配置从设备到安全管理器的同步

目录

<u>简介</u>
先决条件
<u>要求</u>
使用的组件
<u>背景信息</u>
<u>演示方法</u>
<u>单个设备发现</u>
<u>执行单设备发现的步骤:</u>
<u>执行单设备发现的步骤:</u>
<u>步骤 1:</u>
<u>步骤2:</u>
<u>批量设备发现</u>
<u>执行批量设备发现的步骤:</u>
<u>步骤 1:</u>
<u>步骤2:</u>
步骤3:

简介

本文档介绍从ASA到CSM的不同配置同步方式。

先决条件

要求

Cisco 建议您了解以下主题:

- Cisco Security Manager
- 自适应安全设备

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科安全管理器4.25
- 自适应安全设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

思科安全管理器为Cisco ASA设备提供集中管理和监控服务。

演示方法

本文档介绍将配置从ASA同步到CSM的两种不同方法或选项。

- 单个设备发现
- 批量设备重新发现

单个设备发现

仅当设备已添加到资产中时,才能执行单一发现。仅当设备具有

- 在多情景模式下运行的ASA、PIX和FWSM设备的安全情景配置。
- IPS设备的虚拟传感器配置。
- Catalyst设备的服务模块信息。

执行单设备发现的步骤:

当您已对设备CLI执行任何更改或者设备已移除并添加回时,可以执行设备发现。

要检查是否有任何待执行的更改尚未同步(请参阅前面提到的示例),请执行以下操作: 在设备窗格中右键单击相应的设备,然后选择检测带外更改选项。

File	Edit	View	Policy	Map	Manage	Tools	Tickets	Lau	inch	Help
🎒 De	evice	🔀 Мар	🖪 Pol	ay 🖾	Policy Bundle		<u>گە ئە</u>	3		
Devic	es								¢	ĝ
Filter	: [-	none			~					
P-4	🛿 Dep	artment								
6		Frewal	_						_	
		1877 🧰 1897 ASA	(evice P	roperties					
0- <u>/</u>	Loci	ation	(etect O	ut Of Band	Change	5			
÷-2	Al		1	/lake De	vice Operati	ional				
			(lone De	rvice				1	
			(opy Po	licies Betwee	en Devi	ces			
			s	hare De	vice Policies					
			(reate P	olicy Bundle					_
Polici	es		0	evice N	fanager					
⊖-Fi	rewall		0	rime Se	curity Mana	ger				
	-9	AAA Rule	1	ireSIGH	T Managem	ent Ce	nter			
	占	Access R Inspectio	F	review	Configuratio					
	-ğ	Botnet Tr	(elete D	evice(s)					
8	Sett	ings	F	acket T	racer					
	긤	Web Filte	F	acket C	apture					
⊕-N/	NT D		F	ing and	TraceRoute					
-2] Site	to Site VP		iscover	Policies on	Device	(s)		1	
⊕-Re	mote 7 tete	Access Vi	(etect A	SA-CX/FireP	OWER	Module			
-2	J VXL	anaces							_	

如果未发生更改(例如,更改未生效),则页面会显示为"未找到此设备的出站更改"。

🎨 008 Danyes		-	0	х
COE Detail COE Summary				
Devices Groups	CORDenals [Instance Summary]			
Abe:	No Out of Band changes found for this device			
8- Selected Deskes				
- Deprived				
-				
- Claster				
E 29 KM 1				

如果进行了任何更改(例如,更改了图例),则这些行会根据图例突出显示。

COB Changes			- 0 ×
ODE Detail ODE Summery			
Dervices Groups	Contenas (Industry Lanery)		
Meri - none - V	saturat Cardig Service in CSM	Running Carify Tensor from Denice	
P D Secol Jorisa P D Secol Jorisa	PM accesse-list int extended permit -1 any any	ACCOUNT AND A COUNTY	Added new
C C C C C C C C C C C C C C C C C C C	24 no logging hide username 32	to bogging hide unertaine	commands:
iii 📋 Agalaadan iii 🔲 🦲 Inda	20 20 jogging buffered informational	logging monitor informational logging boffword informational	
- 🖂 🕼 ADA 1	45 Logging som udvomstional 41 mmu utslik 1500	Logging seds unformational resu unacide 1500	
	47 Him Colscide 1900 43 Him mant 1900	ets opticide 1900 ets agen 1900	
	** Dot SetTowed	Den Gesterver	

执行单设备发现的步骤:

步骤 1 :

右键点击来自设备窗格的各个设备名称,然后选择选项Discover policies on Device(s)。



对于单设备恢复方法,只能看到Create Discovery Task对话框。如果您正在获取批量发现对话框 (请参阅本文档的"配置"),请关闭并再次打开它。

您有3个选项来执行发现。

- 实时设备 -从网络中的实时设备(本地或远程)获取配置。
- 配置文件-您可以选择配置文件并继续执行发现。
- 出厂默认配置 -将设备重置为默认配置。此方法可用于仅运行单情景模式的设备,或用于具有 单个安全情景的设备。

Create Discovery Task		×
Discovery Task Name:	discovery:2024-Jul-19 09:09:36	
	Live Device	
Discover From:	○ Config File	
	Factory Default Configuration	
	Config File: Browse	
	Discover Policies for Security Contexts	
Policies To Discover		
Select the policies to d	scover	
	POWER PODULE	
Platform Settings		
Firewall Services		
NAT Policies		
Routing Policies		
SSL Policy		
RA VPN Policies		
IPS		
	OK Cancel Help	

继续进行发现之前,请确保您了解网络拓扑和网络中可能发生的更改。

Warning) ×
	Discovery will replace existing policies with those discovered. Loss of sharing, inheritance will happen with all policies associated with the device Do you wish to continue?
	Do not show this again
	Yes No

发现完成后,您会看到状态为发现完成的弹出屏幕。

	80%		
Status: Devices to be discovered: Devices discovered successfully: Devices discovered with errors: Discovery Details	Discovery compi 1 1 0	eted with warrs	ngs
Type Name	Severity	State	Discovered From
ST ASA 1	0	Discovery Co	appleted with Warnings Live Device
Messages OLI not discovered		Severity	Description Palicy decovery does not support the following CLI in your configuration:
Policies discovered		0	Line Sono and history enable
Existing policy objects reused		0	Line 63:arp rate-limit 8:592
Policies discovered		0	Line 68 teneout pat-state 0:00:30
Policies discovered		0	Line 68:timeout pat-vlate 0:00:30 Line 73:timeout top-groxy-reassembly 0:01:00 Line 74:timeout floating-conn 0:00:00 Action If you wish to manage these commands in CS Manager, please use the "Plex Config" function

并且从带外更改中也不能有任何更改。

🆏 008 Danges		-	0	х
COEDetal COESummery				
Devices Groups	CROssis [Intuition Survey]			
4081 -1016 - V	No Out of Band changes found for this device			
8- Selected Deskas				
- Fred				
- I N 243				
- Costa				

批量设备发现

要发现多个设备的策略,可以执行批量重新发现。请务必注意,批量重新发现仅限于当前运行并在您的网络中可访问的设备。

您无法在安全情景(虚拟传感器)上执行批量发现。服务模块可单独选择进行发现。

执行批量设备发现的步骤:

步骤 1:

导航到设备上的策略>发现策略



步骤 2:

如果执行批量重新发现,则只能显示批量重新发现对话框。



步骤 3:

验证是否已列出所有选定的设备,并点击Finish以继续进行批量重新发现。 继续进行发现之前,请确保您了解网络拓扑和网络中可能发生的更改。



Warning	, ×
	Changes that you make to Remote Access VPN policies might not be deployed if you have not performed a prior deployment. Action: Please select File > Deploy immediately after discovery, before making any change to RA VPN policies. We recommend that you perform this initial deployment to a file rather than directly to the device. To change the deployment method, click the Edit Deploy Method button in the Deploy Saved Changes dialog box.
io or oc n	OK

两个设备都已成功发现。

	100%					
Status: Devices to be discovered: Devices discovered successfully: Devices discovered with errors:	Discovery compl 2 2 0	leted with v	ramings			
Tipe Name	Severity	State		Discovered From		
🔗 ASA 1	0	Discover	ry Completed with Warnings	Live Device		
		Discours	ry Completed with Warnings	Live Device		
₩ A5A 2	Ū					
V ASA 2		Seventy	Description	tion the formed on desire		
Nessages	wered.	Severity	Description No DAP sel configur	don file found on device.		
Mon 2 Messages Million figuration was not doco 30 will configuration was not doco	vered.	Severity 0	Description No CAP sel configur	don file found on device.	 	
Kon 2 K	vered.	Severity () ()	A Description	dion file found on device.		
AGA 2 AGA 2 Messages More and configuration was not doco SD xell configuration was not doco tostscan package file is not found o ncomplete Remote Access VPN Con	vered. n device or not figuration	Severity	A Description	dion file found on device.		
Messages Messages SD xml configuration was not doco tostocan package file is not found o recomplete Remote Access VPN Con 11 not docovered	rered. n device or not figuration	Severity () () () () () () () () () () () () ()	A Description	dion file found on device.		
Messages Messages SD xml configuration was not deco tostscan package file is not found o ncomplete Ramote Access VPN Con 11 not decovered skotes discovered	rened. In device or not figuration	Severity	A Description No DAP sel configur. Action	dion file found on device.		
ASA 2 Messages Mostage Konfiguration was not doco tostscan package file is not found o incomplete Remote Access Whi Con CLI not docovered biotes docovered biotes gooly objects reused	vered. n device or not Aguration	Severity 0 0 0 0 0 0 0 0 0 0 0 0 0	A Description No CAP sel configure	don file found on device.		

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。