Provisionar o Secure Firewall ASA para CSM

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Configurações
Configurar ASA para Gerenciamento HTTPS
Provisionar o Secure Firewall ASA para CSM
Verificar

Introdução

Este documento descreve o processo para provisionar o Secure Firewall Adaptive Security Appliance (ASA) para o Cisco Security Manager (CSM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ASA com firewall seguro
- CSM

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Secure Firewall ASA versão 9.18.3
- CSM versão 4.28

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O CSM ajuda a permitir a aplicação consistente de políticas e a rápida solução de problemas de

eventos de segurança, oferecendo relatórios resumidos em toda a implantação de segurança. Usando sua interface centralizada, as organizações podem escalar com eficiência e gerenciar uma ampla variedade de dispositivos de segurança da Cisco com visibilidade aprimorada.

Configurar

No próximo exemplo, um ASA virtual é provisionado para um CSM para gerenciamento centralizado.

Configurações

Configurar ASA para Gerenciamento HTTPS

Etapa 1. Crie um usuário com todos os privilégios.

Sintaxe da linha de comando (CLI):

```
configure terminal
username < user string > password < password > privilege < level number >
```

Isso se traduz no próximo exemplo de comando, que tem o usuário csm-user e a senha cisco123 da seguinte maneira:

ciscoasa# configure terminal ciscoasa(config)# username csm-user password cisco123 privilege 15



Dica: usuários autenticados externamente também são aceitos para essa integração.

Etapa 2. Habilite o servidor HTTP.

Sintaxe da linha de comando (CLI):

configure terminal http server enable

Etapa 3. Permitir acesso HTTPS para o endereço IP do servidor CSM.

Sintaxe da linha de comando (CLI):

configure terminal
http < hostname > < netmask > < interface name >

Isso se traduz no próximo exemplo de comando, que permite que qualquer rede acesse o ASA através de HTTPS na interface externa (GigabitEthernet0/0):

```
ciscoasa# configure terminal
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

Etapa 4. Valide se o HTTPS pode ser acessado do servidor CSM.

Abra qualquer navegador da Web e digite a próxima sintaxe:

```
https://< ASA IP address >/
```

Isso se traduz no próximo exemplo para o endereço IP da interface externa que foi permitido para acesso HTTPS na etapa anterior:

https://10.8.4.11/



404 Not Found

The requested URL /admin/public/index.html was not found on this server.

Resposta ASA HTTPS



Dica: o erro 404 não encontrado é esperado nesta etapa, pois este ASA não tem o Cisco Adaptive Security Device Manager (ASDM) instalado, mas a resposta HTTPS está lá quando a página redireciona para a URL /admin/public/index.html.

Provisionar o Secure Firewall ASA para CSM

Etapa 1. Abra e faça login no cliente CSM.

		8
Cisco Security Manager Version 4.28.0		
Server Name WIN-A7JU18QCA72 Username admin Password		
Default View Default View Login Help		
© 2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.	cisco	•

Logon do cliente CSM

Etapa 2. Abra o Gerenciador de configurações.

🝓 Cisco Security Manager - Dashboard - admin Connected to 'WIN-A'	7JU18QCA72'						- 0	×
File Launch Help								
				_		User: admin Server	r: WIN-A7JU	18QCA72
cisco Security Manager			Configuration Manager	Event Viewer	🐻 Health and Performance M	onitor 🍓 Image Manager	🔓 Repor	t Manager
Summary X Firewall IPS							🔀 Show V	Widgets 😮
Device Health Summary Last updated on Jan-30, 12:5	S PM PST Top	o Signatures	Last updated on Ja	n-30, 12:46 PM PST	Top Malware Sites	Last updated on	Jan-30, 12	:46 PM PST
Group by Category - Q Type to Search	🖲 🖻 Sign	natures		Last 24 Hours 👻	IP Address		Last 24	Hours +
Na Device Not Reachable	0							
🐺 Interface Down	0							
😡 Overall Device Health Alerts	0	No	o data available		No	o data available		
🕮 High Memory Utilization	0							
Sirewall - High CPU Utilization	0							
🎢 IPS - High Inspection Load	0							
🎳 IPS - High Missed Packets	ОТор	Attackers	Last updated on Ja	n-30, 12:46 PM PST	Top Sources	Last updated on	Jan-30, 12	:46 PM PST
🁔 IPS - Bypass Mode	0 Atta	ackers		Last 24 Hours •	Sources		Last 24	Hours +
The contract of the contract o	0							
		No	o data available		No	o data available		
		10-11		- 20 10.40 04 007	Teo Destinations		1 20 10	40 044 007
Deployment Last updated on Jan-30, 01:00	UPMPST Top	time	Last updated on Ja	1 act 24 Hours	Postinations	Last updated on	Jan-30, 12:	Hours -
Type to Search	Vicu	ums		Last 24 Hours +	Desunations		Last 24	mours +
		No	o data available		No	o data available		
			o data avanabro		110			
······								

Etapa 3. Navegue até Devices > New Device.

٩	Cisco Security Manager - Configuratio	n Manager - admin Connected to 'WIN-A7JU180	QCA72'				-	o ×
File	Edit View Policy Map Mana	age Tools Tickets Launch Help					No Open Tickets	ahaha
	New Device Ctrl+N	rde 🗿 🐎 🗉 🗟 🕲 👍 🛍 📫 🛙		i 🔟 🧏 🖪 🔍 🛙	19 🛅 🐴 🏪 🍓 🐻 🕗 👘		Q Search All Categories	cisco.
	Clone Device					Device State		1
	Delete Device(s)	saith and Performance Monitor		Deployment Manager	0	Device State		_
	Save Ctrl+S	Critical: 0 Varning: 0 Normal: 0		e Fait 0 Pending: 0	e Pass: 0	Critical 0 0 Wa	arning: 0 🕒 Normai: 0	
	Import		3			Las	t Update Time: 30 Jan 2024 12:46	PM PST
	Darlas	Filter: (none)					Q.+ Type to Search	
	Deploy	Display Name Managed M	Monitored Alerts	s Connection State	Deployment Additional Information	IP Address	Host.Domain	Targ
	New Device Group Add Devices to Group							
	Print Ctrl+P	·						
	Exit Ctrl+Q	-						
Pol	icies							
	< C							>

Gerenciador de configuração do CSM

Etapa 4. Selecione a opção de adição que preenche o requisito de acordo com o resultado desejado. Como o ASA configurado já está configurado na rede, a melhor opção para este exemplo é **Add Device From Network** e clique em **Next**.

Please choose how you would like to add the device:



Método de Adição de Dispositivo

Etapa 5. Preencha os dados necessários de acordo com a configuração no Secure Firewall ASA e com as configurações de detecção. Em seguida, clique em Next.

Wew Device - Device Information (Step 2 of 4)

Identity				
IP Type;	Static 🗸			
Host Name:	ciscoasa			
Domain Name:				
IP Address:	10.8.4.11			
Display Name:*	ciscoasa			
OS Type:*	ASA 🗸 😵			
Transport Protocol:	HTTPS 🗸			
	System Context			
Discover Device Setting	s			
Perform Device Dis	covery			
Discover:	Policies and Inventory ~			
	Platform Settings			
	Firewall Policies			
	NAT Policies			
	IPS Policies			
	RA VPN Policies			
	Discover Policies for Security Contexts			

Etapa 6. Preencha as credenciais necessárias do usuário CSM configurado no ASA e da senha de ativação.

Configurações do ASA

Wew Device - Device Credentials (Step 3 of 4)

	csm-user				
Password:*	•••••	Confirm:*	•••••		
Enable Password:	•••••	Confirm:*	•••••		
TTP Credentials					
	Use Primary Credentials	s			
	Username;				
	Password:				
	Confirm:				
HTTP Ports	90				
	442		44		
HITPS Port:	443		JIT		
IPS RDEP Mode:	Use Default (HTTPS)	~			
Certificate Common Name:		Confirm:			
RX-Boot Mode S	NMP				
RX-Boot Mode S	NMP				
RX-Boot Mode Si	NMP				
RX-Boot Mode S	NMP				
RX-Boot Mode S	NMP				
RX-Boot Mode S	NMP				
RX-Boot Mode S	NMP				
RX-Boot Mode S	NMP				
RX-Boot Mode S	NMP				

Credenciais do ASA

Passo 7. Selecione os grupos desejados ou ignore esta etapa se nenhum grupo for necessário e clique em Finish.

Wew Device - Device Grouping (Step 4 of 4)

Select the groups that this d	evice belongs to:					
Department:	None	×				
Location:	None	<u>~</u>				
test:	None	M				
Set Values as Default						
		Back	Next	Finish	Cancel	Help

Seleção de grupo CSM

Etapa 8. Uma solicitação de tíquete é gerada para fins de controle, clique em OK.

Wew Device - Device Grouping (Step 4 of 4)

ect the groups that this devi Department:	None	
Location:	None	
test:	None	
LESU.	NOTICE IN THE	
Set Values as Default		
	Ticket Required	×
	You must have an editable ticket opened in order to perform this	action. You may:
	Create a new ticket:	
	admin_30.3an.2024_13.20.25	
	Description:	
	OK Cancel	Help
		- nep
	Back	Nevt Finish Cancel Help
	back	The Third Concerning

Criação de tíquete CSM

Etapa 9. Valide se a descoberta termina sem erros e clique em Fechar.

Discovery Status

	100%					
Status: Devices to be discovered: Devices discovered successfully:	Discovery comp 1 1	leted with warr	nings			
Devices discovered with errors:	0					
Discovery Details						
Type Name	Severity	State		Discovered From		
😽 ciscoasa	0	Discovery C	Completed with Warnings	Live Device		
•						
			Description			
Messages LI not discovered		Severity	Description Policy discovery does r	not support the following C	CLI in your configuratio	n: ,
Messages LI not discovered olicies discovered		Severity	Description Policy discovery does r Line 5:service-module (Line 6:service-module (not support the following C 0 keepalive-timeout 4 0 keepalive-counter 6	CLI in your configuratio	n: ,
Messages CLI not discovered Policies discovered Existing policy objects reused		Severity () () ()	Description Policy discovery does n Line 5:service-module (Line 6:service-module (Line 8:license smart Line 12:no mac-addres	not support the following C 0 keepalive-timeout 4 0 keepalive-counter 6 15 auto	CLI in your configuratio	n: /
Messages CLI not discovered Volicies discovered Existing policy objects reused Value overrides created for device		Severity	Description Policy discovery does n Line 5:service-module (Line 6:service-module (Line 8:license smart Line 12:no mac-address Line 50:no failover wai	not support the following C 0 keepalive-timeout 4 0 keepalive-counter 6 is auto t-disable	LI in your configuratio	n: /
Messages CLI not discovered olicies discovered ixisting policy objects reused alue overrides created for device olicies discovered		Severity	Description Policy discovery does n Line 5:service-module (Line 6:service-module (Line 8:license smart Line 12:no mac-address Line 50:no failover wai Line 55:no asdm histor Line 57:no arp permit-r	not support the following C 0 keepalive-timeout 4 0 keepalive-counter 6 is auto t-disable y enable nonconnected	CLI in your configuratio)n: (
Messages LL not discovered olicies discovered ixisting policy objects reused alue overrides created for device olicies discovered dd Device Successful		Severity () () () () () () () () () ()	Description Policy discovery does n Line 5:service-module (Line 6:service-module (Line 8:license smart Line 12:no mac-addres Line 50:no failover wai Line 55:no asdm histor Line 57:no arp permit-n Action If you wish to manage	not support the following C 0 keepalive-timeout 4 0 keepalive-counter 6 is auto t-disable y enable nonconnected these commands in CS Ma	LI in your configuratio	n: "Flex Config" function

Descoberta do ASA



Dica: os avisos são aceitos como uma saída bem-sucedida, pois nem todas as funcionalidades do ASA são suportadas pelo CSM.

Etapa 10. Valide se o ASA agora aparece como registrado no cliente CSM e exibe as informações corretas.

Cisco Security Manager - Configu	ration Manager - admin Co	nnected to	WIN-A7JU18Q0	CA72' - Ticke	t: admin_30.	Jan.2024_13.20	.26						- C	
File Edit View Policy Map	Manage Tools Tickets	Launch	Help								a	dmin_30.Jan.2024	E 🤵	ababa
Service 🔀 Map 🗊 Policy 🖾 Pol	icy Bundle 🙆 🐉 🛐 🛛	5 🗊 🛙	۵ 🖆 🗋 🕯	. <table-cell> ⊳ I</table-cell>	à 🛛 🖉 🦂	Ł 🖪 🝕	🗊 🖥 🖗	🖣 🍓 🕷	0		0	Search All Categorie	s	cisco
Devices 🔶 😭	Device: ciscoasa Policy Assigned: local						Poli Ass	icy: Interface signed To: loca	s Il device					
Filter : none V	Interfaces Bridge Gri	oups												
Department Location	Interface ^{^ 1} Name	Status	Security L	IP Address	VLAN ID	Secondar	Туре	Interface	Member of	MTU	Route Map	Path Moni Policy	Ro D	escription
- ja test	GigabitEthe outside	Enabled	0	10.8			Physical Int	. All-Interfac		1500				
🖻 – 🎒 All	GigabitEthe	Disabled					Physical Int							
- Se ciscoasa	GigabitEthe	Disabled					Physical Int							
	Managemenmanagement	Enabled	0				Physical Int	All-Interfaces		1500				
Policies Frewal Frewal Bracess Rules (Unified) Bracess Rules (Unified) Bracess Rules (Unified) Bracess Rules (Unified) Bracess Rules Web Filter Rules NAT Site to Site VPN Remote Access VPN Filter Rules VALan Identity Options FrustSec Plaform FlexConfigs	Advanced												•	
														Save

Informações do ASA registradas

Verificar

Uma depuração HTTPS está disponível no ASA para fins de solução de problemas. O próximo comando é usado:

debug http

Este é um exemplo de uma depuração de registro de CSM bem-sucedida:

ciscoasa# debug http debug http enabled at level 1. ciscoasa# HTTP: processing handoff to legacy admin

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.