ASA 8.3 et plus tard : Inspection globale par défaut de débronchement et inspection d'application de Non-par défaut d'enable utilisant l'ASDM

Contenu

Introduction

Ce document fournit à une configuration d'échantillon pour l'appliance de sécurité adaptable Cisco (ASA) des versions 8.3(1) et plus tard 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 utilisant Adaptive Security Device Manager (ASDM).

Référez-vous à PIX/ASA 7.x : Désactivez l'inspection globale par défaut et activez l'inspection d'application de Non-par défaut pour la même configuration sur Cisco ASA avec des versions 8.2 et antérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel d'appareils de Sécurité de Cisco ASA 8.3(1) avec ASDM 6.3.

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, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

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.)

Dans l'ASDM, choisissez les **règles de configuration > de stratégie de Pare-feu > de service** de visualiser la stratégie globale par défaut qui a l'inspection par défaut d'application comme affiché ici :

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
```

Si vous devez désactiver la stratégie globale, n'utilisez l'**aucune commande globale de global_policy de service-stratégie**. Afin de supprimer la stratégie globale utilisant l'ASDM choisissez les **règles de configuration > de stratégie de Pare-feu > de service**. Puis, sélectionnez la stratégie globale et cliquez sur Delete.

Remarque: Quand vous supprimez la stratégie de service avec l'ASDM, la stratégie et les class map associés sont supprimés. Cependant, si la stratégie de service est supprimée utilisant le CLI seulement la stratégie de service est enlevée de l'interface. Le class map et la carte de stratégie restent sans changement.

Inspection globale par défaut de débronchement pour une application

Afin de désactiver l'inspection globale pour une application, n'utilisez l'*aucune* version de la commande d'**examiner**.

Par exemple, afin d'enlever l'inspection globale pour application FTP laquelle les dispositifs de sécurité écoutent, utilisez l'**aucun examinent la** commande de **FTP** dans le mode de configuration de classe.

Le mode de configuration de classe est accessible du mode de configuration de policy-map. Afin de retirer la configuration, utilisez le *forme no de la* commande.

```
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#no inspect ftp
```

Afin de désactiver l'inspection globale pour le FTP utilisant l'ASDM, terminez-vous ces étapes :

Remarque: Référez-vous à permettre à HTTPS Access pour l'ASDM pour des paramètres de base afin d'accéder au PIX/ASA par l'ASDM.

1. Choisissez les **règles de configuration > de stratégie de Pare-feu > de service** et sélectionnez la stratégie globale par défaut. Puis, cliquez sur Edit pour éditer la stratégie globale d'inspection.
2. De la fenêtre de règle de stratégie de service d'éditer, choisissez l'**inspection de Protocol** sous les **actions de règle que** tableau s'assurent que la case de **FTP** est décochée. Ceci désactive l'inspection de FTP suivant les indications de la prochaine image. Puis, cliquez sur OK et puis **appliquez**.

Remarque: Pour plus d'informations sur l'inspection de FTP, référez-vous à PIX/ASA 7.x : L'enable FTP/TFTP entretient l'exemple de configuration.

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

L'inspection améliorée de HTTP est désactivée par défaut. Afin d'activer l'inspection de HTTP dans le global_policy, utilisez la commande de **HTTP d'examiner** sous l'inspection_default de classe.

Dans cet exemple, n'importe quelle connexion HTTP (le trafic TCP sur port 80) qui entre les dispositifs de sécurité par n'importe quelle interface est classifiée pour l'inspection de HTTP. *Puisque la stratégie est une stratégie globale, l'inspection se produit seulement pendant que le trafic écrit chaque interface*.

```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

Dans cet exemple, n'importe quelle connexion HTTP (le trafic TCP sur port 80) qui entre ou quitte les dispositifs de sécurité par l'*interface extérieure est classifiée pour l'inspection de HTTP*.

```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
```

```
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Exécutez ces étapes afin de configurer l'exemple ci-dessus utilisant l'ASDM :

1. Choisissez les **règles de configuration > de stratégie de Pare-feu > de service** et cliquez sur Add afin d'ajouter une nouvelle stratégie de service :
2. De l'assistant de règle de stratégie de service d'ajouter - la fenêtre de stratégie de service, choisissent la case d'option à côté de l'**interface**. Ceci s'applique la stratégie créée à une interface spécifique, qui est l'interface **extérieure** dans cet exemple. Fournissez un nom de stratégie, qui est extérieur-Cisco-**stratégie** dans cet exemple. Cliquez sur **Next** (Suivant).
3. De l'assistant de règle de stratégie de service d'ajouter - la fenêtre de critères de Classification du trafic, fournissent le nouveau nom de classe du trafic. Le nom utilisé dans cet exemple est extérieur-**classe**. Assurez-vous que la case à côté de la **destination port de TCP ou d'UDP** est cochée et cliquez sur Next.
4. De l'assistant de règle de stratégie de service d'ajouter - correspondance du trafic - la fenêtre de destination port, choisissent la case d'option à côté du **TCP** sous la **section Protocole**. Puis, cliquez sur le bouton à côté du **service** afin de choisir le service requis.
5. Du furetage entretenez la fenêtre, choisissent le **HTTP** comme service. Puis, cliquez sur OK.
6. De l'assistant de règle de stratégie de service d'ajouter - correspondance du trafic - fenêtre de destination port, vous pouvez voir que le **service** choisi est **TCP/HTTP**. Cliquez sur **Next** (Suivant).
7. De l'assistant de règle de stratégie de service d'ajouter - ordonnez la fenêtre d'actions, cochent la case à côté du **HTTP**. Puis, cliquez sur Configure à côté du **HTTP**.
8. Du HTTP choisi examinez la fenêtre de carte, vérifient la case d'option à côté de l'**utilisation la carte par défaut d'inspection de HTTP**. L'inspection par défaut de HTTP est utilisée dans cet exemple. Puis, cliquez sur OK.
9. Cliquez sur **Finish** (Terminer).
10. Selon des **règles de configuration > de stratégie de Pare-feu > de service**, vous verrez l'extérieur-Cisco-**stratégie** nouvellement configurée de stratégie de service (pour examiner le HTTP) avec la stratégie de service par défaut déjà actuelle sur l'appliance. Cliquez sur Apply afin de s'appliquer la configuration à Cisco ASA.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Cisco Adaptive Security Device Manager
- Demandes de commentaires (RFC)
- Application de l'inspection de protocole de la couche applicative
- Support et documentation techniques - Cisco Systems