La configuración ASA con la potencia de fuego mantiene las reglas del control de acceso para filtrar el tráfico del cliente VPN de AnyConnect a Internet

Contenido

Introducción

Este documento describe cómo configurar las reglas de la directiva del control de acceso (ACP) para examinar el tráfico que viene de los túneles del Red privada virtual (VPN) o de los usuarios del Acceso Remoto (RA) y utiliza un dispositivo de seguridad adaptante de Cisco (ASA) con los servicios de la potencia de fuego como gateway de Internet.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- IPSec VPN de AnyConnect, del VPN de acceso remoto y/o del peer a peer.
- Configuración de la potencia de fuego ACP.
- Marco de políticas modular ASA (MPF).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 9.6(2.7) ASA5506W para el ejemplo de ASDM
- Versión 6.1.0-330 del módulo de la potencia de fuego para el ejemplo de ASDM.
- Versión 9.7(1) ASA5506W por el ejemplo FMC.

- Versoin 6.2.0 de la potencia de fuego por el ejemplo FMC.
- Versión 6.2.0 del centro de administración de la potencia de fuego (FMC)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

ASA5500-X con los servicios de la potencia de fuego no puede filtrar y/o examinar a los usuarios de AnyConnect trafique como lo mismo que el tráfico originado por otras ubicaciones conectadas por los túneles IPsec que utilizan un monopunto de la Seguridad contenta permietral.

Otro síntoma que esta solución cubre es no poder definir las reglas específicas ACP a las fuentes mencionadas sin la otra afectación de las fuentes.

Este escenario es muy común considerar cuando el diseño de TunnelAll se utiliza para las soluciones de VPN terminadas en un ASA.

Solución

Esto se puede alcanzar a través de las diferentes formas. Sin embargo, este escenario cubre el examen por las zonas.

Configuración ASA

Paso 1. Identifique las interfaces donde los usuarios de AnyConnect o los túneles VPN conectan con el ASA.

Par a mirar túneles

Esto es un pedazo de la salida de la **correspondencia de criptografía del funcionamiento de la demostración**.

```
crypto map outside_map interface outside
```

Usuarios de AnyConnect

El webvpn del comando show run muestra donde se habilita el acceso de AnyConnect.

```
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
```

En este escenario, el **exterior de la** interfaz recibe, los usuarios RA y par para mirar los túneles.

Paso 2. Reoriente el tráfico del ASA al módulo de la potencia de fuego con una política global.

Puede ser hecha con una **coincidencia cualquier** condición o una lista de control de acceso (ACL) definida para el cambio de dirección del tráfico.

El ejemplo con la **coincidencia ninguno** hace juego.

```
class-map SFR
 match any

policy-map global_policy
 class SFR
   sfr fail-open

service-policy global_policy global
```

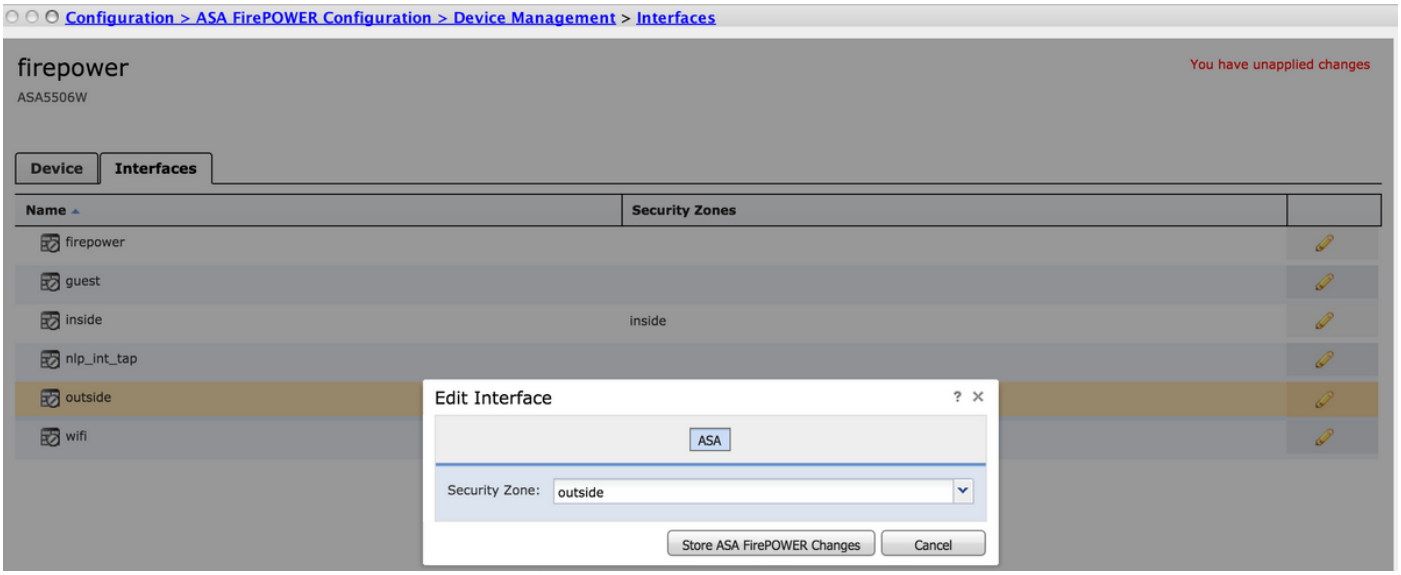
Ejemplo con la coincidencia ACL.

```
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
```

En un menos escenario frecuente, una política de servicio se puede utilizar para la interfaz exterior. Este ejemplo no se cubre en este documento.

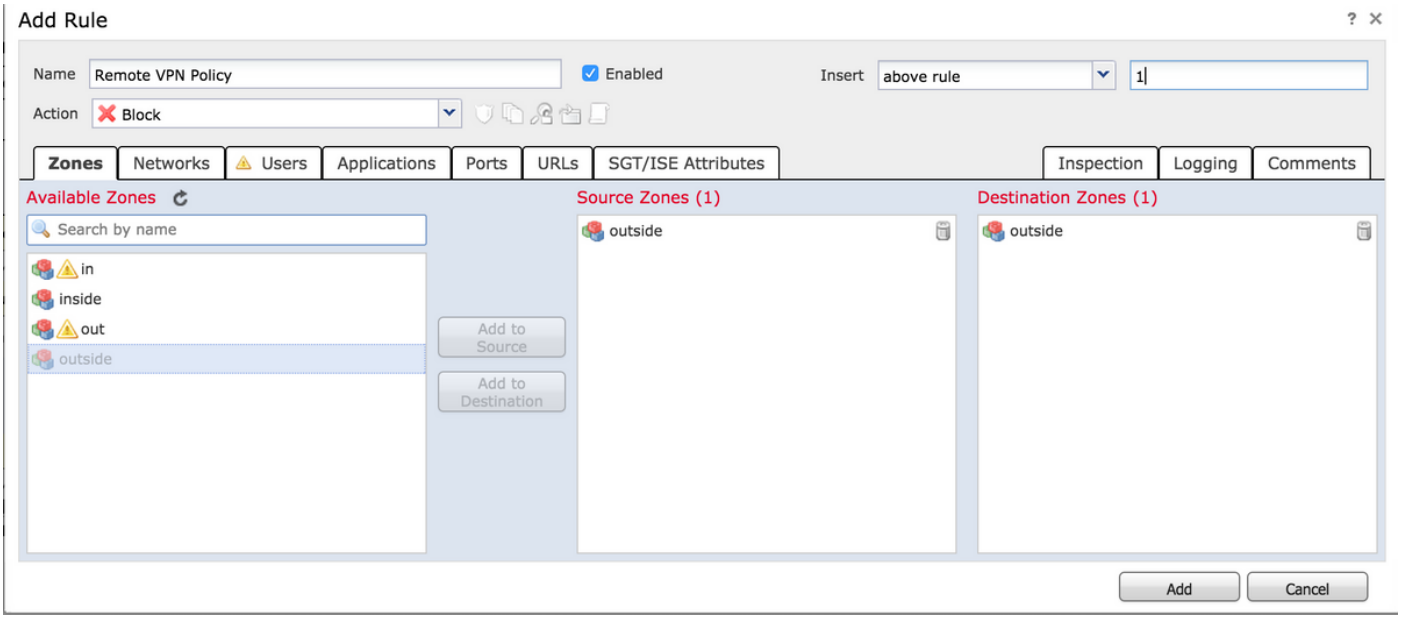
Módulo de la potencia de fuego ASA manejado por la Configuración de ASDM

Paso 1. Asigne a interfaz exterior una zona en la **Administración de dispositivos de la configuración > de la potencia de fuego ASA configuración >**. En este caso, esa zona se llama **afuera**.



Paso 2. Selecto **agregue la regla** en la **configuración de la configuración > de la potencia de fuego ASA > las directivas > la directiva del control de acceso**.

Paso 3. **De las zonas** tabule, seleccione la zona **exterior** como fuente y el destino para su regla.



Paso 4. Seleccione la acción, el título y cualquier otra condición deseada para definir esta regla.

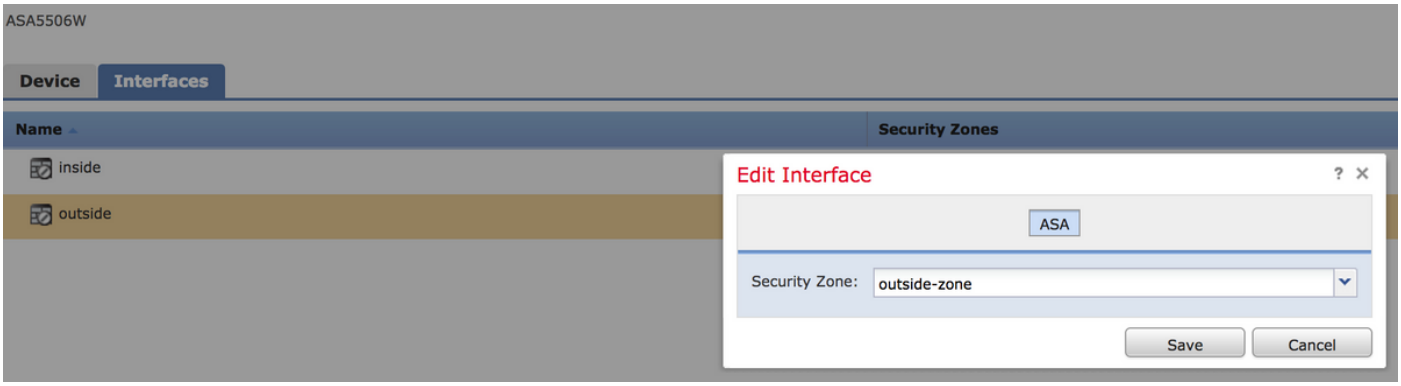
Las reglas múltiples se pueden crear para este flujo de tráfico. Es apenas importante tener presente que la fuente y las Zonas de destino deben ser la zona asignada a las fuentes y a Internet VPN.

Aseegurese que hay no otras más políticas generales que podrían hacer juego antes de estas reglas. Es preferrable tener estas reglas sobre las definidas a **cualquier** zona.

Paso 5. Haga clic en los **cambios de la potencia de fuego del almacén ASA** y después **despliegue los cambios de la potencia de fuego** para hacer que estos cambios tomen el efecto.

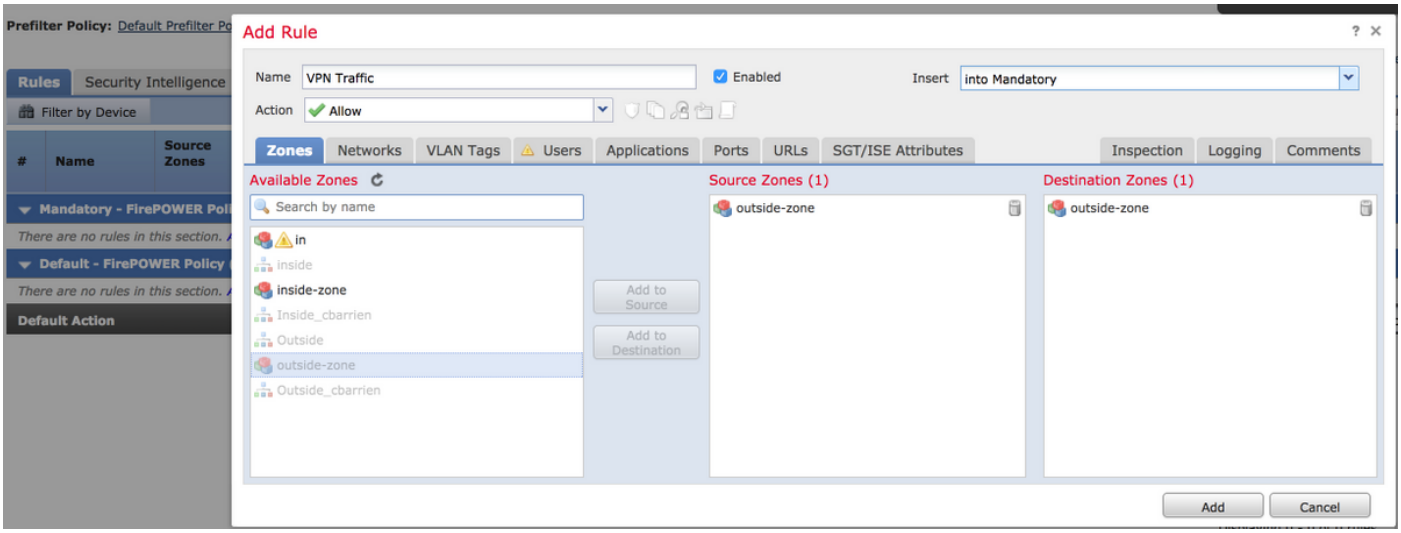
Módulo de la potencia de fuego ASA manejado por la configuración FMC

Paso 1. Asigne a interfaz exterior una zona en los **dispositivos > la Administración > las interfaces**. En este caso, esa zona se llama exterior-**zona**.



Paso 2. Selecto **agregue la regla** en las **directivas > el control de acceso > editan**.

Paso 3. **De las zonas** tabule, seleccione la zona de la exterior-**zona** como fuente y el destino para su regla.



Paso 4. Seleccione la acción, el título y cualquier otra condición deseada para definir esta regla.

Las reglas múltiples se pueden crear para este flujo de tráfico. Es apenas importante tener presente que la fuente y las Zonas de destino deben ser la zona asignada a las fuentes y a Internet VPN.

Aseegurese que hay no otras más políticas generales que podrían hacer juego antes de estas reglas. Es preferrable tener estas reglas sobre las definidas a **cualquier** zona.

Paso 5. Haga clic en la **salvaguardia** y después **despliegúela** para hacer que estos cambios tomen el efecto.

Resultado

Después de que el despliegue acabe, el tráfico de AnyConnect ahora es filtrado/examinado por las reglas ACP aplicadas. En este ejemplo, un URL fue bloqueado con éxito.