ASA 8.3: TACACS-Authentifizierung mit ACS 5.X

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Netzwerkdiagramm Konfigurieren der ASA für die Authentifizierung vom ACS-Server mithilfe der CLI Konfigurieren der ASA für die Authentifizierung vom ACS-Server mithilfe von ASDM Konfigurieren von ACS als TACACS-Server Überprüfen Fehlerbehebung Fehler: AAA-Markierung von TACACS+-Server x.x.x.x in AAA-Servergruppen-Taktiken als FEHLGESCHLAGEN Zugehörige Informationen

Einführung

Dieses Dokument enthält Informationen zur Konfiguration der Sicherheits-Appliance zur Authentifizierung von Benutzern für den Netzwerkzugriff.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die Adaptive Security Appliance (ASA) voll funktionsfähig und so konfiguriert ist, dass der Cisco Adaptive Security Device Manager (ASDM) oder die CLI Konfigurationsänderungen vornehmen kann.

Hinweis: Weitere Informationen zur Remote-Konfiguration des Geräts durch den ASDM finden Sie unter <u>Zulassen von HTTPS-Zugriff für ASDM</u>.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance Software Version 8.3 oder höher
- Cisco Adaptive Security Device Manager Version 6.3 und höher

Cisco Secure Access Control Server 5.x

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurieren der ASA für die Authentifizierung vom ACS-Server mithilfe der CLI

Führen Sie folgende Konfigurationen durch, damit die ASA vom ACS-Server authentifiziert werden kann:

!--- configuring the ASA for TACACS server ASA(config)# <u>aaa-server cisco protocol tacacs+</u> ASA(config-aaa-server-group)# exit !--- Define the host and the interface the ACS server is on. ASA(config)# aaa-server cisco (DMZ) host 192.168.165.29 ASA(config-aaa-server-host)# key cisco !--- Configuring the ASA for HTTP and SSH access using ACS and fallback method as LOCAL authentication. ASA(config)#<u>aaa authentication ssh console cisco LOCAL</u> ASA(config)#aaa authentication http console cisco LOCAL

Hinweis: Erstellen Sie einen lokalen Benutzer auf der ASA mit dem Befehl <u>username cisco</u> <u>password cisco privilege 15</u>, um auf das ASDM mit lokaler Authentifizierung zuzugreifen, wenn der ACS nicht verfügbar ist.

Konfigurieren der ASA für die Authentifizierung vom ACS-Server mithilfe von ASDM

ASDM-Verfahren

Gehen Sie wie folgt vor, um die ASA für die Authentifizierung vom ACS-Server zu konfigurieren:

1. Wählen Sie Configuration > Device Management > Users/AAA > AAA Server Groups > Add aus, um eine AAA-Servergruppe zu

nfiguration > Devi	ce Management	> Users/AAA > AAA 5	erver Groups			
A Server Groups —						
Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add Edk Delete
rvers in the Selected	Group					
Server Name or IP	Address		Interface		Timeout	Add
						Edit

2. Geben Sie die AAA-Servergruppen-Details im Fenster AAA-Servergruppe hinzufügen wie gezeigt ein. Das verwendete Protokoll ist TACACS+, und die erstellte Servergruppe ist

erver Group:	cisco		
rotocol:	TACACS+	*	
accounting Mode:	🚫 Simultaneous	💿 Single	
Reactivation Mode:	 Depletion 	🔿 Timed	
Dead Time: 10	minut	es	
Max Failed Attempts:	3		

3. Wählen Sie **Configuration > Device Management > Users/AAA > AAA Server Groups** aus, und klicken Sie unter **Servers in der ausgewählten Gruppe** auf **Add**, um den AAA-Server hinzuzufügen.

OK.

figuration > Devi	ice Management	:>Users/AAA > AAA S	erver Groups			
A Server Groups						
Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add
isco	TACAC5+	Single	Depletion	10	3	Edit Deleb
vers in the Selected Server Name or IP (Group		Interface		Timeout	Add
						Edit
						Delete

4. Geben Sie die AAA-Serverdetails im Fenster AAA-Server hinzufügen wie gezeigt ein. Die verwendete Servergruppe ist

Server Group:	cisco	
Interface Name:	dmz	*
Server Name or IP Address:	192.168.165.29	
Timeout:	10	second
Server Port: 49 Server Secret Key: ••••	•	
SDI Messages		
Message Table		۲

en Sie auf **OK** und dann auf **Übernehmen**.Sie sehen die **AAA-Servergruppe** und den auf der ASA konfigurierten **AAA-Server**.

5. Klicken Sie auf Übernehmen.

Co	nfiguration > Device	Management	> Users/AAA > AAA S	ierver Groups		
A	AA Server Groups					
	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
	cisco	TACACS+	Single	Depletion	10	3
54	ervers in the Selected Gr	roup				
	Server Name or IP Ad	bhace		Interface		Timerat
	192,168,165,29	Juress		direct		Thiotoc
L	1 JEILOOILOOILO			unz		
	LDAP Attribute Ma	p				
					Apply Re:	set

6. Wählen Sie Configuration > Device Management > Users/AAA > AAA Access > Authentication aus, und aktivieren Sie die Kontrollkästchen neben HTTP/ASDM und SSH. Wählen Sie dann cisco als Servergruppe aus, und klicken Sie auf Apply.

Configuration > Device Management > Users/AAA > AAA Access > Authentication
Authentication Accounting
Enable authentication for administrator access to the ASA.
Require authentication to allow use of privileged mode commands
Enable Server Group: LOCAL 🕑 🗌 Use LOCAL when server group fails
Require authentication for the following types of connections
FTTP/ASDM Server Group: cisco 💟 🔽 Use LOCAL when server group fails
Serial Server Group: LOCAL Server Group LOCAL LOCAL when server group fails
SSH Server Group: cisco V Use LOCAL when server group fails
Telnet Server Group: tac Use LOCAL when server group fails
Apply Reset

Konfigurieren von ACS als TACACS-Server

Führen Sie dieses Verfahren aus, um den ACS als TACACS-Server zu konfigurieren:

 Wählen Sie Network Resources > Network Devices and AAA Clients (Netzwerkressourcen > Netzwerkgeräte und AAA-Clients) aus, und klicken Sie auf Create (Erstellen), um die ASA zum ACS-Server hinzuzufügen.

cisco Cisco Secure Ad	cs
▶ 💮 My Workspace	Network Resources > Network Devices and AAA Clients
In Network Resources Network Device Groups Location	Network Devices
Device Type Network Devices and AAA Clients Default Network Device External PADIUS Servers	Name IP / Mask NDO:Location NDO:Device Type Description No data to display No data to display No No
External PADIUS Servers	
	Create Duplicate Edit Delete File Operations Export

2. Geben Sie die erforderlichen Informationen zum **Client** (hier ist ASA der Client) an, und klicken Sie auf **Senden**. Dadurch kann die ASA zum ACS-Server hinzugefügt werden. Die Details umfassen die **IP-Adresse** der ASA und die Details des **TACACS-**

Servers.

cisco Cisco Secure Ad	cs			ecsailmin EMEAAC
 Metwork Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device Enternal RADUS Servars Wers and Identity Stores Policy Elements Recess Policies Mentering and Reports System Administration 	Natwork Resource > hote Image: Cisc Description ACS Natwork Device Group Location Device Type IP Address IP Address IP 192.168.165 IP : 192.168.165 IP : 192.168.165 IP : 192.168.165	ork Devices and AAA Climits > Dreats	Selec	1 1 Authentication Options TACACS+ Shared Becret Cisco Single Connect Device Legacy TACACS+ Single Connect Bupport TACACS+ Draft Compliant Single Connect * RADIJS Shared Secret:

Sie sehen, dass der Client **Cisco** dem ACS-Server hinzugefügt wird.

cisco Cisco Secure ACS								
+ 💮 MyWorkspace	Network	Resources >	Netw	ork Devices and AAA (lients			
🗴 🦣 Network Resources	Netw	wrk Device:	5					
 Network Device Groups Location Device Text 	Filte	E		Match If.	v	00 🔻		
Network Devices and AAA Clients		Name		IP / Mask	NDG:Location	NDO:Device Type	Description	
Default Network Device External RADIUS Servers		Claco		192.168.165.3/32	All Locations	All Device Types	ACS to ASA	
Busers and Identity Stores								
→ SPolicy Elements								
Access Policies								
 Monitoring and Reports 								
🕨 🍓 System Administration								

3. Wählen Sie **Benutzer und Identitätsspeicher > Interne Identitätsdaten > Benutzer** und klicken Sie auf **Erstellen**, um einen neuen Benutzer zu erstellen

cisco Cisco Secure A	CS
 My Workspace 	Users and identity Stores > Internal identity Stores > Users
In Network Resources	Internal Users
Gentity Groups	Fitter: 💽 Match if: 💽 Go 💌
 Internal Identity Stores Users 	Status User Name Identity Group Description
Hosts	No data to display
 External Identity Stores LDAP 	
Active Directory	
RSA SecurID Token Servers	
RADIUS Identity Servers	
Certificate Authentication Profile	
Identity Store Sequences	
 Policy Elements 	
G Access Policies	
 Monitoring and Reports 	
+ 🍕 System Administration	
	Create Duplicate Edit Delete Change Password File Operations Export

 Geben Sie den Namen, das Kennwort und die Informationen zum Aktivieren des Kennworts an. Kennwort aktivieren ist optional. Wenn Sie fertig sind, klicken Sie auf Senden.

cisco Cisco Secure A	CS acsadmin EMEAACS
 MyWorkspace Network Resources Deers and Identity Stores Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecuriD Token Servers RADIUS Identity Stores Certificate Authomites Certificate Authomites Monitoring and Reports System Administration 	Users and kiertify Stores + Internal identity Stores + Libers + Creets General • Nama: cisco • Description: Test User • Identity Group: Balant Password Information Password must • Contain 4 - 32 characters • Contain 4 - 32 characters • Password: ••••• • Contain Methods Enable Password: • Contain Methods Contain Methods • Contain Methods Enable Password: • Contain Methods • Contain Methods • Contain Methods • Contain Methods • Contain Methods • Contain Methods • Change password on met login • Contain Methods • Enclared fields • • Required fields

Sie sehen, dass der Benutzer **cisco** dem ACS-Server hinzugefügt wird.

cisco Cisco Secure Ad	cs	
🕨 🖓 My Workspace	Users and identity Stores > Internal identity Stores > Users	
Network Resources	Internal Users	
Given and Identity Stores Identity Groups	Filter: Match if: Go	~
 Internal Identity Stores 	Status User Name 🔺 Identity Group	Description
Users Hosts	Cisco All Groups	Test User
 External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Certificate Authorities Certificate Sequences Policy Elements Caccess Policies Monitoring and Reports System Administration 		

<u>Überprüfen</u>

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Verwenden Sie den Befehl **cisco password cisco** überprüfen **mit der neuesten aaa-server-Authentifizierung cisco host 192.168.165.29**, um zu überprüfen, ob die Konfiguration ordnungsgemäß funktioniert. Dieses Image zeigt, dass die Authentifizierung erfolgreich ist und der Benutzer, der eine Verbindung zur ASA herstellt, vom ACS-Server authentifiziert wurde.

🖆 Command Line Interface	X
Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash.	
 Command ⊙ Single Line ✓ Enable context sensitive help 	(?)
test aaa-server authentication cisco host 192.168.165.29 username cisco password cisco	~
Response:	
Result of the command: "test aaa-server authentication cisco host 192.168.165.	
INFO: Attempting Authentication test to IP address <192.168.165.29> (timeout: INFO: Authentication Successful	
	>
ſ	Clear Response
Send Close Help	

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Fehlerbehebung

Fehler: AAA-Markierung von TACACS+-Server x.x.x.x in AAA-Servergruppen-

Taktiken als FEHLGESCHLAGEN

Diese Meldung bedeutet, dass die Cisco ASA die Verbindung zum x.x.x-Server verloren hat. Stellen Sie sicher, dass Sie über eine gültige Verbindung auf TCP 49 mit Server x.x.x.x von der ASA verfügen. Bei einer Netzwerklatenz können Sie die Zeitüberschreitung auf dem ASA-Server für TACACS+ von 5 auf die gewünschte Anzahl von Sekunden erhöhen. Die ASA sendet keine Authentifizierungsanfrage an den FAILED-Server x.x.x.x. Es wird jedoch den nächsten Server in den AAA-Server-Gruppen-Taktiken verwenden.

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliances der Serie ASA 5500
- <u>Cisco Adaptive Security Appliances der Serie ASA 5500 Befehlsreferenzen</u>
- <u>Cisco Adaptive Security Device Manager</u>
- Support-Seite für IPsec-Aushandlung/IKE-Protokolle
- <u>Cisco Secure Access Control Server für Windows</u>
- Anforderungen für Kommentare (RFCs)
- <u>Technischer Support und Dokumentation Cisco Systems</u>