用Firepower服务访问控制规则配置ASA过滤 AnyConnect VPN客户端数据流到互联网

Contents

Introduction Prerequisites Requirements Components Used 问题 解决方案 ASA配置 ASDM配置管理的ASA Firepower模块 FMC配置管理的ASA Firepower模块 结果

Introduction

本文描述如何配置访问控制策略(ACP)规则检查来自虚拟专用网络(VPN)隧道或远程访问的数据流 (RA)用户并且以Firepower服务使用Cisco可适应的安全工具(ASA)作为互联网网关。

Prerequisites

Requirements

Cisco 建议您了解以下主题:

- AnyConnect、远程访问VPN和对等IPSec VPN。
- Firepower ACP配置。
- •ASA模块化政策架构(MPF)。

Components Used

本文档中的信息基于以下软件和硬件版本:

- ASA5506W版本9.6(2.7) ASDM示例
- Firepower模块版本6.1.0-330 ASDM示例。
- ASA5506W版本9.7(1) FMC示例。
- Firepower versoin 6.2.0 FMC示例。
- Firepower管理中心(FMC)版本6.2.0

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.



与Firepower服务的ASA5500-X无法过滤并且/或者检查AnyConnect用户数据流作为同其他位置发出 的数据流一样连接由使用单点permietral内容安全的IPSec隧道。

此解决方案包括没有其他来源做作的另一种症状是无法定义特定ACP规则到被提及的来源。

当Tunnelall设计使用在ASA时,终止的VPN解决方案此方案是非常普通发现。

解决方案

这可以通过多种方式达到。然而,此方案由区域包括检查。

ASA配置

步骤1.识别AnyConnect用户或VPN隧道连接到ASA的接口。

对等隧道

这是show run加密映射输出的报废。

crypto map outside_map interface **outside**

AnyConnect用户

show run命令WebVPN显示AnyConnect访问哪里是启用的。

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 在此方案中,接口外部接受,RA用户和对等隧道。

步骤2.重定向从ASA的数据流到有一个全局策略的Firepower模块。

它可能执行与**匹配所有**条件或被定义的访问控制表(ACL)数据流重定向的。

与**匹配的**示例**任何**匹配。

```
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
与ACL匹配的示例。
```

```
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
在一较少常见情况中,服务策略可以用于外部接口。此示例在本文没有报道。
```

ASDM配置管理的ASA Firepower模块

步骤1.分配外部接口一个区域在Configuration> ASA Firepower Configuration>设备管理。在这种情况下,该区域从外部被呼叫。

0 0 0 Configuration > ASA FirePOWER Configuration > Device Management > Interfaces										
firepower ASA5506W	You have unap	oplied 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									

步骤2.选择增加规则在Configuration> ASA Firepower Configuration>策略>访问控制策略。

第3步:从**区域请**选中,选择**外部**区域作为来源和目的地为您的规则。

Add Rule ?:										
Name Remote VPN Policy	🗸 Er	nabled Insert	above rule	▼ 1						
Action 🔀 Block	▼ ∪ D ,2 ± D									
Zones Networks 🔺 Users Application	6 Ports URLs S	GT/ISE Attributes		Inspection	Logging	Comments				
Available Zones 🖒	Source	ce Zones (1)	Destina	tion Zones (1)						
Search by name	ي 🚱	utside	🗒 🧠 outs	ide		i				
🥞 🔔 in										
🥞 inside										
Sout	Add to Source									
🥞 outside										
	Destination									
					Add	Cancel				

步骤4.选择动作、标题和所有其他期望情况定义此规则。

多个规则可以为此通信流被创建。记住是公正重要的来源和目的地区域必须是区域分配到VPN来源和互联网。

切记没有可能在这些规则前配比的其他一般政策。它是preferrable有在那个上的这些规则被定义对 **所有**区域。

步骤5.点击存储ASA Firepower更改然后配置Firepower更改安排这些更改生效。

FMC配置管理的ASA Firepower模块

步骤1.分配外部接口一个区域在设备> Management>接口。在这种情况下,该区域称为外部区域。

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

步骤2.选择增加规则在策略>访问控制> Edit。

第3步:从**区域请**选中,选择外部**区域**区域作为来源和目的地为您的规则。

Prefilter Policy: Default Prefilter Po										?	×					
Rul	es Security I	Intelligence	Action Allow		▼ □ 2 2 2 Enabled Inse		Insert	sert into Mandatory				~				
#	Name	Source Zones	Zone	Networks	VLAN Tags	🔺 Users	Applications	Ports	URLs	SGT/ISE Attributes	<u> </u>	Destinat	Inspection	Logging	Comments	
Their Their Defi	Aandatory - Fire e are no rules in Default - FirePO e are no rules in hult Action	POWER Poll this section. / WER Policy this section. /	Sea Sea Sea Sea Sea Sea Sea Sea Sea Sea	n de de-zone de_cbarrien side_cbarrien side_cone side_cbarrien			Add to Source Add to Destination	outs	ide-zone	,	8	Cestrial (ide-zone		ť	
														Add	Cancel	

步骤4.选择动作、标题和所有其他期望情况定义此规则。

多个规则可以为此通信流被创建。记住是公正重要的来源和目的地区域必须是区域分配到VPN来源和互联网。

切记没有可能在这些规则前配比的其他一般政策。它是preferrable有在那个上的这些规则被定义对 **所有**区域。

步骤5.点击"Save"然后配置安排这些更改生效。

结果

在配置完成后, AnyConnect数据流由被运用的ACP规则当前过滤/检查。 在本例中, URL顺利地 被阻拦了。

Access Denied

You are attempting to access a forbidden site.

Consult your system administrator for details.