IPS 7.X: Esempio di autenticazione di accesso utente con ACS 5.X come configurazione del server Radius

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Configurare IPS per l'autenticazione dal server ACS tramite IME Configurazione di ACS come server RADIUS Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene illustrato come configurare Cisco Intrusion Prevention System (IPS) per l'autenticazione dell'accesso utente tramite un server RADIUS. ACS viene utilizzato come server RADIUS.

Prerequisiti

Requisiti

In questo documento si presume che Cisco Intrusion Prevention System (IPS) sia completamente operativo e configurato per consentire a Cisco Intrusion Prevention System Manager Express (IME) o CLI di apportare modifiche alla configurazione. Oltre all'autenticazione AAA locale, è ora possibile configurare i server RADIUS per eseguire l'autenticazione dell'utente con sensore. La possibilità di configurare l'IPS in modo che utilizzi l'autenticazione AAA RADIUS per gli account utente, che facilita il funzionamento di distribuzioni IPS di grandi dimensioni, è disponibile in Cisco Intrusion Prevention System 7.0(4)E4 e versioni successive.

Nota: non è disponibile alcuna opzione per abilitare l'accounting su IPS. IPS 7.04 supporta l'autenticazione RADIUS, ma TACACS o Authorization o Accounting non sono supportati.

Componenti usati

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

- Cisco Intrusion Prevention System versione 7.0(4)E4 e successive
- Intrusion Prevention System Manager Express versione 7.1(1) 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>).

Configurare IPS per l'autenticazione dal server ACS tramite IME

Completare questa procedura per aggiungere l'IPS all'IME e quindi configurare l'IPS per l'autenticazione dal server ACS:

1. Scegliere Home > Dispositivi > Elenco dispositivi > Aggiungi per aggiungere un IPS all'IME.



2. Completare i campi nella finestra **Add Device** (Aggiungi dispositivo), come mostrato di seguito, per fornire i dettagli sull'IPS. Il nome del sensore utilizzato è **IPS**. Fare clic su

S Add Device								
Sensor Name:	,IPS							
Sensor IP Address:	192.168.165.8							
Web Server Port:	443							
Communication protocol								
⊙ Use encrypted connection (https)							
O Use non-encrypted connect	ion (http)							
Authentication								
Configuration User Name:	cisco							
Configuration Password:	•••••							
Use the Same Account for Configuration and Event Subscription (This is not recommended):								
Event Subscription User Name:	cisco							
Event Subscription Password:	•••••							
Event Start Time (UTC)								
Most Recent Alerts								
Start Date (YYYY:MM:DD):								
Start Time (HH:MM:SS);								
Exclude alerts of the following severity level(s)								
Informational Low	🗌 Medium 🔄 High							
	OK Capcel							

3. Fare clic su **Sì** per accettare il certificato e continuare la connessione https al sensore. È necessario accettare il certificato per connettersi al sensore e accedervi.

Certificate Information							
Do you want to trust the following certificate?							
Issuer: CN=192.168.165.8, OU=SSM-IPS10, O="Cisco Systems, Inc.", C=US Valid From: Wed Jan 26 00:41:18 IST 2011 Valid To: Sat Jan 26 00:41:18 IST 2013 Serial Number: 6FCB1954093BAD4E Signature Algorithm: SHA1withRSA Subject: CN=192.168.165.8, OU=SSM-IPS10, O="Cisco Systems, Inc.", C=US Fingerprint (MD5): D8 5E 49 86 1B 44 37 11 A9 EB D8 43 13 5E EB 98 Fingerprint (SHA): 24 55 28 03 E2 51 F1 DC 31 04 2C C9 BC 5E AF C6 D4 E3 EE 62							
Select Yes to accept the certificate and continue the https connection with this sensor. The certificate is stored in the C:\Documents and Settings\All Users\Application Data\Cisco Systems\IME\sensorcerts file. If you select No and reject the certificate, IME will not connect to the sensor.							

S denominato IPS viene aggiunto all'IME (Intrusion Prevention System Manager Express).

Home >	Devices > Device Li	ist							
🗣 Add 🗹 Edit 📋 Delete 🗼 Start 👻 📕 Stop 👻 🗞 Status 💸 T 👻									
Time	Device Name	IP Address	Device Type	Event Status	Global Correlation Status	Version			
<u> (</u>	JPS	192.168.165.8	ips-4240-k9	🗞 Connected	🗞 Connected	7.0(4)E4			
•									

4. Scegliere Configurazione > IPS > Impostazione sensore > Autenticazione, quindi attenersi alla seguente procedura:Per selezionare il server RADIUS come dispositivo di autenticazione, fare clic sul pulsante di opzione Server RADIUS.Specificare i parametri di autenticazione RADIUS, come mostrato.Scegliere Locale e RADIUS come autenticazione della console, in modo che venga utilizzata l'autenticazione locale quando il server RADIUS non è disponibile.Fare clic su Apply (Applica).

Jeer Authentication				
acui Authentication peol Authentication peol Authentication active Active Role Role Role Role Role Role Status Active Active				er Authentication: 🔘 Local 💿 Radius Server
peolfy the users that have access to the sensor. The service role is a special role that allows you to bypass the QL if needed. Only one service account is allowed. Username Role Status Status Administrator Administrator Administrator Administrator Administrator Addive Active Administrator Active Administrator Active Administrator Active Administrator Active Administrator Active Addive Active Addive Active Administrator Active Addive Addive Secondary Radius Server (optional) (Contarted on an accel and PADEUS (Contarted on ansole Authentication in Iccel and PADEUS (Contarted on ansole Authentication				cal Authentication
Username Role Status username Role Status sco Administrator Active ervice Service Active adius Authentication etwork Access ID: IPS Default User Role: Infinistrator Advess ID: IPS Default User Role: Infinistrator Infinitrator Infinis		needed. Only one service account is allowed.	e service role is a special role that allows you to bypass	edify the users that have access to the sensor.
Service Administrator Service Administrator Service Administrator Active	Add	Shahi u	Data	lost ama
adus Authentication adus Authentication atus Authentication if all Radius Servers are Unversionsive Primary Radius Server Server IP Address: 192:160.165.29 Authentication Port: 1612 Timeout (seconds): Shared Secret: oiscole		Active	Administrator	sen name
adus Authentication stuvorik Access ID: P5 Default User Role: Altow Local Authentication if all Radius Servers are Unresponsive Yrimary Radius Server Server IP Address: 192.160.165.29 Authentication Port: 1812 Timeout (seconds): 3 Shared Secret: disco	Edit	Active	Service	evice
dus Authentication twork Access ID: P5 Default User Role: Afministrator Allow Local Authentication if all Radius Servers are Unresponsive vimary Radius Server erver IP Address: 192.160.165.29 uthentication Port: 1612 ineout (seconds): 3 hared Secret: disco				
dus Authentication twork Access ID: P5 Default User Role: Allow Local Authentication if all Radius Servers are Unresponsive rimary Radius Server erver IP Address: 192.168.165.29 uthentication Port: 1812 imeout (seconds): 3 hered Seoret: issole Authentication rsole Authentication	Delete			
dus Authentication twork Access ID: IP5 Default User Role: Administrator Allow Local Authentication if all Radius Servers are Unresponsive rimary Radius Server erver IP Address: 192.168.165.29 uthentication Port: 1612 ineout (seconds): 3 hared Secret: disco sole Authentication isole Authentication: Local and RADDLS				
dus Authentication work Access ID: P5 Default User Role: Allow Local Authentication if all Radius Servers are Unresponsive rimary Radius Server erver IP Address: 192.160.165.29 uthentication Port: 1812 imeaut (seconds): 3 hared Seoret: issole Authentication rsole Authentication: Local and RADELS V				
dus Authentication twork Access ID: IP5 Default User Role: Intersponsive Allow Local Authentication if all Radius Servers are Unresponsive rimary Radius Server erver IP Address: I92.168.165.29 uthentication Port: 1812 meout (seconds): 3 hared Secret: disco rsole Authentication tsole Authentication: Local and RADIUS				
dus Authentication twork Access ID: IP5 Default User Role: Allow Local Authentication if all Radius Servers are Unresponsive rimary Radius Server erver IP Address: 192.160.165.29 uthentication Port: 1812 imeout (seconds): 3 hared Secret: disco				
dus Authentication work Access ID: [P5 Default User Role: Administrator Allow Local Authentication if all Radius Servers are Unresponsive rimary Radius Server erver IP Address: 192.166.165.29 uthentication Port: 1612 ineout (seconds): 3 hared Secret: disco msole Authentication rscle Authentication: Local and RADDL5 v	1			
Work Access ID: IP5 Default User Role: Administrator Allow Local Authentication if all Radius Servers are Unresponsive rimary Radius Server erver IP Address: 192.160.165.29 uthentication Port: 1012 imeout (seconds): 3 hered Secret: disco				deep to the effective
twork Access ID: IP5 Default User Role: Allow Local Authentication if all Radius Servers are Unresponsive rimary Radius Server erver IP Address: 192.168.165.29 authentication Port: 1812 ineout (seconds): 3 hared Secret: disco resole Authentication: Local and RADIUS				dius Authentication
Alkow Local Authentication if all Radius Servers are Unresponsive Vimary Radius Server kerver IP Address: 192.168.165.29 Authentication Port: 1812 imeout (seconds): 3 ihared Secret: disco			ser Bole: Administrator	twork Access ID: DP5 Default
Allow Local Authentication if all Radius Servers are Unresponsive Finany Radius Server Secondary Radius Server (optional) (Control (C				CHOICE HOUSES INC. U.S.
Timary Radius Server ierver IP Address: 192.160.165.29 Authentication Port: 1012 Timeout (seconds): 3 Shared Secret: isco			e Loresonnsive	Allow Local Authentication if all Radius Servers
Inviniary Radius Server Ierver IP Address: 192.168.165.29 Authentication Port: 1812 Shared Secret: disco				
Secondary Radius Server (optional) (Control Control Co				rimary Radius Server
lerver IP Address: 192.168.165.29 Authentication Port: 1812 Fineout (seconds): 9 Secondary Radius Server (optional) (s)				interior produces a second
ierver IP Address: 192.168.165.29 Authentication Port: 1812 Fineout (seconds): 3 Shared Secret: isso Fineole Authentication Fineole Authe				
Authentication Port: 1812 Secondary Radius Server (optional) (2) Fineout (seconds): 3 Shared Secret: disco Fineole Authentication Fineole Authentication Fineole Authentication Fineole Authentication: Local and RADIUS V				atuat ID Address: 102 168 165 20
Authentication Port: 1812 Secondary Radius Server (optional) (s) Fineout (seconds): 3 Shared Secret: disco Insole Authentication: Local and RADIUS V				erver IP Address: 192.100.105.29
Imeout (seconds): 5 Shared Secret: disco			Secondary Radius Server (optional) (8)	withantication Darty 1812
imeout (seconds): 3 ihared Secret: disco nsole Authentication nsole Authentication: Local and RADIUS				
hared Secret: disco				menut (seconds): 3
Shared Secret: disco				ineduc (seconds).
Insole Authentication				Shared Secret: disco
nsole Authentication				
nsole Authentication nsole Authentication: Local and RADBUS				
Insole Authentication: Local and RADIUS				made & the structure
insole Authentication: Local and RADIUS 💌				risple Auchentication
				insole Authentication: Local and RADILIS 🔽

Configurazione di ACS come server RADIUS

Per configurare il server ACS come server RADIUS, completare la procedura seguente:

1. Scegliere **Risorse di rete > Dispositivi di rete e client AAA**, quindi fare clic su **Crea** per aggiungere l'IPS al server ACS.

2. Fornire le informazioni richieste sul **client** (IPS è il client qui) e fare clic su **Invia**. In questo modo l'IPS viene aggiunto al server ACS. I dettagli includono l'**indirizzo IP** dell'IPS e i dettagli del **server**

RADIUS.		
Network Resources > Network Devices and	d AAA Clents > Create	
Name: IPS Description: IPS		
Network Device Groups		
Location All Location	ons	Select
Device Type All Device	Types	Select
Address Single IP Address IP: 192.168.165.8 = Required fields	P Range(s)	Authentication Options TACACS+ Shared Secret: Single Connect Device Legacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Support RADIUS Authentication Options Shared Secret: cisco
Submit Cancel		

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

cisco Cisco Secure AC	ecsedmin CS
🕨 🖶 😚 My Workspace	Users and kientty Stores + Internal kientty Stores + Users
Interview Resources	Internal Users
Busers and Identity Stores Identity Groups	Filter: 🕑 Match If: 💽 🐨
Internal Identity Stores	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 Authorities	
Identity Store Sequences	
Policy Elements	
Access Policies	
Monitoring and Reports	
System Administration	
	Create Duplicate Edit Delete [Change Password] File Operations Export

4. Specificare il **nome e la password**. Al termine, fare clic su **Invia**.

General				
Name:	IPS Status: Ena	ibled 🛃		
Description:	IPS access			
Identity Group:	All Groups	Select		
Password Inform Password must: • Contain 4	nation - 32 characters		Enable Password Informa Password must:	tion acters
Password:	••••		Enable Password:	
Confirm Password:	•••••		Confirm Password:	
🖸 Change p	assword on next login			
Jser Information				
Max User Per Session:	1			
E = Required field	19			
ERECUIRED FIELD	3			

Verifica

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

Provare ad accedere all'IPS con l'utente appena creato. Una volta autenticato l'utente, controllare il report su ACS.



Per visualizzare il report corrente, fare clic su Authentication-RADIUS-Today.

cisco Cisco Secure A	CS View								
👻 📄 Monitoring and Reports	Dashboard								
Dashboard E Alarms	General Troublesh	ooting Authentication Trends	ACS Health						
Inbox	S Minimum Severity: Info								
- Thresholds - Schedules									
Favorites	Severity	Name	Date		 Cause 				
Shared	0	ACS - System Errors	Fri Apr 22 01:34:00		Alarm caused by Al				
Catalog Troubleshooting Connectivity Tests ACS Support Bundle Deed Teucheshoote	Critical Alarm	🗥 Waming Alarm	()	nformation Alarm					
Band Troublesholer									
	Favorite Name		▲ F	Report Name					
	ACS - Configuration /	Audit - Today	م	ACS Instance>ACS_Configuration_Audit					
	ACB - System Errors	- Today	p	VCB Instance>ACB_Bys	tem_Diagnostics				
	Authentications - RAD	DIUS - Today	AAA Protocol>RADIUS_Authentication						
	Authentications - RAD	DIUS - Yesterday	ρ	VAA Protocol>RADIUS_A	luthentication				
	Authentications - TAC	ACS - Today	م	VAA Protocol+TACACS_/	Authentication				
	Authentications - TAC	ACS - Yesterday	p	VA Protocol=TACACS_/	Authentication				

Nell'immagine viene mostrato come l'utente che si connette all'IPS venga autenticato dal server ACS.

	Showing	Page 1	of 1						Goto Pag	ge: Go	
AAA Pi	AAA Protocol > RADIUS Authentication										
Authentication Status : Pass or Fail Date : April 29, 2011 (Last 30 Minutes Last Hour Last 12 Hours Today Yesterday Last 7 Days Last 30 Days)											
General	Generated on April 29, 2011 1:31:12 AM UTC										
Relo	Reload										
✓=Pass	s × -Fail	% −c	lick for de	tails	₿-Mot	isə over iten	n for additi	onal information			
	Logged At		RADIUS Status	NAS Failure	Details	Usemame	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address
Apr 29	,11 1:25:51.	.836 AM	1		9	<u>IPS</u>	127.0.1.1	Default Network Access	PAP_ASCII	<u>PS</u>	<u>192.168.165.8</u>

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

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Pagina di supporto per i sensori Cisco IPS serie 4200
- <u>Riferimenti per i comandi dei sensori Cisco IPS serie 4200</u>
- <u>Cisco IPS Manager Express</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