CHAPTER 33

undebug コマンド～ zonelabs integrity ssl-client-authentication コマンド

undebug

現在のセッションでデバッグ情報の表示をディセーブルにするには、特権 EXEC モードで **undebug** コマンドを使用します。

undebug {*command* | **all**}

構文の説明

command	指定したコマンドのデバッグをディセーブルにします。サポートされるコマンドの詳細については、「使用上のガイドライン」を参照してください。
all	すべてのデバッグ出力をディセーブルにします。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。このコマンドには、追加のデバッグ キーワードが含まれます。

使用上のガイドライン

次のコマンドは、undebug コマンドで使用できます。特定のコマンドのデバッグ、または特定の **debug** コマンドに関連付けられた引数とキーワードの詳細については、**debug** *command* のエントリを参照してください。

- aaa：AAA 情報
- acl：ACL 情報
- all：すべてのデバッグ
- appfw：アプリケーション ファイアウォール情報
- arp：NP オペレーションを含む ARP
- asdm：ASDM 情報
- auto-update：Auto-update 情報
- boot-mem：ブート メモリの計算と設定
- cifs：CIFS 情報
- cmgr：CMGR 情報
- context：コンテキスト情報
- cplane：CP 情報

- crypto：クリプト情報
- ctiqbe：CTIQBE 情報
- ctl-provider：CTL プロバイダーのデバッグ情報
- dap：DAP 情報
- dcerpc：DCERPC 情報
- ddns：ダイナミック DNS 情報
- dhcpc：DHCP クライアント情報
- dhcpd：DHCP サーバ情報
- dhcprelay：DHCP リレー情報
- disk：ディスク情報
- dns：DNS 情報
- eap：EAP 情報
- eigrp：EIGRP プロトコル情報
- email：電子メール情報
- entity：エンティティ MIB 情報
- eou：EAPoUDP 情報
- esmtp：ESMTP 情報
- fips：FIPS 140-2 情報
- fixup：フィックスアップ情報
- fover：フェールオーバー情報
- fsm：FSM 情報
- ftp：FTP 情報
- generic：その他の情報
- gtp：GTP 情報
- h323：H323 情報
- http：HTTP 情報
- icmp：ICMP 情報
- igmp：インターネット グループ管理プロトコル
- ils：LDAP 情報
- im：IM インスペクション情報
- imagemgr：Image Manager 情報
- inspect：デバッグ情報のインスペクション
- integrityfw：Integrity ファイアウォール情報
- ip：IP 情報
- ipsec-over-tcp：IPSec over TCP 情報
- IPSec-pass-thru：ipsec-pass-thru 情報のインスペクション
- ipv6：IPv6 情報
- iua-proxy：IUA プロキシ情報

- kerberos：KERBEROS 情報
- l2tp：L2TP 情報
- ldap：LDAP 情報
- mfib：マルチキャスト転送情報ベース
- mgcp：MGCP 情報
- module-boot：サービス モジュール ブート情報
- mrib：マルチキャスト ルーティング情報ベース
- nac-framework：NAC-FRAMEWORK 情報
- netbios-inspect：NETBIOS インスペクション情報
- npshim：NPSHIM 情報
- ntdomain：NT ドメイン情報
- ntp：NTP 情報
- ospf：OSPF 情報
- p2p：P2P インスペクション情報
- parser：パーサー情報
- pim：Protocol Independent Multicast
- pix：PIX 情報
- ppp：PPP 情報
- pppoe：PPPoE 情報
- pptp：PPTP 情報
- radius：RADIUS 情報
- redundant-interface：冗長インターフェイス情報
- rip：RIP 情報
- rtp：RTP 情報
- rtsp：RTSP 情報
- sdi：SDI 情報
- sequence：シーケンス番号の追加
- session-command：セッション コマンド情報
- sip：SIP 情報
- skinny：Skinny 情報
- sla：IP SLA モニタ デバッグ
- smtp-client：電子メール システムのログ メッセージ
- splitdns：スプリット DNS 情報
- sqlnet：SQLNET 情報
- ssh：SSH 情報
- sunrpc：SUNRPC 情報
- tacacs：TACACS 情報
- tcp：WebVPN の TCP

- tcp-map：TCP マップ情報
- timestamps：タイムスタンプの追加
- track：スタティック ルート トラッキング
- vlan-mapping：VLAN マッピング情報
- vpn-sessiondb：VPN セッション データベース情報
- vpnlb：VPN ロード バランシング情報
- wccp：WCCP 情報
- webvpn：WebVPN 情報
- xdmcp：XDMCP 情報
- xml：XML パーサー情報

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべてのデバッグ出力をディセーブルにする例を示します。

```
hostname(config)# undebug all
```

関連コマンド

コマンド	説明
debug	選択したコマンドに関するデバッグ情報を表示します。

unix-auth-gid

UNIX グループ ID 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 モードで **unix-auth-gid** コマンドを使用します。このコマンドを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** バージョンを使用します。

unix-auth-gid <*identifier*>

no storage-objects

構文の説明

identifier	0 ～ 4294967294 の範囲の整数を指定します。

デフォルト

デフォルト値は 65534 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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 モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

文字列で Network File System（NetFS; ネットワーク ファイル システム）の場所を指定します。SMB プロトコルおよび FTP プロトコルだけがサポートされています。たとえば、smb://（NetFS の場所）または ftp://（NetFS の場所）。この場所の名前を **storage-objects** コマンドで使用します。

例

次に、UNIX グループ ID を 4567 に設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# unix-auth-gid 4567
```

関連コマンド

コマンド	説明
unix-auth-uid	UNIX ユーザ ID を設定します。

unix-auth-uid

UNIX ユーザ ID 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 モードで **unix-auth-uid** コマンドを使用します。このコマンドを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** バージョンを使用します。

unix-auth-gid <*identifier*>

no storage-objects

構文の説明

identifier	0 ～ 4294967294 の範囲の整数を指定します。

デフォルト

デフォルト値は 65534 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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 モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

文字列で Network File System（NetFS; ネットワーク ファイル システム）の場所を指定します。SMB プロトコルおよび FTP プロトコルだけがサポートされています。たとえば、smb://（NetFS の場所）または ftp://（NetFS の場所）。この場所の名前を **storage-objects** コマンドで使用します。

例

次に、UNIX ユーザ ID を 333 に設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# unix-auth-gid 333
```

関連コマンド

コマンド	説明
unix-auth-gid	UNIX グループ ID を設定します。

upload-max-size

アップロードするオブジェクトの最大許容サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **upload-max-size** コマンドを使用します。このオブジェクトを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** バージョンを使用します。

upload-max-size <*size*>

no upload-max-size

構文の説明

size	アップロードされるオブジェクトの最大許容サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

デフォルト

デフォルトのサイズは 2147483647 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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 モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

サイズを 0 に設定すると、実質的にオブジェクトのアップロードは許可されません。

例

次に、アップロードされるオブジェクトの最大サイズを 1500 バイトに設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# upload-max-size 1500
```

関連コマンド

コマンド	説明
post-max-size	ポストするオブジェクトの最大サイズを指定します。
download-max-size	ダウンロードするオブジェクトの最大サイズを指定します。

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

urgent-flag

TCP ノーマライザを通して URG ポインタを許可またはクリアするには、tcp マップ コンフィギュレーション モードで **urgent-flag** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

構文の説明

allow	TCP ノーマライザを通して URG ポインタを許可します。
clear	TCP ノーマライザを通して URG ポインタをクリアします。

デフォルト

緊急フラグおよび緊急オフセットはデフォルトでクリアされます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(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

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。その新しい TCP マップを、**policy-map** コマンドを使用して適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **urgent-flag** コマンドを使用して、緊急フラグを許可します。

URG フラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCP RFC では、URG フラグの正確な解釈を明確化していません。したがって、エンド システムにおいては緊急オフセットがさまざまな方法で処理されます。このため、エンド システムが攻撃を受けやすくなります。デフォルトの動作では、URG フラグとオフセットはクリアされます。

例

次に、緊急フラグを許可する例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config)# class-map cmap
```

```
hostname(config-cmap)# match port tcp eq 513
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

uri-non-sip

Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別するには、パラメータ コンフィギュレーション モードで **uri-non-sip** 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 モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。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。

uri-non-sip action {**mask** | **log**} [**log**}

no uri-non-sip action {**mask** | **log**} [**log**}

構文の説明

mask	SIP 以外の URI をマスクします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。

デフォルト

このコマンドは、デフォルトでディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップの Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別する例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# uri-non-sip action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

url

CRL を取得するためのスタティック URL のリストを維持するには、crl 設定コンフィギュレーション モードで **url** コマンドを使用します。crl 設定コンフィギュレーション モードは、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。既存の URL を削除するには、このコマンドの **no** 形式を使用します。

url *index url*

no url *index url*

構文の説明

index	リスト内の各 URL のランクを決定する 1 ～ 5 の値を指定します。セキュリティ アプライアンスは、インデックス 1 から URL を試行します。
url	CRL の取得元となる URL を指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL 設定コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

既存の URL は上書きできません。既存の URL を置き換えるには、まずこのコマンドの **no** 形式を使用して、その URL を削除します。

例

次に、ca-crl コンフィギュレーション モードを開始し、CRL 取得用の URL のリストを作成および維持するためにインデックス 3 を設定して CRL の取得元となる URL https://foobin.com を設定する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# url 3 https://foobin.com
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
policy	CRL の取得元を指定します。

url-block

フィルタリング サーバからのフィルタリング決定を待機する間、Web サーバの応答に使用される URL バッファを管理するには、**url-block** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

url-block block *block_buffer*

no url-block block *block_buffer*

url-block mempool-size *memory_pool_size*

no url-block mempool-size *memory_pool_size*

url-block url-size *long_url_size*

no url-block url-size *long_url_size*

構文の説明

block *block_buffer*	フィルタリング サーバからのフィルタリング決定を待機している間に Web サーバの応答を保存する HTTP 応答バッファを作成します。指定できる値は 1 ～ 128 です。これは、1550 バイトのブロック数を示します。
mempool-size *memory_pool_size*	URL バッファ メモリ プールの最大サイズをキロバイト（KB）単位で設定します。指定できる値は 2 ～ 10240 です。これは、2 ～ 10240 KB の URL バッファ メモリ プールを示します。
url-size *long_url_size*	バッファに保存する長い各 URL の最大許容 URL サイズを KB 単位で設定します。最大 URL サイズとして指定できる値は、Websense では 2、3、または 4（それぞれ 2 KB、3 KB、4KB を表す）、Secure Computing では 2 または 3（それぞれ 2 KB、3 KB を表す）です。

デフォルト

このコマンドは、デフォルトでディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

Websense フィルタリング サーバの場合、**url-block url-size** コマンドを使用すると、最大 4 KB の長い URL をフィルタリングできます。Secure Computing の場合は、**url-block url-size** コマンドを使用して、最大 3 KB の長い URL をフィルタリングできます。Websense フィルタリング サーバおよび N2H2

フィルタリング サーバの場合、**url-block block** コマンドを使用すると、セキュリティ アプライアンスは、URL フィルタリング サーバからの応答を待機している間、Web クライアント要求への応答として Web サーバから受信したパケットをバッファに保存します。これにより、Web クライアントのパフォーマンスがデフォルトのセキュリティ アプライアンス動作よりも向上します。デフォルトの動作では、パケットをドロップし、接続か許可された場合に Web サーバにパケットの再送信を要求します。

url-block block コマンドを使用し、フィルタリング サーバが接続を許可した場合、セキュリティ アプライアンスはブロックを HTTP 応答バッファから Web クライアントに送信し、バッファからブロックを削除します。フィルタリング サーバが接続を拒否した場合、セキュリティ アプライアンスは拒否メッセージを Web クライアントに送信し、HTTP 応答バッファからブロックを削除します。

url-block block コマンドを使用して、フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答のバッファリングに使用するブロック数を指定します。

url-block url-size コマンドを **url-block mempool-size** コマンドとともに使用して、フィルタリングする URL の最大長と URL バッファに割り当てる最大メモリを指定します。Websense サーバまたは Secure-Computing サーバに、1159 バイトよりも長く、最大 4096 バイトまでの URL を渡す場合は、これらのコマンドを使用します。**url-block url-size** コマンドは、1159 バイトよりも長い URL をバッファに保存し、その URL を（TCP パケット ストリームを使用して）Websense サーバまたは Secure-Computing サーバに渡します。これにより、Websense サーバまたは Secure-Computing サーバでは、その URL へのアクセスを許可または拒否できます。

例

次に、URL フィルタリング サーバからの応答をバッファに保存するために 1550 バイトのブロックを 56 個割り当てる例を示します。

```
hostname#(config)# url-block block 56
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファの使用状況カウンタをクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

url-cache

Websense サーバから受信した URL 応答の URL キャッシングをイネーブルにし、キャッシュのサイズを設定するには、グローバル コンフィギュレーション モードで **url-cache** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

no url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

構文の説明

dst	URL 宛先アドレスに基づくキャッシュ エントリ。このモードは、Websense サーバ上ですべてのユーザが同じ URL フィルタリング ポリシーを共有する場合に選択します。
size *kbytes*	キャッシュ サイズの値を 1 ～ 128 KB の範囲で指定します。
src_dst	URL 要求の送信元アドレスと URL 宛先アドレスの両方に基づくキャッシュ エントリ。このモードは、Websense サーバ上でユーザが同じ URL フィルタリング ポリシーを共有しない場合に選択します。
statistics	**statistics** オプションを使用すると、キャッシュ ルックアップの回数やヒット率などの追加の URL キャッシュ統計情報が表示されます。

デフォルト

このコマンドは、デフォルトでディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

（注）　N2H2 サーバ アプリケーションは、URL フィルタリングでこのコマンドをサポートしません。

url-cache コマンドには、URL サーバからの応答をキャッシュするコンフィギュレーション オプションが用意されています。

url-cache コマンドは、URL キャッシングのイネーブル化、キャッシュ サイズの設定、およびキャッシュ統計情報の表示を行う場合に使用します。

キャッシングにより、URL アクセス権限がセキュリティ アプライアンス上のメモリに保存されます。ホストが接続を要求すると、セキュリティ アプライアンスは要求を Websense サーバに転送するのではなく、一致するアクセス権限を URL キャッシュ内で探します。キャッシングをディセーブルにするには、**no url-cache** コマンドを使用します。

（注）　Websense サーバで設定を変更した場合は、**no url-cache** コマンドでキャッシュをディセーブルにした後、**url-cache** コマンドで再度イネーブルにします。

URL キャッシュを使用しても、Websense プロトコル バージョン 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル バージョン 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。セキュリティ ニーズを満たす使用状況プロファイルを取得した後、**url-cache** をイネーブルにしてスループットを向上させます。Websense プロトコル バージョン 4 の URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログが更新されます。

例

次に、送信元アドレスと宛先アドレスに基づいてすべての発信 HTTP 接続をキャッシュする例を示します。

```
hostname(config)# url-cache src_dst 128
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド ステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-cache statistics	Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-server	**filter** コマンドで使用する Websense サーバを指定します。

url-entry

ポータル ページで HTTP/HTTPS URL を入力する機能をイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **url-entry** コマンドを使用します。

url-entry enable | disable

enable | disable	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

例

次に、Finance という DAP レコードの URL エントリをイネーブルにする例を示します。

```
hostname (config) config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dynamic-access-policy-record)# url-entry enable
```

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。
file-entry	アクセス先のファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。

url-length-limit

RTSP メッセージで許可される URL の最大長を設定するには、パラメータ コンフィギュレーション モードで **url-length-limit** 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 モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。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。

url-length-limit *length*

no url-length-limit *length*

構文の説明

length	URL の長さ制限（バイト単位）。値の範囲は、0 ～ 6000 です。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、RTSP インスペクション ポリシー マップで URL の長さ制限を設定する例を示します。

```
hostname(config)# policy-map type inspect rtsp rtsp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# url-length-limit 50
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

url-list（削除）

このコマンドを使用して SSL VPN 接続によるアクセス用の URL リストを定義できなくなりました。今後は **import** コマンドを使用して、URL リストを定義する XML オブジェクトをインポートしてください。詳細については、**import-** コマンドと **export-url-list** コマンドを参照してください。

デフォルト

デフォルトの URL リストはありません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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 モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	このコマンドは廃止されました。このコマンドがソフトウェアのこのリリースに残されているのは、既存の URL リストの下位互換性を維持するためです。セキュリティ アプライアンスは、それらのリストを XML ファイルに変換できます。このコマンドを使用して新しい URL リストを作成することはできません。

使用上のガイドライン

グローバル コンフィギュレーション モードで url-list コマンドを使用して、1 つ以上の URL リストを作成します。特定のグループ ポリシーまたはユーザに対してリスト内の URL へのアクセスを許可するには、ここで作成した *listname* を、webvpn モードで **url-list** コマンドとともに使用します。

例

次に、www.cisco.com、www.example.com、および www.example.org へのアクセスを提供する *Marketing URLs* という名前の URL リストを作成する例を示します。次の表に、各 URL の設定で使用する値を示します。

listname	displayname	url
Marketing URLs	Cisco Systems	http://www.cisco.com
Marketing URLs	Example Company, Inc.	http://www.example.com
Marketing URLs	Example Organization	http://www.example.org

```
hostname(config)# url-list Marketing URLs Cisco Systems http://www.cisco.com
hostname(config)# url-list Marketing URLs Example Company, Inc. http://www.example.com
hostname(config)# url-list Marketing URLs Example Organization http://www.example.org
```

関連コマンド

コマンド	説明
clear configuration url-list	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスは、そのリストのコマンドだけを削除します。
show running-configuration url-list	現在設定されている URL のセットを表示します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

url-list（グループ ポリシー webvpn）

WebVPN サーバと URL のリストを特定のユーザまたはグループ ポリシーに適用するには、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名 webvpn コンフィギュレーション モードで **url-list** コマンドを使用します。**url-list none** コマンドを使用して作成したヌル値を含むリストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。URL リストが継承されないようにするには、**url-list none** コマンドを使用します。次回このコマンドを使用すると、前回までの設定が上書きされます。

url-list {**value** *name* | **none**} [*index*]

no url-list

構文の説明

index	ホームページ上の表示のプライオリティを指定します。
none	URL リストにヌル値を設定します。デフォルトまたは指定したグループ ポリシーからリストが継承されないようにします。
value *name*	設定済み URL リストの名前を指定します。このようなリ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 **url-list** コマンドを使用します。

デフォルト

デフォルトの URL リストはありません。

コマンド モード

次の表に、このコマンドを入力するモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn モード	•	—	•	—	—
ユーザ名モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

次回このコマンドを使用すると、前回までの設定が上書きされます。

webvpn モードで **url-list** コマンドを使用してユーザまたはグループ ポリシーの WebVPN ホームページに表示する URL リストを指定する前に、XML オブジェクトでリストを作成する必要があります。グローバル コンフィギュレーション モードで **import** コマンドを使用して、URL リストをセキュリティ アプライアンスにダウンロードします。次に、url-list コマンドを使用して、リストを特定のグループ ポリシーまたはユーザに適用します。

例

次に、FirstGroupURLs という名前の URL リストを FirstGroup という名前のグループ ポリシーに適用し、このリストを 1 番めの URL リストに指定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
```

関連コマンド

コマンド	説明
clear configure url-list [*listname*]	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスは、そのリストのコマンドだけを削除します。
show running-configuration url-list	現在設定されている一連の **url-list** コマンドを表示します。
webvpn	webvpn モードを開始します。これは、webvpn コンフィギュレーション モード、グループ ポリシー webvpn コンフィギュレーション モード（特定のグループ ポリシーの webvpn 設定を行う場合）、またはユーザ名 webvpn コンフィギュレーション モード（特定のユーザの webvpn 設定を行う場合）のいずれかです。

url-server

filter コマンドで使用する N2H2 サーバまたは Websense サーバを指定するには、グローバル コンフィギュレーション モードで **url-server** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

N2H2

url-server [<(*if_name*)>] **vendor** {smartfilter | n2h2} **host** <*local_ip*> [**port** <*number*>] [**timeout** <seconds>] [**protocol** {**TCP** [connections <*number*>]} | **UDP**]

no url-server [<(*if_name*)>] **vendor** {smartfilter | n2h2} **host** <*local_ip*> [**port** <*number*>] [**timeout** <seconds>] [**protocol** {**TCP** [connections <*number*>]} | **UDP**]

Websense

url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | *version*]

no url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*] | *version*]

構文の説明

N2H2

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに作成される TCP 接続の最大数を指定します。この数はサーバごとであるため、複数のサーバに異なる接続値を指定できます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
if_name	（任意）認証サーバが存在するネットワーク インターフェイス。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。
port *number*	N2H2 サーバ ポート。セキュリティ アプライアンスは、UDP 応答のリッスンもこのポート上で行います。デフォルトのポート番号は 4005 です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP です。
timeout *seconds*	許容される最大アイドル時間で、この時間が経過すると、セキュリティ アプライアンスは指定した次のサーバに切り替わります。デフォルトは 30 秒です。
vendor	「smartfilter」または「n2h2」（下位互換性を維持するため）を使用して URL フィルタリング サービスを指定します。ただし、「smartfilter」はベンダー ストリングとして保存されます。

Websense

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに作成される TCP 接続の最大数を指定します。この数はサーバごとであるため、複数のサーバに異なる接続値を指定できます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。

if_name	認証サーバが存在するネットワーク インターフェイス。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。
timeout *seconds*	許容される最大アイドル時間で、この時間が経過すると、セキュリティ アプライアンスは指定した次のサーバに切り替わります。デフォルトは 30 秒です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP プロトコル バージョン 1 です。
vendor websense	URL フィルタリング サービスのベンダーが Websense であることを示します。
version	プロトコル バージョン **1** または **4** を指定します。デフォルトは TCP プロトコル バージョン 1 です。TCP は、バージョン 1 またはバージョン 4 を使用して設定できます。UDP は、バージョン 4 を使用してのみ設定できます。

デフォルト

このコマンドは、デフォルトでディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•		•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

url-server コマンドでは、N2H2 または Websense URL フィルタリング アプリケーションを実行しているサーバを指定します。URL サーバ数の上限は、シングル コンテキスト モードでは 16、マルチ コンテキスト モードでは 4 ですが、一度に使用できるアプリケーションは、N2H2 または Websense のいずれか 1 つのみです。さらに、セキュリティ アプライアンス上でコンフィギュレーションを変更しても、アプリケーション サーバ上のコンフィギュレーションは更新されないため、ベンダーの指示に従って別途更新する必要があります。

HTTPS および FTP に対して **filter** コマンドを発行するには、事前に **url-server** コマンドを設定する必要があります。すべての URL サーバがサーバ リストから削除されると、URL フィルタリングに関連するすべての **filter** コマンドも削除されます。

サーバを指定した後、**filter url** コマンドを使用して URL フィルタリング サービスをイネーブルにします。

サーバの統計情報（到達不能サーバを含む）を表示するには、**show url-server statistics** コマンドを使用します。

次の手順を実行して、URL フィルタリングを行います。

ステップ 1　ベンダー固有の **url-server** コマンドの適切な形式を使用して、URL フィルタリング アプリケーション サーバを指定します。

ステップ 2　**filter** コマンドを使用して、URL フィルタリングをイネーブルにします。

ステップ 3　（任意）**url-cache** コマンドを使用して、URL キャッシングをイネーブルにし、認識される応答時間を短縮します。

ステップ 4　（任意）**url-block** コマンドを使用して、長い URL および HTTP バッファリングのサポートをイネーブルにします。

ステップ 5　**show url-block block statistics**、**show url-cache statistics**、または **show url-server statistics** コマンドを使用して、実行情報を表示します。

N2H2 によるフィルタリングの詳細については、次の N2H2 の Web サイトを参照してください。

http://www.n2h2.com

Websense フィルタリング サービスの詳細については、次の Web サイトを参照してください。

http://www.websense.com/

例

次に、N2H2 の使用時に 10.0.2.54 ホストからの接続を除くすべての発信 HTTP 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次に、Websense の使用時に 10.0.2.54 ホストからの接続を除くすべての発信 HTTP 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP
version 4
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報をクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。

user-authentication

ユーザ認証をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **user-authentication enable** コマンドを使用します。ユーザ認証をディセーブルにするには、**user-authentication disable** コマンドを使用します。実行コンフィギュレーションからユーザ認証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。このオプションを使用すると、別のグループ ポリシーからユーザ認証の値を継承できます。

ユーザ認証をイネーブルにすると、ハードウェア クライアントの背後にいる個々のユーザは、トンネルを介してネットワークにアクセスするために認証を受けることが必要となります。

user-authentication {**enable | disable**}

no user-authentication

構文の説明

disable	ユーザ認証をディセーブルにします。
enable	ユーザ認証をイネーブルにします。

デフォルト

ユーザ認証はディセーブルです。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

個々のユーザは、設定した認証サーバの順序に従って認証されます。

プライマリ セキュリティ アプライアンスでユーザ認証が必要な場合は、バックアップ サーバでも同様にユーザ認証を設定する必要があります。

例

次に、「FirstGroup」という名前のグループ ポリシーのユーザ認証をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を行わずに IP 電話に接続できるようにします。セキュア ユニット認証は有効なままです。
leap-bypass	イネーブルにすると、VPN クライアントの背後にある無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルを通過します。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。その後、ユーザ認証ごとに再度認証を行います。
secure-unit-authentication	VPN クライアントに、トンネルを開始するたびにユーザ名とパスワードによる認証を要求することによって、セキュリティを強化します。
user-authentication-idle-timeout	個々のユーザのアイドル タイムアウトを設定します。アイドル タイムアウト期間内にユーザ接続上で通信アクティビティが行われない場合、セキュリティ アプライアンスによって接続が切断されます。

user-authentication-idle-timeout

ハードウェア クライアントの背後にいる個々のユーザに対してアイドル タイムアウトを設定するには、グループ ポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを使用します。アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、他のグループ ポリシーからアイドル タイムアウト値を継承できます。アイドル タイムアウト値が継承されないようにするには、**user-authentication-idle-timeout none** コマンドを使用します。

アイドル タイムアウト期間内にハードウェア クライアントの背後にいるユーザによって通信アクティビティが行われない場合、セキュリティ アプライアンスによって接続が切断されます。

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

構文の説明

minutes	アイドル タイムアウト期間の分数を指定します。指定できる範囲は 1 ～ 35791394 分です。
none	無制限のアイドル タイムアウト期間を許可します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトまたは指定したグループ ポリシーからユーザ認証のアイドル タイムアウト値が継承されないようにします。

デフォルト

30 分。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

最小値は 1 分、デフォルトは 30 分、最大値は 10,080 分です。

このタイマーは、VPN トンネル自体ではなく、VPN トンネルを通過するクライアント アクセスだけを終了します。

show uauth コマンドへの応答で示されるアイドル タイムアウトは、常に Cisco Easy VPN リモート デバイスのトンネルを認証したユーザのアイドル タイムアウト値になります。

例

次に、「FirstGroup」という名前のグループ ポリシーに対して 45 分のアイドル タイムアウト値を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

user-storage

クライアントレス SSL VPN セッション間で設定された個人ユーザ情報を保存するには、グループ ポリシー webvpn モードで **user storage** コマンドを使用します。ユーザ ストレージをディセーブルにするには、このコマンドの **no** バージョンを使用します。

user-storage *NETFS-location*

no user-storage]

構文の説明

NETFS-location	ファイル システムの宛先を proto://user:password@host:port/path の形式で指定します。

デフォルト

ユーザストレージはディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ユーザ名、パスワード、および事前共有キーがコンフィギュレーションに示されていますが、セキュリティ アプライアンスではこの情報が内部アルゴリズムを使用して暗号化された形式で格納されるため、セキュリティのリスクは発生しません。

例

次に、anyfiler02a/new_share というパス、anyshare というファイル共有で、パスワードが 12345678 の newuser というユーザとして、ユーザ ストレージを設定する例を示します。

```
hostname(config)# wgroup-policy DFLTGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# user-storage cifs://newuser:12345678@anyfiler02a/new_share
hostname(config-group_webvpn)#
```

関連コマンド

コマンド	説明
storage-key	
storage-objects	

username

ユーザをセキュリティ アプライアンス データベースに追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、削除するユーザ名を指定して、このコマンドの **no** 形式を使用します。すべてのユーザ名を削除するには、ユーザ名を指定せずに、このコマンドの **no** 形式を使用します。

username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

no username *name*

構文の説明

encrypted	パスワードを暗号化することを示します（**mschap** を指定しなかった場合）。**username** コマンド内のパスワードを定義すると、セキュリティ アプライアンスはセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力しても、**username** コマンドによって実際のパスワードは表示されません。暗号化されたパスワードと、その後に **encrypted** キーワードが表示されます。たとえば、「test」というパスワードを入力した場合、**show running-config** コマンドの表示は次のようになります。 `username pat password rvEdRh0xPC8bel7s encrypted` CLI で実際に **encrypted** キーワードを入力するのは、コンフィギュレーションを別のセキュリティ アプライアンスにカット アンド ペーストして、同じパスワードを使用する場合だけです。
mschap	パスワードを入力後に unicode に変換し、MD4 を使用してハッシュすることを指定します。このキーワードは、ユーザを MSCHAPv1 または MSCHAPv2 を使用して認証する場合に使用します。
name	ユーザの名前を 4 ～ 64 文字の長さのストリングとして指定します。
nopassword	このユーザにパスワードが必要ないことを示します。
nt-encrypted	パスワードを MSCHAPv1 または MSCHAPv2 で使用するために暗号化することを示します。ユーザを追加するときに **mschap** キーワードを指定した場合は、**show running-config** コマンドを使用してコンフィギュレーションを表示すると、**encrypted** キーワードではなくこのキーワードが表示されます。 **username** コマンド内のパスワードを定義すると、セキュリティ アプライアンスはセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力しても、**username** コマンドによって実際のパスワードは表示されません。暗号化されたパスワードと、その後に **nt-encrypted** キーワードが表示されます。たとえば、「test」というパスワードを入力した場合、**show running-config** コマンドの表示は次のようになります。 `username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` CLI で実際に **nt-encrypted** キーワードを入力するのは、コンフィギュレーションを別のセキュリティ アプライアンスにカット アンド ペーストし、かつ、同じパスワードを使用する場合のみです。

password *password*	パスワードを 3 ～ 32 文字の長さのストリングとして指定します。
privilege *priv_level*	使用する特権レベルを 0（最低）～ 15（最高）の範囲で設定します。デフォルトの特権レベルは 2 です。この特権レベルは、コマンド認可で使用されます。

デフォルト

デフォルトの特権レベルは 2 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。
7.2(1)	**mschap** キーワードと **nt-encrypted** キーワードが追加されました。

使用上のガイドライン

login コマンドでは、このデータベースを認証用に使用します。

CLI にアクセスできるユーザや特権モードを開始できないユーザをローカル データベースに追加する場合は、コマンド認可をイネーブルにする必要があります（**aaa authorization command** コマンドを参照）。コマンド認可をイネーブルにしなければ、ユーザは、特権レベルが 2 以上（デフォルトは 2）であれば、CLI で独自のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。または、AAA 認証を使用してユーザが **login** コマンドを使用できないようにするか、すべてのローカル ユーザをレベル 1 に設定して **enable** パスワードで特権 EXEC モードにアクセスできるユーザを制御できます。

デフォルトでは、このコマンドで追加した VPN ユーザには属性またはグループ ポリシーが関連付けられません。**username attributes** コマンドを使用して、明示的にすべての値を設定する必要があります。

例

次に、パスワードが 12345678、特権レベルが 12 の「anyuser」という名前のユーザを設定する例を示します。

```
hostname(config)# username anyuser password 12345678 privilege 12
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
clear config username	特定のユーザまたはすべてのユーザのコンフィギュレーションをクリアします。

コマンド	説明
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username attributes	ユーザ名属性コンフィギュレーション モードを開始し、特定のユーザの属性を設定できるようにします。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

username-from-certificate

認可のためのユーザ名として、証明書内のいずれのフィールドを使用するかを指定するには、トンネルグループ一般属性モードで **username-from-certificate** コマンドを使用します。認可のためのユーザ名として使用するピア証明書の DN

属性をコンフィギュレーションから削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no username-from-certificate

構文の説明

primary-attr	証明書から認可クエリーのユーザ名を取得するために使用する属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
secondary-attr	（任意）デジタル証明書から認証または認可クエリーのユーザ名を取得するためにプライマリ属性とともに使用する追加の属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
use-entire-name	セキュリティ アプライアンスでは、完全なサブジェクト DN（RFC1779）を使用して、デジタル証明書から認可クエリーの名前を取得する必要があることを指定します。

デフォルト

プライマリ属性のデフォルト値は CN（一般名）です。

セカンダリ属性のデフォルト値は OU（組織の部門）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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ユーザ名として使用する証明書内のフィールドを選択します。このコマンドは、リリース 8.0.4 以降で廃止された **authorization-dn-attributes** コマンドに代わるものです。**username-from-certificate** コマンドは、セキュリティ アプライアンスに、指定した証明書フィールドをユーザ名 / パスワード認可のためのユーザ名として使用するように強制します。

ユーザ名 / パスワード認証または認可のために、証明書からのユーザ名の事前充填機能で、取得されたこのユーザ名を使用するには、トンネル グループ webvpn 属性モードで **pre-fill-username** コマンドも設定する必要があります。つまり、ユーザ名の事前充填機能を使用するには、両方のコマンドを設定する必要があります。

プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
C	Country（国名）: 2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name（一般名）: 個人、システムなどの名前。セカンダリ属性としては使用できません。
DNQ	Domain Name Qualifier（ドメイン名修飾子）。
EA	E-mail Address（電子メール アドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）: 組織が置かれている市または町。
N	名前
O	Organization（組織）: 会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）: Organization（O; 組織）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）: 組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。
use-entire-name	DN 名全体を使用します。セカンダリ属性としては使用できません。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPSec リモート アクセス トンネル グループを作成し、プライマリ属性として CN（一般名）、セカンダリ属性として OU を使用して、デジタル証明書から認可クエリーの名前を取得するように指定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# username-from-certificate CN OU
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
pre-fill-username	事前入力ユーザ名機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

username attributes

ユーザ名属性モードを開始するには、ユーザ名コンフィギュレーション モードで **username attributes** コマンドを使用します。特定のユーザの属性をすべて削除するには、このコマンドの **no** 形式を使用し、ユーザ名を付加します。すべてのユーザの属性をすべて削除するには、ユーザ名を付加せずに、このコマンドの **no** 形式を使用します。属性モードを使用すると、指定したユーザに対して属性値ペアを設定できます。

username {*name*} **attributes**

no username [*name*] **attributes**

構文の説明

name	ユーザの名前を指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	**service-type** 属性が追加されました。

使用上のガイドライン

内部ユーザ認証データベースは、username コマンドを使用して入力されたユーザで構成されています。**login** コマンドでは、このデータベースを認証用に使用します。ユーザ名属性は、**username** コマンドまたは **username attributes** コマンドを使用して設定できます。

設定ユーザ名コンフィギュレーション モードのコマンドの構文には、次のような共通する特徴があります。

- **no** 形式を使用すると、実行コンフィギュレーションから属性が削除されます。
- **none** キーワードを使用しても、実行コンフィギュレーションから属性が削除されます。ただし、このキーワードでは、属性をヌル値に設定し、継承されないようにすることによって、このことを行います。
- ブール型属性には、イネーブルおよびディセーブルの設定用に明示的な構文があります。

username attributes コマンドは、設定ユーザ名モードを開始し、次の属性を設定できるようにします。

属性	機能
group-lock	ユーザが接続する必要がある既存のトンネル グループを指定します。
password-storage	クライアント システムでのログイン パスワードの保存をイネーブルまたはディセーブルにします。
service-type [login | framed | vpn | admin | nas-prompt]	コンソール ログインを制限し、適切なレベルが割り当てられているユーザのログインをイネーブルにします。**login** オプションでは、基本的な AAA サービスを指定します。これはデフォルトです。**framed** オプションも、基本的な AAA サービスを指定します。**vpn** オプションでは、リモート アクセスのための基本的な AAA サービスを指定します。**admin** オプションは、AAA サービス、ログイン コンソール特権、EXEC モード特権、イネーブル特権、および CLI 特権を指定します。**nas-prompt** オプションは、AAA サービス、ログイン コンソール特権、および EXEC モード特権を指定しますが、イネーブル特権は指定しません。
vpn-access-hours	設定済みの時間範囲ポリシーの名前を指定します。
vpn-filter	ユーザ固有の ACL の名前を指定します。
vpn-framed-ip-address	クライアントに割り当てる IP アドレスとネット マスクを指定します。
vpn-group-policy	属性の継承元となるグループ ポリシーの名前を指定します。
vpn-idle-timeout	アイドル タイムアウト期間を分単位で指定するか、または **none** を指定してディセーブルにします。
vpn-session-timeout	最大ユーザ接続時間を分単位で指定するか、または **none** を指定して時間を無制限にします。
vpn-simultaneous-logins	許可される同時ログインの最大数を指定します。
vpn-tunnel-protocol	使用できるトンネリング プロトコルを指定します。
webvpn	webvpn モードを開始して、webvpn 属性を設定できるようにします。

ユーザ名の webvpn モード属性を設定するには、ユーザ名 webvpn コンフィギュレーション モードで **username attributes** コマンドを入力してから、**webvpn** コマンドを入力します。詳細については、**webvpn** コマンド（グループ ポリシー属性モードおよびユーザ名属性モード）の説明を参照してください。

例

次に、「anyuser」という名前のユーザのユーザ名属性コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)#
```

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースをクリアします。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。

コマンド	説明
username	セキュリティ アプライアンス データベースにユーザを追加します。
webvpn	ユーザ名 webvpn コンフィギュレーション モードを開始し、指定したグループの WebVPN 属性を設定できるようにします。

username-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページ ログイン ボックスのユーザ名プロンプトをカスタマイズするには、Webvpn カスタマイゼーション モードで **username-prompt** コマンドを使用します。

username-prompt {**text** | **style**} *value*

[**no**] **username-prompt** {**text** | **style**} *value*

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。

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
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）です。

デフォルト

ユーザ名プロンプトのデフォルト テキストは、「USERNAME:」です。

ユーザ名プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

style オプションは有効な Cascading Style Sheet（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 Consortium（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。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するための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、テキストを「Corporate Username:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# username-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# username-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
group-prompt	WebVPN ページのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのパスワード プロンプトをカスタマイズします。

user-alert

現在のアクティブ セッションのすべてのクライアントレス SSL VPN ユーザに対して、緊急メッセージをブロードキャストするには、特権 EXEC モードで **user-alert** コマンドを使用します。メッセージをディセーブルにするには、このコマンドの no user-alert 形式を使用します。

user-alert *string cancel*

no user-alert

構文の説明

cancel	ポップアップ ブラウザ ウィンドウの起動を取り消します。
string	英数字

デフォルト

値の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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行すると、設定されたメッセージを含むポップアップ ブラウザ ウィンドウがエンドユーザに表示されます。このコマンドでは、セキュリティ アプライアンス コンフィギュレーション ファイルは変更されません。

例

次の例は、DAP トレース デバッグをイネーブルにする方法を示しています。

```
hostname # We will reboot the security appliance at 11:00 p.m. EST time. We apologize for
any inconvenience.
hostname #
```

user-message

DAP レコードが選択されたときに表示するテキスト メッセージを指定するには、ダイナミック アクセス ポリシー レコード モードで user-message コマンドを使用します。このメッセージを削除するには、このコマンドの **no** 形式を使用します。同じ DAP レコードに対してコマンドを複数回使用した場合、前のメッセージは新しいメッセージに置き換えられます。

user-message *message*

no user-message

構文の説明

message	この DAP レコードに割り当てられているユーザに対するメッセージ。最大 128 文字を入力できます。メッセージにスペースを含める場合は、メッセージを二重引用符で囲みます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ダイナミック アクセス ポリシー レコード	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

SSL VPN 接続に成功すると、ポータル ページに、クリック可能な点滅するアイコンが表示されます。ユーザはそのアイコンをクリックして、接続に関連付けられているメッセージを確認できます。DAP ポリシーからの接続が終了し（アクション = 終了）、その DAP レコードにユーザ メッセージが設定されている場合は、そのメッセージがログイン画面に表示されます。

複数の DAP レコードが接続に適用される場合、セキュリティ アプライアンスは該当するユーザ メッセージを組み合わせて 1 つのストリングとして表示します。

例

次に、Finance という DAP レコードに「Hello Money Managers」というユーザ メッセージを設定する例を示します。

```
hostname (config) config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# user-message "Hello Money Managers"
hostname(config-dynamic-access-policy-record)#
```

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。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

user-parameter

SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求パラメータの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **user-parameter** を使用します。これは HTTP フォームのコマンドを使用した SSO です。

user-parameter *name*

（注） HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	HTTP POST 要求に含まれているユーザ名パラメータの名前。名前の最大の長さは 128 文字です。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

セキュリティ アプライアンスの WebVPN サーバは、SSO サーバにシングル サインオン認証要求を送信することに HTTP POST 要求を使用します。要求されたコマンド **user-parameter** は、HTTP POST 要求に SSO 認証用のユーザ名パラメータを含める必要があることを指定します。

（注） ログイン時に、ユーザは実際の名前を入力します。この名前は、HTTP POST 要求に入力されて認証 Web サーバに渡されます。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、SSO 認証に使用される HTTP POST 要求にユーザ名パラメータ userid を含めることを指定する例を示します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# user-parameter userid
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。

user-storage

クライアントレス SSL VPN セッション間で設定された個人ユーザ情報を保存するには、グループ ポリシー webvpn モードで **user storage** コマンドを使用します。ユーザ ストレージをディセーブルにするには、このコマンドの **no** バージョンを使用します。

user-storage *NETFS-location*

no user-storage]

構文の説明

NETFS-location	ファイル システムの宛先を proto://user:password@host:port/path の形式で指定します。

デフォルト

ユーザストレージはディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ユーザ名、パスワード、および事前共有キーがコンフィギュレーションに示されていますが、セキュリティ アプライアンスではこの情報が内部アルゴリズムを使用して暗号化された形式で格納されるため、セキュリティのリスクは発生しません。

例

次に、anyfiler02a/new_share というパス、anyshare というファイル共有で、パスワードが 12345678 の newuser というユーザとして、ユーザ ストレージを設定する例を示します。

```
hostname(config)# wgroup-policy DFLTGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# user-storage cifs://newuser:12345678@anyfiler02a/new_share
hostname(config-group_webvpn)#
```

関連コマンド

コマンド	説明
storage-key	
storage-objects	

validate-attribute

RADIUS アカウンティングの使用時に RADIUS 属性を検証するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **validate attribute** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。

このオプションは、デフォルトで無効です。

validate-attribute [*attribute_number*]

no validate-attribute [*attribute_number*]

構文の説明

attribute_number	RADIUS アカウンティングで検証する RADIUS 属性。値の範囲は、1 ～ 191 です。ベンダー固有属性はサポートされません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
radius アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドを設定すると、セキュリティ アプライアンスは、Framed IP 属性に加えて RADIUS 属性に対する照合も実行します。このコマンドは、インスタンスを複数設定できます。

RADIUS 属性タイプのリストは、インターネット割り当て番号局の Web サイトで参照できます。

http://www.iana.org/assignments/radius-types/radius-types.xml

例

次に、ユーザ名 RADIUS 属性の RADIUS アカウンティングをイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# validate attribute 1
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクション ポリシー マップのパラメータを設定します。

validation-policy（クリプト CA トラスト ポイント）

着信ユーザ接続に関連付けられている証明書を検証するためにトラストポイントを使用できる条件を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **validation-policy** コマンドを使用します。指定した条件でトラストポイントを使用できないように指定するには、このコマンドの **no** 形式を使用します。

[no] validation-policy {ssl | ipsec} [no-chain] [subordinate-only]

構文の説明

ipsec	トラストポイントと関連付けられている Certificate Authority（CA; 認証局）証明書およびポリシーを IPSec 接続の検証に使用できることを指定します。
no-chain	セキュリティ デバイス上にない下位証明書のチェーンをディセーブルにします。
ssl	トラストポイントと関連付けられている Certificate Authority（CA; 認証局）証明書およびポリシーを SSL 接続の検証に使用できることを指定します。
subordinate-only	このトラストポイントで表される CA から直接発行されたクライアント証明書の検証をディセーブルにします。

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。

コマンド履歴

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

リモート アクセス VPN では、配置の要件に応じて、Secure Sockets Layer（SSL）VPN、IP Security（IPSec; IP セキュリティ）、またはこの両方を使用して、事実上すべてのネットワーク アプリケーションまたはリソースにアクセスを許可できます。**validation-policy** コマンドを使用して、オンボード CA 証明書へのアクセスに使用できるプロトコル タイプを指定できます。

このコマンドで **no-chain** オプションを指定すると、セキュリティ アプライアンスは、そのセキュリティ アプライアンスでトラストポイントとして設定されていない下位 CA 証明書をサポートできません。

セキュリティ アプライアンスでは、同じ CA に対して 2 つのトラストポイントを保持できます。これにより、同じ CA から 2 つの異なるアイデンティティ証明書が発行されます。トラストポイントが、この機能がイネーブルになっている別のトラストポイントにすでに関連付けられている CA に対して認証

される場合、このオプションは自動的にディセーブルになります。これにより、パス検証パラメータの選択であいまいさが生じないようになります。ユーザが、この機能をイネーブルにした別のトラストポイントにすでに関連付けられている CA に認証されたトラストポイントでこの機能を有効化しようとした場合、アクションは許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントを SSL トラストポイントとして指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# validation-policy ssl
hostname(config-ca-trustpoint)#
```

次に、トラストポイント checkin1 に対してクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントが指定したトラストポイントの下位証明書を受け入れるように設定する例を示します。

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# validation-policy subordinates-only
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
id-usage	トラストポイントの登録された ID の使用方法を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

verify

ファイルのチェックサムを確認するには、特権 EXEC モードで **verify** コマンドを使用します。

verify *path*

verify /md5 *path* [*md5-value*]

構文の説明

/md5	（任意）指定したソフトウェア イメージの MD5 値を計算して表示します。この値を、Cisco.com で入手できるこのイメージの値と比較します。
md5-value	（任意）指定したイメージの既知の MD5 値。コマンドで MD5 値を指定すると、指定したイメージの MD5 値が計算され、MD5 値が一致するかどうかを示すメッセージが表示されます。
path	• **disk0:**/[*path*/]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスだけで使用可能であり、内部フラッシュ メモリを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:**/[*path*/]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスだけで使用可能であり、外部フラッシュ メモリ カードを示します。 • **flash:**/[*path*/]*filename* このオプションは、内部フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、**flash** は **disk0** のエイリアスです。 • **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] **type** には次のキーワードのいずれかを指定できます。 – **ap**：ASCII 受動モード – **an**：ASCII 通常モード – **ip**：（デフォルト）バイナリ受動モード – **in**：バイナリ通常モード • **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 パス名にスペースを含めることはできません。パス名にスペースが含まれている場合は、**verify** コマンドではなく **tftp-server** コマンドでパスを設定します。

デフォルト

現在のフラッシュ デバイスがデフォルトのファイル システムです。

（注）　**/md5** オプションを指定する場合、ftp、http、tftp などのネットワーク ファイルをソースとして使用できます。**/md5** オプションを指定せずに **verify** コマンドを使用した場合は、フラッシュのローカル イメージのみを確認できます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(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

verify コマンドを使用して、ファイルを使用する前にそのチェックサムを確認します。

ディスクで配布される各ソフトウェア イメージでは、イメージ全体に対して 1 つのチェックサムが使用されます。このチェックサムは、イメージをフラッシュ メモリにコピーする場合にのみ表示され、イメージ ファイルをあるディスクから別のディスクにコピーする場合は表示されません。

新しいイメージをロードまたは複製する前に、そのイメージのチェックサムと MD5 情報を記録しておき、イメージをフラッシュ メモリまたはサーバにコピーするときにチェックサムを確認できるようにします。Cisco.com では、さまざまなイメージ情報を入手できます。

フラッシュ メモリの内容を表示するには、**show flash** コマンドを使用します。フラッシュ メモリの内容のリストには、個々のファイルのチェックサムは含まれません。イメージをフラッシュ メモリにコピーした後で、そのイメージのチェックサムを再計算して確認するには、**verify** コマンドを使用します。ただし、**verify** コマンドでは、ファイルがファイル システムに保存された後にのみ、整合性チェックを実行します。破損しているイメージがセキュリティ アプライアンスに転送され、検出されずにファイル システムに保存される場合があります。破損しているイメージが正常にセキュリティ アプライアンスに転送されると、ソフトウェアはイメージが壊れていることを把握できず、ファイルの確認が正常に完了します。

Message-Digest5（MD5; メッセージ ダイジェスト 5）ハッシュ アルゴリズムを使用してファイルを検証するには、**/md5** オプションを指定して **verify** コマンドを使用します。MD5（RFC 1321 で規定）は、一意の 128 ビットのメッセージ ダイジェストを作成することによってデータ整合性を確認するアルゴリズムです。**verify** コマンドの **/md5** オプションを使用すると、セキュリティ アプライアンスのソフトウェア イメージの MD5 チェックサム値を、その既知の MD5 チェックサム値と比較することによって、イメージの整合性を確認できます。すべてのセキュリティ アプライアンスのソフトウェア イメージの MD5 値は、ローカル システムのイメージの値と比較するために、Cisco.com から入手できるようになっています。

MD5 整合性チェックを実行するには、**/md5** キーワードを指定して **verify** コマンドを発行します。たとえば、**verify /md5 flash:cdisk.bin** コマンドを発行すると、ソフトウェア イメージの MD5 値が計算され、表示されます。この値を、Cisco.com で入手できるこのイメージの値と比較します。

または、まず Cisco.com から MD5 値を取得し、その値をコマンド構文で指定できます。たとえば、**verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** コマンドを発行すると、MD5 値が一致するかどうかを示すメッセージが表示されます。MD5 値が一致しない場合は、いずれかのイメージが破損しているか、または入力した MD5 値が正しくありません。

例

次に、cdisk.bin というイメージ ファイルに対して使用された verify コマンドの例を示します。わかりやすくするために、一部のテキストは省略されています。

```
hostname# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash      MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
hostname#
```

関連コマンド

コマンド	説明
copy	ファイルをコピーします。
dir	システム内のファイルを一覧表示します。

version

セキュリティ アプライアンスでグローバルに使用する RIP のバージョンを指定するには、ルータ コンフィギュレーション モードで **version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

version {**1** | **2**}

no version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは、バージョン 1 およびバージョン 2 のパケットを受信しますが、送信するのはバージョン 1 のパケットのみです。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

インターフェイスで **rip send version** コマンドと **rip receive version** コマンドを入力することによって、インターフェイスごとにグローバルな設定を上書きすることができます。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、すべてのインターフェイスで RIP バージョン 2 のパケットを送受信するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。

virtual http

仮想 HTTP サーバを設定するには、グローバル コンフィギュレーション モードで **virtual http** コマンドを使用します。仮想サーバ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。

virtual http *ip_address* [**warning**]

no virtual http *ip_address* [**warning**]

構文の説明

ip_address	セキュリティ アプライアンス上の仮想 HTTP サーバの IP アドレスを設定します。このアドレスは必ず、セキュリティ アプライアンスにルーティングされる未使用のアドレスにしてください。
warning	（任意）HTTP 接続をセキュリティ アプライアンスにリダイレクトする必要があることをユーザに通知します。このキーワードは、リダイレクトが自動的に行われないテキストベースのブラウザにのみ適用されます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	以前のリリースで使用されていたインライン基本 HTTP 認証方式がリダイレクション方式に置き換えられたため、このコマンドは廃止され、不要になりました。
7.2(2)	**aaa authentication listener** コマンドを使用して、基本 HTTP 認証（デフォルト）と HTTP リダイレクションのいずれを使用するかを選択できるようになったため、このコマンドは復活しました。リダイレクション方式では、HTTP 認証をカスケードするための特別なコマンドは必要ありません。

使用上のガイドライン

セキュリティ アプライアンスで HTTP 認証を使用する場合は（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、セキュリティ アプライアンスで基本 HTTP 認証がデフォルトで使用されます。**redirect** キーワードを指定した **aaa authentication listener** を使用して、セキュリティ アプライアンスが HTTP 接続をセキュリティ アプライアンスによって生成された Web ページにリダイレクトするように認証方式を変更できます。

ただし、基本 HTTP 認証の使用を続行する場合は、HTTP 認証をカスケードするときに **virtual http** コマンドが必要になることがあります。

セキュリティ アプライアンスに加えて宛先 HTTP サーバで認証が必要な場合は、**virtual http** コマンドを使用して、セキュリティ アプライアンス（AAA サーバ経由）と HTTP サーバで別々に認証を受けることができます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。AAA サーバと HTTP サーバでユーザ名とパスワードが異なる場合、HTTP 認証は失敗します。

このコマンドは、AAA 認証を必要とするすべての HTTP 接続をセキュリティ アプライアンス上の仮想 HTTP サーバにリダイレクトします。セキュリティ アプライアンスにより、AAA サーバのユーザ名とパスワードの入力を求めるプロンプトが表示されます。AAA サーバがユーザを認証すると、セキュリティ アプライアンスは HTTP 接続を元のサーバにリダイレクトして戻しますが、AAA サーバのユーザ名とパスワードは含めません。HTTP パケットにユーザ名とパスワードが含まれていないため、HTTP サーバによりユーザに HTTP サーバのユーザ名とパスワードの入力を求めるプロンプトが別途表示されます。

着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス リストに宛先インターフェイスとして仮想 HTTP アドレスも含める必要があります。さらに、NAT が必要ない場合でも（**no nat-control** コマンドを使用）、仮想 HTTP IP アドレスに対する **static** コマンドを追加する必要があります。通常、アイデンティティ NAT コマンドが使用されます（アドレスを同一アドレスに変換）。

発信ユーザについては、トラフィックの許可は明示的に行われますが、内部インターフェイスにアクセス リストを適用する場合は、必ず仮想 HTTP アドレスへのアクセスを許可してください。**static** ステートメントは不要です。

（注）　**virtual http** コマンドを使用する場合は、**timeout uauth** コマンドの期間を 0 秒に設定しないでください。設定すると、実際の Web サーバへの HTTP 接続ができなくなります。

例

次に、AAA 認証とともに仮想 HTTP をイネーブルにする例を示します。

```
hostname(config)# virtual http 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq http
hostname(config)# access-list ACL-IN remark This is the HTTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list ACL-IN remark This is the virtual HTTP address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq http
hostname(config)# access-list AUTH remark This is the HTTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list AUTH remark This is the virtual HTTP address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

関連コマンド

コマンド	説明
aaa authentication listener http	セキュリティ アプライアンスが認証に使用する方式を設定します。
clear configure virtual	コンフィギュレーションから **virtual** コマンド ステートメントを削除します。
show running-config virtual	セキュリティ アプライアンス仮想サーバの IP アドレスを表示します。

sysopt uauth allow-http-cache	**virtual http** コマンドをイネーブルにする場合は、このコマンドを使用すると、ブラウザ キャッシュ内のユーザ名とパスワードを使用して仮想サーバに再接続できます。
virtual telnet	セキュリティ アプライアンス上に仮想 Telnet サーバを設定して、認証を必要とする他のタイプの接続を開始する前に、ユーザをセキュリティ アプライアンスで認証できるようにします。

virtual telnet

セキュリティ アプライアンス上に仮想 Telnet サーバを設定するには、グローバル コンフィギュレーション モードで **virtual telnet** コマンドを使用します。セキュリティ アプライアンスによって認証プロンプトが表示されない他のタイプのトラフィックに対する認証が必要な場合は、仮想 Telnet サーバでユーザを認証する必要があります。サーバ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。

virtual telnet *ip_address*

no virtual telnet *ip_address*

構文の説明

ip_address	セキュリティ アプライアンス上の仮想 Telnet サーバの IP アドレスを設定します。このアドレスは必ず、セキュリティ アプライアンスにルーティングされる未使用のアドレスにしてください。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

任意のプロトコルまたはサービスのネットワーク アクセス認証を設定できますが（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、HTTP、Telnet、または FTP のみで直接認証することもできます。ユーザはまずこれらのサービスのいずれかで認証を行ってから、認証を要求する他のトラフィックの通過を認可する必要があります。HTTP、Telnet、または FTP のセキュリティ アプライアンスの通過を許可せず、その他のタイプのトラフィックを認証する場合は、セキュリティ アプライアンス上で設定された所定の IP アドレスにユーザが Telnet で接続し、セキュリティ アプライアンスによって Telnet プロンプトが表示されるように、仮想 Telnet を設定できます。

authentication match コマンドまたは **aaa authentication include** コマンドを使用して、仮想 Telnet アドレスおよび認証するその他のサービスへの Telnet アクセスに対する認証を設定する必要があります。

認証が済んでいないユーザが仮想 Telnet IP アドレスに接続すると、ユーザはユーザ名とパスワードを求められ、その後 AAA サーバにより認証されます。認証されると、ユーザには「Authentication Successful.」というメッセージが表示されます。それ以降、ユーザは認証を必要とする他のサービスに正常にアクセスできます。

着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス リストに宛先インターフェイスとして仮想 Telnet アドレスも含める必要があります。さらに、NAT が必要ない場合でも（**no nat-control** コマンドを使用）、仮想 Telnet IP アドレスに対する **static** コマンドを追加する必要があります。通常、アイデンティティ NAT コマンドが使用されます（アドレスを同一アドレスに変換）。

発信ユーザについては、トラフィックの許可は明示的に行われますが、内部インターフェイスにアクセス リストを適用する場合は、必ず仮想 Telnet アドレスへのアクセスを許可してください。**static** ステートメントは不要です。

セキュリティ アプライアンスからログアウトするには、仮想 Telnet IP アドレスに再接続します。ログアウトするように求められます。

例

次に、他のサービスに対する AAA 認証とともに仮想 Telnet をイネーブルにする例を示します。

```
hostname(config)# virtual telnet 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list ACL-IN remark This is the SMTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq
telnet
hostname(config)# access-list ACL-IN remark This is the virtual Telnet address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list AUTH remark This is the SMTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
hostname(config)# access-list AUTH remark This is the virtual Telnet address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

関連コマンド

コマンド	説明
clear configure virtual	コンフィギュレーションから **virtual** コマンド ステートメントを削除します。
show running-config virtual	セキュリティ アプライアンス仮想サーバの IP アドレスを表示します。
virtual http	セキュリティ アプライアンス上で HTTP 認証を使用し、HTTP サーバも認証を要求する場合は、このコマンドを使用して、セキュリティ アプライアンスと HTTP サーバで別々に認証を受けることができます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。

vlan

VLAN ID をサブインターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN ID を削除するには、このコマンドの **no** 形式を使用します。サブインターフェイスでは、トラフィックを通過させるために VLAN ID が必要です。VLAN サブインターフェイスを使用して、1 つの物理インターフェイスに複数の論理インターフェイスを設定できます。VLAN を使用すると、所定の物理インターフェイス上で複数のセキュリティ コンテキストなどのトラフィックを別々に保管できます。

vlan *id*

no vlan

構文の説明

id	1 ～ 4094 の範囲の整数を指定します。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。

使用上のガイドライン

1 つの VLAN をサブインターフェイスにのみ割り当てることができます。物理インターフェイスに割り当てることはできません。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために **no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して **vlan** コマンドを入力すると、セキュリティ アプライアンスによって古い ID が変更されます。

サブインターフェイスをイネーブルにするには、**no shutdown** コマンドを使用して物理インターフェイスをイネーブルにする必要があります。サブインターフェイスをイネーブルにする場合、通常は、物理インターフェイスをトラフィックが通過しないようにします。これは、物理インターフェイスはタグなしパケットを通過させるためです。したがって、インターフェイスの停止によってトラフィックが物理インターフェイスを通過しないようにすることはできません。代わりに、**nameif** コマンドを省略することによって、トラフィックが物理インターフェイスを通過しないようにします。物理インターフェイスでタグなしパケットを通過させる場合は、通常どおり **nameif** コマンドを設定できます。

サブインターフェイスの最大数は、プラットフォームによって異なります。プラットフォームごとのサブインターフェイスの最大数については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

例

次に、VLAN 101 をサブインターフェイスに割り当てる例を示します。

```
hostname(config)# interface gigabitethernet0/0.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次に、VLAN を 102 に変更する例を示します。

```
hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0

hostname(config)# interface gigabitethernet0/0.1
hostname(config-interface)# vlan 102

hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブ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 running-config interface	インターフェイスの現在のコンフィギュレーションを表示します。

vlan（グループ ポリシー）

VLAN をグループ ポリシーに割り当てるには、グループ ポリシー コンフィギュレーション モードで **vlan** コマンドを使用します。グループ ポリシーのコンフィギュレーションから VLAN を削除し、デフォルトのグループ ポリシーの VLAN 設定に置き換えるには、このコマンドの **no** 形式を使用します。

[**no**] **vlan** {*vlan_id* |**none**}

構文の説明

vlan_id	このグループ ポリシーを使用するリモート アクセス VPN セッションに割り当てる VLAN の番号（10 進表記）。インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用して、このセキュリティ アプライアンスに VLAN を設定する必要があります。
none	このグループ ポリシーに一致するリモート アクセス VPN セッションへの VLAN の割り当てをディセーブルにします。グループ ポリシーは、デフォルトのグループ ポリシーから vlan 値を継承しません。

デフォルト

デフォルト値は none 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(0)	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、このグループ ポリシーに割り当てられているセッションの出力 VLAN インターフェイスを指定します。セキュリティ アプライアンスは、このグループのすべてのトラフィックを指定された VLAN に転送します。VLAN を各グループ ポリシーに割り当ててアクセス コントロールを簡素化できます。このコマンドは、セッション上のトラフィックをフィルタリングする ACL の代わりに使用します。

例

次のコマンドでは、VLAN 1 をグループ ポリシーに割り当てます。

```
hostname(config-group-policy)# vlan 1
hostname(config-group-policy)
```

次のコマンドでは、VLAN マッピングをグループ ポリシーから削除します。

```
hostname(config-group-policy)# vlan none
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
show vlan	セキュリティ アプライアンスに設定されている VLAN を表示します。
vlan（インターフェイス コンフィギュレーション モード）	サブインターフェイスに VLAN ID を割り当てます。
show vpn-session_summary.db	IPSec、Cisco AnyConnect、NAC の各セッションの数および使用中の VLAN の数を表示します。
show vpn-session.db	VLAN マッピングと NAC の結果を含む、VPN セッションの情報を表示します。

vpdn group

VPDN グループを作成または編集し、PPPoE クライアントを設定するには、グローバル コンフィギュレーション モードで **vpdn group** コマンドを使用します。コンフィギュレーションからグループ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

vpdn group *group_name* {**localname** *username* | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

no vpdn group *group_name* {**localname** *name* | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

（注） PPPoE は、セキュリティ アプライアンスでフェールオーバーを設定している場合、またはマルチ コンテキスト モードやトランスペアレント モードではサポートされません。PPPoE がサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

構文の説明

vpdn group *group_name*	VPDN グループの名前を指定します。
localname *username*	ユーザ名を認証のために VPDN グループにリンクし、**vpdn username** コマンドで設定された名前と照合する必要があります。
request dialout pppoe	ダイヤルアウト PPPoE 要求を許可することを指定します。
ppp authentication {chap | mschap | pap}}	Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）認証プロトコルを指定します。Windows クライアントのダイヤルアップ ネットワーク設定を使用して、使用する認証プロトコル（PAP、CHAP、または MS-CHAP）を指定できます。クライアントで指定した設定は、セキュリティ アプライアンスで使用する設定と一致している必要があります。Password Authentication Protocol（PAP; パスワード認証プロトコル）を使用すると、PPP ピアは相互に認証できます。PAP は、ホスト名またはユーザ名をクリアテキストで渡します。Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）を使用すると、PPP ピアは、アクセス サーバとの通信によって不正アクセスを防止できます。MS-CHAP は Microsoft 版の CHAP です。PIX Firewall では、MS-CHAP バージョン 1 のみサポートされます（バージョン 2.0 はサポートされません）。 ホストで認証プロトコルが指定されていない場合は、コンフィギュレーションで **ppp authentication** オプションを指定しないでください。

デフォルト

デフォルトの動作や値はありません。「使用上のガイドライン」を参照してください。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2.1	このコマンドが導入されました。

使用上のガイドライン

Virtual Private Network（VPDN; バーチャル プライベート ネットワーク）は、リモート ダイヤルイン ユーザとプライベート ネットワーク間の長距離のポイントツーポイント接続を提供するために使用します。セキュリティ アプライアンス上の VDPN では、レイヤ 2 トンネリング技術の PPPoE を使用して、リモート ユーザからパブリック ネットワーク経由のプライベート ネットワークへのダイヤルアップ ネットワーク接続を確立します。

PPPoE は、Point-to-Point Protocol（PPP）over Ethernet です。PPP は、IP、IPX、ARA などのネットワーク層プロトコルで動作するように設計されています。PPP には、セキュリティ メカニズムとして CHAP と PAP も組み込まれています。

PPPoE 接続のセッション情報を表示するには、**show vpdn session pppoe** コマンドを使用します。コンフィギュレーションからすべての **vpdn group** コマンドを削除して、すべてのアクティブな L2TP トンネルと PPPoE トンネルを停止するには、**clear configure vpdn group** コマンドを使用します。**clear configure vpdn username** コマンドは、すべての **vpdn username** コマンドをコンフィギュレーションから削除します。

PPPoE は PPP をカプセル化するため、PPPoE は PPP を使用して、認証および VPN トンネル内で動作しているクライアント セッションに対する ECP 機能と CCP 機能を実行します。さらに、PPP によって PPPoE に IP アドレスが割り当てられるため、PPPoE と DHCP の併用はサポートされません。

（注） PPPoE に VPDN グループが設定されていない場合、PPPoE は接続を確立できません。

PPPoE に使用する VPDN グループを定義するには、**vpdn group** *group_name* **request dialout pppoe** コマンドを使用します。次に、インターフェイス コンフィギュレーション モードで **pppoe client vpdn group** コマンドを使用して、VPDN グループを特定のインターフェイス上の PPPoE クライアントに関連付けます。

ISP が認証を要求している場合は、**vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} コマンドを使用して、ISP で使用される認証プロトコルを選択します。

ISP によって割り当てられたユーザ名を VPDN グループに関連付けるには、**vpdn group** *group_name* **localname** *username* コマンドを使用します。

PPPoE 接続用のユーザ名とパスワードのペアを作成するには、**vpdn username** *username* password *password* コマンドを使用します。ユーザ名は、PPPoE に指定した VPDN グループにすでに関連付けられているユーザ名にする必要があります。

（注）　ISP で CHAP または MS-CHAP が使用されている場合、ユーザ名はリモート システム名、パスワードは CHAP シークレットと呼ばれることがあります。

PPPoE クライアント機能はデフォルトでオフになっているため、VPDN の設定後、**ip address** *if_name* **pppoe** [**setroute**] コマンドを使用して PPPoE をイネーブルにします。**setroute** オプションを指定すると、デフォルト ルートが存在しない場合にデフォルト ルートが作成されます。

PPPoE の設定後すぐに、セキュリティ アプライアンスは通信する PPPoE アクセス コンセントレータを探します。PPPoE 接続が正常終了または異常終了すると、セキュリティ アプライアンスは通信する新しいアクセス コンセントレータを探します。

次の **ip address** コマンドは、PPPoE セッションの開始後に使用しないでください。使用すると、PPPoE セッションが終了します。

- **ip address outside pppoe**：このコマンドは新しい PPPoE セッションを開始しようとします。
- **ip address outside dhcp**：このコマンドは、インターフェイスがその DHCP 設定を取得するまでインターフェイスをディセーブルにします。
- **ip address outside** *address netmask*：インターフェイスが正常に初期化されたインターフェイスとして起動するため。

例

次に、VDPN グループ *telecommuters* を作成し、PPPoE クライアントを設定する例を示します。

```
F1(config)# vpdn group telecommuters request dialout pppoe
F1(config)# vpdn group telecommuters localname user1
F1(config)# vpdn group telecommuters ppp authentication pap
F1(config)# vpdn username user1 password test1
F1(config)# interface GigabitEthernet 0/1
F1(config-subif)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての vpdn group コマンドをコンフィギュレーションから削除します。
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show vpdn group *group_name*	VPDN グループのコンフィギュレーションを表示します。
vpdn username	PPPoE 接続用のユーザ名とパスワードのペアを作成します。

vpdn username

PPPoE 接続用のユーザ名とパスワードのペアを作成するには、グローバル コンフィギュレーション モードで **vpdn username** コマンドを使用します。

vpdn username *username* **password** *password* [**store-local**]

no vpdn username *username* **password** *password* [**store-local**]

（注） PPPoE は、セキュリティ アプライアンスでフェールオーバーを設定している場合、またはマルチ コンテキスト モードやトランスペアレント モードではサポートされません。PPPoE がサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

構文の説明

username	ユーザ名を指定します。
password	パスワードを指定します。
store-local	ユーザ名とパスワードをセキュリティ アプライアンス上の NVRAM の特別な場所に保存します。Auto Update Server が clear config コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。

デフォルト

デフォルトの動作や値はありません。「使用上のガイドライン」を参照してください。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

VPDN ユーザ名は、**vpdn group** *group_name* **localname** *username* コマンドで指定された VPDN グループにすでに関連付けられているユーザ名にする必要があります。

clear configure vpdn username コマンドは、すべての **vpdn username** コマンドをコンフィギュレーションから削除します。

例

次に、パスワードが *telecommuter*9/8 の *bob_smith* という VPDN ユーザ名を作成する例を示します。

```
F1(config)# vpdn username bob_smith password telecommuter9/8
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての vpdn group コマンドをコンフィギュレーションから削除します。
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show vpdn group	VPDN グループのコンフィギュレーションを表示します。
vpdn group	VPDN グループを作成し、PPPoE クライアントを設定します。

vpn-access-hours

グループ ポリシーを設定済み time-range ポリシーに関連付けるには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-access-hours** コマンドを使用します。実行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。このオプションを使用すると、他のグループ ポリシーから time-range 値を継承できます。値が継承されないようにするには、**vpn-access-hours none** コマンドを使用します。

vpn-access hours value {*time-range*} | **none**

no vpn-access hours

構文の説明

none	VPN アクセス時間をヌル値に設定して、time-range ポリシーを許可しないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
time-range	設定済みの時間範囲ポリシーの名前を指定します。

デフォルト

制限なし。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、FirstGroup というグループ ポリシーを 824 という time-range ポリシーに関連付ける例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours 824
```

関連コマンド

コマンド	説明
time-range	ネットワークにアクセスする曜日と 1 日の時間を設定します（開始日と終了日を含む）。

vpn-addr-assign

IP アドレスをリモート アクセス クライアントに割り当てる方法を指定するには、グローバル コンフィギュレーション モードで **vpn-addr-assign** 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** バージョンを使用します。設定したすべての VPN アドレス割り当て方法をセキュリティ アプライアンスから削除するには、このコマンドの **no** 形式を使用します。引数なしで

vpn-addr-assign {**aaa | dhcp | local** [**reuse-delay** *delay*]}

no vpn-addr-assign {**aaa | dhcp | local** [**reuse-delay** *delay*]}

構文の説明

aaa	外部または内部（ローカル）AAA 認証サーバから IP アドレスを取得します。
dhcp	DHCP 経由で IP アドレスを取得します。
local	セキュリティ アプライアンスに設定されている IP アドレス プールから IP アドレスを割り当てて、トンネル グループに関連付けます。
reuse-delay *delay*	解放された IP アドレスを再利用するまでの遅延時間。指定できる範囲は 0 ～ 480 分です。デフォルトは 0（ディセーブル）です。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(3)	**reuse-delay** オプションが追加されました。

使用上のガイドライン

DHCP を選択する場合は、**dhcp-network-scope** コマンドを使用して、DHCP サーバが使用できる IP アドレスの範囲も定義する必要があります。DHCP サーバが使用する IP アドレスを指定するには、**dhcp-server** コマンドを使用する必要があります。

ローカルを選択する場合は、**ip local pool** コマンドを使用して、使用する IP アドレスの範囲を定義する必要があります。次に、**vpn-framed-ip-address** コマンドと **vpn-framed-netmask** コマンドを使用して、IP アドレスとネットマスクを個々のユーザに割り当てます。

ローカル プールを使用する場合は、**reuse-delay** *delay* オプションを使用して、解放された IP アドレスを再利用するまでの遅延時間を調整します。遅延時間を長くすると、IP アドレスがプールに戻されて即座に再割り当てされるときにファイアウォールで発生する可能性がある問題を回避できます。

AAA を選択する場合は、設定済みのいずれかの RADIUS サーバから IP アドレスを取得します。

例

次に、アドレス割り当て方法として DHCP を設定する例を示します。

```
hostname(config)# vpn-addr-assign dhcp
```

関連コマンド

コマンド	説明
dhcp-network-scope	セキュリティ アプライアンス DHCP サーバがグループ ポリシーのユーザにアドレスを割り当てるために使用する IP アドレスの範囲を指定します。
ip local pool	ローカル IP アドレス プールを作成します。
vpn-framed-ip-address	特定のユーザに割り当てる IP アドレスを指定します。
vpn-framed-ip-netmask	特定のユーザに割り当てるネットマスクを指定します。

vpn-filter

VPN 接続に使用する ACL の名前を指定するには、グローバル ポリシーまたはユーザ名モードで **vpn-filter** コマンドを使用します。**vpn-filter none** コマンドを発行して作成したヌル値を含む ACL を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。値が継承されないようにするには、**vpn-filter none** コマンドを使用します。

このユーザまたはグループ ポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。次に、**vpn-filter** コマンドを使用して、それらの ACL を適用します。

vpn-filter {**value** *ACL name* | **none**}

no vpn-filter

構文の説明

none	アクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACL name*	事前に設定済みのアクセス リストの名前を指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

vpn-filter コマンドで定義された ACL は、クライアントレス SSL VPN 接続には適用されません。この ACL は、IPSec と SSL VPN クライアント セッションのみに適用されます。

例

次に、FirstGroup という名前のグループ ポリシーの、acl_vpn というアクセス リストを呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter value acl_vpn
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。

vpn-framed-ip-address

特定のユーザに割り当てる IP アドレスを指定するには、ユーザ名モードで **vpn-framed-ip-address** コマンドを使用します。IP 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。

vpn-framed-ip-address {*ip_address*}

no vpn-framed-ip-address

構文の説明

ip_address	このユーザの IP アドレスを指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、anyuser という名前のユーザに IP アドレス 10.92.166.7 を設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
```

vpn-group-policy

ユーザが設定済みのグループ ポリシーから属性を継承するようにするには、ユーザ名コンフィギュレーション モードで **vpn-group-policy** コマンドを使用します。グループ ポリシーをユーザ 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。このコマンドを使用すると、ユーザはユーザ名レベルで設定されていない属性を継承できます。

vpn-group-policy {*group-policy name*}

no vpn-group-policy {*group-policy name*}

構文の説明

group-policy name	グループ ポリシーの名前を指定します。

デフォルト

デフォルトでは、VPN ユーザにはグループ ポリシーが関連付けられません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

特定ユーザのグループ ポリシーの属性値を上書きするには、その値をユーザ名モードで設定します（その属性をユーザ名モードで使用できる場合）。

例

次に、FirstGroup という名前のグループ ポリシーから属性を使用するように anyuser という名前のユーザを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーをセキュリティ アプライアンス データベースに追加します。
group-policy attributes	グループ ポリシー属性モードを開始します。これにより、グループ ポリシーの AVP を設定できます。
username	セキュリティ アプライアンス データベースにユーザを追加します。
username attributes	ユーザ名属性モードを開始します。これにより、特定のユーザの AVP を設定できます。

vpn-idle-timeout

ユーザ タイムアウト期間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを使用します。この期間中に接続上で通信アクティビティがない場合、セキュリティ アプライアンスは接続を終了します。

実行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。このオプションを使用すると、他のグループ ポリシーからタイムアウト値を継承できます。値が継承されないようにするには、**vpn-idle-timeout none** コマンドを使用します。

vpn-idle-timeout {*minutes* | **none**}

no vpn-idle-timeout

構文の説明

minutes	タイムアウト期間の分数を指定します。1 ～ 35791394 の整数を使用します。
none	無制限のアイドル タイムアウト期間を許可します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

デフォルト

30 分。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、「FirstGroup」という名前のグループ ポリシーに対して 15 分の VPN アイドル タイムアウトを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 30
```

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-session-timeout	VPN 接続の最大許容時間を設定します。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

vpn load-balancing

VPN ロード バランシングおよび関連機能を設定できる VPN ロード バランシング モードを開始するには、グローバル コンフィギュレーション モードで **vpn load-balancing** コマンドを使用します。

vpn load-balancing

（注） VPN ロード バランシングを使用するには、Plus ライセンスを備えた ASA モデル 5510、または ASA モデル 5520 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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 モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	ASA Model 5510（Plus ライセンス付き）および ASA Model 5520 以降のサポートが追加されました。

使用上のガイドライン

ロード バランシング クラスタには、セキュリティ アプライアンス モデル 5510（Plus ライセンス付き）または ASA 5520 以降を含めることができます。VPN 3000 シリーズのコンセントレータも含めることができます。混合コンフィギュレーションは可能ですが、通常は、同種クラスタにする方が容易に管理できます。

vpn load-balancing コマンドを使用して、VPN ロード バランシング モードを開始します。VPN ロード バランシング モードでは、次のコマンドを使用できます。

- cluster encryption
- cluster ip address
- cluster key

- cluster port
- interface
- nat
- participate
- priority
- redirect-fqdn

詳細については、個々のコマンドの説明を参照してください。

例

次に、**vpn load-balancing** コマンドの例を示します。プロンプトが変わる点に注意してください。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

次に、interface コマンドを含む VPN load-balancing コマンド シーケンスの例を示します。interface コマンドでは、クラスタのパブリック インターフェイスを「test」、クラスタのプライベート インターフェイスを「foo」と指定しています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

コマンド	説明
clear configure vpn load-balancing	ロード バランシングの実行時コンフィギュレーションを削除し、ロード バランシングをディセーブルにします。
show running-config vpn load-balancing	現在の VPN ロード バランシング仮想クラスタのコンフィギュレーションを表示します。
show vpn load-balancing	VPN ロード バランシング実行時の統計情報を表示します。

vpn-sessiondb logoff

すべての VPN セッションまたは選択した VPN セッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff** コマンドを使用します。

vpn-sessiondb logoff {**remote** | **l2l** | **webvpn** | **email-proxy** | **protocol** *protocol-name* | **name** *username* | **ipaddress** *IPaddr* | **tunnel-group** *groupname* | **index** *indexnumber* | **all**}

構文の説明

all	すべての VPN セッションをログオフします。
email-proxy	すべての電子メール プロキシ セッションをログオフします。
index *indexnumber*	インデックス番号で 1 つのセッションをログオフします。セッションのインデックス番号を指定します。
ipaddress *IPaddr*	指定した IP アドレスのセッションをログオフします。
l2l	すべての LAN-to-LAN セッションをログオフします。
name *username*	指定したユーザ名のセッションをログオフします。
protocol *protocol-name*	指定したプロトコルのセッションをログオフします。プロトコルは次のとおりです。 IKE　POP3S IMAP4S　SMTPS IPSec　userHTTPS IPSecLAN2LAN　vcaLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP
remote	すべてのリモートアクセス セッションをログオフします。
tunnel-group *groupname*	指定したトンネル グループのセッションをログオフします。
webvpn	すべての WebVPN セッションをログオフします。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、すべてのリモートアクセス セッションをログオフする例を示します。

```
hostname# vpn-sessiondb logoff remote
```

次に、すべての IPSec セッションをログオフする例を示します。

```
hostname# vpn-sessiondb logoff protocol IPSec
```

vpn-sessiondb max-session-limit

VPN セッションをセキュリティ アプライアンスで許可されているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-session-limit** コマンドを使用します。セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。現在の設定を上書きするには、このコマンドを再度使用します。

vpn-sessiondb max-session-limit {*session-limit*}

no **vpn-sessiondb max-session-limit**

構文の説明

session-limit	許可される最大 VPN セッション数を指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

このコマンドは、IPSec VPN セッションに適用されます。

例

次に、最大 VPN セッション数の制限を 450 に設定する例を示します。

```
hostname# vpn-sessiondb max-session-limit 450
```

関連コマンド

コマンド	説明
vpn-sessiondb logoff	すべて、または特定のタイプの IPSec VPN セッションおよび WebVPN セッションをログオフします。
vpn-sessiondb max-webvpn-session-limit	WebVPN セッションの最大数を設定します。

vpn-sessiondb max-webvpn-session-limit

SSL VPN セッションをセキュリティ アプライアンスで許可されているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-webvpn-session-limit** コマンドを使用します。セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。現在の設定を上書きするには、このコマンドを再度使用します。

vpn-sessiondb max-webvpn-session-limit {*session-limit*}

no vpn-sessiondb max-webvpn-session-limit

構文の説明

session-limit	許可される最大 WebVPN セッション数を指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

このコマンドは、SSL VPN セッション（AnyConnect VPN Client、レガシー SSL VPN Client（SVC）、クライアントレス（以前の WebVPN）セッションなど）に適用されます。

例

次に、最大セッション数の制限を 75 に設定する例を示します。

```
hostname (config)# vpn-sessiondb max-webvpn-session-limit 75
```

関連コマンド

コマンド	説明
vpn-sessiondb logoff	すべて、または特定のタイプの IPSec VPN セッションおよび SSL VPN セッションをログオフします。
vpn-sessiondb max-vpn-session-limit	VPN セッションの最大数を設定します。

vpn-session-timeout

VPN 接続に許可される最大時間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用します。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

実行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。このオプションを使用すると、他のグループ ポリシーからタイムアウト値を継承できます。値が継承されないようにするには、**vpn-session-timeout none** コマンドを使用します。

vpn-session-timeout {*minutes* | **none**}

no vpn-session-timeout

構文の説明

minutes	タイムアウト期間の分数を指定します。1 ～ 35791394 の整数を使用します。
none	無制限のセッション タイムアウト期間を許可します。セッション タイムアウトにヌル値を設定して、セッション タイムアウトを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、FirstGroup という名前のグループ ポリシーに対して 180 分の VPN セッション タイムアウトを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
```

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-idle-timeout	ユーザ タイムアウト期間を設定します。この期間中に接続上で通信アクティビティがない場合、セキュリティ アプライアンスは接続を終了します。

vpn-simultaneous-logins

ユーザに許可される同時ログイン数を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用します。実行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。このオプションを使用すると、別のグループ ポリシーの値を継承できます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

vpn-simultaneous-logins {*integer*}

no vpn-simultaneous-logins

構文の説明

integer	0 ～ 2147483647 の数字。

デフォルト

デフォルトの同時ログイン数は、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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

（注） 同時ログイン数の最大制限は非常に大きい値ですが、複数の同時ログインを許可すると、セキュリティが侵害されたり、パフォーマンスが低下したりすることがあります。

失効した AnyConnect、IPSec クライアント、またはクライアントレス セッション（異常終了したセッション）は、同じユーザ名で「新しい」セッションが確立されても、セッション データベースに残る場合があります。

vpn-simultaneous-logins の値が 1 の場合は、異常終了後に同じユーザが再度ログインすると、失効したセッションはデータベースから削除され、新しいセッションが確立されます。ただし、既存のセッションがまだアクティブな接続である場合は、同じユーザが別の PC などから再度ログインすると、最初のセッションがログオフし、データベースから削除されて、新しいセッションが確立されます。

同時ログイン数が 1 より大きい値の場合、その最大数に達した状態で再度ログインしようとすると、最もアイドル時間の長いセッションがログオフします。現在のすべてのセッションが同じくらい長い間アイドル状態の場合は、最も古いセッションがログオフします。このアクションにより、セッションが解放されて新しいログインが可能になります。

例

次に、FirstGroup という名前のグループ ポリシーに対して最大 4 つの同時ログインを許可する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

VPN トンネル タイプ（IPSec、L2TP over IPSec、SVC、または WebVPN）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 モードまたはユーザ名コンフィギュレーション モードで **vpn-tunnel-protocol** コマンドを使用します。実行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。

vpn-tunnel-protocol {**IPSec** | **l2tp-ipsec** | **svc** | **webvpn**}

no vpn-tunnel-protocol {**IPSec** | **l2tp-ipsec** | **svc** | **webvpn**}

構文の説明

IPSec	2 つのピア（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）間の IPSec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
l2tp-ipsec	L2TP 接続の IPSec トンネルをネゴシエートします。
svc	SSL VPN クライアントについて SSL VPN トンネルをネゴシエートします。
webvpn	HTTPS 対応の Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは必要ありません。

デフォルト

デフォルトは IPSec 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
グループ ポリシー コンフィギュレーション	•	—	•	—	—
ユーザ名コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**l2tp-ipsec** キーワードが追加されました。
7.3(1)	**svc** キーワー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、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザには、少なくとも 1 つのトンネリング モードを設定する必要があります。

（注） IPSec から SSL へのフォールバックをサポートするには、**vpn-tunnel-protocol** コマンドに **svc** 引数と **ipsec** 引数の両方を設定する必要があります。

例

次に、「FirstGroup」という名前のグループ ポリシーに対して WebVPN トンネリング モードと IPSec トンネリング モードを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol webvpn
hostname(config-group-policy)# vpn-tunnel-protocol IPSec
```

関連コマンド

コマンド	説明
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。

vpnclient connect

設定済みサーバへの Easy VPN Remote 接続の確立を試行するには、グローバル コンフィギュレーション モードで **vpnclient connect** コマンドを使用します。

vpnclient connect

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは ASA モデル 5505 にだけ適用されます。

例

次に、設定済み EasyVPN サーバへの Easy VPN リモート接続の確立を試行する例を示します。

```
hostname(config)# vpnclient connect
hostname(config)#
```

vpnclient disconnect

Easy VPN Remote 接続を切断するには、グローバル コンフィギュレーション モードで **vpnclient disconnect** コマンドを使用します。

vpnclient disconnect

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは ASA モデル 5505 にだけ適用されます。

例

次に、Easy VPN Remote 接続を切断する例を示します。

```
hostname(config)# vpnclient disconnect
hostname(config)#
```

vpnclient enable

Easy VPN Remote 機能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 **vpnclient enable** コマンドを使用します。Easy VPN Remote 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。

vpnclient enable

no vpnclient enable

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは、ASA 5505 にのみ適用されます。

vpnclient enable コマンドを入力すると、ASA 5505 は Easy VPN ハードウェア クライアント（「Easy VPN Remote」とも呼ばれます）として機能します。

例

次に、Easy VPN Remote 機能をイネーブルにする例を示します。

```
hostname(config)# vpnclient enable
hostname(config)#
```

次に、Easy VPN Remote 機能をディセーブルにする例を示します。

```
hostname(config)# no vpnclient enable
hostname(config)#
```

vpnclient ipsec-over-tcp

Easy VPN ハードウェア クライアントとして動作している ASA 5505 を、TCP カプセル化 IPSec を使用するように設定するには、グローバル コンフィギュレーション モードで **vpnclient ipsec-over-tcp** コマンドを使用します。実行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。

vpnclient ipsec-over-tcp [**port** *tcp_port*]

no vpnclient ipsec-over-tcp

構文の説明

port	（任意）特定のポートを使用するように指定します。
tcp_port	（**port** キーワードを指定する場合は必須）TCP カプセル化 IPSec トンネルに使用する TCP ポート番号を指定します。

デフォルト

コマンドでポート番号を指定しない場合、Easy VPN Remote 接続では、ポート 10000 が使用されます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは、Easy VPN ハードウェア クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 にのみ適用されます。

デフォルトでは、Easy VPN クライアントおよびサーバは、IPSec をユーザ データグラム プロトコル（UDP）パケットにカプセル化します。一部の環境（特定のファイアウォール ルールが設定されている環境など）または NAT デバイスや PAT デバイスでは、UDP を使用できません。そのような環境で標準の Encapsulating Security Protocol（ESP; カプセル化セキュリティ プロトコル、プロトコル 50）または Internet Key Exchange（IKE; インターネット キー交換、UDP 500）を使用するには、TCP パケット内に IPSec をカプセル化してセキュアなトンネリングをイネーブルにするようにクライアントとサーバを設定します。ただし、UDP が許可されている環境では、IPSec over TCP を設定すると不要なオーバーヘッドが発生します。

TCP カプセル化 IPSec を使用するように ASA 5505 を設定する場合は、次のコマンドを入力して、外部インターフェイスを介して大きなパケットを送信できるようにします。

```
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

このコマンドは、Don't Fragment（DF）ビットをカプセル化されたヘッダーからクリアします。DF ビットは、パケットを断片化できるかどうかを決定する IP ヘッダー内のビットです。このコマンドを使用すると、Easy VPN ハードウェア クライアントは MTU サイズよりも大きいパケットを送信できます。

例

次に、デフォルト ポート 10000 を使用して TCP カプセル化 IPSec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
hostname(config)# vpnclient ipsec-over-tcp
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

次に、ポート 10501 を使用して TCP カプセル化 IPSec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
hostname(config)# vpnclient ipsec-over-tcp port 10501
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

vpnclient mac-exempt

Easy VPN Remote 接続の背後にあるデバイスに対して個々のユーザ認証要件を免除するには、グローバル コンフィギュレーション モードで **vpnclient mac-exempt** コマンドを使用します。実行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。

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

no vpnclient mac-exempt

構文の説明

mac_addr_1	ドット付き 16 進表記の MAC アドレス。個々のユーザ認証を免除するデバイスの製造業者とシリアル番号を指定します。デバイスが複数の場合は、スペースで区切った各 MAC アドレスとそれぞれのネットワーク マスクを指定します。 MAC アドレスの最初の 6 文字はデバイスの製造業者を識別し、最後の 6 文字はシリアル番号です。最後の 24 ビットは、ユニットの 16 進形式のシリアル番号です。
mac_mask_1	対応する MAC アドレスのネットワーク マスク。スペースを使用して、ネットワーク マスク、および後続の MAC アドレスとネットワーク マスクのペアを区切ります。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは ASA モデル 5505 にだけ適用されます。

Cisco IP Phone、無線アクセス ポイント、プリンタなどのデバイスは、認証を実行できないため、個々のユニット認証がイネーブルになっている場合でも認証されません。個々のユーザ認証がイネーブルになっている場合は、このコマンドを使用してこれらのデバイスの認証を免除できます。デバイスに対する個々のユーザ認証の免除は、「デバイス パススルー」とも呼ばれます。

このコマンドでは、MAC アドレスとマスクは、3 つの 16 進数をピリオドで区切って指定します。たとえば、MAC マスク ffff.ffff.ffff は、指定した MAC アドレスとのみ一致します。すべてがゼロの MAC マスクは、いずれの MAC アドレスとも一致しません。MAC マスク ffff.ff00.0000 は、製造業者が同じであるすべてのデバイスと一致します。

例

Cisco IP Phone には、製造業者 ID として 00036b が設定されています。したがって、次のコマンドは、今後追加される可能性がある Cisco IP Phone も含めてすべての Cisco IP Phone を免除します。

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

次に、1 つの特定の Cisco IP Phone を免除する例を示します。このようにすると、セキュリティは向上しますが、柔軟性が低くなります。

```
hostname(config)# vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
hostname(config)#
```

vpnclient management

Easy VPN ハードウェア クライアントへの管理アクセス用の IPSec トンネルを生成するには、グローバル コンフィギュレーション モードで **vpnclient management** コマンドを使用します。

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

vpnclient management clear

実行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。これにより、管理専用の IPSec トンネルが **split-tunnel-policy** コマンドと **split-tunnel-network-list** コマンドに従って設定されます。

no vpnclient management

構文の説明

clear	通常のルーティングを使用して、社内ネットワークから Easy VPN クライアントとして動作している ASA 5505 の外部インターフェイスへの管理アクセスを提供します。このオプションでは、管理トンネルは作成されません。 **（注）** このオプションは、クライアントとインターネット間で NAT デバイスが動作している場合に使用します。
ip_addr	Easy VPN ハードウェア クライアントからの管理トンネルを構築するホストまたはネットワークの IP アドレス。この引数は、**tunnel** キーワードとともに使用します。スペースで区切った 1 つ以上の IP アドレスとそれぞれのネットワーク マスクを指定します。
ip_mask	対応する IP アドレスのネットワーク マスク。スペースを使用して、ネットワーク マスク、および後続の IP アドレスとネットワーク マスクのペアを区切ります。
tunnel	社内ネットワークから Easy VPN クライアントとして動作している ASA 5505 の外部インターフェイスへの管理アクセス専用 IPSec トンネルを自動的に設定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 に対してのみ適用されます。ASA 5505 のコンフィギュレーションに次のコマンドが含まれていることを前提とします。

vpnclient server：ピアを指定します。

vpnclient mode：クライアント モード（PAT）またはネットワーク拡張モードを指定します。

次のいずれかが必要です。

- **vpnclient vpngroup**：Easy VPN サーバで認証に使用するトンネル グループと IKE 事前共有キーを指定します。
- **vpnclient trustpoint**：認証に使用する RSA 証明書を識別するトラストポイントを指定します。

vpnclient enable：ASA 5505 を Easy VPN クライアントとしてイネーブルにします。

（注） NAT デバイスでスタティック NAT マッピングを追加しなければ、NAT デバイスの背後にある ASA 5505 のパブリック アドレスにはアクセスできません。

例

次に、ASA 5505 の外部インターフェイスから IP アドレスとマスクの組み合わせが 192.168.10.10 255.255.255.0 であるホストへの IPSec トンネルを生成する例を示します。

```
hostname(config)# vpnclient management tunnel 192.168.10.0 255.255.255.0
hostname(config)#
```

次に、IPSec を使用しないで ASA 5505 の外部インターフェイスへの管理アクセスを提供する例を示します。

```
hostname(config)# vpnclient management clear
hostname(config)#
```

vpnclient mode

クライアント モードまたはネットワーク拡張モードの Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient mode** コマンドを使用します。実行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。

vpnclient mode {**client-mode** | **network-extension-mode**}

no vpnclient mode

構文の説明

client-mode	クライアント モード（PAT）を使用するように Easy VPN Remote 接続を設定します。
network-extension-mode	ネットワーク拡張モード（NEM）を使用するように Easy VPN Remote 接続を設定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 に対してのみ適用されます。Easy VPN クライアントは、クライアント モードまたは NEM のいずれかの動作モードをサポートします。動作モードによって、企業ネットワークからトンネル経由で内部ホスト（Easy VPN クライアントから見た場合の内部ホスト）に接続できるかどうかが決まります。Easy VPN クライアントにはデフォルト モードがないため、接続前に動作モードを指定する必要があります。

- クライアント モードでは、Easy VPN クライアントは、内部ホストからのすべての VPN トラフィックに対してポート アドレス変換（PAT）を実行します。このモードでは、ハードウェア クライアント（デフォルトの RFC 1918 アドレスが割り当てられています）の内部アドレスまたは内部ホストに対する IP アドレス管理は必要ありません。PAT により、企業ネットワークから内部ホストにはアクセスできません。

- NEM では、内部ネットワーク上のすべてのノードおよび内部インターフェイスに企業ネットワークでルーティング可能なアドレスが割り当てられます。内部ホストには、企業ネットワークからトンネル経由でアクセスできます。内部ネットワーク上のホストには、アクセス可能なサブネットから IP アドレスが（スタティックに、または DHCP によって）割り当てられます。ネットワーク拡張モードの場合、PAT は VPN トラフィックに適用されません。

（注）　Easy VPN ハードウェア クライアントが NEM を使用し、セカンダリ サーバに接続している場合は、各ヘッドエンド デバイスで **crypto map set reverse-route** コマンドを使用して、Reverse Route Injection（RRI; 逆ルート注入）によるリモート ネットワークのダイナミック通知を設定します。

例

次に、クライアント モードの Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# vpnclient mode client-mode
hostname(config)#
```

次に、NEM の Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# vpnclient mode network-extension-mode
hostname(config)#
```

vpnclient nem-st-autoconnect

NEM およびスプリット トンネリングが設定されている場合に、IPSec データ トンネルを自動的に開始するように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient nem-st-autoconnect** コマンドを使用します。実行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。

vpnclient nem-st-autoconnect

no vpnclient nem-st-autoconnect

構文の説明

このコマンドにはキーワードまたは引数はありません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 に対してのみ適用されます。

vpnclient nem-st-autoconnect コマンドを入力する前に、ハードウェア クライアントのネットワーク拡張モードがイネーブルになっていることを確認します。ネットワーク拡張モードを使用すると、ハードウェア クライアントは、単一のルーティング可能なネットワークを VPN トンネルを介してリモート プライベート ネットワークに提供できます。IPSec は、ハードウェア クライアントの背後にあるプライベート ネットワークからセキュリティ アプライアンスの背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、セキュリティ アプライアンスの背後にあるデバイスは、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。ハードウェア クライアントがトンネルを開始する必要があります。トンネルのアップ後、いずれの側からでもデータ交換を開始できます。

（注） ネットワーク拡張モードをイネーブルにするように Easy VPN サーバを設定する必要もあります。そのためには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。

ネットワーク拡張モードでは、スプリット トンネリングが設定されている場合を除き、IPSec データ トンネルが自動的に開始し、保持されます。

例

次に、スプリット トンネリングが設定されたネットワーク拡張モードで自動的に接続するように Easy VPN Remote 接続を設定する例を示します。グループ ポリシー FirstGroup のネットワーク拡張モードがイネーブルになっています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
hostname(config)# vpnclient nem-st-autoconnect
hostname(config)#
```

関連コマンド

コマンド	説明
nem	ハードウェア クライアントのネットワーク拡張モードをイネーブルにします。

vpnclient server-certificate

証明書マップによって指定された特定の証明書を持つ Easy VPN サーバへの接続のみを受け入れるように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient server-certificate** コマンドを使用します。実行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。

vpnclient server-certificate *certmap_name*

no vpnclient server-certificate

構文の説明

certmap_name	受け入れ可能な Easy VPN サーバ証明書を指定する証明書マップの名前を指定します。最大長は、64 文字です。

デフォルト

Easy VPN サーバ証明書のフィルタリングは、デフォルトではディセーブルです。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは ASA モデル 5505 にだけ適用されます。

このコマンドを使用して、Easy VPN サーバ証明書のフィルタリングをイネーブルにします。証明書マップ自体は、crypto ca certificate map コマンドと crypto ca certificate chain コマンドを使用して定義します。

例

次に、homeservers という名前の証明書マップを持つ Easy VPN サーバへの接続のみをサポートするように Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# vpnclient server-certificate homeservers
hostname(config)#
```

関連コマンド

コマンド	説明
certificate	指定された証明書を追加します。
vpnclient trustpoint	Easy VPN Remote 接続で使用する RSA アイデンティティ証明書を設定します。

vpnclient server

Easy VPN Remote 接続用のプライマリおよびセカンダリ IPSec サーバを設定するには、グローバル コンフィギュレーション モードで **vpnclient server** コマンドを使用します。実行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。

vpnclient server *ip_primary_address* [*ip_secondary_address_1 ... ipsecondary_address_10*]

no vpnclient server

構文の説明

ip_primary_address	プライマリ Easy VPN（IPSec）サーバの IP アドレスまたは DNS 名。ASA または VPN 3000 コンセントレータ シリーズは、Easy VPN サーバとして機能できます。
ip_secondary_address_n	（任意）最大 10 台のバックアップ Easy VPN サーバの IP アドレスまたは DNS 名のリスト。スペースを使用して、リスト内の項目を区切ります。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは ASA モデル 5505 にだけ適用されます。

接続を確立する前にサーバを設定する必要があります。**vpnclient server** コマンドでは、IPv4 アドレス、名前データベース、または DNS 名がサポートされ、アドレスはその順に解決されます。

サーバの IP アドレスまたはホスト名を使用できます。

例

次に、名前 headend-1 をアドレス 10.10.10.10 に関連付け、**vpnclient server** コマンドを使用して 3 台のサーバ（headend-dns.domain.com（プライマリ）、headend-1（セカンダリ）、および 192.168.10.10（セカンダリ））を指定する例を示します。

```
hostname(config)# names
hostname(config)# 10.10.10.10 headend-1
hostname(config)# vpnclient server headend-dns.domain.com headend-1 192.168.10.10
hostname(config)#
```

次に、VPN クライアントに IP アドレスが 10.10.10.15 のプライマリ IPSec サーバおよび IP アドレスが 10.10.10.30 と 192.168.10.45 のセカンダリ サーバを設定する例を示します。

```
hostname(config)# vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
hostname(config)#
```

vpnclient trustpoint

Easy VPN Remote 接続で使用する RSA アイデンティティ証明書を設定するには、グローバル コンフィギュレーション モードで **vpnclient trustpoint** コマンドを使用します。実行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。

vpnclient trustpoint *trustpoint_name* [**chain**]

no vpnclient trustpoint

構文の説明

chain	証明書チェーン全体を送信します。
trustpoint_name	認証に使用する RSA 証明書を識別するトラストポイントの名前を指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは、ASA モデル 5505 にのみ適用され、また、デジタル証明書を使用する場合にのみ適用されます。

crypto ca trustpoint コマンドを使用してトラストポイントを定義します。トラストポイントは、CA が発行する証明書に基づいた CA のアイデンティティとデバイスのアイデンティティを表します。トラストポイント サブモード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。これらのパラメータでは、セキュリティ アプライアンスが CA 証明書を取得する方法、セキュリティ アプライアンスが CA から証明書を取得する方法、および CA が発行するユーザ証明書の認証ポリシーを指定します。

例

次に、central という名前の特定のアイデンティティ証明書を使用し、証明書チェーン全体を送信するように Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config)# vpnclient trustpoint central chain
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードを開始し、トラストポイント情報を管理します。

vpnclient username

Easy VPN Remote 接続の VPN ユーザ名とパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient username** コマンドを使用します。実行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。

vpnclient username *xauth_username* **password** *xauth password*

no vpnclient username

構文の説明

xauth_password	XAUTH に使用するパスワードを指定します。最大長は、64 文字です。
xauth_username	XAUTH に使用するユーザ名を指定します。最大長は、64 文字です。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは ASA モデル 5505 にだけ適用されます。

XAUTH ユーザ名とパスワードのパラメータは、セキュア ユニット認証がディセーブルで、サーバが XAUTH クレデンシャルを要求する場合に使用します。セキュア ユニット認証がイネーブルの場合、これらのパラメータは無視され、セキュリティ アプライアンスによって、ユーザにユーザ名とパスワードの入力を求めるプロンプトが表示されます。

例

次に、XAUTH ユーザ名 testuser とパスワード ppurkm1 を使用するように Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# vpnclient username testuser password ppurkm1
hostname(config)#
```

vpnclient vpngroup

Easy VPN Remote 接続の VPN トンネル グループ名とパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient vpngroup** コマンドを使用します。実行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。

vpnclient vpngroup *group_name* **password** *preshared_key*

no vpnclient vpngroup

構文の説明

group_name	Easy VPN サーバで設定された VPN トンネル グループの名前を指定します。最大の長さは 64 文字で、スペースは使用できません。
preshared_key	Easy VPN サーバで認証に使用する IKE 事前共有キー。最大長は 128 文字です。

デフォルト

Easy VPN クライアントとして動作している ASA 5505 のコンフィギュレーションでトンネル グループが指定されていない場合、クライアントは RSA 証明書を使用しようとします。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 に対してのみ適用されます。

事前共有キーをパスワードとして使用します。接続の確立前にサーバを設定する必要があります。

例

次に、グループ名が TestGroup1、パスワードが my_key123 の VPN トンネル グループを Easy VPN Remote 接続に設定する例を示します。

```
hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
hostname(config)#
```

関連コマンド

コマンド	説明
vpnclient trustpoint	Easy VPN 接続で使用する RSA アイデンティティ証明書を設定します。

wccp

容量を割り当て、サービス グループに参加できるように、指定した Web Cache Communication Protocol（WCCP）サービスのサポート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 **wccp** コマンドを使用します。サービス グループをディセーブルにし、容量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。

wccp {**web-cache** | *service-number*} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** password]

no wccp {**web-cache** | *service-number*} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** password [**0** | **7**]]

構文の説明

web-cache	Web キャッシュ サービスを指定します。 **（注）** Web キャッシュは、1 つのサービスとしてカウントされます。サービスの最大数（service-number 引数で割り当てられたサービスを含む）は 256 です。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 で、255 個まで使用できます。**web-cache** キーワードで指定される Web キャッシュ サービスを含めると、許可される最大数は 256 個です。
redirect-list	（任意）このデバイス グループにリダイレクトされたトラフィックを制御するアクセス リストとともに使用します。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。アクセス リストには、ネットワーク アドレスだけを含める必要があります。ポート固有のエントリはサポートされていません。
access-list	アクセス リストの名前を指定します。
group-list	（任意）サービス グループへの参加を許可する Web キャッシュを決定するアクセス リスト。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。
password	（任意）サービス グループから受信したメッセージに対して Message Digest 5（MD5）認証を指定します。認証で受け入れられなかったメッセージは廃棄されます。
password	認証で使用するパスワードを指定します。password 引数の長さは最大 7 文字です。

デフォルト

このコマンドは、デフォルトでディセ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		
				マルチ	
	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例　次に、サービス グループに参加できるように WCCP をイネーブルにする例を示します。

```
hostname(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

wccp redirect

Web Cache Communication Protocol（WCCP）を使用したインターフェイスの入口でのパケット リダイレクションをイネーブルにするには、**wccp redirect** コマンドを使用します。WCCP リダイレクション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。

wccp interface *interface_name service* **redirect in**

no wccp interface *interface_name service* **redirect in**

構文の説明

interface_name	パケットをリダイレクトするインターフェイスの名前。
service	サービス グループを指定します。**web-cache** キーワードを指定するか、サービスの識別番号（0 ～ 99）を指定できます。
in	パケットがこのインターフェイスに着信するときにリダイレクションを実行するように指定します。

デフォルト

このコマンドは、デフォルトでディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、Web キャッシュ サービスの内部インターフェイスでの WCCP リダイレクションをイネーブルにする例を示します。

```
hostname(config)# wccp interface inside web-cache redirect in
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp	サービス グループを使用して、WCCP のサポートをイネーブルにします。

web-agent-url

セキュリティ アプライアンスが SiteMinder-type SSO 認証を要求する SSO サーバの URL を指定するには、config-webvpn-sso-siteminder モードで **web-agent-url** コマンドを使用します。

SSO サーバの認証 URL を削除するには、このコマンドの **no** 形式を使用します。

web-agent-url *url*

no web-agent-url *url*

（注） このコマンドは、SiteMinder-type SSO 認証に必要です。

構文の説明

url	SiteMinder-type SSO サーバの認証 URL を指定します。http:// または https:// を含める必要があります。

デフォルト

デフォルトでは、認証 URL は設定されません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
config-webvpn-sso-siteminder	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、さまざまなサーバで各種のセキュアなサービスにアクセスできます。SSO サーバには、認証要求を処理する URL があります。

このコマンドは、SiteMinder-type の SSO サーバにのみ適用されます。

この URL に認証を送信するようにセキュリティ アプライアンスを設定するには、**web-agent-url** コマンドを使用します。認証 URL を設定する前に、**sso-server** コマンドを使用して SSO サーバを作成する必要があります。

セキュリティ アプライアンスと SSO サーバ間で https 通信を行うには、SSL 暗号化設定が両側で一致することを確認します。セキュリティ アプライアンスでは、これを **ssl encryption** コマンドで確認します。

例

次に、config-webvpn-sso-siteminder モードで認証 URL として http://www.example.com/webvpn を指定する例を示します。

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder-type SSO サーバへの認証要求の暗号化に使用される秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
ssl encryption	SSL/TLS プロトコルで使用される暗号化アルゴリズムを指定します。
sso-server	シングル サインオン サーバを作成します。

web-applications

認証された WebVPN ユーザに表示される WebVPN ホームページの [Web Application] ボックスをカスタマイズするには、webvpn カスタマイゼーション モードで **web-applications** コマンドを使用します。

web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

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。

構文の説明

title	タイトルを変更することを指定します。
message	タイトルの下に表示されるメッセージを変更することを指定します。
dropdown	ドロップダウン ボックスを変更することを指定します。
text	テキストを変更することを指定します。
style	HTML スタイルを変更することを指定します。
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）です。

デフォルト

デフォルトのタイトルのテキストは「Web Application」です。

デフォルトのタイトルのスタイルは background-color:#99CCCC;color:black;font-weight:bold;text-transform uppercase です。uppercase です。

デフォルトのメッセージのテキストは「Enter Web Address (URL)」です。

デフォルトのメッセージのスタイルは background-color:#99CCCC;color:maroon;font-size:smaller です。

デフォルトのドロップダウンのテキストは「Web Bookmarks」です。

デフォルトのドロップダウンのスタイルは border:1px solid black;font-weight:bold;color:black;font-size:80% 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

style オプションは有効な Cascading Style Sheet（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 Consortium（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。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するための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、タイトルを「Applications」に変更し、テキストの色を青に変更する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-applications title text Applications
F1-asa1(config-webvpn-custom)# web-applications title style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックス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。
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-bookmarks

認証された WebVPN ユーザに表示される 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するには、webvpn カスタマイゼーション モードで **web-bookmarks** コマンドを使用します。

web-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

[**no**] **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

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。

構文の説明

link	リンクを変更することを指定します。
title	タイトルを変更することを指定します。
style	HTML スタイルを変更することを指定します。
text	テキストを変更することを指定します。
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）です。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトルのテキストは「Web Bookmarks」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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

style オプションは有効な Cascading Style Sheet（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 Consortium（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。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するための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、[Web Bookmarks] のタイトルを「Corporate Web Bookmarks」にカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックス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] ボックスをカスタマイズします。

webvpn

webvpn モードを開始するには、グローバル コンフィギュレーション モードで **webvpn** コマンドを入力します。このコマンドで入力したコマンドを削除するには、**no webvpn** コマンドを使用します。これらの webvpn コマンドは、すべての WebVPN ユーザに適用されます。

これらの webvpn コマンドを使用して、AAA サーバ、デフォルト グループ ポリシー、デフォルト アイドル タイムアウト、http プロキシと https プロキシ、WebVPN 用の NBNS サーバ、およびエンドユーザに表示される WebVPN 画面の外観を設定できます。

webvpn

no webvpn

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。

デフォルト

WebVPN は、デフォルトではディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

この WebVPN モードでは、WebVPN のグローバル設定を指定できます。グローバル ポリシー モードまたはユーザ名モードから WebVPN モードを開始した場合は、特定のユーザまたはグループ ポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

例

次に、WebVPN コマンド モードを開始する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)#
```

webvpn（グループ ポリシーおよびユーザ名モード）

この webvpn モードを開始するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用します。webvpn モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。これらの webvpn コマンドは、設定元のユーザ名またはグループ ポリシーに適用されます。

グループ ポリシーおよびユーザ名に対する webvpn コマンドでは、ファイルへのアクセス、MAPI プロキシ、URL、および WebVPN を介した TCP アプリケーションを定義できます。ACL およびフィルタリングするトラフィックのタイプも指定します。

webvpn

no webvpn

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。

デフォルト

WebVPN は、デフォルトではディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

グローバル コンフィギュレーション モードから webvpn モードを開始した場合は、WebVPN のグローバル設定を指定できます。グループ ポリシー属性コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **webvpn** コマンドを使用すると、webvpn コマンドで指定された設定が親コマンドで指定されたグループまたはユーザに適用されます。つまり、ここで説明したグローバル ポリシー モードまたはユーザ名モードから開始した webvpn モードでは、特定のユーザまたはグループ ポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

グループ ポリシー属性モードで特定のグループ ポリシーに対して適用した WebVPN 属性は、デフォルト グループ ポリシーで指定された WebVPN 属性を上書きします。ユーザ名属性モードで特定のユーザに対して適用した WebVPN 属性は、デフォルト グループ ポリシー内およびそのユーザが属しているグループ ポリシー内の WebVPN 属性を上書きします。基本的に、これらのコマンドを使用すると、デフォルト グループまたは指定したグループ ポリシーから継承される設定を調整できます。WebVPN 設定の詳細については、グローバル コンフィギュレーション モードの **webvpn** コマンドに関する説明を参照してください。

次の表に、webvpn グループ ポリシー属性モードおよびユーザ名属性モードで設定できる属性を示します。詳細については、個々のコマンドの説明を参照してください。

属性	説明
auto-signon	WebVPN ユーザのログイン クレデンシャルを内部サーバに自動的に渡すようにセキュリティ アプライアンスを設定して、WebVPN ユーザにシングル サインオン方式を提供します。
customization	適用する設定済み WebVPN カスタマイゼーションを指定します。
deny-message	アクセスが拒否されたときにユーザに表示されるメッセージを指定します。
filter	WebVPN 接続に使用するアクセス リストを指定します。
functions	ファイル アクセスとファイル ブラウジング、MAPI プロキシ、および WebVPN を介した URL エントリを設定します。
homepage	WebVPN ユーザがログインしたときに表示される Web ページの URL を設定します。
html-content-filter	WebVPN セッションでフィルタリングする Java、ActiveX、イメージ、スクリプト、およびクッキーを指定します。
http-comp	使用する HTTP 圧縮アルゴリズムを指定します。
keep-alive-ignore	セッションの更新で無視する最大オブジェクト サイズを指定します。
port-forward	WebVPN アプリケーション アクセスをイネーブルにします。
port-forward-name	エンド ユーザに対する TCP ポート フォワーディングを識別する表示名を設定します。
sso-server	SSO サーバ名を設定します。
svc	SSL VPN クライアント属性を設定します。
url-list	ユーザが WebVPN 経由でアクセスできるサーバと URL のリストを指定します。

例

次に、「FirstGroup」という名前のグループ ポリシーの webvpn モードを開始する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-webvpn)#
```

次に、「test」というユーザ名の webvpn モードを開始する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-username)# webvpn
hostname(config-webvpn)#
```

関連コマンド

clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy attributes	設定グループ ポリシー モードを開始します。このモードでは、指定したグループ ポリシーへの属性と値の設定、または webvpn モードでのグループの webvpn 属性の設定ができます。

show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

who

セキュリティ アプライアンス上のアクティブな Telnet 管理セッションを表示するには、特権 EXEC モードで **who** コマンドを使用します。

who [*local_ip*]

構文の説明

local_ip	（任意）リストを 1 つの内部 IP アドレスまたはネットワーク アドレス（IPv4 または IPv6）に制限することを指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

who コマンドを使用すると、現在セキュリティ アプライアンスにログインしている各 Telnet クライアントの TTY_ID と IP アドレスを表示できます。

例

次に、クライアントが Telnet セッションを使用してセキュリティ アプライアンスにログインしている場合の **who** コマンドの出力例を示します。

```
hostname# who
0: 100.0.0.2
hostname# who 100.0.0.2
0: 100.0.0.2
hostname#
```

関連コマンド

コマンド	説明
kill	Telnet セッションを終了します。
telnet	セキュリティ アプライアンス コンソールへの Telnet アクセスを追加して、アイドル タイムアウトを設定します。

window-variation

さまざまなウィンドウ サイズの接続をドロップするには、tcp マップ コンフィギュレーション モードで **window-variation** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

構文の説明

allow-connection	接続を許可します。
drop-connection	接続をドロップします。

デフォルト

デフォルト アクションは、接続の許可です。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(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

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **window-variation** コマンドを使用して、ウィンドウ サイズが縮小されたすべての接続をドロップします。

ウィンドウ サイズ メカニズムによって、TCP は大きなウィンドウをアドバタイズでき、続いて、過剰な量のデータを受け入れずに、はるかに小さなウィンドウをアドバタイズできます。TCP 仕様により、「ウィンドウの縮小」は極力避けることが推奨されています。この条件が検出された場合に、接続をドロップできます。

例

次に、さまざまなウィンドウ サイズの接続をすべてドロップする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# window-variation drop-connection
```

```
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

wins-server

プライマリおよびセカンダリ WINS サーバの IP アドレスを設定するには、グループ ポリシー コンフィギュレーション モードで **wins-server** コマンドを使用します。実行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。このオプションを使用すると、他のグループ ポリシーから WINS サーバを継承できます。サーバが継承されないようにするには、**wins-server none** コマンドを使用します。

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

構文の説明

none	WINS サーバをヌル値に設定して、WINS サーバを許可しないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ WINS サーバの IP アドレスを指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

wins-server コマンドを発行するたびに、既存の設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定してから WINS サーバ y.y.y.y を設定すると、2 番めのコマンドによって最初の設定が上書きされ、y.y.y.y が唯一の WINS サーバになります。複数のサーバを設定する場合も同様です。設定済みのサーバを上書きするのではなく、WINS サーバを追加するには、このコマンドを入力するときに、すべての WINS サーバの IP アドレスを含めます。

例

次に、FirstGroup という名前のグループ ポリシーに IP アドレスが 10.10.10.15、10.10.10.30、および 10.10.10.45 の WINS サーバを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

write erase

スタートアップ コンフィギュレーションを消去するには、特権 EXEC モードで **write erase** コマンドを使用します。実行コンフィギュレーションはそのまま残ります。

write erase

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、セキュリティ コンテキスト内ではサポートされません。コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定します。コンテキスト コンフィギュレーションを削除する場合は、ファイルをリモート サーバ（指定されている場合）から手動で削除するか、またはシステム実行スペースで **delete** コマンドを使用してファイルをフラッシュ メモリからクリアできます。

例

次に、スタートアップ コンフィギュレーションを消去する例を示します。

```
hostname# write erase
Erase configuration in flash memory? [confirm] y
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
delete	フラッシュ メモリからファイルを削除します。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

write memory

実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するには、特権 EXEC モードで **write memory** コマンドを使用します。

write memory [**all** [**/noconfirm**]]

構文の説明

/noconfirm	**all** キーワードを使用するときに、確認プロンプトを表示しません。
all	マルチ コンテキスト モードのシステム実行スペースでこのキーワードを使用すると、すべてのコンテキスト コンフィギュレーションおよびシステム コンフィギュレーションが保存されます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	**all** キーワードを使用して、すべてのコンテキスト コンフィギュレーションを保存できるようになりました。

使用上のガイドライン

実行コンフィギュレーションとは、コマンドラインで行ったすべての変更内容を含む、メモリ内にある現在実行中のコンフィギュレーションです。変更内容は、起動時に実行メモリにロードされるスタートアップ コンフィギュレーションに保存した場合、次のリブートまでの間のみ保持されます。シングル コンテキスト モードまたはマルチ コンテキスト モードにおけるシステムのスタートアップ コンフィギュレーションの場所は、**boot config** コマンドを使用して、デフォルトの場所（隠しファイル）から選択した場所に変更できます。マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定された場所にあります。

マルチ コンテキスト モードでは、各コンテキストで **write memory** コマンドを入力して、現在のコンテキスト コンフィギュレーションを保存できます。すべてのコンテキスト コンフィギュレーションを保存するには、システム実行スペースで **write memory all** コマンドを入力します。コンテキストのスタートアップ コンフィギュレーションは、外部サーバに配置できます。この場合、セキュリティ アプライアンスは、コンフィギュレーションをサーバに戻して保存できない HTTP および HTTPS の URL を除き、**config-url** コマンドで指定されたサーバにコンフィギュレーションを戻して保存します。セキュリティ アプライアンスが **write memory all** コマンドを使用して各コンテキストを保存した後、次のメッセージが表示されます。

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

エラーのためにコンテキストが保存されない場合もあります。エラーについては、次の情報を参照してください。

- メモリ不足のためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- リモートの宛先に到達できないためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- コンテキストがロックされているために保存されない場合は、次のメッセージが表示されます。

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context ‘a’ , context ‘x’ , context ‘z’ .
  ```

  コンテキストがロックされるのは、別のユーザがすでにコンフィギュレーションを保存している場合、またはコンテキストを削除している場合のみです。

- スタートアップ コンフィギュレーションが読み取り専用であるために（たとえば、HTTP サーバで）コンテキストが保存されない場合は、他のすべてのメッセージの最後に次のメッセージ レポートが出力されます。

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context ‘a’ , context ‘b’ , context ‘c’ .
  ```

- フラッシュ メモリに不良セクターがあるためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

システムでは、コンテキストのスタートアップ コンフィギュレーションにアクセスするために管理コンテキスト インターフェイスが使用されるため、**write memory** コマンドでも管理コンテキスト インターフェイスを使用します。ただし、**write net** コマンドでは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。

write memory コマンドは、**copy running-config startup-config** コマンドと同じです。

例

次に、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存する例を示します。

```
hostname# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
hostname#
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
config-url	コンテキスト コンフィギュレーションの場所を指定します。

コマンド	説明
copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

write net

実行コンフィギュレーションを TFTP サーバに保存するには、特権 EXEC モードで **write net** コマンドを使用します。

write net [*server***:**[*filename*] | **:***filename*]

構文の説明

:*filename*	パスとファイル名を指定します。**tftp-server** コマンドを使用してすでにファイル名を設定してある場合、この引数はオプションです。 ファイル名をこのコマンドと **tftp-server** コマンドで指定した場合、セキュリティ アプライアンスは **tftp-server** コマンドのファイル名をディレクトリとして処理し、**write net** コマンドのファイル名をそのディレクトリの下にファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ（//）が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。TFTP サーバでこのタイプの URL がサポートされていない場合は、代わりに **copy running-config tftp** コマンドを使用します。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合は、コロン（:）の後にファイル名だけを入力できます。
*server***:**	TFTP サーバの IP アドレスまたは名前を設定します。**tftp-server** コマンドで設定したアドレスがあっても、このアドレスが優先されます。 デフォルトのゲートウェイ インターフェイスは最もセキュリティが高いインターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

実行コンフィギュレーションとは、コマンドラインで行ったすべての変更内容を含む、メモリ内にある現在実行中のコンフィギュレーションです。

マルチ コンテキスト モードの場合、このコマンドは現在のコンフィギュレーションを保存します。1 つのコマンドですべてのコンテキストを保存することはできません。このコマンドを、システムおよび各コンテキストに対して個別に入力する必要があります。**write net** コマンドでは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。ただし、**write memory** コマンドでは、管理コンテキスト インターフェイスを使用してスタートアップ コンフィギュレーションに保存します。これは、システムで、コンテキストのスタートアップ コンフィギュレーションにアクセスするために管理コンテキスト インターフェイスが使用されるからです。

write net コマンドは、**copy running-config tftp** コマンドと同じです。

例

次に、**tftp-server** コマンドで TFTP サーバおよびファイル名を設定する例を示します。

```
hostname# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
hostname# write net
```

次に、**write net** コマンドにサーバとファイル名を設定する例を示します。**tftp-server** コマンドは入力されていません。

```
hostname# write net 10.1.1.1:/configs/contextbackup.cfg
```

次に、**write net** コマンドにサーバとファイル名を設定する例を示します。**tftp-server** コマンドでディレクトリ名が設定され、サーバ アドレスは上書きされます。

```
hostname# tftp-server 10.1.1.1 configs
hostname# write net 10.1.2.1:context.cfg
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
copy running-config tftp	実行コンフィギュレーションを TFTP サーバにコピーします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

write standby

フェールオーバー スタンバイ装置にセキュリティ アプライアンスまたはコンテキストの実行コンフィギュレーションをコピーするには、特権 EXEC モードで **write standby** コマンドを使用します。

write standby

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、コンフィギュレーションのスタンバイ ユニットまたはスタンバイ フェールオーバー グループと、アクティブなユニットまたはフェールオーバー グループのコンフィギュレーションとの同期が失われた場合にのみ、使用します。通常、この状態は、コマンドがスタンバイ ユニットまたはスタンバイ フェールオーバー グループで入力された場合に発生します。

Active/Standby フェールオーバーの場合、**write standby** コマンドはアクティブなフェールオーバー ユニットの RAM に保存されているコンフィギュレーションをスタンバイ ユニットの RAM に書き込みます。プライマリ ユニットとセカンダリ ユニットのコンフィギュレーションに含まれている情報が異なる場合に、**write standby** コマンドを使用します。このコマンドは、アクティブなユニットで入力します。

アクティブ/アクティブ フェールオーバーの場合、**write standby** コマンドは次のように動作します。

- システム実行スペースで **write standby** コマンドを入力した場合は、セキュリティ アプライアンス上のシステム コンフィギュレーションおよびすべてのセキュリティ コンテキストのコンフィギュレーションがピア ユニットに書き込まれます。これには、スタンバイ状態のセキュリティ コンテキストのコンフィギュレーション情報が含まれています。このコマンドの入力は、フェールオーバー グループ 1 がアクティブ状態の装置上のシステム実行スペースで行う必要があります。
- セキュリティ コンテキストで **write standby** コマンドを入力すると、セキュリティ コンテキストのコンフィギュレーションだけがピア装置に書き込まれます。このコマンドの入力は、セキュリティ コンテキストがアクティブ状態で表示される装置のセキュリティ コンテキストで行う必要があります。

（注）　**write standby** コマンドは、コンフィギュレーションをピア ユニットの実行コンフィギュレーションに複製します。コンフィギュレーションは、スタートアップ コンフィギュレーションに保存されません。コンフィギュレーションの変更をスタートアップ コンフィギュレーションに保存するには、**write standby** コマンドを入力したユニットで **copy running-config startup-config** コマンドを使用します。コマンドはピア ユニットに複製され、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されます。

ステートフル フェールオーバーがイネーブルの場合、**write standby** コマンドは、コンフィギュレーションのレプリケーションが完了した後、状態情報もスタンバイ ユニットに複製します。

例

次に、現在の実行コンフィギュレーションをスタンバイ ユニットに書き込む例を示します。

```
hostname# write standby
Building configuration...
[OK]
hostname#
```

関連コマンド

コマンド	説明
failover reload-standby	スタンバイ ユニットを強制的にリブートします。

write terminal

端末で実行コンフィギュレーションを表示するには、特権 EXEC モードで **write terminal** コマンドを使用します。

write terminal

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、**show running-config** コマンドと同じです。

例

次に、実行コンフィギュレーションを端末に書き込む例を示します。

```
hostname# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

zonelabs-integrity fail-close

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの間の接続で障害が発生したときに VPN クライアントへの接続が閉じるようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-close** コマンドを使用します。Zone Labs 接続で障害が発生しても VPN 接続を開いたままにするデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity fail-close

no zonelabs-integrity fail-close

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。

デフォルト

デフォルトでは、接続は障害が発生しても開いたままです。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバがセキュリティ アプライアンスに応答しない場合も、セキュリティ アプライアンスはプライベート ネットワークとの VPN クライアントの接続を確立します。既存の開いている接続も維持されます。これにより、企業 VPN はファイアウォール サーバで障害が発生しても中断されません。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態に維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。

Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生してもセキュリティ アプライアンスによってクライアント VPN 接続が維持されるデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドを使用します。

例

次に、Zone Labs Integrity ファイアウォール サーバが応答しない場合、または接続が中断された場合に、VPN クライアント接続を閉じるようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# zonelabs-integrity fail-close
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、セキュリティ アプライアンスへの VPN クライアント接続を開いたままにするように指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスが到達不能と見なすまでの秒数を指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。

zonelabs-integrity fail-open

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの間の接続で障害が発生した後も、セキュリティ アプライアンスへのリモート VPN クライアント接続を開いたままにするには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-open** コマンドを使用します。Zone Labs サーバ接続で障害が発生した場合に VPN クライアントへの接続を閉じるには、このコマンドの **no** 形式を使用します。

zonelabs-integrity fail-open

no zonelabs-integrity fail-open

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。

デフォルト

デフォルトでは、セキュリティ アプライアンスで Zone Labs Integrity ファイアウォール サーバへの接続が確立または維持されない場合、リモート VPN 接続は開いたままになります。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバがセキュリティ アプライアンスに応答しない場合も、セキュリティ アプライアンスはプライベート ネットワークとの VPN クライアントの接続を確立します。既存の開いている接続も維持されます。これにより、企業 VPN はファイアウォール サーバで障害が発生しても中断されません。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態に維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生してもセキュリティ アプライアンスによってクライアント VPN 接続が維持されるデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドまたは **no zonelabs-integrity fail-open** コマンドを使用します。

例

次に、Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生しても VPN クライアント接続を開いたままにするデフォルト状態に戻す例を示します。

```
hostname(config)# zonelabs-integrity fail-open
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、セキュリティ アプライアンスが VPN クライアント接続を閉じるように指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスが到達不能と見なすまでの秒数を指定します。

zonelabs-integrity fail-timeout

セキュリティ アプライアンスにおいて、何秒経過すると応答のない Zone Labs Integrity ファイアウォール サーバを到達不能であると見なすかを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-timeout** コマンドを使用します。デフォルトのタイムアウト（10 秒）に戻すには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

構文の説明

timeout	セキュリティ アプライアンスにおいて、応答のない Zone Labs Integrity ファイアウォール サーバを到達不能であると見なすまでの秒数。設定可能な値の範囲は、5 ～ 20 秒です。

デフォルト

デフォルトのタイムアウト値は 10 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

セキュリティ アプライアンスが指定された秒数待機しても Zone Labs サーバから応答がない場合、サーバは応答不能と見なされます。VPN クライアントへの接続は、デフォルトまたは **zonelabs-integrity fail-open** コマンドの設定に従って開いたままになります。ただし、**zonelabs-integrity fail-close** コマンドが発行されている場合は、セキュリティ アプライアンスで Integrity サーバが応答不能と見なされると接続は閉じます。

例

次に、12 秒経過後にアクティブな Zone Labs Intergity サーバを到達不能と見なすようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# zonelabs-integrity fail-timeout 12
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、セキュリティ アプライアンスへの VPN クライアント接続を開いたままにするように指定します。
zonelabs-integrity fail-close	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、セキュリティ アプライアンスが VPN クライアント接続を閉じるように指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。

zonelabs-integrity interface

Zone Labs Integrity サーバとの通信で使用するセキュリティ アプライアンス インターフェイスを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity interface** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバのインターフェイスをデフォルト（none）にリセットするには、このコマンドの **no** 形式を使用します。

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

構文の説明

interface	Zone Labs Integrity ファイアウォール サーバが通信するセキュリティ アプライアンス インターフェイスを指定します。これは、多くの場合、**nameif** コマンドで作成されたインターフェイス名です。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール インターフェイスは none 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、IP アドレス範囲 10.0.0.5 ～ 10.0.0.7 を使用して 3 台の Zone Labs Intergity サーバを設定する例を示します。また、これらのコマンドでは、ポート 300 および inside というインターフェイスでサーバをリッスンするようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
hostname(config)# zonelabs-integrity port 300
hostname(config)# zonelabs-integrity interface inside
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。

コマンド	説明
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity port

Zone Labs Integrity ファイアウォール サーバとの通信で使用するセキュリティ アプライアンス上のポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity port** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバのデフォルト ポート 5054 に戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity port *port_number*

no zonelabs-integrity port *port_number*

構文の説明

port	セキュリティ アプライアンス上の Zone Labs Integrity ファイアウォール サーバのポートを指定します。
port_number	Zone Labs Integrity ファイアウォール サーバのポートの番号。指定できる範囲は、10 ～ 10000 です。

デフォルト

Zone Labs Integrity ファイアウォール サーバのデフォルト ポートは 5054 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

セキュリティ アプライアンスは、**zonelabs-integrity port** コマンドと **zonelabs-integrity interface** コマンドでそれぞれ設定されたポートとインターフェイスで Zone Labs Integrity ファイアウォール サーバをリッスンします。

（注） 現在のリリースのセキュリティ アプライアンスでは同時に 1 台の Integrity サーバのみがサポートされていますが、ユーザ インターフェイスでは最大 5 台の Integrity サーバの設定がサポートされています。アクティブなサーバに障害が発生した場合は、セキュリティ アプライアンス上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

例

次に、IP アドレス 10.0.0.5 を使用して Zone Labs Integrity サーバを設定する例を示します。また、これらのコマンドでは、デフォルト ポート 5054 ではなくポート 300 でアクティブな Zone Labs サーバをリッスンするようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5
```

```
hostname(config)# zonelabs-integrity port 300
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity server-address

Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンス コンフィギュレーションに追加するには、グローバル コンフィギュレーション モードで **zonelabs-integrity server-address** コマンドを使用します。Zone Labs サーバを IP アドレスまたはホスト名で指定します。

Zone Labs Integrity ファイアウォール サーバ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** 形式を引数なしで使用します。

zonelabs-integrity server-address {*hostname1* | *ip-address1*}

no zonelabs-integrity server-address

（注） ユーザ インターフェイスは複数の Integrity サーバのコンフィギュレーションをサポートしているように見えますが、現在のリリースのセキュリティ アプライアンスでは同時に 1 台のサーバのみがサポートされます。

構文の説明

hostname	Zone Labs Integrity ファイアウォール サーバのホスト名を指定します。ホスト名のガイドラインについては、**name** コマンドを参照してください。
ip-address	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。

コマンド デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバは設定されません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このリリースでは、1 台の Zone Labs Integrity ファイアウォール サーバを設定できます。そのサーバで障害が発生した場合は、まず別の Integrity サーバを設定してからクライアント VPN セッションを再確立します。

サーバをホスト名で指定するには、まず **name** コマンドを使用して Zone Labs サーバ名を設定する必要があります。**name** コマンドを使用する前に、**names** コマンドを使用してコマンドをイネーブルにします。

（注）　現在のリリースのセキュリティ アプライアンスでは同時に 1 台の Integrity サーバのみがサポートされていますが、ユーザ インターフェイスでは最大 5 台の Integrity サーバの設定がサポートされています。アクティブなサーバに障害が発生した場合は、セキュリティ アプライアンス上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

例

次に、IP アドレス 10.0.0.5 にサーバ名 ZL-Integrity-Svr を割り当て、その名前を使用して Zone Labs Intergity サーバを設定する例を示します。

```
hostname(config)# names
hostname(config)# name 10.0.0.5 ZL-Integrity-Svr
hostname(config)# zonelabs-integrity server-address ZL-Integrity-Svr
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、セキュリティ アプライアンスが VPN クライアント接続を閉じるように指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-certificate-port

SSL 証明書を取得する場合に Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity ssl-certificate-port** コマンドを使用します。デフォルト ポート番号（80）に戻すには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

構文の説明

cert-port-number	SSL 証明書を要求する場合に Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポート番号を指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバは SSL 証明書をセキュリティ アプライアンスのポート 80 で要求します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの SSL 通信では、セキュリティ アプライアンスが SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始する場合は、SSL サーバ（セキュリティ アプライアンス）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。**zonelabs-integrity ssl-certificate-port** コマンドで、Zone Labs サーバが SSL サーバ証明書を要求する場合に接続するポートを指定します。

例

次に、セキュリティ アプライアンスのポート 30 で Zone Labs Integrity サーバから SSL 証明書要求を受信するように設定する例を示します。

```
hostname(config)# zonelabs-integrity ssl-certificate-port 30
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-client-authentication

Zone Labs Integrity ファイアウォール サーバの SSL 証明書をセキュリティ アプライアンスで認証できるようにするには、グローバル コンフィギュレーション モードで **zonelabs-integrity ssl-client-authentication** コマンドを *enable* 引数を指定して使用します。Zone Labs の SSL 証明書の認証をディセーブルにするには、*disable* 引数を使用するか、またはこのコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

構文の説明

enable	セキュリティ アプライアンスで Zone Labs Integrity ファイアウォール サーバの SSL 証明書を認証することを指定します。
disable	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバの SSL 証明書のセキュリティ アプライアンスによる認証はディセ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの SSL 通信では、セキュリティ アプライアンスが SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始する場合は、SSL サーバ（セキュリティ アプライアンス）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。ただし、クライアント証明書の認証は任意です。Zone Labs サーバの（SSL クライアント）証明書のセキュリティ アプライアンスによる認証をイネーブルまたはディセーブルにするには、**zonelabs-integrity ssl-client-authentication** コマンドを使用します。

例

次に、Zone Labs Integrity サーバの SSL 証明書を認証するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。