CHAPTER 33

urgent-flag コマンド～ zonelabs integrity ssl-client-authentication コマンド

urgent-flag

TCP ノーマライザを通して URG ポインタを許可または消去するには、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**}

シンタックスの説明

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 ポインタを消去します。

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消去されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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 コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用して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。TCP 検査を **service-policy** コマンドを使用して有効にします。

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 モードに入ります。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、ストリーム内の他のデータよりも高い優先順位の情報を含むパケットを示すために使用されます。TCP RFC 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 システムは緊急オフセットをさまざまな方法で処理します。このため、エンド システムが攻撃を受け易くなります。デフォルトの動作は、URG フラグとオフセットを消去します。

例

次の例では、緊急フラグを許可する方法を示します。

```
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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、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**}

シンタックスの説明

mask	SIP 以外の URI をマスクします。
log	違反が発生した場合、独自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、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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

次の例では、SIP 検査ポリシー 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 を識別する方法を示します。

```
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 マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

url

CRL を検索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 モードには、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*

シンタックスの説明

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 の検索元となる 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

次の表は、このコマンドを入力できるモードを示しています。

	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(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

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、まずそれを削除して、このコマンドの **no** 形式を使用します。

例

次の例では、ca-crl コンフィギュレーション モードに入り、CRL 検索用の URL のリストを作成し、維持するためにインデックス 3 を設定して、CRL の検索元となる URL https://foobin.com を設定します。

```
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 モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
policy	CRL の検索元を指定します。

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っている間に 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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

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*

シンタックスの説明

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っている間に 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。許容される値は 1 ～ 128 です。これは、1,550 バイトのブロック数を指定します。
mempool-size *memory_pool_size*	URL バッファ メモリ プールの最大サイズ（KB）を設定します。指定できる値は、2 ～ 10,240（2 KB ～ 10,240 KB）です。
url-size *long_url_size*	バッファする各 URL の最大サイズを KB 単位で設定します。指定できる値は、Websense では 2、3、4（2 KB、3 KB、4KB）、Secure Computing では 2 または 3（2 KB または 3 KB）です。

デフォルト

このコマンドは、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

次の表は、このコマンドを入力できるモードを示しています。

	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のものです。

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 の長さの URL のフィルタリングが可能です。Secure Computing の場合は、**url-block url-size** コマンドを使用して最大 3 KB の長さの 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 サーバの両方の場合、**url-block block** コマンドは、URL フィルタリング サーバからの応答を待つ間の Web クライアント要求に応じて Web サーバから受信したパケットをセキュリティ アプライアンスにバッファします。この処理により、デフォルトのセキュリティ アプライアンスの動作と比較して、Web クライアントのパフォーマンスが改善されます。デフォルトの動作はパケットをドロップし、接続が許可された場合は Web サーバにパケットの再転送を要求します。

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、HTTP 応答バッファから Web クライアントにブロックを送信して、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て、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 サーバからフィルタリングの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の数を指定します。

url-block url-mempool-size コマンドと共に **url-block url-size** コマンドを使用して、フィルタリングする URL の最大長と、URL のバッファに割り当てる最大メモリを指定します。これらのコマンドを使用して、1,159 バイトより長く 4,096 バイト以下の URL を Websense サーバまたは Secure Computing サーバに渡します。**url-block url-size** コマンドは、1,159 バイトより長い URL をバッファに保存した後、その URL を Websense サーバまたは Secure Computing サーバに渡します（TCP パケット ストリームを使用して）。その結果、サーバがその URL へのアクセスを許可または拒否できます。

例

次の例では、1,550 バイトのブロックを 56 個、URL フィルタリング サーバからの応答のバッファリングに割り当てます。

```
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 バッファ使用状況カウンタを消去します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
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** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

url-cache

N2H2 サーバまたは 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て、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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

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、N2H2 サーバまたは 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 要求を発信している送信元アドレスと 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、N2H2 サーバまたは Websense サーバ上で、ユーザが同じ URL フィルタリング ポリシーを共有していない場合に選択します。
statistics	**statistics** オプションを使用すると、追加の URL キャッシュ統計情報、たとえば、キャッシュ ルックアップの回数やヒット率が表示されます。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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のものです。

使用上のガイドライン

url-cache コマンドには、URL サーバから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 キャッシュをイネーブルにし、キャッシュ サイズを設定し、キャッシュの統計情報を表示する場合に使用します。

キャッシュによって URL アクセス特権が、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 N2H2 または Websense サーバに転送するのではなく、まず一致するアクセス特権を URL キャッシュ内で探します。キャッシュ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）　N2H2 サーバまたは 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 Version 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 Version 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。セキュリティの要求に合致する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 Version 4 および N2H2 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 ログがアップデートされます。

例

次の例では、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** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show url-cache statistics	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-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

url-list

WebVPN ユーザがアクセスする URL のセットを設定するには、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。複数の URL でリストを設定するには、各 URL に対して 1 回、同じリスト名でこのコマンドを複数回使用します。設定済みリスト全体を削除するには、**no url-list** *listname* コマンドを使用します。設定済みの URL を削除するには、**no url-list** *listname url* コマンドを使用します。

複数のリストを設定するには、このコマンドを複数回使用して、各リストに固有の *listname* を割り当てます。

url-list {*listname displayname url*}

no url-list *listname*

no url-list *listname url*

シンタックスの説明

displayname	WebVPN エンド ユーザ インターフェイスに表示されるテキストを入力して、URL を識別します。最大 64 文字です。リストごとに固有の名前でなければなりません。スペースを使用できます。
listname	WebVPN ユーザがアクセスできる URL のセットをグループ化します。最大 64 文字です。最大 64 文字です。セミコロン（;）、アンパサンド（&）、小なり（<）記号は使用できません。
url	リンクを指定します。サポートされる URL タイプは http、https、および cifs です。

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

次の表は、このコマンドを入力できるモードを示しています。

	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。

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、URL のリストを 1 つ以上作成します。特定のグループ ポリシーまたはユーザがリスト内の URL にアクセスできるようにするには、WebVPN モードで、ここで作成した *listname* を **url-list** コマンドと共に使用します。

例

次の例は、www.cisco.com、www.example.com、および www.example.org にアクセスする *Marketing URLs* という URL リストを作成する方法を示しています。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のみ削除します。
url-list	WebVPN モードでこのコマンドを使用すると、グループ ポリシーまたはユーザが URL の設定済みリストにアクセスできます。
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 モードに入って、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 コンフィギュレーション値を設定できます。

url-list（webvpn）

WebVPN サーバのリストと URL 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ます。URL リストを継承しないようにするには、**url-list none** コマンドを使用します。コマンドを 2 回使用すると、先行する設定値が上書きされます。

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

no url-list

シンタックスの説明

index	ホームページ上で表示される優先順位を示します。
none	URL リストにヌル値を設定します。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 ポリシーからリストを継承しないようにします。
value *name*	URL の設定済み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

次の表は、このコマンドを入力するモードを示しています。

	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 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

コマンドを 2 回使用すると、先行する設定値が上書きされます。

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 ポリシー用の WebVPN ホームページに表示する URL リストを識別する前に、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 **url-list** コマンドを使用して、1 つ以上のリストを作成します。

例

次の例では、FirstGroupURLs という URL リストを FirstGroup というグループ ポリシーに適用し、このリストを 1 番目の URL リストに指定しています。

```
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のみ削除します。
show running-configuration url-list	現在設定されている **url-list** コマンドのセットを表示します。
url-list	WebVPN ユーザがアクセスできる URL のセットを設定するには、グローバル コンフィギュレーション モードでアクセスできる WebVPN モードでこのコマンドを使用します。
webvpn	webvpn モードに入ります。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 ポリシーに対する webvpn の値を設定するため）、またはユーザ名 webvpn コンフィギュレーション モード（特定のユーザに対する webvpn の値を設定するため）のいずれかです。

url-server

filter コマンドで使用する N2H2 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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

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*]

シンタックスの説明

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 サーバに向かって作成される TCP 接続の最大数を指定します。これはサーバごとの数であるため、複数のサーバに対して、それぞれ別の接続値を指定することができます。
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	（オプション）認証サーバが常駐するネットワーク インターフェイス。指定しない場合、デフォルトは内部インターフェイスです。
port *number*	N2H2 サーバ ポート。セキュリティ アプライアンスは、UDP 返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、経過後にセキュリティ 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（下位互換性を保つため）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 はベンダー文字列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 サーバに向かって作成される TCP 接続の最大数を指定します。これはサーバごとの数であるため、複数のサーバに対して、それぞれ別の接続値を指定することができます。
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	認証サーバが常駐するネットワーク インターフェイス。指定しない場合、デフォルトは内部インターフェイスです。
timeout *seconds*	許容される最大アイドル時間で、経過後にセキュリティ 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、Version 1 です。
vendor websense	URL フィルタリング サービス ベンダーが Websense であることを示します。
version	プロトコル Version **1** または Version **4** を指定します。デフォルトは TCP プロトコル Version 1 です。TCP は、Version 1 または Version 4 を使用して設定できます。UDP の設定に使用できるのは、Version 4 だけです。

デフォルト

このコマンドは、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

次の表は、このコマンドを入力できるモードを示しています。

	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のものです。

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。ただし、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 のどちらか 1 つだけです。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アップデートされないため、ベンダーの指示に従って別途アップデートする必要があります。

HTTPS および FTP に対して **filter** コマンドを実行するには、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 **filter** コマンドもすべて削除されます。

サーバを指示した後、**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（到達できないサーバも含む）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** コマンドを適切な形式で使用して、URL フィルタリング アプリケーション サーバを指示します。

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

ステップ 3　（オプション）**url-cache** コマンドを使用して、URL キャッシュをイネーブルにし、認識される応答時間を改善します。

ステップ 4　（オプション）**url-block** コマンドを使用して、長い URL および HTTP の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** の各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

次の例では、N2H2 を使用している場合に、10.0.2.54 ホストからの接続を除く、発信 HTTP 接続をすべてフィルタリングします。

```
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
```

次の例では、Websense を使用している場合に、10.0.2.54 ホストからの接続を除く、発信 HTTP 接続をすべてフィルタリングします。

```
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消去します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
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。ユーザ認証アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、ユーザ認証の値を別のグループ ポリシーから継承できます。

イネーブルの場合、ユーザ認証ではハードウェア クライアントの背後にいる個々のユーザが、トンネルを越えてネットワークへのアクセスを取得するように認証する必要があります。

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

no user-authentication

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

	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します。

プライマリ セキュリティ アプライアンスでのユーザ認証が必要な場合は、バックアップ サーバでも同様に設定されていることを確認します。

例

次の例は、「FirstGroup」というグループ ポリシーのユーザ認証をイネーブルにする方法を示します。

```
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	ユーザ認証を受けずに IP 電話を接続できるようにします。Secure Unit Authentication は有効なままになります。
leap-bypass	イネーブルの場合、LEAP パケットが VPN クライアントの背後にある無線デバイスから VPN トンネルを通過した後でユーザ認証を行います。これにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できます。確立後、ワークステーションはユーザごとの認証をもう一度実行します。
secure-unit-authentication	クライアントがトンネルを開始するたびに VPN クライアントがユーザ名とパスワードを使用した認証を要求することにより、さらにセキュリティが向上します。
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 タイムアウト期間中にユーザ接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

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、アイドル タイムアウト値を別のグループ ポリシーから継承できます。アイドル タイムアウト値を継承し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 タイムアウト期間中にハードウェア クライアントの背後にいるユーザによる通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

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

no user-authentication-idle-timeout

シンタックスの説明

minutes	アイドル タイムアウト期間を分単位で指定します。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容します。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 ポリシーからユーザ認証のアイドル タイムアウト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

次の表は、このコマンドを入力できるモードを示しています。

	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。

例

次の例は、「FirstGroup」というグループ ポリシーに 45 分のアイドル タイムアウト値を設定する方法を示します。

```
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。

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、削除するユーザ名で、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、ユーザ名を付加せずに、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*

シンタックスの説明

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** コマンドで定義するパスワードは、セキュリティを維持するため、コンフィギュレーションに保存されるときに暗号化されます。**show running-config** コマンドを入力したときに、**username** コマンドで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は、**show running-config** を実行すると次のように表示されます。 `username pat password rvEdRh0xPC8bel7s encrypted` CLI で実際に **encrypted** キーワードを入力するのは、別のセキュリティ アプライアンスにコンフィギュレーションをカット 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	入力したパスワードを unicode に変換し、MD4 でハッシュすることを指定します。ユーザを MSCHAPv1 または MSCHAPv2 を使用して認証している場合に、このキーワードを使用します。
name	ユーザの名前を 4 ～ 15 文字で指定します。
nopassword	このユーザにはパスワードが不要であることを示します。
nt-encrypted	パスワードを MSCHAPv1 または MSCHAPv2 での認証用に暗号化することを指定します。ユーザを追加するときに **mschap** キーワードを指定すると、**show running-config** コマンドでコンフィギュレーションを表示したときに、**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** コマンドで定義するパスワードは、セキュリティを維持するため、コンフィギュレーションに保存されるときに暗号化されます。**show running-config** コマンドを入力したときに、**username** コマンドで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は、**show running-config** を実行すると次のように表示されます。 `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、別のセキュリティ アプライアンスにコンフィギュレーションをカット 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。
password *password*	3 ～ 16 文字のパスワードを設定します。
privilege *priv_level*	使用する特権レベルを 0（最低）～ 15（最高）に指定します。デフォルトの特権レベルは 2 です。この特権レベルは、コマンドの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

次の表は、このコマンドを入力できるモードを示しています。

	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)	**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 コマンドを入力したときに、このデータベースが認証用に使われます。

CLI にアクセスできるユーザや特権 EXEC モードに入れないユーザをローカル データベースに追加する場合は、コマンド認可を設定する必要があります（**aaa authorization command** コマンドを参照）。コマンド認可を設定しないと、ユーザの特権レベルが 2（デフォルト）以上であれば、CLI で自分のパスワードを使って特権 EXEC モード（およびすべてのコマンド）にアクセスできるようになります。または、AAA 認証を使用して、ユーザが **login** コマンドを使えないようにするか、全ローカル ユーザの特権レベルを 1 に設定して、どのユーザが **enable** パスワードで特権 EXEC モードにアクセスできるかを制御します。

デフォルトでは、このコマンドを使用して追加した VPN ユーザには、アトリビュートまたはグループ ポリシーのアソシエーションはありません。**username attributes** コマンドを使用して、すべての値を明示的に設定する必要があります。

例

次の例では、12345678 というパスワードと、特権レベル 12 を持つ anyuser というユーザを設定する方法を示します。

```
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消去します。
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。
username attributes	ユーザ名アトリビュート モードに入って、個々のユーザのアトリビュートを設定できるようにします。
webvpn	config-group-webvpn モードに入ります。このモードで、指定したグループに対する WebVPN アトリビュートを設定できます。

username attributes

ユーザ名アトリビュート モードに入るには、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。特定のユーザのすべてのアトリビュートを削除するには、このコマンドの **no** 形式を使用して、ユーザ名を付加します。すべてのユーザのアトリビュートを削除するには、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。アトリビュート モードを使用すると、指定したユーザに対してアトリビュート値ペアを設定できます。

username {*name*} **attributes**

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

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

	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

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 コマンドは、このデータベースを認証用に使用します。ユーザ名アトリビュートは、**username** コマンドまたは **username attributes** コマンドのいずれかを使用して設定します。

ユーザ名コンフィギュレーション モードのコマンドのシンタックスには、共通する次の特性があります。

- **no** 形式は、実行コンフィギュレーションからアトリビュートを削除します。
- **none** キーワードも、実行コンフィギュレーションからアトリビュートを削除します。ただし、アトリビュートにヌル値を設定することにより削除され、継承しないようにします。
- ブール アトリビュートには、イネーブルまたはディセーブルになっている設定のための明示的なシンタックスがあります。

username attributes コマンドでユーザ名コンフィギュレーション モードに入ると、次のアトリビュートを設定できます。

アトリビュート	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 パスワードの保管をイネーブルまたはディセーブルにします。
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。

アトリビュート	機能
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られる IP アドレスとネット マスクを指定します。
vpn-group-policy	アトリビュートの継承元になるグループ 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で指定するか、または ***none*** を使用してディセーブルにします。
vpn-session-timeout	ユーザの最長接続時間を分単位で指定するか、***none*** を使用して無制限にします。
vpn-simultaneous-logins	使用可能な同時ログインの最大数を指定します。
vpn-tunnel-protocol	許可されたトンネリング プロトコルを指定します。
webvpn	webvpn アトリビュートを設定する webvpn モードに入ります。

ユーザ名に対する webvpn モード アトリビュートは、ユーザ名の 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** コマンドを入力して設定します。詳細については、**webvpn** コマンド（グループ ポリシー アトリビュートおよびユーザ名アトリビュート モード）の説明を参照してください。

例

次の例では、「anyuser」という名前のユーザのユーザ名アトリビュート コンフィギュレーション モードに入る方法を示します。

```
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消去します。
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。
username	ユーザをセキュリティ アプライアンスのデータベースに追加します。
webvpn	指定されたグループの WebVPN アトリビュートを設定するユーザ名の webvpn コンフィギュレーション モードに入ります。

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*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

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のテキストは「USERNAME」です。

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

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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現されます。このパラメータの説明は、このマニュアルでは取り扱いません。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 で入手可能です。

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）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目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 を使用することをお勧めします。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のに便利な機能があります。

例

次の例では、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 に変更しています。

```
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-parameter

SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求の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** コマンドを使用します。これは HTTP Forms コマンドを使用した SSO です。

user-parameter *name*

（注）　HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

シンタックスの説明

name	HTTP POST 要求に含まれるユーザ名パラメータの名前です。最大長は 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

次の表は、このコマンドを入力できるモードを示しています。

	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、HTTP POST 要求を使用して、シングル サインオン認証要求を SSO サーバに送信します。要求されたコマンド **user-parameter** は、この HTTP POST 要求が 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の値を入力します。この値は HTTP POST 要求に入力されて、認証 web サーバに渡されます。

例

AAA サーバ ホスト コンフィギュレーション モードで入力された次の例では、ユーザ名パラメータの userid が SSO 認証で使用される HTTP POST 要求に含まれることを指定します。

```
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とパスワードを受信する 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 サーバとの交換に使用する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 要求のパラメータの名前を指定します。
start-url	事前ログイン クッキーの取得先 URL を指定します。

validate-attribute

RADIUS アカウンティングを使用する際に RADIUS アトリビュートを検証するには、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、デフォルトではディセーブルになっています。

validate-attribute [*attribute_number*]

no validate-attribute [*attribute_number*]

シンタックスの説明

attribute_number	RADIUS アカウンティングで検証する RADIUS アトリビュート。有効な範囲は 1 ～ 191 です。ベンダー固有のアトリビュートはサポートされていません。

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

次の表は、このコマンドを入力できるモードを示しています。

	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 アプライアンスでは、Framed IP アトリビュートに加えて RADIUS アトリビュートも照合します。このコマンドは、インスタンスを複数設定することができます。

RADIUS アトリビュートのタイプのリストを見るには、次のサイトにアクセスしてください。

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

例

次の例では、ユーザ名 RADIUS アトリビュートの RADIUS アカウンティングをイネーブルにする方法を示します。

```
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検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

verify

ファイルのチェックサムを検証するには、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*]

シンタックスの説明

/md5	（オプション）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	（オプション）指定したイメージの既知の MD5 値。このコマンドで 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 アプライアンスのみで使用でき、内蔵フラッシュ 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、エイリアス関係にあります。 • ***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 アプライアンスのみで使用でき、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、内蔵フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、***flash*** は ***disk0*** のエイリアスです。 • ***ftp://***[*user*[***:***password]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;type=***xx] ***type*** には、次のいずれかのキーワードを指定できます。 － ***ap***：ASCII パッシブ モード － ***an***：ASCII 通常モード － ***ip***：（デフォルト）バイナリ パッシブ 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。 ただし、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てください。

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に、ftp、http、tftp などのネットワークのファイルをソースとして指定できます。***/md5*** オプションを指定せずに **verify** コマンドを使用すると、フラッシュ メモリにあるローカル イメージしか検証できません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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、ファイルを使う前にそのチェックサムを検証します。

ディスクで配布されるソフトウェア イメージごとに、イメージ全体用のチェックサムが 1 つあります。このチェックサムは、イメージをフラッシュ メモリにコピーした場合にだけ表示されます。あるディスクから別のディスクにコピーした場合には表示されません。

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 メモリやサーバにコピーしたときにチェックサムを検証できるようにしてください。Cisco.com には、イメージのさまざまな情報が掲載されています。

フラッシュ メモリの内容を表示する場合は、**show flash** コマンドを使用します。表示される内容に、個々のファイルのチェックサムは含まれていません。イメージをフラッシュ メモリにコピーした後で、そのチェックサムを再度計算して検証するには、**verify** コマンドを使用します。ただし、**verify** コマンドは、ファイルがファイル システムに保存されている場合にのみ、整合性のチェックを行うことに注意してください。そのため、壊れた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ている可能性があります。セキュリティ アプライアンスに壊れたイメージが転送された場合、ソフトウェアは、イメージが壊れていることを検出できず、ファイルの検証が問題なく完了します。

Message Digest 5（MD5）ハッシュ アルゴリズムを使ってファイルを検証する場合は、**verify** コマンドと共に ***/md5*** オプションを使用します。MD5（RFC 1321 で規定）は、128 ビットの固有のメッセージ ダイジェストを作成してデータの整合性を検証するアルゴリズムです。**verify** コマンドの ***/md5*** オプションは、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 チェックサムの値を、その既知の MD5 チェックサム値と比較することにより、イメージの整合性を確認します。Cisco.com では、ローカル システム イメージ値との比較用に、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 値を取得できます。

MD5 による整合性の確認を行うには、***/md5*** キーワードを使用して **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 値が計算されて表示されます。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、先に Cisco.com から MD5 値を取得しておき、その値をコマンドのシンタックスで指定できます。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 値が一致しないというのは、イメージが壊れているか、入力された MD5 値が間違っているという意味です。

例

次の例では、cdisk.bin というイメージ ファイルを検証します。ただし、わかりやすいように、テキストの一部が省略されています。

```
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。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

version {*1* | *2*}

no version

シンタックスの説明

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 と 2 の両方のパケットを受け取れますが、バージョン 1 のパケットしか送信しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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

グローバル設定をインターフェイスごとに上書きするには、インターフェイスで **rip send version** コマンドと **rip receive version** コマンドを指定します。

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することで、RIP アップデートを認証できます。

例

次の例では、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	指定した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 モードに入ります。

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**]

シンタックスの説明

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。このアドレスが、セキュリティ アプライアンスに向かってルーティングされる未使用アドレスであることを確認してください。たとえば、外部にアクセスするときに内部アドレスの NAT を実行し、仮想 HTTP サーバへの外部アクセスを提供する場合は、仮想 HTTP サーバ アドレスに対して、グローバル NAT アドレスの 1 つを使用できます。
warning	（オプション）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発生しないテキストベースのブラウザのみに適用されます。

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

次の表は、このコマンドを入力できるモードを示しています。

	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)	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、このコマンドは必要なくなり、廃止されました。
7.2(2)	基本 HTTP 認証（デフォルト）を使用するか、**aaa authentication listener** コマンドによる HTTP リダイレクションを使用するかを選択できるようになったため、このコマンドが復活しました。リダイレクション方式では、HTTP 認証をカスケードする際に特別なコマンドを必要としません。

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（**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 アプライアンスではデフォルトで基本 HTTP 認証が使用されます。セキュリティ アプライアンスが Web ページ（**aaa authentication listener** コマンドに **redirect** キーワードを指定してセキュリティ アプライアンス自身によって生成された Web ページ）に HTTP 接続を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 認証を使用し続ける場合、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 サーバでも認証が必要な場合、**virtual http** コマンドを使用すると、セキュリティ アプライアンス（AAA サーバ経由）と宛先 HTTP サーバで別々に認証することができます。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 サーバおよび HTTP サーバのユーザ名およびパスワードが同じでない場合、HTTP 認証は失敗します。

このコマンドは、セキュリティ アプライアンス上の仮想 HTTP サーバへの AAA 認証を必要とするすべての HTTP 接続をリダイレクトします。セキュリティ アプライアンスは、AAA サーバのユーザ名およびパスワードを要求します。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ますが、AAA サーバのユーザ名およびパスワードは含まれません。HTTP パケットにユーザ名およびパスワードが含まれていないため、HTTP サーバは個々のユーザに HTTP サーバのユーザ名およびパスワードを要求します。

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

例

次の例は、AAA 認証と共に仮想 HTTP 認証をイネーブルにする方法を示しています。

```
hostname(config)# access-list HTTP-ACL extended permit tcp 10.1.1.0 any eq 80
hostname(config)# aaa authentication match HTTP-ACL inside tacacs+
hostname(config)# virtual http 10.1.2.1
```

関連コマンド

コマンド	説明
aaa authentication listener http	セキュリティ アプライアンスで認証に使用され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** コマンド文を削除します。
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と、ブラウザ キャッシュにあるユーザ名および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 サーバを設定することで、認証が必要な他のタイプの接続を開始する前にセキュリティ アプライアンスでユーザを認証できるようにします。

virtual telnet

セキュリティ アプライアンスで仮想 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 アプライアンスで認証プロンプトが表示されない別のタイプのトラフィックを認証する必要がある場合は、仮想 Telnet サーバでユーザを認証しなければならないことがあります。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*

シンタックスの説明

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。このアドレスが、セキュリティ アプライアンスに向かってルーティングされる未使用アドレスであることを確認してください。たとえば、外部にアクセスするときに内部アドレスの NAT を実行し、仮想 Telnet サーバへの外部アクセスを提供する場合は、仮想 Telnet サーバ アドレスに対して、グローバル NAT アドレスの 1 つを使用できます。

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

次の表は、このコマンドを入力できるモードを示しています。

	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のものです。

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（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）に対してネットワーク アクセス認証を設定できますが、直接 HTTP、Telnet、または FTP だけで認証することもできます。ユーザは認証を必要とする別のトラフィックが許可される前に、これらのサービスの 1 つで先に認証する必要があります。セキュリティ アプライアンスを通して HTTP、Telnet、または FTP を許可せずに、別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 アプライアンスで設定された所定の IP アドレスにユーザが Telnet 接続し、セキュリティ アプライアンスが Telnet プロンプトを表示するように、仮想 Telnet を設定できます。

権限のないユーザが仮想 Telnet IP アドレスに接続したとき、ユーザ名とパスワードが要求され、AAA サーバによって認証されます。認証されると、「Authentication Successful.」というメッセージが表示されます。その後、ユーザは認証を必要とするその他のサービスに正常にアクセスできるようになります。

例

次の例では、他のサービスに対する AAA 認証と共に仮想 Telnet をイネーブルにする方法を示します。

```
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 10.1.2.1 eq
telnet
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 209.165.200.225
eq smtp
hostname(config)# aaa authentication match AUTH inside tacacs+
hostname(config)# virtual telnet 10.1.2.1
```

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** コマンド文を削除します。
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している場合、このコマンドを使用すると、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実行できます。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には、トラフィックを渡す VLAN ID が必要です。VLAN サブインターフェイスを使用すると、1 つの物理インターフェイス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（たとえば複数のセキュリティ コンテキスト）にトラフィックを別に保存できます。

vlan *id*

no vlan

シンタックスの説明

id	1 ～ 4094 の整数を指定します。一部の VLAN ID には、接続されたスイッチで予約されているものもあります。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

次の表は、このコマンドを入力できるモードを示しています。

	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)	このコマンドが、**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 モードのコマンドに変更されました。

使用上のガイドライン

1 つの VLAN だけを、物理インターフェイスではなく、サブインターフェイスに割り当てることができます。各サブインターフェイスは、トラフィックを通過する前に VLAN ID を持つ必要があります。VLAN ID を変更するには、**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 を使用して **vlan** コマンドを入力すると、セキュリティ アプライアンスは古い ID を変更します。

サブインターフェイスをイネーブルにするために、**no shutdown** コマンドで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、物理インターフェイスはタグの付かないパケットを通過させるため、一般的には物理インターフェイスがトラフィックを通過させないようにします。したがって、インターフェイスを停止することで物理インターフェイスを介してトラフィックが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で、物理インターフェイスがトラフィックを通過させないことを確認します。物理インターフェイスがタグの付かないパケットを通過させるようにする場合は、通常通り **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変わります。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 Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例では、サブインターフェイスに VLAN 101 を割り当てます。

```
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
```

次の例では、VLAN を 102 に変更します。

```
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	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
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 モードに入ります。
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。

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。グループ ポリシー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** 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、およびマルチ コンテキスト モードや透過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、シングルモードかつルーテッド モードの場合のみです。

シンタックスの説明

vpdn group *group_name*	VPDN グループの名前を指定します。
localname *username*	認証するユーザ名を VPDN グループにリンクします。この名前は、**vpdn username** コマンドで設定した名前と一致する必要があります。
request dialout pppoe	PPPoE のダイヤルアウト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）接続で使用する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 ネットワークを設定するときに、どの認証プロトコル（PAP、CHAP、または MS-CHAP）を使用するかを選択します。クライアントで選択したプロトコルと同じものをセキュリティ アプライアンスでも使用する必要があります。Password Authentication Protocol（PAP; パスワード認証プロトコル）では、PPP のピアがお互いに認証し合います。このとき、クリア テキストのホスト名とユーザ名を渡します。Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）の場合は、PPP のピアがアクセス サーバと通信して不正なアクセスを防ぎます。MS-CHAP は、CHAP を Microsoft が独自に拡張したものです。PIX Firewall は、MS-CHAP バージョン 1 だけをサポートしています（バージョン 2.0 はサポートしていません）。 ホストで認証プロトコルが設定されていない場合は、コンフィギュレーションに **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

次の表は、このコマンドを入力できるモードを示しています。

	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 Dial-up Networking（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）は、遠く離れたダイヤルイン ユーザとプライベート ネットワークを結ぶときに使用するポイントツーポイント接続です。セキュリティ アプライアンスの VDPN は、レイヤ 2 トンネリング技術である PPPoE を使用して、リモート ユーザがパブリック ネットワークを経由してプライベート ネットワークにダイヤルアップ接続できるようにします。

PPPoE とは、Point-to-Point Protocol（PPP）over Ethernet の略です。PPP は、IP、IPX、ARA などのネットワーク レイヤ プロトコルと併用できるように設計されています。また、CHAP と PAP がセキュリティ メカニズムとして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。**clear configure vpdn group** コマンドは、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、アクティブな L2TP トンネルと PPPoE トンネルを停止します。**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 をカプセル化するので、PPP が認証を行うことと、VPN トンネル内で動作するクライアントのセッションで ECP と CCP が機能することが必要です。また、PPPoE では、PPP によって IP アドレスが割り当てられるので、DHCP を使用することはできません。

（注） PPPoE 用の VPDN グループを設定しないと、PPPoE では接続を確立できません。

PPPoE 用の VPDN グループを定義するには、まず **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の PPPoE クライアントに関連付けます。

利用している ISP が認証を必要とする場合は、**vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} コマンドで、ISP で使用されている認証プロトコルを選択します。

ISP が割り当てたユーザ名を VPDN グループと関連付けるには、**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。PPPoE 用に設定した VPDN グループのユーザ名と同じものを指定してください。

（注） ISP が CHAP または MS-CHAP を使用している場合は、ユーザ名のことをリモート システム名、パスワードのことを CHAP シークレットということがあります。

PPPoE クライアントの機能は、デフォルトでオフになっています。そのため、VPDN を設定したら、**ip address** *if_name* **pppoe** [**setroute**] コマンドで、PPPoE をイネーブルにしてください。**setroute** オプションは、デフォルトのルートがない場合に、デフォルト ルートを作成します。

PPPoE を設定するとすぐに、セキュリティ アプライアンスが、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、異常を問わず切断されると、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見つけようとします。

いったん PPPoE セッションを開始したら、次の **ip address** コマンドは使用しないでください。使用すると、PPPoE セッションが終了されます。

- **ip address outside pppoe**：新しい PPPoE セッションを開始しようとします。
- **ip address outside dhcp**：インターフェイスが DHCP コンフィギュレーションを取得するまでディセーブルになります。
- **ip address outside** *address netmask*：インターフェイスを、通常どおり初期化されたインターフェイスとして起動します。

例

次の例では、*telecommuters* という VPDN グループを作成し、PPPoE クライアントを設定します。

```
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、およびマルチ コンテキスト モードや透過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、シングルモードかつルーテッド モードの場合のみです。

シンタックスの説明

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 アプライアンスの NVRAM の特別な場所に保存します。Auto Update Server がセキュリティ アプライアンスにコンフィギュレーションを消去するコマンドを送信した後で接続が中断した場合に、セキュリティ アプライアンスが NVRAM のこの場所からユーザ名とパスワードを読み取って、アクセス コンセントレータとの認証をやり直します。

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

次の表は、このコマンドを入力できるモードを示しています。

	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 のユーザ名は、**vpdn group** *group_name* **localname** *username* コマンドで指定した VPDN グループのユーザ名と同じでなければなりません。

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

次の例では、*bob_smith* というユーザ名と *telecommuter*9/8 というパスワードを作成します。

```
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

設定済みの時間範囲ポリシーをグループ 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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、時間範囲値を別のグループ ポリシーから継承できます。値を継承し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

シンタックスの説明

none	VPN アクセス時間にヌル値を設定することで、時間範囲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

無制限です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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)(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

例

次の例では、824 と呼ばれる時間範囲ポリシーに FirstGroup という名前のグループ ポリシーを関連付ける方法を示します。

```
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および 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。アトリビュー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** 形式を使用します。設定されている Vpn アドレスの割り当て方法をセキュリティ アプライアンスからすべて削除するには、引数なしで、このコマンドの **no** 形式を使用します。

vpn-addr-assign {**aaa** | **dhcp** | **local**}

no vpn-addr-assign [**aaa** | **dhcp** | **local**]

シンタックスの説明

aaa	外部 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	内部認証サーバから IP アドレスを割り当て、トンネル グループに関連付けます。

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

次の表は、このコマンドを入力できるモードを示しています。

	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)(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

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 アドレスの範囲を定義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。**vpn-framed-ip-address** コマンドおよび **vpn-framed-netmask** コマンドを使用して、個々のユーザに IP アドレスとネットマスクを割り当てます。

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

例

次の例では、アドレスの割り当て方法として DHCP を設定する方法を示します。

```
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ときに使用する必要がある 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	IP アドレスを指定して、特定のユーザに割り当てます。
vpn-framed-ip-netmask	ネットマスクを指定して、特定のユーザに割り当てます。

vpn-filter

VPN 接続に使用する ACL の名前を指定するには、グループ 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ます。値を継承しないようにするには、**vpn-filter none** コマンドを使用します。

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

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

no vpn-filter

シンタックスの説明

none	アクセス リストがないことを指定します。ヌル値を設定して、アクセス リストを拒否します。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*	設定済みアクセス 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

次の表は、このコマンドを入力できるモードを示しています。

	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)(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

WebVPN は、**vpn-filter** コマンドで定義された ACL を使用しません。

例

次の例では、FirstGroup という名前のグループ ポリシーの acl_vpn と呼ばれるアクセス リスト名を実行するフィルタを設定する方法を示します。

```
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 リストを作成します。または、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

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

	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)(1)	このコマンドが導入されました。

例

次の例では、anyuser という名前のユーザに 10.92.166.7 という IP アドレスを設定する方法を示します。

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

関連コマンド

コマンド	説明
vpn-framed-ip-netmask	このユーザのサブネット マスクを指定します。

vpn-framed-ip-netmask

特定のユーザに割り当てるサブネット マスクを指定するには、ユーザ名モードで **vpn-framed-ip-netmask** コマンドを使用します。サブネットマスクを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ip-netmask {*netmask*}

no vpn-framed-ip-netmask

シンタックスの説明

netmask	このユーザのサブネット マスクを指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	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)(1)	このコマンドが導入されました。

例

次の例では、anyuser という名前のユーザに 255.255.255. 254 というサブネット マスクを設定する方法を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
```

（注） RADIUS がサブネット マスクだけを返す場合、認証は独自のサブネット ネットマスクを持つローカル プールからの IP アドレスを使用します。RADIUS からのマスクは使用しません。これを防止するには、RADIUS からネットマスクと IP アドレスの両方を返します。

関連コマンド

コマンド	説明
vpn-framed-ip-address	このユーザの IP アドレスを指定します。

vpn-group-policy

ユーザに設定済みのグループ ポリシーからアトリビュートを継承させるには、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。ユーザ 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。このコマンドを使用すると、ユーザがユーザ名 レベルで設定していないアトリビュートを継承できます。

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

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

シンタックスの説明

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 ポリシーのアソシエーションはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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)(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

アトリビュートをユーザ名モードで利用できる場合、ユーザ名モードで設定することにより、特定のユーザに対するグループ ポリシーのアトリビュートの値を上書きできます。

例

次の例では、FirstGroup という名前のグループ ポリシーからアトリビュートを使用するように anyuser という名前のユーザを設定する方法を示します。

```
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 アプライアンスのデータベースに追加します。
group-policy attributes	グループ ポリシーの AVP を設定できるグループ ポリシー アトリビュート モードに入ります。
username	ユーザをセキュリティ アプライアンスのデータベースに追加します。
username attributes	ユーザ名アトリビュート モードに入って、個々のユーザの AVP を設定できるようにします。

vpn-idle-timeout

ユーザの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まったくなかった場合、セキュリティ アプライアンスは接続を終了します。

このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、タイムアウト値を別のグループ ポリシーから継承できます。値を継承し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

シンタックスの説明

minutes	タイムアウト期間を分単位で指定します。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容します。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

次の表は、このコマンドを入力できるモードを示しています。

	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)(1)	このコマンドが導入されました。

例

次の例では、「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方法を示します。

```
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 接続に許可されている最大時間を設定します。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 モードに入るには、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） ASA Models 5540 および 5520 だけが、VPN ロードバランシングをサポートします。VPN ロードバランシングには、有効な 3DES ライセンスまたは 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。有効な 3DES ライセンスまたは AES ライセンスが検出されなかった場合、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しません。また、ライセンスで許可されていない限り、ロードバランシング システムが 3DES の内部設定を行わないようにします。

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	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。

使用上のガイドライン

vpn load-balancing コマンドを使用して、VPN ロードバランシング モードに入ります。次のコマンドは、VPN ロードバランシング モードで使用できます。

cluster encryption

cluster ip address

cluster key

cluster port

interface

nat

participate

priority

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。プロンプト内の変化に注意してください。

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

次に、クラスタのパブリック インターフェイスを「test」として、クラスタのプライベート インターフェイスを「foo」として指定するインターフェイス コマンドを含む、VPN ロードバランシング コマンド シーケンスの例を示します。

```
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
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	ロードバランシング実行時のコンフィギュレーションを削除して、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-nac-exempt

ポスチャ確認を免除するリモート コンピュータのタイプのリストにエントリを追加するには、グループ ポリシー コンフィギュレーション モードで **vpn-nac-exempt** コマンドを使用します。

vpn-nac-exempt os "*os name*" [**filter** {*acl-name* | **none**}] [**disable**]

継承をディセーブルにし、すべてのホストをポスチャ確認の対象にするには、**vpn-nac-exempt** のすぐ後ろに **none** キーワードを入力します。

vpn-nac-exempt none

免除リストからエントリを削除するには、このコマンドの **no** 形式を使用し、削除するエントリのオペレーティング システム（および ACL）を指定します。

no vpn-nac-exempt [os "*os name*"] [**filter** {*acl-name* | **none**}] [**disable**]

このグループ ポリシーの免除リストにある全エントリを削除し、デフォルトのグループ ポリシーの免除リストを継承するには、キーワードを指定せずにこのコマンドの **no** 形式を使用します。

no vpn-nac-exempt

シンタックスの説明

acl-name	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含まれる ACL の名前。
disable	免除リストのエントリを削除せずにディセーブルにします。
filter	コンピュータのオペレーティング システムの名前が *os name* に一致したときに、トラフィックをフィルタリングするために ACL を適用します。
none	このキーワードを **vpn-nac-exempt** のすぐ後ろに入力した場合は、継承がディセーブルになり、すべてのホストがポスチャ確認の対象になります。 **filter** のすぐ後ろに入力した場合は、ACL を指定しないことを示します。
OS	オペレーティング システムのポスチャ確認を免除します。
os name	オペレーティング システムの名前。引用符は、オペレーティング システムの名前にスペースが入っている場合のみ必要です（Windows XP など）。

デフォルト

デフォルトでは、免除リストは空になっています。

フィルタ アトリビュートのデフォルトの値は none です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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
7.2(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　ポスチャ確認を免除するリモート ホストのオペレーティング システム（および ACL）ごとに **vpn-nac-exempt** を 1 回入力します。

例

次の例では、Windows XP を実行しているすべてのホストを、ポスチャ確認を免除するコンピュータのリストに追加します。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows XP"
hostname(config-group-policy)
```

次の例では、Windows 98 を実行しているホストをすべて免除し、これらのホストからのトラフィックに acl-1 という ACL を適用します。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

次の例では、上と同じエントリを免除リストに追加していますが、ディセーブルにしています。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1 disable
hostname(config-group-policy)
```

次の例では、同じエントリを、ディセーブルかどうかにかかわらず、免除リストから削除しています。

```
hostname(config-group-policy)# no vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

次の例では、継承をディセーブルにして、すべてのホストをポスチャ確認の対象にしています。

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

次の例では、免除リストからすべてのエントリを削除しています。

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
nac	グループ ポリシーでネットワーク アドミッション コントロールをイネーブルにします。

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**}

シンタックスの説明

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*	インデックス番号ごとにシングル 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。プロトコルには、次の種類があります。 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

次の表は、このコマンドを入力できるモードを示しています。

	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)(1)	このコマンドが導入されました。

例

次の例では、すべてのリモートアクセス セッションをログオフする方法を示します。

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

次の例では、すべての IPSec セッションをログオフする方法を示します。

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

vpn-sessiondb max-session-limit

VPN セッションをセキュリティ アプライアンスが許可し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。セッションの制限値を削除するには、このコマンドの **no** 形式を使用します。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**

シンタックスの説明

session-limit	許容する VPN セッションの最大数を指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	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

次の例では、VPN セッションの最大制限値である 450 に設定する方法を示します。

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

関連コマンド

コマンド	説明
vpn-sessiondb logoff	IPsec VPN セッションおよび WebVPN セッションのすべてまたは特定のタイプをログオフします。
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

WebVPN セッションをセキュリティ アプライアンスが許可し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。セッションの制限値を削除するには、このコマンドの **no** 形式を使用します。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

シンタックスの説明

session-limit	許容する WebVPN セッションの最大数を指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	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 WebVPN セッションに適用されます。

例

次の例では、WebVPN セッションの最大制限値である 75 に設定する方法を示します。

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

関連コマンド

コマンド	説明
vpn-sessiondb logoff	IPsec VPN セッションおよび WebVPN セッションのすべてまたは特定のタイプをログオフします。
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。

このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、タイムアウト値を別のグループ ポリシーから継承できます。値を継承し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

シンタックスの説明

minutes	タイムアウト期間を分単位で指定します。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容します。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

次の表は、このコマンドを入力できるモードを示しています。

	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)(1)	このコマンドが導入されました。

例

次の例では、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方法を示します。

```
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まったくなかった場合、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

ユーザに許容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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。この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

シンタックスの説明

integer	0 ～ 2147483647 の数値です。

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

次の表は、このコマンドを入力できるモードを示しています。

	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)(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。

例

次の例では、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方法を示します。

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

vpn-tunnel-protocol

VPN トンネルのタイプ（IPSec、L2TP over IPSec、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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no vpn-tunnel-protocol [webvpn | l2tp-ipsec | IPSec]

シンタックスの説明

IPSec	2 つのピア間（リモートアクセス クライアントまたはその他のセキュアなゲートウェイ）で 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、およびキー管理を管理するセキュリティ結合を作成します。
l2tp-ipsec	L2TP 接続のために IPSec トンネルをネゴシエートします。
webvpn	HTTPS 対応の Web ブラウザを経由してリモート ユーザに VPN サービスを提供します。クライアントは不要です。

デフォルト

IPSec です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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)(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。

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 トンネルを越えて接続するには、ユーザに対して少なくとも 1 つのトンネリング モードを設定する必要があります。

例

次の例では、「FirstGroup」という名前のグループ ポリシーに対して WebVPN および IPSec トンネリング モードを設定する方法を示します。

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

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

次の表は、このコマンドを入力できるモードを示しています。

	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 のみに適用されます。

例

次の例は、設定済み EasyVPN サーバへの Easy VPN Remote 接続の確立を試行する方法を示しています。

```
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

次の表は、このコマンドを入力できるモードを示しています。

	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 のみに適用されます。

例

次の例は、Easy VPN Remote 接続を切断する方法を示しています。

```
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

次の表は、このコマンドを入力できるモードを示しています。

	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 のみに適用されます。

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」とも呼ばれる）として機能します。**no vpnclient enable** コマンドを入力すると、Easy VPN サーバ（「ヘッドエンド」とも呼ばれる）として機能します。クライアントまたはサーバとしてのみ機能します。

例

次の例は、Easy VPN Remote 機能をイネーブルにする方法を示しています。

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

次の例は、Easy VPN Remote 機能をディセーブルにする方法を示しています。

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

vpnclient ipsec-over-tcp

TCP カプセル化 IPSec を使用するように、Easy VPN ハードウェア クライアントとして稼働している ASA 5505 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 ipsec-over-tcp** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no vpnclient ipsec-over-tcp

シンタックスの説明

port	（オプション）特定のポートを使用するように指定します。
tcp_port	（***port*** キーワードを指定した場合は必須）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

このコマンドでポート番号が指定されていない場合、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

次の表は、このコマンドを入力できるモードを示しています。

	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」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。

デフォルトでは、Easy VPN クライアントおよびサーバは、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）パケットをカプセル化します。特定のファイアウォール規則が設定されているような環境や、NAT デバイスおよび PAT デバイスでは、UDP が禁止されています。そのような環境で標準の Encapsulating Security Protocol（ESP、プロトコル 50）または Internet Key Exchange（IKE; インターネット キー エクスチェンジ、UDP 500）を使用するには、TCP パケット内の 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する必要があります。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、大きいパケットを外部インターフェイスに送信するようにします。

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

このコマンドは、カプセル化されたヘッダーから Don't Fragment（DF）ビットを消去します。DF ビットとは、パケットのフラグメント化が可能かどうかを判断する、IP ヘッダー内のビットです。このコマンドにより、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

次の例では、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いパケットを送信できるようにする方法を示しています。

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

次の例では、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いパケットを送信できるようにする方法を示しています。

```
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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

シンタックスの説明

mac_addr_1	ドット付き 16 進表記の MAC アドレスで、個々のユーザ認証を免除するデバイスのメーカーおよびシリアル番号を指定します。デバイスが複数の場合は、各 MAC アドレスをスペースで区切り、対応するネットワーク マスクを指定します。 MAC アドレスの最初の 6 文字はデバイスのメーカーを識別し、最後の 6 文字はシリアル番号です。最後の 24 ビットは、16 進形式での装置のシリアル番号です。
mac_mask_1	MAC アドレスに対応するネットワーク マスク。ネットワーク マスクと後続の MAC アドレスおよびネットワーク マスクのペアは、スペースで区切ります。

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

次の表は、このコマンドを入力できるモードを示しています。

	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 のみに適用されます。

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、個々の装置認証がイネーブルになっている場合でも認証しません。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 MAC マスクは、3 桁の 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、指定された MAC アドレスに対応します。すべてゼロの MAC マスクは対応する MAC アドレスがないことを示します。また、ffff.ff00.0000 という MAC マスクは同じメーカーで製造されたすべてのデバイスに対応します。

例

Cisco IP Phone のメーカー ID は 00036b です。したがって、次のコマンドでは、すべての Cisco IP Phone（今後追加する Cisco IP Phone も含む）が免除されます。

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

次の例では、特定の Cisco IP Phone が免除されるため、セキュリティは向上しますが、柔軟性は低下します。

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

vpnclient management

管理アクセス用に Easy VPN ハードウェア クライアントへの 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***

このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。この形式では、**split-tunnel-policy** コマンドと **split-tunnel-network-list** コマンドに従って、管理専用の IPSec トンネルが設定されます。

no vpnclient management

シンタックスの説明

clear	通常のルーティングを使用して、企業ネットワークから ASA 5505（Easy VPN クライアントとして稼働）の外部インターフェイスへの管理アクセスを可能にします。このオプションでは、管理トンネルは作成されません。 **（注）** クライアントとインターネットとの間で NAT デバイスが動作している場合に、このオプションを使用します。
ip_addr	ホストまたはネットワークの IP アドレス。Easy VPN ハードウェア クライアントからこの IP アドレスへの管理トンネルを構築します。この引数は **tunnel** キーワードと共に使用します。1 つまたは複数の IP アドレスおよび対応するネットワーク マスクを指定します。複数の場合は、各 IP アドレスをスペースで区切ります。
ip_mask	IP アドレスに対応するネットワーク マスク。ネットワーク マスクと後続の IP アドレスおよびネットワーク マスクのペアは、スペースで区切ります。
tunnel	企業ネットワークから ASA 5505（Easy VPN クライアントとして稼働）の外部インターフェイスへの管理アクセス専用の IPSec トンネルを自動的にセットアップします。

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　次の表は、このコマンドを入力できるモードを示しています。

	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」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。次の各コマンドが ASA 5505 コンフィギュレーションに含まれていることを前提としています。

vpnclient server コマンド（ピアを指定する）

vpnclient mode コマンド（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する）

次のいずれかのコマンド

- **vpnclient vpngroup** コマンド（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する）
- **vpnclient trustpoint** コマンド（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する）

vpnclient enable コマンド（ASA 5505 を Easy VPN クライアントとしてイネーブルにする）

（注）　NAT デバイス上でスタティック NAT マッピングを追加しないと、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　次の例は、ASA 5505 の外部インターフェイスからホスト（IP アドレス / マスクが 192.168.10.10 255.255.255.0 というの組み合せのホスト）への IPSec トンネルを生成する方法を示しています。

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

次の例は、IPSec を使用せずに、ASA 5505 の外部インターフェイスへの管理アクセスを可能にする方法を示しています。

```
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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no vpnclient mode

シンタックスの説明

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	Network Extension Mode（NEM; ネットワーク拡張モード）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

次の表は、このコマンドを入力できるモードを示しています。

	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」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。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。動作モードは、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）にアクセスできるかどうかによって決まります。Easy VPN クライアントにはデフォルトのモードがないので、接続を行う前に必ず動作モードを指定します。

- 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 Port Address Translation（PAT; ポート アドレス変換）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る）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アクセスすることはできません。
- NEM では、内部ネットワークおよび内部インターフェイス上のすべてのノードに、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。企業ネットワークからトンネル経由で内部ホストにアクセスできます。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の 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では、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な通知を設定します。

例

次の例は、クライアント モードで Easy VPN Remote 接続を設定する方法を示しています。

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

次の例は、NEM で Easy VPN Remote 接続を設定する方法を示しています。

```
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、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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient nem-st-autoconnect

no vpnclient nem-st-autoconnect

シンタックスの説明

このコマンドには、キーワードも引数もありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	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」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。

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により、ハードウェア クライアントは、VPN トンネルを介したリモート プライベート ネットワークに対して、ルーティング可能なネットワークを 1 つ提示できます。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装置は、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。トンネルがアップの状態になった後は、どちらの側からもデータ交換を開始できます。

（注） また、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があります。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されて持続します。

例

次の例は、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 接続を設定する方法を示しています。グループ ポリシー FirstGroup のネットワーク拡張モードは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

証明書マップで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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient server-certificate *certmap_name*

no vpnclient server-certificate

シンタックスの説明

certmap_name	受け入れ可能な Easy VPN サーバ証明書を特定するための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

デフォルトでは、Easy VPN サーバ証明書のフィルタリングはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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 のみに適用されます。

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 コマンドおよび crypto ca certificate chain コマンドを使用して定義します。

例

次の例は、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 接続を設定する方法を示しています。

```
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 ID 証明書を設定します。

vpnclient server

Easy VPN Remote 接続で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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no vpnclient server

シンタックスの説明

ip_primary_address	プライマリ Easy VPN（IPSec）サーバの IP アドレスまたは DSN 名。すべての ASA または VPN 3000 コンセントレータ シリーズが Easy VPN サーバとして機能できます。
ip_secondary_address_n	（オプション）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

次の表は、このコマンドを入力できるモードを示しています。

	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 のみに適用されます。

接続を確立する前に、サーバを設定しておく必要があります。**vpnclient server** コマンドは、IPv4 アドレス、名前データベース、または DNS 名をサポートし、この順序でアドレスを解決します。

サーバの IP アドレスまたはホスト名のいずれかを使用できます。

例

次の例では、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 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）の 3 台のサーバを指定しています。

```
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)#
```

次の例は、VPN クライアントに対し、IP アドレスが 10.10.10.15 のプライマリ IPSec サーバ、IP アドレスが 10.10.10.30 および 192.168.10.45 のセカンダリ サーバを設定する方法を示しています。

```
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 ID 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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no vpnclient trustpoint

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

	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 のみに適用されます。また、このコマンドが適用されるのは、デジタル証明書を使用している場合だけです。

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 によって発行された証明書に基づいて CA の識別情報を表し、また、装置の識別情報を表すことがあります。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 によって発行されるユーザ証明書の認証ポリシーを指定します。

例

次の例は、central という名前の ID 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 接続を設定する方法を示しています。

```
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 サブモードに入り、トラストポイント情報を管理します。

vpnclient username

Easy VPN Remote 接続用の VPN ユーザ名および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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no vpnclient username

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

	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 のみに適用されます。

XAUTH ユーザ名およびパスワードのパラメータは、セキュアな装置認証がディセーブルになっていて、サーバが XAUTH クレデンシャルを要求する場合に使用されます。セキュアな装置認証がイネーブルになっている場合、これらのパラメータは無視され、セキュリティ アプライアンスはユーザにユーザ名およびパスワードを要求します。

例

次の例は、XAUTH ユーザ名 testuser とパスワード ppurkm1 を使用するように Easy VPN Remote 接続を設定する方法を示しています。

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

vpnclient vpngroup

Easy VPN Remote 接続用の VPN トンネル グループ名および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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no vpnclient vpngroup

シンタックスの説明

group_name	Easy VPN サーバ上で設定されている VPN トンネル グループの名前を指定します。最大長は 64 文字で、スペースは使用できません。
preshared_key	Easy VPN サーバが認証に使用する 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稼働している 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 証明書の使用を試行します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。

パスワードとして事前共有キーを使用します。接続を確立する前に、サーバを設定しておく必要があります。

例

次の例は、VPN トンネル グループ名 TestGroup1 とパスワード my_key123 を使用するように、VPN トンネル グループとの Easy VPN Remote 接続を設定する方法を示しています。

```
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 ID 証明書を設定します。

wccp

容量を割り当て、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して、サービス グループに参加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 **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て、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**]]

シンタックスの説明

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数えます。サービスの最大数は、service-number 引数で指定したものも含め、256 個です。
service-number	動的サービス 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。動的サービス数は 0 ～ 254 までの範囲で、255 個です。***web-cache*** キーワードで指定する Web キャッシュ サービスを含め、256 個までに制限されます。
redirect-list	（オプション）このサービス グループにリダイレクトするトラフィックをコントロールするアクセス リストと共に使用します。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。
access-list	アクセス リストの名前を指定します。
group-list	（オプション）サービス グループに参加する Web キャッシュを決めるアクセス 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	（オプション）サービス グループから受信するメッセージを Message Digest 5（MD5）で認証することを指定します。認証でき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。最大長は 7 文字です。

デフォルト

このコマンドは、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

次の表は、このコマンドを入力できるモードを示しています。

	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

次の例では、WCCP のサービス グループへの参加をイネーブルにする方法を示します。

```
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 の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）を使用して、インターフェイスの入り口でパケットのリダイレクトをイネーブルにするには、**wccp redirect** コマンドを使用します。WCCP の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**

シンタックスの説明

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*** キーワードか、サービスの ID 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入ろうとしたときにリダイレクトすることを指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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

次の例では、Web キャッシュ サービスの内部インターフェイスで WCCP リダイレクションをイネーブルにする方法を示します。

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

関連コマンド

コマンド	説明
show wccp	WCCP の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 SSO 認証要求を行う SSO サーバの URL を指定するには、webvpn-sso-siteminder コンフィギュレーション モードで **web-agent-url** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

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）　SSO 認証にはこのコマンドが必要です。

シンタックスの説明

url	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 は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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-sso-siteminder 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

WebVPN だけで使用できるシングル サインオンのサポートは、ユーザが、異なるサーバ上の異なるセキュア サービスにユーザ名とパスワードを複数回入力することなくアクセスできるようにします。SSO サーバには、認証要求を処理する URL があります。

この 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。

例

webvpn-sso-siteminder コンフィギュレーション モードで入力された次の例では、認証 URL に http://www.example.com/webvpn を指定しています。

```
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	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
request-timeout	失敗した SSO 認証試行がタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
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 ユーザに対して表示される 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*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

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 です。
uppercase

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

次の表は、このコマンドを入力できるモードを示しています。

	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現されます。このパラメータの説明は、このマニュアルでは取り扱いません。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 で入手可能です。

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）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目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 を使用することをお勧めします。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のに便利な機能があります。

例

次の例では、タイトルを「Applications」に変更し、テキストの色を青に変更しています。

```
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 の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*}}

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

	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現されます。このパラメータの説明は、このマニュアルでは取り扱いません。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 で入手可能です。

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）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目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 を使用することをお勧めします。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のに便利な機能があります。

例

次の例では、Web Bookmarks のタイトルを「Corporate Web Bookmarks」に変更します。

```
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（グループ ポリシー モードおよびユーザ名モード）

この WebVPN モードに入るには、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 モードで入力したコマンドをすべて削除するには、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、設定する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 コマンドにより、WebVPN を超えたファイル、MAPI プロキシ、URL および TCP アプリケーションへのアクセスが定義されます。また、ACL およびフィルタリングするトラフィックのタイプも識別されます。

webvpn

no webvpn

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	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 モードから入って WebVPN モードを使用すると、WebVPN のグローバル設定値を設定できます。グループ ポリシー アトリビュート コンフィギュレーション モード、またはユーザ名アトリビュート コンフィギュレーション モードの **webvpn** コマンドは、webvpn コマンドで指定された設定を親コマンドで指定されたグループまたはユーザに適用します。つまり、この項で説明したように、グループ ポリシー モードまたはユーザ名モードから入って WebVPN モードを使用すると、特定のユーザ ポリシーまたはグループ 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。

特定のグループ ポリシーに対してグループ ポリシー アトリビュート モードで適用した webvpn アトリビュートは、デフォルトのグループ ポリシーで指定された webvpn アトリビュートを上書きします。ユーザ名アトリビュート モードで特定のユーザに対して適用した webvpn アトリビュートは、デフォルト グループ ポリシーおよび、当該ユーザが所属するグループ ポリシーの両方で webvpn アトリビュートを上書きします。基本的に、これらのコマンドを使用すると、デフォルトのグループまたは特定のグループ ポリシーから継承される設定を微調整できます。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** コマンドの説明を参照してください。

次の表は、webvpn グループ ポリシー アトリビュート モードおよびユーザ名アトリビュート モードで設定できるアトリビュートを示しています。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。

アトリビュート	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	適用する事前設定済みの 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するメッセージを指定します。
filter	WebVPN 接続で使用するアクセス 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 を超える 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する Web ページの URL を設定します。
html-content-filter	WebVPN セッションに対して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	セッションのアップデート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 ユーザに転送する TCP ポート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 Client のアトリビュートを設定します。
url-list	ユーザが WebVPN 経由でアクセスできるサーバおよび URL のリストを指定します。

例

次の例は、「FirstGroup」というグループ ポリシーで WebVPN モードに入る方法を示します。

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

次の例は、「test」というユーザ名で WebVPN モードに入る方法を示します。

```
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	config-group-policy モードに入ります。このモードでは、指定したグループ ポリシーのアトリビュートと値を設定したり、グループの webvpn アトリビュートを設定する webvpn モードに入ったりできます。
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	config-group-webvpn モードに入ります。このモードで、指定したグループに対する WebVPN アトリビュートを設定できます。

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*]

シンタックスの説明

local_ip	（オプション）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）に制限するために指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	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のものです。

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 および IP アドレスを表示できます。

例

次の例では、クライアントが Telnet セッションを通してセキュリティ アプライアンスにログインした場合の ***who*** コマンドの出力を示します。

```
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	Telnet アクセスをセキュリティ アプライアンス コンソールに追加し、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**}

シンタックスの説明

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、接続を許可します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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 コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用して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。TCP 検査を **service-policy** コマンドを使用して有効にします。

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 モードに入ります。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、縮小されたウィンドウ サイズの接続をすべてドロップします。

ウィンドウ サイズ メカニズムを使用すると、TCP は大きなウィンドウをアドバタイズした後、多すぎるデータを受信することなく、小さなウィンドウにアドバタイズできます。TCP の仕様では、「ウィンドウの縮小」は推奨されていません。この状態が検出されると、接続をドロップできます。

例

次の例では、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方法を示します。

```
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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、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。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、WINS サーバを別のグループ ポリシーから継承できます。サーバを継承し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

シンタックスの説明

none	WINS サーバにヌル値を設定して、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

次の表は、このコマンドを入力できるモードを示しています。

	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、既存の設定を上書きします。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 番目のコマンドが最初のコマンドを上書きします。したがって、y.y.y.y は唯一の WINS サーバになります。サーバを複数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

次の例では、FirstGroup という名前のグループ ポリシーに対して IP アドレス 10.10.10.15、10.10.10.30、および 10.10.10.45 で WINS サーバを設定する方法を示します。

```
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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	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のものです。

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** コマンドで識別します。コンテキストのコンフィギュレーションを削除する場合は、リモート サーバ（指定されている場合）からファイルを手作業で削除するか、システム実行スペースで **delete** コマンドを使用してフラッシュ メモリからファイルを消去します。

例

次の例では、スタートアップ コンフィギュレーションを消去します。

```
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 から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とマージします。
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	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write memory

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

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

シンタックスの説明

/noconfirm	**all** キーワードを使用するときに、確認プロンプトをなくします。
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、すべてのコンテキスト コンフィギュレーションとシステム コンフィギュレーションを保存します。

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

次の表は、このコマンドを入力できるモードを示しています。

	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** キーワードで、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は、メモリ内で現在実行されているコンフィギュレーションです。コマンドラインで行った変更がすべて含まれています。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場合は、リブートの間だけ保存されます。これは起動時に実行中のメモリにロードされるコンフィギュレーションです。シングル コンテキスト モード、およびマルチ コンテキスト モードの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）から別の場所に変更できます。マルチ コンテキスト モードの場合は、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の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の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上に配置できます。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 と HTTPS の URL を除き、**config-url** コマンドで指定し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。**write memory all** コマンドで各コンテキストを保存すると、次のメッセージが表示されます。

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

エラーが発生して、コンテキストを保存できないことがあります。次に、そのエラーについて説明します。

- メモリが不足しているためコンテキストを保存できない場合は、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コンテキストを保存できない場合は、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保存できない場合は、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か、コンテキストを削除している場合だけです。

- 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（HTTP サーバの場合など）のため保存できない場合は、他のメッセージの最後に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 have
  read-only config-urls:
  context ‘a’ , context ‘b’ , context ‘c’ .
  ```

- フラッシュ メモリのセクターが壊れているためコンテキストを保存できない場合は、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
  ```

システムは管理コンテキスト インターフェイスを使用して、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、**write memory** コマンド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

次の例では、スタートアップ コンフィギュレーションに実行コンフィギュレーションを保存します。

```
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。
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

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

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

シンタックスの説明

:filename	パスとファイル名を指定します。**tftp-server** コマンドですでにファイル名を設定している場合は、この引数はオプションです。 **tftp-server** コマンドとこのコマンドの両方でファイル名を指定すると、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扱い、***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 サーバがこのタイプの URL をサポートしていない場合は、代わりに **copy running-config tftp** コマンドを使用します。 **tftp-server** コマンドで 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。このアドレスが存在する場合は、**tftp-server** コマンドで設定したアドレスが上書きされます。 デフォルトのゲートウェイ インターフェイスはセキュリティが最高の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

次の表は、このコマンドを入力できるモードを示しています。

	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のものです。

使用上のガイドライン

実行コンフィギュレーションは、メモリ内で現在実行されているコンフィギュレーションです。コマンドラインで行った変更がすべて含まれています。

マルチ コンテキスト モードでこのコマンドを実行すると、現在のコンフィギュレーションのみ保存されます。1 回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。システムおよび各コンテキストについて、このコマンドを個別に入力する必要があります。**write net** コマンドは、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、システムは管理コンテキスト インターフェイスを使用して、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、**write memory** コマンド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。

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

例

次の例では、**tftp-server** コマンドに TFTP サーバとファイル名を設定しています。

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

次の例では、**write net** コマンドにサーバとファイル名を設定しています。**tftp-server** コマンドは入力されません。

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

次の例では、**write net** コマンドにサーバとファイル名を設定しています。**tftp-server** コマンドはディレクトリ名を示し、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 から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とマージします。
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	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	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のものです。

使用上のガイドライン

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装置の RAM に保存されているコンフィギュレーションを、スタンバイ装置の RAM に書き込みます。プライマリ装置とセカンダリ装置のコンフィギュレーションの情報が異なる場合は、**write standby** コマンドを使用します。このコマンドをアクティブ装置に入力します。

Active/Active 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** コマンドを入力すると、システム コンフィギュレーションおよびセキュリティ アプライアンス上のセキュリティ コンテキストのすべてのコンフィギュレーションはピア装置に書き込まれます。これは、スタンバイ状態にあるセキュリティ コンテキストのコンフィギュレーション情報を含みます。アクティブ状態のフェールオーバー グループ 1 を持つ装置のシステム実行スペースに、このコマンドを入力する必要があります。
- セキュリティ コンテキストに **write standby** コマンドを入力する場合、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。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 コンテキストに、このコマンドを入力する必要があります。

（注） **write standby** コマンドはコンフィギュレーションをピア装置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は保存されません。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のと同じ装置で **copy running-config startup-config** コマンドを使用します。コマンドはピア装置に複製され、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されます。

例

次の例では、現在の実行コンフィギュレーションをスタンバイ装置に書き込みます。

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

関連コマンド

コマンド	説明
failover reload-standby	スタンバイ装置を強制的にリブートします。

write terminal

端末に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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	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のものです。

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

次の例では、端末に実行コンフィギュレーションを書き込みます。

```
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 から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とマージします。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

zonelabs-integrity fail-close

セキュリティ アプライアンスが Zone Labs Integrity ファイアウォール サーバに接続できなかった場合に、VPN クライアントへの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 に接続できなかった場合に 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、サーバに障害が発生しても、VPN 接続が開いたままになります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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でも、セキュリティ アプライアンスはプライベート ネットワークに向かう VPN クライアント接続を必要に応じて確立します。また、既存の開いた接続も維持します。これにより、ファイアウォール サーバに障害が発生しても、企業の VPN 接続が中断されないようにします。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で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 サーバに接続できなくなってもクライアントの VPN 接続を維持す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

次の例では、Zone Labs Integrity ファイアウォール サーバが応答しない場合や、サーバとの接続が中断した場合に、VPN クライアントの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ことを指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイウォール 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 サーバの接続が中断した後も、リモート VPN クライアントからセキュリティ アプライアンスへの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 サーバとの接続が中断した場合に、VPN クライアントの接続を閉じる場合は、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

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトでは、セキュリティ アプライアンスが Zone Labs Integrity ファイアウォール サーバに接続できない場合や接続が中断した場合でも、リモート VPN 接続が開いたままになります。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	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でも、セキュリティ アプライアンスはプライベート ネットワークに向かう VPN クライアント接続を必要に応じて確立します。また、既存の開いた接続も維持します。これにより、ファイアウォール サーバに障害が発生しても、企業の VPN 接続が中断されないようにします。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で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 サーバに接続できなくなってもクライアントの VPN 接続を維持するデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドか、**no zonelabs-integrity fail-open** コマンドを使用します。

例

次の例では、Zone Labs Integrity ファイアウォール サーバに接続できなくなっても VPN クライアントの接続が開いたままになるデフォルト状態に戻します。

```
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 アプライアンスで VPN クライアント接続を閉じることを指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイウォール 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 アプライアンスが応答しない Zone Labs Integrity ファイアウォール サーバを到達不能と見なすまでの時間（秒単位）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値 10 秒に戻すには、引数を指定せずにこのコマンドの **no** 形式を使用します。

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

シンタックスの説明

timeout	セキュリティ アプライアンスが、応答しない Zone Labs Integrity ファイアウォール サーバを到達不能と見なすまでの秒数を指定します。5 ～ 20 秒に指定できます。

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

次の表は、このコマンドを入力できるモードを示しています。

	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した秒数待っても Zone Labs サーバから応答がないと、サーバを到達不能と見なします。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** コマンドを発行している場合は、セキュリティ アプライアンスが Zone Labs Integrity ファイアウォール サーバを到達不能と見なした時点で、VPN クライアントの接続が閉じられます。

例

次の例では、12 秒経過すると、アクティブな Zone Labs Intergity ファイアウォール 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ことを指定します。
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 アプライアンスで VPN クライアント接続を閉じることを指定します。
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 interface

Zone Labs Integrity ファイアウォール サーバと通信するセキュリティ アプライアンスの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 サーバとのインターフェイスをデフォルトのインターフェイスなしに戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

シンタックスの説明

interface	Zone Labs Integrity ファイアウォール サーバと通信するセキュリティ アプライアンスのインターフェイスを指定します。**nameif** コマンドで作成したインターフェイスの名前をよく使用します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバとのインターフェイスは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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

次の例では、IP アドレスが 10.0.0.5 ～ 10.0.0.7 の Zone Labs Intergity ファイアウォール サーバを 3 台設定します。さらに、ポート 300 で、また inside というインターフェイスで、サーバからの通信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。
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

セキュリティ アプライアンスが Zone Labs Integrity ファイアウォール サーバとの通信に使用する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。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*

シンタックスの説明

port	セキュリティ アプライアンスの Zone Labs Integrity ファイアウォール サーバ用のポートを指定します。
port_number	Zone Labs Integrity ファイアウォール サーバ用のポートの番号。10 ～ 10000 の範囲になります。

デフォルト

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

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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** コマンドで設定し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 サーバからの接続をリッスンします。

（注） セキュリティ アプライアンスの現在のリリースでは、ユーザ インターフェイスで Integrity サーバを 5 台まで設定できますが、同時にサポートできる Integrity サーバは 1 台です。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 サーバを設定してから、クライアント VPN セッションを再確立してください。

例

次の例では、IP アドレスが 10.0.0.5 の Zone Labs Integrity ファイアウォール サーバを設定します。さらに、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

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 Zone Labs Integrity ファイアウォール サーバを追加するには、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 Integrity ファイアウォール サーバの IP アドレスまたはホスト名を指定します。

実行コンフィギュレーションから Zone Labs Integrity ファイアウォール サーバを削除するには、引数を指定せずにこのコマンドの **no** 形式を使用します。

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

no zonelabs-integrity server-address

（注） セキュリティ アプライアンスのユーザ インターフェイスは、複数の Zone Labs Integrity ファイアウォール サーバを含む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、現在のリリースでは一度に 1 台のサーバにしか接続できません。

シンタックスの説明

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。ホスト名の指定方法については、**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。

コマンドのデフォルト設定

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

次の表は、このコマンドを入力できるモードを示しています。

	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、Zone Labs Integrity ファイアウォール サーバを 1 台だけ設定できます。設定したサーバに障害が発生した場合は、別のサーバを設定してからクライアントの VPN セッションを確立し直してください。

ホスト名でサーバを指定するには、まず **name** コマンドを使用して、Zone Labs サーバの名前を指定する必要があります。このとき、**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）　セキュリティ アプライアンスの現在のリリースでは、ユーザ インターフェイスで Integrity サーバを 5 台まで設定できますが、同時にサポートできる Integrity サーバは 1 台です。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 サーバを設定してから、クライアント VPN セッションを再確立してください。

例

次の例は、IP アドレス 10.0.0.5 に ZL-Integrity-Svr というサーバ名を割り当ててから、この名前を使用して Zone Labs Intergity ファイアウォール サーバを設定しています。

```
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 アプライアンスで VPN クライアント接続を閉じることを指定します。
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 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

Zone Labs Integrity ファイアウォール サーバが、SSL 証明書を取得するときに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。デフォルトのポート番号（80）に戻すには、引数を指定せずにこのコマンドの **no** 形式を使用します。

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

シンタックスの説明

cert-port-number	Zone Labs Integrity ファイアウォール サーバが SSL 証明書を要求するときに接続するセキュリティ アプライアンスのポートの番号を指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバがセキュリティ アプライアンスのポート 80 で SSL 証明書を要求するように設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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 接続では、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 接続を開始するときは、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ときに接続するポートを指定します。

例

次の例では、セキュリティ アプライアンスのポート 30 で、Zone Labs Integrity サーバからの SSL 証明書要求を受信するように設定します。

```
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、引数を指定せずにこのコマンドの **no** 形式を使用します。

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

シンタックスの説明

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、ディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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 接続では、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 接続を開始するときは、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オプションです。Zone Lab サーバ（SSL クライアント）証明書のセキュリティ アプライアンス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

次の例では、Zone Labs Integrity ファイアウォール 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。