

Configurar o RAVPN habilitado para IPv6 com autenticação AAA no FTD Gerenciado pelo FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações no FDM](#)

[Configurações no ISE](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas para configurar a VPN de acesso remoto habilitada para IPv6 com autenticação AAA no FTD gerenciado pelo FDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firepower Device Manager (FDM) Virtual
- Cisco Secure Firewall Threat Defense (FTD) Virtual
- Fluxo de autenticação de VPN

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure FDM Virtual 7.6.0
- Cisco Secure FTD Virtual 7.6.0
- Cisco Secure Client 5.1.6.103

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

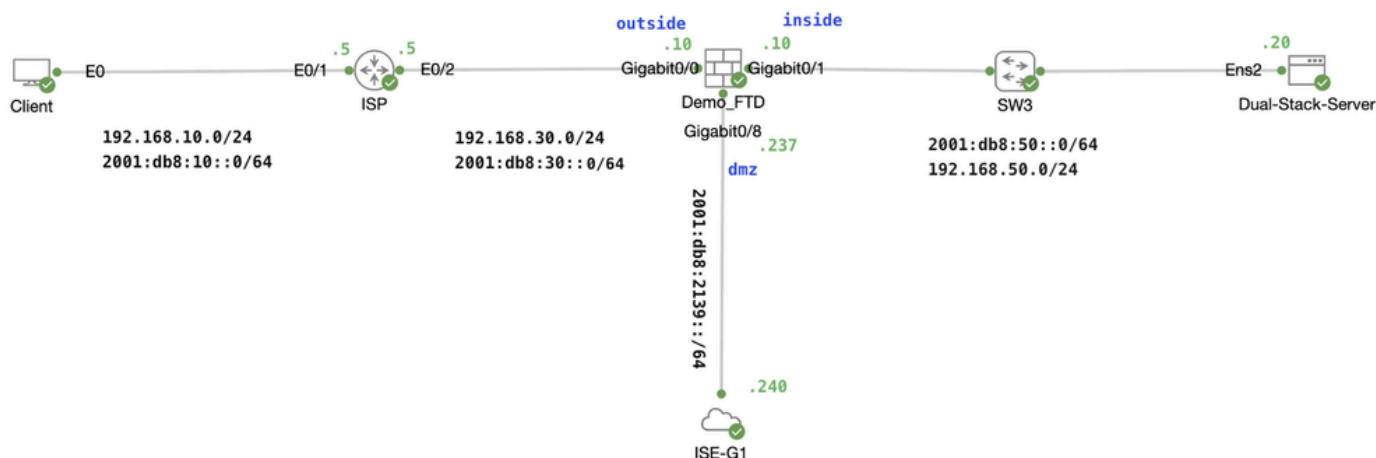
Informações de Apoio

A VPN de acesso remoto IPv6 (RAVPN) está se tornando cada vez mais importante à medida que o mundo faz transições de IPv4 para IPv6, já que os endereços IPv4 são limitados e foram quase esgotados, enquanto o IPv6 oferece um espaço de endereço praticamente ilimitado, acomodando o número crescente de dispositivos conectados à Internet. À medida que mais redes e serviços se movem para IPv6, ter o recurso IPv6 garante que sua rede permaneça compatível e acessível. O IPv6 RAVPN ajuda as organizações a se prepararem para o futuro da rede, garantindo conectividade remota segura e escalável.

Neste exemplo, o cliente se comunica com o gateway VPN usando um endereço IPv6 fornecido pelo provedor de serviços, mas recebe endereços IPv4 e IPv6 dos pools VPN, utilizando o Cisco Identity Service Engine (ISE) como origem de identidade de autenticação. O ISE é configurado apenas com o endereço IPv6. O servidor interno é configurado com endereços IPv4 e IPv6, representando hosts de pilha dupla. O cliente pode acessar recursos internos usando o endereço VPN IPv4 ou IPv6, conforme apropriado.

Configurar

Diagrama de Rede



Topologia

Configurações no FDM

Etapa 1. É essencial garantir que a configuração preliminar da interconexão IPv4 e IPv6 entre os nós tenha sido devidamente concluída. O gateway do Cliente e do FTD é o endereço do ISP relacionado. O gateway do servidor está dentro do IP do FTD. O ISE está localizado na área DMZ do FTD.

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

Static Routing BGP OSPF EIGRP ECMP Traffic Zones

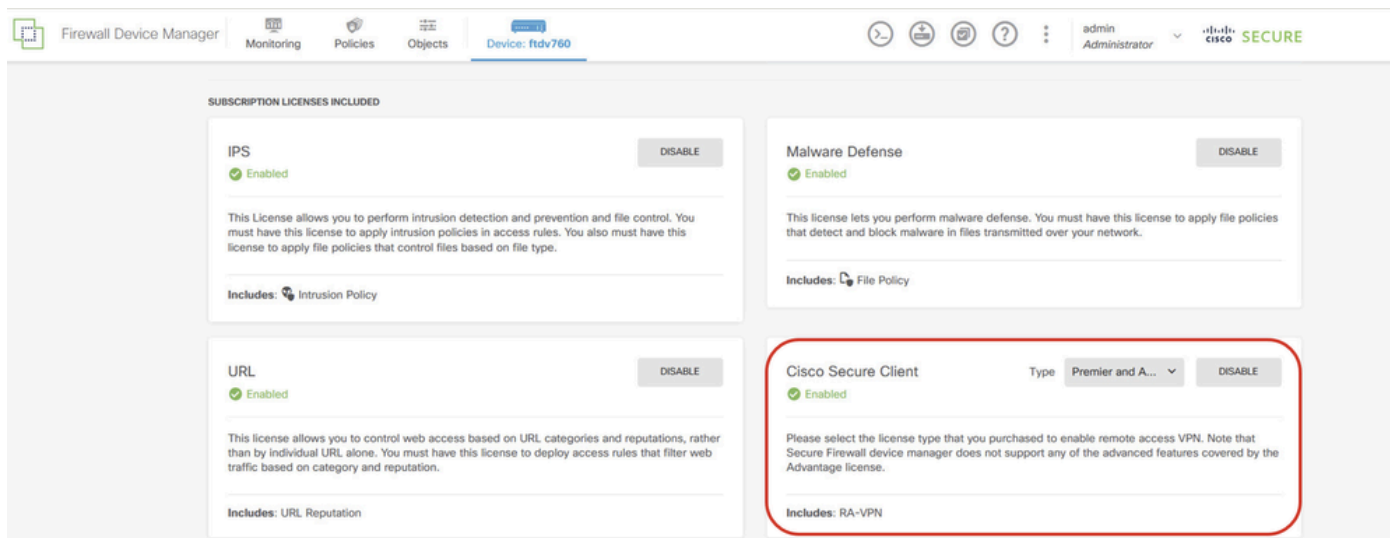
2 routes

#	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

Etapa 2. Faça o download do pacote Cisco Secure Client name `cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg` em [Cisco Software Download](#) e certifique-se de que o arquivo esteja bom após o download confirmando que a soma de verificação md5 do arquivo baixado é a mesma que a página Download do Software Cisco.

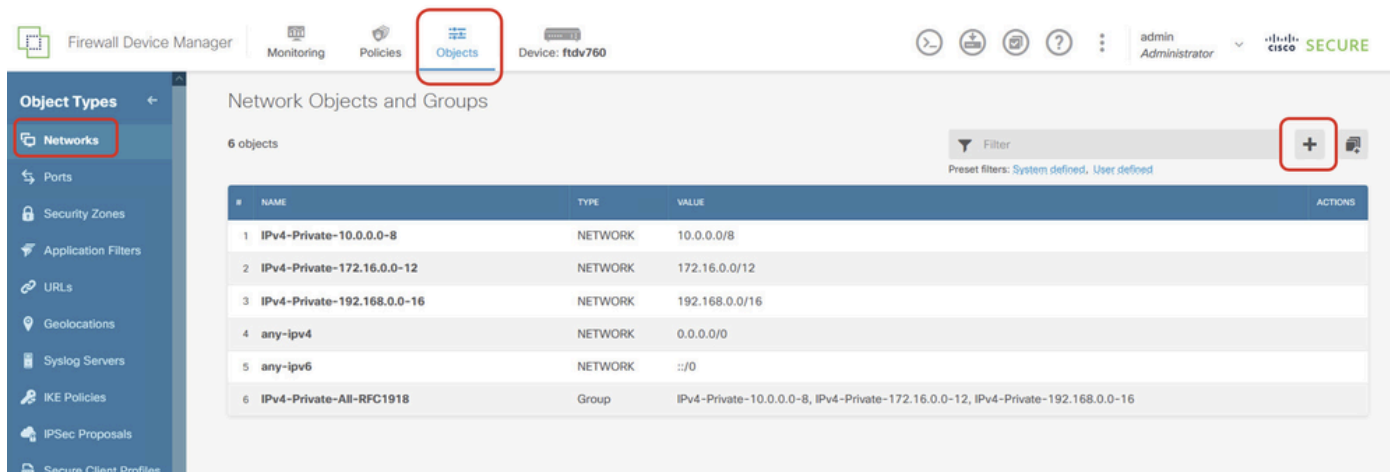
Etapa 3. Verificar se as licenças relacionadas a RAVPN estão habilitadas no FTD.



Licença_FDM

Etapa 4. Criar um pool de endereços VPN.

Etapa 4.1. Crie um pool de endereços IPv6 e IPv4 criando objetos de rede. Navegue até Objetos > Redes e clique no botão +.



Create_VPN_Address_Pool_1

Etapa 4.2. Forneça as informações necessárias de cada objeto de rede. Clique no botão OK.

Para o pool IPv4, o tipo de objeto pode ser escolhido com Rede ou Intervalo. Neste exemplo, o tipo de objeto Rede é escolhido para fins de demonstração.

- Nome: demo_ipv4pool
- Digite: Rede
- Rede: 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

Para o pool IPv6, o tipo de objeto só pode ser escolhido com Rede a partir de agora.

- Nome: demo_ipv6pool
- Digite: Rede
- Rede: 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

Etapa 5. Crie a rede interna para isento de NAT.

Etapa 5.1. Navegue até Objetos > Redes e clique no botão +.

Firewall Device Manager

Monitoring Policies **Objects** Device: ftdv760

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	

Etapa 5.2. Forneça as informações necessárias de cada objeto de rede. Clique na tecla OK.

Neste exemplo, as redes IPv4 e IPv6 são configuradas.

- Nome: inside_net_ipv4
- Digite: Rede
- Rede: 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

- Nome: inside_net_ipv6
- Digite: Rede
- Rede: 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

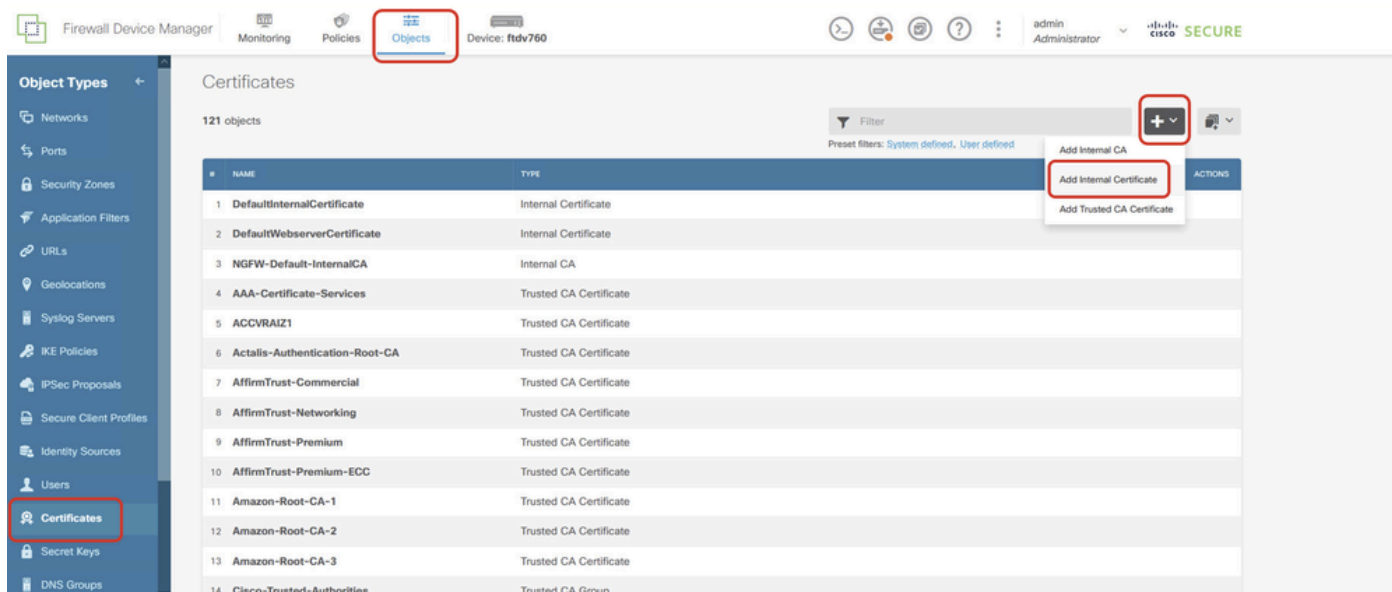
OK

Create_NAT_Exempt_Network_2_IPv6

Etapa 6. Criar o certificado usado para RAVPN. Você tem duas opções: você pode carregar um certificado assinado por uma autoridade de certificação (CA) de terceiros ou gerar um novo certificado autoassinado.

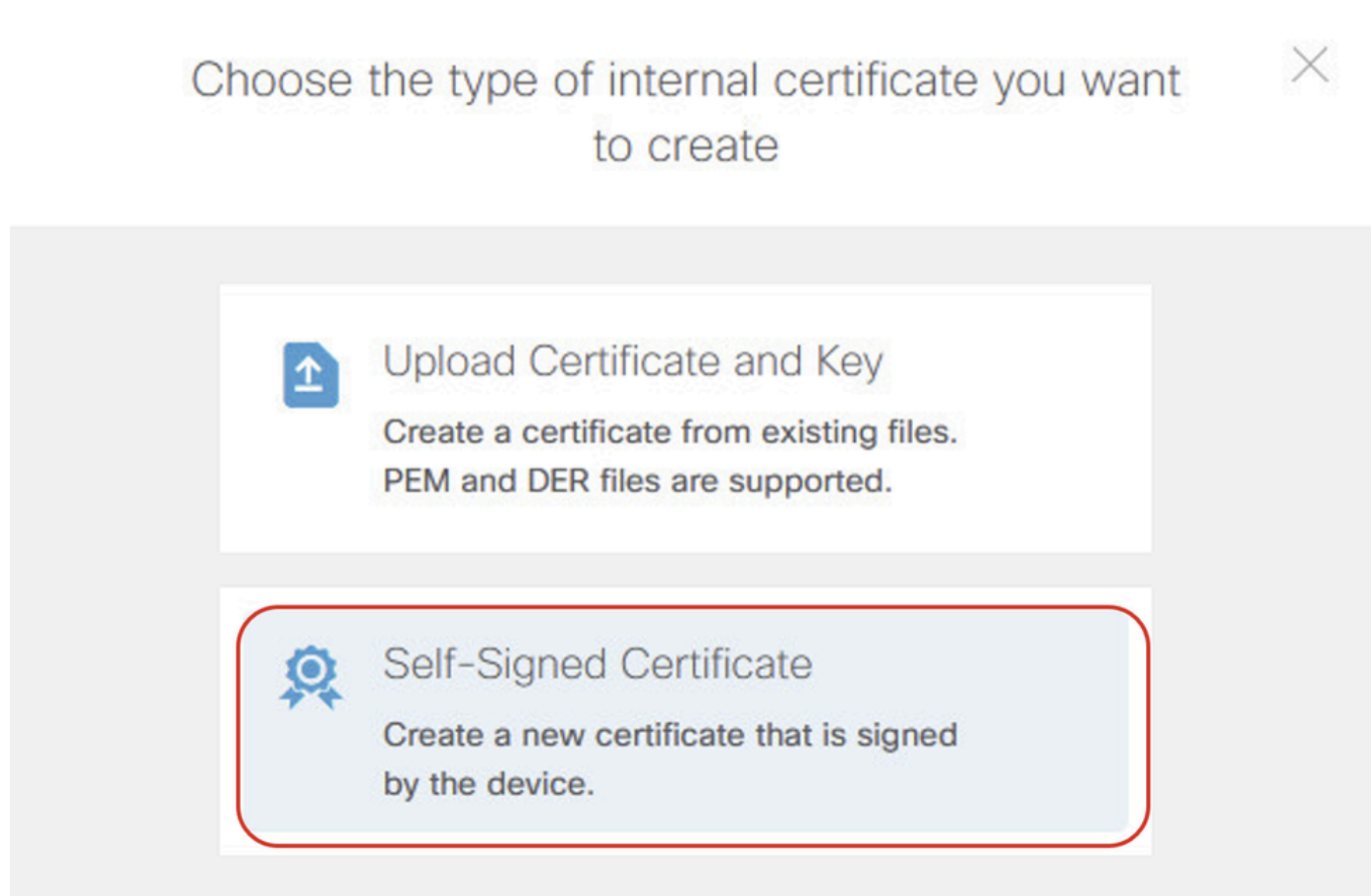
Neste exemplo, um novo certificado autoassinado é usado com conteúdo personalizado do certificado para fins de demonstração.

Etapa 6.1. Navegue até Objetos > Certificados. Clique no botão + e escolha Adicionar certificado interno.



Criar_Certificado_1

Etapa 6.2. Clique em Certificado Autoassinado.



Etapa 6.3. Clique na guia Geral e forneça as informações necessárias.

Nome: demovpn

Tipo de chave: RSA

Tamanho da chave: 2048

Período de validade: Padrão

Data de vencimento: Padrão

Uso da validação para serviços especiais: Servidor SSL

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

Criar_Certificado_3

Etapa 6.4. Clique na guia Emissor e forneça as informações necessárias.

País: Estados Unidos (EUA)

Nome comum: 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

Criar_Certificado_4

Etapa 6.5. Clique na guia Assunto, forneça as informações necessárias e clique em SALVAR.

País: Estados Unidos (EUA)

Nome comum: 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.

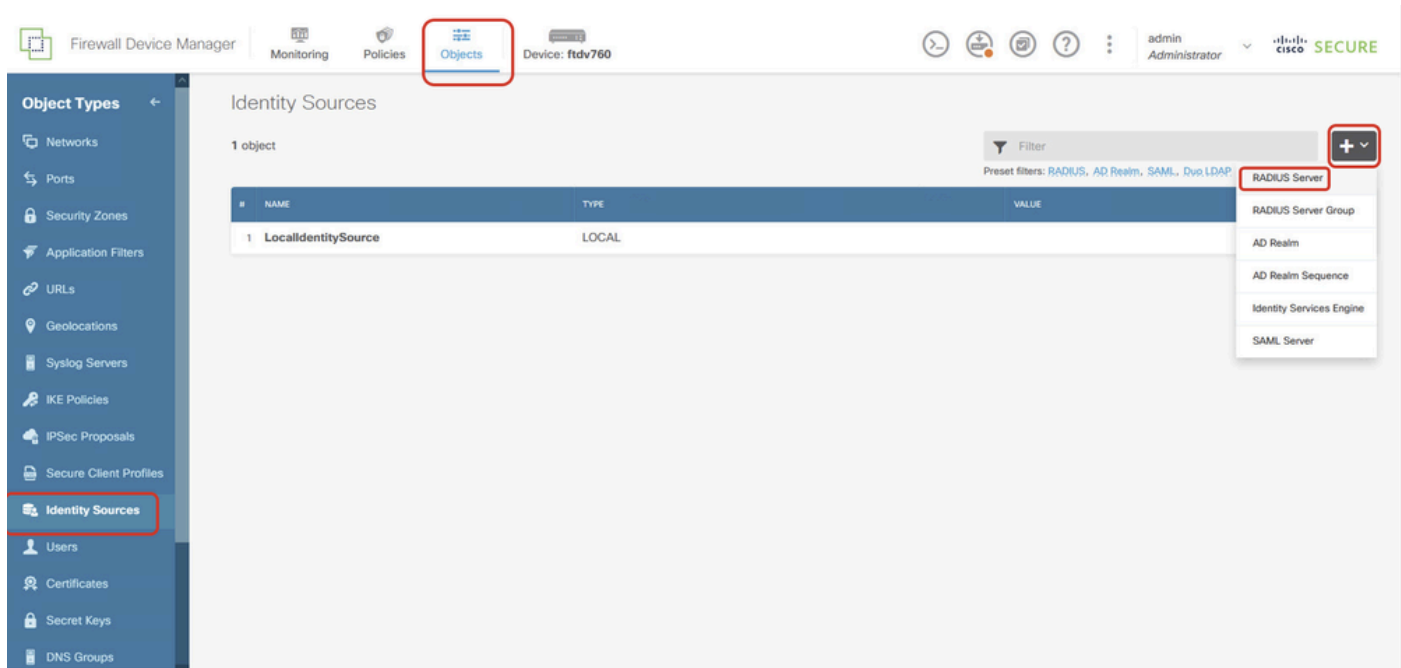
CANCEL

SAVE

Criar_Certificado_5

Etapa 7. Criar a origem da identidade do servidor radius.

Etapa 7.1. Navegue atéObjetos > Fontes de identidade, clique no botão + e escolhaServidor RADIUS.



Create_Radius_Source_1

Etapa 7.2. Forneça as informações necessárias do servidor radius. Clique no botão OK.

Nome: demo_ise

Nome do servidor ou endereço IP: 2001:db8:2139::240

Porta de autenticação: 1812 (padrão)

tempo limite: 10 (padrão)

Chave Secreta do Servidor: cisco

Interface usada para conexão com o servidor Radius: Escolha manualmente a interface. Neste exemplo, escolha 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

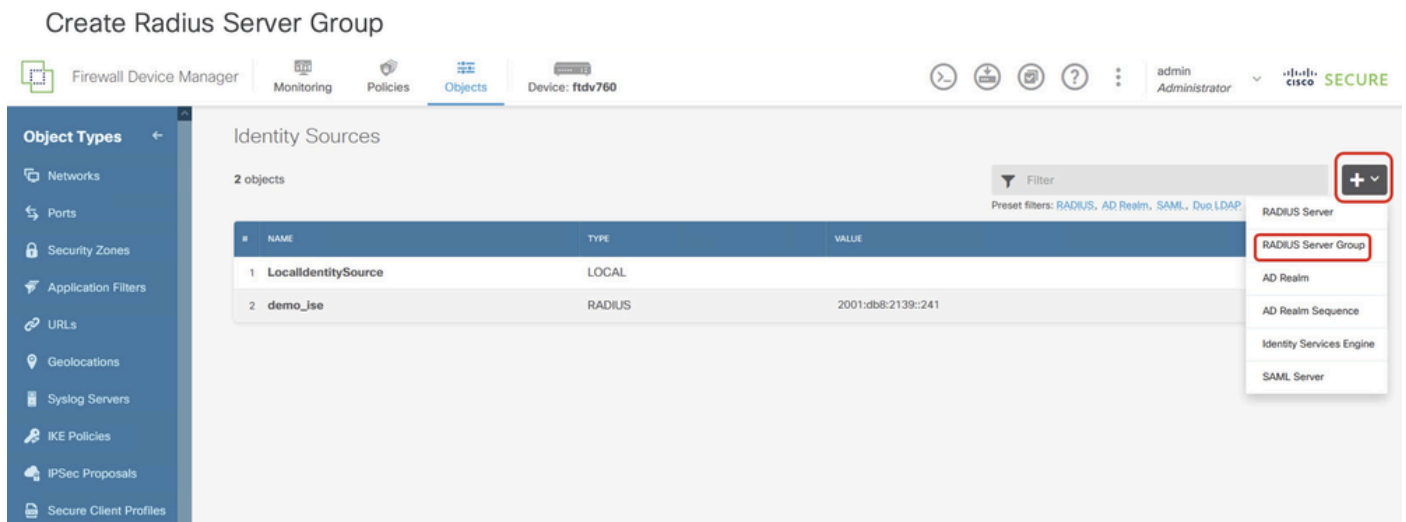
dmz (GigabitEthernet0/8)

CANCEL

OK

Create_Radius_Source_2

Etapa 7.3. Navegue até **Objetos > Fontes de identidade**. Clique no botão **+** e escolha **Grupo de servidores RADIUS**.



Create_Radius_Source_3

Etapa 7.4. Forneça as informações necessárias do grupo de servidores radius. Clique na tecla OK.

Nome: demo_ise_group

Tempo de inoperância: 10 (padrão)

Máximo de Tentativas com Falha: 3 (padrão)

Servidor RADIUS: Clique no botão +, selecione o nome criado na Etapa 6.2. Neste exemplo, é 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

Etapa 8. Criar a política de grupo usada para RAVPN. Neste exemplo, a configuração personalizada do banner e do tempo limite é configurada para fins de demonstração. Você pode modificar com base na sua necessidade real.

Etapa 8.1. Navegue até Remote Access VPN > View Configuration. Clique em Group Policies na barra lateral esquerda e, em seguida, clique no botão +.



Create_Group_Policy_1

Etapa 8.2. Clique em Geral e forneça as informações necessárias.

Nome: demo_gp

Texto do banner para clientes autenticados: banner de demonstração

The screenshot shows the 'Add Group Policy' dialog box. The 'General' tab is selected. The 'Name' field is filled with 'demo_gp'. The 'Banner Text for Authenticated Clients' field is filled with 'demo banner|'. The 'Description' field is empty. The 'DNS Server' dropdown is set to 'Select DNS Group'. The 'Default domain' field is empty. The 'Secure Client profiles' field is empty. The 'OK' button is highlighted.

Create_Group_Policy_2

Etapa 8.3. Clique em Secure Client e forneça as informações necessárias.

Marque Habilitar DTLS (Datagram Transport Layer Security).

The image shows a configuration window for a 'Secure Client'. On the left is a sidebar with a search bar and a list of categories: 'Basic' (General, Session Settings) and 'Advanced' (Address Assignment, Split Tunneling, 'Secure Client', Traffic Filters, Windows Browser Proxy). The 'Secure Client' option is highlighted with a blue bar and a red rectangle. The main area is titled 'SSL SETTINGS' and contains the following options: 'Enable Datagram Transport Layer Security (DTLS)' (checked, highlighted with a red rectangle), 'DTLS Compression' (unchecked), 'SSL Compression' (set to 'Disabled'), 'SSL Rekey Method' (set to 'None'), and 'SSL Rekey Interval' (set to '4' minutes, with a range of '4 ~ 10080' shown below). Below these is the 'CONNECTION SETTINGS' section with 'Ignore the DF (Don't Fragment) bit' (unchecked) and 'Client Bypass Protocol' (unchecked). At the bottom is an 'MTU' field. At the bottom right are 'CANCEL' and 'OK' buttons.

Create_Group_Policy_3

Verifique as mensagens de manutenção de atividade entre o cliente seguro e o gateway VPN (valor padrão).

Verifique o DPD em Gateway Side Interval (valor padrão).

Verifique o DPD em Client Side Interval (valor padrão).

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

Etapa 9. Criar o perfil de conexão RAVPN.

Etapa 9.1. Navegue para VPN de acesso remoto > Exibir configuração. Clique em Connection Profile na barra lateral esquerda e clique no botão + para iniciar o assistente.

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

Etapa 9.2. Forneça as informações necessárias na seção Conexão e Configuração do Cliente e clique no botão NEXT.

Nome do perfil de conexão: demo_ravpn

Alias do grupo: 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

Origem da identidade principal > Tipo de autenticação: Somente AAA

Origem da Identidade Principal > Origem da Identidade Principal: demo_ise_group (o nome configurado na Etapa 7.4.)

Fonte de identidade local de fallback: LocalIdentitySource

Servidor de autorização: demo_ise_group (o nome configurado na Etapa 7.4.)

Servidor de contabilidade: demo_ise_group (o nome configurado na Etapa 7.4.)

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

Pool de Endereços IPv4: demo_ipv4pool (o nome configurado na Etapa 4.2.)

Pool de Endereços IPv6: demo_ipv6pool (o nome configurado na Etapa 4.2.)

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

Etapa 9.3. Escolha a política de grupo configurada na Etapa 8.2. na seção Experiência do usuário remoto e clique no botão NEXT.

Firewall Device Manager

Monitoring

Policies

Objects

Device: ftdv760

admin Administrator

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 Server

None

Banner Text for Authenticated Clients

demo banner - fdm

SESSION SETTINGS

Maximum Connection Time / Alert Interval

Unlimited / 1 Minutes

Idle Time / Alert Interval

30 / 1 Minutes

Simultaneous Login per User

3

BACK

NEXT

Create_RAVPN_Wizard_3

Etapa 9.4. Forneça as informações necessárias na seção Configuração Global e clique no botão NEXT.

Certificado de identidade do dispositivo: demovpn (o nome configurado na Etapa 6.3.)

Interface externa: externa

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

Controle de acesso para tráfego VPN: Verifique a política Bypass Access Control para tráfego descriptografado (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

Isento de NAT: Clique no controle deslizante para a posição Habilitado

Interfaces internas: interna

Redes internas: inside_net_ipv4, inside_net_ipv6 (o nome configurado na Etapa 5.2.)

NAT Exempt



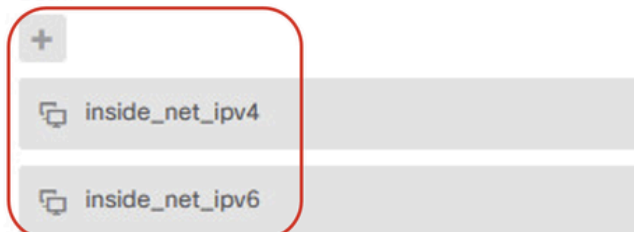
Inside Interfaces

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

Pacote de cliente seguro: Clique em **CARREGAR PACOTE** e carregue o pacote de acordo. Neste exemplo, o pacote do Windows é carregado.

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



 **Windows:** cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg

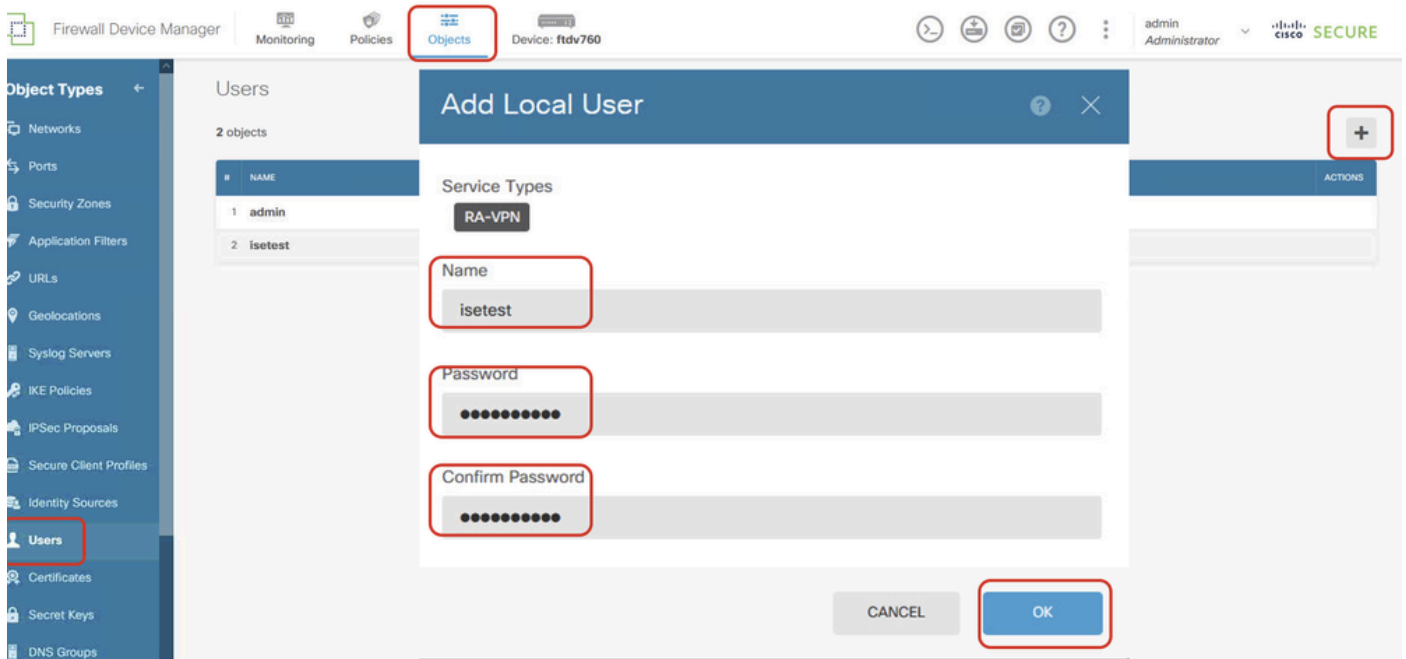
BACK

NEXT

Create_RAVPN_Wizard_4_Image

Etapa 9.5. Revise o resumo. Se algo precisar ser modificado, clique no botão BACK. Se tudo estiver bem, clique no botão FINISH.

Etapa 10. Crie um usuário local se a Origem da Identidade Local de Fallback for escolhida com LocalIdentitySource na Etapa 9.2. A senha do usuário local precisa ser igual à configurada no ISE.



Criar_Usuário_Local

Etapa 11. Implantar as alterações de configuração.



Implantar_alterações

Configurações no ISE

Etapa 12. Criar dispositivos de rede.

Etapa 12.1. Navegue até Administration > Network Resources > Network Devices, clique em Add, forneça o Name, IP Address e role para baixo na página.

Identity Services Engine Administration / Network Resources

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

Network Devices List > New Network Device

Network Devices

Name

Description

IP Address Port

Create_Network_Devices

Etapa 12.2. Marque a caixa de seleção RADIUS Authentication Settings. Forneça o segredo compartilhado e clique em Enviar.

Identity Services Engine Administration / Network Resources

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

Network Devices

Default Device Device Security Settings

☒ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret Show

☐ Use Second Shared Secret ⓘ

Second Shared Secret Show

CoA Port Set To Default

Create_Network_Devices_Cont

Etapa 13. Criar usuários de acesso à rede. Navegue até Administração > Gerenciamento de identidades > Identidades. Clique em Add para criar um novo usuário. A senha é a mesma do usuário local do FDM criado na Etapa 10. para garantir que o fallback funcione.

Identity Services Engine Administration / Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users

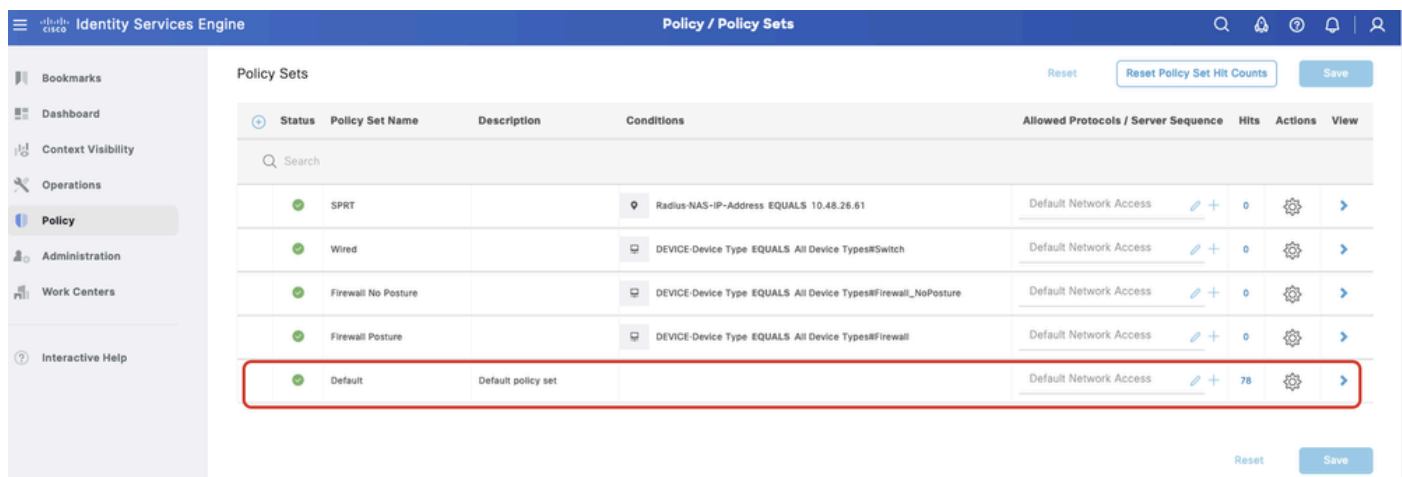
Edit Add Change Status Import Export Delete Duplicate

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input checked="" type="checkbox"/> Enabled	isetest						

Create_ISE_User

Etapa 14. (Opcional) Crie um novo conjunto de políticas com a regra de autenticação

personalizada e a regra de autorização. Neste exemplo, o conjunto de políticas padrão é usado para fins de demonstração.



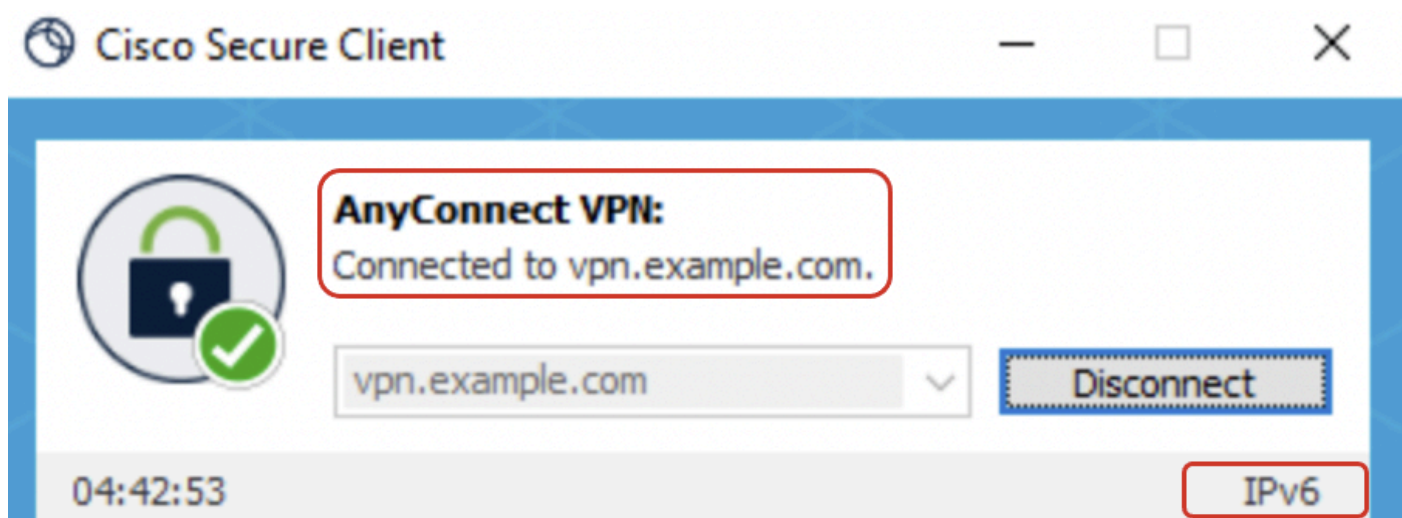
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	SPRT		Radius-NAS-IP-Address EQUALS 10.48.26.61	Default Network Access	0		
✓	Wired		DEVICE-Device Type EQUALS All Device Types#Switch	Default Network Access	0		
✓	Firewall No Posture		DEVICE-Device Type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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 15. Conectar o gateway VPN através do endereço IPv6 no cliente. Conexão VPN bem-sucedida.



Verify_Connection_Successful

Etapa 16. Navegue até a CLI do FTD via SSH ou console. Execute o comando show vpn-sessiondb detail anyconnect na CLI do FTD (Lina) para verificar os detalhes da sessão VPN.

<#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

Etapa 17. Teste de ping no Cliente. Neste exemplo, o cliente efetua ping com êxito nos endereços IPv4 e IPv6 do servidor.

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

Etapa 18. O registro ao vivo do ISE radius mostra uma autenticação bem-sucedida.

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_Success_Log

Etapa 19. A autenticação do FTD de teste vai para o LOCAL quando o FTD não pode acessar o

ISE.

Etapa 19.1. Quando a autenticação do FTD for para o ISE, execute o comando show aaa-server na CLI do FTD (Lina) para verificar as estatísticas.

Neste exemplo, não há contadores para LOCAL e a autenticação é direcionada para o servidor RADIUS.

<#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

Etapa 19.2. Desative a interface do ISE para simular que o FTD não pode receber nenhuma resposta do ISE.

<#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)

Etapa 19.3. O cliente inicia a conexão VPN e insere o mesmo nome de usuário e senha criados na Etapa 10; a conexão VPN ainda é bem-sucedida.

Execute o comando show aaa-server na CLI do FTD (Lina) novamente para verificar a estatística, a autenticação, a autorização e os contadores de aceitação para LOCAL aumentaram. O contador de aceitação do servidor RADIUS não aumentou.

<#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

```

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Você pode executar esses comandos no FTD Lina para solucionar problemas da seção VPN.

```

debug webvpn 255
debug webvpn anyconnect 255

```

Você pode coletar um arquivo DART do cliente para a solução de problemas de VPN para determinar se o problema está no Secure Client. Para obter orientação, consulte o documento CCO relevante [Collect DART Bundle for Secure Client](#).

Você pode executar esses comandos no FTD Lina para solucionar problemas da seção Radius.

```

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>
```

Você pode revisá-los para resolver o problema relacionado ao tráfego após a conexão VPN com êxito.

1. Capture o tráfego no FTD Lina para ver se Lina abandona o tráfego, consultando este documento do CCO; [Use as capturas do Firepower Threat Defense e o Packet Tracer - Cisco](#).
2. Revise a política de controle de acesso para garantir que o tráfego de VPN relacionado tenha permissão para passar se a política Ignorar Controle de Acesso para tráfego descriptografado estiver desabilitada.
3. Revise a isenção de NAT para garantir que o tráfego VPN seja excluído do NAT.

Informações Relacionadas

- [Guia de Configuração do FDM de RAVPN - Cisco](#)
- [Coletar pacote DART para cliente seguro - Cisco](#)
- [Use as capturas do Firepower Threat Defense e o Packet Tracer - Cisco](#)
- [Solução de problemas do Cisco Secure Client - Cisco](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.