Bereitstellung einer sicheren Firewall-ASA für CSM

Inhalt
Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Konfigurationen
ASA für HTTPS-Management konfigurieren
Bereitstellung einer sicheren Firewall-ASA für CSM
Überprüfung

Einleitung

In diesem Dokument wird der Prozess zur Bereitstellung der Secure Firewall Adaptive Security Appliance (ASA) für den Cisco Security Manager (CSM) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sichere Firewall ASA
- CSM

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Secure Firewall ASA Version 9.18.3
- CSM Version 4.28

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

CSM unterstützt die konsistente Durchsetzung von Richtlinien und die schnelle Behebung von Sicherheitsereignissen und bietet für die gesamte Sicherheitsinfrastruktur zusammengefasste Berichte. Die zentrale Benutzeroberfläche ermöglicht eine effiziente Skalierung und Verwaltung einer Vielzahl von Cisco Sicherheitsgeräten bei erhöhter Transparenz.

Konfigurieren

Im nächsten Beispiel wird eine virtuelle ASA für ein zentrales Management auf einem CSM bereitgestellt.

Konfigurationen

ASA für HTTPS-Management konfigurieren

Schritt 1: Erstellen Sie einen Benutzer mit allen Berechtigungen.

Befehlszeilen-Syntax (CLI):

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

Dies wird in das nächste Befehlsbeispiel übersetzt, das den Benutzer csm-user und das Kennwort cisco123 wie folgt enthält:

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



Tipp: Auch extern authentifizierte Benutzer werden für diese Integration akzeptiert.

Schritt 2: HTTP-Server aktivieren.

Befehlszeilen-Syntax (CLI):

configure terminal http server enable

Schritt 3: HTTPS-Zugriff für die IP-Adresse des CSM-Servers zulassen.

Befehlszeilen-Syntax (CLI):

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

Dies wird in das nächste Befehlsbeispiel übersetzt, das jedem Netzwerk den Zugriff auf die ASA über HTTPS an der externen Schnittstelle (GigabitEthernet0/0) ermöglicht:

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

Schritt 4: Überprüfen Sie, ob HTTPS vom CSM-Server aus erreichbar ist.

Öffnen Sie einen beliebigen Webbrowser, und geben Sie die nächste Syntax ein:

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

Dies wird in das nächste Beispiel für die externe Schnittstellen-IP-Adresse übersetzt, die im vorherigen Schritt für den HTTPS-Zugriff zugelassen wurde:

```
https://10.8.4.11/
```



404 Not Found

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

ASA HTTPS-Antwort



Tipp: Fehler 404 Not Found (Nicht gefunden) wird für diesen Schritt erwartet, da auf dieser ASA der Cisco Adaptive Security Device Manager (ASDM) nicht installiert ist. Die HTTPS-Antwort wird jedoch angezeigt, wenn die Seite zu URL /admin/public/index.html umgeleitet wird.

Bereitstellung einer sicheren Firewall-ASA für CSM

Schritt 1: Öffnen und beim CSM-Client anmelden

		e.
Cisco Security Manager Version 4.28.0		
Server Name WIN-A7JU18QCA72		
Password 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	

Anmeldung beim CSM-Client

Schritt 2: Öffnen Sie den Configuration Manager.

Cisco Security Manager - Dashboard - admin Connected to 'WIN-A7.	JU18QCA7	2'			- 🗆 X
File Launch Help					
Cisco Security Manager					User: admin Server: WIN-A7JU18QCA72
cisco			🛛 🎱 Configuration Manager 🖉 Event Viewer	🛛 🍯 Health and Performa	ince Monitor 🍓 Image Manager 嶺 Report Manager
Summary × Firewall IPS					🔜 🧱 Show Widgets 🔮
Device Health Summary Last updated on Jan-30, 12:55	PM PST	Top Signatures	Last updated on Jan-30, 12:46 PM PST	Top Malware Sites	Last updated on Jan-30, 12:46 PM PST
Group by Category		Signatures	Last 24 Hours 👻	IP Address	Last 24 Hours 👻
Na Device Not Reachable	0				
🐺 Interface Down	0				
😡 Overall Device Health Alerts	0		No data available		No data available
🕮 High Memory Utilization	0				
🛐 Firewall - High CPU Utilization	0				
🎢 IPS - High Inspection Load	0				
🎢 IPS - High Missed Packets	0	Top Attackers	Last updated on Jan-30, 12:46 PM PST	Top Sources	Last updated on Jan-30, 12:46 PM PST
🎉 IPS - Bypass Mode	0	Attackers	Last 24 Hours 🔹	Sources	Last 24 Hours 👻
The Alerts	0				
			No data available		No data available
	1				
Deployment Last updated on Jan-30, 01:00	PMPST	Top Victims	Last updated on Jan-30, 12:46 PM PST	Top Destinations	Last updated on Jan-30, 12:46 PM PST
Q Type to Search		Victims	Last 24 Hours 👻	Destinations	Last 24 Hours 👻
- The to office 1				-	
	- 11				
			No data available		No data available
	- 11				

Schritt 3: Navigieren Sie zu Geräte > Neues Gerät.

6	Cisco Security Manager - Configuration	n Manager - admin Connected to "	WIN-A7JU18QCA72'							_		×
Fi	le Edit View Policy Map Manag	ge Tools Tickets Launch H	elp							No Open Tickets		
Г	New Device Ctrl+N	de 🙆 🎥 🗟 🕲 🔒		D- R	1 🗖 🧩 🖪	- C	1 G (A) (🗟 🐱 🖀 👩		Q Search All Categories	CISC	0.
	Clone Device										_	
	Delete Device(s)	alth and Performance Monitor			Deployment Ma	anager			Device State			
	Save Ctrl+S	🕽 Critical: 0 🛛 🖯 Warning: 0 🖯 Norn	mal: 0		😝 Fail: 0 🛛 P	ending: 0	O Pass: 0		😝 Critical: 0 🔍 V	Varning: 0 😑 Normal: 0		
	Import Export		/ 🗈 🖈 😮					^	La	ast Update Time: 30 Jan 2024 12:4	6 PM PST	٦
	Deploy	Filter: (none)								Q. Type to Search		
Po	Edit Device Groups New Device Group Add Devices to Group Print Ctrl+P Exit Ctrl+Q	Jisplay Name	Managed Monitore	d Alerts	s Connection	State	Deployment	Additional Information	IP Address	Host.Domain		Targ
	• • no device selected •											>
	C											

CSM-Konfigurationsmanager

Schritt 4: Wählen Sie die Hinzufügungsoption aus, die die Anforderung gemäß dem gewünschten Ergebnis erfüllt. Da die konfigurierte ASA bereits im Netzwerk eingerichtet ist, ist die beste Option für dieses Beispiel "Gerät vom Netzwerk hinzufügen" und klicken auf "Weiter".

Please choose how you would like to add the device:



Methode zum Hinzufügen von Geräten

Schritt 5: Füllen Sie die erforderlichen Daten entsprechend der Konfiguration auf der Secure Firewall ASA und den Erkennungseinstellungen aus. Klicken Sie dann auf **Weiter**.

Wew Device - Device Information (Step 2 of 4)

IP Type: Static Host Name: discoasa Domain Name:	Identity						
Host Name: ciscoasa Domain Name:	IP Type;	Static 🗸					
Domain Name: IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Host Name:	ciscoasa					
IP Address: 10.8.4.11 Display Name:* ciscoasa OS Type:* ASA ASA > Transport Protocol: HTTPS System Context Discover Device Settings Pelidies and Inventory Discover: Policies Pirewall Policies IPS Policies for Security Contexts	Domain Name:						
Display Name:* discoasa OS Type:* ASA Transport Protocol: HTTPS Discover Device Settings Perform Device Discovery Discover: Policies and Inventory Platform Settings Firewall Policies Discover Policies Discover Policies Discover Policies Discover Policies Discover Policies for Security Contexts	IP Address:	10.8.4.11					
OS Type:* ASA Transport Protocol: HTTPS Discover Device Settings Perform Device Discovery Discover : Policies and Inventory Q Platform Settings G Firewall Policies I TS Policies I TS Policies Discover Policies for Security Contexts	Display Name:*	ciscoasa					
Transport Protocol: HTTPS System Context Discover Device Settings Perform Device Discovery Discover: Policies and Inventory O' Platform Settings Firewall Policies NAT Policies IPS Policies RA VPN Policies Discover Policies for Security Contexts	OS Type:*	ASA 🗸 😣					
□ System Context Discover Device Settings ○ Perform Device Discovery Discover: Policies and Inventory ○ Platform Settings ○ Firewall Policies ○ NAT Policies □ IPS Policies □ IPS Policies □ Discover Policies for Security Contexts	Transport Protocol:	HTTPS 🗸					
Discover Device Settings Perform Device Discovery Discover: Policies and Inventory v Platform Settings Platform Settings Platform Settings NAT Policies IPS Policies RA VPN Policies Discover Policies for Security Contexts		System Context					
Discover Device Settings Perform Device Discovery Discover: Policies and Inventory Platform Settings Firewall Policies NAT Policies IPS Policies RA VPN Policies Discover Policies for Security Contexts							
Perform Device Discovery Discover: Policies and Inventory Platform Settings Platform Settings Firewall Policies NAT Policies IPS Policies RA VPN Policies Discover Policies for Security Contexts	Discover Device Setting	5					
Discover: Policies and Inventory V Platform Settings Platform Settings Platform Settings NAT Policies IPS Policies RA VPN Policies Discover Policies for Security Contexts	Perform Device Dis	covery					
 Platform Settings Firewall Policies NAT Policies IPS Policies RA VPN Policies Discover Policies for Security Contexts 	Discover:	Policies and Inventory ~					
 ✓ Firewall Policies ✓ NAT Policies IPS Policies RA VPN Policies Discover Policies for Security Contexts 		Platform Settings					
 ✓ NAT Policies ☐ IPS Policies ☐ RA VPN Policies ☐ Discover Policies for Security Contexts 		Firewall Policies					
 IPS Policies RA VPN Policies Discover Policies for Security Contexts 		NAT Policies					
RA VPN Policies Discover Policies for Security Contexts		IPS Policies					
Discover Policies for Security Contexts		RA VPN Policies					
		Discover Policies for Security Contexts					
					_		
			Back	Next	Finish	Cancel	Help

ASA-Einstellungen

Schritt 6: Geben Sie die erforderlichen Anmeldeinformationen des konfigurierten CSM-Benutzers auf der ASA und des **aktivierten** Kennworts ein.

Wew Device - Device Credentials (Step 3 of 4)

osernamer	csm-user				
Password:*	•••••	Confirm:*	•••••		
Enable Password:	•••••	Confirm:*	•••••		
ITP Credentials					
	Use Primary Credentials				
	Username:				
	Password:				
	Confirm:				
ITTP Port:	80				
ITTPS Port:	443	🗸 Use Defa	ult		
PS RDEP Mode:	Use Default (HTTPS) 🛛 🧹				
Certificate Common Name:		Confirm:			
RX-Boot Mode S	NMP				

ASA-Anmeldedaten

Schritt 7. Wählen Sie die gewünschten Gruppen aus oder überspringen Sie diesen Schritt, falls keine erforderlich ist, und klicken Sie auf **Fertig** stellen.

Wew Device - Device Grouping (Step 4 of 4)

Sele	ect the groups that this device be	elongs to:					
I	Department:	None	×				
I	Location:	None	×				
	test:	None	1				
ļ	Set Values as Default						
			Back	Next	Finish	Cancel	Help

 $CSM ext{-}Gruppenauswahl$

Schritt 8: Eine Ticketanfrage wird zu Kontrollzwecken generiert, klicken Sie auf OK.

Wew Device - Device Grouping (Step 4 of 4)

Department:	None	<u>~</u>			
Location:	None				
test:	None				
Set Values as Default					
	Ticket Require	d		×	
	You must have Create a new	an editable ticket opened in order to perfo ticket:	rm this action. You may:		
	Ticket:	admin_30.Jan.2024_13.20.26			
	Description:				
			ancel Heln		
			nep		

Erstellung von CSM-Tickets

Schritt 9. Überprüfen Sie, ob die Erkennung fehlerfrei abgeschlossen wurde, und klicken Sie auf Schließen.

Discovery Status

Status:	Discove	ery complet	ted with war	nings				
Devices to be discovered:	1							
Devices discovered successfully:	1							
Devices discovered with errors:	0							
)iscovery Details								
Type Name	Se	everity	State		Discovered From			
😽 ciscoasa		1	Discovery C	Completed with Warnings	Live Device			
•				Description				
• •				1				
Messages			Severity	Description Policy discovery does r	not support the following	CLI in your con	figuration:	
Messages CLI not discovered			Severity	Description Policy discovery does r	not support the following	CLI in your con	figuration:	
Messages CLI not discovered Policies discovered			Severity	Description Policy discovery does r Line 5:service-module Line 6:service-module	not support the following 0 keepalive-timeout 4 0 keepalive-counter 6	CLI in your con	ifiguration:	
Messages CLI not discovered Policies discovered Existing policy objects reused			Severity	Description Policy discovery does r Line 5:service-module Line 6:service-module Line 8:license smart	not support the following 0 keepalive-timeout 4 0 keepalive-counter 6	CLI in your con	ifiguration:	
Messages CLI not discovered Policies discovered Existing policy objects reused Value overrides created for device			Severity Severity	Description Policy discovery does r Line 5:service-module Line 6:service-module Line 8:license smart Line 12:no mac-addres Line 50:no failover wai	not support the following 0 keepalive-timeout 4 0 keepalive-counter 6 is auto t-disable	CLI in your con	ifiguration:	
Messages CLI not discovered Policies discovered Existing policy objects reused Value overrides created for device Policies discovered			Severity (1) (1) (1) (1) (1) (1) (1) (1)	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	not support the following 0 keepalive-timeout 4 0 keepalive-counter 6 is auto t-disable y enable	CLI in your con	ifiguration:	
Messages CLI not discovered Policies discovered Existing policy objects reused Value overrides created for device Policies discovered Policies Successful			Severity	Description Policy discovery does r 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-r Action	not support the following 0 keepalive-timeout 4 0 keepalive-counter 6 is auto t-disable y enable nonconnected	CLI in your con	ifiguration:	
Messages CLI not discovered Policies discovered Existing policy objects reused Value overrides created for device Volicies discovered Volicies discovered Volicies Successful			Severity Severity	Description Policy discovery does r Line 5:service-module I Line 6:service-module I 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 Action If you wish to manage	not support the following 0 keepalive-timeout 4 0 keepalive-counter 6 is auto t-disable y enable nonconnected these commands in CS N	CLI in your con	ifiguration: use the "Flex Cor	nfig" function

ASA-Erkennung



Tipp: Warnungen werden als erfolgreiche Ausgabe akzeptiert, da nicht alle ASA-Funktionen von CSM unterstützt werden.

Schritt 10. Überprüfen Sie, ob die ASA jetzt als auf dem CSM-Client registriert angezeigt wird, und zeigen Sie die richtigen Informationen an.

Cisco Security Manager - Configu	uration Manager - admin Co	nnected to	WIN-A7JU18Q0	A72' - Ticke	t: admin_30.	Jan.2024_13.20	.26						_	
File Edit View Policy Map	Manage Tools Tickets	Launch H	Help								a	dmin_30.Jan.2024_	🗄 🤵	
Sevice Map Sevice Policy Policy	icy Bundle 🙆 🐉 🧾	S 🗊 G	à 🙆 📑 G	🛯 🔓 🕞 I	là 🗖 🧍	Ł 🖪 🝕	🗊 🖷 🖲	🙀 🍓 🕷	0		(Search All Categ	ories	cisco
Devices 🔶 😭	Device: ciscoasa Policy Assigned: local						Poli Ass	cy: Interface igned To: loca	s I device					
Filter : none v	Interfaces Bridge Gri	oups												
Department	Interface^ 1 Name	Status	Security L	IP Address	VLAN ID	Secondar	Туре	Interface	Member of	MTU	Route Map	Path Moni Pol	icy Ro	Description
a test	GigabitEthe outside	Enabled	0	10.8			Physical Int	All-Interfac		1500				
🖻 – 🎒 All	GigabitEthe	Disabled					Physical Int							
- 😭 discoasa	GigabitEthe	Disabled					Physical Int							
	Managemenmanagement	Enabled	0				Physical Int	All-Interfaces		1500				
Policies														
C Devel														
AAA Rules (Unified)														
- Access Rules (Unified)														
- Inspection Rules (Unified)														
Botnet Traffic Filter Rules														
- C Transparent Rules														
Web Filter Rules														
⊕-NAT														
Site to Site VPN														
Remote Access VPN														
Identity Options														
⊕-TrustSec														
Platform ElevConfigs														
) nexcomigs														
													4	
	Advanced													
														Save

Registrierte ASA-Informationen

Überprüfung

Zur Fehlerbehebung steht auf ASA ein HTTPS-Debugging zur Verfügung. Der nächste Befehl wird verwendet:

debug http

Dies ist ein Beispiel für ein erfolgreiches CSM-Registrierungsdebug:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.