# 使用ISE 3.3配置Linux VPN终端安全评估

目录

先决条件
使用的组件
<u>网络图</u>
<u>FMC/FTD上的配置</u>
<u>ISE上的配置</u>
<u>Ubuntu上的配置</u>
<u>验证</u>
<u>故障排除</u>
<u>相关信息</u>

# 简介

本文档介绍如何使用身份服务引擎(ISE)和Firepower威胁防御(FTD)配置Linux VPN状态。

先决条件

# 要求

Cisco 建议您了解以下主题:

- 思科安全客户端
- 基于Firepower威胁防御(FTD)的远程访问VPN
- 身份服务引擎 (ISE)

# 使用的组件

本文档中的信息基于以下软件版本:

- Ubuntu 22.04
- 思科安全客户端5.1.3.62
- 思科Firepower威胁防御(FTD) 7.4.1
- 思科Firepower管理中心(FMC) 7.4.1
- 思科身份服务引擎(ISE) 3.3

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

# 网络图



拓扑

# FMC/FTD上的配置

步骤1:客户端、FTD、FMC和ISE之间的连接已成功配置。因为enroll.cisco.com用于执行重定向探 测的终端(有关详细信息,请参阅终端安全评估流量CCO 文档<u>ISE终端安全评估样式比较以前版本和</u> <u>之后2.2</u>)。确保正确配置了FTD上通往enroll.cisco.com的流量的路由。

第二步:从<u>Cisco软件下载</u>下载软件包名称cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg,通过确认下载文件的 md5校验和与Cisco软件下载页相同,确保文件在下载后一切正常。

第三步: 导航到Objects > Object Management > VPN > Secure Client File。单击Add Secure Client File、提供名称、浏览File Name以选择cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg、在File Type下拉列表中选择Secure Client Image。??然后单击.Save

Firewall Managemer Objects / Object Managemer	nt Center Overview Analysis Polici	as Devices Objects Integration		Deploy	Q 🗳 🌣 🕢 admin ~	ence SECURE
> Distinguished Name DNS Server Group	Secure Client File			Add Secure	Client File Q. Filter	
> External Attributes	File objects represent files used for remote access	/PN policy configurations. They can contain Secure Client profile and image files.				
File List FilexConfig Geolocation		Add Secure Client File	0			
Interface Key Chain Network	Name Client_image	Name:*		n-5.1.3.62-webdeploy-k9.pkg	Type Secure Client Image	1/1
> PKI Policy List	hostscan5_1_3_62	linux_5_1_3_62			HostScan Package	191
Port	linux_image	File Name:*		ux64-5.1.3.62-webdeploy-k9.pkg	Secure Client Image	1/1
Protection     Route Map     Security Intelligence     Sinkhole     SLA Monitor     Time Range     Time Zone     Tunnel Zone     URL     Variable Set     VLAN Tao		cisco-secure-client-linux64-5.1.3.62-wi     Browner       File Type:*     Secure Client Image       Description:	owse			
VLPN rag VIPN Certificate Map Custom Attribute Group Policy IKEV1 Policy IKEV2 Policy IKEV2 Policy Socce Clart Customization		Cano	Save			
Secure Client File				Displa	iying 1 - 4 of 4 rows IC C Page 1	of 1 >> I C

FMC\_Upload\_Secure\_Client\_Image

# 第四步: 导航到Objects > Object Management > Network。

# 步骤 4.1为DNS服务器创建对象。单击Add Object,提供名称和可用的DNS IP地址。单击。Save

Firewall Management Objects / Object Management	Center Overview Analysis Policies	Devices Objects Integration		Deploy	२. 💕 🌣 😰 admin 🗸 👘 darda	SECURE
<ul> <li>Distinguished Name</li> <li>DNS Server Group</li> <li>External Attributes</li> <li>File List</li> </ul>	Network A network object represents one or more IP addresses	. Network objects are used in various places, including acces	is control policies, network variables, intrusion rul	Add Network Add Obj es, identity rules, network discovery rule Import Add Gro	C. Filter     C. Filter     Show Unused Objects     orts, and so on.	
> FlexConfig Geolocation	Name			Value	Type Override	
Interface	any	New Network Object	0	0.0.0.0/0 ::/0	Group 🖬 Q i	8 M
Key Chain Network	any-ipv4	Norma		0.0.0/0	Network 🖪 Q	8 B
		DNS Description Network Host Range Network Allow Overrides	O FQDN			
			Cancel			

FMC\_Add\_Object\_DNS



**注意**:此处配置的DNS服务器将用于VPN用户。

步骤 4.2为ISE PSN创建对象。单击Add Object,提供名称和可用的ISE PSN IP地址。单击。Save

Firewall Managemen Objects / Object Management	t Center Overview Analysis Polici	es Devices Objects Integration		Deploy	Q 💕 🌣 🕢 admin 🗸 👶 SECUR
Distinguished Name     DNS Server Group     External Attributes     File List	Network A network object represents one or more IP address	ves. Network objects are used in various places, including acce	ss control policies, network variables, intrusi	Add Network Add Con rules, identity rules, network discovery rule Impor Add C	Q. Filter      Diject     Officer      Officer      Officer      orts, and so on.      Sroup
<ul> <li>FlexConfig</li> <li>Geolocation</li> <li>Interface</li> </ul>	Nome	New Network Object	0	Value 0.0.0,0/0 -/0	Type Override Group Page 8
Key Chain Network	any-ipv4	Name		0.0.0.0/0	Network 월 Q 🗑 😣
Network		ISE_PSN_ Description Network Host Range Network Allow Overrides	FQDN		
			Cancel Save		

# FMC\_Add\_Object\_ISE

第五步:导航到Objects > Object Management > VPN > Group Policy。单击。Add Group Policy单击DNS/WINS,然后在Primary DNS Server中选择DNS服务器的对象。??然后单击.Save

Firewall Managemen Objects / Object Management	t Center Overview Ana	lysis Policies D	Devices Objects	Integration		Deploy	Q 💕 🌣 🛛	admîn v	cisco SECURE
Distinguished Name     DNS Server Group     External Attributes     File List	Group Policy A Group Policy is a set of attribute a	nd value pairs, stored in a	a group policy object, that	t define the remote access VPN experience.T	he RADIUS authorization server assigns	Add Gro the group policy or it is obtained from the c	up Policy Q, Filter		
> FlexConfig Geolocation	Name		Add Group Police						45
Key Chain Network > PKI Poirt Port Port > Security Intelligence Sinkhole SLA Monitor Time Zone Tunnel Zone Tunnel Zone URL Variable Set VLAN Tag > VPN Certificate Map Custom Attribute Group Policy			Name:* posture_gp Description: General Secur VPN Protocols IP Address Pools Banner DNS/WINS Split Tunneling		+ + + + + +				71
IKEv1 IPsec Proposal IKEv1 Policy IKEv2 IPsec Proposal IKEv2 Policy Secure Client Customizatio Secure Client File					Cancel	Displa	ying 1 - 2 of 2 rows IC <	Page 1	of 1 > >1 C

FMC\_Add\_Group\_Policy



注意:确保VPN组策略中使用的DNS服务器可以解析ISE客户端调配门户FQDN和enroll.cisco.com。

第六步: 导航到Objects > Object Management > Access List > Extended。单击。Add Extended Access List

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🕲 admin 🗸 🕬 SECURE
<ul> <li>AAA Server</li> <li>RADIUS Server Group</li> </ul>	Extended	Add Extended Access List Q, Filter
Single Sign-on Server	An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-identifies traffic based on destination address only. Identifies traffic ba addresses. You use these objects when configuring particular features, such as route maps.	ased on source and destination address and ports. Supports IPv4 and IPv6
Extended	Name Value	Override

FMC\_Add\_Redirect\_ACL

步骤 6.1提供重定向ACL的名称。此名称必须与ISE授权配置文件中的名称相同。单击。Add

#### New Extended Access List Object

Name redirect									
Entries (0)									
									Add
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
No record	s to display								

#### Allow Overrides

 Cancel
 Save

 FMC\_Add\_Redirect\_ACL\_Part\_1
 Save

# 步骤 6.2 阻止DNS流量、发往ISE PSN IP地址的流量以及补救服务器,以将其排除在重定向范围之外。允许其余流量。这将触发重定向。单击。Save

Add Extended Access List Entry		0
Action:		
Logging:		
Default		
Log Level:		
Informational <b>v</b>		
Log Interval:		
300 Sec.		
Network Port <b>()</b> Application <b>()</b> Users <b>()</b> Security G	iroup Tag	
Available Networks C +	Source Networks (0)	Destination Networks (1)
Q Search by name or value	any	ISE_PSN
IPv4-Private-192.168.0.0-16 Add to Source	e	L
IPv4-Private-All-RFC1918 Add to Destin	ation	
IPv4-Private-All-RFC1918 Add to Destin IPv6-IPv4-Mapped	ation	
IPv4-Private-All-RFC1918 Add to Destination IPv6-IPv4-Mapped IPv6-Link-Local	ation	
IPv4-Private-All-RFC1918       Add to Destine         IPv6-IPv4-Mapped       IPv6-Link-Local         IPv6-Private-Unique-Local-Addresses       IPv6-Private-Unique-Local-Addresses	ation	
IPv4-Private-All-RFC1918 Add to Destine IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast	ation	
IPv4-Private-All-RFC1918 Add to Destine IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast ISE_PSN_	ation	
IPv4-Private-All-RFC1918 Add to Destina IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast ISE_PSN	ation Enter an IP address	Add Enter an IP address Add
IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-Link-Local IPv6-to-IPv4-Relay-Anycast ISE_PSN	Enter an IP address	Add Enter an IP address Add
IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast ISE_PSN rtp_ise	ation Enter an IP address	Add Enter an IP address Add

FMC\_Add\_Redirect\_ACL\_Part\_2

Name									
redirect									
Entries (4)									Add
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	any-ipv4	Any	ISE_PSN_	Any	Any	Any	Any	1
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	11
3	Block	Any	Any	FTP	Any	Any	Any	Any	11
4 Allow O	Allow verrides	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	/1

Cancel Save

 $FMC\_Add\_Redirect\_ACL\_Part\_3$ 



步骤 7. 导航到Objects > Object Management > RADIUS Server Group。单击。Add RADIUS Server Group

Firewall Management Objects / Object Management	Center Overvie	w Analysis	Policies	Devices	Objects	Integration		Deploy	۹	¢.
✓ AAA Server RADIUS Server Group Single Sign-on Server ✓ Access List	RADIUS Server	e <b>r Group</b>	or more refere	nces to RADI	IUS Servers. T	hese AAA servers are used to authenticate users logging in through Remote Access VPN conn	ections.	Add RADIUS Se	rver Gro	up
Extended	Name						Value			

 $FMC\_Add\_New\_Radius\_Server\_Group$ 

步骤 7.1提供名称、检查Enable authorize only、检查Enable interim account update、检查Enable dynamic authorization。

Add RADIUS Server Group	0
Name:*	I
rtpise	
Description:	
Group Accounting Mode:	
Single	
Retry Interval:* (1-10) Seconds	
10	
Realms:	
▼	
Enable authorize only	
Enable interim account update	
Interval:* (1-120) hours	
24	
Enable dynamic authorization	
Port:* (1024-65535)	

Cancel

# 步骤 7.2单击Plus 图标添加新的radius服务器。提供ISE PSNIP Address/Hostname, Key。选择specific interface进行连接。选择Redirect ACL。然后,单击Save保存新的radius服务器。然后,再次单击Save,保存新的RADIUS服务器组。

Add RADIUS Server Group	0	New RADIUS Server	0
<ul> <li>Enable authorize only</li> <li>Enable interim account update</li> <li>Interval:* (1-120) hours</li> <li>24</li> <li>Enable dynamic authorization</li> <li>Port:* (1024-65535)</li> <li>1700</li> </ul>		IP Address/Hostname:* Configure DNS at Threat Defense Platform Settings to resolve hostnam Authentication Port:* (1-65535) 1812 Kev:* Confirm Key:*	ne
Merge Downloadable ACL with Cisco AV Pair ACL     After Cisco AV Pair ACL     Before Cisco AV Pair ACL     RADIUS Servers (Maximum 16 servers)		Accounting Port: (1-65535)  1813  Timeout: (1-300) Seconds  10	
IP Address/Hostname No records to display-		Connect using: Routing Specific Interface + Inside_zone + Redirect ACL: redirect +	
C	ancel	Cance	Save

FMC\_Add\_New\_Radius\_Server\_Group\_Part\_2

步骤 8 导航到Objects > Object Management > Address Pools > IPv4 Pools。单击Add IPv4 Pools并提供Name, IPv4 Address Range和 Mask。??然后单击.Save

Firewall Managem Objects / Object Managem	ent Center Overview Analysis Policies Devices	Disjects Integration		Deploy Q 💕	tangni v	ence SECURE
> AAA Server > Access List > Address Pools	IPv4 Pools	ustic interface with clustering, or for VPN remote access profiles.		Add IPv4 Pools	Q, Filter	
Pv4 Pools Pv6 Pools Application Fitters AS Path BFD Template Cipher Suite List Community List DHCP IPv6 Pool DIstinguished Name DNS Server Group External Attributes File List File List File List File List File List Pelicy List Pools List Route Map Security Intelligence Sinkhole SLA Monitor Time Range Time Zone	Name al postura_pood_97_0	Add IPv4 Pool          Name*         posture_pool         Description         IPv4 Address Range*         192.168.6.30-192.168.6.100         Format: Ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150         Mask*         255.255.255.0         I Allow Overrides         Onfigure device overrides in the address pool object to swald IP address conflicts in case of object is shared across multiple devices.         I Override (0)	Save		Override ©	/1
Tunnel Zone URL Variable Set				Displaying 1 - 2 of 2	rows IC C Page 1	of 1 > > C

FMC\_Add\_Newpool

Enrollment Type中选择Self Signed Certificate。单击Certificate Parameters选项卡并提供Common Name和Country Code。??然后单击.Save

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices O	Integration		Deploy Q 🚱 🌣 🕢 fangni - 🖓 thefe SECUR
AAA Server     Access List     Address Pools     Anolication Ellana	Cert Enrollment A certificate enrollment object contains the Certification Authority (CA) serv your Physite Key Infrastructure (PK).	er information and enrollment parameter	s that are required for creating Certificate Signing Requests (CSRs) and obtaining Ide	Add Cert Enrollment Q. Filter
AS Path	Name			Type Override
BFD Template Cloher Suite List	Add Cert Enrollment	0	Add Cert Enrollment	● bert / ¥
Community List     DHCP IPv6 Pool	Name* demo_vpn		Namo* demo_vpn	Dent
> Distinguished Name DNS Server Group	Description		Description	
Constant Attributes File List File List File List File Config Geslocation Interface Key Chain Network File Cert Enrollment External Cert Groups Internal CA Inter	CA Information Certificate Parameters Key Revocation  Fundiment Type: Sett Signed Certificate  Common Name (CN) is mandatory for self-signed certificate that is use VPN. To configure CN, please navigate to 'Certificate Parameters' tab. Validation Usage: ♥ IPsec Client ♥ SSL Client  SSL Server	d in Remote Access	CA Information Certificate Parameters Key Revocation Include FQDN: Don't use FQDN in certificate • Include Device's IP Address: Common Name (CN): demo.example.com Organization Unit (OU): Locality (L): State (ST): County Code (C): CN Email (E): Include Device's Serial Number	
Trusted CAs Policy List	Allow Overrides		Allow Overrides	
Port Prefix List		Cancel Save		Cancel
Route Map				Displaying 1 - 3 of 3 rows: I< < Page 1 of 1 >>I C

FMC\_Add\_New\_Cert\_Enroll

步骤 10 导航到Devices > Certificates。点击Add,在Device下选择FTD名称,在Cert Enrollment下选择以前配置的注册。单击。Add

Firewall Manageme Devices / Certificates	ent Center	Verview Analysis	Policies Devices Objects	Integration			Deploy	۹ 💰	° 0	fangni $\vee$	ence SECURE
Filter											Add
All Certificates	•										
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Explry	Status						
Add New Certificate											
generate CA and id	lentify certificate	e.								<b></b>	
Device*:					O CA					± @	C 🖬
Posture-FTD-CN	L27	•									
Cost Forelly onthe											
demo und		-									
dento_von		• +									
Cert Enrollment De	tails:										
Name:	demo_vpn										
Enrollment Type:	Self-Signed										
Enrollment URL:	N/A										
			Cancel	dd							

 $FMC\_Add\_New\_Cert\_To\_FTD$ 

步骤 11 导航到Devices > VPN > Remote Access。单击。Add

步骤 11.1提供名称,并将FTD添加到Selected Devices。单击。Next

Firewall Management Center Overview	Analysis Policies Devices Objects Integration		Deploy Q 🔮 🌣 🔕 admin 🗸 🖏 SECURE
	Secure Client Access & Certificate Summary Targeted Devices and Protocols   with ward will guide you through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the required minimal steps to configure the Remote access through the result of the remote access through the result of the remote access through the rem	Before You Start     Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.     Authentication Server     Configure LOCAL or Releve or RADUS Server Group or SiD to authenticate VPN clients.     Secure Client Package     Mate sure you have Secure Client package for VPN     Circo credentials to download it during the wizard.     Device Interface     Hendraces should be already configured on targeted     devices so that they can be used as a security zone     or interface group to enable VPN access.	
			Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_1

# 步骤 11.2在Authentication Server, Authorization Server, Accounting Server中选择以前配置的radius服务器组。向下滚动页面。

Errewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 💕 🌣 🕢 admin 🗸 🖏 SECURE
Remote Access VPN Policy Wizard         ① Policy Assignment       ③ Connection Profile         ③ Secure Client       ④ Access & Certificate         ⑤ Summary	
Renote Secure Client Outside User	
Connection Profile: Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accompliabed and how addresses are assigned. They also include user attributes, which are defined in group policies. Connection Profile Name: posture_vpn	
This name is configured as a connection alias, it can be used to connect to the VPN gateway Authentication, Authorization & Accounting (AAA): Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.	
Authentication Method: AAA Oray   Authentication Server.*	
Authorization Server: Tpise	
Client Address Assignment:	Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_2

步骤 11.3在IPv4 Address Pools中选择以前配置的池名称。在Group Policy中选择以前配置的组策略。单击Next。

Firewall Management Center Overview Analysis Policies	Devices Objects Integration	Deploy Q 🚱 🌣 🕢 admin 🗸 🚮 SECURE
Remote Access VPN Policy Wizard		
1 Policy Assignment — 2 Connection Profile 3 Secure Client —	Access & Certificate 5 Summary	
	(Realm or PADBUS) Accounting Server: (RADUS) + (RADUS)	
	Client Address Assignment:	
	Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.	
	Use AAA Server (Realm or RADIUS only)	
	Use DHCP Servers	
	Vise IP Address Pools	
	IPv4 Address Pools: posture_pool	
	IPv6 Address Pools:	
	Group Policy:	
	A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.	
	Group Policy: posture_ap + Edit Group Policy	



FMC\_New\_RAVPN\_Wizard\_3

#### 步骤 11.4选中Linux映像的复选框。单击。Next

Firewall Management Center Overview Analysis Devices / VPN / Setup Wizard	Policies Devices Objects In	tegration		Deploy Q 💕	admin ~ thedex SECURE
Remote Access VPN Policy Wizard					
1 Policy Assignment 2 Connection Profile 3 Secure Cliv	ent 4 Access & Certificate _	5 Summary			
	Remote User Client	Internet	inside Corporate Resources		
			9 4		
	Secure Client Image				
	The VPN gateway can automatically de connection is initiated. Minimize connecti	ownload the latest Secure Client package to ion setup time by choosing the appropriate OS for	he client device when the VPN r the selected package.		
	Download Secure Client packages from (	Cisco Software Download Center.			
			Show Re-order buttons +		
	Secure Client File Object Name	Secure Client Package Name	Operating System		
	client_image	cisco-secure-client-win-5.1.3.62-webdeplo	Windows *		
	Inux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd	Linux		

Cancel Back Next

 $FMC\_New\_RAVPN\_Wizard\_4$ 

步骤 11.5选择VPN接口的接口。选择在第9步中在FTD上注册的证书注册。单击。Next



Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_5

#### 步骤 11.6在摘要页面上再次确认相关信息。如果一切正常,请单击Finish。如果需要修改任何内容,请单击Back。

Firewall Management Center Overview Analysis P	Policies Devices Objects	Integration		Deploy Q 🔮 🌣 🚳 admin ~ 🔤
Remote Access VPN Policy Wizard      1 Policy Assignment — 2 Connection Profile — 3 Secure Clier	nt (4) Access & Certific	ate (3) Summary		
	Rimote User Se	Cure Cient Internet	VPN Inside Compose Device Resources	
	Remote Access VPN Polic Frewall Management Center will of Rame: Device Targets: Connection Profile: Connection Alas: AAA: Authentication Method: Authentication Method: Authentication Server: Address Assignment: Address Assignment: Address Posto (IPA): Address Posto (IPA): Address Posto (IPA): Address Posto (IPA): Address Posto (IPA): Address Posto (IPA): DHOP Servers: DHOP Servers: DHOP Servers: Device Clent Images: Interface Objects: Device Clentity Certificate Enroll	y Configuration Configuration Configure an RA VPN Policy with the following settings posture.ym Posture.ym Posture.ym Posture.ym Posture.ym AAA Ony replate (PADUS) replate re	Additional Configuration Requirements Additional Configuration Requirements Additional Completes, the following configuration meets to be completed for VPN to Access Control Policy Update Access Control Policy Update Access Control not meets be defined to allow POLY to all argeted devices. A T is enabled on the targeted devices, you must define a NAT Policy weempd VPN traffic. A T is enabled on the targeted devices, you must define a NAT Policy weempd VPN traffic. A T is enabled on the targeted devices. A Configuration SSL will be enabled on port 443. Proce-KKiv2 uses port 500 and Client Services wells devided advices ports 43. for Secure Client ing devided advices ports 450. Policy on the targeted Solo. Pase ensure that these ports are not used in NAT Policy on there accelor suberior depolying the configuration.	
de de	on severe enventent ougect. dem	w <sub>w</sub> the in the gorgen of the of the range of		Cancel Back Finish

FMC\_New\_RAVPN\_Wizard\_6

步骤 12将新配置部署到FTD以完成远程访问VPN配置。

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Integration		Deploy 2, 6 to admin	n ~ cisco SECURI
posture_vpn			Q. Advanced Deploy 🔺 Ignore warnings	Deploy
			Posture-FTD-CML27 Ready for Deployment	a ents.(1)
Connection Profile Access Interfaces Advanced				ty: None
				+
Namo	AAA	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	E DftGrpPolicy		
posture_vpn	Authentization: triplee (RADIUS) Authonization: triplee (RADIUS) Accounting: triplee (RADIUS)	E posture_gp	1 selected 0 1 pending	20

FMC\_Deploy\_FTD

#### ISE上的配置

步骤 13 导航到Work Centers > Posture > Network Devices。单击。Add

=	dentity Services	Engine				Work Centers / Posture						Q	۵	<u>۱</u> ©	<b>р</b>	۹
Щ	Bookmarks	Overview	Network Device:	Client Provisioning	g Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings						
-	Dashboard		L													
1d	Context Visibility	Net	work Devic	es												
×	Operations											5	elected 0	Total 4	Ø	0
-0	Policy	/ Edit	+ Add [] Dupli	ate 🕁 Import 🛈 Exp	ort V 🖄 Generate PAC	B Delete ~								A	~	Ŷ
8.	Administration		Name $\land$ IP/M	ask Profile Name	Location	Туре		Description								
al.	Work Centers	0	FTD-CML2	Cisco 🕕	All Locations	Firewall										
-		-	FTD-CML2	Cisco ()	All Locations	Firewall										
3	Interactive Help		PID-CMLZ	Cisco ()	All Locations	Firewall										

ISE\_Add\_New\_Device

步骤 13.1提供Name, IP Address并向下滚动页面。

≡ ::	Identity Ser	vices Engine				w	ork Centers / I	Posture		
Щ	Overview No	etwork Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Network Device	s List > New Network D	evice							
14	Network D	evices								
*	Name	posture-FTD		_						
U 80	Description			_						
	IP Ar	ddress			٥					
?										
	Device Prot	ile 👬 Cisco	~	()						
	Model Nam	e	~	_						
	Software V	ersion	~	, 						
	Network De	evice Group								
	Location	All Locations		~	Set To Default					
	IPSEC	Is IPSEC Devic	e	~	Set To Default					

## ISE\_Add\_New\_Device\_1

步骤 13.2选中RADIUS Authentication Settings复选框。提供Shared Secret。单击。Submit

$\equiv \frac{1}{2000}$ Identity Services	Engine					۷	Vork Centers / P	osture			۹	0 0 0 A
JI Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings			
E. Dashboard		~ RADIUS Authent	ication Settings									
15 Context Visibility	_	RADIUS UDP Setting	5									
Operations		Protocol RAI	DIUS									
<ul> <li>Policy</li> <li>Administration</li> </ul>		Shared Secret		Show								
. Work Contern		Use Second Shared	Secret ()									
Mil Work Centers		Secret	d Shared		Show							
③ Interactive Help		CoA Port 13	700	Set To Defa	uit .							
		RADIUS DTLS Setting	ps 🕕									
		DTLS Required										
		Shared Secret rad	iws/dtls									
		CoA Port 20	083	Set To Defa	uit							
		Issuer CA of ISE Certificates for CoA S	elect if required (optional)	~ 0								
		DNS Name										
		General Settings										
		🗌 Enable KeyWrap 🕕										
		Key Encryption Key		Show								
		Message Authenticator Code		Show								
		Key Input Format ASCII O HEXA	DECIMAL									
		V TACACS Authen	tication Settings									
		<ul> <li>SNMP Settings</li> </ul>										
		<ul> <li>Advanced Trusts</li> </ul>	Sec Settings									
												1
											Submit	Cancel

ISE\_Add\_New\_Device\_2

步骤 14 从<u>Cisco软件下载</u>下载软件包名称cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg,通过确认下载文件的 md5校验和与Cisco软件下载页相同,来确保文件完好。已在步骤1中成功下载软件包名称cisco-secure-client-linux64-5.1.3.62-

步骤 15 导航到Work Cent	ers > Posture > Client Provis	sioning > Resources。单音	击。Add选择.Agent	resources from local disk
--------------------	-------------------------------	------------------------	---------------	---------------------------

≡	dude Identity Services Engine			Wo	rk Centers /	Posture			
Ц	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
== 	Client Provisioning Policy Resources Client Provisioning Portal	Resources	🚺 Duplicate 🏾 🔋 De	ieto				Selec	ited 0 Total 16 🕃
Ψ/ 8.		Agent res	ources from Cisco site		т	ype $\checkmark$	Version	Last Update	Description
-0		Agent res	ources from local disk		v	VinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Pro
-file		Native Su	oplicant Profile		٨	lative Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configurec
		Agent Co	figuration		١	lative Supplicant Pro	Not Applic	2023/07/04 07:55:16	Pre-configurec
?		Agent Por	ture Profile		Ν	MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Pro-
		AMP Enat	ler Profile	5.1.3.062	c	CiscoSecureClientDe	5.1.3.62	2024/05/08 10:20:06	Cisco Secure (
		CiscoSecur	eClientDesktopLinux 5.1	.3.062	c	CiscoSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure (
		CiscoSecur	eClientComplianceModu	leWindows 4.3.4015.819	2 0	CiscoSecureClientCo	4.3.4015	2024/05/08 10:26:57	Cisco Secure (
		CiscoSecur	ClientComplianceModu	leLinux 4.3.3139.0	c	CiscoSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure (
		CiscoAgent	essWindows 5.0.03061		c	CiscoAgentlessWind	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
		CiscoAgent	lessOSX 5.0.03061		c	CiscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
		CiscoTempo	oralAgentWindows 5.0.0	3061	c	CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
		CiscoTempo	oralAgentOSX 5.0.03061	1	c	CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

ISE\_Upload\_Resource

# 步骤 15.1选择.Cisco Provided Package点击Choose File上传cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg。单击。Submit

≡	dentity Services E	ngine	Work C	enters / Posture		Q	۵	0	Q	8
二 三 三 三 三 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	Bookmarks Dashboard Context Visibility Operations	Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Local Disk > Agent Resources From Agent Resources From Local Disk	Local Disk						
U Ao Ali	Policy Administration Work Centers		Category Cisco Provided Packa	ge 💙 🛈						
0	Interactive Help		<ul> <li>Agent Uploaded R</li> <li>Name</li> <li>CiscoSecureClientDeskte</li> <li>Submit</li> <li>Cancel</li> </ul>	PSOUICES       N     Type     Vector       pLi     CiscoSecureClientDe     5.	Description           i.1.3.62         Cisco Secure Client for Ii					

ISE\_Upload\_Resources\_1



注意:重复步骤14.上传cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg。

步骤 16 导航到Work Centers > Posture > Client Provisioning > Resources。单击。Add选择.Agent Posture Profile

= :	diale Identity Services Engine				Work Cent	ers / Posture			
щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports Settings	1	
E A	Client Provisioning Policy Resources	Resources							
×	Client Provisioning Portal							Selected 0 Total 16	S C
0		🖉 Edit 🛛 🕂 Add 🔿	Duplicate 🍵 De	elete				$_{\rm AII}\sim$	$\nabla$
		Agent res	sources from Cisco site	,	Version	Last Update	Description		
40		Agent res	sources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for Ii		
-fil		Native Su	pplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native S		
		Agent Co	nfiguration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu		
?		Agent Por	sture Profile	ntProfile	Not Applic	2024/05/08 10:37:17			
		AMP Enal	bler Profile	ntProfile	Not Applic	2024/05/16 15:15:49			

ISE\_Add\_Agent\_Posture\_Profile

步骤 16.1提供Name, Server name rules,并将剩余部分保留为默认值。单击。Save

# 名称: linux\_agent\_profile

# 服务器名称规则:\*.example.com

≡ :8	sco Identity	Services Engine			Wa	ork Centers /	Posture			
Щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
Ⅲ 	Client Provis Resources Client Provis	ioning Policy	ISE Posture Agent Profile Set Agent Posture Profil Name * linux_agent_profile Description:	e						
(?)			Agent Behavior Parameter Enable debug log		Value No V	D	escription nables the debug log	on the agent		

ISE\_Add\_Agent\_Posture\_Profile\_1

≣ :¦	see Identity	Services Engine			w	ork Centers / I	Posture		
JI.	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
10	Client Provis Resources	ioning Policy	Posture Protocol						
×	Client Provis	lioning Portal	Parameter	Value			Description		
U			PRA retransmission ti	me 120	secs		This is the age communication	nt retry period n failure	if there is a Passive Reassessment
<b>a</b> 0			Retransmission Delay	(i) <u>60</u>	secs		Time (in secon	ids) to wait bef	ore retrying.
Al.			Retransmission Limit	0 4			Number of retr	ies allowed for	a message.
?			Discovery host ()				Enter any IP ac detects and re portal.	ddress or FQDN directs that htt	I that is routed through a NAD. The NAD p traffic to the Client Provisioning
			Discovery Backup Ser	rver List Choose	e		By default, Any PSNs sequenti as the backup discovery prob	yConnect send ally if the PSN list and restric ses.	s discovery probes to all the Cisco ISE is unreachable. Choose specific PSNs t the nodes to which AnyConnect sends
			Server name rules * (	) •.exam	ple.com		A list of wildca servers that th	irded, comma- e agent can co	separated names that defines the nnect to. E.g. "*.cisco.com"
			Call Home List 🕕				A list of IP add that the agent endpoint does	iresses, that de will try to conn n't respond for	fines the all the Policy service nodes ect to if the PSN that authenticated the some reason.
			Back-off Timer ①	30	secs		Agent will cont targets and pro packets till this	tinuously try to eviously conne s max time limi	reach discovery targets (redirection cted PSNs) by sending the discovery t is reached
									Cancel Save

ISE\_Add\_Agent\_Posture\_Profile\_2

# 步骤 17 导航到Work Centers > Posture > Client Provisioning > Resources。单击。Add选择.Agent Configuration

≡ :	ster Identity	Services Engine				Work Cent	ers / Posture				
Щ	Overview	Network Devices	Client Prov	isioning Policy Elements	Posture Policy	Policy S	Sets Troubleshoo	t Reports	Settings		
15 01	Client Provis Resources	loning Policy	Resou	urces							
×	Client Provis	ioning Portal								Selected 0 Total 16	C
			🖉 Edit 🛛 -	+ Add 🔨 📋 Duplicate 🛛 📋 Do	elete					aii $\sim$	$\nabla$
U To				Agent resources from Cisco site	,	Version	Last Update	Description			
				Agent resources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client	for li		
កា				Native Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Nati	ve S		
				Agent Configuration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client	Linu		
?				Agent Posture Profile	ntProfile	Not Applic	2024/05/08 10:37:17				-
				AMP Enabler Profile	ntProfile	Not Applic	2024/05/16 15:15:49				

ISE\_Add\_Agent\_Configuration

# 步骤 17.2配置详细信息:

- 选择代理包:CiscoSecureClientDesktopLinux 5.1.3.062
- 名称: linux\_agent\_config
- 合规性模块:CiscoSecureClientComplianceModuleLinux 4.3.3139.0
- 选中复选框 VPN, Diagnostic and Reporting Tool
- 配置文件选择ISE终端安全评估:linux\_agent\_profile

#### 单击。Submit

≣ :	isco Identity	Services Engine					Work Cent	ters / Postu	re
Щ	Overview	Network Devices	<b>Client Provisioning</b>	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Client Provi	isioning Policy	* Select Agent Package:	Cit	scoSecureClientDesktopLin	nux 5.1.3.062 V	1		
15 15	Client Provi	isioning Portal	* Configuration				1		
			linux_agent_config						
20			Description:						
al.				k					
			Description Value N	otes					
•			Cisco Secure Client Cisco Secure Client ISE Posture VPN Secure Firewall Posture Network Visibility Diagnostic and Reporting Tool Profile Selection	meClientComplianceModulet	Linux 4.3.∨				
			* ISE Posture linux_ager	nt_profile	~			S	ubmit Cance

ISE\_Add\_Agent\_Configuration\_1

步骤 18. 导航到Work Centers > Posture > Client Provisioning > Client Provisioning Policy。在任何规则名称末尾点击Edit 。选择.Insert new policy below

	isco Identity	Services E	ngine									v	/ork Ce	enters / Postu	re				
н	Overview	Network [	Devices	Clien	t Provis	ioning	Policy Elemen	ts	Posture Policy	/	Policy Sets	Troub	leshoo	t Reports	Settings				
11日 1日 火 日 よ。 月1	Client Provis Resources Client Provis	ioning Policy		Clin Define For Ag For Na Intel a For W Mac A If you without	ent I e the Clie gent Con ative Sup wws Agen rchitectu indows A kRM64 po configuru at an ARM	Provision figuration: w plicant Conf it, Mac Ager ires. Mac po gent ARM6- plicies requi e an ARM64 464 conditio	ioning Policy to deter arsion of agent, as iguration: wizard p at, Mac Temporal a licies run the same p policies configue concet, configue client provisioning n. This is because	minipent profi and l a pa re S ions a po a an	cy e what users will recc profile, agent compil le and/or wizard. Dra Mac Agentless polici ckcage for both archit ession: OS-Architect a arm64 configuration licy for an OS, ensur endpoint is matched	eive up ance i g and ecture ure EC s. e that seque	pon login and use module, and/or ag drop rules to chai port ARM64. Wini 39. 2UALS arm64 in ti the ARM64 policy entially with the po	session ent cust ge the o lows pol e Other is at the licies lis	initiation omization order. licies run Conditio top of th ted in thi	1: n package. separate package ns column. he conditions list, 4 s window.	s for ARM4 and ane and				
				~															
?						Rule Name			Identity Groups		Operating Syste	ms		Other Conditions			Resul	lts	
				8		10S		Ħ	Any	and	Apple IOS All		and	Condition(s)		then	Cisco-	-ISE-NSP	Edit 😔
				8	2	Android		If	Any	and	Android		and	Condition(s)		then	Cisco-	-ISE-NSP	Editis
																	(	Duplicate above Duplicate below Insert new policy at Insert new policy be	bove

#### 步骤 18.1 配置详细信息:

#### 规则名称:Linux

操作系统:Linux All

#### 结果:linux\_agent\_config

## 单击Done 和Save。

=	dentity	Services Engine								Work	Cer	nters / Postur	e				
щ	Overview	Network Devices	Clie	nt Provisio	ning Policy Eler	nents	Posture Polic	у	Policy Sets	Troublesh	oot	Reports	Settings				
王 尽 父 む 品	Client Provis Resources Client Provis	lioning Policy	CI Defin For 1 For 1 Wind Intel For 1 Mac If yo with	ient Pi Agent Config Native Suppli dows Agent, architecture: Mindows Age ARM64 polic u configure a out an ARM6	Provisioning Policy to d uration: version of agen cant Configuration: viezi Mac Agent, Mac Tempo s. Mac policies run the int ARM64 policies, con ies require no Other CC is nARM64 deline provisi 4 condition. This is bec	Poli etermin t, agent ral and same pa figure S onditions oning po ause an	e what users will rec profile, agent comp le and/or wizard. Dri Mac Agentiess polici ckcage for both archi ession: OS-Architec a arm64 configuratio licy for an OS, ensur endpoint is matchec	eive u liance ag and ies sup tecture ture E ns. re that I sequ	pon login and use module, and/or a drop rules to cha oport ARM64. Win es. QUALS arm64 in t the ARM64 polic; entially with the p	r session initia gent customiza nge the order. dows policies i he Other Cond r is at the top o plicies listed in	tion: ation p run se litions of the this s	package. eparate packages s column. e conditions list, ah window.	for ARM4 and lead of policies				
0			-	Ri V IK V A	ule Name NS Indroid Inux	H H H	Identity Groups Any Any Any	and and and	Operating Syst Apple IOS All Android Linux All	ems an an	o nd Cr nd Cr	Other Conditions Condition(s) Condition(s)		then then then	Results Cisco-ISE-NSP Cisco-ISE-NSP linux_agent_config	6	idit ∽ idit ∽ idit ∽



=	diale Identity Services Engine	Work Centers / Posture	
н	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
8 18 *	Conditions Anti-Malware Anti-Spyware Anti-Virus	File Conditions	Selected 0 Total 385 👩 🔅
0	Application	Name Description File name Condition Type	
40 51	Dictionary Compound Dictionary Simple	pc_XP64_K82797052_M513 Cisco Predefined Check SYSTEM_PROGRAMS\C Cisco-Defined	8
	Disk Encryption External DataSource	pc_vws_k4_x0312475_xM Cisco Predefined Check SYSTEM_RUOTINyshativ Cisco-Defined     pc_Viss_k82893294_xM513 Cisco Predefined Check SYSTEM_32\/magehip.dll Cisco-Defined	
(?)	File	pc_W81_64_K8023869_M Cisco Predefined Check SYSTEM_ROOT\systaativ Cisco-Defined     pc_V8864_K8025902_M50 Cisco Predefined Check SYSTEM_ROOT\winsxa\a Cisco-Defined	
	Hardware Attributes Patch Management	pc_W10_64_1709_KB45803 Cisco Predefined Check SYSTEM_ROOT\sysnativ Cisco-Defined	
	Registry Script	pc_VP_K02653956_MS12-0 Clsco Predefined Check SYSTEM_32\Wintrust.dll Clsco-Defined     pc_W0_K02092074_MS13 Clsco Predefined Check SYSTEM_32\Scrun.dll Clsco-Defined	
	Service US8	pc_W10_64_1999_KB50139 Clisco Predefined Check SYSTEM_ROOT\SystWO Clisco-Defined	
	Remediations >	pc_wrta_ktereister_watz-:::: Useo Predefined Check::::: SYSTEM_32\Edgehtml.dll Cisco-Defined     pc_wrta_ktereister_watz-::::::::::::::::::::::::::::::::::::	
	Requirements	pc_W81_64_K82v27528_MS Cisco Predefined Check: SYSTEM_ROOT\systaativ Cisco-Defined     pc_W8_64_K82v27528_MS Cisco Predefined Check: SYSTEM_ROOT\systaativ Cisco-Defined	
	Allowed Protocols Authorization Profiles	pc_W8_64_X02992811_M5 Cisco Predefined Check SYSTEM_ROOT\sysnativ Cisco-Defined	
	Downloadable AGLS	pc_W7_K83078601_W515 Clsco Predefined Check: SYSTEM_32(Win32k.sys Clsco-Defined	

# 步骤 19. 导航到Work Centers > Posture > Policy Elements > Conditions > File。单击。Add

ISE\_Add\_New\_File\_Condition

# 步骤 19.1 配置详细信息:

名称: linux\_demo\_file\_exist

操作系统:Linux All

文件类型:FileExist

文件路径:home、Desktop/test.txt

文件运算符:存在

# 单击。Submit

=	dude Identity Services Engine				Work Cen	ters / Post	ture	
н	Overview Network Devices	Client Provisioning Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
	Conditions Anti-Malware Anti-Sayware Anti-Virus Application Compound Dictionary Compound Dictionary Compound Diction	File Conditions List > New File Condition File Condition Name * Inux_demo_file_exist Description * Operating System Linux All Compliance Module Any version * File Type FileExistence * File Path nome * File Operator Exists	Uesktop/	lost.txt	]		Submit	

 $ISE\_Add\_New\_File\_Condition\_1$ 

步骤 20. 导航到Work Centers > Posture > Policy Elements > Requirements。在任何规则名称末尾点击Edit 。选择.Insert new Requirement

≡	dentity Services E	Ingine							Work	Centers / Po	sture					
н	Bookmarks	Overview	Network Devices	Client Provisioning	Policy	y Elements	Posture	Policy Policy Sets	Tro	ubleshoot	Reports \$	settings				
UL I	Dashboard Context Visibility	Conditions Anti-Malw	~									Guide Me				
×	Operations	Anti-Spyw	are	Requirements												
0	Policy	Anti-Virus		Name		Operating Sys	tem	Compliance Module		Posture Type		Conditions		Remediations Actions		
	Administration	Compound	5	Any_AV_Installation_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_av_win_inst	then	Message Text Only	Edit 🛩	
	Automatical action	Dictionary	Compound	Any_AV_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_av_win_def	then	AnyAVDefRemediationWin	Edit - G	uplicat
ก็เ	Work Centers	Dictionary	Simple	Any_AS_installation_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_inst	then	Message Text Only	Edit - B	sert n
		Disk Encry	ption	Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def	then	AnyASDefRemediationWin	Edit - C	alete
1	Interactive Help	File	asabource	Any_AV_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_inst	then	Message Text Only	Edit 🗸	<u>.</u>
		Firewall		Any_AV_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_def	then	AnyAVDefRemediationMac	Edit 🤟	
		Hardware	Attributes	Any_AS_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_inst	then	Message Text Only	Edit 🤟	
		Patch Mar	agement	Any_AS_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_def	then	AnyASDefRemediationMac	Edit 😔	
		Registry		Any_AM_Installation_Wir	for	Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_inst	then	Message Text Only	Edit 🛩	
		Service		Any_AM_Definition_Win	for	Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_def	then	AnyAMDefRemediationWin	Edit 🤟	
		U\$8		Any_AM_Installation_Ma	o for	Mac OSX	using	4.x or later	using	Agent	met if	ANY_am_mac_inst	then	Message Text Only	Edit 😔	
				Any_AM_Definition_Mac	for	Mac OSX	using	4.x or later	using	Agent	met if	ANY_am_mac_def	then	AnyAMDefRemediationMac	Edit 🛩	
		Remediation	• •	Any_AM_Installation_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_inst	then	Select Remediations	Edit 🖂	1
		Requirements		Any_AM_Definition_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_def	then	Select Remediations	Edit 9	
		Allowed Prot	ocols	USB_Block	for	Windows All	using	4.x or later	using	Agent	met if	USB_Check	then	USB_Block	Edit 😔	
		Authorization Downloadabl	Profiles e ACLs	Default_AppVis_Require ent_Win	n for	Windows All	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Win	then	Select Remediations	Edit 9	
				Default_AppVis_Requirer ent_Mac	n for	Mac OSX	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Mac	then	Select Remediations	Edit 🤟	
				Default_Hardware_Attrib es_Requirement_Win	ut for	Windows All	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 👻	
				Default_Hardware_Attrib es_Requirement_Mac	ut for	Mac OSX	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 🛩	

ISE\_Add\_New\_Posture\_Requirement

#### 步骤 20.1 配置详细信息:

名称:Test\_exist\_linux

操作系统:Linux All

合规性模块:4.x或更高版本

状态类型:代理

条件:linux\_demo\_file\_exist

单击Done 和Save。

≡ ;	Indentity Services Engine			Work Centers / Posture		
	Overview Network Devices	Client Provisioning Policy Elem	ments Posture Policy Policy Sets Tr	oubleshoot Reports Sett	tings	
<u> </u>						
	Conditions ~					~ 0
11	Anti-Malware			Guide Me		
*	Anti-Spyware	Requirements				
	Anti-Virus	Name Ope	erating System Compliance Module	Posture Type 0	Conditions Remediations Action	
•	Application		• •			
a.	Compound Dictionary Compound	Test_exist_linux for Linux	xx All using 4.x or later using	Agent met if	inux_demo_file_ex then Select Remediations ist	Edit 🗸
-51	Dictionary Simple	Any_AV_Installation_Win for Wind	dows All using 3.x or earlier using	Agent met if J	ANY_av_win_inst then Message Text Only	Edit 🛩
	Disk Encryption	Any_AV_Definition_Win for Wind	dows All using 3.x or earlier using	Agent met if /	ANY_av_win_def then AnyAVDefRemediationWi	Edit 🛩
0	External DataSource	Any_AS_Installation_Win for Wind	dows All using 3.x or earlier using	Agent met if /	ANY_as_win_inst then Message Text Only	Edit 🛩
	File	Any_AS_Definition_Win for Wind	dows All using 3.x or earlier using	Agent met if A	ANY_as_win_def then AnyASDefRemediationWi	Edit 🗸
	Firewall	Any_AV_Installation_Mac for Mac	OSX using 3.x or earlier using	Agent met if A	ANY_av_mac_inst then Message Text Only	Edit ~
	Patch Management	Any_AV_Definition_Mac for Mac	COSX using 3.x or earlier using	Agent met if J	ANY_av_mac_def then AnyAVDefRemediationMa	e Edit ~
	Registry	Any_AS_Installation_Mac for Mac	: OSX using 3.x or earlier using	Agent met if /	ANY_as_mac_inst then Message Text Only	Edit 👻
	Script	Any_AS_Definition_Mac for Mac	: OSX using 3.x or earlier using	Agent met if J	ANY_as_mac_def then AnyASDefRemediationMa	c Edit ↔
	Service	Any_AM_Installation_Win for Wind	dows All using 4.x or later using	Agent met if /	ANY_am_win_inst then Message Text Only	Edit v
	USB	Any AM Definition Win for Wind	dows All using 4.x or later using	Agent met if A	ANY am win def then AnyAMDefRemediationW	n Edit v
		Any AM Installation Mac for Mac	OSX using 4.x or later using	Agent met if A	ANY am mac inst then Message Text Only	Edit v
	Remediations	Any AM Definition Mac for Mac	DSX using 4.x or later using	Agent met if J	ANY am mac def then AnyAMDefRemediationM	
	Requirements	had been been been been been been been bee	and and the second	- Alexandre - A	an partane and representation of the	Eur v
	Allowed Protocols	Note:				
	Authorization Profiles	Remediation Action is filtered based on the op Remediation Actions are not applicable for App	perating system and stealth mode selection. oplication Conditions (configured using the Provision By Category	or Provision By Everything options), Hardwa	re Conditions, and External Data source conditions.	
	COMPROBIDIE PLOCS	Remediations Actions are not applicable for Ag	Agentiess Posture type.			
						Cause Daset
						Save

ISE\_Add\_New\_Posture\_Requirement\_1



**注意**:到目前为止,Linux代理仅支持shell脚本作为补救。

步骤 21. 导航到Work Centers > Posture > Policy Elements > Authorization Profiles。单击。Add

步骤 21.1 配置详细信息:

名称:unknown\_redirect

选中复选框 Web Redirection(CWA,MDM,NSP,CPP)

选择 Client Provisioning(Posture)

ACL:重定向

# 值:客户端调配门户(默认)

≡ :	dentity Services Engine	Work Centers / Posture
н.	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
11日 12日 12日 13日 13日 13日 13日 13日 13日 13日 13	Conditions Anti-Malware Anti-Spyware Anti-Virus Application Compound Dictionary Compound Dictionary Compound Dictionary Simple Disk Encryption External DataSource File Firewall	* Name       unknown_redirect         Description
	Hardware Attributes Patch Management Registry Script Service USB Remediations Requirements Allowed Protocols Authorization Profiles Downloadable ACLs	Static IP/Host name/FQDN Suppress Profiler CoA for endpoints in Logical Profile

ISE\_Add\_New\_Authorization\_Profile\_Redirect\_1



**注意**:此ACL名称重定向必须与FTD上配置的相应ACL名称匹配。

步骤 21.2重复Add 以为不兼容和兼容的终端创建另外两个授权配置文件及详细信息。

名称:non\_compliant\_profile

DACL名称: DENY\_ALL\_IPv4\_TRAFFIC

名称:compliant\_profile

DACL名称: PERMIT\_ALL\_IPv4\_TRAFFIC



注意:需要根据实际要求配置合规或不合规终端的DACL。

步骤 22. 导航到Work Centers > Posture > Posture Policy。在任何规则末尾单击Edit 。选择.Insert new policy

- Advision Accession	- Franks							- 1		-						<b>•</b> •	~	
<ul> <li>Casco Identity Service</li> </ul>	s Engine							l	Work Centers /	Pos	ture					ч <b>ф</b>	<u>ں</u>	ΨIX
Bookmarks	Overview	w Ne	etwork Devices	Client Provisioning	Policy Elements	Postu	re Policy Policy	Sets	Troubleshoot	R	teports Settings							
E Dashboard		_																
Context Visibility		Post	ure Policy	Guide Me														
% Operations		Define th	e Posture Policy by c	onfiguring rules based on open	ating system and/or of	her cond	itions.									9		Q,
Policy		~																
Administration		Status	Policy Options	Rule Name	Identity Groups		Operating Systems		Compliance Module		Posture Type	Other Conditions		Requirements				
Work Centers			Policy Options	Default_AntiMalware_Policy_Ma c	ii Any	and	Mac OSX	and	4.x or later	and	Agent	and	then	Any_AM_Installation_Ma c	Edit প			- 1
			Policy Options	Default_AntiMalware_Policy_Ma c_temporal	ii Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	044	Any_AM_installation_Ma c_temporal	Edg Insert new policy			
③ Interactive Help			Policy Options	Default_AntiMalware_Policy_Win	ii Any	and	Windows All	and	4.x or later	and	Agent	and	then	Any_AM_Installation_Win	Edit Orace			
			Policy Options	Default_AntiMalware_Policy_Win_temporal	ii Any	and	Windows All	and	4.x or later	and	Temporal Agent	and	then	Any_AM_Installation_Win_temporal	Edit +			
			Policy Options	Default_AppVIs_Policy_Mac	ii Any	and	Mac OSX	and	4.x or later	and	Agent	and	then	Default_AppVis_Require ment_Mac	Edit v			
			Policy Options	Default_AppVIs_Policy_Mac_te mporal	ii Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require ment_Mac_temporal	Edit y			
			Policy Optiona	Default_AppVIs_Policy_Win	i' Any	and	Windows All	and	4.x or later	and	Agent	and	then	Default_AppVis_Require ment_Win	Edit v			
			Policy Options	Default_AppVis_Policy_Win_te mporal	i' Any	and .	Windows All	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require ment_Win_temporal	Edit +			
			Policy Options	Default_Firewalt_Policy_Mac	ii Any	and	Mac OSX	and	4.x or later	and	Agent	and	then.	Default_Firewalt_Require ment_Mac	Edit v			
			Policy Options	Default_Firewall_Policy_Mac_temporal	ii Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_Firewall_Require ment_Mac_temporal	Edit +			
			Policy Optiona	Default_Firewall_Policy_Win	ii Any	and	Windows All	and	4.x or later	and	Agent	and	then	Default_Firewall_Require ment_Win	Edit 4			
			Policy Options	Default_Firewall_Policy_Win_te mporal	II Any	and	Windows All	and	4.x or later	and	Temporal Agent	and	then	Default_Firewall_Require ment_Win_temporal	Edit v			
			Policy Options	Default_Hardware_Attributes_P olicy_Mac	ii Any	and	Mac OSX	and	4.x or later	and	Agent	and	then	Default_Hardware_Attrib utes_Requirement_Mac	Edit v			
			Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	if Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_Hardware_Attrib utes_Requirement_Mac_ temporal	Edt v			
			Policy Options	Default_Hardware_Attributes_P olicy_Win	ii Any	and	Windows All	and	4.x or later	and	Agent	and	then	Default_Hardware_Attrib utes_Requirement_Win	Edit v			
		-	A	-			· · · · · · · · · · · · · · · · · · ·		* *- *-*-		*							

ISE\_Add\_New\_Posture\_Policy

#### 步骤 22.1 配置详细信息:

规则名称:Demo\_test\_exist\_linux

身份组:任意

操作系统:Linux All

合规性模块:4.x或更高版本

状态类型:代理

要求:Test\_exist\_linux

单击Done 和Save。

Post		Guide Me	ting s	system and/or	r other cone	ditions.										2	×
×																	
	Policy Options	Default_Firewall_Policy_Mac	ii.	Atry	and	Mac OSX	an	d 4.)	x or later		nd	Agent	and	the	en.	Default_Firewall_Require ment_Mac	Edit 🗸
	Policy Options	Default_Firewall_Policy_Mac_te mporal	i.	Any	and	Mac OSX	an	d 4.)	x or later	- à	nd	Temporal Agent	and	th	65	Default_Firewall_Require ment_Mac_temporal	Edit 🗸
	Policy Options	Default_Firewall_Policy_Win	H.	Any	and	Windows All	an	d 4.3	x or later		nd	Agent	and	th	en.	Default_Firewall_Require ment_Win	Edit v
	Policy Options	Default_Firewall_Policy_Win_te mporal	H.	Any	and	Windows All	an	d 4.3	x or later	- 1	nd	Temporal Agent	and	the	en	Default_Firewall_Require ment_Win_temporal	Edit v
	Policy Options	Default_Hardware_Attributes_P olicy_Mac	1	Any	and	Mac OSX	an	4.a	x or later	-	nd	Agent	and	th	en	Default_Hardware_Attrib utes_Requirement_Mac	Edit 🗸
	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	1	Any	and	Mac OSX	an	d 4.3	x or later	-	nd	Temporal Agent	and	th	en	Default_Hardware_Attrib utes_Requirement_Mac_ temporal	Edit 👻
	Policy Options	Default_Hardware_Attributes_P olicy_Win	ii.	Any	and	Windows All	an	4 4 b	x or later		nd	Agent	and	th	en.	Default_Hardware_Attrib utes_Requirement_Win	Edit 🗸
	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	R.	Any	and	Windows All	an	d 4.3	x or later	-	nd	Temporal Agent	and	the	65	Default_Hardware_Attrib utes_Requirement_Win_t emporal	Edit v
	Policy Options	Default_US8_Block_Policy_Win	W.	Any	and	Windows All	an	d 4.3	x or later		nd	Agent	and	th	en.	USB_Block	Edit 😔
	Policy Options	Default_USB_Block_Policy_Win	11	Any	and	Windows All	an	d 4.3	x or later		nd	Temporal Agent	and	th	en.	USB_Block_temporal	Edit 😔

ISE\_Add\_New\_Posture\_Policy\_1

#### 步骤 23. 导航到Work Centers > Posture > Policy Sets。单击以Insert new row above。

$\equiv \frac{-de-de-}{cisco}$ Identity Services (	ngine	Work Centers / Posture	A @ @ A   A
JI Bookmarks	Overview Network Devices Client Provisioning Policy Elements Posture Policy	Sets Troubleshoot Reports	Settings
Dashboard	Policy Sets		Basel Reset Policyset Hitrouvet
10 Context Visibility	Pointy Jours		
X Operations	<ul> <li>Status Policy Set Name Description Conditions</li> </ul>		Allowed Protocols / Server Sequence Hits Actions View
Policy	Q. Search		
2 Administration	Default     Default     Default		Default Network Access 🥒 🕂 o 🔯 🗲
③ Interactive Help			Insert new row above
			Reset

ISE\_Add\_New\_Policy\_Set

步骤 23.1 配置详细信息:

策略集名称:Firewall Posture

#### 条件:网络接入设备IP地址等于[FTD IP地址]

单击。 Save

≡ dentity Services	Engline Work Centers / Posture	Q & @ Q   A
Bookmarks	Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
1년 Context Visibility	Policy Sets	Reset Reset Policyset Hitcounts Save
N Operations	Status         Policy Set Name         Description         Conditions	Allowed Protocols / Server Sequence Hits Actions View
E Policy	Q Search	
2 Administration	Firewall Posture     Betweet Access Device IP Address TQUALS *******	Default Network Access 2 + 2
📲 Work Centers	Default     Default     Default	Default Network Access 🥜 + 🔹 🚯 💙
③ Interactive Help		Reset

ISE\_Add\_New\_Policy\_Set\_1

#### 步骤 23.2单击>以输入策略集。为状态兼容、不兼容和未知状态创建新的授权规则。单击。Save

#### 与compliant\_profile兼容

与non\_compliant\_profile不兼容

#### Unknown\_redirect未知

dentity Identity	y Serv	ces Engine						Work Cent	ers / Postu	re						
Overview	Net 2 Searc	work Devices	Client Prov	isioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings						
	٥	Firewall Posture			🖵 Nete	vork Access-Device IP Add	ress EQUALS :						Default Netwo	rk Access	0	+ •
∼Aut	thenticat	ion Policy(1)														
۲	Statu	s Rule Name	с	onditions								Use			Hits	Actions
	Q Sear	ch														
								+								
												All_User_	D_Stores	0		-
		Default										> Option	s		48	<u>{</u> \$}
> Aut	thorizatio	n Policy - Local E	xceptions													
> Aut	thorizatio	n Policy - Global	Exceptions													
∨Aut	thorizatio	n Policy(4)														
										Results						
•	Statu	s Rule Name	c	onditions						Profiles		Security Gr	oups		Hits	Actions
	Q Sear	ch														
	0	Compliant	ł	E Session-P	ostureStatus EQUALS Cor	npliant				compliant_profile	0+	Select fro	m list	<i>ø</i> +	15	<b>@</b>
	٥	Non_Compliant	ł	E Session P	ostureStatus EQUALS Nor	Compliant				non_compliant_profile	0+	Select fro	m list	1	5	(2)
	0	Unknown	ł	is Session-P	ostureStatus EQUALS Uni	ntown				unknown_redirect	0+	Select fro	m list	0 +	47	(2)
	Overview Au Au Au	Overview Net	Overview Network Devices Overview Network Devices  V-Authentication Policy(1)  Status Rule Name  Search  Authorization Policy - Local E  Cuthorization Policy	Overview     Network Devices     Client Prov       Overview     Network Devices     Client Prov       Image: Status     Firewall Posture     Image: Status       Image: Status     Rule Name     C       Image: Status     Dafasti       Image: Authorization Policy - Local Exceptions       Image: Authorization Policy - Local Exceptions       Image: Authorization Policy - Local Exceptions       Image: Authorization Policy (4)       Image: Status     Rule Name       Image: Compliant       Image: Authorization Policy (1)	Overview       Network Devices       Client Provisioning         Overview       Network Devices       Client Provisioning         Image: Status       Rule Name       Conditions         Image: Status </td <th>Overview       Network Devices       Client Provisioning       Policy Elements         Image: Condition Policy(1)       Image: Condition S       Image: Condition S         Image: Condition Policy(1)       Image: Condition S       Image: Condition S         Image: Condition Policy(1)       Image: Condition S       Image: Condition S         Image: Condition Policy(1)       Image: Condition S       Image: Condition S         Image: Condition Policy - Local Exceptions       Image: Condition S       Image: Condition S         Image: Condition Policy(4)       Image: Condition S       Image: Condition S         Image: Condition Compliant       Image: Session PostureStatus EQUALS for Image: Condition S         Image: Condition Image: Condition S       Image: Condition S       Image: Condition S         Image: Condition Image: Condition S       Image: Condition S       Image: Condition S         Image: Condition Image: Condition S       Image: Condition S       Image: Condition S         Image: Condition Image: Condimage: Condimage: Condimage: Condition Image: Condition Image: Con</th> <td>Overview       Network Devices       Client Provisioning       Policy Elements       Posture Policy         Image: Status       Prevail Pathree       Image: Status       Network Access Device IP Add         Image: Authentication Policy(1)       Image: Status       Network Access Device IP Add         Image: Status       Rule Name       Conditions         Image: Status       Rule Name       Conditions         Image: Status       Default       Image: Status         Image: Authorization Policy - Local Exceptions       Image: Authorization Policy(4)         Image: Status       Rule Name       Conditions         Image: Status       Rule Name<!--</td--><td>Overview       Network Devices       Client Provisioning       Policy Elements       Posture Policy       Policy Sets            <ul> <li>Prevail</li> <li>Prevail</li></ul></td><td>Status     Rule Name     Conditions       Vurtication Policy - Local Exceptions       Authorization Policy - Global Exceptions       Authorization Policy - Global Exceptions       Authorization Policy - Global Exceptions       Vurtication Policy - Global Exceptions</td><td>Work Clentity Services Engine     Work Centers / Postur         Overview     Network Devices     Client Provisioning     Policy Elements     Posture Policy     Policy Sets     Troubleshoot     Reports         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions   &lt;</td><td>Udentity Services Engine         Work Centers / Posture           Overview         Network Devices         Client Provisioning         Policy Elements         Posture Policy         Policy Sets         Troubleshoot         Reports         Settings           Image: Setting         Image: Seting         Image: Setting         I</td><td>Udentity Services Engine     Overview     Network Devices     Client Provisioning   Policy Elements     Prevel     Prevel     VAuthentication Policy(1)     Status     Relevint     Pathentication Policy(2)     Default     Outhentication Policy(2)     Status     Relevint     Prevelle     Valuetorization     Policy 1 Conditions     Valuetorization     Policy 1 Conditions     Valuetorization     Policy 2 Conditions     Valuetorization     Valuetorization     Policy 2 Conditions     Valuetorization     Valuetorization     Policy 2     Status   Rue Name   Conditions   Valuetorization   Policy 3   Status   Rue Name   Conditions   Valuetorization   Policy 4   Status   Rue Name   Conditions   Valuetorization   Policy 5   Status   Rue Name   Conditions   Policy 6   Status   Rue Name   Conditions   Rue Name   Conditions   Rue Name   Cond</td><td>Udentity Services Engine         Work Centers / Posture           Overview         Network Devices         Client Provisioning         Policy Elements         Policy Sets         Troubleshoot         Reports         Settings           Image: Setting         Image: Seting         Image: Setting         I</td><td>Work Centers / Potture</td><td>Work Centers / Posture     Overview Network Devices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings       Press Palers  Default Default Default Default Default Default       Press Palers Cenditions Use        Default        &lt;</td><td>Market Identity Services Engine Work Centers / Posture</td></td>	Overview       Network Devices       Client Provisioning       Policy Elements         Image: Condition Policy(1)       Image: Condition S       Image: Condition S         Image: Condition Policy(1)       Image: Condition S       Image: Condition S         Image: Condition Policy(1)       Image: Condition S       Image: Condition S         Image: Condition Policy(1)       Image: Condition S       Image: Condition S         Image: Condition Policy - Local Exceptions       Image: Condition S       Image: Condition S         Image: Condition Policy(4)       Image: Condition S       Image: Condition S         Image: Condition Compliant       Image: Session PostureStatus EQUALS for Image: Condition S         Image: Condition Image: Condition S       Image: Condition S       Image: Condition S         Image: Condition Image: Condition S       Image: Condition S       Image: Condition S         Image: Condition Image: Condition S       Image: Condition S       Image: Condition S         Image: Condition Image: Condimage: Condimage: Condimage: Condition Image: Condition Image: Con	Overview       Network Devices       Client Provisioning       Policy Elements       Posture Policy         Image: Status       Prevail Pathree       Image: Status       Network Access Device IP Add         Image: Authentication Policy(1)       Image: Status       Network Access Device IP Add         Image: Status       Rule Name       Conditions         Image: Status       Rule Name       Conditions         Image: Status       Default       Image: Status         Image: Authorization Policy - Local Exceptions       Image: Authorization Policy(4)         Image: Status       Rule Name       Conditions         Image: Status       Rule Name </td <td>Overview       Network Devices       Client Provisioning       Policy Elements       Posture Policy       Policy Sets            <ul> <li>Prevail</li> <li>Prevail</li></ul></td> <td>Status     Rule Name     Conditions       Vurtication Policy - Local Exceptions       Authorization Policy - Global Exceptions       Authorization Policy - Global Exceptions       Authorization Policy - Global Exceptions       Vurtication Policy - Global Exceptions</td> <td>Work Clentity Services Engine     Work Centers / Postur         Overview     Network Devices     Client Provisioning     Policy Elements     Posture Policy     Policy Sets     Troubleshoot     Reports         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions   &lt;</td> <td>Udentity Services Engine         Work Centers / Posture           Overview         Network Devices         Client Provisioning         Policy Elements         Posture Policy         Policy Sets         Troubleshoot         Reports         Settings           Image: Setting         Image: Seting         Image: Setting         I</td> <td>Udentity Services Engine     Overview     Network Devices     Client Provisioning   Policy Elements     Prevel     Prevel     VAuthentication Policy(1)     Status     Relevint     Pathentication Policy(2)     Default     Outhentication Policy(2)     Status     Relevint     Prevelle     Valuetorization     Policy 1 Conditions     Valuetorization     Policy 1 Conditions     Valuetorization     Policy 2 Conditions     Valuetorization     Valuetorization     Policy 2 Conditions     Valuetorization     Valuetorization     Policy 2     Status   Rue Name   Conditions   Valuetorization   Policy 3   Status   Rue Name   Conditions   Valuetorization   Policy 4   Status   Rue Name   Conditions   Valuetorization   Policy 5   Status   Rue Name   Conditions   Policy 6   Status   Rue Name   Conditions   Rue Name   Conditions   Rue Name   Cond</td> <td>Udentity Services Engine         Work Centers / Posture           Overview         Network Devices         Client Provisioning         Policy Elements         Policy Sets         Troubleshoot         Reports         Settings           Image: Setting         Image: Seting         Image: Setting         I</td> <td>Work Centers / Potture</td> <td>Work Centers / Posture     Overview Network Devices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings       Press Palers  Default Default Default Default Default Default       Press Palers Cenditions Use        Default        &lt;</td> <td>Market Identity Services Engine Work Centers / Posture</td>	Overview       Network Devices       Client Provisioning       Policy Elements       Posture Policy       Policy Sets <ul> <li>Prevail</li> <li>Prevail</li></ul>	Status     Rule Name     Conditions       Vurtication Policy - Local Exceptions       Authorization Policy - Global Exceptions       Authorization Policy - Global Exceptions       Authorization Policy - Global Exceptions       Vurtication Policy - Global Exceptions	Work Clentity Services Engine     Work Centers / Postur         Overview     Network Devices     Client Provisioning     Policy Elements     Posture Policy     Policy Sets     Troubleshoot     Reports         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions         Image: Conditions     Image: Conditions     Image: Conditions     Image: Conditions   <	Udentity Services Engine         Work Centers / Posture           Overview         Network Devices         Client Provisioning         Policy Elements         Posture Policy         Policy Sets         Troubleshoot         Reports         Settings           Image: Setting         Image: Seting         Image: Setting         I	Udentity Services Engine     Overview     Network Devices     Client Provisioning   Policy Elements     Prevel     Prevel     VAuthentication Policy(1)     Status     Relevint     Pathentication Policy(2)     Default     Outhentication Policy(2)     Status     Relevint     Prevelle     Valuetorization     Policy 1 Conditions     Valuetorization     Policy 1 Conditions     Valuetorization     Policy 2 Conditions     Valuetorization     Valuetorization     Policy 2 Conditions     Valuetorization     Valuetorization     Policy 2     Status   Rue Name   Conditions   Valuetorization   Policy 3   Status   Rue Name   Conditions   Valuetorization   Policy 4   Status   Rue Name   Conditions   Valuetorization   Policy 5   Status   Rue Name   Conditions   Policy 6   Status   Rue Name   Conditions   Rue Name   Conditions   Rue Name   Cond	Udentity Services Engine         Work Centers / Posture           Overview         Network Devices         Client Provisioning         Policy Elements         Policy Sets         Troubleshoot         Reports         Settings           Image: Setting         Image: Seting         Image: Setting         I	Work Centers / Potture	Work Centers / Posture     Overview Network Devices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings       Press Palers  Default Default Default Default Default Default       Press Palers Cenditions Use        Default        <	Market Identity Services Engine Work Centers / Posture

ISE\_Add\_New\_Policy\_Set\_2

#### Ubuntu上的配置

步骤 24通过GUI登录到Ubuntu客户端。打开浏览器以登录VPN门户。在本例中为demo.example.com。

demo.ex	xam	nple.com/+CS	COEX	+			-	ē	×
$\leftarrow \rightarrow$	è	С	0 🗛	https://demo.example.com/	CSCOE+/logon.html#form_title_text	ដ	$\bigtriangledown$	$\mathbf{F}$	≡

Logon
Group posture_vpn v Username Password
Logon

Ubuntu\_Browser\_VPN\_Login

步骤 25单击。Download for Linux

Cisco Secur	e Client Insta	llati	+					ē	×
$\leftarrow \   \rightarrow$	C	0 &	https://demo. <b>example.com</b> /CACHE/stc/2/index.html	Ē	80%	ជ	⊘	$\mathbf{F}$	≡
	Secure (	RE Client							
			Cisco Secure Client Download	H		bi			
			Download & Install						
			Download Cisco Secure Client and install it on your computer.		• Inst	ructions			
					U IIISU	u u u u u u u u u			

Ubuntu\_Browser\_VPN\_Download\_1

下载的文件名为cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh。



Ubuntu\_Browser\_VPN\_Download\_2

步骤 26通过浏览器下载VPN证书并将文件重命名为<certificate>.crt。这是使用firefox下载证书的示例。

-	demo.example.	com/+CSCOE× +	$\sim$		đ	×
$\leftarrow$	$\rightarrow$ C	Ttps://demo. <b>example.com</b> /+CSCOE+/logon.html#form_title_text	${igsidential}$	۲	பி	≡

General Media Permissions	COE+/logon.ntml	#rorm_title_text _ U			
Website Identity         Website:       demo.example.com         Owner:       This website does not supply ownership in         Verified by:       C=CN,CN=demo.example.com	formation.	<u>V</u> iew Certificate			
Privacy & History Have I visited this website prior to today?	No				
Is this website storing information on my computer?	Yes, cookies	<u>C</u> lear Cookies and Site Data			
Have I saved any passwords for this website?	No	Vie <u>w</u> Saved Passwords			
Technical Details Connection Encrypted (TLS_AES_128_GCM_SHA256, 12 The page you are viewing was encrypted before being to Encryption makes it difficult for unauthorized people to therefore unlikely that anyone read this page as it trave	8 bit keys, TLS 1.3) ransmitted over the view information t led across the netw	e Internet. raveling between computers. It ork. Help			

Ubuntu\_Browser\_VPN\_Cert\_Download

步骤 27在Ubuntu客户端上打开终端。导航到path home/user/Downloads/安装Cisco安全客户端。

# <#root>

user@ubuntu22-desktop:~\$

cd Downloads/

```
user@ubuntu22-desktop:~/Downloads$
```

```
ls
```

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

demo-example-com.crt

```
user@ubuntu22-desktop:~/Downloads$
```

```
chmod +x cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

[sudo] password for user: Installing Cisco Secure Client... Migrating /opt/cisco/anyconnect directory to /opt/cisco/secureclient directory Extracting installation files to /tmp/vpn.zaeAZd/vpninst959732303.tgz... Unarchiving installation files to /tmp/vpn.zaeAZd... Starting Cisco Secure Client Agent... Done! Exiting now. user@ubuntu22-desktop:~/Downloads\$

步骤 28信任Ubuntu客户端上的VPN门户证书。

<#root>

user@ubuntu22-desktop:~\$

cd Downloads/

user@ubuntu22-desktop:~/Downloads\$

ls

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

demo-example-com.crt

user@ubuntu22-desktop:~/Downloads\$

openssl verify demo-example-com.crt

CN = demo.example.com, C = CN
error 18 at 0 depth lookup: self-signed certificate
Error demo-example-com.crt:

verification failed

user@ubuntu22-desktop:~/Downloads\$

sudo cp demo-example-com.crt /usr/local/share/ca-certificates/

user@ubuntu22-desktop:~/Downloads\$

sudo update-ca-certificates

Updating certificates in /etc/ssl/certs... rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL

#### 1 added

```
, O removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

user@ubuntu22-desktop:~/Downloads\$

openssl verify demo-example-com.crt

demo-example-com.crt: OK

步骤 29在Ubuntu客户端上打开Cisco Secure Client,然后将VPN成功连接到demo.example.com。

		Cisco Secure	Client		•		×
AnyCon	nect VPN	✓ Statist	ics	About			
		ייןיי cisc	ı . 0				
Connect to:	demo.exa	ample.com			~	] [	\$
Group:	posture_v	pn				~	r )
Username:	isetest						
Password:	******						



 $Ubuntu\_Secure\_Client\_Connected$ 

步骤 30打开浏览器以访问触发重定向至ISE CPP门户的任何网站。从ISE CPP门户下载证书并将文件重命名为<certificate>.crt。 这是 使用Firefox进行下载的示例。



```
Ubuntu_Browser_CPP_Cert_Download
```

#### 步骤 30.1信任Ubuntu客户端上的ISE CPP门户证书。

#### <#root>

user@ubuntu22-desktop:~/Downloads\$ ls cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh demo-example-com.crt

ise-cert.crt

user@ubuntu22-desktop:~/Downloads\$

sudo cp ise-cert.crt /usr/local/share/ca-certificates/

user@ubuntu22-desktop:~/Downloads\$

sudo update-ca-certificates

Updating certificates in /etc/ssl/certs... rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL

1 added

```
, O removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

步骤 31在ISE CPP门户上点击Start。

O Device Security Check × +		ø	×					
← → C () A https://demoise.example.com:8443/portal/PortalSetup.action?portal=ee39fd08 ☆		$\bigtriangledown$	≡					
Our must log in to this network before you can access the Internet.								
Client Provisioning Portal								
Device Security Check Your computer requires security software to be installed before you can connect to the network.  Start								
Ubuntu_Browser_CPP_Start								

# 步骤32.Click here to download and install Agent.

Device Security	y Check × +	- • •	¢						
$\leftarrow \   \rightarrow \   G$	https://demoise.example.com ::8443/portal/ClientProvisionStart.action?from=CL 🏠	$\odot$							
You must log	) in to this network before you can access the Internet.	×							
cisco.	Client Provisioning Portal								
Device Security Check Your computer requires security software to be installed before you can connect to the network. Unable to detect Posture Agent									
•	+ This is my first time here								
<ol> <li>You must install Agent to check your device before accessing the network. <u>Click here to download and install Agent</u></li> <li>After installation, Agent will automatically scan your device before allowing you access to the network.</li> <li>You have 20 minutes to install and for the system scan to complete.</li> </ol>									
Note: With some browsers, when you click Download, the script is directly saved in the configured Downloads folder in your system. Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.									
			J						

Ubuntu\_Browser\_CPP\_Download\_Posture

步骤 33在Ubuntu客户端上打开终端。导航到路径home/user/Downloads/,安装状态模块。

# <#root>

user@ubuntu22-desktop:~/Downloads\$ ls

cisco-secure-client-ise-network-assistant-linux64-5.1.3.62\_demoise.example.com\_8443\_0NcLgcMURfyZmR6HoLmL

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
demo-example-com.crt
ise-cert.crt
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
chmod +x cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfy
```

user@ubuntu22-desktop:~/Downloads\$
user@ubuntu22-desktop:~/Downloads\$
user@ubuntu22-desktop:~/Downloads\$

./cisco-secure-client-ise-network-assistant-linux64-5.1.3.62\_demoise.example.com\_8443\_0NcLgcMURfyZmR6HoI

Cisco Network Setup Assistant (c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks Cisco ISE Network Setup Assistant started. Version - 5.1.3.62 Trusted and Secure Connection You are connected to

demoise.example.com

whose identity has been certified. Your connection to this website is encrypted. Downloading Cisco Secure Client... Downloading remote package... Running Cisco Secure Client - Downloader... Installation is completed.

步骤 34在Ubuntu客户端UI上,退出Cisco安全客户端并重新打开它。ISE终端安全评估模块安装成功并运行。



Ubuntu\_Secure\_Client\_ISE\_Posture\_Installed

步骤 35在Ubuntu客户端上打开终端。导航到路径home/user/Desktop,创建test.txt一个文件以满足ISE上配置的文件条件。

# <#root>

user@ubuntu22-desktop:~\$

cd Desktop/

user@ubuntu22-desktop:~/Desktop\$

echo test > test.txt

# 验证

使用本部分可确认配置能否正常运行。

步骤1:在Ubuntu客户端上将VPN连接到demo.example.com。

	- • ×								
AnyConnect VPN	✓ Statistics	lSE Posture	About						
cisco									
Connect to: demo.example.com 🗸 🏹									
Group: posture_vpn ~									
Username: isetest									
Password:									

No. 2010 Disconnect							
Connected to demo.example.com.							

 $Verify\_Ubuntu\_Secure\_Client\_Connected$ 

第二步:检查Ubuntu客户端上的ISE终端安全评估状态。



#### Verify\_Ubuntu\_Secure\_Client\_Compliance

# 第三步:检查ISE上的Radius实时日志。导航到Operations > RADIUS Live Log。

≡	-thathe I	dentity Services Engine				Оре	rations / RADIUS			Q & @ Q   A
Ц	Live	e Logs Live Sessions								
55										
1 <sup>1</sup> 0		Misconfigured Supplicants 🕕		Miscon	figured Network D	evices 🕕	RADIUS Drops		Client Stopped Responding ①	Repeat Counter 🕕
Х		0			0		0		0	0
U									Refresh Show	Within
80									Never v Latest 20 re	cords 🗸 Last 24 hours 🗸
di.		☐	🖞 Export To 🗸							Filter 🗸 🐵
		Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy A	uthorization Policy
?			Y		Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy A	Authorization Policy
		May 29, 2024 09:08:48.798 PM	٠	ò	isetest	52:54:00:17:68:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default Fi	irewall Posture >> Compliant
		May 29, 2024 09:08:48.798 PM		ò		52:54:00:17:6B:FA		Compliant	Firewall Posture Fi	irewall Posture >> Compliant
		May 29, 2024 09:08:13.570 PM		à	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Pending	Firewall Posture >> Default Fi	irewall Posture >> Unknown

Verify\_ISE\_LiveLog

第四步:通过SSH或控制台导航至FTD CLI。

#### <#root>

>

>

```
system support diagnostic-cli
```

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available commands.

ftdv741>

enable

Password: ftdv741# ftdv741#

show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed
```

```
Username : isetest Index : 33
Assigned IP : 192.168.6.30 Public IP : 192.168.10.13
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 51596 Bytes Rx : 17606
Pkts Tx : 107 Pkts Rx : 136
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : posture_gp Tunnel Group : posture_vpn
Login Time : 14:02:25 UTC Fri May 31 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb007182000210006659d871
Security Grp : none Tunnel Zone : 0
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 33.1
Public IP : 192.168.10.13
Encryption : none Hashing : none
TCP Src Port : 59180 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : linux-64
Client OS Ver: Ubuntu 22.04 LTS 22.04 (Jammy Jellyfish)
```

Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62 Bytes Tx : 6364 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 33.2 Assigned IP :192.168.6.30 Public IP : 192.168.10.13 Encryption : AES-GCM-128 Hashing : SHA256 Ciphersuite : TLS\_AES\_128\_GCM\_SHA256 Encapsulation: TLSv1.3 TCP Src Port : 59182 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Linux\_64 Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62 Bytes Tx : 6364 Bytes Rx : 498 Pkts Tx : 1 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3 DTLS-Tunnel: Tunnel ID : 33.3 Assigned IP :192.168.6.30 Public IP : 192.168.10.13 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 56078 UDP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Linux\_64 Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62 Bytes Tx : 38868 Bytes Rx : 17108 Pkts Tx : 105 Pkts Rx : 130 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

#### 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。

对于终端安全评估流程和思科安全客户端和ISE故障排除,请检查CCO<mark>文档ISE终端安全评估样式比较高级版和2.2后版本</mark>以及<u>ISE会</u> 话管理和终端安全评估故障排除</u>。

相关信息

- <u>思科身份服务引擎管理员指南,版本3.3</u>
- 思科技术支持和下载

# 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)。