ASA/PIX 7.X: Deaktivieren Sie die globale Standardinspektion, und aktivieren Sie nicht standardmäßige Anwendungsinspektion mit ASDM.

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Globale Standardrichtlinie Nicht standardmäßige Anwendungsinspektion aktivieren Überprüfen Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie die Standardüberprüfung für eine Anwendung aus der globalen Richtlinie entfernt wird und wie die Überprüfung für eine nicht standardmäßige Anwendung aktiviert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance (ASA), die das 7.x-Software-Image ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit der PIX Security Appliance verwendet werden, die das 7.x-Software-Image ausführt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Globale Standardrichtlinie

Standardmäßig enthält die Konfiguration eine Richtlinie, die dem gesamten standardmäßigen Anwendungsinspektionsverkehr entspricht und bestimmte Überprüfungen auf den Datenverkehr an allen Schnittstellen anwendet (eine globale Richtlinie). Nicht alle Überprüfungen sind standardmäßig aktiviert. Sie können nur eine globale Richtlinie anwenden. Wenn Sie die globale Richtlinie ändern möchten, müssen Sie entweder die Standardrichtlinie bearbeiten oder deaktivieren und eine neue Richtlinie anwenden. (Eine Schnittstellenrichtlinie überschreibt die globale Richtlinie.)

Die Standardrichtlinienkonfiguration umfasst die folgenden Befehle:

```
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
```

Nicht standardmäßige Anwendungsinspektion aktivieren

Gehen Sie wie folgt vor, um eine Nicht-Standard-Anwendungsinspektion auf der Cisco ASA zu aktivieren:

1. Melden Sie sich beim **ASDM an**. Gehen Sie zu **Konfiguration > Firewall > Service Policy Rules**.

| onfiguration > Firew | all > 9 | iervice Pol | icy Rules | | | | | |
|------------------------|--|---|---|---|---|--|------------|--|
| 🕂 Add 🔹 🗹 Edit 👔 | 🔋 Dele | te ∱ - ∳ | 🛛 👗 🛍 | 📖 - 🛛 🔍 Find 🖭 | Diagram 🔫 Packet T | race | | |
| Traffic Classification | | | | | | | | Dula Actions |
| Name | # | Enabled | Match | Source | Destination | Service | Time | Rule Actions |
| Global; Policy: global | _policy | | | | | | | |
| inspection_default | | | 🖣 Match | 🆘 any | 🎨 any | 🔍 default-inspe | | Inspect DNS Map prese Inspect ESMTP (12 more inspect actions) |
| | | | | | | | | |
| | | | | | | | | |
| | Add ✓ Cassification Traffic Classification Name Global; Policy: global inspection_default | Add Add Cassification Firewall > S Cassification Name Global; Policy: global_policy inspection_default | • Add ▼ Firewall > Service Pol • Add ▼ Edit Delete • Add ▼ Edit Delete • Traffic Classification Finabled • Global; Policy: global_policy inspection_default # Enabled | Image: Add Image: Policy Relation Image: Policy Relation Image: Policy Relation Image: Policy Relation Name Image: Policy Relation Image: Policy Relation Image: Policy Relation Image: Policy Relation <th>Image: Add Image: Price Policy Rules Image: Add Image: Policy Rules Image: Policy Rules <tr< th=""><th>Image: Add Image: Price Policy Rules Image: Add Image: Policy Rules Image: Policy Rules <tr< th=""><th>Add ▼ Etit</th><th>Add ■ Enabled ● ↓ ↓ ↓ □ ↓ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □</th></tr<></th></tr<></th> | Image: Add Image: Price Policy Rules Image: Add Image: Policy Rules Image: Policy Rules <tr< th=""><th>Image: Add Image: Price Policy Rules Image: Add Image: Policy Rules Image: Policy Rules <tr< th=""><th>Add ▼ Etit</th><th>Add ■ Enabled ● ↓ ↓ ↓ □ ↓ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □</th></tr<></th></tr<> | Image: Add Image: Price Policy Rules Image: Add Image: Policy Rules Image: Policy Rules <tr< th=""><th>Add ▼ Etit</th><th>Add ■ Enabled ● ↓ ↓ ↓ □ ↓ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □</th></tr<> | Add ▼ Etit | Add ■ Enabled ● ↓ ↓ ↓ □ ↓ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ |

2. Wenn Sie die Konfiguration f
ür globale Richtlinien beibehalten m
öchten, die die Standard-Klassenzuordnung und die Standard-Richtlinienzuordnung enth
ält, die Richtlinie aber global entfernen m
öchten, gehen Sie zu Extras > Befehlszeilenschnittstelle und verwenden Sie den Befehl no service-policy global-policy, um die Richtlinie global zu entfernen. Klicken Sie anschließend auf Senden, um den Befehl auf die ASA anzuwenden.

| 🖆 Command Line Interface | |
|--|----------------------------|
| Type a command to be sent directly to the device. For command help, type a command followed by a mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as para the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash. | question ameter to g |
| Single Line | |
| no service-policy global_policy global | * |
| | |
| Response: | |
| Result of the command: "no service-policy global_policy global" The command has been sent to the device | |
| Clear Send Close Help | Response |

Hinweis: Bei diesem Schritt wird die globale Richtlinie im ASDM (Adaptive Security Device Manager) nicht mehr angezeigt, sondern in der CLI angezeigt.

3. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen, wie hier

| gezeigt: | | | | | | | | |
|---|---|-------------|---------|------|--------------|--|--|--|
| Configuration > | Configuration > Firewall > Service Policy Rules | | | | | | | |
| 🜩 Add 🗸 📷 Edit 🏢 Delete 🖙 🌾 👗 🍋 🏨 - 🔍 Rind 🖽 Diagram 🐗 Packet Trace | | | | | | | | |
| Traffic Classification | | | | | | | | |
| Name | # Enabled Match Source | Destination | Service | Time | Kule Actions | | | |
| | | | | | | | | |
| | | | | | | | | |

4. Stellen Sie sicher, dass das Optionsfeld neben **Interface (Schnittstelle)** aktiviert ist, und wählen Sie im Dropdown-Menü die Schnittstelle aus, die Sie für die Richtlinie verwenden

möchten. Geben Sie dann den **Richtliniennamen** und die **Beschreibung** ein. Klicken Sie auf **Weiter**.

| 📬 Ad | ld Service P | Policy Rule Wizard - Service Policy | | | × |
|-------------------------------------|---|--|--------------------|--|---|
| Addin Step 3 Step 3 Step 3 | ng a new servio 1: Configure (2: Configure (3: Configure (3: Configure (| ce policy rule requires three steps: a service policy. the traffic classification criteria for the service actions on the traffic classified by the service vicy and Apply To: | e polic; polic; | y rule. y rule. | |
| Onl rule | ly one service a into the exist | policy can be configured per interface or at o ing service policy. Otherwise, you can create | global e a ne | level. If a service policy already exists, then you can add a new w service policy. | |
| \odot | Interface: | outside - (create new service policy) 🔽 | | | |
| | Policy Name: | outside-policy | | | |
| | Description: | Policy on outside interface | | | |
| 0 |) Global - apple | es to all interfaces | | | |
| | Policy Name: | global-policy | | | |
| | Description: | | | | ٦ |
| | | | | | _ |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | < Back Next > Cancel He | P |

 Erstellen Sie eine neue Klassenzuordnung, die dem TCP-Datenverkehr entspricht, wenn HTTP unter TCP fällt. Klicken Sie auf Weiter.

| 🖆 Add Service Policy Rule | Wizard - Traffic Classification Criteria | × |
|--|--|---|
| • Create a new traffic dass: | outside-class | |
| Description (optional): | | |
| Traffic Match Criteria | | _ |
| Default Inspection Trai | ffic | |
| Source and Destination | n IP Address (uses ACL) | |
| Tunnel Group | | |
| CP or UDP Destination | n Port | |
| RTP Range | | |
| IP DiffServ CodePoints | (DSCP) | |
| IP Precedence | N | |
| Any traffic | 43 | |
| O Use an existing traffic class: | inspection_default | |
| O Use class-default as the traff | fic class. | |
| If traffic does not match a ex situation. | dsting traffic class, then it will match the class-default traffic class. Class-default can be used in catch all | |
| | | |
| | | |
| | | |
| | | |
| | < Back Next > Cancel Help | |

6. Wählen Sie **TCP** als Protokoll aus.

| 🖆 Add Service Policy Rule Wizard - Traffic Match - Destination Port | × |
|---|---|
| Protocol: | |
| Service: | |
| To specify port range for the service, use nnn-nnn hormat. | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | _ |
| < Back Next > Cancel Hel | P |

Wählen Sie **HTTP-Port 80** als Service aus, und klicken Sie auf **OK**.

| C | Browse Service | | | | | | |
|---|--------------------|----------|-------------------|-------------------|------------|-------------|--------------|
| | 🗣 Add 👻 🖼 Edit | î Delete | 0 | | | | |
| | Elber: | | ~ | | | | Filter Clear |
| | News | Destand | Service Deute | Deskieskies Deska | LCMD Turns | Description | |
| | Name Dradafinad | Protocol | Source Ports | Destination Ports | тсмы туре | Description | |
| | - Predenned | tro | default (1-65535) | 5190 | | | - |
| | ban | trn | default (1-65535) | 179 | | | |
| | - to chargen | tcp | default (1-65535) | 19 | | | |
| | cifs | tcp | default (1-65535) | 3020 | | | |
| | citrix-ica | tcp | default (1-65535) | 1494 | | | = |
| | - re> ctiqbe | tcp | default (1-65535) | 2748 | | | |
| | - 10 daytime | tcp | default (1-65535) | 13 | | | |
| | to discard | tcp | default (1-65535) | 9 | | | |
| | - 100 domain | tcp | default (1-65535) | 53 | | | |
| | 👓 🚥 echo | tcp | default (1-65535) | 7 | | | |
| | exec | tcp | default (1-65535) | 512 | | | |
| | | tcp | default (1-65535) | 79 | | | |
| | 👓 🏧 ftp | tcp | default (1-65535) | 21 | | | |
| | 👓 🏧 ftp-data | tcp | default (1-65535) | 20 | | | |
| | - 100 gopher | tcp | default (1-65535) | 70 | | | |
| | 100 h323 | tcp | default (1-65535) | 1720 | | | |
| | - 100 hostname | tcp | default (1-65535) | 101 | | | |
| | - 😰 http | tcp | default (1-65535) | 80 | | | |
| | nttps | tcp | default (1-65535) | 443 | | | |
| | | tcp | default (1-65535) | 113 | | | ~ |
| | Selected Service | | | | | | |
| | Service -> to | :p/http | | | | | |
| | | | | | | | |
| | | | | | | ОК | Cancel |

7. Wählen Sie HTTP aus, und klicken Sie auf Fertig stellen.

| Add Service Poli | cy Rule Wizard - Rule | e Actions |
|---------------------|---------------------------|---------------------------|
| Protocol Inspection | Intrusion Prevention Conr | nection Settings QoS |
| CTIONS. | | |
| | Coofigure | |
| | Configure | |
| ESMTD | Configure | |
| | Configure | |
| - FIF | Configure | |
| - H.323 H.225 | Configure | |
| | Configure | 1 |
| | Configure | ↓ |
| | | |
| | | |
| | Castlerus | |
| | Configure | |
| IPSec-Pass-Th | ru Configure | |
| MGCP | Configure | |
| NETBIOS | Configure | |
| PPTP | | |
| RSH | | |
| RTSP | Configure | |
| SCCP (Skinny) | Configure | × |
| | | |
| | | < Back Finish Cancel Help |

8. Klicken Sie auf **Apply**, um diese Konfigurationsänderungen vom ASDM an die ASA zu senden. Damit ist die Konfiguration

| Configuration > Firewail > Service Policy Rules | abgeschlossen. | |
|--|---|---|
| Add | Configuration > Firewall > Service Policy Rules | |
| Traffic Classification Rule Actions Name # Enabled Match Source Destination Service Time Image: Policy: outside-policy | 🗣 Add 👻 🎯 Edit 📋 Delete 🖙 🔸 🖌 🏭 🏨 🚽 🔍 Find 🔤 Diagram 💐 Packet Trace | |
| Name # Enabled Match Source Destination Service Time Image: Interface: outside: Policy: outside-policy Image: Interface: outside-class Image: Interface: outside-class Image: Interface: Interface: Image: Im | Traffic Classification | |
| Interface: outside; Policy: outside-policy outside-class Image: A state of the state of | Name # Enabled Match Source Destination Service Time | |
| outside-class Match <table-cell> any <table-cell> Too http 🔍 Inspect HTTP</table-cell></table-cell> | Interface: outside; Policy: outside-policy | |
| | outside-class 🛛 🕒 Match 🕫 any 👘 any 👘 http 🔍 Inspect HTTP | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| <u>(()</u> | | > |
| | | |

<u>Überprüfen</u>

Verwenden Sie die folgenden show-Befehle, um die Konfiguration zu überprüfen:

 Verwenden Sie den Befehl show run class-map, um die konfigurierten Klassenzuordnungen anzuzeigen.

```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class
match port tcp eq www
!
```

• Verwenden Sie den Befehl **show run policy-map**, um die konfigurierten Richtlinienzuordnungen anzuzeigen.

```
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
```

 Verwenden Sie den Befehl show run service-policy, um die konfigurierten Service-Richtlinien anzuzeigen.

```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

Zugehörige Informationen

- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Cisco Serie ASA 5500 Befehlsreferenzen</u>
- Support-Seite für Cisco Adaptive Security Device Manager (ASDM)
- <u>Cisco PIX Firewall-Software</u>
- Anforderungen für Kommentare (RFCs)
- <u>Cisco Security Appliances der Serie PIX 500</u>
- Anwenden der Protokollüberprüfung auf Anwendungsebene
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Technischer Support und Dokumentation Cisco Systems