

# Configuración de RAVPN habilitado para IPv6 con autenticación AAA en FTD administrado por FDM

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones en FDM](#)

[Configuraciones en ISE](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe los pasos para configurar VPN de acceso remoto habilitada para IPv6 con autenticación AAA en FTD administrado por FDM.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firepower Device Manager (FDM) Virtual
- Cisco Secure Firewall Threat Defence (FTD) Virtual
- Flujo de autenticación VPN

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure FDM Virtual 7.6.0
- Cisco Secure FTD Virtual 7.6.0

- Cisco Secure Client 5.1.6.103

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

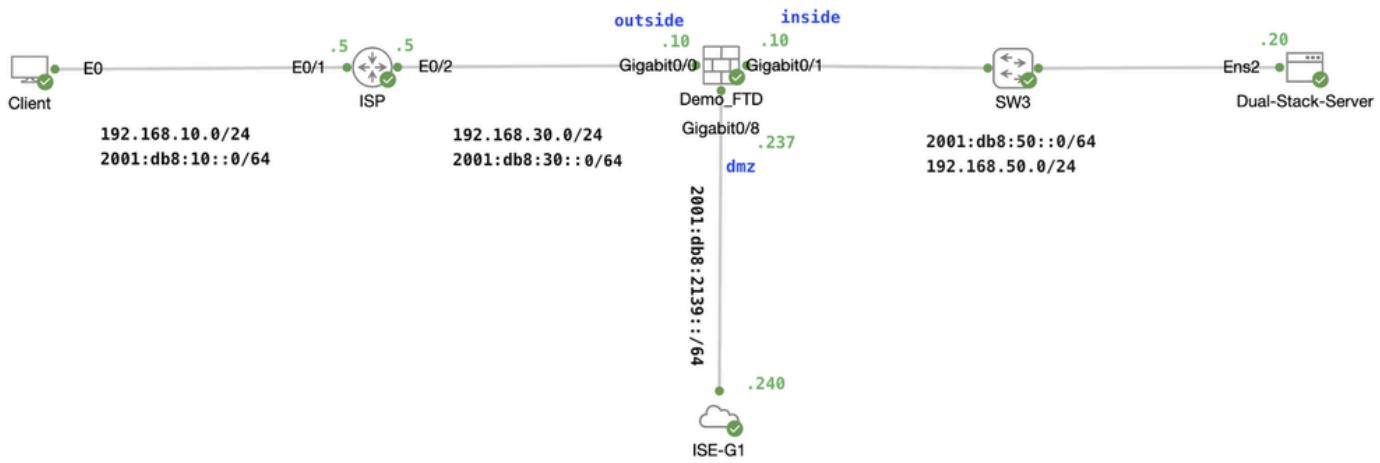
## Antecedentes

La VPN de acceso remoto IPv6 (RAVPN) es cada vez más importante a medida que el mundo pasa de IPv4 a IPv6, ya que las direcciones IPv4 son limitadas y casi se han agotado, mientras que IPv6 ofrece un espacio de direcciones prácticamente ilimitado, que se adapta al creciente número de dispositivos conectados a Internet. A medida que más redes y servicios pasan a IPv6, disponer de capacidad IPv6 garantiza que su red siga siendo compatible y accesible. RAVPN IPv6 ayuda a las organizaciones a prepararse para el futuro de las redes, lo que garantiza una conectividad remota segura y escalable.

En este ejemplo, el cliente se comunica con el gateway VPN mediante una dirección IPv6 proporcionada por el proveedor de servicios, pero recibe las direcciones IPv4 e IPv6 de los grupos VPN, utilizando Cisco Identity Service Engine (ISE) como fuente de identidad de autenticación. ISE se configura solo con direcciones IPv6. El servidor interno se configura con direcciones IPv4 e IPv6, que representan hosts de pila doble. El cliente puede acceder a los recursos internos mediante la dirección VPN IPv4 o IPv6, según corresponda.

## Configurar

### Diagrama de la red



Topología

### Configuraciones en FDM

Paso 1. Es esencial garantizar que la configuración preliminar de la interconexión IPv4 e IPv6

entre nodos se haya completado debidamente. La puerta de enlace del cliente y FTD es la dirección ISP relacionada. El gateway del servidor está dentro de la IP del FTD. ISE se encuentra en el área DMZ del FTD.

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
>  GigabitEthernet0/0	outside	<input checked="" type="checkbox"/>	Routed	192.168.30.10 2001:db8:30::10/64		Enabled	
>  GigabitEthernet0/1	inside	<input checked="" type="checkbox"/>	Routed	192.168.50.10 2001:db8:50::10/64		Enabled	
>  GigabitEthernet0/2		<input type="checkbox"/>	Routed			Enabled	
>  GigabitEthernet0/3		<input type="checkbox"/>	Routed			Enabled	
>  GigabitEthernet0/4		<input type="checkbox"/>	Routed			Enabled	
>  GigabitEthernet0/5		<input type="checkbox"/>	Routed			Enabled	
>  GigabitEthernet0/6		<input type="checkbox"/>	Routed			Enabled	
>  GigabitEthernet0/7		<input type="checkbox"/>	Routed			Enabled	
>  GigabitEthernet0/8	dmz	<input checked="" type="checkbox"/>	Routed	2001:db8:2139::237/64		Enabled	

FTD\_Interface\_IP

#	NAME	INTERFACE	IP-TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	ToISP_v4	outside	IPv4	0.0.0.0/0	192.168.30.5		1	
2	ToISP_v6	outside	IPv6	::/0	2001:db8:30::5		1	

FTD\_Default\_Route

Paso 2. Descargue el paquete de Cisco Secure Client llamado cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg de [Cisco Software Download](#) y asegúrese de que el archivo sea bueno después de la descarga confirmando que la suma de comprobación md5 del archivo descargado es la misma que la página de descarga de software de Cisco.

Paso 3. Verifique que las licencias relacionadas con RAVPN estén habilitadas en FTD.

**SUBSCRIPTION LICENSES INCLUDED**

- IPS** DISABLE  
Enabled  
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.  
Includes: Intrusion Policy
- URL** DISABLE  
Enabled  
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.  
Includes: URL Reputation
- Cisco Secure Client** Type: Premier and A... DISABLE  
Enabled  
Please select the license type that you purchased to enable remote access VPN. Note that Secure Firewall device manager does not support any of the advanced features covered by the Advantage license.  
Includes: RA-VPN

Licencia\_FDM

#### Paso 4. Crear conjunto de direcciones VPN.

Paso 4.1. Cree un pool de direcciones IPv6 e IPv4 creando objetos de red. Navegue hasta Objetos > Redes y haga clic en el botón +.

**Object Types**

- Networks** (highlighted)
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles

**Network Objects and Groups**

6 objects

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	

Create\_VPN\_Address\_Pool\_1

Paso 4.2. Proporcione la información necesaria de cada objeto de red. Haga clic en el botón Aceptar.

Para el grupo IPv4, el tipo de objeto se puede seleccionar con Red o Rango. En este ejemplo, el tipo de objeto Red se elige para fines de demostración.

- Nombre: demo\_ipv4pool
- Tipo: Red
- Red: 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 el grupo IPv6, el tipo de objeto solo se puede seleccionar con Red en este momento.

- Nombre: demo\_ipv6pool
- Tipo: Red
- Red: 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

Paso 5. Crear la red interna para NAT exenta.

Paso 5.1. Navegue hasta Objetos > Redes y haga clic en el botón +.

The screenshot shows the 'Object Types' sidebar with 'Networks' selected. The main area displays a table of network objects:

#	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	

Create\_NAT\_Exempt\_Network\_1

Paso 5.2. Proporcione la información necesaria de cada objeto de red. Haga clic en el botón OK (Aceptar)

En este ejemplo, se configuran las redes IPv4 e IPv6.

- Nombre: inside\_net\_ipv4
- Tipo: Red
- Red: 192.168.50.0/24

### Add Network Object

Name

Description

Type  Network  Host  FQDN  Range

Network   
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/64

Create\_NAT\_Exempt\_Network\_2\_IPv4

- Nombre: inside\_net\_ipv6
- Tipo: Red
- Red: 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

Paso 6. Cree el certificado utilizado para RAVPN. Tiene dos opciones: puede cargar un certificado firmado por una entidad emisora de certificados (CA) de terceros o generar un nuevo certificado autofirmado.

En este ejemplo, se utiliza un nuevo certificado autofirmado con contenido personalizado del certificado para fines de demostración.

Paso 6.1. Navegue hasta Objetos > Certificados. Haga clic en el botón + y seleccione Agregar certificado interno.

Object Types

Certificates

121 objects

#	NAME	TYPE
1	DefaultInternalCertificate	Internal Certificate
2	DefaultWebserverCertificate	Internal Certificate
3	NGFW-Default-InternalCA	Internal CA
4	AAA-Certificate-Services	Trusted CA Certificate
5	ACCVRAIZ1	Trusted CA Certificate
6	Acalis-Authentication-Root-CA	Trusted CA Certificate
7	AffirmTrust-Commercial	Trusted CA Certificate
8	AffirmTrust-Networking	Trusted CA Certificate
9	AffirmTrust-Premium	Trusted CA Certificate
10	AffirmTrust-Premium-ECC	Trusted CA Certificate
11	Amazon-Root-CA-1	Trusted CA Certificate
12	Amazon-Root-CA-2	Trusted CA Certificate
13	Amazon-Root-CA-3	Trusted CA Certificate
14	Cisco-Trusted-Authorities	Trusted CA Group

Create\_Certificate\_1

Paso 6.2. Haga clic en Certificado autofirmado.

Choose the type of internal certificate you want to create X

Upload Certificate and Key

Create a certificate from existing files.  
PEM and DER files are supported.

**Self-Signed Certificate**

Create a new certificate that is signed by the device.

Paso 6.3. Haga clic en la pestaña General y proporcione la información necesaria.

Nombre: demovpn

Tipo de clave: RSA

Tamaño de clave: 2048

Período de validez: Predeterminado

Fecha de vencimiento: Predeterminado

Uso de validación para servicios especiales: Servidor SSL

Add Internal Certificate

Search for attribute

General

Issuer

Subject

Name: demovpn

Key Type: RSA

Key Size: 2048

Validity Period

Expiration Date: (UTC+08:00) Asia/Hong\_Kong  
02/15/2027  
Set default

Validation Usage for Special Services: SSL Server

CANCEL SAVE

Create\_Certificate\_3

Paso 6.4. Haga clic en la pestaña Emisor y proporcione la información necesaria.

País: Estados Unidos (US)

Nombre común: 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

Paso 6.5. Haga clic en la pestaña Asunto, proporcione la información necesaria y luego haga clic en GUARDAR.

País: Estados Unidos (US)

Nombre común: vpn.example.com

## Add Internal Certificate



Search for attribute

Distinguished Name

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\_5

Paso 7. Crear origen de identidad del servidor RADIUS.

Paso 7.1. Navegue hasta **Objetos > Orígenes de identidad**, haga clic en el botón + y elija **Servidor RADIUS**.

The screenshot shows the 'Identity Sources' page in the Firewall Device Manager. The left sidebar lists various object types, with 'Identity Sources' selected. The main area displays a table with one object: 'LocalIdentitySource' of type 'LOCAL'. A context menu is open on the right, with 'RADIUS Server' highlighted.

#	NAME	TYPE	VALUE
1	LocalIdentitySource	LOCAL	

Preset filters: RADIUS, AD Realm, SAML, Duo LDAP

RADIUS Server

RADIUS Server Group

AD Realm

AD Realm Sequence

Identity Services Engine

SAML Server

Create\_Radius\_Source\_1

Paso 7.2. Proporcione la información necesaria del servidor RADIUS. Haga clic en el botón Aceptar.

Nombre: demo\_ise

Nombre de servidor o dirección IP: 2001:db8:2139::240

Puerto de autenticación: 1812 (default)

timeout (tiempo de espera): 10 (default)

Clave secreta del servidor: Cisco

Interfaz utilizada para conectar con el servidor Radius: Seleccione manualmente la interfaz. En este ejemplo, elija 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

Paso 7.3. Navegue hasta Objetos > Orígenes de identidad. Haga clic en el botón + y elija Grupo de servidores RADIUS.

Create Radius Server Group

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

Identity Sources

2 objects

#	NAME	TYPE	VALUE
1	LocalIdentitySource	LOCAL	
2	demo_ise	RADIUS	2001:db8:2139::241

Filter Preset filters: RADIUS, AD Realm, SAML, Duo LDAP

+ RADIUS Server Group AD Realm AD Realm Sequence Identity Services Engine SAML Server

Create\_Radius\_Source\_3

Paso 7.4. Proporcione la información necesaria del grupo de servidores RADIUS. Haga clic en el botón OK (Aceptar)

Nombre: demo\_ise\_group

Tiempo muerto: 10 (default)

Máximo de intentos fallidos: 3 (default)

Servidor RADIUS: Haga clic en el botón + y seleccione el nombre creado en el paso 6.2. En este ejemplo es demo\_ise.

## Add RADIUS Server Group



Name

demo\_ise\_group

Dead Time i

10

minutes

Maximum Failed Attempts

3

0-1440

1-5

Dynamic Authorization (for RA VPN only) i

Port

1700

1024-65535

Realm that Supports the RADIUS Server

Please select

RADIUS Server

i The servers in the group should be backups of each other



Filter

demo\_ise

demo\_ise

Create new RADIUS Server



CANCEL

OK

CANCEL

OK

Paso 8. Cree la política de grupo utilizada para RAVPN. En este ejemplo, se configuran parámetros personalizados de banner y tiempo de espera para fines de demostración. Puede realizar modificaciones en función de sus necesidades reales.

Paso 8.1. Vaya a Remote Access VPN > View Configuration. Haga clic en Políticas de grupo en la barra lateral izquierda y luego haga clic en el botón +.

The screenshot shows the Firewall Device Manager interface. The top navigation bar includes 'Firewall Device Manager', 'Monitoring', 'Policies', 'Objects', and 'Device: ftdv760'. On the left, a sidebar for 'RA VPN' lists 'Connection Profiles', 'Group Policies' (which is selected and highlighted with a red box), and 'SAML Server'. The main content area is titled 'Device Summary' and 'Group Policies', showing '2 objects'. A table lists one object: 'DftGrpPolicy' with columns for NAME, DNS SERVER, IPV4 SPLIT TUNNELING, IPV6 SPLIT TUNNELING, and SECURE CLIENT PROFILES. Both DNS SERVER and SECURE CLIENT PROFILES show 'Allow all traffic'. A large red box highlights the '+' button in the top right corner of the main content area.

Create\_Group\_Policy\_1

Paso 8.2. Haga clic en General y proporcione la información necesaria.

Nombre: demo\_gp

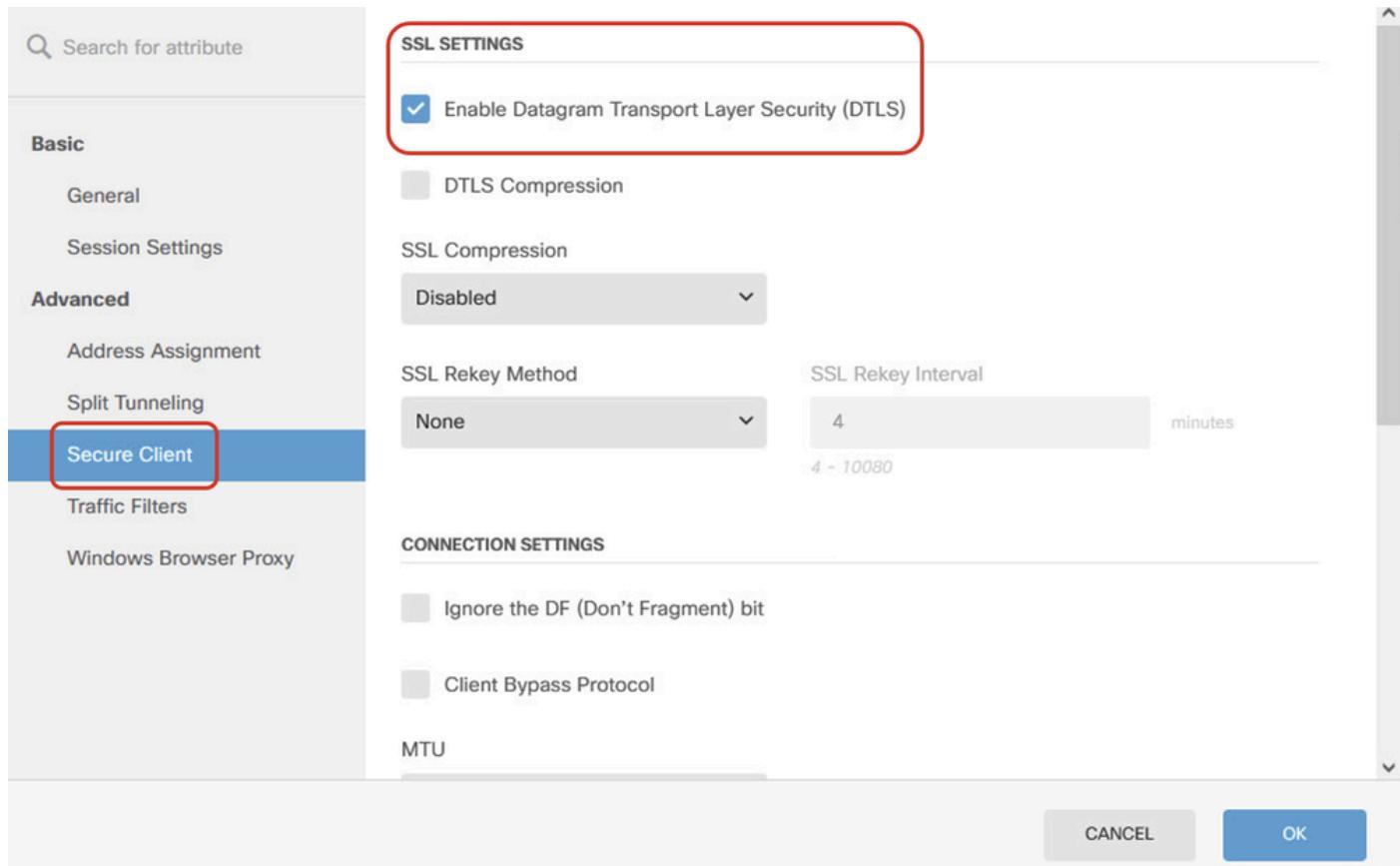
Texto de banner para clientes autenticados: banner de demostración

The screenshot shows the 'Add Group Policy' dialog box. On the left, a sidebar lists 'Basic' (selected) and 'Advanced' sections: Address Assignment, Split Tunneling, Secure Client, Traffic Filters, and Windows Browser Proxy. The 'Basic' section has a red box around the 'General' tab, which is currently active. The main area contains fields for 'Name' (set to 'demo\_gp'), 'Description' (empty), 'DNS Server' (Select DNS Group dropdown), 'Banner Text for Authenticated Clients' (set to 'demo banner'), 'Default domain' (empty), and 'Secure Client profiles' (empty). At the bottom are 'CANCEL' and 'OK' buttons.

Create\_Group\_Policy\_2

Paso 8.3. Haga clic en Secure Client y proporcione la información necesaria.

Marque Enable Datagram Transport Layer Security (DTLS).



Create\_Group\_Policy\_3

Marque Mensajes Keepalive entre Secure Client y VPN Gateway (valor predeterminado).

Marque DPD en Intervalo del lado de la puerta de enlace (valor predeterminado).

Verifique DPD en el Intervalo del Lado del Cliente (valor predeterminado).

Search for attribute

Ignore the DF (Don't Fragment) bit

Client Bypass Protocol

**Basic**

- General
- Session Settings

**Advanced**

- Address Assignment
- Split Tunneling

**Secure Client**

- Traffic Filters
- Windows Browser Proxy

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

### Paso 9. Crear un perfil de conexión RAVPN.

Paso 9.1. Vaya a VPN de acceso remoto > Ver configuración. Haga clic en Perfil de conexión en la barra lateral izquierda y luego haga clic en el botón + para iniciar el asistente.

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.				
<a href="#">CREATE CONNECTION PROFILE</a>				

Create\_RAVPN\_Wizard\_1

Paso 9.2. Proporcione la información necesaria en la sección Conexión y configuración del cliente y haga clic en el botón NEXT (Siguiente).

Nombre del perfil de conexión: demo\_ravpn

Alias de 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

Origen de identidad principal > Tipo de autenticación: Sólo AAA

Origen de identidad principal > Origen de identidad principal: demo\_ise\_group (nombre configurado en el paso 7.4.)

Origen de identidad local de reserva: LocalIdentitySource

Servidor de autorización: demo\_ise\_group (el nombre configurado en el paso 7.4.)

Servidor de cuentas: demo\_ise\_group (el nombre configurado en el paso 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

Conjunto de direcciones IPv4: demo\_ipv4pool (nombre configurado en el paso 4.2.)

Pool de Direcciones IPv6: demo\_ipv6pool (el nombre configurado en el paso 4.2.)

## Client Address Pool Assignment

### IPv4 Address Pool

Endpoints are provided an address from this pool



### IPv6 Address Pool

Endpoints are provided an address from this pool



### DHCP Servers



CANCEL

NEXT

Create\_RAVPN\_Wizard\_2\_Address\_Pool

Paso 9.3. Elija la política de grupo configurada en el Paso 8.2. en la sección Experiencia de usuario remoto y haga clic en el botón NEXT.

A screenshot of the Cisco Firewall Device Manager interface. The top navigation bar shows 'Firewall Device Manager', 'Monitoring', 'Policies', 'Objects', 'Device: ftdv760', and user information 'admin Administrator'. The main content area is titled 'Remote User Experience' and describes group policies. A dropdown menu shows 'View Group Policy' with 'demo\_gp' selected. Below is a 'Policy Group Brief Details' table:

Edit	
<b>DNS + BANNER</b>	
DNS Server	None
Banner Text for Authenticated Clients	demo banner - fdm
<b>SESSION SETTINGS</b>	
Maximum Connection Time / Alert Interval	Unlimited / 1 Minutes
Idle Time / Alert Interval	30 / 1 Minutes
Simultaneous Login per User	3

At the bottom, there are 'BACK' and 'NEXT' buttons. The 'NEXT' button is highlighted with a red box.

Create\_RAVPN\_Wizard\_3

Paso 9.4. Proporcione la información necesaria en la sección Configuración global y haga clic en el botón NEXT (Siguiente).

Certificado de identidad del dispositivo: demovpn (el nombre configurado en el paso 6.3.)

Interfaz externa: fuera

## 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

e.g. 8080

Create\_RAVPN\_Wizard\_4

Control de acceso para tráfico VPN: Verifique 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

Exención de NAT: Haga clic en el control deslizante hasta la posición Activado

Interfaces internas: dentro

Redes internas: inside\_net\_ipv4, inside\_net\_ipv6 (el nombre configurado en el paso 5.2.)

**NAT Exempt**

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

+  
inside (GigabitEthernet0/1)

**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.

+  
inside\_net\_ipv4  
inside\_net\_ipv6

Create\_RAVPN\_Wizard\_4\_VPN\_NATExempt

Paquete de Secure Client: Haga clic en CARGAR PAQUETE y cargue el paquete como corresponda. En este ejemplo, se carga el paquete de Windows.

## 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](http://software.cisco.com).

You must have the necessary secure client software license.

### Packages

UPLOAD PACKAGE

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

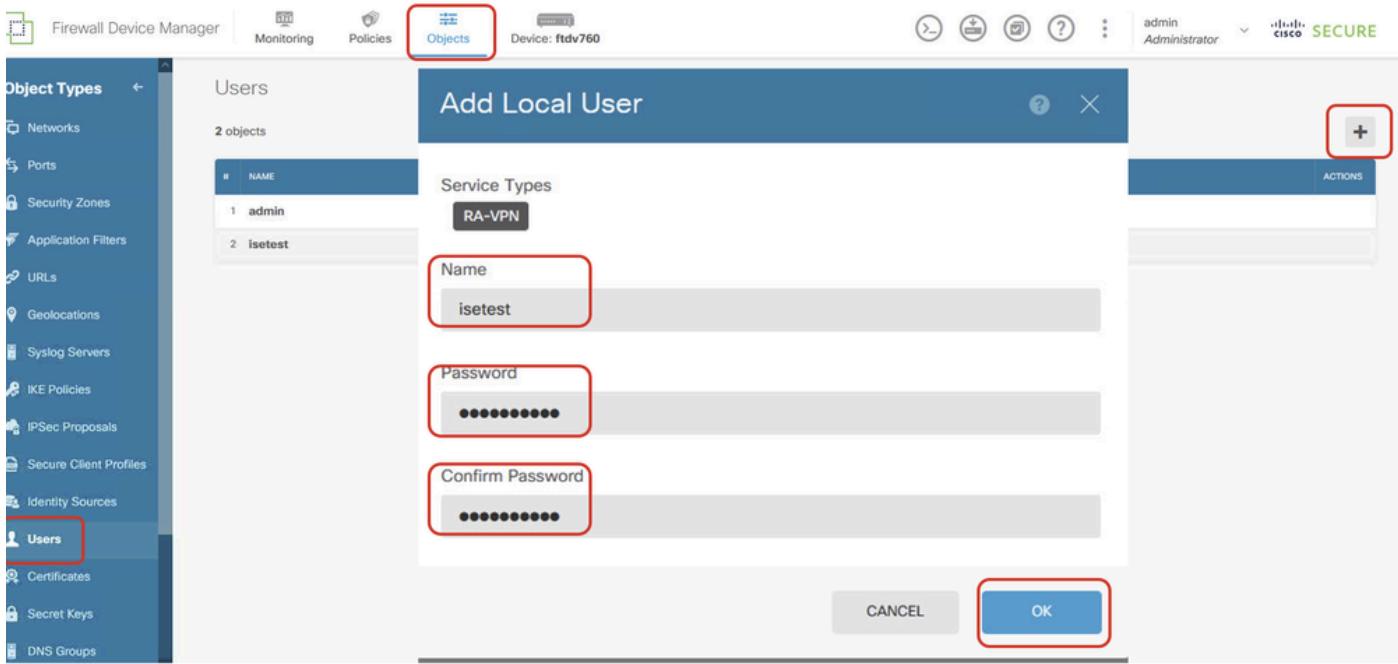
BACK

NEXT

Create\_RAVPN\_Wizard\_4\_Image

Paso 9.5. Revise el resumen. Si necesita modificar algo, haga clic en el botón BACK. Si todo está bien, haga clic en el botón FINISH.

Paso 10. Cree un usuario local si elige Origen de identidad local de reserva con LocalIdentitySource en el paso 9.2. La contraseña del usuario local debe ser la misma que la configurada en ISE.



Create\_Local\_User

## Paso 11. Implementar los cambios de configuración.



Implementar\_cambios

## Configuraciones en ISE

### Paso 12. Crear dispositivos de red.

Paso 12.1. Navegue hasta Administration > Network Resources > Network Devices, haga clic en Add, proporcione el nombre, la dirección IP y desplácese hacia abajo en la página.

Administration / Network Resources

Network Devices

Name demo\_ftd

IP Address 2001:db8:2139::237

Create\_Network\_Devices

Paso 12.2. Marque la casilla de verificación de RADIUS Authentication Settings. Proporcione el secreto compartido y haga clic en Enviar.

RADIUS Authentication Settings

Protocol RADIUS

Shared Secret \*\*\*\*\*

Create\_Network\_Devices\_Cont

Paso 13. Crear usuarios de acceso a la red. Vaya a Administration > Identity Management > Identities. Haga clic en Agregar para crear un nuevo usuario. La contraseña es la misma con el usuario local de FDM creado en el paso 10. para asegurarse de que la reserva funciona.

Administration / Identity Management

Identities

Users

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

Create\_ISE\_User

Paso 14. (Opcional) Cree un nuevo juego de políticas con una regla de autenticación y una regla

de autorización personalizadas. En este ejemplo, el conjunto de políticas predeterminado se utiliza para fines de demostración.

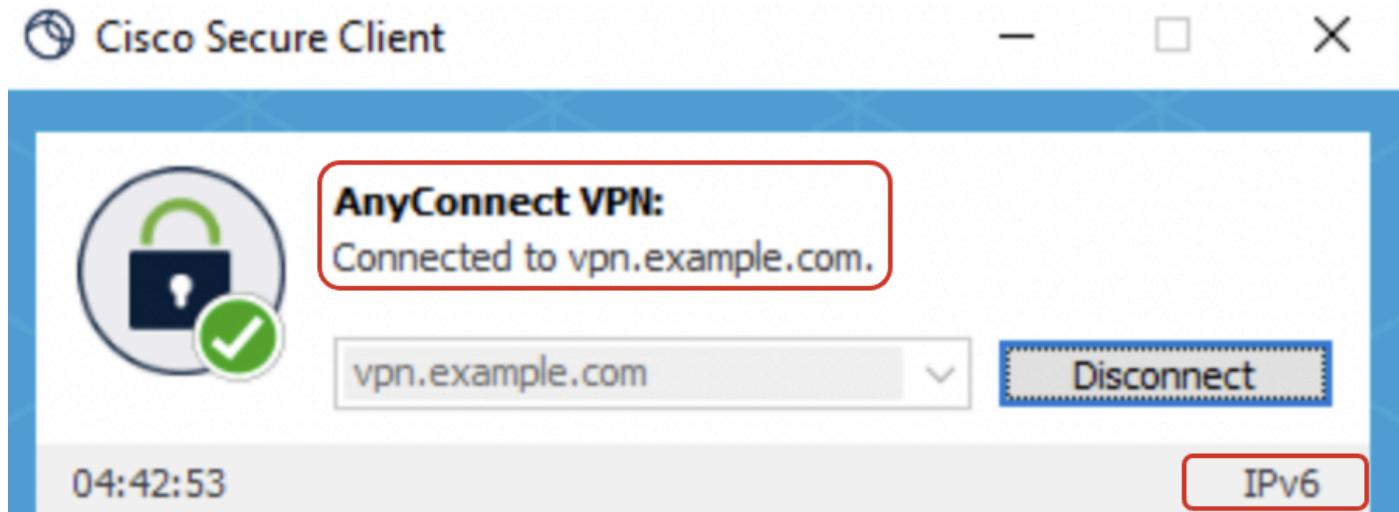
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Normal	SPRT		Radius-NAS-IP-Address EQUALS 10.48.26.61	Default Network Access	0	⚙️	↗️
Normal	Wired		DEVICE-Device Type EQUALS All Device Types#Switch	Default Network Access	0	⚙️	↗️
Normal	Firewall No Posture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

ISE\_Default\_Policy\_Set

## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Paso 15. Conecte el gateway VPN a través de la dirección IPv6 en el cliente. La conexión VPN se ha realizado correctamente.



Verify\_Connection\_Successful

Paso 16. Navegue hasta la CLI de FTD a través de SSH o la consola. Ejecute el comando `show vpn-sessiondb detail anyconnect` en la CLI de FTD (Line) para verificar los detalles de la sesión 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  
Audit 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 T0 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
```

Paso 17. Prueba de ping en el cliente. En este ejemplo, el cliente hace ping correctamente a las direcciones IPv4 e IPv6 del 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

Paso 18. El registro activo de RADIUS de ISE muestra una autenticación correcta.

## 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

Paso 19. La autenticación de prueba de FTD pasa a LOCAL cuando FTD no puede alcanzar ISE.

Paso 19.1. Cuando la autenticación de FTD vaya a ISE, ejecute el comando show aaa-server en FTD (Line) CLI para verificar las estadísticas.

En este ejemplo, no hay contadores para LOCAL y la autenticación se dirige al 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
```

Paso 19.2. Cierre la interfaz de ISE para simular que FTD no puede recibir ninguna respuesta de 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)
```

Paso 19.3. El cliente inicia la conexión VPN e introduce el mismo nombre de usuario y contraseña creados en el paso 10. La conexión VPN sigue siendo correcta.

Ejecute el comando show aaa-server en FTD (Line) CLI nuevamente para verificar la estadística, los contadores de autenticación, autorización y aceptación para LOCAL han aumentado. El contador de aceptaciones para el servidor RADIUS no ha aumentado.

```
<#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

```

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Puede ejecutar estos comandos en FTD Line para resolver problemas de la sección VPN.

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

Puede recopilar un archivo DART del cliente para la resolución de problemas de VPN para determinar si el problema es con Secure Client. Para obtener orientación, consulte el documento de CCO correspondiente [Collect DART Bundle for Secure Client](#).

Puede ejecutar estos comandos en FTD Line para resolver problemas en la sección 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>
```

Puede revisarlos para resolver el problema relacionado con el tráfico después de la conexión VPN exitosamente.

1. Capture el tráfico en FTD Line para ver si Lina descarta el tráfico, refiriéndose a este documento de CCO; [Use las capturas de Firepower Threat Defence y Packet Tracer - Cisco](#).
2. Revise la política de control de acceso para asegurarse de que el tráfico VPN relacionado pueda pasar si se inhabilita la política de control de acceso de omisión para tráfico descifrado.
3. Revise la exención de NAT para asegurarse de que el tráfico VPN se excluya de NAT.

## Información Relacionada

- [Guía de configuración de FDM de RAVPN - Cisco](#)
- [Recopile el paquete DART para Secure Client - Cisco](#)
- [Utilice capturas de Firepower Threat Defence y Packet Tracer - Cisco](#)
- [Solución de problemas de Cisco Secure Client - Cisco](#)
- [Soporte técnico y descargas de Cisco](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).