ASA 8.3: TACACS-verificatie met behulp van ACS 5.X

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configureren Netwerkdiagram Configureer de ASA voor verificatie vanaf de ACS-server met CLI ASA configureren voor verificatie vanaf ACS-server met ASDM ACS als een TACACS-server configureren Verifiëren Problemen oplossen Fout: AAA-markering voor TACACS+ server x.x.x.x in tac's van de a-server als FAILLE Gerelateerde informatie

Inleiding

Dit document bevat informatie over de manier waarop u het security apparaat kunt configureren om gebruikers te controleren op een netwerktoegang.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de adaptieve security applicatie (ASA) volledig gebruiksklaar is en geconfigureerd om Cisco adaptieve security applicatie Manager (ASDM) of CLI in staat te stellen configuratie veranderingen door te voeren.

Opmerking: Raadpleeg <u>HTTPS Access voor ASDM</u> voor meer informatie over hoe u het apparaat op afstand kunt configureren door de ASDM.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Software voor Cisco adaptieve security applicatie, versie 8.3 en hoger
- Cisco adaptieve security applicatie Manager versie 6.3 en hoger

Cisco Secure Access Control Server 5.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het <u>Opdrachtupgereedschap</u> (alleen <u>geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918-adressen die in een labomgeving werden gebruikt.

Configureer de ASA voor verificatie vanaf de ACS-server met CLI

Voert deze configuraties voor de ASA uit om van de ACS server te authentiseren:

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)#aaa authentication ssh console cisco LOCAL ASA(config)#aaa authentication http console cisco LOCAL

Opmerking: Maak een lokale gebruiker op de ASA met de <u>gebruikersnaam cisco password cisco</u> <u>bevoorrecht 15</u> opdracht om ASDM met lokale authenticatie te benaderen wanneer ACS niet beschikbaar is.

ASA configureren voor verificatie vanaf ACS-server met ASDM

ASDM-procedure

Voltooi deze stappen om de ASA voor verificatie van de ACS-server te configureren:

 Kies Configuratie > Apparaatbeheer > Gebruikers/AAA > AAA-servergroepen > Toevoegen om een AAA-servergroep te maken

Server Group	Protocol	Accounting Mode	Reactivation Mode De	ad Time 🛛 M	lax Failed Attempts	Add Edik Delete
vers in the Selected Gr	oup		Telesfore		Timent	
vers in the Selected Gr Server Name or IP Ad	oup tress		Interface		Timeout	Add

2. Geef de gegevens van de **AAA-servergroep op** in het venster **AAA-servergroep** toevoegen zoals weergegeven. Het gebruikte protocol is **TACACS+** en de servergroep die is gemaakt,

Server Group:	cisco		
Protocol:	TACACS+	~	
Accounting Mode:	🚫 Simultaneous	💿 Single	
Reactivation Mode:	 Depletion 	🔿 Timed	
Dead Time: 10	minut	es	
Max Failed Attempts	3		

3. Kies Configuration > Apparaatbeheer > Gebruikers/AAA > AAA-servergroepen en klik op Add onder Server in de Geselecteerde groep om de AAA-server toe te voegen

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add
\$50	TACACS+	Single	Depletion	10	3	Edit Deleb
ers in the Selecter	Group					

4. Geef de informatie over de **AAA-server op** in het venster **Add AAA Server** zoals weergegeven. De gebruikte servergroep is

Server Group:	cisco	
Interface Name:	dmz	*
Server Name or IP Addre	ss: 192.168.165.29	
Timeout:	10	seconds
Server Port: 4		
SDI Messages		
Message Table		۲

op **OK** en vervolgens op **Toepassen**.U ziet de **AAA-servergroep** en de **AAA-server** die in de ASA zijn geconfigureerd.

5. Klik op

Toepassen.

Co	nfiguration > Device	Management	> Users/AAA > AAA S	erver Groups		
AA	A Server Groups					
	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
	cisco	TACACS+	Single	Depletion	10	3
4						
_						
be	rvers in the selected G	roup				
	Server Name or IP Ad	ldress		Interface		Timeout
	192,168,165,29			dmz		
	LDAP Attribute Ma	p				
				Г	Apply Re	set

 Kies Configuratie > Apparaatbeheer > Gebruikers/AAA > Toegang > Verificatie en klik op de vinkjes naast HTTP/ASDM en SSH. Kies vervolgens cisco als de servergroep en klik op Toepassen.

Configuration > Dev	rice Managemen	nt > Users/A	AA > AAA Access > Aut	hentication	
Authentication Au	thorization Accou	unting			
Enable authenticat	ion for administrate	or access to t	he ASA.		
Require authentica	tion to allow use o	f privileged m	ode commands		
Enable	Server Group:	.ocal 🔡	Use LOCAL when server	group fails	
Require authentica	tion for the followi	ing types of co	onnections		
HTTP/ASDM	Server Group:	cisco 💌	Use LOCAL when server	group fails	
Serial	Server Group:	.ocal 💽	Use LOCAL when server	group fails	
SSH	Server Group:	cisco 💌	Use LOCAL when server	group fails	
Telnet	Server Group:	ac 💽	Use LOCAL when server	group fails	
			Ap	ply R	eset

ACS als een TACACS-server configureren

Voltooi deze procedure om ACS als een TACACS-server te configureren:

1. Kies **Netwerkbronnen > Netwerkapparaten en AAA-clients** en klik op **Maken** om de ASA aan de ACS-server toe te voegen.

 My Workspace Network Resources Network Device Groups Location Device Type Network Devices and AAA/Clients Default Network Device Edemai RADIUS Servers Visers and Idantity Starss Policy Elements Access Policies Monitoring and Reports System Administration 	cisco Cisco Secure Ad	cs
 Network Resources Network Device Groups Location Dedice Type Network Devices and AAA Clients Default Network Device External RADIUS Servers Suss and Idanty Stores Policy Elements Access Policies Monitoring and Reports System Administration 	► S My Workspace	Network Resources > Network Devices and AAA Clients
Network Davices and AAA Clients Default Network Device External RADIUS Servers Image: Default Network Devices Image: Device Policy Devices Image: Devices Policy Dev	Network Resources Network Device Groups Location Device Type	Network Devices Filler: Match if. Go 🔻
 B Users and Identity Stores Policy Elements Access Policies Monitoring and Reports System Administration 	Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name A IP/Mask NDG:Location NDG:Device Type Description No data to display
Access Policies Montoring and Reports System Administration	Barrier Clements	
Monitoring and Reports System Administration	Access Policies	
	Monitoring and Reports System Administration	
Overste Durelande Edit Delate Elle Oversteers Event		

 Verstrek de vereiste informatie over de client (ASA is hier de client) en klik op Inzenden. Hierdoor kan de ASA worden toegevoegd aan de ACS-server. De details omvatten het IPadres van de ASA en de TACACS server

cisco Cisco Secure A	cs			əssədmin	EMEAAC
 MyWorkspace Network Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device Ensmal RADUS Servers Wers and Identify Stores Notes and Identify Stores Access Policies Monitoring and Reports System Administration 	Vatiwork Resources > Native e Name: Cisco Description: ACS to Network Device Group Location Device Type IP Address IP Address Single IP Addr IP: 192.168.185.3 IP: 192.168.185.3 IP: Single IP Addr IP: 192.168.185.3	AGA	Select Select Authentication Of ▼ TACACS+ ♥ Shared Bec Shigle (© Legacy TACACS ♥ RADIJS Shared Sec	ptions ret risco Connett Device TACACS+ Single Conne S+ Draft Compliant Sing ret	ect Bupport le Connect

U ziet dat de client-**Cisco** wordt toegevoegd aan de ACSserver.



3. Kies gebruikers en identiteitsopnamen > Interne identiteitsopslag > Gebruikers en klik op Maken om een nieuwe gebruiker te

maken.	
cisco Cisco Secure A	cs
🕞 🖓 My Workspace	Users and identity Stores > Internal identity Stores > Users
+ 💮 Network Resources	Internal Users
Gentity Groups	Filler: 💽 Match if: 💽 Go 🔫
 Internal Identity Stores 	📃 Status User Name 🔺 Identity Group Description
Hosts	No data to display
 External Identity Stores L DAR 	
Active Directory	
RSA SecuriD Token Servers RADIUS Identity Servers	
Certificate Authorities	
Certificate Authentication Profile Identity Store Sequences	
Policy Elements	
+ 🔂 Access Policies	
 Monitoring and Reports 	
System Administration	
1	
	Create Duplicate Edit Delete Change Password File Operations Export

4. Typ de informatie Naam, Wachtwoord en Wachtwoord inschakelen. Wachtwoord inschakelen is optioneel. Klik op Inzenden als u klaar bent.

cisco Cisco Secure Ad	acsadmin EMEAAd
 Network Resources 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 Authentication Profile Identity Store Sequences Policy Elements Access Policies Nonitoring and Reports System Administration 	Users and kientity Stores + Internal identity Stores + Lisers + Greets General • Nama: cisco • Description: Test User • Identity Group: Balact Pessword Information Password must • Contain 4 - 32 characters • Contain 4 - 32 characters • Password: •••••• • Contain 1 - 32 characters • Contain 4 - 32 characters • Password: •••••• • Contain 1 - 32 characters • Contain 4 - 32 characters • Contain 1 - 32 characters • Contain 4 - 32 characters • Contain 1 - 93 characters • Contain 4 - 32 characters • Contain 1 - 93 characters • Contain 4 - 32 characters • Contain 1 - 93 characters • Contain 4 - 93 characters • Contain 1 - 93 characters • Contain 4 - 93 characters • Contain 1 - 93 characters • Contain 4 - 93 characters • Change password on met login • Contain 4 - 93 characters • Password: •

U ziet dat de gebruiker **cisco** wordt toegevoegd aan de ACSserver.

cisco Cisco Secure AC	cs		
 My Workspace 	Users and identity Stores > Internal identity	y Stores > Users	
App Network Resources	Internal Users		
Busers and Identity Stores Identity Groups	Filter: Match if:	Go	
 Internal Identity Stores 	Status User Name	 Identity Group 	Description
Hosts	E Sco	All Groups	TestUser
 External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authonities Certificate Authonities Certificate Authentication Profile Identity Store Sequences Policy Elements Certificate Servers Monitoring and Reports 			

<u>Verifiëren</u>

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Gebruik **de** opdracht **cisco** van de **gebruikersnaam voor Cisco voor de** configuratie **van de** Cisco**server** op **de** testbasis **cisco host 192.168.165.29** om te controleren of de configuratie correct werkt. Dit beeld toont aan dat de authenticatie succesvol is en de gebruiker die verbinding maakt met de ASA is geauthentiseerd door de ACS server.

🖆 Command Line Interface	×
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	(2)
test aaa-server authentication cisco host 192.168.165.29 username cisco password cisco	(f)
Response:	
Result of the command: "test aaa-server authentication cisco host 192.168.165.	
INFO: Attempting Authentication test to IP address <192.168.165.3	29≻ (timeout:
	>
	Clear Response
Send Close Help	

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Fout: AAA-markering voor TACACS+ server x.x.x.x in tac's van de a-server als

FAILLE

Dit bericht betekent dat Cisco ASA de connectiviteit met de x.x.x.x server verloor. Zorg ervoor dat u een geldige verbinding op tcp 49 hebt om x.x.x van de ASA server te serveren. U kunt de timeout op de ASA-server voor TACACS+ ook verhogen van 5 naar het gewenste aantal seconden voor het geval er een netwerkvertraging is. ASA zou geen verificatieaanvraag naar de FAILED server x.x.x.x sturen. Het gebruikt echter de volgende server in de tac's van de a-server groep.

Gerelateerde informatie

- <u>Cisco ASA 5500 Series ondersteuningspagina voor adaptieve security applicaties</u>
- <u>Cisco ASA 5500 Series Opdrachten voor adaptieve security applicaties</u>
- <u>Cisco adaptieve security apparaatbeheer</u>
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- <u>Cisco Secure Access Control Server voor Windows</u>
- Verzoeken om opmerkingen (RFC's)
- <u>Technische ondersteuning en documentatie Cisco Systems</u>