AIP SSM の設定

オプションの AIP SSM は、インライン モードまたは無差別モードでセキュリティ検査を強化する、高度な IPS ソフトウェアを実行します。適応型セキュリティ アプライアンスが AIP SSM にパケットを転送するのは、パケットが出力インターフェイスを通過する直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）と、他のファイアウォール ポリシーが適用された後です。たとえば、アクセスリストによってブロックされたパケットは、AIP SSM に転送されません。

AIP SSM を購入した場合は、この章の手順に従って、次の操作を行います。

- AIP SSM に誘導するトラフィックを特定するための適応型セキュリティ アプライアンスの設定
- AIP SSM へのセッションの接続とセットアップの実行

（注） AIP SSM は、バージョン 7.01 以降の ASA ソフトウェアでサポートされます。

この章は、次の項で構成されています。

AIP SSM の設定

この手順では、AIP SSM 用に適応型セキュリティ アプライアンスを設定するために必要な設定手順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。

設定プロセスの概要

AIP SSM の設定は、3 段階に分けられます。まず適応型セキュリティ アプライアンスを設定し、次に AIP SSM を設定し、最後に IPS ソフトウェアを設定します。

1. ASA 5500 シリーズ 適応型セキュリティ アプライアンスでは、AIP SSM に誘導するトラフィックを特定します（P.9-3 の「トラフィックを AIP SSM に誘導するための ASA 5500 の設定」の説明を参照してください）。
2. AIP SSM では、検査と保護ポリシーを設定することにより、トラフィックの検査方法と侵入検出時の対処を決定します。
3. AIP SSM で実行する IPS ソフトウェアを設定します。IPS ソフトウェアについては、このマニュアルでは扱いません。IPS ソフトウェア設定の詳細については、IPS 製品に同梱されている次のマニュアルを参照してください。
   - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
   - *Cisco Intrusion Prevention System Command Reference*

トラフィックを AIP SSM に誘導するための ASA 5500 の設定

MPF（モジュラ ポリシー フレームワーク）コマンドを使用して、トラフィックを AIP SSM に誘導するように、適応型セキュリティ アプライアンスを設定します。この手順では、AIP SSM 配置の単純なポリシー セットを設定するための情報を示します。複雑なポリシー セットを作成する場合は、Modular Policy Framework の概念と一般的なコマンドを説明する『*Cisco Security Appliance Command Line Configuration Guide*』の「Modular Policy Framework」の章を参照してください。

適応型セキュリティ アプライアンスから AIP SSM に誘導するトラフィックを特定するには、次の手順を実行します。

ステップ 1　すべてのトラフィックと一致するアクセス リストを作成します。

```
hostname(config)# access-list acl-name permit ip any any
```

ステップ 2　AIP SSM に誘導するトラフィックを特定するクラスマップを作成します。次のように、**class-map** コマンドを使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

ここで、*class_map_name* は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI は、クラスマップ コンフィギュレーションモードに移行します。

ステップ 3　ステップ 1 で作成したアクセス リストと **match access-list** コマンドを使用して、スキャンするトラフィックを特定します。

```
hostname(config-cmap)# match access-list acl-name
```

ステップ 4　AIP SSM へのトラフィックの送信に使用するポリシーマップを作成するか、既存のポリシーマップを修正します。次のように、**policy-map** コマンドを使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

ここで、*policy_map_name* は、ポリシーマップの名前です。CLI は、ポリシーマップ コンフィギュレーション モードに移行し、プロンプトが変化します。

ステップ 5　スキャンするトラフィックを特定する、ステップ 2 で作成したクラスマップを指定します。次のように、**class** コマンドを使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

ここで、*class_map_name* は、ステップ 2 で作成したクラスマップの名前です。CLI は、ポリシーマップ クラス コンフィギュレーション モードに移行し、プロンプトが変化します。

ステップ 6　クラスマップで特定されたトラフィックを、AIP SSM に送信するトラフィックとして割り当てます。次のように、**ips** コマンドを使用します。

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open}
```

inline キーワードおよび ***promiscuous*** キーワードによって、AIP SSM の動作モードを制御します。***fail-close*** キーワードおよび ***fail-open*** キーワードによって、AIP SSM を使用できないときに適応型セキュリティ アプライアンスがトラフィックを処理する方法を制御します。動作モードおよび障害発生時の動作の詳細については、P.9-2 の「AIP SSM の設定」を参照してください。

ステップ 7　**service-policy** コマンドを使用して、ポリシーマップをグローバルに、または特定のインターフェイスに適用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global |
interface interface_ID]
hostname(config)#
```

ここで、*policy_map_name* は、ステップ 4 で設定したポリシーマップです。すべてのインターフェイスのトラフィックにポリシーマップを適用するには、**global** キーワードを使用します。特定のインターフェイスのトラフィックにポリシーマップを適用するには、***interface*** *interface_ID* オプションを使用します。ここで、*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てた名前です。

グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

適応型セキュリティ アプライアンスは、指定されたとおりにトラフィックを AIP SSM に誘導し始めます。

次の例では、すべての IP トラフィックが AIP SSM に無差別モードで誘導され、何らかの理由で AIP SSM カードに障害が発生した場合は、すべての IP トラフィックがブロックされます。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

AIP SSM へのセッションの接続とセットアップの実行

トラフィックを AIP SSM に誘導するように、ASA 5500 シリーズ 適応型セキュリティ アプライアンスを設定した後、AIP SSM へのセッションを接続し、初期コンフィギュレーション用のセットアップ ユーティリティを実行します。

（注） （**session 1** コマンドを使用して）適応型セキュリティ アプライアンスから SSM へのセッションを接続することも、管理インターフェイスで SSH または Telnet を使用して、SSM に直接接続することもできます。あるいは、ASDM を使用することもできます。

適応型セキュリティ アプライアンスから AIP SSM へのセッションを接続するには、次の手順を実行します。

ステップ 1　**session 1** コマンドを入力して、ASA 5500 シリーズ適応型セキュリティ アプライアンス から AIP SSM へのセッションを接続します。

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ステップ 2　ユーザ名とパスワードを入力します。デフォルトのユーザ名とパスワードは、どちらも **cisco** です。

（注） 初めて AIP SSM にログインしたときに、デフォルト パスワードの変更を要求するプロンプトが表示されます。パスワードは 8 文字以上で、辞書に載っていない単語にする必要があります。

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

（注） 上記のライセンスの注意が表示された場合（一部のソフトウェア バージョンでのみ表示されます）、AIP SSM でシグニチャ ファイルをアップグレードする必要がなければ、無視してかまいません。有効なライセンス キーがインストールされるまで、AIP SSM は現在のシグニチャ レベルで動作し続けます。ライセンス キーは後でインストールできます。ライセンス キーは、AIP SSM の現在の機能には影響を与えません。

ステップ 3　**setup** コマンドを入力して、AIP SSM の初期コンフィギュレーション用のセットアップ ユーティリティを実行します。

```
AIP SSM# setup
```

次の手順

これで、侵入防止のために適応型セキュリティ アプライアンスを設定する準備ができました。次のマニュアルを参照して、実装に合せて適応型セキュリティ アプライアンスを設定します。

作業内容	参照先
IPS センサーの設定	*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface* *Cisco Intrusion Prevention System Command Reference*
より効率的なサービス ポリシーの作成によるパフォーマンスの最適化	『*Cisco Security Appliance Command Line Configuration Guide*』の「Managing AIP SSM and CSC SSM」

IPS センサーおよび AIP SSM ソフトウェアを設定した後、次の追加の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
DMZ Web サーバの保護の設定	第 6 章「シナリオ：DMZ の設定」
リモートアクセス VPN の設定	第 7 章「シナリオ：リモートアクセス VPN の設定」
サイトツーサイト VPN の設定	第 8 章「シナリオ：サイトツーサイト VPN の設定」

次の手順