CHAPTER 33

upgrade-mp ～ write terminal コマンド

upgrade-mp

メンテナンス パーティション ソフトウェアをアップグレードするには、**upgrade-mp** コマンドを使用します。

upgrade-mp {http[**s**]*://*[*user:password@*]*server*[*:port*]*/pathname* | **tftp**[*://server/pathname*]}

シンタックスの説明

tftp	TFTP（簡易ファイル転送プロトコル）サーバを指定します。サーバおよびパスを指定しない場合は、情報を求めるプロンプトが表示されます。デフォルト TFTP サーバを設定する手順については、**tftp-server** コマンドを参照してください。
http[**s**]	HTTP（S）サーバを指定します。
server	HTTP（S）または TFTP サーバの IP アドレスを指定します。
pathname	ソフトウェア イメージのパス名およびファイル名を指定します。
user	（任意）HTTP（S）ユーザ名を指定します。
password	（任意）ユーザ パスワードを指定します。
port	（任意）HTTP（S）ポートを指定します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

例

次に、TFTP サーバからイメージをダウンロードする例を示します。

```
hostname# upgrade-mp tftp://10.192.1.1/c6svc-mp.2-1-1.bin.gz
```

関連コマンド

コマンド	説明
copy	フラッシュメモリにファイルをコピーします。

url

CRL を取得するためにスタティック URL のリストをメンテナンスするには、crl configure 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 configure コンフィギュレーション モードには、crypto 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。FWSM はインデックスが 1 の URL を最初に試行します。
url	CRL の取得元の URL を指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

既存の URL を上書きすることはできません。既存の URL を置き換えるには、まず、このコマンドの **no** 形式を使用して削除する必要があります。

例

次に、crl configure コンフィギュレーション モードを開始し、CRL 取得用の URL リストを作成およびメンテナンスするために インデックス 3 を設定し、CRL の取得元となる URL https://example.com を設定する例を示します。

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

関連コマンド

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

url-block

フィルタリング サーバのフィルタリング判断を待機する間に Web サーバ応答で使用する URL バッファを管理するには、グローバル コンフィギュレーション モードで **url-block** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

url-block block *block_buffer_limit*

no url-block block *block_buffer_limit*

Websense の場合のみ：

url-block url-mempool *memory_pool_size*

no url-block url-mempool *memory_pool_siz*

シンタックスの説明

block *block_buffer_limit*	フィルタリング サーバのフィルタリング判断を待機する間 Web サーバ応答を保存するための HTTP 応答バッファを作成します。シングル コンテキスト モードでは、使用できる値は 0 ～ 128 です。1550 バイト ブロックの個数が指定されます。マルチ コンテキスト モードでは、使用できる値は 0 ～ 16 です。
url-mempool *memory_pool_size*	Websense URL フィルタリング専用です。キロバイト（KB）単位の URL バッファ メモリ プールのサイズです。シングル コンテキスト モードでは、使用できる値は 2 ～ 10240 です。2 ～ 10240 KB の URL バッファ メモリ プールを指定します。マルチ コンテキスト モードでは、使用できる値は 0 ～ 512 です。
url-size *long_url_size*	Websense URL フィルタリング専用です。最大許容 URL サイズ（KB 単位）です。使用できる値は 2、3、または 4 です。最大 URL サイズを 2 KB、3 KB、または 4 KB に指定します。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

Websense フィルタリング サーバに **url-block url-size** コマンドを使用すると、最大 4 KB の長い URL をフィルタリングできます。Websense および N2H2 フィルタリング サーバに **url-block block** コマンドを使用すると、FWSM が URL フィルタリング サーバからの応答を待機している間、Web クライアント要求への応答として Web サーバから着信したパケットがバッファリングされます。この方法を使用すると、Web クライアントのパフォーマンスがデフォルトの FWSM 動作（パケットを廃棄し、接続が許可された場合は Web サーバにパケットの再送信を要求する）よりも向上します。

url-block block コマンドを使用し、フィルタリング サーバによって接続が許可された場合、FWSM 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、バッファからブロックを削除します。フィルタリング サーバによって接続が拒否されると、FWSM は Web クライアントに拒否メッセージを送信し、HTTP 応答バッファからブロックを削除します。

フィルタリング サーバのフィルタリング判断を待機している間、Web サーバ応答のバッファリングに使用するブロック数を指定するには、**url-block block command** を使用します。

Websense フィルタリング サーバがフィルタリングする最大 URL 長および URL バッファに割り当てる最大メモリを指定するには、**url-block url-size** コマンドおよび **url-block url-mempool** コマンドを使用します。これらのコマンドを使用すると、1159 バイトを超える URL（最大 4096 バイト）を Websense サーバに送信することができます。**url-block url-size** コマンドは、1159 バイトを超える URL をバッファに格納してから、Websense サーバに（TCP パケット ストリームを介して）送信し、Websense サーバがこの URL へのアクセスを許可または拒否できるようにします。

例

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

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

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファ使用率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 サーバに転送します。
show url-block	N2H2 または Websense フィルタリング サーバからの応答を待機する間 URL をバッファに格納するための URL ブロックの情報を表示します。
url-cache	N2H2 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 サイズを設定します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

url-cache

N2H2 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 サイズを設定するには、グローバル コンフィギュレーション モードで **url-cache** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

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

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

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。すべてのユーザが N2H2 または Websense サーバ上で同じ URL フィルタリング ポリシーを共有する場合は、このモードを選択します。
kb	（任意）指定したサイズがキロバイト単位であることを示します。kb を追加することが習慣になっている場合に備え、FWSM はこのキーワードを便宜的に許可しています。
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 要求を開始す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。ユーザが N2H2 または Websense サーバ上で同じ URL フィルタリング ポリシーを共有しない場合は、このモードを選択します。
statistics	キャッシュ検索数およびヒット レートなど､その他の URL キャッシュ統計情報を表示するには、**statistics** オプションを使用します。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

url-cache コマンドを使用すると、Web サーバからの応答が N2H2 または Websense フィルタリング サービス サーバからの応答よりも早い場合に、この応答をバッファに格納するように設定できます。このコマンドにより、Web サーバの応答を 2 回ロードすることがなくなります。

URL キャッシングをイネーブルにしたり、キャッシュ サイズを設定したり、キャッシュ統計情報を表示するには、**url-cache** コマンドを使用します。

キャッシングを行うと、FWSM のメモリに URL へのアクセス権限が格納されます。ホストが接続を要求すると、FWSM は N2H2 または Websense サーバに要求を転送しないで、まず URL キャッシュ内で一致するアクセス権限を検索します。キャッシングをディセーブルにするには、**no url-cache** コマンドを使用します。

（注）　N2H2 または Websense サーバの設定を変更する場合は、**no url-cache** コマンドでキャッシュをディセーブルにしてから、**url-cache** コマンドでキャッシュを再度イネーブルにします。

URL キャッシュを使用しても、Websense プロトコル バージョン 1 の Websense アカウンティング ログは更新されません。Websense プロトコル バージョン 1 を使用している場合は、Websense にログの蓄積を許可して、Websense アカウンティング情報を表示できるようにします。目的のセキュリティ要求を満たす使用プロファイルを取得したら、**url-cache** をイネーブルにしてスループットを増大させます。**url-cache** コマンドの使用中は、Websense プロトコル バージョン 4 および N2H2 URL フィルタリングに対応するように、アカウンティング ログが更新されます。

例

次に、送信元またおよび宛先アドレスに基づくすべての発信 HTTP 接続をキャッシュに格納する例を示します。

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

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンドのステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに転送します。
show url-cache statistics	N2H2 または Websense フィルタリング サーバからの応答を待機する間に URL をバッファに格納するための URL キャッシュの情報を表示します。
url-cache	N2H2 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 サイズを設定します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

url-server

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

N2H2

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

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

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 *num_conns*	許可される最大接続数を制限します。
host *local_ip*	URL フィルタリング アプリケーションが稼働するサーバ
if_name	（任意）認証サーバが存在するネットワーク インターフェイス。指定しない場合、デフォルトは内部です。
port *number*	N2H2 サーバのポート。FWSM はこのポートで UDP 応答も待ち受けます。デフォルトのポート番号は 4005 です。
protocol	プロトコルを設定するには、**TCP** または **UDP** キーワードを使用します。デフォルトは TCP です。
timeout *seconds*	指定した次のサーバに FWSM が切り替わるまでの最大許容アイドル時間。デフォルトは 5 秒です。
vendor n2h2	URL フィルタリング サービス ベンダーが N2H2 であることを示します。

Websense

connections *num_conns*	許可される最大接続数を制限します。
if_name	認証サーバが存在するネットワーク インターフェイス。指定しない場合、デフォルトは内部です。
host *local_ip*	URL フィルタリング アプリケーションが稼働するサーバ
timeout *seconds*	指定した次のサーバに FWSM が切り替わるまでの最大許容アイドル時間。デフォルトは 5 秒です。
protocol	プロトコルを設定するには、**TCP** または **UDP** キーワードを使用します。デフォルトは TCP プロトコル、バージョン 1 です。
vendor websense	URL フィルタリング サービス ベンダーが Websense であることを示します。
version	プロトコル バージョン **1** または **4** を指定します。デフォルトは TCP プロトコル バージョン 1 です。TCP を設定するには、バージョン 1 またはバージョン 4 を使用します。UDP を設定するには、バージョン 4 のみを使用します。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

url-server コマンドは、N2H2 または Websense URL フィルタリング アプリケーションが稼働するサーバを指定します。URL サーバは 16 台まで指定できますが、一度に使用できるアプリケーションは 1 つ（N2H2 または Websense）のみです。FWSM の設定を変更しても、アプリケーション サーバの設定は更新されません。アプリケーション サーバの設定は、ベンダーの指示に従って、個別に行う必要があります。

url-server コマンドは、HTTPS および FTP（ファイル転送プロトコル）に **filter** コマンドを発行する前に設定する必要があります。サーバ リストからすべての URL サーバを削除すると、URL フィルタリングに関連するすべての **filter** コマンドも削除されます。

サーバを指定したら、**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。

URL をフィルタリングする手順は、次のとおりです。

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

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

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

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

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

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

http://www.n2h2.com

（注）　N2H2 社は、2003 年 10 月に Secure Computing 社に買収されました。

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

http://www.websense.com/

例

次に、N2H2 を使用した場合に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTP 接続をフィルタリングする例を示します。

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

次に、Websense を使用した場合に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTP 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) 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 サーバに転送します。
show url-block	N2H2 または Websense フィルタリング サーバからの応答を待機する間に URL をバッファに格納するための URL キャッシュの情報を表示します。
url-cache	N2H2 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 サイズを設定します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

user-authentication

ユーザ認証をイネーブルにするには、グループポリシー コンフィギュレーション モードで **user-authentication enable** コマンドを使用します。ユーザ認証をディセーブルにするには、**user-authentication disable** コマンドを使用します。実行コンフィギュレーションからユーザ認証属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーからユーザ認証に関する値を継承できます。

ユーザ認証がイネーブルな場合、ハードウェア クライアントの背後にいる各ユーザは、トンネルを介してネットワークにアクセスすることを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

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

各ユーザは、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 FWSM でユーザ認証が必要な場合は、すべてのバックアップ サーバにもユーザ認証を設定する必要があります。

例

次に、グループ ポリシー [FirstGroup] のユーザ認証をイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を行わなくても IP Phone を接続できるようにします。Secure Unit Authentication は引き続き有効です。
leap-bypass	ユーザ認証の前に（ユーザ認証がイネーブルな場合）、VPN（バーチャル プライベート ネットワーク）クライアントの背後にある無線デバイスから送信された LEAP パケットが VPN トンネルを通れるようにします。このようにすると、シスコ製無線アクセス 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。その後、ユーザ認証ごとに再認証します。
secure-unit-authentication	クライアントがトンネルを開始するたびに、ユーザ名およびパスワードを使用して認証するように VPN クライアントに要求して、セキュリティを高めます。
user-authentication-idle-timeout	ユーザごとにアイドル タイムアウトを設定します。アイドル タイムアウト期間内にユーザ接続上で通信アクティビティがなかった場合、FWSM 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あるユーザごとにアイドル 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。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。

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 タイムアウト期間の分数を指定します。有効範囲は 1 ～ 35791394 分です。
none	アイドル タイムアウト期間を無制限に許可します。アイドル タイムアウトにヌル値を設定し、アイドル タイムアウトを禁止します。デフォルト グループ ポリシーまたは指定されたグループ ポリシーからのユーザ認証アイドル タイムアウト値の継承を禁止します。

デフォルト

30 分

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このオプションを使用すると、別のグループ ポリシーからアイドル タイムアウト値を継承できます。アイドル タイムアウト値の継承を禁止するには、**user-authentication-idle-timeout none** コマンドを使用します。

アイドル タイムアウト期間内にハードウェア クライアントの背後にあるユーザによる通信アクティビティがなかった場合、FWSM は接続を終了します。

最小値は 1 分、デフォルトは 30 分、最大値は 10,080 分です。

例

次に、グループ ポリシー [FirstGroup] のアイドル タイムアウト値を 45 分に設定する例を示します。

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

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザが、接続前に FWSM に対して自身を識別するように要求します。

username

FWSM 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** コマンドを使用します。ユーザを削除するには、削除するユーザ名を使用して、このコマンドの **no** 形式を使用します。ユーザ名をすべて削除するには、ユーザ名を付加しないで、このコマンドの **no** 形式を使用します。

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

no username [*name*]

シンタックスの説明

encrypted	パスワードが暗号化されていることを示します。**username** コマンドでパスワードを定義すると、FWSM は、セキュリティ向上のため、そのパスワードを暗号化して設定ファイルに保存します。**show running-config** コマンドを入力したとき、**username** コマンドによって表示されるのは、実際のパスワードではなく、暗号化されたパスワードと、その後に続く **encrypted** キーワードです。たとえば、「test」というパスワードを入力した場合、**show running-config** コマンドの出力は次のようになります。 `username pat password rvEdRh0xPC8bel7s encrypted` **encrypted** キーワードを CLI に実際に入力するのは、設定を別の FWSM にカットアンドペーストして同じパスワードを使用する場合だけです。
name	4 ～ 15 文字の文字列としてユーザ名を指定します。
nopassword	このユーザにはパスワードが不要なことを示します。
password *password*	パスワードとして、3 ～ 16 文字までの長さの文字列を設定します。
privilege *priv_level*	このユーザの権限レベルを 0 ～ 15（値が大きいほど権限レベルが高い）に設定します。デフォルトの権限レベルは 2 です。この権限レベルは、コマンド許可に使用します。

デフォルト

デフォルトの特権レベルは 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

login コマンドは、このデータベースを使用して認証します。

CLI にはアクセスできるが、権限モードには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、コマンド許可をイネーブルにする必要があります。詳細については、**aaa authorization** コマンドの項を参照してください。コマンド許可がイネーブルになっていない場合でも、権限レベルが 2 以上であれば（2 がデフォルト）、ユーザは各自のパスワードを使用して CLI から特権 EXEC モード（およびすべてのコマンド）にアクセスできます。あるいは、AAA 認証を使用して、ユーザが **login** コマンドを実行できないようにするか、すべてのローカル ユーザをレベル 1 に設定し、**enable** パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御できるようにすることもできます。

デフォルトでは、このコマンドを使用して追加された VPN（バーチャル プライベート ネットワーク）ユーザには、属性またはグループ ポリシーが関連付けられていません。**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

次に、ユーザ名 anyuser に、暗号化されたパスワード 12345678 および権限レベル 12 を設定する例を示します。

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

関連コマンド

コマンド	説明
clear config username	特定のユーザまたはすべてのユーザの設定を消去します。
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	ユーザ名属性モードを開始し、特定のユーザの AVP を設定できるようにします。

username attributes

ユーザ名属性モードを開始するには、ユーザ名コンフィギュレーション モードで **username attributes** コマンドを使用します。特定のユーザの属性をすべて削除するには、ユーザ名を付加して、このコマンドの **no** 形式を使用します。全ユーザの属性をすべて削除するには、ユーザ名を付加しないで、このコマンドの **no** 形式を使用します。属性モードでは、指定されたユーザの AVP 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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

内部ユーザ認証データベースは、username コマンドで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使用して認証します。

属性モードにおけるこのコマンドの構文には、一般に次の特徴があります。

- **no** 形式は、実行コンフィギュレーションから属性を削除します。
- **none** キーワードも、実行コンフィギュレーションから属性を削除しますが、そのためには属性をヌル値に設定して、継承を禁止します。
- ブール属性には、イネーブル化およびディセーブル化された設定用の明示的な構文があります。

例

次に、ユーザ anyuser に対してユーザ名属性コンフィギュレーション モードを開始する例を示します。

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

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースを消去します。
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	FWSM データベースにユーザを追加します。

virtual http

仮想 HTTP サーバを設定するには、グローバル コンフィギュレーション モードで **virtual http** コマンドを使用します。仮想サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。FWSM 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、FWSM および 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、FWSM での認証に使用したのと同じユーザ名およびパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名およびパスワードが別に要求されることはありません。

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

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

シンタックスの説明

ip_address	FWSM に仮想 HTTP サーバの IP アドレスを設定します。このアドレスは FWSM にルーティングされる未使用アドレスである必要があります。たとえば、外部にアクセスするときに内部アドレスに NAT（ネットワーク アドレス変換）を実行し、仮想 HTTP サーバに外部からアクセスする場合は、仮想 HTTP サーバ アドレスにグローバル NAT アドレスを 1 つ使用します。
warning	（任意）HTTP 接続を FWSM 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。このキーワードを適用できるのは、リダイレクトを自動実行できないテキストベース ブラウザのみです。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

HTTP 認証をイネーブルにすると（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、FWSM は AAA（認証、認可、アカウンティング）サーバによる認証が可能となるように、各ユーザにユーザ名およびパスワードを求めるプロンプトを表示します。AAA サーバがユーザを認証すると、HTTP サーバとの接続が継続的に許可されます。ただし、AAA サーバのユーザ名およびパスワードは HTTP パケットに含まれたままです。パケットにユーザ名およびパスワードがすでに含まれているため、HTTP サーバに独自の認証メカニズムがある場合、ユーザ名およびパスワードを求めるプロンプトは再表示されません。AAA サーバと HTTP サーバでユーザ名およびパスワードが異なる場合は、HTTP 認証に失敗します。

HTTP サーバが個別にユーザにプロンプトを表示できるようにするには、**virtual http** コマンドを使用して、FWSM 上で仮想 HTTP サーバをイネーブルにします。このコマンドは、AAA 認証が必要なすべての HTTP 接続を FWSM 上の仮想 HTTP サーバにリダイレクトします。FWSM は、AAA サーバのユーザ名およびパスワードを求めるプロンプトを表示します。AAA サーバがユーザを認証すると、FWSM 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パケットに含まれません。HTTP パケットにユーザ名およびパスワードが含まれないため、HTTP サーバは HTTP サーバのユーザ名およびパスワードをユーザに個別に要求します。

注意　**virtual http** コマンドを使用する場合は、**timeout uauth** コマンドの期間を 0 秒に設定しないでください。このように設定すると、実際の Web サーバとの HTTP 接続が確立されなくなります。

例

次に、AAA 認証とともに仮想 HTTP をイネーブルにする例を示します。

```
hostname(config)# 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
clear configure virtual	コンフィギュレーションから **virtual** コマンドのステートメントを削除します。
show running-config virtual	FWSM 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 キャッシュ内の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	認証が必要なその他の接続タイプを開始する前に、FWSM に仮想 Telnet サーバを設定して、ユーザが FWSM で認証できるようにします。

virtual telnet

FWSM に仮想 Telnet サーバを設定するには、グローバル コンフィギュレーション モードで **virtual telnet** コマンドを使用します。仮想 Telnet 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	FWSM に仮想 Telnet サーバの IP アドレスを設定します。このアドレスは FWSM にルーティングされる未使用アドレスである必要があります。たとえば、外部にアクセスするときに内部アドレスに NAT（ネットワーク アドレス変換）を実行し、仮想 Telnet サーバに外部からアクセスする場合は、仮想 Telnet サーバ アドレスにグローバル NAT アドレスを 1 つ使用します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

FWSM が認証プロンプトを表示しない、その他のトラフィック タイプの認証が必要な場合は、仮想 Telnet サーバを使用してユーザを認証しなければならないことがあります。

任意のプロトコルまたはサービスに対してネットワーク アクセス認証を設定できますが（**aaa authentication match** または **aaa authentication include** コマンドを参照）、直接認証できるのは HTTP、Telnet、または FTP（ファイル転送プロトコル）の場合のみです。ユーザは認証が必要なその他のトラフィックが許可される前に、まずこれらのサービスのいずれかを使用して認証する必要があります。HTTP、Telnet、または FTP トラフィックの FWSM の通過を禁止し、その他のトラフィック タイプを認証する必要がある場合は、仮想 Telnet を設定することができます。ユーザは FWSM に設定された IP アドレスに Telnet 接続し、FWSM は Telnet プロンプトを表示します。

認証されていないユーザが仮想 Telnet IP アドレスに接続した場合、このユーザはユーザ名およびパスワードを要求され、その後 AAA サーバによって認証されます。認証されたユーザには、メッセージ [Authentication Successful] 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ます。

例

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

```
hostname(config)# 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** コマンドのステートメントを削除します。
show running-config virtual	FWSM 仮想サーバの IP アドレスを表示します。
virtual http	FWSM 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、FWSM および 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、FWSM での認証に使用したのと同じユーザ名およびパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名およびパスワードが別に要求されることはありません。

vpn-access-hours

設定された時間範囲ポリシーにグループ ポリシーを対応付けるには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-access-hours** コマンドを使用します。実行コンフィギュレーションからこの属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーから時間範囲値を継承できます。値の継承を禁止するには、**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 アクセス時間をヌル値に設定して、時間範囲ポリシーを禁止します。デフォルト グループ ポリシーまたは指定されたグループ ポリシーからの値の継承を禁止します。
time-range	設定された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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

例

次に、時間範囲ポリシー 824 にグループ ポリシー FirstGroup を関連付ける例を示します。

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

関連コマンド

コマンド	説明
time-range	開始日や終了日を含めて、ネットワークにアクセスする曜日および時刻を設定します。

vpn-addr-assign

リモート アクセス クライアントに IP アドレスを割り当てる方式を指定するには、グローバル コンフィギュレーション モードで **vpn-addr-assign** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。FWSM から設定済みの VPN（バーチャル プライベート ネットワーク）アドレス割り当て方式をすべて削除するには、引数を指定しないで、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、認可、アカウンティング）認証サーバから IP アドレスを取得します。
dhcp	DHCP を介して 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て、トンネル グループに対応付けます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

DHCP を選択した場合は、**dhcp-network-scope** コマンドを使用して、DHCP サーバで使用できる IP アドレス範囲も定義する必要があります。

local を選択した場合は、**ip-local-pool** コマンドを使用して、使用する IP アドレス範囲も定義する必要があります。その後、**vpn-framed-ip-address** および **vpn-framed-netmask** コマンドを使用して、IP アドレスおよびネットマスクを各ユーザに割り当てます。

AAA を選択した場合は、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

次に、アドレス割り当て方式として DHCP を設定する例を示します。

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

関連コマンド

コマンド	説明
dhcp-network-scope	グループ ポリシーのユーザにアドレスを割り当てるために FWSM の DHCP サーバが使用する IP アドレス範囲を指定します。
ip-local-pool	ローカル IP アドレス プールを作成します。
vpn-framed-ip-address	特定のユーザに割り当てる IP アドレスを指定します。
vpn-framed-ip-netmask	特定のユーザに割り当てるネットマスクを指定します。

vpn-filter

VPN（バーチャル プライベート ネットワーク）接続に使用するアクセス リストの名前を指定するには、グループ ポリシー モード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されたヌル値を含めて、アクセス 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、別のグループ ポリシーから値を継承できます。値の継承を禁止するには、**vpn-filter none** コマンドを使用します。

現在のユーザまたはグループ ポリシーに対応したさまざまなトラフィック タイプを許可または禁止するように、アクセス リストを設定します。その後、**vpn-filter** コマンドを使用して、設定したアクセス リストを適用します。

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、アクセス リストを禁止します。別の グループ ポリシーからアクセス リストを継承できなくなります。
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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

WebVPN は、**vpn-filter** コマンドで定義されたアクセス リストを使用しません。

例

次に、グループ ポリシー FirstGroup のアクセス リスト acl_vpn を呼び出すフィルタを設定する例を示します。

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

関連コマンド

コマンド	説明
access-list	アクセス リストを作成します。

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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドのサポートが追加されました。

例

次に、ユーザ anyuser に IP アドレス 10.92.166.7 を設定する例を示します。

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

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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

例

次に、ユーザ anyuser にサブネット マスク 255.255.255. 254 を設定する例を示します。

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

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

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

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

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

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（バーチャル プライベート ネットワーク）ユーザにグループ ポリシーは対応付けられていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
ユーザ名属性コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

特定のユーザのグループ ポリシー内の属性値を上書きするには、ユーザ名モードで属性値を設定します（この属性をユーザ名モードで使用できる場合）。

例

次に、グループ ポリシー FirstGroup の属性を使用するように、ユーザ anyuser を設定する例を示します。

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

関連コマンド

コマンド	説明
group-policy	FWSM データベースにグループ ポリシーを追加します。
group-policy attributes	グループポリシー属性モードを開始し、グループ ポリシーの AVP を設定できるようにします。
username	FWSM データベースにユーザを追加します。
username attributes	ユーザ名属性モードを開始し、特定のユーザの AVP を設定できるようにします。

vpn-idle-timeout

ユーザ タイムアウト期間を設定するには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを使用します。この期間内に接続上で通信アクティビティがなかった場合、FWSM は接続を終了します。

実行コンフィギュレーションからこの属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーからタイムアウト値を継承できます。値の継承を禁止するには、**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	タイムアウト期間の分数を指定します。1 ～ 35791394 の整数を使用します。
none	アイドル タイムアウト期間を無制限に許可します。アイドル タイムアウトにヌル値を設定し、アイドル タイムアウトを禁止します。デフォルト グループ ポリシーまたは指定されたグループ ポリシーからの値の継承を禁止します。

デフォルト

30 分

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

例

次に、グループ ポリシー [FirstGroup] の VPN アイドル タイムアウトを 15 分に設定する例を示します。

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

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-session-timeout	VPN 接続の最大許容時間を設定します。この期間が終了すると、FWSM は接続を終了します。

vpn-sessiondb logoff

すべての VPN（バーチャル プライベート ネットワーク）セッションまたは選択された 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** | **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*	インデックス番号を使用して、単一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 アドレスに対応する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*	指定したユーザ名に対応する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に対応するセッションをログオフします。指定できるプロトコルは、次のとおりです。 IKE　POP3S IMAP4S　SMTPS IPSec　userHTTPS IPSecLAN2LAN　vcaLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP
remote	すべてのリモートアクセス セッションをログオフします。
tunnel-group *groupname*	指定したトンネル グループに対応するセッションをログオフします。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドのサポートが追加されました。

例

次に、すべてのリモートアクセス セッションをログオフする例を示します。

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

次に、すべての IPSec セッションをログオフする例を示します。

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

vpn-sessiondb max-session-limit

VPN（バーチャル プライベート ネットワーク）セッションを FWSM の許容値よりも小さな値に制限するには、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。セッション制限を削除するには、このコマンドの **no** 形式を使用します。現在の設定を上書きするには、このコマンドを再度実行します。

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

no vpn-sessiondb max-session-limit

シンタックスの説明

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

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、WebVPN を含めて、VPN セッションのすべてのタイプに適用されます。

例

次に、VPN セッションの最大数を 450 に設定する例を示します。

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

vpn-session-timeout

VPN（バーチャル プライベート ネットワーク）接続で許可され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、FWSM は接続を終了します。

実行コンフィギュレーションからこの属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーからタイムアウト値を継承できます。値の継承を禁止するには、**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	タイムアウト期間の分数を指定します。1 ～ 35791394 の整数を使用します。
none	セッション タイムアウト期間を無制限に許可します。セッション タイムアウトにヌル値を設定し、セッション タイムアウトを禁止します。デフォルト グループ ポリシーまたは指定されたグループ ポリシーからの値の継承を禁止します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

例

次に、グループ ポリシー FirstGroup の VPN セッション タイムアウト値を 180 分に設定する例を示します。

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

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-idle-timeout	ユーザ タイムアウト期間を設定します。この期間内に接続上で通信アクティビティがなかった場合、FWSM は接続を終了します。

vpn-simultaneous-logins

ユーザに許可される同時ログイン数を設定するには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用します。実行コンフィギュレーションからこの属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーから値を継承できます。ログインをディセーブルにして、ユーザ 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 の値

デフォルト

デフォルトの同時ログイン数は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

次に、グループ ポリシー FirstGroup の最大同時ログイン数を 4 に設定する例を示します。

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

vpn-tunnel-protocol

VPN（バーチャル プライベート ネットワーク）のトンネル タイプ（IPSec）を設定するには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-tunnel-protocol** コマンドを使用します。実行コンフィギュレーションからこの属性を削除するには、このコマンドの **no** 形式を使用します。

vpn-tunnel-protocol IPSec

no vpn-tunnel-protocol [IPSec]

シンタックスの説明

IPSec	2 つのピア間で IPSec トンネルをネゴシエートします（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）。認証、暗号化、カプセル化、および鍵の管理を行うセキュリティ アソシエーションを作成します。
webvpn	HTTPS 対応 Web ブラウザを介してリモート 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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、1 つまたは複数のトンネリング モードを設定する場合に使用します。ユーザが VPN トンネルを介して接続するには、少なくとも 1 つのトンネリング モードを設定する必要があります。

例

次に、グループ ポリシー [FirstGroup] に IPSec トンネリング モードを設定する例を示します。

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

who

FWSM 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	（任意）特定の内部 IP アドレスまたはネットワーク アドレスのみを表示するように指定します（IPv4 または IPv6）。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

who コマンドを使用すると、現在 FWSM 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

次に、クライアントが Telnet セッションを介して FWSM にログインしている場合の ***who*** コマンドの出力例を示します。

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

関連コマンド

コマンド	説明
kill	Telnet セッションを終了します。
telnet	FWSM コンソールへの Telnet アクセスを追加し、アイドル タイムアウトを設定します。

wins-server

プライマリおよびセカンダリ WINS サーバの IP アドレスを設定するには、グループポリシー コンフィギュレーション モードで **wins-server** コマンドを使用します。実行コンフィギュレーションからこの属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーから WINS サーバを継承できます。サーバの継承を禁止するには、**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-servers をヌル値に設定して、WINS サーバを禁止します。デフォルト グループ ポリシーまたは指定されたグループ ポリシーからの値の継承を禁止します。
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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

wins-server コマンドを発行するたびに、既存設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定してから、WINS サーバ y.y.y.y を設定すると、2 番めのコマンドによって最初の設定が上書きされ、y.y.y.y が単独の WINS サーバになります。複数のサーバがある場合も同様です。設定済みのサーバを上書きしないで 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 アドレスをコマンドに含めます。

例

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

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

write erase

スタートアップ コンフィギュレーションを消去するには、特権 EXEC モードで **write erase** コマンドを使用します。実行コンフィギュレーションは影響を受けません。

write erase

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

セキュリティ コンテキスト内では、このコマンドがサポートされません。コンテキスト スタートアップ コンフィギュレーションを識別するには、システム コンフィギュレーション内で **config-url** コマンドを使用します。コンテキスト コンフィギュレーションを削除する場合は、リモート サーバ（指定されている場合）からファイルを手動で削除するか、または システム実行スペース内で **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削除します。

例

次に、スタートアップ コンフィギュレーションを消去する例を示します。

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

関連コマンド

コマンド	説明
configure net	指定された TFTP URL のコンフィギュレーション ファイルに実行コンフィギュレーションをマージします。
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

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

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

シンタックスの説明

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

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。
3.1(1)	すべてのコンテキスト コンフィギュレーションを保存するには、**all** キーワードを使用します。

使用上のガイドライン

実行コンフィギュレーションは、コマンドラインで実行された変更を含む、メモリ内で現在稼働中の設定です。スタートアップ コンフィギュレーションは、起動時に稼働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。ここに保存された変更のみが、再起動後も維持されます。シングル コンテキスト モードのスタートアップ コンフィギュレーション、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は、非表示ファイルです。マルチ コンテキスト モードの場合、コンテキスト 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内の **config-url** コマンドで指定された場所に配置されます。

マルチ コンテキスト モードでは、各コンテキストで **write memory** コマンドを入力することで、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 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 スタートアップ コンフィギュレーションは外部サーバに配置できます。この場合、FWSM はコンフィギュレーションを **config-url** コマンドで指定されたサーバに保存します。ただし、HTTP および HTTPS URL の場合は、例外的に、サーバにコンフィギュレーションを保存できません。FWSM は、**write memory all** コマンドで各コンテキストを保存した後、次のメッセージを表示します。

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

エラーのため、コンテキストが保存されない場合があります。次のエラー情報を確認してください。

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

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

- リモートの宛先が到達不能のためコンテキストが保存されない場合は、次のメッセージが表示されます。

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

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

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

  コンテキストは、他のユーザが設定を保存中か、コンテキストを削除中の場合のみ、ロックされます。

- 起動コンフィギュレーションが（HTTP サーバ上で）読み取り専用のためコンテキストが保存されない場合は、他のすべてのメッセージの後に次のメッセージ レポートが出力されます。

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

- フラッシュ メモリ内に不良セクタが検出されたためコンテキストが保存されない場合は、次のメッセージが表示されます。

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

コンテキスト 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場合は管理コンテキスト インターフェイスが使用されるため、**write memory** コマンドでも管理コンテキスト インターフェイスを使用します。ただし、**write net** コマンドでは、コンテキスト インターフェイスを使用して、コンフィギュレーションを TFTP（簡易ファイル転送プロトコル）サーバに書き込みます。

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

例

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

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

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

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
configure memory	スタートアップ コンフィギュレーションに実行コンフィギュレーションをマージします。
config-url	コンテキスト設定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	TFTP サーバに実行コンフィギュレーションをコピーします。

write net

実行コンフィギュレーションを TFTP（簡易ファイル転送プロトコル）サーバに保存するには、特権 EXEC モードで **write net** コマンドを使用します。

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

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** コマンドを使用してファイル名が設定されている場合は、この引数を省略できます。 このコマンドでファイル名を指定し、**tftp-server** コマンドで名前を指定した場合、FWSM は **tftp-server** コマンドのファイル名をディレクトリとして処理し、***write net*** コマンドのファイル名をこのディレクトリ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、パスおよび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なく、絶対パスであることを示します。このファイルに対して生成された URL には、ファイル名パスの前に二重スラッシュ（//）が付加されます。必要なファイルが tftpboot ディレクトリ内にある場合は、ファイル名パスに tftpboot ディレクトリ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、**copy running-config tftp** コマンドを使用します。 **tftp-server** コマンドを使用して TFTP サーバ アドレスを指定した場合は、コロン（:）を入力し、そのあとにファイル名のみを入力します。
server:	TFTP サーバの IP アドレスまたは名前を設定します。このアドレスは、**tftp-server** コマンドで設定されたアドレス（存在する場合）を上書きします。 デフォルト ゲートウェイ インターフェイスは、セキュリティが最大のインターフェイスです。**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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

実行コンフィギュレーションは、コマンドラインで実行された変更を含む、メモリ内で現在稼働中の設定です。

マルチ コンテキスト モードの場合、このコマンドは現在のコンフィギュレーションのみを保存します。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。システムごと、およびコンテキストごとに、このコマンドを個別に入力する必要があります。**write net** コマンドでは、コンテキスト インターフェイスを使用して、コンフィギュレーションを TFTP（簡易ファイル転送プロトコル）サーバに書き込みます。ただし、**write memory** コマンドでは、システムがコンテキスト 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場合に管理コンテキスト インターフェイスを使用するため、スタートアップ コンフィギュレーションを保存するには、管理コンテキスト インターフェイスを使用します。

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

例

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

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

次に、**write net** コマンドでサーバおよびファイル名を設定する例を示します。**tftp-server** コマンドは読み込まれません。

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

次に、**write net** コマンドでサーバおよびファイル名を設定する例を示します。**tftp-server** コマンドはディレクトリ名を設定します。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	指定された TFTP URL のコンフィギュレーション ファイルに実行コンフィギュレーションをマージします。
copy running-config tftp	TFTP サーバに実行コンフィギュレーションをコピーします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	その他のコマンドで使用する 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

FWSM またはコンテキスト 実行コンフィギュレーションをフェールオーバー スタンバイ装置にコピーするには、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、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

アクティブ / スタンバイ フェールオーバーの場合、**write standby** コマンドはアクティブ フェールオーバー装置の RAM（ランダム アクセス メモリ）に格納された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。**write standby** コマンドは、プライマリおよびセカンダリ装置の設定情報が異なる場合に使用してください。このコマンドは、アクティブな装置上で入力します。

アクティブ / アクティブ フェールオーバーの場合、**write standby** コマンドの動作は次のとおりです。

- システム実行スペース内で **write standby** コマンドを入力した場合、システム コンフィギュレーションおよび FWSM のすべてのセキュリティ コンテキストのコンフィギュレーションがピア装置に書き込まれます。スタンバイ状態のセキュリティ コンテキストの設定情報も書き込まれます。このコマンドは、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内で入力する必要があります。
- **write standby** コマンドをセキュリティ コンテキスト内で入力した場合は、セキュリティ コンテキストに対応するコンフィギュレーションのみがピア装置に書き込まれます。このコマンドは、セキュリティ コンテキストがアクティブ状態である装置の、セキュリティ コンテキスト内で入力する必要があります。

（注）　**write standby** コマンドは、ピア装置の実行コンフィギュレーションにコンフィギュレーションを複製します。コンフィギュレーションはスタートアップ コンフィギュレーションに保存されません。コンフィギュレーションの変更をスタートアップ コンフィギュレーションに保存するには、**write standby** コマンドで入力したのと同じ装置上で、**copy running-config startup-config** コマンドを使用します。コマンドがピア装置に複製されて、コンフィギュレーションがスタートアップ コンフィギュレーションに保存されます。

例

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

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

関連コマンド

コマンド	説明
failover reload-standby	スタンバイ装置を強制的に再起動します。

write terminal

端末の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、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

次に、実行コンフィギュレーションを端末に表示する例を示します。

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

関連コマンド

コマンド	説明
configure net	指定された TFTP URL のコンフィギュレーション ファイルに実行コンフィギュレーションをマージします。
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。