CHAPTER 3

始める前に

この項では、ASDM を使用する前に実行する必要があるタスクについて説明します。次の項目を取り上げます。

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、PIX 525 および PIX 535 モデルを除き、すべてのセキュリティ アプライアンスでサポートされています。

ASA 5505 モデルの場合、すぐに適応型セキュリティ アプライアンスを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事前定義済みのインターフェイスと NAT が含まれています。

PIX 515、PIX 515E、および ASA 5510 以降のバージョンのモデルの場合、工場出荷時のデフォルト コンフィギュレーションで管理インターフェイスが提供されており、ASDM を使用してセキュリティ アプライアンスに接続し、設定を完了できます。

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 アドレスを変更するには、次のいずれかの操作を実行します。

- ASA 5500 シリーズの場合、**Use this address for the Management 0/0 interface that will be named as “management”** チェックボックスをオンにし、Management IP Address フィールドに新しい IP アドレスを入力して、Management Subnet Mask ドロップダウン リストから新しいサブネット マスクを選択します。
- PIX シリーズの場合、**Use this address for the Ethernet 1 interface, which will be named “inside”** チェックボックスをオンにし、Inside IP Address フィールドに新しい内部 IP アドレスを入力して、Inside Subnet Mask ドロップダウン リストから新しい内部サブネット マスクを選択します。

ステップ 3　**OK** をクリックします。

（注）　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と、適応型セキュリティ アプライアンスは次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を使用してブートします。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。

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、外部インターフェイスにアクセスするときに PAT を使用して変換されます。
- 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 サーバは適応型セキュリティ 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コンピュータは 192.168.1.2 ～ 192.168.1.254 の IP 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 以降のバージョンのデフォルト コンフィギュレーション

ASA 5510 以降のバージョンの適応型セキュリティ アプライアンスでは、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 サーバは適応型セキュリティ 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コンピュータは 192.168.1.2 ～ 192.168.1.254 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** コマンドで IP アドレスを設定していない場合は、IP アドレスとサブネット 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コンピュータは 192.168.1.2 ～ 192.168.1.254 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

CLI ではなく 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、工場出荷時のデフォルト コンフィギュレーションがあれば、ブラウザで https://192.168.1.1 に移動するとデフォルトの管理アドレスに接続できます。または、Cisco ASDM ランチャがインストールされていれば、それを使用して ASDM に接続できます。詳細については、P.3-2 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 適応型セキュリティ アプライアンスでは、ASDM への接続に使用するスイッチ ポートは Ethernet 0/0 以外であればどのポートでもかまいません。ASA 5510 以降のバージョンの適応型セキュリティ アプライアンスでは、ASDM に接続するインターフェイスは Management 0/0 です。PIX 515/515E セキュリティ アプライアンスでは、ASDM に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でない場合、CLI にアクセスする手順については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

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

適応型セキュリティ アプライアンスは、デフォルトのルーテッド ファイアウォール モード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、P.18-1 の「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、適応型セキュリティ 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。すでに設定した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できます。

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、それによってすべてのコンテキストが削除されます。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。

（注） 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、適応型セキュリティ アプライアンスは、このコマンドを実行したら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、適応型セキュリティ 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。

（注） 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する必要があります。

ステップ 1　新しいコンフィギュレーションを作成する前に、必ずスタートアップ　コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルをバックアップして後で参照できるようにしてください。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 ファイルまたは実行コンフィギュレーション ファイル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。

- 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
  ```

  ここでは、*server* は TFTP サーバの名前、*path* はコンフィギュレーション ファイルへのディレクトリ パス、*filename* はコンフィギュレーション ファイルの名前です。

- 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
```

ここでは、*user* は使用するユーザ名、*password* は FTP サーバへのパスワード、*server* は FTP サーバの名前、*path* はコンフィギュレーション ファイルへのディレクトリ パス、*filename* はコンフィギュレーション ファイルの名前です。

- 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
```

ここでは、*path* はコンフィギュレーション ファイルへのディレクトリ パス、*filename* はコンフィギュレーション ファイルの名前です。

（注） 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、**mkdir** コマンドを使用して宛先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、参考情報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表示されることもあるため、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 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 ランチャのダウンロード

ASDM ランチャは Windows 専用です。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　ASDM Welcome 画面で、適切なボタンをクリックして ASDM ランチャのインストール ファイルをダウンロードします。

ステップ 2　**asdm-launcher.exe** ファイルをダブルクリックします。

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

ステップ 3　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。名前とパスワードは空白にします。

インストーラがコンピュータ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 ランチャによる ASDM の起動

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** メニューから開きます。または、ASDM Welcome 画面から、**Run Startup Wizard** をクリックして ASDM を設定できます。

ステップ 2　接続先として適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力するか選択します。IP アドレスのリストをクリアするには、Device/IP Address/Name フィールドの横にあるゴミ箱アイコンをクリックします。

ステップ 3　ユーザ名とパスワードを入力し、**OK** をクリックします。

新しいバージョンの ASDM が適応型セキュリティ アプライアンスにある場合、ASDM ランチャは自動的に新しいバージョンをダウンロードし、ASDM を起動する前に現在のバージョンをアップデートするようにユーザに要求します。

デモ モードでの ASDM の使用

アプリケーション ASDM Demo Mode を別途インストールして使用すると、実デバイスを使用せずに ASDM を実行できます。このモードでは、次の操作を実行できます。

- 実デバイス接続時と同じように、ASDM から設定と選択した監視タスクを実行する。
- 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を実行する。
- CSC SSM を使用して設定および監視タスクを実行する。
- リアルタイムのシステム　ログ　メッセージを含む、シミュレーションした監視データやログ データを取得する。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。

このモードでは、次の機能はサポートされません。

- GUI に表示されたコンフィギュレーションに加えた変更内容の保存
- ファイルまたはディスクの操作
- 履歴モニタリングデータ
- 非管理ユーザ
- 次の機能
  - 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 Software
    File Transfer
    Upload image from Local PC
    System Reload
  - Toolbar/Status bar > Save
  - Configuration > Interface > Edit Interface > Renew DHCP Lease
  - フェールオーバー後のスタンバイ デバイスの設定
- コンフィギュレーションの再読み込みが発生する操作。再読み込みが行われると GUI が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 ペインの変更

- NAT ペインの変更
- Clock ペインの変更

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　ASDM Demo Mode インストーラの asdm-demo-*version*.msi を次のいずれかの場所からダウンロードします。

- http://www.cisco.com/cgi-bin/tablebuild.pl/asa
- http://www.cisco.com/cgi-bin/tablebuild.pl/pix

ステップ 2　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 3　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** メニューから開きます。

ステップ 4　**Run in Demo Mode** チェックボックスをオンにします。

Demo Mode ウィンドウが表示されます。

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*

ここでは、*interface_ip_address* は、適応型セキュリティ アプライアンス ネットワーク上の ASDM の IP アドレスです。

（注）　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。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。ユーザ名とパスワードのプロンプトでも同様です（空白のままにします）。

Cisco ASDM 6.0(3) Welcome ページに次のボタンが表示されます。

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

ステップ 3　**Run ASDM** をクリックします。

ステップ 4　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。

コンフィギュレーションの概要

適応型セキュリティ 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　スタートアップ ウィザードの使用による初期設定を行うには、**Wizards** > **Startup Wizard** を選択します。

ステップ 2　IPSec VPN Wizard を使用して IPSec VPN 接続を設定するには、**Wizards** > **IPSec VPN Wizard** を選択して、表示される各画面で設定を行います。

ステップ 3　SSL VPN Wizard を使用して SSL VPN 接続を設定するには、**Wizards** > **SSL VPN Wizard** を選択して、表示される各画面で設定を行います。

ステップ 4　高可用性とスケーラビリティに関する設定値を設定するには、**Wizards** > **High Availability and Scalability Wizard** を選択します。詳細については、「High Availability and Scalability ウィザードを使用したフェールオーバーの設定」を参照してください。

ステップ 5　Packet Capture Wizard を使用してパケット キャプチャを設定するには、**Wizards** > **Packet Capture Wizard** を選択します。

ステップ 6　ASDM GUI で使用できるさまざまな色とスタイルを表示するには、**View > Office Look and Feel** を選択します。

ステップ 7　機能を設定するには、ツールバーで **Configuration** ボタンをクリックし、**Device Setup**、**Device Management**、**Firewall**、**Remote Access VPN**、**Site-to-Site VPN**、**IPS**、**Trend Micro Content Security** のいずれかのボタンをクリックして関連する設定ペインを表示します。

（注）　Configuration 画面が空白の場合は、ツールバーで **Refresh** をクリックして、画面のコンテンツを表示します。

- Device Setup ペインでは次のことができます。
  - Startup Wizard を起動してセキュリティ ポリシーを作成する。
  - IP アドレス、名前、セキュリティ レベル、透過モードのブリッジ グループなど、インターフェイスの基本パラメータを設定する。詳細については、「インターフェイスの設定」を参照してください。
  - 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する（シングルモードのみ）。詳細については、「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」を参照してください。
  - AAA サービスを設定する。
  - デジタル証明書を設定する。
  - デバイス名とデバイス パスワードを設定する。
  - DHCP サービスを設定する。

- DNS サービスを設定する。

- Firewall ペインでは、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 ルールなどのセキュリティ ポリシーと共に、NAT ルール、URL フィルタリング サーバ、グローバル オブジェクトを設定できます。また、次の高度な設定を行うこともできます。
  - Access Rules では、IP トラフィックがセキュリティ アプライアンスを通過できるかどうかを決定します。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（透過モードのみ）では、非 IP トラフィックがセキュリティ アプライアンスを通過できるかどうかを決定します。
  - Access Rules では、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、または両方を行うかどうかを決定します。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 では、特定の Web 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。**Configuration > Properties > URL Filtering** を選択して URL フィルタリング サーバを設定してから、ルールを追加する必要があります。
  - サービス ポリシー ルールの設定により、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、適応型セキュリティ 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 は、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。この設定によって、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。
  - グローバル オブジェクトの追加では、適用型セキュリティ 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

    サービス グループ

    クラス マップ

    検査マップ

    正規表現

    TCP マップ

    グローバル プール

    時間範囲

- Remote Access VPN ペインでは、ネットワーク クライアント アクセス、クライアントレス SSL VPN ブラウザ アクセスと高度な Web 関連の設定値、AAA 設定、証明書管理、ロードバランシングを設定できます。また、次のような高度な追加の設定を行うことができます。
  - VPN トンネルの IPSec 接続を設定する。
  - クライアントレス SSL VPN 接続を設定する。クライアントレス SSL VPN を使用すると、ユーザは Web ブラウザを使用して、適応型セキュリティ 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。
  - IKE で、クライアントが VPN トンネルから接続した後にクライアントの IP アドレスを設定する。
  - Load Balancing で VPN 接続のロードバランシングを設定する。
  - 電子メール プロキシで電子メール プロキシを設定する。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クライアントレス SSL VPN ユーザに拡張できます。

- Site-to-Site VPN ペインでは、サイト間 VPN 接続、グループ ポリシー、証明書管理を設定できます。また、次のような高度な設定を行うことができます。
  - IKE ポリシーと IKE パラメータ（ISAKMP とも呼ばれる）。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 プロトコルを提供します。
- Device Management ペインでは、次のようなアクセスと管理のための設定を行うことができます。
  - ASDM と HTTP over SSL の管理セッション。
  - FTP および TFTP クライアント。
  - CLI。
  - SNMP および ICMP。
  - 電子メール、イベント リスト、フィルタ、レート制限、syslog サーバ、SMTP などのロギング。詳細については、「ロギングの設定」を参照してください。
  - ユーザおよび AAA 認証。
  - High Availability and Scalability Wizard およびフェールオーバー。
  - 高度な設定。

（注）　CSC SSM カードまたは IPS ソフトウェアがインストールされている場合、**Trend Micro Content Security** または **IPS** 機能ボタンも表示されます。

- IPS ペインでは、IPS センサーを設定できます。詳細については、「IPS の設定」を参照してください。
- Trend Micro Content Security ペインでは、CSC SSM を設定できます（ASA 5500 シリーズ適応型セキュリティ アプライアンスで使用可能）。詳細については、「Trend Micro Content Security の設定」を参照してください。

ステップ 8　適応型セキュリティ 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、続いて **Interfaces**、**VPN**、**Trend Micro Content Security**、**Routing**、**Properties**、**Logging** のいずれかの機能ボタンをクリックして関連する監視ペインを表示します。

- Interfaces ペインでは、ARP テーブル、DHCP サービス、ダイナミック アクセスリスト、PPoE クライアント、接続ステータス、およびインターフェイスの統計情報を監視できます。詳細については、「インターフェイスのモニタリング」を参照してください。
- VPN ペインでは、VPN 接続を監視できます。詳細については、「VPN のモニタリング」を参照してください。
- Routing ペインでは、ルート、OSPF LSA、および OSPF ネイバーを監視できます。詳細については、「ルーティングのモニタリング」を参照してください。
- Properties ペインでは、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できます。詳細については、「プロパティのモニタリング」を参照してください。
- Logging ペインでは、システム ログ メッセージ、Real-Time Log Viewer、およびログ バッファを監視できます。詳細については、「ロギングのモニタリング」を参照してください。
- Trend Micro Content Security ペインでは、CSC SSM 接続を監視できます。詳細については、「Trend Micro Content Security のモニタリング」を参照してください。