Configurez l'ASA avec des règles de contrôle d'accès de services de puissance de feu de filtrer le trafic d'AnyConnect VPN Client à l'Internet

Contenu

Introduction

Ce document décrit comment configurer des règles de la stratégie de contrôle d'accès (ACP) d'examiner le trafic qui provient des tunnels du réseau privé virtuel (VPN) ou des utilisateurs d'Accès à distance (RA) et utilise une appliance de sécurité adaptable Cisco (ASA) avec des services de puissance de feu comme passerelle internet.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- AnyConnect, Accès à distance VPN et/ou IPSec peer-to-peer VPN.
- Configuration ACP de puissance de feu.
- Cadre de stratégie modulaire ASA (MPF).

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 9.6(2.7) ASA5506W pour l'exemple ASDM
- Version 6.1.0-330 de module de puissance de feu pour l'exemple ASDM.
- Version 9.7(1) ASA5506W pour l'exemple FMC.

- Versoin 6.2.0 de puissance de feu pour l'exemple FMC.
- Version 6.2.0 du centre de Gestion de puissance de feu (FMC)

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.

Problème

ASA5500-X avec des services de puissance de feu ne peut pas filtrer et/ou examiner des utilisateurs d'AnyConnect trafiquez comme mêmes que trafiquent originaire par d'autres emplacements se sont connectés par les tunnels d'IPSec qui utilisent un seul point de sécurité du contenu permietral.

Un autre symptôme que cette solution couvre est de ne pouvoir pas définir des règles spécifiques ACP aux sources mentionnées sans l'autre affectation de sources.

Ce scénario est très commun pour voir quand la conception de TunnelAll est utilisée pour des solutions VPN terminées sur une ASA.

Solution

Ceci peut être réalisé par de plusieurs manières. Cependant, ce scénario couvre l'inspection par des zones.

Configuration ASA

Étape 1. Identifiez les interfaces où les utilisateurs ou les tunnels VPN d'AnyConnect se connectent à l'ASA.

Pair à scruter tunnels

C'est une chute de la sortie de **crypto map de passage d'exposition**.

```
crypto map outside_map interface outside
```

Utilisateurs d'AnyConnect

L'exposition de commande **exécutent des** expositions de **webvpn** où l'accès d'AnyConnect est activé.

```
webvpn
 enableoutside hostscan image disk0:/hostscan_4.3.05019-k9.pkg hostscan enable anyconnect image
disk0:/anyconnect-win-4.4.01054-webdeploy-k9.pkg 1 anyconnect image disk0:/anyconnect-macos-
4.4.01054-webdeploy-k9.pkg 2 anyconnect enable
```

Dans ce scénario, l'**extérieur d'**interface reçoit, les utilisateurs de RA et le pair pour scruter des tunnels.

Étape 2. Réorientez le trafic de l'ASA au module de puissance de feu avec une stratégie globale.

Il peut être fait avec une condition de **match any** ou une liste de contrôle d'accès définie (ACL) pour la redirection du trafic.

Exemple avec la correspondance de **match any**.

```
class-map SFR
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

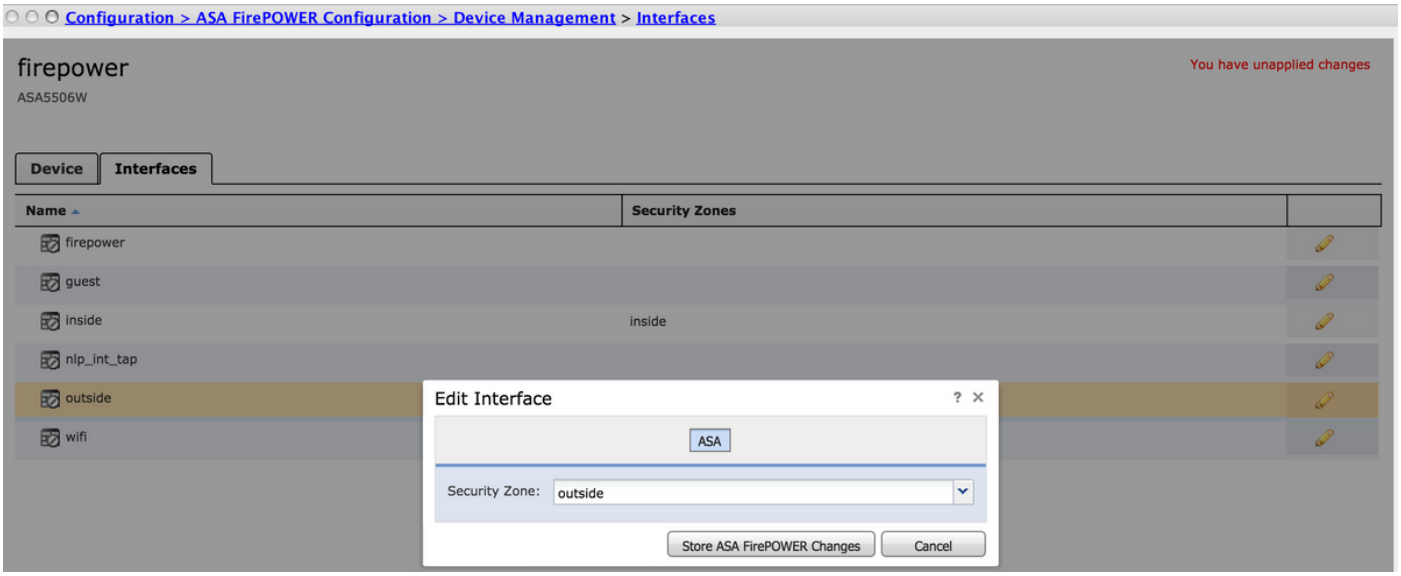
Exemple avec la correspondance d'ACL.

```
access-list sfr-acl extended permit ip any any

class-map SFR
 match access-list sfr-acl

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

Dans un scénario moins commun, une stratégie de service peut être utilisée pour l'interface extérieure. Cet exemple n'est pas couvert dans ce document.

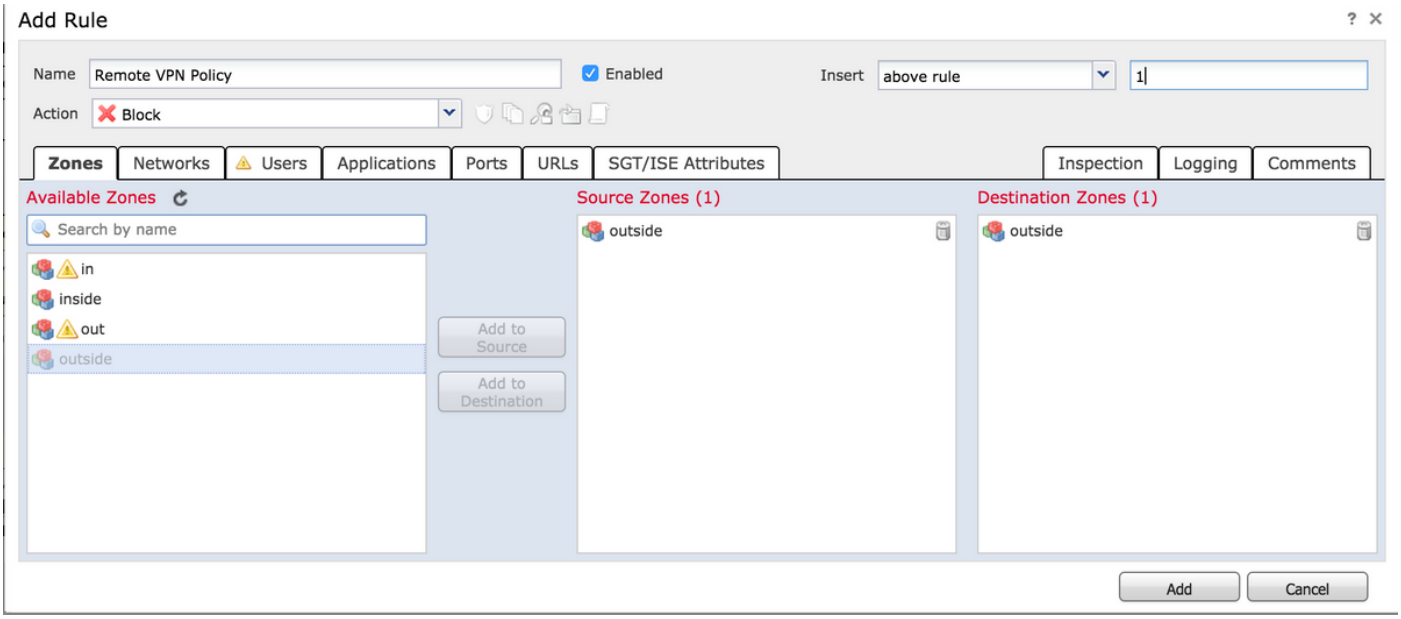
Module de puissance de feu ASA géré par configuration ASDM

Étape 1. Assignez à l'interface extérieure une zone à **Gestion de périphériques de configuration > de puissance de feu ASA à configuration >**. Dans ce cas, cette zone s'appelle **dehors**.



Étape 2. Choisi **ajoutez la règle à la configuration de configuration > de puissance de feu ASA > aux stratégies > à la stratégie de contrôle d'accès**.

Étape 3. **Des zones** tabulez, zone **extérieure** choisie comme source et destination pour votre règle.



Étape 4. Sélectionnez l'action, le titre et toutes les autres conditions désirées de définir cette règle.

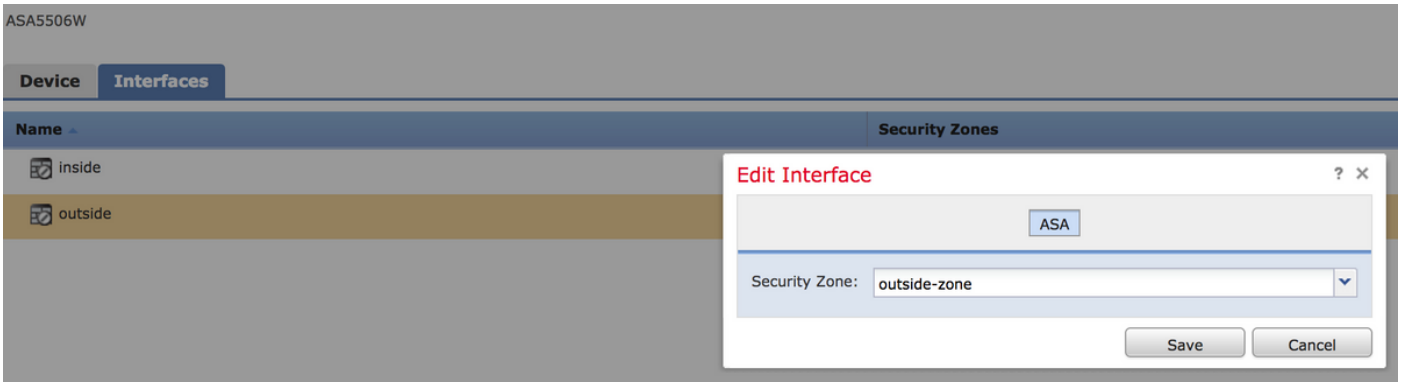
De plusieurs règles peuvent être créées pour cette circulation. Il est simplement important de maintenir dans l'esprit que les zones de source et de destination doivent être la zone assignée aux sources et à l'Internet VPN.

Assurez-vous qu'il n'y a de pas autres stratégies plus générales qui pourraient s'assortir avant ces règles. Il est preferrable pour avoir ces règles au-dessus de celles définies à **n'importe quelle** zone.

Étape 5. Cliquez sur en fonction les **modifications de puissance de feu de la mémoire ASA** et **déployez** alors les **modifications de puissance de feu** pour faire le prendre effet ces modifications.

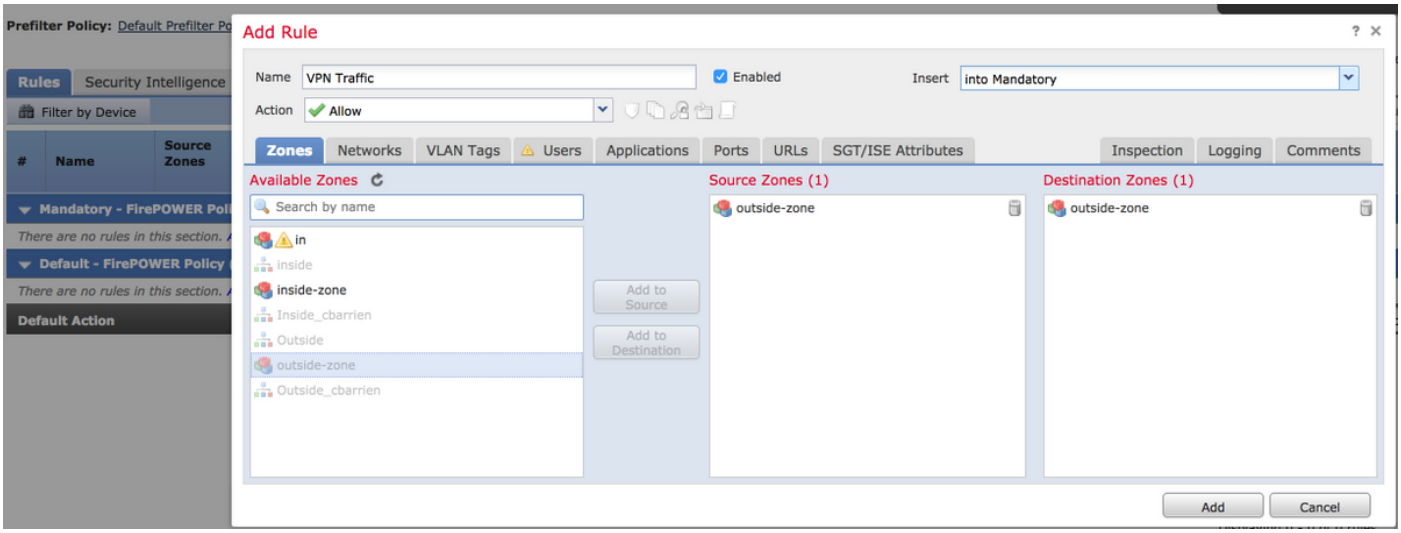
Module de puissance de feu ASA géré par configuration FMC

Étape 1. Assignez à l'interface extérieure une zone aux **périphériques > à la Gestion > aux interfaces**. Dans ce cas, cette zone s'appelle l'extérieur-**zone**.



Étape 2. Choisi **ajoutez la règle aux stratégies > au contrôle d'accès > éditent**.

Étape 3. **Des zones** tabulez, zone choisie d'extérieur-**zone** comme source et destination pour votre règle.



Étape 4. Sélectionnez l'action, le titre et toutes les autres conditions désirées de définir cette règle.

De plusieurs règles peuvent être créées pour cette circulation. Il est simplement important de maintenir dans l'esprit que les zones de source et de destination doivent être la zone assignée aux sources et à l'Internet VPN.

Assurez-vous qu'il n'y a de pas autres stratégies plus générales qui pourraient s'assortir avant ces règles. Il est preferrable pour avoir ces règles au-dessus de celles définies à **n'importe quelle** zone.

Étape 5. Cliquez sur en fonction la **sauvegarde** et **déployez-vous** alors pour faire le prendre effet ces modifications.

Résultat

Après que le déploiement termine, le trafic d'AnyConnect est maintenant filtré/examiné par les règles ACP appliquées. Dans cet exemple, un URL a été avec succès bloqué.