在FMC上配置RAVPN证书身份验证和ISE授权

目录

<u>简介</u>

<u>先决条件</u>

<u>要求</u>

<u>使用的组件</u>

<u>配置</u>

```
<u>第1步:安装受信任CA证书</u>
<u>第2步:配置ISE/Radius服务器组和连接配置文件</u>
<u>第3步:配置ISE</u>
<u>第3.1步:创建用户、组和证书身份验证配置文件</u>
<u>第3.2步:配置身份验证策略</u>
<u>第3.3步:配置授权策略</u>
```

<u>验证</u>

<u>故障排除</u>

简介

本文档介绍如何为FMC上的CSF管理的RAVPN连接中的证书身份验证配置ISE服务器授权策略。

先决条件

要求

Cisco 建议您了解以下主题:

- 思科安全防火墙(CSF)
- 思科安全防火墙管理中心(FMC)
- 思科身份服务引擎(ISE)
- 证书注册和SSL基础知识。
- 证书颁发机构 (CA)

使用的组件

本文档的内容基于这些软件和硬件版本。

- 思科安全客户端5.1.6版
- 思科安全防火墙版本7.2.8
- 思科安全防火墙管理中心版本7.2.8

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

第1步:安装受信任CA证书



注意:如果CA证书与用于服务器身份验证的证书不同,则需要执行此步骤。如果同一CA服 务器颁发用户证书,则无需再次导入同一CA证书。

Firewall Management Center Devices / Certificates	Overview	Analysis	Policies	Devices	Objects	Integration
Name	Domain	Enro	ollment Type	Status		
V 🚥 FTD1						
cisco.com	Global	PKC	S12 file	CA CA	ID Se	erver Certificate
InternalCAServer	Global	Man	ual (CA Only)	CA 6	D ID Inte	ernal CA certificate

a.导航至Devices > Certificates并单击Add。

b.输入trustpoint name并在CA信息下选择Manual作为登记类型。

c.检查CA Only并粘贴以pem格式表示的受信任/内部CA证书。

d.选中Skip Check for CA flag in basic constraints of the CA Certificate并单击Save。

Add Cert Enrollmer	ıt			?
Name*				
InternalCAServer				
Description				
CA Information Co	ertificate Parameters	Key Re	evocation	
Enrollment Type:	Manual CA Only Check this option if you from this CA	▼ do not requir	re an identity certificate to be crea	əted
CA Certificate:	BEGIN CERTIFIC MIB/ zCCAWigAwlBAglBAT G9w0BAQsFADATMR QQDEwhDQVNI cnZlcjAeFw0yNDEwM MDBaFw0yNTExMjAxM aMBMxETAPBgNVBAM CENBU2VydmVyMIGfM GSIb3DQEBAQUAA4G	ATE ANBgkqhki EwDwYDV TcxMDU5 MDU5MDB MT MA0GCSq MA0GCSq MADCBiQ		
Validation Usage:	✓ IPsec Client ✓ SS ✓ Skip Check for CA f	L Client	SSL Server constraints of the CA Certificate	
			Cancel	ave

e.在Cert Enrollment下,从刚创建的下拉菜单中选择trustpoint,然后单击Add。

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

2

Device*:					
FTD1		•			
Cert Enrollment*: InternalCAServer		•	+		
Cert Enrollment Deta	ils:				
Name: Enrollment Type: Enrollment URL:	InternalCAServer Manual (CA Only) N/A				
				Cancel	\dd

第2步:配置ISE/Radius服务器组和连接配置文件

a.导航到Objects > AAA Server > RADIUS Server Group并单击Add RADIUS Server Group。选中Enable authorize only选项。



警告:如果未选中"仅启用授权"选项,则防火墙会发送身份验证请求。但是,ISE会随该请 求接收用户名和密码,并且证书中未使用密码。因此,ISE将请求标记为身份验证失败。

Edit RADIUS Server Group

Name:*	
ISE_Authorization	
Description:	
Group Accounting M	Mode:
Single	•
Retry Interval:*	(1-10) Seconds
10	
Realms:	
	•
Enable authorize	e only
Enable interim a	account update
Interval:*	(1-120) hours
24	
Enable dynamic	authorization
Port:*	(1024-65535)

b.点击Add (+)图标,然后使用IP地址或主机名添加Radius server/ISE server。

	_		
- 4	9	ι.	
	ы		
	v		

Edit RADIUS Server

IP Address/Hostname:*

ISELocal

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:*	(1-65535)	
1812		
Key:*		
••••		
Confirm Key:*		
••••		
Accounting Port:	<mark>(</mark> 1-65535)	
1813		
Timeout: (1-30	00) Seconds	
10]	
Connect using:		
Routing	erface 🕕	
Default: Management/D	iagnostic 🖌 🕂	
Redirect ACL:		
	× +	
		Cancel Save

C.导航至Devices > Remote Access configuration。创建new connection profile,并将身份验证方法设置为Client Certificate Only。对于授权服务器,选择之前步骤中创建的授权服务器。

确保您选中Allow connection only if user exists in authorization database选项。此设置可确保只有在授权允许的情

况下才能完成与RAVPN的连接。

Edit	Connec	tion	Profile

Connection Profile:* FTD_CertAuth
Group Policy:* DfltGrpPolicy
Edit Group Policy
Client Address Assignment AAA Aliases
Authentication
Authoritiestics Mathedu Client Cartificate Only
Authentication Method:
Enable multiple certificate authentication
 Map username from client certificate
Map specific field
Primary Field: Secondary Field:
CN (Common Name)
 Use entire DN (Distinguished Name) as username
Authorization
Authorization Server: ISE_Authorization (RADIUS)
Allow connection only if user exists in authorization database
Accounting
Cancel Save

0

来自客户端证书的Map Username是指从证书获取的信息以识别用户。在本例中,您将保留默认配置,但可根据用于识别用户的信息进行更改。

单击。Save

d.导航至Advanced > Group Policies。单击右侧的Add (+)图标。

Firewall Managemen	nt Center Overview	Analysis F	Policies Device	es Objects	Integration		Deploy	۹	\$ \$	🕜 admin 🕶 🖞	SECURE
FTD_PolicyVPN											Cancel
Enter Description											_
										Policy As:	signments (1)
							Local Realm: No	ne		Dynamic Access	Policy: None
Connection Profile Access Inte	arfaces Advanced										
AnyConnect Client Images	Group Policies										
Address Assignment Policy	Group policy can be assigned to	o VPN user through co	connection profile or t	y RADIUS server d	uring authentication.						
Certificate Maps	Following are the group policies	that are associated v	with this Remote Acc	ess VPN configurat	ion. Add a group poli	cy if it is required to be assigned by RADIUS server during	authentication.				
Group Policies											+
LDAP Attribute Mapping	Name		Protocol			DNS Servers	VPN Filter				
Load Balancing	DfltGrpPolicy		SSL,IKEV2								/
√ IPsec	Marketing Group		SSL IKEV2								1 =
Crypto Maps	manually_croop		000,000 2								
INE POlicy	IT_Group		SSL,IKEV2								1
IPSEC/IKEV2 Parameters											

e.创建group policies。根据组织组和每个组可以访问的网络,配置每个组策略。

Group Policy			0
Available Group Policy C + Q Search DfltGrpPolicy FTD1_GPCertAuth FTD1_GPISE FTD1_GPLocalFull	Add	Selected Group Policy DfltGrpPolicy	
		Cancel	ОК

f.在组策略上,执行特定于每个组的配置。可以添加标语消息以在连接成功后显示。

Add Group Policy

Name:*	
IT_Group	
Description:	
General AnyCon	nect Advanced
VPN Protocols	Banner:
IP Address Pools	Maximum total size: 3999, Maximum characters in a line : 497. In case of a line spanning more than 497 characters, split the line into multiple lines.
Banner	** Only plain text is supported (symbols '<' and '>' are not allowed)
DNS/WINS	IT Group
Split Tunneling	
	1
	Cancel

2

g.选择左侧的group policies命令,然后单击Add将其移到右侧。此关键字指定配置中使用的组策略。

Group Policy



0

e.部署更改。

第3步:配置ISE

第3.1步:创建用户、组和证书身份验证配置文件

a.登录到ISE服务器并导航至Administration > Network Resources > Network Devices。

Cisco ISE	Q What page are you looking							
Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers			
Recent Pages	System Deployment		Network Resource	:es	pxGrid Services			
Users Policy Sets External Identity Sources	Licensing Certificates Logging		Network Device Network Device External RADIU	e Groups e Profiles S Servers	Client Management Diagnostics Settings			
Authorization Profiles	Maintenance Upgrade Health Checks		RADIUS Server NAC Managers External MDM	Sequences	Feed Service			
	Backup & Restore Admin Access Settings		Location Servic	nagement	Profiler Threat Centric NAC			
	Identity Management				Third Party Vendors			
	Identities Groups External Identity Sources Identity Source Sequences		Certificate Prov Client Provision Mobile Device My Devices	risioning hing Management				
Shortcuts Ctril + [/] - Expand menu esc) - Collapse menu	Settings		Custom Portal Settings					
Make a wish								

b.单击Add将防火墙配置为AAA客户端。

Netv	work	Devices				
🖉 Edit	+ Add	Duplicate	ن Import 🚓 Export 🗸	A Generate PAC) Delete 🗸	
	Name	∧ IP/Mask	Profile Name	Location	Туре	Description
	FTD		🗰 Cisco 🧻	All Locations	All Device Types	

c.输入网络设备名称和IP地址字段,然后选中RADIUS Authentication Settings框并添加Shared Secret.此值必须 与在FMC上创建RADIUS服务器对象时使用的值相同。单击。Save

Network Devices List	> FTD							
Network Devices								
Name	FTD							
Description								
IP Address	✓ * IP :		/ 32	ŝ				



RADIUS Authentication Settings

RADIUS UDP Settings

Protocol	RADIUS	
Shared Secret		Show
Use Second	Shared Secret (i)	

d.导航至Administration > Identity Management > Groups。

Cisco ISE	Q What page are you looking	for?				
Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers	
Recent Pages	System		Network Resourc	es	pxGrid Services	
Live Logs Users Policy Sets External Identity Sources Certificate Provisioning	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Ascente		Network Device Network Device Network Device External RADIU: RADIUS Server NAC Managers External MDM Location Servic	rs Groups Profiles S Servers Sequences es	Summary Client Management Diagnostics Settings Feed Service Profiler	
	Settings		Device Portal Ma	nagement	Threat Centric NAC	
Shortcuts	Identity Management Identities Groups External Identity Sources Identity Source Sequences Settings		Blocked List BYOD Certificate Prov Client Provision Mobile Device M My Devices Custom Portal R	isioning ing Management Files	Third Party Vendors	
Ctrl] + (/) - Expand menu esc] - Collapse menu			Settings			6

e.单击User Identity Groups,然后单击Add。

输入group Name,然后单击_{Submit}。

< E
> 🗅 User Identity Groups Name
Group X
🗌 🍕 IT Group
C A Marketing Group

User Identity Groups > New User Identity Group

Identity Gro	pup				
* Name	IT_Group				
Description			<i>I</i> .		
				Submit	Cancel



注意:重复上述步骤可根据需要创建多个组。

d.导航至Administration > Identity Management > Identities。

Cisco ISE	Q What page are you looking	for?				
Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers	
Recent Pages	System		Network Resour	Network Resources		es
Groups Network Devices Live Logs Users Policy Sets	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore		Network Devic Network Devic Network Devic External RADIU RADIUS Server NAC Managers External MDM Location Servic	es e Groups e Profiles IS Servers Sequences ces	Summary Client Mana Diagnostics Settings Feed Service Profiler	
	Admin Access Settings		Device Portal Ma	Device Portal Management		c NAC
Shortcuts	Identity Management Identities Groups External Identity Sources Identity Source Sequences Settings		Blocked List BYOD Certificate Pro Client Provision Mobile Device My Devices Custom Portal	visioning Ning Management Files	Third Party	
Ctrl + [/] - Expand menu esc - Collapse menu			Settings			

e.单击Add以便在服务器本地数据库中创建新用户。

输入Username和Login Password。然后,导航到此页末尾,选择User Group。

单击。Save

Network Access Users

0 Edit	$+ \operatorname{Add}$	🛞 Change Status 🗸 🕁 Import 🔥 Export 🗸 🍵 D	elete 🗸 📋 Duplicate	
	Status	Username \wedge Description First Nam	e Last Name Email Address	User Identity Grou Admin
	Enabled	9_ user1		IT Group
	Enabled	9 user2		Marketing Group

✓ Network Access User

* Username user1		
Status Enabled V		
Email		
✓ Passwords		
Password Type: Internal Users 🗸		
Password	Re-Enter Password	
* Login Password	••••••	Generate Password (i)
Enable Password		Generate Password (i)
v User Groups		



注意:必须配置用户名和密码才能创建内部用户。即使在使用证书执行的RAVPN身份验证 中不需要此功能,这些用户也可以用于不需要密码的其他内部服务。因此,请确保使用强 密码。

f.导航至Administration > Identity Management > External Identify Sources。



g.单击Add创建Certificate Authentication Profile。

Certificate Authentication Profile指定如何验证客户端证书,包括可以检查证书中的哪些字段 (Subject Alternative Name、Common Name等)。

External Identity Sources	Cert	ificate Authe	ntication	Profile
> 🗅 Certificate Authentication Profile	0 Edit	+ Add Duplicate	Delete	
Active Directory	-			
LDAP	0	Name	^	Description
C ODBC		Certificate_Profile		Certificate Authorization Profile.
RADIUS Token				
🗎 RSA SecurID				
SAML Id Providers				
Social Login				

Certificate Authentication Profiles List > Certificate_Profile

Certificate Authentication Profile

* Name	Certificate_Profile
Description	Certificate Authorization Profile.
Identity Store	[not applicable] V
Use Identity From	Certificate Attribute Subject - Common Name () Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only) ()
Match Client Certificate Against Certificate In Identity Store ①	Never Only to resolve identity ambiguity Always perform binary comparison

第3.2步:配置身份验证策略

身份验证策略用于验证请求是否来自防火墙和特定连接配置文件。

a.导航至Policy > Policy Sets。

8	Cisco ISE	Q What page are you looking					
	Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers	
	Recent Pages	Policy Sets		Profiling			
	Settings Identity Source Sequences	Posture		Client Provisioning			
	Policy Sets Authorization Profiles	Policy Elements					
		Dictionaries Conditions					
		Results					
	Shortcuts						
	Ctrl] + [/] - Expand menu						
	esc - Collapse menu						

通过点击屏幕右侧的箭头选择默认授权策略:

Policy Sets						Reset	Reset Policyse	rt Hitcou	nts	Save
÷	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Se	rver Sequence	Hits	Actions	View
0) Search									
					+					
	0	Default	Default policy set			Default Network Acce	ss 🖾 🖂 +	23	ŵ	•
								Reset		Save

b.点击Authentication Policy旁边的下拉菜单箭头将其展开。然后,点击add (+)图标添加新规则。

✓ Authentication Policy (2)			
+ Status Rule Name	Conditions	Use Hits Ar	ctions
Q Search			

输入规则的名称,然后选择条件列下的add (+)图标。

\sim Aut	henticatio	on Policy (2)					
٢	Status	Rule Name	Conditions		Use	Hits	Actions
0) Searc	h					
I	0	RAVPN_CertUsers		+	Internal Users () > Options		¢

c.单击属性编辑器文本框并单击NAS-IP-Address图标。输入防火墙的IP地址。

Conditions Studio						() ×
Library		Editor				_
Search by Name	L O & 4	Click to add a Select attribute for conc	n attribute			×
Catalyst_Switch_Local_Web_Aut	t 🕕		e de la	© 1	ی ا ©	<u></u>
EAP-MSCHAPv2	0	Dictionary	Attribute	ID	Info	
EAP-TLS	0	All Dictionaries ~	nas	× ID	0	*
# MAC_in_SAN	0	V Raulus	NAO-IF*Address	*	U	

d.单击New然后添加另一个属性Tunnel-Group-name。输入在FMC上配置的名称Connection Profile。

Conditions Studio

Conditions Studio

Library

Editor Search by Name Radius-NAS-IP-Address ♥ ☶ □ ▲ ⊕ 〒 〒 〒 〒 〒 〒 ● ▲ ● ≿ 奈 0 Equals 🗸 Catalyst_Switch_Local_Web_Aut hentication Click to add an attribute A... EAP-MSCHAPv2 Select attribute for condition 🗄 \Xi EAP-TLS 0 0 -8 Ę. F . P E MAC_in_SAN Dictionary Attribute : Switch_Local_Web_Authenticatio All Dictionaries 🗸 tunnel-group-name Cisco-VPN3000 CVPN3000/ASA/PIX7x-Tunnel-Group-Name ь E Switch_Web_Authentication

Library		Editor					
Search by Name	<i>f</i> r-	ę	Radius-NAS-IP-Address	××			
Catalyst_Switch_Local_Web_Aut hentication			Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Na	۲			
EAP-MSCHAPv2	A ~	Ŀ	Equals V FTDLCertAuth				
EAP-TLS							
E MAC_in_SAN		+	NEW AND OR				
Switch_Local_Web_Authenticatio		Set to 'Is	not' Duplicate	Save			

e.在"使用"列下,选择创建的Certificate Authentication Profile。通过执行此操作,可以指定配置文件中定义 用于识别用户的信息。

✓ Authenticati	Authentication Policy (2)								
+ Status	Rule Name	Con	nditions	Use	Hits	Actions			
Q Searc	h								
0	RAVPN-Certilizera	11	VerifyCertAuth	Certificate_Profile 🛛 🗸 🖂	7	ŵ			

单击。Save

第3.3步:配置授权策略

0 ×

 \otimes^{\otimes}

8

×

<u></u>

Info

0

1 C

×

ID

146

a.点击Authorization Policy旁边的下拉菜单箭头将其展开。然后,点击add (+)图标添加新规则。

∨ Authorization Policy (13)					
		Results			
(+) Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					

输入规则的名称,然后选择条件列下的add (+)图标。

V Authorization Policy (13)						
			Results			
🕂 Status Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
Q Search						
IT_Group_Policy		+	Select from list \sim +	Select from list \vee +		¢3

b.单击属性编辑器文本框并单击Identity group图标。选择Identity group - Name属性。

Conditions Studio						
Library	Editor					
Search by Name		∃ IT_Group			\otimes^{\otimes}	
		InternalUser-IdentityG	ìroup		\otimes	
BYOD_is_Registered		e.			-	
Catalyst_Switch_Local_Web_Aut hentication	A 🗸	Select attribute for condition Image: Select attribute for condition Image: Select attribute for condition	on 및 중 図 2 1	@ 1 Ø	× چ	
Compliance_Unknown_Devices		Dictionary	Attribute	ID Info		
: F Compliant_Devices		All Dictionaries 🗡	Attribute	ID		
		A CWA	CWA_ExternalGroups	0		
		A IdentityGroup	Description	0	_	
EAP-TLS		aldentityGroup	Name	0		
: E Guest_Flow		a InternalUser	IdentityGroup	0		
: E IT_Group		2. PassiveID	PassiveID_Groups	0		

选择Equals作为运算符,然后单击下拉菜单箭头以显示可用选项并选择User Identity Groups:

o

Conditions Studio

Library		Editor					
Search by Name			E IT_Gr	roup			××
	🛛 k 😤			InternalUs	er∙ldenti	ityGroup	\otimes
BYOD_is_Registered	0		ß	Equals	~	Choose from list or type	
Catalyst_Switch_Local_Web_Aut	b_Aut ()	<u>A</u> ~				User Identity Groups:GuestType_SocialLogin (default)
				User l		User Identity Groups:GuestType_Weekly (defa	ult)
Compliance_Unknown_Devices	0		+			User Identity Groups:IT Group	
E Compliant_Devices	0	User Identity Groups:		User Identity Groups:Marketing Group			
EAP-MSCHAPv2	0					User Identity Groups:OWN_ACCOUNTS (defau	ilt)

c.在配置文件列中,点击add (+)图标并选择Create a New Authorization Profile。

V Authorization Policy (13)								
					Results			
۲	Status	Rule Name	Cond	ions	Profiles	Security Groups	Hits	Actions
0	Cearch	1						
I	0	IT_Group_Policy	AND	IT_Group R InternalUser-IdentityGroup EQUALS User IdentityGroup	Select from list	Select from list V +		ŝ
	0	Wireless Black List Default	AND	Wireless_Access IdentityGroup-Name EQUALS Endpoint Ident	Create a New Authori Diackilore_wireress_	Zelect from list	0	ŝ

输入profile Name。

Authorization Profile

* Name	IT_Group_Profile
Description	
* Access Type	ACCESS_ACCEPT ~
Network Device Profile	dette Cisco ∨⊕
Service Template	
Track Movement	
Agentless Posture	
Passive Identity Tracking	

0 ×

导航到Common Tasks并选中ASA VPN。	然后	, 键入group policy name	,它需要与FMC上创建的相同。
----------------------------	----	-----------------------	-----------------

\sim Common Tasks		
🗹 ASA VPN	IT_Group	~
AVC Profile Name		
UDN Lookup		

下一个属性已分配给每个组:

Attributes Details Access Type = ACCESS_ACCEPT Class = IT_Group

Click Save.



注意:重复第3.3步:为创建的每个组配置授权策略。

验证

1. 运行命令show vpn-sessiondb anyconnect并验证用户是否使用正确的组策略。

<#root>

firepower#

show vpn-sessiondb anyconnect

Session Type : AnyConnect

Username : user1

Index : 64 Assigned IP : 192.168.55.2 Public IP : Protocol : AnyConnect-Parent License : AnyConnect Premium : AnyConnect-Parent: (1)none Encryption : AnyConnect-Parent: (1)none Hashing Bytes Tx : 15084 : 99611 Bytes Rx Group Policy : IT_Group Tunnel Group : FTD_CertAuth : 22:21:43 UTC Tue Oct 22 2024 Login Time Duration : 3h:03m:50s : 0h:41m:44s Inactivity VLAN Mapping : N/A VLAN : none Audt Sess ID : 96130a0f0004000067182577 Security Grp : none Tunnel Zone : 0 : User2 Username : 70 Index Assigned IP Public IP : 192.168.55.3 : Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Hashing : 15112 Bytes Tx Bytes Rx : 19738 Group Policy : Marketing_Group Tunnel Group : FTD_CertAuth Login Time : 01:23:08 UTC Wed Oct 23 2024 Duration : 0h:02m:25s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 96130a0f0004600067184ffc Tunnel Zone : 0 Security Grp : none

firepower#

在组策略中,可以配置在用户成功连接时显示的标语消息。每个标语都可用于标识拥有授权的组。

Cisco AnyConnect		
Accept Disconnect		
	Sisco AnyConnect Secure Mobility Client	- <u> </u>
	VPN: Please respond to banner. FTD1_CertAuth	Connect
	¢ ()	altalta cisco

Cisco AnyConnect		
Marketing Group		
	Sisco AnyConnect Secure Mobility Client 📃	×
	VPN: Please respond to banner.	ect
	\$ (i)	uluulu cisco

3. 在实时日志中,验证连接是否使用适当的授权策略。单击Details并显示身份验证报告。

E Cisco ISE		Operations - RADIUS						
Live Logs Live Sessions								
Misconfigured Supplicants 🕕	Misconfigured Network Device	s ()	RADIUS Drops 🕕	Client Sto	pped Responding 🕕	Repeat Counter 🕕		
0	0		0		0	0		
Ø Refresh 5 Reset Repeat Counts d	jExport To ∽				Refresh Show Latest	100 rec↓ Last 30 minu↓ V Filter ↓ @		
Time Statu:	Details Repea Identity	Endpoint ID E	Endpoint Authenti	Authoriz Authoriz	IP Address Network De	Device Port Identity G		
Oct 25, 2024 08:38:03.6	0 user1	v	Windows1 Default	Default >> IT_Group				
Oct 25, 2024 08:38:03.6	user1	N.	Windows1 Default	Default >> IT_Group	FTD	User Identity		
Last Updated: Fri Oct 25 2024 14:42	41 GMT-0600 (GMT-06:00)					Records Shown: 2		

Last Updated: Fri Oct 25 2024 14:42:41 GMT-0600 (GMT-06:00)

故障排除

本部分提供了可用于对配置进行故障排除的信息。

1. 可以从CSF的诊断CLI运行调试以进行证书身份验证。

debug crypto ca 14 debug webvpn anyconnect 255 debug crypto ike-common 255

2. 使用AAA调试验证本地和/或远程属性的分配。

debug aaa common 255 debug aaa shim 255 debug aaa authentication debug aaa authorization debug radius all

在ISE上:

1. 定位至Operations > RADIUS > Live Logs。

8	Cisco ISE	Q What page are you looking					
	Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers	
	Recent Pages Policy Sets Authorization Profiles Results External Identity Sources Groups	RADIUS Live Logs Live Sessions TACACS		Threat-Centric NAM Troubleshoot Diagnostic Tools Download Logs Debug Wizard	C Live Logs		
		Adaptive Network Control Policy List Endpoint Assignment		Reports			
	Shortcuts Ctrl + [] - Expand menu esc) - Collapse menu					G	3

Live Logs Live Sessions

Misconfigured Supplicants ①	Misconfigured N	letwork Devices 🕕		RADIUS Dro	ps 🕕		Client Stop	ped Respond	ing 🕕		Rej	oeat Counter 🕕
0		0		0				3				0
Ø Refresh 🕁 Reset Repeat Counts එ Export	To 🗸							Refresh Never	~	Show Latest 20	recov L	thin ast 3 hours ↓ ∑ Filter ↓ @
Time Status	Details Repea	Identity	Endpoint ID	Endpoint	Authenti	Authoriz	Authoriz	IP Address	Ne	etwork De	Device Por	t Identity G
×	~	Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	~ N	etwork Device	Device Port	Identity Gro
Oct 23, 2024 01:26:29.3	0	User2		Windows1	Default	Default >>	Marketing		FT	D		User Identity
Oct 23, 2024 01:22:29.3 0	0	User2					DenyAccess		FT	D		User Identity
Oct 23, 2024 01:21:46.9 0	i a	User2					DenyAccess		FT	D		User Identity
Oct 23, 2024 01:16:33.4 0	9	User2					DenyAccess		FT	D		User Identity
Oct 22, 2024 10:25:14.1	0	user1		Windows1	Default	Default >>	IT_Group		FT	D		User Identit
Oct 22, 2024 10:24:18.9	à	user1		Windows1	Default	Default >>	IT_Group		FT	D		User Identit

Last Updated: Wed Oct 23 2024 12:33:54 GMT-0600 (GMT-06:00)

Records Shown: 6

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)。