

在FTD上通过AnyConnect远程访问VPN配置 ISE终端安全评估

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图和流量流程](#)

[配置](#)

[FTD/FMC](#)

[ISE](#)

[验证](#)

[故障排除](#)

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

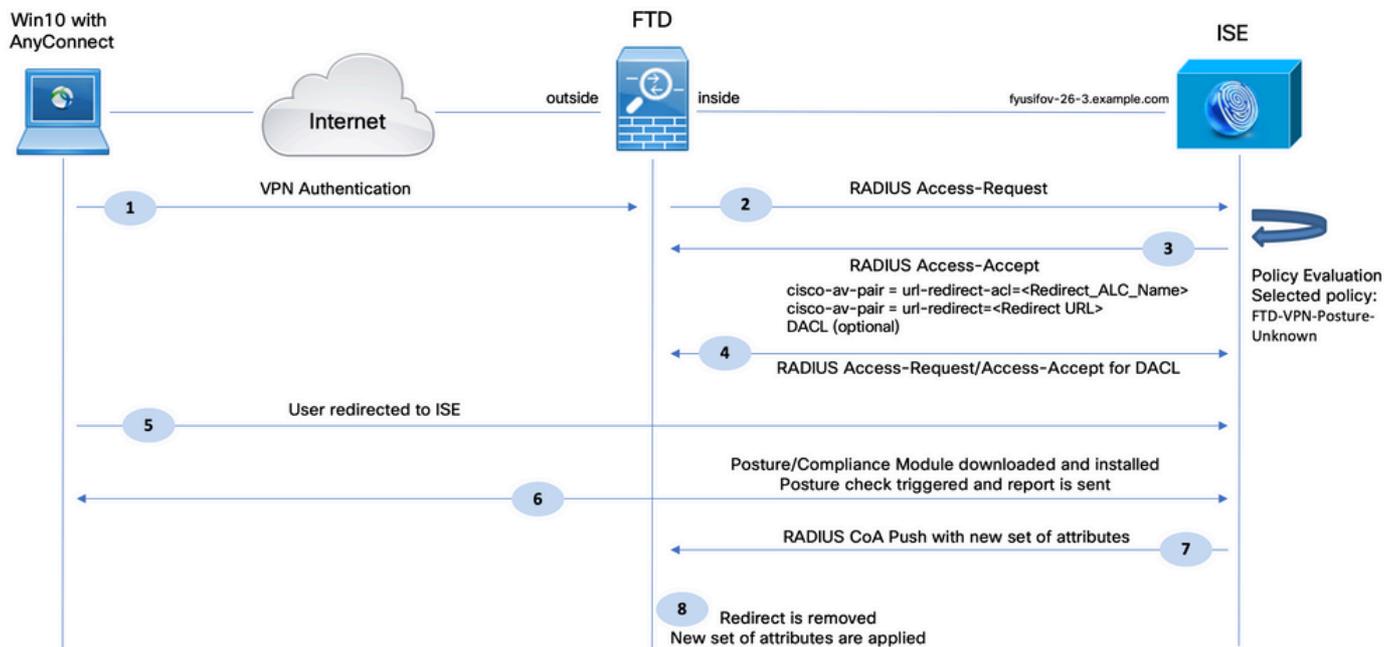
本文档中的信息基于以下软件版本：

- 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 = url-redirect=<https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp> — 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DAACL名称。
- 如果用户不兼容，则会发送允许有限访问的DAACL名称。

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

配置

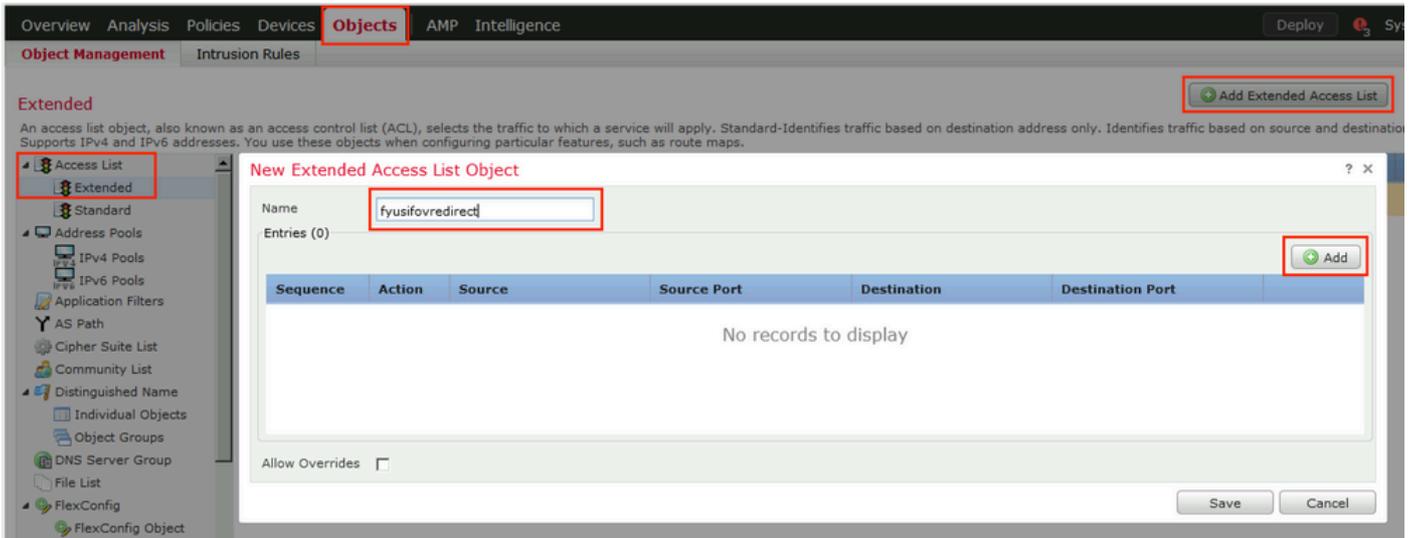
FTD/FMC

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。

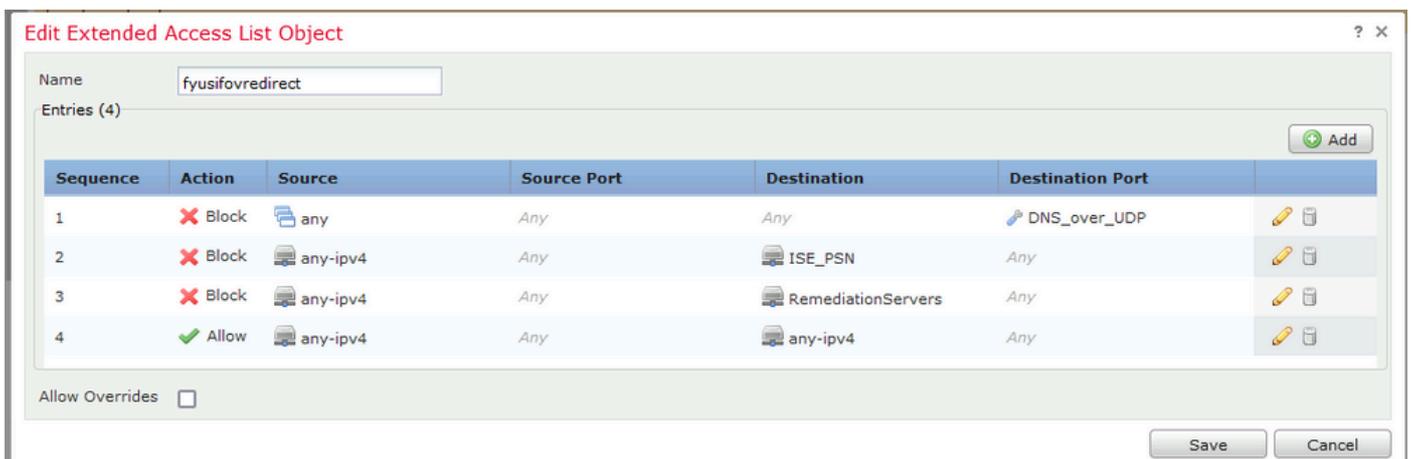
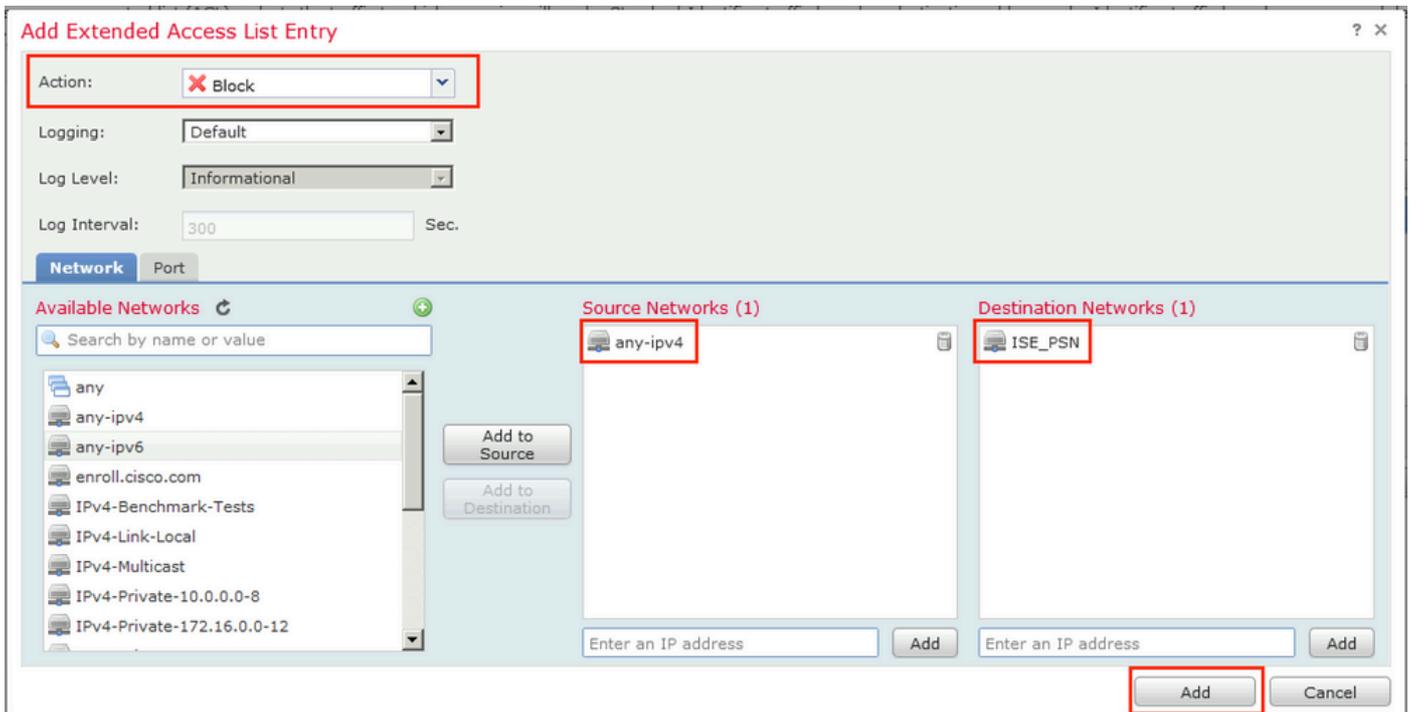
The screenshot shows the Cisco FTD/FMC configuration interface. The 'Objects' tab is selected, and the 'Network' object group is highlighted in the left sidebar. The main area displays a table of network objects. An 'Edit Network Object' dialog box is open, showing the configuration for a new network object named 'ISE_PSN'. The dialog box includes fields for Name, Description, Network (set to Host with value 192.168.15.14), and Allow Overrides (unchecked). The 'Save' and 'Cancel' buttons are visible at the bottom of the dialog.

Name	Value
any-ipv4	0.0.0.0/0
any-ipv6	::/0
enroll.cisco.com	72.163.1.80
IPv4-Benchmark-Tests	
IPv4-Link-Local	
IPv4-Multicast	
IPv4-Private-10.0.0.0-8	
IPv4-Private-172.16.0.0-12	
IPv4-Private-192.168.0.0-16	
IPv4-Private-All-RFC1918	
IPv6-IPv4-Mapped	::ffff:0.0.0.0/96
IPv6-Link-Local	fe80::/10
IPv6-Private-Unique-Local-Addresses	fc00::/7
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。



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）。



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 servers)

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:* Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

Key:*

Confirm Key:*

Accounting Port: (1-65535)

Timeout: (1-300) Seconds

Connect using: Routing Specific Interface i

v +

Redirect ACL: v +

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 Policies Devices **Objects** AMP Intelligence Deploy

Object Management Intrusion Rules Add IPv4 Pools

IPv4 Pools
 IPv4 pool contains list of IPv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles.

Name	Value
VPN-172-Pool	172.16.1.10-172.16.1.20

Edit IPv4 Pool

Name*

IPv4 Address Range*
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

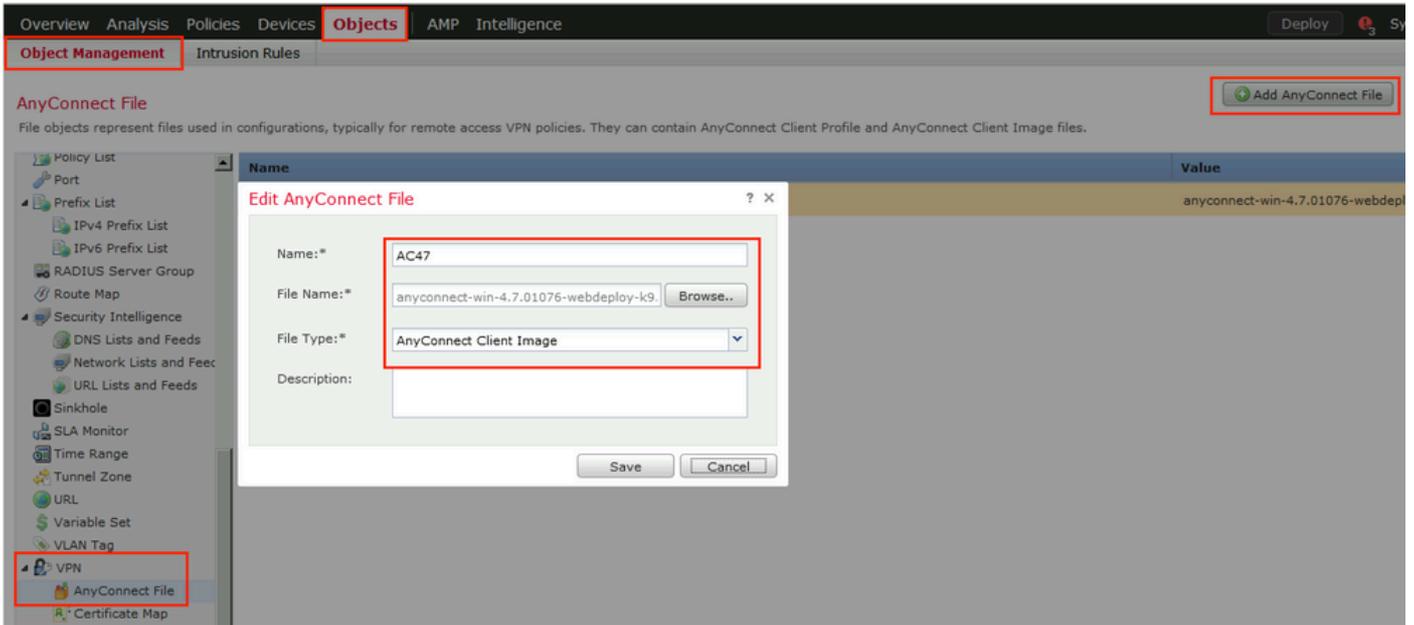
Allow Overrides

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

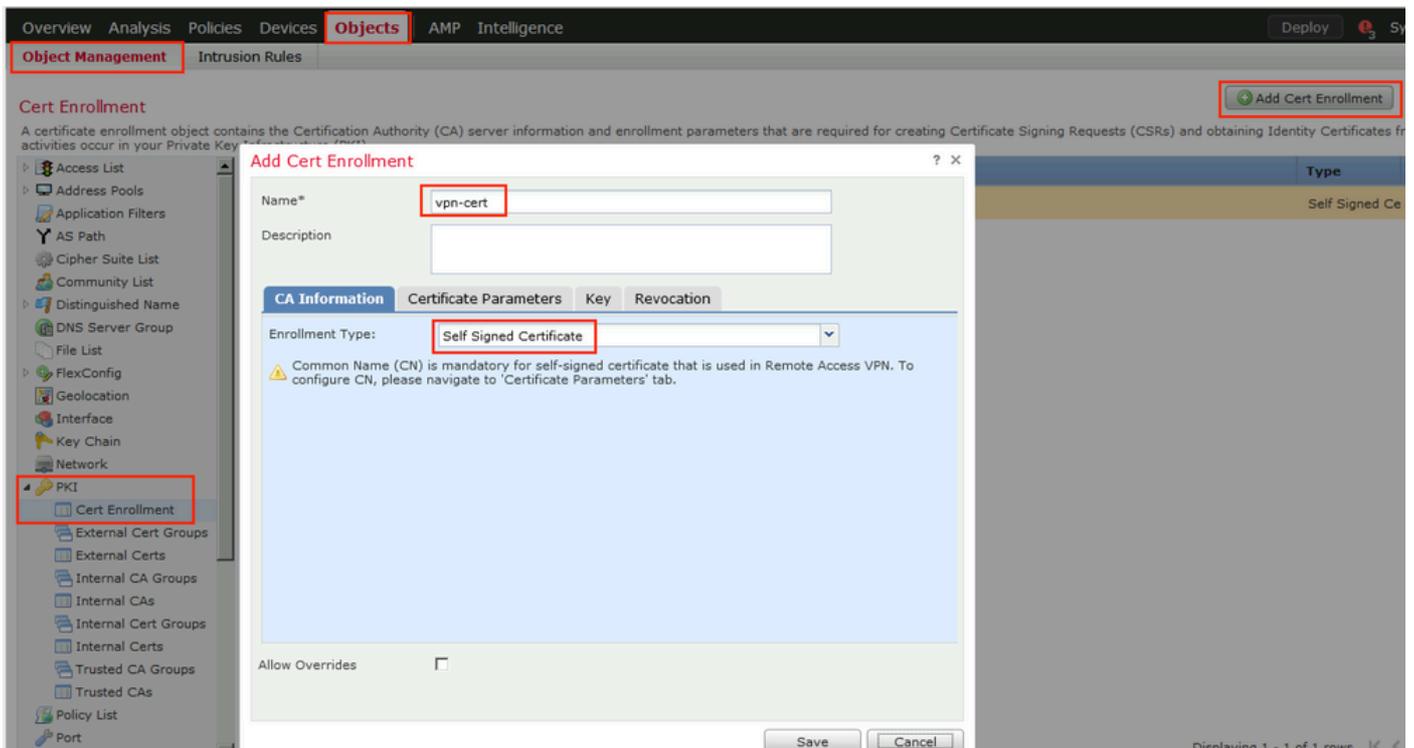
Override (0)

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Cisco

[Software Download](#) 下载软件包，然后选择 [Anyconnect Client Image](#) 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。



Add Cert Enrollment

Name*

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

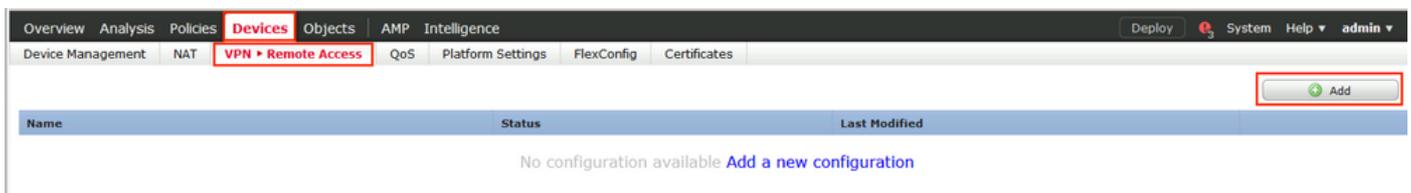
Email (E):

Include Device's Serial Number

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。



步骤 10提供名称，选中SSL as VPN Protocol，选择用作VPN集中器的FTD，然后单击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:*

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices:

Available Devices:
192.168.15.11

Selected Devices:

Before You Start
Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server
Configure [Realm](#) or [RADIUS Server Group](#) to authenticate VPN clients.

AnyConnect Client Package
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface
Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

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)。

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Connection Profile:
Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and 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 Method:

Authentication Servers:* (Realm or RADIUS)

Authorization Server: (RADIUS)

Accounting Server: (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
 Use IP Address Pools

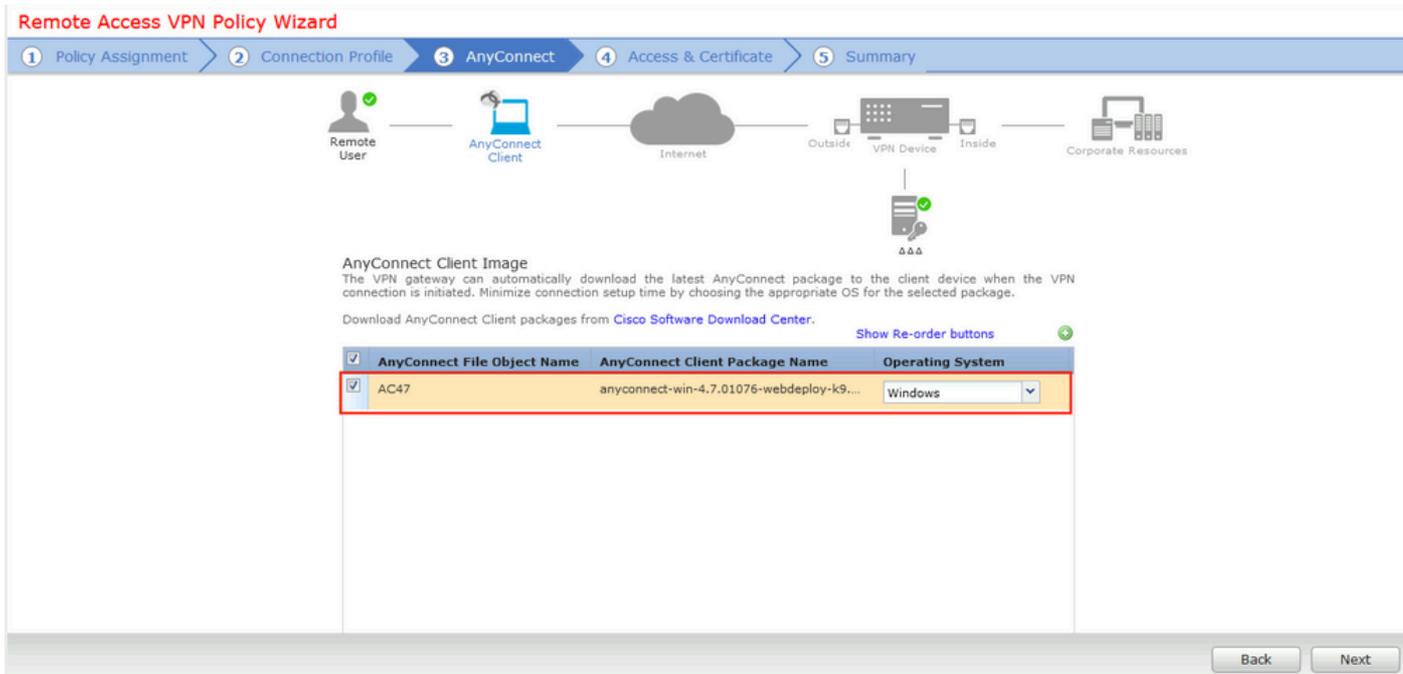
IPv4 Address:
IPv6 Address:

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.

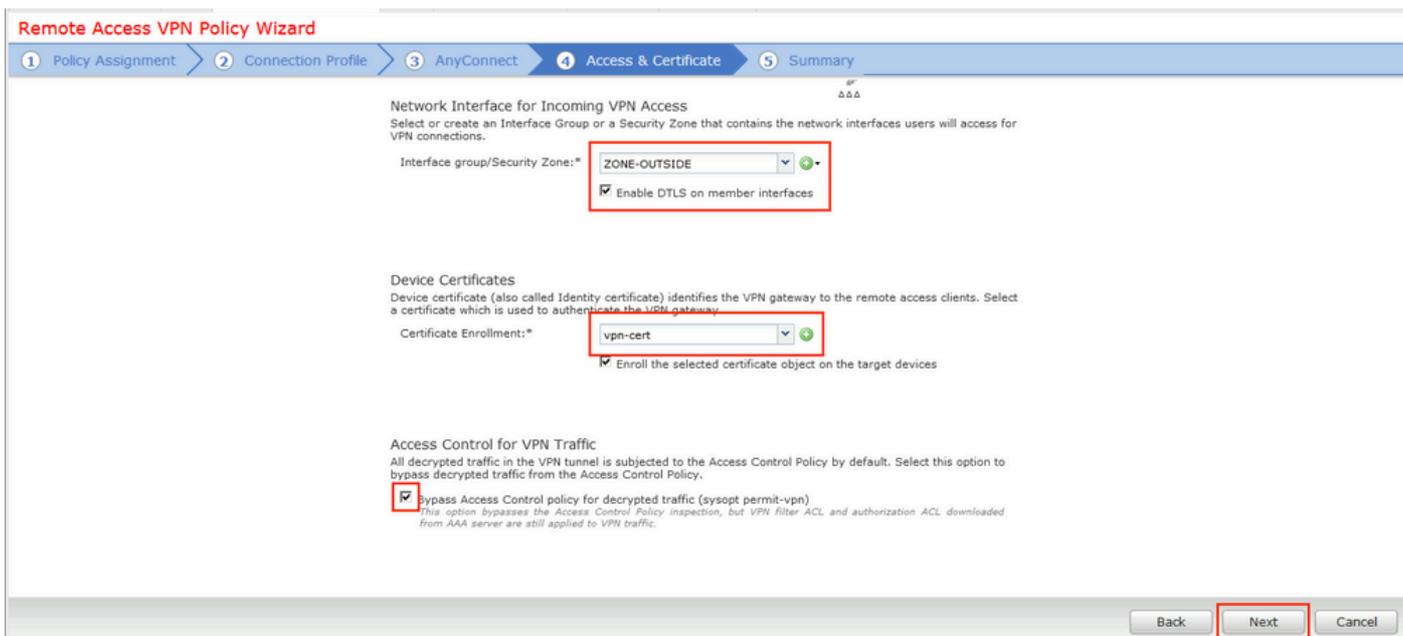
Group Policy:* ⓘ
[Edit Group Policy](#)

Back Next Cancel

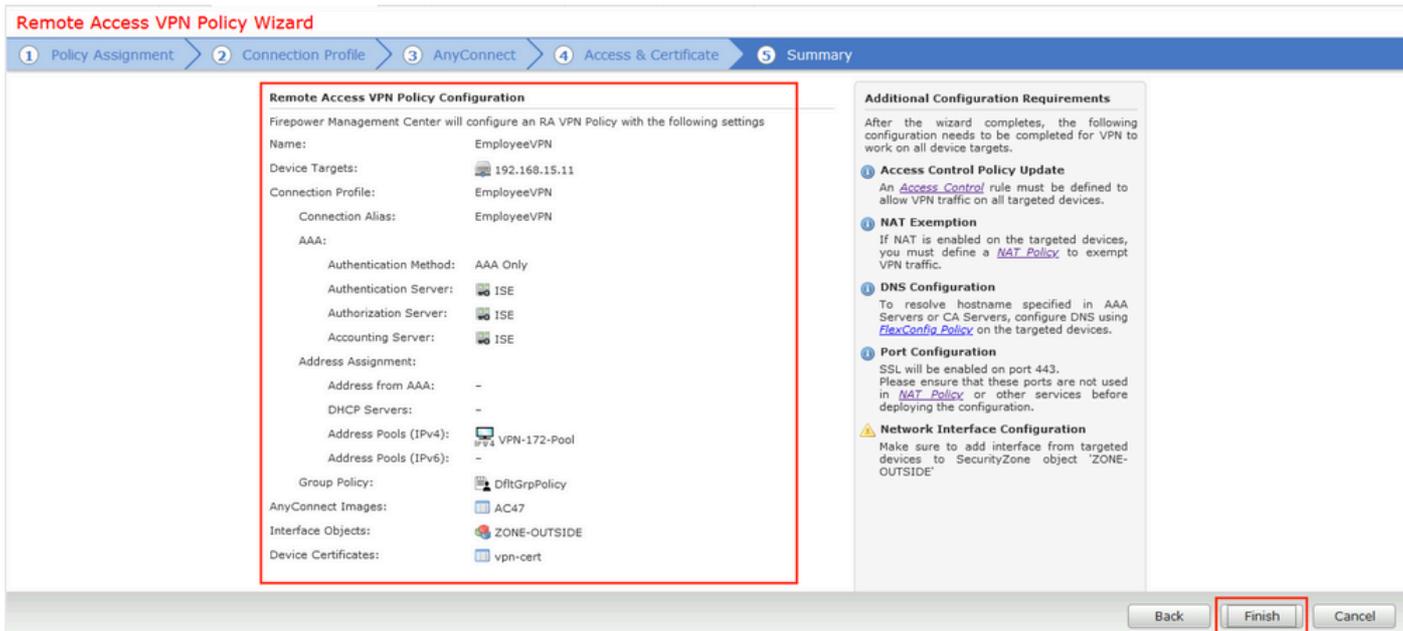
步骤 12选择之前配置的AnyConnect软件包，然后单击Next。



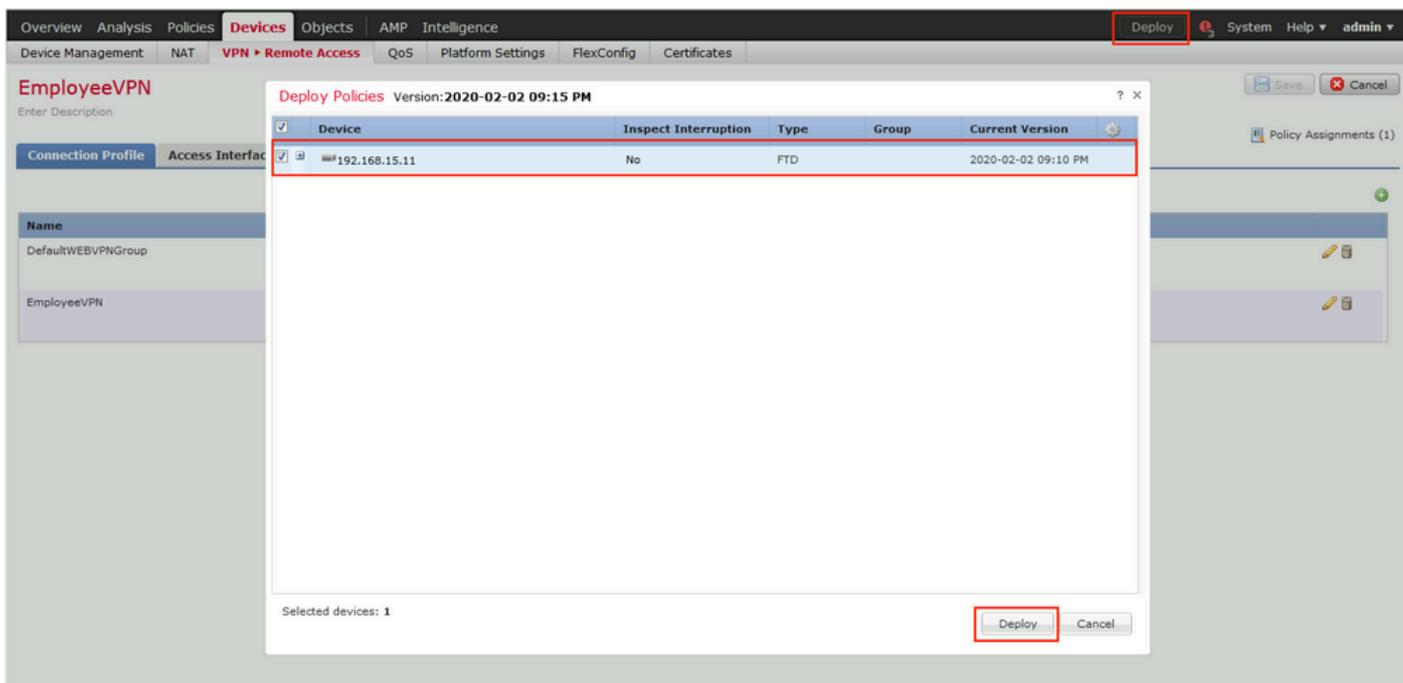
步骤 13选择VPN流量预期来自的接口，选择Certificate Enrollment（之前配置的证书注册），然后单击Next。



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。



ISE

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

Posture Updates

Web Offline

* Update Feed URL

Proxy Address ⓘ

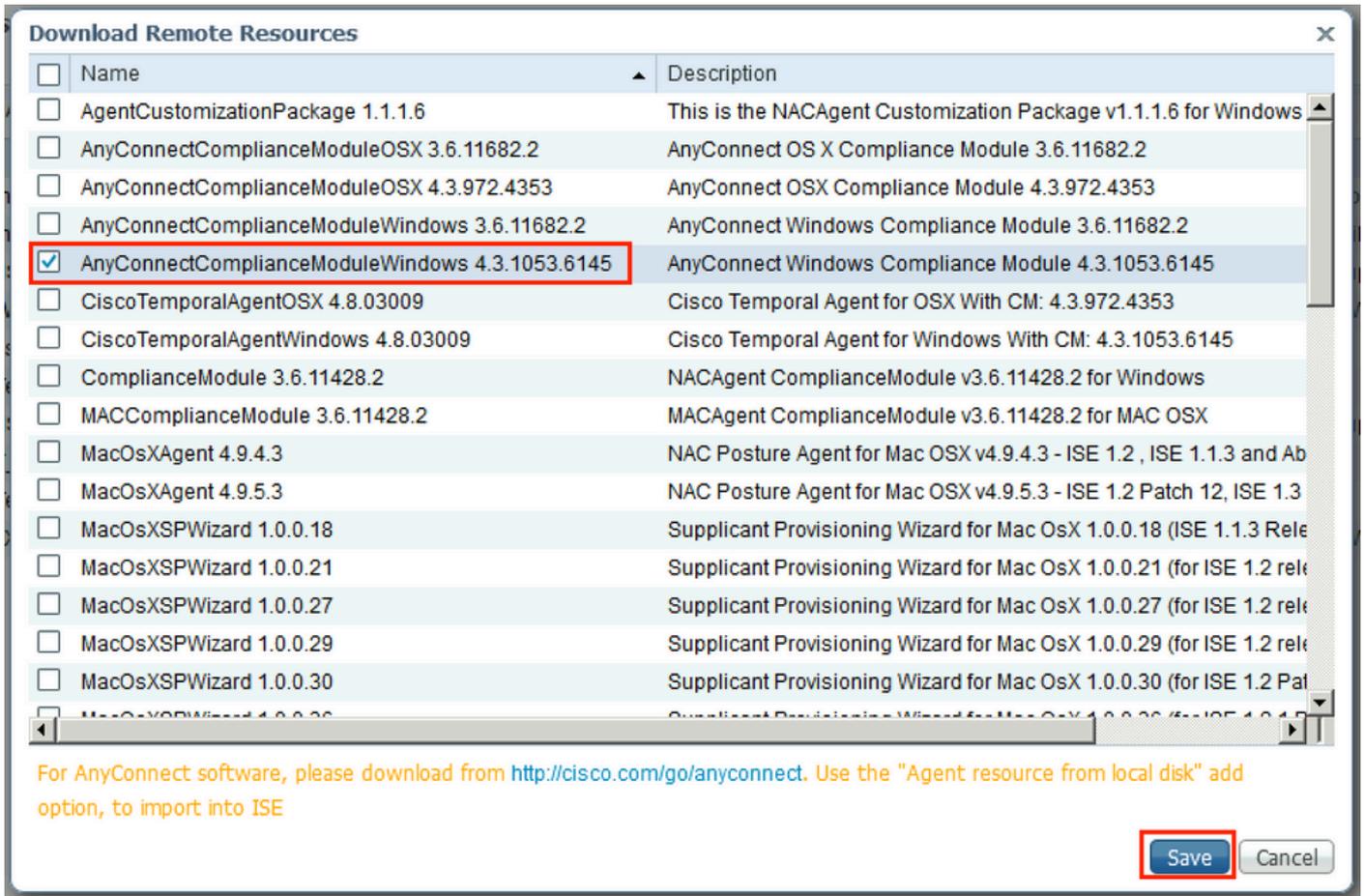
Proxy Port HH MM SS

Automatically check for updates starting from initial delay every hours ⓘ

▼ Update Information

Last successful update on	2020/02/02 20:44:27 ⓘ
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



第三步：从[Cisco Software Download](http://cisco.com/go/anyconnect)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

anyconnect-win-4.7.01076-webdeploy-k9.pkg

▼ AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.7.10...	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secure Mobility Cle...

Submit Cancel

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:

Description:

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host	<input type="text" value="1.2.3.4"/>		The server that the agent should connect to
* Server name rules	<input type="text" value="*"/>	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	<input type="text"/>	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	<input type="text" value="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:

DescriptionValue **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**

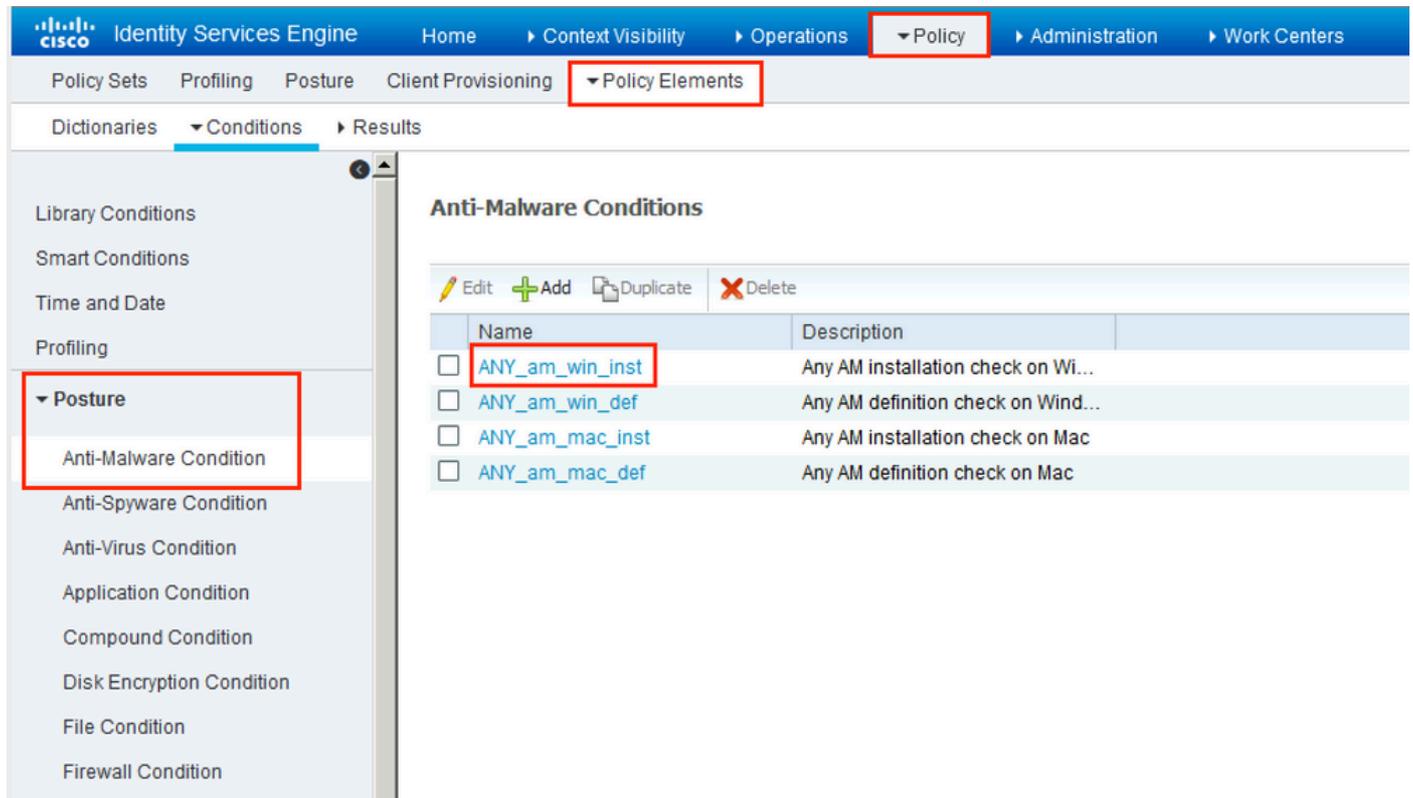
Profile Selection

- * ISE Posture: AC_Posture_Profile
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- Network Visibility
- Umbrella Roaming Security
- Customer Feedback

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。

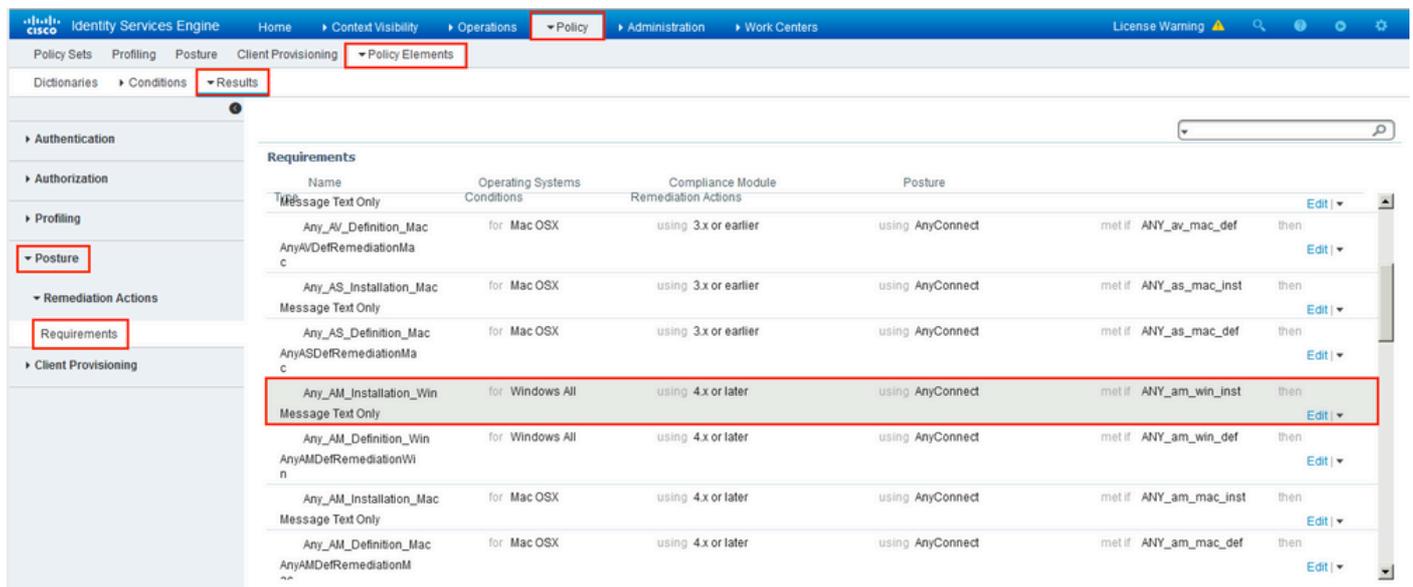
Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
AC_47_Win	If Any	and Windows All	and Condition(s)	then AC_CF_47
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

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”。

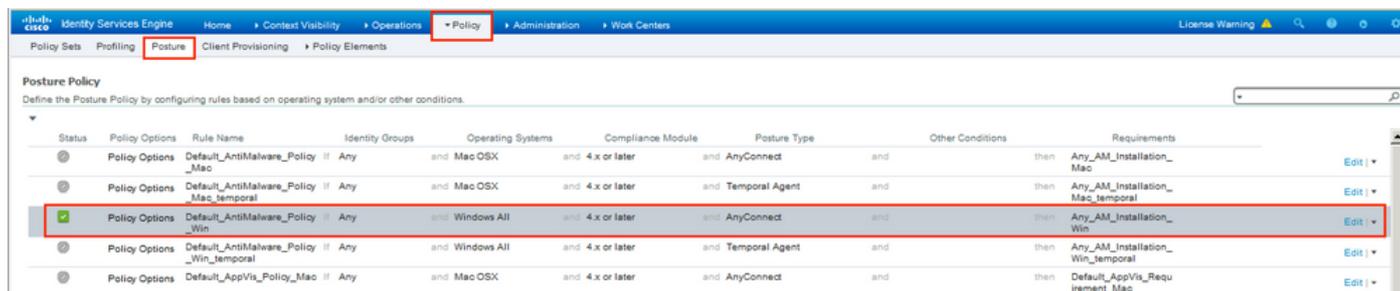


步骤 8导航到Policy > Policy Elements > Results > Posture > Remediation Actions并创建Posture Remediation。在本例中，它被跳过。补救操作可以是文本消息。

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。



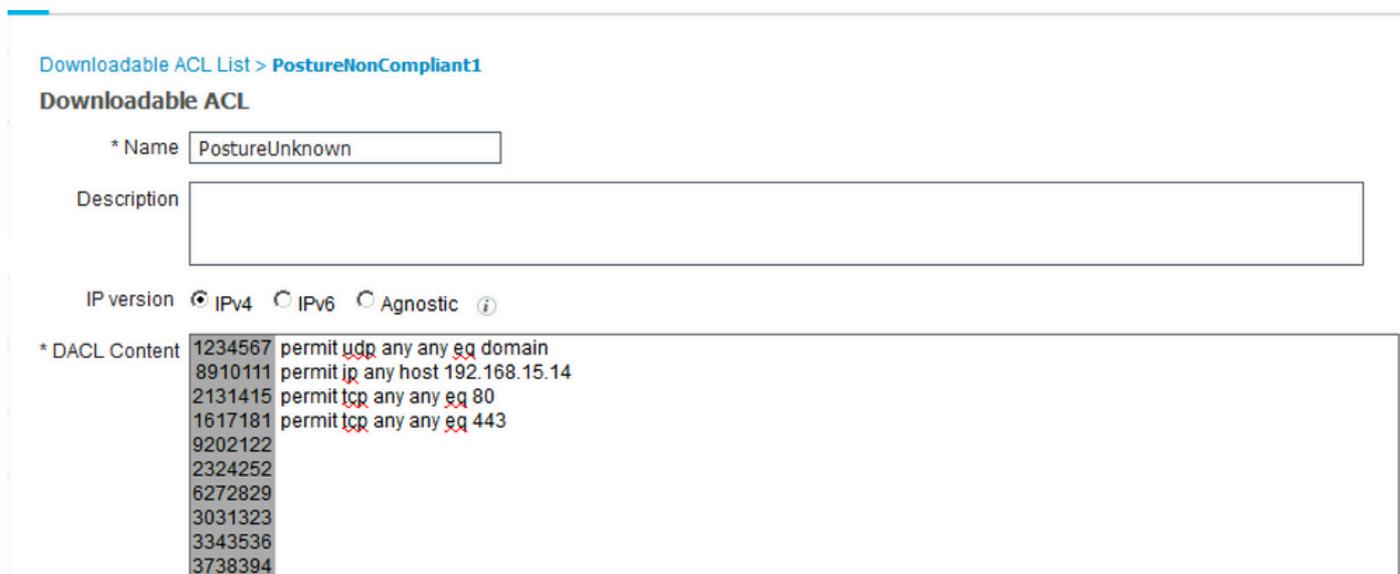
步骤 10在Policies > Posture下创建状况策略。使用适用于Windows操作系统的任何防恶意软件检查的默认安全评估策略。



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 ACL

* Name

Description

IP version IPv4 IPv6 Agnostic 

* DACL Content

```
1234567 deny ip any 10.0.0.0 255.0.0.0
8910111 deny ip any 172.16.0.0 255.240.0.0
2131415 deny ip any 192.168.0.0 255.255.0.0
1617181 permit ip any any
9202122
2324252
6272829
3031323
3343536
3738394
```

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic 

* DACL Content

```
1234567 permit ip any any
7891011
121314
151617
181920
212223
242526
272829
303132
333435
363738
```

[▶ Check DACL Syntax](#)



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 Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

Web Redirection (CWA, MDM, NSP, CPP)

ACL

Value

Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = PostureUnknown
cisco-av-pair = url-redirect-acl=fyusifovredirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&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 Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

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 Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

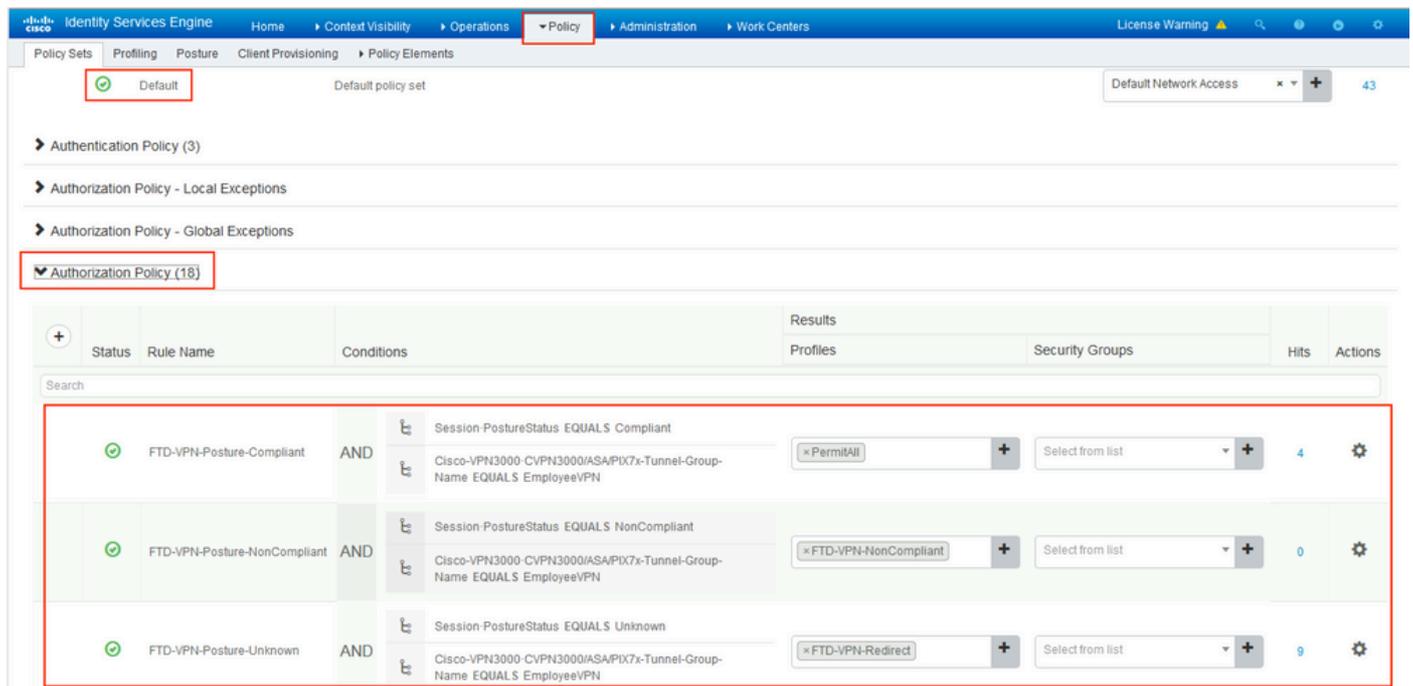
Common Tasks

DACL Name

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PermitAll

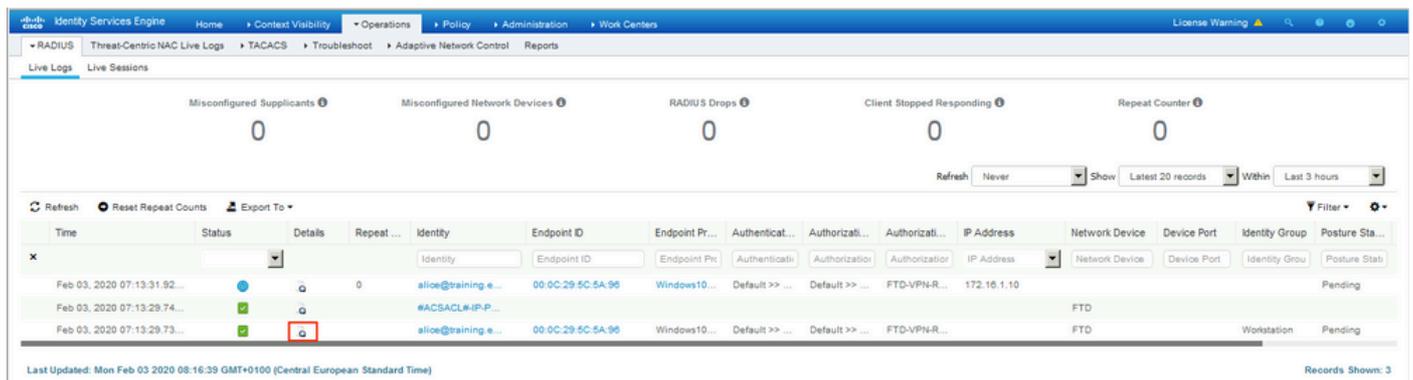
步骤 13在Policy > Policy Sets > Default > Authorization Policy下创建授权策略。As条件使用 Posture Status和VNP TunnelGroup Name。



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。



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 fysisfov-26-3

Event 5200 Authentication succeeded

Username alice@training.example.com

状态待处理。

NAS IPv4 Address 192.168.15.15

NAS Port Type Virtual

Authorization Profile FTD-VPN-Redirect

Posture Status Pending

Response Time 365 milliseconds

“结果”部分显示哪些属性发送到FTD。

Result

Class	CACS:000000000000c0005e37c81a: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=000000000000c0005e37c81a&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp&token=0d90f1cdf40e83039a7ad6a226603112
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
```

```
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License      : AnyConnect Premium
```

```
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
```

```
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
```

```
Duration     : 0h:06m:43s
```

```
Inactivity   : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN           : none
```

```
Audt Sess ID : 000000000000c0005e37c81a
```

```
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
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 : 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 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes
Client OS : Windows
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
Encryption : AES256 Hashing : SHA1
Ciphersuite : DHE-RSA-AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 59396
UDP Dst Port : 443 Auth Mode : userPassword
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

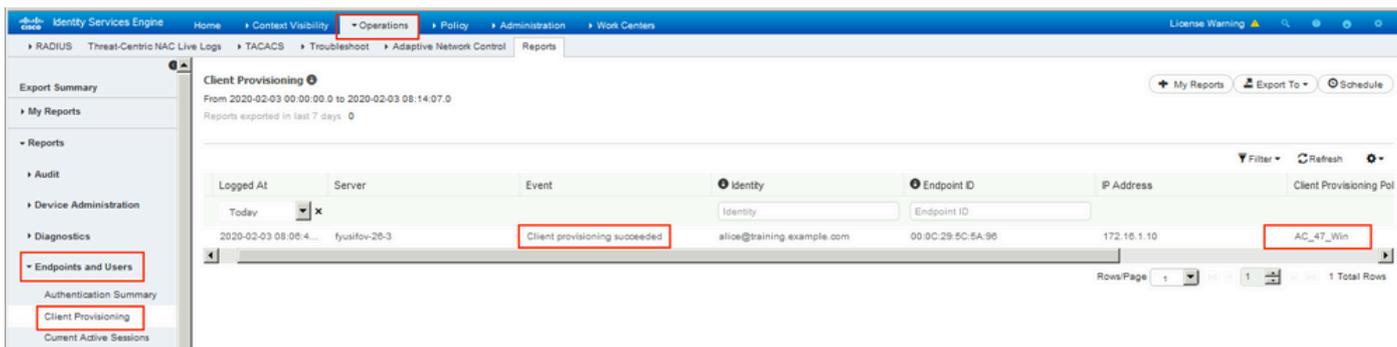
Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

ISE Posture:

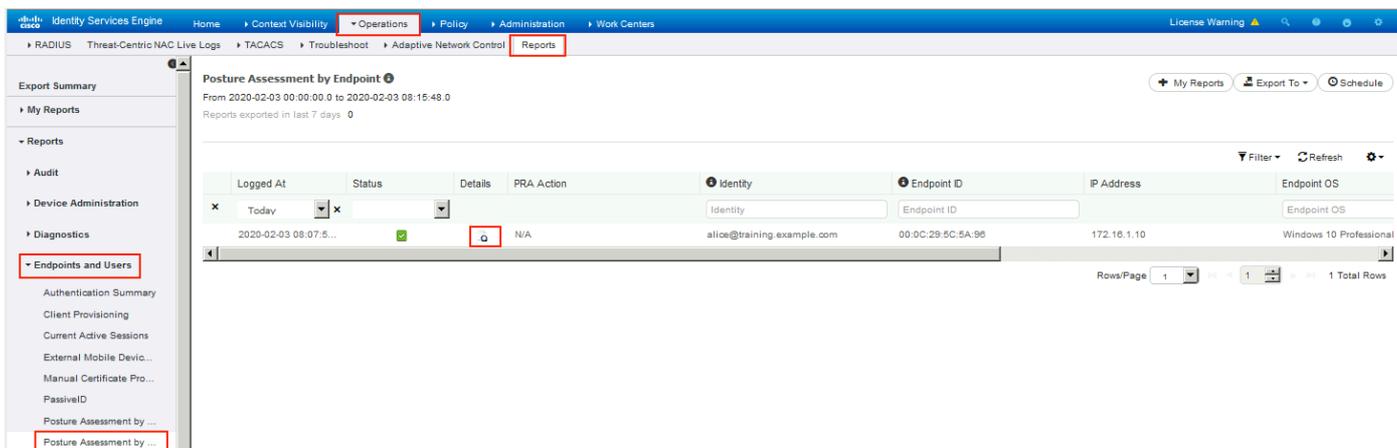
Redirect URL : <https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=00000000000c0005e37c81>
Redirect ACL : fyusifovredirect

fyusifov-ftd-64#

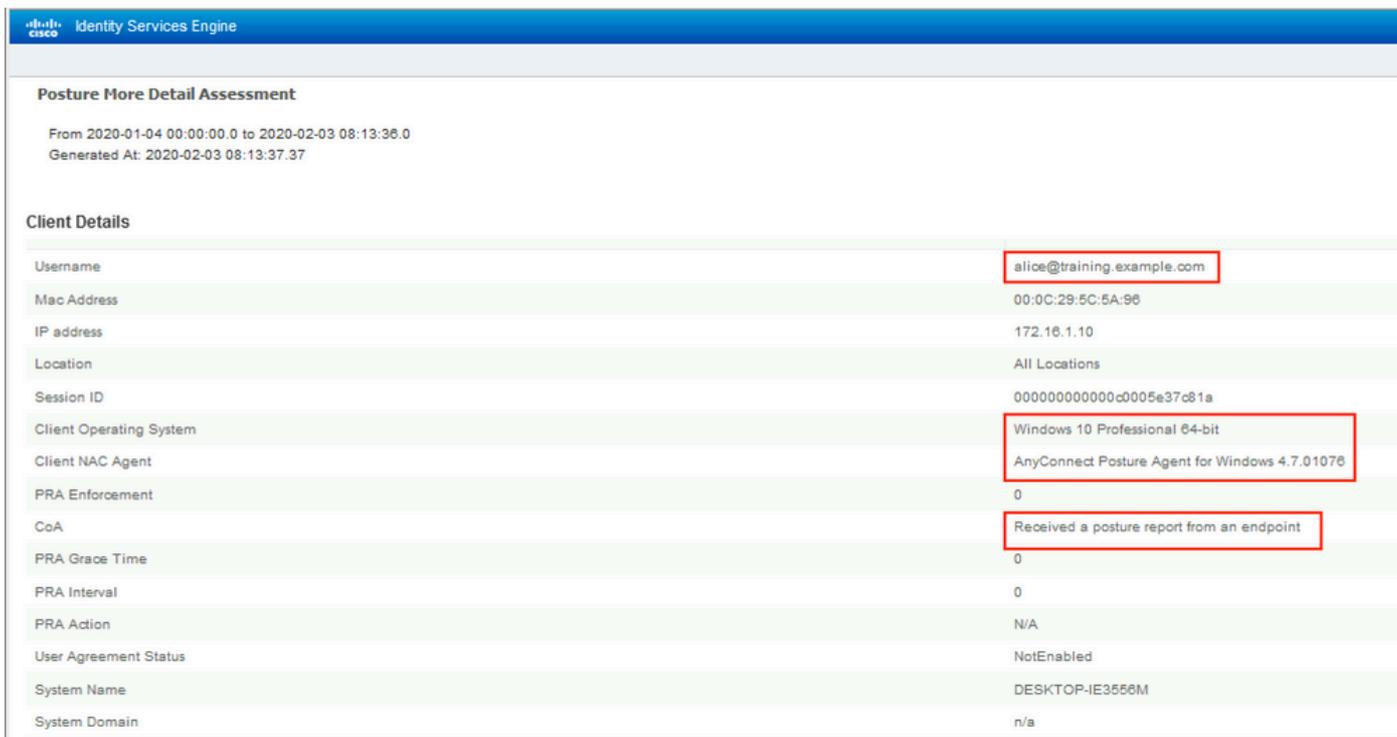
可以验证客户端调配策略。导航到操作>报告>端点和用户>客户端调配。



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。



要查看状态报告的更多详细信息，请单击Details。



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。

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture S
Feb 03, 2020 08:07:52.05...	✓				10.229.16.169				PermitAccess		FTD			Compliar
Feb 03, 2020 08:07:50.03...	ⓘ		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...	✓			#ACSACL#HP.P...							FTD			
Feb 03, 2020 07:13:29.73...	✓			alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...				Workstation	Pending

Last Updated: Mon Feb 03 2020 09:10:20 GMT+0100 (Central European Standard Time) Records Shown: 4

Overview

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

Authentication Details

Source Timestamp	2020-02-03 16:58:39.687
Received Timestamp	2020-02-03 16:58:39.687
Policy Server	fysifov-26-3
Event	5205 Dynamic Authorization succeeded
Endpoint Id	10.55.218.19
Calling Station Id	10.55.218.19
Audit Session Id	000000000000e0005e385132
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	af49ce55-d55c-4778-ad40-b03ea12924d2
CoASourceComponent	Posture
CoAReason	posture status changed
CoAType	COA-push
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
Device IP Address	192.168.15.15
CiscoAVPair	audit-session-id=000000000000e0005e385132, coa-push=true, ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PermitAll-5e384dc0

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: AnyConnect Detailed
```

```
Username      :
```

```
alice@training.example.com
```

```
Index         : 14
```

```
Assigned IP   : 172.16.1.10      Public IP     : 10.55.218.19
```

```
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 53990 Bytes Rx : 23808
Pkts Tx : 73 Pkts Rx : 120
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group :

EmployeeVPN

Login Time : 16:58:26 UTC Mon Feb 3 2020
Duration : 0h:02m:24s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000000e0005e385132
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
Encapsulation: DTLSv1.0 UDP Src Port : 51536
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

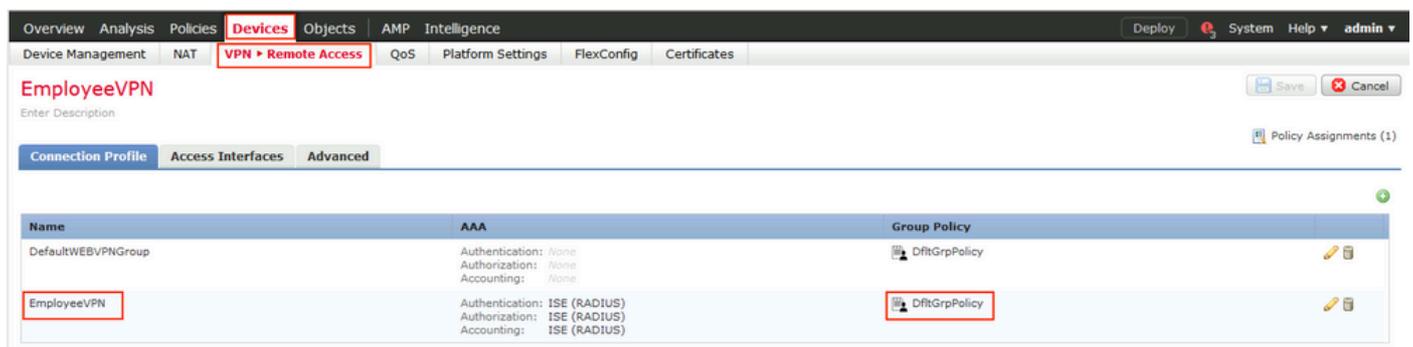
本部分提供了可用于对配置进行故障排除的信息。

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：[高级版和高级版2.2的ISE终端安全评估样式比较。](#)

- 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。

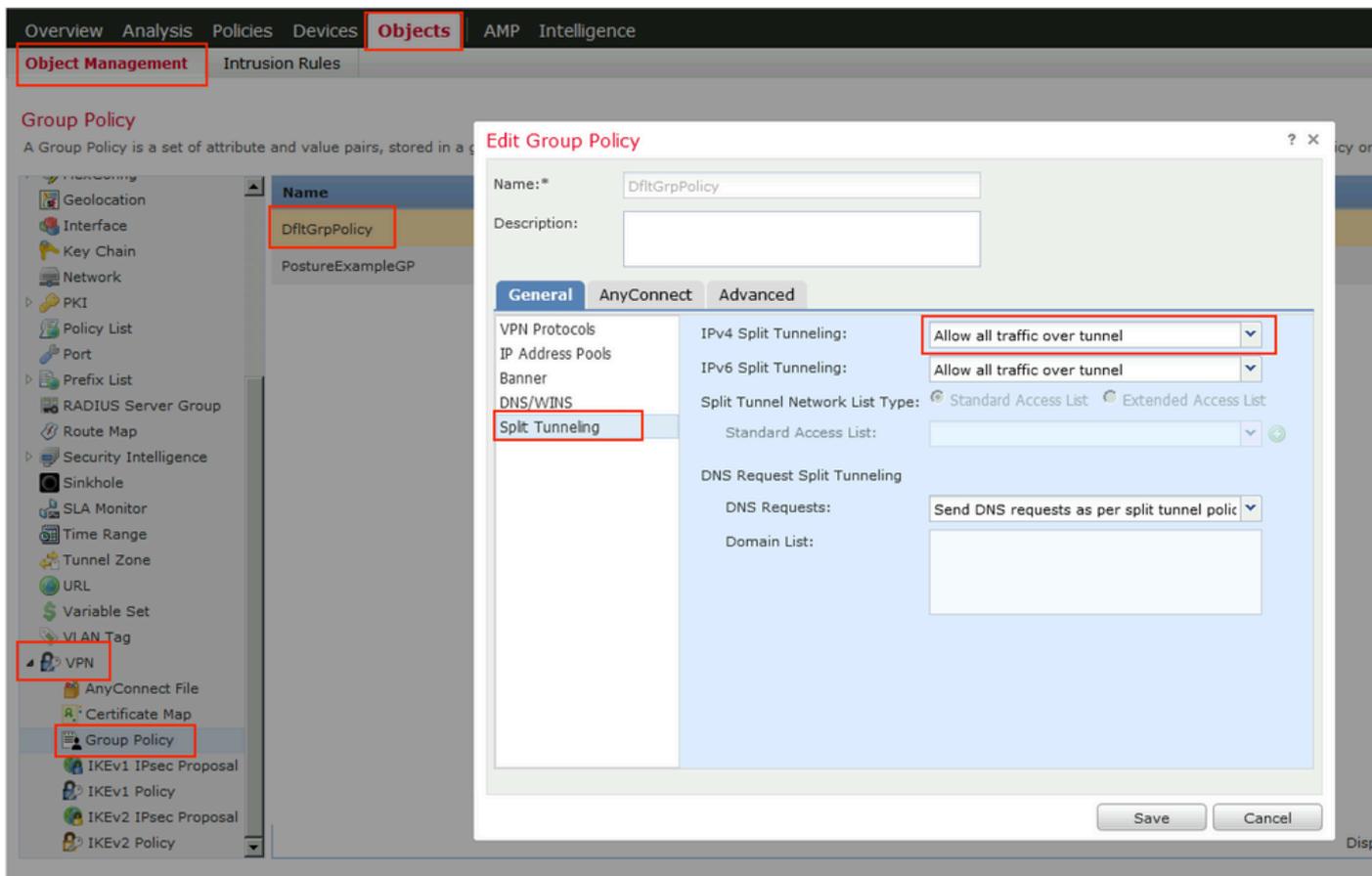
要检查FMC上的隧道策略，首先检查哪个组策略用于VPN连接。导航到设备> VPN远程访问。



The screenshot shows the Cisco FMC interface for configuring a VPN. The 'Devices' tab is selected, and the 'VPN Remote Access' sub-tab is active. The configuration is for 'EmployeeVPN'. The 'Connection Profile' tab is selected, and the 'Advanced' sub-tab is active. A table lists the configuration details for the VPN connection profile.

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
EmployeeVPN	Authentication: ISE (RADIUS) Authorization: ISE (RADIUS) Accounting: ISE (RADIUS)	DfltGrpPolicy

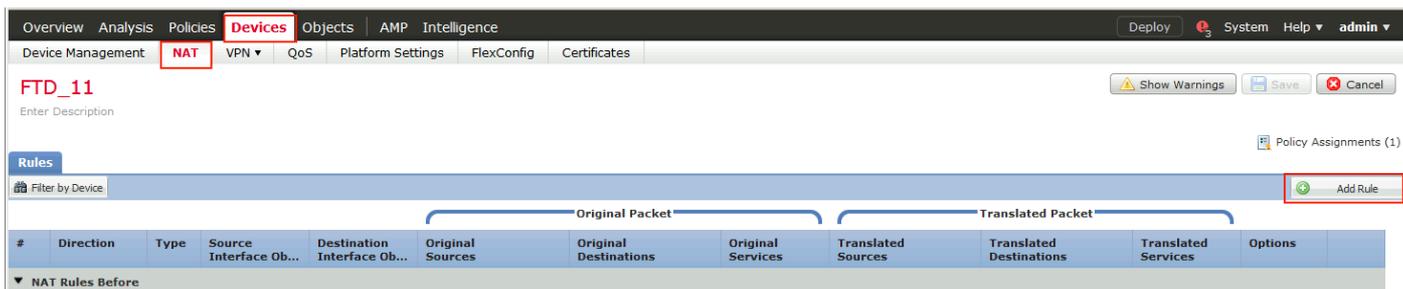
然后，导航到Objects > Object Management > VPN > Group Policy，然后点击Group Policy为VPN配置。



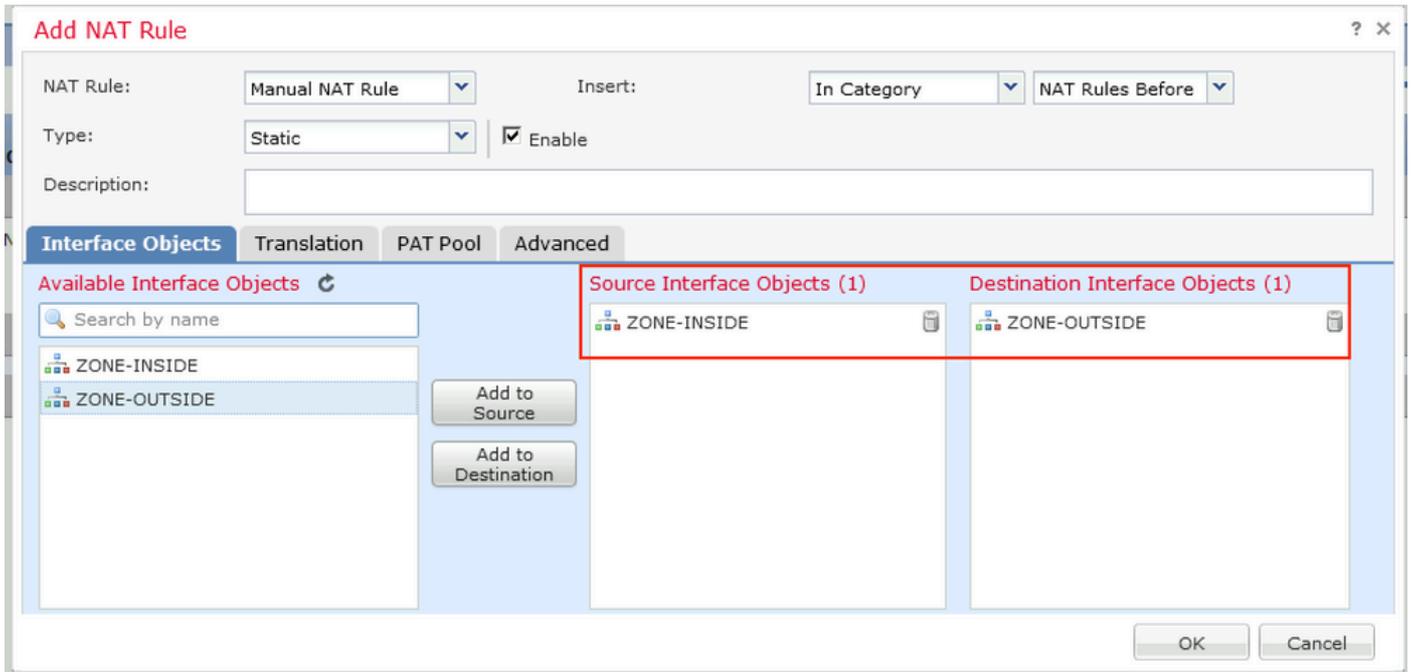
• 身份NAT

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。

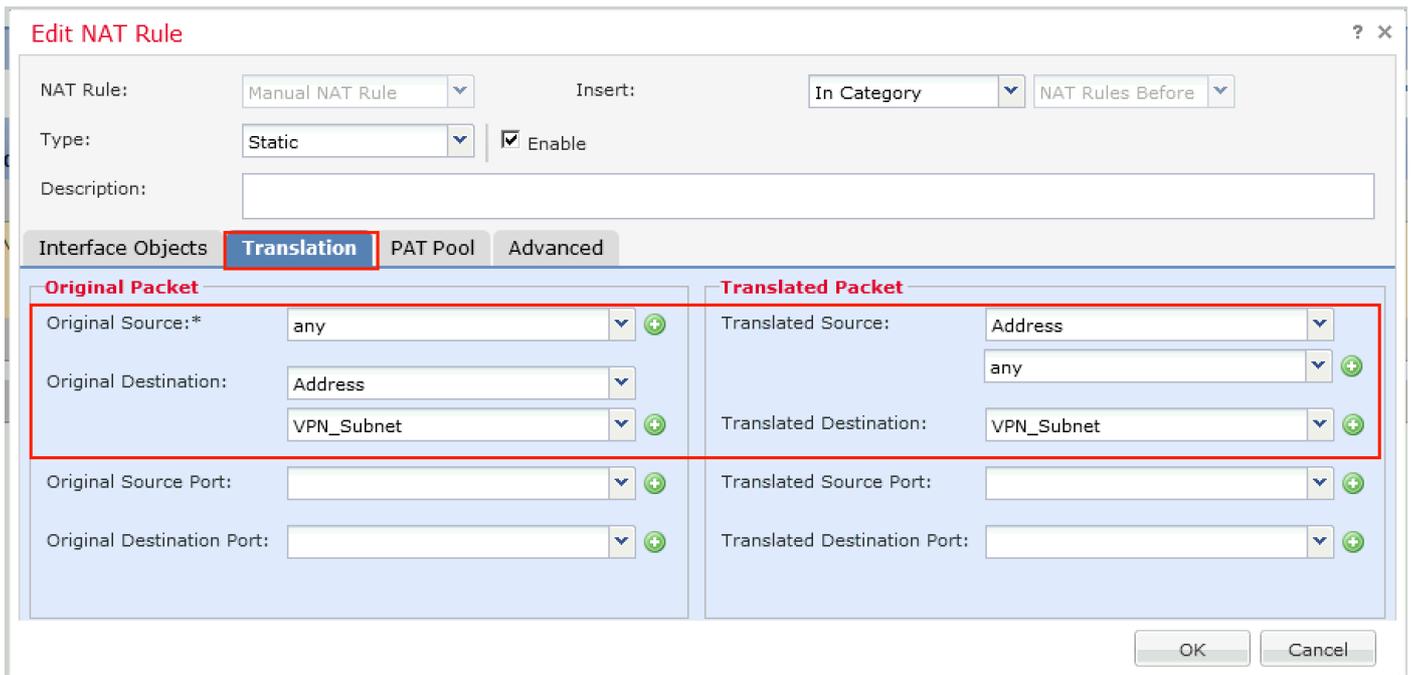
首先，检查此设备的NAT规则。导航到设备 > NAT，然后单击添加规则以创建新规则。



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。



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：



在Advanced选项卡下，选中如下图所示的复选框：

Edit NAT Rule

? X

NAT Rule:

Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

- Translate DNS replies that match this rule
- Fallthrough to Interface PAT(Destination Interface)
- IPv6
- Net to Net Mapping
- Do not proxy ARP on Destination Interface
- Perform Route Lookup for Destination 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）。