Configure Radius and TACACS-Based User Authentication

Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
<u>Configure</u>
Radius-Based User Authentication and Authorization for vEdge and Controllers
TACACS-Based User Authentication and Authorization for vEdge and Controllers
Related Information

Introduction

This document describes how to configure Radius- and TACACS-based user authentication and authorization for vEdge and controllers with ISE.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

For the purpose of the demonstration, ISE version 2.6 is used. vEdge-cloud and controllers running 19.2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

The Viptela software provides three fixed user group names: **basic**, **netadmin**, and **operator**. You must assign the user to at least one group. The Default TACACS/Radius user is automatically placed in the basic group.

Radius-Based User Authentication and Authorization for vEdge and Controllers

Step 1. Create a Viptela radius dictionary for ISE. To do so, create a text file with the content:

```
# -*- text -*-
#
```

<pre># dictionary.v #</pre>	iptela		
# # Version: #	\$Id\$		
VENDOR	Viptela	41916	6
BEGIN-VENDOR	Viptela		
ATTRIBUTE	Viptela-Group-Name	1	string

Step 2. Upload dictionary to ISE. For this, navigate to **Policy > Policy Elements > Dictionaries**. From the list of Dictionaries, navigate to **Radius > Radius Vendors** and then click **Import** as shown.

Join Identity Services Engine Home	Conset Visibility Operations	Policy Administration	+ Mork Centers	
Policy Sets Profiling Posture Client Provision	ing Policy Elements			
Continuentes + Constituente + Resulte				
Contractor - Contractor				
Dictionaries	RADIUS Vendors			
(P				
(1 + K +)),	/ sit +as Xoom	bineet Brineet		
 Used 	Nome	 Vendor ID 	Description	
Ci duestAccess	Arespece	14079	Octonary for Vendor Arespace	
 Identity Mapping 	Atatel-Looent	800	Dictionary for Vendor Alcatel-Lucent	
 El IdentityGroup 	C A164	14023	Dictorary for Vendor Aruba	
• 🔛 InternatCA	Brocade	1588	Dictionary for Vendor Brocade	
 EnternatEndport 	Case	9	Dictionary for Vendor Cace	
 Internal/Jear 	Cecc-885M	99	Dictionary for Vendor Caco-885H	
• UI (05466)	Case-1993000	3076	Dictionary for Vendor Caco-VPN3000	
- 100 P	C HOG	25306	Dictionary for Vendor HOC	
1 ITI MAC	C HP	11	Dictionary for Vendor HP	
 INOM LOG 	avier	2636	Dictionary for Vendor Juniper	
• 🖾 M56	Morenoli	311	Dictionary for Vendor Microsoft	
• 🔛 MUD	Motorola Symbol	388	Dictionary for Vendor Motorola-Symbol	
 El Mutimedia 	C Ruckus	15053	Dictionary for Vendor Ruckus	
 INETFLOW 		14022	Dictionary for Vendor W29h	
 Imbech Access 				
 Eil Natwork Condition 				
• 🔛 (%66%)*				
CO Number Dates				
 Constant 				
 Destars 				
 PROFLOR 				
* 🧱 Radus				
- 11 H H				
 EADUS Mentors 				
• Garator				
• (2) Date				
- (1) Three (1)				
• (1) YEAR				
+ 🖾 Tread				
	1			

Upload the file you created on step 1.

dealer Identi	ty Service:	s Engine	Home I	Context Visibility	Operations	* Policy	+ Administration	+ Work Centers	
Policy Sets	Profiling	Posture	Client Provision	ing Policy Eleme	nts				
Dictionaries	+ Conditi	ons + Ri	esults						

Dictionaries		
		Use this for to import a RADIUS Vendor. Select the file using the browser and click "Impor
		• Vendor file:
0 · 1 = •	·	Choose file dictionary vipilela
 Guest 		
 GuestAccess 		Tennet Count
 Lifentity Mapping 		amport cance
 IdentityGroup 		
 InternalCA 		
 InternalEndpoint 		
 InternalUser 		
 IDIASSET 		
+ 🔟 P		
 LLDP 		
 III MAC 		
 III MDM_LOG 		
 III M88 		
 III MUD 		
 III Multimoda 		
 III NETFLOW 		
 III Network Access 		
Network Condition	i i i i i i i i i i i i i i i i i i i	
 III NMAP 		
 III NMAPExtension 		
 III Normalised Radiu 	6	
 E PassivelD 		
 III Posture 		
 PROFILER 		
 Radius 		
 III III III 		
RADIUS Vendo	a	
 El Session 		
 III SNMP 		
 III SXP 		
 TACACS 		
 III TO-NAC 		
 III Threat 		

Step 3. Create an Authorization Profile. In this step, Radius authorization profile assigns, for example, netadmin privilege level to an authenticated user. For this, navigate to **Policy > Policy Elements > Authorization Profiles** and specify two advanced attributes as shown in the image.

there is a service of the services Engine	Home + Context Visibility + Operations Policy + Administration + Work Centers
Policy Sets Profiling Posture C	Sant Provisioning Policy Demonts
Dictionaries + Conditions + Rasul	ta
0	
Authentication	Authorization Profiles > vEdge-metadmin
	Authorization Profile
 Authorization 	* Name utdge-netadmin
Authorization Profiles	Description
Downloadable ACLs	*Access Type Access_Accept +
+ Profiling	Network Device Profile III Charts = 0
+ Posture	Service Template
+ Client Provisioning	Track Movement 🗁 🗵
	Passive Identity Tracking
	► Common Tasks
	* Advanced Attributes Settings
	Radius:Service-Type 🙃 = NAS Prompt 🌀
	Viptela Viptela Group Name 🙃 = Instadmin 🌀 — 🕂
	w Attributes Partalle
	Access Type = ACCEST
	Service-Type = 7
	Advise month-security
	2000 HERE

Step 4. Depending on your actual setup, your Policy Set may look differently. For the purpose of the demonstration in this article, the Policy entry called **Terminal Access is** created as shown in the image.

22 1	tentity Se	nices Engine	Home	+ Context Validity	+ Operations	+ Policy	Administration	+ Work Centers		- 5	•	
Policy 5	ing Pa	fling Posture	Cherti Provini	oning - + Policy Elem	erin .							
Policy	Sets								Reset Policyset Hitcour	•		Seve.
(\bullet)	Status	Policy Set Nac	Ne	Description		Conditions			Allowed Protocols / Server Sequence	160	Actions	View
learch												
	0	Terrinal Access				10 M	ine INAS Port Type B	DUALE Visual	Oxfaul NationA.Access + +		o	>

Click > and the next screen appears as shown in the image.

· 古古 - 14	entity Ser	vices Engine Pare	· Control Tablety	• Operations • •	where we do	deviction of the	1 Mark Carlles			9,		0 0
Policy Se	es Post	ing Posture Olert Po	minoring + Policy Daman	6								
Policy:	Sets +	Terminal Access							Read Policyaet	Hitopunta	lanet.)	See.
	Status	Policy Set Name	Description	Cor	dtions				Allowed Pro	noosta / Server S	lequence	His
Description												
	٥	Terrinal Access		100	Radius N	Ad-Post-Type D	IGALS Vitual		Default Nat	work.Aurana	• • •	1
3 Auto	entication	Policy (1)										
> Auto	elpation (Policy - Local Exceptions										
) Auto	orization	Policy - Global Exception										
v. _{Auto}	orization I	Policy (2)										
-						Reads						
e	Status	Rule Name	Conditions			Profiles		Secu	rty Groups		100	Actions
beard												
	0	vEstpenetadinin	# Merth/G Groups in	tsu: Name BRGAUB Al, admin	User Dentity	relation	wadnie (+ 50	et hun lat	- +	1	0
	0	Ovtext				(+Ourpho	CHINA .		or how fait	- +		0

This policy matches based on user group lab_admin and assigns an authorization profile that was created in Step 3.

Step 5. Define NAS (vEdge router or controller) as shown in the image.

-Identity Services Engine Home	Context Visibility Operations Policy Administration Work Centers	Q,
System Identity Management ✓ Netw	ork Resources → Device Portal Management pxGrid Services → Feed Service → Threat Centric NAC	
Network Devices Network Device Groups	Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services	
0		
Network Devices	work Devices List > vEdge-01	
Default Device Ne	work Devices	
Device Security Settings	* Name vEdge-01	
	Description	
	10 Address - * ID - 10 49 97 323	542
	IP Address • IF . 10.46.67.232	98 +
	* Device Profile dtt Cisco 💌 🕀	
	Model Name	
	Software Version	
	* Network Device Group	
	Location All Locations 📀 Set To Default	
	IPSEC No Set To Default	
	Device Type All Davies Types 0	
	all bevice types 🗸	
	RADIUS Authentication Settings	-
	RADIUS UDP Settings	
	Protocol RADIUS	
	* Shared Secret Show	
	Use Second Shared Secret	
	Show	
	CoA Port 1700	
	RADIUS DTLS Settings (j)	
	Shared Secret radius/dtle	
	CoA Port 2002 Cet To Default	
	Louis Of at IOE Destination for Oat	
	Issuer CA of ISE Certificates for CoA [Select if required (optional)	
	DNS Name	
	General Settings	
	Enable KeyWran	
	* Key Encryption Key	
	* Message Authenticator Code Key	
	Key Input Format 💿 ASCII 🕕 HEXADECIMAL	

Step 6. Configure vEdge/Controller.

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

Step 7. Verification. Log in to vEdge and ensure netadmin group assigned to the remote user.

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

TACACS-Based User Authentication and Authorization for vEdge and Controllers

Step 1. Create a TACACS profile. In this step, the TACACS profile created is assigned, for example, netadmin privilege level to an authenticated user.

• Select **Mandatory** from the **Custom attribute** section to add the attribute as:

Туре	Name	Value
Mandatory	Viptela-Group-Name	netadmin

Carlo Identity Services Engine	Home + Context Validity + Oy	erators + Policy + Administration	• Work Centers	
Network Access Guest Access	Trutter + 8100 + Polier +	Posture - Ceutos Administration - Fass	well)	
Overview + Identifies User Identified	Croupe Entild Sources + Network	R Resources Policy Elements Device Ad	min Pulicy Sets Reports Settings	
	The second s			
+ Conditions	TACACO Politica - vicioja			
Network Conditions	INCACO PIONO	lame «Estpe_retectmin		
+ Results				
Allowed Protocols	Descri	ption		
TACACE Command Sets				
SAGACS Profiles	Task Athlbute View	Raw View		
	Common Tasks			
	Common Task Type Shell 1	1		
	 Default Privilege 		(Select 0 to 15)	
	 Maximum Phyloge 		😳 (Select 9 to 18)	
	C Access Control Link		0	
	C Auto Command		0	
	· No Escape		Christ line or biles	
	- Tenend			
	0.04.054		Q Minutes (2-0000)	
	Custom Attributes			
	+ AN BINNE CO			۰-
	C Type	Name Value		
	Mandatory 0	Viptela-Group-Name netadmin	0	~*
				Cancer Save

Step 2. Create a device group for SD-WAN.

The Martily Services Engine more a Conset Velocity a Operator	a thing Administration that Carlos	
+ Bysten + Hently Management + Nation's Resources - In Deuter Purse Heney	ament particul benation + Faset Bankar + Thread Caretro NAC	
Natwork Devices Natwork Device Groups Natwork Device Profiles External for	OUS Servers RIGUS Server Sequences IAC Managers External MON	* Location Services
Natwork Device Groups		
Al Grage Choose group *		
Charan + Ant Darion Clin 2 has 0 hourses	nten kinset Zibert Biltelan Zibertik Z	Column All Dev
O Name	Description	No. of Network Devices
A de deven types	All Denits Types	-
0 80-899		1 C
 Alf-Loadons 	AT Loadons	
the PERCONNE	In this a REQUIRING THE POST Device	-

Add Group

Name *	SD-WAN	
Description		
Description		
Parent Group *	All Device Types	x =
	Cancel	Save

Step 3. Configure the device and assign it to the SD-WAN device group:

Network Devices List > vfidge-01	
Network Devices	
* Name widge-01	
Cesoription	
[IP Address → * IP : [10.48.87.232 / [32	÷
* Device Profile 🗰 Cace = 💿	
Mode Name	
Software Version +	
* Network Device Group	
Location at Locations 😳 det To behalt	
PSOC No Set To Default	
Device Type SD-WAN	
• SADUS Automication Settings	
TACACS Authentication Settings	
Shared Secret	
Enable Single Connect Mode	
Espacy Caon Device	
 TACACS Craft Compliance Single Connect Support 	
• INAP lations	
 Advanced trustoec bettings 	
Save Reset	

Step 4. Define Device Administration Policy.

 \times

Depending on your actual setup, your Policy Set may look differently. For the purpose of the demonstration in this document, the Policy is created.

the state the state of the stat	+ Content Visibility + Operation	Palay Adventuries *Web Deters		- 4 - I	• •	
+ Network Access + Quest Access + Trust	lec + 8100 + Poller + Poller	Dense Admonstration + PassiveD				
+ Overview + Identities User Identity Only	 Ext.N Sources + Network Resources 	on + Putry Denerts Desta Admin Putry Earls Reports Bettings				
Policy Sets			Reset Policyset/Nitcourt			ten)
Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	His A	done	Ver
Samb						
× © vitages		Q DEVOLUTION Tops DEMAN At Device TypesHD-MAX	Defaul Device Adres 🔹 + 💌		0	>
O Detect	Taxaca Default policy and		Defaul Device Admin 🔹 🔹 🗮		0	э
				(Res	-	lan)

Click > and the next screen appears as shown in this image. This policy matches based on device type named **SD-WAN** and assigns the Shell profile that is created in step 1.

Carlo Marithy Services Engine House	• Contest Webbly • Operat	on they thereaster **	ton Genters		5 B	• •
+ Network Access + Const Access + Trust	es + 8100 + Poller + Po	Are + Device Adversionalise + PassinetD				
+ Overview + Identities User Identity Onsur	 Extra barrans Method: Network Ne	sources + Pelicy Densets Deuts Admin.1	hity bes Reports Bellings			
Policy Sets + vEdges				Reset Policyset Hilson	ata (Jaset)	See.
Status Policy Set Name	Description	Conditions		Alowed Protocols	/ Server Sequence	165
beet.						
O visiges		Q ODFOL Owner Type DEGALS	At Device Types#50 mms	Default Denter Adr		+
Authentication Policy (1)						
> Authorization Policy - Local Exceptions						
> Authorization Policy - Global Ecosphore						
✓ Authorization Policy (2)						
			Passala			
Data Rule Name	Conditions		Command Bats	Shall Profiles	100	Actions
forst			-		_	
et inperventation	· Interfering Fairs	0206.3 Oar tenty Dropciel, alree		· dap, water	•	0
Q teter			(+(berg/loConstants)	Day IC that Polls	. + .	0

Reset Seve

Step 5. Configure vEdge:

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

Step 6. Verification. Login to vEdge and ensure netadmin group assigned to remote user:

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

Related Information

- Cisco ISE Device Administration Prescriptive Deployment Guide: <u>https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973</u>
- Configuring User Access and Authentication: <u>https://sdwan-</u> docs.cisco.com/Product Documentation/Software Features/Release 18.4/02System and Interfaces/03C