配置具備FirePOWER服務訪問控制規則的ASA以 過濾AnyConnect VPN客戶端流量到網際網路

目錄

簡介 必要條件 需求 採用元件 問題 解決方案 ASA配置 由ASDM配置管理的ASA FirePOWER模組 由FMC配置管理的ASA FirePOWER模組 結果

簡介

本檔案介紹如何設定存取控制原則(ACP)規則,以檢查來自虛擬私人網路(VPN)通道或遠端存取 (RA)使用者的流量,以及將具備FirePOWER服務的思科調適型安全裝置(ASA)用作網際網路閘道。

必要條件

需求

思科建議您瞭解以下主題:

- AnyConnect、遠端訪問VPN和/或點對點IPSec VPN。
- Firepower ACP配置。
- •ASA模組化策略框架(MPF)。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 適用於ASDM的ASA5506W 9.6(2.7)版示例
- 適用於ASDM的FirePOWER模組版本6.1.0-330示例。
- 適用於FMC的ASA5506W 9.7(1)版示例。
- 適用於FMC的FirePOWER版本6.2.0範例。
- Firepower管理中心(FMC)版本6.2.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

問題

具備FirePOWER服務的ASA5500-X無法過濾和/或檢查AnyConnect使用者流量,這些流量與源自 IPSec隧道所連線的其他位置的流量相同,這些隧道使用單點永久內容安全。

此解決方案所涵蓋的另一個症狀是無法定義針對所提及資源的特定ACP規則而不受其他資源的影響 。

在ASA上終止的VPN解決方案使用TunnelAll設計時,經常會看到這種情況。

解決方案

這可以通過多種方式實現。但是,此方案包含按區域進行的檢查。

ASA配置

步驟1. 確定AnyConnect使用者或VPN隧道連線到ASA的介面。

對等通道

這是show run crypto map 輸出的一個片段。

crypto map outside_map interface **outside**

AnyConnect使用者

show run webvpn 命令會顯示啟用AnyConnect存取的位置。

```
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
在此案例中,介面outside會同時接收RA使用者和對等通道。
```

步驟2. 使用全域性策略將流量從ASA重定向到FirePOWER模組。

可使用任何相符條件**或定義**的存取控制清單(ACL)進行流量重新導向。

match any match示例。

```
class-map SFR
match any
policy-map global_policy
class SFR
sfr fail-open
```

service-policy global_policy global ACL匹配示例。 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

在不太常見的情況下,服務策略可用於外部介面。本檔案沒有說明此範例。

由ASDM配置管理的ASA FirePOWER模組

步驟1.在Configuration > ASA FirePOWER Configuration > Device Management處為外部介面分配 一個區域。在本例中,該區域稱為outside。

○ ○ ○ <u>Configuration > ASA FirePOWER Configuration > Device Management</u> > <u>Interfaces</u>										
firepower ASA5506W				You have unap	plied changes					
Device Interfaces										
Name 🔺		Security Zones								
firepower					Ø					
guest					Ø					
inside		inside			Ø					
nlp_int_tap					Ø					
Doutside	Edit Interface		? ×		Ø					
🛃 wifi		ASA			Ø					
	Security Zone: outside	Store ASA FirePOWER Changes	Cancel							

步驟2.在Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy中選擇 Add Rule。

步驟3.在Zones頁籤中,選擇outside區域作為規則的源和目標。

Add Rule		? ×
Name Remote VPN Policy	Enabled	Insert above rule
Action 🔀 Block	▼ V D 2 th I	
Zones Networks 🛆 Users Application:	Ports URLs SGT/ISE Attributes	Inspection Logging Comments
Available Zones 🕐	Source Zones (1)	Destination Zones (1)
Search by name	🧠 outside	📋 🥞 outside 📋
🥞 🔔 in		
🥞 inside		
🥞 🔔 out	Add to	
🍓 outside	Source	
	Add to Destination	
		Add Cancel

步驟4.選擇活動、標題和任何其他所需條件以定義此規則。

可以為此流量建立多個規則。請務必記住,源和目標區域必須是分配給VPN源和Internet的區域。

確保在這些規則之前,沒有其他可以匹配的更常規策略。最好將這些規則置於為任何區域定義的規 **則之**上。

步驟5.按一下儲存ASA FirePOWER更改,然後按一下部署FirePOWER更改以使這些更改生效。

由FMC配置管理的ASA FirePOWER模組

步驟1.在裝置處為外部介面分配一個區域 >管理>介面.在本例中,該區域稱為 outside-zone.

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

步驟2.在Policies > Access Control > Edit中選擇Add Rule。

步驟3.在Zones頁籤中,選擇outside-zone作為規則的源和目標。

Prefilter Policy: Default Prefilter Po										? ×					
Rul 命	es Security I	ntelligence	Name Action	VPN Traffic			 U D .2 d 	🗹 Enab	led	Insert	into Manda	tory			~
#	Name	Source Zones	Zone	Networks	VLAN Tags	🛆 Users	Applications	Ports	URLs	SGT/ISE Attribute	s		Inspection	Logging	Comments
- I	landatory - Fire	POWER Poli	Availab Sea	rch by name				source .	ide-zone)	i		de-zone		
There are no rules in this section. / Section in Default - FirePOWER Policy (n de											
Ther Defa	e are no rules in a ault Action	this section. /	🥞 inside-zone		Add to Source										
		Cut	👬 Outside 🧐 outside-zone		Add to Destination										
			🚠 Out	side_cbarrien											
	Add									Add	Cancel				

步驟4.選擇活動、標題和任何其他所需條件以定義此規則。

可以為此流量建立多個規則。請務必記住,源和目標區域必須是分配給VPN源和Internet的區域。

確保在這些規則之前,沒有其他可以匹配的更常規策略。最好將這些規則置於為任何區域定義的規 **則之**上。

步驟5.按一下Save,然後按一下Deploy,所做的變更就會生效。

結果

部署完成後,AnyConnect流量現在由應用的ACP規則進行過濾/檢查。在此示例中,成功阻止了 URL。

Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.