ASA/PIX 7.X： ASDM を使用したデフォルトのグローバル検査の無効化およびデフォルト以外のアプリケーション検査の有効化

目次

概要

このドキュメントでは、アプリケーションのグローバル ポリシーからデフォルト インスペクションを削除する方法およびデフォルト以外のアプリケーションのインスペクションを有効にする方法を説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、7.x ソフトウェア イメージを実行している Cisco 適応型セキュリティ アプライアンス（ASA）に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、7.x ソフトウェア イメージを実行している PIX セキュリティ アプライアンスでも使用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

デフォルトのグローバル ポリシー

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーが設定に含まれ、特定のインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。 すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。 適用できるグローバル ポリシーは 1 つだけです。 グローバル ポリシーを変更する場合は、デフォルト ポリシーを編集するか無効にし、新しいポリシーを適用する必要があります。（インターフェイス ポリシーはグローバル ポリシーに優先します）。

デフォルト ポリシー設定には、次のコマンドが含まれています。

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
```

デフォルト以外のアプリケーション インスペクションの有効化

Cisco ASA でデフォルト以外のアプリケーション インスペクションを有効にするには、次の手順を実行します。

1. ASDM にログインします。 [Configuration] > [Firewall] > [Service Policy Rules] に移動します。
2. デフォルト クラスマップとデフォルト ポリシーマップが含まれるグローバル ポリシーの構成は維持する一方、ポリシーをグローバルに削除する場合は、[Tools] > [Command Line Interface] に移動し、ポリシーをグローバルに削除するために **no service-policy global-policy global** コマンドを使用します。 それから [Send] をクリックして、このコマンドを ASA に適用します。**注:** この手順によって、グローバル ポリシーは、Adaptive Security Device

Manager (ASDM) には表示されなくなりますが、CLI には表示されます。
3. 以下に示すように、[Add] をクリックし、新しいポリシーを追加します。
4. [Interface] の横のオプション ボタンがオンになっていることを確認してから、ポリシーを適用するインターフェイスをドロップダウン メニューから選択します。 次に、[Policy Name] と [Description] に入力します。 [Next] をクリックします。
5. **HTTP**は TCP で定義されているため、**TCP トラフィック**と一致する新規クラスマップを作成します。 [Next] をクリックします。
6. プロトコルとして **TCP** を選択します。[Service] として HTTP **ポート 80** を選択し、[OK] をクリックします。
7. [HTTP] を選択し、[Finish] をクリックします。
8. [Apply] をクリックし、設定の変更を ASDM から ASA に送信します。 これで、設定は完了です。

確認

設定を検証するには、次の **show** コマンドを使用します。

- **show run class-map** コマンドを使用して、設定されているクラス マップを表示します。
```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class match port tcp eq www !
```
- **show run class-map** コマンドを使用して、設定されているポリシーマップを表示します。
```
ciscoasa# sh run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
policy-map outside-policy description Policy on outside interface class outside-class
inspect http !
```
- **show run service-policy** コマンドを使用して、設定されているサービス ポリシーを表示します。`ciscoasa# sh run service-policy`
```
service-policy outside-policy interface outside
```

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス

- Cisco ASA 5500 シリーズ コマンド リファレンス
- Cisco Adaptive Security Device Manager（ASDM）に関するサポート ページ
- Cisco PIX Firewall ソフトウェア
- Requests for Comments（RFC）
- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- アプリケーション層プロトコル検査の適用
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- テクニカルサポートとドキュメント - Cisco Systems