# Configurar o ASA com regras do controle de acesso dos serviços de FirePOWER para filtrar o tráfego do cliente VPN de AnyConnect ao Internet

# Índice

Introdução Pré-requisitos Requisitos Componentes Utilizados Problema Solução Configuração ASA Módulo ASA FirePOWER controlado pela configuração ASDM Módulo ASA FirePOWER controlado pela configuração FMC Resultado

## 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 de FirePOWER 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 de FirePOWER ACP.
- 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 de FirePOWER para o exemplo de ASDM.
- Versão 9.7(1) ASA5506W para o exemplo FMC.
- Versoin 6.2.0 de FirePOWER para o exemplo FMC.

• Versão 6.2.0 do centro de gerenciamento de FirePOWER (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 de FirePOWER 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
enable outside
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 de FirePOWER 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.

```
webvpn
enable outside
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
Exemplo com fósforo ACL.
```

```
webvpn
enable outside
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
```

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

#### Módulo ASA FirePOWER controlado pela configuração ASDM

Etapa 1. Atribua à interface externa uma zona na **configuração > na configuração > no Gerenciamento de dispositivos ASA FirePOWER**. Neste caso, essa zona é chamada **fora**.

○ ○ ○ <u>Configuration &gt; ASA FirePOWER Configuration &gt; Device Management &gt; Interfaces</u>										
firepower ASA5506W			You have unapplied changes							
Device Interfaces										
Name 🔺	Security Zones									
😿 firepower			Ø							
🔂 guest			Ø							
inside	inside		Ø							
nlp_int_tap			Ø							
🔂 outside	Edit Interface	? ×	Ø							
🛃 wifi	ASA		Ø							
	Security Zone: outside									
	Store ASA FirePOWE	R Changes Cancel								

Etapa 2. Seleto adicionar a regra na configuração > na configuração ASA FirePOWER > 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.

Add Rule

Name Remote VPN Policy		Enabled	Insert above rule	▶ 1	
Action X Block	VD.24				
Zones Networks 🛆 Users Application	s Ports URLs	SGT/ISE Attributes		Inspection	Logging Comments
Available Zones 🕐	S	ource Zones (1)		Destination Zones (1)	)
Search by name	d	🥞 outside	1	🥞 outside	1
🥞 🔔 in					
🥞 inside					
🤹 🛆 out	Add to Source				
🖓 outside					
	Destination				
					Add Cancel

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 loja ASA FirePOWER** e **distribua** então **mudanças de FirePOWER** para mandar estas mudanças tomar o efeito.

#### Módulo ASA FirePOWER 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**.

ASA5506W		
Device Interfaces		
Name 🔺	Security Zones	
😥 inside	Edit Interface	? ×
😥 outside	ASA	
	Security Zone: outside-zone	¥
	Sav	e Cancel

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.

Prefilter Policy: Default Prefilter Po Add Rule										?	×					
Rules Security Intelligence		Name VPN Traffic			C Enabled		Insert	Insert into Mandatory			~					
	Filter by Device	Source	Zone	<ul> <li>Allow</li> <li>Networks</li> </ul>	VLAN Tags	🔺 Users	Applications	Ports	URLs	SGT/ISE Attributes	5		Inspection	Logging	Comments	
# Name Zones		Zones	Available Zones C				Source Zones (1)				Destination Zones (1)					
Mandatory - FirePOWER Poll					🥞 outs	ide-zone		6	🥞 outs	ide-zone		6	1			
There are no rules in this section.		<ul> <li>         In          inside         Inside-zone         inside-zone         inside_cbarrien         </li> </ul>			Add to Source Add to Destination											
Default - FirePOWER Policy (																
There are no rules in this section.																
Default Action																
		📩 Outside														
		🥞 outs	ide-zone													
		📩 Outs	side_cbarrien													
													Add	Cancel		

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.



You are attempting to access a forbidden site.

Consult your system administrator for details.