CHAPTER 2

始める前に

ここでは、次の項目について説明します。

ASDM アクセスに対する FWSM の設定

ASDM を使用するには、HTTPS サーバをイネーブルにし、FWSM への HTTPS 接続を許可する必要があります。**setup** コマンドを使用すれば、これらのタスクが実行されます。ここでは、ASDM へのアクセスを手動で設定する方法について説明します。

FWSM は、コンテキストごとに最大 5 つの同時 ASDM インスタンス、およびすべてのコンテキスト間で最大 80 の ASDM インスタンスを許可します。リソース クラスを使用すると、コンテキストごとに許可する ASDM セッションの数を制御できます（P.7-12 の「リソース クラスの設定」を参照）。

ASDM へのアクセスを設定するには、次の手順を実行します。

ステップ 1　FWSM が HTTPS 接続を受け入れる IP アドレスを識別するには、各アドレスまたはサブネットに次のコマンドを入力します。

```
hostname(config)# http source_IP_address mask source_interface
```

ステップ 2　HTTPS サーバをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# http server enable
```

たとえば、HTTPS サーバをイネーブルにし、アドレスが 192.168.1.2 である内部インターフェイスのホストが ASDM にアクセスするには、次のコマンドを入力します。

```
hostname(config)# http server enable
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

192.168.3.0 ネットワークのすべてのユーザに内部インターフェイスの ASDM へのアクセスを許可するには、次のコマンドを入力します。

```
hostname(config)# http 192.168.3.0 255.255.255.0 inside
```

CLI での透過またはルーテッド ファイアウォール モードの設定

ASDM のシングルモードでは、モードの変更はできません。マルチモードでは、ASDM の管理コンテキストモードでのモード変更はできません。CLI でモードの変更をする必要があります。

モードを変更すると、FWSM はコンフィギュレーションをクリアします。これは、多くのコマンドが両方のモードでサポートされていないためです。すでに実装済みのコンフィギュレーションがある場合は、モードを変更する前に必ずコンフィギュレーションのバックアップを作成してください。新しくコンフィギュレーションを作成するときにこのバックアップを参照する場合があります。

firewall transparent コマンドでモードを変更する FWSM にテキスト コンフィギュレーションをダウンロードする場合は、必ずこのコマンドをコンフィギュレーションの最上部に置いてください。これによって、FWSM は、このコマンドを読み取り次第すぐにモードを変更し、その後は、ダウンロードしたコンフィギュレーションの読み取りを続けます。このコマンドがコンフィギュレーションの後ろの方にあると、FWSM はそれ以前に記述されているコンフィギュレーションの行をすべてクリアします。

- 透過モードに設定するには、各コンテキストで次のコマンドを入力します。

  ```
  hostname(config)# firewall transparent
  ```

- ルーテッド モードに設定するには、各コンテキストで次のコマンドを入力します。

  ```
  hostname(config)# no firewall transparent
  ```

ASDM ランチャのダウンロード

ASDM ランチャは Windows 専用です。ASDM ランチャは、ASDM を Java アプレットとして実行する改良点の 1 つです。重複する認証と証明書ダイアログボックスがなくなり、起動が高速化して、入力済みの IP アドレスとユーザ名をキャッシュします。

ASDM ランチャをダウンロードするには、次の手順を実行します。

ステップ 1　FWSM のネットワークでサポートされている Web ブラウザで、次の URL を入力します。

https://*interface_ip_address*

透過ファイアウォール モードでは、管理 IP アドレスを入力します。

（注）　必ず **https** を入力してください。**http** ではありません。

ステップ 2　すべてのプロンプトで **OK**　または **Yes** をクリックします。名前とパスワードのプロンプトでも同様です。デフォルトでは、名前とパスワードは空白にします。

表示されるページに次のボタンがあります。

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

ステップ 3　**Download ASDM Launcher and Start ASDM** をクリックします。

インストーラが PC にダウンロードされます。

ステップ 4　インストーラを実行して ASDM ランチャをインストールします。

ASDM の起動

この項では、ASDM を起動する方法について説明します。起動するには次の方法があります。

ASDM ランチャによる ASDM の起動

ASDM ランチャは Windows 専用です。

ASDM ランチャから ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップ上の Cisco ASDM Launcher のショートカットをダブルクリックするか、または、**Start** メニューから起動します。

ステップ 2　FWSM の IP アドレスまたはホスト名、ユーザ名、パスワードを入力して **OK** をクリックします。

新しいバージョンの ASDM が FWSM にあれば ASDM ランチャが自動的にダウンロードされ、ASDM を起動します。

デモ モードでの ASDM の使用

ASDM デモ モードは、Windows で実行される別のアプリケーションとして使用できます。ASDM ランチャとあらかじめパッケージされているコンフィギュレーション ファイルを使用して、実デバイスを使用せずに ASDM を実行できます。ASDM デモ モードでは次のようなことができます。

- 実デバイス接続時と同じように、ASDM からコンフィギュレーションを実行して監視タスクを選択。
- ASDM インターフェイスによる ASDM または FWSM 機能のデモ。
- Content Security and Control SSM（CSC SSM）使用時のコンフィギュレーションおよび監視タスクの実行。

ASDM デモ モードは、リアルタイムのシステム ログ メッセージを含む監視結果のシミュレーションを提供します。表示データはランダムに生成されますが、実デバイスに接続しているような体験ができます。

ASDM デモ モードでは、次の制限事項があります。

- コンフィギュレーション変更は GUI に表示されますが、コンフィギュレーション ファイルには適用されません。したがって、Refresh ボタンをクリックすると元のコンフィギュレーションに戻ります。変更はコンフィギュレーション ファイルに保存されません。
- ファイルとディスクの操作はサポートされていません。
- 監視データとログ データはシミュレーション結果です。履歴モニタリング データは使用できません。
- admin ユーザのみログインできます。つまり、monitor-only または read-only ユーザでログインできません。
- デモ モードでは、次の機能はサポートされていません。
  - File メニュー
    Save Running Configuration to Flash

Save Running Configuration to TFTP Server
Save Running Configuration to Standby Unit
Save Internal Log Buffer to Flash
Clear Internal Log Buffer

- Tools メニュー

Command Line Interface
Ping
File Management
Update Image
File Transfer
Upload image from Local PC
System Reload

- Toolbar/Status bar > Save
- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Failover：スタンバイ デバイスの設定

- 次の操作を実行すると、コンフィギュレーションの再読み込みが行われ、結果として元のコンフィギュレーションに戻ります。
  - コンテキストの切り換え
  - Interface パネルの変更
  - NAT パネルの変更
  - Clock パネルの変更

ASDM のデモ モードを実行するには、次の手順を実行します。

ステップ 1　デモ モード アプリケーションがインストールされていない場合、次の手順を実行します。

a. ASDM デモ モードのインストーラを、http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm からダウンロードします。

ファイル名は asdm-*version*-demo.msi です。

b. インストーラをダブルクリックして、ソフトウェアをインストールします。

ステップ 2　デスクトップ上の Cisco ASDM Launcher のショートカットをダブルクリックするか、または、**Start** メニューから起動します。

ステップ 3　**Run in Demo Mode** チェックボックスをオンにします。

ステップ 4　プラットフォーム、コンテキスト モード、ファイアウォール モード、ASDM バージョンを設定するには、**Demo** ボタンをクリックして、Demo Mode エリアから選択します。

ステップ 5　更新された ASDM イメージを使用する場合は、最新のインストーラをダウンロードするか、または通常の ASDM イメージをダウンロードしてからデモ モードにインストールします。

a. イメージは http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm からダウンロードできます。

ファイル名は asdm-*version*.bin です。

b. Demo Mode エリアで **Install ASDM Image** をクリックします。

ファイル ブラウザが表示されます。ブラウザで ASDM イメージ ファイルを検索します。

ステップ 6　**OK** をクリックして、ASDM デモ モードを起動します。

ウィンドウのタイトルバーに Demo Mode のラベルが表示されます。

Web ブラウザによる ASDM の起動

Web ブラウザから ASDM を起動するには、次の手順を実行します。

ステップ 1　FWSM のネットワークでサポートされている Web ブラウザで、次の URL を入力します。

https://*interface_ip_address*

透過ファイアウォール モードでは、管理 IP アドレスを入力します。

（注）　必ず **https** を入力してください。**http** ではありません。

ステップ 2　すべてのブラウザのプロンプトで **OK** または **Yes** をクリックします。名前とパスワードのプロンプトでも同様です。デフォルトでは、名前とパスワードは空白にします。

表示されるページに次のボタンがあります。

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

ステップ 3　**Run ASDM as a Java Applet** をクリックします。

ステップ 4　すべての Java プロンプトで **OK** または **Yes** をクリックします。名前とパスワードのプロンプトでも同様です。デフォルトでは、名前とパスワードは空白にします。

History Metrics

History Metrics ペインで、FWSM を設定してさまざまな統計情報の履歴を保存し、ASDM を使用して Graph/Table で表示できます。履歴メトリックをイネーブルにしない場合、監視できるのはリアルタイムの統計情報だけです。履歴メトリックをイネーブルにすると、直前の 10 分間、60 分間、12 時間、5 日間の統計グラフを表示できます。

フィールド

- ASDM History Metrics : 履歴メトリックをイネーブルにします。このチェックボックスをオフにすると、履歴メトリックはクリアされ、ディセーブルになります。

モード

次の表に、この機能を使用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	
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の概要

FWSM を設定および監視するには、次の手順を実行します。

ステップ 1　初期コンフィギュレーションには Startup Wizard を使用します。**Configuration > Properties > Startup Wizard** の順にクリックします。

ステップ 2　高度な機能を設定するには、ツールバーの **Configuration** ボタンをクリックし、機能のボタンをクリックします。次のような機能があります。

- ルーテッド インターフェイスの設定：IP アドレス、名前、セキュリティ レベルなどのインターフェイスの基本パラメータを設定します。透過モードでは、ブリッジ グループのパラメータも設定できます。
- セキュリティ ポリシー：アクセス ルール、AAA ルール、フィルタ ルール、サービス ポリシー ルールがあります。
  - アクセス ルールの設定：FWSM を通過する IP トラフィックを許可または拒否します。透過ファイアウォール モードでは、非 IP トラフィックを許可するための EtherType アクセス リストも適用できます。
  - EtherType ルールの設定（透過モードのみ）：FWSM を通過する IP トラフィック以外を許可または拒否します。
  - AAA Rules：HTTP など特定のタイプのトラフィックに対して、認証と認可のいずれかまたは両方を要求します。FWSM は、RADIUS サーバまたは TACACS+ サーバにアカウンティング情報を送信することもあります。
  - Filter Rules：特定のウェブサイトまたは FTP サーバへの発信アクセスを禁止します。FWSM は、Websense Enterprise または Sentian を N2H2 で実行する別のサーバと連携して動作します。URL フィルタリング サーバを設定するには、**Configuration > Properties > URL Filtering** を参照します。ルールを追加するには、まず設定が必要です。
  - Service Policy Rules：アプリケーション検査、接続の制限、TCP 正規化を適用します。検査エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、FWSM が詳細なパケット検査を行うことが必要となります。TCP 接続、UDP 接続、および初期接続を制限することもできます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 正規化は、正常に見えないパケットをドロップします。
- NAT の設定：保護されたネットワークで使用するアドレスをパブリック インターネットで使用するアドレスに変換します。これによって、プライベート アドレスを内部ネットワークで使用できます。プライベート アドレスは、インターネットにルーティングできません。
- ダイナミック ルーティングおよびスタティック ルーティングの設定：（シングルモードのみ）OSPF、RIP、マルチキャスト、非対称ルーティングを設定します。
- グローバル オブジェクトの追加：FWSM にポリシーを組み込む際に不可欠な再利用コンポーネントの設定、表示、修正がすべてできます。再利用コンポーネントまたはグローバル オブジェクトには、次のものがあります。
  - ネットワーク オブジェクト グループ
  - IP 名
  - サービス グループ
  - 検査マップ
  - 時間範囲

ステップ 3　FWSM を監視するには、ツールバーの **Monitoring** ボタンをクリックし、機能のボタンをクリックします。次のような機能があります。

- インターフェイス：ARP テーブル、DHCP、ダイナミック アクセスリスト、インターフェイスの統計値を監視します。
- ルーティングのモニタリング：ルート、OSPF LSA、OSPF ネイバーを監視します。
- プロパティのモニタリング：管理セッション、AAA　サーバ、フェールオーバー、CRL、DNS キャッシュ、システムの統計情報を監視します。
- システム ログ メッセージのモニタリング：システム ログ メッセージを監視します。
- フェールオーバーのモニタリング：(マルチモードのシステムの場合) システムのフェールオーバーを監視します。