FireSIGHT系统的集成有ACS的5.x RADIUS用户 验证的

目录

简介 先决条件 要求 使用的组件 配置 ACS 5.x配置 配置网络设备和网络设备组 添加在ACS的一Idenity组 添加本地用户到ACS 配置ACS策略 FireSight管理中心配置 FireSight管理型器系统策略配置 Enable (event)外部验证 验证 相关的思科支持社区讨论

简介

本文描述要求的配置步骤集成思科FireSIGHT管理中心(FMC)或Firepower受管理设备用远程认证拨入用户服务(RADIUS)用户认证的思科安全访问控制系统5.x (ACS)。

<u>先决条件</u>

<u>要求</u>

Cisco 建议您了解以下主题:

- FireSIGHT系统和受管理设备初始配置通过GUI和shell
- 配置在ACS 5.x的认证和授权策略
- •基本RADIUS知识

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科安全访问控制系统5.7 (ACS 5.7)
- •思科FireSight管理器中心5.4.1

在版本上当前是最新的版本联机。所有ACS 5.x版本和FMC 5.x版本支持功能。

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。

配置

ACS 5.x配置

配置网络设备和网络设备组

•从ACS GUI,请导航给网络设备组,点击设备类型并且创建设备组。在跟随的示例屏幕画面,设备类型FireSight配置。此设备类型将被参考在一个最新步骤的授权策略规则定义。 Click Save.

► 😚 My Workspace	Network Resources > Network Device Groups > Device Type > Edit: "Device Type:All Device Types:FireSight"
	Device Group - General Image: Select Image: Select Image: Select Image: Select Image: Select Image: Select
OCSP Services Users and Identity Stores	
Policy Elements	
Access Policies	
Monitoring and Reports	
System Administration	

•从ACS GUI,请导航给**网络设备组**,点击**NetwokDevices和AAA客户端**并且添加设备。提供一 个描述性名称和设备IP地址。 FireSIGHT管理中心在下面示例定义。

+

- 在网络设备组中,请配置设备类型同在上面步骤创建的设备组一样。
- 在**认证选项旁边**检查方框,挑选RADIUS复选框并且输入将使用此纳季的**共享密钥**。 当配置在 FireSIGHT管理中心时的RADIUS服务器请注释同一共享密钥再使用的以后。 要查看纯文本关 键值,请点击**显示**按钮。 单击 submit。
- 重复将要求GUI和shell访问的RADIUS用户认证/授权的所有FireSIGHT管理中心和受管理设备 的上述步骤。

添加在ACS的Idenity组

• 导航给**用户,并且标识存储,**配置**标识组**。 在本例中,创建的标识组是"FireSight管理员"。 此 组与在下面步骤定义的授权配置文件将连接。



添加本地用户到ACS

• 导航给**用户,并且标识存储,**配置**内部标识存储**部分的**用户**。输入本地用户创建的requried信息 ,选择上面步骤创建的**标识组**并且单击**提交。**

▶ → My Workspace	Users and Identity Stores > Internal Identity Stores > Users > Edit: "test"
Network Resources	
Busers and Identity Stores	General ○ Name: test Status: Enabled ♀
Identity Groups Internal Identity Stores 	Description:
Users Hosts	Email Address:
LDAP Active Directory	Assessed Dirable
RSA SecurID Token Servers RADIUS Identity Servers	Disable Account if Date Exceeds: 2015-Nov-01 (yyyy-Mmm-dd)
Certificate Authorities Certificate Authentication Profile	Disable account after 3 successive failed attempts
Identity Store Sequences	Password Hash
Access Policies	Enable Password Hash Authentication types CHAP/MSCHAP will not work if this option is enabled. While disabling the hash, ensure that password is reconfigured using change password option.
Monitoring and Reports	
System Administration	Password Lifetime
Television and the second s	Password Never Expired/Disabled: Overwrites user account blocking in case password expired/disabled
	User Information There are no additional identity attributes defined for user records
	Creation/Modification Information
	Date Wed Sep 02 13:15:56 UTC 2015 Created:
	Date Wed Sep 02 23:12:39 UTC 2015
	Date Wed Sep 02 13:15:56 UTC 2015
	Q = Required fields
	Submit Cancei

配置ACS策略

• 在ACS GUI中,请导航对策略元素>授权和权限>网络访问>授权配置文件。 创建与描述性名称

的一新的授权配置文件。在下面的示例中的,创建的策略是FireSight管理员。

► 🔂 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "FireSight Administrator"
Image: Network Resources	
Users and Identity Stores	General Common Tasks RADIUS Attributes
🔹 🥎 Policy Elements	
 Session Conditions Date and Time 	C = Required fields
Custom ▶ Network Conditions	
 Authorization and Permissions Network Access 	
Authorization Profiles Device Administration 	
Named Permission Objects Access Policies	
Monitoring and Reports	
System Administration	

• 在RADIUS属性请选中,添加授权的创建的标识组手工的属性以上并且单击提交

▶ 🦂 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "FireSight Administrator"
▶ Ŋ Network Resources	
As Users and Identity Stores	General Common Tasks RADIUS Attributes
Policy Elements	Common Tasks Attributes
 Session Conditions Date and Time Custom Network Conditions Authorization and Permissions Network Access Authorization Profiles Device Administration Named Permission Objects Access Policies Monitoring and Reports System Administration 	Attribute Type Value Manually Entered Attribute Type Value Class String Groups:FireSight Administrator
	Add A Edit V Replace A Delete Dictionary Type: RADIUS-IETF C O RADIUS Attribute: Class O Attribute Type: String Attribute Value: Static C O Groups:FireSight Administrator O = Required fields

- 导航对访问策略>Access Services>默认网络网络访问>授权并且配置FireSight管理中心管理会 话的一项新的授权策略。下面的示例使用NDG:设备类型&标识匹配设备类型和标识组的组情 况配置在上述步骤。
- •结果上此策略然后关联与在配置的FireSight管理员授权配置文件。单击 submit。



FireSight管理中心配置

FireSight管理器系统策略配置

- •登陆对FireSIGHT MC并且导航对**系统>本地>用户管理**。 点击**外部验证**选项卡。 点击**+创建验** 证对象按钮添加用户认证/授权的一个新的RADIUS服务器。
- ・选择认证方法的RADIUS。进入RADIUS服务器的一描述性名称。 输入主机名/IP地址和 RADIUS密钥。 密钥应该匹配在ACS以前配置的密钥。 随意地,如果一个存在,请输入一个备 份ACS服务器主机主机名/IP地址。
 Overview Analysis Policies Devices Objects AMP

				Local > User Management	Updates	Licenses	Mor
Users User Roles	External Authentication						
	External Authentication Obj	iect					
	Authentication Method	RADIUS ᅌ					
	Name *	ACS					
	Description						
	Primary Server						
	Host Name/IP Address *	172.18.75.172	ex. IP or h	ostname			
	Port *	1812					
	RADIUS Secret Key	••••					
	Backup Server (Optional)						
	Host Name/IP Address		ex. IP or h	ostname			
	Port	1812					
	RADIUS Secret Key						

• 在RADIUS特定的参数部分下,在本例中, Class=Groups :FireSight管理员值被映射给 FireSight管理员组。 这是作为ACCESS-ACCEPT一部分, ACS返回的值。点击**"Save"**保存配 置或继续到下面Verify部分测试与ACS的验证。

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=Groups:FireSight Administrator

•在Shell访问过滤器下,请进入用户逗号被分离的列表限制shell/SSH会话。

Shell Access Filter		
Administrator Shell Access Jser List	user1, user2, user3	

Enable (event)外部验证

最后,请完成这些步骤为了启用在FMC的外部验证:

- 1. 导航到**系统>本地>**System**策略**。
- 2. 选择在左面板的外部验证。
- 3. 更改状态对已启用默认情况下(禁用)。
- 4. 启用已添加ACS RADIUS服务器。
- 5. 保存策略并且重新应用在设备的策略。

验证

• 对ACS的测试用户验证,请移下来对**另外的测试参数**部分并且输入ACS用户的一个用户名和密码。单击测试。成功的测试将导致一绿色成功:测验全部的消息在浏览器窗口顶部。

Additional	Test Pa	rameters
------------	---------	----------

User Name	test	
Password	•••••	



这应该匹配等级值关联与在上面FireSIGHT MC配置的本地FireSight组。 Click **Save**.

Test Output	
Show Details	•
User Test	check_auth_radius: szUser: test RADIUS config file: /var/tmp/_bcEn4h_wF/radiusclient_0.conf radiusauth - response: [User-Name=test] radiusauth - response: Class=Groups:FireSight Administrator radiusauth - response: Class=CACS:
*Required Field	
	Save Test Cancel