Configurar o ASA com regras do controle de acesso dos serviços da potência de fogo para filtrar o tráfego do cliente VPN de AnyConnect ao Internet

Índice

Introdução

Este documento descreve como configurar regras da política do controle de acesso (ACP) para inspecionar o tráfego que vem dos túneis do Virtual Private Network (VPN) ou dos usuários do Acesso remoto (RA) e usa uma ferramenta de segurança adaptável de Cisco (ASA) com serviços da potência de fogo como o Gateway de Internet.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- AnyConnect, acesso remoto VPN e/ou IPSec VPN peer-to-peer.
- Configuração ACP da potência de fogo.
- Estrutura de política modular ASA (MPF).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 9.6(2.7) ASA5506W para o exemplo de ASDM
- Versão 6.1.0-330 do módulo da potência de fogo para o exemplo de ASDM.
- Versão 9.7(1) ASA5506W para o exemplo FMC.
- Versoin 6.2.0 da potência de fogo para o exemplo FMC.

- Versão 6.2.0 do centro de gerenciamento da potência de fogo (FMC)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Problema

ASA5500-X com serviços da potência de fogo é incapaz de filtrar e/ou para inspecionar usuários de AnyConnect trafique como mesmos que o tráfego originado por outros lugar conectados pelos túneis de IPsec que usam um único ponto da Segurança satisfeita permietral.

Um outro sintoma que esta solução cobre é ser incapaz de definir regras específicas ACP às fontes mencionadas sem o outro emprego das fontes.

Esta encenação é muito comum considerar quando o projeto de TunnelAll é usado para as soluções de VPN terminadas em um ASA.

Solução

Isto pode ser conseguido através das formas múltiplas. Contudo, esta encenação cobre a inspeção por zonas.

Configuração ASA

Etapa 1. Identifique as relações onde os usuários de AnyConnect ou os túneis VPN conectam ao ASA.

Par a espreitar túneis

Esta é uma sucata da saída do **crypto map da corrida da mostra**.

```
crypto map outside_map interface outside
```

Usuários de AnyConnect

O webvpn do comando show run mostra onde o acesso de AnyConnect é permitido.

```
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
```

Nesta encenação, a **parte externa da** relação recebe, usuários RA e par para espreitar túneis.

Etapa 2. Reoriente o tráfego do ASA ao módulo da potência de fogo com uma política global.

Pode ser feita com um **fósforo toda a** condição ou um Access Control List definido (ACL) para a reorientação do tráfego.

Exemplo com **fósforo algum** fósforo.

```
class-map SFR
```

```
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

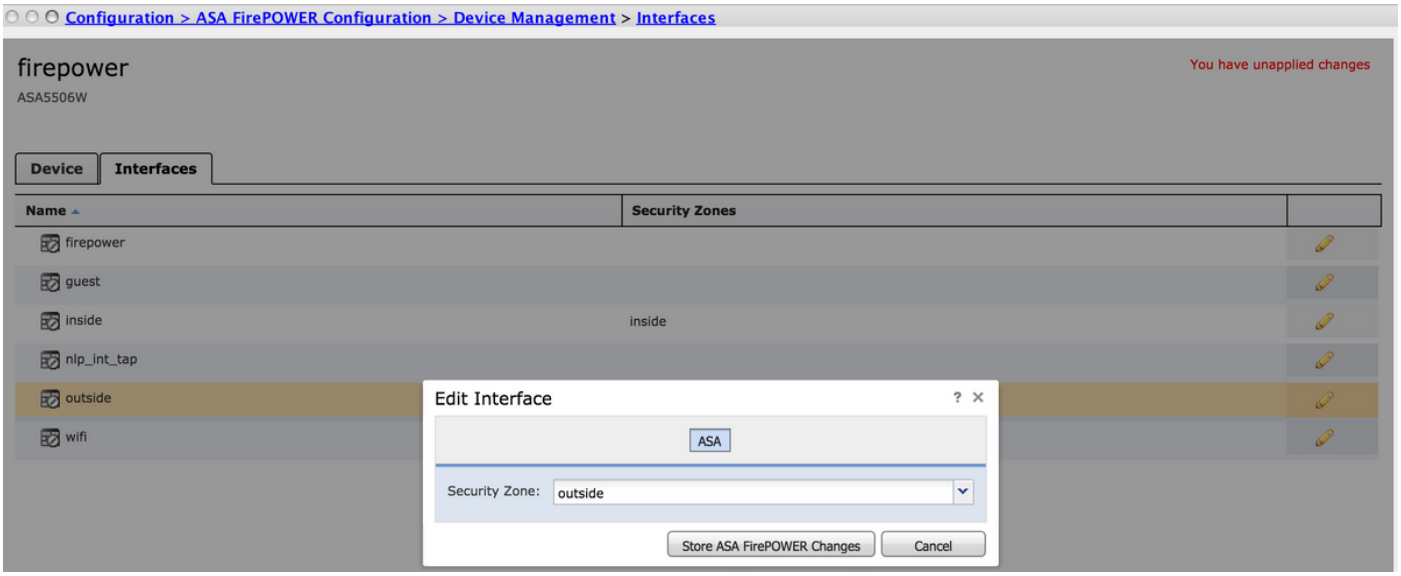
Exemplo com fósforo ACL.

```
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
```

Em menos cenário comum, uma política de serviços pode ser usada para a interface externa. Este exemplo não é coberto neste documento.

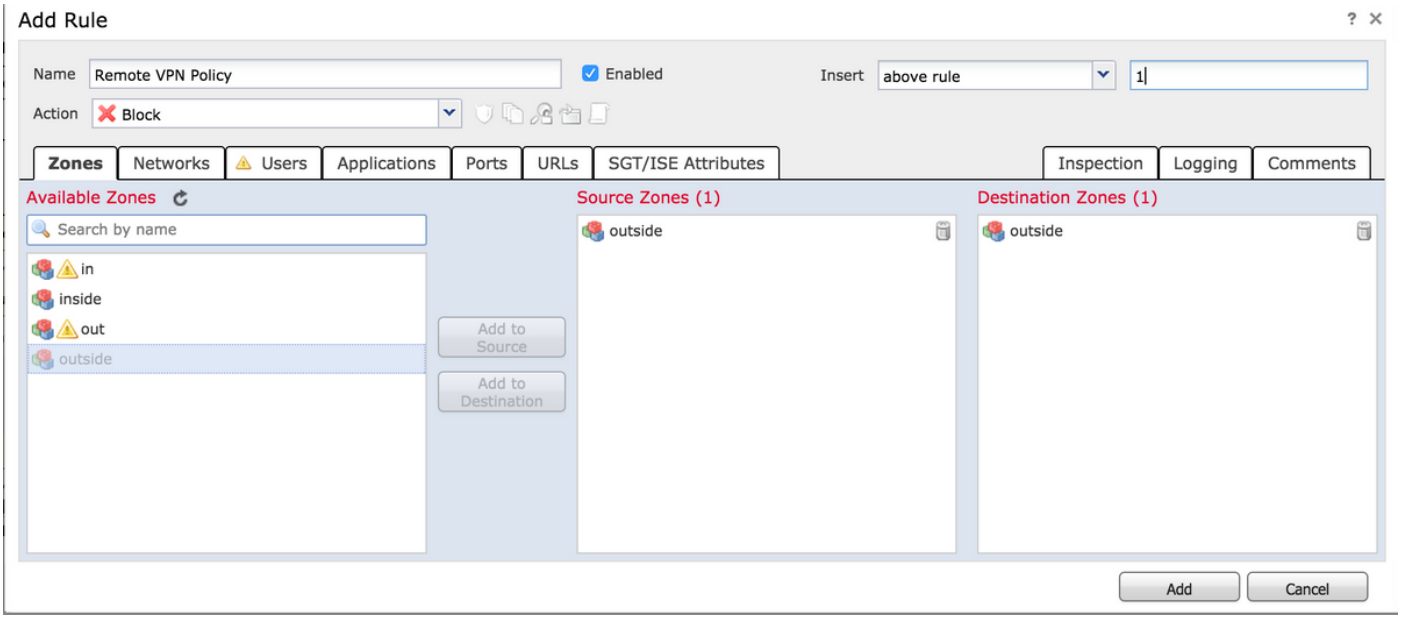
Módulo da potência de fogo ASA controlado pela configuração ASDM

Etapa 1. Atribua à interface externa uma zona em **Gerenciamento de dispositivos da configuração > da potência de fogo ASA em configuração >**. Neste caso, essa zona é chamada **fora**.



Etapa 2. Seleto **adicionar a regra na configuração da configuração > da potência de fogo ASA > nas políticas > na política do controle de acesso**.

Etapa 3. **Das zonas** catalogue, selecione a zona **exterior** como a fonte e o destino para sua regra.



Etapa 4. Selecione a ação, o título e todas as outras circunstâncias desejadas para definir esta regra.

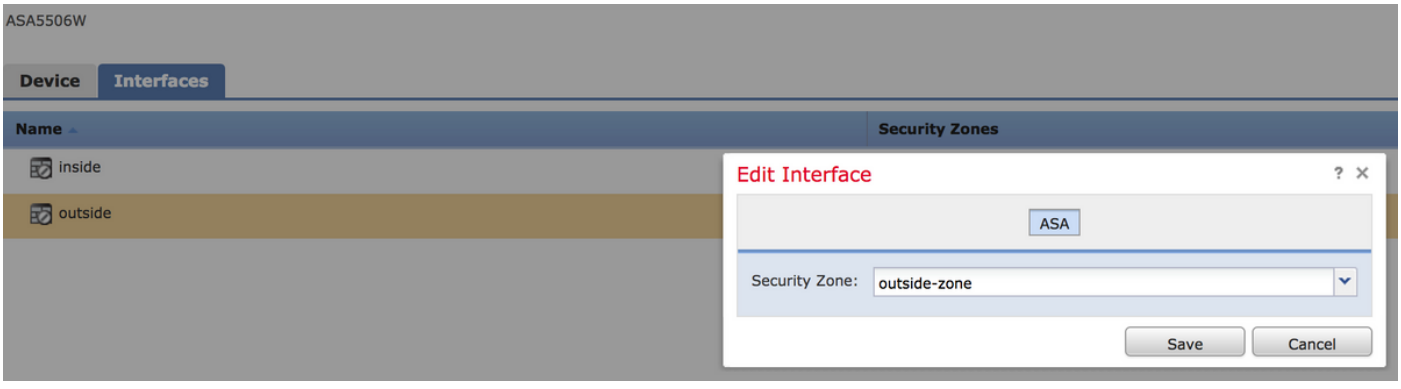
As regras múltiplas podem ser criadas para este fluxo de tráfego. É apenas importante manter-se na mente que a fonte e as zonas de destino devem ser a zona atribuída às fontes e ao Internet VPN.

Certifique-se de que há não outras mais políticas gerais que poderiam combinar antes destas regras. É preferrable ter estas regras acima de essas definidas a **toda a** zona.

Etapa 5. Clique sobre **mudanças da potência de fogo da loja ASA** e **distribua** então **mudanças da potência de fogo** para mandar estas mudanças tomar o efeito.

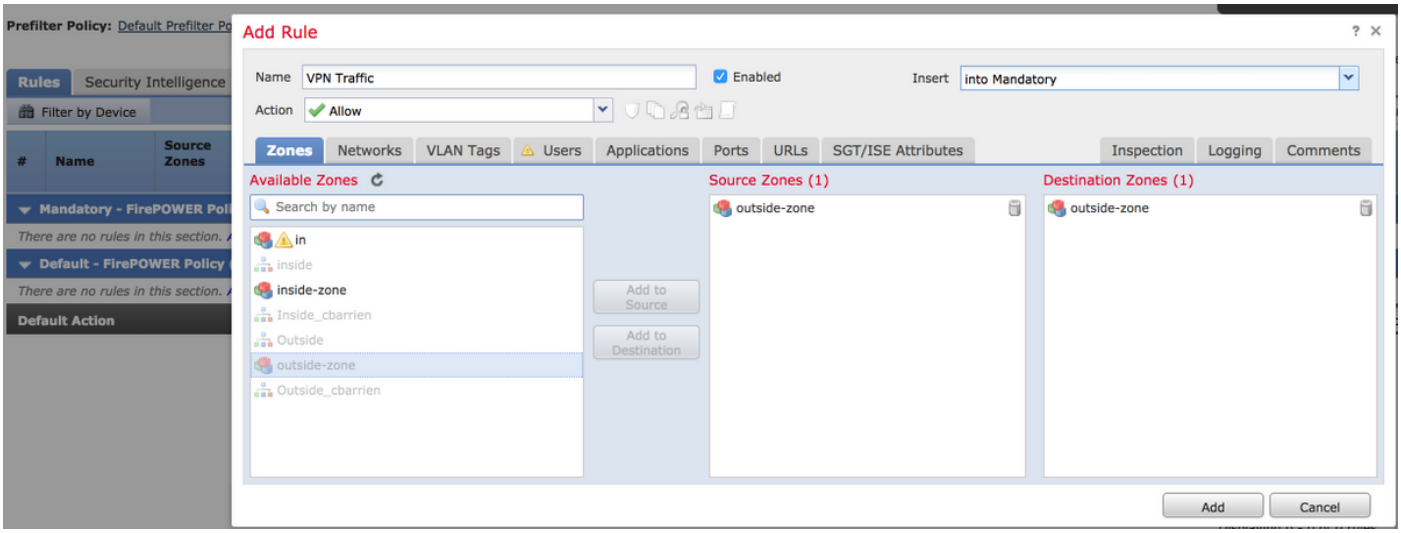
Módulo da potência de fogo ASA controlado pela configuração FMC

Etapa 1. Atribua à interface externa uma zona em **dispositivos > em Gerenciamento > em relações**. Neste caso, essa zona é chamada parte-**zona**.



Etapa 2. Seleto **adicionar a regra em políticas > em controle de acesso > editam**.

Etapa 3. **Das zonas** catalogue, selecione a zona da parte-**zona** como a fonte e o destino para sua regra.



Etapa 4. Selecione a ação, o título e todas as outras circunstâncias desejadas para definir esta regra.

As regras múltiplas podem ser criadas para este fluxo de tráfego. É apenas importante manter-se na mente que a fonte e as zonas de destino devem ser a zona atribuída às fontes e ao Internet VPN.

Certifique-se de que há não outras mais políticas gerais que poderiam combinar antes destas regras. É preferrable ter estas regras acima de essas definidas a **toda a** zona.

Etapa 5. Clique sobre a **salvaguarda** e **distribua-a** então para mandar estas mudanças tomar o efeito.

Resultado

Depois que o desenvolvimento termina, o tráfego de AnyConnect agora está filtrado/inspecionado pelas regras ACP aplicadas. Neste exemplo, uma URL foi obstruída com sucesso.