ASA met FirePOWER Services Access Control Regels configureren om AnyConnect VPNclientverkeer naar internet te filteren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Probleem Oplossing ASA-configuratie ASA FirePOWER-module beheerd door ASDM-configuratie ASA FirePOWER-module beheerd door FMC-configuratie Resultaat

Inleiding

Dit document beschrijft hoe u de Access Control Policy (ACS) regels kunt configureren voor het inspecteren van verkeer dat afkomstig is van VPN-tunnels of gebruikers van Remote Access (RA) en een Cisco adaptieve security applicatie (ASA) kunt gebruiken met FirePOWER Services als internetgateway.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- AnyConnect, Remote Access VPN en/of peer-to-peer IPSec VPN.
- Firepower ACS configuratie.
- ASA modulair beleidskader (MPF).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA 5506W versie 9.6(2.7) voor ASDM-voorbeeld
- FirePOWER Module versie 6.1.0-30 voor ASDM voorbeeld.
- ASA 5506W versie 9.7(1) voor het FMC voorbeeld.
- FirePOWER versie 6.2.0 voor het FMC-voorbeeld.
- Firepower Management Center (FMC) versie 6.2.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Probleem

ASA 5500-X met FirePOWER Services is niet in staat om AnyConnect-gebruikersverkeer te filteren en/of te inspecteren zoals verkeer dat is gegenereerd door andere locaties die zijn aangesloten door IPSec-tunnels die gebruik maken van één punt van voorlopige contentbeveiliging.

Een ander symptoom waarop deze oplossing betrekking heeft, is dat het niet mogelijk is om specifieke ACS-regels voor de genoemde bronnen vast te stellen zonder dat andere bronnen van invloed zijn.

Dit scenario is zeer gebruikelijk om te zien wanneer TunnelAll ontwerp wordt gebruikt voor VPN oplossingen die op een ASA beëindigd worden.

Oplossing

Dit kan op meerdere manieren worden bereikt. Dit scenario betreft echter de inspectie per gebied.

ASA-configuratie

Stap 1. Identificeer de interfaces waar AnyConnect-gebruikers of VPN-tunnels met de ASA verbonden zijn.

Peer-to-peer tunnels

Dit is een schroot van de show run crypto map output.

crypto map outside_map interface **outside**

AnyConnect-gebruikers

De opdracht toont een webvpn die aansluit, laat zien waar AnyConnect-toegang is ingeschakeld.

```
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
```

In dit scenario ontvangt interface buiten zowel RA gebruikers als peer to Peer tunnels.

Stap 2. Verkeer verkeer van ASA naar FirePOWER-module met een mondiaal beleid.

Dit kan met een overeenkomende voorwaarde of met een gedefinieerde toegangscontrolelijst

(ACL) voor verkeersomleiding worden gedaan.

Bijvoorbeeld met elke match.

```
class-map SFR
match any
policy-map global_policy
class SFR
sfr fail-open
service-policy global_policy global
Voorbeeld met ACL-wedstrijd.
```

```
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
```

In een minder gemeenschappelijk scenario kan een dienstbeleid voor de buiteninterface worden gebruikt. Dit voorbeeld wordt in dit document niet behandeld.

ASA FirePOWER-module beheerd door ASDM-configuratie

Stap 1. Pas de externe interface één zone toe bij **Configuratie > ASA FirePOWER Configuration > Apparaatbeheer**. In dit geval wordt die zone **buiten** genoemd.

5 0 0 computation > AsA Hierower computation > Device management > Interfaces										
firepower ASA5506W				You have una	applied changes					
Device Interfaces										
Name 🔺		Security Zones								
7 firepower					Ø					
😨 guest					Ø					
🔂 inside		inside			Ø					
nlp_int_tap					Ø					
🔂 outside	Edit Interface		? ×		Ø					
🔂 wifi		ASA			Ø					
	Security Zone: outside		~							
		Store ASA FirePOWER Changes	Cancel							

Stap 2. Selecteer Toevoegen regel bij configuratie > ASA FirePOWER Configuration > Policy > Access Control Policy.

Stap 3. Selecteer buiten zone op het tabblad Gebieden als bron en als bestemming voor uw regel.

Add Rule

Name Remote VPN Policy		Enabled	Insert	above rule		✓ 1		
Action 🔀 Block	• • • • 2 *							
Zones Networks 🛆 Users Application	s Ports URLs	SGT/ISE Attributes				Inspection	Logging	Comments
Available Zones 🕐	S	ource Zones (1)			Destinatio	on Zones (1)		
Search by name	d	觷 outside		8	🥞 outsid	е		i
🥞 🔔 in								
🥵 inside								
🥞 🔔 out	Add to Source							
Note that the second se	Add to							
	Destination							
							Add	Cancel

Stap 4. Selecteer de actie, de titel en alle andere gewenste voorwaarden om deze regel te definiëren.

Er kunnen meerdere regels worden gecreëerd voor deze verkeersstroom. Het is alleen belangrijk om in gedachten te houden dat bron- en doelgebieden de zone moeten zijn die is toegewezen aan VPN-bronnen en internet.

Zorg ervoor dat er geen andere, meer algemene beleidslijnen zijn die vóór deze regels zouden kunnen overeenkomen. Het verdient de voorkeur deze regels boven de regels te stellen die boven elke zone zijn vastgesteld.

Stap 5. Klik op **Store ASA FirePOWER Veranderingen** en **implementeer FirePOWER Wijzigingen** om deze veranderingen van kracht te laten worden.

ASA FirePOWER-module beheerd door FMC-configuratie

Stap 1. Pas de externe interface aan in één zone op apparaten > Beheer > Interfaces	. In dit geval
heet die zone buiten de zone .	

ASA5506W		
Device Interfaces		
Name 🔺	Security Zones	
inside	Edit Interface	? ×
Doutside	ASA	
	Security Zone: outside-zone	~
	Save	Cancel

Stap 2. Selecteer Regel op beleid toevoegen > Toegangsbeheer > Bewerken.

Stap 3. Selecteer op het tabblad **Gebieden** de zone **buiten de zone** als bron en als bestemming voor de regel.

Prefilter Policy: Default Prefilter Po Add Rule ? ×																
Rul	Rules Security Intelligence Name VPN Traffic			C Enabled		Insert	sert into Mandatory				~					
	ilter by Device	Source	Zone	Allow Networks	VLAN Tags	△ Users	Applications	Ports	URLs	SGT/ISE Attributes			Inspection	Logging	Comments	
# Name Zones			Available Zones C				Source Zones (1)				Destinat	ion Zones (1)				
Mandatory - FirePOWER Poli Search by name							🥞 outs	ide-zone		i	🥞 outs	ide-zone		ĩ	1	
There are no rules in this section.		this section. /	🧠 🛕 in a≞a inside		Add to											
Default - FirePOWER Policy		WER Policy														
There are no rules in this section.		this section. /	🥞 inside-zone													
Default Action		inside_cbarrien														
		- Outs	🚠 Outside		Add to Destination											
		Sutside_zone														
														Add	Cancel	

Stap 4. Selecteer de actie, de titel en alle andere gewenste voorwaarden om deze regel te definiëren.

Er kunnen meerdere regels worden gecreëerd voor deze verkeersstroom. Het is alleen belangrijk om in gedachten te houden dat bron- en doelgebieden de zone moeten zijn die is toegewezen aan VPN-bronnen en internet.

Zorg ervoor dat er geen andere, meer algemene beleidslijnen zijn die vóór deze regels zouden kunnen overeenkomen. Het verdient de voorkeur deze regels boven de regels te stellen die boven elke zone zijn vastgesteld.

Stap 5. Klik op Opslaan en implementeer deze wijzigingen in werking.

Resultaat

Nadat de installatie is voltooid, wordt het AnyConnect-verkeer nu gefilterd/geïnspecteerd door de van toepassing zijnde ACS-regels. In dit voorbeeld werd een URL met succes geblokkeerd.



You are attempting to access a forbidden site.

Consult your system administrator for details.