ASA 8.3: Autenticazione TACACS con ACS 5.X

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Configurazione dell'ASA per l'autenticazione dal server ACS tramite CLI Configurazione di ASA per l'autenticazione dal server ACS con ASDM Configurazione di ACS come server TACACS Verifica Risoluzione dei problemi Errore: AAA Contrassegno di TACACS+ server x.x.x.x in gruppo di server aaa come NON RIUSCITO Informazioni correlate

Introduzione

In questo documento viene illustrato come configurare l'appliance di sicurezza per l'autenticazione degli utenti per l'accesso alla rete.

Prerequisiti

Requisiti

In questo documento si presume che le appliance ASA (Adaptive Security Appliance) siano completamente operative e configurate per consentire a Cisco Adaptive Security Device Manager (ASDM) o alla CLI di apportare modifiche alla configurazione.

Nota: per ulteriori informazioni su come consentire la configurazione remota del dispositivo da parte di ASDM, fare riferimento a <u>Consenti accesso HTTPS per ASDM</u>.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco Adaptive Security Appliance versione 8.3 e successive
- Cisco Adaptive Security Device Manager versione 6.3 e successive

Cisco Secure Access Control Server 5.x

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurazione dell'ASA per l'autenticazione dal server ACS tramite CLI

Per autenticare l'appliance ASA dal server ACS, attenersi alla seguente configurazione:

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

Nota: creare un utente locale sull'appliance ASA usando il comando <u>cisco password cisco</u> <u>privilege 15</u> per accedere all'appliance ASDM con autenticazione locale quando l'appliance ACS non è disponibile.

Configurazione di ASA per l'autenticazione dal server ACS con ASDM

Procedura ASDM

Per configurare l'ASA per l'autenticazione dal server ACS, completare la procedura seguente:

 Per creare un gruppo di server AAA, scegliere Configurazione > Gestione dispositivi > Utenti/AAA > Gruppi di server AAA > Aggiungi

						_
Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add Edk Delete
vers in the Selected G	roup					
vers in the Selected G Server Name or IP Ar	roup		Interface		Timeout	Add

2. Specificare i dettagli del **gruppo di server AAA** nella finestra **Aggiungi gruppo di server AAA**, come mostrato. Il protocollo utilizzato è **TACACS+** e il gruppo di server creato è

rver Group:	cisco		
rotocol:	TACACS+	*	
Accounting Mode:	🚫 Simultaneous	💿 Single	
Reactivation Mode:	 Depletion 	🚫 Timed	
Dead Time: 10	minut	es	
Max Failed Attempts:	3		
01/	Const		

3. Per aggiungere il server AAA, selezionare **Configurazione > Gestione dispositivi > Utenti/AAA >** Gruppi di server AAA, quindi fare clic su **Aggiungi** in **Server nel gruppo selezionato**.

	FIGCOCO	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add
sco	TACACS+	Single	Depletion	10	3	[
						Edit
						Delete
ers in the Selecter	d Group					
ers in the Selecter Server Name or IP	d Group		Interface		Timeout	Add

4. Specificare i dettagli del **server AAA** nella finestra **Add AAA Server** (Aggiungi server AAA), come mostrato. Il gruppo di server utilizzato è

Interface Name:	dmz 💉	
Server Name or IP Address:	192.168.165.29	
Timeout:	10	second
Server Secret Key: ••••	•	
SDI Messages		
		8
Server Secret Key: •••• SDI Messages	•	*

clic su **OK**, quindi su **Applica**.II **gruppo di server AAA** e il **server AAA** sono configurati sull'appliance ASA.

5. Fare clic su **Apply** (Applica).

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
l						
5.	overs in the Selected Gr	000				
~	Sames Name on ID Ad	uluara a		Teberfore		Timerak
	102 169 165 20	aress		Internace		Timeout
	192,100,105,29			amz		
	LDAP Attribute Mar	n				
	Contractioneer to					
					Apply Re:	set

6. Scegliere Configurazione > Gestione dispositivi > Utenti/AAA > Accesso AAA > Autenticazione e fare clic sulle caselle di controllo accanto a HTTP/ASDM e SSH. Quindi, selezionare cisco come gruppo di server e fare clic su Apply (Applica).

Configuration > Device Management > Users/AAA > AAA Access > Authentication
Authentication Authorization Accounting
Enable authentication for administrator access to the ASA.
Require authentication to allow use of privileged mode commands
Enable Server Group: LOCAL V Use LOCAL when server group fails
Require authentication for the following types of connections
✓ HTTP/ASDM Server Group: cisco ✓ Use LOCAL when server group fails
Serial Server Group: LOCAL Server Group fails
SSH Server Group: cisco V Use LOCAL when server group fails
Telnet Server Group: tac Server Group: tac
(Apply) Paret
Appry Reset

Configurazione di ACS come server TACACS

Completare questa procedura per configurare l'ACS come server TACACS:

 Per aggiungere l'appliance ASA al server ACS, selezionare Risorse di rete > Dispositivi di rete e client AAA, quindi fare clic su Crea.

My Workspace Network Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device	Network Resources > Network Devices and AAA Clients Network Devices Filter: Image: Match if: Image: Name IP / Mask No data to display
Instruct Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device	Network Devices Fifter: Match if: Go Co Name IP / Mask NDG:Location NDG:Device Type Description No data to display No data to display No No No No
Location Device Type Network Devices and AAA Clients Default Network Device	Filter: Match it Go Name ▲ IP / Mask NDG:Location No data to display No data to display
External RADIUS Servers	
B Users and Identity Stores Q Policy Elements	
Access Policies	
 Monitoring and Reports System Administration 	

2. Fornire le informazioni richieste sul **client** (qui ASA è il client) e fare clic su **Submit**. In questo modo, l'appliance ASA può essere aggiunta al server ACS. I dettagli includono l'**indirizzo IP** dell'ASA e i dettagli **del server**

TACACS.

cisco Cisco Secure Al	cs			assailmin EMEAAC
Cisco Secure All Cisc	Nativorit Resources > 100 voi Nativorit Resources > 100 voi Description ACS to Network Device Group Location Device Type IP Address Single IP Addr 0 IP: 192.168.165.3	d Devices and AAA Casels > Create D AGA IS All Locations All Device Types ess P Range(s)	Select Select	
	e Required fields			

Il client **Cisco** verrà aggiunto al server ACS.



3. Scegliere Utenti e archivi identità > Archivi identità interni > Utenti e fare clic su Crea per creare un nuovo

utente.	
cisco Cisco Secure A	cs
🔸 💮 My Workspace	Users and identity Stores > Internal identity Stores > Users
+ 💮 Network Resources	Internal Users
Gentity Groups	Filler: 💽 Malch if: 💽 Go 🗢
Internal Identity Stores	Status User Name 🔺 Identity Group Description
Hosts	No data to display
 External Identity Stores DAP 	
Active Directory	
RSA SecuriD Token Servers	
Certificate Authorities	
Certificate Authentication Profile	
Policy Elements	
Access Policies	
 Monitoring and Reports 	
System Administration	
	Create Duplicate Edit Delete Change Password File Operations Export

 Fornire le informazioni su Nome, Password e Abilita password. L'abilitazione della password è facoltativa. Al termine, fare clic su Invia.

cisco Cisco Secure AC	IS accession EMEAAC
 CISCO CISCO SECURE AC NetWork Resources Discrest and Mentity Stores Internal Identity Stores Users Hosts Enternal Identity Stores LDAP Active Directory RSA BecuriD Token Servers RADUS Identity Servers Certificate Authentication Profile Identity Store Sequences Policy Elements Access Policies Monitoring and Reports System Administration 	Sources and kientify Stores > Internal identity Stores > Lovers > Creets Ceneral • Name: Description: Test User • Identity Group: All Omups Password Information Password Information Password Information Password: • Contain 4 - 32 characters • Contain 1 • Contain 2 • Contain 2 • Contain 1 • Contain 2 • Contain 1 • Contain 2 • Contain 2 • Contain 2 • Contain 2 • Contain 3 • Contain 4 • Contain 5 • Contain 4 • Contain 5
	Submit Cancel

L'utente cisco verrà aggiunto al server

ACS.

//00.		
cisco Cisco Secure A	CS	
 MyWorkspace 	Users and identity Stores > Internal identity Stores > Users	
All Network Resources	Internal Users	
B Users and Identity Stores Identity Groups	Filter: Match if: Go	~
 Internal Identity Stores 	Status User Name 🔺 Identity Group	Description
Hosts	🗌 😑 <u>cisco</u> All Groups	Test User
LDAP Active Directory		
RSA SecurID Token Servers		
RADIUS Identity Servers		
Certificate Authorities		
Identity Store Sequences		
Policy Elements		
Access Policies		
Monitoring and Reports		
🕨 🍕 System Administration		

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Per verificare il corretto funzionamento della configurazione, **usare il** comando **cisco password cisco 192.168.165.29 username cisco host 192.168.165.29** username. Nell'immagine viene mostrata la riuscita dell'autenticazione e l'utente che si connette all'appliance ASA viene autenticato dal server ACS.

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	
Single Line ○ Multiple 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 192.168.16	5.
INFO: Attempting Authentication test to IP address <192.168.165.29> (timeout INFO: Authentication Successful	.=
	>
Clear Response	
Send Close Help	

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Errore: AAA Contrassegno di TACACS+ server x.x.x.x in gruppo di server aaa come

NON RIUSCITO

Questo messaggio indica che Cisco ASA ha perso la connettività con il server x.x.x.x. Verificare di disporre di una connettività valida su tcp 49 al server x.x.x.x dall'appliance ASA. Inoltre, è possibile aumentare il timeout sull'appliance ASA per il server TACACS+ da 5 al numero di secondi desiderato in caso di latenza della rete. L'appliance ASA non invierà una richiesta di autenticazione al server x.x.x.x con errori. Tuttavia, utilizzerà il server successivo nel gruppo di tacacs aaa-server.

Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance Pagina di supporto</u>
- Riferimenti per i comandi di Cisco ASA serie 5500 Adaptive Security Appliance
- <u>Cisco Adaptive Security Device Manager</u>
- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- <u>Cisco Secure Access Control Server per Windows</u>
- <u>RFC (Requests for Comments)</u>
- Documentazione e supporto tecnico Cisco Systems