

# 在FTD上配置AnyConnect VPN，使用Cisco ISE作为RADIUS服务器，使用Windows Server 2012根CA

## 目录

[目录](#)

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[从Windows Server导出根CA证书](#)

[在员工Windows/Mac PC上安装根CA证书](#)

[在FTD上生成CSR，获取由Windows Server根CA签名的CSR，并在FTD上安装该签名的证书](#)

[下载AnyConnect映像+ AnyConnect配置文件编辑器并创建.xml配置文件](#)

[在FTD上配置Anyconnect VPN（使用根CA证书）](#)

[配置FTD NAT规则，使VPN流量免于NAT，因为它仍将被解密，并创建访问控制策略/规则](#)

[将FTD添加为网络设备并在思科ISE上配置策略集（使用RADIUS共享密钥）](#)

[在员工Windows/Mac PC上使用AnyConnect VPN客户端下载、安装并连接到FTD](#)

[验证](#)

[FTD](#)

[思科ISE](#)

[AnyConnect VPN客户端](#)

[故障排除](#)

[DNS](#)

[证书强度（用于浏览器兼容性）](#)

[连接和防火墙配置](#)

## 目录

## 简介

本文档介绍如何使用思科ISE（身份服务引擎）作为RADIUS服务器在FTD（Firepower威胁防御）防火墙上配置AnyConnect VPN（虚拟专用网络）。我们使用Windows Server 2012作为根CA（证书颁发机构），以便通过VPN的通信由证书保护，即员工PC将信任FTD的证书，因为FTD VPN证书已由我们的Windows Server 2012根CA签名

## 先决条件

## 要求

您必须在您的网络中部署并运行以下设备：

- 通过基本连接部署Firepower管理中心和Firepower威胁防御防火墙
- 思科ISE在您的网络中部署和运行
- 已部署Windows Server (带Active Directory)，员工的Windows/Mac PC已加入AD(Active Directory)域

在下面的示例中，员工将在其Windows/Mac PC上打开AnyConnect客户端，并使用其凭证通过VPN安全地连接到FTD的外部接口。FTD将对照思科ISE检查其用户名和密码(这将与Windows Server Active Directory检查以验证其用户名、密码和组，即只有AD组“Employees”中的用户才能通过VPN连接到公司网络。

## 使用的组件

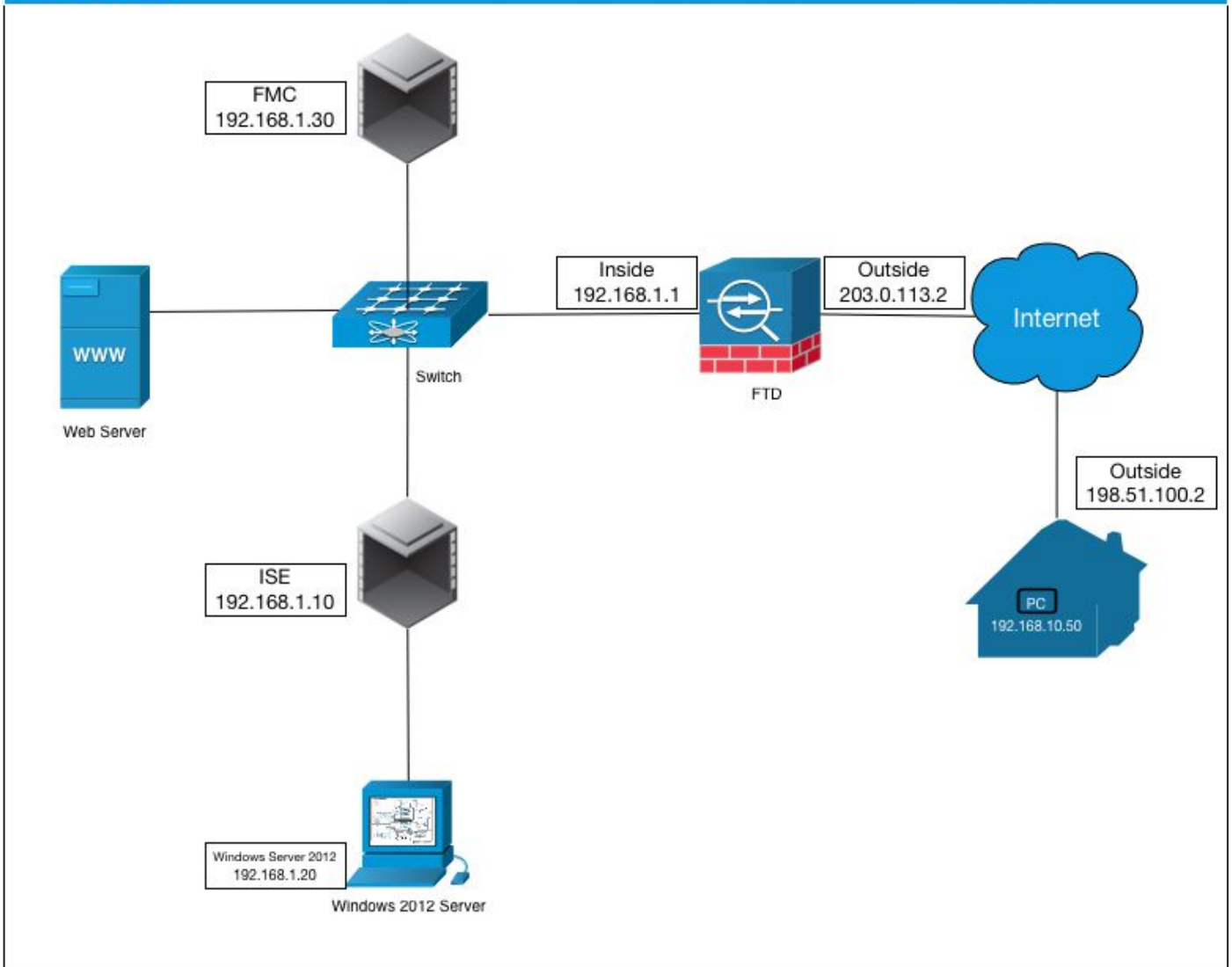
本文档中的信息基于以下软件版本：

- 运行Firepower管理中心和Firepower威胁防御6.2.3
- 运行2.4的思科身份服务引擎
- 运行4.6.03049的Cisco AnyConnect安全移动客户端
- 运行Active Directory和证书服务的Windows Server 2012 R2 (这是所有证书的根CA)
- Windows 7、Windows 10、Mac PC

## 配置

### 网络图

## Topology



在此使用案例中，运行Anyconnect VPN客户端的员工的Windows/Mac PC将连接到FTD防火墙的外部公有IP地址，并且思科ISE将在通过VPN连接时动态地授予他们有限或完全访问某些内部或互联网资源（可配置）的权限，具体取决于他们在Active Directory中的AD组

设备	主机名/FQDN	公共 IP 地址	私有 IP 地址	AnyConnect IP地址
Windows PC	-	198.51.100.2	10.0.0.1	192.168.10.50
FTD	ciscofp3.cisco.com	203.0.113.2	192.168.1.1	-
FMC	-	-	192.168.1.30	-
思科ISE	ciscoise.cisco.com	-	192.168.1.10	-
Windows Server 2012	ciscodc.cisco.com	-	192.168.1.20	-
内部服务器	-	-	192.168.1.x	-

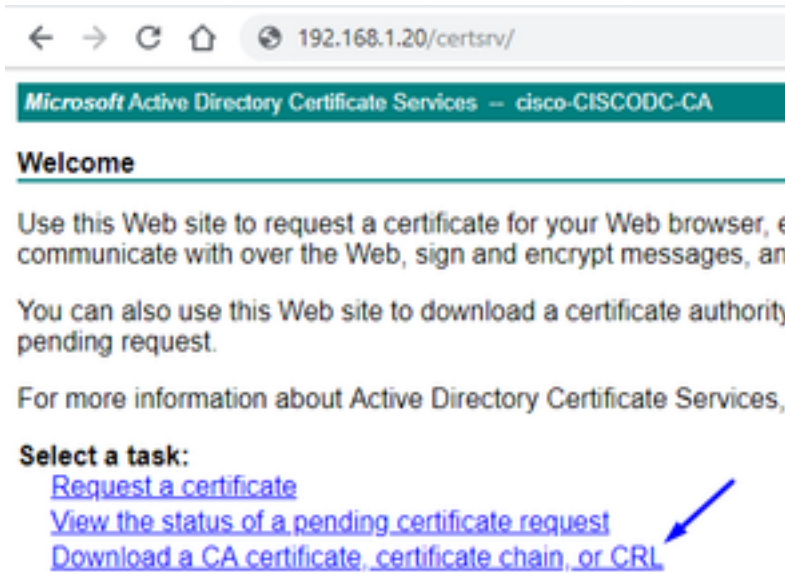
## 配置

### 从Windows Server导出根CA证书

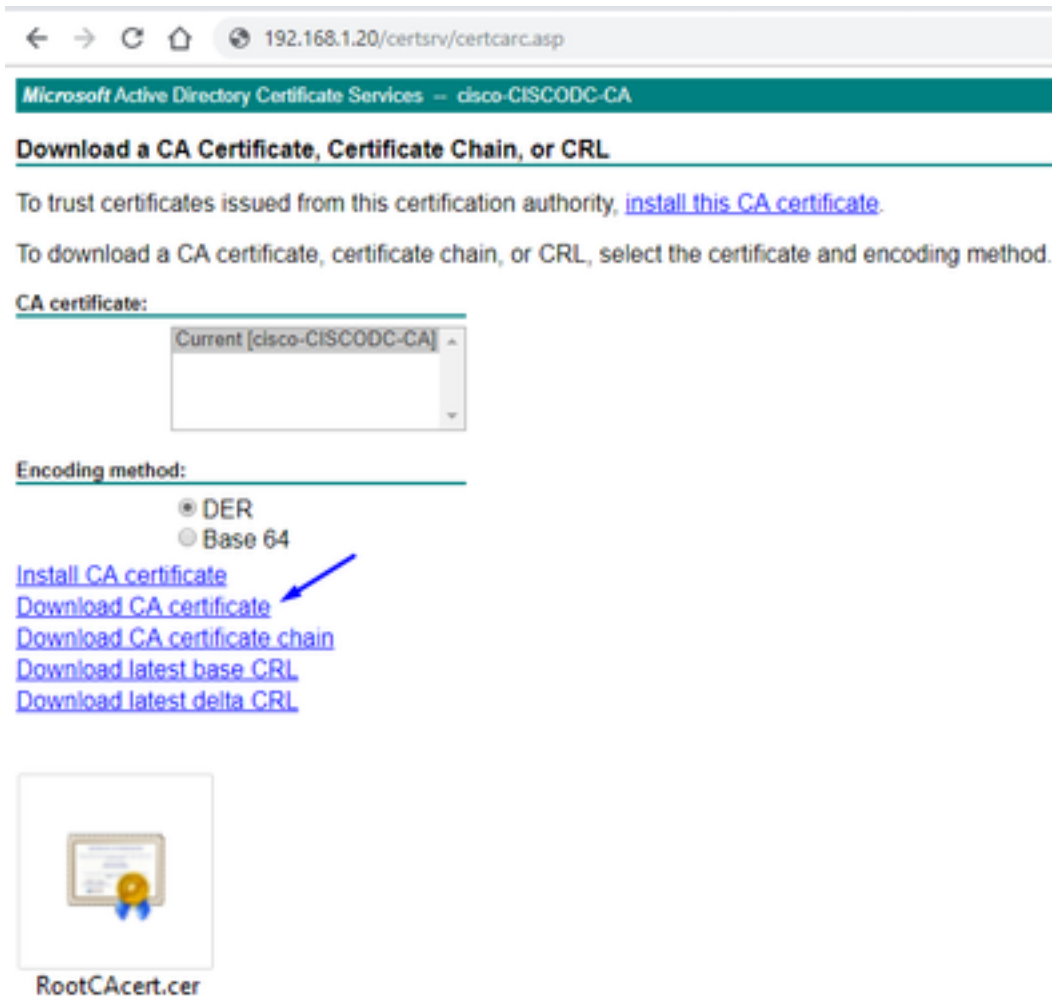
在本文档中，我们将使用Microsoft Windows Server 2012作为证书的根CA。客户端PC将信任此根CA通过VPN安全地连接到FTD（请参阅以下步骤）。这将确保他们可以通过互联网安全地连接到FTD，并从家访问内部资源。其PC将信任其浏览器和AnyConnect客户端中的连接。

转到<http://192.168.1.20/certsrv>，按照以下步骤下载您的Windows Server根CA证书：

单击Download a CA certificate, certificate chain, or CRL



单击Download Certificate , 将其重命名为“RootCAcert3.cer”



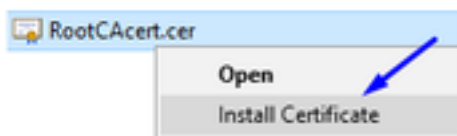
### 在员工Windows/Mac PC上安装根CA证书

方法 1：通过Windows Server组策略推送证书，在所有员工PC上安装证书（适合10个以上VPN用户的任何设备）：

[如何使用Windows Server通过组策略将证书分发到客户端计算机](#)

方法 2：在所有员工PC上安装证书，方法是在每台PC上单独安装证书（非常适合测试一个VPN用户）：

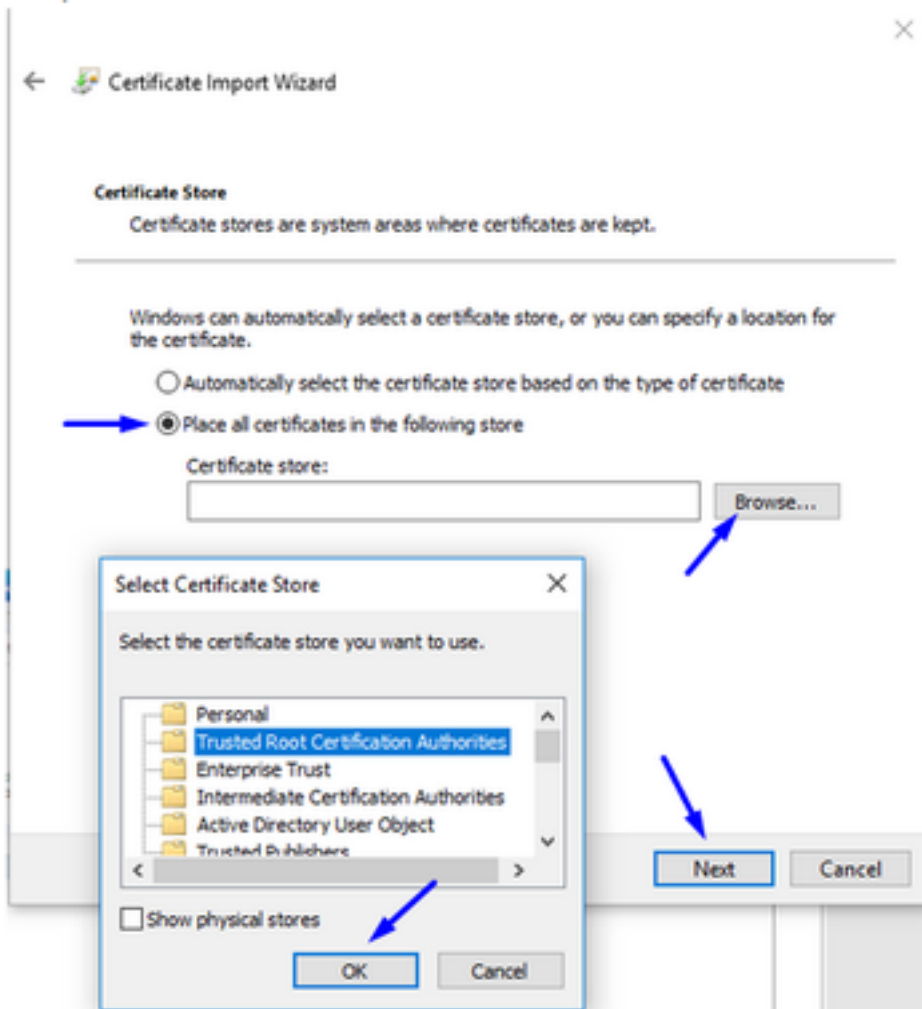
右键单击员工的Windows/Mac PC上的证书，然后单击“安装证书”



选择“当前用户”

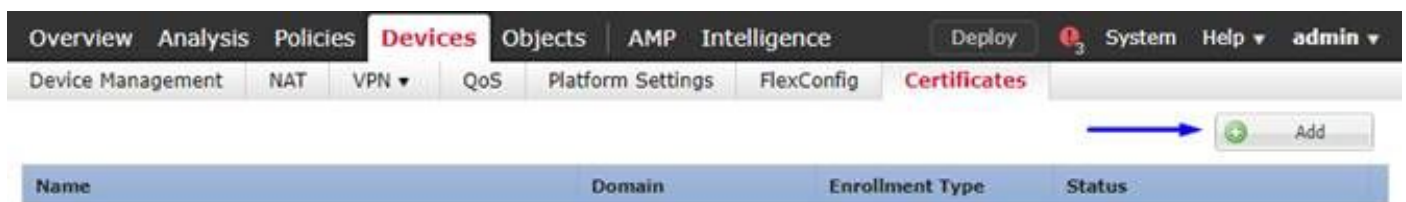


选择将所有证书放在以下存储中，然后选择受信任根证书颁发机构，单击确定，单击下一步，然后单击完成

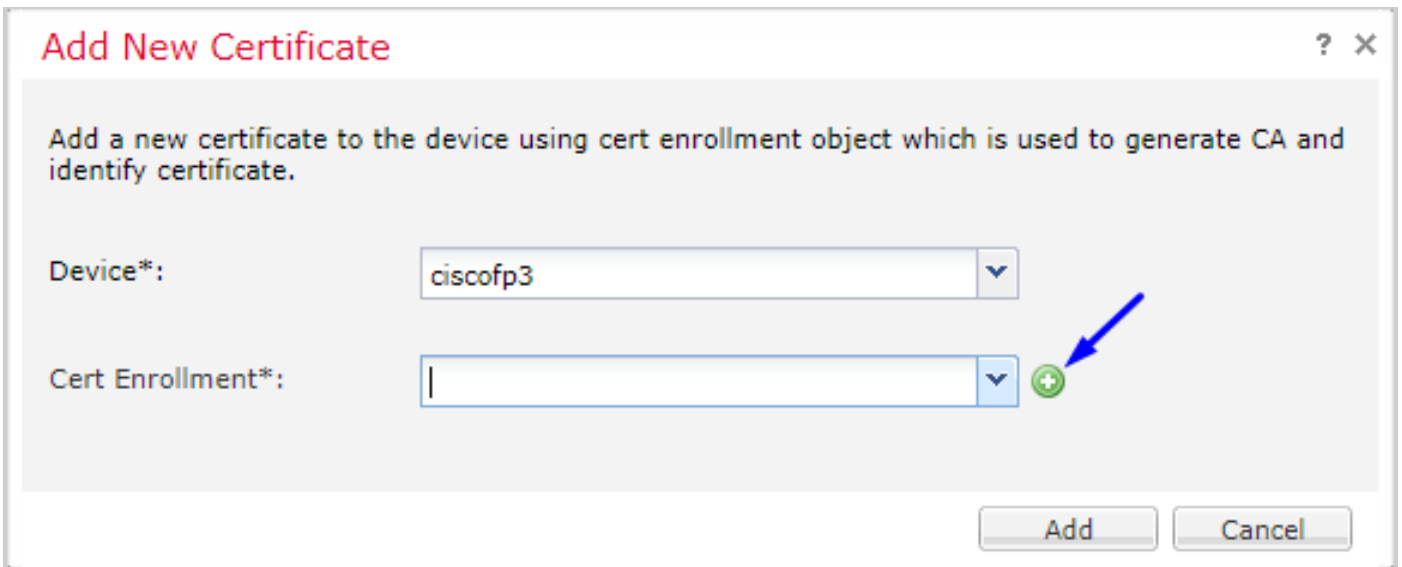


在FTD上生成CSR，获取由Windows Server根CA签名的CSR，并在FTD上安装该签名的证书

转至Objects > Object Management > PKI > Cert Enrollment，单击Add Cert Enrollment




单击“添加证书注册”按钮



**Add New Certificate** ? X

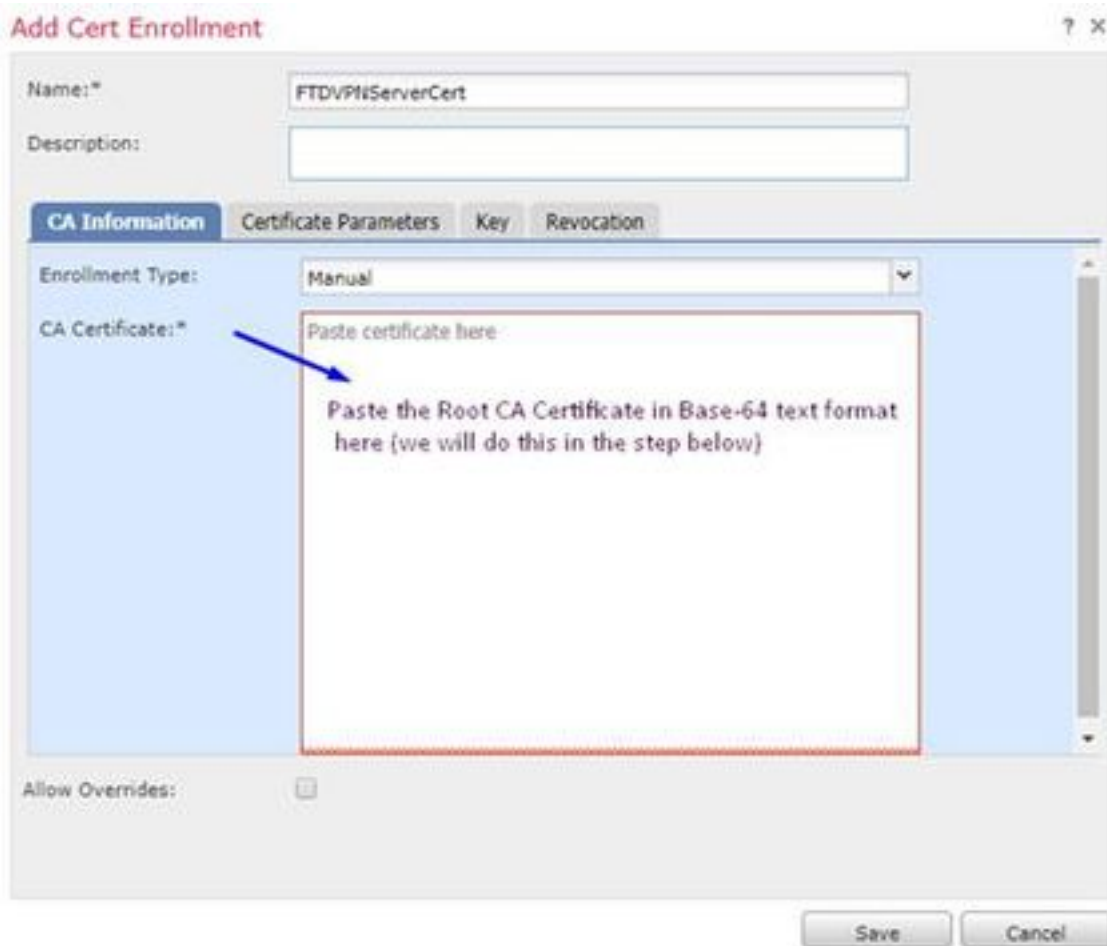
Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:  ▼

Cert Enrollment\*:  ▼ 

选择“登记类型”>“手动”

如下图所示，我们需要将根CA证书粘贴到此处：




**Add Cert Enrollment** ? X

Name\*:

Description:

**CA Information** | Certificate Parameters | Key | Revocation

Enrollment Type:  ▼

CA Certificate\*:    
Paste the Root CA Certificate in Base-64 text format here (we will do this in the step below)

Allow Overrides:

以下是如何下载您的根CA证书，以文本格式查看证书，并将其粘贴到上面的框中：

转至 <http://192.168.1.20/certsrv>

单击Download a CA certificate, certificate chain, or CRL

← → ↻ 🏠 192.168.1.20/certsrv/

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

### Welcome

Use this Web site to request a certificate for your Web browser, e communicate with over the Web, sign and encrypt messages, an

You can also use this Web site to download a certificate authority pending request.

For more information about Active Directory Certificate Services,

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

单击“Base 64”按钮>单击“Download CA Certificate”

← → ↻ 🏠 192.168.1.20/certsrv/certcarc.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.


CA certificate:

Current [cisco-CISCODC-CA]

Encoding method:

- DER
- Base 64

- [Install CA certificate](#)
- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)



RootCAcertBase64  
4.cer

在记事本中打开RootCAcertBase64.cer文件

从Windows AD Server复制并粘贴.cer内容（根CA证书）：



## Add Cert Enrollment



Name: \*

Description:

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate: \*

```
QgizA0KCRWEAA8INZPIHQWCWTDVK0PBRQDAGGDMR6GR10UEW
EB/wQFMAMBAf8wHQYD
VR00BBYEF0lpC7y9musCkmDJaKVus9bJUoMIMBAGCSsGAQQBg
jcVAQQDAgEBMCMG
CSsGAQQBgjcVAgQWBBQXIqPq2/dCT41fyYZHPxKhGEYNnzANBg
kqhkiG9w0BAQsF
AAOCAQEAOTa5S8Zw7RfarjTGm7HHJHZsA2p9CHdsvB/I35nYeac
OnxyeTWFN7by6
C43uyBFTWTpU3LlJr1mCgEo72qJErJOoU/Y4y7ADAKJF8RtUIb4H
Zq13XNW7Tu9X
DbZCTeYL7INbzZxPyfcuZWIBk5I8uHRvqq2YkBdx6YUYJocNTshH
WwZIXYvQPwwc
yjHrFjm0/YIQIJMhyIVULXXxWGP7diLIEQ67aHsdz+UZq9JofVYa
heHBjzbzIF
zvN2WWFXQs3mFMUxkrjEyzNlDws6vrm6ZhqjvOupzmeC6YqByK
QIEAggjevemL7Zd
8DufTZQ4E4VQ9Kp4hrSdzuHSggDTuw==
-----END CERTIFICATE-----
```

Allow Overrides:

单击**Certificate Parameters**选项卡>>键入您的证书信息

注意：

自定义FQDN字段必须是FTD的FQDN

公用名字段必须是FTD的FQDN

## Add Cert Enrollment



Name:\*

Description:

CA Information Certificate Parameters Key Revocation

Include FQDN:

Custom 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

提示：您可以通过从FTD CLI键入以下命令来获取FTD的FQDN:

```
> show network
===== [ System Information ] =====
Hostname : ciscofp3.cisco.com
Domains : cisco
DNS Servers : 192.168.1.20
Management port : 8305
IPv4 Default route
Gateway : 192.168.1.1

===== [ br1 ] =====
State : Enabled
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 00:0C:29:4F:AC:71
----- [ IPv4 ] -----
Configuration : Manual
Address : 192.168.1.2
Netmask : 255.255.255.0
```

单击“键”选项卡，然后键入任何键名

**Add Cert Enrollment** ? X

Name: \*

Description:

CA Information | Certificate Parameters | **Key** | Revocation

Key Type:  RSA  ECDSA

Key Name: \*

Key Size:

**Advanced Settings**

Ignore IPsec Key Usage  
Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.

Allow Overrides:

Save Cancel

点击**保存**

选择您的FTDVPNServerCert，然后单击“添加”(Add)

**Add New Certificate** ? X

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

Device\*:

Cert Enrollment\*:

**Cert Enrollment Details:**

Name: FTDVPNServerCert

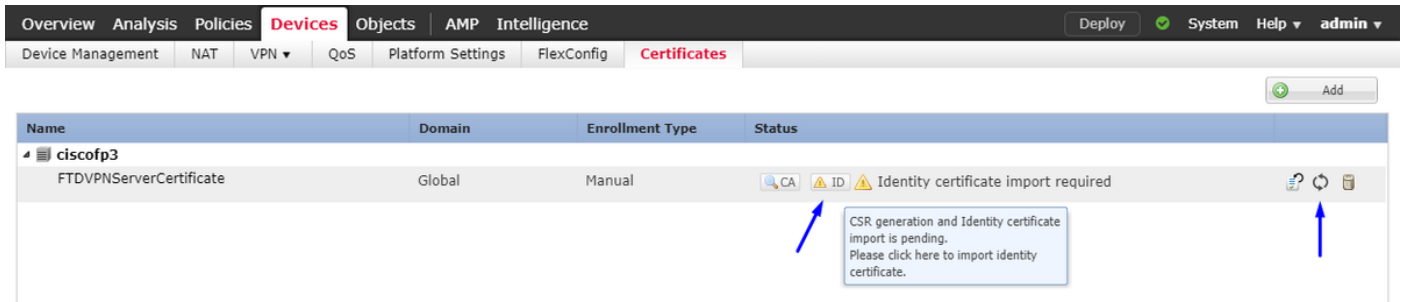
Enrollment Type: Manual

SCEP URL: NA

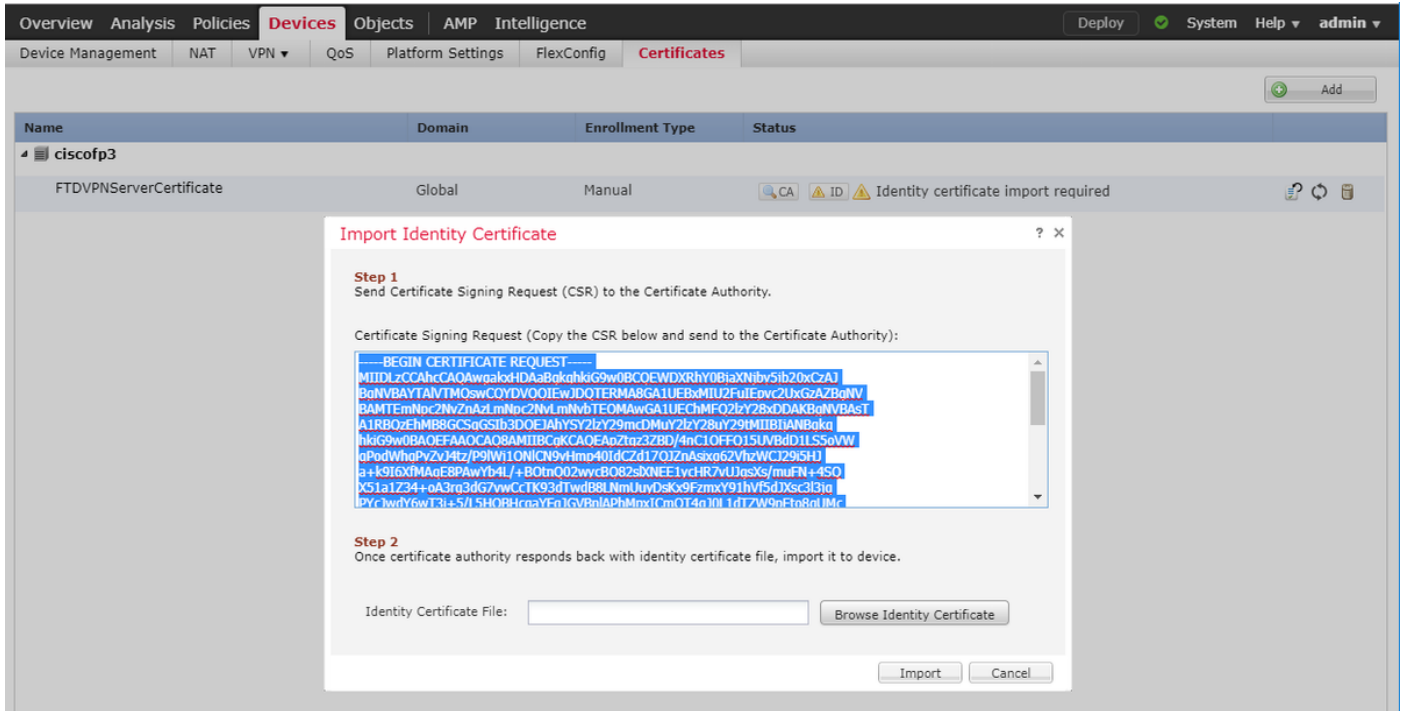
Add Cancel

提示：等待大约10-30秒，使FMC + FTD验证和安装根CA证书（如果未显示，请点击Refresh图标）

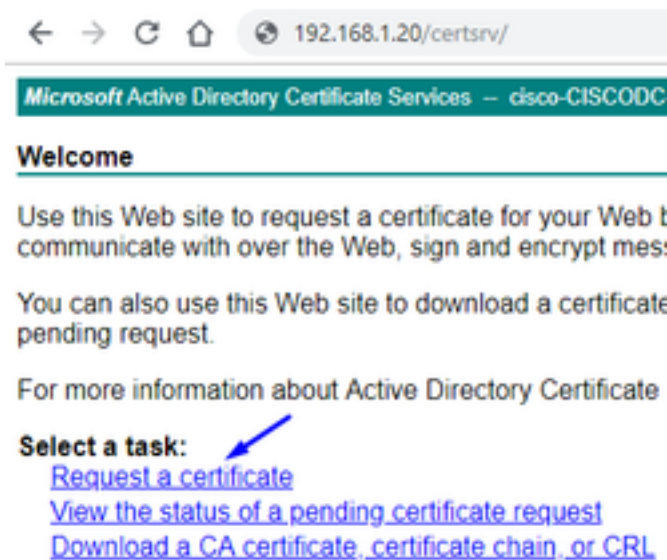
单击“ID”按钮：



复制并粘贴此CSR，并将其带到Windows Server根CA:



转至 <http://192.168.1.20/certsrv>



单击“高级证书请求”

← → ↻ 🏠 192.168.1.20/certsrv/certrqus.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

### Request a Certificate

Select the certificate type:  
[User Certificate](#)

Or, submit an [advanced certificate request](#).

将您的证书签名请求(CSR)粘贴到下面的字段中，然后选择**Web服务器**作为证书模板

← → ↻ 🏠 192.168.1.20/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
DbZCTeYL7lMbzZxPyfcuZw18k518uHRvqq2Yk8.
y1HrFjm0/YlIQIjJmhyIVULXXxMGP7d1LEQ67.
zvN2WwFXQs3mFMUxkrfEyzNlDws6vrm6ZhaJvO.
8DufT2Q4E4VQ9Kp4hr5dzuH5ggDTuv==
-----END CERTIFICATE-----
```

Certificate Template:  
Web Server

Additional Attributes:  
Attributes:


Submit >

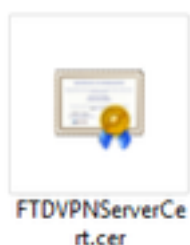
单击 **Submit**  
单击**Base 64 encoded**按钮，然后单击**Download certificate**

### Certificate Issued

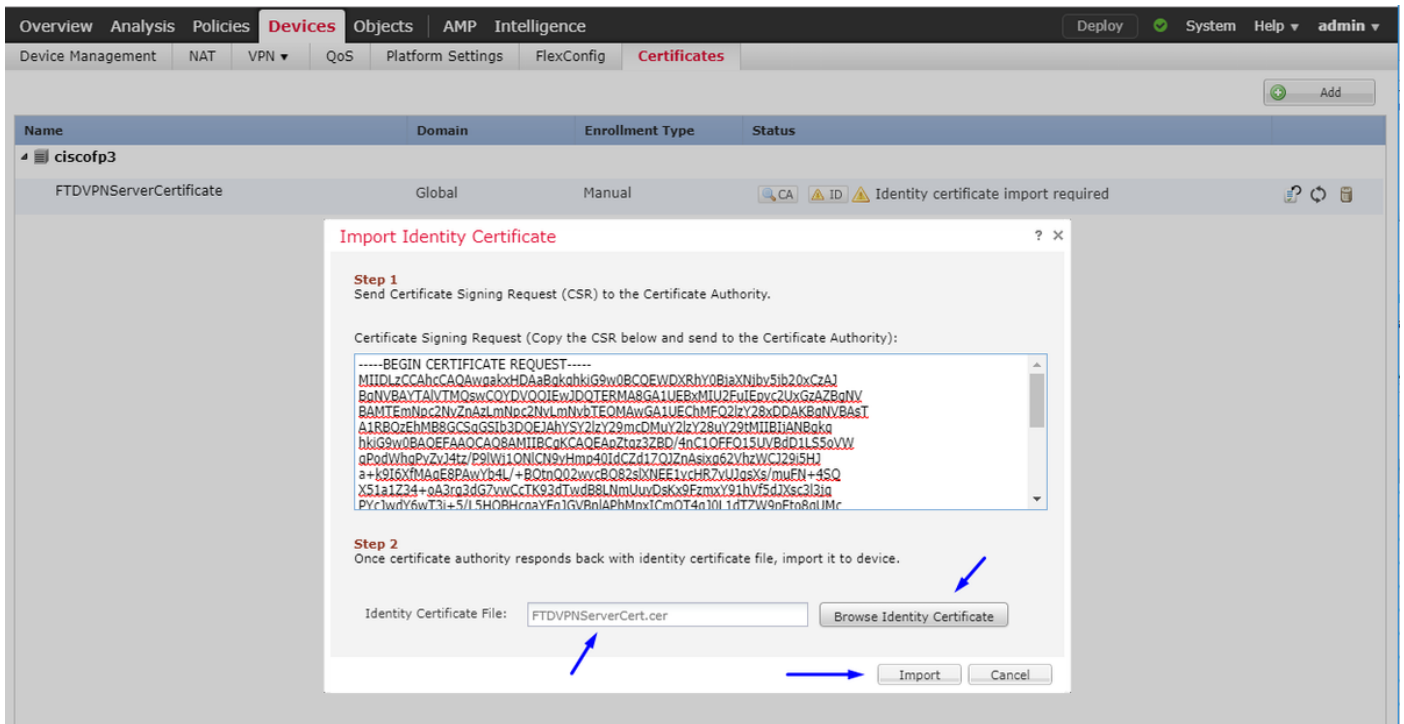
The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

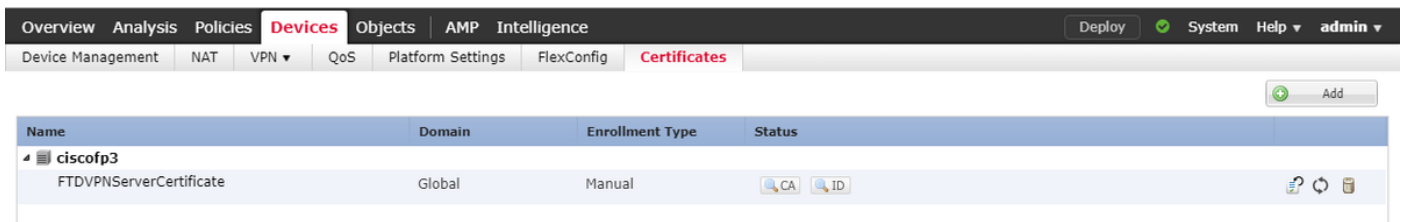
 [Download certificate](#)  
[Download certificate chain](#)



单击Browse Identity Certificate并选择我们刚下载的证书



已成功安装FTD VPN服务器证书 (由Windows Server根CA签名)



下载AnyConnect映像+ AnyConnect配置文件编辑器并创建.xml配置文件

下载并安装[Cisco AnyConnect配置文件编辑器](#)

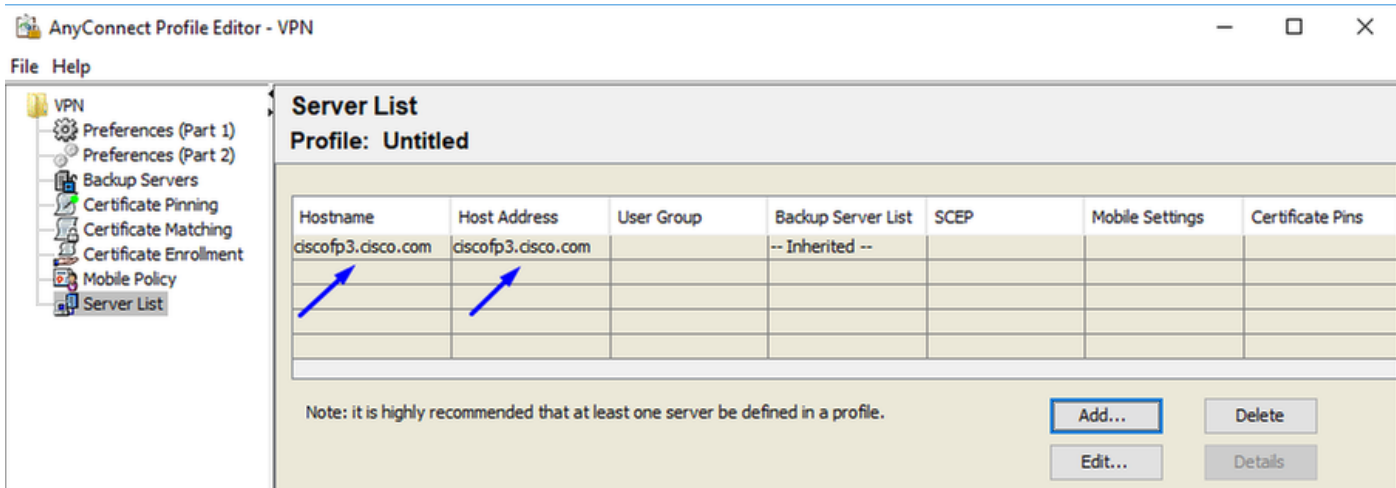
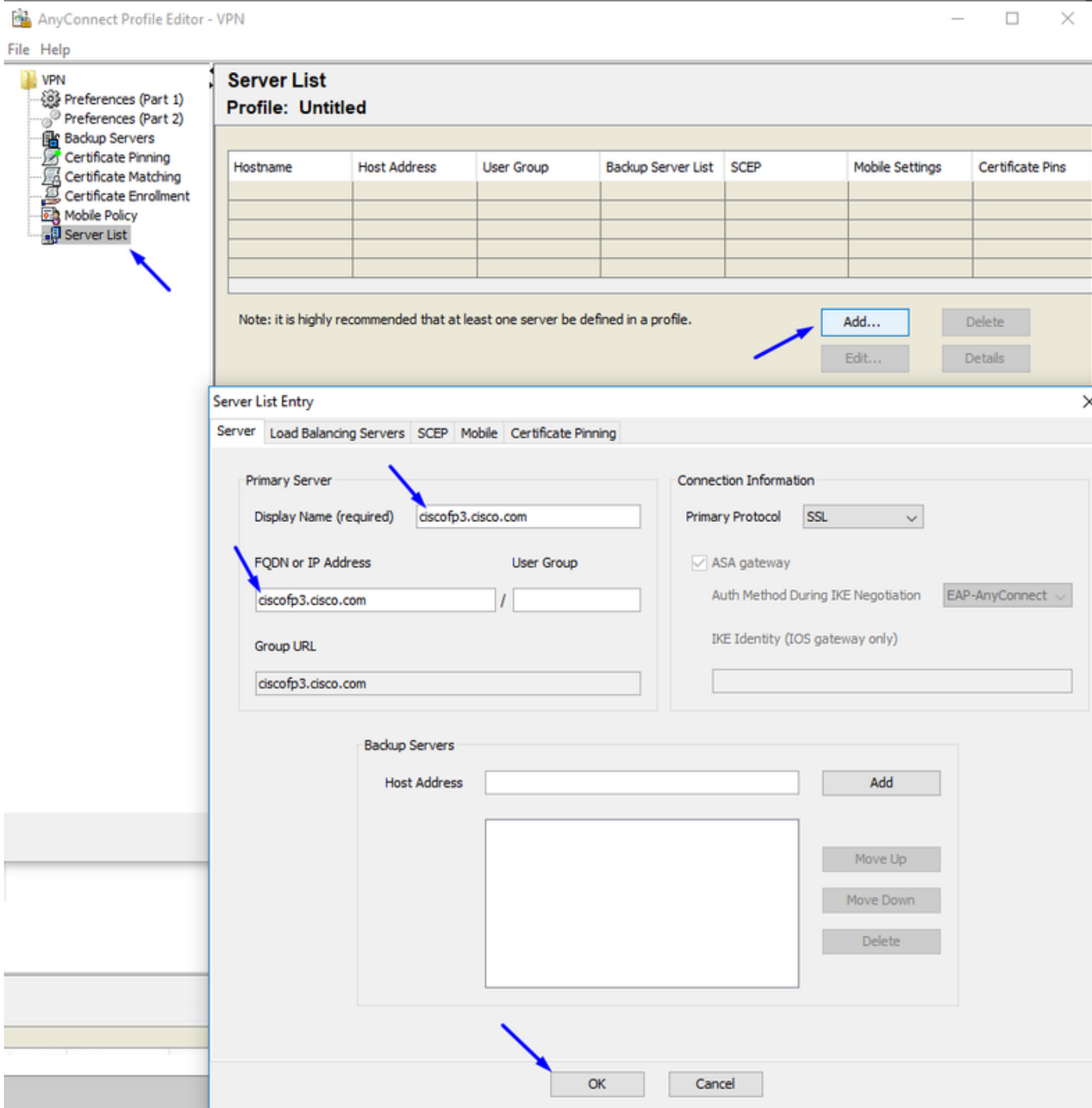


打开AnyConnect配置文件编辑器

单击Server List >单击Add ...

键入Display Name和FTD的外部接口IP地址的FQDN。您应在服务器列表中看到条目





单击确定并文件>另存为.....

VPNprofile.xml

从此处下载Windows和Mac .pkg映像

AnyConnect Headend Deployment Package (Windows) 	20-SEP-2018	41.34 MB
anyconnect-win-4.6.03049-webdeploy-k9.pkg		
AnyConnect Headend Deployment Package (Mac OS) 	20-SEP-2018	41.13 MB
anyconnect-macos-4.6.03049-webdeploy-k9.pkg		

转至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File

**Edit AnyConnect File** ? x

Name: \*

File Name: \*

File Type: \*  ▾

Description:

**Add AnyConnect File** ? x

Name: \*

File Name: \*

File Type: \*  ▾

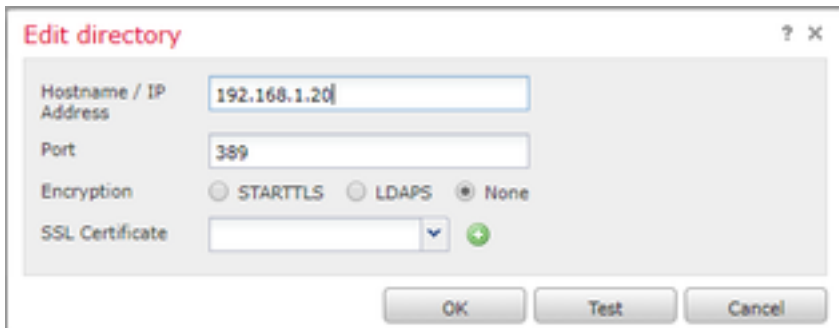
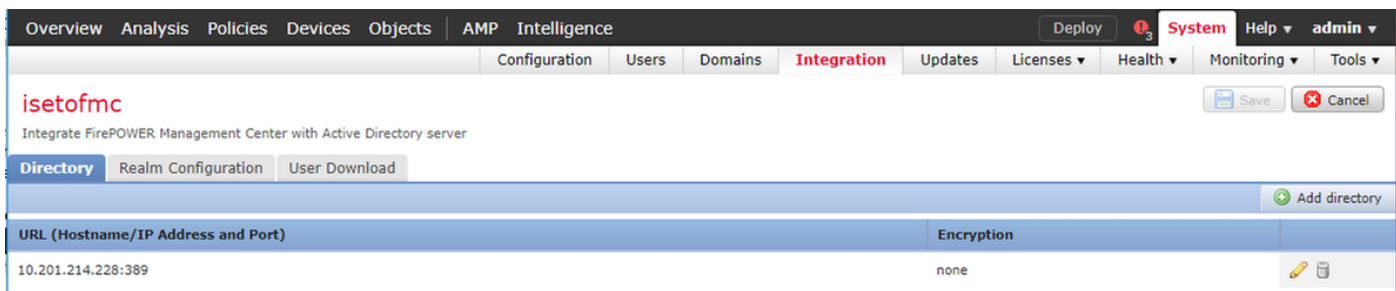
Description:

在FTD上配置Anyconnect VPN (使用根CA证书)

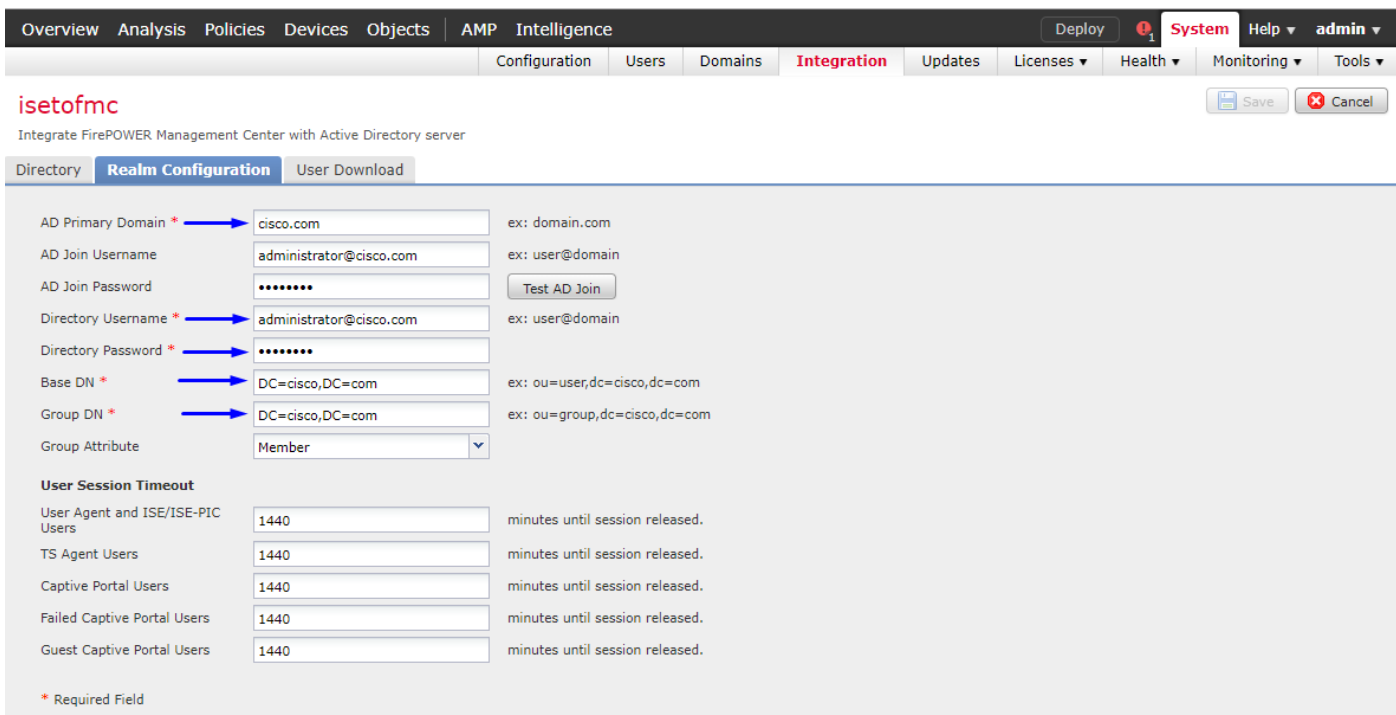
登录FirePOWER管理中心

单击System > Integration > Realms >单击New Realm >>单击Directory (目录) 选项卡>单击Add directory (添加目录)



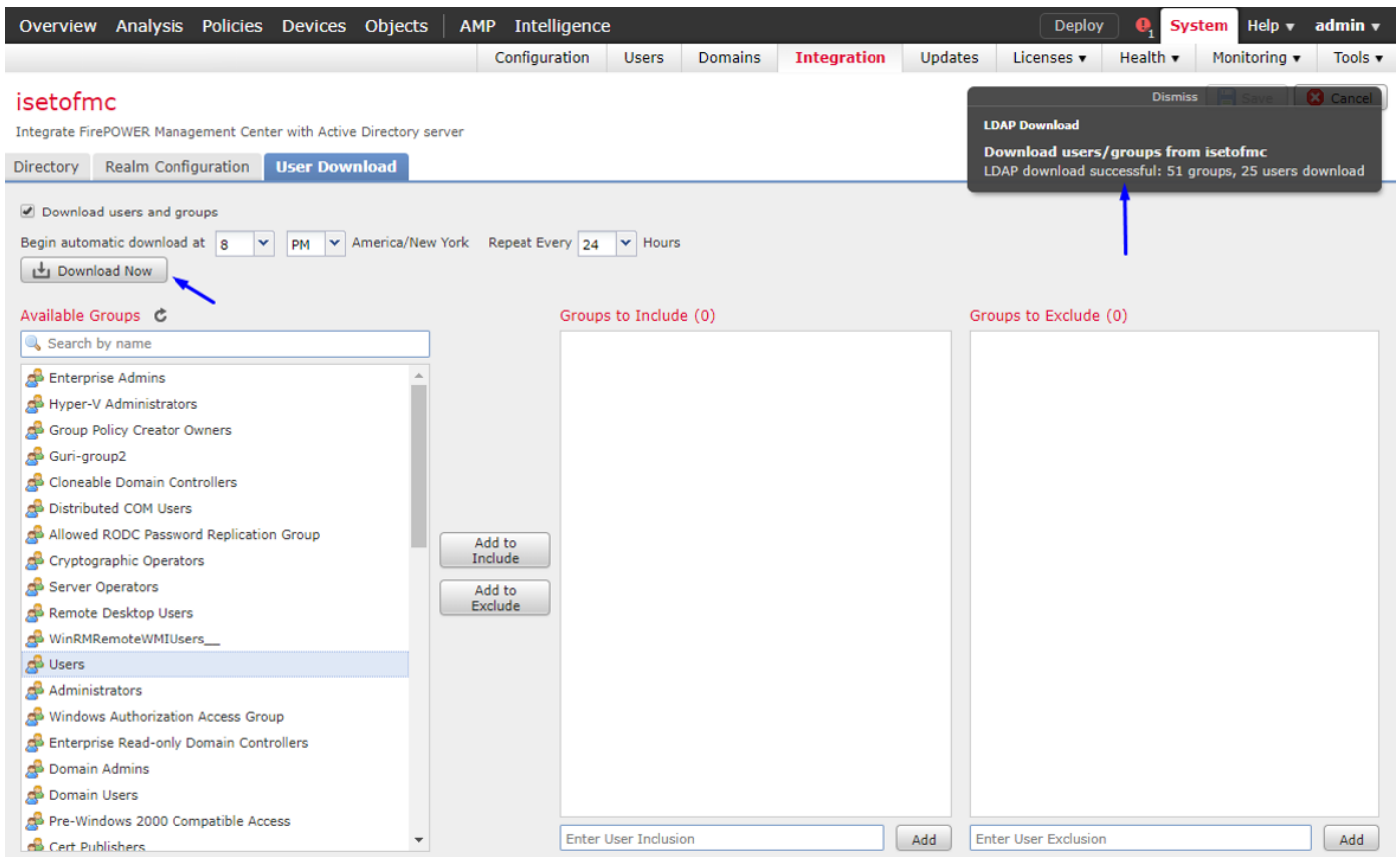


单击**领域配置**选项卡 — 在此处配置域控制器的信息

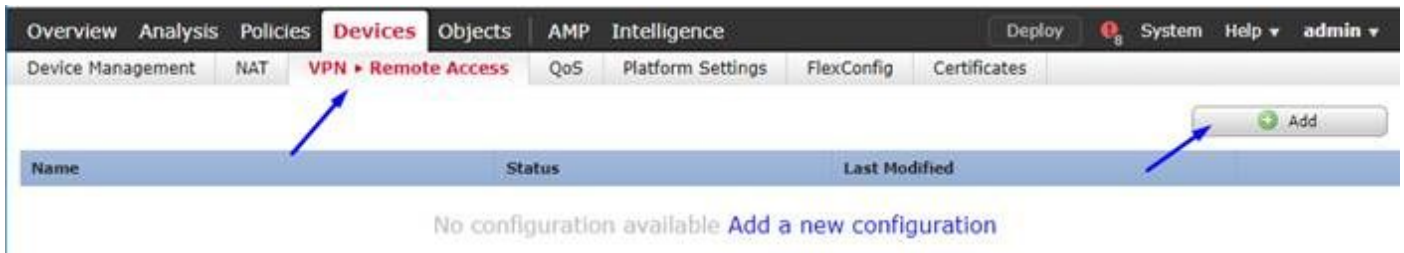


注意：在上例中，使用在Windows AD Server中具有“域管理”权限的AD用户名。如果要为用户配置更具体、最低权限的FMC，以加入Active Directory域进行领域配置，可以在此处看到步骤

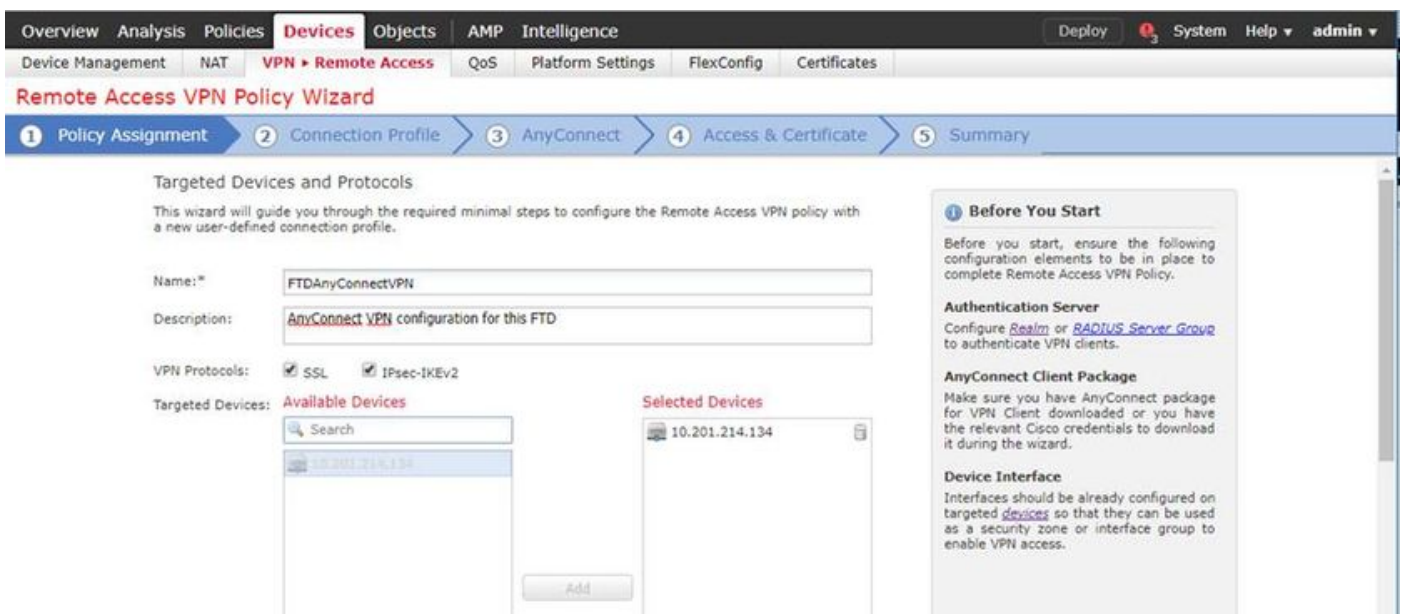
单击“**User Download ( 用户下载 )**”选项卡 — 确保“**User Download ( 用户下载 )**”成功



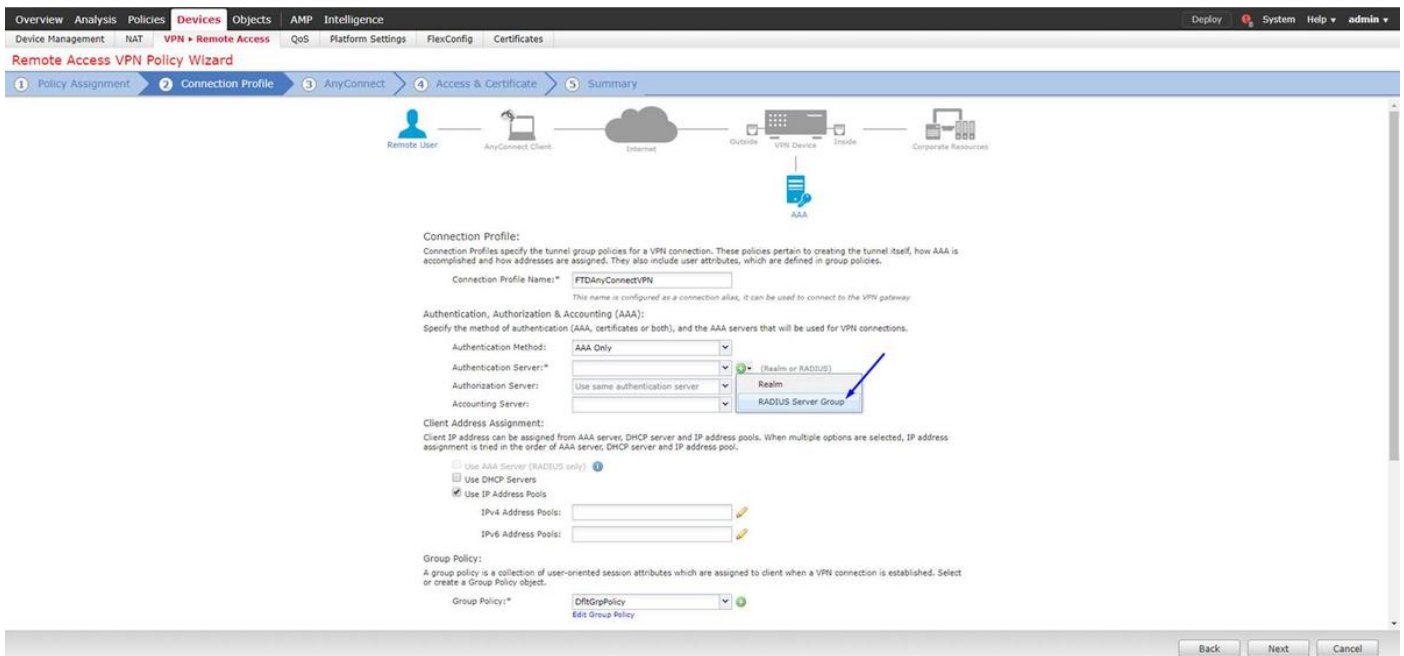
单击Devices > VPN >> Remote Access >单击Add



键入Name、Description，然后单击Add以选择要在上配置Anyconnect VPN的FTD设备



单击Add for the Authentication Server并选择RADIUS Server Group — 这将是您的思科身份服务引擎PSN (策略服务节点)



键入RADIUS服务器的名称  
选择上面配置的领域  
单击Add

### Add RADIUS Server Group

Name: CiscoISE

Description: Cisco ISE (Joined to Windows AD Server)

Group Accounting Mode: Single

Retry Interval: 10 (1-10) Seconds

Realms: isetofmc

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

为您的思科ISE节点键入以下信息：

IP地址/主机名:思科ISE PSN (策略服务节点) 的IP地址 — 这是身份验证请求的位置

密钥:Cisco123

确认密钥:Cisco123

**警告：**以上是您的RADIUS共享密钥 — 我们将在后续步骤中使用此密钥

**Edit RADIUS Server** ? X

IP Address/Hostname:\* 192.168.1.10  
Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:\* 1812 (1-65535)

Key:\* \*\*\*\*\*

Confirm Key:\* \*\*\*\*\*

Accounting Port: 1813 (1-65535)

Timeout: 10 (1-300) Seconds

Connect using:  Routing  Specific Interface ⓘ

Redirect ACL:

Save Cancel

**注意：**当最终用户尝试通过AnyConnect VPN连接到FTD时，他们键入的用户名+密码将作为身份验证请求发送到此FTD。FTD将该请求转发到思科ISE PSN节点进行身份验证（思科ISE随后将检查Windows Active Directory中的用户名和密码，并根据我们当前在思科ISE中配置的条件实施访问控制/网络访问）

**Add RADIUS Server Group** ? X

Name:\* CiscoISE

Description: Cisco ISE (joined to Windows AD server)

Group Accounting Mode: Single

Retry Interval:\* 10 (1-10) Seconds

Realms: isetofmd

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
192.168.1.10

Save Cancel

点击保存

## 单击Edit for IPv4 Address Pool

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN Remote Access QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

Remote User AnyConnect Client Internet VPN Device (Outside/Inside) Corporate Resources AAA

**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 Server\*  (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 Pools:  ⓘ  
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\*  ⓘ  
[Edit Group Policy](#)

Back Next Cancel

Last login on Wednesday, 2018-10-10 at 10:30:14 AM from 10.152.21.157

How-To Cisco

## 单击Add

Address Pools

Available IPv4 Pools  ⓘ

Selected IPv4 Pools

Add

Add

OK Cancel

键入Name、IPv4 Address Range和Subnet Mask

### Add 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)

Save Cancel

选择您的IP地址池，然后单击“确定”

### Address Pools

Available IPv4 Pools

Search

Inside-Pool

Selected IPv4 Pools

Inside-Pool  
192.168.10.50-192.168.10.250

Add

OK Cancel

单击Edit Group Policy



Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

### Remote Access VPN Policy Wizard

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

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 Server: \*  (Realm   
 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 Pools:    
 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: \*    
[Edit Group Policy](#)

单击“Anyconnect”选项卡> “配置文件”>单击“添加”

### Edit Group Policy

Name: \*   
 Description:

General **AnyConnect** Advanced

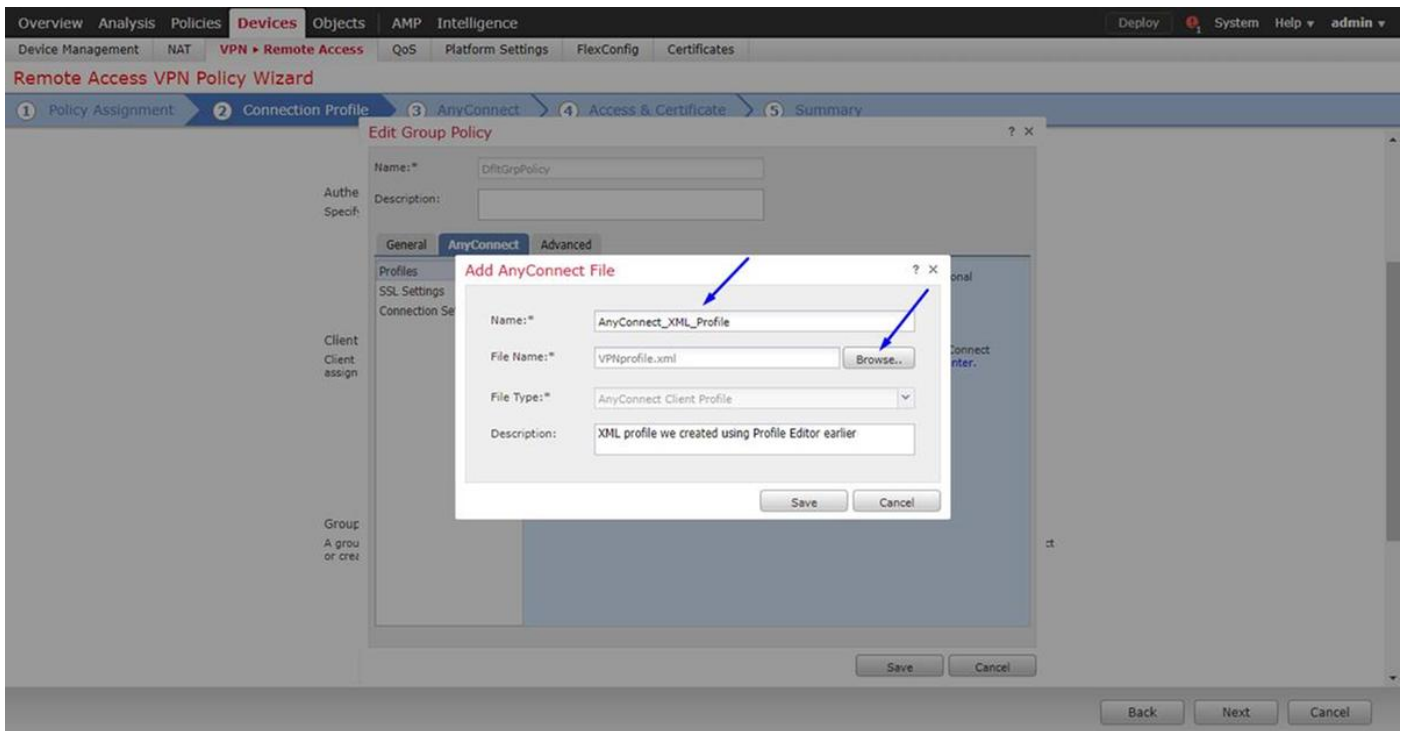
Profiles  
 SSL Settings  
 Connection Settings

AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.

Client Profile:

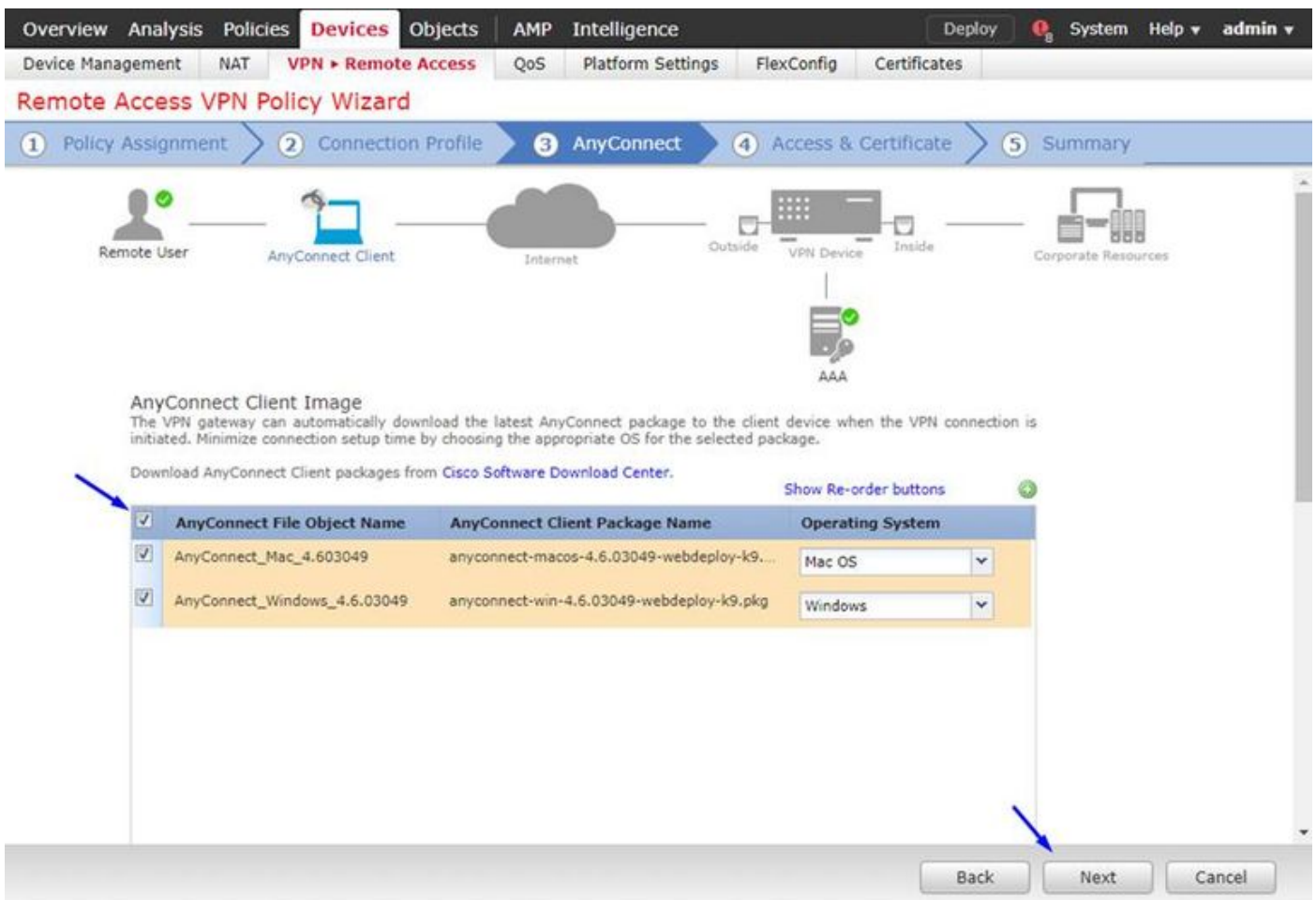
Standalone profile editor can be used to create a new or modify existing Anyconnect profile. You can download the profile editor from [Cisco Software Download Center](#).

键入名称并单击Browse...，然后从上述步骤4中选择您的VPNprofile.xml文件



单击“保存”，然后单击“下一步”

选中上述步骤4中AnyConnect Windows/Mac文件的复选框

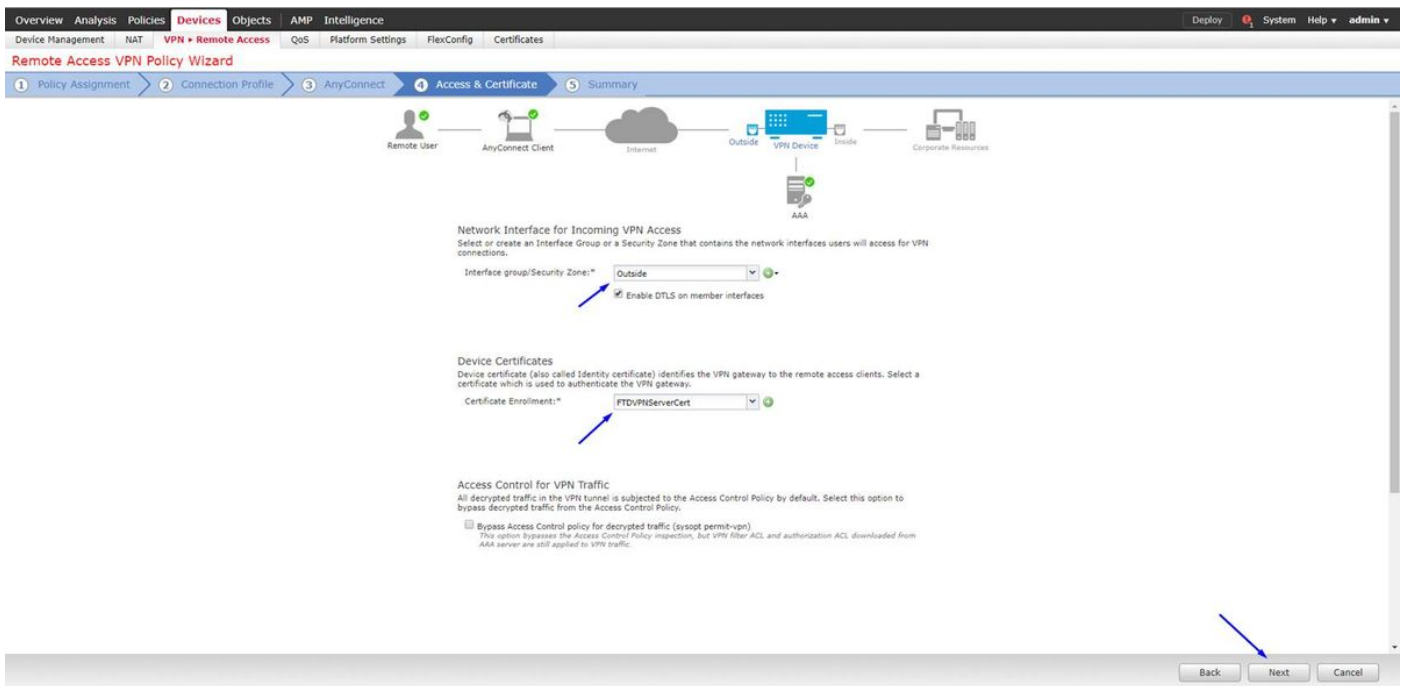


单击“下一步”

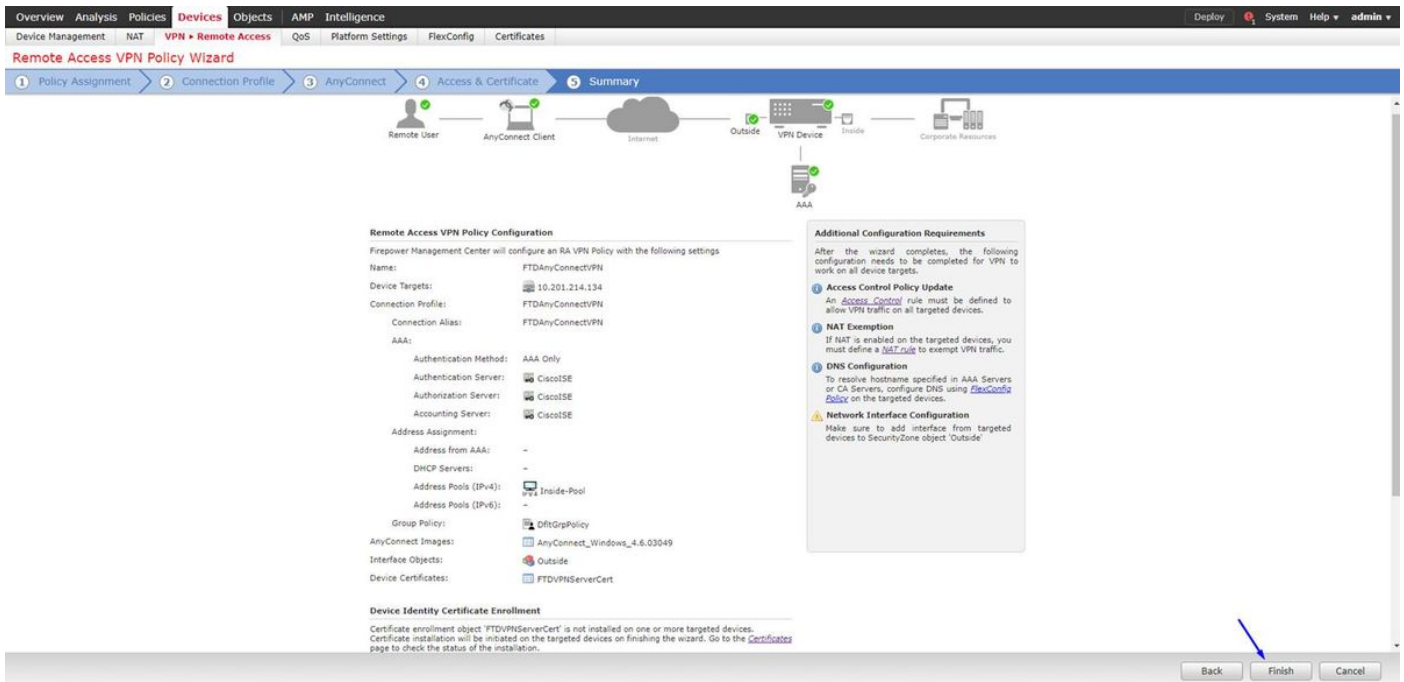
选择接口组/安全区域为外部

选择Certificate Enrollment作为我们在上述步骤3中创建的证书





查看您的配置并单击“下一步”



配置FTD NAT规则，使VPN流量免于NAT，因为它仍将被解密，并创建访问控制策略/规则

创建静态NAT规则以确保VPN流量不获得NAT'd(FTD在AnyConnect数据包进入外部接口时已将其解密，因此，PC好像已经位于内部接口后，并且它们已具有私有IP地址 — 我们仍需配置NAT-Exempt (否) NAT)规则):

转到“对象”>单击“添加网络”>单击“添加对象”

### Edit Network Objects ? X

Name:

Description:

Network:   
*Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)*

Allow Overrides:

### Edit Network Objects ? X

Name:

Description:

Network:   
*Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)*

Allow Overrides:

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Example\_Company\_NAT\_Policy Save Cancel

NAT policy Policy Assignments (1)

Rules Filter by Device Add Rule

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet		Translated Packet			Options
					Original Sources	Original Destinations	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before										
1	→	Static	Inside	Outside	inside-subnet	outside-subnet-anyconnect-pool	inside-subnet	outside-subnet-anyconnect-pool		Dns: false route-lookup no-proxy-arp
▼ Auto NAT Rules										
#	→	Dynamic	Inside	Outside	inside-subnet		Interface	inside-subnet		Dns: false
▼ NAT Rules After										

此外，必须允许数据流量在用户VPN进入后流动。您有两种选择：

a. 创建允许或拒绝规则允许或拒绝VPN用户访问某些资源

b. 启用“绕过已解密流量的访问控制策略”(Bypass Access Control Policy for decrypted traffic) — 这允许任何能够通过VPN绕过ACL成功连接到FTD并访问FTD后面任何内容的人，而无需通过访问控制策略中的“允许”或“拒绝”规则

在以下位置为已解密流量启用绕行访问控制策略：设备 > VPN > 远程访问 > VPN配置文件 > 接入接口：

## Access Control for VPN Traffic

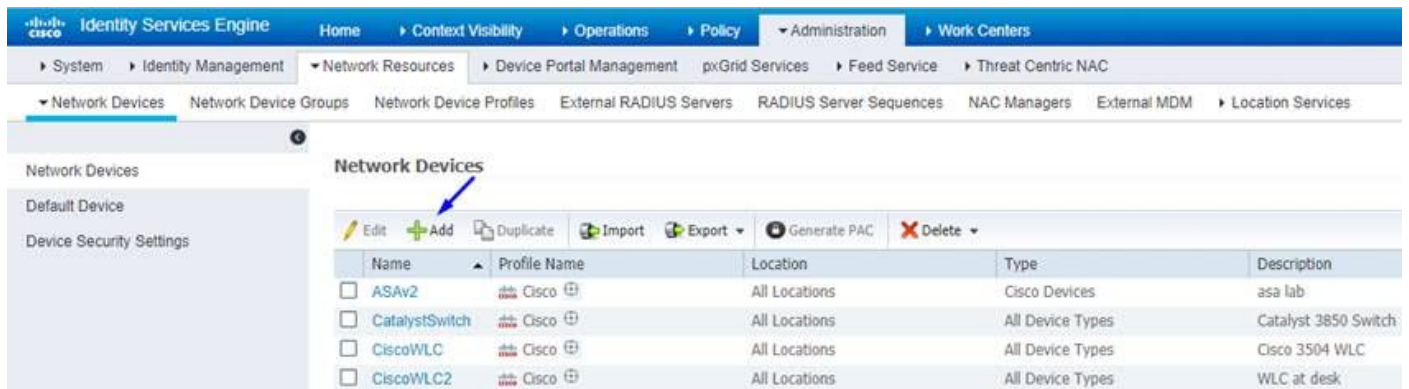
- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**  
*Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

注意：如果不启用此选项，则需要转到**Policies > Access Control Policy**并创建Allow规则，使VPN用户能够访问内部或dmz内的事物

点击FirePOWER管理中心右上角的部署

将FTD添加为网络设备并在思科ISE上配置策略集（使用RADIUS共享密钥）

登录到Cisco身份服务引擎，然后单击**Administration > Network Devices > Add**



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Network Resources' menu is further expanded to show 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', and 'Location Services'. The 'Network Devices' page is displayed, showing a table of existing devices and a toolbar with 'Edit', 'Add', 'Duplicate', 'Import', 'Export', 'Generate PAC', and 'Delete' buttons. A blue arrow points to the 'Add' button.

Name	Profile Name	Location	Type	Description
<input type="checkbox"/> ASAv2	Cisco	All Locations	Cisco Devices	asa lab
<input type="checkbox"/> CatalystSwitch	Cisco	All Locations	All Device Types	Catalyst 3850 Switch
<input type="checkbox"/> CiscoWLC	Cisco	All Locations	All Device Types	Cisco 3504 WLC
<input type="checkbox"/> CiscoWLC2	Cisco	All Locations	All Device Types	WLC at desk

键入**Name**，键入FTD的IP地址，然后在上述步骤中键入**RADIUS共享密钥**

警告：这必须是FTD可以到达您的思科ISE（RADIUS服务器）的接口/IP地址，即您的思科ISE可以通过FTD到达的FTD接口

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices List > FTDVPN

Network Devices

Default Device.

Device Security Settings.

\* Name

Description

IP Address \* IP:  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

\* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

单击Policy > Policy Set >为进入以下类型的任何身份验证请求创建Policy Set:

**RADIUS-NAS — 端口类型等于虚拟**

这意味着，如果进入ISE的任何RADIUS请求看起来像VPN连接，它们将点击此策略集

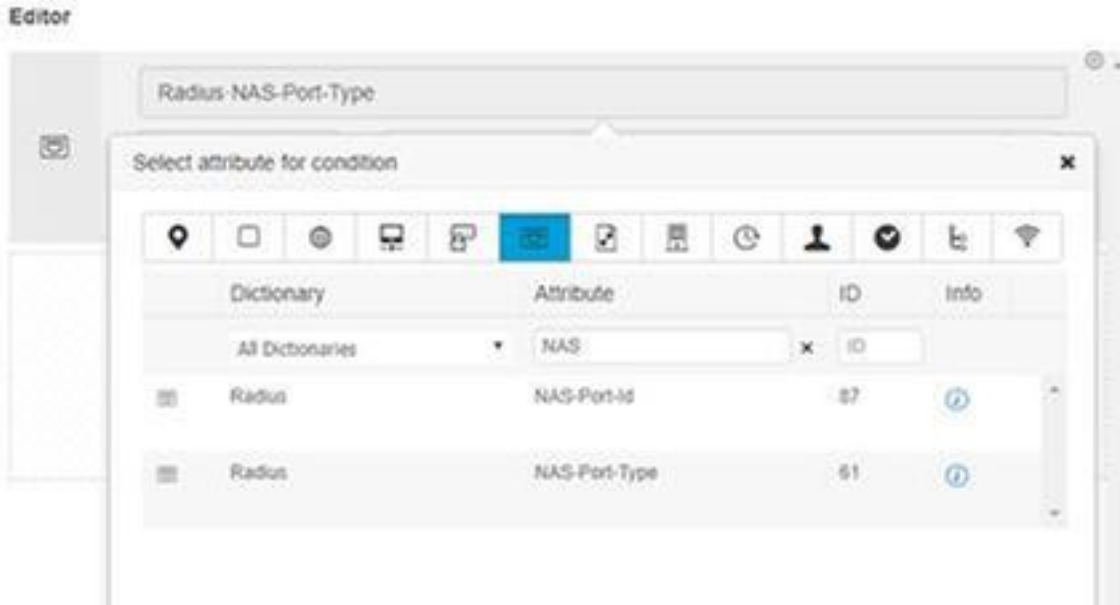
Identity Services Engine Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

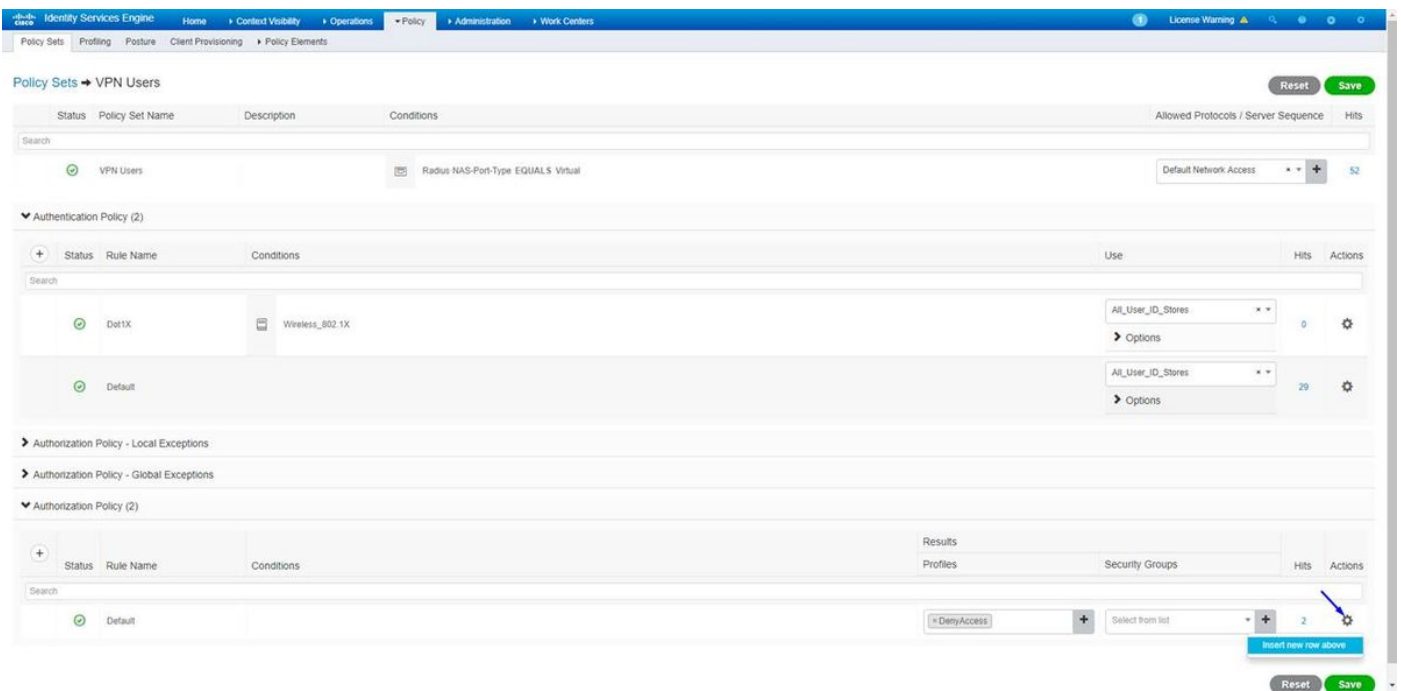
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	QuestSSID		Airspace Airspace-Wan-Id EQUALS 1	Default Network Access	181	<input type="button" value="i"/> <input type="button" value="x"/>	<input type="button" value="x"/>
<input checked="" type="checkbox"/>	EmployeeSSID		Airspace Airspace-Wan-Id EQUALS 2	Default Network Access	686	<input type="button" value="i"/> <input type="button" value="x"/>	<input type="button" value="x"/>
<input checked="" type="checkbox"/>	Users		Radius NAS-Port-Type EQUALS Virtual	Default Network Access		<input type="button" value="i"/> <input type="button" value="x"/>	<input type="button" value="x"/>
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	1300	<input type="button" value="i"/> <input type="button" value="x"/>	<input type="button" value="x"/>

您可以在思科ISE中找到该条件：



### 编辑您在上面创建的策略集

在默认阻止规则上方添加规则，仅在人员位于名为“Employees”的Active Directory组中时，才为其提供Permit Access授权配置文件：



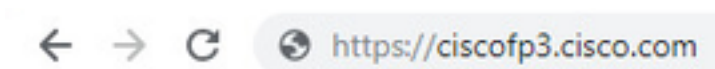
下面是规则完成后的外观

The screenshot displays the Cisco ISE Policy Sets configuration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area is titled 'Policy Sets → VPN Users' and contains several sections:

- Authentication Policy (2):** A table listing policies like 'Dot1X' and 'Default' with their respective conditions and hit counts.
- Authorization Policy - Local Exceptions:** A section for local exceptions.
- Authorization Policy - Global Exceptions:** A section for global exceptions.
- Authorization Policy (2):** A table listing policies like 'Allow FTD VPN connections if AD Group VPNUsers' and 'Default'. Two blue arrows point to the 'Conditions' column, highlighting the rule 'cisco:dc:ExternalGroups EQUALS cisco.com/Users/Employees'.

在员工Windows/Mac PC上使用AnyConnect VPN客户端下载、安装并连接到FTD

在员工Windows/Mac PC上打开浏览器，在浏览器中转到FTD的外部地址



键入Active Directory用户名和密码

Logon

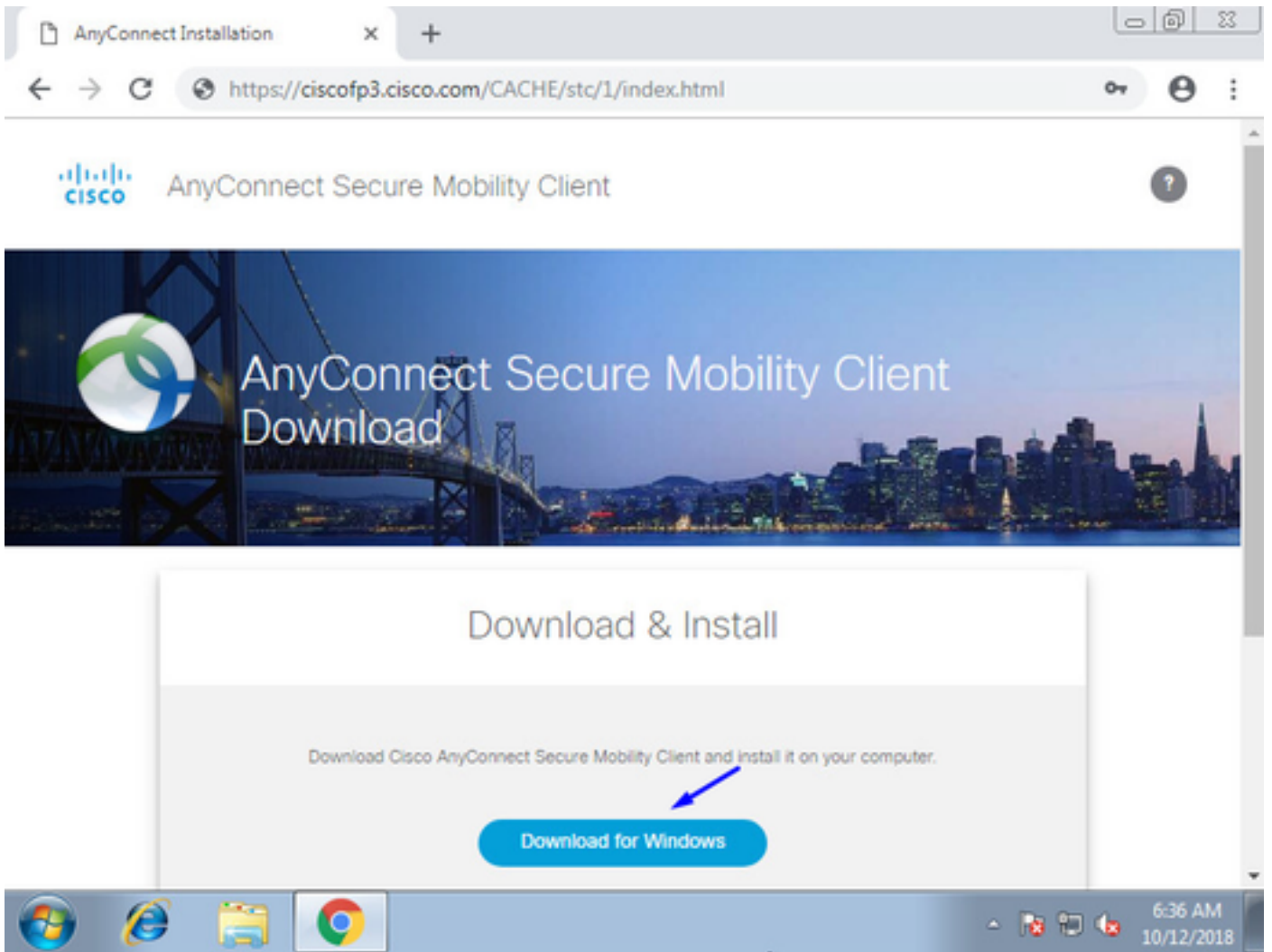
Group

Username

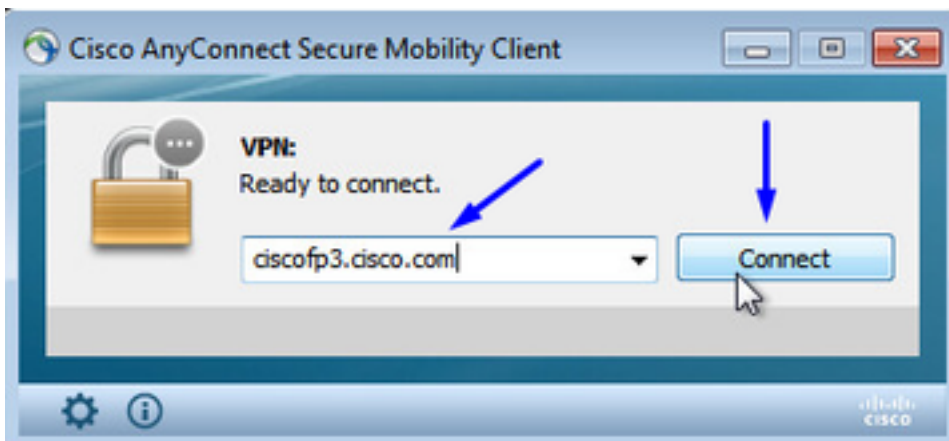
Password

单击“下载”





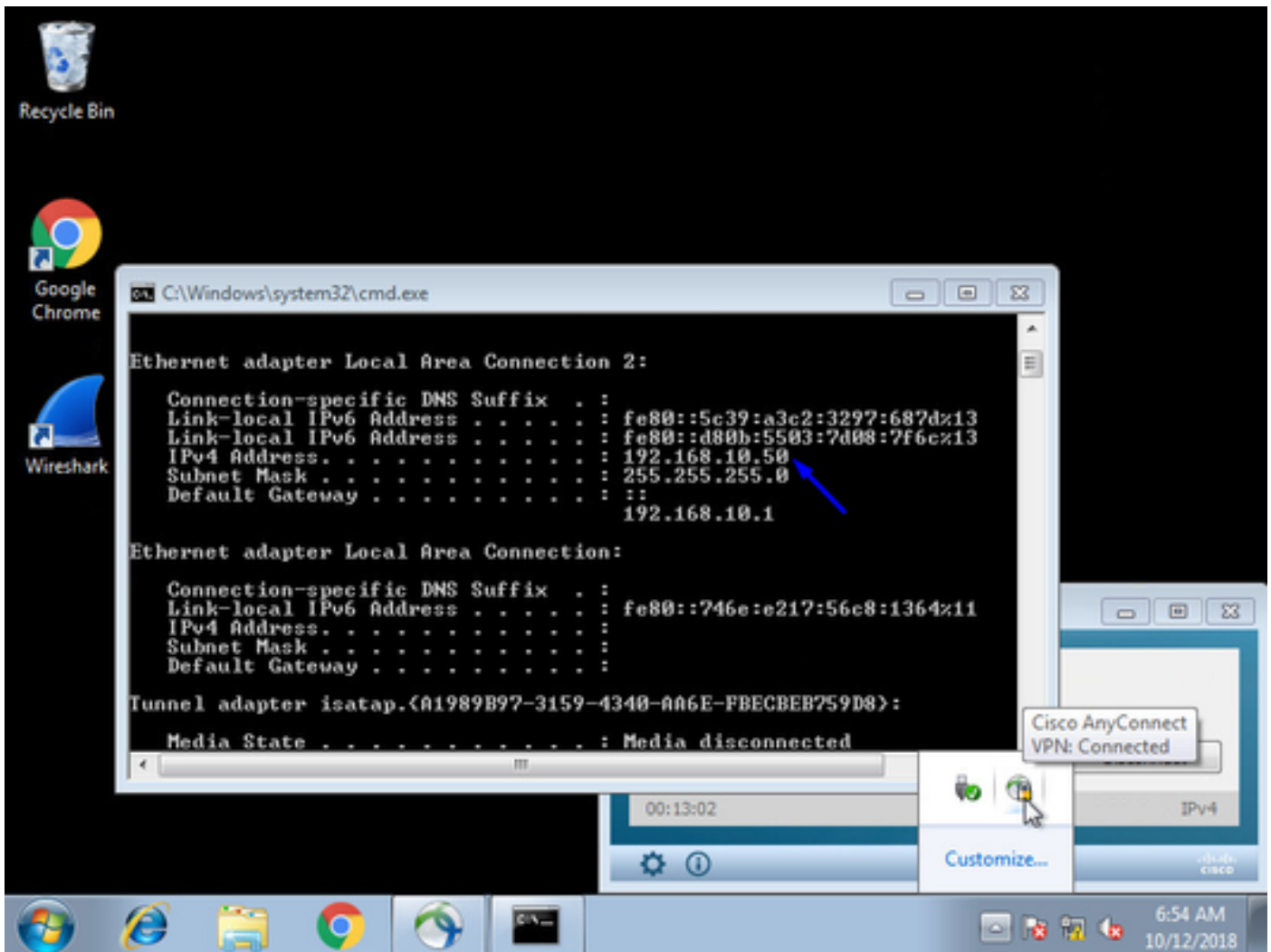
在Windows/Mac PC上安装并运行AnyConnect VPN安全移动客户端



出现提示时，键入Active Directory用户名和密码

您将获得第5步中创建的IP地址池的IP地址，以及该子网中。1的默认网关





## 验证

### FTD

### 显示命令

在FTD上验证最终用户是否已连接到AnyConnect VPN:

```
> show ip
```

```
System IP Addresses:
```

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	inside	192.168.1.1	255.255.255.240	CONFIG
GigabitEthernet0/1	outside	203.0.113.2	255.255.255.240	CONFIG

```
Current IP Addresses:
```

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	inside	192.168.1.1	255.255.255.240	CONFIG
GigabitEthernet0/1	outside	203.0.113.2	255.255.255.240	CONFIG

```
> show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : jsmith Index : 2
```

```
Assigned IP : 192.168.10.50 Public IP : 198.51.100.2
```

```
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 : 18458 Bytes Rx : 2706024  
Pkts Tx : 12 Pkts Rx : 50799  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : DfltGrpPolicy Tunnel Group : FTDAnyConnectVPN  
Login Time : 15:08:19 UTC Wed Oct 10 2018  
Duration : 0h:30m:11s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 0ac9d68a000020005bbe15e3  
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:  
Tunnel ID : 2.1  
**Public IP : 198.51.100.2**  
Encryption : none Hashing : none  
TCP Src Port : 53956 TCP Dst Port : 443  
Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 0 Minutes  
Client OS : win  
Client OS Ver: 6.1.7601 Service Pack 1  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049  
Bytes Tx : 10572 Bytes Rx : 289  
Pkts Tx : 6 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:  
Tunnel ID : 2.2  
**Assigned IP : 192.168.10.50 Public IP : 198.51.100.2**  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384  
Encapsulation: TLSv1.2 TCP Src Port : 54634  
TCP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049  
Bytes Tx : 7886 Bytes Rx : 2519  
Pkts Tx : 6 Pkts Rx : 24  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:  
Tunnel ID : 2.3  
**Assigned IP : 192.168.10.50 Public IP : 198.51.100.2**  
Encryption : AES256 Hashing : SHA1  
Ciphersuite : DHE-RSA-AES256-SHA  
Encapsulation: DTLSv1.0 UDP Src Port : 61113  
UDP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049  
Bytes Tx : 0 Bytes Rx : 2703216  
Pkts Tx : 0 Pkts Rx : 50775  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

在Windows 7 PC上单击Cisco AnyConnect客户端上的“断开连接”后，您将获得：

```
> show vpn-sessiondb detail anyconnect
INFO: There are presently no active sessions
```

## 捕获

在AnyConnect客户端上点击连接时，工作捕获在外部接口上的外观

示例：

例如，最终用户的公有IP将是其家中路由器的公有IP

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
```

```
<now hit Connect on AnyConnect Client from employee PC>
```

```
ciscofp3# show cap
```

```
capture capin type raw-data trace detail trace-count 100 interface outside [Buffer Full - 524153 bytes]
```

```
match ip any host 198.51.100.2
```

查看从最终用户PC到达FTD外部接口的数据包，以确保它们到达我们的外部FTD接口：

```
ciscofp3# show cap capin
```

```
2375 packets captured
```

```
1: 17:05:56.580994      198.51.100.2.55928 > 203.0.113.2.443: S 2933933902:2933933902(0) win
8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
2: 17:05:56.581375      203.0.113.2.443 > 198.51.100.2.55928: S 430674106:430674106(0) ack
2933933903 win 32768 <mss 1460>
3: 17:05:56.581757      198.51.100.2.55928 > 203.0.113.2.443: . ack 430674107 win 64240
4: 17:05:56.582382      198.51.100.2.55928 > 203.0.113.2.443: P 2933933903:2933934036(133) ack
430674107 win 64240
5: 17:05:56.582458      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933934036 win 32768
6: 17:05:56.582733      203.0.113.2.443 > 198.51.100.2.55928: P 430674107:430675567(1460) ack
2933934036 win 32768
7: 17:05:56.790211      198.51.100.2.55928 > 203.0.113.2.443: . ack 430675567 win 64240
8: 17:05:56.790349      203.0.113.2.443 > 198.51.100.2.55928: P 430675567:430676672(1105) ack
2933934036 win 32768
9: 17:05:56.791691      198.51.100.2.55928 > 203.0.113.2.443: P 2933934036:2933934394(358) ack
430676672 win 63135
10: 17:05:56.794911      203.0.113.2.443 > 198.51.100.2.55928: P 430676672:430676763(91) ack
2933934394 win 32768
11: 17:05:56.797077      198.51.100.2.55928 > 203.0.113.2.443: P 2933934394:2933934703(309) ack
430676763 win 63044
12: 17:05:56.797169      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933934703 win 32768
13: 17:05:56.797199      198.51.100.2.55928 > 203.0.113.2.443: P 2933934703:2933935524(821) ack
430676763 win 63044
14: 17:05:56.797276      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933935524 win 32768
15: 17:05:56.798634      203.0.113.2.443 > 198.51.100.2.55928: P 430676763:430677072(309) ack
2933935524 win 32768
16: 17:05:56.798786      203.0.113.2.443 > 198.51.100.2.55928: P 430677072:430677829(757) ack
2933935524 win 32768
17: 17:05:56.798817      203.0.113.2.443 > 198.51.100.2.55928: P 430677829:430677898(69) ack
2933935524 win 32768
18: 17:05:56.799397      198.51.100.2.55928 > 203.0.113.2.443: . ack 430677898 win 64240
19: 17:05:56.810215      198.51.100.2.55928 > 203.0.113.2.443: P 2933935524:2933935593(69) ack
430677898 win 64240
20: 17:05:56.810398      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933935593 win 32768
21: 17:05:56.810428      198.51.100.2.55928 > 203.0.113.2.443: F 2933935593:2933935593(0) ack
430677898 win 64240
```

22: 17:05:56.810489 203.0.113.2.443 > 198.51.100.2.55928: . ack 2933935594 win 32768  
23: 17:05:56.810627 203.0.113.2.443 > 198.51.100.2.55928: FP 430677898:430677898(0) ack  
2933935594 win 32768  
24: 17:05:56.811008 198.51.100.2.55928 > 203.0.113.2.443: . ack 430677899 win 64240  
25: 17:05:59.250566 198.51.100.2.56228 > 203.0.113.2.443: S 2614357960:2614357960(0) win  
8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>  
26: 17:05:59.250963 203.0.113.2.443 > 198.51.100.2.56228: S 3940915253:3940915253(0) ack  
2614357961 win 32768 <mss 1460>  
27: 17:05:59.251406 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940915254 win 64240  
28: 17:05:59.252062 198.51.100.2.56228 > 203.0.113.2.443: P 2614357961:2614358126(165) ack  
3940915254 win 64240  
29: 17:05:59.252138 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614358126 win 32768  
30: 17:05:59.252458 203.0.113.2.443 > 198.51.100.2.56228: P 3940915254:3940915431(177) ack  
2614358126 win 32768  
31: 17:05:59.253450 198.51.100.2.56228 > 203.0.113.2.443: P 2614358126:2614358217(91) ack  
3940915431 win 64063  
32: 17:05:59.253679 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614358217 win 32768  
33: 17:05:59.255235 198.51.100.2.56228 > 203.0.113.2.443: P 2614358217:2614358526(309) ack  
3940915431 win 64063  
34: 17:05:59.255357 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614358526 win 32768  
35: 17:05:59.255388 198.51.100.2.56228 > 203.0.113.2.443: P 2614358526:2614359555(1029)  
ack 3940915431 win 64063  
36: 17:05:59.255495 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614359555 win 32768  
37: 17:05:59.400110 203.0.113.2.443 > 198.51.100.2.56228: P 3940915431:3940915740(309) ack  
2614359555 win 32768  
38: 17:05:59.400186 203.0.113.2.443 > 198.51.100.2.56228: P 3940915740:3940917069(1329)  
ack 2614359555 win 32768  
39: 17:05:59.400675 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940917069 win 64240  
40: 17:05:59.400736 203.0.113.2.443 > 198.51.100.2.56228: P 3940917069:3940918529(1460)  
ack 2614359555 win 32768  
41: 17:05:59.400751 203.0.113.2.443 > 198.51.100.2.56228: P 3940918529:3940919979(1450)  
ack 2614359555 win 32768  
42: 17:05:59.401544 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940919979 win 64240  
43: 17:05:59.401605 203.0.113.2.443 > 198.51.100.2.56228: P 3940919979:3940921439(1460)  
ack 2614359555 win 32768  
44: 17:05:59.401666 203.0.113.2.443 > 198.51.100.2.56228: P 3940921439:3940922899(1460)  
ack 2614359555 win 32768  
45: 17:05:59.401727 203.0.113.2.443 > 198.51.100.2.56228: P 3940922899:3940923306(407) ack  
2614359555 win 32768  
46: 17:05:59.401743 203.0.113.2.443 > 198.51.100.2.56228: P 3940923306:3940923375(69) ack  
2614359555 win 32768  
47: 17:05:59.402185 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940923375 win 64240  
48: 17:05:59.402475 198.51.100.2.56228 > 203.0.113.2.443: P 2614359555:2614359624(69) ack  
3940923375 win 64240  
49: 17:05:59.402597 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614359624 win 32768  
50: 17:05:59.402628 198.51.100.2.56228 > 203.0.113.2.443: F 2614359624:2614359624(0) ack  
3940923375 win 64240  
51: 17:05:59.402673 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614359625 win 32768  
52: 17:05:59.402765 203.0.113.2.443 > 198.51.100.2.56228: FP 3940923375:3940923375(0) ack  
2614359625 win 32768  
53: 17:05:59.413384 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940923376 win 64240  
54: 17:05:59.555665 198.51.100.2.56280 > 203.0.113.2.443: S 1903869753:1903869753(0) win  
8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>  
55: 17:05:59.556154 203.0.113.2.443 > 198.51.100.2.56280: S 2583094766:2583094766(0) ack  
1903869754 win 32768 <mss 1460>  
56: 17:05:59.556627 198.51.100.2.56280 > 203.0.113.2.443: . ack 2583094767 win 64240  
57: 17:05:59.560502 198.51.100.2.56280 > 203.0.113.2.443: P 1903869754:1903869906(152) ack  
2583094767 win 64240  
58: 17:05:59.560578 203.0.113.2.443 > 198.51.100.2.56280: . ack 1903869906 win 32768  
59: 17:05:59.563996 203.0.113.2.443 > 198.51.100.2.56280: P 2583094767:2583096227(1460)  
ack 1903869906 win 32768  
60: 17:05:59.780034 198.51.100.2.56280 > 203.0.113.2.443: . ack 2583096227 win 64240  
61: 17:05:59.780141 203.0.113.2.443 > 198.51.100.2.56280: P 2583096227:2583097673(1446)  
ack 1903869906 win 32768

```

62: 17:05:59.998376      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583097673 win 62794
63: 17:06:14.809253      198.51.100.2.56280 > 203.0.113.2.443: P 1903869906:1903870032(126) ack
2583097673 win 62794
64: 17:06:14.809970      203.0.113.2.443 > 198.51.100.2.56280: P 2583097673:2583097724(51) ack
1903870032 win 32768
65: 17:06:14.815768      198.51.100.2.56280 > 203.0.113.2.443: P 1903870032:1903870968(936) ack
2583097724 win 64240
66: 17:06:14.815860      203.0.113.2.443 > 198.51.100.2.56280: . ack 1903870968 win 32768
67: 17:06:14.816913      203.0.113.2.443 > 198.51.100.2.56280: P 2583097724:2583099184(1460)
ack 1903870968 win 32768
68: 17:06:14.816928      203.0.113.2.443 > 198.51.100.2.56280: P 2583099184:2583099306(122) ack
1903870968 win 32768
69: 17:06:14.816959      203.0.113.2.443 > 198.51.100.2.56280: P 2583099306:2583100766(1460)
ack 1903870968 win 32768
70: 17:06:14.816974      203.0.113.2.443 > 198.51.100.2.56280: P 2583100766:2583100888(122) ack
1903870968 win 32768
71: 17:06:14.816989      203.0.113.2.443 > 198.51.100.2.56280: P 2583100888:2583102142(1254)
ack 1903870968 win 32768
72: 17:06:14.817554      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583102142 win 64240
73: 17:06:14.817615      203.0.113.2.443 > 198.51.100.2.56280: P 2583102142:2583103602(1460)
ack 1903870968 win 32768
74: 17:06:14.817630      203.0.113.2.443 > 198.51.100.2.56280: P 2583103602:2583103930(328) ack
1903870968 win 32768
75: 17:06:14.817630      203.0.113.2.443 > 198.51.100.2.56280: P 2583103930:2583104052(122) ack
1903870968 win 32768
76: 17:06:14.817645      203.0.113.2.443 > 198.51.100.2.56280: P 2583104052:2583105512(1460)
ack 1903870968 win 32768
77: 17:06:14.817645      203.0.113.2.443 > 198.51.100.2.56280: P 2583105512:2583105634(122) ack
1903870968 win 32768
78: 17:06:14.817660      203.0.113.2.443 > 198.51.100.2.56280: P 2583105634:2583105738(104) ack
1903870968 win 32768
79: 17:06:14.818088      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583105512 win 64240
80: 17:06:14.818530      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583105738 win 64014
81: 17:06:18.215122      198.51.100.2.58944 > 203.0.113.2.443: udp 99
82: 17:06:18.215610      203.0.113.2.443 > 198.51.100.2.58944: udp 48
83: 17:06:18.215671      198.51.100.2.56280 > 203.0.113.2.443: P 1903870968:1903872025(1057)
ack 2583105738 win 64014
84: 17:06:18.215763      203.0.113.2.443 > 198.51.100.2.56280: . ack 1903872025 win 32768
85: 17:06:18.247011      198.51.100.2.58944 > 203.0.113.2.443: udp 119
86: 17:06:18.247728      203.0.113.2.443 > 198.51.100.2.58944: udp 188
87: 17:06:18.249285      198.51.100.2.58944 > 203.0.113.2.443: udp 93
88: 17:06:18.272309      198.51.100.2.58944 > 203.0.113.2.443: udp 93
89: 17:06:18.277680      198.51.100.2.58944 > 203.0.113.2.443: udp 93
90: 17:06:18.334501      198.51.100.2.58944 > 203.0.113.2.443: udp 221
91: 17:06:18.381541      198.51.100.2.58944 > 203.0.113.2.443: udp 109
92: 17:06:18.443565      198.51.100.2.58944 > 203.0.113.2.443: udp 109
93: 17:06:18.786702      198.51.100.2.58944 > 203.0.113.2.443: udp 157
94: 17:06:18.786870      198.51.100.2.58944 > 203.0.113.2.443: udp 157
95: 17:06:18.786931      198.51.100.2.58944 > 203.0.113.2.443: udp 157
96: 17:06:18.952755      198.51.100.2.58944 > 203.0.113.2.443: udp 109
97: 17:06:18.968272      198.51.100.2.58944 > 203.0.113.2.443: udp 109
98: 17:06:18.973902      198.51.100.2.58944 > 203.0.113.2.443: udp 109
99: 17:06:18.973994      198.51.100.2.58944 > 203.0.113.2.443: udp 109
100: 17:06:18.989267      198.51.100.2.58944 > 203.0.113.2.443: udp 109

```

## 查看从防火墙内的最终用户传入的数据包的详细信息

```

ciscofp3# show cap capin packet-number 1 trace detail
2943 packets captured

```

```

1: 17:05:56.580994 006b.f1e7.6c5e 000c.294f.ac84 0x0800 Length: 66

```

198.51.100.2.55928 > 203.0.113.2.443: S [tcp sum ok] 2933933902:2933933902(0) win 8192 <mss 1460,nop,wscale 8,nop,nop,sackOK> (DF) (ttl 127, id 31008)

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace13beec90, priority=13, domain=capture, deny=false

hits=2737, user\_data=0x2ace1232af40, cs\_id=0x0, l3\_type=0x0

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0000.0000.0000

input\_ifc=outside, output\_ifc=any

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace107c8480, priority=1, domain=permit, deny=false

hits=183698, user\_data=0x0, cs\_id=0x0, l3\_type=0x8

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0100.0000.0000

input\_ifc=outside, output\_ifc=any

Phase: 3

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 203.0.113.2 using egress ifc identity

Phase: 4

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace1199f680, priority=119, domain=permit, deny=false

hits=68, user\_data=0x0, cs\_id=0x0, flags=0x0, protocol=6

src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0

input\_ifc=outside, output\_ifc=identity

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace1199efd0, priority=8, domain=conn-set, deny=false

hits=68, user\_data=0x2ace1199e5d0, cs\_id=0x0, reverse, flags=0x0, protocol=6

src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0

input\_ifc=outside, output\_ifc=identity

Phase: 6  
Type: NAT  
Subtype: per-session  
Result: ALLOW  
Config:  
Additional Information:  
Forward Flow based lookup yields rule:  
in id=0x2ace0fa81330, priority=0, domain=nat-per-session, deny=false  
hits=178978, user\_data=0x0, cs\_id=0x0, reverse, use\_real\_addr, flags=0x0, protocol=6  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=any, output\_ifc=any

Phase: 7  
Type: IP-OPTIONS  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Forward Flow based lookup yields rule:  
in id=0x2ace107cdb00, priority=0, domain=inspect-ip-options, deny=true  
hits=174376, user\_data=0x0, cs\_id=0x0, reverse, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=any

Phase: 8  
Type: CLUSTER-REDIRECT  
Subtype: cluster-redirect  
Result: ALLOW  
Config:  
Additional Information:  
Forward Flow based lookup yields rule:  
in id=0x2ace107c90c0, priority=208, domain=cluster-redirect, deny=false  
hits=78, user\_data=0x0, cs\_id=0x0, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=identity

Phase: 9  
Type: TCP-MODULE  
Subtype: webvpn  
Result: ALLOW  
Config:  
Additional Information:  
Forward Flow based lookup yields rule:  
in id=0x2ace1199df20, priority=13, domain=soft-np-tcp-module, deny=false  
hits=58, user\_data=0x2ace061efb00, cs\_id=0x0, reverse, flags=0x0, protocol=6  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=identity

Phase: 10  
Type: VPN  
Subtype: ipsec-tunnel-flow  
Result: ALLOW  
Config:  
Additional Information:  
Forward Flow based lookup yields rule:  
in id=0x2ace11d455e0, priority=13, domain=ipsec-tunnel-flow, deny=true  
hits=87214, user\_data=0x0, cs\_id=0x0, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0

input\_ifc=outside, output\_ifc=any

Phase: 11

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace11da7000, priority=13, domain=capture, deny=false  
hits=635, user\_data=0x2ace1232af40, cs\_id=0x2ace11f21620, reverse, flags=0x0, protocol=0  
src ip/id=198.51.100.2, mask=255.255.255.255, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=any

Phase: 12

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

out id=0x2ace10691780, priority=13, domain=capture, deny=false  
hits=9, user\_data=0x2ace1232af40, cs\_id=0x2ace11f21620, reverse, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=198.51.100.2, mask=255.255.255.255, port=0, tag=any, dscp=0x0  
input\_ifc=any, output\_ifc=outside

Phase: 13

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 87237, packet dispatched to next module

Module information for forward flow ...

snp\_fp\_inspect\_ip\_options  
snp\_fp\_tcp\_normalizer  
snp\_fp\_tcp\_mod  
snp\_fp\_adjacency  
snp\_fp\_fragment  
snp\_fp\_drop

Module information for reverse flow ...

snp\_fp\_inspect\_ip\_options  
snp\_fp\_tcp\_normalizer  
snp\_fp\_adjacency  
snp\_fp\_fragment  
snp\_ifc\_stat

Result:

input-interface: outside  
input-status: up  
input-line-status: up  
output-interface: NP Identity Ifc  
Action: allow

1 packet shown

ciscofp3#

将捕获复制到disk0:FTD的。然后，您可以通过SCP、FTP或TFTP下载

( 或者从FirePOWER管理中心Web UI >> System >> Health >> Health Monitor >>单击Advanced Troubleshooting >>单击Download File选项卡 )



```
ciscofp3# copy /pcap capture:capin disk0:/capin.pcap
```

```
Source capture name [capin]? <hit Enter>
```

```
Destination filename [capin.pcap]? <hit Enter>
```

```
!!!!!!!!!!!!!!!!!!!!
```

```
207 packets copied in 0.0 secs
```

```
ciscofp3# dir
```

```
Directory of disk0:/
```

```
122 -rwx 198 05:13:44 Apr 01 2018 lina_phase1.log
```

```
49 drwx 4096 21:42:20 Jun 30 2018 log
```

```
53 drwx 4096 21:42:36 Jun 30 2018 coredumpinfo
```

```
110 drwx 4096 14:59:51 Oct 10 2018 csm
```

```
123 -rwx 21074 01:26:44 Oct 10 2018 backup-config.cfg
```

```
124 -rwx 21074 01:26:44 Oct 10 2018 startup-config
```

```
125 -rwx 20354 01:26:44 Oct 10 2018 modified-config.cfg
```

```
160 -rwx 60124 17:06:22 Oct 10 2018 capin.pcap
```

```
ciscofp3# copy disk0:/capin.pcap tftp:/
```

```
Source filename [capin.pcap]? <hit Enter>
```

```
Address or name of remote host []? 192.168.1.25 (your TFTP server IP address (your PC if using  
tftpd32 or Solarwinds TFTP Server))
```

```
Destination filename [capin.pcap]? <hit Enter>
```

```
113645 bytes copied in 21.800 secs (5411 bytes/sec)
```

```
ciscofp3#
```

(or from FirePOWER Management Center Web GUI >> System >> Health >> Health Monitor >> click  
Advanced Troubleshooting >> click Download File tab)

**验证NAT规则配置是否正确：**

```
ciscofp3# packet-tracer input outside tcp 192.168.10.50 1234 192.168.1.30 443 detailed
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x2ace0fa90e70, priority=13, domain=capture, deny=false
```

```
hits=11145169, user_data=0x2ace120c4910, cs_id=0x0, l3_type=0x0
```

```
src mac=0000.0000.0000, mask=0000.0000.0000
```

```
dst mac=0000.0000.0000, mask=0000.0000.0000
```

```
input_ifc=outside, output_ifc=any
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x2ace107c8480, priority=1, domain=permit, deny=false
```

```
hits=6866095, user_data=0x0, cs_id=0x0, l3_type=0x8
```

```
src mac=0000.0000.0000, mask=0000.0000.0000
```

```
dst mac=0000.0000.0000, mask=0100.0000.0000
```

```
input_ifc=outside, output_ifc=any
```

```
Phase: 3
```

```
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

Result: ALLOW  
Config:  
Additional Information:  
found next-hop **192.168.1.30** using egress ifc inside

Phase: 4  
Type: UN-NAT  
Subtype: static  
Result: ALLOW  
Config:

**nat (inside,outside) source static inside-subnet inside-subnet destination static outside-subnet-anyconnect-pool outside-subnet-anyconnect-pool no-proxy-arp route-lookup**

Additional Information:  
NAT divert to egress interface inside  
Untranslate 192.168.1.30/443 to 192.168.1.30/443

Phase: 5  
Type: ACCESS-LIST  
Subtype: log  
Result: ALLOW  
Config:

access-group CSM\_FW\_ACL\_ global  
access-list CSM\_FW\_ACL\_ advanced trust ip ifc outside any any rule-id 268436481 event-log flow-end  
access-list CSM\_FW\_ACL\_ remark rule-id 268436481: PREFILTER POLICY:  
Example\_Company\_Prefilter\_Policy  
access-list CSM\_FW\_ACL\_ remark rule-id 268436481: RULE: AllowtoVPNOutsideinterface

Additional Information:  
Forward Flow based lookup yields rule:  
in id=0x2ace0fa8f4e0, priority=12, domain=permit, trust  
hits=318637, user\_data=0x2ace057b9a80, cs\_id=0x0, use\_real\_addr, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=outside  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0  
input\_ifc=any, output\_ifc=any

...

Phase: 7  
Type: NAT  
Subtype:  
Result: ALLOW  
Config:

**nat (inside,outside) source static inside-subnet inside-subnet destination static outside-subnet-anyconnect-pool outside-subnet-anyconnect-pool no-proxy-arp route-lookup**

Additional Information:  
Static translate 192.168.10.50/1234 to 192.168.10.50/1234  
Forward Flow based lookup yields rule:  
in id=0x2ace11975cb0, priority=6, domain=nat, deny=false  
hits=120, user\_data=0x2ace0f29c4a0, cs\_id=0x0, flags=0x0, protocol=0  
src ip/id=192.168.10.0, mask=255.255.255.0, port=0, tag=any  
dst ip/id=10.201.214.128, mask=255.255.255.240, port=0, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=inside

...

Phase: 10 Type: VPN Subtype: ipsec-tunnel-flow Result: ALLOW Config: Additional Information:  
Forward Flow based lookup yields rule: in id=0x2ace11d455e0, priority=13, domain=ipsec-tunnel-flow, deny=true hits=3276174, user\_data=0x0, cs\_id=0x0, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=any Phase: 11 Type: NAT Subtype: rpf-check Result: ALLOW Config:  
**nat (inside,outside) source static inside-subnet inside-subnet destination static outside-subnet-anyconnect-pool outside-subnet-anyconnect-pool no-proxy-arp route-lookup**

Additional Information:  
Forward Flow based lookup yields rule:  
out id=0x2ace0d5a9800, priority=6, domain=nat-reverse, deny=false

```
hits=121, user_data=0x2ace1232a4c0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.10.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.201.214.128, mask=255.255.255.240, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=inside
```

...

```
Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3279248, packet dispatched to next module
```

Module information for reverse flow ...

...

```
Phase: 15
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.30 using egress ifc inside
```

```
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

ciscofp3#

## 通过AnyConnect VPN成功连接到FTD的PC的员工PC上捕获的数据

anyconnectinitiation.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr ==

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
129	3.685253		56501		443	TCP	66	56501 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
130	3.685868		443		56501	TCP	60	443 → 56501 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
131	3.685917		56501		443	TCP	54	56501 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
132	3.687035		56501		443	TLSv1.2	187	Client Hello
133	3.687442		443		56501	TCP	60	443 → 56501 [ACK] Seq=1 Ack=134 Win=32768 Len=0
134	3.687806		443		56501	TLSv1.2	1514	Server Hello
142	3.899719		56501		443	TCP	54	56501 → 443 [ACK] Seq=134 Ack=1461 Win=64240 Len=0
143	3.900303		443		56501	TLSv1.2	1159	Certificate, Server Hello Done
144	3.901003		56501		443	TLSv1.2	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
145	3.904245		443		56501	TLSv1.2	145	Change Cipher Spec, Encrypted Handshake Message
146	3.907281		56501		443	TLSv1.2	363	Application Data
147	3.907374		56501		443	TLSv1.2	875	Application Data
148	3.907797		443		56501	TCP	60	443 → 56501 [ACK] Seq=2657 Ack=801 Win=32768 Len=0
149	3.907868		443		56501	TCP	60	443 → 56501 [ACK] Seq=2657 Ack=1622 Win=32768 Len=0
150	3.909600		443		56501	TLSv1.2	363	Application Data
151	3.909759		443		56501	TLSv1.2	811	Application Data

Transmission Control Protocol, Src Port: 56501, Dst Port: 443, Seq: 0, Len: 0  
Source Port: 56501  
Destination Port: 443

您还可以看到DTLS隧道在此捕获的后面形成

capin.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
76	12:06:14.817645		443		56280	TCP	1514	443 → 56280 [PSH, ACK] Seq=9286 Ack=1215 Win=32768 Len=1460 [TCP segment of a reassembled PDU]
77	12:06:14.817645		443		56280	TLsv1.2	176	Application Data
78	12:06:14.817660		443		56280	TLsv1.2	158	Application Data
79	12:06:14.818088		56280		443	TCP	54	56280 → 443 [ACK] Seq=1215 Ack=10746 Win=64240 Len=0
80	12:06:14.818530		56280		443	TCP	54	56280 → 443 [ACK] Seq=1215 Ack=10972 Win=64014 Len=0
81	12:06:18.215122		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	141	Client Hello
82	12:06:18.215619		443		58944	DTLS 1.0 (OpenSSL pre 0.9.8f)	90	Hello Verify Request
83	12:06:18.215671		56280		443	TLsv1.2	1111	Application Data
84	12:06:18.215763		443		56280	TCP	54	443 → 56280 [ACK] Seq=10972 Ack=2272 Win=32768 Len=0
85	12:06:18.247011		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	161	Client Hello
86	12:06:18.247728		443		58944	DTLS 1.0 (OpenSSL pre 0.9.8f)	230	Server Hello, Change Cipher Spec, Encrypted Handshake Message
87	12:06:18.249285		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Change Cipher Spec, Encrypted Handshake Message
88	12:06:18.272309		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
89	12:06:18.277680		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
90	12:06:18.334501		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	263	Application Data

> Frame 81: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits)

> Ethernet II, Src: Cisco\_e7:6c:5e (00:6b:f1:e7:6c:5e), Dst: Vmware\_4f:ac:84 (00:0c:29:4f:ac:84)

> Internet Protocol Version 4, Src: , Dst:

> User Datagram Protocol, Src Port: 58944, Dst Port: 443

> Datagram Transport Layer Security

- DTLS 1.0 (OpenSSL pre 0.9.8f) Record Layer: Handshake Protocol: Client Hello
  - Content Type: Handshake (22)
  - Version: DTLS 1.0 (OpenSSL pre 0.9.8f) (0x0100)
  - Epoch: 0
  - Sequence Number: 0
  - Length: 86
  - Handshake Protocol: Client Hello
    - Handshake Type: Client Hello (1)
    - Length: 74
    - Message Sequence: 0
    - Fragment Offset: 0
    - Fragment Length: 74

在FTD的外部接口上捕获，显示AnyConnect PC已成功连接到VPN

capin.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
1	12:05:56.580994		55928		443	TCP	66	55928 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	12:05:56.581375		443		55928	TCP	58	443 → 55928 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
3	12:05:56.581757		55928		443	TCP	54	55928 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	12:05:56.582382		55928		443	TLsv1.2	187	Client Hello
5	12:05:56.582458		443		55928	TCP	54	443 → 55928 [ACK] Seq=1 Ack=134 Win=32768 Len=0
6	12:05:56.582733		443		55928	TLsv1.2	1514	Server Hello
7	12:05:56.790211		55928		443	TCP	54	55928 → 443 [ACK] Seq=134 Ack=1461 Win=64240 Len=0
8	12:05:56.790349		443		55928	TLsv1.2	1159	Certificate, Server Hello Done
9	12:05:56.791691		55928		443	TLsv1.2	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	12:05:56.794911		443		55928	TLsv1.2	145	Change Cipher Spec, Encrypted Handshake Message
11	12:05:56.797077		55928		443	TLsv1.2	363	Application Data
12	12:05:56.797169		443		55928	TCP	54	443 → 55928 [ACK] Seq=2657 Ack=801 Win=32768 Len=0
13	12:05:56.797199		55928		443	TLsv1.2	875	Application Data
14	12:05:56.797276		443		55928	TCP	54	443 → 55928 [ACK] Seq=2657 Ack=1622 Win=32768 Len=0
15	12:05:56.798634		443		55928	TLsv1.2	363	Application Data
16	12:05:56.798786		443		55928	TLsv1.2	811	Application Data

> Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

> Ethernet II, Src: Vmware\_4f:ac:84 (00:0c:29:4f:ac:84), Dst: Cisco\_e7:6c:5e (00:6b:f1:e7:6c:5e)

> Internet Protocol Version 4, Src: , Dst:

> Transmission Control Protocol, Src Port: 443, Dst Port: 55928, Seq: 1, Ack: 134, Len: 1460

Source Port: 443

Destination Port: 55928

[Stream index: 0]

[TCP Segment Len: 1460]

Sequence number: 1 (relative sequence number)

[Next sequence number: 1461 (relative sequence number)]

Acknowledgment number: 134 (relative ack number)

0101 .... = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window size value: 32768

[Calculated window size: 32768]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x3693 [unverified]

```

00c0 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 51 31 15  .*.H....001.
00d0 30 13 06 0a 09 92 26 89 93 f2 2c 64 01 19 16 05  0.....&...d...
00e0 6c 6f 63 61 6c 31 19 30 17 06 0a 09 92 26 89 93  local1-0....&..
00f0 f2 2c 64 01 19 16 09 63 6f 68 61 64 6c 65 79 33  .,d....c....
0100 31 1d 30 1b 06 03 55 04 03 13 14 63 6f 68 61 64  1-0...U....
0110 6c 65 79 33 2d 43 4f 52 42 44 43 33 2d 43 41 30  .c.65.79.33.2d.43.4f.52.42.44.43.33.2d.43.41.30.
0120 1e 17 0d 31 38 31 30 31 30 30 32 34 35 30 30 5a  .1e.17.0d.31.38.31.30.31.30.30.32.34.35.30.30.5a.
0130 17 0d 32 30 31 30 30 39 30 32 34 35 30 30 5a 30  .17.0d.32.30.31.30.30.39.30.32.34.35.30.30.5a.30.
0140 61 b3 31 26 30 24 06 09 2a 86 48 86 f7 0d 01 09  .1&05...*.H....
0150 02 13 17 63 6f 72 62 66 70 33 2e 63 6f 68 61 64  .02.13.17.63.6f.72.62.66.70.33.2e.63.6f.68.61.64.
0160 6c 65 79 33 2e 6c 6f 63 61 6c 31 0b 30 09 06 03  .c.65.79.33.2e.6c.6f.63.61.6c.31.0b.30.09.06.03.
0170 55 04 06 13 02 55 53 31 0b 30 09 06 03 55 04 08  U...US1-0...U...
0180 13 02 43 41 31 11 30 0f 06 03 55 04 07 13 08 53  .-CA1-0...U...S
0190 61 6e 20 4a 6f 73 65 31 0e 30 0c 06 03 55 04 0a  an Jose1-0...U...
01a0 13 05 43 69 73 63 6f 31 0c 30 0a 06 03 55 04 0b  .-Ciscot-0...U...
01b0 13 03 54 41 43 31 20 30 1e 06 03 55 04 03 13 17  .-TAC1 0...U...
01c0 63 6f 72 62 66 70 33 2e 63 6f 68 61 64 6c 65 79  .f.p3.
01d0 33 2e 6c 6f 63 61 6c 31 1c 30 1a 06 09 2a 86 48  3.local1-0...*.H
01e0 86 f7 0d 01 09 01 16 0d 74 61 63 40 63 69 73 63  .0.....tac@cis
01f0 6f 2e 63 6f 6d 30 82 01 22 30 0d 06 09 2a 86 48  o.com0...0...*.H
0200 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01  .0.....0...

```

capin.pcap

注意：当我们通过VPN连接到FTD的外部接口时，您可以在“服务器问候”数据包中看到FTD VPN服

务器证书。员工PC将信任此证书，因为员工PC上有根CA证书，并且FTD VPN服务器证书由同一根CA签名。

捕获FTD的FTD，询问RADIUS服务器用户名和密码是否正确(Cisco ISE)

The image shows a Wireshark capture of RADIUS traffic. The packet list pane shows several RADIUS messages, with packet 2 (Access-Accept) selected. The packet details pane shows the RADIUS protocol structure, and the packet bytes pane shows the raw data. A blue arrow points to the 'jsmith' username in the raw data.

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
1	13:05:36.771841		3238		1812	RADIUS	701	Access-Request id=93
2	13:05:42.865342		1812		3238	RADIUS	201	Access-Accept id=93
3	13:05:42.865937		3238		1812	RADIUS	701	Access-Request id=94
4	13:05:42.911314		1812		3238	RADIUS	62	Access-Reject id=94
5	13:05:43.302825		19500		1813	RADIUS	756	Accounting-Request id=95
6	13:05:43.309294		1813		19500	RADIUS	62	Accounting-Response id=95

```

> Frame 2: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)
> Ethernet II, Src: Cisco_e7:6c:5e (00:0b:f1:e7:6c:5e), Dst: Vmware_4f:ac:84 (00:0c:29:4f:ac:84)
> Internet Protocol Version 4, Src: ..., Dst: ...
> User Datagram Protocol, Src Port: 1812, Dst Port: 3238
  RADIUS Protocol
    Code: Access-Accept (2)
0000  00 0c 29 4f ac 84 00 6b f1 e7 6c 5e 08 00 45 00  ..)O...k..1^..E.
0010  00 bb 5f 66 40 00 3f 11 18 bc 0a c9 d6 e6 0a c9  .._f@:?. .....
0020  d6 97 07 14 0c a6 00 a7 4e 17 02 5d 00 9f 7f b9  ....N..]....
0030  c7 a6 65 6d e7 75 c7 64 7f 0f d5 54 d7 59 01 08  ..em ud ...T.Y..
0040  6a 73 6d 69 74 68 18 28 52 65 61 75 74 68 53 65  jsmith( ReauthSe ←
0050  73 73 69 6f 6e 3a 30 61 63 39 64 36 38 61 30 30  ssion:0a c9d68a00
0060  30 31 61 30 30 30 35 62 62 66 39 30 66 30 19 3b  01a0005b bf90f0.;
0070  43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30  CACS:0ac 9d68a000
0080  31 61 30 30 30 35 62 62 66 39 30 66 30 3a 63 6f  1a0005bb f90f0:co
0090  72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38  rbinise/ 32234408
00a0  34 2f 31 39 37 34 32 39 39 1a 20 00 00 09 01 4/197429 9. ....
00b0  1a 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 6f  :profile -name=Wo
00c0  72 6b 73 74 61 74 69 6f 6e rkstatio n
  
```

如上所示，我们的VPN连接获得Access-Accept，而我们的AnyConnect VPN客户端通过VPN成功连接到FTD

FTD的捕获(CLI)，询问思科ISE用户名和密码是否有效 (即确保RADIUS请求在FTD和ISE之间成功传输并验证它们离开哪个接口)

```

ciscofp3# capture capout interface inside trace detail trace-count 100 [Capturing - 35607 bytes]
ciscofp3# show cap
ciscofp3# show cap capout | i 192.168.1.10
37: 01:23:52.264512 192.168.1.1.3238 > 192.168.1.10.1812: udp 659
38: 01:23:52.310210 192.168.1.10.1812 > 192.168.1.1.3238: udp 159
39: 01:23:52.311064 192.168.1.1.3238 > 192.168.1.10.1812: udp 659
40: 01:23:52.326734 192.168.1.10.1812 > 192.168.1.1.3238: udp 20
82: 01:23:52.737663 192.168.1.1.19500 > 192.168.1.10.1813: udp 714
85: 01:23:52.744483 192.168.1.10.1813 > 192.168.1.1.19500: udp 20
  
```

在Cisco ISE RADIUS服务器下方显示身份验证成功。单击放大镜查看身份验证成功的详细信息

Time	Status	Username	IP	Interface	Group	Access
Oct 11, 2018 06:10:08.808 PM	●	jsmith	00:0C:29:37:EF:BF	Workstation	VPN Users >> Default	VPN Users >> Allow FTD VPN connections if AD Group VPNUsers
Oct 11, 2018 06:10:08.808 PM	■	jsmith	00:0C:29:37:EF:BF	FTDVPN	Workstation	VPN Users >> Default



## Overview

Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	00:0C:29:37:EF:BF ⓘ
Endpoint Profile	Workstation
Authentication Policy	VPN Users >> Default
Authorization Policy	VPN Users >> Allow FTD VPN connections if AD Group VPNusers
Authorization Result	PermitAccess

在员工PC的员工PC的AnyConnect适配器上捕获，通过HTTPS（即，在成功VPN登录时）访问内部网站：

\*Local Area Connection 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
49	1.545946	192.168.10.50	192.168.10.50	TCP	66	63576 → 443 [SYN] Seq=0 Win=8192
50	1.547622	192.168.10.50	192.168.10.50	TCP	66	443 → 63576 [SYN, ACK] Seq=0 Ack=
51	1.547675	192.168.10.50	192.168.10.50	TCP	54	63576 → 443 [ACK] Seq=1 Ack=1 Win
52	1.549052	192.168.10.50	192.168.10.50	TLSv1.2	240	Client Hello
53	1.550413	192.168.10.50	192.168.10.50	TLSv1.2	900	Server Hello, Certificate, Server
54	1.550909	192.168.10.50	192.168.10.50	TLSv1.2	372	Client Key Exchange, Change Ciper
58	1.562066	192.168.10.50	192.168.10.50	TLSv1.2	105	Change Cipher Spec, Encrypted Har
59	1.562718	192.168.10.50	192.168.10.50	TLSv1.2	469	Application Data
60	1.595405	192.168.10.50	192.168.10.50	TLSv1.2	1007	Application Data
61	1.628938	192.168.10.50	192.168.10.50	TLSv1.2	437	Application Data
64	1.666995	192.168.10.50	192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=1851 Ack=13
65	1.667232	192.168.10.50	192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=3217 Ack=13
66	1.667284	192.168.10.50	192.168.10.50	TCP	54	63576 → 443 [ACK] Seq=1303 Ack=45
67	1.667423	192.168.10.50	192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=4583 Ack=13

Frame 49: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: Cisco\_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Cimsys\_33:44:55 (00:11:22:33:44:55)

Internet Protocol Version 4, Src: 192.168.10.50, Dst: 192.168.10.50

Transmission Control Protocol, Src Port: 63576, Dst Port: 443, Seq: 0, Len: 0

Source Port: 63576

Destination Port: 443

```

0000  00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00  .."3DU...<Z...E.
0010  00 34 25 44 40 00 80 06 29 59 c0 a8 0a 32 0a c9  -4%D@... )Y...2..
0020  d6 83 f8 58 01 bb 21 bb a9 32 00 00 00 80 02  ...X...!..2.....
0030  20 00 de 45 00 00 02 04 05 56 01 03 03 08 01 01  ..E....~V...|...
0040  04 02
    
```

Transmission Control Protocol (tcp), 32 bytes | Packets: 260 · Displayed: 125 (48.1%) · Dropped: 0 (0.0%) | Profile: Default

## 调试

debug radius all

debug webvpn anyconnect 255

在FTD诊断CLI上运行“debug radius all”命令(>system support diagnostic-cli) , 在Cisco Anyconnect客户端的Windows/Mac PC上点击“Connect”

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
ciscofp3> enable
Password: <hit enter>
ciscofp3# terminal monitor
ciscofp3# debug radius all
<hit Connect on Anyconnect client on PC>

radius mkreq: 0x15
alloc_rip 0x00002ace10875428
new request 0x15 --> 16 (0x00002ace10875428)
got user 'jsmith'
got password
add_req 0x00002ace10875428 session 0x15 id 16
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=198.51.100.2

RADIUS packet decode (authentication request)

-----
Raw packet data (length = 659).....
01 10 02 93 fb 19 19 df f6 b1 c7 3e 34 fc 88 ce | .....>4...
75 38 2d 55 01 08 6a 73 6d 69 74 68 02 12 a0 83 | u8-U..jsmith....
c9 bd ad 72 07 d1 bc 24 34 9e 63 a1 f5 93 05 06 | ...r...$4.c.....
00 00 50 00 1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...198.51.100.2
2e 31 35 31 1f 10 31 30 2e 32 30 31 2e 32 31 34 | .151..198.51.100.2
2e 32 35 31 3d 06 00 00 05 42 10 31 30 2e 32 | .4=.....B.198.
30 31 2e 32 31 34 2e 32 35 31 1a 23 00 00 09 | 51.100.2#....
01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device
2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win,..
00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....&mdm-tlv=dev
69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29
2d 33 37 2d 65 66 2d 62 66 1a 33 00 00 09 01 | -37-ef-bf.3.....
2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | -mdm-tlv=device-
70 75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf...
00 09 01 34 6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u
73 65 72 2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon
6e 65 63 74 20 57 69 6e 64 6f 77 73 20 34 2e 36 | nect Windows 4.6
2e 30 33 30 34 39 1a 3f 00 00 09 01 39 6d 64 | .03049.?......9md
6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 6c 61 | m-tlv=device-pla
74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6.
31 2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P
61 63 6b 20 31 1a 40 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 79 70 65 | -tlv=device-type
3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e 20 56 4d | =VMware, Inc. VM
77 61 72 65 20 56 69 72 74 75 61 6c 20 50 6c 61 | ware Virtual Pla
74 66 6f 72 6d 1a 5b 00 00 09 01 55 6d 64 6d | tform.[.....Umdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 69 64 3d | -tlv=device-uid=
33 36 39 33 43 36 34 30 37 43 39 32 35 32 35 31 | 3693C6407C925251
46 46 37 32 42 36 34 39 33 42 44 44 38 37 33 31 | FF72B6493BDD8731
38 41 42 46 43 39 30 43 36 32 31 35 34 32 43 33 | 8ABFC90C621542C3
38 46 41 46 38 37 38 45 46 34 39 36 31 34 41 31 | 8FAF878EF49614A1
04 06 00 00 00 00 1a 31 00 00 09 01 2b 61 75 | .....1.....+au
64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 3d 30 | dit-session-id=0
61 63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 | ac9d68a000050005
62 62 65 31 66 39 31 1a 23 00 00 09 01 1d 69 | bbe1f91.#.....i
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1
```



```
30 31 2e 32 31 34 2e 32 35 31 1a 18 00 00 0c 04 | 68.10.50.....
92 12 46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 | ..FTDAnyConnectV
50 4e 1a 0c 00 00 0c 04 96 06 00 00 00 02 1a 15 | PN.....
00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d 74 | .....coa-push=t
72 75 65 | rue
```

Parsed packet data.....

```
Radius: Code = 1 (0x01)
Radius: Identifier = 16 (0x10)
Radius: Length = 659 (0x0293)
Radius: Vector: FB1919DFF6B1C73E34FC88CE75382D55
Radius: Type = 1 (0x01) User-Name
Radius: Length = 8 (0x08)
Radius: Value (String) =
6a 73 6d 69 74 68 | jsmith
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
a0 83 c9 bd ad 72 07 d1 bc 24 34 9e 63 a1 f5 93 | .....r...$4.c...
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5000
Radius: Type = 30 (0x1E) Called-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2
Radius: Type = 31 (0x1F) Calling-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 44 (0x2C)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 38 (0x26)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m
61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e
66 2d 62 66 | f-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 51 (0x33)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 45 (0x2D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf
Radius: Type = 26 (0x1A) Vendor-Specific
```

Radius: Length = 58 (0x3A)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 52 (0x34)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-  
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect  
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030  
34 39 | 49  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 63 (0x3F)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 57 (0x39)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=  
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service  
20 50 61 63 6b 20 31 | Pack 1  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 64 (0x40)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 58 (0x3A)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t  
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.  
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual  
50 6c 61 74 66 6f 72 6d | Platform  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 91 (0x5B)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 85 (0x55)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u  
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925  
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8  
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154  
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961  
34 41 31 | 4A1  
Radius: Type = 4 (0x04) NAS-IP-Address  
Radius: Length = 6 (0x06)  
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 49 (0x31)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 43 (0x2B)  
Radius: Value (String) =  
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id  
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500  
30 35 62 62 65 31 66 39 31 | 05bbe1f91  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 35 (0x23)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 29 (0x1D)  
Radius: Value (String) =  
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192.  
32 30 31 2e 32 31 34 2e 32 35 31 | 168.10.50  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 24 (0x18)  
Radius: Vendor ID = 3076 (0x00000C04)

```
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true
send pkt 192.168.1.10/1812
rip 0x00002ace10875428 state 7 id 16
rad_vrfy() : response message verified
rip 0x00002ace10875428
: chall_state ''
: state 0x7
: reqauth:
fb 19 19 df f6 b1 c7 3e 34 fc 88 ce 75 38 2d 55
: info 0x00002ace10875568
session_id 0x15
request_id 0x10
user 'jsmith'
response '****'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 1
```

RADIUS packet decode (response)

```
-----
Raw packet data (length = 159).....
02 10 00 9f 39 45 43 cf 05 be df 2f 24 d5 d7 05 | ....9EC..../$...
47 67 b4 fd 01 08 6a 73 6d 69 74 68 18 28 52 65 | Gg....jsmith.(Re
61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 63 39 | authSession:0ac9
64 36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 | d68a000050005bbe
31 66 39 31 19 3b 43 41 43 53 3a 30 61 63 39 64 | 1f91.;CACS:0ac9d
36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 31 | 68a000050005bbe1
66 39 31 3a 63 6f 72 62 69 6e 69 73 65 2f 33 32 | f91:corbinise/32
32 33 34 34 30 38 34 2f 31 39 33 31 36 38 32 1a | 2344084/1931682.
20 00 00 00 09 01 1a 70 72 6f 66 69 6c 65 2d 6e | .....profile-n
61 6d 65 3d 57 6f 72 6b 73 74 61 74 69 6f 6e | ame=Workstation
```

```
Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 16 (0x10)
Radius: Length = 159 (0x009F)
Radius: Vector: 394543CF05BEDF2F24D5D7054767B4FD
Radius: Type = 1 (0x01) User-Name
Radius: Length = 8 (0x08)
Radius: Value (String) =
6a 73 6d 69 74 68 | jsmith
Radius: Type = 24 (0x18) State
Radius: Length = 40 (0x28)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 | ReauthSession:0a
```

```

63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 62 | c9d68a000050005b
62 65 31 66 39 31 | be1f91
Radius: Type = 25 (0x19) Class
Radius: Length = 59 (0x3B)
Radius: Value (String) =
43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000
30 35 30 30 30 35 62 62 65 31 66 39 31 3a 63 6f | 050005bbe1f91:co
72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408
34 2f 31 39 33 31 36 38 32 | 4/1931682
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 32 (0x20)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 26 (0x1A)
Radius: Value (String) =
70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 6f 72 | profile-name=Wor
6b 73 74 61 74 69 6f 6e | kstation
rad_procpkt: ACCEPT
Got AV-Pair with value profile-name=Workstation
RADIUS_ACCESS_ACCEPT: normal termination
radius mkreq: 0x16
alloc_rip 0x00002ace10874b80
new request 0x16 --> 17 (0x00002ace10874b80)
got user 'jsmith'
got password
add_req 0x00002ace10874b80 session 0x16 id 17
RADIUS_DELETE
remove_req 0x00002ace10875428 session 0x15 id 16
free_rip 0x00002ace10875428
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=198.51.100.2

```

RADIUS packet decode (authentication request)

```

-----
Raw packet data (length = 659).....
01 11 02 93 c6 fc 11 c1 0e c4 81 ac 09 a7 85 a8 | .....
83 c1 e4 88 01 08 6a 73 6d 69 74 68 02 12 79 41 | .....jsmith..yA
0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 05 06 | .q.8..I.<...e...
00 00 50 00 1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...203.0.113
2e 31 35 31 1f 10 31 30 2e 32 30 31 2e 32 31 34 | .2..203.0.113
2e 32 35 31 3d 06 00 00 05 42 10 31 30 2e 32 | .2=.....<ip addr
30 31 2e 32 31 34 2e 32 35 31 1a 23 00 00 00 09 | ess>.#....
01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device
2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win,..
00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ...&mdm-tlv=dev
69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29
2d 33 37 2d 65 66 2d 62 66 1a 33 00 00 00 09 01 | -37-ef-bf.3.....
2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | -mdm-tlv=device-
70 75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf....
00 09 01 34 6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u
73 65 72 2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon
6e 65 63 74 20 57 69 6e 64 6f 77 73 20 34 2e 36 | nect Windows 4.6
2e 30 33 30 34 39 1a 3f 00 00 00 09 01 39 6d 64 | .03049.?.....9md
6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 6c 61 | m-tlv=device-pla
74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6.
31 2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P
61 63 6b 20 31 1a 40 00 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 79 70 65 | -tlv=device-type
3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e 20 56 4d | =VMware, Inc. VM
77 61 72 65 20 56 69 72 74 75 61 6c 20 50 6c 61 | ware Virtual Pla
74 66 6f 72 6d 1a 5b 00 00 00 09 01 55 6d 64 6d | tform.[.....Umdm

```

```
2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 69 64 3d | -tlv=device-uid=
33 36 39 33 43 36 34 30 37 43 39 32 35 32 35 31 | 3693C6407C925251
46 46 37 32 42 36 34 39 33 42 44 44 38 37 33 31 | FF72B6493BDD8731
38 41 42 46 43 39 30 43 36 32 31 35 34 32 43 33 | 8ABFC90C621542C3
38 46 41 46 38 37 38 45 46 34 39 36 31 34 41 31 | 8FAF878EF49614A1
04 06 00 00 00 00 1a 31 00 00 00 09 01 2b 61 75 | .....1.....+au
64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 3d 30 | dit-session-id=0
61 63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 | ac9d68a000050005
62 62 65 31 66 39 31 1a 23 00 00 00 09 01 1d 69 | bbe1f91.#.....i
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1
30 31 2e 32 31 34 2e 32 35 31 1a 18 00 00 0c 04 | 68.10.50.....
92 12 46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 | ..FTDAnyConnectV
50 4e 1a 0c 00 00 0c 04 96 06 00 00 00 02 1a 15 | PN.....
00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d 74 | .....coa-push=t
72 75 65 | rue
```

Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 17 (0x11)

Radius: Length = 659 (0x0293)

Radius: Vector: C6FC11C10EC481AC09A785A883C1E488

Radius: Type = 1 (0x01) User-Name

Radius: Length = 8 (0x08)

Radius: Value (String) =

6a 73 6d 69 74 68 | jsmith

Radius: Type = 2 (0x02) User-Password

Radius: Length = 18 (0x12)

Radius: Value (String) =

79 41 0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 | yA.q.8..I.<...e.

Radius: Type = 5 (0x05) NAS-Port

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5000

Radius: Type = 30 (0x1E) Called-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2

Radius: Type = 31 (0x1F) Calling-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 61 (0x3D) NAS-Port-Type

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

Radius: Type = 66 (0x42) Tunnel-Client-Endpoint

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 35 (0x23)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 29 (0x1D)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p

6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 44 (0x2C)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 38 (0x26)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m

61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e

66 2d 62 66 | f-bf

Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 51 (0x33)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 45 (0x2D)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-  
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 58 (0x3A)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 52 (0x34)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-  
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect  
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030  
34 39 | 49  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 63 (0x3F)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 57 (0x39)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=  
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service  
20 50 61 63 6b 20 31 | Pack 1  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 64 (0x40)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 58 (0x3A)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t  
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.  
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual  
50 6c 61 74 66 6f 72 6d | Platform  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 91 (0x5B)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 85 (0x55)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u  
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925  
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8  
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154  
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961  
34 41 31 | 4A1  
Radius: Type = 4 (0x04) NAS-IP-Address  
Radius: Length = 6 (0x06)  
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 49 (0x31)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 43 (0x2B)  
Radius: Value (String) =  
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id  
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500  
30 35 62 62 65 31 66 39 31 | 05bbe1f91  
Radius: Type = 26 (0x1A) Vendor-Specific

```
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192.
32 30 31 2e 32 31 34 2e 32 35 31 | 168.10.50
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 24 (0x18)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true
send pkt 192.168.1.10/1812
rip 0x00002ace10874b80 state 7 id 17
rad_vrfy() : response message verified
rip 0x00002ace10874b80
: chall_state ''
: state 0x7
: reqauth:
c6 fc 11 c1 0e c4 81 ac 09 a7 85 a8 83 c1 e4 88
: info 0x00002ace10874cc0
session_id 0x16
request_id 0x11
user 'jsmith'
response '****'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 1
```

RADIUS packet decode (response)

```
-----
Raw packet data (length = 20).....
03 11 00 14 15 c3 44 44 7d a6 07 0d 7b 92 f2 3b | .....DD}...{...;
0b 06 ba 74 | ...t
```

Parsed packet data.....

```
Radius: Code = 3 (0x03)
Radius: Identifier = 17 (0x11)
Radius: Length = 20 (0x0014)
Radius: Vector: 15C344447DA6070D7B92F23B0B06BA74
rad_procpkt: REJECT
RADIUS_DELETE
remove_req 0x00002ace10874b80 session 0x16 id 17
free_rip 0x00002ace10874b80
radius: send queue empty
radius mkreq: 0x18
```



alloc\_rip 0x00002ace10874b80  
new request 0x18 --> 18 (0x00002ace10874b80)  
add\_req 0x00002ace10874b80 session 0x18 id 18  
ACCT\_REQUEST  
radius.c: rad\_mkpkt

RADIUS packet decode (accounting request)

-----  
Raw packet data (length = 714).....  
04 12 02 ca be a0 6e 46 71 af 5c 65 82 77 c7 b5 | .....nFq.\e.w..  
50 78 61 d7 01 08 6a 73 6d 69 74 68 05 06 00 00 | Pxa...jsmith....  
50 00 06 06 00 00 00 02 07 06 00 00 00 01 08 06 | P.....  
c0 a8 0a 32 19 3b 43 41 43 53 3a 30 61 63 39 64 | ...2.;CACS:0ac9d  
36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 31 | 68a000050005bbe1  
66 39 31 3a 63 6f 72 62 69 6e 69 73 65 2f 33 32 | f91:corbinise/32  
32 33 34 34 30 38 34 2f 31 39 33 31 36 38 32 1e | 2344084/1931682.  
10 31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 1f | .203.0.113.2.  
10 31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 28 | .198.51.100.2(  
06 00 00 00 01 29 06 00 00 00 00 2c 0a 43 31 46 | .....),.....,C1F  
30 30 30 30 35 2d 06 00 00 00 01 3d 06 00 00 00 | 00005-.....=....  
05 42 10 31 30 2e 32 30 31 2e 32 31 34 2e 32 35 | .B.203.0.113.2  
31 1a 18 00 00 0c 04 92 12 46 54 44 41 6e 79 43 | .....FTDAnyC  
6f 6e 6e 65 63 74 56 50 4e 1a 0c 00 00 0c 04 96 | onnectVPN.....  
06 00 00 00 02 1a 0c 00 00 0c 04 97 06 00 00 00 | .....  
01 1a 0c 00 00 0c 04 98 06 00 00 00 03 1a 23 00 | .....#.  
00 00 09 01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....mdm-tlv=dev  
69 63 65 2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e | ice-platform=win  
1a 2c 00 00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d | ,.....&mdm-tlv=  
64 65 76 69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 | device-mac=00-0c  
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 31 00 00 | -29-37-ef-bf.1..  
00 09 01 2b 61 75 64 69 74 2d 73 65 73 73 69 6f | ...+audit-sessio  
6e 2d 69 64 3d 30 61 63 39 64 36 38 61 30 30 30 | n-id=0ac9d68a000  
30 35 30 30 30 35 62 62 65 31 66 39 31 1a 33 00 | 050005bbelf91.3.  
00 00 09 01 2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....-mdm-tlv=dev  
69 63 65 2d 70 75 62 6c 69 63 2d 6d 61 63 3d 30 | ice-public-mac=0  
30 2d 30 63 2d 32 39 2d 33 37 2d 65 66 2d 62 66 | 0-0c-29-37-ef-bf  
1a 3a 00 00 00 09 01 34 6d 64 6d 2d 74 6c 76 3d | :.....4mdm-tlv=  
61 63 2d 75 73 65 72 2d 61 67 65 6e 74 3d 41 6e | ac-user-agent=An  
79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f 77 73 | yConnect Windows  
20 34 2e 36 2e 30 33 30 34 39 1a 3f 00 00 00 09 | 4.6.03049.?....  
01 39 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | .9mdm-tlv=device  
2d 70 6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f | -platform-versio  
6e 3d 36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 | n=6.1.7601 Servi  
63 65 20 50 61 63 6b 20 31 1a 40 00 00 00 09 01 | ce Pack 1.@.....  
3a 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | :mdm-tlv=device-  
74 79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 | type=VMware, Inc  
2e 20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c | . VMware Virtual  
20 50 6c 61 74 66 6f 72 6d 1a 5b 00 00 00 09 01 | Platform.[.....  
55 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | Umdm-tlv=device-  
75 69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 | uid=3693C6407C92  
35 32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 | 5251FF72B6493BDD  
38 37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 | 87318ABFC90C6215  
34 32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 | 42C38FAF878EF496  
31 34 41 31 04 06 00 00 00 00 | 14A1.....

Parsed packet data.....  
Radius: Code = 4 (0x04)  
Radius: Identifier = 18 (0x12)  
Radius: Length = 714 (0x02CA)  
Radius: Vector: BEA06E4671AF5C658277C7B5507861D7  
Radius: Type = 1 (0x01) User-Name  
Radius: Length = 8 (0x08)  
Radius: Value (String) =

6a 73 6d 69 74 68 | jsmith  
Radius: Type = 5 (0x05) NAS-Port  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x5000  
Radius: Type = 6 (0x06) Service-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x2  
Radius: Type = 7 (0x07) Framed-Protocol  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x1  
Radius: Type = 8 (0x08) Framed-IP-Address  
Radius: Length = 6 (0x06)  
Radius: Value (IP Address) = 192.168.10.50 (0xC0A80A32)  
Radius: Type = 25 (0x19) Class  
Radius: Length = 59 (0x3B)  
Radius: Value (String) =  
43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000  
30 35 30 30 30 35 62 62 65 31 66 39 31 3a 63 6f | 050005bbelf91:co  
72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408  
34 2f 31 39 33 31 36 38 32 | 4/1931682  
Radius: Type = 30 (0x1E) Called-Station-Id  
Radius: Length = 16 (0x10)  
Radius: Value (String) =  
31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2  
Radius: Type = 31 (0x1F) Calling-Station-Id  
Radius: Length = 16 (0x10)  
Radius: Value (String) =  
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2  
Radius: Type = 40 (0x28) Acct-Status-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x1  
Radius: Type = 41 (0x29) Acct-Delay-Time  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x0  
Radius: Type = 44 (0x2C) Acct-Session-Id  
Radius: Length = 10 (0x0A)  
Radius: Value (String) =  
43 31 46 30 30 30 30 35 | C1F00005  
Radius: Type = 45 (0x2D) Acct-Authentic  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x1  
Radius: Type = 61 (0x3D) NAS-Port-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x5  
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint  
Radius: Length = 16 (0x10)  
Radius: Value (String) =  
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 24 (0x18)  
Radius: Vendor ID = 3076 (0x00000C04)  
Radius: Type = 146 (0x92) Tunnel-Group-Name  
Radius: Length = 18 (0x12)  
Radius: Value (String) =  
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAAnyConnectVPN  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 12 (0x0C)  
Radius: Vendor ID = 3076 (0x00000C04)  
Radius: Type = 150 (0x96) Client-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Integer) = 2 (0x0002)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 12 (0x0C)  
Radius: Vendor ID = 3076 (0x00000C04)

Radius: Type = 151 (0x97) VPN-Session-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Integer) = 1 (0x0001)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 12 (0x0C)  
Radius: Vendor ID = 3076 (0x00000C04)  
Radius: Type = 152 (0x98) VPN-Session-Subtype  
Radius: Length = 6 (0x06)  
Radius: Value (Integer) = 3 (0x0003)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 35 (0x23)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 29 (0x1D)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 44 (0x2C)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 38 (0x26)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m  
61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e  
66 2d 62 66 | f-bf  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 49 (0x31)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 43 (0x2B)  
Radius: Value (String) =  
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id  
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500  
30 35 62 62 65 31 66 39 31 | 05bbe1f91  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 51 (0x33)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 45 (0x2D)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-  
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 58 (0x3A)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 52 (0x34)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-  
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect  
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030  
34 39 | 49  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 63 (0x3F)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 57 (0x39)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=  
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service  
20 50 61 63 6b 20 31 | Pack 1

```

Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 64 (0x40)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 58 (0x3A)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual
50 6c 61 74 66 6f 72 6d | Platform
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 91 (0x5B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 85 (0x55)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961
34 41 31 | 4A1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)
send pkt 192.168.1.10/1813
rip 0x00002ace10874b80 state 6 id 18
rad_vrfy() : response message verified
rip 0x00002ace10874b80
: chall_state ''
: state 0x6
: reqauth:
be a0 6e 46 71 af 5c 65 82 77 c7 b5 50 78 61 d7
: info 0x00002ace10874cc0
session_id 0x18
request_id 0x12
user 'jsmith'
response '****'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 3

```

RADIUS packet decode (response)

```

-----
Raw packet data (length = 20).....
05 12 00 14 e5 fd b1 6d fb ee 58 f0 89 79 73 8e | .....m..X..ys.
90 dc a7 20 | ...

```

```

Parsed packet data.....
Radius: Code = 5 (0x05)
Radius: Identifier = 18 (0x12)
Radius: Length = 20 (0x0014)
Radius: Vector: E5FDB16DFBEE58F08979738E90DCA720
rad_procpkt: ACCOUNTING_RESPONSE
RADIUS_DELETE
remove_req 0x00002ace10874b80 session 0x18 id 18
free_rip 0x00002ace10874b80
radius: send queue empty
ciscofp3#

```

在FTD诊断CLI上运行“debug webvpn anyconnect 255”命令(>system support diagnostic-cli)，在

## Cisco Anyconnect客户端的Windows/Mac PC上点击“Connect”

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
ciscofp3> enable
```

```
Password: <hit enter>
```

```
ciscofp3# terminal monitor
```

```
ciscofp3# debug webvpn anyconnect 255
```

```
<hit Connect on Anyconnect client on PC>
```

```
http_parse_cstp_method()
```

```
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'Host: ciscofp3.cisco.com'
```

```
Processing CSTP header line: 'Host: ciscofp3.cisco.com'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
```

```
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
```

```
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 4.6.03049'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'Cookie: webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
Processing CSTP header line: 'Cookie:
```

```
webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
Found WebVPN cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
WebVPN Cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Version: 1'
```

```
Processing CSTP header line: 'X-CSTP-Version: 1'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Hostname: jsmith-PC'
```

```
Processing CSTP header line: 'X-CSTP-Hostname: jsmith-PC'
```

```
Setting hostname to: 'jsmith-PC'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-MTU: 1399'
```

```
Processing CSTP header line: 'X-CSTP-MTU: 1399'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
```

```
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
```

```
Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Base-MTU: 1500'
```

```
Processing CSTP header line: 'X-CSTP-Base-MTU: 1500'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
```

```
Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Full-IPv6-Capability: true'
```

```
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-DTLS-Master-Secret:
```

```
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
```

```
'
```

```
Processing CSTP header line: 'X-DTLS-Master-Secret:
```

```
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
```

```
'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-
```

```
SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:AES256-SHA:AES128-
```

```
SHA:DES-CBC3-SHA'
```

```
Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
```

```
SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:AES256-SHA:AES128-SHA:DES-CBC3-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
cstp_util_address_ipv4_accept: address assigned: 192.168.10.50
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0x7000, 0x00002acdfff1d6440, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.50!
No SVC ACL
Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406
tcp-mss = 1460
path-mtu = 1460(mss)
TLS Block size = 16, version = 0x303
mtu = 1460(path-mtu) - 0(opts) - 5(ssl) - 16(iv) = 1439
mod-mtu = 1439(mtu) & 0xffff0(complement) = 1424
tls-mtu = 1424(mod-mtu) - 8(cstp) - 48(mac) - 1(pad) = 1367
DTLS Block size = 16
mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dtls_hdr) - 16(dtls_iv) = 1443
mod-mtu = 1443(mtu) & 0xffff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cstp) - 20(mac) - 1(pad) = 1418
computed tls-mtu=1367 dtls-mtu=1418 conf-mtu=1406
DTLS enabled for intf=3 (outside)
override computed dtls-mtu=1418 with conf-mtu=1406
tls-mtu=1367 dtls-mtu=1406
SVC: adding to sessmgmt
Sending X-CSTP-MTU: 1367
Sending X-DTLS-MTU: 1406
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false
```

## 思科ISE

思科ISE >操作> RADIUS >实时日志>点击每个身份验证的详细信息

在思科ISE上验证您的VPN登录，并且ACL结果“PermitAccess”已提供实时日志显示jsmith通过VPN成功通过FTD身份验证

**Overview**

Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	
Endpoint Profile	
Authentication Policy	VPN Users >> Default
Authorization Policy	VPN Users >> Allow ASA VPN connections if AD Group VPNUsers
Authorization Result	PermitAccess

**Authentication Details**

Source Timestamp	2018-10-09 01:47:55.112
Received Timestamp	2018-10-09 01:47:55.113
Policy Server	corbinise
Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	
Calling Station Id	
Authentication Identity Store	corbdc3
Audit Session Id	0000000000070005bbc08c3
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	FTDVPN
Device Type	All Device Types
Location	All Locations

**Steps**

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Airespace Airespace-Wlan-Id
- 15048 Queried PIP - Radius.NAS-Port-Type
- 15041 Evaluating Identity Policy
- 15048 Queried PIP - Normalised Radius.RadiusFlowType
- 22072 Selected identity source sequence - All\_User\_ID\_Stores
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore - jsmith
- 24216 The user is not found in the internal users identity store
- 15013 Selected Identity Source - All\_AD\_Join\_Points
- 24430 Authenticating user against Active Directory - All\_AD\_Join\_Points
- 24325 Resolving identity - jsmith (Step latency=7106 ms)
- 24313 Search for matching accounts at join point -
- 24319 Single matching account found in forest -
- 24313 Search for matching accounts at join point - windows\_ad\_server.com
- 24366 Skipping unjoined domain - Windows\_AD\_Server.com
- 24323 Identity resolution detected single matching account
- 24343 RPC Logon request succeeded - jsmith
- 24402 User authentication against Active Directory succeeded - All\_AD\_Join\_Points
- 22037 Authentication Passed
- 24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
- 15036 Evaluating Authorization Policy
- 24432 Looking up user in Active Directory -
- 24355 LDAP fetch succeeded -
- 24416 User's Groups retrieval from Active Directory succeeded -
- 15048 Queried PIP - ExternalGroups
- 15016 Selected Authorization Profile - PermitAccess
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept



Location	All Locations
NAS IPv4 Address	0.0.0.0
NAS Port Type	Virtual
Authorization Profile	PermitAccess
Response Time	7294 milliseconds

**Other Attributes**

ConfigVersionId	257
DestinationPort	1812
Protocol	Radius
NAS-Port	28672
Tunnel-Client-Endpoint	(tag=0)
CVPN3000/ASA/PIX7x-Tunnel-Group-Name	FTDAnyConnectVPN
OriginalUserName	jsmith
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PIX7x-Client-Type	3
Acs SessionID	corbinise/322344084/1870108
SelectedAuthenticationIdentity Stores	Internal Users
SelectedAuthenticationIdentity Stores	All_AD_Join_Points
SelectedAuthenticationIdentity Stores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Allow ASA VPN connections if AD Group VPNusers
CPMSessionID	00000000000070005bbc08c3

CPMSessionID	00000000000070005bbc08c3
ISEPolicySetName	VPN Users
Identity SelectionMatchedRule	Default
StepLatency	14=7106
AD-User-Resolved-Identities	jsmith@cohadley3.local
AD-User-Candidate-Identities	jsmith@cohadley3.local
AD-User-Join-Point	COHADLEY3.LOCAL
AD-User-Resolved-DNs	CN=John Smith,CN=Users,DC=cohadley3,DC=local
AD-User-DNS-Domain	cohadley3.local

AD-User-NetBios-Name	COHADLEY3
IsMachineIdentity	false
UserAccountControl	66048
AD-User-SamAccount-Name	jsmith
AD-User-Qualified-Name	jsmith@cohadley3.local
DTLS Support	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
ExternalGroups	S-1-5-21-872014162-156988481-842954196-1121
IdentityAccessRestricted	false
RADIUS Username	jsmith
Device IP Address	
Called-Station-ID	
CiscoAVPair	audit-session-id=00000000000070005bbc08c3, ip:source-ip= coa-push=true

## AnyConnect VPN客户端

### DART捆绑包

[如何收集AnyConnect的DART捆绑包](#)

## 故障排除

### DNS

验证思科ISE、FTD、Windows Server 2012和Windows/Mac PC都可以相互解析或反向解析 ( 检查所有设备上的DNS )

#### Windows PC

启动命令提示符，并确保您可以在FTD的主机名上执行“nslookup”

#### FTD CLI

```
>show network
```

```
> nslookup 192.168.1.10
Server: 192.168.1.10
Address: 192.168.1.10#53
10.1.168.192.in-addr.arpa name = ciscoise.cisco.com
```

## ISE CLI:

```
ciscoise/admin# nslookup 192.168.1.20
Trying "20.1.168.192.in-addr.arpa"
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 56529
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;20.1.168.192.in-addr.arpa. IN PTR

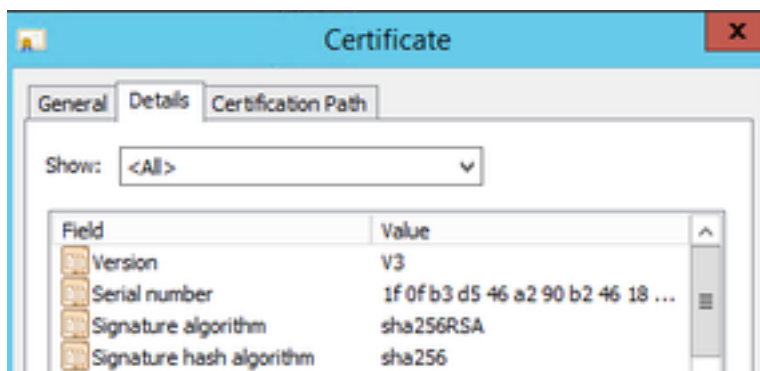
;; ANSWER SECTION:
20.1.168.192.in-addr.arpa. 1200 IN PTR ciscodc.cisco.com
```

## Windows Server 2012

启动命令提示符，并确保您可以在FTD的主机名/FQDN上执行“nslookup”

## 证书强度 (用于浏览器兼容性)

验证Windows Server 2012是否将证书签名为SHA256或更高版本。在Windows中双击您的根CA证书并检查“签名算法”字段



如果它们是SHA1，则大多数浏览器会显示这些证书的浏览器警告。要更改它，您可以在此处进行检查：

### [如何将Windows Server认证中心升级到SHA256](#)

验证FTD VPN服务器证书的以下字段是否正确 (当您在浏览器中连接到FTD时)

公用名= <FTDFQDN>

主题备用名称(SAN)= <FTDFQDN>

示例：

公用名：ciscofp3.cisco.com

主题备用名称(SAN):DNS名称=ciscofp3.cisco.com

## 连接和防火墙配置

在FTD CLI上使用捕获和在员工PC上使用Wireshark进行捕获，以验证数据包是否通过TCP+UDP 443传到FTD的外部IP。验证这些数据包是否来自员工家庭路由器的公有IP地址

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
```

```
<now hit Connect on AnyConnect Client from employee PC>
```

```
ciscofp3# show cap
```

```
capture capin type raw-data trace detail trace-count 100 interface outside [Buffer Full - 524153 bytes]
```

```
match ip any host 198.51.100.2
```

```
ciscofp3# show cap capin
```

```
2375 packets captured
```

```
1: 17:05:56.580994 198.51.100.2.55928 > 203.0.113.2.443: S 2933933902:2933933902(0) win 8192
```

```
2: 17:05:56.581375 203.0.113.2.443 > 198.51.100.2.55928: S 430674106:430674106(0) ack 2933933903 win 32768
```

```
3: 17:05:56.581757 198.51.100.2.55928 > 203.0.113.2.443: . ack 430674107 win 64240
```

```
...
```