

在FDM管理的FTD上配置启用IPv6的RAVPN和AAA身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[FDM上的配置](#)

[ISE上的配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍在FDM管理的FTD上配置启用IPv6的远程访问VPN并使用AAA身份验证的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全Firepower设备管理器(FDM)虚拟
- 思科安全防火墙威胁防御(FTD)虚拟
- VPN身份验证流程

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全FDM虚拟7.6.0
- 思科安全FTD虚拟7.6.0
- 思科安全客户端5.1.6.103

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。

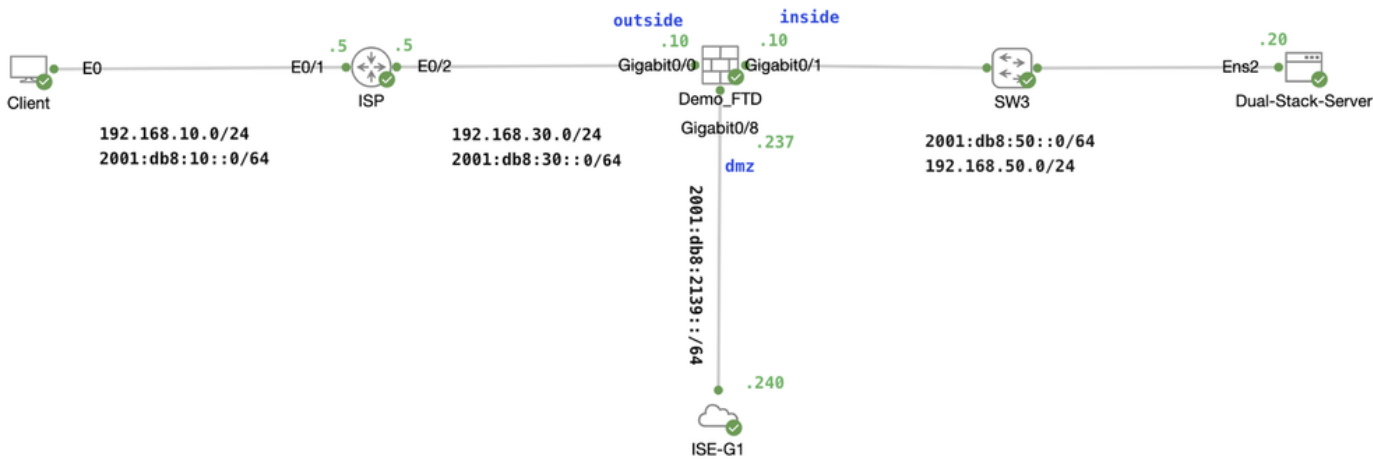
背景信息

IPv6远程访问VPN(RAVPN)正变得越来越重要，因为随着IPv4地址有限且几乎耗尽，IPv6提供的地址空间几乎是无限的，可容纳越来越多的互联网连接设备。随着更多的网络和服务迁移到IPv6，具有IPv6功能可确保您的网络保持兼容和访问。IPv6 RAVPN可帮助组织为未来的网络做好准备，确保安全且可扩展的远程连接。

在本示例中，客户端使用服务提供商提供的IPv6地址与VPN网关通信，但从VPN池接收IPv4和IPv6地址，使用思科身份服务引擎(ISE)作为身份验证身份源。ISE仅配置了IPv6地址。内部服务器配置有IPv4和IPv6地址，代表双堆栈主机。客户端可根据需要使用IPv4或IPv6 VPN地址访问内部资源。

配置

网络图



拓扑

FDM上的配置

步骤1.确保节点之间IPv4和IPv6互联的初步配置已适当完成。客户端和FTD的网关是相关的ISP地址。服务器的网关位于FTD的IP内部。ISE位于FTD的DMZ区域。

Firewall Device Manager

Monitoring Policies Objects **Device: ftdv760**

Device Summary
Interfaces

Cisco Secure Firewall Threat Defense for KVM

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7 0/8

MONITOR

CONSOLE

Interfaces Virtual Tunnel Interfaces

10 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ GigabitEthernet0	outside	ON	Routed	192.168.30.10	2001:db8:30::10/64	Enabled	
> ✓ GigabitEthernet1	inside	ON	Routed	192.168.50.10	2001:db8:50::10/64	Enabled	
> ○ GigabitEthernet2		OFF	Routed			Enabled	
> ○ GigabitEthernet3		OFF	Routed			Enabled	
> ○ GigabitEthernet4		OFF	Routed			Enabled	
> ○ GigabitEthernet5		OFF	Routed			Enabled	
> ○ GigabitEthernet6		OFF	Routed			Enabled	
> ○ GigabitEthernet7		OFF	Routed			Enabled	
> ✓ GigabitEthernet8	dmz	ON	Routed	2001:db8:2139::237/64		Enabled	

FTD_Interface_IP

Firewall Device Manager

Monitoring Policies Objects **Device: ftdv760**

Device Summary
Routing

Add Multiple Virtual Routers

Commands BGP Global Settings

Static Routing BGP OSPF EIGRP ECMP Traffic Zones

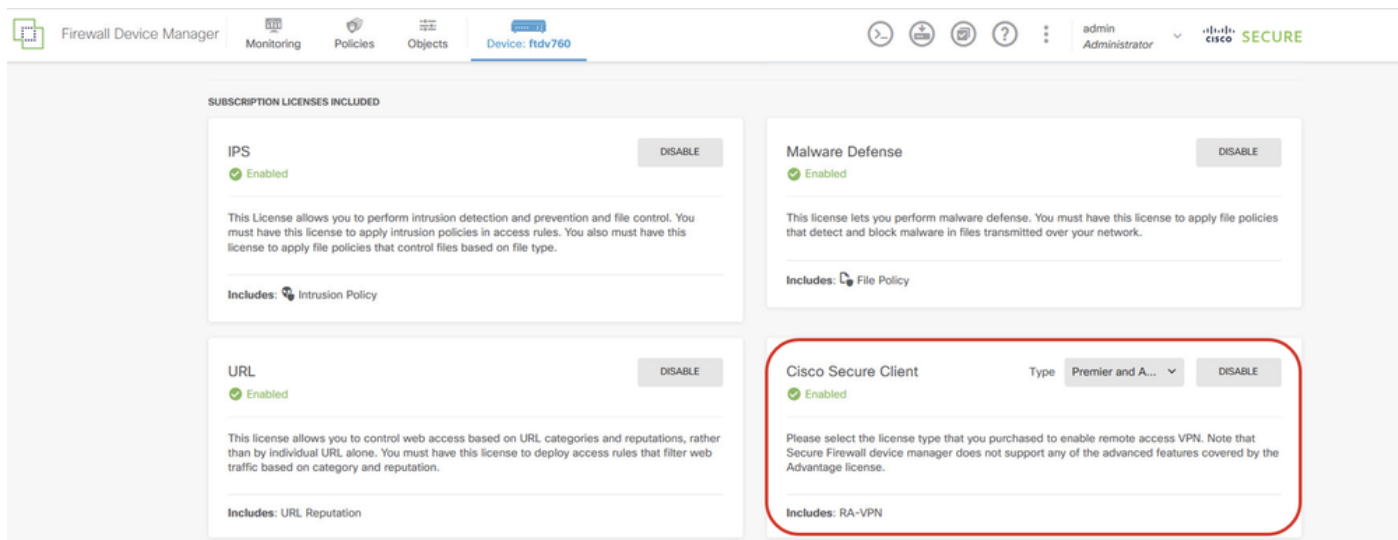
2 routes

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	TotISP_v4	outside	IPv4	0.0.0.0/0	192.168.30.5		1	
2	TotISP_v6	outside	IPv6	::/0	2001:db8:30::5		1	

FTD_Default_Route

第2步：从[Cisco软件下载](#)下载Cisco安全客户端软件包cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg，并确认下载文件的md5校验和与Cisco软件下载页面相同，以确保文件在下载后完好。

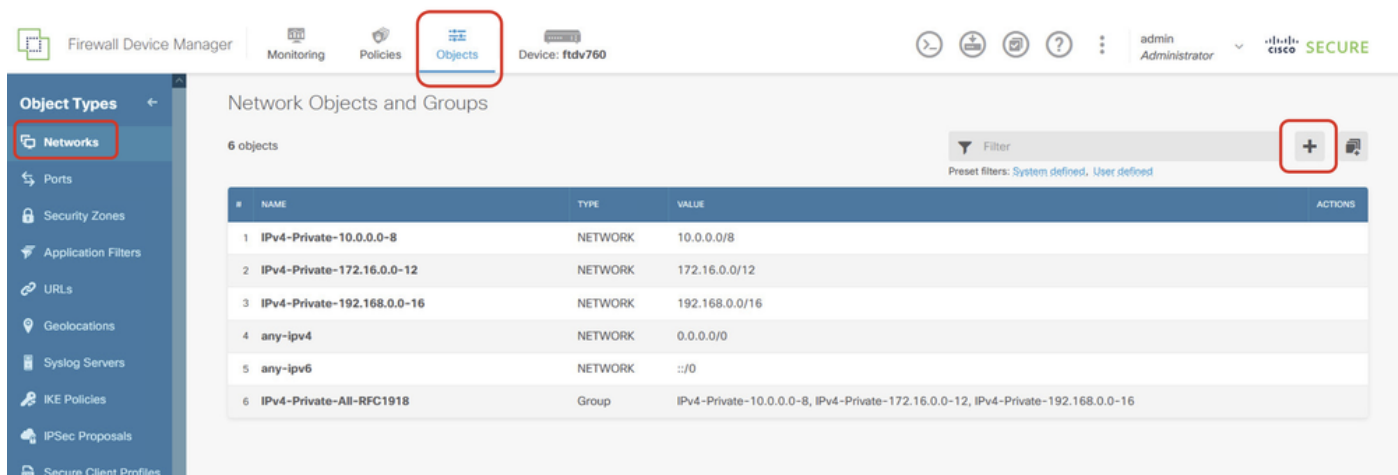
步骤3.检查是否在FTD上启用了RAVPN相关许可证。



FDM_License

步骤4.创建VPN地址池。

第4.1步：通过创建网络对象创建IPv6和IPv4地址池。导航到对象>网络，然后单击+按钮。



Create_VPN_Address_Pool_1

步骤4.2.提供每个网络对象的必要信息。单击OK按钮。

对于IPv4池，对象类型可以与“网络”或“范围”一起选择。在本示例中，为演示目的选择对象类型“网络”。

- 名称：demo_ipv4pool
- type：网络
- 网络:10.37.254.16/30

Add Network Object



Name

demo_ipv4pool

Description

Type



Network



Host



FQDN



Range

Network

10.37.254.16/30

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

Create_VPN_Address_Pool_2_IPv4

对于IPv6池，现在只能使用网络选择对象类型。

- 名称：demo_ipv6pool
- type：网络
- 网络:2001:db8:1234:1234::/124

Add Network Object

?

×

Name

demo_ipv6pool

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

2001:db8:1234:1234::/124

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

Create_VPN_Address_Pool_2_IPv6

步骤5.创建NAT豁免的内部网络。

第5.1步：导航到对象>网络，然后点击+按钮。

Firewall Device Manager

Monitoring

Policies

Objects

Device: ftdv760

admin Administrator

CISCO SECURE

Object Types

Networks

Ports

Security Zones

Application Filters

URLs

Geolocations

Syslog Servers

IKE Policies

IPSec Proposals

Secure Client Profiles

Network Objects and Groups

6 objects

Filter

+

Preset filters: System defined, User defined

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	
2	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12	
3	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16	
4	any-ipv4	NETWORK	0.0.0.0/0	
5	any-ipv6	NETWORK	::/0	
6	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16	

步骤5.2.提供每个网络对象的必要信息。单击 OK 按钮。

在本例中，IPv4和IPv6网络都已配置。

- 名称：inside_net_ipv4
- type：网络
- 网络:192.168.50.0/24

Add Network Object

Name

inside_net_ipv4

Description

Type

☒ Network ☐ Host ☐ FQDN ☐ Range

Network

192.168.50.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

- 名称：inside_net_ipv6
- type：网络
- 网络:2001:db8:50::/64

Add Network Object



Name

inside_net_ipv6

Description

Type



Network



Host



FQDN



Range

Network

2001:db8:50::/64

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

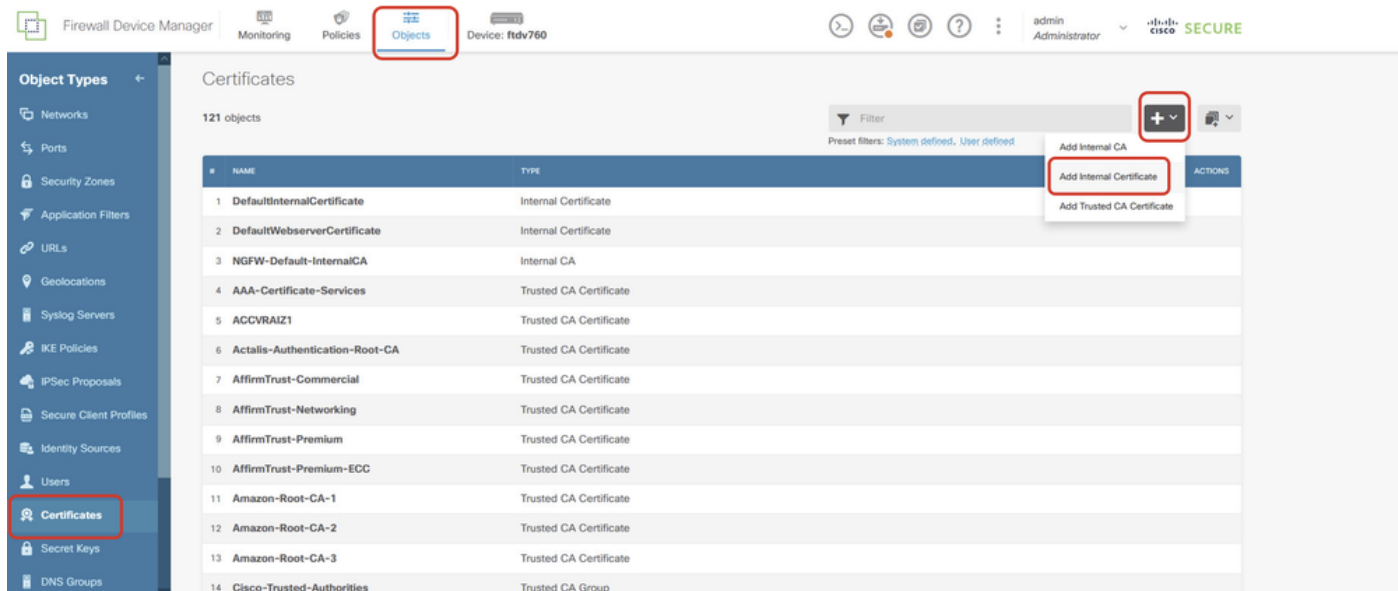
OK

Create_NAT_Exempt_Network_2_IPv6

步骤6.创建用于RAVPN的证书。您有两种选择：您可以上传由第三方证书颁发机构(CA)签名的证书，也可以生成新的自签名证书。

在本示例中，新的自签名证书与自定义的证书内容配合使用，用于演示目的。

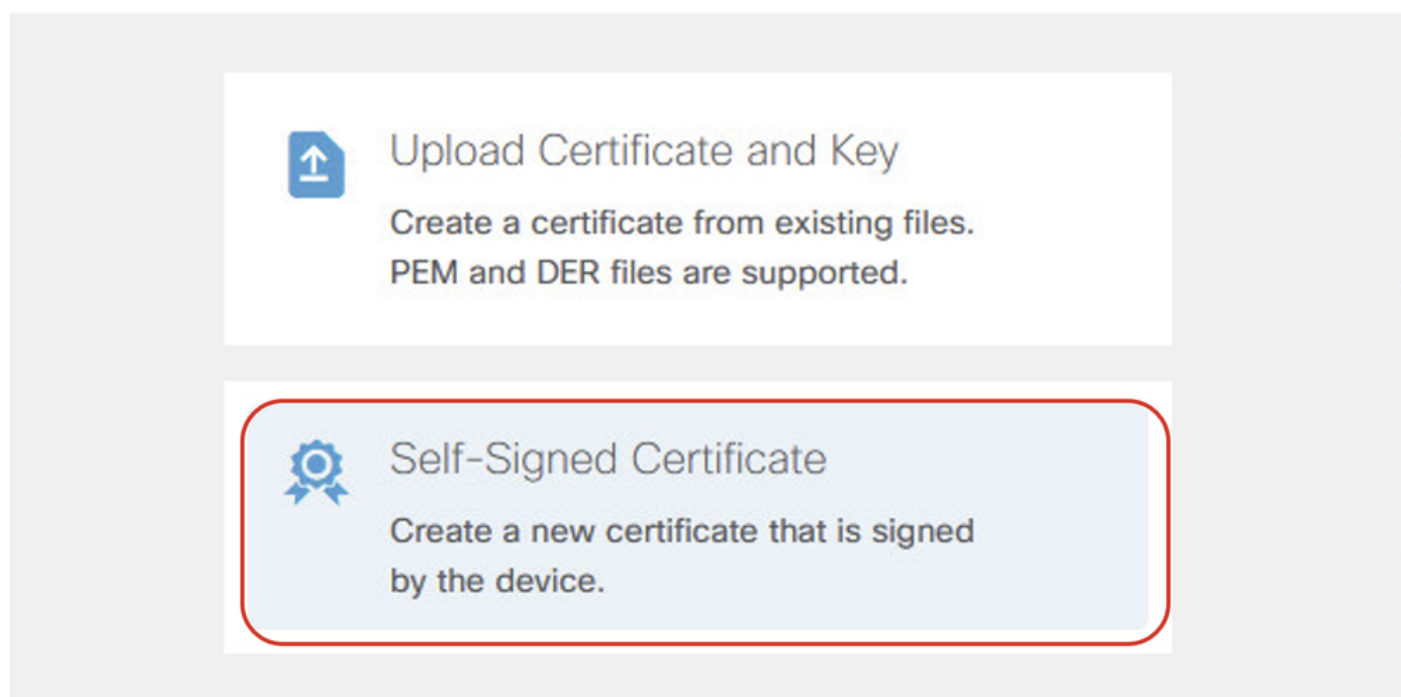
第6.1步：导航到对象>证书。单击+按钮，然后选择Add Internal Certificate。



Create_Certificate_1

步骤6.2.单击Self-Signed Certificate。

Choose the type of internal certificate you want to create



步骤6.3.单击General选项卡并提供必要信息。

名称 : demovpn

密钥类型 : RSA

密钥大小:2048

有效期:默认

到期日期：默认

特殊服务的验证用法：SSL服务器

?

×

Add Internal Certificate

Search for attribute

General

Issuer

Subject

Name

demovpn

Key Type

RSA

▼

Key Size

2048

▼

Validity Period

By Date

By Number of Days

Expiration Date

(UTC+08:00) Asia/Hong_Kong

02/15/2027

[Set default](#)

Default: 02/15/2027 (calculated based on 825 days according to [Apple requirements](#))

Validation Usage for Special Services

SSL Server ×

▼

CANCEL

SAVE

Create_Certificate_3

第6.4步：单击Issuer选项卡，并提供必要的信息。

国家/地区：美国

公用名：vpn.example.com

Add Internal Certificate

Search for attribute

General

Issuer

Subject

Country

United States (US)

State or Province

Locality or City

Organization

Organizational Unit (Department)

Common Name

vpn.example.com

You must specify a Common Name to use the certificate with remote access VPN.

CANCEL

SAVE

Create_Certificate_4

步骤6.5.单击Subject选项卡，提供必要信息，然后单击SAVE。

国家/地区：美国

公用名：vpn.example.com

Add Internal Certificate

Search for attribute

General

Issuer

Subject

Distinguished Name

Country

United States (US)

State or Province

Locality or City

Organization

Organizational Unit (Department)

Common Name

vpn.example.com

You must specify a Common Name to use the certificate with remote access VPN.

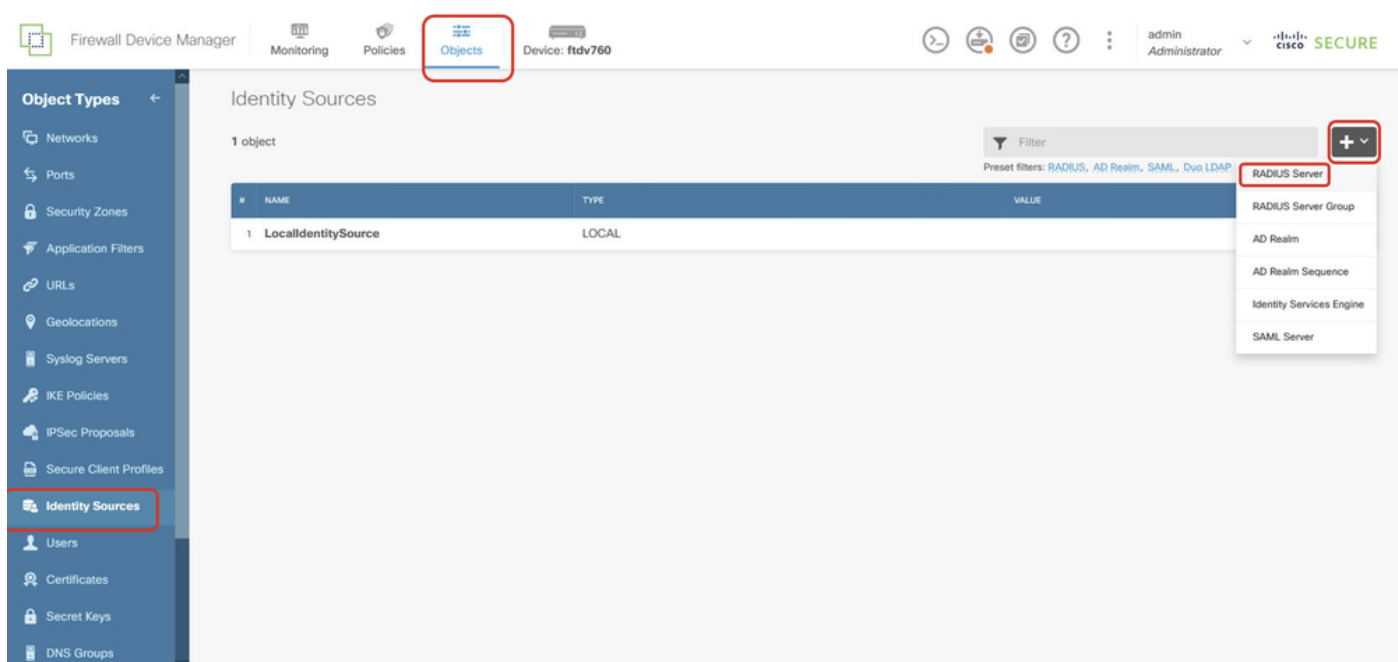
CANCEL

SAVE

Create_Certificate_5

步骤7.创建RADIUS服务器身份源。

第7.1步：导航到Objects > Identity Sources,点击+按钮，然后选择RADIUS Server。



Create_Radius_Source_1

步骤7.2.提供radius服务器的必要信息。单击OK按钮。

名称：demo_ise

服务器名称或IP地址：2001:db8:2139::240

验证端口:1812 (default)

超时：10 (default)

服务器密钥：思科

用于连接到Radius服务器的接口：手动选择接口。在本示例中，选择dmz(GigabitEthernet0/8)。

Add RADIUS Server



Name

demo_ise

Server Name or IP Address

2001:db8:2139::240

Authentication Port

1812

Timeout

10

seconds

1-60

Server Secret Key

●●●●●●●●

RA VPN Only (if this object is used in RA VPN Configuration)

Redirect ACL

Please select

Interface used to connect to Radius server



Resolve via route lookup



Manually choose interface

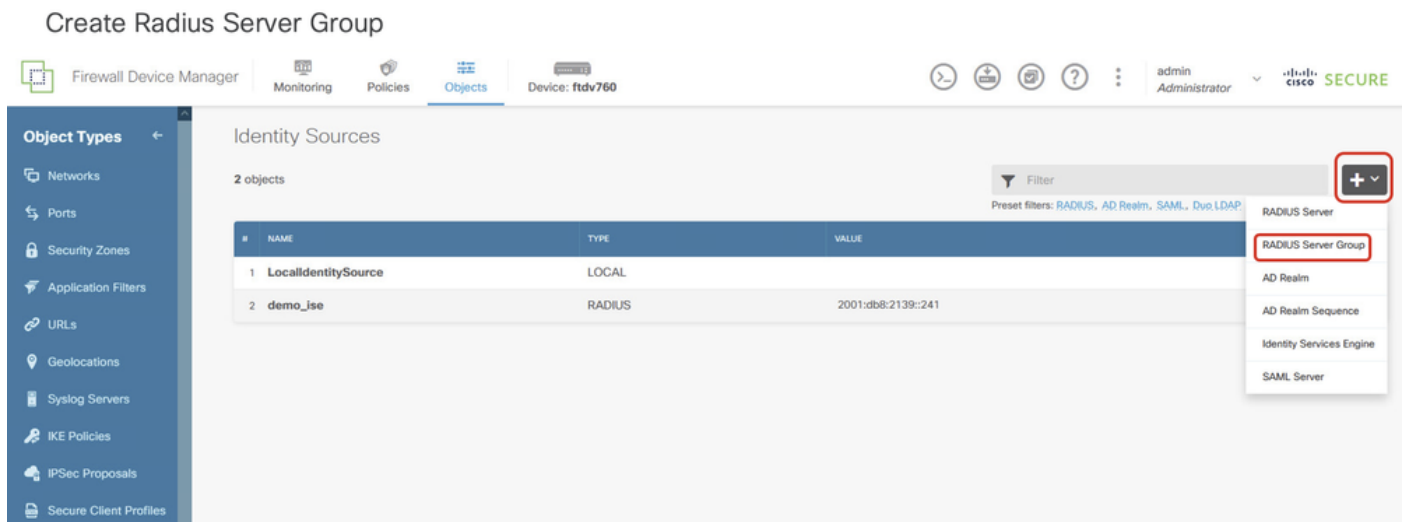
dmz (GigabitEthernet0/8)

CANCEL

OK

Create_Radius_Source_2

第7.3步：导航到对象>身份源。单击+按钮，然后选择RADIUS Server Group。



Create_Radius_Source_3

步骤7.4.提供radius服务器组的必要信息。单击 OK 按钮。

名称 : demo_ise_group

失效时间:10 (default)

最大失败尝试次数 : 3 (default)

RADIUS 服务器:单击+按钮，选择在步骤6.2中创建的名称。在本例中为demo_ise。

Add RADIUS Server Group



Name

demo_ise_group

Dead Time

10

minutes

0-1440

Maximum Failed Attempts

3

1-5



Dynamic Authorization (for RA VPN only)

Port

1700

1024-65535

Realm that Supports the RADIUS Server

Please select



RADIUS Server



The servers in the group should be backups of each other



Filter



demo_ise



CANCEL

OK

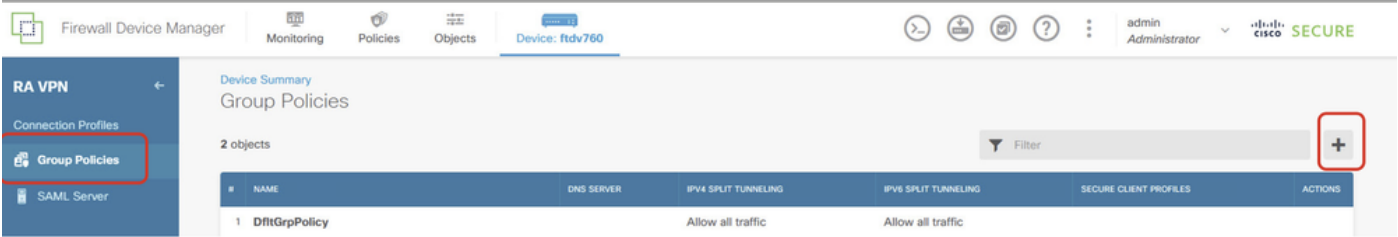
Create new RADIUS Server

CANCEL

OK

步骤8.创建用于RAVPN的组策略。在本示例中，为演示目的配置了自定义标语和超时设置。您可以根据实际需求进行修改。

第8.1步：导航到远程接入VPN >查看配置。在左侧栏中单击Group Policies，然后单击+按钮。

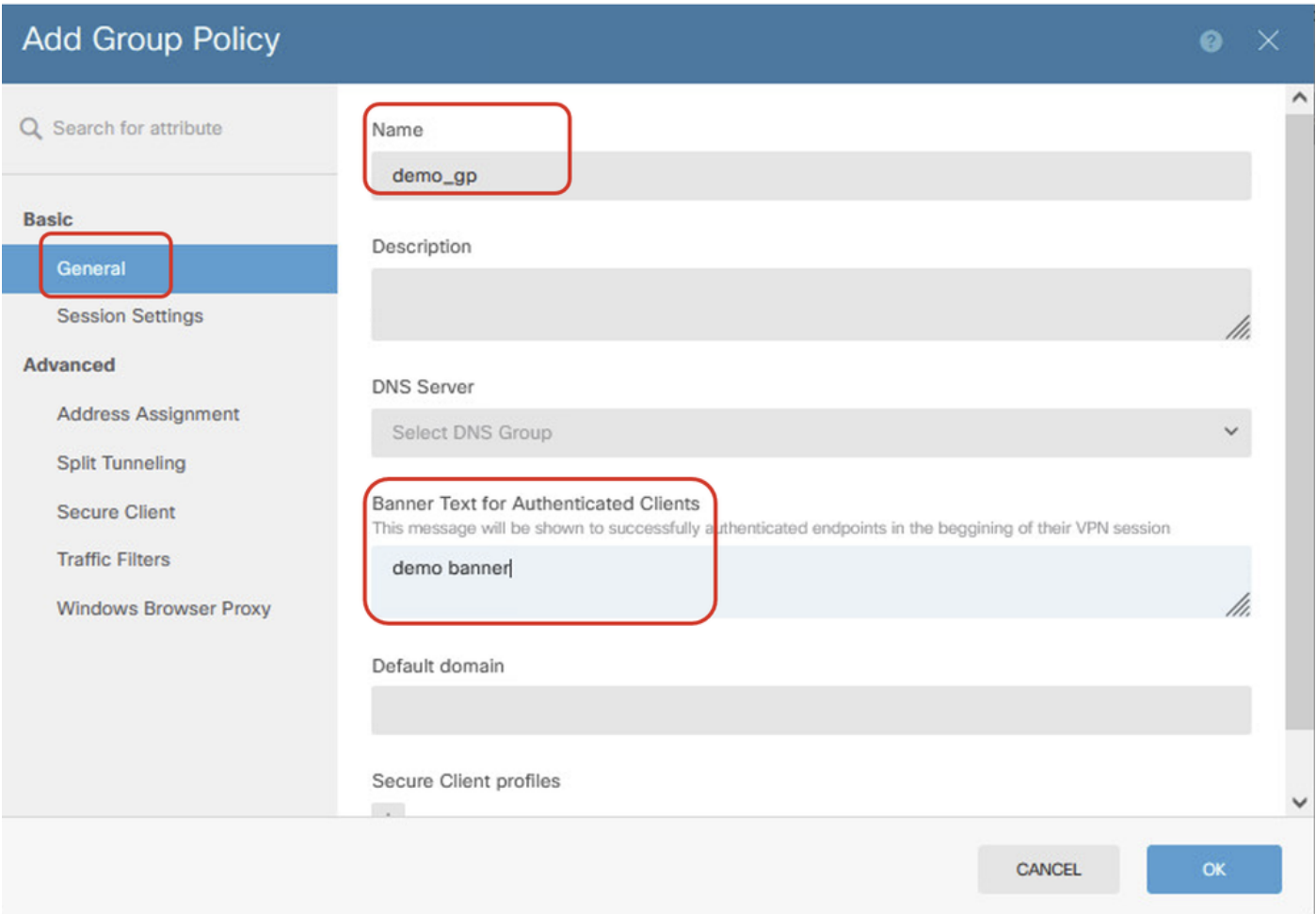


Create_Group_Policy_1

步骤8.2.单击General并提供必需的信息。

名称：demo_gp

经过身份验证的客户端的标语文本：演示横幅



Create_Group_Policy_2

步骤8.3.单击Secure Client并提供必要信息。

选中Enable Datagram Transport Layer Security(DTLS)。

The screenshot displays the configuration interface for a Secure Client. On the left, a sidebar contains a search bar and a list of settings categories: Basic (General, Session Settings), Advanced (Address Assignment, Split Tunneling, Secure Client, Traffic Filters, Windows Browser Proxy). The 'Secure Client' option is highlighted with a red rectangle. The main panel is titled 'SSL SETTINGS' and contains the following options: 'Enable Datagram Transport Layer Security (DTLS)' is checked and highlighted with a red rectangle; 'DTLS Compression' is unchecked; 'SSL Compression' is set to 'Disabled'; 'SSL Rekey Method' is set to 'None'; 'SSL Rekey Interval' is set to '4' minutes, with a range of '4 - 10080' minutes indicated below. Below the SSL settings is the 'CONNECTION SETTINGS' section, which includes 'Ignore the DF (Don't Fragment) bit' (unchecked), 'Client Bypass Protocol' (unchecked), and 'MTU' (partially visible). At the bottom right, there are 'CANCEL' and 'OK' buttons.

Create_Group_Policy_3

检查安全客户端和VPN网关之间的Keepalive消息（默认值）。

检查网关端间隔上的DPD（默认值）。

选中DPD on Client Side Interval(Default value)。

Search for attribute

Basic

General

Session Settings

Advanced

Address Assignment

Split Tunneling

Secure Client

Traffic Filters

Windows Browser Proxy

☐ Ignore the DF (Don't Fragment) bit

☐ Client Bypass Protocol

MTU

1406 bytes

576 - 1462

☒ Keepalive Messages Between Secure Client and VPN Gateway

20 seconds

15 - 600; (Default: 20)

☒ DPD on Gateway Side Interval ⓘ

30 seconds

5 - 3600

☒ DPD on Client Side Interval

30 seconds

5 - 3600

CANCEL OK

Create_Group_Policy_3_Cont

步骤9.创建RAVPN连接配置文件。

第9.1步：导航到远程接入VPN >查看配置。单击左侧栏中的Connection Profile，然后单击+按钮以启动向导。

Config RAVPN Connection Profile

Firewall Device Manager Monitoring Policies Objects Device: ftdv760

RA VPN

Connection Profiles

Group Policies

SAML Server

Device Summary

Remote Access VPN Connection Profiles

Filter +

#	NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.				

CREATE CONNECTION PROFILE

Create_RAVPN_Wizard_1

第9.2步：在Connection and Client Configuration部分提供必要信息，然后单击“下一步”按钮。

连接配置文件名称：demo_ravpn

组别名：demo_ravpn

Connection and Client Configuration

Specify how to authenticate remote users and the secure clients they can use to connect to the inside network.

Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

demo_ravpn

Group Alias (one per line, up to 5)

demo_ravpn

[Add Another Group Alias](#)

Group URL (one per line, up to 5)

[Add Another Group URL](#)

Create_RAVPN_Wizard_2_Conn_Name

Primary Identity Source > Authentication Type:仅AAA

Primary Identity Source > Primary Identity Source:demo_ise_group (步骤7.4中配置的名称。)

回退本地身份源：LocalIdentitySource

授权服务器：demo_ise_group (步骤7.4中配置的名称。)

记帐服务器：demo_ise_group (在步骤7.4中配置的名称。)

Primary Identity Source

Authentication Type

AAA Only



Primary Identity Source for User Authentication

demo_ise_group



Fallback Local Identity Source ⚠

LocalIdentitySource



⌵ Advanced

Secondary Identity Source

Secondary Identity Source for User Authentication

Please Select Identity Source



⌵ Advanced

Authorization Server

demo_ise_group



Accounting Server

demo_ise_group



Create_RAVPN_Wizard_2_Identity_Source

IPv4地址池：demo_ipv4pool (步骤4.2中配置的名称。)

IPv6地址池：demo_ipv6pool (步骤4.2中配置的名称。)

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool

+

demo_ipv4pool

IPv6 Address Pool

Endpoints are provided an address from this pool

+

demo_ipv6pool

DHCP Servers

+

CANCEL

NEXT

Create_RAVPN_Wizard_2_Address_Pool

第9.3步：在远程用户体验部分，选择在步骤8.2.中配置的组策略，然后单击NEXT按钮。

Firewall Device Manager

Monitoring

Policies

Objects

Device: ftdv760

admin Administrator

CISCO SECURE

Remote User Experience

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.

View Group Policy

demo_gp

Policy Group Brief Details

DNS - BANNER

DNS ServerNone

Banner Text for Authenticated Clientsdemo banner - fdm

SESSION SETTINGS

Maximum Connection Time / Alert IntervalUnlimited / 1 Minutes

Idle Time / Alert Interval30 / 1 Minutes

Simultaneous Login per User3

IPsec Tunneling

BACK

NEXT

IPsec Tunneling

Create_RAVPN_Wizard_3

第9.4步：在“全局设置”部分提供必要的信息，然后单击NEXT按钮。

设备身份证书：demovpn(步骤6.3中配置的名称。)

外部接口:外部

Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity

demovpn (Validation Usage: SSL Server) ▾

Outside Interface

outside (GigabitEthernet0/0) ▾

Fully-qualified Domain Name for the Outside Interface

e.g. ravpn.example.com

Port

443

e.g. 8080

Create_RAVPN_Wizard_4

VPN流量的访问控制：选中Bypass Access Control policy for decrypted traffic(sysopt permit-vpn)。

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic.



Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

Create_RAVPN_Wizard_4_VPN_ACP

NAT免除：单击滑块到“已启用”位置

内部接口：内部

内部网络：inside_net_ipv4、inside_net_ipv6（步骤5.2中配置的名称。）

NAT Exempt



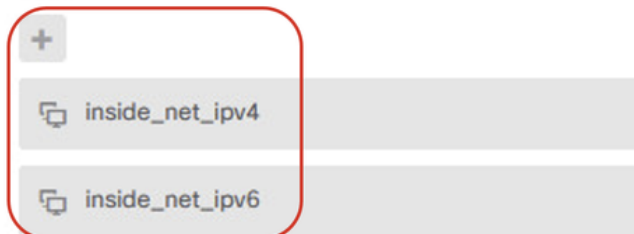
Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



Create_RAVPN_Wizard_4_VPN_NATExempt

安全客户端软件包：单击UPLOAD PACKAGE，然后相应地上传包。在本例中，Windows程序包已上传。

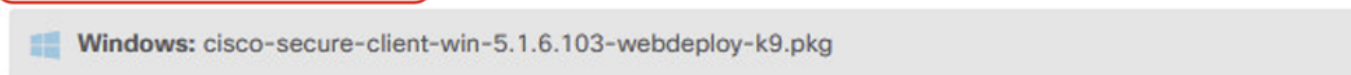
Secure Client Package

If a user does not already have the right secure client package installed, the system will launch the secure client installer when the client authenticates for the first time. The user can then install the package from the system.

You can download secure client packages from software.cisco.com.

You must have the necessary secure client software license.

Packages



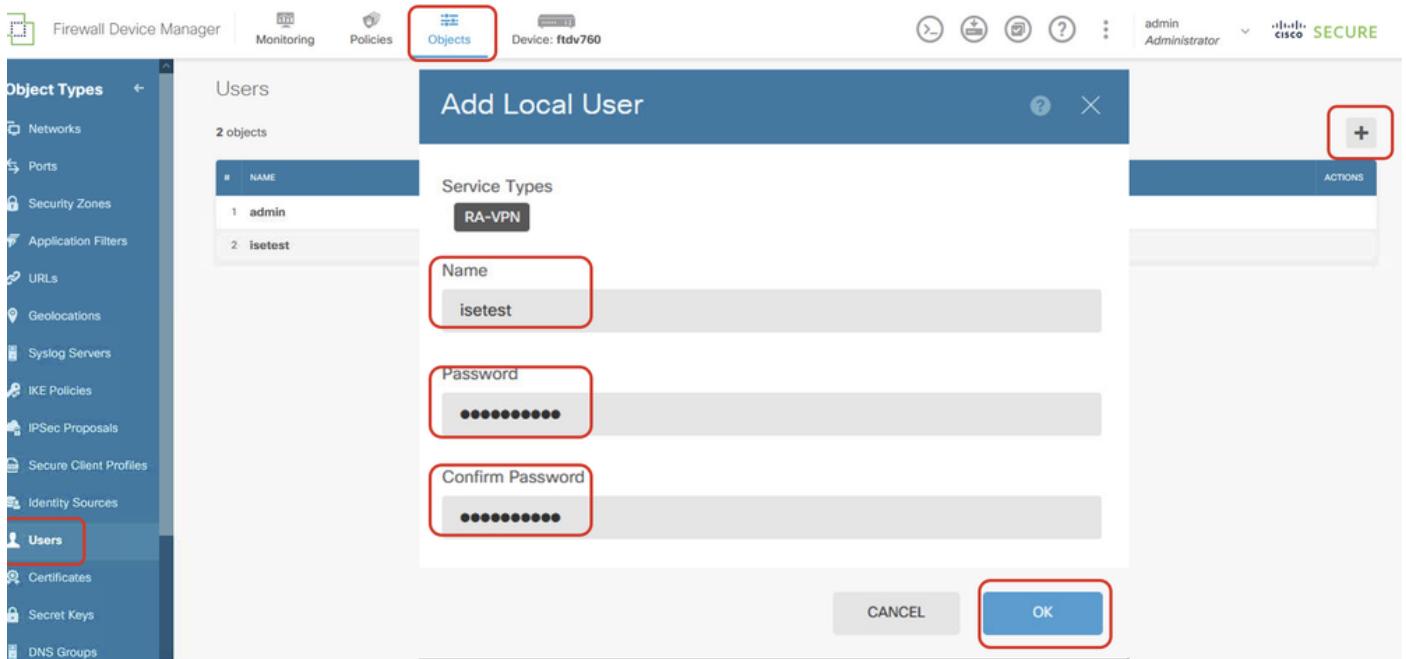
BACK

NEXT

Create_RAVPN_Wizard_4_Image

步骤9.5.查看摘要。如果需要修改任何内容，请单击BACK按钮。如果一切正常，请单击FINISH按钮。

第10步：如果第9.2步中的LocalIdentitySource选择了Fallback Local Identity Source，则创建本地用户。本地用户的密码需要与ISE上配置的密码相同。



Create_Local_User

步骤11.部署配置更改。

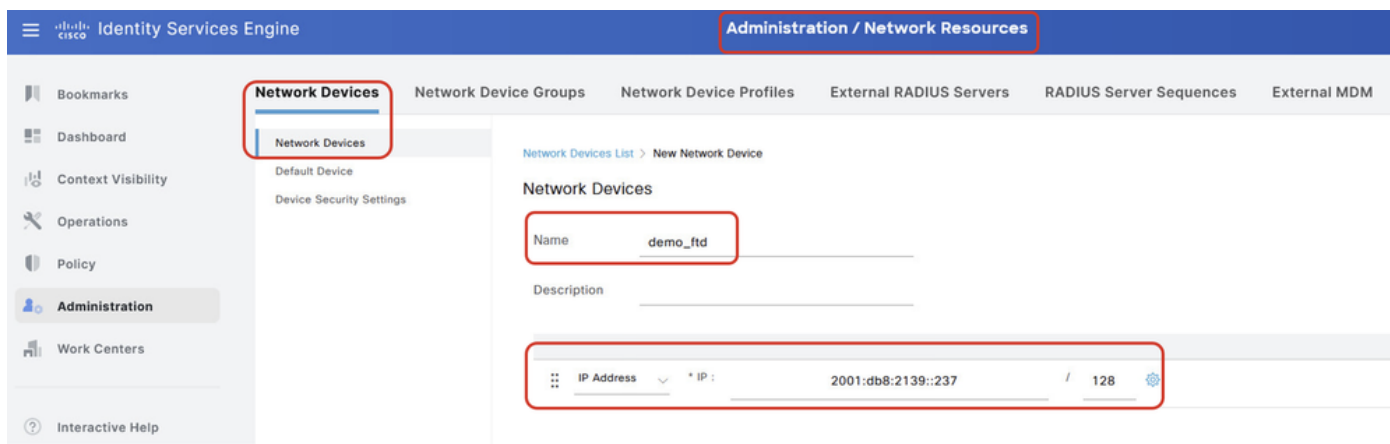


部署_更改

ISE上的配置

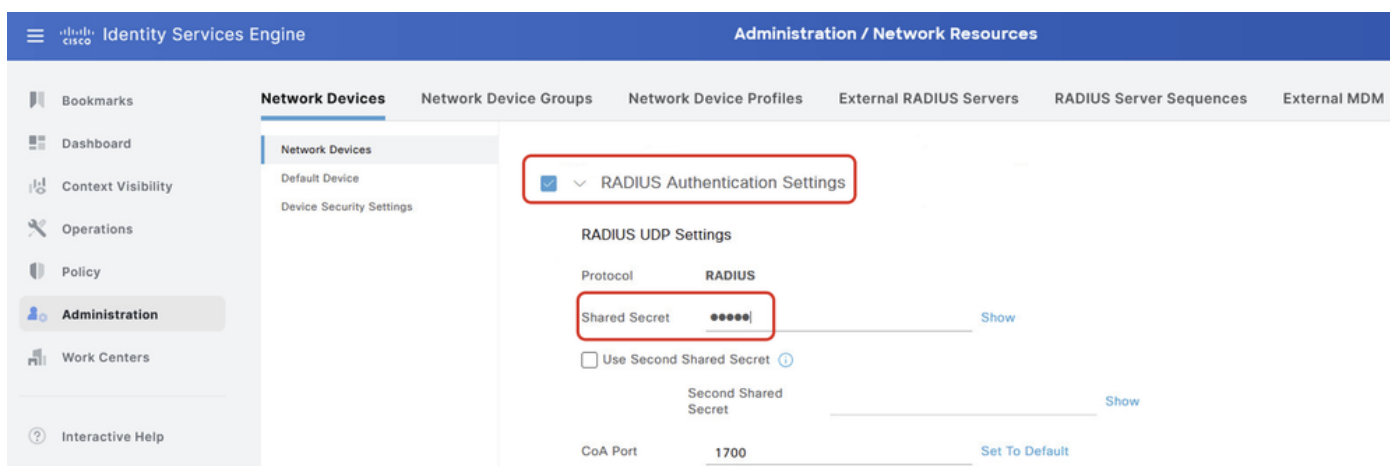
步骤12.创建网络设备。

第12.1步：导航到Administration > Network Resources > Network Devices，点击Add，提供Name，IP Address，然后向下滚动页面。



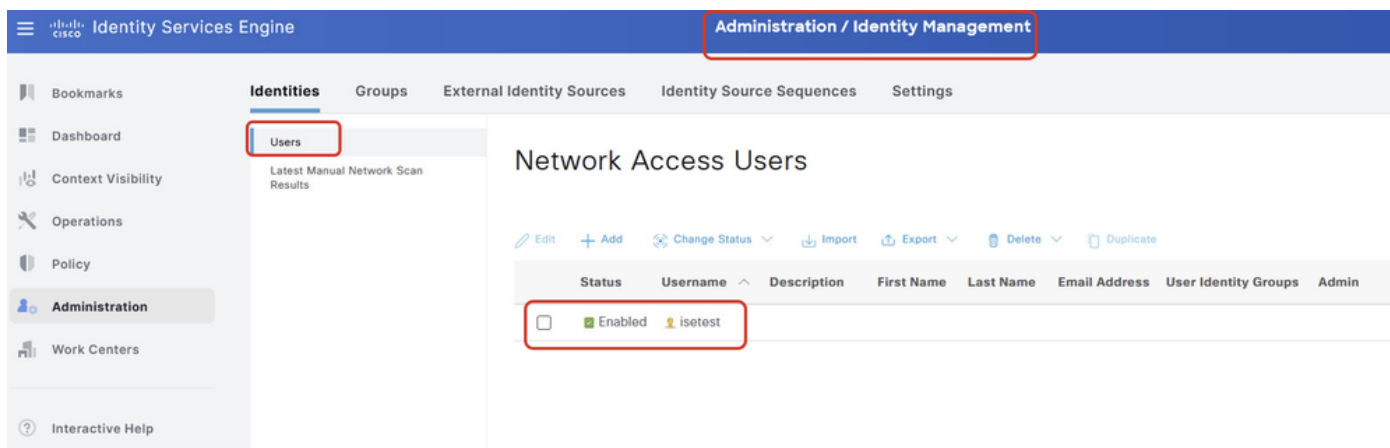
创建_网络设备

步骤12.2.选中RADIUS Authentication Settings复选框。提供Shared Secret，然后单击Submit。



Create_Network_Devices_Cont

步骤13.创建网络访问用户。导航到Administration > Identity Management > Identities。单击Add以创建新用户。密码与在步骤10中创建的FDM本地用户相同。以确保回退生效。



Create_ISE_User

步骤14. (可选) 使用自定义身份验证规则和授权规则创建新策略集。在本示例中，默认策略集用于演示目的。

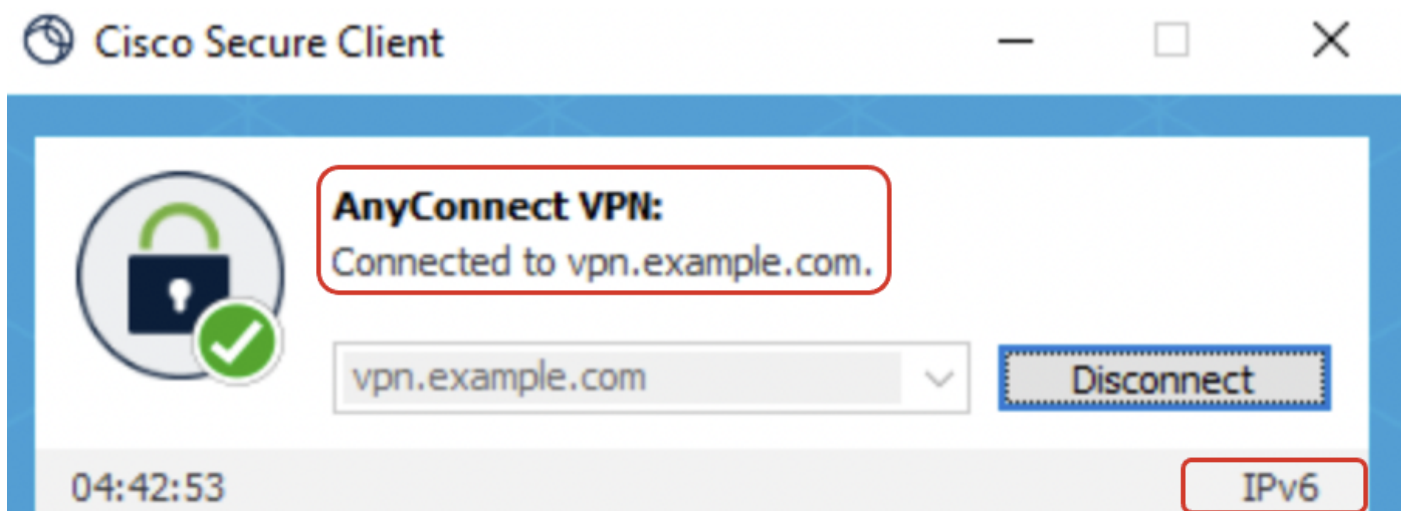
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	SPRT		Radius-NAS-IP-Address EQUALS 10.48.26.61	Default Network Access	0		
●	Wired		DEVICE-Device Type EQUALS All Device Types#Switch	Default Network Access	0		
●	Firewall No Posture		DEVICE-Device Type EQUALS All Device Types#Firewall_NoPosture	Default Network Access	0		
●	Firewall Posture		DEVICE-Device Type EQUALS All Device Types#Firewall	Default Network Access	0		
●	Default	Default policy set		Default Network Access	78		

ISE_Default_Policy_Set

验证

使用本部分可确认配置能否正常运行。

步骤15.通过客户端上的IPv6地址连接VPN网关。VPN连接成功。



Verify_Connection_Success

步骤16.通过SSH或控制台导航到FTD的CLI。在FTD(Lina)CLI中运行命令show vpn-sessiondb detail anyconnect，以检查VPN会话详细信息。

```
<#root>
```

```
ftdv760# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : isetest
```

```
Index : 2
```

```
Assigned IP : 10.37.254.17
```

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 15402 Bytes Rx : 14883
Pkts Tx : 10 Pkts Rx : 78
Pkts Tx Drop : 0 Pkts Rx Drop : 10
Group Policy : demo_gp Tunnel Group : demo_ravpn
Login Time : 05:22:30 UTC Mon Dec 23 2024
Duration : 0h:05m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a81e0a000020006768f396
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 : 2001:db8:10:0:a8a5:6647:b275:acc2

Encryption : none Hashing : none
TCP Src Port : 58339 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes
Client OS : win
Client OS Ver: 10.0.19042
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 2.2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 58352
TCP Dst Port : 443 Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 25 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 152
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 2.3

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 58191
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 560 Bytes Rx : 14731
Pkts Tx : 8 Pkts Rx : 76
Pkts Tx Drop : 0 Pkts Rx Drop : 10

步骤17.在客户端上执行ping测试。在本示例中，客户端成功ping服务器的IPv4和IPv6地址。

Command Prompt

```
C:\Users\admin>
C:\Users\admin>ping 2001:db8:50::20

Pinging 2001:db8:50::20 with 32 bytes of data:
Request timed out.
Reply from 2001:db8:50::20: time=4ms
Reply from 2001:db8:50::20: time=4ms
Reply from 2001:db8:50::20: time=3ms

Ping statistics for 2001:db8:50::20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Select Command Prompt

```
C:\Users\admin>
C:\Users\admin>ping 192.168.50.20

Pinging 192.168.50.20 with 32 bytes of data:
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.50.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Verify_Cisco_Secure_Client_Ping

步骤18. ISE radius实时日志显示身份验证成功。

Overview

Event	5200 Authentication succeeded
Username	isetest
Endpoint Id	52:54:00:16:12:64 ⓘ
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-12-09 10:56:38.389
Received Timestamp	2024-12-09 10:56:38.389
Policy Server	cmlise-psn
Event	5200 Authentication succeeded
Username	isetest
User Type	User
Endpoint Id	52:54:00:16:12:64
Calling Station Id	192.168.10.1
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users

ISE_Authentication_Sucess_Log

步骤19.当FTD无法到达ISE时，测试FTD身份验证转为本地。

第19.1步：当FTD身份验证转至ISE时，在FTD(Lina)CLI中运行命令show aaa-server以检查统计信息。

在本示例中，没有LOCAL计数器，并且身份验证定向到RADIUS服务器。

<#root>

ftdv760# show aaa-server

Server Group: LOCAL
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 08:18:11 UTC Fri Dec 6 2024
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 0
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
Number of rejects 0
Number of challenges 0
Number of bad authenticators 0
Number of timeouts 0
Number of unrecognized responses 0
Server Group: demo_ise_group
Server Protocol: radius

Server Address: 2001:db8:2139::240

Server port: 1812(authentication), 1646(accounting)
Server status: ACTIVE, Last transaction at 02:56:41 UTC Mon Dec 9 2024
Number of pending requests 0
Average round trip time 100ms

Number of authentication requests 1 <== Increased

Number of authorization requests 1 <== Increased

Number of accounting requests 1 <== Increased

Number of retransmissions 0

Number of accepts 2 <== Increased

Number of rejects 0
Number of challenges 0
Number of bad authenticators 0
Number of timeouts 0
Number of unrecognized responses 0

步骤19.2.关闭ISE接口以模拟FTD无法从ISE接收任何响应。

<#root>

```
ftdv760# ping 2001:db8:2139::240
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:db8:2139::240, timeout is 2 seconds:

???

Success rate is 0 percent (0/3)

步骤19.3.客户端启动VPN连接并输入在步骤10中创建的相同用户名密码，VPN连接仍然成功。

再次在FTD(Lina)CLI中运行命令show aaa-server，以检查统计信息，LOCAL的身份验证、授权和接受计数器现已增加。RADIUS服务器的接受计数器没有增加。

<#root>

```
ftdv760# show aaa-server
```

Server Group: LOCAL

Server Protocol: Local database

Server Address: None

Server port: None

Server status: ACTIVE, Last transaction at 03:36:26 UTC Mon Dec 9 2024

Number of pending requests 0

Average round trip time 0ms

Number of authentication requests 1 <== Increased

Number of authorization requests 1 <== Increased

Number of accounting requests 0

Number of retransmissions 0

Number of accepts 2 <== Increased

Number of rejects 0

Number of challenges 0

Number of bad authenticators 0

Number of timeouts 0

Number of unrecognized responses 0

Server Group: demo_ise_group

Server Protocol: radius

Server Address: 2001:db8:2139::240

Server port: 1812(authentication), 1646(accounting)

Server status: ACTIVE, Last transaction at 03:36:41 UTC Mon Dec 9 2024

Number of pending requests 0

Average round trip time 100ms

Number of authentication requests 2

Number of authorization requests 1

Number of accounting requests 6

Number of retransmissions 0

Number of accepts	2 <== Not increased
Number of rejects	0
Number of challenges	0
Number of bad authenticators	0
Number of timeouts	6
Number of unrecognized responses	0

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。

可以在FTD Lina上运行这些命令以对VPN部分进行故障排除。

```
debug webvpn 255
debug webvpn anyconnect 255
```

您可以从客户端收集DART文件以进行VPN故障排除，以确定问题是否出在安全客户端上。有关指南，请参阅相关的CCO文档[收集安全客户端的DART捆绑包](#)。

可以在FTD Lina上运行这些命令以对Radius部分进行故障排除。

```
ftdv760# debug radius ?

all          All debug options
decode       Decode debug option
dynamic-authorization CoA listener debug option
session      Session debug option
user         User debug option
<cr>
```

```
ftdv760# debug aaa ?
```

```
accounting
authentication
authorization
common
condition
internal
shim
url-redirect
<cr>
```

您可以查看这些信息，以便对VPN连接成功后的流量相关问题进行故障排除。

1. 在FTD Lina上捕获流量，以查看Lina是否丢弃流量（请参阅此CCO文档）；使用[Firepower威胁防御捕获和Packet Tracer - Cisco](#)。
2. 检查访问控制策略，以确保如果禁用了解密流量的旁路访问控制策略，则允许相关VPN流量通过。
3. 检查NAT免除以确保从NAT中排除VPN流量。

相关信息

- [RAVPN的FDM配置指南 — 思科](#)
- [收集安全客户端的DART捆绑包 — 思科](#)
- [使用Firepower威胁防御捕获和Packet Tracer — 思科](#)
- [Cisco安全客户端故障排除 — Cisco](#)
- [思科技术支持和下载](#)

关于此翻译

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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