CHAPTER 12

mfib forwarding コマンド～ mus server コマンド

mfib forwarding

インターフェイスで MFIB 転送を再びイネーブルにするには、インターフェイス コンフィギュレーション モードで **mfib forwarding** を使用します。インターフェイスで MFIB 転送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。

mfib forwarding

no mfib forwarding

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

multicast-routing コマンドは、デフォルトではすべてのインターフェイスの MFIB 転送をイネーブルにします

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

マルチキャスト ルーティングをイネーブルにすると、デフォルトではすべてのインターフェイスで MFIB 転送がイネーブルになります。特定のインターフェイスで MFIB 転送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。実行コンフィギュレーションには、このコマンドの **no** 形式だけが表示されます。

インターフェイスで MFIB 転送がディセーブルになっている場合、特に他の方法を設定しない限り、そのインターフェイスはマルチキャスト パケットを受け付けません。MFIB 転送がディセーブルになっていると、IGMP パケットも阻止されます。

例

次に、指定されたインターフェイスで MFIB 転送をディセーブルにする例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/0
ciscoasa(config-if)# no mfib forwarding
```

関連コマンド

コマンド	説明
multicast-routing	マルチキャスト ルーティングをイネーブルにします。
pim	インターフェイスに対して PIM をイネーブルにします。

migrate

LAN-to-LAN の設定（IKEv1）やリモート アクセスの設定（SSL または IKEv1）を IKEv2 に移行するには、グローバル コンフィギュレーション モードで **migrate** コマンドを使用します。

migrate {**l2l** | **remote-access** {**ikev2** | **ssl**} | **overwrite**}

構文の説明

l2l	IKEv1 の LAN-to-LAN の設定を IKEv2 に移行します。
remote-access	リモート アクセスの設定を指定します。
ikev2	リモート アクセスの IKEv1 設定を IKEv2 に移行します。
ssl	リモート アクセスの SSL 設定を IKEv2 に移行します。
overwrite	既存の IKEv2 設定を上書きします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	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	• Yes	—	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

migrate l2l コマンドを使用すると、LAN-to-LAN のすべての IKEv1 設定が IKEv2 に移行されます。

overwrite キーワードを使用すると、既存の IKEv2 設定がある場合に、ASA で移行されたコマンドとマージされるのではなく、それらのコマンドで上書きされます。

migrate remote-access コマンドを使用すると、IKEv1 または SSL の設定が IKEv2 に移行されます。ただし、次の設定タスクは別途実行する必要があります。

- webvpn コンフィギュレーション モードで AnyConnect クライアント パッケージ ファイルをロードします。
- AnyConnect クライアント プロファイルを設定し、グループ ポリシーに対して指定します。
- IKEv1 接続にカスタマイゼーション オブジェクトを使用している場合は、IKEv2 接続に使用するトンネル グループにそれらを関連付けます。
- サーバ認証のアイデンティティ証明書（トラストポイント）を **crypto ikev2 remote-access trust-point** コマンドを使用して指定します。このトラストポイントは、IKEv2 で接続しているリモートの AnyConnect クライアントに ASA を認証するときに使用します。
- デフォルトのもの以外にもトンネル グループおよび/またはグループ ポリシーを設定している場合は、それらに対して IKEv2 または SSL を指定します（デフォルトの DefaultWEBVPNGroup トンネル グループとデフォルトのグループ ポリシーは IKEv2 または SSL を許可するように設定されています）。
- クライアントからデフォルト以外のグループに接続できるようにするには、トンネル グループでグループのエイリアスまたは URL を設定します。
- 外部のグループ ポリシーやユーザ レコードを更新します。
- グローバル、トンネル グループ、またはグループ ポリシーのその他の設定でクライアントの動作を変更します。
- クライアントで IKEv2 のファイルのダウンロードやソフトウェアのアップグレードに使用するポートを **crypto ikev2 enable** <*interface*> [**client-services** [*port*]] コマンドを使用して設定します。

関連コマンド

コマンド	説明
crypto ikev2 enable	IPsec ピアの通信に使用するインターフェイスで IKEv2 ネゴシエーションをイネーブルにします。
show run crypto ikev2	IKEv2 設定情報を表示します。

min-object-size

WebVPN セッションに対して ASA がキャッシュできるオブジェクトの最小サイズを設定するには、キャッシュ モードで min-object-size コマンドを使用します。サイズを変更するには、このコマンドを再度使用します。最小オブジェクト サイズを設定しないようにするには、値にゼロ(0)を入力します。

min-object-size *integer range*

構文の説明

integer range	0 ～ 10000 KB。

デフォルト

デフォルトのサイズは 0 KB です。

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	トランスペアレント	シングル	コンテキスト	システム
キャッシュ モード	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

最小オブジェクト サイズは、最大オブジェクト サイズよりも小さい値である必要があります。キャッシュ圧縮がイネーブルになっている場合、ASA は、オブジェクトを圧縮してからサイズを計算します。

例

次に、最大オブジェクト サイズを 40 KB に設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# min-object-size 40
ciscoasa(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。

mkdir

新規ディレクトリを作成するには、特権 EXEC モードで **mkdir** コマンドを使用します。

mkdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

構文の説明

noconfirm	（任意）確認プロンプトを表示しないようにします。
disk0*:*	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。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** キーワードは **disk0** とエイリアス関係にあります。
path	作成するディレクトリの名前およびパス。

デフォルト

パスを指定しないと、現在の作業ディレクトリにディレクトリが作成されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

同じ名前のディレクトリがすでに存在する場合、新規のディレクトリは作成されません。

例

次に、新規ディレクトリを「backup」という名前で作成する例を示します。

```
ciscoasa# mkdir backup
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
dir	ディレクトリの内容を表示します。
rmdir	指定されたディレクトリを削除します。
pwd	現在の作業ディレクトリを表示します。

mobile-device portal

すべてのモバイル デバイスのクライアントレス VPN アクセス Web ポータルをミニポータルからフルブラウザ ポータルに変更するには、webvpn コンフィギュレーション モードで **mobile-device portal** コマンドを使用します。この設定が必要なのは、Windows CE などの古いオペレーティング システムを実行するスマートフォンだけです。新しいスマートフォンではデフォルトでフルブラウザ ポータルが使用されているため、このオプションを設定する必要はありません。

mobile-device portal {full}

no mobile-device portal {full}

構文の説明

mobile-device portal {full}	すべてのモバイル デバイスのクライアントレス VPN アクセス ポータルをミニポータルからフルブラウザ ポータルに変更します。

コマンドデフォルト

このコマンドを実行する前のデフォルトの動作では、モバイル デバイスによって、クライアントレス VPN アクセスにミニ ポータルを使用するかフル ポータルを使用するかが異なります。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(5)	このコマンドが 8.2(5) と 8.4(2) で同時に追加されました。
8.4(2)	このコマンドが 8.2(5) と 8.4(2) で同時に追加されました。

使用上のガイドライン　このコマンドは、Cisco Technical Assistance Center（TAC）から推奨された場合にのみ使用してください。

例　すべてのモバイル デバイスのクライアントレス VPN アクセス ポータルをフルブラウザ ポータルに変更します。

```
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mobile-device portal full
```

関連コマンド

コマンド	説明
show running-config webvpn	WebVPN の実行コンフィギュレーションを表示します。

mode

セキュリティ コンテキスト モードを single または multiple に設定するには、グローバル コンフィギュレーション モードで **mode** コマンドを使用します。1 つの ASA をいくつかのパーティションに分けて複数の仮想デバイス（セキュリティ コンテキストと呼びます）に配置できます。各コンテキストは独立したデバイスとして動作し、独自のセキュリティ ポリシー、インターフェイス、および管理者で構成されています。複数のコンテキストが存在することは、複数のスタンドアロン アプライアンスが設置されていることと同じです。シングル モードでは、ASA はシングル コンフィギュレーションを備え、単一デバイスとして動作します。マルチ モードでは、複数のコンテキストを作成し、それぞれに独自のコンフィギュレーションを設定できます。許可されるコンテキストの数は、保有するライセンスによって異なります。

mode {**single** | **multiple**} [**noconfirm**]

構文の説明

複数	マルチ コンテキスト モードを設定します。
noconfirm	(任意)ユーザに確認を求めることなく、モードを設定します。このオプションは自動スクリプトで役立ちます。
single	コンテキスト モードを single に設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、ASA に各コンテキストのコンフィギュレーションが含まれ、それぞれのコンフィギュレーションでは、スタンドアロン デバイスに設定できるセキュリティ ポリシー、インターフェイス、およびほぼすべてのオプションが識別されます(コンテキスト コンフィギュレーションの場所を識別するには、**config-url** コマンドを参照してください)。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに(サーバからコンテキストをダウンロードするなど)、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

mode コマンドを使用してコンテキスト モードを変更すると、再起動するように求められます。

コンテキスト モード(シングルまたはマルチ)は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、**mode** コマンドを使用して、新規デバイスのモードを match に設定します。

シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。システム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーションと、(内部フラッシュ メモリのルート ディレクトリの)管理コンテキストで構成される admin.cfg です。元の実行コンフィギュレーションは、old_running.cfg として(内部フラッシュ メモリのルート ディレクトリに)保存されます。元のスタートアップ コンフィギュレーションは保存されません。ASA は、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

マルチ モードからシングル モードに変換する場合は、先にスタートアップ コンフィギュレーション全体（使用可能な場合）を ASA にコピーすることを推奨します。マルチ モードから継承されるシステム コンフィギュレーションは、シングル モード デバイスで完全に機能するコンフィギュレーションではありません。

マルチ コンテキスト モードのすべての機能がサポートされるわけではありません。詳細については、CLI 設定ガイドを参照してください。

例

次に、モードを multiple に設定する例を示します。

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode

Rebooting....

Booting system, please wait...
```

次に、モードを single に設定する例を示します。

```
ciscoasa(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode



Rebooting....

Booting system, please wait...
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードを開始します。
show mode	現在のコンテキスト モード（シングルまたはマルチ）を表示します。

monitor-interface

特定のインターフェイスでヘルス モニタリング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 **monitor-interface** コマンドを使用します。インターフェイスのモニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

monitor-interface {*if_name* | **service-module**}

no monitor-interface {*if_name* | **service-module**}

構文の説明

if_name	モニタするインターフェイスの名前を指定します。
service-module	サービス モジュールをモニタします。ASA FirePOWER モジュールなど、ハードウェア モジュールの障害でフェールオーバーが開始されないようにする場合は、このコマンドの **no** 形式を使用してモジュールのモニタリングをディセーブルにできます。

デフォルト

物理インターフェイスとサービス モジュールのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.3(1)	service-module キーワードが追加されました。

使用上のガイドライン

ASA についてモニタできるインターフェイスの数はプラットフォームごとに異なり、**show failover** コマンドの出力で確認できます。

インターフェイス ポーリング頻度ごとに、ASA フェールオーバー ペア間で hello メッセージが交換されます。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、あるインターフェイスで 5 回連続して hello が検出されないと（25 秒間）、そのインターフェイスでテストが開始します。

モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

アクティブ/アクティブ フェールオーバーでは、このコマンドはコンテキスト内でだけ有効です。

例

次の例では、「inside」という名前のインターフェイスでモニタリングをイネーブルにしています。

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure monitor-interface	すべてのインターフェイスでデフォルトのインターフェイス ヘルス モニタリングに戻します。
failover interface-policy	モニタするインターフェイスの数または割合を指定します。モニタの対象となるのは、障害が発生すると、フェールオーバーが発生するインターフェイスです。
failover polltime	インターフェイスでの hello メッセージ間の間隔を指定します（Active/Standby フェールオーバー）。
polltime interface	インターフェイスでの hello メッセージ間の間隔を指定します（Active/Active フェールオーバー）。
show running-config monitor-interface	実行コンフィギュレーション内の **monitor-interface** コマンドを表示します。

more

ファイルの内容を表示するには、特権 EXEC モードで **more** コマンドを使用します。

more {**/ascii** | **/binary**| **/ebcdic** | **disk0**: | **disk1**: | **flash**: | **ftp**: | **http**: | **https**: | **system**: | **tftp**:}*filename*

構文の説明

/ascii	（任意）バイナリ ファイルをバイナリ モード、ASCII ファイルをバイナリ モードで表示します。
/binary	（任意）任意のファイルをバイナリ モードで表示します。
/ebcdic	（任意）バイナリ ファイルを EBCDIC で表示します。
disk0*:*	（任意）内部フラッシュ メモリのファイルを表示します。
disk1:	（任意）外部フラッシュ メモリ カードのファイルを表示します。

filename	表示するファイルの名前を指定します。
flash:	(任意)内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズの適応型セキュリティ アプライアンスでは、**flash** キーワードは **disk0** のエイリアスです。
ftp:	(任意)FTP サーバ上のファイルを表示します。
http:	(任意)Web サイト上のファイルを表示します。
https:	(任意)セキュアな Web サイト上のファイルを表示します。
system:	(任意)ファイル システムを表示します。
tftp:	(任意)TFTP サーバ上のファイルを表示します。

デフォルト

ASCII モード

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	• Yes	• Yes	• Yes	—	• Yes

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

more filesystem: コマンドは、ローカル ディレクトリまたはファイル システムのエイリアスを入力するように求めます。

(注) **more** コマンドを使用して保存したコンフィギュレーション ファイルを表示すると、このコンフィギュレーション ファイルのトンネル グループ パスワードがクリア テキストに表示されます。

例

次に、「test.cfg」というローカル ファイルの内容を表示する例を示します。

```
ciscoasa# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005

XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
```

```
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

関連コマンド

コマンド	説明
cd	指定されたディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。

mount type cifs

セキュリティ アプライアンスから共通インターネット ファイル システム（CIFS）にアクセス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 **mount type cifs** コマンドを使用します。このコマンドを使用すると、mount cifs コンフィギュレーション モードに入ることができます。CIFS ネットワーク ファイル システムをマウント解除するには、このコマンドの **no** 形式を使用します。

mount *name* **type cifs server** *server-name* **share** *share {***status enable | status disable} [domain** *domain-name* **] username** *username* **password** *password*

[**no**] **mount** *name* **type cifs server** *server-name* **share** *share {***status enable | status disable} [domain** *domain-name* **] username** *username* **password** *password*

構文の説明

domain *domain-name*	（任意）CIFS ファイル システムでのみ、この引数には Windows NT ドメイン名を指定します。最大 63 文字が許可されます。
name	ローカル CA に割り当てられる既存のファイル システムの名前を指定します。
password *password*	ファイル システムのマウントのための認可されたパスワードを指定します。
server *server-name*	CIFS ファイル システム サーバの定義済みの名前（またはドット付き 10 進表記の IP アドレス）を指定します。
share *sharename*	サーバ内のファイル データにアクセスするために、特定のサーバ共有（フォルダ）を名前で明示的に識別します。
status enable または **disable**	ファイル システムの状態をマウント済みまたはマウント解除済み（使用可能または使用不能）として識別します。
user *username*	ファイル システムのマウントが認可されているユーザ名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

mount コマンドは、Installable File System（IFS）を使用して、CIFS ファイル システムをマウントします。IFS（ファイル システム API）を使用すると、セキュリティ アプライアンスはファイル システム用のドライバを認識し、ロードすることができます。

mount コマンドは、セキュリティ アプライアンス上の CIFS ファイル システムを UNIX ファイル ツリーにアタッチします。逆に、**no mount** コマンドはそのアタッチを解除します。

mount コマンドに指定されている *mount-name* は、セキュリティ アプライアンスにすでにマウントされているファイル システムを参照するために、他の CLI コマンドで使用されます。たとえば、ローカル認証局用にファイル ストレージを設定する **database** コマンドでは、データベース ファイルをフラッシュ ストレージでないストレージに保存するために、すでにマウントされているファイル システムのマウント名が必要です。

CIFS リモート ファイル アクセス プロトコルは、アプリケーションがローカル ディスクおよびネットワーク ファイル サーバ上のデータを共有する方法と互換性があります。TCP/IP を運用し、インターネットのグローバル DNS を使用する CIFS は、Windows オペレーティング システムにネイティブのファイル共有プロトコルである Microsoft のオープンでクロス プラットフォームのサーバ メッセージ ブロック（SMB）プロトコルを拡張したものです。

mount コマンドを使用した後は、必ずルート シェルを終了してください。mount-cifs-config モードの **exit** キーワードは、ユーザをグローバル コンフィギュレーション モードに戻します。

再接続するには、接続をストレージに再マッピングします。

（注） CIFS ファイル システムと FTP ファイル システムのマウントがサポートされています（**mount** *name* **type ftp** コマンドを参照）。このリリースではネットワーク ファイル システム（NFS）ボリュームのマウントはサポートされていません。

例

次に、*cifs://amer;chief:big-boy@myfiler02/my_share* を *cifs_share* というラベルとしてマウントする例を示します。

```
ciscoasa(config)# mount cifs_share type CIFS
ciscoasa (config-mount-cifs)# server myfiler02a
```

関連コマンド

コマンド	説明
debug cifs	CIFS デバッグ メッセージをロギングします。
debug ntdomain	Web VPN NT ドメイン デバッグ メッセージをロギングします。
debug webvpn cifs	WebVPN CIFS デバッグ メッセージをロギングします。
dir all-filesystems	ASA にマウントされているすべてのファイル システムのファイルを表示します。

mount type ftp

セキュリティ アプライアンスからファイル転送プロトコル（FTP）ファイル システムにアクセス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 **mount type ftp** コマンドを使用して、マウント FTP コンフィギュレーション モードを開始します。**no mount type ftp** コマンドは、FTP ネットワーク ファイル システムをマウント解除するために使用されます。

[**no**] **mount** *name* **type ftp server** *server-name* **path** *pathname* {**status enable** | **status disable**} {**mode active** | **mode passive**} **username** *username* **password** *password*

構文の説明

mode active または **passive**	FTP 転送モードをアクティブまたはパッシブとして識別します。
no	すでにマウントされている FTP ファイル システムを削除し、アクセスできないようにします。
password *password*	ファイル システムのマウントのための認可されたパスワードを指定します。
path *pathname*	指定された FTP ファイル システム サーバへのディレクトリ パス名を指定します。パス名にスペースを含めることはできません。
server *server-name*	FTPFS ファイル システム サーバの定義済みの名前（またはドット付き 10 進表記の IP アドレス）を指定します。
status enable または **disable**	ファイル システムの状態をマウント済みまたはマウント解除済み（使用可能または使用不能）として識別します。
username *username*	ファイル システムのマウントが認可されているユーザ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

mount *name* **type ftp** コマンドは、Installable File System（IFS）を使用して、指定されたネットワーク ファイル システムをマウントします。IFS（ファイル システム API）を使用すると、セキュリティ アプライアンスはファイル システム用のドライバを認識し、ロードすることができます。

FTP ファイル システムが実際にマウントされていることを確認するには、**dir all-filesystems** 命令を使用します。

mount コマンドに指定されているマウント名は、他の CLI コマンドがセキュリティ アプライアンスですでにマウントされているファイル システムを参照するときに使用されます。たとえば、ローカル認証局用にファイル ストレージを設定する **database** コマンドでは、データベース ファイルをフラッシュ ストレージでないストレージに保存するために、すでにマウントされているファイル システムのマウント名が必要です。

(注) FTP タイプのマウントの作成時に **mount** コマンドを使用するには、FTP サーバに UNIX ディレクトリ リスト スタイルが必要です。Microsoft FTP サーバには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

(注) CIFS ファイル システムと FTP ファイル システムのマウントがサポートされています（**mount** *name* **type ftp** コマンドを参照）。このリリースではネットワーク ファイル システム（NFS）ボリュームのマウントはサポートされていません。

例

次に、*ftp://amor;chief:big-kid@myfiler02* を *my ftp:* というラベルとしてマウントする例を示します。

```
ciscoasa(config)# mount myftp type ftp server myfiler02a path status enable username chief
password big-kid
```

関連コマンド

コマンド	説明
debug webvpn	WebVPN デバッグ メッセージをロギングします。
ftp mode passive	ASA 上の FTP クライアントと FTP サーバとの通信を制御します。

mroute

スタティック マルチキャスト ルートを設定するには、グローバル コンフィギュレーション モードで **mroute** コマンドを使用します。スタティック マルチキャスト ルートを削除するには、このコマンドの **no** 形式を使用します。

mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

no mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

構文の説明

dense *output_if_name*	（任意）デンス モード出力のインターフェイス名。 **dense** *output_if_name* キーワードと引数のペアは、SMR スタブ マルチキャスト ルーティング（igmp 転送）に対してだけサポートされます。
distance	（任意）ルートのアドミニストレーティブ ディスタンス。ディスタンスが小さいルートが優先されます。デフォルトは 0 です。
in_if_name	mroute の着信インターフェイス名を指定します。
rpf_addr	mroute の着信インターフェイスを指定します。RPF アドレスが PIM ネイバーである場合、PIM Join メッセージ、接合メッセージ、および Prune メッセージがそのアドレスに送信されます。*rpf-addr* 引数には、直接接続されたシステムのホスト IP アドレスまたはネットワーク/サブネット番号を指定します。ルートである場合、直接接続されたシステムを検索するために、ユニキャスト ルーティング テーブルから再帰検索が実施されます。
smask	マルチキャスト送信元ネットワーク アドレス マスクを指定します。
src	マルチキャスト送信元の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、マルチキャスト送信元の検索場所をスタティックに設定できます。ASA は、特定の送信元にユニキャスト パケットを送信する際に使用したものと同じインターフェイスでマルチキャスト パケットを受信するものと想定します。場合によっては、マルチキャスト ルーティングをサポートしないルートをバイパスするなど、マルチキャスト パケットがユニキャスト パケットとは別のパスをたどることがあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

マルチキャスト ルート テーブルの内容を表示するには、**show mroute** コマンドを使用します。実行コンフィギュレーションで mroute コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次に、**mroute** コマンドを使用して、スタティック マルチキャスト ルートを設定する例を示します。

```
ciscoasa(config)# mroute 172.16.0.0 255.255.0.0 inside
```

関連コマンド

コマンド	説明
clear configure mroute	コンフィギュレーションから **mroute** コマンドを削除します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	コンフィギュレーションの **mroute** コマンドを表示します。

mschapv2-capable

RADIUS サーバに対する MS-CHAPv2 認証要求をイネーブルにするには、aaa-server ホスト コンフィギュレーション モードで **mschapv2-capable** コマンドを使用します。MS-CHAPv2 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。

mschapv2-capable

no mschapv2-capable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、MS-CHAPv2 はイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
AAA サーバ ホスト コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASA と RADIUS サーバとの間で VPN 接続に使用されるプロトコルとして MS-CHAPv2 をイネーブルにするには、トンネル グループ一般属性でパスワード管理をイネーブルにする必要があります。パスワード管理をイネーブルにすると、ASA から RADIUS サーバへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネル グループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバが MS-CHAPv2 以外の認証要求を送信するように設定できます。

例

次に、RADIUS サーバ authsrv1.cisco.com の MS-CHAPv2 をディセーブルにする例を示します。

```
ciscoasa(config)# aaa-server rsaradius protocol radius
ciscoasa(config-aaa-server-group)# aaa-server rsaradius (management) host
authsrv1.cisco.com
ciscoasa(config-aaa-server-host)# key secretpassword
```

```
ciscoasa(config-aaa-server-host)# authentication-port 21812
ciscoasa(config-aaa-server-host)# accounting-port 21813
ciscoasa(config-aaa-server-host)# no mschapv2-capable
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ グループの AAA サーバを識別します。
password-management	password-management コマンドを設定すると、ASA は、リモート ユーザがログインするときに、そのユーザの現在のパスワードの期限切れが迫っている、または期限が切れたことを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。
secondary-authentication-server-group	SDI サーバ グループになることができないセカンダリ AAA サーバ グループを指定します。

msie-proxy except-list

クライアント デバイスのブラウザがローカルでプロキシをバイパスするために使用するプロキシの例外リストを設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy except-list** 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。

msie-proxy except-list {value *server*[*:port*] **| none}**

no msie-proxy except-list

構文の説明

none	IP アドレス/ホスト名またはポートがなく、例外リストを継承しないことを示します。
value *server:port*	IP アドレスまたは MSIE サーバの名前、およびこのクライアント デバイスに適用されるポートを指定します。ポート番号は任意です。

デフォルト

デフォルトでは、msie-proxy except-list はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

プロキシ設定の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1*』、またはお使いのモバイル デバイスのリリース ノートを参照してください。

例

次に、Microsoft Internet Explorer のプロキシ例外リストを設定する例を示します。IP アドレス 192.168.20.1 のサーバで構成され、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象とします。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy local-bypass

クライアント デバイスのブラウザ プロキシ ローカル バイパス設定を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy local-bypass** コマンドを入力します。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。

msie-proxy local-bypass {enable | disable}

no msie-proxy local-bypass {enable | disable}

構文の説明

disable	クライアント デバイスのブラウザ プロキシ ローカル バイパス設定をディセーブルにします。
enable	クライアント デバイスのブラウザ プロキシ ローカル バイパス設定をイネーブルにします。

デフォルト

デフォルトでは、msie-proxy local-bypass はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

プロキシ設定の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1*』、またはお使いのモバイル デバイスのリリース ノートを参照してください。

例

次に、FirstGroup というグループ ポリシーの Microsoft Internet Explorer のプロキシ ローカル バイパスをイネーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy local-bypass enable
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy lockdown

この機能をイネーブルにすると AnyConnect VPN セッション時にブラウザの接続タブが非表示になります。この機能をディセーブルにしても接続タブの表示はそのままです。

AnyConnect VPN セッション時に接続タブを非表示にする、またはそのままにするには、グループ ポリシー コンフィギュレーション モードで、**msie-proxy lockdown** コマンドを使用します。

msie-proxy lockdown [enable | disable]

構文の説明

disable	ブラウザの接続タブをそのままにします。
enable	AnyConnect VPN セッション時にブラウザの接続タブを非表示にします。

デフォルト

デフォルトのグループ ポリシーでのこのコマンドのデフォルト値はイネーブルです。グループ ポリシーそれぞれがデフォルトのグループ ポリシーからデフォルト値を継承します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(3)	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、ユーザ レジストリを AnyConnect VPN セッションの間、一時的に変更します。AnyConnect が VPN セッションを閉じると、レジストリはセッション前の状態に戻ります。

この機能をイネーブルにして、ユーザがプロキシ サービスを指定して LAN 設定を変更することを防止できます。これらの設定へのユーザ アクセスを防止すると、AnyConnect セッション中のエンドポイント セキュリティが向上します。

プロキシ設定の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1*』、またはお使いのモバイル デバイスのリリース ノートを参照してください。

例

次の例では、AnyConnect セッションの間、接続タブを非表示にします。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy lockdown enable
```

次の例では、接続タブをそのままにします。

```
ciscoasa(config-group-policy)# msie-proxy lockdown disable
```

関連コマンド

コマンド	説明
msie-proxy except-list	クライアント デバイスのブラウザのプロキシ サーバの例外リストを指定します。
msie-proxy local-bypass	クライアント デバイスで設定されているローカル ブラウザ プロキシ設定をバイパスします。
msie-proxy method	クライアント デバイスのブラウザ プロキシ アクションを指定します。
msie-proxy pac-url	プロキシ サーバを定義するプロキシ自動コンフィギュレーション ファイルの取得元の URL を指定します。

コマンド	説明
msie-proxy server	クライアント デバイスのブラウザのプロキシ サーバを設定します。
show running-config group-policy	実行コンフィギュレーションのグループ ポリシー設定を表示します。

msie-proxy method

クライアント デバイスのブラウザ プロキシ アクション(「メソッド」)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 **msie-proxy method** コマンドを入力します。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。

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

(注) この構文に適用される条件については、「使用上のガイドライン」を参照してください。

構文の説明

auto-detect	クライアントデバイスのブラウザでプロキシ サーバの自動検出の使用をイネーブルにします。
no-modify	このクライアント デバイスでは、ブラウザの HTTP ブラウザ プロキシ サーバ設定をそのままにしておきます。
no-proxy	このクライアント デバイスでは、ブラウザの HTTP プロキシ設定をディセーブルにします。
use-pac-url	**msie-proxy pac-url** コマンドに指定されているプロキシ自動コンフィギュレーション ファイル URL から HTTP プロキシ サーバ設定を取得するようにブラウザに指示します。
use-server	**msie-proxy server** コマンドに設定された値を使用するように、ブラウザの HTTP プロキシ サーバ設定を設定します。

デフォルト

デフォルトのメソッドは use-server 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 コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	use-pac-url オプションが追加されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行には、最大 100 文字含めることができます。

このコマンドでサポートされるオプションの組み合わせは次のとおりです。

- **[no] msie-proxy method no-proxy**
- **[no] msie-proxy method no-modify**
- **[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]**

テキスト エディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバを指定するロジックを含む JavaScript ファイルです。.pac ファイルは、Web サーバにあります。**use-pac-url** を指定すると、ブラウザは .pac ファイルを使用してプロキシ設定を判別します。.pac ファイルの取得元の URL を指定するには、**msie-proxy pac-url** コマンドを使用します。

プロキシ設定の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1*』、またはお使いのモバイル デバイスのリリース ノートを参照してください。

例

次に、FirstGroup というグループ ポリシーの Microsoft Internet Explorer プロキシ設定として自動検出を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy method auto-detect
ciscoasa(config-group-policy)#
```

次に、クライアント PC のサーバとしてサーバ QASERVER、ポート 1001 を使用するように、FirstGroup というグループ ポリシーの Microsoft Internet Explorer プロキシ設定を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server QAserver:port 1001
ciscoasa(config-group-policy)# msie-proxy method use-server
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
msie-proxy pac-url	プロキシ自動コンフィギュレーション ファイルの取得先となる URL を指定します。
msie-proxy server	クライアント デバイスのブラウザ プロキシ サーバおよびポートを設定します。
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy pac-url

プロキシ情報の検索場所をブラウザに指示するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy pac-url** コマンドを入力します。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。

msie-proxy pac-url {**none** | **value** *url*}

no msie-proxy pac-url

構文の説明

none	URL 値がないことを指定します。
value *url*	使用するプロキシ サーバが 1 つ以上定義されているプロキシ自動コンフィギュレーション ファイルをブラウザが取得できる Web サイトの URL を指定します。

デフォルト

デフォルト値は none です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

要件

プロキシ自動コンフィギュレーション機能を使用するには、リモート ユーザは Cisco AnyConnect VPN クライアントを使用する必要があります。プロキシ自動コンフィギュレーション URL の使用をイネーブルにするには、**msie-proxy method** コマンドを **use-pac-url** オプションとともに設定する必要があります。

このコマンドを使用する理由

多くのネットワーク環境が、Web ブラウザを特定のネットワーク リソースに接続する HTTP プロキシを定義しています。HTTP トラフィックがネットワーク リソースに到達できるのは、プロキシがブラウザに指定され、クライアントが HTTP トラフィックをプロキシにルーティングする場合だけです。SSLVPN トンネルにより、HTTP プロキシの定義が複雑になります。企業ネットワークにトンネリングするときに必要なプロキシが、ブロードバンド接続経由でインターネットに接続されるときや、サード パーティ ネットワーク上にあるときに必要なものとは異なることがあるためです。

また、大規模ネットワークを構築している企業では、複数のプロキシ サーバを設定し、一時的な状態に基づいてユーザがその中からプロキシ サーバを選択できるようにすることが必要になる場合があります。.pac ファイルを使用すると、管理者は数多くのプロキシからどのプロキシを社内のすべてのクライアント コンピュータに使用するかを決定する単一のスクリプト ファイルを作成できます。

次に、PAC ファイルを使用する例をいくつか示します。

- ロード バランシングのためリストからプロキシをランダムに選択します。
- サーバのメンテナンス スケジュールに対応するために、時刻または曜日別にプロキシを交代で使用します。
- プライマリ プロキシで障害が発生した場合に備えて、使用するバックアップ プロキシ サーバを指定します。
- ローカル サブネットを元に、ローミング ユーザ用に最も近いプロキシを指定します。

プロキシ自動コンフィギュレーション機能の使用方法

テキスト エディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバを指定するロジックを含む JavaScript ファイルです。.pac ファイルの取得元の URL を指定するには、**msie-proxy pac-url** コマンドを使用します。次に、**msie-proxy method** コマンドに **use-pac-url** を指定すると、ブラウザは .pac ファイルを使用してプロキシ設定を判別します。

プロキシ設定の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1*』、またはお使いのモバイル デバイスのリリース ノートを参照してください。

例

次に、FirstGroup というグループ ポリシーのプロキシ設定を www.example.com という URL から取得するように、ブラウザを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url value http://www.example.com
ciscoasa(config-group-policy)#
```

次に、FirstGroup というグループ ポリシーのプロキシ自動コンフィギュレーション機能をディセーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url none
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
msie-proxy method	クライアント デバイスのブラウザ プロキシ アクション(「メソッド」)を設定します。
msie-proxy server	クライアント デバイスのブラウザ プロキシ サーバおよびポートを設定します。
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy server

クライアント デバイスのブラウザ プロキシ サーバおよびポートを設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy server** コマンドを入力します。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。

msie-proxy server {value *server*[*:port*] **| none}**

no msie-proxy server

構文の説明

none	プロキシ サーバに指定されている IP アドレス/ホスト名またはポートがなく、サーバが継承されないことを示します。
value *server:port*	IP アドレスまたは MSIE サーバの名前、およびこのクライアント デバイスに適用されるポートを指定します。ポート番号は任意です。

デフォルト

デフォルトでは、no msie-proxy server が指定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

プロキシ設定の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1*』、またはお使いのモバイル デバイスのリリース ノートを参照してください。

例

次に、Microsoft Internet Explorer プロキシ サーバとして IP アドレス 192.168.10.1 を設定し、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象にする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server value 192.168.21.1:880
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

mtu

インターフェイスの最大伝送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 **mtu** コマンドを使用します。イーサネット インターフェイスの MTU ブロック サイズを 1500 にリセットするには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 トラフィックと IPv6 トラフィックをサポートしています。

mtu *interface_name bytes*

no mtu *interface_name bytes*

構文の説明

bytes	MTU のバイト数。有効な値は 64 ～ 9198 バイト（ASAv および Firepower 9300 ASA セキュリティ モジュールの場合は 9000）です。
interface_name	内部または外部ネットワーク インターフェイス名。

デフォルト

イーサネット インターフェイスのデフォルトの *bytes* は 1500 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	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	—	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(6)	最大 MTU が 65535 から 9198（モデルによっては 9000）に変更されました。

使用上のガイドライン

mtu コマンドを使用すると、接続上で送信されるペイロード サイズ（レイヤ 2 ヘッダーまたは VLAN タギングを除く）を設定できます。MTU 値よりも大きいデータは、送信前にフラグメント化されます。イーサネット インターフェイスのデフォルト MTU は 1500 バイトです（これは、ジャンボ フレーム予約なしの最大サイズでもある）。この場合、レイヤ 2 ヘッダー（14 バイト）と VLAN タギング（4 バイト）を持つパケットのサイズは 1518 バイトです。ほとんどのアプリケーションではこの値で十分ですが、ネットワーク状況によってはこれよりも小さい値にすることもできます。

ASA は、IP パス MTU ディスカバリを（RFC 1191 での規定に従って）サポートします。これにより、ホストはパスに沿ったさまざまなリンクで許容される最大 MTU サイズをダイナミックに検出し、各サイズの差に対処できます。パケットがインターフェイスに対して設定されている MTU よりも大きくなっているものの、「Don't Fragment」（DF）ビットが設定されているために、ASA がデータグラムを転送できないことがあります。ネットワーク ソフトウェアは、メッセージを送信ホストに送信して、問題を警告します。送信ホストは、パスに沿ったすべてのリンクのうち最小のパケット サイズに適合するように、宛先へのパケットをフラグメント化する必要があります。

レイヤ 2 トンネリング プロトコル（L2TP）を使用するときは、L2TP ヘッダーと IPsec ヘッダーの長さを踏まえて MTU サイズを 1380 に設定することを推奨します。

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

バージョン 9.1(6) 以降では、ASA が使用できる最大 MTU は 9198 バイトです。この値にはレイヤ 2 ヘッダーは含まれません。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、これは不正確であり、問題が発生する可能性がありました。9198 よりも大きいサイズに MTU を設定している場合は、アップグレード時に MTU のサイズが自動的に削減されます。場合によっては、この MTU の変更により MTU の不一致が発生する可能性があります。接続している機器が新しい MTU 値を使用するように設定されていることを確認してください。

例

次に、インターフェイスの MTU を指定する例を示します。

```
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
ciscoasa(config)# mtu inside 8192
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

関連コマンド

コマンド	説明
clear configure mtu	すべてのインターフェイスの設定済み最大伝送単位値をクリアします。
show running-config mtu	現在の最大伝送単位のブロック サイズを表示します。

mtu cluster

クラスタ制御リンクの最大伝送単位を設定するには、グローバル コンフィギュレーション モードで **mtu cluster** コマンドを使用します。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。

mtu cluster *bytes*

no mtu cluster [*bytes*]

構文の説明

bytes	クラスタ制御リンク インターフェイスの最大伝送単位を 64 ～ 65,535 バイトの範囲内で指定します。デフォルトの MTU は 1500 バイトです。

コマンド デフォルト

デフォルトの MTU は 1500 バイトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	• Yes	• Yes	• Yes	—	• Yes

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

MTU を 1600 バイト以上に設定することを推奨します。このようにするには、**jumbo-frame reservation** コマンドを使用してジャンボ フレームの予約をイネーブルにする必要があります。

このコマンドはグローバル コンフィギュレーション コマンドですが、ブートストラップ コンフィギュレーションの一部でもあります。ブートストラップ コンフィギュレーションは、ユニット間で複製されません。

例

次に、クラスタ制御リンクの MTU を 9000 バイトに設定する例を示します。

```
ciscoasa(config)# mtu cluster 9000
```

関連コマンド

コマンド	説明
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
jumbo frame-reservation	ジャンボ イーサネット フレームの使用をイネーブルにします。

multicast boundary

管理用スコープのマルチキャスト アドレスのマルチキャスト境界を設定するには、インターフェイス コンフィギュレーション モードで **multicast boundary** コマンドを使用します。境界を削除するには、このコマンドの **no** 形式を使用します。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できるようになります。

multicast boundary *acl* [**filter-autorp**]

no multicast boundary *acl* [**filter-autorp**]

構文の説明

acl	アクセス リストの名前または番号を指定します。アクセス リストには、境界の影響を受けるアドレスの範囲を定義します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。
filter-autorp	境界 ACL によって拒否された Auto-RP メッセージをフィルタリングします。指定されていない場合、すべての Auto-RP メッセージが通過します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、*acl* 引数によって定義されている範囲でマルチキャスト グループ アドレスをフィルタリングするようにインターフェイスに管理用スコープの境界を設定するために使用されます。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。このコマンドが設定されている場合、マルチキャスト データ パケットはいずれの方向であっても境界を通過できません。マルチキャスト データ パケット フローを制限すると、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できます。

filter-autorp キーワードを設定した場合、管理用スコープの境界は Auto-RP 検出メッセージおよびアナウンス メッセージを調べ、境界 ACL によって拒否される Auto-RP パケットから Auto-RP グループ範囲アナウンスメントを削除します。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

例

次に、すべての管理用スコープのアドレスの境界を設定し、Auto-RP メッセージをフィルタリングする例を示します。

```
ciscoasa(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
ciscoasa(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# multicast boundary boundary_test filter-autorp
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャスト ルーティングをイネーブルにします。

multicast-routing

ASA の IP マルチキャスト ルーティング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 **multicast routing** コマンドを使用します。IP マルチキャスト ルーティング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。

multicast-routing

no multicast-routing

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

multicast-routing コマンドは、デフォルトですべてのインターフェイスで PIM および IGMP をイネーブルにします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

multicast-routing コマンドは、すべてのインターフェイスで PIM および IGMP をイネーブルにします。

(注) PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

セキュリティ アプライアンスが PIM RP である場合は、セキュリティ アプライアンスの未変換の外部アドレスを RP アドレスとして使用します。

マルチキャスト ルーティング テーブルのエントリの数は、システムに搭載されているメモリの量によって制限されます。表 12-1 に、セキュリティ アプライアンス上のメモリの量に基づく特定のマルチキャスト テーブルのエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 12-1　マルチキャスト テーブルのエントリ制限（スタティック エントリとダイナミック エントリの組み合わせ）

テーブル	16 MB	128 MB	128 + MB
MFIB	1000	3000	5000
IGMP グループ	1000	3000	5000
PIM ルート	3000	7000	12000

例

次に、ASA で IP マルチキャスト ルーティングをイネーブルにする例を示します。

```
ciscoasa(config)# multicast-routing
```

関連コマンド

コマンド	説明
igmp	インターフェイスに対して IGMP をイネーブルにします。
pim	インターフェイスに対して PIM をイネーブルにします。

mus

ASA が WSA を指定する IP 範囲と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 **mus** コマンドを使用します。このサービスを無効にするには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 トラフィックと IPv6 トラフィックをサポートしています。指定したサブネットおよびインターフェイスで検索される WSA のみが登録されます。

mus *IPv4 address IPv4 mask interface_name*

no mus *IPv4 address IPv4 mask interface_name*

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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

次のコマンドを使用できます。

- A.B.C.D：ASA へのアクセスを認可された WSA の IP アドレスです。
- host：クライアントは、架空のホストに要求を送信して Web セキュリティ アプライアンスへの接続を定期的にチェックします。デフォルトでは、架空のホストの URL は mus.cisco.com です。AnyConnect Security Mobility をイネーブルにすると、Web セキュリティ アプライアンスは、この架空のホストへの要求を傍受し、このクライアントに応答します。
- password：WSA パスワードを設定します。
- server：WSA サーバを設定します。

例

次の例では、1.2.3.x サブネットの WSA サーバが、*inside* インターフェイスのセキュア モビリティ ソリューションにアクセスすることを許可します。

```
ciscoasa(config)# mus 1.2.3.0 255.255.255.0 inside
```

関連コマンド

コマンド	説明
mus password	AnyConnect Secure Mobility 通信の共有秘密を設定します。
mus server	ASA が WSA 通信を聴取するポートを指定します。
show webvpn mus	アクティブな WSA 接続セキュリティ アプライアンスに関する情報を表示します。

mus host

ASA で MUS ホスト名を指定するには、グローバル コンフィギュレーション モードで **mus host** コマンドを入力します。これは、ASA から AnyConnect クライアントに送信されるテレメトリの URL です。AnyConnect クライアントでは、この URL を使用して、MUS 関連サービス用のプライベート ネットワークにある WSA と通信します。このコマンドで入力したコマンドを削除するには、**no mus host** コマンドを使用します。

mus host *host name*

no mus host

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

所定のポートに対して AnyConnect Secure Mobility をイネーブルにできます。WSA ポートの値は 1 ～ 21000 です。このコマンドでポートが指定されていない場合、ポート 11999 が使用されます。

このコマンドを実行する前に AnyConnect Secure Mobility の共有秘密を設定する必要があります。

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

例

次の例では、AnyConnect Secure Mobility ホストと WebVPN コマンド サブモードを入力する方法を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mus 0.0.0.0 0.0.0.0 inside
ciscoasa(config-webvpn)# mus password abcdefgh123
ciscoasa(config-webvpn)# mus server enable 960 # non-default port
ciscoasa(config-webvpn)# mus host mus.cisco.com
```

関連コマンド

コマンド	説明
mus	ASA が WSA を指定する IP 範囲およびインターフェイスを指定します。
mus password	AnyConnect Secure Mobility 通信の共有秘密を設定します。
show webvpn mus	アクティブな WSA 接続セキュリティ アプライアンスに関する情報を表示します。

mus password

AnyConnect Secure Mobility 通信の共有秘密を設定するには、グローバル コンフィギュレーション モードで **mus password** コマンドを入力します。共有秘密を削除するには、**no mus password** コマンドを使用します。

mus password

no mus password

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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

有効なパスワードは、正規表現 [0-9, a-z, A-Z,:;_/-]{8,20} で定義されます。共有秘密パスワードの全長は、最小 8 文字、最大 20 文字です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン　この WebVPN サブモードを使用すると、WebVPN 用のグローバル設定を設定できます。AnyConnect Secure Mobility 通信に共有秘密を設定できます。

例　次の例では、AnyConnect Secure Mobility パスワードと WebVPN コマンド サブモードを入力する方法を示します。

```
ciscoasa(config)# mus password <password_string>
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
mus	ASA が WSA を指定する IP 範囲およびインターフェイスを指定します。
mus server	ASA が WSA 通信を聴取するポートを指定します。
show webvpn mus	アクティブな WSA 接続セキュリティ アプライアンスに関する情報を表示します。

mus server

ASA が WSA 通信を聴取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 **mus server** コマンドを入力します。このコマンドを使用して入力したコマンドを削除するには、**no mus server** コマンドを使用します。

mus server enable

no mus server enable

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

構文の説明　このコマンドには引数またはキーワードはありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン　AnyConnect Secure Mobility サービスで使用するポートを指定する必要があります。ASA と WSA の間の通信には、管理者が指定したポート（1 ～ 21000）で確立されたセキュアな SSL 接続が使用されます。

このコマンドを実行する前に AnyConnect Secure Mobility の共有秘密を設定する必要があります。

例　次の例では、AnyConnect Secure Mobility パスワードと WebVPN コマンド サブモードを入力する方法を示します。

```
ciscoasa(config-webvpn)# mus server enable?
webvpn mode commands/options
    port Configure WSA port
ciscoasa(config-webvpn)# mus server enable port 12000
```

関連コマンド

コマンド	説明
mus	ASA が WSA を指定する IP 範囲およびインターフェイスを指定します。
mus password	AnyConnect Secure Mobility 通信の共有秘密を設定します。
show webvpn mus	アクティブな WSA 接続セキュリティ アプライアンスに関する情報を表示します。