ASA/PIX 7.X : Inspection globale par défaut de débronchement et inspection d'application de Non-par défaut d'enable utilisant l'ASDM

Contenu

Introduction Conditions préalables Conditions requises Composants utilisés Produits connexes Conventions Stratégie globale par défaut Inspection d'application de Non-par défaut d'enable Vérifiez Informations connexes

Introduction

Ce document décrit comment enlever l'inspection par défaut de la stratégie globale pour une application et comment activer l'inspection pour une application de non-par défaut.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur l'appliance de sécurité adaptable Cisco (ASA) ces passages l'image logicielle 7.x.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurezvous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Cette configuration peut également être utilisée avec les dispositifs de sécurité PIX qui exécutent

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco</u>.

Stratégie globale par défaut

Par défaut, la configuration inclut une stratégie qui apparie tout le trafic par défaut d'inspection d'application et s'applique certaines inspections au trafic sur toutes les interfaces (une stratégie globale). Non toutes les inspections sont activées par défaut. Vous pouvez appliquer seulement une stratégie globale. Si vous voulez modifier la stratégie globale, vous devez éditer la stratégie par défaut ou la désactiver et appliquer un neuf. (Une stratégie d'interface ignore la stratégie globale.)

La configuration de stratégie par défaut inclut ces commandes :

```
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
```

Inspection d'application de Non-par défaut d'enable

Remplissez cette procédure pour activer l'inspection d'application de Non-par défaut sur Cisco ASA :

 Procédure de connexion à l'ASDM. Allez aux règles de configuration > de stratégie de Parefeu > de service.

| I | Configuration > Firew | all > 9 | Service Pol | cy Rules | | | | | | |
|---|--------------------------|--|-------------|----------|--------|-------------|-----------------|---------|--|--|
| | 🕈 Add 🔹 🗹 Edit 👔 | 🕨 Add 💌 🖉 Edit: 🍿 Delete 🎓 🌾 👗 🛍 📖 - 🔍 Find 🖼 Diagram 🗠 Packet Trace | | | | | | | | |
| | Traffic Classification | Traffic Classification | | | | | | | Dulo Actions | |
| | Name | # | Enabled | Match | Source | Destination | Service | ce Time | RUP ACOULS | |
| | 🖃 Global; Policy: global | _policy | | | | | | | | |
| | inspection_default | | | La Match | 🆘 any | 🍫 any | 🔍 default-inspe | | Inspect DNS Map prese Inspect ESMTP (12 more inspect actions) | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

2. Si vous voulez garder la configuration pour la stratégie globale qui inclut le policy-map par défaut de class-map et de par défaut, mais voulez enlever la stratégie globalement, allez aux outils > à l'interface de ligne de commande et n'utilisez l'aucune commande globale de global-stratégie de service-stratégie d'enlever la stratégie globalement. Puis, le clic envoient ainsi la commande est appliquée à l'ASA.

| 鱰 Command Line Interface | N 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 |
|--|--|
| Type a command to be sent directly to the o mark. For commands that would prompt for the command and send it to the device. To Configuration to Flash menu option to save | device. For command help, type a command followed by a question confirmation, add an appropriate noconfirm option as parameter to make the changes permanent, use the File > Save Running the configuration to flash. |
| 💿 Single Line 🛛 Multiple Line | Enable context sensitive help (?) |
| no service-policy global_policy global | × |
| | |
| Response: | |
| Result of the command: "no se | rvice-policy global_policy global" the device |
| Send | Clear Response Close Help |

Remarque: Avec cette étape la stratégie globale devient invisible dans Adaptive Security Device Manager (ASDM), mais est affichée dans le CLI.

3. Cliquez sur Add afin d'ajouter une nouvelle stratégie comme affiché ici

| Configuration > | >Firewall > Service Policy Rules | | | | | |
|-------------------|-------------------------------------|----------------------|-----------|------|--------------|--|
| 🗣 Add 🝷 🛒 | Edit 🏦 Delete 🛧 🗲 🐰 🖿 🏨 - 🔍 F | ind 🖭 Diagram 🐙 Paci | ket Trace | | | |
| Traffic Classific | ation | | | | Dula Óstians | |
| Name | # Enabled Match Source | Destination | Service | Time | Kule Actions | |
| | | | | | | |
| | | | | | | |

4. Assurez-vous que la case d'option à côté de l'**interface** est vérifiée et choisissez l'interface que vous voulez appliquer la stratégie à partir du menu déroulant. Puis, fournissez le **nom de**

stratégie et la description. Cliquez sur Next

| 10 | | ~ | |
|-----|-------|-----|--|
| 191 | 111/2 | nt) | |
| 100 | JIVO | | |

| 🖆 Add Se | rvice P | olicy Rule Wizard - Service Policy | | × | | | | | | |
|---------------------------|---|---|--|---|--|--|--|--|--|--|
| Adding a ne Step 1: Co | Adding a new service policy rule requires three steps: Step 1: Configure a service policy. | | | | | | | | | |
| Step 2: Co | Step 2: Configure the traffic classification criteria for the service policy rule. | | | | | | | | | |
| Step 3: Co | nfigure a | actions on the traffic classified by the service po | licy rule. | | | | | | | |
| Create a Se | ervice Po | licy and Apply To: | alland 15° a second an allan allan da sudda allan allan ann | | | | | | | |
| rule into | the exist | policy can be configured per interface or at goi ing service policy. Otherwise, you can create a | allevel. If a service policy already exists, then you can add a new new service policy. | | | | | | | |
| Inter | face: | outside - (create new service policy) 🔽 | | | | | | | | |
| Policy | Name: | outside-policy | | | | | | | | |
| Desci | iption: | Policy on outside interface | | | | | | | | |
| 🔾 Globa | al - applie | es to all interfaces | | | | | | | | |
| Policy | Name: | global-policy | | | | | | | | |
| Desci | iption: | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | < Back Next > Cancel He | Þ | | | | | | |

 Créez un nouveau class-map pour apparier le trafic TCP comme le HTTP tombe sous le TCP. Cliquez sur Next (Suivant).

| 🖆 Add Service Policy Rule Wiza | rd - Traffic Classification Crit | leria | |
|--|--|---|--------|
| • Create a new traffic class: outside | e-class |] | |
| Description (optional): | | • | |
| Traffic Match Criteria | | | |
| Default Inspection Traffic | | | |
| Source and Destination IP Ad | dress (uses ACL) | | |
| Tunnel Group | _ | | |
| TCP or UDP Destination Port | | | |
| RTP Range | - | | |
| IP DiffServ CodePoints (DSCP |) | | |
| IP Precedence | N | | |
| Any traffic | 13 | | |
| OUse an existing traffic class: insp | ection_default 📝 | | |
| OUse class-default as the traffic class | | | |
| If traffic does not match a existing t situation. | raffic class, then it will match the class | s-default traffic class. Class-default can be used in cat | ch all |
| | | | |
| | | | |
| | | | |
| | | < Back Next > Cancel | Help |

6. Choisissez le **TCP** comme protocole.

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

Choisissez le **port HTTP 80** comme service et cliquez sur OK.

| C | Browse Service | | | | | | |
|---|--------------------|----------|-------------------|-------------------|------------|-------------|--------------|
| | 💠 Add 👻 🔟 Edit | î Delete | 0 | | | | |
| F | iter: | | ~ | | | | Filter Clear |
| ľ | Name | Destand | Courses Davids | Deskieskies Deska | ICMD Trues | Description | Tiller Clear |
| | Name DuadaSiand | Protocol | Source Ports | Destination Ports | тсмь туре | Description | |
| | = Prederined | tro | default (1-65535) | 5190 | | | - |
| | han | ten | default (1-65535) | 179 | | | |
| | | tep | default (1-65535) | 19 | | | |
| | in the cifs | tcp | default (1-65535) | 3020 | | | |
| | to citrix-ica | tcp | default (1-65535) | 1494 | | | a |
| | tigbe | tcp | default (1-65535) | 2748 | | | |
| | daytime | tcp | default (1-65535) | 13 | | | |
| | to discard | tcp | default (1-65535) | 9 | | | |
| | | tcp | default (1-65535) | 53 | | | |
| | 😳 echo | tcp | default (1-65535) | 7 | | | |
| | ···· 102> exec | tcp | default (1-65535) | 512 | | | |
| | • finger | tcp | default (1-65535) | 79 | | | |
| | ttp | tcp | default (1-65535) | 21 | | | |
| | 😰 ftp-data | tcp | default (1-65535) | 20 | | | |
| | gopher | tcp | default (1-65535) | 70 | | | |
| | 10 h323 | tcp | default (1-65535) | 1720 | | | |
| | nostname | tcp | default (1-65535) | 101 | | | |
| | - 😰 http | tcp | default (1-65535) | 80 | | | |
| | 😳 https | tcp | default (1-65535) | 443 | | | |
| | 🗠 🚾 ident | tcp | default (1-65535) | 113 | | | ~ |
| s | elected Service | | | | | | |
| | Service -> | oftto | | | | | |
| | | -bureb] | | | | | |
| | | | | | | ОК | Cancel |

7. Choisissez le **HTTP** et cliquez sur Finish.

| Add Service Pol | icy Rule Wizard - | - Rule Actions | |
|---------------------|----------------------|-------------------------|-----|
| Protocol Inspection | Intrusion Prevention | Connection Settings QoS | |
| CTIONE | | | ~ |
| | Configure | | |
| DNS | Configures | | |
| ESMTP | Configures | | |
| FTP | Configure | **** **** | |
| H.323 H.225 | Configure. | e | |
| H.323 RA5 | Configure. | e | |
| | Configure. | e | |
| ICMP | | | |
| ICMP Error | | | |
| ILS | | | |
| IM 🔄 | Configure. | 8 | |
| IPSec-Pass-T | hru Configure. | 8 | |
| MGCP | Configure. | B | - |
| NETBIOS | Configure. | | |
| PPTP | | | |
| 🖸 RSH | | | |
| RTSP | Configure. | p | |
| SCCP (Skinny |) Configure. | p | ¥ |
| | | | _ |
| | | Rack Finish Cased | Hal |

8. Cliquez sur Apply pour envoyer ces modifications de configuration à l'ASA de l'ASDM. Ceci se termine la

| configuration. | | | | | | | | | |
|------------------------|----------|----------------|----------|----------------|-----------------|----------|------|--------------|---|
| Configuration > Fire | wall > ! | Service Poli | cy Rules | | | | | | |
| 💠 Add 👻 🛃 Edit | 📋 Dek | ete 🛉 🗲 | 👗 🖻 | 💼 - 🛛 🔍 Find 🖭 | Diagram 🕂 Packe | t Trace | | | |
| Traffic Classification | | | | | | | | Dula áctions | |
| Name | # | Enabled | Match | Source | Destination | Service | Time | Rule Accord | |
| □ Interface: outside; | Policy: | outside-policy | , | | | | | | |
| outside-class | | | 🕒 Match | 🍫 any | 🦚 any | 100 http | | Inspect HTTP | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| <u><</u> | _ | | | Ш | | | | | > |
| | | | | Apply | Reset | | | | |

<u>Vérifiez</u>

Utilisez ces commandes show de vérifier la configuration :

• Utilisez la commande de class-map de passage d'exposition de visualiser les class map configurés.ciscoasa# sh run class-map

```
class-map inspection_default
 match default-inspection-traffic
 class-map outside-class match port tcp eq www !

    Utilisez la commande de policy-map de passage d'exposition de visualiser les cartes de

 stratégie configurées.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 !
```

 Utilisez la commande de service-stratégie de passage d'exposition de visualiser les stratégies de service configurées.ciscoasa# sh run service-policy service-policy outside-policy interface outside

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- <u>Références de commandes de gamme de Cisco ASA 5500</u>
- Page de support du Cisco Adaptive Security Device Manager (ASDM)
- Logiciels pare-feu Cisco PIX
- Demandes de commentaires (RFC)
- Dispositifs de sécurité de la gamme Cisco PIX 500
- Application de l'inspection de protocole de la couche applicative
- <u>Références des commandes du pare-feu Cisco Secure PIX</u>
- <u>Support et documentation techniques Cisco Systems</u>