始める前に

ここでは、次の項目について説明します。

工場出荷時のデフォルト コンフィギュレーション

工場出荷時のデフォルト コンフィギュレーションは、シスコが新しいセキュリティ アプライアンスに適用するコンフィギュレーションです。工場出荷時のデフォルト コンフィギュレーションは、PIX 525 および PIX 535 セキュリティ アプライアンスを除くすべてのモデルでサポートされています。

PIX 515/515E および ASA 5510 以降のセキュリティ アプライアンスの場合、ASDM を使用してこれに接続できるように、工場出荷時のデフォルト コンフィギュレーションにより管理用のインターフェイスが設定されます。この設定により、コンフィギュレーションを完了することができます。

ASA 5505 適応型セキュリティ アプライアンスの場合、すぐにセキュリティ アプライアンスがネットワークで利用できるように、工場出荷時のデフォルト コンフィギュレーションによりインターフェイスおよび NAT が設定されます。

工場出荷時のデフォルト コンフィギュレーションは、ルーテッド ファイアウォール モードおよびシングルコンテキスト モードでのみ利用可能です。マルチコンテキスト モードの詳細については、「セキュリティ コンテキストの設定」を参照してください。ルーテッド ファイアウォール モードと透過ファイアウォール モードの詳細については、「ファイアウォール モードの概要」を参照してください。

ここでは、次の項目について説明します。

工場出荷時のデフォルト コンフィギュレーションの復元

工場出荷時のデフォルト コンフィギュレーションを復元するには、次の手順を実行します。

ステップ 1　**File > Reset Device to the Factory Default Configuration** の順に選択します。

ステップ 2　デフォルトの IP アドレスを変更して、使用する IP アドレスを指定するには、<default interface> の **Use this address** チェックボックスをオンにします。<name> チェックボックスに名前が表示されています。

ステップ 3　Management IP Address フィールドに新しい IP アドレスを入力します。

ステップ 4　Management Mask フィールドに新しいサブネット マスクを入力します。

ステップ 5　**OK** をクリックします。

ip_address を指定する場合、デフォルト IP アドレスの 198.168.1.1 を使用するのではなく、ご使用のモデルに応じた内部または管理インターフェイスの IP アドレスを設定してください。**http** は、指定されたサブセットを使用します。同様に、**dhcpd address** コマンドの処理範囲は、指定されたサブセット内のアドレスで構成されます。

工場出荷時のデフォルト コンフィギュレーションの復元後、**write memory** コマンドで内部フラッシュ メモリにこれを保存します。**write memory** コマンドは、実行中の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のデフォルトの場所に保存します。別の場所を設定するために **boot config** コマンドを事前に設定した場合でも同様です。コンフィギュレーションをクリアした場合、このパスもクリアされます。

（注）　また、このコマンドは、**boot system** コマンドが存在する場合、コンフィギュレーションの残りの部分とともにこのコマンドをクリアします。**boot system** コマンドを使用すると、外部フラッシュ メモリ カード上のイメージなど、特定のイメージからブートすることができます。工場出荷時のデフォルト コンフィギュレーションの復元後に、セキュリティ アプライアンスをリロードすると、内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合、セキュリティ アプライアンスはブートしません。

フル コンフィギュレーションに役立つ補助的な設定を行うには、**setup** コマンドを参照してください。

ASA 5505 デフォルト コンフィギュレーション

ASA 5505 適応型セキュリティ アプライアンスの工場出荷時のデフォルト コンフィギュレーションは、次のように設定されています。

- Ethernet 0/1 ～ 0/7 スイッチ ポートを含む内部 VLAN 1 インターフェイス。
  configure factory-default コマンドに IP アドレスを 設定していない場合、VLAN 1 IP アドレスとマスクは 192.168.1.1 と 255.255.255.0 です。
- Ethernet 0/0 スイッチ ポートを含む外部 VLAN 2 インターフェイス。VLAN 2 は DHCP を使用してその IP アドレスを取得します。
- デフォルト ルートも DHCP から取得されます。
- すべての内部 IP アドレスは、インターフェイス PAT を使用して外部アクセスを行うときに変換されます。
- デフォルトでは、内部ユーザはアクセスリストを使用して外部にアクセスでき、外部ユーザは内部にアクセスできません。
- DHCP サーバはセキュリティ アプライアンス上でイネーブルになっているので、VLAN 1 インターフェイスに接続している PC は 192.168.1.2 と 192.168.1.254 間のアドレスを受信します。
- HTTP サーバは ASDM に対してイネーブルになっており、192.168.1.0 ネットワーク上でユーザにアクセスできます。

このコンフィギュレーションは、次のコマンドで構成されています。

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 以降のデフォルト コンフィギュレーション

ASA 5510 以降の適応型セキュリティ アプライアンスの工場出荷時のデフォルト コンフィギュレーションは、次のように設定されています。

- 管理インターフェイスは Management 0/0 です。**configure factory-default** コマンドに IP アドレスを設定していない場合は、IP アドレスとマスクは 192.168.1.1 と 255.255.255.0 です。
- DHCP サーバはセキュリティ アプライアンス上でイネーブルになっているので、インターフェイスに接続している PC は 192.168.1.2 と 192.168.1.254 間のアドレスを受信します。
- HTTP サーバは ASDM に対してイネーブルになっており、192.168.1.0 ネットワーク上でユーザにアクセスできます。

このコンフィギュレーションは、次のコマンドで構成されています。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E のデフォルト コンフィギュレーション

PIX 515/515E セキュリティ アプライアンスの工場出荷時のデフォルト コンフィギュレーションは、次のように設定されています。

- 内部 Ethernet1 インターフェイス。**configure factory-default** コマンドに IP アドレスを設定していない場合は、IP アドレスとマスクは 192.168.1.1 と 255.255.255.0 です。
- DHCP サーバはセキュリティ アプライアンス上でイネーブルになっているので、インターフェイスに接続している PC は 192.168.1.2 と 192.168.1.254 間のアドレスを受信します。
- HTTP サーバは ASDM に対してイネーブルになっており、192.168.1.0 ネットワーク上でユーザにアクセスできます。

このコンフィギュレーションは、次のコマンドで構成されています。

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

ASDM アクセスに対するセキュリティ アプライアンスの設定

コマンドライン インターフェイスの代わりに、ASDM を使用してセキュリティ アプライアンスを設定する場合、デフォルトの管理アドレス 192.168.1.1 に接続することができます（セキュリティ アプライアンスが工場出荷時のデフォルト コンフィギュレーションの状態にある場合。P.2-2 の「工場出荷時のデフォルト コンフィギュレーション」を参照してください）。ASA 5510 以降の適応型セキュリティ アプライアンスでは、ASDM で接続するインターフェイスは Management 0/0 です。ASA 5505 適応型セキュリティ アプライアンスでは、ASDM で接続するスイッチ ポートは Ethernet 0/0 以外の任意のポートです。PIX 515/515E セキュリティ アプライアンスでは、ASDM で接続するインターフェイスは Ethernet 1 です。

工場出荷時のデフォルト コンフィギュレーションになっていない場合は、『*Cisco Security Appliance Command Line Configuration Guide*』の手順でコマンドライン インターフェイスにアクセスします。そこで、**setup** コマンドを入力すると、ASDM にアクセスするための最小限のパラメータが設定できます。

CLI による透過ファイアウォール モードまたはルーテッド ファイアウォール モードの設定

セキュリティ アプライアンスは、ルーテッド ファイアウォール モード（デフォルト）または透過ファイアウォール モードで動作するように設定できます。ファイアウォール モードの詳細については、「ファイアウォール モードの概要」を参照してください。

マルチコンテキスト モードでは、すべてのコンテキストで 1 つのファイアウォール モードしか使用できません。モードの設定は、システム実行スペースで行う必要があります。

モードを変更すると、セキュリティ アプライアンスはコンフィギュレーションをクリアします。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。マルチコンテキスト モードの場合は、システム コンフィギュレーションが消去されます。このアクションでは、実行中のコンテキストが削除されます。その後、別のモード用に作成された既存のコンフィギュレーションを持つコンテキストを再度追加しても、コンテキスト コンフィギュレーションは正常に動作しません。再度追加する前に、コンテキスト コンフィギュレーションを正しいモード用に作成するか、新規のコンフィギュレーション用の新しいパスを指定して、コンテキストを新たに追加してください。

firewall transparent コマンドでモードを変更するセキュリティ アプライアンスにテキスト 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、セキュリティ アプライアンスは、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、セキュリティ アプライアンス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。

ファイアウォール モードを設定するには、次の手順を実行します。マルチコンテキスト モードの場合は、システム実行スペースで実行します。

ステップ 1　次のいずれかのコマンドで、シングルコンテキスト　モードまたはマルチモードのシステム　コンフィギュレーションから、スタートアップ コンフィギュレーションまたは実行コンフィギュレーションを外部サーバやローカル フラッシュ メモリにコピーできます。コンフィギュレーションをバックアップしておくと、新しいコンフィギュレーションを作成するときに参照できます。

- TFTP サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {startup-config | running-config} tftp://server[/path]/filename
  ```

- FTP サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {startup-config | running-config}
  ftp://[user[:password]@]server[/path]/filename
  ```

- ローカルのフラッシュ メモリにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {startup-config | running-config} {flash:/ | disk0:/ |
  disk1:/}[path/]filename
  ```

  宛先のディレクトリが存在することを確認してください。存在しない場合は、最初に、**mkdir** コマンドを使用してディレクトリを作成します。

ステップ 2　モードを変更するには、次のコマンドのいずれかを入力します。

- 透過モードに設定するには、次のコマンドを入力します。
  ```
  hostname(config)# firewall transparent
  ```
  このコマンドは、情報提供のためだけに各コンテキスト コンフィギュレーションにも表示されるため、このコマンドをコンテキストに入力することはできません。
- ルーテッド モードに設定するには、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　セキュリティ アプライアンス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　セキュリティ アプライアンスの 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 がセキュリティ アプライアンスにあれば 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 またはセキュリティ アプライアンス機能のデモ。
- 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　セキュリティ アプライアンス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

Configuration > Properties > History Metrics

History Metrics ペインで、セキュリティ アプライアンス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

セキュリティ アプライアンス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。**Wizards** > **Startup Wizard** の順にクリックします。

ステップ 2　VPN 接続を設定するには VPN Wizard を使用します。**Wizards** > **VPN Wizard** の順にクリックし、表示される画面に入力します。

ステップ 3　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。

- 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。
  - Access Rules：セキュリティ アプライアンスを通過する 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 Rules（透過モード専用）：セキュリティ アプライアンスを通過する 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。セキュリティ アプライアンスは、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。セキュリティ アプライアンスは、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は、セキュリティ アプライアンスが詳細なパケット検査を行うことを要求します。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：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。
- VPN：VPN 接続を設定します。
  - VPN Wizard：VPN ウィザードを実行します。
  - 電子メール プロキシ：電子メール プロキシを設定します。電子メール プロキシを設定すると、リモート電子メール機能を WebVPN ユーザに拡張できます。
  - 一般的な VPN 設定：VPN コンフィギュレーションの一般的なパラメータを設定します。
  - IKE：IKE は ISAKMP とも呼ばれ、2 台のホストで IPSec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。
  - IP アドレス管理：クライアントが VPN トンネルから接続した場合、接続後にクライアントの IP アドレスを設定します。
  - IPSec：VPN トンネルの IPSec プロトコルを設定します。

  - Load Balancing：VPN 接続のロードバランシングを設定します。
  - WebVPN：WebVPN を設定します。WebVPN によってユーザは、ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。
- CSD Manager：CSC SSM を設定します（ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみ使用できます）。
- IPS の設定：AIP SSM を設定します（ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみ使用できます）。
- 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、スタティック ルーティング、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：セキュリティ アプライアンス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。
  - ホスト / ネットワーク
  - 検査マップ
  - TCP マップ
  - 時間範囲

ステップ 4　セキュリティ アプライアンスを監視するには、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。

- インターフェイスのモニタリング：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。