

通过IKEv2将Anyconnect VPN配置为FTD与ISE

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[1. 导入SSL证书](#)

[2. 配置RADIUS服务器](#)

[2.1. 在FMC上管理FTD](#)

[2.2. 在ISE上管理FTD](#)

[3. 在FMC上为VPN用户创建地址池](#)

[4. 上传AnyConnect映像](#)

[5. 创建XML配置文件](#)

[5.1. 在配置文件编辑器上](#)

[5.2. 在FMC上](#)

[6. 配置远程访问](#)

[7. Anyconnect配置文件配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍在FMC管理的FTD上使用IKEv2和ISE身份验证的远程访问VPN的基本配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本VPN、TLS和互联网密钥交换版本2 (IKEv2)
- 基本身份验证、授权和记帐(AAA)以及RADIUS
- 使用Firepower管理中心(FMC)的经验

使用的组件

本文档中的信息基于以下软件版本：

- 思科Firepower威胁防御(FTD) 7.2.0
- 思科FMC 7.2.0

- AnyConnect 4.10.07073
- 思科ISE 3.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

IKEv2和安全套接字层(SSL)都是用于建立安全连接的协议，特别是在VPN环境中。IKEv2提供强大的加密和身份验证方法，为VPN连接提供高级别的安全性。

本文档提供了FTD版本7.2.0及更高版本的配置示例，它允许远程访问VPN使用传输层安全(TLS)和IKEv2。作为客户端，可以使用Cisco AnyConnect，它受多个平台支持。

配置

1. 导入SSL证书

配置AnyConnect时，证书至关重要。

手动注册证书有以下限制：

1. 在FTD上，生成证书签名请求(CSR)之前需要证书颁发机构(CA)证书。
2. 如果从外部生成CSR，则使用PKCS12的其他方法。

在FTD设备上获取证书有多种方法，但安全简单的方法是创建CSR并由CA签署。具体操作如下：

1. 定位至Objects > Object Management > PKI > Cert Enrollment，然后单击Add Cert Enrollment。
2. 输入信任点名称RAVPN-SSL-cert。
3. 在CA Information选项卡下，选择Manual“注册类型”，然后粘贴CA证书，如图所示。

Add Cert Enrollment



Name*

RAVPN-SSL-cert

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
-----BEGIN CERTIFICATE-----
MIIG1jCCBL6gAwIBAgIQQAFu+
wogXPrr4Y9x1zq7eDANBgkqhki
G9w0BAQsFADBK
MQswCQYDVQQGEwJVUzESMB
AGA1UEChMJSWRlbiRydXN0MS
cwJQYDVQQDEw5JZGVu
VHJ1c3QgQ29tbWVyY2lhbCBSb
290IENBIDEwHhcNMTkxMjE1
Y1NjE1WhcNMjkx
MiEvMTY1NiE1WiBvMOswCOYD
```

FMC - CA证书

4. 在Certificate Parameters下，输入主题名称。例如：

Add Cert Enrollment



Name*

RAVPN-SSL-cert

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN: Don't use FQDN in certificate ▼

Include Device's IP Address:

Common Name (CN): ftd.cisco.com

Organization Unit (OU): TAC

Organization (O): cisco

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Cancel

Save

FMC -证书参数

5. 在Key 选项卡下，选择密钥类型，然后提供名称和位大小。对于RSA，最少2048位。

6. 单击Save。

Add Cert Enrollment



Name*
RAVPN-SSL-cert

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:
 RSA ECDSA EdDSA

Key Name:*
RSA-key

Key Size:
2048 ▼

▼ Advanced Settings

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

Cancel **Save**

FMC -证书密钥

7. 定位至Devices > Certificates > Add > New Certificate。

8. 选择Device。在Cert Enrollment下，选择创建的信任点，然后单击Add（如图所示）。

Add New Certificate



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: RAVPN-SSL-cert
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Cancel

Add

FMC -向FTD注册证书

9. 单击ID，屏幕上将显示生成CSR的提示，请选择Yes。

The screenshot shows the Firewall Management Center interface. The top navigation bar includes "Overview", "Analysis", "Policies", "Devices", "Objects", and "Integration". The "Devices" tab is selected. The main content area displays a table of certificates for the device "ftd".

Name	Domain	Enrollment Type	Status
Root-CA	Global	Manual (CA Only)	
RAVPN-SSL-cert	Global	Manual (CA & ID)	Identity certificate import required

FMC -已注册证书CA

Warning

This operation will generate Certificate Signing Request do you want to continue?

No

Yes

FMC -生成CSR

10. 会生成一个可与CA共享的CSR，以便获取身份证书。

11. 从CA收到base64格式的身份证书后，请从磁盘上选择，方法是单击Browse Identity Certificate和Import，如图所示。

Import Identity Certificate



Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----
MIICqjCCAZICAQAwNjEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEWMBQGA1UEAwwNRIRELmNpc2NvLmNvbTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPLLwTQ6BkGjER2FfyofT+RMcCT5FQTrrMnFYok7drSKmdaKlycKM8Ljn+2m8BeVcfHsCpUybxn/ZrlsDMxSHo4E0oJEUgutsk++p1jIWcdVROn0vtahe+BRxC3qjo1FsLcp5zQru5goloRQRoiFwn5syAqOztgl0aUrFSSWF/Kdh3GeDE1XHPP1zzl4
```

Step 2

Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

[Import](#)

FMC -导入身份证书

12. 导入成功后，信任点RAVPN-SSL-cert将显示为：

Name	Domain	Enrollment Type	Status
RAVPN-SSL-cert	Global	Manual (CA & ID)	

FMC -信任点注册成功

2. 配置RADIUS服务器

2.1.在FMC上管理FTD

1. 导航至Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group。
2. 输入名称ISE，并单击+添加RADIUS服务器。

Name:*

ISE

Description:

Group Accounting Mode:

Single ▼

Retry Interval:* (1-10) Seconds

10

Realms:

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24



Enable dynamic authorization

Port:* (1024-65535)

1700

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname	
10.197.224.173	 

Cancel

Save

FMC - Radius服务器配置

- 提及ISE Radius服务器的IP地址以及与ISE服务器相同的共享密钥（密钥）。
- 选择FTD与ISE服务器通信时使用的Routing 或Specific Interface。

5. 单击Save 如图所示。

Edit RADIUS Server ?

IP Address/Hostname:*

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

Key:*

Confirm Key:*

Accounting Port: (1-65535)

Timeout: (1-300) Seconds

Connect using:
 Routing Specific Interface i

▼ +

Redirect ACL:
 ▼ +

6. 保存后，服务器即会添加到RADIUS Server Group 下，如图所示。

Name	Value
ISE	1 Server

FMC - RADIUS服务器组

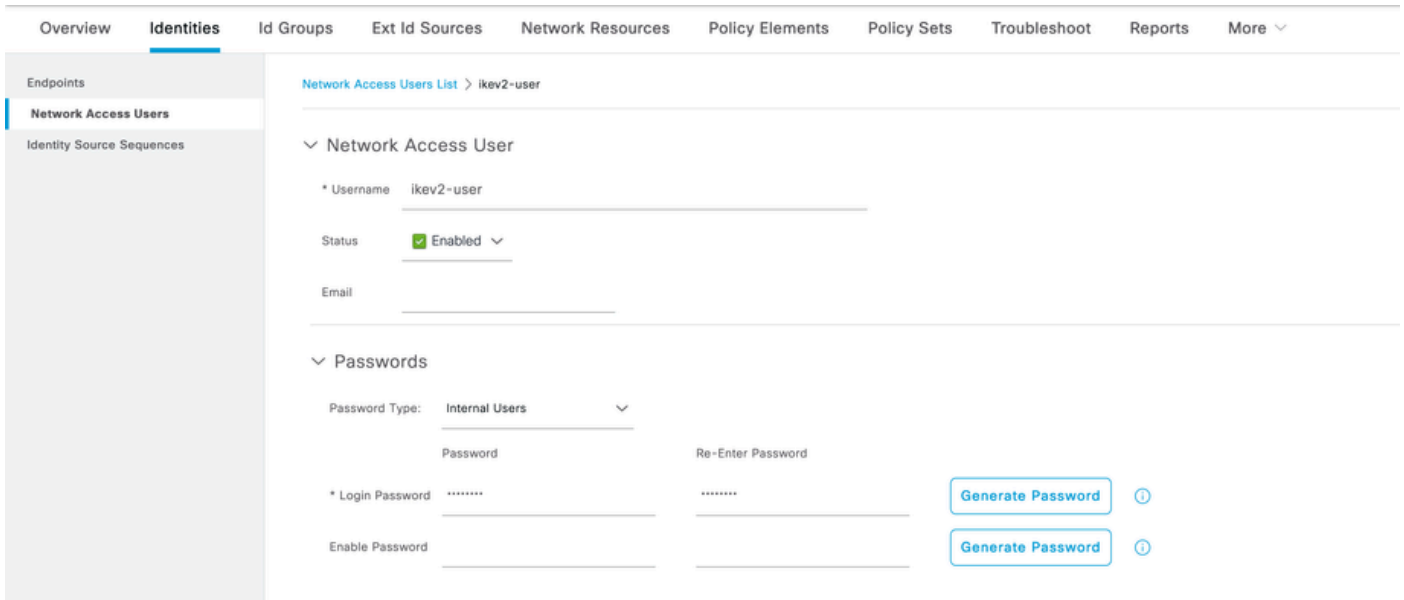
2.2.在ISE上管理FTD

1. 导航至Network Devices ，然后单击Add。
2. 输入服务器和FTD通信接口IP Address的RADIUS客户端的名称“Cisco-Radius”。
3. 在Radius Authentication Settings下，添加Shared Secret。
4. 单击Save。

The screenshot shows the configuration page for a Network Device in Cisco ISE. The device name is 'Cisco-Radius'. The IP address is set to 10.197.167.5/25. The device profile is 'Cisco-Radius'. Under 'RADIUS Authentication Settings', the protocol is 'RADIUS', and a shared secret has been entered. The CoA Port is set to 1700.

ISE -网络设备

5. 要创建用户，请导航至Network Access > Identities > Network Access Users ，然后单击 Add。
6. 根据需要创建UsernameandLogin Password。

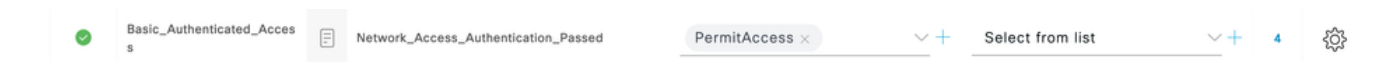


ISE -用户

7. 要设置基本策略，请定位至Policy > Policy Sets > Default > Authentication Policy > Default，选择All_User_ID_Stores。
8. 定位至Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access，并选择，如PermitAccess图所示。



ISE -身份验证策略



ISE -授权策略

3. 在FMC上为VPN用户创建地址池

1. 定位至Objects > Object Management > Address Pools > Add IPv4 Pools。
2. 输入名称RAVPN-Pool和地址范围，掩码是可选的。
3. 单击Save。

Edit IPv4 Pool



Name*

IPv4 Address Range*

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

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

▶ Override (0)

Cancel

Save

FMC - 地址池

4. 上传AnyConnect映像

1. 定位至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。
2. 输入名称anyconnect-win-4.10.07073-webdeploy，然后单击Browse 从磁盘中选择Anyconnect文件，然后单击Save（如图所示）。

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

FMC - Anyconnect客户端映像

5. 创建XML配置文件

5.1. 在配置文件编辑器上

1. 从software.cisco.com下载配置文件编辑器并打开它。
2. 定位至**Server List > Add...**
3. 输入“显示名称”RAVPN-IKEV2和FQDN以及“用户组”（别名）。
4. 选择主要协议 IPsec , 单击**Ok** 如图所示。

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) RAVPN-IKEV2

FQDN or IP Address User Group

ftd.cisco.com / RAVPN-IKEV2

Group URL

ftd.cisco.com/RAVPN-IKEV2

Connection Information

Primary Protocol IPsec

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

配置文件编辑器-服务器列表

5. 添加服务器列表。另存为ClientProfile.xml。

AnyConnect Profile Editor - VPN

File Help

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Profile: C:\Users\Amrutha\Documents\ClientProfile.xml

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins
RAVPN-IKEV2	ftd.cisco.com	RAVPN-IKEV2	-- Inherited --			

Note: it is highly recommended that at least one server be defined in a profile.

Add... Delete

Edit... Details

配置文件编辑器- ClientProfile.xml

5.2. FMC上

1. 定位至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。
2. 输入名称ClientProfile，然后单击Browse 以选择ClientProfile.xml磁盘文件。
3. 单击Save。

Edit AnyConnect File



Name:*

ClientProfile

File Name:*

ClientProfile.xml

Browse..

File Type:*

AnyConnect VPN Profile

Description:

Cancel

Save

FMC - Anyconnect VPN配置文件

6. 配置远程访问

1. 导航到Devices > VPN > Remote Access并单击+以添加连接配置文件 (如图所示)。

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy

FMC - 远程访问连接配置文件

2. 输入连接配置文件名称RAVPN-IKEV2 + , 并单击Group Policy中的创建组策略 (如图所示)。

Add Connection Profile



Connection Profile:*

Group Policy:* 

[Edit Group Policy](#)

Client Address Assignment

AAA

Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the '*Client Address Assignment Policy*' in the Advanced tab to define the assignment criteria.

Address Pools: 

Name	IP Address Range	

DHCP Servers: 

Name	DHCP Server IP Address	

Cancel

Save

FMC -组策略

3. 输入名称RAVPN-group-policy，选择VPN协议，SSL and IPsec-IKEv2 如图所示。

Edit Group Policy



Name:*

RAVPN-group-policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

FMC - VPN协议

4. 在AnyConnect > Profile下，从下拉列表中选择XML配置文件ClientProfile，然后单击Save(如图所示)。

Edit Group Policy



Name:*

RAVPN-group-policy

Description:

General

AnyConnect

Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

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

Client Profile:

ClientProfile



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](#).

Cancel

Save

FMC - Anyconnect配置文件

5.单击+ as shown in the image添加地址池RAVPN-Pool。

Edit Connection Profile

Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)



Client Address Assignment

AAA

Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
RAVPN-Pool	10.1.1.0-10.1.1.255	 

DHCP Servers: +

Name	DHCP Server IP Address	

Cancel

Save

FMC -客户端地址分配

6. 定位至AAA > Authentication Method , 然后选择AAA Only。

7. 选择Authentication Server作为ISE (RADIUS)。

Edit Connection Profile



Connection Profile:* RAVPN-IKEV2

Group Policy:* RAVPN-group-policy +

[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: ISE (RADIUS)

Fallback to LOCAL Authentication

Use secondary authentication

Authorization

Authorization Server: Use same authentication server

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

▶ Advanced Settings

Cancel

Save

FMC - AAA身份验证

8. 导航到Aliases ，输入RAVPN-IKEV2别名，在ClientProfile.xml中将其用作用户组。

9. 单击Save。

Edit Connection Profile



Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

Client Address Assignment

AAA

Aliases

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.



Name	Status	
RAVPN-IKEV2	Enabled	

URL Alias:

Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.



URL	Status	
-----	--------	--

Cancel

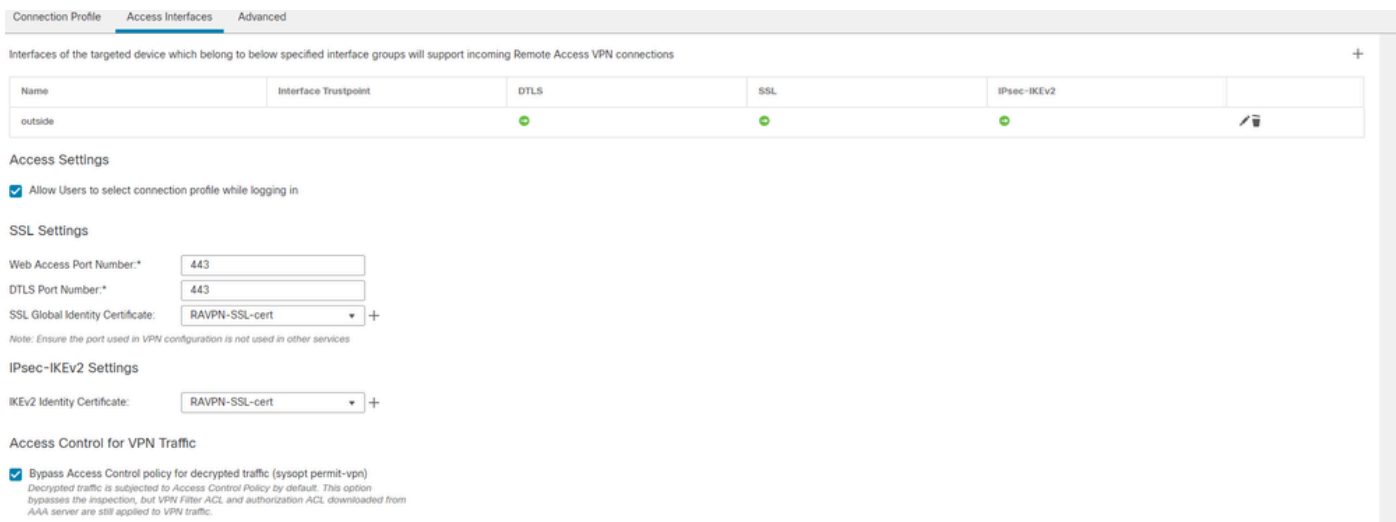
Save

FMC -别名

10. 导航到Access Interfaces(IKEv2) , 然后选择必须启用RAVPN IKEv2的接口。

11. 选择SSL和IKEv2的身份证书。

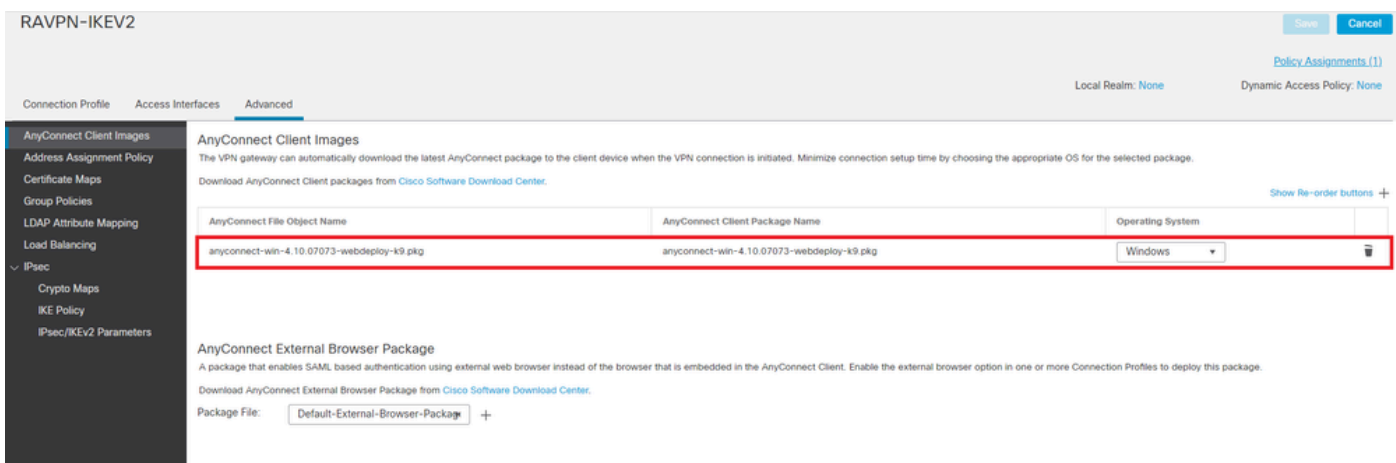
12. 单击Save。



FMC -接入接口

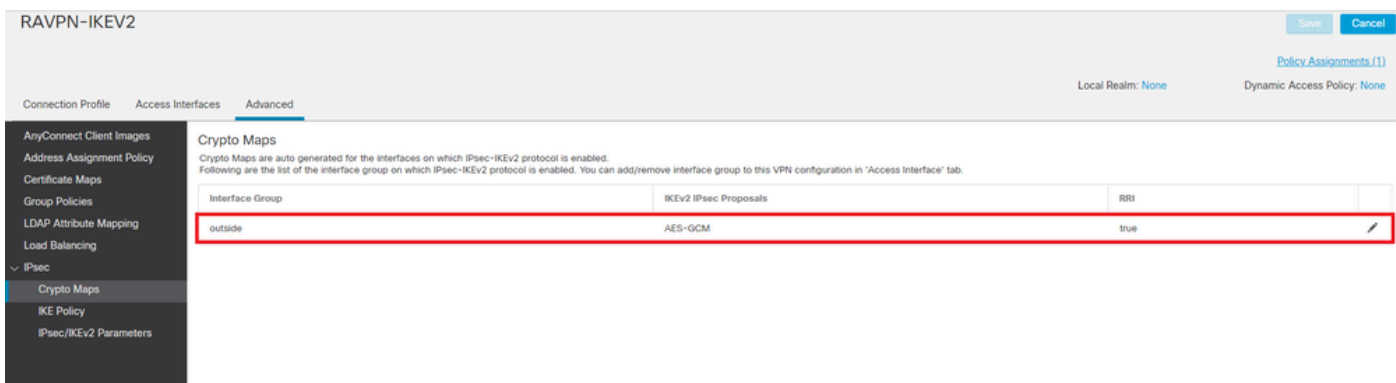
13. 导航至Advanced。

14. 单击+添加Anyconnect客户端映像。



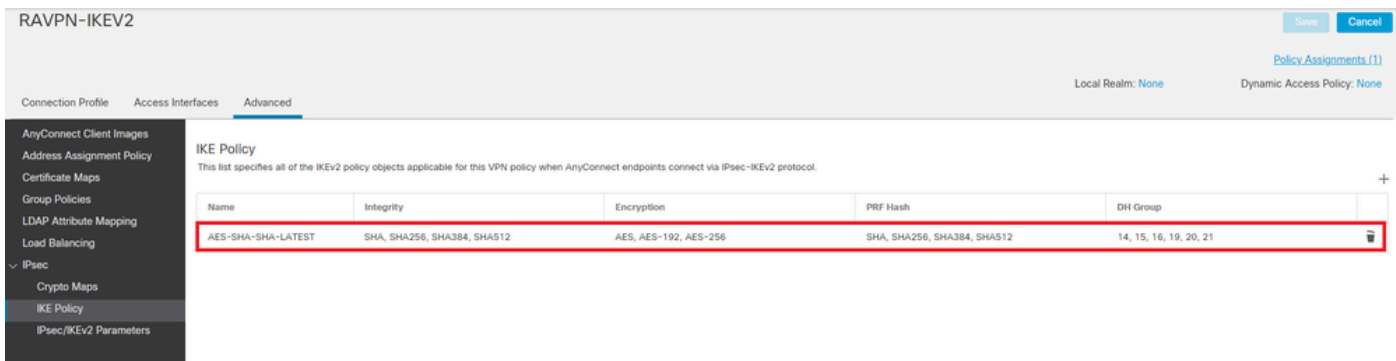
FMC - Anyconnect客户端软件包

15. 在IPsec下，添加如图所示的Crypto Maps。



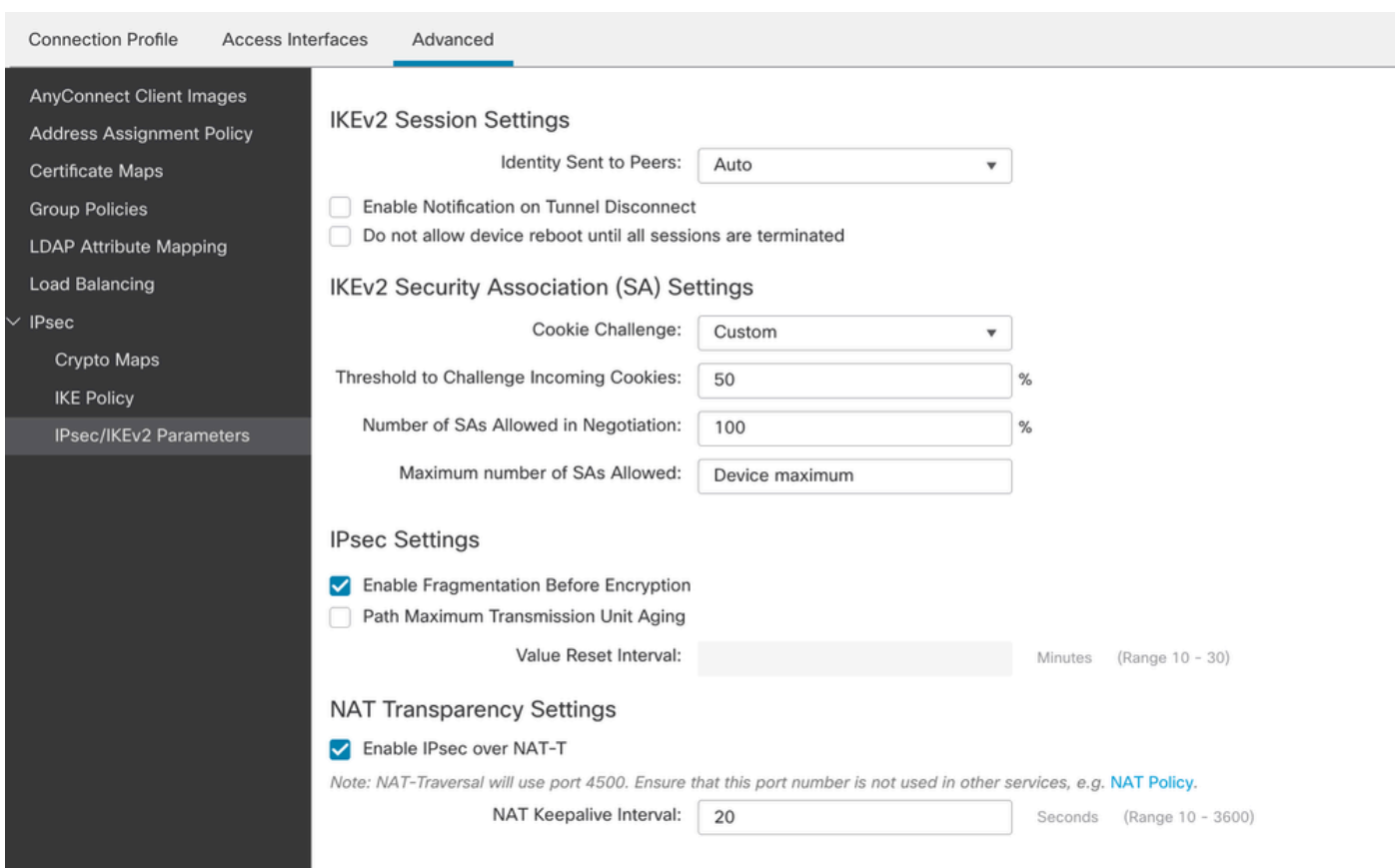
FMC -加密映射

16. 在IPsec下，单击+添加IKE Policy 命令。



FMC - IKE策略

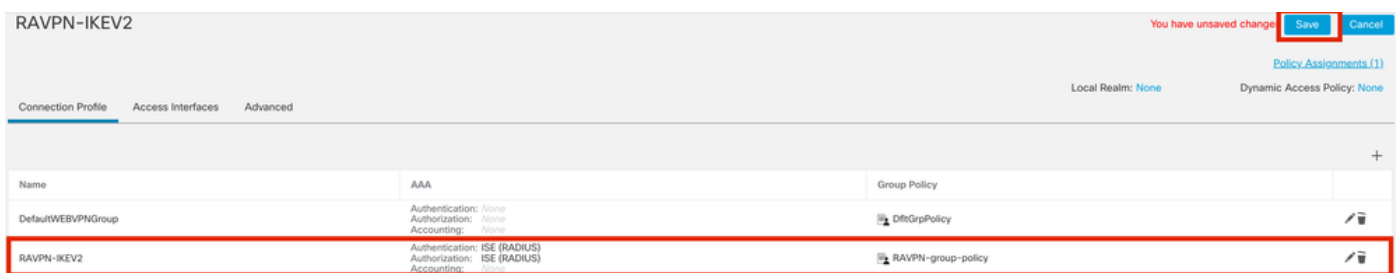
17. 在IPsec 下，添加IPsec/IKEv2 Parameters。



FMC - IPsec/IKEv2参数

18. 在Connection Profile下，创建新的配置文件RAVPN-IKEV2。

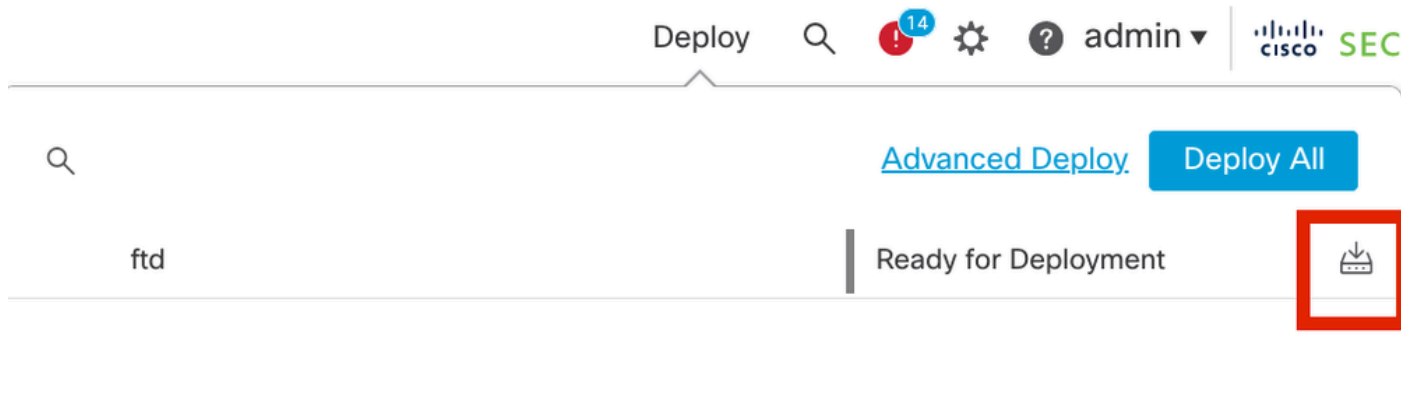
19. Save单击图中所示。



FMC -

连接配置文件RAVPN-IKEV2

20. 部署配置。



FMC - FTD部署

7. Anyconnect配置文件配置

PC上的配置文件，保存在 C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile .

<#root>

```
<?xml version="1.0" encoding="UTF-8"?> <AnyConnectProfile xmlns="http://schemas[dot]xmlsoap[dot]org/encoding/" xmlns:xsi="http://www[dot]w3[dot]org/2001/XMLSchema-instance">
  <HostName>RAVPN-IKEV2</HostName> <HostAddress>ftd.cisco.com</HostAddress> <UserGroup>RAVPN-IKEV2</UserGroup>
</HostEntry> </ServerList> </AnyConnectProfile>
```



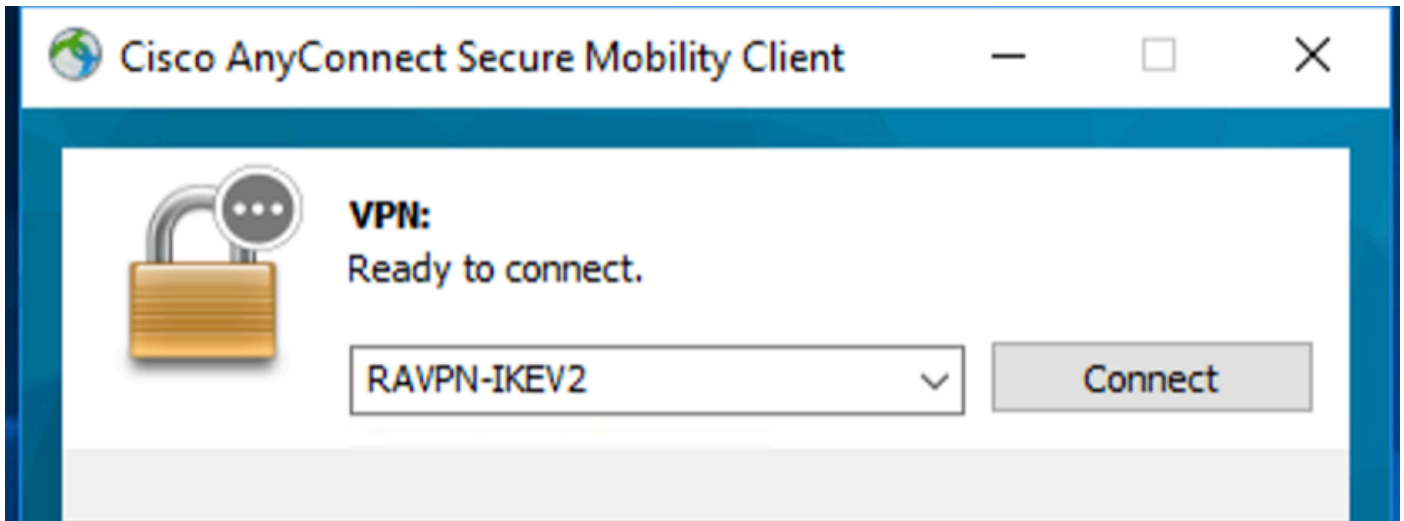
注意：建议在将客户端配置文件下载到所有用户的PC后，在组策略下禁用SSL客户端作为隧道协议。这可确保用户可以使用IKEv2/IPsec隧道协议以独占方式连接。

验证

您可以使用此部分来确认您的配置是否正常工作。

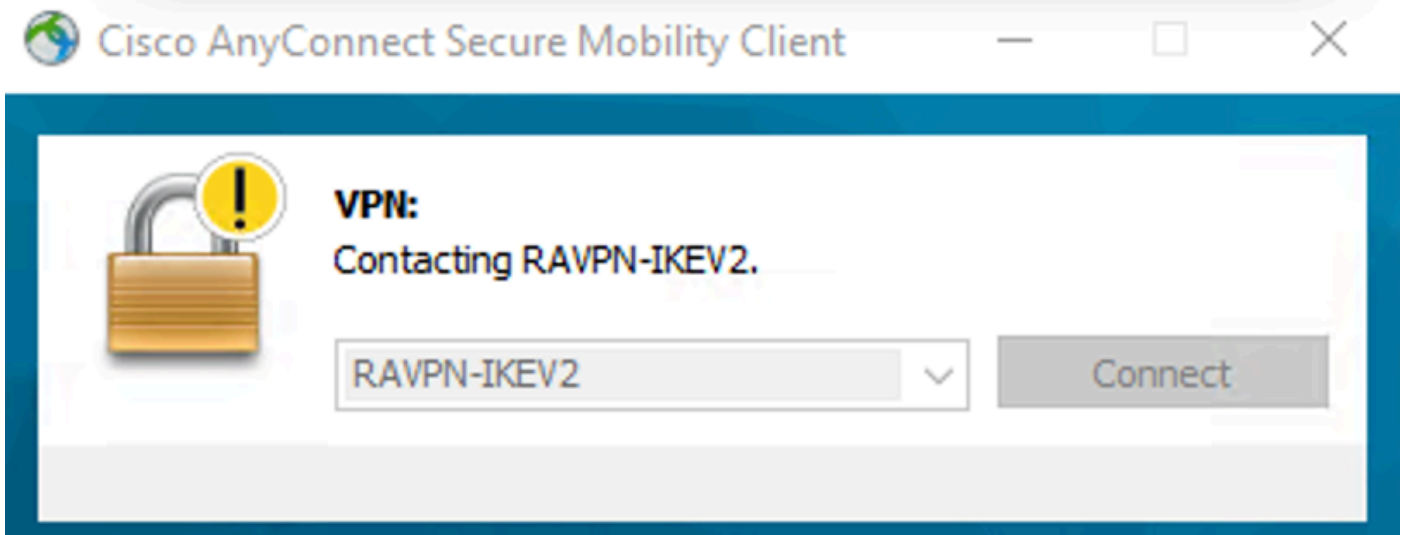
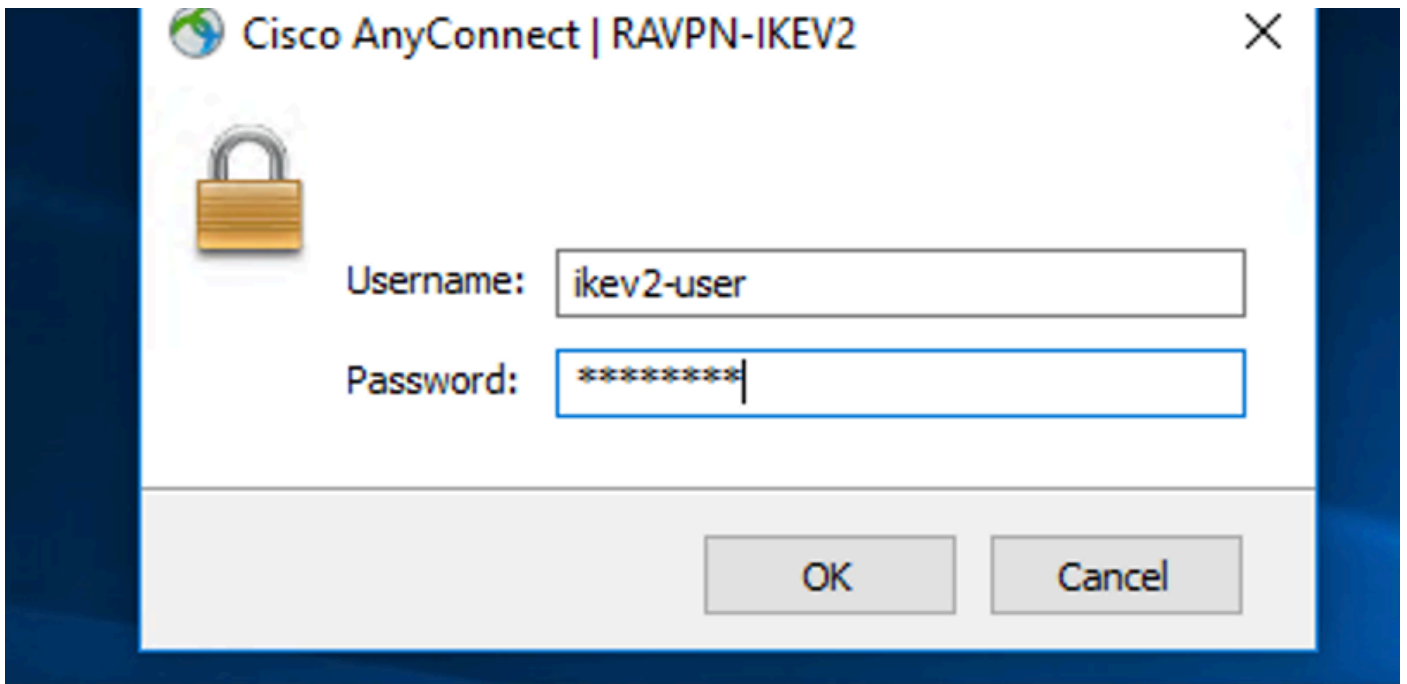
1. 对于第一个连接，使用FQDN/IP通过Anyconnect从用户的PC建立SSL连接。
2. 如果已禁用SSL协议且无法执行之前步骤，请确保客户端配置文件ClientProfile.xml存在于PC上的路径C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile下。
3. 系统提示后，输入用于身份验证的用户名和密码。

- 身份验证成功后，客户端配置文件会下载到用户的PC上。
- 断开与Anyconnect的连接。
- 下载配置文件后，请使用下拉列表选择客户端配置文件中提及的主机名，**RAVPN-IKEV2** 以便使用IKEv2/IPsec连接到Anyconnect。
- 单击Connect。



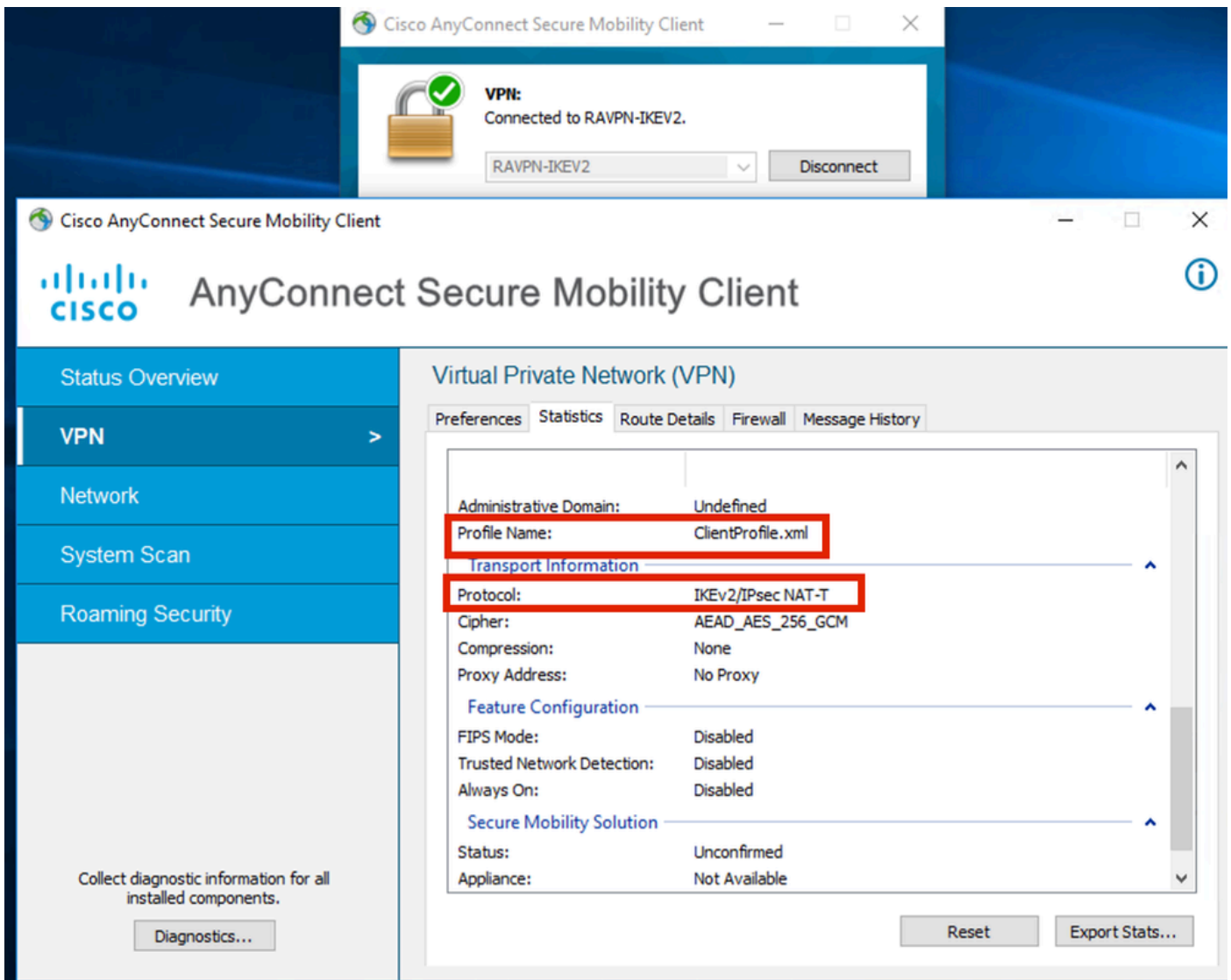
Anyconnect下拉列表

- 输入在ISE服务器上创建的身份验证的用户名和密码。



Anyconnect连接

9. 验证连接后使用的配置文件和协议(IKEv2/IPsec)。



已连接 AnyConnect

FTD CLI输出：

```
<#root>
```

```
firepower# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect
```

```
Username : ikev2-user                Index      : 9
Assigned IP : 10.1.1.1                Public IP  : 10.106.55.22
Protocol    : IKEv2 IPsecOverNatT AnyConnect-Parent
License     : AnyConnect Premium
Encryption  : IKEv2: (1)AES256 IPsecOverNatT: (1)AES-GCM-256 AnyConnect-Parent: (1)none
```

Hashing : IKEv2: (1)SHA512 IPsecOverNatT: (1)none AnyConnect-Parent: (1)none
Bytes Tx : 450 Bytes Rx : 656
Pkts Tx : 6 Pkts Rx : 8
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : RAVPN-group-policy Tunnel Group : RAVPN-IKEV2
Login Time : 07:14:08 UTC Thu Jan 4 2024
Duration : 0h:00m:08s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac5e205000090006596618c
Security Grp : none Tunnel Zone : 0

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 9.1
Public IP : 10.106.55.22
Encryption. : none. Hashing : none

Auth Mode : userPassword
Idle Time out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : 4.10.07073

IKEv2:

Tunnel ID : 9.2
UDP Src Port : 65220 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : AES256 Hashing : SHA512
Rekey Int (T): 86400 Seconds Rekey Left(T): 86391 Seconds
PRF : SHA512 D/H Group : 19
Filter Name :
Client OS : Windows Client Type : AnyConnect

IPsecOverNatT:

Tunnel ID : 9.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 10.1.1.1/255.255.255.255/0/0
Encryption : AES-GCM-256 Hashing : none
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T) : 28791 Seconds
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 450 Bytes Rx : 656
Pkts Tx : 6 Pkts Rx : 8

firepower# show crypto ikev2 sa

IKEv2 SAs:

Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote fvr/ivrf
16530741 10.197.167.5/4500 10.106.55.22/65220
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify: EAP
Life/Active Time: 86400/17 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 10.1.1.1/0 - 10.1.1.1/65535
ESP spi in/out: 0x6f7efd61/0xded2cbc8
```

firepower# show crypto ipsec sa

interface: Outside

Crypto map tag: CSM_Outside_map_dynamic, seq num: 30000, local addr: 10.197.167.5

Protected vrf:

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
current_peer: 10.106.55.22, username: ikev2-user
dynamic allocated peer ip: 10.1.1.1
dynamic allocated peer ip(ipv6): 0.0.0.0

#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.197.167.5/4500, remote crypto endpt.: 10.106.55.22/65220
path mtu 1468, ipsec overhead 62(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: DED2CBC8
current inbound spi : 6F7EFD61

inbound esp sas:

spi: 0x6F7EFD61 (1870593377)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={RA, Tunnel, NAT-T-Encaps, IKEv2, }
slot: 0, conn_id: 9, crypto-map: CSM_Outside_map_dynamic
sa timing: remaining key lifetime (sec): 28723
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:

0x00000000 0x000001FF

outbound esp sas:

spi: 0xDEDED2CBC8 (3738356680)

SA State: active

transform: esp-aes-gcm-256 esp-null-hmac no compression

in use settings = {RA, Tunnel, NAT-T-Encaps, IKEv2, }

slot: 0, conn_id: 9, crypto-map: CSM_Outside_map_dynamic

sa timing: remaining key lifetime (sec): 28723

IV size: 8 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

ISE日志：

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server	Mdm Ser...
Jan 04, 2024 07:14:10.4...			1	ikev2-user	00:50:56:8D:6B...	Windows1...	Default >>...	Default >>...	PermitAcc...						ise	
Jan 04, 2024 07:14:10.4...				ikev2-user	00:50:56:8D:6B...	Windows1...	Default >>...	Default >>...	PermitAcc...		Cisco-Radius		Workstation		ise	

ISE -实时日志

故障排除

本部分提供了可用于对配置进行故障排除的信息。

```
debug radius all
```

```
debug crypto ikev2 platform 255
```

```
debug crypto ikev2 protocol 255
```

```
debug crypto ipsec 255
```


关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。