IPS 7.x: Konfigurationsbeispiel für die Benutzeranmeldung mit ACS 5.X als Radius-Server-Authentifizierung

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Konfigurieren von IPS für die Authentifizierung vom ACS-Server mithilfe von IME Konfigurieren des ACS als RADIUS-Server Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument enthält Informationen zur Konfiguration des Cisco Intrusion Prevention System (IPS) für die Benutzeranmeldeauthentifizierung mithilfe eines RADIUS-Servers. ACS wird als RADIUS-Server verwendet.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass das Cisco Intrusion Prevention System (IPS) voll betriebsbereit und so konfiguriert ist, dass das Cisco Intrusion Prevention System Manager Express (IME) oder die CLI Konfigurationsänderungen vornehmen kann. Neben der lokalen AAA-Authentifizierung können Sie jetzt auch RADIUS-Server für die Sensorbenutzerauthentifizierung konfigurieren. Die Konfiguration des IPS für die Verwendung der AAA RADIUS-Authentifizierung für Benutzerkonten, die den Betrieb großer IPS-Bereitstellungen unterstützt, ist in Cisco Intrusion Prevention System 7.0(4)E4 und höher möglich.

Hinweis: Es gibt keine Option, die Abrechnung auf dem IPS zu aktivieren. IPS 7.04 unterstützt die RADIUS-Authentifizierung, jedoch werden TACACS oder Authorization oder Accounting nicht unterstützt.

Verwendete Komponenten

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

- Cisco Intrusion Prevention System Version 7.0(4)E4 oder höher
- Intrusion Prevention System Manager Express Version 7.1(1) 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.

Konfigurieren von IPS für die Authentifizierung vom ACS-Server mithilfe von IME

Gehen Sie wie folgt vor, um IPS zu IME hinzuzufügen und das IPS für die Authentifizierung vom ACS-Server zu konfigurieren:

1. Wählen Sie Home > Devices > Device List > Add (Startseite > Geräte > Geräteliste > Hinzufügen, um ein IPS zum IME

Home > Devices > Device List • Add • Edit • Device Name • Device Type • Event Status • Sensor Health Global Correlation Status Version Click the • Add • Device to the system. or Click the • Video Help, to see the tutorial.	nınzuz	zutugen.									
Add Click the Edit Device Name IP Address Device Type Event Status Sensor Health Global Correlation Status Version Click the Add Dutton to add a device to the system. Or Click the Video Help to see the tutorial.	Home >	Devices > Device Li	st								
Time Device Name IP Address Device Type Event Status Sensor Health Global Correlation Status Version Click the Add button to add a device to the system. or or Click the Video Help to see the tutorial.	🙅 Add 🗃 Edit 🏦 Delete 🗼 Start 🕞 📰 Stop 👻 🖏 Status 😽 T 👻										
Click the Add button to add a device to the system. or Click the III <u>Yideo Help</u> to see the tutorial.	Time	Device Name	IP Address	Device Type	Event Status	Sensor Health	Global Correlation Status	Version			
Click the Add button to add a device to the system. or Click the III <u>Video Help</u> to see the tutorial.											
Click the Add button to add a device to the system. or Click the III <u>Video Help</u> to see the tutorial.											
Click the Add button to add a device to the system. or Click the III <u>Yideo Help</u> to see the tutorial.											
Click the Video Help to see the tutorial.						cleb the 🤹 add	hutton to add a davina to the	evetam			
or Click the 📔 <u>Video Help</u> to see the tutorial.						Cick the P Add	botton to abu a device to the	system.			
Click the 🔡 <u>Video Help</u> to see the tutorial.							OF				
						Click the 📕	<u>Video Help</u> to see the tutoria	l			
	1										
	- T						10				

2. Füllen Sie die Felder im Fenster **Add Device** (Gerät hinzufügen) aus, wie hier gezeigt, um Details zum IPS anzuzeigen. Der hier verwendete Sensorname ist **IPS**. Klicken Sie auf

😨 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 (recommended):	Configuration and Event Subscription (This is not							
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 s	everity level(s)							
Informational Low	Medium 🔄 High							
	Capcel							

3. Klicken Sie auf **Ja**, um das Zertifikat zu akzeptieren und die HTTPS-Verbindung zum Sensor fortzusetzen. Sie müssen das Zertifikat akzeptieren, um eine Verbindung zum Sensor herzustellen und auf diesen zuzugreifen.

© 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.
Yes No

IPS mit dem Namen IPS wird dem Intrusion Prevention System Manager Express (IME) hinzugefügt.

Add[🔏 Edit 📋 Delete	🕨 Start 👻 📕	Stop 👻 🗞 St	atus 💸 T 🝷		
Time	Device Name	IP Address	Device Type	Event Status	Global Correlation Status	Version
6 1	JPS	192.168.165.8	ips-4240-k9	🗞 Connected	🗞 Connected	7.0(4)E4

4. Wählen Sie Configuration > IPS > Sensor Setup > Authentication (Konfiguration > IPS > Sensor-Setup > Authentifizierung), und führen Sie die folgenden Schritte aus:Klicken Sie auf das Optionsfeld RADIUS Server, um den RADIUS-Server als Authentifizierungsgerät auszuwählen.Stellen Sie die RADIUS-Authentifizierungsparameter wie gezeigt bereit.Wählen Sie Lokal und RADIUS als Konsolenauthentifizierung aus, damit die lokale Authentifizierung verwendet wird, wenn der RADIUS-Server nicht verfügbar ist.Klicken Sie auf Übernehmen.

er Authentication: 🔘 Local 💿 Ra	dius Server		
cal Authentication			
early the users that have access to t	he sensor. The service role is a special role that allows you to bypass the	e CLI if needed. Only one service account is	allowed.
Username	Role	Status	Add
sco	Administrator	Active	Edb
arvice	Service	Active	Cak
			Delete
dius Authentication			
hunde Accord ID: 195	Default Lines Boles Education at a set		
(NUTR HOUSSS 10: 0-5			
Allow Local Authentication if all Rad	us Servers are Unresponsive		
Primary Radius Server			
Server IP Address: 192.168.165.2	9		
	Secondary Radius Server (optional) (8)		
Authentication Port: 1812			
Emerget (seconds): 3			
Theode (Secondary)			
Shared Secret: disco			
onsole Authentication			
onsole Authentication			
nsole Authentication Insole Authentication: Local and RAI	7.US M		
msole Authentication Local and RAI			

Konfigurieren des ACS als RADIUS-Server

Gehen Sie wie folgt vor, um den ACS als RADIUS-Server zu konfigurieren:

1. Wählen Sie Netzwerkressourcen > Netzwerkgeräte und AAA-Clients, und klicken Sie auf Erstellen, um das IPS dem ACS-Server hinzuzufügen.

 Geben Sie die erforderlichen Informationen zum Client an (hier ist IPS der Client), und klicken Sie auf Senden. Dadurch kann das IPS zum ACS-Server hinzugefügt werden. Zu den Details gehören die IP-Adresse des IPS und die Details des RADIUS-Servers

Description: IPS		
Network Device Groups	and the second s	
Location	All Locations	Belect
Device Type	All Device Types	Select
Single IP Address Single IP Addres IP: 192.168.165.8	s O IP Range(s)	Authentication Options TACACS+ Shared Secret Single Connect Device Eggacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Sup

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

cisco Cisco Secure Ad	CS
🕨 💮 MyWorkspace	Users and kientity Stores > Internet kientity Stores > Users
Network Resources	Internal Users
Identity Groups	Filter. Vlatch if. Oo 🔻
 Internal Identity Stores 	Status User Name 🔺 Identity Group Description
Hosts	No data to display
 External identity Stores 	
Active Directory	
RSA SecuriD Token Servers	
RADIUS Identity Servers Certificate Authorities	
Certificate Authentication Profile	
Identity Store Sequences	
E Arsono Delleino	
Mentarine and Reports	
Custom Administration	
P 😽 aystern Aurhinistration	
	Create Duplicate Edit Delete [Change Password] File Operations Export

4. Geben Sie den Namen und das Kennwort an. Wenn Sie fertig sind, klicken Sie auf Senden.

General		
o Name:	IPS Status: Enab	led 🗹 😐
Description:	IPS access	
Identity Group	All Groups	Select
Password Infor	mation	Enable Password Information
Password must		Password must:
 Contain 	4 - 32 characters	 Contain 4 - 32 characters
Password:	*****	Enable Password:
Confirm	•••••	Confirm
Change	password on next login	Password.
Jser Information	-	
Max User Per		
Session:		
= Required fiel	de la	

<u>Überprüfen</u>

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

Versuchen Sie, sich mit dem neu erstellten Benutzer beim IPS anzumelden. Überprüfen Sie den Bericht auf ACS, sobald der Benutzer authentifiziert wurde.



Klicken Sie auf Authentications-RADIUS-Today, um den aktuellen Bericht anzuzeigen.

cisco Cisco Secure A	CS View							
👻 📄 Monitoring and Reports	Dashboard							
Dashboard E Alams	General Troubleshooting Authentication Trends ACS Health Top 5 Alarms							
Inbox								
Thresholds Schedules Bennts	Minimum Severity: Info							
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 Expert Troubleshooter	Critical Alarm	🕰 Waming Alarm	() in	formation Alarm				
• 🧞 Monitoring Configuration								
10	Favorite Name		A R	eport Name				
	ACS - Configuration.	Audit - Today	A	CS Instance>ACS_C	configu	iration_Audit		
	ACB - System Errors	- Today	A	CB Instance>ACB_8	lystem	_Diagnostics		
	Authentications - RA	DIUS - Today	A	AA Protocol>RADIUS	3_Auth	entication		
	Authentications - RA	DIUS - Yesterday	A4	AA Protocol>RADIUS	S_Auth	entication		
	Authentications - TAC	CACS - Today	AAA Protocol > TACACS_Authentication					
	Authentications - TAC	CACS - Yesterday	N	AA Protocol>TACACI	8_Auth	entication		

Dieses Bild zeigt, dass der Benutzer, der eine Verbindung zum IPS herstellt, vom ACS-Server authentifiziert wird.

	Showing Pa	ige 1 d	of 1						Goto Paç	je: Go	
AAA Pr	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)											
Generat	Generated on April 29, 2011 1:31:12 AM UTC										
Reloa	<u>d</u>										
✓=Pass	×-Fail	Q=cl	ick for de	tails	₿-Mou	isə oyar itan	n for additi	onal information			
	Logged At		RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address
Apr 29,	11 1:25:51.83	36 AM	× .		<u>_</u>	IPS	127.0.1.1	Default Network Access	PAP_ASCI	IPS	<u>192.168.165.8</u>

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

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Support-Seite für Cisco IPS Sensoren der Serie 4200
- <u>Cisco Sensoren der Serie IPS 4200 Befehlsreferenzen</u>
- <u>Cisco IPS Manager Express</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>