配置基于Radius和TACACS的用户身份验证

目录 简介 <u>先决条件</u> <u>要求</u> <u>使用的组件</u> 配置 <u>vEdge和控制器基于RADIUS的用户身份验证和授权</u> <u>vEdge和控制器基于TACACS的用户身份验证和授权</u> <u>相关信息</u>

简介

本文档介绍如何使用ISE为vEdge和控制器配置基于RADIUS和TACACS的用户身份验证和授权。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本演示使用ISE版本2.6。vEdge云和运行19.2.1的控制器

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。

配置

Viptela软件提供三个固定用户组名称:basic、netadmin和operator。 您必须将用户分配到至少一个 组。默认TACACS/Radius用户自动置于基本组中。

vEdge和控制器基于RADIUS的用户身份验证和授权

步骤1:为ISE创建虚拟RADIUS字典。为此,请创建包含以下内容的文本文件:

```
# -*- text -*-
#
# dictionary.viptela
#
```

# # Version: #	\$Id\$		
VENDOR	Viptela	4191	6
BEGIN-VENDOR	Viptela		
ATTRIBUTE	Viptela-Group-Name	1	string

第二步:将词典上传到ISE。为此,请导航到策略>Policy元素>词典。从字典列表中,导航到Radius >Radius Vendors,然后单击Import,如下所示。

sourcey pervices Engine Home	Control Visibility + Operations + Pub	* Administration +1	Wiph Carllen
cy Sets Profiling Posture Client Provision	ng: Thuicy Elements		
ionaries + Conditions + Results			
	REPORT Vendors		
Nithenartes	PORCESSION REPORTS		
A)	Anna Anna Marca Marca		
0 * E *	A rot deves Moneter	(toport	
 Count 	Name	 Vendor ID 	Description
 ConstAccess 	Arespece	14079	Dictorary for Vendor Arespace
 Identity Mapping 	Alahei-Lucent	800	Dictionary for Vendor Ricatel-Lucent
 Eil IdentityGroup 	C Andre	14823	Dictorary for Weidor Anaba
 InternatCA: 	Decorde	1588	Dictionary for Vendor Brexade
 Immediation 	Case	9	Dictionary for Vendor Cisco
 Internal/Dear 	Case-865M	99	Dictionary for Windor Clace-BBSH
 IORASISEY 	Case vPN3000	3076	Dictorary for Werdor Caco VPRO000
• 🔟 P	Hec	25506	Dictionary for Wendor HOC
	0 10	11	Dictorary for Medor HP
· Carlos a contra	Aniper	2636	Dictionary for Vendor Juniper
- <u></u> =000,000	Moseat	311	Dictionary for Vendor Microsoft
• CI NUD	Motorola-Bymbol	388	Dictionary for Vendor Hotorola Symbol
 Continuing 	C Ruba	25053	Dictionary for Vendor Ruckus
 METLOW 		14022	Dictionary for Wender WESPy
 Statustik Recent 			
 Eine Network Condition 			
 Interv 			
 EditorPExtension 			
 Improve Participation 			
• E Passive®			
 E Pestare 			
El PROFILIR			
· Ratur			
· · · · · · · · · · · · · · · · · · ·			
a UT Basel			
- CL 547			
 III TACACE 			
 III 10 MAG 			
 Treat 			

上传您在第1步中创建的文件。

rdada Identity Services Engine	Home + O	ontext Visibility 🔹 🕨	Operations	* Policy	+ Administration	Work Centers
Policy Sets Profiling Posture	Client Provisioning	Policy Elements				
Dictionaries + Conditions + I	Results					

ctionaries		Use this for to import a RADIUS Vendor. Select the file using the browser and click "import
	<i>a</i> ,	
- <u>-</u> -	÷.	Chose fiel dictionary violatia
• Guest		
GuestAccess		
 Identity Mapping 		Import Cancel
 IdentityGroup 		
 InternatCA 		
 InternalEndpoint 		
 InternalUser 		
 IOTASSET 		
• 🔟 P		
 ULDP 		
 III MAC 		
 MOM_LOG 		
 III MBE 		
 III MUD 		
 Mutimedia 		
 III NETFLOW 		
 I Network Access 		
 Interview Condition 		
 III MMP 		
 MMPEdension 		
 I Normalised Radius 		
 PassiveD 		
 Desture 		
 PROFILER 		
Radus		
 III IETF 		
 RADIUS Vendors 		
 Ession 		
 III SNMP 		
• 🔟 \$50P		
 LLI TACACS 		
 LLI TO-MAD 		
 III Threat 		

第三步:创建授权配置文件。在此步骤中,Radius授权配置文件将(例如)netadmin权限级别分配 给经过身份验证的用户。为此,请导航到策略>策略元素>授权配置文件,并指定两个高级属性(如 图所示)。

thereity Services Engine	Home + Context Visibility + Operations Policy + Administration + Work Centers
Policy Sets Profiling Posture C	Sant Provisioning - Policy Demons
Dictionaries + Conditions + Rasul	
0	
+ Authentication	Authorization Profiles > vEdge-netadmin
	Nacionazioni Provine
Authorization	• Name utop-retadron
Authorization Profiles	Description
Downloadable ACLs	*Access Type Access Accept *
+ Profiling	Network Device Profile (BCOsto) + (9)
1 Barbar	
	Service Template
+ Client Provisioning	Track Movement () (2)
	Passive Identity Tracking
	Common Tasks
	* Advanced Attributes Settings
	Radue:Service-Type 🙃 * NAS Prompt O
	Viptela Viptela Group Name 💿 = (vetadmin 🌀 — 🕂
	* Attributes Details
	Access Type = ACCESS ACCEPT
	Service-Type = 7 Vertela Column Name = netation

第四步:根据实际设置,策略集的外观可能会有所不同。出于本文演示的目的,我们创建了称为终 端访问的策略条目,如图所示。

thereity Services Engine	Mone +	Context Velocity	+ Operations	- Policy	+ Administration	+ West Centers		Α.		
Policy Sets Polling Pollure	Chart Provisioni	ing - + Policy Dama	erita							
Data Data							_			
Poncy Sets							Reset Policyset Hitcourt	•		Bave
Bata PolyBeth	ame	Description		Gendition			Allowed Protocols / Server Sequence	1426	Actions	View
bard-										
Terroral Acce				55 14	dua NAS Part Type B	DOALS VILLE	Oxfaul Network Access + 1		0	>

单击>,此时将显示下一个屏幕,如图所示。

Card I clently Services Engine	Home I Control Holdity I	Operations + Policy +	Administration + Work Centers		5	0 0
Putry Sets Profiling Posture Cl	ent Provisioning + Palcy Elements					
Policy Sets + Terminal Acce	15			Reset Polic	and Hiltonetia Reset	lan
Status Policy Set Name	Description	Conditions		Algue	d Protocola / Bener Beques	e His
Dearch						
O Territor Access		25 Patra	NAS-Port-Type EDDALS Vitual	Oute	d Network Access	•
Authentication Policy (1)						
> Authorization Policy - Local Exce	ptone					
> Authorization Policy - Global Exc	eptions					
♥Authorization Policy (2)						
			Results			
Status Rule Name	Conditione		Profiles	Security Groups	168	Actions
Search						
1 Q vitpensatris	 MenthyGroup Groups tell, 	e Name BRGAUB User (danti) jednik	(ralitye-ratadros)	• Selection Int	- + - 1	0
© Default			· Oursphotess	Detect from het		0

Rest Seve

此策略根据用户组lab_admin进行匹配并分配在步骤3中创建的授权配置文件。

第五步:定义NAS(vEdge路由器或控制器),如图所示。

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	٥,
System Identity Management	▼ Network Resources → Device Portal Management pxGrid Services → Feed Service → Threat Centric NAC	
Network Devices Network Device C	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
0		
Network Devices	Network Devices	
Default Device	* Name vEdge-01	
Device Security Settings	Description	
	IP Address 🔹 IP : 10.48.87.232 / 32	<u>.</u>
	* Device Profile 📾 Cisco 💌 🕀	
	Model Name	
	Software Version	
	* Network Device Group	
	Location All Locations Set To Default	
	IPSEC No.	
	Secto Deadic	
	Autoros Autoentication Setungs	
	RADIUS UDP Settings	
	Protocol RADIUS	
	* Shared Secret Show	
	Use Second Shared Secret 🔲 🕡	
	Show	
	CoA Port 1700 Set To Default	
	RADIUS DTLS Settings 👔	
	DTLS Required 🔲 🕧	
	Shared Secret radius/dtls	
	CoA Port 2083 Set To Default	
	Issuer CA of ISE Certificates for CoA Select if required (optional)	
	DNS Name	
	General Settings	
	Enable KeyWrap 🗌 🥡	
	Show	
	Message Authenticator Code Key Show	
	Key Input Format 💿 ASCII 🔘 HEXADECIMAL	

第六步:配置vEdge/控制器。

```
system
aaa
auth-order radius local
radius
server 10.48.87.210
vpn 512
key cisco
exit
!
```

步骤 7.验证。登录到vEdge并确保将netadmin组分配给远程用户。

vEdgeCloud1# show users

SESSION	USER	CONTEXT	FROM	PROTO	AUTH GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

vEdge和控制器基于TACACS的用户身份验证和授权

步骤1:创建TACACS配置文件。在此步骤中,将创建的TACACS配置文件分配给经过身份验证的用 户,例如netadmin权限级别。

• 从自定义属性部分选择必填,将属性添加为:

类型	名称	价值
必需	Viptela-Group-Name	网络管理 员

thereity Services Engine	Home + Contact Validity + Operation	ors + Policy + Administration 🗖	Set Carton	
NationAccess GuestAccess	Thatlac + 8100 + Poliar + Pol	Auro - Centra Administration - X PasalvelD		
Overview + Identifies User Identify	y Groups Ext M Sources + Network Res	enurose Policy Elements Device Admin.1	Pulicy Sets Reports Settings	
• Conditions	TACACS Profiles > +Edge			
Network Conditions	Name	vEdge_netectmin		
• Results	Description			
Alowed Protocols				
TACACE Command Sets TACACE Profiles	Task Atribute View Ra	a View		
	Common Tasks			
	Common Task Type (Shot) 4			
	Orlant Printage	0	(Select # to 18)	
	Maximum Privilege	0	(Select 4 to 16)	
	C Access Control Line	0]	
	 Add Command 	0]	
	O No Escape	0	(Select lines or failes)	
	Timest	0	Minutes (2-0000)	
	ide Tine	0	Minutes (2-0090)	
	Custom Attributes			
	+ AN BINN+ COM			۰-
	C Type Nam	ne Value		
	Mandatory 8 Wet	tela-Group-Name Autophia	0	~*
				Cancel Ser

第二步:为SD-WAN创建设备组。

the standy barries Draine more a Canad Malaky a C	pendiers + Policy Coloradors + West Carriers		
+ Bystein + Mersly Management + Nation Resources + Deuter Ports	Management prOnt Sensors + Feet Sensor + Tread Centro AAC		
Natural Devices Network Device Groups Network Device Profiles Ext	and NOUS Servers. NOUS Server Sequences. NAC Managers. External N	OW + Location Services	
Network Device Groups Al Groups Choose group *			
O Mark . A Mark Darlow C Ed. 2 Test. + Door	representation à la bourt - E fait baie - / bound Al	/ Column 40	ø -
C Name	Description	No. of Network Devices	
 * All device types 	All Device Types	-	
O 80-894			
All Loadow	#Classifiers		

Add Group

Name *	SD-WAN	
Description		
Parent Group *	All Device Types	x *
	·	

Х

Save

Cancel

第三步:配置设备并将其分配给SD-WAN设备组:

Network Devices List > vfdge-01	
Network Devices	
* Name v6dge-01	
Cesoription	
[IP Address +] * P : [10.48.87.232 // 32	- Q.,
* Desire Rodia 10 Const - 10	
Model Name -	
Software Version	
* Network Device Group	
Location at Locations	
Contra type So-way 😳 Sel Sa Default	
BADUS Authentication Settings	
TACACS Authentication Settings	
Shared Secret Show, Autor, 2	
Enable Single Connect Mode	
Esgacy Caon Device	
 MUAUS Unit Compliance single Connect support 	
• SAMP Settings	
 Advanced inserved beitings 	
Seve Reset	

根据实际设置,策略集的外观可能会有所不同。出于本文档演示的目的,将创建策略。

22.1	dentity Se	rnices Engine	Home + Context Visibility + Operations	• Paley • Marca	witten - Wark Centers	•				4	•	
a team	ort Access	A Quest Access	+ Trustee + 8100 + Poller + Poller	+ Dense Administration	* PassiveD							
N Quer	aller in t	dentities. Unit offer	Scholar Delicitudes + Network Resources	an Pring Denets	Device Advice Policy Data	Reports Define						
Policy	Sets							Class	Policy and Million			Less.
	Status	Policy Set Name	Description	Conditions				Alternal Protocols (Server Sequence	184	Actions	Vew
bard							_					
/	۲	võiges		Q DEVELOPING	e Type DBIALS At Device	Specific ANN		Default Device Adver			0	>
	0	Default	Texaco Default policy and					Ovlaut Deutos Adrio	** *		0	
										•	land)	lan

点击>,系统将显示如下图所示的下一个屏幕。此策略根据名为SD-WAN的设备类型进行匹配,并 分配在步骤1中创建的外壳配置文件。

the sheets for	vices Englise Harra +	Context Malitity - Operations	1 Pale 1	American	* Work-Centers			5.1	• • •	
A Reference Access	+ Guest Access + Trustles	+ 8100 + Poller + Poller	• On the Adverse	tation A Passis	-00					
+ Overview - + 10	terms variently-brase 6	et le Bources - Metwork Resource	 Margitters 	ette Devisione	in Policy Sets Reports	Settings				
Policy Sets +	vEdges						Reset Policyaet IS	teaunta (Tree	0.000	
Status.	Policy Set Name	Description	Conditions				Allowed Prote	oon / Dever Depa	ence Mits	
Search .										
۲	rtiges		Q 05×05	Dentos Notes 1930	ALS AT Device Types#0019	-	Delast Device		•	
3 Autorituator	Pulicy (1)									
> Authorization	Pulley - Local Exceptions									
> Authorization	Policy - Global Ecosphores									
* Autorization	Pulicy (2)									
					Fends					
- 5MM	Rule Name	Conditions			Command Batt		Shell Profiles	10	is Adore	6
forest.		-			_					
۵	-Citys-relativity	a IntertryGroup Name (CQ)	ALC: UNIT MARKED	Onanite, alter		+	days, seasons	+	• •	
٥	Owland				Abergettion	+	Dery NI Shat Profile	•• +	• •	

Reset Seve

第五步:配置vEdge:

```
system
aaa
auth-order tacacs local
!
tacacs
server 10.48.87.210
vpn 512
key cisco
exit
!
```

第六步:验证。登录vEdge并确保将netadmin组分配给远程用户:

vEdgeCloud1# show users

SESSION	USER	CONTEXT	FROM	PROTO	AUTH GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

相关信息

- 思科ISE设备管理规范部署指南:<u>https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hld-298630973</u>
- 配置用户访问和身份验证: <u>https://sdwan-</u> <u>docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。