使用思科身份服务引擎(RADIUS)的AsyncOS外部 身份验证

目录

简介 <u>先决条件</u> 要求 使用的组件 背景信息 配置 网络图 步骤1.创建身份验证组。 步骤2.创建本地用户进行身份验证。 步骤3.创建授权配置文件。 步骤4.创建授权策略。 验证 故障排除 相关信息

简介

本文档介绍在邮件安全设备(ESA)/安全管理设备(SMA)和思科身份服务引擎(ISE)之间成功实施 RADIUS外部身份验证所需的配置。

先决条件

要求

Cisco 建议您了解以下主题:

- •验证、授权和记帐 (AAA)
- RADIUS类属性。
- •思科ISE身份管理和授权策略。
- Cisco ESA/SMA用户角色。

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ISE 2.4
- 思科ESA 13.5.1、13.7.0
- 思科SMA 13.6.2

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。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

相关产品

未测试所用组件部分所列版本之外的版本。

背景信息

RADIUS类属性

对于记帐,RADIUS服务器在所有记帐数据包中包含的值是任意值。

类属性在ISE(RADIUS)中按组配置。

当用户被视为与其关联的属性为25的ISE/VPN组的一部分时,NAC根据身份服务引擎服务器(ISE)中 配置的映射规则实施策略。

配置

网络图



身份服务引擎接受来自ESA/SMA的身份验证请求,并将其与用户身份和组进行匹配。

步骤1.创建身份验证组。

登录ISE服务器并创建身份组:

导航至管理(Administration)->身份管理(Identity Management)->组(Groups)->用户身份组(User Identity Group)。如图所示.



注意:思科建议在ISE中为分配的每个ESA/SMA角色设置身份组。

步骤2.创建本地用户进行身份验证。

在此步骤中,创建新用户或分配已存在于我们在步骤1中创建的身份组的用户。请登录到ISE**并导航 至Administration -> Identity Management -> Identities**,然后创建新用户或分配给您创建的组中的 用户。如图所示.

Network Access Users List > New Netwo	rk Access User	
 Network Access User 		
* Name ESA_admin		
Status 🔽 Enabled 👻		
Email admins@mydomain.com		
▼ Passwords		
Password Type: Internal Users	•	
Password	Re-Enter Password	
* Login Password		Generate Password (i)
Enable Password		Generate Password
 User Information 	User Groups	
First Name		
Last Name	ALL_ACCOUNTS (default)	
	Anyconnect	
 Account Options 	Not1X	
	A Employee	
Description	SA_Admin	
Change password on next login \Box	ESA_DEMO	
0	ESA_Diego_Admins	
Account Disable Policy	ESA_Monitor	
	GROUP_ACCOUNTS (default)	
Disable account if date exceeds	GuestType_Contractor (default)	/y-mm-dd)
	GuestType_Daily (default)	
▼ User Groups	GuestType_Weekly (default)	
Select an item	- +	
Submit Cancel		

步骤3.创建授权配置文件。

RADIUS身份验证可以在没有授权配置文件的情况下成功完成,但是,不分配角色。要完成设置 ,请导**航至策略(Policy)->策略元素(Policy Elements)->结果(Results)->授权(Authorization)->授权配 置文件(Authorization profile)。**

注意:为每个要分配的角色创建一个授权配置文件。

Authorization Profiles > Aav	ega_ESA_Admin
Authorization Profile	
* Name	ESA_Admin
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	titte Cisco 💌 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
Common Tasks Web Authentication (I Airespace ACL Name ASA VPN AVC Profile Name	Local Web Auth)
 Advanced Attribute 	s Settings
Select an item	

注意:确保使用radius类属性25并指定名称。此名称必须与AsyncOS(ESA/SMA)上的配置匹配。从图3中,管理员是CLASS属性名称。

步骤4.创建授权策略。

最后一步允许ISE服务器识别用户登录尝试并映射到正确的授权配置文件。

如果授权成功,ISE会返回访问接受,并将CLASS值定义到授权配置文件。

导航至策略>策略集>添加(+符号)

+	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequence	Hits	Actions	View
Searc	5								
1	0	New Policy Set 1			+	Select from list 💌 🕇		٥	>

指定名称并选择加号以添加所需条件。本实验环境使用Radius。NAS-IP-Address。保存新策略。

ces Engine Home → C	Context Visibility	▼ Policy	Administration Work Centers		1 Lk	cense Warning 🔺	٩,	0	o o
g Posture Client Provisioning	Policy Elements			Click h	ere to do vis	ibility setup Do not	show thi	is again.	×
					eset Poli	cyset Hitcounts	E F	Reset	Save
olicy Set Name	Description	Conditio	ns	Allowed Proto	cols / Serv	er Sequence	Hits	Actions	View
SA_Policy			Network Access-Device IP Address EQUALS 10.122.111.238	Default Netwo	k Access	x = +	16	¢	>
	es Engine Home C Posture Client Provisioning blicy Set Name SA_Policy	es Engine Home Context Visibility Operations Posture Client Provisioning Policy Elements Dicy Set Name Description SA_Policy	es Engine Home Context Visibility Policy Posture Client Provisioning Policy Elements Conditio SA_Policy	es Engine Home Context Visibility Operations Policy Administration Work Centers a Posture Client Provisioning Policy Elements	es Engline Home	es Engine Home Context Visibility Operations Policy Administration Work Centers Click here to do vis Posture Client Provisioning Policy Elements Click here to do vis Click here to do vis Click here to do vis Reset Policy SA_Policy Lie Policy Network Access-Device IP Address EQUALS 10.122.111.238 Default Network Access	es Engine Home Context Valability Operations Policy Administration Work Centers Client Provisioning Policy Elements Click here to do visibility setup Do not Reset Policyset Hitcounts Click here to do visibility setup Click here to do visibility	es Engine Home Context Visibility Operations	es Engine Home Context Valbility Operations Policy Administration Work Centers Client Provisioning Client Provisioning Policy Elements Click here to do visibility setup Do not show this egain. Posture Client Provisioning Policy Elements Click here to do visibility setup Do not show this egain. Click here Description Conditions Allowed Protocols / Server Sequence Hits Actions SA_Policy Network Access: Device IP Address EQUALS 10.122.111.238 Default Network Access * * * 16 *

>

要正确匹配授权请求,必须添加条件。**选择**

图标并添加条件。

实验环境使用InternalUser-IdentityGroup并与每个授权配置文件匹配。

✓ Auth	orization F	Policy (5)							
					Results				
+	Status	Rule Name	Cond	itions	Profiles	Security Groups		Hits	Actions
Search	h								
	ø	ESA Monitor	牛	InternalUser-IdentityGroup EQUALS User Identity Groups:ESA_Monitor	ESA_Monitors	Select from list	- +	0	٥
	Ø	ESA HelpDesk	48-	InternalUser-IdentityGroup EQUALS User Identity Groups:HelpDesk	ESA_admin +	Select from list	- +	0	٥

步骤5.在AsyncOS ESA/SMA中启用外部身份验证。

登录AsyncOS设备(ESA/SMA/WSA)。 并导**航至ESA上的系统管理>用户>外部身份验证>启用外**部 身份验证。

Edit External Authentication

External Authentication Settings	
Enable External Authentication	
Cancel	Submit

提供以下值:

- RADIUS服务器主机名
- ▪端口
- 共享密钥
- 超时值(以秒为单位)
- 身份验证协议

选择将外部身份验证用户映射到多个本地角色(推荐)。 如图所示.

Edit External Authentication

External Authentication Settings								
C Enable External Authentication								
Authentication Type:	RADIUS 🔁							
RADIUS Server Information:	RADIUS Server Hostname	Port	Share	ed Secret	Timeout Value (in seconds)	Authentic	cation	Add Row
	x.x.x.x	1812	••••	••••	5	PAP	0	۵
External Authentication Cache Timeout: 🕐	0 seconds							
Group Mapping:	O Map externally authe	nticated u	sers to	multiple local rol	es. (recomme	ended)		
	RADIUS CLASS At	tribute		Role 🥐			Ad	dd Row
	Administrators			Administrator	0			Ŵ
	Monitors			Operator	0			Ŵ
	RADIUS CLASS attr	ibutes are	case-s	ensitive.				
	 Map all externally aut 	nenticated	users t	to the Administra	tor role.			
Cancel								Submit

注意:RADIUS CLASS属性必须与步骤3中定义的属性名称匹配(在映射为ASA VPN的常见 任务下)。

验证

请登录到您的AsyncOS设备,确认已授予访问权限并已正确分配分配的角色。如具有访客用户角色 的映像所示。

CISCO Email Secur	000V ity Virtual Appliance			Email Security Applianc	e is gett
Monitor					
My Dashboard					
				📜 Printable	PDF 🗗
Attention - A You ca	in customize this "My Dashboard"	nage by addi	ing report modules from different re	ports	
Some > Ove	modules are added for you by definition	ault. The Ove	erview page can be accessed from M	Ionitor	
System Overview	modules are added for you by definitient	ault. The Ove	erview page can be accessed from M	Ionitor	•
System Overview Overview > Status	rview.	ault. The Ove	Overview > Quarantines - Top 3 by D	isk Usage (Policy and Virus)	•
System Overview Overview > Status	rview. System Status:	Online	Overview > Quarantines - Top 3 by Di No quarantines are available	isk Usage (Policy and Virus)	+
System Overview Overview > Status	System Status: Incoming Messages per hour:	Online	Overview > Quarantines - Top 3 by Di No quarantines are available	isk Usage (Policy and Virus)	Ð
Some > Ove	System Status: Incoming Messages per hour: Messages in Work Queue:	Online 0	Overview > Quarantines - Top 3 by Di No quarantines are available	isk Usage (Policy and Virus)	•



如果登录尝试在ESA上失败,并显示消息"用户名或密码无效"。问题可能出在授权策略上。

登录ESA并从外部身份验证选择将所有外部身份验证用户映射到管理员角色。

RADIUS CLASS attributes are case-sensitive.

Map all externally authenticated users to the Administrator role.

提交并提交更改。尝试重新登录。如果登录成功,请双击ISE RADIUS授权配置文件(CLASS属性 25)和授权策略设置。

ISE 2.4AsyncOS