IPS 7.X :用户登录验证使用ACS 5.X作为 RADIUS服务器配置示例

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 规则 配置 使用IME,配置验证的IPS从ACS服务器 配置ACS作为RADIUS服务器 验证 <u>故障排除</u> 相关信息

<u>简介</u>

本文提供信息关于怎样配置思科入侵防御系统(IPS)使用RADIUS服务器,用户登录验证的。ACS使 用作为RADIUS服务器。

<u>先决条件</u>

<u>要求</u>

本文假设,思科入侵防御系统(IPS)是完全能操作和已配置的允许思科入侵防御系统管理器Express (IME)或CLI做配置更改。除本地AAA认证之外,您能当前配置RADIUS服务器进行传感器用户认证 。能力配置IPS使用AAA RADIUS验证用户帐户,在大IPS部署的操作帮助,是可用的在思科入侵防 御系统7.0(4)E4和以后。

注意:没有选项对在IPS的启用帐户。有在IPS 7.04的RADIUS验证支持,但是不支持TACACS或授 权或者核算。

<u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

- •思科入侵防御系统版本7.0(4)E4和以上
- •入侵防御系统管理器Express版本7.1(1)和以上
- 思科安全访问控制服务器5.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

<u>规则</u>

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意: 使用<u>命令查找工具(仅限注册用户</u>)可获取有关本部分所使用命令的详细信息。

使用IME, 配置验证的IPS从ACS服务器

完成这些步骤为了添加IPS到IME从ACS服务器然后配置验证的IPS:

1. 选择**霍姆>设备>设备清单>Add**为了添加IPS到IME。

Home >	Home > Devices > Device List									
🗣 Add	🗃 Edit 💼 Delete	🕨 Start 🕞 🖬	Stop 🕞 📑 Sta	atus 💸 T 🝷						
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				
					disk the 📕	Uiden Hele, to can the tutorio	J			
					Click the	HORD HELD CO SEE THE CULONA	31.			
<										
Device D	Details									

 填入添加设备窗口的字段,如显示此处,为了提供关于IPS的细节。使用的传感器名称这里是 IPS。单击 Ok。

😨 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)									
Start Data (VVVV/MM/DD))									
Start Date (YYYY:MM:DD):									
Start Time (HH:MM:SS):									
Exclude alerts of the following s	everity level(s)								
	_ meuium _ High								
	X Cancel								

3. 点击是为了接受证书和继续对传感器的https连接。您必须接受证书为了连接对和访问传感器。



4. 选择Configuration>设置的IPS >传感器>验证,并且完成这些步骤:点击RADIUS服务器单选按钮为了选择RADIUS服务器作为认证设备。提供RADIUS验证参数,如显示。选择本地和 RADIUS作为控制台验证,因此使用本地认证,当RADIUS服务器不是可用的时。单击 Apply。

ecify the users that have access to	the sensor. The service role is a special role that allows you to bypass t	he CLI if needed. Only one service account is allo	wed.
Username	Role	Status	Add
500	Administrator	Active	Edit
adius Authentication stwork Access ID: 075	Defauk User Role: Stimmstrator		
Primary Radius Server			
Server IP Address: 192.168.165.2	Secondary Radius Server (optional)		
Authentication Port: 1812			

配置ACS作为RADIUS服务器

完成这些步骤为了配置ACS作为RADIUS服务器:

1. 选择网络资源>网络设备和AAA客户端,并且单击创建为了添加IPS到ACS服务器。

 My Workspace Metwork Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers System Administration 	
 Network Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers Servers Vers and Identity Stores No data to display 	
 Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers No data to display Filter: Match if: Marne IP / Mask NDG:Location NDG:Device Type No data to display	
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers Image: Client Se	
Network Devices and AAA Clients Default Network Device External RADIUS Servers Image: Control of the servers <th>Description</th>	Description
External RADIUS Servers	Description
Weers and Identity Stores Over Policy Elements Constraints Monitoring and Reports System Administration	
Policy Elements Access Policies Monitoring and Reports System Administration	
Access Policies Monitoring and Reports System Administration	
Monitoring and Reports System Administration	
System Administration	
	-

2. 提供关于**客户端的**必填信息(IPS客户端在这里),并且单击**提交**。这使IPS添加到ACS服务器。 详细信息包括IPS和**RADIUS服务器**详细信息的I**P地址**。

Description: IPS		
Network Device Groups		
Location	All Locations	Select
Device Type	All Device Types	Select
Single IP Address Single IP Addres IP: 192.168.165.8	IS IP Range(S)	Authentication Options TACACS+ Shared Secret Single Connect Device Legacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Sc RADIUS RADIUS

3. 选择用户,并且标识存储>内部标识存储> Users,并且单击创建为了创建新用户。

cisco Cisco Secure A	CS
🕨 🚳 My Workspace	Users and klentty Stores > Internal klentty Stores > Users
Image:	Internal Users
Gentliky 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. 提供**名称和密码信息**。完成时,请单击 Submit。

General			
Name:	IPS	Status: Enabled 💌 😬	
Description:	IPS access		
Identity Group	All Groups	Select	
Password Inform Password must • Contain -	mation : 4 - 32 characters		Enable Password Information Password must: Contain 4 - 32 characters
 Password: Confirm Password: Change (+++++ +++++ password on next login		Enable Password: Confirm Password:
User Information Max User Per Session:	1		

<u>验证</u>

使用本部分可确认配置能否正常运行。

设法登录与新建立的用户的IPS。一旦用户验证,请检查关于ACS的报告。



点击认证RADIUS**今天**为了查看当前报告。

cisco Cisco Secure A	CS View				
Monitoring and Reports Dashboard Alarms Inbox Therebolis	Dashboard General Troubleshi Top 5 Alarms				
Bchedules E Reports Favorites	Minimum Severity: Info	Name	Date	•	Cause
Catalog Troubleshooting Connectivity Tests ACS Support Bundle	Critical Alarm	A Warning Alarm	Information Alarm		Main caused by A
Expert Troubleshooter Jonitoring Configuration					
	Favorite Name ACB - Configuration A ACB - System Errors Buthentications - RAD Authentications - TAC Authentications - TAC	Audit - Today - <u>Today</u> DIUS - Today DIUS - Yesterday ACS - Today ACS - Yesterday	Report Name ACS Instance>ACS ACS Instance>ACS AAA Protocol>RAD AAA Protocol>RAD AAA Protocol>RAD AAA Protocol>TAC/ AAA Protocol>TAC/	\$_Configur }_System_ IUS_Authe IUS_Authe ACS_Authe ACS_Authe	ration_Audit _Diagnostics entication entication entication

此镜像显示连接对IPS的用户由ACS服务器验证。

	Showing I	Page 1	of 1						Goto Pag	je: Go	
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)											
Generate	Generated on April 29, 2011 1:31:12 AM UTC										
Reload											
✓=Pass	×-Fail	C	lick for de	dails	₿-Mou	isə over iten	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.	836 AM	× .		୍	<u>IPS</u>	127.0.1.1	Default Network Access	PAP_ASCII	IPS	<u>192.168.165.8</u>

<u>命令输出解释程序(仅限注册用户</u>)(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输 出的分析。

<u>故障排除</u>

目前没有针对此配置的故障排除信息。

相关信息

- Cisco IPS 4200系列传感器支持页面
- <u>Cisco IPS 4200系列传感器命令参考</u>
- <u>Cisco IPS Manager Express</u>
- IPsec 协商/IKE 协议支持页
- <u>用于 Windows 的 Cisco 安全访问控制服务器</u>
- <u>请求注解 (RFC)</u>
- <u>技术支持和文档 Cisco Systems</u>