ad - aq

ad-agent-mode

Cisco アイデンティティ ファイアウォール インスタンスの Active Directory エージェントを設定できるように AD エージェントモードをイネーブルにするには、グローバル コンフィギュレーション モードで **ad-agent-mode** コマンドを使用します。

ad-agent-mode

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォールに対して Active Directory エージェントを設定するには、**aaa-server** コマンドのサブモードである **ad-agent-mode** コマンドを入力します。**ad-agent-mode** コマンドを入力すると、AAA サーバー グループ コンフィギュレーション モードが開始されます。

AD エージェントは、定期的に、または要求に応じて、WMI を介して Active Directory サーバーのセキュリティ イベント ログ ファイルをモニターし、ユーザーのログインおよびログオフ イベントを調べます。AD エージェントは、ユーザー ID および IP アドレスマッピングのキャッシュを保持し、ASA に変更を通知します。

AD エージェント サーバー グループのプライマリ AD エージェントとセカンダリ AD エージェントを設定します。プライマリ AD エージェントが応答していないことを ASA が検出し、セカンダリ エージェントが指定されている場合、ASA はセカンダリ AD エージェントに切り替えます。AD エージェントの Active Directory サーバーは、通信プロトコルとして RADIUS を使用します。そのため、ASA と AD エージェントとの共有秘密のキー属性を指定する必要があります。

例

次に、アイデンティティ ファイアウォールの Active Directory エージェントを設定するときに、**ad-agent-mode** をイネーブルにする例を示します。

```
ciscoasa(config)# aaa-server adagent protocol radius
ciscoasa(config)# ad-agent-mode
ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
ciscoasa(config-aaa-server-host)# key mysecret
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
ciscoasa(config-aaa-server-host)# test aaa-server ad-agent
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバー グループを作成し、グループ固有の AAA サーバー パラメータとすべてのグループ ホストに共通の AAA サーバー パラメータを設定します。
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

address（ダイナミック フィルタ ブラックリスト、ホワイトリスト）

IP アドレスをボットネット トラフィック フィルタのブラックリストまたはホワイトリストに追加するには、ダイナミック フィルタ ブラックリストまたはホワイトリスト コンフィギュレーション モードで **address** コマンドを使用します。アドレスを削除するには、このコマンドの **no** 形式を使用します。

address *ip_address mask*
no address *ip_address mask*

構文の説明

ip_address	ブラックリストに IP アドレスを追加します。
mask	IP アドレスのサブネットマスクを定義します。*mask* には、単一ホストまたはサブネットのマスクを指定できます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ダイナミック フィルタ ブラックリストまたはホワイトリスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

スタティック データベースを使用すると、ホワイトリストまたはブラックリストに追加するドメイン名または IP アドレスでダイナミック データベースを増強できます。ダイナミック フィルタ ホワイトリストまたはブラックリスト コンフィギュレーション モードを開始した後、**address** コマンドおよび **name** コマンドを使用して、適切な名前としてホワイトリストに、ま

たは不適切な名前としてブラックリストにタグ付けするドメイン名または IP アドレス（ホストまたはサブネット）を手動で入力できます。

このコマンドを複数回入力して、複数のエントリを追加できます。最大 1000 個のブラックリスト エントリと、最大 1000 個のホワイトリスト エントリを追加できます。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2
 255.255.255.255
```

関連コマンド

コマンド	説明
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネームルックアップを実行するために、ASA が DNS サーバーに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバーを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。

コマンド	説明
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニターされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバーの IP アドレス、ASA が次にサーバーに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデートサーバーに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

address（media-termination）（廃止）

電話プロキシ機能へのメディア接続に使用するメディア ターミネーション インスタンスのアドレスを指定するには、メディア ターミネーション コンフィギュレーション モードで **address** コマンドを使用します。メディア ターミネーション コンフィギュレーションからアドレスを削除するには、このコマンドの **no** 形式を使用します。

address *ip_address* ［ **interface** *intf_name* ］
no address *ip_address* ［ **interface** *intf_name* ］

構文の説明

interface *intf_name*	メディア ターミネーション アドレスを使用するインターフェイスの名前を指定します。1つのインターフェイスに設定できるメディア ターミネーション アドレスは 1 つだけです。
ip_address	メディア ターミネーション インスタンスに使用する IP アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
メディア ターミネーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** コマンドおよび **uc-ime** コマンドとともに廃止されました。

使用上のガイドライン

ASA では、次の基準を満たすメディアターミネーションの IP アドレスが設定されている必要があります。

- メディアターミネーションインスタンスでは、すべてのインターフェイスに対してグローバルなメディア ターミネーション アドレスを設定することも、インターフェイスごとに

メディア ターミネーション アドレスを設定することもできます。しかし、グローバルなメディア ターミネーション アドレスと、インターフェイスごとに設定するメディア ターミネーション アドレスは同時に使用できません。

- 複数のインターフェイスに対してメディア ターミネーション アドレスを設定する場合、IP 電話との通信時に ASA で使用するアドレスを、インターフェイスごとに設定する必要があります。
- IP アドレスは、そのインターフェイスのアドレス範囲内で使用されていない、パブリックにルーティング可能な IP アドレスです。

例

次に、media-termination address コマンドを使用して、メディア接続に使用する IP アドレスを指定する例を示します。

```
ciscoasa(config)# media-termination mediaterm1
ciscoasa(config-media-termination)# address 192.0.2.25 interface inside
ciscoasa(config-media-termination)# address 10.10.0.25 interface outside
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
media-termination	電話プロキシ インスタンスに適用するメディア ターミネーション インスタンスを設定します。

address-family ipv4

標準IP Version 4（IPv4）アドレスプレフィックスを使用してルーティングセッションを設定するためのアドレスファミリを入力するには、ルータ コンフィギュレーション モードでaddress-family ipv4コマンドを使用します。アドレス ファミリ コンフィギュレーション モードを終了し、実行コンフィギュレーションからIPv4アドレス ファミリ コンフィギュレーションを削除するには、このコマンドのno形式を使用します。

address-family ipv4
no address-family ipv4

コマンド デフォルト

IPv4アドレス プレフィックスはイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ モード コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

address-family ipv4コマンドは、コンテキストルータをアドレス ファミリ コンフィギュレーション モードにします。このルータから、標準IPv4アドレスプレフィックスを使用するルーティングセッションを設定できます。アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻るには、exitと入力します。

（注） アドレスファミリ IPv4のルーティング情報が、neighbor remote-asコマンドを使用して設定した各BGPルーティングセッションにデフォルトでアドバタイズされます。ただし、neighbor remote-asコマンドを設定する前にno bgp default ipv4-unicastコマンドを入力している場合は除きます。

例

次に、ルータをIPv4アドレス ファミリのアドレス ファミリ コンフィギュレーション モードにする例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)#
```

関連コマンド

コマンド	説明
bgp default ipv4-unicast	BGP ピアリング セッションのデフォルトとして IP Version 4（IPv4）ユニキャスト アドレス ファミリを設定します。
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。

address-family ipv6

標準 IP Version 6（IPv6）アドレスプレフィックスを使用してルーティングセッション（BGP など）を設定するためのアドレスファミリを入力するには、ルータ コンフィギュレーション モードで address-family ipv6 コマンドを使用します。アドレス ファミリ コンフィギュレーション モードを終了し、実行コンフィギュレーションから IPv6 アドレス ファミリ コンフィギュレーションを削除するには、このコマンドの no 形式を使用します。

address-family ipv6 [**unicast**]
no address-family ipv6

構文の説明

unicast	（オプション）IPv6 ユニキャスト アドレス プレフィックスを指定します。

コマンド デフォルト

IPv6 アドレス プレフィックスはイネーブルではありません。IPv6 アドレス プレフィックスが設定されている場合は、ユニキャスト アドレス プレフィックスがデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ モード コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

address-family ipv6 コマンドは、コンテキストルータをアドレス ファミリ コンフィギュレーション モードにします。このルータから、標準 IPv6 アドレスプレフィックスを使用するルーティングセッションを設定できます。アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻るには、exit と入力します。

例

次に、ルータを IPv4 アドレス ファミリのアドレス ファミリ コンフィギュレーション モードにする例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv6
ciscoasa(config-router-af)#
```

関連コマンド

コマンド	説明
neighbor ipv6-address activate	BGP ネイバーとの情報交換をイネーブルにします。

address-pool

アドレスをリモートクライアントに割り当てるためのアドレスプールのリストを指定するには、トンネルグループ一般属性コンフィギュレーションモードで **address-pool** コマンドを使用します。アドレスプールを削除するには、このコマンドの **no** 形式を使用します。

address-pool [（ *interface name* ）] *address_pool1* [*...address_pool6*]
no address-pool [（ *interface name* ）] *address_pool1* [*...address_pool6*]

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレスプールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
interface name	（任意）アドレス プールに使用するインターフェイスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

これらのコマンドは、インターフェイスごとに1つずつ、複数入力できます。インターフェイスが指定されていない場合、コマンドは明示的に参照されていないインターフェイスすべてに対してデフォルトを指定します。

グループポリシーの **address-pools** コマンドによるアドレスプール設定は、トンネルグループの **address-pool** コマンドによるローカルプール設定を上書きします。

プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

例

次に、設定トンネル一般コンフィギュレーション モードで、IPsec リモート アクセス トンネル グループ テスト用にアドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定する例を示します。

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
ip local pool	VPN リモート アクセス トンネルに使用する IP アドレス プールを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ トンネルをトンネル グループに関連付けます。

address-pools

アドレスをリモートクライアントに割り当てるためのアドレスプールのリストを指定するには、グループポリシー属性コンフィギュレーション モードで **address-pools** コマンドを使用します。グループポリシーから属性を削除し、別のグループポリシーソースからの継承をイネーブルにするには、このコマンドの **no** 形式を使用します。

address-pools value *address_pool1*［ *...address_pool6* ］
no address-pools value *address_pool1*［ *...address_pool6* ］
address-pools none
no address-pools none

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレスプールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
none	アドレス プールを設定しないことを指定し、他のグループ ポリシーからの継承をディセーブルにします。
value	アドレスの割り当てに使用する最大 6 個のアドレス プールのリストを指定します。

コマンド デフォルト

デフォルトでは、アドレス プールの属性は継承を許可します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドによるアドレス プール設定は、グループ内のローカル プール設定を上書きします。ローカル アドレスの割り当てに使用する最大 6 個のローカル アドレス プールのリストを指定できます。

プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

address-pools none コマンドは、ポリシーの別のソース（DefaultGrpPolicy など）からこの属性を継承することをディセーブルにします。**no address pools none** コマンドは、 **address-pools none** コマンドをグループポリシーから削除して、デフォルト値（継承の許可）に戻します。

例

次に、GroupPolicy1 の設定一般コンフィギュレーション モードで、アドレスをリモート クライアントに割り当てるために使用するアドレス プールのリストとして pool_1 および pool_20 を設定する例を示します。

```
ciscoasa(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
ciscoasa(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# address-pools value pool_1 pool_20
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
ip local pool	VPN グループ ポリシーで使用する IP アドレス プールを設定します。
clear configure group-policy	設定されているすべてのグループ ポリシーをクリアします。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

admin-context

システム コンフィギュレーションの管理コンテキストを設定するには、グローバル コンフィギュレーション モードで **admin-context** コマンドを使用します。

admin-context *name*

構文の説明

name 名前を最大 32 文字のストリングで設定します。コンテキストをまだ定義していない場合は、まずこのコマンドで管理コンテキスト名を指定します。次に、**context** コマンドを使用して最初に追加するコンテキストを、指定した管理コンテキスト名にする必要があります。

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。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。

「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。

コマンド デフォルト

マルチコンテキストモードの新しい ASA の場合、管理コンテキスト名は「admin」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

コンテキスト コンフィギュレーションが内部フラッシュメモリにある限り、任意のコンテキストを管理コンテキストに設定できます。

現在の管理コンテキストは削除できません。ただし、**clear configure context** コマンドを使用してすべてのコンテキストを削除すれば、管理コンテキストも削除できます。

システム コンフィギュレーションには、システム自体のネットワーク インターフェイスまたはネットワーク設定は含まれません。代わりに、システムは、ネットワークリソースにアクセスする必要がある場合に（ASA ソフトウェアをダウンロードしたり、管理者に対してリモート

アクセスを許可する場合など）、管理コンテキストとして指定されたコンテキストのいずれかを使用します。

例

次に、管理コンテキストを「administrator」に設定する例を示します。

```
ciscoasa(config)# admin-context administrator
```

関連コマンド

コマンド	説明
clear configure context	システム コンフィギュレーションからすべてのコンテキストを削除します。
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードを開始します。
show admin-context	現在の管理コンテキスト名を表示します。

advertise passive-only

パッシブインターフェイスに属するプレフィックスだけをアドバタイズするように IS-IS を設定するには、ルータ コンフィギュレーション モードで **advertise passive-only** コマンドを使用します。制限を削除するには、このコマンドの **no** 形式を使用します。

advertise passive-only
no advertise passive-only

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドには、デフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、リンクステート パケット（LSP）アドバタイズメントから、接続されたネットワークの IP プレフィックスを除外し、IS-IS コンバージェンス時間を削減するための IS-IS メカニズムです。

IS-IS インスタンスごとにこのコマンドを設定すると、ルータの非疑似ノード LSP でアドバタイズされるプレフィックスの数が少なくなるため、IS-IS コンバージェンス時間の削減という課題をスケーラブルに解決することができます。

このコマンドは、「ループバック インターフェイスで IS-IS をイネーブルにする場合、通常、ループバックを受動に設定する」という事実に依存しています。この設定は、ループバックの背後にネイバーが見つかる可能性はないため、ループバックを通じて、必要のないHelloパケットの送信を防ぐために行われます。したがって、アドバタイズする必要があるものがループバックだけで、このループバックがすでに受動に設定されている場合、IS-IS インスタンスごとに **advertise passive-only** コマンドを設定することにより、ルーティングテーブルのデータ過剰を防ぐことができます。

このコマンドの代わりが **no isis advertise-prefix** コマンドです。**no isis advertise-prefix** コマンドは、インターフェイスごとに設定される、規模の小さいソリューションです。

例

次に、**advertise passive-only** コマンドを使用する例を示します。このコマンドは、IS-IS インスタンスに作用し、イーサネット インターフェイス 0 の IP ネットワークのアドバタイズを阻止します。ループバック インターフェイス 0 の IP アドレスだけがアドバタイズされます。

```
!
!
!
interface Gi0/0
 ip address 192.168.20.1 255.255.255.0
router isis
!.
int gi0/1
  ip add 171.1.1.1 255.255.255.0
   router isis
!.
router isis
 passive-interface outside
 net 47.0004.004d.0001.0001.0c11.1111.00
 advertise-passive-only
 log-adjacency-changes
!
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。

コマンド	説明
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。

コマンド	説明
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。

コマンド	説明
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

aggregate-address

Border Gateway Protocol（BGP）データベース内に集約エントリを作成するには、アドレス ファミリ コンフィギュレーション モードで aggregate-address コマンドを使用します。この機能をディセーブルにするには、このコマンドの no 形式を使用します。

aggregate-address *address mask* ［ **as-set** ］［ **summary-only** ］［ **suppress-map** *map-name* ］［ **advertise-map** *map-name* ］［ **attribute-map** *map-name* ］
no aggregate-address *address mask* ［ **as-set** ］［ **summary-only** ］［ **suppress-map** *map-name* ］［ **advertise-map** *map-name* ］［ **attribute-map** *map-name* ］

構文の説明

address	集約アドレス。
mask	集約マスク。
as-set	（オプション）自律システム設定パス情報を生成します。
summary-only	（任意）アップデートからのすべてのより具体的なルートをフィルタ処理します。
suppress-map map-name	（オプション）抑制するルートの選択に使用されるルートマップの名前を指定します。
advertise-map map-name	（オプション）AS_SET 送信元コミュニティを作成するルートの選択に使用されるルート マップの名前を指定します。
attribute-map map-name	（オプション）集約ルートの属性を設定するために使用されるルートマップの名前を指定します。

コマンド デフォルト

アトミック集約属性は、as-set キーワードが指定されない限り、このコマンドによって集約ルートが作成されるときに自動的に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
コンテキスト コンフィギュレーション、アドレス ファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ ipv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

集約ルートを BGP またはマルチプロトコル BGP（mBGP）に再配布するか、条件付きの集約ルーティング機能を使用することにより、BGP および mBGP に集約ルーティングを実装できます。

キーワードなしで aggregate-address コマンドを使用すると、指定された範囲内にあるより具体的な BGP または mBGP ルートが使用できる場合、BGP または mBGP ルーティング テーブルに集約エントリが作成されます（集約に一致する長いプレフィックスは、ルーティング情報ベース（RIB）に存在する必要があります）。集約ルートは自律システムからのルートとしてアドバタイズされます。また、この集約ルートには、情報が失われている可能性を示すために、アトミック集約属性が設定されます（as-set キーワードを指定しない場合は、アトミック集約属性がデフォルトで設定されます）。

as-set キーワードを使用すると、コマンドがこのキーワードなしで従う同じルールを使用する集約エントリが作成されますが、このルートにアドバタイズされるパスは、集約されている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。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。

summary-only キーワードを使用すると、集約ルート（192.*.*.* など）が作成されるだけでなく、すべてのネイバーへのより具体的なルートのアドバタイズメントが抑制されます。特定のネイバーへのアドバタイズメントのみを抑制したい場合、neighbor distribute-list コマンドを使用できますが、慎重に使用すべきです。より具体的なルートがリークした場合、すべての BGP または mBGP ルータは、生成中の具体的でない集約よりもこのルートを優先します（最長一致ルーティングによる）。

suppress-map キーワードを使用すると、集約ルートは作成されますが、指定されたルートのアドバタイズメントが抑制されます。ルートマップの一致句を使用して、集約のより具体的な一部のルートを選択的に抑制し、他のルートを抑制しないでおくことができます。IP アクセス リストと自律システム パス アクセス リストの一致句がサポートされています。

advertise-map キーワードを使用すると、集約ルートの異なるコンポーネント（AS_SET やコミュニティなど）を構築するために使用する特定のルートが選択されます。集約のコンポーネントが別々の自律システムにあり、AS_SET で集約を作成して同じ自律システムの一部にアドバタイズしたい場合、aggregate-address コマンドのこの形式は役に立ちます。AS_SET から特定の自律システム番号を省略し、集約が受信ルータの BGP ループ検出メカニズムによってドロップされるのを防ぐことを忘れてはなりません。IP アクセス リストと自律システム パス アクセス リストの一致句がサポートされています。

attribute-map キーワードを使用すると、集約ルートの属性を変更できます。AS_SET を構成するルートの 1 つが community no-export 属性（集約ルートがエクスポートされるのを防ぐ）などの属性で設定されている場合、aggregate-address コマンドのこの形式は役に立ちます。属性マップ ルート マップを作成し、集約の属性を変更することができます。

例

次に、集約ルートを作成し、すべてのネイバーへのより具体的なルートのアドバタイズメントを抑制する例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

関連コマンド

コマンド	説明
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 を使用するルーティング セッションを設定します。

alarm contact description

ISA 3000 でアラーム入力の説明を入力するには、グローバル コンフィギュレーション モードで **alarm contact description** コマンドを使用します。デフォルトの説明を対応するコンタクト番号に設定するには、このコマンドの no 形式を使用します。

alarm contact { **1** | **2** } **description** *string*
no alarm contact { **1** | **2** } **description**

構文の説明

1 | 2	説明が設定されているアラーム コンタクトを指定します。1 または 2 を入力します。
string	説明を指定します。説明には最大 80 文字の英数字を使用でき、syslog メッセージに含められます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、アラーム コンタクト 1 の説明を指定する例を示します。

```
ciscoasa(config)# alarm contact 1 description Door Open
```

関連コマンド

コマンド	説明
alarm contact severity	ISA 3000 の LED 状態に順に影響を与えるアラームのシビラティ（重大度）を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。

コマンド	説明
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature (high and low thresholds)	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定されたシビラティ（重大度）に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm contact severity

ISA 3000 でアラームのシビラティ（重大度）を指定するには、グローバル コンフィギュレーション モードで **alarm contact severity** コマンドを使用します。デフォルトのシビラティ（重大度）に戻すには、このコマンドの no 形式を使用します。

alarm contact { **1** | **2** | **all** } **severity** { **major** | **minor** | **none** }
no alarm contact { **1** | **2** | **all** } **severity**

構文の説明

{**1** | **2** | **all**}	シビラティ（重大度）を設定するアラーム コンタクトを指定します。1、2、または all を入力します。
severity {**major** | **minor** | **none**}	このアラーム コンタクトによってトリガーされたアラームのシビラティ（重大度）。このシビラティ（重大度）でアラームをラベル付けするほか、このシビラティ（重大度）により、コンタクトに関連付けられた LED の動作が制御されます。 • **major**：LED が赤色で点滅します。 • **minor**：LED が赤色で点灯します。これがデフォルトです。 • **none**：LED が消灯します。

コマンド デフォルト

デフォルトでは、シビラティ（重大度）はマイナーになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、アラーム コンタクト 1 のシビラティ（重大度）を指定する例を示します。

```
ciscoasa(config)# alarm contact 1 severity major
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature (high and low thresholds)	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定されたシビラティ（重大度）に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm contact trigger

ISA 3000 で 1 つまたはすべてのアラーム入力にトリガーを指定するには、グローバル コンフィギュレーション モードで **alarm contact trigger** コマンドを使用します。デフォルトのトリガーに戻すには、このコマンドの **no** 形式を使用します。

alarm contact { **1** | **2** | **all** } **trigger** { **open** | **closed** }
alarm contact { **1** | **2** | **all** } **trigger**

構文の説明

{**1** | **2** | **all**}	トリガーを設定するアラーム コンタクトを指定します。1、2、または all を入力します。
trigger {**open** | **closed**}	トリガーは、アラート信号を発する電気条件を決定します。 • **open**：コンタクトの通常状態はクローズです。つまり、コンタクトに電流が流れています。コンタクトがオープンになる、つまり電流が停止するとアラートがトリガーされます。 • **closed**：コンタクトの通常状態はオープンです。つまり、コンタクトに電流は流れていません。コンタクトがクローズになる、つまり電流がコンタクトを流れ始めるとアラートがトリガーされます。これはデフォルトです。

コマンド デフォルト

デフォルトでは、クローズ状態がトリガーです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、アラーム コンタクト 1 にトリガーを設定する例を示します。

```
ciscoasa(config)# alarm contact 1 trigger open
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームのシビラティ（重大度）を指定します。
alarm facility input-alarm	アラーム入力のロギングオプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature (high and low thresholds)	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定されたシビラティ（重大度）に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility input-alarm

ISA 3000 でアラーム入力のロギングおよび通知オプションを指定するには、グローバル コンフィギュレーション モードで **alarm facility input-alarm** コマンドを使用します。ロギングおよび通知オプションを削除するには、このコマンドの **no** 形式を使用します。

alarm facility input-alarm { **1** | **2** } { **notifies** | **relay** | **syslog** }
no alarm facility input-alarm { **1** | **2** } { **notifies** | **relay** | **syslog** }

構文の説明

{**1** | **2**}	アラーム コンタクト（1 または 2）を指定します。
notifies	アラームがトリガーされたときに SNMP トラップの送信を有効にします。
relay	アラームがトリガーされたときにハードウェア出力リレーを有効にします。これにより、接続されている外部アラームがアクティブになります。
syslog	アラームがトリガーされたとき、およびアラーム条件が終了したときに syslog メッセージの送信を有効にします。

コマンド デフォルト

デフォルトでは、syslog は有効になっていますが、その他のオプションは無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、アラーム入力 1 にロギングおよび通知オプションを指定する例を示します。

```
ciscoasa(config)# alarm facility input-alarm 1 notifies

ciscoasa(config)# alarm facility input-alarm 1 relay
```

```
ciscoasa(config)# alarm facility input-alarm 1 syslog
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームのシビラティ（重大度）を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature (high and low thresholds)	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定されたシビラティ（重大度）に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility power-supply rps

ISA 3000 で電源アラームを設定するには、グローバル コンフィギュレーション モードで **alarm facility power-supply rps** コマンドを使用します。電源アラーム、リレー、SNMP トラップおよび syslog を無効にするには、**alarm facility power-supply rps disable** コマンドまたは **no** バージョンを使用します。

alarm facility power-supply rps { **disable** | **notifies** | **relay** | **syslog** }
no alarm facility power-supply rps { **disable** | **notifies** | **relay** | **syslog** }

構文の説明

disable	電源アラーム、リレー、SNMP トラップおよび syslog を無効にします。
notifies	アラームがトリガーされたときに SNMP トラップの送信を有効にします。
relay	アラームがトリガーされたときにハードウェア出力リレーを有効にします。これにより、接続されている外部アラームがアクティブになります。
syslog	アラームがトリガーされたとき、およびアラーム条件が終了したときに syslog メッセージの送信を有効にします。

コマンド デフォルト

デフォルトで、**syslog** はイネーブルになっており、**relay** および **notifies** はディセーブルになっています。このアラームは、デフォルトで有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

ISA 3000 には、電源装置が 2 台搭載されています。デフォルトでは、システムはシングル電源モードで稼働しています。ただし、デュアルモードでシステムを稼働するよう設定できます。その場合、プライマリ電源が故障すると 2 つ目の電源が自動的に電力を供給します。デュアルモードを有効にすると、電源アラームが自動的に有効になって syslog アラートが送信されます

が、アラートを無効にしたり、SNMP トラップまたはアラーム ハードウェア リレーを有効にすることもできます。

alarm facility power-supply rps disable コマンドは、電源アラーム、リレー、SNMP トラップおよび syslog を無効にします。**no alarm facility power-supply rps disable** コマンドを使用すると、電源アラームのみが有効になります。リレー、SNMP トラップ、および syslog を個別に有効にする必要があります。

また、デュアルモードを有効にするには、**power-supply dual** コマンドも設定する必要があります。このアラームは、デュアル モードで自動的に有効になります。

例

次に、デュアル電源モードを有効にし、すべてのアラート オプションを設定する例を示します。

```
ciscoasa(config)# power-supply dual
ciscoasa(config)# alarm facility power-supply rps relay
ciscoasa(config)# alarm facility power-supply rps syslog
ciscoasa(config)# alarm facility power-supply rps notifies
```

次に、デュアル電源アラームを無効にする例を示します。

```
ciscoasa(config)# alarm facility power-supply rps disable
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームのシビラティ（重大度）を指定します。
alarm contact trigger	1つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature (high and low thresholds)	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。

コマンド	説明
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定されたシビラティ（重大度）に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility temperature（アクション）

ISA 3000 で温度アラームを設定するには、グローバル コンフィギュレーション モードで **alarm facility temperature** コマンドを使用します。温度アラームを無効にするには、このコマンドの **no** 形式を使用します。

alarm facility temperature { **primary** | **secondary** } { **notifies** | **relay** | **syslog** }
no alarm facility temperature { **primary** | **secondary** } { **notifies** | **relay** | **syslog** }

構文の説明

primary	プライマリ温度アラームを設定します。
secondary	セカンダリ温度アラームを設定します。
notifies	アラームがトリガーされたときに SNMP トラップの送信を有効にします。
relay	アラームがトリガーされたときにハードウェア出力リレーを有効にします。これにより、接続されている外部アラームがアクティブになります。
syslog	アラームがトリガーされたとき、およびアラーム条件が終了したときに syslog メッセージの送信を有効にします。

コマンド デフォルト

プライマリ温度アラームは、すべてのアラーム アクションに対して有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

デバイスの CPU カードの温度に基づいてアラームを設定できます。

alarm facility temperature コマンドで **high** および **low** キーワードを使用して、プライマリとセカンダリの温度範囲を設定できます。温度が下限しきい値以下になるか上限しきい値以上になると、アラームがトリガーされます。

プライマリ温度アラームは、すべてのアラームアクション（出力リレー、syslog、およびSNMP）についてデフォルトで有効になっています。プライマリ温度範囲のデフォルト設定値は -40 °C ～ 92 °C です。

セカンダリ温度アラームはデフォルトでディセーブルになっています。セカンダリ温度は、-35 °C ～ 85 °C の範囲で設定できます。

セカンダリ温度範囲はプライマリ範囲よりも制限されているため、セカンダリの低温または高温を設定すると、プライマリ設定にデフォルト以外の値を設定している場合でも、対応するプライマリ設定はセカンダリの設定によって無効になります。2 つの異なる高温アラームと 2 つの異なる低温アラームを有効にすることはできません。

したがって、実際には、プライマリのみまたはセカンダリのみの高温値および低温値を設定する必要があります。

例

次の例では、セカンダリ アラームの高温値および低温値を設定し、すべてのアラート アクションを有効にしています。

```
ciscoasa(config)# alarm facility temperature secondary low -20
ciscoasa(config)# alarm facility temperature secondary high 80
ciscoasa(config)# alarm facility temperature secondary notifies
ciscoasa(config)# alarm facility temperature secondary relay
ciscoasa(config)# alarm facility temperature secondary syslog
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームのシビラティ（重大度）を指定します。
alarm contact trigger	1つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature (high and low thresholds)	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。

コマンド	説明
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定されたシビラティ（重大度）に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility temperature（上限および下限しきい値）

ISA 3000 で上限および下限の温度しきい値を設定するには、グローバル コンフィギュレーション モードで **alarm facility temperature** {**low** | **high**} コマンドを使用します。しきい値を削除するか、プライマリの値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

alarm facility temperature { **primary** | **secondary** } { **high** | **low** } *threshold*
no alarm facility temperature { **primary** | **secondary** } { **high** | **low** } *threshold*

構文の説明

primary	プライマリ温度アラームを設定します。
secondary	セカンダリ温度アラームを設定します。
high しきい値	上限しきい値を摂氏で設定します。プライマリの最大値は 92 です。セカンダリの最大値は 85 です。
low しきい値	下限しきい値を摂氏で設定します。プライマリの最小値は -40 です。セカンダリの最小値は -35 です。

コマンド デフォルト

デフォルトのプライマリ高温値は 92 ℃、低温値は -40 ℃ です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

デバイスの CPU カードの温度に基づいてアラームを設定できます。

alarm facility temperature コマンドで **high** および **low** キーワードを使用して、プライマリとセカンダリの温度範囲を設定できます。温度が下限しきい値以下になるか上限しきい値以上になると、アラームがトリガーされます。

プライマリ温度アラームは、すべてのアラームアクション（出力リレー、syslog、およびSNMP）についてデフォルトで有効になっています。プライマリ温度範囲のデフォルト設定値は -40 °C ～ 92 °C です。

セカンダリ温度アラームはデフォルトでディセーブルになっています。セカンダリ温度は、-35 °C ～ 85 °C の範囲で設定できます。

セカンダリ温度範囲はプライマリ範囲よりも制限されているため、セカンダリの低温または高温を設定すると、プライマリ設定にデフォルト以外の値を設定している場合でも、対応するプライマリ設定はセカンダリの設定によって無効になります。2 つの異なる高温アラームと 2 つの異なる低温アラームを有効にすることはできません。

したがって、実際には、プライマリのみまたはセカンダリのみの高温値および低温値を設定する必要があります。

例

次の例では、セカンダリ アラームの高温値および低温値を設定し、すべてのアラート アクションを有効にしています。

```
ciscoasa(config)# alarm facility temperature secondary low -20
ciscoasa(config)# alarm facility temperature secondary high 80
ciscoasa(config)# alarm facility temperature secondary notifies
ciscoasa(config)# alarm facility temperature secondary relay
ciscoasa(config)# alarm facility temperature secondary syslog
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームのシビラティ（重大度）を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。

コマンド	説明
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定されたシビラティ（重大度）に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LEDのアラーム状態をクリアします。

allocate-interface

インターフェイスをセキュリティコンテキストに割り当てるには、コンテキストコンフィギュレーションモードで**allocate-interface**コマンドを使用します。インターフェイスをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-interface *physical_interface*［ *map_name* ］［ **visible** | **invisible** ］
no allocate-interface *physical_interface*
allocate-interface *physical_interface* **.** *subinterface*［ *- physical interface* **.** *subinterface* ］［ *map_name*［ *- map_name* ］］［ **visible** | **invisible** ］
no allocate-interface *physical_interface* **.** *subinterface*［ *- physical interface* **.** *subinterface* ］

構文の説明

invisible	（デフォルト）コンテキストユーザーが **show interface** コマンドでマッピング名（設定されている場合）だけを表示できるようにします。

map_name	（任意）マッピング名を設定します。
	
	map_name は、インターフェイス ID の代わりにコンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しない場合、インターフェイス ID がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているインターフェイスをコンテキスト管理者に知らせない場合があります。
	
	マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。
	
	`int0`
	`inta`
	`int_0`
	
	サブインターフェイスの場合は、マッピング名の範囲を指定できます。
	
	詳細については、「使用上のガイドライン」を参照してください。

physical_interface	**gigabitethernet0/1** などのインターフェイス ID を設定します。有効値については、**interface** コマンドを参照してください。インターフェイス タイプとポート番号の間にスペースを含めないでください。
サブインターフェイス	サブインターフェイス番号を設定します。サブインターフェイスの範囲を指定できます。
visible	（任意）マッピング名を設定した場合でも、コンテキストユーザーが **show interface** コマンドで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します。

コマンド デフォルト

マッピング名を設定した場合、デフォルトでは、**show interface** コマンドの出力にインターフェイス ID は表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
コンテキストコンフィギュレーション	• 対応	• 対応	—	—	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを複数回入力して、異なる範囲を指定できます。マッピング名または参照できる設定を変更するには、所定のインターフェイス ID のコマンドを再入力して、新しい値を設定します。**no allocate-interface** コマンドを入力して、もう一度やり直す必要はありません。**allocate-interface** コマンドを削除すると、ASA によって、コンテキスト内のインターフェイス関連のコンフィギュレーションがすべて削除されます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA では、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。

（注） トランスペアレント モードの管理インターフェイスは、MAC アドレス テーブルにないパケットをインターフェイスにフラッディングしません。

ルーテッド モードでは、必要に応じて同じインターフェイスを複数のコンテキスト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、インターフェイスを共有できません。

サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。

- マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。

```
int0-int10
```

たとえば、**gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5** と入力した場合、このコマンドは失敗します。

- マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。

```
gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
```

たとえば、**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15** と入力した場合、このコマンドは失敗します。

例

次に、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/1.305 をコンテキストに割り当てる例を示します。マッピング名は、int1 ～ int8 です。

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

allocate-ips

IPS 仮想センサーをセキュリティコンテキストに割り当てるには、AIP SSM がインストールされている場合には、コンテキスト コンフィギュレーション モードで **allocate-ips** コマンドを使用します。仮想センサーをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-ips *sensor_name* [*mapped_name*] [**default**]
no allocate-ips *sensor_name* [*mapped_name*] [**default**]

構文の説明

default	（任意）コンテキストごとに 1 つのセンサーをデフォルト センサーとして設定します。コンテキスト コンフィギュレーションでセンサー名が指定されていない場合は、コンテキストでこのデフォルト センサーが使用されます。コンテキストごとに設定できるデフォルトセンサーは1つのみです。デフォルトセンサーを変更する場合は、 **no allocate-ips** コマンドを入力して現在のデフォルトセンサーを削除してから、新しいデフォルトセンサーを割り当てます。デフォルトとしてセンサーを指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、AIP SSM でトラフィックはデフォルト センサーを使用します。
mapped_name	（任意）コンテキスト内で実際のセンサー名の代わりに使用できるセンサー名のエイリアスとして、マッピング名を設定します。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」および「sensor2」というセンサーを使用する場合、コンテキスト A の sensor1 と sensor2 に「highsec」センサーと「lowsec」センサーをマッピングし、コンテキスト B の sensor1 と sensor2 に「medsec」センサーと「lowsec」センサーをマッピングできます。
sensor_name	AIP SSM にセンサー名を設定します。AIP SSM に設定されているセンサーを表示するには、**allocate-ips ?** と入力します。使用可能なすべてのセンサーが表示されます。**show ips** コマンドを入力することもできます。システム実行スペースで **show ips** コマンドを入力すると、使用可能なすべてのセンサーが表示されます。このコマンドをコンテキストで入力すると、そのコンテキストにすでに割り当てられているセンサーが表示されます。AIP SSM にまだ存在しないセンサー名を指定すると、エラーになりますが、**allocate-ips** コマンドはそのまま入力されます。AIP SSM に指定した名前のセンサーを作成するまで、コンテキストはセンサーがダウンしていると見なします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
コンテキストコンフィギュレーション	• 対応	• 対応	—	—	

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

各コンテキストに 1 つ以上の IPS 仮想センサーを割り当てることができます。その後、**ips** コマンドを使用して AIP SSM にトラフィックを送信するようにコンテキストを設定するときに、コンテキストに割り当てられているセンサーを指定できます。コンテキストに割り当てられていないセンサーは指定できません。コンテキストにセンサーを割り当てない場合は、AIP SSM に設定されているデフォルトセンサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。

（注） 仮想センサーを使用するためにマルチ コンテキスト モードを開始する必要はありません。シングル モードでトラフィック フローごとに異なるセンサーを使用できます。

例

次に、sensor1 と sensor2 をコンテキスト A に、sensor1 と sensor3 をコンテキスト B に割り当てる例を示します。どちらのコンテキストもセンサー名を「ips1」と「ips2」にマップします。コンテキスト A では sensor1 をデフォルトセンサーとして設定しますが、コンテキスト B ではデフォルトを設定しないため、AIP SSM に設定されているデフォルトが使用されます。

```
ciscoasa(config-ctx)# context
 A
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1 default
ciscoasa(config-ctx)# allocate-ips sensor2 ips2
ciscoasa(config-ctx)# config-url
 ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold
ciscoasa(config-ctx)# context
 sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
```

```
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1
ciscoasa(config-ctx)# allocate-ips sensor3 ips2
ciscoasa(config-ctx)# config-url
 ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
ips	トラフィックをインスペクションのために AIP SSM に転送します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。
show ips	AIP SSM に仮想センサーを設定します。

allowed-eid

IP アドレスに基づいて検査対象 EID を制限するための LISP インスペクションマップを設定するには、パラメータ コンフィギュレーション モードで **allowed-eid** コマンドを使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect lisp** コマンドを入力します。すべての EID を許可するには、このコマンドの **no** 形式を使用します。

allowed-eid access-list *eid_acl_name*
no allowed-eid access-list *eid_acl_name*

構文の説明

access-list *eid_acl_name*	宛先 IP アドレスのみが EID 組み込みアドレスと照合される拡張 ACL を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

IP アドレスに基づいて検査対象 EID を制限するための LISP インスペクション マップを設定します。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. （オプション）ホストまたはサーバーの IP アドレスに基づく検査される EID の限定：最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関す

る EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバーまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid,** および **validate-key** コマンドを参照してください。

2. LISP トラフィックのインスペクション：ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフローモビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID：ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、EID を 10.10.10.0/24 ネットワーク上の EID に制限する例を示します。

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
cluster flow-mobility lisp	サービス ポリシーのフローモビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。

コマンド	説明
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

allow-ssc-mgmt

ASA 5505 のインターフェイスを SSC 管理インターフェイスとして設定するには、インターフェイス コンフィギュレーション モードで **allow-ssc-mgmt** コマンドを使用します。インターフェイスの割り当てを解除するには、このコマンドの **no** 形式を使用します。

allow-ssc-mgmt
no allow-ssc-mgmt

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、VLAN 1 用の出荷時のデフォルトのコンフィギュレーションでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

SSC に外部インターフェイスはありません。管理 VLAN として VLAN を設定し、バックプレーン経由での内部 IP 管理アドレスへのアクセスを許可できます。デフォルトでは、VLAN 1 は SSC 管理アドレスでイネーブルになります。SSC 管理 VLAN として割り当てることができるのは 1 つの VLAN だけです。

ASDM を使用してアクセスする場合は、管理アドレス用に NAT を設定しないでください。ASDM の初期セットアップでは、実際のアドレスにアクセスする必要があります。初期セットアップ後（SSC でパスワードを設定した後）は、NAT を設定し、SSC にアクセスするときの変換アドレスを ASDM に提供できます。

例

次に、管理アクセスを VLAN 1 でディセーブルにし、VLAN 2 でイネーブルにする例を示します。

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# no allow-ssc-mgmt
ciscoasa(config-if)# interface vlan 2
ciscoasa(config-if)# allow-ssc-mgmt
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。
hw-module module ip	SSC の管理 IP アドレスを設定します。
hw-module module allow-ip	管理IPアドレスにアクセスできるホストを設定します。

allow-tls

TLS セッションを許可または禁止するように ESMTP インスペクションを設定するには、パラメータ コンフィギュレーション モードで **allow-tls** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

allow-tls ［ **action log** ］
no allow-tls

構文の説明

action log	暗号化された接続をログに記録するかどうか。

コマンド デフォルト

allow-tls コマンドが ESMTP インスペクションのデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドが追加されました。
9.4(1)	デフォルトが **allow-tls** から **no allow-tls.** 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。

使用上のガイドライン

ESMTP インスペクションでは、暗号化された接続を検査できません。すべての ESMTP セッションの検査を強制するには、**no allow-tls** コマンドを使用します。TLS を無効にすると、STARTTLS インジケータが接続要求から削除され、強制的にクライアントとサーバーがクリアテキスト接続をネゴシエートします。

クライアントとサーバーが暗号化された接続をネゴシエートできるようにする場合は、ESMTP インスペクション ポリシー マップのパラメータセクションに **allow-tls** コマンドを含め、マップを ESMTP インスペクション サービス ポリシーに接続します。また、_default_esmtp_map（これは独自のマップを適用しない場合に適用されます）を編集することもできます。

例

次に、ESMTP インスペクションをバイパスする暗号化された ESMTP セッションを許可する方法の例を示します。

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allow-tls
```

関連コマンド

コマンド	説明
policy-map type inspect esmtp	インスペクションの ESMTP ポリシーマップを設定します。

always-on-vpn

AnyConnect クライアント Always-On-VPN 機能の動作を設定するには、グループ ポリシー コンフィギュレーション モードで **always-on-vpn** コマンドを使用します。

always-on-vpn [**profile-setting | disable**]

構文の説明

disable	Always-On-VPN 機能をオフにします。
profile-setting	AnyConnect クライアント プロファイルで設定された **always-on-vpn** 設定を使用します。

コマンド デフォルト

Always-On-VPN 機能は、デフォルトでオンになっています。

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

AnyConnect クライアント ユーザーのために Always-On-VPN 機能を有効にするには、プロファイルエディタで AnyConnect クライアント プロファイルを設定します。次に、適切なポリシーのグループ ポリシー属性を設定します。

例

次の例では、設定されたグループ ポリシーに対して Always-On 機能を有効にしています。

```
ciscoasa(config)# group-policy <group policy> attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# always-on-vpn profile-setting
```

関連コマンド

コマンド	説明
webvpn	WebVPN のグループ ポリシーを設定します。

anti-replay

GTP-Uのメッセージシーケンス番号のアンチリプレイを有効にするには、GTPインスペクション ポリシー マップ パラメータ設定モードで **anti-replay** コマンドを使用します。アンチリプレイを無効にするには、このコマンドの **no** 形式を使用します。

anti-replay [*window_size*]
no anti-replay [*window_size*]

構文の説明

window_size	スライディング ウィンドウのサイズはメッセージの数です。ウィンドウのサイズは、128、256、512、または1024になります。値を入力しない場合は、デフォルトの 512 になります。

コマンド デフォルト

デフォルトでは、アンチリプレイは無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが導入されました。

使用上のガイドライン

GTP-U メッセージのスライディング ウィンドウを指定することによって、アンチリプレイを有効にできます。

スライディング ウィンドウのサイズはメッセージの数であり、128、256、512、または1024になります。有効なメッセージが表示されると、ウィンドウは新しいシーケンス番号に移行します。シーケンス番号は 0 ～ 65535 の範囲であり、最大値に達するとラッピングされます。また、これらは PDP コンテキストごとに一意です。メッセージは、シーケンス番号がウィンドウ内であれば有効と見なされます。

アンチリプレイは、ハッカーが GTP データ パケットをキャプチャし、それらをリプレイするときに発生する可能性があるセッション ハイジャックや DoS 攻撃を防ぐのに役立ちます。

例

次の例では、ウィンドウ サイズ 512 のアンチリプレイを有効にしています。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# anti-replay 512
```

関連コマンド

コマンド	説明
inspect gtp	GTP アプリケーション インスペクションをイネーブルにします。
policy-map type inspect gtp	GTP インスペクション ポリシー マップを作成または編集します。
show service-policy inspect gtp	GTP 設定および統計情報を表示します。

anyconnect ask

ASA がリモート SSL VPN クライアントユーザーに対してクライアントのダウンロードを要求するには、グループポリシー webvpn またはユーザー名 webvpn コンフィギュレーション モードで **anyconnect ask** コマンドを使用します。設定からコマンドを削除するには、コマンドの **no** 形式を使用します。

anyconnect ask { **none** | **enable** [**default** { **webvpn** | **anyconnect** } **timeout** *value*] }
no anyconnect ask none [**default** { **webvpn** | **anyconnect** }]

構文の説明

default anyconnect timeout *value*	リモートユーザーにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルトアクション（クライアントのダウンロード）を実行します。
default webvpn timeout *value*	リモートユーザーにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルト アクション（WebVPN ポータル ページの表示）を実行します。
enable	リモートユーザーにクライアントのダウンロードを要求するか、クライアントレス接続のポータルページに移動してユーザー応答を無期限に待機します。
none	デフォルト アクションをただちに実行します。

コマンド デフォルト

このコマンドのデフォルトは、anyconnect **ask none default webvpn** です。ASA によって、クライアントレス接続のポータルページがただちに表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

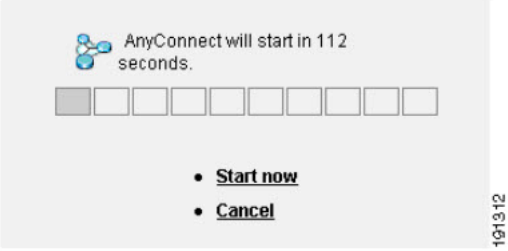
コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.4(1)	svc ask コマンドが anyconnect ask コマンドに置き換えられました。

使用上のガイドライン

<xref> に、**default** anyconnect **timeout** *value* コマンド または **default webvpn timeout** *value* コマンド が設定された場合にリモートユーザーに表示されるプロンプトを示します。

図 *1:* リモート ユーザーに表示される *SSL VPN* クライアントのダウンロードを求めるプロンプト



例

次に、ASA を設定して、リモートユーザーにクライアントのダウンロードを要求するか、ポータル ページに移動して、ユーザーの応答を 10 秒待機してからクライアントをダウンロードするように設定する例を示します。

```
ciscoasa(config-group-webvpn)# anyconnect ask enable default svc timeout 10
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている SSL VPN クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザーに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュメモリで展開するクライアント パッケージ ファイルを指定します。

anyconnect-custom（バージョン 9.0 から 9.2 まで）

カスタム属性の値を設定または更新するには、AnyConnectカスタム属性コンフィギュレーション モードで **anyconnect-custom** コマンドを使用します。カスタム属性の値を削除するには、このコマンドの **no** 形式を使用します。

anyconnect-custom *attr-name* **value** *attr-value*
anyconnect-custom *attr-name* **none**
no anyconnect-custom *attr-name*

構文の説明

attr-name	**anyconnnect-custom-attr** コマンドで定義された、現在のグループポリシーでの属性の名前。
none	デフォルト アクションをただちに実行します。
value *attr-value*	属性値を含む文字列。値は、属性名に関連付けられ、接続の確立時にクライアントに渡されます。450 文字以内で指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AnyConnect カスタム属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、グループ ポリシーにカスタム属性の値を設定します。『*AnyConnect Administrator's Guide*』に、そのリリースに適用されるカスタム属性の有効な値を示します。カスタム属性は、**anyconnect-custom-attr** コマンドで作成します。

属性のマルチライン値を作成するために、このコマンドの複数のインスタンスがサポートされています。特定の属性名に関連付けられたすべてのデータが、CLI で入力された順序に従ってクライアントに提供されます。マルチライン値の個別の行は削除できません。

このコマンドの **no** 形式では、**value** または **none** キーワードは使用できません。

属性名に関連付けられたデータを複数の CLI 行に入力した場合、そのデータは改行文字（\n）で区切られた単一の連結文字列としてエンドポイントに送信されます。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed true
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
anyconnect-custom-attr	カスタム属性を作成します。

anyconnect-custom（バージョン 9.3 以降）

カスタム属性の値を設定または更新するには、グループポリシーまたはダイナミックアクセスポリシー レコード コンフィギュレーション モードで **anyconnect-custom** コマンドを使用します。カスタム属性を削除するには、このコマンドの **no** 形式を使用します。

anyconnect-custom *attr-type* **value** *attr-name*
anyconnect-custom *attr-type* **none**
no anyconnect-custom *attr-type*

構文の説明

attr-type	**anyconnnect-custom-attr** コマンドで定義されたカスタム属性のタイプ。
none	このカスタム属性は、ポリシーから明示的に除外されます。
value *attr-name*	**anyconnect-custom-data** コマンドで定義されたカスタム属性値の名前。 カスタム属性のタイプと名前付き値は、接続の確立時にクライアントに渡されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシーまたはダイナミック アクセス ポリシー レコード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが再定義されました。

使用上のガイドライン

このコマンドは、グループ ポリシーまたは DAP にカスタム属性の値を設定します。

『*AnyConnect Administrator's Guide*』に、そのリリースに適用されるカスタム属性の有効な値を示します。カスタム属性は、**anyconnect-custom-attr** コマンドおよび **anyconnect-custom-data** コマンドで作成します。

このコマンドの **no** 形式では、**none** キーワードは使用できません。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
ciscoasa(config-webvpn)# exit
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed def-allowed
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループポリシーに関する設定情報を表示します。
show running-config dynamic-access-policy-record	DAP ポリシーで使用されるカスタム属性を表示します。
anyconnect-custom-attr	このコマンドで使用されるカスタム属性のタイプを作成します。
anyconnect-custom-data	このコマンドで使用されるカスタム属性の名前付き値を作成します。

anyconnect-custom-attr（バージョン 9.0 から 9.2 まで）

カスタム属性のタイプを作成するには、Anyconnect-custom-attr コンフィギュレーション モードで **anyconnect-custom-attr** コマンドを使用します。カスタム属性を削除するには、この コマンドの **no** 形式を使用します。

[**no**] **anyconnect-custom-attr** *attr-name* [**description** *description*]

構文の説明

attr-name	属性の名前。この名前は、グループ ポリシー構文および集約認証プロトコル メッセージで参照されます。最大長は 32 文字です。
description *description*	属性の使用方法の自由形式の説明。このテキストは、カスタム属性がグループ ポリシー属性コンフィギュレーション モードから参照された場合に、コマンド ヘルプで表示されます。最大長は 128 文字です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AnyConnect カスタム属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、AnyConnect クライアント の特殊機能をサポートするカスタム属性を作成します。特定の機能に対してカスタム属性を作成した後、それらをグループ ポリシーに追加して、機能が VPN クライアントに適用されるようにします。このコマンドでは、定義されたすべての属性名が一意であることが保証されます。

一部のバージョンの AnyConnect クライアント では、機能の設定にカスタム属性が使用されます。各バージョンのリリース ノートおよび『*AnyConnect Administrator's Guide*』に、カスタム属性を必要とするすべての機能を示します。

グループ ポリシーで使用される属性の定義を削除しようとすると、エラー メッセージが表示され、操作は失敗します。ユーザーが既存の属性をカスタム属性として追加しようとすると、説明への変更は組み込まれますが、それ以外についてはコマンドは無視されます。

属性のマルチライン値を作成するために、このコマンドの複数のインスタンスがサポートされています。特定の属性名に関連付けられたすべてのデータが、CLI で入力された順序に従ってクライアントに提供されます。マルチライン値の個別の行は削除できません。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description Indicates
 if the deferred update feature is enabled or not
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
anyconnect-custom	カスタム属性のタイプおよび名前付き値をグループ ポリシーまたはダイナミック アクセス ポリシーに関連付けます。

anyconnect-custom-attr（バージョン 9.3 以降）

カスタム属性のタイプを作成するには、config-webvpn コンフィギュレーション モードで **anyconnect-custom-attr** コマンドを使用します。カスタム属性を削除するには、この コマンドの **no** 形式を使用します。

［ **no** ］**anyconnect-custom-attr** *attr-type*［ **description** *description* ］

構文の説明

attr-type	属性のタイプ。このタイプは、グループ ポリシー構文、DAP ポリシー構文、および集約認証プロトコル メッセージで参照されます。最大長は 32 文字です。
description *description*	属性の使用方法の自由形式の説明。このテキストは、カスタム属性がグループ ポリシー属性コンフィギュレーション モードから参照された場合に、コマンド ヘルプで表示されます。最大長は文字です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
config-webvpn	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが再定義されました。

使用上のガイドライン

このコマンドは、AnyConnect クライアント の特殊機能をサポートするカスタム属性を作成します。特定の機能に対してカスタム属性を作成した後、その属性の値を定義し、その属性をグループ ポリシーに追加して、対応する機能が VPN クライアントに適用されるようにします。このコマンドでは、定義されたすべての属性名が一意であることが保証されます。

一部のバージョンの AnyConnect クライアント では、機能の設定にカスタム属性が使用されます。各バージョンのリリース ノートおよび『*AnyConnect Administrator's Guide*』に、カスタム属性を必要とするすべての機能を示します。

グループ ポリシーで使用される属性の定義を削除しようとすると、エラー メッセージが表示され、操作は失敗します。ユーザーが既存の属性をカスタム属性として追加しようとすると、説明への変更は組み込まれますが、それ以外についてはコマンドは無視されます。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description Indicates
 if the deferred update feature is enabled or not
```

ciscoasa(config)# **anyconnect-custom-data DeferredUpdateAllowed def-allowed true**

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
show running-config dynamic-access-policy-record	DAP ポリシーで使用されるカスタム属性を表示します。
anyconnect-custom	ポリシーで使用するためのカスタム属性の値を設定します。
anyconnect-custom-data	カスタム属性の名前付き値を作成します。

anyconnect-custom-data

カスタム属性の名前付き値を作成するには、グローバル コンフィギュレーション モードで **anyconnect-custom-data** コマンドを使用します。カスタム属性を削除するには、この コマンドの **no** 形式を使用します。

anyconnect-custom-data *attr-type attr-name attr-value*
no anyconnect-custom-data *attr-type attr-name*

構文の説明

attr-type	**anyconnect-custom-attr** を使用して以前に定義された属性のタイプ。
attr-name	指定した値を持つ属性の名前。これは、グループ ポリシーおよびダイナミック アクセス ポリシー レコード コンフィギュレーション モードで参照できます。
attr-value	属性値を含む文字列。 最大 420 文字です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、AnyConnect クライアント の特殊機能をサポートするカスタム属性の名前付き値を定義します。特定の機能に対してカスタム属性を作成した後、その属性の値を定義し、その属性を DAP またはグループ ポリシーに追加して、対応する機能が VPN クライアントに適用されるようにします。

一部のバージョンの AnyConnect クライアント では、機能の設定にカスタム属性が使用されます。各バージョンのリリース ノートおよび『*AnyConnect Administrator's Guide*』に、カスタム属性を必要とするすべての機能を示します。

グループ ポリシーで使用される属性の名前付き値を削除しようとすると、エラー メッセージが表示され、操作は失敗します。

属性のマルチライン値を作成するために、このコマンドの複数のインスタンスがサポートされています。特定の属性名に関連付けられたすべてのデータが、CLI で入力された順序に従ってクライアントに提供されます。マルチライン値の個別の行は削除できません。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
show running-config dynamic-access-policy-record	DAP ポリシーで使用されるカスタム属性を表示します。
show run anyconnect-custom-data	定義されているすべてのカスタム属性の名前付き値を表示します。
anyconnect-custom	カスタム属性のタイプおよび値をグループ ポリシーまたは DAP に関連付けます。
anyconnect-custom-attr	カスタム属性を作成します。

anyconnect df-bit-ignore

フラグメンテーションが必要なパケットのDFビットを無視するには、グループポリシーwebvpnコンフィギュレーション モードで **anyconnect-df-bit-ignore** コマンドを使用します。フラグメンテーションが必要な DF ビットを許可するには、このコマンドの **no** 形式を使用します。

anyconnect df-bit-ignore { **enable** | **none** }
no anyconnect df-bit-ignore { **enable** | **none** }

構文の説明

enable	AnyConnect クライアントに対して DF ビットの無視を有効にします。
none	AnyConnect クライアント に対して DF ビットを無効にします。

コマンド デフォルト

デフォルトでは、このオプションはイネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(2)	**svc df-bit-ignore** コマンドが追加されました。
8.4(3)	svc df-bit-ignore コマンドが anyconnect df-bit-ignore コマンドに置き換えられました。

例

```
vmb-5520(config-group-webvpn)# anyconnect routing-filtering-ignore ?
config-group-webvpn mode commands/options:
  enable  Enable Routing/Filtering for AnyConnect Client
  none    Disable Routing/Filtering for AnyConnect Client
```

anyconnect dpd-interval

デッドピア検出（DPD）をASAでイネーブルにし、リモートクライアントとASAのいずれかでSSL VPN接続を介したDPDを実行する頻度を設定するには、グループ ポリシー webvpn またはユーザー名 webvpn コンフィギュレーション モードで anyconnect **dpd-interval** コマンドを使用します。コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect dpd-interval { [**gateway** { *seconds* | **none** }] | [**client** { *seconds* | **none** }] }
no anyconnect dpd-interval { [**gateway** { *seconds* | **none** }] | [**client** { *seconds* | **none** }] }

構文の説明

client なし	クライアントで実行される DPD をディセーブルにします。
client seconds	クライアントで DPD が実行される頻度（30 ～ 3600 秒）を指定します。
gateway none	ASA で実行される DPD テストをディセーブルにします。
gateway seconds	ASA で DPD が実行される頻度（30 ～ 3600 秒）を指定します。値 300 が推奨されます。

コマンド デフォルト

デフォルトでは、DPD はイネーブルであり、ASA（ゲートウェイ）とクライアントの両方で 30 秒に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

リリース	変更内容
8.0(3)	デフォルト設定が、ディセーブルから、ASA（ゲートウェイ）とクライアントの両方で 30 秒に変更されました。
8.4(1)	svc dpd-interval コマンドが anyconnect dpd-interval コマンドに置き換えられました。

使用上のガイドライン

gateway は、ASA のことです。DPD をイネーブルにし、ASA がクライアントからのパケットを待機する間隔を指定します。その間隔内にパケットが受信されない場合、ASA は同じ間隔で DPD テストを 3 回試行します。クライアントからの応答を受信しない場合、ASA は TLS/DTLS トンネルを切断します。

ASA の DPD プロセスは、TLS/DTLS トンネルを介してクライアントに送信するパケットが ASA にある場合にのみトリガーされます。

例

次に、既存のグループポリシー *sales* について、ASA（ゲートウェイ）で実行される DPD の頻度を 3000 秒に設定し、クライアントで実行される DPD の頻度を 1000 秒に設定する例を示します。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect dpd-interval gateway 3000
ciscoasa(config-group-webvpn)# anyconnect dpd-interval client 1000
```

anyconnect dtls compression

特定のグループまたはユーザーに対して低帯域幅リンクの圧縮を有効にするには、グループポリシー webvpn またはユーザー名 webvpn コンフィギュレーション モードで AnyConnect クライアント **dtls compression** コマンドを使用します。グループからコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

anyconnect dtls compression { **lzs** | **none** }
no anyconnect dtls compression { **lzs** | **none** }

構文の説明

lzs	ステートレス圧縮アルゴリズムをイネーブルにします。
none	圧縮をディセーブルにします。

コマンド デフォルト

デフォルトでは、AnyConnect クライアント 圧縮は有効になっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

例

次に、圧縮をディセーブルにするシーケンスの例を示します。

```
asa# config terminal
asa(config)# group-policy DfltGrpPolicy attributes
asa(config-group-policy)# webvpn
asa(config-group-webvpn)# anyconnect ssl compression none
asa(config-group-webvpn)# anyconnect dtls compression none
```

anyconnect enable

ASA が AnyConnect クライアント をリモートコンピュータにダウンロードする、または SSL または IKEv2 搭載の AnyConnect クライアント を使用して ASA に接続できるようにするには、webvpn コンフィギュレーション モードで anyconnect enable コマンドを使用します。設定からコマンドを削除するには、コマンドの **no** 形式を使用します。

anyconnect enable
no anyconnect enable

コマンド デフォルト

このコマンドのデフォルトはディセーブルです。ASA はクライアントをダウンロードしません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが svc enable として追加されました。
8.4(1)	svc enable コマンドが anyconnect enable コマンドに置き換えられました。

使用上のガイドライン

no anyconnect enable コマンドを入力しても、アクティブなセッションは終了しません。

anyconnect enable コマンドは、**anyconnect image xyz** コマンドで AnyConnect クライアント イメージを設定してから発行する必要があります。AnyConnect クライアント または AnyConnect クライアント weblaunch を使用するには、**anyconnect enable** が必要です。 **anyconnect enable** コマンドを SSL または IKEv2 とともに発行しないと、AnyConnect クライアント は想定どおりに動作せず、IPsec VPN 接続終了エラーでタイムアウトします。その結果、**show webvpn svc** コマンドは SSL VPN クライアントが有効になっていると見なさず、インストールされた AnyConnect クライアント パッケージを一覧表示しません。

例

次に、ASA でクライアントをダウンロードできるようにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect enable
```

関連コマンド

コマンド	説明
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュメモリで展開する AnyConnect SSL VPN クライアント パッケージ ファイルを指定します。
anyconnect modules	AnyConnect SSL VPN Client でオプション機能に必要なモジュールの名前を指定します。
anyconnect profiles	ASA によって Cisco AnyConnect SSL VPN Client にダウンロードされるプロファイルを保管するために使用するファイルの名前を指定します。
show webvpn anyconnect	ASA にインストールされ、リモート PC へのダウンロード用にキャッシュメモリにロードされた SSL VPN クライアントの情報を表示します。
anyconnect localization	Cisco AnyConnect VPN Client にダウンロードされたローカリゼーション ファイルを保管するために使用するパッケージ ファイルを指定します。

anyconnect-essentials

ASA の AnyConnect Essentials をイネーブルにするには、グループポリシー webvpn コンフィギュレーション モードで **anyconnect-essentials** コマンドを使用します。AnyConnect Essentials の使用を無効にし、プレミアム AnyConnect クライアント を有効にするには、このコマンドの **no** 形式を使用します。

anyconnect-essentials
no anyconnect-essentials

コマンド デフォルト

AnyConnect Essentials は、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、AnyConnect SSL VPN クライアント全体の使用と AnyConnect Essentials SSL VPN クライアントの使用を切り替えます（完全な AnyConnect クライアント ライセンスがインストールされている場合）。AnyConnect Essentials は個別にライセンス供与される SSL VPN クライアントで、すべて ASA 上に設定されます。プレミアム AnyConnect クライアントの機能が提供されますが、次の例外があります。

- CSD を使用できない（HostScan/Vault/Cache Cleaner を含む）
- クライアントレス SSL VPN 非対応

AnyConnect Essentials クライアントは、Microsoft Windows Vista、Windows Mobile、Windows XP、Windows 2000、Linux、または Macintosh OS X を実行しているリモート エンド ユーザーに Cisco SSL VPN Client の利点をもたらします。

AnyConnect Essentials ライセンスは、**anyconnect-essentials** コマンドを使用してイネーブルまたはディセーブルにします。このコマンドは、AnyConnect Essentials ライセンスが ASA にインストールされている場合にのみ有効です。このライセンスがない場合は、このコマンドを実行すると次のエラー メッセージが表示されます。

```
ERROR: Command requires AnyConnect Essentials license
```

（注） このコマンドは、AnyConnect Essentials の使用をイネーブルまたはディセーブルにするだけです。AnyConnect Essentials ライセンス自体は、**anyconnect-essentials** コマンドの設定の影響を受けません。

AnyConnect Essentials ライセンスが有効になっている場合、AnyConnect クライアントは Essentials モードを使用し、クライアントレス SSL VPN アクセスは無効になります。AnyConnect Essentials ライセンスが無効になっている場合、AnyConnect クライアントは完全な AnyConnect SSL VPN クライアントライセンスを使用します。

（注） このコマンドは、ASA 仮想 またはデバイスではサポートされていません。詳細については、ライセンスのマニュアルを参照してください。

アクティブなクライアントレス SSL VPN 接続がある場合に AnyConnect Essentials ライセンスをイネーブルにすると、すべての接続がログオフするため、接続を再確立する必要があります。

例

次に、ユーザーが webvpn コンフィギュレーション モードを開始して AnyConnect Essentials VPN Client をイネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect-essentials
```

anyconnect external-browser-pkg

AnyConnect クライアント 外部ブラウザパッケージのパスを設定するには、webvpn コンフィギュレーション モードで **anyconnect external-browser-pkg** コマンドを使用します。外部ブラウザのパスを削除するには、このコマンドの **no** 形式を使用します。

anyconnect external-browser-pkg { *package path* }

no anyconnect external-browser-pkg { *package path* }

構文の説明

{*packagepath*} シングルサインオン認証に使用するデバイス上の外部ブラウザパッケージのパスを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
WebVPN コンフィギュレーション	• 対応	• —	• 対応	• —	• —

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、AnyConnect クライアント は SAML シングルサインオン認証に組み込みのブラウザを使用します。SAML 認証にオペレーティングシステムのデフォルトのブラウザ（プラットフォームのネイティブブラウザ）を使用するように設定できます。オペレーティングシステムのデフォルトのブラウザを選択するには、AnyConnect クライアント がシングルサインオン認証にデフォルトの OS ブラウザを使用するための外部ブラウザパッケージが必要です。

anyconnect external-browser-pkg コマンドを使用すると、AnyConnect クライアント シングルサインオン認証に使用する外部ブラウザのパスを設定できます。

次に、**anyconnect external-browser-pkg** コマンドを使用して、AnyConnect クライアント シングルサインオン認証に使用する外部ブラウザのパスを設定する例を示します。

```
ciscoasa
#
```

```
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-webvpn)# anyconnect external-browser-pkg disk0:
```

関連コマンド

コマンド	説明
external-browser	AnyConnect クライアント 外部ブラウザによるシングルサインオン認証を設定します。
tunnel-group	VPN 接続プロファイルを作成するか、または VPN 接続プロファイルのデータベースにアクセスします。
show webvpnanyconnect external-browser-pkg	指定したシングルサインオン パッケージ ファイルに関する情報を表示します。

anyconnect firewall-rule

パブリックまたはプライベートの ACL ファイアウォールを確立するには、グループポリシー webvpn またはユーザー名 webvpn コンフィギュレーション モードで **anyconnect firewall-rule** コマンドを使用します。

anyconnect firewall-rule client interface { **public** | **private** } *ACL*

構文の説明

ACL	アクセス コントロール リストを指定します。
client interface	クライアント インターフェイスを指定します。
private	プライベート インターフェイス ルールを設定します。
public	パブリック インターフェイス ルールを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	この svc firewall-rule コマンドが追加されました。
8.4(1)	svc firewall-rule コマンドが anyconnect firewall-rule コマンドに置き換えられました。
9.0(1)	コマンドの ACL を、IPv4 アドレスと IPv6 アドレスの両方を指定できるユニファイド アクセス コントロール ルールにすることができるようになりました。

使用上のガイドライン

このコマンドを想定どおりに機能させるためには、AnyConnect クライアントの AnyConnect セキュア モビリティ ライセンス サポートを提供する AsyncOS for Web バージョン 7.0 のリリースが必要です。また、AnyConnect クライアント、ASA 8.3、ASDM 6.3 をサポートする AnyConnect クライアント リリースが必要です。

以下は、AnyConnect クライアント でのファイアウォールの使用方法に関する注意事項です。

- ファイアウォール ルールには送信元 IP は使用されません。クライアントでは、ASA から送信されたファイアウォール ルール内の送信元 IP 情報は無視されます。送信元 IP は、ルールがパブリックかプライベートかに応じてクライアントが特定します。パブリック ルールは、クライアント上のすべてのインターフェイスに適用されます。プライベート ルールは、仮想アダプタに適用されます。
- ASA は、ACL ルールに対して数多くのプロトコルをサポートしています。ただし、AnyConnect のファイアウォール機能でサポートされているのは、TCP、UDP、ICMP、および IP のみです。クライアントでは、異なるプロトコルでルールが受信された場合、そのルールは無効なファイアウォール ルールとして処理され、さらにセキュリティ上の理由からスプリット トンネリングが無効となり、フル トンネリングが使用されます。

ただし次のように、オペレーティング システムによって動作が異なるため注意が必要です。

- Windows コンピュータの場合、Windows Firewall では拒否ルールが許可ルールに優先します。ASA により許可ルールが AnyConnect クライアント にプッシュされても、ユーザーがカスタムの拒否ルールを作成している場合、AnyConnect クライアント ルールは適用されません。
- Windows Vista では、ファイアウォール ルールが作成されると、ポート番号の範囲がカンマ区切りの文字列として認識されます（たとえば、1 ～ 300 や 5000 ～ 5300）。許可されているポートの最大数は 300 です。指定した数が 300 ポートを超える場合は、最初の 300 ポートに対してのみファイアウォール ルールが適用されます。
- ファイアウォールサービスが AnyConnect クライアント により開始される必要がある（システムにより自動的に開始されない）Windows ユーザーは、VPN 接続の確立時間が大幅に増える場合があります。
- Mac コンピュータの場合、AnyConnect クライアント では、ASA で適用された順序と同じ順序でルールが適用されます。グローバル ルールは必ず最後になるようにしてください。
- サードパーティ ファイアウォールの場合、AnyConnect クライアント ファイアウォールとサードパーティ ファイアウォールの両方で許可されているトラフィック タイプのトラフィックのみ通過できます。AnyConnect クライアント で許可されている特定のトラフィック タイプがサードパーティ ファイアウォールでブロックされる場合、そのタイプのトラフィックはクライアントでブロックされます。

ローカル印刷およびテザーデバイスサポートに関する ACL ルールの例を含め、AnyConnect クライアント ファイアウォールの詳細については、AnyConnect 管理者ガイド [英語] を参照してください。

例

次に、ACL AnyConnect_Client_Local_Print をパブリック ファイアウォールとしてイネーブルにする例を示します。

```
ciscoasa(config)# group-policy example_group attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect firewall-rule client-interface public value
AnyConnect_Client_Local_Print
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている SSL VPN クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザーに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュメモリで展開するクライアント パッケージ ファイルを指定します。

anyconnect image

AnyConnect クライアント 配布パッケージをインストールまたはアップグレードして、実行コンフィギュレーションに追加するには、webvpn コンフィギュレーション モードで anyconnect image コマンドを使用します。AnyConnect クライアント 配布パッケージを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

anyconnect image *path* **order** [**regex** *expression*]
no anyconnect image *path* **order** [**regex** *expression*]

構文の説明

order	クライアントパッケージファイルが複数である場合は、パッケージファイルの順序（1 ～ 65535）を指定します。ASA では、オペレーティングシステムと一致するまで、指定した順序に従って、各クライアントの一部をリモート PC にダウンロードします。
path	AnyConnect クライアント パッケージのパスおよびファイル名を 255 文字以内で指定します。
regex *expression*	ブラウザから渡される user-agent 文字列と照合するために ASA によって使用される文字列を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが svc image として追加されました。
8.0(1)	**regex** キーワードが追加されました。
8.4(1)	svc image コマンドが AnyConnect クライアント image コマンドに置き換えられました。

使用上のガイドライン

パッケージファイルの番号付けにより、ASAが、オペレーティングシステムと一致するまで、パッケージファイルの一部をリモート PC にダウンロードする順序が確立されます。最も番号の小さいパッケージ ファイルが最初にダウンロードされます。したがって、リモート PC で最も一般的に使用されるオペレーティング システムと一致するパッケージ ファイルに、最も小さい番号を割り当てる必要があります。

デフォルトの順序は 1 です。*order* 引数を指定しない場合は、**svc image** コマンドを入力するたびに、以前に番号 1 と見なされたイメージに上書きします。

クライアント パッケージ ファイルごとに任意の順序で **anyconnect image** コマンドを入力できます。たとえば、2番目（*order* 2）にダウンロードされるパッケージファイルを指定してから、最初（*order* 1）にダウンロードされるパッケージファイルを指定する **anyconnect image** コマンドを入力できます。

モバイルユーザーの場合、 **regex keyword** を使用してモバイルデバイスの接続時間を短縮できます。ブラウザは ASA に接続するときに、HTTP ヘッダーに User-agent 文字列を含めます。ASAが文字列を受信し、その文字列がいずれかのイメージ用に設定された式と一致すると、他のクライアント イメージはテストされず、一致したイメージがただちにダウンロードされます。

（注） スタンドアロンクライアントを使用している場合、**regex** コマンドは無視されます。また、パフォーマンス向上のため Web ブラウザでのみ使用され、正規表現文字列はスタンドアロン クライアントから提供されるユーザーまたはエージェントと照合されません。

ASA では、AnyConnect クライアント と Cisco Secure Desktop（CSD）の両方のパッケージファイルがキャッシュメモリに展開されます。ASA でパッケージファイルを正常に展開するには、パッケージファイルのイメージとファイルを保管するのに十分なキャッシュメモリが必要です。

パッケージの展開に十分なキャッシュメモリがないことを ASA が検出した場合、コンソールにエラーメッセージが表示されます。次に、**svc image** コマンドを使用してパッケージファイルをインストールしようとした後でレポートされるエラーメッセージの例を示します。

```
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0520-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

これがパッケージファイルのインストール試行中に発生した場合、グローバル コンフィギュレーション モードから **dir cache:/** コマンドを使用して、キャッシュメモリの残りとこれまでにインストールされたパッケージのサイズを確認します。

（注） ASA にデフォルトの内部フラッシュメモリサイズまたはデフォルトの DRAM サイズ（キャッシュメモリ用）のみ存在する場合、ASA 上で複数の AnyConnect クライアントパッケージを保存およびロードすると、問題が発生することがあります。フラッシュメモリにパッケージファイルに十分な容量がある場合でも、クライアントの unzip とロードのときに ASA のキャッシュメモリが不足する場合があります。AnyConnect クライアントを展開する場合の ASA のメモリ要件、および ASA メモリのアップグレード（可能な場合）の詳細については、ASA 5500 シリーズの最新のリリースノートを参照してください。

例

次に、Windows、MAC、Linux 用の AnyConnect クライアント パッケージファイルをこの順序でロードする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect image
 disk0:/anyconnect-win-3.0.0527-k9.pkg 1
ciscoasa(config-webvpn)# anyconnect image
 disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2
ciscoasa(config-webvpn)# anyconnect image
 disk0:/anyconnect-linux-3.0.0414-k9.pkg 3
ciscoasa(config-webvpn)
```

次に、ロードされた AnyConnect クライアント パッケージとその順序を表示する、show webvpn AnyConnect クライアント コマンドの出力例を示します。

```
ciscoasa(config-webvpn)# show webvpn anyconnect
1. disk0:/anyconnect-win-3.0.0527-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,0,0527
  Hostscan Version 3.0.0527
  Tue 10/19/2010 16:16:56.25
2. disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2 dyn-regex=/Intel Mac OS X/
  CISCO STC Darwin_i386
  3.0.0414
  Wed Oct 20 20:39:53 MDT 2010
3. disk0:/anyconnect-linux-3.0.0414-k9.pkg 3 dyn-regex=/Linux i[1-9]86/
  CISCO STC Linux
  3.0.0414
  Wed Oct 20 20:42:02 MDT 2010
3 AnyConnect Client(s) installed
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
anyconnect modules	AnyConnect SSL VPN Client でオプション機能に必要なモジュールの名前を指定します。
anyconnect profiles	ASA によって Cisco AnyConnect SSL VPN Client にダウンロードされるプロファイルを保管するために使用するファイルの名前を指定します。

コマンド	説明
show webvpn anyconnect	ASA にインストールされ、リモート PC へのダウンロード用にキャッシュメモリにロードされた SSL VPN クライアントの情報を表示します。
anyconnect localization	Cisco AnyConnect VPN Client にダウンロードされたローカリゼーション ファイルを保管するために使用するパッケージ ファイルを指定します。

anyconnect keep-installer

（注） このコマンドは、2.5 より後の AnyConnect クライアント バージョンには適用されませんが、後方互換性のために引き続き使用できます。**anyconnect keep-installer** コマンドを設定しても、AnyConnect クライアント 3.0 以降には影響しません。

リモート PC への SSL VPN クライアントの永続インストールをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードで、AnyConnect keep-installer コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect keep-installer { **installed** | **none** }
no anyconnect keep-installer { **installed** | **none** }

構文の説明

installed	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
none	アクティブな接続の終了後にクライアントがリモート コンピュータからアンインストールされることを指定します。

コマンド デフォルト

デフォルトでは、クライアントの永続インストールがイネーブルです。セッションの終了時に、クライアントはリモート コンピュータ上に残ります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	svc keep-installer コマンドが追加されました。
8.4(1)	svc keep-installer コマンドが anyconnect keep-installer コマンドに置き換えられました。

例

次の例では、ユーザーはグループ ポリシー webvpn コンフィギュレーション モードを開始し、セッションの終了時にクライアントを削除するようにグループ ポリシーを設定します。

```
ciscoasa(config-group-policy)#webvpn
ciscoasa(config-group-webvpn)# anyconnect keep-installer none
ciscoasa(config-group-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn anyconnect	ASA にインストールされ、リモート PC へのダウンロード用にキャッシュメモリにロードされた AnyConnect クライアント に関する情報を表示します。
anyconnect	特定のグループまたはユーザーに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect enable	ASA が AnyConnect クライアント ファイルをリモート PC にダウンロードできるようにします。
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュメモリで展開する AnyConnect クライアント パッケージファイルを指定します。

anyconnect modules

オプション機能のために AnyConnect SSL VPN Client で必要となるモジュールの名前を指定するには、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーションモードで、**anyconnect modules** コマンドを使用します。設定からコマンドを削除するには、コマンドの **no** 形式を使用します。

anyconnect modules { **none** | **value** *string* }
no anyconnect modules { **none** | **value** *string* }

構文の説明

string オプションモジュールの名前（最大 256 文字）。 複数のストリングを指定する場合は、カンマで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	svc modules コマンドが追加されました。
8.4(1)	svc modules コマンドが anyconnect modules コマンドに置き換えられました。

使用上のガイドライン

ダウンロード時間を最小にするために、クライアントでは、サポートする各機能に必要なモジュールのダウンロード（ASA から）のみを要求します。**anyconnect modules** コマンドにより、ASA でこれらのモジュールをダウンロードできます。

次の表に、AnyConnect モジュールを表す文字列値を示します。

AnyConnect モジュールを表す文字列	AnyConnect モジュール名
dart	AnyConnect DART（診断およびレポート ツール）
nam	AnyConnect ネットワーク アクセス マネージャ
vpngina	AnyConnect SBL（ログイン前の起動）
websecurity	AnyConnect Web セキュリティ モジュール
telemetry	AnyConnect テレメトリ モジュール
posture	AnyConnect ポスチャ モジュール
none	**none** を選択すると、ASA によって基本的なファイルがダウンロードされ、オプションのモジュールはダウンロードされません。既存のモジュールはグループ ポリシーから削除されます。

例

次の例では、ユーザーはグループ ポリシー *PostureModuleGroup* のグループ ポリシー属性モードを開始し、そのグループ ポリシーの webvpn コンフィギュレーション モードを開始しています。さらに、ASA に接続すると AnyConnect ポスチャ モジュールおよび AnyConnect テレメトリ モジュールがエンドポイントにダウンロードされるように、文字列 *posture* および *telemetry* を指定しています。

```
ciscoasa> en

Password:
ciscoasa# config t
ciscoasa(config)# group-policy PostureModuleGroup attributes

ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect modules value posture,telemetry

ciscoasa(config-group-webvpn)# write mem

Building configuration...
Cryptochecksum: 40975338 b918425d 083b391f 9e5a5c69
22055 bytes copied in 3.440 secs (7351 bytes/sec)
[OK]
ciscoasa(config-group-webvpn)#
```

グループ ポリシーからモジュールを削除するには、保持するモジュールの値だけを指定したコマンドを再送信します。たとえば、このコマンドはテレメトリ モジュールを削除します。

```
ciscoasa(config-group-webvpn)# anyconnect modules value posture
```

関連コマンド

コマンド	説明
show webvpn anyconnect	ASA のキャッシュメモリにロードされていてダウンロード可能な AnyConnect クライアント パッケージについての情報を表示します。
anyconnect enable	特定のグループまたはユーザーに対して、AnyConnect クライアントを有効にします。
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュメモリで展開する AnyConnect クライアント パッケージファイルを指定します。

anyconnect mtu

Cisco AnyConnect VPN Client によって確立された VPN 接続の MTU サイズを調整するには、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードで、**anyconnect mtu** コマンドを使用します。設定からコマンドを削除するには、コマンドの **no** 形式を使用します。

anyconnect mtu *size*
no anyconnect mtu *size*

構文の説明

size	MTU サイズ（バイト単位）。576 ～ 1406 バイトです。

コマンド デフォルト

デフォルトのサイズは 1406 バイトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	svc mtu コマンドが追加されました。
8.4(1)	svc mtu コマンドが anyconnect mtu コマンドに置き換えられました。

使用上のガイドライン

このコマンドは、AnyConnect クライアント のみに影響します。VPN Client は、異なる MTU サイズに調整できません。

デフォルトのグループポリシーでのこのコマンドのデフォルトは、**no svc mtu** です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

例

次の例では、グループポリシー >*telecommuters* の MTU サイズを 500 バイトに設定します。

```
ciscoasa(config)# group-policy telecommuters attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect mtu 500
```

関連コマンド

コマンド	説明
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。初期ダウンロード後、接続が終了した後もクライアントはリモート PC 上に残ります。
anyconnect ssl dtls	SSL VPN 接続を確立する CVC に対して DTLS をイネーブルにします。
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。

anyconnect profiles（グループ ポリシー属性 webvpn、ユーザー名属性 webvpn）

Cisco AnyConnect VPN Client（CVC）ユーザーにダウンロードされる CVC プロファイルパッケージを指定するには、webvpn またはコンフィギュレーション モードで **anyconnect profiles** コマンドを使用します。webvpn コンフィギュレーション モードにアクセスするには、最初にグループ ポリシー属性コマンドまたはユーザー名属性を入力します。コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect profiles { **value** プロファイル | **none** } [**type** *type*]
no anyconnect profiles { **value** プロファイル | **none** } [**type** *type*]

構文の説明

value *profile*	プロファイル名。
none	ASA によってプロファイルはダウンロードされません。
type *type*	（任意）プロファイル タイプデフォルトは **user** です。次のいずれかを指定します。 • **user**：AnyConnect VPN プロファイル。 • **vpn-mgmt**：AnyConnect 管理 VPN プロファイル。 • **umbrella**：Umbrella ローミング セキュリティ プロファイル • **ampenabler**：AMP イネーブラ サービス プロファイル • **websecurity**：Web セキュリティ サービス プロファイル • **nam**：NAM サービスモジュール • **iseposture**：ISE ポスチャプロファイル • **nvm**：ネットワーク可視性サービスプロファイル

コマンド デフォルト

デフォルトは none です。ASA によってプロファイルはダウンロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	svc profiles コマンドが追加されました。
8.3(1)	オプションのタイプ **value** が追加されました。
8.4(1)	svc profiles コマンドが anyconnect profiles コマンドに置き換えられました。

使用上のガイドライン

このコマンドをグループポリシー webvpn コンフィギュレーション モードまたはユーザー名属性 webvpn コンフィギュレーション モードで入力すると、ASA によってグループポリシーまたはユーザー名に基づいてプロファイルを CVC ユーザーにダウンロードできます。CVC プロファイルをすべての CVC ユーザーにダウンロードするには、このコマンドを webvpn コンフィギュレーション モードで使用します。

CVC プロファイルとは、CVC ユーザー インターフェイスに表示される接続エントリを設定するために CVC が使用するコンフィギュレーションパラメータのグループで、ホスト コンピュータの名前とアドレスが含まれます。CVC ユーザー インターフェイスを使用して、プロファイルを作成および保存できます。また、テキスト エディタでこのファイルを編集し、ユーザー インターフェイスからは設定できないパラメータの詳細を設定することもできます。

CVC のインストレーションには、他のプロファイル ファイルを編集し、作成するための基礎として使用できる、1 つのプロファイル テンプレート（cvcprofile.xml）が含まれています。CVC プロファイルの編集の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

例

次の例では、ユーザーは使用可能なプロファイルを表示する **anyconnect profiles value** コマンドを入力します。

```
ciscoasa(config-group-webvpn)# anyconnect profiles value ?
config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

次に、ユーザーは CVC プロファイル sales を使用するようにグループ ポリシーを設定します。

```
ciscoasa(config-group-webvpn)# anyconnect profiles sales
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている AnyConnect クライアント に関する情報を表示します。
anyconnect	特定のグループまたはユーザーにSSL VPNクライアントをイネーブルにします。または、要求します。
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュメモリで展開する AnyConnect クライアント パッケージファイルを指定します。

anyconnect profiles（webvpn）

ASA によってキャッシュメモリにロードされて、Cisco AnyConnect VPN Client（CVC）ユーザーのグループポリシーおよびユーザー名属性で使用可能となるプロファイルパッケージとしてファイルを指定するには、webvpn コンフィギュレーション モードで **anyconnect profiles** コマンドを使用します。コンフィギュレーションからこのコマンドを削除し、ASA によってパッケージファイルがキャッシュメモリからアンロードされるようにするには、このコマンドの **no** 形式を使用します。

anyconnect profiles { *profile path* }
no anyconnect profiles { *profile path* }

構文の説明

path	ASA のフラッシュメモリ内のプロファイルファイルのパスおよびファイル名。
profile	キャッシュメモリ内に作成するプロファイルの名前。

コマンド デフォルト

デフォルトは none です。プロファイルパッケージは ASA によってキャッシュメモリにロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	svc profiles コマンドが追加されました。
8.4(1)	svc profiles コマンドが anyconnect profiles コマンドに置き換えられました。

使用上のガイドライン

CVC プロファイルとは、CVC ユーザー インターフェイスに表示される接続エントリを設定するために CVC が使用するコンフィギュレーションパラメータのグループで、ホスト コンピュータの名前とアドレスが含まれます。CVC ユーザー インターフェイスを使用して、プロファイルを作成および保存できます。

また、テキスト エディタでこのファイルを編集し、ユーザー インターフェイスからは設定できないパラメータの詳細を設定することもできます。CVC のインストレーションには、他の

プロファイルファイルを編集し、作成するための基礎として使用できる、1 つのプロファイルテンプレート（cvcprofile.xml）が含まれています。CVC プロファイルの編集の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

新しい CVC プロファイルを作成してフラッシュメモリにアップロードした後、webvpn コンフィギュレーション モードで **anyconnect profiles** コマンドを使用して、ASA に対して XML ファイルをプロファイルとして指定します。このコマンドを入力すると、ファイルは ASA のキャッシュメモリにロードされます。次に、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名属性コンフィギュレーション モードで **anyconnect profiles** コマンドを使用して、グループまたはユーザーのプロファイルを指定できます。

例

次の例では、ユーザーは、以前に CVC のインストールで提供された cvcprofile.xml ファイルから 2 つの新しいプロファイルファイル（sales_hosts.xml および engineering_hosts.xml）を作成し、ASA のフラッシュメモリにアップロードしています。

さらに、ユーザーはそれらのファイルを CVC のプロファイルとして ASA に指定し、*>sales* と *>engineering* という名前を指定しています。

```
ciscoasa(config-webvpn)# anyconnect profiles sales disk0:sales_hosts.xml
ciscoasa(config-webvpn)# anyconnect profiles engineering disk0:engineering_hosts.xml
```

dir cache:stc/profiles コマンドを入力すると、キャッシュメモリにロードされているプロファイルが表示されます。

```
ciscoasa(config-webvpn)# dir cache:stc/profiles
Directory of cache:stc/profiles/
0      ----  774         11:54:41 Nov 22 2006  engineering.pkg
0      ----  774         11:54:29 Nov 22 2006  sales.pkg
2428928 bytes total (18219008 bytes free)
ciscoasa(config-webvpn)#
```

これらのプロトコルは、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名属性コンフィギュレーション モードでの **svc profiles** コマンドで使用できます。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect profiles value ?
config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている AnyConnect クライアント に関する情報を表示します。
anyconnect	特定のグループまたはユーザーに対して SSL VPN クライアントをイネーブルまたは必須にします。

コマンド	説明
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュメモリで展開する AnyConnect クライアント パッケージファイルを指定します。

anyconnect ssl compression

特定のグループまたはユーザーについて、SSL VPN 接続での http データの圧縮をイネーブルにするには、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードで、anyconnect **ssl compression** コマンドを使用します。コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl compression { **deflate** | **lzs** | **none** }
no anyconnect ssl compression { **deflate** | **lzs** | **none** }

構文の説明

deflate	デフレート圧縮アルゴリズムをイネーブルにします。
lzs	ステートレス圧縮アルゴリズムをイネーブルにします。
none	圧縮をディセーブルにします。

コマンド デフォルト

デフォルトでは、圧縮は none（ディセーブル）に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	**anyconnect compression** コマンドが追加されました。

使用上のガイドライン

SSL VPN 接続の場合、webvpn コンフィギュレーション モードで設定された **compression** コマンドによって、グループポリシー webvpn モードおよびユーザー名 webvpn モードで設定された anyconnect **ssl compression** コマンドは上書きされます。

例

次の例では、グループ ポリシー sales に対して SVC 圧縮はディセーブルです。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl compression none
```

関連コマンド

コマンド	説明
anyconnect	特定のグループまたはユーザーに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect keepalive	リモートコンピュータ上のクライアントから ASA にキープアライブメッセージが SSL VPN 接続で送信される頻度を指定します。
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
anyconnect rekey	SSL VPN 接続でクライアントがキーの再生成を実行できるようにします。
compression	すべての SSL、WebVPN、および IPsec VPN 接続で、圧縮をイネーブルにします。
show webvpn anyconnect	インストールされている SSL VPN クライアントに関する情報を表示します。

anyconnect ssl df-bit-ignore

特定のグループまたはユーザーについて SSL VPN 接続でパケットを強制的にフラグメント化（トンネルを通過）できるようにするには、グループ ポリシー webvpn またはユーザー名 webvpn コンフィギュレーション モードで **anyconnect ssl df-bit-ignore** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl df-bit-ignore { **enable** | **disable** }
no anyconnect ssl df-bit-ignore

構文の説明

enable	SSL 搭載の AnyConnect クライアント に対して DF ビットの無視を有効にします。
disable	SSL 搭載の AnyConnect クライアント に対して DF ビットを無効にします。

コマンド デフォルト

DF ビットの無視は、ディセーブルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	svc df-bit-ignore コマンドが anyconnect ssl df-bit-ignore コマンドに置き換えられました。

使用上のガイドライン

この機能では、DF ビットが設定されているパケットを強制的にフラグメント化して、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバーに対する使用などがあります。

例

次の例では、グループ ポリシー sales に対して DF ビットの無視がイネーブルになっています。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl df-bit-ignore enable
```

関連コマンド

コマンド	説明
anyconnect	特定のグループまたはユーザーに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect keepalive	リモートコンピュータ上のクライアントから ASA にキープアライブメッセージが SSL VPN 接続で送信される頻度を指定します。
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
anyconnect rekey	SSL VPN 接続でクライアントがキーの再生成を実行できるようにします。

anyconnect ssl dtls enable

Cisco AnyConnect VPN Client との SSL VPN 接続を確立している特定のグループまたはユーザーのインターフェイスで Datagram Transport Layer Security（DTLS）接続をイネーブルにするには、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名属性 webvpn コンフィギュレーション モードで **anyconnect ssl dtls enable** コマンドを使用します。コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl dtls enable *interface*
no anyconnect ssl dtls enable *interface*

構文の説明

interface	インターフェイスの名前。

コマンド デフォルト

デフォルトではイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	svc dtls コマンドが追加されました。
8.4(1)	svc dtls コマンドが anyconnect ssl dtls コマンドに置き換えられました。

使用上のガイドライン

DTLS を有効にすると、SSL VPN 接続を確立している AnyConnect クライアント で、2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用できます。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

DTLS を有効にしない場合、SSL VPN 接続を確立している AnyConnect クライアントユーザーは SSL トンネルのみで接続します。

このコマンドでは、特定のグループまたはユーザーについてDTLSをイネーブルにします。すべての AnyConnect クライアント ユーザーに対して DTLS を有効にするには、webvpn コンフィギュレーション モードで **anyconnect ssl dtls enable** コマンドを使用します。

例

次に、グループ ポリシー *sales* のグループ ポリシー webvpn コンフィギュレーション モードを開始し、DTLS をイネーブルにする例を示します。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl dtls enable
```

関連コマンド

コマンド	説明
dtls port	DTLS の UDP ポートを指定します。
anyconnect dtls	SSL VPN 接続を確立するグループまたはユーザーに対して、DTLS をイネーブルにします。
vpn-tunnel-protocol	ASA がリモートアクセス用に許可する VPN プロトコル（SSL を含む）を指定します。

anyconnect ssl keepalive

SSL VPN 接続でリモートクライアントから ASA に送信されるキープアライブメッセージの頻度を設定するには、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードで、**anyconnect ssl keepalive** コマンドを使用します。コンフィギュレーションからこのコマンドを削除し、値を継承するには、コマンドの **no** 形式を使用します。

anyconnect ssl keepalive { **none** | *seconds* }
no anyconnect ssl keepalive { **none** | *seconds* }

構文の説明

none	キープアライブ メッセージをディセーブルにします。
seconds	キープアライブ メッセージをイネーブルにし、メッセージの頻度（15 ～ 600 秒）を指定します。

コマンド デフォルト

デフォルトは 20 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	svc keepalive コマンドが追加されました。
8.0(3)	デフォルト設定がディセーブルから 20 秒に変更されました。
8.4(1)	svc keepalive コマンドが anyconnect ssl keepalive コマンドに置き換えられました。

使用上のガイドライン

Cisco SSL VPN Client（SVC）と Cisco AnyConnect VPN Client の両方で、ASA への SSL VPN 接続を確立するときにキープアライブメッセージを送信できます。

接続をアイドル状態で維持できる時間がデバイスによって制限されている場合も、プロキシ、ファイアウォール、または NAT デバイスを経由した SSL VPN 接続が確実に開いたままで保たれるように、キープアライブメッセージの頻度を調整できます（*seconds* で指定）。

また、頻度を調整すると、リモート ユーザーが Microsoft Outlook または Microsoft Internet Explorer などのソケット ベース アプリケーションをアクティブに実行していない場合でも、クライアントは切断および再接続されません。

（注） キープアライブはデフォルトでイネーブルになっています。キープアライブをディセーブルにすると、フェールオーバー イベントの際に、SSL VPN クライアント セッションはスタンバイ デバイスに引き継がれません。

例

次の例では、ユーザーは、>*sales* という名前の既存のグループポリシーについて、ASA を設定し、クライアントがキープアライブメッセージを 300 秒（5 分）の頻度で送信できるようにします。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl keepalive 300
```

関連コマンド

コマンド	説明
anyconnect	特定のグループまたはユーザーに SSL VPN クライアントをイネーブルにします。または、要求します。
anyconnect dpd-interval	ASA でデッドピア検出（DPD）をイネーブルにし、クライアントまたは ASA によって DPD が実行される頻度を設定します。
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
anyconnect ssl rekey	セッションでクライアントがキーの再生成を実行できるようにします。

anyconnect ssl rekey

SSL VPN 接続でリモート クライアントがキーの再生成を実行できるようにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードで anyconnect ssl rekey コマンドを使用します。コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl rekey { **method** { **ssl** | **new-tunnel** } | **time** *minutes* | **none** }
no anyconnect ssl rekey { **method** { **ssl** | **new-tunnel** } | **time** *minutes* | **none** }

構文の説明

method ssl	キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
method new-tunnel	キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
method none	キーの再生成をディセーブルにします。
time *minutes*	セッションの開始からキーの再生成が発生するまでの時間（分）を指定します。4 ～ 10080（1 週間）の範囲です。

コマンド デフォルト

デフォルトは none（ディセーブル）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	svc rekey コマンドが追加されました。

リリース	変更内容
8.0(2)	「中間者」攻撃の可能性を防ぐため、**svc rekey method ssl** コマンドの動作が **svc rekey method new-tunnel** コマンドの動作に変更されました。
8.4(1)	svc rekey コマンドが anyconnect ssl rekey コマンドに置き換えられました。

使用上のガイドライン

Cisco AnyConnect クライアント は、ASA への SSL VPN 接続でキーの再生成を実行できます。キーの再生成方法を **ssl** または **new-tunnel** に設定すると、キー再生成時に SSL 再ネゴシエーションが行われず、クライアントがキー再生成時に新規トンネルを確立することが指定されます。

例

次の例では、ユーザーは、グループポリシー *sales* に属するリモートクライアントがキーの再生成時に SSL と再ネゴシエートし、セッションの開始後 30 分でキーの再生成が発生することを指定します。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anycoanynnect ssl rekey method ssl
ciscoasa(config-group-webvpn)# anyconnect ssl rekey time 30
```

関連コマンド

コマンド	説明
anyconnect enable	特定のグループまたはユーザーに対して AnyConnect クライアントを有効または必須にします。
anyconnect dpd-interval	ASA で Dead Peer Detection（DPD; デッド ピア検出）を有効にし、AnyConnect クライアント または ASA によって DPD が実行される頻度を設定します。
anyconnect keepalive	リモートコンピュータ上の AnyConnect クライアント から ASA にキープアライブメッセージが送信される頻度を指定します。
anyconnect keep-installer	リモートコンピュータへの AnyConnect クライアント の永続インストールを有効にします。

apcf（廃止）

Application Profile Customization Framework プロファイルをイネーブルにするには、webvpn コンフィギュレーション モードで **apcf** コマンドを使用します。特定の APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を使用します。すべての APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

apcf URL / **filename.ext**
no apcf [**URL** / **filename.ext**]

構文の説明

filename.extension	APCF カスタマイゼーション スクリプトの名前を指定します。これらのスクリプトは、常に XML 形式です。拡張子は、.xml、.txt、.doc などです。
URL	ASA でロードして使用する APCF プロファイルの場所を指定します。http://、https://、tftp://、ftp://、flash:/、disk#:/' のいずれかの URL を使用します。 URL には、サーバー、ポート、およびパスを含めることができます。ファイル名のみを指定した場合、デフォルトの URL は flash:/ です。**copy** コマンドを使用して、APCF プロファイルをフラッシュメモリにコピーできます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

使用上のガイドライン

apcf コマンドを使用すると、ASA は非標準の Web アプリケーションと Web リソースを WebVPN 接続で正しくレンダリングされるように処理できます。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どこの（ヘッダー、本文、要求、応答）、どのデータを変換するかを指定するスクリプトがあります。

ASA で複数の APCF プロファイルを使用できます。その場合、ASA は、それらのプロファイルを古いものから新しいものの順に 1 つずつ適用します。

APCF コマンドは、Cisco TAC のサポートがある場合にのみ使用することを推奨します。

例

次に、フラッシュ メモリの /apcf にある apcf1 という名前の APCF をイネーブルにする例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 apcf
flash:/apcf/apcf1.xml
ciscoasa(config-webvpn)#
```

次に、myserver という名前の HTTPS サーバー（ポート 1440）のパス /apcf にある apcf2.xml という名前の APCF をイネーブルにする例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 apcf
https://myserver:1440/apcf/apcf2.xml
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
proxy-bypass	特定のアプリケーションに対してコンテンツの最低限の書き換えを設定します。
rewrite	トラフィックが ASA を通過するかどうかを決定します。
show running config webvpn apcf	APCF 設定を表示します。

app-agent heartbeat

ASA で実行されている app-agent（アプリケーション エージェント）のハートビートメッセージ間隔を設定して、シャーシの健全性をチェックするには、グローバル コンフィギュレーション モードで **app-agent heartbeat** コマンドを使用します。

app-agent heartbeat ［ **interval** *ms* ］［ **retry-count** *number* ］

（注） シャーシでのみサポートされます。

構文の説明

interval *ms*	ハートビートの時間間隔を 100 ～ 6000 ms の範囲の 100 の倍数単位で設定します。デフォルトは 1000 ms です。
retry-count *number*	再試行の回数を 1 ～ 30 の間で設定します。デフォルトの試行回数は 3 回です。

コマンド デフォルト

デフォルトの間隔は 1000 ms です。

デフォルトの再試行回数は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.6(2)	コマンドが追加されました。
9.9(1)	最小インターフェイスが 300 ms から 100 ms に変更されました。

使用上のガイドライン

ASA はホストシャーシとのバックプレーンを介して通信できるかどうかをチェックします。

Firepower 4100/9300 の場合、最小の結合時間（*interval* x *retry-count*）は、600 ミリ秒未満にはできません。たとえば、間隔を 100 に、再試行回数を 3 に設定した場合、合計結合時間は 300 ミ

リ秒になりますが、これはサポートされていません。たとえば、間隔を100に設定し、再試行回数を 6 に設定して最小時間（600 ms）を満たすことができます。

例

次に、間隔を 300 ミリ秒に設定する例を示します。

```
ciscoasa(config)# app-agent heartbeat interval 300
```

関連コマンド

コマンド	説明
health-check	クラスタ ヘルス チェックのパラメータを設定します。

app-id

ネットワークサービス オブジェクトにシスコ定義のアプリケーション ID を追加するには、オブジェクト コンフィギュレーション モードで **app-id** コマンドを使用します。ID を削除するには、このコマンドの **no** 形式を使用します。

app-id *number*
no app-id *number*

構文の説明

number 特定のアプリケーションに対してシスコが割り当てた 1 ～ 4294967295 の範囲の一意の番号です。このコマンドは、主に外部デバイスマネージャを使用する場合に使用します。

コマンド デフォルト

オブジェクトにアプリケーション ID は割り当てられません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
オブジェクト ネットワーク サービス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドが導入されました。

関連コマンド

コマンド	説明
object network-service	ネットワークサービス オブジェクトを作成します。
object-group network-service	ネットワークサービス オブジェクト グループを作成します。

appl-acl

セッションに適用する設定済みのWebタイプACLを指定するには、DAP webvpnコンフィギュレーションモードで**appl-acl**コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの**no**形式を使用します。すべてのWebタイプACLを削除するには、このコマンドの**no**形式を引数なしで使用します。

appl-acl［ *identifier* ］
no appl-acl［ *identifier* ］

構文の説明

identifier	以前に設定したWebタイプACLの名前。最大長は240文字です。

コマンド デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
DAP webvpnコンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Webタイプ ACLを設定するには、グローバル コンフィギュレーション モードで**access-list webtype**コマンドを使用します。

appl-aclコマンドを複数回使用して、複数のWebタイプ ACLをDAPポリシーに適用できます。

例

次に、newaclという名前の設定済みのWebタイプ ACLをダイナミック アクセス ポリシーに適用する例を示します。

```
ciscoasa
 (config)#
config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
```

```
 webvpn
ciscoasa
(config-dynamic-access-policy-record)#
 appl-acl newacl
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
access-list_webtype	Web タイプ ACL を作成します。

application-access

認証された WebVPN ユーザーに表示される WebVPN ホームページの [アプリケーションアクセス（Application Access）] フィールド、およびユーザーがアプリケーションを選択したときに表示される [アプリケーションアクセス（Application Access）] ウィンドウをカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **application-access** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access { **title** | **message** | **window** } { **text** | **style** } *value*
no application-access { **title** | **message** | **window** } { **text** | **style** } *value*

構文の説明

message	[Application Access] フィールドのタイトルの下に表示されるメッセージを変更します。
style	[Application Access] フィールドのスタイルを変更します。
text	[Application Access] フィールドのテキストを変更します。
title	[Application Access] フィールドのタイトルを変更します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）。
window	[Application Access] ウィンドウを変更します。

コマンド デフォルト

[Application Access] フィールドのデフォルトのタイトルテキストは「Application Access」です。

[Application Access] フィールドのデフォルトのタイトル スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

[Application Access] フィールドのデフォルトのメッセージテキストは「Start Application Client」です。

[Application Access] フィールドのデフォルトのメッセージ スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller.

[Application Access] ウィンドウのデフォルトのウィンドウ テキストは次のとおりです。

「Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications.」

[Application Access] ウィンドウのデフォルトのウィンドウ スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。

style オプションは有効なカスケーディング スタイル シート（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSSパラメータの詳細については、World Wide Web コンソーシアム（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

次に、WebVPNページに対する変更で最もよく行われるページ配色の変更に役立つヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Application Access] フィールドの背景色を RGB 16 進値 66FFFF（緑色の一種）にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

関連コマンド

コマンド	説明
application-access hide-details	[Application Access] ウィンドウのアプリケーション詳細の表示をイネーブルまたはディセーブルにします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

application-access hide-details

WebVPN の [アプリケーションアクセス（Application Access）] ウィンドウに表示されるアプリケーション詳細を非表示にするには、カスタマイゼーション コンフィギュレーション モードで **application-access hide-details** コマンドを使用します。このモードには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access hide − details { **enable** | **disable** }
no application-access [**hide - details** { **enable** | **disable** }]

構文の説明

disable	[Application Access] ウィンドウにアプリケーション詳細を表示します。
enable	[Application Access] ウィンドウのアプリケーション詳細を非表示にします。

コマンド デフォルト

デフォルトではディセーブルになっています。[Application Access] ウィンドウにアプリケーション詳細が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

例

次に、アプリケーション詳細の表示をディセーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access hide-details disable
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] フィールドをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。

翻訳について
このドキュメントは、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。