# 在FTD上通过AnyConnect远程访问VPN配置 ISE终端安全评估

目录	
<u>新介</u>	
<u> </u>	
使用的组件	
网络图和流量流程	
<u>FTD/FMC</u>	
ISE	
<u>文障排除</u>	

# 简介

本文档介绍如何配置Firepower威胁防御(FTD)版本6.4.0以根据身份服务引擎(ISE)对VPN用户进行 安全评估。

# 先决条件

# 要求

Cisco 建议您了解以下主题:

- AnyConnect远程访问VPN
- FTD上的远程访问VPN配置
- 身份服务引擎和状态服务

# 使用的组件

本文档中的信息基于以下软件版本:

- 思科Firepower威胁防御(FTD)软件版本6.4.0
- 思科Firepower管理控制台(FMC)软件版本6.5.0
- 带Cisco AnyConnect安全移动客户端的Microsoft Windows 10版本4.7
- 思科身份服务引擎(ISE)版本2.6,带补丁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

# 网络图和流量流程



1.远程用户使用Cisco Anyconnect对FTD进行VPN访问。

2. FTD向ISE发送该用户的RADIUS访问请求。

3.该请求到达ISE上名为FTD-VPN-Posture-Unknown的策略。ISE发送RADIUS Access-Accept三个属性:

- cisco-av-pair = url-redirect-acl=fyusifovredirect 这是在FTD上本地定义的访问控制列表 (ACL)名称,它决定重定向的流量。
- cisco-av-pair = urlredirect=<u>https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-</u> <u>11e9-98fb-0050568775a3&action=cpp</u> — 这是远程用户重定向到的URL。
- DACL = PERMIT\_ALL\_IPV4\_TRAFFIC 可下载ACL此属性是可选的。在这种情况下,所有流 量都在DACL中允许)
- 4.如果发送DACL,则交换RADIUS Access-Request/Access-Accept以下载DACL的内容

5.当来自VPN用户的流量与本地定义的ACL匹配时,流量会重定向到ISE客户端调配门户。ISE调配 AnyConnect状态模块和合规性模块。

6.在客户端计算机上安装代理后,代理会自动使用探测功能搜索ISE。当成功检测到ISE时,终端安 全评估要求会被检查。在本示例中,代理会检查任何已安装的防恶意软件软件。然后向ISE发送状 态报告。 7.当ISE收到来自代理的状态报告时,ISE更改此会话的状态并触发具有新属性的RADIUS CoA类型 推送。此时,状态为已知,另一规则已命中。

- 如果用户兼容,则发送允许完全访问的DACL名称。
- 如果用户不兼容,则会发送允许有限访问的DACL名称。

8. FTD删除重定向。FTD发送访问请求以便从ISE下载DACL。特定的DACL连接到VPN会话。

### 配置

FTD/FMC

步骤1:为ISE和修正服务器(如果有)创建网络对象组。导航到对象>对象管理>网络。

Overview Analysis Polic	ties Devices Objects AM	P Intelligence		
Object Management Intr	rusion Rules			
Network A network object represents one	e or more IP addresses. Network obje	ects are used in various places, in	cluding access control policies, network	variables, intrusion rules, identity rules, ne
Extended	Name			Value
📑 Standard	any-ipv4			0.0.0/0
Address Pools	any-ipv6			::/0
IPv6 Pools	enroll.cisco.com			72.163.1.80
Application Filters	IPv4-Benchmark-Tests	Edit Network Object		? ×
💮 Cipher Suite List	IPv4-Link-Local	Name ISE PSN		
Community List	IPv4-Multicast	Description		
Individual Objects	IPv4-Private-10.0.0.0-8			
Object Groups     ONS Server Group	IPv4-Private-172.16.0.0-12	Network • Host	C Range C Network	C FQDN
File List	IPv4-Private-192.168.0.0-16	192.168.15.	.14	
FlexConfig      FlexConfig Object      Text Object	IPv4-Private-All-RFC1918	Allow Overrides		Save Cancel
Geolocation	IPv6-IPv4-Mapped			::###:0.0.0.0/96
Interface Key Chain	IPv6-Link-Local			fe80::/10
Network	IPv6-Private-Unique-Local-Addre	sses		fc00::/7
Þ 🏓 PKI	IPv6-to-IPv4-Relay-Anycast			192.88.99.0/24

第二步:创建重定向ACL。导航到对象>对象管理>访问列表>扩展。单击Add Extended Access List并提供重定向ACL的名称。此名称必须与ISE授权结果中的名称相同。

Overview Analysis Policie	s Devices Obj	ects AN	IP Intelligence				Deploy 🧶 S
Object Management Intrus	sion Rules						3
Extended An access list object, also known a Supports IPv4 and IPv6 addresses	as an access control I You use these obje	st (ACL), sel tts when con	ects the traffic to which a figuring particular feature	a service will apply. Standard-Ide es, such as route maps.	ntifies traffic based on destina	tion address only. Identifies traffic based of	xtended Access List
Access List	New Extended	Access Li	st Object				? ×
Standard	Name	fyusifovre	direct	]			
Address Pools	Entries (0)						Add
IPv6 Pools	Sequence	Action	Source	Source Port	Destination	Destination Port	
Y AS Path				No rocord	de to dieplay		
Cipher Suite List				NO TECOLO	is to display		
Community List							
Distinguished Name     Individual Objects							
Cobject Groups							
DNS Server Group	Allow Overrides	Г					
File List							
FlexConfig						Save	Cancel
FlexConfig Object							

第三步:添加重定向ACL条目。单击 Add 按钮。阻止发往DNS、ISE和补救服务器的流量以将其从 重定向中排除。允许其余流量,这将触发重定向(如果需要,ACL条目可能更加具体)。

Add Extended A	Access List Entry					? ×
Action:	× Block	~				
Logging:	Default	×				
Log Level:	Informational	<b>*</b>				
Log Interval:		Sec.				
Network Po	rt					
Available Netwo	rks Ċ	$\odot$	Source Networks (1)		Destination Networks (1)	
🔍 Search by nar	me or value		📰 any-ipv4	1	💭 ISE_PSN	5
any 🔁		-				
any-ipv4						
any-ipv6		Add to Source				
nroll.cisco.c	com	Add to				
IPv4-Benchn	nark-Tests	Destination				
IPv4-Link-Lo	cal					
IPv4-Multicas	st					
IPv4-Private	-10.0.0-8					
IPv4-Private	-172.16.0.0-12	<b>_</b>	Enter an IP address	Add	Enter an IP address	Add
					Add	Cancel

Edit E	Edit Extended Access List Object ? ×								
Name	e es (4)	fyusifovredirect							
Linco	00 (4)						O Add		
Se	quence	Action	Source	Source Port	Destination	Destination Port			
1		🗙 Block	🖶 any	Any	Any	DNS_over_UDP	6		
2		🗙 Block	🚍 any-ipv4	Any	EISE_PSN	Any	0		
3		🗙 Block	any-ipv4	Any	RemediationServers	Any	0		
4		🖋 Allow	💭 any-ipv4	Any	📰 any-ipv4	Any	6		
Allow	Overrides	-							
Allow	overnites					Save	Cancel		

第四步:添加ISE PSN节点。导航到对象>对象管理> RADIUS服务器组。单击Add RADIUS Server Group,然后提供名称,启用选中所有复选框并点击加号图标。

Edit RADIUS Server Group							
	Name:*	ISE		]			
	Description:			-			
	Group Accounting Mode:	Single	•				
	Retry Interval:*	10	(1-10) Seconds				
	Realms:		•				
	Enable authorize only						
	Enable interim account update						
	Interval:*	24	(1-120) hours				
	🗹 Enable dynamic authorization						
	Port:*	1700	(1024-65535)				
	RADIUS Servers (Maximum 16 serv	vers)		٢			
	IP Address/Hostname						
		No records to display					
			Save	Cancel			

第五步:在打开的窗口中,提供ISE PSN IP地址、RADIUS密钥,选择Specific Interface,然后选 择可访问ISE的接口(此接口用作RADIUS流量的源),然后选择Redirect ACL(以前配置的)。

New RADIUS Server		? ×
IP Address/Hostname:*	192.168.15.13 Configure DNC at Threat Defense Platform Settings t	to resolve hostname
Authentication Port:*	1812	(1-65535)
Key:*	•••••	
Confirm Key:*	•••••	
Accounting Port:	1813	(1-65535)
Timeout:	10	(1-300) Seconds
Connect using:	C Routing 🖲 Specific Interface 🕕	
	ZONE-INSIDE	▼ ◎-
Redirect ACL:	fyusifovredirect	▼ ②
	Save	Cancel

第六步:为VPN用户创建地址池。导航到对象>对象管理>地址池> IPv4池。单击Add IPv4 Pools,并填写详细信息。

Overview Analysis Polici	es Devices Objects AMP Intelligence		Deploy 🤑 Sy
Object Management Intr	usion Rules		
IPv4 Pools IPv4 pool contains list of IPv4 ad	dresses, it is used for diagnostic interface with clustering, or for VPN remo	te access profiles.	Add IPv4 Pools
Standard	Name		Value
Address Pools	Edit IPv4 Pool	? ×	172.16.1.10-172.16.1.20
A Prote Pools     A Polication Filters     A S Path     Cipher Suite List     Community List     Distinguished Name     Individual Objects     Object Groups     File List     File List     File Config     File Config     File Config     File Config     File Config     File List     Geolocation     Text Object     Geolocation	Name* VPN-172-Pool IPv4 Address Range* IPv4 Address Range* I22.16.1.10-172.16.1.20 Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1. 255.255.0 Description Allow Overrides Allow Overrides Override (0)	ddress conflicts in case of object	

步骤 7.创建AnyConnect软件包。导航到对象(Objects)>对象管理(Object Management)> VPN > AnyConnect文件(AnyConnect File)。单击Add AnyConnect File,提供软件包名称,从<u>Cisco</u>

<u>Software Download</u>下载软件包,然后选择<u>Anyconnect Client Image</u>文件类型。



步骤 8导航到证书对象(Certificate Objects)>对象管理(Object Management)> PKI >证书注册(Cert Enrollment)。单击Add Cert Enrollment,提供名称,在Enrollment Type中选择Self Signed Certificate。点击Certificate Parameters选项卡并提供CN。

Overview Analysis	Policies Devices Obje	cts AMP Intelligence		Deploy 🍳 Sy
Object Management	Intrusion Rules			
Cert Enrollment A certificate enrollment of activities occur in your Pri	ject contains the Certification vate Key	Authority (CA) server information and 4	nrollment parameters that are required for creating G	Add Cert Enrollment
Access List				Туре
Application Filters	Name*	vpn-cert		Self Signed Ce
Y AS Path	Description			
🝰 Community List	CA Informatic	Cartificato Darametera - Kou	Reverstion	
Distinguished Name	CA Informatio	Certificate Parameters Key	Revocation	
DNS Server Group	Enrollment Type	Self Signed Certificate	*	
Ga Elex Config	Common Na	ne (CN) is mandatory for self-signed or	rtificate that is used in Remote Access VPN. To	
Geolocation	- configure CN	please navigate to 'Certificate Parame	ters' tab.	
Interface				
陷 Key Chain				
Network				
a 🖗 PKI				
Cert Enrollment				
External Cert Gro	lups			
Internal CA Grou	DS			
Internal CAs				
🔚 Internal Cert Gro	ups			
Internal Certs		_		
Trusted CA Group	Allow Overrides			
Trusted CAs				
Policy List				
Ø <sup>29</sup> Port			Save Cancel	Displaying 1 - 1 of 1 rows 🛛 🐇

ŀ	dd Cert Enrollme	nt						? ×
	Name*	vpr	-cert					
	Description							
	CA Information	Certific	ate Parameters	Кеу	Revocation			
	Include FQDN:		Use Device Hostna	me as f	-QDN	*	•	
	Include Device's IP	Address:	10.48.26.99					
	Common Name (CN	1):	vpn-cert.example.	com				
	Organization Unit (C	DU):						
	Organization (O):		example					
	Locality (L):							
	State (ST):		Krakow					
	Country Code (C):		PL					
	Email (E):							
	Include Device's	Serial Nu	mber					
	Allow Overrides							
						Save		Cancel

### 步骤 9启动远程访问VPN向导。导航到设备> VPN >远程访问,然后单击添加。

Overview Analysis	Policies	Devices Objects	AMP	Intelligence				Deploy	<b>e</b> ,	System	Help 🔻	admin 🔻
Device Management	NAT	VPN • Remote Access	QoS	Platform Settings	FlexConfig	Certificates						
											0 /	Add
Name				Status			Last Modified					
No configuration available Add a new configuration												

步骤 10提供名称,选中SSL as VPN Protocol,选择用作VPN集中器的FTD,然后点击Next。

Remote Access VPN Policy Wizard	
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary	
Targeted Devices and Protocols         This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.         Name:*       EmployeeVPN         Description:       VPN Protocols:         VPN Protocols:       SSL         Targeted Devices:       Selected Devices         Search       # 192.168.15.11         192.168.15.11       # 192.168.15.11	<section-header><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></section-header>
	Back Next Cancel

步骤 11提供Connection Profile名称,选择Authentication/Accounting Servers,选择之前配置的地 址池,然后单击Next。

✤ 注:请勿选择授权服务器。它为单个用户触发两次访问请求(一次使用用户密码,第二次使用 密码cisco)。

Connection Profile     AnyConnect     Access & Certificate     Summary     Connection Profile:     Second Profile:     Second Profile:     Connection Profile:     Second Profile:     Second Profile:     Connection Profile:     Second Profile:     Second Profile:     Connection Profile:     Second Profile:     Connection Profile:     Second Profile:
Connection Profile: Connection Profile specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how addresses are assigned. They also include user attributes, which are defined in group policies. Connection Profile Name:* 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, Authorization & Accounting (AAA): Spacify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VDN connections.
Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.
Authentication Methods AAAA Only
Authentication Server:* ISE V . (Realm or RADIUS)
Authorization Server: Use same authentication server 🗸 🕼 (RADIUS)
Accounting Server: ISE 🔍 🕼 (RADIUS)
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 (RADIUS only) 👔
Use DHCP Servers
U use IP Address Pools
Invia address VPR-172-Pool
IPv6 Address
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 Palicy:* DfHtGrpPalicy V G Group Palicy:*
Back Next Cancel

步骤 12选择之前配置的AnyConnect软件包,然后单击Next。

Remote Access VPN Policy Wizard
Policy Assignment 2 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary
Remote       AnyConnect         User       AnyConnect         Internet       Outside         User       Inside         Corporate Resources         Internet       Inside         Outside       Upil Device         Inside       Corporate Resources         Inside       Inside         Inside       Corporate Resources         Inside       Inside         Inside       Inside </td
Download AnyConnect Client packages from Cisco Software Download Center. Show Re-order buttons
AnyConnect File Object Name AnyConnect Client Package Name Operating System
AC47 anyconnect-win-4.7.01076-webdeploy-k9 Windows
Back Next

步骤 13选择VPN流量预期来自的接口,选择Certificate Enrollment(之前配置的证书注册),然后 单击Next。

Remote Access VPN Policy Wizard			
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary			
Network Interface for Incoming VPN Access Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections. Interface group/Security Zone: ZONE-OUTSIDE Contended of the DTLS on member interfaces			
Device Certificates Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VDN gateway Certificate Enrollment:* Vpn-cert Enroll the selected certificate object on the target devices			
Access Control for VPN Traffic All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypase decrypted traffic from the Access Control Policy. Physic access Control Policy for decrypted traffic (sysopt permit-vpn) Physic option bypases the Access Control Policy imprection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.			
	Back	Next	Cancel

步骤 14检查摘要页面,然后单击Finish。



### 步骤 15将配置部署到FTD。单击Deploy并选择用作VPN集中器的FTD。

Overview Analysis Policies Devic	Ces Objects AMP Intelligence			Deploy 🍳 System Help 🔻 admin 🔻
Device Management NAT VPN >	Remote Access QoS Platform Settings FlexC	onfig Certificates		
EmployeeVPN	Deploy Policies Version:2020-02-02 09:15 PM			? X Save Save
Enter Description	Device	Inspect Interruption Type	Group Current Version	Policy Assignments (1)
Connection Profile Access Interfac		No FTD	2020-02-02 09:10 PM	
				0
Name				
DefaultWEBVPNGroup				/ 8
EmployeeVPN				48
Lingity Govern				<i>~</i> 0
	Selected devices: 1		Deploy Cance	el

#### ISE

步骤1:运行状态更新。导航到Administration > System > Settings > Posture > Updates。

Posture Updates	
<ul> <li>Web</li> </ul>	○ Offline
* Update Feed URL	https://www.cisco.com/web/secure/spa/posture-update.xml Set to Default
Proxy Address	(i)
Proxy Port	HH MM SS
Automatically che	eck for updates starting from initial delay 20 🔻 49 🔻 18 🔻 every 2 hours 🤅
Save	date Now Reset

Vpdate Information	
Last successful update on	2020/02/02 20:44:27(j)
Last update status since ISE was started	Last update attempt at 2020/02/02 20:44:27 was successful 👔
Cisco conditions version	257951.0.0.0
Cisco AV/AS support chart version for windows	227.0.0.0
Cisco AV/AS support chart version for Mac OSX	148.0.0.0
Cisco supported OS version	49.0.0.0

第二步:上传合规性模块。导航到Policy > Policy Elements > Results > Client Provisioning > Resources。单击Add并选择Agent resources from Cisco site

Download Remote Resources	×
Name 🔺	Description
AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2
AnyConnectComplianceModuleOSX 4.3.972.4353	AnyConnect OSX Compliance Module 4.3.972.4353
AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance Module 3.6.11682.2
AnyConnectComplianceModuleWindows 4.3.1053.6145	AnyConnect Windows Compliance Module 4.3.1053.6145
CiscoTemporalAgentOSX 4.8.03009	Cisco Temporal Agent for OSX With CM: 4.3.972.4353
CiscoTemporalAgentWindows 4.8.03009	Cisco Temporal Agent for Windows With CM: 4.3.1053.6145
ComplianceModule 3.6.11428.2	NACAgent ComplianceModule v3.6.11428.2 for Windows
MACComplianceModule 3.6.11428.2	MACAgent ComplianceModule v3.6.11428.2 for MAC OSX
MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Ab
MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3
MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Rele
MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 rele
MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 rele
MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 rele
MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE 1.2 Pat
For AnyConnect software, please download from http://cisco.com	/go/anyconnect. Use the "Agent resource from local disk" add
option, to import into ISE	
	Save

第三步:从<u>Cisco Software Download</u>下载AnyConnect,然后将其上传到ISE。导航到Policy > Policy Elements > Results > Client Provisioning > Resources。

单击Add,然后选择Agent Resources From Local Disk。在Category下选择Cisco Provided Packages,从本地磁盘中选择AnyConnect package,然后单击Submit。

Agent Resources From Local Disk > Agent Resources From Local Disk Agent Resources From Local Disk													
Category	Cisco Provided Packages • (i)												
	Browse anyconnect-win-4.7.01076-webdeploy-k9.pkg												
	AnyConnect Uploaded Resources	5											
	Name 🔺	Туре	Version	Description									
	AnyConnectDesktopWindows 4.7.10	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secure Mobility Clie									



第四步:创建AnyConnect终端安全评估配置文件。导航到Policy > Policy Elements > Results > Client Provisioning > Resources。

单击Add并选择AnyConnect Posture Profile。填写名称和状态协议。

在\*Server name rules put\*下,将任何虚构IP地址放在Discovery host下。

ISE Posture Agent Profile Settings > AC_Posture_Profile											
* Name: AC Posture Profile Description											
Parameter	Value	Notes	Description								
PRA retransmission time 120 secs		inces	This is the agent retry period if there is a Passive Reassessment communication failure								
Discovery host	1.2.3.4		The server that the agent should connect to								
* Server name rules		need to be blank by default to force admin to enter a value. *** means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com								
Call Home List		List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port Example: IPaddress/FQDN.Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.								
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached								

第五步:导航到Policy > Policy Elements > Results > Client Provisioning > Resources并创建 AnyConnect Configuration。单击Add并选择AnyConnect Configuration。选择AnyConnect Package,提供配置名称,选择Compliance Module,选中Diagnostic and Reporting Tool,选择 Posture Profile,然后单击Save。

* Select AnyConnect Package	AnyConnectDesktopWindows 4.7.1076.0 👻	
* Configuration Name	AC CF 47	]
Description		
Description	Value	Notes
* Compliance Module	AnyConnectComplianceModuleWindows 4.3.1012.6 -	

#### AnyConnect Module Selection ISE Posture VPN Network Access Manager Web Security AMP Enabler ASA Posture Network Visibility Umbrella Roaming Security Start Before Logon Diagnostic and Reporting Tool

#### **Profile Selection**

		-
* ISE Posture	AC_Posture_Profile 🔹	
VPN	<b>T</b>	
Network Access Manager	<b>T</b>	
Web Security	×	
AMP Enabler	<b>*</b>	
Network Visibility	<b>T</b>	
Umbrella Roaming Security	<b>*</b>	
Customer Feedback	<b>*</b>	

第六步:导航到Policy > Client Provisioning并创建Client Provisioning Policy。单击Edit,然后选择 Insert Rule Above,提供名称,选择OS,然后选择在上一步中创建的AnyConnect Configuration。

cisco Identi	ity Services Engine	Home	Context Visi	bility	Operations	▼Policy	•	Administration			License Warning 🔺	Q,	0	•	Φ.
Policy Sets	Profiling Posture	Client Provisi	oning + Polic	y Elemen	ts										
Client Provis Define the Clier For Agent Confi For Native Supp	sioning Policy nt Provisioning Policy to iguration: version of age plicant Configuration: wi	determine wh: nt, agent profil izard profile an	at users will rece e, agent complia d/or wizard. Drag	ive upon l nce modu and drop	login and user si ile, and/or agent rules to change	ession initiati customizatio the order.	on: n pac	ikage.							
•	Rule Name		Identity Group	s	Operating Sys	tems		Other Conditions		Results					
	AC_47_Win	If	Any	and	Windows All	8	and	Condition(s)	then	AC_CF_47				Edit   •	
	IOS	lf	Any	and	Apple iOS All	а	and	Condition(s)	then	Cisco-ISE-NSP				Edit   •	
	Android	lf	Any	and	Android	а	and	Condition(s)	then	Cisco-ISE-NSP				Edit   •	
	Windows	If	Any	and	Windows All	а	ind	Condition(s)	then	CiscoTemporalAgentWi ndows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP				Edit   🕶	
	MAC OS	И	Any	and	Mac OSX	а	and	Condition(s)	then	CiscoTemporalAgentO SX 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE- NSP				Edit   •	
	Chromebook	Ц	Any	and	Chrome OS A	ll a	ind	Condition(s)	then	Cisco-ISE-Chrome- NSP				Edit   •	

步骤 7.在Policy > Policy Elements > Conditions > Posture > Anti-Malware Condition下创建安全评 估条件。在本示例中,使用预定义的"ANY\_am\_win\_inst"。

.

cisco Identity Services Engine	Home ► Context Visibility	→ Operations ▼Policy	Administration	▶ Work Centers
Policy Sets Profiling Posture	Client Provisioning   Policy Eleme	nts		
Dictionaries - Conditions + Res	sults			
Library Conditions Smart Conditions Time and Date Profiling Posture Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition	Anti-Malware Conditions	➤ Delete     Description     Any AM installation chec     Any AM definition chec     Any AM definition chec     Any AM definition chec	ack on Wi k on Wind ack on Mac k on Mac	
Compound Condition Disk Encryption Condition				
File Condition Firewall Condition				

步骤 8导航到Policy > Policy Elements > Results > Posture > Remediation Actions并创建Posture Remediation。在本例中,它被跳过。补救操作可以是文本消息。

步骤 9 导航到Policy > Policy Elements > Results > Posture > Requirements并创建Posture Requirements。使用预定义要求Any\_AM\_Installation\_Win。

dentity Services Engine	Home	Operations   Policy	Administration     Work Centers		License Warning 🔺 🔍	. 0 0	ø
Policy Sets Profiling Posture	Client Provisioning Policy Elements	3					
Dictionaries + Conditions - Re	esults						
	0						
Authentication					*		Q
	Requirements						
<ul> <li>Authorization</li> </ul>	Name	Operating Systems	Compliance Module	Posture			
- Destiling	Wessage Text Only	Conditions	Remediation Actions			Edit   🕶	-
• Proming	Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_av_mac_def	then	
✓ Posture	AnyAVDefRemediationMa c					Edit   🔻	
	Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_inst	then	
Remediation Actions	Message Text Only					Edit   🔻	
Requirements	Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_def	then	
Client Provisioning	AnyASDefRemediationMa c					Edit   🔻	
	Any_AM_Installation_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_inst	then	
	Message Text Only					Edit   🕶	
	Any_AM_Definition_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_def	then	
	AnyAMDefRemediationWi n					Edit   🕶	
	Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_inst	then	
	Message Text Only					Edit   •	
	Any AM Definition Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_def	then	
	AnyAMDefRemediationM					Edit   🕶	-

步骤 10在Policies > Posture下创建状况策略。使用适用于Windows操作系统的任何防恶意软件检查 的默认安全评估策略。

aha) cisco	dentity S	ervices Engine	Home	ty + Operations	* Policy	+ Administrati	on	Work Centers							License Warning 🔺	્ ૭	•	0
Pol	icy Sets P	rofiling Posture	e Client Provisioning + Poli	oy Elements														
Post	ure Policy e the Postur	e Policy by config	uring rules based on operating sy	stem and/or other co	nditions.										-			ρ
	Status	Policy Options	Rule Name	Identity Groups	Opera	ting Systems		Compliance Module		Posture Type		Other Conditions		Requirements				-
	0	Policy Options	Default_AntiMalware_Policy If _Mac	Any	and Mac OS	× °	nd 43	k or later	and A	AnyConnect	and		then	Any_AM_Installation_ Mao			Edit	•
	0	Policy Options	Default_AntiMalware_Policy If _Mac_temporal	Any	and Mac OS	x a	nd 43	k or later	and 1	Temporal Agent	and		then	Any_AM_Installation_ Mac_temporal			Edit	•
		Policy Options	Default_AntiMalware_Policy II _Win	Any	and Windows	All a	nd <b>4</b> 3	k or later	and A	AnyConnect	and		then	Any_AM_Installation_ Win			Edit	-
	0	Policy Options	Default_AntiMalware_Policy If _Win_temporal	Any	and Windows	All a	nd 43	k or later	and 1	Temporal Agent	and		then	Any_AM_Installation_ Win_temporal			Edit	•
	0	Policy Options	Default_AppVis_Policy_Mac If	Any	and Mac OS	×	nd 43	c or later	and A	AnyConnect	and		then	Default_AppVis_Requ irement_Mac			Edit	•

步骤 11导航到Policy > Policy Elements > Results > Authorization > Downloadable ACL,并为不同 的安全评估状态创建DACL。

在本例中:

- 状态未知DACL 允许流量到达DNS、PSN以及HTTP和HTTPS流量。
- 安全评估不合规的DACL 拒绝访问私有子网并仅允许互联网流量。
- Permit All DACL 允许所有流量进入Posture Compliant Status。

Downloadable A	CL List > PostureNonCompliant1
Downloadabl	e ACL
* Name	PostureUnknown
Description	
IP version	© IPv4 C IPv6 C Agnostic ⊕
* DACL Content	1234567       permit udp any any eq domain         8910111       permit ip any host 192.168.15.14         2131415       permit icp any any eq 80         1617181       permit icp any any eq 443         9202122       2324252         6272829       3031323         3343536       3738394

#### Downloadable ACL List > New Downloadable ACL

Downloadabl	e ACL
* Name	PostureNonCompliant
Description	
IP version	€ IPv4 C IPv6 C Agnostic (j)
* DACL Content	1234567 deny jg any 10.0.0.0 255.0.0.0
	8910111 deny jg any 172, 16,0,0 255,254,0,0,0 2131415 denv in pay 192,16,0,0 255,255,0,0
	1617181 permit in any any
	9202122
	2324252
	6272829
	3031323
	3343536
	3738394

Downloadable A	CL List > New Downloadable ACL	
* Name	Permit All	
Description		
Description		
IP version	● IPv4 O IPv6 O Agnostic ①	
* DACL Content	123456 permit jg any any 7891011	
	121314 151617	
	181920	
	242528	
	303132	
	333430	I
	► Check DACL Syntax	i

步骤 12为状况未知、状况不合规和状况合规状态创建三个授权配置文件。为此,请导航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。在Posture Unknown配置文件中,选择Posture Unknown DACL,选中Web Redirection,选择Client Provisioning,提供重定向ACL名称(在FTD上配置)并选择门户。

Authorization Profiles > New A Authorization Profile	uthorization Profile		
* Name	FTD-VPN-Redirect		
Description			1
* Access Type	ACCESS_ACCEPT	<b>*</b>	
Network Device Profile	ditto Cisco 👻 🕀		
Service Template			
Track Movement	_ (i)		
Passive Identity Tracking			
<ul> <li>Common Tasks</li> </ul>			
🔽 DACL Name	PostureUn	nknown 📀	
Web Redirection (CWA, MDI	M, NSP, CPP)	fyusifovredirect	Value ut Provisioning Portal (default)
Attributes Details			
DACLE = PostureUnknown cisco-av-pair = url-redirect-acl=fyusifovred cisco-av-pair = url-redirect=https://ip:por	direct rt/portal/gateway?sessionId=Sessio	nIdValue&portal=27b1bc30-2e58-11e9-98fb-	0050568775a3&action=cpp

在Posture NonCompliant配置文件中,选择DACL以限制对网络的访问。

#### Authorization Profiles > New Authorization Profile

Authorization Profile	
* Name	FTD-VPN-NonCompliant
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	dtt: Cisco 👻 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
▼ Common Tasks	
DACL Name	PostureNonCompliant 📀

#### Attributes Details

Access Type = ACCESS\_ACCEPT DACL = PostureNonCompliant

# 在Posture Compliant配置文件中,选择DACL以允许对网络的完全访问。

#### Authorization Profiles > New Authorization Profile

Authorization Profile	
* Name	PermitAll
Description	
* Access Type	ACCESS_ACCEPT *
Network Device Profile	🗰 Cisco 💌 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
<ul> <li>Common Tasks</li> </ul>	
DACL Name	PermitAll
▼ Attributes Details	
Access Type = ACCESS_ACCEPT	
Dacl = Permitali	line in the second s

步骤 13在Policy > Policy Sets > Default > Authorization Policy下创建授权策略。As条件使用 Posture Status和VNP TunnelGroup Name。

alada id	entity Serv	rices Engine Home → C	ontext Vis	ibility	<ul> <li>Operations</li> </ul>		Administration	Work Ce	nters		Lic	ense Warning 🔺	Q	Θ	•	3
Policy S	ets Profi	ling Posture Client Provisionin	g 🕨 Po	licy Eler	nents		,									
	Ø	Default	Default p	olicy set							Def	ault Network Acces	s	× • +	43	
> Autr > Autr > Autr	entication orization F orization F	Policy (3) Policy - Local Exceptions Policy - Global Exceptions														
▲ Auth	iorization F	Policy (18)														
									Results							
+	Status	Rule Name	Condit	ions					Profiles	S	ecurity Groups	÷		Hits	Actions	5
Searc	h															)
				Ê;	Session-Posture	Status EQUA	ALS Compliant									1
	$\odot$	FTD-VPN-Posture-Compliant	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000/A EmployeeVP	ASA/PIX7x-Tunnel-Gr 'N	roup-	( × PermitAII	+	Select from list	٣	+	4	¢	
				ĥ	Session-Posture	Status EQUA	ALS NonCompliant									
	0	FTD-VPN-Posture-NonCompliant	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000/A EmployeeVP	NSA/PIX7x-Tunnel-Gr	roup-	×FTD-VPN-NonCompliant	+	Select from list	×	+	0	¢	
				ĥ	Session-Posture	Status EQUA	ALS Unknown			_			_			
	$\odot$	FTD-VPN-Posture-Unknown	AND	ŝ	Cisco-VPN3000 Name EQUALS	CVPN3000/A EmployeeVP	ASA/PIX7x-Tunnel-Gr 'N	roup-	× FTD-VPN-Redirect	+	Select from list	3	+	9	\$	

# 验证

使用本部分可确认配置能否正常运行。

在ISE上,第一个验证步骤是RADIUS实时日志。导航到操作> RADIUS实时日志。此时,用户 Alice已连接,且已选择预期的授权策略。

cisco source	tity Services Engine	Home + Co	ntext Visibility	* Operations	Policy Ad	dministration + Work Ce	nters							License Wan	ning 🔺 🔍	
+ RADIUS	Threat-Centric NAC Li	ive Logs + TAC	ACS + Troub	leshoot + Ad	aptive Network Control	Reports										
Live Logs	Live Sessions															
		Misconfigured S	upplicants 0	N	lisconfigured Network	Devices ()	RADIUS Dro	ops O	Cli	ent Stopped Res	ponding ()		Repeat	Counter ()		
		0			0		0			0				0		
										Refr	sh Never		Show Lates	t 20 records	Within Last 3	hours
C Refrest	h 🛛 Reset Repeat Co	unts 📕 Expor	t To •							Refr	Ish Never		Show Lates	t 20 records	Within Last 3	Filter • Q
C Refresh	h O Reset Repeat Co	unts 🛃 Expor	t To • Details	Repeat	identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Authorizati	IP Address		Show Lates	Device Port	Within Last 3	Filter • •
C Refrest Time	h OReset Repeat Co	unts 🛓 Expor	t To • Details	Repeat	Identity	Endpoint ID Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Authorizati	IP Address	•	Network Device	Device Port	Within Last 3 Identity Group	Filter • • • • • • • • • • • • • • • • • • •
C Refresh Time X Feb	<ul> <li>Reset Repeat Core</li> <li>03, 2020 07:13:31.92</li> </ul>	unts 🛓 Expor	Details	Repeat	Identity Identity alice@training.e	Endpoint ID Endpoint ID 00:00:29:50:5A:98	Endpoint Pr Endpoint Pre Windows10	Authenticat Authenticatik Default >>	Authorizati Authorization Default >>;	Authorizati Authorizatior FTD-VPN-R	IP Address IP Address IP Address 172.16.1.10		Network Device	Device Port Device Port	Identity Group	Filter • • • • • • • • • • • • • • • • • • •
C Refrest Time X Feb Feb	<ul> <li>Reset Repeat Core</li> <li>03, 2020 07:13:31.92</li> <li>03, 2020 07:13:29.74</li> </ul>	unts 🛓 Expor	t To + Details	Repeat	Identity Identity alice@training.e #ACSACL#-IP-P	Endpoint ID Endpoint ID 00:00:29:50:54:90	Endpoint Pr Endpoint Pre Windows10	Authenticat Authenticatk Default >>	Authorizati Authorization Default >>	Authorizati Authorizatior FTD-VPN-R	IP Address IP Address IP Address 172.16.1.10		Show Lates Network Device Network Device	Device Port	Identity Grou	Filter • • • • • • • • • • • • • • • • • • •

授权策略FTD-VPN-Posture-Unknown匹配,因此会将FTD-VPN-Profile发送到FTD。

### **Overview**

Event	5200 Authentication succeeded	
Username	alice@training.example.com	
Endpoint Id	00:0C:29:5C:5A:96 ⊕	
Endpoint Profile	Windows10-Workstation	
Authentication Policy	Default >> Default	
Authorization Policy	Default >> FTD-VPN-Posture-Unknown	
Authorization Result	FTD-VPN-Redirect	

# **Authentication Details**

Source Timestamp	2020-02-03 07:13:29.738
Received Timestamp	2020-02-03 07:13:29.738
Policy Server	fyusifov-28-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

## 状态待处理。

"结果"部分显示哪些属性发送到FTD。

tesult	
Class	CACS:000000000000005e37c81a:fyusifov-26-3/368560500/45
cisco-av-pair	url-redirect-acl=fyusifovredirect
cisco-av-pair	url-redirect=https://fyusifov-26-3.example.com:8443/portal /gateway?sessionId=0000000000000005e37c81a& portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp& token=0d90f1cdf40e83039a7ad8a226803112
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PostureUnknown-5e37414d
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base and Apex license consumed

在FTD上,为了验证VPN连接,请通过SSH连接到设备,执行system support diagnostic-cli,然后 执行show vpn-sessiondb detail anyconnect。从此输出中,验证从ISE发送的属性是否应用于此 VPN会话。

```
<#root>
fyusifov-ftd-64#
show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username
            : alice@training.example.com
Index
            : 12
Assigned IP : 172.16.1.10
            Public IP
                       : 10.229.16.169
            : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
License
            : AnyConnect Premium
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Encryption
Hashing
            : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx
            : 15326
                                     Bytes Rx
                                                 : 13362
Pkts Tx
            : 10
                                     Pkts Rx
                                                  : 49
Pkts Tx Drop : 0
                                     Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy
Tunnel Group : EmployeeVPN
Login Time
           : 07:13:30 UTC Mon Feb 3 2020
            : 0h:06m:43s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                     VLAN
                                                   : none
Audt Sess ID : 000000000000005e37c81a
Security Grp : none
                                     Tunnel Zone : 0
```

AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 12.1 Public IP : 10.229.16.169 Encryption : none Hashing : none TCP Src Port : 56491 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes : win Client OS Client OS Ver: 10.0.18363 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7663 Bytes Rx : 0 Pkts Tx : 5 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 12.2 Assigned IP : 172.16.1.10 Public IP : 10.229.16.169 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 56495 TCP Dst Port : 443 : userPassword Auth Mode Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes : Windows Client OS Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7663 Bytes Rx : 592 Pkts Tx : 5 Pkts Rx : 7 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d DTLS-Tunnel: Tunnel ID : 12.3 Assigned IP : 172.16.1.10 Public IP : 10.229.16.169 : AES256 Encryption Hashing : SHA1 Ciphersuite : DHE-RSA-AES256-SHA UDP Src Port : 59396 Encapsulation: DTLSv1.0 : userPassword UDP Dst Port : 443 Auth Mode Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 0 Bytes Rx : 12770 Pkts Tx : 0 Pkts Rx : 42 Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

ISE Posture: Redirect URL : https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=00000000000000005e37c83 Redirect ACL : fyusifovredirect 可以验证客户端调配策略。导航到操作>报告>端点和用户>客户端调配。

deaths Identity Services Engine	Home + Context Visibili	ty Operations + Policy	Administration      Work Centers			License Wa	ming 🔺 🔍 😝 🧑 Ó
+ RADIUS Threat-Centric NAC Lin	e Logs + TACACS + Tro	ubleshoot + Adaptive Network	Control Reports				
Export Summary My Reports	Client Provisioning From 2020-02-03 00:00:00 Reports exported in last 7	0.0 to 2020-02-03 08:14:07.0 days 0				+ My Report	Export To • O Schedule
- Reports							Filter • CRefresh ••
+ Audit	Logged At	Server	Event	Identity	Endpoint ID	IP Address	Client Provisioning Pol
Device Administration	Today 💌 🗙			Identity	Endpoint ID		
Diagnostics	2020-02-03 08:06:4	fyusifov-26-3	Client provisioning succeeded	alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	AC_47_Win
Endpoints and Users     Authentication Summary     Client Provisioning     Current Active Sessions	<u> </u>					Rows/Page 1	1 📩 1 Total Rows

# 可以检查从AnyConnect发送的状况报告。导航到操作>报告>端点和用户>按端点进行状态评估。

dentity Services Engine	Home   Context Visibility   Operations   Policy	Administration     Work Centers			License Warning 🔺	
RADIUS Threat-Centric NAC L	ive Logs + TACACS + Troubleshoot + Adaptive Network	Control Reports				
Export Summary	Posture Assessment by Endpoint  From 2020-02-03 00:00:00 0 to 2020-02-03 08:15:48.0 Reports exported in last 7 days 0				🕈 My Reports 🖾 t	Export To
- Reports					<b>T</b> =	
▶ Audit	Logged At Status De	tails PRA Action	Identity	Endpoint ID	IP Address	Endpoint OS
Device Administration	× <sub>Todav</sub> • × •		Identity	Endpoint ID		Endpoint OS
▶ Diagnostics	2020-02-03 08:07:5 🔽	N/A.	alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	Windows 10 Professional
▼ Endpoints and Users						
Authentication Summary					Rows/Page 1	I lotal Rows
Client Provisioning						
Current Active Sessions						
External Mobile Devic						
Manual Certificate Pro						
PassiveID						
Posture Assessment by						
Posture Assessment by						

## 要查看状态报告的更多详细信息,请单击Details。

الاستان، Identity Services Engine	
Posture More Detail Assessment	
From 2020-01-04 00:00:00.0 to 2020-02-03 08:13:36.0 Generated At: 2020-02-03 08:13:37.37	
Client Details	
Username	alice@training.example.com
Mac Address	00:0C:29:5C:5A:96
IP address	172.16.1.10
Location	All Locations
Session ID	00000000000c0005e37c81a
Client Operating System	Windows 10 Professional 64-bit
Client NAC Agent	AnyConnect Posture Agent for Windows 4.7.01076
PRA Enforcement	0
CoA	Received a posture report from an endpoint
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEnabled
System Name	DESKTOP-IE3556M
System Domain	n/a

在ISE上收到报告后,安全评估状态会更新。在本示例中,安全评估状态是合规的,CoA推送使用一

# 组新属性触发。

C Refresh O Reset Repeat Counts 🕹 Export To -								▼ Filter	- 0-						
	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Authorizati	IP Address	Network Device	Device Port	Identity Group	Posture S
×		•			Identity	Endpoint ID	Endpoint Prc	Authenticatic	Authorization	Authorization	IP Address	Network Device	Device Port	Identity Group	Posture
	Feb 03, 2020 08:07:52.05		0			10.229.16.169				PermitAccess	]	FTD			Compliar
	Feb 03, 2020 08:07:50.03	0	0	0	alice@training.e	00:0C:29:5C:5A:96	Windows10	Default >>	Default >>	FTD-VPN-R	172.16.1.10				Compliar
	Feb 03, 2020 07:13:29.74		0		#ACSACL#-IP-P							FTD			
	Feb 03, 2020 07:13:29.73		à		alice@training.e	00:0C:29:5C:5A:98	Windows10	Default >>	Default >>	FTD-VPN-R		FTD		Workstation	Pending

Records Shown: 4

Last Updated: Mon Feb 03 2020 09:10:20 GMT+0100 (Central European Standard Time)

verview	
Event	5205 Dynamic Authorization succeeded
Username	
Endpoint Id	10.55.218.19 🕀
Endpoint Profile	
Authorization Result	PermitAll

uthentication Details	
Source Timestamp	2020-02-03 16:58:39.687
Received Timestamp	2020-02-03 16:58:39.687
Policy Server	fyusifov-28-3
Event	5205 Dynamic Authorization succeeded
Endpoint Id	10.55.218.19
Calling Station Id	10.55.218.19
Audit Session Id	00000000000e0005e385132
Network Device	FTD
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.15.15
Authorization Profile	PermitAll
Posture Status	Compliant
Response Time	2 milliseconds

Other Attributes	
ConfigVersionId	21
Event-Timestamp	1580749119
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	af49œ55-d55o-4778-ad40-b03ea12924d2
CoASourceComponent	Posture
CoAReason	posture status changed
CoAReason CoAType	posture status changed COA-push
CoAReason CoAType Network Device Profile	posture status changed COA-push Cisco
CoAReason CoAType Network Device Profile Location	posture status changed COA-push Cisco Location#All Locations
CoAReason CoAType Network Device Profile Location Device Type	posture status changed         COA-push         Cisco         Location#All Locations         Device Type#All Device Types
CoAReason CoAType Network Device Profile Location Device Type IPSEC	posture status changed         COA-push         Cisco         Location#All Locations         Device Type#All Device Types         IPSEC#ls IPSEC Device#No
CoAReason CoAType Network Device Profile Location Device Type IP SEC Device IP Address	posture status changed         COA-push         Cisco         Location#All Locations         Device Type#All Device Types         IPSEC#ls IPSEC Device#No         192.168.15.15

在FTD上验证是否已为VPN会话删除新的重定向ACL和重定向URL,并已应用PermitAll DACL。

<#root>								
fyusifov-ftd-	-64#							
show vpn-sessiondb detail anyconnect								
Session Type:	Session Type: AnyConnect Detailed							
Username	:							
alice@training.example.com								
Index Assigned IP Protocol	: 14 : 172.16.1.10 : AnyConnect-Parent SSL-T	Public IP unnel DTLS-Tur	: 10.55.218.19 mel					

License : AnyConnect Premium : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256 Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1 Hashing : 53990 Bytes Rx : 23808 Bytes Tx Pkts Tx Pkts Rx : 120 : 73 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : EmployeeVPN : 16:58:26 UTC Mon Feb 3 2020 Login Time : 0h:02m:24s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 000000000000005e385132 Security Grp : none Tunnel Zone : 0 AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 14.1 Public IP : 10.55.218.19 Encryption : none Hashing : none TCP Src Port : 51965 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes Client OS : win Client OS Ver: 10.0.18363 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7663 Bytes Rx : 0 Pkts Tx : 5 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 14.2 Assigned IP : 172.16.1.10 Public IP : 10.55.218.19 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 51970 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7715 Bytes Rx : 10157 Pkts Tx : 6 Pkts Rx : 33 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PermitAll-5e384dc0 DTLS-Tunnel: Tunnel ID : 14.3 Assigned IP : 172.16.1.10 Public IP : 10.55.218.19 Encryption : AES256 Hashing : SHA1 Ciphersuite : DHE-RSA-AES256-SHA UDP Src Port : 51536 Encapsulation: DTLSv1.0 UDP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes

Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 38612 Bytes Rx : 13651 Pkts Tx : 62 Pkts Rx : 87 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name :

#ACSACL#-IP-PermitAll-5e384dc0

fyusifov-ftd-64#

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。

有关详细的终端安全评估流程和对AnyConnect和ISE进行故障排除,请检查以下链接: <u>高级版和高</u> 级版2.2的ISE终端安全评估样式比较。</u>

• Spilt隧道

当配置了备用隧道时,常见问题之一。在本示例中,使用默认组策略,通过隧道传输所有流量。如 果仅通过隧道传输特定流量,则AnyConnect探测器(enroll.cisco.com和发现主机)除了流向ISE和其 他内部资源的流量外,还必须通过隧道。

要检查FMC上的隧道策略,首先检查哪个组策略用于VPN连接。导航到设备> VPN远程访问。

Overview Analysis Policies Devices Objects	AMP Intelligence		Deploy 🍳 System Help 🔻 admin 🔻
Device Management NAT VPN > Remote Access	QoS Platform Settings FlexConfig	Certificates	
EmployeeVPN Enter Description			Save Save
Connection Profile Access Interfaces Advance	1		Policy Assignments (1)
			0
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy	/ 6
EmployeeVPN	Authentication: ISE (RADIUS) Authorization: ISE (RADIUS) Accounting: ISE (RADIUS)	DftGrpPolicy	/ 6

然后,导航到Objects > Object Management > VPN > Group Policy,然后点击Group Policy为 VPN配置。



・ 身份NAT

另一个常见问题是,当VPN用户的返回流量使用错误的NAT条目被转换时。要解决此问题,必须按 照适当的顺序创建身份NAT。

首先,检查此设备的NAT规则。导航到设备> NAT,然后单击添加规则以创建新规则。

Ove	Overview Analysis Policies Devices Objects AMP Intelligence									Deploy 🧛 S	ystem Help 🔻	admin 🔻
Dev	ce Management	NAT	VPN VQ0	6 Platform Setti	ings FlexConfig	Certificates						
FTI	0_11									\lambda Show Warnings	Save	🔀 Cancel
Enter	Description											
	_										📑 Policy As	signments (1)
Rule	5											
台 Filt	# Fiter by Device O Add Rule											
						Original Packet			Translated Packet		۱	
#	Direction	Туре	Source Interface Ob	Destination Interface Ob	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
V NAT Rules Refore												

在打开的窗口中,在Interface Objects选项卡下,选择Security Zones。在本示例中,NAT条目是从 ZONE-INSIDE到ZONE-OUTSIDE创建的。

Add NAT Rule						? :	
NAT Rule:	NAT Rule: Manual NAT Rule Type: Static		Insert:	In Category	VAT Rules Befo	ore 💌	
Type:			✓ Enable				
Description:	Description:						
Interface Objects	Translation PA	T Pool Advand	ced				
Available Interface C	)bjects 🖒		Source Interface Object	ts (1)	Destination Interface	e Objects (1)	
Search by name			ZONE-INSIDE	ũ	ZONE-OUTSIDE	ii ii	
ZONE-INSIDE	ZONE-INSIDE						
ZONE-OUTSIDE	ZONE-OUTSIDE						
		Add to Destination					
						OK Cancel	

在Translation选项卡下,选择原始和转换的数据包详细信息。因为它是身份NAT,所以源和目标保 持不变:

Edit NAT Rule										? ×
NAT Rule:	AT Rule: Manual NAT Rule 💌 Insert:					In Category	▼ NAT Rules I	Before 💌		
Туре:	Static	<b>v</b>	🗹 Enable							
Description:										
Interface Objects	Translation	PAT Pool	Advanced							
Original Packet					Translat	ed Packet				
Original Source:*	any			<b>~</b> 📀	Translate	d Source:	Address		~	
Original Destination:	Address			<b>*</b>			any		<b>~</b> (	۷
	VPN_Subne	et		<b>v</b> ()	Translate	d Destination:	VPN_Subnet		<b>~</b> (	>
Original Source Port:				<b>v</b> ()	Translate	d Source Port:			<b>~</b> (	>
Original Destination Po	ort:			<b>v</b> 📀	Translate	d Destination Port:			<b>~</b> (	)
							(	ок	ancel	

在Advanced选项卡下,选中如下图所示的复选框:

Edit NAT Rule						? >
NAT Rule:	Manual NAT F	Rule 💌	Insert:	In Category	▼ NAT Rules 8	Before 💙
Type:	Static	•	Enable			
Description:						
Interface Objects	Translation	PAT Pool	Advanced			
Translate DNS repl	ies that match tl	his rule				
Fallthrough to Inter	face PAT(Destin	ation Interfac	ce)			
IPv6						
Net to Net Mapping						
Do not proxy ARP	on Destination I	nterface	7			
Perform Route Loo	kup for Destinat	ion Interface				
🗖 Unidirectional			- `			
					[	OK Cancel

### 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)。