパスワードまたはイメージの回復 969

パスワード回復のディセーブル化 970

Packet Capture Wizard を使用したキャプチャの設定と実行 971

パケットキャプチャのガイドライン 974

入力トラフィック セレクタ 974

出力トラフィック セレクタ 975

Buffers 976

概要 976

キャプチャの実行 976

キャプチャの保存 977

ASAv の vCPU 使用量 977

CPU 使用率の例 977

VMware の CPU 使用率のレポート 978

ASAv のグラフと vCenter のグラフ 978

設定のテスト 979

基本接続のテスト：アドレス向けの ping の実行 979

ping で実行可能なテスト 979

ICMP ping と TCP ping の選択 980

ICMP の有効化 980

ホストの ping 982

ASA 接続の体系的なテスト 982

ホストまでのルートの追跡 985

トレースルート上の ASA の表示 985

パケットルートの決定 986

パケット トレーサを使用したポリシー設定のテスト 987

パフォーマンスとシステム リソースのモニタリング	988
パフォーマンスのモニタリング	988
メモリ ブロックのモニタリング	989
CPU のモニタリング	989
メモリのモニタリング	990
プロセス単位の CPU 使用率のモニタリング	990
接続のモニタリング	991

第 VIII 部 : **モニタリング 993**

第 40 章 **ロギング 995**

ロギングの概要	995
マルチ コンテキスト モードでのロギング	996
syslog メッセージ分析	996
syslog メッセージ形式	997
重大度	997
syslog メッセージ フィルタリング	998
syslog メッセージ クラス	998
ログ ビューアのメッセージのソート	1002
カスタム メッセージ リスト	1002
クラスタ	1002
ロギングのガイドライン	1003
ロギングの設定	1004
ロギングのイネーブル化	1004
出力先の設定	1005
外部 syslog サーバへの syslog メッセージの送信	1005
内部ログ バッファへの syslog メッセージの送信	1009
電子メール アドレスへの syslog メッセージの送信	1011
コンソール ポートへの syslog メッセージの送信	1013
Telnet または SSH セッションへの syslog メッセージの送信	1013
syslog メッセージの設定	1014

syslog メッセージの設定	1014
syslog ID 設定の編集	1015
非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力	1016
syslog メッセージに日付と時刻を含める	1016
syslog メッセージの無効化	1016
syslog メッセージの重大度の変更	1017
スタンバイ装置の syslog メッセージのブロック	1017
非 EMBLEM 形式の syslog メッセージにデバイス ID を含める	1017
カスタム イベント リストの作成	1018
ロギング フィルタの設定	1019
ロギングの宛先へのメッセージ フィルタの適用	1019
ロギング フィルタの適用	1020
syslog メッセージ ID フィルタの追加または編集	1021
メッセージ クラスと重大度 フィルタの追加または編集	1021
指定した出力先へのクラス内のすべての syslog メッセージの送信	1022
syslog メッセージの生成レートの制限	1022
個々の syslog メッセージに対するレート制限の割り当てまたは変更	1023
syslog メッセージに対するレート制限の追加または編集	1023
syslog 重大度に対するレート制限の編集	1024
ログのモニタリング	1024
ログ ビューアを使用した syslog メッセージのフィルタリング	1024
フィルタリング設定の編集	1027
ログ ビューアを使用した特定のコマンドの発行	1027
ロギングの履歴	1028

第 41 章	SNMP	1033
	SNMP の概要	1033
	SNMP の用語	1034
	SNMP バージョン 3 の概要	1034
	セキュリティ モデル	1035
	SNMP グループ	1035

SNMP ユーザ	1035
SNMP ホスト	1035
ASA と Cisco IOS ソフトウェアの実装の相違点	1036
SNMP syslog メッセージ	1036
アプリケーション サービスとサードパーティ ツール	1036
SNMP のガイドライン	1037
SNMP を設定します。	1039
SNMP 管理ステーションの設定	1039
Configure SNMP Traps	1040
SNMP バージョン 1 または 2c のパラメータの設定	1040
SNMP バージョン 3 のパラメータの設定	1042
ユーザのグループの設定	1043
SNMP モニタリング	1044
SNMP の履歴	1045

 第 42 章

Anonymous Reporting および Smart Call Home	1051
Anonymous Reporting について	1051
DNS 要件	1052
Smart Call Home の概要	1052
Anonymous Reporting および Smart Call Home のガイドライン	1053
Anonymous Reporting および Smart Call Home の設定	1054
Anonymous Reporting の設定	1054
Smart Call Home の設定	1055
Anonymous Reporting および Smart Call Home のモニタリング	1059
Anonymous Reporting および Smart Call Home の履歴	1060

 第 IX 部 :

参照先	1063
------------	-------------

 第 43 章

アドレス、プロトコル、およびポート	1065
IPv4 アドレスとサブネット マスク	1065
クラス	1065

プライベート ネットワーク	1066
サブネット マスク	1066
サブネットマスクの決定	1067
サブネットマスクに使用するアドレスの決定	1068
IPv6 アドレス	1069
IPv6 アドレスの形式	1070
IPv6 アドレス タイプ	1071
ユニキャストアドレス	1071
マルチキャストアドレス	1073
エニーキャストアドレス	1075
必須アドレス	1075
IPv6 アドレス プレフィックス	1076
プロトコルとアプリケーション	1076
TCP ポートおよび UDP ポート	1077
ローカル ポートとプロトコル	1081
ICMP タイプ	1082



このマニュアルについて

ここでは、このガイドを使用する方法について説明します。

- 本書の目的 (xlvi ページ)
- 関連資料 (xlvi ページ)
- 表記法 (xlvii ページ)
- 通信、サービス、およびその他の情報 (xlix ページ)

本書の目的

このマニュアルの目的は、Adaptive Security Device Manager (ASDM) を使用して、Cisco ASA シリーズ用の一般的な動作の設定を支援することです。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。



-
- (注) ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンラインヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。各 ASA のバージョンでサポートされている ASDM の最小バージョンについては、『*Cisco ASA Series Compatibility*』を参照してください。
-

関連資料

詳細については、『*Navigating the Cisco ASA Series Documentation*』 (<http://www.cisco.com/go/asadocs>) を参照してください。

表記法

このマニュアルでは、文字、表示、および警告に関する次の規則に準拠しています。

文字表記法

表記法	説明
boldface	コマンド、キーワード、ボタンラベル、フィールド名、およびユーザ入力テキストは、 boldface で示しています。メニューベースコマンドの場合は、メニュー項目を [] で囲み、コマンドのフルパスを示しています。
<i>italic</i>	ユーザが値を指定する変数は、イタリック体で示しています。 イタリック体は、マニュアルタイトルと一般的な強調にも使用されています。
等幅	システムが表示するターミナルセッションおよび情報は、等幅文字で記載されます。
{x y z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[]	角カッコの中の要素は、省略可能です。
[x y z]	いずれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
[]	システムプロンプトに対するデフォルトの応答も、角カッコで囲んで記載されます。
<>	パスワードなどの出力されない文字は、山カッコ (<>) で囲んで示しています。
!, #	コードの先頭に感嘆符 (!) または番号記号 (#) がある場合は、コメント行であることを示します。

読者への警告

このマニュアルでは、読者への警告に以下を使用しています。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



ヒント 「問題解決に役立つ情報」です。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



ワンポイントアドバイス

時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。



警告 「警告」の意味です。人身事故を予防するための注意事項が記述されています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#)にアクセスしてください。
- サービス リクエストを送信するには、[シスコ サポート](#)にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

Cisco バグ検索ツール

[Cisco Bug Search Tool](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



第 1 部

ASA の開始

- [Cisco ASA の概要 \(1 ページ\)](#)
- [使用する前に \(27 ページ\)](#)
- [ASDM グラフィカル ユーザ インターフェイス \(61 ページ\)](#)
- [ライセンス：製品認証キー ライセンス \(105 ページ\)](#)
- [ライセンス：スマート ソフトウェア ライセンス \(ASA v、ASA on Firepower\) \(169 ページ\)](#)
- [論理デバイス Firepower 9300 \(191 ページ\)](#)
- [トランスペアレントファイアウォールモードまたはルーテッドファイアウォールモード \(207 ページ\)](#)
- [Startup Wizard \(231 ページ\)](#)



第 1 章

Cisco ASA の概要

Cisco ASA は、追加モジュールとの統合サービスに加え、高度なステートフルファイアウォールおよび VPN コンセントレータ機能を 1 つのデバイスで提供します。ASA は、複数のセキュリティコンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを 1 つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォールオペレーション、高度なインスペクションエンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。



(注) ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンラインヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。ASA の各バージョンでサポートされている ASDM の最小バージョンについては、『Cisco ASA Compatibility (Cisco ASA の互換性)』[英語]を参照してください。特殊なサービス非推奨のサービスおよびレガシーサービス (25 ページ) も参照してください。

- [ASDM 要件 \(2 ページ\)](#)
- [ハードウェアとソフトウェアの互換性 \(6 ページ\)](#)
- [VPN の互換性 \(6 ページ\)](#)
- [新機能 \(6 ページ\)](#)
- [ファイアウォール機能の概要 \(19 ページ\)](#)
- [VPN 機能の概要 \(24 ページ\)](#)
- [セキュリティ コンテキストの概要 \(25 ページ\)](#)
- [ASA クラスタリングの概要 \(25 ページ\)](#)
- [特殊なサービス非推奨のサービスおよびレガシー サービス \(25 ページ\)](#)

ASDM 要件

ASDM Java の要件

ASDM は、Oracle JRE 8.0を使用してインストールできます。OpenJRE はサポートされていません。

表 1: ASA と ASA FirePOWER : ASDM オペレーティング システムとブラウザの要件

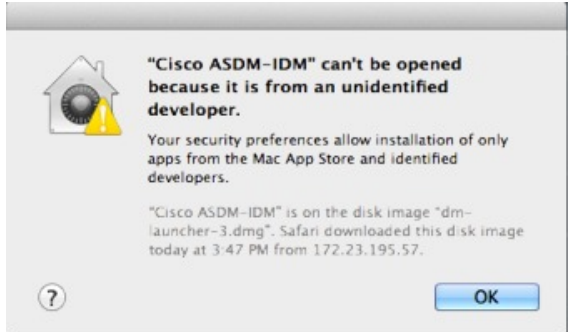
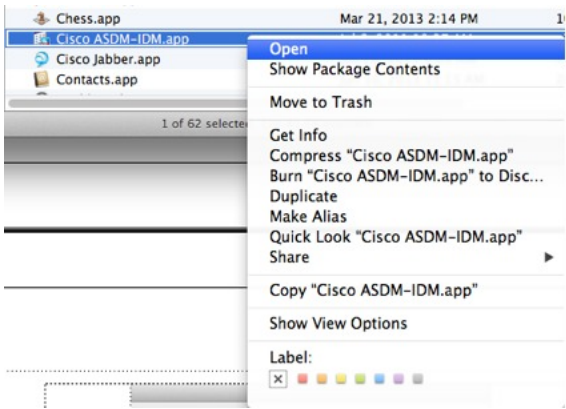

オペレーティング システム	ブラウザ				Oracle JRE
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows (英語および日本語) : 8 7 Server 2012 Server 2008	対応	対応	サポートなし	対応	8.0
Apple OS X 10.4 以降	サポートなし	対応	対応	Yes (64 ビットバージョンのみ)	8.0
Ubuntu Linux 14.04 Debian Linux 7	該当なし	対応	該当なし	対応	8.0

ASDM の互換性に関する注意事項

次の表に、ASDM の互換性に関する警告を示します。

条件	注意
<p>ASA では高度暗号化ライセンス (3DES/AES) が必要</p> <p>(注) スマートライセンスモデルを使用すると、高度暗号化ライセンスを使用せずに ASDM での最初のアクセスが可能になります。</p>	<p>ASDM では、ASA に SSL 接続する必要があります。シスコが提供している 3DES ライセンスを要求できます。</p> <ol style="list-style-type: none"> 1. www.cisco.com/go/license にアクセスします。 2. [Continue to Product License Registration] をクリックします。 3. ライセンシング ポータルで、テキストフィールドの横にある [Get Other Licenses] をクリックします。 4. ドロップダウンリストから、[IPS, Crypto, Other...] を選択します。 5. [Search by Keyword] フィールドに「ASA」と入力します。 6. [Product] リストで [Cisco ASA 3DES/AES License] を選択し、[Next] をクリックします。 7. ASA のシリアル番号を入力し、プロンプトに従って ASA の 3DES/AES ライセンスを要求します。
<ul style="list-style-type: none"> • 自己署名証明書または信頼できない証明書 • IPv6 • Firefox および Safari 	<p>ASA が自己署名証明書または信頼できない証明書を使用する場合、Firefox と Safari では、IPv6 を介した HTTPS を使用して参照する場合にはセキュリティ例外を追加することはできません。</p> <p>https://bugzilla.mozilla.org/show_bug.cgi?id=633001 を参照してください。この警告は、Firefox または Safari から ASA に発信されるすべての SSL 接続に影響します (ASDM 接続を含む)。この警告を回避するには、信頼できる認証局が ASA に対して発行した適切な証明書を設定します。</p>
<ul style="list-style-type: none"> • ASA で SSL 暗号化を行うには、RC4-MD5 と RC4-SHA1 を両方とも含めるか、Chrome で SSL false start を無効にする必要があります。 • Chrome 	<p>RC4-MD5 および RC4-SHA1 アルゴリズム (これらのアルゴリズムはデフォルトでイネーブル) の両方を除外するために ASA の SSL 暗号化を変更した場合、Chrome の「SSL false start」機能のために Chrome は ASDM を起動できません。これらのアルゴリズムの1つを再度有効にすることを推奨します ([Configuration] > [Device Management] > [Advanced] > [SSL Settings] ペインを参照)。または、Run Chromium with flags に従って <code>--disable-ssl-false-start</code> フラグを使用して Chrome の SSL false start を無効にできます。</p>

条件	注意
サーバの IE9	サーバの Internet Explorer 9.0 の場合は、[Do not save encrypted pages to disk] オプションがデフォルトで有効になっています（[Tools] > [Internet Options] > [Advanced] を参照）。このオプションでは、最初の ASDM のダウンロードは失敗します。ASDM でダウンロードを行うには、このオプションを確実にディセーブルにしてください。
OS X	OS X では、ASDM の初回実行時に、Java のインストールを要求される場合があります。必要に応じて、プロンプトに従います。インストールの完了後に ASDM が起動します。

条件	注意
OS X 10.8 以降	<p>ASDM は Apple Developer ID で署名されていないため、実行できるようにする必要があります。セキュリティの設定を変更しないと、エラー画面が表示されます。</p>  <ol style="list-style-type: none"> ASDM を実行できるようにするには、[Cisco ASDM-IDM Launcher] アイコンを右クリック（または Ctrl キーを押しながらクリック）して、[Open] を選択します。  <ol style="list-style-type: none"> 同様のエラー画面が表示されますが、この画面から ASDM を起動できます。[Open] をクリックします。ASDM-IDM ランチャが起動します。 

条件	注意
Windows 10	<p>「This app can't run on your PC」エラーメッセージ。</p> <p>ASDM ランチャをインストールすると、Windows 10 によって ASDM ショートカットターゲットが Windows Scripting Host パスに置き換えられて、このエラーが発生することがあります。ショートカットターゲットを修正するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [Start] > [Cisco ASDM-IDM Launcher] を選択し、[Cisco ASDM-IDM Launcher] アプリケーションを右クリックします。 2. [More] > [Open file location] を選択します。 Windows は、ショートカットアイコンを使用してディレクトリを開きます。 3. ショートカットアイコンを右クリックして、[Properties] を選択します。 4. [Target] を次のように変更します。 C:\Windows\System32\wscript.exe invisible.vbs run.bat 5. [OK] をクリックします。

ハードウェアとソフトウェアの互換性

サポートされるすべてのハードウェアおよびソフトウェアの一覧は、『[Cisco ASA Compatibility \(Cisco ASA の互換性\)](#)』[英語]を参照してください。

VPN の互換性

『[Supported VPN Platforms, Cisco ASA Series](#)』[英語]を参照してください。

新機能

このセクションでは、各リリースの新機能を示します。



(注) 『syslog メッセージガイド』に、新規、変更済み、および廃止された syslog メッセージを記載しています。

ASA 9.4(4.5)/ASDM 7.6(2) の新機能

リリース：2017年4月3日



(注) バージョン 9.4(4) は、バグ [CSCvd78303](#) のため、Cisco.com から削除されました。

このリリースに新機能はありません。

ASA 9.4(3)/ASDM 7.6(1) の新機能

リリース：2016年4月25日

機能	説明
ファイアウォール機能	
ルートの収束に対する接続ホールドダウンタイムアウト。	<p>接続で使用されているルートがもう存在していない、または非アクティブになったときに、システムが接続を保持する時間を設定できるようになりました。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。ルートの収束がさらに迅速に行われるようにホールドダウンタイマーを短縮することができます。ただし、ほとんどのネットワークでは、ルートのフラッピングを防止するためにデフォルトの 15 秒が適切です。</p> <p>次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [Global Timeouts]</p>
リモート アクセス機能	
設定可能な SSH 暗号機能と HMAC アルゴリズム	<p>ユーザは SSH 暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。</p> <p>次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [SSH Ciphers]</p> <p>9.1(7) でも使用可能です。</p>
IPv6 の HTTP リダイレクトサポート	<p>ASDM アクセスまたはクライアントレス SSL VPN 用の HTTPS に HTTP リダイレクトを有効にすると、IPv6 アドレスへ送信されるトラフィックもリダイレクトできるようになりました。</p> <p>次の画面に機能が追加されました。[Configuration] > [Device Management] > [HTTP Redirect]</p> <p>9.1(7) でも使用可能です。</p>
モニタリング機能	

機能	説明
フェールオーバーの SNMP engineID の同期	<p>フェールオーバー ペアでは、一対の ASA の SNMP engineID は両方のユニットで同期されます。ASA ごとに、同期された engineID、ネイティブ engineID、およびリモート engineID による engineID が 3 セット維持されます。</p> <p>SNMPv3 ユーザは、ローカライズされた snmp-server user 認証とプライバシー オプションを保存するためのプロファイルを作成するときに ASA の engineID も指定できます。ユーザがネイティブ engineID を指定しない場合、show running config 出力に engineID がユーザごとに 2 つずつ表示されます。</p> <p>次のコマンドが変更されました。 snmp-server user ASDM サポートはありません。</p>
show tech support の強化	<p>show tech support コマンドは現在次のとおりです。</p> <ul style="list-style-type: none"> • dir all-filesystems の出力が含まれます。この出力は次の場合に役立つことがあります。 <ul style="list-style-type: none"> • SSL VPN コンフィギュレーション：必要なリソースが ASA にあるかどうかを確認します。 • クラッシュ：クラッシュファイルの日付のタイムスタンプと存在を確認します。 • show kernel cgroup-controller detail の出力の削除：このコマンド出力は show tech-support detail の出力内に残されます。 <p>追加または変更された画面はありません。</p> <p>9.1(7) でも使用可能です。</p>
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	<p>CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプールモニタリング エントリのテーブルです。</p> <p>(注) CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポートをサポートします。</p> <p>追加または変更された画面はありません。</p> <p>9.1(7) でも使用可能です。</p>

ASA 9.4(2.145)/ASDM 7.5(1) の新機能

リリース：2015年11月13日

このリリースに新機能はありません。



(注) このリリースは Firepower 9300 ASA セキュリティ モジュールのみをサポートします。

ASA 9.4(2)/ASDM 7.5(1) の新機能

リリース : 2015年9月24日

このリリースに新機能はありません。



(注) ASA 9.4(1.200) の各機能はこのリリースには含まれません。



(注) このバージョンは ISA 3000 をサポートしません。

ASA 9.4(1.225)/ASDM 7.5(1) の新機能

リリース : 2015年9月17日



(注) このリリースは Cisco ISA 3000 のみをサポートします。

機能	説明
プラットフォーム機能	
Cisco ISA 3000 サポート	<p>Cisco ISA 3000 は、DIN レールにマウントされた高耐久型の産業用セキュリティアプライアンスです。ギガビットイーサネットと専用管理ポートを備えた、低消費電型ファンレス デバイスです。このモデルには ASA Firepower モジュールが事前にインストールされています。このモデルの特別な機能として、カスタマイズされたトランスペアレントモードのデフォルト設定と、電源喪失時もトラフィックがアプライアンスを通過することを可能にするハードウェア バイパス機能があります。</p> <p>次の画面が導入されました。[Configuration] > [Device Management] > [Hardware Bypass]</p> <p>hardware-bypass boot-delay コマンドは ASDM 7.5(1) では使用できません。</p> <p>この機能は、バージョン 9.5(1) では使用できません。</p>

ASA 9.4(1.152)/ASDM 7.4(3) の新機能

リリース : 2015年7月13日



(注) このリリースは、Firepower 9300 の ASA のみをサポートします。

機能	説明
プラットフォーム機能	
Firepower 9300 の ASA セキュリティ モジュール	<p>Firepower 9300 の ASA セキュリティ モジュールに ASA を導入しました。</p> <p>(注) Firepower Chassis Manager 1.1.1 は Firepower 9300 の ASA セキュリティ モジュールの VPN 機能 (サイト間またはリモート アクセス) を一切サポートしません。</p>
ハイ アベイラビリティ機能	
Firepower 9300 用シャーシ内 ASA クラスタリング	<p>FirePOWER 9300 シャーシ内では、最大 3 つセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。</p> <p>次の画面を導入しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]</p>
ライセンス機能	
Firepower 9300 の ASA のシスコ スマートソフトウェア ライセンシング	<p>FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Smart License]</p>

ASAv 9.4(1.200)/ASDM 7.4(2) の新機能

リリース : 2015年5月12日



(注) このリリースは、ASAv のみをサポートします。

機能	説明
プラットフォーム機能	

機能	説明
VMware 上の ASAv では vCenter サポートは不要になりました。	vCenter なしで、vSphere クライアントまたは OVFTool のデイゼロ設定を使用して ASAv を VMware 上にインストールできるようになりました。
Amazon Web Services (AWS) の ASAv	Amazon Web Services (AWS) とデイゼロ設定で ASAv を使用できるようになりました。 (注) Amazon Web Services は ASAv10 と ASAv30 のモデルのみをサポートします。

ASDM 7.4(2) の新機能

リリース : 2015年5月6日

機能	説明
リモート アクセス機能	
AnyConnect バージョン 4.1 のサポート	ASDM は AnyConnect バージョン 4.1 をサポートできるようになりました。 次の画面が変更されました。[Configuration]>[Remote Access VPN]>[Network (Client) Access]>[AnyConnect Client Profile] ([AMP Enabler Service Profile] という新しいプロファイル)

ASA 9.4(1)/ASDM 7.4(1) の新機能

リリース : 2015年3月30日

機能	説明
プラットフォーム機能	
ASA 5506W-X、ASA 5506H-X、ASA 5508-X、ASA 5516-X	ワイヤレスアクセスポイントを内蔵した ASA 5506W-X、強化された ASA 5506H-X、ASA 5508-X、ASA 5516-X の各モデルが導入されました。 変更された ASDM 画面はありません。
認定機能	

機能	説明
国防総省 (DoD) 統一機能規則 (UCR) 2013 証明書	<p>ASA は、DoD UCR 2013 規則を遵守するように更新されています。この証明書に追加された次の機能については、この表の行を参照してください。</p> <ul style="list-style-type: none"> • 定期的な証明書認証 • 証明書有効期限のアラート • 基本制約 CA フラグの適用 • 証明書コンフィギュレーションの ASDM ユーザ名 • ASDM 管理認証 • IKEv2 無効セレクタの通知設定 • 16 進数の IKEv2 事前共有キー
FIPS 140-2 認証のコンプライアンス更新	<p>ASA で FIPS モードを有効にすると、ASA が FIPS 140-2 に準拠するように追加制限が設定されます。次の制限があります。</p> <ul style="list-style-type: none"> • RSA および DH キーサイズの制限：RSA および DH キー 2K (2048 ビット) 以上のみが許可されます。DH の場合、これはグループ 1 (768 ビット)、2 (1024 ビット)、5 (1536 ビット) が許可されないことを意味します。 <p>(注) キーサイズの制限により、FIPS での IKEv1 の使用が無効になります。</p> <ul style="list-style-type: none"> • デジタル署名のハッシュアルゴリズムの制限：SHA 256 以上のみが許可されます。 • SSH 暗号の制限：許可された暗号は aes128-cbc または aes256-cbc です。MAC は SHA1 です。 <p>ASA の FIPS 認証ステータスを表示するには、次の URL を参照してください。 http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProgress.pdf</p> <p>この PDF は毎週更新されます。</p> <p>詳細については、Computer Security Division Computer Security Resource Center のサイトを参照してください。 http://csrc.nist.gov/groups/STM/cmvp/inprocess.html</p> <p>fips enable コマンドが変更されました。</p>
ファイアウォール機能	

機能	説明
複数のコアを搭載した ASA での SIP インспекションのパフォーマンスが向上。	複数のコアで ASA を通過する SIP シグナリングが複数存在する場合の SIP インспекションパフォーマンスが向上しました。ただし、TLS、電話、または IME プロキシを使用する場合、パフォーマンスの向上は見られません。 変更された画面はありません。
電話プロキシおよび UC-IME プロキシに対する SIP インспекションのサポートが削除されました。	SIP インспекションを設定する際、電話プロキシまたは UC-IME プロキシは使用できなくなります。暗号化されたトラフィックを検査するには、TLS プロキシを使用します。 [Select SIP Inspect Map] サービス ポリシー ダイアログボックスから [Phone Proxy] と [UC-IME Proxy] が削除されました。
ISystemMapper UUID メッセージ RemoteGetObject opnum3 の DCERPC インспекションのサポート。	ASA は、リリース 8.3 で EPM 以外の DCERPC メッセージのサポートを開始し、ISystemMapper UUID メッセージ RemoteCreateInstance opnum4 をサポートしています。この変更により、RemoteGetObject opnum3 メッセージまでサポートが拡張されます。 変更された画面はありません。
コンテキストごとに無制限の SNMP サーバトラップホスト	ASA では、コンテキストごとに SNMP サーバのトラップホスト数の制限がありません。show snmp-server host コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。 変更された画面はありません。
VXLAN パケットインспекション	ASA は、標準形式に準拠するために VXLAN ヘッダーを検査できます。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [Protocol Inspection]
IPv6 の DHCP モニタリング	IPv6 の DHCP 統計情報および DHCP バインディングをモニタできます。 次の画面が導入されました。 [Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Statistics Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Binding]
ESMTP インспекションの TLS セッションでのデフォルトの動作が変更されました。	ESMTP インспекションのデフォルトが、検査されない、TLS セッションを許可するように変更されました。ただし、このデフォルトは新しい、または再イメージングされたシステムに適用されます。no allow-tls を含むシステムをアップグレードする場合、このコマンドは変更されません。 デフォルトの動作の変更は、古いバージョンでも行われました：8.4 (7.25)、8.5 (1.23)、8.6 (1.16)、8.7 (1.15)、9.0 (4.28)、9.1 (6.1)、9.2 (3.2)、9.3 (1.2)、9.3 (2.2)。
ハイアベイラビリティ機能	

機能	説明
スタンバイ ASA での syslog 生成のブロック	<p>スタンバイ装置で特定の syslog の生成をブロックできます。</p> <p>変更された画面はありません。</p>
インターフェイスごとに ASA クラスターのヘルス モニタリングをイネーブルまたはディセーブル	<p>ヘルスモニタリングは、インターフェイスごとにイネーブルまたはディセーブルにすることができます。デフォルトでは、ポートチャネル、冗長、および単一のすべての物理インターフェイスでヘルスモニタリングがイネーブルになっています。ヘルスモニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスター制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]</p>
DHCP リレーの ASA クラスターリングのサポート	<p>ASA クラスターで DHCP リレーを設定できます。クライアントの DHCP 要求は、クライアントの MAC アドレスのハッシュを使用してクラスターメンバにロードバランスされます。DHCP クライアントおよびサーバ機能はサポートされていません。</p> <p>変更された画面はありません。</p>
ASA クラスターリングでの SIP インспекションのサポート	<p>ASA クラスターで SIP インспекションを設定できます。制御フローは、任意のユニットで作成できますが（ロードバランシングのため）、その子データフローは同じユニットに存在する必要があります。TLS プロキシ設定はサポートされていません。</p> <p>変更された画面はありません。</p>
ルーティング機能	
Policy Based Routing : ポリシーベース ルーティング	<p>ポリシーベース ルーティング (PBR) は、ACL を使用して指定された QoS でトラフィックが特定のパスを経由するために使用するメカニズムです。ACL では、パケットのレイヤ 3 およびレイヤ 4 ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックに QoS を提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチドパスの間でインタラクティブトラフィックとバッチトラフィックを分散でき、インターネット サービス プロバイダーとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザから送信されるトラフィックをルーティングできます。</p> <p>次の画面が導入または変更されました。</p> <p>[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Policy Based Routing] [Configuration] > [Device Setup] > [Routing] > [Interface Settings] > [Interfaces]</p>
インターフェイス機能	

機能	説明
VXLAN のサポート	<p>VXLAN のサポートが追加されました (VXLAN トンネルエンドポイント (VTEP) のサポートを含む)。ASA またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを定義できます。</p> <p>次の画面が導入されました。</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VNI Interface] [Configuration] > [Device Setup] > [Interface Settings] > [VXLAN]</p>
モニタリング機能	
EEM のメモリ トラッキング	<p>メモリの割り当てとメモリの使用状況をログに記録してメモリ ロギングのラップ イベントに反応するための新しいデバッグ機能が追加されました。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager] > [Add Event Manager Applet] > [Add Event Manager Applet Event]</p>
トラブルシューティングのクラッシュ	<p>show tech-support コマンドの出力と show crashinfo コマンドの出力には、生成された syslog の最新 50 行が含まれます。これらの結果を表示できるようにするには、logging buffer コマンドをイネーブルにする必要があります。</p>
リモート アクセス機能	
ECDHE-ECDSA 暗号のサポート	<p>TLSv1.2 では、次の暗号のサポートが追加されています。</p> <ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 <p>(注) 優先度が最も高いのは ECDSA 暗号および DHE 暗号です。</p> <p>次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]。</p>

機能	説明
クライアントレス SSL VPN セッション Cookie アクセスの制限	<p>クライアントレス SSL VPN セッション Cookie が JavaScript などのクライアント側のスクリプトを介してサードパーティからアクセスされないようにすることができます。</p> <p>(注) この機能は、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、次のクライアントレス SSL VPN 機能が警告なしで動作しなくなるため、セキュリティ上のリスクが発生します。</p> <ul style="list-style-type: none"> • Java プラグイン • Java リライタ • ポート フォワーディング。 • ファイルブラウザ • デスクトップ アプリケーション (Microsoft Office アプリケーションなど) を必要とする Sharepoint 機能 • AnyConnect Web 起動 • Citrix Receiver、XenDesktop、および Xenon • その他の非ブラウザ ベース アプリケーションおよびブラウザ プラグイン ベースのアプリケーション <p>次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [HTTP Cookie]。</p> <p>この機能は、9.2(3) にもあります。</p>
セキュリティ グループ タギングを使用した仮想デスクトップのアクセス制御	<p>ASA では、内部アプリケーションおよび Web サイトへのクライアントレス SSL リモートアクセス用にセキュリティ グループ タギングベースのポリシー制御をサポートしています。この機能では、配信コントローラおよび ASA のコンテンツ変換エンジンとして XenDesktop による Citrix の仮想デスクトップ インフラストラクチャ (VDI) を使用します。</p> <p>詳細については、次の Citrix 製品のマニュアルを参照してください。</p> <ul style="list-style-type: none"> • XenDesktop および XenApp のポリシー : http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • XenDesktop 7 でのポリシーの管理 : http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • XenDesktop 7 のポリシー用のグループ ポリシー エディタの使用 : http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html

機能	説明
クライアントレスSSL VPN に OWA 2013 機能のサポートを追加	<p>クライアントレス SSL VPN では、以下を除き、OWA 2013 の新機能をサポートしています。</p> <ul style="list-style-type: none"> • タブレットおよびスマートフォンのサポート • オフライン モード • Active Directory Federation Services (AD FS) 2.0. ASA および AD FS 2.0 は、暗号化プロトコルをネゴシエートできません。 <p>変更された画面はありません。</p>
クライアントレスSSL VPN に Citrix XenDesktop 7.5 および StoreFront 2.5 のサポートを追加	<p>クライアントレス SSL VPN では、XenDesktop 7.5 および StoreFront 2.5 のアクセスをサポートしています。</p> <p>XenDesktop 7.5 の機能の完全なリストと詳細については、http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html を参照してください。</p> <p>StoreFront 2.5 の機能の完全なリストと詳細については、http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html を参照してください。</p> <p>変更された画面はありません。</p>
定期的な証明書認証	<p>定期的な証明書認証を有効にすると、ASA は、VPN クライアントから受信した証明書チェーンを保存し、それらを定期的に再認証します。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] [Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]</p>
証明書有効期限のアラート	<p>ASA は、トラスト ポイントですべての CA および ID の証明書の有効期限について 24 時間ごとにチェックします。証明書の有効期限がまもなく切れる場合は、syslog がアラートとして発行されます。リマインダおよび繰り返しの間隔を設定できます。デフォルトでは、リマインダは有効期限の 60 日前に開始し、7 日ごとに繰り返されます。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] [Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]</p>

機能	説明
基本制約 CA フラグの適用	<p>デフォルトでは、CA フラグのない証明書を CA 証明書として ASA にインストールできなくなりました。基本制約拡張は、証明書のサブジェクトが CA で、この証明書を含む有効な認証パスの最大深さかどうかを示すものです。必要に応じて、これらの証明書のインストールを許可するように ASA を設定できます。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]</p>
IKEv2 無効セレクタの通知設定	<p>現在、ASA が SA 上で着信パケットを受信し、そのパケットのヘッダーフィールドが SA 用のセレクタに適合しなかった場合、ASA はそのパケットを廃棄します。ピアへの IKEv2 通知の送信をイネーブルまたはディセーブルにすることができます。この通知の送信はデフォルトで無効になっています。</p> <p>(注) この機能は、AnyConnect 3.1.06060 以降でサポートされています。</p>
16 進数の IKEv2 事前共有キー	16 進数の IKEv2 事前共有キーを設定できます。
管理機能	
ASDM 管理認証	<p>HTTP アクセスと Telnet および SSH アクセス別に管理認証を設定できるようになりました。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]</p>
証明書コンフィギュレーションの ASDM ユーザ名	<p>ASDM の証明書認証を有効にすると、ASDM が証明書からユーザ名を抽出する方法を設定できます。また、ログインプロンプトでユーザ名を事前に入力して表示できます。</p> <p>次の画面が導入されました。[Configuration] > [Device Management] > [Management Access] > [HTTP Certificate Rule]</p>
CLI で ? の入力時にヘルプを有効または無効にするための terminal interactive コマンド	<p>通常、ASA CLI で ? を入力すると、コマンドヘルプが表示されます。コマンド内にテキストとして ? を入力できるようにするには（たとえば、URL の一部として ? を含めるには）、no terminal interactive コマンドを使用してインタラクティブなヘルプを無効にします。</p> <p>次のコマンドが導入されました。terminal interactive</p>
REST API の機能	
REST API バージョン 1.1	REST API バージョン 1.1 のサポートが追加されました。
トークンベース認証が（既存の基本認証に加えて）サポートされるようになりました。	<p>クライアントは特定の URL にログイン要求を送信でき、成功すると、（応答ヘッダーに）トークンが返されます。クライアントはさらなる API コールを送信するために、（特別な要求ヘッダー内で）このトークンを使用します。トークンは明示的に無効にするまで、またはアイドル/セッションタイムアウトに到達するまで有効です。</p>

機能	説明
マルチ コンテキスト モードの限定的なサポート	<p>REST API エージェントをマルチ コンテキスト モードで有効にできるようになりました。CLI コマンドはシステム コンテキスト モードでのみ発行できます（シングル コンテキスト モードと同じコマンド）。</p> <p>次のようにパススルー CLI の API コマンドを使用して、コンテキストを設定できます。</p> <pre>https://<asa_admin_context_ip>/api/cli?context=<context_name></pre> <p>context パラメータがない場合、要求は admin コンテキストに向けられたものとみなされます。</p>
高度な（粒状の）インスペクション	<p>次のプロトコルの詳細なインスペクションをサポートします。</p> <ul style="list-style-type: none"> • DNS over UDP • HTTP • ICMP • ICMP ERROR • RTSP • SIP • FTP • DCERPC • IP オプション • NetBIOS Name Server over IP • SQL*Net

ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザによる不正アクセスから内部ネットワークを保護します。また、ファイアウォールは、人事部門ネットワークをユーザネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバまたは FTP サーバなど、外部のユーザが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（非武装地帯（DMZ）と呼ばれる）上に配置します。ファイアウォールによって DMZ に許可されるアクセスは限定されますが、DMZ にあるのは公開サーバだけのため、この地帯が攻撃されても影響を受けるのは公開サーバに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または認可を義務づける、または外部の URL フィルタリング サーバと協調するといった手段

によって、内部ユーザが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、外部ネットワークはファイアウォールの手前にあるネットワーク、内部ネットワークはファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数の *DMZ*、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用だけです。

セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティポリシーによって決められます。デフォルトでは、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。

アクセスルールによるトラフィックの許可または拒否

アクセスルールを適用することで、内部から外部に向けたトラフィックを制限したり、外部から内部に向けたトラフィックを許可したりできます。ブリッジグループ インターフェイスでは、EtherType アクセスルールを適用して、非 IP トラフィックを許可できます。

NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベートアドレスを使用できます。プライベートアドレスは、インターネットにルーティングできません。
- NAT はローカルアドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

IP フラグメントからの保護

ASA は、IP フラグメント保護を提供します。この機能は、すべての ICMP エラーメッセージの完全なリアセンブリと、ASA 経由でルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティチェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

HTTP、HTTPS、または FTP フィルタリングの適用

アクセスリストを使用して、特定の Web サイトまたは FTP サーバへの発信アクセスを禁止できますが、このような方法で Web サイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。

ASA でクラウド Web セキュリティを設定したり、URL およびその他のフィルタリングサービス（ASA CX や ASA FirePOWER など）を提供する ASA モジュールをインストールすることができます。ASA は、Cisco Web セキュリティ アプライアンス（WSA）などの外部製品とともに使用することも可能です。

アプリケーションインスペクションの適用

インスペクションエンジンは、ユーザのデータパケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリチャネルを開くサービスに必要です。これらのプロトコルは、ASA によるディープパケットインスペクションの実行を必要とします。

サポート対象のハードウェアモジュールまたはソフトウェアモジュールへのトラフィックの送信

一部の ASA モデルでは、ソフトウェアモジュールの設定、またはハードウェアモジュールのシャーシへの挿入を行うことで、高度なサービスを提供することができます。これらのモジュールを通じてトラフィックインスペクションを追加することにより、設定済みのポリシーに基づいてトラフィックをブロックできます。また、これらのモジュールにトラフィックを送信することで、高度なサービスを利用することができます。

QoS ポリシーの適用

音声やストリーミングビデオなどのネットワークトラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoS とは、選択したネットワークトラフィックによりよいサービスを提供するネットワークの機能です。

接続制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッドする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試みます（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャン脅威検出機能は、スキャンアクティビティに関して分析できるホスト統計を含む膨大なデータベースを維持します。

ホストデータベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービスポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。

ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- Transparent

ルーテッドモードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレントモードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータホップとは見なされません。ASA は「ブリッジグループ」の内部および外部インターフェイスと同じネットワークに接続します。

トランスペアレントファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレントモードは、攻撃者からファイアウォールが見えないようにする場合にも有効です。トランスペアレントファイアウォールは、他の場合にはルーテッドモードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレントファイアウォールでは、EtherType アクセスリストを使用するマルチキャストストリームが許可されます。

ステートフル インспекションの概要

ASA を通過するトラフィックはすべて、アダプティブセキュリティアルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケットフィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケット

シーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。



(注) TCP ステート バイパス機能を使用すると、パケット フローをカスタマイズできます。

ただし、ASA のようなステートフル ファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

新規の接続の場合、ASA は、パケットをアクセス リストと照合してチェックする必要があります。これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロールプレーンパス」も通過する場合があります。

セッション管理パスで行われるタスクは次のとおりです。

- アクセス リストとの照合チェック
- ルート ルックアップ
- NAT 変換 (xlates) の割り当て
- 「ファスト パス」でのセッションの確立

ASA は、TCP トラフィックのファスト パスに転送フローとリバース フローを作成します。ASA は、高速パスも使用できるように、UDP、ICMP (ICMP インスペクションがイネーブルの場合) などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファスト パスを使用できます。



(注) SCTP などの他の IP プロトコルの場合、ASA はリバース パス フローを作成しません。そのため、これらの接続を参照する ICMP エラー パケットはドロップされます。

レイヤ7インスペクションが必要なパケット (パケットのペイロードの検査または変更が必要) は、コントロールプレーンパスに渡されます。レイヤ7インスペクションエンジンは、2つ以上のチャネルを持つプロトコルが必要です。2つ以上のチャネルの1つは周知のポート番号を使用するデータチャネルで、その他はセッションごとに異なるポート番号を使用するコントロールチャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

- 確立済みの接続かどうか。

接続がすでに確立されている場合は、ASA でパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向で「ファースト」パスを通過できます。高速パスで行われるタスクは次のとおりです。

- IP チェックサム検証
- セッション ルックアップ
- TCP シーケンス番号のチェック
- 既存セッションに基づく NAT 変換
- レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

レイヤ 7 インスペクションを必要とするプロトコルに合致するデータ パケットも高速パスを通過できます。

確立済みセッション パケットの中には、セッション管理パスまたはコントロールプレーンパスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロールプレーンパスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロール パケットが含まれます。

VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーンパケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA は、次の機能を実行します。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザの認証
- ユーザ アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

セキュリティ コンテキストの概要

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチコンテキストモードでは、ルーティングテーブル、ファイアウォール機能、IPS、管理など、さまざまな機能がサポートされています。ただし、サポートされていない機能もあります。詳細については、機能に関する各章を参照してください。

マルチ コンテキストモードの場合、ASA には、セキュリティポリシー、インターフェイス、およびスタンドアロンデバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステムコンフィギュレーションに設定します。これが、シングルモード設定と同じく、スタートアップコンフィギュレーションとなります。システムコンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワークリソースにアクセスする必要があるときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただし、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システムコンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して、1つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、マスターユニット上でのみ実行します。コンフィギュレーションは、メンバユニットに複製されます。

特殊なサービス非推奨のサービスおよびレガシーサービス

一部のサービスのマニュアルは、主要な設定ガイドおよびオンラインヘルプとは別の場所にあります。

特殊なサービスに関するガイド

特殊なサービスを利用して、たとえば、電話サービス（Unified Communications）用のセキュリティプロキシを提供したり、ボットネットトラフィックフィルタリングを Cisco アップデートサーバのダイナミックデータベースと組み合わせて提供したり、Cisco Web セキュリティアプライアンス用の WCCP サービスを提供したりすることにより、ASA と他のシスコ製品の相互運用が可能になります。これらの特殊なサービスの一部については、別のガイドで説明されています。

- 『Cisco ASA Botnet Traffic Filter Guide』
- 『Cisco ASA NetFlow Implementation Guide』
- 『Cisco ASA Unified Communications Guide』
- 『Cisco ASA WCCP Traffic Redirection Guide』
- 『SNMP Version 3 Tools Implementation Guide』

非推奨のサービス

非推奨の機能については、ASA バージョンの設定ガイドを参照してください。同様に、設計の見直しが行われた機能（NAT（バージョン 8.2 と 8.3 の間に見直しを実施）、トランスペアレントモードのインターフェイス（バージョン 8.3 と 8.4 の間に見直しを実施）など）については、各バージョンの設定ガイドを参照してください。ASDM は以前の ASA リリースとの後方互換性を備えていますが、設定ガイドおよびオンラインヘルプでは最新のリリースの内容しか説明されていません。

レガシー サービス ガイド

レガシー サービスは現在も ASA でサポートされていますが、より高度なサービスを代わりに使用できる場合があります。レガシーサービスについては別のガイドで説明されています。

『Cisco ASA Legacy Feature Guide』

このマニュアルの構成は、次のとおりです。

- RIP の設定
- ネットワーク アクセスの AAA 規則
- IP スプーフィングの防止などの保護ツールの使用（**ip verify reverse-path**）、フラグメントサイズの設定（**fragment**）、不要な接続のブロック（**shun**）、TCP オプションの設定（ASDM 用）、および基本 IPS をサポートする IP 監査の設定（**ip audit**）。
- フィルタリング サービスの設定



第 2 章

使用する前に

この章では、Cisco ASA の使用を開始する方法について説明します。

- コマンドライン インターフェイス (CLI) のコンソールへのアクセス (27 ページ)
- ASDM アクセスの設定 (36 ページ)
- ASDM の起動 (42 ページ)
- ASDM 動作のカスタマイズ (44 ページ)
- 工場出荷時のデフォルト設定 (46 ページ)
- 設定の開始 (56 ページ)
- ASDM でのコマンドライン インターフェイス ツールの使用 (57 ページ)
- 接続の設定変更の適用 (59 ページ)

コマンドライン インターフェイス (CLI) のコンソールへのアクセス

ASDM アクセスの基本的な設定を、CLI を使用して行う必要がある場合があります。

初期設定を行うには、コンソールポートから直接 CLI にアクセスします。その後、[#unique_43](#) に従って Telnet または SSH を使用して、リモート アクセスを設定できます。システムがすでにマルチ コンテキスト モードで動作している場合は、コンソールポートにアクセスするとシステムの実行スペースに入ります。



(注) ASAv のコンソールアクセスについては、ASAv のクイック スタートガイドを参照してください。

アプライアンス コンソールへのアクセス

アプライアンス コンソールにアクセスするには、次の手順に従います。

手順

ステップ 1 付属のコンソール ケーブルを使用してコンピュータをコンソール ポートに接続します。ターミナルエミュレータを回線速度 9600 ボー、データ ビット 8、パリティなし、ストップ ビット 1、フロー制御なしに設定して、コンソールに接続します。

コンソール ケーブルの詳細については、ASA のハードウェア ガイドを参照してください。

ステップ 2 **Enter** キーを押して、次のプロンプトが表示されることを確認します。

```
ciscoasa>
```

このプロンプトは、ユーザ EXEC モードで作業していることを示します。ユーザ EXEC モードでは、基本コマンドのみを使用できます。

ステップ 3 特権 EXEC モードにアクセスします。

enable

パスワードを入力するように求められます。デフォルトではパスワードは空白に設定されているため、**Enter** キーを押して先に進みます。イネーブルパスワードを変更するには、[ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定 \(571 ページ\)](#) を参照してください。

例：

```
ciscoasa> enable
Password:
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 4 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

Firepower 9300 シャーシ上の ASA コンソールへのアクセス

初期設定の場合、Firepower 9300 シャーシ スーパーバイザに（コンソールポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドラインインターフェイスにアクセスし、ASA セキュリティ モジュールに接続します。

手順

- ステップ 1** Firepower 9300 シャーシ スーパーバイザ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module slot console

初めてモジュールにアクセスするときは、FXOS モジュールの CLI にアクセスします。その後 ASA アプリケーションに接続する必要があります。

connect asa

例：

```
Firepower# connect module 1 console
Firepower-module1> connect asa
```

asa>

- ステップ 2** 最高の特権レベルである特権 EXEC モードにアクセスします。

enable

パスワードを入力するように求められます。デフォルトではパスワードは空白に設定されているため、**Enter** キーを押して先に進みます。イネーブルパスワードを変更するには、[ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定（571 ページ）](#)を参照してください。

例：

```
asa> enable
Password:
asa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーションモードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

- ステップ 3** グローバル コンフィギュレーション モードを開始します。

configure terminal

例：

```
asa# configure terminal
asa(config)#
```

グローバル コンフィギュレーション モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 4 **Ctrl-a, d** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

トラブルシューティングのために FXOS モジュールの CLI を使用する場合があります。

ステップ 5 FXOS CLI のスーパーバイザ レベルに戻ります。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

```
telnet>quit
```

ASA サービス モジュール コンソールへのアクセス

初期設定の場合、スイッチに（コンソールポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイス（CLI）にアクセスし、ASASM に接続します。ASASM には工場出荷時のデフォルトコンフィギュレーションが含まれていないため、ASDM を使用してアクセスする前に CLI で設定を行う必要があります。ここでは、ASASM CLI にアクセスする方法について説明します。

接続方法について

スイッチ CLI から ASASM に接続するには、次の 2 つの方法が使用できます。

- 仮想コンソール接続： **service-module session** コマンドを使用して、ASASM への仮想コンソール接続を作成します。仮想コンソール接続には、実際のコンソール接続のすべての利点と制限があります。

利点を次に示します。

- 接続はリロード中も持続し、タイムアウトしません。
- ASASM リロード中も接続を維持でき、スタートアップメッセージを閲覧できます。
- ASASM がイメージをロードできない場合、ROMMON にアクセスできます。
- 初期パスワードの設定は必要ではありません。

制限を次に示します。

- 接続が低速です（9600 ボー）。

- 一度にアクティブにできるコンソール接続は 1 つだけです。
- このコマンドは、**Ctrl+Shift+6, x** がターミナル サーバ プロンプトに戻るためのエスケープシーケンスであるターミナルサーバとともに使用することはできません。**Ctrl+Shift+6, x** は、ASASM コンソールをエスケープして、スイッチプロンプトに戻るためのシーケンスでもあります。したがって、この状況で ASASM を終了しようとする、代わりにターミナルサーバプロンプトに戻ります。スイッチにターミナルサーバを再接続した場合、ASASM コンソールセッションがアクティブのままです。スイッチプロンプトを終了することはできません。コンソールをスイッチプロンプトに戻すには、直接シリアル接続を使用する必要があります。この場合、Cisco IOS でターミナルサーバまたはスイッチエスケープ文字を変更するか、または **Telnet session** コマンドを使用します。



(注) コンソール接続の永続性のため、ASASM を正しくログアウトしないと、意図よりも長く接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。

- Telnet 接続 : **session** コマンドを使用して、ASASM への Telnet 接続を作成します。



(注) 新しい ASASM に対してはこの方式を使用して接続できません。この方式では、ASASM 上での Telnet ログインパスワードの設定が必要です (デフォルトのパスワードはありません)。**passwd** コマンドを使用してパスワードを設定した後に、この方式を使用できます。

利点を次に示します。

- ASASM への複数のセッションを同時に使用できます。
- Telnet セッションは、高速接続です。

制限を次に示します。

- Telnet セッションは、ASASM リロード時に終了し、タイムアウトします。
- ASASM が完全にロードするまで ASASM にはアクセスできません。したがって、ROMMON にアクセスできません。
- 最初に Telnet ログインパスワードを設定する必要があります。デフォルトのパスワードはありません。

ASA サービス モジュールへのログイン

初期設定の場合、スイッチに（スイッチのコンソール ポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドラインインターフェイスにアクセスし、ASASM に接続します。

システムがすでにマルチコンテキストモードで動作している場合は、スイッチ環境から ASASM にアクセスするとシステムの実行スペースに入ります。

その後は、Telnet または SSH を使用してリモート アクセスを ASASM に直接設定できます。

手順

ステップ 1 スイッチから、次のいずれかを実行します。

- 最初のアクセスで使用可能：スイッチ CLI からこのコマンドを入力し、ASASM にコンソール アクセスします。

service-module session [switch {1 | 2}] slot number

例：

```
Router# service-module session slot 3
ciscoasa>
```

VSS 内のスイッチの場合、**switch** 引数を入力します。

モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。

ユーザ EXEC モードにアクセスします。

- ログインパスワードの設定後に使用可能：スイッチ CLI からこのコマンドを入力し、バックプレーンを介して ASASM に Telnet 接続します。

session [switch {1 || 2}] slot number processor 1

ログインパスワードの入力が求められます。

```
ciscoasa passwd:
```

例：

```
Router# session slot 3 processor 1
ciscoasa passwd: cisco
ciscoasa>
```

VSS 内のスイッチの場合、**switch** 引数を入力します。

session slot processor 0 コマンドは、他のサービス モジュールではサポートされていますが、ASASM ではサポートされていません。ASASM にはプロセッサ 0 がありません。

モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。

ASADM へのログインパスワードを入力します。 **passwd** コマンドを使用してパスワードを設定します。デフォルトのパスワードはありません。

ユーザ EXEC モードにアクセスします。

ステップ 2 最高の特権レベルである特権 EXEC モードにアクセスします。

enable

パスワードを入力するように求められます。デフォルトではパスワードは空白に設定されているため、**Enter** キーを押して先に進みます。イネーブルパスワードを変更するには、[ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定 \(571 ページ\)](#) を参照してください。

例：

```
ciscoasa> enable
Password:
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

グローバル コンフィギュレーション モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

関連トピック

[管理アクセスのガイドライン](#)

[ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定 \(571 ページ\)](#)

コンソール セッションのログアウト

ASASM からログアウトしない場合、コンソール接続は維持され、タイムアウトはありません。ASASM コンソールセッションを終了してスイッチの CLI にアクセスするには、次の手順を実行します。

意図せずに開いたままになっている可能性のある、別のユーザのアクティブな接続を終了するには、[アクティブなコンソール接続の終了 \(34 ページ\)](#) を参照してください。

手順

スイッチ CLI に戻るには、次を入力します。

Ctrl+Shift+6, x

スイッチ プロンプトに戻ります。

```
asasm# [Ctrl-Shift-6, x]
Router#
```

(注) 米国および英国キーボードの Shift+6 はキャレット記号 (^) を出力します。別のキーボードを使用しており、単独の文字としてキャレット記号 (^) を出力できない場合、一時的または永続的に、エスケープ文字を別の文字に変更できます。 **terminal escape-character *ascii_number*** コマンド (このセッションで変更する)、または **default escape-character *ascii_number*** コマンド (永続的に変更する) を使用します。たとえば、現在のセッションのシーケンスを **Ctrl-w, x** に変更するには、**terminal escape-character 23** を入力します。

アクティブなコンソール接続の終了

コンソール接続の永続性のために、ASASM を正しくログアウトしないと、意図したよりも長い時間にわたって接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。

手順

ステップ 1 スイッチ CLI から、**show users** コマンドを使用して、接続されたユーザを表示します。コンソールユーザは「con」と呼ばれます。ホストアドレスは、127.0.0.slot0 と表示されます (slot はモジュールのスロット番号です)。

show users

たとえば、次のコマンド出力は、スロット 2 にあるモジュールのライン 0 のユーザ「con」を示しています。

```
Router# show users
Line      User      Host(s)              Idle      Location
* 0       con 0     127.0.0.20          00:00:02
```

ステップ 2 コンソール接続のあるラインをクリアするには、次のコマンドを入力します。

clear line number

次に例を示します。

```
Router# clear line 0
```

Telnet セッションのログアウト

Telnet セッションを終了してスイッチ CLI にアクセスするには、次の手順を実行します。

手順

スイッチ CLI に戻るには、ASASM 特権モードまたはユーザ EXEC モードから **exit** を入力します。コンフィギュレーションモードに入っている場合は、Telnet セッションが終了するまで繰り返し **exit** を入力します。

スイッチ プロンプトに戻ります。

```
asasm# exit  
Router#
```

(注) 代わりに、エスケープシーケンス Ctrl+Shift+6, x を使用して、Telnet セッションをエスケープすることができます。このエスケープシーケンスを使用すると、スイッチ プロンプトで Enter キーを押すことで、Telnet セッションを再開できます。スイッチ から Telnet セッションを切断するには、スイッチ CLI で **disconnect** を入力します。セッションを切断しない場合、ASASM 設定に従って最終的にタイムアウトします。

ソフトウェア モジュール コンソールへのアクセス

ASA 5506-X に ASA FirePOWER などのソフトウェア モジュールをインストールしている場合、モジュール コンソールへのセッションを実行できます。



(注) **session** コマンドを使用して ASA バックプレーンを介してハードウェア モジュール CLI にアクセスすることはできません。

手順

ASA CLI から、モジュールへのセッションを実行します。

```
session {sfr | cxsc | ips} console
```

例 :

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

ASA 5506W-X ワイヤレス アクセス ポイント コンソールへのアクセス

ワイヤレス アクセス ポイント コンソールにアクセスするには、次の手順を実行します。

手順

ステップ 1 ASA CLI から、アクセス ポイントへのセッションを実行します。

session wlan console

例 :

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is 'CTRL-^X'

ap>
```

ステップ 2 アクセス ポイント CLI については、『[Cisco IOS Configuration Guide for Autonomous Aironet Access Points](#)』 [英語] を参照してください。

ASDM アクセスの設定

ここでは、デフォルト コンフィギュレーションで ASDM にアクセスする方法、およびデフォルト設定がない場合にアクセスを設定する方法について説明します。

ASDM アクセス（アプライアンス、ASA v）に対する工場出荷時のデフォルト コンフィギュレーションの使用

工場出荷時のデフォルト コンフィギュレーションでは、ASDM 接続はデフォルトのネットワーク設定で事前設定されています。

手順

次のインターフェイスおよびネットワーク設定を使用して ASDM に接続します。

- 管理インターフェイスは、ご使用のモデルによって異なります。
 - Firepower 9300 : 展開時に定義された管理タイプインターフェイスと IP アドレス。管理ホストは任意のネットワークからアクセスできます。
 - ASA 5506-X、ASA 5508-X および ASA 5516-X : 内部 GigabitEthernet 1/2 (192.168.1.1) および ASA 5506W-X、Wi-Fi GigabitEthernet 1/9 (192.168.10.1) 用。内部ホストは 192.168.1.0/24 ネットワークに限定され、Wi-Fi ホストは 192.168.10.0/24 に限定されません。
 - ASA 5512-X 以降 : 管理 0/0 (192.168.1.1) 。管理ホストは 192.168.1.0/24 ネットワークに限定されます。
 - ASA : 管理 0/0 (導入時に設定) 。管理ホストは管理ネットワークに限定されます。
 - ISA 3000 : 管理 1/1 (192.168.1.1) 。管理ホストは 192.168.1.0/24 ネットワークに限定されます。

(注) マルチ コンテキスト モードに変更すると、上記のネットワーク設定を使用して管理コンテキストから ASDM にアクセスできるようになります。

関連トピック

[工場出荷時のデフォルト設定](#) (46 ページ)

[マルチ コンテキスト モードの有効化またはディセーブル化](#) (253 ページ)

[ASDM の起動](#) (42 ページ)

ASDM アクセスのカスタマイズ

この手順は、ASA サービス モジュールを除くすべてのモデルに適用されます。

次の条件に 1 つ以上当てはまる場合は、この手順を使用します。

- 工場出荷時のデフォルト コンフィギュレーションがない。
- トランスペアレント ファイアウォール モードに変更したい。
- マルチ コンテキスト モードに変更したい。

シングルルーテッドモードの場合、ASDM に迅速かつ容易にアクセスするために、独自の管理 IP アドレスを設定できるオプションを備えた工場出荷時のデフォルト コンフィギュレーションを適用することを推奨します。この項に記載されている手順は、特別なニーズ (トランスペアレントモードやマルチ コンテキスト モードの設定など) がある場合や、他の設定を維持する必要がある場合にのみ使用してください。



- (注) ASA の場合、導入時にトランスペアレントモードを設定できるため、この手順は、設定をクリアする必要がある場合など、導入後に特に役立ちます。

手順

ステップ 1 コンソールポートで CLI にアクセスします。

ステップ 2 (オプション) トランスペアレントファイアウォールモードをイネーブルにします。

このコマンドは、設定をクリアします。

firewall transparent

ステップ 3 管理インターフェイスを設定します。

```
interface interface_id
  nameif name
  security-level level
  no shutdown
  ip address ip_address mask
```

例 :

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level は、1 ~ 100 の数字です。100 が最も安全です。

ステップ 4 (直接接続された管理ホスト用) 管理ネットワークの DHCP プールを設定します。

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

例 :

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

その範囲にインターフェイスアドレスが含まれていないことを確認します。

ステップ 5 (リモート管理ホスト用) 管理ホストへのルートを設定します。

```
route management_ifc management_host_ip mask gateway_ip 1
```

例 :

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

ステップ 6 ASDM の HTTP サーバをイネーブルにします。

http server enable

ステップ 7 管理ホストの ASDM へのアクセスを許可します。

http ip_address mask interface_name

例 :

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

ステップ 8 設定を保存します。

write memory

ステップ 9 (オプション) モードをマルチ モードに設定します。

mode multiple

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASA をリロードするよう求められます。

例

次の設定では、ファイアウォール モードがトランスペアレント モードに変換され、Management 0/0 インターフェイスが設定され、管理ホストに対して ASDM がイネーブルにされます。

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

関連トピック

[工場出荷時のデフォルト設定の復元 \(47 ページ\)](#)

[ファイアウォール モード \(シングル モード\) の設定 \(216 ページ\)](#)

[アプライアンス コンソールへのアクセス \(27 ページ\)](#)

[ASDM の起動 \(42 ページ\)](#)

ASA サービス モジュールの ASDM アクセスの設定

ASASMには物理インターフェイスがないため、ASDMアクセスが事前設定されていません。ASASMのCLIを使用してASDMアクセスを設定する必要があります。ASDMアクセス用にASASMを設定するには、次の手順を実行します。

始める前に

ASASMのクイックスタートガイドに従って、ASASMにVLANインターフェイスを割り当てます。

手順

ステップ1 ASASMに接続し、グローバルコンフィギュレーションモードにアクセスします。

ステップ2 (オプション) トランスペアレントファイアウォールモードをイネーブルにします。

firewall transparent

このコマンドは、設定をクリアします。

ステップ3 ご使用のモードに応じて、次のいずれかの操作を行って管理インターフェイスを設定します。

- ルーテッドモード：インターフェイスをルーテッドモードで設定します。

```
interface vlan number
  ip address ip_address [mask]
  nameif name
  security-level level
```

例：

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level は、1～100の数字です。100が最も安全です。

- トランスペアレントモード：ブリッジ仮想インターフェイスを設定し、ブリッジグループに管理VLANを割り当てます。

```
interface bvi number
  ip address ip_address [mask]

interface vlan number
  bridge-group bvi_number
  nameif name
  security-level level
```

例：

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level は、1 ~ 100 の数字です。100 が最も安全です。

ステップ 4 (直接接続された管理ホスト用) 管理インターフェイス ネットワーク上の管理ホストの DHCP をイネーブルにします。

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

例 :

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside
```

この範囲内には管理アドレスを含めないでください。

ステップ 5 (リモート管理ホスト用) 管理ホストへのルートを設定します。

```
route management_ifc management_host_ip mask gateway_ip 1
```

例 :

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50
```

ステップ 6 ASDM の HTTP サーバをイネーブルにします。

```
http server enable
```

ステップ 7 管理ホストの ASDM へのアクセスを許可します。

```
http ip_address mask interface_name
```

例 :

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

ステップ 8 設定を保存します。

```
write memory
```

ステップ 9 (オプション) モードをマルチ モードに設定します。

```
mode multiple
```

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASASM をリロードするよう求められます。

例

次のルーテッドモードの設定では、VLAN 1 のインターフェイスを設定し、管理ホストの ASDM のイネーブルにします。

```
interface vlan 1
nameif inside
ip address 192.168.1.1 255.255.255.0
security-level 100

dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

次の設定では、ファイアウォールモードをトランスペアレントモードに変換し、VLAN 1 インターフェイスを設定して BVI 1 に割り当てた後、管理ホストの ASDM をイネーブルにします。

```
firewall transparent
interface bvi 1

ip address 192.168.1.1 255.255.255.0
interface vlan 1
bridge-group 1
nameif inside
security-level 100

dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

関連トピック

[ASA サービス モジュール コンソールへのアクセス \(30 ページ\)](#)

[接続方法について \(30 ページ\)](#)

[コンソールセッションのログアウト \(33 ページ\)](#)

[アクティブなコンソール接続の終了 \(34 ページ\)](#)

[Telnet セッションのログアウト \(35 ページ\)](#)

[ファイアウォールモード \(シングルモード\) の設定 \(216 ページ\)](#)

ASDM の起動

ASDM は、次の 2 つの方法で起動できます。

- **ASDM-IDM ランチャ**：ランチャは、ASA から Web ブラウザを使用してダウンロードされるアプリケーションです。これを使用すると、任意の ASA IP アドレスに接続できます。他の ASA に接続する場合、ランチャを再度ダウンロードする必要はありません。
- **Java Web Start**：管理する ASA ごとに Web ブラウザで接続して、Java Web Start アプリケーションを保存または起動する必要があります。任意でコンピュータにショートカットを保存できます。ただし、ASA IP アドレスごとにショートカットを分ける必要があります。



(注) Web Start を使用する場合は、Java キャッシュをクリアしてください。クリアしない場合、Hostscan などのログイン前ポリシーに対する変更が失われる可能性があります。この問題は、ランチャを使用している場合には発生しません。

ASDM では、管理のために別の ASA IP アドレスを選択できます。ランチャと Java Web Start の機能の違いは、主に、ユーザが最初にどのように ASA に接続し、ASDM を起動するかにあります。

ここでは、まず ASDM に接続する方法について説明します。次にランチャまたは Java Web Start を使用して ASDM を起動する方法について説明します。

ASDM はローカルの \Users\\.asdm ディレクトリ内にキャッシュ、ログ、および設定などのファイルを保存し、Temp ディレクトリ内にも AnyConnect プロファイルなどのファイルを保存します。

手順

ステップ 1 ASDM クライアントとして指定したコンピュータで次の URL を入力します。

`https://asa_ip_address/admin`

次のボタンを持つ ASDM 起動ページが表示されます。

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

ステップ 2 ランチャをダウンロードするには、次の手順を実行します。

- a) [Install ASDM Launcher and Run ASDM] をクリックします。
- b) ユーザ名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザ名およびイネーブルパスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。**注**：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力すると、ASDM によってローカルデータベースで一致がチェックされます。

- c) インストーラをコンピュータに保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。
- d) 管理IPアドレス、および同じユーザ名とパスワード（新規インストールの場合は空白）を入力し、[OK] をクリックします。

ステップ 3 Java Web Start を使用するには：

- a) [Run ASDM] または [Run Startup Wizard] をクリックします。
- b) プロンプトが表示されたら、ショートカットをコンピュータに保存します。オプションで、アプリケーションを保存せずに開くこともできます。
- c) ショートカットから Java Web Start を起動します。
- d) 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。
- e) ユーザ名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザ名およびイネーブルパスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。**注：**HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力すると、ASDMによってローカルデータベースで一致がチェックされます。

ASDM 動作のカスタマイズ

アイデンティティ証明書をインストールして ASDM を正常に起動するだけでなく、ASDM ヒープメモリを増大することもできるため、より大きいサイズのコンフィギュレーションを処理できます。

ASDM のアイデンティティ証明書のインストール

Java 7 Update 51 以降を使用する場合、ASDM ランチャには信頼できる証明書が必要です。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。証明書をインストールするまで、Java Web Start を使用して ASDM を起動することができます。

ASDM で使用するために ASA に自己署名された ID 証明書をインストールし、Java を使用して証明書を登録するには、次のマニュアルを参照してください。

<http://www.cisco.com/go/asdm-certificate>

ASDM コンフィギュレーションメモリの増大

ASDM でサポートされる最大設定サイズは 512 KB です。このサイズを超えると、パフォーマンスの問題が生じることがあります。たとえば、コンフィギュレーションのロード時には、完了したコンフィギュレーションの割合がステータスダイアログボックスに表示されます。この

とき、サイズの大きいコンフィギュレーションでは、ASDM によってまだコンフィギュレーションの処理が行われていても、完了した割合の増分が停止し、操作が中断されているように見えます。このような状況が発生した場合は、ASDM システム ヒープメモリの増大を検討することを推奨します。

Windows での ASDM コンフィギュレーションメモリの増大

ASDM ヒープメモリ サイズを増大するには、次の手順を実行して **run.bat** ファイルを編集します。

手順

-
- ステップ 1** ASDM インストールディレクトリ（たとえば、C:\Program Files (x86)\Cisco Systems\ASDM）に移動します。
 - ステップ 2** 任意のテキストエディタを使用して **run.bat** ファイルを編集します。
 - ステップ 3** 「start javaw.exe」で始まる行で、「-Xmx」のプレフィックスが付いた引数を変更し、目的のヒープサイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。
 - ステップ 4** **run.bat** ファイルを保存します。
-

Mac OS での ASDM コンフィギュレーションメモリの増大

ASDM ヒープメモリ サイズを増大するには、次の手順を実行して **Info.plist** ファイルを編集します。

手順

-
- ステップ 1** [Cisco ASDM-IDM] アイコンを右クリックし、[Show Package Contents] を選択します。
 - ステップ 2** [Contents] フォルダで、Info.plist ファイルをダブルクリックします。開発者ツールをインストールしている場合は、プロパティリストエディタで開きます。そうでない場合は、TextEdit で開きます。
 - ステップ 3** [Java] > [VMOptions] で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープサイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```

<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

<key>VMOptions</key>
<string>-Xms64m -Xmx512m</string>

<key>CFBundleDocumentTypes</key>
<array>

```

ステップ 4 このファイルがロックされると、次のようなエラーが表示されます。



ステップ 5 [Unlock] をクリックし、ファイルを保存します。

[Unlock] ダイアログボックスが表示されない場合は、エディタを終了します。[Cisco ASDM-IDM] アイコンを右クリックし、[Copy Cisco ASDM-IDM] を選択して、書き込み権限がある場所（デスクトップなど）に貼り付けます。その後、このコピーからヒープサイズを変更します。

工場出荷時のデフォルト設定

工場出荷時のデフォルト設定とは、シスコが新しい ASA に適用したコンフィギュレーションです。

- ASA 5506-X、5508-X および 5516-X：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、内部インターフェイスから ASDM を使用して管理できます。
- ASA 5512-X ～ ASA 5585-X：管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。
- Firepower 9300 シャーシ：ASA のスタンドアロンまたはクラスタを展開する場合、管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。
- ASA v：ハイパーバイザによっては、導入の一環として、管理用のインターフェイス導入設定（初期の仮想導入設定）によって設定されるため、ASDM を使用してこのインター

フェイスに接続して設定を完了できます。フェールオーバー IP アドレスも設定できます。また、必要に応じて、「工場出荷時のデフォルト」コンフィギュレーションを適用することもできます。

- **ASASM** : デフォルト設定はありません。コンフィギュレーションを開始するには、[ASA サービス モジュール コンソールへのアクセス \(30 ページ\)](#) を参照してください。
- **ISA 3000** : 工場出荷時のデフォルト設定は、同じネットワーク上のすべての内部および外部インターフェイスを使用した、ほぼ完全なトランスペアレントファイアウォールモード設定です。ASDM を使用して管理インターフェイスに接続し、ネットワークの IP アドレスを設定できます。ハードウェアバイパスは2つのインターフェイスペアに対して有効になっており、すべてのトラフィックはインラインタップモニタ専用モードで ASA FirePOWER モジュールに送信されます。このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。

アプライアンス および Firepower 9300 シャーシの場合、工場出荷時のデフォルト設定は、ルーテッドファイアウォールモードとシングルコンテキストモードのみで使用できます。ASA の場合、導入時にトランスペアレントモードまたはルーテッドモードを選択できます。



- (注) イメージファイルと (隠された) デフォルト コンフィギュレーションに加え、`log/`、`crypto_archive/`、および `coredumpinfo/coredump.cfg` がフラッシュ メモリ内の標準のフォルダとファイルです。フラッシュ メモリ内で、これらのファイルの日付は、イメージファイルの日付と一致しない場合があります。これらのファイルは、トラブルシューティングに役立ちますが、障害が発生したことを示すわけではありません。

工場出荷時のデフォルト設定の復元

この項では、工場出荷時のデフォルトコンフィギュレーションを復元する方法について説明します。CLI および ASDM の両方の手順が提供されています。ASA では、この手順を実行することで導入設定が消去され、ASA 5525-X の場合と同じ工場出荷時のデフォルト設定が適用されます。



- (注) ASASM で出荷時のデフォルトコンフィギュレーションを復元すると、設定は消去されます。工場出荷時のデフォルトコンフィギュレーションはありません。

Firepower 9300 では、工場出荷時のデフォルト設定を復元すると単に設定が消去されるだけです。デフォルト設定を復元するには、スーパーバイザから ASA をもう一度展開する必要があります。

始める前に

この機能は、ルーテッドファイアウォールモードでのみ使用できます。トランスペアレントモードの場合、インターフェイスの IP アドレスがサポートされません。さらに、この機能は

シングル コンテキスト モードでのみ使用できます。コンフィギュレーションがクリアされた ASA には、この機能を使用して自動的に設定する定義済みコンテキストがありません。

手順

ステップ 1 工場出荷時のデフォルト コンフィギュレーションを復元します。

configure factory-default [*ip_address* [*mask*]]

例 :

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

ip_address を指定する場合は、デフォルトの IP アドレスを使用する代わりに、お使いのモデルに応じて、内部または管理インターフェイスの IP アドレスを設定します。*ip_address* オプションで設定されているインターフェイスについては、次のモデルのガイドラインを参照してください。

- Firepower 9300 : 効果はありません。
- ASA v : 管理インターフェイスの IP アドレスを設定します。
- ASA 5506-X : 内部インターフェイスの IP アドレスを設定します。
- ASA 5508-X および 5516-X : 内部インターフェイスの IP アドレスを設定します。
- ASA 5512-X、5515-X、5525-X、5545-X、5555-X : 管理インターフェイスの IP アドレスを設定します。
- ASA 5585-X : 管理インターフェイスの IP アドレスを設定します。
- ISA 3000 : 管理インターフェイスの IP アドレスを設定します。
- ASASM : 効果はありません。

http コマンドでは、ユーザが指定するサブネットが使用されます。同様に、**dhcpd address** コマンドの範囲は、指定したサブネット内のアドレスで構成されます。

Firepower 2100 の場合 : このモデルでは、**boot system** コマンドは使用されません。パッケージは FXOS によって管理されます。

その他すべてのモデルの場合 : このコマンドは、残りの設定とともに **boot system** コマンドをクリアします (存在する場合)。**boot system** コマンドを使用すると、特定のイメージから起動できます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合、ASA はブートしません。

ステップ 2 デフォルト コンフィギュレーションをフラッシュ メモリに保存します。

write memory

このコマンドでは、事前に **boot config** コマンドを設定して、別の場所を設定していた場合でも、実行コンフィギュレーションはスタートアップコンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションがクリアされると、このパスもクリアされます。

ステップ 3 (ASDM での手順。) メイン ASDM アプリケーション ウィンドウで、次を実行します。

a) **[File] > [Reset Device to the Factory Default Configuration]** の順に選択します。

[Reset Device to the Default Configuration] ダイアログボックスが表示されます。

b) (オプション) デフォルトアドレスを使用する代わりに、管理または内部インターフェイスの**管理 IP アドレス**を入力します。

モデルごとに設定されているインターフェイス IP の詳細については、前述の CLI 手順を参照してください。

c) (オプション) ドロップダウン リストから **[Management Subnet Mask]** を選択します。

d) **[OK]** をクリックします。

確認用のダイアログボックスが表示されます。

(注) Firepower 2100 の場合：このモデルでは、ブートイメージの場所は使用されません。パッケージは FXOS によって管理されます。

その他すべてのモデルの場合：この操作により、残りの設定とともにブートイメージの場所もクリアされます (存在する場合)。**[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration]** ペインでは、外部メモリ上のイメージを含む、特定のイメージからブートできます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュメモリの最初のイメージからブートします。内部フラッシュメモリにイメージがない場合、ASA はブートしません。

e) **[Yes]** をクリックします。

f) デフォルト設定を復元したら、この設定を内部フラッシュメモリに保存します。**[File] > [Save Running Configuration to Flash]** を選択します。

このオプションを選択すると、以前に別の場所を設定している場合でも、実行コンフィギュレーションがスタートアップコンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションをクリアした場合は、このパスもクリアされています。

ASAv 導入設定の復元

この項では、ASAv の導入 (第 0 日) 設定を復元する方法について説明します。

手順

ステップ 1 フェールオーバーを行うために、スタンバイ装置の電源を切ります。

スタンバイ ユニットがアクティブになることを防ぐために、電源をオフにする必要があります。電源を入れたままにした場合、アクティブ装置の設定を消去すると、スタンバイ装置がアクティブになります。以前のアクティブ ユニットのデータをリロードし、フェールオーバー リンクを介して再接続すると、古い設定は新しいアクティブユニットから同期し、必要な導入コンフィギュレーションが消去されます。

ステップ 2 リロード後に導入設定を復元します。フェールオーバーを行うために、アクティブ装置で次のコマンドを入力します。

write erase

(注) ASA が現在の実行イメージをブートするため、元のブート イメージには戻りません。元のブート イメージを使用するには、**boot image** コマンドを参照してください。コンフィギュレーションは保存しないでください。

ステップ 3 ASA をリロードし、導入設定をロードします。

reload

ステップ 4 フェールオーバーを行うために、スタンバイ装置の電源を投入します。

アクティブ装置のリロード後、スタンバイ装置の電源を投入します。導入設定がスタンバイ装置と同期されます。

ASA 5506-X、5508-X、および 5516-X のデフォルト設定

ASA 5506-X シリーズ、5508-X、および 5516-X の工場出荷時のデフォルト設定は、次のとおりです。

- 内部 --> 外部へのトラフィック フロー：GigabitEthernet 1/1（外部）、GigabitEthernet 1/2（内部）
- DHCP の外部 IP アドレス、内部 IP アドレス：192.168.1.1
- (ASA 5506W-X) WiFi<--> 内部のトラフィック フロー、WiFi --> 外部へのトラフィック フロー：GigabitEthernet 1/9 (WiFi)
- (ASA 5506W-X) WiFi の IP アドレス：192.168.10.1
- 内部および WiFi 上のクライアントに対する DHCP。アクセス ポイント自体とそのすべてのクライアントが ASA を DHCP サーバとして使用します。
- 管理 1/1 インターフェイスが稼働しているが、そうでない場合は未設定。ASA FirePOWER モジュールは、このインターフェイスを使用して ASA 内部ネットワークに接続し、内部インターフェイスをインターネットへのゲートウェイとして使用できます。
- ASDM アクセス：内部ホストおよび WiFi ホストに許可されます。

- NAT : 内部、WiFi、および管理から外部へのすべてのトラフィックのインターフェイス PAT。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
interface GigabitEthernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

ASA 5506W-X の場合は、次のコマンドも含まれます。

```
same-security-traffic permit inter-interface
!
interface GigabitEthernet 1/9
  security-level 100
  nameif wifi
  ip address 192.168.10.1 255.255.255.0
  no shutdown
!
http 192.168.10.0 255.255.255.0 wifi
!
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi
```

ASA 5512-X ~ ASA 5585-X デフォルト設定

ASA 5512-X ~ ASA 5585-X の工場出荷時のデフォルト設定は、次のとおりです。

- 管理インターフェイス : Management 0/0 (管理)。
- IP アドレス : 管理アドレスは 192.168.1.1/24 です。

- DHCP サーバ：管理ホストでは DHCP サーバがイネーブルにされているため、管理インターフェイスに接続するコンピュータには、192.168.1.2～192.168.1.254 の間のアドレスが割り当てられます。
- ASDM アクセス：管理ホストに許可されます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
 ip address 192.168.1.1 255.255.255.0
 nameif management
 security-level 100
 no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

Firepower 9300 シャーシ デフォルト設定

Firepower 9300 シャーシ上に ASA を展開した場合、ASDM を使用して管理インターフェイスへの接続が可能になる多くのパラメータを事前設定できます。一般的な構成には次の設定があります。

- 管理インターフェイス：
 - Firepower 9300 シャーシスーパーバイザ上で定義された任意の管理タイプインターフェイス
 - 名前は「management」
 - 任意の IP アドレス
 - セキュリティ レベル 0
 - 管理専用
- 管理インターフェイス内のデフォルト ルート
- ASDM アクセス：すべてのホストが許可されます。

スタンドアロンユニットの設定は、次のコマンドで構成されます。クラスタユニットの追加の設定については、[ASA クラスタの作成 \(434 ページ\)](#) を参照してください。

```
interface <management_ifc>
 management-only
 ip address <ip_address> <mask>
 ipv6 address <ipv6_address>
```



```
ipv6 enable
nameif management
security-level 0
no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

ISA 3000 のデフォルト設定

ISA 3000 の工場出荷時のデフォルト設定は、次のとおりです。

- トランスペアレントファイアウォールモード：トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。
- 1ブリッジ仮想インターフェイス：すべてのメンバーインターフェイスは同じネットワーク内に存在しています（IPアドレスは事前設定されていません。ネットワークと一致するように設定する必要があります）：GigabitEthernet 1/1（outside1）、GigabitEthernet 1/2（inside1）、GigabitEthernet 1/3（outside2）、GigabitEthernet 1/4（inside2）
- すべての内部および外部インターフェイスは相互通信できます。
- 管理 1/1インターフェイス：ASDM アクセスの 192.168.1.1/24。
- 管理上のクライアントに対する DHCP。
- ASDM アクセス：管理ホストに許可されます。
- ハードウェア バイパスは、次のインターフェイス ペアで有効になっています。GigabitEthernet 1/1 および 1/2。GigabitEthernet 1/3 および 1/4



(注) ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのは上記のインターフェイス ペアのみになります。inside1 と inside2 および outside1 と outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。電源が再投入されると、ASA がフローを引き継ぐため、接続が短時間中断されます。

- ASA Firepower モジュール：すべてのトラフィックが、Inline Tap Monitor-Only モードのモジュールに送信されます。このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。

このコンフィギュレーションは次のコマンドで構成されています。

```

firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management

access-list sfrAccessList extended permit ip any any
class-map sfrclass
  match access-list sfrAccessList
policy-map global_policy
  class sfrclass
    sfr fail-open monitor-only
service-policy global_policy global

```

ASAv 導入設定

ASAv 上に ASA を展開した場合、ASDM を使用して管理 0/0 インターフェイスへの接続が可能になる多くのパラメータを前もって設定できます。一般的な構成には次の設定があります。

- ルーテッドファイアウォールモードまたはトランスペアレントファイアウォールモード
- Management 0/0 インターフェイス :
 - 名前は「management」
 - IP アドレスまたは DHCP
 - セキュリティ レベル 0
 - 管理専用
- 管理ホスト IP アドレスのスタティック ルート (管理サブネット上にない場合)
- HTTP サーバの有効または無効
- 管理ホスト IP アドレス用の HTTP アクセス
- (オプション) GigabitEthernet 0/8 用のフェールオーバー リンク IP アドレス、Management 0/0 のスタンバイ IP アドレス
- DNS サーバ
- スマート ライセンス ID トークン
- スマート ライセンスのスループット レベルおよび標準機能ティア
- (オプション) Smart Call Home HTTP プロキシ URL およびポート
- (オプション) SSH 管理設定 :
 - クライアント IP アドレス
 - ローカル ユーザ名とパスワード
 - ローカル データベースを使用する SSH に必要な認証
- (オプション) REST API の有効または無効



(注) Cisco 認証局に正常に登録するには、ASAv をインターネットアクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、導入後に追加の設定が必要になることがあります。

スタンドアロンユニットについては、次の設定例を参照してください。

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address
  management-only
  no shutdown
  http server enable
  http management_host_IP mask management
```

```

route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent

```

フェールオーバー ペアのプライマリ ユニットについては、次の設定例を参照してください。

```

nameif management
  security-level 0
  ip address ip_address standby standby_ip
  management-only
  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http management_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip

```

設定の開始

ASA を設定してモニタするには、次の手順を実行します。



-
- (注) ASDM では、最大 512 KB の設定をサポートしています。このサイズを超えると、パフォーマンスの問題が生じることがあります。[ASDM コンフィギュレーションメモリの増大 \(44 ページ\)](#) を参照してください。
-

手順

- ステップ 1 Startup Wizard を使用して初期設定を行うには、[Wizards] > [Startup Wizard] を選択します。
- ステップ 2 IPsec VPN Wizard を使用して IPsec VPN 接続を設定するには、[Wizards] > [IPsecVPN Wizard] を選択して、表示される各画面で設定を行います。
- ステップ 3 SSL VPN Wizard を使用して SSL VPN 接続を設定するには、[Wizards] > [SSL VPN Wizard] を選択して、表示される各画面で設定を行います。
- ステップ 4 高可用性とスケーラビリティに関する設定値を設定するには、[Wizards] > [High Availability and Scalability Wizard] を選択します。
- ステップ 5 Packet Capture Wizard を使用してパケットキャプチャを設定するには、[Wizards] > [Packet Capture Wizard] を選択します。
- ステップ 6 ASDM GUI で使用できるさまざまな色とスタイルを表示するには、[View] > [Office Look and Feel] を選択します。
- ステップ 7 機能を設定するには、ツールバーの [Configuration] ボタンをクリックし、いずれかの機能ボタンをクリックして、関連する設定ペインを表示します。

(注) [Configuration] 画面が空白の場合は、ツールバーで [Refresh] をクリックして、画面のコンテンツを表示します。
- ステップ 8 ASA をモニタするには、ツールバーの [Monitoring] ボタンをクリックし、機能ボタンをクリックして、関連するモニタリング ペインを表示します。

ASDM でのコマンドラインインターフェイス ツールの使用

この項では、ASDM を使用してコマンドを入力する方法および CLI の使用方法について説明します。

コマンドライン インターフェイス ツールの使用

この機能には、コマンドを ASA に送信して結果を表示する、テキストベースのツールが用意されています。

CLI ツールによって入力可能なコマンドは、ユーザ権限によって異なります。メイン ASDM アプリケーションウィンドウの下部にあるステータスバーの権限レベルを見て、CLI 特権コマンドを実行するために必要な特権があるかどうかを確認してください。

始める前に

- ASDM の CLI ツールから入力するコマンドは、ASA の接続ターミナルから入力するコマンドと動作が異なる場合があります。

- コマンドエラー：誤った入力コマンドによってエラーが発生した場合、その誤ったコマンドはスキップされ、その他のコマンドは処理されます。[Response] 領域には、他の関連情報とともに、エラーが発生したかどうかについての情報を示すメッセージが表示されます。
- インタラクティブ コマンド：インタラクティブ コマンドは、CLI ツールではサポートされていません。これらのコマンドを ASDM で使用するには、次のコマンドに示すように、**noconfirm** キーワード（使用可能な場合）を使用します。

```
crypto key generate rsa modulus 1024 noconfirm
```

- 他の管理者との競合を回避：複数の管理ユーザが ASA の実行コンフィギュレーションをアップデートできます。ASDM の CLI ツールでコンフィギュレーションを変更する場合は、アクティブな管理セッションが他にないことを事前に確認してください。複数のユーザが同時に ASA を設定した場合、最新の変更が有効になります。

同じ ASA で現在アクティブな他の管理セッションを表示するには、[Monitoring]>[Properties]>[Device Access] の順に選択します。

手順

-
- ステップ 1** メイン ASDM アプリケーション ウィンドウで、[Tools] > [Command Line Interface] の順に選択します。
[Command Line Interface] ダイアログボックスが表示されます。
 - ステップ 2** 必要なコマンドのタイプ（1行または複数行）を選択し、ドロップダウンリストからコマンドを選択するか、または表示されたフィールドにコマンドを入力します。
 - ステップ 3** [Send] をクリックしてコマンドを実行します。
 - ステップ 4** 新しいコマンドを入力するには、[Clear Response] をクリックしてから、実行する別のコマンドを選択（または入力）します。
 - ステップ 5** この機能の状況依存ヘルプを表示するには、[Enable context-sensitive help (?)] チェックボックスをオンにします。文脈依存ヘルプをディセーブルにするには、このチェックボックスをオフにします。
 - ステップ 6** 設定を変更した場合は、[Command Line Interface] ダイアログボックスを閉じた後に、[Refresh] をクリックして ASDM での変更内容を表示します。
-

ASDM によって無視されるコマンドのデバイス上での表示

この機能により、ASDM がサポートしていないコマンドの一覧を表示できます。通常 ASDM は、これらのコマンドを無視します。ASDM は、実行コンフィギュレーションのこれらのコマンドを変更、削除することはありません。詳細については、「[サポートされていないコマンド \(100 ページ\)](#)」を参照してください。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、[Tools] > [Show Commands Ignored by ASDM on Device] の順に選択します。

ステップ 2 完了したら、[OK] をクリックします。

接続の設定変更の適用

コンフィギュレーションに対してセキュリティポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティポリシーが使用されます。既存の接続は、接続の確立時に設定されたポリシーを引き続き使用します。古い接続の **show** コマンド出力には古い設定が反映され、古い接続に関するデータを含まない場合があります。

たとえば、インターフェイスから **QoS service-policy** を削除し、修正バージョンを再度追加する場合、**show service-policy** コマンドには、新しいサービス ポリシーと一致する新規接続と関連付けられている **QoS** カウンタのみ表示されます。古いポリシーの既存の接続はコマンド出力には表示されません。

すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。

接続を解除するには、次のいずれかのコマンドを入力します。

- **clear local-host** [*ip_address*] [**all**]

このコマンドは、接続制限値や初期接続の制限など、クライアントごとのランタイム ステートを再初期化します。これにより、このコマンドは、これらの制限を使用しているすべての接続を削除します。ホストごとの現在のすべての接続を表示するには、**show local-host all** コマンドを参照してください。

引数を指定しないと、このコマンドは、影響を受けるすべての **through-the-box** 接続をクリアします。**to-the-box** 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。特定の IP アドレスへの、または特定の IP アドレスからの接続をクリアするには、*ip_address* 引数を使用します。

- **clear conn**[**all**] [**protocol** {**tcp** |**udp**}] [**address src_ip** [-*src_ip*] [**netmask mask**] [**port src_port** [-*src_port*] [**address dest_ip** [-*dest_ip*] [**netmask mask**] [**port dest_port** [-*dest_port*]

このコマンドは、すべての状態の接続を終了します。現在のすべての接続を表示するには、**show conn** コマンドを参照してください。

引数を指定しないと、このコマンドはすべての **through-the-box** 接続をクリアします。**to-the-box** 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。送信元 IP アドレス、宛先 IP アドレス、ポート、プロトコルに基づいて特定の接続をクリアするには、必要なオプションを指定できます。



第 3 章

ASDM グラフィカル ユーザ インターフェイス

この章では、ASDM ユーザ インターフェイスの使用方法について説明します。

- [ASDM ユーザ インターフェイスについて \(61 ページ\)](#)
- [ASDM ユーザ インターフェイスのナビゲーション \(64 ページ\)](#)
- [メニュー \(65 ページ\)](#)
- [ツールバー \(72 ページ\)](#)
- [ASDM Assistant \(73 ページ\)](#)
- [ステータス バー \(73 ページ\)](#)
- [Device List \(74 ページ\)](#)
- [共通ボタン \(75 ページ\)](#)
- [キーボードショートカット \(76 ページ\)](#)
- [ASDM ペインの検索機能 \(78 ページ\)](#)
- [ルール リストの検索機能 \(78 ページ\)](#)
- [拡張スクリーン リーダ サポートの有効化 \(79 ページ\)](#)
- [整理用フォルダー \(80 ページ\)](#)
- [\[Home\] ペイン \(シングル モードとコンテキスト\) \(80 ページ\)](#)
- [\[Home\] ペイン \(システム\) \(95 ページ\)](#)
- [ASDM 設定の定義 \(97 ページ\)](#)
- [ASDM Assistant での検索 \(99 ページ\)](#)
- [履歴メトリックの有効化 \(100 ページ\)](#)
- [サポートされていないコマンド \(100 ページ\)](#)

ASDM ユーザ インターフェイスについて

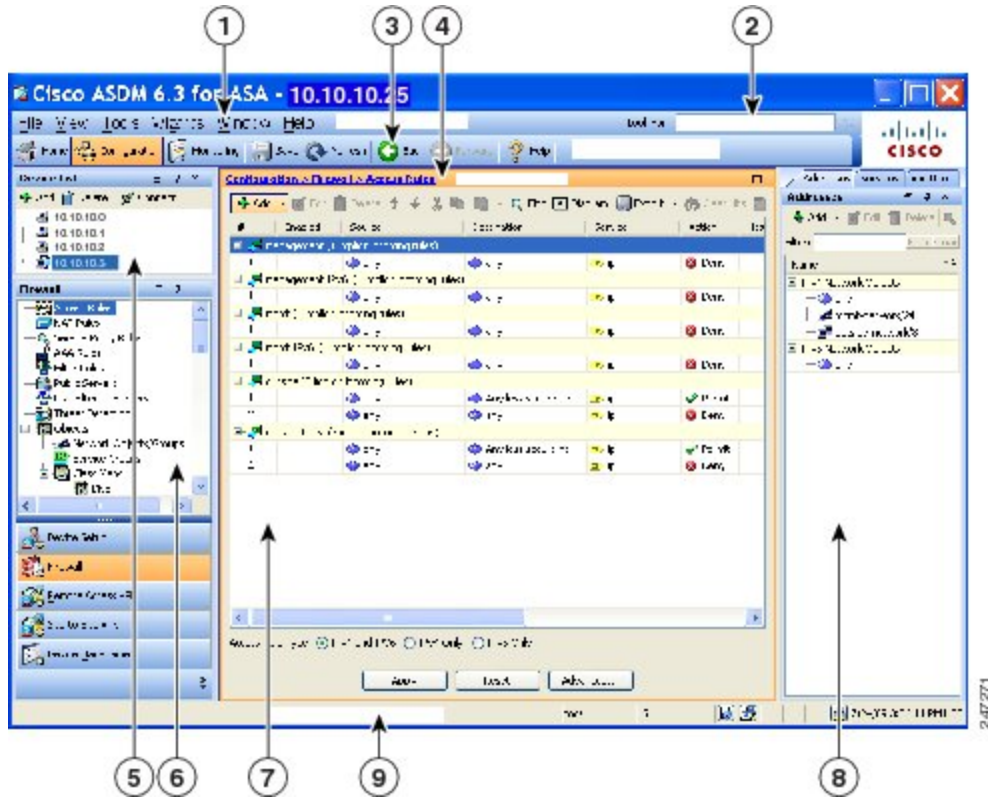
ASDM ユーザ インターフェイスは、ASA がサポートしているさまざまな機能に簡単にアクセスできるように設計されています。ASDM ユーザ インターフェイスには次の要素があります。

- ファイル、ツール、ウィザード、およびヘルプにすぐにアクセスできるメニューバー。メニュー項目の多くにはキーボードショートカットもあります。

- ASDM の操作のためのツールバー。ツールバーから [Home] ペイン、[Configuration] ペイン、および [Monitoring] ペインにアクセスできます。また、ヘルプの参照やペイン間のナビゲーションもできます。
- ドッキング可能な左側の [Navigation] ペイン。[Configuration] ペインや [Monitoring] ペイン内の移動に使用します。ヘッダーにある3つのボタンをそれぞれクリックすると、ペインの最大化または復元、移動可能なフローティングペインへの変更、ペインの非表示化、またはペインを閉じることができます。[Configuration] ペインおよび [Monitoring] ペインにアクセスするには、次のいずれかを実行します。
 - アプリケーション ウィンドウの左端にある左側の [Navigation] ペインのリンクをクリックします。選択した [Content] ペインのタイトルバーにパスが表示されます ([Configuration] > [Device Setup] > [Startup Wizard] など)。
 - 正確なパスがわかっている場合、左側の [Navigation] ペインでリンクをクリックしなくても、アプリケーション ウィンドウの右側にある [Content] ペインのタイトルバーに直接入力できます。
- 左側の [Navigation] ペインを非表示/表示できる [Content] ペインの右端にある [maximize and restore] ボタン。
- ドッキング可能な [Device List] ペイン。ASDM からアクセスできるデバイスのリストを表示します。ヘッダーにある3つのボタンをそれぞれクリックすると、ペインの最大化または復元、移動可能なフローティングペインへの変更、ペインの非表示化、またはペインを閉じることができます。
- 時間、接続ステータス、ユーザ、メモリステータス、実行コンフィギュレーションステータス、権限レベル、および SSL ステータスをアプリケーション ウィンドウの下部に表示するステータス バー。
- 左側の [Navigation] ペイン。アクセスルール、NAT ルール、AAA ルール、フィルタルール、およびサービスルールの作成時にルールテーブルで使用できるさまざまなオブジェクトを表示します。ペイン内のタブタイトルは、表示している機能に応じて変わります。また、このペインには **ASDM Assistant** が表示されます。

次の図に、ASDM ユーザ インターフェイスの要素を示します。

図 1: ASDM ユーザ インターフェイス



凡例

GUI 要素	説明
1	メニュー バー
2	検索フィールド
3	ツールバー
4	ナビゲーションパス
5	[Device List] ペイン
6	左側のナビゲーション ペイン
7	[Content] ペイン
8	右側のナビゲーション ペイン
9	ステータス バー



- (注) ツール ヒントが、[Wizards]、[Configuration] ペイン、[Monitoring] ペイン、ステータス バーを含む、GUI のさまざまな部分に追加されています。ツール ヒントを表示するには、マウスをステータスバーにあるアイコンなど、特定のユーザ インターフェイス要素の上に置きます。

ASDM ユーザ インターフェイスのナビゲーション

ASDM ユーザ インターフェイスを効率的に移動するために、前の項で説明したメニュー、ツールバー、ドッキング可能ペイン、および左側と右側の [Navigation] ペインを組み合わせることで使用できます。使用できる機能は、[Device List] ペインの下のボタン リストに表示されます。リスト例には、次の機能ボタンが入っている場合があります。

- **Device Setup**
- **Firewall**
- **Botnet Traffic Filter**
- **Remote Access VPN**
- **Site to Site VPN**
- **Device Management**

表示される機能ボタンのリストは、購入したライセンス機能に基づいて表示されます。コンフィギュレーション ビューまたはモニタリング ビューの選択した機能の最初のペインにアクセスするには、それぞれのボタンをクリックします。ホーム ビューでは、機能ボタンは使用できません。

機能ボタンの表示を変える場合は、次の手順を実行します。

手順

ステップ 1 最後の機能ボタンの下にあるドロップダウンリストボタンを選択して、コンテキストメニューを表示します。

ステップ 2 次のいずれかのオプションを選択します。

- 表示するボタンを増やすには、[Show More Buttons] をクリックします。
- 表示するボタンを減らすには、[Show Fewer Buttons] をクリックします。
- ボタンを追加または削除するには、[Add or Remove Buttons] をクリックし、表示されたリストから追加または削除するボタンをクリックします。
- [Option] を選択すると [Option] ダイアログボックスが表示され、ボタンのリストが現在の順序で表示されます。次のいずれかを選択します。
 - リスト内のボタンを上に移動するには、[Move Up] をクリックします。

- リスト内のボタンを下に移動するには、[Move Down] をクリックします。
- リスト内の項目の順序をデフォルト設定に戻すには、[Reset] をクリックします。

ステップ 3 [OK] をクリックして設定を保存し、ダイアログボックスを閉じます。

メニュー

ASDM の各メニューには、マウスまたはキーボードを使用してアクセスできます。

[File] メニュー

[File] メニューでは、ASA のコンフィギュレーションを管理できます。

[File] メニュー項目	説明
Refresh ASDM with the Running Configuration on the Device	実行コンフィギュレーションのコピーを ASDM にロードします。
Reset Device to the Factory Default Configuration	コンフィギュレーションを工場出荷時のデフォルトに復元します。
Show Running Configuration in New Window	現在の実行コンフィギュレーションを新しいウィンドウに表示します。
Save Running Configuration to Flash	実行コンフィギュレーションのコピーをフラッシュ メモリに書き込みます。
Save Running Configuration to TFTP Server	現在の実行コンフィギュレーションファイルのコピーを TFTP サーバに保存します。
Save Running Configuration to Standby Unit	プライマリ装置の実行コンフィギュレーション ファイルのコピーを、フェールオーバー スタンバイ装置の実行コンフィギュレーションに送信します。
Save Internal Log Buffer to Flash	内部ログ バッファをフラッシュ メモリに保存します。
Print	現在のページを印刷します。ルールを印刷する場合、ページを横方向にすることをお勧めします。Internet Explorer の場合は、署名付きアプレットを最初に承認した時点で印刷権限が与えられています。

[File] メニュー項目	説明
Clear ASDM Cache	ローカル ASDM イメージを削除します。ASDM に接続すると、ASDM によりイメージがローカルにダウンロードされません。
Clear ASDM Password Cache	新しいパスワードを定義した後に、それとは異なる既存のパスワードがまだ残っている場合は、パスワードキャッシュを削除します。
Clear Internal Log Buffer	syslog メッセージバッファを空にします。
Exit	ASDM を閉じます。

[View] メニュー

[View] メニューでは、ASDM ユーザ インターフェイスのさまざまな部分を表示できます。現在のビューに応じた特定の項目が表示されます。現在のビューに表示できない項目は選択できません。

[View] メニュー項目	説明
Home	ホーム ビューを表示します。
Configuration	コンフィギュレーションビューを表示します。
Monitoring	モニタリング ビューを表示します。
Device List	ドッキング可能なペインにデバイスのリストを表示します。
Navigation	コンフィギュレーション ビューおよびモニタリング ビューで [Navigation] ペインを表示または非表示にします。
ASDM Assistant	タスクに応じた ASDM の使用方法のヘルプを検索し、見つけます。
Latest ASDM Syslog Messages	ホーム ビューで [Latest ASDM Syslog Messages] ペインを表示または非表示にします。このペインは、ホーム ビューでのみ使用できます。最新のリリースにアップグレードするためのメモリが不足している場合は、syslog メッセージ %ASA-1-211004 が生成され、インストールされているメモリ、および必要なメモリが表示されます。このメッセージは、メモリがアップグレードされるまで、24 時間ごとに再表示されます。

[View] メニュー項目	説明
Addresses	[Addresses] ペインを表示または非表示にします。[Addresses] ペインは、コンフィギュレーションビューの [Access Rules]、[NAT Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでのみ使用できます。
Services	[Services] ペインを表示または非表示にします。[Services] ペインは、コンフィギュレーションビューの [Access Rules]、[NAT Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでのみ使用できます。
Time Ranges	[Time Ranges] ペインを表示または非表示にします。[Time Ranges] ペインは、コンフィギュレーションビューの [Access Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでのみ使用できます。
Select Next Pane	マルチペイン画面で次のペインを強調表示します。たとえば、[Service Policies Rules] ペインからその隣の [Address] ペインに移動します。
Select Previous Pane	マルチペイン画面で前のペインを強調表示します。
Back	前のペインに戻ります。
Forward	以前に表示した次のペインに移動します。
Find in ASDM	機能や ASDM Assistant などの項目を検索します。
Reset Layout	レイアウトをデフォルトのコンフィギュレーションに戻します。
Office Look and Feel	画面のフォントと色を Microsoft Office 設定に変更します。

[Tools] メニュー

[Tools] メニューは、ASDM で使用できる次の一連のツールを提供します。

[Tools] メニュー項目	説明
Command Line Interface	コマンドを ASA に送信して結果を表示します。
Show Commands Ignored by ASDM on Device	ASDM に無視されたサポート対象外のコマンドを表示します。
Packet Tracer	指定した送信元アドレスとインターフェイスから宛先まで、パケットをトレースします。プロトコルおよびポートをデータタイプに関わりなく指定でき、そこで実行された処理の詳細データを含むパケットの一部始終を表示できます。詳細については、ファイアウォールの設定ガイドを参照してください。
ping	ASA および関係する通信リンクのコンフィギュレーションや動作を検証し、他のネットワーク デバイスの基本的なテストを実行します。詳細については、ファイアウォールの設定ガイドを参照してください。
tracert	パケットが宛先に到着するまでのルートを判断します。詳細については、ファイアウォールの設定ガイドを参照してください。
File Management	フラッシュ メモリに保存されたファイルを表示、移動、コピー、および削除します。また、フラッシュ メモリにディレクトリを作成することもできます。また、TFTP、フラッシュメモリ、ローカル PC などさまざまなファイル システム間でファイル転送ができます。
Check for ASA/ASDM Updates	ウィザードを使用して ASA ソフトウェアおよび ASDM ソフトウェアをアップグレードします。
Upgrade Software from Local Computer	ASA イメージ、ASDM イメージ、またはユーザ PC の他のイメージをフラッシュ メモリにアップロードします。
Downgrade Software	現在実行中のものよりも古い ASA イメージをロードします。
Backup Configurations	ASA のコンフィギュレーション、Cisco Secure Desktop イメージ、および SSL VPN Client イメージおよびプロファイルをバックアップします。

[Tools] メニュー項目	説明
Restore Configurations	ASA のコンフィギュレーション、Cisco Secure Desktop イメージ、および SSL VPN Client イメージおよびプロファイルを復元します。
System Reload	ASDM を再起動し、保存したコンフィギュレーションをメモリにリロードします。
Administrator's Alert to Clientless SSL VPN Users	管理者が、クライアントレス SSL VPN ユーザーにアラートメッセージを送信できるようにします。詳細については、VPN 構成ガイドを参照してください。
Migrate Network Object Group Members	<p>8.3以降に移行する場合、ASA は名前付きネットワーク オブジェクトを作成して、一部の機能のインライン IP アドレスを置き換えます。名前付きオブジェクトに加えて、ASDM はコンフィギュレーションで使用されているすべての IP アドレスに対して名前なしオブジェクトを自動的に作成します。これらの自動作成されるオブジェクトは IP アドレスによるみ識別され、名前がなく、プラットフォーム設定に名前付きオブジェクトとしては存在しません。</p> <p>移行の一部として名前付きオブジェクトを ASA が作成する場合、合致する非名前付き ASDM 専用オブジェクトは、名前付きオブジェクトに置換されます。唯一の例外は、ネットワーク オブジェクト グループの非名前付きオブジェクトです。ネットワーク オブジェクト グループ内にある IP アドレスの名前付きオブジェクトを ASA が作成する場合、ASDM は非名前付きオブジェクトを維持したまま、重複したオブジェクトを ASDM で作成します。これらのオブジェクトをマージするには、[Tools] > [Migrate Network Object Group Members] を選択します。</p> <p>詳細については、「Cisco ASA 5500 Migration to Version 8.3 and Later」を参照してください。</p>
Preferences	セッション間での特定の ASDM 機能の動作を変更します。
ASDM Java Console	Java コンソールを表示します。

[Wizards] メニュー

[Wizards] メニューにより、さまざまな機能を設定するウィザードを実行できます。

[Wizards] メニュー項目	説明
Startup Wizard	ASA の初期設定を段階的にガイドします。
VPN Wizard	さまざまな VPN 設定用のウィザードが用意されています。詳細については、VPN 構成ガイドを参照してください。
High Availability and Scalability Wizard	フェールオーバーの設定が可能になります： VPN クラスタ ロードバランシングまたは ASA 上の ASA クラスタリング
Unified Communication Wizard	ASA 上で、IP 電話などのユニファイドコミュニケーション機能の設定が可能になります。詳細については、ファイアウォールの設定ガイドを参照してください。
ASDM Identity Certificate Wizard	Java 7 Update 51 以降を使用する場合、ASDM ランチャには信頼できる証明書が必要です。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。このウィザードを使用して証明書をインストールするまでは、Java Web Start を使用して ASDM を起動することができます。詳細については、 http://www.cisco.com/go/asdm-certificate を参照してください。
Packet Capture Wizard	ASA 上で、パケットキャプチャの設定が可能になります。このウィザードは、入出力インターフェイスのそれぞれでパケットキャプチャを1回実行します。キャプチャの実行後、キャプチャをコンピュータに保存し、パケットアナライザを使用してキャプチャを調査および分析できます。

[Window] メニュー

[Window] メニューを使用して、ASDM のウィンドウ間を移動できます。アクティブなウィンドウが選択されたウィンドウとして表示されます。

[Help] メニュー

[Help] メニューでは、オンラインヘルプへのリンクの他に、ASDM と ASA の情報も提供されます。

[Help] メニュー項目	説明
Help Topics	新しいブラウザ ウィンドウが開いて ASDM のオンラインヘルプが表示されます。ASDM で ASA Firepower モジュールを管理している場合は、この項目に [ASDM Help Topics] というラベルが表示されます。
ASA FirePOWER Help Topics	新しいブラウザ ウィンドウが開いて、ASA Firepower モジュールのオンラインヘルプが表示されます。この項目は、ASDM でモジュールをインストールして管理している場合にだけ使用できます。
Help for Current Screen	表示されている画面に関する状況依存ヘルプが開きます。または、ツールバーの [?] Help ボタンをクリックすることもできます。
Release Notes	Cisco.com にある最新バージョンの [ASDM release notes] を開きます。リリースノートには、ASDM のソフトウェアとハードウェア要件の最新情報、およびソフトウェア変更に関する最新情報が記載されています。
Cisco ASA Series Documentation	入手可能なすべての製品マニュアルへのリンクを含む Cisco.com 上のドキュメントが開きます。
ASDM Assistant	Cisco.com からダウンロード可能なコンテンツを検索でき、特定のタスクの実行に関する詳細がわかる ASDM Assistant を開きます。
About Cisco Adaptive Security Appliance (ASA)	ソフトウェアバージョン、ハードウェア構成、スタートアップ時にロードされるコンフィギュレーションファイルやソフトウェアイメージなど、ASA に関する情報を表示します。これらはトラブルシューティングの際に役立つ情報です。
About Cisco ASDM	ソフトウェアバージョン、ホスト名、権限レベル、オペレーティングシステム、デバイスタイプ、Java のバージョンなど、ASDM に関する情報を表示します。

ツールバー

メニューの下にある **ツールバー** から、ホーム ビュー、コンフィギュレーション ビュー、およびモニタリング ビューにアクセスできます。また、マルチ コンテキスト モードでシステムとセキュリティ コンテキストを選択したり、ナビゲーションおよびその他よく使用する機能を実行できます。

ツールバー ボタン	説明
Home	インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなど、ASA の重要な情報を表示できる [Home] ペインを表示します。マルチ モードの場合、[Home] ペインはありません。
Configuration	ASA を設定します。左側の [Navigation] ペインの機能ボタンをクリックして機能を設定します。
Monitoring	ASA をモニタします。左側の [Navigation] ペインの機能ボタンをクリックして、さまざまな要素をモニタします。
Save	書き込みアクセスが可能なコンテキストに限り、実行コンフィギュレーションをスタートアップ コンフィギュレーションとして保存します。 デバイス上に ASA FirePOWER モジュールがインストールされており、それを ASDM 経由で設定している場合は、このボタンに [Save ASA Changes] というラベルが表示されます。
Refresh	現在の実行コンフィギュレーションで ASDM をリフレッシュします。ただし、モニタリング ペインのグラフはリフレッシュしません。
Back	直前に表示した ASDM のペインに戻ります。
Forward	直前に表示した ASDM のペインに進みます。
Help	その時点で表示されている画面の状況依存ヘルプを表示します。
Search	ASDM 内で機能を検索します。検索機能は、各ペインのタイトルをすべて検索して一致項目を表示します。ハイパーリンクをクリックすると、該当ペインがただちに表示されます。[Back] または [Forward] をクリックすると、検出した2つのペインをすばやく切り替えることができます。

ASDM Assistant

ASDM Assistant では、タスクに応じた ASDM の使用方法のヘルプを検索し、表示できます。この機能は、シングル コンテキストとシステム コンテキストのルーテッドモードおよびトランスペアレントモードで使用できます。

[View] > [ASDM Assistant] > [How Do I?] の順に選択するか、メニューバーの [Look For] フィールドから検索リクエストを入力して情報にアクセスします。[Find] ドロップダウンリストから [How Do I?] を選択すると、検索が開始します。

ASDM Assistant を使用するには、次の手順を実行します。

手順

-
- ステップ 1** [View] > [ASDM Assistant] を選択します。
[ASDM Assistant] ペインが表示されます。
- ステップ 2** [Search] フィールドに検索する情報を入力して [Go] をクリックします。
要求された情報が [Search Results] ペインに表示されます。
- ステップ 3** [Search Results] 領域および [Features] 領域に表示される任意のリンクをクリックし、詳細情報を入手します。
-

ステータス バー

ステータス バーは ASDM ウィンドウの下部に表示されます。次の表に、左から右に表示される領域を示します。

エリア	説明
Status	コンフィギュレーションのステータス（「Device configuration loaded successfully.」など）。
Failover	フェールオーバー装置のステータスで、アクティブまたはスタンバイのいずれか。
User Name	ASDM ユーザのユーザ名。ユーザ名なしでログインした場合、ユーザ名は「admin」です。
User Privilege	ASDM ユーザの特権。

エリア	説明
Commands Ignored by ASDM	アイコンをクリックすると、ASDM で処理されなかったコンフィギュレーションのコマンドのリストが表示されます。これらのコマンドはコンフィギュレーションから削除されません。
Connection to Device	ASDM の ASA との接続ステータス。
Syslog Connection	syslog 接続が動作しており、ASA が監視されています。
SSL Secure	ASDM への接続に SSL を使用し、安全であることを示します。
時刻	ASA に設定された時刻。

Connection to Device

ASDM は ASA との接続を常に維持し、[Monitoring] ペインおよび [Home] ペインのデータを最新に保ちます。このダイアログボックスに接続ステータスが表示されます。コンフィギュレーションを変更する場合、変更している間 ASDM は接続をもう一つ開き、変更が終わるとその接続を閉じますが、このダイアログボックスには 2 つ目の接続は表示されません。

Device List

[Device List] はドッキング可能なペインです。ヘッダーにある 3 つのボタンをそれぞれクリックすると、ペインの最大化または復元、移動可能なフローティングペインへの変更、ペインの非表示化、またはペインを閉じることができます。このペインはホーム、コンフィギュレーション、モニタリング、およびシステムの各ビューで使用できます。このペインを使用して、別のデバイスに切り替えたり、システムとコンテキスト間で切り替えたりすることができますが、現在実行中のものと同じバージョンの ASDM がそのデバイスでも動作している必要があります。ペインを完全に表示するには、少なくとも 2 つのデバイスがリストに表示されている必要があります。このペインは、シングル コンテキスト、マルチ コンテキストおよびシステム コンテキストのルーテッドモードおよびトランスペアレントモードで使用できます。

このペインを使用して別のデバイスに接続するには、次の手順を実行します。

手順

ステップ 1 [Add] をクリックしてリストに別のデバイスを追加します。

[Add Device] ダイアログボックスが表示されます。

ステップ 2 デバイス名またはデバイスの IP アドレスを入力し、[OK] をクリックします。

ステップ 3 リストから選択したデバイスを削除するには、[Delete] をクリックします。

ステップ 4 [Connect] をクリックして別のデバイスに接続します。

[Enter Network Password] ダイアログボックスが表示されます。

ステップ 5 ユーザ名とパスワードを該当するフィールドに入力し、[Login] をクリックします。

共通ボタン

多くの ASDM ペインには、次の表に示すボタンが含まれています。目的の作業を完了するには、該当するボタンをクリックします。

ボタン	説明
Apply	ASDM での変更内容を ASA に送信し、実行コンフィギュレーションに適用します。
Save	実行コンフィギュレーションのコピーをフラッシュメモリに書き込みます。
Reset	変更内容を破棄して、変更前、または [Refresh] や [Apply] を最後にクリックした時点の表示情報に戻します。[Reset] をクリックした後、[Refresh] をクリックして、現在の実行コンフィギュレーションの情報が表示されていることを確認します。
Restore Default	選択した設定をクリアしてデフォルト設定に戻します。
Cancel	変更内容を破棄して、前のペインに戻ります。
Enable	機能について読み取り専用の統計情報を表示します。
Close	開いているダイアログボックスを閉じます。
Clear	フィールドから情報を削除します。または、チェックボックスをオフにします。
Back	前のペインに戻ります。
Forward	次のペインに移動します。
Help	選択したペインまたはダイアログボックスを表示します。

キーボードショートカット

キーボードを使用して ASDM ユーザ インターフェイスをナビゲートできます。

次の表に、ASDM ユーザ インターフェイスの 3 つの主要な領域間を移動するために使用可能なキーボードショートカットの一覧を示します。

表 2: メインウィンドウ内のキーボードショートカット

表示対象	Windows/Linux	MacOS
[Home] ペイン	Ctrl+H	Shift+Command+H
[Configuration] ペイン	Ctrl+G	Shift+Command+G
[Monitoring] ペイン	Ctrl+M	Shift+Command+M
Help	F1	Command+?
Back	Alt+左矢印	Command+[
Forward	Alt+右矢印	Command+]
表示のリフレッシュ	F5	Command+R
Cut	Ctrl+X	Command+X
Copy	Ctrl+C	Command+C
Paste	Ctrl+V	Command+V
コンフィギュレーションの保存	Ctrl+S	Command+S
ポップアップメニュー	Shift+F10	—
セカンダリ ウィンドウを閉じる	Alt+F4	Command+W
Find	Ctrl+F	Command+F
Exit	Alt+F4	Command+Q
テーブルまたはテキスト領域の終了	Ctrl_Shift または Ctrl+Shift+Tab	Ctrl+Shift または Ctrl+Shift+Tab

次に表に、ペイン内部のナビゲーションに使用可能なキーボードショートカットの一覧を示します。

表 3: ペイン内のキーボードショートカット

フォーカスの移動先	キー
次のフィールド	タブ
前のフィールド	Shift+Tab
次のフィールド (テーブル内にフォーカスがある場合)	Ctrl+Tab
前のフィールド (テーブル内にフォーカスがある場合)	Shift+Ctrl+Tab
次のタブ (タブにフォーカスがある場合)	右矢印
前のタブ (タブにフォーカスがある場合)	左矢印
テーブル内の次のセル	タブ
テーブル内の前のセル	Shift+Tab
次のペイン (複数のペインが表示されている場合)	F6
前のペイン (複数のペインが表示されている場合)	Shift+F6

次の表に、Log Viewer で使用可能なキーボード ショートカットの一覧を示します。

表 4: ログビューアのキーボードショートカット

目的	Windows/Linux	MacOS
Real-Time Log Viewer の一時停止および再開	Ctrl+U	Command+
ログバッファ ペインのリフレッシュ	F5	Command+R
Clear Internal Log Buffer	Ctrl+Delete	Command+Delete
選択したログ エントリのコピー	Ctrl+C	Command+C
ログの保存	Ctrl+S	Command+S
印刷	Ctrl+P	Command+P
セカンダリ ウィンドウを閉じる	Alt+F4	Command+W

次の表に、メニュー項目へのアクセスに使用可能なキーボードショートカットの一覧を示します。

表 5: メニュー項目にアクセスするためのキーボードショートカット

アクセス対象	Windows/Linux
メニュー バー	Alt
次のメニュー	右矢印
前のメニュー	左矢印
次のメニュー オプション	下矢印
前のメニュー オプション	上矢印
選択したメニュー オプション	Enter

ASDM ペインの検索機能

一部の ASDM ペインには、多くの要素を持つテーブルが含まれています。特定のエントリを簡単に検索および強調表示して編集するために、複数の ASDM ペインには、これらのペイン内のオブジェクトを検索できる検索機能が含まれています。

検索を実行する場合は、[Find] フィールドにフレーズを入力し、特定のペイン内のすべてのコラムを検索できます。フレーズにはワイルドカード文字の「*」および「?」を含めることができます。* は 1 つ以上の文字と一致し、? は 1 つの文字と一致します。[Find] フィールドの右にある上矢印と下矢印を使用して、次（上）または前（下）のフレーズの出現に移動します。[Match Case] チェックボックスをオンにすると、入力した大文字および小文字に正確に一致するエントリを検索します。

たとえば、**B*ton-L*** と入力すると、次の一致が返されます。

Boston-LA, Boston-Lisbon, Boston-London

Bo?ton と入力すると、次の一致が返されます。

Boston, Bolton

ルール リストの検索機能

ACL や ACE およびその他のルールにはさまざまなタイプの多数の要素が含まれているため、ルールを表示する任意のペインの検索機能では、他のペインの検索機能よりも対象を絞った検

索を実行できます。これには、アクセスルール、サービス ポリシー ルール、ACL Manager、ACL ルールを一覧表示するその他のペイン、および NAT ルールも含まれます。

ルール リスト内で要素を検索するには、次の手順を実行します。

手順

ステップ 1 [Find] をクリックします。

ステップ 2 [Filter] フィールドで、ドロップダウン リストから次のオプションのいずれかを選択します。

検索可能な項目は、ルールタイプによって異なり、表の列に対応しています。複数のフィールドを使用する複雑な検索を作成する場合は、[Query] を選択します。

ステップ 3 [Query] を選択しなかった場合は、2 番目のフィールドで、ドロップダウン リストから次のいずれかのオプションを選択します。

- [is] : 検索文字列に対する完全一致を指定します。これは常にクエリのオプションです。
- [contains] : 検索文字列の一部または全部を含む任意のルールに対する一致を指定します。

ステップ 4 3 番目のフィールドに、検索する文字列を入力します。... をクリックすると、リストからオブジェクトを選択できます。クエリを使用している場合は、[Define Query] をクリックします。

IP アドレスを検索する場合は、ASDM によって作成されたオブジェクトまたはグループである限り、ネットワーク オブジェクトまたはグループ内のアドレスに一致するものを取得できません。つまり、グループ名は DM_INLINE で始まります。検索機能は、ユーザが作成したオブジェクト内の IP アドレスを検索できません。

ステップ 5 検索を実行するには、[Filter] をクリックします。

ビューが更新され、一致するルールのみが表示されます。ルール番号は、ルールリスト内の絶対位置を確認できるように維持されます。

ステップ 6 [Clear] をクリックすると、フィルタが削除され、リスト全体が再度表示されます。

ステップ 7 完了したら、赤色の **x** をクリックして検索コントロールを閉じます。

拡張スクリーン リーダ サポートの有効化

デフォルトでは、Tab キーを押してペイン内を移動するときに、ラベルと説明はタブの移動先から除外されます。JAWS のような一部のスクリーンリーダだけが、フォーカスのある画面オブジェクトを読み取ります。拡張スクリーン リーダ サポートをイネーブルにすると、ラベルと説明にもタブを移動させることができます。

拡張スクリーン リーダ サポートをイネーブルにするには、次の手順を実行します。

手順

- ステップ 1** [Tools] > [Preferences] の順に選択します。
[Preferences] ダイアログボックスが表示されます。
- ステップ 2** [General] タブの [Enable screen reader support] チェックボックスをオンにします。
- ステップ 3** [OK] をクリックします。
- ステップ 4** スクリーン リーダ サポートをアクティブにするには、ASDM を再起動します。
-

整理用フォルダー

コンフィギュレーション ビューおよびモニタリング ビューのナビゲーション ペインに含まれる一部のフォルダには、関連付けられたコンフィギュレーション ペインやモニタリング ペインがありません。これらのフォルダは、関連するコンフィギュレーション タスクやモニタリング タスクを整理するために使用します。これらのフォルダをクリックすると、右側の [Navigation] ペインにサブ項目のリストが表示されます。サブ項目の名前をクリックするとその項目に移動できます。

[Home] ペイン（シングル モードとコンテキスト）

ASDM の [Home] ペインでは、ASA に関する重要な情報を表示できます。[Home] ペインのステータス情報は 10 秒間隔で更新されます。このペインには通常、[Device Dashboard] と [Firewall Dashboard] の 2 つのタブがあります。

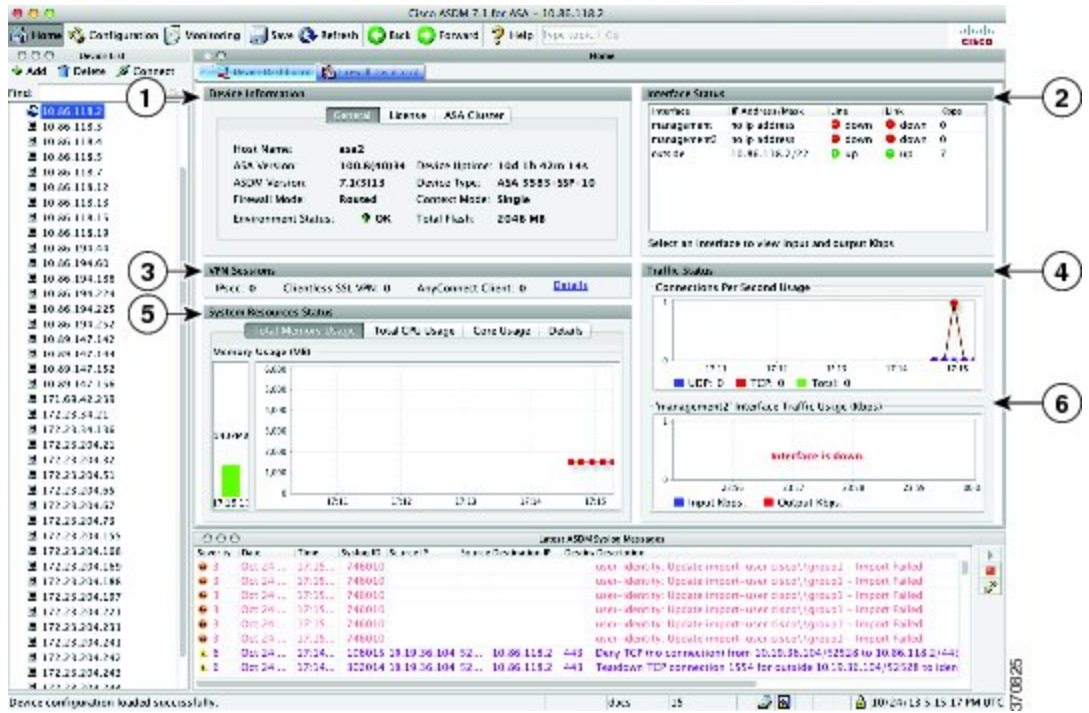
IPS モジュール、CX モジュール、ASA Firepower モジュールなどのハードウェアまたはソフトウェア モジュールがデバイスにインストールされている場合は、それ専用のタブが表示されます。

[Device Dashboard] タブ

[Device Dashboard] タブでは、インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなど、ASA の重要な情報を一目で確認できます。

次の図に、[Device Dashboard] タブの要素を示します。

図 2: [Device Dashboard] タブ



凡例

GUI 要素	説明
1	[Device Information] ペイン (82 ページ)
2	[Interface Status] ペイン (83 ページ)
3	[VPN Sessions] ペイン (83 ページ)
4	[Traffic Status] ペイン (84 ページ)
5	[System Resources Status] ペイン (83 ページ)
6	[Traffic Status] ペイン (84 ページ)
—	Device List (74 ページ)
—	[Latest ASDM Syslog Messages] ペイン (84 ページ)

[Device Information] ペイン

[Device Information] ペインには、[General] タブと [License] タブというデバイス情報を表示する 2 つのタブがあります。[General] タブでは、システムヘルスが一目でわかる [Environment Status] ボタンにアクセスできます。

[General] タブ

このタブには、ASA に関する次の基本情報が表示されます。

- [Host name] : デバイスのホスト名を表示します。
- [ASA version] : デバイス上で実行されている ASA ソフトウェアのバージョンを示します。
- [ASDM version] : デバイス上で実行されている ASDM ソフトウェアのバージョンを表示します。
- [Firewall mode] : デバイスが実行されているファイアウォール モードを表示します。
- [Total flash] : 現在使用されている RAM の合計を表示します。
- [ASA Cluster Role] : クラスタリングが有効の場合に、この装置のロール (マスターまたはスレーブ) を表示します。
- [Device uptime] : 最後にソフトウェアをアップロードしてから、デバイスが動作している時間を表示します。
- [Context mode] : デバイスが実行されているコンテキスト モードを表示します。
- [Total Memory] : ASA にインストールされている DRAM を表示します。
- [Environment status] : システムヘルスを表示します。[General] タブの [Environment Status] というラベルの右側にあるプラス記号 (+) をクリックして、ハードウェア統計情報を表示します。設置されている電源装置数の確認、ファンと電源モジュールの動作ステータスの追跡、および CPU の温度とシステムの周囲温度の追跡を実行できます。

一般に、[Environment Status] ボタンでシステムヘルスが一目でわかります。システム内のモニタ対象のすべてのハードウェアコンポーネントが正常な範囲内で動作している場合、プラス記号 (+) ボタンには [OK] が緑で表示されます。一方、ハードウェアシステム内のコンポーネントが 1 つでも正常な範囲外で動作している場合は、プラス記号 (+) ボタンが赤色の丸になってクリティカルステータスを示し、ハードウェアコンポーネントに関してすぐに対処が必要であることを示します。

特定のハードウェアの統計情報に関する詳細については、そのデバイスの『ハードウェアガイド』を参照してください。



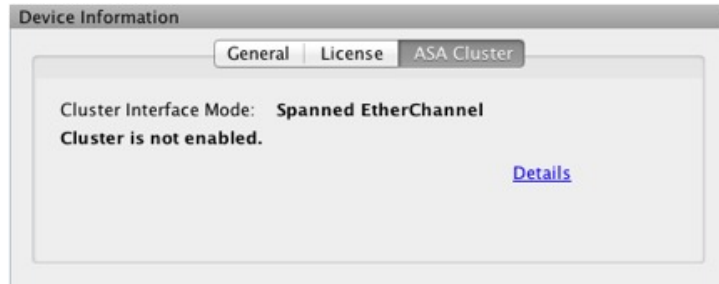
- (注) 最新リリースの ASA にアップグレードするにはメモリが不足している場合は、[Memory Insufficient Warning] ダイアログボックスが表示されます。このダイアログボックスに表示される指示に従って、サポートされている方法で ASA および ASDM を継続して使用します。[OK] をクリックして、このダイアログボックスを閉じます。

[License] タブ

このタブには、ライセンス機能のサブセットが表示されます。詳細なライセンス情報の表示または新しいアクティベーションキーの入力を行うには、[More Licenses] をクリックします。[Configuration] > [Device Management] > [Licensing] > [Activation Key] ペインが表示されます。

[Cluster] タブ

このタブには、クラスタのインターフェイスモードおよびクラスタのステータスが表示されます。



仮想リソース タブ (ASAv)

このタブは、ASA によって使用されている仮想リソースを表示します。vCPU の数、RAM、ASA のプロビジョニングの過不足が含まれます。

[Interface Status] ペイン

このペインには、各インターフェイスのステータスが表示されます。インターフェイスの行を選択すると、入力および出力スループットが Kbps 単位でテーブルの下に表示されます。

[VPN Sessions] ペイン

このペインには、VPN トンネルステータスが表示されます。[Details] をクリックすると、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] ペインに移動します。

[Failover Status] ペイン

このペインには、フェールオーバーステータスが表示されます。

[Configure] をクリックして、High Availability and Scalability Wizard を起動します。このウィザードを完了すると、フェールオーバーコンフィギュレーションステータス ([Active/Active] または [Active/Standby]) が表示されます。

フェールオーバーが設定されている場合は、[Details] をクリックすると、[Monitoring] > [Properties] > [Failover] > [Status] ペインが開きます。

[System Resources Status] ペイン

このペインには、CPU およびメモリの使用状況に関する統計情報が表示されます。

[Traffic Status] ペイン

このペインには、インターフェイス全体の接続数/秒と、最も遅いセキュリティ インターフェイスのトラフィック スループットのグラフが表示されます。

コンフィギュレーションにセキュリティ レベルが最も低いインターフェイスが複数含まれており、そのいずれかの名前が「outside」である場合、そのインターフェイスがトラフィック スループットのグラフに使用されます。それ以外の場合、ASDM はセキュリティ レベルが最も低いインターフェイスのアルファベット順のリストから最初のインターフェイスを選択します。

[Latest ASDM Syslog Messages] ペイン

このペインには、ASA が生成した最新のシステム メッセージが 100 個まで表示されます。ロギングがディセーブルになっている場合は、[Enable Logging] をクリックしてイネーブルにします。

次の図に、[Latest ASDM Syslog Messages] ペインの要素を示します。

図 3: [Latest ASDM Syslog Messages] ペイン



凡例

GUI 要素	説明
1	ペインのサイズを変更するには、 ディバイダ を上または下にドラッグします。
2	ペインを展開します。ペインをデフォルトのサイズに戻すには、 二重の正方形のアイコン をクリックします。
3	フローティング ペインを作成します。ペインをドッキングするには、 ドッキングしたペインアイコン をクリックします。

GUI 要素	説明
4	自動非表示をイネーブルまたはディセーブルにします。自動非表示がイネーブルな場合は、左下隅にある [Latest ASDM Syslog Messages] ボタンの上にカーソルを移動すると、ペインが表示されます。カーソルをペインから離すと、ペインは非表示になります。
5	ペインを閉じます。ペインを表示するには、[View Latest ASDM Syslog Messages] を選択します。
6	右側にある緑のアイコンをクリックすると、syslog メッセージの表示の更新を続行します。
7	右側にある赤いアイコンをクリックすると、syslog メッセージの表示の更新を停止します。
8	右側にあるフィルタ アイコンをクリックすると、[Logging Filters] ペインが開きます。

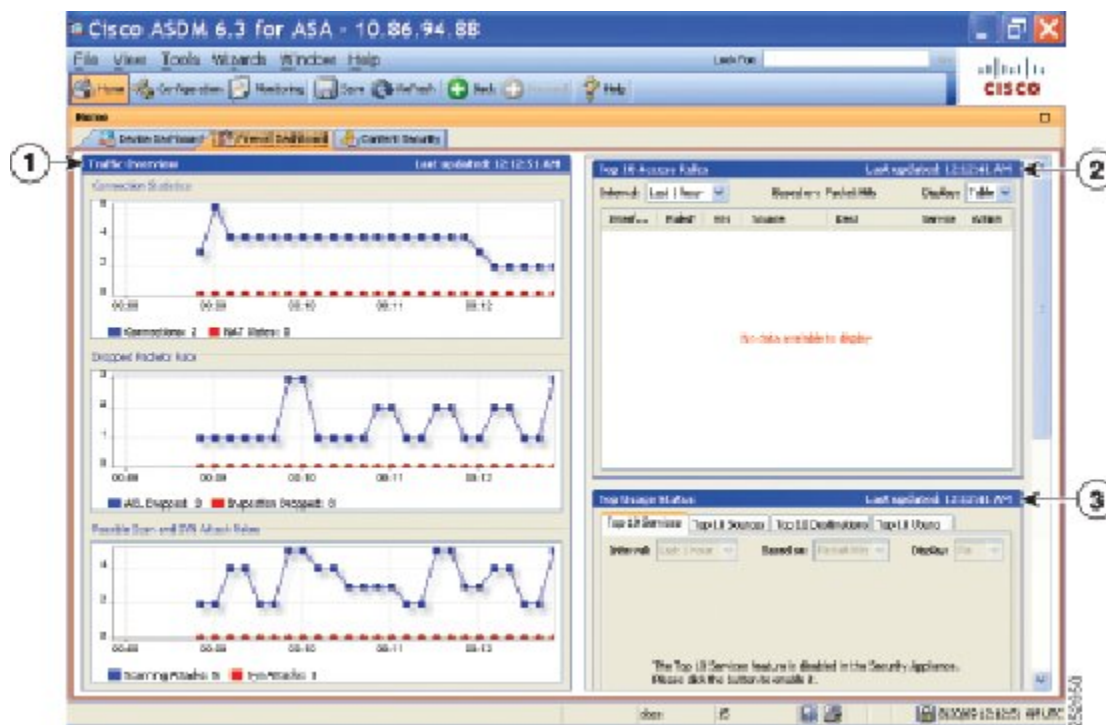
- イベントを右クリックして [Clear Content] を選択すると、現在のメッセージを消去します。
- イベントを右クリックして [Save Content] をクリックすると、現在のメッセージを PC 上のファイルに保存します。
- イベントを右クリックして [Copy] を選択すると、現在の内容をコピーします。
- イベントを右クリックして [Color Settings] を選択すると、重大度に基づいて syslog メッセージの背景色と前景色を変更します。

[Firewall Dashboard] タブ

[Firewall Dashboard] タブでは、ASA を通過するトラフィックに関する重要な情報を確認できます。このダッシュボードは、シングル コンテキスト モードまたはマルチ コンテキスト モードのどちらであるかにより異なります。マルチ コンテキスト モードでは、[Firewall Dashboard] は各コンテキスト内に表示できます。

次の図に、[Firewall Dashboard] タブの要素の一部を示します。

図 4: [Firewall Dashboard] タブ



凡例

GUI 要素	説明
1	[Traffic Overview] ペイン (86 ページ)
2	[Top 10 Access Rules] ペイン (87 ページ)
3	[Top Usage Status] ペイン (87 ページ)
(表示なし)	[Top Ten Protected Servers Under SYN Attack] ペイン (88 ページ)
(表示なし)	[Top 200 Hosts] ペイン (88 ページ)
(表示なし)	[Top Botnet Traffic Filter Hits] ペイン (88 ページ)

[Traffic Overview] ペイン

デフォルトでは、イネーブルです。基本脅威検出をディセーブルにすると (を参照)、この領域には [Enable] ボタンが表示されます。[Enable] ボタンを使用して基本脅威検出をディセーブルにできます。実行時の統計情報には、表示専用の次の情報が含まれます。

- 接続数と NAT 変換数。

- アクセスリストによる拒否およびアプリケーション インспекションによってドロップされたパケット数/秒。
- ドロップパケット数/秒。これは、スキャン攻撃の一部として特定される場合と、不完全なセッションとして検出される場合（TCP SYN 攻撃やデータなし UDP セッション攻撃を検出した場合など）があります。

[Top 10 Access Rules] ペイン

デフォルトでは、イネーブルです。アクセスルールの脅威検出統計情報をディセーブルにすると（『ファイアウォールの設定ガイド』を参照）、この領域には [Enable] ボタンが表示されます。[Enable] ボタンを使用してアクセスルールの統計情報を有効にできます。

テーブルビューでは、リストからルールを選択して右クリックし、ポップアップメニュー項目の [Show Rule] を表示できます。この項目を選択して [Access Rules] テーブルに移動し、テーブル内にあるそのルールを選択します。

[Top Usage Status] ペイン

デフォルトでは、ディセーブルです。このペインには、次の4つのタブがあります。

- [Top 10 Services] : 脅威検出サービス
- [Top 10 Sources] : 脅威検出サービス
- [Top 10 Destinations] : 脅威検出サービス
- [Top 10 Users] : アイデンティティ ファイアウォール サービス

最初の3つのタブ（[Top 10 Services]、[Top 10 Sources]、および [Top 10 Destinations]）では、脅威検出サービスに関する統計情報を提供します。各タブには、それぞれの脅威検出サービスをイネーブルにする [Enable] ボタンがあります。『ファイアウォールの設定ガイド』に従って、これらを有効にできます。

[Top 10 Services Enable] ボタンを使用すると、ポートとプロトコルの両方の統計情報がイネーブルになります（どちらも表示用にイネーブルにする必要があります）。[Top 10 Sources] ボタンおよび [Top 10 Destinations Enable] ボタンを使用すると、ホストの統計情報がイネーブルになります。ホスト（送信元および宛先）の上位使用ステータス統計情報、およびポートとプロトコルが表示されます。

4番目のタブ [Top 10 Users] では、アイデンティティ ファイアウォール サービスに関する統計情報を提供します。アイデンティティ ファイアウォール サービスでは、ユーザのアイデンティティに基づくアクセスコントロールを提供します。送信元 IP アドレスではなくユーザ名とユーザグループ名に基づいてアクセスルールとセキュリティ ポリシーを設定できます。ASA は、IP とユーザのマッピング データベースにアクセスして、このサービスを提供します。

[Top 10 Users] タブは、次のいずれかを設定した場合のみ、データを表示します。

- Identity Firewall サービス コンフィギュレーション : Microsoft Active Directory および Cisco Active Directory (AD) エージェントの追加コンポーネントの設定を含みます。Identity Firewall

サービスは、**user-identity enable** コマンド（デフォルトで有効）および **user-accounting statistics** コマンドを衣装して有効化されます。

- VPN ユーザの認証、認可またはアカウンティングを行うために RADIUS サーバを使用する VPN コンフィギュレーション。

選択したオプションに応じて、[Top 10 Users] タブに、上位 10 ユーザの受信した EPS パケット、送信した EPS パケット、および送信された攻撃に関する統計情報が表示されます。

(*domain\user_name* として表示される) 各ユーザに関して、このタブには、そのユーザの平均 EPS パケット、現在の EPS パケット、トリガー、および合計イベント数が表示されます。



注意 拡張統計情報を有効にすると、有効にする統計情報のタイプに応じて、ASA のパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きな影響があります。トラフィックの負荷が高い場合は、このタイプの統計情報は一時的にイネーブルにすることを検討してください。ただし、ポートの統計情報をイネーブルにしても、それほど影響はありません。

[Top Ten Protected Servers Under SYN Attack] ペイン

デフォルトでは、ディセーブルです。この領域に表示されている [Enable] ボタンを使用して、この機能を有効にできます。または、『ファイアウォール設定ガイド』に従って有効にすることもできます。攻撃を受けて保護された上位 10 サーバの統計情報が表示されます。

平均攻撃レートの場合、ASA はレート間隔（デフォルトは 30 分）に対して 30 秒ごとにデータをサンプリングします。

複数の攻撃者がいる場合は、「<various>」の後に最後の攻撃者の IP アドレスが表示されます。

[Detail] をクリックして、10 台のサーバだけでなく、すべてのサーバ（最大 1000 台）の統計情報を表示します。履歴サンプリング データを確認することもできます。ASA はレート間隔の間に攻撃の数を 60 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。

[Top 200 Hosts] ペイン

デフォルトでは、ディセーブルです。ASA を介して接続中の上位 200 のホストを表示します。ホストの各エントリには、ホストの IP アドレスと、ホストによって開始された接続の数が含まれ、このエントリは 120 秒ごとにアップデートされます。この表示をイネーブルにするには **hpm topnenable** コマンドを入力します。

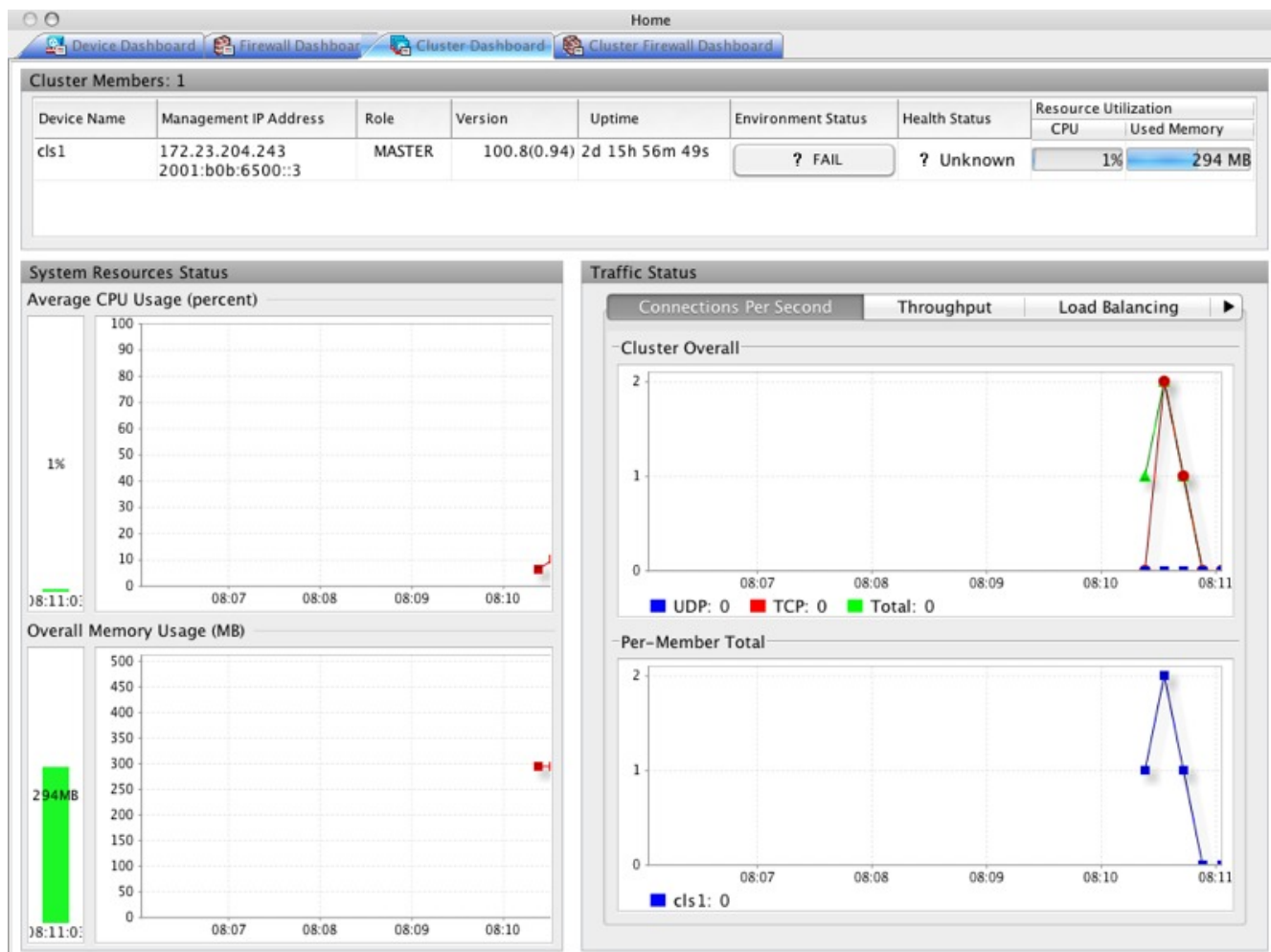
[Top Botnet Traffic Filter Hits] ペイン

デフォルトでは、ディセーブルです。この領域には、ボットネットトラフィックフィルタを設定するためのリンクが含まれています。上位 10 個のボットネットサイト、ポート、および感染ホストのレポートは、データのスナップショットを提供し、統計情報の収集開始以降の上位 10 項目に一致しない場合があります。IP アドレスを右クリックすると、**whois** ツールが起動してボットネットサイトの詳細が表示されます。

詳細については、『ボットネット設定ガイド』を参照してください。

[Cluster Dashboard] タブ

ASA クラスタリングをイネーブルにして、マスターユニットに接続している場合は、[Cluster Dashboard] タブにクラスタのメンバーシップとリソース使用率の概要が表示されます。



- [Cluster Members] : クラスタを構成するメンバーの名前と基本情報（管理 IP アドレス、バージョン、クラスタ内のロールなど）およびメンバーのヘルスステータス（環境ステータス、ヘルスステータス、およびリソース使用率）を表示します。

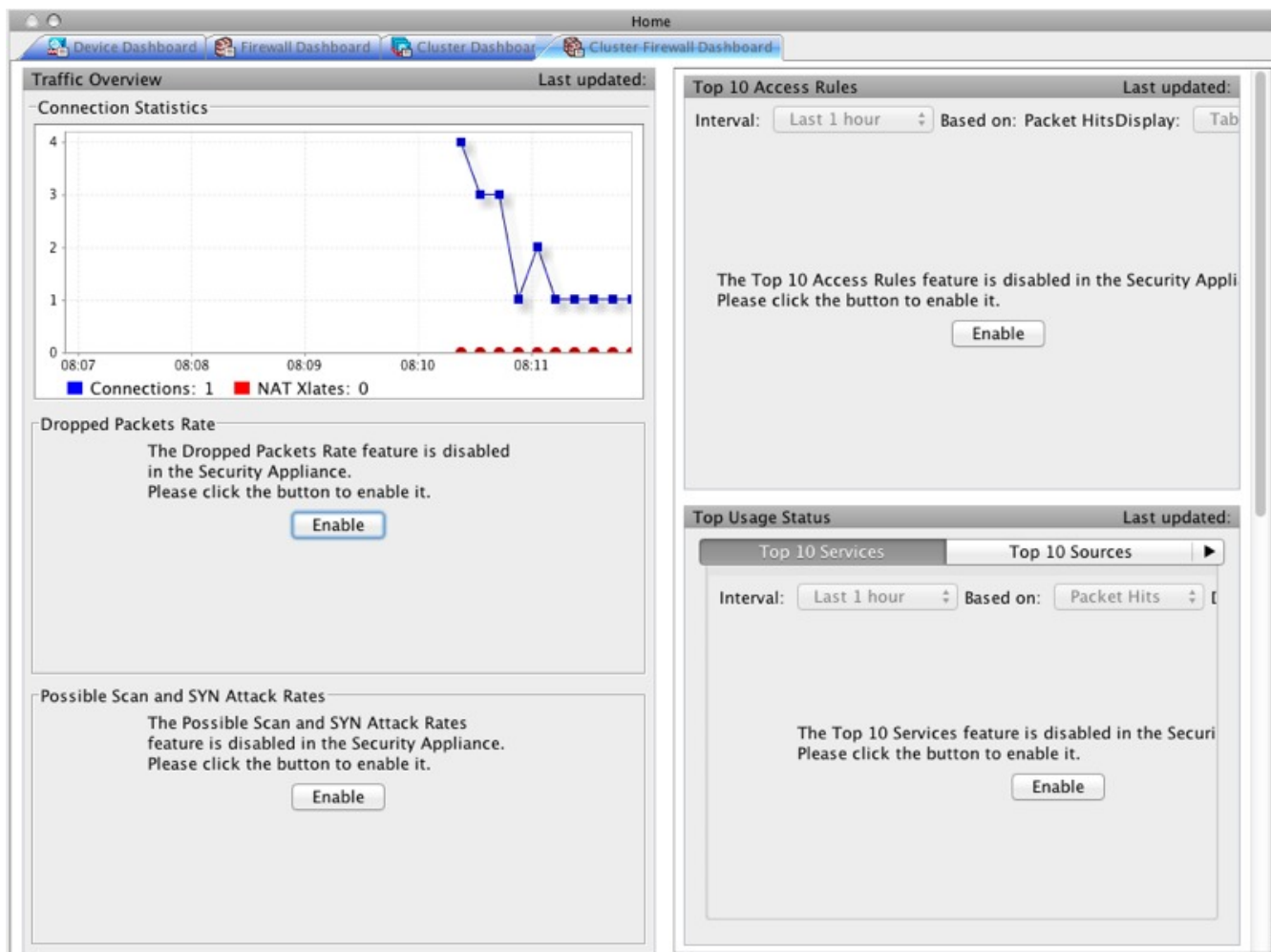


(注) マルチ コンテキスト モードでは、管理コンテキストに ASDM を接続し、次に別のコンテキストに変更しても、リスト表示されている管理 IP アドレスは現在のコンテキストの管理 IP アドレスに変更されません。ASDM が現在接続されているメインクラスターの IP アドレスを含む管理コンテキストの管理 IP アドレスを、引き続き表示し続けます。

- [System Resource Status] : クラスタ全体のリソース使用率 (CPU およびメモリ) とトラフィックのグラフ (クラスタ全体およびデバイスごと) を表示します。
- [Traffic Status] : 各タブには次のグラフがあります。
 - [Connections Per Second] タブ
 - [Cluster Overall] : クラスタ全体の秒単位の接続数が表示されます。
 - [Per-Member Total] : 各メンバーの秒単位の平均接続数が表示されます。
 - [Throughput] タブ
 - [Cluster Overall] : クラスタ全体の総出力スループットが表示されます。
 - [Per-Member Throughput] : メンバーのスループットが、メンバーごとに 1 行ずつ表示されます。
 - [Load Balancing] タブ
 - [Per-Member Percentage of Total Traffic] : メンバーが受信した総クラスタ トラフィックの割合が、メンバーごとに表示されます。
 - [Per-Member Locally Processed Traffic] : ローカルに処理されたトラフィックの割合が、メンバーごとに表示されます。
 - [Control Link Usage] タブ
 - [Per-Member Receiving Capacity Utilization] : 送信容量の使用率が、メンバーごとに表示されます。
 - [Per-Member Transmittal Capacity Utilization] : 受信容量の使用率が、メンバーごとに表示されます。

[Cluster Firewall Dashboard] タブ

[Cluster Firewall Dashboard] タブには、[Firewall Dashboard] に表示される情報と同様のトラフィックの概要および「top N」統計情報が表示されますが、クラスタ全体にわたる総計は表示されません。



[Content Security] タブ

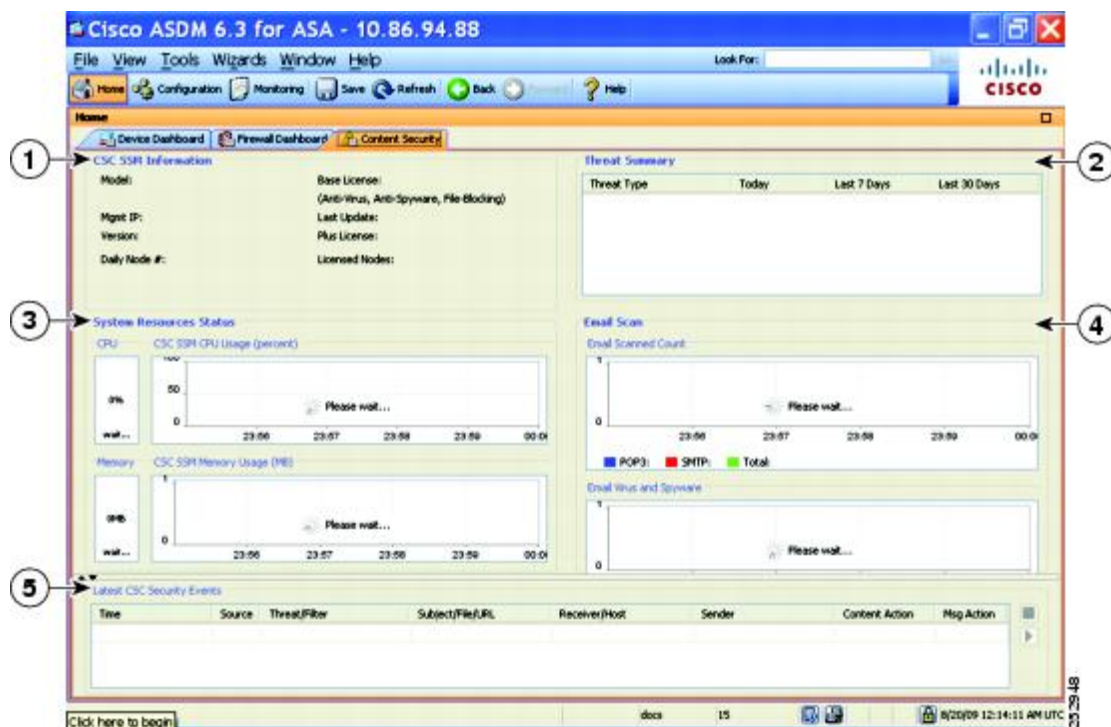
[Content Security] タブでは、CSC（Content Security and Control）SSM に関する重要な情報を確認できます。このペインは、CSC SSM で動作している CSC ソフトウェアが ASA にインストールされている場合のみ表示されます。



- (注) [Configuration] > [Trend Micro Content Security] > [CSC Setup] を選択して **CSC Setup Wizard** を完了していないと、[Home] > [Content Security] の下にあるペインにアクセスできません。代わりにダイアログボックスが表示され、この場所から **CSC Setup Wizard** に直接アクセスできます。

次の図に、[Content Security] タブの要素を示します。

図 5: [Content Security] タブ



凡例

GUI 要素	説明
1	[CSC SSM Information] ペイン。
2	[Threat Summary] ペイン。CSC SSM により検出された脅威の集約データを表示します。ウイルス、スパイウェア、フィルタリングまたはブロックされた URL、ブロックされたスパム、ブロックされたファイル、損害制御サービスなどがあります。
3	[System Resources Status] ペイン。
4	[Email Scan] ペイン。グラフには、10 秒間隔でデータが表示されます。
5	[Latest CSC Security Events] ペイン。

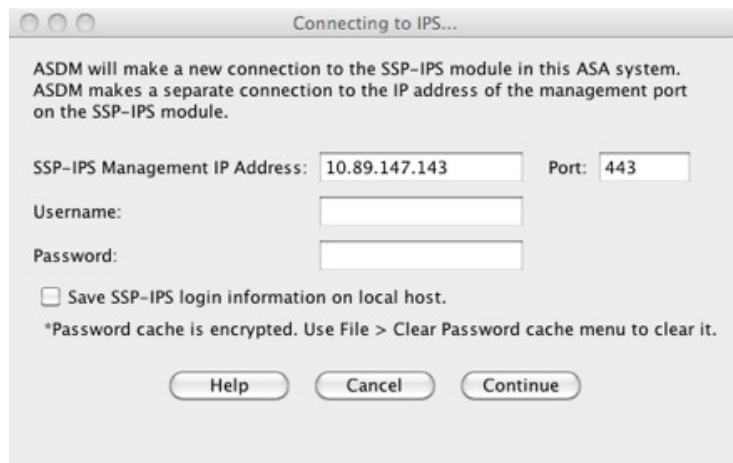
[Intrusion Prevention] タブ

[Intrusion Prevention] タブでは、IPS に関する重要な情報を確認できます。このタブは、ASA に IPS モジュールがインストールされている場合にのみ表示されます。

IPS モジュールに接続するには、次の手順を実行します。

1. [Intrusion Prevention] タブをクリックします。

[Connecting to IPS] ダイアログボックスが表示されます。

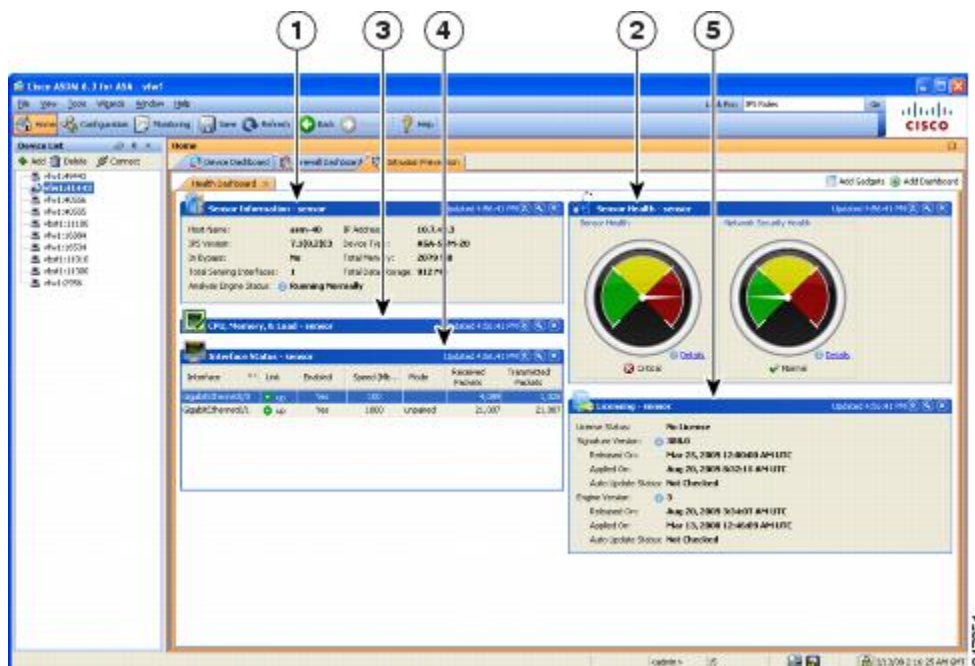


2. IP アドレス、ポート、ユーザ名、およびパスワードを入力します。デフォルトの IP アドレスとポートは 192.168.1.2:443 です。デフォルトのユーザ名およびパスワードは、**cisco** と **cisco** です。
3. ログイン情報をローカル PC に保存するには、[Save IPS login information on local host] チェックボックスをオンにします。
4. [Continue] をクリックします。

侵入防御に関する詳細については、『IPS クイック スタート ガイド』を参照してください。

次の図に、[Intrusion Prevention] タブにある [Health Dashboard] タブの要素を示します。

図 6 : [Intrusion Prevention] タブ (Health Dashboard)



凡例

GUI 要素	説明
1	[Sensor Information] ペイン。
2	[Sensor Health] ペイン。
3	[CPU, Memory, and Load] ペイン。
4	[Interface Status] ペイン。
5	[Licensing] ペイン。

[ASA CX Status] タブ

[ASA CX Status] タブには、ASA CX モジュールに関する重要な情報が表示されます。このタブは、ASA に ASA CX モジュールがインストールされている場合にのみ表示されます。

Device Information		Interface Status	
Last updated: 10:56:39 AM		Last updated: 10:56:39 AM	
Model:	ASA5585-SSP-CX10	Application Name:	ASA CX Security Module
Hardware Version:	1.3	Application Status:	Up
Serial Number:	JAF1543CGRB	Application Status Description:	Normal Operation
Firmware Version:	2.0(13)0	Application Version:	0.6.1
Software Version:	0.6.1	Data plane Status:	Up
MAC Address Range:	70ca.9bf0.1ca0 to 70ca.9bf0.1cab	Status:	Up

Connect to the ASA CX application: <https://10.89.147.153:443>

[ASA Firepower Status] タブ

[ASA FirepowerStatus] タブには、このモジュールに関する情報が表示されます。この情報には、モデル、シリアル番号、ソフトウェアバージョンなどのモジュール情報と、アプリケーション名、アプリケーションステータス、データプレーンステータス、全体のステータスなどのモジュールステータスが含まれます。モジュールが FireSIGHT Management Center に登録されている場合は、リンクをクリックしてアプリケーションを開き、詳細な分析やモジュールの設定を行うことができます。

このタブは、ASA Firepower モジュールがデバイスにインストールされている場合にのみ表示されます。

FireSIGHT Management Center ではなく ASDM を使用して ASA Firepower モジュールを管理している場合は、追加のタブが表示されます。

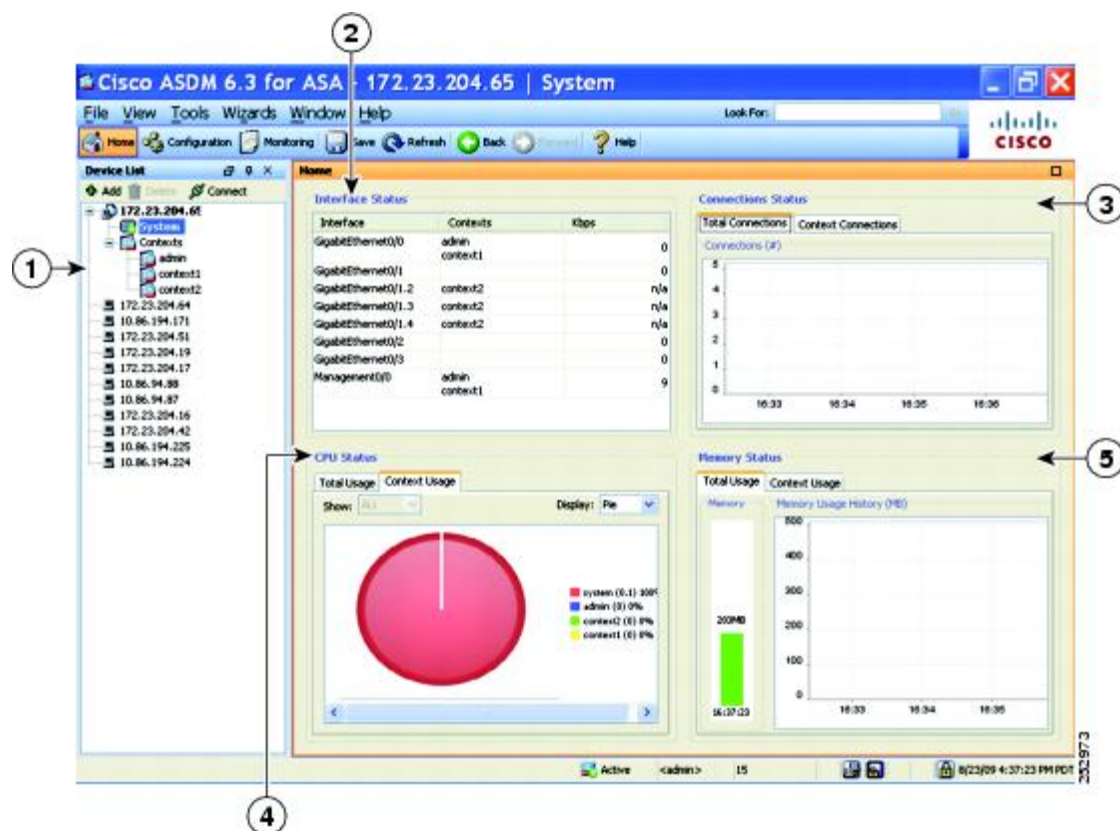
- **[ASA Firepower Dashboard]** : ダッシュボードには、モジュールで実行中のソフトウェア、製品のアップデート、ライセンス、システムの負荷、ディスクの使用、システム時間、およびインターフェイスのステータスについての概要情報が提示されます。
- **[ASA Firepower Reporting]** : レポート作成のページには、Web カテゴリ、ユーザ、送信元、モジュールを通じてトラフィックが渡される宛先など、さまざまなモジュールの統計に対して上位 10 個のダッシュボードが提示されます。

[Home] ペイン (システム)

ASDM システムの [Home] ペインでは、ASA に関する重要なステータス情報を表示できます。ASDM システムの [Home] ペインに表示される詳細のほとんどは、ASDM の他の場所でも参照できますが、このペインでは ASA の動作状態を一目で確認できます。システムの [Home] ペインのステータス情報は 10 秒間隔で更新されます。

次の図に、システムの [Home] ペインの要素を示します。

図 7: システムの [Home] ペイン



凡例

GUI 要素	説明
1	システムとコンテキストの選択。
2	[Interface Status] ペイン。インターフェイスを通過するトラフィックの総数を表示するには、インターフェイスを選択します。
3	[Connection Status] ペイン。
4	[CPU Status] ペイン。
5	[Memory Status] ペイン。

ASDM 設定の定義

特定の ASDM 設定の動作を定義できます。

ASDM のさまざまな設定を変更するには、次の手順を実行します。

手順

ステップ 1 [Tools] > [Preferences] の順に選択します。

[General]、[Rules Table]、および [Syslog] の 3 つのタブのある [Preferences] ダイアログボックスが表示されます。

ステップ 2 設定を定義するには、これらのタブの 1 つをクリックします。[General] タブでは汎用プリファレンスを指定し、[Rules Table] タブでは [Rules] テーブルのプリファレンスを指定します。また、[Syslog] タブでは、[Home] ペインに表示される syslog メッセージの外観を指定したり、NetFlow 関連の syslog メッセージの警告メッセージの表示をイネーブルにしたりできます。

ステップ 3 [General] タブでは、次の項目を指定します。

- スタートアップコンフィギュレーションと実行コンフィギュレーションが同期していないときに通知されるようにする場合は、[Warn that configuration in ASDM is out of sync with the configuration in ASA] チェックボックスをオンにします。
- 起動時に read-only ユーザに対して次のメッセージを表示する場合は、[Show configuration restriction message to read-only user] チェックボックスをオンにします。このオプションは、デフォルトでオンです。

"You are not allowed to modify the ASA configuration, because you do not have sufficient privileges."

- スレーブユニットに接続されたユーザに設定制限メッセージを表示するには、[Show configuration restriction message on a slave unit in an ASA cluster] チェックボックスをオンにします。
- ASDM を閉じるときに終了を確認するプロンプトが表示されるようにするには、[Confirm before exiting from] チェックボックスをオンにします。このオプションは、デフォルトでオンです。
- スクリーンリーダーをイネーブルにするには、[Enable screen reader support (requires ASDM restart)] チェックボックスをオンにします。このオプションをイネーブルにするには、ASDM を再起動する必要があります。
- ASA メモリの最小空き容量が、ASDM アプリケーションの完全な機能を実行するには不十分である場合に通知を受信するには、[Warn of insufficient ASA memory when ASDM loads] チェックボックスをオンにします。ASDM は、起動時にテキスト バナー メッセージにメモリ警告を表示し、ASDM のタイトル バー テキストにメッセージを表示し、24 時間ごとに syslog アラートを送信します。

- [Communications] 領域で：
 - ASDM によって生成される CLI コマンドを表示するには、[Preview commands before sending them to the device] チェックボックスをオンにします。
 - ASA に複数のコマンドを 1 つのグループとして送信するには、[Enable cumulative (batch) CLI delivery] チェックボックスをオンにします。
 - [Minimum Configuration Sending Timeout] フィールドにタイムアウトメッセージの送信設定の最短時間を秒単位で入力します。デフォルトは 60 秒です。
- [Logging] 領域で：
 - Java ロギングを設定するには、[Enable logging to the ASDM Java console] チェックボックスをオンにします。
 - ドロップダウンリストから [Logging Level] を選択して、重大度を設定します。
- [Packet Capture Wizard] 領域で、キャプチャされたパケットを表示するには、[Network Sniffer Application] に名前を入力するか、[Browse] をクリックしてファイルシステムで検索します。

ステップ 4 [Rules Table] タブで、次の項目を指定します。

- [Display settings] では、[Rules] テーブルでのルールを表示方法を変更できます。
 - Auto-Expand Prefix 設定に基づいて自動展開されたネットワークおよびサービス オブジェクト グループを表示するには、[Auto-expand network and service object groups with specified prefix] チェックボックスをオンにします。
 - [Auto-Expand Prefix] フィールドに、表示するときに自動的に展開するネットワークおよびサービス オブジェクト グループのプレフィックスを入力します。
 - ネットワークおよびサービス オブジェクト グループのメンバーとそのグループ名を [Rules] テーブルに表示するには、[Show members of network and service object groups] チェックボックスをオンにします。チェックボックスがオフの場合は、グループ名だけが表示されます。
 - [Limit Members To] フィールドに、表示するネットワークおよびサービス オブジェクト グループの数を入力します。オブジェクト グループ メンバーが表示される際には、最初の n 個のメンバーだけが表示されます。
 - [Rules] テーブルにすべてのアクションを表示するには、[Show all actions for service policy rules] チェックボックスをオンにします。オフの場合は、サマリーが表示されません。
- [Deployment Settings] では、[Rules] テーブルに変更内容を適用するときの ASA の動作を設定できます。
 - 新しいアクセスリストを適用するときに NAT テーブルをクリアするには、[Issue “clear xlate” command when deploying access lists] チェックボックスをオンにします。この設

定により、ASA で設定されるアクセス リストが、すべての変換アドレスに対して確実に適用されるようにします。

- [Access Rule Hit Count Settings] では、[Access Rules] テーブルのヒット数をアップデートする頻度を設定できます。ヒット数は、明示的なルールにだけ適用されます。暗黙的なルールのヒット数は、[Access Rules] テーブルには表示されません。
 - [Access Rules] テーブルでヒット数が自動的にアップデートされるようにするには、[Update access rule hit counts automatically] チェックボックスをオンにします。
 - [Access Rules] テーブルに、ヒット数カラムを更新する頻度を秒単位で指定します。有効値の範囲は 10 ~ 86400 秒です。

ステップ 5 [Syslog] タブでは、次の項目を指定します。

- [Syslog Colors] 領域では、重大度レベルごとに背景色と前景色を設定し、メッセージ表示をカスタマイズできます。[Severity] カラムには、各重大度レベルが名前および番号ごとに表示されます。各重大度レベルでメッセージの背景色または前景色を変更するには、対応するカラムをクリックします。[Pick a Color] ダイアログボックスが表示されます。次のいずれかのタブをクリックします。
 - [Swatches] タブでパレットから色を選択し、[OK] をクリックします。
 - [HSB] タブで H、S、B の設定を指定し、[OK] をクリックします。
 - [RGB] タブで赤、緑、青の設定を指定し、[OK] をクリックします。
- 冗長な syslog メッセージをディセーブルにするよう警告するメッセージの表示をイネーブルにするには、[NetFlow] 領域で [Warn to disable redundant syslog messages when NetFlow action is first applied to the global service policy rule] チェックボックスをオンにします。

ステップ 6 これら 3 つのタブの設定を指定した後で、[OK] をクリックして設定を保存し、[Preferences] ダイアログボックスを閉じます。

- (注) プリファレンス設定をオンまたはオフにするたびに、変更内容は .conf ファイルに保存され、その時点でワークステーション上で実行中のその他の ASDM セッションから利用できるようになります。すべての変更を有効にするには、ASDM を再起動する必要があります。

ASDM Assistant での検索

ASDM Assistant ツールでは、タスクに応じた ASDM の使用方法のヘルプを検索し、表示できます。

情報にアクセスするには **[View] > [ASDM Assistant] > [How Do I?]** の順に選択するか、メニューバーの **[Look For]** フィールドから検索要求を入力します。 **[Find]** ドロップダウンリストから **[How Do I?]** を選択して検索を開始します。

ASDM Assistant を表示するには、次の手順を実行します。

手順

-
- ステップ 1** **[View] > [ASDM Assistant]** を選択します。
[ASDM Assistant] ペインが表示されます。
 - ステップ 2** **[Search]** フィールドに検索する情報を入力して **[Go]** をクリックします。
要求された情報が **[Search Results]** ペインに表示されます。
 - ステップ 3** **[Search Results]** セクションおよび **[Features]** セクションに表示される任意のリンクをクリックし、詳細情報を入手します。
-

履歴メトリックの有効化

[History Metrics] ペインでは、さまざまな統計情報の履歴を保存するように ASA を設定でき、ASDM を使用してそれをグラフやテーブルに表示できます。履歴メトリックをイネーブルにしない場合、監視できるのはリアルタイムの統計情報だけです。履歴メトリックをイネーブルにすると、直前の 10 分間、60 分間、12 時間、5 日間の統計グラフを表示できます。

履歴メトリックを設定するには、次の手順を実行します。

手順

-
- ステップ 1** **[Configuration] > [Device Management] > [Advanced] > [History Metrics]** を選択します。
[History Metrics] ペインが表示されます。
 - ステップ 2** **[ASDM History Metrics]** チェックボックスをオンにして履歴メトリックをイネーブルにし、**[Apply]** をクリックします。
-

サポートされていないコマンド

ASA で使用可能なコマンドはほとんどすべて ASDM でサポートされますが、既存のコンフィギュレーションのコマンドの一部は無視される場合があります。これらのコマンドのほとん

どはコンフィギュレーションに残すことができます。詳細については、[Tools]>[Show Commands Ignored by ASDM on Device] を参照してください。

無視される表示専用コマンド

次の表に、CLI 経由で追加された場合に ASDM のコンフィギュレーションでサポートされるが、ASDM で追加または編集できないコマンドの一覧を示します。ASDM で無視されるコマンドは ASDM の GUI に一切表示されません。表示専用コマンドは GUI に表示されますが、編集はできません。

表 6: サポートされていないコマンドの一覧

サポートされていないコマンド	ASDM の動作
capture	無視されます。
coredump	無視されます。これは、CLI を使用してのみ設定できます。
crypto engine large-mod-accel	無視されます。
dhcp-server (トンネルグループ名一般属性)	ASDM では、すべての DHCP サーバに対して 1 つの設定のみが許可されます。
eject	サポート対象外
established	無視されます。
failover timeout	無視されます。
fips	無視されます。
nat-assigned-to-public-ip	無視されます。
pager	無視されます。
pim accept-register route-map	無視されます。ASDM では [List] オプションだけ設定可。
service-policy global	match access-list クラスで使用されている場合は無視。次に例を示します。 <pre>access-list myacl extended permit ip any any class-map mycm match access-list myacl policy-map mypm class mycm inspect ftp service-policy mypm global</pre>
set metric	無視されます。

サポートされていないコマンド	ASDM の動作
<code>sysopt nodnsalias</code>	無視されます。
<code>sysopt uauth allow-http-cache</code>	無視されます。
<code>terminal</code>	無視されます。
<code>threat-detection rate</code>	無視されます。

サポートされていないコマンドの影響

既存の実行コンフィギュレーションを ASDM にロードした場合、そこにサポート対象外のコマンドがあっても、ASDM の操作には影響しません。サポート対象外のコマンドを表示するには、[Tools] > [Show Commands Ignored by ASDM on Device] を選択します。

サポート対象外の連続していないサブネットマスク

ASDM では、255.255.0.255 のように連続していないサブネットマスクはサポートされていません。たとえば、次は使用できません。

```
ip address inside 192.168.2.1 255.255.0.255
```

ASDM CLI ツールでサポートされていないインタラクティブ ユーザ コマンド

ASDM CLI ツールは、インタラクティブ ユーザ コマンドをサポートしていません。インタラクティブな確認を必要とする CLI コマンドを入力すると、「[yes/no]」の入力を要求するプロンプトが表示されますが、入力内容は認識されません。続いて ASDM は、応答の待機をタイムアウトします。

次に例を示します。

1. [Tools] > [Command Line Interface] を選択します。
2. `crypto key generate rsa` コマンドを入力します。
デフォルトの 1024 ビット RSA キーが生成されます。
3. `crypto key generate rsa` コマンドを再度入力します。
以前の RSA キーを上書きして再生成するのではなく、次のエラーが表示されます。

```
Do you really want to replace them? [yes/no]:WARNING: You already have
RSA ke00000000000000$A key
Input line must be less than 16 characters in length.
```

```
%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

回避策：

- [ASDM] ペインから、ユーザ介入が必要なほとんどのコマンドを設定できます。
- **noconfirm** オプションがある CLI コマンドについては、CLI コマンド入力時にこのオプションを使用します。次に例を示します。

```
crypto key generate rsa noconfirm
```




第 4 章

ライセンス：製品認証キーライセンス

ライセンスでは、特定の Cisco ASA 上でイネーブルにするオプションを指定します。このマニュアルでは、すべての物理 ASA の製品認証キー（PAK）のライセンスについて説明します。ASA v については、[ライセンス：スマートソフトウェアライセンス（ASA v、ASA on Firepower）](#)（169 ページ）を参照してください。

- [PAK ライセンスについて](#)（105 ページ）
- [PAK ライセンスのガイドライン](#)（120 ページ）
- [PAK ライセンスの設定](#)（122 ページ）
- [共有ライセンスの設定（AnyConnect 3 以前）](#)（127 ページ）
- [モデルごとにサポートされている機能のライセンス](#)（133 ページ）
- [PAK ライセンスのモニタリング](#)（154 ページ）
- [PAK ライセンスの履歴](#)（156 ページ）

PAK ライセンスについて

ライセンスでは、特定の ASA 上でイネーブルにするオプションを指定します。ライセンスは、160 ビット（32 ビットのワードが 5 個、または 20 バイト）値であるアクティベーションキーで表されます。この値は、シリアル番号（11 文字の文字列）とイネーブルになる機能とを符号化します。

事前インストール済みライセンス

デフォルトでは、ASA は、ライセンスがすでにインストールされた状態で出荷されます。このライセンスは、注文した内容およびベンダーがインストールした内容に応じて、ライセンスを追加できる基本ライセンスの場合と、すべてのライセンスがすでにインストールされている場合があります。

関連トピック

- [PAK ライセンスのモニタリング](#)（154 ページ）

永続ライセンス

永続アクティベーションキーを1つインストールできます。永続アクティベーションキーは、1つのキーにすべてのライセンス機能を格納しています。時間ベースライセンスもインストールすると、ASA は永続ライセンスと時間ベース ライセンスを1つの実行ライセンスに結合します。

関連トピック

[永続ライセンスと時間ベース ライセンスの結合](#) (107 ページ)

時間ベース ライセンス

永続ライセンスに加えて、時間ライセンスを購入したり、時間制限のある評価ライセンスを入手したりできます。たとえば、SSL VPN の同時ユーザの短期増加に対処するために時間ベースの AnyConnect Premium ライセンスを購入したり、1年間有効なボットネットトラフィックフィルタ時間ベース ライセンスを注文したりできます。



(注) ASA 5506-X および ASA 5506W-X は、時間ベース ライセンスをサポートしません。

時間ベース ライセンス有効化ガイドライン

- 複数の時間ベースライセンスをインストールし、同じ機能に複数のライセンスを組み込むことができます。ただし、一度にアクティブ化できる時間ベースライセンスは、1機能につき1つだけです。非アクティブのライセンスはインストールされたままで、使用可能な状態です。たとえば、1000セッション AnyConnect Premium ライセンスと2500セッション AnyConnect Premium ライセンスをインストールした場合、これらのライセンスのうちいずれか1つだけをアクティブにできます。
- キーの中に複数の機能を持つ評価ライセンスをアクティブにした場合、そこに含まれている機能のいずれかに対応する時間ベースライセンスを同時にアクティブ化することはできません。たとえば、評価ライセンスにボットネットトラフィックフィルタと1000セッション AnyConnect Premium ライセンスが含まれる場合、スタンドアロンの時間ベース2500セッション AnyConnect Premium ライセンスをこの評価ライセンスと同時にアクティブ化することはできません。

時間ベース ライセンス タイマーの動作

- 時間ベース ライセンスのタイマーは、ASA 上でライセンスをアクティブにした時点でカウントダウンを開始します。
- タイムアウト前に時間ベースライセンスの使用を中止すると、タイマーが停止します。時間ベースライセンスを再度アクティブ化すると、タイマーが再開します。
- 時間ベースライセンスがアクティブになっているときに ASA をシャットダウンすると、タイマーはカウントダウンを停止します。時間ベースライセンスでは、ASA が動作して

いる場合にのみカウントダウンします。システムクロック設定はライセンスに影響しません。つまり、ASA稼働時間ではライセンス継続期間に対してのみカウントします。

永続ライセンスと時間ベース ライセンスの結合

時間ベースライセンスをアクティブにすると、永続ライセンスと時間ベースライセンスに含まれる機能を組み合わせた実行ライセンスが作成されます。永続ライセンスと時間ベースライセンスの組み合わせ方は、ライセンスのタイプに依存します。次の表に、各機能ライセンスの組み合わせルールを示します。



- (注) 永続ライセンスが使用されていても、時間ベースライセンスがアクティブな場合はカウントダウンが続行されます。

表 7: 時間ベースライセンスの組み合わせルール

時間ベース機能	結合されたライセンスのルール
AnyConnect Premium セッション	時間ベースライセンスまたは永続ライセンスのうち、値の高い方が使用されます。たとえば、永続ライセンスが1000セッション、時間ベースライセンスが2500セッションの場合、2500セッションがイネーブルになります。通常は、永続ライセンスよりも機能の低い時間ベースライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。
Unified Communications Proxy セッション	時間ベースライセンスのセッションは、プラットフォームの制限数まで永続セッションに追加されます。たとえば、永続ライセンスが2500セッション、時間ベースライセンスが1000セッションの場合、時間ベースライセンスがアクティブである限り、3500セッションがイネーブルになります。
セキュリティ コンテキスト	時間ベースライセンスのコンテキストは、プラットフォームの制限数まで永続コンテキストに追加されます。たとえば、永続ライセンスが10コンテキスト、時間ベースライセンスが20コンテキストの場合、時間ベースライセンスがアクティブである限り、30コンテキストがイネーブルになります。

時間ベース機能	結合されたライセンスのルール
Botnet Traffic Filter	使用可能な永続ボットネットトラフィックフィルタライセンスはありません。時間ベースライセンスが使用されます。
その他	時間ベースライセンスまたは永続ライセンスのうち、値の高い方が使用されます。ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブルステータスのライセンスが使用されます。数値ティアを持つライセンスの場合、高い方の値が使用されます。通常は、永続ライセンスよりも機能の低い時間ベースライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。

関連トピック

[PAK ライセンスのモニタリング](#) (154 ページ)

時間ベース ライセンスのスタッキング

多くの場合、時間ベースライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベースライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベースライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。

すでにインストールされているのと同じ時間ベースライセンスをインストールすると、それらのライセンスは結合され、有効期間は両者を合わせた期間になります。

次に例を示します。

1. 52 週のボットネットトラフィックフィルタライセンスをインストールし、このライセンスを 25 週間使用します（残り 27 週）。
2. 次に、別の 52 週ボットネットトラフィックフィルタライセンスを購入します。2 つめのライセンスをインストールすると、ライセンスが結合され、有効期間は 79 週（52+27 週）になります。

同様の例を示します。

1. 8 週 1000 セッションの AnyConnect Premium ライセンスをインストールし、これを 2 週間使用します（残り 6 週）。

- 次に、別の 8 週 1000 セッションのライセンスをインストールすると、これらのライセンスは結合され、14 週 (8 + 6 週) 1000 セッションのライセンスになります。

これらのライセンスが同一でない場合 (たとえば、1000 セッション AnyConnect Premium ライセンスと 2500 セッション ライセンス)、これらのライセンスは結合されません。1 つの機能につき時間ベースライセンスを 1 つだけアクティブにできるので、ライセンスのうちいずれか 1 つだけをアクティブにすることができます。

同一でないライセンスは結合されませんが、現在のライセンスの有効期限が切れた場合、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。

関連トピック

[キーのアクティブ化または非アクティブ化](#) (125 ページ)

[時間ベース ライセンスの有効期限](#) (109 ページ)

時間ベース ライセンスの有効期限

機能に対応する現在のライセンスが期限切れになると、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。その機能に使用できる時間ベース ライセンスが他にない場合は、永続ライセンスが使用されます。

その機能に対して複数の時間ベース ライセンスを追加でインストールした場合、ASA は最初に検出されたライセンスを使用します。どのライセンスを使用するかは、ユーザが設定することはできず、内部動作に依存します。ASA がアクティブ化したライセンスとは別の時間ベースライセンスを使用するには、目的のライセンスを手動でアクティブにする必要があります。

たとえば、2500 セッションの時間ベース AnyConnect Premium ライセンス (アクティブ)、1000 セッションの時間ベース AnyConnect Premium ライセンス (非アクティブ)、500 セッションの永続 AnyConnect Premium ライセンスを所有しているとします。2500 セッション ライセンスの有効期限が切れた場合、ASA は 1000 セッション ライセンスを有効化します。1000 セッション ライセンスの有効期限が切れた後、ASA は 500 セッション永久ライセンスを使用します。

関連トピック

[キーのアクティブ化または非アクティブ化](#) (125 ページ)

ライセンスに関する注意事項

次の項で、ライセンスに関する追加情報について説明します。

AnyConnect Plus および Apex ライセンス

AnyConnect Plus および Apex ライセンスは、ライセンスが指定するユーザプールを共有するすべての複数の ASA に適用できる同時使用ライセンスです。<https://www.cisco.com/go/license> [英語] を参照し、各 ASA に個別に PAK を割り当てます。ASA に取得したアクティブセッションキーを適用すると、VPN 機能が最大許容数に切り替わりますが、ライセンスを共有するすべて

の ASA 上の実際の一意のユーザ数はライセンス限度を超えることはできません。詳細については、以下を参照してください。

- [『Cisco AnyConnect Ordering Guide』](#)
- [AnyConnect Licensing Frequently Asked Questions \(FAQ\)](#)

その他の VPN ライセンス

その他の VPN セッションには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN セッション、全タイプ

- VPN セッションの最大数の合計が、VPN AnyConnect とその他の VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、ASA をオーバーロードして、適切なネットワークのサイズに設定してください。
- クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアントセッションを開始した場合は、合計1つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロンクライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2つのセッションが使用されています。

VPN ロード バランシング

VPN ロード バランシングには、強力な暗号化（3DES/AES）ライセンスが必要です。

レガシー VPN ライセンス

ライセンスに関するすべての関連情報については、「[AnyConnect の補足エンド ユーザ ライセンス契約書（Supplemental end User License Agreement for AnyConnect）](#)」を参照してください。

暗号化ライセンス

DES ライセンスはディセーブルにできません。3DES ライセンスをインストールしている場合、DES は引き続き使用できます。強力な暗号化だけを使用したい場合に DES の使用を防止するには、強力な暗号化だけを使用するようにすべての関連コマンドを設定する必要があります。

合計 UC プロキシセッション

Encrypted Voice Inspection の各 TLS プロキシセッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシセッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy など）では、TLS 制限に対してカウントしません。

アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は 2 つ使用されます。

TLS プロキシの制限は、`tls-proxy maximum-sessions` コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、`tls-proxy maximum-sessions ?` コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのライセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。



(注) 「K8」で終わるライセンス製品番号（たとえばユーザ数が 250 未満のライセンス）では、TLS プロキシセッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザ数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

（たとえば `clear configure all` コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、`tls-proxy maximum-sessions` コマンドを使用したときに、再び制限を高めるようにエラーメッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、`write standby` コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で `clear configure all` コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合があります。

- K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
- K9 ライセンスでは、制限はありません。



- (注) メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

ボットネット トラフィック フィルタ ライセンス

ダイナミック データベースをダウンロードするには、強力な暗号化 (3DES/AES) ライセンスが必要です。

IPS モジュールのライセンス

IPS モジュール ライセンスがあると、ASA で IPS ソフトウェア モジュールを実行することができます。また、IPS 側の IPS シグニチャ サブスクリプションが必要です。

次のガイドラインを参照してください。

- IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です (製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります)。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。
- フェールオーバーについては、両方のユニットで IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスでないため、フェールオーバー時に共有されません。
- フェールオーバーについて、IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスター ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、フェールオーバーの装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。

AnyConnect Premium 共有ライセンス (AnyConnect 3 以前)



- (注) ASA の共有ライセンス機能は、AnyConnect 4 以降のライセンスではサポートされていません。AnyConnect ライセンスが共有されているため、共有サーバまたは参加ライセンスは不要になりました。

共有ライセンスを使用すると、多数の AnyConnect Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバとして、残りを共有ライセンス参加システムとして設定します。

フェールオーバーまたは ASA クラスタ ライセンス

いくつかの例外を除き、フェールオーバーおよびクラスタユニットは、各ユニット上で同一のライセンスを必要としません。以前のバージョンについては、お使いのバージョンに該当するライセンシング マニュアルを参照してください。

フェールオーバー ライセンスの要件および例外

フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5506-X および ASA 5506W-X	<ul style="list-style-type: none"> • アクティブ/スタンバイ：Security Plus ライセンス。 • アクティブ/アクティブ：サポートなし。 <p>(注) 各ユニットに同じ暗号化ライセンスが必要です。</p>

モデル	ライセンス要件
ASA 5512-X ~ ASA 5555-X	<ul style="list-style-type: none"> • ASA 5512 : Security Plus ライセンス。 • その他のモデル : 基本ライセンス。 <p>(注)</p> <ul style="list-style-type: none"> • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。 • 各ユニットに同じ IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。 <ul style="list-style-type: none"> • IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です (ASA5525-IPS-K9 のように、製品番号に「IPS」が含まれている必要があります)。IPS 以外の製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。 • 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。 • IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
ASAv	<p>ASAv のフェールオーバー ライセンス (176 ページ) を参照してください。</p>

モデル	ライセンス要件
Firepower 9300	Firepower 9300 シャーシの ASA のフェールオーバー ライセンス (176 ページ) を参照してください。
他のすべてのモデル	基本ライセンスまたは標準ライセンス。 (注) <ul style="list-style-type: none"> 各ユニットに同じ暗号化ライセンスが必要です。 マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。



- (注) 有効な永続キーが必要です。まれに、PAK 認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

ASA クラスタ ライセンスの要件および例外

クラスタ ユニットは、各ユニット上で同じライセンスを必要としません。一般的には、マスター ユニット用のライセンスのみを購入します。スレーブ ユニットはマスターのライセンスを継承します。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。

このルールには、例外があります。クラスタリングの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5585-X	クラスタ ライセンス、最大 16 ユニットのサポートします。 (注) 各ユニットに、同じ暗号化ライセンスが必要です。各ユニットに同じ 10 GE I/O/Security Plus ライセンスが必要です (ASA 5585-X と SSP-10 および SSP-20)。
ASA 5512-X	Security Plus ライセンス、2 ユニットのサポートします。 (注) 各ユニットに同じ暗号化ライセンスが必要です。
ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X	基本ライセンス、2 ユニットのサポートします。 (注) 各ユニットに同じ暗号化ライセンスが必要です。

モデル	ライセンス要件
Firepower 9300 シャーシ	Firepower 9300 シャーシ上の ASA の ASA クラスタ ライセンス (177 ページ) を参照してください。
他のすべてのモデル	サポートしない

フェールオーバーまたは ASA クラスタ ライセンスの結合方法

フェールオーバー ペアまたは ASA クラスタでは、各ユニットのライセンスが結合されて1つの実行クラスタライセンスとなります。ユニットごとに別のライセンスを購入した場合は、結合されたライセンスには次のルールが使用されます。

- 数値ティアを持つライセンスの場合は（セッション数など）、各ユニットのライセンスの値が合計されます。ただし、プラットフォームの制限を上限とします。使用されているライセンスがすべて時間ベースの場合は、ライセンスのカウンタダウンは同時に行われません。

たとえば、フェールオーバーの場合は次のようになります。

- 2つの ASA があり、それぞれに 10 個の TLS プロキシセッションが設定されている場合、ライセンスは結合され、合計で 20 個の TLS プロキシセッションになります。
- 1000 個の TLS プロキシセッションを設定した ASA 5545-X と、2000 個のセッションを設定した ASA 5545-X がある場合、プラットフォームの制限が 2000 であるため、結合されたライセンスでは 2000 個の TLS プロキシセッションを使用できます。
- 2つの ASA 5545-X ASA があり、一方は 20 コンテキスト、もう一方は 10 コンテキストである場合、結合されたライセンスでは 30 コンテキストを使用できます。アクティブ/アクティブ フェールオーバーの場合は、コンテキストが 2つのユニットに分配されます。たとえば、一方のユニットが 18 コンテキストを使用し、他方が 12 コンテキストを使用します（合計 30 の場合）。

たとえば、ASA クラスタリングの場合は次のようになります。

- デフォルトの 2 コンテキストの 2つの ASA 5516-X ASA があります。プラットフォームの制限が 5 であるため、結合されたライセンスでは最大 4 のコンテキストが許容されます。したがって、プライマリ ユニット上で最大 4 のコンテキストを設定できます。各セカンダリユニットも、コンフィギュレーションの複製経路で 4 のコンテキストを持つことになります。
- 4つの ASA 5516-X ASA があります。これは、それぞれが 5 コンテキストの 3つのユニットと、デフォルトの 2 コンテキストの 1つのユニットです。プラットフォームの制限が 5 であるため、ライセンスは合計で 5 コンテキストに結合されます。したがって、プライマリ ユニット上で最大 5 のコンテキストを設定できます。各セカンダリユニットも、コンフィギュレーションの複製経路で 5 のコンテキストを持つことになります。

- ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブルステータスのライセンスが使用されます。
- イネーブルまたはディセーブル状態（かつ数値ティアを持たない）の時間ベースライセンスの場合、有効期間はすべてのライセンスの期間の合計となります。最初にプライマリ/マスターユニットのライセンスがカウントダウンされ、期限切れになると、セカンダリ/スレーブユニットのライセンスのカウントダウンが開始し、以下も同様です。このルールは、アクティブ/アクティブフェールオーバーと ASA クラスタリングにも適用されます（すべてのユニットがアクティブに動作していても適用されます）。

たとえば、2つのユニットのボットネットトラフィックフィルタライセンスの有効期間が48週残っている場合は、結合された有効期間は96週です。

関連トピック

[PAK ライセンスのモニタリング](#) (154 ページ)

フェールオーバーまたは ASA クラスタ ユニット間の通信の途絶

ユニットの通信が途絶えてからの期間が30日を超えた場合は、各ユニットにはローカルにインストールされたライセンスが適用されます。30日の猶予期間中は、結合された実行ライセンスが引き続きすべてのユニットで使用されます。

30日間の猶予期間中に通信が復旧した場合は、時間ベースライセンスについては、経過した時間がプライマリ/マスターライセンスから差し引かれます。プライマリ/マスターライセンスが期限切れになるまでは、セカンダリ/スレーブライセンスのカウントダウンが開始することはありません。

30日間の期間が終了しても通信が復旧しなかった場合は、時間ベースライセンスについては、その時間がすべてのユニットのライセンスから差し引かれます（インストールされている場合）。これらはそれぞれ別のライセンスとして扱われ、ライセンスの結合によるメリットはありません。経過時間には30日の猶予期間も含まれます。

次に例を示します。

1. 52週のボットネットトラフィックフィルタライセンスが2つのユニットにインストールされています。結合された実行ライセンスでは、合計期間は104週になります。
2. これらのユニットが、1つのフェールオーバーユニット/ASA クラスタとして10週間動作すると、結合ライセンスの期間の残りは94週となります（プライマリ/マスターに42週、セカンダリ/スレーブに52週）。
3. ユニットの通信が途絶えた場合（たとえば、プライマリ/マスターユニットが停止した場合）は、セカンダリ/スレーブユニットは結合されたライセンスを引き続き使用し、94週からカウントダウンを続行します。
4. 時間ベースライセンスの動作は、通信がいつ復元されるかによって次のように異なります。
 - 30日以内：経過した時間がプライマリ/マスターユニットのライセンスから差し引かれます。この場合、通信は4週間後に復元されます。したがって、4週がプライマリ/

マスター ライセンスから差し引かれて、残りは合計 90 週となります（プライマリに 38 週、セカンダリに 52 週）。

- 30 日経過以降：経過時間が両方の装置から差し引かれます。この場合、通信は 6 週間後に復元されます。したがって、6 週がプライマリ/マスターとセカンダリ/スレーブの両方のライセンスから差し引かれて、残りは合計 84 週となります（プライマリ/マスターに 36 週、セカンダリ/スレーブに 46 週）。

フェールオーバー ペアのアップグレード

フェールオーバー ペアでは、両方の装置に同一のライセンスがインストールされている必要はないので、ダウンタイムなしに各装置に新しいライセンスを適用できます。リロードが必要な永続ライセンスを適用する場合、リロード中に他の装置へのフェールオーバーを実行できません。両方の装置でリロードが必要な場合は、各装置を個別にリロードするとダウンタイムは発生しません。

関連トピック

[キーのアクティブ化または非アクティブ化](#)（125 ページ）

ペイロード暗号化機能のないモデル

ペイロード暗号化機能のないモデルを購入することができます。輸出先の国によっては、Cisco ASA シリーズでペイロード暗号化をイネーブルにできません。ASA ソフトウェアは、ペイロード暗号化なしモデルを検出し、次の機能をディセーブルにします。

- ユニファイド コミュニケーション
- [VPN]

このモデルでも管理接続用に高度暗号化（3DES/AES）ライセンスをインストールできます。たとえば、ASDM HTTPS/SSL、SSHv2、Telnet、および SNMPv3 を使用できます。ポットネットトラフィック フィルタ（SSL を使用）用のダイナミック データベースをダウンロードすることもできます。

ライセンスを表示すると、VPN およびユニファイド コミュニケーションのライセンスはリストに示されません。

関連トピック

[PAK ライセンスのモニタリング](#)（154 ページ）

ライセンスの FAQ

AnyConnect Premium とポットネットトラフィック フィルタなど、複数の時間ベース ライセンスをアクティブにできますか。

はい。一度に使用できる時間ベース ライセンスは、1 機能につき 1 つです。

複数の時間ベースライセンスを「スタック」し、時間制限が切れると自動的に次のライセンスが使用されるようにできますか。

はい。ライセンスが同一の場合は、複数の時間ベースライセンスをインストールすると、時間制限が結合されます。ライセンスが同一でない場合（1000 セッション AnyConnect Premium ライセンスと 2500 セッション ライセンスなど）、ASA はその機能に対して検出された次の時間ベース ライセンスを自動的にアクティブにします。

アクティブな時間ベースライセンスを維持しながら、新しい永続ライセンスをインストールできますか。

はい。永続ライセンスをアクティブ化しても、時間ベースライセンスには影響しません。

フェールオーバーのプライマリ装置として共有ライセンスサーバを、セカンダリ装置として共有ライセンス バックアップ サーバを使用できますか。

いいえ。セカンダリ装置は、プライマリ装置と同じ実行ライセンスを使用します。共有ライセンス サーバには、サーバライセンスが必要です。バックアップ サーバには、参加ライセンスが必要です。バックアップサーバは、2つのバックアップサーバの別々のフェールオーバー ペアに配置できます。

フェールオーバーペアのセカンダリ装置用に、同じライセンスを購入する必要がありますか。

いいえ。バージョン 8.3(1) から、両方の装置に同一のライセンスをインストールする必要はなくなりました。一般的に、ライセンスはプライマリ装置で使用するために購入されます。セカンダリ装置は、アクティブになるとプライマリライセンスを継承します。セカンダリ装置に別のライセンスを持っている場合は（たとえば、8.3 よりも前のソフトウェアに一致するライセンスを購入した場合）、ライセンスは実行フェールオーバー クラスターライセンスに結合されます。ただし、モデルの制限が最大数になります。

AnyConnect Premium（共有）ライセンスに加えて、時間ベースまたは永続の AnyConnect Premium ライセンスを使用できますか。

はい。ローカルにインストールされたライセンス（時間ベースライセンスまたは永続ライセンス）のセッション数を使い果たした後、共有ライセンスが使用されます。



(注) 共有ライセンス サーバでは、永続 AnyConnect Premium ライセンスは使用されません。ただし、共有ライセンス サーバライセンスと同時に時間ベース ライセンスを使用することはできます。この場合、時間ベース ライセンスのセッションは、ローカルの AnyConnect Premium セッションにだけ使用できます。共有ライセンスプールに追加して参加システムで使用することはできません。

PAK ライセンスのガイドライン

コンテキスト モードのガイドライン

マルチ コンテキスト モードでシステム実行スペース内にアクティベーション キーを適用しません。

フェールオーバーのガイドライン

フェールオーバーまたは [ASA クラスタ ライセンス \(113 ページ\)](#) を参照してください。

モデルのガイドライン

- スマート ライセンスは、ASA_v でのみサポートされます。
- 共有ライセンスは、ASA_v、ASA 5506-X、ASA 5508-X および ASA 5516-X ではサポートされません。
- ASA 5506-X および ASA 5506W-X は、時間ベース ライセンスをサポートしません。

アップグレードとダウングレードのガイドライン

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーションキーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合：アップグレード後に、8.2 よりも前に導入された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、8.2 以降で導入された機能ライセンスをアクティブ化した場合は、アクティベーションキーの下位互換性がなくなります。互換性のないライセンスキーがある場合は、次のガイドラインを参照してください。
 - 以前のバージョンでアクティベーション キーを入力した場合は、ASA はそのキーを使用します（バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合）。
 - 新しいシステムで、以前のアクティベーションキーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。
- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、よりロバストな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
 - 複数の時間ベースのアクティベーションキーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。最後の時間ベース ライセンスが 8.3 で導入された機能に対応している場合、そのライセンスは旧バージョンでの使用はできなくて

も、アクティブ ライセンスのままです。永続キーまたは有効な時間ベース キーを再入力してください。

- フェールオーバーペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。
- 1つの時間ベース ライセンスをインストールしているが、それが 8.3 で導入された機能に対応している場合、ダウングレードの実行後、その時間ベース ライセンスはアクティブなままです。この時間ベース ライセンスをディセーブルにするには、永続キーを再入力する必要があります。

その他のガイドライン

- アクティベーション キーは、コンフィギュレーション ファイルには保存されません。隠しファイルとしてフラッシュ メモリに保存されます。
- アクティベーションキーは、デバイスのシリアル番号に関連付けられます。機能ライセンスは、デバイス間で転送できません（ハードウェア障害の発生時を除く）。ハードウェア障害が発生したためにデバイスを交換する必要があり、このことが Cisco TAC によってカバーされている場合は、シスコのライセンスチームに連絡して、既存のライセンスを新しいシリアル番号に転送するよう依頼してください。シスコのライセンスチームから、製品認証キーの参照番号と既存のシリアル番号を求められます。
- ライセンシングで使うシリアル番号は、([Activation Key] ページ内) で表示されるものです。このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。
- 購入後に、返金またはアップグレードしたライセンスのためにライセンスを返却できません。
- 1つのユニット上で、同じ機能の2つの別個のライセンスを加算することはできません。たとえば、25 セッション SSL VPN ライセンスを購入した後で 50 セッション ライセンスを購入しても、75 個のセッションを使用できるわけではなく、使用できるのは最大 50 個のセッションです。（アップグレード時に、数を増やしたライセンスを購入できることがあります。たとえば 25 セッションから 75 セッションへの増加です。このタイプのアップグレードは、2つのライセンスの加算とは別のものです）。
- すべてのライセンスタイプをアクティブ化できますが、機能によっては、機能どうしの組み合わせができないものがあります。AnyConnect Essentials ライセンスの場合、次のライセンスとは互換性がありません。AnyConnect Premium ライセンス、AnyConnect Premium (共有) ライセンス、および Advanced Endpoint Assessment ライセンス。デフォルトでは、AnyConnect Essentials ライセンスをインストールした場合（使用中のモデルで利用できる場合）、このライセンスが前述のライセンスの代わりに使用されます。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials] ペインを使用して、設定で AnyConnect Essentials ライセンスを無効にし、他のライセンスを使用できます。

PAK ライセンスの設定

この項では、アクティベーションキーを取得する方法とそれをアクティブ化する方法について説明します。また、キーを非アクティブ化することもできます。

ライセンスの PAK の注文とアクティベーション キーの取得

ASA にライセンスをインストールするには製品認証キーが必要です。その後、それを Cisco.com に登録してアクティベーションキーを取得することができます。次に、ASA のアクティベーションキーを入力できます。機能ライセンスごとに個別の製品認証キーが必要になります。PAK が組み合わせられて、1つのアクティベーションキーになります。デバイス発送時に、すべてのライセンス PAK が提供されている場合もあります。ASA には基本ライセンスまたは Security Plus ライセンスがプリインストールされ、ご使用資格を満たしている場合には Strong Encryption (3DES/AES) ライセンスも提供されます。無料の Strong Encryption ライセンスを手動でリクエストする必要がある場合は、<http://www.cisco.com/go/license> を参照してください。

始める前に

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

<https://software.cisco.com/#module/SmartLicensing>

まだアカウントをお持ちでない場合は、このリンクをクリックして[新しいアカウントをセットアップ](#)してください。Smart Software Manager では、組織のマスターアカウントを作成できます。

手順

ステップ 1 追加ライセンスを購入するには、<http://www.cisco.com/go/ccw> を参照してください。次の AnyConnect 発注ガイドおよび FAQ を参照してください。

- 『Cisco AnyConnect Ordering Guide』
- AnyConnect Licensing Frequently Asked Questions (FAQ)

ライセンスを購入した後、製品認証キー (PAK) が記載された電子メールを受け取ります。AnyConnect ライセンスの場合、ユーザセッションの同じプールを使用する複数の ASA に適用できるマルチユース PAK を受け取ります。場合によっては、PAK が記載された電子メールを受け取るまで数日かかることがあります。

ASA FirePOWER モジュールは、ASA とは別のライセンスメカニズムを使用します。詳しくは、ご使用のモデルの[クイックスタートガイド](#)を参照してください。

ステップ 2 [Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択して、ご使用の ASA のシリアル番号を取得します（マルチ コンテキスト モードでは、システム実行スペースにシリアル番号を表示します）。

ライセンスに使用されるシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。

ステップ 3 アクティベーション キーを取得するには、以下のライセンス Web サイトに移動します。

<http://www.cisco.com/go/license>

ステップ 4 プロンプトが表示されたら、次の情報を入力します。

- Product Authorization Key（キーが複数ある場合は、まず 1 つを入力します。キーごとに個別のプロセスとして入力する必要があります）
- ASA のシリアル番号
- 電子メールアドレス

アクティベーションキーが自動的に生成され、指定した電子メールアドレスに送信されます。このキーには、永続ライセンス用にそれまでに登録した機能がすべて含まれています。時間ベースライセンスの場合は、ライセンスごとに個別のアクティベーションキーがあります。

ステップ 5 さらに追加の製品認証キーがある場合は、製品認証キーごとにこの手順を繰り返します。すべての Product Authorization Key を入力した後、最後に送信されるアクティベーションキーには、登録した永続機能がすべて含まれています。

ステップ 6 キーのアクティブ化または非アクティブ化（125 ページ）に基づいて、アクティベーションキーをインストールします。

高度暗号化ライセンスの取得

ASDM（および他の多数の機能）を使用するには、高度暗号化（3DES/AES）ライセンスをインストールする必要があります。ASA に高度暗号化ライセンスがプリインストールされていない場合は、ライセンスを無料で入手できます。高度暗号化ライセンスに関するそれぞれ国の資格を満たす必要があります。

手順

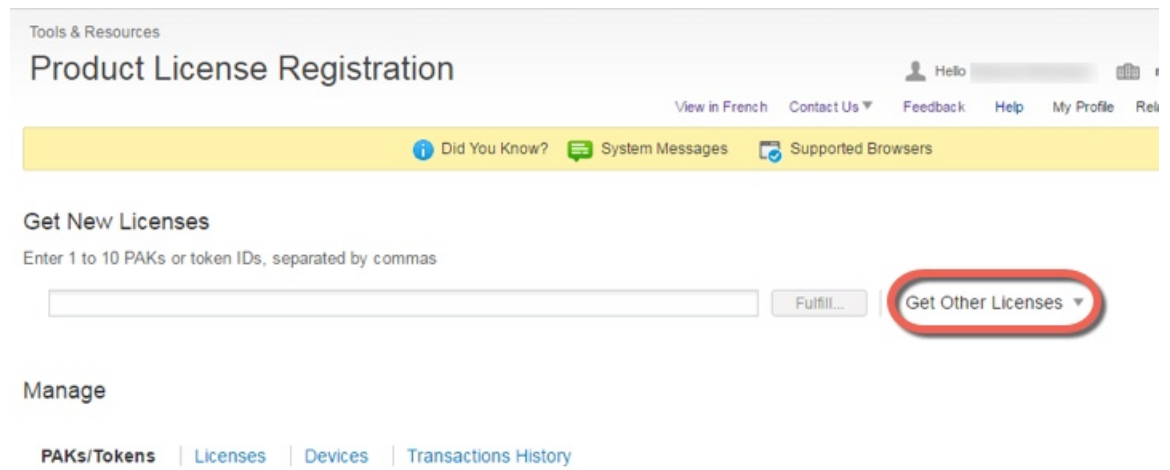
ステップ 1 次のコマンドを入力して、ASA のシリアル番号を取得します。

show version | grep Serial

このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。

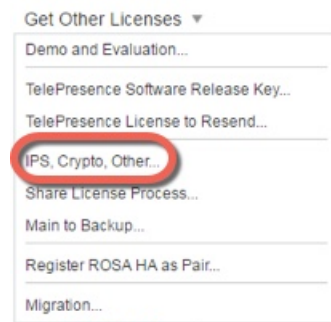
ステップ 2 <https://www.cisco.com/go/license> を参照し、[Get Other Licenses] をクリックしてください。

図 8: 他のライセンスの取得



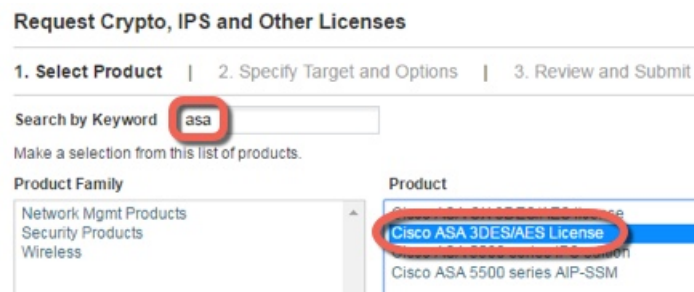
ステップ 3 [IPS, Crypto, Other] を選択します。

図 9: IPS、Crypto、その他



ステップ 4 [Search by Keyword] フィールドに **asa** と入力し、[Cisco ASA 3DES/AES License] を選択します。

図 10: Cisco ASA 3DES/AES ライセンス



ステップ 5 [Smart Acfcount]、[Virtual Account] を選択し、ASA の [Serial Number] を入力して、[Next] をクリックします。

図 11: スマート アカウント、バーチャルアカウント、シリアル番号

Request Crypto, IPS and Other Licenses

1. Select Product | 2. Specify Target and Options

Smart Account
Select one ...

Virtual Account
Select one... *Required with Smart Account*

Cisco ASA 3DES/AES License

Serial Number: FCH1714J6HP

ステップ 6 送信先の電子メールアドレスとエンドユーザ名は自動的に入力されます。必要に応じて追加の電子メールアドレスを入力します。[I Agree] チェックボックスをオンにして、[Submit] をクリックします。

図 12: 送信

Request Crypto, IPS and Other Licenses

1. Select Product | 2. Specify Target and Options | 3. Review and Submit

Recipient and Owner Information

Enter multiple email addresses separated by commas. Your License Key will be emailed within the hour to the specified email addresses.

Send To: Add...

End User: Edit..

License Request

Serial Number
FCH1714J6HP

Smart Account	SKU Name	Qty
▶ Cisco Internal	ASA5500-ENCR-K9	1

ステップ 7 その後、アクティベーションキーの記載された電子メールが届きますが、[Manage] > [Licenses] エリアからキーをすぐにダウンロードすることもできます。

ステップ 8 キーのアクティブ化または非アクティブ化 (125 ページ) に基づいて、アクティベーションキーを適用します。

キーのアクティブ化または非アクティブ化

この項では、新しいアクティベーションキーの入力と、時間ベース キーのアクティブ化および非アクティブ化の方法について説明します。

始める前に

- すでにマルチ コンテキスト モードに入っている場合は、システム実行スペースにこのアクティベーション キーを入力します。
- 一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。次の表に、リロードが必要なライセンスを示します。

表 8: 永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
すべてのモデル	暗号化ライセンスのダウングレード

手順

ステップ 1 [Configuration] > [Device Management] の順に選択し、モデルに応じて、[Licensing] > [Activation Key] または [Licensing Activation Key] ペインを選択します。

ステップ 2 永続または時間ベースの新しいアクティベーションキーを入力するには、[New Activation Key] フィールドで新しいアクティベーション キーを入力します。

キーは、5つの要素で構成される 16 進ストリングで、各要素は 1 つのスペースで区切られています。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。次に例を示します。

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

1 つの永続キーおよび複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。新しい時間ベース キーを入力した場合、デフォルトでアクティブになり、[Time-based License Keys Installed] テーブルに表示されます。特定の機能に対して最後にアクティブ化した時間ベース キーがアクティブになります。

ステップ 3 インストール済みの時間ベース キーをアクティブ化または非アクティブ化するには、そのキーを [Time-based License Keys Installed] テーブルで選択し、[Activate] または [Deactivate] をクリックします。

各機能でアクティブにできる時間ベース キーは 1 つのみです。

ステップ 4 [Update Activation Key] をクリックします。

永続ライセンスによっては、新しいアクティベーション キーの入力後に ASA をリロードする必要があります。必要な場合は、リロードするよう求められます。

関連トピック

[時間ベース ライセンス](#) (106 ページ)

共有ライセンスの設定 (AnyConnect 3 以前)



- (注) ASAの共有ライセンス機能は、AnyConnect4以降のライセンスではサポートされていません。AnyConnect ライセンスが共有されているため、共有サーバまたは参加ライセンスは不要になりました。

この項では、共有ライセンス サーバと参加システムを設定する方法について説明します。

共有ライセンスについて

共有ライセンスを使用すると、多数の AnyConnect Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバとして、残りを共有ライセンス参加システムとして設定します。

共有ライセンスのサーバと参加システムについて

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバを含む共有ライセンス参加者とするかを決定し、各デバイスシリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. (オプション) 別の ASA を共有ライセンス バックアップ サーバとして指定します。バックアップ サーバには 1 台のみ指定できます。



- (注) 共有ライセンス バックアップ サーバに必要なのは参加ライセンスのみです。

4. 共有ライセンスサーバ上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
5. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバに登録します。



- (注) 参加者は IP ネットワークを経由してサーバと通信する必要がありますが、同じサブネット上にある必要はありません。

6. 共有ライセンス サーバは、参加者がサーバにポーリングするべき頻度の情報で応答します。

7. 参加者がローカルライセンスのセッションを使い果たした場合、参加者は共有ライセンスサーバに 50 セッション単位で追加セッションの要求を送信します。
8. 共有ライセンスサーバは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。



(注) 共有ライセンスサーバは、共有ライセンスプールに参加することもできます。参加には参加ライセンスもサーバライセンスも必要ありません。

1. 参加者に対して共有ライセンスプールに十分なセッションがない場合、サーバは使用可能な限りのセッション数で応答します。
 2. 参加者はさらなるセッションを要求するリフレッシュメッセージの送信をサーバが要求に適切に対応できるまで続けます。
9. 参加者の負荷が減少した場合、参加者はサーバに共有セッションを解放するようにメッセージを送信します。



(注) ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

参加者とサーバ間の通信問題

参加者とサーバ間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔3倍の時間が経過した後で、サーバはセッションを解放して共有ライセンスプールに戻します。
- 参加者が更新を送信するためにライセンスサーバに到達できない場合、参加者はサーバから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24 時間を経過しても参加者がまだライセンスサーバと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバに再接続したが、サーバが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバは、参加者に再割り当てできる限りのセッション数で応答します。

共有ライセンス バックアップサーバについて

共有ライセンス バックアップサーバは、バックアップの役割を実行する前にメインの共有ライセンスサーバへの登録に成功している必要があります。登録時には、メインの共有ライセンスサーバは共有ライセンス情報に加えてサーバ設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メインサーバとバック

アップサーバは、10 秒間隔でデータを同期します。初回同期の後で、バックアップサーバはリロード後でもバックアップの役割を実行できます。

メインサーバがダウンすると、バックアップサーバがサーバ動作を引き継ぎます。バックアップサーバは継続して最大 30 日間動作できます。30 日を超えると、バックアップサーバは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メインサーバをこの 30 日間中に確実に復旧するようにします。クリティカルレベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メインサーバが復旧した場合、メインサーバはバックアップサーバと同期してから、サーバ動作を引き継ぎます。

バックアップサーバがアクティブでないときは、メインの共有ライセンスサーバの通常の参加者として動作します。



- (注) メインの共有ライセンスサーバの初回起動時には、バックアップサーバは独立して 5 日間のみ動作できます。動作制限は 30 日に到達するまで日ごとに増加します。また、メインサーバがその後短時間でもダウンした場合、バックアップサーバの動作制限は日ごとに減少します。メインサーバが復旧した場合、バックアップサーバは再び日ごとに増加を開始します。たとえば、メインサーバが 20 日間ダウンしていて、その期間中バックアップサーバがアクティブであった場合、バックアップサーバには、10 日間の制限のみが残っています。バックアップサーバは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

フェールオーバーと共有ライセンス

ここでは、共有ライセンスとフェールオーバーの相互作用について説明します。

フェールオーバーと共有ライセンス サーバ

この項では、メインサーバおよびバックアップサーバと、フェールオーバーとの相互作用について説明します。共有ライセンスサーバでは、VPN ゲートウェイやファイアウォールなど、ASA としての通常機能も実行されます。このため、メインとバックアップの共有ライセンスサーバにフェールオーバーを設定して、信頼性を高めることをお勧めします。



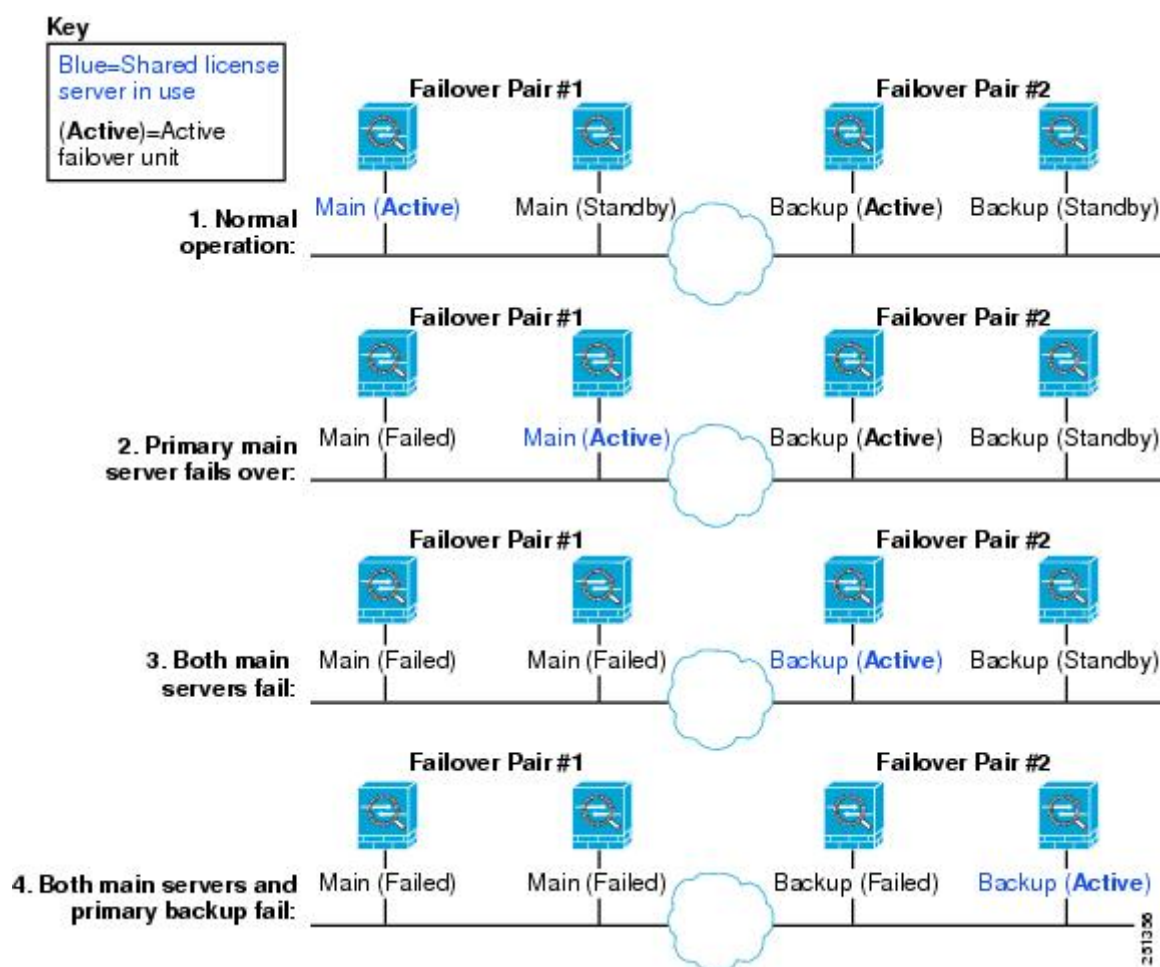
- (注) バックアップサーバメカニズムとフェールオーバーは異なりますが、両者には互換性があります。
- 共有ライセンスはシングルコンテキストモードでだけサポートされるため、アクティブ/アクティブフェールオーバーはサポートされません。

アクティブ/スタンバイフェールオーバーでは、プライマリ装置が主要な共有ライセンスサーバとして機能し、スタンバイ装置はフェールオーバー後に主要な共有ライセンスサーバとして

機能します。スタンバイ装置は、バックアップの共有ライセンスサーバとしては機能しません。必要に応じて、バックアップサーバとして機能する装置のペアを追加します。

たとえば、2組のフェールオーバーペアがあるネットワークを使用するとします。ペア #1にはメインのライセンスサーバが含まれます。ペア #2にはバックアップサーバが含まれます。ペア #1のプライマリ装置がダウンすると、ただちに、スタンバイ装置が新しくメインライセンスサーバになります。ペア #2のバックアップサーバが使用されることはありません。ペア #1の装置が両方ともダウンした場合だけ、ペア #2のバックアップサーバが共有ライセンスサーバとして使用されるようになります。ペア #1がダウンしたままで、ペア #2のプライマリ装置もダウンした場合は、ペア #2のスタンバイ装置が共有ライセンスサーバとして使用されるようになります（次の図を参照）。

図 13: フェールオーバーと共有ライセンスサーバ



スタンバイバックアップサーバは、プライマリバックアップサーバと同じ動作制限を共有します。スタンバイ装置がアクティブになると、その時点からプライマリ装置のカウントダウンを引き継ぎます。

関連トピック

[共有ライセンスバックアップサーバについて](#) (128 ページ)

フェールオーバーと共有ライセンス参加システム

参加システムのペアについては、両方の装置を共有ライセンスサーバに登録します。登録時には、個別の参加システム ID を使用します。アクティブ装置の参加システム ID は、スタンバイ装置と同期されます。スタンバイ装置は、アクティブに切り替わる時に、この ID を使用して転送要求を生成します。この転送要求によって、以前にアクティブだった装置から新しくアクティブになる装置に共有セッションが移動します。

参加者の最大数

ASA では、共有ライセンスの参加システム数に制限がありません。ただし、共有ネットワークの規模が非常に大きいと、ライセンスサーバのパフォーマンスに影響する場合があります。この場合は、参加システムのリフレッシュ間隔を長くするか、共有ネットワークを2つ作成することをお勧めします。

共有ライセンス サーバの設定

この項では、ASA を共有ライセンス サーバとして設定する方法について説明します。

始める前に

サーバが共有ライセンス サーバキーを持っている必要があります。

手順

- ステップ 1** [Configuration] > [Device Management] > [Licenses] > [Shared SSL VPN Licenses] ペインを選択します。
- ステップ 2** [Shared Secret] フィールドに、共有秘密を 4 ～ 128 ASCII 文字のストリングで入力します。
この秘密を持つすべての参加ユニットがライセンス サーバを使用できます。
- ステップ 3** (オプション) [TCP IP Port] フィールドに、サーバが参加ユニットからの SSL 接続を受信するポート (1 ～ 65535) を入力します。
デフォルトは、TCP ポート 50554 です。
- ステップ 4** (オプション) [Refresh interval] フィールドで、10 ～ 300 秒の更新間隔を入力します。
この値は、サーバと通信する頻度を設定するために参加ユニットに提供されます。デフォルトは 30 秒です。
- ステップ 5** [Interfaces that serve shared licenses] 領域で、[Shares Licenses] チェック ボックスをオンにします。パーティシパントからサーバへの通信には、このチェックボックスに対応するインターフェイスが使用されます。
- ステップ 6** (オプション) バックアップ サーバを指定するには、[Optional backup shared SSL VPN license server] 領域で次の手順を実行します。
 - a) [Backup server IP address] フィールドにバックアップ サーバの IP アドレスを入力します。

- b) [Primary backup server serial number] フィールドにバックアップサーバのシリアル番号を入力します。
- c) バックアップサーバがフェールオーバーペアの一部の場合は、[Secondary backup server serial number] フィールドでスタンバイユニットのシリアル番号を指定します。

1つのバックアップサーバとそのオプションのスタンバイユニットのみを指定できます。

ステップ7 [Apply] をクリックします。

共有ライセンス パーティシパントとオプションのバックアップサーバの設定

この項では、共有ライセンスサーバと通信する共有ライセンス参加システムを設定します。このセクションでは、オプションで参加者をバックアップサーバとして設定する方法も説明します。

始める前に

参加システムが共有ライセンス参加キーを持っている必要があります。

手順

ステップ1 [Configuration] > [Device Management] > [Licenses] > [Shared SSL VPN Licenses] ペインを選択します。

ステップ2 [Shared Secret] フィールドに、共有秘密を4～128 ASCII文字のストリングで入力します。

ステップ3 (任意) [TCP IP Port] フィールドに、SSLを使用してサーバと通信するポート(1～65535)を入力します。

デフォルトは、TCPポート50554です。

ステップ4 (任意) 参加ユニットをバックアップサーバとして指定するには、[Select backup role of participant] エリアで、次の手順を実行します。

- a) [Backup Server] オプション ボタンをクリックします。
- b) [Shares Licenses] チェックボックスをオンにします。パーティシパントからバックアップサーバへの通信には、このチェックボックスに対応するインターフェイスが使用されません。

ステップ5 [Apply] をクリックします。

モデルごとにサポートされている機能のライセンス

この項では、各モデルに使用できるライセンスと、ライセンスに関する特記事項について説明します。

モデルごとのライセンス

この項では、各モデルに使用できる機能のライセンスを示します。

イタリック体で示された項目は、基本ライセンス（または Security Plus など）ライセンスバージョンを置換できる個別のオプションライセンスです。オプションライセンスは、混在させることも統一することもできます。



(注) 一部の機能は互換性がありません。互換性情報については、個々の機能の章を参照してください。

ペイロード暗号化機能のないモデルの場合は、次に示す機能の一部がサポートされません。サポートされない機能のリストについては、[ペイロード暗号化機能のないモデル \(118 ページ\)](#)を参照してください。

ライセンスの詳細については、[ライセンスに関する注意事項 \(109 ページ\)](#)を参照してください。

ASA 5506-X および ASA 5506W-X のライセンス機能

次の表に、ASA 5506-X および ASA 5506W-X のライセンス機能を示します。

ライセン ス	基本ライセンス	Security Plus ライセンス
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし	サポートなし (注) ライセンス情報は、このライセンスが有効になっていることを示すことがあります。このライセンスがサポートされていないため、ディスプレイは無視するべきです。
ファイ ア ウォー ルの接 続、同 時	20,000	50,000

ライセンス	基本ライセンス		Security Plus ライセンス	
GIPGPRS	サポートなし		サポートなし	
合計 UC プロキシセッション	160		160	
VPN ライセンス				
AnyConnectピア	ディセーブル	オプションの AnyConnect Plus または Apex ライセンス : 最大 50	ディセーブル	オプションの AnyConnect Plus または Apex ライセンス : 最大 50
その他の VPN ピア	10		50	
合計 VPN ピア。全タイプの合計	50		50	
VPN ロードバランシング	サポートなし		サポートなし	
一般ライセンス				
暗号化	基本 (DES)	オプションライセンス : 強化 (3DES/AES)	基本 (DES)	オプションライセンス : 強化 (3DES/AES)
フェールオーバー	サポートなし		アクティブ/スタンバイ	
セキュリティコンテキスト	サポートなし		サポートなし	
クラスター	サポートなし		サポートなし	

ライセンス	基本ライセンス	Security Plus ライセンス
VLAN、最大	5	30

ASA 5506H-X ライセンスの各機能

次の表に、ASA 5506H-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし (注) ライセンス情報は、このライセンスが有効になっていることを示すことがあります。このライセンスがサポートされていないため、ディスプレイは無視すべきです。	
ファイアウォールの接続、同時	50,000	
GTP/GPRS	サポートなし	
合計 UC プロキシセッション	160	
VPN ライセンス		
AnyConnect Plus または Apex ライセンス (個別に購入)、最大プレミアムピア	50	
合計 VPN ピア。全タイプの合計	50	
その他の VPN ピア	50	
VPN ロードバランシング	イネーブル	
一般ライセンス		
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)

ライセンス	基本ライセンス
フェールオーバー	Active/Standby または Active/Active
セキュリティコンテキスト	サポートなし
クラスター	サポートなし
VLAN、最大	30

ASA 5508-X ライセンスの各機能

次の表に、ASA 5508-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし (注) ライセンス情報は、このライセンスが有効になっていることを示すことがあります。このライセンスがサポートされていないため、ディスプレイは無視すべきです。	
ファイアウォールの接続、同時	100,000	
GTP/GPRS	サポートなし	
合計 UC プロキシセッション	320	
VPN ライセンス		
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス : 最大 100
合計 VPN ピア。全タイプの合計	100	
その他の VPN ピア	100	
VPN ロードバランシング	イネーブル	
一般ライセンス		

ライセンス	基本ライセンス		
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)	
フェールオーバー	Active/Standby または Active/Active		
セキュリティコンテキスト	2	オプション ライセンス :	5
クラスタ	サポートなし		
VLAN、最大	50		

ASA 5512-X ライセンスの機能

次の表に、ASA 5512-X のライセンス機能を示します。

ライセン ス	基本ライセンス					Security Plus ライセンス						
ファイアウォール ライセンス												
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセン ス : 使用可能				ディセーブル	オプションの時間ベース ライセン ス : 使用可能					
ファイ ア ウォ ールの接 続、同 時	100,000					250,000						
GIP/GPRS	サポートなし					サポートなし						
合計 UC プ ロキシ セッ ション	2	オプション ライセンス :				2	オプション ライセンス :					
		24	50	100	250	500		24	50	100	250	500
VPN ライセンス												
AnyConnect ピア	ディセーブル	オプションの AnyConnect Plus また は Apex ライセンス : 最大 250				ディセーブル	オプションの AnyConnect Plus また は Apex ライセンス : 最大 250					

ライセンス	基本ライセンス		Security Plus ライセンス	
その他の VPN ピア	250		250	
合計 VPN ピア。全タイプの合計	250		250	
VPN ロード バランシング	サポートなし		イネーブル	
一般ライセンス				
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)
フェールオーバー	サポートなし		Active/Standby または Active/Active	
セキュリティ コンテキスト	サポートなし		2	オプション ライセンス : 5
クラス タ	サポートなし		2	
IPS モジュール	ディセーブル	オプション ライセンス : 使用可能	ディセーブル	オプション ライセンス : 使用可能
VLAN、最大	50		100	

ASA 5515-X ライセンスの機能

次の表に、ASA 5515-X のライセンス機能を示します。

ライセンス	基本ライセンス						
ファイアウォール ライセンス							
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス : 使用可能					
ファイアウォールの接続、同時	250,000						
GIP/GPRS	サポートなし						
合計 UC プロキシセッション	2	オプション ライセンス :	24	50	100	250	500
VPN ライセンス							
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス : 最大 250					
その他の VPN ピア	250						
合計 VPN ピア。全タイプの合計	250						
VPN ロードバランシング	イネーブル						
一般ライセンス							
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)					

ライセンス	基本ライセンス		
フェールオーバー	Active/Standby または Active/Active		
セキュリティコンテキスト	2	オプション ライセンス :	5
クラスタ	2		
IPS モジュール	ディセーブル	オプション ライセンス : 使用可能	
VLAN、最大	100		

ASA 5516-X ライセンスの機能

次の表に、ASA 5516-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし (注) ライセンス情報は、このライセンスが有効になっていることを示すことがあります。このライセンスがサポートされていないため、ディスプレイは無視する必要があります。	
ファイアウォールの接続、同時	250,000	
GTP/GPRS	サポートなし	
合計 UC プロキシセッション	1000	
VPN ライセンス		
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス : 最大 300

ライセンス	基本ライセンス		
その他の VPN ピア	300		
合計 VPN ピア。全タイプの合計	300		
VPN ロード バランシング	イネーブル		
一般ライセンス			
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)	
フェールオーバー	Active/Standby または Active/Active		
セキュリティ コンテキスト	2	オプション ライセンス :	5
クラスタ	サポートなし		
VLAN、最大	150		

ASA 5525-X ライセンスの各機能

次の表に、ASA 5525-X のライセンス機能を示します。

ライセンス	基本ライセンス		
ファイアウォール ライセンス			
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス : 使用可能	
ファイアウォールの接続、同時	500,000		
GIP/GPRS	ディセーブル	オプション ライセンス : 使用可能	

ライセンス	基本ライセンス								
合計 UC プロキシセッション	2	オプションライセンス :	24	50	100	250	500	750	1000
VPN ライセンス									
AnyConnectピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス : 最大 750							
その他の VPN ピア	750								
合計 VPN ピア。全タイプの合計	750								
VPN ロードバランシング	イネーブル								
一般ライセンス									
暗号化	基本 (DES)	オプションライセンス : 強化 (3DES/AES)							
フェールオーバー	Active/Standby または Active/Active								
セキュリティコンテキスト	2	オプションライセンス :	5	10	20				
クラスタ	2								
IPS モジュール	ディセーブル	オプションライセンス : 使用可能							

ライセンス	基本ライセンス
VLAN、 最大	200

ASA 5545-X ライセンスの機能

次の表に、ASA 5545-X のライセンス機能を示します。

ライセンス	基本ライセンス									
ファイアウォール ライセンス										
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス : 使用可能								
ファイ ア ウォ ールの接 続、同 時	750,000									
GIG/GPRS	ディセーブル	オプション ライセンス : 使用可能								
合計 UC プ ロキシ セッ ション	2	オプション ライセンス :	24	50	100	250	500	750	1000	2000
VPN ライセンス										
AnyConnect ピア	ディセーブル	オプションの AnyConnect Plus または Apex ライセンス : 最大 2500								
その他 の VPN ピア	2500									
合計 VPN ピ ア。全 タイプ の合計	2500									

ライセンス	基本ライセンス					
VPN ロード バラン シング	イネーブル					
一般ライセンス						
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)				
フェー ルオー バー	Active/Standby または Active/Active					
セキュ リティ コンテ キスト	2	オプション ライセンス :	5	10	20	50
クラス タ	2					
IPS モ ジュー ル	ディセーブル	オプション ライセンス : 使用可能				
VLAN、 最大	300					

ASA 5555-X ライセンスの機能

次の表に、ASA 5555-X のライセンス機能を示します。

ライセ ンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス : 使用可能

ライセンス	基本ライセンス									
ファイアウォールの接続、同時	1,000,000									
GIP/GPRS	ディセーブル	オプションライセンス：使用可能								
合計 UC プロキシセッション	2	オプションライセンス：								
		24	50	100	250	500	750	1000	2000	3000
VPN ライセンス										
AnyConnectピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 5000								
その他の VPN ピア	5000									
合計 VPN ピア。全タイプの合計	5000									
VPN ロードバランシング	イネーブル									
一般ライセンス										
暗号化	基本 (DES)	オプションライセンス：強化 (3DES/AES)								
フェールオーバー	Active/Standby または Active/Active									

ライセンス	基本ライセンス						
セキュリティコンテキスト	2	オプション ライセンス :	5	10	20	50	100
クラスター	2						
IPS モジュール	ディセーブル	オプション ライセンス : 使用可能					
VLAN、最大	500						

ASA 5585-X (SSP-10) ライセンスの各機能

次の表に、ASA 5585-X (SSP-10) のライセンス機能を示します。

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません (たとえば、SSP-10 と SSP-20 の組み合わせはサポートされていません)。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。

ライセンス	基本ライセンスと Security Plus ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス : 使用可能
ファイアウォールの接続、同時	1,000,000	
GIPGPRS	ディセーブル	オプション ライセンス : 使用可能

ライセンス	基本ライセンスと Security Plus ライセンス								
合計 UC プ ロキシ セッ ション	2	オプション ライセンス :							
		24	50	100	250	500	750	1000	2000
VPN ライセンス									
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス : 最大 5000							
その他 の VPN ピア	5000								
合計 VPN ピ ア。全 タイプ の合計	5000								
VPN ロード バラ ン シ ン グ	イネーブル								
一般ライセンス									
10 GE I/O	基本ライセンス : ディセーブル。ファイバ ifcs は 1 GE で動作します					Security Plus ライセンス : イネーブル。ファイバ ifcs は 10 GE で動作します			
暗号化	基本 (DES)		オプション ライセンス : 強化 (3DES/AES)						
フェー ルオー バー	Active/Standby または Active/Active								
セキュ リティ コンテ キスト	2	オプション ライセンス :			5	10	20	50	100
クラス タ	ディセーブル	オプション ライセンス: 16 単位で利用可能							

ライセンス	基本ライセンスと Security Plus ライセンス
VLAN、 最大	1024

ASA 5585-X (SSP-20) ライセンスの機能

次の表に、ASA 5585-X (SSP-20) のライセンス機能を示します。

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-20 と SSP-40 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。



(注) 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシセッションの最大数は 5000 です。

ライセンス	基本ライセンスと Security Plus ライセンス											
ファイアウォール ライセンス												
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能										
ファイ ア ウォー ルの接 続、同 時	2,000,000											
GIPGPRS	ディセーブル	オプション ライセンス：使用可能										
合計 UC プ ロキシ セッ ション	2	オプション ライセンス：										
		24	50	100	250	500	750	1000	2000	3000	5000	10,000
VPN ライセンス												
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 10,000										

ライセンス	基本ライセンスと Security Plus ライセンス								
その他の VPN ピア	10,000								
合計 VPN ピア。全タイプの合計	10,000								
VPN ロード バランシング	イネーブル								
一般ライセンス									
10 GE I/O	基本ライセンス：ディセーブル。ファイバ ifcs は 1 GE で動作します				Security Plus ライセンス：イネーブル。ファイバ ifcs は 10 GE で動作します				
暗号化	基本 (DES)		オプション ライセンス：強化 (3DES/AES)						
フェールオーバー	Active/Standby または Active/Active								
セキュリティ コンテキスト	2	オプション ライセンス：		5	10	20	50	100	250
クラス タ	ディセーブル		オプション ライセンス: 16 単位で利用可能						
VLAN、最大	1024								

ASA 5585-X (SSP-40 および -60) ライセンスの機能

次の表に、ASA 5585-X (SSP-40 および -60) のライセンス機能を示します。

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません (たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません)。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。



(注) 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシセッションの最大数は 5000 です。

ライセンス	基本ライセンス											
ファイアウォール ライセンス												
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス : 使用可能										
ファイアウォールの接続、同時	5585-X (SSP-40) : 4,000,000						5585-X (SSP-60) : 10,000,000					
GIPGPRS	ディセーブル	オプション ライセンス : 使用可能										
合計 UC プロキシセッション	2	オプション ライセンス :										
		24	50	100	250	500	750	1000	2000	3000	5000	10,000
VPN ライセンス												
AnyConnectピア	ディセーブル	オプションの AnyConnect Plus または Apex ライセンス : 最大 10,000										
その他の VPN ピア	10,000											
合計 VPN ピア。全タイプの合計	10,000											
VPN ロードバランシング	イネーブル											

ライセンス	基本ライセンス							
一般ライセンス								
10 GE I/O	イネーブル。ファイバインターフェイスは 10 GE で動作							
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)						
フェールオーバー	Active/Standby または Active/Active							
セキュリティコンテキスト	2	オプション ライセンス :	5	10	20	50	100	250
クラスタ	ディセーブル	オプション ライセンス: 16 単位で利用可能						
VLAN、最大	1024							

ASASM ライセンスの機能

次の表に、ASA サービス モジュールのライセンス機能を示します。



(注) 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシセッションの最大数は 5000 です。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス : 使用可能

ライセンス	基本ライセンス											
ファイアウォールの接続、同時	10,000,000											
GIPGPRS	ディセーブル	オプションライセンス：使用可能										
合計 UC プロキシセッション	2	オプションライセンス：										
	24	50	100	250	500	750	1000	2000	3000	5000	10,000	
VPN ライセンス												
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 10,000										
その他の VPN ピア	10,000											
合計 VPN ピア。全タイプの合計	10,000											
VPN ロードバランシング	イネーブル											
一般ライセンス												
暗号化	基本 (DES)	オプションライセンス：強化 (3DES/AES)										
フェールオーバー	Active/Standby または Active/Active											

ライセンス	基本ライセンス					
セキュリティ コンテ キスト	2	オプション ライセンス :				
	5	10	20	50	100	250
クラス タ	サポートなし					
VLAN、 最大	1000					

ISA 3000 ライセンスの各機能

次の表に、ISA 3000 のライセンス機能を示します。

ライセ ンス	基本ライセンス	Security Plus ライセンス
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし	サポートなし
ファイ ア ウォ ールの接 続、同 時	20,000	50,000
GiPGPRS	サポートなし	サポートなし
合計 UC プ ロキシ セッ ション	160	160
VPN ライセンス		
AnyConnect ピア	ディセーブル オプションの AnyConnect Plus また は Apex ライセンス : 最大 25	ディセーブル オプションの AnyConnect Plus また は Apex ライセンス : 最大 25

ライセンス	基本ライセンス	Security Plus ライセンス
その他の VPN ピア	10	50
合計 VPN ピア。全タイプの合計	25	50
VPN ロード バランシング	サポートなし	サポートなし
一般ライセンス		
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)
フェールオーバー	サポートなし	アクティブ/スタンバイ
セキュリティ コンテキスト	サポートなし	サポートなし
クラス タ	サポートなし	サポートなし
VLAN、最大	5	25

PAK ライセンスのモニタリング

この項では、ライセンス情報の表示方法について説明します。

現在のライセンスの表示

この項では、現在のライセンスと、時間ベース アクティベーション キーの残り時間を表示する方法について説明します。

始める前に

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN および Unified Communications ライセンスは一覧に示されません。詳細については、「[ペイロード暗号化機能のないモデル \(118 ページ\)](#)」を参照してください。

手順

ステップ 1 (永続ライセンスとアクティブな時間ベースライセンスの組み合わせである) 実行ライセンスを表示するには、**[Configuration] > [Device Management] > [Licensing] > [Activation Key]** ペインを選択します。

マルチ コンテキスト モードでは、**[Configuration] > [Device Management] > [Activation Key]** ペインを選択し、システム実行スペースでアクティベーション キーを表示します。

フェールオーバーペアの場合、表示される実行ライセンスは、プライマリ装置とセカンダリ装置からの結合されたライセンスです。詳細については、「[フェールオーバーまたは ASA クラスタライセンスの結合方法 \(116 ページ\)](#)」を参照してください。数値が割り当てられた時間ベースライセンス (期間は結合されません) の場合、**[License Duration]** カラムには、プライマリ装置またはセカンダリ装置からの最短の時間ベースライセンスが表示されます。このライセンスの有効期限が切れると他の装置のライセンスの期間が表示されます。

ステップ 2 (任意) 時間ベースライセンスの詳細 (ライセンスに含まれる機能やライセンス期間など) を **[Time-Based License Keys Installed]** 領域に表示するには、ライセンス キーを選択し、**[Show License Details]** をクリックします。

ステップ 3 (任意) フェールオーバーユニットで、そのユニットにインストールされている (プライマリ装置とセカンダリ装置からの結合ライセンスではない) ライセンスを **[Running Licenses]** 領域に表示するには、**[Show information of license specifically purchased for this device alone]** をクリックします。

共有ライセンスのモニタリング

共有ライセンスをモニタするには、**[Monitoring] > [VPN] > [Clientless SSL VPN] > [Shared Licenses]** を選択して。

PAK ライセンスの履歴

機能名	プラットフォーム リリース	説明
接続数と VLAN 数の増加	7.0(5)	次の制限値が増加されました。 <ul style="list-style-type: none"> • ASA5510 Base ライセンス接続は 32000 から 5000 に、VLAN は 0 から 10 に増加。 • ASA5510 Security Plus ライセンス接続は 64000 から 130000 に、VLAN は 10 から 25 に増加。 • ASA5520 接続は 130000 から 280000 に、VLAN は 25 から 100 に増加。 • ASA5540 接続は 280000 から 400000 に、VLAN は 100 から 200 に増加。
SSL VPN ライセンス	7.1(1)	SSL VPN ライセンスが導入されました。
SSL VPN ライセンスの追加	7.2(1)	5000 ユーザの SSL VPN ライセンスが ASA 5550 以降に対して導入されました。
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。

機能名	プラットフォーム リリース	説明
VLAN 数の増加	7.2(2)	<p>ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5 (3つのフル機能インターフェイス、1つのフェールオーバーインターフェイス、1つのバックアップインターフェイスに制限されるインターフェイス) から 20のフル機能インターフェイスに増加されました。また、トランクポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために <code>backup interface</code> コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。<code>backup interface</code> コマンドは、これまでどおり Easy VPN 設定用に使用できます。</p> <p>VLAN の制限値も変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。</p>
ASA 5510 Security Plus ライセンスに対するギガビットイーサネットサポート	7.2(3)	<p>ASA 5510 は、Security Plus ライセンスを使用する Ethernet 0/0 および 0/1 ポート用にギガビットイーサネット (1000 Mbps) をサポートしています。基本ライセンスでは、これらのポートは引き続きファストイーサネット (100 Mbps) ポートとして使用されます。いずれのライセンスに対しても、Ethernet 0/2、0/3、および 0/4 はファストイーサネットポートのままです。</p> <p>(注) インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。</p>

機能名	プラットフォーム リリース	説明
Advanced Endpoint Assessment ライセンス	8.0(2)	<p>Advanced Endpoint Assessment ライセンスが導入されました。Cisco AnyConnect またはクライアントレス SSL VPN 接続の条件としてリモートコンピュータでスキャン対象となる、アンチウイルスアプリケーションやアンチスパイウェアアプリケーション、ファイアウォール、オペレーティングシステム、および関連アップデートの種類が、大幅に拡張されました。また、任意のレジストリ エントリ、ファイル名、およびプロセス名を指定してスキャン対象にすることもできます。スキャン結果を ASA に送信します。ASA は、ユーザ ログイン クレデンシャルとコンピュータ スキャン結果の両方を使用して、ダイナミック アクセス ポリシー (DAP) を割り当てます。</p> <p>Advanced Endpoint Assessment ライセンスを使用すると、バージョン要件を満たすように非標準拠コンピュータのアップデートを試行する機能を設定して、Host Scan を拡張できます。</p> <p>シスコは、Host Scan でサポートされるアプリケーションとバージョンの一覧に、Cisco Secure Desktop とは異なるパッケージで、タイムリーなアップデートを提供できます。</p>
ASA 5510 の VPN ロード バランシング	8.0(2)	VPN ロード バランシングが ASA 5510 Security Plus ライセンスでサポートされるようになりました。
AnyConnect for Mobile ライセンス	8.0(3)	AnyConnect for Mobile ライセンスが導入されました。これにより、Windows モバイル デバイスは AnyConnect クライアントを使用して、ASA に接続できます。
時間ベース ライセンス	8.0(4)/8.1(2)	時間ベースライセンスがサポートされるようになりました。

機能名	プラットフォーム リリース	説明
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
Unified Communications Proxy セッション ライセンス	8.0(4)	<p>UC Proxy セッション ライセンスが導入されました。電話プロキシ、Presence Federation Proxy、および Encrypted Voice Inspection アプリケーションでは、それらの接続に TLS プロキシセッションが使用されます。各 TLS プロキシセッションは、UC ライセンスの制限に対してカウントされます。これらのアプリケーションは、すべて UC Proxy として包括的にライセンスされるので、混在させたり、組み合わせたりできます。</p> <p>この機能は、バージョン 8.1 では使用できません。</p>
ボットネット トラフィック フィルタ ライセンス	8.2(1)	ボットネット トラフィック フィルタ ライセンスが導入されました。ボットネット トラフィック フィルタでは、既知の不正なドメインや IP アドレスに対する接続を追跡して、マルウェア ネットワーク アクティビティから保護します。

機能名	プラットフォーム リリース	説明
AnyConnect Essentials ライセンス	8.2(1)	

機能名	プラットフォーム リリース	説明
		<p>AnyConnect Essentials ライセンスが導入されました。このライセンスにより、AnyConnect VPN クライアントは ASA にアクセスできるようになります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。</p> <p>(注) AnyConnect Essentials ライセンスを所有する VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントをダウンロードおよび起動 (WebLaunch) することができます。</p> <p>このライセンスと AnyConnect Premium ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアントソフトウェアには同じクライアント機能のセットが装備されています。</p> <p>特定の ASA では、AnyConnect Premium ライセンス (全タイプ) または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。</p> <p>デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials] ペインを使用すると、AnyConnect Essentials ライセンスを無効にして他のライセンスを使</p>

機能名	プラットフォーム リリース	説明
		用できます。
SSL VPN ライセンスの AnyConnect Premium SSL VPN Edition ライセンスへの変更	8.2(1)	SSL VPN ライセンスの名前が AnyConnect Premium SSL VPN Edition ライセンスに変更されました。
SSL VPN の共有ライセンス	8.2(1)	SSL VPN の共有ライセンスが導入されました。複数の ASA で、SSL VPN セッションのプールを必要に応じて共有できます。
モビリティ プロキシ アプリケーションでの Unified Communications Proxy ライセンス不要化	8.2(2)	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。
ASA 5585-X (SSP-20) 用 10 GE I/O ライセンス	8.2(3)	ASA 5585-X (SSP-20) の 10 GE I/O ライセンスを導入し、ファイバポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-60 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 (注) ASA 5585-X は 8.3(x) ではサポートされていません。
ASA 5585-X (SSP-10) 用 10 GE I/O ライセンス	8.2(4)	ASA 5585-X (SSP-10) の 10 GE I/O ライセンスを導入し、ファイバポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-40 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 (注) ASA 5585-X は 8.3(x) ではサポートされていません。
同一でないフェールオーバー ライセンス	8.3(1)	フェールオーバー ライセンスが各ユニット上で同一である必要なくなりました。両方のユニットで使用するライセンスは、プライマリユニットおよびセカンダリユニットからの結合されたライセンスです。 次の画面が変更されました。 [Configuration] > [Device Management] > [Licensing] > [Activation Key]。

機能名	プラットフォーム リリース	説明
スタック可能な時間ベースライセンス	8.3(1)	時間ベースライセンスがスタック可能になりました。多くの場合、時間ベースライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベースライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベースライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。
Intercompany Media Engine ライセンス	8.3(1)	IME ライセンスが導入されました。
複数の時間ベースライセンスの同時アクティブ化	8.3(1)	時間ベースライセンスを複数インストールできるようになり、同時に機能ごとに1つのアクティブなライセンスを保持できるようになりました。 次の画面が変更されました。 [Configuration] > [Device Management] > [Licensing] > [Activation Key]。
時間ベースライセンスのアクティブ化と非アクティブ化の個別化	8.3(1)	コマンドを使用して、時間ベースライセンスをアクティブ化または非アクティブ化できるようになりました。 次の画面が変更されました。 [Configuration] > [Device Management] > [Licensing] > [Activation Key]。
AnyConnect Premium SSL VPN Edition ライセンスの AnyConnect Premium SSL VPN ライセンスへの変更	8.3(1)	AnyConnect Premium SSL VPN Edition ライセンスの名前が AnyConnect Premium SSL VPN ライセンスに変更されました。

機能名	プラットフォーム リリース	説明
輸出用のペイロード暗号化なしイメージ	8.3(2)	<p>ASA 5505 ～ 5550 にペイロード暗号化機能のないソフトウェアをインストールした場合、Unified Communications、強力な暗号化VPN、強力な暗号化管理プロトコルをディセーブルにします。</p> <p>(注) この特殊なイメージは 8.3(x) でのみサポートされます。 8.4(1) 以降で暗号化機能のないソフトウェアをサポートするには、ASA の特別なハードウェア バージョンを購入する必要があります。</p>
ASA 5550、5580、および 5585-X でのコンテキストの増加	8.4(1)	<p>ASA 5550 および ASA 5585-X (SSP-10) では、コンテキストの最大数が 50 から 100 に引き上げられました。ASA 5580 および 5585-X (SSP-20) 以降では、コンテキストの最大数が 50 から 250 に引き上げられました。</p>
ASA 5580 および 5585-X での VLAN 数の増加	8.4(1)	<p>ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上げられました。</p>
ASA 5580 および 5585-X での接続数の増加	8.4(1)	<p>ファイアウォール接続の最大数が次のように引き上げられました。</p> <ul style="list-style-type: none"> • ASA 5580-20 : 1,000,000 から 2,000,000 へ。 • ASA 5580-40 : 2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-10 : 750,000 から 1,000,000 へ。 • ASA 5585-X with SSP-20 : 1,000,000 から 2,000,000 へ。 • ASA 5585-X with SSP-40 : 2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-60 : 2,000,000 から 10,000,000 へ。

機能名	プラットフォーム リリース	説明
AnyConnect Premium SSL VPN ライセンスの AnyConnect Premium ライセンスへの変更	8.4(1)	AnyConnect Premium SSL VPN ライセンスの名前が AnyConnect Premium ライセンスに変更されました。ライセンス情報の表示が「SSL VPN ピア」から「AnyConnect Premium ピア」に変更されました。
ASA 5580 での AnyConnect VPN セッション数の増加	8.4(1)	AnyConnect VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
ASA 5580 での AnyConnect 以外の VPN セッション数の増加	8.4(1)	AnyConnect 以外の VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
IKEv2 を使用した IPsec リモートアクセス	8.4(1)	<p>AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに IKEv2 を使用した IPsec リモートアクセス VPN が追加されました。</p> <p>(注) ASA での IKEv2 のサポートに関して、重複するセキュリティアソシエーションがサポートされていないという制約が現在あります。</p> <p>Other VPN ライセンス（以前の IPsec VPN）には IKEv2 サイトツーサイトセッションが追加されました。Other VPN ライセンスは基本ライセンスに含まれています。</p>
輸出用のペイロード暗号化なしハードウェア	8.4(1)	ペイロード暗号化機能のないモデルでは（ASA 5585-X など）、特定の国に ASA を輸出できるよう、ASA ソフトウェアのユニファイドコミュニケーションと VPN 機能を無効にしています。

機能名	プラットフォーム リリース	説明
デュアル SSP (SSP-20 および SSP-40)	8.4(2)	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません (たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません)。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバーペアとして使用できます。2 個の SSP をシャーシで使用する場合、VPN はサポートされません。しかし、VPN がディセーブルになっていないことに注意してください。
ASA 5512-X ~ ASA 5555-X での IPS モジュール ライセンス	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X での IPS SSP ソフトウェア モジュールには IPS モジュールライセンスが必要です。
ASA 5580 および ASA 5585-X のクラスタリング ライセンス。	9.0(1)	クラスタリングライセンスが ASA 5580 および ASA 5585-X に対して追加されました。
ASASM での VPN のサポート	9.0(1)	ASASM は、すべての VPN 機能をサポートするようになりました。
ASASM でのユニファイド コミュニケーションのサポート	9.0(1)	ASASM は、すべてのユニファイド コミュニケーション機能をサポートするようになりました。
SSP-10 および SSP-20 に対する ASA 5585-X デュアル SSP サポート (SSP-40 および SSP-60 に加えて)、デュアル SSP に対する VPN サポート	9.0(1)	ASA 5585-X は、すべての SSP モデルでデュアル SSP をサポートするようになりました (同一シャーシ内で同じレベルの SSP を 2 つ使用できます)。デュアル SSP を使用するとき VPN がサポートされるようになりました。

機能名	プラットフォーム リリース	説明
ASA 5500-X でのクラスタリングのサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニット クラスタ をサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになります。ASA 5512-X では Security Plus ライセンスが必要です。
ASA 5585-X の 16 の クラスタ メンバ のサポート	9.2(1)	ASA 5585-X が 16 ユニット クラスタ をサポートするようになりました。
ASAv4 および ASAv30 の標準およびプレミアム モデル ライセンスの導入	9.2(1)	シンプルなライセンス方式で ASAv が導入されました（標準またはプレミアム レベルの ASAv4 および ASAv30 永続ライセンス）。アドオンライセンスは使用できません。



第 5 章

ライセンス：スマート ソフトウェア ライセンス（ASA v、ASA on Firepower）

シスコ スマート ソフトウェア ライセンスによって、ライセンスを購入し、ライセンスのプールを一元管理できます。製品認証キー（PAK）ライセンスとは異なり、スマートライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンスキーを管理しなくても、簡単に ASA を導入したり使用を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。



(注) スマート ソフトウェア ライセンスは、ASA v および ASA Firepower シャーシでのみサポートされます。他のモデルは、PAK ライセンスを使用します。「[PAK ライセンスについて \(105 ページ\)](#)」を参照してください。

- [スマート ソフトウェア ライセンスについて \(169 ページ\)](#)
- [スマート ソフトウェア ライセンスの前提条件 \(177 ページ\)](#)
- [スマート ソフトウェア ライセンスのガイドライン \(178 ページ\)](#)
- [スマート ソフトウェア ライセンスのデフォルト \(179 ページ\)](#)
- [ASA v：スマート ソフトウェア ライセンシングの設定 \(179 ページ\)](#)
- [Firepower 9300 シャーシ：スマート ソフトウェア ライセンスの設定 \(183 ページ\)](#)
- [モデルごとのライセンス \(187 ページ\)](#)
- [Smart Software Licensing のモニタリング \(189 ページ\)](#)
- [スマート ソフトウェア ライセンスの履歴 \(190 ページ\)](#)

スマート ソフトウェア ライセンスについて

ここでは、スマート ソフトウェア ライセンスの仕組みについて説明します。

Firepower 9300 シャーシの ASA のスマート ソフトウェア ライセンシング

Firepower 9300 シャーシ 上の ASA では、スマート ソフトウェア ライセンシングの設定は、Firepower 9300 シャーシ スーパーバイザと ASA に分割されています。

- Firepower 9300 シャーシ : License Authority との通信に使用するパラメータなど、すべてのスマート ソフトウェア ライセンシング インフラストラクチャをシャーシで設定します。Firepower 9300 シャーシ 自体の動作にライセンスは必要ありません。
- ASA アプリケーション : ASA のすべてのライセンスの権限付与を設定します。

Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

<https://software.cisco.com/#module/SmartLicensing>

Smart Software Manager では、組織のマスター アカウントを作成できます。



(注) まだアカウントをお持ちでない場合は、リンクをクリックして**新しいアカウントを設定**してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトで、ライセンスはマスターアカウントの下のデフォルト仮想アカウントに割り当てられます。アカウント管理者であれば、任意で追加の仮想アカウントを作成できます。たとえば、地域、部門、または子会社のアカウントを作成できます。複数の仮想アカウントを使用すると、大量のライセンスおよびデバイスをより簡単に管理できます。

仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。アカウントに割り当てられたライセンスを使用できるのは、その仮想アカウントのデバイスのみです。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。仮想アカウント間でデバイスを転送することもできます。

Firepower 9300 シャーシ 上で動作する ASA の場合 : シャーシのみがデバイスとして登録される一方で、シャーシ内の ASA アプリケーションはそれぞれ固有のライセンスを要求します。たとえば、3つのセキュリティ モジュールを搭載した Firepower 9300 シャーシでは、全シャーシが1つのデバイスとして登録されますが、各モジュールは合計3つのライセンスを別個に使用します。

評価ライセンス

ASAv

ASAv は、評価モードをサポートしていません。Licensing Authority への登録の前に、ASAv は厳しいレート制限状態で動作します。

Firepower 9300 シャーシ

Firepower 9300 シャーシは、次の 2 種類の評価ライセンスをサポートしています。

- シャーシ レベル評価モード : Firepower 9300 シャーシによる Licensing Authority への登録の前に、評価モードで 90 日間 (合計使用期間) 動作します。このモードでは、ASA は固有の権限付与を要求できません。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 9300 シャーシはコンプライアンス違反の状態になります。
- 権限付与ベースの評価モード : Firepower 9300 シャーシが Licensing Authority に登録をした後、ASA に割り当て可能な時間ベースの評価ライセンスを取得できます。ASA で、通常どおりに権限付与を要求します。時間ベースのライセンスの期限が切れると、時間ベースのライセンスを更新するか、または永続ライセンスを取得する必要があります。



(注) 高度暗号化 (3DES/AES) の評価ライセンスを受け取ることはできません。License Authority に登録して永続ライセンスを取得する必要があります。

Smart Software Manager 通信

このセクションでは、デバイスの Smart Software Manager に対する通信方法について説明します。

デバイスの登録とトークン

各仮想アカウントに対し、登録トークンを作成できます。このトークンは、デフォルトで 30 日間有効です。各デバイスを展開するか、または既存のデバイスを登録する場合は、このトークン ID と権限レベルを入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。



(注) Firepower 9300 シャーシ : デバイス登録は、ASA 論理デバイス上ではなく、シャーシで設定されます。

展開後の起動時、または既存のデバイスでこれらのパラメータを手動で設定した後、デバイスは Cisco License Authority に登録されます。デバイスがトークンにより登録されると、デバイスとライセンス機関との間の通信に使用する ID 証明書がライセンス機関により発行されます。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。

License Authority との定期通信

デバイスは 30 日ごとに License Authority と通信します。Smart Software Manager に変更を行う場合、デバイスの認証を更新して変更をすぐに反映させることができます。またはスケジュール設定されたデバイスの通信を待つこともできます。

必要に応じて、HTTP プロキシを設定できます。

ASAv

ASAv は直接または HTTP プロキシ経由で少なくとも 30 日ごとにインターネット アクセスを行う必要があります。ASAv には猶予期間がありません。Licensing Authority に連絡しない限り、正常に再認証できるまで、ASAv は厳しくレート制限されます。

Firepower 9300

Firepower 9300では、少なくとも 90 日おきに、直接接続または HTTP プロキシを介したインターネット アクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Licensing Authority に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行なえませんが、動作には影響ありません。

非適合状態

デバイスは、次の状況においてコンプライアンス違反になる可能性があります。

- 使用率超過：デバイスが使用不可のライセンスを使用している場合。
- ライセンスの有効期限切れ：時間ベースのライセンスの有効期限が切れている場合。
- 通信の欠落：デバイスが再許可を得るために Licensing Authority に到達できない場合。

アカウントのステータスがコンプライアンス違反状態なのか、違反状態に近づいているのかを確認するには、デバイスで現在使用中の権限付与とスマートアカウントのものを比較する必要があります。

コンプライアンス違反状態では、モデルによってはデバイスが制限されている可能性があります。

- ASAv：正常に再認証できるまで、ASAv は厳しくレート制限されます。
- Firepower 9300：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。

Smart Call Home インフラストラクチャ

デフォルトでは、Licensing Authority の URL を指定する Smart Call Home プロファイルがコンフィギュレーションに存在します。このプロファイルは削除できません。ライセンスプロファ

イルの唯一の設定可能なオプションが License Authority の宛先アドレス URL であることに注意してください。Cisco TAC に指示されない限り、License Authority の URL は変更しないでください。



(注) Firepower 9300 シャーシの場合、ライセンスの Smart Call Home は ASA ではなく Firepower 9300 シャーシ スーパーバイザで設定されます。

スマート ソフトウェア ライセンスの Smart Call Home をディセーブルにすることはできません。たとえば、**no service call-home** コマンドを使用して Smart Call Home を無効化しても、スマート ソフトウェア ライセンシングは無効化されません。

他の Smart Call Home の機能は、特に設定しない限り、有効になりません。

ライセンスに関する注意事項

次の表に、ライセンスに関する追加情報を示します。

AnyConnect Plus および Apex ライセンス

AnyConnect Plus および Apex ライセンスは、ライセンスが指定するユーザプールを共有するすべての複数の ASA に適用できる同時使用ライセンスです。スマート ライセンスを使用するデバイスでは、実際のプラットフォームに AnyConnect ライセンスを物理的に適用する必要はありません。ただし、同じライセンスを購入して、ソフトウェアセンターへのアクセスやテクニカル サポートを使用するために契約番号を Cisco.com ID に関連付ける必要があります。詳細については、以下を参照してください。

- [『Cisco AnyConnect Ordering Guide』](#)
- [AnyConnect Licensing Frequently Asked Questions \(FAQ\)](#)

その他の VPN ライセンス

その他の VPN セッションには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN セッション、全タイプ

- VPN セッションの最大数の合計が、VPN AnyConnect とその他の VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えるこ

とはできません。VPN の最大セッション数を超えた場合、ASA をオーバーロードして、適切なネットワークのサイズに設定してください。

- クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアントセッションを開始した場合は、合計1つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロンクライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2つのセッションが使用されています。

暗号化ライセンス

高度暗号化 : ASA v

ライセンス認証局に接続する前に、高度暗号化（3DES/AES）を管理接続に使用できるので、ASDM を起動してライセンス認証局に接続することができます。through-the-box トラフィックの場合、License Authority に接続して高度暗号化ライセンスを取得するまで、スループットは厳しく制限されます。

ASA v が後でコンプライアンス違反になった場合、ASA v はレート制限状態に戻ります。

高度暗号化 : Firepower 9300 シャーシ

ASDM には 3DES が必要なため、CLI を使用して ASA 設定で高度暗号化ライセンスを手動で要求する必要があります。ASA がコンプライアンス違反になると、管理トラフィックやこのライセンスを必要とするスループットは許可されません。

DES : すべてのモデル

DES ライセンスはディセーブルにできません。3DES ライセンスをインストールしている場合、DES は引き続き使用できます。強力な暗号化だけを使用したい場合に DES の使用を防止するには、強力な暗号化だけを使用するようにすべての関連コマンドを設定する必要があります。

合計 UC プロキシセッション

Encrypted Voice Inspection の各 TLS プロキシセッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシセッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy など）では、TLS 制限に対してカウントしません。

アプリケーションによっては、1つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は2つ使用されます。

TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのラ

ライセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。



(注) 「K8」で終わるライセンス製品番号（たとえばユーザ数が250未満のライセンス）では、TLS プロキシセッション数は1000までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザ数が250以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8とK9は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8は制限されず、K9は制限されます。

（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラーメッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合があります。

- K8 ライセンスでは、SRTP セッション数は250までに制限されます。
- K9 ライセンスでは、制限はありません。



(注) メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグがSRTPであっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

ボットネットトラフィックフィルタ ライセンス

ダイナミック データベースをダウンロードするには、強力な暗号化（3DES/AES）ライセンスが必要です。

フェールオーバーまたは ASA クラスタ ライセンス

ASAv のフェールオーバー ライセンス

スタンバイ ユニットにはプライマリ ユニットと同じモデル ライセンスが必要です。

Firepower 9300 シャーシの ASA のフェールオーバー ライセンス

各 Firepower 9300 シャーシは、License Authority またはサテライト サーバに登録されている必要があります。セカンダリユニットに追加費用はかかりません。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。

各 ASA に同じ暗号化ライセンスが必要です。通常の Smart Software Manager (SSM) ユーザの場合、強力な暗号化ライセンスは、Firepower 9300 シャーシで登録トークンを適用すると、対象となるお客様の場合には自動的に有効化されます。古い Cisco Smart Software Manager サテライトが導入されている場合は、以下を参照してください。

ASA ライセンス設定では、その他のライセンスは各フェールオーバー ユニットで一致している必要はなく、各ユニットで別個にライセンスを設定できます。各ユニットには、サーバからの各自のライセンスが必要です。両方のユニットから要求されるライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライセンスはスタンバイユニットにキャッシュされ、将来アクティブなユニットとなったときに使用されます。通常、プライマリユニットのみライセンスを設定すれば済みます。

各ライセンス タイプは次のように処理されます：

- **Standard** : デフォルトで各ユニットに Standard ライセンスが含まれています。したがって、フェールオーバーのペアでは、サーバから 2 つの標準ライセンスが要求されます。
- **Context** : 各ユニットは自身の Context ライセンスを要求できます。ただし、デフォルトで Standard ライセンスには 10 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Standard ライセンスの値と、両方のユニットにあるオプションの Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
 - Standard ライセンスに 10 のコンテキストが含まれ、2 つのユニットでは 20 のコンテキストがあります。250 の Context ライセンスをアクティブ/スタンバイペアのプライマリユニットに設定した場合を考えます。この場合、集約されたフェールオーバーライセンスには 270 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。この場合では、プライマリの Context ライセンスとして 230 コンテキストを設定する必要があります。
 - Standard ライセンスには 10 のコンテキストがあり、2 つユニットがあるため、合計で 20 のコンテキストがあります。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定し、セカンダリ ユニットにも 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 40 のコンテキストが含まれています。たとえば、一方のユニットが 22 コンテキストを使用し、他方が 18 コンテキストを使用します (合計 40 の場合)。ユニットごとのプラットフォーム

ムの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。40 コンテキストは制限の範囲内です。

- キャリア：ユニット 1 つのみがこのライセンスを要求する必要があり、両方のユニットがこれを使用できます。
- 高度暗号化（3DES）（2.3.0 より前の Cisco Smart Software Manager サテライト導入の場合のみ）：各ユニットがサーバからの各自のライセンスを要求する必要があります。他のライセンス設定とは異なり、この設定はスタンバイユニットに複製されます。スマートソフトウェア マネージャ サテライトが導入されている場合、ASDM や他の高度暗号機能を使用するには、クラスタ展開後にプライマリユニットで ASA CLI を使い高度暗号化ライセンスを有効にする必要があります。高度暗号化（3DES）ライセンスの評価ライセンスは一切ありません。

Firepower 9300 シャーシ上の ASA の ASA クラスタ ライセンス

マスターユニットでのみライセンスを要求できます。ライセンスはスレーブユニットでは集約されます。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。マスターユニットで完了したライセンス設定はスレーブユニットに複製されません。クラスタリングを無効にし、ライセンスを設定し、クラスタリングを再度有効にした場合限り、スレーブユニットに個別のライセンス権限付与を設定できます。



- (注) ASDM や他の高度暗号機能を使用するには、クラスタ展開後にマスターユニットで ASA CLI を使用して高度暗号化（3DES）ライセンスを有効にする必要があります。このライセンスは、スレーブユニットによって継承されます。このライセンスは、各ユニットで個別に設定する必要はありません。高度暗号化（3DES）ライセンスの評価ライセンスは一切ありません。



- (注) マスターユニットに障害が発生し、30 日（ライセンス猶予期間）以内に再参加しない場合、継承されたライセンスは消滅します。その場合、新しいマスターユニットに消滅したライセンスを手動で設定する必要があります。

スマートソフトウェアライセンスの前提条件

- ASAv：デバイスからのインターネットアクセス、または HTTP プロキシアクセスを確保します。
- ASAv：デバイスが License Authority の名前を解決できるように DNS サーバを設定します。
- ASAv：デバイスのクロックを設定します。
- Firepower 9300 シャーシ：ASA ライセンス資格を設定する前に、Firepower 9300 シャーシでスマートソフトウェアライセンス インフラストラクチャを設定します。

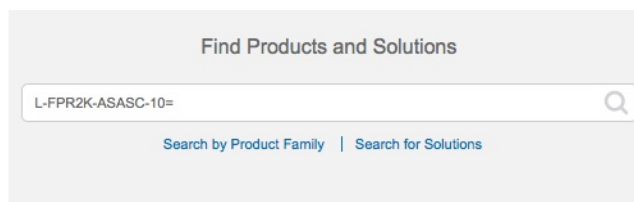
- Cisco Smart Software Manager でマスター アカウントを作成します。

<https://software.cisco.com/#module/SmartLicensing>

まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

- ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェアライセンシングアカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [Find Products and Solutions] 検索フィールドを使用します。次のライセンス PID を検索します。

図 14: ライセンス検索



ASAv PID :

- ASAv5 : L-ASAV5S-K9=
- ASAv10 : L-ASAV10S-K9=
- ASAv30 : L-ASAV30S-K9=
- ASAv50 : L-ASAV50S-K9=

Firepower 4100 PID :

Firepower 9300 PID :

スマートソフトウェアライセンスのガイドライン

- スマートソフトウェアライセンスのみがサポートされます。ASAvの古いソフトウェアについては、PAKライセンスが供与された既存のASAvをアップグレードする場合、前にインストールしたアクティベーションキーは無視されますが、デバイスに保持されます。ASAvをダウングレードすると、アクティベーションキーが復活します。
- (FirePOWER 9300 ASA セキュリティ モジュール) ASDM および VPN などの他の強力な暗号化機能を使用するには、ASA の展開後、ASA CLI を使用するマスター ユニット上で Strong Encryption (3DES) ライセンスを有効にする必要があります。クラスタリングの場合、マスター ユニットのライセンスを設定します。このライセンスは、スレーブ ユニットによって継承されます。このライセンスは、各ユニットで個別に設定する必要はありません。

スマート ソフトウェア ライセンスのデフォルト

ASA v

- ASA v のデフォルト設定には、認証局の URL を指定する Smart Call Home プロファイルが含まれています。
- ASA v を導入するときに、機能層とスループット レベルを設定します。現時点では、標準レベルのみを使用できます。
- また、導入時に任意で HTTP プロキシを設定できます。

Firepower 9300 シャーシ 上の ASA

デフォルト設定はありません。標準ライセンス階層、およびその他のオプションライセンスは手動で有効化する必要があります。

ASA v : スマート ソフトウェア ライセンシングの設定

このセクションでは、ASA v にスマート ソフトウェア ライセンスを設定する方法を説明します。

手順

[ASA v : スマート ソフトウェア ライセンシングの設定 \(179 ページ\)](#)。

ASA v : スマート ソフトウェア ライセンシングの設定

ASA v を展開する場合は、デバイスを事前に設定し、License Authority に登録するために登録トークンを適用して、スマート ソフトウェア ライセンシングを有効にすることができます。HTTP プロキシサーバ、ライセンス権限付与を変更する必要がある場合、または ASA v を登録する必要がある場合 (Day0 コンフィギュレーションに ID トークンを含めなかった場合など) は、このタスクを実行します。



- (注) ASA v を展開したときに、HTTP プロキシとライセンス権限付与が事前に設定されている可能性があります。また、ASA v を展開したときに Day0 コンフィギュレーションで登録トークンが含まれている可能性があります。その場合は、この手順を使用して再登録する必要はありません。
-

手順

ステップ 1 Smart Software Manager (Cisco Smart Software Manager) で、このデバイスを追加するバーチャルアカウントの登録トークンを要求してコピーします。

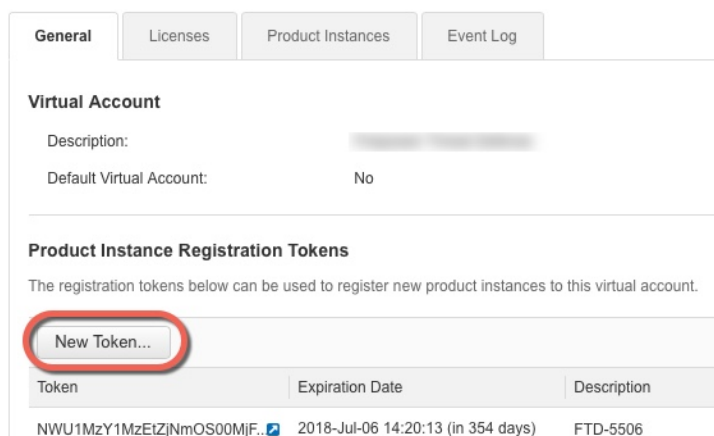
a) [Inventory] をクリックします。

図 15: インベントリ



b) [General] タブで、[New Token] をクリックします。

図 16: 新しいトークン



c) [Create Registration Token] ダイアログボックスで、以下の設定値を入力してから [Create Token] をクリックします。

- [説明 (Description)]
- Expire After : 推奨値は 30 日です。
- Allow export-controlled functionality on the products registered with this token : 輸出コンプライアンス フラグを有効にします。

図 17: 登録トークンの作成

Create Registration Token

This dialog will generate the token required to register your product instances with your Smart Account.

Virtual Account: [Redacted]

Description: [Redacted]

* Expire After: 30 Days

Enter the value between 1 and 365, but Cisco recommends a maximum of 30 days.

Allow export-controlled functionality on the products registered with this token

Create Token Cancel

トークンはインベントリに追加されます。

- d) トークンの右側にある矢印アイコンをクリックして [Token] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 18: トークンの表示

General Licenses Product Instances Event Log

Virtual Account

Description: [Redacted]

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjhhYTItZGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed	[Redacted]	Actions

図 19: トークンのコピー

Token

MjM3ZjhhYTItZGQ4OS00Yjk2LTgzMGItMThmZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFjN2dYQjI5QWRhOEEdscDU4cWI5NFNWRUtsa2wz%0AMFd0ST0%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjhhYTItZGQ4OS00Yjk2LT... 2017-Aug-16 1

ステップ 2 (任意) HTTP プロキシの URL を指定します。

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマートソフトウェア ライセンスのプロキシアドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

- a) **[Configuration] > [Device Management] > [Smart Call-Home]** を選択します。

- b) [Enable HTTP Proxy] をオンにします。
- c) [Proxy server] および [Proxy port] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバのポート 443 を入力します。
- d) [Apply] をクリックします。

ステップ 3 ライセンス権限付与を設定します。

- a) [Configuration] > [Device Management] > [Licensing] > [Smart Licensing] の順に選択します。
- b) [Enable Smart license configuration] をオンにします。
- c) [Feature Tier] ドロップダウンメニューから [Standard] を選択します。
使用できるのは標準層だけです。

- d) [Throughput Level] ドロップダウンメニューから [100M]、[1G]、[2G]、[10G] を選択します。
(注) [Enable strong-encryption protocol] チェックボックスはオンにしないでください。
この設定は、2.3.0 より前のサテライト サーバ専用です。

- e) [Apply] をクリックします。

ステップ 4 ASAv の License Authority への登録。

- a) [Configuration] > [Device Management] > [Licensing] > [Smart Licensing] の順に選択します。
- b) [Register] をクリックします。
- c) [ID Token] フィールドに登録トークンを入力します。
- d) (オプション) [Force registration] チェックボックスをオンにして、License Authority と同期されていない可能性がある登録済みの ASAv を登録します。

たとえば、Smart Software Manager から誤って ASAv を削除した場合に **Force registration** を使用します。

- e) [Register] をクリックします。

ASAv は、License Authority への登録を試み、設定されたライセンス資格の認証を要求します。

(オプション) ASAv の登録解除

ASAv の登録を解除すると、アカウントから ASAv が削除され、ASAv のすべてのライセンス資格と証明書が削除されます。登録を解除することで、ライセンスを新しい ASAv に利用することもできます。あるいは、Smart Software Manager (SSM) から ASAv を削除できます。

手順

ステップ 1 [Configuration] > [Device Management] > [Licensing] > [Smart Licensing] の順に選択します。

ステップ 2 [Unregister] をクリックします。

ASAv がリロードされます。

(オプション) ASA ID 証明書またはライセンス権限付与の更新

デフォルトでは、アイデンティティ証明書は 6 ヶ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネットアクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 [Configuration] > [Device Management] > [Licensing] > [Smart Licensing] の順に選択します。

ステップ 2 アイデンティティ証明書を更新するには、[Renew ID Certificate] をクリックします。

ステップ 3 ライセンス資格を更新するには、[Renew Authorization] をクリックします。

Firepower 9300 シャーシ : スマート ソフトウェア ライセンスの設定

このセクションでは、Firepower 9300 シャーシにスマート ソフトウェア ライセンスを設定する方法を説明します。

手順

ステップ 1 [Firepower 9300 シャーシ : スマート ソフトウェア ライセンシングの設定 \(183 ページ\)](#)。最初に; ASA CLI でライセンスを設定する必要があります。事前のライセンスに関する通信を設定する FXOS 構成ガイドを参照してください。

ステップ 2 [Firepower 9300 シャーシ : ASDM を使用したスマート ソフトウェア ライセンシングの設定の変更 \(186 ページ\)](#)。CLI でライセンスを有効にした後、ASDM を使用して設定を変更できます。

Firepower 9300 シャーシ : スマート ソフトウェア ライセンシングの設定

最初に; ASA CLI でライセンスを設定する必要があります。事前のライセンスに関する通信を設定する FXOS 構成ガイドを参照してください。。



(注) 高度暗号化 (3DES/AES) ライセンスはデフォルトで有効になっていないため、ASA CLI を使用して高度暗号化ライセンスをリクエストするまで、ASA の設定に ASDM を使用することはできません。他の強力な暗号化機能も、このリクエストを行うまでは使用できません。

CLI で強力な暗号化を有効にした後、ASDM でライセンスを設定するには、**[Configuration] > [Device Management] > [Licensing] > [Smart Licensing]** ペインを参照してください。

始める前に

ASA クラスタの場合は、設定作業のために標準出荷単位にアクセスする必要があります。Firepower Chassis Manager で、標準出荷単位を確認します。この手順に示すように、ASA CLI から確認できます。

手順

ステップ 1 Firepower 9300 シャーシ CLI (コンソールまたは SSH) に接続し、次に ASA にセッション接続します。

connect module slot console connect asa

例 :

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

次回 ASA コンソールに接続するときは、ASA に直接移動します。**connect asa** を再入力する必要はありません。

ASA クラスタの場合、ライセンス設定などの設定を行う場合にのみ、マスターユニットにアクセスする必要があります。通常、マスターユニットがスロット 1 にあるため、このモジュールにまず接続する必要があります。

ステップ 2 ASA CLI で、グローバルコンフィギュレーションモードを入力します。デフォルトではイネーブルパスワードは空白ですが。

enable configure terminal

例 :

```
asa> enable
Password:
asa# configure terminal
asa(config)#
```

ステップ 3 ASA クラスタの場合は、必要に応じて、このユニットが標準出荷単位であることを確認します。

show cluster info

例 :

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
  Other members in the cluster:
    Unit "unit-1-2" in state SLAVE
      ID : 1
      Version : 9.5(2)
      Serial No.: P3000000001
      CCL IP : 127.2.1.2
      CCL MAC : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2015
      Last leave: N/A
    Unit "unit-1-3" in state MASTER
      ID : 2
      Version : 9.5(2)
      Serial No.: JAB0815R0JY
      CCL IP : 127.2.1.3
      CCL MAC : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2015
      Last leave: N/A
```

別のユニットが標準出荷単位の場合は、接続を終了し、正しいユニットに接続します。接続の終了については、以下を参照してください。

ステップ 4 ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例 :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

ステップ 5 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。ティアライセンスは、他の機能ライセンスを追加するための前提条件です。

ステップ 6 次の機能の 1 つ以上をリクエストします。

- モバイル SP (GTP/GPRS)

feature mobile-sp

- セキュリティ コンテキスト
`feature context <1-248>`
- 高度暗号化 (3DES/AES)
`feature strong-encryption`

ステップ7 ASA コンソールを終了して Telnet アプリケーションに戻るには、プロンプトで「~」と入力します。スーパーバイザ CLI に戻るには、「quit」と入力します。

Firepower 9300 シャーシ : ASDM を使用したスマートソフトウェアライセンスの設定の変更

ASDM を使用するには、まず CLI で 3DES (高度暗号化) ライセンスを要求する必要があります。Firepower 9300 シャーシ : スマートソフトウェアライセンスの設定 (183 ページ) を参照してください。ASDM へのアクセス後に設定を変更するには、この手順を使用します。

始める前に

ASA クラスタの場合は、設定作業のために標準出荷単位にアクセスする必要があります。Firepower Chassis Manager で、標準出荷単位を確認します。

手順

- ステップ1 ASDM で、[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] の順に選択します。
- ステップ2 [Feature Tier] ドロップダウンメニューから [Standard] を選択します。
使用できるのは標準層だけです。
- ステップ3 [Strong Encryption] ライセンスを無効にしないでください。これは ASDM アクセスに必要です。
- ステップ4 (任意) [Mobile SP] [Carrier] を確認します。
- ステップ5 (任意) [Context] ドロップダウンメニューから、必要なコンテキストの番号を選択します。
- ステップ6 [Apply] をクリックします。
- ステップ7 ASDM を終了し、再起動します。

ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

モデルごとのライセンス

このセクションでは、ASA v および Firepower 9300 シャーシASA セキュリティ モジュールに使用可能なライセンス資格を示します。

ASA v

次の表に、ASA v シリーズのライセンス機能を示します。

ライセンス	Standard ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	イネーブル	
ファイアウォールの接続、同時	ASA v5 : 100,000 ASA v10 : 100,000 ASA v30 : 500,000	
GTP/GPRS	イネーブル	
合計 UC プロキシセッション	ASA v5: 500 ASA v10 : 500 ASA v30 : 1000	
VPN ライセンス		
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス、最大： <i>ASA v5: 50</i> <i>ASA v10 : 250</i> <i>ASA v30 : 750</i>
その他の VPN ピア	ASA v5 : 250 ASA v10 : 250 ASA v30 : 1000	
合計 VPN ピア。全タイプの合計	ASA v5 : 250 ASA v10 : 250 ASA v30 : 1000	

ライセンス	Standard ライセンス
一般ライセンス	
スループット レベル	ASAv5 : 1 Gbps ASAv10 : 1 Gbps ASAv30 : 2 Gbps
暗号化	Strong (3DES/AES)
フェールオーバー	アクティブ/スタンバイ
セキュリティ コンテキスト	サポートなし
クラスタ	サポートなし
VLAN、最大	ASAv5 : 50 ASAv10 : 50 ASAv30 : 200
RAM、vCPUs	ASAv5 : 2 GB、1 vCPU ASAv10 : 2 GB、1 vCPU ASAv30 : 8 GB、4 vCPU

Firepower 9300 ASA アプリケーション

次の表に、Firepower 9300 ASA アプリケーションのライセンス機能を示します。

ライセンス	Standard ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 9300 SM-36 : 60,000,000、最大 70,000,000 (3 モジュールを搭載したシャーシ) Firepower 9300 SM-24 : 55,000,000、最大 70,000,000 (3 モジュールを搭載したシャーシ)	
GTP/GPRS	無効	オプション ライセンス : <i>Mobile SP</i>
合計 UC プロキシセッション	15,000	
VPN は、Firepower Chassis Manager 1.1.2 以前にはサポートしていません。		

ライセンス	Standard ライセンス	
一般ライセンス		
暗号化	Base (DES) または Strong (3DES/AES)	
セキュリティ コンテキスト	10	オプション ライセンス : 最大 250、10 単位
クラスタ	イネーブル	
VLAN、最大	1024	

Smart Software Licensing のモニタリング

デバッグメッセージをイネーブルにするだけでなく、ライセンスの機能、ステータス、および証明書をモニタすることもできます。

現在のライセンスの表示

ライセンスを表示するには、次の画面を参照してください。

- [Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ペインで、[Effective Running Licenses] 領域を表示します。

スマート ライセンス ステータスの表示

ライセンス ステータスを表示するには、次のコマンドを参照してください。

- : [Monitoring] > [Properties] > [Smart License]

スマート ソフトウェア ライセンシング、スマート エージェントのバージョン、UDI 情報、スマート エージェントの状態、グローバルコンプライアンスステータス、資格ステータス、使用許可証明書情報および予定のスマート エージェント タスクを表示します。

- [Configuration] > [Device Management] > [Licensing] > [Smart Licensing] > [Registration Status]

現在のスマート ライセンスの登録ステータスを表示します。

スマートソフトウェアライセンスの履歴

機能名	プラットフォーム リリース	説明
FirePOWER 9300 の ASA のシスコ スマートソフトウェアライセンシング	9.4(1.150)	<p>FirePOWER 9300 に ASA のシスコ スマートソフトウェアライセンシングが導入されました。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [Licensing] > [Smart License]</p>
ASAv のシスコ スマートソフトウェアライセンシング	9.3(2)	<p>Smart Software Licensing では、ライセンスのプールを購入して管理することができます。PAK ライセンスとは異なり、スマートライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンスキーを管理しなくても、簡単に ASAv を導入したり導入を終了したりできます。スマートソフトウェアライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。</p> <p>次の画面が導入または変更されました。</p> <p>[Configuration] > [Device Management] > [Licensing] > [Smart License] [Configuration] > [Device Management] > [Smart Call-Home] [Monitoring] > [Properties] > [Smart License]</p>



第 6 章

論理デバイス Firepower 9300

Firepower 9300は柔軟なセキュリティプラットフォームが1つまたは複数の論理デバイスをインストールすることができます。この章では、基本的なインターフェイスの設定、および Firepower Chassis Manager を使用したスタンドアロンまたはハイ アベイラビリティ論理デバイスの追加方法について説明します。クラスタ化された論理デバイスを追加する場合は、[Firepower 9300 シャーシの ASA クラスタ \(421 ページ\)](#) を参照してください。FXOS CLI を使用する場合は、FXOS CLI コンフィギュレーションガイドを参照してください。高度なFXOSの手順とトラブルシューティングについては、FXOS コンフィギュレーションガイドを参照してください。

- [Firepower インターフェイスについて \(191 ページ\)](#)
- [論理デバイスについて \(193 ページ\)](#)
- [ハードウェアとソフトウェアの組み合わせの要件と前提条件 \(193 ページ\)](#)
- [論理デバイスに関する注意事項と制約事項 \(194 ページ\)](#)
- [インターフェイスの設定 \(195 ページ\)](#)
- [論理デバイスの設定 \(198 ページ\)](#)
- [論理デバイスの履歴 \(205 ページ\)](#)

Firepower インターフェイスについて

Firepower 9300 シャーシは、物理インターフェイスおよび EtherChannel (ポートチャネル) インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバインターフェイスを最大で 16 個含めることができます。

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firepower Chassis Manager で、FXOS シャーシの管理に使用されます。このインターフェイスはMGMTとして、[Interfaces] タブの上部に表示されます。[Interfaces] タブでは、このインターフェイスの有効化または無効化のみを実行できます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLI から設定にする必要があります。このインターフェイスについての情報を FXOS CLI で表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER connect local-mgmt

```
firepower(local-mgmt) # show mgmt-port
```

物理ケーブルまたは SFP モジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

インターフェイスタイプ

各インターフェイスは、次のいずれかのタイプになります。

- Data** : 通常のデータに使用します。データインターフェイスは論理デバイス間で共有できません。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- Mgmt** : アプリケーションインスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。
- Firepower-eventing** : FTD デバイスのセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント (Web イベントなど) から管理トラフィックを分類できます。Firepower Management Center 構成ガイドのシステム設定の章にある「管理インターフェイス」のセクションを参照してください。Firepower-eventing インターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の論理デバイスと通信することはできません。
- Cluster** : クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャンネル上に自動的に作成されます。このタイプは、EtherChannel インターフェイスのみでサポートされます。

シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティングシステムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシとアプリケーションの間に不一致が生じることがあります。

論理デバイスについて

論理デバイスでは、1つのアプリケーション インスタンス。

論理デバイスを追加するときに、アプリケーション インスタンスのタイプおよびバージョンの定義、インターフェイスの割り当て、アプリケーション 構成にプッシュされるブートストラップ設定の構成も行います。

スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- **スタンドアロン**：スタンドアロン論理デバイスは、スタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。
- **クラスタ**：クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュールデバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 の場合、3つすべてのモジュールが。

ハードウェアとソフトウェアの組み合わせの要件と前提条件

Firepower 9300では、複数のモデル、セキュリティモジュール、アプリケーションタイプ、および高可用性と拡張性の機能がサポートされています。許可された組み合わせについては、次の要件を参照してください。

Firepower 9300 の要件

Firepower 9300 には、3つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を参照してください。

- **セキュリティモジュール タイプ**：Firepower 9300 のすべてのモジュールは同じタイプである必要があります。
- **クラスタリング**：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内のすべてのセキュリティモジュールは同じタイプである必要があります。各シャーシに異なる数のセキュリティモジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。たとえば、シャーシ 1 に 2つの SM-36 を、シャーシ 2 に 3つの SM-36 をインストールできます。
- **高可用性**：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。

- ASA および FTD のアプリケーションタイプ：シャーシ、ASA、または FTD には、1 つのアプリケーションタイプのみインストールできます。
- ASA または FTD のバージョン：個別のモジュールで異なるバージョンのアプリケーションインスタンスタイプを実行することもたとえば、モジュール 1 に FTD 6.3 を、モジュール 2 に FTD 6.4 を、モジュール 3 に FTD 6.5 をインストールできます。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

Firepower インターフェイスに関する注意事項と制約事項

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは、Burned-in MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャンネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャンネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。

一般的なガイドラインと制限事項

ファイアウォール モード

FTD のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定できます。ASA の場合、展開後に、ファイアウォール モードをトランスペアレントに変更することができます。[ASA のトランスペアレントファイアウォールモードへの変更 \(201 ページ\)](#) を参照してください。

ハイアベイラビリティ

- アプリケーション設定内でハイアベイラビリティを設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。
- ハイアベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。

- 同じモデルであること。
 - ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
 - インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 詳細については、[フェールオーバーのシステム要件 \(276ページ\)](#) を参照してください。

コンテキスト モード

- ASA ではマルチ コンテキスト モードはサポートされていません。
- 展開後に、ASA のマルチ コンテキスト モードを有効にします。
- ので TLS 暗号化アクセラレーション を有効にできます。

インターフェイスの設定

デフォルトでは、物理インターフェイスはディセーブルになっています。インターフェイスを有効にし、EtherChannels、インターフェイス プロパティを編集して。



(注) FXOS でインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。





インターフェイスの有効化または無効化

各インターフェイスの **[Admin State]** を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスはディセーブルになっています。

手順

ステップ 1 [Interfaces] を選択して [Interfaces] ページを開きます。

[Interfaces] ページには、ページの上部に現在インストールされているインターフェイスが視覚的に表示され、下の表にはインストールされているインターフェイスのリストが示されています。

- ステップ 2** インターフェイスを有効にするには、[disabled スライダ ()] をクリックします。これで、[enabled スライダ ()] に変わります。
- [Yes] をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグレーからグリーンに変わります。
- ステップ 3** インターフェイスを無効にするには、[enabled スライダ ()] をクリックします。これで、[disabled スライダ ()] に変わります。
- [Yes] をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグリーンからグレーに変わります。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

手順

- ステップ 1** [Interfaces] を選択して [Interfaces] ページを開きます。
- [All Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。
- ステップ 2** 編集するインターフェイスの行の [Edit] をクリックし、[Edit Interface] ダイアログボックスを開きます。
- ステップ 3** インターフェイスをイネーブルにするには、[Enable] チェックボックスをオンにします。インターフェイスをディセーブルにするには、[Enable] チェックボックスをオフにします。
- ステップ 4** インターフェイスの [タイプ (Type)] を次から選択します。Data、Mgmt、または Cluster。
- Cluster** タイプは選択しないでください。デフォルトでは、Cluster Control Link はポートチャネル 48 に自動的に作成されます。
- ステップ 5** (任意) [Speed] ドロップダウン リストからインターフェイスの速度を選択します。
- ステップ 6** (任意) インターフェイスで [Auto Negotiation] がサポートされている場合は、[Yes] または [No] オプション ボタンをクリックします。
- ステップ 7** (任意) [Duplex] ドロップダウン リストからインターフェイスのデュプレックスを選択します。

ステップ 8 [OK] をクリックします。

EtherChannel (ポート チャネル) の追加

EtherChannel (別名ポートチャネル) には、同じタイプのメンバーインターフェイスを最大 16 個含めることができます。リンク集約制御プロトコル (LACP) では、2 つのネットワーク デバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

各メンバー インターフェイスが LACP 更新を送受信するように、Firepower 9300 シャーシは Etherchannel をアクティブ LACP モードでしかサポートしません。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。

手順

ステップ 1 [Interfaces] を選択して [Interfaces] ページを開きます。

[All Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 インターフェイステーブルの上にある [Add Port Channel] をクリックして、[Add Port Channel] ダイアログボックスを開きます。

ステップ 3 [Port Channel ID] フィールドに、ポートチャネルの ID を入力します。有効な値は、1 ~ 47 です。

クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、別の ID で EtherChannel を設定し、インターフェイスにクラスタタイプを選択できます。シャーシ内クラスタリングでは、クラスタ EtherChannel にインターフェイスを割り当てないでください。

ステップ 4 ポートチャネルを有効化するには、[Enable] チェックボックスをオンにします。ポートチャネルをディセーブルにするには、[Enable] チェックボックスをオフにします。

ステップ 5 インターフェイスの [Type] を次から選択します。Data、Mgmt、または Cluster。

デフォルトの代わりに、このポートチャネルを Cluster Control Link として使用する場合は、Cluster タイプを選択しないでください。

ステップ 6 ドロップダウン リストでメンバー インターフェイスの [Admin Speed] を設定します。

ステップ 7 [Admin Duplex]、[Full Duplex] または [Half Duplex] を設定します。

- ステップ 8** ポートチャンネルにインターフェイスを追加するには、**[Available Interface]**リストでインターフェイスを選択し、**[Add Interface]**をクリックしてそのインターフェイスを **[Member ID]** リストに移動します。同じタイプと速度の最大 16 のインターフェイスを追加できます。
- ヒント** 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、**Ctrl**キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、**Shift**キーを押しながら最後のインターフェイスをクリックして選択します。
- ステップ 9** ポートチャンネルからインターフェイスを削除するには、**[Member ID]**リストでそのインターフェイスの右側にある**[Delete]**ボタンをクリックします。
- ステップ 10** **[OK]**をクリックします。

論理デバイスの設定

Firepower 9300 シャーシに、スタンドアロン論理デバイスまたはハイアベイラビリティペアを追加します。

クラスタリングについては、[#unique_263](#)を参照してください。

スタンドアロン ASA の追加

スタンドアロンの論理デバイスは、単独またはハイアベイラビリティペアで動作します。複数のセキュリティモジュールを搭載する Firepower 9300 では、クラスタまたはスタンドアロンデバイスのいずれかを展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2モジュールクラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

Firepower 9300 シャーシからルーテッドファイアウォールモード ASA を展開できます。ASA をトランスペアレントファイアウォールモードに変更するには、この手順を完了し、[ASA のトランスペアレントファイアウォールモードへの変更 \(201 ページ\)](#) を参照してください。

マルチコンテキストモードの場合、最初に論理デバイスを展開してから、ASAアプリケーションでマルチコンテキストモードを有効にする必要があります。

始める前に

- 論理デバイスに使用するアプリケーションイメージを [Cisco.com](#) からダウンロードして、そのイメージを Firepower 9300 シャーシにアップロードします。
- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません（また、**[Interfaces]** タブの上部に **[MGMT]** として表示されません）。
- 次の情報を用意します。

- このデバイスのインターフェイス ID
- 管理インターフェイス IP アドレスとネットワーク マスク
- ゲートウェイ IP アドレス

手順

ステップ 1 [論理デバイス (Logical Devices)] を選択します。

ステップ 2 [デバイスの追加 (Add Device)] をクリックし、次のパラメータを設定します。

a) デバイス名を入力します。

この名前は、シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

b) [Template] では、[Cisco Adaptive Security Appliance] を選択します。

c) [Image Version] を選択します。

d) [使用方法 (Usage)] で、[スタンドアロン (Standalone)] オプション ボタンをクリックします。

e) [OK] をクリックします。

[Provisioning - device name] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるポートをそれぞれクリックします。

以前に[インターフェイス (Interfaces)] ページで有効にしたデータインターフェイスのみを割り当てることができます。後ほど ASA でこれらのインターフェイスを有効にして設定します (IP アドレスの設定を含む)。

ステップ 4 画面中央のデバイス アイコンをクリックします。

初期ブートストラップ設定を設定できるダイアログボックスが表示されます。これらの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [General Information] ページで、次の手順を実行します。

a) (Firepower 9300 の場合) [Security Module Selection] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。

b) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

c) 管理インターフェイスを選択します。[Address Type] : [IPv4 only]、[IPv6 only]、または [IPv4 and IPv6]。

d) [Management IP] アドレスを設定します。

このインターフェイスの一意の IP アドレスを設定します。

- e) ネットワーク マスクまたはプレフィックス長を入力します。
- f) ネットワーク ゲートウェイ アドレスを入力します。

ステップ 6 [Settings] タブをクリックします。

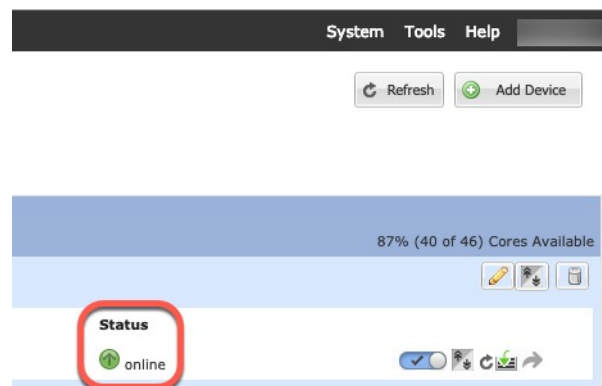
ステップ 7 管理者ユーザの [Password] を入力して確認します。

事前設定されている ASA 管理者ユーザ/パスワードは、パスワードの回復に役立ちます。FXOS アクセスが可能な場合、管理者ユーザ パスワードを忘れたときにリセットできます。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 [Save] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[論理デバイス (Logical Devices)] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



ステップ 10 セキュリティ ポリシーの設定を開始するには、ASA コンフィギュレーション ガイドを参照してください。

ハイアベイラビリティペアの追加

ASA ハイアベイラビリティ (フェールオーバーとも呼ばれます) は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイアベイラビリティのシャーシを準備するには、次の手順を参照してください。

始める前に

- ハイアベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
 - 同じモデルであること。

- ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
- インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 高可用性システム要件については、[フェールオーバーのシステム要件 \(276 ページ\)](#) を参照してください。

手順

- ステップ 1** 各論理デバイスは個別のシャーシ上にある必要があります。Firepower 9300 のシャーシ内のハイアベイラビリティは推奨されず、サポートされない可能性があります。
- ステップ 2** 各論理デバイスに同一のインターフェイスを割り当てます。
- ステップ 3** フェールオーバー リンクとステート リンクに 1 つまたは 2 つのデータ インターフェイスを割り当てます。

これらのインターフェイスは、2 つのシャーシ間でハイアベイラビリティトラフィックを交換します。統合されたフェールオーバーリンクとステートリンクには、10GB のデータインターフェイスを使用することを推奨します。別のフェールオーバーおよび状態のリンクを使用できます使用可能なインターフェイスがあれば、状態のリンクには、ほとんどの帯域幅が必要です。フェールオーバー リンクまたはステート リンクに管理タイプのインターフェイスを使用することはできません。同じネットワーク セグメント上で他のデバイスをフェールオーバーインターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

- ステップ 4** 論理デバイスでハイアベイラビリティを有効にします。[ハイアベイラビリティのためのフェールオーバー \(275 ページ\)](#) を参照してください。
- ステップ 5** ハイアベイラビリティを有効にした後でインターフェイスを変更する必要がある場合は、最初にスタンバイ装置で変更を実行してから、アクティブ装置で変更を実行します。

(注) ASA の場合、FXOS でインターフェイスを削除すると (たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど)、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

ASA のトランスペアレント ファイアウォール モードへの変更

Firepower 9300 シャーシのルーテッドファイアウォールモード ASA のみを導入できます。ASA をトランスペアレントファイアウォールモードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォールモードを変更します。スタンドアロン ASA の場合、ファイアウォールモードを変更すると設定が消去されるため、Firepower 9300 シャーシから設定を再展開して、

ブートストラップ設定を回復する必要があります。ASA はトランスペアレント モードのまま、ブートストラップ設定が機能した状態になっています。クラスタ化 ASA の場合、設定は消去されないため、FXOS からブートストラップ設定を再導入する必要はありません。

手順

ステップ 1 アプリケーションのコンソールへの接続 (204ページ) に従って、ASA コンソールに接続します。クラスタの場合、プライマリ ユニットに接続します。フェールオーバー ペアの場合、アクティブユニットに接続します。

ステップ 2 コンフィギュレーションモードに入ります。

enable

configure terminal

デフォルトでは、イネーブルパスワードは空白です。

ステップ 3 ファイアウォールモードをトランスペアレントに設定します。

firewall transparent

ステップ 4 設定を保存します。

write memory

クラスタまたはフェールオーバー ペアの場合、この設定はセカンダリ ユニットに複製されます。

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to Slave unit-1-2
End Configuration Replication to slave.

asa(config)#
```

ステップ 5 Firepower Chassis Manager の [Logical Devices] ページで、[Edit] アイコンをクリックして ASA を編集します。

[Provisioning] ページが表示されます。

ステップ 6 デバイスのアイコンをクリックして、ブートストラップ設定を編集します。設定の値を変更し、[OK] をクリックします。

少なくとも 1 つのフィールド ([Password] フィールドなど) の値を変更する必要があります。

ブートストラップ設定の変更に関する警告が表示されます。[Yes] をクリックします。

ステップ 7 ASA に設定を再配置する **保存** をクリックします。

シャーシ/セキュリティ モジュールがリロードし、ASA が再度稼働するまで数分待ちます。ASA は、これでブートストラップ設定が機能するようになりますが、トランスペアレントモードのままです。

ASA 論理デバイスのインターフェイスの変更

ASA 論理デバイスでは、管理インターフェイスの割り当て、割り当て解除、または置き換えを行うことができます。ASDM は、新しいインターフェイスを自動的に検出します。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、ASA の設定に与える影響は最小限です。ただし、FXOS で割り当てられたインターフェイスを削除する場合（ネットワーク モジュールの削除、EtherChannel の削除、割り当てられたインターフェイスの EtherChannel への再割り当てなど）、そのインターフェイスがセキュリティポリシーで使用されると、削除は ASA の設定に影響を与えます。この場合、ASA 設定では元のコマンドが保持されるため、必要な調整を行うことができます。ASA OS の古いインターフェイス設定は手動で削除できます。



(注) 論理デバイスに影響を与えずに、割り当てられた EtherChannel のメンバーシップを編集できます。

始める前に

- [物理インターフェイスの設定 \(196 ページ\)](#) および [EtherChannel \(ポート チャネル\) の追加 \(197 ページ\)](#) に従って、インターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトではすべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。
- 管理インターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータ メンバーインターフェイスが少なくとも 1 つある EtherChannel を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。ASA がリロードし（管理インターフェイスを変更するとリロードします）、（現在未割り当ての）管理インターフェイスも EtherChannel に追加できます。
- クラスタ リングまたはフェールオーバーを追加するか、すべてのユニット上のインターフェイスの削除を確認します。最初にスレーブ/スタンバイ ユニットでインターフェイスを変更してから、マスター/アクティブ ユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼしません。

手順

- ステップ 1** Firepower Chassis Manager で、[Logical Devices] を選択します。
- ステップ 2** 右上にある [Edit] アイコンをクリックして、その論理デバイスを編集します。
- ステップ 3** [Data Ports] 領域でデータ インターフェイスの選択を解除して、そのインターフェイスの割り当てを解除します。
- ステップ 4** [Data Ports] 領域で新しいデータ インターフェイスを選択して、そのインターフェイスを割り当てます。
- ステップ 5** 次のように、管理インターフェイスを置き換えます。
- このタイプのインターフェイスでは、変更を保存するとデバイスがリロードします。
- ページ中央のデバイス アイコンをクリックします。
 - [General/Cluster Information] タブで、ドロップダウンリストから新しい [Management Interface] を選択します。
 - [OK] をクリックします。
- ステップ 6** [保存 (Save)] をクリックします。
-

アプリケーションのコンソールへの接続

次の手順に従ってアプリケーションのコンソールに接続します。

手順

- ステップ 1** 、モジュール CLI に接続します。

connect module slot_number console

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

- ステップ 2** アプリケーションのコンソールに接続します。

connect asa

例 :

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- ASA : **Ctrl-a, d** と入力

ステップ 4 FXOS CLI のスーパーバイザ レベルに戻ります。

- ~ と入力

Telnet アプリケーションに切り替わります。

- Telnet アプリケーションを終了するには、次を入力します。

```
telnet>quit
```

論理デバイスの履歴

機能	バージョン	詳細
Firepower 9300 用シャーシ内 ASA クラスタリング	9.4 (1.150)	<p>FirePOWER 9300 シャーシ内では、最大3つセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。</p> <p>次の画面を導入しました。 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]</p>



第 7 章

トランスペアレントファイアウォールモードまたはルーテッドファイアウォールモード

この章では、ファイアウォールモードをルーテッドまたはトランスペアレントに設定する方法と、ファイアウォールが各ファイアウォールモードでどのように機能するかについて説明します。

マルチコンテキストモードでは、コンテキストごとに別個にファイアウォールモードを設定できます。

- [ファイアウォールモードについて \(207 ページ\)](#)
- [デフォルト設定 \(215 ページ\)](#)
- [ファイアウォールモードのガイドライン \(215 ページ\)](#)
- [ファイアウォールモード \(シングルモード\) の設定 \(216 ページ\)](#)
- [ファイアウォールモードの例 \(217 ページ\)](#)
- [ファイアウォールモードの履歴 \(228 ページ\)](#)

ファイアウォールモードについて

ASA は、ルーテッドファイアウォールモードとトランスペアレントファイアウォールモードの 2 つのファイアウォールモードをサポートします。

ルーテッドファイアウォールモードについて

ルーテッドモードでは、ASA はネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。コンテキスト間でレイヤ 3 インターフェイスを共有することもできます。

トランスペアレント ファイアウォール モードについて

従来、ファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルトゲートウェイとして機能します。これに対し、トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。ただし、他のファイアウォールのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

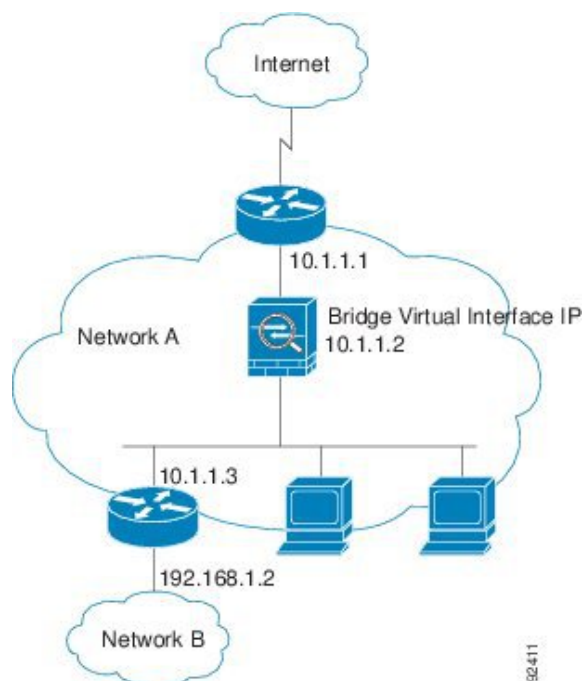
レイヤ2の接続は、ネットワークの内部と外部のインターフェイスをまとめた「ブリッジグループ」を使用して実現されます。また、ASAはブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジグループには、ネットワーク上でIPアドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互通信できません。

ネットワーク内でトランスペアレントファイアウォールの使用

ASAは、自身のインターフェイス間を同じネットワークで接続します。トランスペアレントファイアウォールはルーティングされたホップではないため、既存のネットワークに簡単に導入できます。

次の図に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレントファイアウォールネットワークを示します。内部ルータとホストは、外部ルータに直接接続されているように見えます。

図 20: トランスペアレントファイアウォールネットワーク



ブリッジグループについて

ブリッジグループは、ASA がルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレント ファイアウォールモードでのみサポートされています。他のファイアウォールインターフェイスのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

ブリッジ仮想インターフェイス (BVI)

各ブリッジグループには、ブリッジ仮想インターフェイス (BVI) が含まれます。ASA は、ブリッジグループから発信されるパケットの送信元アドレスとしてこの BVI IP アドレスを使用します。BVI IP アドレスは□ブリッジグループメンバー インターフェイスと同じサブネット上になければなりません。BVI では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

インターフェイス ベースの各機能はブリッジグループのメンバー インターフェイスだけを指定でき、これらについてのみ使用できます。

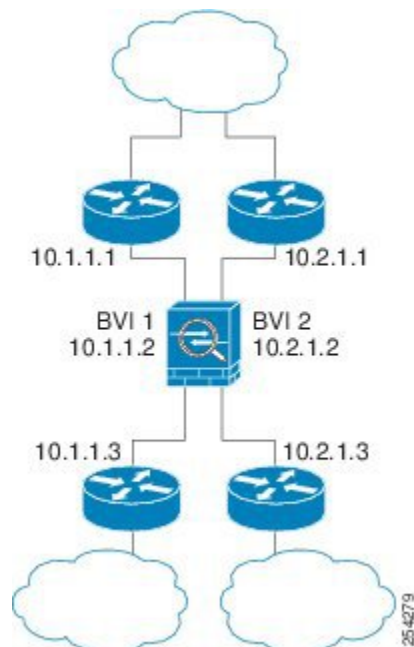
トランスペアレント ファイアウォールモードのブリッジグループ

ブリッジグループのトラフィックは他のブリッジグループから隔離され、トラフィックは ASA 内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジグループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジグループごとに分かれています。その他の多くの機能はすべてのブリッジグループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジグループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジグループにして、セキュリティ コンテキストを使用します。

1 つのブリッジグループにつき複数のインターフェイスを入れることができます。サポートされるブリッジグループとインターフェイスの正確な数については、[ファイアウォールモードのガイドライン \(215 ページ\)](#) を参照してください。ブリッジグループごとに 2 つ以上のインターフェイスを使用する場合は、内部、外部への通信だけでなく、同一ネットワーク上の複数のセグメント間の通信を制御できます。たとえば、相互通信を希望しない内部セグメントが 3 つある場合、インターフェイスを別々のセグメントに置き、外部インターフェイスとのみ通信させることができます。または、インターフェイス間のアクセスルールをカスタマイズし、希望通りのアクセスを設定できます。

次の図に、2 つのブリッジグループを持つ、ASA に接続されている 2 つのネットワークを示します。

図 21: 2つのブリッジグループを持つトランスペアレントファイアウォールネットワーク



管理 [インターフェイス (Interface)]

各ブリッジ仮想インターフェイス (BVI) IP アドレスのほかに、別の管理 スロット/ポート インターフェイスを追加できます。このインターフェイスはどのブリッジグループにも属さず、ASA への管理トラフィックのみを許可します。詳細については、[管理インターフェイス \(464 ページ\)](#) を参照してください。

レイヤ 3 トラフィックの許可

- ユニキャストの IPv4 および IPv6 トラフィックは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスに移動する場合、アクセスルールなしで自動的にブリッジグループを通過できます。
- セキュリティの低いインターフェイスからセキュリティの高いインターフェイスに移動するレイヤ 3 トラフィックの場合、セキュリティの低いインターフェイスでアクセスルールが必要です。
- ARP は、アクセスルールなしで両方向にブリッジグループを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。
- IPv6 ネイバー探索およびルータ送信要求パケットは、アクセスルールを使用して通過させることができます。
- ブロードキャストおよびマルチキャスト トラフィックは、アクセスルールを使用して通過させることができます。

許可される MAC アドレス

アクセス ポリシーで許可されている場合、以下の宛先 MAC アドレスをブリッジグループで使用できます（[レイヤ3 トラフィックの許可 \(210 ページ\)](#) を参照）。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャスト アドレス
- 0900.0700.0000 ～ 0900.07FF.FFFF までの AppleTalk マルチキャスト MAC アドレス

ルーテッドモードで許可されないトラフィックの通過

ルーテッドモードでは、アクセスルールで許可しても、いくつかのタイプのトラフィックは ASA を通過できません。ただし、ブリッジグループは、アクセスルール（IP トラフィックの場合）または EtherType ルール（非 IP トラフィックの場合）を使用してほとんどすべてのトラフィックを許可できます。

- IP トラフィック：ルーテッドファイアウォールモードでは、ブロードキャストとマルチキャストトラフィックは、アクセスルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミックルーティングプロトコルおよび DHCP（DHCP リレーを設定している場合を除く）が含まれます。ブリッジグループ内では、このトラフィックをアクセスルールで許可できます。
- 非 IP トラフィック：AppleTalk、IPX、BPDU や MPLS などは、EtherType ルールを使用することで、通過するように設定できます。



(注) ブリッジグループは、CDP パケットおよび 0x600 以上の有効な EtherType を持たないパケットの通過を拒否します。サポートされる例外は、BPDU および IS-IS です。

BPDU の処理

スパニングツリープロトコルの使用によるループを回避するために、デフォルトで BPDU が渡されます。BPDU をブロックするには、これらを拒否する EtherType ルールを設定する必要があります。フェールオーバーを使用している場合、BPDU をブロックして、トポロジが変更されたときにスイッチポートがブロッキングステートに移行することを回避できます。詳細については、「[フェールオーバーのトランスペアレントファイアウォールモードブリッジグループ要件 \(292 ページ\)](#)」を参照してください。

MAC アドレスとルートルックアップ

ブリッジグループ内のトラフィックでは、パケットの発信インターフェイスは、ルートルックアップではなく宛先 MAC アドレスルックアップを実行することによって決定されます。

ただし、次の場合にはルート ルックアップが必要です。

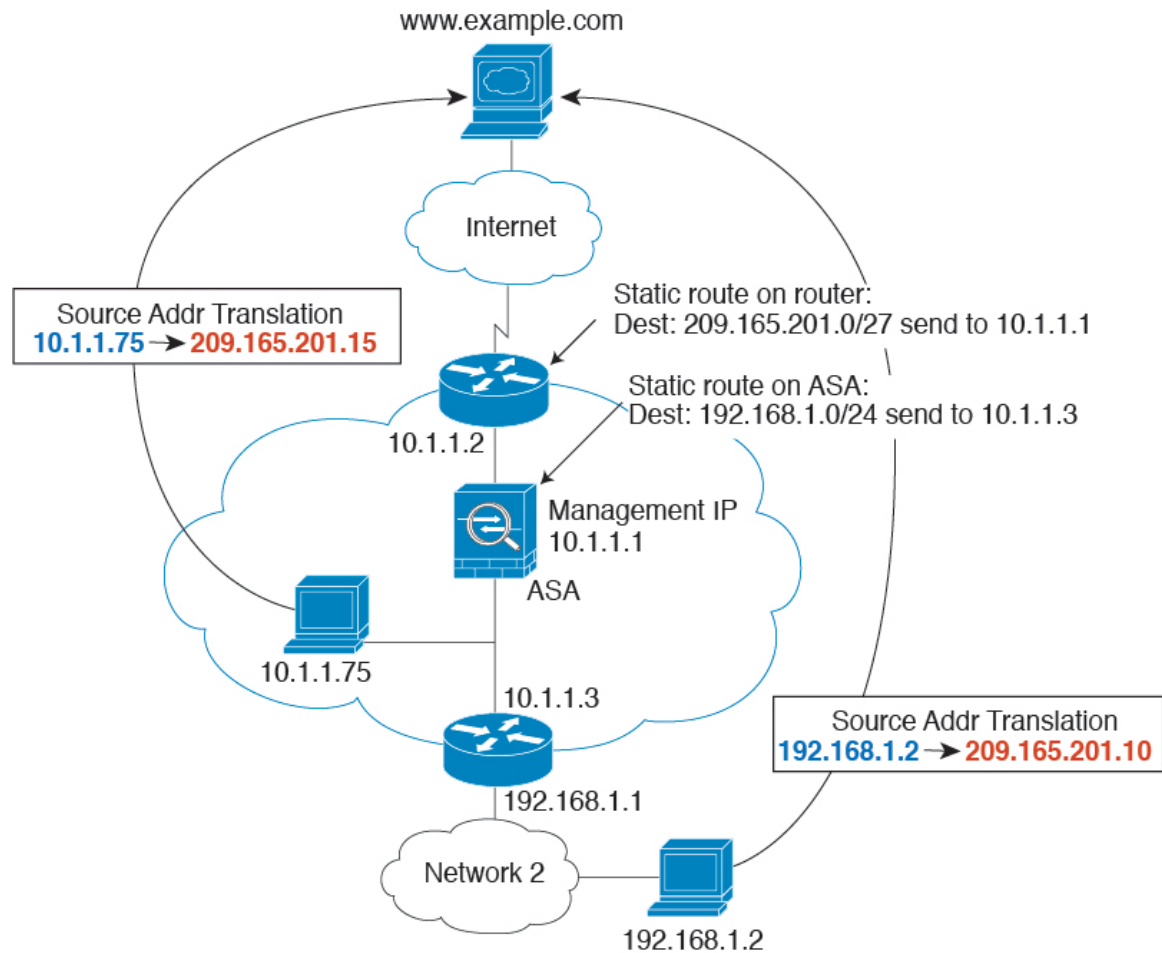
- トラフィックの発信元が ASA : syslog サーバなどがあるリモート ネットワーク宛でのトラフィック用に、ASA にデフォルト/スタティック ルートを追加します。
- インспекションが有効になっている Voice over IP (VoIP) および TFTP トラフィック、エンドポイントが1ホップ以上離れている：セカンダリ接続が成功するように、リモートエンドポイント宛でのトラフィック用に、ASA にスタティックルートを追加します。ASA は、セカンダリ接続を許可するためにアクセス コントロール ポリシーに一時的な「ピンホール」を作成します。セカンダリ接続ではプライマリ接続とは異なる IP アドレスのセットが使用される可能性があるため、ASA は正しいインターフェイスにピンホールをインストールするために、ルート ルックアップを実行する必要があります。

影響を受けるアプリケーションは次のとおりです。

- CTIQBE
 - GTP
 - H.323
 - MGCP
 - RTSP
 - SIP
 - Skinny (SCCP)
 - SQL*Net
 - SunRPC
 - TFTP
- ASA が NAT を実行する 1 ホップ以上離れたトラフィック：リモート ネットワーク宛でのトラフィック用に、ASA にスタティック ルートを設定します。また、ASA に送信されるマッピング アドレス宛でのトラフィック用に、上流に位置するルータにもスタティック ルートが必要です。

このルーティング要件は、インспекションと NAT が有効になっている VoIP と DNS の、1 ホップ以上離れている組み込み IP アドレスにも適用されます。ASA は、変換を実行できるように正しい出力インターフェイスを識別する必要があります。

図 22: NAT の例 : ブリッジグループ内の NAT



トランスペアレントモードのブリッジグループのサポートされていない機能

次の表に、トランスペアレントモードのブリッジグループでサポートされない機能を示します。

表 9: トランスペアレントモードでサポートされない機能

機能	説明
ダイナミック DNS	-

機能	説明
DHCP リレー	トランスペアレントファイアウォールは DHCPv4 サーバとして機能することができませんが、DHCP リレー コマンドはサポートしません。2つのアクセスルールを使用してDHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。1つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう1つはサーバからの応答を逆方向に許可します。
ダイナミック ルーティング プロトコル	ただし、ブリッジグループメンバーインターフェイスの場合、ASAで発信されたトラフィックにスタティック ルートを追加できます。アクセスルールを使用して、ダイナミックルーティングプロトコルがASAを通過できるようにすることもできます。
マルチキャスト IP ルーティング	アクセスルールで許可することによって、マルチキャストトラフィックがASAを通過できるようにすることができます。
QoS	—
通過トラフィック用のVPNターミネーション	トランスペアレントファイアウォールは、ブリッジグループメンバーインターフェイスでのみ、管理接続用のサイト間VPNトンネルをサポートします。これは、ASAを通過するトラフィックに対してVPN接続を終端しません。アクセスルールを使用してVPNトラフィックにASAを通過させることはできますが、非管理接続は終端されません。クライアントレスSSLVPNもサポートされていません。
ユニファイドコミュニケーション	—

ルーテッドモード機能のためのトラフィックの通過

トランスペアレントファイアウォールで直接サポートされていない機能の場合は、アップストリームルータとダウンストリームルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、アクセスルールを使用することによって、(サポートされていないDHCPリレー機能の代わりに)DHCPトラフィックを許可したり、IP/TVで作成されるようなマルチキャストトラフィックを許可したりできます。また、トランスペアレントファイアウォールを通過するルーティングプロトコル隣接関係を確立することもできます。つ

まり、OSPF、RIP、EIGRP、または BGP トラフィックをアクセスルールに基づいて許可できます。同様に、HSRP や VRRP などのプロトコルは ASA を通過できます。

デフォルト設定

デフォルト モード

デフォルト モードはルーテッドモードです。

ブリッジグループのデフォルト

デフォルトでは、すべての ARP パケットはブリッジグループ内で渡されます。

ファイアウォール モードのガイドライン

コンテキスト モードのガイドライン

コンテキストごとにファイアウォール モードを設定します。

ブリッジグループのガイドライン (トランスペアレントモード)

- 4 のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方の各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされませんが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホストサブネット (255.255.255.255) を設定することはできません。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- トランスペアレントモードでは、少なくとも 1 つのブリッジグループを使用し、データインターフェイスがブリッジグループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは ASA の他方側のルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジグループネットワークからの管理トラフィックにだけ適

用されます。これは、デフォルトルートはブリッジグループのインターフェイスとブリッジグループネットワークのルータ IP アドレスを指定しますが、ユーザは1つのデフォルトルートしか定義できないためです。複数のブリッジグループネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティックルートを指定する必要があります。

- トランスペアレントモードでは、PPPoE は管理インターフェイスでサポートされません。
- Bidirectional Forwarding Detection (BFD) エコーパケットは、ブリッジグループメンバを使用するときに、ASA を介して許可されません。BFD を実行している ASA の両側に2つのネイバーがある場合、ASA は BFD エコーパケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

その他のガイドラインと制限事項

- ファイアウォールモードを変更すると、多くのコマンドが両方のモードでサポートされていないため、ASA は実行コンフィギュレーションをクリアします。スタートアップコンフィギュレーションは変更されません。保存しないでリロードすると、スタートアップコンフィギュレーションがロードされて、モードは元の設定に戻ります。コンフィギュレーションファイルのバックアップについては、[ファイアウォールモード（シングルモード）の設定（216 ページ）](#) を参照してください。
- `firewall transparent` コマンドでモードを使用して変更するテキストコンフィギュレーションを ASA にダウンロードする場合、コマンドをコンフィギュレーションの先頭に配置してください。このコマンドが読み込まれるとすぐに ASA がモードを変更し、その後ダウンロードされたコンフィギュレーションを引き続き読み込みます。コマンドがコンフィギュレーションの後ろの方にあると、ASA はそのコマンドよりも前の位置に記述されているすべての行をクリアします。

ファイアウォールモード（シングルモード）の設定

この項では、CLI を使用してファイアウォールモードを変更する方法を説明します。シングルモードの場合およびマルチモードで現在接続されているコンテキスト（通常は管理コンテキスト）の場合は、ASDM でモードを変更できません。他のマルチモードのコンテキストでは、コンテキストごとに ASDM でモードを設定できます。[セキュリティコンテキストの設定（258 ページ）](#) を参照してください。



- (注) ファイアウォールモードを変更すると実行コンフィギュレーションがクリアされるので、他のコンフィギュレーションを行う前にファイアウォールモードを設定することをお勧めします。

始める前に

モードを変更すると、ASA は実行コンフィギュレーションをクリアします（詳細については、[ファイアウォールモードのガイドライン（215 ページ）](#) を参照してください）。

- 設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。
- モードを変更するには、コンソールポートで CLI を使用します。ASDM コマンドラインインターフェイスツールや SSH などの他のタイプのセッションを使用する場合、コンフィギュレーションがクリアされる時にそれが切断されるので、いずれの場合もコンソールポートを使用して ASA に再接続する必要があります。
- コンテキスト内でモードを設定します。



(注) 設定が削除された後にファイアウォールモードをトランスペアレントに設定し、ASDM への管理アクセスを設定するには、[ASDM アクセスの設定（36 ページ）](#) を参照してください。

手順

ファイアウォールモードをトランスペアレントに設定します。

firewall transparent

例：

```
ciscoasa(config)# firewall transparent
```

モードをルーテッドに変更するには、**no firewall transparent** コマンドを入力します。

(注) ファイアウォールモードの変更では確認は求められず、ただちに変更が行われます。

ファイアウォールモードの例

このセクションには、ルーテッドファイアウォールモードとトランスペアレントファイアウォールモードで、ASA を介してどのようにトラフィックが転送されるかを説明する例が含まれます。

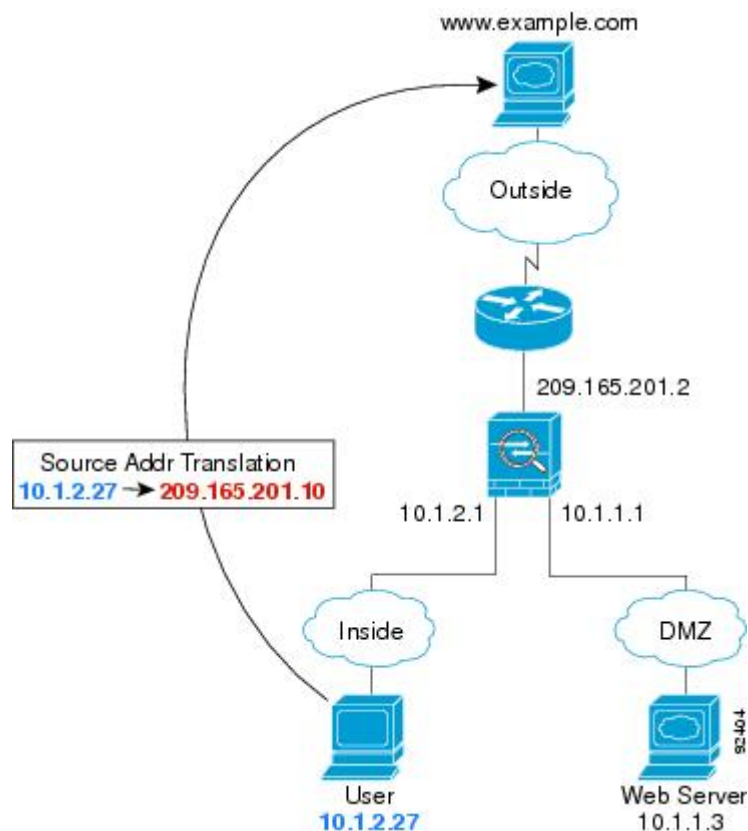
ルーテッドファイアウォールモードで ASA を通過するデータ

次のセクションでは、複数のシナリオのルーテッドファイアウォールモードで、データが ASA をどのように通過するかを示します。

内部ユーザが Web サーバにアクセスする

次の図は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 23: 内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーの条件に従って、パケットが許可されているか確認します。
マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASA は、実アドレス (10.1.2.27) をマップアドレス 209.165.201.10 に変換します。このマップアドレスは外部インターフェイスのサブネット上にあります。
マップアドレスは任意のサブネット上に設定できますが、外部インターフェイスのサブネット上に設定すると、ルーティングが簡素化されます。
4. 次に、ASA はセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. www.example.com が要求に応答すると、パケットは ASA を通過します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連する多くのルックアップ

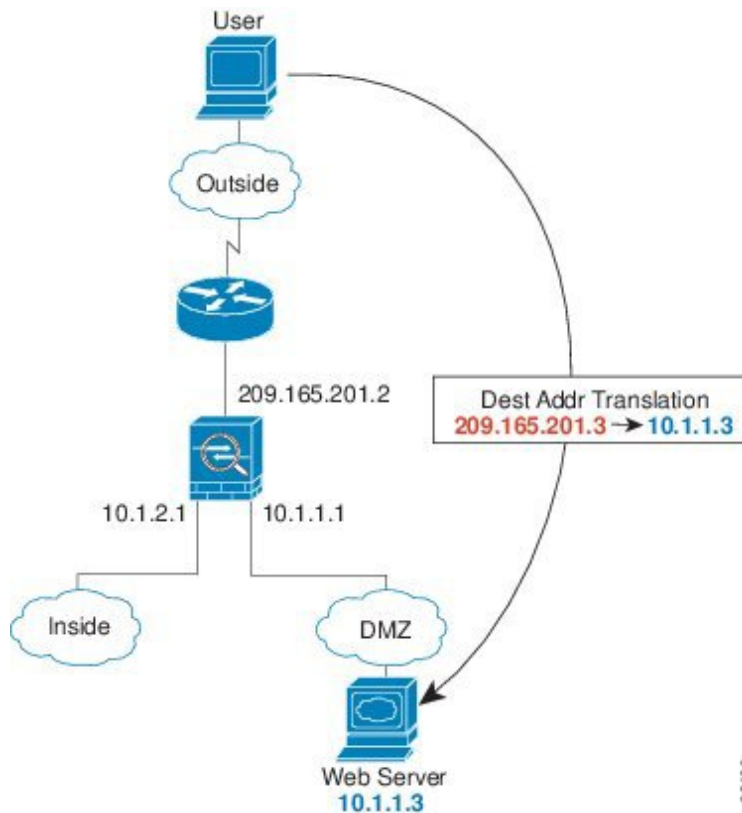
プをバイパスします。ASA は、グローバル宛先アドレスをローカルユーザアドレス 10.1.2.27 に変換せずに、NAT を実行します。

- ASA は、パケットを内部ユーザに転送します。

外部ユーザが DMZ 上の Web サーバにアクセスする

次の図は、外部ユーザが DMZ の Web サーバにアクセスしていることを示しています。

図 24: 外部から DMZ へ



次の手順では、データが ASA をどのように通過するかを示します。

- 外部ネットワーク上のユーザがマップアドレス 209.165.201.3 を使用して、DMZ 上の Web サーバに Web ページを要求します。これは、外部インターフェイスのサブネット上のアドレスです。
- ASA はパケットを受信し、マッピングアドレスは実アドレス 10.1.1.3 に変換しません。
- ASA は新しいセッションであるため、セキュリティポリシーの条件に従って、パケットが許可されていることを確認します。

マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。

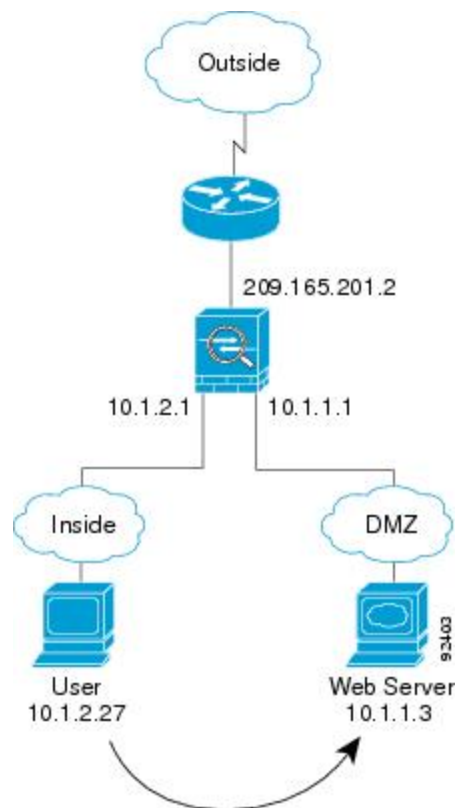
- 次に、ASA はセッションエントリを高速パスに追加し、DMZ インターフェイスからパケットを転送します。

- DMZ Web サーバが要求に応答すると、パケットはASAを通過します。また、セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。ASA は、実アドレスを 209.165.201.3 に変換することで NAT を実行します。
- ASAは、パケットを外部ユーザに転送します。

内部ユーザが DMZ 上の Web サーバにアクセスする

次の図は、内部ユーザが DMZ の Web サーバにアクセスしていることを示しています。

図 25: 内部から DMZ へ



次の手順では、データが ASA をどのように通過するかを示します。

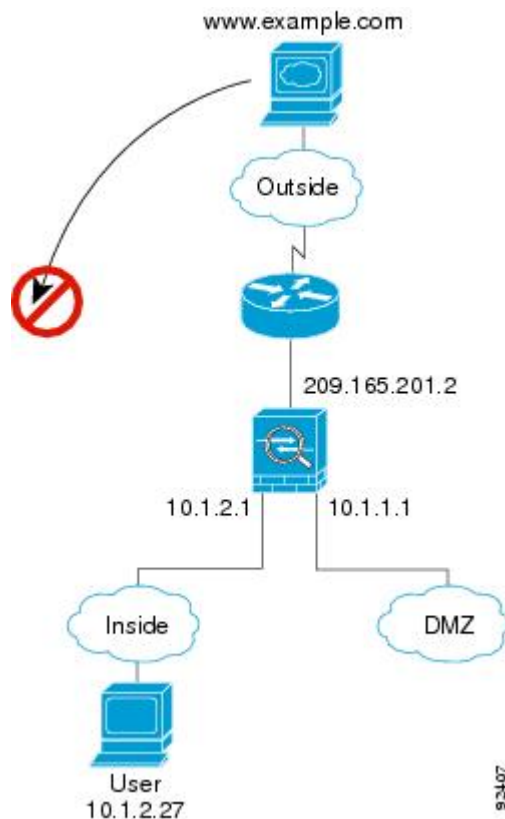
- 内部ネットワーク上のユーザは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバから Web ページを要求します。
- ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーの条件に従ってパケットが許可されているか確認します。
マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
- 次に、ASA はセッションが確立されたことを記録し、DMZ インターフェイスからパケットを転送します。

4. DMZ Web サーバが要求に応答すると、パケットは高速パスを通過します。このため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
5. ASAは、パケットを内部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

次の図は、外部ユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 26: 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

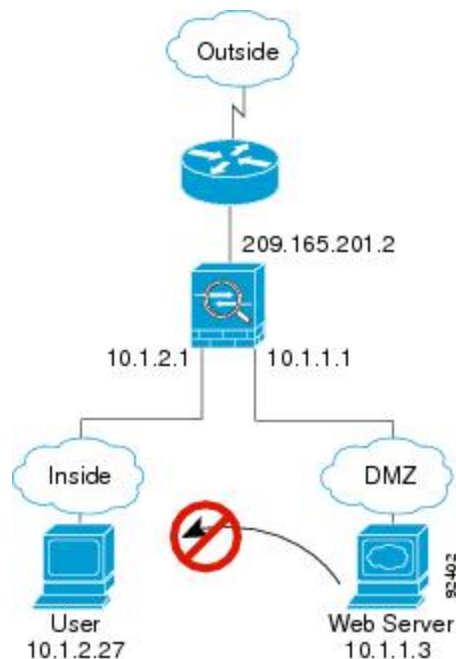
1. 外部ネットワーク上のユーザが、内部ホストに到達しようとし、ホストにルーティング可能な IP アドレスがあると想定します。
内部ネットワークがプライベートアドレスを使用している場合、外部ユーザが NAT なしで内部ネットワークに到達することはできません。外部ユーザは既存の NAT セッションを使用して内部ユーザに到達しようとするのが考えられます。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーに従って、パケットが許可されているか確認します。
3. パケットが拒否され、ASA はパケットをドロップし、接続試行をログに記録します。

外部ユーザが内部ネットワークを攻撃しようとした場合、ASAは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

DMZ ユーザによる内部ホストへのアクセスの試み

次の図は、DMZ 内のユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 27: DMZ から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

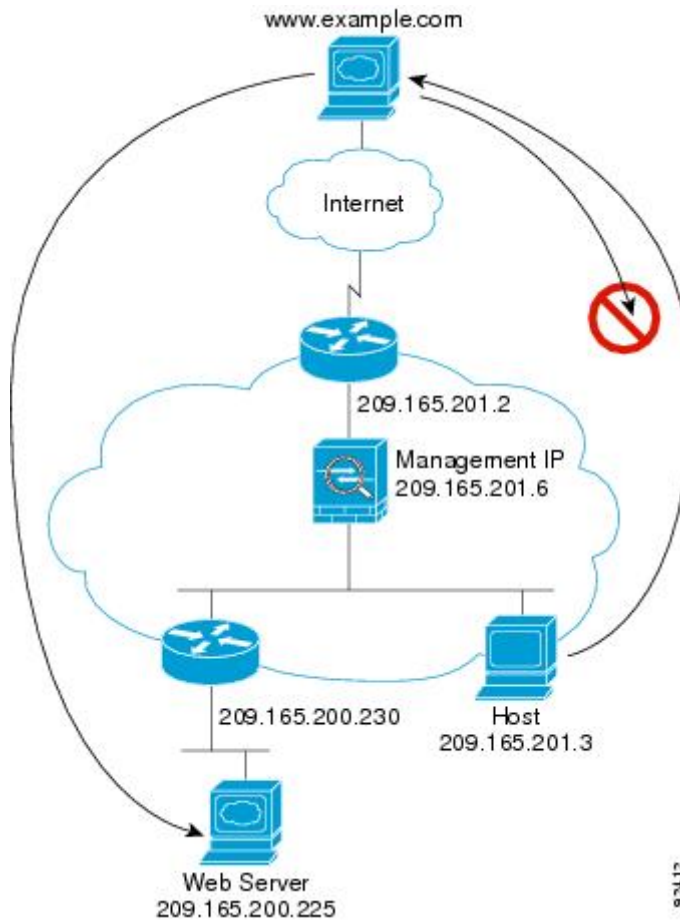
1. DMZ ネットワーク上のユーザが、内部ホストに到達しようとしています。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベートアドレッシング方式はルーティングを回避しません。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーに従って、パケットが許可されているか確認します。

パケットが拒否され、ASA はパケットをドロップし、接続試行をログに記録します。

トランスペアレント ファイアウォールを通過するデータの動き

次の図に、パブリック Web サーバを含む内部ネットワークを持つ一般的なトランスペアレント ファイアウォールの実装を示します。内部ユーザがインターネットリソースにアクセスできるように、ASA にはアクセスルールがあります。別のアクセスルールによって、外部ユーザは内部ネットワーク上の Web サーバだけにアクセスできます。

図 28:一般的なトランスパレント ファイアウォールのデータパス

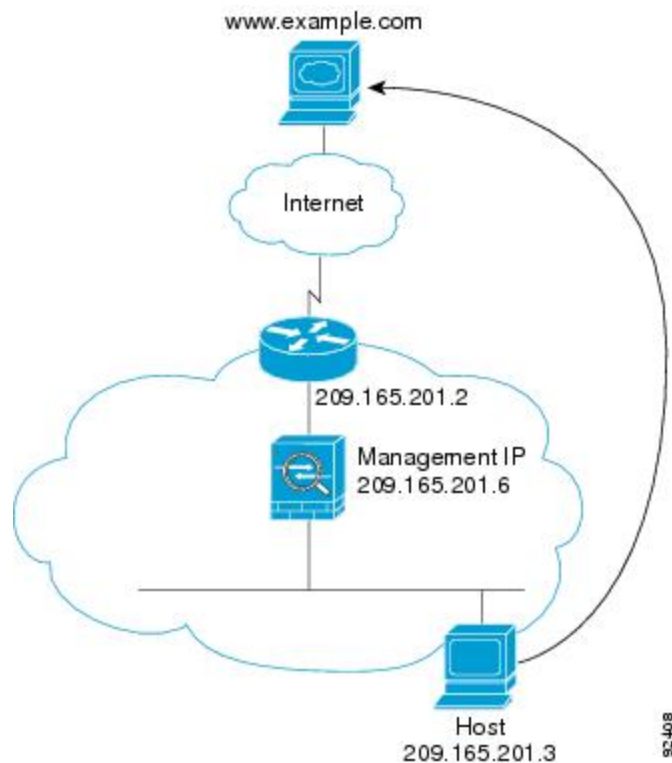


次のセクションでは、データが ASA をどのように通過するかを示します。

内部ユーザが Web サーバにアクセスする

次の図は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 29: 内部から外部へ



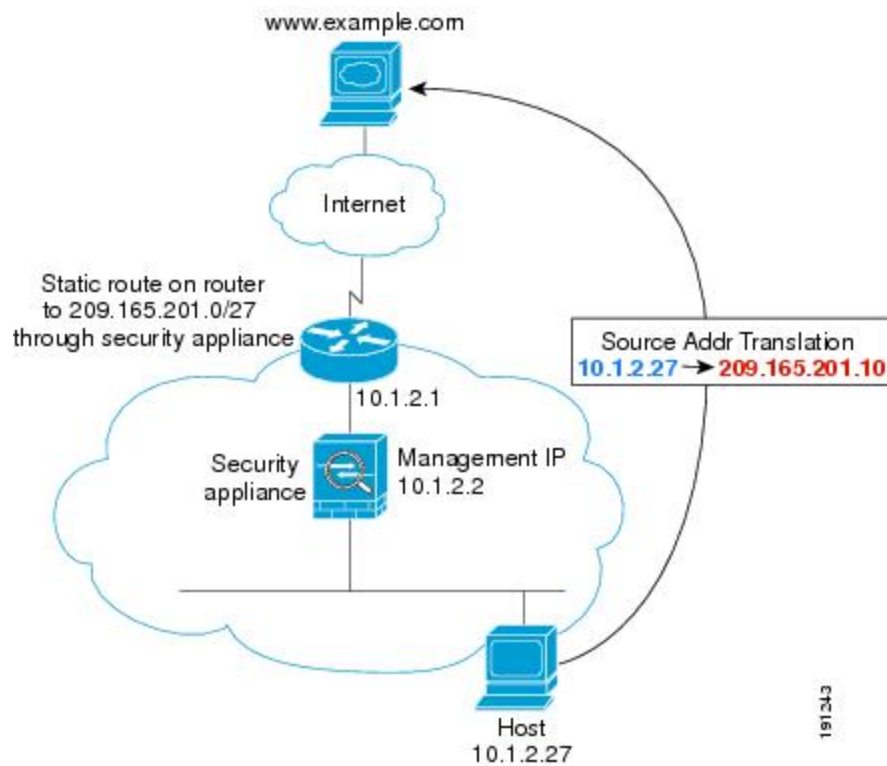
次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティポリシーの条件に従って、パケットが許可されていることを確認します。
マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASAは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASAは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.165.201.2 です。
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求または ping を送信します。最初のパケットはドロップされます。
5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのロックアップをバイパスします。
6. ASAは、パケットを内部ユーザに転送します。

NAT を使用して内部ユーザが Web サーバにアクセスする

次の図は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 30: NAT を使用して内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティポリシーの条件に従って、パケットが許可されていることを確認します。
マルチ コンテキスト モードの場合、ASAは、固有なインターフェイスに従ってパケットを分類します。
3. ASAは実際のアドレス (10.1.2.27) をマッピング アドレス 209.165.201.10 に変換します。
マッピングアドレスは外部インターフェイスと同じネットワーク上にないため、アップストリーム ルータにASAをポイントするマッピング ネットワークへのスタティック ルートがあることを確認します。
4. 次に、ASAはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. 宛先 MAC アドレスがテーブル内にある場合、ASAは外部インターフェイスからパケットを転送します。宛先MACアドレスは、アップストリームルータのアドレス 10.1.2.1 です。

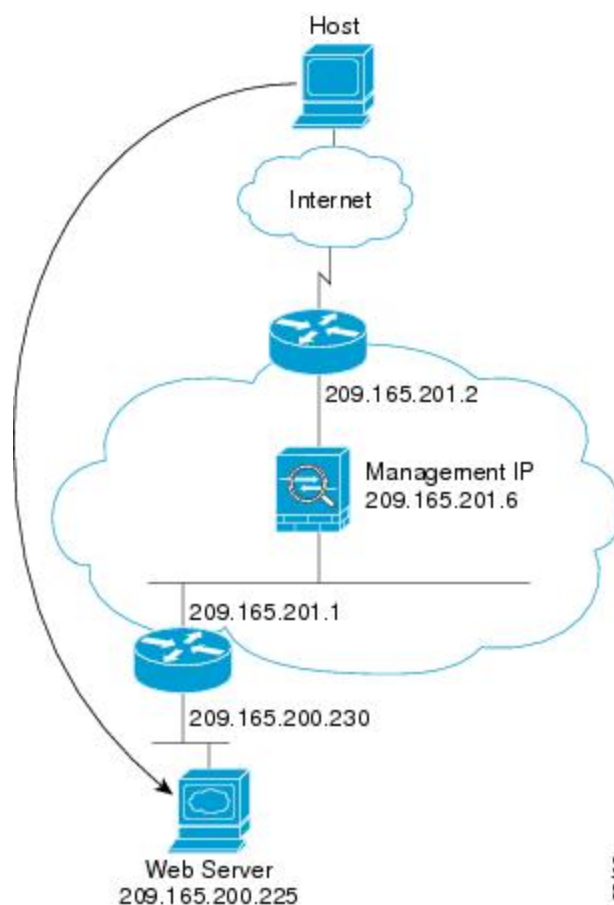
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

6. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
7. ASA は、マッピングアドレスを実際のアドレス 10.1.2.27 にせずに、NAT を実行します。

外部ユーザが内部ネットワーク上の Web サーバにアクセスする

次の図は、外部ユーザが内部の Web サーバにアクセスしていることを示しています。

図 31: 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザは、内部 Web サーバから Web ページを要求します。
2. ASA はパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティポリシーの条件に従って、パケットが許可されていることを確認します。

マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。

3. ASAは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASAは内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリームルータ 209.165.201.1 のアドレスです。

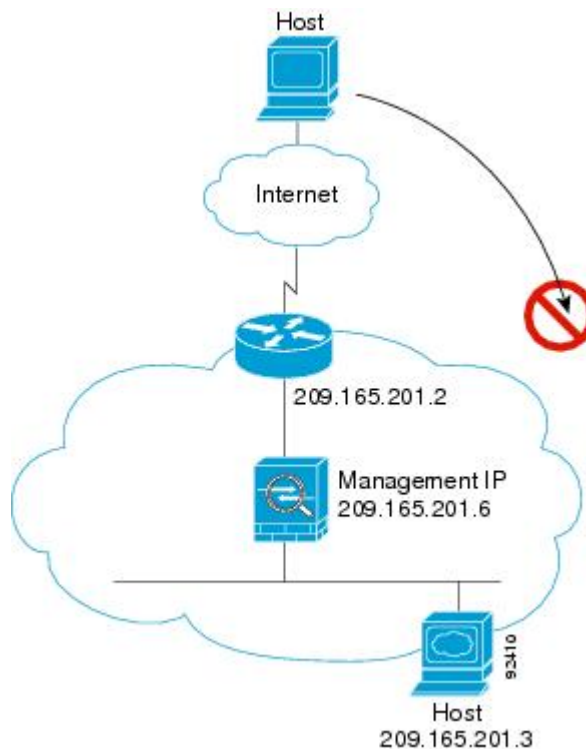
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. ASAは、パケットを外部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

次の図は、外部ユーザが内部ネットワーク上のホストにアクセスしようとしていることを示しています。

図 32: 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとしています。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティポリシーの条件に従って、パケットが許可されているか確認します。

マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。

3. 外部ホストを許可するアクセス ルールは存在しないため、パケットは拒否され、ASA によってドロップされます。
4. 外部ユーザが内部ネットワークを攻撃しようとした場合、ASA は多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

ファイアウォール モードの履歴

表 10: ファイアウォール モードの各機能履歴

機能名	プラットフォーム リリース	機能情報
トランスペアレントファイアウォールモード	7.0(1)	トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。 firewall transparent 、および show firewall コマンドが導入されました。 ASDM ではファイアウォールモードを設定できません。コマンドラインインターフェイスを使用する必要があります。

機能名	プラットフォーム リリース	機能情報
トランスペアレントファイアウォールブリッジグループ	8.4(1)	<p>セキュリティコンテキストのオーバーヘッドを避けたい場合、またはセキュリティコンテキストを最大限に使用したい場合、インターフェイスをブリッジグループにグループ化し、各ネットワークに1つずつ複数のブリッジグループを設定できます。ブリッジグループのトラフィックは他のブリッジグループから隔離されます。シングルモードでは最大8個、マルチモードではコンテキストあたり最大8個のブリッジグループを設定でき、各ブリッジグループには最大4個のインターフェイスを追加できます。</p> <p>(注) ASA 5505 に複数のブリッジグループを設定できますが、ASA 5505 のトランスペアレントモードのデータインターフェイスは2つという制限は、実質的にブリッジグループを1つだけ使用できることを意味します。</p> <p>次の画面が変更または導入されました。</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]</p>

機能名	プラットフォーム リリース	機能情報
マルチ コンテキスト モードのファイアウォールモードの混合がサポートされます。	8.5(1)/9.0(1)	<p>セキュリティ コンテキストごとに個別のファイアウォールモードを設定できます。したがってその一部をトランスペアレントモードで実行し、その他をルーテッドモードで実行することができます。</p> <p>firewall transparent コマンドが変更されました。</p> <p>シングルモードでは、ASDMでファイアウォールモードを設定することはできません。コマンドライン インターフェイスを使用する必要があります。</p> <p>マルチモードでは、次の画面が変更になりました。[Configuration] > [Context Management] > [Security Contexts]。</p>
トランスペアレントモードのブリッジグループの最大数が 250 に増加	9.3(1)	<p>ブリッジグループの最大数が8個から250個に増えました。シングルモードでは最大250個、マルチモードではコンテキストあたり最大8個のブリッジグループを設定でき、各ブリッジグループには最大4個のインターフェイスを追加できます。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]</p>



第 8 章

Startup Wizard

この章では、ASDM Startup Wizard について説明します。このウィザードでは、手順に従って Cisco ASA の初期設定を行い、基本設定を定義できます。

- [Startup Wizard へのアクセス](#) (231 ページ)
- [Startup Wizard のガイドライン](#) (231 ページ)
- [Startup Wizard の画面](#) (231 ページ)
- [Startup Wizard の履歴](#) (235 ページ)

Startup Wizard へのアクセス

Startup Wizard にアクセスするには、以下のいずれかのオプションを選択します。

- [Wizards] > [Startup Wizard] を選択する。
- [Configuration] > [Device Setup] > [Startup Wizard] を選択して、[Launch Startup Wizard] をクリックする。

Startup Wizard のガイドライン

コンテキスト モードのガイドライン

Startup Wizard はシステム コンテキストではサポートされません。

Startup Wizard の画面

画面の実際の順序は、設定時の選択によって決まります。特に明記していない限り、各画面はすべてのモードまたはモデルで使用できます。

開始点またはウェルカム

- 既存の設定を変更するには、[Modify existing configuration] オプションボタンをクリックします。
- 設定を工場出荷時のデフォルト値に設定するには、[Reset configuration to factory defaults] オプション ボタンをクリックします。
 - Management 0/0 インターフェイスの IP アドレスとサブネット マスクをデフォルト値 (192.168.1.1) と異なる値に設定するには、[Configure the IP address of the management interface] チェックボックスをオンにします。



(注) 設定を工場出荷時のデフォルト値にリセットすると、[Cancel] をクリックしたり、この画面を閉じたりしても、変更を元に戻せません。

マルチ コンテキスト モードでは、この画面にパラメータは含まれていません。

基本設定

この画面では、ホスト名、ドメイン名、およびイネーブルパスワードを設定します。

インターフェイスの画面

インターフェイスの画面は、選択したモードとモデルによって異なります。

外部インターフェイスの設定 (ルーテッド モード)

- Outside インターフェイス (セキュリティ レベルが最も低いインターフェイス) の IP アドレスを設定します。
- IPv6 アドレスを設定します。

外部インターフェイスの設定 - PPPoE (ルーテッド モード、シングル モード)

Outside インターフェイスの PPPoE 設定を行います。

Management IP Address Configuration (トランスペアレント モード)

IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方の各ブリッジグループに対し、管理 IP アドレスが必要です。この画面では、BVI 1 の IP アドレスを設定します。

その他のインターフェイスの設定

その他のインターフェイスのパラメータを設定します。

スタティック ルート

スタティック ルートを設定します。

DHCP サーバ

DHCP サーバを設定します。

アドレス変換 (NAT/PAT)

外部（セキュリティレベルが最も低いインターフェイス）にアクセスするときの内部アドレス（セキュリティレベルが最も高いインターフェイス）の NAT または PAT を設定します。詳細については、ファイアウォールの設定ガイドを参照してください。

管理アクセス

- ASDM、Telnet、または SSH アクセスを設定します。
- ASDM にアクセスするための HTTP サーバへのセキュアな接続をイネーブルにするには、[Enable HTTP server for HTTPS/ASDM access] チェックボックスをオンにします。
- [Enable ASDM history metrics] チェックボックスをオンにします。

IPS の基本設定

シングル コンテキスト モードでは、ASDM で Startup Wizard を使用して、基本的な IPS ネットワーク設定を行います。これらの設定は、コンフィギュレーションではなく ASA コンフィギュレーションに保存されます。詳細については、IPS のクイック スタートガイドを参照してください。

ASA CX の基本設定 (ASA 5585-X)

ASDM の Startup Wizard を使用して、ASA CX の管理アドレスおよび Auth Proxy Port を設定できます。これらの設定は、ASA コンフィギュレーションではなく、ASACX コンフィギュレーションに保存されます。ASA CX CLI での追加のネットワーク設定も必要です。この画面に関する詳細については、『ASA CX クイック スタートガイド』を参照してください。

ASA FirePOWER の基本設定

ASDM の Startup Wizard を使用して、ASA FirePOWER の管理アドレス情報を設定し、エンドユーザライセンス契約 (EULA) を承認することができます。これらの設定は、ASA コンフィギュレーションではなく、ASA FirePOWER コンフィギュレーションに保存されます。ASA FirePOWER CLI でも、いくつかの設定を行う必要があります。詳細については、ファイアウォールの設定ガイドの ASA FirePOWER モジュールに関する章を参照してください。

タイムゾーンおよびクロック コンフィギュレーション

時計のパラメータを設定します。

Auto Update サーバ (シングルモード)

これらのガイドラインに従って Auto Update サーバを設定します。

- [Enable Auto Update Server for ASA] チェックボックスをオンにして、Auto Update サーバを設定します。
- IPS モジュールがある場合は、[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにします。次の追加パラメータを設定します。
 - Cisco.com のユーザ名とパスワードを入力し、確認のためにパスワードを再入力します。
 - 24 時間制を使用して、hh:mm:ss 形式で開始時間を入力します。

スタートアップウィザードの概要

この画面には、ASA に対して行ったすべての設定の概要が表示されます。

- 前の画面での設定を変更するには、[Back] をクリックします。
- 次のいずれかを選択します。
 - スタートアップウィザードをブラウザから直接起動した場合は、[Finish] をクリックすると、ウィザードで作成された構成時の設定が ASA に自動的に送信され、フラッシュメモリに保存されます。
 - ASDM 内でスタートアップウィザードを実行した場合は、[File] > [Save Running Configuration to Flash] を選択し、その設定を明示的にフラッシュメモリに保存する必要があります。

Startup Wizard の履歴

表 11 : Startup Wizard の履歴

機能名	プラットフォーム リリース	説明
スタートアップ ウィザード	7.0(1)	このウィザードが導入されました。 [Wizards] > [Startup Wizard] 画面が導入されました。
ASA IPS の設定	8.4(1)	ASA IPS モジュールでは、[IPS Basic Configuration] 画面が Startup Wizard に追加されました。IPS モジュールに対するシグニチャアップデートが、[Auto Update] 画面に追加されました。ASA でクロックが設定されるように、[Time Zone and Clock Configuration] 画面が追加されました。IPS モジュールはそのクロックを ASA から取得します。 次の画面が導入または変更されました。 [Wizards] > [Startup Wizard] > [IPS Basic Configuration] [Wizards] > [Startup Wizard] > [Auto Update] [Wizards] > [Startup Wizard] > [Time Zone and Clock Configuration]
ASA CX の設定	9.1(1)	ASA CX モジュールでは、[ASA CX Basic Configuration] 画面が Startup Wizard に追加されました。 次の画面が導入されました。 [Wizards] > [Startup Wizard] > [ASA CX Basic Configuration]
ASA FirePOWER の設定	9.2(2.4)	ASA FirePOWER モジュールでは、[ASA FirePOWER Basic Configuration] 画面が Startup Wizard に追加されました。 次の画面が導入されました。 [Wizards] > [Startup Wizard] > [ASA FirePOWER Basic Configuration]



第 II 部

ハイアベイラビリティとスケールビリティ

- [マルチコンテキストモード \(239 ページ\)](#)
- [ハイアベイラビリティのためのフェールオーバー \(275 ページ\)](#)
- [ASA クラスタ \(331 ページ\)](#)
- [Firepower 9300 シャーシの ASA クラスタ \(421 ページ\)](#)



第 9 章

マルチ コンテキスト モード

この章では、Cisco ASA でマルチセキュリティ コンテキストの設定方法について説明します。

- [セキュリティ コンテキストについて \(239 ページ\)](#)
- [マルチ コンテキスト モードのライセンス \(250 ページ\)](#)
- [マルチ コンテキスト モードの前提条件 \(252 ページ\)](#)
- [マルチ コンテキスト モードのガイドライン \(252 ページ\)](#)
- [マルチ コンテキスト モードのデフォルト \(253 ページ\)](#)
- [マルチ コンテキスト の設定 \(253 ページ\)](#)
- [コンテキスト とシステム実行スペースの切り替え \(262 ページ\)](#)
- [セキュリティ コンテキスト の管理 \(262 ページ\)](#)
- [セキュリティ コンテキスト のモニタリング \(266 ページ\)](#)
- [マルチ コンテキスト モードの履歴 \(269 ページ\)](#)

セキュリティ コンテキスト について

単一の ASA は、セキュリティ コンテキスト と呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスとして機能します。マルチコンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでサポートされない機能については、[マルチ コンテキスト モードのガイドライン \(252 ページ\)](#) を参照してください。

この項では、セキュリティ コンテキスト の概要について説明します。

セキュリティ コンテキスト の一般的な使用方法

マルチセキュリティ コンテキスト を使用する状況には次のようなものがあります。

- サービス プロバイダーとして、多数のカスタマーにセキュリティ サービスを販売する。ASA 上でマルチ セキュリティ コンテキスト を有効にすることによって、費用対効果の高い、省スペースソリューションを実装できます。このソリューションでは、カスタマーのトラフィックすべての分離とセキュリティが確保され、設定も容易です。

- 大企業または広大な大学の構内で、各部門の完全な独立を維持する必要がある。
- 企業で、部門ごとに個別のセキュリティ ポリシーの提供が求められている。
- 複数の ASA が必要なネットワークを使用する場合。

コンテキストコンフィギュレーションファイル

この項では、ASA がマルチ コンテキスト モードのコンフィギュレーションを実装する方法について説明します。

コンテキストコンフィギュレーション

コンテキストごとに、ASA の中に 1 つのコンフィギュレーションがあり、この中ではセキュリティ ポリシーやインターフェイスに加えて、スタンドアロンデバイスで設定できるすべてのオプションが指定されています。コンテキストコンフィギュレーションはフラッシュメモリ内に保存することも、TFTP、FTP、または HTTP (S) サーバからダウンロードすることもできます。

システム設定

システム管理者は、各コンテキストコンフィギュレーションの場所、割り当てられたインターフェイス、およびその他のコンテキスト操作パラメータをシステムコンフィギュレーションに設定することで、コンテキストを追加および管理します。このコンフィギュレーションは、シングルモードのコンフィギュレーション同様、スタートアップコンフィギュレーションです。システムコンフィギュレーションは、ASA の基本設定を識別します。システムコンフィギュレーションには、ネットワークインターフェイスやネットワーク設定は含まれません。その代わりに、ネットワークリソースにアクセスする必要があるときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。システムコンフィギュレーションに含まれているものに、フェールオーバートラフィック専用の特殊なフェールオーバーインターフェイスがあります。

管理コンテキストの設定

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システムコンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザに制限する必要があります。管理コンテキストは、リモートではなくフラッシュメモリに置く必要があります。

システムがすでにマルチ コンテキスト モードになっている場合、またはシングルモードから変換された場合、管理コンテキストが `admin.cfg` と呼ばれるファイルとして内部フラッシュメモリに自動的に作成されます。このコンテキストの名前は "admin" です。admin.cfg を管理コンテキストとして使用しない場合は、管理コンテキストを変更できます。

ASA がパケットを分類する方法

ASA に入ってくるパケットはいずれも分類する必要があります。その結果、ASA は、どのコンテキストにパケットを送信するかを決定できます。



- (注) 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製され、各コンテキストに送信されます。

有効な分類子基準

この項では、分類子で使用される基準について説明します。



- (注) インターフェイス宛の管理トラフィックでは、インターフェイス IP アドレスが分類に使用されます。

ルーティング テーブルはパケット分類には使用されません。

固有のインターフェイス

入力インターフェイスに関連付けられているコンテキストが1つだけの場合、ASA はパケットをそのコンテキストに分類します。トランスペアレント ファイアウォール モードでは、各コンテキストに固有のインターフェイスが必要なため、この方法は、常にパケット分類の目的で使用されます。

固有の MAC アドレス

複数のコンテキストが同じインターフェイスを共有している場合は、各コンテキストでそのインターフェイスに割り当てられた一意の MAC アドレスが分類子で使用されます。固有の MAC アドレスがないと、アップストリーム ルータはコンテキストに直接ルーティングできません。MAC アドレスの自動生成を有効にできます。各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。

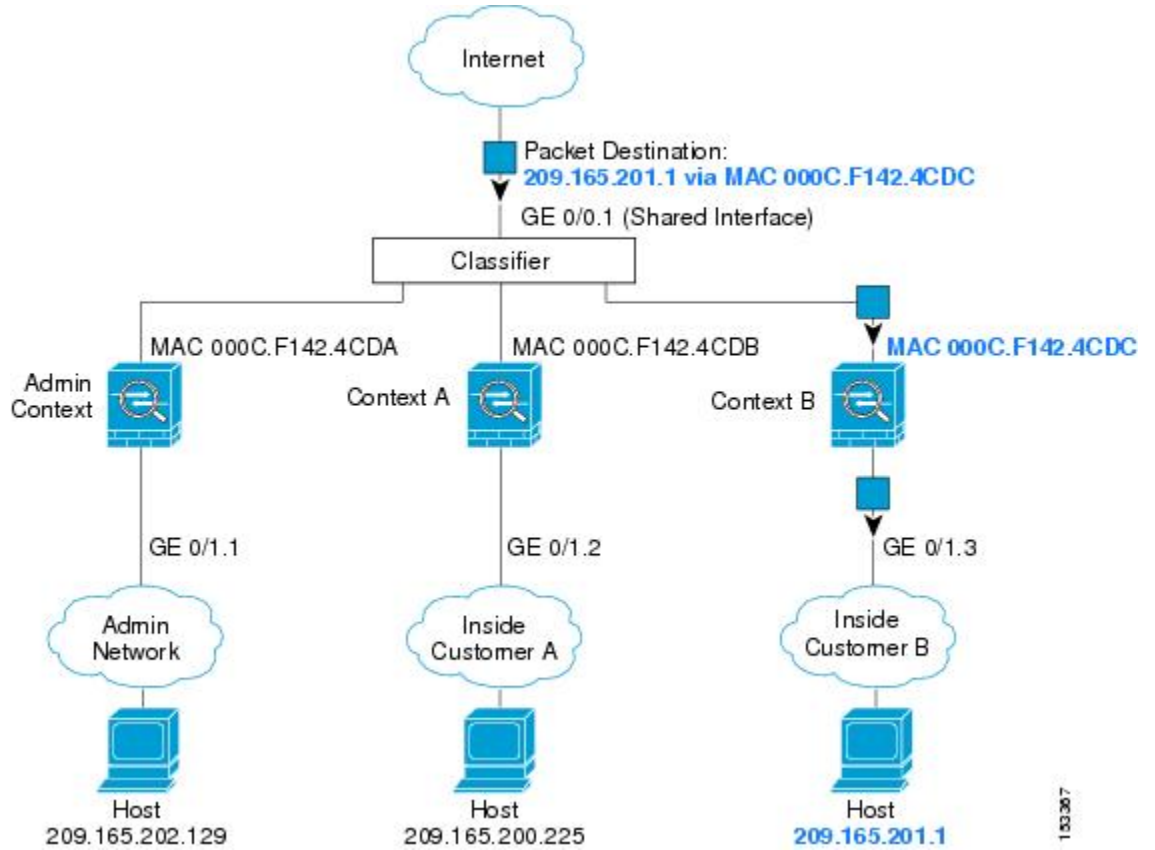
NAT の設定

固有の MAC アドレスの使用を有効にしなければ、ASA は、NAT コンフィギュレーション内のマッピングされたアドレスを使用してパケットを分類します。NAT コンフィギュレーションの完全性に関係なくトラフィック分類を行うことができるように、NAT ではなく MAC アドレスを使用することをお勧めします。

分類例

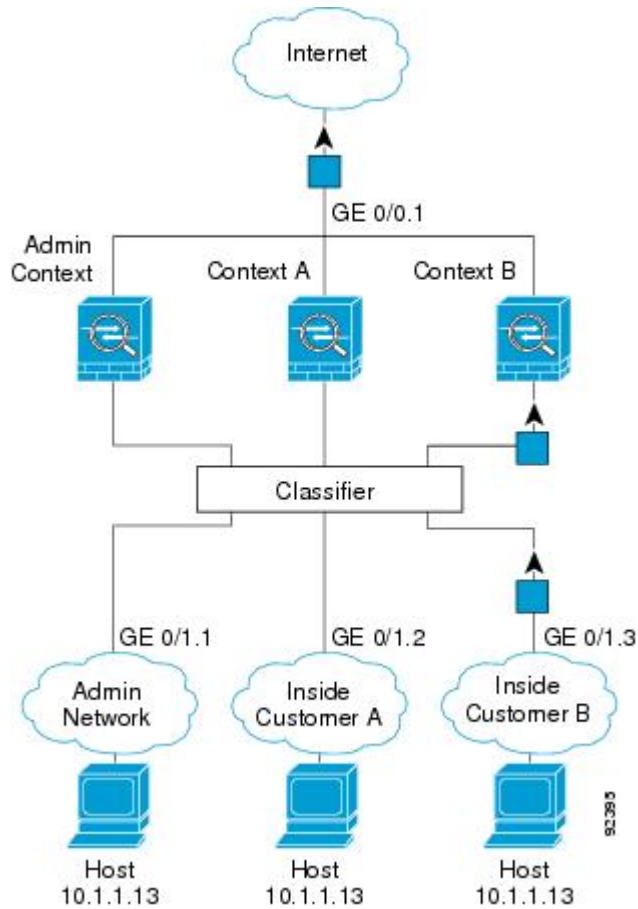
次の図に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 33: MAC アドレスを使用した共有インターフェイスのパケット分類



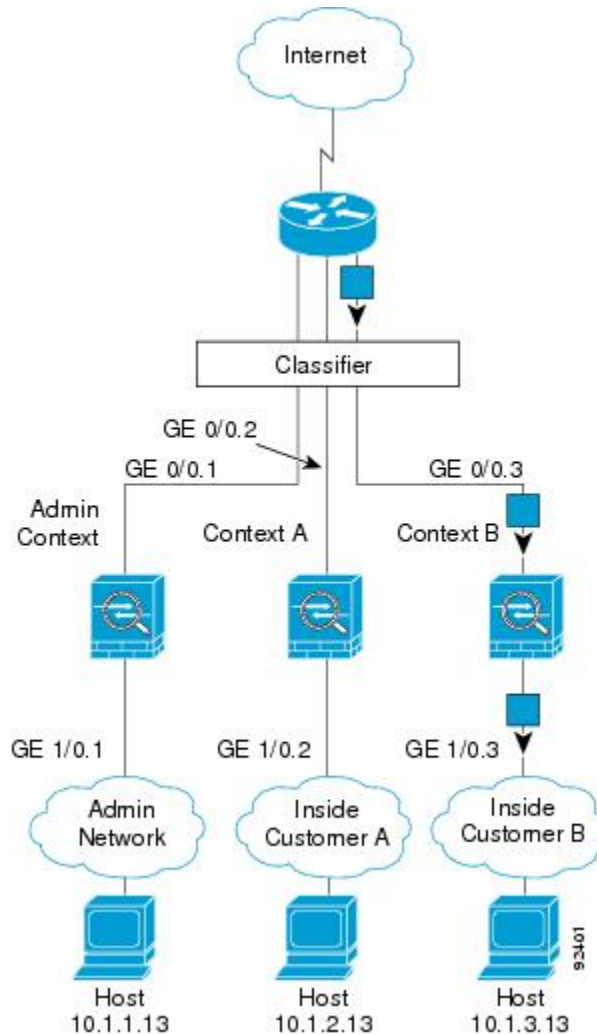
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のコンテキストBのホストを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビットイーサネット 0/1.3 で、このイーサネットがコンテキストBに割り当てられているためです。

図 34: 内部ネットワークからの着信トラフィック



トランスパレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のコンテキストBのホストに向けられたインターネットからのパケットを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビットイーサネット 1/0.3 で、このイーサネットがコンテキストBに割り当てられているためです。

図 35: トランスペアレントファイアウォールコンテキスト



セキュリティコンテキストのカスケード接続

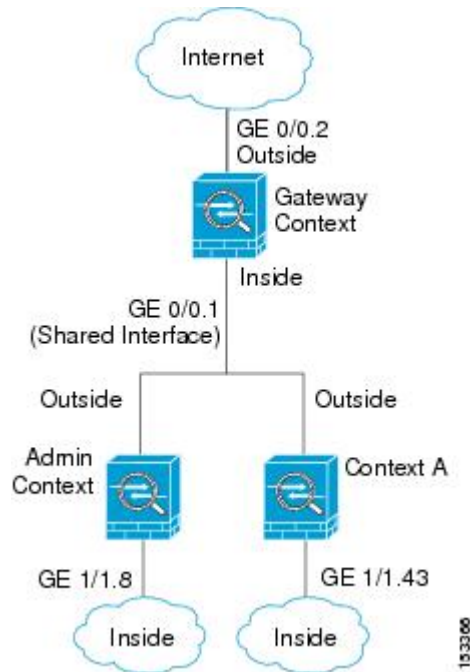
コンテキストを別のコンテキストのすぐ前に置くことを、コンテキストをカスケード接続するといいます。一方のコンテキストの外部インターフェイスは、他方のコンテキストの内部インターフェイスと同じインターフェイスです。いくつかのコンテキストのコンフィギュレーションを単純化する場合、最上位のコンテキストの共有パラメータを設定することで、コンテキストをカスケード接続できます。



- (注) コンテキストをカスケード接続するには、各コンテキストインターフェイスに固有の MAC アドレスが必要です。MAC アドレスのない共有インターフェイスの packets を分類するには限界があるため、固有の MAC アドレスを設定しないでコンテキストのカスケード接続を使用することはお勧めしません。

次の図に、ゲートウェイの背後に2つのコンテキストがあるゲートウェイ コンテキストを示します。

図 36: コンテキストのカスケード接続



セキュリティ コンテキストへの管理アクセス

ASA では、マルチ コンテキスト モードでのシステム管理アクセスと、各コンテキスト管理者のアクセスを提供します。次の各項では、システム管理者またはコンテキスト管理者としてのログインについて説明します。

システム管理者のアクセス

2つの方法で、システム管理者として ASA をアクセスできます。

- ASA コンソールにアクセスする。

コンソールからシステム実行スペースにアクセスします。この場合、入力したコマンドは、システム コンフィギュレーションまたはシステムの実行 (run-time コマンド) だけに影響します。

- Telnet、SSH、または ASDM を使用して管理コンテキストにアクセスする

システム管理者として、すべてのコンテキストにアクセスできます。

システム実行スペースでは AAA コマンドはサポートされていませんが、個別のログインのために、固有のイネーブルパスワードおよびユーザ名をローカル データベースに設定することができます。

コンテキスト管理者のアクセス

Telnet、SSH、または ASDM を使用して、コンテキストにアクセスできます。管理外コンテキストにログインすると、アクセスできるのはそのコンテキストのコンフィギュレーションだけになります。そのコンテキストに個別のログインを付与できます。

リソース管理の概要

デフォルトでは、すべてのセキュリティ コンテキストは ASA のリソースに無制限でアクセスできますが、コンテキストあたりの上限が定められている場合を除きます。唯一の例外は、VPN のリソース（デフォルトでディセーブルになっています）です。特定のコンテキストが使用しているリソースが多すぎることが原因で、他のコンテキストが接続を拒否されるといった現象が発生した場合は、コンテキストあたりのリソースの使用量を制限するようにリソース管理を設定できます。VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

リソース クラス

ASA は、リソースクラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。クラスの設定を使用するには、コンテキストを定義するときに、そのコンテキストをクラスに割り当てます。すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルトクラスに属します。したがって、コンテキストをデフォルト クラスに割り当てる必要は特にありません。コンテキストは1つのリソースクラスにだけ割り当てることができます。このルール例外は、メンバクラスで未定義の制限はデフォルト クラスから継承されることです。そのため実際には、コンテキストがデフォルト クラスおよび別のクラスのメンバになります。

リソース制限値

個々のリソースの制限値は、パーセンテージ（ハードシステム制限がある場合）または絶対値として設定できます。

ほとんどのリソースについては、ASA はクラスに割り当てられたコンテキストごとにリソースの一部を確保することはしません。代わりに、ASA はコンテキストごとに上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。例外は、VPN リソース タイプです。このリソースはオーバーサブスクライブできないため、各コンテキストに割り当てられたリソースは保証されます。割り当てられた量を超える、VPN セッションの一時的なバーストに対応できるように、ASA は「burst」という VPN リソース タイプをサポートしています。このリソースは、残りの未割り当て VPN セッションに等しくなります。バーストセッションはオーバーサブスクライブでき、コンテキストが先着順で使用できます。

デフォルト クラス

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルトクラスに属します。コンテキストをデフォルトクラスに積極的に割り当てる必要はありません。

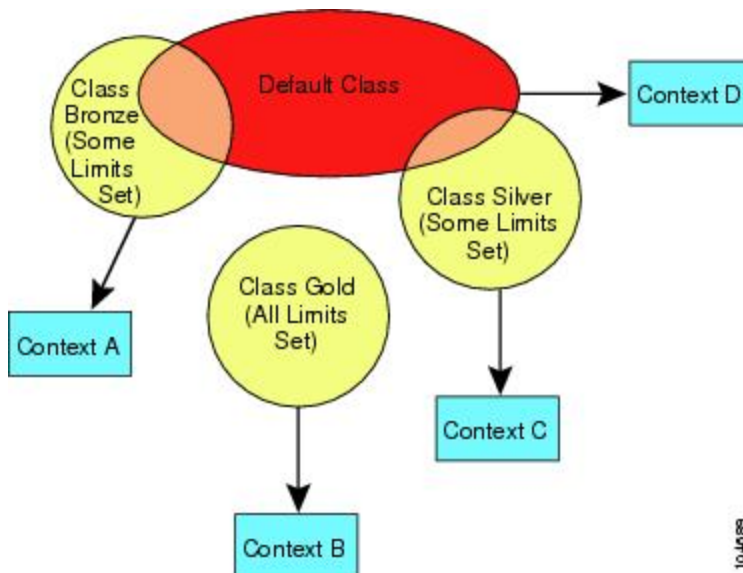
コンテキストがデフォルトクラス以外のクラスに属する場合、それらのクラス設定は常にデフォルトクラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバコンテキストはそれらの制限にデフォルトクラスを使用します。たとえば、すべての同時接続に2%の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルトクラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルトクラスの設定を何も使用しません。

ほとんどのリソースについては、デフォルトクラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- Telnet セッション：5 セッション。（コンテキストあたりの最大値）。
- SSH セッション：5 セッション。（コンテキストあたりの最大値）。
- IPsec セッション：5 セッション。（コンテキストあたりの最大値）。
- MAC アドレス：65,535 エントリ。（システムの最大値）。
- VPN サイトツーサイト トンネル：0 セッション（VPN セッションを許可するようにクラスを手動で設定する必要があります）。

次の図に、デフォルトクラスと他のクラスの関係を示します。コンテキスト A および C は、いくつかの制限が設定されたクラスに属しており、それ以外の制限はデフォルトクラスから継承します。コンテキスト B は、属している Gold クラスですべての制限が設定されているため、デフォルトクラスから制限値を継承しません。コンテキスト D はクラスに割り当てられなかったため、デフォルトでデフォルトクラスのメンバになります。

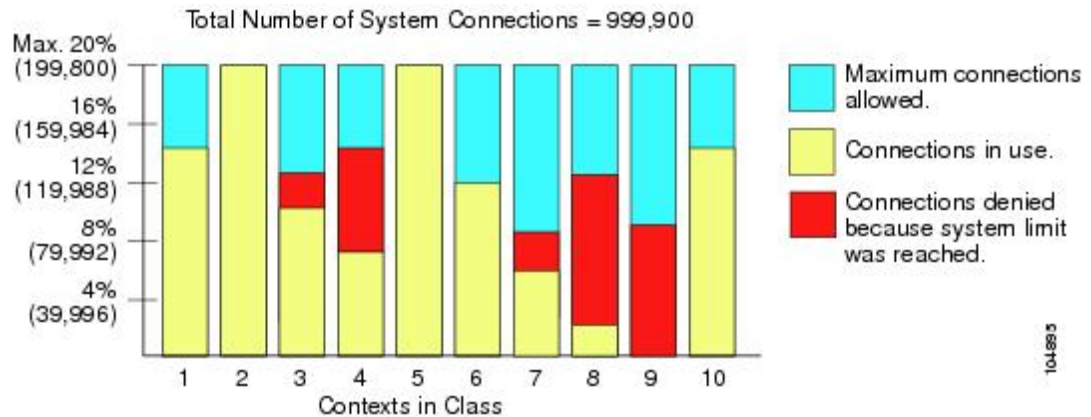
図 37: リソースクラス



オーバーサブスクライプ リソースの使用

ASA をオーバーサブスクライプするには、割り当て率の合計が 100% を超えるようにあるリソースをすべてのコンテキストに割り当てます（非バーストの VPN リソースを除く）。たとえば、接続がコンテキストあたり 20% までに制限されるように Bronze クラスを設定し、それから 10 個のコンテキストをそのクラスに割り当てれば、リソースの合計を 200% にできます。コンテキストがシステム制限を超えて同時に使用する場合、各コンテキストは意図した 20% を下回ります。

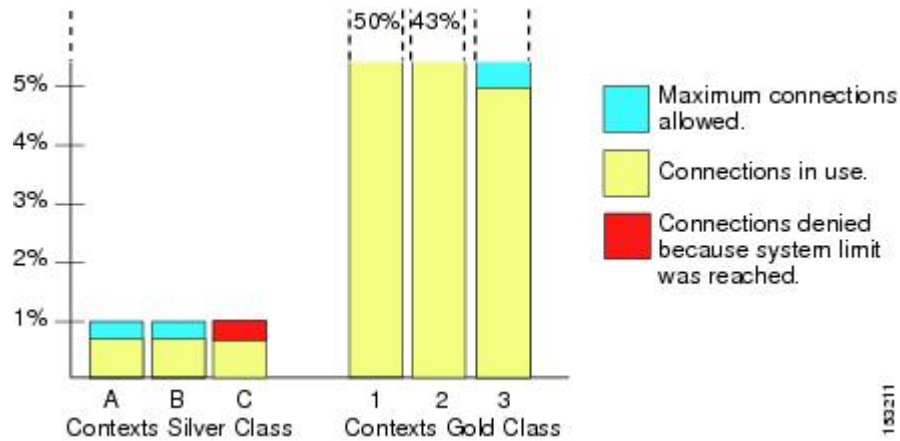
図 38: リソース オーバーサブスクリプション



無限リソースの使用

ASA は、パーセンテージや絶対値ではなく、クラス内の 1 つ以上のリソースに無制限アクセスを割り当てることができます。リソースが無制限の場合、コンテキストはシステムで使用可能な量までリソースを使用できます。たとえば、コンテキスト A、B、C が Silver クラスに属しており、クラスの各メンバの使用量が接続の 1% に制限されていて、合計 3% が割り当てられているが、3 つのコンテキストが現在使用しているのは合計 2% だけだとします。Gold クラスは、接続に無制限にアクセスできます。Gold クラスのコンテキストは、「未割り当て」接続のうち 97% を超える分も使用できます。つまり、現在コンテキスト A、B、C で使用されていない、接続の 1% も使用できます。その場合は、コンテキスト A、B、C の使用量が、これらの制限の合計である 3% に達することは不可能になります。無制限アクセスの設定は、ASA のオーバーサブスクライプと同様ですが、システムをどの程度オーバーサブスクライプできるかを詳細には制御できません。

図 39: 無限リソース



13021

MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと。



- (注) 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセスコントロールを実行する場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

マルチコンテキストモードでの MAC アドレス

MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。あるインターフェイスを共有させる場合に、コンテキストごとにそのインターフェイスの固有 MAC アドレスを設定していなかった場合は、他の分類方法が試行されますが、その方法では十分にカバーされないことがあります。

コンテキスト間でのインターフェイス共有を許可するには、共有されるコンテキストインターフェイスそれぞれで仮想 MAC アドレスの自動生成を有効にしてください。ASASM の場合のみ、自動生成はマルチコンテキストモードではデフォルトで有効になっています。

自動 MAC アドレス

マルチコンテキストモードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効になっている場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2xx.yyzz.zzzz

xx.yy はユーザ定義プレフィックスまたはインターフェイス MAC アドレスの最後の 2 バイトに基づいて自動生成されるプレフィックスです。zz.zzzz は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D (yyxx) に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます (xyyy)。

A24D.00zz.zzzz

プレフィックス 1009 (03F1) の場合、MAC アドレスは次のようになります。

A2F1.03zz.zzzz



(注) プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンドリファレンスの **mac-address auto** コマンドを参照してください。

VPN サポート

VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

マルチ コンテキスト モードでサイト間 VPN を使用できます。

リモート アクセス VPN はサポートされていません。

マルチ コンテキスト モードのライセンス

モデル	ライセンス要件
ASA 5506-X	サポートしない

モデル	ライセンス要件
ASA 5508-X	Security Plus ライセンス : 2 コンテキスト オプション ライセンス : 5 コンテキスト
ASA 5512-X	<ul style="list-style-type: none"> • 基本ライセンス : サポートされない。 • Security Plus ライセンス : 2 コンテキスト オプション ライセンス : 5 コンテキスト
ASA 5515-X	基本ライセンス : 2 コンテキスト オプション ライセンス : 5 コンテキスト
ASA 5516-X	Security Plus ライセンス : 2 コンテキスト オプション ライセンス : 5 コンテキスト
ASA 5525-X	基本ライセンス : 2 コンテキスト オプション ライセンス : 5、10、または 20 コンテキスト
ASA 5545-X	基本ライセンス : 2 コンテキスト オプション ライセンス : 5、10、20、または 50 コンテキスト
ASA 5555-X	基本ライセンス : 2 コンテキスト オプション ライセンス : 5、10、20、50、または 100 コンテキスト。
ASA 5585-X (SSP-10)	基本ライセンス : 2 コンテキスト オプション ライセンス : 5、10、20、50、または 100 コンテキスト。
ASA 5585-X (SSP-20、-40、および -60)	基本ライセンス : 2 コンテキスト オプション ライセンス : 5、10、20、50、100、または 250 コンテキスト。
ASASM	基本ライセンス : 2 コンテキスト オプション ライセンス : 5、10、20、50、100、または 250 コンテキスト。
Firepower 9300	基本ライセンス : 10 コンテキスト オプションのライセンス : 10 コンテキストずつの追加で、250 コンテキストまで。
ASAv	サポートしない

マルチ コンテキスト モードの前提条件

マルチ コンテキスト モードに切り替えた後で、システム コンフィギュレーションにアクセスするために管理コンテキストに接続します。管理以外のコンテキストからシステムを設定することはできません。デフォルトでは、マルチ コンテキスト モードをイネーブルにした後はデフォルトの管理 IP アドレスを使用して管理コンテキストに接続できます。

マルチ コンテキスト モードのガイドライン

フェールオーバー

アクティブ/アクティブモードフェールオーバーは、マルチ コンテキスト モードでのみサポートされます。

IPv6

クロス コンテキスト IPv6 ルーティングはサポートされません。

サポートされない機能

マルチコンテキスト モードでは、次の機能をサポートしません。

- RIP
- OSPFv3 (OSPFv2 がサポートされます)。
- マルチキャスト ルーティング
- 脅威の検出
- ユニファイド コミュニケーション
- QoS
- リモート アクセス VPN (サイトツーサイト VPN がサポートされます)。

その他のガイドライン

- コンテキストモード (シングルまたはマルチ) は、リブートされても持続されますが、コンフィギュレーションファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、新規デバイスのモードを **match** に設定します。
- フラッシュ メモリのルート ディレクトリにコンテキスト コンフィギュレーションを保存する場合、一部のモデルでは、メモリに空き容量があっても、そのディレクトリに保存する余地がなくなることがあります。この場合は、コンフィギュレーションファイルのサブディレクトリを作成します。背景：一部のモデル (ASA 5585-X など) では内部フラッシュメモリに FAT 16 ファイルシステムが使用されており、8.3 形式に準拠した短い名前を使用

していない、または大文字を使用している場合、長いファイル名を保存するためにファイルシステムのスロットが使い尽くされるため、512以上のファイルやフォルダを保存できません (<http://support.microsoft.com/kb/120138/en-us> を参照)。

マルチコンテキストモードのデフォルト

- デフォルトで、ASA はシングルコンテキストモードになります。
- 「[デフォルトクラス \(246 ページ\)](#)」を参照してください。

マルチコンテキストの設定

手順

-
- ステップ1** [マルチコンテキストモードの有効化またはディセーブル化 \(253 ページ\)](#)。
- ステップ2** (任意) [リソース管理用のクラスの設定 \(255 ページ\)](#)。
- (注) VPN のサポートのために、リソースクラスの VPN リソースを設定する必要があります。デフォルトクラスは VPN を許可しません。
- ステップ3** システム実行スペースでインターフェイスを設定します。
- ASA 5500-X : [基本的なインターフェイス設定 \(463 ページ\)](#)。
 - Firepower 9300—[論理デバイス Firepower 9300 \(191 ページ\)](#)
 - ASASM : [ASASM クイックスタート ガイド](#)。
- ステップ4** [セキュリティコンテキストの設定 \(258 ページ\)](#)。
- ステップ5** (任意) [コンテキストインターフェイスへのMACアドレスの自動割り当て \(261 ページ\)](#)。
- ステップ6** コンテキストのインターフェイスコンフィギュレーションを完成させます。「[ルーテッドモードインターフェイスとトランスペアレントモードインターフェイス \(513 ページ\)](#)」を参照してください。
-

マルチコンテキストモードの有効化またはディセーブル化

シスコへの発注方法によっては、ASA がすでにマルチセキュリティコンテキスト用に設定されている場合があります。シングルモードからマルチモードに変換する必要がある場合は、この項の手順に従ってください。

ASDM では、High Availability and Scalability Wizard を使用し、Active/Active フェールオーバーをイネーブルにした場合、シングルモードからマルチモードへの変更をサポートします。詳細については、「[ハイアベイラビリティのためのフェールオーバー \(275ページ\)](#)」を参照してください。アクティブ/アクティブフェールオーバーを使用するか、またはシングルモードに戻す場合は、CLIを使用してモードを変更する必要があります。モードの変更には確認を必要とするため、コマンドラインインターフェイスツールは使用できません。この項では、CLIでのモード変更について説明します。

マルチコンテキストモードの有効化

シングルモードからマルチモードに変換すると、ASA は実行コンフィギュレーションを2つのファイルに変換します。これらはシステムコンフィギュレーションで構成される新規スタートアップコンフィギュレーションと、(内部フラッシュメモリのルートディレクトリの)管理コンテキストで構成される `admin.cfg` です。元の実行コンフィギュレーションは、`old_running.cfg` として (内部フラッシュメモリのルートディレクトリに) 保存されます。元のスタートアップコンフィギュレーションは保存されません。ASA は、管理コンテキストのエントリをシステムコンフィギュレーションに「`admin`」という名前で自動的に追加します。

始める前に

スタートアップの設定をバックアップします。シングルモードからマルチモードに変換すると、ASA は実行コンフィギュレーションを2つのファイルに変換します。元のスタートアップコンフィギュレーションは保存されません。[ファイルの管理 \(930ページ\)](#) を参照してください。

手順

マルチコンテキストモードに変更します。

mode multiple

例：

```
ciscoasa(config)# mode multiple
```

ASA をリブートするよう求められます。

シングルコンテキストモードの復元

以前の実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーしてモードをシングルモードに変更するには、次の手順を実行します。

始める前に

この手順はシステム実行スペースで実行します。

手順

ステップ 1 元の実行コンフィギュレーションのバックアップバージョンを現在のスタートアップコンフィギュレーションにコピーします。

copy disk0:old_running.cfg startup-config

例 :

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

ステップ 2 モードをシングルモードに設定します。

mode single

例 :

```
ciscoasa(config)# mode single
```

ASA をリブートするよう求められます。

リソース管理用のクラスの設定

システムコンフィギュレーションでクラスを設定するには、次の手順を実行します。新しい値を指定してコマンドを再入力すると、特定のリソース制限値を変更できます。

始める前に

- この手順はシステム実行スペースで実行します。
- 以下の表に、リソースタイプおよび制限を記載します。



(注) 「システム制限」に「該当なし」と記述されている場合、そのリソースにはハードシステム制限がないため、リソースのパーセンテージを設定できません。

表 12: リソース名および制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
ASDM Sessions	同時接続数	最小 1 最大 20	32	SSH 管理セッション。 ASDM セッションでは、2つの HTTPS 接続が使用されます。一方は常に存在するモニタ用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、ASDM セッションのシステム制限が 32 の場合、HTTPS セッション数は 64 に制限されます。
Connections Conns/Sec	同時またはレート	該当なし	同時接続数：モデルごとの接続制限については、 モデルごとにサポートされている機能のライセンス (133 ページ) を参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。 (注) syslog メッセージは、xlates または conns のいずれか制限が低い方に対して生成されます。たとえば、xlates の制限を 7、conns の制限を 9 に設定した場合、ASA は syslog メッセージ 321001（「Resource 'xlates' limit of 7 reached for context 'ctx1'」）のみ生成し、321002（「Resource 'conn rate' limit of 5 reached for context 'ctx1'」）は生成しません。
Hosts	同時接続数	該当なし	該当なし	ASA 経由で接続可能なホスト。
Inspects/sec	レート	該当なし	該当なし	アプリケーションインスペクション数/秒。
MAC Entries	同時接続数	該当なし	65,535	トランスペアレントファイアウォールモードでは、MAC アドレステーブルで許可される MAC アドレス数。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
Routes	同時接続数	該当なし	該当なし	ダイナミック ルート。
Other VPN Burst	同時接続数	該当なし	モデルに応じた Other VPN セッション数から、Other VPN 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	Other VPN でコンテキストに割り当てられた数を超過して許可されるサイトツーサイト VPN セッションの数。たとえばモデルが 5000 セッションをサポートしており、Other VPN のすべてのコンテキスト全体で 4000 セッションを割り当てると、残りの 1000 セッションは Other VPN Burst に使用できます。Other VPN ではセッション数がコンテキストに対して保証されますが、対照的に Other VPN Burst ではオーバーサブスクライブが可能です。すべてのコンテキストでバースト プールを先着順に使用できます。
その他の VPN	同時接続数	該当なし	モデルごとの使用可能な Other VPN セッション数については、モデルごとにサポートされている機能のライセンス (133 ページ) を参照してください。	サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。
IKEv1 SAs In Negotiation	同時 (パーセンテージのみ)	該当なし	このコンテキストに割り当てられている Other VPN セッションのパーセンテージ。セッションをコンテキストに割り当てするには、Other VPN リソースを参照してください。	コンテキストでの Other VPN パーセンテージ制限として表される、着信 IKEv1 SA ネゴシエーション。
SSH	同時接続数	最小 1 最大 5	100	SSH セッション
Syslogs/sec	レート	該当なし	該当なし	Syslog メッセージ数/秒。
Telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
Xlates	同時接続数	該当なし	該当なし	ネットワーク アドレス変換。

手順

ステップ 1 まだシステム コンフィギュレーションモードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2 [Configuration] > [Context Management] > [Resource Class] の順に選択し、[Add] をクリックします。

[Add Resource Class] ダイアログボックスが表示されます。

ステップ 3 [Resource Class] フィールドに、最大 20 文字のクラス名を入力します。

ステップ 4 [Count Limited Resources] 領域で、リソースの同時接続制限を設定します。

各リソース タイプの説明については、上記の表を参照してください。

システム制限のないリソースは、パーセント (%) で設定できません。設定できるのは絶対値だけです。制限を設定しない場合、デフォルトクラスの制限値が継承されます。制限値がデフォルトクラスにない場合は、リソースは無制限またはシステム制限値（使用できる場合）に設定されます。ほとんどのリソースについて、0 を指定すると無制限と設定されます。VPN タイプについて、0 を指定すると制限なしと設定されます。

ステップ 5 [Rate Limited Resources] 領域で、リソースのレート制限を設定します。

各リソース タイプの説明については、上記の表を参照してください。

制限を設定しない場合、デフォルトクラスの制限値が継承されます。制限値がデフォルトクラスにない場合は、デフォルトでは無制限になります。0 は制限を無制限に設定します。

ステップ 6 [OK] をクリックします。

セキュリティ コンテキストの設定

システム コンフィギュレーションのセキュリティ コンテキスト定義では、コンテキスト名、コンフィギュレーションファイルの URL、コンテキストが使用できるインターフェイス、およびその他の設定値を指定します。

始める前に

- この手順はシステム実行スペースで実行します。
- インターフェイスを設定します。

- ASA 5500-X : 基本的なインターフェイス設定 (463 ページ) 。
- Firepower 9300—論理デバイス Firepower 9300 (191 ページ)
- ASASM : ASASM クイックスタートガイド。

手順

- ステップ 1** まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- ステップ 2** [Configuration] > [Context Management] > [Security Contexts] の順に選択し、[Add] をクリックします。
- [Add Context] ダイアログボックスが表示されます。
- ステップ 3** [Security Context] フィールドに、コンテキストの名前を 32 文字以内の文字列で入力します。
- この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。
- ステップ 4** [Interface Allocation] 領域で、[Add] ボタンをクリックし、コンテキストにインターフェイスを割り当てます。
- a) [Interfaces] > [Physical Interface] ドロップダウン リストからインターフェイスを選択します。
- メイン インターフェイスを割り当てる場合、サブインターフェイス ID を空白にします。サブインターフェイスまたはその範囲を指定すると、このインターフェイスに設定されます。トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないインターフェイスだけが表示されます。メイン インターフェイスが他のコンテキストに割り当てられている場合、サブインターフェイスを選択する必要があります。
- b) (オプション) [Interfaces] > [Subinterface Range] ドロップダウン リストからサブインターフェイス ID を選択します。
- サブインターフェイス ID の範囲を指定する場合、2 つ目のドロップダウン リストが有効であれば、そこから最後の ID を選択します。
- トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないサブインターフェイスだけが表示されます。
- c) (オプション) [Aliased Names] 領域で、[Use Aliased Name in Context] をオンにして、このインターフェイスに対して、コンテキスト コンフィギュレーションでインターフェイス ID の代わりに使用するエイリアス名を設定します。
- [Name] フィールドに、エイリアス名を設定します。

エイリアス名の先頭および最後は英字にします。間の文字として使用できるのは、英字、数字、下線だけです。このフィールドで名前の最後を英字または下線にした場合、その名前の後に追加する数字を [Range] フィールドで設定できます。

- (オプション) [Range] フィールドで、エイリアス名のサフィックスを数字で設定します。

サブインターフェイスに範囲がある場合、範囲の数字を入力して名前の後に追加できます。

- d) (オプション) エイリアス名を設定した場合でも、コンテキストのユーザが物理インターフェイスのプロパティを表示できるようにするには、[Show Hardware Properties in Context] をオンにします。
- e) [OK] をクリックして、[Add Context] ダイアログボックスに戻ります。

ステップ 5 (任意) IPS 仮想センサーを使用する場合は、[IPS Sensor Allocation] 領域でセンサーをコンテキストに割り当てます。

IPS および仮想センサーの詳細については、IPS クイック スタート ガイドを参照してください。

ステップ 6 (任意) [Resource Assignment] 領域で、[Resource Class] ドロップダウンリストから、このコンテキストをリソース クラスに割り当てるクラス名を選択します。

この領域から直接リソース クラスを追加または編集できます。

ステップ 7 [Config URL] ドロップダウン リストから、ファイル システム タイプを選択します。フィールドに、コンテキスト コンフィギュレーションの場所の URL を指定します。

FTP の場合、URL は次の形式になります。

```
ftp://server.example.com/configs/admin.cfg
```

ステップ 8 (任意) [Login] をクリックし、外部ファイル システムのユーザ名とパスワードを設定します。

ステップ 9 (任意) [Failover Group] ドロップダウン リストからグループ名を選択し、アクティブ/アクティブ フェールオーバーのフェールオーバー グループを設定します。

ステップ 10 (任意) [Cloud Web Security] の [Enable] をクリックして、このコンテキストで Web セキュリティ インспекションをイネーブルにします。システム コンフィギュレーションに設定されたライセンスを上書きする場合は、[License] フィールドにライセンスを入力します。

ステップ 11 (任意) [Description] フィールドに、説明を追加します。

ステップ 12 [OK] をクリックして、[Security Contexts] ペインに戻ります。

ステップ 13 (任意) コンテキストを選択してから [Change Firewall Mode] をクリックし、ファイアウォール モードをトランスペアレントに設定します。

新しいコンテキストの場合は、消去するための設定はありません。[Change Mode] をクリックして、トランスペアレント ファイアウォール モードに変更します。

既存のコンテキストの場合は、モードを変更する前に設定をバックアップするのを忘れないでください。

(注) ASDMの現在接続されているコンテキストのモード (通常は管理コンテキスト) は変更できません。コマンドラインでモードを設定するには、[ファイアウォール モード \(シングルモード\) の設定 \(216 ページ\)](#) を参照してください。

ステップ 14 (任意) MACアドレスの自動生成をカスタマイズするには、[コンテキストインターフェイスへの MAC アドレスの自動割り当て \(261 ページ\)](#) を参照してください。

ステップ 15 (任意) デバイスの最大 TLS プロキシセッション数を指定するには、[ASA でサポートされる必要がある TLS プロキシセッションの最大数の指定 (Specify the maximum number of TLS Proxy sessions that the ASA needs to support)] チェックボックスをオンにします。TLS プロキシの詳細については、『[ファイアウォールの構成ガイド](#)』を参照してください。

コンテキスト インターフェイスへの MAC アドレスの自動割り当て

この項では、MACアドレスの自動生成の設定方法について説明します。MACアドレスは、コンテキスト内でパケットを分類するために使用されます。

始める前に

- コンテキストでインターフェイスの名前を設定すると、ただちに新規 MAC アドレスが生成されます。コンテキストインターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。
- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。

手順

ステップ 1 まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2 [Configuration] > [Context Management] > [Security Contexts] の順に選択し、[Mac-Address auto] をオンにします。プレフィックスを入力しない場合は、ASAによって、インターフェイス (ASA 5500-X) またはバックプレーン (ASASM) MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

ステップ 3 (オプション) [プレフィックス (Prefix)] チェックボックスをオンにしてから、フィールドに 0 ~ 65535 の範囲内の 10 進数値を入力します。

このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

コンテキストとシステム実行スペースの切り替え

システム実行スペース（または管理コンテキスト）にログインした場合は、コンテキストを切り替えながら、各コンテキスト内でコンフィギュレーションやタスクのモニタリングを実行することができます。コンフィギュレーションモードで編集される実行コンフィギュレーションは、ユーザのログイン先によって決まります。システム実行スペースにログインした場合、実行コンフィギュレーションはシステムコンフィギュレーションのみで構成され、コンテキストにログインした場合は、実行コンフィギュレーションはそのコンテキストのみで構成されます。

手順

-
- ステップ 1** [Device List] ペインでシステムを設定するには、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- ステップ 2** コンテキストを設定するには、[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
-

セキュリティ コンテキストの管理

この項では、セキュリティ コンテキストを管理する方法について説明します。

セキュリティ コンテキストの削除

現在の管理コンテキストは削除できません。



-
- (注) フェールオーバーを使用すると、アクティブ装置でコンテキストを削除した時刻と、スタンバイ装置でコンテキストが削除された時刻との間で遅延が生じます。
-

始める前に

この手順はシステム実行スペースで実行します。

手順

-
- ステップ 1** まだシステムコンフィギュレーションモードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。
- ステップ 2** [Configuration] > [Context Management] > [Security Contexts] の順に選択します。

ステップ3 削除するユーザを選択し、[Delete] をクリックします。

[Delete Context] ダイアログボックスが表示されます。

ステップ4 このコンテキストを再追加するかもしれない、再使用できるようにコンフィギュレーションファイルを保持する場合は、[Also delete config URL file from the disk] チェックボックスをオフにします。

コンフィギュレーションファイルを削除するには、チェックボックスをオンにしたままにします。

ステップ5 [Yes] をクリックします。

管理コンテキストの変更

システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要があるときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システムコンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザに制限する必要があります。



(注) ASDM の場合、ASDM セッションが切断されるため、ASDM 内の管理コンテキストを変更できません。新しい管理コンテキストに再割り当てなければならないことに注意するコマンドライン インターフェイス ツールを使用してこの手順を実行できます。

始める前に

- コンフィギュレーション ファイルが内部フラッシュ メモリに保存されている限り、任意のコンテキストを管理コンテキストとして設定できます。
- この手順はシステム実行スペースで実行します。

手順

ステップ1 まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ2 [Tools] > [Command Line Interface] を選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 3 次のコマンドを入力します。

```
admin-context context_name
```

ステップ 4 [Send] をクリックします。

Telnet、SSH、HTTPS (ASDM) など、管理コンテキストに接続しているリモート管理セッションはすべて終了します。新しい管理コンテキストに再接続する必要があります。

(注) いくつかのシステム コンフィギュレーション コマンド、たとえば **ntp server** では、管理コンテキストに所属するインターフェイス名が指定されます。管理コンテキストを変更した場合に、そのインターフェイス名が新しい管理コンテキストに存在しないときは、そのインターフェイスを参照するシステム コマンドはすべて、アップデートしてください。

セキュリティ コンテキスト URL の変更

この項では、コンテキスト URL を変更する方法について説明します。

始める前に

- セキュリティ コンテキスト URL は、新しい URL からコンフィギュレーションをリロードしないと変更できません。ASA は、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。
- 同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。
- マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。
 - コンフィギュレーションが同じ場合、変更は発生しません。
 - コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。
- コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。
- この手順はシステム実行スペースで実行します。

手順

- ステップ 1 まだシステム コンフィギュレーションモードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。
- ステップ 2 [Configuration] > [Context Management] > [Security Contexts] の順に選択します。
- ステップ 3 編集するコンテキストを選択して、[Edit] をクリックします。
[Edit Context] ダイアログボックスが表示されます。
- ステップ 4 [Config URL] フィールドに新しい URL を入力して、[OK] をクリックします。
システムは、動作中になるように、ただちにコンテキストをロードします。

セキュリティ コンテキストのリロード

セキュリティ コンテキストは、次の 2 つの方法でリロードできます。

- 実行コンフィギュレーションをクリアしてからスタートアップコンフィギュレーションをインポートする。
このアクションでは、セキュリティ コンテキストに関連付けられている接続や NAT テーブルなどの属性の大部分がクリアされます。
- セキュリティ コンテキストをシステム コンフィギュレーションから削除する。
このアクションでは、トラブルシューティングに役立つ可能性のあるメモリ割り当てなど補足的な属性がクリアされます。しかし、コンテキストをシステムに戻して追加するには、URL とインターフェイスを再指定する必要があります。

コンフィギュレーションのクリアによるリロード

手順

- ステップ 1 [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
- ステップ 2 [Tools] > [Command Line Interface] を選択します。
[Command Line Interface] ダイアログボックスが表示されます。
- ステップ 3 次のコマンドを入力します。
clear configure all
- ステップ 4 [Send] をクリックします。
コンテキストの設定が削除されます。

ステップ5 [Tools] > [Command Line Interface] を再度選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ6 次のコマンドを入力します。

copy startup-config running-config

ステップ7 [Send] をクリックします。

ASA が設定をリロードします。ASA は、システム コンフィギュレーションに指定された URL からコンフィギュレーションをコピーします。コンテキスト内で URL を変更することはできません。

コンテキストの削除および再追加によるリロード

コンテキストを削除し、その後再追加することによってコンテキストをリロードするには、次の手順を実行してください。

手順

- ステップ1 [セキュリティ コンテキストの削除 \(262 ページ\)](#) 。 [Also delete config URL file from the disk] チェックボックスがオフになっていることを確認します。
- ステップ2 [セキュリティ コンテキストの設定 \(258 ページ\)](#)

セキュリティ コンテキストのモニタリング

この項では、コンテキスト情報を表示およびモニタリングする方法について説明します。

コンテキスト リソースの使用状況のモニタリング

手順

- ステップ1 まだシステム モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。
- ステップ2 ツールバーの [Monitoring] ボタンをクリックします。
- ステップ3 [Context Resource Usage] をクリックします。

すべてのコンテキストのリソース使用状況を表示するには、次の各リソースタイプをクリックします。

- [ASDM/Telnet/SSH] : ASDM、Telnet、SSH 接続状況を表示します。

- [Context] : 各コンテキストの名前を表示します。
各アクセス方式に対して、次の使用状況統計が表示されます。
 - [Existing Connections (#)] : 既存の接続の数を表示します。
 - [Existing Connections (%)] : このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
 - [Peak Connections (#)] : **clear resource usage** コマンドの使用またはデバイスのリポートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
-
- [Routes] : ダイナミック ルートの使用状況を表示します。
 - [Context] : 各コンテキストの名前を表示します。
 - [Existing Connections (#)] : 既存の接続の数を表示します。
 - [Existing Connections (%)] : このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
 - [Peak Connections (#)] : **clear resource usage** コマンドの使用またはデバイスのリポートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
-
- [Xlates] : ネットワーク アドレス変換の使用状況を表示します。
 - [Context] : 各コンテキストの名前を表示します。
 - [Xlates (#)] : 現在の xlate の数を表示します。
 - [Xlates (%)] : このコンテキストで使用されている xlate 数を、すべてのコンテキストで使用されている xlate の総数のパーセントとして表示します。
 - [Peak (#)] : **clear resource usage** コマンドの使用またはデバイスのリポートにより統計情報が最後にクリアされて以降のピーク xlate 数を表示します。
-
- [NATs] : NAT ルールの数を表示します。
 - [Context] : 各コンテキストの名前を表示します。
 - [NATs (#)] : 現在の NAT ルールの数を表示します。
 - [NATs (%)] : このコンテキストで使用されている NAT ルール数を、すべてのコンテキストで使用されている NAT ルールの総数のパーセントとして表示します。
 - [Peak NATs (#)] : **clear resource usage** コマンドの使用またはデバイスのリポートにより統計情報が最後にクリアされて以降のピーク NAT ルール数を表示します。
-
- [Syslogs] : システム ログ メッセージのレートを表示します。
 - [Context] : 各コンテキストの名前を表示します。
 - [Syslog Rate (#/sec)] : システム ログ メッセージの現在のレートを表示します。

- [Syslog Rate (%)] : このコンテキストで生成されたシステム ログ メッセージ数を、すべてのコンテキストで生成されたシステム ログ メッセージの総数のパーセントとして表示します。
- [Peak Syslog Rate (#/sec)] : **clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のシステム ログ メッセージのピーク レートを表示します。
- [VPN] : VPN サイトツーサイト トンネルの使用状況を表示します。
 - [Context] : 各コンテキストの名前を表示します。
 - [VPN Connections] : 保証された VPN セッションの使用状況を表示します。
 - [VPN Burst Connections] : バースト VPN セッションの使用状況を表示します。
 - [Existing (#)] : 既存トンネルの数を表示します。
 - [Peak (#)] : **clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク トンネル数を表示します。

ステップ 4 表示をリフレッシュするには、[Refresh] をクリックします。

割り当てられた MAC アドレスの表示

システム コンフィギュレーション内またはコンテキスト内の自動生成された MAC アドレスを表示できます。

システム設定での MAC アドレスの表示

この項では、システム コンフィギュレーション内の MAC アドレスを表示する方法について説明します。

始める前に

MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

手順

ステップ 1 まだシステム コンフィギュレーションモードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ2 **[Configuration] > [Context Management] > [Security Contexts]** を選択し、**[Primary MAC]** カラムと **[Secondary MAC]** カラムを表示します。

コンテキスト内の MAC アドレスの表示

この項では、コンテキスト内で MAC アドレスを表示する方法について説明します。

手順

ステップ1 まだシステム コンフィギュレーションモードに入っていない場合、**[Device List]** ペインで、アクティブなデバイス IP アドレスの下にある **[System]** をダブルクリックします。

ステップ2 **[Configuration] > [Interfaces]** を選択し、**[MAC Address]** アドレス カラムを表示します。

このテーブルには、使用中の MAC アドレスが表示されます。MAC アドレスを手動で割り当てており、自動生成もイネーブルになっている場合は、システム コンフィギュレーションからは未使用の自動済み生成アドレスのみを表示できます。

マルチ コンテキスト モードの履歴

表 13: マルチ コンテキスト モードの履歴

機能名	プラットフォーム リリース	機能情報
マルチセキュリティ コンテキスト	7.0(1)	マルチ コンテキスト モードが導入されました。 次の画面が導入されました。 [Configuration] > [Context Management] 。
MAC アドレス自動割り当て	7.2(1)	コンテキスト インターフェイスへの MAC アドレス自動割り当てが導入されました。 次の画面が変更されました。 [Configuration] > [Context Management] > [Security Contexts] 。
リソース管理	7.2(1)	リソース管理が導入されました。 次の画面が導入されました。 [Configuration] > [Context Management] > [Resource Management] 。

機能名	プラットフォーム リリース	機能情報
IPS 仮想センサー	8.0(2)	<p>IPS ソフトウェアのバージョン 6.0 以降を実行している AIP SSM では、複数の仮想センサーを実行できます。つまり、AIP SSM に複数のセキュリティポリシーを設定することができます。各コンテキストまたはシングルモード ASA を 1 つまたは複数の仮想センサーに割り当てたり、複数のセキュリティコンテキストを同じ仮想センサーに割り当てることができます。</p> <p>次の画面が変更されました。 [Configuration] > [Context Management] > [Security Contexts]。</p>
MAC アドレス自動割り当ての機能強化	8.0(5)/8.2(2)	<p>MAC アドレス形式が変更されました。プレフィックスが使用され、固定開始値 (A2) が使用されます。また、フェールオーバーペアのプライマリ装置とセカンダリ装置の MAC アドレスそれぞれに異なるスキームが使用されます。MAC アドレスはリロード後も維持されるようになりました。コマンドパーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MAC アドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。</p> <p>次の画面が変更されました。 [Configuration] > [Context Management] > [Security Contexts]。</p>
ASA 5550 および 5580 の最大コンテキスト数の増加	8.4(1)	<p>ASA 5550 の最大セキュリティコンテキスト数が 50 から 100 に増加しました。ASA 5580 での最大数が 50 から 250 に増加しました。</p>
MAC アドレスの自動割り当てのデフォルトでの有効化	8.5(1)	<p>MAC アドレスの自動割り当てが、デフォルトでイネーブルになりました。</p> <p>次の画面が変更されました。 [Configuration] > [Context Management] > [Security Contexts]。</p>

機能名	プラットフォーム リリース	機能情報
MAC アドレス プレフィックスの自動生成	8.6(1)	

機能名	プラットフォーム リリース	機能情報
		<p>マルチ コンテキスト モードで、ASA が MAC アドレス自動生成のコンフィギュレーションを変換し、デフォルトのプレフィックスを使用できるようになりました。ASA は、インターフェイス (ASA 5500-X) またはバックプレーン (ASASM) の MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時または MAC アドレス生成を再度イネーブルにすると、自動的に行われます。生成のプレフィックス方式は、セグメント上で一意の MAC アドレスがより適切に保証されるなど、多くの利点をもたらします。プレフィックスを変更する場合、カスタムプレフィックスによって機能を再設定できます。MAC アドレス生成の従来の方法は使用できなくなります。</p> <p>(注) フェールオーバーペアのヒットレス アップグレードを維持するため、ASA は、フェールオーバーが有効である場合、既存のコンフィギュレーションの MAC アドレス メソッドをリロード時に変換しません。ただし、フェールオーバーを使用するときは、生成メソッドをプレフィックスに手動で変更することを強く推奨します (特に ASASM の場合)。プレフィックスメソッドを使用しない場合、異なるスロット番号にインストールされた ASASM では、フェールオーバーが発生した場合に MAC アドレスの変更が行われ、トラフィックの中断が発生することがあります。アップグレード後に、MAC アドレス生成のプレフィックス方式を使用するには、デフォルトのプレフィッ</p>

機能名	プラットフォーム リリース	機能情報
		<p>クスを使用する MAC アドレス生成を再びイネーブルにします。</p> <p>次の画面が変更されました。 [Configuration] > [Context Management] > [Security Contexts]</p>
ASASM 以外のすべてのモデル上での MAC アドレスの自動割り当てはデフォルトでディセーブル	9.0(1)	<p>自動 MAC アドレスの割り当ては ASASM を除いて、デフォルトでディセーブルになりました。</p> <p>次の画面が変更されました。 [Configuration] > [Context Management] > [Security Contexts]。</p>
セキュリティコンテキストでのダイナミックルーティング	9.0(1)	<p>EIGRP と OSPFv2 ダイナミックルーティングプロトコルが、マルチコンテキストモードでサポートされるようになりました。OSPFv3、RIP、およびマルチキャストルーティングはサポートされません。</p>
ルーティングテーブルエントリのための新しいリソースタイプ	9.0(1)	<p>新規リソースタイプ <code>routes</code> が作成されました。これは、各コンテキストでのルーティングテーブルエントリの最大数を設定するためです。</p> <p>次の画面が変更されました。 [Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]</p>
マルチコンテキストモードのサイトツーサイト VPN	9.0(1)	<p>サイトツーサイト VPN トンネルが、マルチコンテキストモードでサポートされるようになりました。</p>
サイトツーサイト VPN トンネルのための新しいリソースタイプ	9.0(1)	<p>新しいリソースタイプ <code>vpn other</code> と <code>vpn burst other</code> が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。</p> <p>次の画面が変更されました。 [Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]</p>

機能名	プラットフォーム リリース	機能情報
IKEv1 SA ネゴシエーションの新しいリソース タイプ	9.1(2)	<p>CPU と暗号化エンジンの過負荷を防ぐため、コンテキストごとに IKEv1 SA ネゴシエーションの最大パーセンテージを設定するための新しいリソース タイプ <code>ikev1 in-negotiation</code> が作成されました。特定の条件（大容量の証明書、CRL、チェックなど）によっては、このリソースを制限する必要がある場合があります。</p> <p>次の画面が変更されました。 [Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]</p>
IKEv2 のリモート アクセス VPN は、マルチ コンテキスト モードでサポートされています。	9.9(2)	リモート アクセス VPN は、IKEv2 のマルチ コンテキスト モードで構成できます。



第 10 章

ハイ アベイラビリティのためのフェールオーバー

この章では、Cisco ASA のハイ アベイラビリティを達成するために、アクティブ/スタンバイまたはアクティブ/アクティブ フェールオーバーを設定する方法について説明します。

- [フェールオーバーについて \(275 ページ\)](#)
- [フェールオーバーのライセンス \(305 ページ\)](#)
- [フェールオーバーのガイドライン \(307 ページ\)](#)
- [フェールオーバーのデフォルト \(309 ページ\)](#)
- [アクティブ/スタンバイ フェールオーバーの設定 \(310 ページ\)](#)
- [アクティブ/アクティブ フェールオーバーの設定 \(311 ページ\)](#)
- [オプションのフェールオーバー パラメータの設定 \(312 ページ\)](#)
- [フェールオーバー の管理 \(319 ページ\)](#)
- [モニタリング フェールオーバー \(325 ページ\)](#)
- [フェールオーバーの履歴 \(328 ページ\)](#)

フェールオーバーについて

フェールオーバーの設定では、専用フェールオーバーリンク（および任意でステートリンク）を介して相互に接続された 2 つの同じ ASA が必要です。アクティブ装置およびインターフェイスのヘルスがモニタされて、所定のフェールオーバー条件に一致しているかどうか判断されます。所定の条件に一致すると、フェールオーバーが行われます。

フェールオーバー モード

ASA は、アクティブ/アクティブフェールオーバーとアクティブ/スタンバイ フェールオーバーの 2 つのフェールオーバーモードをサポートします。各フェールオーバーモードには、フェールオーバーを判定および実行する独自の方式があります。

- アクティブ/スタンバイ フェールオーバーでは、1 台の装置がアクティブ装置です。この装置がトラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを渡しま

せん。フェールオーバーが発生すると、アクティブ装置がスタンバイ装置にフェールオーバーし、そのスタンバイ装置がアクティブになります。シングルまたはマルチコンテキストモードでは、ASAのアクティブ/スタンバイフェールオーバーを使用できます。

- アクティブ/アクティブフェールオーバーコンフィギュレーションでは、両方のASAがネットワークトラフィックを渡すことができます。アクティブ/アクティブフェールオーバーは、マルチコンテキストモードのASAでのみ使用できます。アクティブ/アクティブフェールオーバーでは、ASAのセキュリティコンテキストを2つのフェールオーバーグループに分割します。フェールオーバーグループは、1つまたは複数のセキュリティコンテキストの論理グループにすぎません。一方のグループは、プライマリASAでアクティブになるよう割り当てられます。他方のグループは、セカンダリASAでアクティブになるよう割り当てられます。フェールオーバーが行われる場合は、フェールオーバーグループレベルで行われます。

両方のフェールオーバーモードとも、ステートフルまたはステートレスフェールオーバーをサポートします。

フェールオーバーのシステム要件

この項では、フェールオーバーコンフィギュレーションにあるASAのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

フェールオーバーコンフィギュレーションの2台の装置は、次の条件を満たしている必要があります。

- 同じモデルであること。
- インターフェイスの数とタイプが同じであること。

Firepower 9300 シャーシでは、フェールオーバーを有効にする前に、すべてのインターフェイスがFXOSで同一に事前構成されている必要があります。フェールオーバーを有効にした後でインターフェイスを変更する場合は、スタンバイユニットのFXOSでインターフェイスを変更し、アクティブユニットで同じ変更を行います。FXOSでインターフェイスを削除した場合（たとえば、ネットワークモジュールの削除、EtherChannelの削除、またはEtherChannelへのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OSの古いインターフェイス設定は手動で削除できます。

- 同じモジュール（存在する場合）がインストールされていること。
- 同じRAMがインストールされていること。

フェールオーバーコンフィギュレーションで装置に異なるサイズのフラッシュメモリを使用している場合、小さい方のフラッシュメモリを取り付けた装置に、ソフトウェアイメージファイルおよびコンフィギュレーションファイルを格納できる十分な容量があることを確認してく

ださい。十分な容量がない場合、フラッシュメモリの大きい装置からフラッシュメモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

ソフトウェア要件

フェールオーバーコンフィギュレーションの2台の装置は、次の条件を満たしている必要があります。

- コンテキストモードが同じであること（シングルまたはマルチ）。
- 単一モードの場合：同じファイアウォールモードにあること（ルーテッドまたはトランスペアレント）。

マルチコンテキストモードでは、ファイアウォールモードはコンテキストレベルで設定され、混合モードを使用できます。

- ソフトウェアバージョンが、メジャー（最初の番号）およびマイナー（2番目の番号）ともに同じであること。ただし、アップグレードプロセス中は、異なるバージョンのソフトウェアを一時的に使用できます。たとえば、ある装置をバージョン 8.3(1) からバージョン 8.3(2) にアップグレードし、フェールオーバーをアクティブ状態のままにできます。長期的に互換性を維持するために、両方の装置を同じバージョンにアップグレードすることをお勧めします。
- 同じ AnyConnect イメージを持っていること。中断のないアップグレードを実行するときにフェールオーバーペアのイメージが一致しないと、アップグレードプロセスの最後のレポート手順でクライアントレス SSL VPN 接続が切断され、データベースには孤立したセッションが残り、IP プールではクライアントに割り当てられた IP アドレスが「使用中」として示されます。

ライセンス要件

フェールオーバーコンフィギュレーションの2台の装置は、ライセンスが同じである必要はありません。これらのライセンスは結合され、1つのフェールオーバークラスタライセンスが構成されます。

フェールオーバーリンクとステートフルフェールオーバーリンク

フェールオーバーリンクとオプションのステートフルフェールオーバーリンクは、2つの装置間の専用接続です。シスコでは、フェールオーバーリンクまたはステートフルフェールオーバーリンク内の2つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバーリンクで、デバイス1で eth0 を使用していた場合は、デバイス2でも同じインターフェイス（eth0）を使用します。



注意 フェールオーバー リンクおよびステート リンク経由で送信される情報は、IPsec トンネルまたはフェールオーバー キーを使用して通信を保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信を IPsec トンネルまたはフェールオーバー キーによってセキュリティ保護することをお勧めします。

フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないデータ インターフェイス（物理、サブインターフェイス、冗長、または EtherChannel）はいずれもフェールオーバー リンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバーリンク用にのみ使用できます（ステートリンク用としても使用できます）。ほとんどのモデルでは、以下で明示的に説明されていない限り、フェールオーバー用の管理インターフェイスを使用できません。

ASA は、ユーザデータとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。同じ親の別のサブインターフェイスをフェールオーバーリンクやデータのために使用することもできません。

フェールオーバー リンクについては、次のガイドラインを参照してください。

- 5506-X ~ 5555-X：管理インターフェイスをフェールオーバー リンクとして使用できません。データ インターフェイスを使用する必要があります。
- 5585-X：データ インターフェイスとしては使用できますが、管理 0/0 インターフェイスは使用しないでください。この用途で必要とされるパフォーマンスをサポートしていません。

- **Firepower 4100/9300** : 統合されたフェールオーバー リンクとステート リンクには、10 GB のデータ インターフェイスを使用することを推奨します。フェールオーバー リンクに管理タイプのインターフェイスを使用することはできません。
- 他のすべてのモデル : 1 GB インターフェイスは、フェールオーバーとステート リンクを組み合わせるには十分な大きさです。

フェールオーバーリンクとして使用される冗長インターフェイスについては、冗長性の増強による次の利点を参照してください:

- フェールオーバー ユニットが起動すると、メンバー インターフェイスを交互に実行し、アクティブ ユニットの検出します。
- メンバー インターフェイスの 1 つにあるピアからのキープアライブ メッセージの受信をフェールオーバー ユニットが停止した場合、別のメンバー インターフェイスに切り替えます。

フェールオーバーリンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバーリンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- ASA のフェールオーバーインターフェイスと同じネットワークセグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。
- イーサネット ケーブルを使用して装置を直接接続します。外部スイッチは必要ありません。

装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASA は、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

ステートフル フェールオーバー リンク

ステートフルフェールオーバーを使用するには、接続ステート情報を渡すためのステートフルフェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。



- (注) ステートフル フェールオーバー リンクの帯域幅は、少なくともデータ インターフェイスの帯域幅と同等にすることを推奨します。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクの共有です。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステートリンクとフェールオーバー リンク専用のインターフェイスを検討する必要があります。

専用のインターフェイス

ステートリンク専用のデータ インターフェイス（物理、冗長、または EtherChannel）を使用できます。ステートリンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。

次の 2 つの方法のいずれかで、専用のステートリンクを接続します。

- ASA デバイスのフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。
- イーサネットケーブルを使用してアプライアンスを直接接続します。外部スイッチは必要ありません。

装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASAは、銅線イーサネットポートで Auto-MDI/MDIX をサポートしているため、クロスオーバーケーブルまたはストレートケーブルのいずれかを使用できます。ストレートケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のステートリンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバーメッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバーの中断の回避とデータ リンク

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバーリンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバーリンクがダウンした場合、フェールオーバーが必要かどうかの決定に、ASA はデータ インターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバーリンクのヘルスが復元されるまで停止されます。

耐障害性のあるフェールオーバーネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

単一のスイッチまたはスイッチセットが2つの ASA 間のフェールオーバー インターフェイスとデータインターフェイスの両方の接続に使用される場合、スイッチまたはスイッチ間リンクがダウンすると、両方の ASA がアクティブになります。したがって、次の図で示されている次の2つの接続方式は推奨しません。

図 40: 単一のスイッチを使用した接続：非推奨

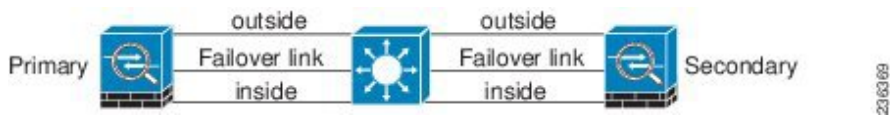
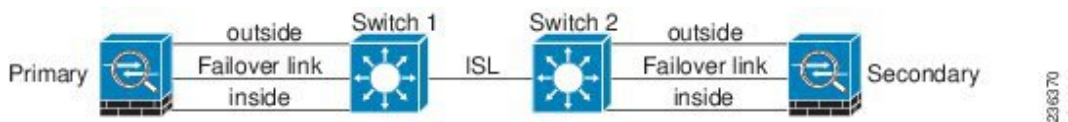


図 41: 2つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 42: 異なるスイッチを使用した接続

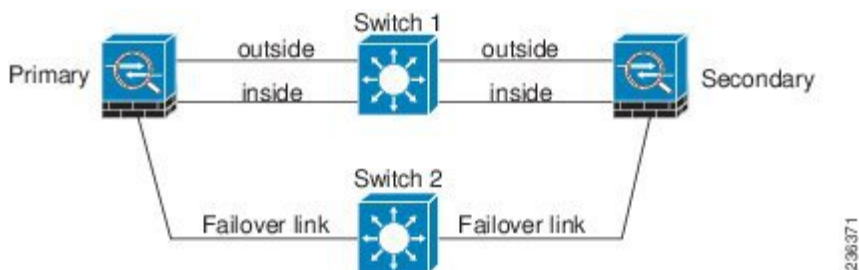
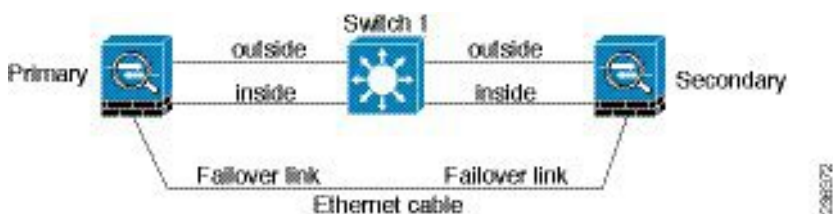


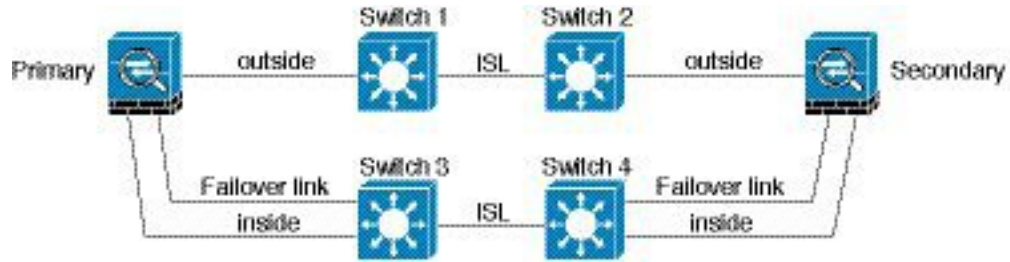
図 43: ケーブルを使用した接続



シナリオ 3：推奨

ASA データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバーリンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 44:セキュアスイッチを使用した接続



シナリオ 4：推奨

最も信頼性の高いフェールオーバー構成では、次の図に示すように、フェールオーバーリンクに冗長インターフェイスを使用します。

図 45:冗長インターフェイスを使用した接続

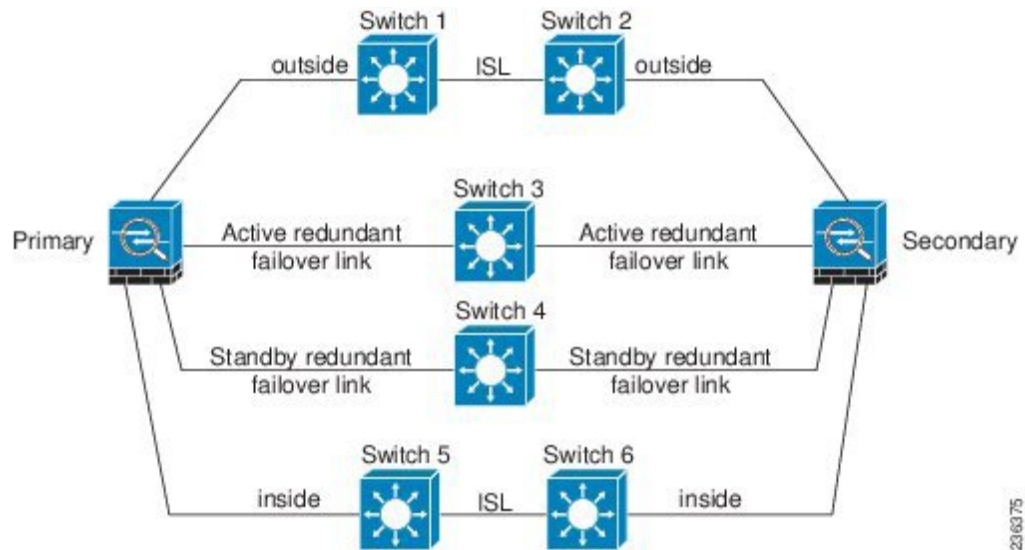
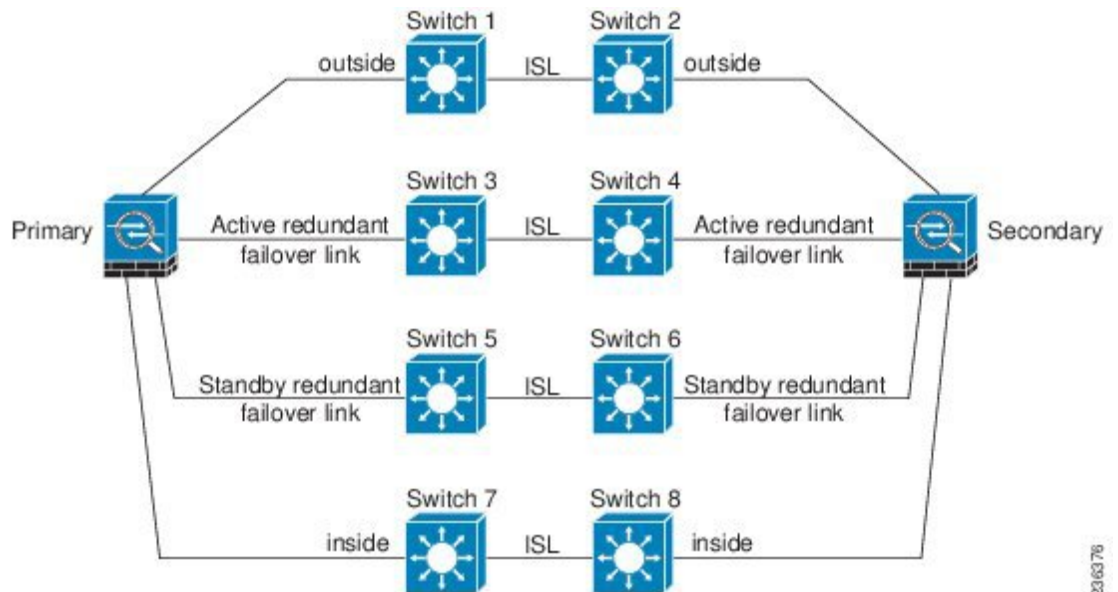


図 46: Inter-Switch Link (ISL) を使用した接続



200376

フェールオーバーの MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。一般的に、フェールオーバーが発生した場合、新しいアクティブ装置がアクティブな IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。



- (注) スタンバイアドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

ステートリンク用の IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。

アクティブ/スタンバイ IP アドレスと MAC アドレス

アクティブ/スタンバイ フェールオーバー の場合、フェールオーバー イベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

1. アクティブ装置は常にプライマリ装置の IP アドレスと MAC アドレスを使用します。
2. アクティブ装置が故障すると、スタンバイ装置は故障した装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。

- 故障した装置がオンラインに復帰すると、スタンバイ状態となり、スタンバイ IP アドレスと MAC アドレスを引き継ぎます。

ただし、セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MAC アドレスを使用します。プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワークトラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。仮想 MAC アドレスを設定しなかった場合、トラフィックフローを復元するために、接続されたルータの ARP テーブルをクリアする必要がある場合があります。ASA は MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

アクティブ/アクティブ IP アドレスと MAC アドレス

アクティブ/アクティブフェールオーバーの場合、フェールオーバーイベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

- プライマリ装置は、フェールオーバーグループ1および2のコンテキストのすべてのインターフェイスに対して、アクティブおよびスタンバイ MAC アドレスを自動生成します。必要に応じて、たとえば、MAC アドレスの競合がある場合は、MAC アドレスを手動で設定できます。
- 各装置は、そのアクティブフェールオーバーグループにアクティブな IP アドレスと MAC アドレスを使用し、そのスタンバイフェールオーバーグループにスタンバイアドレスを使用します。たとえば、フェールオーバーグループ1でプライマリ装置がアクティブである場合、フェールオーバーグループ1のコンテキストでアクティブなアドレスを使用します。フェールオーバーグループ2のコンテキストではスタンバイであるため、スタンバイアドレスを使用します。
- 装置が故障すると、他の装置は故障したフェールオーバーグループのアクティブな IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
- 故障した装置がオンラインに戻り、preempt オプションが有効になっている場合、フェールオーバーグループを再開します。

仮想 MAC アドレス

ASA には、仮想 MAC アドレスを設定する複数の方法があります。1つの方法のみ使用することをお勧めします。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。手動方法にはインターフェイスモードの `mac-address` コマンド、`failover mac address` コマンドが

含まれ、アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ モードの **mac address** コマンドが、以下で説明する自動生成方法に加えて含まれます。

マルチ コンテキスト モードでは、共有インターフェイスに仮想アクティブおよびスタンバイ MAC アドレスを自動的に生成するように ASA を設定することができ、これらの割り当てはセカンダリ ユニットに同期されます (**mac-address auto** コマンドを参照してください)。共有以外のインターフェイスでは、アクティブ/スタンバイ モードの MAC アドレスを手動で設定することができます (アクティブ/アクティブ モードはすべてのインターフェイスに MAC アドレスを自動生成します)。

アクティブ/アクティブ フェールオーバーでは、仮想 MAC アドレスはデフォルト値またはインターフェイスごとに設定できる値のいずれかとともに常に使用されます。

ASA サービス モジュールのシャーシ内およびシャーシ間モジュール配置

プライマリとセカンダリの ASASM は、同じスイッチ内または 2 台の異なるスイッチに搭載できます。

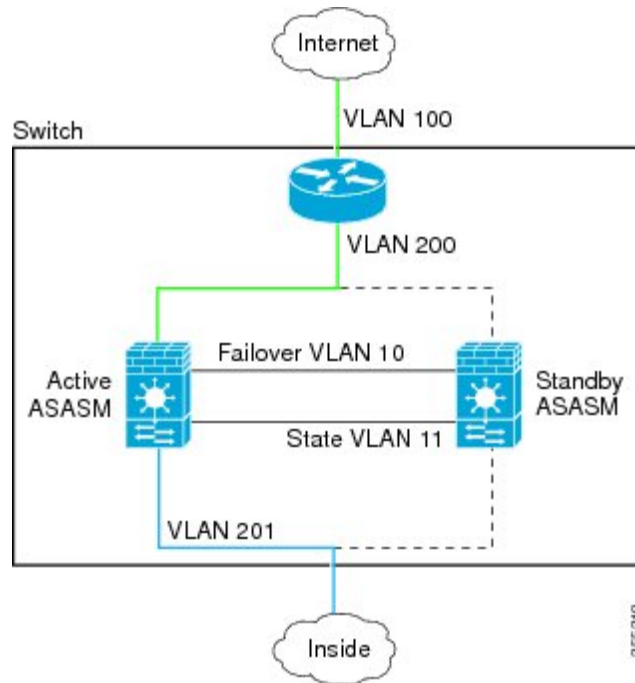
シャーシ内フェールオーバー

セカンダリ ASASM をプライマリ ASASM と同じスイッチに搭載した場合は、モジュールレベルの障害から保護する必要があります。

両方の ASASM に同じ VLAN が割り当てられますが、ネットワーキングに参加するのはアクティブ モジュールだけです。スタンバイ モジュールは、トラフィックを転送しません。

次の図は、一般的なスイッチ内の構成を示します。

図 47: スイッチ内フェールオーバー



シャーシ間フェールオーバー

スイッチレベルの障害から保護するため、セカンダリ ASASM を別のスイッチに搭載できます。ASASM は直接スイッチとフェールオーバーを調整するのではなく、スイッチと協調してフェールオーバー操作を行います。スイッチのフェールオーバー設定については、スイッチのマニュアルを参照してください。

ASASM 間のフェールオーバー通信の信頼性を高めるために、2 台のスイッチ間に EtherChannel トランク ポートを設定して、フェールオーバーおよびステート VLAN を伝送することをお勧めします。

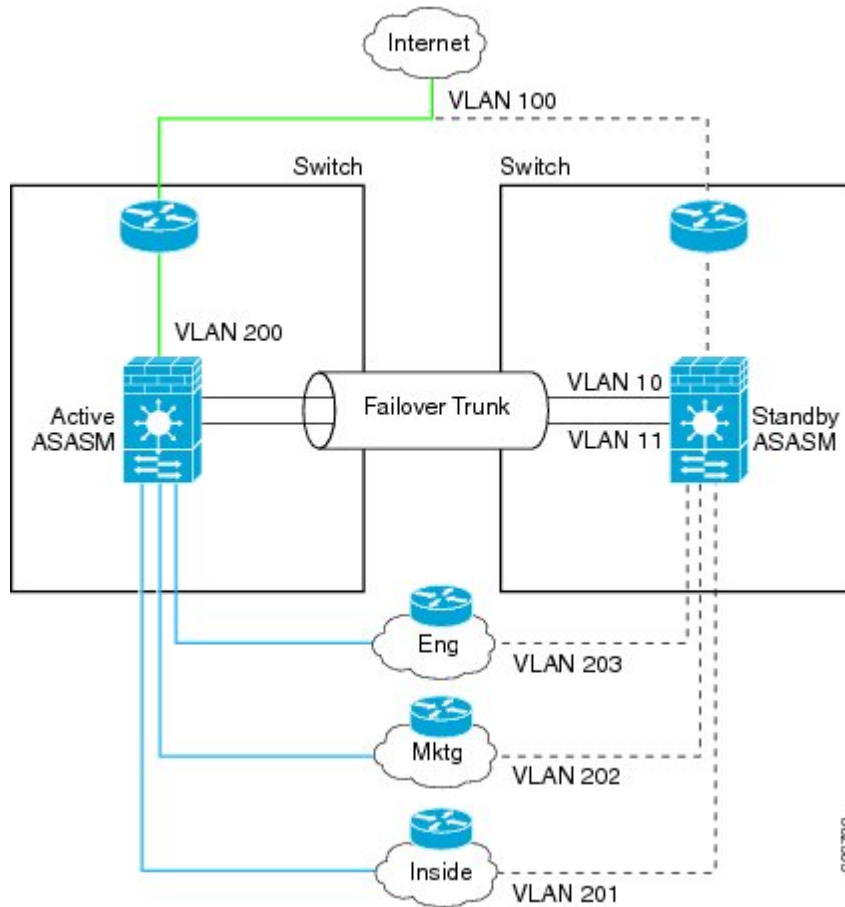
他の VLAN については、両方のスイッチがすべてのファイアウォール VLAN にアクセスでき、モニタ対象 VLAN が両方のスイッチ間で正常に hello パケットを渡すことができるようにします。

次の図は、スイッチと ASASM の一般的な冗長構成を示します。2 台のスイッチ間のトランクは、フェールオーバー ASASM VLAN (VLAN 10 と 11) を転送します。



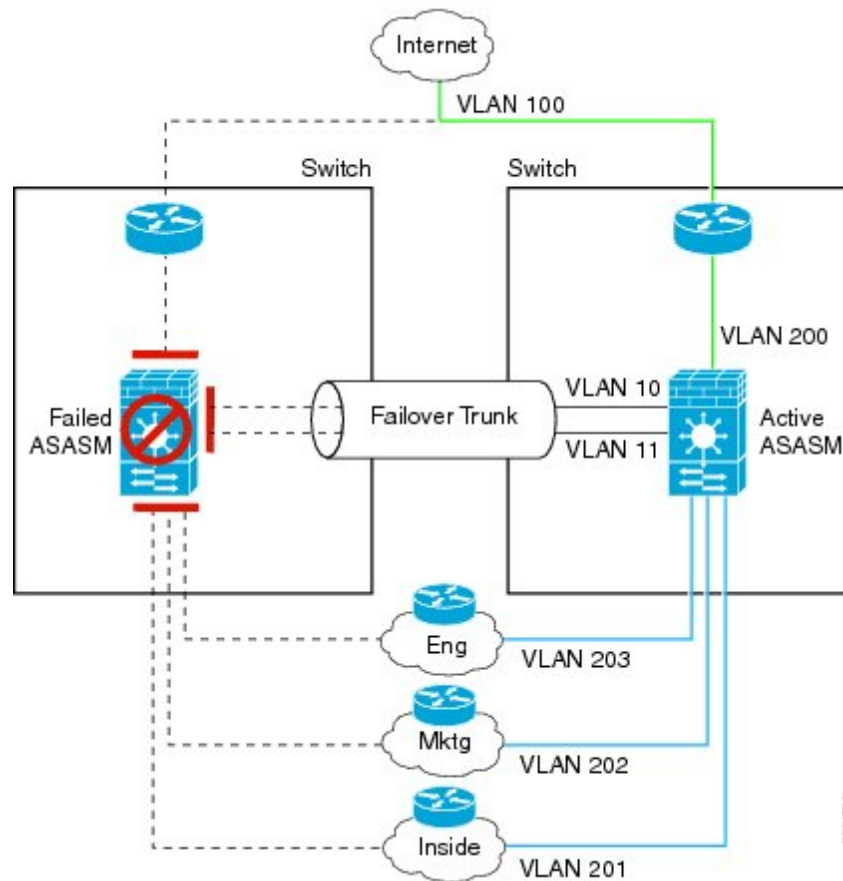
- (注) ASASM のフェールオーバーはスイッチのフェールオーバーに依存しない独立した機能ですが、スイッチのフェールオーバーが発生した場合には、ASASM もそれに対応します。

図 48: 通常の動作



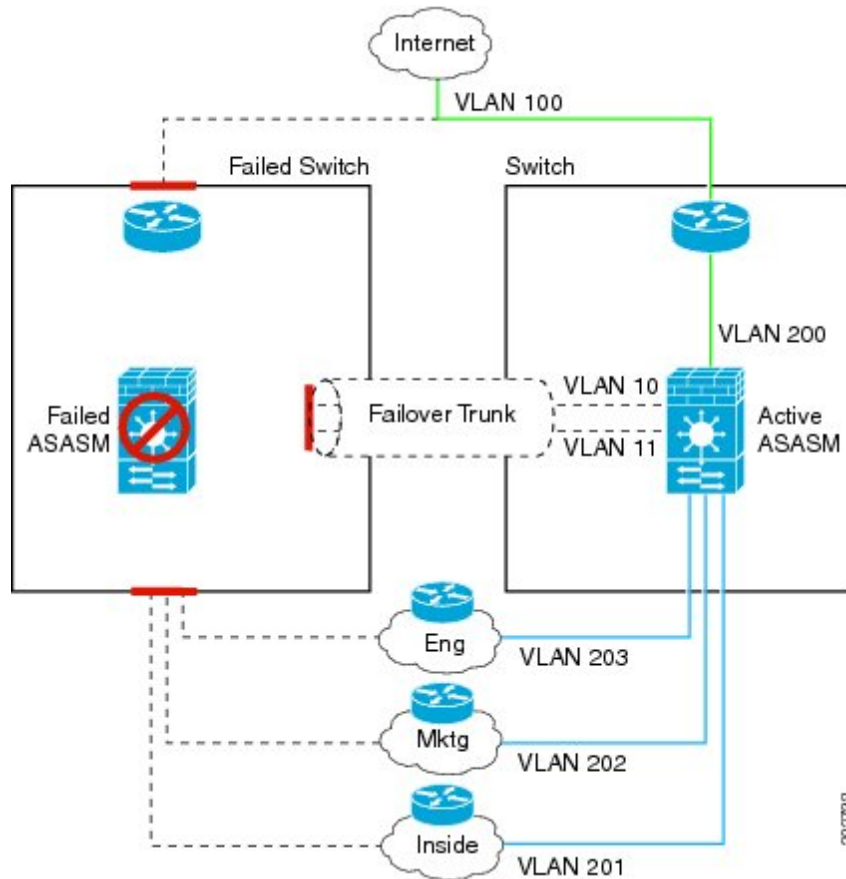
プライマリ ASASM に障害が発生すると、セカンダリ ASASM がアクティブになってファイアウォール VLAN を通過します。

図 49: ASASM の障害



スイッチ全体に障害が発生し、ASASMにも障害が発生した場合（電源切断など）には、スイッチと ASASM の両方でセカンダリ ユニットへのフェールオーバーが実行されます。

図 50: スイッチの障害



ステートレスフェールオーバーとステートフルフェールオーバー

ASA は、アクティブ/スタンバイモードとアクティブ/アクティブモードの両方に対して、ステートレスとステートフルの2種類のフェールオーバーをサポートします。



- (注) クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）は VPN フェールオーバーサブシステムを使用していますが、これはステートフルフェールオーバーの一部です。フェールオーバーペアのメンバ間でこれらの要素を同期するには、ステートフルフェールオーバーを使用する必要があります。ステートレスフェールオーバーは、クライアントレス SSL VPN には推奨されません。

ステートレスフェールオーバー

フェールオーバーが行われると、アクティブ接続はすべてドロップされます。新しいアクティブ装置が引き継ぐ場合、クライアントは接続を再確立する必要があります。



- (注) クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）はVPNフェールオーバーサブシステムを使用していますが、これはステートフルフェールオーバーの一部です。フェールオーバーペアのメンバー間でこれらの要素を同期するには、ステートフルフェールオーバーを使用する必要があります。ステートレス（標準）フェールオーバーは、クライアントレス SSL VPN には推奨できません。

Stateful Failover

ステートフルフェールオーバーが有効の場合、アクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。アクティブ/アクティブフェールオーバーの場合は、アクティブとスタンバイのフェールオーバーグループ間でこれが行われます。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

サポートされる機能

ステートフルフェールオーバーでは、次のステート情報がスタンバイ ASA に渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および状態。他のタイプの IP プロトコルおよび ICMP は、新しいパケットが到着したときに新しいアクティブユニットで確立されるため、アクティブ装置によって解析されません。
- HTTP 接続テーブル（HTTP 複製を有効にしない場合）。
- HTTP 接続状態（HTTP 複製が有効化されている場合）：デフォルトでは、ステートフルフェールオーバーが有効化されているときには、ASA は HTTP セッション情報を複製しません。HTTP レプリケーションを有効にすることをお勧めします。
- ARP テーブル
- レイヤ 2 ブリッジテーブル（ブリッジグループ用）
- ISAKMP および IPsec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリングセッションとピンホール。
- ICMP 接続状態：ICMP 接続の複製は、個々のインターフェイスが非対称ルーティンググループに割り当てられている場合にだけイネーブルになります。
- スタティックおよびダイナミックルーティングテーブル：ステートフルフェールオーバーはダイナミックルーティングプロトコル（OSPF や EIGRP など）に参加するため、アクティブ装置上のダイナミックルーティングプロトコルによる学習ルートが、スタンバイ装置のルーティング情報ベース（RIB）テーブルに維持されます。フェールオーバーイベントで、アクティブなセカンダリユニットには最初にプライマリユニットをミラーリン

グするルールがあるため、パケットは通常は最小限の中断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンスタイマーが開始されます。次に、RIBテーブルのエポック番号が増加します。再コンバージェンス中に、OSPFおよびEIGRPルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルートエントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIBには新しくアクティブになった装置での最新のルーティングプロトコル転送情報が含まれています。



(注) ルートは、アクティブ装置上のリンクアップまたはリンクダウンイベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミックルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイスで設定された DHCP サーバは、DHCP クライアントにアドレスを付与する前にアドレスが使用されていないことを確認するために ping を送信するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS とは関連性はありません。
- Cisco IP SoftPhone セッション：コールセッションステート情報がスタンバイ装置に複製されるため、Cisco IP SoftPhone セッションの実行中にフェールオーバーが起こっても、コールは実行されたままです。コールが終了すると、IP SoftPhone クライアントは Cisco Call Manager との接続を失います。これは、CTIQBE ハングアップメッセージのセッション情報がスタンバイ装置に存在しないために発生します。IP SoftPhone クライアントでは、一定の時間内に CallManager からの応答が受信されない場合、CallManager に到達できないものと判断されて登録が解除されます。
- RA VPN：リモートアクセス VPN エンドユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバープロセス中にパケットを失って、パケット損失から回復できない可能性があります。

サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ ASA に渡されません。

- ユーザ認証 (uauth) テーブル
- TCP ステートバイパス接続
- マルチキャストルーティング。
- ASA FirePOWER モジュールなどのモジュールのステート情報。
- 選択された次のクライアントレス SSL VPN 機能：
 - スマート トンネル

- ポート転送
- プラグイン
- Java アプレット
- IPv6 クライアントレスまたは Anyconnect セッション
- Citrix 認証 (Citrix ユーザはフェールオーバー後に再認証が必要です)

フェールオーバーのトランスペアレント ファイアウォール モード ブリッジグループ要件

ブリッジグループを使用する際に、フェールオーバーの特殊な考慮事項があります。

トランスペアレント モードアプライアンス、ASA のブリッジグループ必須要件

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパンニングツリープロトコル (STP) を実行している接続済みスイッチ ポートは、トポロジ変更を検出すると 30 ~ 50 秒間ブロッキング ステートに移行できます。ポートがブロッキング ステートである間のトラフィックの損失を回避するために、スイッチ ポート モードに応じて次の回避策のいずれかを設定できます。

- アクセス モード : スイッチで STP PortFast 機能をイネーブルにします。

```
interface interface_id
  spanning-tree portfast
```

PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがグループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- トランク モード : EtherType アクセスルールを使用して、ブリッジグループのメンバーインターフェイス上の ASA の BPDU をブロックします。

```
access-list id ethertype deny bpd
access-group id in interface name1
access-group id in interface name2
```

BPDU をブロックすると、スイッチの STP はディセーブルになります。ネットワークレイアウトで ASA を含むループを設定しないでください。

上記のオプションのどちらも使用できない場合は、フェールオーバー機能または STP の安定性に影響する、推奨度の低い次の回避策のいずれかを使用できます。

- インターフェイス モニタリングをディセーブルにします。

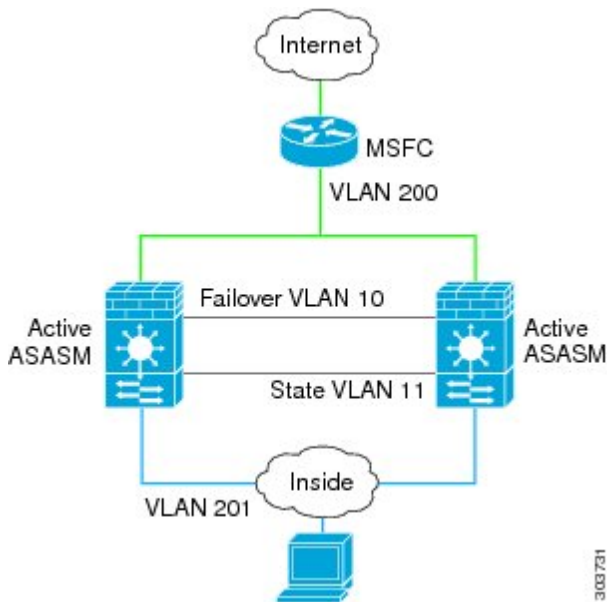
- ASA がフェールオーバーする前に、インターフェイスのホールド時間を STP が収束可能になる大きい値に増やします。
- STP がインターフェイスのホールド時間よりも速く収束するように、STP タイマーを減らします。

トランスペアレントモードASA サービス モジュールのブリッジグループ必須要件

ブリッジグループでのフェールオーバーの使用時にループを回避するには、BPDUの通過を許可し（デフォルト）、BPDU転送をサポートするスイッチソフトウェアを使用する必要があります。

両方のモジュールが互いの存在を検出する場合や、不正なフェールオーバーリンクなどによって、両方のモジュールが同時にアクティブになるときに、ループが発生することがあります。両方の ASASM が2つの同じ VLAN 間でパケットをブリッジングするので、ブリッジグループメンバー間のパケットが両方の ASASM によって無限に複製され、ループが発生します。BPDU がタイミングよく交換された場合は、スパニングツリープロトコルによって、これらのループが遮断されます。ループを遮断するには、VLAN 200 と VLAN 201 間で送信される BPDU をブリッジングする必要があります。

図 51: ブリッジグループループ



フェールオーバーのヘルス モニタ

ASAは、各装置について全体的なヘルスおよびインターフェイスヘルスをモニタします。この項では、各装置の状態を判断するために、ASAがテストを実行する方法について説明します。

ユニットのヘルス モニタリング

ASAは、hello メッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで3回連続してhello メッセージを受信しなかったときは、フェールオーバーリンクを含む各データインターフェイスでLANTESTメッセージを送信し、ピアが応答するかどうかを確認します。ASAが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- ASAがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- ASAがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバーリンクが故障とマークされます。フェールオーバーリンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。
- ASAがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

インターフェイス モニタリング

最大 1025 のインターフェイスを監視できます（マルチコンテキスト モードでは、すべてのコンテキスト間で分割）。重要なインターフェイスをモニタする必要があります。たとえば、マルチコンテキストモードでは、共有インターフェイスを監視するように1つのコンテキストを設定する場合があります（インターフェイスが共有されているため、すべてのコンテキストがそのモニタリングによる利点を得ることができます）。

ユニットは、モニタ対象のインターフェイス上で15秒間helloメッセージを受信しなかった場合に（デフォルト）、インターフェイステストを実行します。（この時間を変更するには、**[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Criteria] > [Failover Poll Times]** を参照してください。）1つのインターフェイスに対するインターフェイステストのいずれかが失敗したものの、他のユニット上のこの同じインターフェイスが正常にトラフィックを渡し続けている場合は、そのインターフェイスに障害があるものと見なされ、ASAはテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ（**[設定 (Configuration)] > [デバイス管理 (Device Management)] > [ハイアベイラビリティとスケラビリティ (High Availability and Scalability)] > [フェールオーバー (Failover)] > [基準 (Criteria)] > [インターフェイスポリシー (Interface Policy)]** を参照）、さらに、アクティブユニットでスタンバイ装置よりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバーインターフェイスポリシーで定義されているフェールオーバー限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したASAは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイモードに戻ります。

ASA FirePOWER モジュールがある場合、ASA はバックプレーンインターフェイスを介してモジュールの健全性もモニタします。モジュールの障害は装置の障害と見なされ、フェールオーバーがトリガーされます。この設定は設定可能です。

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、ASA は IPv4 を使用してヘルス モニタリングを実行します。インターフェイスに IPv6 アドレスだけが設定されている場合、ASA は ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリングテストを実行します。ブロードキャスト ping テストの場合、ASA は IPv6 全ノードアドレス (FE02::1) を使用します。



(注) 障害が発生した装置が回復せず、実際には障害は発生していないと考えられる場合は、**failover reset** コマンドを使用して状態をリセットできます。ただし、フェールオーバー条件が継続している場合、装置は再び障害状態になります。

インターフェイステスト

ASA では、次のインターフェイステストが使用されます。各テストの時間はデフォルトで約 1.5 秒、またはフェールオーバー インターフェイスの保留時間の 1/16 です ([**Configuration**] > [**Device Management**] > [**High Availability and Scalability**] > [**Failover**] > [**Criteria**] > [**Failover Poll Times**] を参照)。

1. リンクアップ/ダウンテスト：インターフェイスステータスのテストです。リンクアップ/ダウンテストでインターフェイスがダウンしていることが示された場合、ASA は障害が発生し、テストが停止したと見なします。ステータスがアップの場合、ASA はネットワークアクティビティを実行します。
2. ネットワーク動作のテスト：ネットワークの受信動作のテストです。テストの開始時に、各装置はインターフェイスの受信パケットカウントをリセットします。テスト中にユニットが適切なパケットを受信すると、すぐにインターフェイスは正常に動作していると思なされます。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると思なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA は ARP テストを開始します。
3. ARP テスト：ARP が正しく応答するかどうかをテストします。各ユニットは、ARP テーブル内の最新のエントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワークトラフィックを受信する場合、インターフェイスは動作していると思なされます。ユニットが ARP 応答を受信しない場合、ASA は、ARP テーブル内の「次の」エントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワークトラフィックを受信する場合、インターフェイスは動作していると思なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると思なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA はブートストラップ ping テストを開始します。

4. **ブロードキャスト Ping テスト** : ping 応答が正しいかどうかをテストします。各ユニットがブロードキャスト ping を送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、インターフェイスは正常に動作していると思なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると思なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARP テストを使用してテストが再開されます。両方の装置が ARP およびブロードキャスト ping テストからトラフィックを受信し続けられない場合、これらのテストは永久に実行し続けます。

Interface Status

モニタ対象のインターフェイスには、次のステータスがあります。

- **Unknown** : 初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合があります。
- **Normal** : インターフェイスはトラフィックを受信しています。
- **Testing** : ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- **Link Down** : インターフェイスまたは VLAN は管理のためにダウンしています。
- **No Link** : インターフェイスの物理リンクがダウンしています。
- **Failed** : インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

フェールオーバー 時間

次の表に、最小、デフォルト、最大フェールオーバー時間を示します。



- (注) CLI または ASDM を使用して手動でフェールオーバーした場合、もしくは ASA をリロードした場合、フェールオーバーはすぐに開始され、次に示すタイマーの影響は受けません。

表 14: ASA

フェールオーバー条件	最小ハードウェア	デフォルト	最大
アクティブ装置で電源断が生じる、または通常の動作が停止する。	800 ミリ秒	15 秒	45 秒
アクティブ ユニットメインボードインターフェイスリンクがダウンする。	500 ミリ秒	5 秒	15 秒

フェールオーバー条件	最小ハードウェア	デフォルト	最大
アクティブ装置の 4GE モジュール インターフェイスリンクがダウンする。	2 秒	5 秒	15 秒
アクティブ ユニット Firepower モジュールは失敗する。	2 秒	2 秒	2 秒
アクティブ装置のインターフェイスは実行されているが、接続の問題によりインターフェイステストを行っている。	5 秒	25 秒	75 秒

設定の同期

フェールオーバーには、さまざまなタイプのコンフィギュレーション同期があります。

コンフィギュレーションの複製の実行

コンフィギュレーションの複製は、フェールオーバー ペア的一方または両方のデバイスのブート時に実行されます。

アクティブ/スタンバイ フェールオーバーでは、コンフィギュレーションは常に、アクティブ装置からスタンバイ装置に同期化されます。

アクティブ/アクティブ フェールオーバーでは、起動ユニットのプライマリまたはセカンダリ指定に関係なく、2番目に起動したユニットは、最初に起動したユニットから実行コンフィギュレーションを取得します。両方のユニットの起動後、システム実行スペースに入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態であるユニットから複製されます。

スタンバイ/セカンドユニットが初期スタートアップを完了すると、実行コンフィギュレーションを削除し（アクティブユニットとの通信に必要な **failover** コマンドを除く）、アクティブユニットはコンフィギュレーション全体をスタンバイ/セカンドユニットに送信します。複製が開始されると、アクティブユニットの ASA コンソールに「Beginning configuration replication: Sending to mate.」というメッセージが表示され、完了すると ASA に「End Configuration Replication to mate.」というメッセージが表示されます。コンフィギュレーションのサイズによって、複製には数秒から数分かかります。

コンフィギュレーションを受信する装置の場合、コンフィギュレーションは実行メモリにだけ存在します。コンフィギュレーションをフラッシュメモリに保存する必要があります。たとえば、アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブ状態であるユニット上のシステム実行スペースに **write memory all** コマンドを入力します。コマンドはピア装置に複製され、コンフィギュレーションがフラッシュメモリに書き込まれます。



(注) 複製中、コンフィギュレーションを送信しているユニット上に入力されたコマンドは、ピアユニットに正常に複製されず、コンフィギュレーションを受信するユニット上に入力されたコマンドは、受信したコンフィギュレーションによって上書きできます。コンフィギュレーションの複製処理中には、フェールオーバーペアのどちらの装置にもコマンドを入力しないでください。



(注) **crypto ca server** コマンドおよび関連するサブコマンドはフェールオーバーをサポートしません。**no crypto ca server** コマンドを使用して削除する必要があります。

File Replication

コンフィギュレーションの同期は次のファイルと構成コンポーネントを複製しません。したがって、これらのファイルが一致するように手動でコピーする必要があります。

- AnyConnect イメージ
- CSD イメージ
- AnyConnect プロファイル

ASA では、フラッシュファイルシステムに保存されたファイルではなく、`cache:/stc/profiles` に保存された AnyConnect クライアント ファイルのキャッシュ済みファイルが使用されます。AnyConnect クライアント プロファイルをスタンバイ装置に複製するには、次のいずれかを実行します。

- アクティブ装置で **write standby** コマンドを入力します。
 - アクティブ装置でプロファイルを再適用します。
 - スタンバイ装置をリロードします。
- ローカル認証局 (CA)
 - ASA イメージ
 - ASDM イメージ

Command Replication

起動した後、アクティブ装置で入力したコマンドはただちにスタンバイ装置に複製されます。コマンドを複製する場合、アクティブ コンフィギュレーションをフラッシュ メモリに保存する必要はありません。

アクティブ/アクティブ フェールオーバーでは、システム実行スペースに入力した変更は、フェールオーバー グループ 1 がアクティブ状態である装置から複製されます。

コマンドの複製を行うのに適切な装置上で変更を入力しなかった場合は、コンフィギュレーションは同期されません。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

スタンバイ ASA に複製されるコマンドは、次のとおりです。

- すべてのコンフィギュレーション コマンド (**mode**、**firewall**、および **failover lan unit** を除く)
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

スタンバイ ASA に複製されないコマンドは、次のとおりです。

- すべての形式の **copy** コマンド (**copy running-config startup-config** を除く)
- すべての形式の **write** コマンド (**write memory** を除く)
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** および **pager**

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ ASA に引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。



- (注) マルチ コンテキスト モードでは、ASA は装置全体 (すべてのコンテキストを含む) のフェールオーバーを行います。各コンテキストを個別にフェールオーバーすることはできません。

プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットがアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリである装置（コンフィギュレーションで指定）とセカンダリである装置との間で、いくつかの相違点があります。

- 両方の装置が同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。
- プライマリユニットのMACアドレスは常に、アクティブIPアドレスと結び付けられています。このルールの例外は、セカンダリユニットがアクティブであり、フェールオーバーリンク経由でプライマリユニットのMACアドレスを取得できない場合に発生します。この場合、セカンダリ装置のMACアドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時にブートされた場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーはユニットごとに行われます。マルチコンテキストモードで動作中のシステムでも、個々のコンテキストまたはコンテキストのグループをフェールオーバーすることはできません。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバーイベントに対して、フェールオーバーポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、スタンバイ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 15: フェールオーバー イベント

障害の状況	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
アクティブ装置が故障（電源またはハードウェア）	フェールオーバー	n/a	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバーリンクでhelloメッセージは受信されません。
以前にアクティブであった装置の復旧	フェールオーバーなし	スタンバイになる	動作なし	なし。

障害の状況	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
スタンバイ装置が故障（電源またはハードウェア）	フェールオーバーなし	スタンバイに故障とマークする	n/a	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	フェールオーバーリンクに故障とマークする	フェールオーバーリンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。
スタートアップ時にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	アクティブになる	スタートアップ時にフェールオーバーリンクがダウンしていると、両方の装置がアクティブになります。
ステートリンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
アクティブ装置におけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイ装置におけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。

アクティブ/アクティブ フェールオーバーの概要

この項では、アクティブ/アクティブ フェールオーバーについて説明します。

アクティブ/アクティブ フェールオーバーの概要

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチコンテキストモードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つまでのフェールオーバー グループに分割します。

フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。フェールオーバー グループをプライマリ ASA でアクティブに割り当て、フェールオーバー グループ 2 をセカンダリ ASA でアクティブに割り当てることができます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。たとえば、インターフェイス障害パターンに応じて、フェールオーバー グループ 1 をセカンダリ ASA にフェールオーバーし、続いてフェールオーバー グループ 2 をプライマリ ASA にフェールオーバーすることができます。このイベントは、プライマリ ASA でフェールオーバー グループ 1 のインターフェイスがダウンしたがセカンダリではアップしており、セカンダリ ASA でフェールオーバー グループ 2 のインターフェイスがダウンしたがプライマリ ASA ではアップしている場合に発生する可能性があります。

管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバーグループ1のメンバです。アクティブ/アクティブ フェールオーバーが必要であるが複数コンテキストは必要ない場合、最もシンプルな設定は他のコンテキストを 1 つ追加し、それをフェールオーバー グループ 2 に割り当てることです。



(注) アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。



(注) 必要に応じて両方のフェールオーバー グループを 1 つの ASA に割り当てることもできますが、この場合、アクティブな ASA を 2 つ持つというメリットはありません。

フェールオーバー グループのプライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーと同様、アクティブ/アクティブ フェールオーバー ペアの 1 つの装置がプライマリ ユニットに指定され、もう 1 つの装置がセカンダリ ユニットに指定されます。アクティブ/スタンバイ フェールオーバーの場合とは異なり、両方の装置が同時に起動された場合、この指定ではどちらの装置がアクティブになるか指示しません。代わりに、プライマリまたはセカンダリの指定時に、次の 2 つの点を判定します。

- ペアが同時に起動したときに、プライマリ装置が実行コンフィギュレーションを提供します。
- コンフィギュレーションの各フェールオーバーグループは、プライマリまたはセカンダリ装置プリファレンスが設定されます。プリエンブションで使用すると、このプリファレンスはフェールオーバーグループが起動後に正しいユニットで実行されるようにします。プリエンブションがない場合、両方のグループは最初に起動したユニットで動作します。

起動時のフェールオーバーグループのアクティブ装置の決定

フェールオーバーグループがアクティブになる装置は、次のように決定されます。

- ピア装置が使用できないときに装置がブートされると、両方のフェールオーバーグループがピア装置でアクティブになります。
- ピア装置がアクティブ（両方のフェールオーバーグループがアクティブ状態）の場合に装置がブートされると、フェールオーバーグループは、アクティブ装置でアクティブ状態のままになります。これは、次のいずれかの状態になるまで、フェールオーバーグループのプライマリプリファレンスまたはセカンダリプリファレンスには関係ありません。
 - フェールオーバーが発生した。
 - 手動でフェールオーバーを強制実行した。
 - フェールオーバーグループにプリエンブションを設定した。この設定により、優先する装置が使用可能になると、フェールオーバーグループはその装置上で自動的にアクティブになります。

フェールオーバーイベント

アクティブ/アクティブフェールオーバーコンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバーグループごとに行われます。たとえば、プライマリ装置で両方のフェールオーバーグループをアクティブと指定し、フェールオーバーグループ1が故障すると、フェールオーバーグループ2はプライマリ装置でアクティブのままですが、フェールオーバーグループ1はセカンダリ装置でアクティブになります。

フェールオーバーグループには複数のコンテキストを含めることができ、また各コンテキストには複数のインターフェイスを含めることができるので、1つのコンテキストのインターフェイスがすべて故障しても、そのコンテキストに関連するフェールオーバーグループが故障と判断されない可能性があります。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。各障害イベントに対して、ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブフェールオーバーグループのアクション、およびスタンバイフェールオーバーグループのアクションを示します。

フェールオーバー イベント

表 16: フェールオーバー イベント

障害の状況	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
装置で電源断またはソフトウェア障害が発生した	フェールオーバー	スタンバイになり、故障とマークする	アクティブになる アクティブに故障とマークする	フェールオーバーペアの装置が故障すると、その装置のアクティブフェールオーバーグループはすべて故障とマークされ、ピア装置のフェールオーバーグループがアクティブになります。
アクティブフェールオーバーグループにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブグループに故障とマークする	アクティブになる	なし。
スタンバイフェールオーバーグループにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイグループに故障とマークする	スタンバイフェールオーバーグループが故障とマークされている場合、インターフェイスフェールオーバー障害しきい値を超えても、アクティブフェールオーバーグループはフェールオーバーを行いません。
以前にアクティブであったフェールオーバーグループの復旧	フェールオーバーなし	動作なし	動作なし	フェールオーバーグループのプリエンプションが設定されている場合を除き、フェールオーバーグループは現在の装置でアクティブのままです。
スタートアップ時にフェールオーバーリンクに障害が発生した	フェールオーバーなし	アクティブになる	アクティブになる	スタートアップ時にフェールオーバーリンクがダウンしていると、両方の装置の両方のフェールオーバーグループがアクティブになります。

障害の状況	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
ステートリンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	n/a	n/a	各装置で、フェールオーバーリンクが故障とマークされます。フェールオーバーリンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。

フェールオーバーのライセンス

フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバークラスライセンスに結合されます。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5506-X および ASA 5506W-X	<ul style="list-style-type: none"> • アクティブ/スタンバイ：Security Plus ライセンス。 • アクティブ/アクティブ：サポートなし。 <p>(注) 各ユニットに同じ暗号化ライセンスが必要です。</p>

モデル	ライセンス要件
ASA 5512-X ~ ASA 5555-X	<ul style="list-style-type: none"> • ASA 5512 : Security Plus ライセンス。 • その他のモデル : 基本ライセンス。 <p>(注)</p> <ul style="list-style-type: none"> • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。 • 各ユニットに同じ IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。 <ul style="list-style-type: none"> • IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です (ASA5525-IPS-K9 のように、製品番号に「IPS」が含まれている必要があります)。IPS 以外の製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。 • 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。 • IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
ASAv	<p>ASAv のフェールオーバー ライセンス (176 ページ) を参照してください。</p>

モデル	ライセンス要件
Firepower 9300	Firepower 9300 シャーシの ASA のフェールオーバー ライセンス (176 ページ) を参照してください。
他のすべてのモデル	基本ライセンスまたは標準ライセンス。 (注) <ul style="list-style-type: none"> 各ユニットに同じ暗号化ライセンスが必要です。 マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。



(注) 有効な永続キーが必要です。まれに、PAK 認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

フェールオーバーのガイドライン

コンテキスト モード

- アクティブ/アクティブ モードは、マルチ コンテキスト モードでのみサポートされます。
- マルチ コンテキスト モードでは、特に注記がない限り、手順はすべてシステム実行スペースで実行します。
- ステートフル フェールオーバーは、マルチ コンテキスト モードの AnyConnect 接続ではサポートされません。

サポート モデル

- ASA 5506W-X : 内部 GigabitEthernet 1/9 インターフェイスのインターフェイス モニタリングを無効にする必要があります。これらのインターフェイスは、デフォルトのインターフェイス モニタリング チェックを実行するために通信することができないため、予期されたインターフェイス通信の障害により、スイッチがアクティブからスタンバイに切り替えられ、元に戻ります。
- Firepower 9300 : シャーシ間フェールオーバーを使用して最良の冗長性を確保することを推奨します。
- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク 上の ASA では、レイヤ 2 接続が必要なため、フェールオーバーはサポートされません。

- ASA FirePOWER モジュールはフェールオーバーを直接サポートしていません。ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールが、その転送の時点からトラフィックの検査を開始します。古いインスペクションのステートは転送されません。
- フェールオーバーの動作の整合性を保つために、ハイアベイラビリティな ASA ペアの ASA FirePOWER モジュールで一貫したポリシーを保持する必要があります。



- (注) ASA FirePOWER モジュールを設定する前に、フェールオーバーペアを作成します。モジュールが両方のデバイスにすでに設定されている場合は、フェールオーバーペアを作成する前にスタンバイデバイスのインターフェイスの設定をクリアします。スタンバイデバイスの CLI から、**clear configure interface** コマンドを入力します。

ハイアベイラビリティのための ASA フェールオーバー

ASA を使用してフェールオーバーペアを作成する場合は、データインターフェイスを各 ASA に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASA に追加されると、ASA コンソールにエラーが表示される可能性があります。また、フェールオーバー機能にも影響が出る可能性があります。

その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパンニングツリープロトコル (STP) を実行している接続済みスイッチポートは、トポロジ変更を検出すると 30 ~ 50 秒間ブロッキングステートに移行できます。ポートがブロッキングステートである間のトラフィック損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

interface interface_id spanning-tree portfast

この回避策は、ルーテッドモードおよびブリッジグループインターフェイスの両方に接続されているスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディングモードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがグループの一部になる場合、最終的には STP ブロッキングモードに遷移します。

- ローカル CA サーバが設定されている場合、フェールオーバーを有効にできません。CA コンフィギュレーションを削除するには、**no crypto ca server** コマンドを使用します。
- ASA フェールオーバーペアに接続されたスイッチ上でポートセキュリティを設定すると、フェールオーバーイベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュアポートで設定または学習されたセキュア MAC アドレスが別のセキュアポートに移動し、スイッチのポートセキュリティ機能によって違反フラグが付けられた場合に発生します。

- すべてのコンテキストにわたり、1台の装置の最大1025のインターフェイスをモニタできます。
- アクティブ/スタンバイ フェールオーバーと VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブ ユニットとスタンバイ ユニットの両方をモニタすることはできません。スタンバイ ユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。
- アクティブ/アクティブ フェールオーバーでは、同じコンテキスト内の2つのインターフェイスを同じ ASR グループ内で設定することはできません。
- アクティブ/アクティブ フェールオーバーでは、最大2つのフェールオーバー グループを定義できます。
- アクティブ/アクティブ フェールオーバーでフェールオーバー グループを削除する場合は、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には常に管理コンテキストが含まれます。フェールオーバー グループに割り当てられていないコンテキストはすべて、デフォルトでフェールオーバー グループ 1 になります。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。

フェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次の事項が含まれます。

- ステートフル フェールオーバーでの HTTP 複製は行われません。
- 単一のインターフェイス障害でフェールオーバーが行われます。
- インターフェイスのポーリング時間は5秒です。
- インターフェイスのホールド時間は25秒です。
- 装置のポーリング時間は1秒です。
- 装置のホールド時間は15秒です。
- 仮想MACアドレスはマルチコンテキストモードで無効化されていますが、ASASMでは、デフォルトで有効になっています。
- すべての物理インターフェイスをモニタリングします。ASASMでは、すべてのVLANインターフェイスをモニタリングします。

アクティブ/スタンバイ フェールオーバーの設定

アクティブ/スタンバイ フェールオーバーを設定するには、プライマリ装置とセカンダリ装置の両方で基本的なフェールオーバー設定を構成します。その他すべての設定をプライマリ装置でのみ行った後、セカンダリ装置に設定を同期させます。

High Availability and Scalability Wizard を使用して、手順を踏んでアクティブ/スタンバイ フェールオーバー コンフィギュレーションを作成することができます。

手順

- ステップ 1** [Wizards] > [High Availability and Scalability] を選択します。次の手順でこのウィザードのガイドラインを確認してください。
- ステップ 2** [Failover Peer Connectivity and Compatibility] 画面で、ピア装置の IP アドレスを入力します。このアドレスは、ASDM アクセスがイネーブルになっているインターフェイスである必要があります。デフォルトでは、ピアアドレスは ASDM 管理インターフェイスのスタンバイアドレスに割り当てられます。
- ステップ 3** [LAN Link Configuration] 画面で次のように設定します。
- [Interface] : 物理インターフェイス ID、サブインターフェイス ID、冗長インターフェイス ID、または EtherChannel インターフェイス ID を指定できます。ASASM の場合、インターフェイスは VLAN ID です。Firepower 9300 では、任意のデータタイプ インターフェイスを使用できます。
 - [Active IP Address] : この IP アドレスは、未使用のサブネット上にある必要があります。169.254.0.0/16 と fd00:0:0::*:/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。
 - [Standby IP Address] : この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。
 - (オプション) [Communications Encryption] : フェールオーバーリンクの通信を暗号化します。注：秘密キーの代わりに、IPsec 事前共有キーを使用することをお勧めします。これはウィザードを終了した後設定できます ([フェールオーバーの設定変更 \(320 ページ\)](#) を参照)。
- ステップ 4** ステートフル フェールオーバー用に別のインターフェイスを選択する場合は、[State Link Configuration] 画面で次の設定を行います。
- [Active IP Address] : この IP アドレスは、フェールオーバーリンクとは異なる未使用のサブネット上にある必要があります。169.254.0.0/16 と fd00:0:0::*:/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。

- [Standby IP Address] : この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。

ステップ 5 [Finish] をクリックすると、ウィザードは [Waiting for Config Sync] 画面を表示します。

指定された時間が経過した後、ウィザードはセカンダリ装置にフェールオーバー設定を送信し、フェールオーバー設定が完了したことを示す情報画面が表示されます。

- フェールオーバーがセカンダリ装置でイネーブルになっているかどうか分からない場合は、指定した時間だけ待ちます。
- フェールオーバーがすでにイネーブルなことがわかっている場合は、[Skip configuring peer] をクリックします。
- セカンダリ装置でフェールオーバーがイネーブルでないことがわかっている場合は、[Stop waiting xx more seconds] をクリックすると、フェールオーバーのブートストラップ設定はすぐにセカンダリ装置に送信されます。

アクティブ/アクティブ フェールオーバーの設定

ここでは、アクティブ/アクティブ フェールオーバーの設定方法について説明します。

High Availability and Scalability Wizard を使用して、手順を踏んでアクティブ/アクティブ フェールオーバー コンフィギュレーションを作成することができます。

手順

ステップ 1 [Wizards] > [High Availability and Scalability] を選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2 [Failover Peer Connectivity and Compatibility Check] 画面では、ピアの IP アドレスは、ASDM アクセスが有効になっているインターフェイスである必要があります。

デフォルトでは、ピアアドレスは、ASDM の接続先インターフェイスのスタンバイ アドレスに割り当てられます。

ステップ 3 [Security Context Configuration] 画面では、ウィザード内でマルチ コンテキスト モードに変換した場合、管理コンテキストのみが表示されます。ウィザードを終了した後他のコンテキストを追加できます。

ステップ 4 [LAN Link Configuration] 画面で次のように設定します。

- [Interface] : 物理インターフェイス ID、サブインターフェイス ID、冗長インターフェイス ID、または EtherChannel インターフェイス ID を指定できます。ASASM では、インターフェイス ID は VLAN ID です。Firepower 9300 では、任意のデータタイプ インターフェイスを使用できます。

- [Active IP Address] : この IP アドレスは、未使用のサブネット上にある必要があります。169.254.0.0/16 と fd00:0:0::*:/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。
- [Standby IP Address] : この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。
- (オプション) [Communications Encryption] : フェールオーバーリンクの通信を暗号化します。**注** : 秘密キーの代わりに、IPsec 事前共有キーを使用することをお勧めします。これはウィザードを終了した後に設定できます ([フェールオーバーの設定変更 \(320 ページ\)](#) を参照)。

ステップ 5 ステートフル フェールオーバー用に別のインターフェイスを選択する場合は、[State Link Configuration] 画面で次の設定を行います。

- [Active IP Address] : この IP アドレスは、フェールオーバーリンクとは異なる未使用のサブネット上にある必要があります。169.254.0.0/16 と fd00:0:0::*:/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。
- [Standby IP Address] : この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。

ステップ 6 [Finish] をクリックすると、ウィザードは [Waiting for Config Sync] 画面を表示します。

指定された時間が経過した後に、ウィザードはセカンダリ装置にフェールオーバー設定を送信し、フェールオーバー設定が完了したことを示す情報画面が表示されます。

- フェールオーバーがセカンダリ装置でイネーブルになっているかどうかわからない場合は、指定した時間だけ待ちます。
- フェールオーバーがすでにイネーブルなことがわかっている場合は、[Skip configuring peer] をクリックします。
- セカンダリ装置でフェールオーバーがイネーブルでないことがわかっている場合は、[Stop waiting xx more seconds] をクリックすると、フェールオーバーのブートストラップ設定はすぐにセカンダリ装置に送信されます。

オプションのフェールオーバーパラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

フェールオーバー基準とその他の設定の構成

この項で変更可能な多くのパラメータのデフォルト設定については、[フェールオーバーのデフォルト \(309ページ\)](#) を参照してください。アクティブ/アクティブモードでは、ほとんどの条件をフェールオーバーグループごとに設定します。ここでは、アクティブ/アクティブモードでのフェールオーバーグループごとのHTTP複製のイネーブル化について説明します。アクティブ/スタンバイモードでHTTP複製を設定する場合は、[フェールオーバーの設定変更 \(320ページ\)](#) を参照してください。

始める前に

- マルチコンテキストモードのシステム実行スペースで次の設定を行います。

手順

- ステップ 1** [Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] の順に選択します。
- ステップ 2** スタンバイ装置またはコンテキストのコンフィギュレーションを直接変更できないようにするには、[Setup] タブをクリックし、[Disable configuration changes on the standby unit] チェックボックスをオンにします。

デフォルトでは、スタンバイユニットまたはスタンバイコンテキストに対するコンフィギュレーションは、警告メッセージ付きで許可されます。
- ステップ 3** [Criteria] タブをクリックします。
- ステップ 4** 装置のポーリング時間を設定します。

[Failover Poll Times] 領域で、次を設定します。
 - [Unit Failover] : 装置間の Hello メッセージの間の時間。範囲は 1 ~ 15 秒または 200 ~ 999 ミリ秒です。
 - [Unit Hold Time] : 装置がフェールオーバーリンク上で Hello メッセージを受信する必要がある時間（この時間に受信しなかった場合は、装置がピアの障害のテストプロセスを開始する）を設定します。範囲は 1 ~ 45 秒または 800 ~ 999 ミリ秒です。ポーリング時間の 3 倍より少ない値は入力できません。

(注) このペインの他の設定はアクティブ/スタンバイモードにのみ適用されます。アクティブ/アクティブモードでは、フェールオーバーグループごとに残りのパラメータを設定する必要があります。
- ステップ 5** (アクティブ/アクティブモードのみ) [Active/Active] タブをクリックし、フェールオーバーグループを選択して [Edit] をクリックします。
- ステップ 6** (アクティブ/アクティブモードのみ) プリエンプションでの使用時にフェールオーバーグループの優先するロールを変更するには、[Primary] または [Secondary] をクリックします。

ウィザードを使用した場合、フェールオーバーグループ1はプライマリ装置に割り当てられ、フェールオーバーグループ2はセカンダリ装置に割り当てられます。標準以外の設定が必要な場合は、別の装置を優先するように指定できます。これらの設定は、プリエンプション処理の設定と併用してのみ使用されます。グループの **primary** または **secondary** の設定にかかわらず、両方のフェールオーバーグループが最初にブートしたユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。

ステップ7 (アクティブ/アクティブモードのみ) フェールオーバーグループプリエンプションを設定するには、[Preempt after booting with optional delay of] チェック ボックスをオンにします。

グループの **primary** または **secondary** の設定にかかわらず、両方のフェールオーバーグループが最初にブートしたユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。

オプションの **delay** 値に秒数を入力して、その時間フェールオーバーグループが現在の装置でアクティブ状態に維持され、その後指定された装置で自動的にアクティブになるようにできます。有効な値は 1 ~ 1200 です。

手動でフェールオーバーすると、プリエンプション処理のオプションが無視されます。

(注) ステートフルフェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバーグループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

ステップ8 [Interface Policy] を設定します。

- [Number of failed interfaces that triggers failover] : フェールオーバーをトリガーするために必要な障害が発生したインターフェイスの具体的な数を 1 ~ 250 で定義します。障害が発生したモニタ対象インターフェイスの数が指定した値を超えると、ASA はフェールオーバーします。
- [Percentage of failed interfaces that triggers failover] : フェールオーバーをトリガーするために必要な障害が発生した設定済みインターフェイスの割合を定義します。障害が発生したモニタ対象インターフェイスの数が設定した割合を超えると、ASA はフェールオーバーします。

(注) [Use system failover interface policy] オプションは使用しないでください。現時点ではグループごとのポリシーのみが設定できます。

ステップ9 (アクティブ/スタンバイ モード) インターフェイスのポーリング時間を設定します。

[Failover Poll Time] 領域で、次を設定します。

- **Monitored Interfaces** : インターフェイスのポーリング時間を指定します。ピアに hello パケットを送信するまで待機する時間。範囲は 1 ~ 15 秒または 500 ~ 999 ミリ秒です。デフォルトは 5 秒です。
- **Interface Hold Time** : ピアユニットからの最後に受信した hello メッセージとインターフェイステストの開始との間の時間（計算として）を設定して、インターフェイスの健全性を判断します。また、各インターフェイステストの期間を *holdtime/16* として設定します。

有効な値は 5～75 秒です。デフォルトは、`polltime` の 5 倍です。`polltime` の 5 倍よりも短い `holdtime` 値は入力できません。

インターフェイステストを開始するまでの時間 (y) を計算するには、次のようにします。

1. $x = (\text{holdtime}/\text{polltime})/2$ 、最も近い整数に丸められます。(4 以下は切り下げ、.5 以上は切り上げ。)
2. $y = x * \text{polltime}$

たとえば、デフォルトの `holdtime` は 25 で、`polltime` が 5 の場合は y は 15 秒です。

アクティブ/アクティブモードの場合、[Add/Edit Failover Group] ダイアログボックスでインターフェイスポーリング時間を設定します。

ステップ 10 (アクティブ/アクティブモードのみ) HTTP 複製をイネーブルにするには、[Enable HTTP Replication] チェックボックスをオンにします。

セッションの複製レートについては、「[フェールオーバーの設定変更 \(320 ページ\)](#)」の項を参照してください。

(注) フェールオーバーを使用しているときに、スタンバイ装置から HTTP フローを削除すると遅延が生じます。このため `show conn count` 出力には、アクティブ装置とスタンバイ装置で異なる数が表示されることがあります。数秒待ってコマンドを再発行すると、両方の装置で同じカウントが表示されます。

ステップ 11 仮想 MAC アドレスを設定します。

- アクティブ/スタンバイモード: [MAC Addresses] タブをクリックし、[Add] をクリックします。

[Add/Edit Interface MAC Address] ダイアログボックスが表示されます。

- アクティブ/アクティブモード: [Active/Active] [タブの下部に移動します。

他の方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

- a) [Physical Interface] ドロップダウンリストからインターフェイスを選択します。
- b) [Active MAC Address] フィールドに、アクティブインターフェイスの新しい MAC アドレスを入力します。
- c) [Standby MAC Address] フィールドに、スタンバイインターフェイスの新しい MAC アドレスを入力します。
- d) [OK] をクリックします。(アクティブ/アクティブモードのみ) 再度 [OK] をクリックします。

ステップ 12 [Apply] をクリックします。

インターフェイス モニタリングの設定およびスタンバイ アドレスの設定

デフォルトでは、すべての物理インターフェイス、またはASASMの場合、すべてのVLANインターフェイス、およびASAにインストールされるすべてのハードウェアまたはソフトウェアモジュール（ASA FirePOWER モジュールなど）でモニタリングが有効になっています。

重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないように除外できます。

装置ごとに最大 1025 のインターフェイスをモニタできます（マルチ コンテキスト モードのすべてのコンテキストにわたって）。

ウィザードでスタンバイ IP アドレスを設定しなかった場合は、手動で設定できます。

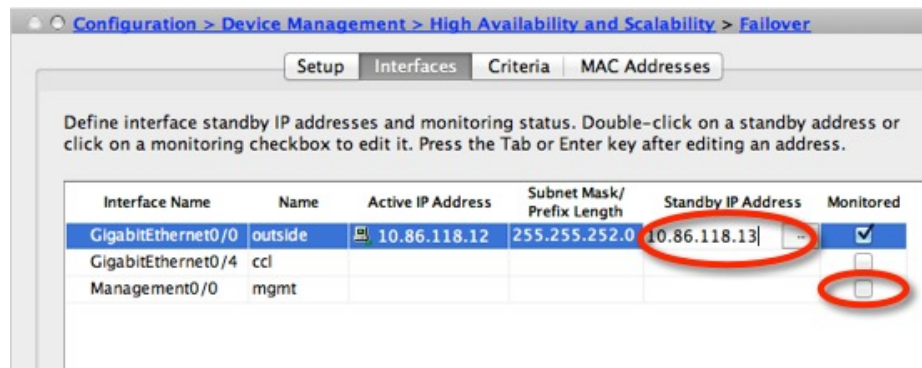
始める前に

マルチ コンテキスト モードで、各コンテキスト内のインターフェイスを設定します。

手順

ステップ 1 シングルモードでは、**[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces]** の順に選択します。

マルチ コンテキスト モードでは、コンテキスト内で **[Configuration] > [Device Management] > [Failover] > [Interfaces]** を選択します。



設定されているインターフェイスのリストが、ASA FirePOWER モジュールなどのすべてのインストール済みのハードウェア/ソフトウェア モジュールと共に表示されます。[Monitored] カラムに、フェールオーバー基準の一部としてインターフェイスがモニタされているかどうかが表示されます。モニタされている場合は、[Monitored] チェック ボックスがオンになっています。

特定のハードウェア/ソフトウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングを無効化できます。なお、ASA

5585-X では、サービス モジュールのモニタリングを無効にする場合、個別にモニタされるモジュール上の各インターフェイスのモニタリングを無効にすることもできます。

各インターフェイスの IP アドレスが [Active IP Address] カラムに表示されます。インターフェイスのスタンバイ IP アドレスが設定されている場合は、[Standby IP address] カラムに表示されます。フェールオーバーリンクおよびステートリンクについては IP アドレスは表示されません。これらのアドレスはこのタブから変更できません。

- ステップ 2 表示されているインターフェイスのモニタリングをディセーブルにするには、インターフェイスの [Monitored] チェックボックスをオフにします。
- ステップ 3 表示されているインターフェイスのモニタリングをイネーブルにするには、インターフェイスの [Monitored] チェックボックスをオンにします。
- ステップ 4 スタンバイ IP アドレスを持っていない各インターフェイスに対して、[Standby IP Address] フィールドをダブルクリックしてフィールドに IP アドレスを入力します。
- ステップ 5 [Apply] をクリックします。

非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブモード）

アクティブ/アクティブ フェールオーバーでの実行中に、ピア装置を経由して開始された接続に対する返送パケットを、装置が受信する場合があります。そのパケットを受信する ASA にはそのパケットの接続情報がないために、パケットはドロップされます。このドロップが多く発生するのは、アクティブ/アクティブ フェールオーバー ペアの 2 台の ASA が異なるサービスプロバイダーに接続されており、アウトバウンド接続に NAT アドレスが使用されていない場合です。

返送パケットのドロップは、非対称にルーティングされたパケットを許可することによって防ぐことができます。そのためには、それぞれの ASA の同様のインターフェイスを同じ ASR グループに割り当てます。たとえば、両方の ASA が、内部インターフェイスでは同じ内部ネットワークに接続している一方、外部インターフェイスでは別の ISP に接続しているとします。プライマリ装置で、アクティブ コンテキストの外部インターフェイスを ASR グループ 1 に割り当て、セカンダリ装置でも、アクティブ コンテキストの外部インターフェイスを同じ ASR グループ 1 に割り当てます。プライマリ装置の外部インターフェイスがセッション情報を持たないパケットを受信すると、同じグループ（この場合 ASR グループ 1）内のスタンバイ コンテキストの他のインターフェイスのセッション情報をチェックします。一致する情報が見つからない場合、パケットはドロップされます。一致する情報が見つかり、次の動作のうちいずれかが開始します。

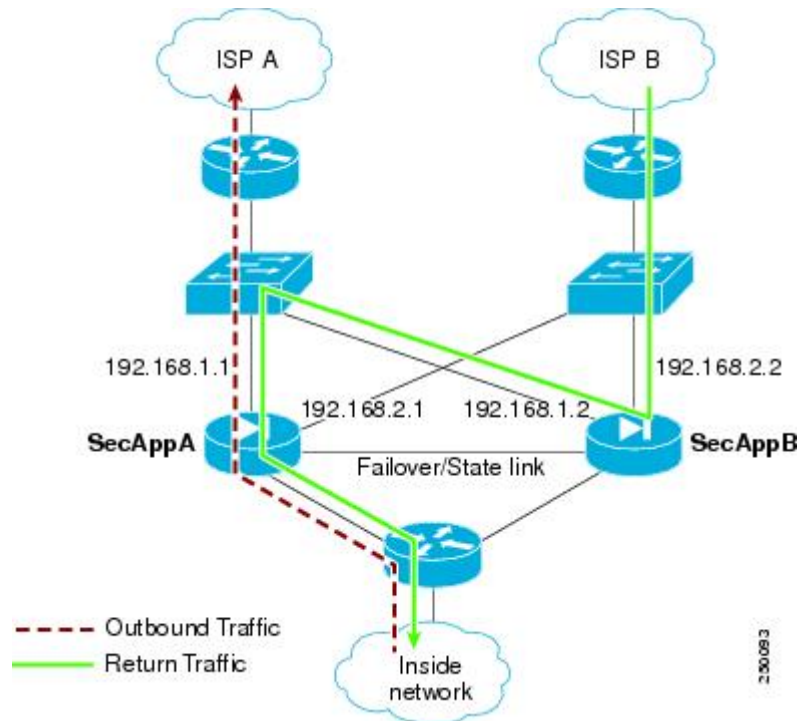
- 着信トラフィックがピア装置に発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットは他の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。
- 着信トラフィックが同じ装置の別のインターフェイスに発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットはストリームに再注入されます。



(注) この機能は、非対称ルーティングを提供しません。非対称にルーティングされたパケットを正しいインターフェイスに戻します。

次の図に、非対称にルーティングされたパケットの例を示します。

図 52: ASR の例



1. アウトバウンドセッションが、アクティブな SecAppA コンテキストを持つ ASA を通過します。このパケットは、インターフェイス外の ISP-A (192.168.1.1) から送信されます。
2. 非対称ルーティングがアップストリームのどこかで設定されているため、リターントラフィックは、アクティブな SecAppB コンテキストを持つ ASA のインターフェイス外部の ISP-B (192.168.2.2) 経由で戻ります。
3. 通常、リターントラフィックは、そのインターフェイス 192.168.2.2 上にリターントラフィックに関するセッション情報がないので、ドロップされます。しかし、このインターフェイスは、ASR グループ 1 の一部として設定されています。装置は、同じ ASR グループ ID で設定された他のインターフェイス上のセッションを探します。
4. このセッション情報は、SecAppB を持つ装置上のスタンバイ状態のインターフェイス outsideISP-A (192.168.1.2) にあります。ステートフルフェールオーバーは、SecAppA から SecAppB にセッション情報を複製します。
5. ドロップされる代わりに、レイヤ 2 ヘッダーはインターフェイス 192.168.1.1 の情報で書き直され、トラフィックはインターフェイス 192.168.1.2 からリダイレクトされます。そこか

ら、発信元の装置のインターフェイスを経由して戻ります (SecAppA の 192.168.1.1)。この転送は、必要に応じて、セッションが終了するまで続行されます。

始める前に

- ステートフル フェールオーバー：アクティブ フェールオーバー グループにあるインターフェイスのセッションのステート情報を、スタンバイ フェールオーバー グループに渡します。
- replication http：HTTPセッションのステート情報は、スタンバイ フェールオーバー グループに渡されないため、スタンバイ インターフェイスに存在しません。ASA が非対称にルーティングされた HTTP パケットを再ルーティングできるように、HTTP ステート情報を複製する必要があります。
- プライマリ装置およびセカンダリ装置の各アクティブ コンテキスト内でこの手順を実行します。
- コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキスト インターフェイスも ASR グループに含めることはできません。

手順

-
- ステップ 1 プライマリ装置のアクティブ コンテキストで、**[Configuration] > [Device Setup] > [Routing] > [ASR Groups]** の順に選択します。
 - ステップ 2 非対称にルーティングされたパケットを受信するインターフェイスについて、ドロップダウンリストから **ASR グループ ID** を選択します。
 - ステップ 3 **[Apply]** をクリックし、変更内容を実行コンフィギュレーションに保存します。
 - ステップ 4 ASDM をセカンダリ装置に接続し、プライマリ装置のコンテキストと同様のアクティブ コンテキストを選択します。
 - ステップ 5 **[Configuration] > [Device Setup] > [Routing] > [ASR Groups]** の順に選択します。
 - ステップ 6 この装置の同様のインターフェイスについて、同じ **ASR グループ ID** を選択します。
 - ステップ 7 **[Apply]** をクリックし、変更内容を実行コンフィギュレーションに保存します。
-

フェールオーバーの管理

この項では、フェールオーバーの設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、フェールオーバーをイネーブルにした後にフェールオーバー装置を管理する方法について説明します。

フェールオーバーの設定変更

ウィザードを使用しない場合や、設定を変更する場合に、手動でフェールオーバーを設定できます。ここでは、ウィザードに含まれていないため手動で設定する必要がある次のオプションについても説明します。

- フェールオーバー トラフィックを暗号化するための IPsec 事前共有キー
- HTTP 複製レート
- HTTP 複製 (アクティブ/スタンバイ モード)

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 シングルモードでは、**[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup]** の順に選択します。

マルチ コンテキスト モードでは、システム実行スペースで **[Configuration] > [Device Management] > [Failover] > [Setup]** を選択します。

ステップ 2 **[Enable Failover]** チェックボックスをオンにします。

(注) デバイスに変更を適用するまで、フェールオーバーは実際にはイネーブルになりません。

ステップ 3 フェールオーバー リンクおよびステート リンクの通信を暗号化するには、次のオプションのいずれかを使用します。

- **[IPsec Preshared Key]** (優先) : フェールオーバー装置間のフェールオーバーリンクで IPsec LAN-to-LAN トンネルを確立するために、IKEv2 によって使用される事前共有キーです。
注: フェールオーバー LAN-to-LAN トンネルは、IPsec (他の VPN) ライセンスには適用されません。
- **[Secret Key]** : フェールオーバー通信の暗号化に使用される秘密キーを入力します。このフィールドを空白のままにした場合は、コマンド複製中に送信されるコンフィギュレーション内のパスワードまたはキーを含め、フェールオーバー通信がクリアテキストになります。

[Use 32 hexadecimal character key] : 秘密キーに 32 文字の 16 進キーを使用するには、このチェック ボックスをオンにします。

ステップ 4 **[LAN Failover]** 領域で、フェールオーバー リンクの次のパラメータを設定します。

- **[Interface]** : フェールオーバー リンクに使用するインターフェイスを選択します。フェールオーバーには専用インターフェイスが必要ですが、ステートフルフェールオーバーとインターフェイスを共有できます。

このリストには、未設定のインターフェイスまたはサブインターフェイスのみが表示され、フェールオーバーリンクとして選択できます。インターフェイスをフェールオーバーリンクに指定すると、そのインターフェイスは **[Configuration] > [Interfaces]** ペインでは編集できません。

- **[Logical Name]** : 「failover」などのフェールオーバー通信に使用するインターフェイスの論理名を指定します。この名前は情報を提供するためのものです。
- **[Active IP]** : インターフェイスのアクティブ IP アドレスを指定します。IP アドレスは、IPv4 または IPv6 アドレスのどちらにすることもできます。この IP アドレスは未使用のサブネット上になければなりません。
- **[Standby IP]** : インターフェイスのスタンバイ IP アドレスを指定します。アクティブ IP アドレスと同じサブネット上のアドレスを指定します。
- **[Subnet Mask]** : サブネット マスクを指定します。
- **[Preferred Role]** : この ASA の優先されるロールがプライマリ装置であるかセカンダリ装置であるかを指定するために、**[Primary]** または **[Secondary]** を選択します。

ステップ 5 (オプション) 次の手順でステート リンクを設定します。

- **[Interface]** : ステートリンクに使用するインターフェイスを選択します。選択できるのは、未設定のインターフェイスまたはサブインターフェイス、フェールオーバーリンク、または **[--Use Named--]** オプションです。

(注) フェールオーバー リンク専用インターフェイスとステート リンク専用インターフェイスの 2 つのインターフェイスを別々に使用することを推奨します。

未設定のインターフェイスまたはサブインターフェイスを選択した場合、そのインターフェイスの**アクティブ IP**、**サブネットマスク**、**論理名**、および**スタンバイ IP**を入力する必要があります。

フェールオーバーリンクを選択した場合は、**アクティブ IP**、**サブネットマスク**、**論理名**、および**スタンバイ IP**の値を指定する必要はありません。フェールオーバー リンクに指定されている値が使用されます。

[--Use Named--] オプションを選択した場合、**[Logical Name]** フィールドは、名前のついたインターフェイスのドロップダウンリストになります。このリストからインターフェイスを選択します。**アクティブ IP**、**サブネットマスク/プレフィックスの長さ**、**スタンバイ IP**の値を指定する必要はありません。そのインターフェイスに指定された値が使用されます。

- **[Logical Name]** : 「state」などのステート通信に使用するインターフェイスの論理名を指定します。この名前は情報を提供するためのものです。

- [Active IP] : インターフェイスのアクティブ IP アドレスを指定します。IP アドレスは、IPv4 または IPv6 アドレスのどちらにすることもできます。この IP アドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。
- [Standby IP] : インターフェイスのスタンバイ IP アドレスを指定します。アクティブ IP アドレスと同じサブネット上のアドレスを指定します。
- [Subnet Mask] : サブネット マスクを指定します。
- (オプション、アクティブ/スタンバイのみ) [Enable HTTP Replication] : このオプションにより、アクティブ HTTP セッションをスタンバイファイアウォールにコピーするステータスフェールオーバーがイネーブルになります。HTTP 複製を許可しない場合、HTTP 接続はフェールオーバーの発生時に切断されます。アクティブ/アクティブ モードでは、フェールオーバー グループごとに HTTP 複製を設定します。

(注) フェールオーバーを使用しているときに、スタンバイ装置から HTTP フローを削除すると遅延が生じます。このため **show conn count** 出力には、アクティブ装置とスタンバイ装置で異なる数が表示されることがあります。数秒待つてコマンドを再発行すると、両方の装置で同じカウントが表示されます。

ステップ 6 [Replication] 領域で、セッション複製レートを 1 秒あたり接続数で設定します。最小および最大レートはモデルによって決まります。デフォルトは最大レートです。デフォルトを使用するには、[Use Default] チェックボックスをオンにします。

ステップ 7 [Apply] をクリックします。

コンフィギュレーションがデバイスに保存されます。

ステップ 8 フェールオーバーをイネーブルにすると、フェールオーバーピアを設定するためのダイアログボックスが表示されます。

- 後でフェールオーバーピアに接続して手動で同様の設定を行う場合は、[No] をクリックします。
- ASDM によって自動的にフェールオーバーピア上の関連するフェールオーバー設定が行われるようにするには、[Yes] をクリックします。[Peer IP Address] フィールドにピアの IP アドレスを指定します。

フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 フェールオーバーを装置レベルで強制するには次を行います。

- a) コンテキスト モードに応じて画面を選択します。
 - シングル コンテキスト モードでは、[Monitoring] > [Properties] > [Failover] > [Status] を選択します。
 - マルチ コンテキスト モードでは、システムで [Monitoring] > [Failover] > [System] を選択します。
- b) 次のいずれかのボタンをクリックします。
 - [Make Active] をクリックすると、この装置がアクティブ装置になります。
 - [Make Standby] をクリックすると、相手装置がアクティブ装置になります。

ステップ 2 (アクティブ/アクティブモードのみ) フェールオーバーをフェールオーバー グループ レベルで強制するには次を行います。

- a) システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。#は、制御するフェールオーバー グループの番号です。
- b) 次のいずれかのボタンをクリックします。
 - [Make Active] をクリックすると、この装置でフェールオーバー グループがアクティブになります。
 - [Make Standby] をクリックすると、相手装置でフェールオーバー グループがアクティブになります。

フェールオーバーのディセーブル化

1 つまたは両方の装置でフェールオーバーをディセーブルにすると、リロードするまで各装置のアクティブおよびスタンバイ状態が維持されます。アクティブ/アクティブフェールオーバーペアの場合、どの装置を優先するように設定されていると、フェールオーバーグループはアクティブであるすべての装置でアクティブ状態のまま維持されます。

フェールオーバーをディセーブルにする際、次の特性を参照してください。

- スタンバイ装置/コンテキストはスタンバイ モードのまま維持されるので、両方の装置はトラフィックの転送を開始しません（これは疑似スタンバイ状態と呼ばれます）。
- スタンバイ装置/コンテキストは、アクティブ装置/コンテキストに接続されていない場合でもそのスタンバイ IP アドレスを引き続き使用します。
- スタンバイ装置/コンテキストによる、フェールオーバー上における接続に対するリッスン は継続されます。フェールオーバーをアクティブ装置/コンテキストで再度イネーブル

にすると、そのコンフィギュレーションの残りが再同期化された後に、スタンバイ装置/コンテキストが通常のスタンバイ状態に戻ります。

- スタンバイ装置で手動でフェールオーバーをイネーブルにしてアクティブ化しないでください。代わりに、[フェールオーバーの強制実行 \(322 ページ\)](#) を参照してください。スタンバイ装置でフェールオーバーをイネーブルにすると、MAC アドレスの競合が発生し、IPv6 トラフィックが中断される可能性があります。
- 完全にフェールオーバーをディセーブルにするには、no failover コンフィギュレーションをスタートアップ コンフィギュレーションに保存してからリロードします。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 シングルモードでは、**[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup]** の順に選択します。

マルチ コンテキスト モードでは、システム実行スペースで **[Configuration] > [Device Management] > [Failover] > [Setup]** を選択します。

ステップ 2 **[Enable Failover]** チェックボックスをオフにします。

ステップ 3 **[Apply]** をクリックします。

ステップ 4 完全にフェールオーバーをディセーブルにするには、コンフィギュレーションを保存してをリロードします。

a) **[Save]** ボタンをクリックします。

b) **[Tools] > [System Reload]** を選択して、ASA をリロードします。

障害が発生した装置の復元

障害が発生した装置を障害のない状態に復元するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 フェールオーバーを装置レベルで復元するには次を行います。

a) コンテキスト モードに応じて画面を選択します。

- シングル コンテキスト モードでは、[Monitoring] > [Properties] > [Failover] > [Status] を選択します。
- マルチ コンテキスト モードでは、システムで [Monitoring] > [Failover] > [System] を選択します。

b) [Reset Failover] をクリックします。

ステップ 2 (アクティブ/アクティブモードのみ) フェールオーバーをフェールオーバー グループ レベルで復元するには次を行います。

- a) システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。#は、制御するフェールオーバー グループの番号です。
- b) [Reset Failover] をクリックします。

コンフィギュレーションの再同期

複製されたコマンドは、実行コンフィギュレーションに保存されます。複製されたコマンドをスタンバイ装置のフラッシュ メモリに保存するには、[File] > [Save Running Configuration to Flash] の順に選択します。

モニタリング フェールオーバー

このセクションでは、フェールオーバー ステータスをモニタできます。

フェールオーバー メッセージ

フェールオーバーが発生すると、両方の ASA がシステム メッセージを送信します。

フェールオーバーの syslog メッセージ

ASA は、深刻な状況を表すプライオリティ レベル 2 のフェールオーバーについて、複数の syslog メッセージを発行します。これらのメッセージを表示するには、『syslog メッセージ ガイド』を参照してください。フェールオーバーに関連付けられているメッセージ ID の範囲は次のとおりです：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx、727xxx。たとえば、105032 および 105043 はフェールオーバー リンクとの問題を示しています。



(注) フェールオーバーの最中に、ASAは論理的にシャットダウンした後、インターフェイスを起動し、syslog メッセージ 411001 および 411002 を生成します。これは通常のアクティビティです。

フェールオーバー デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、コマンドリファレンスを参照してください。



- (注) CPUプロセスではデバッグ出力に高プライオリティが割り当てられているため、デバッグ出力を行うとシステムパフォーマンスに大きく影響することがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TACとのトラブルシューティングセッションの間に限り **debug fover** コマンドを使用してください。

SNMP のフェールオーバー トラップ

フェールオーバーに対する SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、お使いの SNMP 管理ステーションに Cisco syslog MIB をコンパイルします。

フェールオーバー ステータスのモニタリング



- (注) フェールオーバー イベントが発生した後、デバイスのモニタリングを継続するには、ASDM を再起動するか、または [Devices] ペインに表示される別のデバイスに切り替えて、元の ASA に戻る手順を実行する必要があります。この操作が必要なのは、ASDM がデバイスから切断されて再接続された場合、接続のモニタリングが再確立されないためです。

[Monitoring] > [Properties] > [Failover] を選択して、アクティブ/スタンバイ フェールオーバーをモニタします。

[Monitoring] > [Properties] > [Failover] 領域で次の画面を使用して、アクティブ/アクティブ フェールオーバーをモニタします。

システム

[System] ペインには、システムのフェールオーバー状態が表示されます。また、システムのフェールオーバー状態を次の方法で制御できます。

- デバイスのアクティブ/スタンバイ状態を切り替える。
- 障害が発生したデバイスをリセットする。
- スタンバイ装置をリロードする。

フィールド

[Failover state of the system] : 表示専用。ASA のフェールオーバー状態を表示します。表示される情報は、**show failover** コマンドで受け取る出力と同じです。表示出力に関する詳細については、コマンドリファレンスを参照してください。

[System] ペインでは、次のアクションを使用できます。

- [Make Active] : アクティブ/スタンバイ コンフィギュレーションで、このボタンをクリックすると、ASA がアクティブ装置になります。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、ASA で両方のフェールオーバー グループがアクティブになります。
- [Make Standby] : アクティブ/スタンバイ ペアで、このボタンをクリックすると、ASA がスタンバイ装置になります。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、ASA で両方のフェールオーバー グループがスタンバイ状態になります。
- [Reset Failover] : このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Reload Standby] : このボタンをクリックして、スタンバイ装置を強制的にリロードします。
- [Refresh] : このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

フェールオーバー グループ1 およびフェールオーバー グループ2

[Failover Group 1] ペインおよび [Failover Group 2] ペインには、選択したグループのフェールオーバー状態が表示されます。また、グループのアクティブ/スタンバイ状態を切り替えるか、または障害が発生したグループをリセットして、グループのフェールオーバー状態を制御することもできます。

フィールド

[Failover state of Group[x]] : 表示専用。選択したフェールオーバー グループのフェールオーバー状態を表示します。表示される情報は、**show failover group** コマンドで受け取る出力と同じです。

このペインで次のアクションを実行できます。

- [Make Active] : このボタンをクリックして、フェールオーバー グループを ASA のアクティブユニットにします。
- [Make Standby] : このボタンをクリックして、フェールオーバー グループを ASA で強制的にスタンバイ状態にします。

- [Reset Failover] : このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Refresh] : このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

フェールオーバーの履歴

機能名	リリース	機能情報
アクティブ/スタンバイ フェールオーバー	7.0(1)	この機能が導入されました。
アクティブ/アクティブ フェールオーバー	7.0(1)	この機能が導入されました。
フェールオーバー キーの 16 進数値サポート	7.0(4)	フェールオーバー リンクの暗号化用に 16 進数値が指定できるようになりました。 次の画面が変更になりました。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。
フェールオーバー キーのマスター パスフレーズのサポート	8.3(1)	フェールオーバー キーが、実行コンフィギュレーションとスタートアップコンフィギュレーションの共有キーを暗号化するマスターパスフレーズをサポートするようになりました。一方の ASA から他方に共有秘密をコピーする場合、たとえば、 more system:running-config コマンドを使用して、正常に暗号化共有キーをコピーして貼り付けることができます。 (注) failover key の共有秘密は、 show running-config の出力に ***** と表示されます。このマスクされたキーはコピーできません。 ASDM の変更はありませんでした。

機能名	リリース	機能情報
フェールオーバーにIPv6のサポートが追加されました。	8.2(2)	次の画面が変更されました。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces]。
「同時」ブートアップ中のフェールオーバーグループのユニットの設定の変更。	9.0(1)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバーグループを優先ユニットでアクティブにする preempt コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバーグループが最初に起動するユニットでアクティブになるように変更されました。
フェールオーバーリンクおよびステートリンクの通信を暗号化する IPsec LAN-to-LAN トンネルのサポート	9.1(2)	フェールオーバーキーに独自の暗号化を使用する代わりに、フェールオーバーリンクおよびステートリンクの暗号化に IPsec LAN-to-LAN トンネルが使用できるようになりました。 (注) フェールオーバー LAN-to-LAN トンネルは、IPsec (その他のVPN) ライセンスには適用されません。 次の画面が変更されました。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。

機能名	リリース	機能情報
ハードウェア モジュールのヘルス モニタリングの無効化	9.3(1)	<p>ASA はデフォルトで、インストール済みハードウェア モジュール (ASA FirePOWER モジュールなど) のヘルス モニタリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングをディセーブルにできます。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Interfaces]</p>
フェールオーバーペアのスタンバイ装置またはスタンバイ コンテキストのコンフィギュレーション変更のロック	9.3(2)	<p>通常のコフィギュレーションの同期を除いてスタンバイ装置上で変更ができないように、スタンバイ装置 (アクティブ/スタンバイフェールオーバー) またはスタンバイ コンテキスト (アクティブ/アクティブフェールオーバー) のコンフィギュレーション変更をロックできるようになりました。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup]</p>



第 11 章

ASA クラスタ

クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。



(注) 一部の機能は、クラスタリングを使用する場合、サポートされません。「[クラスタリングでサポートされない機能 \(342 ページ\)](#)」を参照してください。

- [ASA クラスタリングの概要 \(331 ページ\)](#)
- [ASA クラスタリングのライセンス \(351 ページ\)](#)
- [ASA クラスタリングの要件と前提条件 \(352 ページ\)](#)
- [ASA クラスタリングのガイドライン \(354 ページ\)](#)
- [ASA クラスタリングの設定 \(359 ページ\)](#)
- [クラスタ メンバの管理 \(391 ページ\)](#)
- [ASA クラスタのモニタリング \(398 ページ\)](#)
- [ASA クラスタリングの例 \(399 ページ\)](#)
- [ASA クラスタリングの履歴 \(417 ページ\)](#)

ASA クラスタリングの概要

ここでは、クラスタリングアーキテクチャとその動作について説明します。

ASA クラスタをネットワークに適合させる方法

クラスタは、1 つのユニットとして機能する複数の ASA から構成されます。ASA をクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離された高速バックプレーンネットワーク。クラスタ制御リンクと呼ばれます。
- 各 ASA への管理アクセス（コンフィギュレーションおよびモニタリングのため）。

クラスタをネットワーク内に配置するときは、クラスタが送受信するデータのロードバランシングを、アップストリームおよびダウンストリームのルータが次のいずれかの方法で行うことが必要です。

- スパンド EtherChannel（推奨）：クラスタ内の複数のメンバのインターフェイスをグループ化して1つの EtherChannel とします。この EtherChannel がユニット間のロードバランシングを実行します。
- ポリシーベース ルーティング（ルーテッドファイアウォールモードのみ）：アップストリームとダウンストリームのルータが、ルートマップと ACL を使用してユニット間のロードバランシングを実行します。
- 等コストマルチパスルーティング（ルーテッドファイアウォールモードのみ）：アップストリームとダウンストリームのルータが、等コストのスタティックまたはダイナミックルートを使用してユニット間のロードバランシングを実行します。

パフォーマンス スケーリング係数

複数のユニットを結合して1つのクラスタとしたときに、期待できるパフォーマンスの概算値は次のようになります。

- 合計スループットの 70 %
- 最大接続数の 60 %
- 接続数/秒の 50 %

たとえば、スループットについては、ASA 5585-X と SSP-40 が処理できる実際のファイアウォールトラフィックは、単独動作時は約 10 Gbps となります。8 ユニットのクラスタでは、合計スループットの最大値は約 80 Gbps（8 ユニット x 10 Gbps）の 70 %、つまり 56 Gbps となります。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。ここでは、各メンバーのロールの特長について説明します。

Bootstrap Configuration

各デバイスで、最小限のブートストラップコンフィギュレーション（クラスタ名、クラスタ制御リンク インターフェイスなどのクラスタ設定）を設定します。クラスタリングを最初にイネーブルにしたユニットが一般的にはマスターユニットとなります。以降のユニットに対してクラスタリングをイネーブルにすると、そのユニットはスレーブとしてクラスタに参加します。

マスターおよびスレーブユニットの役割

クラスタ内のメンバの1つがマスターユニットです。マスターユニットは、ブートストラップコンフィギュレーション内のプライオリティ設定によって決まります。プライオリティは1～100の範囲内で設定され、1が最高のプライオリティです。他のすべてのメンバはスレーブユニットです。一般的には、クラスタを作成した後で最初に追加したユニットがマスターユニットとなります。これは単に、その時点でクラスタに存在する唯一のユニットであるからです。

すべてのコンフィギュレーション作業（ブートストラップコンフィギュレーションを除く）は、マスターユニット上のみで実行する必要があります。コンフィギュレーションは、スレーブユニットに複製されます。物理的資産（たとえばインターフェイス）の場合は、マスターユニットのコンフィギュレーションがすべてのスレーブユニット上でミラーリングされます。たとえば、GigabitEthernet 0/1を内部インターフェイスとして、GigabitEthernet 0/0を外部インターフェイスとして設定した場合は、これらのインターフェイスはスレーブユニット上でも、内部および外部のインターフェイスとして使用されます。

機能によっては、クラスタ内でスケリングしないものがあり、そのような機能についてはマスターユニットがすべてのトラフィックを処理します。

マスターユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. ユニットに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのユニットは選定要求を3秒間隔でブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティは1～100の範囲内で設定され、1が最高のプライオリティです。
3. 45秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。



(注) 最高のプライオリティを持つユニットが複数ある場合は、クラスタユニット名、次にシリアル番号を使用してマスターが決定されます。

4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスターユニットになることはありません。既存のマスターユニットは常にマスターのままです。ただし、マスターユニットが応答を停止すると、その時点で新しいマスターユニットが選定されます。



- (注) 特定のユニットを手動で強制的にマスターにすることができます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

クラスタ インターフェイス

データインターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。1つのクラスタ内のすべてのデータインターフェイスのタイプが同一である必要があります。詳細については、「[クラスタインターフェイスについて \(360 ページ\)](#)」を参照してください。

クラスタ制御リンク

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。詳細については、「[クラスタ制御リンクについて \(360 ページ\)](#)」を参照してください。

ASA クラスタ内のハイ アベイラビリティ

ASA クラスタリングは、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

ユニットのヘルス モニタリング

マスターユニットは、各スレーブユニットをモニタするために、クラスタ制御リンクを介してキープアライブメッセージを定期的送信します（間隔は設定可能です）。各スレーブユニットは、同じメカニズムを使用してマスターユニットをモニタします。ユニットの健全性チェックが失敗すると、ユニットはクラスタから削除されます。

インターフェイス モニタリング

各ユニットは、使用中のすべての指名されたハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をマスターユニットに報告します。

- スパンド EtherChannel : クラスタ Link Aggregation Control Protocol (cLACP) を使用します。各ユニットは、リンク ステータスおよび cLACP プロトコル メッセージをモニタして、ポートがまだ EtherChannel でアクティブであるかどうかを判断します。ステータスがマスターユニットに報告されます。
- 個別インターフェイス (ルーテッドモードのみ) : 各ユニットが自身のインターフェイスを自己モニタし、インターフェイスのステータスをマスターユニットに報告します。

ヘルス モニタリングをイネーブルにすると、すべての物理インターフェイス（主要な EtherChannel インターフェイスおよび冗長インターフェイスのタイプを含む）がデフォルトでモニタされるため、オプションでインターフェイスごとのモニタリングをディセーブルにすることができます。指名されたインターフェイスのみモニタできます。たとえば、指名された EtherChannel に障害が発生したと判断される必要がある場合、つまり、EtherChannel のすべてのメンバーポートはクラスタ削除をトリガーすることに失敗する必要があります（最小ポートバンドリング設定に応じて）。

ユニットのモニタ対象のインターフェイスが失敗した場合、そのユニットはクラスタから削除されます。ASA がメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。EtherChannel の場合（スパンニングかどうかを問わない）は、確立済みメンバーのインターフェイスがダウン状態のときに、ASA はそのメンバーを 9 秒後に削除します。ASA は、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視ししません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。非 EtherChannel の場合は、メンバー状態に関係なく、ユニットは 500 ミリ秒後に削除されます。

障害後のステータス

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィックフローのステート情報は、クラスタ制御リンクを介して共有されます。

マスターユニットで障害が発生した場合は、そのクラスタの他のメンバーのうち、プライオリティが最高（番号が最小）のものがマスター ユニットになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。



- (注) ASA が非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはディセーブルになります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタメンバがクラスタから削除された後、クラスタに再参加できる方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決した後、。

- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データ インターフェイスの問題を解決した後、。
- ASA 5585-X 上の ASA FirePOWER モジュールの障害：ASA は自動的に 5 分後に再参加を試行します。
- ASA FirePOWE ソフトウェア モジュールの障害：モジュールの問題を解決した後、手動でクラスタリングをイネーブルにする必要があります。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働していて、クラスタリングがまだイネーブルになっているなら、ユニットは再起動するとクラスタに再参加することを意味します。ASA は 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。問題を解決したら、クラスタリングを再び有効にして、クラスタに手動で再参加する必要があります。

ASA クラスタの基本パラメータの設定 (386 ページ) を参照してください。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 17: クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システム アップタイムをトラッキングします。
ARP Table	Yes	トランスペアレント モードのみ。
MAC アドレス テーブル	Yes	トランスペアレント モードのみ。
ユーザ アイデンティティ	Yes	AAA ルール (uauth) とアイデンティティ ファイアウォールが含まれます。

Traffic	状態のサポート	注意
IPv6 ネイバー データベース	Yes	—
ダイナミック ルーティング	Yes	—
SNMP エンジン ID	なし	—
集中型 VPN (サイト間)	なし	VPN セッションは、マスターユニットで障害が発生すると切断されます。

設定の複製

クラスタ内のすべてのユニットは、単一のコンフィギュレーションを共有します。コンフィギュレーション変更を加えることができるのはマスターユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに同期されます。

ASA クラスタ管理

ASA クラスタリングを使用することの利点の1つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理インターフェイスについては、専用管理インターフェイスの1つを使用することを推奨します。管理インターフェイスは、個別インターフェイスとして設定することも（ルーテッドモードとトランスペアレントモードの両方）、スパンド EtherChannel インターフェイスとして設定することもできます。

管理用には、個別インターフェイスを使用することを推奨します（スパンド EtherChannel をデータインターフェイスに使用している場合でも）。個別インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンド EtherChannel インターフェイスでは、現在のマスターユニットへのリモート接続しかできません。



- (注) スパンド EtherChannel インターフェイスモードを使用しているときに、管理インターフェイスを個別インターフェイスとして設定する場合は、管理インターフェイスに対してダイナミックルーティングをイネーブルにすることはできません。スタティックルートを使用する必要があります。

個別インターフェイスの場合は、メイン クラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在のマスターユニットに属します。インターフェイスごとに、管理者はアドレス範囲も設定します。これで、各ユニット（現在のマスターも含まれます）がその範囲内のローカルアドレスを使用できるようになります。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスターユニットが変更されると、メインクラスタ IP アドレスは新しいマスターユニットに移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。

たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在のマスターユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、マスターユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

スバンド EtherChannel インターフェイスの場合は、IP アドレスは 1 つだけ設定でき、その IP アドレスは常にマスターユニットに関連付けられます。EtherChannel インターフェイスを使用してスレーブ ユニットに直接接続することはできません。管理インターフェイスは個別インターフェイスとして設定することを推奨します。各ユニットに接続できるようにするためです。デバイス ローカル EtherChannel を管理に使用できます。

マスター ユニット管理とスレーブ ユニット管理

すべての管理とモニタリングはマスターユニットで実行できます。マスターユニットから、すべてのユニットの実行時統計情報やリソース使用状況などのモニタリング情報を調べることができます。また、クラスタ内のすべてのユニットに対してコマンドを発行することや、コンソールメッセージをスレーブユニットからマスターユニットに複製することもできます。

必要に応じて、スレーブユニットを直接モニタできます。マスターユニットからでもできますが、ファイル管理をスレーブユニット上で実行できます（コンフィギュレーションのバックアップや、イメージの更新など）。次の機能は、マスターユニットからは使用できません。

- ユニットごとのクラスタ固有統計情報のモニタリング。
- ユニットごとの Syslog モニタリング（コンソール レプリケーションが有効な場合にコンソールに送信される syslog を除く）。
- SNMP
- NetFlow

RSA キー複製

マスターユニット上で RSA キーを作成すると、そのキーはすべてのスレーブユニットに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合に、マスターユニットで障害が発生すると接続が切断されます。新しいマスターユニットは、SSH 接続に対して同じキーを使用するので、新しいマスターユニットに再接続するときに、キャッシュ済みの SSH ホスト キーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続する場合は、IP アドレス不一致に関する警告メッセージが表示されます。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないからです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメインクラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。

サイト間クラスタリング

サイト間インストールの場合、推奨されるガイドラインに従っていれば、ASA クラスタリングを活用できます。

各クラスタ シャーシを個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスと連動します。クラスタから送信されたパケットは、サイト固有の MAC アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。サイト固有の MAC アドレスは、スパンド EtherChannel のみを使用したルーテッドモードでサポートされます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング : [ASA クラスタリングの要件と前提条件 \(352 ページ\)](#)
- サイト間のガイドライン : [ASA クラスタリングのガイドライン \(354 ページ\)](#)
- サイト間での例 : [サイト間クラスタリングの例 \(413 ページ\)](#)

ASA クラスタが接続を管理する方法

接続をクラスタの複数のメンバにロードバランスできます。接続のロールにより、通常動作時とハイアベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー : 通常、最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいユニットが接続からパケットを受信したときにディレクタがこれらのユニットの新しいオーナーを選択します。

- **バックアップ オーナー**：オーナーから受信した TCP/UDP ステート情報を格納するユニット。これにより、障害が発生した場合に新しいオーナーにシームレスに接続を転送できます。バックアップ オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロードバランシングに基づく）がバックアップ オーナーに問い合わせ、関連するステート情報を取得し、これでそのユニットが新しいオーナーになることができます。

ディレクタ（下記参照）がオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

- **ディレクタ**：フォワーダからのオーナー ルックアップ 要求を処理するユニット。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニットはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

ディレクタがオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

- **フォワーダ**：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせ、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN キーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化をディセーブルにした場合は、SYN Cookie は使用されないため、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえば DNS や ICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

接続でポート アドレス変換（PAT）を使用すると、PAT のタイプ（per-session または multi-session）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- **Per-session PAT**：オーナーは、接続の最初のパケットを受信するユニットです。
デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。
- **Multi-session PAT**：オーナーは常にマスターユニットです。multi-session PAT 接続がスレーブ ユニットで最初に受信される場合、スレーブ ユニットはその接続をマスター ユニットに転送します。

デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するの、これらの接続は常にマスターユニットによって所有されています。

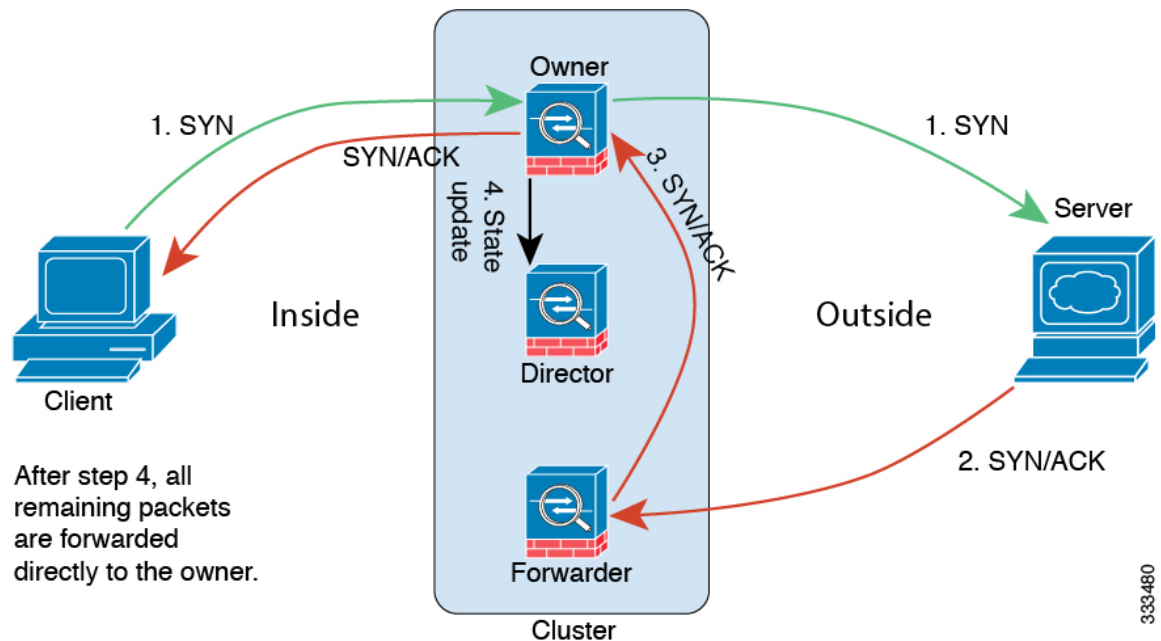
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーユニットに転送されます。最適なパフォーマンスを得るには、適切な外部ロードバランシングが必要です。1つのフローの両方向が同じユニットに到着するとともに、フローがユニット間に均等に分散されるようにするためです。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

サンプル データ フロー

次の例は、新しい接続の確立を示します。



1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロードバランシング方法に基づく）に配信されます。この ASA はフォワーダです。

3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様にTCPステート情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせさせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

新しいTCP接続のクラスタ全体での再分散

アップストリームまたはダウンストリーム ルータによるロードバランシングの結果として、フロー分散に偏りが生じた場合は、新しいTCPフローを過負荷のユニットから他のユニットにリダイレクトするように設定できます。既存のフローは他のユニットには移動されません。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部はマスターユニットだけでサポートされます。その他の機能については適切な使用に関する警告があります。

クラスタリングでサポートされない機能

これらの機能は、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモートアクセス VPN (SSL VPN および IPsec VPN)
- 次のアプリケーション インспекション :
 - CTIQBE
 - GTP
 - H323、H225、および RAS
 - IPsec パススルー
 - MGCP
 - MMP

- RTSP
- SCCP (Skinny)
- WAAS
- WCCP

- Botnet Traffic Filter
- Auto Update Server
- DHCP クライアント、サーバ、およびプロキシDHCP リレーがサポートされている。
- VPN ロード バランシング
- フェールオーバー
- ASA CX モジュール
- デッド接続検出 (DCD)

クラスタリングの中央集中型機能

次の機能は、マスターユニット上だけでサポートされます。クラスタの場合もスケーリングされません。たとえば、8ユニットから成るクラスタがあるとしします (5516-X)。その他のVPN ライセンスでは、1つのASA 5516-Xに対して最大300のサイト間IPsecトンネルが許可されますが、8ユニットのクラスタ全体では、300トンネルのみ使用できます。この機能は拡張されません。



(注) 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバユニットからマスターユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがマスターユニットに送り返されます。

中央集中型機能については、マスターユニットで障害が発生するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

- サイト間 VPN
- 次のアプリケーション インспекション :
 - DCERPC
 - ESMTP
 - IM
 - NetBIOS
 - PPTP

- RADIUS
 - RSH
 - SNMP
 - SQLNET
 - SUNRPC
 - TFTP
 - XDMCP
- ダイナミック ルーティング (スパンド EtherChannel モードのみ)
 - マルチキャスト ルーティング (個別インターフェイス モードのみ)
 - スタティック ルート モニタリング
 - IGMP マルチキャスト コントロールプレーン プロトコル処理 (データ プレーン フォワーディングはクラスタ全体に分散されます)
 - PIM マルチキャスト コントロールプレーン プロトコル処理 (データ プレーン 転送はクラスタ全体に分散されます)
 - ネットワーク アクセスの認証および許可。アカウントリングは非集中型です。
 - フィルタリング サービス

個々のユニットに適用される機能

これらの機能は、クラスタ全体またはマスター ユニットではなく、各 ASA ユニットに適用されます。

- QoS : QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは、各ユニットに対して個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定のASAから出て行くトラフィックに適用されます。3 ユニットから成るクラスタがあり、トラフィックが均等に分散している場合は、適合レートは実際にクラスタのレートの3倍になります。
- 脅威検出 : 脅威検出は、各ユニットに対して個別に機能します。たとえば、上位統計情報は、ユニット別です。たとえば、ポート スキャン検出が機能しないのは、スキャントラフィックが全ユニット間で分散されるので、1つのユニットがすべてのトラフィックを読み取ることはないからです。
- リソース管理 : マルチ コンテキスト モードでのリソース管理は、ローカル使用状況に基づいて各ユニットに個別に適用されます。
- ASA Firepower モジュール : ASA Firepower モジュール間でのコンフィギュレーションの同期や状態の共有は行われません。Firepower Management Center を使用して、クラスタ内の

ASA Firepower モジュールで一貫したポリシーを保持する必要があります。クラスタ内のデバイスに異なる ASA インターフェイススペースのゾーン定義を使用しないでください。

- ASA IPS モジュール：IPS モジュール間でのコンフィギュレーションの同期や状態の共有は行われません。IPS シグニチャによっては、IPS が複数の接続にわたって状態を保持することが必要になります。たとえば、ポート スキャン シグニチャが使用されるのは、同じ人物が同じサーバへの多数の接続を、それぞれ異なるポートを使用して開いていることを IPS モジュールが検出した場合です。クラスタリングでは、これらの接続は複数の ASA デバイス間で分散されます。これらのデバイスそれぞれに専用の IPS モジュールがあります。これらの IPS モジュールはステート情報を共有しないので、結果としてのポート スキャンをクラスタが検出できない場合があります。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウントिंगの 3 つのコンポーネントで構成されます。認証および許可は、クラスタリング マスター上で中央集中型機能として実装されており、データ構造がクラスタスレーブに複製されます。マスターが選定されたときは、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するのに必要なすべての情報を、新しいマスターが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、マスター ユニット変更が発生したときも維持されます。

アカウントINGは、クラスタ内の分散型機能として実装されています。アカウントINGはフロー単位で実行されるので、フローを所有するクラスタユニットがアカウントING開始と停止のメッセージを AAA サーバに送信します（フローに対するアカウントINGが設定されているとき）。

FTP とクラスタリング

- FTP データ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタメンバによって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- FTP アクセスに AAA を使用している場合、制御チャネルのフローはマスターユニットに集中化されます。

アイデンティティ ファイアウォールとクラスタリング

マスターユニットのみが AD から user-group を取得し、AD エージェントから user-ip マッピングを取得します。マスターユニットからユーザ情報がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいてユーザ ID の一致の決定を行うことができます。

マルチキャスト ルーティングとクラスタリング

マルチキャスト ルーティングは、インターフェイス モードによって動作が異なります。

スパンド EtherChannel モードでのマルチキャスト ルーティング

スパンド EtherChannel モードでは、ファーストパス転送が確立されるまでの間、マスターユニットがすべてのマルチキャストルーティングパケットとデータパケットを処理します。接続が確立された後は、各スレーブがマルチキャストデータパケットを転送できます。

個別インターフェイスモードでのマルチキャストルーティング

個別インターフェイスモードでは、マルチキャストに関してユニットが個別に動作することはありません。データおよびルーティングのパケットはすべてマスターユニットで処理されて転送されるので、パケットレプリケーションが回避されます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。着信および発信の NAT パケットが、クラスタ内のそれぞれ別の ASA に送信されることがあります。これは、ロードバランシングアルゴリズムは IP アドレスとポートに依存していますが、NAT が使用される場合、着信と発信でパケットの IP アドレスやポートが異なるためです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。NAT オーナーはセキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成するため、受信側ユニットは転送フローをオーナーに作成しません。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピングアドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリームルータは、メインクラスタ IP アドレスを指すマッピングアドレスについてはステティックルートまたは PBR とオブジェクトトラッキングを使用する必要があります。これは、スパンド EtherChannel の問題ではありません。クラスタインターフェイスには関連付けられた IP アドレスが 1 つしかないためです。
- 個別インターフェイスのインターフェイス PAT なし：インターフェイス PAT は、個別インターフェイスではサポートされていません。
- ダイナミック PAT 用 NAT プールアドレス分散：マスターユニットは、アドレスをクラスタ全体に均等に分配します。メンバーが接続を受信したときに、そのメンバーのアドレスが 1 つも残っていない場合は、接続はドロップされます（他のメンバーにはまだ使用可能なアドレスがある場合でも）。最低でも、クラスタ内のユニットと同数の NAT アドレスが含まれていることを確認してください。各ユニットが確実に 1 つのアドレスを受け取るようにするためです。アドレス割り当てを表示するには、**show nat pool cluster** コマンドを使用します。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- マスターユニットによって管理されるダイナミック NAT xlate：マスターユニットが xlate テーブルを維持し、スレーブユニットに複製します。ダイナミック NAT を必要とする接

続をスレーブ ユニットが受信したときに、その xlate がテーブル内にはない場合は、スレーブはマスター ユニットに xlate を要求します。スレーブ ユニットが接続を所有します。

- **Per-session PAT 機能**：クラスタリングに限りませんが、Per-session PAT 機能によって PAT のスケーラビリティが向上します。クラスタリングの場合は、各スレーブユニットが独自の PAT 接続を持てるようになります。対照的に、Multi-Session PAT 接続はマスターユニットに転送する必要があり、マスターユニットがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。
- 次のインスペクション用のスタティック PAT はありません。
 - FTP
 - PPTP
 - RSH
 - SQLNET
 - TFTP
 - XDMCP
 - SIP

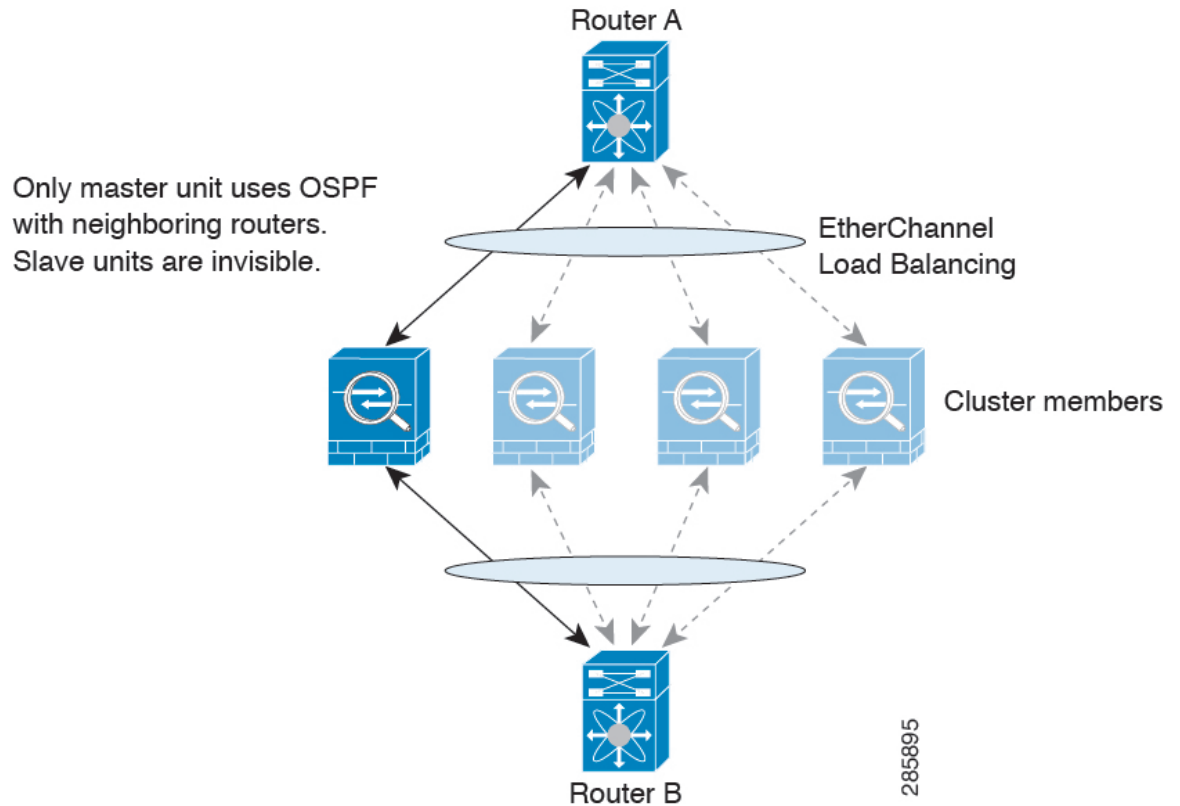
ダイナミック ルーティングおよびクラスタリング

ここでは、クラスタリングでダイナミック ルーティングを使用する方法について説明します。

スパンド EtherChannel モードでのダイナミック ルーティング

スパンド EtherChannel モード：ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスターユニットを介して学習され、スレーブに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 53: スパンド EtherChannel モードでのダイナミック ルーティング



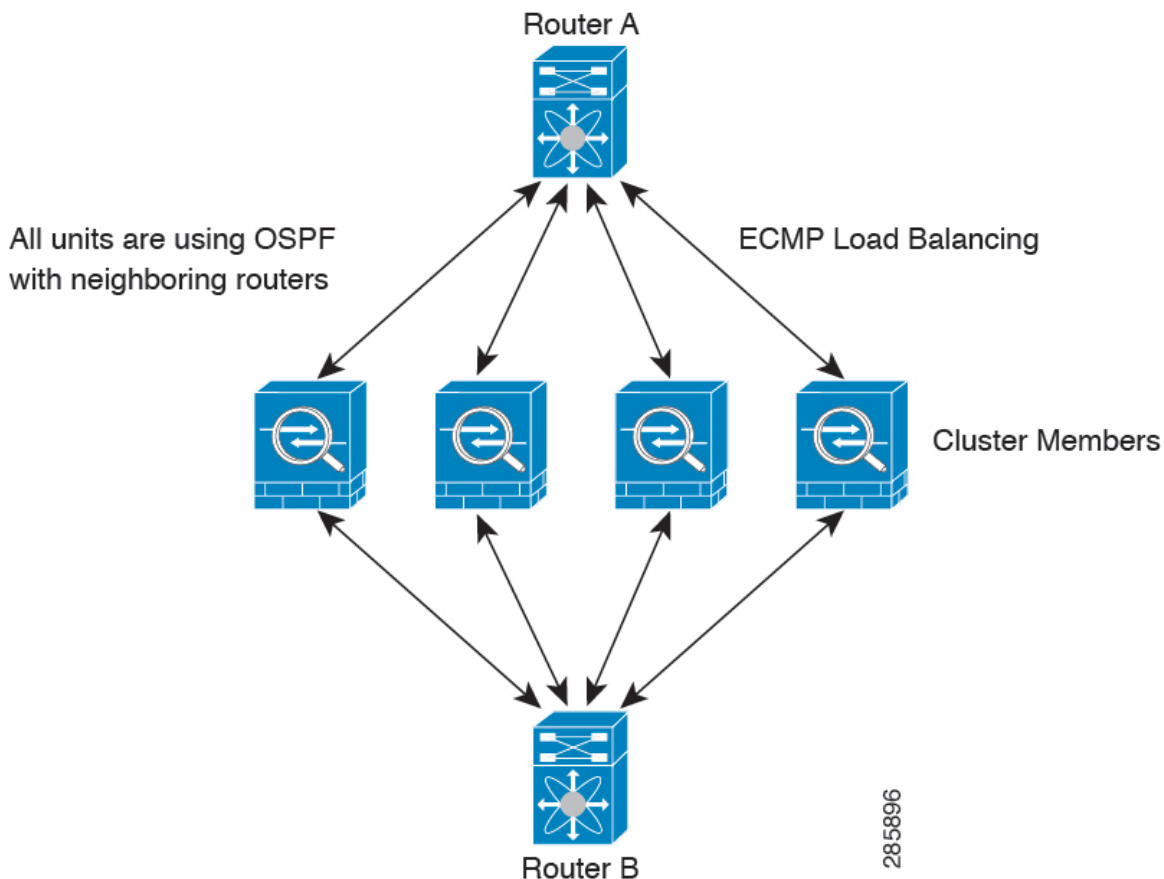
スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイス モードでは、各ユニットがスタンドアロンルータとしてルーティング プロトコルを実行します。ルートの学習は、各ユニットが個別に行います。

図 54: 個別インターフェイスモードでのダイナミックルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つの ASA を通過します。ECMP を使用して、4 パス間でトラフィックのロードバランシングを行います。各 ASA は、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ユニットが別のルータ ID を使用できるように、ルータ ID のクラスタープールを設定する必要があります。

EIGRP は、個別のインターフェイスモードのクラスターピアとのネイバー関係を形成しません。



- (注) 冗長性の目的で、クラスターに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィックゾーンにこれらすべての ASA インターフェイスをまとめます。[トラフィックゾーンの設定 \(561 ページ\)](#) を参照してください。

SIP インспекションとクラスタリング

制御フローは、任意のユニットで作成できます（ロードバランシングのため）。その子データフローは同じユニットに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、そのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メインクラスタ IP アドレスではなく、常にローカルアドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合は、新しいマスターが選定されたときに、新しいマスターユニットのポーリングに失敗します。

syslog および NetFlow とクラスタリング

- **Syslog** : クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージヘッダーフィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名コンフィギュレーションはクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタブートストラップコンフィギュレーションで割り当てられたローカルユニット名をデバイス ID として使用するようロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。
- **NetFlow** : クラスタの各ユニットは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポートとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

マスターユニットだけがセキュリティグループタグ (SGT) 情報を学習します。マスターユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティポリシーに基づいて SGT の一致決定を下せます。

VPN とクラスタリング

サイトツーサイト VPN は、中央集中型機能です。マスターユニットだけが VPN 接続をサポートします。分散型サイト間 VPN クラスタリングがサポートされています。詳細については、この [pdf](#) のハイアベイラビリティオプションを検索してください。



(注) リモートアクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのはマスターユニットだけであり、クラスタのハイアベイラビリティ能力は活用されません。マスターユニットで障害が発生した場合は、すべての既存の VPN 接

続が失われ、VPNユーザにとってはサービスの中断となります。新しいマスターが選定されたときに、VPN 接続を再確立する必要があります。

VPN トンネルをスパンド EtherChannel アドレスに接続すると、接続が自動的にマスターユニットに転送されます。PBR または ECMP を使用する際の個別インターフェイスへの接続については、ローカルアドレスではなく、常にメインクラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのユニットに複製されます。

ASA クラスタリングのライセンス

クラスタユニットは、各ユニット上で同じライセンスを必要としません。一般的には、マスターユニット用のライセンスのみを購入します。スレーブユニットはマスターのライセンスを継承します。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタライセンスとなります。

このルールには、例外があります。クラスタリングの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5585-X	クラスタライセンス、最大 16 ユニットのサポートします。 (注) 各ユニットに、同じ暗号化ライセンスが必要です。各ユニットに同じ 10 GE I/O/Security Plus ライセンスが必要です (ASA 5585-X と SSP-10 および SSP-20)。
ASA 5512-X	Security Plus ライセンス、2 ユニットのサポートします。 (注) 各ユニットに同じ暗号化ライセンスが必要です。
ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X	基本ライセンス、2 ユニットのサポートします。 (注) 各ユニットに同じ暗号化ライセンスが必要です。
Firepower 9300 シャーシ	Firepower 9300 シャーシ上の ASA の ASA クラスタライセンス (177 ページ) を参照してください。
他のすべてのモデル	サポートしない

ASA クラスタリングの要件と前提条件

モデルの要件

- ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X : 最大 2 ユニット
- ASA 5585 X : 最大 16 ユニット

ASA 5585-X と SSP-10 および SSP-20 (2 個の 10 ギガビット イーサネット インターフェイスを持つ) については、一方のインターフェイスをクラスタ制御リンクに使用し、他方をデータに使用することを推奨します (データについてはサブインターフェイスを使用できません)。この設定は、クラスタ制御リンクの冗長性には対応しませんが、クラスタ制御リンクのサイズをデータ インターフェイスのサイズと一致させるという要件は満たされます。

- ASA FirePOWER モジュール : ASA FirePOWER モジュールはクラスタリングを直接サポートしていませんが、クラスタ内でこれらのモジュールを使用できます。クラスタ内の ASA FirePOWER モジュールで一貫したポリシーを保持する必要があります。



(注) ASA FirePOWER モジュールを設定する前に、クラスタを作成します。モジュールがスレーブデバイスにすでに設定されている場合、クラスタにこれらを追加する前に、デバイスのインターフェイスの設定をクリアします。CLI から **clear configure interface** コマンドを入力します。

ASA のハードウェアおよびソフトウェア要件

クラスタ内のすべてのユニット :

- 同じ DRAM を使用する同じモデルである必要があります。フラッシュ メモリの容量は同一である必要はありません。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレス アップグレードがサポートされます。
- セキュリティ コンテキスト モードが一致している必要があります (シングルまたはマルチ)。
- (シングル コンテキスト モード) ファイアウォール モードが一致している必要があります (ルーテッドまたはトランスペアレント)。
- コンフィギュレーション複製前の初期クラスタ制御リンク通信のために、新しいクラスタメンバは、マスターユニットと同じ SSL 暗号化設定 (**ssl encryption** コマンド) を使用する必要があります。

- 同じクラスタライセンス、暗号化ライセンス、そして ASA 5585-X の場合は 10 GE I/O ライセンスが必要です。

スイッチ要件

- ASA でクラスタリングを設定する前に、スイッチのコンフィギュレーションを完了する必要があります。
- サポートされているスイッチのリストについては、『[Cisco ASA Compatibility](#)』 [英語] を参照してください。

ASA の要件

- ユニットを管理ネットワークに追加する前に、一意の IP アドレスを各ユニットに提供します。
 - ASA への接続および管理 IP アドレスの設定に関する詳細については、「使用する前に」の章を参照してください。
 - マスター装置（通常は最初にクラスタに追加された装置）で使用される IP アドレスを除き、これらの管理 IP アドレスは一時的に使用されるだけです。
 - スレーブがクラスタに参加すると、管理インターフェイス設定はマスター装置からの複製に置き換えられます。
- クラスタ制御リンクでジャンボフレームを使用する場合は（推奨）、クラスタリングをイネーブルにする前に、ジャンボフレームの予約をイネーブルにする必要があります。

サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用に Data Center Interconnect (DCI) に確保する必要があります。

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCIの最小帯域幅は、1つのメンバに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバの場合。
 - 合計 4 クラスタ メンバ
 - 各サイト 2 メンバ
 - メンバあたり 5 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 5 Gbps (2/2 x 5 Gbps)。

- 3 サイトの 6 メンバの場合、サイズは増加します。
 - 合計 6 クラスタ メンバ
 - サイト 1 は 3 メンバ、サイト 2 は 2 メンバ、サイト 3 は 1 メンバ
 - メンバあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 15 Gbps (3/2 x 10 Gbps)。

- 2 サイトの 2 メンバの場合。
 - 合計 2 クラスタ メンバ
 - 各サイト 1 メンバ
 - メンバあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 10 Gbps (1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク (10 Gbps) のサイズ未満になってはなりません)。

その他の要件

ターミナルサーバを使用して、すべてのクラスタメンバユニットのコンソールポートにアクセスすることをお勧めします。初期設定および継続的な管理（ユニットがダウンしたときなど）では、ターミナルサーバがリモート管理に役立ちます。

ASA クラスタリングのガイドライン

コンテキストモード

モードは、各メンバーユニット上で一致している必要があります。

ファイアウォールモード

シングルモードの場合、ファイアウォールモードがすべてのユニットで一致している必要があります。

フェールオーバー

フェールオーバーは、クラスタリングではサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

スイッチ

- ASR 9006 では、非デフォルト MTU を設定する場合は、ASR インターフェイス MTU をクラスタデバイス MTU より 14 バイト大きく設定します。そうしないと、**mtu-ignore** オプ

ションを使用しない限り、OSPF 隣接関係（アジャセンシー）ピアリングの試行が失敗する可能性があります。クラスタ デバイス MTU は、ASR IPv4 MTU と一致する必要があります。

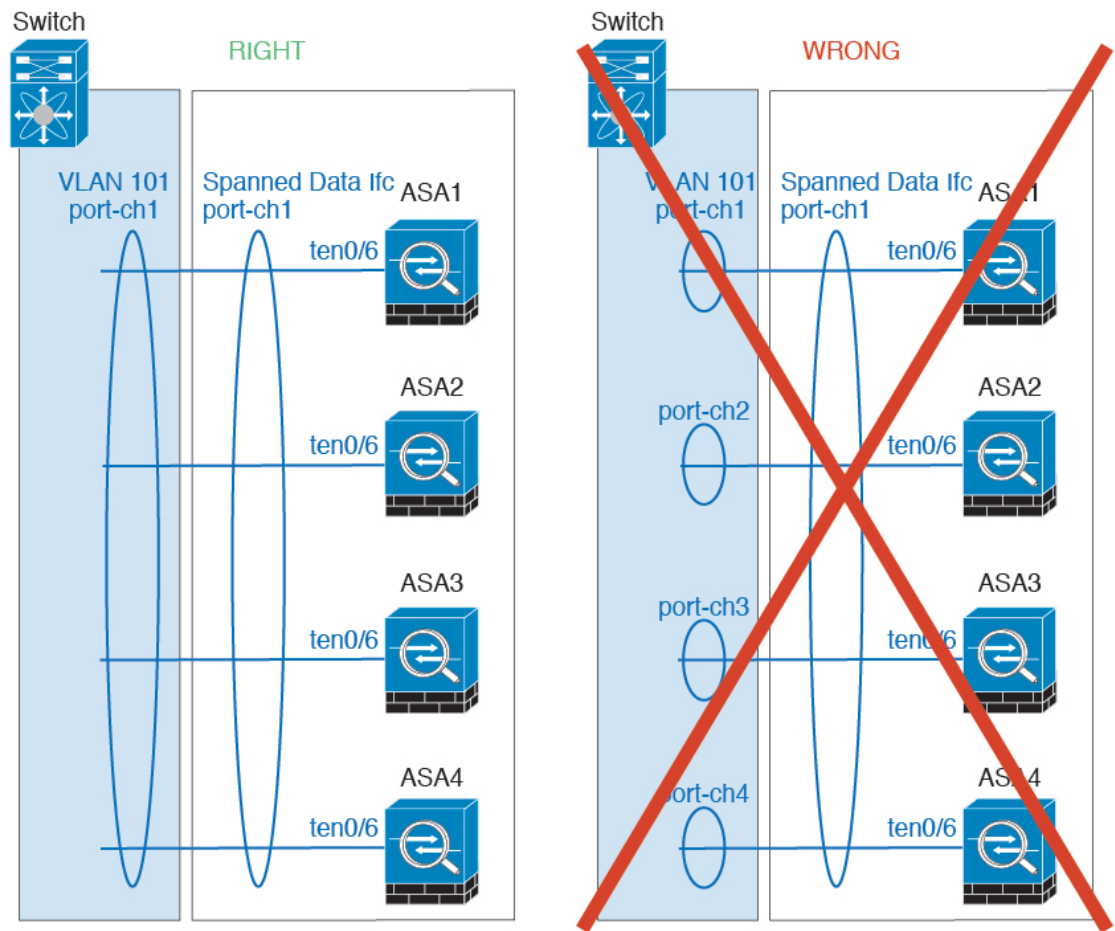
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチポートに対してSpanning Tree PortFastをイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチ上のSpanning Tree EtherChannelのバンドリングが遅いときは、スイッチの個別インターフェイスに対してLACP高速レートをイネーブルにできます。Nexusシリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際にLACP高速レートがサポートされないことに注意してください。そのため、クラスターリングでISSUを使用することは推奨されません。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均等に配分する場合がありますので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。クラスタデバイスのデフォルトのロードバランシングアルゴリズムは変更しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、Spanning Tree プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティを無効にすることで、Spanning Tree EtherChannel との互換性を高めることができます。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネルバンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタデバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

```
router(config)# port-channel id hash-distribution fixed
```

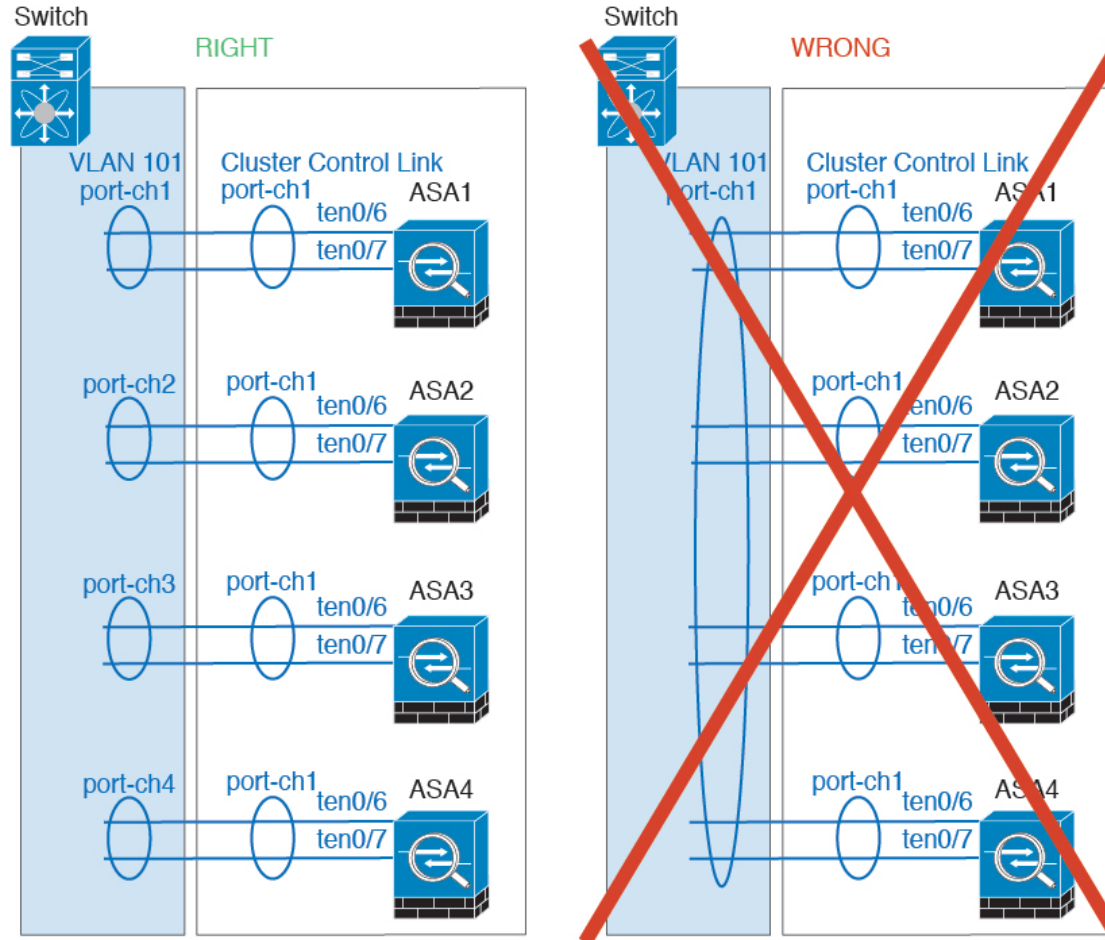
アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。
- Cisco Nexus スイッチのクラスタに接続されたすべての EtherChannel インターフェイスで、LACP グレースフル コンバージェンス機能をディセーブルにする必要があります。

EtherChannel

- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェアバージョンでは、クラスタユニットはスイッチスタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、マスタースイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチソフトウェアバージョンにアップグレードできます。
- スパンド EtherChannel とデバイスローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel とデバイスローカル EtherChannel に対してスイッチを適切に設定します。
 - スパンド EtherChannel：クラスタユニットスパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャンネルグループ内にあることを確認してください。



- デバイス ローカル EtherChannel : クラスタ ユニット デバイス ローカル EtherChannel (クラスタ制御リンク用に設定された EtherChannel もこれに含まれます) は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数の クラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



サイト間のガイドライン

サイト間クラスタリングについては、次のガイドラインを参照してください。

- 次のインターフェイスおよびファイアウォールモードで Inter-Site クラスタリングをサポートします。

インターフェイス モード	ファイアウォール モード	
	ルーテッド	Transparent
個別インターフェイス	○	該当なし
スバンド EtherChannel	なし	○

- 個別インターフェイスモードでは、マルチキャストランデブーポイント（RP）に向けて ECMP を使用する場合、ネクストホップとしてメインクラスタ IP アドレスを使用する RP IP アドレスのスタティックルートを使用することをお勧めします。このスタティックルートは、スレーブユニットにユニキャスト PIM 登録パケットが送信されるのを防ぎます。スレーブユニットが PIM 登録パケットを受け取った場合、パケットはドロップされ、マルチキャストストリームは登録できません。
- クラスタ制御リンクの遅延が、ラウンドトリップ時間（RTT）20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタメンバには接続を再分散できません。
- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。
- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じ MAC アドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタメンバがサイト 2 のメンバに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。
- トランスペアレントモードの場合、内部ネットワーク間のファイル用に各サイトのデータネットワークとゲートウェイルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイルータは、HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ VLAN は、オーバーレイトランスポート仮想化（OTV）または同様のものを使用してサイト全体にわたって拡張されます。ローカルゲートウェイルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイルータが 1 つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannel インターフェイスの追加または削除、ASA 上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルスチェック機能や無効なインターフェイスのインターフェイスモニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、インターフェイスのヘルスチェック機能を再度有効にできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合

によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。

- スパンド EtherChannel に接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンし、サーバが ICMP エラーメッセージを調整しないと、多数の ICMP メッセージが ASA クラスタに送信されます。このようなメッセージにより、ASA クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラーメッセージを調節することを推奨します。
- 個別インターフェイスモードの VXLAN はサポートされていません。スパンド EtherChannel モードでのみ VXLAN をサポートしています。

ASA クラスタリングのデフォルト

- スパンド EtherChannel を使用するときは、cLACP システム ID は自動生成され、システムプライオリティはデフォルトで 1 です。
- クラスタのヘルスチェック機能は、デフォルトでイネーブルになり、ホールド時間は 3 秒です。デフォルトでは、すべてのインターフェイスでインターネットヘルスマonitoring がイネーブルになっています。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。

ASA クラスタリングの設定

クラスタリングを設定するには、次のタスクを実行します。



- (注) クラスタリングを有効または無効にするには、コンソール接続 (CLI の場合) または ASDM 接続を使用します。

コンフィギュレーションのバックアップ (推奨)

セカンダリユニットでクラスタリングをイネーブルにすると、現在のコンフィギュレーションは同期した標準出荷単位の設定に置き換えられます。クラスタ全体を解除する場合、使用可能な管理インターフェイスコンフィギュレーションのバックアップコンフィギュレーションを取っておくと役立つ場合があります。

始める前に

各ユニットのバックアップを実行します。

手順

ステップ 1 [Tools] > [Backup Configurations] を選択します。

ステップ 2 最低でも実行コンフィギュレーションをバックアップします。詳細な手順については、[コンフィギュレーションまたはその他のファイルのバックアップおよび復元 \(941 ページ\)](#) を参照してください。

ユニットのケーブル接続およびインターフェイスの設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。次に、インターフェイスを設定します。

クラスタ インターフェイスについて

データインターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。1つのクラスタ内のすべてのデータインターフェイスのタイプが同一であることが必要です。また、各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。

クラスタ制御リンクについて

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- マスター選定。
- コンフィギュレーションの複製
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンク インターフェイスとネットワーク

次の例外を除き、クラスタ制御リンクには任意のデータ インターフェイスを使用できます。

- VLAN サブインターフェイスをクラスタ制御リンクとして使用することはできません。

- 管理 x/x インターフェイスをクラスタ制御リンクとして使用することはできません（単独か EtherChannel かにかかわらず）。
- ASA FirePOWER モジュールを搭載した ASA 5585-X では、クラスタ制御リンクに ASA FirePOWER モジュール上のインターフェイスではなく、ASA インターフェイスを使用することを推奨しています。モジュール インターフェイスは、ソフトウェア アップグレード中に発生するリロードを含め、モジュールのリロード中に最大 30 秒間トラフィックをドロップできます。ただし、必要に応じて、モジュール インターフェイスと ASA インターフェイスを同じクラスタ制御リンク EtherChannel で使用できます。モジュール インターフェイスがドロップした場合、EtherChannel の残りのインターフェイスはまだ稼働しています。ASA 5585-X ネットワーク モジュールは別のオペレーティングシステムを実行しないため、この問題の影響を受けません。

モジュール上のデータ インターフェイスはリロードの低下によっても影響を受けることに注意してください。シスコでは、EtherChannel 内で常に ASA インターフェイスをモジュール インターフェイスと冗長的に使用することを推奨しています。

ASA 5585-X と SSP-10 および SSP-20（2 個の 10 ギガビットイーサネット インターフェイスを持つ）については、一方のインターフェイスをクラスタ制御リンクに使用し、他方をデータに使用することを推奨します（データについてはサブインターフェイスを使用できます）。この設定は、クラスタ制御リンクの冗長性には対応しませんが、クラスタ制御リンクのサイズをデータ インターフェイスのサイズと一致させるという要件は満たされます。

EtherChannel インターフェイスまたは冗長インターフェイスを使用できます。

各クラスタ制御リンクは、同じサブネット上の IP アドレスを持ちます。このサブネットは、他のすべてのトラフィックからは隔離し、ASA クラスタ制御リンク インターフェイスだけが含まれるようにしてください。

2 メンバー クラスタの場合、ASA と ASA の間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンクのサイズ

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。たとえば、ASA 5585-X と SSP-60 を使用する場合は、クラスタのユニットあたり最大 14 Gbps を通過させることができるので、クラスタ制御リンクに割り当てるインターフェイスも、最低 14 Gbps の通過が可能となるようにしてください。この場合は、たとえば 10 ギガビットイーサネット インターフェイス 2 つを EtherChannel としてクラスタ制御リンクに使用し、残りのインターフェイスを必要に応じてデータ リンクに使用します。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの

量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロードバランシングが低下するので、すべてのリターントラフィックを正しいユニットに再分散する必要があります。
- ネットワークアクセスに対する AAA は一元的な機能であるため、すべてのトラフィックがマスターユニットに転送されます。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

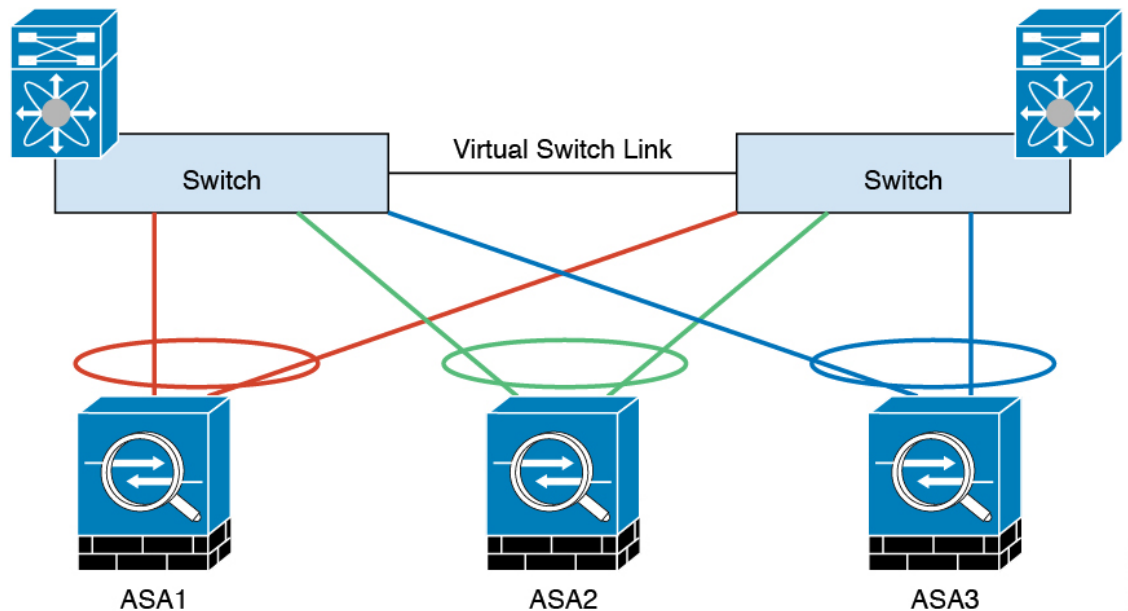


- (注) クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

クラスタ制御リンク冗長性

クラスタ制御リンクには EtherChannel を使用することを推奨します。冗長性を実現しながら、EtherChannel 内の複数のリンクにトラフィックを渡すことができます。

次の図は、仮想スイッチングシステム (VSS) または仮想ポートチャネル (vPC) 環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内の ASA インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバーです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



333222

クラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタメンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンクの障害

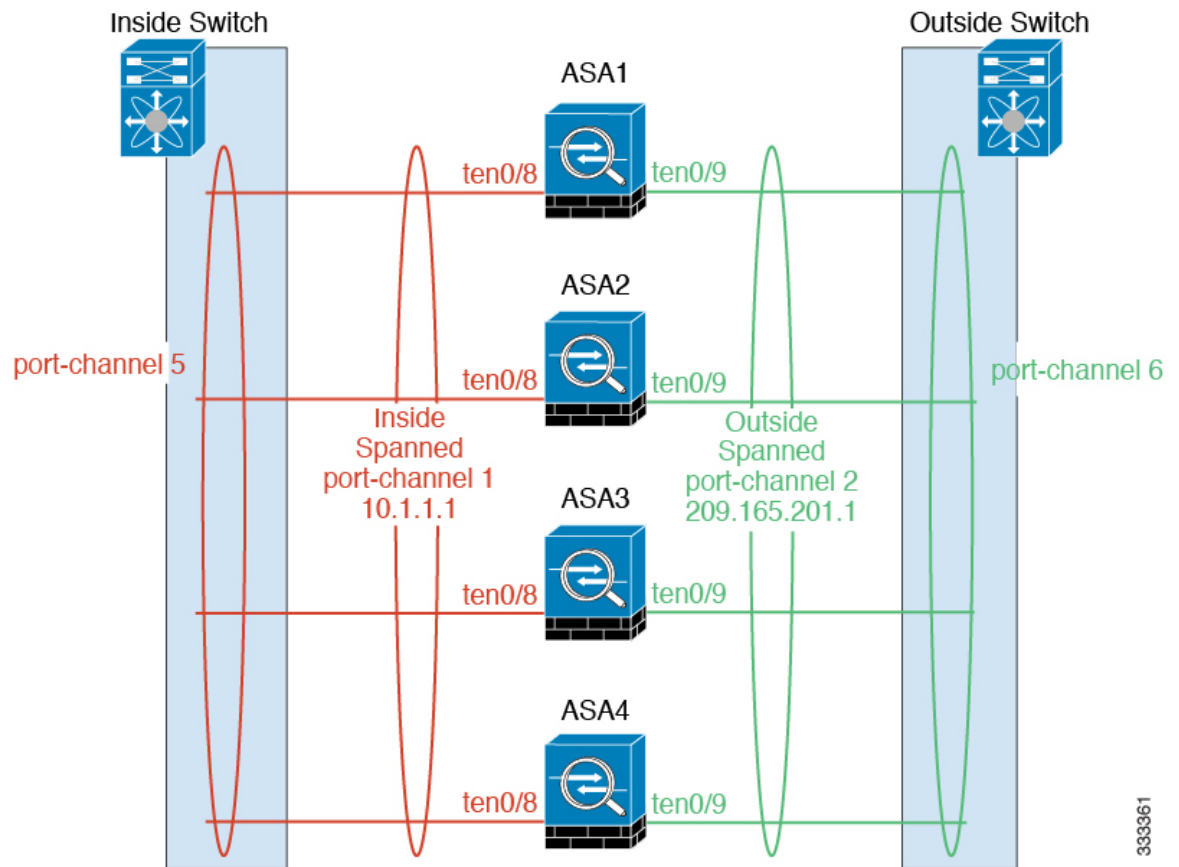
ユニットのクラスタ制御リンク回線プロトコルがダウンした場合、クラスタリングはディセーブルになります。データ インターフェイスはシャットダウンされます。クラスタ制御リンクの修復後、クラスタリングを再度イネーブルにして手動でクラスタに再参加する必要があります。



(注) ASAが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（マスターユニットと同じメイン IP アドレスを使用するため）。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

スパンド EtherChannel (推奨)

シャーシあたり1つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャンネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォールモードでも設定できます。ルーテッドモードでは、EtherChannel は単一の IP アドレスを持つルーテッドインターフェイスとして設定されます。トランスペアレントモードでは、IP アドレスはブリッジグループメンバーではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



333361

スパンド EtherChannel の利点

EtherChannel 方式のロードバランシングは、次のような利点から、他の方式よりも推奨されます。

- 障害検出までの時間が短い。
- コンバージェンス時間が短い。個別インターフェイスはルーティングプロトコルに基づきトラフィックをロードバランシングしますが、ルーティングプロトコルはリンク障害時にコンバージェンスが遅くなることがよくあります。
- コンフィギュレーションが容易である。

最大スループットのガイドライン

最大スループットを実現するには、次のことを推奨します。

- 使用するロードバランシングハッシュアルゴリズムは「対称」であるようにします。つまり、どちらの方向からのパケットも同じハッシュを持たせて、スパンド EtherChannel 内の同じ ASA に送信します。送信元と宛先の IP アドレス（デフォルト）または送信元と宛先のポートをハッシュアルゴリズムとして使用することを推奨します。
- ASA をスイッチに接続するときは、同じタイプのラインカードを使用します。すべてのパケットに同じハッシュアルゴリズムが適用されるようにするためです。

ロードバランシング

EtherChannel リンクは、送信元または宛先 IP アドレス、TCP ポートおよび UDP ポート番号に基づいて、専用のハッシュアルゴリズムを使用して選択されます。



- (注) ASA では、デフォルトのロードバランシングアルゴリズムを変更しないでください。スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port** (Cisco Nexus OS または Cisco IOS の **port-channel load-balance** コマンドを参照) を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシングアルゴリズムでは、**vlan** キーワードを使用しないでください。

EtherChannel 内のリンク数はロードバランシングに影響を及ぼします。

対称ロードバランシングは常に可能とは限りません。NAT を設定する場合は、フォワードパケットとリターンパケットとで IP アドレスやポートが異なります。リターントラフィックはハッシュに基づいて別のユニットに送信されるため、クラスタはほとんどのリターントラフィックを正しいユニットにリダイレクトする必要があります。

EtherChannel の冗長性

EtherChannel には、冗長性機能が組み込まれています。これは、すべてのリンクの回線プロトコルステータスをモニタします。リンクの1つで障害が発生すると、トラフィックは残りのリンク間で再分散されます。EtherChannel のすべてのリンクが特定のユニット上で停止したが、他方のユニットがまだアクティブである場合は、そのユニットはクラスタから削除されます。

VSS または vPC への接続

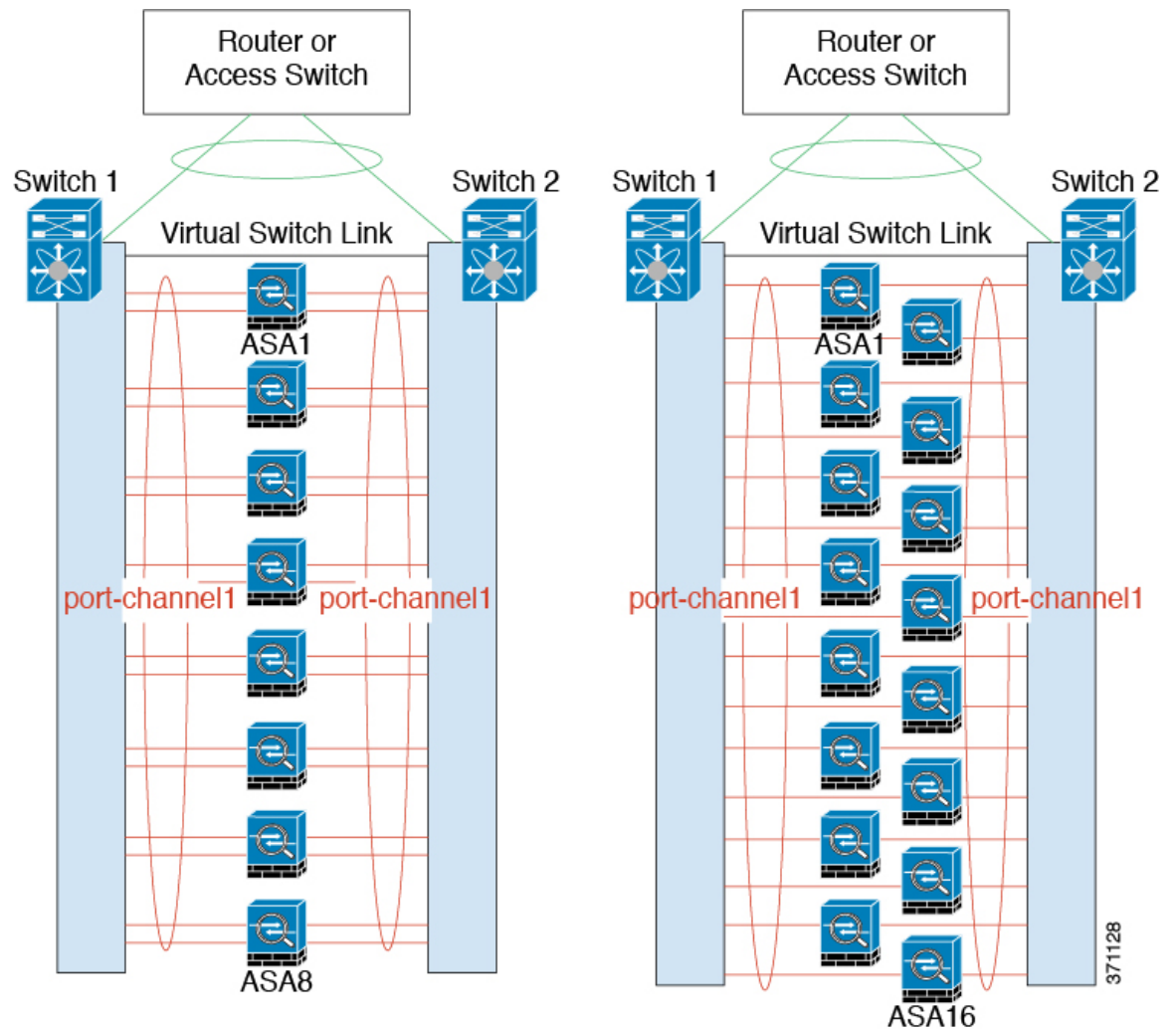
1 つの ASA につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの ASA につき複数のインターフェイスが特に役立つのは、VSS または vPC の両方のスイッチに接続するときです。

スイッチによっては、スパンド EtherChannel に最大 32 個のアクティブリンクを設定できます。この機能では、vPC 内の両方のスイッチが、それぞれ 16 個のアクティブリンクの EtherChannel をサポートする必要があります (例: Cisco Nexus 7000 と F2 シリーズ 10 ギガビットイーサネットモジュール)。

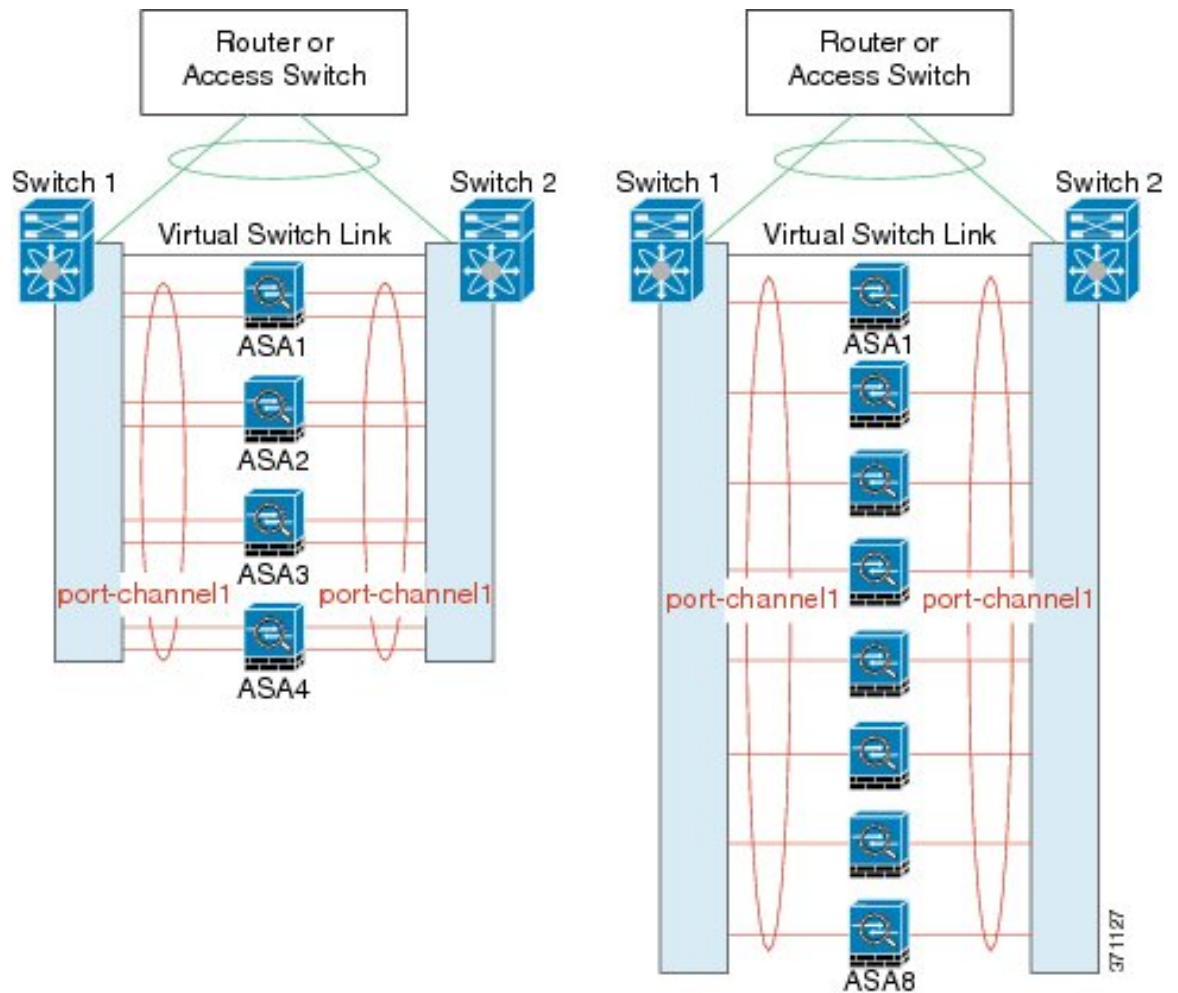
EtherChannel で 8 個のアクティブリンクをサポートするスイッチの場合、VSS/vPC で 2 台のスイッチに接続すると、スパンド EtherChannel に最大 16 個のアクティブリンクを設定できます。

スパンド EtherChannel で 8 個より多くのアクティブリンクを使用する場合は、スタンバイリンクも使用できません。9～32 個のアクティブリンクをサポートするには、スタンバイリンクの使用を可能にする cLACP ダイナミックポートプライオリティをディセーブルにする必要があります。それでも、必要であれば、たとえば 1 台のスイッチに接続するときに、8 個のアクティブリンクと 8 個のスタンバイリンクを使用できます。

次の図では、8 ASA クラスタおよび 16 ASA クラスタでの 32 アクティブリンクのスパンド EtherChannel を示します。

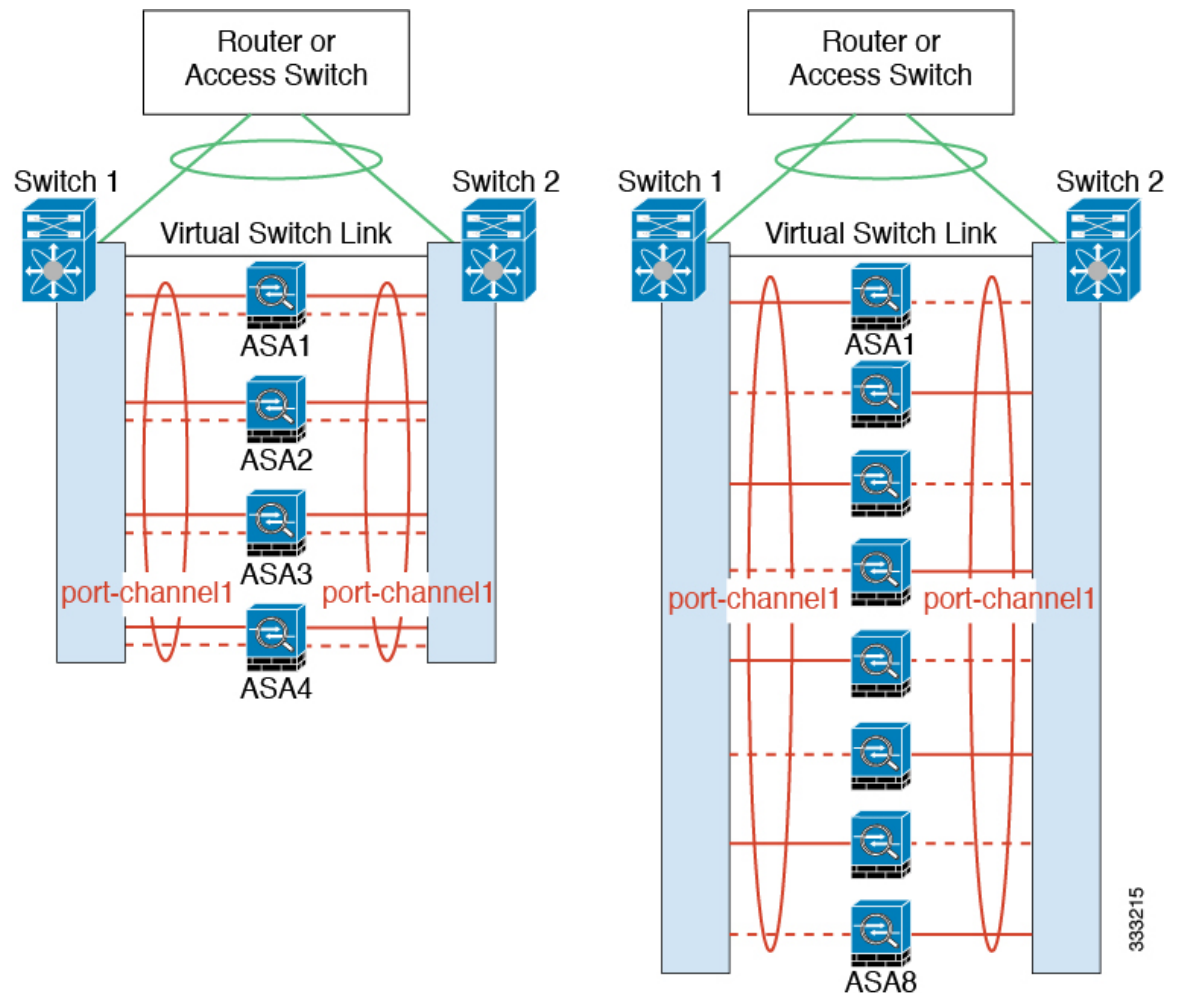


次の図では、4 ASA クラスタおよび 8 ASA クラスタでの 16 アクティブリンクのスパンド EtherChannel を示します。



次の図では、4 ASA クラスタおよび 8 ASA クラスタでの従来の 8 アクティブ リンク/8 スタンバイ リンクのスパンド EtherChannel を示します。アクティブ リンクは実線で、非アクティブ リンクは点線で示しています。cLACP ロードバランシングは、EtherChannel のリンクのうち最良の 8 本を自動的に選択してアクティブにできます。つまり、cLACP は、リンク レベルでのロードバランシング実現に役立ちます。

個別インターフェイス（ルーテッドファイアウォールモードのみ）



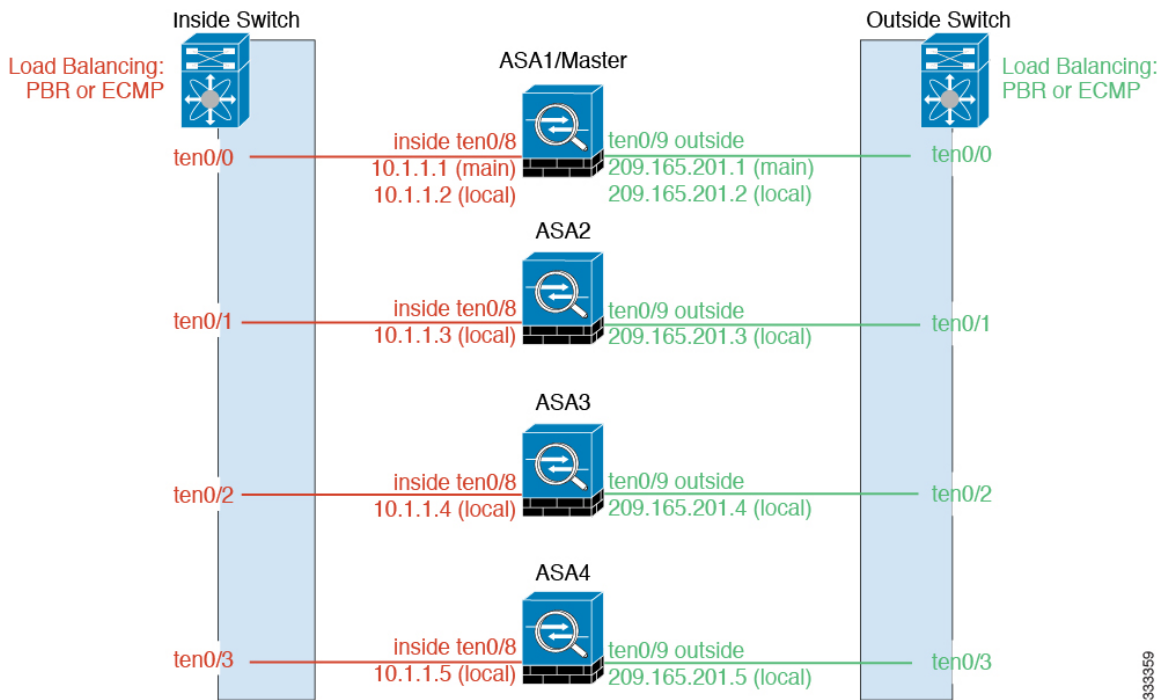
333215

個別インターフェイス（ルーテッドファイアウォールモードのみ）

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のローカル IP アドレスを持ちます。インターフェイス コンフィギュレーションはマスターユニット上だけで行う必要があるため、このインターフェイス コンフィギュレーションの中で IP アドレスプールを設定して、このプールのアドレスをクラスターメンバ（マスター用を含む）のインターフェイスに使用させることができます。メインクラスター IP アドレスは、そのクラスターのための固定アドレスであり、常に現在のマスターユニットに属します。メインクラスター IP アドレスは、マスターユニットのスレーブ IP アドレスです。ローカル IP アドレスが常にルーティングのマスターアドレスになります。このメインクラスター IP アドレスによって、管理アクセスのアドレスが一本化されます。マスターユニットが変更されると、メインクラスター IP アドレスは新しいマスターユニットに移動するので、クラスターの管理をシームレスに続行できます。ただし、ロードバランシングを別途する必要があります（この場合はアップストリームスイッチ上で）。



(注) 個別インターフェイスはルーティングプロトコルに基づきトラフィックをロードバランシングしますが、ルーティングプロトコルはリンク障害時にコンバージェンスが遅くなるのがよくあるので、個別インターフェイスの代わりにスパンド EtherChannel を推奨します。



ポリシーベース ルーティング (ルーテッドファイアウォールモードのみ)

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロードバランシング方法の 1 つが、ポリシーベース ルーティング (PBR) です。

この方法が推奨されるのは、すでに PBR を使用しており、既存のインフラストラクチャを活用したい場合です。また、この方法を使用すると、スパンド EtherChannel の場合と比べて、追加の調整オプションを利用できる場合もあります。

PBR は、ルートマップおよび ACL に基づいて、ルーティングの決定を行います。管理者は、手動でトラフィックをクラスタ内のすべての ASA 間で分ける必要があります。PBR は静的であるため、常に最適なロードバランシング結果を実現できないこともあります。最高のパフォーマンスを達成するには、PBR ポリシーを設定するときに、同じ接続のフォワードとリターンのパケットが同じ物理的 ASA に送信されるように指定することを推奨します。たとえば、Cisco ルータがある場合は、冗長性を実現するには Cisco IOS PBR をオブジェクトトラッキングとともに使用します。Cisco IOS オブジェクトトラッキングは、ICMP ping を使用して各 ASA をモニタします。これで、PBR は、特定の ASA の到達可能性に基づいてルートマップをイネーブルまたはディセーブルにできます。詳細については、次の URL を参照してください。

<http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html>

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml



- (注) このロードバランシング方法を使用する場合は、デバイス ローカル EtherChannel を個別インターフェイスとして使用できます。

等コストマルチパスルーティング (ルーテッドファイアウォールモードのみ)

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロードバランシング方法の1つが、等コストマルチパス (ECMP) ルーティングです。

この方法が推奨されるのは、すでに ECMP を使用しており、既存のインフラストラクチャを活用したい場合です。また、この方法を使用すると、スパンド EtherChannel の場合と比べて、追加の調整オプションを利用できる場合もあります。

ECMP ルーティングでは、ルーティングメトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannel のように、送信元および宛先の IP アドレスや送信元および宛先のポートのハッシュを使用してネクストホップの1つにパケットを送信できます。ECMP ルーティングにスタティックルートを使用する場合は、ASA の障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生した ASA へのトラフィックが失われるからです。スタティックルートを使用する場合は必ず、オブジェクトトラッキングなどのスタティックルートモニタリング機能を使用してください。ダイナミックルーティングプロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミックルーティングに参加するように各 ASA を設定する必要があります。



- (注) このロードバランシング方法を使用する場合は、デバイス ローカル EtherChannel を個別インターフェイスとして使用できます。

Nexus Intelligent Traffic Director (ルーテッドファイアウォールモードのみ)

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。Intelligent Traffic Director (ITD) とは、Nexus 5000、6000、7000 および 9000 スイッチシリーズの高速ハードウェアロードバランシングソリューションです。従来の PBR の機能を完全に網羅していることに加え、簡略化された構成ワークフローを提供し、粒度の細かい負荷分散を実現するための複数の追加機能を備えています。

ITD は、IP スティキ性、双方向フロー対称性のためのコンシステントハッシュ法、仮想 IP アドレッシング、ヘルスモニタリング、高度な障害処理ポリシー (N+M 冗長性)、加重ロードバランシング、およびアプリケーション IP SLA プロブ (DNS を含む) をサポートします。ロードバランシングの動的な性質により、PBR に比べて、すべてのクラスタメンバーでより均一なトラフィック分散を実現します。双方向フロー対称性を実現するために、接続のフォワードおよびリターンパケットが同じ物理 ASA に送信されるように ITD を設定することを推奨します。詳細については、次の URL を参照してください。

<http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html>

クラスタユニットのケーブル接続とアップストリームおよびダウンストリーム機器の設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

手順

クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

(注) クラスタに参加するようにユニットを設定する前に、少なくとも、アクティブなクラスタ制御リンク ネットワークが必要です。

アップストリームとダウンストリームの機器も設定する必要があります。たとえば、EtherChannel を使用する場合は、EtherChannel のアップストリーム/ダウンストリーム機器を設定する必要があります。

例

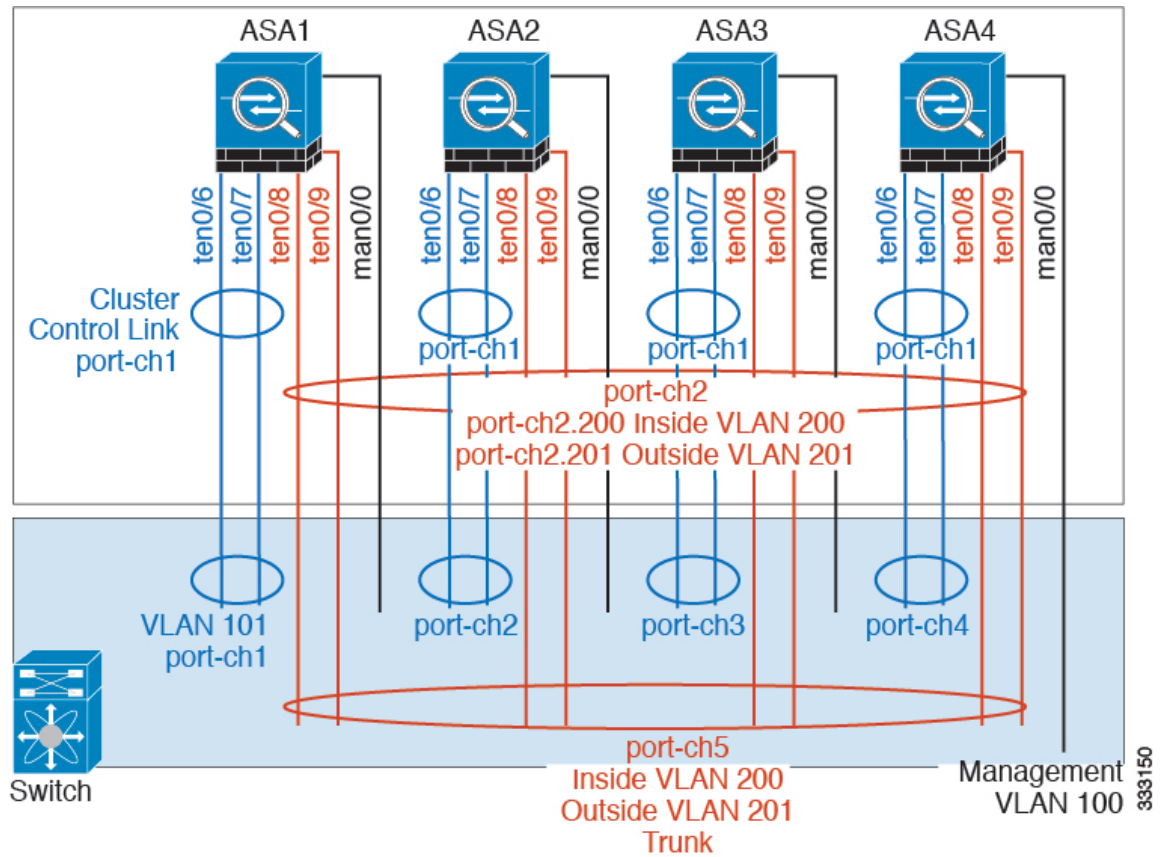


(注) この例では、ロードバランシングに EtherChannel を使用します。PBR または ECMP を使用する場合は、スイッチ コンフィギュレーションが異なります。

たとえば、4 台の ASA 5585-X のそれぞれにおいて、次のものを使用します。

- デバイス ローカル EtherChannel の 10 ギガビットイーサネット インターフェイス 2 個 (クラスタ制御リンク用)。
- スパンド EtherChannel の 10 ギガビットイーサネット インターフェイス 2 個 (内部および外部ネットワーク用)。各インターフェイスは、EtherChannel の VLAN サブインターフェイスです。サブインターフェイスを使用すると、内部と外部の両方のインターフェイスが EtherChannel の利点を活用できます。
- 管理インターフェイス 1 個。

内部と外部の両方のネットワーク用に 1 台のスイッチがあります。



目的	4台の各ASAの接続インターフェイス	スイッチポートへ
クラスタ制御リンク	TenGigabitEthernet 0/6 および TenGigabitEthernet 0/7	合計 8 ポート TenGigabitEthernet 0/6 と TenGigabitEthernet 0/7 のペアごとに、4 個の EtherChannel (ASA ごとに 1 個の EC) を設定します。 これらの EtherChannel すべてが、同一の独立クラスタ制御 VLAN 上 (たとえば VLAN 101) に存在する必要があります。

目的	4 台の各 ASA の接続インターフェイス	スイッチ ポートへ
内部および外部インターフェイス	TenGigabitEthernet 0/8 および TenGigabitEthernet 0/9	合計 8 ポート 単一の EtherChannel を設定します (すべての ASA にまたがる)。 スイッチでは、この VLAN およびネットワークをここで設定できます。たとえば、VLAN 200 (内部用) および VLAN 201 (外部用) が含まれるトランクを設定します。
管理インターフェイス	Management 0/0	合計 4 ポート すべてのインターフェイスを、同一の独立管理 VLAN (たとえば VLAN 100) 上に置きます。

マスターユニットでのクラスタ インターフェイス モードの設定

クラスタリング用に設定できるインターフェイスのタイプは、スパンド EtherChannel と個別インターフェイスのいずれか一方のみです。1つのクラスタ内でインターフェイスタイプを混在させることはできません。



- (注) マスターユニットからスレーブユニットを追加しない場合は、マスターユニットだけでなく全ユニットのインターフェイスモードをこの項の説明に従って手動で設定する必要があります。マスターユニットからセカンダリユニットを追加する場合は、ASDM がスレーブユニットのインターフェイスモードを自動的に設定します。

始める前に

- 管理専用インターフェイスはいつでも、個別インターフェイス (推奨) として設定できます (スパンド EtherChannel モードのときでも)。管理インターフェイスは、個別インターフェイスとすることができます (トランスペアレント ファイアウォール モードのときでも)。
- スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミックルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。

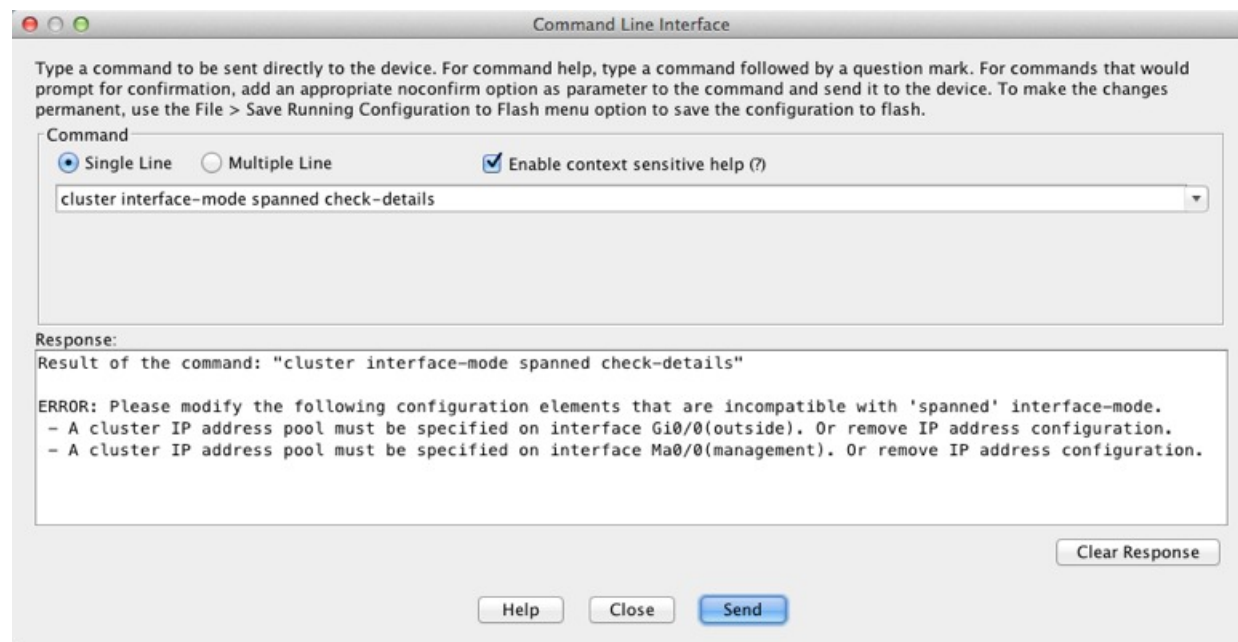
- マルチ コンテキスト モードでは、すべてのコンテキストに対して1つのインターフェイス タイプを選択する必要があります。たとえば、トランスペアレント モードとルーテッド モードのコンテキストが混在している場合は、すべてのコンテキストにスパンド EtherChannel モードを使用する必要があります。これが、トランスペアレントモードで許可される唯一のインターフェイス タイプであるからです。

手順

ステップ 1 In ASDM on the master unit, choose **Tools > Command Line Interface**. 互換性のないコンフィギュレーションを表示し、強制的にインターフェイスモードにして後でコンフィギュレーションを修正できるようにします。このコマンドではモードは変更されません。

cluster interface-mode {individual | spanned} check-details

例 :

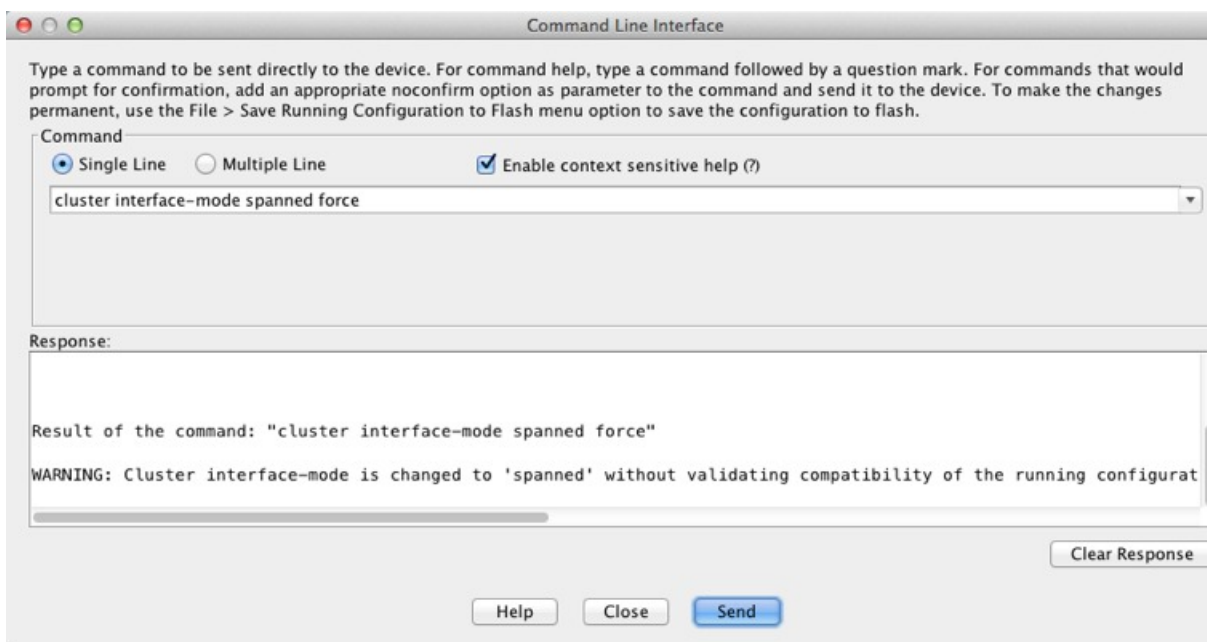


注意 インターフェイスモードを設定した後は、常にインターフェイスに接続できるようになります。ただし、クラスタリング要件に適合するように管理インターフェイスを設定する前にASAをリロードすると（たとえば、クラスタIPプールを追加するため）、クラスタと互換性のないインターフェイス コンフィギュレーションが削除されるため、再接続できなくなります。その場合は、コンソールポートに接続してインターフェイス コンフィギュレーションを修正する必要があります。

ステップ 2 クラスタリング用にインターフェイスモードを設定します。

cluster interface-mode {individual | spanned} force

例 :



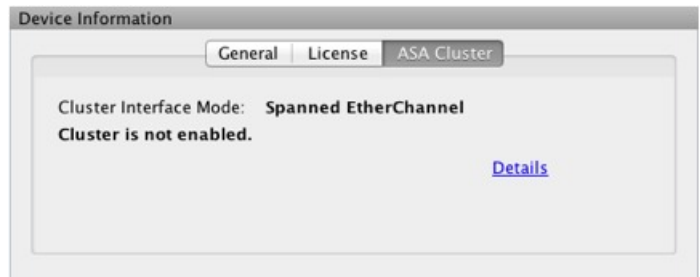
デフォルト設定はありません。明示的にモードを選択する必要があります。モードを設定していない場合は、クラスタリングをイネーブルにできません。

force オプションを指定すると、互換性のないコンフィギュレーションの検査は行わずにモードが変更されます。コンフィギュレーションの問題がある場合は、モードを変更した後に手動で解決する必要があります。インターフェイス コンフィギュレーションの修正ができるのはモードの設定後に限られるので、**force** オプションを使用することを推奨します。このようにすれば、最低でも、既存のコンフィギュレーションの状態から開始できます。さらにガイダンスが必要な場合は、モードを設定した後で **check-details** オプションを再実行します。

force オプションを指定しないと、互換性のないコンフィギュレーションがある場合は、コンフィギュレーションをクリアしてリロードするように求められるので、コンソールポートに接続して管理アクセスを再設定する必要があります。コンフィギュレーションに互換性の問題がない場合は（まれなケース）、モードが変更され、コンフィギュレーションは維持されます。コンフィギュレーションをクリアしたくない場合は、**n** を入力してコマンドを終了します。

インターフェイス モードを解除するには、**no cluster interface-mode** コマンドを入力します。

- ステップ 3** ASDM を終了し、リロードします。クラスタ インターフェイス モードに正しく対応するように ASDM を再起動する必要があります。リロードの後、ホームページに [ASA Cluster] タブが表示されます。



(推奨、マルチ コンテキスト モードでは必須) マスター ユニットでのインターフェイスの設定

クラスタリングを有効にする前に、現在 IP アドレスが設定されているインターフェイスをクラスタ対応に変更する必要があります。少なくとも、ASDM が現在接続されている管理インターフェイスを変更する必要があります。他のインターフェイスについては、クラスタリングをイネーブルにする前またはした後で設定できます。完全なコンフィギュレーションが新しいクラスタメンバと同期するように、すべてのインターフェイスを事前に設定することを推奨します。マルチ コンテキスト モードでは、この項の手順を使用して、既存のインターフェイスを修正するか、新しいインターフェイスを設定する必要があります。一方、シングルモードでは、この項を省略し、High Availability and Scalability ウィザードで共通インターフェイス パラメータを設定できます (高可用性のウィザードの実行 (383 ページ) を参照)。個別インターフェイス用の EtherChannel の作成などの高度なインターフェイス設定はウィザードでは実行できないことに注意してください。

ここでは、クラスタリング互換となるようにインターフェイスを設定する方法について説明します。データ インターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。各方式は別のロードバランシングメカニズムを使用します。同じコンフィギュレーションで両方のタイプを設定することはできません。ただし、管理インターフェイスは例外で、スパンド EtherChannel モードであっても個別インターフェイスにできます。

個別のインターフェイスの設定 (管理インターフェイスに推奨)

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のプライマリ ユニットに属します。

スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定することを推奨します。個別管理インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンド EtherChannel インターフェイスでは、現在のプライマリ ユニットへの接続しかできません。

始める前に

- 管理専用インターフェイスの場合を除き、個別インターフェイスモードであることが必要です。

- マルチ コンテキスト モードの場合は、この手順を各コンテキストで実行します。まだコンテキスト コンフィギュレーション モードに入っていない場合は、**changeto context name** コマンドを入力します。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
- 個別インターフェイスの場合は、ネイバー デバイスでのロード バランシングを設定する必要があります。管理インターフェイスには、外部のロードバランシングは必要ありません。
- （オプション）インターフェイスをデバイス ローカル EtherChannel インターフェイスとして設定する、冗長インターフェイスを設定する、およびサブインターフェイスを設定する作業を必要に応じて行います。
 - EtherChannel の場合、この EtherChannel はユニットに対してローカルであり、スパン ド EtherChannel ではありません。
 - 管理専用インターフェイスを冗長インターフェイスにすることはできません。
- ASDM を使用して管理インターフェイスにリモートに接続している場合は、将来のセカンダリ ユニットの現在の IP アドレスは一時的なものです。
 - 各メンバには、プライマリ ユニットで定義されたクラスタ IP プールから IP アドレスが割り当てられます。
 - クラスタ IP プールには、将来のセカンダリ IP アドレスを含む、ネットワークですでに使用中のアドレスを含めることはできません。次に例を示します。
 1. プライマリ ユニットに 10.1.1.1 を設定します。
 2. 他のユニットには、10.1.1.2、10.1.1.3、10.1.1.4 を使用します。
 3. プライマリ ユニットのクラスタの IP プールを設定する場合、使用中であるために .2、.3、.4 のアドレスをプールに含めることはできません。
 4. 代わりに、.5、.6、.7、.8 のような、ネットワークの他の IP アドレスを使用する必要があります。



(注) プールには、プライマリ ユニットを含むクラスタのメンバ数分のアドレスが必要です。元の .1 アドレスはメインクラスタ IP アドレスであり、現在のプライマリ ユニットのものです。

5. クラスタに参加すると古い一時的なアドレスは放棄され、他の場所で使用できません。

手順

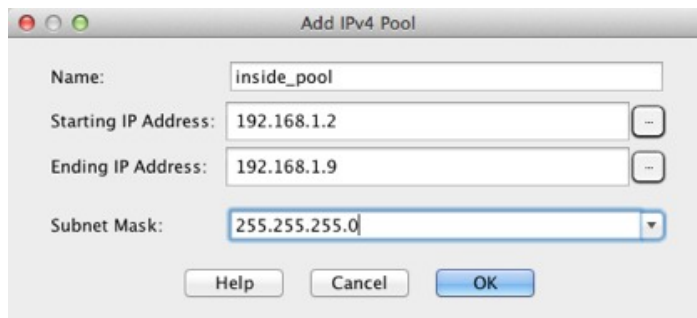
ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。

ステップ 2 インターフェイス行を選択して、[Edit] をクリックします。インターフェイスのパラメータを設定します。次のガイドラインを参照してください。

- （スバンド EtherChannel モードの管理インターフェイスでは必須）[Dedicate this interface to management only]：インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。デフォルトでは、管理タイプのインターフェイスは管理専用として設定されます。トランスペアレントモードでは、このコマンドは管理タイプのインターフェイスに対して常にイネーブルになります。
- [Use Static IP]：DHCP と PPPoE はサポートされません。

ステップ 3 IPv4 クラスタ IP プール、MAC アドレス プールを追加するには、[Advanced] タブをクリックして、[ASA Cluster] エリア パラメータを設定します。

- [IP Address Pool] フィールドの横にある [...] ボタンをクリックしてクラスタ IP プールを作成します。表示される有効範囲は、[General] タブで設定するメイン IP アドレスにより決定します。
- [Add] をクリックします。
- メインクラスタの IP アドレスを含まないアドレス範囲を設定します。ネットワーク内で現在使用されているアドレスも含みません。範囲は、たとえば 8 アドレスというように、クラスタのサイズに合わせて十分に大きくする必要があります。



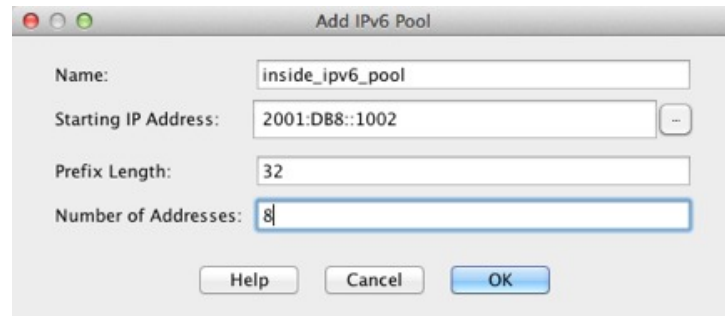
- [OK] をクリックして、新しいプールを作成します。
- 作成した新しいプールを選択して、[Assign] をクリックし、次に [OK] をクリックします。プール名が [IP Address Pool] フィールドに表示されます。
- （任意）（オプション）MAC アドレスを手動で設定する場合は、[MAC Address Pool] を設定します。

ステップ 4 IPv6 アドレスを設定するには、[IPv6] タブをクリックします。

- [Enable IPv6] チェックボックスをオンにします。
- [Interface IPv6 Addresses] エリアで、[Add] をクリックします。
[Enable address autoconfiguration] オプションはサポートされません。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

- c) [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。
- d) [...] ボタンをクリックして、クラスター IP プールを設定します。
- e) [Add] をクリックします。



- f) プールの開始 IP アドレス（ネットワーク プレフィックス）、プレフィックス長、アドレス数を設定します。
- g) [OK] をクリックして、新しいプールを作成します。
- h) 作成した新しいプールを選択して、[Assign] をクリックし、次に [OK] をクリックします。

[ASA Cluster IP Pool] フィールドにプールが表示されます。

- i) [OK] をクリックします。

ステップ 5 [OK] をクリックして、[Interfaces] ペインに戻ります。

ステップ 6 [Apply] をクリックします。

スパンド EtherChannel の設定

スパンド EtherChannel は、クラスター内のすべての ASA に広がるものであり、EtherChannel の動作の一部としてロード バランシングを行うことができます。

始める前に

- スパンド EtherChannel インターフェイス モードにする必要があります。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。[ブリッジ仮想インターフェイス \(BVI\) の設定 \(521 ページ\)](#) を参照してください。
- EtherChannel には最大および最小のリンク数を指定しないでください。EtherChannel の最大および最小のリンク数の指定は、ASA とスイッチのどちらにおいても行わないことを推奨します。これらを使用する必要がある場合は、次の点に注意してください。

- ASA 上で設定されるリンクの最大数は、クラスタ全体のアクティブ ポートの合計数です。スイッチ上で設定された最大リンク数の値が、ASA での値を超えていないことを確認してください。
- ASA 上で設定される最小リンク数は、ポートチャネル インターフェイスを起動するための最小アクティブポート数（ユニットあたり）です。スイッチ上では、最小リンク数はクラスタ全体の最小リンク数であるため、この値は ASA での値とは一致しません。
- デフォルトのロードバランシングアルゴリズムを変更しないでください。スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシングアルゴリズムでは、**vlan** キーワードを使用しないでください。
- スバンド EtherChannel を使用している場合、クラスタリングが完全にイネーブルになるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

- ステップ 1** コンテキスト モードによって次のように異なります。
- シングル モードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
 - マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。
- ステップ 2** [Add] > [EtherChannel Interface] の順に選択します。
[Add EtherChannel Interface] ダイアログボックスが表示されます。
- ステップ 3** 次をイネーブルにします。
- [Port Channel ID]
 - [Span EtherChannel across the ASA cluster]
 - [Enable Interface]（デフォルトでオンになります）
 - [Members in Group] : [Members in Group] リストに、インターフェイスを少なくとも 1 つ追加する必要があります。ユニットごとに複数のインターフェイスが EtherChannel に含まれていると、VSS または vPC のスイッチに接続する場合に役立ちます。デフォルトでは、クラスタの全メンバで最大 16 個のアクティブ インターフェイスのうち、スバンド EtherChannel が使用できるのは 8 個だけであることを注意してください。残りの 8 インターフェイスはリンク障害時のためのスタンバイです。8 個より多くのアクティブ インターフェイスを使用するには（ただしスタンバイ インターフェイスではなく）、ダイナミック ポート プライオリティをディセーブルにします。ダイナミック ポート プライオリティを

ディセーブルにすると、クラスタ全体で最大 32 個のアクティブリンクを使用できます。たとえば、16 台の ASA から成るクラスタの場合は、各 ASA で最大 2 個のインターフェイスを使用でき、スパンド EtherChannel の合計は 32 インターフェイスとなります。

すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。ASDM では、一致しないインターフェイスの追加は防止されません。

この画面の残りのフィールドは、この手順の後半で説明します。

ステップ 4 (オプション) すべてのメンバーインターフェイスについて、メディアタイプ、二重通信、速度、フロー制御のポーズフレームを上書きするには、[Configure Hardware Properties] をクリックします。これらのパラメータはチャンネルグループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

[OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 5 MAC アドレスおよびオプションパラメータを設定するには、[Advanced] タブをクリックします。

- [MAC Address Cloning] 領域で、EtherChannel の手動グローバル MAC アドレスを設定します。スタンバイ MAC アドレスを設定しないでください。無視されます。潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel にはグローバル MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在のマスターユニットに留まります。MAC アドレスを設定していない場合に、マスターユニットが変更された場合、新しいマスターユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

マルチコンテキストモードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

- (オプション) VSS または vPC の 2 台のスイッチに ASA を接続する場合は、[Enable load balancing between switch pairs in VSS or vPC mode] チェックボックスをオンにして、VSS ロードバランシングをイネーブルにする必要があります。この機能を使用すると、ASA と VSS (または vPC) ペアとの間の物理リンク接続の負荷が確実に分散されます。

[Member Interface Configuration] 領域で、1 または 2 のどちらのスイッチに特定のインターフェイスを接続するかを特定する必要があります。

(注) [Minimum Active Members] と [Maximum Active Members] は設定しないことを推奨します。

ステップ 6 (オプション) この EtherChannel に VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。

- ステップ 7** (マルチ コンテキスト モード) この手順を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。
- [OK] をクリックして変更内容を確定します。
 - インターフェイスを割り当てます。
 - ユーザが設定するコンテキストを変更します。[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
 - [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択し、カスタマイズするポートチャネルインターフェイスを選択して、[Edit] をクリックします。
- [Edit Interface] ダイアログボックスが表示されます。
- ステップ 8** [General] タブをクリックします。
- ステップ 9** (トランスペアレントモード) [Bridge Group] ドロップダウンリストから、このインターフェイスを割り当てるブリッジグループを選択します。
- ステップ 10** [Interface Name] フィールドに、名前を 48 文字以内で入力します。
- ステップ 11** [Security level] フィールドに、0 (最低) ~ 100 (最高) のレベルを入力します。
- ステップ 12** (ルーテッドモード) IPv4 アドレスに対して [Use Static IP] オプションボタンをクリックし、IP およびマスクを入力します。DHCP と PPPoE はサポートされません。トランスペアレントモードの場合は、EtherChannel インターフェイスではなく、ブリッジグループインターフェイスの IP アドレスを設定します。
- ステップ 13** (ルーテッドモード) IPv6 アドレスを設定するには、[IPv6] タブをクリックします。
- トランスペアレントモードの場合は、EtherChannel インターフェイスではなく、ブリッジグループインターフェイスの IP アドレスを設定します。
- [Enable IPv6] チェックボックスをオンにします。
 - [Interface IPv6 Addresses] エリアで、[Add] をクリックします。
- [Add IPv6 Address for Interface] ダイアログボックスが表示されます。
- (注) [Enable address autoconfiguration] オプションはサポートされません。
- [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、2001:DB8::BA98:0:3210/64。
 - (オプション) ホストアドレスとして Modified EUI-64 インターフェイス ID を使用するには、[EUI-64] チェックボックスをオンにします。この場合は、単に [Address/Prefix Length] フィールドにプレフィックスを入力します。
 - [OK] をクリックします。
- ステップ 14** [OK] をクリックして、[Interfaces] 画面に戻ります。
- ステップ 15** [Apply] をクリックします。

ASA クラスタの作成または ASA クラスタへの参加

クラスタ内の各ユニットがクラスタに参加するには、ブートストラップコンフィギュレーションが必要です。

高可用性のウィザードの実行

クラスタ内の各ユニットがクラスタに参加するには、ブートストラップコンフィギュレーションが必要です。1台のユニット（マスターユニットになる）上で **High Availability and Scalability** ウィザードを実行してクラスタを作成し、続いてスレーブユニットを追加します。



(注) マスターユニットに対して、**cLACP** システム ID およびプライオリティのデフォルトを変更する場合は、ウィザードを使用できません。クラスタを手動で設定する必要があります。

始める前に

- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある **[System]** をダブルクリックします。
- クラスタ制御リンクの MTU を 1600 バイト以上に設定することを推奨します。このようにするには、この手順を続ける前に各ユニットでジャンボフレームの予約をイネーブルにする必要があります。ジャンボ フレームの予約には、ASA のリロードが必要です。
- クラスタ制御リンク インターフェイスに使用するインターフェイスは、接続されたスイッチでアップ状態になっている必要があります。
- 稼働中のクラスタにユニットを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがあります。これは予定どおりの動作です。

手順

ステップ 1 **[Wizards] > [High Availability and Scalability Wizard]** の順に選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2 **[Interfaces]** 画面からは新しい EtherChannel を作成できません（クラスタ制御リンクを除く）。

ステップ 3 **[ASA Cluster Configuration]** 画面で、ブートストラップの設定を構成します。

- [Member Priority]** : マスターユニット選定用に、このユニットのプライオリティを 1 ~ 100 の範囲で設定します。1 が最高のプライオリティです。
- (オプション) **[Shared Key]** : クラスタ制御リンクの制御トラフィックの暗号キーを設定します。共有秘密は、1 ~ 63 文字の ASCII 文字列です。共有秘密は、暗号キーを生成するために使用されます。このパラメータは、データパストラフィック（接続状態アップ

データや転送されるパケットなど)には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。パスワードの暗号化サービスをイネーブルにする場合にも、このパラメータを設定する必要があります。

- (オプション) [Enable connection rebalancing for TCP traffic across all the ASAs in the cluster] : 接続の再分散をイネーブルにします。このパラメータはデフォルトではディセーブルになっています。イネーブルの場合は、クラスタの ASA は定期的に負荷情報を交換し、負荷のかかっているデバイスから負荷の少ないデバイスに新しい接続をオフロードします。負荷情報を交換する間隔を、1 ~ 360 秒の範囲内で指定します。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブユニットに複製されます。

(注) サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。

- (オプション) [Enable health monitoring of this device within the cluster] : クラスタユニットのヘルスチェック機能を有効にします。ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにキープアライブ メッセージを送信します。ユニットが保留時間内にピア ユニットからキープアライブ メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。

(注) 何らかのトポロジ変更を行うとき (たとえば、データインターフェイスの追加または削除、ASA またはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSS または vPC を形成するスイッチの追加など) は、ヘルスチェックをディセーブルにし、ディセーブルにしたインターフェイスのモニタリングもディセーブルにする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルスチェックを再度イネーブルにします。

- [Time to Wait Before Device Considered Failed] : この値は、ユニットのキープアライブ ステータス メッセージの間隔を指定します。0.8 ~ 45 秒です。デフォルトは 3 秒です。
- (オプション) [Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support] : クラスタ制御リンクが EtherChannel として設定されていて (推奨)、VSS または vPC ペアに接続されている場合は、このオプションをイネーブルにすることが必要になる場合があります。一部のスイッチでは、VSS/vPC の 1 つのユニットがシャットダウンまたは起動すると、そのスイッチに接続された EtherChannel メンバー インターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値 (0.8 秒など) に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキープアライブ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。このオプションをイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブ メッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。

- (オプション) [Replicate console output to the master's console] : スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。この機能はデフォルトで無効に設定されています。ASAは、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力する場合があります。コンソール複製をイネーブルにすると、スレーブユニットからマスターユニットにコンソールメッセージが送信されるので、モニタが必要になるのはクラスタのコンソールポート1つだけとなります。このパラメータは、ブートストラップコンフィギュレーションの一部ではなく、マスターユニットからスレーブユニットに複製されます。
- [Cluster Control Link] : クラスタ制御リンク インターフェイスを指定します。
 - (オプション) [MTU] : クラスタ制御リンク インターフェイスの最大伝送単位を 1400 ~ 9198 バイトの範囲内で指定します。MTU 値よりも大きいデータは、送信前にフラグメント化されます。デフォルトのMTUは1500バイトです。すでにジャンボフレームの予約をイネーブルにしてある場合は、MTUを1600バイト以上に設定することを推奨します。ジャンボフレームを使用する必要があり、まだジャンボフレームの予約をイネーブルにしていない場合は、ウィザードを終了し、ジャンボフレームをイネーブルにしてから、この手順を再開する必要があります。

ステップ4 [Interfaces for Health Monitoring] 画面で、一部のインターフェイスを障害のモニタリング対象から除外できます。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。

(注) 何らかのトポロジ変更を行うとき (たとえば、データインターフェイスの追加または削除、ASAまたはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSSまたはvPCを形成するスイッチの追加など) は、ヘルスチェックをディセーブルにし、ディセーブルにしたインターフェイスのモニタリングもディセーブルにする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルスチェックを再度イネーブルにします。

ステップ5 [Finish] をクリックします。

ステップ6 ASAは実行コンフィギュレーションをスキャンして、クラスタリングに対応していない機能の非互換コマンドの有無を調べます。デフォルトコンフィギュレーションにあるコマンドも、これに該当することがあります。互換性のないコマンドを削除するには[OK]をクリックします。[Cancel] をクリックすると、クラスタリングはイネーブルになりません。

しばらくすると、ASDMがクラスタをイネーブルにしてASAに再接続し、ASAがクラスタに追加されたことを確認する[Information]画面が表示されます。

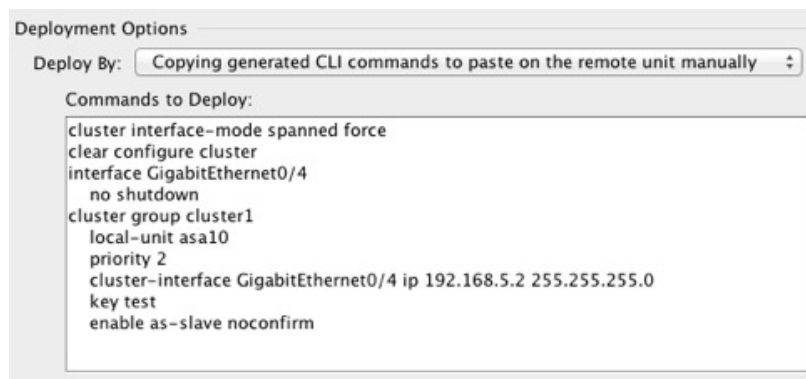
(注) 場合によっては、ウィザードの完了後にクラスタに参加した際にエラーが発生する可能性があります。ASDMが切断されていると、ASDMはそれに続くエラーをASAから受信しません。ASDMに再接続した後もクラスタリングがディセーブルの場合は、ASAコンソールポートに接続して、クラスタリングがディセーブルになっている詳細なエラー状況を判断する必要があります。たとえば、クラスタ制御リンクがダウンしている可能性があります。

ステップ7 スレーブユニットを追加するには、[Yes] をクリックします。

マスターからウィザードを再実行する場合、ウィザードを最初に開始するときに [Add another member to the cluster] オプションを選択してスレーブ ユニットの追加できます。

ステップ 8 [Deployment Options] 領域で、次の [Deploy By] オプションのいずれかを選択します。

- [Sending CLI commands to the remote unit now] : ブートストラップ コンフィギュレーションをスレーブ (一時) 管理 IP アドレスに送信します。スレーブ管理 IP アドレス、ユーザー名、パスワードを入力します。
- [Copying generated CLI commands to paste on the remote unit manually] : スレーブ ユニットの CLI でコマンドをカットアンドペースト、または ASDM の CLI ツールを使用するようにコマンドを生成します。[Commands to Deploy] ボックスで、後で使用するためのコマンドを選択してコピーします。



クラスタリング動作のカスタマイズ

クラスタリングヘルス モニタリング、TCP 接続複製の遅延、フローのモビリティ、他の最適化をカスタマイズできます。

マスターユニットで次の手順を実行します。

ASA クラスターの基本パラメータの設定

マスターユニット上のクラスター設定をカスタマイズできます。クラスターへのユニットの追加にウィザードを使用しない場合は、クラスターパラメータを手動で設定できます。すでにクラスタリングがイネーブルであれば、いくつかのクラスターパラメータを編集できます。クラスタリングがイネーブルになっている間は編集できないものは、グレイ表示されます。この手順には、ウィザードに含まれていない高度なパラメータも含まれます。

始める前に

- クラスターに参加する前に、各ユニットでクラスター制御リンク インターフェイスを事前に設定します。シングルインターフェイスの場合、イネーブルにする必要があります。他の設

定を構成しないでください。EtherChannel インターフェイスの場合は、イネーブルにして、EtherChannel モードをオンに設定します。

- マルチ コンテキスト モードでは、マスター ユニット上のシステム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある **[System]** をダブルクリックします。

手順

ステップ 1 **[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]** の順に選択します。

すでにクラスタにデバイスが追加されており、それがマスターユニットの場合は、このペインは **[Cluster Configuration]** タブにあります。

ステップ 2 **[Configure ASA cluster settings]** チェックボックスをオンにします。

チェックボックスをオフにすると、設定が消去されます。パラメータの設定がすべて完了するまで、**[Participate in ASA cluster]** をオンにしないでください。

- (注) クラスタリングをイネーブルにした後、**[Configure ASA cluster settings]** チェックボックスをオフにする場合は、結果をよく理解したうえで行ってください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

ステップ 3 次のブートストラップ パラメータを設定します。

- **[Cluster Name]** : クラスタに名前を付けます。名前は 1 ~ 38 文字の ASCII 文字列であることが必要です。クラスタはユニットあたり 1 つしか設定できません。クラスタのすべてのメンバが同じ名前を使用する必要があります。
- **[Member Name]** : このクラスタ メンバの固有の名前を 1 ~ 38 文字の ASCII 文字列で指定します。
- **[Member Priority]** : マスターユニット選定用に、このユニットのプライオリティを 1 ~ 100 の範囲内で設定します。1 が最高のプライオリティです。
- (オプション) **[Shared Key]** : クラスタ制御リンクの制御トラフィックの暗号キーを設定します。共有秘密は、1 ~ 63 文字の ASCII 文字列です。共有秘密は、暗号キーを生成するために使用されます。このパラメータは、データパストラフィック (接続状態アップデートや転送されるパケットなど) には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。パスワードの暗号化サービスをイネーブルにする場合にも、このパラメータを設定する必要があります。

- (オプション) [Enable connection rebalancing for TCP traffic across all the ASAs in the cluster] : 接続の再分散をイネーブルにします。このパラメータはデフォルトではディセーブルになっています。イネーブルの場合は、クラスタの ASA は定期的に負荷情報を交換し、負荷のかかっているデバイスから負荷の少ないデバイスに新しい接続をオフロードします。負荷情報を交換する間隔を、1 ~ 360 秒の範囲内で指定します。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブユニットに複製されます。
- (オプション) [Enable health monitoring of this device within the cluster] : クラスタ ユニットのヘルスチェック機能を有効にして、ユニット キープアライブ ステータス メッセージ間の時間間隔を決定します。0.8 から 45 秒の間で選択できます。デフォルトは 3 秒です。
注 : 新しいユニットをクラスタに追加していて、ASA またはスイッチのトポロジが変更される場合、クラスタが完成するまでこの機能を一時的にディセーブルにし、ディセーブルにされたインターフェイスのインターフェイス モニタリングもディセーブルにする必要があります ([Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring])。クラスタとトポロジの変更が完了したら、この機能を再度イネーブルにすることができます。ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにキープアライブ メッセージを送信します。ユニットが保留時間内にピア ユニットからキープアライブ メッセージを受信しない場合は、そのピアユニットは応答不能またはデッド状態と見なされます。
 - (オプション) [Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support] : クラスタ制御リンクが EtherChannel として設定されていて (推奨)、VSS または vPC ペアに接続されている場合は、このオプションをイネーブルにすることが必要になる場合があります。一部のスイッチでは、VSS/vPC の 1 つのユニットがシャットダウンまたは起動すると、そのスイッチに接続された EtherChannel メンバー インターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値 (0.8 秒など) に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキープアライブ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。このオプションをイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブ メッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。
- (オプション) [Replicate console output to the master's console] : スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力する場合があります。コンソール複製をイネーブルにすると、スレーブユニットからマスターユニットにコンソール メッセージが送信されるので、モニタが必要になるのはクラスタのコンソールポート 1 つだけとなります。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスターユニットからスレーブユニットに複製されます。

- **[Cluster Control Link]** : クラスタ制御リンク インターフェイスを指定します。このインターフェイスは、設定されている名前を使用できません。使用可能なインターフェイスがドロップダウン リストに表示されます。
 - **[Interface]** : インターフェイス ID、できれば EtherChannel を指定します。サブインターフェイスと管理タイプ インターフェイスは許可されません。
 - **[IP Address]** : IP アドレスには IPv4 アドレスを指定します。IPv6 は、このインターフェイスではサポートされません。
 - **[Subnet Mask]** : サブネット マスクを指定します。
 - (オプション) **[MTU]** : クラスタ制御リンク インターフェイスの最大伝送単位を 1400 ~ 9198 バイトの範囲内で指定します。MTU 値よりも大きいデータは、送信前にフラグメント化されます。デフォルトの MTU は 1500 バイトです。MTU を 1600 バイト以上に設定することを推奨します。このようにするには、ジャンボフレームの予約をイネーブルにする必要があります。
- (オプション) **[Cluster LACP]** : スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel のネゴシエーションを行います。cLACP ネゴシエーションの際に、同じクラスタ内の ASA は互いに連携するため、スイッチには 1 つの (仮想) デバイスであるかのように見えます。
 - **[Enable static port priority]** : LACP のダイナミック ポートプライオリティをディセーブルにします。一部のスイッチはダイナミック ポートプライオリティをサポートしていないので、このパラメータによりスイッチの互換性が向上します。さらに、8 個より多くのアクティブなスパンド EtherChannel メンバのサポートがイネーブルになります (最大 32 メンバ)。このパラメータを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このパラメータをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。
 - **[Virtual System MAC Address]** : MAC アドレス形式である cLACP システム ID を設定します。すべての ASA が同じシステム ID を使用します。これはマスター ユニットによって自動生成され (デフォルト)、すべてのセカンダリ ユニットに複製されます。あるいは *H.H.H* の形式で手動で指定することもできます。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。ただし、この値は、クラスタリングを無効にした場合にのみ変更できます。
 - **[System Priority]** : 1 ~ 65535 の範囲でシステム プライオリティを設定します。プライオリティは意思決定を担当するユニットの決定に使用されます。デフォルトでは、ASA はプライオリティ 1 (最高のプライオリティ) を使用します。このプライオリティは、スイッチのプライオリティよりも高いことが必要です。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットから

スレーブユニットに複製されます。ただし、この値は、クラスタリングを無効にした場合にのみ変更できます。

ステップ 4 [Participate in ASA cluster] チェックボックスをオンにして、クラスタに参加します。

ステップ 5 [Apply] をクリックします。

インターフェイスのヘルスマonitoringの設定

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスマonitoringをディセーブルにすることができます。任意のポートチャネル ID、冗長 ID、単一の物理インターフェイス ID、をモニタできます。ヘルスマonitoringはVLANサブインターフェイス、またはVNIやBVIなどの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring] の順に選択します。

ステップ 2 [Monitored Interfaces] ボックスでインターフェイスを選択し、[Add] をクリックして [Unmonitored Interfaces] ボックスにそのインターフェイスを移動します。

インターフェイスステータスメッセージによって、リンク障害が検出されます。特定の論理インターフェイスのすべての物理ポートが、特定のユニット上では障害が発生したが、別のユニット上の同じ論理インターフェイスでアクティブポートがある場合、そのユニットはクラスタから削除されます。ユニットがホールド時間内にインターフェイスステータスメッセージを受信しない場合に、ASAがメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスマonitoringをディセーブルにすることができます。ポートチャネル ID と冗長 ID、または単一の物理インターフェイス ID を指定できます。ヘルスマonitoringはVLANサブインターフェイス、またはVNIやBVIなどの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ASAまたはスイッチ上のインターフェイスの有効化/無効化、VSSまたはvPCを形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし（[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]）、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルスチェック機能を再度イネーブルにできます。

ステップ3 [Apply] をクリックします。

クラスタメンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタメンバを管理できます。

マスターユニットからの新しいスレーブの追加

マスターユニットからクラスタにセカンダリを追加できます。[High Availability and Scalability] ウィザードを使用してセカンダリを追加することもできます。マスターユニットからスレーブを追加すると、クラスタ制御リンクを設定でき、追加する各スレーブユニットにクラスタインターフェイスモードを設定できるというメリットがあります。

または、スレーブユニットにログインし、ユニット上で直接クラスタリングを設定することもできます。ただし、クラスタリングをイネーブルにした後は、ASDMセッションが切断されるので、再接続する必要があります。

始める前に

- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- 管理ネットワーク上でブートストラップ コンフィギュレーションを送信する場合は、スレーブユニットにアクセス可能な IP アドレスがあることを確認してください。

手順

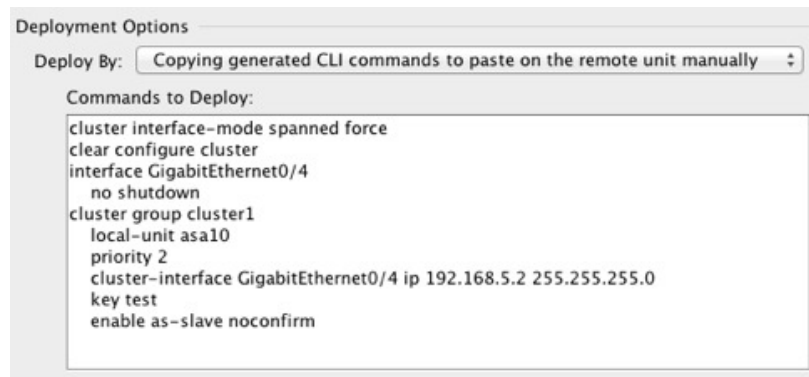
ステップ1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Members] の順に選択します。

ステップ2 [Add] をクリックします。

ステップ3 次のパラメータを設定します。

- [Member Name] : このクラスタメンバの固有の名前を 1 ~ 38 文字の ASCII 文字列で指定します。
- [Member Priority] : マスターユニット選定用に、このユニットのプライオリティを 1 ~ 100 の範囲内で設定します。1 が最高のプライオリティです。
- [Cluster Control Link] > [IP Address] : マスター クラスタ制御リンクと同じネットワーク上で、クラスタ制御リンクのこのメンバに一意の IP アドレスを指定します。

- [Deployment Options] 領域で、次の [Deploy By] オプションのいずれかを選択します。
 - [Sending CLI commands to the remote unit now] : ブートストラップ コンフィギュレーションをスレーブ（一時）管理 IP アドレスに送信します。スレーブ管理 IP アドレス、ユーザ名、パスワードを入力します。
 - [Copying generated CLI commands to paste on the remote unit manually] : スレーブ ユニットの CLI でコマンドをカットアンドペースト、または ASDM の CLI ツールを使用するようにコマンドを生成します。[Commands to Deploy] ボックスで、後で使用するためのコマンドを選択してコピーします。



ステップ 4 [OK] をクリックし、さらに [Apply] をクリックします。

非アクティブなメンバーになる

クラスタの非アクティブなメンバーになるには、クラスタリング コンフィギュレーションは変更せずに、そのユニット上でクラスタリングをディセーブルにします。



- (注) ASA が（手動で、またはヘルスチェックエラーにより）非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのユニットをクラスタから完全に削除します。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] の順に選択します。

ステップ 2 [Participate in ASA cluster] チェックボックスをオフにします。

- (注) [Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

ステップ 3 [Apply] をクリックします。

マスターユニットからのスレーブメンバーの非アクティブ化

スレーブメンバを非アクティブにするには、次のステップを実行します。



- (注) ASA が非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

-
- ステップ 1** **[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]** の順に選択します。
- ステップ 2** 削除するスレーブを選択して **[Delete]** をクリックします。
- スレーブ ブートストラップ コンフィギュレーションは同じであり、その設定を失うことなく以後スレーブを再追加できます。
- ステップ 3** **[Apply]** をクリックします。
-

クラスタへの再参加

ユニットがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルにするには、コンソール ポートを使用する必要があります。他のインターフェイスはシャットダウンされます。ただし、ASDM でクラスタリングを手動で無効にした場合、設定を保存してリロードしなかった場合は、ASDM でクラスタリングを再び有効にできます。リロード後、管理インターフェイスは無効になるため、コンソール アクセスがクラスタリングを再び有効にする唯一の方法です。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある **[System]** をダブルクリックします。
- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

-
- ステップ 1** ASDM にまだアクセスしている場合は、再イネーブル化するユニットに ASDM を接続して、ASDM でクラスタリングを再び有効にすることができます。
- 新しいメンバーとして追加していない限り、スレーブ ユニットのクラスタリングをマスターユニットから再び有効にすることはできません。
- a) **[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]** の順に選択します。
 - b) **[Participate in ASA cluster]** チェックボックスをオンにします。
 - c) **[Apply]** をクリックします。

ステップ2 ASDM を使用できない場合：コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group name

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ3 クラスタリングをイネーブルにします。

enable

クラスタからの脱退

クラスタから完全に脱退するには、クラスタ ブートストラップ コンフィギュレーション全体を削除する必要があります。各メンバの現在のコンフィギュレーションは（プライマリユニットから同期されて）同じであるため、クラスタから脱退すると、クラスタリング前のコンフィギュレーションをバックアップから復元するか、IPアドレスの競合を避けるためコンフィギュレーションを消去して初めからやり直すことも必要になります。

始める前に

コンソールポートを使用する必要があります。クラスタのコンフィギュレーションを削除すると、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスがシャットダウンされます。

手順

ステップ1 セカンダリ ユニットの場合、クラスタリングを次のようにディセーブルにします。

cluster group cluster_name no enable

例：

```
ciscoasa(config)# cluster group cluster1  
ciscoasa(cfg-cluster)# no enable
```

クラスタリングがセカンダリ ユニット上でイネーブルになっている間は、コンフィギュレーション変更を行うことはできません。

ステップ2 クラスタ コンフィギュレーションをクリアします。

clear configure cluster

ASAは、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスをシャットダウンします。

ステップ3 クラスタ インターフェイス モードをディセーブルにします。

no cluster interface-mode

モードはコンフィギュレーションには保存されないため、手動でリセットする必要があります。

ステップ4 バックアップ コンフィギュレーションがある場合、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

copy backup_cfg running-config

例 :

```
ciscoasa(config)# copy backup_cluster.cfg running-config
Source filename [backup_cluster.cfg]?
Destination filename [running-config]?
ciscoasa(config)#
```

ステップ5 コンフィギュレーションをスタートアップに保存します。

write memory

ステップ6 バックアップ コンフィギュレーションがない場合は、管理アクセスを再設定します。たとえば、インターフェイス IP アドレスを変更し、正しいホスト名を復元します。

マスターユニットの変更



注意 マスターユニットを変更する最良の方法は、マスターユニットでクラスタリングを無効にし、新しいマスターの選択を待ってから、クラスタリングを再度有効にする方法です。マスターにするユニットを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用してマスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

マスターユニットを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーションモードに入っていない場合は、[Configuration]>[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ1 [Monitoring]>[ASA Cluster]>[Cluster Summary] を選択します。

- ステップ2 [Change Master To] ドロップダウン リストから、マスターにするスレーブ ユニットを選択し、[Make Master] をクリックします。
- ステップ3 マスター ユニット変更の確認を求められます。[Yes] をクリックします。
- ステップ4 ASDM を終了し、メイン クラスタ IP アドレスを使用して再接続します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのメンバに、または特定のメンバに送信するには、次の手順を実行します。**show** コマンドをすべてのメンバに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。その他のコマンド、たとえば **capture** や **copy** も、クラスタ全体での実行を活用できます。

始める前に

コマンドライン インターフェイス ツールでこの手順を実行します。[Tools] > [Command Line Interface] を選択します。

手順

コマンドをすべてのメンバに送信します。ユニット名を指定した場合は、特定のメンバに送信されます。

cluster exec [unit unit_name] command

例：

```
ciscoasa# cluster exec show xlate
```

メンバー名を一覧表示するには、**cluster exec unit ?**（現在のユニットを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから1つずつ）が TFTP サーバにコピーされます。宛先のキャプチャファイル名には自動的にユニット名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 および asa2 がクラスタユニット名です。

次の例では、**cluster exec show port-channel summary** コマンドの出力に、クラスタの各メンバーの EtherChannel 情報が表示されています。

```
ciscoasa# cluster exec show port-channel summary
master(LOCAL):*****
Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
-----+-----+-----+-----+-----
1          Po1             LACP      Yes   Gi0/0 (P)
2          Po2             LACP      Yes   Gi0/1 (P)
slave:*****
Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
-----+-----+-----+-----+-----
1          Po1             LACP      Yes   Gi0/0 (P)
2          Po2             LACP      Yes   Gi0/1 (P)
```

ASA クラスタのモニタリング

クラスタの状態と接続をモニタおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [Cluster Summary]**

このペインには、接続相手のユニットとクラスタのその他のユニットの情報が表示されます。また、このペインでプライマリ装置を変更することができます。

- **[Cluster Dashboard]**

プライマリ装置のホームページの **[Cluster Dashboard]** と **[Cluster Firewall Dashboard]** を使用してクラスタをモニタできます。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次の画面を参照してください。

- **[Wizards] > [Packet Capture Wizard]**

クラスタ全体のトラブルシューティングをサポートするには、マスターユニット上でのクラスタ固有トラフィックのキャプチャをイネーブルにします。これで、クラスタ内のすべてのスレーブユニットでも自動的にイネーブルになります。

クラスタ リソースのモニタリング

クラスタ リソースのモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [System Resources Graphs] > [CPU]**

このペインでは、クラスタ メンバ全体の CPU 使用率を示すグラフまたはテーブルを作成することができます。

- **[Monitoring] > [ASA Cluster] > [System Resources Graphs] > [Memory]**。このペインでは、クラスタ メンバ全体の **[Free Memory]** と **[Used Memory]** を表示するグラフまたはテーブルを作成することができます。

クラスタ トラフィックのモニタリング

クラスタ トラフィックのモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Connections]**。

このペインでは、クラスタ メンバ全体の接続を示すグラフまたはテーブルを作成することができます。

- **[Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Throughput]**。

このペインでは、クラスタ メンバ全体のトラフィックのスループットを示すグラフまたはテーブルを作成することができます。

クラスタ制御リンクのモニタリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

[Monitoring] > [Properties] > [System Resources Graphs] > [Cluster Control Link]。

このペインでは、クラスタ制御リンクの **[Receival]** および **[Transmittal]** 容量使用率を表示するグラフまたはテーブルを作成することができます。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次の画面を参照してください。

[Configuration] > [Device Management] > [Logging] > [Syslog Setup]

クラスタ内の各ユニットは、syslog メッセージを個別に生成します。同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

ASA クラスタリングの例

以下の例には、一般的な導入での ASA のクラスタ関連のすべてのコンフィギュレーションが含まれます。

ASA およびスイッチのコンフィギュレーションの例

次のコンフィギュレーション例は、ASA とスイッチ間の次のインターフェイスを接続します。

ASA インターフェイス	スイッチ インターフェイス
GigabitEthernet 0/2	GigabitEthernet 1/0/15
GigabitEthernet 0/3	GigabitEthernet 1/0/16
GigabitEthernet 0/4	GigabitEthernet 1/0/17
GigabitEthernet 0/5	GigabitEthernet 1/0/18

ASA の設定

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface GigabitEthernet0/0
  channel-group 1 mode on
  no shutdown
!
interface GigabitEthernet0/1
  channel-group 1 mode on
  no shutdown
!
interface Port-channel1
  description Clustering Interface
!
cluster group Moya
  local-unit A
  cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
  priority 10
  key emphyri0
  enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface GigabitEthernet0/0
  channel-group 1 mode on
  no shutdown
!
interface GigabitEthernet0/1
  channel-group 1 mode on
  no shutdown
!
interface Port-channel1
  description Clustering Interface
!
```

```
cluster group Moya
local-unit B
cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
priority 11
key emphyri0
enable as-slave
```

マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface GigabitEthernet0/2
channel-group 10 mode active
no shutdown
!
interface GigabitEthernet0/3
channel-group 10 mode active
no shutdown
!
interface GigabitEthernet0/4
channel-group 11 mode active
no shutdown
!
interface GigabitEthernet0/5
channel-group 11 mode active
no shutdown
!
interface Management0/0
management-only
nameif management
ip address 10.53.195.230 cluster-pool mgmt-pool
security-level 100
no shutdown
!
interface Port-channel10
port-channel span-cluster
mac-address aaaa.bbbb.cccc
nameif inside
security-level 100
ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
port-channel span-cluster
mac-address aaaa.dddd.cccc
nameif outside
security-level 0
ip address 209.165.201.1 255.255.255.224
```

Cisco IOS スイッチのコンフィギュレーション

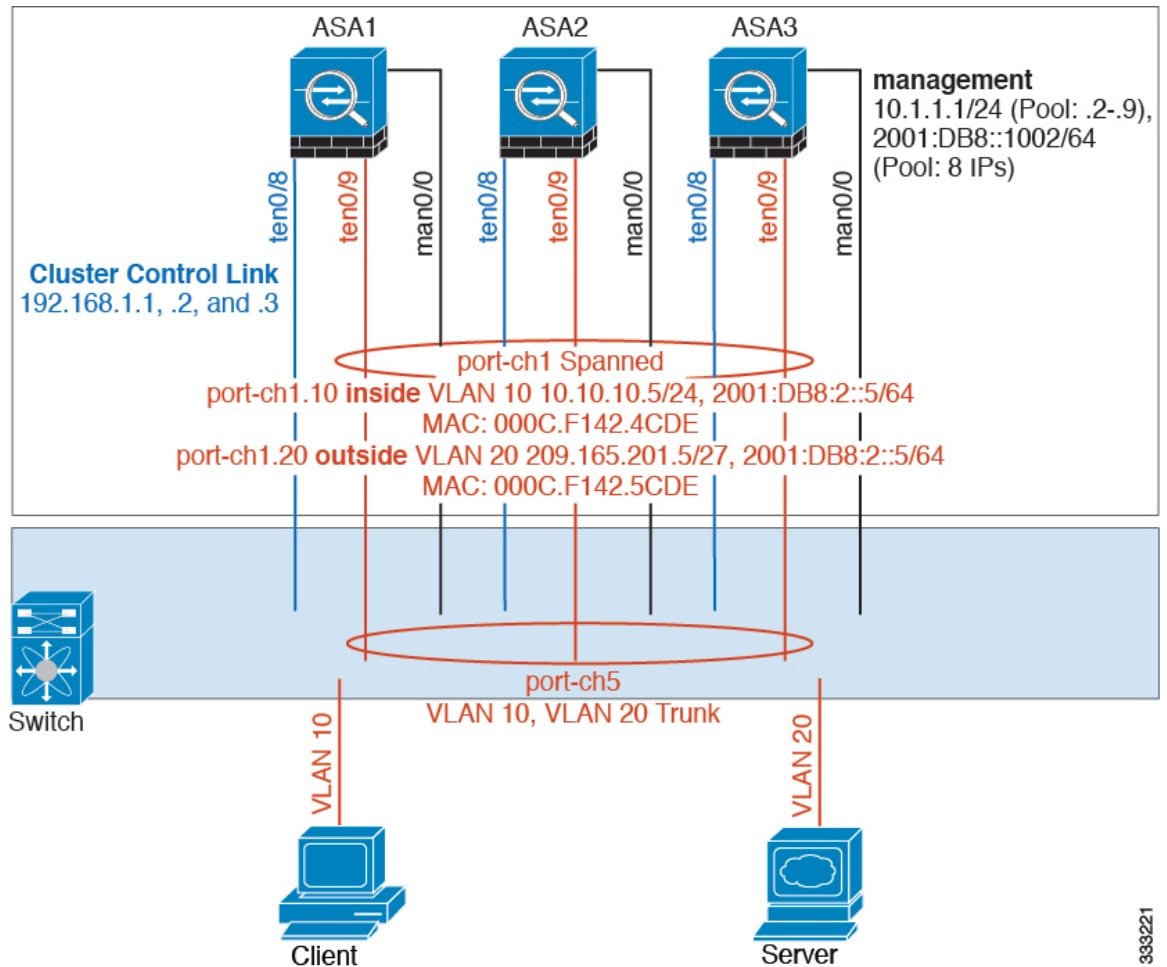
```
interface GigabitEthernet1/0/15
switchport access vlan 201
switchport mode access
spanning-tree portfast
channel-group 10 mode active
!
interface GigabitEthernet1/0/16
switchport access vlan 201
switchport mode access
```

```
spanning-tree portfast
channel-group 10 mode active
!
interface GigabitEthernet1/0/17
switchport access vlan 401
switchport mode access
spanning-tree portfast
channel-group 11 mode active
!
interface GigabitEthernet1/0/18
switchport access vlan 401
switchport mode access
spanning-tree portfast
channel-group 11 mode active

interface Port-channel10
switchport access vlan 201
switchport mode access

interface Port-channel11
switchport access vlan 401
switchport mode access
```

スティック上のファイアウォール



異なるセキュリティドメインからのデータトラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各 ASA は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランキングがイネーブされているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。ASA は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンド EtherChannel を使用するとき、スイッチ側ですべてのデータリンクがグループ化されて 1 つの EtherChannel となります。ASA の 1 つが使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

各ユニットのインターフェイスモード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/8

no shutdown
description CCL

cluster group cluster1

local-unit asa1
cluster-interface tengigabitethernet0/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/8

no shutdown
description CCL

cluster group cluster1

local-unit asa2
cluster-interface tengigabitethernet0/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

ASA3 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/8

no shutdown
description CCL

cluster group cluster1

local-unit asa3
cluster-interface tengigabitethernet0/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8
interface management 0/0

nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
```



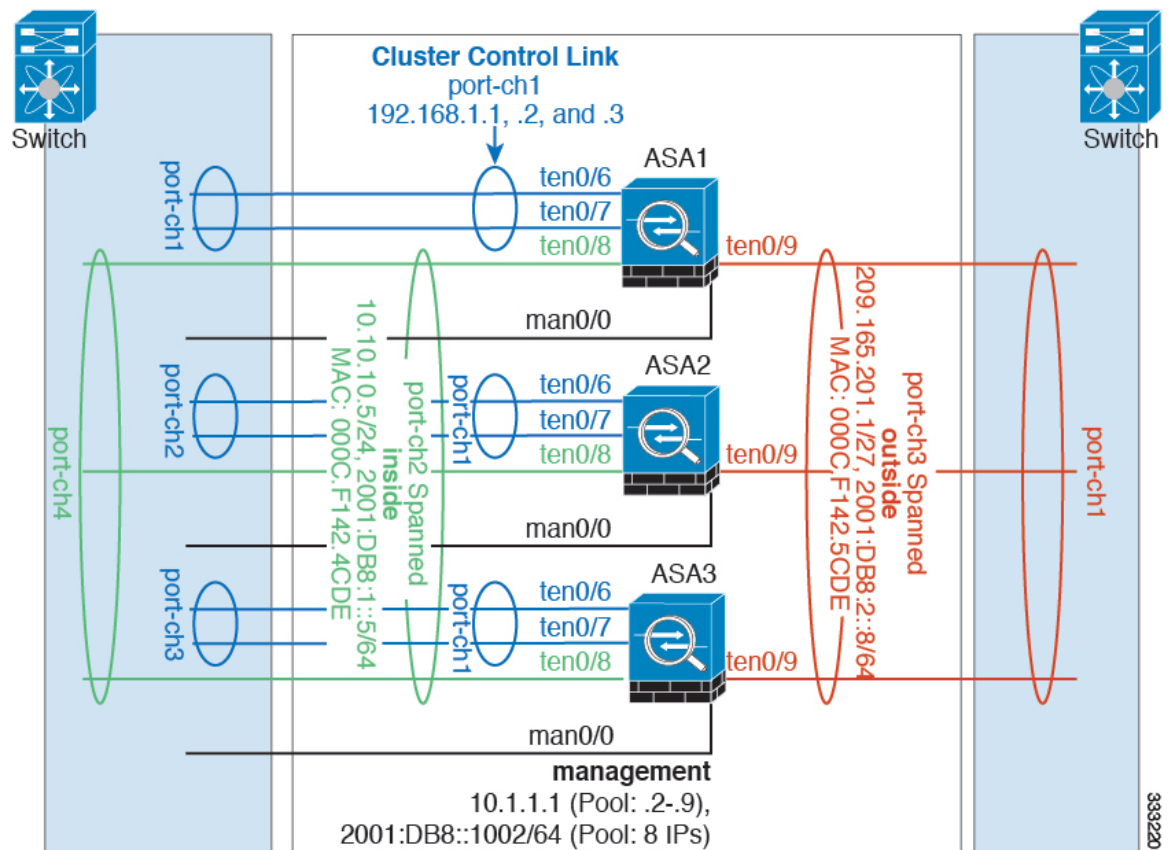
```

no shutdown

interface tengigabitethernet 0/9

channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
interface port-channel 2.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE
interface port-channel 2.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
    
```

トラフィックの分離



内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

上の図に示すように、左側に一方のスパンドEtherChannelがあり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各EtherChannel上にVLANサブインターフェイスを作成することもできます。

各ユニットのインターフェイスモード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa1
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

ASA3 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa3
cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8
interface management 0/0

nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
no shutdown

interface tengigabitethernet 0/8

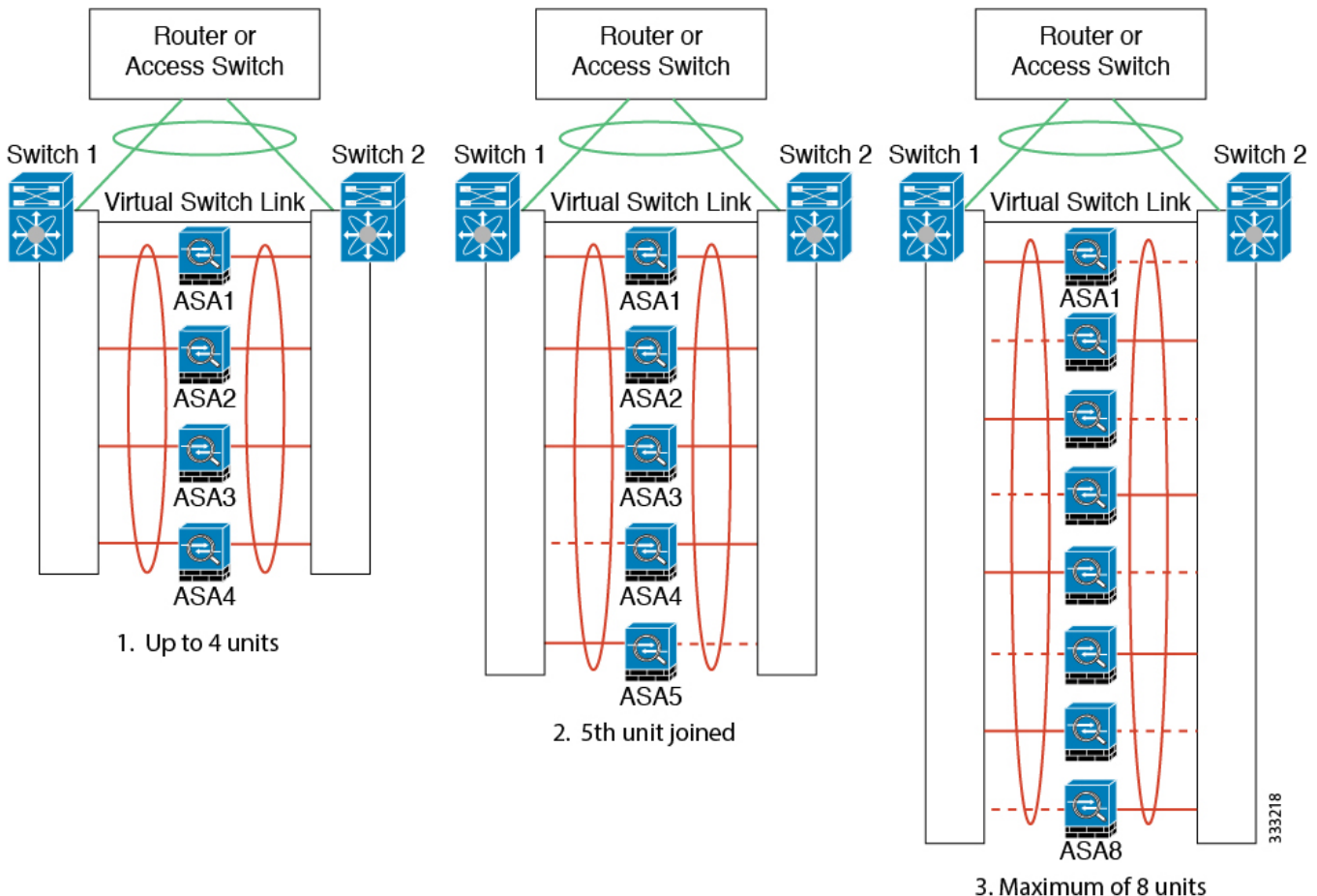
channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface tengigabitethernet 0/9

channel-group 3 mode active
no shutdown
interface port-channel 3
port-channel span-cluster
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

スバンド EtherChannel とバックアップリンク（従来の 8 アクティブ/8 スタンバイ）

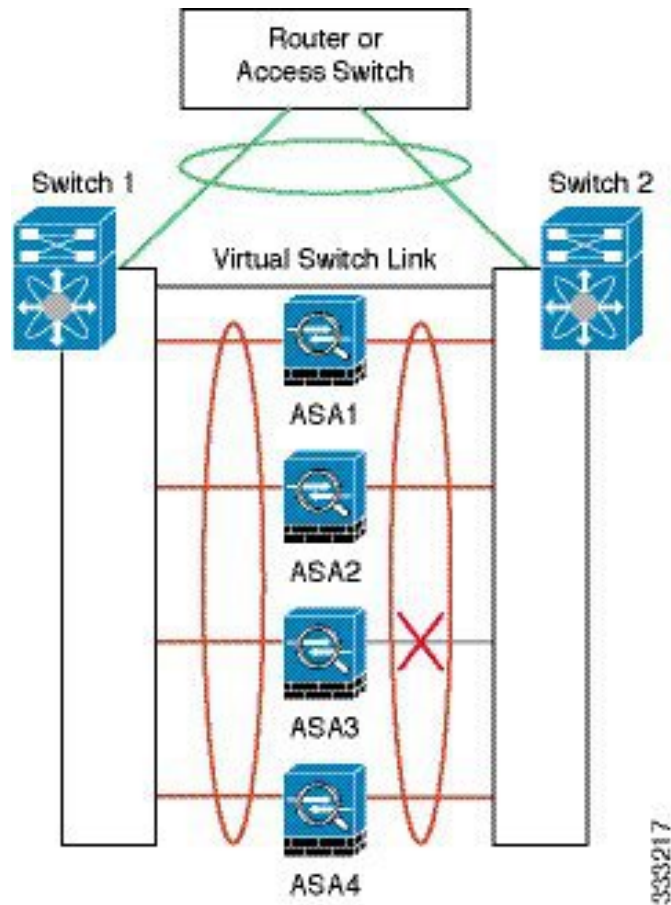
従来の EtherChannel のアクティブ ポートの最大数は、スイッチ側からの 8 に制限されます。8 台の ASA から成るクラスタがあり、EtherChannel にユニットあたり 2 ポートを割り当てた場合は、合計 16 ポートのうち 8 ポートをスタンバイ モードにする必要があります。ASA は、どのリンクをアクティブまたはスタンバイにするかを、LACP を使用してネゴシエートします。VSS または vPC を使用してマルチスイッチ EtherChannel をイネーブルにした場合は、スイッチ間の冗長性を実現できます。ASA では、すべての物理ポートが最初にスロット番号順、次にポート番号順に並べられます。次の図では、番号の小さいポートが「マスター」ポートとなり（たとえば GigabitEthernet 0/0）、他方が「スレーブ」ポートとなります（たとえば GigabitEthernet 0/1）。ハードウェア接続の対称性を保証する必要があります。つまり、すべてのマスターリンクは 1 台のスイッチが終端となり、すべてのスレーブリンクは別のスイッチが終端となっている必要があります（VSS/vPC が使用されている場合）。次の図は、クラスタに参加するユニットが増えてリンクの総数が増加したときに、どのようになるかを示しています。



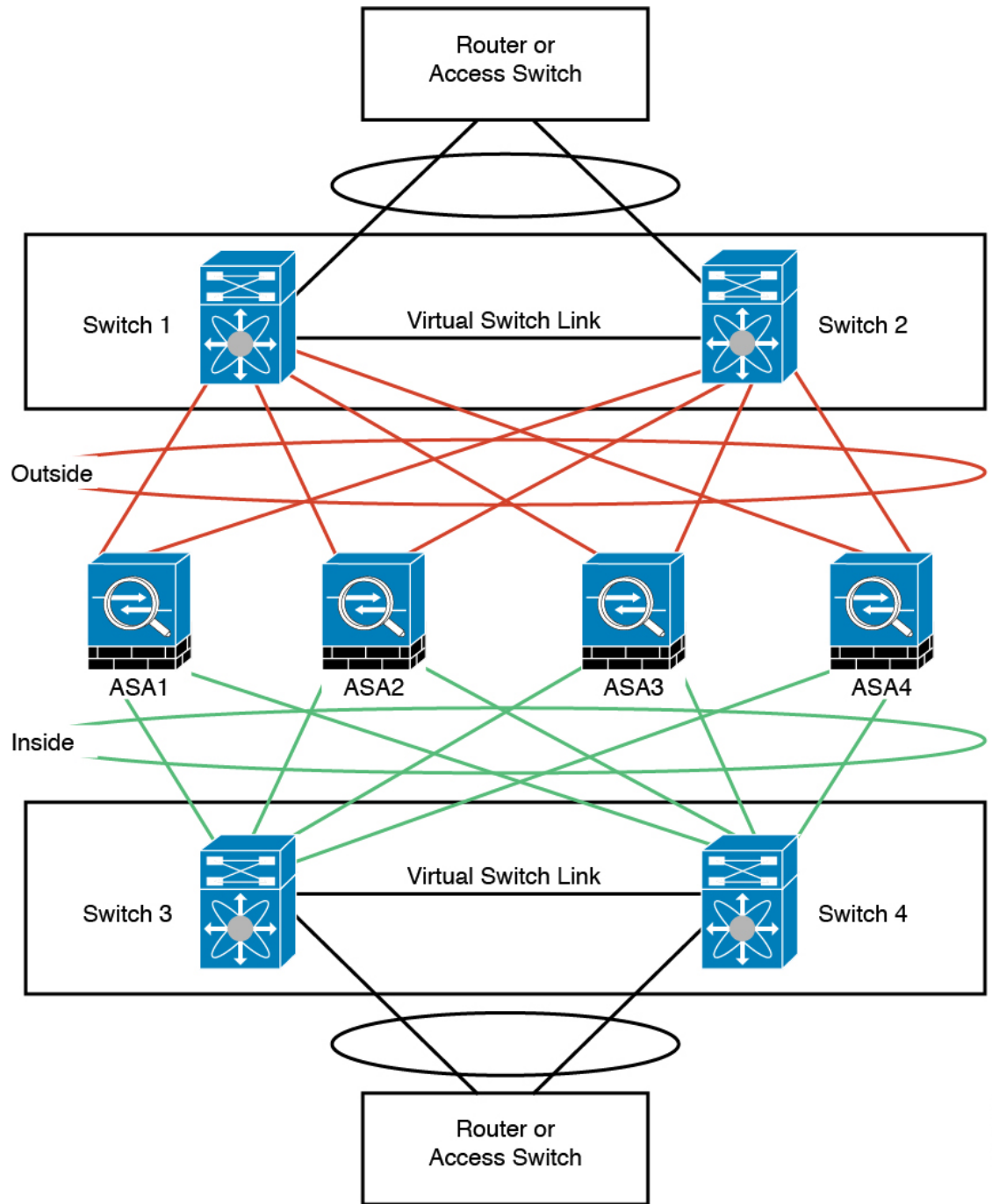
原則として、初めにチャンネル内のアクティブポート数を最大化し、そのうえで、アクティブなマスターポートとアクティブなスレーブポートの数のバランスを保ちます。5番目のユニット

がクラスタに参加したときは、トラフィックがすべてのユニットに均等には分散されないことに注意してください。

リンクまたはデバイスの障害が発生したときも、同じ原則で処理されます。その結果、ロードバランシングが理想的な状態にはならないこともあります。次の図は、4 ユニットのクラスタを示しています。このユニットの1つで、単一リンク障害が発生しています。



ネットワーク内に複数の EtherChannel を設定することも考えられます。次の図では、EtherChannel が内部に 1 つ、外部に 1 つあります。ASA は、一方の EtherChannel でマスターとスレーブの両方のリンクが障害状態になった場合にクラスタから削除されます。これは、その ASA がすでに内部ネットワークへの接続を失っているにもかかわらず、外部ネットワークからトラフィックを受信するのを防ぐためです。



333216

各ユニットのインターフェイスモード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asal
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
```

```
key chuntheunavoidable
enable as-slave
```

ASA3 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa3
cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

ASA4 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL
```



```
cluster group cluster1

local-unit asa4
cluster-interface port-channel1 ip 192.168.1.4 255.255.255.0
priority 4
key chuntheunavoidable
enable as-slave
```

マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt 10.1.1.2-10.1.1.9
interface management 0/0

channel-group 2 mode active
no shutdown

interface management 0/1

channel-group 2 mode active
no shutdown
interface port-channel 2
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
security-level 100
management-only

interface tengigabitethernet 1/6

channel-group 3 mode active vss-id 1
no shutdown

interface tengigabitethernet 1/7

channel-group 3 mode active vss-id 2
no shutdown
interface port-channel 3
port-channel span-cluster vss-load-balance
nameif inside
ip address 10.10.10.5 255.255.255.0
mac-address 000C.F142.4CDE

interface tengigabitethernet 1/8

channel-group 4 mode active vss-id 1
no shutdown

interface tengigabitethernet 1/9

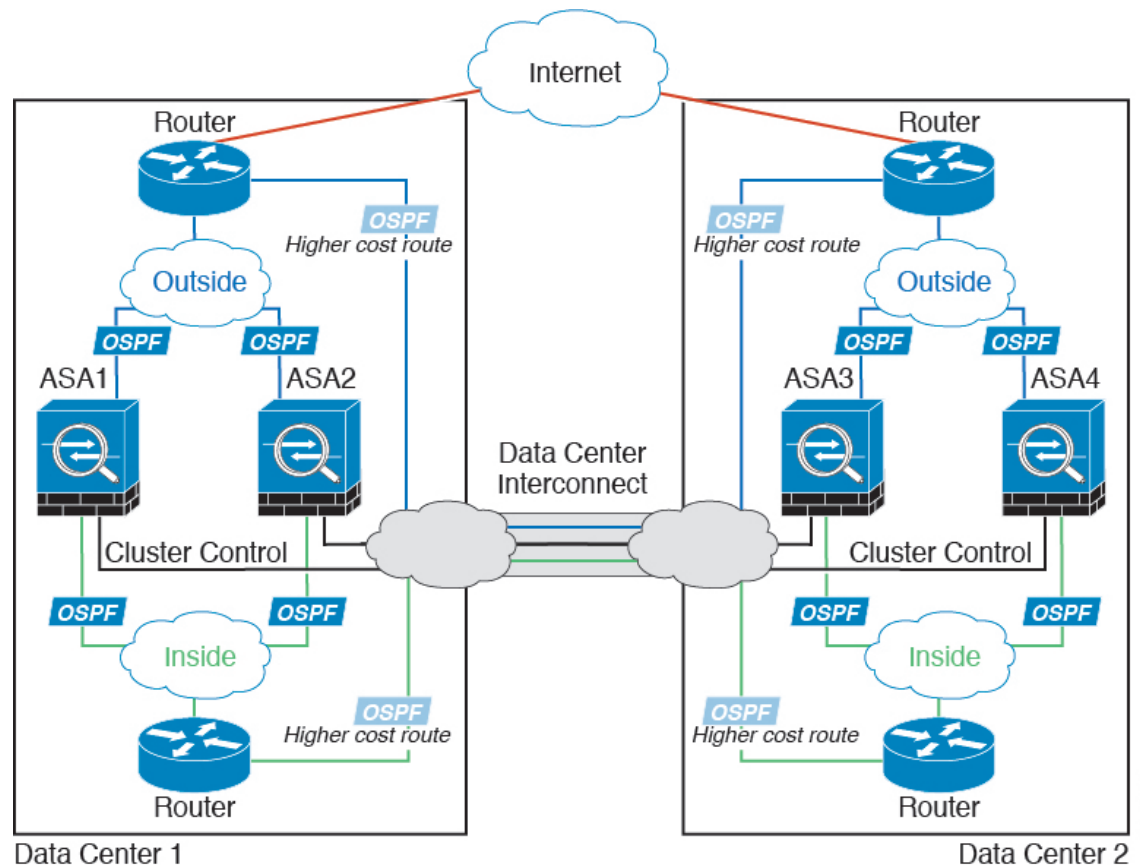
channel-group 4 mode active vss-id 2
no shutdown
interface port-channel 4
port-channel span-cluster vss-load-balance
nameif outside
ip address 209.165.201.1 255.255.255.224
mac-address 000C.F142.5CDE
```

サイト間クラスタリングの例

次の例ではサポートされるクラスタの導入を示します。

個別インターフェイスルーテッドモードノースサウスサイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2つのデータセンターのそれぞれに2つのASA クラスタメンバがある場合を示します。クラスタメンバは、DCI経由のクラスタ制御リンクによって接続されています。各データセンターの内部ルータと外部ルータは、OSPFとPBRまたはECMPを使用してクラスタメンバ間でトラフィックをロードバランスします。DCIに高コストルートを割り当てることにより、特定のサイトのすべてのASA クラスタメンバがダウンしない限り、トラフィックは各データセンター内に維持されます。1つのサイトのすべてのクラスタメンバに障害が発生した場合、トラフィックは各ルータからDCI経由で他のサイトのASA クラスタメンバに送られます。



370998

スバンド EtherChannel トランスペアレントモードノースサウスサイト間の例

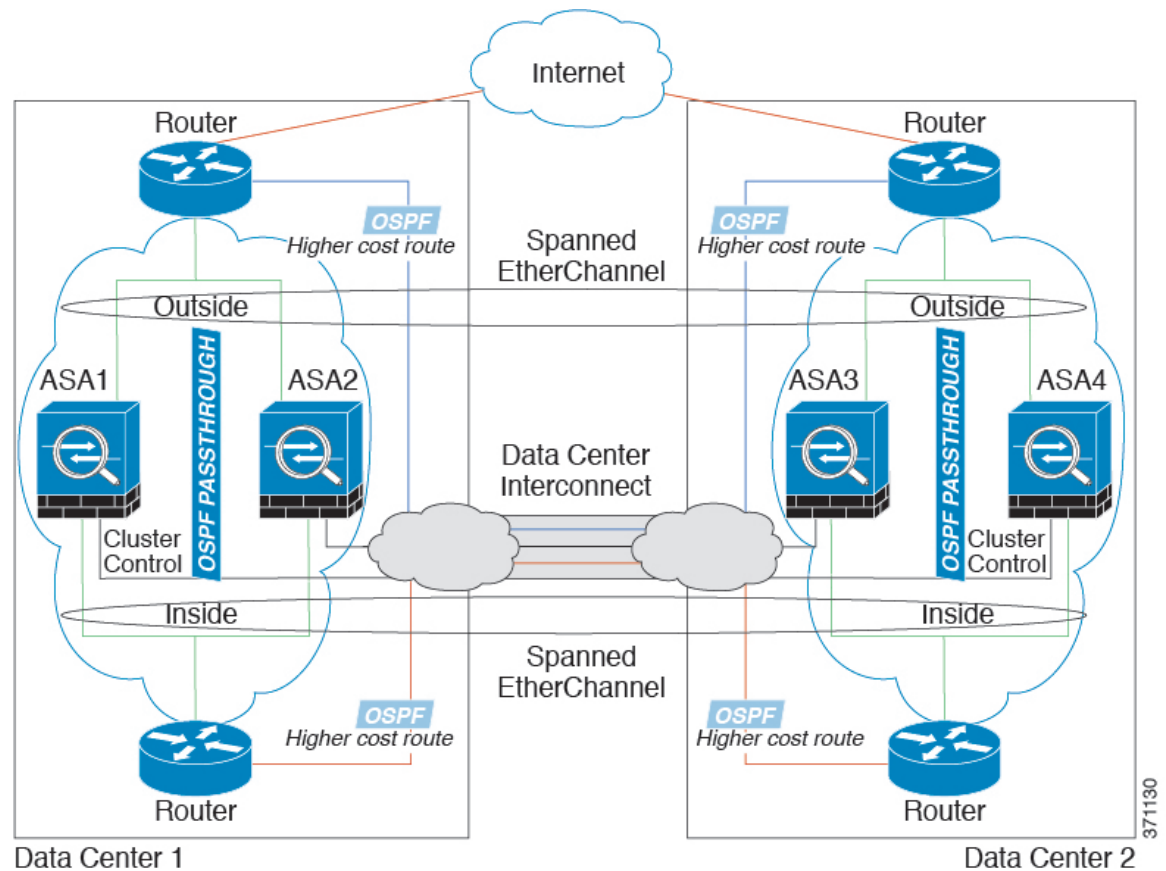
次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2つのデータセンターのそれぞれに2つのクラスタメンバがある場合を示します。クラスタメンバは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバは、内部および外部のスバンドEtherChannelsを使用してローカルスイッチに接続します。各EtherChannelは、クラスタ内のすべてのシャージにスパンされます。

各データセンターの内部ルータと外部ルータはOSPFを使用し、トランスペアレントASAを通過します。MACとは異なり、ルータのIPはすべてのルータで一意です。DCIに高コストルートを割り当てることにより、特定のサイトですべてのクラスタメンバがダウンしない限

り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジグループを横断する必要があります。1つのサイトのすべてのクラスタメンバに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトのクラスタメンバに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

- サイト間 VSS/vPC : このシナリオでは、データセンター1に1台のスイッチをインストールし、データセンター2に別のスイッチをインストールします。1つのオプションとして、各データセンターのクラスタユニットはローカルスイッチだけに接続し、VSS/vPC トラフィックはDCIを経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。オプションとして、DCIが余分なトラフィック量を処理できる場合、各ユニットをDCI経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCIを非常に堅牢にするためには不可欠です。
- 各サイトのローカルVSS/vPC : スwitchの冗長性を高めるには、各サイトに2つの異なるVSS/vPC ペアをインストールできます。この場合、クラスタユニットは、両方のローカルスイッチだけに接続されたデータセンター1のシャーシおよびこれらのローカルスイッチに接続されたデータセンター2のシャーシとはスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル VSS/vPC は、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。

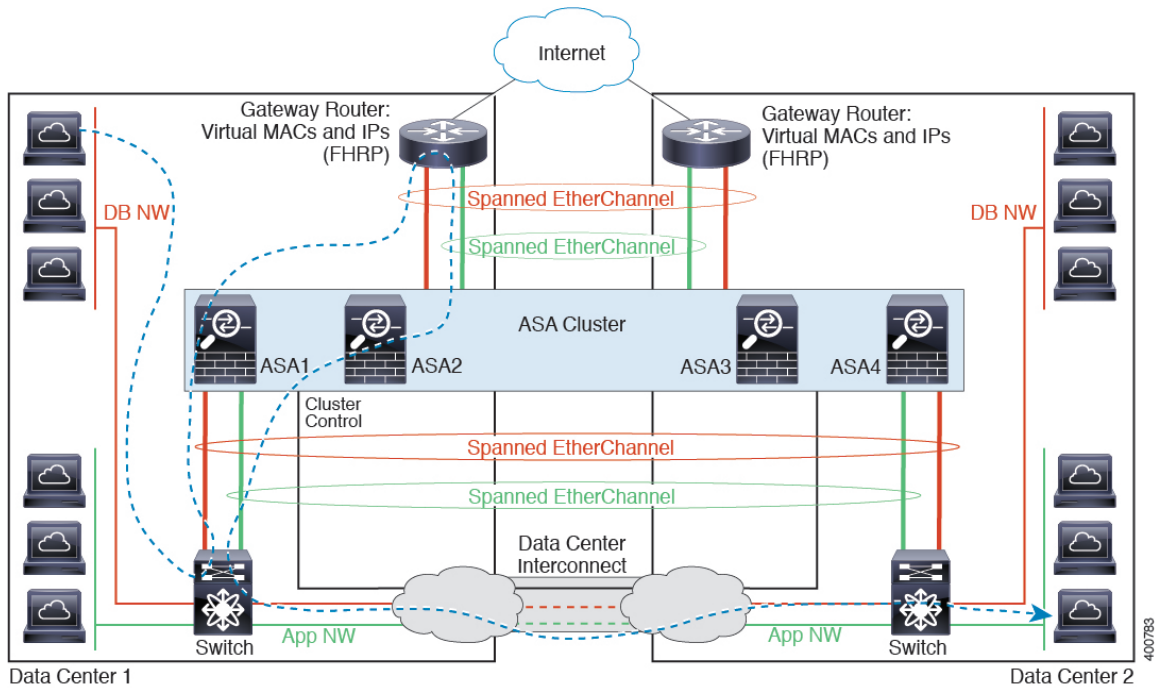


371130

スバンド EtherChannel トランスペアレントモード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイルータと2つの内部ネットワーク（アプリケーションネットワークとDBネットワーク）間に配置された（イーストウェスト挿入）2つのデータセンターのそれぞれに2つのクラスタメンバがある場合を示します。クラスタメンバは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバは、内部および外部のアプリケーションネットワークとDBネットワークの両方にスバンドEtherChannelsを使用してローカルスイッチに接続します。各EtherChannelは、クラスタ内のすべてのシャーシにスパンされます。

各サイトのゲートウェイルータは、HSRPなどのFHRPを使用して、各サイトで同じ宛先の仮想MACアドレスとIPアドレスを提供します。MACアドレスの予期せぬフラッピングを避けるため、を使用して、ゲートウェイルータの実際のMACアドレスをASA MACアドレステーブルに静的に追加することをお勧めします。これらのエントリがないと、サイト1のゲートウェイがサイト2のゲートウェイと通信する場合に、そのトラフィックがASAを通過して、内部インターフェイスからサイト2に到達しようとして、問題が発生する可能性があります。データVLANは、オーバーレイトランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがゲートウェイルータ宛てである場合にトラフィックがDCIを通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1つのサイトのゲートウェイルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



vPC/VSS オプションについては、[スパンド EtherChannel トランスペアレントモード ノースサウス サイト間の例 \(414 ページ\)](#) を参照してください。

ASA クラスタリングの履歴

機能名	バージョン	機能情報
インターフェイスごとの ASA クラスターのヘルスマonitoringの有効化またはディセーブル化	9.4(1)	<p>ヘルスマonitoringは、インターフェイスごとにイネーブルまたはディセーブルにすることができます。デフォルトでは、ポートチャネル、冗長、および単一のすべての物理インターフェイスでヘルスマonitoringがイネーブルになっています。ヘルスマonitoringは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスター制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスマonitoringをディセーブルにすることができます。</p> <p>次の画面を導入しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]。</p>
DHCP リレーの ASA クラスタリングのサポート	9.4(1)	<p>ASA クラスタで DHCP リレーを設定できます。クライアントの DHCP 要求は、クライアントの MAC アドレスのハッシュを使用してクラスターメンバにロードバランスされます。DHCP クライアントおよびサーバ機能はサポートされていません。</p> <p>変更された画面はありません。</p>

機能名	バージョン	機能情報
ASA クラスタリングでの SIP インспекションのサポート	9.4(1)	ASA クラスタで SIP インспекションを設定できます。制御フローは、任意のユニットで作成できますが（ロード バランシングのため）、その子データ フローは同じユニットに存在する必要があります。TLS プロキシ設定はサポートされていません。 変更された画面はありません。
内部ネットワーク間に ASA クラスタ ファイアウォールを備えたトランスペアレントモードのサイト間導入	9.3(2)	各サイトの内部ネットワークとゲートウェイ ルータ間にトランスペアレントモードのクラスタを導入し（AKA イーストウェスト挿入）、サイト間に内部 VLAN を拡張できます。オーバーレイ トランスポート 仮想化（OTV）の使用を推奨しますが、ゲートウェイ ルータの重複する MAC アドレスおよび IP アドレスがサイト間で漏えいしないようにする任意の方法を使用できます。HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、同じ仮想 MAC アドレスおよび IP アドレスをゲートウェイ ルータに提供します。
ASA クラスタリングに対する BGP のサポート	9.3(1)	ASA クラスタリングに対する BGP のサポートが追加されました。 次の画面を変更しました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [General]。
トランスペアレントモードでの異なる地理的位置にあるクラスタメンバのサポート（サイト間）	9.2(1)	トランスペアレント ファイアウォール モードでスパンド EtherChannel モードを使用すると、クラスタメンバを異なる地理的な場所に配置できるようになりました。ルーテッドファイアウォールモードのスパンド EtherChannel での Inter-Site クラスタリングはサポートされません。 変更された ASDM 画面はありません。
クラスタリングに対するスタティック LACP ポートプライオリティのサポート	9.2(1)	一部のスイッチは、LACP でのダイナミック ポートプライオリティをサポートしていません（アクティブおよびスタンバイリンク）。ダイナミック ポートプライオリティをディセーブルにすることで、スパンド EtherChannel との互換性を高めることができます。次の注意事項にも従う必要があります。 <ul style="list-style-type: none"> クラスタ制御リンク パスのネットワーク エレメントでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。 ポートチャネルバンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。 次の画面を変更しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]。

機能名	バージョン	機能情報
スパンド EtherChannel での 32 個のアクティブリンクのサポート	9.2(1)	<p>ASA EtherChannels は最大 16 個のアクティブリンクをサポートするようになりました。スパンド EtherChannel ではその機能が拡張されて、vPC の 2 台のスイッチで使用し、ダイナミックポートプライオリティをディセーブルにした場合、クラスタ全体で最大 32 個のアクティブリンクをサポートします。スイッチは、16 個のアクティブリンクの EtherChannel をサポートする必要があります（例：Cisco Nexus 7000 と F2 シリーズ 10 ギガビットイーサネットモジュール）。</p> <p>8 個のアクティブリンクをサポートする VSS または vPC のスイッチの場合は、スパンド EtherChannel に 16 個のアクティブリンクを設定できます（各スイッチに接続された 8 個）。従来は、VSS/vPC で使用する場合であっても、スパンド EtherChannel は 8 個のアクティブリンクと 8 個のスタンバイリンクしかサポートしていませんでした。</p> <p>（注） スパンド EtherChannel で 8 個より多くのアクティブリンクを使用する場合は、スタンバイリンクも使用できません。9～32 個のアクティブリンクをサポートするには、スタンバイリンクの使用を可能にする cLACP ダイナミックポートプライオリティをディセーブルにする必要があります。</p> <p>次の画面を変更しました。[Configuration]>[Device Management]>[High Availability and Scalability]>[ASA Cluster]。</p>
ASA 5585-X の 16 のクラスタメンバのサポート	9.2(1)	<p>ASA 5585-X が 16 ユニットクラスタをサポートするようになりました。</p> <p>変更された画面はありません。</p>
ASA 5500-X でのクラスタリングのサポート	9.1(4)	<p>ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニットクラスタをサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになります。ASA 5512-X では Security Plus ライセンスが必要です。</p> <p>変更された ASDM 画面はありません。</p>

機能名	バージョン	機能情報
ヘルス チェック モニタリングの VSS および vPC によるサポートの強化	9.1(4)	<p>クラスタ制御リンクが EtherChannel として設定されていて（推奨）、VSS または vPC ペアに接続されている場合、ヘルス チェック モニタリングによって安定性を高めることができます。一部のスイッチ（Cisco Nexus 5000 など）では、VSS/vPC の 1 つのユニットがシャットダウンまたは起動すると、そのスイッチに接続されている EtherChannel メンバー インターフェイスが ASA に対してアップと認識される場合がありますが、スイッチ側にはトラフィックが渡されていません。ASA holdtime timeout を低い値（0.8 秒など）に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキープアライブ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。VSS/vPCヘルス チェック機能をイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブメッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。</p> <p>次の画面を変更しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]。</p>
異なる地理的位置にあるクラスタメンバのサポート（サイト間）。個別インターフェイスモードのみ	9.1(4)	<p>個別インターフェイスモードを使用すると、クラスタメンバを異なる地理的な場所に配置できるようになりました。</p> <p>変更された ASDM 画面はありません。</p>
ASA 5580 および 5585-X の ASA クラスタリング	9.0(1)	<p>ASA クラスタリングを利用すると、最大で 8 の ASA をグループ化して、1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。ASA クラスタリングは、ASA 5580 および ASA 5585-X でサポートされます。1 つのクラスタ内のすべてのユニットが同一モデル、同一ハードウェア仕様であることが必要です。クラスタリングがイネーブルのときにサポートされない機能のリストについては、コンフィギュレーションガイドを参照してください。</p> <p>次の画面が導入または変更されました。</p> <p>[Home] > [Device Dashboard] [Home] > [Cluster Dashboard] [Home] > [Cluster Firewall Dashboard] [Configuration] > [Device Management] > [Advanced] > [Address Pools] > [MAC Address Pools] [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] [Configuration] > [Device Management] > [Logging] > [Syslog Setup] > [Advanced] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [Advanced] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [IPv6] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit EtherChannel Interface] > [Advanced] [Configuration] > [Firewall] > [Advanced] > [Per-Session NAT Rules] [Monitoring] > [ASA Cluster] [Monitoring] > [Properties] > [System Resources Graphs] > [Cluster Control Link] [Tools] > [Preferences] > [General] [Tools] > [System Reload] [Tools] > [Upgrade Software from Local Computer] [Wizards] > [High Availability and Scalability Wizard] [Wizards] > [Packet Capture Wizard] [Wizards] > [Startup Wizard]</p>



第 12 章

Firepower 9300 シャーシの ASA クラスタ

クラスタリングを利用すると、複数の Firepower 9300 シャーシ ASA をグループ化して、1 つの論理デバイスにすることができます。Firepower 9300 シャーシシリーズには、Firepower 9300。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。



(注) FirePOWER 9300 は複数のシャーシにまたがる（シャーシ間）クラスタをサポートしません。シャーシ内クラスタリングのみをサポートします。



(注) 一部の機能は、クラスタリングを使用する場合、サポートされません。「[クラスタリングでサポートされない機能（426 ページ）](#)」を参照してください。

- [Firepower 9300 シャーシでのクラスタリングについて（421 ページ）](#)
- [ASA の各機能とクラスタリング（425 ページ）](#)
- [Firepower 9300 シャーシでのクラスタリングの要件と前提条件（432 ページ）](#)
- [上のクラスタリングのライセンス Firepower 9300 シャーシ（432 ページ）](#)
- [クラスタリングガイドラインと制限事項（433 ページ）](#)
- [クラスタリングの設定 Firepower 9300 シャーシ（433 ページ）](#)
- [FXOS : クラスタ メンバの削除（444 ページ）](#)
- [ASA : クラスタ メンバの管理（446 ページ）](#)
- [ASA : での ASA クラスタのモニタリング Firepower 9300 シャーシ（451 ページ）](#)
- [クラスタリングの参考資料（452 ページ）](#)
- [Firepower 9300 シャーシ上の ASA クラスタリングの履歴（459 ページ）](#)

Firepower 9300 シャーシでのクラスタリングについて

クラスタは、単一の論理ユニットとして機能する複数のデバイスから構成されます。Firepower 9300 シャーシにクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポート チャネル 48）を作成します。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。
- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。
クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成が Firepower 9300 シャーシスーパーバイザからプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。
- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。
シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのように EtherChannel に制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部で EtherChannel テクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。



(注) 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。[クラスタリングの参考資料 \(452 ページ\)](#) も参照してください。

Bootstrap Configuration

クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成が Firepower 9300 シャーシスーパーバイザからプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップ コンフィギュレーションの一部はユーザが設定できます。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。

クラスタ内のメンバの 1 つが **マスター** ユニットです。マスター ユニットは自動的に決定されます。他のすべてのメンバは **スレーブ** ユニットです。

すべてのコンフィギュレーション作業はマスターユニット上でのみ実行する必要があります。コンフィギュレーションはその後、スレーブ ユニットに複製されます。

機能によっては、クラスタ内でスケリングしないものがあり、そのような機能についてはマスターユニットがすべてのトラフィックを処理します。[クラスタリングの中央集中型機能（426 ページ）](#) を参照してください。

マスターおよびスレーブユニットの役割

クラスタ内のメンバの1つがマスターユニットです。マスターユニットは自動的に決定されます。他のすべてのメンバはスレーブユニットです。

すべてのコンフィギュレーション作業はマスターユニット上でのみ実行する必要があります。コンフィギュレーションはその後、スレーブユニットに複製されます。

機能によっては、クラスタ内でスケリングしないものがあり、そのような機能についてはマスターユニットがすべてのトラフィックを処理します。[クラスタリングの中央集中型機能（426 ページ）](#) を参照してください。

クラスタ制御リンク

クラスタ制御リンクはユニット間通信用の EtherChannel（ポートチャンネル48）です。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- マスター選定。
- コンフィギュレーションの複製
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンク ネットワーク

Firepower 9300 シャーシは、シャーシ ID およびスロット ID (`127.2.chassis_id.slot_id`) に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。FXOS とアプリケーション内のどちらでも、この IP アドレスを手動で設定することはできません。クラスタ制御リンク ネットワークには、ユニット間のルータを含めることはできません。レイヤ 2 スイッチングのみが許可されます。

クラスタ インターフェイス

シャーシ内クラスタリングでは、物理インターフェイス、EtherChannel（ポートチャネルとも呼ばれる）の両方を割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロードバランシングを行うスパンドインターフェイスです。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

VSS または vPC への接続

インターフェイスに冗長性を確保するため、EtherChannel を VSS または vPC に接続することを推奨します。

設定の複製

クラスタ内のすべてのユニットは、単一のコンフィギュレーションを共有します。コンフィギュレーション変更を加えることができるのはマスターユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに同期されます。

ASA クラスターの管理

ASA クラスタリングを使用することの利点の1つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンドインターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各単位に直接接続できます。

メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のマスターユニットに属します。アドレス範囲も設定して、現在のマスターを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスターユニットが変更されると、メインクラスタ IP アドレスは新しいマスターユニットに移動するので、クラスタの管理をシームレスに続行できます。

たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在のマスターユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、マスターユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

マスターユニット管理とスレーブユニット管理

すべての管理とモニタリングはマスターユニットで実行できます。マスターユニットから、すべてのユニットの実行時統計情報やリソース使用状況などのモニタリング情報を調べることができます。また、クラスタ内のすべてのユニットに対してコマンドを発行することや、コンソールメッセージをスレーブユニットからマスターユニットに複製することもできます。

必要に応じて、スレーブユニットを直接モニタできます。マスターユニットからでもできますが、ファイル管理をスレーブユニット上で実行できます（コンフィギュレーションのバックアップや、イメージの更新など）。次の機能は、マスターユニットからは使用できません。

- ユニットごとのクラスタ固有統計情報のモニタリング。
- ユニットごとの Syslog モニタリング（コンソール レプリケーションが有効な場合にコンソールに送信される syslog を除く）。
- SNMP
- NetFlow

RSA キー複製

マスターユニット上で RSA キーを作成すると、そのキーはすべてのスレーブユニットに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合に、マスターユニットで障害が発生すると接続が切断されます。新しいマスターユニットは、SSH 接続に対して同じキーを使用するので、新しいマスターユニットに再接続するときに、キャッシュ済みの SSH ホスト キーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続する場合は、IP アドレス不一致に関する警告メッセージが表示されます。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないからです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメインクラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部はマスターユニットだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

これらの機能は、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されません。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- 次のアプリケーション インспекション：
 - CTIQBE
 - GTP
 - H323、H225、および RAS
 - IPsec パススルー
 - MGCP
 - MMP
 - RTSP
 - SCCP (Skinny)
 - WAAS
 - WCCP
- Botnet Traffic Filter
- Auto Update Server
- DHCP クライアント、サーバ、およびプロキシDHCP リレーがサポートされている。
- フェールオーバー
- デッド接続検出 (DCD)

クラスタリングの中央集中型機能

次の機能は、マスターユニット上だけでサポートされます。クラスタの場合もスケーリングされません。



(注) 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバユニットからマスターユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがマスターユニットに送り返されます。

中央集中型機能については、マスターユニットで障害が発生するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

• 次のアプリケーションインスペクション：

- DCERPC
 - NetBIOS
 - PPTP
 - RADIUS
 - RSH
 - SUNRPC
 - TFTP
 - XDMCP
-
- ダイナミック ルーティング
 - スタティック ルート モニタリング
 - IGMP マルチキャスト コントロール プレーン プロトコル処理 (データ プレーン フォワーディングはクラスタ全体に分散されます)
 - PIM マルチキャスト コントロール プレーン プロトコル処理 (データ プレーン 転送はクラスタ全体に分散されます)
 - ネットワーク アクセスの認証および許可。アカウントリングは非集中型です。
 - フィルタリング サービス

個々のユニットに適用される機能

これらの機能は、クラスタ全体またはマスターユニットではなく、各 ASA ユニットに適用されます。

- QoS : QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは、各ユニットに対して個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ユニットから成るクラスタがあり、トラ

フィックが均等に分散している場合は、適合レートは実際にクラスタのレートの3倍になります。

- 脅威検出：脅威検出は、各ユニットに対して個別に機能します。たとえば、上位統計情報は、ユニット別です。たとえば、ポート スキャン検出が機能しないのは、スキャントラフィックが全ユニット間で分散されるので、1つのユニットがすべてのトラフィックを読み取ることはないからです。
- リソース管理：マルチ コンテキスト モードでのリソース管理は、ローカル使用状況に基づいて各ユニットに個別に適用されます。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウントिंगの3つのコンポーネントで構成されます。認証および許可は、クラスタリングマスター上で中央集中型機能として実装されており、データ構造がクラスタスレーブに複製されます。マスターが選定されたときは、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するのに必要なすべての情報を、新しいマスターが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、マスターユニット変更が発生したときも維持されます。

アカウントINGは、クラスタ内の分散型機能として実装されています。アカウントINGはフロー単位で実行されるので、フローを所有するクラスタユニットがアカウントING開始と停止のメッセージを AAA サーバに送信します（フローに対するアカウントINGが設定されているとき）。

FTP とクラスタリング

- FTPデータチャンネルとコントロールチャンネルのフローがそれぞれ別のクラスタメンバによって所有されている場合は、データチャンネルのオーナーは定期的にアイドルタイムアウトアップデートをコントロールチャンネルのオーナーに送信し、アイドルタイムアウト値を更新します。ただし、コントロールフローのオーナーがリロードされて、コントロールフローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロールフローのアイドルタイムアウトは更新されません。
- FTPアクセスにAAAを使用している場合、制御チャンネルのフローはマスターユニットに集中化されます。

アイデンティティ ファイアウォールとクラスタリング

マスターユニットのみがADから user-group を取得し、AD エージェントから user-ip マッピングを取得します。マスターユニットからユーザ情報がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいてユーザ ID の一致の決定を行うことができます。

マルチキャストルーティングとクラスタリング

ファーストパス転送が確立されるまでの間、マスターユニットがすべてのマルチキャストルーティングパケットとデータパケットを処理します。接続が確立された後は、各スレーブがマルチキャストデータパケットを転送できます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。着信および発信の NAT パケットが、クラスタ内のそれぞれ別の ASA に送信されることがあります。これは、ロードバランシングアルゴリズムは IP アドレスとポートに依存していますが、NAT が使用される場合、着信と発信でパケットの IP アドレスやポートが異なるためです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。NAT オーナーはセキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成するため、受信側ユニットは転送フローをオーナーに作成しません。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

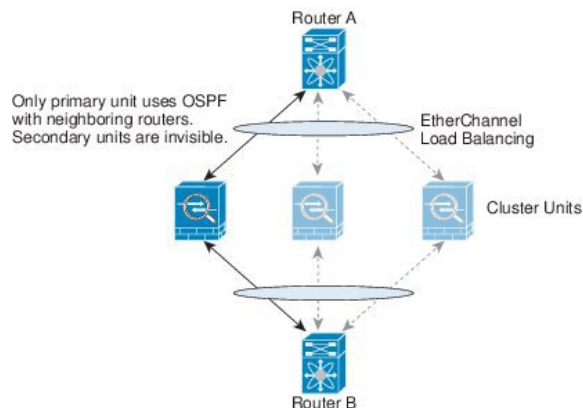
- **ダイナミック PAT 用 NAT プールアドレス分散**：マスターユニットは、アドレスをクラスタ全体に均等に分配します。メンバーが接続を受信したときに、そのメンバーのアドレスが1つも残っていない場合は、接続はドロップされます（他のメンバーにはまだ使用可能なアドレスがある場合でも）。最低でも、クラスタ内のユニットと同数の NAT アドレスが含まれていることを確認してください。各ユニットが確実に1つのアドレスを受け取るようにするためです。アドレス割り当てを表示するには、**show nat pool cluster** コマンドを使用します。
- **ラウンドロビンなし**：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- **マスターユニットによって管理されるダイナミック NAT xlate**：マスターユニットが xlate テーブルを維持し、スレーブユニットに複製します。ダイナミック NAT を必要とする接続をスレーブユニットが受信したときに、その xlate がテーブル内にない場合は、スレーブはマスターユニットに xlate を要求します。スレーブユニットが接続を所有します。
- **Per-session PAT 機能**：クラスタリングに限りませんが、Per-session PAT 機能によって PAT のスケラビリティが向上します。クラスタリングの場合は、各スレーブユニットが独自の PAT 接続を持てるようになります。対照的に、Multi-Session PAT 接続はマスターユニットに転送する必要があり、マスターユニットがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

- 次のインスペクション用のスタティック PAT はありません。
 - FTP
 - PPTP
 - RSH
 - SQLNET
 - TFTP
 - XDMCP
 - SIP

ダイナミック ルーティングおよびクラスタリング

ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニットを介して学習され、セカンダリに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 55: ダイナミック ルーティング



スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

SIP インспекションとクラスタリング

制御フローは、任意のユニットで作成できます（ロードバランシングのため）。その子データフローは同じユニットに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、そのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メインクラスタ IP アドレスではなく、常にローカルアドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合は、新しいマスターが選定されたときに、新しいマスターユニットのポーリングに失敗します。

syslog および NetFlow とクラスタリング

- **Syslog** : クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージヘッダーフィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名コンフィギュレーションはクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタブートストラップコンフィギュレーションで割り当てられたローカルユニット名をデバイス ID として使用するようロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。
- **NetFlow** : クラスタの各ユニットは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポートとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

マスターユニットだけがセキュリティグループタグ (SGT) 情報を学習します。マスターユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティポリシーに基づいて SGT の一致決定を下せます。

Firepower 9300 シャーシでのクラスタリングの要件と前提条件

モデルあたりの最大クラスタリングユニット

- Firepower 9300 : 16 モジュール。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。

スイッチ要件

- Firepower 9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチのリストについては、「[Cisco FXOS Compatibility](#)」を参照してください。

上のクラスタリングのライセンス Firepower 9300 シャーシ

マスターユニットでのみライセンスを要求できます。ライセンスはスレーブユニットでは集約されます。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。マスターユニットで完了したライセンス設定はスレーブユニットに複製されません。クラスタリングを無効にし、ライセンスを設定し、クラスタリングを再度有効にした場合限り、スレーブユニットに個別のライセンス権限付与を設定できます。



-
- (注) ASDM や他の高度暗号機能を使用するには、クラスタ展開後にマスターユニットで ASA CLI を使用して高度暗号化 (3DES) ライセンスを有効にする必要があります。このライセンスは、スレーブユニットによって継承されます。このライセンスは、各ユニットで個別に設定する必要はありません。高度暗号化 (3DES) ライセンスの評価ライセンスは一切ありません。
-



-
- (注) マスターユニットに障害が発生し、30 日 (ライセンス猶予期間) 以内に再参加しない場合、継承されたライセンスは消滅します。その場合、新しいマスターユニットに消滅したライセンスを手動で設定する必要があります。
-

クラスタリングガイドラインと制限事項

- 大々的なトポロジ変更が発生する場合（EtherChannel インターフェイスの追加または削除、Firepower 9300 シャーシ上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルス チェック機能や無効なインターフェイスのインターフェイスモニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。
- ユニットの既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制しないと、多数の ICMP メッセージがクラスタに送信されることとなります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラーメッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS または vPC に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロン モードで一部のシャーシセキュリティ モジュールをクラスタ化し、他のセキュリティモジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

デフォルト

- クラスタのヘルス チェック機能は、デフォルトでイネーブルになり、ホールド時間は 3 秒です。デフォルトでは、すべてのインターフェイスでインターネットヘルスモニタリングがイネーブルになっています。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。

クラスタリングの設定 Firepower 9300 シャーシ

クラスタは、Firepower 9300 シャーシスーパーバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。このセクションでは、デフォルトのブートストラップ設定と ASA で実行できるオプションのカスタマイズについて説明します。また、ASA 内からクラスタメンバーを管理する方法についても説明します。クラスタメンバーシップは Firepower 9300 シャーシからも管理できます。詳細については、Firepower 9300 シャーシのマニュアルを参照してください。

手順

-
- ステップ1 [FXOS : ASA クラスタの追加 \(434 ページ\)](#)
 - ステップ2 [ASA : ファイアウォール モードとコンテキスト モードの変更 \(438 ページ\)](#)
 - ステップ3 [ASA : データ インターフェイスの設定 \(438 ページ\)](#)
 - ステップ4 [ASA : クラスタ設定のカスタマイズ \(441 ページ\)](#)
 - ステップ5 [ASA : クラスタ メンバの管理 \(446 ページ\)](#)
-

FXOS : ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、することもできます。

ASA クラスタの作成

クラスタは、Firepower 9300 シャーシスーパーバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。

モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュールスロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

マルチコンテキストモードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチコンテキストモードを有効にする必要があります。

ASA をトランスペアレントファイアウォールモードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォールモードを変更します。

クラスタを導入すると、Firepower 9300 シャーシスーパーバイザが次のブートストラップ コンフィギュレーションで各 ASA アプライアンスを設定します。ブートストラップ コンフィギュレーションの一部 (**太字**のテキストで示されている部分) は、後から必要に応じて ASA から変更できます。

```
interface Port-channel48
  description Clustering Interface
  cluster group <service_type_name>
  key <secret>
  local-unit unit-<chassis#-module#>

  cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
  priority <auto>
  health-check holdtime 3
  health-check data-interface auto-rejoin 3 5 2
  health-check cluster-interface auto-rejoin unlimited 5 1
  enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
```

```
management-only individual
nameif management
security-level 0
ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```



(注) **local-unit** 名は、クラスタリングを無効化した場合にのみ変更できます。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 9300 シャーシにアップロードします。
- 次の情報を用意します。
 - 管理インターフェイス ID、IP アドレス、およびネットワーク マスク
 - ゲートウェイ IP アドレス

手順

ステップ 1 インターフェイスを設定します。

- a) クラスタを展開する前に、1つ以上のデータタイプのインターフェイスまたは EtherChannel (ポートチャネルとも呼ばれる) を追加します。

デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。導入後にもクラスタにデータ インターフェイスを追加できます。

- b) 管理タイプのインターフェイスまたは EtherChannel を追加します。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません (FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前が表示されます)。

ステップ 2 [論理デバイス (Logical Devices)] を選択します。

ステップ 3 をクリックし、次のパラメータを設定します。

- a) **デバイス名**を入力します。

この名前は、シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

- b) [Template] では、[Cisco Adaptive Security Appliance] を選択します。
c) [Image Version] を選択します。

- d) [Instance Type] では、[Native] タイプのみがサポートされます。
- e) [Usage] では、[Cluster] オプションボタンをクリックします。
- f) [OK] をクリックします。

[Provisioning - device name] ウィンドウが表示されます。デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

初期ブートストラップ設定を設定できるダイアログボックスが表示されます。これらの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [Cluster Information] ページで、次の手順を実行します。

The screenshot shows the 'Cisco: Adaptive Security Appliance - Bootstrap Configuration' dialog box with the 'Cluster Information' tab selected. The 'Settings' sub-tab is also active. The 'Security Module' section contains a text box with 'Security Module-1, Security Module-2, Security Module-3'. The 'Interface Information' section includes fields for Chassis ID (1), Site ID (1), Cluster Key (masked with dots), Confirm Cluster Key (masked with dots), Cluster Group Name (asa_cluster), Management Interface (Ethernet1/4), and CCL Subnet IP (Eg:x.x.0.0). The 'DEFAULT' section has an Address Type dropdown set to 'IPv4 only'. The 'IPv4' section includes fields for Management IP Pool (10.89.5.10 - 10.89.5.22), Virtual IPv4 Address (10.89.5.25), Network Mask (255.255.255.192), and Network Gateway (10.89.5.1). At the bottom are 'OK' and 'Cancel' buttons.

- a) [Cluster Key] フィールドで、クラスタ制御リンクの制御トラフィックの認証キーを設定します。
- 共有秘密は、1～63文字のASCII文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。
- b) [Cluster Group Name] を設定します。これは、論理デバイス設定のクラスタグループ名です。
- 名前は1～38文字のASCII文字列である必要があります。
- c) [Management Interface] を選択します。
- このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。
- d) 管理インターフェイスの [Address Type] を選択します。
- この情報は、ASA設定で管理インターフェイスを設定するために使用されます。次の情報を設定します。
- [Management IP Pool] : 開始アドレスと終了アドレスをハイフンで区切って入力し、ローカルIPアドレスのプールを設定します。このうちの1つがインターフェイス用に各クラスタユニットに割り当てられます。
- 最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300の場合、すべてのモジュールスロットが埋まっていないとしても、シャーシごとに3つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のマスターユニットに属する仮想IPアドレス（メインクラスタIPアドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークのIPアドレスの1つをメインクラスタIPアドレス用に確保してください。IPv4アドレスとIPv6アドレス（どちらか一方も可）を使用できます。
- ネットワーク マスクまたはプレフィックス長
 - ネットワーク ゲートウェイ
 - [VIRTUAL IP address] : 現在のマスターユニットの管理IPアドレスを設定します。このIPアドレスは、クラスタプールアドレスと同じネットワーク上に存在している必要がありますが、プールに含まれてはいけません。

ステップ 6 [Settings] ページで、以下を実行します。

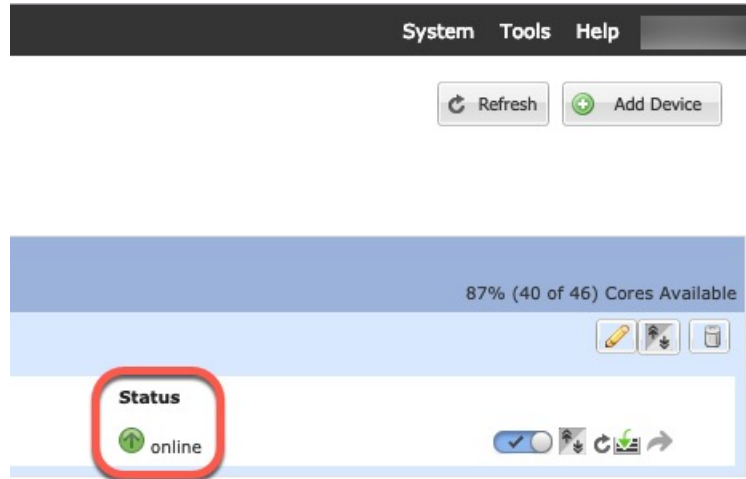
- a) 管理者ユーザの [Password] を入力して確認します。

事前設定されているASA管理者ユーザはパスワードの回復時に役立ちます。FXOSアクセスができる場合、管理者ユーザパスワードを忘れたときにリセットできます。

ステップ 7 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[論理デバイス (Logical Devices)] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。

**ステップ 9** マスター ユニット ASA に接続して、クラスタリング設定をカスタマイズします。

ASA : ファイアウォール モードとコンテキスト モードの変更

デフォルトでは、FXOS シャーシはルーテッドまたはトランスペアレント ファイアウォール モード、およびシングル コンテキスト モードでクラスタを展開します。

- **ファイアウォール モードの変更** : 展開後にモードを変更するには、マスター ユニットでモードを変更します。モードは一致するようにすべてのスレーブユニットで自動的に変更されます。を参照してください。 [ファイアウォール モード \(シングルモード\) の設定 \(216 ページ\)](#) マルチ コンテキスト モードでは、コンテキストごとにファイアウォールモードを設定します。 [セキュリティ コンテキストの設定 \(258 ページ\)](#) を参照してください。
- **マルチ コンテキスト モードに変更** : 展開後にマルチ コンテキスト モードに変更するには、マスター ユニットのモードを変更します。これにより、すべてのスレーブユニットのモードは一致するように自動的に変更されます。 [マルチ コンテキスト モードの有効化 \(254 ページ\)](#) を参照してください。

ASA : データ インターフェイスの設定

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。シャーシ間クラスタリングの場合、データ インターフェイスは常にスパンド EtherChannel インターフェイスです。



- (注) 管理インターフェイスは、クラスタを展開したときに事前設定されました。ASA で管理インターフェイス パラメータを変更することもできますが、この手順はデータ インターフェイスに焦点を当てています。管理インターフェイスは、スパンドインターフェイスとは対照的に、個別のインターフェイスです。詳細については、「[管理インターフェイス \(424 ページ\)](#)」を参照してください。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。
- シャーシ間クラスタリングにスパンド EtherChannel を使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

- ステップ 1** コンテキスト モードによって次のように異なります。
- シングル モードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
 - マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。
- ステップ 2** インターフェイスを選択して、[Edit] をクリックします。
[Edit Interface] ダイアログボックスが表示されます。
- ステップ 3** 次の設定を行います。
- (EtherChannel の場合) [MIO Port-channel ID] : FXOS で使用されるのと同じ ID を入力します。
 - **[Enable Interface]** (デフォルトでオンになります)
- この画面の残りのフィールドは、この手順の後半で説明します。
- ステップ 4** MAC アドレスおよびオプション パラメータを設定するには、[Advanced] タブをクリックします。

- [MAC Address Cloning] 領域で、EtherChannel の手動グローバル MAC アドレスを設定します。スタンバイ MAC アドレスを設定しないでください。無視されます。潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel にはグローバル MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在のマスター ユニットに留まります。MAC アドレスを設定していない場合に、マスター ユニットが変更された場合、新しいマスター ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

マルチコンテキストモードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

- ステップ 5** (オプション) この EtherChannel に VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。
- ステップ 6** (マルチ コンテキスト モード) この手順を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。
- a) [OK] をクリックして変更内容を確定します。
 - b) インターフェイスを割り当てます。
 - c) ユーザが設定するコンテキストを変更します。[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
 - d) [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択し、カスタマイズするポートチャネルインターフェイスを選択して、[Edit] をクリックします。
- [Edit Interface] ダイアログボックスが表示されます。
- ステップ 7** [General] タブをクリックします。
- ステップ 8** (トランスペアレント モード) [Bridge Group] ドロップダウンリストから、このインターフェイスを割り当てるブリッジグループを選択します。
- ステップ 9** [Interface Name] フィールドに、名前を 48 文字以内で入力します。
- ステップ 10** [Security level] フィールドに、0 (最低) ~ 100 (最高) のレベルを入力します。
- ステップ 11** (ルーテッドモード) IPv4 アドレスに対して [Use Static IP] オプションボタンをクリックし、IP およびマスクを入力します。DHCP と PPPoE はサポートされません。トランスペアレントモードの場合は、EtherChannel インターフェイスではなく、ブリッジグループインターフェイスの IP アドレスを設定します。
- ステップ 12** (ルーテッドモード) IPv6 アドレスを設定するには、[IPv6] タブをクリックします。
- トランスペアレントモードの場合は、EtherChannel インターフェイスではなく、ブリッジグループインターフェイスの IP アドレスを設定します。
- a) [Enable IPv6] チェックボックスをオンにします。
 - b) [Interface IPv6 Addresses] エリアで、[Add] をクリックします。
- [Add IPv6 Address for Interface] ダイアログボックスが表示されます。

(注) [Enable address autoconfiguration] オプションはサポートされません。

- c) [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、2001:DB8::BA98:0:3210/64。
- d) (オプション) ホストアドレスとして Modified EUI-64 インターフェイス ID を使用するには、[EUI-64] チェックボックスをオンにします。この場合は、単に [Address/Prefix Length] フィールドにプレフィックスを入力します。
- e) [OK] をクリックします。

ステップ 13 [OK] をクリックして、[Interfaces] 画面に戻ります。

ステップ 14 [Apply] をクリックします。

ASA : クラスタ設定のカスタマイズ

クラスタを展開した後にブートストラップ設定を変更する場合や、クラスタリングヘルスマニタリング、TCP 接続複製の遅延、フローモビリティ、およびその他の最適化など、追加のオプションを設定する場合は、マスターユニットで行うことができます。

ASA クラスタの基本パラメータの設定

マスターユニット上のクラスタ設定をカスタマイズできます。

始める前に

- マルチコンテキストモードでは、マスターユニット上のシステム実行スペースで次の手順を実行します。まだシステムコンフィギュレーションモードに入っていない場合、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある **[System]** をダブルクリックします。
- **local-unit Member Name** およびその他の複数のオプションは、FXOS シャーシでのみ設定することができます。また、それらのオプションは、クラスタリングを無効にしている場合に ASA でのみ変更できます。そのため、次の手順には含まれていません。

手順

ステップ 1 **[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]** の順に選択します。

ステップ 2 (任意) 次のオプションパラメータを設定します。

- **[Enable connection rebalancing for TCP traffic across all the ASAs in the cluster]** : 接続の再分散をイネーブルにします。このパラメータはデフォルトではディセーブルになっています。イネーブルの場合は、クラスタの ASA は定期的に負荷情報を交換し、負荷のかかっているデバイスから負荷の少ないデバイスに新しい接続をオフロードします。負荷情報を交換する間隔を、1 ~ 360 秒の範囲内で指定します。このパラメータは、ブートストラップコ

ンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

- **[Enable health monitoring of this device within the cluster]** : クラスタユニットのヘルスチェック機能を有効にして、ユニット キープアライブ ステータス メッセージ間の間隔を .8 から 45 秒の間で設定します。デフォルトは 3 秒です。**注** : 新しいユニットをクラスタに追加していて、ASA またはスイッチのトポロジが変更される場合、クラスタが完成するまでこの機能を一時的にディセーブルにし、ディセーブルにされたインターフェイスのインターフェイス モニタリングもディセーブルにする必要があります (**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]**)。クラスタとトポロジの変更が完了したら、この機能を再度イネーブルにすることができます。ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにキープアライブ メッセージを送信します。ユニットが保留時間内にピア ユニットからキープアライブ メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。
- **[Replicate console output to the master's console]** : スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力する場合があります。コンソール複製をイネーブルにすると、スレーブ ユニットからマスター ユニットにコンソール メッセージが送信されるので、モニタが必要になるのはクラスタのコンソール ポート 1 つだけとなります。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

ステップ 3 **[Cluster Control Link]** 領域で、クラスタ制御リンクの MTU を設定できます。この領域のその他のオプションは、ASA では設定できません。

- **[MTU]** : クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。MTU の最大値を 9000 バイトに設定し、最小値を 1400 バイトに設定することをお勧めします。

ステップ 4 (任意) **[Cluster LACP]** 領域で、スタティック ポートの優先順位を有効にできます。ASA は cLACP を使用して、EtherChannel とネイバースイッチのネゴシエーションを行います。cLACP ネゴシエーションの際に、同じクラスタ内の ASA は互いに連携するため、スイッチには 1 つの (仮想) デバイスであるかのように見えます。この領域のその他のオプションは、クラスタリングを無効化せずに、ASA では設定できません。

- **[Enable static port priority]** : LACP のダイナミック ポートプライオリティをディセーブルにします。一部のスイッチはダイナミック ポートプライオリティをサポートしていないので、このパラメータによりスイッチの互換性が向上します。さらに、8 個より多くのアクティブなスバンド EtherChannel メンバのサポートがイネーブルになります (最大 32 メンバ)。このパラメータを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このパラメータをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

ステップ5 [Apply] をクリックします。

インターフェイスのヘルス モニタリングの設定

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ポートチャネル ID、または単一の物理インターフェイス ID をモニタできます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring] の順に選択します。

ステップ2 [Monitored Interfaces] ボックスでインターフェイスを選択し、[Add] をクリックしてそのインターフェイスを [Unmonitored Interfaces] ボックスに移動します。

インターフェイス ステータス メッセージによって、リンク障害が検出されます。特定の論理インターフェイスのすべての物理ポートが、特定のユニット上では障害が発生したが、別のユニット上の同じ論理インターフェイスでアクティブポートがある場合、そのユニットはクラスタから削除されます。ユニットがホールド時間内にインターフェイス ステータス メッセージを受信しない場合に、ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ポートチャネル ID、または単一の物理インターフェイス ID を指定できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ASA、Firepower 9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルス チェック機能を無効にし（[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]）、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルスチェック機能を再度イネーブルにできます。

ステップ3 [Apply] をクリックします。

クラスタ TCP 複製の遅延の設定

TCP 接続のクラスタ複製の遅延を有効化して、ディレクタ/バックアップフロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。ディレクタ/バックアップフローが作成される前にユニットが失敗する場合は、それらのフローを回復することはできません。同様に、フローを作成する前にトラフィックが別のユニットに再調整される場合、流れを回復することはできません。TCP のランダム化を無効化するトラフィックの TCP の複製の遅延を有効化しないようにする必要があります。

手順

ステップ 1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication] の順に選択します。

ステップ 2 [Add] をクリックして次の値を設定します。

- [Replication delay] : 1 ~ 15 の範囲で秒数を設定します。
- [HTTP] : すべての HTTP トラフィックの遅延を設定します。デフォルトでは、この設定は 5 秒間で有効化されています。
- [Source Criteria]
 - [Source] : 送信元 IP アドレスを設定します。
 - [Service] : (オプション) 送信元ポートを設定します。通常は、送信元または宛先ポートのいずれかを設定するか、両方ともに設定しません。
- [Destination Criteria]
 - [Source] : 宛先 IP アドレスを設定します。
 - [Service] : (オプション) 宛先ポートを設定します。通常は、送信元または宛先ポートのいずれかを設定するか、両方ともに設定しません。

ステップ 3 [OK] をクリックします。

ステップ 4 [Apply] をクリックします。

FXOS : クラスタ メンバの削除

ここでは、メンバを一時的に、またはクラスタから永続的に削除する方法について説明します。

一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因で、クラスタメンバはクラスタから自動的に削除されます。この削除は、条件が修正されるまでの一時的なものであるため、クラスタに再参加できます。また、手動でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内にあるかどうかを確認するには、Firepower Chassis Manager の [Logical Devices] ページで、のクラスタ ステータスを確認します。

Management Port	Status
Ethernet1/4	online


Attributes

Cluster Operational Status : not-in-cluster
 FIREPOWER-MGMT-IP : 10.89.5.20
 CLUSTER-ROLE : none
 CLUSTER-IP : 127.2.1.1
 MGMT-URL : https://10.89.5.35/
 UUID : 8e459170-451d-11e9-8475-f22f06c32630

- アプリケーションでのクラスタリングの無効化 : アプリケーション CLI を使用してクラスタリングを無効にすることができます。 **cluster remove unit name** コマンドを入力して、ログインしているユニット以外のすべてのユニットを削除します。ブートストラップ コンフィギュレーションは変更されず、マスターユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスターユニットを削除するためにスレーブユニットでこのコマンドを入力した場合は、新しいマスターユニットが選定されます。

デバイスが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。

クラスタリングを再度有効にするには、ASA で **cluster group name** を入力してから **enable** を入力します。

- アプリケーション インスタンスの無効化 : Firepower Chassis Manager の [Logical Devices] ページでスライダの無効化 () をクリックします。[Enable] スライダ () を使用して後で再度有効にすることができます。
- セキュリティ モジュール/エンジンのシャットダウン : Firepower Chassis Manager の [Module/Engine] ページで、[Power Off] アイコン () をクリックします。
- シャーシのシャットダウン : Firepower Chassis Manager の [Overview] ページで、[Shut Down] アイコン () をクリックします。

完全な削除

次の方法を使用して、クラスタメンバを完全に削除できます。

- 論理デバイスの削除：Firepower Chassis Manager の [Logical Devices] ページで、[Delete] アイコン (🗑️) をクリックします。その後、スタンドアロンの論理デバイスや新しいクラスタを展開したり、同じクラスタに新しい論理デバイスを追加したりすることもできます。
- サービスからのシャーシまたはセキュリティモジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

ASA : クラスタメンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタメンバを管理できます。

非アクティブなメンバーになる

クラスタの非アクティブなメンバーになるには、クラスタリングコンフィギュレーションは変更せずに、そのユニット上でクラスタリングをディセーブルにします。



- (注) ASA が (手動で、またはヘルスチェックエラーにより) 非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのユニットをクラスタから完全に削除します。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合 (クラスタリングが無効な状態で設定を保存した場合など)、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

- ステップ 1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] の順に選択します。

ステップ2 [Participate in ASA cluster] チェックボックスをオフにします。

(注) [Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソールポートで CLI にアクセスする必要があります。

ステップ3 [Apply] をクリックします。

マスターユニットからのスレーブメンバーの非アクティブ化

スレーブメンバを非アクティブにするには、次のステップを実行します。



(注) ASA が非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーションモードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] の順に選択します。

ステップ2 削除するスレーブを選択して [Delete] をクリックします。

スレーブ ブートストラップ コンフィギュレーションは同じであり、その設定を失うことなく以後スレーブを再追加できます。

ステップ3 [Apply] をクリックします。

クラスタへの再参加

ユニットがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルするには、コンソール ポートを使用する必要があります。他のインターフェイスはシャットダウンされます。ただし、ASDMでクラスタリングを手動で無効にした場合、設定を保存してリロードしなかった場合は、ASDMでクラスタリングを再び有効にできます。リロード後、管理インターフェイスは無効になるため、コンソール アクセスがクラスタリングを再び有効にする唯一の方法です。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

ステップ 1 ASDM にまだアクセスしている場合は、再イネーブル化するユニットに ASDM を接続して、ASDM でクラスタリングを再び有効にすることができます。

新しいメンバーとして追加していない限り、スレーブ ユニットのクラスタリングをマスター ユニットから再び有効にすることはできません。

- a) [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] の順に選択します。
- b) [Participate in ASA cluster] チェックボックスをオンにします。
- c) [Apply] をクリックします。

ステップ 2 ASDM を使用できない場合：コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group name

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 3 クラスタリングをイネーブルにします。

enable

マスターユニットの変更



注意 マスターユニットを変更する最良の方法は、マスターユニットでクラスタリングを無効にし、新しいマスターの選択を待ってから、クラスタリングを再度有効にする方法です。マスターにするユニットを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用してマスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

マスターユニットを変更するには、次の手順を実行します。

始める前に

マルチコンテキストモードの場合は、この手順をシステム実行スペースで実行します。まだシステムコンフィギュレーションモードに入っていない場合は、[Configuration]>[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

- ステップ 1 [Monitoring]>[ASA Cluster]>[Cluster Summary] を選択します。
- ステップ 2 [Change Master To] ドロップダウンリストから、マスターにするスレーブユニットを選択し、[Make Master] をクリックします。
- ステップ 3 マスターユニット変更の確認を求められます。[Yes] をクリックします。
- ステップ 4 ASDM を終了し、メインクラスタ IP アドレスを使用して再接続します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのメンバに、または特定のメンバに送信するには、次の手順を実行します。**show** コマンドをすべてのメンバーに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。（または、マスターユニットで **show** コマンドを入力するとクラスタ全体の統計情報を表示できます。）**capture** や **copy** などのその他のコマンドも、クラスタ全体での実行を活用できます。

始める前に

コマンドラインインターフェイス ツールでこの手順を実行します。[Tools]>[Command Line Interface] を選択します。

手順

コマンドをすべてのメンバに送信します。ユニット名を指定した場合は、特定のメンバに送信されます。

cluster exec [unit *unit_name*] コマンド

例 :

```
cluster exec show xlate
```

メンバー名を表示するには、**cluster exec unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。

例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで次のコマンドを入力します。

```
cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから1つずつ）が TFTP サーバにコピーされます。宛先のキャプチャファイル名には自動的にユニット名が付加され、**capture1_asa1.pcap**、**capture1_asa2.pcap** などとなります。この例では、**asa1** および **asa2** がクラスタユニット名です。

次の **cluster exec show memory** コマンドの出力例では、クラスタの各メンバーのメモリ情報が表示されています。

```
cluster exec show memory
unit-1-1 (LOCAL) :*****
Free memory:      108724634538 bytes (92%)
Used memory:      9410087158 bytes ( 8%)
-----
Total memory:     118111600640 bytes (100%)

unit-1-3:*****
Free memory:      108749922170 bytes (92%)
Used memory:      9371097334 bytes ( 8%)
-----
Total memory:     118111600640 bytes (100%)

unit-1-2:*****
Free memory:      108426753537 bytes (92%)
Used memory:      9697869087 bytes ( 8%)
-----
Total memory:     118111600640 bytes (100%)
```

ASA : での ASA クラスタのモニタリング Firepower 9300 シャーシ

クラスタの状態と接続をモニタおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [Cluster Summary]**

このペインには、接続相手のユニットとクラスタのその他のユニットの情報が表示されます。また、このペインでプライマリ装置を変更することができます。

- **[Cluster Dashboard]**

プライマリ装置のホームページの **[Cluster Dashboard]** と **[Cluster Firewall Dashboard]** を使用してクラスタをモニタできます。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次の画面を参照してください。

- **[Wizards] > [Packet Capture Wizard]**

クラスタ全体のトラブルシューティングをサポートするには、マスターユニット上でのクラスタ固有トラフィックのキャプチャをイネーブルにします。これで、クラスタ内のすべてのスレーブユニットでも自動的にイネーブルになります。

クラスタ リソースのモニタリング

クラスタ リソースのモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [System Resources Graphs] > [CPU]**

このペインでは、クラスタ メンバ全体の CPU 使用率を示すグラフまたはテーブルを作成することができます。

- **[Monitoring] > [ASA Cluster] > [System Resources Graphs] > [Memory]**

このペインでは、クラスタ メンバ全体の **[Free Memory]** と **[Used Memory]** を表示するグラフまたはテーブルを作成することができます。

クラスタ トラフィックのモニタリング

クラスタ トラフィックのモニタリングについては、次の画面を参照してください。

- [Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Connections]。

このペインでは、クラスタメンバ全体の接続を示すグラフまたはテーブルを作成することができます。

- [Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Throughput]。

このペインでは、クラスタメンバ全体のトラフィックのスループットを示すグラフまたはテーブルを作成することができます。

クラスタ制御リンクのモニタリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

[Monitoring] > [Properties] > [System Resources Graphs] > [Cluster Control Link]。

このペインでは、クラスタ制御リンクの [Receival] および [Transmittal] 容量使用率を表示するグラフまたはテーブルを作成することができます。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次の画面を参照してください。

[Configuration] > [Device Management] > [Logging] > [Syslog Setup]

クラスタ内の各ユニットは、syslog メッセージを個別に生成します。同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合した場合、期待できる合計クラスタパフォーマンスの概算値は次のようになります。

- TCP または CPS の合計スループットの 80 %
- UDP の合計スループットの 90 %
- トラフィックの混在に応じて、イーサネット MIX (EMIX) の合計スループットの 60 %。

たとえば、TCP スループットについては、3つのモジュールを備えた Firepower 9300 は、単独で動作している場合、約 135 Gbps の実際のファイアウォールトラフィックを処理できます。2シャーシの場合、最大スループットの合計は 270 Gbps (2 シャーシ X 135 Gbps) の約 80 %、つまり 216 Gbps です。

マスターユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. クラスタを展開すると、各ユニットは選定要求を3秒ごとにブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。
3. 45秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。
4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスターユニットになることはありません。既存のマスターユニットは常にマスターのままです。ただし、マスターユニットが応答を停止すると、その時点で新しいマスターユニットが選定されます。



(注) 特定のユニットを手動で強制的にマスターにすることができます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

クラスタ内のハイアベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイアベイラビリティを提供します。

シャーシアプリケーションのモニタリング

シャーシアプリケーションのヘルスモニタリングは常に有効になっています。Firepower 9300 シャーシスーパーバイザはASAアプリケーションを定期的に確認します（毎秒）。ASAが作動中で、Firepower 9300 シャーシスーパーバイザと3秒間通信できなければASAはsyslogメッセージを生成して、クラスタを離れます。

Firepower 9300 シャーシスーパーバイザが45秒後にアプリケーションと通信できなければ、ASAをリロードします。ASAがスーパーバイザと通信できなければ、自身をクラスタから削除します。

ユニットのヘルスモニタリング

マスターユニットは、各スレーブユニットをモニタするために、クラスタ制御リンクを介してキープアライブメッセージを定期的に送信します（間隔は設定可能です）。各スレーブユニットは、同じメカニズムを使用してマスターユニットをモニタします。ユニットの健全性チェックが失敗すると、ユニットはクラスタから削除されます。

インターフェイス モニタリング

各ユニットは、使用中のすべてのハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をマスターユニットに報告します。ヘルス モニタリングを有効にすると、デフォルトではすべての物理インターフェイスがモニタされます (EtherChannel インターフェイスのメイン EtherChannel を含む)。アップ状態の指名されたインターフェイスのみモニタできます。たとえば、名前付き EtherChannel がクラスタから削除される前に、EtherChannel のすべてのメンバー ポートがエラーとなる必要があります (最小ポート バンドル設定に基づく)。ヘルスチェックは、インターフェイスごとに、モニタリングをオプションで無効にすることができます。

あるモニタ対象のインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。ASA がメンバーをクラスタから削除するまでの時間は、そのユニットが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。ASA は、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。設定済みのメンバーの場合は、500 ミリ秒後にユニットが削除されます。

障害後のステータス

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィックフローのステート情報は、クラスタ制御リンクを介して共有されます。

マスターユニットで障害が発生した場合は、そのクラスタの他のメンバーのうち、プライオリティが最高 (番号が最小) のものがマスターユニットになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。



- (注) ASA が非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはディセーブルになります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタメンバがクラスタから削除された後、クラスタに再参加できる方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決した後、と入力して、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。

- データインターフェースの障害：ASAは自動的に最初は5分後、次に10分後、最終的に20分後に再参加を試みます。20分後に参加できない場合、ASAはクラスタリングをディセーブルにします。データインターフェースの問題を解決した後、と入力して、クラスタリングを手動でイネーブルにする必要があります。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。ユニットは5秒ごとにクラスタへの再参加を試みます。
- シャーシアプリケーション通信の障害：ASAがシャーシアプリケーションの状態が回復したことを検出すると、ASAは自動的にクラスタの再参加を試みます。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーションステータスなどがあります。問題を解決したら、クラスタリングを再び有効にして、クラスタに手動で再参加する必要があります。

データパス接続状態の複製

どの接続にも、1つのオーナーおよび少なくとも1つのバックアップオーナーがクラスタ内にあります。バックアップオーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDPのステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップオーナーは通常ディレクタでもありません。

トラフィックの中には、TCPまたはUDPレイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 18: クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システムアップタイムをトラッキングします。
ARP Table	Yes	トランスペアレントモードのみ。
MAC アドレス テーブル	Yes	トランスペアレントモードのみ。
ユーザ アイデンティティ	Yes	AAA ルール (uauth) とアイデンティティ ファイアウォールが含まれます。
IPv6 ネイバー データベース	Yes	—
ダイナミック ルーティング	Yes	—

Traffic	状態のサポート	注意
SNMP エンジン ID	なし	—
集中型 VPN (サイト間)	なし	VPN セッションは、マスターユニットで障害が発生すると切断されます。

クラスタが接続を管理する方法

接続をクラスタの複数のメンバにロードバランスできます。接続のルールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のルール

接続ごとに定義された次のルールを参照してください。

- **オーナー**：通常、最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1つの接続に対してオーナーは1つだけです。元のオーナーに障害が発生すると、新しいユニットが接続からパケットを受信したときにディレクタがこれらのユニットの新しいオーナーを選択します。
- **バックアップ オーナー**：オーナーから受信した TCP/UDP ステート情報を格納するユニット。これにより、障害が発生した場合に新しいオーナーにシームレスに接続を転送できます。バックアップ オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロードバランシングに基づく）がバックアップ オーナーに問い合わせ、関連するステート情報を取得し、これでそのユニットが新しいオーナーになることができます。

ディレクタ（下記参照）がオーナーと同じユニットでない限り、ディレクタはバックアップオーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップオーナーが選択されます。

- **ディレクタ**：フォワーダからのオーナーバックアップ要求を処理するユニット。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニットはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

ディレクタがオーナーと同じユニットでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップオーナーが選択されます。

- **フォワーダ**：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせ、そのオーナーへのフローを確立します。これは、この接続

に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化をディセーブルにした場合は、SYN Cookie は使用されないの、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえば DNS や ICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

接続でポート アドレス変換 (PAT) を使用すると、PAT のタイプ (per-session または multi-session) が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- **Per-session PAT** : オーナーは、接続の最初のパケットを受信するユニットです。
デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。
- **Multi-session PAT** : オーナーは常にマスターユニットです。multi-session PAT 接続がスレーブユニットで最初に受信される場合、スレーブユニットはその接続をマスターユニットに転送します。

デフォルトでは、UDP (DNS UDP を除く) および ICMP トラフィックは multi-session PAT を使用するの、これらの接続は常にマスターユニットによって所有されています。

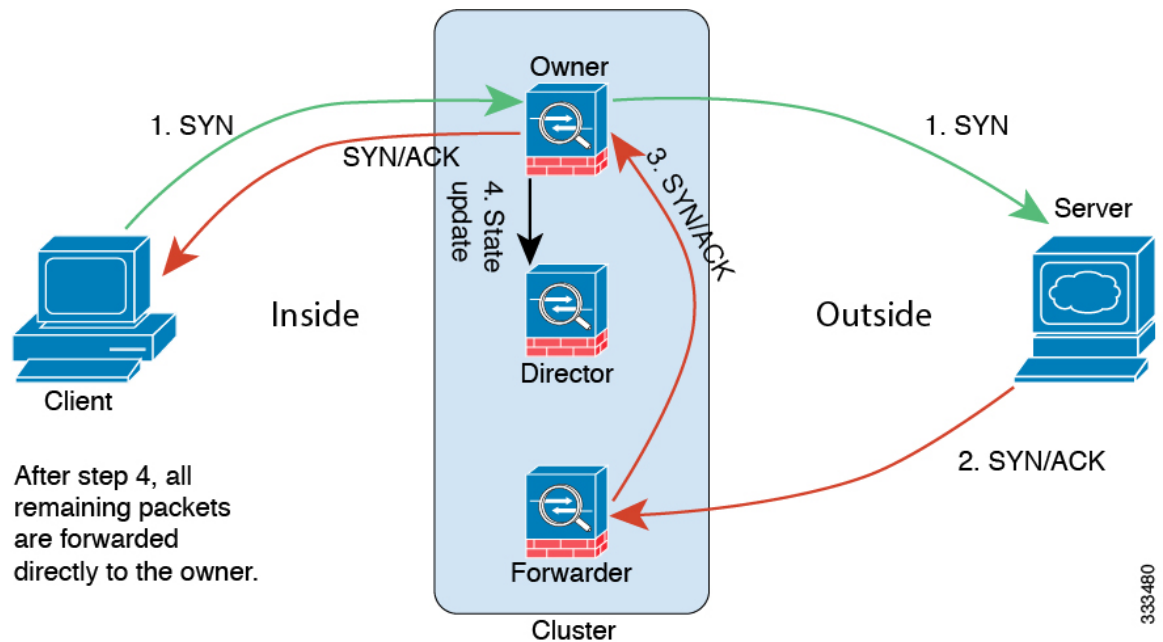
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーユニットに転送されます。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

サンプル データ フロー

次の例は、新しい接続の確立を示します。



1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロードバランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせ、オーナーを特定し、フローを確立します。
8. フローの状態が変化した場合、状態アップデートがオーナーからディレクタに送信されます。

Firepower 9300 シャーシ上の ASA クラスタリングの履歴

機能名	バージョン	機能情報
Firepower 9300 用 シャーシ内 ASA クラ スタリング	9.4 (1150)	FirePOWER 9300 シャーシ内では、最大 3 つセキュリティ モジュールをクラスタ化できません。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次の画面を導入しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]



第 III 部

インターフェイス

- [基本的なインターフェイス設定 \(463 ページ\)](#)
- [EtherChannel インターフェイスと冗長インターフェイス \(475 ページ\)](#)
- [VLAN サブインターフェイス \(493 ページ\)](#)
- [VXLAN インターフェイス \(499 ページ\)](#)
- [ルーテッドモードインターフェイスとトランスペアレントモードインターフェイス \(513 ページ\)](#)
- [高度なインターフェイス設定 \(539 ページ\)](#)
- [トラフィックゾーン \(551 ページ\)](#)



第 13 章

基本的なインターフェイス設定

この章では、イーサネット設定、ジャンボフレーム設定などの基本インターフェイス設定について説明します。



(注) マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。まだシステム実行スペースに入っていない場合は、[Configuration] > [Device List] ペイン内で、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。



(注) ASA サービス モジュール インターフェイスについては、[『ASA Services Module quick start guide』](#) を参照してください。

Firepower 9300 シャーシでは、FXOS オペレーティング システムで基本的なインターフェイス設定を行います。詳細については、お使いのシャーシの設定または導入ガイドを参照してください。

- [基本的なインターフェイス設定について \(463 ページ\)](#)
- [基本インターフェイスの設定のライセンス \(467 ページ\)](#)
- [基本インターフェイスの設定のガイドライン \(467 ページ\)](#)
- [基本インターフェイスのデフォルト設定 \(468 ページ\)](#)
- [物理インターフェイスのイネーブル化およびイーサネットパラメータの設定 \(469 ページ\)](#)
- [ジャンボ フレーム サポートの有効化 \(471 ページ\)](#)
- [基本インターフェイスの例 \(472 ページ\)](#)
- [基本インターフェイスの設定の履歴 \(473 ページ\)](#)

基本的なインターフェイス設定について

この項では、インターフェイスの機能と特殊なインターフェイスについて説明します。

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーションフェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロスケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。ギガビットイーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

管理インターフェイス

管理インターフェイスは、使用しているモデルに応じて、管理トラフィック専用の個別インターフェイスとなります。

管理インターフェイスの概要

次のインターフェイスに接続して ASA を管理できます。

- 任意の通過トラフィック インターフェイス
- 専用の管理スロット/ポート インターフェイス（使用しているモデルで使用できる場合）

[管理アクセス（885ページ）](#) の説明に従って、管理アクセスへのインターフェイスを設定する必要がある場合があります。

管理スロット/ポート インターフェイス

次の表に、モデルごとの管理インターフェイスを示します。

表 19: モデルごとの管理インターフェイス

モデル	管理 0/0	管理 0/1	管理 1/0	管理 1/1	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
Firepower 9300	該当なし インターフェイス ID は ASA 論理デバイスに割り当てた物理 mgmt タイプ インターフェイスに基づいています。	—	—	—	—	○

モデル	管理 0/0	管理 0/1	管理 1/0	管理 1/1	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
ASA 5506-X	—	—	—	○	—	—
ASA 5508-X	—	—	—	○	—	—
ASA 5512-X	○	—	—	—	—	—
ASA 5515-X	○	—	—	—	—	—
ASA 5516-X	—	—	—	○	—	—
ASA 5525-X	○	—	—	—	—	—
ASA 5545-X	○	—	—	—	—	—
ASA 5555-X	○	—	—	—	—	—
ASA 5585-X	○	○	○ SSP をスロット 1 に設置した場合は、 Management 1/0 および 1/1 ではスロット 1 の SSP への管理アクセスのみが提供されます。	○	○	○
ISA 3000	—	—	—	○	—	—
ASASM	—	—	—	—	—	—
ASAv	○	—	—	—	—	—



(注) モジュールをインストールした場合は、モジュール管理インターフェイスでは、モジュールの管理アクセスのみが提供されます。ソフトウェア モジュールを搭載したモデルでは、ソフトウェア モジュールによって ASA と同じ物理管理インターフェイスが使用されます。

管理専用トラフィックに対する任意のインターフェイスの使用

任意のインターフェイスを、管理トラフィック用として設定することによって管理専用インターフェイスとして使用できます。これには、EtherChannel インターフェイスも含まれます。

トランスペアレントモードの管理インターフェイス

トランスペアレントファイアウォールモードでは、許可される最大通過トラフィックインターフェイスに加えて、管理インターフェイス（物理インターフェイス、サブインターフェイス（使用しているモデルでサポートされている場合）、管理インターフェイスからなるEtherChannelインターフェイス（複数の管理インターフェイスがある場合）のいずれか）を個別の管理インターフェイスとして使用できます。他のインターフェイスタイプは管理インターフェイスとして使用できません。Firepower 9300 シャーシでは、管理インターフェイス ID は ASA 論理デバイスに割り当てた `mgmt-type` インターフェイスに基づいています。

マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。コンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイスを各コンテキストに割り当てます。ASA 5555-X 以前では、管理インターフェイスのサブインターフェイスは許可されないため、コンテキスト単位で管理を行うには、データインターフェイスに接続する必要があります。

管理インターフェイスは、通常のブリッジグループの一部ではありません。動作上の目的から、設定できないブリッジグループの一部です。



- (注) トランスペアレントファイアウォールモードでは、管理インターフェイスによってデータインターフェイスと同じ方法でMACアドレステーブルがアップデートされます。したがって、いずれかのスイッチポートをルーテッドポートとして設定しない限り、管理インターフェイスおよびデータインターフェイスを同じスイッチに接続しないでください（デフォルトでは、Catalyst スイッチがすべてのVLANスイッチポートのMACアドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASAによって、データインターフェイスではなく、管理インターフェイスを使用してスイッチにアクセスするようにMACアドレステーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも30秒間は、スイッチからデータインターフェイスへのパケットのためにMACアドレステーブルがASAによって再アップデートされることはありません。

冗長管理インターフェイスの非サポート

冗長インターフェイスは、`Management slot/port` インターフェイスをメンバとしてサポートしません。ただし、管理インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

ASA モデルの管理インターフェイスの特性

ASA 5585-X を除く ASA 5500-X モデルの管理インターフェイスには、次の特性があります。

- 通過トラフィックはサポートされません。
- サブインターフェイスはサポートされません
- プライオリティ キューはサポートされません

- マルチキャスト MAC はサポートされません
- ソフトウェア モジュールは、管理インターフェイスを共有します。ASA とモジュールに対して、別の MAC アドレスと IP アドレスがサポートされます。モジュールのオペレーティング システムでモジュールの IP アドレスのコンフィギュレーションを実行する必要があります。ただし、物理特性（インターフェイスの有効化など）は、ASA 上で設定されます。

基本インターフェイスの設定のライセンス

モデル	ライセンス要件
ASA 5585-X	SSP-10 および SSP-20 のインターフェイス速度： <ul style="list-style-type: none"> • 基本ライセンス：ファイバインターフェイスの場合 1 ギガビットイーサネット • 10 GE I/O ライセンス（Security Plus）：ファイバインターフェイスの場合 10 ギガビットイーサネット • （SSP-40 および SSP-60 は 10 ギガビットイーサネットをデフォルトでサポートします）。

基本インターフェイスの設定のガイドライン

トランスペアレント ファイアウォール モード

マルチコンテキストのトランスペアレントモードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。

フェールオーバー

データインターフェイスと、フェールオーバーまたはステートのインターフェイスを共有することはできません。

その他のガイドライン

一部の管理関連のサービスは、管理対象外のインターフェイスが有効になり、ASA が「システム レディ」状態になるまで使用できません。ASA が「System Ready」状態になると、次の syslog メッセージを生成します。

```
%ASA-6-199002: Startup completed. Beginning operation.
```

基本インターフェイスのデフォルト設定

この項では、工場出荷時のデフォルトコンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- VLAN サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- VXLAN VNI インターフェイス：イネーブル。
- EtherChannel ポートチャネルインターフェイス（ASA モデル）：イネーブル。ただし、トラフィックが EtherChannel を通過するためには、チャンネルグループ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネルインターフェイス（Firepower モデル）：ディセーブル。



(注) Firepower 9300 の場合、管理上、シャーシおよび ASA の両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシと ASA の間の不一致が生じることがあります。

デフォルトの速度および二重通信

- デフォルトでは、銅線（RJ-45）インターフェイスの速度とデュプレックスは、オートネゴシエーションに設定されます。
- 5585-X のファイバインターフェイスでは、自動リンク ネゴシエーションの速度が設定されます。

デフォルトのコネクタタイプ

2つのコネクタタイプ（copper RJ-45 と fiber SFP）を持つモデルもあります。RJ-45 がデフォルトです。ASA にファイバ SFP コネクタを使用するように設定できます。

デフォルトの MAC アドレス

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

物理インターフェイスのイネーブル化およびイーサネットパラメータの設定

ここでは、次の方法について説明します。

- 物理インターフェイスをイネーブルにする。
- 特定の速度と二重通信（使用できる場合）を設定する。
- フロー制御のポーズフレームをイネーブルにする。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある **[System]** をダブルクリックします。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、**[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]** ペインを選択します。
- マルチ モードの場合、システム実行スペースで、**[Configuration] > [Context Management] > [Interfaces]** ペインを選択します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。

ステップ 2 設定する物理インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

(注) シングルモードでは、この手順では [Edit Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。マルチコンテキストモードでは、インターフェイスの設定を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。

ステップ 3 インターフェイスをイネーブルにするには、[Enable Interface] チェックボックスをオンにします。

ステップ 4 説明を追加するには、[Description] フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステートリンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステートリンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 5 (任意) メディア タイプ、二重通信、速度を設定し、フロー制御のポーズフレームをイネーブルにするには、[Configure Hardware Properties] をクリックします。

a) インターフェイス タイプに応じて、[Media Type] ドロップダウンリストから [RJ-45] または [SFP] のいずれかを選択できます。

RJ-45 がデフォルトです。

b) RJ-45 インターフェイスにデュプレックスを設定するには、[Duplex] ドロップダウンリストからインターフェイス タイプに応じて [Full]、[Half]、または [Auto] を選択します。

(注) EtherChannel インターフェイスのデュプレックスの設定は [Full] または [Auto] である必要があります。

c) 速度を設定するには、[Speed] ドロップダウンリストから値を選択します。

使用できる速度は、インターフェイス タイプによって異なります。SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate] (デフォルト) ではリンクネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンクパラメータのネゴシエーションを行いません。RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。

d) 1 ギガビットイーサネットインターフェイスおよび 10 ギガビットイーサネットインターフェイスでフロー制御のポーズ (XOFF) フレームをイネーブルにするには、[Enable Pause Frame] チェックボックスをオンにします。

トラフィックバーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リングバッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズフレームをイネーブルにすると、このような問題の発生を

抑制できます。ポーズ (XOFF) および XON フレームは、FIFO バッファ使用量に基づいて、NIC ハードウェアによって自動的に生成されます。バッファ使用量が高ウォーターマークを超えると、ポーズ フレームが送信されます。デフォルトの *high_water* 値は 128 KB (10 ギガビット イーサネット) および 24 KB (1 ギガビット イーサネット) です。0 ~ 511 (10 ギガビット イーサネット) または 0 ~ 47 KB (1 ギガビット イーサネット) に設定できます。ポーズの送信後、バッファ使用量が低ウォーターマークよりも下回ると、XON フレームを送信できます。デフォルトでは、*low_water* 値は 64 KB (10 ギガビット イーサネット) および 16 KB (1 ギガビット イーサネット) です。0 ~ 511 (10 ギガビット イーサネット) または 0 ~ 47 KB (1 ギガビット イーサネット) に設定できます。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。デフォルトの *pause_time* 値は 26624 です。この値は 0 ~ 65535 に設定できます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズリフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。

[Low Watermark]、[High Watermark]、[Pause Time] のデフォルト値を変更するには、[Use Default Values] チェックボックスをオフにします。

(注) 802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

e) [OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 6 [OK] をクリックして [Interface] の変更を受け入れます。

ジャンボ フレーム サポートの有効化

ジャンボ フレームとは、標準的な最大値 1518 バイト (レイヤ 2 ヘッダーおよび VLAN ヘッダーを含む) より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能 (ACL など) の最大使用量が制限される場合があります。ASA MTU はレイヤ 2 (14 バイト) および VLAN ヘッダー (4 バイト) を含まずにペイロードサイズを設定するので、モデルによっては MTU 最大値が 9198 になることに注意してください。

始める前に

- マルチコンテキストモードでは、システム実行スペースでこのオプションを設定します。
- この設定を変更した場合は、ASA のリロードが必要です。
- ジャンボフレームを送信する必要がある各インターフェイスの MTU を、デフォルト値の 1500 より大きい値に設定してください。たとえば、マルチコンテキストモードでは、各コンテキスト内で MTU を設定します。

- Be sure to adjust the TCP MSS, either to disable it for non-IPsec traffic, or to increase it in accord with the MTU.

手順

コンテキストモードによって次のように異なります。

- マルチモード：ジャンボフレームサポートをイネーブルにするには、[Configuration] > [Context Management] > [Interfaces] を選択し、[Enable jumbo frame support] チェックボックスをオンにします。
- シングルモード：1500 バイトを超える MTU を設定すると、ジャンボフレームが自動的にイネーブルになります。この設定を手動でイネーブルまたはディセーブルにするには、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] を選択し、[Enable jumbo frame support] チェックボックスをオンにします。

基本インターフェイスの例

次の設定例を参照してください。

物理インターフェイスパラメータの例

次に、シングルモードで物理インターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

マルチコンテキストモードの例

次に、システムコンフィギュレーション用にマルチコンテキストモードでインターフェイスパラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

基本インターフェイスの設定の履歴

表 20: インターフェイスの履歴

機能名	リリース	機能情報
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。
ASA 5510 Security Plus ライセンスに対するギガビットイーサネットサポート	7.2(3)	ASA 5510 は、GE（ギガビットイーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファストイーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。
ASA 5580 に対するジャンボ パケットサポート	8.1(1)	<p>Cisco ASA 5580 はジャンボフレームをサポートしています。ジャンボフレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネットパケットのことです。イーサネットフレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボフレームのサポートをイネーブルにできます。ジャンボフレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。</p> <p>この機能は、ASA 5585-X でもサポートされます。</p> <p>次の画面が変更されました。 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [Advanced]。</p>

機能名	リリース	機能情報
ASA 5580 10 ギガビットイーサネット インターフェイスでのフロー制御の ポーズ フレームのサポート	8.2(2)	<p>フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。</p> <p>この機能は、ASA 5585-X でもサポートされます。</p> <p>次の画面が変更されました。[(Single Mode) Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [General (Multiple Mode, System)]</p> <p>[Configuration] > [Interfaces] > [Add/Edit Interface]</p>
ギガビットイーサネットインターフェイスでのフロー制御のポーズフレームのサポート	8.2(5)/8.4(2)	<p>すべてのモデルでギガビットインターフェイスのフロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。</p> <p>次の画面が変更されました。[(Single Mode) Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [General (Multiple Mode, System)]</p> <p>[Configuration] > [Interfaces] > [Add/Edit Interface]</p>



第 14 章

EtherChannel インターフェイスと冗長インターフェイス

この章では、EtherChannel インターフェイスと冗長インターフェイスを設定する方法について説明します。



(注) マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。まだシステム実行スペースに入っていない場合は、[Configuration] > [Device List] ペイン内で、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

特殊な必須要件を保有する ASA クラスタ インターフェイスについては、[ASA クラスタ \(331 ページ\)](#) を参照してください。



(注) Firepower 9300 シャーシ、EtherChannel インターフェイスは FXOS オペレーティングシステムで設定されます。冗長インターフェイスはサポートされません。詳細については、お使いのシャーシの設定または導入ガイドを参照してください。

- [EtherChannel インターフェイスと冗長インターフェイスについて \(476 ページ\)](#)
- [EtherChannel インターフェイスと冗長インターフェイスのガイドライン \(479 ページ\)](#)
- [EtherChannel インターフェイスと冗長インターフェイスのデフォルト設定 \(482 ページ\)](#)
- [冗長インターフェイスの設定 \(482 ページ\)](#)
- [EtherChannel の設定 \(485 ページ\)](#)
- [EtherChannel インターフェイスと冗長インターフェイスの例 \(489 ページ\)](#)
- [EtherChannel インターフェイスと冗長インターフェイスの履歴 \(490 ページ\)](#)

EtherChannel インターフェイスと冗長インターフェイスについて

この項では、EtherChannel インターフェイスと冗長インターフェイスについて説明します。

冗長インターフェイスについて

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブインターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してASAの信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものです。必要な場合はデバイスレベルのフェールオーバーとともに冗長インターフェイスも設定できます。

最大 8 個の冗長インターフェイス ペアを設定できます。

冗長インターフェイスの MAC アドレス

冗長インターフェイスでは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに手動で MAC アドレスを割り当てることができます。これはメンバー インターフェイスの MAC アドレスに関係なく使用されます。アクティブ インターフェイスがスタンバイインターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

関連トピック

[手動 MAC アドレス、MTU、および TCP MSS の設定](#) (546 ページ)

[マルチ コンテキストの設定](#) (253 ページ)

EtherChannel について

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャンネル グループ）のバンドルで構成される論理インターフェイスです（ポートチャンネル インターフェイスと呼びます）。ポートチャンネル インターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

モデルでサポートされているインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。

チャンネルグループのインターフェイス

各チャンネルグループには、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャンネルグループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイリンクとして動作できます。16 個のアクティブ インターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

チャンネルグループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャンネルグループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

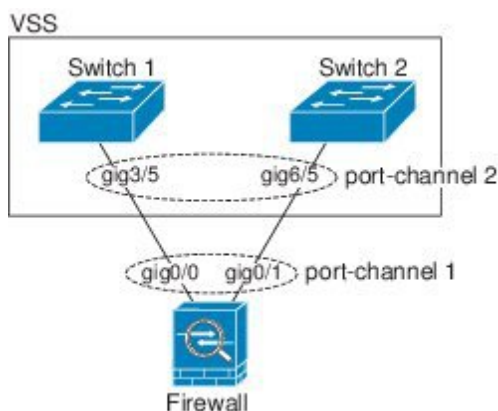
EtherChannel によって、チャンネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

ASA EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 に接続できます。

スイッチが仮想スイッチング システム (VSS) または 仮想ポート チャンネル (vPC) の一部である場合、同じ EtherChannel 内の ASA インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャンネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。

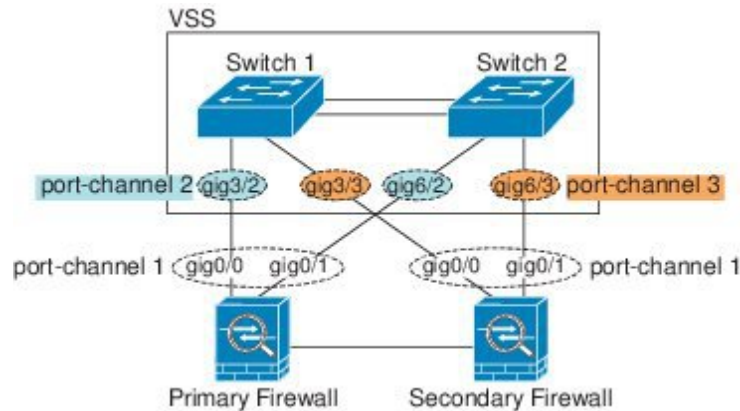
図 56: VSS/vPC への接続



ASA をアクティブ/スタンバイ フェールオーバー配置で使用する場合、ASA ごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel を作成する必要があります。各 ASA で、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチ インターフェイスを両方の ASA に接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の ASA シ

システム ID のため、EtherChannel は確立されません)、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ ASA に送信しないようにするためです。

図 57: アクティブ/スタンバイ フェールオーバーと VSS/vPC



リンク集約制御プロトコル

リンク集約制御プロトコル (LACP) では、2つのネットワーク デバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- **アクティブ** : LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- **パッシブ** : LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。Firepower ハードウェア モデルではサポートされていません。
- **オン** : EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。Firepower ハードウェア モデルではサポートされていません。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャンネルグループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャンネルグループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

ASA は、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します (この基準は設定可能です)。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフ

ローの割り当て先のインターフェイスが決まります。`hash_value mod active_links`の結果が0となるパケットはすべて、EtherChannel内の最初のインターフェイスに送信されます。以降は同様に、結果が1となるものは2番目のインターフェイスに、結果が2となるものは3番目のインターフェイスに送信されます。たとえば、15個のアクティブリンクがある場合、モジュロ演算では0～14の値が得られます。6個のアクティブリンクの場合、値は0～5となり、以降も同様になります。

クラスタリングのスパンドEtherChannelでは、ロードバランシングはASAごとに行われます。たとえば、8台のASAにわたるスパンドEtherChannel内に32個のアクティブインターフェイスがあり、EtherChannel内の1台のASAあたり4個のインターフェイスがある場合、ロードバランシングは1台のASAの4個のインターフェイス間でのみ行われます。

アクティブインターフェイスがダウンし、スタンバイインターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ2のスパニングツリーとレイヤ3のルーティングテーブルの両方からマスクされるため、他のネットワークデバイスへのスイッチオーバーはトランスペアレントです。

関連トピック

[EtherChannelのカスタマイズ](#) (487 ページ)

EtherChannel MAC アドレス

1つのチャンネルグループに含まれるすべてのインターフェイスは、同じMACアドレスを共有します。この機能によって、EtherChannelはネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないからです。

ポートチャンネルインターフェイスは、最も小さいチャンネルグループインターフェイスのMACアドレスをポートチャンネルMACアドレスとして使用します。または、ポートチャンネルインターフェイスのMACアドレスを手動で設定することもできます。マルチコンテキストモードでは、EtherChannelポートインターフェイスを含め、一意のMACアドレスを共有インターフェイスに自動的に割り当てることができます。グループチャンネルインターフェイスのメンバーシップを変更する場合は、固有のMACアドレスを手動で設定するか、または共有インターフェイスのマルチコンテキストモードでは自動的に設定することを推奨します。ポートチャンネルMACアドレスを提供していたインターフェイスを削除すると、そのポートチャンネルのMACアドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

EtherChannel インターフェイスと冗長インターフェイスのガイドライン

フェールオーバー

- 冗長インターフェイスまたはEtherChannelインターフェイスをフェールオーバーリンクとして使用する場合、フェールオーバーペアの両方のユニットでその事前設定を行う必要

があります。プライマリユニットで設定し、セカンダリ装置に複製されることは想定できません。これは、複製にはフェールオーバーリンク自体が必要であるためです。

- 冗長インターフェイスまたは EtherChannel インターフェイスをステートリンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリ装置から複製されます。Firepower 9300 シャーシでは、Etherchannel を含むすべてのインターフェイスを両方のユニットで事前に設定する必要があります。
- **monitor-interface** コマンドを使用して、フェールオーバー。When an active member interface fails over to a standby interface, this activity does not cause the redundant or EtherChannel interface to appear to be failed when being monitored for device-level フェールオーバー。すべての物理インターフェイスで障害が発生した場合にのみ、冗長インターフェイスまたは EtherChannel インターフェイスで障害が発生しているように見えます (EtherChannel インターフェイスでは、障害の発生が許容されるメンバインターフェイスの数を設定できます)。
- If you use an EtherChannel interface for a フェールオーバー or state link, then to prevent out-of-order packets, only one interface in the EtherChannel is used. そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバーリンクとして使用中の EtherChannel の設定は変更できません。設定を変更するには、フェールオーバーを一時的に無効にする必要があります。これにより、フェールオーバーがその期間に発生することはありません。

サポート モデル

- Firepower 4100/9300、ASA v、または ASASM の場合、ASA に EtherChannel を追加することはできません。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャーシ上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。
- Firepower 9300 シャーシおよび ASASM では、冗長インターフェイスはサポートされていません。

クラスタ

- スパンド EtherChannel または個別クラスタインターフェイスを設定するには、クラスタリングの章を参照してください。

冗長インターフェイスの一般的なガイドライン

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- すべての ASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを ASA 上で設定することができます。

- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。
- 冗長インターフェイスは、管理 *slot/port* インターフェイスをメンバーとしてサポートしません。ただし、管理インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

EtherChannel の一般的なガイドライン

- モデルで使用可能なインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。
- 各チャンネル グループには、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブインターフェイスだけをサポートするスイッチの場合、1つのチャンネルグループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16 個のアクティブインターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビットイーサネット モジュール）。
- チャンネルグループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャンネルグループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。
- ASA の EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- ASA は、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS **vlan dot1Q tag native** コマンドを使用して、隣接スイッチのネイティブ VLAN タギングをイネーブルにすると ASA はタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。マルチ コンテキスト モードでは、これらのメッセージはパケットキャプチャに含まれていないため、問題を効率的に診断できません。
- 15.1(1)S2 以前の Cisco IOS ソフトウェアバージョンを実行する ASA では、スイッチスタックへの EtherChannel の接続がサポートされていませんでした。デフォルトのスイッチ設定では、ASA EtherChannel がクロススタックに接続されている場合、マスタースイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- すべての ASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用でき

ません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを ASA 上で設定することができます。

EtherChannel インターフェイスと冗長インターフェイスのデフォルト設定

この項では、工場出荷時のデフォルトコンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス：イネーブル。ただし、トラフィックが EtherChannel を通過するためには、チャネルグループ物理インターフェイスもイネーブルになっている必要があります。

冗長インターフェイスの設定

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブインターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものです。必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。

この項では、冗長インターフェイスを設定する方法について説明します。

冗長インターフェイスの設定

この項では、冗長インターフェイスを作成する方法について説明します。デフォルトでは、冗長インターフェイスはイネーブルになっています。

始める前に

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- 冗長インターフェイス遅延値は設定可能ですが、デフォルトでは、ASA はそのメンバーインターフェイスの物理タイプに基づくデフォルトの遅延値を継承します。
- 両方のメンバインターフェイスが同じ物理タイプである必要があります。たとえば、両方もギガビットイーサネットにする必要があります。
- 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。最初に、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインで、名前を削除する必要があります。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステムコンフィギュレーションモードを開始していない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。



注意

コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングルモードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
- マルチモードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2 [Add] > [Redundant Interface] の順に選択します。

[Add Redundant Interface] ダイアログボックスが表示されます。

(注) シングルモードでは、この手順では [Edit Redundant Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。マルチ コンテキスト モードでは、インターフェイスの設定を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。マルチ コンテキスト の設定 (253 ページ) を参照してください。

ステップ 3 [Redundant ID] フィールドで、1～8の整数を入力します。

ステップ 4 [Primary Interface] ドロップダウンリストから、プライマリにする物理インターフェイスを選択します。

サブインターフェイスを持たず、まだコンテキストに割り当てられていないインターフェイスを必ず選択してください。冗長インターフェイスは、Management slot/port インターフェイスをメンバとしてサポートしません。

ステップ 5 [Secondary Interface] ドロップダウンリストから、セカンダリにする物理インターフェイスを選択します。

ステップ 6 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。


インターフェイスはデフォルトでイネーブルになっています。

ステップ 7 説明を追加するには、[Description] フィールドにテキストを入力します。

説明は240文字以内で入力できます。改行を入れずに1行で入力します。マルチコンテキストモードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステートリンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステートリンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8 [OK] をクリックします。

[Interfaces] ペインに戻ります。メンバーインターフェイスで、基本パラメータのみが設定できることを示すロックが、インターフェイス ID の左側に表示されます。冗長インターフェイスがテーブルに追加されます。

 GigabitEthernet0/2	Enabled	No	Redundant8	Hardware	native
GigabitEthernet0/3	Enabled	No		Hardware	native
GigabitEthernet0/3.10	Enabled	No		Logical	vlan100
GigabitEthernet0/3.11	Enabled	No		Logical	vlan11
Management0/0	Enabled	No		Hardware	native
Redundant8	Enabled	Yes		Logical	native

254710

アクティブインターフェイスの変更

デフォルトでは、コンフィギュレーションで最初にリストされているインターフェイスが（使用可能であれば）、アクティブインターフェイスになります。

手順

ステップ 1 どのインターフェイスがアクティブかを表示するには、[Tools] > [Command Line Interface] ツールで次のコマンドを入力します。


```
show interface redundant number detail | grep Member
```

例：

```
show interface redundant1 detail | grep Member
Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

ステップ 2 アクティブ インターフェイスを変更します。

```
redundant-interface redundant number active-member physical_interface
```

redundantnumber 引数には、冗長インターフェイス ID (**redundant1** など) を指定します。

physical_interface には、アクティブにするメンバインターフェイスの ID を指定します。

EtherChannel の設定

ここでは、EtherChannel ポートチャネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。

EtherChannel へのインターフェイスの追加

ここでは、EtherChannel ポートチャネル インターフェイスを作成し、インターフェイスを EtherChannel に割り当てる方法について説明します。デフォルトでは、ポートチャネル インターフェイスはイネーブルになっています。

始める前に

- 使用しているモデルに設定されているインターフェイスの数に応じて、最大 48 個の EtherChannel を設定できます。
- 各チャネルグループには、最大 16 個のアクティブ インターフェイスをサポートしていません。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネルグループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
- クラスタリング用にスパンド EtherChannel を設定するには、この手順の代わりにクラスタリングの章を参照してください。
- チャネルグループのすべてのインターフェイスは、同じタイプ、速度、および二重通信である必要があります。半二重はサポートされません。RJ-45 または SFP コネクタを使用するように設定できるインターフェイスの場合、同一の EtherChannel に RJ-45 インターフェイスと SFP インターフェイスの両方を含めることができることに注意してください。

- 名前が設定されている場合は、物理インターフェイスをチャンネルグループに追加できません。最初に、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインで、名前を削除する必要があります。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードを開始していない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。



注意 コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2 [Add] > [EtherChannel Interface] の順に選択します。

[Add EtherChannel Interface] ダイアログボックスが表示されます。

(注) シングル モードでは、この手順では [Edit EtherChannel Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。マルチ コンテキスト モードでは、インターフェイスの設定を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。 [マルチ コンテキスト の設定 \(253 ページ\)](#) を参照してください。

ステップ 3 [Port Channel ID] フィールドに 1 ~ 48 の範囲の数値を入力します。

ステップ 4 [Available Physical Interface] 領域で、インターフェイスをクリックし、[Add] をクリックしてそれを [Members in Group] 領域に移動します。

トランスペアレント モードで、複数の管理インターフェイスがあるチャンネルグループを作成する場合は、この EtherChannel を管理専用インターフェイスとして使用できます。

(注) EtherChannel モードをオンに設定する場合、最初はインターフェイスを 1 個のみ含める必要があります。この手順を完了後、メンバーインターフェイスを編集し、このモードを **オン** に設定します。変更を適用し、EtherChannel を編集してメンバーインターフェイスをさらに追加します。

ステップ 5 チャンネルグループに追加するインターフェイスごとに繰り返します。

すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。ASDM では、一致しないインターフェイスの追加は防止されません。

ステップ 6 [OK] をクリックします。

[Interfaces] ペインに戻ります。メンバーインターフェイスで、基本パラメータのみが設定できることを示すロックが、インターフェイス ID の左側に表示されます。EtherChannel インターフェイスがテーブルに追加されます。

🔒 GigabitEthernet0/3	Disabled			Port-channel1	Hardw
Management0/0	Disabled				Hardw
Port-channel1	Enabled				EtherC 254690

ステップ 7 [Apply] をクリックします。すべてのメンバー インターフェイスは自動的にイネーブルになります。

関連トピック

[リンク集約制御プロトコル](#) (478 ページ)

[EtherChannelのカスタマイズ](#) (487 ページ)

EtherChannelのカスタマイズ

この項では、EtherChannel のインターフェイスの最大数、EtherChannel をアクティブにするための動作インターフェイスの最小数、ロード バランシング アルゴリズム、およびその他のオプション パラメータを設定する方法について説明します。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングルモードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
- マルチモードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2 カスタマイズするポートチャネルインターフェイスをクリックし、[Edit] をクリックします。
[Edit Interface] ダイアログボックスが表示されます。

ステップ 3 すべてのメンバインターフェイスについて、メディアタイプ、二重通信、速度、およびフロー制御のポーズ フレームを上書きするには、[Configure Hardware Properties] をクリックします。これらのパラメータはチャネルグループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

ステップ 4 (オプション) EtherChannel をカスタマイズするには、[Advanced] タブをクリックします。

- a) [EtherChannel] 領域で、[Minimum] ドロップダウンリストから、EtherChannel をアクティブにするために必要なアクティブインターフェイスの最小数を 1～16 の範囲で選択します。デフォルトは 1 です。
- b) [Maximum] ドロップダウンリストから、EtherChannel で許可されるアクティブ インターフェイスの最大数を 1～16 の範囲で選択します。デフォルトは 16 です。スイッチが 16 個のアクティブインターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。
- c) [Load Balance] ドロップダウンリストから、パケットをグループ チャネル インターフェイス間でロード バランスするために使用する基準を選択します。デフォルトでは、ASA はパケットの送信元および宛先 IP アドレスに従って、インターフェイスでのパケットのロードをバランスします。パケットが分類される基準になるプロパティを変更する場合は、別の基準のセットを選択します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。ロード バランシングの詳細については、[ロード バランシング \(478 ページ\)](#) を参照してください。
- d) [Secure Group Tagging] 設定については、[ファイアウォール コンフィギュレーション ガイド](#)を参照してください。
- e) [ASA Cluster] 設定については、[\(推奨、マルチ コンテキスト モードでは必須\) マスター ユニットでのインターフェイスの設定 \(376 ページ\)](#) を参照してください。

ステップ 5 [OK] をクリックします。

[Interfaces] ペインに戻ります。

ステップ 6 チャネルグループ内の物理インターフェイスのモードおよびプライオリティを設定するには、次の手順を実行します。

- a) [Interfaces] テーブルで物理インターフェイスを選択し、[Edit] をクリックします。
[Edit Interface] ダイアログボックスが表示されます。
- b) [Advanced] タブをクリックします。
- c) [EtherChannel] 領域で、[Mode] ドロップダウンリストから、[Active]、[Passive]、または [On] を選択します。[Active] モード (デフォルト) を使用することを推奨します。
- d) (オプション) [LACP Port Priority] フィールドで、ポートプライオリティを 1～65535 の範囲で設定します。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。使用可能な数よりも多くのインターフェイスを割り当てた場合、ASA ではこの設定を使用して、アクティブ インターフェイスとスタンバイ インターフェイスを決定します。ポートプライオリティ設定がすべてのインターフェイスで同じ場合、プライオリティはインターフェイス ID (スロット/ポート) で決まります。最も小さいインターフェイス ID が、最も高いプライオリティになります。たとえば、GigabitEthernet 0/0 のプライオリティは GigabitEthernet 0/1 よりも高くなります。

あるインターフェイスについて、インターフェイス ID は大きいですが、そのインターフェイスがアクティブになるように優先順位を付ける場合は、より小さい値を持つようにこのコマンドを設定します。たとえば、GigabitEthernet 1/3 を GigabitEthernet 0/7 よりも前にアク

タイプにするには、0/7 インターフェイスでのデフォルトの 32768 に対し、1/3 インターフェイスでプライオリティ値を 12345 にします。

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。システム プライオリティを設定するには、[ステップ 9](#) を参照してください。

ステップ 7 [OK] をクリックします。

[Interfaces] ペインに戻ります。

ステップ 8 [Apply] をクリックします。

ステップ 9 (オプション) LACP システムプライオリティを設定するには、次の手順を実行します。

EtherChannel の反対の端にあるデバイスのポートプライオリティが衝突している場合、システムプライオリティを使用して使用するポートプライオリティが決定されます。詳細については、[ステップ 6d](#) を参照してください。

a) コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [EtherChannel] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [EtherChannel] ペインを選択します。

b) [LACP System Priority] フィールドに、プライオリティを 1 ~ 65535 の範囲で入力します。デフォルトは 32768 です。

関連トピック

[ロード バランシング](#) (478 ページ)

[EtherChannel へのインターフェイスの追加](#) (485 ページ)

EtherChannel インターフェイスと冗長インターフェイスの例

次の例では、3つのインターフェイスを EtherChannel の一部として設定します。また、システムプライオリティをより高く設定するとともに、GigabitEthernet 0/2 のプライオリティを他のインターフェイスよりも高く設定します。これは、8個を超えるインターフェイスが EtherChannel に割り当てられた場合に備えるためです。

```
lACP system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
```

```

lacp port-priority 1234
channel-group 1 mode passive
interface Port-channell
lacp max-bundle 4
port-channel min-bundle 2
port-channel load-balance dst-ip

```

EtherChannel インターフェイスと冗長インターフェイスの履歴

表 21: EtherChannel インターフェイスと冗長インターフェイスの履歴

機能名	リリース	機能情報
冗長インターフェイス	8.0(2)	論理冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです。アクティブインターフェイスで障害が発生すると、スタンバイインターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。最大 8 個の冗長インターフェイスペアを設定できます。

機能名	リリース	機能情報
EtherChannel サポート	8.4(1)	<p>最大 48 個の 802.3ad EtherChannel (1 つあたりのアクティブインターフェイス 8 個) を設定できます。</p> <p>次の画面が変更または導入されました。</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit EtherChannel Interface]</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]</p> <p>[Configuration] > [Device Setup] > [EtherChannel]</p> <p>(注) EtherChannel は ASA 5505 ではサポートされません。</p>
EtherChannel あたり 16 個のアクティブリンクのサポート	9.2(1)	<p>EtherChannel あたり最大で 16 個のアクティブリンクを設定できるようになりました。これまでは、8 個のアクティブリンクと 8 個のスタンバイリンクが設定できました。スイッチは、16 個のアクティブリンクをサポート可能である必要があります (たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビットイーサネット モジュール)。</p> <p>(注) 旧バージョンの ASA からアップグレードする場合、互換性を得るために、アクティブなインターフェイスの最大数を 8 に設定します。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit EtherChannel Interface] > [Advanced]。</p>



第 15 章

VLAN サブインターフェイス

この章では、VLAN サブインターフェイスを設定する方法について説明します。



(注) マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。システム実行スペースに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイス IP アドレスの下にある **[System]** をダブルクリックします。

- [VLAN サブインターフェイスについて \(493 ページ\)](#)
- [VLAN サブインターフェイスのライセンス \(494 ページ\)](#)
- [VLAN サブインターフェイスのガイドラインと制限事項 \(495 ページ\)](#)
- [VLAN サブインターフェイスのデフォルト設定 \(495 ページ\)](#)
- [VLAN サブインターフェイスと 802.1Q トランキングの設定 \(496 ページ\)](#)
- [VLAN のサブインターフェイスの例 \(497 ページ\)](#)
- [VLAN サブインターフェイスの履歴 \(498 ページ\)](#)

VLAN サブインターフェイスについて

VLAN サブインターフェイスを使用すると、1つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが1つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたは ASA を追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。この機能は、各コンテキストに固有のインターフェイスを割り当てることができるので、マルチ コンテキスト モードで特に便利です。

VLAN サブインターフェイスのライセンス

モデル	ライセンス要件
Firepower 9300	標準ライセンス : 1024
ASAv5	標準ライセンス : 25
ASAv10	標準ライセンス : 50
ASAv30	標準ライセンス : 200
ASA 5506-X	基本ライセンス : 5
ASA 5506W-X	Security Plus ライセンス : 30
ASA 5506H-X	
ASA 5508-X	基本ライセンス : 50
ASA 5512-X	基本ライセンス : 50 Security Plus ライセンス : 100
ASA 5515-X	基本ライセンス : 100
ASA 5516-X	基本ライセンス : 50
ASA 5525-X	基本ライセンス : 200
ASA 5545-X	基本ライセンス : 300
ASA 5555-X	基本ライセンス : 500
ASA 5585-X	基本ライセンスと Security Plus ライセンス : 1024
ASASM	サポートしない
ISA 3000	基本ライセンス : 5 Security Plus ライセンス : 25



(注) VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

VLAN サブインターフェイスのガイドラインと制限事項

モデルのサポート

- ASASM : VLAN サブインターフェイスは、ASASM ではサポートされません。ASASM のインターフェイスは、すでにスイッチから割り当てられた VLAN インターフェイスです。

その他のガイドライン

- 物理インターフェイス上のタグなしパケットの禁止 : サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイスペアのアクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。トラフィックがサブインターフェイスを通過するには、物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスがイーネブルになっている必要があるため、トラフィックが物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを通過しないように、インターフェイスには名前を設定しないでください。物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスでタグのないパケットを通過させる場合は、通常通り `name` コマンドを設定できます。
- 多くのモデルでは、管理インターフェイスのサブインターフェイスを設定できません。サブインターフェイスのサポートについては、[管理スロット/ポートインターフェイス \(464 ページ\)](#) を参照してください。
- ASA は Dynamic Trunking Protocol (DTP) をサポートしていないため、接続されているスイッチポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスの同じ Burned-In MAC Address を使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセスコントロールを実行する場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

VLAN サブインターフェイスのデフォルト設定

この項では、工場出荷時のデフォルトコンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- VLAN サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

VLAN サブインターフェイスと 802.1Q トランキングの設定

VLAN サブインターフェイスを物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスに追加します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングルモードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
- マルチモードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2 [Add] > [Interface] の順に選択します。

[Add Interface] ダイアログボックスが表示されます。

(注) シングルモードの場合、この手順で対象としているのは [Edit Interface] ダイアログボックスのパラメータのサブセットのみであるため、他のパラメータを設定する場合は、[ルーテッドモードインターフェイスとトランスペアレントモードインターフェイス \(513 ページ\)](#) を参照してください。マルチコンテキストモードでは、インターフェイスの設定を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。[マルチコンテキストの設定 \(253 ページ\)](#) を参照してください。

ステップ 3 [Hardware Port] ドロップダウンリストから、サブインターフェイスを追加する物理インターフェイス、冗長インターフェイス、またはポートチャンネルインターフェイスを選択します。

ステップ 4 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

インターフェイスはデフォルトでイネーブルになっています。

ステップ 5 [VLAN ID] フィールドに、1 ~ 4094 の VLAN ID を入力します。

VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。マルチコンテキストモードの場合、VLAN はシステム設定でしか設定できません。

ステップ 6 [Subinterface ID] フィールドに、サブインターフェイス ID を 1 ~ 4294967293 の整数で入力します。

許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

ステップ 7 (オプション) [Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。マルチコンテキストモードの場合、システムの説明とコンテキストの説明には関係ありません。フェールオーバーまたはステートリンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステートリンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8 [OK] をクリックします。

[Interfaces] ペインに戻ります。

関連トピック

[VLAN サブインターフェイスのライセンス \(494 ページ\)](#)

VLAN のサブインターフェイスの例

次に、シングルモードでサブインターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
```

```

no nameif
no security-level
no ip address
no shutdown
interface gigabitethernet 0/1.1
vlan 101
nameif inside
security-level 100
ip address 192.168.6.6 255.255.255.0
no shutdown

```

VLAN サブインターフェイスの履歴

表 22: VLAN サブインターフェイスの履歴

機能名	バージョン	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 <ul style="list-style-type: none"> • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
VLAN 数の増加	7.2(2)	VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。



第 16 章

VXLAN インターフェイス

この章では、仮想拡張 LAN (VXLAN) インターフェイスを設定する方法について説明します。VXLAN は、レイヤ 2 ネットワークを拡張するためにレイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。

- [VXLAN インターフェイスの概要 \(499 ページ\)](#)
- [VXLAN インターフェイスのガイドライン \(505 ページ\)](#)
- [VXLAN インターフェイスのデフォルト設定 \(505 ページ\)](#)
- [VXLAN インターフェイスの設定 \(505 ページ\)](#)
- [VXLAN インターフェイスの例 \(508 ページ\)](#)
- [VXLAN インターフェイスの履歴 \(512 ページ\)](#)

VXLAN インターフェイスの概要

VXLAN は、VLAN の場合と同じイーサネットレイヤ 2 ネットワーク サービスを提供しますが、より優れた拡張性と柔軟性を備えています。VLAN と比較して、VXLAN には次の利点があります。

- データセンター全体でのマルチテナント セグメントの柔軟な配置。
- より多くのレイヤ 2 セグメント (最大 1600 万の VXLAN セグメント) に対応するための高度なスケーラビリティ。

ここでは、VXLAN の動作について説明します。詳細については、RFC 7348 を参照してください。

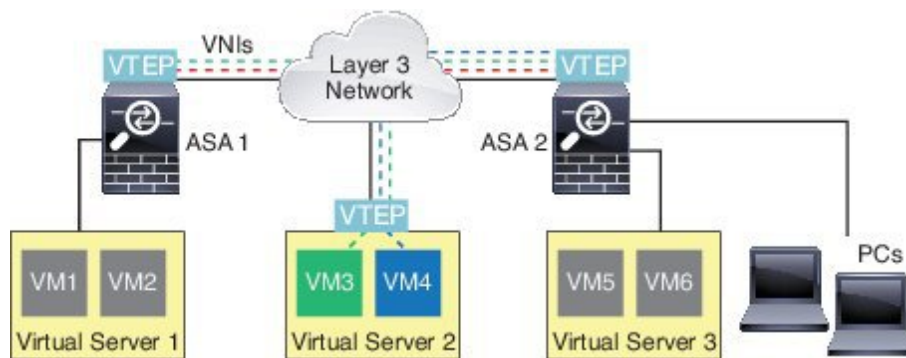
VXLAN カプセル化

VXLAN は、レイヤ 3 ネットワーク上のレイヤ 2 オーバーレイ方式です。VXLAN は、MAC Address-in-User Datagram Protocol (MAC-in-UDP) のカプセル化を使用します。元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。

VXLAN トンネル エンドポイント

VXLAN トンネル エンドポイント (VTEP) デバイスは、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP には 2 つのインターフェイス タイプ (セキュリティ ポリシーを適用する VXLAN Network Identifier (VNI) インターフェイスと呼ばれる 1 つ以上の仮想インターフェイスと、VTEP 間に VNI をトンネリングする VTEP 送信元インターフェイスと呼ばれる通常のインターフェイス) があります。VTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

次の図に、レイヤ 3 ネットワークで VTEP として機能し、サイト間の VNI 1、2、3 を拡張する 2 つの ASA と仮想サーバ 2 を示します。ASA は、VXLAN と VXLAN 以外のネットワークの間のブリッジまたはゲートウェイとして機能します。



VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。カプセル化されたパケットは、発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてルーティングされます。宛先 IP アドレスは、リモート VTEP が不明な場合、マルチキャストグループにすることができます。デフォルトでは、宛先ポートは UDP ポート 4789 です (ユーザ設定可能)。

VTEP 送信元インターフェイス

VTEP 送信元インターフェイスは、すべての VNI インターフェイスに関連付けられる予定の標準の ASA インターフェイス (物理、冗長、EtherChannel、または VLAN) です。ASA/セキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。

VTEP 送信元インターフェイスは、VXLAN トラフィック専用にすることができますが、その使用に制限されません。必要に応じて、インターフェイスを通常のトラフィックに使用し、そのトラフィックのインターフェイスにセキュリティポリシーを適用できます。ただし、VXLAN トラフィックの場合は、すべてのセキュリティポリシーを VNI インターフェイスに適用する必要があります。VTEP インターフェイスは、物理ポートとしてのみ機能します。

トランスペアレントファイアウォールモードでは、VTEP 送信元インターフェイスは、BVI の一部ではないため、その IP アドレスを設定しません。このインターフェイスは、管理インターフェイスが処理される方法に似ています。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持する仮想インターフェイスです。各VNI インターフェイスにセキュリティポリシーを直接適用します。

すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられます。

VXLAN パケット処理

VTEP 送信元インターフェイスを出入りするトラフィックは、VXLAN 処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP 送信元インターフェイスにより、VXLAN ヘッダーが含まれている内部 MAC フレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP が VTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP がリモート VTEP IP ルックアップによって決定されます。

カプセル化解除については、次の場合に ASA によって VXLAN パケットのみがカプセル化解除されます。

- これが、宛先ポートが 4789 に設定された UDP パケットである場合（この値はユーザ設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。
- VXLAN パケット形式が標準に準拠します。

ピア VTEP

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA がこの情報を検出するには 2 つの方法があります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。
手動で複数のピアを定義することはできません。

ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンドノードの MAC アドレスを取得します。

- マルチキャストグループは、VNI インターフェイスごとに（または VTEP 全体に）設定できます。

ASA は、IP マルチキャストパケット内の VXLAN カプセル化 ARP ブロードキャストパケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモートエンドノードの宛先 MAC アドレスの両方を取得することができます。

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

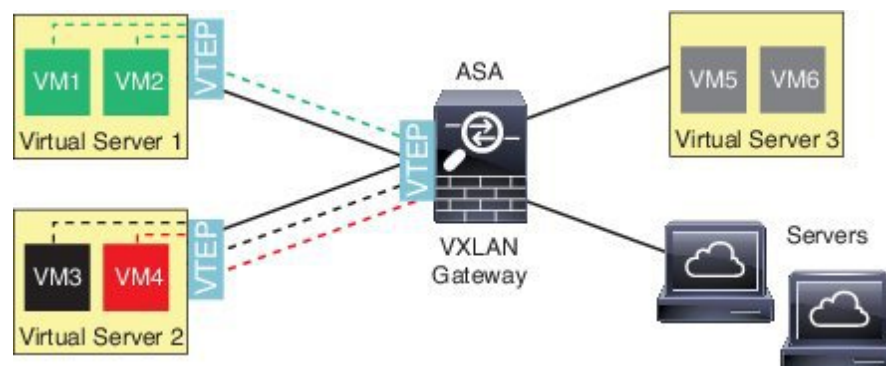
VXLAN 使用例

ここでは、ASA 上への VXLAN の実装事例について説明します。

VXLAN ブリッジまたはゲートウェイの概要

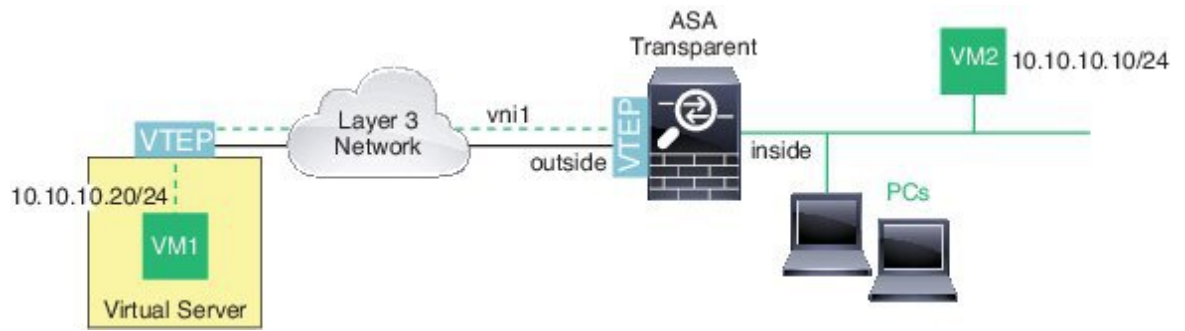
各 ASA の VTEP は、VM、サーバ、PC、VXLAN のオーバーレイ ネットワークなどのエンドノードの間のブリッジまたはゲートウェイとして機能します。VTEP 送信元インターフェイス経由の VXLAN カプセル化を使用して受信された着信フレームの場合は、ASA が VXLAN ヘッダーを抽出して、内部イーサネットフレームの宛先 MAC アドレスに基づいて非 VXLAN ネットワークに接続された物理インターフェイスにその着信フレームを転送します。

ASA は、常に VXLAN パケットを処理します。未処理の VXLAN パケットを他の 2 つの VTEP 間でそのまま転送しません。



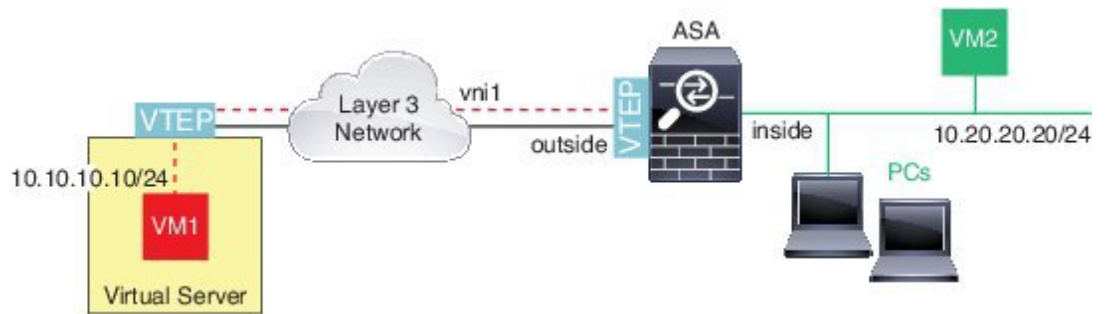
VXLAN ブリッジ（トランスペアレントモード）

ブリッジグループを使用する場合（トランスペアレントファイアウォールモード）、ASA は、同じネットワークに存在する VXLAN セグメント（リモート）とローカルセグメント間の VXLAN ブリッジとして機能できます。この場合、ブリッジグループのメンバーは通常インターフェイス 1 つのメンバーが通常のインターフェイスで、もう 1 つのメンバーが VNI インターフェイスです。



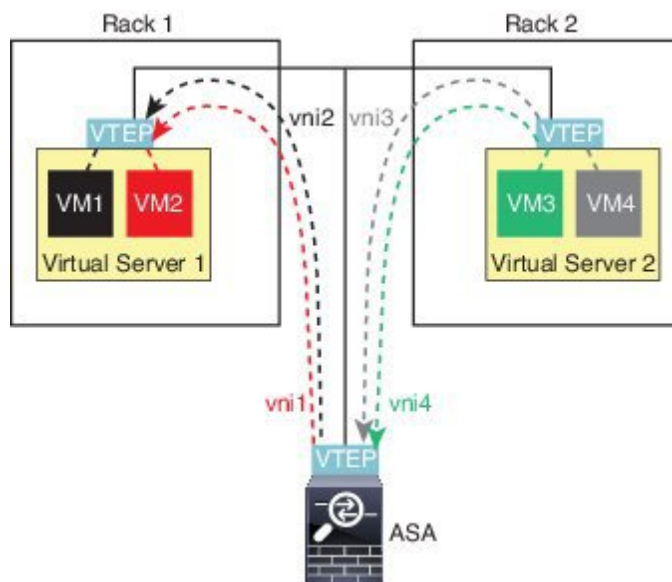
VXLAN ゲートウェイ (ルーテッドモード)

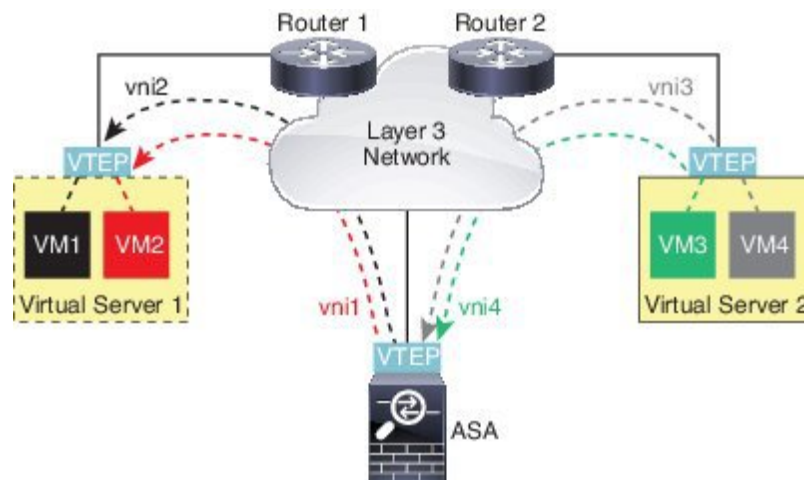
ASA は、VXLAN ドメインと VXLAN 以外のドメインの間のルータとして機能し、異なるネットワーク上のデバイスを接続できます。



VXLAN ドメイン間のルータ

VXLAN 拡張レイヤ2 ドメインを使用すると、VM は、ASA が同じラックにないとき、あるいは ASA がレイヤ3 ネットワーク上の離れた場所にあるときに、ゲートウェイとして ASA を指し示すことができます。





このシナリオに関する次の注意事項を参照してください。

1. VM3からVM1へのパケットでは、ASAがデフォルトゲートウェイであるため、宛先MACアドレスはASAのMACアドレスです。
2. 仮想サーバ2のVTEP送信元インターフェイスは、VM3からパケットを受信してから、VNI3のVXLANタグでパケットをカプセル化してASAに送信します。
3. ASAは、パケットを受信すると、パケットをカプセル化解除して内部フレームを取得します。
4. ASAは、ルートルックアップに内部フレームを使用して、宛先がVNI2上であることを認識します。VM1のマッピングがまだない場合、ASAはVNI2カプセル化されたARPブロードキャストをVNI2のマルチキャストグループIPで送信します。



(注) このシナリオでは複数のVTEPピアがあるため、ASAは複数のダイナミックVTEPピアディスカバリを使用する必要があります。

5. ASAはVNI2のVXLANタグでパケットを再度カプセル化し、仮想サーバ1に送信します。カプセル化の前に、ASAは内部フレームの宛先MACアドレスを変更してVM1のMACにします(ASAでVM1のMACアドレスを取得するためにマルチキャストカプセル化ARPが必要な場合があります)。
6. 仮想サーバ1は、VXLANパケットを受信すると、パケットをカプセル化解除して内部フレームをVM1に配信します。

VXLAN インターフェイスのガイドライン

IPv6

- VNI インターフェイスでは、IPv6 トラフィックをサポートしますが、VTEP 送信元インターフェイス IP アドレスでは、IPv4 のみをサポートします。
- IPv6 OSPF インターフェイス設定はサポートされていません。

クラスタ

ASA クラスタリングでは、個別インターフェイス モードの VXLAN をサポートしません。Spanned EtherChannel モードでのみ VXLAN をサポートします。

Routing

- VNI インターフェイスでは、スタティック ルーティングのみをサポートします。ダイナミック ルーティング プロトコルはサポートされません。
- ポリシーベース ルーティングはサポートされません。

MTU

送信元インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。この場合、イーサネットデータグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。他のデバイスが使用する MTU の方が大きい場合、送信元インターフェイス MTU を、ネットワーク MTU + 54 バイトに設定する必要があります。この MTU は、[ジャンボフレームサポートの有効化 \(471 ページ\)](#) を参照してください。

VXLAN インターフェイスのデフォルト設定

デフォルトでは、VNI インターフェイスはイネーブルになっています。

VXLAN インターフェイスの設定

VXLAN を設定するには、次の手順を実行します。

手順

- ステップ 1 [VTEP 送信元インターフェイスの設定 \(506 ページ\)](#)。

ステップ 2 VNI インターフェイスの設定 (507 ページ)

VTEP 送信元インターフェイスの設定

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント (NVE) として定義されます。VXLAN VTEP が現時点でサポートされている NVE です。

始める前に

マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択し、VTEP 送信元インターフェイスに使用するインターフェイスを編集します。

ステップ 2 (トランスペアレント モード) [VTEP Source Interface] チェック ボックスをオンにします。

この設定により、インターフェイスの IP アドレスを設定することができます。このコマンドは、この設定によってトラフィックがこのインターフェイスの VXLAN のみに制限されるルーテッドモードではオプションです。

ステップ 3 送信元インターフェイス名と IPv4 アドレスを設定し、[OK] をクリックします。

ステップ 4 [Configuration] > [Device Setup] > [Interface Settings] > [VXLAN] の順に選択します。

ステップ 5 (オプション) デフォルト 4789 から変更する場合は、[VXLAN Destination Port] の値を入力します。

マルチ コンテキスト モードでは、システム実行スペースでこの設定を行います。

ステップ 6 [Enable Network Virtualization Endpoint encapsulation using VXLAN] チェック ボックスをオンにします。

ステップ 7 ドロップダウン リストから [VTEP Tunnel Interface] を選択します。

(注) VTEP インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。

ステップ 8 (オプション) [Configure Packet Recipient] チェック ボックスをオンにします。

- (マルチ コンテキスト モード (シングル モードではオプション) [Specify Peer VTEP IP Address] を入力して、手動でピア VTEP の IP アドレスを指定します。

ピア IP アドレスを指定した場合、マルチキャスト グループ ディスカバリは使用できません。マルチキャストは、マルチ コンテキスト モードではサポートされていないため、手動設定が唯一のオプションです。VTEP には 1 つのピアのみを指定できます。

- (シングルモードのみ) [Multicast traffic to default multicast address] を入力して、関連付けられたすべての VNI インターフェイスにデフォルトのマルチキャストグループを指定します。

VNI インターフェイスごとにマルチキャストグループを設定していない場合は、このグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。

ステップ 9 [Apply] をクリックします。

VNI インターフェイスの設定

VNI インターフェイスを追加してそれを VTEP 送信元インターフェイスに関連付けて、基本インターフェイス パラメータを設定します。

手順

- ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択し、[Add] > [VNI Interface] をクリックします。
- ステップ 2 [VNI ID] は 1 ~ 10000 の間で入力します。
この ID は内部インターフェイス識別子です。
- ステップ 3 [VNI Segment ID] は 1 ~ 16777215 の間で入力します。
セグメント ID は VXLAN タギングに使用されます。
- ステップ 4 (トランスペアレントモード) このインターフェイスを割り当てる [Bridge Group] を指定します。
BVI インターフェイスを設定して通常のインターフェイスをこのブリッジグループに関連付けるには、[トランスペアレントモードのブリッジグループインターフェイスの設定 \(521 ページ\)](#) を参照してください。
- ステップ 5 [Interface Name] を入力します。
name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。
- ステップ 6 [Security Level] に 0 (最低) ~ 100 (最高) を入力します。[セキュリティレベル \(514 ページ\)](#) を参照してください。
- ステップ 7 (シングルモード) [Multicast Group IP Address] を入力します。
VNI インターフェイスに対してマルチキャストグループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルトグループが使用されます (使用可能な場合)。VTEP 送信元インターフェイスに対して手動で VTEP ピア IP を設定した場合、VNI インターフェイスに対し

マルチキャスト グループを指定することはできません。マルチキャストは、マルチ コンテキスト モードではサポートされていません。

ステップ 8 [NVE Mapped to VTEP Interface] チェック ボックスをオンにします。

この設定により、VNI インターフェイスが VTEP 送信元インターフェイスに関連付けられます。

ステップ 9 [Enable Interface] チェック ボックスをオンにします。この設定はデフォルトでイネーブルになっています。

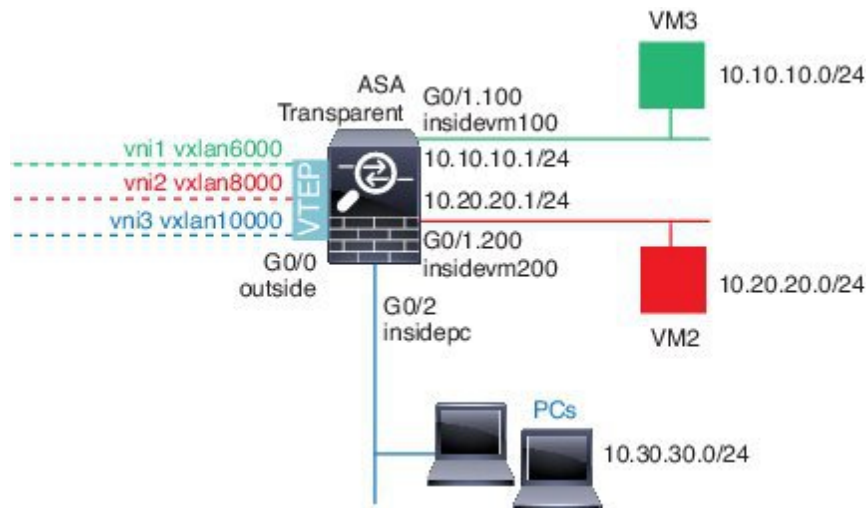
ステップ 10 (ルーテッドモード) [IP Address] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。

ステップ 11 [OK]、続いて [Apply] をクリックします。

VXLAN インターフェイスの例

次の VXLAN の設定例を参照してください。

トランスペアレント VXLAN ゲートウェイの例



この例の次の説明を参照してください。

- GigabitEthernet 0/0 の外部インターフェイスは、VTEP 送信元インターフェイスとして使用され、レイヤ 3 ネットワークに接続されます。
- GigabitEthernet 0/1.100 の insidevm100 VLAN サブインターフェイスは、VM3 が存在する 10.10.10.0/24 ネットワークに接続されます。VM3 が VM1 と通信する場合（表示されません。両方とも、10.10.10.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 6000 を使用します。

- GigabitEthernet 0/1.200 の insidevm200 VLAN サブインターフェイスは、VM2 が存在する 10.20.20.0/24 ネットワークに接続されます。VM2 が VM4 と通信する場合（表示されませんが、両方とも、10.20.20.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 8000 を使用します。
- GigabitEthernet 0/2 の insidepc インターフェイスは、数台の PC が存在する 10.30.30.0/24 ネットワークに接続されます。それらの PC が、同じネットワーク（すべて 10.30.30.0/24 の IP アドレスを持つ）に属するリモート VTEP の裏の VMs/PCs（表示されません）と通信する場合、ASA は VXLAN タグ 10000 を使用します。

ASA の設定

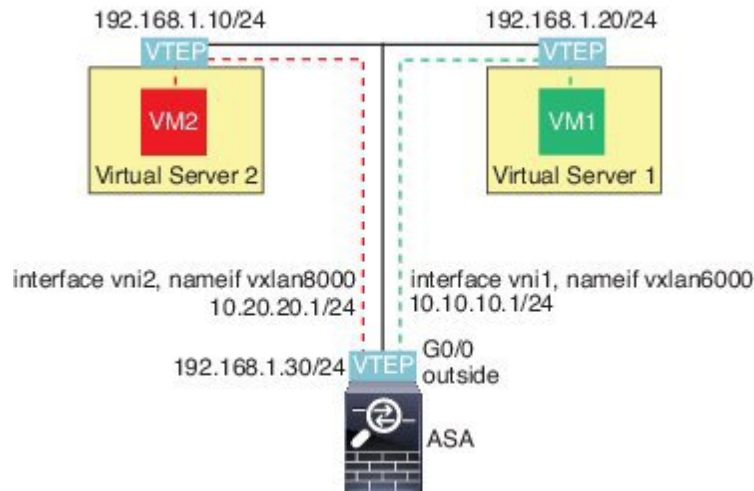
```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
  bridge-group 2
!
```

```
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
  ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
  ip address 10.30.30.1 255.255.255.0
```

注意

- VNI インタフェース `vni1` と `vni2` の場合、カプセル化時に内部 VLAN タグが削除されません。
- VNI インタフェース `vni2` と `vni3` は、マルチキャストでカプセル化された ARP に対して同じマルチキャスト IP アドレスを共有します。この共有は許可されます。
- ASA は、上記の BVI とブリッジグループ設定に基づいて VXLAN トラフィックを非 VXLAN でサポートされているインタフェースにブリッジします。拡張されたレイヤ 2 ネットワークの各セグメント（10.10.10.0/24、10.20.20.0/24、10.30.30.0/24）の場合、ASA はブリッジとして機能します。
- 複数の VNI または複数の通常のインタフェース（VLAN または単に物理インタフェース）をブリッジグループに設定できます。VXLAN セグメント ID から VLAN ID（物理インタフェース）の転送または関連付けは、宛先 MAC アドレスによって決定され、どちらかのインタフェースが宛先に接続されます。
- VTEP 送信元インタフェースは、インタフェース設定で `nve-only` によって示されるトランスペアレントファイアウォールモードのレイヤ 3 インタフェースです。VTEP 送信元インタフェースは、BVI インタフェースまたは管理インタフェースではありませんが、IP アドレスがあり、ルーティングテーブルを使用します。

VXLAN ルーティングの例



この例の次の説明を参照してください。

- VM1 (10.10.10.10) は仮想サーバ 1 にホストされ、VM2 (10.20.20.20) は仮想サーバ 2 にホストされます。
- VM1 のデフォルト ゲートウェイは ASA であり、仮想サーバ 1 と同じのポッドにありませんが、VM1 はそれを認識しません。VM1 は、そのデフォルト ゲートウェイの IP アドレスが 10.10.10.1 であることを認識します。同様に、VM2 はデフォルト ゲートウェイの IP アドレスが 10.20.20.1 であることを認識します。
- 仮想サーバ 1 および 2 の VTEP サポート型ハイパーバイザは、同じサブネットまたはレイヤ 3 ネットワーク（表示なし。この場合、ASA と仮想サーバのアップリンクに異なるネットワーク アドレスがある）経由で ASA と通信できます。
- VM1 のパケットは、そのハイパーバイザの VTEP によってカプセル化され、VXLAN トネリングを使用してそのデフォルト ゲートウェイに送信されます。
- VM1 がパケットを VM2 に送信すると、パケットはその観点からデフォルト ゲートウェイ 10.10.10.1 を介して送信されます。仮想サーバ 1 は 10.10.10.1 がローカルにないことを認識しているため、VTEP は VXLAN 経由でパケットをカプセル化し、ASA の VTEP に送信します。
- ASA で、パケットはカプセル化解除されます。VXLAN セグメント ID は、カプセル化解除時に取得されます。次に、ASA は、VXLAN セグメント ID に基づいて、VNI インターフェイス (vni1) に対応する内部フレームを再投入します。その後、ASA はルートルックアップを実行し、別の VNI インターフェイス (vni2) 経由で内部パケットを送信します。vni2 を経由するすべての出力パケットは、VXLAN セグメント 8000 でカプセル化され、VTEP 経由で外部に送信されます。
- 最後に、カプセル化されたパケットが仮想サーバ 2 の VTEP によって受信され、カプセル化解除され、VM2 に転送されます。

ASA の設定

```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
  ip address 10.10.10.1 255.255.255.0
!
```

VXLAN インターフェイスの履歴

表 23: VXLAN インターフェイスの履歴

機能名	リリース	機能情報
VXLAN のサポート	9.4(1)	<p>VXLAN のサポートが追加されました (VXLAN トンネル エンドポイント (VTEP) のサポートを含む)。ASA またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを定義できます。</p> <p>次の画面が導入されました。</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VNI Interface]</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [VXLAN]</p>



第 17 章

ルーテッドモードインターフェイスとトランスペアレントモードインターフェイス

この章では、ルーテッドファイアウォールモードおよびトランスペアレントファイアウォールモードですべてのモデルのインターフェイス コンフィギュレーションを実行するためのタスクについて説明します。



(注) マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

- [ルーテッドモードインターフェイスとトランスペアレントモードインターフェイスについて \(514 ページ\)](#)
- [ルーテッドモードおよびトランスペアレントモードのインターフェイスのガイドラインおよび要件 \(515 ページ\)](#)
- [ルーテッドモードのインターフェイスの設定 \(517 ページ\)](#)
- [トランスペアレントモードのブリッジグループインターフェイスの設定 \(521 ページ\)](#)
- [IPv6 アドレスの設定 \(526 ページ\)](#)
- [ルーテッドモードおよびトランスペアレントモードのインターフェイスのモニタリング \(535 ページ\)](#)
- [ルーテッドモードおよびトランスペアレントモードのインターフェイスの例 \(536 ページ\)](#)
- [ルーテッドモードおよびトランスペアレントモードのインターフェイスの履歴 \(537 ページ\)](#)

ルータードモードインターフェイスとトランスペアレントモードインターフェイスについて

ASA は、ルータードおよびブリッジという 2 つのタイプのインターフェイスをサポートします。

各レイヤ 3 ルータードインターフェイスは一意のサブネット上に IP アドレスを必要とします。

ブリッジインターフェイスはブリッジグループに属し、すべてのインターフェイスは同じネットワーク内にあります。ブリッジグループはブリッジネットワーク上に IP アドレスを持つブリッジ仮想インターフェイス (BVI) で表されます。ルータードモードはルータードインターフェイスのみをサポートします。トランスペアレントファイアウォールモードでは、ブリッジグループと BVI インターフェイスのみがサポートされます。

セキュリティ レベル

ブリッジグループメンバーインターフェイスを含む各インターフェイスには、0 (最下位) ~ 100 (最上位) のセキュリティレベルを設定する必要があります。たとえば、内部ホストネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティレベルに割り当てることができます。

トランスペアレントモードでは、BVI インターフェイスはインターフェイス間のルーティングに参加しないため、BVI インターフェイスにはセキュリティレベルが割り当てられていません。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティレベルのインターフェイスから低いセキュリティレベルのインターフェイスへの通信 (発信) は暗黙的に許可されます。高いセキュリティレベルのインターフェイス上のホストは、低いセキュリティレベルのインターフェイス上の任意のホストにアクセスできます。ACL をインターフェイスに適用して、アクセスを制限できます。

同じセキュリティレベルのインターフェイスの通信をイネーブルにすると、同じセキュリティレベルまたはそれより低いセキュリティレベルの他のインターフェイスにアクセスするインターフェイスは、暗黙的に許可されます。

- インспекションエンジン：一部のアプリケーションインспекションエンジンはセキュリティレベルに依存します。同じセキュリティレベルのインターフェイス間では、インспекションエンジンは発信と着信のいずれのトラフィックに対しても適用されます。
 - NetBIOS インспекションエンジン：発信接続に対してのみ適用されます。

- SQL*Net インспекション エンジン : SQL*Net (旧称 OraServ) ポートとの制御接続が一对のホスト間に存在する場合、着信データ接続だけが ASA を通過することが許可されます。

デュアル IP スタック (IPv4 および IPv6)

ASA は、インターフェイスで IPv6 アドレスと IPv4 アドレスの両方をサポートしています。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

ルーテッドモードおよびトランスペアレントモードのインターフェイスのガイドラインおよび要件

コンテキスト モード

- マルチコンテキストモードで設定できるのは、[マルチコンテキストの設定 \(253 ページ\)](#) に従ってシステムコンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- PPPoE は、マルチ コンテキスト モードではサポートされていません。
- トランスペアレント モードのマルチ コンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- トランスペアレント モードのマルチ コンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。

フェールオーバー

- フェールオーバー リンクは、この章の手順で設定しないでください。詳細については、フェールオーバーの章も参照してください。
- フェールオーバーを使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。

IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。
- ASA は、IPv6 エニーキャスト アドレスはサポートしません。

サポート モデル

- ASASM では、PPPoE および DHCP はサポートされません。

ASASM の VLAN ID

コンフィギュレーションにはあらゆる VLAN ID を追加できますが、トラフィックを転送できるのはスイッチによって ASA に割り当てられた VLAN だけです。ASA に割り当てられたすべての VLAN を表示するには、**show vlan** コマンドを使用します。

スイッチによって ASA にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウンステートになります。ASA に VLAN を割り当てた時点で、インターフェイスはアップステートに変化します。インターフェイスステートの詳細については、**show interface** コマンドを参照してください。

トランスペアレントモードとブリッジグループのガイドライン

- 4 のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方の各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされませんが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホストサブネット (255.255.255.255) を設定することはできません。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- トランスペアレントモードでは、少なくとも 1 つのブリッジグループを使用し、データインターフェイスがブリッジグループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは ASA の他方側のルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジグループネットワークからの管理トラフィックにだけ適用されます。これは、デフォルトルートはブリッジグループのインターフェイスとブリッジグループネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルトルートしか定義できないためです。複数のブリッジグループネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティックルートを指定する必要があります。

- トランスペアレントモードでは、PPPoEは管理インターフェイスでサポートされません。
- Bidirectional Forwarding Detection (BFD) エコーパケットは、ブリッジグループメンバを使用するときに、ASAを介して許可されません。BFDを実行しているASAの両側に2つのネイバーがある場合、ASAはBFDエコーパケットをドロップします。両方が同じ送信元および宛先IPアドレスを持ち、LAND攻撃の一部であるように見えるからです。

デフォルトのセキュリティレベル

デフォルトのセキュリティレベルは0です。インターフェイスに「inside」という名前を付けて、明示的にセキュリティレベルを設定しないと、ASAはセキュリティレベルを100に設定します。



- (注) インターフェイスのセキュリティレベルを変更したときに、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して接続をクリアできます。

ルーテッドモードのインターフェイスの設定

ルーテッドモードのインターフェイスを設定するには、次の手順を実行します。

ルーテッドモードの一般的なインターフェイスパラメータの設定

この手順では、名前、セキュリティレベル、IPv4アドレス、およびその他のオプションを設定する方法について説明します。

始める前に

マルチコンテキストモードでは、コンテキスト実行スペースで次の手順を実行します。システムコンフィギュレーションからコンテキストコンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスのIPアドレスの下にあるコンテキスト名をダブルクリックします。

手順

- ステップ 1** [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。
- ステップ 2** インターフェイス行を選択して、[Edit] をクリックします。
[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。
- ステップ 3** [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 4 [Security level] フィールドに、0（最低）～100（最高）のレベルを入力します。

ステップ 5 （任意）このインターフェイスを管理専用インターフェイスとして設定するには、[Dedicate this interface to management-only] チェックボックスをオンにします。

管理専用インターフェイスでは、通過トラフィックは受け入れられません。

（注） [Channel Group] フィールドは読み取り専用で、インターフェイスが EtherChannel の一部であるかどうかを示します。

ステップ 6 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

ステップ 7 IP アドレスを設定するには、次のいずれかのオプションを使用します。

（注） フェールオーバーで使用する場合、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブのスタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。

- IP アドレスを手動で設定するには、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。
 1. MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。

いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。
 2. オプション 61 用に生成された文字列を使用するには、[Use “Cisco-<MAC>-<interface_name>-<host>”] をクリックします。
 3. （任意）DHCP サーバからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。
 4. （オプション）アドミニストレーティブディスタンスを既知のルートに割り当てるには、[DHCP Learned Route Metric] フィールドに 1～255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブディスタンスは 1 になります。
 5. （任意）DHCP の既知のルートのトラッキングをイネーブルにするには、[Enable Tracking for DHCP Learned Routes] をオンにします。次の値を設定します。

[Track ID] : ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1～500 です。

[Track IP Address] : トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワークオブジェクトがあれば表示されます。

(注) ルートトラッキングは、シングルルーテッドモードでだけ使用できます。

[SLA ID] : SLA モニタリングプロセスの一意の識別子。有効な値は 1 ~ 2147483647 です。

[Monitor Options] : このボタンをクリックすると [Route Monitoring Options] ダイアログボックスが開きます。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリングプロセスのパラメータを設定できます。

6. (オプション) DHCP クライアントが IP アドレス要求の探索を送信する場合には、DHCP パケットヘッダーでブロードキャストフラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

DHCP サーバはこのブロードキャストフラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

7. (任意) リースを更新するには、[Renew DHCP Lease] をクリックします。

- (シングルモードのみ) PPPoE を使用して IP アドレスを取得するには、[Use PPPoE] をオンにします。

1. [Group Name] フィールドで、グループ名を指定します。
2. [PPPoE Username] フィールドで、ISP から提供されたユーザ名を指定します。
3. [PPPoE Password] フィールドで、ISP から提供されたパスワードを指定します。
4. [Confirm Password] フィールドに、パスワードを再入力します。
5. PPP 認証の場合、[PAP]、[CHAP]、または [MSCHAP] のいずれかのオプションボタンをクリックします。

PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリアテキストパスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

6. (オプション) フラッシュメモリにユーザ名とパスワードを保存するには、[Store Username and Password in Local Flash] チェックボックスをオンにします。

ASA は、NVRAM の特定の場所にユーザ名とパスワードを保存します。Auto Update Server が **clear config** コマンドを ASA に送信して、接続が中断されると、ASA は NVRAM からユーザ名とパスワードを読み取り、アクセスコンセントレータに対して再度認証できます。

7. (オプション) [PPPoE IP Address and Route Settings] ダイアログボックスを表示し、アドレスリングおよびトラッキングのオプションを選択するには、[IP Address and Route Settings] をクリックします。

ステップ 8 (オプション) [Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステートリンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステートリンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 9 [OK] をクリックします。

関連トピック

[IPv6 アドレスの設定](#) (526 ページ)

[物理インターフェイスのイネーブル化およびイーサネットパラメータの設定](#) (469 ページ)

[PPPoE の設定](#) (520 ページ)

PPPoE の設定

インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。

手順

ステップ 1 [Configuration] > [Interfaces] > [Add/Edit Interface] > [General] の順に選択し、[PPPoE IP Address and Route Settings] をクリックします。

ステップ 2 [IP Address] 領域で、次のいずれかを選択します。

- [Obtain IP Address using PPP] : IP アドレスを動的に設定します。
- [Specify an IP Address] : IP アドレスを手動で設定します。

ステップ 3 [Route Settings Area] で、次の設定を行います。

- [Obtain default route using PPPoE] : PPPoE クライアントがまだ接続を確立していない場合に、デフォルトルートを設定します。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。
- [PPPoE learned route metric] : アドミニストレーティブディスタンスを学習したルートに割り当てます。有効な値は、1 ~ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブディスタンスは 1 になります。
- [Enable tracking] : PPPoE の既知のルートのルートトラッキングをイネーブルにします。ルートトラッキングは、シングルルーテッドモードでだけ使用できます。

- [Primary Track] : プライマリ PPPoE ルート トラッキングを設定します。
- [Track ID] : ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ~ 500 です。
- [Track IP Address] : トラッキングの対象 IP アドレスを入力します。通常、ルートのネクスト ホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。
- [SLA ID] : SLA モニタリング プロセスの一意の識別子。有効な値は 1 ~ 2147483647 です。
- [Monitor Options] : このボタンをクリックすると [Route Monitoring Options] ダイアログボックスが開きます。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。
- [Secondary Track] : セカンダリ PPPoE ルート トラッキングを設定します。
- [Secondary Track ID] : ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ~ 500 です。

ステップ 4 [OK] をクリックします。

トランスペアレントモードのブリッジグループインターフェイスの設定

ブリッジグループは、ASA がルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレント ファイアウォール モードでのみサポートされています。ブリッジグループの詳細については、[ブリッジグループについて \(209 ページ\)](#) を参照してください。

ブリッジグループと関連インターフェイスを設定するには、次の手順を実行します。

ブリッジ仮想インターフェイス (BVI) の設定

ブリッジグループごとに、IP アドレスを設定する BVI が必要です。ASA は、ブリッジグループから発信されるパケットの送信元アドレスとしてこの IP アドレスを使用します。BVI IP アドレスは、接続されているネットワークと同じサブネット上になければなりません。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカルアドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

一部のモデルでは、デフォルト コンフィギュレーションにブリッジグループと BVI が含まれています。追加のブリッジグループおよび BVI を作成して、グループの間でメンバーインターフェイスを再割り当てすることもできます。



- (注) トランスペアレントモードの個別の管理インターフェイスでは（サポートされているモデルの場合）、設定できないブリッジグループ（ID301）がコンフィギュレーションに自動的に追加されます。このブリッジグループはブリッジグループの制限に含まれません。

手順

ステップ 1 [Configuration] > [Interfaces] の順に選択し、[Add] > [Bridge Group Interface] を選択します。

ステップ 2 [Bridge Group ID] フィールドに、1 ~ 250 の間のブリッジグループ ID を入力します。

このブリッジグループメンバーには、後で物理インターフェイスを割り当てます。

ステップ 3 IP アドレスを設定します。

- [IP Address] フィールドに、IPv4 アドレスを入力します。
- [Subnet Mask] フィールドにサブネットマスクを入力するか、またはメニューから選択します。

トランスペアレントファイアウォールにホストアドレス (/32 または 255.255.255.255) を割り当てないでください。また、/30 サブネットなど (255.255.255.252)、ホストアドレスが 3 つ未満（アップストリームルータ、ダウンストリームルータ、トランスペアレントファイアウォールにそれぞれ 1 つずつ）の他のサブネットを使用しないでください。ASA は、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリームルータへの予約アドレスを割り当てた場合、ASA はダウンストリームルータからアップストリームルータへの ARP 要求をドロップします。

ステップ 4 （オプション）[Description] フィールドに、このブリッジグループの説明を入力します。

ステップ 5 [OK] をクリックします。

ブリッジ仮想インターフェイス（BVI）が、物理およびサブインターフェイスとともに、インターフェイステーブルに追加されます。

ブリッジグループメンバーの一般的なインターフェイスパラメータの設定

この手順は、ブリッジグループメンバーインターフェイスの名前、セキュリティレベル、およびブリッジグループを設定する方法について説明します。

始める前に

- 同じブリッジグループで、さまざまな種類のインターフェイス（物理インターフェイス、VLAN サブインターフェイス、VNI インターフェイス、EtherChannel、冗長インターフェイス）を含めることができます。管理インターフェイスはサポートされていません。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration]>[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
- トランスペアレントモードの場合、管理インターフェイスにはこの手順を使用しないでください。管理インターフェイスを設定する場合は、[トランスペアレントモードの管理インターフェイスの設定（524 ページ）](#) を参照してください。

手順

ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。

BVI は、物理インターフェイス、サブインターフェイス、冗長インターフェイス、EtherChannel ポートチャンネルインターフェイスとともにテーブルに表示されます。マルチコンテキストモードでは、システム実行スペースでコンテキストに割り当てられたインターフェイスだけがテーブルに表示されます。

ステップ 2 非 BVI インターフェイスの行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3 [Bridge Group] ドロップダウン メニューで、このインターフェイスを割り当てるブリッジグループを選択します。

ステップ 4 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 5 [Security level] フィールドに、0（最低）～100（最高）のレベルを入力します。

ステップ 6 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

（注） [Channel Group] フィールドは読み取り専用で、インターフェイスが EtherChannel の一部であるかどうかを示します。

ステップ 7 （任意） モジュールを取り付けて非実稼働 ASA 上でモジュール機能をデモンストレーションする場合、[Forward traffic to the ASA module for inspection and reporting] チェックボックスをオンにします。詳細については、のモジュールに関する章またはクイック スタート ガイドを参照してください。

ステップ 8 （任意） [Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステートリンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。こ

のインターフェイスをフェールオーバーまたはステートリンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 9 [OK] をクリックします。

関連トピック

[手動 MAC アドレス、MTU、および TCP MSS の設定](#) (546 ページ)

トランスペアレントモードの管理インターフェイスの設定

トランスペアレントファイアウォールモードでは、すべてのインターフェイスがブリッジグループに属している必要があります。唯一の例外は管理インターフェイス（物理インターフェイス、サブインターフェイス（ご使用のモデルでサポートされている場合）、または管理インターフェイスを構成する EtherChannel インターフェイス（複数の管理インターフェイスがある場合）のいずれか）です。管理インターフェイスは個別の管理インターフェイスとして設定できます。Firepower 9300 シャーシでは、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt タイプ インターフェイスに基づいています。他のインターフェイスタイプは管理インターフェイスとして使用できません。シングルモードまたはコンテキストごとに1つの管理インターフェイスを設定できます。詳細については、[トランスペアレントモードの管理インターフェイス](#) (466 ページ) を参照してください。

始める前に

- このインターフェイスをブリッジグループに割り当てないでください。設定できないブリッジグループ (ID301) は、コンフィギュレーションに自動的に追加されます。このブリッジグループはブリッジグループの制限に含まれません。
- モデルに管理インターフェイスが含まれていない場合、データインターフェイスからトランスペアレントファイアウォールを管理する必要があります。この手順はスキップします。（たとえば、ASASM の場合。） Firepower 9300 シャーシでは、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt-type インターフェイスに基づいています。
- マルチコンテキストモードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。データインターフェイスに接続する必要があります。
- マルチコンテキストモードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキストコンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。

ステップ 2 管理インターフェイス、サブインターフェイス、または管理インターフェイスからなる EtherChannel ポートチャネル インターフェイスの行を選択して、[Edit] をクリックします。
[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

Firepower 9300 シャーシでは、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt タイプ インターフェイス（個別インターフェイスまたは EtherChannel インターフェイス）に基づいています。

ステップ 3 [Bridge Group] ドロップダウンメニューで、デフォルトの [--None--] のままにします。管理インターフェイスをブリッジグループに割り当てることはできません。

ステップ 4 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 5 [Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

(注) [Dedicate this interface to management only] チェックボックスは、デフォルトでイネーブルであり、設定することはできません。

ステップ 6 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

ステップ 7 IP アドレスを設定するには、次のいずれかのオプションを使用します。

(注) フェールオーバーとともに使用する場合は、IP アドレスとスタンバイアドレスを手動で設定する必要があります。DHCP はサポートされません。[Configuration]>[Device Management]>[High Availability]>[Failover]>[Interfaces] タブのスタンバイ IP アドレスを設定します。

- IP アドレスを手動で設定するには、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。
 - MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。
いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。
 - オプション 61 用に生成された文字列を使用するには、[Use “Cisco-<MAC>-<interface_name>-<host>”] をクリックします。
 - (任意) DHCP サーバからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。
 - (オプション) DHCP クライアントが IP アドレス要求の探索を送信する場合に、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

DHCP サーバはこのブロードキャストフラグをリッスンし、フラグが1に設定されている場合は応答パケットをブロードキャストします。

- (任意) リースを更新するには、[Renew DHCP Lease] をクリックします。

ステップ 8 (オプション) [Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 9 [OK] をクリックします。

IPv6 アドレスの設定

この項では、IPv6 アドレッシングを設定する方法について説明します。

IPv6 について

このセクションには、IPv6 に関する情報が含まれています。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャストアドレスを設定できます。

- **グローバル** : グローバルアドレスは、パブリック ネットワークで使用可能なパブリックアドレスです。ブリッジグループの場合、このアドレスは各メンバー インターフェイスごとに設定するのではなく、BVI用に設定する必要があります。また、トランスペアレントモードで管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- **リンクローカル** : リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベートアドレスです。ルータは、リンクローカルアドレスを使用してパケットを転送するのではなく、特定の物理ネットワークセグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決などの Neighbor Discovery 機能に使用できます。ブリッジグループでは、メンバー インターフェイスのみがリンクローカルアドレスを所有しています。BVI にはリンクローカルアドレスはありません。

最低限、IPv6 が動作するようにリンクローカルアドレスを設定する必要があります。グローバルアドレスを設定すると、リンクローカルアドレスがインターフェイスに自動的に設定されるため、リンクローカルアドレスを個別に設定する必要はありません。ブリッジグループ インターフェイスでは、BVIでグローバルアドレスを設定した場合、ASAが自動的にメンバー インターフェイスのリンクローカルアドレスを生成します。グローバルアドレスを設定しない場合は、リンクローカルアドレスを自動的にするか、手動で設定する必要があります。

Modified EUI-64 インターフェイス ID

RFC 3513 「Internet Protocol Version 6 (IPv6) Addressing Architecture」 (インターネットプロトコルバージョン6アドレッシングアーキテクチャ) では、バイナリ値000で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。ASAでは、ローカルリンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスでイネーブルになっていると、そのインターフェイスIDがModified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合のみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカルリンク上のホストに対してのみ実行できます。

グローバル IPv6 アドレスの設定

ルーテッドモードの任意のインターフェイスとトランスペアレントモードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。



(注) グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。

サブインターフェイスの場合、親インターフェイスの同じ Burned-In MAC Address を使用するので、MAC アドレスも手動で設定することをお勧めします。IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。[手動MACアドレス、MTU、およびTCP MSSの設定 \(546 ページ\)](#) を参照してください。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration]>[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

トランスペアレントモードの場合、BVIを選択します。トランスペアレントモードの場合は、管理専用インターフェイスも選択できます。

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 [Enable IPv6] チェックボックスをオンにします。

ステップ 5 (任意) ローカルリンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

ステップ 6 (ルーテッドインターフェイス) グローバル IPv6 アドレスを次のいずれかの方法で設定します。

- ステートレス自動設定：[Interface IPv6 Addresses] 領域で、[Enable address autoconfiguration] チェックボックスをオンにします。

インターフェイス上でステートレス自動設定をイネーブルにすると、受信したルータアドバタイズメントメッセージのプレフィックスに基づいて IPv6 アドレスを設定します。ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカルアドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

(注) RFC 4862 では、ステートレスな自動設定に設定されたホストはルータアドバタイズメントメッセージを送信しないと規定していますが、ASAはこの場合、ルータアドバタイズメントメッセージを送信します。メッセージを抑制するには、[Suppress RA] チェックボックスをオンにします。

- 手動設定：グローバル IPv6 アドレスを手動で設定するには、次の手順を実行します。

1. [Interface IPv6 Addresses] 領域で、[Add] をクリックします。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

2. [Address/Prefix Length] フィールドに入力する値は、使用方法によって異なります。

- 完全なグローバルアドレス：手動でアドレス全体を入力する場合は、完全なアドレスに加え、プレフィックス長を入力します。

- Modified EUI 64 形式：IPv6 プレフィックスとプレフィックス長を入力した後、[EUI 64] チェックボックスをオンにします。これにより、Modified EUI 64 形式を使用してインターフェイス ID が生成されるようになります。たとえば、2001:0DB8::BA98:0:3210/48 (完全なアドレス) または 2001:0DB8::/48 (プレフィックス、[EUI 64] はオン)。

3. [OK] をクリックします。

ステップ7 (BVIインターフェイス) BVIに手動でグローバルアドレスを割り当てます。トランスペアレントモードの管理インターフェイスでも、この方法を使用します。

a) [Interface IPv6 Addresses] 領域で、[Add] をクリックします。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

b) [Address/Prefix Length] フィールドに、完全なグローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。

c) [OK] をクリックします。

ステップ8 [OK] をクリックします。

[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインに戻ります。

(オプション) リンクローカルアドレスの自動設定

グローバルアドレスを設定する必要がなく、リンクローカルアドレスだけを設定する必要がある場合は、リンクローカルアドレスをインターフェイスの MAC アドレス (Modified EUI-64 形式。MAC アドレスで使用するビット数は 48 ビットであるため、インターフェイス ID に必要な 64 ビットを埋めるために追加ビットを挿入する必要があります。)

リンクローカルアドレスをインターフェイスに自動的に設定するには、次の手順を実行します。

始める前に

ルーテッドモードのみでサポートされます。

手順

ステップ1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。

ステップ2 インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ3 [IPv6] タブをクリックします。

ステップ4 [IPv6 configuration] 領域で、[Enable IPv6] チェックボックスをオンにします。

このオプションでは、IPv6 をイネーブルにし、インターフェイスの MAC アドレスに基づく Modified EUI-64 インターフェイス ID を使用してリンクローカルアドレスを自動的に生成します。

ステップ5 [OK] をクリックします。

(オプション) リンクローカルアドレスの手動設定

グローバルアドレスを設定する必要がなく、リンクローカルアドレスだけを設定する必要がある場合は、リンクローカルアドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカルアドレスを自動的に割り当てることを推奨します。たとえば、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカルアドレスの packets はドロップされる可能性があります。

インターフェイスにリンクローカルアドレスを割り当てるには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ブリッジグループの場合は、ブリッジグループ メンバー インターフェイスを選択します。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 (任意) ローカルリンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

ステップ 5 リンクローカルアドレスを設定するには、[Link-local address] フィールドにアドレスを入力します。

リンクローカルアドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。たとえば fe80::20d:88ff:feec:6a82 のようになります。IPv6 アドレッシングの詳細については、[IPv6 アドレス \(1069 ページ\)](#) を参照してください。

ステップ 6 [OK] をクリックします。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび送信要求ノード マルチキャスト アドレスを使用して、同じネットワーク (ローカルリンク) 上のネイバーのリンク層アドレスを決定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード (ホスト) はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失敗すると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

手順

- ステップ 1** [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。
- ステップ 2** IPv6 ネイバーの設定を行う IPv6 インターフェイスを選択し、[Edit] をクリックします。
- ステップ 3** [IPv6] タブをクリックします。
- ステップ 4** 許可される [DAD Attempts] の回数を入力します。

値の範囲は 0 ～ 600 です。この値が 0 の場合、指定されたインターフェイスでの DAD 処理が無効化されます。デフォルト値は 1 件です。

DAD は、割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認し、ネットワークに重複する IPv6 アドレスが検出されていないかをリンク ベースで確認します。ASA は、ネイバー送信要求メッセージを使用して、DAD を実行します。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上で IPv6 パケットの処理はディセーブルになります。重複アドレスがグローバルアドレスであれば、そのアドレスは使用されません。

- ステップ 5** [NS Interval] (ミリ秒単位) に入力して、IPv6 ネイバー要請メッセージの再送信間隔を設定します。

value 引数の有効な値は、1000 ～ 3600000 ミリ秒です。

ローカル リンク上にある他のノードのリンクレイヤアドレスを検出するため、ノードからネイバー送信要求メッセージ (ICMPv6 Type 135) がローカル リンクに送信されます。ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバーアドバタイズメントメッセージ (ICMPv6 Type 136) をローカル リンク上に送信して応答します。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがネイバーの到達可能性を確認するときに、ネイバー送信要求メッセージの宛先アドレスは、ネイバーのユニキャストアドレスです。

ネイバーアドバタイズメントメッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。

- ステップ 6** [Reachable Time] (秒単位) に入力して、リモート IPv6 ノードに到達可能な時間を設定します。
- 到達可能時間を 0 ～ 3600000 ミリ秒で設定します。時間を 0 に設定すると、到達可能時間は「不明」として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

ステップ 7 [RA Lifetime] (秒単位) に入力して、ローカルリンク上のノードが、ASA をリンク上のデフォルト ルータと見なす時間の長さを設定します。

値の範囲は 0 ～ 9000 秒です。0 を入力すると、ASA は選択したインターフェイスのデフォルト ルータと見なされません。

ステップ 8 ルータ アドバタイズメントを抑制するには、[Suppress RA] チェックボックスをオンにします。

ルータ要請メッセージ (ICMPv6 Type 133) に応答して、ルータ アドバタイズメントメッセージ (ICMPv6 Type 134) が自動的に送信されます。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

ASA で IPv6 プレフィックスを提供する必要がないインターフェイス (外部インターフェイスなど) では、これらのメッセージをディセーブルにできます。

このオプションを有効にすると、ASA がリンク上では IPv6 ルータではなく、通常の IPv6 ネイバーのように見えるようになります。

ステップ 9 [RA Interval] に入力して、IPv6 ルータ アドバタイズメントの送信間隔を設定します。

有効値の範囲は 3 ～ 1800 秒です。デフォルトは 200 秒です。

ルータ アドバタイズメント送信間隔の値をミリ秒単位で追加するには、[RA Interval in Milliseconds] チェックボックスをオンにして、500 ～ 1800000 の範囲で値を入力します。

ステップ 10 [Hosts should use DHCP for address config] チェックボックスをオンにして、取得されるステートレス自動設定のアドレス以外のアドレスの取得には DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

このオプションは、IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定します。

ステップ 11 [Hosts should use DHCP for non-address config] チェックボックスをオンにして、DNS サーバアドレスなどの追加情報を DHCPv6 から取得するには DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

このオプションは、IPv6 ルータ アドバタイズメント パケットのその他のアドレス設定フラグを設定します。

ステップ 12 IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定します。

a) [Interface IPv6 Prefixes] 領域で、[Add] をクリックします。

b) デフォルトのプレフィックスを使用するには、[Address/Prefix Length] に入力するか、[Default] チェック ボックスをオンにします。

- c) IPv6 アドレスを手動で設定するようにホストに強制するには、[No Auto-Configuration] チェックボックスをオンにします。指定したプレフィックスのローカルリンク上のホストでは、IPv6 自動設定を使用できません。
- d) プレフィックスアドバタイズメントを無効にするには、[No Advertisements] チェックボックスをオンにします。
- e) 指定したプレフィックスをオフリンクとして設定するには、[Off Link] チェックボックスをオンにします。プレフィックスはLビットクリアでアドバタイズされます。プレフィックスは、接続されたプレフィックスとしてルーティングテーブルに挿入されません。
- f) [Prefix Lifetime] 領域で、[Lifetime Duration] または [Lifetime Expiration Date] を指定します。

優先有効期間を過ぎると、アドレスは廃止状態になります。廃止状態のアドレスの使用は推奨されませんが、固く禁じられているわけではありません。有効期間の期限が切れた後に、アドレスは無効になり、使用できません。有効ライフタイムは優先ライフタイムと同じかそれより長い必要があります。

- [Lifetime Duration] : 値の範囲は0～4294967295です。デフォルトの有効期間は2592000 (30日間) です。デフォルトの優先有効期間は604800 (7日間) です。最大値は無限大です。
- [Lifetime Expiration Date] : 有効かつ優先する月と日をドロップダウンリストから選択し、時間を hh:mm 形式で入力します。

- g) [OK] をクリックして設定内容を保存します。

ステップ 13 [OK] をクリックします。

ステップ 14 スタティック IPv6 ネイバーを設定します。

次のガイドラインと制限事項は、スタティック IPv6 ネイバーの設定に適用されます。

- この機能は、スタティック ARP エントリの追加に似ています。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティックエントリに変換されます。これらのエントリは、copy コマンドを使用して設定を保存するときに設定に保存されます。
- IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。
- 生成された ICMP syslog は、IPv6 ネイバー エントリの定期的な更新に起因します。IPv6 ネイバー エントリの ASA デフォルト タイマーは30秒であるため、ASA は30秒おきに ICMPv6 ネイバー探索および応答パケットを生成します。ASA にフェールオーバー LAN および IPv6 アドレスで設定された状態インターフェイスの両方がある場合は、30秒ごとに、ICMPv6 ネイバー探索および応答パケットが、設定済みのリンクローカル IPv6 アドレスの両方の ASA で生成されます。また、各パケットは複数の syslog (ICMP 接続およびローカルホストの作成またはティアダウン) を生成するため、連続 ICMP syslog が生成されているように見ることがあります。IPv6 ネイバー エントリのリフレッシュ時間は、通常データ インターフェイスに設定可能ですが、フェールオーバー インターフェイスでは設定可能ではありません。ただし、この ICMP ネイバー探索トラフィックの CPU の影響はわずかです。

[ダイナミックに検出されたネイバーの表示とクリア \(534 ページ\)](#) も参照してください。

- a) [Configuration] > [Device Management] > [Advanced] > [IPv6 Neighbor Discovery Cache] を選択します。
- b) [Add] をクリックします。
[Add IPv6 Static Neighbor] ダイアログボックスが表示されます。
- c) [Interface Name] ドロップダウンリストから、ネイバーを追加するインターフェイスを選択します。
- d) [IP Address] フィールドにローカルデータリンク アドレスに対応する IPv6 アドレスを入力するか、省略符号 ([...]) をクリックしてアドレスを参照します。
- e) [MAC address] フィールドに、ローカルのデータ回線 (ハードウェア) MAC アドレスを入力します。
- f) [OK] をクリックします。

ステップ 15 [Apply] をクリックして、実行コンフィギュレーションを保存します。

ダイナミックに検出されたネイバーの表示とクリア

ホストまたはノードがネイバーと通信する場合、ネイバーはネイバー探索キャッシュに追加されます。ネイバーがキャッシュから削除されるのは、そのネイバーとの通信が行われなくなったときです。

ダイナミックに検出されたネイバーを表示し、そのネイバーを IPv6 ネイバー探索キャッシュから削除するには、次の手順を実行します。

手順

ステップ 1 [Monitoring] > [Interfaces] > [IPv6 Neighbor Discovery Cache] を選択します。

[IPv6 Neighbor Discovery Cache] ペインでは、スタティックおよびダイナミックに検出されたネイバーをすべて表示できます。

ステップ 2 ダイナミックに検出されたネイバーをすべてキャッシュから削除するには、[Clear Dynamic Neighbor Entries] をクリックします。

ダイナミックに検出されたネイバーがキャッシュから削除されます。

(注) この手順では、ダイナミックに検出されたネイバーだけがキャッシュから削除され、スタティックなネイバーは削除されません。

ルーテッドモードおよびトランスペアレントモードのインターフェイスのモニタリング

インターフェイスの統計情報、ステータス、PPPoEなどをモニタできます。

インターフェイス統計情報

- **[Monitoring] > [Interfaces] > [Interface Graphs]**

インターフェイスの統計情報をグラフ形式またはテーブル形式で表示できます。インターフェイスをコンテキスト間で共有している場合、ASAには現在のコンテキストの統計情報だけが表示されます。サブインターフェイスに表示される統計情報の数は、物理インターフェイスに表示される統計情報の数のサブセットです。

- **[Monitoring] > [Interfaces] > [Interface Graphs] > [Graph/Table]**

選択した統計情報のグラフを表示します。[Graph] ウィンドウには、最大4つのグラフおよびテーブルを同時に表示することができます。デフォルトで、グラフまたはテーブルにリアルタイムな統計情報が表示されます。履歴メトリックをイネーブルにすると、過去の期間の統計情報を表示できます。

スタティックルートトラッキング

- **[Monitoring] > [Interfaces] > [interface connection] > [Track Status]**

追跡対象オブジェクトに関する情報を表示します。

- **[Monitoring] > [Interfaces] > [interface connection] > [Monitoring Statistics]**

SLA モニタリングプロセスの統計情報を表示します。

PPPoE

- **[Monitoring] > [Interfaces] > [PPPoE Client] > [PPPoE Client Lease Information]**

現在のPPPoE接続に関する情報を表示します。

ダイナミックACL

- **[Monitoring] > [Interfaces] > [Dynamic ACLs]**

ダイナミックACLのテーブルを表示します。ダイナミックACLは、ASAによって自動的に作成、アクティブ化、および削除される点を除いて、ユーザ設定のACLと機能上同じです。これらのACLはコンフィギュレーションには表示されず、このテーブルだけに表示されます。ダイナミックACLは、ACLヘッダーの“(dynamic)”キーワードで区別されます。

ルーテッドモードおよびトランスペアレントモードのインターフェイスの例

2つのブリッジグループを含むトランスペアレントモードの例

トランスペアレントモードの次の例では、3つのインターフェイスそれぞれの2つのブリッジグループと管理専用インターフェイスを示します。

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

ルーテッドモードおよびトランスペアレントモードのインターフェイスの履歴

機能名	プラットフォーム リリース	機能情報
IPv6 ネイバー探索	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Monitoring] > [Interfaces] > [IPv6 Neighbor Discovery Cache.Configuration] > [Device Management] > [Advanced] > [IPv6 Neighbor Discovery Cache.Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [IPv6]。
トランスペアレントモードの IPv6 のサポート	8.2(1)	トランスペアレントファイアウォールモードの IPv6 サポートが導入されました。
トランスペアレントモードのブリッジグループ	8.4(1)	セキュリティコンテキストのオーバーヘッドを避けたい場合、またはセキュリティコンテキストを最大限に使用したい場合、インターフェイスをブリッジグループにグループ化し、各ネットワークに1つずつ複数のブリッジグループを設定できます。ブリッジグループのトラフィックは他のブリッジグループから隔離されます。シングルモードまたはコンテキストごとに、それぞれ4つのインターフェイスからなる最大8個のブリッジグループを設定できます。 次の画面が変更または導入されました。 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]

機能名	プラットフォーム リリース	機能情報
IPv6 DHCP リレーのアドレス設定フラグ	9.0(1)	次の画面が変更されました。 [Configuration] > [Device Setup] > [Interfaces] > [IPv6]。
トランスペアレントモードのブリッジグループの最大数が 250 に増加	9.3(1)	<p>ブリッジグループの最大数が 8 個から 250 個に増えました。シングルモードでは最大 250 個、マルチモードではコンテキストあたり最大 8 個のブリッジグループを設定でき、各ブリッジグループには最大 4 個のインターフェイスを追加できます。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface]</p> <p>[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]</p>



第 18 章

高度なインターフェイス設定

この章では、インターフェイスのMACアドレスを設定する方法、最大伝送ユニット (MTU) を設定する方法、TCP最大セグメントサイズ (TCP MSS) を設定する方法、および同じセキュリティ レベルの通信を許可する方法について説明します。最高のネットワーク パフォーマンスを実現するには、正しい MTU と最大 TCP セグメント サイズの設定が不可欠です。

- [高度なインターフェイス設定について \(539 ページ\)](#)
- [マルチ コンテキスト モードでの MAC アドレスの自動割り当て \(545 ページ\)](#)
- [手動 MAC アドレス、MTU、および TCP MSS の設定 \(546 ページ\)](#)
- [同一のセキュリティ レベル通信の許可 \(548 ページ\)](#)
- [ARP および MAC アドレス テーブルのモニタリング \(548 ページ\)](#)
- [インターフェイスの詳細設定の履歴 \(549 ページ\)](#)

高度なインターフェイス設定について

この項では、インターフェイスの高度な設定について説明します。

MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、(コンテキストに割り当てられているすべてのインターフェイスの) 一意の MAC アドレスと。



- (注) 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは、Burned-in MAC Address を使用します。
- 冗長インターフェイス：冗長インターフェイスでは、最初に追加された物理インターフェイスの MAC アドレスが使用されます。構成でメンバーインターフェイスの順序を変更すると、MAC アドレスがリストの先頭にあるインターフェイスの MAC アドレスと一致するように変更されます。冗長インターフェイスに MAC アドレスを割り当てると、メンバーインターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。
- EtherChannel (Firepower Models)：EtherChannel の場合は、そのチャンネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないからです。ポートチャンネルインターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。
- EtherChannel (ASA モデル)：ポートチャンネルインターフェイスは、最も小さいチャンネルグループインターフェイスの MAC アドレスをポートチャンネル MAC アドレスとして使用します。または、ポートチャンネルインターフェイスの MAC アドレスを設定することもできます。グループチャンネルインターフェイスのメンバーシップが変更された場合に備えて、一意の MAC アドレスを設定することを推奨します。ポートチャンネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャンネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス：物理インターフェイスのすべてのサブインターフェイスは同じ Burned-In MAC Address を使用します。サブインターフェイスに一意の MAC アドレスを割り当てる必要がある場合があります。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセスコントロールを実行する場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。
- ASASM VLAN：ASASM では、すべての VLAN がバックプレーンから提供される同じ MAC アドレスを使用します。

自動 MAC アドレス

マルチ コンテキスト モードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効になっている場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2xx.yyzz.zzzz

xx.yy はユーザ定義プレフィックスまたはインターフェイス MAC アドレスの最後の 2 バイトに基づいて自動生成されるプレフィックスです。zz.zzzz は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D (yyxx) に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます (xxyy)。

A24D.00zz.zzzz

プレフィックス 1009 (03F1) の場合、MAC アドレスは次のようになります。

A2F1.03zz.zzzz



(注) プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンドリファレンスの **mac-address auto** コマンドを参照してください。

MTU について

MTU は、ASA が特定のイーサネットインターフェイスで送信する最大フレームペイロードサイズを指定します。MTU の値は、イーサネットヘッダー、VLAN タギング、他のオーバーヘッドを含まないフレームサイズです。たとえば、MTU を 1500 に設定すると、予想されるフレームサイズは、ヘッダーを含めて 1518 バイトです。または、VLAN を使用している場合は、1522 バイトです。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

VXLAN については、イーサネット データグラム全体がカプセル化されるため、新しい IP パケットにより大きな MTU が必要です。ASA VTEP 送信元インターフェイスの MTU を 54 バイト以上のネットワーク MTU に設定する必要があります。

『Path MTU Discovery』

ASA は、Path MTU Discovery (RFC 1191 の定義に従う) をサポートします。つまり、2 台のホスト間のネットワークパス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

デフォルト MTU

ASA のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、VLAN タギングや他のオーバーヘッドのための 18~22 バイト以上は含まれません。

VTEP 送信元インターフェイスの VXLAN を有効にし、MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットにはより大きな MTU が必要です。一般的には、ASA ソースインターフェイス MTU をネットワーク MTU + 54 バイトに設定する必要があります。

MTU とフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは送信先（場合によっては中継先）で組立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットはフラグメント化を許可されていません。したがってフラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

TCP パケットでは、通常、エンドポイントは MTU を使用して TCP の最大セグメント サイズ（たとえば、MTU - 40）を判別します。途中で追加の TCP ヘッダーが追加された場合（たとえば、サイト間 VPN トンネル）、TCP MSS はトンネリング エンティティで下方調整しないといけない場合があります。TCP MSS について (543 ページ) を参照してください。

UDP または ICMP では、フラグメンテーションを回避するために、アプリケーションは MTU を考慮する必要があります。



(注) ASA はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信できます。

MTU とジャンボ フレーム

より大きな MTU は、より大きなパケットの送信が可能です。より大きなパケットは、ネットワークにとってより効率的な場合があります。次のガイドラインを参照してください。

- トラフィック パスの MTU の一致：すべての ASA インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームに対応する：ジャンボ フレームを有効にすると、MTU を最大 9198 バイトに設定できます。最大値は、Firepower 9300 シャーシの ASA v で 9000、ASA です。



(注) ASA 5585-X と Firepower 9300 では、VLAN タギングを使用している場合、最大 MTU は 4 バイト小さいです：ASA 5585-X では 9194、Firepower 9300 では 8996 です。

TCP MSS について

最大セグメントサイズ (TCP MSS) とは、あらゆる TCP および IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

を参照してください。デフォルトでは、最大 TCP MSS は 1380 バイトに設定されます。この設定は、ASA が IPsec VPN カプセル化のパケットサイズを追加する必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、ASA の最大 TCP MSS を無効にする必要がありません。

最大 TCP MSS を設定している場合、接続のいずれかのエンドポイントが ASA に設定された値を超える TCP MSS を要求すると、ASA は要求パケット内の TCP MSS を ASA の最大サイズで上書きします。ホストまたはサーバが TCP MSS を要求しない場合、ASA は RFC 793 のデフォルト値 536 バイト (IPv4) または 1220 バイト (IPv6) を想定しますが、パケットは変更しません。たとえば、MTU をデフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。ASA の最大 TCP MSS が 1380 (デフォルト) の場合、ASA は TCP 要求パケットの MSS 値を 1380 に変更します。その後、サーバは、1380 バイトのペイロードを含むパケットを送信します。ASA は、最大 120 バイトのヘッダーをパケットに追加しても、1500 バイトの MTU サイズに適応することができます。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、ASA は値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含め、to-the-box トラフィックの場合、この設定は適用されません。ASA は MTU を使用して、TCP MSS を導き出します。MTU - 40 (IPv4) または MTU - 60 (IPv6) となります。

デフォルト TCP MSS

デフォルトでは、ASA の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU のデフォルトの 1500 バイト内にも収まっています。

TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、ASA が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。ASA が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして ASA を使用しない場合は、FlexConfig の Sysopt_Basic オブジェクトを使用して TCP MSS 設定を参照してください。次のガイドラインを参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。通常、接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。

- IPv4 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボフレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。
- IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

インターフェイス間通信

同じセキュリティレベルのインターフェイスで相互通信を許可する利点としては、次のものがあります。

- 101 より多い数の通信インターフェイスを設定できます。
各インターフェイスで異なるセキュリティレベルを使用したときに、同一のセキュリティレベルにインターフェイスを割り当てないと、各レベル（0～100）に1つのインターフェイスしか設定できません。
- ACL がなくても同じセキュリティレベルのインターフェイスすべての中で自由にトラフィックが流れるようにできます。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティレベルで通常どおりインターフェイスを設定できます。

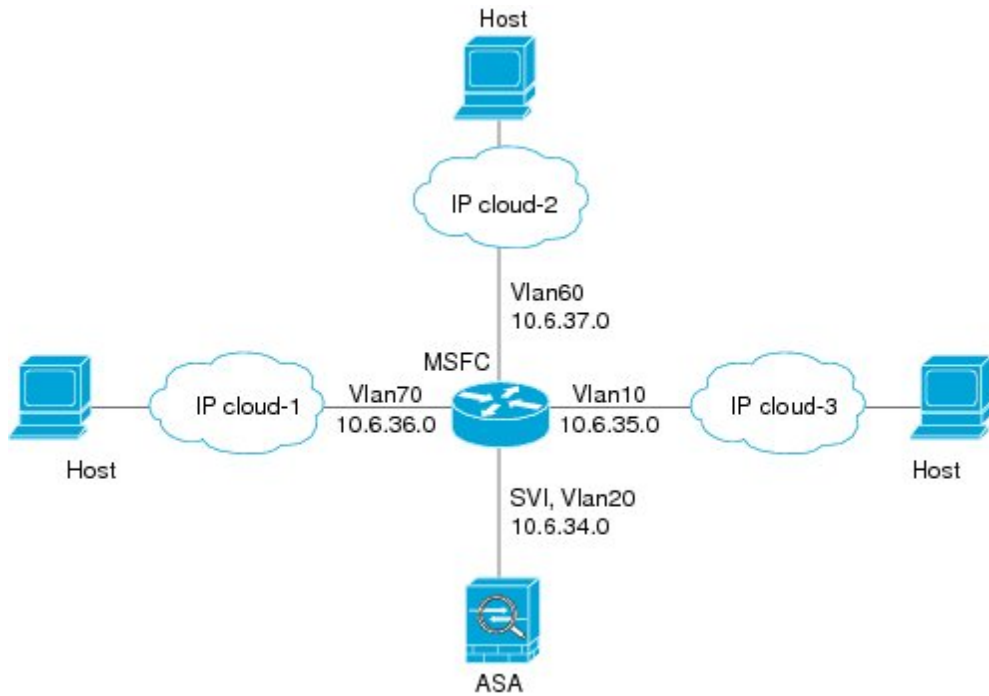
インターフェイス内通信（ルーテッドファイアウォールモード）

インターフェイス内通信は、インターフェイスに入ってくる VPN トラフィックに対して使用できますが、その場合は同じインターフェイスのルートから外されます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブアンドスポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。



- (注) この機能で許可されたすべてのトラフィックは、引き続きファイアウォール規則に従います。リターントラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

ASASM の場合、この機能をイネーブルにするには、まず、パケットがスイッチ経由で宛先ホストに直接送信されるのではなく、ASA の MAC アドレスに送信されるように、MSFC を正しく設定する必要があります。次の図に、同一インターフェイス上のホストが通信する必要があるネットワークを示します。



次の設定例では、次の図に示すネットワークのポリシー ルーティングをイネーブルにするために使用される Cisco IOS **route-map** コマンドを示します。

```

route-map intra-inter3 permit 0
  match ip address 103
  set interface Vlan20
  set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
  match ip address 102
  set interface Vlan20
  set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
  match ip address 101
  set interface Vlan20
  set ip next-hop 10.6.34.7

```

マルチ コンテキスト モードでの MAC アドレスの自動割り当て

この項では、MAC アドレスの自動生成の設定方法について説明します。マルチ コンテキスト モードの場合、この機能によって、コンテキストに割り当てられたすべてのインターフェイス タイプに一意的な MAC アドレスが割り当てられます。

始める前に

- インターフェイスの名前を設定すると、ただちに新規 MAC アドレスが生成されます。インターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。
- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある **[System]** をダブルクリックします。

手順

ステップ 1 システムで次の手順を実行します。

- a) **[Configuration] > [Context Management] > [Security Contexts]** の順に選択します。
- b) **[Mac-Address auto]** をオンにします。
- c) (任意) **[Prefix]** チェックボックスをオンにしてから、フィールドに 0 ~ 65535 の範囲内の 10 進数値を入力します。

このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。プレフィックスを入力しない場合は、ASA によって、インターフェイス MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

ステップ 2 **[Apply]** をクリックします。

手動 MAC アドレス、MTU、および TCP MSS の設定

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。

ステップ 2 インターフェイス行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 MTU を設定する場合、またはジャンボ フレームのサポートをイネーブルにする場合（サポート対象モデルのみ）、[MTU] フィールドに 300 ~ 9198（ASA の場合は 9000、Firepower 9300 シャーシの場合は）バイトの範囲で値を入力します。

デフォルトは 1500 バイトです。

(注) 冗長インターフェイスまたはポートチャンネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバー インターフェイスに適用します。

- ジャンボフレームをサポートする、シングルモードのモデルの場合：いずれかのインターフェイスに 1500 を超える値を入力すると、ジャンボフレーム サポートがすべてのインターフェイスに対して自動的にイネーブルになります。すべてのインターフェイスの MTU の設定を 1500 未満に戻すと、ジャンボフレーム サポートがディセーブルになります。
- ジャンボフレームをサポートするマルチモードの場合：いずれかのインターフェイスに 1500 を超える値を入力する場合、必ずシステムコンフィギュレーションのジャンボフレーム サポートをイネーブルにしてください。 [ジャンボフレームサポートの有効化 \(471 ページ\)](#) を参照してください。

(注) ジャンボフレーム サポートをイネーブルまたはディセーブルにするには、ASA をリロードする必要があります。

ステップ 5 MAC アドレスをこのインターフェイスに手動で割り当てるには、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ステップ 6 フェールオーバーを使用する場合、[Standby Mac Address] フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイアドレスを使用します。

ステップ 7 TCP MSS を設定するには、[Configuration] > [Firewall] > [Advanced] > [TCP Options] の順に選択します。 次のオプションを設定します。

- [Force Maximum Segment Size for TCP]：最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能は、0 バイトに設定することによってディセーブルにできます。

- [Force Minimum Segment Size for TCP] : 48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメントサイズを上書きします。この機能は、デフォルトでディセーブルです (0 に設定)。

ステップ 8 [Secure Group Tagging] 設定については、ファイアウォール コンフィギュレーション ガイドを参照してください。

ステップ 9 [ASA Cluster] 設定については、[\(推奨、マルチ コンテキスト モードでは必須\) マスターユニットでのインターフェイスの設定 \(376 ページ\)](#) を参照してください。

同一のセキュリティ レベル通信の許可

デフォルトでは、同じセキュリティ レベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。この項では、複数のインターフェイスが同じセキュリティ レベルの場合にインターフェイス間通信をイネーブルにする方法と、インターフェイス内通信をイネーブルにする方法について説明します。

手順

ステップ 1 同じセキュリティ レベルのインターフェイス間の通信を有効にするには、**[Configuration] > [Interfaces]** ペインで、**[Enable traffic between two or more interfaces which are configured with same security level]** をオンにします。

ステップ 2 同じインターフェイスに接続されているホスト間の通信をイネーブルにするには、**[Enable traffic between two or more hosts connected to the same interface]** をオンにします。

ARP および MAC アドレス テーブルのモニタリング

- **[Monitoring] > [Interfaces] > [ARP Table]**

スタティック エントリやダイナミック エントリを含む ARP テーブルを表示します。ARP テーブルには、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするエントリが含まれます。

- **[Monitoring] > [Interfaces] > [MAC Address Table]**

スタティックおよびダイナミック MAC アドレス エントリを表示します。

インターフェイスの詳細設定の履歴

表 24: インターフェイスの詳細設定の履歴

機能名	リリース	機能情報
最大 MTU が 9198 バイトになりました	9.1(6)、9.2(1)	<p>ASA で使用できる最大の MTU は 9198 バイトです (CLI のヘルプでご使用のモデルの正確な最大値を確認してください)。この値にはレイヤ 2 ヘッダーは含まれません。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、これは不正確であり、問題が発生する可能性があります。9198 よりも大きいサイズに MTU を設定している場合は、アップグレード時に MTU のサイズが自動的に削減されます。場合によっては、この MTU の変更により MTU の不一致が発生する可能性があります。接続している機器が新しい MTU 値を使用するように設定されていることを確認してください。</p> <p>次の画面が変更されました。 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Edit Interface] > [Advanced]</p>



第 19 章

トラフィック ゾーン

トラフィックゾーンに複数のインターフェイスを割り当てることができます。これにより、既存のフローのトラフィックがゾーン内のインターフェイスで ASA に出入りできるようになります。この機能により、ASA 上での等コストマルチパス (ECMP) のルーティングや、ASA へのトラフィックの複数のインターフェイスにわたる外部ロードバランシングが可能になります。

- [トラフィックゾーンの概要 \(551 ページ\)](#)
- [トラフィックゾーン的前提条件 \(558 ページ\)](#)
- [トラフィックゾーンのガイドライン \(560 ページ\)](#)
- [トラフィックゾーンの設定 \(561 ページ\)](#)
- [トラフィックゾーンのモニタリング \(561 ページ\)](#)
- [トラフィックゾーンの例 \(564 ページ\)](#)
- [トラフィックゾーンの履歴 \(567 ページ\)](#)

トラフィックゾーンの概要

この項では、ネットワークでトラフィックゾーンを使用する方法について説明します。

ゾーン分割されていない動作

アダプティブセキュリティアルゴリズムは、トラフィックの許可または拒否を決定する際に、パケットの状態を考慮します。フローに適用されたパラメータの1つは、トラフィックが同じインターフェイスに出入りすることです。異なるインターフェイスに入る既存のフローのトラフィックは、ASA によってドロップされます。

トラフィックゾーンにより、複数のインターフェイスを1つにまとめることができるため、ゾーン内の任意のインターフェイスに出入りするトラフィックがアダプティブセキュリティアルゴリズムのセキュリティチェックを満たすことができますようになります。

関連トピック

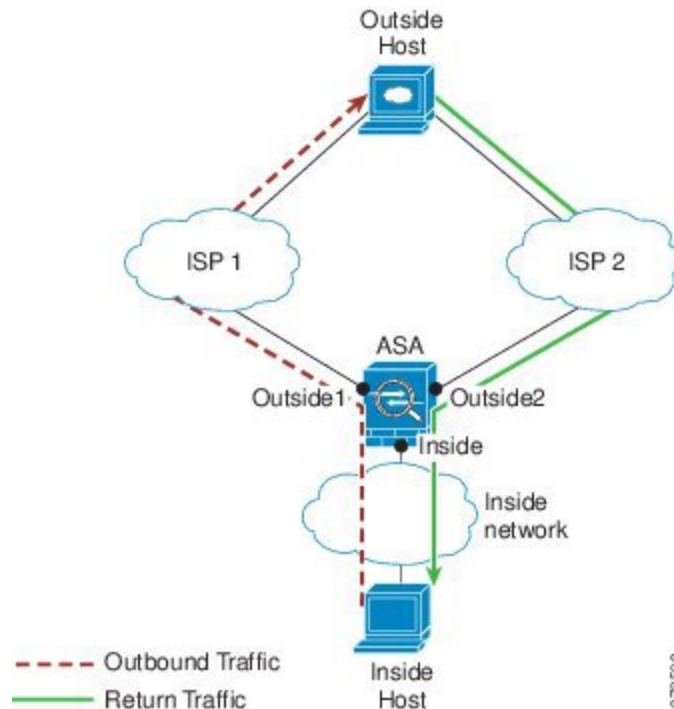
- [ステートフルインスペクションの概要 \(22 ページ\)](#)

ゾーンを使用する理由

ゾーンを使用して、複数のルーティングのシナリオに対応することができます。

非対称ルーティング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。宛先ネットワークの非対称ルーティングが原因で、Outside2 インターフェイスの ISP 2 からリターントラフィックが到達しています。

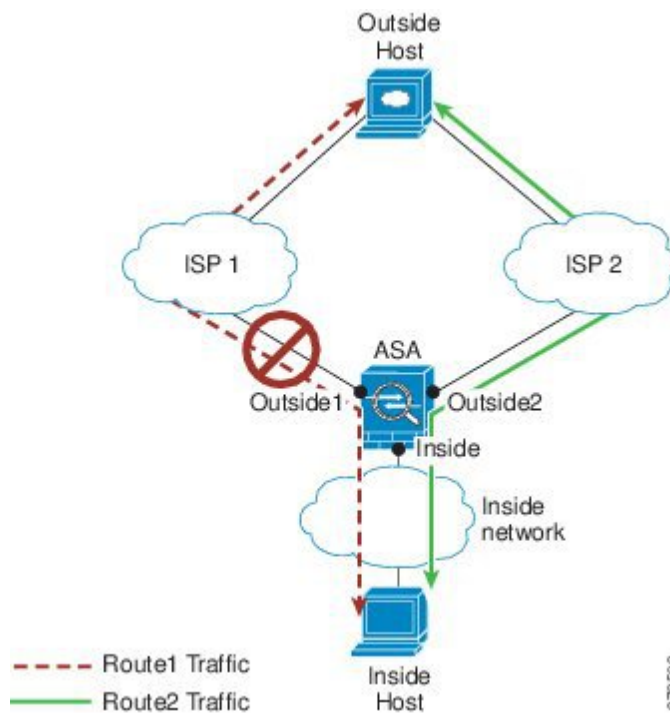


ゾーン分割されていない場合の問題：ASAは、インターフェイスごとに接続テーブルを保持します。リターントラフィックが Outside2 に到達すると、そのトラフィックは、接続テーブルに一致しないため、ドロップされます。ASA クラスタに関しては、クラスタが同一ルータに対して複数の隣接関係（アジャセンシー）を持つ場合、非対称ルーティングは許容できないトラフィック紛失の原因となることがあります。

ゾーン分割されたソリューション：ASAは、ゾーンごとに接続テーブルを保持します。Outside1 と Outside2 を一つのゾーンにグループ化した場合、リターントラフィックが Outside2 に到達すると、ゾーンごとの接続テーブルに一致するため、接続が許可されます。

紛失したルート

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。Outside1 と ISP 1 間でルートが紛失または移動したため、トラフィックは ISP 2 を経由する別のルートを通る必要があります。

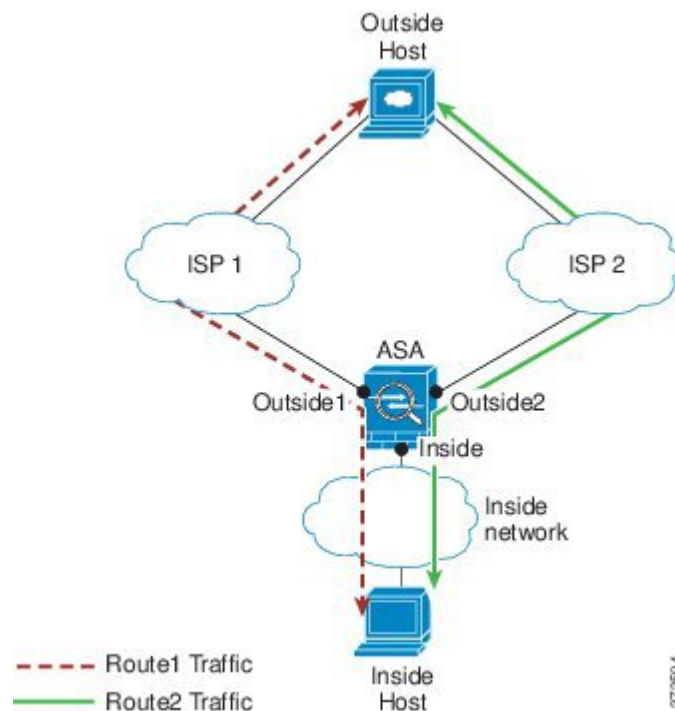


ゾーン分割されていない場合の問題：内部ホストと外部ホスト間の接続が削除されるため、新しい次善のルートを使用して新しい接続を確立する必要があります。UDP の場合、1 つのパケットがドロップダウンすると新しいルートが使用され、UDPがない場合は、新しい接続を再確立する必要があります。

ゾーン分割されたソリューション：ASA は、紛失したルートを検出し、フローを ISP 2 経由の新しいパスに切り替えます。トラフィックは、パケットがドロップすることなくシームレスに転送されます。

ロードバランシング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。2 番目の接続が Outside2 の ISP 2 を経由する等コストルートを介して確立されています。



ゾーン分割されていない場合の問題：インターフェイス間でロードバランシングを行うことができません。可能なのは、1つのインターフェイスの等コストルートによるロードバランスだけです。

ゾーン分割されたソリューション：ASAは、ゾーン内のすべてのインターフェイスで最大8つの等コストルート間の接続をロードバランスすることができます。

ゾーンごとの接続テーブルおよびルーティングテーブル

ASAは、トラフィックがゾーンのインターフェイスのいずれかに到達できるようにゾーンごとの接続テーブルを保持します。また、ASAは、ECMPサポート用にゾーンごとのルーティングテーブルも保持します。

ECMP ルーティング

ASAでは、等コストマルチパス（ECMP）ルーティングをサポートしています。

ゾーン分割されていないECMPサポート

ゾーンがない場合は、インターフェイスごとに最大8つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスに3つのデフォルトルートを設定できます。

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
```

```
route outside 0 0 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMPは複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route outside2 0 0 10.2.1.1
```

ゾーン分割された ECMP サポート

ゾーンがある場合は、ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイス間に 3 つのデフォルトルートを設定できます。

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同様に、ダイナミックルーティングプロトコルは、自動的に等コストルートを設定できます。ASA では、より堅牢なロードバランシングメカニズムを使用してインターフェイス全体でトラフィックをロードバランスします。

ルートが紛失した場合、ASA はフローをシームレスに別のルートに移動させます。

接続のロードバランス方法

ASA では、パケットの 6 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコル、入力インターフェイス）から生成されたハッシュを使用して、等コストルート間の接続をロードバランスします。ルートが紛失しない限り、接続は接続期間中、インターフェイスで継続されます。

接続内のパケットは、ルート間でロードバランスされません。接続では、そのルートが紛失しない限り、単一ルートを使用します。

ASA では、ロードバランシング時にインターフェイス帯域幅やその他のパラメータを考慮しません。同じゾーン内のすべてのインターフェイスが MTU、帯域幅などの同じ特性を持つことを確認します。

ロードバランシングアルゴリズムは、ユーザ設定可能ではありません。

別のゾーンのルートへのフォールバック

ルートがインターフェイスで紛失したときにゾーン内で使用可能な他のルートがない場合、ASA では、異なるインターフェイス/ゾーンからのルートを使用します。このバックアップ

ルートを使用した場合、ゾーン分割されていないルーティングのサポートと同様にパケットのドロップが発生することがあります。

インターフェイスベースのセキュリティポリシーの設定

ゾーンを使用すると、トラフィックはゾーン内のすべてのインターフェイスで出入りを許可されますが、セキュリティポリシー自体（アクセスルール、NAT など）は、ゾーン単位ではなく、インターフェイス単位で適用されます。ゾーン内のすべてのインターフェイスに同じセキュリティポリシーを設定すると、そのトラフィックの ECMP およびロードバランシングを適切に実装できます。必須の平行インターフェイス設定の詳細については、[トラフィックゾーンの前提条件（558 ページ）](#) を参照してください。

トラフィックゾーンでサポートされるサービス

次のサービスがゾーンでサポートされています。

- アクセルルール
- NAT
- QoS トラフィックポリシングを除くサービスルール。
- Routing

完全にゾーン分割されたサポートは利用できませんが、[To-the-Box](#) および [From-the-Box](#) [トラフィック（557 ページ）](#) に示した to-the-box サービスおよび from-the-box サービスを設定することもできます。

トラフィックゾーンのインターフェイスに他のサービス（VPN、ボットネットトラフィックフィルタなど）を設定しないでください。これらのサービスは、想定どおりに機能または拡張しないことがあります。



(注) セキュリティポリシーの設定方法の詳細については、[トラフィックゾーンの前提条件（558 ページ）](#) を参照してください。

セキュリティレベル

ゾーンに最初に追加するインターフェイスによってゾーンのセキュリティレベルが決まります。追加のインターフェイスは、すべて同じセキュリティレベルにする必要があります。ゾーン内のインターフェイスのセキュリティレベルを変更するには、1つのインターフェイスを除くすべてのインターフェイスを削除してからセキュリティレベルを変更し、インターフェイスを再度追加します。

フローのプライマリおよび現在のインターフェイス

各接続フローは、最初の入出力インターフェイスに基づいて構築されます。これらのインターフェイスは、プライマリ インターフェイスです。

ルート変更または非対称ルーティングにより、新しい出力インターフェイスが使用されている場合は、新しいインターフェイスが現在のインターフェイスになります。

ゾーンの追加または削除

ゾーンにインターフェイスを割り当てる場合、そのインターフェイスのすべての接続が削除されます。接続を再確立する必要があります。

ゾーンからインターフェイスを削除する場合、そのインターフェイスをプライマリ インターフェイスとしているすべての接続が削除されます。接続を再確立する必要があります。そのインターフェイスが現在のインターフェイスの場合、ASA は接続をプライマリ インターフェイスに戻します。ゾーンのルート テーブルも更新されます。

ゾーン内トラフィック

トラフィックがあるインターフェイスに入り、同じゾーンの別のインターフェイスから出ることができるようにするには、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Enable traffic between two or more hosts connected to the same interface]をイネーブルにしてトラフィックが同じインターフェイスを出入りできるようにし、さらに、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Enable traffic between two or more interfaces which are configured with same security level]をイネーブルにして same-security インターフェイス間のトラフィックを許可します。このように設定しない場合、フローは同じゾーンの2つのインターフェイス間をルーティングできません。

To-the-Box および From-the-Box トラフィック

- management-only インターフェイスまたは management-access インターフェイスをゾーンに追加することはできません。
- ゾーンの通常のインターフェイスでの管理トラフィックでは、既存のフローの非対称ルーティングのみがサポートされます。ECMP サポートはありません。
- 1つのゾーンインターフェイスにのみ管理サービスを設定できますが、非対称ルーティング サポートを利用するには、すべてのインターフェイスでそれを設定する必要があります。構成がすべてのインターフェイスでパラレルである場合でも、ECMPはサポートされません。
- ASA は、ゾーンで次の To-the-Box および From-the-Box サービスをサポートします。
 - Telnet
 - SSH

- HTTPS
- SNMP
- Syslog

ゾーン内の IP アドレスのオーバーラップ

ゾーン分割されていないインターフェイスの場合、ASA では、NAT が正しく設定されていれば、インターフェイスでの IP アドレス ネットワークのオーバーラップをサポートします。ただし、同じゾーンのインターフェイスでは、ネットワークのオーバーラップはサポートされていません。

トラフィック ゾーンの前提条件

- 名前、IP アドレス、およびセキュリティ レベルを含むすべてのインターフェイスパラメータを設定します。ゾーンのすべてのインターフェイスでセキュリティ レベルが一致する必要がありますことに注意してください。帯域幅および他のレイヤ 2 のプロパティについては、インターフェイスのようにグループ化する計画を立てる必要があります。
- 次のサービスをゾーンのすべてのインターフェイスで一致するように設定します。
 - アクセス ルール：同じアクセス ルールをゾーンのすべてのメンバー インターフェイスに適用するか、グローバル アクセス ルールを使用します。

次に例を示します。

```
access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
access-group ZONE1 in interface outside1
access-group ZONE1 in interface outside2
access-group ZONE1 in interface outside3
```

- NAT：ゾーンのすべてのメンバー インターフェイスで同じ NAT ポリシーを設定するか、グローバル NAT ルールを使用します（つまり、「any」を使用して NAT ルールでゾーンのインターフェイスを表します）。

インターフェイス PAT はサポートされていません。

次に例を示します。

```
object network WEBSERVER1
  host 10.9.9.9 255.255.255.255
  nat (inside,any) static 209.165.201.9
```



(注) インターフェイス固有の NAT および PAT プールを使用したときに元のインターフェイスの障害が発生した場合、ASA は接続を切り替えることはできません。

インターフェイス固有の PAT プールを使用する場合、同じホストからの複数の接続は、別のインターフェイスにロードバランスし、別のマッピング IP アドレスを使用することがあります。この場合、複数の同時接続を使用するインターネットサービスが正しく機能しないことがあります。

- サービス ルール : グローバル サービス ポリシーを使用するか、ゾーンの各インターフェイスに同じポリシーを割り当てます。

QoS トラフィック ポリシングはサポートされていません。

次に例を示します。

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```



(注) VoIP インспекションでは、ゾーンのロード バランシングにより、順序が正しくないパケットが増加する可能性があります。この状況は、異なるパスを通る先行パケットの前に後行パケットが ASA に到達する可能性があるために発生することがあります。順序が正しくないパケットには、次のような症状があります。

- キューイングを使用した場合に、中間ノード（ファイアウォールと IDS）および受信エンドノードでメモリ使用率が高い。
- ビデオまたは音声の品質が低い。

これらの影響を軽減するには、VoIP トラフィックのロード分散にのみ IP アドレスを使用することを推奨します。

- ECMP ゾーン機能を考慮してルーティングを設定します。

トラフィック ゾーンのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モード。

フェールオーバー

- フェールオーバー リンクまたはステート リンクをゾーンに追加することはできません。
- アクティブ/アクティブ フェールオーバー モードでは、各コンテキストのインターフェイスを非対称ルーティング (ASR) グループに割り当てることができます。このサービスにより、ピア装置の同様のインターフェイスに戻るトラフィックを元の装置に復元することができます。コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキスト インターフェイスも ASR グループに含めることはできません。ASR グループに関する詳細については、[非対称にルーティングされたパケットのサポートの設定 \(アクティブ/アクティブ モード\)](#) (317 ページ) を参照してください。
- 各接続のプライマリ インターフェイスのみがスタンバイ装置に複製されます。現在のインターフェイスは複製されません。スタンバイ装置がアクティブになると、その装置によって必要に応じて現在の新しいインターフェイスが割り当てられます。

クラスタ

- クラスタ制御リンクをゾーンに追加することはできません。

その他のガイドライン

- 最大 256 ゾーンを作成できます。
- 次のタイプのインターフェイスをゾーンに追加できます。
 - 物理
 - VLAN
 - EtherChannel
 - Redundant
- 次のタイプのインターフェイスは追加できません。
 - 管理専用
 - 管理アクセス
 - フェールオーバーまたはステート リンク

- クラスタ制御リンク
 - EtherChannel インターフェイスまたは冗長インターフェイスのメンバーインターフェイス
 - VNI（さらに、通常のデータ インターフェイスが nve 専用としてマークされている場合、ゾーンのメンバーにすることはできません）
 - BVI、またはブリッジグループ メンバー インターフェイス。
-
- 1つのインターフェイスがメンバーになることができるゾーンは1つだけです。
 - ゾーンごとに最大8つのインターフェイスを含めることができます。
 - ECMP の場合、ゾーンのすべてのインターフェイス間で、ゾーンごとに最大8つの等コストルートを追加できます。また、8ルート制限の一部として1つのインターフェイスに複数のルートを設定することもできます。
 - ゾーンにインターフェイスを追加すると、それらのインターフェイスのすべてのスタティック ルートが削除されます。
 - ゾーン内のインターフェイスで DHCP リレー を有効にできません。

トラフィック ゾーンの設定

名前を付けたゾーンを設定し、インターフェイスをそのゾーンに割り当てます。

手順

ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Zones] の順に選択し、[Add] をクリックします。

または、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] ダイアログボックスのゾーンにインターフェイスを割り当てることもできます。

ステップ 2 ゾーンに最大 48 文字で名前を付けます。

ステップ 3 1つ以上のインターフェイスを [Member] 領域に追加します。すべてのインターフェイスのセキュリティ レベルが同じになっていることを確認します。

ステップ 4 [Apply] をクリックします。

トラフィック ゾーンのモニタリング

この項では、トラフィック ゾーンをモニタする方法について説明します。

ゾーン情報

- **show zone** [*name*]

ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示します。

show zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
Zone Member(s) : 2
  outside1      GigabitEthernet0/0
  outside2      GigabitEthernet0/1
```

- **show nameif zone**

インターフェイス名およびゾーン名を表示します。

show nameif zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show nameif zone

Interface          Name                zone-name      Security
GigabitEthernet0/0  inside-1           inside-zone    100
GigabitEthernet0/1.21  inside             inside-zone    100
GigabitEthernet0/1.31  4                  0
GigabitEthernet0/2  outside            outside-zone   0
Management0/0        lan                0
```

ゾーン接続

- **show conn** [*long* | *detail*] [*zone zone_name*] [*zone zone_name*] [...]

show conn zone コマンドは、ゾーンの接続を表示します。**long** キーワードと **detail** キーワードは、接続が構築されたプライマリ インターフェイスと、トラフィックの転送に使用される現在のインターフェイスを表示します。

show conn long zone コマンドの次の出力を参照してください。

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

デバッグ目的で高速セキュリティ パス テーブルを表示します。

- **show local-host** [*zone zone_name*] [*zone zone_name*] [...]

ゾーン内のローカル ホストのネットワーク状態を表示します。

show local-host zone コマンドについては、次の出力を参照してください。プライマリ インターフェイスが最初に表示され、現在のインターフェイスがカッコに囲まれています。

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

Conn:
TCP outside-zone:outsidel(outside2): 10.122.122.1:1080
inside-zone:insidel(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

ゾーンルーティング

• show route zone

ゾーン インターフェイスのルートを表示します。

show route zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outsidel
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

• show asp table routing

デバッグ目的で高速セキュリティパステーブルを表示し、各ルートに関連付けられたゾーンを表示します。

show asp table routing コマンドについては次の出力を参照してください。

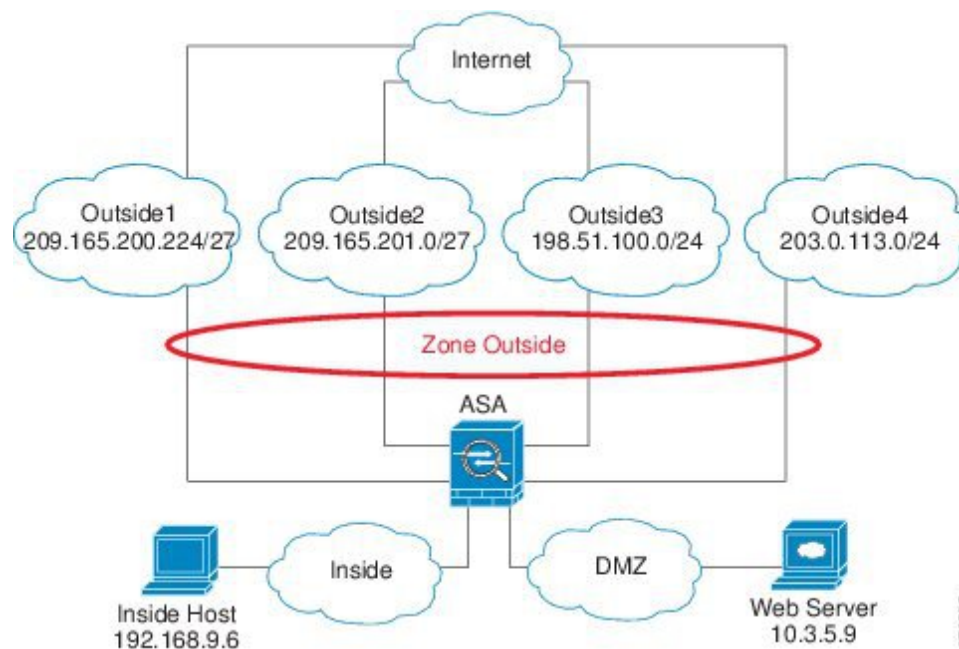
```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1        255.255.255.255 identity
in   10.2.0.1        255.255.255.255 identity
in   10.6.6.4        255.255.255.255 identity
```

```

in 10.4.4.4 255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in 172.0.0.67 255.255.255.255 identity
in 172.0.0.0 255.255.255.0 wan-zone:outside2
in 10.85.43.0 255.255.255.0 via 10.4.0.3 (unresolved, timestamp: 50)
in 10.85.45.0 255.255.255.0 via 10.4.0.20 (unresolved, timestamp: 51)
in 192.168.0.0 255.255.255.0 mgmt
in 192.168.1.0 255.255.0.0 lan-zone:inside
out 255.255.255.255 255.255.255.255 mgmt
out 172.0.0.67 255.255.255.255 mgmt
out 172.0.0.0 255.255.255.0 mgmt
out 10.4.0.0 240.0.0.0 mgmt
out 255.255.255.255 255.255.255.255 lan-zone:inside
out 10.1.0.1 255.255.255.255 lan-zone:inside
out 10.2.0.0 255.255.0.0 lan-zone:inside
out 10.4.0.0 240.0.0.0 lan-zone:inside
    
```

トラフィック ゾーンの例

次に、4つの VLAN インターフェイスを外部ゾーンに割り当てて、4つの等コストのデフォルトルートを設定する例を示します。PAT は内部インターフェイスに設定され、Web サーバはスタティック NAT を使用して DMZ インターフェイスで使用できます。



```

interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch
    
```



```
zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
```

```
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

トラフィック ゾーンの履歴

機能名	プラットフォーム リリース	説明
トラフィック ゾーン	9.3(2)	<p>インターフェイスをトラフィックゾーンにグループ化することで、トラフィックのロードバランシング（等コストマルチパス（ECMP）ルーティングを使用）、ルートの冗長性、および複数のインターフェイス間での非対称ルーティングを実現できます。</p> <p>(注) 名前付きゾーンにはセキュリティポリシーを適用できません。セキュリティポリシーはインターフェイスに基づきます。ゾーン内のインターフェイスが同じアクセスルール、NAT、およびサービスポリシーを使用して設定されていれば、ロードバランシングおよび非対称ルーティングは正しく動作します。</p> <p>次の画面が導入または変更されました。</p> <p>[Configuration] > [Device Setup] > [Interface Parameters] > [Zones]</p> <p>[Configuration] > [Device Setup] > [Interface Parameters] > [Interfaces]。</p>



第 **IV** 部

基本設定

- [基本設定 \(571 ページ\)](#)
- [DHCP サービスと DDNS サービス \(587 ページ\)](#)
- [デジタル証明書 \(603 ページ\)](#)
- [トランスペアレント ファイアウォール モードの ARP インスペクションおよび MAC アドレス テーブル \(639 ページ\)](#)



第 20 章

基本設定

この章では、ASA上でコンフィギュレーションを機能させるために通常必要な基本設定を行う方法について説明します。

- [ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定 \(571 ページ\)](#)
- [日時の設定 \(573 ページ\)](#)
- [マスターパスフレーズの設定 \(576 ページ\)](#)
- [DNS サーバの設定 \(578 ページ\)](#)
- [ハードウェア バイパス \(Cisco ISA 3000\) の設定 \(581 ページ\)](#)
- [ASP \(高速セキュリティ パス\) のパフォーマンスと動作の調整 \(582 ページ\)](#)
- [DNS キャッシュのモニタリング \(585 ページ\)](#)
- [基本設定の履歴 \(585 ページ\)](#)

ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定

ホスト名、ドメイン名、イネーブルパスワード、Telnet パスワードを設定するには、次の手順を実行します。

始める前に

ホスト名、ドメイン名、イネーブルパスワード、Telnet パスワードを設定する前に、次の要件を確認します。

- マルチ コンテキスト モードでは、コンテキスト実行スペースとシステム実行スペースの両方のホスト名とドメイン名を設定できます。
- イネーブルパスワードと Telnet パスワードは、各コンテキストで設定します。システムでは使用できません。マルチ コンテキスト モードのスイッチから ASASM へのセッションを実行する場合、ASASM は管理コンテキストで設定したログインパスワードを使用します。

- システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration]>[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 [Configuration] > [Device Setup] > [Device Name/Password] を選択します。

ステップ 2 ホスト名を入力します。デフォルトのホスト名は「ciscoasa」です。

ホスト名はコマンドラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。ホスト名は syslog メッセージでも使用されます。

マルチ コンテキスト モードでは、システム実行スペースに設定したホスト名がすべてのコンテキストのコマンドラインプロンプトに表示されます。コンテキストで設定したホスト名を、コマンドラインに表示せず、バナーに表示するオプションもあります。

ステップ 3 ドメイン名を入力します。デフォルト ドメイン名は default.domain.invalid です。

ASA は、修飾子を持たない名前のサフィックスとして、ドメイン名を追加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。

ステップ 4 特権モード（イネーブル）パスワードを変更します。デフォルトのパスワードは空白ですが。

enable 認証を設定しない場合、イネーブルパスワードによって特権 EXEC モードが開始されます。HTTP 認証を設定しない場合、イネーブルパスワードによって空のユーザ名で ASDM にログインできます。

- a) [Change the privileged mode password] チェックボックスをオンにします。
- b) 古いパスワード（デフォルトのパスワードは空白）、新しいパスワードを入力し、新しいパスワードを確認します。最大 から 32 文字のパスワードを設定します。大文字と小文字が区別されます。スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせてすることができます。

ステップ 5 Telnet アクセスのためのログインパスワードを設定します。デフォルトのパスワードはありません。

Telnet 認証を設定しない場合、ログインパスワードは Telnet アクセスに使用されます。session コマンドを使用してスイッチから ASDM にアクセスする場合にも、このパスワードを使用します。

- a) [Change the password to access the console of the security appliance] チェックボックスをオンにします。
- b) 古いパスワード（新しい ASA の場合はこのフィールドを空白にしておきます）、新しいパスワードを入力し、新しいパスワードを確認します。パスワードには最大 16 文字の長さを使用できます。スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせてすることができます。

ステップ 6 [Apply] をクリックして変更内容を保存します。

日時の設定



(注) ASASM または Firepower 2100、4100、または 9300 の日時を設定しないでください。ASA はシャーシから日時の設定を受信します。

NTP サーバを使用した日付と時刻の設定

NTP を利用して階層的なサーバシステムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバを設定できます。ASA は、データ信頼度の尺度となる一番下のストラタムのサーバを選択します。

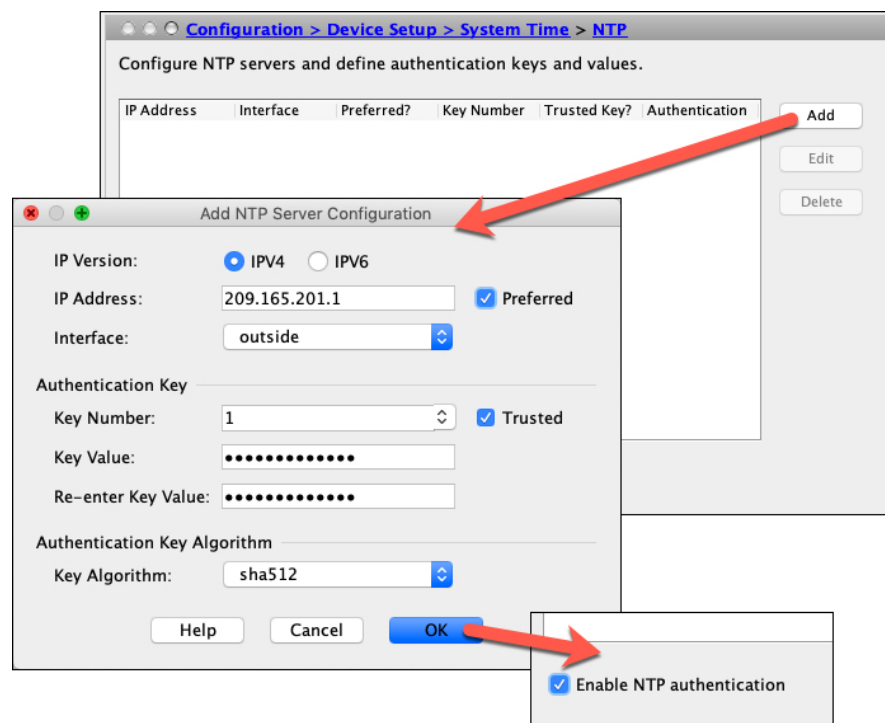
手動で設定した時刻はすべて、NTP サーバから取得された時刻によって上書きされます。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1 [Configuration] > [Device Setup] > [System Time] > [NTP] を選択します。



ステップ 2 [Add] をクリックして、[Add NTP Server Configuration] ダイアログボックスを表示します。

ステップ 3 NTP サーバの **IPv4 IP アドレス** を入力します。

サーバのホスト名を入力することはできません。ASA は、NTP サーバの DNS ルックアップをサポートしていません。

ステップ 4 (任意) [Preferred] チェックボックスをオンにして、このサーバを優先サーバに設定します。

NTP では、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。精度が同じ程度であれば、優先サーバを使用します。ただし、優先サーバよりも精度が大幅に高いサーバがある場合、ASA は精度の高いそのサーバを使用します。

ステップ 5 (任意) ドロップダウンリストから [Interface] を選択します。

この設定では、NTP パケットの発信インターフェイスが指定されます。インターフェイスが空白の場合、ASA が使用するデフォルトの管理コンテキストインターフェイスは、管理ルーティングテーブルによって決まります。

ステップ 6 (任意) NTP 認証を設定します。

a) 1～4294967295 の間の **キー番号** を入力するか、または、再利用する別の NTP サーバのキーを以前に作成している場合は、ドロップダウンリストから既存のキー番号を選択します。

この設定では、この認証キーのキー ID を指定します。これにより、MD5 認証を使用して NTP サーバと通信できます。NTP サーバのパケットも、常にこのキー ID を使用する必要があります。

b) [Trusted] チェックボックスをオンにします。

- c) キー値を入力します。これは、最大 32 文字の文字列です。その後、キー値を再入力します。
- d) [OK] をクリックします。

ステップ 7 [Enable NTP authentication] チェックボックスをオンにして、NTP 認証を有効にします。

ステップ 8 [Apply] をクリックして変更内容を保存します。

手動での日時の設定

日付と時刻を手動で設定するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1 [Configuration] > [Device Setup] > [System Time] > [Clock] を選択します。

ステップ 2 ドロップダウンリストからタイムゾーンを選択します。この設定では、適切な時差を GMT に加えた（または GMT から差し引いた）タイムゾーンを指定します。[Eastern Time]、[Central Time]、[Mountain Time]、または [Pacific Time] ゾーンを選択すると、3 月の第 2 日曜日の午前 2 時から 11 月の第 1 日曜日の午前 2 時間での時間が自動的に夏時間に調整されます。

(注) ASA の時間帯を変更すると、インテリジェント SSM との接続がドロップされる場合があります。

ステップ 3 [Date] ドロップダウンリストをクリックしてカレンダーを表示します。続いて、次の方法を使用して正しい日付を検索します。

- 月の名前をクリックし、月のリストを表示し、次に目的の月をクリックします。カレンダーがその月に変わります。
- 年をクリックして年を変更します。上矢印と下矢印を使用して複数年をスクロールすることも、入力フィールドに年を入力することもできます。
- 年月の左右にある矢印をクリックすると、カレンダーが一度に 1 か月ずつ前後にスクロールします。
- カレンダーの日にちをクリックして日を設定します。

ステップ 4 時刻（時間、分、および秒）を手動で入力します。

ステップ 5 [Update Display Time] をクリックして、ASDM ペインの右下に表示される時刻を更新します。現在時刻は 10 秒ごとに自動更新されます。

マスターパスワードの設定

マスターパスワードを利用すると、プレーンテキストのパスワードが安全に、暗号化形式で保存され、1つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。マスターパスワードを使用する機能としては、次のものがあります。

- OSPF
- EIGRP
- VPN ロード バランシング
- VPN (リモート アクセスおよびサイトツーサイト)
- フェールオーバー
- AAA サーバ
- Logging
- 共有ライセンス

マスターパスワードの追加または変更

マスターパスワードを追加または変更するには、次の手順を実行します。

始める前に

- この手順を実行できるのは、コンソール、SSH、HTTPS 経由の ASDM などによるセキュアセッションにおいてのみです。
- フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスターパスワードを変更すると、エラーメッセージが表示されます。このメッセージには、マスターパスワードの変更がプレーンテキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

[Configuration]>[Device Management]>[High Availability]>[Failover]の順に選択し、[Shared Key] フィールドに任意の文字を入力するか、またはフェールオーバー 16 進キーを選択している場合はバックスペースを除く 32 の 16 進数 (0-9A-Fa-f) を入力します。次に、[Apply] をクリックします。

- アクティブ/スタンバイ フェールオーバーでパスワードの暗号化を有効化または変更すると、**write standby** が実行されます。これは、アクティブな構成をスタンバイユニットに複製します。この複製が行われない場合、スタンバイユニットの暗号化されたパスワードは、同じパスワードを使用している場合でも異なるものになります。構成を複製することで、構成が同じであることが保証されます。アクティブ/アクティブ フェールオーバーの場合は、手動で **write standby** を入力する必要があります。**write standby** は、アクティブ/アクティブ モードでトラフィックの中断を引き起こす場合があります。これは、新し

い構成が同期される前に、セカンダリ ユニットで構成が消去されるためです。 **failover active group 1** および **failover active group 2** コマンドを使用してプライマリ ASA ですべてのコンテキストをアクティブにし、 **write standby** を入力してから、 **no failover active group 2** コマンドを使用してセカンダリ ユニットにグループ 2 コンテキストを復元する必要があります。

手順

ステップ 1 次のいずれかのオプションを選択します。

- シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。
- マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] を選択します。

ステップ 2 [Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスター パスフレーズがない場合は、[Apply] をクリックすると警告メッセージが表示されます。[OK] または [Cancel] をクリックして続行できます。

後からパスワードの暗号化をディセーブルにすると、暗号化された既存のパスワードはいずれも変更されず、マスターパスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号化されます。

ステップ 3 [Change the encryption master passphrase] チェックボックスをオンにして、新しいマスター パスフレーズを入力および確認できるようにします。デフォルトでは、これらはディセーブルです。

新しいマスター パスフレーズの長さは 8 ~ 128 文字にする必要があります。

既存のパスフレーズを変更する場合は、新しいパスフレーズを入力する前に、古いパスフレーズを入力する必要があります。

マスター パスフレーズを削除するには [New] および [Confirm master passphrase] フィールドを空白のままにします。

ステップ 4 [Apply] をクリックします。

マスター パスフレーズの無効化

マスター パスフレーズをディセーブルにすると、暗号化されたパスワードがプレーン テキストパスワードに戻ります。暗号化されたパスワードをサポートしていない以前のソフトウェアバージョンにダウングレードする場合は、パスフレーズを削除しておくとも便利です。

始める前に

- ディセーブルにする現在のマスター パスフレーズがわかっていなければなりません。
- この手順が機能するのは、HTTPS を介した Telnet、SSH、または ASDM によるセキュアセッションだけです。

マスター パスフレーズをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択します。

- シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。
- マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] を選択します。

ステップ 2 [Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスターパスフレーズがない場合は、[Apply] をクリックすると警告文が表示されます。
[OK] または [Cancel] をクリックして続行します。

ステップ 3 [Change the encryption master passphrase] チェックボックスをオンにします。

ステップ 4 [Old master passphrase] フィールドに、古いマスターパスフレーズを入力します。ディセーブルにする古いマスターパスフレーズを指定する必要があります。

ステップ 5 [Newmaster master passphrase] フィールドと [Confirm master passphrase] フィールドを空白のままにします。

ステップ 6 [Apply] をクリックします。

DNS サーバの設定

DNS サーバを設定して、ASA がホスト名を IP アドレスに解決できるようにする必要があります。また、アクセスルールに完全修飾ドメイン名 (FQDN) ネットワークオブジェクトを使用するように、DNS サーバを設定する必要があります。

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネットトラフィックフィルタ機能では、ダイナミックデータベースサーバにアクセスして、スタティックデータベースのエントリを解決するために DNS サーバが必要です。他の機能 (ping コマンドや traceroute コマンドなど) では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。



(注) ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。

始める前に

DNS ドメインルックアップをイネーブルにするすべてのインターフェイスに対して適切なルーティングおよびアクセスルールを設定し、DNS サーバに到達できるようにしてください。

手順

ステップ 1 [Configuration] > [Device Management] > [DNS] > [DNS Client] の順に選択します。

ステップ 2 [DNS Setup] 領域で、次のいずれかのオプションを選択します。

- **Configure one DNS server group** : このオプションは DefaultDNS グループにサーバを定義します。
- **Configure multiple DNS server groups** : このオプションでも、DefaultDNS グループは設定する必要があります。FQDN ネットワーク オブジェクトの名前解決に使用されるのは DefaultDNS グループのみです。DefaultDNS はアクティブ グループのままにします。ただし、リモート アクセス SSL VPN グループ ポリシーで使用する追加のグループを作成することもできます。DefaultDNS グループのみを設定したとしても、グループで使用するタイムアウトやその他の特性を変更する場合は、このオプションを選択する必要があります。

ステップ 3 [Configure one DNS server group] を選択した場合は、DefaultDNS グループにサーバを設定します。

- a) [Primary DNS Server] に、可能な限り使用する必要がある DNS サーバの IP アドレスを入力します。
- b) [Add] をクリックして、セカンダリ DNS サーバを追加します。
最大 6 個の DNS サーバを追加できます。ASA では、応答を受信するまで各 DNS サーバを順に試します。[Move Up]/[Move Down] ボタンを使用して、サーバを優先度の順に並べます。
- c) ホスト名に追加する DNS ドメイン名を入力します（完全修飾されていない場合）。

ステップ 4 [Configure multiple DNS server groups] を選択した場合は、サーバグループのプロパティを定義します。

- a) [Add] をクリックして新しいグループを作成するか、グループを選択して [Edit] をクリックします。
DefaultDNS グループは常にリストに表示されます。
- b) グループ プロパティを設定します。
 - [Server IP Address to Add]、[Source Interface] : DNS サーバの IP アドレスを入力し、[Add>>] をクリックします。

最大 6 個の DNS サーバを追加できます。ASA では、応答を受信するまで各 DNS サーバを順に試します。[Move Up]/[Move Down] ボタンを使用して、サーバを優先度の順に並べます。

- [Timeout] : 次の DNS サーバを試行する前に待機する秒数 (1 ~ 30)。デフォルト値は 2 秒です。ASA がサーバのリストを再試行するたびに、このタイムアウトは倍増します。
- [Retries] : ASA が応答を受信しないときに、DNS サーバのリストを再試行する回数 (0 ~ 10)。
- [Expire Entry Timer] (DefaultDNS またはアクティブ グループのみ) : DNS エントリの期限が切れた (TTL が経過した) 後、そのエントリが DNS ルックアップ テーブルから削除されるまでの分数。エントリを削除するとテーブルの再コンパイルが必要になります。このため、頻繁に削除するとデバイスの処理負荷が大きくなる可能性があります。DNS エントリによっては TTL が極端に短い (3 秒程度) 場合があるため、この設定を使用して TTL を実質的に延長できます。デフォルトは 1 分です (つまり、TTL が経過してから 1 分後にエントリが削除されます)。指定できる範囲は 1 ~ 65535 分です。このオプションは、FQDN ネットワーク オブジェクトの解決時にのみ使用されます。
- [Poll Timer] (DefaultDNS またはアクティブ グループのみ) : FQDN ネットワーク/ホスト オブジェクトを IP アドレスに解決するために使用されるポーリング サイクルの時間 (分単位)。FQDN オブジェクトはファイアウォールポリシーで使用される場合にのみ解決されます。タイマーによって解決間隔の最大時間が決まります。IP アドレス解決に対して更新するタイミングの決定には DNS エントリの存続可能時間 (TTL) 値も使用されるため、個々の FQDN がポーリング サイクルよりも頻繁に解決される場合があります。デフォルトは 240 (4 時間) です。指定できる範囲は 1 ~ 65535 分です。
- [Domain Name] : ホスト名に追加するドメイン名 (完全修飾されていない場合)。

c) [OK] をクリックします。

d) 複数のグループがある場合は、DNS 要求に使用するグループを選択して [Set Active] をクリックすれば変更できます。

ステップ 5 DNS ルックアップが少なくとも 1 つのインターフェイスでイネーブルになっていることを確認します。DNS サーバグループの表の下にある [DNS lookup] インターフェイスリストで、[DNS Enabled] カラムをクリックして [True] を選択し、インターフェイスでのルックアップを有効化します。

ステップ 6 (任意) クエリーごとに 1 つの DNS 応答を強制するには、[Enable DNS Guard on all interfaces] チェックボックスをオンにします。

DNS インспекションを設定するときに、DNS ガードも設定できます。特定のインターフェイスでは、DNS インспекションで設定されている DNS ガードの設定がこのグローバル設定より優先されます。デフォルトでは、DNS インспекションは DNS ガードがイネーブルになっているすべてのインターフェイスでイネーブルになっています。

ステップ7 [Apply] をクリックして変更内容を保存します。

ハードウェアバイパス (Cisco ISA 3000) の設定

ハードウェアバイパスを有効化して、停電時にもインターフェイス ペア間のトラフィックのフローを継続することができます。サポートされているインターフェイス ペアは、銅線 GigabitEthernet 1/1 と 1/2 および GigabitEthernet 1/3 と 1/4 です。ハードウェアバイパスがアクティブな場合はファイアウォール機能が設定されていません。したがって、トラフィックの通過を許可しているリスクをご自身が理解していることを確認してください。次のハードウェアバイパスのガイドラインを参照してください。

- この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。
- 光ファイバーサネット モデルがある場合は、銅線イーサネット ペア (GigabitEthernet 1/1 および 1/2) のみがハードウェアバイパスをサポートします。
- ISA 3000 への電源が切断され、ハードウェアバイパス モードに移行すると、通信できるのはサポートされているインターフェイスペアだけになります。つまり、デフォルトの設定を使用している場合、inside1 と inside2 間および outside1 と outside2 間は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。
- シスコでは、TCPシーケンスのランダム化を無効にすることを推奨しています (下記の手順を参照)。ランダム化が有効化されている場合 (デフォルト)、ハードウェアバイパスを有効化するときに TCPセッションを再確立する必要があります。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号 (ISN) が乱数に書き換えられます。ハードウェアバイパスが有効化されると、ISA 3000 はデータパスに存在しなくなり、シーケンス番号を変換しません。受信するクライアントは予期しないシーケンス番号を受信し、接続をドロップします。TCPシーケンスのランダム化が無効になっていても、スイッチオーバーの際に一時的にダウンしたリンクのために、一部の TCP 接続は再確立される必要があります。
- ハードウェアのバイパス インターフェイスでの Cisco TrustSec の接続は、ハードウェアのバイパスが有効化されているときにはドロップされます。ISA 3000 の電源がオンになり、ハードウェアのバイパスが非アクティブ化されている場合、接続は再ネゴシエートされません。
- ハードウェアバイパスを非アクティブ化し、トラフィックが ISA 3000 のデータパスを経由することを再開した場合、スイッチオーバー時に一時的にダウンしたリンクがあるために、既存の TCP セッションの一部を再確立する必要があります。
- ハードウェアバイパスをアクティブにすると、イーサネット PHY が切断され、ASA はインターフェイスのステータスを判断できなくなります。インターフェイスはダウン状態であるかのように表示されます。

始める前に

- ハードウェアバイパスインターフェイスはスイッチのアクセスポートに接続する必要があります。トランクポートには接続しないでください。

手順

ステップ 1 ハードウェアバイパスを設定するには、**[Configuration] > [Device Management] > [Hardware Bypass]** の順に選択します。

ステップ 2 **[Enable Bypass during Power Down]** チェックボックスをオンにして、各インターフェイスペアのハードウェアバイパスを有効化するように設定します。

ステップ 3 （任意） **[Enable Bypass after Power Up]** チェックボックスをオンにして、電源が回復してアプリケーションが起動した後にハードウェアバイパスモードの状態に維持されるように、各インターフェイスペアを設定します。

ハードウェアバイパスを非アクティブ化すると、ASA がフローを引き継ぐため、接続が短時間中断されます。この場合、準備が整った時点でハードウェアバイパスを手動でオフにする必要があります。このオプションを使用すると、短時間の割り込みがいつ発生するかを制御できます。

ステップ 4 インターフェイスペアに対しては、**[Bypass Immediately]** チェックボックスをオン/オフして、手動でハードウェアバイパスを有効化または非アクティブ化します。

ステップ 5 **[Apply]** をクリックします。

ステップ 6 TCP のランダム化を無効化します。この例では、デフォルト設定に設定を追加することによって、すべてのトラフィックのランダム化を無効化する方法を示します。

- a) **[Configuration] > [Firewall] > [Service Policy]** を選択します。
- b) **sfrclass** ルールを選択して **[Edit]** をクリックします。
- c) **[Rule Actions]** に続いて、**[Connection Settings]** をクリックします。
- d) **[Randomize Sequence Number]** チェックボックスをオフにします。
- e) **[OK]**、続いて **[Apply]** をクリックします。

ASP（高速セキュリティパス）のパフォーマンスと動作の調整

ASP はポリシーおよび設定を利用可能にする実装レイヤです。Cisco Technical Assistance Center とのトラブルシューティング時以外は直接影響することはありません。ただし、パフォーマンスと信頼性に関連するいくつかの動作を調節することができます。

ルールエンジンのトランザクションコミットモデルの選択

デフォルトでは、ルールベースのポリシー（アクセスルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性によりパフォーマンスにわずかな負担がかかります。パフォーマンスコストは、1秒あたりの接続数が多い環境で大量のルールリストがある場合に顕著です。たとえば、ASAが1秒あたり18,000個の接続を処理しながら、25,000個のルールがあるポリシーを変更する場合などです。

ルールエンジンはさらに迅速なルールルックアップを実現するためにルールをコンパイルするため、パフォーマンスに影響します。デフォルトでは、システムは接続試行の評価時にコンパイルされていないルールも検索して、新しいルールが適用されるようにします。ルールがコンパイルされていないため、検索に時間がかかります。

この動作を変更して、ルールエンジンがトランザクションモデルを使用してルールの変更を導入し、新しいルールがコンパイルされて使用可能な状態になるまで古いルールを引き続き使用するようにできます。トランザクションモデルを使用することで、ルールのコンパイル中にパフォーマンスが落ちることはありません。次の表は、その動作の違いを明確にします。

モデル	コンパイル前	コンパイル中	コンパイル後
デフォルト	古いルールに一致します。	新しいルールに一致します (接続数/秒のレートは減少します)。	新しいルールに一致します。
トランザクション	古いルールに一致します。	古いルールに一致します (接続数/秒のレートは影響を受けません)。	新しいルールに一致します。

トランザクションモデルのその他のメリットには、インターフェイス上のACLを交換するときに、古いACLを削除して新しいポリシーを適用するまでに時間差がないことがあります。この機能により受け入れ可能な接続が操作中にドロップされる可能性が削減されます。



ヒント

ルールタイプのトランザクションモデルをイネーブルにする場合、コンパイルの先頭と末尾をマークするSyslogが生成されます。これらのSyslogには780001～780004までの番号が付けられます。

ルールエンジンのトランザクションコミットモデルを有効にするには、次の手順を使用します。

手順

[Configuration] > [Device Management] > [Advanced] > [Rule Engine] の順に選択し、目的のオプションを選択します。

- **Access group** : グローバルにまたはインターフェイスに適用されるアクセスルール。
- **NAT** : ネットワーク アドレス変換ルール。

ASP ロード バランシングの有効化

ASP のロード バランシング機能によって、次の問題を回避しやすくなります。

- フロー上での突発的なトラフィックの増加によって発生するオーバーラン
- 特定のインターフェイス受信リングをオーバーサブスクライブするバルク フローによるオーバーラン
- 比較的高過負荷のインターフェイス受信リングによるオーバーラン（シングルコアでは負荷を維持できません）

ASP ロードバランシングにより、1つのインターフェイス受信リングから受信したパケットを複数のコアが同時に処理できます。システムがパケットをドロップし、**show cpu** コマンドの出力が 100% を大きく下回る場合、互いに関連のない多数の接続にパケットが属しているのであれば、この機能によってスループットが向上することがあります。

手順

ステップ 1 ASP ロードバランシングの自動切り替えをイネーブルまたはディセーブルにするには、**[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]** の順に選択して、**[Dynamically enable or disable ASP load balancing based on traffic monitoring]** チェックボックスをオンにします。

このオプションは ASA v では使用できません。手動で ASP ロードバランシングをイネーブル/ディセーブルにする必要があります。

ステップ 2 手動で ASP ロードバランシングをイネーブルまたはディセーブルにするには、**[Enable ASP load balancing]** チェックボックスをオンまたはオフにします。

手動で ASP ロードバランシングをイネーブルにすると、動的オプションをイネーブルにした場合でも、手動でディセーブルにするまではイネーブル状態となります。手動で ASP ロードバランシングをイネーブルにした場合にのみ、ASP ロードバランシングの手動ディセーブル化が適用されます。動的オプションもまたイネーブルにすると、システムは ASP ロードバランシングの自動イネーブル/ディセーブル化に戻ります。

DNS キャッシュのモニタリング

ASA では、特定のクライアントレス SSL VPN および `certificate` コマンドに送信された外部 DNS クエリーの DNS 情報のローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカル キャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバに DNS クエリーが送信されます。外部 DNS サーバによって要求が解決された場合、結果の IP アドレスが、対応するホスト名とともにローカル キャッシュに格納されます。

DNS キャッシュのモニタリングについては、次のコマンドを参照してください。

- `show dns-hosts`

DNS キャッシュを表示します。これには、DNS サーバからダイナミックに学習したエントリと `name` コマンドを使用して手動で入力された名前および IP アドレスが含まれます。

基本設定の履歴

機能名	プラットフォームリリース	説明
ISA 3000 ハードウェアバイパス	9.4(1225)	ISA 3000 は、トラフィックが電源喪失時にアプライアンスを通過し続けるようにするハードウェア バイパス機能をサポートします。 次の画面が導入されました。[Configuration] > [Device Management] > [Hardware Bypass]
自動 ASP ロード バランシング	9.3(2)	ASP ロード バランシング 機能の自動切替を有効または無効に設定できるようになりました。 (注) 自動機能は ASA v ではサポートされません。手動による有効化または無効化のみがサポートされます。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]

機能名	プラットフォームリリース	説明
デフォルトの Telnet パスワードの削除	9.0(2)、9.1(2)	<p>ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ログインパスワードが削除されました。Telnet を使用してログインする前に、パスワードを手動で設定する必要があります。</p> <p>(注) ログインパスワードが使用されるのは、Telnet ユーザ認証を設定しない場合の Telnet に対してのみです。</p> <p>以前はパスワードをクリアすると、ASA がデフォルト「cisco」を復元していました。今ではパスワードをクリアすると、パスワードは削除されるようになりました。</p> <p>ログインパスワードは、スイッチから ASASM への Telnet セッションでも使用されず (session コマンドを参照)。最初 ASASM のアクセスでは、ログインパスワードを設定するまで、service-module session コマンドを使用します。</p> <p>変更された ASDM 画面はありません。</p>
パスワード暗号化の可視性	8.4(1)	<p>show password encryption コマンドが変更されました。</p>
マスターパスフレーズ	8.3(1)	<p>この機能が導入されました。マスターパスフレーズを利用すると、プレーンテキストのパスワードが安全に、暗号化形式で保存され、1つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。</p> <p>次の画面が導入されました。</p> <p>[Configuration] > [Device Management] > [Advanced] > [Master Passphrase]。</p> <p>[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase]。</p>



第 21 章

DHCP サービスと DDNS サービス

この章では、ダイナミック DNS (DDNS) のアップデート方式のほか、DHCP サーバまたは DHCP リレーを設定する方法について説明します。

- [DHCP サービスと DDNS サービスについて \(587 ページ\)](#)
- [DHCP サービスと DDNS サービスのガイドライン \(590 ページ\)](#)
- [DHCP サーバの設定 \(591 ページ\)](#)
- [DHCP リレー エージェントの設定 \(595 ページ\)](#)
- [DDNS の設定 \(597 ページ\)](#)
- [DHCP および DDNS サービスのモニタリング \(598 ページ\)](#)
- [DHCP および DDNS サービスの履歴 \(599 ページ\)](#)

DHCP サービスと DDNS サービスについて

次の項では、DHCP サーバ、DHCP リレー エージェント、および DDNS 更新について説明します。

DHCPv4 サーバについて

DHCP は、IP アドレスなどのネットワーク コンフィギュレーション パラメータを DHCP クライアントに提供します。ASA は ASA インターフェイスに接続されている DHCP クライアントに、DHCP サーバを提供します。DHCP サーバは、ネットワーク コンフィギュレーション パラメータを DHCP クライアントに直接提供します。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。

IPv6 の DHCP サーバはサポートされていません。ただし、IPv6 トラフィックの DHCP リレーを有効にできます。

DHCP オプション

DHCPは、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータはDHCP メッセージの Options フィールドにストアされているタグ付けされたアイテムにより送信され、このデータはオプションとも呼ばれます。ベンダー情報も Options に保存され、ベンダー拡張情報はすべて DHCP オプションとして使用できます。

たとえば、Cisco IP Phone が TFTP サーバから設定をダウンロードする場合を考えます。Cisco IP Phone の起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合、Cisco IP Phone ではオプション 150 または 66 を伴う要求を DHCP サーバに送信して、この情報を取得します。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。
- DHCP オプション 3 はデフォルト ルートを設定します。

1 つの要求にオプション 150 と 66 の両方が含まれている場合があります。この場合、両者が ASA ですでに設定されていると、ASA の DHCP サーバは、その応答で両方のオプションに対する値を提供します。

高度な DHCP オプションにより、DNS、WINS、ドメインネームパラメータを DHCP クライアントに提供できます。DNS ドメインサフィックスは DHCP オプション 15 を使用します。これらの値は DHCP 自動設定により、または手動で設定できます。この情報の定義に2つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動コンフィギュレーションの設定

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動コンフィギュレーションをイネーブルにできます。DHCP 自動構成によって、DNS サーバおよび WINS サーバとともにドメインが検出されても、手動で定義したドメイン名が、検出された DNS サーバ名および WINS サーバ名とともに DHCP クライアントに渡されます。これは、DHCP 自動構成プロセスで検出されたドメイン名よりも、手動で定義されたドメイン名の方が優先されるためです。

DHCP リレー エージェントについて

インターフェイスで受信した DHCP 要求を1つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワークセグメントにクライアントがある場合、ASA はブロードキャストトラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレー エージェントを使用して、ブロード

キャストを受信している ASA のインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定できます。

DDNS の概要

DDNS アップデートでは、DNS を DHCP に組み込みます。これら 2 つのプロトコルは相互補完します。DHCP は、IP アドレス割り当てを集中化および自動化します。DDNS アップデートは、割り当てられたアドレスとホスト名の間のアソシエーションを事前定義された間隔で自動的に記録します。DDNS は、頻繁に変わるアドレスとホスト名のアソシエーションを頻繁にアップデートできるようにします。これにより、たとえばモバイルホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。DDNS は、DNS サーバ上で、名前からアドレスへのマッピングと、アドレスから名前へのマッピングをダイナミックにアップデートして、同期化します。

DDNS の名前とアドレスのマッピングは、DHCP サーバ上で 2 つのリソース レコード (RR) で行われます。A RR では、名前から IP アドレスへのマッピングが保持され、PTR RR では、アドレスから名前へのマッピングが行われます。DDNS 更新を実行するための 2 つの方式 (RFC 2136 で規定されている IETF 標準規格、および一般的な HTTP 方式) のうち、ASA では、IETF 方式をサポートしています。



(注) DDNS は BVI またはブリッジグループのメンバーインターフェイスではサポートされません。

DDNS アップデート コンフィギュレーション

2 つの最も一般的な DDNS アップデート コンフィギュレーションは次のとおりです。

- DHCP クライアントは A RR をアップデートし、DHCP サーバは PTR RR をアップデートします。
- DHCP サーバは、A RR と PTR RR の両方をアップデートします。

通常、DHCP サーバはクライアントの代わりに DNS PTR RR を保持します。クライアントは、必要なすべての DNS アップデートを実行するように設定できます。サーバは、これらのアップデートを実行するかどうかを設定できます。DHCP サーバは、PTR RR をアップデートするクライアントの完全修飾ドメイン名 (FQDN) を認識する必要があります。クライアントは Client FQDN と呼ばれる DHCP オプションを使用して、サーバに FQDN を提供します。

UDP パケット サイズ

DDNS は、DNS 要求者が UDP パケットのサイズをアドバタイズできるようにし、512 オクテットより大きいパケットの転送を容易にします。DNS サーバは UDP 上で要求を受信すると、OPT RR から UDP パケット サイズを識別し、要求者により指定された最大 UDP パケット サイズにできるだけ多くのリソース レコードを含めることができるよう、応答のサイズを調整します。DNS パケットのサイズは、BIND の場合は最大 4096 バイト、Windows 2003 DNS サーバの場合は 1280 バイトです。

次に示す追加の **message-length maximum** コマンドを使用できます。

- 既存のグローバル制限：**message-length maximum 512**
- クライアントまたはサーバ固有の制限：**message-length maximum client 4096** および **message-length maximum server 4096**
- OPT RR フィールドで指定されたダイナミック値：**message-length maximum client auto**

3つのコマンドが同時に存在する場合、ASA は、設定されたクライアントまたはサーバ制限まで長さの自動設定を可能にします。他のすべての DNS トラフィックについては、**message-length maximum** が使用されます。

DHCP サービスと DDNS サービスのガイドライン

この項では、DHCP および DDNS サービスを設定する前に確認する必要があるガイドラインおよび制限事項について説明します。

ファイアウォール モード

- DHCP リレーは、トランスペアレント ファイアウォール モード。
- DHCP サーバは、ブリッジグループ メンバー インターフェイス上のトランスペアレント ファイアウォール モードでサポートされます。
- DDNS は、トランスペアレント ファイアウォール モード。

IPv6

DHCP サーバの IPv6 はサポートされません。DHCP リレーの IPv6 は、。

DHCPv4 サーバ

- 使用可能な DHCP の最大プールは 256 アドレスです。
- インターフェイスごとに 1 つの DHCP サーバのみを設定できます。各インターフェイスは、専用のアドレスプールのアドレスを使用できます。しかし、DNS サーバ、ドメイン名、オプション、ping のタイムアウト、WINS サーバなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバによって使用されます。
- DHCP クライアントや DHCP リレー サービスは、サーバがイネーブルになっているインターフェイス上では設定できません。また、DHCP クライアントは、サーバがイネーブルになっているインターフェイスに直接接続する必要があります。
- ASA は、QIP DHCP サーバと DHCP プロキシ サービスとの併用をサポートしません。
- DHCP サーバもイネーブルになっている場合、リレーエージェントをイネーブルにすることはできません。
- DHCP サーバは、BOOTP 要求をサポートしません。

DHCP リレー

- シングルモードとコンテキストごとに、グローバルおよびインターフェイス固有のサーバを合わせて 10 台までの DHCPv4 リレー サーバを設定できます。インターフェイスごとに、4 台まで設定できます。
- シングルモードとコンテキストごとに、10 台までの DHCPv6 リレー サーバを設定できます。IPv6 のインターフェイス固有のサーバはサポートされません。
- DHCP サーバもイネーブルになっている場合、リレーエージェントをイネーブルにできません。
- DHCP リレー サービスは、トランスペアレントファイアウォールモード。ただし、アクセスルールを使用して DHCP トラフィックを通過させることはできます。DHCP 要求と応答が ASA を通過できるようにするには、2 つのアクセスルールを設定する必要があります。1 つは内部インターフェイスから外部（UDP 宛先ポート 67）への DHCP 要求を許可するもので、もう 1 つは逆方向（UDP 宛先ポート 68）に向かうサーバからの応答を許可するためのものです。
- IPv4 の場合、クライアントは直接 ASA に接続する必要があり、他のリレー エージェントやルータを介して要求を送信できません。IPv6 の場合、ASA は別のリレー サーバからのパケットをサポートします。
- DHCP クライアントは、ASA が要求をリレーする DHCP サーバとは別のインターフェイスに存在する必要があります。
- トラフィック ゾーン内のインターフェイスで DHCP リレーを有効にできません。

DHCP サーバの設定

ここでは、ASA の DHCP サーバを設定する方法について説明します。

手順

- ステップ 1 [DHCPv4 サーバの有効化（591 ページ）](#)。
- ステップ 2 [高度な DHCPv4 オプションの設定（594 ページ）](#)。

DHCPv4 サーバの有効化

ASA のインターフェイスで DHCP サーバをイネーブルにするには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [DHCP] > [DHCP Server] の順に選択します。

ステップ 2 インターフェイスを選択し、[Edit] をクリックします。

トランスペアレントモードでは、ブリッジグループメンバーインターフェイスを選択します。

- a) 選択したインターフェイス上でDHCPサーバをイネーブルにするには、[Enable DHCP Server] チェックボックスをオンにします。
- b) [DHCP Address Pool] フィールドに、DHCP サーバが使用する最下位から最上位の IP アドレスの範囲を入力します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があるため、インターフェイス自身の IP アドレスを含めることはできません。
- c) [Optional Parameters] 領域で、次の項目を設定します。
 - インターフェイスに設定された DNS サーバ (1 および 2)。
 - インターフェイスに設定された WINS サーバ (プライマリおよびセカンダリ)。
 - インターフェイスのドメイン名。
 - インターフェイス上で ASA が ICMP ping の応答を待つ時間 (ミリ秒単位)。
 - インターフェイス上に設定された DHCP サーバが、割り当てた IP アドレスの使用を DHCP クライアントに許可する時間。
 - 指定のインターフェイス (通常は外側) 上で ASA が DHCP クライアントとして動作している場合に、自動コンフィギュレーションのための DNS、WINS、ドメイン名情報を提供する DHCP クライアントのインターフェイス。
 - より多くの DHCP オプションを設定するには、[Advanced] をクリックして [Advanced DHCP Options] ダイアログボックスを表示します。詳細については、「[高度な DHCPv4 オプションの設定 \(594 ページ\)](#)」を参照してください。
- d) [Dynamic Settings for DHCP Server] 領域の [Update DNS Clients] チェックボックスをオンにして、クライアントの PTR リソース レコードを更新するデフォルトのアクションに加えて、選択した DHCP サーバでの次の更新アクションの実行を指定します。
 - [Update Both Records] チェックボックスをオンにして、DHCP サーバが A レコードと PTR RR の両方を更新するように指定します。
 - [Override Client Settings] チェックボックスをオンにして、DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションを上書きするように指定します。
- e) [OK] をクリックして、[Edit DHCP Server] ダイアログボックスを閉じます。

ステップ 3 (任意) (ルーテッドモード) 指定したインターフェイス (通常は外側) で ASA が DHCP クライアントとして動作している場合に限り、DHCP 自動コンフィギュレーションをイネーブル

にするには、DHCP サーバテーブルの下にある [Global DHCP Options] 領域の [Enable Auto-configuration from interface] チェックボックスをオンにします。

DHCP 自動コンフィギュレーションでは、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。自動コンフィギュレーションを介して取得された情報が、[Global DHCP Options] 領域でも手動で指定されている場合、検出された情報よりも手動で指定した情報の方が優先されます。

- ステップ 4** ドロップダウン リストから [auto-configuration interface] を選択します。
- ステップ 5** インターフェイスの DHCP または PPPoE クライアントの WINS パラメータを VPN クライアントのパラメータで上書きするには、[Allow VPN override] チェックボックスをオンにします。
- ステップ 6** [DNS Server 1] フィールドに、DHCP クライアント用のプライマリ DNS サーバの IP アドレスを入力します。
- ステップ 7** [DNS Server 2] フィールドに、DHCP クライアント用の代替 DNS サーバの IP アドレスを入力します。
- ステップ 8** [Domain Name] フィールドに、DHCP クライアント用の DNS ドメイン名（たとえば、example.com）を入力します。
- ステップ 9** [Lease Length] フィールドに、リースが期限切れになるまでにクライアントが割り当てられた IP アドレスを使用可能な時間を秒数で入力します。有効値の範囲は 300 ~ 1048575 秒です。デフォルト値は 3600 秒（1 時間）です。
- ステップ 10** [Primary WINS Server] フィールドに、DHCP クライアント用のプライマリ WINS サーバの IP アドレスを入力します。
- ステップ 11** [Secondary WINS Server] フィールドに、DHCP クライアント用の代替 WINS サーバの IP アドレスを入力します。
- ステップ 12** アドレスの衝突を避けるために、ASA は 1 つのアドレスに 2 つの ICMP ping パケットを送信してから、そのアドレスを DHCP クライアントに割り当てます。[Ping Timeout] フィールドに、ASA が DHCP ping の試行のタイムアウトを待つ時間をミリ秒単位で入力します。有効値の範囲は 10 ~ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。
- ステップ 13** 追加の DHCP オプションとパラメータを指定するには、[Advanced] をクリックして [Configuring Advanced DHCP Options] ダイアログボックスを表示します。詳細については、[高度な DHCPv4 オプションの設定（594 ページ）](#) を参照してください。
- ステップ 14** [Dynamic DNS Settings for DHCP Server] 領域で、DHCP サーバ用の DDNS 更新設定を設定します。[Update DNS Clients] チェックボックスをオンにして、クライアントの PTR リソースレコードを更新するデフォルトのアクションに加えて、選択した DHCP サーバが次の更新アクションも実行するように指定します。
- [Update Both Records] チェックボックスをオンにして、DHCP サーバが A レコードと PTR RR の両方を更新するように指定します。
 - [Override Client Settings] チェックボックスをオンにして、DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションを上書きするように指定します。

ステップ 15 [Apply] をクリックして変更内容を保存します。

高度な DHCPv4 オプションの設定

ASA は、RFC 2132、RFC 2562、および RFC 5510 に記載されている情報を送信する DHCP オプションをサポートしています。オプション 1、12、50～54、58～59、61、67、82 を除き、すべての DHCP オプション（1～255）がサポートされています。

手順

ステップ 1 [Configuration] > [Device Management] > [DHCP] > [DHCP Server] の順に選択し、[Advanced] をクリックします。

ステップ 2 ドロップダウンリストからオプションコードを選択します。

ステップ 3 設定するオプションを選択します。一部のオプションは標準です。標準オプションの場合、オプション名がオプション番号の後のカッコ内に表示され、オプション番号およびオプションパラメータは、オプションでサポートされるものに制限されます。他のすべてのオプションにはオプション番号だけが表示され、オプションに指定する適切なパラメータを選択する必要があります。たとえば、DHCP オプション 2（タイムオフセット）を選択した場合、このオプションに入力できるのは 16 進数値だけです。他のすべての DHCP オプションでは、すべてのオプション値タイプを使用できますが、適切なものを選択する必要があります。

ステップ 4 [Option Data] 領域に、このオプションによって DHCP クライアントに返す情報のタイプを指定します。標準 DHCP オプションの場合、サポートされるオプションの値タイプだけが使用可能です。他のすべての DHCP オプションでは、すべてのオプション値タイプを使用できます。

[Add] をクリックして、オプションを DHCP オプションリストに追加します。[Delete] をクリックして、オプションを DHCP オプションリストから削除します。

- [IP Address] をクリックして、IP アドレスが DHCP クライアントに返されることを示します。IP アドレスは最大 2 つまで指定できます。IP アドレス 1 および IP アドレス 2 は、ドット付き 10 進数表記の IP アドレスを示します。

(注) 関連付けられた [IP Address] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 3（ルーター）を選択した場合、フィールド名は [Router 1] および [Router 2] に変わります。

- [ASCII] をクリックして、ASCII 値が DHCP クライアントに返されることを指定します。[Data] フィールドに ASCII 文字列を入力します。文字列にスペースを含めることはできません。

(注) 関連付けられた [Data] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 14（ダンプファイル名）を選択した場合、関連付けられた [Data] フィールドの名前は [File Name] に変わります。

- [Hex] をクリックして、16 進数値が DHCP クライアントに返されることを指定します。[Data] フィールドに、偶数個の数字（スペースを含まない）から成る 16 進数文字列を入力します。0x プレフィックスを使用する必要はありません。

(注) 関連付けられた [Data] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 2（タイム オフセット）を選択した場合、関連付けられた [Data] フィールドは [Offset] フィールドになります。

ステップ 5 [OK] をクリックして、[Advanced DHCP Options] ダイアログボックスを閉じます。

ステップ 6 [Apply] をクリックして変更内容を保存します。

DHCP リレー エージェントの設定

インターフェイスに DHCP 要求が届くと、ユーザの設定に基づいて、ASA からその要求がリレーされる DHCP サーバが決定されます。設定できるサーバのタイプは次のとおりです。

- インターフェイス固有の DHCP サーバ：特定のインターフェイスに DHCP 要求が届くと、ASA はその要求をインターフェイス固有のサーバにだけリレーします。
- グローバル DHCP サーバ：インターフェイス固有のサーバが設定されていないインターフェイスに DHCP 要求が届くと、ASA はその要求をすべてのグローバル サーバにリレーします。インターフェイスにインターフェイス固有のサーバが設定されている場合、グローバル サーバは使用されません。

手順

ステップ 1 [Configuration] > [Device Management] > [DHCP] > [DHCP Relay] の順に選択します。

ステップ 2 [DHCP Relay Agent] 領域で、各インターフェイスに必要なサービスのチェックボックスをオンにします。

- [IPv4] > [DHCP Relay Enabled]。
- [IPv4] > [Set Route]：サーバからの DHCP メッセージのデフォルト ゲートウェイアドレスを、元の DHCP 要求をリレーした DHCP クライアントに最も近い ASA インターフェイスのアドレスに変更します。このアクションを行うと、クライアントは、自分のデフォルト ルートを設定して、DHCP サーバで異なるルータが指定されている場合でも、ASA をポイントすることができます。パケット内にデフォルトのルータオプションがなければ、ASA は、そのインターフェイスのアドレスを含んでいるデフォルト ルータを追加します。
- [IPv6] > [DHCP Relay Enabled]。
- [Trusted Interface]：信頼する DHCP クライアント インターフェイスを指定します。DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リ

レー エージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバにパケットを転送する前に、リレーエージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。[Set dhcp relay information as trusted on all interfaces] チェックボックスをオンにして、すべてのインターフェイスを信頼することもできます。

ステップ 3 [Global DHCP Relay Servers] 領域に、DHCP 要求をリレーする 1 つまたは複数の DHCP サーバを追加します。

- a) [Add] をクリックします。[Add Global DHCP Relay Server] ダイアログボックスが表示されます。
- b) [DHCP Server] フィールドに、DHCP サーバの IPv4 アドレスまたは IPv6 アドレスを入力します。
- c) [Interface] ドロップダウン リストから、指定した DHCP サーバが接続されているインターフェイスを選択します。
- d) [OK] をクリックします。

新たに追加されたグローバル DHCP リレー サーバが、[Global DHCP Relay Servers] リストに表示されます。

ステップ 4 （オプション）[IPv4 Timeout] フィールドに、DHCPv4 アドレス処理のために許容する時間を秒数で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 60 秒です。

ステップ 5 （オプション）[IPv6 Timeout] フィールドに、DHCPv6 アドレス処理のために許容する時間を秒数で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 60 秒です。

ステップ 6 [DHCP Relay Interface Servers] 領域で、特定のインターフェイスの DHCP 要求がリレーされるインターフェイス固有の DHCP サーバを 1 台以上追加します。

- a) [Add] をクリックします。[Add DHCP Relay Server] ダイアログボックスが表示されます。
- b) [Interface] ドロップダウン リストから、DHCP クライアントが接続されているインターフェイスを選択します。グローバル DHCP サーバの場合とは異なり、要求の出力インターフェイスを指定しないことに注意してください。代わりに、ASA はルーティングテーブルを使用して出力インターフェイスを決定します。
- c) [Server to] フィールドに DHCP サーバの IPv4 アドレスを入力し、[Add] をクリックします。サーバが右側のリストに追加されます。全体の最大数に余裕があれば、4 台までサーバを追加します。インターフェイス固有のサーバでは、IPv6 はサポートされていません。
- d) [OK] をクリックします。

新しく追加したインターフェイスの DHCP リレー サーバが、[DHCP Relay Interface Server] リストに表示されます。

ステップ 7 すべてのインターフェイスを信頼するインターフェイスとして設定するには、[Set dhcp relay information as trusted on all interfaces] チェックボックスをオンにします。あるいは、個々のインターフェイスを信頼することもできます。

ステップ 8 [Apply] をクリックして設定値を保存します。

DDNS の設定

ダイナミック DNS を設定し、DNS サーバをアップデートするには、次の手順を実行します。

手順

- ステップ 1 [Configuration] > [Device Management] > [DNS] > [Dynamic DNS] を選択します。
- ステップ 2 [Add] をクリックして、[Add Dynamic DNS Update Method] ダイアログボックスを表示します。
- ステップ 3 DDNS のアップデート方式の名前を入力します。
- ステップ 4 アップデート方式で設定された DNS 更新試行間の更新間隔を日、時間、分、および秒で指定します。
- 更新試行間の日数を 0 ～ 364 日の間で選択します。
 - 更新試行間の時間数を 0 ～ 23（整数）から選択します。
 - 更新試行間の分数を 0 ～ 59（整数）から選択します。
 - 更新試行間の秒数を 0 ～ 59（整数）から選択します。
- これらの単位は、追加式です。つまり、日数に 0、時間数に 0、分数に 5、秒数に 15 を入力した場合、このアップデート方式がアクティブである限り、5 分 15 秒ごとに更新が試行されます。
- ステップ 5 DNS クライアントがアップデートするサーバリソース レコードアップデートを保存するには、次のいずれかのオプションを選択します。
- A リソース レコードと PTR リソース レコードの両方。
 - A リソース レコードのみ。
- ステップ 6 [OK] をクリックして、[Add Dynamic DNS Update Method] ダイアログボックスを表示します。新しいダイナミック DNS クライアント設定が表示されます。
- (注) 既存の方式を編集する場合、[Name] フィールドは表示専用となっており、編集のために選択した方式の名前が表示されます。
- ステップ 7 設定されている各インターフェイスの DDNS 設定を追加するには、[Add] をクリックしての [Dynamic DNS Interface Settings] ダイアログボックスを表示します。
- ステップ 8 ドロップダウン リストからインターフェイスを選択します。
- ステップ 9 インターフェイスに割り当てられたアップデート方式をドロップダウン リストから選択します。

ステップ 10 DDNS クライアントのホスト名を入力します。

ステップ 11 リソース レコード アップデートを保存するには、次のいずれかのオプションを選択します。

- **[Default] (PTR Records)** では、サーバによりクライアントが PTR レコードの更新を要求するように指定されます。
- **[Both] (PTR Records および A Records)** では、サーバによりクライアントが A および PTR DNS リソース レコードの両方を要求するように指定されます。
- **[None]** では、サーバによりクライアントが更新を要求しないように指定されます。

(注) このアクションを有効にするには、選択したインターフェイス上で DHCP がイネーブルになっている必要があります。

ステップ 12 [OK] をクリックして、[Add Dynamic DNS Interface Settings] ダイアログボックスを閉じます。新しいダイナミック DNS インターフェイス設定が表示されます。

ステップ 13 変更を保存するには [Apply] をクリックし、変更を破棄して新しく入力するには [Reset] をクリックします。

DHCP および DDNS サービスのモニタリング

この項では、DHCP および DDNS の両方のサービスをモニタする手順について説明します。

DHCP サービスのモニタリング

- **[Monitoring] > [Interfaces] > [DHCP] > [DHCP Client Lease Information]**

このペインには、設定されている DHCP クライアントの IP アドレスが表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [DHCP Server Table]**

このペインには、設定されている動的な DHCP クライアントの IP アドレスが表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [DHCP Statistics]**

このペインには、DHCPv4 メッセージのタイプ、カウンタ、値、方向、受信メッセージ数、および送信メッセージ数が表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPv6 DHCP Relay Statistics]**

このペインには、DHCPv6 Relay メッセージのタイプ、カウンタ、値、方向、受信メッセージ数、および送信メッセージ数が表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPv6 DHCP Relay Binding]**

このペインには、DHCPv6 Relay バインディングが表示されます。

DDNS ステータスのモニタリング

DDNS ステータスのモニタリングについては、次のコマンドを参照してください。[Tools]> [Command Line Interface] でコマンドを入力します。

- **show running-config ddns**

このコマンドは、現在の DDNS コンフィギュレーションを表示します。

- **show running-config dns server-group**

このコマンドは、現在の DNS サーバグループのステータスを表示します。

DHCP および DDNS サービスの履歴

機能名	プラットフォーム リリース	説明
DHCP	7.0(1)	ASA は、DHCP サーバまたは DHCP リレー サービスを ASA のインターフェイスに接続されている DHCP クライアントに提供することができます。 次の画面が導入されました。 [Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。 [Configuration] > [Device Management] > [DHCP] > [DHCP Server]
DDNS	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Configuration] > [Device Management] > [DNS] > [DNS Client] [Configuration] > [Device Management] > [DNS] > [Dynamic DNS]
DHCP relay for IPv6 (DHCPv6)	9.0(1)	DHCP リレーに IPv6 サポートが追加されました。 次の画面が変更されました。 [Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。

機能名	プラットフォーム リリース	説明
インターフェイスごとのDHCP リレーサーバ (IPv4 のみ)	9.1(2)	<p>DHCP リレーサーバをインターフェイスごとに設定できるようになりました。特定のインターフェイスに届いた要求は、そのインターフェイス用に指定されたサーバに対してのみリレーされます。インターフェイス単位のDHCP リレーでは、IPv6 はサポートされません。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。</p>
DHCP の信頼できるインターフェイス	9.1(2)	<p>DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレーエージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド (サーバにパケットを転送する前に、リレーエージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド) が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。</p>

機能名	プラットフォーム リリース	説明
DHCP 再バインド機能	9.1(4)	DHCP 再バインドフェーズに、クライアントはトンネル グループ リスト内の他の DHCP サーバへの再バインドを試みるようになりました。このリリース以前には、DHCP リースの更新に失敗した場合、クライアントは代替サーバへ再バインドしませんでした。 変更された ASDM 画面はありません。
DHCP リレー サーバは、応答用の DHCP サーバ識別子を確認します。	9.2(4)/ 9.3(3)	ASA DHCP リレー サーバが不適切な DHCP サーバから応答を受信すると、応答を処理する前に、その応答が適切なサーバからのものであることを確認するようになりました。導入または変更されたコマンドはありません。変更された ASDM 画面はありません。 変更された ASDM 画面はありません。
DHCPv6 モニタリング	9.4(1)	IPv6 の DHCP 統計情報および IPv6 の DHCP バインディングをモニタできます。 次の画面が導入されました。[DHCPv6 monitoring] [Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Statistics, Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Binding]。



第 22 章

デジタル証明書

この章では、デジタル証明書の設定方法について説明します。

- [デジタル証明書の概要](#) (603 ページ)
- [デジタル証明書のガイドライン](#) (613 ページ)
- [デジタル証明書の設定](#) (615 ページ)
- [特定の証明書タイプの設定方法](#) (616 ページ)
- [証明書の有効期限アラートの設定 \(ID 証明書または CA 証明書用\)](#) (634 ページ)
- [デジタル証明書のモニタリング](#) (635 ページ)
- [証明書管理の履歴](#) (636 ページ)

デジタル証明書の概要

デジタル証明書は、認証に使用されるデジタル ID を保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASA に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。ASA では CRL (認証局の失効リストとも呼ばれます) に照らしてサードパーティの証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

次に、使用可能な各種デジタル証明書について説明します。

- CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。
- ID 証明書は、特定のシステムまたはホストの証明書です。この証明書も CA により発行されます。

- コード署名者証明書は、コードに署名するためのデジタル署名を作成する際に使用される特殊な証明書であり、署名されたコードそのものが証明書の作成元を示しています。

ローカルCAは、ASAの独立認証局機能を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。Webサイトのログインページからユーザ登録を行う場合には、ローカルCAにより実現されるセキュアで設定可能な内部認証局機能によって、証明書の認証を行うことができます。



- (注) CA証明書およびID証明書は、サイトツーサイトVPN接続およびリモートアクセスVPN接続の両方に適用されます。このマニュアルに記載の手順は、ASDM GUIでリモートアクセスVPNを使用する場合の手順です。

デジタル証明書は、認証に使用されるデジタルIDを保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、またはIPアドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CAは、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CAは、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証するPKIコンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASAに1つ以上のID証明書と、その発行元のCA証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。次に、使用可能な各種デジタル証明書について説明します。

- CA証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。
- 別のCA証明書により発行される証明書は、下位証明書と呼ばれます。

CAは、証明書要求の管理とデジタル証明書の発行を行います。デジタル証明書には、名前、シリアル番号、会社、部門、またはIPアドレスなど、ユーザまたはデバイスを識別する情報が含まれます。デジタル証明書には、ユーザまたはデバイスの公開キーのコピーも含まれています。CAは、信頼できるサードパーティ（VeriSignなど）の場合もあれば、組織内に設置したプライベートCA（インハウスCA）の場合もあります。



- ヒント 証明書コンフィギュレーションおよびロードバランシングの例は、次のURLを参照してください。<https://supportforums.cisco.com/docs/DOC-5964>

公開キー暗号化

デジタル署名は、公開キー暗号化によってイネーブルになり、デバイスおよびユーザを認証する手段です。RSA暗号化システムなどのPublic Key Cryptographyでは、各ユーザは、公開キーと秘密キーの両方を含むキーペアを使用します。これらのキーは、補足として機能し、一方で暗号化されたものは、もう一方で復号化できます。

簡単に言えば、データが秘密キーで暗号化されたとき、署名が形成されます。署名はデータに付加されて受信者に送信されます。受信者は送信者の公開キーをデータに適用します。データとともに送信された署名が、公開キーをデータに適用した結果と一致した場合、メッセージの有効性が確立されます。

このプロセスは、受信者が送信者の公開キーのコピーを持っていること、およびその公開キーが送信者になりすました別人のものではなく、送信者本人のものであることを受信者が強く確信していることに依存しています。

通常、送信者の公開キーは外部で取得するか、インストール時の操作によって取得します。たとえば、ほとんどの Web ブラウザでは、いくつかの CA のルート証明書がデフォルトで設定されています。VPN の場合、IKE プロトコルは IPsec のコンポーネントであり、デジタル署名を使用してピア デバイスを認証した後で、セキュリティ アソシエーションをセットアップできます。

証明書のスケーラビリティ

デジタル証明書がない場合、通信するピアごとに各 IPsec ピアを手動で設定する必要があります。そのため、ネットワークにピアを新たに追加するたびに、安全に通信するために各ピアで設定変更を行わなければなりません。

デジタル証明書を使用している場合、各ピアは CA に登録されます。2 つのピアは、通信を試みるときに、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアがネットワークに追加された場合は、そのピアを CA に登録するだけで済みます。他のピアを修正する必要はありません。新しいピアが IPsec 接続を試みると、証明書が自動的に交換され、そのピアの認証ができます。

CA を使用した場合、ピアはリモートピアに証明書を送り、公開キー暗号化を実行することによって、そのリモートピアに対して自分自身を認証します。各ピアから、CA によって発行された固有の証明書が送信されます。このプロセスが機能を果たすのは、関連付けられているピアの公開キーが各証明書にカプセル化され、各証明書が CA によって認証され、参加しているすべてのピアによって CA が認証権限者として認識されるためです。このプロセスは、RSA 署名付きの IKE と呼ばれます。

ピアは、証明書が期限満了になるまで、複数の IPsec セッションに対して、および複数の IPsec ピア宛てに証明書を送り続けることができます。証明書が期限満了になったときは、ピアの管理者は新しい証明書を CA から入手する必要があります。

CA は、IPsec に参加しなくなったピアの証明書を無効にすることもできます。無効にされた証明書は、他のピアからは有効な証明書とは認識されなくなります。無効にされた証明書は CRL に記載され、各ピアは別のピアの証明書を受け取る前に、CRL をチェックします。

CA の中には、実装の一部として RA を持つものもあります。RA は CA のプロキシの役割を果たすサーバであるため、CA が使用できないときも CA 機能は継続しています。

キーペア

キーペアは、RSA または楕円曲線署名アルゴリズム (ECDSA) キーであり、次の特性があります。

- RSA キーは SSH や SSL に使用できます。
- SCEP 登録は、RSA キーの証明書をサポートしています。
- RSA キー サイズの最大値は 4096 で、デフォルトは 2048 です。
- ECDSA キー長の最大値は 521 で、デフォルトは 384 です。
- 署名にも暗号化にも使用できる汎用 RSA キーペアを生成することも、署名用と暗号化用に別々の RSA キーペアを生成することもできます。SSL では署名用ではなく暗号化用のキーが使用されるので、署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。ただし、IKE では暗号化用ではなく署名用のキーが使用されます。キーを用途別に分けることで、キーの公開頻度が最小化されます。

トラストポイント

トラストポイントを使用すると、CA と証明書の管理とトレースができます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーションパラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

トラストポイントの定義が完了したら、CA の指定を必要とするコマンドで、名前によってトラストポイントを参照できます。トラストポイントは複数設定できます。



- (注) Cisco ASA に同じ CA を共有するトラストポイントが複数ある場合、CA を共有するトラストポイントのうち、ユーザ証明書の検証に使用できるのは 1 つだけです。CA を共有するどのトラストポイントを使用して、その CA が発行したユーザ証明書を検証するかを制御するには、**support-user-cert-validation** コマンドを使用します。

自動登録の場合は、登録 URL がトラストポイントに設定されている必要があります。また、トラストポイントが示す CA がネットワーク上で使用可能であり、SCEP をサポートしている必要があります。

キーペアと、トラストポイントに関連付けられている発行済み証明書は、PKCS12 形式でエクスポートとインポートができます。この形式は、異なる ASA 上のトラストポイントコンフィギュレーションを手動でコピーする場合に便利です。

認証登録

ASA は、トラストポイントごとに 1 つの CA 証明書が必要で、セキュリティアプライアンス自体には、トラストポイントで使用するキーのコンフィギュレーションに応じて 1 つまたは 2 つの証明書が必要です。トラストポイントが署名と暗号化に別々の RSA キーを使用する場合、

ASAには署名用と暗号化用の2つの証明書が必要になります。署名用と暗号化用のキーが同じである場合、必要な証明書は1つだけです。

ASAは、SCEPを使用した自動登録と、base-64-encoded証明書を直接端末に貼り付けられる手動登録をサポートしています。サイトツーサイトVPNの場合は、各ASAを登録する必要があります。リモートアクセスVPNの場合は、各ASAと各リモートアクセスVPNクライアントを登録する必要があります。

SCEP 要求のプロキシ

ASAは、AnyConnectとサードパーティCA間のSCEP要求のプロキシとして動作することができます。プロキシとして動作する場合に必要なのはCAがASAからアクセス可能であることのみです。ASAのこのサービスが機能するには、ASAが登録要求を送信する前に、ユーザがAAAでサポートされているいずれかの方法を使用して認証されている必要があります。また、ホストスキャンおよびダイナミックアクセスポリシーを使用して、登録資格のルールを適用することもできます。

ASAは、AnyConnect SSLまたはIKEv2 VPNセッションでのみこの機能をサポートしています。これは、Cisco IOS CS、Windows Server 2003 CA、およびWindows Server 2008 CAを含む、すべてのSCEP準拠CAをサポートしています。

クライアントレス（ブラウザベース）でのアクセスはSCEPプロキシをサポートしていませんが、WebLaunch（クライアントレス起動AnyConnect）はサポートしていません。

ASAは、証明書のポーリングはサポートしていません。

ASAはこの機能に対するロードバランシングをサポートしています。

失効チェック

証明書は発行されると、一定期間有効です。CAは、安全上の問題や名前またはアソシエーションの変更などの理由で、期限が切れる前に証明書を無効にすることがあります。CAは、無効になった証明書の署名付きリストを定期的に発行します。失効確認を有効にすることにより、CAが認証にその証明書を使用するたびに、その証明書が無効にされていないかどうか、ASAによってチェックされます。

失効確認を有効にすると、PKI証明書検証プロセス時にASAによって証明書の失効ステータスがチェックされます。これには、CRLチェック、OCSP、またはその両方が使用されます。OCSPは、最初の方式がエラーを返した場合に限り使用されます（たとえば、サーバが使用不可であることを示すエラー）。

CRLチェックを使用すると、ASAによって、無効になった（および失効解除された）証明書とその証明書シリアル番号がすべてリストされているCRLが取得、解析、およびキャッシュされます。ASAはCRL（認証局の失効リストとも呼ばれます）に基づいて証明書を検証します。検証は、ID証明書から下位証明書チェーンの認証局までさかのぼって行われます。

OCSPは、検証局に特定の証明書のステータスを問い合わせ、チェックを検証局が扱う範囲に限定するため、よりスケーラブルな方法を提供します。

サポート対象の CA サーバ

ASA は次の CA サーバをサポートしています。

Cisco IOS CS、ASA ローカル CA、およびサードパーティの X.509 準拠 CA ベンダー（次のベンダーが含まれますが、これらに限定はされません）。

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための1つの方法です。CRL コンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

証明書を認証するときに必ず **revocation-check crl** コマンドを使用して CRL チェックを行うように、ASA を設定できます。また、**revocation-check crl none** コマンドを使用して、CRL チェックをオプションにすることもできます。オプションにすると、更新された CRL データが CA から提供されない場合でも、証明書認証は成功します。

ASA は HTTP、SCEP、または LDAP を使用して、CA から CRL を取得できます。トラストポイントごとに取得された CRL は、トラストポイントごとに設定可能な時間だけキャッシュされます。

CRL のキャッシュに設定された時間を超過して ASA にキャッシュされている CRL がある場合、ASA はその CRL を、古すぎて信頼できない、つまり「失効した」と見なします。ASA は、次の証明書認証で失効した CRL のチェックが必要な場合に、より新しいバージョンの CRL を取得しようとします。

CRL のエン트리制限を超えると、ユーザ接続/証明書で失効チェックエラーが表示されることがあります。CRL あたりの最大エン트리数が 65534 を超えている場合、処理するエン트리数が多すぎることを示すメッセージが `syslog` から返されます。

ASA によって CRL がキャッシュされる時間は、次の 2 つの要素によって決まります。

- **cache-time** コマンドで指定される分数。デフォルト値は 60 分です。

- 取得した CRL 中の NextUpdate フィールド。このフィールドが CRL にない場合もあります。ASA が NextUpdate フィールドを必要とするかどうか、およびこのフィールドを使用するかどうかは、**enforcenextupdate** コマンドで制御します。

ASA では、これらの 2 つの要素が次のように使用されます。

- NextUpdate フィールドが不要の場合、**cache-time** コマンドで指定された時間が経過すると、ASA は CRL に失効のマークを付けます。
- NextUpdate フィールドが必要な場合、ASA は、**cache-time** コマンドと NextUpdate フィールドで指定されている 2 つの時間のうち短い方の時間で、CRL に失効のマークを付けます。たとえば、**cache-time** コマンドによってキャッシュ時間が 100 分に設定され、NextUpdate フィールドによって次のアップデートが 70 分後に指定されている場合、ASA は 70 分後に CRL に失効のマークを付けます。

ASA がメモリ不足で、特定のトラストポイント用にキャッシュされた CRL をすべて保存することができない場合、使用頻度が最も低い CRL が削除され、新しく取得した CRL 用の空き領域が確保されます。

OCSP

OCSP は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための 1 つの方法です。OCSP のコンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

OCSP によって、証明書のステータスをチェックする範囲が検証局（OCSP サーバ、応答側とも呼ばれます）に限定され、ASA によって検証局に特定の証明書のステータスに関する問い合わせが行われます。これは、CRL チェックよりもスケーラブルで、最新の失効ステータスを確認できる方法です。この方法は、PKI の導入規模が大きい場合に便利で、安全なネットワークを拡大できます。



(注) ASA では、OCSP 応答に 5 秒間のスキューを許可します。

証明書を認証するときに必ず **revocation-check ocsp** コマンドを使用して OCSP チェックを行うように、ASA を設定できます。また、**revocation-check ocsp none** コマンドを使用して、OCSP チェックをオプションにすることもできます。オプションにすると、更新された OCSP データが検証局から提供されない場合でも、証明書認証は成功します。

OCSP を利用すると、OCSP サーバの URL を 3 つの方法で定義できます。ASA は、これらのサーバを次の順に使用します。

1. **match certificate** コマンドの使用による証明書の照合の上書きルールで定義されている OCSP サーバの URL
2. **ocsp url** コマンドを使用して設定されている OCSP サーバの URL
3. クライアント証明書の AIA フィールド



- (注) トラストポイントでOCSPの応答側の自己署名した証明書を検証するように設定するには、信頼できるCA証明書として、この自己署名した応答側の証明書をそのトラストポイントにインポートします。次に、クライアント証明書を検証するトラストポイントで **match certificate** コマンドを設定して、応答側の証明書を検証するために、OCSPの応答側の自己署名された証明書を含むトラストポイントを使用するようにします。クライアント証明書の検証パスの外部にある応答側の証明書を検証する場合も、同じ手順で設定します。

通常、OCSPサーバ（応答側）の証明書によって、OCSP 応答が署名されます。ASA が応答を受け取ると、応答側の証明書を検証しようとします。通常、CA は、侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は一般に、応答側証明書に **ocsp-no-check** 拡張を含めて、この証明書では失効ステータスチェックが必要ないことを示します。ただし、この拡張がない場合、ASA はトラストポイントで指定されている方法で失効ステータスをチェックします。応答側の証明書を検証できない場合、失効ステータスをチェックできなくなります。この可能性を防ぐには、**revocation-check none** コマンドを使用して応答側の証明書を検証するトラストポイントを設定し、**revocation-check ocsp** コマンドを使用してクライアント証明書を設定します。

ローカル CA

ローカル CA では、次のタスクが実行されます。

- ASA で基本的な証明機関動作を統合する。
- 証明書を導入する。
- 発行済み証明書のセキュアな失効チェックを実行する。
- ブラウザベースとクライアントベースの両方で SSL VPN 接続とともに使用するために、ASA 上に認証局を提供する。
- 外部の証明書認証に依存することなく、ユーザに信頼できるデジタル証明書を提供する。
- 証明書認証のためのセキュアな内部認証局を提供し、Web サイト ログインを使用した簡単なユーザ登録を実現する。

ローカル CA ファイル用のストレージ

ASA では、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にローカル CA データベースが使用されます。このデータベースは、デフォルトでローカルフラッシュメモリに存在するか、または、マウントされて ASA にアクセス可能な外部のファイルシステム上に設定することもできます。

ローカル CA ユーザデータベースに保存できるユーザの数に制限はありませんが、フラッシュメモリストレージに問題がある場合、管理者に対策を取るよう警告する **syslog** が作成され、ローカル CA はストレージの問題が解決されるまでディセーブルになることがあります。フ

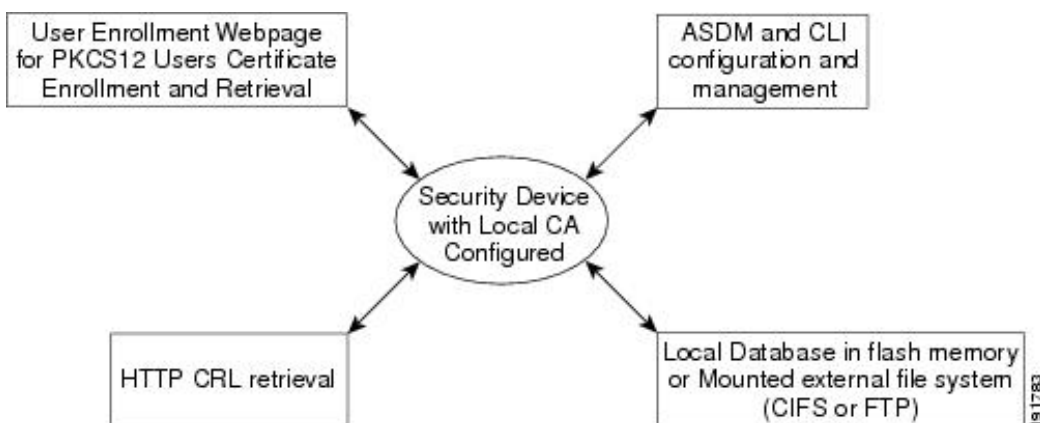
ラッシュメモリは、3500人以下のユーザを持つデータベースを保存できますが、ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

ローカル CA サーバ

ASA にローカル CA サーバを設定すると、ユーザは、Web サイトにログインし、ユーザの登録資格を検証するためにローカル CA 管理者によって与えられたユーザ名とワンタイムパスワードを入力することで、証明書を登録できます。

次の図に示すように、ローカル CA サーバは ASA に常駐し、Web サイトユーザからの登録要求や、その他の証明書を検証するデバイスおよび ASA から発信された CRL の問い合わせを処理します。ローカル CA データベースおよびコンフィギュレーションファイルは、ASA のフラッシュメモリ（デフォルトのストレージ）または個別のストレージデバイスに保持されます。

図 58: ローカル CA



証明書とユーザ ログイン クレデンシャル

この項では、認証と認可に証明書およびユーザ ログイン クレデンシャル（ユーザ名とパスワード）を使用する、さまざまな方法について説明します。これらの方式は、IPSec、AnyConnect、およびクライアントレス SSL VPN に適用されます。

すべての場合において、LDAP 認可では、パスワードをクレデンシャルとして使用しません。RADIUS 認可では、すべてのユーザの共通パスワードまたはユーザ名のいずれかを、パスワードとして使用します。

ユーザ ログイン クレデンシャル

認証および認可のデフォルトの方法では、ユーザ ログイン クレデンシャルを使用します。

- 認証
 - トンネルグループ（ASDM 接続プロファイルとも呼ばれます）の認証サーバグループ設定によりイネーブルにされます。

- ユーザ名とパスワードをクレデンシャルとして使用します。
- 認証
 - トンネルグループ (ASDM 接続プロファイルとも呼ばれます) の認可サーバグループ設定によりイネーブルにされます。
 - ユーザ名をクレデンシャルとして使用します。

証明書

ユーザデジタル証明書が設定されている場合、ASA によって最初に証明書が検証されます。ただし、証明書の DN は認証用のユーザ名として使用されません。

認証と認可の両方がイネーブルになっている場合、ASA によって、ユーザの認証と認可の両方にユーザ ログイン クレデンシャルが使用されます。

- 認証
 - 認証サーバグループ設定によってイネーブルにされます。
 - ユーザ名とパスワードをクレデンシャルとして使用します。
- 認証
 - 認可サーバグループ設定によってイネーブルにされます。
 - ユーザ名をクレデンシャルとして使用します。

認証がディセーブルで認可がイネーブルになっている場合、ASA によって認可にプライマリ DN のフィールドが使用されます。

- 認証
 - 認証サーバグループ設定によってディセーブル ([None] に設定) になります。
 - クレデンシャルは使用されません。
- 認証
 - 認可サーバグループ設定によってイネーブルにされます。
 - 証明書のプライマリ DN フィールドのユーザ名の値をクレデンシャルとして使用します。



(注) 証明書にプライマリ DN のフィールドが存在しない場合、ASA では、セカンダリ DN のフィールド値が認可要求のユーザ名として使用されます。

次のサブジェクト DN フィールドと値が含まれるユーザ証明書を例に挙げます。


```
Cn=anyuser,OU=sales,O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

プライマリ DN = EA (電子メールアドレス) およびセカンダリ DN = CN (一般名) の場合、許可要求で使われるユーザ名は `anyuser@example.com` になります。

デジタル証明書のガイドライン

この項では、デジタル証明書を設定する前に確認する必要があるガイドラインおよび制限事項について説明します。

コンテキストモードのガイドライン

- サードパーティ CA ではシングル コンテキスト モードでのみサポートされています。

フェールオーバーのガイドライン

- ステートフル フェールオーバーではセッションの複製はサポートされません。
- ローカル CA のフェールオーバーはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

ローカル CA 証明書

- 証明書をサポートするように ASA が正しく設定されていることを確認します。ASA の設定が正しくないと、登録に失敗したり、不正確な情報を含む証明書が要求されたりする可能性があります。
- ASA のホスト名とドメイン名が正しく設定されていることを確認します。現在設定されているホスト名とドメイン名を表示するには、**show running-config** コマンドを入力します。
- CA を設定する前に、ASA のクロックが正しく設定されていることを確認します。証明書には、有効になる日時と満了になる日時が指定されています。ASA が CA に登録して証明書を取得するとき、ASA は現在の時刻が証明書の有効期間の範囲内であるかどうかをチェックします。現在の時刻が有効期間の範囲外の場合、登録は失敗します。
- ローカル CA 証明書の有効期限の 30 日前に、ロールオーバー代替証明書が生成され、syslog メッセージ情報で管理者にローカル CA のロールオーバーの時期であることが知らされます。新しいローカル CA 証明書は、現在の証明書が有効期限に達する前に、必要なすべてのデバイスにインポートする必要があります。管理者が、新しいローカル CA 証明書としてロールオーバー証明書をインストールして応答しない場合、検証が失敗する可能性があります。
- ローカル CA 証明書は、同じキーペアを使用して期限満了後に自動的にロールオーバーします。ロールオーバー証明書は、base 64 形式でエクスポートに使用できます。

次に、base 64 で符号化されたローカル CA 証明書の例を示します。

```
MIIXlWIBAZCCF1EGCSqGSIB3DQEHAaCCF0IEghc+MIIXOjCCFzYGCsGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMQwDQIjph4SxJoyTgCAQGAgHbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWktHBIqkrm+td34q1NE1iGeP2YC94/NQ2z+4kS+uZzwcRh1lKEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMY6qbx2AC8I+q57+QG5vG515Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBghAzzuSmElm3j/2dQ3AtrolG9nIsRHgV39fcBgz4fEabHG7/Vanb+fj81d5n1OiJjDYD
bP86tvbZ2yOVZR6aKfVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWSyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUR0oG1DSrQrKeq/hj...
```

END OF CERTIFICATE

SCEP プロキシ サポート

- ASA と Cisco ISE ポリシー ノードが、同じ NTP サーバを使用して同期されていることを確認します。
- AnyConnect セキュア モビリティ クライアント 3.0 以降がエンドポイントで実行中である必要があります。
- グループ ポリシーの接続プロファイルで設定される認証方式は、AAA 認証と証明書認証の両方を使用するように設定する必要があります。
- SSL ポートが、IKEv2 VPN 接続用に開いている必要があります。
- CA は、自動許可モードになっている必要があります。

ローカル CA 証明書データベース

ローカル CA 証明書データベースを維持するため、データベースに変更が加えられるたびに **write memory** コマンドを使用して、証明書データベース ファイル LOCAL-CA-SERVER.cdb を保存してください。ローカル CA 証明書データベースには、次のファイルが含まれます。

- LOCAL-CA-SERVER.p12 は、ローカル CA サーバを最初にイネーブルにしたときに生成されたローカル CA 証明書とキー ペアのアーカイブです。
- LOCAL-CA-SERVER.crl ファイルは、実際の CRL です。
- LOCAL-CA-SERVER.ser ファイルでは、発行済み証明書のシリアル番号が追跡されます。

その他のガイドライン

- ASA が CA サーバまたはクライアントとして設定されている場合、推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期を制限してください。このガイドラインは、サードパーティベンダーからインポートした証明書にも適用されます。
- フェールオーバーがイネーブルになっている場合、ローカル CA は設定できません。ローカル CA サーバを設定できるのは、フェールオーバーのないスタンドアロン ASA のみです。詳細については、「CSCty43366」を参照してください。

- 証明書の登録が完了すると、ASA により、ユーザのキー ペアと証明書チェーンを含む PKCS12 ファイルが保存されます。これには、登録ごとに約 2 KB のフラッシュ メモリまたはディスク領域が必要です。実際のディスク領域の量は、設定されている RSA キー サイズと証明書フィールドによって異なります。使用できるフラッシュ メモリの量が限られている ASA に、保留中の証明書登録を多数追加する場合には、このガイドラインに注意してください。これらの PKCS12 ファイルは、設定されている登録の取得タイムアウトの間、フラッシュ メモリに保存されます。キー サイズは 2048 以上を使用することをお勧めします。
- **lifetime ca-certificate** コマンドは、ローカル CA サーバ証明書の初回生成時（初めてローカル CA サーバを設定し、**no shutdown** コマンドを発行するとき）に有効になります。CA 証明書の期限が切れると、設定されたライフタイム値を使用して新しい CA 証明書が生成されます。既存の CA 証明書のライフタイム値は変更できません。
- 管理インターフェイスへの ASDM トラフィックと HTTPS トラフィックを保護するために、アイデンティティ証明書を使用するよう ASA を設定する必要があります。SCEP により自動的に生成される ID 証明書はレポートのたびに再生成されるため、必ず独自の ID 証明書を手動でインストールしてください。SSL のみに適用されるこのプロシージャの例については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml.
- ASA および AnyConnect クライアントで検証できるのは、[X520Serialnumber] フィールド ([SubjectName] のシリアル番号) が PrintableString 形式である証明書のみです。シリアル番号の形式に UTF8 などのエンコーディングが使用されている場合、証明書認証は失敗します。
- ASA でのインポート時は、有効な文字と値だけを証明書パラメータに使用してください。
- ワイルドカード (*) 記号を使用するには、文字列値でこの文字を使用できるエンコードを CA サーバで使用していることを確認してください。RFC 5280 では UTF8String または PrintableString を使用することを推奨していますが、PrintableString ではこのワイルドカード文字を有効であると認識しないため UTF8String を使用する必要があります。ASA は、インポート中に無効な文字または値が見つかったら、インポートした証明書を拒否します。次に例を示します。

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H+ytes
as CA certificate:0U0= \Ivr"phÖV°3é4p0 CRYPTO_PKI (make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

デジタル証明書の設定

ここでは、デジタル証明書の設定方法について説明します。

特定の証明書タイプの設定方法

信頼できる証明書を確立すると、アイデンティティ証明書の確立などの基本的なタスクや、ローカル CA 証明書やコード署名証明書の確立などのさらに高度な設定を行なえるようになります。

始める前に

デジタル証明書情報に目を通し、信頼できる証明書を確立します。秘密キーが設定されていない CA 証明書は、すべての VPN プロトコルと webvpn で使用され、トラストポイントで着信クライアント証明書を検証するように設定されています。また、トラストポイントとは、HTTPS サーバにプロキシ接続された接続を検証し、smart-call-home 証明書を検証する、webvpn 機能によって使用される信頼できる証明書の一覧のことです。

手順

-
- ステップ 1** アイデンティティ証明書は、対応する秘密キーとともに ASA に設定される証明書です。これは、SSL サービスや IPsec サービスを確立する際のアウトバウンドの暗号化またはシグネチャの生成に使用され、トラストポイントを登録することによって取得されます。アイデンティティ証明書を設定するには、[ID 証明書 \(616 ページ\)](#) を参照してください。
 - ステップ 2** ローカル CA を設定すると、VPN クライアントが ASA から証明書を直接登録できるようになります。この高度な設定により、ASA は CA に変換されます。CA を設定するには、[CA 証明書 \(623 ページ\)](#) を参照してください。
 - ステップ 3** WebVPN Java コード署名機能の一部としてアイデンティティ証明書を使用する場合は、[コード署名者証明書 \(633 ページ\)](#) を参照してください。
-

次のタスク

証明書の有効期限にアラートを設定するか、デジタル証明書や証明書の管理履歴をモニタします。

ID 証明書

アイデンティティ証明書は、ASA 内の VPN アクセスの認証に使用できます。

[Identity Certificates Authentication] ペインでは、次のタスクを実行できます。

- [アイデンティティ証明書の追加またはインポート \(617 ページ\)](#)。
- CA からの要求として CMPv2 登録の有効化
- ID 証明書の詳細を表示する。
- 既存の ID 証明書を削除する。

- [アイデンティティ証明書のエクスポート \(620 ページ\)](#)。
- 証明書有効期限のアラートを設定する。
- Etrust でアイデンティティ証明書を登録する [証明書署名要求の生成 \(620 ページ\)](#)。

アイデンティティ証明書の追加またはインポート

新しい ID 証明書コンフィギュレーションを追加またはインポートするには、次の手順を実行します。

手順

- ステップ 1** [Configuration] > [Remote Access VPN] > [Certificate Management] > [Identity Certificates] の順に選択します。
- ステップ 2** [Add] をクリックします。
選択されたトラストポイント名が上部に示された [Add Identity Certificate] ダイアログボックスが表示されます。
- ステップ 3** [Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)] オプション ボタンをクリックして、既存のファイルから ID 証明書をインポートします。
- ステップ 4** PKCS12 ファイルの復号化に使用するパスフレーズを入力します。
- ステップ 5** ファイルのパス名を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示します。証明書ファイルを見つけて、[Import ID Certificate File] をクリックします。
- ステップ 6** [Add a new Global Controller] オプション ボタンをクリックして、新しい ID 証明書を追加します。
- ステップ 7** [New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。
- ステップ 8** RSA または ECDSA キーのタイプを選択します。
- ステップ 9** [Use default keypair name] オプション ボタンをクリックして、デフォルトのキー ペア名を使用します。
- ステップ 10** [Enter a new key pair name] オプション ボタンをクリックして、新しい名前を入力します。
- ステップ 11** ドロップダウン リストから係数サイズを選択します。係数サイズが不明な場合は、Etrust にお問い合わせください。
- ステップ 12** [General purpose] オプション ボタン (デフォルト) または [Special] オプション ボタンをクリックして、キー ペアの用途を選択します。[Special] オプション ボタンを選択すると、ASA により署名用と暗号化用の 2 つのキー ペアが生成されます。この選択は、対応する識別用に 2 つの証明書が必要なことを示します。
- ステップ 13** [Generate Now] をクリックして新しいキー ペアを作成し、[Show] をクリックして [Key Pair Details] ダイアログボックスを表示します。ここには、次の表示専用の情報が示されます。
 - 公開キーが認証の対象となるキー ペアの名前。
 - キー ペアの生成日時。

- RSA キー ペアの用途。
- キー ペアの係数サイズ (512、768、1024、2048、および 4096 ビット)。デフォルトは 1024 です。
- テキスト形式の特定のキー データを含むキー データ。

ステップ 14 完了したら、[OK] をクリックします。

ステップ 15 ID 証明書で DN を形成するための証明書サブジェクト DN を選択します。その後、[Select] をクリックして [Certificate Subject DN] ダイアログボックスを表示します。

ステップ 16 ドロップダウンリストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- **Common Name (CN)**
- **Department (OU)**
- **Company Name (O)**
- **Country (C)**
- **State/Province (ST)**
- **Location (L)**
- **E-mail Address (EA)**

ステップ 17 完了したら、[OK] をクリックします。

ステップ 18 自己署名証明書を作成するには、[Generate self-signed certificate] チェック ボックスをオンにします。

ステップ 19 アイデンティティ証明書をローカル CA として機能させるには、[Act as local certificate authority and issue dynamic certificates to TLS proxy] チェックボックスをオンにします。

ステップ 20 追加のアイデンティティ証明書設定を行うには、[Advanced] をクリックします。

[Certificate Parameters]、[Enrollment Mode]、および [SCEP Challenge Password] の 3 つのタブを持つ [Advanced Options] ダイアログボックスが表示されます。

(注) 登録モード設定と SCEP チャレンジパスワードは自己署名証明書では使用できません。

ステップ 21 [Certificate Parameters] タブをクリックし、次の情報を入力します。

- DNS ツリー階層内のノードの位置を示す FQDN (完全修飾ドメイン名)。
- ID 証明書に関連付けられている電子メールアドレス。
- 4 分割ドット付き 10 進表記の、ネットワーク上の ASA IP アドレス。
- [Include serial number of the device] チェックボックスをオンにして、ASA のシリアル番号を証明書パラメータに追加します。

ステップ 22 [Enrollment Mode] タブをクリックし、次の情報を入力します。

- [Request by manual enrollment] オプション ボタンまたは [Request from a CA] オプション ボタンをクリックして、登録方式を選択します。
- SCEP を介して自動的にインストールされる証明書の登録 URL。
- ID 証明書のインストールに許可される最大再試行回数。デフォルトは 1 分です。
- ID 証明書のインストールに許可される最大再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

ステップ 23 [SCEP Challenge Password] タブをクリックし、次の情報を入力します。

- SCEP パスワード
- SCEP パスワードを確認のために再入力

ステップ 24 完了したら、[OK] をクリックします。

ステップ 25 この証明書で他の証明書に署名できるようにする場合は、[Enable CA flag in basic constraints extension] をオンにします。

基本制約の拡張によって、証明書のサブジェクトが認証局 (CA) かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。これらの項目が証明書に存在することは、証明書の公開キーを使用して証明書の署名を検証できることを示します。このオプションをオンのままにしておいても、特に問題はありません。

ステップ 26 [Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。

[Identity Certificates] リストに新しい ID 証明書が表示されます。

ステップ 27 [Apply] をクリックし、新しい ID 証明書コンフィギュレーションを保存します。

ステップ 28 [Show Details] をクリックして、次の 3 つの表示専用タブが含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キータイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

ステップ 29 ID 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

- (注) 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

アイデンティティ証明書のエクスポート

ID 証明書をエクスポートするには、次の手順を実行します。

手順

- ステップ 1 [Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。
- ステップ 2 証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。または、[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。
- ステップ 3 [PKCS12 Format] オプション ボタンまたは [PEM Format] オプション ボタンをクリックして、証明書の形式を選択します。
- ステップ 4 PKCS12 ファイルをエクスポート用に暗号化するために使用するパスフレーズを入力します。
- ステップ 5 暗号化パスフレーズを確認のために再入力します。
- ステップ 6 [Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

情報ダイアログボックスが表示され、証明書コンフィギュレーションファイルが指定の場所に正常にエクスポートされたことが示されます。

証明書署名要求の生成

Entrust に送信する証明書署名要求を生成するには、次の手順を実行します。

手順

- ステップ 1 [Enroll ASA SSL VPN with Entrust] をクリックして、[Generate Certificate Signing Request] ダイアログボックスを表示します。
- ステップ 2 [Key Pair] 領域で次の手順を実行します。
 - a) ドロップダウンリストから、設定されたキー ペアのいずれかを選択します。
 - b) [Show] をクリックして [Key Details] ダイアログボックスを表示します。ここには、選択されたキー ペアの生成日時、用途（一般的または特殊な用途）、係数サイズ、およびキー データといった情報が示されます。
 - c) 完了したら、[OK] をクリックします。
 - d) [New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。生成したキー ペアを ASA に送信するか、ファイルに保存することができます。

ステップ 3 [Certificate Subject DN] 領域に次の情報を入力します。

- a) ASA の FQDN または IP アドレス。
- b) 会社の名前。
- c) 2 文字の国番号。

ステップ 4 [Optional Parameters] 領域で次の手順を実行します。

- a) [Select] をクリックして、[Additional DN Attributes] ダイアログボックスを表示します。
- b) ドロップダウンリストから追加する属性を選択し、値を入力します。
- c) [Add] をクリックして、各属性を [attribute] テーブルに追加します。
- d) [Delete] をクリックして、[attribute] テーブルから属性を削除します。
- e) 完了したら、[OK] をクリックします。

[Additional DN Attributes] フィールドに追加された属性が表示されます。

ステップ 5 CA から要求された場合は、完全修飾ドメイン名情報を追加で入力します。

ステップ 6 [Generate Request] をクリックして、証明書署名要求を生成します。これを Entrust に送信することも、ファイルに保存して後で送信することもできます。

CSR が示された [Enroll with Entrust] ダイアログボックスが表示されます。

ステップ 7 [request a certificate from Entrust] リンクをクリックして、登録プロセスを完了します。その後、示された CSR をコピーして貼り付け、それを Entrust Web フォーム (<http://www.entrust.net/cisco/>) を使用して送信します。後で登録する場合は、生成された CSR をファイルに保存し、[Identity Certificates] ペインで [enroll with Entrust] リンクをクリックします。

ステップ 8 Entrust により、要求の認証が確認された後、証明書が発行されます。これには数分かかる場合があります。次に、[Identity Certificate] ペインで保留中の要求を選択し、[Install] をクリックして、証明書をインストールする必要があります。

ステップ 9 [Close] をクリックして、[Enroll with Entrust] ダイアログボックスを閉じます。

アイデンティティ証明書のインストール

新しい ID 証明書をインストールするには、次の手順を実行します。

手順

- ステップ 1** [Identity Certificates] ペインで [Add] をクリックし、[Add Identity Certificate] ダイアログボックスを表示します。
- ステップ 2** [Add a new identity certificate] オプション ボタンをクリックします。
- ステップ 3** キー ペアを変更するか、新しいキー ペアを作成します。キー ペアは必須です。
- ステップ 4** 証明書サブジェクト DN 情報を入力し、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。
- ステップ 5** 関係する CA で必要なサブジェクト DN 属性をすべて指定し、[OK] をクリックして [Certificate Subject DN] ダイアログボックスを閉じます。

- ステップ 6** [Add Identity Certificate] ダイアログボックスで、[Advanced] をクリックして [Advanced Options] ダイアログボックスを表示します。
- ステップ 7** 以降の手順については、[アイデンティティ証明書の追加またはインポート \(617ページ\)](#) の手順 17 ~ 23 を参照してください。
- ステップ 8** [Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。
[Identity Certificate Request] ダイアログボックスが表示されます。
- ステップ 9** テキストタイプの CSR ファイル名 (c:\verisign-csr.txt など) を入力し、[OK] をクリックします。
- ステップ 10** CSR テキスト ファイルを CA に送信します。送信する代わりに、CA の Web サイトにある CSR 登録ページにテキスト ファイルを貼り付けることもできます。
- ステップ 11** CA から ID 証明書が返されたら、[Identity Certificates] ペインに移動し、保留中の証明書エントリを選択して、[Install] をクリックします。
[Install Identity Certificate] ダイアログボックスが表示されます。
- ステップ 12** 該当するオプション ボタンをクリックして、次のいずれかのオプションを選択します。
- Install from a file
または、[Browse] をクリックし、ファイルを検索します。
 - Paste the certificate data in base-64 format
コピーした証明書データを指定された領域に貼り付けます。
- ステップ 13** [Install Certificate] をクリックします。
- ステップ 14** [Apply] をクリックし、新しくインストールした証明書とその ASA コンフィギュレーションを保存します。
- ステップ 15** 選択した ID 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの表示専用タブが含まれる [Certificate Details] ダイアログボックスを表示します。
[General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
[Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
[Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。
- ステップ 16** コード署名者証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

(注) 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Import] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

CA 証明書

このページで、CA 証明書を管理します。次のトピックでは、実行できることについて説明します。

CA 証明書の追加またはインストール

CA 証明書を追加またはインストールするには、次の手順を実行します。

手順

- ステップ 1 [Configuration] > [Remote Access VPN] > [Certificate Management] > [CA Certificates] の順に選択します。
- ステップ 2 [Add] をクリックします。
[Install Certificate] ダイアログボックスが表示されます。
- ステップ 3 [Install from a file] オプション ボタンをクリックして、既存のファイルから証明書設定を追加します（これがデフォルト設定です）。
- ステップ 4 パスおよびファイル名を入力するか、または[Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。
- ステップ 5 [Certificate Installation] ダイアログボックスが表示され、証明書が正常にインストールされたことを示す確認メッセージが示されます。[OK] をクリックして、このダイアログボックスを閉じます。
- ステップ 6 [Paste certificate in PEM format] オプション ボタンをクリックして、手動で登録します。
- ステップ 7 PEM 形式（base64 または 16 進数）の証明書をコピーして、指定の領域に貼り付け、[Install Certificate] をクリックします。
- ステップ 8 [Certificate Installation] ダイアログボックスが表示され、証明書が正常にインストールされたことを示す確認メッセージが示されます。[OK] をクリックして、このダイアログボックスを閉じます。
- ステップ 9 [Use SCEP] オプション ボタンをクリックして、自動で登録します。ASA が、SCEP を使用して CA に接続し、証明書を取得して、証明書をデバイスにインストールします。SCEP を使用するには、インターネットを介して、SCEP をサポートする CA に登録する必要があります。SCEP を使用した自動登録では、ユーザは次の情報を入力する必要があります。
 - 自動インストールする証明書のパスとファイル名。
 - 証明書のインストールの最大再試行分数。デフォルトは 1 分です。

- 証明書のインストールの再試行回数。デフォルトは0です。この場合は、再試行時間内であれば何度でも再試行できます。

ステップ 10 新規および既存の証明書のその他のコンフィギュレーションオプションを表示するには、[More Options] をクリックします。

[Configuration Options for CA Certificates] ペインが表示されます。

ステップ 11 既存の CA 証明書コンフィギュレーションを変更するには、コンフィギュレーションを選択し、[Edit] をクリックします。

ステップ 12 CA 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

(注) 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

ステップ 13 [Show Details] をクリックして、次の3つの表示専用タブが含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キータイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

失効に関する CA 証明書の設定

失効に関して CA 証明書を設定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Revocation Check] タブをクリックします。

ステップ 3 証明書の失効チェックをディセーブルにするには、[Do not check certificates for revocation] オプション ボタンをクリックします。

ステップ 4 1つ以上の失効チェック方式 (CRL または OCSP) を選択するには、[Check certificates for revocation] オプション ボタンをクリックします。

- ステップ 5** [Add] をクリックして失効方式を右側に移動すると、その方式が使用可能になります。[Move Up] または [Move Down] をクリックして、方式の順序を変更します。
- 選択した方式は、追加した順序で実装されます。方式からエラーが返された場合は、その次の失効チェック方式がアクティブになります。
- ステップ 6** 証明書の検証中に失効チェックのエラーを無視するには、[Consider certificate valid if revocation checking returns errors] チェックボックスをオンにします。
- ステップ 7** [OK] をクリックして、[Revocation Check] タブを閉じます。

CRL 取得ポリシーの設定

CRL 取得ポリシーを設定するには、次の手順を実行します。

手順

-
- ステップ 1** [Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。
- ステップ 2** [Use CRL Distribution Point from the certificate] チェックボックスをオンにして、チェック対象の証明書から CRL 分散ポイントに失効チェックを転送します。
- ステップ 3** [Use Static URLs configured below] チェックボックスをオンにして、CRL の取得に使用する特定の URL を一覧表示します。選択した URL は、追加した順序で実装されます。指定した URL でエラーが発生した場合は、その次の URL が使用されます。
- ステップ 4** [Static Configuration] 領域の [Add] をクリックします。
- [Add Static URL] ダイアログボックスが表示されます。
- ステップ 5** CRL の分散に使用するスタティック URL を入力して、[OK] をクリックします。
- 入力した URL が [Static URLs] リストに表示されます。
- ステップ 6** [OK] をクリックして、このダイアログボックスを閉じます。

CRL 取得方式の設定

CRL 取得方式を設定するには、次の手順を実行します。

手順

-
- ステップ 1** [Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Configuration Options for CA Certificates] ペインで [CRL Retrieval Methods] タブをクリックします。

ステップ 3 次の 3 つの取得方式のいずれかを選択します。

- CRL の取得で LDAP をイネーブルにするには、[Enable Lightweight Directory Access Protocol (LDAP)] チェックボックスをオンにします。LDAP を使用して CRL を取得する場合は、指定した LDAP サーバにパスワードを使用して接続することで、LDAP セッションが開始されます。デフォルトの場合、この接続には TCP ポート 389 を使用されます。次の必須パラメータを入力します。

- **Name**
- **Password**
- **Confirm Password**
- デフォルト サーバ (サーバ名)
- デフォルト ポート (389)

- CRL の取得で HTTP をイネーブルにするには、[Enable HTTP] チェックボックスをオンにします。

ステップ 4 [OK] をクリックして、このタブを閉じます。

OCSP ルールの設定

X.509 デジタル証明書の失効ステータスを取得するための OCSP ルールを設定するには、次の手順を実行します。

始める前に

OCSP ルールを追加する前に、必ず証明書マップを設定しておいてください。証明書マップが設定されていない場合、エラーメッセージが表示されます。

手順

ステップ 1 [Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Configuration Options for CA Certificates] ペインで [OCSP Rules] タブをクリックします。

ステップ 3 この OCSP ルールと一致する証明書マップを選択します。証明書マップにより、ユーザ権限と、証明書の特定のフィールドとの照合が行われます。[Certificate] フィールドに、ASA において応答側の証明書の検証に使用される CA の名前が表示されます。[Index] フィールドに、ルールプライオリティ番号が表示されます。[URL] フィールドに、この証明書の OCSP サーバの URL が表示されます。

- ステップ 4** [Add] をクリックします。
[Add OCSP Rule] ダイアログボックスが表示されます。
- ステップ 5** 使用する証明書マップをドロップダウンリストから選択します。
- ステップ 6** 使用する証明書をドロップダウンリストから選択します。
- ステップ 7** ルールのプライオリティ番号を入力します。
- ステップ 8** この証明書の OCSP サーバの URL を入力します。
- ステップ 9** 完了したら、[OK] をクリックして、このダイアログボックスを閉じます。
新しく追加された OCSP ルールがリストに表示されます。
- ステップ 10** [OK] をクリックして、このタブを閉じます。

高度な CRL および OCSP の設定

CRL および OCSP の追加設定を行うには、次の手順を実行します。

手順

- ステップ 1** [Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。
- ステップ 2** [Configuration Options for CA Certificates] ペインで [Advanced] タブをクリックします。
- ステップ 3** [CRL Options] 領域にキャッシュの更新間隔を分数で入力します。デフォルトは 60 分です。範囲は 1 ~ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。
- ステップ 4** [Enforce next CRL update] チェックボックスをオンにして、Next Update 値の有効期限が切れていない CRL に限り、有効な CRL として使用できるようにします。[Enforce next CRL update] チェックボックスをオフにすると、Next Update 値がない場合や、Next Update 値の有効期限が切れている場合でも有効な CRL として使用できます。
- ステップ 5** [OCSP Options] 領域に OCSP サーバの URL を入力します。ASA で使用される OCSP サーバは、次の順で選択されます。
- 一致証明書上書きルールの OCSP URL に対応するサーバ
 - 選択された [OCSP Options] 属性に設定した OCSP URL に対応するサーバ
 - ユーザ証明書の AIA フィールド
- ステップ 6** デフォルトでは、[Disable nonce extension] チェックボックスがオンになっています。この設定では、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンズ拡張を照合し、両者が同一であることを確認す

ることで、リプレイアタックを防ぐことができます。ただし、事前に生成した応答には、各要求と一致するナンス拡張は含まれていません。そのため、使用している OCSP サーバから、事前に生成した応答を送信する場合は、[Disable nonce extension] チェックボックスをオフにしてください。

ステップ 7 [Other Options] 領域で、次のいずれかのオプションを選択します。

- 指定した CA の証明書を ASA で受け入れるようにするには、[Accept certificates issued by this CA] チェックボックスをオンにします。
- 下位 CA の証明書を ASA で受け入れるようにするには、[Accept certificates issued by the subordinate CAs of this CA] チェックボックスをオンにします。

ステップ 8 [OK] をクリックしてこのタブを閉じ、[Apply] をクリックしてコンフィギュレーションの変更を保存します。

ローカル CA サーバの設定

ASA でローカル CA サーバを設定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Certificate Management] > [Local Certificate Authority] > [CA Server] の順に選択します。

ステップ 2 ローカル CA サーバをアクティブにするには、[Enable Certificate Authority Server] チェックボックスをオンにします。デフォルト設定は、ディセーブル（オフ）です。ローカル CA サーバをイネーブルにすると、ASA によりローカル CA サーバ証明書、キー ペア、および必要なデータベース ファイルが生成され、ローカル CA サーバ証明書とキー ペアが PKCS12 ファイルにアーカイブされます。

(注) 設定済みのローカル CA をイネーブルにする前に、オプションのすべての設定を慎重に見直してください。イネーブルにした後で、証明書の発行者名とキー サイズ サーバ値を変更することはできません。

自己署名した証明書のキーの使用拡張により、キー暗号化、キー シグニチャ、CRL 署名、および証明書署名がイネーブルになります。

ステップ 3 ローカル CA を初めてイネーブルにするときには、英数字のイネーブル パスフレーズを入力し、確認のために再入力する必要があります。イネーブル パスフレーズは、7 文字以上の英数字である必要があります。このパスフレーズにより、ストレージにアーカイブされたローカル CA 証明書およびローカル CA 証明書のキー ペアが保護され、不正なシャットダウンや予期しないシャットダウンが発生しないようにローカル CA サーバが保護されます。ローカル CA 証明書またはキー ペアが失われ、その復元が必要となった場合、PKCS12 アーカイブのロックを解除するためには、このパスフレーズが必要です。

(注) ローカル CA サーバをイネーブルにするには、イネーブルパスフレーズが必要です。イネーブルパスフレーズの記録は、必ず安全な場所に保管してください。

ステップ 4 ASA をリブートしてもコンフィギュレーションが失われないように、[Apply] をクリックして、ローカル CA 証明書とキーペアを保存します。

ステップ 5 ローカル CA の初回設定後にローカル CA を変更または再設定する場合は、[Enable Certificate Authority Server] チェックボックスをオフにして、ASA 上のローカル CA サーバをシャットダウンする必要があります。この状態では、コンフィギュレーションおよびすべての関連ファイルはストレージ内に保持され、登録はディセーブルになっています。

設定したローカル CA がイネーブルになると、次の 2 つの設定が表示専用になります。

- [Issuer Name] フィールド。発行元のサブジェクト名とドメイン名がリストで示されます。これは、ユーザ名とサブジェクト名のデフォルト DN 設定により構成され、cn=FQDN という形式で示されます。ローカル CA サーバは、証明書を付与するエンティティです。証明書のデフォルト名は、cn=hostname.domainname という形式で表示されます。
- [CA Server Key Size] 設定。これは、ローカル CA サーバに生成されるサーバ証明書を対象とします。キーサイズには、キーごとに 512、768、1024、2048、または 4096 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。キーサイズは 2048 以上を使用することをお勧めします。

ステップ 6 ドロップダウンリストから、ローカル CA サーバが発行した各ユーザ証明書に対して生成されるキーペアのクライアントキーサイズを選択します。キーサイズには、キーごとに 512、768、1024、2048、または 4096 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。キーサイズは 2048 以上を使用することをお勧めします。

ステップ 7 CA 証明書のライフタイム値を入力します。これは、CA サーバ証明書の有効期間を日数単位で指定するものです。デフォルトは 3650 日 (10 年) です。推奨される終了日 (2038 年 1 月 19 日 03:14:08 UTC) を超えないよう、証明書の有効期間を制限します。

ローカル CA サーバでは、CA 証明書の期限が切れる 30 日前に後継の CA 証明書が自動的に生成されます。この証明書をエクスポートし、他のデバイスにインポートすることにより、ローカル CA が発行したユーザ証明書のローカル CA 証明書検証を、期限が切れた後に行うことができます。

期限切れが近付いていることをユーザに通知するために、次の syslog メッセージが [Latest ASDM Syslog Messages] ペインに表示されます。

```
%ASA-1-717049: Local CA Server certificate is due to expire in days days and a replacement certificate is available for export.
```

(注) この自動ロールオーバーが通知されたら、管理者は、新しいローカル CA 証明書が有効期限の前に必要なすべてのデバイスにインポートされるようにする必要があります。

- ステップ 8** クライアント証明書のライフタイム値を入力します。これは、CA サーバが発行したユーザ証明書の有効期間を日数単位で指定するものです。365 日（1 年）です。推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期間を制限します。
- ステップ 9** [SMTP Server & Email Settings] 領域で次の設定を指定することで、ローカル CA サーバの電子メールアクセスを設定します。
- SMTP メールサーバ名または IP アドレスを入力します。または、省略符号 ([...]) をクリックして [Browse Server Name/IP Address] ダイアログボックスを表示し、ここからサーバ名または IP アドレスを選択します。完了したら、[OK] をクリックします。
 - ローカル CA ユーザに電子メールメッセージを送信する際に使用する From アドレスを「adminname@host.com」という形式で入力します。自動電子メールメッセージは、新規登録ユーザへのワンタイムパスワードの送信や、証明書の更新が必要などの電子メールメッセージの発行に使用されます。
 - ローカル CA サーバからユーザに送信されるすべてのメッセージで使用される件名を入力します。件名を指定しない場合のデフォルトは「Certificate Enrollment Invitation」です。
- ステップ 10** 追加オプションを設定するには、[More Options] ドロップダウン矢印をクリックします。
- ステップ 11** CRL 分散ポイント（ASA 上の CRL の場所）を入力します。デフォルトの場所は `http://hostname.domain/+CSCOCA+/asa_ca.crl` です。
- ステップ 12** 特定のインターフェイスおよびポートで、CRL に HTTP ダウンロードできるようにするには、ドロップダウンリストから `publish-CRL` インターフェイスを選択します。次に、1 ~ 65535 の任意のポート番号を入力します。デフォルトのポート番号は TCP ポート 80 です。
- （注） CRL の名前は変更できません。LOCAL-CA-SERVER.crl という名前が常に使用されます。
- たとえば、`http://10.10.10.100/user8/my_crl_file` という URL を入力します。この場合、指定された IP アドレスを持つインターフェイスのみが動作します。要求を受信すると、ASA によってパス `/user8/my_crl_file` と設定済み URL が照合されます。パスが一致すると、ASA から、保存されている CRL ファイルが返されます。
- ステップ 13** CRL の有効期間である CRL ライフタイムを時間単位で入力します。CA 証明書のデフォルトは 6 時間です。
- ローカル CA では、ユーザ証明書が失効するたびまたは失効解除されるたびに、更新された CRL が再発行されますが、失効状態に変更がない場合、CRL の再発行は、そのライフタイムの中で 1 回しか行われません。[CA Certificates] ペインで [Request CRL] をクリックすると、CRL を即時に更新して再生成できます。
- ステップ 14** データベース ストレージの場所を入力して、ローカル CA コンフィギュレーションとデータファイル用のストレージ領域を指定します。ASA では、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にローカル CA データベースが使用されます。外部ファイルを指定する場合は、外部ファイルへのパス名を入力するか、[Browse] をクリックして [Database Storage Location] ダイアログボックスを表示します。
- ステップ 15** 表示されるフォルダのリストからストレージの場所を選択し、[OK] をクリックします。
- （注） フラッシュ メモリには、3500 人以下のユーザを持つデータベースを保存できます。ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

ステップ 16 発行された証明書のユーザ名に追加されるデフォルトサブジェクト (DN 文字列) を入力します。次に示す DN 属性を指定できます。

- CN (一般名)
- SN (姓名の姓)
- O (組織名)
- L (地名)
- C (国)
- OU (組織ユニット)
- EA (電子メール アドレス)
- ST (州/都道府県)
- T (タイトル)

ステップ 17 登録されたユーザがユーザ証明書を登録および取得するための PKCS12 登録ファイルを取得できる期間を、時間単位で入力します。この登録期間は、ワンタイムパスワード (OTP) の有効期間とは関係ありません。デフォルトは 24 時間です。

(注) ローカル CA の証明書の登録は、クライアントレス SSL VPN 接続でのみサポートされます。このタイプの接続の場合、クライアントと ASA の通信は、標準の HTML を使用して Web ブラウザ経由で行われます。

ステップ 18 登録ユーザに電子メールで送信されたワンタイムパスワードの有効期間を入力します。デフォルトは 72 時間です。次に、[Email OTP] をクリックします。

OTP が新規ユーザに送信されたことを示す [Information] ダイアログボックスが表示されます。

[Replace OTP] をクリックし、自動的に新しい OTP を再発行して、新しいパスワードが記載された電子メール通知を既存のユーザまたは新規ユーザに送信します。

OTP を表示または再生成するには、リストからユーザを選択し、[View/Regenerate OTP] をクリックして [View & Regenerate OTP] ダイアログボックスを表示します。

現在の OTP が表示されます。

[Regenerate OTP] をクリックします。

新しく再生成された OTP が表示されます。

ステップ 19 [OK] をクリックします。

ステップ 20 期限の何日前になったら、ユーザに期限切れ通知の電子メールを送信するかを入力します。デフォルトは、14 日です。

ステップ 21 [Apply] をクリックし、新しいまたは変更された CA 証明書コンフィギュレーションを保存します。

ASA からローカル CA サーバを削除するには、[Delete Certificate Authority Server] をクリックして [Delete Certificate Authority] ダイアログボックスを表示します。[OK] をクリックします。

(注) 削除したローカル CA サーバは、復元および復旧できません。削除した CA サーバコンフィギュレーションを再作成する場合は、CA サーバコンフィギュレーション情報をすべて再入力する必要があります。

CA サーバ管理

ローカル CA ユーザの追加

ローカル CA ユーザを追加するには、次の手順を実行します。

手順

- ステップ 1 新しいユーザをローカル CA データベースに追加するには、[Add] をクリックして、[Add User] ダイアログボックスを表示します。
- ステップ 2 有効なユーザ名を入力します。
- ステップ 3 既存の有効な電子メールアドレスを入力します。
- ステップ 4 サブジェクト (DN 文字列) を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。
- ステップ 5 ドロップダウンリストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。
 - Common Name (CN)
 - Department (OU)
 - Company Name (O)
 - Country (C)
 - State/Province (ST)
 - Location (L)
 - E-mail Address (EA)
- ステップ 6 完了したら、[OK] をクリックします。
- ステップ 7 [Allow enrollment] チェックボックスをオンにしてユーザを登録し、[Add User] をクリックします。

[Manage User Database] ペインに新しいユーザが表示されます。

ローカル CA ユーザの編集

データベース内の既存のローカル CA ユーザに関する情報を変更するには、次の手順を実行します。

手順

- ステップ 1** 特定のユーザを選択し、[Edit] をクリックして [Edit User] ダイアログボックスを表示します。
- ステップ 2** 有効なユーザ名を入力します。
- ステップ 3** 既存の有効な電子メールアドレスを入力します。
- ステップ 4** サブジェクト (DN 文字列) を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。
- ステップ 5** ドロップダウン リストから変更する DN 属性を 1 つ以上選択し、値を入力し、[Add] または [Delete] をクリックします。
- ステップ 6** 完了したら、[OK] をクリックします。

ユーザをデータベースから削除し、そのユーザに発行されたすべての証明書をローカル CA データベースから削除するには、ユーザを選択し、[Delete] をクリックします。

(注) 削除されたユーザは復元できません。削除したユーザ レコードを再作成するには、[Add] をクリックして、そのユーザの情報をすべて再入力します。

- ステップ 7** [Allow enrollment] チェック ボックスをオンにしてユーザを登録し、[Edit User] をクリックします。

(注) ユーザがすでに登録されている場合は、エラー メッセージが表示されます。

[Manage User Database] ペインに更新されたユーザ詳細が表示されます。

コード署名者証明書

コード署名者証明書のインポート

コード署名者証明書をインポートするには、次の手順を実行します。

手順

- ステップ 1** [Code Signer] ペインで、[Import] をクリックし、[Import Certificate] ダイアログボックスを表示します。
- ステップ 2** PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。
- ステップ 3** インポートするファイルの名前を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示し、ファイルを検索します。

- ステップ 4** インポートするファイルを選択し、[Import ID Certificate File] をクリックします。
[Import Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。
- ステップ 5** [Import Certificate] をクリックします。
[Code Signer] ペインにインポートされた証明書が表示されます。
- ステップ 6** [Apply] をクリックし、新しくインポートしたコード署名者証明書コンフィギュレーションを保存します。
-

コード署名者証明書のエクスポート

コード署名者証明書をエクスポートするには、次の手順を実行します。

手順

- ステップ 1** [Code Signer] ペインで、[Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。
- ステップ 2** 証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。
- ステップ 3** 公開キー暗号化標準 (base64 エンコードまたは 16 進数形式を使用できます) を使用するには、[Certificate Format] 領域で [PKCS12 format] オプション ボタンをクリックします。使用しない場合は、[PEM format] オプション ボタンをクリックします。
- ステップ 4** [Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。
- ステップ 5** ファイルを選択し、[Export ID Certificate File] をクリックします。
[Export Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。
- ステップ 6** エクスポート用の PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。
- ステップ 7** 復号化パスフレーズを確認のために再入力します。
- ステップ 8** [Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。
-

証明書の有効期限アラートの設定 (ID 証明書または CA 証明書用)

ASA は、トラストポイントの CA 証明書および ID 証明書について有効期限を 24 時間ごとに 1 回チェックします。証明書の有効期限がまもなく終了する場合、syslog がアラートとして発行されます。

更新リマインダに加え、コンフィギュレーションに期限が切れた証明書が見つかった場合、その証明書を更新するか、または削除することで、コンフィギュレーションを修正するために `syslog` が毎日 1 回生成されます。

たとえば、有効期限アラートが 60 日に開始され、その後 6 日ごとに繰り返すように設定されているとします。ASA が 40 日に再起動されると、アラートはその日に送信され、次のアラートは 36 日目に送信されます。



(注) 有効期限チェックは、トラストプールの証明書では実行されません。ローカル CA トラストポイントは、有効期限チェックの通常のトラストポイントとしても扱われます。

手順

ステップ 1 `[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificate/CA Certificate]` を参照します。

ステップ 2 `[Enable Certificate Expiration Alert]` チェックボックスをオンにします。

ステップ 3 目的の日数を入力します。

- `[Repeat the alert for]` : 最初のアラートが発行される有効期限までの日数 (1 ~ 90) を設定します。
- `[Repeat the alert for]` : 証明書が更新されない場合のアラート頻度 (1 ~ 14 日) を設定します。デフォルトでは、最初のアラートは有効期限の 60 日前に送信され、その後は証明書が更新または削除されるまで毎週 1 回送信されます。また、アラートは有効期限日に送信され、その後は毎日 1 回送信され、アラートの設定に関係なく、有効期限の直前の週はアラートが毎日送信されます。

デジタル証明書のモニタリング

デジタル証明書ステータスのモニタリングについては、次のコマンドを参照してください。

- `[Monitoring] > [Properties] > [CRL]`

このペインには、CRL の詳細が表示されます。

- `[Tools] > [Command Line Interface]`

このペインでは、さまざまな非インタラクティブコマンドを発行し、結果を表示することができます。

証明書管理の履歴

表 25: 証明書管理の履歴

機能名	プラットフォーム リリース	説明
証明書管理	7.0(1)	<p>デジタル証明書（CA 証明書、ID 証明書、およびコード署名者証明書など）は、認証用のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。</p> <p>次の画面が導入されました。</p> <p>[Configuration] > [Remote Access VPN] > [Certificate Management Configuration] > [Site-to-Site VPN] > [Certificate Management]。</p> <p>次の画面が導入または変更されました。</p> <p>[Configuration] > [Firewall] > [Advanced] > [Certificate Management] > [CA Certificates Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]。</p>
証明書管理	7.2(1)	
証明書管理	8.0(2)	
SCEP プロキシ	8.4(1)	サードパーティ CA からのデバイス証明書を安全に構成できる機能を導入しました。

機能名	プラットフォーム リリース	説明
ローカル CA サーバ	9.12(1)	<p>ASA の構成済み FQDN を使用する代わりに設定可能な登録用 URL の FQDN を作成するため、新しい CLI オプションが導入されました。この新しいオプションは、<code>ccrypto ca server</code> の <code>smpt</code> モードに追加されます。</p> <p>ローカル CA サーバは廃止され、以降のリリースで削除されます。ASA がローカル CA サーバとして設定されている場合、デジタル証明書の発行、証明書失効リスト (CRL) の発行、および発行された証明書の安全な取り消しを行うために有効になります。この機能は古くなったため、<code>crypto ca server</code> コマンドは廃止されています。</p>



第 23 章

トランスペアレントファイアウォールモードの ARP インспекションおよび MAC アドレス テーブル

この章では、MACアドレステーブルのカスタマイズ方法、およびブリッジグループのARPインспекションの設定方法について説明します。

- [ARP インспекションと MAC アドレス テーブルについて \(639 ページ\)](#)
- [デフォルト設定 \(641 ページ\)](#)
- [ARP インспекションと MAC アドレス テーブルのガイドライン \(641 ページ\)](#)
- [ARP インспекションとその他の ARP パラメータの設定 \(641 ページ\)](#)
- [トランスペアレントモードのブリッジグループにおける MAC アドレス テーブルのカスタマイズ \(644 ページ\)](#)
- [ARP インспекションと MAC アドレス テーブルの履歴 \(645 ページ\)](#)

ARP インспекションと MAC アドレス テーブルについて

ブリッジグループのインターフェイスでは、ARP インспекションは「中間者」攻撃を防止します。他の ARP の設定をカスタマイズすることも可能です。ブリッジグループの MAC アドレス テーブルのカスタマイズができます。これには、MAC スプーフィングに対する防御としてのスタティック ARP エントリの追加が含まれます。

ブリッジグループのトラフィックの ARP インспекション

デフォルトでは、ブリッジグループのメンバーの間ですべての ARP パケットが許可されます。ARP パケットのフローを制御するには、ARP インспекションをイネーブルにします。

ARP インспекションによって、悪意のあるユーザが他のホストやルータになります (ARP スプーフィングと呼ばれる) のを防止できます。ARP スプーフィングが許可されていると、

「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インスペクションをイネーブルにすると、ASA は、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASA はパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするように ASA を設定できます。



(注) 専用の管理インターフェイスは、このパラメータが **flood** に設定されている場合でもパケットをフラッディングしません。

MAC アドレス テーブル

ブリッジ グループを使用する場合、ASA は、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレス テーブルを作成します。デバイスがブリッジ グループ経由でパケットを送信すると、ASA が MAC アドレスをアドレス テーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、ASA は、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。ブリッジ グループ メンバー間のトラフィックには ASA セキュリティ ポリシーが適用されるため、パケットの宛先 MAC アドレスがテーブルに含まれていなくても、通常のブリッジのように、すべてのインターフェイスに元のパケットを ASA がフラッディングすることはありません。代わりに、直接接続されたデバイスまたはリモートデバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：ASA は宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。
- リモートデバイスへのパケット：ASA は宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

デフォルト設定

- ARP インспекションをイネーブルにした場合、デフォルト設定では、一致しないパケットはフラッドします。
- ダイナミック MAC アドレス テーブルのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、ASAは対応するエントリを MAC アドレス テーブルに追加します。

ARP インспекションと MAC アドレス テーブルのガイドライン

- ARP インспекションは、ブリッジグループでのみサポートされます。
- MAC アドレス テーブル構成は、ブリッジグループでのみサポートされます。
- ブリッジグループは、トランスペアレント ファイアウォール モードでのみサポートされます。

ARP インспекションとその他の ARP パラメータの設定

トランスペアレント ファイアウォール モードのブリッジグループでは、ARP インспекションをイネーブルにすることができます。その他の ARP パラメータは、ブリッジグループとルーテッドモードのインターフェイスの両方で設定できます。

手順

- ステップ 1** [スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ \(642 ページ\)](#) に従って、スタティック ARP エントリを追加します。ARP インспекションは ARP パケットを ARP テーブルのスタティック ARP エントリと比較するので、この機能にはスタティック ARP エントリが必要です。その他の ARP パラメータも設定できます。
- ステップ 2** (トランスペアレントモードのみ) [ARP インспекションの有効化 \(643 ページ\)](#) に従って ARP インспекションを有効にします。

スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ

ブリッジグループのデフォルトでは、ブリッジグループメンバーインターフェイス間の ARP パケットはすべて許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。ARP インスペクションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。

ルーテッドインターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッドインターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレントモードの場合、管理トラフィックなどの ASA との間のトラフィックに、ASA は ARP テーブルのダイナミック ARP エントリのみを使用します。

ARP タイムアウトなどの ARP 動作を設定することもできます。

手順

ステップ 1 [Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Static Table] の順に選択します。

ステップ 2 [Add] をクリックして、スタティック ARP エントリを追加します。

[Add ARP Static Configuration] ダイアログボックスが表示されます。

- a) [Interface] ドロップダウンリストから、ホストネットワークに接続されているインターフェイスを選択します。
- b) [IP Address] フィールドにホストの IP アドレスを入力します。
- c) [MAC Address] フィールドにホストの MAC アドレスを入力します（00e0.1e4e.3d8b など）。
- d) このアドレスでプロキシ ARP を実行するには、[Proxy ARP] チェックボックスをオンにします。

ASA は、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。

- e) [OK] をクリックします。

ステップ3 ダイナミック ARP エントリの ARP タイムアウトを設定するには、[ARP Timeout] フィールドに値を入力します。

このフィールドでは、ASA が ARP テーブルを再構築するまでの時間を、60 ～ 4294967 秒の範囲で設定します。デフォルトは14400秒です。ARP テーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。

ステップ4 非接続サブネットを使用するには、[Allow non-connected subnets] チェックボックスをオンにします。ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。ARP キャッシュをイネーブルにして、間接接続されたサブネットを含めることもできます。セキュリティリスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否 (DoS) 攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。

次の機能を使用する場合は、この機能を使用する必要がある可能性があります。

- セカンダリ サブネット。
- トラフィック転送の隣接ルートのプロキシ ARP。

ステップ5 [Apply] をクリックします。

ARP インспекションの有効化

この項では、ブリッジグループ用に ARP インспекションをイネーブルにする方法について説明します。

手順

ステップ1 [Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Inspection] ペインの順に選択します。

ステップ2 ARP インспекションをイネーブルにするインターフェイス行を選択し、[Edit] をクリックします。

[Edit ARP Inspection] ダイアログボックスが表示されます。

ステップ3 ARP インспекションをイネーブルにするには、[Enable ARP Inspection] チェックボックスをオンにします。

ステップ4 (任意) 一致しない ARP パケットをフラディングするには、[Flood ARP Packets] チェックボックスをオンにします。

デフォルトでは、スタティック ARP エントリのどの要素にも一致しないパケットが、送信元のインターフェイスを除くすべてのインターフェイスからフラッドされます。MAC アドレス、

IP アドレス、またはインターフェイス間で不一致がある場合、ASA はパケットをドロップします。

このチェックボックスをオフにすると、一致しないパケットはすべてドロップされます。これにより、スタティック エントリにある ARP だけが ASA を通過するように制限されます。

(注) Management 0/0 または 0/1 インターフェイスあるいはサブインターフェイスがある場合、これらのインターフェイスは、このパラメータがフラッドに設定されていてもパケットをフラッドしません。

ステップ 5 [OK]、続いて [Apply] をクリックします。

トランスペアレントモードのブリッジグループにおける MAC アドレス テーブルのカスタマイズ

ここでは、ブリッジグループの MAC アドレス テーブルをカスタマイズする方法について説明します。

ブリッジグループのスタティック MAC アドレスの追加

通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。スタティック MAC アドレスは、MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、ASA はトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに ([スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ \(642 ページ\)](#) を参照)、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

MAC アドレス テーブルにスタティック MAC アドレスを追加するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Setup] > [Bridging] > [MAC Address Table] ペインを選択します。

ステップ 2 (オプション) MAC アドレス エントリがタイムアウトするまで MAC アドレス テーブル内に留まる時間を設定するには、[Dynamic Entry Timeout] フィールドに値を入力します。

この値は、5 ~ 720 分 (12 時間) の範囲で指定します。5 分がデフォルトです。

ステップ 3 [Add] をクリックします。

[Add MAC Address Entry] ダイアログボックスが表示されます。

- ステップ 4 [Interface Name] ドロップダウンリストから、MAC アドレスに関連付けられている送信元インターフェイスを選択します。
- ステップ 5 [MAC Address] フィールドに MAC アドレスを入力します。
- ステップ 6 [OK]、続いて [Apply] をクリックします。

MAC アドレス ラーニングのディセーブル化

デフォルトで、各インターフェイスは着信トラフィックの MAC アドレスを自動的に学習し、ASA は対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできますが、この場合、MAC アドレスをテーブルにスタティックに追加しないと、トラフィックが ASA を通過できなくなります。

MAC アドレス ラーニングをディセーブルにするには、次の手順を実行します。

手順

- ステップ 1 [Configuration] > [Device Setup] > [Bridging] > [MAC Learning] の順に選択します。
- ステップ 2 MAC ラーニングをディセーブルにするには、インターフェイス行を選択して、[Disable] をクリックします。
- ステップ 3 MAC ラーニングを再度イネーブルにするには、[Enable] をクリックします。
- ステップ 4 [Apply] をクリックします。

ARP インスペクションと MAC アドレス テーブルの履歴

機能名	プラットフォーム リリース	機能情報
ARP インスペクション	7.0(1)	<p>ARP インスペクションは、すべての ARP パケットの MAC アドレス、IP アドレス、および送信元インターフェイスを、ARP テーブルのスタティック エントリと比較します。この機能は、トランスペアレントファイアウォールモード。</p> <p>arp、arp-inspection、および show arp-inspection コマンドが導入されました。</p>

機能名	プラットフォーム リリース	機能情報
MAC アドレス テーブル	7.0(1)	<p>トランスペアレント モード。</p> <p>mac-address-table static、mac-address-table aging-time、mac-learn disable、および show mac-address-table コマンドが導入されました。</p>
間接接続されたサブネットの ARP キャッシュの追加	8.4(5)/9.1(2)	<p>ASA ARP キャッシュには、直接接続されたサブネットからのエン트리だけがデフォルトで含まれています。また、ARP キャッシュに間接接続されたサブネットを含めることができるようになりました。セキュリティリスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否 (DoS) 攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。</p> <p>次の機能を使用する場合は、この機能を使用する必要がある可能性があります。</p> <ul style="list-style-type: none"> • セカンデリ サブネット。 • トラフィック転送の隣接ルートのプロキシ ARP。 <p>次の画面が変更されました。 [Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Static Table]。</p>



第 **V** 部

IP ルーティング

- ルーティングの概要 (649 ページ)
- スタティック ルートとデフォルト ルート (663 ページ)
- Policy Based Routing : ポリシー ベース ルーティング (673 ページ)
- ルート マップ (681 ページ)
- BGP (693 ページ)
- OSPF (723 ページ)
- EIGRP (775 ページ)
- マルチキャスト ルーティング (799 ページ)



第 24 章

ルーティングの概要

この章では、ASA 内でのルーティングの動作について説明します。

- [パス判別 \(649 ページ\)](#)
- [サポートされるルート タイプ \(650 ページ\)](#)
- [ルーティングにサポートされているインターネットプロトコル \(652 ページ\)](#)
- [ルーティング テーブル \(652 ページ\)](#)
- [等コスト マルチパス \(ECMP\) ルーティング \(660 ページ\)](#)
- [プロキシ ARP 要求のディセーブル化 \(660 ページ\)](#)
- [ルーティング テーブルの表示 \(661 ページ\)](#)

パス判別

ルーティングプロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティングアルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティングアルゴリズムは、ルート情報が格納されるルーティングテーブルを初期化して保持します。ルート情報は、使用するルーティング アルゴリズムによって異なります。

ルーティングアルゴリズムにより、さまざまな情報がルーティングテーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティングテーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決めます。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティングテーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの 1 つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデートを他のすべてのルータから分析することで、ルータはネットワーク トポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう 1 つの例であるリンクステートアドバ

タイズメントは、他のルータに送信元のリンクのステータスを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワーク トポロジの全体像の構築に使用できます。



(注) 非対称ルーティングがサポートされるのは、マルチ コンテキスト モードでのアクティブ/アクティブ フェールオーバーに対してのみです。

サポートされるルート タイプ

ルータが使用できるルート タイプには、さまざまなものがあります。ASAでは、次のルート タイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステータスと距離ベクトル型の比較

スタティックとダイナミックの比較

スタティックルーティングアルゴリズムは、実はネットワーク管理者が確立したテーブルマップです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティングアルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティングソフトウェアはルートを再計算し、新しいルーティングアップデートメッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できません。たとえば、ラストリゾートルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティングプロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパスアルゴリズムとは異なり、これらのマルチパスアルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパスアルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

フラットと階層型の比較

ルーティングアルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラットルーティングシステムでは、ルータは他のすべてのルータのピアになります。階層型ルーティングシステムでは、一部のルータが実質的なルーティングバックボーンを形成します。バックボーン以外のルータからのパケットはバックボーンルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーンルータから、1つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティングシステムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティングバックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織に類似しているため、そのトラフィックパターンもサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティングアルゴリズムを簡素化できます。また、使用しているルーティングアルゴリズムに応じて、ルーティングアップデートトラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステートアルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティングテーブルの一部だけを送信します。リンクステートアルゴリズムでは、各ルータはネットワークの全体像をそのルーティングテーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Fordアルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティングテーブル全体または一部を送信するように要求されます。つまり、リンクステートアルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステートアルゴリズムは OSPF ルーティングプロトコルとともに使用されます。

ルーティングにサポートされているインターネットプロトコル

ASA は、ルーティングに対してさまざまなインターネットプロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

- Open Shortest Path First (OSPF)

OSPF は、インターネットプロトコル (IP) ネットワーク向けに、インターネット技術特別調査委員会 (IETF) の Interior Gateway Protocol (IGP) 作業部会によって開発されたルーティングプロトコルです。OSPF は、リンクステートアルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステートデータベースが置かれています。

- ルーティング情報プロトコル (RIP)

RIP は、ホップカウントをメトリックとして使用するディスタンスベクトルプロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol (IGP) です。つまり、1 つの自律システム内部でルーティングを実行します。

- Border Gateway Protocol (BGP)

BGP は自律システム間のルーティングプロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネットサービスプロバイダー (ISP) 間で使用されるプロトコルです。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム (AS) 間で BGP を使用する場合、このプロトコルは外部 BGP (EBGP) と呼ばれます。サービスプロバイダーが BGP を使用して AS 内でルートを交換する場合、このプロトコルは内部 BGP (IBGP) と呼ばれます。

ルーティング テーブル

ここでは、ルーティング テーブルの仕組みについて説明します。

ルーティング テーブルへの入力方法

ASAのルーティング テーブルには、スタティックに定義されたルート、直接接続されているルート、およびダイナミック ルーティング プロトコルで検出されたルートを入力できます。ASAは、ルーティング テーブルに含まれるスタティック ルートと接続されているルートに加えて、複数のルーティングプロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への2つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2つのルートのネットワークプレフィックス長（ネットワークマスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティング テーブルに入力されます。入力された後は、パケット転送ロジックが2つのうちどちらを使用するかを決定します。

たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

- RIP : 192.168.32.0/24
- OSPF : 192.168.32.0/19

OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方のルートがルーティング テーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- ASAが、1つのルーティングプロトコル（RIP など）から同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティング テーブルに入力されます。

メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックスの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティング テーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コスト パスに対してロード バランシングが行われます。

- ASA が、ある宛先へのルーティングプロトコルが複数あることを検知すると、ルートのアドミニストレーティブ ディスタンスが比較され、アドミニストレーティブ ディスタンスが最も小さいルートがルーティング テーブルに入力されます。

ルートのアドミニストレーティブ ディスタンス

ルーティングプロトコルによって検出されるルート、またはルーティングプロトコルに再配布されるルートのアドミニストレーティブ ディスタンスは変更できます。2つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブ ディスタンスが同じ場合、デフォルトのアドミニストレーティブ ディスタンスが小さい方のルートがルーティング テーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブ ディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に複数の異なるルートがある場合に、ASAが最適なパスの選択に使用するルートパラメータです。ルーティングプロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティングプロトコルによって生成された、同じ宛先への2つのルートについて常に最適パスを判定できるわけではありません。

各ルーティングプロトコルには、アドミニストレーティブディスタンス値を使用して優先順位が付けられています。次の表に、ASAがサポートするルーティングプロトコルのデフォルトのアドミニストレーティブディスタンス値を示します。

表 26: サポートされるルーティングプロトコルのデフォルトのアドミニストレーティブディスタンス

ルートの送信元	デフォルトのアドミニストレーティブディスタンス
接続されているインターフェイス	0
スタティックルート	1
EIGRP サマリールート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
内部およびローカル BGP	200
不明 (Unknown)	255

アドミニストレーティブディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、ASAが OSPF ルーティングプロセス（デフォルトのアドミニストレーティブディスタンスが 110）と RIP ルーティングプロセス（デフォルトのアドミニストレーティブディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPF ルーティングプロセスの方が優先度が高いため、ASAは OSPF ルートを選択します。この場合、ルータは OSPF バージョンのルートを選択してルーティングテーブルに追加します。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、ASAは、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブディスタンスはローカルの設定値です。たとえば、OSPF を通じて取得したルートのアドミニストレーティブディスタンスを変更する場合、その変更は、コマンドが入力された ASA のルーティングテーブルにだけ影響します。アドミニストレーティブディスタンスがルーティングアップデートでアドバタイズされることはありません。

アドミニストレーティブ ディスタンスは、ルーティング プロセスに影響を与えません。ルーティング プロセスは、ルーティング プロセスで検出されたか、またはルーティング プロセスに再配布されたルートだけをアドバタイズします。たとえば、RIP ルーティング プロセスは、のルーティング テーブルで OSPF ルーティング プロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

ダイナミック ルートとフローティングスタティック ルートのバックアップ

ルートを最初にルーティング テーブルにインストールしようとしたとき、他のルートがインストールされてしまい、インストールできなかった場合に、そのルートはバックアップルートとして登録されます。ルーティング テーブルにインストールされたルートに障害が発生すると、ルーティング テーブル メンテナンス プロセスが、登録されたバックアップルートを持つ各ルーティング プロトコル プロセスを呼び出し、ルーティング テーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブ ディスタンスに基づいて優先順位の高いルートが選択されます。

このプロセスのため、ダイナミック ルーティング プロトコルによって検出されたルートに障害が発生したときにルーティング テーブルにインストールされるフローティングスタティック ルートを作成できます。フローティングスタティック ルートとは、単に、ASA で動作しているダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスが設定されているスタティック ルートです。ダイナミック ルーティング プロセスで検出された対応するルートに障害が発生すると、このスタティック ルートがルーティング テーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエン트리と一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティング テーブル内の1つのエン트리と一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティング テーブル内の複数のエン트리と一致する場合、パケットはネットワークプレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 のゲートウェイ 10.1.1.2
- 192.168.32.0/19 のゲートウェイ 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティング テーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます (24 ビットと 19 ビット)。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。



(注) ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

ダイナミック ルーティングと フェールオーバー

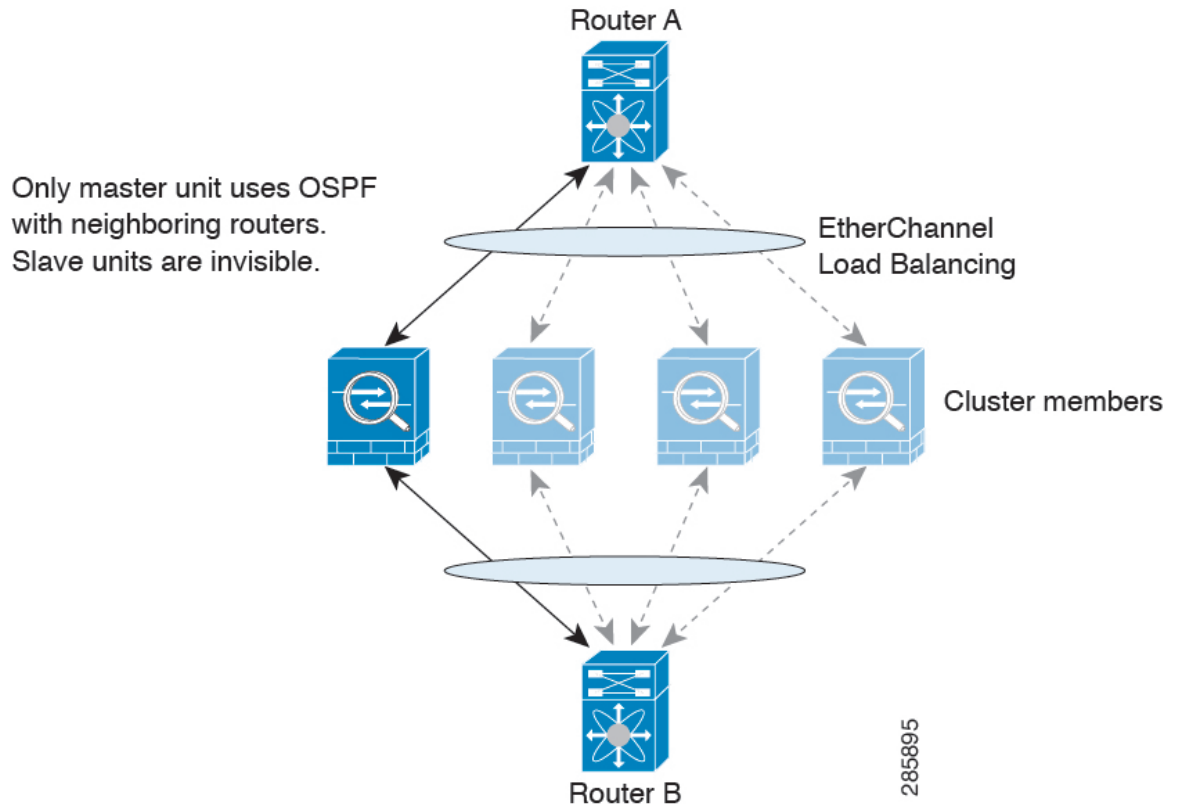
アクティブなユニットでルーティング テーブルが変更されると、スタンバイ ユニットでダイナミック ルートが同期されます。これは、アクティブ ユニットのすべての追加、削除、または変更がただちにスタンバイ ユニットに伝播されることを意味します。スタンバイ ユニットがアクティブ/スタンバイの待受中 フェールオーバー ペアでアクティブになると、ルートはフェールオーバー バルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブ ユニットと同じルーティング テーブルがすでに作成されています。

ダイナミック ルーティングおよびクラスタリング

ここでは、クラスタリングでダイナミック ルーティングを使用する方法について説明します。

スパンド EtherChannel モードでのダイナミック ルーティング

スパンド EtherChannel モード：ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニートを介して学習され、スレーブに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 59: スパンド *EtherChannel* モードでのダイナミック ルーティング

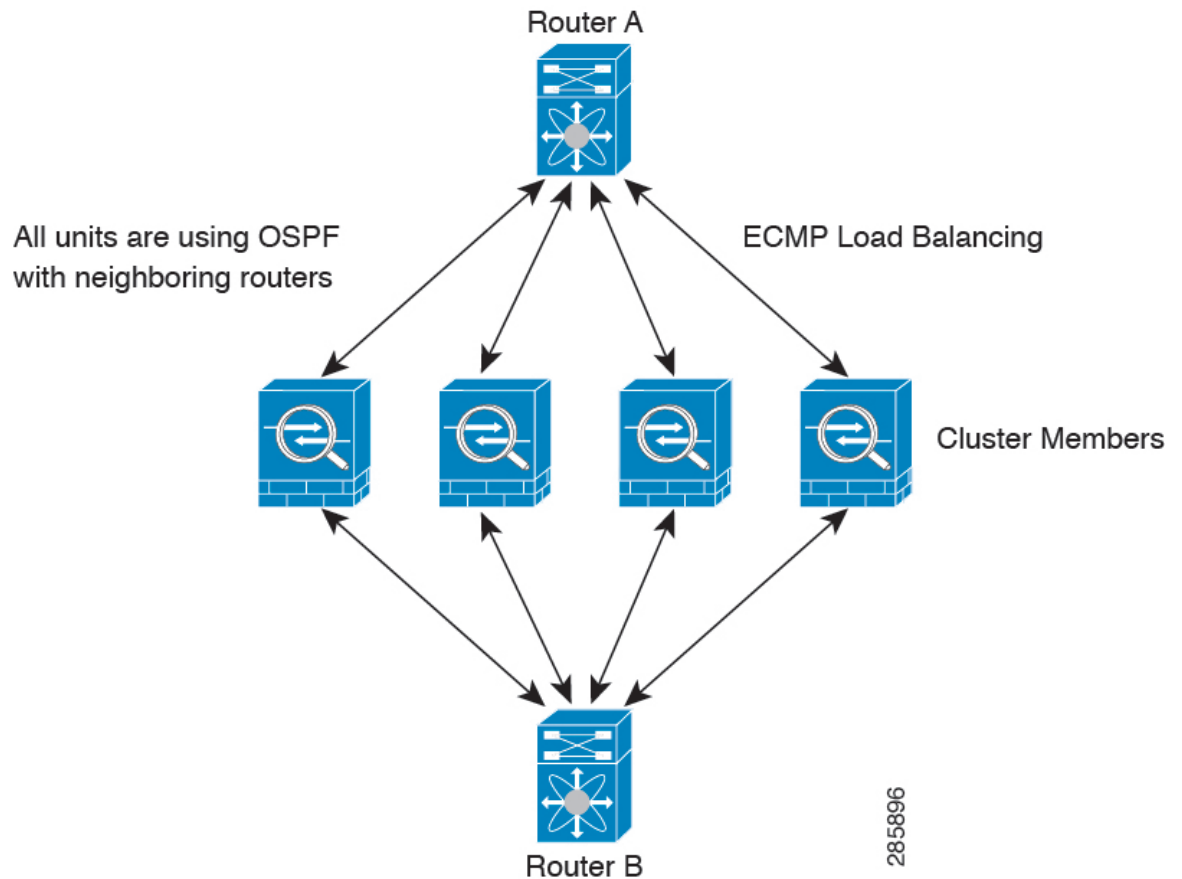
スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスターユニットからスレーブユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイス モードでは、各ユニットがスタンドアロンルータとしてルーティング プロトコルを実行します。ルートの学習は、各ユニットが個別に行います。

図 60: 個別インターフェイスモードでのダイナミックルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つの ASA を通過します。ECMP を使用して、4 パス間でトラフィックのロードバランシングを行います。各 ASA は、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ユニットが別のルータ ID を使用できるように、ルータ ID のクラスタプールを設定する必要があります。

EIGRP は、個別のインターフェイスモードのクラスタピアとのネイバー関係を形成しません。



- (注) 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィックゾーンにこれらすべての ASA インターフェイスをまとめます。[トラフィックゾーンの設定 \(561 ページ\)](#) を参照してください。

マルチ コンテキスト モードのダイナミック ルーティング

マルチ コンテキスト モードでは、各コンテキストで個別のルーティング テーブルおよびルーティング プロトコル データベースが維持されます。これにより、各コンテキストの OSPFv2 および EIGRP を個別に設定することができます。EIGRP をあるコンテキストで設定し、OSPFv2 を同じまたは異なるコンテキストで設定できます。混合コンテキストモードでは、ルーテッドモードのコンテキストの任意のダイナミック ルーティング プロトコルをイネーブルにできます。RIP および OSPFv3 は、マルチ コンテキスト モードではサポートされていません。

次の表に、EIGRP、OSPFv2、OSPFv2 および EIGRP プロセスへのルートの配布に使用されるルート マップ、およびマルチ コンテキスト モードで使用されている場合にエリアを出入りするルーティング アップデートをフィルタリングするために OSPFv2 で使用されるプレフィックス リストの属性を示します。

EIGRP	OSPFv2	ルートマップとプレフィックスのリスト
コンテキストごとに 1 つのインスタンスがサポートされます。	コンテキストごとに 2 つのインスタンスがサポートされます。	該当なし
システム コンテキストでディセーブルになっています。		該当なし
2 つのコンテキストが同じまたは異なる自律システム番号を使用できます。	2 つのコンテキストが同じまたは異なるエリア ID を使用できます。	該当なし
2 つのコンテキストの共有インターフェイスでは、複数の EIGRP のインスタンスを実行できます。	2 つのコンテキストの共有インターフェイスでは、複数の OSPF のインスタンスを実行できます。	該当なし
共有インターフェイス間の EIGRP インスタンスの相互作用がサポートされます。	共有インターフェイス間の OSPFv2 インスタンスの相互作用がサポートされます。	該当なし
シングルモードで使用可能なすべての CLI はマルチ コンテキスト モードでも使用できます。		
各 CLI は使用されているコンテキストでだけ機能します。		

ルートのリソース管理

routes というリソース クラスは、コンテキストに存在できるルーティング テーブル エントリの最大数を指定します。これは、別のコンテキストの使用可能なルーティング テーブル エントリに影響を与える 1 つのコンテキストの問題を解決し、コンテキストあたりの最大ルート エントリのより詳細な制御を提供します。

明確なシステム制限がないため、このリソース制限には絶対値のみを指定できます。割合制限は使用できません。また、コンテキストあたりの上限および下限がないため、デフォルトクラスは変更されません。コンテキストのスタティックまたはダイナミック ルーティング プロトコル (接続、スタティック、OSPF、EIGRP、および RIP) のいずれかに新しいルートを追加し、そのコンテキストのリソース制限を超えた場合、ルートの追加は失敗し、syslog メッセージが生成されます。

等コスト マルチパス (ECMP) ルーティング

ASA は、等コスト マルチパス (ECMP) ルーティングをサポートしています。

インターフェイスごとに最大 8 の等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロード バランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレス、着信トラフィック、プロトコル、送信元ポートおよび宛先ポートをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMP は複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.1
```

ゾーンがある場合は、各ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイス間に複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同様に、ダイナミックルーティングプロトコルは、自動的に等コストルートを設定できます。ASAでは、より堅牢なロード バランシング メカニズムを使用してインターフェイス間でトラフィックをロード バランスします。

ルートが紛失した場合、デバイスはフローをシームレスに別のルートに移動させます。

プロキシ ARP 要求のディセーブル化

あるホストから同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信する場合、そのホストは送信先のデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者

を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが ARP 要求に対してその IP アドレスを所有しているかどうかに関係なく自分の MAC アドレスで応答するときに使用されます。NAT を設定し、ASA インターフェイスと同じネットワーク上のマッピングアドレスを指定する場合、ASA でプロキシ ARP が使用されます。トラフィックがホストに到達できる唯一の方法は、ASA でプロキシ ARP が使用されている場合、MAC アドレスが宛先マッピングアドレスに割り当てられていると主張することです。

まれに、NAT アドレスに対してプロキシ ARP をディセーブルにすることが必要になります。

既存のネットワークと重なる VPN クライアントアドレスプールがある場合、ASA はデフォルトで、すべてのインターフェイス上でプロキシ ARP 要求を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターントラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP 要求をそれらが不要なインターフェイスでディセーブルにする必要があります。

手順

ステップ 1 **[Configuration] > [Device Setup] > [Routing] > [Proxy ARP/Neighbor Discovery]** の順に選択します。

[Interface] フィールドにインターフェイス名が一覧表示されます。[Enabled] フィールドには、NAT グローバルアドレスに対してプロキシ ARP/ネイバー探索がイネーブルか (Yes) ディセーブルか (No) が表示されます。

ステップ 2 選択したインターフェイスに対してプロキシ ARP/ネイバー探索をイネーブルにするには、[Enable] をクリックします。デフォルトでは、プロキシ ARP/ネイバー探索はすべてのインターフェイスに対してイネーブルです。

ステップ 3 選択したインターフェイスに対してプロキシ ARP/ネイバー探索をディセーブルにするには、[Disable] をクリックします。

ステップ 4 [Apply] をクリックして設定を実行コンフィギュレーションに保存します。

ルーティング テーブルの表示

ルーティング テーブルにある ASDM のすべてのルートを表示するには、**[Monitoring] > [Routing] > [Routes]** の順に選択します。各行は 1 つのルートを表します。



第 25 章

スタティック ルートとデフォルト ルート

この章では、Cisco ASA でスタティック ルートとデフォルト ルートを設定する方法について説明します。

- [スタティック ルートとデフォルト ルートについて \(663 ページ\)](#)
- [スタティック ルートとデフォルト ルートのガイドライン \(666 ページ\)](#)
- [デフォルト ルートおよびスタティック ルートの設定 \(666 ページ\)](#)
- [スタティック ルートまたはデフォルト ルートのモニタリング \(670 ページ\)](#)
- [スタティック ルートまたはデフォルト ルートの例 \(670 ページ\)](#)
- [スタティック ルートおよびデフォルト ルートの履歴 \(671 ページ\)](#)

スタティック ルートとデフォルト ルートについて

トラフィックを接続されていないホストやネットワークにルーティングするには、スタティック ルーティングまたはダイナミックルーティングを使用して、ホストやネットワークへのルートを実行する必要があります。通常は、少なくとも1つのスタティック ルート、つまり、他の方法でデフォルトのネットワーク ゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルト ルート（通常、ネクストホップ ルータ）を設定する必要があります。

デフォルト ルート

最も単純なオプションは、すべてのトラフィックをアップストリーム ルータに送信するようにデフォルト スタティック ルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、ASA が送信するゲートウェイの IP アドレスを特定するルートです。デフォルト スタティック ルートとは、つまり宛先の IP アドレスとして 0.0.0.0/0 (IPv4) または ::/0 (IPv6) が指定されたスタティック ルートのことです。

デフォルト ルートを常に定義する必要があります。

スタティック ルート

次の場合は、スタティック ルートを使用します。

- ネットワークがサポート対象外のルータ ディスカバリ プロトコルを使用している。
- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- 場合によっては、デフォルトルートだけでは不十分である。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティックルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルトルートは、ASA に直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。

不要なトラフィックを「ブラックホール化」するための null0 インターフェイスへのルート

アクセスルールを使用すると、ヘッダーに含まれている情報に基づいてパケットをフィルタ処理することができます。null0 インターフェイスへのスタティック ルートは、アクセスルールを補完するソリューションです。null0 ルートを使用して、不要なトラフィックや望ましくないトラフィックを「ブラックホール」に転送できるため、トラフィックがドロップされます。

スタティック null0 ルートには、望ましいパフォーマンス プロファイルがあります。また、スタティック null0 ルートを使用して、ルーティング ループ回避することもできます。BGP では、リモート トリガ型ブラック ホールルーティングのためにスタティック null0 ルートを活用できます。

ルートのプライオリティ

- 特定の宛先が特定されたルートはデフォルト ルートより優先されます。
- 宛先が同じルートが複数存在する場合（スタティックまたはダイナミック）、ルートのアドミニストレーティブディスタンスによってプライオリティが決まります。スタティック ルートは 1 に設定されるため、通常、それらが最もプライオリティの高いルートです。
- 宛先かつアドミニストレーティブディスタンスが同じスタティック ルートが複数存在する場合は、[等コスト マルチパス \(ECMP\) ルーティング \(660 ページ\)](#) を参照してください。
- [トンネル化 (Tunneled)] オプションを使用してトンネルから出力されるトラフィックの場合、このルートが他の設定済みルートまたは学習されたデフォルトルートをすべてオーバーライドします。

トランスパアレント ファイアウォール モード ルート

ブリッジグループメンバーインターフェイスを通じて直接には接続されていないネットワークに向かう ASA で発信されるトラフィックの場合、ASA がどのブリッジグループメンバーインターフェイスからトラフィックを送信するかを認識するように、デフォルトルートまたはスタティック ルートを設定する必要があります。ASA で発信されるトラフィックは、syslog サーバまたは SNMP サーバへの通信も含むことがあります。1つのデフォルトルートで到達できないサーバがある場合、スタティックルートを設定する必要があります。トランスパアレントモードの場合、ゲートウェイインターフェイスに BVI を指定できません。メンバーインターフェイスのみが使用できます。詳細については、「[MAC アドレスとルート ルックアップ \(211 ページ\)](#)」を参照してください。

スタティック ルート トラッキング

スタティックルートの問題の1つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクストホップゲートウェイが使用できなくなった場合でも、ルーティングテーブルに保持されています。スタティックルートは、ASA 上の関連付けられたインターフェイスがダウンした場合に限りルーティングテーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップルートをインストールするための方式が用意されています。たとえば、ISPゲートウェイへのデフォルトルートを定義し、かつ、プライマリ ISPが使用できなくなった場合に備えて、セカンダリ ISP へのバックアップデフォルトルートを定義できます。

ASA では、ASA が ICMP エコー要求を使用してモニタする宛先ネットワーク上でモニタリング対象スタティック ルートを関連付けることでスタティック ルート トラッキングを実装します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると思われ、関連付けられたルートはルーティングテーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップルートの使用されます。

モニタリング対象の選択時には、その対象が ICMP エコー要求に応答できることを確認してください。対象には任意のネットワークオブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス (デュアル ISP サポート用)
- ネクストホップゲートウェイアドレス (ゲートウェイの使用可能状況に懸念がある場合)
- ASA が通信を行う必要のある対象ネットワーク上のサーバ (syslog サーバなど)
- 宛先ネットワーク上の永続的なネットワーク オブジェクト



(注) 夜間にシャットダウンする PC は適しません。

スタティックルートトラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルトルートに対して設定することができます。設定済みのルートトラッキングでは、複数のインターフェイス上の PPPoE クライアントだけをイネーブルにすることができます。

スタティックルートとデフォルトルートのガイドライン

ファイアウォールモードとブリッジグループ

- トランスペアレントモードでは、スタティックルートをブリッジグループメンバーインターフェイスをゲートウェイとして使用する必要があります。BVI を指定することはできません。
- スタティックルートトラッキングは、ブリッジグループメンバーインターフェイス

IPv6

- IPv6 では、スタティックルートトラッキングはサポートされません。

クラスタ

クラスタリングでは、スタティックルートモニタリングはプライマリユニットでのみサポートされます。

デフォルトルートおよびスタティックルートの設定

少なくとも1つのデフォルトルートを設定する必要があります。また、スタティックルートの設定が必要になる場合があります。このセクションでは、デフォルトルートの設定、スタティックルートの設定、スタティックルートの追跡を行います。

デフォルトルートの設定

デフォルトルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティックルートです。この手順に従って手動で設定するか、DHCP サーバや他のルーティングプロトコルから取得するかに関わらず、デフォルトルートは必ず設定する必要があります。

始める前に

[Tunneled] オプションについては、次のガイドラインを参照してください。

- トンネルルートの出力インターフェイスで、ユニキャスト RPF を有効にしないでください。この設定を行うと、セッションでエラーが発生します。

- トンネルルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。この設定を行うと、セッションでエラーが発生します。
- これらのインスペクション エンジン はトンネルルートを無視するため、トンネルルートで VoIP インスペクション エンジン (CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY)、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンを使用しないでください。
- tunneled オプションで複数のデフォルトルートを定義することはできません。
- トンネルトラフィックの ECMP はサポートされません。

手順

ステップ 1 [Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択し、[Add] をクリックします。

ステップ 2 [IP Address Type]、[IPv4]、または [IPv6] を選択します。

ステップ 3 特定のトラフィックの送信を行う **インターフェイス** を選択します。

トランスペアレント モードの場合は、ブリッジグループのメンバー インターフェイスの名前を指定します。

ステップ 4 ネットワークの場合は、そのタイプに応じて **any4** または **any6** を入力します。

ステップ 5 トラフィックを送信する **ゲートウェイ IP** を入力します。

ステップ 6 **メトリック** を設定して、ルートのアドミニストレーティブ ディスタンスを設定します。

デフォルトは **1** です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティックルートのデフォルトのアドミニストレーティブ ディスタンスは **1** で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは **110** です。スタティック ルートとダイナミックルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

ステップ 7 (オプション) [Options] 領域で、以下を設定します。

- [Tunneled] : VPN トラフィックに非 VPN トラフィックとは別のデフォルトルートを使用する必要がある場合は、VPN トラフィック用の別個のデフォルトルートを定義できます。その場合、たとえば VPN 接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。tunneled オプションを使用してデフォルトルートを作成すると、ASA に着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。
- [Tracked] : (IPv4 のみ) ルートのトラッキングについては、[スタティック ルート トラッキングの設定 \(669 ページ\)](#) を参照してください。

ステップ 8 [OK] をクリックします。

スタティック ルートの設定

スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。

手順

ステップ 1 [Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択し、[Add] をクリックします。

ステップ 2 [IP Address Type]、[IPv4]、または [IPv6] を選択します。

ステップ 3 特定のトラフィックの送信を行う **インターフェイス** を選択します。

不要なトラフィックを「ブラック ホール化」するには、**Null0** インターフェイスを選択します。トランスペアレントモードの場合は、ブリッジグループのメンバー インターフェイスの名前を指定します。

ステップ 4 **ネットワーク** の場合は、トラフィックをルーティングする宛先ネットワークを入力します。

ステップ 5 トラフィックを送信する **ゲートウェイ IP** を入力します。

ステップ 6 **メトリック** を設定して、ルートのアドミニストレーティブ ディスタンスを設定します。

デフォルトは **1** です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートと比較するのに使用されるパラメータです。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは **1** で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは **110** です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

ステップ 7 (オプション) [Options] 領域で、以下を設定します。

- [Tunneled] : VPN トラフィックに非 VPN トラフィックとは別のデフォルト ルートを使用する必要がある場合は、VPN トラフィック用の別個のデフォルト ルートを定義できます。その場合、たとえば VPN 接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。tunneled オプションを使用してデフォルト ルートを作成すると、ASA に着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。
- [Tracked] : (IPv4 のみ) ルートのトラッキングについては、[スタティック ルート トラッキングの設定 \(669 ページ\)](#) を参照してください。

ステップ 8 [OK] をクリックします。

スタティック ルート トラッキングの設定

スタティック ルート トラッキングを設定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Setup] > [Routing] > [Static Routes] の順に選択し、[スタティック ルートの設定 \(668 ページ\)](#) に従ってスタティック ルートを追加または編集します。

ステップ 2 [Options] 領域で [Tracked] オプション ボタンをクリックします。

ステップ 3 [Track ID] フィールドに、ルート トラッキング プロセスの固有識別子を入力します。

ステップ 4 [Track IP Address/DNS Name] フィールドに、追跡対象の IP アドレスまたはホスト名を入力します。これは通常、このルートのネクスト ホップ ゲートウェイの IP アドレスになりますが、そのインターフェイスから利用できる任意のネットワーク オブジェクトとすることもできます。

ステップ 5 [SLA ID] フィールドに、SLA モニタリング プロセスの固有識別子を入力します。

ステップ 6 (任意) [Monitoring Options] をクリックします。

[Route Monitoring Options] ダイアログボックスが表示されます。ここから、次のトラッキング オブジェクトのモニタリング プロパティを変更します。

- [Frequency] : 追跡対象の存在を ASA がテストする頻度を秒数で設定します。有効な値の範囲は、1 ~ 604800 秒です。デフォルト値は 60 秒です。
- [Threshold] : しきい値を超えたイベントを示す時間をミリ秒数で設定します。この値に、タイムアウト値より大きい値は指定できません。
- [Timeout] : ルート監視操作が要求パケットからの応答を待つ時間をミリ秒数で設定します。有効な値の範囲は、0 ~ 604800000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
- [Data Size] : エコー要求パケットで使用するデータ ペイロードのサイズを設定します。デフォルト値は 28 です。有効値の範囲は 0 ~ 16384 です。
(注) この設定では、ペイロードのサイズだけが指定されます。パケット全体のサイズは指定されません。
- [ToS] : エコー要求の IP ヘッダーにあるサービス バイトのタイプの値を設定します。有効な値は、0 ~ 255 です。デフォルト値は 0 です
- [Number of Packets] : 各テストに送信されるエコー要求の数を設定します。有効値の範囲は 1 ~ 100 です。デフォルト値は 1 です。

[OK] をクリックします。

ステップ 7 [OK] をクリックしてルートを保存してから、[Apply] をクリックします。

追跡するルートを適用するとすぐに、モニタリング プロセスが開始されます。

ステップ 8 追跡対象外のバックアップ ルートを作成します。

バックアップ ルートは、追跡されたルートと同じ宛先へのスタティック ルートですが、異なるインターフェイスまたはゲートウェイを経由します。このルートは、追跡されたルートより長いアドミニストレーティブ ディスタンス（メトリック）に割り当てる必要があります。

スタティック ルートまたはデフォルト ルートのモニタリング

- [Monitoring] > [Routing] > [Routes]

[Routes] ペインでは、それぞれの行が 1 つのルートを表しています。IPv4 接続、IPv6 接続、またはその両方でフィルタリングできます。ルーティング情報には、プロトコル、ルートタイプ、宛先 IP アドレス、ネットマスクまたはプレフィックスの長さ、ゲートウェイ IP アドレス、ルートに接続するときを経由するインターフェイス、およびアドミニストレーティブ ディスタンスが含まれています。

スタティック ルートまたはデフォルト ルートの例

次の例は、スタティック ルートの作成方法を示します。スタティック ルートは、宛先が 10.1.1.0/24 のトラフィックすべてを内部インターフェイスに接続されているルータ（10.1.2.45）に送信します。また、dmz インターフェイスで 3 つの異なるゲートウェイにトラフィックを誘導する 3 つの等コスト スタティック ルートを定義し、トンネルトラフィックのデフォルト ルートと通常のトラフィックのデフォルト ルートを追加します。

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

スタティック ルートおよびデフォルト ルートの履歴

表 27:スタティック ルートおよびデフォルト ルートの機能履歴

機能名	プラットフォーム リリース	機能情報
スタティック ルート トラッキング	7.2(1)	<p>スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリルートがダウンした場合のバックアップルートをインストールするための方式が用意されています。</p> <p>次の画面が導入または変更されました。</p> <p>[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route] [Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route] > [Route Monitoring Options]</p>
トラフィックを「ブラックホール化」するためのスタティック null0 ルート	9.2(1)	<p>トラフィックを null0 インターフェイスへ送信すると、指定したネットワーク宛の packets はドロップします。この機能は、BGP の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route]</p>



第 26 章

Policy Based Routing : ポリシーベースルーティング

この章では、ポリシーベースルーティング (PBR) をサポートするように Cisco ASA を設定する方法について説明します。この項では、ポリシーベースルーティング、PBR のガイドライン PBR の設定について説明します。

- [ポリシーベースルーティングについて \(673 ページ\)](#)
- [ポリシーベースルーティングのガイドライン \(676 ページ\)](#)
- [ポリシーベースルーティングの設定 \(676 ページ\)](#)
- [ポリシーベースルーティングの履歴 \(679 ページ\)](#)

ポリシーベースルーティングについて

従来のルーティングは宛先ベースであり、パケットは宛先 IP アドレスに基づいてルーティングされます。ただし、宛先ベースのルーティングシステムでは特定トラフィックのルーティングを変更することが困難です。ポリシーベースルーティング (PBR) では、宛先ネットワークではなく条件に基づいてルーティングを定義できます。PBR では、送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、プロトコル、またはこれらの組み合わせに基づいてトラフィックをルーティングできます。

ポリシーベースルーティング：

- 区別したトラフィックに Quality of Service (QoS) を提供できます。
- 低帯域幅、低コストの永続パスと、高帯域幅、高コストのスイッチドパスに、インタラクティブトラフィックとバッチトラフィックを分散できます。
- インターネットサービスプロバイダーやその他の組織が、さまざまなユーザセットから発信されるトラフィックを、適切に定義されたインターネット接続を経由してルーティングできます。

ポリシーベースルーティングには、ネットワークエッジでトラフィックを分類およびマークし、ネットワーク全体で PBR を使用してマークしたトラフィックを特定のパスに沿ってルーティングすることで、QoS を実装する機能があります。これにより、宛先が同じ場合でも、異

なる送信元から送信されるパケットを別のネットワークにルーティングすることができます。これは、複数のプライベート ネットワークを相互接続する場合に役立ちます。

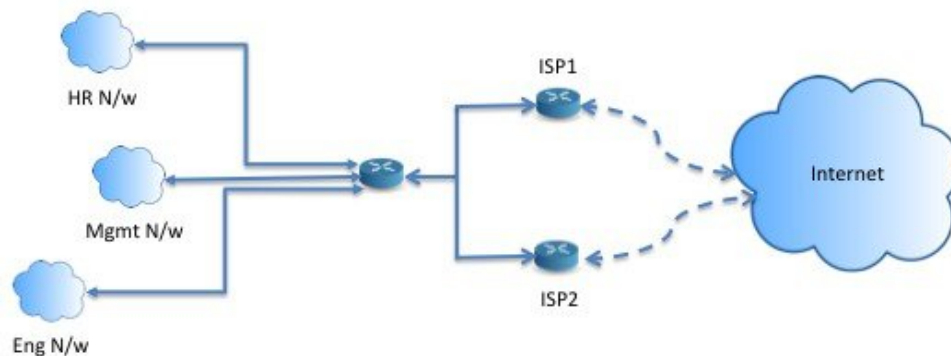
ポリシーベース ルーティングを使用する理由

ロケーション間に2つのリンクが導入されている企業を例に説明します。1つのリンクは高帯域幅、低遅延、高コストのリンクであり、もう1つのリンクは低帯域幅、高遅延、低コストのリンクです。従来のルーティングプロトコルを使用する場合、高帯域幅リンクで、リンクの（EIGRP または OSPF を使用した）帯域幅/遅延の特性により実現するメトリックの節約に基づいて、ほぼすべてのトラフィックが送信されます。PBR では、優先度の高いトラフィックを高帯域幅/低遅延リンク経由でルーティングし、その他のすべてのトラフィックを低帯域幅/高遅延リンクで送信します。

ポリシーベース ルーティングの用途のいくつかを以下に示します。

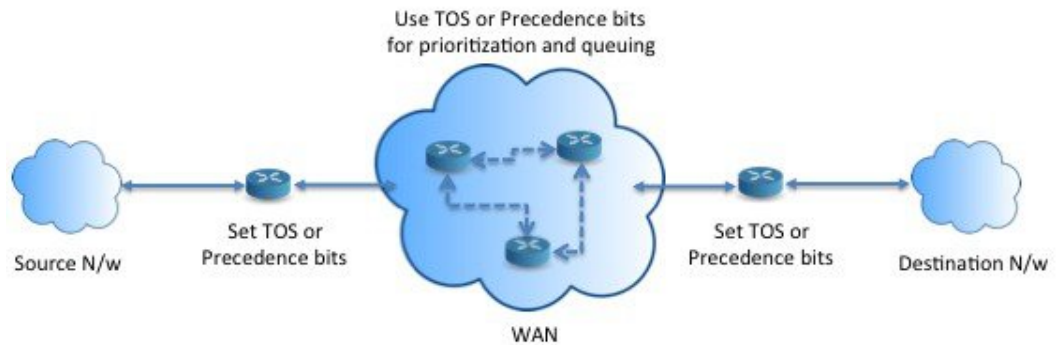
同等アクセスおよび送信元依存ルーティング

このトポロジでは、HR ネットワークと管理ネットワークからのトラフィックはISP1 を経由するように設定し、エンジニアリング ネットワークからのトラフィックは ISP2 を経由するように設定できます。したがって、ここに示すように、ネットワーク管理者は、ポリシーベース ルーティングを使用して同等アクセスおよび送信元依存ルーティングを実現できます。



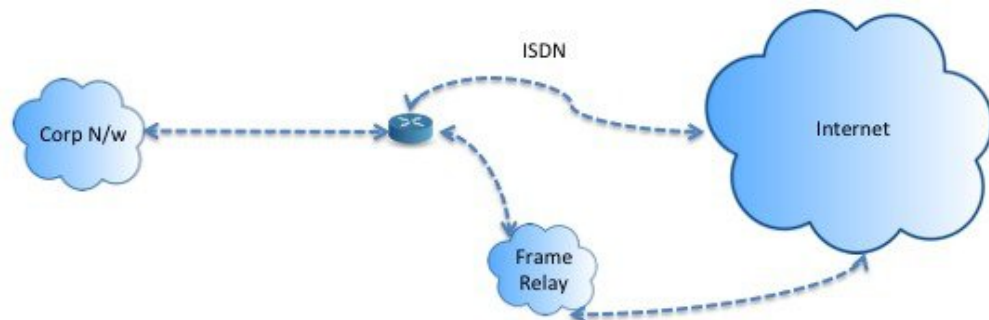
QoS

ネットワーク管理者は、ポリシーベースルーティングでパケットにタグを付けることにより、ネットワークトラフィックをネットワーク境界でさまざまなサービスクラスのために分類し、プライオリティ、カスタム、または重み付け均等化のキューイングを使用してそれらのサービスクラスをネットワークのコアに実装できます（下の図を参照）。この設定では、バックボーンネットワークのコアの各 WAN インターフェイスでトラフィックを明示的に分類する必要がなくなるため、ネットワーク パフォーマンスが向上します。



コスト節約

組織は、特定のアクティビティに関連付けられている一括トラフィックを転送して、帯域幅が高い高コストリンクの使用を短時間にし、さらにここに示すようにトポロジを定義することで帯域幅が低い低コストリンク上の基本的な接続を継続できます。



ロードシェアリング

ECMP ロードバランシングによって提供されるダイナミックなロードシェアリング機能に加え、ネットワーク管理者は、トラフィックの特性に基づいて複数のパス間にトラフィックを分散するためのポリシーを実装できます。

たとえば、同等アクセスおよび送信元依存ルーティングのシナリオに示すトポロジでは、管理者は、ISP1 を経由する HR netto からのトラフィックと ISP2 を経由するエンジニアリングネットワークからのトラフィックをロードシェアするようにポリシーベースルーティングを設定できます。

PBR の実装

ASA は、ACL を使用してトラフィックを照合してから、トラフィックのルーティングアクションを実行します。具体的には、照合のために ACL を指定するルートマップを設定し、次にそのトラフィックに対して1つ以上のアクションを指定します。最後に、すべての着信トラフィックに PBR を適用するインターフェイスにルートマップを関連付けます。

ポリシーベース ルーティングのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フロー別のルーティング

ASA はフロー別にルーティングを実行するため、ポリシー ルーティングは最初のパケットに適用され、その結果決定したルーティングが、そのパケットに対して作成されたフローに格納されます。同一接続に属する後続のパケットはすべてこのフローと照合され、適切にルーティングされます。

出力ルート ルックアップに適用されない PBR ポリシー

ポリシーベースルーティングは入力専用機能です。つまり、この機能は新しい着信接続の最初のパケットだけに適用され、この時点で接続のフォワードレグの出力インターフェイスが選択されます。着信パケットが既存の接続に属している場合、または NAT が適用されない場合には、PBR がトリガーされないことに注意してください。

クラスタ

- クラスタリングがサポートされています。
- クラスタのシナリオでは、スタティック ルートまたはダイナミック ルートがない場合、`ip-verify-reverse` パスを有効にした非対称トラフィックはドロップされる可能性があります。したがって、`ip-verify-reverse` パスを無効にすることが推奨されます。

その他のガイドライン

ルート マップ関連の既存のすべての設定の制限事項が引き続き適用されます。

ポリシーベース ルーティングの設定

ルート マップは、1 つ以上のルート マップ文で構成されます。文ごとに、シーケンス番号と `permit` 句または `deny` 句が付加されます。各ルート マップ文には、`match` コマンドと `set` コマンドが含まれています。`match` コマンドは、パケットデータに適用される一致基準を示します。`set` コマンドは、パケットに対して実行されるアクションを示します。

- 複数のネクストホップまたはインターフェイスを `set` アクションとして設定すると、使用できる有効なオプションが見つかるまですべてのオプションが順に評価されます。設定された複数のオプション間のロード バランシングは実行されません。
- `verify-availability` オプションは、マルチ コンテキスト モードではサポートされません。

手順

- ステップ 1** ASDM で、ポリシーベース ルーティングを実行するトラフィックを特定する 1 つ以上の標準または拡張 ACL を設定します。[Configuration] > [Firewall] > [Advanced] > [ACL Manager] を表示します。
- ステップ 2** [Configuration] > [Device Setup] > [Routing] > [Route Maps] の順に選択し、[Add] をクリックします。
- [Add Route Map] ダイアログボックスが表示されます。
- ステップ 3** ルート マップ名とシーケンス番号を入力します。オプションでルート マップ文を追加する場合は、このルート マップ名と同じ名前を使用します。シーケンス番号は、ASA がルートマップを評価する順序です。
- ステップ 4** [Deny] または [Permit] をクリックします。
- ACL には、固有の permit および deny 文も含まれます。ルート マップと ACL が permit/permit で一致する場合、ポリシーベース ルーティング処理が続行されます。permit/deny で一致する場合、このルート マップでの処理が終了し、別のルート マップがチェックされます。それでも結果が permit/deny であれば、通常のルーティングテーブルが使用されます。deny/deny で一致する場合、ポリシーベース ルーティング処理が続行されます。
- ステップ 5** [Match Clause] タブをクリックし、作成した ACL を確認します。
- [IPv4] セクションで、ドロップダウンメニューから [Access List] を選択し、ダイアログボックスで 1 つ以上の標準または拡張 ACL を選択します。
- 標準 ACL を使用する場合、照合は宛先アドレスに対してのみ行われます。拡張 ACL を使用する場合、送信元、宛先、またはその両方に対して照合を行えます。
- IPv6 ACL はサポートされません。
- ステップ 6** [Policy Based Routing] タブをクリックし、トラフィック フローのポリシーを定義します。
- 一致するトラフィック フローに対して実行する set アクションを、次のうちから 1 つ以上選択します。
- [Set PBR next hop address] : IPv4 では、複数のネクストホップ IP アドレスを設定できます。その場合、ルーティングできる有効なネクスト ホップ IP アドレスが見つかるまで、それらのアドレスが指定された順で評価されます。設定済みのネクストホップは、直接接続する必要があります。そうでなければ、set アクションが適用されません。
 - [Set default next-hop IP address] : IPv4 では、一致するトラフィックに対する通常のルート ルックアップが失敗した場合、ASA はここで指定されたネクストホップ IP アドレスを使用してトラフィックを転送します。
 - [Recursively find and set next-hop IP address] : ネクストホップ アドレスとデフォルトのネクストホップアドレスのいずれでも、直接接続されたサブネット上でネクストホップが検出されることが要件となります。このオプションを指定した場合、ネクストホップアドレスが直接接続されている必要はありません。代わりにネクストホップアドレスで再帰ルック

アップが実行され、一致するトラフィックは、ルータで使用されているルーティングパスに従って、そのルート エントリで使用されているネクストホップに転送されます。

- **[Configure Next Hop Verifiability]** : ルート マップの次の IPv4 ホップが使用できるかどうかを確認します。ネクスト ホップの到達可能性を確認するには、SLA モニタ追跡オブジェクトを設定できます。**[Add]** をクリックして、ネクストホップ IP アドレス エントリを追加し、次の情報を指定します。
 - **[Sequence Number]** : エントリはシーケンス番号を使用して順に評価されます。
 - **[IP Address]** : ネクスト ホップ IP アドレスを入力します。
 - **[Tracking Object ID]** : 有効な ID を入力します。
- **[Set interfaces]**: このオプションを使用して、一致するトラフィックを転送するために使用するインターフェイスを設定します。複数のインターフェイスを設定できます。その場合、有効なインターフェイスが見つかるまで、それらのインターフェイスが指定された順で評価されます。**null0** を指定すると、ルート マップと一致するすべてのトラフィックがドロップされます。指定されたインターフェイス（静的または動的のいずれか）経由でルーティングできる宛先のルートが存在している必要があります。
- **[Set null0 interface as the default interface]** : 通常のルート ルックアップが失敗すると、ASA はトラフィックを null0 に転送し、トラフィックがドロップされます。
- **[Set do-not-fragment bit to either 1 or 0]** : 適切なオプション ボタンを選択します。
- **[Set differential service code point (DSCP) value in QoS bits]** : [IPv4] ドロップダウン リストから値を選択します。

ステップ 7 **[OK]** をクリックし、さらに **[Apply]** をクリックします。

ステップ 8 既存の PBR ルート マップを削除するには、**[Route Maps]** リストで削除するマップを選択し、**[Delete]** をクリックします。

ポリシーベース ルーティングの履歴

表 28: ルート マップの履歴

機能名	プラットフォーム リリース	機能情報
ポリシーベース ルーティング	9.4(1)	<p>ポリシーベースルーティング (PBR) は、ACL を使用して指定された QoS でトラフィックが特定のパスを経由するために使用するメカニズムです。ACL では、パケットのレイヤ3 およびレイヤ4 ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックに QoS を提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチドパスの間にインタラクティブトラフィックとバッチトラフィックを分散でき、インターネット サービス プロバイダーとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザから送信されるトラフィックをルーティングできます。</p> <p>次の画面が更新されました。 [Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Policy Based Routing]、 [Configuration] > [Device Setup] > [Routing] > [Interface Settings] > [Interfaces]</p>



第 27 章

ルート マップ

この章では、Cisco ASA にルート マップを設定およびカスタマイズする方法について説明します。

- [ルート マップについて \(681 ページ\)](#)
- [ルート マップのガイドライン \(683 ページ\)](#)
- [ルート マップの定義 \(683 ページ\)](#)
- [ルート マップのカスタマイズ \(686 ページ\)](#)
- [ルート マップの例 \(689 ページ\)](#)
- [ルート マップの履歴 \(690 ページ\)](#)

ルート マップについて

ルート マップは、ルート を OSPF、RIP、EIGRP、または BGP ルーティング プロセスに再配布するとき に使用 します。また、デフォルト ルート を OSPF ルーティング プロセスに生成するときにも使用 します。ルート マップは、指定されたルーティング プロトコルのどのルート を対象ルーティング プロセスに再配布できるのかを定義 します。

ルート マップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。ACL またはルート マップの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクションが実行されると中断 します。
- これらは一般的なメカニズムです。基準一致と一致解釈は、適用方法とこれらを使用する機能によって決定 します。異なる機能に適用される同じルート マップの解釈が異なることがあります。

次のように、ルート マップと ACL には違いがいくつかあります。

- ルート マップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認 できます。たとえば、ルート マップはルートのタイプが内部であるかどうかを確認 できます。

- 設計規則により、各 ACL は暗黙の deny 文で終了します。一致試行の間にルートマップの終わりに達した場合は、そのルートマップの特定のアプリケーションによって結果が異なります。再配布に適用されるルートマップの動作は ACL と同じです。ルートがルートマップのどの句とも一致しない場合は、ルートマップの最後に deny 文が含まれている場合と同様に、ルートの再配布が拒否されます。

permit 句と deny 句

ルートマップでは permit 句と deny 句を使用できます。deny 句は、ルートの照合の再配布を拒否します。ルートマップでは、一致基準として ACL を使用できます。ACL には permit 句と deny 句もあるため、パケットが ACL と一致した場合に次のルールが適用されます。

- ACL permit + route map permit : ルートは再配布されます。
- ACL permit + route map deny : ルートは再配布されません。
- ACL deny + route map permit or deny : ルートマップの句は一致せず、次のルートマップ句が評価されます。

match 句と set 句の値

各ルートマップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択します。
- set 値は、ターゲットプロトコルに再配布される情報を変更します。

再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、set コマンドによって設定された値で変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句でルート进行评估します。ルートマップのスキューン、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の match エントリが句に含まれる場合に、特定のルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用される）。
- match エントリが 1 つのエントリの複数のオブジェクトを指している場合は、そのいずれかが一致していなければなりません（論理 OR アルゴリズムが適用される）。
- match エントリがない場合は、すべてのルートが句に一致します。
- ルートマップの permit 句に set エントリが存在しない場合、ルートは、その現在の属性を変更されずに再配布されます。



- (注) ルートマップの deny 句では set エントリを設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。

match エントリまたは set エントリがないルートマップ句はアクションを実行します。空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の deny 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルトアクションです。

ルートマップのガイドライン

ファイアウォールモード

ルーテッドファイアウォールモードでだけサポートされています。トランスペアレントファイアウォールモードはサポートされません。

その他のガイドライン

ルートマップは、ユーザ、ユーザグループ、または完全修飾ドメイン名のオブジェクトを含む ACL をサポートしていません。

ルートマップの定義

ルートマップを定義する必要があるのは、指定したルーティングプロトコルからのどのルートを対象ルーティングプロセスに再配布できるのかを指定するときです。ASDMでルートマップを定義するには、ルートマップ名、シーケンス番号、または再配布を追加、編集、または削除します。

手順

ステップ 1 ASDM で、[Configuration] > [Device Setup] > [Routing] > [Route Maps] の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Route Map] または [Edit Route Map] ダイアログボックスが表示されます。

ステップ 3 ルートマップ名とシーケンス番号を入力します。ルートマップ名とは、特定のルートに割り当てる名前です。シーケンス番号とは、ルートマップエントリを ASA に追加または削除するときの順序です。

- (注) 既存のルートマップ名を編集する場合、ルートマップ名とシーケンス番号のフィールドにはすでに値が入力されています。

ステップ 4 一致するルートの再配布を拒否するには、[Deny] をクリックします。ルートマップの Deny 句で ACL を使用すると、その ACL で許可されるルートは再配布されなくなります。一致するルートの再配布を許可するには、[Permit] をクリックします。ルートマップの Permit 句で ACL を使用すると、その ACL で許可されるルートが再配布されます。

さらに、ルートマップの Permit または Deny 句で ACL を使用する場合に、その ACL でルートが拒否されたときは、そのルートマップ句に一致するものは見つからなかったことになり、次のルートマップ句が評価されます。

ステップ 5 [Match Clause] タブをクリックして、この句を適用する必要があるルートを選択し、次のパラメータを設定します。

- [Match first hop interface of route] チェックボックスをオンにして、ルートのファーストホップインターフェイスの照合をイネーブルにするか、オフにしてディセーブルにし、指定されたネクストホップインターフェイスを任意のルートと照合します。2つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。
 - [Interface] フィールドにインターフェイス名を入力するか、または省略記号をクリックして [Browse Interface] ダイアログボックスを表示します。
 - 1つ以上のインターフェイスを選択し、[Interface] をクリックして [OK] をクリックします。
- [IPv4] および [IPv6] セクションで、次の1つ以上を行います。
 - [Match Address] チェックボックスをオンにして、ルートの一致アドレスをイネーブルにするか、オフにしてディセーブルにし、パケットを照合します。
 - [Match Next Hop] チェックボックスをオンにするとルートのネクストホップアドレスの照合がイネーブルになり、オフにするとディセーブルになります。
 - [Match Route Source] チェックボックスをオンにするとルートのアドバタイジングソースアドレスの照合がイネーブルになり、オフにするとディセーブルになります。
 - ドロップダウンリストで [Access List] から [Prefix List] を選択して、IP アドレスを照合します。
 - 以前の選択内容に従って、省略記号をクリックして [Browse Access List] または [Browse Prefix List] ダイアログボックスを表示します。
 - 必要な ACL またはプレフィックスリストを選択します。
- [Match metric of route] チェックボックスをオンにするとルートのメトリックの照合がイネーブルになり、オフにするとディセーブルになります。
 - [Metric Value] フィールドに、メトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ~ 4294967295 の範囲で指定します。
- [Match Route Type] チェックボックスをオンにするとルートタイプの照合がイネーブルになり、オフにするとディセーブルになります。有効なルートタイプは、External1、

External2、Internal、Local、NSSA-External1、NSSA-External2 です。イネーブルの場合、複数のルート タイプをリストから選択することができます。

ステップ 6 [Set Clause] タブをクリックして、ターゲットプロトコルに再配布される次の情報を変更します。

- [Set Metric Clause] チェックボックスを使用して、宛先ルーティングプロトコルに対するメトリック値をイネーブルにするかディセーブルにするかを指定し、値を [Value] フィールドに入力します。
- [Set Metric Type] チェックボックスをオンにすると宛先ルーティングプロトコルのメトリックタイプがイネーブルになり、オフにするとディセーブルになります。ドロップダウンリストからメトリックタイプを選択します。

ステップ 7 [BGP Match Clause] タブをクリックして、この句を適用する必要があるルートを選択し、次のパラメータを設定します。

- [Match AS path access lists] チェックボックスをオンにすると、BGP 自律システムパスアクセスリストと指定されたパスアクセスリストの照合がイネーブルになります。複数のパスアクセスリストを指定した場合、ルートはいずれかのパスアクセスリストと一致します。
- [Match Community] チェックボックスをオンにすると、BGP コミュニティと指定されたコミュニティの照合がイネーブルになります。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。少なくとも1つの Match コミュニティと一致しないルートは、アウトバウンドルートマップにアドバタイズされません。
 - [Match the specified community exactly] チェックボックスをオンにすると、BGP コミュニティと指定されたコミュニティの厳密な照合がイネーブルになります。
- BGP ポリシーを評価および処理するためのルートマップを設定するには、[Match Policy list] チェックボックスをオンにします。複数のポリシーリストを指定した場合、ルートはいずれかのポリシーリストを処理できます。

ステップ 8 [BGP Set Clause] タブをクリックして、BGP プロトコルに再配布される次の情報を変更します。

- BGP ルートの自律システムパスを変更するには、[Set AS Path] チェックボックスをオンにします。
 - BGP ルートの前に任意の自律システムパス文字列を付加するには、[Prepend AS path] チェックボックスをオンにします。通常、ローカルな AS 番号が複数回追加され、自律システムパス長が増します。複数の AS パス番号を指定した場合、ルートはいずれかの AS 番号を付加できます。
 - 最後の AS 番号の AS パスを先頭に追加するには、[Prepend Last AS to the AS Path] チェックボックスをオンにします。AS 番号の値を 1 ~ 10 の範囲で入力します。
 - ルートのタグを自律システムパスに変換するには、[Convert route tag into AS Path] チェックボックスをオンにします。

- BGP コミュニティ属性を設定するには、[Set Community] チェックボックスをオンにします。
 - コミュニティ番号を入力するには、[Specify Community] をクリックします（必要な場合）。有効な値は、1 ~ 4294967200、internet、no-advertise、no-export です。
 - 既存のコミュニティにコミュニティを追加するには、[Add to the existing communities] チェックボックスをオンにします。
 - ルートマップをパスするプレフィックスからコミュニティ属性を除去するには、[None] をクリックします。
- 自律システムパスのプリファレンス値を指定するには、[Set local preference] チェックボックスをオンにします。
- ルーティングテーブルに対して BGP ウェイトを指定するには、[Set weight] チェックボックスをオンにします。0 ~ 65535 の範囲で値を入力します。
- BGP 送信元コードを指定するには、[Set origin] チェックボックスをオンにします。有効な値は [Local IGP] および [Incomplete] です。
- ルートマップの match 句を満たすパケットの出力アドレスを指定するには、[Set next hop] チェックボックスをオンにします。
 - パケットが出力されるネクストホップの IP アドレスを入力するには、[Specify IP address] をクリックします。隣接ルータである必要はありません。複数の IP アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。
 - BGP ピアアドレスにするネクストホップを設定するには、[Use peer address] をクリックします。

ステップ 9 [OK] をクリックします。

ルートマップのカスタマイズ

ここでは、ルートマップをカスタマイズする方法について説明します。

特定の宛先アドレスに一致するルートの定義

手順

ステップ 1 ASDM で、[Configuration] > [Device Setup] > [Routing] > [Route Maps] の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Route Map] ダイアログボックスが表示されます。このダイアログボックスでは、ルートマップ名、シーケンス番号、その再配布アクセス（許可または拒否）の割り当てまたは選択を行うことができます。ルートマップのエントリは順番に読み取られます。この順序は、シーケンス番号で指定できます。シーケンス番号が指定されていない場合は、ASA にエントリを追加した順序が使用されます。

ステップ 3 [Match Clause] タブをクリックして、この句を適用する必要があるルートを選択し、次のパラメータを設定します。

- [Match first hop interface of route] チェックボックスをオンにして、ルートのファーストホップインターフェイスの照合をイネーブルにするか、オフにしてディセーブルにし、指定されたネクストホップインターフェイスを任意のルートと照合します。2つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。
 - [Interface] フィールドにインターフェイス名を入力するか、または省略記号をクリックして [Browse Interface] ダイアログボックスを表示します。
 - インターフェイス タイプ ([inside] または [outside]) を選択し、[Selected Interface] をクリックして、[OK] をクリックします。
 - [Match IP Address] チェックボックスをオンにして、ルートの一致アドレスをイネーブルにするか、オフにしてディセーブルにし、パケットを照合します。
 - [Match Next Hop] チェックボックスをオンにするとルートのネクストホップアドレスの照合がイネーブルになり、オフにするとディセーブルになります。
 - [Match Route Source] チェックボックスをオンにするとルートのアドバタイジングソースアドレスの照合がイネーブルになり、オフにするとディセーブルになります。
 - ドロップダウンリストで [Access List] から [Prefix List] を選択して、IP アドレスを照合します。
 - 以前の選択内容に従って、省略記号をクリックして [Browse Access List] または [Browse Prefix List] ダイアログボックスを表示します。
 - 必要な ACL またはプレフィックスリストを選択します。
- [Match metric of route] チェックボックスをオンにするとルートのメトリックの照合がイネーブルになり、オフにするとディセーブルになります。
 - [Metric Value] フィールドに、メトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ~ 4294967295 の範囲で指定します。
- [Match Route Type] チェックボックスをオンにするとルートタイプの照合がイネーブルになり、オフにするとディセーブルになります。有効なルートタイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。イネーブルの場合、複数のルートタイプをリストから選択することができます。

プレフィックス ルールの設定



(注) プレフィックス ルールを設定する前に、プレフィックス リストを設定する必要があります。

プレフィックス ルールを設定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Setup] > [Routing] > [IPv4 Prefix Rules] または [IPv6 Prefix Rules] を選択します。

ステップ 2 [Add] をクリックし、[Add Prefix Rule] を選択します。

[Add Prefix Rule] ダイアログボックスが表示されます。このダイアログボックスでは、シーケンス番号を追加し、IP のバージョン (IPv4 または IPv6) を選択し、ネットワークのプレフィックス、再配布アドレス (許可または禁止)、プレフィックスの最小長と最大長を指定できます。

ステップ 3 オプションの [Sequence Number} を入力するか、デフォルト値を受け入れます。

ステップ 4 IP アドレス/マスク長の形式で [Prefix] 番号を指定します。

ステップ 5 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 6 オプションの [Minimum length] および [Maximum length] を入力します。

ステップ 7 完了したら、[OK] をクリックします。

新規追加または修正したプレフィックス ルールがリストに表示されます。

ステップ 8 [Apply] をクリックして変更内容を保存します。

プレフィックス リストの設定

ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。

プレフィックス リストを追加するには、次の手順を実行します。

手順

- ステップ 1 **[Configuration] > [Device Setup] > [Routing] > [IPv4 Prefix Rules]** または **[IPv6 Prefix Rules]** を選択します。
- ステップ 2 **[Add] > [Add Prefix List]** をクリックします。
[Add Prefix List] ダイアログボックスが表示されます。
- ステップ 3 プレフィックス名と説明を入力して **[OK]** をクリックします。

ルートアクションのメトリック値の設定

ルートアクションのメトリック値を設定するには、次の手順を実行します。

手順

- ステップ 1 ASDM で、**[Configuration] > [Device Setup] > [Routing] > [Route Maps]** の順に選択します。
- ステップ 2 **[Add]** をクリックします。
[Add Route Map] または [Edit Route Map] ダイアログボックスが表示されます。このダイアログボックスでは、ルートマップ名、シーケンス番号、およびその再配布アクセス（許可または拒否）の割り当てまたは選択を行うことができます。ルートマップのエントリは順番に読み取られます。この順序は、シーケンス番号で指定できます。シーケンス番号が指定されていない場合は、ASA にルートマップ エントリを追加した順序が使用されます。
- ステップ 3 **[Set Clause]** タブをクリックして、ターゲットプロトコルに再配布される次の情報を変更します。
 - **[Set Metric Clause]** チェックボックスを使用して、宛先ルーティングプロトコルに対するメトリック値をイネーブルにするかディセーブルにするかを指定し、値を **[Value]** フィールドに入力します。
 - **[Set Metric Type]** チェックボックスをオンにすると宛先ルーティングプロトコルのメトリックタイプがイネーブルになり、オフにするとディセーブルになります。ドロップダウンリストからメトリックタイプを選択します。

ルートマップの例

次の例は、ホップカウント 1 でルートを OSPF に再配布する方法を示しています。

1. ASDM で、[Configuration] > [Device Setup] > [Routing] > [Route Maps] の順に選択します。
2. [Add] をクリックします。
3. [Route Map Name] フィールドに **1-to-2** と入力します。
4. ルーティング シーケンス番号を [Sequence Number] フィールドに入力します。
5. [Permit] オプション ボタンをクリックします。
デフォルトでは、このタブが一番上にあります。
6. [Match Clause] タブをクリックします。
7. [Match Metric of Route] チェックボックスをオンにして、メトリック値 **1** を入力します。
8. [Set Clause] タブをクリックします。
9. [Set Metric Value] チェックボックスをオンにして、メトリック値 **5** を入力します。
10. [Set Metric-Type] チェックボックスをオンにして、[Type-1] を選択します。

ルートマップの履歴

表 29: ルートマップの機能履歴

機能名	プラットフォーム リリース	機能情報
ルート マップ	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [Route Maps]。
スタティックおよびダイナミックルートマップのサポートの強化	8.0(2)	ダイナミックおよびスタティックルートマップのサポートが強化されました。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	ルート マップは、マルチ コンテキスト モードでサポートされます。
BGP のサポート	9.2(1)	この機能が導入されました。 [Configuration] > [Device Setup] > [Routing] > [Route Maps] 画面が更新され、2つのタブ [BGP match clause] および [BGP set clause] が追加されました。

機能名	プラットフォーム リリース	機能情報
プレフィックス ルールの IPv6 サポート	9.3.2	この機能が導入されました。 次の画面が更新されました。 [Configuration] > [Device Setup] > [Routing] > [IPv4 Prefix Rules] および [IPv6 Prefix Rules]



第 28 章

BGP

この章では、Border Gateway Protocol (BGP) を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように Cisco ASA を設定する方法について説明します。

- [BGPについて \(693 ページ\)](#)
- [BGP のガイドライン \(697 ページ\)](#)
- [BGP を設定する \(697 ページ\)](#)
- [BGP のモニタリング \(719 ページ\)](#)
- [BGP の履歴 \(720 ページ\)](#)

BGPについて

BGP は相互および内部の自律システムのルーティング プロトコルです。自律システムとは、共通の管理下にあり、共通のルーティングポリシーを使用するネットワークまたはネットワーク グループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー (ISP) 間で使用されるプロトコルです。

BGP を使用する状況

大学や企業などの顧客ネットワークでは、そのネットワーク内でルーティング情報を交換するために OSPF などの内部ゲートウェイ プロトコル (IGP) を通常使用しています。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム (AS) 間で BGP を使用する場合、このプロトコルは外部 BGP (EBGP) と呼ばれます。サービス プロバイダーが BGP を使用して AS 内でルートを交換する場合、このプロトコルは内部 BGP (IBGP) と呼ばれます。

BGP は、IPv6 ネットワーク上で IPv6 プレフィックスのルーティング情報を伝送するために使用することができます。



(注) BGPv6 デバイスがクラスタに参加すると、ロギング レベル 7 が有効の場合、ソフト トレース バックを生成します。

ルーティングテーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティングテーブルで変更が検出された場合、BGP ルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティングアップデートを送信しません。また BGP ルーティングアップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

BGP により学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。これらのプロパティは BGP 属性と呼ばれ、ルート選択プロセスで使用されます。

- **Weight** : これは、シスコ定義の属性で、ルータに対してローカルです。Weight 属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、Weight が最も大きいルートが優先されます。
- **Local preference** : Local preference 属性は、ローカル AS からの出力点を選択するために使用されます。Weight 属性とは異なり、Local preference 属性は、ローカル AS 全体に伝搬されます。AS からの出力点が複数ある場合は、Local preference 属性が最も高い出力点が特定のルートの出力点として使用されます。
- **Multi-exit discriminator** : メトリック属性である Multi-exit discriminator (MED) は、メトリックをアドバタイズしている AS への優先ルートに関して、外部 AS への提案として使用されます。これが提案と呼ばれるのは、MED を受信している外部 AS がルート選択の際に他の BGP 属性も使用している可能性があるためです。MED メトリックが小さい方のルートが優先されます。
- **Origin** : Origin 属性は、BGP が特定のルートについてどのように学習したかを示します。Origin 属性は、次の 3 つの値のいずれかに設定することができ、ルート選択に使用されます。
 - **IGP** : ルートは発信側 AS の内部にあります。この値は、ネットワーク ルータ コンフィギュレーション コマンドを使用して BGP にルートを挿入する場合に設定されます。
 - **EGP** : ルートは Exterior Border Gateway Protocol (EBGP) を使用して学習されます。
 - **Incomplete** : ルートの送信元が不明であるか、他の方法で学習されています。Incomplete の Origin は、ルートが BGP に再配布される時に発生します。
- **AS_path** : ルートアドバタイズメントが自律システムを通過すると、ルートアドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティングテーブルにインストールされます。
- **Next hop** : EBGP の Next-hop 属性は、アドバタイズしているルータに到達するために使用される IP アドレスです。EBGP ピアの場合、ネクスト ホップ アドレスは、ピア間の接続の IP アドレスです。IBGP の場合、EBGP のネクスト ホップ アドレスがローカル AS に伝送されます。

- **Community** : Community 属性は、ルーティングの決定（承認、優先度、再配布など）を適用できる宛先をグループ化する方法、つまりコミュニティを提供します。ルートマップは、Community 属性を設定するために使用されます。事前定義済みの Community 属性は次のとおりです。
 - **no-export** : EBGp ピアにこのルートを実バタイズしません。
 - **no-advertise** : このルートをどのピアにも実バタイズしない。
 - **internet** : インターネット コミュニティにこのルートを実バタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP パスの選択

BGP は、異なる送信元から同じルートの複数の実バタイズメントを受信する場合があります。BGP は最適なパスとして 1 つのパスだけを選択します。このパスを選択すると、BGP は IP ルーティング テーブルに選択したパスを格納し、そのネイバーにパスを伝搬します。BGP は次の基準を使用して（示されている順序で）、宛先へのパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、このアップデートは削除されず。
- **Weight** が最大のパスが優先されます。
- **Weight** が同じである場合、**Local preference** が最大のパスが優先されます。
- **Local preference** が同じである場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、**AS_path** が最短のルートが優先されます。
- すべてのパスの **AS_path** の長さが同じである場合、**Origin** タイプが最下位のパス（IGP は EGP よりも低く、EGP は **Incomplete** よりも低い）が優先されます。
- **Origin** コードが同じである場合、最も小さい **MED** 属性を持つパスが優先されます。
- パスの **MED** が同じである場合、内部パスより外部パスが優先されます。
- それでもパスが同じである場合、最も近い IGP ネイバーを経由するパスが優先されます。
- **BGP マルチパス** ([696 ページ](#)) のルーティング テーブルで、複数のパスのインストールが必要かどうかを判断します。
- 両方のパスが外部の場合、最初に受信したパス（最も古いパス）が優先されます。
- BGP ルータ ID で指定された、IP アドレスが最も小さいパスが優先されます。
- 送信元またはルータ ID が複数のパスで同じである場合、クラスタ リストの長さが最小のパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

BGP マルチパス

BGP マルチパスでは、同一の宛先プレフィックスへの複数の等コスト BGP パスを IP ルーティング テーブルに組み込むことができます。その場合、宛先プレフィックスへのトラフィックは、組み込まれたすべてのパス間で共有されます。

これらのパスは、負荷共有のためのベストパスと共にテーブルに組み込まれます。BGP マルチパスは、ベストパスの選択には影響しません。たとえば、ルータは引き続き、アルゴリズムに従っていずれかのパスをベストパスとして指定し、このベストパスをルータの BGP ピアにアドバタイズします。

同一宛先へのパスをマルチパスの候補にするには、これらのパスの次の特性がベストパスと同等である必要があります。

- 重量
- ローカル プリファレンス
- AS-PATH の長さ
- オリジン コード
- Multi Exit Discriminator (MED)
- 次のいずれかです。
 - ネイバー AS またはサブ AS (BGP マルチパスの追加前)
 - AS-PATH (BGP マルチパスの追加後)

一部の BGP マルチパス機能では、マルチパス候補に要件が追加されます。

- パスは外部ネイバーまたは連合外部ネイバー (eBGP) から学習される必要があります。
- BGP ネクストホップへの IGP メトリックは、ベストパス IGP メトリックと同等である必要があります。

内部 BGP (iBGP) マルチパス候補の追加要件を次に示します。

- 内部ネイバー (iBGP) からパスが学習される必要があります。
- ルータが不等コスト iBGP マルチパス用に設定されていない限り、BGP ネクストホップへの IGP メトリックは、ベストパス IGP メトリックと同等です。

BGP はマルチパス候補から最近受信したパスのうち、最大 n 本のパスを IP ルーティング テーブルに挿入します。この n は、BGP マルチパスの設定時に指定した、ルーティング テーブルに組み込まれるルートの数です。マルチパスが無効な場合のデフォルト値は 1 です。

不等コスト ロード バランシングの場合、BGP リンク帯域幅も使用できます。



(注) 内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対し、同等の next-hop-self が実行されます。

BGP のガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

トランスペアレントファイアウォールモードはサポートされません。BGP は、ルーテッドモードでのみサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。グレースフル リスタートは、IPv6 アドレス ファミリではサポートされません。

BGP を設定する

ここでは、システムで BGP プロセスをイネーブルにして設定する方法について説明します。

手順

- ステップ 1 [BGP の有効化 \(697 ページ\)](#)。
- ステップ 2 [BGP ルーティング プロセスの最適なパスの定義 \(699 ページ\)](#)。
- ステップ 3 [ポリシー リストの設定 \(700 ページ\)](#)。
- ステップ 4 [AS パス フィルタの設定 \(701 ページ\)](#)。
- ステップ 5 [コミュニティ ルールの設定 \(702 ページ\)](#)。
- ステップ 6 [IPv4 アドレス ファミリの設定 \(703 ページ\)](#)。
- ステップ 7 [IPv6 アドレス ファミリの設定 \(712 ページ\)](#)。

BGP の有効化

ここでは、BGP の有効化、BGP ルーティング プロセスの確立、一般的な BGP パラメータの設定に必要な手順について説明します。

手順

- ステップ 1** シングルモードの場合、ASDMで **[Configuration] > [Device Setup] > [Routing] > [BGP] > [General]** の順に選択します。
- (注) マルチモードの場合、ASDMで **[Configuration] > [Context Management] > [BGP]** の順に選択します。BGPをイネーブルにした後に、セキュリティコンテキストに切り替え、**[Configuration] > [Device Setup] > [Routing] > [BGP] > [General]** の順に選択してBGPをイネーブルにします。
- ステップ 2** **[Enable BGP Routing]** チェックボックスをオンにします。
- ステップ 3** **[AS Number]** フィールドに、BGPプロセスの自律システム (AS) 番号を入力します。AS番号内部には、複数の自律番号が含まれます。AS番号には、1～4294967295 または 1.0～XX.YY を指定できます。
- ステップ 4** (オプション) **[Limit the number of AS numbers in the AS_PATH attribute of received routes]** チェックボックスをオンにして、AS_PATH属性のAS番号の数を特定数に制限します。有効値は1～254です。
- ステップ 5** (オプション) **[Log neighbor changes]** チェックボックスをオンにして、BGPネイバーの変更 (アップ状態またはダウン状態) およびリセットのロギングをイネーブルにします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。
- ステップ 6** (オプション) **[Use TCP path MTU discovery]** チェックボックスをオンにし、パスMTUディスカバリ手法を使用して2つのIPホスト間のネットワークパスにおける最大伝送単位 (MTU) のサイズを決定します。これにより、IPフラグメンテーションが回避されます。
- ステップ 7** (オプション) **[Enable fast external failover]** チェックボックスをオンにして、リンク障害の発生時に外部BGPセッションをただちにリセットします。
- ステップ 8** (オプション) **[Enforce that first AS is peer's AS for EBGp routes]** チェックボックスをオンにすると、AS_PATH属性の最初のセグメントとしてそのAS番号をリストしていない外部BGPピアから受信される着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。
- ステップ 9** (オプション) **[Use dot notation for AS numbers]** チェックボックスをオンにして、完全なバイナリ4バイトのAS番号を、ドットで区切られた16ビットの2文字ずつに分割します。0～65535のAS番号は10進数で表され、65535を超えるAS番号はドット付き表記を使用して表されます。
- ステップ 10** **[Neighbor timers]** 領域でタイマー情報を指定します。
- [Keepalive interval]** フィールドに、BGPネイバーがキープアライブメッセージを送信しなくなった後アクティブな状態を継続する時間を入力します。このキープアライブインターバルが終わると、メッセージが送信されない場合、BGPピアはデッドとして宣言されます。デフォルト値は60秒です。
 - [Hold Time]** フィールドに、BGP接続が開始されて設定されている間BGPネイバーがアクティブな状態を維持する時間を入力します。デフォルト値は180秒です。

- c) (オプション) [Min. Hold Time] フィールドに、BGP 接続の開始中/設定中に BGP ネイバーがアクティブな状態を維持する最小時間を入力します。0 ~ 65535 の値を指定します。

ステップ 11 (オプション) [Non Stop Forwarding] セクションで、次の手順を実行します。

- a) [Enable Graceful Restart] チェックボックスをオンにして、ASA ピアがスイッチオーバー後のルートフラップを回避できるようにします。
- b) [Restart Time] フィールドに、BGP オープンメッセージを受信するまで ASA が古いルートを削除するのを待機する時間を入力します。デフォルト値は 120 秒です。有効な値は 1 ~ 3600 秒です。
- c) [Stale Path Time] フィールドに、リスタートする ASA から End Of Record (EOR) メッセージを受信した後、古いルートを削除するまで ASA が待機する時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ~ 3600 秒です。

ステップ 12 [OK] をクリックします。

ステップ 13 [Apply] をクリックします。

BGP ルーティング プロセスの最適なパスの定義

ここでは、BGP の最適なパスを設定するために必要な手順について説明します。最適なパスの詳細については、[BGP パスの選択 \(695 ページ\)](#) を参照してください。

手順

- ステップ 1** ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [Best Path] の順に選択します。
[Best Path configuration] ペインが表示されます。
- ステップ 2** [Default Local Preference] フィールドに、0 ~ 4294967295 の値を指定します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバに送信されます。
- ステップ 3** [Allow comparing MED from different neighbors] チェックボックスをオンにして、さまざまな自律システムのネイバーからのパスにおいて Multi-exit discriminator (MED) の比較ができるようにします。
- ステップ 4** [Compare router-id for identical EBGp paths] チェックボックスをオンにして、最適なパスの選択プロセス中に、外部 BGP ピアから受信した類似のパスを比較し、最適なパスをルータ ID が最も小さいルートに切り替えます。
- ステップ 5** [Pick the best MED path among paths advertised from the neighboring AS] チェックボックスをオンにして、連合ピアから学習したパス間における MED 比較をイネーブルにし、新しいネットワーク エントリを追加します。MED 間の比較は、外部の自律システムがパスに存在しない場合のみ行われます。

ステップ 6 [Treat missing MED as the least preferred one] チェックボックスをオンにして、欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

ポリシー リストの設定

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の **match** 文すべてが評価され、処理されます。1つのルートマップに2つ以上のポリシー リストを設定できる。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の **match** および **set** 文とも共存できます。ここでは、ポリシー リストを設定するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration] > [Device Setup] > [Routing] > [BGP] > [Policy Lists]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Policy List] ダイアログボックスが表示されます。このダイアログボックスでは、ポリシー リスト名、その再配布アクセス（許可または拒否）、一致インターフェイス、一致 IP アドレス、一致 AS パス、一致コミュニティ名リスト、一致メトリック、一致タグ番号を追加することができます。

ステップ 3 [Policy List Name] フィールドに、ポリシー リストの名前を入力します。

ステップ 4 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 5 [Match Interfaces] チェックボックスをオンにして、指定のインターフェイスの1つのネクストホップを持つルートを配布し、次のいずれかを実行します。

- [Interface] フィールドに、インターフェイス名を入力します。
- [Interface] フィールドで、省略記号をクリックすると、手動でインターフェイスを参照し、指定できます。1つ以上のインターフェイスを選択し、[Interface] をクリックして [OK] をクリックします。

ステップ 6 [Specify IP] 領域で、次のように設定します。

- a) [Match Address] チェックボックスをオンにして、標準アクセスリストまたはプレフィックスリストで許可された宛先ネットワーク番号アドレスを持つルートを再配布し、パケットにポリシー ルーティングを実行します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセスリストを参照し、指定します。1つ以上のアクセスリストを選択し、[Access List] をクリックして [OK] をクリックします。

- b) [Match Next Hop] チェックボックスをオンにして、指定したアクセス リストまたはプレフィックス リストの1つから渡されたネクスト ホップ ルータ アドレスを持つルートを再配布します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

- c) [Match Route Source] チェックボックスをオンにして、アクセス リストまたはプレフィックス リストで指定されたアドレスのルータおよびアクセス サーバによってアドバタイズされたルートを再配布します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

ステップ 7 [Match AS Path] チェックボックスをオンにして、BGP 自律システム パスを一致させます。

AS パス フィルタを指定するか、省略記号をクリックして手動で AS パス フィルタを参照し、指定します。1つ以上の AS パス フィルタを選択し、[AS Path Filter] をクリックして [OK] をクリックします。

ステップ 8 [Match Community Names List] チェックボックスをオンにして、BGP コミュニティを一致させます。

- a) コミュニティ ルールを指定するか、省略記号をクリックしてコミュニティ ルールを手動で参照し、指定します。1つ以上のコミュニティ ルールを選択し、[Community Rules] をクリックして [OK] をクリックします。
- b) [Match the specified community exactly] チェックボックスをオンにして、特定の BGP コミュニティを一致させます。

ステップ 9 [Match Metrics] チェックボックスをオンにして、指定したメトリックを持つルートを再配布します。複数のメトリックを指定する場合、ルートはいずれかのメトリックと一致します。

ステップ 10 [Match Tag Numbers] チェックボックスをオンにして、指定したタグと一致するルーティング テーブル内のルートを再配布します。複数のタグ番号を指定した場合、ルートはいずれかのメトリックと一致します。

ステップ 11 [OK] をクリックします。

ステップ 12 [Apply] をクリックします。

AS パス フィルタの設定

AS パス フィルタで、アクセス リストを使用してルーティング アップデート メッセージをフィルタリングし、アップデート メッセージ内の個々のプレフィックスを確認できます。アップデート メッセージ内のプレフィックスがフィルタ基準に一致すると、フィルタ エントリで実行するように設定されているアクションに応じて、個々のプレフィックスは除外されるか受け入れられます。ここでは、AS パス フィルタを設定するために必要な手順について説明します。



(注) AS パス アクセス リストは、通常のファイアウォール ACL とは異なります。

手順

- ステップ 1** ASDM で、**[Configuration] > [Device Setup] > [Routing] > [BGP] > [AS Path Filters]** の順に選択します。
- ステップ 2** **[Add]** をクリックします。
- [Add Filter]** ダイアログボックスが表示されます。このダイアログボックスで、フィルタの名前、その再配布アクセス（許可または拒否）、および正規表現を追加できます。
- ステップ 3** **[Name]** フィールドに、AS パス フィルタの名前を入力します。
- ステップ 4** **[Permit]** または **[Deny]** オプション ボタンをクリックして再配布アクセスを指定します。
- ステップ 5** 正規表現を指定します。正規表現を作成するには、**[Build]** をクリックします。
- ステップ 6** **[Test]** をクリックして、正規表現が選択した文字列と一致するかどうかテストします。
- ステップ 7** **[OK]** をクリックします。
- ステップ 8** **[Apply]** をクリックします。

コミュニティ ルールの設定

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。コミュニティリストを使用すると、ルートマップの **match** 句で使用されるコミュニティグループを作成できます。アクセスリストと同様に、一連のコミュニティリストを作成できます。ステートメントは一致が見つかるまでチェックされ、1つのステートメントが満たされると、テストは終了します。ここでは、コミュニティルールを設定するために必要な手順について説明します。

手順

- ステップ 1** ASDM で、**[Configuration] > [Device Setup] > [Routing] > [BGP] > [Community Rules] >** の順に選択します。
- ステップ 2** **[Add]** をクリックします。
- [Add Community Rule]** ダイアログボックスが表示されます。このダイアログボックスで、ルール名、ルールタイプ、その再配布アクセス（許可または拒否）、および特定のコミュニティを追加できます。
- ステップ 3** **[Rule Name]** フィールドに、コミュニティ ルールの名前を入力します。
- ステップ 4** **[Standard]** または **[Expanded]** オプション ボタンをクリックして、コミュニティ ルールタイプを指定します。

ステップ 5 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 6 標準コミュニティ ルールを追加するには、次の手順を実行します。

- a) [Communities] フィールドで、コミュニティ番号を指定します。有効値は 1 ~ 4294967200 です。
- b) (オプション) [Internet] (既知のコミュニティ) チェックボックスをオンにして、インターネットコミュニティを指定します。このコミュニティのルートは、すべてのピア (内部および外部) にアドバタイズされます。
- c) (オプション) [Do not advertise to any peers] (既知のコミュニティ) チェックボックスをオンにして、no-advertise コミュニティを指定します。このコミュニティのあるルートはピア (内部または外部) にはアドバタイズされません。
- d) (オプション) [Do not export to next AS] (既知のコミュニティ) チェックボックスをオンにして、no-export コミュニティを指定します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。

ステップ 7 拡張コミュニティ ルールを追加するには、次の手順を実行します。

- a) [Regular Expression] フィールドに、正規表現を入力します。または、[Build] をクリックして正規表現を作成します。
- b) [Test] をクリックして、作成した正規表現が選択した文字列と一致するかどうか調べます。

ステップ 8 [OK] をクリックします。

ステップ 9 [Apply] をクリックします。

IPv4 アドレス ファミリの設定

BGP の IPv4 設定は、BGP 設定セットアップ内の IPv4 ファミリ オプションから指定できます。IPv4 ファミリ セクションには、一般設定、集約アドレスの設定、フィルタリング設定、ネイバー設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv4 ファミリに固有のパラメータをカスタマイズすることができます。

IPv4 ファミリの一般設定

ここでは、一般的な IPv4 の設定に必要な手順を説明します。

手順

- ステップ 1** ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。
- ステップ 2** [General] をクリックします。
[General IPv4 family BGP parameters] 設定ペインが表示されます。

- ステップ 3** [Administrative Distances] 領域で、[External]、[Internal] および [Local] のディスタンスを指定します。
- ステップ 4** [Learned Routes Map] ドロップダウン リストからルート マップ名を選択します。[Manage] をクリックして、ルート マップを追加および設定します。
- ステップ 5** (オプション) [Generate Default Route] チェックボックスをオンにして、デフォルト ルート (ネットワーク 0.0.0.0) を配布するように BGP ルーティング プロセスを設定します。
- ステップ 6** (オプション) [Summarize subnet routes into network-level routes] チェックボックスをオンにして、ネットワーク レベルのルートへのサブネット ルートの自動集約を設定します。
- ステップ 7** (オプション) [Advertise inactive routes] チェックボックスをオンにして、ルーティング情報 ベース (RIB) にインストールされていないルートをアドバタイズします。
- ステップ 8** (オプション) [Redistribute iBGP into an IGP] チェックボックスをオンにして、IS-IS や OSPF などの Interior Gateway Protocol (IGP) への iBGP の再配布を設定します。
- ステップ 9** (オプション) [Scanning Interval] フィールドに、ネクスト ホップの検証用に BGP ルータのスキャン間隔 (秒) を入力します。有効な値は 5 ~ 60 秒です。
- ステップ 10** (オプション) [Enable address tracking] チェックボックスをオンにして、BGP ネクスト ホップ アドレス トラッキングを有効化します。[Delay Interval] フィールドで、ルーティング テーブルにインストールされている更新済みのネクストホップルートのチェック間の遅延間隔を指定します。
- ステップ 11** (オプション) ルーティング テーブルにインストールできる並列の内部ボーダー ゲートウェイ プロトコル (iBGP) ルートの最大数を [Number of paths] フィールドで指定し、[iBGP multipaths] チェックボックスをオンにします。
- ステップ 12** [Apply] をクリックします。

IPv4 ファミリ集約アドレスの設定

ここでは、特定のルートの1つのルートへの集約を定義するために必要な手順について説明します。

手順

- ステップ 1** ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。
- ステップ 2** [Aggregate Address] をクリックします。
[Aggregate Address parameters] 設定ペインが表示されます。
- ステップ 3** [Add] をクリックします。
[Add Aggregate Address] ペインが表示されます。
- ステップ 4** [Network] フィールドでネットワーク オブジェクトを指定します。
- ステップ 5** [Generate autonomous system set path information] チェックボックスをオンにして、自律システムの設定パス情報を生成します。

- ステップ 6** [Filters all more- specific routes from the updates] チェックボックスをオンにして、アップデートから固有性の強いルートすべてをフィルタリングします。
- ステップ 7** [Attribute Map] ドロップダウンリストからルートマップを選択します。[Manage] をクリックして、ルートマップを追加または設定します。
- ステップ 8** [Advertise Map] ドロップダウンリストからルートマップを選択します。[Manage] をクリックして、ルートを追加または設定します。
- ステップ 9** [Suppress Map] ドロップダウンリストからルートマップを選択します。[Manage] をクリックして、ルートを追加または設定します。
- ステップ 10** [OK] をクリックします。
- ステップ 11** [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ~ 60 の値です。
- ステップ 12** [Apply] をクリックします。

IPv4 ファミリのフィルタリング設定

ここでは、着信 BGP アップデートで受信したルートまたはネットワークをフィルタリングするために必要な手順について説明します。

手順

- ステップ 1** [Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] を選択します。
- ステップ 2** [Filtering] をクリックします。
- [Define filters for BGP updates] ペインが表示されます。
- ステップ 3** [Add] をクリックします。
- [Add Filter] ペインが表示されます。
- ステップ 4** [Direction] ドロップダウンリストから方向を選択します。方向は、フィルタを着信アップデートに適用するか、または発信アップデートに適用するかを指定します。
- ステップ 5** [Access List] ドロップダウンリストから標準アクセスリストを選択します。[Manage] をクリックして、新しい ACL を追加します。
- ステップ 6** 発信フィルタには、オプションで、配信されるルートのタイプを指定できます。
- a) [Protocol] ドロップダウンリストからオプションを選択します。
- [BGP]、[EIGRP]、[OSPF]、または[RIP]などのルーティングプロトコルを選択できます。
- 接続ルートから学習されたピアおよびネットワークをフィルタリングするには、[Connected] を選択します。
- スタティックルートから学習されたピアおよびネットワークをフィルタリングするには、[Static] を選択します。

- b) [BGP]、[EIGRP]、または [OSPF] を選択した場合は、そのプロトコルのプロセス ID も [Process ID] で選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IPv4 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

- ステップ 1** ASDM で、[Configuration] > [Device Setup] > [Routing] [BGP] > [IPv4 Family] の順に選択します。
- ステップ 2** [Neighbor] をクリックします。
- ステップ 3** [Add] をクリックします。
- ステップ 4** 左側のペインで、[General] をクリックします。
- ステップ 5** [IP Address] フィールドに BGP ネイバーの IP アドレスを入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。
- ステップ 6** [Remote AS] フィールドに、BGP ネイバーが属する自律システムを入力します。
- ステップ 7** (オプション) [Description] フィールドに BGP ネイバーの説明を入力します。
- ステップ 8** (オプション) [Shutdown neighbor administratively] チェックボックスをオンにして、ネイバーまたはピア グループを無効にします。
- ステップ 9** (オプション) [Enable address family] チェックボックスをオンにして、BGP ネイバーとの通信を有効にします。
- ステップ 10** (オプション) [Global Restart Functionality for this peer] チェックボックスをオンにして、ASA ネイバーまたはピア グループの Border Gateway Protocol (BGP) グレースフルリスタート機能をイネーブルまたはディセーブルにします。
- ステップ 11** 左側のペインで、[Filtering] をクリックします。
- ステップ 12** (オプション) [Filter routes using an access list] 領域で、適切な着信または発信アクセス コントロール リストを選択して BGP ネイバー情報を配布します。必要に応じて、[Manage] をクリックして、ACL と ACE を追加します。
- ステップ 13** (オプション) [Filter routes using a route map] 領域で、適切な着信または発信ルート マップを選択して、着信ルートまたは発信ルートにルート マップを適用します。[Manage] をクリックして、ルート マップを設定します。
- ステップ 14** (オプション) [Filter routes using a prefix list] 領域で、適切な着信または発信プレフィックス リストを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、プレフィックス リストを設定します。

- ステップ 15** (オプション) [Filter routes using AS path filter] 領域で、適切な着信または発信 AS パス フィルタを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、AS パス フィルタを設定します。
- ステップ 16** (オプション) [Limit the number of prefixes allowed from the neighbor] チェックボックスをオンにして、ネイバーから受信できるプレフィックスの数を制御します。
- [Maximum prefixes] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
 - [Threshold level] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ (最大数に対する割合) を入力します。有効な値は 1 ~ 100 の整数です。デフォルト値は 75 です。
 - (オプション) [Control prefixes received from a peer] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。
 - プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[Terminate peering when prefix limit is exceeded] をクリックします。[Restart interval] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。
 - 最大プレフィックス数の制限値を超えたときにログメッセージを生成するには、[Give only warning message when prefix limit is exceeded] をクリックします。この場合、BGP ネイバーは終了しません。
- ステップ 17** 左側のペインで、[Routes] をクリックします。
- ステップ 18** [Advertisement Interval] フィールドに、BGP ルーティング アップデートが送信される最小間隔 (秒) を入力します。
- ステップ 19** (オプション) [Generate Default route] チェックボックスをオンにして、ローカル ルータにネイバーへのデフォルトルート 0.0.0.0 の送信を許可して、このルートがデフォルトルートとして使用されるようにします。
- [Route map] ドロップダウン リストから、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを選択します。[Manage] をクリックして、ルート マップを追加および設定します。
- ステップ 20** (オプション) 条件に応じてアドバタイズされるルートを追加するには、次の手順を実行します。
- a) [Conditionally Advertised Routes] セクションで [Add] をクリックします。
 - b) exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップを [Advertise Map] ドロップダウン リストから選択します。
 - c) 次のいずれかを実行します。
 - [Exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。

- [Non-exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。

d) [OK] をクリックします。

ステップ 21 (オプション) [Remove private autonomous system (AS) numbers from outbound routing updates] チェックボックスをオンにし、プライベート AS 番号を発信ルートにおけるアドバタイズ対象から除外します。

ステップ 22 左側のペインで、[Timers] をクリックします。

ステップ 23 (オプション) [Set timers for the BGP peer] チェックボックスをオンにし、キープアライブ頻度、保持時間、最小保持時間を設定します。

- [Keepalive frequency] フィールドに、ASA がキープアライブ メッセージをネイバーに送信する頻度 (秒) を入力します。有効な値は、0 ~ 65535 です。デフォルト値は 60 秒です。
- [Holdtime] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間 (秒) を入力します。デフォルト値は 180 秒です。
- (オプション) [Min Hold time] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間 (秒) を入力します。

ステップ 24 左側のペインで、[Advanced] をクリックします。

ステップ 25 (オプション) [Enable Authentication] チェックボックスをオンにして、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。

- [Encryption Type] ドロップダウン リストから暗号化タイプを選択します。
- パスワードを [Password] フィールドに入力します。[パスワードの確認 (Confirm Password)] フィールドにパスワードを再入力します。

(注) パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字を指定できます。最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 26 (オプション) [Send Community Attribute to this neighbor] チェックボックスをオンにします。

ステップ 27 (オプション) [Use ASA as next hop for neighbor] チェックボックスをオンにし、ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

ステップ 28 次のいずれかを実行します。

- [Allow connections with neighbor that is not directly connected] をクリックして、直接接続されていないネットワーク上で外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
 - (オプション) [TTL hops] フィールドに持続可能時間を入力します。有効な値は、1 ~ 255 です。
 - (オプション) [Disable connection verification] チェックボックスをオンにし、ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認を無効にします。
- [Limit number of TTL hops to neighbor] をクリックして、BGP ピアリング セッションを保護できるようにします。
 - [TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ~ 254 です。

ステップ 29 (オプション) [Weight] フィールドに BGP ネイバー接続の重みを入力します。

ステップ 30 [BGP version] ドロップダウンリストから、ASA が受け入れる BGP バージョンを選択します。

(注) バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 31 (オプション) [TCP Path MTU Discovery] チェックボックスをオンにして、BGP セッションの TCP トランスポート セッションをイネーブルにします。

ステップ 32 [TCP transport mode] ドロップダウンリストから TCP 接続モードを選択します。

ステップ 33 左側のペインで、[Migration] をクリックします。

ステップ 34 (オプション) [Customize the AS number for routes received from the neighbor] チェックボックスをオンにして、eBGP ネイバーから受信したルートの AS_path 属性をカスタマイズします。

- [Local AS Number] フィールドにローカル自律システム番号を入力します。有効な値は、1 ~ 65535 です。
- (オプション) [Do not prepend local AS number for routes received from neighbor] チェックボックスをオンにします。ローカル AS 番号は、eBGP ピアから受信したルートの前に追加されません。
- (オプション) [Replace real AS number with local AS number in routes received from neighbor] チェックボックスをオンにします。ローカルルーティングプロセスの AS 番号は前に追加されません。
- (オプション) [Accept either real AS number or local AS number in routes received from neighbor] チェックボックスをオンにします。

ステップ 35 [OK] をクリックします。

ステップ 36 [Apply] をクリックします。

IPv4 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

- ステップ 1 ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。
- ステップ 2 [Networks] をクリックします。
[Define networks to be advertised by the BGP routing process] 設定ペインが表示されます。
- ステップ 3 [Add] をクリックします。
[Add Network] ペインが表示されます。
- ステップ 4 [Address] フィールドで BGP がアドバタイズするネットワークを指定します。
- ステップ 5 (オプション) [Netmask] ドロップダウン リストからネットワーク マスクまたはサブネットワーク マスクを選択します。
- ステップ 6 [Route Map] ドロップダウン リストから、アドバタイズされるネットワークをフィルタリングするために調べる必要があるルート マップを選択します。[Manage] をクリックして、ルート マップを設定または追加します。
- ステップ 7 [OK] をクリックします。
- ステップ 8 [Apply] をクリックします。
-

IPv4 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

- ステップ 1 ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > の順に選択します。
- ステップ 2 [Redistribution] をクリックします。
[Redistribution] ペインが表示されます。
- ステップ 3 [Add] をクリックします。

[Add Redistribution] ペインが表示されます。

- ステップ 4** [Source Protocol] ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。
- ステップ 5** [Process ID] ドロップダウン リストからソース プロトコルのプロセス ID を選択します。
- ステップ 6** (オプション) [Metric] フィールドに、再配布されるルートのメトリックを入力します。
- ステップ 7** [Route Map] ドロップダウン リストから、再配布されるネットワークをフィルタリングするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルート マップを設定または追加します。
- ステップ 8** [Internal]、[External]、および [NSSA External Match] チェックボックスのうち 1 つ以上をオンにして、OSPF ネットワークからルートを再配布します。
- この手順は、OSPF ネットワークからの再配布にのみ適用できます。
- ステップ 9** [OK] をクリックします。
- ステップ 10** [Apply] をクリックします。

IPv4 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

- ステップ 1** ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > の順に選択します。
- ステップ 2** [Route Injection] をクリックします。
- [Route Injection] ペインが表示されます。
- ステップ 3** [Add] をクリックします。
- [Add Conditionally injected route] ペインが表示されます。
- ステップ 4** [Inject Map] ドロップダウンリストから、ローカル BGP ルーティングテーブルに注入するプレフィックスを指定するルート マップを選択します。
- ステップ 5** [Exist Map] ドロップダウンリストから、BGP スピーカーが追跡するプレフィックスを含むルート マップを選択します。
- ステップ 6** [Injected routes will inherit the attributes of the aggregate route] チェックボックスをオンにし、集約ルートの属性を継承するよう注入されたルートを設定します。
- ステップ 7** [OK] をクリックします。
- ステップ 8** [Apply] をクリックします。

IPv6 アドレス ファミリの設定

BGP の IPv6 設定は、BGP 設定セットアップ内の IPv6 ファミリ オプションから指定できます。IPv6 ファミリ セクションには、一般設定、集約アドレスの設定、ネイバー設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv6 ファミリに固有のパラメータをカスタマイズすることができます。

ここでは、BGP IPv6 ファミリの設定をカスタマイズする方法について説明します。

IPv6 ファミリの一般設定

ここでは、一般的な IPv6 の設定に必要な手順を説明します。

手順

-
- ステップ 1 ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] の順に選択します。
 - ステップ 2 [General] をクリックします。
[General IPv6 family BGP parameters] 設定ペインが表示されます。
 - ステップ 3 [Administrative Route Distances] 領域で、外部、内部およびローカル ディスタンスを指定します。
 - ステップ 4 (オプション) [Generate Default Route] チェックボックスをオンにして、デフォルト ルート (ネットワーク 0.0.0.0) を配布するように BGP ルーティング プロセスを設定します。
 - ステップ 5 (オプション) [Advertise inactive routes] チェックボックスをオンにして、ルーティング情報 ベース (RIB) にインストールされていないルートを実体化します。
 - ステップ 6 (オプション) [Redistribute iBGP into an IGP] チェックボックスをオンにして、IS-IS や OSPF などの Interior Gateway Protocol (IGP) への iBGP の再配布を設定します。
 - ステップ 7 (オプション) [Scanning Interval] フィールドに、ネクスト ホップの検証用に BGP ルータのスキャン間隔 (秒) を入力します。有効な値は 5 ~ 60 秒です。
 - ステップ 8 (オプション) [Number of paths] フィールドに、Border Gateway Protocol ルートの最大数を指定します。
 - ステップ 9 (オプション) [iBGP multipaths] チェックボックスをオンにし、[Number of paths] フィールドに、ルーティング テーブルにインストールできる並列の内部ボーダー ゲートウェイ プロトコル (iBGP) ルートの最大数を指定します。
 - ステップ 10 [Apply] をクリックします。
-

IPv6 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

-
- ステップ 1** ASDM で、[**Configuration**] > [**Device Setup**] > [**Routing**] > [**BGP**] > [**IPv6 Family**] の順に選択します。
- ステップ 2** [Aggregate Address] をクリックします。
[Aggregate Address parameters] 設定ペインが表示されます。
- ステップ 3** [Add] をクリックします。
[Add Aggregate Address] ペインが表示されます。
- ステップ 4** [IPv6/Address Mask] フィールドで IPv6 アドレスを指定します。または、ネットワークオブジェクトを参照して追加します。
- ステップ 5** [Generate autonomous system set path information] チェックボックスをオンにして、自律システムの設定パス情報を生成します。このルートにアドバタイズされるパスは、集約中のすべてのパス内に含まれるすべての要素で構成される AS_SET になります。
- (注) このルートは集約されたルート変更に関する自律システムパス到着可能性情報として継続的に削除してアップデートする必要があるため、多くのパスを集約する際に aggregate-address コマンドのこの形式を使用しないでください。
- ステップ 6** [Filters all more- specific routes from the updates] チェックボックスをオンにして、アップデートから固有性の強いルートをすべてフィルタリングします。これにより、集約ルートが作成されるだけでなく、すべてのネイバーへの固有性の強いルートのアドバタイズメントが抑制されません。
- ステップ 7** [Attribute Map] ドロップダウンリストからルートマップを選択します。[Manage] をクリックして、ルートマップを追加または設定します。これにより、集約ルートの属性を変更できます。
- ステップ 8** [Advertise Map] ドロップダウンリストからルートマップを選択します。[Manage] をクリックして、ルートを追加または設定します。これにより、集約ルートのさまざまなコンポーネントの作成に使用される特定のルートが選択されます。
- ステップ 9** [Suppress Map] ドロップダウンリストからルートマップを選択します。[Manage] をクリックして、ルートを追加または設定します。これにより、集約ルートが作成されますが、指定したルートのアドバタイズメントは抑制されます。
- ステップ 10** [OK] をクリックします。
- ステップ 11** [Aggregate Timer] フィールドで、集約タイマーの値 (秒) を指定します。有効な値は、0 または 6 ~ 60 の値です。この値で、ルートが集約される間隔を指定します。デフォルト値は 30 秒です。
- ステップ 12** [Apply] をクリックします。
-

IPv6 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

- ステップ 1 ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] の順に選択します。
- ステップ 2 [Neighbor] をクリックします。
- ステップ 3 [Add] をクリックします。
- ステップ 4 左側のペインで、[General] をクリックします。
- ステップ 5 [IPv6 Address] フィールドに BGP ネイバーの IPv6 アドレスを入力します。この IPv6 アドレスは、BGP ネイバー テーブルに追加されます。
- ステップ 6 [Remote AS] フィールドに、BGP ネイバーが属する自律システムを入力します。
- ステップ 7 (オプション) [Description] フィールドに BGP ネイバーの説明を入力します。
- ステップ 8 (オプション) [Shutdown neighbor administratively] チェックボックスをオンにして、ネイバーまたはピア グループを無効化します。
- ステップ 9 (オプション) [Enable address family] チェックボックスをオンにして、BGP ネイバーとの通信を有効にします。
- ステップ 10 左側のペインで、[Filtering] をクリックします。
- ステップ 11 (オプション) [Filter routes using a route map] 領域で、適切な着信または発信ルート マップを選択して、着信ルートまたは発信ルートにルート マップを適用します。[Manage] をクリックして、ルート マップを設定します。
- ステップ 12 (オプション) [Filter routes using a prefix list] 領域で、適切な着信または発信プレフィックス リストを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、プレフィックス リストを設定します。
- ステップ 13 (オプション) [Filter routes using AS path filter] 領域で、適切な着信または発信 AS パス フィルタを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、AS パス フィルタを設定します。
- ステップ 14 (オプション) [Limit the number of prefixes allowed from the neighbor] チェックボックスをオンにして、ネイバーから受信できるプレフィックスの数を制御します。
- ステップ 15 [Maximum prefixes] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
- ステップ 16 [Threshold level] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ (最大数に対する割合) を入力します。有効な値は 1 ~ 100 の整数です。デフォルト値は 75 です。
- ステップ 17 (オプション) [Control prefixes received from a peer] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。
 - プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[Terminate peering when prefix limit is exceeded] をクリックします。[Restart interval] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。
 - 最大プレフィックス数の制限値を超えたときにログメッセージを生成するには、[Give only warning message when prefix limit is exceeded] をクリックします。この場合、BGP ネイバーは終了しません。
- ステップ 18 左側のペインで、[Routes] をクリックします。

- ステップ 19** [Advertisement Interval] フィールドに、BGP ルーティング アップデートが送信される最小間隔 (秒) を入力します。
- ステップ 20** (オプション) [Generate Default route] チェックボックスをオンにして、ローカル ルータにネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。
- ステップ 21** [Route map] ドロップダウン リストから、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを選択します。[Manage] をクリックして、ルート マップを追加および設定します。
- ステップ 22** (オプション) 条件に応じてアドバタイズされるルートを追加するには、次の手順を実行します。
- a) [Conditionally Advertised Routes] セクションで [Add] をクリックします。
 - b) exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップを [Advertise Map] ドロップダウン リストから選択します。
 - c) 次のいずれかを実行します。
 - [Exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
 - [Non-exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
 - d) [OK] をクリックします。
- ステップ 23** (オプション) [Remove private autonomous system (AS) numbers from outbound routing updates] チェックボックスをオンにし、プライベート AS 番号を発信ルートにおけるアドバタイズ対象から除外します。
- ステップ 24** 左側のペインで、[Timers] をクリックします。
- ステップ 25** (オプション) [Set timers for the BGP peer] チェックボックスをオンにし、キープアライブ頻度、保持時間、最小保持時間を設定します。
- ステップ 26** [Keepalive frequency] フィールドに ASA がキープアライブ メッセージをネイバーに送信する頻度 (秒) を入力します。有効な値は、0 ~ 65535 です。デフォルト値は 60 秒です。
- ステップ 27** [Hold time] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間 (秒) を入力します。デフォルト値は 180 秒です。
- ステップ 28** (オプション) [Min Hold time] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間 (秒) を入力します。
- ステップ 29** 左側のペインで、[Advanced] をクリックします。
- ステップ 30** (オプション) [Enable Authentication] チェックボックスをオンにして、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。
- ステップ 31** [Encryption Type] ドロップダウン リストから暗号化タイプを選択します。
- ステップ 32** パスワードを [Password] フィールドに入力します。[Confirm Password] フィールドにパスワードを再入力します。

(注) パスワードは大文字と小文字を区別し、`service password-encryption` コマンドが有効な場合は最大 25 文字、`service password-encryption` コマンドが有効でない場合は最大 81 文字を指定できます。最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 33 (オプション) [Send Community Attribute to this neighbor] チェックボックスをオンにします。

ステップ 34 (オプション) [Use ASA as next hop for neighbor] チェックボックスをオンにし、ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

ステップ 35 次のいずれかを実行します。

- [Allow connections with neighbor that is not directly connected] をクリックして、直接接続されていないネットワーク上で外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
 - (オプション) [TTL hops] フィールドに存続可能時間を入力します。有効な値は、1 ~ 255 です。
 - (オプション) [Disable connection verification] チェックボックスをオンにし、ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認を無効にします。
- [Limit number of TTL hops to neighbor] をクリックして、BGP ピアリングセッションを保護できるようにします。[TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ~ 254 です。

ステップ 36 (オプション) [Weight] フィールドに BGP ネイバー接続の重みを入力します。

ステップ 37 [BGP version] ドロップダウン リストから、ASA が受け入れる BGP バージョンを選択します。

(注) バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 38 (オプション) [TCP Path MTU Discovery] チェックボックスをオンにして、BGP セッションの TCP トランスポートセッションをイネーブルにします。

ステップ 39 [TCP transport mode] ドロップダウン リストから TCP 接続モードを選択します。

ステップ 40 左側のペインで、[Migration] をクリックします。

ステップ 41 (オプション) [Customize the AS number for routes received from the neighbor] チェックボックスをオンにして、eBGP ネイバーから受信したルートの AS_path 属性をカスタマイズします。

- [Local AS Number] フィールドにローカル自律システム番号を入力します。有効な値は、1 ~ 65535 です。
- (オプション) [Do not prepend local AS number for routes received from neighbor] チェックボックスをオンにします。ローカル AS 番号は、eBGP ピアから受信したルートの前に追加されません。

- (オプション) [Replace real AS number with local AS number in routes received from neighbor] チェックボックスをオンにします。ローカルルーティングプロセスの AS 番号は前に追加されません。
- (オプション) [Accept either real AS number or local AS number in routes received from neighbor] チェックボックスをオンにします。

ステップ 42 [OK] をクリックします。

ステップ 43 [Apply] をクリックします。

IPv6 ネットワークの設定

ここでは、BGP ルーティングプロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] の順に選択します。

ステップ 2 [Networks] をクリックします。

[Define the networks to be advertised by the BGP routing process] 設定ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Network] ペインが表示されます。

ステップ 4 [IPv6 Address/mask] フィールドで、BGP がアドバタイズするネットワークを指定します。

ステップ 5 [Route Map] ドロップダウン リストから、アドバタイズされるネットワークをフィルタリングするために調べる必要のあるルートマップを選択します。任意で、[Manage] をクリックして、ルートマップを設定または追加します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックします。

IPv6 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] の順に選択します。

- ステップ 2 [Redistribution] をクリックします。
- ステップ 3 [Add] をクリックします。
[Add Redistribution] ペインが表示されます。
- ステップ 4 [Source Protocol] ドロップダウン リストで、BGP ドメインにルートを再配布する元となるプロトコルを選択します。
- ステップ 5 [Process ID] ドロップダウン リストで、ソース プロトコルのプロセス ID を選択します。これは OSPF ソース プロトコルに対してのみ使用できます。
- ステップ 6 (オプション) [Metric] フィールドに、再配布されるルートのメトリックを入力します。
- ステップ 7 [Route Map] ドロップダウン リストで、再配布されるネットワークをフィルタリングをするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルート マップを設定または追加します。
- ステップ 8 [Match] チェックボックス ([Internal]、[External 1]、[External 2]、[NSSA External 1]、[NSSA External 2] チェックボックス) を 1 つ以上オンにして、OSPF ネットワークからルートを再配布します。
この手順は、OSPF ネットワークからの再配布にのみ適用できます。
- ステップ 9 [OK] をクリックします。
- ステップ 10 [Apply] をクリックします。

IPv6 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

- ステップ 1 ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。
- ステップ 2 [Route Injection] をクリックします。
- ステップ 3 [Add] をクリックします。
[Add Conditionally injected route] ペインが表示されます。
- ステップ 4 [Inject Map] ドロップダウン リストで、ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップを選択します。
- ステップ 5 [Exist Map] ドロップダウン リストで、BGP スピーカーが追跡するプレフィックスを含むルート マップを選択します。
- ステップ 6 [Injected routes will inherit the attributes of the aggregate route] チェックボックスをオンにし、集約ルートの属性を継承するよう注入されたルートを設定します。
- ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

BGP のモニタリング

次のコマンドを使用して、BGP ルーティング プロセスをモニタできます。コマンド出力の例と説明については、コマンドリファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな BGP ルーティング 統計情報をモニタするには、次のコマンドの 1 つを入力します。



(注) BGP ログメッセージを無効にするには、ルータ コンフィギュレーション モードで **no bgp log-neighbor-changes** コマンドを入力します。これにより、ネイバー変更メッセージのロギングが無効になります。BGP ルーティング プロセスのルータ コンフィギュレーション モードでこのコマンドを入力します。デフォルトでは、ネイバー変更はログに記録されます。

- **[Monitoring] > [Routing] > [BGP Neighbors]**

各行は 1 つの BGP ネイバーを表します。リストには、ネイバーごとに、IP アドレス、AS 番号、ルータ ID、状態（アクティブ、アイドルなど）、稼働時間、グレースフルリスタート機能、再起動時間、stalepath 時間が含まれます。

- **[Monitoring] > [Routing] > [BGP Routes]**

各行は 1 つの BGP ルートを表します。リストには、ルートごとに、ステータス コード、IP アドレス、ネクスト ホップ アドレス、ルート メトリック、Local preference 値、重み、パスが含まれます。

BGP の履歴

表 30: BGP の各機能の履歴

機能名	プラットフォーム リリース	機能情報
BGP のサポート	9.2(1)	<p>Border Gateway Protocol を使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニタについて、サポートが追加されました。</p> <p>次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [BGP Monitoring] > [Routing] > [BGP Neighbors, Monitoring] > [Routing] > [BGP Routes]</p> <p>次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [Static Routes > Add] > [Add Static Route Configuration] > [Device Setup] > [Routing] > [Route Maps > Add] > [Add Route Map]</p>
ASA クラスタリングに対する BGP のサポート	9.3(1)	<p>L2 および L3 クラスタリングのサポートが追加されました。</p> <p>次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [General]</p>
ノンストップフォワーディングに対する BGP のサポート	9.3(1)	<p>ノンストップフォワーディングのサポートが追加されました。</p> <p>次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [BGP] > [General]、 [Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor]、[Monitoring] > [Routing] > [BGP Neighbors]</p>

機能名	プラットフォーム リリース	機能情報
アドバタイズされたマップに対する BGP のサポート	9.3(1)	アドバタイズされたマップに対する BGPv4 のサポートが追加されました。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor] > [Add BGP Neighbor] > [Routes]
IPv6 に対する BGP のサポート	9.3(2)	IPv6 のサポートが追加されました。 次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family]



第 29 章

OSPF

この章では、Open Shortest Path First (OSPF) ルーティングプロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Cisco ASA を設定する方法について説明します。

- [OSPF の概要 \(723 ページ\)](#)
- [OSPF のガイドライン \(727 ページ\)](#)
- [OSPFv2 の設定 \(729 ページ\)](#)
- [OSPFv2 ルータ ID の設定 \(730 ページ\)](#)
- [OSPFv2 のカスタマイズ \(731 ページ\)](#)
- [OSPFv3 の設定 \(751 ページ\)](#)
- [グレースフルリスタートの設定 \(763 ページ\)](#)
- [OSPFv2 の例 \(766 ページ\)](#)
- [OSPFv3 の例 \(768 ページ\)](#)
- [OSPF のモニタリング \(770 ページ\)](#)
- [OSPF の履歴 \(772 ページ\)](#)

OSPF の概要

OSPF は、パスの選択に距離ベクトル型ではなくリンク ステートを使用する Interior Gateway Routing Protocol (IGRP) です。OSPF は、ルーティング テーブル アップデートではなく、リンクステートアドバタイズメントを伝搬します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、リンクステートアルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステートデータベースが置かれています。

RIP に比べると OSPF は次の点で有利です。

- OSPF のリンクステート データベースのアップデート送信は RIP ほど頻繁ではありません。また、古くなった情報がタイムアウトしたときに、リンクステート データベースは徐々にアップデートされるのではなく、瞬時にアップデートされます。

- ルーティング決定はコストに基づいて行われます。これは、特定のインターフェイスを介してパケットを送信するためにオーバーヘッドが必要であることを示しています。ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストは優先パスを指定するために設定できます。

最短パス優先アルゴリズムの欠点は、CPU サイクルとメモリが大量に必要なことです。

ASA は、OSPF プロトコルの 2 つのプロセスを異なるセットのインターフェイス上で同時に実行できます。同じ IP アドレスを使用する複数のインターフェイス (NAT ではこのようなインターフェイスは共存可能ですが、OSPF ではアドレスの重複は許しません) があるときに、2 つのプロセスを実行する場合があります。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの 2 つのプロセス間で再配布する場合があります。同様に、プライベートアドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティックルートおよび接続されているルートから、ルートを再配布できます。

ASA では、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート (タイプ I とタイプ II) 。
- 仮想リンク。
- LSA フラッドイング。
- OSPF パケットの認証 (パスワード認証と MD5 認証の両方)
- ASA の指定ルータまたは指定バックアップルータとしての設定。ASA は、ABR として設定することもできます。
- スタブエリアと not so stubby エリア。
- エリア境界ルータのタイプ 3 LSA フィルタリング

OSPF は、MD5 とクリアテキストネイバー認証をサポートしています。OSPF と他のプロトコル (RIP など) の間のルート再配布は、攻撃者によるルーティング情報の悪用に使用される可能性があるため、できる限りすべてのルーティングプロトコルで認証を使用する必要があります。

NAT が使用されている場合、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2 つの OSPF プロセス (1 つはパブリック エリア用、1 つはプライベート エリア用) を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ (ABR) と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティングプロトコルを使用しているルータの間でトラフィックを再配布するルータは、自律システム境界ルータ (ASBR) と呼ばれます。

ABR は LSA を使用して、使用可能なルータに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、ABR として機能する ASA で、プライベート

エリアとパブリックエリアを分けることができます。タイプ3LSA（エリア間ルート）は、プライベートネットワークをアドバタイズしなくてもNATとOSPFと一緒に使用できるように、1つのエリアから他のエリアにフィルタリングできます。



(注) フィルタリングできるのはタイプ3LSAだけです。プライベートネットワーク内のASBRとして設定されているASAは、プライベートネットワークを記述するタイプ5LSAを送信しますが、これはAS全体（パブリックエリアも含む）にフラッドングされます。

NATが採用されているが、OSPFがパブリックエリアだけで実行されている場合は、パブリックネットワークへのルートを、デフォルトまたはタイプ5AS外部LSAとしてプライベートネットワーク内で再配布できます。ただし、ASAにより保護されているプライベートネットワークにはスタティックルートを設定する必要があります。また、同一のASAインターフェイス上で、パブリックネットワークとプライベートネットワークを混在させることはできません。

ASAでは、2つのOSPFルーティングプロセス（1つのRIPルーティングプロセスと1つのEIGRPルーティングプロセス）を同時に実行できます。

fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First (OSPF) ネットワークでの統合がより迅速になります。

fast hello パケットに対する OSPF のサポートの前提条件

OSPF がネットワークですでに設定されているか、fast hello パケットに対する OSPF のサポートと同時に設定される必要があります。

fast hello パケットに対する OSPF のサポートについて

次に、fast hello パケットに関する OSPF のサポートと、OSPF fast hello パケットの利点について説明します。

OSPF Hello インターバルおよび dead 間隔

OSPF hello パケットとは、OSPF プロセスがネイバーとの接続を維持するために OSPF ネイバーに送信するパケットです。hello パケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネットリンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。hello パケットには、デッドインターバル中に受信したすべてのネイバーのリストが含まれます。デッドインターバルも設定可能なインターバル（秒単位）で送信されます。デフォルトは hello インターバルの値の 4 倍です。hello インターバルの値は、ネットワーク内ですべて同一にする必要があります。デッドインターバルの値も、ネットワーク内ですべて同一にする必要があります。

この2つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータがデッドインターバル内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

OSPF fast hello パケット

OSPF fast hello パケットとは、1秒よりも短いインターバルで送信される hello パケットのことです。fast hello パケットを理解するには、OSPF hello パケットインターバルとデッドインターバルとの関係についてあらかじめ理解しておく必要があります。[OSPF Hello インターバルおよび dead 間隔 \(725 ページ\)](#) を参照してください。

OSPF fast hello パケットは、ospf dead-interval コマンドで設定されます。デッドインターバルは1秒に設定され、hello-multiplier の値は、その1秒間に送信する hello パケット数に設定されるため、1秒未満の「fast」hello パケットになります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる hello 間隔は0に設定されます。このインターフェイス経由で受信した hello パケットの hello 間隔は無視されます。

デッドインターバルは、1つのセグメント上で一貫している必要があります、1秒に設定するか (fast hello パケットの場合)、他の任意の値を設定します。デッドインターバル内に少なくとも1つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

OSPF fast hello パケットの利点

OSPF fast hello パケット機能を利用すると、ネットワークがこの機能を使用しない場合よりも、短い時間で統合されます。この機能によって、失われたネイバーを1秒以内に検出できるようになります。この機能は、ネイバーの損失が Open System Interconnection (OSI) 物理層またはデータリンク層で検出されないことがあっても、特に LAN セグメントで有効です。

OSPFv2 および OSPFv3 間の実装の差異

OSPFv3 には、OSPFv2 との下位互換性はありません。OSPF を使用して、IPv4 および IPv6 トラフィックの両方をルーティングするには、OSPFv2 および OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携していません。

OSPFv3 では、次の追加機能が提供されます。

- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッドイング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- ネイバー探索およびその他の機能に対する IPv6 リンクローカルアドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。
- 2つの LSA タイプの追加。

- 未知の LSA タイプの処理。
- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPsec ESP 標準を使用する認証サポート。

OSPF のガイドライン

コンテキスト モードのガイドライン

OSPFv2 は、シングル コンテキスト モードとマルチ コンテキスト モードをサポートしています。

- デフォルトでは、共有インターフェイス間でのマルチキャストトラフィックのコンテキスト間交換がサポートされていないため、OSPFv2 インスタンスは共有インターフェイス間で相互に隣接関係を形成できません。ただし、OSPFv2 プロセスの OSPFv2 プロセス設定で静的ネイバー設定を使用すると、共有インターフェイスでの OSPFv2 ネイバーシップを形成できます。
- 個別のインターフェイスでのコンテキスト間 OSPFv2 がサポートされています。

OSPFv3 は、シングル モードのみをサポートしています。

ファイアウォール モードのガイドライン

OSPF は、ルーテッドファイアウォールモードのみをサポートしています。OSPF は、トランスパレントファイアウォールモードをサポートしません。

フェールオーバー ガイドライン

OSPFv2 および OSPFv3 は、ステートフルフェールオーバーをサポートしています。

IPv6 のガイドライン

- OSPFv2 は IPv6 をサポートしません。
- OSPFv3 は IPv6 をサポートしています。
- OSPFv3 は、IPv6 を使用して認証を行います。
- ASA は、OSPFv3 ルートが最適なルートの場合、IPv6 RIB にこのルートをインストールします。
- OSPFv3 パケットは、**capture** コマンドの IPv6 ACL を使用してフィルタリングで除外できます。

クラスタリングのガイドライン

- OSPFv3 暗号化はサポートされていません。クラスタリング環境で OSPFv3 暗号化を設定しようとすると、エラーメッセージが表示されます。
- スパンドインターフェイスモードでは、ダイナミックルーティングは管理専用インターフェイスではサポートされません。
- 個別インターフェイスモードで、OSPFv2 または OSPFv3 ネイバーとしてマスターユニットおよびスレーブユニットが確立されていることを確認します。
- 個別インターフェイスモードでは、OSPFv2 との隣接関係は、マスターユニットの共有インターフェイスの2つのコンテキスト間でのみ確立できます。スタティックネイバーの設定は、ポイントツーポイントリンクでのみサポートされます。したがって、インターフェイスで許可されるのは1つのネイバーステートメントだけです。
- クラスタでマスターロールの変更が発生した場合、次の挙動が発生します。
 - スパンドインターフェイスモードでは、ルータプロセスはマスターユニットでのみアクティブになり、スレーブユニットでは停止状態になります。コンフィギュレーションがマスターユニットと同期されているため、各クラスタユニットには同じルータ ID があります。その結果、隣接ルータはロール変更時のクラスタのルータ ID の変更を認識しません。
 - 個別インターフェイスモードでは、ルータプロセスはすべての個別のクラスタユニットでアクティブになります。各クラスタユニットは設定されたクラスタプールから独自の個別のルータ ID を選択します。クラスタでマスターシップロールが変更されても、ルーティングトポロジは変更されません。

マルチプロトコルラベルスイッチング (MPLS) と OSPF のガイドライン

MPLS 設定ルータから送信されるリンクステート (LS) アップデートパケットに、Opaque Type-10 リンクステートアドバタイズメント (LSA) が含まれており、この LSA に MPLS ヘッダーが含まれている場合、認証は失敗し、アプライアンスはアップデートパケットを確認せずにサイレントにドロップします。ピアルータは確認応答を受信していないため、最終的にネイバー関係を終了します。

ネイバー関係の安定を維持するため、ASA の Opaque 機能を無効にします。

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

その他のガイドライン

- OSPFv2 および OSPFv3 は1つのインターフェイス上での複数インスタンスをサポートしています。
- OSPFv3 は、非クラスタ環境での ESP ヘッダーを介した暗号化をサポートしています。
- OSPFv3 は非ペイロード暗号化をサポートします。

- OSPFv2 は RFC 4811、4812 および 3623 でそれぞれ定義されている、Cisco NSF グレースフルリスタートおよび IETF NSF グレースフルリスタートメカニズムをサポートします。
- OSPFv3 は RFC 5187 で定義されているグレースフルリスタートメカニズムをサポートします。
- 配布可能なエリア内（タイプ 1）ルート数は限られています。これらのルートでは、1 つのタイプ 1 LSA にすべてのプレフィックスが含まれています。システムではパケットサイズが 35 KB に制限されているため、3000 ルートの場合、パケットがこの制限を超過します。2900 本のタイプ 1 ルートが、サポートされる最大数であると考えてください。

OSPFv2 の設定

ここでは、ASA で OSPFv2 プロセスを有効化する方法について説明します。

OSPFv2 をイネーブルにした後、ルートマップを定義する必要があります。詳細については、[ルートマップの定義（683 ページ）](#) を参照してください。その後、デフォルトルートを生成します。詳細については、[スタティックルートの設定（668 ページ）](#) を参照してください。

OSPFv2 プロセスのルートマップを定義した後で、ニーズに合わせてカスタマイズできます。ASA 上で OSPFv2 プロセスをカスタマイズする方法については、[OSPFv2 のカスタマイズ（731 ページ）](#) を参照してください。

OSPFv2 をイネーブルにするには、OSPFv2 ルーティングプロセスを作成し、このルーティングプロセスに関連付ける IP アドレスの範囲を指定し、さらにその IP アドレスの範囲にエリア ID を割り当てる必要があります。

最大 2 つの OSPFv2 プロセス インスタンスをイネーブルにできます。各 OSPFv2 プロセスには、独自のエリアとネットワークが関連付けられます。

OSPFv2 をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup]** の順に選択します。

[OSPF Setup] ペインでは、OSPF プロセスのイネーブル化、OSPF エリアおよびネットワークの設定、および OSPF ルート集約の定義を行うことができます。

ステップ 2 ASDM で OSPF をイネーブルにするには、次の 3 つのタブを使用します。

- [Process Instances] タブでは、各コンテキストに対して最大 2 つの OSPF プロセス インスタンスを有効化できます。シングル コンテキスト モードおよびマルチ コンテキスト モードの両方がサポートされます。[Enable Each OSPF Process] チェックボックスをオンにすると、その OSPF プロセスの固有識別子である数値識別子を入力できるようになります。このプロセス ID は内部的に使用されるものであり、他の OSPF デバイスでの OSPF プロセ

ス ID と一致している必要はありません。有効な値の範囲は 1 ～ 65535 です。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。

[Advanced] をクリックすると、[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。ここで、各 OSPF プロセスに対して、[Router ID]、スパンド EtherChannel または個別インターフェイス クラスティングの クラスタ IP アドレス プール、[Adjacency Changes]、[Administrative Route Distances]、[Timers] および [Default Information Originate] を設定することができます。

- [Area/Networks] タブでは、ASA 上で各 OSPF プロセスに対して指定されているエリアとネットワークが表示されます。このタブからは、エリア ID、エリア タイプ、およびそのエリアに対して設定された認証のタイプを表示できます。OSPF のエリアまたはネットワークを追加または編集する方法については、[OSPFv2 エリアパラメータの設定 \(740 ページ\)](#) を参照してください。
- [Route Summarization] タブでは、ABR を設定できます。OSPF では、ABR が 1 つのエリアのネットワークを別のエリアにアドバタイズします。1 つのエリア内のネットワーク番号が連続するように割り当てられている場合は、サマリールートアドバタイズするように ABR を設定できます。このサマリールートには、そのエリア内の個々のネットワークのうち、指定の範囲に当てはまるものがすべて含まれます。詳細については、「[OSPFv2 エリア間のルート集約の設定 \(736 ページ\)](#)」を参照してください。

OSPFv2 ルータ ID の設定

OSPF ルータ ID は、OSPF データベース内の特定のデバイスを識別するために使用されます。OSPF システム内の 2 台のルータが同じルータ ID を持つことはできません。

ルータ ID が OSPF ルーティング プロセスで手動で設定されていない場合、ルータは論理インターフェイス（ループバック インターフェイス）の最も高い IP アドレスまたはアクティブ インターフェイスの最も高い IP アドレスから決定されたルータ ID を自動的に設定します。ルータ ID を設定すると、ルータに障害が発生するか、または OSPF プロセスがクリアされ、ネイバー関係が再確立されるまで、ネイバーは自動的に更新されません。

OSPF ルータ ID の手動設定

ここでは、ASA の OSPFv2 プロセスで `router-id` を手動で設定する方法について説明します。

手順

ステップ 1 固定ルータ ID を使用するには、`router-id` コマンドを使用します。

`router-id ip-address`

例：

```
ciscoasa(config-router)# router-id 193.168.3.3
```

ステップ 2 以前の OSPF ルータ ID の動作に戻すには、**no router-id** コマンドを使用します。

```
no router-id ip-address
```

例：

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

移行中のルータ ID の挙動

ある ASA、たとえば ASA 1 から別の ASA、たとえば ASA 2 に OSPF 設定を移行すると、次のルータ ID 選択動作が見られます。

1. すべてのインターフェイスがシャットダウンモードの場合、ASA 2 は OSPF router-id に IP アドレスを使用しません。すべてのインターフェイスが「admin down」ステートまたはシャットダウンモードの場合に考えられる router-id の設定は次のとおりです。

- ASA 2 に以前設定された router-id がない場合は、次のメッセージが表示されます。

```
%OSPF: Router process 1 is not running, please configure a router-id
```

最初のインターフェイスが起動すると、ASA 2 はこのインターフェイスの IP アドレスをルータ ID として取得します。

- ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときにすべてのインターフェイスが「admin down」ステートになっていた場合、ASA 2 は古いルータ ID を使用します。ASA 2 は、「clear ospf process」コマンドが発行されるまで、起動されたインターフェイスの IP アドレスが変更されても、古いルータ ID を使用します。

2. ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときに少なくとも 1 つのインターフェイスが「admin down」ステートまたはシャットダウンモードになっていない場合、ASA 2 は新しいルータ ID を使用します。インターフェイスが「down/down」ステートの場合でも、ASA 2 はインターフェイスの IP アドレスから新しいルータ ID を使用します。

OSPFv2 のカスタマイズ

ここでは、OSPFv2 プロセスをカスタマイズする方法について説明します。

OSPFv2 へのルートの再配布

ASA は、OSPFv2 ルーティング プロセス間のルート再配布を制御できます。



- (注) 指定されたルーティング プロトコルから、ターゲット ルーティング プロセスに再配布できるルートを定義することでルートを再配布する場合は、デフォルトルートを最初に生成する必要があります。[スタティックルートの設定 \(668 ページ\)](#) を参照し、その後に[ルートマップの定義 \(683 ページ\)](#) に従ってルートマップを定義します。

スタティック ルート、接続されているルート、RIP ルート、または OSPFv2 ルートを OSPFv2 プロセスに再配布するには、次の手順を実行します。

手順

- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution]** の順に選択します。

[Redistribution] ペインには、1 つのルーティング プロセスから OSPF ルーティング プロセスへのルートを再配布する場合のルールが表示されます。RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。スタティックまたは接続されているルートが、[Setup] > [Networks] タブで設定されたネットワークの範囲内にある場合は、そのルートを再配布する必要はありません。

- ステップ 2** [Add] または [Edit] をクリックします。

または、[Redistribution] ペインでテーブル エントリ (ある場合) をダブルクリックすると、そのエントリの [Add/Edit OSPF Redistribution Entry] ダイアログボックスが開きます。

(注) 以降のステップはすべて、省略可能です。

[Add/Edit OSPF Redistribution Entry] ダイアログボックスでは、[Redistribution] テーブルに新しい再配布ルールを追加することや、既存の再配布ルールを編集することができます。既存の再配布ルールを編集するとき、一部の再配布ルール情報は変更できません。

- ステップ 3** ルート再配布 エントリに関連付ける OSPF プロセスを選択します。既存の再配布ルールを編集している場合、この設定は変更できません。

- ステップ 4** どのソースプロトコルからルートを再配布するかを選択します。次のいずれかのオプションを選択できます。

- [Static] : スタティック ルートを OSPF ルーティング プロセスに再配布します。
- [Connected] : 接続されたルート (インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート) を OSPF ルーティング プロセスに再配布します。接続済みルートは、AS の外部として再配布されます。

- [OSPF] : 別の OSPF ルーティングプロセスからのルートを再配布します。リストから OSPF プロセス ID を選択してください。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、または EIGRP ルートを再配布するときに選択できます。ステップ 5 に進みます。
- [RIP] : RIP ルーティングプロセスからルートを再配布します。
- [BGP] : BGP ルーティングプロセスからルートを再配布します。
- [EIGRP] : EIGRP ルーティングプロセスからルートを再配布します。リストから EIGRP ルーティングプロセスの自律システム番号を選択してください。

ステップ 5 OSPF をソースプロトコルとして選択した場合は、選択した OSPF ルーティングプロセスに別の OSPF ルーティングプロセスからのルートを再配布するのに使用される条件を選択します。これらのオプションは、スタティック、接続済み、RIP、または EIGRP ルートを再配布するときに選択できます。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。

- [Internal] : ルートは特定の AS の内部です。
- [External 1] : 自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。
- [External 2] : 自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。
- [NSSA External 1] : 自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。
- [NSSA External 2] : 自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

ステップ 6 [Metric Value] フィールドに、再配布されるルートのメトリック値を入力します。有効値の範囲は 1 ~ 16777214 です。

同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

ステップ 7 [Metric Type] で、次のオプションのいずれかを選択します。

- メトリックがタイプ 1 外部ルートの場合は、[1] を選択します。
- メトリックがタイプ 2 外部ルートの場合は、[2] を選択します。

ステップ 8 タグ値を [Tag Value] フィールドに入力します。

タグ値は 32 ビット 10 進数値です。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。有効値の範囲は、0～4294967295 です。

- ステップ 9** [Use Subnets] チェックボックスをオンにすると、サブネット化ルートの再配布がイネーブルになります。サブネットされていないルートだけを再配布するには、このチェックボックスをオフにします。
- ステップ 10** 再配布エントリに適用するルートマップの名前を [Route Map] ドロップダウンリストで選択します。
- ステップ 11** ルートマップを追加または設定するには、[Manage] をクリックします。
[Configure Route Map] ダイアログボックスが表示されます。
- ステップ 12** [Add] または [Edit] をクリックしてから、指定したルーティングプロトコルからのルートのうち、どれをターゲットのルーティングプロセスに再配布するかを定義します。詳細については、[ルートマップの定義 \(683 ページ\)](#) を参照してください。
- ステップ 13** [OK] をクリックします。

OSPFv2 にルート を再配布する場合のルート集約の設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。その一方で、指定したネットワークアドレスとマスクに含まれる再配布ルートすべてに対して 1 つのルートをアドバタイズするように ASA を設定することができます。この設定によって OSPF リンクステートデータベースのサイズが小さくなります。

指定した IP アドレスマスク ペアと一致するルートは廃止できます。ルートマップで再配布を制御するために、タグ値を一致値として使用できます。

ルート サマリー アドレスの追加

[Summary Address] ペインには、各 OSPF ルーティングプロセスに設定されたサマリーアドレスに関する情報が表示されます。

他のルーティングプロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。サマリールートは、ルーティングテーブルのサイズを削減するのに役立ちます。

OSPF のサマリールートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティングプロトコルからのルートだけをサマライズできます。



(注) OSPF は summary-address 0.0.0.0 0.0.0.0 をサポートしません。

ネットワークアドレスとマスクに含まれる再配布ルートすべてに対して 1 つのサマリールートをアドバタイズするようにソフトウェアを設定するには、次の手順を実行します。

手順

-
- ステップ 1** メインの ASDM ホーム ページで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Summary Address]** の順に選択します。
- ステップ 2** **[Add]** をクリックします。
- [Add OSPF Summary Address Entry] ダイアログボックスが表示されます。[Summary Address] テーブルの既存のエントリに新しいエントリを追加できます。既存のエントリを編集するとき、一部のサマリーアドレス情報は変更できません。
- ステップ 3** **[OSPF Process]** ドロップダウン リストから、サマリーアドレスに関連付けられた指定 OSPF プロセス ID を選択します。既存のエントリを編集する場合、この情報は変更できません。
- ステップ 4** **[IP Address]** フィールドにサマリーアドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。
- ステップ 5** サマリーアドレスのネットワークマスクを **[Netmask]** ドロップダウンリストから選択します。既存のエントリを編集する場合、この情報は変更できません。
- ステップ 6** **[Advertise]** チェックボックスをオンにして、サマリールートアドバタイズします。サマリーアドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオンになっています。
- [Tag value] に表示される値は、各外部ルートに付加される 32 ビットの 10 進数値です。この値は OSPF 自身には使用されませんが、ASBR 間の情報伝達に使用できます。
- ステップ 7** **[OK]** をクリックします。
-

OSPF サマリー アドレスの追加または編集

手順

-
- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup]** の順に選択します。
- ステップ 2** **[Route Summarization]** タブをクリックします。
- [Add/Edit Route Summarization Entry] ダイアログボックスが表示されます。
- [Add/Edit Route Summarization Entry] ダイアログボックスでは、[Summary Address] テーブルに新しいエントリを追加したり、[Summary Address] テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリーアドレス情報は変更できません。
- ステップ 3** **[OSPF Process]** ドロップダウン リストから、サマリーアドレスに関連付けられた指定 OSPF プロセス ID を選択します。既存のエントリを編集する場合、この情報は変更できません。
- ステップ 4** **[IP Address]** フィールドにサマリーアドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

- ステップ5** サマリーアドレスのネットワークマスクを [Netmask] ドロップダウンリストから入力します。既存のエントリを編集する場合、この情報は変更できません。
- ステップ6** [Advertise] チェックボックスをオンにして、サマリールートアドバタイズします。サマリーアドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオンになっています。

OSPFv2 エリア間のルート集約の設定

ルート集約は、アドバタイズされるアドレスを統合することです。この機能を実行すると、1つのサマリールートがエリア境界ルータを通して他のエリアにアドバタイズされます。OSPFのエリア境界ルータは、ネットワークをある1つのエリアから別のエリアへとアドバタイズしていきます。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべて含むサマリールートをアドバタイズするようにエリア境界ルータを設定することができます。

ルート集約のアドレス範囲を定義するには、次の手順を実行します。

手順

- ステップ1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。
- ステップ2** [Route Summarization] タブをクリックします。
[Add/Edit Route Summarization Entry] ダイアログボックスが表示されます。
[Add/Edit Route Summarization Entry] ダイアログボックスでは、[Summary Address] テーブルに新しいエントリを追加したり、[Summary Address] テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリーアドレス情報は変更できません。
- ステップ3** [Area ID] フィールドに OSPF エリア ID を入力します。既存のエントリを編集する場合、この情報は変更できません。
- ステップ4** [IP Address] フィールドにサマリーアドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

OSPFv2 インターフェイスパラメータの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello インターバル、デッドインターバル、認証キーの各インターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

ASDM では、[Interface] ペインでインターフェイス固有の OSPF ルーティング プロパティ（たとえば OSPF メッセージ認証やプロパティ）を設定できます。OSPF のインターフェイスを設定するためのタブは次の 2 つです。

- [Authentication] タブには、ASA インターフェイスの OSPF 認証情報が表示されます。
- [Properties] タブには、各インターフェイスに定義された OSPF プロパティがテーブル形式で表示されます。

OSPFv2 インターフェイス パラメータを設定するには、次の手順を実行します。

手順

-
- ステップ 1** [Authentication] タブをクリックすると、ASA のインターフェイスの認証情報が表示されます。このテーブルの行をダブルクリックすると、選択したインターフェイスの [Edit OSPF Authentication Interface] ダイアログボックスが開きます。
- ステップ 2** [Edit] をクリックします。
[Edit OSPF Authentication Interface] ダイアログボックスが表示されます。[Edit OSPF Interface Authentication] ダイアログボックスでは、選択したインターフェイスの OSPF 認証タイプおよびパラメータを設定できます。
- ステップ 3** 関連するオプション ボタンをクリックして、認証タイプを選択します。
- [No authentication] : OSPF 認証が無効になります。
 - [Area authentication, if defined] (デフォルト) : そのエリアに指定された認証タイプを使用します。エリア認証の設定については、[OSPFv2 エリア パラメータの設定 \(740 ページ\)](#) を参照してください。エリア認証はデフォルトでディセーブルになっています。したがって、それ以前にエリア認証タイプを指定していない限り、エリア認証を設定するインターフェイスでは、設定するまで認証がディセーブルになっています。
 - [Password authentication] : クリア テキストによるパスワード認証が使用されます（セキュリティの懸念がある場合は推奨しません）。
 - [MD5 authentication] : MD5 認証を使用します。
- ステップ 4** パスワード認証を選択した場合は、[Authentication Password] 領域で次のようにパスワードを入力します。
- a) [Enter Password] フィールドに、最大 8 文字のテキスト文字列を入力します。
 - b) [Re-enter Password] フィールドに、パスワードを再入力します。
- ステップ 5** MD5 の ID とキーの設定を [ID] 領域で選択します。この領域には、MD5 認証がイネーブルのときの MD5 キーとパラメータの入力に関する設定があります。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。
- a) [Key ID] フィールドに、数値のキー ID を入力します。有効値の範囲は、1 ~ 255 です。選択したインターフェイスのキー ID が表示されます。

- b) [Key] フィールドに、最大 16 バイトの英数字文字列を入力します。選択したインターフェイスのキーが表示されます。
- c) [Add] または [Delete] をクリックして、指定された MD5 キーを [MD5 ID and Key] テーブルに追加またはテーブルから削除します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Properties] タブをクリックします。

ステップ 8 編集するインターフェイスを選択します。テーブルの行をダブルクリックすると、選択したインターフェイスの [Properties] タブ ダイアログボックスが開きます。

ステップ 9 [Edit] をクリックします。

[Edit OSPF Interface Properties] ダイアログボックスが表示されます。[Interface] フィールドに、OSPF プロパティ設定の対象であるインターフェイスの名前が表示されます。このフィールドは編集できません。

ステップ 10 このインターフェイスがブロードキャスト インターフェイスかどうかに応じて、[Broadcast] チェックボックスをオンまたはオフにします。

デフォルトでは、イーサネットインターフェイスの場合はこのチェックボックスがオンになっています。このチェックボックスをオフにすると、インターフェイスをポイントツーポイントの非ブロードキャスト インターフェイスとして指定したことになります。インターフェイスをポイントツーポイントの非ブロードキャストとして指定すると、OSPF ルートを VPN トンネル経由で送信できます。

インターフェイスをポイントツーポイント、非ブロードキャストとして設定すると、次の制限が適用されます。

- インターフェイスにはネイバーを 1 つだけ定義できます。
- ネイバーは手動で設定する必要があります詳細については、「[スタティック OSPFv2 ネイバーの定義 \(746 ページ\)](#)」を参照してください。
- クリプト ポイントを指すスタティック ルートを定義する必要があります。詳細については、「[スタティック ルートの設定 \(668 ページ\)](#)」を参照してください。
- トンネル経由の OSPF がインターフェイスで実行中である場合は、アップストリームルータを使用する通常の OSPF を同じインターフェイス上で実行することはできません。
- OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。これは、OSPF アップデートが VPN トンネルを通過できるようにするためです。OSPF ネイバーを指定した後で暗号マップをインターフェイスにバインドした場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。これで、OSPF 隣接関係を VPN トンネル経由で確立できるようになります。

ステップ 11 次のオプションを設定します。

- [Cost] フィールドに、このインターフェイスを通してパケット 1 個を送信するコストを決定する値を入力します。デフォルト値は 10 です。
- [Priority] フィールドに、OSPF ルータ優先順位の値を入力します。

2つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。

この設定の有効値の範囲は 0 ~ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。この設定は、ポイントツーポイントの非ブロードキャストインターフェイスとして設定されているインターフェイスには適用されません。

- [MTU Ignore] チェックボックスをオンまたはオフにします。

OSPF は、ネイバーが共通インターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーによる DBD パケットの交換時に行われます。DBD パケットに受信した MTU が着信インターフェイスに設定されている IP MTU より高い場合、OSPF の隣接性は確立されません。

- [Database filter] チェックボックスをオンまたはオフにします。

この設定は、同期とフラッディングのときに発信 LSA インターフェイスをフィルタリングするのに使用します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。完全メッシュ化トポロジでは、このフラッディングによって帯域幅が浪費されて、リンクおよび CPU の過剰使用につながる可能性があります。このチェックボックスをオンにすると、選択されているインターフェイスでは OSPF の LSA フラッディングが行われなくなります。

ステップ 12 (任意) [Advanced] をクリックして [Edit OSPF Advanced Interface Properties] ダイアログボックスを開きます。ここでは、OSPF hello 間隔、再送信間隔、送信遅延、およびデッド間隔の値を変更できます。

通常は、ネットワーク上で OSPF の問題が発生した場合にだけ、これらの値をデフォルトから変更する必要があります。

ステップ 13 [Intervals] セクションには、次の値を入力します。

- [Hello Interval] には、インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバで同じである必要があります。有効な値の範囲は、1 ~ 8192 秒です。デフォルト値は 10 秒です。
- [Retransmit Interval] には、このインターフェイスに属する隣接関係の LSA 再送信の間隔を秒単位で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効な値の範囲は、1 ~ 8192 秒です。デフォルト値は 5 秒です。
- [Transmit Delay] には、このインターフェイス上で LSA パケット 1 個を送信するのに必要な時間の推定値を秒単位で指定します。更新パケット内の LSA には、送信前に、この

フィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 1 秒です。

ステップ 14 [Detecting Lost Neighbors] セクションで、次のいずれかを実行します。

- [Configure interval within which hello packets are not received before the router declares the neighbor to be down] をクリックします。[Dead Interval] フィールドで、ルータがダウンしていると見なす基準となる時間を秒数で指定します。この時間が経過しても hello パケットが 1 つも受信されない場合は、ネイバーがルータのダウンを宣言します。有効な値の範囲は、1 ～ 8192 秒です。この設定のデフォルト値は、[Hello Interval] フィールドで設定された時間の長さの 4 倍です。
- [Send fast hello packets within 1 seconds dead interval] をクリックします。[Hello multiplier] フィールドで、1 秒ごとに送信される hello パケットの数を指定します。有効な値は、3 ～ 20 です。

OSPFv2 エリアパラメータの設定

複数の OSPF エリアパラメータを設定できます。これらのエリアパラメータ（後述のタスクリストに表示）には、認証の設定、スタブエリアの定義、デフォルトサマリールートへの特定のコストの割り当てがあります。認証では、エリアへの不正アクセスに対してパスワードベースで保護します。

スタブエリアは、外部ルート情報が送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブエリアに送信されます。OSPF スタブエリアのサポートを活用するには、デフォルトのルーティングをスタブエリアで使用する必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2 [Area/Networks] タブをクリックします。

[Add OSPF Area] ダイアログボックスが表示されます。

ステップ 3 次に示す [Area Type] のオプションのいずれかを選択します。

- [Normal] を選択すると、このエリアは標準の OSPF エリアとなります。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。

- [Stub] を選択すると、このエリアはスタブエリアとなります。スタブエリアには、その向こう側にルータまたはエリアはありません。スタブエリアは、AS External LSA（タイプ 5 LSA）がスタブエリアにフラッドされないようにします。スタブエリアを作成するときに、サマリー LSA（タイプ 3 および 4）がそのエリアにフラッディングされないように設定するには、[Summary] チェックボックスをオフにします。
- [Summary] チェックボックスは、エリアをスタブエリアとして定義するときに、LSA がこのエリアに送信されないよう設定する場合にオフにします。デフォルトでは、スタブエリアの場合にこのチェックボックスはオンになります。
- [NSSA] を選択すると、このエリアは Not-So-Stubby Area となります。NSSA は、タイプ 7 LSA を受け入れます。NSSA を作成するときに、[Summary] チェックボックスをオフにすることでサマリー LSA がそのエリアにフラッディングされないようにするオプションがあります。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることもできます。

ステップ 4 [IP Address] フィールドに、エリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルトエリアを作成するには、**0.0.0.0** および ネットマスク **0.0.0.0** を入力できるエリアは 1 つだけです。

ステップ 5 [Network Mask] フィールドに、エリアに追加する IP アドレスまたはホストのネットワーク マスクを入力します。ホストを追加する場合、**255.255.255.255** マスクを選択します。

ステップ 6 [OSPF Authentication type] で、次のオプションから選択します。

- [None] を選択すると、OSPF エリア認証が無効になります。これがデフォルト設定です。
- [Password] を選択すると、クリアテキストパスワードがエリア認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
- [MD5] を選択すると、MD5 認証ができるようになります。

ステップ 7 [Default Cost] フィールドに値を入力して、[OSPF] エリアのデフォルト コストを指定します。有効値の範囲は、0 ～ 65535 です。デフォルト値は 1 です。

ステップ 8 [OK] をクリックします。

OSPFv2 フィルタ ルールの設定

OSPF アップデートで受信または送信されるルートまたはネットワークをフィルタリングするには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Filter Rules] の順に選択します。

- ステップ 2 [Add] をクリックします。
- ステップ 3 [OSPF AS] で OSPF プロセス ID を選択します。
- ステップ 4 [Access List] ドロップダウンリストから標準アクセスリストを選択します。[Manage] をクリックして、新しい ACL を追加します。
- ステップ 5 [Direction] ドロップダウンリストから方向を選択します。方向は、フィルタを着信アップデートに適用するか、または発信アップデートに適用するかを指定します。
- ステップ 6 着信フィルタには、オプションでインターフェイスを指定して、そのインターフェイスが受信するアップデートにフィルタを制限することができます。
- ステップ 7 発信フィルタには、オプションで、配信されるルートのタイプを指定できます。
- [Protocol] ドロップダウンリストからオプションを選択します。
[BGP]、[EIGRP]、[OSPF]、または[RIP]などのルーティングプロトコルを選択できます。
接続ルートから学習されたピアおよびネットワークをフィルタリングするには、[Connected] を選択します。
スタティックルートから学習されたピアおよびネットワークをフィルタリングするには、[Static] を選択します。
 - [BGP]、[EIGRP]、または [OSPF] を選択した場合は、そのプロトコルのプロセス ID も [Process ID] で選択します。
- ステップ 8 [OK] をクリックします。
- ステップ 9 [Apply] をクリックします。

OSPFv2 NSSA の設定

NSSA の OSPFv2 への実装は、OSPFv2 のスタブエリアに似ています。NSSA は、タイプ 5 の外部 LSA をコアからエリアにフラッドिंगすることはありませんが、自律システムの外部ルートのある限られた方法でエリア内にインポートできます。

NSSA は、再配布によって、タイプ 7 の自律システムの外部ルートを NSSA エリア内部にインポートします。これらのタイプ 7 の LSA は、NSSA の ABR によってタイプ 5 の LSA に変換され、ルーティングドメイン全体にフラッドिंगされます。変換中は集約とフィルタリングがサポートされます。

OSPFv2 を使用する中央サイトから異なるルーティングプロトコルを使用するリモートサイトに接続しなければならない ISP またはネットワーク管理者は、NSSA を使用することによって管理を簡略化できます。

NSSA が実装される前は、企業サイトの境界ルータとリモートルータ間の接続では、OSPFv2 スタブエリアとしては実行されませんでした。これは、リモートサイト向けのルートは、スタブエリアに再配布することができず、2 種類のルーティングプロトコルを維持する必要があったためです。RIP のようなシンプルなプロトコルを実行して再配布を処理する方法が一般的でした。NSSA が実装されたことで、企業ルータとリモートルータ間のエリアを NSSA として定義することにより、NSSA で OSPFv2 を拡張してリモート接続をカバーできます。

この機能を使用する前に、次のガイドラインを参考にしてください。

- 外部の宛先に到達するために使用可能なタイプ7のデフォルトルートを設定できます。設定すると、NSSA または NSSA エリア境界ルータまでのタイプ7のデフォルトがルータによって生成されます。
- 同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。そうでない場合、ルータは互いに通信できません。

手順

- ステップ 1** メインの ASDM ホーム ページで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup]** の順に選択します。
- ステップ 2** **[Area/Networks]** タブをクリックします。
- ステップ 3** **[Add]** をクリックします。
[Add OSPF Area] ダイアログボックスが表示されます。
- ステップ 4** **[Area Type]** 領域の **[NSSA]** オプション ボタンをクリックします。
エリアを **Not-So-Stubby Area** にするには、このオプションを選択します。NSSA は、タイプ7 LSA を受け入れます。NSSA を作成するときに、**[Summary]** チェックボックスをオフにすることでサマリー LSA がそのエリアにフラッドされないようにするオプションがあります。また、**[Redistribute]** チェックボックスをオフにし、**[Default Information Originate]** チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることもできます。
- ステップ 5** **[IP Address]** フィールドに、エリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルトエリアを作成するには、**0.0.0.0** およびネットマスク **0.0.0.0** を入力できるエリアは1つだけです。
- ステップ 6** **[Network Mask]** フィールドに、エリアに追加する IP アドレスまたはホストのネットワーク マスクを入力します。ホストを追加する場合、**255.255.255.255** マスクを選択します。
- ステップ 7** **[Authentication]** 領域の **[None]** オプション ボタンをクリックすると、OSPF エリア認証がディセーブルになります。
- ステップ 8** **[Default Cost]** フィールドに値を入力して、**[OSPF]** エリアのデフォルト コストを指定します。有効値の範囲は、0 ~ 65535 です。デフォルト値は 1 です。
- ステップ 9** **[OK]** をクリックします。

クラスタリングの IP アドレス プールの設定 (OSPFv2 および OSPFv3)

個別インターフェイスクラスタリングを使用する場合は、ルータ ID のクラスタプールの IPv4 アドレスの範囲を割り当てることができます。

OSPFv2 の個別インターフェイスのルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てるには、次の手順を実行します。

手順

- ステップ 1 メインの ASDM ホーム ページで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup]** の順に選択します。
- ステップ 2 **[Process Instances]** タブをクリックします。
- ステップ 3 編集する OSPF プロセスを選択してから **[Advanced]** をクリックします。
[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。
- ステップ 4 **[Cluster Pool]** オプション ボタンをクリックします。クラスタリングを使用している場合は、ルータ ID の IP アドレス プールを指定する必要はありません（つまりフィールドは空）。IP アドレス プールを入力しない場合、ASA は自動的に生成されたルータ ID を使用します。
- ステップ 5 IP アドレス プールの名前を入力するか、省略記号をクリックして **[Select IP Address Pool]** ダイアログボックスを表示します。
- ステップ 6 既存の IP アドレス プール名をダブルクリックして、**[Assign]** フィールドに追加します。**[Add]** をクリックして、新しい IP アドレス プールを作成することもできます。
[Add IPv4 Pool] ダイアログボックスが表示されます。
- ステップ 7 **[Name]** フィールドに新しい IP アドレス プール名を入力します。
- ステップ 8 開始 IP アドレスを入力するか、または省略記号をクリックして、**[Browse Starting IP Address]** ダイアログボックスを表示します。
- ステップ 9 エントリをダブルクリックして、**[Starting IP Address]** フィールドに追加し、続いて **[OK]** をクリックします。
- ステップ 10 最後の IP アドレスを入力するか、または省略記号をクリックして、**[Browse Ending IP Address]** ダイアログボックスを表示します。
- ステップ 11 エントリをダブルクリックして、**[Ending IP Address]** フィールドに追加し、続いて **[OK]** をクリックします。
- ステップ 12 ドロップダウン リストからサブネット マスクを選択し、続いて **[OK]** をクリックします。
[Select IP Address Pool] リストに、新しい IP アドレス プールが表示されます。
- ステップ 13 新しい IP アドレス プール名をダブルクリックして、**[Assign]** フィールドに追加し、続いて **[OK]** をクリックします。
[Edit OSPF Process Advanced Properties] ダイアログボックスの **[Cluster Pool]** フィールドに、新しい IP アドレス プール名が表示されます。
- ステップ 14 **[OK]** をクリックします。
- ステップ 15 新しく追加された IP アドレス プール設定を変更する場合は、**[Edit]** をクリックします。
[Edit IPv4 Pool] ダイアログボックスが表示されます。
- ステップ 16 ステップ 4 ~ 14 を繰り返します。

(注) すでに割り当てられ、1 つ以上の接続プロファイルによってすでに使用されている既存の IP アドレス プールを編集または削除することはできません。

ステップ 17 [OK] をクリックします。

ステップ 18 OSPFv3 の個別インターフェイス クラスタリングのルータ ID のクラスタ プールに IPv4 アドレス範囲を割り当てるには、次の手順を実行します。

- a) メインの ASDM ホーム ページで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。
- b) **[Process Instances]** タブをクリックします。
- c) 編集する OSPF プロセスを選択してから **[Advanced]** をクリックします。
[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。
- d) **[Router ID]** ドロップダウン リストから **[Cluster Pool]** オプションを選択します。ルータ ID の IP アドレス プールを指定する必要がない場合は、**[Automatic]** オプションを選択します。IP アドレス プールを設定しない場合、ASA は自動的に生成されたルータ ID を使用します。
- e) IP アドレス プール名を入力します。省略記号をクリックして、**[IP Address Pool]** ダイアログボックスを表示することもできます。
- f) 既存の IP アドレス プール名をダブルクリックして、**[Assign]** フィールドに追加します。**[Add]** をクリックして、新しい IP アドレス プールを作成することもできます。
[Add IPv4 Pool] ダイアログボックスが表示されます。
- g) **[Name]** フィールドに新しい IP アドレス プール名を入力します。
- h) 開始 IP アドレスを入力するか、または省略記号をクリックして、**[Browse Starting IP Address]** ダイアログボックスを表示します。
- i) エントリをダブルクリックして、**[Starting IP Address]** フィールドに追加し、続いて **[OK]** をクリックします。
- j) 最後の IP アドレスを入力するか、または省略記号をクリックして、**[Browse Ending IP Address]** ダイアログボックスを表示します。
- k) エントリをダブルクリックして、**[Ending IP Address]** フィールドに追加し、続いて **[OK]** をクリックします。
- l) ドロップダウン リストからサブネット マスクを選択し、続いて **[OK]** をクリックします。
[Select IP Address Pool] リストに、新しい IP アドレス プールが表示されます。
- m) 新しい IP アドレス プール名をダブルクリックして、**[Assign]** フィールドに追加し、続いて **[OK]** をクリックします。
[Edit OSPF Process Advanced Properties] ダイアログボックスの **[Cluster Pool]** フィールドに、新しい IP アドレス プール名が表示されます。
- n) **[OK]** をクリックします。
- o) 新しく追加されたクラスタ プールの設定を変更する場合は、**[Edit]** をクリックします。
[Edit IPv4 Pool] ダイアログボックスが表示されます。

p) ステップ 4～14 を繰り返します。

(注) すでに割り当てられ、別の OSPFv3 プロセスによってすでに使用されている既存の IP アドレス プールを編集または削除することはできません。

q) [OK] をクリックします。

スタティック OSPFv2 ネイバーの定義

ポイントツーポイントの非ブロードキャストネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv2 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、[スタティック ルートの設定 \(668 ページ\)](#) を参照してください。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Static Neighbor]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add/Edit OSPF Neighbor Entry] ダイアログボックスが表示されます。このダイアログボックスでは、新しいスタティック ネイバーを定義することや、既存のスタティック ネイバーの情報を変更することができます。ポイントツーポイントの非ブロードキャストインターフェイスごとに、スタティック ネイバーを 1 つ定義する必要があります。次の制約事項に注意してください。

- 異なる 2 つの OSPF プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります

ステップ 3 [OSPF Process] ドロップダウンリストで、スタティック ネイバーに関連付ける OSPF プロセスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 4 [Neighbor] フィールドに、スタティック ネイバーの IP アドレスを入力します。

ステップ 5 [Interface] フィールドで、スタティック ネイバーに関連付けるインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 6 [OK] をクリックします。

ルート計算タイマーの設定

OSPFv2 によるトポロジ変更受信と最短パス優先（SPF）計算開始との間の遅延時間が設定できます。最初に SPF を計算してから次に計算するまでの保持時間も設定できます。

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。
- ステップ 2 **[Process Instances]** タブをクリックします。
- ステップ 3 編集する OSPF プロセスを選択してから **[Advanced]** をクリックします。
[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。
- ステップ 4 **[Timers]** 領域では、LSA ペーシングおよび SPF 計算のタイマーの設定に使用される値を変更できます。**[Timers]** 領域で、次の値を入力します。
 - **[Initial SPF Delay]** は、OSPF がトポロジ変更を受信してから SPF 計算が開始されるまでの時間（ミリ秒）を指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。
 - **[Minimum SPF Hold Time]** は、連続する SPF 計算間の保持時間をミリ秒で指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。
 - **[Maximum SPF Wait Time]** は、2 回の連続する SPF 計算間の最大待機時間を指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。
- ステップ 5 **[OK]** をクリックします。

ネイバーの起動と停止のロギング

デフォルトでは、OSPFv2 ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。
- ステップ 2 **[Process Instances]** タブをクリックします。
- ステップ 3 **[Advanced]** をクリックします。
[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。
- ステップ 4 **[Adjacency Changes]** 領域には、syslog メッセージ送信を引き起こす隣接関係変更を定義するための設定があります。**[Adjacency Changes]** 領域で、次の値を入力します。

- [Log Adjacency Changes] チェックボックスをオンにすると、OSPFv2 ネイバーがアップ状態またはダウン状態になるたびに ASA によって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
- [Log Adjacency Changes Detail] チェックボックスをオンにすると、ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも ASA によって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

ステップ 5 [OK] をクリックします。

(注) ネイバーのアップまたはダウンのメッセージが送信されるには、ロギングがイネーブルになっている必要があります。

OSPFでのフィルタリングの設定

[Filtering] ペインには、各 OSPF プロセスに対して設定済みの ABR タイプ 3 LSA フィルタが表示されます。

ABR タイプ 3 LSA フィルタを設定すると、指定したプレフィックスだけが 1つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。このタイプのエリアフィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。

OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。



(注) フィルタリングされるのは、ABR から送信されるタイプ 3 LSA だけです。

OSPF でのフィルタリングを設定するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Filtering] の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add or OSPF Filtering Entry] ダイアログボックスでは、新しいフィルタを [Filter] テーブルに追加することや、既存のフィルタを修正することができます。既存のフィルタを編集するとき、一部のフィルタリング情報は変更できません。

ステップ 3 フィルタエントリに関連付ける OSPF プロセスを [OSPF Process] ドロップダウンリストで選択します。

- ステップ 4** フィルタ エントリに関連付けるエリア ID を [Area ID] ドロップダウン リストで選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- ステップ 5** プレフィックス リストを [Prefix List] ドロップダウン リストで選択します。
- ステップ 6** フィルタリングするトラフィックの方向を [Traffic Direction] ドロップダウン リストで選択します。
- OSPF エリアへの LSA をフィルタリングするには [Inbound] を選択し、OSPF エリアからの LSA をフィルタリングするには [Outbound] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- ステップ 7** [Manage] をクリックすると [Configure Prefix Lists] ダイアログボックスが表示され、ここでプレフィックス リストとプレフィックス ルールを追加、編集、または削除できます。詳細については、[プレフィックス リストの設定 \(688 ページ\)](#) および [ルートアクションのメトリック値の設定 \(689 ページ\)](#) を参照してください。
- ステップ 8** [OK] をクリックします。

OSPF の仮想リンクの設定

OSPF ネットワークにエリアを追加し、そのエリアをバックボーンエリアに直接接続できない場合、仮想リンクを作成する必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ 2 つの OSPF デバイスを接続します。OSPF デバイスのいずれかは、バックボーンエリアに接続されている必要があります。

新しい仮想リンクを定義する、または既存の仮想リンクのプロパティを変更するには、次の手順を実行します。

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Virtual Link] の順に選択します。
- ステップ 2** [Add] または [Edit] をクリックします。
- [Add OSPF Virtual Link] または [Edit OSPF Virtual Link] ダイアログボックスが表示され、ここで新しい仮想リンクを定義することや、既存の仮想リンクのプロパティを変更することができます。
- ステップ 3** 仮想リンクに関連付ける OSPF プロセス ID を [OSPF Process] ドロップダウン リストで選択します。既存の仮想リンク エントリを編集している場合、この設定は変更できません。
- ステップ 4** 仮想リンクに関連付けるエリア ID を [Area ID] ドロップダウン リストで選択します。
- ネイバー OSPF デバイスによって共有されるエリアを選択します。[NSSA] エリアまたは [Stub] エリアは選択できません。既存の仮想リンク エントリを編集している場合、この設定は変更できません。
- ステップ 5** [Peer Router ID] フィールドに、仮想リンク ネイバーのルータ ID を入力します。

既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 6 仮想リンクの詳細プロパティを編集するには、[Advanced] をクリックします。

[Advanced OSPF Virtual Link Properties] ダイアログボックスが表示されます。このエリアにある仮想リンクに対して、OSPF プロパティを設定できます。プロパティには、認証およびパケット間隔設定が含まれます。

ステップ 7 [Authentication] 領域で、[Authentication type] を選択します。次のオプション ボタンのいずれかをクリックします。

- [No authentication] : OSPF 認証が無効になります。
- [Password authentication] : クリア テキストによるパスワード認証が使用されます (セキュリティの懸念がある場合は推奨しません)。
- [MD5 authentication] : MD5 認証を使用します。

ステップ 8 [Authentication Password] 領域で、パスワードを入力し、もう一度入力します (パスワード認証がイネーブルのとき)。パスワードは、最大 8 文字のテキスト文字列であることが必要です。

ステップ 9 [MD5 IDs and Key] 領域で、MD5 のキーとパラメータを入力します (MD5 認証がイネーブルのとき)。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。次の設定を指定します。

- a) [Key ID] フィールドに、数値のキー ID を入力します。有効値の範囲は、1 ~ 255 です。選択したインターフェイスのキー ID が表示されます。
- b) [Key] フィールドに、最大 16 バイトの英数字文字列を入力します。選択したインターフェイスのキー ID が表示されます。
- c) [Add] または [Delete] をクリックして、指定された MD5 キーを [MD5 ID and Key] テーブルに追加またはテーブルから削除します。

ステップ 10 [Interval] 領域で、パケットの間隔を指定します。次のオプションから選択します。

- [Hello Interval] には、インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバで同じである必要があります。有効値の範囲は、1 ~ 65535 秒です。デフォルト値は 10 秒です。
- [Retransmit Interval] には、このインターフェイスに属する隣接関係の LSA 再送信の間隔を秒単位で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ~ 65535 秒です。デフォルト値は 5 秒です。
- [Transmit Delay] には、このインターフェイス上で LSA パケット 1 個を送信するのに必要な時間の推定値を秒単位で指定します。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。

値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1～65535 秒です。デフォルト値は 1 秒です。

- [Dead Interval] には、ルータがダウンしていると思える基準となる時間を秒数で指定します。この時間が経過しても hello パケットが 1 つも受信されない場合は、ネイバーがルータのダウンを宣言します。有効値の範囲は 1～65535 です。このフィールドのデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

ステップ 11 [OK] をクリックします。

OSPFv3 の設定

ここでは、OSPFv3 ルーティング プロセスの設定に関連するタスクについて説明します。

OSPFv3 の有効化

OSPFv3 をイネーブルにするには、OSPFv3 ルーティング プロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスをイネーブルにする必要があります。その後、ターゲットの OSPFv3 ルーティング プロセスにルートを再配布する必要があります。

手順

- ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。
- ステップ 2 [Process Instances] タブで、[Enable OSPFv3 Process] チェックボックスをオンにします。最大 2 つの OSPF プロセス インスタンスをイネーブルにできます。シングル コンテキスト モードだけがサポートされます。
- ステップ 3 [Process ID] フィールドにプロセス ID を入力します。ID は、任意の正の整数が可能です。
- ステップ 4 [Apply] をクリックして変更内容を保存します。
- ステップ 5 以降の手順については、[OSPFv3 エリアパラメータの設定 \(753 ページ\)](#) を参照してください。

OSPFv3 インターフェイス パラメータの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello interval と dead interval というインターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Interfaces]** の順に選択します。
- ステップ 2 **[Authentication]** タブをクリックします。
- ステップ 3 インターフェイスの認証パラメータを指定するには、インターフェイスを選択し、**[Edit]** をクリックします。
[Edit OSPFv3 Interface Authentication] ダイアログボックスが表示されます。
- ステップ 4 **[Authentication Type]** ドロップダウンリストから認証タイプを選択します。使用可能なオプションは、**[Area]**、**[Interface]**、**[None]** です。**[None]** オプションを選択すると、認証が行われません。
- ステップ 5 **[Authentication Algorithm]** ドロップダウンリストから認証アルゴリズムを選択します。サポートされる値は、**[SHA-1]** および **[MD5]** です。
- ステップ 6 **[Authentication Key]** フィールドに認証キーを入力します。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数 (16 バイト) である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数 (20 バイト) である必要があります。
- ステップ 7 **[Encryption Algorithm]** ドロップダウンリストから暗号化アルゴリズムを選択します。サポートされる値は、**[AES-CDC]**、**[3DES]**、**[DES]** です。ヌルのエントリは暗号化されません。
- ステップ 8 **[Encryption Key]** フィールドに暗号キーを入力します。
- ステップ 9 **[OK]** をクリックします。
- ステップ 10 **[Properties]** タブをクリックします。
- ステップ 11 プロパティを変更するインターフェイスを選択し、**[Edit]** をクリックします。
[Edit OSPFv3 Interface Properties] ダイアログボックスが表示されます。
- ステップ 12 **[Enable OSPFv3 on this interface]** チェックボックスをオンにします。
- ステップ 13 ドロップダウンリストからプロセス ID を選択します。
- ステップ 14 ドロップダウンリストから領域 ID を選択します。
- ステップ 15 (オプション) インターフェイスに割り当てる領域インスタンス ID を指定します。インターフェイスは、OSPFv3 エリアを 1 つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリアインスタンス ID を使用できます。
- ステップ 16 ドロップダウンリストからネットワークタイプを選択します。サポートされるオプションは、**[Default]**、**[Broadcast]**、**[Point-to-Point]** です。
- ステップ 17 **[Cost]** フィールドにインターフェイスでのパケット送信コストを入力します。
- ステップ 18 **[Priority]** フィールドにルータプライオリティを入力します。これは、ネットワークにおける指定ルータの特定に役立ちます。有効値の範囲は 0 ~ 255 です。
- ステップ 19 **[Disable MTU mismatch detection]** チェックボックスをオンにして、DBD パケットが受信された場合の OSPF MTU 不一致検出をディセーブルにします。OSPF MTU 不一致検出は、デフォルトでイネーブルになっています。

- ステップ 20** [Filter outgoing link state advertisements] チェックボックスをオンにして、OSPFv3 インターフェイスに対する出力 LSA をフィルタします。デフォルトでは、すべての発信 LSA がインターフェイスにフラッドイングされます。
- ステップ 21** [Timers] 領域の [Dead Interval] フィールドに hello パケットが表示されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間を秒単位で入力します。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ~ 65535 です。
- ステップ 22** [Hello Interval] フィールドに、hello パケットがインターフェイスに送信される間隔を秒単位で入力します。この値は特定のネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ~ 65535 です。デフォルトの間隔は、イーサネットインターフェイスで 10 秒、非ブロードキャストインターフェイスで 30 秒です。
- ステップ 23** [Retransmit Interval] フィールドに、インターフェイスに属する隣接ルータの LSA 再送信間隔を秒単位で入力します。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効値の範囲は、1 ~ 65535 秒です。デフォルトは 5 秒です。
- ステップ 24** [Transmit Delay] フィールドに、インターフェイスでリンク ステート アップデート パケットを送信する予想時間を秒単位で入力します。有効値の範囲は、1 ~ 65535 秒です。デフォルト値は 1 秒です。
- ステップ 25** [OK] をクリックします。
- ステップ 26** [Apply] をクリックして変更内容を保存します。

OSPFv3 エリア パラメータの設定

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。
- ステップ 2** [Areas] タブをクリックします。
- ステップ 3** 新しいエリアを追加するには、[Add] をクリックします。既存のエリアを変更するには、[Edit] をクリックします。選択したエリアを削除するには、[Delete] をクリックします。
- [Add OSPFv3 Area] ダイアログボックスまたは [Edit OSPFv3 Area] ダイアログボックスが表示されます。
- ステップ 4** [OSPFv3 Process ID] ドロップダウン リストから、プロセス ID を選択します。
- ステップ 5** ルートが集約されるエリアを指定するエリア ID を [Area ID] フィールドに入力します。
- ステップ 6** [Area Type] ドロップダウン リストからエリアタイプを選択します。使用可能なオプションは、[Normal]、[NSSA]、[Stub] です。
- ステップ 7** エリアにサマリー LSA の送信を許可する場合は、[Allow sending of summary LSAs into the area] チェックボックスをオンにします。
- ステップ 8** 標準および not so stubby エリアへのインポートルートの再配布を許可するには、[Redistribution imports routes to normal and NSSA areas] チェックボックスをオンにします。

- ステップ 9** OSPFv3 ルーティング ドメインにデフォルト外部ルートを生成するには、[Default information originate] チェックボックスをチェックします。
- ステップ 10** デフォルトルートの生成に使用するメトリックを [Metric] フィールドに入力します。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ~ 16777214 です。
- ステップ 11** [Metric Type] ドロップダウンリストからメトリック タイプを選択します。メトリック タイプは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- ステップ 12** [Default Cost] フィールドにコストを入力します。
- ステップ 13** [OK] をクリックします。
- ステップ 14** [Route Summarization] タブをクリックします。
- ステップ 15** ルートを統合および集約するための新しい範囲を指定するには、[Add] をクリックします。ルートを統合および集約する既存の範囲を変更するには、[Edit] をクリックします。
[Add Route Summarization] ダイアログボックスまたは [Edit Route Summarization] ダイアログボックスが表示されます。
- ステップ 16** [Process ID] ドロップダウンリストからプロセス ID を選択します。
- ステップ 17** [Area ID] ドロップダウンリストからエリア ID を選択します。
- ステップ 18** [IPv6 Prefix/Prefix Length] フィールドに IPv6 プレフィックスとプレフィックス長を入力します。
- ステップ 19** (オプション) このサマリールートのメトリックまたはコストを入力します。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効値の範囲は 0 ~ 16777215 です。
- ステップ 20** [Advertised] チェックボックスをオンにして、アドレス範囲の状態をアドバタイズされた設定し、タイプ 3 サマリー LSA を生成します。
- ステップ 21** [OK] をクリックします。
- ステップ 22** 以降の手順については、[仮想リンク ネイバーの設定 \(754 ページ\)](#) を参照してください。

仮想リンク ネイバーの設定

仮想リンク ネイバーを設定するには、次の手順を実行します。

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Virtual Link] の順に選択します。
- ステップ 2** 新しい仮想リンク ネイバーを追加するには、[Add] をクリックします。既存の仮想リンク ネイバーを変更するには、[Edit] をクリックします。指定された仮想リンク ネイバーを削除するには、[Delete] をクリックします。
[Add Virtual Link] ダイアログボックスまたは [Edit Virtual Link] ダイアログボックスが表示されます。

- ステップ 3** [Process ID] ドロップダウン リストからプロセス ID を選択します。
- ステップ 4** [Area ID] ドロップダウン リストからエリア ID を選択します。
- ステップ 5** [Peer Router ID] フィールドにピア ルータ ID (IP アドレス) を入力します。
- ステップ 6** (オプション) [TTL Security] フィールドに仮想リンクの存続可能時間 (TTL) のセキュリティのホップ数を入力します。ホップ数の値は 1 ~ 254 の範囲で指定します。
- ステップ 7** [Timers] 領域の [Dead Interval] フィールドに、hello パケットが表示されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間を秒単位で入力します。デッド間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセスサーバで同じである必要があります。有効値の範囲は 1 ~ 8192 です。
- ステップ 8** [Hello Interval] フィールドに、インターフェイスで送信される hello パケットの間隔を秒単位で入力します。hello 間隔は、hello パケットでアダプタイズされる符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセスサーバで同じである必要があります。有効値の範囲は 1 ~ 8192 です。デフォルトは 10 です。
- ステップ 9** [Retransmit Interval] フィールドに、インターフェイスに属している隣接ルータの LSA 再送信間隔を秒単位で入力します。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ~ 8192 の範囲で指定できます。デフォルトは 5 分です。
- ステップ 10** [Transmit Delay] フィールドに、インターフェイスのリンク ステート アップデート パケットの送信に必要な予想時間を秒単位で入力します。ゼロよりも大きい整数値を指定します。アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。値の範囲は 1 ~ 8192 です。デフォルトは 1 です。
- ステップ 11** [Authentication] 領域の [Enable Authentication] チェックボックスをオンにして、認証をイネーブルにします。
- ステップ 12** [Security Policy Index] フィールドに、セキュリティ ポリシー インデックスを入力します。値の範囲は、256 ~ 4294967295 の数字です。
- ステップ 13** [Authentication Algorithm] ドロップダウン リストから認証アルゴリズムを選択します。サポートされる値は、[SHA-1] および [MD5] です。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数 (16 バイト) である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数 (20 バイト) である必要があります。
- ステップ 14** [Authentication Key] フィールドに認証キーを入力します。キーは 32 文字の 16 進数文字で構成される必要があります。
- ステップ 15** [Encryption Algorithm] ドロップダウン リストから暗号化アルゴリズムを選択します。サポートされる値は、[AES-CDC]、[3DES]、[DES] です。ヌルのエント리는暗号化されません。
- ステップ 16** [Encryption Key] フィールドに暗号キーを入力します。
- ステップ 17** [OK] をクリックします。
- ステップ 18** [Apply] をクリックして変更内容を保存します。

OSPFv3 受動インターフェイスの設定

手順

-
- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。
- ステップ 2** [Process Instances] タブをクリックします。
- ステップ 3** 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。
[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。
- ステップ 4** [Passive Interfaces] 領域では、インターフェイスのパッシブ OSPFv3 ルーティングをイネーブルにすることができます。パッシブルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信をディセーブルにします。[Passive Interfaces] 領域で、次の設定を選択します。
- [Global passive] チェックボックスをオンにして、テーブルに表示されているインターフェイスすべてをパッシブにします。個々のインターフェイスをオフにすると、そのインターフェイスは非パッシブになります。
 - [Global passive] チェックボックスをオフにすると、すべてのインターフェイスが非パッシブになります。個々のインターフェイスをオンにすると、そのインターフェイスはパッシブになります。
- ステップ 5** [OK] をクリックします。
- ステップ 6** [Apply] をクリックして変更内容を保存します。
-

OSPFv3 アドミニストレーティブ ディスタンスの設定

手順

-
- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。
- ステップ 2** [Process Instances] タブをクリックします。
- ステップ 3** 編集する OSPF プロセスを選択してから [Advanced] をクリックします。
[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。
- [Administrative Route Distances] 領域では、管理ルート間隔の設定に使用された設定を変更することができます。管理ルート間隔は 10~254 の整数です。[Administrative Route Distances] 領域で、次の値を入力します。
- [Inter Area] には、IPv6 ルートの OSPFv3 のエリア間ルートを指定します。

- [Intra Area] には、IPv6 ルートの OSPF のエリア内ルートを指定します。
- [External] には、IPv6 ルートの OSPF の外部タイプ 5 および外部タイプ 7 のルートを指定します。

ステップ 4 [OK] をクリックします。

ステップ 5 [Apply] をクリックして変更内容を保存します。

OSPFv3 タイマーの設定

OSPFv3 の LSA 到着タイマー、LSA ペーシング タイマー、およびスロットリング タイマーを設定できます。

手順

- ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。
- ステップ 2 [Process Instances] タブをクリックします。
- ステップ 3 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。
[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。
- ステップ 4 [Timers] 領域では、LSA 到着、LSA ペーシング、LSA 再送信、LSA スロットル、SPF スロットル時間の設定に使用された設定を変更することができます。[Timers] 領域で、次の値を入力します。
 - [LSA Arrival] には、ネイバーから到着する同一 LSA の最短受信間隔をミリ秒単位で指定します。有効な範囲は 0 ~ 6000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
 - [LSA Flood Pacing] には、フラッディングキュー内の LSA のアップデートのペースをミリ秒単位で指定します。設定できる範囲は 5 ~ 100 ミリ秒です。デフォルト値は 33 ミリ秒です。
 - [LSA Group Pacing] には、LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効値の範囲は 10 ~ 1800 です。デフォルト値は 240 です。
 - [LSA Retransmission Pacing] には、再送信キュー内の LSA がペースされる時間をミリ秒単位で指定します。設定できる範囲は 5 ~ 200 ミリ秒です。デフォルト値は 66 ミリ秒です。
 - [LSA Throttle Initial] には、LSA の最初のオカレンスを生成する遅延をミリ秒単位で指定します。デフォルト値は 0 ミリ秒です。
 - [LSA Throttle Min Hold] には、同じ LSA を発信する最短遅延時間をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。

- [LSA Throttle Max Wait] には、同じ LSA を発信する最長遅延時間をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。
 - (注) LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。
- [SPF Throttle Initial] には、SPF 計算の変更を受信する遅延をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。
- [SPF Throttle Min Hold] には、1 番目と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。デフォルト値は 10000 ミリ秒です。
- [SPF Throttle Max Wait] には、SPF 計算の最長待機時間をミリ秒単位で指定する。デフォルト値は 10000 ミリ秒です。
 - (注) SPF スロットリングでは、最短時間または最長時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

スタティック OSPFv3 ネイバーの定義

ポイントツーポイントの非ブロードキャストネットワークを介して OSPFv3 ルートをアドバタイズするには、スタティック OSPF ネイバーを定義する必要があります。この機能により、OSPFv3 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv3 ネイバーに対するスタティックルートを作成する必要があります。スタティックルートの作成方法の詳細については、[スタティックルートの設定 \(668 ページ\)](#) を参照してください。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Static Neighbor] の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add Static Neighbor] または [Edit Static Neighbor] ダイアログボックスが表示されます。このダイアログボックスでは、新しいスタティックネイバーを定義することや、既存のスタティックネイバーの情報を変更することができます。ポイントツーポイントの非ブロードキャストイン

ターフェイスごとに、スタティック ネイバーを1つ定義する必要があります。次の制約事項に注意してください。

- 異なる2つの OSPFv3 プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります

ステップ3 [Interface] ドロップダウンリストから、スタティック ネイバーに関連付けられたインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ4 [Link-local address] フィールドに、スタティック ネイバーの IPv6 アドレスを入力します。

ステップ5 (オプション) [Priority] フィールドに、プライオリティ レベルを入力します。

ステップ6 (オプション) [Poll Interval] フィールドに、ポーリング間隔を秒単位で入力します。

ステップ7 [OK] をクリックします。

Syslog メッセージの送信

OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

手順

ステップ1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ2 [Process Instances] タブをクリックします。

ステップ3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

[Adjacency Changes] 領域では、OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するための設定を変更することができます。[Adjacency Changes] 領域で、次の手順を実行します。

- OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するには、[Log Adjacency Changes] チェックボックスをオンにします。
- OSPFv3 ネイバーが起動または停止したときだけでなく、各状態の syslog メッセージを送信するには、[Include Details] チェックボックスをオンにします。

ステップ4 [OK] をクリックします。

ステップ5 [Apply] をクリックして変更内容を保存します。

Syslog メッセージの抑止

ルータがサポートされていない LSA タイプ 6 Multicast OSPF (MOSPF) パケットを受信した場合の syslog メッセージの送信を抑止するには、次の手順を実行します。

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup]** の順に選択します。
- ステップ 2 **[Process Instances]** タブをクリックします。
- ステップ 3 編集する OSPFv3 プロセスを選択してから **[Advanced]** をクリックします。
[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。
- ステップ 4 **[Ignore LSA MOSPF]** チェックボックスをオンにして、**[OK]** をクリックします。

集約ルートコストの計算

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup]** の順に選択します。
- ステップ 2 **[Process Instances]** タブをクリックします。
- ステップ 3 編集する OSPF プロセスを選択してから **[Advanced]** をクリックします。
[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。
- ステップ 4 **[RFC1583 Compatible]** チェックボックスをオンにして、**[OK]** をクリックします。

OSPFv3 ルーティング ドメインへのデフォルトの外部ルートの生成

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup]** の順に選択します。
- ステップ 2 **[Process Instances]** タブをクリックします。
- ステップ 3 編集する OSPFv3 プロセスを選択してから **[Advanced]** をクリックします。
[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Default Information Originate Area] で、次の手順を実行します。

- a) [Enable] チェックボックスをオンにして、OSPFv3 ルーティング プロセスをイネーブルにします。
- b) [Always advertise] チェックボックスをオンにして、出口が 1 つであるかどうかにかかわらず、常時デフォルト ルートをアドバタイズします。
- c) デフォルト ルートの生成に使用するメトリックを [Metric] フィールドに入力します。有効なメトリック値の範囲は、0 ~ 16777214 です。デフォルト値は 10 です。
- d) [Metric Type] ドロップダウン リストは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。有効な値は次のとおりです。

- 1 : タイプ 1 外部ルート
- 2 : タイプ 2 外部ルート

デフォルトはタイプ 2 外部ルートです。

- e) [Route Map] ドロップダウン リストから、ルート マップが満たされている場合に、デフォルト ルートを生成するルーティング プロセスを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

IPv6 サマリー プレフィックスの設定

手順

ステップ 1 ASDM のメイン ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Summary Prefix] の順に選択します。

ステップ 2 新しいサマリープレフィックスを追加するには、[Add] をクリックします。既存のサマリープレフィックスを適用するには、[Edit] をクリックします。サマリープレフィックスを削除するには、[Delete] をクリックします。

[Add Summary Prefix] ダイアログボックスまたは [Edit Summary Prefix] ダイアログボックスが表示されます。

ステップ 3 [Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4 [IPv6 Prefix/Prefix Length] フィールドに IPv6 プレフィックスとプレフィックス長を入力します。

ステップ 5 [Advertise] チェックボックスをオンにして、指定したプレフィックスとマスクのペアに一致するルートをアドバタイズします。このチェックボックスをオフにすると、指定されたプレフィックスとマスク ペアと一致するルートが抑制されます。

ステップ 6 ルートマップを使用して再配布を制御するように照合値として使用できるタグ値を [Tag] フィールドに入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックして変更内容を保存します。

IPv6 ルートの再配布

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Redistribution]** の順に選択します。
- ステップ 2 OSPFv3 プロセスに接続済みルートを再配布するための新しいパラメータを追加するには、**[Add]** をクリックします。OSPFv3 プロセスに接続済みルートを再配布するための既存のパラメータを変更するには、**[Edit]** をクリックします。パラメータの選択したセットを削除するには **[Delete]** をクリックします。
- [Add Redistribution] ダイアログボックスまたは [Edit Redistribution] ダイアログボックスが表示されます。
- ステップ 3 [Process ID] ドロップダウン リストからプロセス ID を選択します。
- ステップ 4 [Source Protocol] ドロップダウン リストから、ルートが再配布されるソース プロトコルを選択します。サポートされるプロトコルは、接続済み、スタティック、OSPF です。
- ステップ 5 [Metric] フィールドにメトリック値を入力します。同じルータ上の一方の OSPF プロセスから他方の OSPF プロセスにルートを再配布する場合、メトリック値を指定しないと、メトリックは一方のプロセスから他方のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
- ステップ 6 [Metric Type] ドロップダウン リストからメトリック タイプを選択します。使用可能なオプションは、[None]、[1]、[2] です。
- ステップ 7 (オプション) [Tag] フィールドにタグ値を入力します。このパラメータは、ASBR 間で情報の転送に使用される可能性のある各外部ルートに付加される 32 ビットの 10 進数値を指定します。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は、0 ~ 4294967295 です。
- ステップ 8 [Route Map] ドロップダウン リストからルート マップを選択して、ソースルーティング プロトコルから現在のルーティングプロトコルへのルートのインポートのフィルタリングをオンにします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。
- ステップ 9 再配布に接続済みルートを含めるには、**[Include Connected]** チェックボックスをオンにします。
- ステップ 10 [Match] チェックボックスをオンにして他のルーティング ドメインへのルートを再配布し、次のチェックボックスの 1 つをオンにします。
- [Internal] は、特定の自律システムの内部にあるルートです。
 - [External 1] は、自律システムの外部ながら、OSPFv3 にタイプ 1 外部ルートとしてインポートされるルートです。

- [External 2] は、自律システムの外部ながら、OSPFv3 にタイプ 2 外部ルートとしてインポートされるルートです。
- [NSSA External 1] は、自律システムの外部ながら、IPv6 用の NSSA の OSPFv3 にタイプ 1 の外部ルートとしてインポートされるルートです。
- [NSSA External 2] は、自律システムの外部ながら、IPv6 用の NSSA の OSPFv3 にタイプ 2 の外部ルートとしてインポートされるルートです。

ステップ 11 [OK] をクリックします。

ステップ 12 [Apply] をクリックして変更内容を保存します。

グレースフル リスタートの設定

ASA では、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding (NSF) 機能では、ルーティングプロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、コンポーネントに障害がある場合（フェールオーバー（HA）モードで処理を引き継ぐスタンバイユニットが存在するアクティブユニットがクラッシュした場合や、クラスタモードで新しいマスターとして選択されたスレーブユニットが存在するマスターユニットがクラッシュした場合など）、またはスケジュールされたヒットレスソフトウェア アップグレードがある場合に役立ちます。

グレースフル リスタートは、OSPFv2 と OSPFv3 の両方でサポートされています。NSF Cisco (RFC 4811 および RFC 4812) または NSF IETF (RFC 3623) のいずれかを使用して、OSPFv2 上でグレースフルリスタートを設定できます。graceful-restart (RFC 5187) を使用して、OSPFv3 上でグレースフルリスタートを設定できます。

NSF グレースフルリスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタートアクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel (L2) クラスタモードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステートアドバタイズメント (LSA) /リンクローカルシングナリング (LLS) ブロックの機能を使って設定する必要があります。



- (注) OSPFv2 用に fast hello が設定されている場合、アクティブユニットのリロードが発生し、スタンバイユニットがアクティブになっても、グレースフルリスタートは発生しません。これは、ロール変更にかかる時間は、設定されているデッドインターバルよりも大きいからです。

OSPFv2 のグレースフル リスタートの設定

OSPFv2、Cisco NSF および IETF NSF には、2つのグレースフルリスタートメカニズムがあります。OSPF インスタンスに対しては、これらのグレースフルリスタートメカニズムのうち一度に設定できるのは1つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスは OSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

OSPFv2 の Cisco NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフルリスタートを設定します。

手順

- ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。
- ステップ 2 [Configuring Cisco NSF] の下で、[Enable Cisco nonstop forwarding (NSF)] チェックボックスをオンにします。
- ステップ 3 (オプション) 必要に応じて、[Cancels NSF restart when non-NSF-aware neighboring networking devices are detected] チェックボックスをオンにします。
- ステップ 4 (オプション) [Configuring Cisco NSF helper] の下で、[Enable Cisco nonstop forwarding (NSF) for helper mode] チェックボックスをオフにします。

- (注) このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスで Cisco NSF ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

- ステップ 5 [OK] をクリックします。
- ステップ 6 [Apply] をクリックして変更内容を保存します。

OSPFv2 の IETF NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフルリスタートを設定します。

手順

-
- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。
- ステップ 2** [Configuring IETF NSF] で、[Enable IETF nonstop forwarding (NSF)] チェックボックスをオンにします。
- ステップ 3** (オプション) [Length of graceful restart interval] フィールドに、リスタート間隔を秒単位で入力します。
- (注) デフォルト値は 120 秒です。30 秒以下のリスタート間隔の場合、グレースフル リスタートは終了します。
- ステップ 4** (オプション) [Configuring IETF NSF helper] で、[Enable IETF nonstop forwarding (NSF) for helper mode] チェックボックスをオフにします。
- このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスで IETF NSF ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。
- ステップ 5** [OK] をクリックします。
- ステップ 6** [Apply] をクリックして変更内容を保存します。
-

OSPFv3 のグレースフル リスタートの設定

OSPFv3 の NSF グレースフル リスタート機能を設定するには、2 つのステップを伴います。NSF 対応としてのデバイスの設定と、NSF 認識としてのデバイスの設定です。

手順

-
- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。
- ステップ 2** [Configuring Graceful Restart] の下で、[Enable Graceful Restart] チェックボックスをオンにします。
- ステップ 3** (オプション) [Restart Interval] フィールドにリスタート間隔の値を入力します。
- (注) デフォルト値は 120 秒です。30 秒以下のリスタート間隔の場合、グレースフル リスタートは終了します。
- ステップ 4** [Configuring Graceful Restart Helper] の下で、[Enable Graceful Restart Helper] チェックボックスをオンにします。
- このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスでグレースフル リスタート ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5 (オプション) [Enable LSA checking] チェックボックスをオンにして、厳密なリンク ステート アドバタイズメント チェックをイネーブルにします。

イネーブルにすると、再起動ルータにフラッシュされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックして変更内容を保存します。

OSPFv2 設定の削除

OSPFv2 設定を削除します。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2 [Enable this OSPF Process] チェックボックスをオフにします。

ステップ 3 [Apply] をクリックします。

OSPFv3 設定の削除

OSPFv3 設定を削除します。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2 [Enable OSPFv3 Process] チェックボックスをオフにします。

ステップ 3 [Apply] をクリックします。

OSPFv2 の例

次の例に、さまざまなオプションのプロセスを使用して OSPFv2 をイネーブルにし、設定する方法を示します。

1. メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup]** の順に選択します。
2. [Process Instances] タブをクリックし、[OSPF Process 1] フィールドに **2** と入力します。
3. [Area/Networks] タブをクリックし、[Add] をクリックします。
4. [Area ID] フィールドに **0** と入力します。
5. [Area Networks] 領域の [IP Address] フィールドに **10.0.0.0** と入力します。
6. [Netmask] ドロップダウン リストで [255.0.0.0] を選択します。
7. [OK] をクリックします。
8. メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution]** の順に選択します。
9. [Add] をクリックします。
[Add/Edit OSPF Redistribution Entry] ダイアログボックスが表示されます。
10. [Protocol] 領域の [OSPF] オプション ボタンをクリックして、ルートが再配布されるソース プロトコルを指定します。[OSPF] を選択すると、別の OSPF ルーティング プロセスからのルートが再配布されるようになります。
11. OSPF プロセス ID を [OSPF Process] ドロップダウン リストで選択します。
12. [Match] 領域の [Internal] チェックボックスをオンにします。
13. [Metric Value] フィールドに、再配布されるルーティングのメトリック値として **5** を入力します。
14. [Metric Type] ドロップダウン リストで、メトリック タイプの値として **1** を選択します。
15. [Route Map] ドロップダウン リストで、**1** を選択します。
16. [OK] をクリックします。
17. メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Interface]** の順に選択します。
18. [Properties] タブで、[inside] インターフェイスを選択して [Edit] をクリックします。
[Edit OSPF Properties] ダイアログボックスが表示されます。
19. [Cost] フィールドに **20** と入力します。
20. [Advanced] をクリックします。
21. [Retransmit Interval] フィールドに **15** と入力します。
22. [Transmit Delay] フィールドに **20** と入力します。
23. [Hello Interval] フィールドに **10** と入力します。
24. [Dead Interval] フィールドに **40** と入力します。

25. [OK] をクリックします。
26. [Edit OSPF Properties] ダイアログボックスで、[Priorities] フィールドに **20** と入力して [OK] をクリックします。
27. [Authentication] タブをクリックします。
[Edit OSPF Authentication] ダイアログボックスが表示されます。
28. [Authentication] 領域の [MD5] オプション ボタンをクリックします。
29. [MD5 and Key ID] 領域の [MD5 Key] フィールドに **cisco** と入力し、[MD5 Key ID] フィールドに **1** と入力します。
30. [OK] をクリックします。
31. **[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup]** を選択し、[Area/Networks] タブをクリックします。
32. [OSPF 2] プロセスを選択し、[Edit] を選択します。
[Edit OSPF Area] ダイアログボックスが表示されます。
33. [Area Type] 領域で、[Stub] を選択します。
34. [Authentication] 領域で、[None] を選択し、[Default Cost] フィールドに **20** と入力します。
35. [OK] をクリックします。
36. メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup]** の順に選択します。
37. [Process Instances] タブをクリックし、[OSPF process 2] チェックボックスをオンにします。
38. [Advanced] をクリックします。
[Edit OSPF Area] ダイアログボックスが表示されます。
39. [Timers] 領域で、[SPF Delay Time] フィールドに **10** と入力し、[SPF Hold Time] フィールドに **20** と入力します。
40. [Adjacency Changes] 領域の [Log Adjacency Change Details] チェックボックスをオンにします。
41. [OK] をクリックします。
42. [リセット (Reset)] をクリックします。

OSPFv3 の例

次に、ASDM で OSPFv3 ルーティングを設定する例を示します。

1. メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup]** の順に選択します。
2. [Process Instances] タブで、次の手順を実行します。
 1. [Enable OSPFv3 Process] チェックボックスをオンにします。
 2. [Process ID] フィールドに **1** を入力します。
3. [Areas] タブをクリックし、続いて [Add] をクリックして、[Add OSPFv3 Area] ダイアログボックスを表示します。
4. [OSPFv3 Process ID] ドロップダウン リストから、**1** を選択します。
5. [Area ID] フィールドに **22** と入力します。
6. [Area Type] ドロップダウン リストから [Normal] を選択します。
7. [Default Cost] フィールドに **10** を入力します。
8. [Redistribution imports routes to normal and NSSA areas] をオンにします。
9. [Metric] フィールドに **20** を入力します。
10. [Metric Type] ドロップダウン リストから **1** を選択します。
11. 使用されているインターフェイスの指定に合わせて、**内部**チェックボックスをオンにします。
12. [Enable Authentication] チェックボックスをオンにします。
13. [Security Policy Index] フィールドに **300** を入力します。
14. [Authentication Algorithm] ドロップダウン リストから [SHA-1] を選択します。
15. [Authentication Key] フィールドに **12345ABCDE** を入力します。
16. [Encryption Algorithm] ドロップダウン リストから [DES] を選択します。
17. [Encryption Key] フィールドに **1122334455aabbccdde** を入力します。
18. [OK] をクリックします。
19. [Route Summarization] タブをクリックし、続いて [Add] をクリックして、[Add Route Summarization] ダイアログボックスを表示します。
20. [Process ID] ドロップダウン リストから **1** を選択します。
21. [Area ID] ドロップダウン リストから **22** を選択します。
22. [IPv6 Prefix/Prefix Length] フィールドに **2000:122::/64** を入力します。
23. (オプション) [Cost] フィールドに **100** を入力します。
24. [Advertised] チェックボックスをオンにします。

25. [OK] をクリックします。
26. メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Interface] の順に選択します。
27. [Properties] タブをクリックします。
28. 内部チェックボックスをオンにし、[Edit] をクリックして、[Edit OSPF Properties] ダイアログボックスを表示します。
29. [Cost] フィールドに **20** と入力します。
30. [Priority] フィールドに **1** を入力します。
31. [Point-to-Point] チェックボックスをオンにします。
32. [Dead Interval] フィールドに **40** と入力します。
33. [Hello Interval] フィールドに **10** と入力します。
34. [Retransmit Interval] フィールドに **15** と入力します。
35. [Transmit Delay] フィールドに **20** と入力します。
36. [OK] をクリックします。
37. メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Redistribution] の順に選択します。
38. [Process ID] ドロップダウン リストから **1** を選択します。
39. [Source Protocol] ドロップダウン リストから [OSPF] を選択します。
40. [Metric] フィールドに **50** を入力します。
41. [Metric Type] ドロップダウン リストから **1** を選択します。
42. [OK] をクリックします。
43. [Apply] をクリックして変更内容を保存します。

OSPF のモニタリング

IP ルーティング テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示できます。提供される情報は、リソースの使用状況を判定してネットワークの問題を解決するために使用することもできます。また、ノードの到達可能性情報を表示して、デバイス パケットがネットワークを通過するときにとるルーティングパスを見つけることもできます。

OSPFv2 ルーティングのさまざまな統計情報を ASDM でモニタまたは表示するには、次の手順を実行します。

1. メイン ASDM ウィンドウで、[Monitoring] > [Routing] > [OSPF LSAs] の順に選択します。

2. 選択してモニタできる OSPF LSA は、タイプ 1～5 と 7 です。各ペインには、次のように 1 つの LSA タイプが表示されます。
 - [Type 1 LSAs] は、特定のエリア内の特定プロセス下にあるすべてのルートを表します。
 - [Type 2 LSAs] には、ルータをアドバタイズする指定ルータの IP アドレスが表示されます。
 - [Type 3 LSAs] には、宛先ネットワークの IP アドレスが表示されます。
 - [Type 4 LSAs] には、AS 境界ルータの IP アドレスが表示されます。
 - [Type 5 LSAs] と [Type 7 LSAs] には、AS 外部ネットワークの IP アドレスが表示されます。

3. [Refresh] をクリックすると、各 LSA タイプのペインが更新されます。
4. メイン ASDM ウィンドウで、[Monitoring] > [Routing] > [OSPF Neighbors] の順に選択します。

[OSPF Neighbors] ペインの各行は 1 つの OSPF ネイバーを表します。さらに、[OSPF Neighbors] ペインにはそのネイバーが実行されているネットワーク、優先度、状態、デッド時間（秒単位）、ネイバーの IP アドレス、および実行されているインターフェイスも表示されます。OSPF ネイバーが取る可能性のある状態の一覧については、RFC 2328 を参照してください。

5. [Refresh] をクリックすると、[OSPF Neighbors] ペインが更新されます。

OSPFv3 ルーティングのさまざまな統計情報を ASDM でモニタまたは表示するには、次の手順を実行します。

1. メイン ASDM ウィンドウで、[Monitoring] > [Routing] > [OSPFv3 LSAs] の順に選択します。
2. OSPFv3 LSA を選択し、モニタすることができます。[Link State type] ドロップダウンリストでリンク ステートタイプを選択し、指定されたパラメータに従って状態を表示します。サポートされるリンク ステートタイプは、ルータ、ネットワーク、エリア間プレフィックス、エリア間ルータ、AS エクスターナル、NSSA、リンク、エリア内プレフィックスです。
3. [Refresh] をクリックして、各リンク ステートタイプを更新します。
4. メイン ASDM ウィンドウで、[Monitoring] > [Routing] > [OSPFv3 Neighbors] の順に選択します。

[OSPFv3 Neighbors] ペインの各行は 1 つの OSPFv3 ネイバーを表します。さらに、[OSPFv3 Neighbors] ペインには、ネイバーの IP アドレス、優先度、状態、秒単位のデッドタイム量、動作中のインターフェイスが表示されます。OSPFv3 ネイバーが取る可能性のある状態の一覧については、RFC 5340 を参照してください。

5. [Refresh] をクリックすると、[OSPFv3 Neighbors] ペインが更新されます。

OSPF の履歴

表 31: OSPF の機能履歴

機能名	プラットフォーム リリース	機能情報
OSPF サポート	7.0(1)	Open Shortest Path First (OSPF) ルーティングプロトコルを使用した、データのルーティング、認証、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [OSPF]。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	OSPFv2 ルーティングは、マルチ コンテキスト モードでサポートされます。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup]
クラスタ	9.0(1)	OSPFv2 および OSPFv3 の場合、パルク同期、ルートの同期およびスパンド EtherChannel ロード バランシングは、クラスタリング環境でサポートされます。
IPv6 の OSPFv3 サポート	9.0(1)	OSPFv3 ルーティングが IPv6 に対してサポートされます。 次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup]、 [Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Interface]、 [Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Redistribution]、 [Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Summary Prefix]、 [Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Virtual Link]、 [Monitoring] > [Routing] > [OSPFv3 LSAs]、 [Monitoring] > [Routing] > [OSPFv3 Neighbors]。

機能名	プラットフォーム リリース	機能情報
Fast Hello に対する OSPF サポート	9.2(1)	OSPF は、Fast Hello パケット機能をサポートしているため、OSPF ネットワークでのコンバージェンスが高速なコンフィギュレーションになります。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Interface] > [Edit OSPF Interface Advanced Properties]
タイマー	9.2(1)	新しい OSPF タイマーを追加し、古いタイマーを廃止しました。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Edit OSPF Process Advanced Properties]
アクセスリストを使用したルートフィルタリング	9.2(1)	ACL を使用したルート フィルタリングがサポートされるようになりました。 次の画面が追加されました。 [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Filtering Rules] > [Add Filter Rules]
OSPF モニタリングの強化	9.2(1)	OSPF モニタリングの詳細情報が追加されました。
OSPF 再配布 BGP	9.2(1)	OSPF 再配布機能が追加されました。 次の画面が追加されました。 [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution]
ノンストップ フォワーディング (NSF) に対する OSPF のサポート	9.3(1)	NSF に対する OSPFv2 および OSPFv3 のサポートが追加されました。 次の画面が追加されました。 [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [NSF Properties]、 [Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > [NSF Properties]

機能名	プラットフォーム リリース	機能情報
		<p>NSF 待機タイマーが追加されました。</p> <p>NSF 再起動間隔のタイマーを設定するための新しいコマンドが追加されました。このコマンドが導入され、待機間隔がルータの dead 間隔よりも長くならないようになりました。</p> <p>次のコマンドが導入されました。</p> <p>timers nsf wait <seconds></p>



第 30 章

EIGRP

この章では、Enhanced Interior Gateway Routing Protocol (EIGRP) を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Cisco ASA を設定する方法について説明します。

- [EIGRP について \(775 ページ\)](#)
- [EIGRP のガイドライン \(777 ページ\)](#)
- [EIGRP プロセスの設定 \(777 ページ\)](#)
- [EIGRP の設定 \(778 ページ\)](#)
- [EIGRP のカスタマイズ \(781 ページ\)](#)
- [EIGRP のモニタリング \(796 ページ\)](#)
- [EIGRP の履歴 \(797 ページ\)](#)

EIGRP について

EIGRP は、シスコが開発した、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルートアップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。EIGRP を他のルーティング プロトコルと区別する主な機能には、迅速なコンバージェンス、可変長サブネットマスクのサポート、部分的アップデートのサポート、複数のネットワーク レイヤ プロトコルのサポートなどがあります。

EIGRP を実行するルータでは、すべてのネイバー ルーティング テーブルが格納されているため、代替ルートに迅速に適応できます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリーは、代替ルートが検出されるまで伝搬します。EIGRP では可変長サブネットマスクがサポートされているため、ルートはネットワーク番号の境界で自動的に集約されます。さらに、任意のインターフェイスの任意のビット境界で集約を行うように EIGRP を設定することもできます。EIGRP は定期的なアップデートを行いません。その代わりに、ルートのメトリックが変更されたときだけ、部分的なアップデートを送信します。部分的アップデートの伝搬では、境界が自動的に設定されるため、その情報を必要とするルータだけがアップデートされます。これらの 2 つの機能により、EIGRP の帯域幅消費量は IGRP に比べて大幅に減少します。

ネイバー探索は、ASA が直接接続されているネットワーク上にある他のルータをダイナミックに把握するために使用するプロセスです。EIGRP ルータは、マルチキャスト hello パケットを送信して、ネットワーク上に自分が存在していることを通知します。ASA は、新しいネイバーから hello パケットを受信すると、トポロジテーブルに初期化ビットを設定してそのネイバーに送信します。ネイバーは、初期化ビットが設定されたトポロジアップデートを受信すると、自分のトポロジテーブルを ASA に返送します。

hello パケットはマルチキャストメッセージとして送信されます。hello メッセージへの応答は想定されていません。ただし、スタティックに定義されたネイバーの場合は例外です。neighbor コマンドを使用して（または ASDM で [Hello Interval] を設定して）ネイバーを設定すると、そのネイバーへ送信される hello メッセージはユニキャストメッセージとして送信されます。ルーティングアップデートと確認応答が、ユニキャストメッセージとして送信されます。

このネイバー関係が確立した後は、ネットワークトポロジが変更された場合にだけ、ルーティングアップデートが交換されます。ネイバー関係は、hello パケットによって維持されます。ネイバーから受信した各 hello パケットには、保持時間が含まれています。ASA は、この時間内にそのネイバーから hello パケットを受信すると想定できます。ASA が保持時間内にそのネイバーからアドバタイズされた hello パケットを受信しない場合、ASA はそのネイバーを使用不能と見なします。

EIGRP プロトコルは、ネイバーの検出、ネイバーの回復、Reliable Transport Protocol (RTP)、およびルート計算に重要な DUAL を含む、4 の主要なアルゴリズムテクノロジーと 4 つの主要なテクノロジーを使用します。DUAL は、最小コストのルートだけでなく、宛先へのすべてのルートをとポロジテーブルに保存します。最小コストのルートはルーティングテーブルに挿入されます。その他のルートは、トポロジテーブルに残ります。メインのルートに障害が発生したら、フィジブルサクセサから別のルートが選択されます。サクセサとは、宛先への最小コストパスを持ち、パケット転送に使用される隣接ルータです。フィジビリティ計算によって、パスがルーティングループを形成しないことが保証されます。

フィジブルサクセサがトポロジテーブル内にない場合、必ずルート計算が発生します。ルートの再計算中、DUAL は EIGRP ネイバーにルートを求めるクエリーを送信して、次に EIGRP ネイバーがそのネイバーにクエリーを送信します。ルートのフィジブルサクセサがないルータは、到達不能メッセージを返します。

ルートの再計算中、DUAL は、ルートをアクティブとマークします。デフォルトでは、ASA は、ネイバーから応答が返ってくるのを 3 分間待ちます。ASA がネイバーから応答を受信しないと、そのルートは stuck-in-active とマークされます。トポロジテーブル内のルートのうち、応答しないネイバーをフィジブルサクセサとして指しているものはすべて削除されます。



(注) EIGRP ネイバー関係では、GRE トンネルを使用しない IPsec トンネルの通過はサポートされていません。

EIGRP のガイドライン

ファイアウォールモードのガイドライン

ルーテッドファイアウォールモードでだけサポートされています。トランスペアレントファイアウォールモードはサポートされません。

クラスタのガイドライン

EIGRP は、個別のインターフェイスモードのクラスタピアとのネイバー関係を形成しません。

IPv6 のガイドライン

IPv6 はサポートされません。

コンテキストのガイドライン

- デフォルトでは、共有インターフェイス間でのマルチキャストトラフィックのコンテキスト間交換がサポートされていないため、EIGRP インスタンスは共有インターフェイス間で相互に隣接関係を形成できません。ただし、EIGRP プロセスの EIGRP プロセス設定で静的ネイバー設定を使用すると、共有インターフェイスでの EIGRP ネイバーシップを形成できます。
- 個別のインターフェイスでのコンテキスト間 EIGRP がサポートされています。

その他のガイドライン

- 最大 1 つの EIGRP プロセスがサポートされます。
- 設定の変更が適用されるたびに、EIGRP 隣接関係のフラップが発生し、特に配布リスト、オフセットリスト、および集約への変更のネイバーからの（送信または受信された）ルーティング情報が変更されます。ルータが同期されると、EIGRP はネイバー間の隣接関係を再確立します。隣接関係が壊れて再確立されると、ネイバー間で学習されたすべてのルートが消去され、新しい配布リストを使用して、ネイバー間の同期がすべて新しく実行されます。

EIGRP プロセスの設定

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [EIGRP]** の順に選択します。

- ステップ 2** EIGRP ルーティング プロセスをイネーブルにするには、[Process Instances] タブの [Enable this EIGRP process] チェックボックスをオンにします。[EIGRP のイネーブル化 \(778 ページ\)](#) または [EIGRP スタブ ルーティングのイネーブル化 \(780 ページ\)](#) を参照してください。
- ステップ 3** [Setup] > [Networks] タブで、EIGRP ルーティングに参加するネットワークとインターフェイスを定義します。詳細については、「[EIGRP ルーティングプロセスのネットワークの定義 \(781 ページ\)](#)」を参照してください。
- ステップ 4** (任意) [Filter Rules] ペインでルート フィルタを定義します。ルート フィルタにより、EIGRP 更新で送受信することを許可されているルートをより細かく制御できます。詳細については、「[EIGRP でのネットワークのフィルタリング \(790 ページ\)](#)」を参照してください。
- ステップ 5** (任意) [Redistribution] ペインでルート再配布を定義します。
- RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。詳細については、「[EIGRP へのルート再配布 \(788 ページ\)](#)」を参照してください。
- ステップ 6** (任意) [Static Neighbor] ペインでスタティック EIGRP ネイバーを定義します。詳細については、「[EIGRP ネイバーの定義 \(787 ページ\)](#)」を参照してください。
- ステップ 7** (任意) [Summary Address] ペインで、サマリー アドレスを定義します。
- サマリーアドレスの定義の詳細については、[インターフェイスでのサマリー集約アドレスの設定 \(784 ページ\)](#) を参照してください。
- ステップ 8** (任意) [Interfaces] ペインで、インターフェイス固有の EIGRP パラメータを定義します。これらのパラメータには、EIGRP メッセージ認証、保持時間、hello 間隔、遅延メトリック、スプリットホライズンの使用などがあります。詳細については、「[EIGRP のインターフェイスの設定 \(782 ページ\)](#)」を参照してください。
- ステップ 9** (任意) [Default Information] ペインで、EIGRP 更新でのデフォルト ルート情報の送受信を制御します。デフォルトでは、デフォルトルートが送信され、受け入れられます。詳細については、「[EIGRP でのデフォルト情報の設定 \(793 ページ\)](#)」を参照してください。

EIGRP の設定

この項では、システムで EIGRP プロセスをイネーブルにする方法について説明します。EIGRP をイネーブルにした後に、システムで EIGRP プロセスをカスタマイズする方法については、次の項を参照してください。

EIGRP のイネーブル化

ASA でイネーブルにすることができる EIGRP ルーティング プロセスは 1 つだけです。

手順

- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup]** の順に選択します。
- [EIGRP Setup] ペインが表示されます。
- メインの [EIGRP Setup] ペインには、EIGRP をイネーブルにするための次の 3 つのタブがあります。
- [Process Instances] タブでは、各コンテキストの EIGRP ルーティング プロセスをイネーブルにすることができます。シングル コンテキスト モードおよびマルチ コンテキスト モードの両方がサポートされます。詳細については、[EIGRP のイネーブル化 \(778 ページ\)](#) と [EIGRP スタブルーティングのイネーブル化 \(780 ページ\)](#) を参照してください。
 - [Networks] タブでは、EIGRP ルーティングプロセスで使用されるネットワークを指定できます。EIGRP ルーティングに参加するインターフェイスは、これらのネットワーク エントリで定義されるアドレスの範囲内に存在する必要があります。アドバタイズされる直接接続およびスタティックのネットワークも、これらのネットワーク エントリの範囲内である必要があります。詳細については、「[EIGRP ルーティング プロセスのネットワークの定義 \(781 ページ\)](#)」を参照してください。
 - [Passive Interfaces] タブでは、1 つ以上のインターフェイスをパッシブインターフェイスとして設定できます。EIGRP では、パッシブ インターフェイスはルーティングアップデートの送受信を行いません。[Passive Interface] テーブルには、パッシブ インターフェイスとして定義されているインターフェイスが一覧表示されます。
- ステップ 2** [Enable this EIGRP process] チェックボックスをオンにします。
- デバイスでイネーブルにすることができる EIGRP ルーティング プロセスは 1 つだけです。変更を保存できるようにするには、ルーティングプロセスの自律システム (AS) 番号を [EIGRP Process] フィールドに入力する必要があります。
- ステップ 3** [EIGRP Process] フィールドに、EIGRP プロセスの自律システム (AS) 番号を入力します。指定できる AS 番号の範囲は 1 ~ 65535 です。
- ステップ 4** (任意) EIGRP プロセスの設定を指定するには、[Advanced] をクリックします。指定できる設定には、ルータ ID、デフォルトのメトリック、スタブルーティング、ネイバー変更、EIGRP ルートのアドミニストレーティブ ディスタンスなどがあります。
- ステップ 5** [Networks] タブをクリックします。
- ステップ 6** 新しいネットワーク エントリを追加するには、[Add] をクリックします。
- [Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択して [Delete] をクリックします。
- ステップ 7** ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。
- ステップ 8** [IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

(注) ネットワークエントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 9 [Network Mask] フィールドに、IP アドレスに適用するネットワーク マスクを入力します。

ステップ 10 [OK] をクリックします。

EIGRP スタブルルーティングのイネーブル化

ASA を EIGRP スタブルータとしてイネーブル化し、設定することができます。スタブルルーティングを使用すると、ASA で必要となるメモリおよび処理要件を減らすことができます。ASA をスタブルータとして設定すると、ローカル以外のトラフィックがすべて配布ルータに転送されるようになり、完全な EIGRP ルーティングテーブルを維持する必要がなくなります。一般に、配布ルータからスタブルートに送信する必要があるのは、デフォルトルートだけです。

スタブルータから配布ルータには、指定されたルートだけが伝搬されます。スタブルータである ASA は、サマリー、接続されているルート、再配布されたスタティックルート、外部ルート、および内部ルートに対するクエリーすべてに、応答として「inaccessible」というメッセージを返します。ASA がスタブとして設定されているときは、自身のスタブルータとしてのステータスを報告するために、特殊なピア情報パケットをすべての隣接ルータに送信します。スタブステータスの情報を伝えるパケットを受信したネイバーはすべて、スタブルータにルートのクエリーを送信しなくなり、スタブピアを持つルータはそのピアのクエリーを送信しなくなります。スタブルータが正しいアップデートをすべてのピアに送信するには、配布ルータが必要です。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの自律システム (AS) 番号を入力します。指定できる AS 番号の範囲は 1 ~ 65535 です。

ステップ 4 EIGRP スタブルルーティング プロセスを設定するには、[Advanced] をクリックします。

[Edit EIGRP Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 5 [Edit EIGRP Process Advanced Properties] ダイアログボックスの [Stub] 領域で、次の EIGRP スタブルルーティング プロセスのうち 1 つ以上を選択します。

- [Stub Receive only] : 隣接ルータからルート情報を受信しても、それらの隣接ルータにルート情報を送信しない EIGRP スタブルルーティング プロセスを設定します。このオプションを選択する場合は、他のスタブルルーティング オプションを選択できません。

- [Stub Connected] : 接続済みルートアドバタイズします。
- [Stub Static] : スタティック ルートアドバタイズします。
- [Stub Redistributed] : 再配布ルートアドバタイズします。
- [Stub Summary] : サマリー ルートアドバタイズします。

ステップ 6 [OK] をクリックします。

ステップ 7 [Networks] タブをクリックします。

ステップ 8 [Add] をクリックして、新しいネットワーク エントリを追加します。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

ステップ 9 ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 10 [IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

(注) ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 11 [Network Mask] フィールドに、IP アドレスに適用するネットワーク マスクを入力します。

ステップ 12 [OK] をクリックします。

EIGRP のカスタマイズ

ここでは、EIGRP ルーティングをカスタマイズする方法について説明します。

EIGRP ルーティング プロセスのネットワークの定義

[Network] テーブルでは、EIGRP ルーティング プロセスで使用されるネットワークを指定できます。EIGRP ルーティングに参加するインターフェイスは、これらのネットワーク エントリで定義されるアドレスの範囲内に存在する必要があります。アドバタイズされる直接接続およびスタティックのネットワークも、これらのネットワーク エントリの範囲内である必要があります。

[Network] テーブルには、EIGRP ルーティング プロセス用に設定されているネットワークが表示されます。このテーブルの各行には、指定した EIGRP ルーティング プロセス用に設定されているネットワーク アドレスおよび関連するマスクが表示されます。

手順

- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup]** の順に選択します。
- [EIGRP Setup] ペインが表示されます。
- ステップ 2** [Enable EIGRP routing] チェックボックスをオンにします。
- ステップ 3** [EIGRP Process] フィールドに、EIGRP プロセスの自律システム (AS) 番号を入力します。指定できる AS 番号の範囲は 1 ~ 65535 です。
- ステップ 4** [Networks] タブをクリックします。
- ステップ 5** [Add] をクリックして、新しいネットワーク エントリを追加します。
- [Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。
- ステップ 6** ドロップダウンリストから、EIGRP ルーティング プロセスの AS 番号を選択します。
- ステップ 7** [IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。
- (注) ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。
- ステップ 8** [Network Mask] フィールドに、IP アドレスに適用するネットワーク マスクを入力します。
- ステップ 9** [OK] をクリックします。
-

EIGRP のインターフェイスの設定

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、インターフェイスが接続されているネットワークが対象に含まれるように ASA を設定し、そのインターフェイスが EIGRP アップデートを送受信しないようにします。

手順

- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup]** の順に選択します。
- [EIGRP Setup] ペインが表示されます。
- ステップ 2** [Enable EIGRP routing] チェックボックスをオンにします。
- ステップ 3** [OK] をクリックします。
- ステップ 4** **[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces]** の順に選択します。

[Interface] ペインが表示され、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、インターフェイスごとに次の設定を修正できます。

- 認証キーとモード。
- EIGRP hello 間隔と保持時間。
- EIGRP メトリックの計算で使用されるインターフェイス遅延メトリック。
- インターフェイスでのスプリットホライズンの使用。

ステップ 5 インターフェイス エントリを選択するには、インターフェイス エントリをダブルクリックするか、そのエントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 6 [EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ~ 65535 です。

ステップ 7 [Hello Interval] フィールドに、インターフェイス上で送信される EIGRP hello パケット間の間隔を入力します。

有効値の範囲は、1 ~ 65535 秒です。デフォルト値は 5 秒です。

ステップ 8 [Hold Time] フィールドに、保持時間を秒単位で入力します。有効値の範囲は、1 ~ 65535 秒です。デフォルト値は 15 秒です。

ステップ 9 [Split Horizon] の [Enable] チェックボックスをオンにします。

ステップ 10 [Delay] フィールドに、遅延の値を入力します。遅延時間は 10 マイクロ秒単位です。有効値の範囲は 1 ~ 16777215 です。

ステップ 11 [Enable MD5 Authentication] チェックボックスをオンにして、EIGRP プロセス メッセージの MD5 認証をイネーブルにします。

ステップ 12 [Key] または [Key ID] の値を入力します。

- [Key] フィールドに、EIGRP 更新を認証するキーを入力します。このキーには、最大 16 文字を含めることができます。
- [Key ID] フィールドに、キー ID 値を入力します。有効値の範囲は、1 ~ 255 です。

ステップ 13 [OK] をクリックします。

パッシブインターフェイスの設定

1つ以上のインターフェイスを受動インターフェイスとして設定できます。EIGRP の場合、受動インターフェイスではルーティング アップデートが送受信されません。ASDM の [Passive Interface] テーブルには、パッシブインターフェイスとして設定されているインターフェイスが一覧表示されます。

手順

-
- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup]** の順に選択します。
- [EIGRP Setup] ペインが表示されます。
- ステップ 2** [Enable EIGRP routing] チェックボックスをオンにします。
- ステップ 3** [OK] をクリックします。
- ステップ 4** [Passive Interfaces] タブをクリックします。
- ステップ 5** 設定するインターフェイスをドロップダウン リストから選択します。
- ステップ 6** [Suppress routing updates on all interfaces] チェックボックスをオンにすると、すべてのインターフェイスがパッシブとして指定されます。[Passive Interface] テーブルに表示されていないインターフェイスも、このチェックボックスがオンのときはパッシブとして設定されます。
- ステップ 7** パッシブ インターフェイス エントリを追加するには [Add] をクリックします。
- [Add EIGRP Passive Interface] ダイアログボックスが表示されます。パッシブにするインターフェイスを選択して [Add] をクリックします。パッシブ インターフェイスを削除するには、テーブルでそのインターフェイスを選択して [Delete] をクリックします。
- ステップ 8** [OK] をクリックします。
-

インターフェイスでのサマリー集約アドレスの設定

サマリーアドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリーアドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリーアドレスを使用する場合は、手動でサマリーアドレスを定義する必要があります。ルーティング テーブルに他にも個別のルートがある場合、EIGRP は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。

手順

-
- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces]** の順に選択します。
- [Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、設定をインターフェイスごとに修正できます。これらの設定の詳細については、[EIGRP のインターフェイスの設定 \(782 ページ\)](#) を参照してください。
- ステップ 2** インターフェイスの EIGRP パラメータを設定するには、インターフェイス エントリをダブルクリックするか、そのエントリを選択して [Edit] をクリックします。

- ステップ 3** [OK] をクリックします。
- ステップ 4** [Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Summary Address] の順に選択します。
- [Summary Address] ペインには、スタティックに定義された EIGRP サマリーアドレスのテーブルが表示されます。デフォルトでは、EIGRP はサブネット ルートをネットワーク レベルに集約します。[Summary Address] ペインでは、サブネット レベルに集約されるスタティックに定義された EIGRP サマリーアドレスを作成できます。
- ステップ 5** 新しい EIGRP サマリーアドレスを追加するには [Add] をクリックし、テーブル内の既存の EIGRP サマリーアドレスを編集するには [Edit] をクリックします。
- [Add Summary Address] または [Edit Summary Address] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。
- ステップ 6** [EIGRP Process] フィールドに、EIGRP プロセスの自律システム (AS) 番号を入力します。指定できる AS 番号の範囲は 1 ~ 65535 です。
- ステップ 7** [Interface] ドロップダウンリストで、どのインターフェイスからこのサマリーアドレスをアドバタイズするかを選択します。
- ステップ 8** [IP Address] フィールドに、サマリールートの IP アドレスを入力します。
- ステップ 9** [Netmask] フィールドで、IP アドレスに適用されるネットワーク マスクを選択または入力します。
- ステップ 10** ルートのアドミニストレーティブディスタンスを [Administrative Distance] フィールドに入力します。空白のままにすると、ルートのアドミニストレーティブディスタンスはデフォルト値の 5 になります。
- ステップ 11** [OK] をクリックします。

インターフェイス遅延値の変更

インターフェイス遅延値は、EIGRP ディスタンス計算で使用されます。この値は、インターフェイスごとに変更できます。

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces] の順に選択します。
- [Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、設定をインターフェイスごとに変更できます。これらの設定の詳細については、[EIGRP のインターフェイスの設定 \(782 ページ\)](#) を参照してください。
- ステップ 2** インターフェイスの EIGRP パラメータの遅延値を設定するには、インターフェイス エントリをダブルクリックするか、インターフェイス エントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 3 [Delay] フィールドに、遅延時間を 10 マイクロ秒単位で入力します。有効な値は、1 ~ 16777215 です。

ステップ 4 [OK] をクリックします。

インターフェイスでの EIGRP 認証のイネーブル化

EIGRP ルート認証では、EIGRP ルーティング プロトコルからのルーティング アップデートに対する MD5 認証を提供します。MD5 キーを使用したダイジェストが各 EIGRP パケットに含まれており、承認されていない送信元からの不正なルーティング メッセージや虚偽のルーティング メッセージが取り込まれないように阻止します。

EIGRP ルート認証は、インターフェイスごとに設定します。EIGRP メッセージ認証対象として設定されたインターフェイス上にあるすべての EIGRP ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。



(注) EIGRP ルート認証をイネーブルにするには、事前に EIGRP をイネーブルにする必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] を選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの自律システム (AS) 番号を入力します。指定できる AS 番号の範囲は 1 ~ 65535 です。

ステップ 4 [Networks] タブをクリックします。

ステップ 5 [Add] をクリックして、新しいネットワーク エントリを追加します。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

ステップ 6 ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 7 [IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

(注) ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

- ステップ 8** [Network Mask] フィールドで、IP アドレスに適用されるネットワーク マスクを選択するか入力します。
- ステップ 9** [OK] をクリックします。
- ステップ 10** [Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces] の順に選択します。
- [Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、インターフェイスごとに設定を修正できます。これらの設定の詳細については、[EIGRP のインターフェイスの設定 \(782 ページ\)](#) を参照してください。
- ステップ 11** [Enable MD5 Authentication] チェックボックスをオンにして、EIGRP プロセス メッセージの MD5 認証をイネーブルにします。このチェックボックスをオンにした後で、次のいずれかを指定します。
- [Key] フィールドに、EIGRP 更新を認証するキーを入力します。このキーの最大長は 16 文字です。
 - [Key ID] フィールドに、キー ID 値を入力します。有効値の範囲は、1 ~ 255 です。
- ステップ 12** [OK] をクリックします。

EIGRP ネイバーの定義

EIGRP hello パケットはマルチキャスト パケットとして送信されます。EIGRP ネイバーが、トンネルなど、非ブロードキャストネットワークを越えた場所にある場合、手動でネイバーを定義する必要があります。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャストメッセージとしてそのネイバーに送信されます。

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。
- [EIGRP Setup] ペインが表示されます。
- ステップ 2** [Enable EIGRP routing] チェックボックスをオンにします。
- ステップ 3** [EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ~ 65535 です。
- ステップ 4** [Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Static Neighbor] の順に選択します。
- [Static Neighbor] ペインが開き、スタティックに定義された EIGRP ネイバーが表示されます。EIGRP ネイバーは、ASA との間で EIGRP ルーティング情報を送受信します。通常は、ネイバー探索プロセスによってネイバーがダイナミックに検出されます。ただし、ポイントツーポイントの非ブロードキャストネットワークでは、ネイバーをスタティックに定義する必要があります。

[Static Neighbor] テーブルの各行には、ネイバーの EIGRP 自律システム番号、ネイバー IP アドレス、およびネイバーに接続するためのインターフェイスが表示されます。

[Static Neighbor] ペインでは、スタティック ネイバーを追加または編集できます。

ステップ 5 EIGRP スタティック ネイバーを追加または編集するには、[Add] または [Edit] をクリックします。

[Add EIGRP Neighbor Entry] または [Edit EIGRP Neighbor Entry] ダイアログボックスが表示されます。

ステップ 6 ネイバーを設定する EIGRP プロセスのドロップダウンリストで EIGRP AS 番号を選択します。

ステップ 7 [Interface Name] ドロップダウン リストからインターフェイス名を選択します。このインターフェイスを通してネイバーが使用可能になります。

ステップ 8 ネイバーの IP アドレスを [Neighbor IP Address] フィールドに入力します。

ステップ 9 [OK] をクリックします。

EIGRP へのルート再配布

RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。接続されているルートが、EIGRP コンフィギュレーション内の **network** 文で指定された範囲に含まれている場合、再配布する必要はありません。



(注) RIP 限定：この手順を開始する前に、ルート マップを作成し、指定されたルーティング プロトコルのうち RIP ルーティング プロセスに再配布されるルートを詳細に定義する必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ~ 65535 です。

ステップ 4 [Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Redistribution] の順に選択します。

[Redistribution] ペインには、他のルーティング プロトコルから EIGRP ルーティング プロセスにルートを再配布するためのルールが表示されます。スタティック ルートや接続済みルートを EIGRP ルーティング プロセスに再配布する場合は、メトリックの設定は必須ではありません。

が、設定することを推奨します。[Redistribution] ペインのテーブルの各行に、1 つのルート再配布エントリが表示されます。

ステップ 5 新しい再配布ルールを追加するには、[Add] をクリックします。既存の再配布ルールを編集する場合は、ステップ 6 に進んでください。

[Add EIGRP Redistribution Entry] ダイアログボックスが表示されます。

ステップ 6 既存の EIGRP スタティック ネイバーを編集するには、テーブル内のアドレスを選択して [Edit] をクリックします。テーブル内のエントリをダブルクリックするという方法でも、そのエントリを編集できます。

[Edit EIGRP Redistribution Entry] ダイアログボックスが表示されます。

ステップ 7 このエントリが適用される EIGRP ルーティングプロセスの AS 番号をドロップダウンリストで選択します。

ステップ 8 [Protocol] 領域で、ルーティングプロセスのプロトコルとして次のいずれかを選択してそのオプション ボタンをクリックします。

- [Static] を選択すると、スタティック ルートが EIGRP ルーティングプロセスに再配布されます。ネットワーク設定の範囲内にあるスタティック ルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。
- [Connected] を選択すると、接続されているルートが EIGRP ルーティングプロセスに再配布されます。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。
- [RIP] を選択すると、RIP ルーティングプロセスで検出されたルートが EIGRP に再配布されます。
- [OSPF] を選択すると、OSPF ルーティングプロセスで検出されたルートが EIGRP に再配布されます。

ステップ 9 [Optional Metrics] 領域で、再配布されるルートに使用するメトリックとして次のいずれかを選択します。

- [Bandwidth] は EIGRP 帯域幅メトリックで、単位はキロビット/秒です。有効値の範囲は 1 ~ 4294967295 です。
- [Delay] は EIGRP 遅延メトリックで、単位は 10 マイクロ秒です。有効値の範囲は、0 ~ 4294967295 です。
- [Reliability] は EIGRP 信頼性メトリックです。有効値の範囲は 0 ~ 255 で、255 は信頼性が 100 % であることを示します。
- [Loading] は EIGRP 有効帯域幅（負荷）メトリックです。有効値の範囲は 1 ~ 255 で、255 は負荷が 100 % であることを示します。
- [MTU] はパスの MTU です。有効値の範囲は 1 ~ 65535 です。

- ステップ 10** ルート マップを [Route Map] ドロップダウンリストで選択し、EIGRP ルーティングプロセスに再配布するルートを実験します。ルート マップの設定方法の詳細については、[ルート マップ \(681 ページ\)](#) を参照してください。
- ステップ 11** [Optional OSPF Redistribution] 領域で、どの OSPF ルートを EIGRP ルーティングプロセスに再配布するかをさらに詳しく指定するために、次の OSPF オプションボタンのいずれかをクリックします。
- [Match Internal] を選択すると、指定されている OSPF プロセスの内部であるルートが対象となります。
 - [Match External 1] を選択すると、指定されている OSPF プロセスの外部であるタイプ 1 ルートが対象となります。
 - [Match External 2] を選択すると、指定されている OSPF プロセスの外部であるタイプ 2 ルートが対象となります。
 - [Match NSSA-External 1] を選択すると、指定されている OSPF NSSA の外部であるタイプ 1 ルートが対象となります。
 - [Match NSSA-External 2] を選択すると、指定されている OSPF NSSA の外部であるタイプ 2 ルートが対象となります。
- ステップ 12** [OK] をクリックします。

EIGRP でのネットワークのフィルタリング



- (注) この手順を開始する前に、標準の ACL を作成し、その中にアドバタイズするルートを定義する必要があります。つまり、標準の ACL を作成し、その中に送信または受信したアップデートからフィルタリングするルートを定義します。

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。
- [EIGRP Setup] ペインが表示されます。
- ステップ 2** [Enable EIGRP routing] チェックボックスをオンにします。
- ステップ 3** [EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ~ 65535 です。
- ステップ 4** [Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Filter Rules] の順に選択します。

EIGRP ルーティング プロセスに対して設定されているルート フィルタリング ルールが [Filter Rules] ペインに表示されます。フィルタ ルールによって、EIGRP ルーティング プロセスで受け入れまたはアドバタイズされるルートを制御できます。

[Filter Rule] テーブルの各行には、特定のインターフェイスまたはルーティング プロトコルに適用されるフィルタ ルールについての情報が記載されます。たとえば、フィルタ ルールで外部インターフェイスでの「in」方向が指定されている場合は、外部インターフェイスで受信された EIGRP アップデートすべてにフィルタリングが適用されます。フィルタ ルールで方向が「out」、ルーティング プロトコルとして OSPF 10 が指定されている場合は、発信 EIGRP アップデートで EIGRP ルーティング プロセスに再配布されるルートにフィルタ ルールが適用されます。

- ステップ 5** フィルタ ルールを追加するには [Add] をクリックします。既存のフィルタ ルールを編集する場合は、ステップ 6 に進んでください。
- [Add Filter Rules] ダイアログボックスが表示されます。
- ステップ 6** フィルタ ルールを編集するには、テーブルでそのフィルタ ルールを選択して [Edit] をクリックします。
- [Edit Filter Rules] ダイアログボックスが表示されます。フィルタ ルールをダブルクリックして編集することもできます。フィルタ ルールを削除するには、テーブルでそのフィルタ ルールを選択して [Delete] をクリックします。
- ステップ 7** このエントリが適用される EIGRP ルーティング プロセスの AS 番号をドロップダウン リストで選択します。
- ステップ 8** フィルタ ルートの方向をドロップダウン リストで選択します。
- 着信 EIGRP ルーティング アップデートからのルートをフィルタリングするルールの場合は、[in] を選択します。ASA から送信される EIGRP ルーティング アップデートからのルートをフィルタリングするには、[out] を選択します。
- [out] を選択した場合、[Routing process] フィールドがアクティブになります。フィルタリングするルートのタイプを選択します。スタティック、接続済み、RIP、および OSPF のルーティング プロセスから再配布されるルートをフィルタリングできます。ルーティング プロセスを指定するフィルタは、すべてのインターフェイスで送信される更新からのルートをフィルタリングします。
- ステップ 9** OSPF プロセス ID を [ID] フィールドに入力します。
- ステップ 10** [Interface] オプション ボタンをクリックしてから、フィルタを適用するインターフェイスを選択します。
- ステップ 11** [Add] または [Edit] をクリックして、フィルタ ルールの ACL を定義します。[Edit] をクリックすると、選択されているネットワーク ルールの [Network Rule] ダイアログボックスが開きます。
- ステップ 12** [Action] ドロップダウン リストで、[Permit] を選択すると指定のネットワークのアドバタイズが許可され、[Deny] を選択すると指定のネットワークのアドバタイズが禁止されます。

- ステップ 13** [IP Address] フィールドに、許可または禁止するネットワークの IP アドレスを入力します。すべてのアドレスを許可または禁止するには、IP アドレス **0.0.0.0** とネットワーク マスク **0.0.0.0** を使用します。
- ステップ 14** [Netmask] ドロップダウン リストで、ネットワークの IP アドレスに適用するネットワーク マスクを選択します。このフィールドにネットワークマスクを入力するか、リストから共通マスクの 1 つを選択します。
- ステップ 15** [OK] をクリックします。

EIGRP Hello 間隔と保持時間のカスタマイズ

ASA は、ネイバーを検出する目的、およびネイバーが到達不能または動作不能になったことを把握する目的で、定期的に hello パケットを送信します。デフォルトでは、hello パケットは 5 秒間隔で送信されます。

hello パケットは、ASA の保持時間をアドバタイズします。保持時間によって、EIGRP ネイバーに、ASA を到達可能と見なす時間の長さを知らせます。アドバタイズされた保持時間内にネイバーが hello パケットを受信しなかった場合、ASA は到達不能と見なされます。デフォルトでは、アドバタイズされる保持時間は 15 秒です (hello 間隔の 3 倍)。

hello 間隔とアドバタイズされる保持時間のいずれも、インターフェイスごとに設定します。保持時間は hello 間隔の 3 倍以上に設定することをお勧めします。

手順

- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup]** の順に選択します。
- [EIGRP Setup] ペインが表示されます。
- ステップ 2** [Enable EIGRP routing] チェックボックスをオンにします。
- ステップ 3** [OK] をクリックします。
- ステップ 4** **[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces]** の順に選択します。
- [Interface] ペインに、EIGRP インターフェイスのすべての設定が表示されます。
- ステップ 5** インターフェイス エントリをダブルクリックするか、またはエントリを選択して [Edit] をクリックします。
- [Edit EIGRP Interface Entry] ダイアログボックスが表示されます。
- ステップ 6** EIGRP AS 番号をドロップダウン リストで選択します。このリストに表示されるのは、EIGRP ルーティング プロセスをイネーブルにしたときに設定されていたシステム番号です。
- ステップ 7** [Hello Interval] フィールドに、インターフェイス上で送信される EIGRP hello パケット間の間隔を入力します。
- 有効値の範囲は、1 ~ 65535 秒です。デフォルト値は 5 秒です。

- ステップ 8** [Hold Time] フィールドで、保持時間を秒単位で指定します。
有効値の範囲は、1 ~ 65535 秒です。デフォルト値は 15 秒です。
- ステップ 9** [OK] をクリックします。

自動ルート集約の無効化

自動ルート集約は、デフォルトでイネーブルになっています。EIGRP ルーティングプロセスは、ネットワーク番号の境界で集約を行います。このことは、不連続ネットワークがある場合にルーティングの問題の原因となることがあります。

たとえば、ネットワーク 192.168.1.0、192.168.2.0、192.168.3.0 が接続されているルータがあり、それらのネットワークがすべて EIGRP に参加しているとすると、EIGRP ルーティングプロセスはそれらのルートに対しサマリーアドレス 192.168.0.0 を作成します。さらにネットワーク 192.168.10.0 と 192.168.11.0 が接続されているルータがこのネットワークに追加され、それらのネットワークが EIGRP に参加すると、これらもまた 192.168.0.0 として集約されます。トラフィックが誤った場所にルーティングされる可能性をなくすために、競合するサマリーアドレスを作成するルータでの自動ルート集約をディセーブルにする必要があります。

手順

-
- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。
[EIGRP Setup] ペインが表示されます。
- ステップ 2** [Enable EIGRP routing] チェックボックスをオンにします。
- ステップ 3** [Process Instance] タブをクリックします。
- ステップ 4** [Advanced] をクリックします。
- ステップ 5** [Summary] 領域の [Auto-Summary] チェックボックスをオフにします。
(注) この設定はデフォルトでイネーブルになっています。
- ステップ 6** [OK] をクリックします。

EIGRP でのデフォルト情報の設定

EIGRP アップデート内のデフォルトルート情報の送受信を制御できます。デフォルトでは、デフォルトルートが送信され、受け入れられます。デフォルト情報の受信を禁止するように ASA を設定すると、候補のデフォルトルートビットが受信ルート上でブロックされます。デフォルト情報の送信を禁止するように ASA を設定すると、アドバタイズされるルートのデフォルトルートビット設定が無効になります。

ASDM では、[Default Information] ペインに、EIGRP アップデートでのデフォルト ルート情報の送受信を制御するルールテーブルが表示されます。EIGRP ルーティングプロセスごとに、「in」ルールと「out」ルールを1つずつ設定できます（現在は1つのプロセスだけがサポートされています）。

デフォルトでは、デフォルトルートが送信され、受け入れられます。デフォルトのルート情報の送受信を制限またはディセーブルにするには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

メインの [EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [OK] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいエントリを作成するには、[Add] をクリックします。
- エントリを編集するには、テーブル内のエントリをダブルクリックするか、テーブル内のエントリを選択して [Edit] をクリックします。

そのエントリの [Add Default Information] または [Edit Default Information] ダイアログボックスが表示されます。EIGRP AS 番号が [EIGRP] フィールドで自動的に選択されています。

ステップ 5 [Direction] フィールドで、ルールの方向として次のオプションのいずれかを選択します。

- [in] : このルールは、着信 EIGRP アップデートからのデフォルトルート情報をフィルタリングします。
- [out] : このルールは、発信 EIGRP アップデートからのデフォルトルート情報をフィルタリングします。

EIGRP プロセスごとに、「in」ルールと「out」ルールを1つずつ設定できます。

ステップ 6 ネットワーク ルール テーブルにネットワーク ルールを追加します。ネットワーク ルールでは、デフォルト ルート情報を送受信するときに許可されるネットワークと拒否されるネットワークを定義します。デフォルト情報フィルタルールに追加するネットワークルールごとに、次の手順を繰り返します。

- a) ネットワークルールを追加するには [Add] をクリックします。既存のネットワークルールをダブルクリックしてルールを編集します。
- b) [Action] フィールドで、そのネットワークを許可する場合は [Permit] をクリックし、ブロックする場合は [Deny] をクリックします。
- c) [IP Address] フィールドと [Network Mask] フィールドに、ルールによって許可または拒否されるネットワークの IP アドレスとネットワーク マスクを入力します。

すべてのデフォルト ルート情報の受け入れや送信を拒否するには、ネットワーク アドレスとして **0.0.0.0** を入力し、ネットワーク マスクとして **0.0.0.0** を選択します。

- d) 指定したネットワーク ルールをデフォルト情報フィルタ ルールに追加するには、[OK] をクリックします。

ステップ 7 デフォルト情報フィルタ ルールを受け入れるには、[OK] をクリックします。

EIGRP スプリット ホライズンのディセーブル化

スプリット ホライズンは、EIGRP アップデート パケットとクエリー パケットの送信を制御します。スプリット ホライズンがインターフェイスでイネーブルになると、アップデート パケットとクエリー パケットは、このインターフェイスがネクスト ホップとなる宛先には送信されません。この方法でアップデート パケットとクエリー パケットを制御すると、ルーティング ループが発生する可能性が低くなります。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスでイネーブルになっています。

スプリット ホライズンは、ルート情報が、その情報の発信元となるインターフェイスからルータによってアドバタイズされないようにします。通常、特にリンクが切断された場合には、この動作によって複数のルーティング デバイス間の通信が最適化されます。ただし、非ブロードキャスト ネットワークでは、この動作が望ましくない場合があります。このような場合は、EIGRP を設定したネットワークを含め、スプリット ホライズンをディセーブルにする必要が生じることもあります。

インターフェイスでのスプリット ホライズンをディセーブルにする場合、そのインターフェイス上のすべてのルータとアクセス サーバに対してディセーブルにする必要があります。

EIGRP スプリット ホライズンをディセーブルにするには、次の手順を実行します。

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces] の順に選択します。

[Interface] ペインが表示され、EIGRP インターフェイスの設定が表示されます。

- ステップ 2** インターフェイス エントリをダブルクリックするか、またはエントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

- ステップ 3** EIGRP 自律システム (AS) 番号をドロップダウン リストで選択します。このリストに表示されるのは、EIGRP ルーティング プロセスをイネーブルにしたときに設定されていたシステム番号です。

- ステップ 4** [Split Horizon] チェックボックスをオフにします。

ステップ5 [OK] をクリックします。

EIGRP プロセスの再始動

EIGRP プロセスを再始動したり、再配布またはカウンタをクリアしたりすることができます。

手順

ステップ1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ2 [リセット (Reset)] をクリックします。

EIGRP のモニタリング

次のコマンドを使用して、EIGRP ルーティングプロセスをモニタできます。コマンド出力の例と説明については、コマンドリファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな EIGRP ルーティング統計情報をモニタまたはディセーブル化するには、次の手順を実行します。

手順

ステップ1 メイン ASDM ウィンドウで、**[Monitoring] > [Routing] > [EIGRP Neighbor]** の順に選択します。

各行は1つの EIGRP ネイバーを表します。ネイバーごとに、リストにはその IP アドレス、接続先のネットワーク、保持時間、アップタイム、キュー長、シーケンス番号、スムーズラウンドトリップ時間、再送信タイムアウトが表示されます。考えられる状態変更のリストは次のとおりです。

- [NEW ADJACENCY] : 新しいネイバーが確立されました。
- [PEER RESTARTED] : 他のネイバーがネイバー関係のリセットを開始しました。メッセージを受け取ったルータは、ネイバーをリセットしているルータではありません。
- [HOLD TIME EXPIRED] : 保持時間が経過しても、ルータは EIGRP パケットをネイバーから受け取っていません。

- [RETRY LIMIT EXCEEDED] : EIGRP は EIGRP 高信頼性パケットに対する確認応答をネイバーから受け取らなかったため、高信頼性パケットの再送信をすでに 16 回試行しましたが、一度も成功しませんでした。
- [ROUTE FILTER CHANGED] : ルートフィルタに変更があったため、EIGRP ネイバーがリセットしています。
- [INTERFACE DELAY CHANGED] : インターフェイスでの遅延パラメータの手動設定変更があったため、EIGRP ネイバーがリセットしています。
- [INTERFACE BANDWIDTH CHANGED] : インターフェイスでのインターフェイス帯域幅の手動設定変更があったため、EIGRP ネイバーがリセットしています。
- [STUCK IN ACTIVE] : EIGRP がアクティブ状態のままスタックしているため、EIGRP ネイバーがリセットしています。ネイバーがリセットされるのは、`stuck-in-active`状態となったためです。

ステップ 2 モニタする EIGRP ネイバーをクリックします。

ステップ 3 現在のネイバー リストを削除するには、[Clear Neighbors] をクリックします。

ステップ 4 現在のネイバー リストの表示を更新するには、[Refresh] をクリックします。

(注) デフォルトでは、ネイバー変更メッセージとネイバー警告メッセージはロギングされません。

EIGRP の履歴

表 32: EIGRP の機能の履歴

機能名	プラットフォーム リリース	機能情報
EIGRP サポート	7.0(1)	Enhanced Interior Gateway Routing Protocol (EIGRP) を使用するデータのルーティング、認証の実行、およびルーティング情報の再配布とモニタリングのサポートが追加されました。 次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [EIGRP]。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	EIGRP ルーティングは、マルチ コンテキスト モードでサポートされます。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup]。

機能名	プラットフォーム リリース	機能情報
クラスタ	9.0(1)	EIGRP の場合、バルク同期、ルートの同期およびレイヤ2 ロードバランシングは、クラスタリング環境でサポートされます。
EIGRP Auto-Summary	9.2(1)	EIGRP の [Auto-Summary] フィールドはデフォルトでディセーブルになりました。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] > [Edit EIGRP Process Advanced Properties]



第 31 章

マルチキャストルーティング

この章では、マルチキャストルーティングプロトコルを使用するように Cisco ASA を設定する方法について説明します。

- [マルチキャストルーティングの概要 \(799 ページ\)](#)
- [マルチキャストルーティングのガイドライン \(801 ページ\)](#)
- [マルチキャストルーティングの有効化 \(802 ページ\)](#)
- [マルチキャストルーティングのカスタマイズ \(803 ページ\)](#)
- [マルチキャストルーティングの例 \(819 ページ\)](#)
- [マルチキャストルーティングの履歴 \(820 ページ\)](#)

マルチキャストルーティングの概要

マルチキャストルーティングは、単一の情報ストリームを数千もの企業や家庭に同時に配信することでトラフィックを軽減する帯域幅節約型のテクノロジーです。マルチキャストルーティングを活用するアプリケーションには、ビデオ会議、企業通信、遠隔学習に加えて、ソフトウェア、株価、およびニュースの配信などがあります。

マルチキャストルーティングプロトコルでは、競合テクノロジーのネットワーク帯域幅の使用量を最小限に抑えながら、発信元や受信者の負荷を増加させずに発信元のトラフィックを複数の受信者に配信します。マルチキャストパケットは、Protocol Independent Multicast (PIM) やサポートする他のマルチキャストプロトコルを使用したASAによりネットワークで複製されるため、複数の受信者にできる限り高い効率でデータを配信できます。

ASAは、スタブマルチキャストルーティングとPIMマルチキャストルーティングの両方をサポートしています。ただし、1つのASAに両方を同時に設定できません。



(注) UDP と非 UDP の両方のトランスポートがマルチキャストルーティングに対してサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

スタブマルチキャストルーティング

スタブマルチキャストルーティングは、ダイナミックホスト登録の機能を提供して、マルチキャストルーティングを容易にします。スタブマルチキャストルーティングを設定すると、ASAはIGMPのプロキシエージェントとして動作します。ASAは、マルチキャストルーティングに全面的に参加するのではなく、IGMPメッセージをアップストリームのマルチキャストルーターに転送し、そのルーターがマルチキャストデータの送信をセットアップします。スタブマルチキャストルーティングを設定する場合は、ASAをPIMスパースモードまたは双方向モードに設定できません。IGMPスタブマルチキャストルーティングに参加しているインターフェイス上でPIMを有効にする必要があります。

ASAは、PIM-SMおよび双方向PIMの両方をサポートしています。PIM-SMは、基盤となるユニキャストルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャストルーティングプロトコルです。このプロトコルは、マルチキャストグループあたり1つのランデブーポイント（RP）をルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パスツリーを作成します。

PIMマルチキャストルーティング

双方向PIMはPIM-SMの変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャストトポロジの各リンクで動作する指定フォワーダ（DF）選択プロセスを使用して構築されます。DFに支援されたマルチキャストデータは発信元からランデブーポイント（RP）に転送されます。この結果、マルチキャストデータは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DFの選択はRPの検出中に行われ、これによってデフォルトルートがRPに提供されます。



(注) ASAがPIM RPの場合は、ASAの変換されていない外部アドレスをRPアドレスとして使用してください。

マルチキャストグループの概念

マルチキャストはグループの概念に基づくものです。受信者の任意のグループは、特定のデータストリームを受信することに関心があります。このグループには物理的または地理的な境界がなく、インターネット上のどの場所にホストを置くこともできます。特定のグループに流れるデータの受信に関心があるホストは、IGMPを使用してグループに加入する必要があります。ホストがデータストリームを受信するには、グループのメンバでなければなりません。マルチキャストグループの設定方法の詳細については、[マルチキャストグループの設定（815ページ）](#)を参照してください。

マルチキャストアドレス

マルチキャストアドレスは、グループに加入し、このグループに送信されるトラフィックの受信を希望するIPホストの任意のグループを指定します。

クラスタ

マルチキャストルーティングは、クラスタリングをサポートします。スパンド EtherChannel クラスタリングでは、ファーストパス転送が確立されるまでの間、プライマリ ユニットがすべてのマルチキャストルーティング パケットとデータ パケットを送信します。ファーストパス転送が確立されると、従属ユニットがマルチキャスト データ パケットを転送できます。すべてのデータ フローは、フルフローです。スタブ転送フローもサポートされます。スパンド EtherChannel クラスタリングでは1つのユニットだけがマルチキャストパケットを受信するため、プライマリ ユニットへのリダイレクションは共通です。個別インターフェイス クラスタリングでは、ユニットは個別に機能しません。すべてのデータとルーティングパケットはプライマリユニットで処理され、転送されます。従属ユニットは、送信されたすべてのパケットをドロップします。

クラスタリングの詳細については、[ASA クラスタ \(331 ページ\)](#) を参照してください。

マルチキャスト ルーティングのガイドライン

コンテキスト モード

シングル コンテキスト モードでサポートされています。

ファイアウォール モード

ルーテッドファイアウォールモードでだけサポートされています。トランスペアレントファイアウォールモードはサポートされません。

IPv6

IPv6 はサポートされません。

クラスタ

IGMP および PIM のクラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。

その他のガイドライン

224.1.2.3 などのマルチキャスト ホストへのトラフィックを許可するには、インバウンドインターフェイス上のアクセス制御ルールを設定する必要があります。ただし、ルールの宛先インターフェイスを指定したり、初期接続確認の間にマルチキャストの接続に適用したりすることはできません。

マルチキャスト ルーティングの有効化

ASA でマルチキャストルーティングを有効にすると、デフォルトではすべてのデータインターフェイスで IGMP と PIM が有効になりますが、5506-X ~ 5555-X モデルの管理インターフェイスでは有効になりません。IGMP は、直接接続されているサブネット上にグループのメンバが存在するかどうか学習するために使用されます。ホストは、IGMP 報告メッセージを送信することにより、マルチキャストグループに参加します。PIM は、マルチキャストデータグラムを転送するための転送テーブルを維持するために使用されます。

5506-X ~ 5555-X モデルの管理インターフェイスでマルチキャストルーティングを有効にするには、管理インターフェイスでマルチキャスト境界を明示的に設定する必要があります。



(注) マルチキャストルーティングでは、UDP トランスポート レイヤだけがサポートされています。

以下の表に、ASA の RAM の量に基づいた特定のマルチキャスト テーブルのエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 33: マルチキャスト テーブルのエントリの上限 (スタティック/ダイナミック エントリの合計の上限)

Table	16 MB	128 MB	128 + MB
MFIB	1000	3000	30000
IGMP グループ	1000	3000	30000
PIM ルート	3000	7000	72000

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast]** の順に選択します。

ステップ 2 **[Multicast]** ペインで、**[Enable Multicast routing]** チェックボックスをオンにします。

このチェックボックスをオンにすると、ASA 上で IP マルチキャストルーティングがイネーブルになります。このチェックボックスをオフにすると、IP マルチキャストルーティングがディセーブルになります。デフォルトでは、マルチキャストはディセーブルになっています。マルチキャストルーティングをイネーブルにすると、すべてのインターフェイス上でマルチキャストがイネーブルになります。マルチキャストはインターフェイスごとにディセーブルにできません。

マルチキャスト ルーティングのカスタマイズ

ここでは、マルチキャスト ルーティングをカスタマイズする方法について説明します。

スタブマルチキャストルーティングの設定とIGMPメッセージの転送



(注) スタブマルチキャストルーティングは、PIM スパース モードおよび双方向モードと同時にサポートされません。

スタブエリアへのゲートウェイとして動作しているASAは、PIM スパース モードまたは双方向モードに参加する必要はありません。その代わりに、そのセキュリティアプライアンスをIGMP プロキシエージェントとして設定すると、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータにIGMP メッセージを転送することができます。ASA をIGMP プロキシエージェントとして設定するには、ホスト加入 (join) メッセージおよびホスト脱退 (leave) メッセージをスタブエリアからアップストリーム インターフェイスに転送します。スタブモードのマルチキャストルーティングに参加しているインターフェイスでも、PIM を有効にする必要があります。

手順

- ステップ1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] の順に選択します。
- ステップ2 [Multicast] ペインで、[Enable Multicast routing] チェックボックスをオンにします。
- ステップ3 [Apply] をクリックして変更内容を保存します。
- ステップ4 [Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol] の順に選択します。
- ステップ5 どのインターフェイスからIGMPメッセージを転送するかを変更するには、インターフェイスを選択して [Edit] をクリックします。
[Configure IGMP Parameters] ダイアログボックスが表示されます。
- ステップ6 [Forward Interface] ドロップダウン リストで、どのインターフェイスからIGMPメッセージを送信するかを選択します。
- ステップ7 [OK] をクリックしてこのダイアログボックスを閉じてから、[Apply] をクリックして変更内容を保存します。

スタティック マルチキャスト ルートの設定

スタティック マルチキャスト ルートを設定すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、送信元と宛先の間のパスでマルチキャスト ルーティングがサポートされていない場合は、その解決策として、2つのマルチキャスト デバイスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

PIMを使用する場合、ASAは、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートバイパスする場合などは、ユニキャスト パケットで1つのパスを使用し、マルチキャスト パケットで別の1つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast] > [MRoute]** の順に選択します。

ステップ 2 **[Add]** または **[Edit]** を選択します。

[Add Multicast Route] または **[Edit Multicast Route]** ダイアログボックスが表示されます。

ASA に新しいスタティック マルチキャスト ルートを追加する場合は、**[Add Multicast Route]** ダイアログボックスを使用します。既存のスタティック マルチキャスト ルートを変更する場合は、**[Edit Multicast Route]** ダイアログボックスを使用します。

ステップ 3 **[Source Address]** フィールドに、マルチキャスト送信元の IP アドレスを入力します。既存のスタティック マルチキャスト ルートを編集しているときは、この値は変更できません。

ステップ 4 **[Source Mask]** ドロップダウン リストからマルチキャスト送信元の IP アドレスのネットワーク マスクを選択します。

ステップ 5 **[Incoming Interface]** 領域で、**[RPF Interface]** オプション ボタンをクリックしてルートを転送する RPF を選択するか、**[Interface Name]** オプション ボタンをクリックし、次に以下を入力します。

- **[Source Interface]** フィールドで、ドロップダウン リストからマルチキャスト ルートの着信 インターフェイスを選択します。
- **[Destination Interface]** フィールドで、どの宛先インターフェイスを通してルートを転送するかをドロップダウン リストで選択します。

(注) インターフェイスまたは RPF ネイバーを指定できますが、同時に両方は指定できません。

ステップ 6 **[Administrative Distance]** フィールドで、スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスを選択します。スタティック マルチキャスト ルートのアドミニスト

レーティブ デスタンスがユニキャスト ルートのアドミストレーティブ デスタンスと同じである場合は、スタティック マルチキャスト ルートが優先されます。

ステップ 7 [OK] をクリックします。

IGMP 機能の設定

IP ホストは、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブ ネットでアクティブなグループと非アクティブなグループを検出します。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。

インターフェイスでの IGMP の有効化

IGMP は、特定のインターフェイスでディセーブルにできます。この情報は、特定のインターフェイスにマルチキャスト ホストがないことがわかっている、ASA からそのインターフェイスにホスト クエリー メッセージを発信しないようにする場合に有用です。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol] の順に選択します。

[Protocol] ペインには、ASA 上の各インターフェイスの IGMP パラメータが表示されます。

ステップ 2 ディセーブルにするインターフェイスを選択して [Edit] をクリックします。

ステップ 3 指定したインターフェイスをディセーブルにするには、[Enable IGMP] チェックボックスをオフにします。

ステップ 4 [OK] をクリックします。

[Protocol] ペインに「Yes」と表示される場合は IGMP がそのインターフェイス上でイネーブルになっており、「No」の場合はそのインターフェイス上で IGMP がディセーブルになっていません。

IGMP グループ メンバーシップの設定

ASA をマルチキャスト グループのメンバとして設定できます。マルチキャスト グループに加入するように ASA を設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティングテーブル情報を維持して、このグループをアクティブにするパスを保持します。



- (注) 特定のグループのマルチキャストパケットを特定のインターフェイスに転送する必要がある場合に、ASAがそのパケットをそのグループの一部として受け付けることがないようにする方法については、[スタティック加入したIGMPグループの設定 \(806ページ\)](#) を参照してください。

手順

- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Join Group]** の順に選択します。
- ステップ 2** [Join Group] ペインの [Add] または [Edit] をクリックします。 > > >
- [Add IGMP Join Group] ダイアログボックスでは、インターフェイスをマルチキャスト グループのメンバーに設定することができます。[Edit IGMP Join Group] ダイアログでは、既存のメンバーシップ情報を変更することができます。
- ステップ 3** [Interface Name] フィールドで、ドロップダウンリストからインターフェイス名を選択します。既存のエントリを編集しているときは、この値は変更できません。
- ステップ 4** [Multicast Group Address] フィールドで、インターフェイスが属するマルチキャスト グループのアドレスを入力します。有効なグループアドレスの範囲は、224.0.0.0 ~ 239.255.255.255 です。
- ステップ 5** [OK] をクリックします。

スタティック加入した IGMP グループの設定

設定によってはグループメンバがグループ内で自分のメンバーシップを報告できない場合があります。また、ネットワークセグメント上にグループのメンバが存在しないこともあります。しかし、それでも、そのグループのマルチキャストトラフィックをそのネットワークセグメントに送信することが必要になる場合があります。そのようなグループのマルチキャストトラフィックをそのセグメントに送信するには、スタティック加入したIGMPグループを設定します。

メイン ASDM ウィンドウで、**[Configuration] > [Routing] > [Multicast] > [IGMP] > [Static Group]** の順に選択すると、ASAをスタティックに接続されたグループメンバーとして設定できます。この方法の場合、ASAはパケットそのものを受信せず、転送だけを実行します。そのため、スイッチングが高速に実施されます。発信インターフェイスはIGMPキャッシュ内に存在しますが、このインターフェイスはマルチキャストグループのメンバーではありません。

手順

- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Static Group]** の順に選択します。

ステップ 2 [Static Group] ペインの [Add] または [Edit] をクリックします。

インターフェイスに対してマルチキャストグループをスタティックに割り当てる場合は、[Add IGMP Static Group] ダイアログボックスを使用します。既存のスタティック グループの割り当てを変更する場合は、[Edit IGMP Static Group] ダイアログボックスを使用します。

ステップ 3 [Interface Name] フィールドで、ドロップダウンリストからインターフェイス名を選択します。既存のエントリを編集しているときは、この値は変更できません。

ステップ 4 [Multicast Group Address] フィールドで、インターフェイスが属するマルチキャストグループのアドレスを入力します。有効なグループアドレスの範囲は、224.0.0.0 ~ 239.255.255.255 です。

ステップ 5 [OK] をクリックします。

マルチキャスト グループへのアクセスの制御

アクセス コントロール リストを使用して、マルチキャスト グループへのアクセスを制御できます。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Access Group] の順に選択します。

[Access Group] ペインが表示されます。[Access Group] ペインのテーブル エントリは、上から下の順に処理されます。具体的なエントリはテーブルの上方に、一般的なエントリは下方に配置してください。たとえば、特定のマルチキャストグループを許可するためのアクセスグループ エントリはテーブルの上方に配置し、許可ルールに指定されたグループなど、一定のまとまりを持った複数のマルチキャスト グループを拒否するようなアクセスグループ エントリは下方に配置します。ただし、拒否ルールよりも許可ルールの方が優先的に適用されるため、許可ルールに指定されているグループは、拒否ルールが適用されて場合でも許可されます。

テーブルのエントリをダブルクリックすると、選択したエントリの [Add/Edit Access Group] ダイアログボックスが開きます。

ステップ 2 [Add] または [Edit] をクリックします。

[Add Access Group] または [Edit Access Group] ダイアログボックスが表示されます。[Add Access Group] ダイアログボックスでは、新しいアクセスグループを [Access Group] テーブルに追加できます。[Edit Access Group] ダイアログボックスでは、既存のアクセスグループ エントリの情報を変更できます。既存のエントリを編集するときは、一部のフィールドがグレー表示されることがあります。

ステップ 3 アクセスグループを関連付けるインターフェイスの名前を [Interface] ドロップダウンリストで選択します。既存のアクセスグループを編集しているときは、関連インターフェイスは変更できません。

- ステップ 4** [permit] を [Action] ドロップダウンリストで選択すると、選択されているインターフェイス上でそのマルチキャストグループが許可されます。[deny] を [Action] ドロップダウンリストで選択すると、選択されているインターフェイスからそのマルチキャストグループがフィルタリングされます。
- ステップ 5** [Multicast Group Address] フィールドで、そのアクセスグループの適用先となるマルチキャストグループのアドレスを入力します。
- ステップ 6** マルチキャストグループアドレスのネットワークマスクを入力するか、一般的なネットワークマスクの1つを [Netmask] ドロップダウンリストから選択します。
- ステップ 7** [OK] をクリックします。

インターフェイスにおける IGMP 状態の数の制限

IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告は IGMP キャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol] の順に選択します。
- ステップ 2** [Protocol] ペインのテーブルから限定するインターフェイスを選択し、[Edit] をクリックします。
- [Configure IGMP Parameters] ダイアログボックスが表示されます。
- ステップ 3** [Group Limit] フィールドに、インターフェイス上で参加できる最大ホスト数を入力します。
- デフォルト値は 500 です。有効な値は 0 ~ 500 です。
- (注) この値を 0 に設定すると、学習したグループが追加されなくなりますが、手動で定義したメンバーシップは引き続き許可されます。
- ステップ 4** [OK] をクリックします。

マルチキャストグループに対するクエリーメッセージの変更

ASA は、クエリーメッセージを送信して、インターフェイスに接続されているネットワークにメンバを持つマルチキャストグループを検出します。メンバは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャストパケットの受信を希望していることを示します。クエリーメッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システムマルチキャストグループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、ASA に保存されているメンバーシップ情報はリフレッシュされます。ASA で、ローカルメンバがいなくなったマルチキャストグルー

プがまだインターフェイスに接続されていることがわかると、そのグループへのマルチキャストパケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にルーティングメッセージを戻します。

デフォルトでは、サブネット上のPIM指定ルータがクエリーメッセージの送信を担当します。このメッセージは、デフォルトでは125秒間に1回送信されます。

クエリー応答時間を変更する場合は、IGMPクエリーでアドバタイズする最大クエリー応答時間はデフォルトで10秒になります。ASAがこの時間内にホストクエリーの応答を受信しなかった場合、グループを削除します。

クエリー間隔、クエリー応答時間、クエリータイムアウト値を変更するには、次の手順を実行します。

手順

-
- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol]** の順に選択します。
 - ステップ 2** **[Protocol]** ペインのテーブルから限定するインターフェイスを選択し、**[Edit]** をクリックします。
[Configure IGMP Parameters] ダイアログボックスが表示されます。
 - ステップ 3** **[Query Interval]** フィールドに、指定したルータから IGMP ホストクエリーメッセージが送信される時間間隔を秒単位で入力します。
有効な値の範囲は 1 ~ 3600 秒です。デフォルト値は 125 秒です。
(注) 指定されたタイムアウト値の時間が経過しても、ASA がインターフェイス上でクエリーメッセージを検出できなかった場合は、その ASA が指定ルータになり、クエリーメッセージの送信を開始します。
 - ステップ 4** **[Query Timeout]** に、前のインターフェイスのリクエストがリクエストとしての動作を停止してから、ASA がそのインターフェイスのリクエストの役割を引き継ぐまでの期間を秒単位で入力します。
有効な値の範囲は 60 ~ 300 秒です。デフォルト値は 255 秒です。
 - ステップ 5** **[Response Time]** フィールドには、IGMP クエリーでアドバタイズされる最大クエリー応答時間を秒数で入力します。
有効範囲は 1 ~ 25 秒です。デフォルト値は 10 秒です。
 - ステップ 6** **[OK]** をクリックします。
-

IGMP バージョンの変更

デフォルトでは、ASA は IGMP バージョン 2 を実行します。このバージョンではなどの、いくつかの追加機能を使用できます。

サブネットのマルチキャストルータはすべて、同じ IGMP バージョンをサポートしている必要があります。ASA は、バージョン 1 ルータを自動的に検出してバージョン 1 に切り替えることはありません。しかし、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストが混在しても問題はありません。IGMP バージョン 2 を実行している ASA は、IGMP バージョン 1 のホストが存在しても正常に動作します。

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol]** の順に選択します。
- ステップ 2 どのインターフェイスの IGMP バージョンを変更するかを [Protocol] ペインのテーブルで選択し、**[Edit]** をクリックします。
[Configure IGMP Interface] ダイアログボックスが表示されます。
- ステップ 3 バージョン番号を [Version] ドロップダウン リストから選択します。
- ステップ 4 **[OK]** をクリックします。

PIM 機能の設定

ルータは PIM を使用して、マルチキャスト ダイアグラムを転送するために使われる転送テーブルを維持します。ASA でマルチキャストルーティングをイネーブルにすると、PIM および IGMP がすべてのインターフェイスで自動的にイネーブルになります。



- (注) PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

ここでは、任意の PIM 設定を行う方法について説明します。

インターフェイスでの PIM の有効化またはディセーブル化

PIM は、特定のインターフェイスでイネーブルまたはディセーブルにできます。

手順

- ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Protocol]** の順に選択します。

- ステップ 2** どのインターフェイスで PIM をイネーブルにするかを [Protocol] ペインのテーブルで選択し、[Edit] をクリックします。
- [Edit PIM Protocol] ダイアログボックスが表示されます。
- ステップ 3** [Enable PIM] チェックボックスをオンにします。PIM をディセーブルにするには、このチェックボックスをオフにします。
- ステップ 4** [OK] をクリックします。

スタティック ランデブーポイントアドレスの設定

共通の PIM スパースモードまたは双方向ドメイン内のルータはすべて、PIM RP アドレスを認識する必要があります。このアドレスは、**pim rp-address** コマンドを使用してスタティックに設定されます。



(注) ASA は、Auto-RP または PIM BSR をサポートしていません。

複数のグループの RP として機能するように ASA を設定することができます。ACL に指定されているグループ範囲によって、PIM RP のグループマッピングが決まります。ACL が指定されていない場合は、マルチキャストグループ全体の範囲 (224.0.0.0/4) にグループの RP が適用されます。

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Rendezvous Points] の順に選択します。
- ステップ 2** [Add] または [Edit] をクリックします。
- [Add Rendezvous Point] または [Edit Rendezvous Point] ダイアログボックスが表示されます。[Add Rendezvous Point] ダイアログボックスでは、新しいエントリを [Rendezvous Point] テーブルに追加できます。[Edit Rendezvous Point] ダイアログボックスでは、既存の RP エントリを変更できます。さらに、[Delete] をクリックして、選択されているマルチキャストグループエントリをテーブルから削除できます。
- RP を使用する場合の制限事項は、次のとおりです。
- 同じ RP アドレスは、2 度使用できません。
 - 複数の RP に対しては、[All Groups] を指定できません。
- ステップ 3** [Rendezvous Point Address] フィールドに、RP の IP アドレスを入力します。
- 既存の RP エントリを編集しているときは、この値は変更できません。

ステップ 4 [Use bi-directional forwarding] チェックボックスをオンにすると、指定されているマルチキャストグループは双方向モードで動作します。[Rendezvous Point] ペインに「Yes」と表示されている場合は、指定されているマルチキャストグループが双方向モードで動作し、「No」の場合はスパスモードで動作します。双方向モードでは、ASA がマルチキャストパケットを受信したときに、直接接続されたメンバーも PIM ネイバーも存在しない場合は、送信元にブルーニングメッセージが返されます。

ステップ 5 [Use this RP for All Multicast Groups] オプション ボタンをクリックすると、指定した RP がそのインターフェイス上のすべてのマルチキャストグループに使用され、[Use this RP for the Multicast Groups as specified below] オプション ボタンをクリックすると、指定した RP をどのマルチキャストグループで使用するかを指定できます。

マルチキャストグループの詳細については、[マルチキャストグループの設定 \(815 ページ\)](#) を参照してください。

ステップ 6 [OK] をクリックします。

指定ルータのプライオリティの設定

DR は、PIM 登録メッセージ、PIM 加入メッセージ、およびブルーニングメッセージの RP への送信を担当します。1つのネットワークセグメントに複数のマルチキャストルータがある場合は、DR プライオリティに基づいて DR が選択されます。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。

デフォルトでは、ASA の DR プライオリティは 1 です。この値を変更できます。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Protocol] の順に選択します。

ステップ 2 [Protocol] ペインのテーブルから PIM にイネーブルにするインターフェイスを選択し、[Edit] をクリックします。

[Edit PIM Protocol] ダイアログボックスが表示されます。

ステップ 3 [DR Priority] フィールドに、選択されているインターフェイスの指定ルータプライオリティの値を入力します。サブネット上のルータのうち、DR プライオリティが最いものが指定ルータになります。有効な値の範囲は 0 ~ 4294967294 です。デフォルトの DR プライオリティは 1 です。この値を 0 に設定した場合は、その ASA インターフェイスがデフォルトのルータになることはありません。

ステップ 4 [OK] をクリックします。

PIM 登録メッセージの設定とフィルタリング

ASA が RP として動作しているときは、特定のマルチキャスト送信元を登録できないように制限することができます。このようにすると、未許可の送信元が RP に登録されるのを回避できます。[Request Filter] ペインでは、ASA で PIM 登録メッセージが受け入れられるマルチキャストソースを定義できます。

手順

- ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Request Filter] の順に選択します。
- ステップ 2 [Add] をクリックします。

[Request Filter Entry] ダイアログボックスでは、ASA が RP として動作する際に ASA に登録できるマルチキャスト送信元を定義できます。送信元 IP アドレスおよび宛先マルチキャストアドレスに基づいて、フィルタルールを作成します。
- ステップ 3 [Action] ドロップダウンリストで、[Permit] を選択すると、指定のマルチキャストトラフィックの指定の送信元に ASA への登録を許可するルールが作成され、[Deny] を選択すると、指定のマルチキャストトラフィックの指定の送信元による ASA への登録を禁止するルールが作成されます。
- ステップ 4 [Source IP Address] フィールドに、登録メッセージの送信元の IP アドレスを入力します。
- ステップ 5 [Source Netmask] フィールドに、登録メッセージの送信元のネットワークマスクを入力するか、ドロップダウンリストから選択します。
- ステップ 6 [Destination IP Address] フィールドに、マルチキャストの宛先アドレスを入力します。
- ステップ 7 [Destination Netmask] フィールドに、マルチキャストの宛先アドレスのネットワークマスクを入力するか、ドロップダウンリストから選択します。
- ステップ 8 [OK] をクリックします。

PIM メッセージ間隔の設定

ルータ クエリーメッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリーメッセージを送信します。デフォルトでは、ルータ クエリーメッセージは 30 秒間隔で送信されます。さらに、60 秒ごとに、ASA は PIM 加入メッセージおよびプルーニングメッセージを送信します。

手順

- ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Protocol] の順に選択します。
- ステップ 2 [Protocol] ペインのテーブルから PIM にイネーブルにするインターフェイスを選択し、[Edit] をクリックします。

[Edit PIM Protocol] ダイアログボックスが表示されます。

- ステップ 3** [Hello Interval] フィールドに、インターフェイスから PIM hello メッセージが送信される時間間隔を秒単位で入力します。
- ステップ 4** [Prune Interval] フィールドに、インターフェイスから PIM 参加およびプルーンングのアドバタイズメントが送信され時間間隔を秒単位で入力します。
- ステップ 5** [OK] をクリックします。

ルートツリーの設定

デフォルトでは、PIM リーフルータは、新しい送信元から最初のパケットが到着した直後に、最短パスツリーに加入します。この方法では、遅延が短縮されますが、共有ツリーに比べて多くのメモリが必要になります。すべてのマルチキャストグループまたは特定のマルチキャストアドレスに対して、ASA を最短パス ツリーに加入させるか、共有ツリーを使用するかを設定できます。

手順

- ステップ 1** メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Route Tree] の順に選択します。
- ステップ 2** 次のいずれかのオプション ボタンをクリックします。

- [Use Shortest Path Tree for All Groups] : すべてのマルチキャストグループに最短パス ツリーを使用する場合は、このオプションを選択します。
- [Use Shared Tree for All Groups] : すべてのマルチキャストグループに共有ツリーを使用する場合は、このオプションを選択します。
- [Use Shared Tree for the Groups specified below] : [Multicast Groups] テーブルで指定したグループに共有ツリーを使用する場合は、このオプションを選択します。[Multicast Groups] テーブルで指定されていないグループには最短パス ツリーが使用されます。

[Multicast Groups] テーブルには、共有ツリーを使用するマルチキャストグループが表示されます。

テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャストグループが含まれるエントリを作成し、その範囲の中から特定のグループを除外するには、その除外するグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャストグループ全体に対する許可ルールを deny 文の下に配置します。

マルチキャストグループを編集するには、[マルチキャストグループの設定 \(815 ページ\)](#) を参照してください。

マルチキャスト グループの設定

マルチキャスト グループとは、どのマルチキャスト アドレスがグループの一部であるかを定義するアクセス ルールのリストです。1つのマルチキャスト グループに、マルチキャスト アドレスが1つだけ含まれることも、特定の範囲のマルチキャスト アドレスが含まれることもあります。新しいマルチキャスト グループ ルールを作成する場合は、[Add Multicast Group] ダイアログボックスを使用します。既存のマルチキャスト グループ ルールを修正する場合は、[Edit Multicast Group] ダイアログボックスを使用します。

マルチキャスト グループを設定するには、次の手順を実行します。

手順

- ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Rendezvous Points] の順に選択します。
- ステップ 2 [Rendezvous Point] ペインが表示されます。設定するグループをクリックします。
[Edit Rendezvous Point] ダイアログボックスが表示されます。
- ステップ 3 [Use this RP for the Multicast Groups as specified below] オプション ボタンをクリックすると、指定の RP とともに使用するマルチキャスト グループを指定できます。
- ステップ 4 [Add] または [Edit] をクリックします。
[Add Multicast Group] または [Edit Multicast Group] ダイアログボックスが表示されます。
- ステップ 5 [Action] ドロップダウン リストで、[Permit] を選択すると指定のマルチキャスト アドレスを許可するグループ ルールが作成され、[Deny] を選択すると指定のマルチキャスト アドレスをフィルタリングするグループ ルールが作成されます。
- ステップ 6 [Multicast Group Address] フィールドに、このグループに関連付けるマルチキャスト アドレスを入力します。
- ステップ 7 [Netmask] ドロップダウン リストで、マルチキャスト グループ アドレスのネットワーク マスクを選択します。
- ステップ 8 [OK] をクリックします。

PIM ネイバーのフィルタリング

PIM ネイバーにできるルータの定義が可能です。PIM ネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブ ルータが PIM に参加できないようにする。

手順

-
- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Neighbor Filter]** の順に選択します。
- ステップ 2** **[Add]/[Edit]/[Insert]** をクリックして、テーブルから設定する PIM ネイバーを選択します。
- [Add/Edit/Insert Neighbor Filter Entry]** ダイアログボックスが表示されます。このダイアログボックスでは、マルチキャスト境界 ACL の ACL エントリを作成できます。選択されている PIM ネイバー エントリを削除することもできます。
- ステップ 3** **[Interface Name]** ドロップダウン リストからインターフェイス名を選択します。
- ステップ 4** **[Action]** ドロップダウン リストから、ネイバー フィルタ ACL エントリに対して **[Permit]** または **[Deny]** を選択します。
- [Permit]** を選択すると、マルチキャストグループアドバタイズメントがこのインターフェイスを通過できるようになります。**[Deny]** を選択すると、指定したマルチキャストグループアドバタイズメントはこのインターフェイスを通過できなくなります。インターフェイスに対してマルチキャスト境界を設定すると、ネイバー フィルタ エントリで許可されていない限り、すべてのマルチキャストトラフィックが、インターフェイスの通過を拒否されます。
- ステップ 5** **[IP Address]** フィールドに、許可または拒否するマルチキャスト PIM グループの IP アドレスを入力します。有効なグループアドレスの範囲は、224.0.0.0 ~ 239.255.255.255 です。
- ステップ 6** **[Netmask]** ドロップダウンリストで、マルチキャストグループアドレスのネットマスクを選択します。
- ステップ 7** **[OK]** をクリックします。
-

双方向ネイバー フィルタの設定

ASA に PIM 双方向ネイバー フィルタが設定されている場合、**[Bidirectional Neighbor Filter]** ペインにそれらのフィルタが表示されます。PIM 双方向ネイバー フィルタは、DF 選定に参加できるネイバー デバイスを定義する ACL です。PIM 双方向ネイバー フィルタがインターフェイスに設定されていない場合は、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選定プロセスに参加できます。

PIM 双方向ネイバー フィルタ設定が ASA に適用されると、実行コンフィギュレーションに *interface-name_multicast* という名前の ACL が表示されます。ここで、*interface-name* はマルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます (*inside_multicast_1* など)。この ACL により、どのデバイスが ASA の PIM ネイバーになれるか定義されます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

PIM 双方向ネイバー フィルタを利用すると、スパースモード専用ネットワークから双方向ネットワークへの移行が可能になります。このフィルタで、DF 選定に参加するルータを指定する

一方で、引き続きすべてのルータにスパースモードドメインへの参加を許可できるからです。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセットクラウドに出入りできないようにします。

PIM 双方向ネイバー フィルタがイネーブルの場合、その ACL によって許可されるルータは、双方向に対応していると見なされます。したがって、次のことが当てはまります。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

手順

- ステップ 1** メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Bidirectional Neighbor Filter]** の順に選択します。
- ステップ 2** [PIM Bidirectional Neighbor Filter] テーブルのエントリの 1 つをダブルクリックすると、そのエントリの [Edit Bidirectional Neighbor Filter Entry] ダイアログボックスが表示されます。
- ステップ 3** [Add]/[Edit]/[Insert] をクリックして、テーブルから設定する PIM ネイバーを選択します。
[Add/Edit/Insert Bidirectional Neighbor Filter Entry] ダイアログボックスが表示され、ここで PIM 双方向ネイバー フィルタ ACL の ACL エントリを作成できます。
- ステップ 4** [Interface Name] ドロップダウン リストからインターフェイス名を選択します。どのインターフェイスに対して PIM 双方向ネイバー フィルタ ACL エントリを設定するかを選択します。
- ステップ 5** [Action] ドロップダウン リストから、ネイバー フィルタ ACL エントリに対して [Permit] または [Deny] を選択します。
[Permit] を選択すると、指定したデバイスが DF 選定に参加できるようになります。指定したデバイスを DF 選定プロセスに参加させない場合は、[Deny] を選択します。
- ステップ 6** 許可または拒否するマルチキャスト PIM グループの IP アドレスを入力します。[IP Address] フィールドで有効なグループアドレスの範囲は、224.0.0.0 ~ 239.255.255.255 です。
- ステップ 7** [Netmask] ドロップダウンリストで、マルチキャストグループアドレスのネットマスクを選択します。
- ステップ 8** [OK] をクリックします。

マルチキャスト境界の設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

インターフェイスでマルチキャスト グループ アドレスの管理スコープ境界を設定できます。IANA では、239.0.0.0 ~ 239.255.255.255 のマルチキャスト アドレス範囲が管理スコープ アドレスとして指定されています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。このアドレスはグローバルではなく、ローカルで一意であると見なされます。

影響を受けるアドレスの範囲は、標準 ACL で定義します。境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

管理スコープ境界で Auto-RP 検出メッセージと通知メッセージを設定、検証、フィルタリングできます。境界の ACL で拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Routing] > [Multicast] > [MBoundary]** の順に選択します。

[MBoundary] ペインでは、管理スコープマルチキャストアドレスのマルチキャスト境界を設定できます。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャストグループアドレスを複数の管理ドメインで再利用できるようになります。インターフェイスに対してマルチキャスト境界が定義されている場合、フィルタ ACL により許可されたマルチキャストトラフィックだけが、そのインターフェイスを通過します。

ステップ 2 [Edit] をクリックします。

[Edit Boundary Filter] ダイアログボックスに、マルチキャスト境界フィルタ ACL が表示されます。このダイアログボックスを使用すれば、境界フィルタ ACL エントリを追加したり削除したりできます。

境界フィルタのコンフィギュレーションが ASA に適用されると、実行コンフィギュレーションに *interface-name_multicast* という名前の ACL が追加されます。*interface-name* は、マルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます (*inside_multicast_1* など)。

ステップ 3 どのインターフェイスに対してマルチキャスト境界フィルタ ACL を設定するかを [Interface] ドロップダウン リストで選択します。

ステップ 4 [Remove any Auto-RP group range] チェックボックスをオンにすると、境界 ACL で拒否された送信元からの Auto-RP メッセージがフィルタリングされます。[Remove any Auto-RP group range] チェックボックスがオフの場合は、すべての Auto-RP メッセージが通過できます。

ステップ 5 [OK] をクリックします。

マルチキャストルーティングの例

次の例に、さまざまなオプションのプロセスを使用してマルチキャストルーティングをイネーブルにし、設定する方法を示します。

1. メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] の順に選択します。
2. [Multicast] ペインで、[Enable Multicast routing] チェックボックスをオンにして [Apply] をクリックします。
3. メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [MRoute] の順に選択します。
4. [Add] または [Edit] をクリックします。

[Add Multicast Route] または [Edit Multicast Route] ダイアログボックスが表示されます。

ASA に新しいスタティック マルチキャストルートを追加する場合は、[Add Multicast Route] ダイアログボックスを使用します。既存のスタティックマルチキャストルートを変更する場合は、[Edit Multicast Route] ダイアログボックスを使用します。

5. [Source Address] フィールドに、マルチキャスト送信元の IP アドレスを入力します。既存のスタティックマルチキャストルートを編集しているときは、この値は変更できません。
6. [Source Mask] ドロップダウン リストからマルチキャスト送信元の IP アドレスのネットワーク マスクを選択します。
7. [Incoming Interface] 領域で、[RPF Interface] オプション ボタンをクリックしてルートを転送する RPF を選択するか、[Interface Name] オプション ボタンをクリックし、次に以下を入力します。

- [Source Interface] フィールドで、ドロップダウン リストからマルチキャストルートの着信インターフェイスを選択します。
- [Destination Interface] フィールドでは、選択されているインターフェイスからどの宛先インターフェイスにルートを転送するかをドロップダウンリストで選択します。



(注) インターフェイスまたは RPF ネイバーを指定できますが、同時に両方は指定できません。

8. [Administrative Distance] フィールドで、スタティック マルチキャストルートのアドミニストレーティブ ディスタンスを選択します。スタティック マルチキャストルートのアドミニストレーティブ ディスタンスがユニキャストルートのアドミニストレーティブ ディスタンスと同じである場合は、スタティック マルチキャストルートが優先されます。
9. [OK] をクリックします。
10. メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Join Group] の順に選択します。
[Join Group] ペインが表示されます。
11. [Add] または [Edit] をクリックします。
[Add IGMP Join Group] ダイアログボックスでは、インターフェイスをマルチキャストグループのメンバーに設定することができます。[Edit IGMP Join Group] ダイアログボックスでは、既存のメンバーシップ情報を変更することができます。
12. [Interface Name] フィールドで、ドロップダウンリストからインターフェイス名を選択します。既存のエントリを編集しているときは、この値は変更できません。
13. [Multicast Group Address] フィールドで、インターフェイスが属するマルチキャストグループのアドレスを入力します。有効なグループアドレスの範囲は、224.0.0.0 ~ 239.255.255.255 です。
14. [OK] をクリックします。

マルチキャスト ルーティングの履歴

表 34: マルチキャスト ルーティングの機能履歴

機能名	プラットフォーム リリース	機能情報
マルチキャスト ルーティング サポート	7.0(1)	マルチキャスト ルーティング プロトコルを使用した、データのマルチキャスト ルーティング データ、認証、およびルーティング情報の再配布とモニタリングのサポートが追加されました。 次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [Multicast]。
クラスタリングのサポート	9.0(1)	クラスタリングのサポートが追加されました。

機能名	プラットフォーム リリース	機能情報
Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) パススルーのサポート	9.5(1)	ASA が最後のホップ ルータである場合を除いて、マルチキャストルーティングが有効になっているときに PIM-SSM パケットが通過できるようサポートを追加しました。これにより、さまざまな攻撃から保護すると同時に、マルチキャストグループをより柔軟に選択できるようになりました。ホストは、明示的に要求された送信元からのトラフィックのみを受信します。変更された画面はありません。



第 **VI** 部

AAA サーバおよびローカル データベース

- [AAA サーバとローカルデータベース \(825 ページ\)](#)
- [AAA の RADIUS サーバ \(833 ページ\)](#)
- [AAA 用の TACACS+ サーバ \(863 ページ\)](#)
- [AAA の LDAP サーバ \(871 ページ\)](#)



第 32 章

AAA サーバとローカル データベース

この章では、認証、認可、アカウントिंग（AAA は「トリプル A」と読む）について説明します。AAA は、コンピュータ リソースへのアクセスを制御するための一連のサービスで、サービスの課金に必要な情報を提供します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

この章では、AAA 機能用にローカル データベースを設定する方法について説明します。外部 AAA サーバについては、ご使用のサーバタイプに関する章を参照してください。

- [AAA とローカル データベースについて](#) (825 ページ)
- [ローカル データベースのガイドライン](#) (829 ページ)
- [ローカル データベースへのユーザ アカウントの追加](#) (829 ページ)
- [ローカル データベースの認証および認可のテスト](#) (831 ページ)
- [ローカル データベースのモニタリング](#) (831 ページ)
- [ローカル データベースの履歴](#) (832 ページ)

AAA とローカル データベースについて

ここでは、AAA とローカル データベースについて説明します。

認証

認証はユーザを特定する方法です。アクセスが許可されるには、ユーザは通常、有効なユーザ名と有効なパスワードが必要です。AAA サーバは、データベースに保存されている他のユーザ クレデンシャルとユーザの認証資格情報を比較します。クレデンシャルが一致する場合、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合は、認証は失敗し、ネットワーク アクセスは拒否されます。

次の項目を認証するように、Cisco ASA を設定できます。

- ASA へのすべての管理接続（この接続には、次のセッションが含まれます）
 - Telnet
 - SSH

- シリアル コンソール
 - ASDM (HTTPS を使用)
 - VPN 管理アクセス
-
- **enable** コマンド
 - ネットワーク アクセス層
 - VPN アクセス

認証

許可はポリシーを適用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。ユーザが認証されると、そのユーザはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

次の項目を認可するように、ASA を設定できます。

- 管理コマンド
- ネットワーク アクセス層
- VPN アクセス

アカウントティング

アカウントティングは、アクセス時にユーザが消費したリソースを測定します。これには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウントティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティプランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウントティング間の相互作用

認証だけで使用することも、認可およびアカウントティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウントティングだけで使用することも、認証および認可とともに使用することもできます。

AAA Servers

AAA サーバは、アクセス制御に使用されるネットワーク サーバです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実行します。アカウントティングは、課金と分析に使用される時間とデータのリソースを追跡します。

AAA Server Groups

認証、許可、またはアカウントिंगに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバグループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバグループは名前で識別されます。各サーバグループは、あるサーバまたはサービスに固有です。

次の項を参照してください。

- [RADIUS サーバグループの設定 \(855 ページ\)](#)
- [TACACS+ サーバグループの設定 \(866 ページ\)](#)
- [LDAP サーバグループの設定 \(877 ページ\)](#)

Kerberos、SDI および HTTP フォーム用のサーバグループも設定できます。これらのグループは VPN 設定で使用されます。これらのグループのタイプについては、『VPN 構成ガイド』を参照してください。

ローカル データベースについて

ASA は、ユーザプロファイルを取り込むことができるローカルデータベースを管理します。AAA サーバの代わりにローカルデータベースを使用して、ユーザ認証、認可、アカウントングを提供することもできます。

次の機能にローカルデータベースを使用できます。

- ASDM ユーザごとのアクセス
- コンソール認証
- Telnet 認証および SSH 認証
- **enable** コマンド認証

この設定は、CLI アクセスにだけ使用され、Cisco ASDM ログインには影響しません。

- コマンド許可

ローカルデータベースを使用するコマンド許可を有効にすると、Cisco ASA では、ユーザ特権レベルを参照して、どのコマンドが使用できるかが特定されます。コマンド許可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。ASDM には、コマンドへの割り当てをイネーブルにできる特権レベルが事前に定義されています。割り当てることができるレベルは、15 (管理)、5 (読み取り専用)、3 (監視専用) の 3 種類です。事前定義済みのレベルを使用する場合は、ユーザを 3 種類の特権レベルのいずれかに割り当てます。

- ネットワーク アクセス認証
- VPN クライアント認証

マルチ コンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する AAA ルールは設定できません。



(注) ローカル データベースはネットワーク アクセス認可には使用できません。

フォールバック サポート

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、ASA から誤ってロックアウトされないように設計されています。

ログインすると、コンフィギュレーション内で指定されている最初のサーバから、応答があるまでグループ内のサーバが順に1つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ローカルデータベースがフォールバック方式（管理認証および許可限定）として設定されていると、ASA はローカル データベースに接続しようとします。フォールバック方式として設定されていない場合、ASA は引き続き AAA サーバにアクセスしようとします。

フォールバック サポートを必要とするユーザについては、ローカル データベース内のユーザ名およびパスワードと、AAA サーバ上のユーザ名およびパスワードとを一致させることを推奨します。これにより、透過フォールバックがサポートされます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用する場合は、指定すべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブルパスワード認証：グループ内のサーバがすべて使用できない場合、ASA ではローカルデータベースを使用して管理アクセスを認証します。これには、イネーブルパスワード認証が含まれる場合があります。
- コマンド許可：グループ内の TACACS+サーバがすべて使用できない場合、特権レベルに基づいてコマンドを認可するためにローカル データベースが使用されます。
- VPN 認証および認可：VPN 認証および認可は、通常この VPN サービスをサポートしている AAA サーバが使用できない場合、ASA へのリモートアクセスをイネーブルにするためにサポートされます。管理者である VPN クライアントが、ローカル データベースへのフォールバックを設定されたトンネルグループを指定する場合、AAA サーバグループが使用できない場合でも、ローカル データベースが必要な属性で設定されていれば、VPN トンネルが確立できます。

グループ内の複数のサーバを使用したフォールバックの仕組み

サーバグループ内に複数のサーバを設定し、サーバグループのローカル データベースへのフォールバックをイネーブルしている場合、ASAからの認証要求に対してグループ内のどのサーバからも応答がないと、フォールバックが発生します。次のシナリオで例証します。

サーバ1、サーバ2の順で、LDAP サーバグループに2台の Active Directory サーバを設定します。リモートユーザがログインすると、ASAによってサーバ1に対する認証が試みられます。

サーバ1から認証エラー（「user not found」など）が返されると、ASAによるサーバ2に対する認証は試みられません。

タイムアウト期間内にサーバ1から応答がないと（または認証回数が、設定されている最大数を超えている場合）、ASAによってサーバ2に対する認証が試みられます。

グループ内のどちらのサーバからも応答がなく、ASAにローカル データベースへのフォールバックが設定されている場合、ASAによってローカル データベースに対する認証が試みられます。

ローカル データベースのガイドライン

ローカル データベースを認証または認可に使用する場合、ASAからのロックアウトを必ず防止してください。

ローカル データベースへのユーザ アカウントの追加

ユーザをローカル データベースに追加するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] を選択し、次に [Add] をクリックします。

[Add User Account-Identity] ダイアログボックスが表示されます。

ステップ 2 4～64文字の長さのユーザ名を入力します。

ステップ 3 3～32文字のパスワードを入力します。パスワードでは大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。セキュリティを確保するために、パスワードの長さは8文字以上にするのを推奨します。

(注) [User Accounts] ペインでイネーブルパスワードを設定する場合は、ユーザ名 enable_15 に対するパスワードを変更します。ユーザ名 enable_15 は常に [User Accounts] ペインに表示され、デフォルトユーザ名を表します。この方法は、ASDM のシステム コンフィギュレーションでイネーブルパスワードを設定する唯一の方法です。CLI で他のイネーブル レベルパスワード (enable password 10 など) を設定すると、そのユーザ名は enable_10 という形式で表示されます。

ステップ 4 パスワードを再度入力します。

セキュリティ上の理由から、パスワードを入力するこの2つのフィールドには、アスタリスクだけが表示されます。

ステップ 5 MSCHAP を認証に使用している場合は、[User authenticated using MSCHAP] チェックボックスをオンにします。

ステップ 6 [Access Restriction] 領域で、ユーザの管理アクセス レベルを設定します。まず、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] タブの順に移動し、[Perform authorization for exec shell access] オプションをクリックして、管理認可を有効にする必要があります。

次のいずれかのオプションを選択します。

- [Full Access (ASDM, Telnet, SSH and console)] : ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定するとユーザは ASDM、SSH、Telnet、およびコンソールポートを使用できます。さらに認証もイネーブルにすると、ユーザはグローバル コンフィギュレーション モードにアクセスできます。
- [Privilege Level] : ASDM およびローカル コマンド認可用の特権レベルを設定します。範囲は、0 (最低) ~ 15 (最高) です。無制限の管理者アクセス権を付与するには、15 を指定します。事前定義された ASDM ロールでは、管理者用の 15、読み取り専用の 5、およびモニタ専用の 3 (ユーザによる [Home] ペインと [Monitoring] ペインの使用を制限する) が使用されます。
- [CLI login prompt for SSH, Telnet and console (no ASDM access)] : ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定するとユーザは SSH、Telnet、およびコンソールポートを使用できます。ユーザは設定に ASDM を使用できません (HTTP 認証を設定している場合)。ASDM 監視は可能です。さらにイネーブル認証も設定すると、ユーザはグローバル コンフィギュレーション モードにアクセスできません。
- [No ASDM, SSH, Telnet, or console access] : ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定すると、ユーザは認証用に設定した管理アクセス方式を利用できなくなります (ただし、[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます)。

ステップ 7 (オプション) ユーザ単位で ASA への SSH 接続の公開キー認証をイネーブルにする方法については、[HTTPS \(ASDM\) アクセスの設定 \(886 ページ\)](#) を参照してください。

ステップ 8 [VPN Policy] をクリックして、このユーザの VPN ポリシー属性を設定します。VPN 構成ガイドを参照してください。

ステップ 9 [Apply] をクリックします。

ユーザがローカルデータベースに追加され、変更内容が実行コンフィギュレーションに保存されます。

ヒント [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] ペインの各コラムで特定のテキストを検索できます。[Find] ボックスに検索する特定のテキストを入力し、[Up] または [Down] 矢印をクリックします。テキスト検索にアスタリスク（「*」）と疑問符（「?」）をワイルドカードとして使用することもできます。

ローカル データベースの認証および認可のテスト

ASA がローカル データベースに接続してユーザを認証または許可できるかどうか確認するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [AAA Server Groups] テーブルで、サーバが含まれるサーバグループをクリックします。

ステップ 2 [Servers in the Selected Group] テーブルでテストするサーバをクリックします。

ステップ 3 [Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4 実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5 ユーザ名を入力します。

ステップ 6 認証をテストする場合は、ユーザ名のパスワードを入力します。

ステップ 7 [OK] をクリックします。

認証または認可のテストメッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラーメッセージが表示されます。

ローカル データベースのモニタリング

ローカル データベースのモニタリングについては、次のコマンドを参照してください。

- [Monitoring] > [Properties] > [AAA Servers]

このペインには、AAA サーバの統計情報が表示されます。

- [Tools] > [Command Line Interface]

このペインでは、さまざまな非インタラクティブコマンドを発行し、結果を表示することができます。

ローカル データベースの履歴

表 35: ローカル データベースの履歴

機能名	プラットフォーム リリース	説明
AAA のローカル データベース設定	7.0(1)	<p>AAA 用にローカル データベースを設定する方法について説明します。</p> <p>次の画面が導入されました。</p> <p>[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts]</p>
SSH 公開キー認証のサポート	9.1(2)	<p>ASA への SSH 接続の公開キー認証は、ユーザ単位で有効にできるようになりました。公開キーファイル (PKF) でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式 (最大 2048 ビット) では大きすぎるキーについては、PKF 形式を使用します。</p> <p>次の画面が導入されました。</p> <p>[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication][Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF]。</p> <p>8.4(4.1) でも使用可能。PKF キー形式は 9.1(2) でのみサポートされます。</p>



第 33 章

AAA の RADIUS サーバ

この章では、AAA 用に RADIUS サーバを設定する方法について説明します。

- [AAA 用の RADIUS サーバについて \(833 ページ\)](#)
- [AAA の RADIUS サーバのガイドライン \(854 ページ\)](#)
- [AAA 用の RADIUS サーバの設定 \(855 ページ\)](#)
- [RADIUS サーバの認証および認可のテスト \(861 ページ\)](#)
- [AAA 用の RADIUS サーバのモニタリング \(861 ページ\)](#)
- [AAA 用の RADIUS サーバの履歴 \(862 ページ\)](#)

AAA 用の RADIUS サーバについて

Cisco ASA は AAA について、次の RFC 準拠 RADIUS サーバをサポートしています。

- Cisco Secure ACS 3.2、4.0、4.1、4.2、および 5.x
- Cisco Identity Services Engine (ISE)
- RSA 認証マネージャ 5.2、6.1 および 7.x の RSA Radius
- Microsoft

サポートされている認証方式

ASA は、RADIUS サーバでの次の認証方式をサポートします。

- PAP : すべての接続タイプの場合。
- CHAP および MS-CHAPv1 : L2TP-over-IPsec 接続の場合。
- MS-CHAPv2 : L2TP-over-IPsec 接続の場合。また、パスワード管理機能がイネーブルで、通常の IPsec リモート アクセス接続の場合。MS-CHAPv2 は、クライアントレス接続でも使用できます。
- 認証プロキシモード : RADIUS から Active Directory、RADIUS から RSA/SDI、Radius から トークンサーバ、RSA/SDI から RADIUS の各接続。



(注) MS-CHAPv2 を、ASA と RADIUS サーバの間の VPN 接続で使用されるプロトコルとしてイネーブルにするには、トンネルグループ一般属性でパスワード管理をイネーブルにする必要があります。パスワード管理を有効にすると、ASA から RADIUS サーバへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネルグループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバが MS-CHAPv2 以外の認証要求を送信するように設定できます。

VPN 接続のユーザ認証

ASA は、RADIUS サーバを使用して、ダイナミック ACL またはユーザごとの ACL 名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシセッションのユーザ許可を実行できます。ダイナミック ACL を実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによってダウンロード可能 ACL、または ACL 名が ASA に送信されます。所定のサービスへのアクセスが ACL によって許可または拒否されます。認証セッションの有効期限が切れると、ASA は ACL を削除します。

ACL に加えて、ASA は、VPN リモート アクセスおよびファイアウォール カットスルー プロキシセッションの認証およびアクセス許可の設定を行うための多くの属性をサポートしています。

RADIUS 属性のサポートされるセット

ASA は次の RADIUS 属性のセットをサポートしています。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウント属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- Cisco IOS ベンダー固有属性 (VSA) は、RADIUS ベンダー ID 9 で識別されます。
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

サポートされる RADIUS 認証属性

認可では、権限または属性を使用するプロセスを参照します。認証サーバとして定義されている RADIUS サーバは、権限または属性が設定されている場合はこれらを使用します。これらの属性のベンダー ID は 3076 です。

次の表に、ユーザ認可に使用可能な、サポートされている RADIUS 属性の一覧を示します。



- (注) RADIUS 属性名には、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS の属性名にはまだ cVPN3000 プレフィックスが含まれています。ASA は、属性名ではなく数値の属性 ID に基づいて RADIUS 属性を使用します。

次の表に示した属性はすべてダウンストリーム属性であり、RADIUS サーバから ASA に送信されます。ただし、属性番号 146、150、151、および 152 を除きます。これらの属性番号はアップストリーム属性であり、ASA から RADIUS サーバに送信されます。RADIUS 属性 146 および 150 は、認証および認可の要求の場合に ASA から RADIUS サーバに送信されます。前述の 4 つの属性はすべて、アカウント開始、中間アップデート、および終了の要求の場合に ASA から RADIUS サーバに送信されます。アップストリーム RADIUS 属性 146、150、151、152 は、バージョン 8.4(3) で導入されました。

表 36: サポートされる RADIUS 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	文字列	シングル	時間範囲の名前 (Business-hours など)
Access-List-Inbound	Y	86	文字列	シングル	ACL ID
Access-List-Outbound	Y	87	文字列	シングル	ACL ID
Address-Pools	Y	217	文字列	シングル	IP ローカルプールの名前
Allow-Non-Extension Mode	Y	64	ブール	シングル	0 = 無効 1 = 有効
Authentication-Use-Idle Timeout	Y	50	整数	シングル	1 ~ 35791394 分

サポートされる RADIUS 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Authorization-DN-Field	Y	67	文字列	シングル	有効な値 : UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
Authorization-Required		66	整数	シングル	0 = いいえ 1 = はい
Authorization-Type	Y	65	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	15	文字列	シングル	Cisco VPN リモートアクセスセッション (IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL) に対して表示されるバナー文字列
Banner2	Y	36	文字列	シングル	Cisco VPN リモートアクセスセッション (IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL) に対して表示されるバナー文字列。 Banner2 文字列は Banner1 文字列に連結されます (設定されている場合)。
Cisco-IP-Phone-Bypass	Y	51	整数	シングル	0 = 無効 1 = 有効
Cisco-LEAP-Bypass	Y	75	整数	シングル	0 = 無効 1 = 有効

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
クライアントタイプ	Y	150	整数	シングル	1 = Cisco VPN Client (IKEv1) 2 = AnyConnect Client SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = AnyConnect Client IPsec VPN (IKEv2)
Client-Type-Version-Limiting	Y	77	文字列	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	文字列	シングル	IP アドレス
Extended-Authentication-On-Relay	Y	122	整数	シングル	0 = 無効 1 = 有効
Framed-Interface-Id	Y	96	文字列	シングル	割り当てられた IPv6 インターフェイス ID。完全に割り当てられた IPv6 アドレスを作成するために、Framed-IPv6-Prefix と組み合わせます。例： Framed-Interface-ID=1:1:1:1 と Framed-IPv6-Prefix=2001:0db8: を組み合わせると、IP アドレス 2001:0db8::1:1:1:1 が得られます。

サポートされる RADIUS 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Framed-IPv6-Prefix	Y	97	文字列	シングル	<p>割り当てられた IPv6 プレフィックスと長さ。完全に割り当てられた IPv6 アドレスを作成するために、Framed-Interface-Id と組み合わせます。例：プレフィックス 2001:0db8::/64 と Framed-Interface-Id=1:1:1:1 を組み合わせると、IP アドレス 2001:0db8::1:1:1:1 が得られます。この属性を使用し、プレフィックス長 /128 の完全な IPv6 アドレスを割り当てて、Framed-Interface-Id を使用せずに IP アドレスを割り当てることができます。例： Framed-Interface-Id=2001:0db8::/128</p>

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Group-Policy	Y	25	文字列	シングル	リモートアクセス VPN セッションのグループポリシーを設定します。 バージョン 8.2.x 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の形式のいずれかを使用できます。 <ul style="list-style-type: none"> • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名;
IE-Proxy-Bypass-Local		83	整数	シングル	0 = なし 1 = ローカル
IE-Proxy-Exception-List		82	文字列	シングル	改行 (\n) 区切りの DNS ドメインのリスト
IE-Proxy-PAC-URL	Y	133	文字列	シングル	PAC アドレス文字列
IE-Proxy-Server		80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy		81	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検出 4 = コンセントレータ設定を使用する
IKE-Keep-Alive-Interval	Y	68	整数	シングル	10 ~ 300 秒
IKE-Keep-Alive-Retry-Interval	Y	84	整数	シングル	2 ~ 10 秒
IKE-Keep-Alive	Y	41	ブール	シングル	0 = 無効 1 = 有効

サポートされる RADIUS 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
InterceptDHCPConfigureMsg	Y	62	ブール	シングル	0 = 無効 1 = 有効
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = 無効 1 = 有効
IPsec-Authentication		13	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP (認可のみ) 3 = NT ドメイン 4 = SDI 5 = 内部 6 = RADIUS での Expiry 認証 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = 無効 1 = 有効
IPsec-Backup-Server-List	Y	60	文字列	シングル	サーバアドレス (スペース区切り)
IPsec-Backup-Servers	Y	59	文字列	シングル	1 = クライアントが設定したリストを使用する 2 = クライアントリストをディセーブルにして消去する 3 = バックアップサーバリストを使用する
IPsec-Client-Firewall-File-Name		57	文字列	シングル	クライアントにファイアウォールポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-File-Optional	Y	58	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	28	文字列	シングル	クライアントに送信するデフォルトドメイン名を 1 つだけ指定します (1 ~ 255 文字)。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-IKE-Peer-ID-Check	Y	40	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	39	整数	シングル	0 = 無効 1 = 有効
IPsec-Mode-Config	Y	31	ブール	シングル	0 = 無効 1 = 有効
IPsec-Over-UDP	Y	34	ブール	シングル	0 = 無効 1 = 有効
IPsec-Over-UDP-Port	Y	35	整数	シングル	4001 ~ 49151。デフォルトは 10000 です。
IPsec-Remote-Auth-CP	Y	56	整数	シングル	0 = なし 1 = リモート FW Are-You-There (AYT) で定義されているポリシー 2 = Policy pushed CPP 4 = サーバからのポリシー
IPsec-Sec-Association		12	文字列	シングル	セキュリティアソシエーションの名前
IPsec-Split-DNS-Names	Y	29	文字列	シングル	クライアントに送信するセカンダリドメイン名のリストを指定します (1 ~ 255 文字)。
IPsec-Split-Tunneling-Policy	Y	55	整数	シングル	0 = スプリットトンネリングなし 1 = スプリットトンネリング 2 = ローカル LAN を許可

サポートされる RADIUS 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-Split-Tunnel-List	Y	27	文字列	シングル	スプリットトンネルの包含リストを記述したネットワークまたは ACL の名前を指定します。
IPsec-Tunnel-Type	Y	30	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	ブール	シングル	0 = 無効 1 = 有効
IPv6-Address-Pools	Y	218	文字列	シングル	IP ローカルプール IPv6 の名前
IPv6-VPN-Filter	Y	219	文字列	シングル	ACL 値
L2TP-Encryption		21	整数	シングル	ビットマップ: 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
L2TP-MPPC-Compression		38	整数	シングル	0 = 無効 1 = 有効
Member-Of	Y	145	文字列	シングル	カンマ区切りの文字列。例: Engineering, Sales ダイナミックアクセスポリシーで使用できる管理属性。グループポリシーは設定されません。
MS-Client-Subnet-Mask	Y	63	ブール	シングル	IP アドレス
NAC-Default-ACL		92	文字列		ACL

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
NAC-Enable		89	整数	シングル	0=いいえ 1=はい
NAC-Revalidation-Timer		91	整数	シングル	300 ~ 86400 秒
NAC-Settings	Y	141	文字列	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	整数	シングル	30 ~ 1800 秒
PerfctForwardSecrecyEnable	Y	88	ブール	シングル	0=いいえ 1=はい
PPTP-Encryption		20	整数	シングル	ビットマップ: 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
PPTP-MPPC-Compression		37	整数	シングル	0 = 無効 1 = 有効
Primary-DNS	Y	5	文字列	シングル	IP アドレス
Primary-WINS	Y	7	文字列	シングル	IP アドレス
Privilege-Level	Y	220	整数	シングル	0 ~ 15 の整数。
Required-Client-Firewall-Vendor-Code	Y	45	整数	シングル	1 = Cisco Systems (Cisco Integrated Client を使用) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems (Cisco Intrusion Prevention Security Agent を使用)
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
RequireFirewallAuth	Y	46	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client (CIC) Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
RequireIndividualUserAuth	Y	49	整数	シングル	0 = 無効 1 = 有効
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = 無効 1 = 有効
Secondary-DNS	Y	6	文字列	シングル	IP アドレス
Secondary-WINS	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment		9	整数	シングル	未使用
Session Subtype	Y	152	整数	シングル	0 = なし 1 = クライアントレス 2 = クライアント 3 = クライアントのみ Session Subtype が適用されるのは、Session Type (151) 属性の値が 1、2、3、または 4 の場合のみです。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Session Type	Y	151	整数	シングル	0 = なし 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN (IKEv2) 3 = クライアントレス SSL VPN 4 = クライアントレス電子メールプロキシ 5 = Cisco VPN Client (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロードバランシング
Simultaneous-Logins	Y	2	整数	シングル	0-2147483647
Smart-Tunnel	Y	136	文字列	シングル	スマートトンネルの名前
Smart-Tunnel-Auto	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動スタート
Smart-Tunnel-Auto-Signon-Enable	Y	139	文字列	シングル	ドメイン名が付加された Smart Tunnel Auto Signon リストの名前
Strip-Realm	Y	135	ブール	シングル	0 = 無効 1 = 有効
SVC-Ask	Y	131	文字列	シングル	0 = ディセーブル 1 = イネーブル 3 = デフォルトサービスをイネーブルにする 5 = デフォルトクライアントレスをイネーブルにする (2 と 4 は使用しない)
SVC-Ask-Timeout	Y	132	整数	シングル	5 ~ 120 秒

サポートされる RADIUS 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
SVC-DPD-Interval-Client	Y	108	整数	シングル	0 = オフ 5 ~ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	整数	シングル	0 = オフ 5 ~ 3600 秒
SVC-DTLS	Y	123	整数	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	整数	シングル	0 = オフ 15 ~ 600 秒
SVC-Modules	Y	127	文字列	シングル	文字列 (モジュールの名前)
SVC-MTU	Y	125	整数	シングル	MTU 値 256 ~ 1406 バイト
SVC-Profiles	Y	128	文字列	シングル	文字列 (プロファイルの名前)
SVC-Rekey-Time	Y	110	整数	シングル	0 = ディセーブル 1 ~ 10080 分
Tunnel Group Name	Y	146	文字列	シングル	1 ~ 253 文字
Tunnel-Group-Lock	Y	85	文字列	シングル	トンネルグループの名前または「none」
Tunneling-Protocols	Y	11	整数	シングル	1 = PPTP 2 = L2TP 4 = IPsec (IKEv1) 8 = L2TP/IPsec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 と 4 は相互排他。0 ~ 11、16 ~ 27、32 ~ 43、48 ~ 59 は有効な値。
Use-Client-Address		17	プール	シングル	0 = 無効 1 = 有効
VLAN	Y	140	整数	シングル	0 ~ 4094
WebVPN-Access-List	Y	73	文字列	シングル	アクセスリスト名
WebVPN ACL	Y	73	文字列	シングル	デバイスの WebVPN ACL 名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-ActiveX-Relay	Y	137	整数	シングル	0 = 無効 その他 = 有効
WebVPN-Apply-ACL	Y	102	整数	シングル	0 = 無効 1 = 有効
WebVPN-Auto-HTTPS-Conn	Y	124	文字列	シングル	予約済み
WebVPN-Cisco-Forms-Enable	Y	101	整数	シングル	0 = 無効 1 = 有効
WebVPN-Cross-File-Params	Y	69	整数	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメージ 8 = イメージに含まれるクッキー
WebVPN-Customization	Y	113	文字列	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	文字列	シングル	URL (たとえば http://example.com)
WebVPN-Deny-Message	Y	116	文字列	シングル	有効な文字列 (500文字以内)
WebVPN-Download-Max-Size	Y	157	整数	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	整数	シングル	0 = 無効 1 = 有効
WebVPN-File-Save-Downing-Enable	Y	96	整数	シングル	0 = 無効 1 = 有効
WebVPN-File-Save-Entry-Enable	Y	95	整数	シングル	0 = 無効 1 = 有効
WebVPN-Global-HTTPS-Exclude	Y	78	文字列	シングル	オプションのワイルドカード (*) を使用したカンマ区切りのDNS/IP (たとえば、*.cisco.com、192.168.1.*、wwwin.cisco.com)
WebVPN-Hidden-Shares	Y	126	整数	シングル	0 = なし 1 = 表示される

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-HomePageSmart	Y	228	ブール	シングル	クライアントレスホームページをスマートトンネル経由で表示する場合にイネーブルにします。
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ 8 = クッキー
WebVPN-HTTP-Compression	Y	120	整数	シングル	0 = オフ 1 = デフォルト圧縮
WebVPN-HTTP-Proxy-Path	Y	74	文字列	シングル	http= または https= プレフィックス付きの、カンマ区切りの DNS/IP:ポート (例 : http=10.10.10.10:80、https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert	Y	148	整数	シングル	0 ~ 30。0 = デイセーブル。
WebVPN-Keepalive-Ignore	Y	121	整数	シングル	0 ~ 900
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。
WebVPN-Port-Forwarding-Enable	Y	97	整数	シングル	0 = 無効 1 = 有効
WebVPN-Port-Forwarding-Enable	Y	98	整数	シングル	0 = 無効 1 = 有効
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	整数	シングル	0 = 無効 1 = 有効
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Forwarding-Name	Y	79	文字列	シングル	名前の文字列（例、「Corporate-Apps」）。このテキストでクライアントレスポータル ホームページのデフォルト文字列「Application Access」が置き換えられます。
WebVPN-Post-Max-Size	Y	159	整数	シングル	0x7fffffff
WebVPN-Smart-Tunnel-Auth-Interval	Y	149	整数	シングル	0 ～ 30。0 = デイセーブブル。
WebVPN-Smart-Tunnel-Auth-Interval	Y	225	ブール	シングル	0 = 無効1 = 有効
WebVPN-Smart-Tunnel-Name	Y	136	文字列	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auth-Interval	Y	139	文字列	シングル	ドメイン名が付加されたスマートトンネル自動サインオンリストの名前
WebVPN-Smart-Tunnel-Auth-Interval	Y	138	整数	シングル	0 = 無効1 = 有効2 = 自動スタート

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPNStorage-Filter	Y	227	文字列	シングル	「e ネットワーク名」、「i ネットワーク名」、「a」のいずれか。ここで、ネットワーク名は、スマートトンネルネットワークのリストの名前です。e はトンネルが除外されることを示し、i はトンネルが指定されることを示し、a はすべてのトンネルを示します。
WebVPNSSLVPNClient-Enable	Y	103	整数	シングル	0 = 無効 1 = 有効
WebVPNSSLVPNClient-Keep-Installation	Y	105	整数	シングル	0 = 無効 1 = 有効
WebVPNSSLVPNClient-Require	Y	104	整数	シングル	0 = 無効 1 = 有効
WebVPNSSO-Save-Name	Y	114	文字列	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	文字列	シングル	
WebVPN-Storage-Objects	Y	161	文字列	シングル	
WebVPNSVCKeepalive-Timeout	Y	107	整数	シングル	15 ~ 600 秒、0 = オフ
WebVPNSVCClient-Idle-Timeout	Y	108	整数	シングル	5 ~ 3600 秒、0 = オフ
WebVPNSVCDILSEnable	Y	123	整数	シングル	0 = 無効 1 = 有効
WebVPNSVCDILSMTU	Y	125	整数	シングル	MTU 値は 256 ~ 1406 バイトです。
WebVPNSVCGroup-Idle-Timeout	Y	109	整数	シングル	5 ~ 3600 秒、0 = オフ
WebVPNSVCRetry-Time	Y	110	整数	シングル	4 ~ 10080 分、0 = オフ

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-SVC-Radius-Method	Y	111	整数	シングル	0 (オフ)、1 (SSL)、2 (新しいトンネル)
WebVPN-SVC-Compression	Y	112	整数	シングル	0 (オフ)、1 (デフォルトの圧縮)
WebVPN-UNIX-Group-ID (GID)	Y	222	整数	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	整数	シングル	UNIX での有効なユーザ ID
WebVPN-Upload-Max-Size	Y	158	整数	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	整数	シングル	0 = 無効 1 = 有効
WebVPN-URL-List	Y	71	文字列	シングル	URL リスト名
WebVPN-User-Storage	Y	160	文字列	シングル	
WebVPN-VDI	Y	163	文字列	シングル	設定のリスト

サポートされる IETF RADIUS 認証属性

次の表に、サポートされる IETF RADIUS 属性の一覧を示します。

表 37: サポートされる IETF RADIUS 属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Class	Y	25		シングル	バージョン 8.2.x 以降では、Group-Policy 属性 (VSA 3076、#25) を使用することをお勧めします。 <ul style="list-style-type: none"> • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名
IETF-Radius-Filter-Id	Y	11	文字列	シングル	フル トンネルの IPsec クライアントと SSL VPN クライアントのみに適用される、ASA で定義された ACL 名。
IETF-Radius-Framed-IP-Address	Y	n/a	文字列	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	n/a	文字列	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	28	整数	シングル	Seconds

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Service-Type	Y	6	整数	シングル	秒。使用可能なサービスタイプの値： <ul style="list-style-type: none"> • Administrative : ユーザは <code>configure</code> プロンプトへのアクセスを許可されています。 • .NAS-Prompt : ユーザは <code>exec</code> プロンプトへのアクセスを許可されています。 • .remote-access : ユーザはネットワークアクセスを許可されています。
IETF-Radius-Session-Timeout	Y	27	整数	シングル	Seconds

RADIUS アカウンティング切断の理由コード

これらのコードは、パケットを送信するときに ASA が切断された場合に返されます。

切断の理由コード

ACCT_DISC_USER_REQ = 1

ACCT_DISC_LOST_CARRIER = 2

ACCT_DISC_LOST_SERVICE = 3

ACCT_DISC_IDLE_TIMEOUT = 4

ACCT_DISC_SESS_TIMEOUT = 5

ACCT_DISC_ADMIN_RESET = 6

切断の理由コード

ACCT_DISC_ADMIN_REBOOT = 7

ACCT_DISC_PORT_ERROR = 8

ACCT_DISC_NAS_ERROR = 9

ACCT_DISC_NAS_REQUEST = 10

ACCT_DISC_NAS_REBOOT = 11

ACCT_DISC_PORT_UNNEEDED = 12

ACCT_DISC_PORT_PREEMPTED = 13

ACCT_DISC_PORT_SUSPENDED = 14

ACCT_DISC_SERV_UNAVAIL = 15

ACCT_DISC_CALLBACK = 16

ACCT_DISC_USER_ERROR = 17

ACCT_DISC_HOST_REQUEST = 18

ACCT_DISC_ADMIN_SHUTDOWN = 19

ACCT_DISC_SA_EXPIRED = 21

ACCT_DISC_MAX_REASONS = 22

AAA の RADIUS サーバのガイドライン

ここでは、AAA 用の RADIUS サーバを設定する前に確認する必要があるガイドラインおよび制限事項について説明します。

- シングルモードで最大 100 個のサーバグループ、またはマルチモードでコンテキストごとに 4 つのサーバグループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 4 台のサーバを含めることができます。

IPv6

AAA サーバは IPv4 アドレスを使用する必要がありますが、エンドポイントは IPv6 を使用できます。

AAA 用の RADIUS サーバの設定

ここでは、AAA 用に RADIUS サーバを設定する方法について説明します。

手順

-
- ステップ 1** ASA の属性を RADIUS サーバにロードします。属性をロードするために使用する方法は、使用している RADIUS サーバのタイプによって異なります。
- Cisco ACS を使用している場合：サーバには、これらの属性がすでに統合されています。したがって、この手順をスキップできます。
 - 他のベンダーの RADIUS サーバ（たとえば Microsoft Internet Authentication Service）の場合：ASA の各属性を手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダーコード（3076）を使用します。
- ステップ 2** [RADIUS サーバグループの設定（855 ページ）](#)。
- ステップ 3** [グループへの RADIUS サーバの追加（858 ページ）](#)。
- ステップ 4**（任意） [認証プロンプトの追加（860 ページ）](#)。
-

RADIUS サーバグループの設定

認証、許可、またはアカウントिंगに外部 RADIUS サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの RADIUS サーバグループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。

手順

-
- ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。
- ステップ 2** [AAA Server Group] 領域で、[Add] をクリックします。
[Add AAA Server Group] ダイアログボックスが表示されます。
- ステップ 3** [Server Group] フィールドにグループの名前を入力します。
- ステップ 4** [Protocol] ドロップダウンリストから RADIUS サーバタイプを選択します。
- ステップ 5** [Accounting Mode] を選択します。
- [Simultaneous]：グループ内のすべてのサーバにアカウントングデータを送信します。
 - [Single]：1 つのサーバにだけアカウントングデータを送信します。
- ステップ 6** グループ内で障害の発生したサーバを再度アクティブ化する方法 ([Reactivation Mode]) を設定します。

- [Depletion]、[Dead Time] : グループ内のすべてのサーバが非アクティブになった後に、障害の発生したサーバを再度アクティブ化します。これがデフォルトの再アクティブ化モードです。グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を 0 ~ 1440 分の範囲で指定します。デフォルトは 10 分です。
- [timed] : 30 秒のダウン時間の後、障害が発生したサーバを再度アクティブ化します。

ステップ 7 [Max Failed Attempts] で、次のサーバを試す前にグループ内の RADIUS サーバでの AAA トランザクションの失敗の最大数を指定します。

範囲は、1 ~ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定すると、グループ内のすべてのサーバが応答しない場合にグループは応答なしと見なされ、フォールバック方式が試行されます。サーバグループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間続くと（デフォルトの再アクティブ化モードとデッド時間を使用する場合）、ただちにフォールバック方式が使用されます。非応答時間をデフォルト値から変更するには、[Dead Time] の変更方法を参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバにアクセスしようとしています。

ステップ 8 （任意）適切なオプションを選択して、RADIUS 中間アカウント更新メッセージの定期的な生成をイネーブルにします。

これらのオプションが関連するのは、このサーバグループを AnyConnect またはクライアントレス SSL VPN に使用している場合のみです。

- [Enable interim accounting update] : [Update Interval] オプションを選択せずにこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときにのみ中間アカウント更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウント更新メッセージが生成されます。
- [Update Interval] : 対象のサーバグループにアカウント更新メッセージを送信するように設定されたすべての VPN セッションのアカウント更新メッセージの定期的な生成と伝送をイネーブルにします。これらの更新を送信する間隔を時間単位で変更できます。デフォルトは 24 時間で、指定できる範囲は 1 ~ 120 です。

(注) ISE サーバが含まれるサーバグループには、両方のオプションを選択します。ISE は、ASA などの NAS デバイスから受信するアカウント更新メッセージに基づいて、アクティブセッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知（アカウント更新メッセージまたはポスチャ トランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブセッションについて ISE に定期的に中間アカウント更新メッセージを送信するように、グループを設定します。

ステップ 9 (任意) このグループに AD エージェントまたは Cisco Directory Agent (CDA) サーバしか含まれていない場合は、[Enable Active Directory Agent Mode] を選択します。

CDA または AD エージェントはアイデンティティ ファイアウォールで使用されるサーバであり、完全な機能を備えた RADIUS サーバではありません。このオプションを選択すると、このグループをアイデンティティ ファイアウォール専用として使用できます。

ステップ 10 (任意) このサーバグループをリモートアクセス VPN で ISE ポリシーを適用するために使用する場合、次のオプションを設定します。

- [Enable dynamic authorization] : AAA サーバグループの RADIUS の動的認可 (ISE 許可変更、CoA) サービスをイネーブルにします。VPN トンネルでサーバグループを使用すると、対応する RADIUS サーバグループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。このサーバグループを ISE と併せてリモートアクセス VPN で使用する場合にのみ動的認可をイネーブルにします。

- [Dynamic Authorization Port] : 動的認可をイネーブルにする場合、RADIUS CoA 要求のリスニングポートを指定できます。デフォルト値は 1700 です。有効な範囲は 1024 ~ 65535 です。

- [Use authorization only mode] : 認証に ISE を使用しない場合は、RADIUS サーバグループに対し認可専用モードをイネーブルにします。これは、サーバグループを認可に使用するときに、RADIUS アクセス要求メッセージが、AAA サーバ用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。RADIUS サーバの共通パスワードを設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバグループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウンティングにこのサーバグループを使用する可能性があるからです。

ステップ 11 (任意) [VPN3K Compatibility Option] を設定して、RADIUS パケットから受信したダウンロード可能 ACL を Cisco AV ペアの ACL と結合するかどうかを指定します。

このオプションは、VPN 接続にのみ適用されます。VPN ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

- [Do not merge] : ダウンロード可能 ACL は Cisco AV ペアの ACL と結合されません。AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。これがデフォルトのオプションです。

- **Place the downloadable ACL after Cisco AV-pair ACL**

- **Place the downloadable ACL before Cisco AV-pair ACL**

ステップ 12 [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバグループが [AAA Server Groups] テーブルに追加されます。

ステップ 13 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

グループへの RADIUS サーバの追加

RADIUS サーバをグループに追加するには、次の手順を実行します。

手順

- ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択し、[AAA Server Groups] 領域で、サーバを追加するサーバグループをクリックします。
- ステップ 2 [Servers in the Selected Group] 領域（下側のペイン）で、[Add] をクリックします。
サーバグループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。
- ステップ 3 認証サーバが存在するインターフェイス名を選択します。
- ステップ 4 グループに追加するサーバのサーバ名または IP アドレスを追加します。
- ステップ 5 サーバへの接続試行のタイムアウト値を指定します。
サーバのタイムアウト間隔（1～300 秒）を指定します。デフォルトは 10 秒です。各 AAA トランザクションに対して、タイムアウトに達するまで（再試行間隔に基づいて）ASA による接続の再試行が行われます。連続して失敗したトランザクションの数が AAA サーバグループ内の指定された **maximum-failed-attempts** 制限に達すると、AAA サーバは非アクティブ化され、ASA は別の AAA サーバ（設定されている場合）への要求の送信を開始します。
- ステップ 6 ダウンロード可能な ACL で受信されたネットマスクを ASA でどのように処理するかを指定します。次のオプションから選択します。
- [Detect automatically] : ASA で、使用されているネットマスク表現のタイプが判定されます。ASA は、ワイルドカードネットマスク表現を検出した場合、標準ネットマスク表現に変換します。
(注) 一部のワイルドカード表現は明確な検出が困難なため、この設定を選択した場合には、ワイルドカードネットマスク表現が誤って標準ネットマスク表現として検出されることもあります。
 - [Standard] : ASA は、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現のみが含まれていると見なします。ワイルドカードネットマスク表現からの変換は実行されません。
 - [Wildcard] : ASA は、RADIUS サーバから受信したダウンロード可能 ACL に、ワイルドカードネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。

- ステップ 7** この ASA を介して RADIUS 認可サーバにアクセスするユーザに共通のパスワードを指定します。このパスワードは大文字と小文字が区別されます。この情報は、RADIUS サーバ管理者に伝えてください。
- (注) RADIUS 認証サーバ (認可サーバではない) に対しては、共通のパスワードは設定しないでください。
- このフィールドを空白のままにした場合は、RADIUS 認可サーバにアクセスする際のパスワードには、各ユーザ名が使用されます。
- RADIUS 認可サーバを認証に使用することは避けてください。共通パスワードやユーザ名を転用したパスワードは、ユーザごとに一意のパスワードに比べ、安全性が低くなります。
- このパスワードは、RADIUS プロトコルや RADIUS サーバによって要求されますが、ユーザが知っている必要はありません。
- ステップ 8** 二重認証を使用し、トンネルグループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしていない場合、このチェックボックスをオンにすれば、そのサーバから非 MS-CHAPv2 認証要求が送信されるようになります。
- ステップ 9** ASA からサーバへ接続を試行した後、次に試行するまでの待機時間を、1 ~ 10 秒の間で指定します。
- (注) RADIUS プロトコルの場合、サーバが ICMP ポート到達不能メッセージで応答すると、再試行間隔の設定が無視され、AAA サーバはただちに障害状態になります。このサーバが AAA グループ内の唯一のサーバである場合は、サーバが再アクティブ化され、別の要求がサーバに送信されます。これは意図された動作です。
- ステップ 10** [Simultaneous] または [Single] をクリックします。
- [Single] モードの場合、ASA ではアカウントिंग データが 1 つのサーバにだけ送信されます。
- [Simultaneous] モードの場合、ASA ではアカウントिंग データがグループ内のすべてのサーバに送信されます。
- ステップ 11** ユーザのアカウントिंगに使用するサーバポートを指定します。デフォルトのポートは 1646 です。
- ステップ 12** ユーザの認証に使用するサーバポートを指定します。デフォルトのポートは 1645 です。
- ステップ 13** ASA で RADIUS サーバを認証する際に使用される共有秘密キーを指定します。設定したサーバ秘密キーは、RADIUS サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーが不明の場合は、RADIUS サーバの管理者に問い合わせてください。最大フィールド長は、64 文字です。
- ステップ 14** [OK] をクリックします。
- [Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバが AAA サーバグループに追加されます。

- ステップ 15** [AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

認証プロンプトの追加

RADIUS サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジテキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワードプロンプトの上に表示されます。認証プロンプトを指定しなかった場合は、ユーザが RADIUS サーバで認証中に以下の内容が表示されます。

Connection Type	デフォルトのプロンプト
FTP	FTP authentication
HTTP	HTTP 認証
Telnet	なし

認証プロンプトを追加するには、次の手順を実行します。

手順

- ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt] の順に選択します。
- ステップ 2** ログイン時にユーザ名とパスワードプロンプトの上に表示するメッセージとして追加するテキストを、[Prompt] フィールドに入力します。

次の表に、認証プロンプトの文字数制限を示します。

アプリケーション	文字制限
Microsoft Internet Explorer	37
Telnet	235
FTP	235

- ステップ 3** [User accepted message] フィールドと [User rejected message] フィールドにメッセージを追加します。

Telnet からのユーザ認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証の試みが RADIUS サーバによって承認または拒否されたことを示す、異なる状態のプロンプトを表示できます。

これらのメッセージテキストをそれぞれ指定した場合、ASA では、RADIUS サーバにより認証されたユーザに対しては [User accepted message] テキストが表示され、認証されなかったユー

ザに対しては ASA により [User rejected message] テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジテキストのみが表示されます。ユーザ承認メッセージテキストおよびユーザ拒否メッセージテキストは表示されません。

ステップ 4 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

RADIUS サーバの認証および認可のテスト

ASA が RADIUS サーバに接続してユーザを認証または承認できるかどうかを判別するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] の順に選択します。

ステップ 2 サーバが [AAA Server Groups] テーブル内に存在するサーバグループをクリックします。

ステップ 3 [Servers in the Selected Group] テーブルでテストするサーバをクリックします。

ステップ 4 [Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 5 実行するテストのタイプ ([Authentication] または [Authorization]) をクリックします。

ステップ 6 ユーザ名を入力します。

ステップ 7 認証をテストする場合は、ユーザ名に対応するパスワードを入力します。

ステップ 8 [OK] をクリックします。

認証または認可のテストメッセージが ASA からサーバへ送信されます。テストが失敗した場合は、エラーメッセージが表示されます。

AAA 用の RADIUS サーバのモニタリング

AAA 用の RADIUS サーバのステータスのモニタリングについては、次のコマンドを参照してください。

- [Monitoring] > [Properties] > [AAA Servers]

このペインには、RADIUS サーバの実行コンフィギュレーションが表示されます。

- [Tools] > [Command Line Interface]

このペインでは、さまざまな非インタラクティブコマンドを発行し、結果を表示することができます。

AAA 用の RADIUS サーバの履歴

表 38: AAA 用の RADIUS サーバの履歴

機能名	プラットフォーム リリース	説明
AAA の RADIUS サーバ	7.0(1)	AAA 用の RADIUS サーバを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]
ASA からの RADIUS アクセス要求パケットおよびアカウントिंग要求パケットでの主なベンダー固有属性 (VSA) の送信	8.4(3)	4 つの新しい VSA : Tunnel Group Name (146) および Client Type (150) は、ASA からの RADIUS アクセス要求パケットで送信されます。Session Type (151) および Session Subtype (152) は、ASA からの RADIUS アカウントING要求パケットで送信されます。4 つのすべての属性が、すべてのアカウントING要求パケットタイプ (開始、中間アップデート、および終了) に送信されます。RADIUS サーバ (ACS や ISE など) は、認可属性やポリシー属性を強制適用したり、アカウントINGや課金のためにそれらの属性を使用したりできます。



第 34 章

AAA 用の TACACS+ サーバ

この章では、AAA で使われる TACACS+ サーバの設定方法について説明します。

- [AAA 用の TACACS+ サーバについて \(863 ページ\)](#)
- [AAA 用の TACACS+ サーバのガイドライン \(865 ページ\)](#)
- [TACACS+ サーバの設定 \(865 ページ\)](#)
- [TACACS+ サーバの認証および許可のテスト \(869 ページ\)](#)
- [AAA 用の TACACS+ サーバのモニタリング \(869 ページ\)](#)
- [AAA 用の TACACS+ サーバの履歴 \(870 ページ\)](#)

AAA 用の TACACS+ サーバについて

ASA は、ASCII、PAP、CHAP、MS-CHAPv1 の各プロトコルで TACACS+ サーバ認証をサポートします。

TACACS+ 属性

Cisco ASA は、TACACS+ 属性をサポートします。TACACS+ 属性は、認証、許可、アカウントिंगの機能を分離します。プロトコルでは、必須とオプションの2種類の属性をサポートします。サーバとクライアントの両方で必須属性を解釈できる必要があります。また、必須属性はユーザに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。



(注) TACACS+ 属性を使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認してください。

次の表に、カットスループロキシ接続に対してサポートされる TACACS+ 許可応答属性の一覧を示します。

表 39: サポートされる TACACS+ 許可応答属性

属性	説明
acl	接続に適用する、ローカルで設定済みの ACL を識別します。
idletime	認証済みユーザセッションが終了する前に許可される非アクティブ時間 (分) を示します。
timeout	認証済みユーザセッションが終了する前に認証クレデンシャルがアクティブな状態である絶対時間 (分) を指定します。

次の表に、サポートされる TACACS+ アカウンティング属性の一覧を示します。

。

表 40: サポートされる TACACS+ アカウンティング属性

属性	説明
bytes_in	この接続中に転送される入力バイト数を指定します (ストップレコードのみ)。
bytes_out	この接続中に転送される出力バイト数を指定します (ストップレコードのみ)。
cmd	実行するコマンドを定義します (コマンドアカウンティングのみ)。
disc-cause	切断理由を特定する数字コードを示します (ストップレコードのみ)。
elapsed_time	接続の経過時間 (秒) を定義します (ストップレコードのみ)。
foreign_ip	トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティインターフェイスでカットスループロキシ接続のアドレスを定義します。
local_ip	トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティインターフェイスでカットスループロキシ接続のアドレスを定義します。
NAS port	接続のセッション ID が含まれます。

属性	説明
packs_in	この接続中に転送される入力パケット数を指定します。
packs_out	この接続中に転送される出力パケット数を指定します。
priv-level	コマンド アカウンティング要求の場合はユーザの権限レベル、それ以外の場合は 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。
service	使用するサービスを指定します。コマンド アカウンティングの場合にのみ、常に「shell」に設定されます。
task_id	アカウンティング トランザクションに固有のタスク ID を指定します。
username	ユーザの名前を示します。

AAA 用の TACACS+ サーバのガイドライン

ここでは、AAA 用の TACACS+ サーバを設定する前に確認する必要があるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバは IPv4 アドレスを使用する必要がありますが、エンドポイントは IPv6 を使用できます。

その他のガイドライン

- シングルモードで最大 100 個のサーバグループ、またはマルチモードでコンテキストごとに 4 つのサーバグループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 4 台のサーバを含めることができます。

TACACS+ サーバの設定

ここでは、TACACS+ サーバを設定する方法について説明します。

手順

-
- ステップ 1 TACACS+ サーバグループの設定 (866 ページ)。
 - ステップ 2 グループへの TACACS+ サーバの追加 (867 ページ)。
 - ステップ 3 (任意) 認証プロンプトの追加 (868 ページ)。
-

TACACS+ サーバグループの設定

認証、許可、アカウントिंगに TACACS+ サーバを使用する場合は、まず TACACS+ サーバグループを少なくとも 1 つ作成し、各グループに 1 台以上のサーバを追加する必要があります。TACACS+ サーバグループは名前でも識別されます。

TACACS+ サーバグループを追加するには、次の手順を実行します。

手順

-
- ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。
 - ステップ 2 [AAA Server Group] 領域で、[Add] をクリックします。
[Add AAA Server Group] ダイアログボックスが表示されます。
 - ステップ 3 [Server Group] フィールドにグループの名前を入力します。
 - ステップ 4 [Protocol] ドロップダウンリストから、[TACACS+] サーバタイプを選択します。
 - ステップ 5 [Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。
[Single] モードの場合、ASA ではアカウントングデータが 1 つのサーバにだけ送信されます。
[Simultaneous] モードの場合、ASA ではアカウントングデータがグループ内のすべてのサーバに送信されます。
 - ステップ 6 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。
[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバが非アクティブになった場合、そのサーバは、グループの他のすべてのサーバが非アクティブになるまで非アクティブのままとなります。すべてのサーバが非アクティブになると、グループ内のすべてのサーバが再アクティブ化されます。このアプローチでは、障害が発生したサーバに起因する接続遅延の発生を最小限に抑えられます。
Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。
 - ステップ 7 [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

- ステップ 8** 許可するサーバでの AAA トランザクションの失敗の最大数を追加します。
- このオプションで設定するのは、応答のないサーバを非アクティブと宣言する前の AAA トランザクションの失敗回数です。
- ステップ 9** [OK] をクリックします。
- [Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバグループが [AAA Server Groups] テーブルに追加されます。
- ステップ 10** [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

グループへの TACACS+ サーバの追加

TACACS+ サーバをグループに追加するには、次の手順を実行します。

手順

- ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。
- ステップ 2** サーバを追加するサーバグループをクリックします。
- ステップ 3** [Servers in the Selected Group] 領域で、[Add] をクリックします。
- サーバグループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。
- ステップ 4** 認証サーバが存在するインターフェイス名を選択します。
- ステップ 5** グループに追加するサーバのサーバ名または IP アドレスを追加します。
- ステップ 6** サーバへの接続試行のタイムアウト値を指定します。
- サーバのタイムアウト間隔 (1 ~ 300 秒) を指定します。デフォルトは 10 秒です。各 AAA トランザクションに対して、タイムアウトに達するまで (再試行間隔に基づいて) ASA による接続の再試行が行われます。連続して失敗したトランザクションの数が AAA サーバグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバは非アクティブ化され、ASA は別の AAA サーバ (設定されている場合) への要求の送信を開始します。
- ステップ 7** サーバポートを指定します。サーバポートは、ポート番号 139、または ASA によって TACACS+ サーバとの通信に使用される TCP ポートの番号です。
- ステップ 8** サーバ秘密キーを指定します。ASA で TACACS+ サーバを認証する際に使用される共有秘密キーを指定します。ここで設定したサーバ秘密キーは、TACACS+ サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーが不明の場合は、TACACS+ サーバの管理者に問い合わせてください。最大フィールド長は、64 文字です。
- ステップ 9** [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバが AAA サーバグループに追加されます。

ステップ 10 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

認証プロンプトの追加

AAA 認証チャレンジプロセスの実行中にユーザに表示するテキストを指定できます。TACACS+ サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジテキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワードプロンプトの上に表示されます。

認証プロンプトを指定しない場合、TACACS+ サーバでの認証時にユーザに対して表示される内容は次のようになります。

Connection Type	デフォルトのプロンプト
FTP	FTP authentication
HTTP	HTTP 認証
Telnet	なし

認証プロンプトを追加するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt] の順に選択します。

ステップ 2 ログイン時にユーザに表示されるユーザ名とパスワードのプロンプトの上に表示するテキストを追加します。

次の表に、認証プロンプトの文字数制限を示します。

アプリケーション	認証プロンプトの文字数制限
Microsoft Internet Explorer	37
Telnet	235
FTP	235

ステップ 3 [User accepted message] フィールドと [User rejected message] フィールドにメッセージを追加します。

Telnet からのユーザ認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証試行が AAA サーバにより受け入れられた、または拒否されたことを示すさまざまな状態のプロンプトを表示できます。

これらのメッセージテキストをそれぞれ指定した場合、ASA では、AAA サーバにより認証されたユーザに対しては [User accepted message] テキストが表示され、認証されなかったユーザに対しては ASA により [User rejected message] テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジテキストのみが表示されます。ユーザ承認メッセージテキストおよびユーザ拒否メッセージテキストは表示されません。

ステップ 4 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

TACACS+ サーバの認証および許可のテスト

ASA が TACACS+ サーバに接続してユーザを認証または承認できるかどうかを判別するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] の順に選択します。

ステップ 2 サーバが存在するサーバグループをクリックします。

ステップ 3 テストするサーバをクリックします。

ステップ 4 [Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 5 実行するテストのタイプ ([Authentication] または [Authorization]) をクリックします。

ステップ 6 ユーザ名を入力します。

ステップ 7 認証をテストする場合は、ユーザ名のパスワードを入力します。

ステップ 8 [OK] をクリックします。

認証または認可のテストメッセージが ASA からサーバへ送信されます。テストが失敗した場合は、エラーメッセージが表示されます。

AAA 用の TACACS+ サーバのモニタリング

AAA 用の TACACS+ サーバのモニタリングについては、次のコマンドを参照してください。

• [Monitoring] > [Properties] > [AAA Servers]

このペインには、設定された TACACS+ サーバの統計情報が表示されます。

- [Tools] > [Command Line Interface]

このペインでは、さまざまな非インタラクティブコマンドを発行し、結果を表示することができます。

AAA 用の TACACS+ サーバの履歴

表 41: AAA 用の TACACS+ サーバの履歴

機能名	プラットフォーム リリース	説明
TACACS+ サーバ	7.0(1)	AAA に TACACS+ サーバを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]。



第 35 章

AAA の LDAP サーバ

この章では、AAA で使用される LDAP サーバの設定方法について説明します。

- [LDAP および ASA について \(871 ページ\)](#)
- [AAA の LDAP サーバのガイドライン \(875 ページ\)](#)
- [AAA の LDAP サーバの設定 \(876 ページ\)](#)
- [LDAP サーバによる認証および許可のテスト \(880 ページ\)](#)
- [AAA の LDAP サーバのモニタリング \(881 ページ\)](#)
- [AAA の LDAP サーバの履歴 \(881 ページ\)](#)

LDAP および ASA について

Cisco ASA はほとんどの LDAPv3 ディレクトリ サーバと互換性があり、それには次のものが含まれます。

- Sun Microsystems JAVA System Directory Server (現在は Oracle Directory Server Enterprise Edition の一部、旧名 Sun ONE Directory Server)
- Microsoft Active Directory
- Novell
- OpenLDAP

デフォルトでは、ASA によって Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP、または汎用 LDAPv3 ディレクトリ サーバに接続しているかどうかは自動検出されます。ただし、LDAP サーバタイプの自動検出による決定が失敗した場合は、手動で設定できます。

LDAP での認証方法

認証中、ASA は、ユーザの LDAP サーバへのクライアント プロキシとして機能し、プレーンテキストまたは Simple Authentication and Security Layer (SASL) プロトコルのいずれかを使って LDAP サーバに対する認証を行います。デフォルトで、ASA は、通常はユーザ名とパスワードである認証パラメータを LDAP サーバにプレーンテキストで渡します。

ASA では、次の SASL メカニズムをサポートしています。次に、強度の低い順番に示します。

- **Digest-MD5** : ASA は、ユーザ名とパスワードから計算した MD5 値を使用して LDAP サーバに応答します。
- **Kerberos** : ASA は、GSSAPI Kerberos メカニズムを使用して、ユーザ名とレムを送信することで LDAP サーバに応答します。

ASA と LDAP サーバは、これらの SASL メカニズムの任意の組み合わせをサポートします。複数のメカニズムを設定した場合、ASA ではサーバに設定されている SASL メカニズムのリストが取得され、認証メカニズムは ASA とサーバの両方に設定されているメカニズムのなかで最も強力なものに設定されます。たとえば、LDAP サーバと ASA の両方がこれら両方のメカニズムをサポートしている場合、ASA は、強力な方の Kerberos メカニズムを選択します。

ユーザ LDAP 認証が成功すると、LDAP サーバは認証されたユーザの属性を返します。VPN 認証の場合、通常これらの属性には、VPN セッションに適用される認可データが含まれます。この場合、LDAP の使用により、認証と許可を 1 ステップで実行できます。



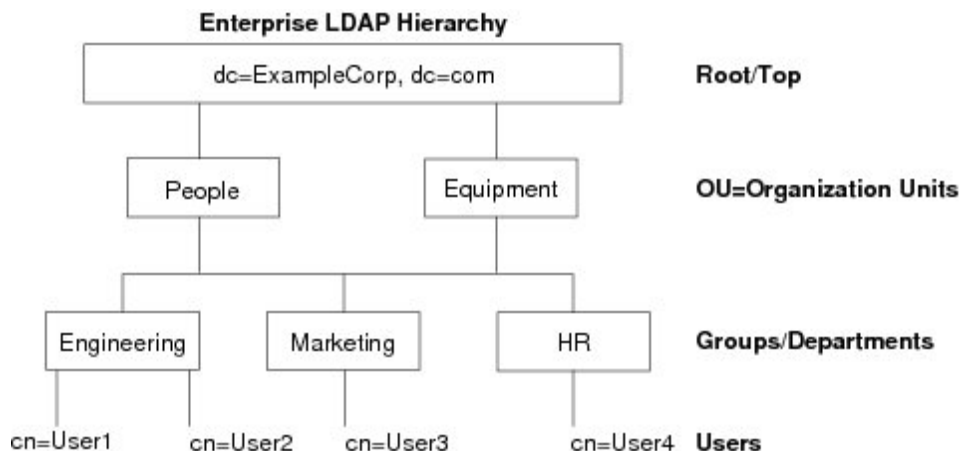
(注) LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP 階層

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Employee1 を例に考えてみます。Employee1 は Engineering グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。たとえば、シングルレベル階層をセットアップします。この中で、Employee1 は Example Corporation のメンバーであると見なされます。あるいは、マルチレベル階層をセットアップします。この中で、Employee1 は Engineering 部門のメンバーであると見なされ、この部門は People という名称の組織ユニットのメンバーであり、この組織ユニットは Example Corporation のメンバーです。マルチレベル階層の例については、次の図を参照してください。

マルチレベル階層の方が詳細ですが、検索結果が速く返されるのはシングルレベル階層の方です。

図 61: マルチレベルの LDAP 階層



LDAP 階層の検索

ASA は、LDAP 階層内での検索を調整できます。ASA に次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドは、ユーザの権限が含まれている部分だけを検索するように階層の検索を限定します。

- **LDAP Base DN** では、サーバが ASA から認可要求を受信したときに LDAP 階層内のどの場所からユーザ情報の検索を開始するかを定義します。
- **Search Scope** では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバによる検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- **Naming Attribute** では、LDAP サーバのエントリを一意に識別する RDN を定義します。一般的な名前属性には、`cn` (一般名)、`sAMAccountName`、および `userPrincipalName` を含めることができます。

次の図に、Example Corporation の LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。次の表に、2 つの検索コンフィギュレーションの例を示します。

最初のコンフィギュレーションの例では、Employee1 が IPSec トンネルを確立するときに LDAP 認可が必要であるため、ASA から LDAP サーバに検索要求が送信され、この中で Employee1 を Engineering グループの中で検索することが指定されます。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、ASA から送信される検索要求の中で、Employee1 を Example Corporation 全体の中で検索することが指定されています。この検索には時間がかかります。

表 42: 検索コンフィギュレーションの例

番号	LDAP Base DN	検索範囲	名前属性	結果
1	group= Employee1,ou=ExampleCorporation, dc=com	1 レベル	cn=Employee1	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Employee1	検索に時間がかかる

LDAP サーバへのバインド

ASA は、ログイン DN とログインパスワードを使用して、LDAP サーバとの信頼（バインド）を築きます。Microsoft Active Directory の読み取り専用操作（認証、許可、グループ検索など）を行うとき、ASA では特権の低いログイン DN でバインドできます。たとえば、Login DN には、AD の「Member Of」の指定が Domain Users の一部であるユーザを指定することができます。VPN のパスワード管理操作では、Login DN にはより高い特権が必要となり、AD の Account Operators グループの一部を指定する必要があります。

次に、Login DN の例を示します。

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA は次の認証方式をサポートしています。

- 暗号化されていないパスワードを使用したポート 389 での簡易 LDAP 認証
- ポート 636 でのセキュアな LDAP (LDAP-S)
- Simple Authentication and Security Layer (SASL) MD5
- SASL Kerberos

ASA は匿名認証をサポートしていません。



(注) LDAP クライアントとしての ASA は、匿名のバインドや要求の送信をサポートしていません。

LDAP 属性マップ

ASA では、次の目的での認証のために LDAP ディレクトリを使用できます。

- VPN リモート アクセス ユーザ
- ファイアウォール ネットワークのアクセス/カットスルー プロキシセッション
- ACL、ブックマーク リスト、DNS または WINS 設定、セッション タイマーなどのポリシーの権限（または許可属性と呼ばれる）の設定

- ローカル グループ ポリシーのキー属性の設定

ASA は、LDAP 属性マップを使用して、ネイティブ LDAP ユーザ属性を Cisco ASA 属性に変換します。それらの属性マップを LDAP サーバにバインドしたり、削除したりすることができます。また、属性マップを表示または消去することもできます。

LDAP 属性マップは複数値属性をサポートしません。たとえば、あるユーザが複数の AD グループのメンバで、LDAP 属性マップが複数のグループと一致する場合、選択される値は一致するエントリのアルファベット順に基づくものです。

属性マッピング機能を適切に使用するには、LDAP 属性の名前と値およびユーザ定義の属性の名前と値を理解する必要があります。

頻繁にマッピングされる LDAP 属性の名前と、一般にマッピングされるユーザ定義の属性のタイプは次のとおりです。

- IETF-Radius-Class (ASA バージョン 8.2 以降における Group_Policy) : ディレクトリ部門またはユーザグループ (たとえば、Microsoft Active Directory memberOf) 属性値に基づいてグループポリシーを設定します。ASDM バージョン 6.2/ASA バージョン 8.2 以降では、IETF-Radius-Class 属性の代わりに group-policy 属性が使用されます。
- IETF-Radius-Filter-Id : VPN クライアント、IPSec、SSL に対するアクセスコントロールリスト (ACL) に適用されます。
- IETF-Radius-Framed-IP-Address : VPN リモートアクセスクライアント、IPSec、および SSL にスタティック IP アドレスを割り当てます。
- Banner1 : VPN リモートアクセスユーザのログイン時にテキストバナーを表示します。
- Tunneling-Protocols : アクセスタイプに基づいて、VPN リモートアクセスセッションを許可または拒否します。



(注) 1つの LDAP 属性マップに、1つ以上の属性を含めることができます。特定の LDAP サーバからは、1つの LDAP 属性のみをマップすることができます。

AAA の LDAP サーバのガイドライン

この項では、AAA の LDAP サーバを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバは IPv4 アドレスを使用する必要がありますが、エンドポイントは IPv6 を使用できます。

その他のガイドライン

- Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN が、サーバのデフォルトパスワードポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルトパスワードポリシーに ACL を設定できます。
- Microsoft Active Directory および Sun サーバでのパスワード管理をイネーブルにするために LDAP over SSL を設定する必要があります。
- ASA は、Novell、OpenLDAP およびその他の LDAPv3 ディレクトリ サーバによるパスワード管理をサポートしません。
- バージョン 7.1 (x) 以降、ASA はネイティブ LDAP スキーマを使用して認証および認可を行うため、Cisco スキーマは必要なくなりました。
- シングルモードの場合は最大 100 台の LDAP サーバグループを使用でき、マルチモードの場合は各コンテキストで最大 4 台の LDAP サーバグループを使用できます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 4 台の LDAP サーバを含めることができます。
- ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまで LDAP サーバが 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ASA は、ローカルデータベースがフォールバック方式として設定されていると、ローカルデータベースに接続しようとします（管理認証および認可限定）。フォールバックメソッドとして設定されていない場合、ASA は LDAP サーバに引き続きアクセスしようとします。

AAA の LDAP サーバの設定

この項では、AAA に LDAP サーバを設定する方法について説明します。

手順

- ステップ 1 LDAP 属性マップを設定します。[LDAP 属性マップの設定 \(876 ページ\)](#) を参照してください。
- ステップ 2 LDAP サーバグループを追加します。[LDAP サーバグループの設定 \(877 ページ\)](#) を参照してください。
- ステップ 3 サーバをグループに追加し、サーバパラメータを設定します。[LDAP サーバのサーバグループへの追加 \(878 ページ\)](#) を参照してください。

LDAP 属性マップの設定

LDAP 属性マップを設定するには、次の手順を実行します。

手順

-
- ステップ 1** ローカル ユーザの場合は **[Configuration] > [Remote Access VPN] > [AAA Local Users] > [LDAP Attribute Map]** の順に選択し、その他すべてのユーザの場合は **[Configuration] > [Device Management] > [Users/AAA] > [LDAP Attribute Map]** の順に選択して、**Add** をクリックします。
- [Map Name] タブが表示された状態で [Mapping of Attribute Name] ダイアログボックスが開きます。
- ステップ 2** この属性マップの名前を作成します。
- ステップ 3** マッピングする LDAP 属性の 1 つの名前を追加します。
- ステップ 4** Cisco 属性を選択します。
- ステップ 5** [Add] をクリックします。
- ステップ 6** さらに属性をマップする場合は、ステップ 1～5 を繰り返します。
- ステップ 7** [Mapping of Attribute Value] タブをクリックして、マップされた Cisco 属性の新しい値に LDAP 属性の値をマッピングします。
- ステップ 8** [Add] をクリックして、[Add Mapping of Attribute Value] ダイアログボックスを表示します。
- ステップ 9** LDAP サーバから返されると予想されるこの LDAP 属性の値を入力します。
- ステップ 10** この LDAP 属性が以前の LDAP 属性値を含める場合に、Cisco 属性で使用する値を入力します。
- ステップ 11** [Add] をクリックします。
- ステップ 12** さらに属性値をマップする場合は、ステップ 8～11 を繰り返します。
- ステップ 13** [OK] を 2 回クリックして、各ダイアログボックスを閉じます。
- ステップ 14** [Apply] をクリックし、実行コンフィギュレーションの設定を保存します。
-

LDAP サーバグループの設定

LDAP サーバグループを作成して設定し、LDAP サーバをそのグループに追加するには、次の手順を実行します。

始める前に

LDAP サーバを LDAP サーバグループに追加する前に、属性マップを追加する必要があります。

手順

-
- ステップ 1** **[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]**、または VPN ユーザの場合は **[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 AAA サーバグループの名前を入力します。

ステップ 4 [Protocol] ドロップダウンリストから LDAP サーバタイプを選択します。

ステップ 5 使用する再アクティブ化モードのオプションボタン ([Depletion] または [Timed]) をクリックします。

[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。

Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。

a) [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 6 許可するサーバでの AAA トランザクションの失敗の最大数を追加します。

これは、応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数です。

ステップ 7 [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバグループが AAA サーバグループに追加されます。

ステップ 8 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

LDAP サーバのサーバグループへの追加

LDAP サーバをサーバグループに追加するには、次の手順を実行します。

手順

ステップ 1 次のいずれかを選択します。

- VPN ユーザの場合は、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups]。
- [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]

ステップ 2 サーバを追加するサーバグループを選択し、**Add** をクリックします。

選択したサーバグループに対応する [Add AAA Server] ダイアログボックスが表示されます。

ステップ 3 LDAP サーバに接続するインターフェイスの名前を選択します。

ステップ 4 LDAP サーバのサーバ名または IP アドレスを追加します。

ステップ 5 タイムアウト値を追加するか、デフォルト値をそのまま使用します。[Timeout] フィールドには、バックアップサーバへ要求を送信する前に、ASA がプライマリサーバからの応答を待機する時間を秒単位で指定します。

ステップ 6 [LDAP Parameters for authentication/authorization] 領域で、次の設定を行います。

- [Enable LDAP over SSL] (セキュア LDAP または LDAP-S と呼ばれる) : ASA と LDAP サーバの間のセキュアな通信に SSL を使用する場合に、このチェックボックスをオンにします。
 - (注) SASL プロトコルを設定しない場合は、SSL を使用して LDAP 通信のセキュリティを確保することを強く推奨します。
- [Server Port] : ASA から LDAP サーバへアクセスする際、単純認証 (セキュアでない認証) に使用される TCP ポート番号 389 またはセキュアな認証 (LDAP-S) に使用される TCP ポート番号 636 を指定します。LDAP サーバはすべて、認証および認可をサポートしています。Microsoft AD サーバおよび Sun LDAP サーバに限っては、さらに、LDAP-S を必要とする VPN リモート アクセス パスワード管理機能もサポートしています。
- [Server Type] : ドロップダウンリストから LDAP サーバタイプを指定します。使用できるオプションは、次のとおりです。
 - Detect Automatically/Use Generic Type
 - Microsoft
 - Novell
 - OpenLDAP
 - Sun (現在では Oracle Directory Server Enterprise Edition の一部)
- [Base DN] : ベース識別名 (DN)、または LDAP 要求を受け取ったサーバで検索が開始される LDAP 階層内の位置を指定します (例: OU=people, dc=cisco, dc=com)。
- [Scope] : ドロップダウンリストからの認証要求を受信する場合に、LDAP 階層内でサーバの実行が必要な検索範囲を指定します。次のオプションを使用できます。
 - [One Level] : ベース DN の 1 つ下のレベルだけが検索対象となります。このオプションを選択すると、検索の実行時間が短縮されます。
 - [All Levels] : ベース DN の下にあるすべてのレベル (つまりサブツリー階層全体) が検索対象となります。このオプションを選択すると、検索の実行に時間がかかります。
- [Naming Attribute (s)] : LDAP サーバのエントリを一意に識別する相対識別名属性を入力します。共通の名前付き属性は、Common Name (CN)、sAMAccountName、userPrincipalName、および User ID (uid) です。

- [Login DN and Login Password] : ASA は、LDAP サーバとの信頼 (バインド) を確立するために、ログイン DN とログインパスワードを使用します。ログイン DN のユーザアカウントのパスワードをログインパスワードとして指定します。
- [LDAP Attribute Map] : この LDAP サーバで使用するために作成された属性マップの 1 つを選択します。これらの属性マップは、LDAP 属性名をシスコの属性名と値にマップします。
- [SASL MD5 authentication] : ASA と LDAP サーバの間の通信を認証するための SASL の MD5 メカニズムをイネーブルにします。
- [SASL Kerberos authentication] : ASA と LDAP サーバの間のセキュアな認証通信のための SASL の Kerberos メカニズムをイネーブルにします。このオプションを有効にするためには、Kerberos サーバを定義しておく必要があります。
- [LDAP Parameters for Group Search] : この領域のフィールドは、ASA が AD グループを要求する方法を設定します。
 - [Group Base DN] : この DN により、LDAP 階層内で AD グループ (つまり、memberOf 列挙のリスト) の検索を開始する位置が指定されます。このフィールドの設定を行わない場合、ASA では、AD グループの取得にベース DN が使用されます。ASDM では、取得した AD グループのリストに基づいて、ダイナミックアクセスポリシーの AAA 選択基準が定義されます。詳細については、**show ad-groups** コマンドを参照してください。
 - [Group Search Timeout] : 使用できるグループについてのクエリーに対して AD サーバから応答があるまでの最長待機時間を指定します。

ステップ 7 [OK] をクリックします。

[Add AAA Server] ダイアログボックスが閉じ、AAA サーバが AAA サーバグループに追加されます。

ステップ 8 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

LDAP サーバによる認証および許可のテスト

ASA が LDAP サーバに接続してユーザを認証または承認できるかどうかを判別するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] の順に選択します。

ステップ 2 サーバが存在するサーバグループを選択します。

ステップ 3 テストするサーバを選択します。

ステップ 4 [Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 5 実行するテストのタイプ ([Authentication] または [Authorization]) をクリックします。

ステップ 6 ユーザ名を入力します。

ステップ 7 認証をテストする場合は、ユーザ名のパスワードを入力します。

ステップ 8 [OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、エラー メッセージが表示されます。

AAA の LDAP サーバのモニタリング

AAA の LDAP サーバのモニタリングについては、次のコマンドを参照してください。

- [Monitoring] > [Properties] > [AAA Servers]

このペインは、設定された AAA サーバの統計情報を表示します。

- [Tools] > [Command Line Interface]

このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

AAA の LDAP サーバの履歴

表 43: AAA サーバの履歴

機能名	プラットフォーム リリース	説明
AAA の LDAP サーバ	7.0(1)	LDAP サーバの AAA のサポートと LDAP サーバの設定方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups Configuration] > [Remote Access VPN] > [AAA Local Users] > [LDAP Attribute Map]。



第 **VII** 部

システム管理

- [管理アクセス \(885 ページ\)](#)
- [ソフトウェアおよびコンフィギュレーション \(923 ページ\)](#)
- [システム イベントに対する応答の自動化 \(957 ページ\)](#)
- [テストとトラブルシューティング \(965 ページ\)](#)



第 36 章

管理アクセス

この章では、Telnet、SSH、および HTTPS (ASDM を使用) 経由でシステム管理を行うために Cisco ASA にアクセスする方法と、ユーザを認証および許可する方法、ログインバナーを作成する方法について説明します。

- [管理リモートアクセスの設定 \(885 ページ\)](#)
- [システム管理者用 AAA の設定 \(899 ページ\)](#)
- [デバイスアクセスのモニタリング \(917 ページ\)](#)
- [管理アクセスの履歴 \(918 ページ\)](#)

管理リモートアクセスの設定

ここでは、ASDM 用の ASA アクセス、Telnet または SSH、およびログインバナーなどのその他のパラメータの設定方法について説明します。

HTTPS (ASDM)、Telnet、または SSH の ASA アクセス

この項では、ASDM および CSM、Telnet、または SSH など、HTTPS に ASA アクセスを設定する方法について説明します。次のガイドラインを参照してください。

- ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセスルールは必要ありません。必要なのは、この章の各項の説明に従って管理アクセスを設定することだけです。ただし、HTTP リダイレクトを設定して HTTP 接続を HTTPS に自動的にリダイレクトするには、HTTP を許可するアクセスルールを有効化する必要があります。そうしないと、インターフェイスが HTTP ポートをリッスンできません。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスはサポートされません。たとえば、管理ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです。[VPN トンネルを介した管理アクセスの設定 \(894 ページ\)](#) を参照してください。
- ASA では以下の接続が許可されます。

- コンテキストごとに最大 5 つの同時 Telnet 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。
- コンテキストごとに最大 5 つの同時 SSH 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。
- コンテキストごとに最大 5 つの同時 ASDM インスタンスを使用でき、全コンテキスト間で最大 32 の ASDM インスタンスの使用が可能です。

HTTPS (ASDM) アクセスの設定

この項では、ASDM や CSM など、HTTPS に ASA アクセスを設定する方法について説明します。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH] の順に選択し、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2 [ASDM/HTTPS] を選択します。

ステップ 3 管理インターフェイスを選択し、許可するホスト IP アドレスを設定して、[OK] をクリックします。

名前付きインターフェイスを指定します。ブリッジグループの場合、ブリッジグループメンバインターフェイスを指定します。

ステップ 4 [HTTP Settings] を設定します。

- [Enable HTTP Server] チェックボックスがオンになっていることを確認します。この設定はデフォルトでイネーブルになっています。
- 必要に応じて、[Port Number]、[Idle Timeout]、[Session Timeout] の値を変更します。
- 証明書認証を要件にするには、[Require client certificate to access ASDM on the following interfaces] の下にあるドロップダウン矢印をクリックし、ASDM がイネーブルにされているすべてのインターフェイスに対応するチェックボックスをオンにします。詳細については、[ASDM 証明書認証の設定 \(902 ページ\)](#) を参照してください。

ステップ5 [Apply] をクリックします。

SSH アクセスの設定

この項では、SSH に ASA アクセスを設定する方法について説明します。

(8.4 以降) SSH デフォルト ユーザ名はサポートされなくなりました。 **pix** または **asa** ユーザ名とログインパスワードで SSH を使用して ASA に接続することができなくなりました。 SSH を使用するには、AAA 認証を設定し ([Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] の順に選択)、続いてローカル ユーザを定義する必要があります ([Configuration] > [Device Management] > [Users/AAA] の順に選択)。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ1 [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH] の順に選択し、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ2 [SSH] を選択します。

ステップ3 管理インターフェイスを選択し、許可するホスト IP アドレスを設定して、[OK] をクリックします。

名前付きインターフェイスを指定します。ブリッジグループの場合、ブリッジグループ メンバインターフェイスを指定します。

ステップ4 (任意) [SSH Settings] を設定します。

- [Allowed SSH Versions] : [1 & 2]、[1]、または [2] を選択します。デフォルトでは、SSH はバージョン 1 と 2 の両方を許可します。
- [SSH Timeout] : 1 ~ 60 分にタイムアウトを設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。
- [DH Key Exchange] : 該当するオプション ボタンをクリックして、Diffie-Hellman (DH) キー交換グループ 1 またはグループ 14 を選択します。DH グループ キー交換方式を指定

しないと、DH グループ 1 のキー交換方式が使用されます。DH キー交換方法の使用方法の詳細については、RFC 4253 を参照してください。

ステップ 5 [Apply] をクリックします。

ステップ 6 SSH ユーザ認証を設定します。

- a) (パスワードアクセス用) **[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication]** の順に選択します。

AAA 認証は、[Public Key Using PKF] オプションが指定されたユーザ名に対するローカル公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカルデータベースを暗黙的に使用します。SSH 認証は、パスワードを持つユーザ名にのみ影響します。ローカルユーザが公開キー認証またはパスワードを使用できるようにするには、この手順を使用してローカル認証を明示的に設定し、パスワードアクセスを許可する必要があります。

- b) [SSH] チェックボックスをオンにします。
c) [Server Group] ドロップダウンリストから [LOCAL] データベース (または AAA サーバ) を選択します。
d) [Apply] をクリックします。
e) ローカルユーザを追加します。ユーザアクセスに AAA サーバを使用することもできますが、ローカルユーザ名の使用を推奨します。 **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts]** の順に選択し、[Add] をクリックします。

[Add User Account-Identity] ダイアログボックスが表示されます。

- f) ユーザ名とパスワードを入力し、パスワードを確認します。ユーザにパスワードを割り当てたが、ユーザが公開キー認証のみを使用するように制限するには、この手順に従ってパスワードの使用に対する AAA 認証を有効にしないでください。
g) (任意) 個々のユーザごとに、パスワード認証ではなく公開キー認証のみ、またはこれら両方の認証を有効にするには、次のいずれかのペインを選択します。

- **[Public Key Authentication]** : Base64 でエンコードされた公開キーに貼り付けます。SSH-RSA raw キー (証明書なし) を生成可能な任意の SSH キー生成ソフトウェア (ssh keygen など) を使用して、キーを生成できます。既存のキーを表示する場合は、キーは SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼り付ける場合は、[Key is hashed] チェックボックスをオンにします。
- 認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。認証キーを削除する場合は [Yes] をクリックし、認証キーを保持する場合は [No] をクリックします。
- **[Public Key Using PKF]** : [Specify a new PKF key] チェックボックスをクリックして、公開キーファイル (PKF) でフォーマットされたキー (4096 ビットまで) を貼りつけるかインポートします。Base64 形式で貼り付けるには大きすぎるキーにはこのフォーマットを使用します。たとえば、ssh の keygen を使用して 4096 ビット キーを生成し、PKF に変換して、このペインでインポートします。既存のキーを表示する場合は、SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼り付ける

必要がある場合は、[Public Key Authentication] ペインからコピーし、[Key is hashed] チェックボックスをオンにした新しい ASA のペインに貼り付けます。

認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。認証キーを削除する場合は [Yes] をクリックし、認証キーを保持する場合は [No] をクリックします。

h) [OK] をクリックし、続いて [Apply] をクリックします。

ステップ 7 RSA キーのペアを生成します（物理 ASA の場合のみ。ASA v の場合は、導入後に自動的に RSA キー ペアが作成されます）。

- a) [Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] の順に選択します。
- b) [Add] をクリックし、[Add a new identity certificate] オプション ボタンをクリックします。
- c) [New] をクリックします。
- d) [Add Key Pair] ダイアログボックスで、デフォルトを受け入れて [Generate Now] をクリックします。

ステップ 8 （任意） SSH 暗号の暗号化アルゴリズムと整合性アルゴリズムを設定します。

- a) [Configuration] > [Device Management] > [Advanced] > [SSH Ciphers] の順に選択します。
- b) [Encryption] を選択し、[Edit] をクリックします。
- c) [SSH cipher security level] ドロップダウン リストから、次のいずれかのレベルを選択します。
 - [All] : すべての暗号方式（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr）を使用する場合は、このオプションを選択します。
 - [Custom] : カスタム暗号ストリングを設定する場合はこのオプションを選択し、[Cipher algorithms/custom string] フィールドに各暗号ストリングをコロンで区切って入力します。
 - [Fips] : FIPS 対応の暗号方式（aes128-cbc aes256-cbc）のみを使用する場合は、このオプションを選択します。
 - [High] : 強度が高の暗号方式のみ（aes256-cbc aes256-ctr）を使用する場合は、このオプションを選択します。
 - [Low] : 強度が低、中、高の暗号方式（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr）を使用する場合は、このオプションを選択します。
 - [Medium] : 強度が中および高の暗号方式（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr）を使用する場合は、このオプションを選択します（デフォルト）。
- d) [Integrity] を選択し、[Edit] をクリックします。
- e) [SSH cipher security level] ドロップダウン リストから、次のいずれかのレベルを選択します。

- [All] : すべての暗号方式 (hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96) を使用することを指定します。
- [Custom] : カスタム暗号ストリングを設定する場合はこのオプションを選択し、[Cipher algorithms/custom string] フィールドに各暗号ストリングをコロンで区切って入力します。
- [Fips] : FIPS 対応の暗号方式のみ (hmac-sha1) を指定します。
- [High] : 強度が高い暗号方式のみ (hmac-sha1) を指定します。
- [Low] : 強度が低、中、高の暗号方式 (hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96) を使用する場合は、このオプションを選択します。
- [Medium] : 強度が中および高の暗号方式 (hmac-sha1 hmac-sha1-96) を指定します (デフォルト)。

例

次の例では、Linux または Macintosh システムの SSH の共有キーを生成して、ASA にインポートします。

1. コンピュータで 4096 ビットの ssh-rsa 公開キーおよび秘密キーを生成します。

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]-----+
| .                    |
| o .                  |
|+... o                |
|B.+.....             |
|.B ..+ S              |
| = o                  |
| + . E                |
| o o                  |
| ooooo                |
+-----+

```

2. PKF 形式にキーを変換します。

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:~.ssh john$ ssh-keygen -e -f id_rsa.pub

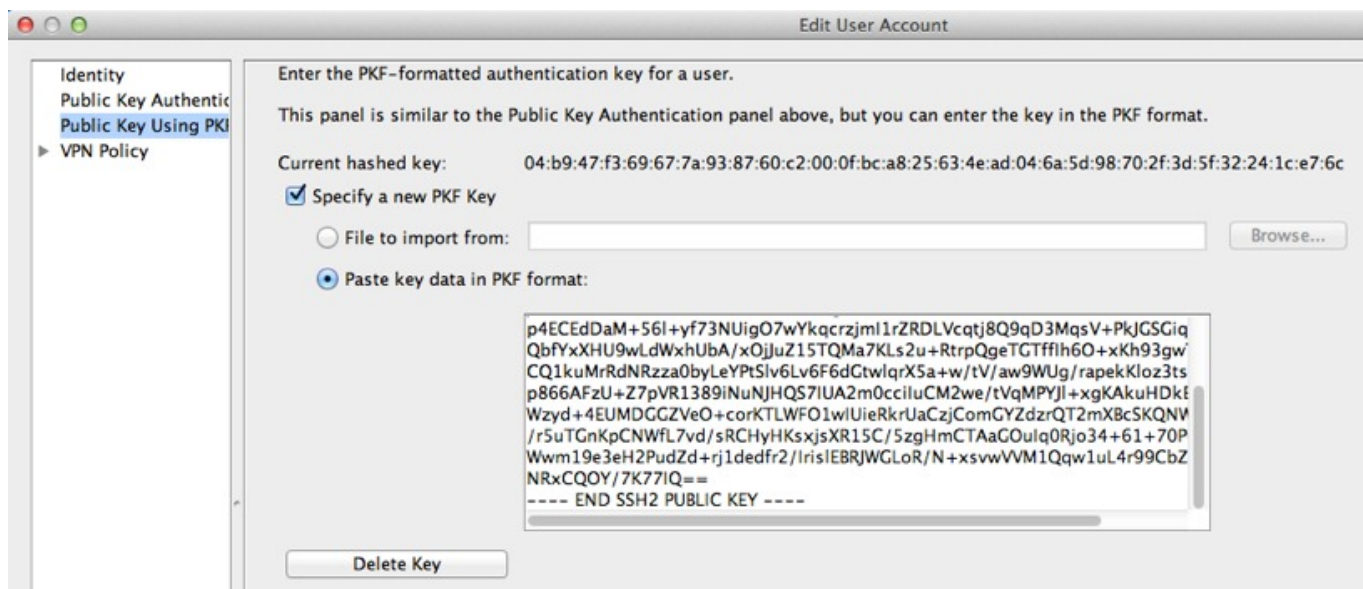
```

```

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAQADNUvkgza371B/Q/fljplAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRedoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjm1lrZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyI1
QbfYxXHU9wLdWxhUBA/xOjJuZ15TQMa7KLS2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYptSlv6Lv6F6dGtlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNjHQS7IUA2m0cciuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wUieRkrUaCzjComGYZdZrQT2mXbcSKQNW1SCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGouIqORjo34+61+70PctYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/Iris1EBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZf9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichon-mac:~$ ssh john$

```

3. キーをクリップボードにコピーします。
4. ASDM で、**[Configuration] > [Device Management] > [Users/AAA] > [User Accounts]** の順に選択し、ユーザ名を選択してから **[Edit]** をクリックします。**[Public Key Using PKF]** をクリックして、ウィンドウにキーを貼り付けます。



5. ユーザが ASA に SSH できることを確認 (テスト) します。

```

jcrichon-mac:~$ ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes

```

次のダイアログボックスが、パズフレーズを入力するために表示されます。



一方、端末セッションでは、以下が表示されます。

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

Telnet アクセスの設定

この項では、Telnet に ASA アクセスを設定する方法について説明します。VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティインターフェイスに対して Telnet は使用できません。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration]>[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
- ASA CLI に Telnet を使用してアクセスするには、ログインパスワードを入力します。Telnet を使用する前に手動でパスワードを設定する必要があります。

手順

ステップ 1 [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH] の順に選択し、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2 [Telnet] を選択します。

ステップ 3 管理インターフェイスを選択し、許可するホスト IP アドレスを設定して、[OK] をクリックします。

名前付きインターフェイスを指定します。ブリッジグループの場合、ブリッジグループメンバインターフェイスを指定します。

ステップ 4 (任意) [Telnet Timeout] を設定します。デフォルトのタイムアウト値は 5 分です。

ステップ 5 [Apply] をクリックします。

ステップ 6 Telnet で接続する前に、ログインパスワードを設定します。デフォルトのパスワードはありません。

- a) [Configuration] > [Device Setup] > [Device Name/Password] の順に選択します。
- b) [Telnet Password] 領域で [Change the password to access the console of the security appliance] チェックボックスをオンにします。
- c) 古いパスワードを入力して (新しい ASA の場合はこのフィールドを空白にする)、新しいパスワードを入力してから、確認として新しいパスワードを再入力します。
- d) [Apply] をクリックします。

ASDM アクセスまたはクライアントレス SSL VPN のための HTTP リダイレクトの設定

ASDM またはクライアントレス SSL VPN を使用して ASA に接続するには、HTTPS を使用する必要があります。利便性のために、HTTP 管理接続を HTTPS にリダイレクトすることができます。たとえば、HTTP をリダイレクトすることによって、**http://10.1.8.4/admin/** または **https://10.1.8.4/admin/** と入力し、ASDM 起動ページで HTTPS アドレスにアクセスできます。

この機能は、IPv4 のリダイレクションのみをサポートします。

始める前に

通常、ホスト IP アドレスを許可するアクセスルールは必要ありません。ただし、HTTP リダイレクトのためには、HTTP を許可するアクセスルールを有効化する必要があります。そうしないと、インターフェイスが HTTP ポートをリッスンできません。

手順

ステップ 1 [Configuration] > [Device Management] > [HTTP Redirect] の順に選択します。

表には、現在設定されているインターフェイスと、リダイレクトがインターフェイスで有効化されているかどうかを示しています。

ステップ 2 ASDM に使用するインターフェイスを選択し、[Edit] をクリックします。

ステップ 3 [Edit HTTP/HTTPS Settings] ダイアログボックスで次のオプションを設定します。

- [Redirect HTTP to HTTPS] : HTTP 要求を HTTPS にリダイレクトします。
- [HTTP Port] : インターフェイスが HTTP 接続のリダイレクトに使用するポートを指定します。デフォルトは 80 です。

ステップ4 [OK] をクリックします。

VPN トンネルを介した管理アクセスの設定

あるインターフェイスで VPN トンネルが終端している場合、別のインターフェイスにアクセスして ASA を管理するには、そのインターフェイスを管理アクセス インターフェイスとして指定する必要があります。たとえば、outside インターフェイスから ASA に入る場合は、この機能を使用して、ASDM、SSH、Telnet、または SNMP 経由で Inside インターフェイスに接続するか、outside インターフェイスから入るときに Inside インターフェイスに ping を実行できます。

ASA への通過ルートとなるインターフェイス以外のインターフェイスへの VPN アクセスはサポートされません。たとえば、VPN アクセスが外部インターフェイスにある場合、外部インターフェイスへの直接接続のみ開始できます。複数のアドレスを覚える必要がないように、ASA の直接アクセス可能インターフェイスの VPN を有効にし、名前解決を使用してください。

管理アクセスは、IPsec クライアント、IPsec サイト間、AnyConnect SSL VPN クライアントの VPN トンネル タイプ 経由で行えます。

手順

ステップ1 [Configuration] > [Device Management] > [Management Access] > [Management Interface] の順に選択します。

ステップ2 [Management Access Interface] ドロップダウンリストからセキュリティが最も高いインターフェイス（内部インターフェイス）を選択します。

ブリッジグループ インターフェイスはサポートされません。

ステップ3 [Apply] をクリックします。

管理インターフェイスが割り当てられ、変更内容が実行コンフィギュレーションに保存されます。

コンソール タイムアウトの変更

コンソール タイムアウトでは、接続を特権 EXEC モードまたはコンフィギュレーション モードにしておくことができる時間を設定します。タイムアウトに達すると、セッションはユーザ EXEC モードになります。デフォルトでは、セッションはタイムアウトしません。この設定は、コンソールポートへの接続を保持できる時間には影響しません。接続がタイムアウトすることはありません。

手順

- ステップ 1 **[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Console Timeout]** の順に選択します。
- ステップ 2 新しいタイムアウト値を分単位で定義します。無制限の時間を指定する場合は、「0」と入力します。デフォルト値は 0 です
- ステップ 3 **[Apply]** をクリックします。
タイムアウト値の変更が実行コンフィギュレーションに保存されます。

CLI プロンプトのカスタマイズ

プロンプトに情報を追加する機能により、複数のモジュールが存在する場合にログインしている ASA を一目で確認することができます。この機能は、フェールオーバー時に、両方の ASA に同じホスト名が設定されている場合に便利です。

マルチ コンテキスト モードでは、システム実行スペースまたは管理コンテキストにログインするときに、拡張プロンプトを表示できます。非管理コンテキスト内では、デフォルトのプロンプト（ホスト名およびコンテキスト名）のみが表示されます。

デフォルトでは、プロンプトに ASA のホスト名が表示されます。マルチ コンテキスト モードでは、プロンプトにコンテキスト名も表示されます。CLI プロンプトには、次の項目を表示できます。

cluster-unit	クラスタ ユニット名を表示します。クラスタの各ユニットは一意的な名前を持つことができます。
コンテキスト	(マルチ モードのみ) 現在のコンテキストの名前を表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
priority	フェールオーバー プライオリティを [pri] (プライマリ) または [sec] (セカンダリ) として表示します。

<p>state</p>	<p>ユニットのトラフィック通過状態またはロールを表示します。</p> <p>フェールオーバーの場合、state キーワードに対して次の値が表示されます。</p> <ul style="list-style-type: none"> • [act] : フェールオーバーが有効であり、装置ではトラフィックをアクティブに通過させています。 • [stby] : フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailover] : フェールオーバーは無効であり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover] : フェールオーバーは無効であり、装置ではトラフィックを通過させていません。これは、スタンバイユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 <p>クラスタリングの場合、state キーワードに対して次の値が表示されます。</p> <ul style="list-style-type: none"> • master • slave
---------------------	--

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Command Line (CLI)]** > **[CLI Prompt]** の順に選択します。

ステップ 2 次のいずれかを実行してプロンプトをカスタマイズします。

- **[Available Prompts]** リストで属性をクリックしてから、**[Add]** をクリックします。プロンプトには複数の属性を追加できます。属性が **[Available Prompts]** リストから **[Selected Prompts]** リストに移動します。
- **[Selected Prompts]** リストで属性をクリックしてから、**[Delete]** をクリックします。属性が **[Selected Prompts]** リストから **[Available Prompts]** リストに移動します。
- **[Selected Prompts]** リストで属性をクリックして、**[Move Up]** または **[Move Down]** をクリックして属性の表示順序を変更します。

プロンプトが変化して、[CLI Prompt Preview] フィールドに表示されます。

ステップ 3 Apply をクリックします。

変更されたプロンプトが、実行コンフィギュレーションに保存されます。

ログインバナーの設定

ユーザが ASA に接続するとき、ログインする前、または特権 EXEC モードに入る前に表示されるメッセージを設定できます。

始める前に

- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。「ウェルカム」や「お願いします」などの表現は侵入者を招き入れているような印象を与えるので使用しないでください。以下のバナーでは、不正アクセスに対して正しい表現を設定しています。

```
You have logged in to a secure device.  
If you are not authorized to access this device,  
log out immediately or risk possible criminal consequences.
```

- バナーが追加された後、次の場合に ASA に対する Telnet または SSH セッションが終了する可能性があります。
 - バナー メッセージを処理するためのシステム メモリが不足している場合。
 - バナー メッセージの表示を試みたときに、TCP 書き込みエラーが発生した場合。
- バナー メッセージのガイドラインについては、RFC 2196 を参照してください。

手順

ステップ 1 [Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner] の順に選択します。

ステップ 2 CLI 用に作成するバナー タイプ用のフィールドにバナー テキストを追加します。

- [session (exec)] バナーは、ユーザが CLI で特権 EXEC モードにアクセスした場合に表示されます。
- [login] バナーは、ユーザが CLI にログインした場合に表示されます。
- [message-of-the-day (motd)] バナーは、ユーザが CLI に初めて接続する場合に表示されます。

- [ASDM] バナーは、ユーザが認証を受けた後 ASDM に接続した場合に表示されます。ユーザは、次のいずれかのオプションを使用して、表示されたバナーを消去できます。
 - [Continue] : バナーを消去して、ログインを完了します。
 - [Disconnect] : バナーを消去して、接続を終了します。
- 使用できるのは、改行 (Enter キー) も含めて ASCII 文字だけです。ただし、改行文字は 2 文字に相当します。
- また、タブ文字は、CLI バージョンでは無視されるため、バナーには使用しないでください。
- RAM およびフラッシュ メモリに関するもの以外、バナーに長さ制限はありません。
- ASA のホスト名またはドメイン名は、**\$(hostname)** 文字列と **\$(domain)** 文字列を組み込むことによって動的に追加できます。
- システムコンフィギュレーションでバナーを設定する場合は、コンテキストコンフィギュレーションで **\$(system)** という文字列を使用することにより、コンテキスト内でバナーテキストを使用できます。

ステップ 3 [Apply] をクリックします。

新しいバナーが、実行コンフィギュレーションに保存されます。

管理セッションクォータの設定

ASA で許可する ASDM、SSH、および Telnet の同時最大セッション数を設定できます。この最大値に達すると、それ以降のセッションは許可されず、syslog メッセージが生成されます。システム ロックアウトを回避するために、管理セッション割り当て量のメカニズムではコンソールセッションをブロックできません。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキスト コンフィギュレーションからシステム コンフィギュレーションに切り替えるには、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下の **[System]** をダブルクリックします。

手順

ステップ 1 **[Configuration] > [Device Management] > [Management Access] > [Management Session Quota]** の順に選択します。

ステップ 2 ASA で許可される ASDM、SSH、および Telnet の同時セッションの最大数を入力します。有効値の範囲は 0 ~ 10000 です。

ステップ3 [Apply] をクリックして、設定の変更を保存します。

システム管理者用 AAA の設定

この項では、システム管理者の認証、管理許可、コマンド許可を設定する方法について説明します。

管理認証の設定

CLI および ASDM アクセスの認証を設定します。

管理認証について

ASA へのログイン方法は、認証を有効にしているかどうかによって異なります。

SSH 認証の概要

認証ありまたは認証なしでの SSH アクセスについては、次の動作を参照してください。

- 認証なし：SSH は認証なしでは使用できません。
- 認証あり：SSH 認証を有効にした場合は、AAA サーバまたはローカルユーザデータベースに定義されているユーザ名とパスワードを入力します。公開キーの認証では、ASA はローカルデータベースのみをサポートします。SSH 公開キー認証を設定した場合、ASA ではローカルデータベースを暗黙的に使用します。ログインにユーザ名とパスワードを使用する場合に必要なのは、SSH 認証を明示的に設定することのみです。ユーザ EXEC モードにアクセスします。

Telnet 認証の概要

認証の有無にかかわらず、Telnet アクセスについては、次の動作を参照してください。

- 認証なし：Telnet の認証を有効にしていない場合は、ユーザ名を入力しません。ログインパスワードを入力します。デフォルトのパスワードはありません。したがって、ASA へ Telnet 接続するには、パスワードを設定する必要があります。ユーザ EXEC モードにアクセスします。
- 認証あり：Telnet 認証を有効にした場合は、AAA サーバまたはローカルユーザデータベースに定義されているユーザ名とパスワードを入力します。ユーザ EXEC モードにアクセスします。

ASDM 認証の概要

認証ありまたは認証なしでの ASDM アクセスに関しては、次の動作を参照してください。AAA 認証の有無にかかわらず、証明書認証を設定することも可能です。

- 認証なし：デフォルトでは、ブランクのユーザ名と **enable password** コマンドを使用して ASDM にログインできます。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定 (571 ページ) を参照してください。ログイン画面で (ユーザ名をブランクのままにしないで) ユーザ名とパスワードを入力した場合は、ASDM によってローカルデータベースで一致がチェックされることに注意してください。
- 証明書認証 (シングル、ルーテッドモードのみ)：ユーザに有効な証明書を要求できます。証明書のユーザ名とパスワードを入力すると、ASA が PKI トラストポイントに対して証明書を検証します。
- AAA 認証：ASDM (HTTPS) 認証を有効にした場合は、AAA サーバまたはローカルユーザデータベースに定義されているユーザ名とパスワードを入力します。これで、ブランクのユーザ名とイネーブルパスワードで ASDM を使用できなくなりました。
- AAA 認証と証明書認証の併用 (シングル、ルーテッドモードのみ)：ASDM (HTTPS) 認証を有効にした場合は、AAA サーバまたはローカルユーザデータベースに定義されているユーザ名とパスワードを入力します。証明書認証用のユーザ名とパスワードが異なる場合は、これらも入力するように求められます。ユーザ名を証明書から取得してあらかじめ入力しておくよう選択できます。

シリアル認証の概要

認証ありまたは認証なしでのシリアル コンソール ポートへのアクセスに関しては、次の動作を参照してください。

- 認証なし：シリアルアクセスの認証を有効にしていない場合は、ユーザ名、パスワードを入力しません。ユーザ EXEC モードにアクセスします。
- 認証あり：シリアルアクセスの認証を有効にした場合は、AAA サーバまたはローカルユーザデータベースで定義されているユーザ名とパスワードを入力します。ユーザ EXEC モードにアクセスします。

enable 認証の概要

ログイン後に特権 EXEC モードに入るには、**enable** コマンドを入力します。このコマンドの動作は、認証がイネーブルかどうかによって異なります。

- 認証なし：**enable** 認証を設定していない場合は、**enable** コマンドを入力するときにシステムイネーブルパスワードを入力します。デフォルトは空白です。ただし、**enable** 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザとしてログインしていません。これにより、コマンド認可などユーザベースの各機能が影響を受けることがあります。ユーザ名を維持するには、**enable** 認証を使用してください。
- 認証あり：**enable** 認証を設定した場合は、ASA はプロンプトにより AAA サーバまたはローカルユーザデータベースで定義されているユーザ名とパスワードを要求します。この機能は、ユーザが入力できるコマンドを判別するためにユーザ名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

ローカルデータベースを使用する **enable** 認証の場合は、**enable** コマンドの代わりに **login** コマンドを使用できます。**login** コマンドによりユーザ名が維持されますが、認証をオンにするための設定は必要ありません。



注意 CLIにアクセスできるユーザや特権 EXEC モードを開始できないようにするユーザをローカルデータベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可がない場合、特権レベルが 2 以上 (2 がデフォルト) のユーザは、CLI で自分のパスワードを使用して特権 EXEC モード (およびすべてのコマンド) にアクセスできます。あるいは、認証処理でローカルデータベースではなく AAA サーバを使用してログインコマンドを回避するか、またはすべてのローカルユーザをレベル 1 に設定することにより、システムイネーブルパスワードを使用して特権 EXEC モードにアクセスできるユーザを制御できます。

ホスト オペレーティングシステムから ASA へのセッション

一部のプラットフォームでは、ASA の実行を別のアプリケーションとしてサポートしています (例: Catalyst 6500 の ASASM、Firepower 4100/9300 の ASA)。ホストオペレーティングシステムから ASA へのセッションの場合、接続のタイプに応じてシリアルおよび Telnet 認証を設定できます。

マルチ コンテキスト モードでは、システム コンフィギュレーションで AAA コマンドを設定できません。ただし、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はこれらのセッションにも適用されます。この場合、管理コンテキストの AAA サーバまたはローカル ユーザ データベースが使用されます。

CLI、ASDM、および enable コマンド アクセス認証の設定

始める前に

- Telnet、SSH、または HTTP アクセスを設定します。
- 外部認証の場合は、AAA サーバグループを設定します。ローカル認証の場合は、ローカルデータベースにユーザを追加します。
- HTTP 管理認証では、AAA サーバグループの SDI プロトコルをサポートしていません。
- この機能は、**ssh authentication** コマンドによるローカル ユーザ名に関する SSH 公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカルデータベースを暗黙的に使用します。この機能は、ユーザ名とパスワードにのみ影響します。ローカルユーザが公開キー認証またはパスワードを使用できるようにするには、この手順を使用してローカル認証を明示的に設定し、パスワードアクセスを許可する必要があります。

手順

ステップ 1 **enable** コマンドを使用するユーザを認証する場合は、**[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication]** の順に選択し、次の設定を行います。

- a) [Enable] チェックボックスを選択します。
- b) サーバグループ名または LOCAL データベースを選択します。
- c) (オプション) AAA サーバを選択する場合は、AAA サーバが使用不可になった場合のフォールバック方式としてローカルデータベースが使用されるように ASA を設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカルデータベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。

ステップ 2 CLI または ASDM にアクセスするユーザを認証する場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] の順に選択し、次の設定を行います。

- a) 次のチェックボックスをオンにします (複数可)。
 - [HTTP/ASDM] : HTTPS を使用して ASA にアクセスする ASDM クライアントを認証します。
 - [Serial] : コンソールポートを使用して ASA にアクセスするユーザを認証します。ASASM の場合、このパラメータは **service-module session** コマンドを使用してスイッチからアクセスする仮想コンソールに影響します。
 - **SSH** : SSH を使用して ASA にアクセスするユーザを認証します (パスワードのみ。公開キー認証では暗黙のうちにローカルデータベースが使用されます)。
 - [Telnet] : Telnet を使用して ASA にアクセスするユーザを認証します。ASASM の場合、このパラメータは **session** コマンドを使用するスイッチからのセッションにも影響します。
- b) チェックボックスをオンにしたサービスごとに、サーバグループ名または LOCAL データベースを選択します。
- c) (オプション) AAA サーバを選択する場合は、AAA サーバが使用不可になった場合のフォールバック方式としてローカルデータベースが使用されるように ASA を設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカルデータベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。

ステップ 3 [Apply] をクリックします。

ASDM 証明書認証の設定

AAA 認証の有無にかかわらず証明書認証を必須にできます。ASA は証明書を PKI トラストポイントに照合して検証します。

始める前に

この機能は、シングルルーテッドモードでのみサポートされます。

手順

ステップ 1 [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH] の順に選択します。

ステップ 2 [Require client certificate to access ASDM on the following interfaces] の下にあるドロップダウン矢印をクリックし、ASDM がイネーブルにされているすべてのインターフェイスに対応するチェックボックスをオンにします。

証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上の接続については証明書の提示が不要になります。

ステップ 3 (任意) ASDM で証明書からユーザ名を抽出する際に使用する属性を設定するには、[Configuration] > [Device Management] > [Management Access] > [HTTP Certificate Rule] の順に選択します。

次の方法の中から 1 つを選択してください。

- [Specify the Certificate Fields to be used] : [Primary Field] ドロップダウン リストと [Secondary Field] ドロップダウン リストから値を選択します。
- [Use the entire DN as the username]
- [Use script to select username] : [Add] をクリックし、スクリプトの内容を追加します。

認証を求めるプロンプトにユーザ名を事前入力するには、[Prefill Username] チェックボックスをオンにします。そのユーザ名が最初に入力したものと異なる場合、最初のユーザ名が事前入力された新しいダイアログボックスが表示されます。そこに、認証用のパスワードを入力できます。

デフォルトでは、ASDM は CN OU 属性を使用します。

ステップ 4 [Apply] をクリックします。

管理許可による CLI および ASDM アクセスの制限

ASA ではユーザの認証時に管理アクセスユーザとリモートアクセスユーザを区別できるようになっています。ユーザ ロールを区別することで、リモートアクセス VPN ユーザやネットワーク アクセスユーザが ASA に管理接続を確立するのを防ぐことができます。

始める前に

RADIUS または LDAP (マッピング済み) ユーザ

ユーザが LDAP 経由で認証されると、ネイティブ LDAP 属性およびその値が Cisco ASA 属性にマッピングされ、特定の許可機能が提供されます。Cisco VSA CVPN3000-Privilege-Level の値を 0 ~ 15 の範囲で設定した後、LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。

RADIUS IETF の **service-type** 属性が、RADIUS 認証および許可要求の結果として **access-accept** メッセージで送信される場合、この属性は認証されたユーザにどのタイプのサービスを付与するかを指定するために使用されます。

RADIUS Cisco VSA **privilege-level** 属性（ベンダー ID 3076、サブ ID 220）が **access-accept** メッセージで送信される場合は、ユーザの権限レベルを指定するために使用されます。

TACACS+ ユーザ

「**service=shell**」で許可が要求され、サーバは **PASS** または **FAIL** で応答します。

ローカル ユーザ

指定したユーザ名の [Access Restriction] オプションを設定します。アクセス制限のデフォルト値は [Full Access] です。この場合、[Authentication] タブのオプションで指定されたすべてのサービスに対して、フルアクセスが許可されます。

管理許可の属性

管理許可の AAA サーバタイプおよび有効な値については、次の表を参照してください。ASA ではこれらの値を使用して管理アクセス レベルを決定します。

Management Level	RADIUS/LDAP の (マッピングされた) 属性	TACACS+ 属性	ローカル データベースの属性
[Full Access] : [Authentication] タブのオプションで指定されたすべてのサービスに対してフルアクセスが許可されます。	Service-Type 6 (アドミニストレーティブ)、Privilege-Level 1	PASS、特権レベル 1	admin
[Partial Access] : [Authentication] タブのオプションで設定すると、CLI または ASDM に対するアクセスが許可されます。ただし、[Enable] オプションを使用して enable 認証を設定する場合、CLI y ユーザは enable コマンドを使用して特権 EXEC モードにアクセスすることはできません。	Service-Type 7 (NAS プロンプト)、Privilege-Level 2 以上 Framed (2) および Login (1) サービスタイプは同様に扱われます。	PASS、特権レベル 2 以上	nas-prompt
[No Access] : 管理アクセスが拒否されます。ユーザは [Authentication] タブのオプションで指定されたいずれのサービスも使用できません ([Serial] オプションは除きます。つまり、シリアルアクセスは許可されません)。リモートアクセス (IPsec および SSL) ユーザは、引き続き自身のリモートアクセスセッションを認証および終了できます。他のすべてのサービスタイプ (ボイス、ファクスなど) も同様に処理されます。	Service-Type 5 (アウトバウンド)	FAIL	remote-access

その他のガイドライン

- シリアル コンソール アクセスは管理許可に含まれません。
- この機能を使用するには、管理アクセスに AAA 認証も設定する必要があります。CLI、ASDM、および **enable** コマンドアクセス認証の設定 (901 ページ) を参照してください。
- 外部認証を使用する場合は、この機能をイネーブルにする前に、AAA サーバグループを設定しておく必要があります。
- HTTP 許可は、シングルルーテッドモードでのみサポートされます。

手順

ステップ 1 HTTP セッションの管理許可をイネーブルにするには、**[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]** の順に選択し、[Enable Authorization for ASA Command Access] 領域の [HTTP] チェックボックスをオンにします。

(注) ASA コマンドアクセスを設定するには、[ローカルコマンド許可の設定 \(907 ページ\)](#) を参照してください。

ステップ 2 Telnet および SSH セッションの管理許可をイネーブルにするには、**[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]** の順に選択し、[Perform authorization for exec shell access] 領域の [Enable] チェックボックスをオンにします。

ステップ 3 [Remote] または [Local] オプション ボタンを選択して、EXEC シェルアクセスの許可に使用するサーバを指定します。

ステップ 4 管理認可をイネーブルにするには、[Allow privileged users to enter into EXEC mode on login] チェックボックスをオンにします。

[auto-enable] オプションを選択すると、フルアクセスが許可されたユーザが直接特権 EXEC モードを開始できます。それ以外では、ユーザはユーザ EXEC モードになります。

コマンド認可の設定

コマンドへのアクセスを制御する場合、ASA ではコマンド許可を設定でき、ユーザが使用できるコマンドを決定できます。デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド (または、ローカルデータベースを使用するときは **login** コマンド) を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル
- TACACS+ サーバ特権レベル

コマンド認可について

コマンド認可を有効にし、承認済みのユーザにのみコマンド入力を許容することができます。

サポートされるコマンド認可方式

次の2つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：ASAでコマンド特権レベルを設定します。ローカルユーザ、RADIUSユーザ、またはLDAPユーザ（LDAP属性をRADIUS属性にマッピングする場合）をCLIアクセスについて認証する場合、ASAはそのユーザをローカルデータベース、RADIUS、またはLDAPサーバで定義されている特権レベルに所属させます。ユーザは、割り当てられた特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインするときに、ユーザEXECモード（レベル0または1のコマンド）にアクセスします。ユーザは、特権EXECモード（レベル2以上のコマンド）にアクセスするために再び**enable**コマンドで認証するか、**login**コマンドでログイン（ローカルデータベースに限る）できます。



(注) ローカルデータベース内にユーザが存在しなくても、またCLI認証や**enable**認証がない場合でも、ローカルコマンド許可を使用できます。代わりに、**enable**コマンドを入力するときにシステムイネーブルパスワードを入力すると、ASAによってレベル15に置かれます。次に、すべてのレベルのイネーブルパスワードを作成します。これにより、**enable n**（2～15）を入力したときに、ASAによってレベルnに置かれるようになります。これらのレベルは、ローカルコマンド許可を有効にするまで使用されません。

- TACACS+サーバ特権レベル：TACACS+サーバで、ユーザまたはグループがCLIアクセスについて認証した後で使用できるコマンドを設定します。CLIでユーザが入力するすべてのコマンドは、TACACS+サーバで検証されます。

セキュリティコンテキストとコマンド許可

AAA設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

コマンド許可を設定する場合は、各セキュリティコンテキストを別々に設定する必要があります。この設定により、異なるセキュリティコンテキストに対して異なるコマンド許可を実行できます。

セキュリティコンテキストを切り替える場合、管理者は、ログイン時に指定したユーザ名で許可されるコマンドが新しいコンテキストセッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。コマンド許可がセキュリティコンテキストによって異なる場合があることを管理者が理解していないと、混乱が生じる可能性があります。この動作は、次の仕組みによってさらに複雑になります。



- (注) システム実行スペースでは AAA コマンドがサポートされないため、システム実行スペースではコマンド許可を使用できません。

コマンド権限レベル

デフォルトでは、次のコマンドが特権レベル0に割り当てられます。その他のすべてのコマンドは特権レベル 15 に割り当てられます。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーションモードコマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。このようにしないと、ユーザはコンフィギュレーションモードに入ることができません。

ローカル コマンド許可の設定

ローカル コマンド許可を使用して、コマンドを 16 の特権レベル (0 ~ 15) の 1 つに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。各ユーザを特定の特権レベルに定義でき、各ユーザは割り当てられた特権レベル以下のコマンドを入力できます。ASA は、ローカルデータベース、RADIUS サーバ、または LDAP サーバ (LDAP 属性を RADIUS 属性にマッピングする場合) に定義されているユーザ特権レベルをサポートしています。

手順

- ステップ 1 **[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]** の順に選択します。
- ステップ 2 **[Enable authorization for ASA command access] > [Enable]** チェック ボックスをオンにします。

ステップ 3 [Server Group] ドロップダウンリストから [LOCAL] を選択します。

ステップ 4 ローカルコマンド許可をイネーブルにすると、オプションで、特権レベルを個々のコマンドまたはコマンドグループに手動で割り当てたり、事前定義済みユーザアカウント特権をイネーブルにしたりできます。

- 事前定義のユーザアカウント特権を使用するには、[Set ASDM Defined User Roles] をクリックします。

[ASDM Defined User Roles Setup] ダイアログボックスが表示されます。[Yes] をクリックすると、事前定義済みユーザアカウント特権を使用できるようになります。事前定義済みユーザアカウント特権には、[Admin] (特権レベル 15、すべての CLI コマンドへのフルアクセス権)、[Read Only] (特権レベル 5、読み取り専用アクセス権)、[Monitor Only] (特権レベル 3、[Monitoring] セクションへのアクセス権のみ) があります。

- コマンドレベルを手動で設定するには、[Configure Command Privileges] をクリックします。

[Command Privileges Setup] ダイアログボックスが表示されます。[Command Mode] ドロップダウンリストから [All Modes] を選択すると、すべてのコマンドを表示できます。代わりに、コンフィギュレーションモードを選択し、そのモードで使用可能なコマンドを表示することもできます。たとえば、[context] を選択すると、コンテキストコンフィギュレーションモードで使用可能なすべてのコマンドを表示できます。コンフィギュレーションモードだけでなく、ユーザ EXEC モードや特権 EXEC モードでも入力が可能で、かつモードごとに異なるアクションが実行されるようなコマンドを使用する場合は、これらのモードに対して別個に特権レベルを設定できます。

[Variant] カラムには、[show]、[clear]、または [cmd] が表示されます。特権は、コマンドの show 形式、clear 形式、または configure 形式に対してのみ設定できます。コマンドの configure 形式は、通常、未修正コマンド (show または clear プレフィックスなしで) または no 形式として、コンフィギュレーションの変更を引き起こす形式です。

コマンドのレベルを変更する場合は、コマンドをダブルクリックするか、[Edit] をクリックします。レベルは 0 ~ 15 の範囲で設定できます。設定できるのは、main コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

表示されているすべてのコマンドのレベルを変更する場合は、[Select All] をクリックした後に、[Edit] をクリックします。

[OK] をクリックして変更内容を確定します。

ステップ 5 (任意) [Perform authorization for exec shell access] > [Enable] チェックボックスをオンにして、コマンド認可のための AAA ユーザを有効にします。このオプションを入力しない場合、ASA は、ローカルデータベースユーザの特権レベルだけをサポートし、他のタイプのユーザをすべてデフォルトでレベル 15 に割り当てます。

さらに、このコマンドは管理認証を有効にします。[管理許可による CLI および ASDM アクセスの制限 \(903 ページ\)](#) を参照してください。

ステップ 6 [Apply] をクリックします。

許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

TACACS+ サーバでのコマンドの設定

グループまたは個々のユーザの共有プロファイル コンポーネントとしての Cisco Secure Access Control Server (ACS) TACACS+サーバでコマンドを設定できます。サードパーティの TACACS+サーバの場合は、コマンド許可サポートの詳細については、ご使用のサーバのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- ASA は、シェル コマンドとして許可するコマンドを送信し、TACACS+ サーバでシェル コマンドとしてコマンドを設定します。



(注) Cisco Secure ACS には、「pix-shell」と呼ばれるコマンドタイプが含まれている場合があります。このタイプは ASA コマンド許可に使用しないでください。

- コマンドの最初のワードは、メインコマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンドフィールドに **show running-configuration** を追加し、引数フィールドに **permit aaa-server** を入力します。

- [Permit Unmatched Args] チェックボックスをオンにすると、明示的に拒否していないすべてのコマンド引数を許可できます。

たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す疑問符や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします (次の図を参照)。

図 62: 関連するすべてのコマンドの許可

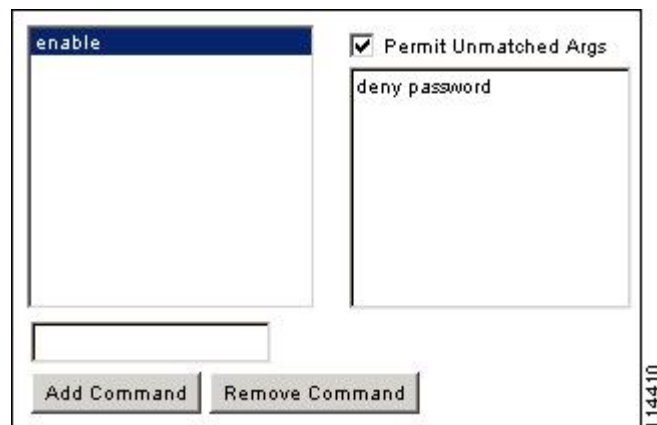
- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する必要があります（次の図を参照）。

図 63: 単一ワードのコマンドの許可

- 引数を拒否するには、その引数の前に **deny** を入力します。

たとえば、**enable** コマンドを許可し、**enable password** コマンドを許可しない場合には、コマンドフィールドに **enable** を入力し、引数フィールドに **deny password** を入力します。**enable** だけが許可されるように、必ず、[Permit Unmatched Args] チェックボックスをオンにしてください（次の図を参照）。

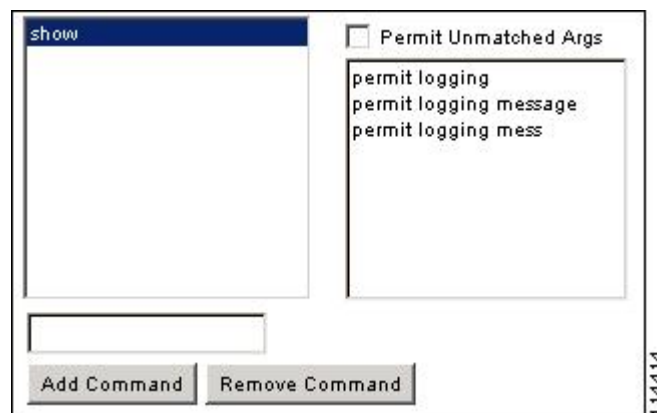
図 64: 引数の拒否



- コマンドラインでコマンドを省略形で入力した場合、ASA はプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバに送信します。

たとえば、**sh log** と入力すると、ASA は完全なコマンド **show logging** を TACACS+ サーバに送信します。一方、**sh log mess** と入力すると、ASA は展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバに送信します。省略形を予想して同じ引数の複数のスペルを設定できます（次の図を参照）。

図 65: 省略形の指定



- すべてのユーザに対して次の基本コマンドを許可することをお勧めします。
 - **show checksum**
 - **show curpriv**
 - **enable**
 - **help**
 - **show history**
 - **login**

- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

TACACS+ コマンド許可の設定

TACACS+ コマンド認可をイネーブルにし、ユーザが CLI でコマンドを入力すると、ASA はそのコマンドとユーザ名を TACACS+ サーバに送信し、コマンドが認可されているかどうかを判別します。

TACACS+ コマンド許可をイネーブルにする前に、TACACS+ サーバで定義されたユーザとして ASA にログインしていること、および ASA の設定を続けるために必要なコマンド許可があることを確認してください。たとえば、すべてのコマンドが認可された管理ユーザとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

意図したとおりに機能することが確認できるまで、設定を保存しないでください。間違いによりロックアウトされた場合、通常は ASA を再始動することによってアクセスを回復できます。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバシステムと ASA への完全冗長接続が必要です。たとえば、TACACS+ サーバプールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。

TACACS+ サーバを使用したコマンド許可を設定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] の順に選択します。

ステップ 2 [Enable authorization for command access] > [Enable] チェックボックスをオンにします。

ステップ 3 [Server Group] ドロップダウンリストから AAA サーバグループ名を選択します。

ステップ 4 (オプション) AAA サーバが使用不可になった場合のフォールバック方式としてローカルデータベースが使用されるように ASA を設定できます。設定するには、[Use LOCAL when server group fails] チェックボックスをオンにします。ローカルデータベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。必ずローカルデータベースのユーザとコマンド特権レベルを設定してください。

ステップ 5 [Apply] をクリックします。

コマンド許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されません。

ローカル データベース ユーザのパスワード ポリシーの設定

ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定できます。

パスワード ポリシーはローカル データベースを使用する管理ユーザに対してのみ適用されません。ローカル データベースを使用するその他のタイプのトラフィック（VPN や AAA によるネットワークアクセスなど）や、AAA サーバによって認証されたユーザには適用されません。

パスワードポリシーの設定後は、自分または別のユーザのパスワードを変更すると、新しいパスワードに対してパスワードポリシーが適用されます。既存のパスワードについては、現行のポリシーが適用されます。新しいポリシーは、[User Accounts] ペインおよび [Change My Password] ペインを使用したパスワードの変更に適用されます。

始める前に

- ローカルデータベースを使用して CLI または ASDM アクセスの AAA 認証を設定します。
- ローカル データベース内にユーザ名を指定します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [Password Policy] の順に選択します。

ステップ 2 次のオプションを任意に組み合わせて設定します。

- [Minimum Password Length] : パスワードの最小長を入力します。有効値の範囲は 3 ~ 64 文字です。推奨されるパスワードの最小長は 8 文字です。
- [Lifetime] : リモートユーザ (SSH、Telnet、HTTP) のパスワードの有効期間を日数で指定します。コンソールポートのユーザが、パスワードの有効期限切れでロックされることはありません。有効な値は、0 ~ 65536 です。デフォルト値は 0 日です。この場合、パスワードは決して期限切れになりません。

パスワードの有効期限が切れる 7 日前に、警告メッセージが表示されます。パスワードの有効期限が切れると、リモートユーザのシステム アクセスは拒否されます。有効期限が切れた後アクセスするには、次のいずれかの手順を実行します。

- 他の管理者にパスワードを変更してもらいます。
- 物理コンソールポートにログインして、パスワードを変更します。
- [Minimum Number Of] : 次のタイプの最短文字数を指定します。

- [Numeric Characters] : パスワードに含めなければならない数字の最小文字数を入力します。有効な値は、0 ~ 64 文字です。デフォルト値は 0 です
- [Lower Case Characters] : パスワードに含めなければならない小文字の最小文字数を入力します。有効値の範囲は 0 ~ 64 文字です。デフォルト値は 0 です
- [Upper Case Characters] : パスワードに含めなければならない大文字の最小文字数を入力します。有効値の範囲は 0 ~ 64 文字です。デフォルト値は 0 です
- [Special Characters] : パスワードに含めなければならない特殊文字の最小文字数を入力します。有効値の範囲は 0 ~ 64 文字です。特殊文字には、!、@、#、\$、%、^、&、*、(および) が含まれます。デフォルト値は 0 です。
- [Different Characters from Previous Password] : 新しいパスワードと古いパスワードで変えなければならない最小文字数を入力します。有効な値は、0 ~ 64 文字です。デフォルト値は 0 です文字マッチングは位置に依存しません。したがって、新しいパスワードで使用される文字が、現在のパスワードのどこにも使用されていない場合に限り、パスワードが変更されたとみなされます。

ステップ 3 (オプション) [Enable Password and Account Protection] チェックボックスをオンにして、ユーザが [User Accounts] ペインではなく、[Change My Password] ペインでパスワードを変更することを要件とします。デフォルト設定はディセーブルです。どちらの方法でも、ユーザはパスワードを変更することができます。

この機能をイネーブルにして、[User Accounts] ペインでパスワードを変更しようとする、次のエラーメッセージが表示されます。

```
ERROR: Changing your own password is prohibited
```

ステップ 4 [Apply] をクリックして、設定内容を保存します。

パスワードの変更

パスワードポリシーでパスワードの有効期間を設定した場合、有効期間を過ぎるとパスワードを新しいパスワードに変更する必要があります。パスワードポリシー認証をイネーブルにした場合は、このパスワード変更のスキームが必須です。パスワードポリシー認証がイネーブルでない場合は、このメソッドを使用することも、直接ユーザアカウントを変更することもできます。

username パスワードを変更するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [Change Password] の順に選択します。

ステップ 2 古いパスワードを入力します。

- ステップ3 新しいパスワードを入力します。
- ステップ4 確認のために新しいパスワードを再度入力します。
- ステップ5 [Make Change] をクリックします。
- ステップ6 [Save] アイコンをクリックして、実行コンフィギュレーションに変更を保存します。

管理アクセス アカウンティングの設定

CLIで **show** コマンド以外のコマンドを入力する場合、アカウンティングメッセージを TACACS+ アカウンティング サーバに送信できます。ユーザがログインするとき、ユーザが **enable** コマンドを入力するとき、またはユーザがコマンドを発行するときのアカウンティングを設定できます。

コマンドアカウンティングに使用できるサーバは、TACACS+ だけです。

管理アクセスおよびイネーブル コマンドアカウンティングを設定するには、次の手順を実行します。

手順

- ステップ1 **enable** コマンドを入力したユーザのアカウンティングを有効にするには、次の手順を実行します。
 - a) **[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Accounting]** の順に選択し、**[Require accounting to allow accounting of user activity] > [Enable]** チェックボックスをオンにします。
 - b) RADIUS または TACACS+ サーバグループ名を選択します。
- ステップ2 ユーザが Telnet、SSH、またはシリアル コンソールを使用して ASA にアクセスした場合にそのユーザのアカウンティングを有効化するには、次の手順を実行します。
 - a) **[Require accounting for the following types of connections]** 領域で、**[Serial]**、**[SSH]**、または **[Telnet]** チェックボックスをオンにします。
 - b) 各接続タイプの RADIUS または TACACS+ サーバグループ名を選択します。
- ステップ3 コマンドアカウンティングを設定するには、次の手順を実行します。
 - a) **[Require accounting for the following types of connections]** エリアで **[Enable]** チェックボックスをオンにします。
 - b) TACACS+ サーバグループ名を選択します。RADIUS はサポートされていません。

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティングメッセージを TACACS+ アカウンティング サーバに送信できます。
 - c) **[Command Privilege Setup]** ダイアログボックスを使用してコマンド特権レベルをカスタマイズする際、**[Privilege level]** ドロップダウンリストで最小特権レベルを指定することで、ASA のアカウンティング対象となるコマンドを制限できます。最小特権レベルよりも下のコマンドは、ASA で処理の対象となりません。

ステップ4 [Apply] をクリックします。

アカウント設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

ロックアウトからの回復

状況によっては、コマンド許可やCLI認証をオンにすると、ASA CLIからロックアウトされる場合があります。通常は、ASAを再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。

次の表に、一般的なロックアウト条件とその回復方法を示します。

表 44: CLI 認証およびコマンド許可のロックアウトシナリオ

機能	ロックアウト条件	説明	対応策：シングルモード	対応策：マルチモード
ローカル CLI 認証	ローカルデータベースにユーザが設定していない。	ローカルデータベース内にユーザが存在しない場合は、ログインできず、ユーザの追加もできません。	ログインし、パスワードと aaa コマンドをリセットします。	スイッチからASAへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザを追加することができます。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバが到達不能である場合は、ログインもコマンドの入力もできません。	<ol style="list-style-type: none"> ログインし、パスワードと AAA コマンドをリセットします。 サーバがダウンしたときにロックアウトされないように、ローカルデータベースをフォールバック方式として設定します。 	<ol style="list-style-type: none"> ASAでネットワークコンフィギュレーションが正しくないためにサーバが到達不能である場合は、スイッチからASAへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。 サーバがダウンしたときにロックアウトされないように、ローカルデータベースをフォールバック方式として設定します。

機能	ロックアウト条件	説明	対応策：シングルモード	対応策：マルチモード
TACACS+ コマンド許可	十分な特権のないユーザまたは存在しないユーザとしてログインした。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できません。	TACACS+ サーバのユーザアカウントを修正します。 TACACS+ サーバへのアクセス権がなく、ASA をすぐに設定する必要がある場合は、メンテナンスパーティションにログインして、パスワードと aaa コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド許可をディセーブルにすることもできます。
ローカル コマンド許可	十分な特権のないユーザとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できません。	ログインし、パスワードと aaa コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザレベルを変更することができます。

デバイス アクセスのモニタリング

- **[Monitoring] > [Properties] > [Device Access] > [ASDM/HTTPS/Telnet/SSH Sessions]**

上部ペインには、ASDM、HTTPS、および Telnet のセッションを介して接続するユーザの接続タイプ、セッション ID、および IP アドレスが示されます。特定のセッションを切断するには、[Disconnect] をクリックします。

下部ペインには、クライアント、ユーザ名、接続ステータス、ソフトウェアバージョン、入力暗号化タイプ、出力暗号化タイプ、入力 HMAC、出力 HMAC、SSH セッション ID、残りのキー再生成データ、残りのキー再生成時間、データベースのキー再生成、時間ベースのキー再生成、最後のキー再生成の時間が表示されます。特定のセッションを切断するには、[Disconnect] をクリックします。

- **[Monitoring] > [Properties] > [Device Access] > [Authenticated Users]**

このペインには、AAA サーバによって認証されたユーザのユーザ名、IP アドレス、ダイナミック ACL、非活動タイムアウト（存在する場合）、および絶対タイムアウトが一覧表示されます。

- **[Monitoring] > [Properties] > [Device Access] > [AAA Locked Out Users]**

このペインには、ロックアウトされた AAA ローカルユーザのユーザ名、失敗した認証の試行回数、およびユーザがロックアウトされた回数が一覧表示されます。ロックアウトさ

れた特定のユーザをクリアするには、[Clear Selected Lockout] をクリックします。ロックアウトされたすべてのユーザをクリアするには、[Clear All Lockouts] をクリックします。

• [Tools] > [Command Line Interface]

このペインでは、さまざまな非インタラクティブコマンドを発行し、結果を表示することができます。

管理アクセスの履歴

表 45: 管理アクセスの履歴

機能名	プラットフォーム リリース	説明
ASDM 管理認証	9.4(1)	<p>HTTP アクセスと Telnet および SSH アクセス別に管理認証を設定できるようになりました。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]</p>
証明書コンフィギュレーションの ASDM ユーザ名	9.4(1)	<p>ASDM の証明書認証を有効にすると、ASDM が証明書からユーザ名を抽出する方法を設定できます。また、ログインプロンプトでユーザ名を事前に入力して表示できます。</p> <p>次の画面が導入されました。 [Configuration] > [Device Management] > [Management Access] > [HTTP Certificate Rule]</p>
改善されたワンタイムパスワード認証	9.2(1)	<p>十分な認可特権を持つ管理者は、認証クレデンシャルを一度入力すると特権 EXEC モードに移行できます。 auto-enable オプションが aaa authorization exec コマンドに追加されました。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]。</p>

機能名	プラットフォーム リリース	説明
設定可能な SSH 暗号機能と整合性アルゴリズム	9.1(7)/9.4(3)	<p>ユーザは SSH 暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム (3des-cbc) が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、ssh cipher encryption custom aes128-cbc を使用します。</p> <p>次の画面が導入されました。 [Configuration] > [Device Management] > [Advanced] > [SSH Ciphers]</p>
SSH の AES-CTR 暗号化	9.1(2)	ASA での SSH サーバの実装が、AES-CTR モードの暗号化をサポートするようになりました。
SSH キー再生成間隔の改善	9.1(2)	SSH 接続は、接続時間 60 分間またはデータ トラフィック 1 GB ごとに再生成されます。 。
マルチコンテキストモードの ASASM において、スイッチからの Telnet 認証および仮想コンソール認証をサポートしました。	8.5(1)	マルチコンテキストモードのスイッチから ASASM への接続はシステム実行スペースに接続しますが、これらの接続を制御するために管理コンテキストでの認証を設定できます。

機能名	プラットフォーム リリース	説明
ローカルデータベースを使用する場合の管理者パスワードポリシーのサポート	8.4(4.1)、9.1(2)	<p>ローカルデータベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワードポリシーを設定できます。</p> <p>次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [Password Policy]。</p>
SSH 公開キー認証のサポート	8.4(4.1)、9.1(2)	<p>ASA への SSH 接続の公開キー認証は、ユーザ単位で有効にできます。公開キーファイル (PKF) でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式 (最大 2048 ビット) では大きすぎるキーについては、PKF 形式を使用します。</p> <p>次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication][Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF]。</p> <p>PKF キー形式のサポートは 9.1(2) 以降のみです。</p>
SSH キー交換の Diffie-Hellman グループ 14 のサポート	8.4(4.1)、9.1(2)	<p>SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまでは、グループ 1 だけがサポートされていました。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]。</p>

機能名	プラットフォーム リリース	説明
管理セッションの最大数のサポート	8.4(4.1)、9.1(2)	<p>同時 ASDM、SSH、Telnet セッションの最大数を設定できます。</p> <p>次の画面が導入されました。 [Configuration] > [Device Management] > [Management Access] > [Management Session Quota]。</p>
SSH セキュリティが向上し、SSH デフォルトユーザ名はサポートされなくなりました。	8.4(2)	<p>8.4(2) 以降、pix または asa ユーザ名とログインパスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、aaa authentication ssh console LOCAL コマンド (CLI) または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカルユーザを定義する必要があります。定義するには、username コマンド (CLI) を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカルデータベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。</p>

機能名	プラットフォーム リリース	説明
管理アクセス	7.0(1)	<p>この機能が導入されました。</p> <p>次の画面が導入されました。</p> <p>[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH][Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner][Configuration] > [Device Management] > [Management Access] > [CLI Prompt][Configuration] > [Device Management] > [Management Access] > [ICMP][Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client][Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server][Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points][Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication][Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization][Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Accounting]。</p>



第 37 章

ソフトウェアおよびコンフィギュレーション

この章では、Cisco ASA ソフトウェアおよびコンフィギュレーションの管理方法について説明します。

- ソフトウェアのアップグレード (923 ページ)
- ROMMON を使用したイメージのロード (923 ページ)
- ROMMON を使用した ASASM のイメージのロード (925 ページ)
- ROMMON イメージのアップグレード (ASA 5506-X、5508-X、および 5516-X) (927 ページ)
- ASA 5506W-X ワイヤレスアクセスポイントのイメージの回復およびロード (928 ページ)
- ソフトウェアのダウングレード (929 ページ)
- ファイルの管理 (930 ページ)
- ASA イメージ、ASDM、およびスタートアップコンフィギュレーションの設定 (939 ページ)
- コンフィギュレーションまたはその他のファイルのバックアップおよび復元 (941 ページ)
- システム再起動のスケジュール (946 ページ)
- Auto Update の設定 (947 ページ)
- ソフトウェアとコンフィギュレーションの履歴 (954 ページ)

ソフトウェアのアップグレード

完全なアップグレードの手順については、『[Cisco ASA Upgrade Guide](#)』を参照してください。

ROMMON を使用したイメージのロード

TFTP を使用して ROMMON モードから ASA へソフトウェア イメージをロードするには、次の手順を実行します。

手順

- ステップ1** [アプライアンス コンソールへのアクセス \(27 ページ\)](#) に従って、ASA のコンソール ポートに接続します。
- ステップ2** ASA の電源を切ってから、再び電源をオンにします。
- ステップ3** スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。
- ステップ4** ROMMON モードで、IP アドレス、TFTP サーバアドレス、ゲートウェイアドレス、ソフトウェア イメージ ファイル、およびポートを含む、ASA に対するインターフェイス設定を次のように定義します。

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

(注) ネットワークへの接続がすでに存在することを確認してください。

インターフェイス コマンドは ASA 5506-X、ASA 5508-X、および ASA 5516-X プラットフォームで無視されるため、これらのプラットフォームで Management 1/1 インターフェイスから TFTP リカバリを実行する必要があります。

- ステップ5** 設定を検証します。

```
rommon #6> set
ROMMON Variable Settings:
ADDRESS=10.86.118.3
SERVER=10.86.118.21
GATEWAY=10.86.118.21
PORT=GigabitEthernet0/0
VLAN=untagged
IMAGE=asa961-smp-k8.bin
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20
```

- ステップ6** TFTP サーバに ping を送信します。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

- ステップ7** ネットワーク設定を、後で使用できるように保管しておきます。

```
rommon #8> sync
Updating NVRAM Parameters...
```


ステップ 8 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

ステップ 9 ROMMON モードから ASA を起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュメモリにダウンロードする必要があります。「[ソフトウェアのアップグレード \(923 ページ\)](#)」を参照してください。

ROMMON を使用した ASASM のイメージのロード

TFTP を使用して ROMMON モードから ASASM へソフトウェア イメージをロードするには、次の手順を実行します。

手順

- ステップ 1** [ASA サービス モジュール コンソールへのアクセス \(30 ページ\)](#) に従って、ASA のコンソール ポートに接続します。
- ステップ 2** ASASM イメージをリロードすることを確認してください。
- ステップ 3** スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。
- ステップ 4** ROMMON モードで、IP アドレス、TFTP サーバアドレス、ゲートウェイアドレス、ソフトウェア イメージファイル、ポートおよび VLAN を含む、ASASM に対するインターフェイス設定を次のように定義します。

```
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
rommon #5> interface Data0
rommon #6> vlan 1
Data0
Link is UP
MAC Address: 0012.d949.15b8
```

(注) ネットワークへの接続がすでに存在することを確認してください。

ステップ5 設定を検証します。

```
rommon #7> set
ROMMON Variable Settings:
ADDRESS=10.86.118.4
SERVER=10.86.118.21
GATEWAY=10.86.118.21
PORT=Data0
VLAN=1
IMAGE=asa961-smp-k8.bin
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=2
RETRY=20
```

ステップ6 TFTP サーバに ping を送信します。

```
rommon #8> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 2 seconds:

Success rate is 100 percent (20/20)
```

ステップ7 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
Clearing EOBC receive queue ...
cmostime_set = 1
ROMMON Variable Settings:
ADDRESS=10.86.118.3
SERVER=10.86.118.21
GATEWAY=10.86.118.21
PORT=Data0
VLAN=1
IMAGE=asa961-smp-k8.bin
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21
Starting download. Press ESC to abort.
```

ソフトウェアイメージが正常にロードされると、ASASM は自動的に ROMMON モードを終了します。

- ステップ 8** ROMMON モードからモジュールを起動する場合、システムイメージはリロード間で保持されないため、やはりイメージをフラッシュメモリにダウンロードする必要があります。「[ソフトウェアのアップグレード \(923 ページ\)](#)」を参照してください。

ROMMON イメージのアップグレード (ASA 5506-X、5508-X、および 5516-X)

ASA 5506-X シリーズ、ASA 5508-X、および ASA 5516-X の ROMMON イメージをアップグレードするには、次の手順に従います。システムの ROMMON バージョンは 1.1.8 以上でなければなりません。



注意

1.1.15 の ROMMON のアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります (約 15 分)。アップグレード中はデバイスの電源を再投入しないでください。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコテクニカルサポートに連絡してください。デバイスの電源を再投入したり、リセットしたりしないでください。

始める前に

新バージョンへのアップグレードのみ可能です。ダウングレードはできません。現在のバージョンを確認するには、**show module** コマンドを入力して、MAC アドレス範囲テーブルの Mod 1 の出力で Fw バージョンを調べます。

```
ciscoasa# show module
[...]
Mod  MAC Address Range                Hw Version  Fw Version  Sw Version
-----
  1  7426.aceb.ccea to 7426.aceb.ccf2  0.3         1.1.5       9.4(1)
sfr  7426.aceb.cce9 to 7426.aceb.cce9  N/A         N/A
```

手順

- ステップ 1** Cisco.com から新しい ROMMON イメージを取得して、サーバ上に置いて ASA にコピーします。この手順では、TFTP コピーの方法を説明します。

次の URL からイメージをダウンロードします。

<https://software.cisco.com/download/type.html?mdfid=286283326&flowid=77251>

- ステップ 2** ROMMON イメージを ASA フラッシュメモリにコピーします。

```
copy tftp://server_ip/asa5500-firmware-xxxx.SPA disk0:asa5500-firmware-xxxx.SPA
```

ステップ 3 ROMMON イメージをアップグレードします。

```
upgrade rommon disk0:asa5500-firmware-xxxx.SPA
```

例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecce1308fc64427367fa559e9
                ee8f182491652ee4c05e6e751f7a4f
                5cdea28540cf60acde3ab9b65ff55a9f
                4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecce1308fc64427367fa559e9
                ee8f182491652ee4c05e6e751f7a4f
                5cdea28540cf60acde3ab9b65ff55a9f
                4e0cfb84b9e2317a856580576612f4af

Digital signature successfully validated
File Name       : disk0:/asa5500-firmware-1108.SPA
Image type      : Release
  Signer Information
    Common Name      : abraxas
    Organization Unit : NCS_Kenton_ASA
    Organization Name : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm   : SHA2 512
    Signature Algorithm : 2048-bit RSA
    Key Version      : A
Verification successful.
Proceed with reload? [confirm]
```

ステップ 4 プロンプトが表示されたら、確認して ASA をリロードします。

ASA が ROMMON イメージをアップグレードした後、ASA の OS をリロードします。

ASA 5506W-X ワイヤレス アクセス ポイントのイメージの回復およびロード

TFTP を使用してソフトウェア イメージを回復して ASA 5506W-X にロードするには、次の手順を実行します。

手順

ステップ 1 アクセス ポイント (AP) へのセッションを確立し、AP ROMMON (ASA ROMMON ではなく) を開始します。

```
ciscoasa# hw-module module wlan recover image
```

ステップ2 [Cisco Aironet アクセス ポイント Cisco IOS ソフトウェア コンフィギュレーション ガイド \[英語\]](#) の手順に従います。

ソフトウェアのダウングレード

ダウングレードでは、以下の機能を完了するためのショートカットが存在します。

- ブート イメージ コンフィギュレーションのクリア (**clear configure boot**)。
- 古いイメージへのブート イメージの設定 (**boot system**)。
- (オプション) 新たなアクティベーション キーの入力 (**activation-key**)。
- 実行コンフィギュレーションのスタートアップへの保存 (**write memory**)。これにより、BOOT環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
- スタートアップコンフィギュレーションへの古いコンフィギュレーションのコピー (**copy old_config_url startup-config**)。
- リロード (**reload**)。

始める前に

- クラスタリング用の公式のゼロ ダウンタイム ダウングレードのサポートはありません。ただし場合によっては、ゼロ ダウンタイム ダウングレードが機能します。ダウングレードに関する次の既知の問題を参照してください。この他の問題が原因でクラスタユニットのリロードが必要になることもあり、その場合はダウンタイムが発生します。
 - クラスタリングを使用する場合に 9.2(1)以降から 9.1 以前にダウングレードする：ゼロ ダウンタイム ダウングレードはサポートされません。
- PBKDF2 (パスワードベースのキー派生関数2) ハッシュをパスワードで使用する場合に 9.5 以前のバージョンにダウングレードする：9.6 より前のバージョンはPBKDF2ハッシュをサポートしていません。9.6(1)では、32文字より長い **enable** パスワードおよび **username** パスワードでPBKDF2ハッシュを使用します。ダウングレードすると、**enable** パスワードがデフォルト (空白) に戻ります。ユーザ名は正しく解析されず、**username** コマンドが削除されます。ローカルユーザをもう一度作成する必要があります。
- ASAv 用のバージョン 9.5(2.200) からのダウングレード：ASAv はライセンス登録状態を保持しません。**license smart register idtoken id_token force** コマンドで再登録する必要があります (ASDM の場合、[Configuration]>[Device Management]>[Licensing]>[Smart Licensing] ページで [Force registration] オプションを使用)。Smart Software Manager から ID トークンを取得します。

- 設定を移行すると、ダウングレードの可否に影響を与える可能性があります。そのため、ダウングレード時に使用できる古い設定のバックアップを保持することを推奨します。8.3 へのアップグレード時には、バックアップが自動的に作成されます (`<old_version>_startup_cfg.sav`)。他の移行ではバックアップが作成されません。古いバージョンでは利用できなかったコマンドが新しい設定に含まれていると、設定がロードされたときにそれらのコマンドのエラーが表示されます。ただし、エラーは無視できます。各バージョンの設定の移行または廃止の詳細については、各バージョンのアップグレードガイドを参照してください。
- 元のトンネルがネゴシエートした暗号スイートをサポートしないソフトウェアバージョンをスタンバイ装置が実行している場合でも、VPN トンネルがスタンバイ装置に複製されます。このシナリオは、ダウングレード時に発生します。その場合、VPN 接続を切断して再接続してください。

手順

ステップ 1 [Tools] > [Downgrade Software] を選択します。

[Downgrade Software] ダイアログボックスが表示されます。

ステップ 2 ASA イメージの場合、[Select Image File] をクリックします。

[Browse File Locations] ダイアログボックスが表示されます。

ステップ 3 次のいずれかのオプション ボタンをクリックします。

- [Remote Server] : ドロップダウン リストで [ftp]、[smb]、[http] のいずれかを選択し、以前のイメージファイルのパスを入力します。
- [Flash File System] : [Browse Flash] をクリックして、ローカル フラッシュ ファイル システムにある以前のイメージファイルを選択します。

ステップ 4 [Configuration] で [Browse Flash] をクリックし、移行前の設定ファイルを選択します。

ステップ 5 (任意) バージョン 8.3 よりも前のアクティベーション キーに戻す場合は、[Activation Key] フィールドで以前のアクティベーション キーを入力します。

ステップ 6 [Downgrade] をクリックします。

ファイルの管理

ASDM には、基本的なファイル管理タスクを実行するのに便利なファイル管理ツールセットが用意されています。ファイル管理ツールにより、フラッシュメモリに保存されているファイルの表示、移動、コピー、および削除、ファイルの転送、およびリモートストレージデバイス (マウントポイント) のファイルの管理を行うことができます。



(注) マルチコンテキスト モードの場合、このツールはシステムのセキュリティ コンテキストでだけ使用できます。

ファイルアクセスの設定

ASA では、FTP クライアント、セキュア コピー クライアント、または TFTP クライアントを使用できます。また、ASA をセキュア コピー サーバとして設定することもできるため、コンピュータでセキュア コピー クライアントを使用できます。

FTP クライアント モードの設定

ASA では、FTP サーバとの間で、イメージファイルやコンフィギュレーションファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブモードではデータ接続の受け入れ側となるサーバは、今回の特定の接続においてリッスンするポート番号を応答として返します。

手順

ステップ 1 [Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client] ペインで、[Specify FTP mode as passive] チェックボックスをオンにします。

ステップ 2 [Apply] をクリックします。

FTP クライアントのコンフィギュレーションが変更され、その変更内容が実行コンフィギュレーションに保存されます。

セキュア コピー サーバとしての ASA の設定

ASA 上でセキュア コピー (SCP) サーバをイネーブルにできます。SSH による ASA へのアクセスを許可されたクライアントだけが、セキュア コピー接続を確立できます。

始める前に

- サーバにはディレクトリサポートがありません。ディレクトリサポートがないため、ASA の内部ファイルへのリモート クライアント アクセスは制限されます。
- サーバでは、バナーまたはワイルドカードがサポートされていません。
- [HTTPS \(ASDM\) アクセスの設定 \(886 ページ\)](#) に従って、ASA で SSH を有効にします。
- SSH バージョン 2 接続をサポートするには、ASA のライセンスに強力な暗号化 (3DES/AES) ライセンスが必要です。

- 特に指定されていないかぎり、マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、[Configuration]>[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- セキュア コピーのパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム (3des-cbc) が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提示された暗号方式を変更するには、[Configuration] > [Device Management] > [Advanced] > [SSH Ciphers] ペインを使用します。たとえば、[Custom] を選択して aes128-cbc に設定します。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP)] の順に選択します。
- マルチ モードの場合、[Configuration] > [Device Management] > [Device Administration] > [Secure Copy] の順に選択します。

ステップ 2 [Enable secure copy server] チェック ボックスをオンにします。

ステップ 3 (オプション) ASA は接続先の各 SCP サーバの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバとそのキーを追加または削除できます。

キーを追加するには、次の手順を実行します。

- a) 新しいサーバの [Add] をクリックするか、または信頼できる SSH ホストのテーブルからサーバを選択し、[Edit] をクリックします。
- b) 新しいサーバの [Host] フィールドに、サーバの IP アドレスを入力します。
- c) [Add public key for the trusted SSH host] チェックボックスをオンにします。
- d) 次のいずれかのキーを指定します。
 - フィンガープリント：すでにハッシュされているキーを入力します。たとえば、**show** コマンドの出力からコピーしたキーです。
 - キー：SSH ホストの公開キーまたはハッシュ値を入力します。キー スtring はリモートピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから (言い換えると .ssh/id_rsa.pub ファイルから) 公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

キーを削除するには、信頼できる SSH ホストのテーブルからサーバを選択し、[Delete] をクリックします。

ステップ 4 (オプション) 新しいホストキーが検出されたときに通知を受け取るには、[Inform me when a new host key is detected] チェックボックスをオンにします。

デフォルトで、このオプションは有効になっています。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められます。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

ステップ 5 [Apply] をクリックします。

例

外部ホストのクライアントから、SCP ファイル転送を実行します。たとえば、Linux では次のコマンドを入力します。

```
scp -v -pw password source_filename username@asa_address:{disk0|disk1}:/dest_filename
```

-v は冗長を表します。-pw が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

ASA TFTP クライアントのパス設定

TFTP は、単純なクライアント/サーバファイル転送プロトコルで、RFC 783 および RFC 1350 Rev. 2 で規定されています。TFTP サーバとの間でファイルをコピーできるように、ASA を TFTP クライアントとして設定できます。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数の ASA にプロパゲートできます。

ここでは、TFTP サーバへのパスを事前定義できるため、**copy** および **configure net** などのコマンドで入力する必要がなくなります。

手順

- ステップ 1** [Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択し、[Enable] チェックボックスをオンにします。
- ステップ 2** [Interface Name] ドロップダウン リストから、TFTP クライアントとして使用するインターフェイスを選択します。
- ステップ 3** コンフィギュレーション ファイルの保存先とする TFTP サーバの IP アドレスを [IP Address] フィールドに入力します。
- ステップ 4** コンフィギュレーション ファイルの保存先とする TFTP サーバへのパスを [Path] フィールドに入力します。
例 : /tftpboot/asa/config3
- ステップ 5** Apply をクリックします。

マウントポイントの追加

CIFS マウントポイントまたは FTP マウントポイントを追加できます。

CIFS マウントポイントの追加

共通インターネットファイルシステム (CIFS) マウントポイントを定義するには、次の手順を実行します。

手順

-
- ステップ 1 **[Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points]** の順に選択し、**[Add] > [CIFS Mount Point]** の順にクリックします。
[Add CIFS Mount Point] ダイアログボックスが表示されます。
 - ステップ 2 **[Enable mount point]** チェックボックスをオンにします。
これにより、ASA 上の CIFS ファイルシステムが UNIX のファイルツリーに接続されます。
 - ステップ 3 **[Mount Point Name]** フィールドに、既存の CIFS が存在する位置の名前を入力します。
 - ステップ 4 **[Server Name]** フィールドまたは **[IP Address]** フィールドに、マウントポイントを配置するサーバの名前または IP アドレスを入力します。
 - ステップ 5 **[Share Name]** フィールドに、CIFS サーバ上のフォルダの名前を入力します。
 - ステップ 6 **[NT Domain Name]** フィールドに、サーバが常駐する NT ドメインの名前を入力します。
 - ステップ 7 サーバに対するファイルシステムのマウントを認可されているユーザの名前を、**[User Name]** フィールドに入力します。
 - ステップ 8 サーバに対するファイルシステムのマウントを認可されているユーザのパスワードを、**[Password]** フィールドに入力します。
 - ステップ 9 **[Confirm Password]** フィールドにパスワードを再入力します。
 - ステップ 10 **[OK]** をクリックします。
[Add CIFS Mount Point] ダイアログボックスが閉じます。
 - ステップ 11 **[Apply]** をクリックします。
-

FTP マウントポイントの追加

FTP マウントポイントの場合、FTP サーバには UNIX のディレクトリリストスタイルが必要です。Microsoft FTP サーバには、デフォルトで MS-DOS ディレクトリリストスタイルがあります。

手順

-
- ステップ 1** [Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points] の順に選択し、[Add] > [FTP Mount Point] の順にクリックします。
- [Add FTP Mount Point] ダイアログボックスが表示されます。
- ステップ 2** [Enable] チェックボックスを選択します。
- これにより、ASA 上の FTP ファイル システムが UNIX のファイル ツリーに接続されます。
- ステップ 3** [Mount Point Name] フィールドに、既存の FTP が存在する位置の名前を入力します。
- ステップ 4** [Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバの名前または IP アドレスを入力します。
- ステップ 5** [Mode] フィールドで、オプション ボタン ([Active] または [Passive]) をクリックして FTP モードを選択します。[Passive] モードを選択した場合、クライアントでは、FTP コントロール接続とデータ接続がともに起動します。サーバは、この接続をリッスンするポートの番号で応答します。
- ステップ 6** FTP ファイル サーバへのディレクトリ パス名を [Path to Mount] フィールドに入力します。
- ステップ 7** サーバに対するファイル システムのマウントを認可されているユーザの名前を、[User Name] フィールドに入力します。
- ステップ 8** サーバに対するファイル システムのマウントを認可されているユーザのパスワードを、[Password] フィールドに入力します。
- ステップ 9** [Confirm Password] フィールドにパスワードを再入力します。
- ステップ 10** [OK] をクリックします。
- [Add FTP Mount Point] ダイアログボックスが閉じます。
- ステップ 11** [Apply] をクリックします。
-

ファイル管理ツールへのアクセス

ファイル管理ツールを使用するには、次の手順を実行します。

手順

-
- ステップ 1** メイン ASDM アプリケーション ウィンドウで、[Tools] > [File Management] の順に選択します。
- [File Management] ダイアログボックスが表示されます。
- [Folders] ペインには、ディスク上にあるフォルダが表示されます。
 - [Flash Space] は、フラッシュ メモリの合計容量と、使用可能なメモリ容量を示します。

- [Files] 領域には、選択したフォルダのファイルについて次の情報が表示されます。
 - パス
 - ファイル名
 - サイズ (バイト単位)
 - 修正時刻
 - 選択したファイルの種類 (ブート コンフィギュレーション、ブートイメージファイル、ASDM イメージファイル、SVC イメージファイル、CSD イメージファイル、または APCF イメージファイル) を示す、ステータス

- ステップ 2** 選択したファイルをブラウザに表示するには、[View] をクリックします。
- ステップ 3** 選択したファイルを切り取って別のディレクトリに貼り付けるには、[Cut] をクリックします。
- ステップ 4** 選択したファイルをコピーして別のディレクトリに貼り付けるには、[Copy] をクリックします。
- ステップ 5** コピーしたファイルを選択した場所に貼り付けるには、[Paste] をクリックします。
- ステップ 6** 選択したファイルをフラッシュ メモリから削除するには、[Delete] をクリックします。
- ステップ 7** ファイルの名前を変更するには、[Rename] をクリックします。
- ステップ 8** ファイルを保存するディレクトリを新規作成するには、[New Directory] をクリックします。
- ステップ 9** [File Transfer] ダイアログボックスを開くには、[File Transfer] をクリックします。詳細については、「[ファイルの転送 \(936 ページ\)](#)」を参照してください。
- ステップ 10** [Manage Points] ダイアログボックスを開くには、[Mount Points] をクリックします。詳細については、「[マウント ポイントの追加 \(934 ページ\)](#)」を参照してください。

ファイルの転送

File Transfer ツールにより、ローカルにあるファイルとリモートにあるファイルを転送できます。PC またはフラッシュ ファイル システムのローカル ファイルを ASA との間で転送できます。HTTP、HTTPS、TFTP、FTP、または SMB を使用して、ASA との間でファイルを転送できます。



- (注) IPS SSP ソフトウェア モジュールの場合、IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリに少なくとも 50% の空きがあることを確認してください。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。

ローカル PC とフラッシュ間でのファイル転送

ローカル PC とフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

手順

-
- ステップ 1** メイン ASDM アプリケーション ウィンドウで、**[Tools] > [File Management]** の順に選択します。
- [File Management] ダイアログボックスが表示されます。
- ステップ 2** [File Transfer] の横にある下矢印をクリックし、続いて [Between Local PC and Flash] をクリックします。
- [File Transfer] ダイアログボックスが表示されます。
- ステップ 3** ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、目的の場所にドラッグします。または、ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、右矢印または左矢印をクリックし、目的の場所にファイルを転送します。
- ステップ 4** 完了したら [Close] をクリックします。
-

リモートサーバとフラッシュ間でのファイル転送

リモートサーバとフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

手順

-
- ステップ 1** メイン ASDM アプリケーション ウィンドウで、**[Tools] > [File Management]** の順に選択します。
- [File Management] ダイアログボックスが表示されます。
- ステップ 2** [File Transfer] ドロップダウン リストで下矢印をクリックし、[Between Remote Server and Flash] をクリックします。
- [File Transfer] ダイアログボックスが表示されます。
- ステップ 3** リモートサーバからファイルを転送するには、[Remote server] オプションをクリックします。
- ステップ 4** 転送対象になるソース ファイルを定義します。
- サーバの IP アドレスを含めたファイルの場所へのパスを選択します。
- (注) ファイル転送は IPv4 および IPv6 のアドレスをサポートしています。
- FTP の場合はリモートサーバのタイプを、HTTP または HTTPS の場合はリモートサーバのポート番号を入力します。有効な FTP タイプは次のとおりです。
 - ap : パッシブ モードの ASCII ファイル
 - an : 非パッシブ モードの ASCII ファイル

- ip : パッシブモードのバイナリイメージファイル
- in : 非パッシブモードのバイナリイメージファイル

- ステップ 5** フラッシュファイルシステムからファイルを転送するには、[Flash file system] オプションを選択します。
- ステップ 6** ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。
- ステップ 7** また、CLIにより、スタートアップコンフィギュレーション、実行コンフィギュレーション、またはSMBファイルシステムからファイルをコピーすることもできます。**Copy** コマンドの使用方法については、CLIコンフィギュレーションガイドを参照してください。
- ステップ 8** 転送するファイルの宛先を定義します。
- a) フラッシュファイルシステムにファイルを転送するには、[Flash file system] オプションを選択します。
 - b) ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。
- ステップ 9** リモートサーバにファイルを転送するには、[Remote server] オプションを選択します。
- a) ファイルの場所へのパスを入力します。
 - b) FTP転送の場合はタイプを入力します。有効なタイプは次のとおりです。
 - ap : パッシブモードのASCIIファイル
 - an : 非パッシブモードのASCIIファイル
 - ip : パッシブモードのバイナリイメージファイル
 - in : 非パッシブモードのバイナリイメージファイル
- ステップ 10** [Transfer] をクリックしてファイル転送を開始します。
[Enter Username and Password] ダイアログボックスが表示されます。
- ステップ 11** リモートサーバのユーザ名、パスワード、ドメイン（必要な場合）が表示されます。
- ステップ 12** [OK] をクリックし、ファイル転送を続行します。
ファイル転送プロセスには数分かかる場合があります。必ず終了するまでお待ちください。
- ステップ 13** ファイル転送が完了したら [Close] をクリックします。
-

ASA イメージ、ASDM、およびスタートアップコンフィギュレーションの設定

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブートイメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップコンフィギュレーションでは、コンフィギュレーションファイルを任意で指定できます。

次のモデルのガイドラインを参照してください。

- Firepower 9300 シャーシ：ASA のアップグレードは FXOS によって管理されます。ASA オペレーティングシステム内で ASA をアップグレードすることはできません。したがって、この手順を ASA イメージに使用しないでください。ASA と FXOS を別々にアップグレードすることができ、FXOS ディレクトリ リストに別々にリストされます。ASA パッケージには常に ASDM が含まれています。
- Firepower 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージと一緒にバンドルされています。パッケージ更新は FXOS によって管理されます。ASA オペレーティングシステム内で ASA をアップグレードすることはできません。したがって、この手順を ASA イメージに使用しないでください。ASA と FXOS を個別にアップグレードすることはできません。常にバンドルされています。
- Firepower モデルの ASDM：ASDM は ASA オペレーティングシステム内からアップグレードできるため、バンドルされた ASDM イメージのみを使用する必要はありません。手動でアップロードする ASDM イメージは FXOS イメージリストに表示されません。ASA から ASDM イメージを管理する必要があります。



(注) ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、バンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。ただし、アップロードした別の ASDM イメージ (たとえば **asdm-782.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ (**asdm.bin**) を使用するよう ASA を再設定する必要があります。

- ASAv：初期展開の ASAv パッケージでは、ASA イメージが読み取り専用 boot:/パーティションに配置されます。ASAv をアップグレードするときは、フラッシュメモリに別のイメージを指定します。後でコンフィギュレーションをクリアすると、ASAv は元の展開のイメージをロードするようになることに注意してください。初期展開の ASAv パッケージ

には、フラッシュ メモリに配置される ASDM イメージも含まれています。ASDM イメージを個別にアップグレードできます。

次のデフォルト設定を参照してください。

- ASA イメージ：
 - 物理 ASA：内部フラッシュ メモリ内で見つかった最初のアプリケーション イメージをブートします。
 - ASA v：最初に展開したときに作成された、読み取り専用の boot:/パーティションにあるイメージをブートします。
 - Firepower 9300 シャーシ：どの ASA イメージをブートするかは FXOS システムによって決定されます。この手順を使用して ASA イメージを設定することはできません。
- すべての ASA の ASDM イメージ：内部フラッシュ メモリ内で見つかった（またはここにイメージがない場合は、外部フラッシュ メモリ内で見つかった）最初の ASDM イメージをブートします。
- スタートアップ コンフィギュレーション：デフォルトでは、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

手順

ステップ 1 [Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration] の順に選択します。

起動イメージとして使用するバイナリ イメージ ファイルは、ローカルから 4 つまで指定できます。また TFTP サーバのイメージを 1 つ指定して、そこからデバイスをブートできます。TFTP サーバに格納されているイメージを指定する場合は、そのファイルをリスト内の先頭に配置する必要があります。デバイスが、イメージのロード元の TFTP サーバに到達できない場合は、フラッシュ メモリに保存されているリスト内の次のイメージ ファイルのロードが試行されます。

ステップ 2 [Boot Image/Configuration] ペインで [Add] をクリックします。

ステップ 3 ブートするイメージを参照します。TFTP イメージの場合は、[File Name] フィールドに TFTP URL を入力します。[OK] をクリックします。

ステップ 4 上へ移動ボタンと下へ移動ボタンを使用してイメージの順番を並べ替えます。

ステップ 5 (オプション) [Boot Configuration File Path] フィールドで、[Browse Flash] をクリックしてコンフィギュレーションを選択してスタートアップ コンフィギュレーション ファイルを指定します。[OK] をクリックします。

ステップ 6 [ASDM Image File Path] フィールドで、[Browse Flash] をクリックしてイメージを選択して ASDM イメージを指定します。[OK] をクリックします。

ステップ 7 [Apply] をクリックします。

コンフィギュレーションまたはその他のファイルのバックアップおよび復元

システム障害から保護するために、コンフィギュレーションおよびその他のファイルの定期的なバックアップを実行することを推奨します。

完全なシステム バックアップまたは復元の実行

次の手順では、コンフィギュレーションおよびイメージの zip バックアップ zip ファイルへのバックアップおよび復元方法と、そのファイルのローカルコンピュータへの転送方法について説明します。

バックアップまたは復元を開始する前に

- バックアップまたは復元を開始する前に、バックアップまたは復元場所に使用可能なディスク領域が少なくとも 300 MB ある必要があります。
- ASA は、シングル コンテキスト モードである必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。結果として、ASA は異なる挙動をすることもあります。
- 一度に開始できるバックアップまたは復元は 1 つだけです。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、ASA は、新しい ASA OS をロードした時に常駐するスタートアップコンフィギュレーションを自動的にアップグレードします。
- クラスタリングを使用する場合、バックアップまたは復元できるのは、スタートアップコンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみです。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップコンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスター パスフレーズが不明な場合は、[マスター パスフレーズの設定 \(576 ページ\)](#) を参照して、バックアップを続行する前に、マスター パスフレーズをリセットする方法を確認してください。

- PKCS12 データをインポート (**crypto ca trustpoint** コマンドを使用) する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップコンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キーペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキーペアには必ず同じ名前を使用してください。
- CLI を使用してバックアップしてから ASDM を使用して復元したり、その逆を行うことはできません。
- 各バックアップ ファイルに含まれる内容は次のとおりです。
 - 実行コンフィギュレーション
 - スタートアップ コンフィギュレーション
 - すべてのセキュリティ イメージ
 - Cisco Secure Desktop およびホスト スキャンのイメージ
 - Cisco Secure Desktop およびホスト スキャンの設定
 - AnyConnect (SVC) クライアントのイメージおよびプロファイル
 - AnyConnect (SVC) のカスタマイズおよびトランスフォーム
 - アイデンティティ証明書 (アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される)
 - VPN 事前共有キー
 - SSL VPN コンフィギュレーション
 - アプリケーション プロファイルのカスタム フレームワーク (APCF)
 - ブックマーク
 - カスタマイゼーション
 - ダイナミック アクセス ポリシー (DAP)
 - プラグイン
 - 接続プロファイル用の事前入力スクリプト
 - プロキシ自動設定
 - 変換テーブル
 - Web コンテンツ
 - バージョン情報

システムのバックアップ

この手順では、完全なシステム バックアップを実行する方法について説明します。

手順

- ステップ 1 コンピュータ上にフォルダを作成し、バックアップファイルを保存します。こうすると、後で復元するときに探しやすくなります。
- ステップ 2 **[Tools] > [Backup Configurations]** を選択します。

[Backup Configurations] ダイアログボックスが表示されます。[SSL VPN Configuration] 領域の下矢印をクリックし、SSL VPN コンフィギュレーションのバックアップ オプションを確認します。デフォルトでは、すべてのコンフィギュレーションファイルがチェックされ、利用できる場合にはバックアップされます。リスト内のすべてのファイルをバックアップするには、手順 5 に進みます。
- ステップ 3 バックアップするコンフィギュレーションを選択する場合は、[Backup All] チェックボックスをオフにします。
- ステップ 4 バックアップするオプションの横にあるチェックボックスをオンにします。
- ステップ 5 **[Browse Local to specify a directory and file name for the backup .zip file]** をクリックします。
- ステップ 6 **[Select]** ダイアログボックスで、バックアップファイルを格納するディレクトリを選択します。
- ステップ 7 **[Select]** をクリックします。[Backup File] フィールドにパスが表示されます。
- ステップ 8 ディレクトリパスの後にバックアップファイルの宛先の名前を入力します。バックアップファイルの名前の長さは、3 ～ 232 文字の間である必要があります。
- ステップ 9 **[Backup]** をクリックします。証明書をバックアップする場合や、ASA でマスター パスフレーズを使用している場合を除き、すぐにバックアップが続行されます。
- ステップ 10 ASA でマスター パスフレーズを設定し、イネーブルにしている場合、バックアップを続行する前に、マスター パスフレーズが不明な場合は変更することを推奨する警告メッセージが表示されます。マスター パスフレーズがわかっている場合は、**[Yes]** をクリックしてバックアップを続行します。ID 証明書をバックアップする場合を除き、すぐにバックアップが続行されます。
- ステップ 11 ID 証明書をバックアップする場合は、証明書を PKCS12 形式でエンコーディングするために使用する別のパスフレーズを入力するように求められます。パスフレーズを入力するか、またはこの手順をスキップすることができます。

(注) ID 証明書だけがこのプロセスによってバックアップされます。ただし、認証局の証明書はバックアップされません。CA 証明書のバックアップ手順については、[ローカル CA サーバのバックアップ \(945 ページ\)](#) を参照してください。

- 証明書を暗号化するには、[Certificate Passphrase] ダイアログボックスで証明書のパスフレーズを入力および確認し、[OK] をクリックします。証明書の復元時に必要となるため、このダイアログボックスに入力したパスワードを覚えておく必要があります。
- [Cancel] をクリックすると、この手順がスキップされ、証明書はバックアップされません。

[OK] または [Cancel] をクリックすると、すぐにバックアップが開始されます。

ステップ 12 バックアップが完了すると、ステータス ウィンドウが閉じ、[Backup Statistics] ダイアログボックスが表示され、成功または失敗のメッセージが表示されます。

(注) バックアップの「失敗」メッセージは多くの場合、指定されたタイプの既存のコンフィギュレーションが存在しない場合に表示されます。

ステップ 13 [OK] をクリックし、[Backup Statistics] ダイアログボックスを閉じます。

バックアップの復元

zip tar.gz ファイルからローカル PC に復元するコンフィギュレーションやイメージを指定します。

手順

ステップ 1 [Tools] > [Restore Configurations] を選択します。

ステップ 2 [Restore Configurations] ダイアログボックスで、[Browse Local Directory] をクリックし、ローカル コンピュータ上の、復元するコンフィギュレーションが含まれている zip ファイルを選択し、[Select] をクリックします。[Local File] フィールドにパスと zip ファイル名が表示されます。

復元する zip ファイルは、[Tools] > [Backup Configurations] オプションを選択して作成したものである必要があります。

ステップ 3 [Next] をクリックします。2つ目の [Restore Configuration] ダイアログボックスが表示されます。復元するコンフィギュレーションの横にあるチェックボックスをオンにします。使用可能なすべての SSL VPN コンフィギュレーションがデフォルトで選択されています。

ステップ 4 [Restore] をクリックします。

ステップ 5 バックアップファイルの作成時に、証明書の暗号化に使用する証明書パスフレーズを指定している場合は、このパスフレーズを入力するように ASDM から求められます。

ステップ 6 実行コンフィギュレーションの復元を選択した場合、実行コンフィギュレーションを結合するか、実行コンフィギュレーションを置換するか、または復元プロセスのこの部分をスキップするかを尋ねられます。

- コンフィギュレーションの結合では、現在の実行コンフィギュレーションとバックアップされた実行コンフィギュレーションが結合されます。
- 実行コンフィギュレーションの置換では、バックアップされた実行コンフィギュレーションのみが使用されます。
- この手順をスキップすると、バックアップされた実行コンフィギュレーションは復元されません。

ASDM では、復元操作が完了するまでステータス ダイアログボックスが表示されます。

- ステップ7** 実行コンフィギュレーションを置換または結合した場合は、ASDM を閉じてから再起動します。実行コンフィギュレーションを復元しなかった場合は、ASDMセッションをリフレッシュして、変更を有効にします。

ローカル CA サーバのバックアップ

ASDM バックアップを実行した場合、ローカル CA サーバデータベースは含まれていないため、サーバ上の CA 証明書はバックアップされません。ローカル CA サーバをバックアップする場合は、ASA CLI による次の手動プロセスを使用します。

手順

- ステップ1** `show run crypto ca server` コマンドを入力します。

```
crypto ca server
  keysize server 2048
  subject-name-default OU=aa,O=Cisco,ST=ca,
  issuer-name CN=xxx,OU=yyy,O=Cisco,L=Bxb,St=Mass
  smtp from-address abcd@cisco.com
  publish-crl inside 80
  publish-crl outside 80
```

- ステップ2** `crypto ca import` コマンドを使用して、ローカル CA PKCS12 ファイルをインポートして LOCAL-CA-SERVER トラストポイントを作成し、キーペアを復元します。

```
crypto ca import LOCAL-CA-SERVER pkcs12 <passphrase> (paste the pkcs12
base64 data here)
```

(注) この手順では、正確な名前「LOCAL-CA-SERVER」を必ず使用してください。

- ステップ3** LOCAL-CA-SERVER ディレクトリが存在しない場合、`mkdir LOCAL-CA-SERVER` を入力して作成する必要があります。

- ステップ4** ローカル CA ファイルを LOCAL-CA-SERVER ディレクトリにコピーします。

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.ser
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.cdb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.udb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.crl
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.p12
```

```
disk0:/LOCAL-CA-SERVER/
```

ステップ 5 `crypto ca server` コマンドを入力して、ローカル CA サーバをイネーブルにします。

```
crypto ca server  
no shutdown
```

ステップ 6 `show crypto ca server` コマンドを入力して、ローカル CA サーバが起動し、動作していることを確認します。

ステップ 7 設定を保存します。

TFTP サーバへの実行コンフィギュレーションの保存

この機能により、現在の実行コンフィギュレーションファイルのコピーを TFTP サーバに保存します。

手順

ステップ 1 [File] > [Save Running Configuration to TFTP Server] を選択します。

[Save Running Configuration to TFTP Server] ダイアログボックスが表示されます。

ステップ 2 TFTP サーバの IP アドレスと、コンフィギュレーションファイルの保存先となる TFTP サーバ上のファイルパスを入力して、[Save Configuration] をクリックします。

(注) デフォルトの TFTP 設定を行うには、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択します。この設定を行った後は、このダイアログボックスに、TFTP サーバの IP アドレスと TFTP サーバ上でのファイルパスが自動的に表示されます。

システム再起動のスケジュール

System Reload ツールにより、システムの再起動をスケジュールしたり、現在の再起動をキャンセルしたりできます。

手順

ステップ 1 [Tools] > [System Reload] を選択します。

ステップ 2 [Reload Scheduling] 領域で、次の設定を定義します。

- a) [Configuration State] では、再起動時に実行コンフィギュレーションを保存するか、破棄するかのどちらかを選択します。
- b) [Reload Start Time] では、次のオプションから選択します。
 - 再起動をただちに実行するには、[Now] をクリックします。
 - 指定した時間だけ再起動を遅らせるには、[Delay by] をクリックします。再起動開始までの時間を、時間と分単位、または分単位だけで入力します。
 - 指定した時刻と日付に再起動を実行するようにスケジュールするには、[Schedule at] をクリックします。再起動の実行時刻を入力し、再起動のスケジュール日を選択します。
- c) [Reload Message] フィールドに、再起動時に開いている ASDM インスタンスに送信するメッセージを入力します。
- d) 再起動を再試行するまでの経過時間を時間と分単位で、または分単位だけで表示するには、[On reload failure force immediate reload after] チェックボックスをオンにします。
- e) 設定に従って再起動をスケジュールするには、[Schedule Reload] をクリックします。
[Reload Status] 領域には、再起動のステータスが表示されます。

ステップ 3 次のいずれかを選択します。

- スケジュールされた再起動を停止するには、[Cancel Reload] をクリックします。
- スケジュールされた再起動の終了後に [Reload Status] 表示をリフレッシュするには、[Refresh] をクリックします。
- スケジュールされた再起動の詳細を表示するには、[Details] をクリックします。

Auto Update の設定

Auto Update は、Auto Update サーバがコンフィギュレーションおよびソフトウェアイメージを多数の ASA にダウンロードすることを許可し、中央からの ASA の基本的なモニタリングを提供するプロトコル仕様です。

Auto Update について

この項では、Auto Update の実装方法と Auto Update が必要になる理由について説明します。

Auto Update クライアントまたはサーバ

ASA は、クライアントまたはサーバとして設定できます。Auto Update クライアントとして動作する場合は、ソフトウェアイメージおよびコンフィギュレーションファイルへのアップデー

トのため、Auto Update サーバを定期的にポーリングします。Auto Update サーバとして動作する場合は、Auto Update クライアントとして設定された ASA のアップデートを発行します。

Auto Update の利点

Auto Update は、次のように、管理者が ASA の管理で直面するさまざまな問題を解決できる便利な機能です。

- ダイナミック アドレッシングおよび NAT に関する問題点の解決。
- コンフィギュレーションの変更を 1 つのアクションでコミット。
- ソフトウェア更新用の信頼度の高い方式の提供。
- ハイ アベイラビリティ用の十分実績のある方式の活用（フェールオーバー）。
- オープン インターフェイスによる柔軟性の提供。
- サービス プロバイダー環境のセキュリティ ソリューションの簡素化。

Auto Update 仕様は、中央、または複数の場所から、リモート管理アプリケーションにより ASA のコンフィギュレーションやソフトウェアイメージをダウンロードしたり、基本的な監視機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update 仕様に従うと、Auto Update サーバから ASA にコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりすることも、ASA から Auto Update サーバに定期的にポーリングすることによって、最新のコンフィギュレーション情報を引き出す（プルする）こともできます。また、Auto Update サーバはいつでも ASA にコマンドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバと ASA の通信では、通信パスとローカル CLI コンフィギュレーションをすべての ASA に設定する必要があります。

フェールオーバー設定での Auto Update サーバサポート

Auto Update サーバを使用して、ソフトウェア イメージとコンフィギュレーション ファイルを、アクティブ/スタンバイ フェールオーバー コンフィギュレーションの ASA に配置できます。アクティブ/スタンバイフェールオーバーコンフィギュレーションで Auto Update をイネーブルにするには、フェールオーバー ペアのプライマリ装置に Auto Update サーバのコンフィギュレーションを入力します。

フェールオーバー コンフィギュレーションの Auto Update サーバサポートには、次の制限と動作が適用されます。

- アクティブ/スタンバイ コンフィギュレーションがサポートされるのは、シングルモードだけです。
- 新しいプラットフォーム ソフトウェア イメージをロードする際、フェールオーバー ペアはトラフィックの転送を停止します。
- LAN ベースのフェールオーバーを使用する場合、新しいコンフィギュレーションによってフェールオーバー リンクのコンフィギュレーションが変更されてはいけません。フェー

ルオーバー リンクのコンフィギュレーションが変更されると、装置間の通信は失敗します。

- Auto Update サーバへの Call Home を実行するのはプライマリ装置だけです。Call Home を実行するには、プライマリ装置がアクティブ状態である必要があります。そうでない場合、ASA は自動的にプライマリ装置にフェールオーバーします。
- ソフトウェアイメージまたはコンフィギュレーションファイルをダウンロードするのは、プライマリ装置だけです。その後、ソフトウェアイメージまたはコンフィギュレーションファイルはセカンダリ装置にコピーされます。
- インターフェイス MAC アドレスとハードウェアのシリアル番号は、プライマリ装置のものであります。
- Auto Update サーバまたは HTTP サーバに保存されたコンフィギュレーションファイルは、プライマリ装置専用です。

Auto Update プロセスの概要

次に、フェールオーバー コンフィギュレーションでの Auto Update プロセスの概要を示します。このプロセスは、フェールオーバーがイネーブルであり、動作していることを前提としています。装置がコンフィギュレーションを同期化している場合、SSM カードの不具合以外の理由でスタンバイ装置に障害が発生している場合、または、フェールオーバー リンクがダウンしている場合、Auto Update プロセスは実行できません。

1. 両方の装置は、プラットフォームおよび ASDM ソフトウェア チェックサムとバージョン情報を交換します。
2. プライマリ装置は Auto Update サーバにアクセスします。プライマリ装置がアクティブ状態でない場合、ASA はプライマリ装置にフェールオーバーした後、Auto Update サーバにアクセスします。
3. Auto Update サーバは、ソフトウェア チェックサムと URL 情報を返します。
4. プライマリ装置が、アクティブまたはスタンバイ装置のプラットフォーム イメージ ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
 1. プライマリ装置は、Auto Update サーバの URL を使用して、HTTP サーバから適切なファイルを取得します。
 2. プライマリ装置は、そのイメージをスタンバイ装置にコピーしてから、自身のイメージをアップデートします。
 3. 両方の装置に新しいイメージがある場合は、セカンダリ（スタンバイ）装置が最初にリロードされます。
 - セカンダリ装置のブート時にヒットレスアップグレードが可能な場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。リロードが終了すると、プライマリ装置がアクティブ装置になります。

- スタンバイ装置のブート時にヒットレスアップグレードができない場合は、両方の装置が同時にリロードされます。
4. セカンダリ（スタンバイ）装置だけに新しいイメージがある場合は、セカンダリ装置だけがリロードされます。プライマリ装置は、セカンダリ装置のリロードが終了するまで待機します。
 5. プライマリ（アクティブ）装置だけに新しいイメージがある場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。
 6. もう一度アップデート プロセスが手順 1 から開始されます。
5. ASA が、プライマリまたはセカンダリ装置の ASDM ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
 1. プライマリ装置は、Auto Update サーバから提供された URL を使用して、HTTP サーバから ASDM イメージ ファイルを取得します。
 2. プライマリ装置は、必要に応じてそのイメージをスタンバイ装置にコピーします。
 3. プライマリ装置は、自身の ASDM イメージをアップデートします。
 4. もう一度アップデート プロセスが手順 1 から開始されます。
 6. プライマリ装置が、コンフィギュレーション ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
 1. プライマリ装置は、指定された URL を使用して、からコンフィギュレーション ファイルを取得します。
 2. 両方の装置で同時に、古いコンフィギュレーションが新しいコンフィギュレーションに置換されます。
 3. もう一度アップデート プロセスが手順 1 から開始されます。
 7. チェックサムがすべてのイメージおよびコンフィギュレーション ファイルと一致している場合、アップデートは必要ありません。このプロセスは、次のポーリング時間まで中断されます。

Auto Update のガイドライン

コンテキスト モード

Auto Update は、シングル コンテキスト モードでのみサポートされます。

クラスタ

クラスタリングはサポートされません。

モデル

次のモデルではサポートされません。

- ASA 5506-X、5508-X、5516-X
- Firepower 4100、および 9300
- ASAv

その他のガイドライン

- Auto Update サーバから ASA のコンフィギュレーションが更新されても、ASDM には通知されません。[Refresh] または [File] > [RefreshASDM with the Running Configuration on the Device] を選択して、最新のコンフィギュレーションを取得する必要があります。また、ASDM でコンフィギュレーションに加えた変更は失われます。
- Auto Update サーバと通信するためのプロトコルとして HTTPS が選択されている場合は、ASA は SSL を使用します。これは、ASA による DES または 3DES ライセンスの保有が必須です。

Auto Update サーバとの通信の設定

手順

ステップ 1 [Configuration] > [Device Management] > [System Image/Configuration] > [Auto Update] を選択します。

[Auto Update] ペインには、[Auto Update Servers] テーブルの他に [Timeout] 領域と [Polling] 領域があります。

[Auto Update Servers] テーブルで、Auto Update サーバにすでに設定されているパラメータを確認できます。ASA は、テーブルの一番上にあるサーバを最初にポーリングします。

ステップ 2 テーブル内のサーバの順序を変更するには、[Move Up] または [Move Down] をクリックします。

[Auto Update Servers] テーブルには次のカラムがあります。

- [Server] : Auto Update サーバの名前または IP アドレス。
- [User Name] : Auto Update サーバのアクセス時に使用されるユーザ名。
- [Interface] : Auto Update サーバへの要求送信時に使用されるインターフェイス。
- [Verify Certificate] : Auto Update サーバが返した証明書を、ASA で CA のルート証明書と照合して確認するかどうかを指定します。Auto Update サーバおよび ASA は同じ CA を使用する必要があります。

ステップ 3 [Auto Update Server] テーブルの行のいずれかをダブルクリックすると、[Edit Auto Update Server] ダイアログボックスが開き、Auto Update サーバのパラメータを変更できます。ここで行った変更はただちにテーブルに反映されますが、コンフィギュレーションに保存するには [Apply] をクリックする必要があります。

ステップ 4 [Timeout] エリアでは、ASA が Auto Update サーバのタイムアウトを待つ時間を設定できます。[Timeout] 領域には次のフィールドがあります。

- [Enable Timeout Period] : ASA が Auto Update サーバから応答を受信しなかった場合にタイムアウトするには、オンにします。
- [Timeout Period (Minutes)] : Auto Update サーバから応答がなかった場合の ASA のタイムアウト時間（分単位）を指定します。

ステップ 5 [Polling] エリアで、ASA から Auto Update サーバの情報をポーリングする頻度を設定できます。[Polling] 領域には次のフィールドがあります。

- [Polling Period (minutes)] : ASA から Auto Update サーバに新しい情報をポーリングするときの待ち時間（分単位）。
- [Poll on Specified Days] : ポーリングのスケジュールを指定します。
- [Set Polling Schedule] : [Set Polling Schedule] ダイアログボックスが表示され、Auto Update サーバをポーリングする日付と時刻を設定できます。
- [Retry Period (minutes)] : サーバのポーリングに失敗した場合、ASA から Auto Update サーバに新しい情報をポーリングするまでの待ち時間（分単位）。
- [Retry Count] : ASA から Auto Update サーバに新しい情報をポーリングするときの再試行回数。

ステップ 6 ポーリング スケジュールの設定

[Set Polling Schedule] ダイアログボックスでは、ASA から Auto Update サーバをポーリングする特定の日付と時刻を設定できます。

[Set Polling Schedule] ダイアログボックスには次のフィールドがあります。

[Days of the Week] : ASA から Auto Update サーバをポーリングする曜日のチェックボックスを選択します。

[Daily Update] ペイングループでは、ASA が Auto Update サーバをポーリングする時刻を設定できます。次のフィールドがあります。

- [Start Time] : Auto Update のポーリング開始時刻を入力します。
- [Enable randomization] : ASA から Auto Update サーバをランダムに選択した時刻にポーリングするには、オンにします。

Auto Update のモニタリング

Auto Update プロセスのモニタリング

debug auto-update client または **debug fover cmd-exe** コマンドを使用して、Auto Update プロセスで実行される処理を表示できます。次に、**debug auto-update client** コマンドの出力例を示します。**debug**ターミナルセッションからコマンドを実行します。

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
  Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
  Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
  Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msec
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
```

```

auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
  Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419

```

Auto Update プロセスが失敗すると、次の syslog メッセージが生成されます。

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

file は、失敗したアップデートに応じて “image”、“asdm”、または “configuration” になります。
version は、アップデートのバージョン番号です。*reason* は、アップデートが失敗した原因です。

ソフトウェアとコンフィギュレーションの履歴

機能名	プラットフォームリリース	機能情報
セキュア コピー クライアント	9.1(5)/9.2(1)	<p>SCP サーバとの間でファイルを転送するため、ASA は Secure Copy (SCP) クライアントをサポートするようになりました。</p> <p>次の画面が変更されました。</p> <p>[Tools] > [File Management] > [File Transfer] > [Between Remote Server and Flash] [Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server]</p>
設定可能な SSH 暗号機能と整合性アルゴリズム	9.1(7)/9.4(3)	<p>ユーザは SSH 暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム (3des-cbc) が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、ssh cipher encryption custom aes128-cbc を使用します。</p> <p>次の画面が導入されました。 [Configuration] > [Device Management] > [Advanced] > [SSH Ciphers]</p>

機能名	プラットフォームリリース	機能情報
デフォルトでイネーブルになっている Auto Update サーバ証明書の検証	9.2(1)	<p>Auto Update サーバ証明書の検証がデフォルトでイネーブルになりました。新しいコンフィギュレーションでは証明書の検証を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとする、証明書の確認はイネーブルではなく、次の警告が表示されます。</p> <pre>WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.</pre> <p>設定を移行する場合は、次のように確認なしを明示的に設定します。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [System/Image Configuration] > [Auto Update] > [Add Auto Update Server]。</p>
CLIを使用したシステムのバックアップと復元	9.3(2)	<p>CLIを使用してイメージや証明書を含む完全なシステムコンフィギュレーションをバックアップおよび復元できるようになりました。</p> <p>変更された ASDM 画面はありません。</p>
新しい ASA 5506W-X イメージの回復およびロード	9.4(1)	<p>新しい ASA 5506W-X イメージのリカバリおよびロードがサポートされています。</p> <p>変更された ASDM 画面はありません。</p>



第 38 章

システム イベントに対する応答の自動化

この章では、Embedded Event Manager (EEM) を設定する方法について説明します。

- [EEM について \(957 ページ\)](#)
- [EEM のガイドライン \(959 ページ\)](#)
- [EEM の設定 \(959 ページ\)](#)
- [EEM のモニタリング \(963 ページ\)](#)
- [EEM の履歴 \(963 ページ\)](#)

EEM について

EEM サービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ロギングを提供できます。EEM サービスには2つのコンポーネント、つまり EEM が応答またはリスンするイベント、およびアクションと EEM が応答するイベントを定義するイベントマネージャアプレットがあります。さまざまなイベントにตอบสนองし、さまざまなアクションを実行するために、複数のイベントマネージャアプレットを設定できます。

サポートされるイベント

EEM は次のイベントをサポートします。

- **Syslog** : ASA は、syslog メッセージの ID を使用して、イベントマネージャアプレットをトリガーする syslog メッセージを識別します。複数の syslog イベントを設定できますが、単一のイベントマネージャアプレット内で syslog メッセージの ID が重複することはできません。
- **タイマー** : タイマーを使用して、イベントをトリガーできます。各タイマーは、各イベントマネージャアプレットに対して一度だけ設定できます。各イベントマネージャアプレットには最大で3つのタイマーがあります。3種類のタイマーは次のとおりです。
 - **ウォッチドッグ (定期的) タイマー** は、アプレットアクションの完了後に指定された期間が経過するとイベントマネージャアプレットをトリガーし、自動的にリスタートします。

- カウントダウン（ワンショット）タイマーは、指定された期間が経過するとイベント マネージャ アプレットを1回トリガーします。削除および再追加されない限りはリスタートしません。
- 絶対（1日1回）タイマーは、イベントを1日1回指定された時刻に発生させ、自動的にリスタートします。時刻の形式は `hh:mm:ss` です。
各イベント マネージャ アプレットに対して、各タイプのタイマー イベントを1つだけ設定できます。
- なし：CLI または ASDM を使用してイベント マネージャ アプレットを手動で実行する場合、イベントはトリガーされません。
- クラッシュ：ASA がクラッシュした場合、クラッシュ イベントがトリガーされます。
output コマンドの値に関係なく、**action** コマンドはクラッシュ情報ファイルを対象とします。出力は **show tech** コマンドの前に生成されます。

イベント マネージャ アプレットのアクション

イベント マネージャ アプレットがトリガーされると、そのイベント マネージャ アプレットのアクションが実行されます。各アクションには、アクションの順序を指定するために使用される番号があります。このシーケンス番号は、イベント マネージャ アプレット内で一意である必要があります。イベント マネージャ アプレットには複数のアクションを設定できます。コマンドは典型的な CLI コマンドです（**show blocks** など）。

出力先

output コマンドを使用すると、アクションの出力を指定した場所に送信できます。一度にイネーブルにできる出力値は1つだけです。デフォルト値は **output none** です。この値は、**action** コマンドによるすべての出力を破棄します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けられない場合があります。次の3つの場所のいずれかに **action** CLI コマンドの出力を送信できます。

- なし：デフォルトの設定です。出力を破棄します。
- コンソール：出力を ASA コンソールに送信します。
- ファイル：出力をファイルに送信します。次の4つのファイル オプションを使用できます。
 - 一意のファイルを作成する：イベント マネージャ アプレットが呼び出されるたびに、一意の名前を持つ新しいファイルを作成します。
 - ファイルを作成する/ファイルを上書きする：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルを上書きします。

- **ファイルを作成する/ファイルに付加する**：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルに付加します。ファイルがまだ存在しない場合は作成されます。
- **一連のファイルを作成する**：イベント マネージャ アプレットが呼び出されるたびにローテーションされる、一意の名前を持つ一連のファイルを作成します。

EEM のガイドライン

ここでは、EEM を設定する前に確認する必要があるガイドラインおよび制限事項について説明します。

コンテキスト モードのガイドライン

マルチ コンテキスト モードではサポートされません。

その他のガイドライン

- 通常、クラッシュ時は、ASA の状態は不明です。こうした状況では、一部のコマンドの実行は安全ではない可能性があります。
- イベント マネージャ アプレットの名前にはスペースを含めることができません。
- None イベントおよび Crashinfo イベント パラメータは変更できません。
- syslog メッセージが EEM に送信されて処理されるため、パフォーマンスが影響を受ける可能性があります。
- 各イベント マネージャ アプレットのデフォルトの出力は **output none** です。この設定を変更するには、異なる出力値を入力する必要があります。
- 各イベント マネージャ アプレットに定義できる出力オプションは 1 つだけです。

EEM の設定

EEM の設定は、次のタスクで構成されています。

手順

- ステップ 1** [イベント マネージャ アプレットの作成とイベントの設定 \(960 ページ\)](#)。
- ステップ 2** [アクションおよびアクションの出力先の設定 \(961 ページ\)](#) を使用して無効にすることができます。
- ステップ 3** [イベント マネージャ アプレットの実行 \(962 ページ\)](#) を使用して無効にすることができます。

- ステップ4 **トラックメモリ割り当ておよびメモリ使用量 (962ページ)** を使用して無効にすることができません。

イベントマネージャアプレットの作成とイベントの設定

イベントマネージャアプレットを作成してイベントを設定するには、次の手順を実行します。

手順

- ステップ1 ASDM で、**[Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager]** の順に選択します。
- ステップ2 **[Add]** をクリックして、**[Add Event Manager Applet]** ダイアログボックスを表示します。
- ステップ3 アプレット名 (スペースを含まない) を入力し、そのアプレットに関する説明を入力します。説明の長さは最大256文字です。引用符内であれば、説明テキストにスペースを含めることができます。
- ステップ4 **[Events]** 領域にある **[Add]** をクリックして、**[Add Event Manager Applet Event]** ダイアログボックスを表示します。
- ステップ5 **[Type]** ドロップダウンリストから設定したいイベントタイプを選択します。使用可能なオプションは、**[Crashinfo]**、**[None]**、**[Syslog]**、**[Once-a-day timer]**、**[One-shot timer]**、および **[Periodic timer]** です。
- **[Syslog]** : 単一の syslog メッセージまたは syslog メッセージの範囲を入力します。指定された個々の syslog メッセージまたは syslog メッセージの範囲に一致する syslog メッセージが発生すると、イベントマネージャアプレットがトリガーされます。(オプション) イベントマネージャアプレットを呼び出すために syslog メッセージが発生する必要がある回数を **[Occurrences]** フィールドに入力します。デフォルトの発生回数は0秒ごとに1回です。有効な値は、1 ~ 4294967295 です。(オプション) アクションを呼び出すために syslog メッセージが発生しなければならない許容時間(秒数)を **[Period]** フィールドに入力します。この値によって、イベントマネージャアプレットが設定された期間に1回呼び出される際の最大の間隔が制限されます。有効な値は、0 ~ 604800 です。値0は、期間が定義されていないことを示しています。
 - **[Periodic]** : 期間を秒単位で入力します。秒数は、1 ~ 604800 の範囲で設定してください。
 - **[Once-a-day timer]** : 時刻を hh:mm:ss の形式で入力します。時刻の範囲は 00:00:00 (真夜中) から 23:59:59 です。
 - **[One-shot timer]** : 期間を秒単位で入力します。秒数は、1 ~ 604800 の範囲で設定してください。
 - **[None]** : イベントマネージャアプレットを手動で呼び出すには、このオプションを選択します。

- [Crashinfo] : ASA のクラッシュ時にクラッシュ イベントをトリガーするには、このオプションを選択します。

アクションおよびアクションの出力先の設定

アクションおよびアクションの出力を送信する特定の宛先を設定するには、次の手順を実行します。

手順

- ステップ 1** [Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを表示します。
- ステップ 2** アプレット名（スペースを含まない）を入力し、そのアプレットに関する説明を入力します。説明の長さは最大 256 文字です。
- ステップ 3** [Actions] 領域にある [Add] をクリックして、[Add Event Manager Applet Action] ダイアログボックスを表示します。
- ステップ 4** [Sequence #] フィールドに一意のシーケンス番号を入力します。有効なシーケンス番号の範囲は 0 ~ 4294967295 です。
- ステップ 5** CLI コマンドを [CLI Command] フィールドに入力します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。
- ステップ 6** [OK] をクリックして、[Add Event Manager Applet Action] ダイアログボックスを閉じます。新しく追加されたアクションが [Actions] リストに表示されます。
- ステップ 7** [Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを開きます。
- ステップ 8** 使用可能な出力先オプションを 1 つ選択します。
 - **action** コマンドからの出力を破棄するには、[Output Location] ドロップダウン リストから [None] オプションを選択します。これがデフォルト設定です。
 - **action** コマンドの出力をコンソールに送信するには、[Output Location] ドロップダウン リストから [Console] オプションを選択します。

(注) このコマンドを実行すると、パフォーマンスに影響を及ぼします。
 - **action** コマンドの出力を呼び出された各イベント マネージャ アプレットの新しいファイルに送信するには、[Output Location] ドロップダウン リストから [File] オプションを選択します。[Create a unique file] オプションがデフォルトとして自動的に選択されます。ファイル名の形式は、`eem-applet-timestamp.log` です。ここで、*applet* はイベント マネージャ アプレットの名前、*timestamp* は日付のタイム スタンプ（形式は YYYYMMDD-hhmmss）を示しています。

- ローテーションされる一連のファイルを作成するには、[Output Location] ドロップダウンリストから [File] オプションを選択し、続いてドロップダウンリストから [Create a set of files] オプションを選択します。

新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。最も新しいファイルが0で示され、最も古いファイルが最大数で示されます。有効なローテーションの値の範囲は2～100です。ファイル名の形式は、`cem-applet-x.log` です。ここで、*applet* はアプレットの名前、*x* はファイル番号を示しています。

- **action** コマンドの出力を毎回上書きされる単一のファイルに書き込むには、[Output Location] ドロップダウンリストから [File] オプションを選択し、続いてドロップダウンリストから [Create/overwrite a file] オプションを選択します。
- **action** コマンドの出力を毎回上書きされる単一のファイルに書き込むには、[Output Location] ドロップダウンリストから [File] オプションを選択し、続いてドロップダウンリストから [Create/append a file] オプションを選択します。

ステップ9 [OK] をクリックして、[Add Event Manager Applet] ダイアログボックスを閉じます。

指定した出力先は [Embedded Event Manager] ペインに表示されます。

イベント マネージャ アプレットの実行

イベント マネージャ アプレットを実行するには、次の手順を実行します。

手順

ステップ1 [Embedded Event Manager] ペインで、**None** イベントで設定されたイベント マネージャ アプレットをリストから選択します。

ステップ2 [Run] をクリックします。

トラック メモリ割り当ておよびメモリ使用量

メモリ割り当てとメモリ使用量をログに記録するには、次の手順を実行します。

手順

ステップ1 [Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager] の順に選択します。

ステップ2 [Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを表示します。

- ステップ3 もう一度 [Add] をクリックして、[Add Event Manager Applet Event] ダイアログボックスを表示します。
- ステップ4 ドロップダウンリストから [memory-logging-wrap] を選択します。
- ステップ5 [OK] をクリックして、それを [Events] リストに追加します。
- ステップ6 もう一度 [OK] をクリックして、それを [Applets] リストに追加します。

EEM のモニタリング

EEM をモニタするには、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [EEM Applets]**

このペインでは、EEM アプレットとそのヒット カウント値のリストを表示します。

- **[Tools] > [Command Line Interface]**

このペインでは、さまざまな非インタラクティブコマンドを発行し、結果を表示することができます。

EEM の履歴

表 46: EEM の履歴

機能名	プラットフォーム リリース	説明
Embedded Event Manager (EEM)	9.2(1)	<p>EEM サービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ログギングを提供できます。EEM サービスには2つのコンポーネント、つまり EEM が応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。</p> <p>次の画面が導入されました。 [Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager]、[Monitoring] > [Properties] > [EEM Applets]。</p>

機能名	プラットフォーム リリース	説明
EEM のメモリ トラッキング	9.4(1)	<p>メモリ割り当てとメモリ使用量をログに記録し、メモリ ロギング ラップ イベントに応答する新しいデバッグ機能が追加されました。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager] > [Add Event Manager Applet] > [Add Event Manager Applet Event]</p>



第 39 章

テストとトラブルシューティング

この章では、Cisco ASA のトラブルシューティング方法および基本接続のテスト方法について説明します。

- [イネーブルパスワードと Telnet パスワードの回復 \(965 ページ\)](#)
- [Packet Capture Wizard を使用したキャプチャの設定と実行 \(971 ページ\)](#)
- [ASAv の vCPU 使用量 \(977 ページ\)](#)
- [設定のテスト \(979 ページ\)](#)
- [パフォーマンスとシステムリソースのモニタリング \(988 ページ\)](#)
- [接続のモニタリング \(991 ページ\)](#)

イネーブルパスワードと Telnet パスワードの回復

イネーブルパスワードまたは Telnet パスワードを忘れた場合は、それらを回復できます。手順は、デバイスタイプによって異なります。CLI を使用してタスクを実行する必要があります。

ASA のパスワードの回復

ASA のパスワードを回復するには、次の手順を実行します。

手順

- ステップ 1** ASA のコンソールポートに接続します。
- ステップ 2** ASA の電源を切ってから、再び電源をオンにします。
- ステップ 3** スタートアップ後、ROMMON モードに入るようにプロンプトが表示されたら、**Escape** キーを押します。
- ステップ 4** コンフィギュレーションレジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

- ステップ 5** スタートアップ コンフィギュレーションを無視するように ASA を設定するには、次のコマンドを入力します。

```
rommon #1> confreg
```

ASAによって現在のコンフィギュレーションのレジスタ値が表示され、それを変更するかどうか尋ねられます。

```
Current Configuration Register: 0x00000041
Configuration Summary:
  boot default image from Flash
  ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```

- ステップ 6** 後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

- ステップ 7** 値を変更する場合は、プロンプトに対して **Y** を入力します。

ASAによって、新しい値の入力を求めるプロンプトが表示されます。

- ステップ 8** 「disable system configuration?」の値を除き、すべての設定についてデフォルト値を受け入れません。

- ステップ 9** プロンプトに対して、**Y** を入力します。

- ステップ 10** 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASAは、スタートアップコンフィギュレーションの代わりにデフォルトコンフィギュレーションをロードします。

- ステップ 11** 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

- ステップ 12** パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

- ステップ 13** 次のコマンドを入力して、スタートアップコンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

- ステップ 14** 次のコマンドを入力して、グローバルコンフィギュレーションモードにアクセスします。

```
ciscoasa# configure terminal
```

- ステップ 15** 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password  
ciscoasa(config)# enable password password  
ciscoasa(config)# username name password password
```

- ステップ 16** 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、[コマンド リファレンス](#)を参照してください。

- ステップ 17** 次のコマンドを入力して、新しいパスワードをスタートアップコンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASA 5506-X、ASA 5508-X、ASA 5516-X でのパスワードの回復

ASA 5506-X、ASA 5508-X、ASA 5516-X のパスワードの回復には、次の手順を実行します。

手順

- ステップ 1** ASA のコンソール ポートに接続します。
- ステップ 2** ASA の電源を切ってから、再び電源をオンにします。
- ステップ 3** スタートアップ後、ROMMON モードに入るようにプロンプトが表示されたら、**Escape** キーを押します。
- ステップ 4** コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41
```

```
You must reset or power cycle for new config to take effect
```

ASA で現在のコンフィギュレーションレジスタ値と構成オプションのリストが表示されます。後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

```
Configuration Register: 0x00000041
```

```
Configuration Summary
[ 0 ] password recovery
[ 1 ] display break prompt
[ 2 ] ignore system configuration
[ 3 ] auto-boot image in disks
[ 4 ] console baud: 9600
boot: ..... auto-boot index 1 image in disks
```

ステップ 5 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASA は、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 6 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 7 パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 8 次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 9 次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 10 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 11 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、[コマンド リファレンス](#)を参照してください。

- ステップ 12** 次のコマンドを入力して、新しいパスワードをスタートアップコンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASA vでのパスワードまたはイメージの回復

ASA vのパスワードまたはイメージを回復するには、次の手順を実行します。

手順

- ステップ 1** 実行コンフィギュレーションを ASA vのバックアップ ファイルにコピーします。

copy running-config filename

例 :

```
ciscoasa# copy running-config backup.cfg
```

- ステップ 2** ASA vを再始動します。

reload

- ステップ 3** [GNU GRUB]メニューから、下矢印を押し、コンフィギュレーションをロードしないオプションで <filename> を選択し、Enter キーを押します。ファイル名は、ASA vのデフォルトのブートイメージのファイル名です。デフォルトのブートイメージは、**fallback** コマンドによって自動的にブートされることはありません。その後、選択したブートイメージをロードします。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

例 :

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

- ステップ 4** 実行コンフィギュレーションにバックアップ コンフィギュレーション ファイルをコピーします。

copy filename running-config

例 :

```
ciscoasa (config)# copy backup.cfg running-config
```

ステップ5 パスワードのリセット。

enable password *password*

例：

```
ciscoasa(config)# enable password cisco123
```

ステップ6 新しい設定を保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

パスワード回復のディセーブル化



(注) ASA_v 上でパスワード回復をディセーブルにすることはできません。

権限のないユーザがパスワード回復メカニズムを使用して ASA を危険にさらすことがないように、パスワード回復をディセーブルにするには、次の手順を実行します。

始める前に

ASA で、**no service password-recovery** コマンドを使用すると ROMMON モードに入って、コンフィギュレーションの変更を防ぐことができます。ROMMON モードに入ると、ASA では、すべてのフラッシュ ファイル システムの消去を求めるプロンプトが表示されます。最初に消去を実行しないと、ROMMON モードを開始できません。フラッシュ ファイル システムを消去しない場合、ASA はリロードされます。パスワード回復は ROMMON モードの使用と既存のコンフィギュレーションの保持に依存しているため、この消去によって、パスワードの回復ができなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態に回復するには、新しいイメージとバックアップコンフィギュレーション ファイル（入手できる場合）をロードします。

service password-recovery コマンドは、コンフィギュレーション ファイルに通知用としてのみ表示されます。CLI プロンプトに対してコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。（パスワード回復の準備段階で）スタートアップ時にスタートアップコンフィギュレーションを無視するよう ASA が設定されている場合にパスワード回復をディセーブルにすると、通常どおりスタートアップコンフィギュレーションをロードするように ASA の設定が変更されます。フェールオーバーを使用し、スタートアップコンフィギュレーションを無視するよう

にスタンバイ装置が設定されている場合は、**no service password-recovery** コマンドでスタンバイ装置に複製したときに、コンフィギュレーションレジスタに同じ変更が加えられます。

手順

パスワード回復をディセーブルにします。

no service password-recovery

例：

```
ciscoasa (config)# no service password-recovery
```

Packet Capture Wizard を使用したキャプチャの設定と実行

Packet Capture Wizard を使用して、エラーのトラブルシューティングを行う場合のキャプチャを設定および実行できます。キャプチャでは ACL を使用して、キャプチャされるトラフィックのタイプを、送信元と宛先のアドレスとポート、および1つ以上のインターフェイスで制限できます。このウィザードは、入出力インターフェイスのそれぞれでキャプチャを1回実行します。キャプチャしたパケットは、PC に保存してパケットアナライザで分析できます。



(注) このツールは、クライアントレス SSL VPN キャプチャをサポートしていません。

キャプチャを設定および実行するには、次の手順を実行します。

手順

ステップ 1 [Wizards] > [Packet Capture Wizard] の順に選択します。

[Overview of Packet Capture] 画面には、ウィザードを完了するまでに行うタスクの一覧が表示されます。これらのタスクには、以下が含まれます。

- 入力インターフェイスの選択。
- 出力インターフェイスの選択。
- バッファパラメータの設定。
- キャプチャの実行。
- (オプション) キャプチャデータの PC への保存。

- ステップ 2** [Next] をクリックします。
- クラスタ環境では、[Cluster Option] 画面が表示されます。ステップ 3 に進みます。
- 非クラスタ環境では、[Ingress Traffic Selector] 画面が表示されます。ステップ 4 に進みます。
- ステップ 3** [Cluster Option] 画面で、キャプチャの実行対象として [This device only] または [The whole cluster] のいずれかのオプションを選択します。[Next] をクリックして [Ingress Selector] 画面を表示します。
- ステップ 4** インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。
- ステップ 5** ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。
- ステップ 6** [Packet Match Criteria] 領域で、次のいずれかを実行します。
- パケットの照合に使用する ACL を指定するには、[Specify access-list] オプション ボタンをクリックし、[Select ACL] ドロップダウンリストから ACL を選択します。以前設定した ACL を現在のドロップダウンリストに追加するには、[Manage] をクリックして [ACL Manager] ペインを表示します。ACL を選択して [OK] をクリックします。
 - [Specify Packet Parameters] オプション ボタンをクリックして、パケットパラメータを指定します。
- ステップ 7** 以降の手順については、[入力トラフィック セレクタ \(974 ページ\)](#) を参照してください。
- ステップ 8** [Next] をクリックして、[Egress Traffic Selector] 画面を表示します。
- ステップ 9** インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。
- (注) [Egress Traffic Selector] のフィールドの詳細については[出力トラフィック セレクタ \(975 ページ\)](#) を参照してください。
- [Egress Traffic Selector] のフィールドの詳細については[出力トラフィック セレクタ \(975 ページ\)](#) を参照してください。
- ステップ 10** [Next] をクリックして [Buffers & Captures] 画面を表示します。続行するには、「バッファ」(34-8 ページ) を参照してください。
- ステップ 11** 最新のキャプチャを 10 秒ごとに自動的に取得するように、[Capture Parameters] 領域で [Get capture every 10 seconds] チェックボックスをオンにします。デフォルトでは、このキャプチャは循環バッファを使用します。
- ステップ 12** [Buffer Parameters] 領域で、バッファサイズとパケットサイズを指定します。バッファサイズは、キャプチャがパケットを保存するために使用可能なメモリの最大容量です。パケットサイズは、キャプチャが保持できる最長のパケットです。できる限り多くの情報をキャプチャするため、最長パケットサイズを使用することを推奨します。
- a) パケットサイズを入力します。有効なサイズ範囲は 14 ~ 1522 バイトです。
 - b) バッファサイズを入力します。有効なサイズ範囲は 1534 ~ 33554432 バイトです。

- c) キャプチャされたパケットを保存するには、[Use circular buffer] チェックボックスをオンにします。

(注) この設定を選択すると、すべてのバッファ ストレージが使用されている場合、キャプチャは最も古いパケットへの上書きを始めます。

- ステップ 13** [Next] をクリックして、入力したクラスタ内の全装置のクラスタ オプション (クラスタを使用している場合)、トラフィック セレクタ、バッファ パラメータを表示する [Summary] 画面を表示します。続行するには、「サマリー」(34-8 ページ) を参照してください。
- ステップ 14** [Next] をクリックして [Run Captures] 画面を表示し、次に [Start] をクリックしてパケットのキャプチャを開始します。[Stop] をクリックしてキャプチャを終了します。以降の手順については、[キャプチャの実行 \(976 ページ\)](#) を参照してください。クラスタリングを使用している場合は、ステップ 14 に進みます。
- ステップ 15** 残りのバッファ スペースを確認するには、[Get Capture Buffer] をクリックします。現在のパケットの内容を削除して、バッファに別のパケットをキャプチャするスペースを確保するには、[Clear Buffer on Device] をクリックします。
- ステップ 16** クラスタ環境では、[Run Captures] 画面で、次の手順の 1 つ以上を実行します。
- [Get Cluster Capture Summary] をクリックすると、クラスタ内の全装置のパケット キャプチャ情報のサマリーに続いて、各装置のパケット キャプチャ情報が表示されます。
 - [Get Capture Buffer] をクリックすると、クラスタの各装置にどの程度バッファ スペースが残っているかが表示されます。[Capture Buffer from Device] ダイアログ ボックスが表示されます。
 - [Clear Capture Buffer] をクリックすると、クラスタ内の特定の装置またはすべての装置の現在のコンテンツを削除し、さらにパケットをキャプチャするためのバッファ容量を確保します。
- ステップ 17** [Save captures] をクリックして、[Save Capture] ダイアログボックスを表示します。入力キャプチャ、出力キャプチャ、またはその両方を保存するオプションを選択できます。続行するには、「キャプチャの保存」(34-9 ページ) を参照してください。
- ステップ 18** [Save Ingress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。
- ステップ 19** [Launch Network Sniffer Application] をクリックして、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動し、入力キャプチャを分析します。
- ステップ 20** [Save Egress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。
- ステップ 21** [Launch Network Sniffer Application] をクリックして、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動し、出力キャプチャを分析します。
- ステップ 22** [Close] をクリックし、次に [Finish] をクリックしてウィザードを終了します。

パケットキャプチャのガイドライン

コンテキストモード

- コンテキスト内のクラスタ制御リンクでキャプチャを設定できます。この場合、そのクラスタ制御リンクで送信されるコンテキストに関連付けられているパケットだけがキャプチャされます。
- VLAN ごとに設定できるキャプチャは1つだけです。共有 VLAN の複数のコンテキストでキャプチャを設定した場合は、最後に設定したキャプチャだけが使用されます。
- 最後に設定した（アクティブ）キャプチャを削除した場合は、別のコンテキストで事前に設定したキャプチャがあっても、アクティブになるキャプチャはありません。キャプチャをアクティブにするには、キャプチャを削除して追加し直す必要があります。
- キャプチャを指定したインターフェイスに着信するすべてのトラフィックがキャプチャされます。これには、共有 VLAN 上の他のコンテキストへのトラフィックも含まれます。したがって、ある VLAN のコンテキスト A でのキャプチャをイネーブルにしたときに、その VLAN がコンテキスト B でも使用される場合は、コンテキスト A とコンテキスト B の両方の入力トラフィックがキャプチャされます。
- 出力トラフィックの場合は、アクティブキャプチャのあるコンテキストのトラフィックだけがキャプチャされます。唯一の例外は、ICMP 検査をイネーブルにしない（したがって、ICMP トラフィックのセッションが高速パスにない）場合です。この場合は、共有 VLAN のすべてのコンテキストで入力と出力の ICMP トラフィックがキャプチャされます。

その他のガイドライン

- ASA が不正な形式の TCP ヘッダーを持つパケットを受信し、ASP が *invalid-tcp-hdr-length* であるというドロップ理由でそのパケットをドロップする場合、そのパケットを受信したインターフェイス上の **show capture** コマンド出力は、そのパケットを表示しません。
- IP トラフィックだけをキャプチャできます。ARP などの非 IP パケットはキャプチャできません。
- インライン SGT タグ付きパケットの場合、キャプチャされたパケットに含まれている追加 CMD ヘッダーを、PCAP ビューアが認識しないことがあります。
- パケットキャプチャには、システムを変更する、またはインスペクションのために接続に挿入されるパケット、NAT、TCP の正規化、パケットの内容を調整するその他の機能が含まれます。

入力トラフィック セレクタ

パケットキャプチャの入力インターフェイス、送信元と宛先のホストまたはネットワーク、およびプロトコルを設定するには、次の手順を実行します。

手順

-
- ステップ 1** ドロップダウン リストから入力インターフェイス名を選択します。
- ステップ 2** 入力送信元ホストおよびネットワークを入力します。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。
- ステップ 3** 入力宛先ホストおよびネットワークを入力します。
- ステップ 4** キャプチャするプロトコルタイプを指定します。指定できるプロトコルは、ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snmp、tcp、またはudpです。
- ICMP にのみ ICMP タイプを入力します。指定できるタイプは、all、alternate address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute、または unreachable です。
 - TCP および UDP プロトコルだけの送信元および宛先ポートのサービスを指定します。指定できるオプションは次のとおりです。
 - すべてのサービスを含めるには、[All Services] を選択します。
 - サービス グループを含めるには、[Service Groups] を選択します。

特定のサービスを含めるには、aol、bgp、chargen、cifs、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、kerberos、klogin、kshell、ldap、ldaps、login、lotusnotes、lpd、netbios-ssn、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpe、tacacs、talk、telnet、uucp、または whois のいずれかを指定します。
- ステップ 5** Cisco TrustSec サービスのパケットキャプチャをイネーブルにするには、[Security Group Tagging] 領域の [SGT number] チェックボックスをオンにして、セキュリティ グループ タグ番号を入力します。有効なセキュリティ グループ タグ番号は 2 ~ 65519 です。
-

出カトラフィック セレクタ

パケットキャプチャでの出力インターフェイス、送信元と宛先のホストとネットワーク、および送信元と宛先ポートのサービスを設定するには、次の手順を実行します。

手順

-
- ステップ 1** インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。
- ステップ 2** ドロップダウン リストから出力インターフェイス名を選択します。

ステップ3 出力送信元ホストおよびネットワークを入力します。

ステップ4 出力宛先ホストおよびネットワークを入力します。

入力設定時に選択したプロトコルタイプがすでにリストされています。

Buffers

パケット キャプチャのパケット サイズ、バッファ サイズ、および循環バッファを使用するかどうかを設定するには、次の手順を実行します。

手順

ステップ1 キャプチャが保持できる最長のパケットを入力します。できるだけ多くの情報をキャプチャするために、指定可能な最長サイズを使用してください。

ステップ2 パケットを保存するためにキャプチャが使用できるメモリの最大容量を入力します。

ステップ3 パケットの保存には循環バッファを使用します。循環バッファのバッファストレージがすべて使い尽くされると、キャプチャは最も古いパケットから上書きを始めます。

概要

[Summary] 画面には、クラスタオプション（クラスタリングを使用している場合）、トラフィック セレクタ、前のウィザード画面で選択したパケット キャプチャのためのバッファ パラメータが表示されます。

キャプチャの実行

キャプチャ セッションの開始および停止、キャプチャ バッファの表示、ネットワーク アナライザ アプリケーションの起動、パケット キャプチャの保存、およびバッファのクリアを行うには、次の手順を実行します。

手順

ステップ1 [Start] をクリックして、選択したインターフェイス上でパケット キャプチャ セッションを開始します。

ステップ2 [Stop] をクリックして、選択したインターフェイス上のパケット キャプチャ セッションを停止します。

ステップ3 [Get Capture Buffer] をクリックして、インターフェイス上でキャプチャされたパケットのスナップショットを取得します。

ステップ4 [Ingress] をクリックして、入力インターフェイスのキャプチャ バッファを表示します。

- ステップ 5** [Egress] をクリックして、出力インターフェイスのキャプチャバッファを表示します。
- ステップ 6** [Clear Buffer on Device] をクリックして、デバイス上のバッファを消去します。
- ステップ 7** [Launch Network Sniffer Application] をクリックして、[Tools] > [Preferences] で指定した、入力キャプチャまたは出力キャプチャを分析するためのパケット分析アプリケーションを起動します。
- ステップ 8** [Save Captures] をクリックして、入力キャプチャおよび出力キャプチャを ASCII または PCAP 形式で保存します。

キャプチャの保存

パケットをさらに分析するために、入力および出力パケットキャプチャを ASCII または PCAP ファイル形式で保存するには、次の手順を実行します。

手順

- ステップ 1** キャプチャバッファを ASCII 形式で保存するには、[ASCII] をクリックします。
- ステップ 2** キャプチャバッファを PCAP 形式で保存するには、[PCAP] をクリックします。
- ステップ 3** 入力パケットキャプチャを保存するファイルを指定するには、[Save ingress capture] をクリックします。
- ステップ 4** 出力パケットキャプチャを保存するファイルを指定するには、[Save egress capture] をクリックします。

ASAv の vCPU 使用量

ASAv の vCPU 使用率では、データパス、制御ポイント、および外部プロセスで使用されている vCPU の量を表示します。

vSphere で報告される vCPU の使用率には、この ASAv の使用率に加えて、次のものが含まれます。

- ASAv アイドル時間
- ASAv VM に使用された %SYS オーバーヘッド
- vSwitch、vNIC および pNIC の間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASAv のレポート : 40%
- DP : 35%
- 外部プロセス : 5%
- vSphere のレポート : 95%
- ASA (ASAv レポートとして) : 40%
- ASA アイドル ポーリング : 10%
- オーバーヘッド : 45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

ASAv のためのオーバーヘッドとして、ESXi サーバが追加のコンピューティング リソースを使用する場合があるため、使用率は 100% を超えることがあります。

VMware の CPU 使用率のレポート

vSphere で [VM Performance] タブをクリックし、[Advanced] をクリックすると [Chart Options] ドロップダウンリストが表示されます。ここには VM の各ステート (%USER、%IDLE、%SYS など) の vCPU 使用率が表示されます。この情報は、VMware の観点から CPU リソースが使用されている場所を理解するのに役立ちます。

ESXi サーバのシェル (ホストへの接続に SSH を使用してシェルにアクセスします) では、esxtop を使用できます。Esxtop は Linux の top コマンドに似た操作性と外観を持ち、次の内容を含む vSphere のパフォーマンスに関する VM のステート情報を提供します。

- vCPU、メモリ、ネットワーク使用率の詳細
- 各 VM のステートごとの vCPU 使用率
- メモリ (実行中に「M」と入力) とネットワーク (実行中に「N」と入力) に加えて、統計情報と RX ドロップ数

ASAv のグラフと vCenter のグラフ

ASAv と vCenter の間で CPU 使用率の数字に違いがあります。

- vCenter のグラフの数値は常に ASAv の数値よりも大きくなります。
- vCenter ではこの値は「%CPU usage」と呼ばれ、ASAv ではこの値は「%CPU utilization」と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。

- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

vCenter は CPU % usage を次のように計算します。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲストオペレーティングシステムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。

使用率を MHz で比較すると、vCenter と ASAv の両方の数値は一致します。vCenter グラフから、MHz % CPU 使用率は $60 / (2499 \times 1 \text{ vCPU}) = 2.4$ と求められます。

設定のテスト

ここでは、シングルモード ASA または各セキュリティ コンテキストの接続性のテスト方法、ASA インターフェイスを ping する方法、およびあるインターフェイス上のホストから他のインターフェイス上のホストに ping できるようにする方法について説明します。

基本接続のテスト：アドレス向けの ping の実行

ping は、特定のアドレスが使用可能で、応答するかどうかを確認するための単純なコマンドです。次のトピックでは、このコマンドの詳細とそれを使って実行可能なテストについて説明します。

ping で実行可能なテスト

デバイスを ping すると、そのデバイスにパケットが送信され、デバイスが応答を返します。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。

ping を使用して、次のテストを実行できます。

- 2 つのインターフェイスのループバック テスト：同じ ASA で一方のインターフェイスからもう一方のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。
- ASA の ping：別の ASA のインターフェイスを ping し、そのインターフェイスがアップして応答することを確認できます。

- ASA 経由の ping : ASA の反対側のデバイスを ping することによって、中間 ASA 経由で ping することができます。パケットは、それぞれの方向に移動するときに、2つの中間 ASA のインターフェイスを通過します。このアクションは、中間ユニットのインターフェイス、動作、および応答時間の基本テストになります。
- ネットワーク デバイスの疑わしい動作をテストするための ping : ASA インターフェイスから、正常に機能していないと思われるネットワーク デバイスに ping することができます。インターフェイスが正しく設定されているにもかかわらずエコーが受信されない場合は、デバイスに問題があると考えられます。
- 中間通信をテストするための ping : ASA インターフェイスから、正常に機能することがわかっているネットワーク デバイスに ping することができます。エコーを受信した場合、中間にあるデバイスがすべて正常に動作し、物理的に正しく接続されていることが確認されたこととなります。

ICMP ping と TCP ping の選択

ASA には、ICMP エコー要求パケットを送信して、エコー応答パケットを受信する従来の ping が付属しています。これは、標準ツールで、すべての仲介ネットワークデバイスで ICMP トラフィックが許可される場合にうまく機能します。ICMP ping を使用して、IPv4/IPv6 アドレスまたはホスト名を ping することができます。

ただし、ICMP を禁止しているネットワークもあります。ご使用のネットワークがこれに該当する場合は、代わりに、TCP ping を使用してネットワーク接続をテストできます。TCP ping では、ping から TCP SYN パケットが送信され、応答で SYN-ACK が受信された段階でその ping が成功したと見なされます。また、TCP ping では、IPv4 アドレスまたはホスト名は ping できますが、IPv6 アドレスは ping できません。

正常な ICMP または TCP ping とは、使用されているアドレスが有効で特定のタイプのトラフィックに応答することを意味しているにすぎません。これは基本接続が機能していることを意味します。デバイス上で動作する他のポリシーで、特定のタイプのトラフィックがデバイスを通過できないようにすることができます。

ICMP の有効化

デフォルトでは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへの ping を実行できます。リターン トラフィックを通過させるように ICMP インспекションをイネーブルにすることがだけです。セキュリティの低いインターフェイスから高いインターフェイスに ping するには、トラフィックを許可する ACL を適用する必要があります。

ASA インターフェイスを ping する場合は、そのインターフェイスに適用された ICMP ルールによって、エコー要求パケットとエコー応答パケットが許可される必要があります。ICMP ルールは省略可能です。このルールを設定しなかった場合は、インターフェイスへのすべての ICMP トラフィックが許可されます。

この手順では、ASA インターフェイスの ICMP ping をイネーブルにするため、または、ASA 経由の ping 用に構成する必要がある ICMP コンフィギュレーションのすべてについて説明します。

手順

ステップ 1 ICMP ルールでエコー要求/エコー応答が許可されることを確認します。

ICMP ルールは、省略可能で、インターフェイスに直接送信される ICMP パケットに適用されます。ICMP ルールを適用しなかった場合は、すべての ICMP アクセスが許可されます。この場合は、アクションが不要です。

ただし、ICMP ルールを実装する場合は、エコー要求メッセージとエコー応答メッセージのアドレスを許可するルールが各インターフェイスに含まれていることを確認します。[Configuration] > [Device Management] > [Management Access] > [ICMP] ペインで ICMP ルールを設定します。

ステップ 2 アクセスルールで ICMP が許可されることを確認します。

ASA 経由でホストを ping する場合は、アクセスルールで ICMP トラフィックの送受信が許可される必要があります。アクセスルールは、少なくとも、エコー要求/エコー応答 ICMP パケットを許可する必要があります。これらのルールはグローバルルールとして追加することができます。

アクセスルールを使用しない場合は、必要な他のタイプのトラフィックも許可する必要があります。これは、インターフェイスにアクセスルールを適用すると、暗黙の deny が追加されるため、他のすべてのトラフィックが破棄されるためです。

[Configuration] > [Firewall] > [Access Rules] ペインでアクセスルールを設定します。単にテスト目的でルールを追加する場合は、テストの終了後にそのルールを削除できます。

ステップ 3 ICMP インスペクションをイネーブルにします。

インターフェイスの ping とは対照的に、ASA 経由で ping する場合は、ICMP インスペクションが必要です。インスペクションを使用すれば、リターントラフィック（つまり、エコー応答パケット）を ping を開始したホストに返すことができるうえ、パケットあたり 1 つの応答の存在が保証されるため、特定のタイプの攻撃を防止することができます。

ICMP インスペクションは、デフォルトのグローバルインスペクションポリシーでイネーブルにできます。

- a) [Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。
- b) **inspection_default** グローバルルールを編集します。
- c) [Rule Actions] > [Protocol Inspection] タブで、ICMP を選択します。
- d) [OK] をクリックし、さらに [Apply] をクリックします。

ホストの ping

デバイスを ping するには、[Tools] > [Ping] を選択して、ping する宛先の IP アドレスまたはホスト名を入力し、[Ping] をクリックするだけです。TCP ping の場合は、[TCP] を選択して、宛先ポートも含めます。通常は、実行する必要があるテストの範囲にします。

成功した ping の出力例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping が失敗した場合は、失敗した試行が ? で示され、成功率が 100% 未満になります（すべて失敗した場合は 0% になります）。

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
????
Success rate is 0 percent (0/5)
```

ただし、ping の一部の側面を制御するパラメータを追加することもできます。以下に基本オプションを示します。

- ICMP ping：宛先ホストに接続するインターフェイスを選択できます。インターフェイスを選択しなかった場合は、ルーティングテーブルを使用して、適切なインターフェイスが決定されます。IPv4/IPv6 アドレスまたはホスト名を ping することができます。
- TCP ping：ping する宛先の TCP ポートを選択する必要もあります。たとえば、HTTP ポートを ping するには **www.example.com 80** とします。IPv4 アドレスまたはホスト名を ping することはできますが、IPv6 アドレスを ping することはできません。

ping を送信する送信元アドレスおよびポートを指定するオプションもあります。この場合は、任意で、送信元から ping が送信されるインターフェイスを選択します（インターフェイスを選択しなかった場合は、ルーティングテーブルが使用されます）。

最後に、ping を繰り返す回数（デフォルトは 5 回）または各試行のタイムアウト（デフォルトは 2 秒）を指定できます。

ASA 接続の体系的なテスト

ASA 接続のさらに体系的なテストを実行する場合は、次の一般的な手順を使用できます。

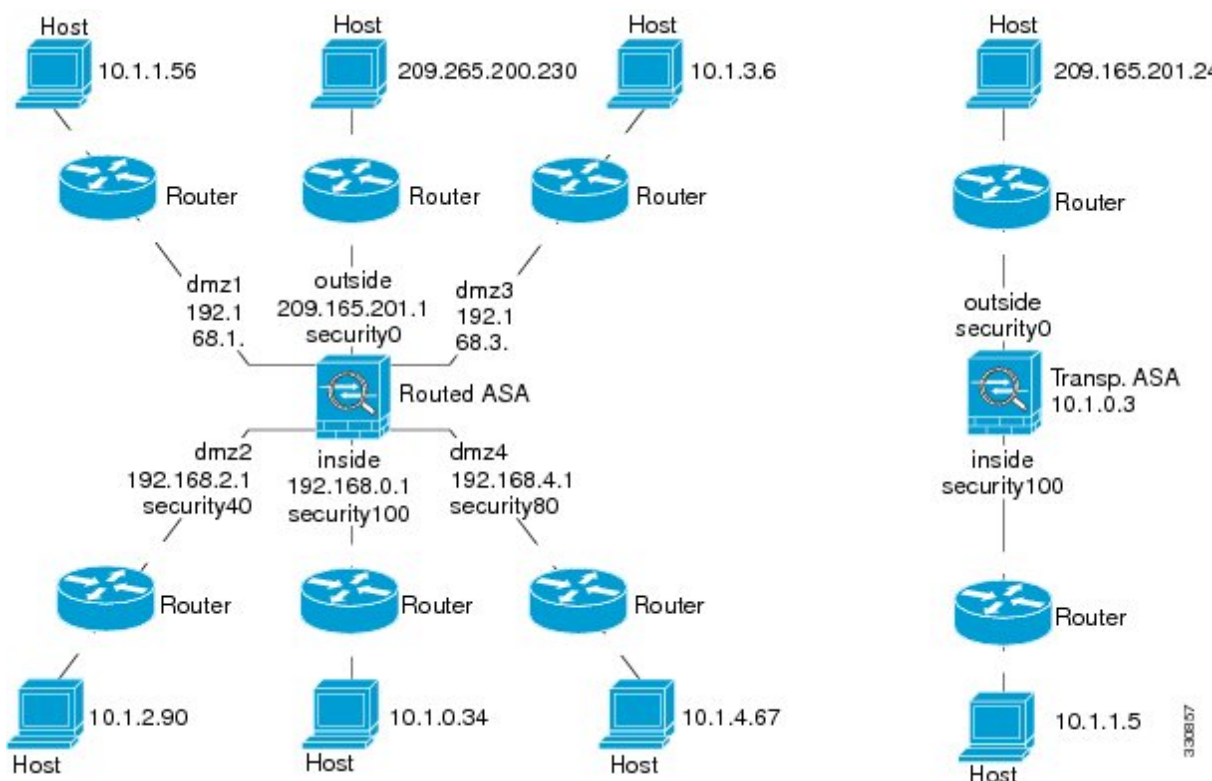
始める前に

手順で説明した syslog メッセージを確認する場合は、ロギングをイネーブルにします（**logging enable** コマンドまたは ASDM の [Configuration] > [Device Management] > [Logging] > [Logging Setup]）。

手順

- ステップ1** インターフェイス名、セキュリティレベル、およびIPアドレスを示すシングルモードのASAまたはセキュリティコンテキストの図を作成します。図には、直接接続されたすべてのルータ、およびASAをpingするルータの反対側にあるホストも含める必要があります。

図 66: インターフェイス、ルータ、およびホストを含むネットワーク図



- ステップ2** 直接接続されたルータから各ASAインターフェイスをpingします。トランスペアレントモードでは、BVI IPアドレスをpingします。このテストでは、ASAインターフェイスがアクティブであること、およびインターフェイスコンフィギュレーションが正しいことを確認します。

ASAインターフェイスがアクティブではない場合、インターフェイスコンフィギュレーションが正しくない場合、またはASAとルータの間でスイッチがダウンしている場合、pingは失敗する可能性があります（次の図を参照）。この場合は、パケットがASAに到達しないので、デバッグメッセージやsyslogメッセージは表示されません。

図 67: ASAインターフェイスでのpingの失敗

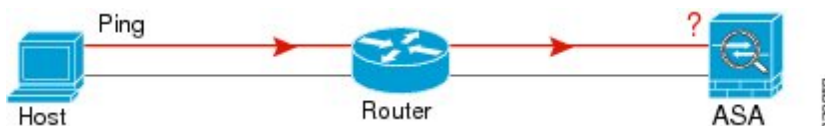
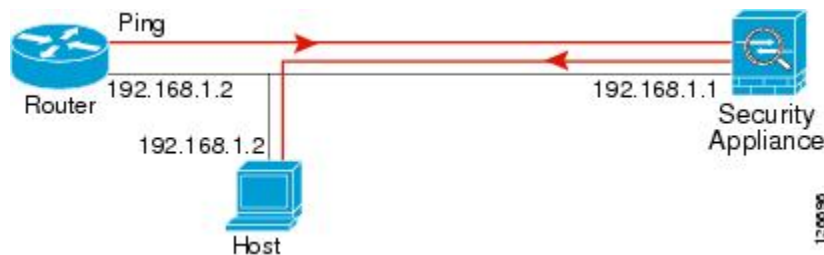


図 68: IP アドレッシングの問題による ping の失敗



ping 応答がルータに戻されない場合は、スイッチループまたは冗長 IP アドレスが存在する可能性があります (次の図を参照)。

ステップ 3 リモートホストから各 ASA インターフェイスを ping します。トランスペアレントモードでは、BVI IP アドレスを ping します。このテストでは、直接接続されたルータがホストと ASA の間でパケットをルーティングできるかどうか、および ASA がパケットを正確にルーティングしてホストに戻せるかどうかを確認します。

中間ルータを通してホストに戻るルートが ASA がない場合、ping は失敗する可能性があります (次の図を参照)。この場合は、デバッグメッセージは ping が成功したことを示しますが、ルーティングの失敗を示す syslog メッセージ 110001 が表示されます。

図 69: ASA の戻りルート未設定による ping の失敗



ステップ 4 ASA インターフェイスから既知のネットワーク デバイスへの ping は正しく機能しています。

- ping を受信しない場合は、送信ハードウェアまたはインターフェイスのコンフィギュレーションに問題がある可能性があります。
- ASA のインターフェイスが正しく設定されているにもかかわらず、「既知の正常な」デバイスからエコー応答を受信しない場合は、インターフェイスハードウェアの受信機能に問題があると考えられます。「既知の正常な」受信機能を持つ別のインターフェイスで、同じ「既知の正常な」デバイスに対して ping を送信してエコーを受信できる場合、最初のインターフェイスのハードウェアの受信機能に問題があると確認されたことになります。

ステップ 5 ホストまたはルータから発信元インターフェイスを介して別のインターフェイス上の別のホストまたはルータに ping します。確認が必要なすべてのインターフェイス ペアに対して、このステップを繰り返します。NAT を使用する場合は、このテストを行うと NAT が正しく動作していることがわかります。

ping が成功すると、ルーテッドモードのアドレス変換 (305009 または 305011) と ICMP 接続が確立されたこと (302020) を確認する syslog メッセージが表示されます。show xlate コマンドまたは show conns コマンドを入力してこの情報を表示することもできます。

NAT が正しく設定されていないことが原因で、ping に失敗することもあります。この場合、NAT が失敗したことを示す syslog メッセージが表示されます (305005 または 305006)。ping

が外部ホストから内部ホストへ送信され、スタティック変換が存在しない場合は、メッセージ 106010 が表示されます。

図 70: ASA のアドレス変換の問題による ping の失敗



ホストまでのルートの追跡

IP アドレスへのトラフィックの送信で問題が発生している場合は、ホストまでのルートを追跡することによってネットワークパスに問題がないかどうかを確認できます。

手順

- ステップ 1 [トレースルート上の ASA の表示 \(985 ページ\)](#)。
- ステップ 2 [パケットルートの決定 \(986 ページ\)](#) を使用して無効にすることができます。

トレースルート上の ASA の表示

デフォルトで、ASA はトレースルート上にホップとして表示されません。これを表示するには、ASA を通過するパケットの存続可能時間を減らして、ICMP 到達不能メッセージのレート制限を増やす必要があります。

手順

- ステップ 1 サービスポリシーを使用して TTL を減らします。
 - a) [Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。
 - b) ルールを追加または編集します。たとえば、TTL を減らすためのオプションを追加可能なルールがすでに存在する場合は、新しいルールを作成する必要はありません。
 - c) ルールをグローバルまたはインターフェイスに適用し、トラフィック照合を指定する [Rule Actions] ページまでウィザードを進めます。たとえば、グローバル match any ルールを作成できます。
 - d) [Rule Actions] ページで、[Connection Settings] タブをクリックして、[Decrement time to live for a connection] を選択します。
 - e) [OK] または [Finish] をクリックしてから、[Apply] をクリックします。
- ステップ 2 ICMP 到達不能レート制限を増やします。

- a) [Configuration] > [Device Management] > [Management Access] > [ICMP] を選択します。
- b) ページの下部にある [IPv4 ICMP Unreachable Message Limits] > [Rate Limit] の値を増やします。たとえば、50 に増やします。
- c) [Apply] をクリックします。

パケットルートの決定

traceroute を使用すれば、パケットが宛先に到着するまでのルートを特定できます。traceroute は、無効なポート上の宛先に UDP パケットを送信することで機能します。ポートが有効でないため、宛先への途中にあるルータは ICMP Time Exceeded Message で応答し、そのエラーを ASA に報告します。

traceroute は送信された各プローブの結果を表示します。出力の各行が 1 つの TTL 値に対応します (昇順)。次の表に、出力記号の説明を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
<i>nn msec</i>	各ノードに対する、指定した数のプローブのラウンドトリップ時間 (ミリ秒)。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP に到達できません。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

始める前に

traceroute は IPv6 をサポートしません。

手順

- ステップ 1** **Tools** > **Traceroute** の順に選択します。
- ステップ 2** ルートを追跡する宛先ホスト名または IP アドレスを入力します。ホスト名を使用するように DNS サーバを設定します。
- ステップ 3** (オプション) トレースの特性を設定します。デフォルトがほとんどのケースに適合します。
 - [Timeout] : タイムアウトするまで応答を待機する時間。デフォルトは 3 秒です。

- [Port] : 使用する UDP ポート。デフォルトは 33434 です。
- [Probe] : 各 TTL レベルで送信するプローブの数。デフォルトは 3 です。
- [TTL] : プローブの最小および最大存続可能時間。デフォルトの最小値は 1 ですが、この値を増やして、既知のホップの表示を抑制することができます。デフォルトの最大値は 30 です。トレースルートは、パケットが宛先に到達するか、または最大値に達すると終了します。
- [Specify source interface or IP address] : トレースの送信元として使用するインターフェイス。インターフェイスは、名前または IP アドレスで指定できます。トランスペアレントモードでは、管理アドレスを使用する必要があります。
- [Reverse Resolve] : DNS 名前解決が設定されている場合に検出されたホップの名前を出力に表示するかどうか。IP アドレスのみを表示するオプションを選択解除します。
- [Use ICMP] : UDP プローブ パケットの代わりに ICMP プローブ パケットを送信するかどうか。

ステップ 4 [Trace Route] をクリックしてトレースルートを開始します。

[Traceroute Output] 領域に、トレースルートの結果についての詳細なメッセージが表示されます。

パケット トレーサを使用したポリシー設定のテスト

送信元と宛先のアドレスおよびプロトコルの特性に基づいてパケットをモデル化することによってポリシー設定をテストできます。トレースは、ポリシー参照を実行してアクセスルールや NATなどをテストし、パケットを許可するか、拒否するかを確認します。

このようにパケットをテストすることによって、ポリシーの結果を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。設定の確認に加えて、トレーサを使用して許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。

手順

ステップ 1 [Tools] > [Packet Tracer] の順に選択します。

ステップ 2 パケット トレースの送信元インターフェイスを選択します。

ステップ 3 パケット トレースのパケットタイプを指定します。指定できるプロトコルタイプは、ICMP、IP、TCP、UDP、およびです。

ステップ 4 (オプション)。セキュリティグループタグの値がレイヤ 2 CMD ヘッダーに埋め込まれたパケットを追跡する (Trustsec) 場合は、[SGT number] をオンにして、セキュリティグループタグの番号 (0 ~ 65533) を入力します。

ステップ5 パケットの送信元と宛先を指定します。

Cisco TrustSec を使用する場合は、IPv4 または IPv6 アドレス、完全修飾ドメイン名 (FQDN)、またはセキュリティグループの名前あるいはタグを指定できます。送信元アドレスに対して、Domain\username 形式でユーザ名を指定することもできます。

ステップ6 プロトコルの特性を指定します。

- [ICMP] : ICMP タイプ、ICMP コード (0 ~ 255)、およびオプションで ICMP 識別子を入力します。
- [TCP/UDP] : 送信元および宛先のポート番号を入力します。
- [Raw IP] : プロトコル番号(0 ~ 255) を入力します。

ステップ7 [Start] をクリックして、パケットをトレースします。

[Information Display Area] に、パケットトレースの結果に関する詳細情報が表示されます。

パフォーマンスとシステムリソースのモニタリング

さまざまなシステムリソースをモニタすることによって、パフォーマンス上の問題またはその他の潜在的な問題を特定することができます。

パフォーマンスのモニタリング

ASA のパフォーマンス情報をグラフ形式または表形式で表示できます。

手順

ステップ1 [Monitoring] > [Properties] > [Connection Graphs] > [Perfmon] の順に選択します。

ステップ2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ3 [Available Graphs] リストから最大 4 つのエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [AAA Perfmon] : 認証、許可、およびアカウンティング要求に関する秒単位の要求数。
- [Inspection Perfmon] : HTTP、FTP、および TCP インスペクションに関する秒単位のパケット数。
- [Web Perfmon] : URL アクセス要求と URL サーバ要求に関する秒単位の要求数。

- [Connections Perfmom] : すべての接続、UDP 接続、TCP 接続、および TCP 代行受信に関する秒単位の接続数。
- [Xlate Perfmom] : 秒単位の NAT xlate。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

メモリ ブロックのモニタリング

空きメモリ ブロックと使用中のメモリ ブロックをグラフ形式または表形式で表示できます。

手順

ステップ 1 [Monitoring] > [Properties] > [System Resources Graphs] > [Blocks] の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストからエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [Blocks Used] : ASA で使用中のメモリ ブロックを表示します。
- [Blocks Free] : ASA の空きメモリ ブロックを表示します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

CPU のモニタリング

CPU 使用率を表示できます。

手順

ステップ 1 [Monitoring] > [Properties] > [System Resources Graphs] > [CPU] の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Selected Graphs] リストに [CPU Utilization] を追加します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間で表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

メモリのモニタリング

メモリ使用量情報をグラフ形式または表形式で表示できます。

手順

ステップ 1 [Monitoring] > [Properties] > [System Resources Graphs] > [Memory] の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストからエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [Free Memory] : ASA の空きメモリを表示します。
- [Used Memory] : ASA の使用中のメモリを表示します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

プロセス単位の CPU 使用率のモニタリング

CPU で実行されているプロセスをモニタできます。特定のプロセスで使用される CPU の使用率に関する情報を取得できます。CPU 使用率の統計情報は降順で並べられ、使用率の最も高いプロセスが先頭に表示されます。また、プロセスごとの CPU に対する負荷に関する情報（記録時間の 5 秒前、1 分前、および 5 分前の情報）も含まれています。この情報は 5 秒おきに自動的に更新され、リアルタイムの統計情報が表示されます。ASDM では、30 秒おきに更新されます。

プロセス単位の CPU 使用率を表示するには、[Monitoring] > [Properties] > [Per-Process CPU Usage] の順に選択します。

自動更新を停止して、情報を手動で更新し、ファイルに保存することができます。[Configure CPU Usage Colors] をクリックして、使用率に基づいて背景色と前景色を選択することによって、使用率の高いプロセスのスキャンを実行しやすくすることもできます。

接続のモニタリング

現在の接続を表形式で表示するには、ASDM メイン ウィンドウで、[Monitoring] > [Properties] > [Connections] の順に選択します。各接続に関する情報には、プロトコル、送信元アドレスと宛先アドレスの特性、最後のパケットが送信または受信されてからのアイドル時間、および接続中のトラフィック量が含まれます。



第 **VIII** 部

モニタリング

- [ロギング \(995 ページ\)](#)
- [SNMP \(1033 ページ\)](#)
- [Anonymous Reporting および Smart Call Home \(1051 ページ\)](#)



第 40 章

ロギング

この章では、システムメッセージを記録して、トラブルシューティングに使用する方法について説明します。

- [ロギングの概要 \(995 ページ\)](#)
- [ロギングのガイドライン \(1003 ページ\)](#)
- [ロギングの設定 \(1004 ページ\)](#)
- [ログのモニタリング \(1024 ページ\)](#)
- [ロギングの履歴 \(1028 ページ\)](#)

ロギングの概要

システム ロギングは、デバイスから `syslog` デーモンを実行するサーバへのメッセージを収集する方法です。中央の `syslog` サーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの `syslog` サービスに送信できます。`syslog` サービスは、シンプル コンフィギュレーションファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、保護された長期的な保存場所をログに提供します。ログは、ルーチントラブルシューティングおよびインシデント処理の両方で役立ちます。

ASA のシステム ログにより、ASA のモニタリングおよびトラブルシューティングに必要な情報を得ることができます。ロギング機能を使用して、次の操作を実行できます。

- ログに記録する `syslog` メッセージを指定する。
- `Syslog` メッセージの重大度のディセーブル化または変更
- 次を含む、`syslog` メッセージ送信先となる、1 つ以上の場所を指定する。
 - 内部バッファ
 - 1 台以上の `syslog` サーバ
 - ASDM
 - SNMP 管理ステーション

- 指定の電子メールアドレス
 - コンソール
 - Telnet と SSH セッション
- 重大度レベルやメッセージクラスなどによる、グループ内での `syslog` メッセージを設定および管理する。
 - `syslog` の生成にレート制限を適用するかどうかを指定する。
 - 内部ログバッファがいっぱいになった場合に、その内容に対して実行する処理（バッファを上書きする、バッファの内容を FTP サーバに送信する、または内容を内部フラッシュメモリに保存する）を指定する。
 - 場所、重大度レベル、クラス、またはカスタムメッセージリストにより、`syslog` メッセージをフィルタリングする。

マルチコンテキストモードでのロギング

それぞれのセキュリティ コンテキストには、独自のロギング コンフィギュレーションが含まれており、独自のメッセージが生成されます。システム コンテキストまたは管理コンテキストにログインし、別のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するメッセージに限定されます。

システム実行スペースで生成されるフェールオーバーメッセージなどの `syslog` メッセージは、管理コンテキストで生成されるメッセージとともに管理コンテキストで表示できます。システム実行スペースでは、ロギングの設定やロギング情報の表示はできません。

ASA は、各メッセージとともにコンテキスト名を含めるように設定できます。これによって、単一の `syslog` サーバに送信されるコンテキストメッセージを区別できます。この機能は、管理コンテキストから送信されたメッセージとシステムから送信されたメッセージの判別にも役立ちます。これが可能なのは、送信元がシステム実行スペースであるメッセージではシステムのデバイス ID が使用され、管理コンテキストが送信元であるメッセージではデバイス ID として管理コンテキストの名前が使用されるからです。

syslog メッセージ分析

次に、さまざまな `syslog` メッセージを確認することで取得できる情報タイプの例を示します。

- ASA セキュリティ ポリシーで許可された接続。これらのメッセージは、セキュリティ ポリシーで開いたままのホールを発見するのに役立ちます。
- ASA セキュリティ ポリシーで拒否された接続。これらのメッセージは、セキュアな内部ネットワークに転送されているアクティビティのタイプを示します。
- ACE 拒否率ロギング機能を使用すると、使用している ASA に対して発生している攻撃が表示されます。

- IDS アクティビティ メッセージには、発生した攻撃が示されます。
- ユーザ認証とコマンドの使用により、セキュリティポリシーの変更を監査証跡することができます。
- 帯域幅使用状況メッセージには、確立および切断された各接続のほか、使用された時間とトラフィック量が示されます。
- プロトコル使用状況メッセージには、各接続で使用されたプロトコルとポート番号が示されます。
- アドレス変換監査証跡メッセージは、確立または切断されている NAT または PAT 接続を記録します。この情報は、内部ネットワークから外部に送信される悪意のあるアクティビティのレポートを受信した場合に役立ちます。

syslog メッセージ形式

syslog メッセージはパーセントの記号 (%) で始まり、次のように構造化されています。

```
%ASA Level Message_number: Message_text
```

次の表に、フィールドの説明を示します。

ASA	ASA が生成するメッセージの syslog メッセージファシリティコード。この値は常に ASA です。
Level	1 ~ 7。レベルは、syslog メッセージに記述されている状況の重大度を示します。値が低いほどその状況の重大度は高くなります。
Message_number	syslog メッセージを特定する 6 桁の固有の番号。
Message_text	状況を説明するテキスト文字列。syslog メッセージのこの部分には、IP アドレス、ポート番号、またはユーザ名が含まれていることがあります。

重大度

次の表に、syslog メッセージの重大度の一覧を示します。それぞれの重大度にカスタムカラーを割り当て、ASDM ログビューアで重大度を識別しやすくなります。syslog メッセージの色設定を行うには、[Tools] > [Preferences] > [Syslog] タブを選択するか、またはログビューア自体のツールバーで [Color Settings] をクリックします。

表 47: Syslog メッセージの重大度

レベル番号	重大度	説明
0	緊急	システムが使用不可能な状態。
1	アラート	すぐに措置する必要があります。

レベル番号	重大度	説明
2	重大	深刻な状況です。
3	エラー	エラー状態です。
4	警告	警告状態。
5	通知	正常ですが、注意を必要とする状況です。
6	情報	情報メッセージです。
7	デバッグ	デバッグメッセージです。



(注) ASAは、重大度 0 (emergencies) の syslog メッセージを生成しません。

syslog メッセージフィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、ASAを設定して、すべての syslog メッセージを1つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるようにできます。

- syslog メッセージの ID 番号
- syslog メッセージの重大度
- syslog メッセージクラス (機能エリアと同等)

これらの基準は、出力先を設定するときに指定可能なメッセージリストを作成して、カスタマイズできます。あるいは、メッセージリストとは無関係に、特定のメッセージクラスを各タイプの出力先に送信するようにASAを設定することもできます。

syslog メッセージクラス

syslog メッセージのクラスは次の2つの方法で使用できます。

- syslog メッセージのカテゴリ全体の出力場所を指定します。
- メッセージクラスを指定するメッセージリストを作成します。

syslog メッセージクラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc (VPN クライアント) クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ~ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージ生成時にオブジェクトが不明な場合、特定の heading = value の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*, Username = *user*, IP = *IP_address*

Group はトンネルグループ、Username はローカルデータベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモートアクセスクライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージクラスと各クラスのメッセージ ID の範囲をリストします。

表 48: syslog メッセージクラスおよび関連付けられているメッセージ ID 番号

クラス	定義	Syslog メッセージ ID 番号
auth	User Authentication	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 認証局	717
citrix	Citrix Client	723
—	クラスタ	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、 eapoudp	ネットワーク アドミッション コントロール の EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336

クラス	定義	Syslog メッセージ ID 番号
電子メール	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレス割り当て	735
ips	侵入防御システム	400、401、420
—	IPv6	325
—	ブラック リスト、ホワイト リスト、およびグレー リスト	338
—	ライセンス	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用する NAC 設定	732
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	電話プロキシ	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
—	Smart Call Home	120

クラス	定義	Syslog メッセージ ID 番号
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL スタック	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tre	トランザクションルール エンジン	780
—	UC-IME	339
tag-switching	サービス タグ スイッチング	779
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
—	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN と AnyConnect Client	716
—	NAT および PAT	305

ログビューアのメッセージのソート

すべての ASDM ログビューア（Real-Time Log Viewer、Log Buffer Viewer、および Latest ASDM Syslog Events Viewer）でメッセージをソートできます。複数のカラムでテーブルをソートするには、ソートの基準とする、最初のカラムのヘッダーをクリックし、**Ctrl** キーを押したまま、同時にソート順に含める他のカラムのヘッダーをクリックします。時間順にメッセージをソートするには、日付と時刻のカラムを両方選択します。どちらか一方だけを選択した場合は、（時刻に関係なく）日付のみまたは（日付に関係なく）時刻のみでメッセージがソートされます。

Real-Time Log Viewer および Latest ASDM Syslog Events Viewer でメッセージをソートすると、記録された新しいメッセージは通常の表示位置となる一番上ではなく、ソートされた順序で表示されます。つまり、メッセージはその他のメッセージの中に混ざって表示されます。

カスタムメッセージリスト

カスタムメッセージリストを作成して、送信する syslog メッセージとその出力先を柔軟に制御できます。カスタム syslog メッセージのリストで、次の条件のいずれかまたはすべてを使用して syslog メッセージのグループを指定します。

- 重大度
- メッセージ ID
- syslog メッセージ ID の範囲
- メッセージクラス

たとえば、メッセージリストを使用して次の操作を実行できます。

- 重大度が 1 および 2 の syslog メッセージを選択し、1 つ以上の電子メールアドレスに送信する。
- メッセージクラス（「ha」など）に関連付けられたすべての syslog メッセージを選択し、内部バッファに保存する。

メッセージリストには、メッセージを選択するための複数の基準を含めることができます。ただし、メッセージ選択基準の追加は、それぞれ個別のコマンドエントリで行う必要があります。重複したメッセージ選択基準を含むメッセージリストが作成される可能性もあります。メッセージリストの 2 つの基準によって同じメッセージが選択される場合、そのメッセージは一度だけログに記録されます。

クラスタ

syslog メッセージは、クラスタリング環境でのアカウントティング、モニタリング、およびトラブルシューティングのための非常に重要なツールです。クラスタ内の各 ASA ユニット（最大 8 ユニットを使用できます）は、syslog メッセージを個別に生成します。特定の **logging** コマンドを使用すると、タイムスタンプおよびデバイス ID を含むヘッダーフィールドを制御できま

す。syslog サーバは、syslog ジェネレータを識別するためにデバイス ID を使用します。logging device-id コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。



(注) クラスタの装置から syslog メッセージをモニタするには、モニタする各装置に対して ASDM セッションを開く必要があります。

ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要がある制限事項とガイドラインについて説明します。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

- syslog サーバでは、syslogd というサーバプログラムを実行する必要があります。Windows では、オペレーティング システムの一部として syslog サーバを提供しています。
- ASA が生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、ASA はメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。たとえば、出力先として複数の syslog サーバを指定するには、各 syslog サーバの [Syslog Server] ペインで、個別のエントリを指定します。
- スタンドバイ デバイスでは、TCP 上での syslog の送信はサポートされません。
- 2 つの異なるリストまたはクラスを、異なる syslog サーバまたは同じロケーションに割り当てることはできません。
- 最大 16 台の syslog サーバを設定できます。ただし、マルチ コンテキスト モードでは、コンテキストごとに 4 サーバに制限されています。
- syslog サーバは、ASA 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスが ICMP 到達不能メッセージを拒否し、同じサーバに syslog を送信するように設定する必要があります。すべての重大度に対してロギングがイネーブルであることを確認します。syslog サーバがクラッシュしないようにするため、syslog 313001、313004、および 313005 の生成を抑制します。
- アクセスリストのヒット数だけを照合するためにカスタム メッセージ リストを使用すると、ロギング重大度がデバッグ (レベル 7) のアクセスリストに対しては、アクセスリストのログは生成されません。logging list コマンドのロギング重大度のデフォルトは、6 に設定されています。このデフォルト動作は設計によるものです。アクセスリストコンフィ

ギューションのロギング重大度をデバッグに明示的に変更する場合は、ロギング コンフィギュレーション自体も変更する必要があります。

ロギング重大度がデバッグに変更されたため、アクセスリストのヒットが含まれていない **show running-config logging** コマンドの出力例を次に示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

次に、アクセスリストヒットを含む **show running-config logging** コマンドの出力例を示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

この場合、アクセスリスト コンフィギュレーションは変更せず、アクセスリストヒット数が次の例のように表示されます。

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

- ASA が TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。

ロギングの設定

ここでは、ロギングの設定方法について説明します。

ロギングのイネーブル化

ロギングをイネーブルにするには、次の手順を実行します。

手順

ステップ 1 ASDM で、次のいずれかを選択します。

- [Home] > [Latest ASDM Syslog Messages] > [Enable Logging]

- **[Configuration] > [Device Management] > [Logging] > [Logging Setup]**
- **[Monitoring] > [Real-Time Log Viewer] > [Enable Logging]**
- **[Monitoring] > [Log Buffer] > [Enable Logging]**

ステップ 2 [Enable logging] チェックボックスをオンにして、ロギングをオンにします。

出力先の設定

トラブルシューティングおよびパフォーマンスのモニタリング用に syslog メッセージの使用状況を最適化するには、syslog メッセージの送信先（内部ログ バッファ、1 つまたは複数の外部 syslog サーバ、ASDM、SNMP 管理ステーション、コンソールポート、指定した電子メールアドレス、または Telnet および SSH セッションなど）を 1 つまたは複数指定することをお勧めします。

外部 syslog サーバへの syslog メッセージの送信

外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、その保存後、ロギングデータを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたり、ログからデータが抽出されてレポート用の別のファイルにその記録が保存されたり、あるいはサイト固有のスクリプトを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

外部 syslog サーバに syslog メッセージを送信するには、次の手順を実行します。

手順

- ステップ 1** **[Configuration] > [Device Management] > [Logging] > [Logging Setup]** を選択します。
- ステップ 2** [Enable logging] チェックボックスをオンにして、ASA に対するロギングを有効にします。
- ステップ 3** [Enable logging on the failover standby unit] チェックボックスをオンにして、スタンバイ ASA に対するロギングを有効にします（可能な場合）。
- ステップ 4** [Send debug messages as syslogs] チェックボックスをオンにして、すべてのデバッグトレース出力がシステムログにリダイレクトされるようにします。このオプションがイネーブルになっている場合、syslog メッセージはコンソールには表示されません。そのため、デバッグメッセージを表示するには、コンソールでロギングをイネーブルにし、デバッグ syslog メッセージ番号および重大度レベルの宛先としてコンソールを設定する必要があります。使用する syslog メッセージ番号は、[711001] です。この syslog メッセージに対するデフォルトの重大度レベルは、[Debugging] です。
- ステップ 5** [Send syslogs in EMBLEM format] チェックボックスをオンにして、EMBLEM 形式をイネーブルにします。これにより、syslog サーバを除くロギングの宛先すべてに対して EMBLEM 形式が使用されます。
- ステップ 6** ロギングバッファがイネーブルの場合、syslog メッセージを保存する内部ログバッファのサイズを指定します。バッファの空き容量がなくなると、FTP サーバまたは内部フラッシュメモ

りにログを保存していない限り、メッセージは上書きされます。デフォルトのバッファサイズは 4096 バイトです。有効な範囲は 4096 ~ 1048576 です。

ステップ 7 バッファ内のデータが上書きされる前に、それらを FTP サーバに保存する場合は、[Save Buffer To FTP Server] チェックボックスをオンします。バッファ内のデータが上書きされるようになる場合は、このチェックボックスをオフにします。

ステップ 8 [Configure FTP Settings] をクリックして、FTP サーバを指定し、バッファ内のデータを保存する際に使用する FTP パラメータを設定します。

ステップ 9 [Save Buffer To Flash] チェックボックスをオンにして、上書きする前に内部フラッシュメモリにバッファの内容を保存します。

(注) このオプションは、ルーテッドまたはトランスペアレントシングルモードだけで使用できます。

ステップ 10 [Configure Flash Usage] をクリックし、ロギングに使用する内部フラッシュメモリの最大容量、および最低限維持すべき空き容量を KB 単位で指定します。このオプションをイネーブルにすると、メッセージが格納されるデバイスディスク上に、「syslog」という名前のディレクトリが作成されます。

(注) このオプションは、単一ルーテッドモードまたはトランスペアレントモードでだけ使用できます。

ステップ 11 ASA で表示するシステムログのキューサイズを指定します。

FTP の設定

ログバッファの内容の保存に使用する FTP サーバのコンフィギュレーションを指定するには、次の手順を実行します。

手順

ステップ 1 [Enable FTP client] チェックボックスをオンにして、FTP クライアントのコンフィギュレーションをイネーブルにします。

ステップ 2 FTP サーバの IP アドレスを指定します。

ステップ 3 保存されるログ バッファ コンテンツの格納先となる FTP サーバ上のディレクトリパスを指定します。

ステップ 4 FTP サーバにログインするためのユーザ名を指定します。

ステップ 5 FTP サーバへログインするためのユーザ名に関連付けられたパスワードを指定します。

ステップ 6 パスワードを確認し、[OK] をクリックします。

ロギングに使用するフラッシュメモリの設定

ログバッファの内容を内部フラッシュメモリに保存する場合の制限事項を指定するには、次の手順を実行します。

手順

- ステップ 1 ロギングに使用できる内部フラッシュメモリの最大容量を指定します (KB 単位)。
- ステップ 2 維持する内部フラッシュメモリの容量を指定します (KB 単位)。内部フラッシュメモリがこの制限値に近づくと、新しいログが保存されなくなります。
- ステップ 3 [OK] をクリックして、[Configure Logging Flash Usage] ダイアログボックスを閉じます。

セキュアロギングの有効化

手順

- ステップ 1 [Configuration] > [Device Management] > [Logging] > [Syslog Server] の順に選択します。
- ステップ 2 セキュアロギングをイネーブルにする syslog サーバを選択し、[Edit] をクリックします。
[Edit Syslog Server] ダイアログボックスが表示されます。
- ステップ 3 [TCP] オプション ボタンをクリックします。
セキュアロギングでは UDP をサポートしていないため、このプロトコルを使用しようとするとエラーが発生します。
- ステップ 4 [Enable secure syslog with SSL/TLS] チェックボックスをオンにして、[OK] をクリックします。

syslog サーバに送信する EMBLEM 形式の syslog メッセージの生成

syslog サーバへの EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

- ステップ 1 [Configuration] > [Device Management] > [Logging] > [Syslog Server] の順に選択します。
- ステップ 2 [Add] をクリックして、新しい syslog サーバを追加します。
[Add Syslog Server] ダイアログボックスが表示されます。
(注) 1つのセキュリティ コンテキストに対して設定できる syslog サーバの数は最大で 4 です (合計で 16 まで)。

ステップ 3 syslog サーバがビジー状態の場合、ASA でキューに入れることができるメッセージ数を指定します。値がゼロの場合は、キューに入れられるメッセージ数が無制限になります。

ステップ 4 [Allow user traffic to pass when TCP syslog server is down] チェックボックスをオンにして、いずれかの syslog サーバがダウンした場合にすべてのトラフィックを制限するかどうかを指定します。TCP を指定すると、ASA は syslog サーバの障害を検出し、セキュリティ保護として ASA を経由する新しい接続をブロックします。UDP を指定すると、ASA は、syslog サーバが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ~ 65535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

(注) TCP での syslog の送信は、スタンバイ ASA ではサポートされていません。

他の出力先への EMBLEM 形式の syslog メッセージの生成

他の出力先への EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Logging] > [Logging Setup] を選択します。

ステップ 2 [Send syslogs in EMBLEM format] チェックボックスをオンにします。

syslog サーバの設定の追加または編集

syslog サーバ設定を追加または編集するには、次の手順を実行します。

手順

ステップ 1 syslog サーバとの通信に使用するインターフェイスを、ドロップダウン リストから選択します。

ステップ 2 syslog サーバとの通信に使用する IP アドレスを入力します。

syslog サーバが ASA または ASASM との通信に使用するプロトコル (TCP または UDP) を選択します。UDP または TCP のいずれかを使用して syslog サーバにデータを送信するように ASA および ASASM を設定することができます。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

ステップ 3 syslog サーバにおいて、ASA または ASASM との通信に使用されるポート番号を入力します。

ステップ 4 [Log messages in Cisco EMBLEM format (UDP only)] チェックボックスをオンにして、シスコの EMBLEM 形式でメッセージをログに記録するかどうかを指定します (プロトコルとして UDP が選択されている場合に限る)。

ステップ 5 [Enable secure logging using SSL/TLS (TCP only)] チェックボックスをオンにして、syslog サーバへの接続が SSL/TLS over TCP の使用により保護され、syslog メッセージの内容が暗号化されるよう指定します。

ステップ 6 [OK] をクリックして設定を完了します。

内部ログバッファへの syslog メッセージの送信

一時的な保存場所となる内部ログバッファに送信する syslog メッセージを指定する必要があります。新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになったとき、つまりバッファラップが発生した場合、ASA がいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。

syslog メッセージを内部ログバッファに送信するには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択して、内部ログバッファに送信する syslog メッセージを指定します。

- [Home] > [Latest ASDM Syslog Messages] > [Configure ASDM Syslog Filters]
- [Configuration] > [Device Management] > [Logging] > [Logging Filters]

ステップ 2 [Monitoring] > [Logging] > [Log Buffer] > [View] の順に選択します。次に [Log Buffer] ペインで [File] > [Clear Internal Log Buffer] の順に選択して、内部ログバッファを空にします。

ステップ 3 [Configuration] > [Device Management] > [Logging] > [Logging Setup] の順に選択して、内部ログバッファのサイズを変更します。デフォルトのバッファサイズは 4 KB です。

ASA は、新しいメッセージを引き続き内部ログバッファに保存し、いっぱいになったログバッファの内容を内部フラッシュメモリに保存します。バッファの内容を別の場所に保存するとき、ASA は、次のタイムスタンプ形式を使用する名前でログファイルを作成します。

`LOG-YYYY-MM-DD-HHMMSS.TXT`

YYYY は年、MM は月、DD は日付、HHMMSS は時間、分、および秒で示された時刻です。

ステップ 4 別の場所に新しいメッセージを保存するには、次のオプションから 1 つを選択します。

- 内部フラッシュメモリに新しいメッセージを送信するには、[Flash] チェックボックスをオンにして、[Configure Flash Usage] をクリックします。[Configure Logging Flash Usage] ダイアログボックスが表示されます。

1. ロギングに使用するフラッシュメモリの最大容量を KB で指定します。
2. ロギングをフラッシュメモリに保持する最小空き領域量を KB で指定します。

3. [OK] をクリックして、このダイアログボックスを閉じます。
- FTP サーバに新しいメッセージを送信するには、[FTP Server] チェックボックスをオンにし、[Configure FTP Settings] をクリックします。[Configure FTP Settings] ダイアログボックスが表示されます。
 1. [Enable FTP Client] チェックボックスをオンにします。
 2. 表示されたフィールドに、FTP サーバ IP アドレス、パス、ユーザ名、パスワードを入力します。
 3. パスワードを確認し、[OK] をクリックしてこのダイアログボックスを閉じます。

内部ログバッファのフラッシュへの保存

内部ログ バッファをフラッシュ メモリに保存するには、次の手順を実行します。

手順

- ステップ 1** [File] > [Save Internal Log Buffer to Flash] の順に選択します。
[Enter Log File Name] ダイアログボックスが表示されます。
- ステップ 2** 最初のオプションを選択し、LOG-YYYY-MM-DD-hhmmss.txt 形式のデフォルト ファイル名でログ バッファを保存します。
- ステップ 3** 2 番目のオプションを選択し、そのログ バッファのファイル名を指定します。
- ステップ 4** ログ バッファのファイル名を入力して [OK] をクリックします。

ログの記録で使用可能な内部フラッシュ メモリの容量の変更

ログの記録で使用可能な内部フラッシュ メモリの容量を変更するには、次の手順を実行します。

手順

- ステップ 1** [Configuration] > [Device Management] > [Logging] > [Logging Setup] を選択します。
- ステップ 2** [Enable Logging] チェックボックスをオンにします。
- ステップ 3** [Logging to Internal Buffer] 領域の [Save Buffer to Flash] チェックボックスをオンにします。
- ステップ 4** [Configure Flash Usage] をクリックします。
[Configure Logging Flash Usage] ダイアログボックスが表示されます。
- ステップ 5** ログインに使用できるフラッシュ メモリの最大容量を KB で入力します。

デフォルトでは、ASAは、内部フラッシュメモリの最大1MBをログデータに使用できます。ASAでログデータを保存するために必要な内部フラッシュメモリの最小空き容量は3MBです。内部フラッシュメモリに保存されているログファイルにより、内部フラッシュメモリの空き容量が設定された最小限の容量を下回ってしまう場合、ASAは最も古いログファイルを削除し、新しいログファイルの保存後も最小限の容量が確保されるようにします。削除するファイルがない場合、または古いファイルをすべて削除しても空きメモリの容量が最小限の容量を下回っている場合、ASAはその新しいログファイルを保存できません。

ステップ6 フラッシュメモリにロギングするために維持する空き領域の最小容量をKBで入力します。

ステップ7 [OK]をクリックして、[Configure Logging Flash Usage]ダイアログボックスを閉じます。

ASDM Java Console による記録されたエントリの参照とコピー

ASDM Java コンソールを使用して、ASDM エラーのトラブルシューティングに役立つ、記録されたエントリをテキスト形式で表示およびコピーできます。

ASDM Java Console にアクセスするには、次の手順を実行します。

手順

ステップ1 [Tools] > [ASDM Java Console] の順に選択します。

ステップ2 コンソールで **m** と入力して、仮想マシンのメモリ統計情報を表示します。

ステップ3 コンソールで **g** と入力して、ガベージコレクションを実行します。

ステップ4 Windows タスク マネージャを開き、**asdm_launcher.exe** ファイルをダブルクリックして、メモリ使用量を監視します。

(注) メモリ割り当ての最大値は256MBです。

電子メールアドレスへの syslog メッセージの送信

syslog メッセージを電子メールアドレスに送信するには、次の手順を実行します。

手順

ステップ1 [Configuration] > [Device Management] > [Logging] > [E-mail Setup] を選択します。

ステップ2 電子メールメッセージとして送信される syslog メッセージの送信元アドレスとして使用する電子メールアドレスを指定します。

ステップ3 [Add] をクリックして、指定した syslog メッセージの受信者の電子メールアドレスを入力します。

ステップ4 その受信者に送信する syslog メッセージの重大度レベルを、ドロップダウンリストから選択します。宛先の電子メールアドレスに対して適用される syslog メッセージの重大度フィルタ

により、指定された重大度レベル以上のメッセージが送信されます。[Logging Filters] ペインで指定されたグローバル フィルタも、各電子メール受信者に適用されます。

ステップ 5 [Edit] をクリックして、この受信者へ送信する syslog メッセージの現在の重大度を変更します。

ステップ 6 [OK] をクリックして、[Add E-mail Recipient] ダイアログボックスを閉じます。

電子メール受信者の追加または編集

電子メールの受信者および重大度を追加または編集するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Logging] > [E-mail Setup] を選択します。

ステップ 2 [Add] または [Edit] をクリックして、[Add/Edit E-Mail Recipient] ダイアログボックスを表示します。

ステップ 3 宛先の電子メールアドレスを入力し、ドロップダウンリストから syslog 重大度を選択します。重大度レベルは次のように定義されています。

- Emergency (レベル 0、システムが使用不能)
 - (注) 重要度レベル 0 を使用することはお勧めできません。
- Alert (レベル 1、即時対処が必要)
- Critical (レベル 2、クリティカル条件)
- Error (レベル 3、エラー条件)
- Warning (レベル 4、警告条件)
- Notification (レベル 5、正常だが顕著な条件)
- Informational (レベル 6、情報メッセージのみ)
- Debugging (レベル 7、デバッグメッセージのみ)

(注) 宛先電子メールアドレスへのメッセージをフィルタリングする場合は、[Add/Edit E-Mail Recipient] ダイアログボックスで指定した重大度と、[Logging Filters] ペインですべての電子メール受信者に対して設定したグローバルフィルタの重大度のうち、上位にある方が使用されます。

ステップ 4 [OK] をクリックして、[Add/Edit E-Mail Recipient] ダイアログボックスを閉じます。

追加または修正されたエントリが [E-mail Recipients] ペインに表示されます。

ステップ 5 [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

リモート SMTP サーバの設定

特定のイベントに対する電子メールアラートおよび通知の送信先となるリモート SMTP サーバを設定するには、次の手順を実行します。

手順

-
- ステップ 1** [Configuration] > [Device Setup] > [Logging] > [SMTP] の順に選択します。
 - ステップ 2** プライマリ SMTP サーバの IP アドレスを入力します。
 - ステップ 3** (任意) スタンバイ SMTP サーバの IP アドレスを入力し、[Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。
-

コンソールポートへの syslog メッセージの送信

syslog メッセージをコンソールポートに送信するには、次の手順を実行します。

手順

-
- ステップ 1** 次のいずれかのオプションを選択します。
 - [Home] > [Latest ASDM Syslog Messages] > [Configure ASDM Syslog Filters]
 - [Configuration] > [Device Management] > [Logging] > [Logging Filters]
 - ステップ 2** [Logging Destination] カラムでコンソールを選択し、[Edit] をクリックします。
[Edit Logging Filters] ダイアログボックスが表示されます。
 - ステップ 3** すべてのイベントクラスまたは特定のイベントクラスのいずれかから syslog を選択して、コンソールポートに送信する syslog メッセージを指定します。
-

Telnet または SSH セッションへの syslog メッセージの送信

syslog メッセージを Telnet または SSH セッションに送信するには、次の手順を実行します。

手順

-
- ステップ 1** 次のいずれかのオプションを選択します。
 - [Home] > [Latest ASDM Syslog Messages] > [Configure ASDM Syslog Filters]
 - [Configuration] > [Device Management] > [Logging] > [Logging Filters]
 - ステップ 2** [Logging Destination] カラムの [Telnet and SSH Sessions] を選択し、[Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

- ステップ 3** すべてのイベント クラスまたは特定のイベント クラスのいずれかから **syslog** を選択して、Telnet または SSH セッションに送信する **syslog** メッセージを指定します。
- ステップ 4** **[Configuration] > [Device Management] > [Logging] > [Logging Setup]** の順に選択して、現在のセッションのロギングだけをイネーブルにします。
- ステップ 5** **[Enable logging]** チェックボックスをオンにし、**[Apply]** をクリックします。

syslog メッセージの設定

syslog メッセージの設定

syslog メッセージを設定するには、次の手順を実行します。

手順

- ステップ 1** **[Configuration] > [Device Management] > [Logging] > [Syslog Setup]** の順に選択します。
- ステップ 2** ファイルメッセージのベースとして使用する **syslog** サーバのシステムログ機能を選択します。デフォルトは **LOCAL(4)20** です。これは、ほとんどの UNIX システムで必要となるコードです。ただし、ネットワークデバイス間では8つのファシリティが共用されているため、システムログではこの値を変更しなければならない場合があります。
- ステップ 3** **[Include timestamp in syslog]** チェックボックスをオンにして、送信される各 **syslog** メッセージに日付と時刻を追加します。
- ステップ 4** ログイン試行が失敗した場合に無効なユーザ名を **syslog** メッセージに表示する場合は、**[Hide username if its validity cannot be determined]** チェックボックスをオフにします。デフォルト設定では、ユーザ名が無効な場合、または有効かどうか不明な場合、ユーザ名は非表示です。たとえば、ユーザが誤ってユーザ名の代わりにパスワードを入力した場合、結果として生成される **syslog** メッセージで「ユーザ名」を隠すのが安全です。ログインに関するトラブルシューティングに役立てるために、無効なユーザ名を表示することもできます。
- ステップ 5** **[Syslog ID]** テーブルに表示する情報を選択します。使用可能なオプションは、次のとおりです。
- **[Syslog ID]** テーブルにすべての **syslog** メッセージ ID を表示するように指定するには、**[Show all syslog IDs]** を選択します。
 - **[Syslog ID]** テーブルに明示的にディセーブルにした **syslog** メッセージ ID だけを表示するように指定するには、**[Show disabled syslog IDs]** を選択します。
 - **[Syslog ID]** テーブルにデフォルト値から変更された重大度を含む **syslog** メッセージ ID だけを表示するように指定するには、**[Show syslog IDs with changed logging]** を選択します。

- [Syslog ID] テーブルに重大度が変更された syslog メッセージ ID と、明示的にディセーブルにされた syslog メッセージ ID だけを表示するように指定するには、[Show syslog IDs that are disabled or with a changed logging level] を選択します。

ステップ 6 [Syslog ID Setup] テーブルには、その設定内容に基づいて、syslog メッセージのリストが表示されます。変更する個々のメッセージ ID またはメッセージ ID の範囲を選択します。選択したメッセージ ID は、ディセーブルにすることも、その重大度レベルを変更することもできます。リストから複数のメッセージ ID を選択する場合は、その範囲の先頭にあたる ID を選択し、Shift キーを押しながらその範囲の最後にあたる ID をクリックします。

ステップ 7 syslog メッセージにデバイス ID が含まれるよう設定する場合は、[Advanced] をクリックします。

syslog ID 設定の編集

syslog メッセージの設定を変更するには、次の手順を実行します。



(注) [Syslog ID(s)] フィールドは表示専用です。この領域に表示される値は、[Syslog Setup] ペインにある [Syslog ID] テーブルで選択されたエントリにより決まります。

手順

- ステップ 1** [Disable Message(s)] チェックボックスをオンにして、[Syslog ID(s)] リストに ID が表示されている syslog メッセージをディセーブルにします。
- ステップ 2** [Syslog ID(s)] リストに表示される syslog メッセージ ID に送信するメッセージの重大度のロギングレベルを選択します。重大度レベルは次のように定義されています。
- Emergency (レベル 0、システムが使用不能)
 - (注) 重要度レベル 0 を使用することはお勧めできません。
 - Alert (レベル 1、即時対処が必要)
 - Critical (レベル 2、クリティカル条件)
 - Error (レベル 3、エラー条件)
 - Warning (レベル 4、警告条件)
 - Notification (レベル 5、正常だが顕著な条件)
 - Informational (レベル 6、情報メッセージのみ)
 - Debugging (レベル 7、デバッグメッセージのみ)

ステップ 3 [OK] をクリックして [Edit Syslog ID Settings] ダイアログボックスを閉じます。

非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

ステップ 1 [Enable syslog device ID] チェックボックスをオンにして、非 EMBLEM 形式の syslog メッセージすべてにデバイス ID が含まれるように指定します。

ステップ 2 次のいずれかのオプションを選択して、どのようなデバイス ID を使用するかを指定します。

- ASA のホスト名
- インターフェイス IP アドレス

選択した IP アドレスに対応するインターフェイス名を、ドロップダウン リストから選択します。

クラスタリングを使用する場合は、[In an ASA cluster, always use master's IP address for the selected interface] チェックボックスをオンにします。

- 文字列
英数字のユーザ定義文字列を入力します。
- ASA クラスタ名

ステップ 3 [OK] をクリックして、[Advanced Syslog Configuration] ダイアログボックスを閉じます。

syslog メッセージに日付と時刻を含める

syslog メッセージに日付と時刻を含めるには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Logging] > [Syslog Setup] の順に選択します。

ステップ 2 [Syslog ID Setup] 領域で [Include timestamp in syslogs] チェックボックスをオンにします。

ステップ 3 [Apply] をクリックして変更内容を保存します。

syslog メッセージの無効化

指定した syslog メッセージをディセーブルにするには、次の手順を実行します。

手順

-
- ステップ 1 **[Configuration] > [Device Management] > [Logging] > [Syslog Setup]** の順に選択します。
 - ステップ 2 テーブルからディセーブルにする syslog を選択して、**[Edit]** をクリックします。
[Edit Syslog ID Settings] ダイアログボックスが表示されます。
 - ステップ 3 **[Disable messages]** チェックボックスをオンにし、**[OK]** をクリックします。
-

syslog メッセージの重大度の変更

syslog メッセージの重大度を変更するには、次の手順を実行します。

手順

-
- ステップ 1 **[Configuration] > [Device Management] > [Logging] > [Syslog Setup]** の順に選択します。
 - ステップ 2 重大度を変更する syslog をテーブルから選択して、**[Edit]** をクリックします。
[Edit Syslog ID Settings] ダイアログボックスが表示されます。
 - ステップ 3 適切な重大度を **[Logging Level]** ドロップダウンリストから選択し、**[OK]** をクリックします。
-

スタンバイ装置の syslog メッセージのブロック

スタンバイ装置で特定の syslog メッセージが生成されないようにするには、次の手順を実行します。

手順

-
- ステップ 1 **[Configuration] > [Device Management] > [Logging] > [Syslog Settings]** の順に選択します。
 - ステップ 2 テーブルの syslog ID を選択し、**[Edit]** をクリックします。
[Edit Syslog ID Settings] ダイアログボックスが表示されます。
 - ステップ 3 スタンバイ装置で syslog メッセージが生成されないようにするには、**[Disable messages on standby unit]** チェックボックスをオンにします。
 - ステップ 4 **[OK]** をクリックして、このダイアログボックスを閉じます。
-

非 EMBLEM 形式の syslog メッセージにデバイス ID を含める

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

-
- ステップ 1** **[Configuration] > [Device Management] > [Logging] > [Syslog Setup] > [Advanced] > [Advanced Syslog Configuration]** の順に選択します。
- ステップ 2** **[Enable syslog device ID]** チェックボックスをオンにします。
- ステップ 3** **[Device ID]** 領域で、**[Hostname]**、**[Interface IP Address]** または **[String]** オプション ボタンをクリックします。
- **[Interface IP Address]** オプションを選択した場合は、ドロップダウン リストで正しいインターフェイスが選択されていることを確認します。
 - **[String]** オプションを選択した場合は、**[User-Defined ID]** フィールドにデバイス ID を入力します。文字列の長さは、最大で 16 文字です。
- (注) イネーブルにすると、EMBLEM 形式の syslog メッセージや SNMP トラップにデバイス ID は表示されません。
- ステップ 4** **[OK]** をクリックして、**[Advanced Syslog Configuration]** ダイアログボックスを閉じます。
-

カスタム イベント リストの作成

イベントリストの定義には、次の 3 つの基準を使用します。

- イベント クラス
- 重大度
- メッセージ ID

特定のロギングの宛先 (SNMP サーバなど) に送信するカスタム イベント リストを作成するには、次の手順を実行します。

手順

-
- ステップ 1** **[Configuration] > [Device Management] > [Logging] > [Event Lists]** の順に選択します。
- ステップ 2** **[Add]** をクリックして、**[Add Event List]** ダイアログボックスを表示します。
- ステップ 3** イベント リストの名前を入力します。スペースは使用できません。
- ステップ 4** **[Add]** をクリックして、**[Add Class and SeverityFilter]** ダイアログボックスを表示します。
- ステップ 5** ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。
- ステップ 6** ドロップダウン リストから重大度レベルを選択します。重大度レベルは次のとおりです。
- Emergency (レベル 0、システムが使用不能)

(注) 重要度レベル 0 を使用することはお勧めできません。

- Alert (レベル 1、即時対処が必要)
- Critical (レベル 2、クリティカル条件)
- Error (レベル 3、エラー条件)
- Warning (レベル 4、警告条件)
- Notification (レベル 5、正常だが顕著な条件)
- Informational (レベル 6、情報メッセージのみ)
- Debugging (レベル 7、デバッグメッセージのみ)

ステップ 7 [OK] をクリックして、[Add Event List] ダイアログボックスを閉じます。

ステップ 8 [Add] をクリックして、[Add Syslog Message ID Filter] ダイアログボックスを表示します。

ステップ 9 フィルタに含める syslog メッセージ ID または syslog メッセージ ID の範囲 (101001 ~ 199012 など) を入力します。

ステップ 10 [OK] をクリックして、[Add Event List] ダイアログボックスを閉じます。

目的のイベントがリストに表示されます。

ロギングフィルタの設定

ロギングの宛先へのメッセージフィルタの適用

ロギングの宛先にメッセージフィルタを適用するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Logging] > [Logging Filters] を選択します。

ステップ 2 フィルタを適用するロギングの宛先の名前を選択します。選択できるロギングの宛先は次のとおりです。

- ASDM
- コンソール ポート
- 電子メール
- 内部バッファ
- SNMP サーバ
- Syslog サーバ

- Telnet または SSH セッション

このほか、2 番目のカラム [Syslogs From All Event Classes] と 3 番目のカラム [Syslogs From Specific Event Classes] でも選択操作を行います。2 番目のカラムでは、ロギングの宛先へのメッセージをフィルタリングする場合に使用する重大度やイベントクラスが表示されるほか、すべてのイベントクラスに対してロギングをディセーブルにするかを選択することもできます。3 番目のカラムには、選択したロギングの宛先へのメッセージをフィルタリングする場合に使用するイベントクラスが表示されます。

ステップ 3 [Edit] をクリックして、[Edit Logging Filters] ダイアログボックスを表示します。フィルタを適用、編集、またはディセーブルにする手順については、[ロギングフィルタの適用 \(1020 ページ\)](#) を参照してください。

ロギングフィルタの適用

フィルタを適用するには、次の手順を実行します。

手順

- ステップ 1** 重大度レベルに基づいて syslog メッセージのフィルタリングを行う場合は、[Filter on severity] オプションを選択します。
- ステップ 2** イベントリストに基づいて syslog メッセージのフィルタリングを行う場合は、[Use event list] オプションを選択します。
- ステップ 3** 選択した宛先に対するロギングをすべてディセーブルにする場合は、[Disable logging from all event classes] オプションを選択します。
- ステップ 4** [New] をクリックして、新しいイベントリストを追加します。イベントリストを新たに追加する手順については、[カスタムイベントリストの作成 \(1018 ページ\)](#) を参照してください。
- ステップ 5** ドロップダウンリストからイベントクラスを選択します。使用できるイベントクラスは、使用しているデバイスモードによって異なります。
- ステップ 6** ドロップダウンリストから、ロギングメッセージの重大度レベルを選択します。重大度レベルは次のとおりです。
- Emergency (レベル 0、システムが使用不能)
(注) 重要度レベル 0 を使用することはお勧めできません。
 - Alert (レベル 1、即時対処が必要)
 - Critical (レベル 2、クリティカル条件)
 - Error (レベル 3、エラー条件)
 - Warning (レベル 4、警告条件)
 - Notification (レベル 5、正常だが顕著な条件)

- Informational (レベル 6、情報メッセージのみ)
- Debugging (レベル 7、デバッグ メッセージのみ)

ステップ 7 [Add] をクリックして、イベント クラスおよび重大度レベルを追加し、[OK] をクリックします。

ダイアログボックスの上部には、フィルタに対して選択したロギングの宛先が表示されます。

syslog メッセージ ID フィルタの追加または編集

syslog メッセージ ID フィルタを作成または編集する手順については、[syslog ID 設定の編集 \(1015 ページ\)](#) を参照してください。

メッセージクラスと重大度フィルタの追加または編集

メッセージのフィルタリングに使用するメッセージクラスおよび重大度レベルを追加または編集するには、次の手順を実行します。

手順

ステップ 1 ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 2 ドロップダウン リストから、ロギング メッセージの重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency (レベル 0、システムが使用不能)
(注) 重要度レベル 0 を使用することはお勧めできません。
- Alert (レベル 1、即時対処が必要)
- Critical (レベル 2、クリティカル条件)
- Error (レベル 3、エラー条件)
- Warning (レベル 4、警告条件)
- Notification (レベル 5、正常だが顕著な条件)
- Informational (レベル 6、情報メッセージのみ)
- Debugging (レベル 7、デバッグ メッセージのみ)

ステップ 3 選択が終了したら、[OK] をクリックします。

指定した出力先へのクラス内のすべての syslog メッセージの送信

クラス内のすべての syslog メッセージを指定した出力先に送信するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Logging] > [Logging Filters] を選択します。

ステップ 2 指定した出力先の設定をオーバーライドするには、変更する出力先を選択してから [Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3 [Syslogs from All Event Classes] または [Syslogs from Specific Event Classes] 領域のいずれかで設定を変更し、[OK] をクリックしてこのダイアログボックスを閉じます。

たとえば、重大度 7 のメッセージが内部ログバッファに送信されるように指定し、重大度 3 の ha クラスのメッセージが内部ログバッファに送信されるように指定すると、後のコンフィギュレーションが優先されます。

1 つのクラスが複数の出力先に送信されるように指定する場合は、出力先ごとに異なるフィルタリング オプションを選択します。

syslog メッセージの生成レートの制限

syslog メッセージの生成レートを制限するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Logging] > [Rate Limit] を選択します。

ステップ 2 レート制限を割り当てるロギングレベル（メッセージの重大度）を選択します。重大度レベルは次のように定義されています。

- Emergency（レベル 0、システムが使用不能）
- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）

- Debugging (レベル7、デバッグメッセージのみ)

- ステップ3** 送信されるメッセージの数が [No of Messages] フィールドに表示されます。また、選択したロギングレベルで送信できるメッセージ数を制限する際の基準となる時間間隔 (秒単位) が [Interval (Seconds)] フィールドに表示されます。テーブルからロギングレベルを選択し、[Edit] をクリックして [Edit Rate Limit for Syslog Logging Level] ダイアログボックスを表示します。
- ステップ4** 以降の手順については、[個々の syslog メッセージに対するレート制限の割り当てまたは変更 \(1023 ページ\)](#) を参照してください。

個々の syslog メッセージに対するレート制限の割り当てまたは変更

個々の syslog メッセージにレート制限を割り当てる、またはメッセージごとにレート制限を変更するには、次の手順を実行します。

手順

- ステップ1** 特定の syslog メッセージにレート制限を割り当てる場合は、[Add] をクリックして、[Add Rate Limit for Syslog Message] ダイアログボックスを表示します。
- ステップ2** 以降の手順については、[syslog メッセージに対するレート制限の追加または編集 \(1023 ページ\)](#) を参照してください。
- ステップ3** 特定の syslog メッセージに対するレート制限を変更する場合は、[Edit] をクリックして、[Edit Rate Limit for Syslog Message] ダイアログボックスを表示します。
- ステップ4** 以降の手順については、[syslog 重大度に対するレート制限の編集 \(1024 ページ\)](#) を参照してください。

syslog メッセージに対するレート制限の追加または編集

特定の syslog メッセージに対するレート制限を追加または変更するには、次の手順を実行します。

手順

- ステップ1** 特定の syslog メッセージに対するレート制限を追加する場合は、[Add] をクリックして、[Add Rate Limit for Syslog Message] ダイアログボックスを表示します。特定の syslog メッセージに対するレート制限を変更する場合は、[Edit] をクリックして、[Edit Rate Limit for Syslog Message] ダイアログボックスを表示します。
- ステップ2** レートを制限する syslog メッセージの ID を入力します。
- ステップ3** 指定した時間内に送信できるメッセージの最大数を入力します。
- ステップ4** 指定したメッセージのレートを制限する際の基準となる時間間隔を秒単位で入力し、[OK] をクリックします。

(注) メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

syslog 重大度に対するレート制限の編集

指定した syslog 重大度のレート制限を変更するには、次の手順を実行します。

手順

- ステップ1 指定した重大度で送信可能なメッセージの最大数を指定します。
- ステップ2 指定した重大度のメッセージに対するレートを制限する基準となる時間間隔を秒単位で入力し、[OK] をクリックします。

選択したメッセージ重大度が表示されます。

(注) メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

ログのモニタリング

ロギング ステータスの監視については、次のコマンドを参照してください。

- [Monitoring] > [Logging] > [Log Buffer] > [View]

このペインでは、ログ バッファを表示できます。

- [Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]

このペインでは、リアルタイムのログを表示できます。

- [Tools] > [Command Line Interface]

このペインでは、さまざまな非インタラクティブコマンドを発行し、結果を表示することができます。

ログ ビューアを使用した syslog メッセージのフィルタリング

Real-Time Log Viewer および Log Buffer Viewer の任意のカラムに対応する 1 つ以上の値に基づいて、syslog メッセージをフィルタリングできます。

ログ ビューアのいずれかを使用して syslog メッセージをフィルタリングするには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択します。

- **[Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]**
- **[Monitoring] > [Logging] > [Log Buffer] > [View]**

ステップ 2 [Real-Time Log Viewer] または [Log Buffer Viewer] ダイアログボックスのいずれかで、ツールバーの [Build Filter] をクリックします。

ステップ 3 [Build Filter] ダイアログボックスで、syslog メッセージに適用するフィルタリング基準を指定します。

- a) [Date and Time] 領域で、リアルタイム、特定時刻、時間範囲の 3 つのオプションから 1 つを選択します。特定時刻を選択した場合は、数値を入力してドロップダウンリストから時または分を選択し、時刻を指定します。時間範囲を選択した場合、[Start Time] フィールドのドロップダウン矢印をクリックすると、カレンダーが表示されます。ドロップダウンリストから開始日と開始時刻を選択し、[OK] をクリックします。[End Time] フィールドのドロップダウン矢印をクリックすると、カレンダーが表示されます。ドロップダウンリストから終了日と終了時刻を選択し、[OK] をクリックします。
- b) [Severity] フィールドに有効な重大度を入力します。または、[Severity] フィールドの右側で [Edit] アイコンをクリックします。フィルタリングする重大度をリストでクリックします。重大度 1～7 を含めるには、[All] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Severity] フィールドの右側にある [Info] アイコンをクリックします。
- c) [Syslog ID] フィールドに有効な syslog ID を入力します。または、[Syslog ID] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウンリストからフィルタ対象の条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Syslog ID] フィールドの右側にある [Info] アイコンをクリックします。
- d) [Source IP Address] フィールドに有効な送信元 IP アドレスを入力するか、または [Source IP Address] フィールドの右側で [Edit] アイコンをクリックします。単一の IP アドレスまたは IP アドレスの特定の範囲を選択し、[Add] をクリックします。特定の IP アドレスまたは IP アドレスの範囲を除外するには、[Do not include (exclude) this address or range] チェックボックスをオンにして、[OK] をクリックし、[Build Filter] ダイアログボックスにこれらの設定を表示します。使用する正しい入力形式に関する詳細な情報については、[Source IP Address] フィールドの右側にある [Info] アイコンをクリックします。
- e) [Source Port] フィールドに有効な送信元ポートを入力するか、または [Source Port] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウンリストからフィルタ対象の条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Source Port] フィールドの右側にある [Info] アイコンをクリックします。
- f) [Destination IP Address] フィールドに有効な宛先 IP アドレスを入力するか、または [Destination IP Address] フィールドの右側で [Edit] アイコンをクリックします。単一の IP アドレスまた

はIPアドレスの特定の範囲を選択し、[Add] をクリックします。特定のIPアドレスまたはIPアドレスの範囲を除外するには、[Do not include (exclude) this address or range] チェックボックスをオンにします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Destination IP Address] フィールドの右側にある [Info] アイコンをクリックします。

- g) [Destination Port] フィールドに有効な宛先ポートを入力するか、または [Destination Port] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウンリストからフィルタ対象の条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Destination Port] フィールドの右側にある [Info] アイコンをクリックします。
- h) [Description] フィールドにフィルタリングテキストを入力します。このテキストには、正規表現を含む、1 つ以上の文字からなる任意の文字列を指定できます。ただし、セミコロンは有効な文字ではありません。また、この設定では大文字と小文字が区別されます。複数のエントリを指定する場合は、カンマで区切ります。
- i) [OK] をクリックして、指定したフィルタリング設定をログビューアの [Filter By] ドロップダウンリストに追加します。フィルタ文字列は特定の形式に従います。FILTER: プレフィックスは、[Filter By] ドロップダウンリストに表示されるすべてのカスタム フィルタを示します。このフィールドにはランダムなテキストを入力することもできます。

次の表に、使用される形式の例を示します。

Build Filter の例	フィルタ文字列形式
Source IP = 192.168.1.1 または 0.0.0.0 Source Port = 67	FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67;
Severity = Informational Destination IP = 1.1.1.1 ~ 1.1.1.10	FILTER: sev=6;dstIP=1.1.1.1-1.1.1.10;
725001 ~ 725003 の範囲外の syslog ID	FILTER: sysID=!725001-725003;
Source IP = 1.1.1.1 Description = Built outbound	FILTER: srcIP=1.1.1.1;descr=Built outbound

ステップ 4 [Filter By] ドロップダウンリストの設定の 1 つを選択し、ツールバーの [Filter] をクリックして、syslog メッセージをフィルタリングします。この設定は、これ以降のすべての syslog メッセージにも適用されます。すべてのフィルタをクリアするには、ツールバーにある [Show All] をクリックします。

(注) [Build Filter] ダイアログボックスを使用して指定したフィルタは保存できません。これらのフィルタは、そのフィルタが作成された ASDM セッションのみで有効です。

フィルタリング設定の編集

[Build Filter] ダイアログボックスを使用して作成したフィルタリング設定を編集するには、次の手順を実行します。

手順

次のいずれかのオプションを選択します。

- [Filter By] ドロップダウンリストで変更を入力して、フィルタを直接修正します。
- [Filter By] ドロップダウンリストでフィルタを選択し、[Build Filter] をクリックして [Build Filter] ダイアログボックスを表示します。[Clear Filter] をクリックして、現在のフィルタ設定を削除し、新しい値を入力します。それ以外の場合は、表示された設定を変更して [OK] をクリックします。

(注) これらのフィルタリング設定は、[Build Filter] ダイアログボックスで定義されたフィルタのみに適用されます。

- ツールバーの [Show All] をクリックすると、フィルタリングが停止し、すべての syslog メッセージが表示されます。

ログビューアを使用した特定のコマンドの発行

いずれかのログビューアを使用して、**ping**、**tracert**、**whois**、および **dns lookup** コマンドを発行できます。

これらのコマンドのいずれかを実行するには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択します。

- [Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]
- [Monitoring] > [Logging] > [Log Buffer] > [View]

ステップ 2 [Real-Time Log Viewer] または [Log Buffer] ペインから [Tools] をクリックし、実行するコマンドを選択します。または、表示された特定の syslog メッセージを右クリックしてコンテキストメニューを表示し、実行するコマンドを選択します。

[Entering command] ダイアログボックスが表示され、選択したコマンドが自動的にドロップダウンリストに表示されます。

ステップ 3 選択した syslog メッセージの送信元 IP アドレスまたは宛先 IP アドレスのいずれかを [Address] フィールドに入力し、[Go] をクリックします。

指定した領域にコマンド出力が表示されます。

ステップ 4 [Clear] をクリックして出力を削除し、実行する別のコマンドをドロップダウンリストから選択します。必要に応じてステップ 3 を繰り返します。完了したら [Close] をクリックします。

ロギングの履歴

表 49: ロギングの履歴

機能名	プラットフォーム リリース	説明
Logging	7.0(1)	さまざまな出力先を経由して ASA ネットワーク ロギング情報を提供します。ログファイルを表示して保存するオプションも含まれています。 次の画面が導入されました。 [Configuration] > [Device Management] > [Logging] > [Logging Setup]。
レート制限	7.0(4)	syslog メッセージが生成されるレートを制限します。 次の画面が変更されました。 [Configuration] > [Device Management] > [Logging] > [Rate Limit]。
ロギング リスト	7.2(1)	さまざまな基準（ロギングレベル、イベントクラス、およびメッセージ ID）でメッセージを指定するために他のコマンドで使用されるロギングリストを作成します。 次の画面が変更されました。 [Configuration] > [Device Management] > [Logging] > [Event Lists]。

機能名	プラットフォーム リリース	説明
セキュア ロギング	8.0(2)	<p>リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [Logging] > [Syslog Server]。</p>
ロギング クラス	8.0(4)、8.1(1)	<p>ロギング メッセージの ipaa イベントクラスに対するサポートが追加されました。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [Logging] > [Logging Filters]。</p>
ロギングクラスと保存されたロギングバッファ	8.2(1)	<p>ロギング メッセージの dap イベントクラスに対するサポートが追加されました。</p> <p>保存されたロギング バッファ (ASDM、内部、FTP、およびフラッシュ) をクリアする追加サポート。</p> <p>次の画面が変更されました。 [Configuration] > [Device Management] > [Logging] > [Logging Setup]。</p>
パスワードの暗号化	8.3(1)	<p>パスワードの暗号化に対するサポートが追加されました。</p>
ログ ビューア	8.3(1)	<p>送信元 IP アドレスおよび宛先 IP アドレスがログ ビューアに追加されました。</p>

機能名	プラットフォーム リリース	説明
拡張ロギングと接続ブロック	8.3(2)	<p>TCPを使用するように syslog サーバを設定すると、syslog サーバを使用できない場合、ASA はサーバが再び使用可能になるまで syslog メッセージを生成する新しい接続をブロックします（たとえば、VPN、ファイアウォール、カットスループロキシ接続）。この機能は、ASA のロギング キューがいっぱいになるときに新しい接続をブロックするように拡張されました。接続は、ロギング キューがクリアされると再開されます。</p> <p>この機能は、Common Criteria EAL4+ への準拠のために追加されました。必要でない限り、syslog メッセージを送受信できない場合でも接続を許可することを推奨します。接続を許可するには、[Configuration] > [Device Management] > [Logging] > [Syslog Servers] ペインで [Allow user traffic to pass when TCP syslog server is down] チェックボックスをオンにします。</p> <p>414005、414006、414007、414008 の各 syslog メッセージが導入されました。変更された ASDM 画面はありません。</p>

機能名	プラットフォーム リリース	説明
syslog メッセージのフィルタリングとソート	8.4(1)	<p>次のサポートが追加されました。</p> <ul style="list-style-type: none"> さまざまなカラムに対応する複数のテキスト文字列に基づく syslog メッセージフィルタリング。 カスタム フィルタの作成。 メッセージのカラムによるソート。詳細については、『ASDM 構成ガイド』を参照してください。 <p>この機能は、すべての ASA バージョンと相互運用性があります。</p> <p>次の画面が変更されました。</p> <p>[Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]。</p> <p>[Monitoring] > [Logging] > [Log Buffer Viewer] > [View]。</p>
クラスタ	9.0(1)	<p>ASA 5580 および 5585-X のクラスタリング環境での syslog メッセージ生成のサポートが追加されました。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Logging] > [Syslog Setup] > [Advanced] > [Advanced Syslog Configuration]。</p>
スタンバイ装置の syslog のブロック	9.4(1)	<p>フェールオーバー コンフィギュレーションのスタンバイ装置で特定の syslog メッセージの生成をブロックするためのサポートを追加しました。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Management] > [Logging] > [Syslog Setup]。</p>
syslog サーバでの IPv6 アドレスのサポート	9.7(1)	<p>TCP と UDP 経由で syslog を記録、送信、受信するために、syslog サーバを IPv6 アドレスで設定できるようになりました。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Management] > [Logging] > [Syslog Servers] > [Add Syslog Server]</p>



第 41 章

SNMP

この章では、Simple Network Management Protocol (SNMP) に Cisco ASA をモニタさせるための設定方法について説明します。

- [SNMP の概要 \(1033 ページ\)](#)
- [SNMP のガイドライン \(1037 ページ\)](#)
- [SNMP を設定します。 \(1039 ページ\)](#)
- [SNMP モニタリング \(1044 ページ\)](#)
- [SNMP の履歴 \(1045 ページ\)](#)

SNMP の概要

SNMP は、ネットワークデバイス間での管理情報の交換を容易にするアプリケーション層プロトコルで、TCP/IP プロトコルスイートの一部です。ASA は SNMP バージョン 1、2c、および 3 を使用したネットワーク監視に対するサポートを提供し、3 つのバージョンの同時使用をサポートします。ASA のインターフェイス上で動作する SNMP エージェントを使用すると、HP OpenView などのネットワーク管理システム (NMS) を使用してネットワークデバイスをモニタできます。ASA は GET 要求の発行を通じて SNMP 読み取り専用アクセスをサポートします。SNMP 書き込みアクセスは許可されていないため、SNMP を使用して変更することはできません。さらに、SNMP SET 要求はサポートされていません。

NMS (ネットワーク管理システム) に特定のイベント (イベント通知) を送信するために、管理対象デバイスから管理ステーションへの要求外のメッセージであるトラップを送信するように ASA を設定したり、NMS を使用してセキュリティデバイス上で管理情報ベース (MIB) を検索できます。MIB は定義の集合であり、ASA は各定義に対応する値のデータベースを保持しています。MIB をブラウズすることは、NMS から MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して値を決定することを意味します。

ASA には SNMP エージェントが含まれています。このエージェントは、通知を必要とすることが事前に定義されているイベント (たとえば、ネットワーク内のリンクがアップ状態またはダウン状態になる) が発生すると、指定した管理ステーションに通知します。このエージェントが送信する通知には、管理ステーションに対して自身を識別する SNMP OID が含まれています。ASA エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP の用語

次の表に、SNMP で頻繁に使用される用語を示します。

表 50: SNMP の用語

用語	説明
エージェント	ASAで稼働する SNMP サーバ。SNMP エージェントは、次の機能を搭載しています。 <ul style="list-style-type: none"> ネットワーク管理ステーションからの情報の要求およびアクションに応答する。 管理情報ベース (SNMP マネージャが表示または変更できるオブジェクトの集合) へのアクセスを制御する。 SET 操作を許可しない。
ブラウジング	デバイス上の SNMP エージェントから必要な情報をポーリングすることによって、ネットワーク管理ステーションからデバイスのヘルスをモニタすること。このアクティビティには、ネットワーク管理ステーションから MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して、値を決定することが含まれる場合があります。
管理情報ベース (MIB)	パケット、接続、バッファ、フェールオーバーなどに関する情報を収集するための標準化されたデータ構造。MIBは、大部分のネットワークデバイスで使用される製品、プロトコル、およびハードウェア標準によって定義されます。SNMP ネットワーク管理ステーションは、MIB をブラウズし、特定のデータまたはイベントの発生時にこれらを要求できます。
ネットワーク管理ステーション (NMS)	SNMP イベントのモニタやASAなどのデバイスの管理用に設定されている、PC またはワークステーション。
オブジェクト ID (OID)	NMS に対してデバイスを識別し、モニタおよび表示される情報の源をユーザに示すシステム。
Trap	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslogメッセージなどのアラーム状態が含まれます。

SNMP バージョン 3 の概要

SNMP バージョン 3 は SNMP バージョン 1 またはバージョン 2c では使用できなかったセキュリティ拡張機能を提供します。SNMP バージョン 1 とバージョン 2c は SNMP サーバと SNMP エージェント間でデータをクリアテキストで転送します。SNMP バージョン 3 は認証とプライバシー オプションを追加してプロトコルオペレーションをセキュリティ保護します。また、このバージョンはユーザベースセキュリティモデル (USM) とビューベースアクセスコントロールモデル (VACM) を通して SNMP エージェントと MIB オブジェクトへのアクセスをコ

ントロールします。ASA は、SNMP グループとユーザの作成、およびセキュアな SNMP 通信の転送の認証と暗号化を有効にするために必要なホストの作成もサポートします。

セキュリティモデル

設定上の目的のために、認証とプライバシーのオプションはセキュリティモデルにまとめられます。セキュリティモデルはユーザとグループに適用され、次の3つのタイプに分けられます。

- **NoAuthPriv** : 認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
- **AuthNoPriv** : 認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- **AuthPriv** : 認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

SNMP グループ

SNMP グループはユーザを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティモデルを使用して設定され、SNMP ビューに関連付けられます。SNMP グループ内のユーザは、SNMP グループのセキュリティモデルに一致する必要があります。これらのパラメータは、SNMP グループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティモデルのペアは固有である必要があります。

SNMP ユーザ

SNMP ユーザは、指定されたユーザ名、ユーザが属するグループ、認証パスワード、暗号化パスワード、および使用する認証アルゴリズムと暗号化アルゴリズムを持ちます。認証アルゴリズムのオプションは MD5 と SHA です。暗号化アルゴリズムのオプションは DES、3DES、および AES (128、192、および 256 バージョンで使用可能) です。ユーザを作成した場合は、それを SNMP グループに関連付ける必要があります。その後、そのユーザはグループのセキュリティモデルを継承します。

SNMP ホスト

SNMP ホストは SNMP 通知とトラップの送信先となる IP アドレスです。トラップは設定されたユーザだけに送信されるため、ターゲット IP アドレスとともに SNMP バージョン 3 のホストを設定するには、ユーザ名を設定する必要があります。SNMP ターゲット IP アドレスとターゲットパラメータ名は ASA で一意である必要があります。各 SNMP ホストはそれぞれに関連付けられているユーザ名を1つだけ持つことができます。SNMP トラップを受信するには、SNMP NMS を設定し、NMS のユーザクレデンシャルが ASA のクレデンシャルと一致するように設定してください。

ASA と Cisco IOS ソフトウェアの実装の相違点

ASA での SNMP バージョン 3 の実装は、Cisco IOS ソフトウェアでの SNMP バージョン 3 の実装とは次の点で異なります。

- ローカル エンジン ID とリモート エンジン ID は設定できません。ローカルエンジン ID は、ASA が起動されたとき、またはコンテキストが作成されたときに生成されます。
- ビューベースのアクセス コントロールに対するサポートはないため、結果として MIB のブラウジングは無制限になります。
- サポートは、USM、VACM、FRAMEWORK、および TARGET という MIB に制限されません。
- 正しいセキュリティ モデルを使用してユーザとグループを作成する必要があります。
- 正しい順序でユーザ、グループ、およびホストを削除する必要があります。
- `snmp-server host` コマンドを使用すると、着信 SNMP トラフィックを許可する ASA ルールが作成されます。

SNMP syslog メッセージ

SNMP では、`212nnn` という番号が付いた詳細な syslog メッセージが生成されます。syslog メッセージは、ASA または ASASM から、SNMP 要求、SNMP トラップ、SNMP チャンネルのステータスを、指定のインターフェイスの指定のホストに表示します。

syslog メッセージの詳細については、『[syslog メッセージガイド](#)』を参照してください。



(注) SNMP syslog メッセージがレート制限（毎秒約 4000）を超えた場合、SNMP ポーリングは失敗します。

アプリケーション サービスとサードパーティ ツール

SNMP サポートについては、次の URL を参照してください。

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP バージョン 3 MIB をウォークするためのサードパーティ ツールの使い方については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP のガイドライン

この項では、SNMPを設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

フェールオーバーのガイドライン

各 ASA の SNMP クライアントはそれぞれのピアとエンジン データを共有します。エンジン データには、SNMP-FRAMEWORK-MIB の engineID、engineBoots、および engineTime オブジェクトが含まれます。エンジン データは `flash:/snmp/contextname` にバイナリ ファイルとして書き込まれます。

その他のガイドライン

- SNMP トラップを受信するか MIB をブラウズするには、CiscoWorks for Windows か別の SNMP MIB-II 互換ブラウザを持っている必要があります。
- ビューベースのアクセス コントロールはサポートされませんが、ブラウジングに VACM MIB を使用してデフォルトのビュー設定を決定できます。
- ENTITY-MIB は管理外コンテキストでは使用できません。代わりに IF-MIB を使用して、管理外コンテキストでクエリーを実行します。
- ENTITY-MIB は Firepower 9300 では使用できません。代わりに、CISCO-FIREPOWER-EQUIPMENT-MIB および CISCO-FIREPOWER-SM-MIB を使用します。
- AIP SSM または AIP SSC では、SNMP バージョン 3 はサポートされません。
- SNMP デバッグはサポートされません。
- ARP 情報の取得はサポートされません。
- SNMP SET コマンドはサポートされません。
- NET-SNMP バージョン 5.4.2.1 を使用する場合、暗号化アルゴリズム バージョン AES128 だけがサポートされます。暗号化アルゴリズム バージョンの AES256 または AES192 はサポートされません。
- 結果として SNMP 機能の整合性が取れない状態になる場合、既存の設定への変更は拒否されます。
- SNMP バージョン 3 の設定は、グループ、ユーザ、ホストの順に行う必要があります。
- グループを削除する前に、そのグループに関連付けられているすべてのユーザが削除されていることを確認する必要があります。
- ユーザを削除する前に、そのユーザ名に関連付けられているホストが設定されていないことを確認する必要があります。

- 特定のセキュリティモデルを使用して特定のグループに属するようにユーザが設定されている場合にそのグループのセキュリティレベルを変更する場合は、次の順に操作を実行する必要があります。
 - そのグループからユーザを削除します。
 - グループのセキュリティレベルを変更します。
 - 新しいグループに属するユーザを追加します。
- MIB オブジェクトのサブセットへのユーザアクセスを制限するためのカスタムビューの作成はサポートされていません。
- すべての要求とトラップは、デフォルトの読み取り/通知ビューだけで使用できます。
- `connection-limit-reached` トラップは管理コンテキストで生成されます。このトラップを生成するには、接続制限に達したユーザ コンテキストで設定された SNMP サーバ ホストが少なくとも 1 つ必要です。
- ASA 5585 SSP-40 (NPE) のシャーシ温度を問い合わせることはできません。
- NMS が正常にオブジェクトを要求できない場合、または ASA からの着信トラップを適切に処理していない場合は、パケットキャプチャの実行が問題を判別する最も有効な方法となります。[Wizards]>[Packet Capture Wizard]を選択して、画面に表示される指示に従います。
- 最大 4000 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。
- サポートされるアクティブなポーリング先の総数は 128 個です。
- ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。
- 1 つのホストに複数のユーザを関連付けることができます。
- ネットワーク オブジェクトは、別の `host-group` コマンドと重複して指定することができます。異なるネットワーク オブジェクトの共通のホストに対しては、最後のホストグループに指定した値が適用されます。
- ホスト グループや他のホスト グループと重複するホストを削除すると、設定済みのホストグループで指定されている値を使用してホストが再設定されます。
- ホストで取得される値は、コマンドの実行に使用するよう指定したシーケンスによって異なります。
- SNMP で送信できるメッセージのサイズは 1472 バイトまでです。
- SNMPv3 エンジン ID はクラスタのメンバー間で同期されません。そのため、SNMPv3 については、クラスタの各ユニットでそれぞれ設定する必要があります。

- バージョン9.4(1)では、ASAがサポートするコンテキストあたりのSNMPサーバのトラップホスト数に制限はありません。show snmp-server host コマンドの出力にはASAをポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。

SNMP を設定します。

ここでは、SNMP の設定方法について説明します。

手順

- ステップ1 ASA から要求を受信するように SNMP 管理ステーションを設定します。
- ステップ2 SNMP トラップを設定します。
- ステップ3 SNMP バージョン 1 および 2c のパラメータまたは SNMP バージョン 3 のパラメータを設定します。

SNMP 管理ステーションの設定

SNMP 管理ステーションを設定するには、次の手順を実行します。

手順

- ステップ1 **[Configuration] > [Device Management] > [Management Access] > [SNMP]** の順に選択します。デフォルトでは、SNMP サーバはイネーブルになっています。
- ステップ2 **[SNMP Management Stations]** ペインで **[Add]** をクリックします。
[Add SNMP Host Access Entry] ダイアログボックスが表示されます。
- ステップ3 SNMP ホストが存在するインターフェイスを選択します。
- ステップ4 SNMP ホストの IP アドレスを入力します。
- ステップ5 SNMP ホストの UDP ポートを入力します。デフォルトのポート 162 をそのまま使用することもできます。
- ステップ6 SNMP ホストのコミュニティストリングを追加します。管理ステーションに対してコミュニティストリングが指定されていない場合は、**[SNMP Management Stations]** ペインの **[Community String (default)]** フィールドに設定されている値が使用されます。
- ステップ7 SNMP ホストで使用される SNMP のバージョンを選択します。
- ステップ8 前の手順で SNMP バージョン 3 を選択した場合は、設定済みユーザの名前を選択します。
- ステップ9 **[Poll]** チェックボックスまたは **[Trap]** チェックボックスのいずれかをオンにして、NMS との通信に使用する方式を指定します。
- ステップ10 **[OK]** をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

NMS が設定され、その変更内容が実行コンフィギュレーションに保存されます。SNMP バージョン 3 の NMS ツールの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_tools.html

Configure SNMP Traps

SNMP エージェントが生成するトラップ、およびそのトラップを収集し、NMS に送信する方法を指定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Management Access] > [SNMP] の順に選択します。

ステップ 2 [Configure Traps] をクリックします。

[SNMP Trap Configuration] ダイアログボックスが表示されます。

ステップ 3 [SNMP Server Traps Configuration] チェックボックスをオンにします。

トラップは、[standard]、[IKEv2]、[entity MIB]、[IPsec]、[remote access]、[resource]、[NAT]、[syslog]、[CPU utilization]、[CPU utilization and monitoring interval]、および [SNMP interface threshold and interval] のカテゴリに分類されます。SNMP トラップを介して通知を発行するための SNMP イベントを指定するため、目的のチェックボックスをオンにします。デフォルトの設定では、すべての SNMP 標準トラップがイネーブルです。トラップタイプを指定しない場合、デフォルトで **syslog** トラップに設定されます。デフォルトの SNMP トラップは、**syslog** トラップとともにイネーブルの状態を続けます。デフォルトでは他のトラップはすべてディセーブルです。トラップをディセーブルにするには、該当するチェックボックスをオフにします。**syslog** トラップの重大度レベルを設定するには、[Configuration] > [Device Management] > [Logging] > [Logging Filters] の順に選択します。

ステップ 4 [OK] をクリックして、[SNMP Trap Configuration] ダイアログボックスを閉じます。

ステップ 5 [Apply] をクリックします。

SNMP トラップが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP バージョン 1 または 2c のパラメータの設定

SNMP バージョン 1 または 2c のパラメータを設定するには、次の手順を実行します。

手順

-
- ステップ1** [Configuration] > [Device Management] > [Management Access] > [SNMP] の順に選択します。
- ステップ2** SNMPバージョン1または2cを使用する場合は、[Community String (default)] フィールドにデフォルトのコミュニティストリングを入力します。要求をASAに送信するときにSNMP NMSで使用されるパスワードを入力します。SNMPコミュニティストリングは、SNMP NMSと管理対象のネットワークノード間の共有秘密です。ASAでは、着信SNMP要求が有効かどうかを判断するためにパスワードが使用されます。パスワードは、大文字と小文字が区別される、最大32文字の英数字です。スペースは使用できません。デフォルトはpublicです。SNMPバージョン2cでは、NMSごとに、別々のコミュニティストリングを設定できます。コミュニティストリングがどのNMSにも設定されていない場合、ここで設定した値がデフォルトとして使用されます。
- ステップ3** ASAシステム管理者の名前を入力します。テキストは、大文字と小文字が区別される、最大127文字の英数字です。スペースを使用できますが、複数のスペースを入力しても1つのスペースになります。
- ステップ4** SNMPで管理しているASAの場所を入力します。テキストは、大文字と小文字が区別され、最大127文字です。スペースを使用できますが、複数のスペースを入力しても1つのスペースになります。
- ステップ5** NMSからのSNMP要求をリッスンするASAポートの番号を入力します。デフォルトのポート番号161をそのまま使用することもできます。
- ステップ6** [SNMP Host Access List] ペインで[Add]をクリックします。
[Add SNMP Host Access Entry] ダイアログボックスが表示されます。
- ステップ7** トラップの送信元となるインターフェイスの名前をドロップダウンリストから選択します。
- ステップ8** ASAに接続できるNMSまたはSNMPマネージャのIPアドレスを入力します。
- ステップ9** UDPのポート番号を入力します。デフォルトは162です。
- ステップ10** 使用するSNMPのバージョンをドロップダウンリストから選択します。バージョン1または2cを選択した場合は、コミュニティストリングを入力する必要があります。バージョン3を選択した場合は、ドロップダウンリストからユーザ名を選択する必要があります。
- ステップ11** 要求の送信（ポーリング）だけにNMSを制限する場合は、[Server Poll/Trap Specification] 領域の[Poll]チェックボックスをオンにします。トラップの受信だけにNMSを制限する場合は、[Trap]チェックボックスをオンにします。両方のチェックボックスをオンにすると、SNMPホストの両方の機能が実行されます。
- ステップ12** [OK]をクリックして、[Add SNMP Host Access Entry] ダイアログボックスを閉じます。
新しいホストが[SNMP Host Access List] ペインに表示されます。
- ステップ13** Applyをクリックします。
SNMPバージョン1、2c、または3のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。
-

SNMP バージョン 3 のパラメータの設定

SNMP バージョン 3 のパラメータを設定するには、次の手順を実行します。

手順

- ステップ 1** [Configuration] > [Device Management] > [Management Access] > [SNMP] の順に選択します。
- ステップ 2** [SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで [Add] > [SNMP User] の順にクリックして、設定済みのユーザまたは新規ユーザをグループに追加します。グループ内に残る最後のユーザを削除すると、そのグループは ASDM により削除されます。
- (注) ユーザが作成された後は、そのユーザが属するグループは変更できません。
- [Add SNMP User Entry] ダイアログボックスが表示されます。
- ステップ 3** SNMP ユーザが属するグループを選択します。選択できるグループは次のとおりです。
- [Auth&Encryption] : このグループに属するユーザには、認証と暗号化が設定されます。
 - [Authentication_Only] : このグループに属するユーザには、認証だけ設定されます。
 - [No_Authentication] : このグループに属するユーザには、認証も暗号化も設定されません。
- (注) グループ名は変更できません。
- ステップ 4** ユーザセキュリティ モデル (USM) グループを使用する場合は、[USM Model] タブをクリックします。
- ステップ 5** [Add] をクリックします。
- [Add SNMP USM Entry] ダイアログボックスが表示されます。
- ステップ 6** グループ名を入力します。
- ステップ 7** ドロップダウンリストからセキュリティレベルを選択します。設定済みの USM グループをセキュリティ レベルとして SNMPv3 ユーザに割り当てることができます。
- ステップ 8** 設定済みユーザまたは新規ユーザの名前を入力します。ユーザ名は、選択した SNMP サーバグループ内で一意であることが必要です。
- ステップ 9** [Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。
- ステップ 10** [MD5] と [SHA] のいずれかのオプション ボタンをクリックして、使用する認証のタイプを指定します。
- ステップ 11** 認証に使用するパスワードを入力します。
- ステップ 12** [DES]、[3DES]、[AES] の中からいずれかのオプション ボタンをクリックして、使用する暗号化のタイプを指定します。
- ステップ 13** AES 暗号化を選択した場合は、使用する AES 暗号化のレベルとして、128、192、256 のいずれかを選択します。

- ステップ 14** 暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大64文字です。
- ステップ 15** [OK] をクリックすると、グループが作成され（指定したユーザがそのグループに属する最初のユーザである場合）、[Group Name] ドロップダウンリストにそのグループが表示されます。またそのグループ内にユーザが作成されます。
- [Add SNMP User Entry] ダイアログボックスが閉じます。
- ステップ 16** [Apply] をクリックします。
- SNMP バージョン3のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

ユーザのグループの設定

指定したユーザのグループからなる SNMP ユーザ リストを設定するには、次の手順を実行します。

手順

- ステップ 1** [Configuration] > [Device Management] > [Management Access] > [SNMP] の順に選択します。
- ステップ 2** [SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで [Add] > [SNMP User Group] の順にクリックし、設定済みのユーザ グループまたは新規ユーザ グループを追加します。グループ内に残る最後のユーザを削除すると、そのグループは ASDM により削除されます。
- [Add SNMP User Group] ダイアログボックスが表示されます。
- ステップ 3** ユーザ グループ名を入力します。
- ステップ 4** 既存のユーザまたはユーザ グループを選択する場合は、[Existing User/User Group] オプション ボタンをクリックします。
- ステップ 5** 新規ユーザを作成する場合は、[Create new user] オプション ボタンをクリックします。
- ステップ 6** SNMP ユーザが属するグループを選択します。選択できるグループは次のとおりです。
- [Auth&Encryption] : このグループに属するユーザには、認証と暗号化が設定されます。
 - [Authentication_Only] : このグループに属するユーザには、認証だけ設定されます。
 - [No_Authentication] : このグループに属するユーザには、認証も暗号化も設定されません。
- ステップ 7** 設定済みユーザまたは新規ユーザの名前を入力します。ユーザ名は、選択した SNMP サーバグループ内で一意であることが必要です。
- ステップ 8** [Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。
- ステップ 9** [MD5] と [SHA] のいずれかのオプション ボタンをクリックして、使用する認証のタイプを指定します。

- ステップ 10** 認証に使用するパスワードを入力します。
- ステップ 11** 認証に使用するパスワードを確認のためにもう一度入力します。
- ステップ 12** [DES]、[3DES]、[AES] の中からいずれかのオプション ボタンをクリックして、使用する暗号化のタイプを指定します。
- ステップ 13** 暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大 64 文字です。
- ステップ 14** 暗号化に使用するパスワードを確認のためにもう一度入力します。
- ステップ 15** [Members in Group] ペインの指定したユーザ グループに新規ユーザを追加するには、[Add] をクリックします。[Members in Group] ペインから既存のユーザを削除するには、[Remove] をクリックします。
- ステップ 16** [OK] をクリックすると、指定したユーザ グループに新規ユーザが作成されます。
[Add SNMP User Group] ダイアログボックスが閉じます。
- ステップ 17** [Apply] をクリックします。
SNMP バージョン 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP モニタリング

次の SNMP モニタリング用のコマンドを参照してください。[Tools] > [Command Line Interface] を使用して次のコマンドを入力できます。

- **show running-config snmp-server [default]**
すべての SNMP サーバのコンフィギュレーション情報を表示します。
- **show running-config snmp-server group**
SNMP グループのコンフィギュレーション設定を表示します。
- **show running-config snmp-server host**
リモート ホストに送信されるメッセージと通知を制御するために SNMP によって使用されているコンフィギュレーション設定を表示します。
- **show running-config snmp-server host-group**
SNMP ホスト グループのコンフィギュレーションを表示します。
- **show running-config snmp-server user**
SNMP ユーザベースのコンフィギュレーション設定を表示します。
- **show running-config snmp-server user-list**
SNMP ユーザ リストのコンフィギュレーションを表示します。
- **show snmp-server engineid**
設定されている SNMP エンジンの ID を表示します。

• **show snmp-server group**

設定されている SNMP グループの名前を表示します。コミュニティ スtring がすでに設定されている場合、デフォルトでは2つの別のグループが出力に表示されます。この動作は通常のものであります。

• **show snmp-server statistics**

SNMP サーバの設定済み特性を表示します。すべての SNMP カウンタをゼロにリセットするには、**clear snmp-server statistics** コマンドを使用します。

• **show snmp-server user**

ユーザの設定済み特性を表示します。

SNMP の履歴

表 51 : SNMP の履歴

機能名	バージョン	説明
SNMP バージョン 1 および 2c	7.0(1)	クリア テキスト コミュニティ スtring を使用した SNMP サーバと SNMP エージェント間のデータ送信によって、ASA ネットワーク モニタリング と イベント情報を提供します。 次の画面が変更されました。[Configuration]>[Device Management]>[Management Access]>[SNMP]。
SNMP バージョン 3	8.2(1)	3DES または AES 暗号化、およびサポートされているセキュリティ モデルの中で最もセキュアな形式である SNMP バージョン 3 のサポートを提供します。このバージョンでは、USM を使用して、ユーザ、グループ、ホスト、および認証の特性を設定できます。さらに、このバージョンでは、エージェントと MIB オブジェクトへのアクセス コントロールが許可され、追加の MIB サポートが含まれます。 次の画面が変更されました。[Configuration]>[Device Management]>[Management Access]>[SNMP]。
パスワードの暗号化	8.3(1)	パスワードの暗号化がサポートされます。

機能名	バージョン	説明
SNMP トラップと MIB	8.4(1)	<p>追加のキーワードとして、connection-limit-reached、cpu threshold rising、entity cpu-temperature、entity fan-failure、entity power-supply、ikev2 stop start、interface-threshold、memory-threshold、nat packet-discard、warmstart をサポートします。</p> <p>entPhysicalTable によって、センサー、ファン、電源、および関連コンポーネントのエントリがレポートされます。</p> <p>追加の MIB として、CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、DISMAN-EVENT-MIB、DISMAN-EXPRESSION-MIB、ENTITY-SENSOR-MIB、NAT-MIB をサポートします。</p> <p>さらに ceSensorExtThresholdNotification、clrResourceLimitReached、cpmCPURisingThreshold、mteTriggerFired、natPacketDiscard、warmStart トラップをサポートしています。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。</p>
IF-MIB ifAlias OID のサポート	8.5(1)	<p>ASA は、ifAlias OID をサポートするようになりました。IF-MIB をブラウズする際、fAlias OID はインターフェイスの記述に設定済みの値に設定されます。</p>
ASA サービス モジュール (ASASM)	8.5(1)	<p>ASASM は、次を除く 8.4(1) にあるすべての MIB およびトラップをサポートします。</p> <p>8.5(1) のサポートされていない MIB :</p> <ul style="list-style-type: none"> • CISCO-ENTITY-SENSOR-EXT-MIB (entPhySensorTable グループのオブジェクトだけがサポートされます)。 • ENTITY-SENSOR-MIB (entPhySensorTable グループのオブジェクトだけがサポートされます)。 • DISMAN-EXPRESSION-MIB (expExpressionTable、expObjectTable、および expValueTable グループのオブジェクトだけがサポートされます)。 <p>8.5(1) のサポートされていないトラップ :</p> <ul style="list-style-type: none"> • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)。このトラップは、電源障害、ファン障害および高 CPU 温度のイベントだけに使用されません。 • InterfacesBandwidthUtilization。

機能名	バージョン	説明
SNMP トラップ	8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の追加のキーワードとして、 entity power-supply-presence 、 entity power-supply-failure 、 entity chassis-temperature 、 entity chassis-fan-failure 、 entity power-supply-temperature をサポートします。 次のコマンドが変更されました。 snmp-server enable traps 。
VPN-related MIB	9.0(1)	CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB の更新バージョンが、次世代の暗号化機能をサポートするために実装されました。 ASASM では、次の MIB が有効になりました。 <ul style="list-style-type: none"> • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	CISCO-TRUSTSEC-SXP-MIB のサポートが追加されました。
SNMP OID	9.1(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために 5 つの新しい SNMP 物理ベンダー タイプ OID が追加されました。
NAT MIB	9.1(2)	cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID が、xlate_count および max_xlate_count エントリをサポートするようになりました。これは、 show xlate count コマンドを使用したポーリングの許可と同等です。
SNMP のホスト、ホストグループ、ユーザリスト	9.1(5)	最大 4000 個までホストを追加できるようになりました。サポートされるアクティブなポーリング先の数は 128 個です。ホストグループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。1 つのホストに複数のユーザを関連付けることができます。 次の画面が変更されました。 [Configuration]>[Device Management]>[Management Access]> [SNMP]。
SNMP メッセージのサイズ	9.2(1)	SNMP で送信できるメッセージのサイズが 1472 バイトまでに増えました。

機能名	バージョン	説明
SNMP の MIB および OID	9.2(1)	<p>ASA は、cpmCPUTotal5minRev OID をサポートするようになりました。</p> <p>SNMP の sysObjectID OID および entPhysicalVendorType OID に、新しい製品として ASA v が追加されました。</p> <p>新しい ASA v プラットフォームをサポートするよう、CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。</p> <p>VPN 共有ライセンスの使用状況をモニタするための新しい SNMP MIB が追加されました。</p>
SNMP の MIB および OID	9.3(1)	<p>ASASM 用に CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) のサポートが追加されました。</p>
SNMP の MIB およびトラップ	9.3(2)	<p>ASA 5506-X をサポートするよう、CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。</p> <p>SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506-X が追加されました。</p> <p>ASA で CISCO-CONFIG-MAN-MIB がサポートされるようになりました。以下が可能です。</p> <ul style="list-style-type: none"> • 特定のコンフィギュレーションについて入力されたコマンドを確認する。 • 実行コンフィギュレーションに変更が発生したときに NMS に通知する。 • 実行コンフィギュレーションが最後に変更または保存されたときのタイムスタンプを追跡する。 • 端末の詳細やコマンドのソースなど、コマンドに対するその他の変更を追跡する。 <p>次の画面が変更されました。[Configuration]>[Device Management]>[Management Access]>[SNMP]>[Configure Traps]>[SNMP Trap Configuration]。</p>
SNMP の MIB およびトラップ	9.4(1)	<p>SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506W-X、ASA 5506H-X、ASA 5508-X、および ASA 5516-X が追加されました。</p>
コンテキストごとに無制限の SNMP サーバトラップホスト	9.4(1)	<p>ASA は、コンテキストごとに無制限の SNMP サーバトラップホストをサポートします。show snmp-server host コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。</p> <p>変更された ASDM 画面はありません。</p>

機能名	バージョン	説明
ISA 3000 のサポートが追加されました。	94(1225)	<p>ISA 3000 製品ファミリーで SNMP がサポートされました。このプラットフォームに新しい OID が追加されました。 snmp-server enable traps entity コマンドが変更され、新しい変数 <i>II-bypass-status</i> が追加されました。これにより、ハードウェアのバイパス状態の変更が可能になりました。</p> <p>変更された ASDM 画面はありません。</p>
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	9.6(1)	<p>CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプール モニタリング エントリのテーブルです。</p> <p>(注) CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4GB 以上のメモリのレポートをサポートします。</p>
Precision Time Protocol (PTP) の E2E トランスペアレントクロックモード MIB のサポート	9.7(1)	<p>E2E トランスペアレント クロック モードに対応する MIB がサポートされます。</p> <p>(注) SNMP の bulkget、getnext、walk 機能のみがサポートされています。</p>
SNMP over IPv6	9.9(2)	<p>ASA は、IPv6 経由での SNMP サーバとの通信、IPv6 経由でのクエリとトラップの実行許可、既存の MIB に対する IPv6 アドレスのサポートなど、SNMP over IPv6 をサポートするようになりました。RFC 8096 で説明されているように、次の新しい SNMP IPv6 MIB オブジェクトが追加されました。</p> <ul style="list-style-type: none"> • ipv6InterfaceTable (OID : 1.3.6.1.2.1.4.30) : インターフェイスごとの IPv6 固有の情報が含まれています。 • ipAddressPrefixTable (OID : 1.3.6.1.2.1.4.32) : このエンティティによって学習されたすべてのプレフィックスが含まれています。 • ipAddressTable (OID : 1.3.6.1.2.1.4.34) : エンティティのインターフェイスに関連するアドレッシング情報が含まれています。 • ipNetToPhysicalTable (OID : 1.3.6.1.2.1.4.35) : IP アドレスから物理アドレスへのマッピングが含まれています。 <p>新規または変更された画面 : [Configuration] > [Device Management] > [Management Access] > [SNMP]</p>
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.10(1)	<p>CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。</p> <p>変更された ASDM 画面はありません。</p>

機能名	バージョン	説明
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.12(1)	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規または変更された画面： [Configuration] > [Device Management] > [Management Access] > [SNMP]



第 42 章

Anonymous Reporting および Smart Call Home

この章では、Anonymous Reporting および Smart Call Home サービスを設定する方法について説明します。

- [Anonymous Reporting について](#) (1051 ページ)
- [Smart Call Home の概要](#) (1052 ページ)
- [Anonymous Reporting および Smart Call Home のガイドライン](#) (1053 ページ)
- [Anonymous Reporting および Smart Call Home の設定](#) (1054 ページ)
- [Anonymous Reporting および Smart Call Home のモニタリング](#) (1059 ページ)
- [Anonymous Reporting および Smart Call Home の履歴](#) (1060 ページ)

Anonymous Reporting について

Anonymous Reporting をイネーブルにして、Cisco ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。この機能をイネーブルにした場合、お客様のアイデンティティは匿名のままとなり、識別情報は送信されません。

Anonymous Reporting をイネーブルにすると、トラストポイントが作成され、証明書がインストールされます。CA 証明書は、ASA でメッセージを安全に送信できるように、Smart Call Home Web サーバ上のサーバ証明書を検証して、HTTPS セッションを形成するために必要です。ソフトウェアに事前定義済みの証明書が、シスコによってインポートされます。Anonymous Reporting をイネーブルにする場合は、ハードコードされたトラストポイント名の `_SmartCallHome_ServerCA` で証明書が ASA にインストールされます。Anonymous Reporting をイネーブルにすると、このトラストポイントが作成され、適切な証明書がインストールされて、このアクションに関するメッセージが表示されます。これで、証明書が設定の中に存在するようになります。

Anonymous Reporting をイネーブルにしたときに、適切な証明書がすでに設定に存在する場合、トラストポイントは作成されず、証明書はインストールされません。



- (注) Anonymous Reporting をイネーブルにすると、指定されたデータをシスコまたはシスコの代わりに運用するベンダー（米国以外の国を含む）に転送することに同意することになります。シスコでは、すべてのお客様のプライバシーを保護しています。シスコの個人情報の取り扱いに関する詳細については、次の URL にあるシスコのプライバシー声明を参照してください。
<http://www.cisco.com/web/siteassets/legal/privacy.html>

DNS 要件

ASA が Cisco Smart Call Home サーバに到達してシスコにメッセージを送信できるように DNS サーバを正しく設定する必要があります。ASA をプライベートネットワークに配置し、パブリックネットワークにはアクセスできないようにすることが可能なため、シスコでは DNS 設定を検証し、必要な場合には次の手順を実行して、ユーザの代わりにこれを設定します。

1. 設定されているすべての DNS サーバに対して DNS ルックアップを実行します。
2. 最もセキュリティレベルの高いインターフェイスで DHCPINFORM メッセージを送信して、DHCP サーバから DNS サーバを取得します。
3. ルックアップにシスコの DNS サーバを使用します。
4. tools.cisco.com に対してランダムに静的 IP アドレスを使用します。

これらの作業は、現在の設定を変更せずに実行されます。（たとえば、DHCPから学習された DNS サーバは設定には追加されません）。

設定されている DNS サーバがなく、ASA が Cisco Smart Call Home サーバに到達できない場合は、各 Smart Call Home メッセージに対して、重大度「warning」の syslog メッセージが生成されます。これは、DNS を適切に設定するようお願いするためです。

syslog メッセージについては、『syslog メッセージガイド』を参照してください。

Smart Call Home の概要

完全に設定が終わると、Smart Call Home は設置場所での問題を検出し、多くの場合はそのような問題があることにユーザが気付く前に、シスコにレポートを返すか、別のユーザ定義のチャネル（ユーザ宛の電子メールまたはユーザに直接など）を使用してレポートを返します。シスコでは、これらの問題の重大度に応じて次のサービスを提供することにより、システムコンフィギュレーションの問題、製品ライフサイクル終了通知の発表、セキュリティ警告問題などに対応します。

- 継続的モニタリング、リアルタイムの予防的なアラート、および詳細な診断により、問題を迅速に識別する。
- サービス要求が開かれ、すべての診断データが添付された Smart Call Home 通知を使用して、潜在的な問題をユーザに認識させる。

- Cisco TAC の専門家に自動的に直接アクセスすることにより、重大な問題を迅速に解決する。
- トラブルシューティングに必要な時間を短縮することにより、スタッフリソースを効率よく使用する。
- Cisco TAC へのサービス リクエストを自動的に生成し（サービス契約がある場合）、適切なサポート チームに提出する。問題解決の時間を短縮する、詳細な診断情報を提供します。

Smart Call Home ポータルを使用すると必要な情報に迅速にアクセスできるため、以下の事項が実現されます。

- すべての Smart Call Home メッセージ、診断、および推奨事項を一箇所で確認する。
- サービス リクエスト ステータスを確認する。
- すべての Smart Call Home 対応デバイスに関する最新のインベントリ情報およびコンフィギュレーション情報を表示する。

Anonymous Reporting および Smart Call Home のガイドライン

この項では、Anonymous Reporting と Smart Call Home を設定する前に考慮する必要があるガイドラインおよび制限事項について説明します。

Anonymous Reporting のガイドライン

- DNS が設定されていること。
- Anonymous Reporting のメッセージを最初の試行で送信できなかった場合、ASA はメッセージをドロップする前にさらに 2 回試行します。
- Anonymous Reporting は、既存の設定を変更せずに、他の Smart Call Home 設定と共存させることができます。たとえば、Anonymous Reporting をイネーブルにする前に Smart Call Home がディセーブルになっている場合、Anonymous Reporting をイネーブルにした後でも、ディセーブルのままです。
- Anonymous Reporting をイネーブルにしている場合、トラスト ポイントを削除することはできません。また、Anonymous Reporting をディセーブルにした場合、トラスト ポイントはそのまま残ります。Anonymous Reporting がディセーブルの場合は、トラスト ポイントを削除できますが、Anonymous Reporting をディセーブルにしてもトラスト ポイントは削除されません。
- マルチ コンテキスト モード設定を使用している場合は、**dns**、**interface**、**trustpoint** コマンドは管理コンテキストにあり、**call-home** コマンドはシステムコンテキストにあります。
-

Smart Call Home のガイドライン

- マルチ コンテキスト モードでは、`subscribe-to-alert-group snapshot periodic` コマンドは、システム コンフィギュレーションから情報を取得するコマンドと、ユーザ コンテキストから情報を取得するコマンドの2つのコマンドに分割されます。
- Smart Call Home のバックエンドサーバは、XML 書式のメッセージのみ受け取ることができます。
- Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタ イベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次のイベントに対してのみ送信されます。
 - ユニットがクラスタに参加したとき
 - ユニットがクラスタから脱退したとき
 - クラスタ ユニットがクラスタ マスターになったとき
 - クラスタのセカンダリ ユニットが故障したとき

送信される各メッセージには次の情報が含まれています。

- アクティブ クラスタのメンバ数
- クラスタ マスターでの `show cluster info` コマンドおよび `show cluster history` コマンドの出力

Anonymous Reporting および Smart Call Home の設定

Anonymous Reporting は Smart Call Home サービスの一部であり、これを使用すると、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに匿名で送信できます。一方、Smart Call Home サービスは、システム ヘルスのサポートをカスタマイズする機能です。Cisco TAC がお客様のデバイスをモニタして、問題があるときにケースを開くことができるようになります。多くの場合は、お客様がその問題に気付く前に発見できます。

両方のサービスをシステム上で同時に設定できますが、Smart Call Home サービスを設定すれば、Anonymous Reporting と同じ機能に加えて、カスタマイズされたサービスも使用できるようになります。

Anonymous Reporting の設定

Anonymous Reporting を設定するには、次の手順を実行します。

手順

-
- ステップ 1** [Configuration] > [Device Management] > [Smart Call Home] の順に選択します。
- ステップ 2** [Enable Anonymous Reporting] チェックボックスをオンにします。
- ステップ 3** [Test Connection] をクリックして、システムでメッセージを送信できることを確認します。
ASDM は成功メッセージまたはエラーメッセージを返して、テスト結果を通知します。
- ステップ 4** [Apply] をクリックして設定を保存し、Anonymous Reporting をイネーブルにします。
-

Smart Call Home の設定

Smart Call Home サービス、システムセットアップ、およびアラートサブスクリプションプロファイルを設定するには、次の手順を実行します。

手順

-
- ステップ 1** [Configuration] > [Device Management] > [Smart Call Home] の順に選択します。
- ステップ 2** [Enable Registered Smart Call Home] チェックボックスをオンにして、Smart Call Home をイネーブルにし、ASA を Cisco TAC に登録します。
- ステップ 3** [Advanced System Setup] をダブルクリックします。この領域は、3 個のペインで構成されています。各ペインは、タイトル行をダブルクリックすると展開または縮小できます。
- [Mail Servers] ペインで、Smart Call Home メッセージを電子メールのサブスクライバに配信する際に通過するメールサーバを設定できます。
 - ASA の [Contact Information] ペインで、Smart Call Home メッセージに表示される担当者の個人情報を入力できます。このペインには、次の情報が含まれます。
 - 連絡先担当者の名前。
 - 連絡先の電話番号。
 - 連絡先担当者の住所。
 - 連絡先の電子メールアドレス。
 - Smart Call Home 電子メールの「from」電子メールアドレス。
 - Smart Call Home 電子メールの「reply-to」電子メールアドレス。
 - カスタマー ID。
 - サイト ID。
 - 連絡先 ID。

- c) [Alert Control] ペインで、アラートの制御パラメータを調整できます。このペインには、[Alert Group Status] ペインが含まれ、ここには次のアラートグループのステータス（イネーブルまたはディセーブル）がリストされます。
- 診断アラート グループ。
 - コンフィギュレーション アラート グループ。
 - 環境アラート グループ。
 - インベントリ アラート グループ。
 - スナップショット アラート グループ。
 - syslog アラート グループ。
 - テレメトリ アラート グループ。
 - 脅威アラート グループ。
 - 1 分間に処理される Smart Call Home メッセージの最大数。
 - Smart Call Home 電子メールの「from」電子メールアドレス。

ステップ 4 [Alert Subscription Profiles] をダブルクリックします。指定した各サブスクリプションプロファイルによって、サブスクライバおよび対象とするアラート グループが特定されます。

- a) [Add] または [Edit] をクリックして、**サブスクリプション プロファイル エディタ**を表示します。ここでは、新規サブスクリプションプロファイルを作成したり、既存のサブスクリプションプロファイルを編集したりできます。
- b) [Delete] をクリックして、選択したプロファイルを削除します。
- c) [Active] チェックボックスをオンにして、選択されたサブスクリプションプロファイルの Smart Call Home メッセージをサブスクライバに送信します。

ステップ 5 [Add] または [Edit] をクリックして、[Add Alert Subscription Profile] ダイアログボックスまたは [Edit Alert Subscription Profile] ダイアログボックスを表示します。

- a) [Name] フィールドは読み取り専用であり、編集できません。
- b) [Enable this subscription profile] チェックボックスをオンにして、この特定のプロファイルをイネーブルまたはディセーブルにします。
- c) [Alert Delivery Method] 領域で、[HTTP] または [Email] オプション ボタンのいずれかをクリックします。
- d) [Subscribers] フィールドに電子メールアドレスまたは Web アドレスを入力します。

ステップ 6 [Alert Dispatch] 領域では、管理者が、サブスクライバに送信する Smart Call Home 情報の種類と送信の条件を指定できます。時間ベースとイベントベースの 2 種類のアラートがあり、アラートのトリガー方法に応じて選択します。コンフィギュレーション、インベントリ、スナップショット、およびテレメトリの各アラートグループは時間ベースです。診断、環境、Syslog、および脅威の各アラート グループはイベントベースです。

ステップ 7 [Message Parameters] 領域では、優先されるメッセージ形式や最大メッセージサイズなど、サブスクライバに送信されるメッセージを制御するパラメータを調整できます。

- ステップ 8** 時間ベースのアラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Add Configuration Alert Dispatch Condition] または [Edit Configuration Alert Dispatch Condition] ダイアログボックスを表示します。
- a) [Alert Dispatch Frequency] 領域で、サブスクリイバに情報を送信する頻度を指定します。
- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
 - 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
 - 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
 - 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。
- b) [Basic] または [Detailed] オプション ボタンをクリックして、サブスクリイバに必要な情報のレベルを指定します。
- c) [OK] をクリックしてコンフィギュレーションを保存します。
- ステップ 9** イベントベースの診断、環境、および脅威アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Diagnostic Alert Dispatch Condition] または [Edit Diagnostic Alert Dispatch Condition] ダイアログボックスを表示します。
- ステップ 10** [Event Severity] ドロップダウンリストで、サブスクリイバへのアラートのディスパッチをトリガーするイベントの重大度を指定し、[OK] をクリックします。
- ステップ 11** 時間ベースのインベントリアラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Inventory Alert Dispatch Condition] または [Edit Inventory Alert Dispatch Condition] ダイアログボックスを表示します。
- ステップ 12** [Alert Dispatch Frequency] ドロップダウン リストで、サブスクリイバにアラートをディスパッチする頻度を指定し、[OK] をクリックします。
- ステップ 13** 時間ベースのスナップショットアラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Snapshot Alert Dispatch Condition] または [Edit Snapshot Alert Dispatch Condition] ダイアログボックスを表示します。
- a) [Alert Dispatch Frequency] 領域で、サブスクリイバに情報を送信する頻度を指定します。
- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
 - 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
 - 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。

- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。
- 間隔サブスクリプションの場合、サブスクライバに情報を送信する頻度を分単位で指定します。この要件は、スナップショット アラート グループにのみ適用されます。

b) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 14 イベントベースの syslog アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Syslog Alert Dispatch Condition] または [Edit Syslog Alert Dispatch Condition] ダイアログボックスを表示します。

- a) [Specify the event severity which triggers the dispatch of alert to subscribers] チェックボックスをオンにして、ドロップダウン リストからイベントの重大度を選択します。
- b) [Specify the message IDs of syslogs which trigger the dispatch of alert to subscribers] チェックボックスをオンにします。
- c) 画面の指示に従って、サブスクライバへのアラートのディスパッチをトリガーする syslog メッセージ ID を指定します。
- d) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 15 イベントベースのテレメトリ アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Telemetry Alert Dispatch Condition] または [Edit Telemetry Alert Dispatch Condition] ダイアログボックスを表示します。

- a) [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。
 - 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
 - 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
 - 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
 - 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。

b) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 16 [Test] をクリックして、設定したアラートが正しく動作しているかどうかを判別します。

Anonymous Reporting および Smart Call Home のモニタリング

Anonymous Reporting および Smart Call Home サービスのモニタリングについては、次のコマンドを参照してください。[Tools] > [Command Line Interface]を使用してこのコマンドを入力できます。

- **show call-home detail**

このコマンドは、現在の Smart Call Home の詳細設定を表示します。

- **show call-home mail-server status**

このコマンドは、現在のメール サーバのステータスを表示します。

- **show call-home profile {profile name | all}**

このコマンドは、Smart Call Home プロファイルのコンフィギュレーションを表示します。

- **show call-home registered-module status [all]**

このコマンドは、登録されているモジュールのステータスを表示します。

- **show call-home statistics**

このコマンドは、Call Home の詳細ステータスを表示します。

- **show call-home**

このコマンドは、現在の Smart Call Home のコンフィギュレーションを表示します。

- **show running-config call-home**

このコマンドは、現在の Smart Call Home の実行コンフィギュレーションを表示します。

- **show smart-call-home alert-group**

このコマンドは、Smart Call Home アラート グループの現在のステータスを表示します。

- **show running-config all**

このコマンドは、Anonymous Reporting ユーザ プロファイルに関する詳細を表示します。

Anonymous Reporting および Smart Call Home の履歴

表 52: Anonymous Reporting および Smart Call Home の履歴

機能名	プラットフォーム リリース	説明
Smart Call Home	8.2(2)	<p>Smart Call Home サービスは、ASA に関するプロアクティブ診断およびリアルタイム アラートを提供し、ネットワークの可用性と運用効率を向上させます。</p> <p>次の画面が導入されました。</p> <p>[Configuration] > [Device Management] > [Smart Call Home]。</p>
Anonymous Reporting	9.0(1)	<p>Anonymous Reporting をイネーブルにして、ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Monitoring] > [Smart Call Home]。</p>
Smart Call Home	9.1(2)	<p>テレメトリ アラート グループ レポートのための show local-host コマンドは、show local-host include interface コマンドに変更になりました。</p>

機能名	プラットフォーム リリース	説明
Smart Call Home	9.1(3)	<p>Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラートグループに登録するように Smart Call Home を設定してある場合に、重要なクラスタイベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次の 3 種類のイベントに対してのみ送信されます。</p> <ul style="list-style-type: none"> • ユニットがクラスタに参加したとき • ユニットがクラスタから脱退したとき • クラスタ ユニットがクラスタ マスターになったとき <p>送信される各メッセージには次の情報が含まれています。</p> <ul style="list-style-type: none"> • アクティブ クラスタのメンバ数 • クラスタ マスターでの show cluster info コマンドおよび show cluster history コマンドの出力



第 IX 部

参照先

- [アドレス、プロトコル、およびポート \(1065 ページ\)](#)



第 43 章

アドレス、プロトコル、およびポート

この章では、IP アドレス、プロトコル、およびアプリケーションのクイック リファレンスを提供します。

- [IPv4 アドレスとサブネットマスク \(1065 ページ\)](#)
- [IPv6 アドレス \(1069 ページ\)](#)
- [プロトコルとアプリケーション \(1076 ページ\)](#)
- [TCP ポートおよび UDP ポート \(1077 ページ\)](#)
- [ローカル ポートとプロトコル \(1081 ページ\)](#)
- [ICMP タイプ \(1082 ページ\)](#)

IPv4 アドレスとサブネットマスク

この項では、Cisco ASA で IPv4 アドレスを使用する方法について説明します。IPv4 アドレスはドット付き 10 進数表記の 32 ビットの数値であり、バイナリから 10 進数に変換されドットで区切られた 4 つの 8 ビットフィールド（オクテット）で構成されます。IP アドレスの最初の部分はホストが常駐するネットワークを示し、2 番目の部分は所定のネットワーク上の特定のホストを示します。ネットワーク番号フィールドは、ネットワークプレフィックスと呼ばれます。所定のネットワーク上のホストはすべて、同じネットワークプレフィックスを共有しますが、固有のホスト番号を持つ必要があります。クラスフル IP では、アドレスのクラスがネットワークプレフィックスとホスト番号の間の境界を決定します。

クラス

IP ホストアドレスは、Class A、Class B、Class C の 3 つの異なるアドレスクラスに分かれています。各クラスは、32 ビットアドレス内の異なるポイントで、ネットワークプレフィックスとホスト番号の間の境界を決定します。Class D アドレスは、マルチキャスト IP 用に予約されています。

- Class A アドレス (1.xxx.xxx.xxx ~ 126.xxx.xxx.xxx) は、最初のオクテットのみをネットワークプレフィックスとして使用します。

- Class B アドレス (128.0.xxx.xxx ~ 191.255.xxx.xxx) は、最初の 2 つのオクテットをネットワーク プレフィックスとして使用します。
- Class C アドレス (192.0.0.xxx ~ 223.255.255.xxx) は、最初の 3 つのオクテットをネットワーク プレフィックスとして使用します。

Class A アドレスには 16,777,214 個のホストアドレス、Class B アドレスには 65,534 個のホストがあるので、サブネットマスクを使用してこれらの膨大なネットワークを小さいサブネットに分割することができます。

プライベート ネットワーク

ネットワーク上に多数のアドレスが必要な場合、それらをインターネットでルーティングする必要がないときは、インターネット割り当て番号局 (IANA) が推奨するプライベート IP アドレスを使用できます (RFC 1918 を参照)。次のアドレス範囲が、アドバタイズされないプライベート ネットワークとして指定されています。

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

サブネット マスク

サブネット マスクを使用すると、単一の Class A、B、または C ネットワークを複数のネットワークに変換できます。サブネットマスクを使用して、ホスト番号からネットワークプレフィックスにビットを追加する拡張ネットワークプレフィックスを作成することができます。たとえば、Class C ネットワークプレフィックスは常に、IP アドレスの最初の 3 つのオクテットで構成されます。一方、Class C 拡張ネットワークプレフィックスは、4 番目のオクテットの一部も使用します。

ドット付き 10 進数の代わりにバイナリ表記を使用している場合は、サブネットマスクを容易に理解できます。サブネットマスク内のビットには、インターネットアドレスとの 1 対 1 の対応関係があります。

- IP アドレス内の対応するビットが拡張ネットワークプレフィックスの一部である場合、ビットは 1 に設定されます。
- ビットがホスト番号の一部である場合、ビットは 0 に設定されます。

例 1 : Class B アドレスが 129.10.0.0 の場合に 3 番目のオクテット全体をホスト番号ではなく拡張ネットワークプレフィックスの一部として使用するには、サブネットマスクとして 11111111.11111111.11111111.00000000 を指定する必要があります。このサブネットマスクによって、Class B アドレスは、ホスト番号が最後のオクテットだけで構成される Class C アドレスに相当するものに変換されます。

例 2 : 3 番目のオクテットの一部だけを拡張ネットワークプレフィックスに使用する場合は、11111111.11111111.11111000.00000000 のようなサブネットマスクを指定する必要があります。ここでは、3 番目のオクテットのうち 5 ビットだけが拡張ネットワークプレフィックスに使用されます。

サブネットマスクは、ドット付き 10 進数マスクまたは /ビット（「スラッシュ ビット」）マスクとして記述できます。例 1 では、ドット付き 10 進数マスクに対して、各バイナリオクテットを 10 進数の 255.255.255.0 に変換します。/ビットマスクの場合は、1s:/24 の数値を追加します。例 2 では、10 進数は 255.255.248.0 で、/ビットは /21 です。

3 番目のオクテットの一部を拡張ネットワークプレフィックスに使用して、複数の Class C ネットワークを大規模なネットワークにスーパーネット化することもできます。たとえば、192.168.0.0/20 です。

サブネットマスクの決定

必要なホストの数に基づいてサブネットマスクを決定するには、次の表を参照してください。



(注) 単一のホストを示す /32 を除き、サブネットの最初と最後の数は予約されています。

表 53: ホスト、ビット、ドット区切りの 10 進数マスク

ホスト	/ビット マスク	ドット付き 10 進数マスク
16,777,216	/8	255.0.0.0 Class A ネットワーク
65,536	/16	255.255.0.0 Class B ネットワーク
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 Class C ネットワーク
128	/25	255.255.255.128
64	/26	255.255.255.192

ホスト	/ビットマスク	ドット付き 10 進数マスク
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
使用不可	/31	255.255.255.254
1	/32	255.255.255.255 単一ホストアドレス

サブネットマスクに使用するアドレスの決定

次の各項では、Class C サイズおよび Class B サイズのネットワークに対してサブネットマスクで使用するネットワークアドレスを判別する方法について説明します。

クラス C 規模ネットワークアドレス

2 ~ 254 のホストを持つネットワークの場合、4 番目のオクテットは、0 から始まるホストアドレスの数の倍数になります。例として、次の表に 8 個のホストを持つサブネット (/29)、192.168.0.x を示します。



(注) サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、192.168.0.0 と 192.168.0.7 は使用できません。

表 54: クラス C 規模ネットワークアドレス

マスク /29 (255.255.255.248) でのサブネット	アドレス範囲
192.168.0.0	192.168.0.0 ~ 192.168.0.7
192.168.0.8	192.168.0.8 ~ 192.168.0.15
192.168.0.16	192.168.0.16 ~ 192.168.0.31
—	—
192.168.0.248	192.168.0.248 ~ 192.168.0.255

クラス B 規模ネットワークアドレス

254 ~ 65,534 のホストを持つネットワークのサブネットマスクで使用するネットワークアドレスを判別するには、可能な拡張ネットワークプレフィックスそれぞれについて 3 番目のオクテットの値を判別する必要があります。たとえば、10.1.x.0 のようなアドレスをサブネット化

することができます。ここで、最初の2つのオクテットは拡張ネットワークプレフィックスで使用されるため固定されています。4番目のオクテットは、すべてのビットがホスト番号に使用されるため、0です。

3番目のオクテットの値を判別するには、次の手順を実行します。

1. 65,536 (3番目と4番目のオクテットを使用するアドレスの合計) を必要なホストアドレスの数で割って、ネットワークから作成できるサブネットの数を計算します。

たとえば、65,536 を 4096 のホストで割ると、16 になります。したがって、Class B サイズのネットワークでは、それぞれ 4096 個のアドレスを持つサブネットが 16 個できます。

2. 256 (3番目のオクテットの値の数) をサブネットの数で割って、3番目のオクテット値の倍数を判別します。

この例では、 $256/16 = 16$ です。

3番目のオクテットは、0 から始まる 16 の倍数になります。

次の表に、ネットワーク 10.1 の 16 個のサブネットを示します。



- (注) サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、10.1.0.0 と 10.1.15.255 は使用できません。

表 55: ネットワークのサブネット

マスク /20 (255.255.240.0) でのサブネット	アドレス範囲
10.1.0.0	10.1.0.0 ~ 10.1.15.255
10.1.16.0	10.1.16.0 ~ 10.1.31.255
10.1.32.0	10.1.32.0 ~ 10.1.47.255
—	—
10.1.240.0	10.1.240.0 ~ 10.1.255.255

IPv6 アドレス

IPv6 は、IPv4 後の次世代インターネットプロトコルです。これにより、アドレス空間の拡張、ヘッダー形式の簡略化、拡張子とオプションのサポートの向上、フローラベル機能、および認証とプライバシーの機能が提供されます。IPv6 については RFC 2460 で説明されています。IPv6 アドレッシングアーキテクチャについては RFC 3513 で説明されています。

この項では、IPv6 のアドレス形式とアーキテクチャについて説明します。

IPv6 アドレスの形式

IPv6 アドレスは、x:x:x:x:x:x のように、コロン (:) で区切られた 8 つの一連の 16 ビット 16 進数フィールドとして表されます。次に、IPv6 アドレスの例を 2 つ示します。

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A



(注) IPv6 アドレスの 16 進文字は大文字と小文字が区別されません。

アドレスの個々のフィールドに先行ゼロを入れる必要はありませんが、各フィールドに 1 個以上の桁が含まれている必要があります。したがって、例のアドレス

2001:0DB8:0000:0000:0008:0800:200C:417A は、左から 3 番目～6 番目のフィールドから先行ゼロを削除して、2001:0DB8:0:0:8:800:200C:417A のように短縮することができます。ゼロだけを含むフィールド（左から 3 番目と 4 番目のフィールド）は、単一のゼロに短縮されています。左から 5 番目のフィールドでは、3 つの先行ゼロが削除され、単一の 8 がフィールドに残されています。左から 6 番目のフィールドでは、1 つの先行ゼロが削除され、800 がフィールドに残されています。

IPv6 アドレスには、ゼロの 16 進数フィールドがいくつか連続して含まれていることがよくあります。IPv6 アドレスの先頭、中間、または末尾で 2 つのコロン (::) を使用して、ゼロの連続フィールドを圧縮することができます（コロンは、ゼロの 16 進数フィールドが連続していることを表します）。次の表に、さまざまなタイプの IPv6 アドレスでのアドレス圧縮の例をいくつか示します。

表 56: IPv6 アドレスの圧縮例

Address Type	標準形式	圧縮形式
ユニキャスト	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
マルチキャスト	FF01:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::



(注) ゼロのフィールドが連続することを表す 2 つのコロン (::) は、IPv6 アドレスの中で一度だけ使用できます。

IPv4 アドレスと IPv6 アドレスの両方を含む環境に対処するため、別の IPv6 形式がよく使用されます。その形式は x:x:x:x:x:y.y.y.y です。ここで、x は IPv6 アドレスの 6 つの高次の部分の 16 進数値を表し、y はアドレスの 32 ビット IPv4 部分（IPv6 アドレスの残りの 2 つの 16 ビット

ト部分を占める) の 10 進数値を表します。たとえば、IPv4 アドレス 192.168.1.1 は、IPv6 アドレス 0:0:0:0:0:FFFF:192.168.1.1 または ::FFFF:192.168.1.1 として表すことができます。

IPv6 アドレス タイプ

次に、IPv6 アドレスの 3 つの主なタイプを示します。

- **ユニキャスト** : ユニキャストアドレスは、単一インターフェイスの識別子です。ユニキャストアドレスに送信されたパケットは、そのアドレスで示されたインターフェイスに送信されます。1 つのインターフェイスに複数のユニキャストアドレスが割り当てられている場合もあります。
- **マルチキャスト** : マルチキャストアドレスは、インターフェイスのセットを表す識別子です。マルチキャストアドレスに送信されたパケットは、そのアドレスで示されたすべてのアドレスに送信されます。
- **エニーキャスト** : エニーキャストアドレスは、インターフェイスのセットを表す識別子です。マルチキャストアドレスと違い、エニーキャストアドレスに送信されたパケットは、ルーティングプロトコルの距離測定によって判別された「最も近い」インターフェイスにだけ送信されます。



(注) IPv6 にはブロードキャスト アドレスはありません。マルチキャストアドレスにブロードキャスト機能があります。

ユニキャスト アドレス

この項では、IPv6 ユニキャストアドレスについて説明します。ユニキャストアドレスは、ネットワーク ノード上のインターフェイスを識別します。

グローバル アドレス

IPv6 グローバル ユニキャストアドレスの一般的な形式では、グローバルルーティングプレフィックス、サブネット ID、インターフェイス ID の順に並んでいます。グローバルルーティングプレフィックスは、別の IPv6 アドレスタイプによって予約されていない任意のプレフィックスです。

バイナリ 000 で始まるものを除くすべてのグローバルユニキャストアドレスが、Modified EUI-64 形式で 64 ビットのインターフェイス ID を持っています。

バイナリ 000 で始まるグローバルユニキャストアドレスには、アドレスのインターフェイス ID 部分のサイズまたは構造に対する制約がありません。このタイプのアドレスの一例として、IPv4 アドレスが埋め込まれた IPv6 アドレスがあります。

サイトローカル アドレス

サイトローカルアドレスは、サイト内のアドレッシングに使用されます。このアドレスを使用すると、グローバルで一意的なプレフィックスを使用せずにサイト全体をアドレッシングするこ

とができます。サイトローカルアドレスでは、プレフィックス FEC0::/10、54 ビットサブネット ID、64 ビット インターフェイス ID (Modified EUI-64 形式) の順に並んでいます。

サイトローカルルータは、サイト外の送信元または宛先にサイトローカルアドレスを持つパケットを転送しません。したがって、サイトローカルアドレスは、プライベートアドレスと見なされます。

リンクローカルアドレス

すべてのインターフェイスに、少なくとも 1 つのリンクローカルアドレスが必要です。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカルアドレスは 1 つだけです。

リンクローカルアドレスは、Modified EUI-64 形式でリンクローカルプレフィックス FE80::/10 とインターフェイス識別子を使用して任意のインターフェイスで自動的に設定できる IPv6 ユニキャストアドレスです。リンクローカルアドレスは、ネイバー探索プロトコルとステートレス自動設定プロセスで使用されます。リンクローカルアドレスを持つノードは、通信が可能です。これらのノードは通信にサイトローカルアドレスまたはグローバルに固有なアドレスを必要としません。

ルータは、送信元または宛先にリンクローカルアドレスを持つパケットを送信しません。したがって、リンクローカルアドレスは、プライベートアドレスと見なされます。

IPv4 互換 IPv6 アドレス

IPv4 アドレスを組み込むことができる IPv6 アドレスのタイプは 2 つあります。

最初のタイプは、IPv4 互換 IPv6 アドレスです。IPv6 移行メカニズムには、IPv4 ルーティングインフラストラクチャ上で IPv6 パケットを動的にトンネリングさせるためのホストおよびルータの技術が実装されています。この技術を使用する IPv6 ノードには、低次 32 ビットでグローバル IPv4 アドレスを伝送する特別な IPv6 ユニキャストアドレスが割り当てられます。このタイプのアドレスは「IPv4 互換 IPv6 アドレス」と呼ばれ、形式は ::y.y.y.y です。この y.y.y.y は IPv4 ユニキャストアドレスになります。



(注) 「IPv4 互換 IPv6 アドレス」で使用する IPv4 アドレスは、グローバルに固有な IPv4 ユニキャストアドレスである必要があります。

2 つ目のタイプの IPv6 アドレスは、IPv4 アドレスが埋め込まれたもので、「IPv4 マッピング IPv6 アドレス」と呼ばれます。このアドレスタイプは、IPv4 ノードのアドレスを IPv6 アドレスとして表すために使用されます。このタイプのアドレス形式は ::FFFF:y.y.y.y です。ここで、y.y.y.y は IPv4 ユニキャストアドレスです。

未指定アドレス

未指定アドレス 0:0:0:0:0:0:0 は、IPv6 アドレスがないことを示しています。たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6 アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。



- (注) IPv6 未指定アドレスは、インターフェイスに割り当てることができません。未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティングヘッダーで宛先アドレスとして使用することはできません。

ループバックアドレス

ループバックアドレス `0:0:0:0:0:0:1` は、ノードが IPv6 パケットをそれ自体に送信するために使用できます。IPv6 のループバックアドレスは、IPv4 のループバックアドレス (`127.0.0.1`) と同じように機能します。



- (注) IPv6 ループバックアドレスは、物理インターフェイスに割り当てることができません。IPv6 ループバックアドレスを送信元アドレスまたは宛先アドレスとするパケットは、そのパケットを作成したノード内に留まっている必要があります。IPv6 ルータは、IPv6 ループバックアドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。

インターフェイス識別子

IPv6 ユニキャストアドレス内のインターフェイス識別子は、リンク上でインターフェイスを識別するために使用されます。これらの識別子は、サブネットプレフィックス内で固有である必要があります。多くの場合、インターフェイス識別子はインターフェイスリンク層アドレスから導出されます。各インターフェイスが異なるサブネットに接続されていれば、単一ノードの複数のインターフェイスで同一のインターフェイス識別子を使用することもできます。

バイナリ `000` で始まるものを除くすべてのユニキャストアドレスで、インターフェイス識別子は、64 ビットの長さで Modified EUI-64 形式で構築されている必要があります。Modified EUI-64 形式は、アドレス内のユニバーサル/ローカルビットを逆にし、MAC アドレスの上の 3 つのバイトと下の 3 つのバイトの間に 16 進数 `FFFE` を挿入することによって、48 ビット MAC アドレスから作成されます。

たとえば、MAC アドレスが `00E0.b601.3B7A` のインターフェイスの場合、64 ビットインターフェイス ID は `02E0:B6FF:FE01:3B7A` になります。

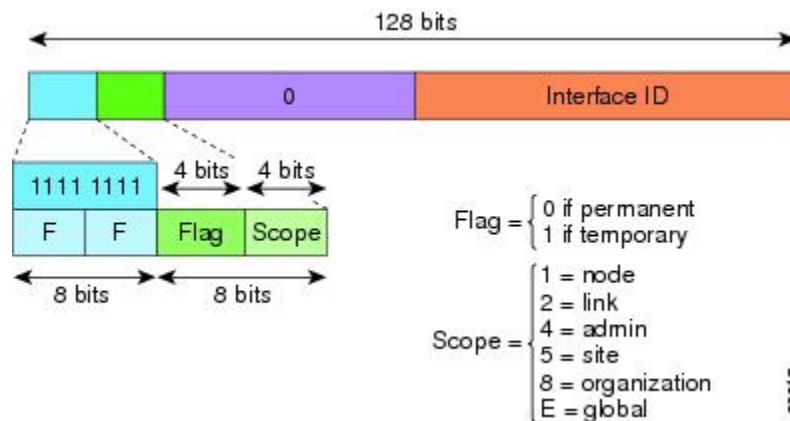
マルチキャストアドレス

IPv6 マルチキャストアドレスは、通常は異なるノード上にある、インターフェイスのグループの識別子です。マルチキャストアドレスに送信されたパケットは、マルチキャストアドレスが示すすべてのインターフェイスに配信されます。1 つのインターフェイスが任意の数のマルチキャストグループに属することができます。

IPv6 マルチキャストアドレスのプレフィックスは `FF00::/8` (`1111 1111`) です。オクテットとそれに続くプレフィックスは、マルチキャストアドレスのタイプとスコープを定義します。永続的に割り当てられた (周知の) マルチキャストアドレスには、0 に等しいフラグパラメータがあり、一時的な (過渡) マルチキャストアドレスには 1 に等しいフラグパラメータがあります。ノード、リンク、サイト、組織のスコープ、またはグローバルスコープを持つマルチ

キャストアドレスのスコープパラメータは、それぞれ1、2、5、8、またはEです。たとえば、プレフィックスがFF02::/16のマルチキャストアドレスは、リンクスコープを持つ永続マルチキャストアドレスです。次の図に、IPv6マルチキャストアドレスの形式を示します。

図 71: IPv6マルチキャストアドレス形式



IPv6 ノード（ホストとルータ）は、次のマルチキャストグループに参加する必要があります。

- All Nodes マルチキャストアドレス：
 - FF01::（インターフェイスローカル）
 - FF02::（リンクローカル）
- ノード FF02:0:0:0:1:FFXX:XXXX/104 上の各 IPv6 ユニキャストアドレスおよびエニーキャストアドレスの送信要求ノードアドレス。ここで、XX:XXXX は低次 24 ビットのユニキャストアドレスまたはエニーキャストアドレスです。



(注) 送信要求ノードアドレスは、ネイバー送信要求メッセージで使用されます。

IPv6 ルータは、次のマルチキャストグループに参加する必要があります。

- FF01::2（インターフェイスローカル）
- FF02::2（リンクローカル）
- FF05::2（サイトローカル）

マルチキャストアドレスは、IPv6 パケットで送信元アドレスとして使用できません。



(注) IPv6 にはブロードキャストアドレスはありません。ブロードキャストアドレスの代わりに IPv6 マルチキャストアドレスが使用されます。

エニーキャストアドレス

IPv6 エニーキャストアドレスは、複数のインターフェイス（通常は異なるノードに属す）に割り当てられたユニキャストアドレスです。エニーキャストアドレスにルーティングされたパケットは、そのアドレスを持ち、有効なルーティングプロトコルによって最も近いと判別されたインターフェイスにルーティングされます。

エニーキャストアドレスは、ユニキャストアドレス空間から割り当てられます。エニーキャストアドレスは、複数のインターフェイスに割り当てられたユニキャストアドレスにすぎません。インターフェイスは、アドレスをエニーキャストアドレスとして認識するように設定されている必要があります。

エニーキャストアドレスには次の制限が適用されます。

- エニーキャストアドレスは、IPv6 パケットの送信元アドレスとして使用できません。
- エニーキャストアドレスは、IPv6 ホストに割り当ててはできません。IPv6 ルータにだけ割り当てることができます。



(注) ASA では、エニーキャストアドレスをサポートされていません。

必須アドレス

IPv6 ホストには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 各インターフェイスのリンクローカルアドレス
- ループバックアドレス
- All-Nodes マルチキャストアドレス
- 各ユニキャストアドレスまたはエニーキャストアドレスの送信要求ノード マルチキャストアドレス

IPv6 ルータには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 必須ホストアドレス
- このルータがルータとして動作するように設定されているすべてのインターフェイスのサブネットルータ エニーキャストアドレス
- All-Routers マルチキャストアドレス

IPv6 アドレス プレフィックス

IPv6 アドレス プレフィックスは、`ipv6-prefix/prefix-length` の形式で、アドレス空間全体のビット連続ブロックを表すために使用できます。IPv6-prefix は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、`2001:0DB8:8086:6502::/32` は有効な IPv6 プレフィックスです。

IPv6 プレフィックスは、IPv6 アドレスのタイプを特定します。次の表に、各 IPv6 アドレスタイプのプレフィックスを示します。

表 57: IPv6 アドレス タイプのプレフィックス

Address Type	バイナリ プレフィックス	IPv6 表記
未指定	000...0 (128 ビット)	::/128
ループバック	000...1 (128 ビット)	::1/128
マルチキャスト	11111111	FF00::/8
リンクローカル (ユニキャスト)	1111111010	FE80::/10
サイトローカル (ユニキャスト)	1111111111	FEC0::/10
グローバル (ユニキャスト)	その他すべてのアドレス。	
エニーキャスト	ユニキャストアドレス空間から取得。	

プロトコルとアプリケーション

次の表に、プロトコルのリテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。

表 58: プロトコルのリテラル値

リテラル	値	説明
ah	51	IPv6 の認証ヘッダー (RFC 1826)。
eigrp	88	Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)。
esp	50	IPv6 の暗号ペイロード (RFC 1827)。
gre	47	総称ルーティング カプセル化。

リテラル	値	説明
icmp	1	インターネット制御メッセージプロトコル (RFC 792)。
icmp6	58	IPv6 のインターネット制御メッセージプロトコル (RFC 2463)。
igmp	2	インターネットグループ管理プロトコル (RFC 1112)。
igrp	9	Interior Gateway Routing Protocol。
ip	0	インターネットプロトコル。
ipinip	4	IP-in-IP カプセル化。
ipsec	50	IPセキュリティ。ipsec プロトコルリテラルを入力すると、esp プロトコルリテラルを入力した場合と同じ結果が得られます。
nos	94	ネットワークオペレーティングシステム (Novell の NetWare)。
ospf	89	OSPF ルーティングプロトコル (RFC 1247)。
pcp	108	ペイロード圧縮プロトコル。
pim	103	プロトコル独立型マルチキャスト。
pptp	47	ポイントツーポイントトンネリングプロトコル。pptp プロトコルリテラルを入力すると、gre プロトコルリテラルを入力した場合と同じ結果が得られます。
snp	109	Sitara Networks Protocol。
tcp	6	伝送制御プロトコル (RFC 793)。
udp	17	ユーザデータグラムプロトコル (RFC 768)。

IANA の Web サイトでオンラインでプロトコル番号を確認できます。

<http://www.iana.org/assignments/protocol-numbers>

TCP ポートおよび UDP ポート

次の表に、リテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。次の警告を参照してください。

- ASA は、SQL*Net 用にポート 1521 を使用します。これは、Oracle が SQL*Net に使用するデフォルトのポートです。ただし、この値は IANA ポート割り当てとは一致しません。
- ASA は、ポート 1645 と 1646 で RADIUS をリッスンしています。RADIUS サーバが標準ポート 1812 と 1813 を使用している場合は、**authentication-port** コマンドと **accounting-port** コマンドを使用して、それらのポートでリッスンするように ASA を設定できます。

- DNS アクセスにポートを割り当てるには、**dns** ではなく **domain** リテラル値を使用します。**dns** を使用した場合、ASA では、**dnsix** リテラル値を使用すると見なされます。

IANA の Web サイトでオンラインでポート番号を確認できます。

<http://www.iana.org/assignments/port-numbers>

表 59: ポートのリテラル値

リテラル	TCP または UDP	値	説明
aol	TCP	5190	America Online
bgp	TCP	179	ボーダー ゲートウェイ プロトコル (RFC 1163)
biff	UDP	512	新しいメールの受信をユーザに通知するために、メール システムが使用
bootpc	UDP	68	ブートストラップ プロトコル クライアント
bootps	UDP	67	ブートストラップ プロトコル サーバ
chargen	TCP	19	キャラクタ ジェネレータ
cifs	TCP、UDP	3020	Common Internet File System
citrix-ica	TCP	1494	Citrix Independent Computing Architecture (ICA) プロトコル
cmd	TCP	514	cmd は自動認証機能がある点を除いて、exec と同様。
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time (日時) (RFC 867)
discard	TCP、UDP	9	廃棄
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
domain	TCP、UDP	53	DNS
echo	TCP、UDP	7	Echo
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	Finger
ftp	TCP	21	ファイル転送プロトコル (コンソールポート)

リテラル	TCP または UDP	値	説明
ftp-data	TCP	20	ファイル転送プロトコル (データ ポート)
gopher	TCP	70	Gopher
h323	TCP	1720	H.323 発呼信号
hostname	TCP	101	NIC ホスト ネーム サーバ
http	TCP、UDP	80	World Wide Web HTTP
https	TCP	443	HTTP over SSL
ident	TCP	113	ID 認証サービス
imap4	TCP	143	Internet Message Access Protocol バージョン 4
irc	TCP	194	インターネット リレー チャット プロトコル
isakmp	UDP	500	Internet Security Association and Key Management Protocol
kerberos	TCP、UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn シェル
ldap	TCP	389	Lightweight Directory Access Protocol。
ldaps	TCP	636	ライトウェイトディレクトリアクセスプロトコル (SSL)
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
lpd	TCP	515	ライン プリンタ デーモン (プリンタ スプーラー)
mobile-ip	UDP	434	モバイル IP-Agent
nameserver	UDP	42	ホスト ネーム サーバ
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ns	UDP	137	NetBIOS ネーム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス

リテラル	TCP または UDP	値	説明
nfs	TCP、UDP	2049	ネットワーク ファイル システム (Sun Microsystems)
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	ネットワーク タイム プロトコル
pcanywhere-data	TCP	5631	pcAnywhere データ
pcanywhere-status	UDP	5632	pcAnywhere ステータス
pim-auto-rp	TCP、UDP	496	Protocol Independent Multicast、逆パス フラッド、デンス モード
pop2	TCP	109	Post Office Protocol (POP) Version 2
pop3	TCP	110	Post Office Protocol - Version 3
pptp	TCP	1723	ポイントツーポイントトンネリングプロトコル
radius	UDP	1645	リモート認証ダイヤルイン ユーザ サービス
radius-acct	UDP	1646	リモート認証ダイヤルイン ユーザ サービス (アカウントिंग)
rip	UDP	520	ルーティング情報プロトコル
rsh	TCP	514	リモート シェル
rtsp	TCP	554	Real Time Streaming Protocol
secureid-udp	UDP	5510	SecureID over UDP
sip	TCP、UDP	5060	Session Initiation Protocol
smtp	TCP	25	シンプル メール転送プロトコル
snmp	UDP	161	簡易ネットワーク管理プロトコル
snmptrap	UDP	162	簡易ネットワーク管理プロトコル (トラップ)
sqlnet	TCP	1521	構造化照会言語ネットワーク
ssh	TCP	22	セキュア シェル
sunrpc	TCP、UDP	111	Sun Remote Procedure Call
syslog	UDP	514	システム ログ

リテラル	TCP または UDP	値	説明
tacacs	TCP、UDP	49	Terminal Access Controller Access Control System Plus
talk	TCP、UDP	517	Talk
Telnet	TCP	23	Telnet (RFC 854)
tftp	UDP	69	『Trivial File Transfer Protocol』
time	UDP	37	時刻
uucp	TCP	540	UNIX 間コピー プログラム
vxlan	UDP	4789	Virtual eXtensible Local Area Network (VXLAN)
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP、UDP	80	ワールドワイド ウェブ
xdmcp	UDP	177	X Display Manager Control Protocol

ローカルポートとプロトコル

次の表に、ASA に向かうトラフィックを処理するために ASA が開くプロトコル、TCP ポート、および UDP ポートを示します。この表に記載されている機能とサービスをイネーブルにしない限り、ASA は、TCP または UDP ポートでローカルプロトコルを開きません。ASA がデフォルトのリスニングプロトコルまたはポートを開くように機能またはサービスを設定する必要があります。多くの場合、機能またはサービスをイネーブルにすると、デフォルトポート以外のポートを設定できます。

表 60: 機能とサービスによって開かれるプロトコルとポート

機能またはサービス	プロトコル	Port Number	注
DHCP	UDP	67、68	—
フェールオーバー制御	105	該当なし	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	該当なし	—

機能またはサービス	プロトコル	Port Number	注
IGMP	2	該当なし	プロトコルは宛先 IP アドレス 224.0.0.1 でだけ開かれます
ISAKMP/IKE	UDP	500	設定可能。
IPsec (ESP)	50	該当なし	—
IPsec over UDP (NAT-T)	UDP	4500	—
IPsec over TCP (CTCP)	TCP	—	デフォルト ポートは使用されません。IPsec over TCP の設定時にポート番号を指定する必要があります。
NTP	UDP	123	—
OSPF	89	該当なし	プロトコルは宛先 IP アドレス 224.0.0.5 および 224.0.0.6 でだけ開かれます
PIM	103	該当なし	プロトコルは宛先 IP アドレス 224.0.0.13 でだけ開かれます
RIP	UDP	520	—
RIPv2	UDP	520	ポートは宛先 IP アドレス 224.0.0.9 でだけ開かれます
SNMP	UDP	161	設定可能。
SSH	TCP	22	—
ステートフルアップ デート	8 (ノンセキュ ア) 9 (セキュ ア)	該当なし	—
Telnet	TCP	23	—
VPN ロードバランシ ング	UDP	9023	設定可能。
VPN 個別ユーザ認証 プロキシ	UDP	1645、1646	ポートは VPN トンネルでだけアクセス できます。

ICMP タイプ

次の表に、ASA のコマンドで入力できる ICMP タイプの番号と名前を示します。

表 61 : ICMP タイプ

ICMP 番号	ICMP 名
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect

