CHAPTER 2

プリファレンスの定義およびコンフィギュレーション、診断、ファイル管理ツールの使用

この章では、プリファレンスについて、およびコンフィギュレーション、問題診断、ファイル管理で使用可能なツールについて説明します。この項では、次のトピックについて取り上げます。

プリファレンス

この機能により、セッション間での一部の ASDM 機能の動作を変更できます。

ASDM のさまざまな設定を変更するには、次の手順を実行します。

ステップ 1 ASDM アプリケーションのメイン ウィンドウで、[Tools] > [Preferences] の順に選択します。

[General]、[Rules Table]、および [Syslog Colors] の 3 つのタブのある [Preferences] ダイアログボックスが表示されます。

ステップ 2 これらのタブの 1 つをクリックして次のように設定を定義します。[General] タブでは汎用プリファレンスを指定し、[Rules Tables] タブでは Rules テーブルのプリファレンスを指定し、[Syslog Colors] タブでは、[Home] ペインに表示されるシステム ログ メッセージの背景色、前景色、およびフォントの色を指定します。

ステップ 3 [General] タブでは、次の項目を指定します。

a. ASDM によって生成される CLI コマンドを表示するには、[Preview commands before sending them to the device] チェックボックスをオンにします。

b. 適応型セキュリティ アプライアンスに複数のコマンドを 1 つのグループとして送信するには、[Enable cumulative (batch) CLI delivery] チェックボックスをオンにします。

c. ASDM を閉じるときに終了を確認するプロンプトが表示されるようにするには、[Confirm before exiting ASDM] チェックボックスをオンにします。このオプションは、デフォルトでオンです。

d. 起動時に read-only ユーザに対して次のメッセージを表示するには、[Show configuration restriction message to read-only user] チェックボックスをオンにします。このオプションは、デフォルトでオンです。

```
"You are not allowed to modify the ASA configuration, because you do not have
sufficient privileges."
```

e. スクリーン リーダーをイネーブルにするには、[Enable screen reader support (requires ASDM restart)] チェックボックスをオンにします。このオプションをイネーブルにするには、ASDM を再起動する必要があります。

f. ユーザが VPN 接続によって ASDM にアクセスするときに警告メッセージを表示するには、[Warn that Easy VPN is enabled when visiting VPN section] チェックボックスをオンにします。このオプションは、ASA 5505 でだけ使用可能です。

g. Packet Capture Wizard で、キャプチャされたパケットが表示されるようにするには、ネットワーク スニファ アプリケーションの名前を入力するか、または [Browse] をクリックして指定します。

ステップ 4　[Rules Tables] タブで、次の項目を指定します。

a. [Display settings] では、[Rules] テーブルでのルールの表示方法を変更できます。

- Auto-Expand Prefix に基づいて自動展開されたネットワークおよびサービス オブジェクト グループを表示するには、[Auto-expand network and service object groups with specified prefix] チェックボックスをオンにします。
- [Auto-Expand Prefix] フィールドで、表示されるときに自動で展開されるネットワークおよびサービス オブジェクト グループのプレフィックスを指定します。
- ネットワークおよびサービス オブジェクト グループのメンバーとそのグループ名を [Rules] テーブルに表示するには、[Show members of network and service object groups] チェックボックスをオンにします。チェックボックスがオフの場合は、グループ名だけが表示されます。
- [Limit Members To] フィールドに、表示するネットワークおよびサービス オブジェクト グループの数を入力します。オブジェクト グループ メンバが表示されるときには、最初の *n* 個のメンバだけが表示されます。
- [Rules] テーブルにすべてのアクションを表示するには、[Show all actions for service policy rules] チェックボックスをオンにします。オフの場合は、サマリーが表示されます。

b. [Deployment Settings] では、[Rules] テーブルに変更内容を適用するときのセキュリティ アプライアンスの動作を設定できます。

- 新しいアクセス リストを適用するときに [NAT] テーブルをクリアするには、[Issue "clear xlate" command when deploying access lists] チェックボックスをオンにします。この設定により、セキュリティ アプライアンスで設定されるアクセス リストが、すべての変換アドレスに対して確実に適用されるようにします。

c. [Access Rule Hit Count Settings] では、[Access Rules] テーブルのヒット数をアップデートする頻度を設定できます。ヒット数は、明示的なルールにだけ適用されます。暗黙的なルールのヒット数は、[Access Rules] テーブルには表示されません。

- [Access Rules] テーブルでヒット数が自動的にアップデートされるようにするには、[Update access rule hit counts automatically] チェックボックスをオンにします。
- [Update Frequency] フィールドで、[Access Rules] テーブルのヒット数カラムをアップデートする頻度を秒単位で指定します。有効値の範囲は 10 ～ 86400 秒です。

ステップ 5　[Syslog Colors] タブで、次の項目を指定します。

- 各重大度レベルでメッセージの背景テキストまたは前景テキストの色を変更するには、対応するカラムをクリックします。[Pick a Color] ダイアログボックスが表示されます。次のいずれかのタブを選択します。
  - [Swatches] タブでは、パレットから色を選択して [OK] をクリックします。
  - [HSB] タブでは、[H]、[S]、および [B] 設定を指定して [OK] をクリックします。
  - [RGB] タブでは、[Red]、[Green]、および [Blue] 設定を指定して [OK] をクリックします。

[Severity] カラムは編集できません。このカラムには、名前と番号ごとの各重大度レベルが一覧表示されます。

（注）　プリファレンスのチェックボックスのオン/オフを切り替えると、そのたびに変更結果が .conf ファイルに保存され、その時点でワークステーションで実行中の他のすべての ASDM セッションで使用可能になります。すべての変更を有効にするには、ASDM を再起動する必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

コンフィギュレーション ツール

この項では、次のトピックについて取り上げます。

- 「Reset Device to the Factory Default Configuration」（P.2-3）
- 「Save Running Configuration to TFTP Server」（P.2-4）
- 「Save Internal Log Buffer to Flash」（P.2-5）
- 「コマンドライン インターフェイス」（P.2-5）
- 「Show Commands Ignored by ASDM on Device」（P.2-7）

Reset Device to the Factory Default Configuration

デフォルト コンフィギュレーションには、ASDM を使用して適応型セキュリティ アプライアンスに接続するために必要な最小限のコマンドが含まれています。

（注）　この機能は、ルーテッド ファイアウォール モードでのみ使用できます。トランスペアレント モードの場合、インターフェイスの IP アドレスがサポートされません。さらに、この機能はシングル コンテキスト モードでのみ使用できます。コンフィギュレーションがクリアされたセキュリティ アプライアンスには、この機能を使用して自動的に設定する定義済みのコンテキストがありません。

適応型セキュリティ アプライアンスを工場出荷時のデフォルト コンフィギュレーションにリセットするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Reset Device to the Factory Default Configuration] の順に選択します。

[Reset Device to the Default Configuration] ダイアログボックスが表示されます。

ステップ 2　デフォルト アドレスの 192.168.1.1 を使用する代わりに、管理インターフェイスの管理 IP アドレスを入力します。専用管理インターフェイスを備える適応型セキュリティ アプライアンスの場合、そのインターフェイスは「Management0/0」と呼ばれます。他の適応型セキュリティ アプライアンスの場合、設定済みインターフェイスは Ethernet 1 で、「inside」と呼ばれます。

ステップ 3　ドロップダウン リストから [Management（または Inside）Subnet Mask] を選択します。

ステップ 4　この設定を内部フラッシュ メモリに保存するには、[File] > [Save Running Configuration to Flash] を選択します。このオプションを選択すると、以前にシステム時刻で別の場所を設定している場合でも、実行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のデフォルトの場所に保存されます。コンフィギュレーションをクリアした場合は、このパスもクリアされています。工場出荷時のコンフィギュレーションの復元後、適応型セキュリティ アプライアンスを次回にリロードするときに、内部フラッシュ メモリの最初のイメージからこのデバイスがブートします。内部フラッシュ メモリにイメージがない場合、適応型セキュリティ アプライアンスはブートしません。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Save Running Configuration to TFTP Server

この機能により、現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバに保存します。

実行コンフィギュレーションを TFTP サーバに保存するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Save Running Configuration to TFTP Server] の順に選択します。

[Save Running Configuration to TFTP Server] ダイアログボックスが表示されます。

ステップ 2　TFTP サーバの IP アドレスと、コンフィギュレーション ファイルの保存先となる TFTP サーバ上のファイル パスを入力して、[Save Configuration] をクリックします。

（注）　デフォルトの TFTP 設定を行うには、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択します。この設定を行った後は、このダイアログボックスに、TFTP サーバの IP アドレスと TFTP サーバ上でのファイル パスが自動的に表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

Save Internal Log Buffer to Flash

この機能により、内部ログ バッファをフラッシュ メモリに保存できます。

内部ログ バッファをフラッシュ メモリに保存するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Save Internal Log Buffer to Flash] の順に選択します。

[Enter Log File Name] ダイアログボックスが表示されます。

ステップ 2　最初のオプションを選択し、LOG-YYYY-MM-DD-hhmmss.txt 形式のデフォルト ファイル名でログ バッファを保存します。

ステップ 3　2 番目のオプションを選択し、そのログ バッファのファイル名を指定します。

ステップ 4　ログ バッファのファイル名を入力して [OK] をクリックします。

コマンドライン インターフェイス

この機能には、コマンドを適応型セキュリティ アプライアンスに送信して結果を表示する、テキストベースのツールが用意されています。

CLI ツールによって入力可能なコマンドは、ユーザ権限によって異なります。詳細については、[システム管理者用 AAA の設定] ペインを参照してください。 メイン ASDM アプリケーション ウィンドウの下部にあるステータスバーの権限レベルを見て、CLI 特権コマンドを実行するために必要な特権があるかどうかを確認してください。

（注）　ASDM の CLI ツールから入力したコマンドは、適応型セキュリティ アプライアンスの接続ターミナルから入力したコマンドと異なる動作をする場合があります。

CLI ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Command Line Interface] の順に選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 2　必要なコマンドのタイプ（1 行または複数行）を選択し、ドロップダウン リストからコマンドを選択するか、または表示されたフィールドにコマンドを入力します。

ステップ 3　[Send] をクリックしてコマンドを実行します。

ステップ 4　新しいコマンドを入力するには、[Clear Response] をクリックしてから、実行する別のコマンドを選択（または入力）します。

ステップ 5　この機能の状況依存ヘルプを表示するには、[Enable context-sensitive help (?)] チェックボックスをオンにします。文脈依存ヘルプをディセーブルにするには、このチェックボックスをオフにします。

ステップ 6　設定を変更した場合は、[Command Line Interface] ダイアログボックスを閉じた後に、[Refresh] をクリックして ASDM での変更内容を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

コマンド エラー

誤った入力コマンドによってエラーが発生した場合、その誤ったコマンドはスキップされ、その他のコマンドは処理されます。[Response] 領域には、他の関連情報とともに、エラーが発生したかどうかについての情報を示すメッセージが表示されます。

（注）　ASDM は、ほとんどすべての CLI コマンドをサポートしています。コマンドのリストについては、『*Cisco Security Appliance Command Reference*』を参照してください。

インタラクティブ コマンド

インタラクティブ コマンドは、CLI ツールではサポートされていません。これらのコマンドを ASDM で使用するには、次のコマンドに示すように、**noconfirm** キーワード（使用できる場合）を使用します。

```
crypto key generate rsa modulus 1024 noconfirm
```

管理者間の競合の回避

管理者権限を持つ複数のユーザが、適応型セキュリティ アプライアンスの実行コンフィギュレーションをアップデートできます。ASDM の CLI ツールでコンフィギュレーションを変更する場合は、アクティブな管理セッションが他にないことを事前に確認してください。複数のユーザが同時に適応型セキュリティ アプライアンスを設定する場合は、最新の変更が有効になります。

同じ適応型セキュリティ アプライアンスで現在アクティブな他の管理セッションを表示するには、[Monitoring] > [Properties] > [Device Access] の順に選択します。

Show Commands Ignored by ASDM on Device

この機能により、ASDM がサポートしていないコマンドの一覧を表示できます。通常 ASDM は、これらのコマンドを無視します。ASDM は、ユーザの実行コンフィギュレーションのコマンドを変更、削除することはありません。詳細については、「サポートされていないコマンド」を参照してください。

ASDM でサポートされていないコマンドの一覧を表示するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Show Commands Ignored by ASDM on Device] の順に選択します。

ステップ 2　完了したら、[OK] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

診断ツール

ASDM には、問題のトラブルシューティングで使用できる診断ツール セットがあります。この項では、次のトピックについて取り上げます。

- 「Packet Tracer」（P.2-7）
- 「ping」（P.2-8）
- 「traceroute」（P.2-11）
- 「管理者によるクライアントレス SSL VPN ユーザへのアラート」（P.2-12）
- 「ASDM Java コンソール」（P.2-13）
- 「Packet Capture Wizard」（P.2-13）

Packet Tracer

パケット トレーサ ツールは、パケット スニフィングとネットワーク障害箇所特定のためのパケット追跡を実現するとともに、パケットに関する詳細情報と適応型セキュリティ アプライアンスによるパケットの処理方法を示します。コンフィギュレーション コマンドによってパケットがドロップされたのではない場合、パケット トレーサ ツールは、その原因に関する情報をわかりやすく提供します。たとえば、無効なヘッダー検証が原因でパケットがドロップされた場合は、次のメッセージが表示されます。

```
“packet dropped due to bad ip header (reason).”
```

パケットをキャプチャするだけでなく、適応型セキュリティ アプライアンスを使用してパケットの一部始終をトレースし、パケットが想定どおり動作するかどうかを確認できます。パケット トレーサ ツールでは次のことができます。

- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適切なルールと、ルールを追加する CLI 行の表示
- データ パス内でのパケット変化を時系列で表示する。
- データ パスでパケットをトレースします。

パケット トレーサを開くには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Packet Tracer] の順に選択します。

[Cisco ASDM Packet Tracer] ダイアログボックスが表示されます。

ステップ 2　ドロップダウン リストからパケット トレースの送信元インターフェイスを選択します。

ステップ 3　パケット トレースのプロトコル タイプを指定します。指定できるプロトコル タイプは、ICMP、IP、TCP、および UDP です。

ステップ 4　[Source IP Address] フィールドにパケット トレースの送信元アドレスを入力します。

ステップ 5　ドロップダウン リストからパケット トレースの送信元ポートを選択します。

ステップ 6　[Destination IP Address] フィールドに、パケット トレースの宛先 IP アドレスを入力します。

ステップ 7　ドロップダウン リストからパケット トレースの宛先ポートを選択します。

ステップ 8　[Start] をクリックして、パケットをトレースします。

[Information Display Area] に、パケット トレースの詳細情報が表示されます。

（注）　パケット トレースをグラフィカルに表現するには、[Show animation] チェックボックスをオンにします。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

ping

ping ツールは、適応型セキュリティ アプライアンスおよび関係する通信リンクのコンフィギュレーションおよび動作を検証する場合、また他のネットワーク デバイスをテストする場合に便利です。

ping が IP アドレスに送信されると、応答が返されます。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。

ping ツールでは、ICMP（RFC-777 および RFC-792 に記載）を使用して、2 つのネットワーク デバイス間でのエコー要求とエコー応答のトランザクションを定義します。エコー要求パケットは、ネットワーク デバイスの IP アドレスへ送信されます。受信側のデバイスは送信元と宛先のアドレスを逆にしてから、そのパケットをエコー応答として送り返します。

ping ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Ping] の順に選択します。

[Ping] ダイアログボックスが表示されます。

ステップ 2　[IP Address] フィールドに、ICMP エコー要求パケットの宛先 IP アドレスを入力します。

（注）　[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] ペインでホスト名が割り当てられている場合は、IP アドレスの代わりにホスト名を使用できます。

ステップ 3　（任意）ドロップダウン リストから、エコー要求パケットを送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選択します。指定しない場合、セキュリティ アプライアンスはルーティング テーブルを調べ、宛先アドレスを見つけて必要なインターフェイスを使用します。

ステップ 4　[Ping] をクリックして、指定したインターフェイスまたはデフォルトのインターフェイスから、指定した IP アドレスに ICMP エコー要求パケットを送信し、応答タイマーを開始します。

応答は [Ping Output] 領域に表示されます。IP アドレスへの ping は 3 回送信され、結果は次のフィールドに表示されます。

- ping が送信されたデバイスの IP アドレスまたはデバイス名（設定されている場合）。ホストやネットワークに割り当てたデバイス名は、結果が「NO response」でも表示される場合があります。
- ping が送信されると、指定した最大値つまりタイムアウト値でミリ秒タイマーが作動します。このタイマーは、異なるルートやアクティビティ レベルの相対応答時間をテストするのに便利です。
- ping の実行結果の例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
If the ping fails, the output is as follows:
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ステップ 5　新しい IP アドレスを入力するには、[Clear Screen] をクリックして、[Ping Output] 領域から前の応答を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

ping ツールの使い方

管理者は、次の方法で ASDM の ping インタラクティブ診断ツールを使用できます。

- 2 つのインターフェイス間のループバック テスト：同じセキュリティ アプライアンスで一方のインターフェイスから相手側のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。
- セキュリティ アプライアンスへの ping 送信：ping ツールにより、別のセキュリティ アプライアンスのインターフェイスに ping を送信し、そのインターフェイスがアップしていて応答することを確認できます。
- セキュリティ アプライアンスを通過する ping 送信：ping ツールから発信した ping パケットは、デバイスに向かう途中、中間にあるセキュリティ アプライアンスを通過する場合があります。エコー パケットは、返されるときにそのインターフェイスを両方とも通過します。この手順によって、中間にある装置のインターフェイス、動作、応答時間についての基本的なテストができます。
- ネットワーク デバイスの疑わしい動作をテストするための ping 送信：正常に機能していないと思われるネットワーク デバイスに対して、適応型セキュリティ アプライアンスのインターフェイスから ping を送信できます。インターフェイスが正しく設定されているにもかかわらずエコーを受信しない場合は、デバイスに問題があると考えられます。
- 中間の通信状態をテストする場合の ping 送信：正常に機能し、エコー要求を返すことがわかっているネットワーク デバイスに対して、適応型セキュリティ アプライアンスのインターフェイスから ping を送信できます。エコーを受信した場合、中間にあるデバイスがすべて正常に動作し、物理的に正しく接続されていることが確認されたことになります。

ping ツールのトラブルシューティング

ping を送信してエコーを受信しない場合は、適応型セキュリティ アプライアンスのコンフィギュレーションまたは動作にエラーがあることも原因として考えられます。必ずしも ping を送信した IP アドレスから応答がないことが原因であるとは限りません。ping ツールを使用して、適応型セキュリティ アプライアンスのインターフェイスから、インターフェイスに、またはインターフェイスを通過させて ping を送信する前に、次の基本的な確認を行ってください。

- [Configuration] > [Device Setup] > [Interfaces] の順に選択して、インターフェイスが設定されていることを確認します。
- スイッチやルータなど通信パスの中間デバイスで、他のタイプのネットワーク トラフィックが正常に配信されていることを確認します。
- [Monitoring] > [Interfaces] > [Interface Graphs] の順に選択して、「既知の正常な」送信元からの他のタイプのトラフィックが通過することを確認します。

セキュリティ アプライアンスのインターフェイスからの ping 送信

インターフェイスの基本的なテストを行う場合は、正常に機能し、中間通信パスを経由して応答を返すことがわかっているネットワーク デバイスに対して、適応型セキュリティ アプライアンスのインターフェイスから ping 送信を開始できます。基本的なテストの場合は、次の手順を必ず実行してください。

- 「既知の正常な」デバイスが、適応型セキュリティ アプライアンスのインターフェイスから送信された ping を受信することを確認します。ping を受信しない場合は、送信ハードウェアまたはインターフェイスのコンフィギュレーションに問題がある可能性があります。
- 適応型セキュリティ アプライアンスのインターフェイスが正しく設定されているにもかかわらず、「既知の正常な」デバイスからエコー応答を受信しない場合は、インターフェイス ハードウェアの受信機能に問題があると考えられます。「既知の正常な」受信機能を持つ別のインターフェイスで、同じ「既知の正常な」デバイスに対して ping を送信してエコーを受信できる場合、最初のインターフェイスのハードウェアの受信機能に問題があると確認されたことになります。

セキュリティ アプライアンスのインターフェイスへの ping 送信

適応型セキュリティ アプライアンスのインターフェイスに ping を送信しようとする場合は、[Tools] > [Ping] の順に選択して、そのインターフェイスで ping 応答（ICMP エコー応答）がイネーブルになっていることを確認してください。ping 機能がディセーブルになっていると、適応型セキュリティ アプライアンスは他のデバイスやソフトウェア アプリケーションから検出されず、ASDM の ping ツールに応答しません。

セキュリティ アプライアンス経由の ping の実行

「既知の正常な」送信元からの他のタイプのネットワーク トラフィックが適応型セキュリティ アプライアンスを通過していることを確認するには、[Monitoring] > [Interfaces] > [Interface Graphs] または SNMP 管理ステーションを選択します。

内部ホストから外部ホストへの ping 送信をイネーブルにするには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] の順に選択して、内部および外部インターフェイスの両方の ICMP アクセスを正しく設定します。

traceroute

Traceroute ツールにより、パケットが宛先に到着するまでのルートを判断できます。このツールは、送信される各プローブの結果を出力します。出力の各行が 1 つの TTL 値に対応します（昇順）。次の表に、このツールによって出力される記号の一覧を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP プロトコルに到達できません。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

Traceroute ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Traceroute] の順に選択します。

[Traceroute] ダイアログボックスが表示されます。

ステップ 2　ルート トレースの対象となるホストの名前を入力します。ホスト名が指定されている場合は、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] の順に選択して名前を定義するか、またはこのツールをイネーブルにするように DNS サーバを設定して、ホスト名を IP アドレスに解決します。

ステップ 3　応答を待機しているときの接続タイムアウト時間を秒単位で入力します。デフォルトは 3 秒です。

ステップ 4　UDP プローブ メッセージで使用される宛先ポートを入力します。デフォルト値は 33434 です。

ステップ 5　各 TTL レベルで送信されるプローブ数を入力します。デフォルトは 3 です。

ステップ 6　最初のプローブの最小および最大 TTL 値を指定します。デフォルトの最小値は 1 です。値を大きくすると、始めに表示される既知のホップが少なくなります。デフォルトの最大値は 30 です。トレースルートは、パケットが宛先に到達するか、または最大値に達すると終了します。

ステップ 7　UDP プローブ メッセージで使用される宛先ポートを入力します。デフォルト値は 33434 です。

ステップ 8　ドロップダウン リストから、パケット トレースの送信元インターフェイスまたは IP アドレスを選択します。この IP アドレスはいずれかのインターフェイスの IP アドレスにする必要があります。トランスペアレント モードでは、適応型セキュリティ アプライアンスの管理 IP アドレスにする必要があります。

ステップ 9　名前解決が設定されている場合、使用されたホップ名を出力結果に表示するには、[Reverse Resolve] チェックボックスをオンにします。出力結果に IP アドレスを表示するには、このチェックボックスをオフにします。

ステップ 10　UDP プローブ パケットの代わりに ICMP プローブ パケットを使用するよう指定するには、[Use ICMP] チェックボックスをオンにします。

ステップ 11　[Trace Route] をクリックしてトレースルートを開始します。

[Traceroute Output] 領域に、トレースルートの結果についての詳細なメッセージが表示されます。

ステップ 12　[Clear Output] をクリックして新しいトレースルートを開始します。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

管理者によるクライアントレス SSL VPN ユーザへのアラート

この機能により、クライアントレス SSL VPN ユーザにアラート メッセージ（たとえば、接続ステータスについて）を送信できます。

アラート メッセージを送信するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Administrator's Alert Message to Clientless SSL VPN Users] の順に選択します。

[Administrator's Alert Message to Clientless SSL VPN Users] ダイアログボックスが表示されます。

ステップ 2　送信する新規または編集済みのアラート内容を入力して、[Post Alert] をクリックします。

ステップ 3　現在のアラート内容を削除して新しいアラート内容を入力するには、[Cancel Alert] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

ASDM Java コンソール

ASDM Java コンソールを使用して、ASDM エラーのトラブルシューティングに役立つ、記録されたエントリをテキスト形式で表示およびコピーできます。このツールにアクセスするには、メイン ASDM アプリケーション ウィンドウで、[Tools] > [ASDM Java Console] の順に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

Packet Capture Wizard

Packet Capture Wizard を使用して、エラーのトラブルシューティングを行う場合のキャプチャを設定および実行できます。キャプチャでは、アクセス リストを使用して、送信元と宛先のアドレスとポート、および 1 つ以上のインターフェイスにキャプチャされるトラフィックのタイプを制限できます。このウィザードは、入出力インターフェイスのそれぞれでキャプチャを 1 回実行します。キャプチャしたパケットは、PC に保存してパケット アナライザで分析できます。

（注）　このツールは、クライアントレス SSL VPN キャプチャをサポートしていません。

キャプチャを設定および実行するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Wizards] > [Packet Capture Wizard] の順に選択します。

[Overview of Packet Capture] 画面には、ウィザードを完了するまでに行うタスクの一覧が表示されます。

ステップ 2　[Next] をクリックして [Ingress Traffic Selector] 画面を表示します。

ステップ 3　ドロップダウン リストから、入力インターフェイス（内部または外部）を選択します。

ステップ 4　送信元ホストの IP アドレスを入力し、ドロップダウン リストからネットワーク IP アドレスを選択します。

ステップ 5　ドロップダウン リストからプロトコルを選択します。

ステップ 6　選択したプロトコルによっては、送信元ポートのサービスと宛先ポートのサービスの両方を定義する必要もあります。次のいずれかのオプションを選択します。

- All Services
- Service group（ドロップダウン リストから選択）
- Service（事前定義済みパラメータのセットに従って選択）

ステップ 7　[Next] をクリックして、[Egress Traffic Selector] 画面を表示します。

ステップ 8　ドロップダウン リストから出力インターフェイスを選択します。

ステップ 9　送信元ホストの IP アドレスを入力し、ドロップダウン リストからネットワーク IP アドレスを選択します。

（注）　送信元ポートのサービスおよび宛先ポートのサービスは、[Ingress Traffic Selector] 画面での選択に基づいて読み取り専用になります。

ステップ 10　[Next] をクリックして [Buffers] 画面を表示します。バッファ サイズは、キャプチャがパケットを保存するために使用可能なメモリの最大容量です。パケット サイズは、キャプチャが保持できる最長のパケットです。できる限り多くの情報をキャプチャするため、最長パケット サイズを使用することを推奨します。

ステップ 11　パケット サイズを入力します。有効なサイズ範囲は 14 ～ 1522 バイトです。

ステップ 12　バッファ サイズを入力します。有効なサイズ範囲は 1534 ～ 33554432 バイトです。

ステップ 13　キャプチャされたパケットを保存するには、[Use circular buffer] チェックボックスをオンにします。

（注）　この設定を選択すると、すべてのバッファ ストレージが使用されている場合、キャプチャは最も古いパケットへの上書きを始めます。

ステップ 14　[Next] をクリックして [Summary] 画面を表示します。画面に、入力したトラフィック セレクタとバッファ パラメータが表示されます。

ステップ 15　[Next] をクリックして [Run Capture] 画面を表示し、次に [Start] をクリックしてパケットのキャプチャを開始します。[Stop] をクリックしてキャプチャを終了します。

ステップ 16　残りのバッファ スペースを確認するには、[Get Capture Buffer] をクリックします。現在のパケットの内容を削除して、バッファに別のパケットをキャプチャするスペースを確保するには、[Clear Buffer on Device] をクリックします。

ステップ 17　[Save captures] をクリックして、[Save Capture] ダイアログボックスを表示します。キャプチャしたパケットを保存するときの形式として、[ASCII] または [PCAP] を選択します。入力キャプチャ、出力キャプチャ、またはその両方を保存するオプションを選択できます。

ステップ 18　入力パケット キャプチャを保存するには、[Save Ingress Capture] をクリックして [Save capture file] ダイアログボックスを表示します。PC 上でのストレージの場所を指定し、[Save] をクリックします。

ステップ 19　出力パケット キャプチャを保存するには、[Save Egress Capture] をクリックして [Save capture file] ダイアログボックスを表示します。PC 上でのストレージの場所を指定し、[Save] をクリックします。

ステップ 20　[Close] をクリックし、次に [Finish] をクリックしてウィザードを終了します。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

Packet Capture Wizard のフィールド情報

ここでは、次の内容について説明します。

Ingress Traffic Selector

[Ingress Traffic Selector] ダイアログボックスでは、パケット キャプチャの入力インターフェイス、送信元と宛先のホスト/ネットワーク、およびプロトコルを設定できます。

フィールド

- [Ingress Interface]：入力インターフェイス名を指定します。
- [Source Host/Network]：入力送信元ホストおよびネットワークを指定します。
- [Destination Host/Network]：入力宛先ホストおよびネットワークを指定します。
- [Protocol]：キャプチャするプロトコル タイプを指定します（ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snp、tcp、または udp）。
  - [ICMP type]：ICMP プロトコルのみの ICMP タイプを指定します（all、alternate address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute、または unreachable）。
  - [Source/Destination Port Services]：TCP および UDP プロトコルのみの送信元および宛先ポートのサービスを指定します。

[All Services]：すべてのサービスを指定します。

[Service Group]：サービス グループを指定します。

[Service]：サービスを指定します（aol、bgp、chargen、cifx、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、kerberos、klogin、kshell、ldap、ldaps、login、lotusnotes、lpd、netbios-ssn、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpc、tacacs、talk、telnet、uucp、または whois）。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Egress Traffic Selector

[Egress Traffic Selector] ダイアログボックスでは、パケット キャプチャの出力インターフェイス、送信元と宛先のホスト / ネットワーク、および送信元と宛先ポートのサービスを設定できます。

フィールド

- [Egress Interface]：出力インターフェイス名を指定します。
- [Source Host/Network]：出力送信元ホストおよびネットワークを指定します。
- [Destination Host/Network]：出力宛先ホストおよびネットワークを指定します。
- [Protocol]：入力設定時に選択したプロトコル タイプを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Buffers

[Buffers] ダイアログボックスでは、パケット キャプチャのパケット サイズ、バッファ サイズ、および循環バッファを使用するかどうかを設定できます。

フィールド

- [Packet Size]：キャプチャが保持できる最長のパケットを指定します。できるだけ多くの情報をキャプチャするために、指定可能な最長サイズを使用してください。

- [Buffer Size]：パケットを保存するためにキャプチャが使用できるメモリの最大容量を指定します。
- [Use circular buffer]：パケットの保存に循環バッファを使用するかどうかを指定します。循環バッファのバッファ ストレージがすべて使い尽くされると、キャプチャは最も古いパケットから上書きを始めます。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Summary

[Summary] ダイアログボックスには、パケット キャプチャのトラフィック セレクタおよびバッファ パラメータが表示されます。

フィールド

- [Traffic Selectors]：前の手順で指定したキャプチャおよびアクセス リストのコンフィギュレーションを表示します。
- [Buffer Parameters]：前の手順で指定したバッファ パラメータを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

キャプチャの実行

[Run Captures] ダイアログボックスでは、キャプチャ セッションを開始および停止できます。また、キャプチャ バッファの表示、ネットワーク アナライザ アプリケーションの起動、パケット キャプチャの保存、およびバッファのクリアも実行できます。

フィールド

- [Start]：選択したインターフェイスでパケット キャプチャ セッションを開始します。
- [Stop]：選択したインターフェイスでキャプチャ セッションを停止します。
- [Get Capture Buffer]：インターフェイスでキャプチャされたパケットのスナップショットを表示するよう指定します。
- [Ingress]：入力インターフェイスでのキャプチャ バッファを表示します。

  - [Launch Network Sniffer Application]：入力キャプチャを分析する場合に、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動します。
- [Egress]：出力インターフェイスでのキャプチャ バッファを表示します。
  - [Launch Network Sniffer Application]：出力キャプチャを分析する場合に、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動します。
- [Save Captures]：入力キャプチャと出力キャプチャを ASCII または PCAP 形式で保存できます。
- [Clear Buffer on Device]：デバイスのバッファをクリアします。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

キャプチャの保存

[Save Captures] ダイアログボックスでは、パケットをさらに分析するために、入力および出力パケット キャプチャを ASCII または PCAP ファイル形式で保存できます。

フィールド

- [ASCII]：キャプチャ バッファを ASCII 形式で保存する場合に指定します。
- [PCAP]：キャプチャ バッファを PCAP 形式で保存する場合に指定します。
- [Save ingress capture]：入力パケット キャプチャを保存するファイルを指定します。
- [Save egress capture]：出力パケット キャプチャを保存するファイルを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ファイル管理ツール

ASDM には、基本的なファイル管理タスクを実行するのに便利なファイル管理ツール セットが用意されています。この項では、次のトピックについて取り上げます。

- 「File Management」（P.2-19）
- 「Manage Mount Points」（P.2-20）

File Management

ファイル管理ツールにより、フラッシュ メモリに保存されているファイルの表示、移動、コピー、および削除、ファイルの転送、およびリモート ストレージ デバイス（マウント ポイント）のファイルの管理を行うことができます。

（注） マルチコンテキスト モードの場合、このツールはシステムのセキュリティ コンテキストでだけ使用できます。

ファイル管理ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [File Management] の順に選択します。

[File Management] ダイアログボックスが表示されます。

- [Folders] ペインには、ディスク上にあるフォルダが表示されます。
- [Flash Space] は、フラッシュ メモリの合計容量と、使用可能なメモリ容量を示します。
- [Files] 領域には、選択したフォルダのファイルについて次の情報が表示されます。
  - パス
  - ファイル名
  - サイズ（バイト単位）
  - 修正時刻
  - 選択したファイルの種類（ブート コンフィギュレーション、ブート イメージ ファイル、ASDM イメージ ファイル、SVC イメージ ファイル、CSD イメージ ファイル、または APCF イメージ ファイル）を示す、ステータス

ステップ 2　選択したファイルをブラウザに表示するには、[View] をクリックします。

ステップ 3　選択したファイルを切り取って別のディレクトリに貼り付けるには、[Cut] をクリックします。

ステップ 4　選択したファイルをコピーして別のディレクトリに貼り付けるには、[Copy] をクリックします。

ステップ 5　コピーしたファイルを選択した場所に貼り付けるには、[Paste] をクリックします。

ステップ 6　選択したファイルをフラッシュ メモリから削除するには、[Delete] をクリックします。

ステップ 7　ファイルの名前を変更するには、[Rename] をクリックします。

ステップ 8　ファイルを保存するディレクトリを新規作成するには、[New Directory] をクリックします。

ステップ 9　[File Transfer] ダイアログボックスを開くには、[File Transfer] をクリックします。詳細については、「File Transfer」（P.2-23）を参照してください。

ステップ 10　[Manage Points] ダイアログボックスを開くには、[Mount Points] をクリックします。詳細については、「Manage Mount Points」（P.2-20）を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Manage Mount Points

この機能により、CIFS または FTP 接続を使用して、ネットワーク ファイル システムのリモート ストレージ（マウント ポイント）を設定できます。このダイアログボックスには、マウント ポイント、接続タイプ、サーバ名または IP アドレス、およびイネーブルにされた設定（yes または no）の一覧が表示されます。マウント ポイントは、追加、編集、または削除できます。詳細については、「CIFS/FTP マウント ポイントの追加 / 編集」（P.2-20）を参照してください。作成後に、CIFS マウント ポイントにアクセスできます。詳細については、「CIFS マウント ポイントのアクセス」（P.2-21）を参照してください。

（注）　シングル ルーテッド モードの PIX 535 セキュリティ アプライアンスでは、Manage Mount Point 機能を使用できません。

CIFS/FTP マウント ポイントの追加 / 編集

CIFS マウント ポイントを追加するには、次の手順を実行します。

ステップ 1　[Add] をクリックし、[CIFS Mount Point] を選択します。

[Add CIFS Mount Point] ダイアログボックスが表示されます。

[Enable mount point] チェックボックスは、デフォルトで自動的にオンになります。

ステップ 2　該当するフィールドに、マウント ポイント、サーバ名または IP アドレス、および共有名を入力します。

ステップ 3　[Authentication] セクションで、NT ドメイン、ユーザ名、およびパスワードを入力し、続いてパスワードを確認します。

ステップ 4　[OK] をクリックします。

FTP マウント ポイントを追加するには、次の手順を実行します。

ステップ 1　[Add] をクリックし、[FTP Mount Point] を選択します。

[Add FTP Mount Point] ダイアログボックスが表示されます。

[Enable mount point] チェックボックスは、デフォルトで自動的にオンになります。

ステップ 2　該当するフィールドに、マウント ポイント名と、サーバ名または IP アドレスを入力します。

ステップ 3　[FTP Mount Options] セクションで、[Active Mode] または [Passive Mode] オプションを選択します。

ステップ 4　リモート ストレージをマウントするパスを入力します。

ステップ 5　[Authentication] セクションで、NT ドメイン、ユーザ名、およびパスワードを入力し、続いてパスワードを確認します。

ステップ 6　[OK] をクリックします。

CIFS マウント ポイントを編集するには、次の手順を実行します。

ステップ 1　変更する CIFS マウント ポイントを選択し、[Edit] をクリックします。

[Edit CIFS Mount Point] ダイアログボックスが表示されます。

（注）　CIFS マウント ポイントは変更できません。

ステップ 2　残りの設定に変更を加え、変更が済んだら [OK] をクリックします。

FTP マウント ポイントを編集するには、次の手順を実行します。

ステップ 1　変更する FTP マウント ポイントを選択し、[Edit] をクリックします。

[Edit FTP Mount Point] ダイアログボックスが表示されます。

（注）　FTP マウント ポイントは変更できません。

ステップ 2　残りの設定に変更を加え、変更が済んだら [OK] をクリックします。

CIFS マウント ポイントのアクセス

作成後に CIFS マウント ポイントにアクセスするには、次の手順を実行します。

ステップ 1　セキュリティ アプライアンス CLI を起動します。

ステップ 2　**mount <name of mount> type cifs** コマンドを入力し、マウントを作成します。

ステップ 3　**show run mount** コマンドを入力します。

次の出力が表示されます。

（注）　この例では、マウント名は win2003 です。

```
server kmmwin2003
share sharefolder
username webvpnuser2
password ********
status enable
```

ステップ 4　**dir** コマンドを入力し、イネーブルになっているすべてのマウントをサブディレクトリとして表示します。これは、Windows PC でドライブをマウントするのに似ています。たとえば、次の出力結果 FTP2003:、FTPLINUX:、win2K: は設定されたマウントです。

次に、**dir** コマンドの出力例を示します。

```
FTP2003: Directory or file name
FTPLINUX: Directory or file name
WIN2003: Directory or file name
all-filesystems List files on all filesystems
disk0: Directory or file name
disk1: Directory or file name
flash: Directory or file name
system: Directory or file name
win2K: Directory or file name
```

ステップ 5　そのマウントに対して **dir** コマンドを入力します（たとえば、**dir WIN2003**）。そして、フラッシュ メモリ（disk0:）からリストされたマウントのいずれかへ、またはマウントからフラッシュメモリへファイルをコピーします。

次に、**dir WIN2003** コマンドの出力例を示します。

```
Directory of WIN2003:/
---- 14920928 08:33:36 Apr 03 2009 1_5_0_01-windows-i586-p.exe
---- 33 11:27:16 Jun 07 2007 AArenameIE70
---- 28213021 15:15:22 Apr 03 2009 atest2(3).bin
---- 61946730 12:09:40 Mar 17 2009 atest2.bin
---- 5398366 14:52:10 Jul 28 2008 atest222.bin
---- 2587728 10:07:44 Dec 06 2005 cCITRIXICA32t.exe
---- 1499578 15:26:50 Dec 02 2005 ccore.exe
---- 61946728 11:40:36 Dec 09 2005 CIFSTESTT.bin
---- 2828 13:46:04 May 11 2009 ClientCert.pfx
d--- 16384 14:48:28 Mar 20 2007 cookiefolder
---- 4399 15:58:46 Jan 06 2006 Cookies.plist
---- 2781710 12:35:00 Dec 12 2006 coreftplite1.3.exe
---- 0 10:22:52 Jul 13 2007 coreftplite1.3.exe.download
---- 245760 15:13:38 Dec 21 2005 Dbgview.exe
---- 1408249 11:01:34 Dec 08 2005 expect-5.21r1b1-setup.exe
d--- 16384 14:49:14 Jul 28 2008 folder157
---- 101 09:33:48 Dec 12 2005 FxSasser.log
---- 2307104 09:54:12 Dec 12 2005 ica32t.exe
---- 8732552 10:14:32 Apr 29 2009 iclientSetup_IFen_flex51.exe
d--- 16384 08:32:46 Apr 03 2009 IE8withVistaTitan
---- 15955208 08:34:18 Aug 14 2007 j2re.exe
---- 16781620 13:38:22 Jul 23 2008 jre-1_5_0_06-windows-i586-p.exe
<--- More --->
```

Upgrade Software from Local Computer

Upgrade Software from Local Computer ツールにより、PC からフラッシュ ファイル システムにイメージ ファイルをアップロードし、適応型セキュリティ アプライアンスをアップグレードできます。

PC からソフトウェアをアップグレードするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] の順に選択します。

[Upgrade Software from Local Computer] ダイアログボックスが表示されます。

ステップ 2　ドロップダウン リストから、アップロードするイメージ ファイルを選択します。

ステップ 3　PC 上のファイルへのローカル パスを入力するか、または [Browse Local Files] をクリックして PC 上のファイルを指定します。

ステップ 4　フラッシュ ファイル システムへのパスを入力するか、または [Browse Flash] をクリックしてフラッシュ ファイル システムのディレクトリまたはファイルを指定します。

ステップ 5　[Image to Upload] をクリックします。アップグレード プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

File Transfer

File Transfer ツールにより、HTTP、HTTP over SSL、TFTP、FTP、または SMB を使用して、PC またはフラッシュ ファイル システムのローカル ファイルをセキュリティ アプライアンスとの間でコピーできます。

ファイルを転送するには、次の手順を実行します。

ステップ 1　リモート サーバからファイルを転送するには、[Remote server] オプションを選択します。

ステップ 2　転送対象になるソース ファイルを定義します。

a.　サーバの IP アドレスを含めたファイルの場所へのパスを選択します。

b.　リモート サーバのポート番号またはタイプ（FTP の場合）を入力します。有効な FTP タイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 3　フラッシュ ファイル システムからファイルをコピーするには、[Flash file system] オプションを選択します。

ステップ 4　ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 5　ローカル PC からファイルをコピーするには、[Local computer] オプションを選択します。

ステップ 6　ファイルの場所へのパスを入力するか、[Browse Local Files] をクリックしてファイルの場所を指定します。

ステップ 7　また、CLI により、スタートアップ コンフィギュレーション、実行コンフィギュレーション、または SMB ファイル システムからファイルをコピーすることもできます。**copy** コマンドの使用方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

ステップ 8　転送するファイルの宛先を定義します。

a. フラッシュ ファイル システムにファイルを転送するには、[Flash file system] オプションを選択します。

b. ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 9　リモート サーバにファイルを転送するには、[Remote server] オプションを選択します。

a. ファイルの場所へのパスを入力します。

b. FTP 転送の場合はタイプを入力します。有効なタイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 10　[Transfer File] をクリックしてファイル転送を開始します。ファイル転送プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Upgrade Software from Cisco.com Wizard

Upgrade Software from Cisco.com Wizard により、ASDM および適応型セキュリティ アプライアンスを最新のバージョンに自動的にアップグレードできます。

（注）　この機能は、コンテキスト モードでは使用できません。

このウィザードでは、次の操作を実行できます。

- Cisco.com から使用可能なリリースのリストをダウンロードする。
- アップグレード用の ASDM イメージ ファイルまたは ASA イメージ ファイルを選択する。
- 選択したイメージをアップグレードする。
- ASA イメージをアップグレードした場合はファイアウォールをリロードする（任意）。

（注）　1 つのバージョンから次のバージョンに、順次アップグレードする必要があります（たとえば、バージョン 5.1 から 5.2、バージョン 5.2 から 6.0(2) など）。バージョン 5.1 から 6.0(2) へはアップグレードできません。

Upgrade Software from Cisco.com Wizard を完了するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Cisco.com] の順に選択します。

[Upgrade Software from Cisco.com Wizard] が表示されます。[Overview] 画面に、イメージ アップグレード プロセスの手順が表示されます。

ステップ 2　[Next] をクリックして続行します。

[Authentication] 画面が表示されます。

ステップ 3　割り当てられている Cisco.com ユーザ名、および Cisco.com パスワードを入力し、[Next] をクリックします。

[Image Selection] 画面が表示されます。

ステップ 4　リストにある 2 つのオプションの一方または両方を選択します。

- アップグレードする最新の適応型セキュリティ アプライアンス イメージを指定するには、[Upgrade the ASA version] チェックボックスをオンにします。
- アップグレードする最新の ASDM バージョンを指定するには、[Upgrade the ASDM version] チェックボックスをオンにします。

（注）　ASA バージョン リストまたは ASDM バージョン リストが空の場合は、アップグレード可能な新しい ASA または ASDM イメージはないことを示す文が表示されます。この文が表示されたら、ウィザードを終了できます。

ステップ 5　[Next] をクリックして続行します。

[Selected Images] 画面が表示されます。

ステップ 6　選択したイメージ ファイルが正しいことを確認し、[Next] をクリックしてアップグレードを開始します。

アップグレードに数分かかることを示すメッセージがウィザードに表示されます。アップグレードの進行状況を示すステータスを表示できます。

[Results] 画面が表示されます。この画面には、アップグレードに失敗したかどうか、またはコンフィギュレーションを保存して適応型セキュリティ アプライアンスをリロードするかどうかなどの、詳細な情報が表示されます。

適応型セキュリティ アプライアンスのバージョンをアップグレードし、そのアップグレードに成功した場合は、コンフィギュレーションを保存して適応型セキュリティ アプライアンスをリロードするオプションが表示されます。

ステップ 7　[Yes] をクリックします。

アップグレード バージョンを有効にするには、コンフィギュレーションを保存し、適応型セキュリティ アプライアンスをリロードし、それから ASDM を再起動する必要があります。

（注）　次のバージョンへの 1 回のアップグレードを完了した後にウィザードを再起動する必要はありません。次のバージョンがある場合には、ウィザードの手順 3 に戻り、そのバージョンへのアップグレードを実行できます。

ステップ 8　アップグレードが終了した場合は、[Finish] をクリックしてウィザードを終了します。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

Upload ASDM Assistant Guide

Upload ASDM Assistant Guide ツールにより、特定のタスクについての便利な ASDM の使用方法のヘルプを含む XML ファイルを、フラッシュ メモリにアップロードできます。Cisco.com からファイルを取得できます。

ファイルをアップロードした後は、メニュー バーの [Look For] フィールドから [Help] > [ASDM Assistant] > [How Do I?] を選択して、ファイルの情報にアクセスできます。[Find] ドロップダウン リストで、[How Do I?] を選択して検索を開始します。

ASDM Assistant Guide をアップロードするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upload ASDM Assistant Guide] の順に選択します。

[Upload ASDM Assistant Guide] ダイアログボックスが表示されます。

ステップ 2　[File to Upload] フィールドに、PC 上の XML ファイルの名前を入力するか、または [Browse Local] をクリックしてアップロードする PC 上の XML ファイルを指定します。

ステップ 3　[Flash File System Path] フィールドのドロップダウン リストから、XML ファイルのコピー先となるパスを選択（または入力）します。

ステップ 4　アップロードを開始するには、[Upload File] をクリックします。

（注）　この機能は、PIX セキュリティ アプライアンスでは使用できません。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

System Reload

System Reload ツールにより、システムのリロードをスケジュールしたり、保留中のリロードをキャンセルしたりできます。

リロードのスケジュールを設定するには、次の手順を実行します。

ステップ 1　[Reload Scheduling] セクションで、次のリロード スケジューリング設定を定義します。

a. [Configuration State] では、リロード時に実行コンフィギュレーションを保存するか、またはリロード時に実行コンフィギュレーションに対するコンフィギュレーション変更を破棄するかのどちらかを選択します。

b. [Reload Start Time] では、次のオプションから選択できます。

- リロードをただちに実行するには、[Now] をクリックします。
- 指定した時間だけリロードを遅らせるには、[Delay by] をクリックします。リロード開始までの経過時間を、時間と分単位、または分単位だけで入力します。
- 指定した時刻と日付にリロードを実行するようにスケジュールするには、[Schedule at] をクリックします。リロードの実行時刻を入力し、リロードのスケジュール日を選択します。

c. [Reload Message] フィールドに、リロード時に ASDM の開いているインスタンスに送信するメッセージを入力します。

d. リロードを再試行するまでの経過時間を時間と分単位で、または分単位だけで表示するには、[On reload failure force immediate reload after] チェックボックスをオンにします。

e. 設定に従ってリロードをスケジュールするには、[Schedule Reload] をクリックします。

ステップ 2　[Reload Status] 領域には、リロードのステータスが表示されます。

- スケジュールされたリロードを停止するには、[Cancel Reload] をクリックします。
- スケジュールされたリロードの終了後に [Reload Status] 表示をリフレッシュするには、[Refresh] をクリックします。
- スケジュールされたリロードの詳細を表示するには、[Details] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•