

Configurar la autenticación de certificado de cliente seguro en FTD administrado por FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[a. Crear/importar un certificado utilizado para la autenticación del servidor](#)

[b. Agregar un certificado de CA interna/de confianza](#)

[c. Configure el Pool de Direcciones para los Usuarios de VPN](#)

[d. Cargar imágenes de Secure Client](#)

[e. Crear y cargar perfil XML](#)

[Configuración de VPN de acceso remoto](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el proceso de configuración de VPN de acceso remoto en Firepower Threat Defense (FTD) administrado por Firepower Management Center (FMC) con autenticación de certificados.

Colaboración de Dolly Jain y Rishabh Aggarwal, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Inscripción manual de certificados y aspectos básicos de SSL
- FMC
- Conocimientos básicos de autenticación para VPN de acceso remoto
- Autoridad de certificación (CA) de terceros como Entrust, Geotrust, GoDaddy, Thawte y VeriSign

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Secure Firepower Threat Defense versión 7.4.1
- Firepower Management Center (FMC) versión 7.4.1
- Secure Client versión 5.0.05040
- Microsoft Windows Server 2019 como servidor de la CA

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.

Configurar

Diagrama de la red

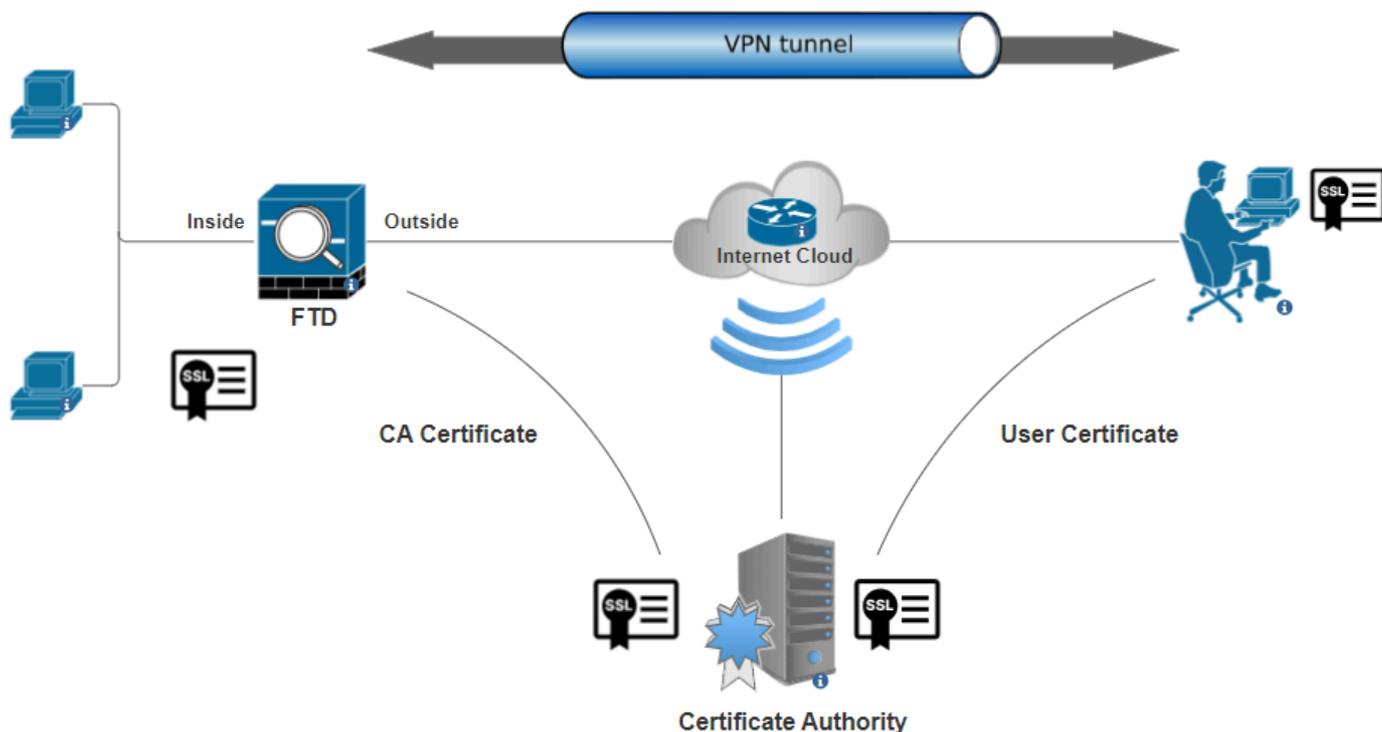


Diagrama de la red

Configuraciones

a. Crear/importar un certificado utilizado para la autenticación del servidor



Nota: En FMC, se necesita un certificado de CA para poder generar el CSR. Si se genera CSR a partir de una fuente externa (OpenSSL o de terceros), el método manual falla y se debe utilizar el formato de certificado PKCS12.

Paso 1. Desplácese hasta `Devices > Certificates` y haga clic en `Add`. Seleccione Dispositivo y haga clic en el signo más (+) en `Inscripción de certificados`.

Add New Certificate



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

Device*:

Cert Enrollment*:

Cancel

Add

Agregar inscripción de certificados

Paso 2. En la CA Information, seleccione el Tipo de inscripción como Manual y pegue el certificado de la Autoridad de certificación (CA) utilizado para firmar el CSR.

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

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

CA Certificate:

```
HQYDVQQDEZXIeWRyYVw5O5
UQgU2VydMvYlENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID-7zooQw
```

Validation Usage:

IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Cancel

Save

Agregar información de CA

Paso 3. Para el uso de validación, seleccione IPsec Client, SSL Client y Skip Check for CA flag in basic constraints of the CA Certificate.

Paso 4. En Certificate Parameters, rellene los detalles del nombre del sujeto.

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN: Don't use FQDN in certificate ▼

Include Device's IP Address:

Common Name (CN): certauth.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): Bangalore

State (ST): KA

Country Code (C): IN

Email (E):

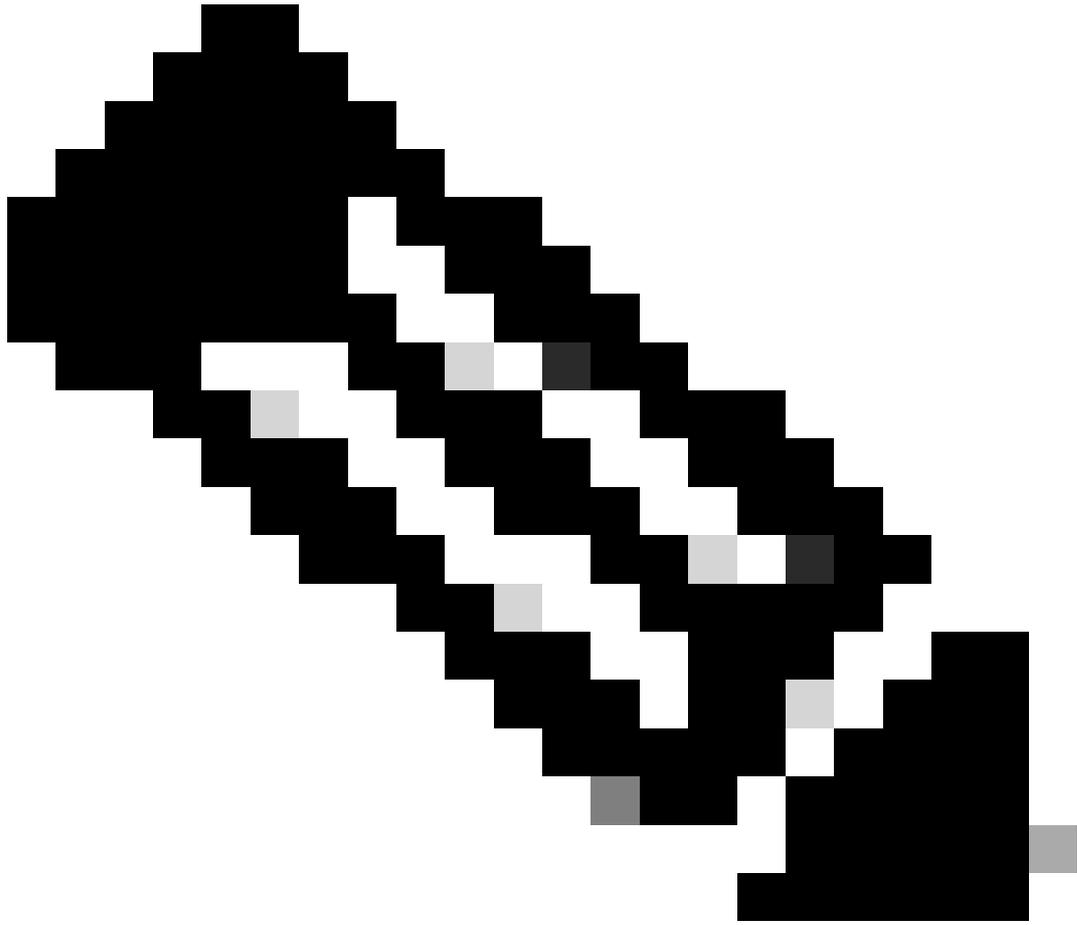
Include Device's Serial Number

Cancel

Save

Agregar parámetros de certificado

Paso 5. En Keyseleccione el tipo de clave como RSA con un nombre y tamaño de clave. Haga clic en Save.



Nota: Para el tipo de clave RSA, el tamaño mínimo de clave es 2048 bits.

Add Cert Enrollment



Name*
ssl_certificate

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:
 RSA ECDSA EdDSA

Key Name:*
rsakey

Key Size:
2048 ▼

▼ Advanced Settings

Ignore IPsec Key Usage

Cancel **Save**

Agregar clave RSA

Paso 6. En Cert Enrollment, seleccione el punto de confianza en el menú desplegable que acaba de crear y haga clic en Add.

Add New Certificate



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

Device*:

Cert Enrollment*:

 +

Cert Enrollment Details:

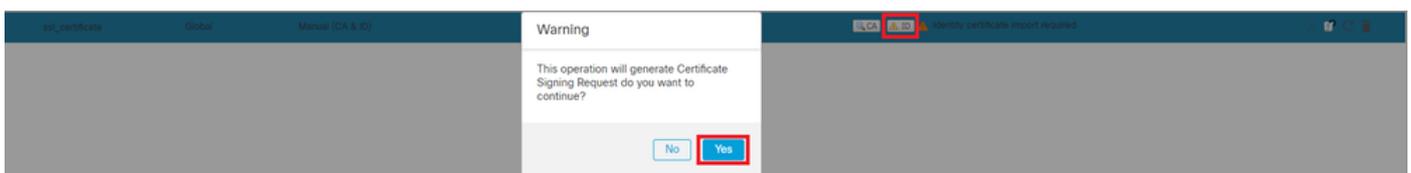
Name: ssl_certificate
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Cancel

Add

Agregar nuevo certificado

Paso 7. Haga clic en ID y, a continuación, haga clic Yes en el mensaje adicional para generar el CSR.



Generar CSR

Paso 8. Copie la CSR y consígala firmada por la autoridad de certificación. Una vez que la CA haya emitido el certificado de identidad, impórtelo haciendo clic en Browse Identity Certificate y haga clic en Import .

Import Identity Certificate



Step 1

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

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMakGA1UEBhMC
SU4wggliMA0GCsqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1pLEdR4X6ZlnM5fNA/GLV9MnPoP
ppzi0uLlbVmb5iKQexllaur/e3PBccc3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

Step 2

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

Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

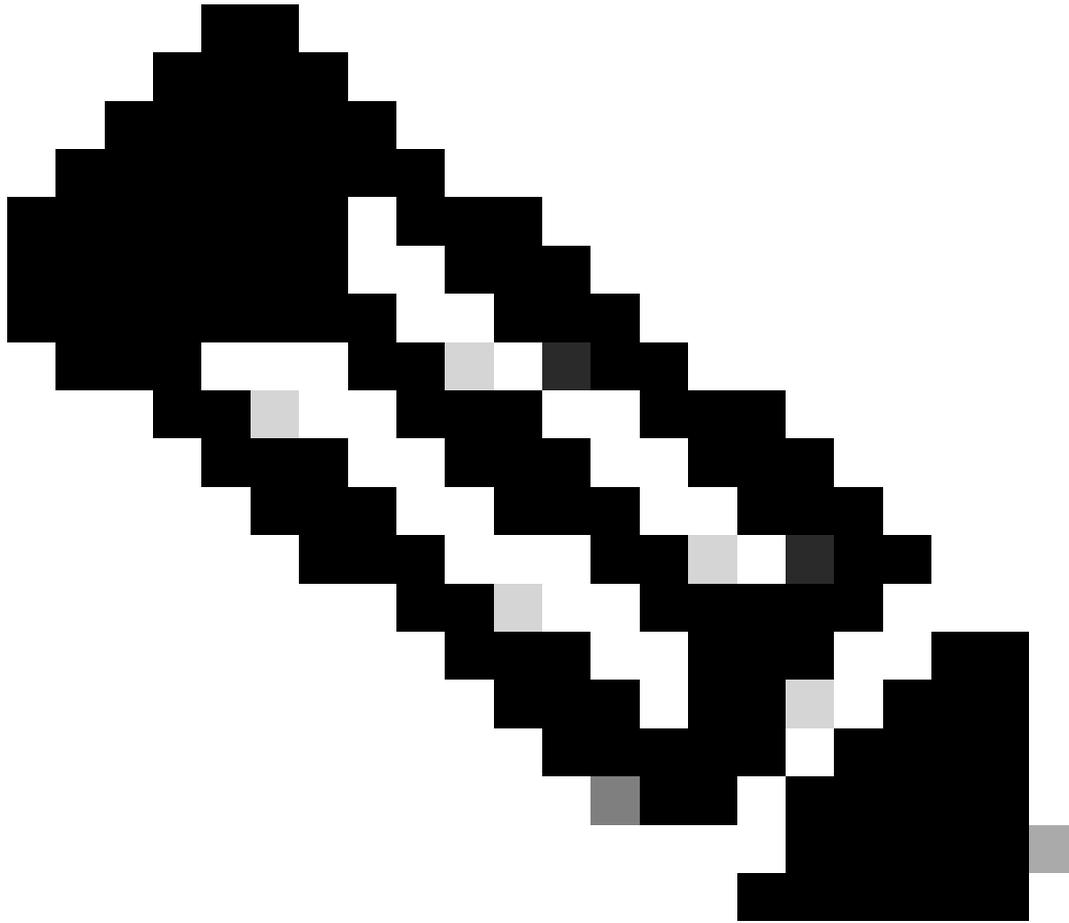
[Import](#)

Importar certificado de ID



Nota: Si la emisión del certificado de ID lleva tiempo, puede repetir el paso 7 más tarde. Esto generará la misma CSR y podemos importar el certificado de ID.

b. Agregar un certificado de CA interna/de confianza



Nota: Si la autoridad de certificación (CA) utilizada en el paso (a), "**Crear/importar un certificado utilizado para la autenticación del servidor**" también emite certificados de usuario, puede omitir el **paso (b)**, "**Agregar un certificado de CA de confianza/interno**". No es necesario volver a agregar el mismo certificado de CA, por lo que también se debe evitar. Si se agrega el mismo certificado de CA nuevamente, el punto de confianza se configura con "validation-usage none" que puede afectar la autenticación del certificado para RAVPN.

Paso 1. Desplácese hasta Devices > Certificates y haga clic en Add.

Seleccione Dispositivo y haga clic en el signo más (+) en Inscripción de certificados.

Aquí, "auth-risaggar-ca" se utiliza para emitir certificados de identidad/usuario.

General Details Certification Path



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: auth-risaggar-ca

Issued by: auth-risaggar-ca

Valid from 04-03-2023 **to** 04-03-2033

Issuer Statement

OK

auth-risaggar-ca

Paso 2. Introduzca un nombre de punto de confianza y seleccione Manual como tipo de inscripción en CA information.

Paso 3. Verifique CA Onlyy pegue el certificado de CA interna/de confianza en formato pem.

Paso 4. Marque **Skip Check for CA flag in basic constraints of the CA Certificate** haga clic en Save.

Add Cert Enrollment ?

Internal_CA

Description

CA InformationCertificate ParametersKeyRevocation

Enrollment Type: Manual

CA Only

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

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
--  
MIIG1jCCBL6gAwIBAgIQQAFu  
+wogXPrr4Y9x1zq7eDANBgk  
qhkiG9w0BAQsFADBK  
MQswCQYDVQQGEwJVUzES  
MBAGA1UEChMJSWRlbiRydX  
N0MScwJQYDVQQDEx5JZGV  
u  
VHJ1c3QgQ29tbWVyY2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage: IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Cancel Save

Paso 5. En Cert Enrollment, seleccione el punto de confianza en el menú desplegable que acaba de crear y haga clic en Add.

Add New Certificate



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

Device*:

Cert Enrollment*:

 +

Cert Enrollment Details:

Name: Internal_CA
Enrollment Type: Manual (CA Only)
Enrollment URL: N/A

Cancel

Add

Agregar CA interna

Paso 6. El certificado agregado anteriormente se muestra como:

Internal_CA	Global	Manual (CA Only)	Mar 4, 2033	CA ID	⌵ ⌵ ⌵ ⌵
-------------	--------	------------------	-------------	-------	---------

Certificado agregado

c. Configure el Pool de Direcciones para los Usuarios de VPN

Paso 1. Vaya a Objects > Object Management > Address Pools > IPv4 Pools .

Paso 2. Introduzca el nombre y el intervalo de direcciones IPv4 con una máscara.

Edit IPv4 Pool



Name*

vpn_pool

Description

IPv4 Address Range*

10.20.20.1-10.20.20.130

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

Mask*

255.255.255.0

Allow Overrides

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

▶ Override (0)

Cancel

Save

Agregar conjunto IPv4

d. Cargar imágenes de Secure Client

Paso 1. Descargue las imágenes de cliente seguras de implementación web según el sistema operativo desde el sitio [Cisco Software](#).

Paso 2. Vaya a Objects > Object Management > VPN > Secure Client File > Add Secure Client File .

Paso 3. Introduzca el nombre y seleccione el archivo Secure Client del disco.

Paso 4. Seleccione el tipo de archivo como Secure Client Image y haga clic en Save.

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

Agregar imagen de cliente seguro

e. Crear y cargar perfil XML

Paso 1. Descargue e instale Secure Client Profile Editor desde el sitio [Cisco Software](#).

Paso 2. Cree un nuevo perfil y selecciónelo All en el menú desplegable Selección de certificado de cliente. Controla principalmente los almacenes de certificados que Secure Client puede utilizar para almacenar y leer certificados.

Otras dos opciones disponibles son:

- **Equipo:** Secure Client está restringido a la búsqueda de certificados en el almacén de certificados del equipo local de Windows.
- **Usuario:** Secure Client está restringido a la búsqueda de certificados en el almacén de certificados de usuario local de Windows.

Establecer la invalidación del almacén de certificados como True .

Esto permite a un administrador indicar a Secure Client que utilice certificados del almacén de certificados del equipo Windows (sistema local)

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

Preferences (Part 2)

Profile: C:\Users\dolljain\Downloads\client_profile.xml

Disable Automatic Certificate Selection

User Controllable

Proxy Settings

Native

User Controllable

Public Proxy Server Address:

Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080

Allow Local Proxy Connections

Enable Optimal Gateway Selection

User Controllable

Suspension Time Threshold (hours)

Performance Improvement Threshold (%)

Automatic VPN Policy

Trusted Network Policy

Disconnect

Untrusted Network Policy

Connect

Bypass connect upon VPN session timeout

Trusted DNS Domains

Trusted DNS Servers

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Trusted Servers @ https://<server>[:<port>]

https://

Add

Delete

Certificate Hash:

Set

Disable interfaces without trusted server connectivity while in truste...

Always On

(More Information)

Allow VPN Disconnect

Allow access to the following hosts with VPN disconn...

Connect Failure Policy

Closed

Allow Captive Portal Remediation

Remediation Timeout (min.)

Apply Last VPN Local Resource Rules

Captive Portal Remediation Browser Failover

Allow Manual Host Input

PPP Exclusion

Disable

User Controllable

PPP Exclusion Server IP

User Controllable

Enable Scripting

User Controllable

Terminate Script On Next Event

Enable Post SBL On Connect Script

Retain VPN on Logoff

User Enforcement

Same User Only

Authentication Timeout (seconds)

Server List Entry para configurar un perfil en Secure Client VPN proporcionando group-alias y group-url en la Lista de servidores y guarde el perfil XML.

The screenshot shows the Cisco Secure Client Profile Editor - VPN interface. The main window displays the 'Server List' configuration for a profile named 'C:\Users\dolljain\Downloads\client_profile.xml'. A table lists the servers, with the first entry highlighted in red:

Hostname	Host Address	User Group	Backup Serve...	SCEP	Mobile Settings	Certificate Pins
SSL-VPN	https://certaut...	ssl-cert	-- Inherited --			

Below the table, a note states: "Note: it is highly recommended that at least one server be defined in a profile." Buttons for 'Add...', 'Delete', 'Edit...', and 'Details' are visible.

The 'Server List Entry' dialog box is open, showing the configuration for the selected server. The 'Primary Server' section includes:

- Display Name (required): SSL-VPN
- FQDN or IP Address: https://certauth.cisco.com
- User Group: ssl-cert
- Group URL: (empty field)

The 'Connection Information' section includes:

- Primary Protocol: SSL
- ASA gateway: (unchecked)
- Auth Method During IKE Negotiation: EAP-AnyConnect
- IKE Identity (IOS gateway only): (empty field)

The 'Backup Servers' section includes a table for adding backup servers:

Host Address	Action
	Add
	Move Up
	Move Down
	Delete

Buttons for 'OK' and 'Cancel' are at the bottom of the dialog.

Agregar lista de servidores

Paso 5. Por último, el perfil XML está listo para utilizarse.

```

<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStoreAll</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreLinux>All</CertificateStoreLinux>
    <CertificateStoreOverride>true</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>30</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
    <ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
    <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
    <AutoReconnect UserControllable="false">true
      <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
    </AutoReconnect>
    <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
    <AutoUpdate UserControllable="false">true</AutoUpdate>
    <RSA SecurIDIntegration UserControllable="false">Automatic</RSA SecurIDIntegration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVFNEstablishment>AllowRemoteUsers</WindowsVFNEstablishment>
    <LinuxVFNEstablishment>LocalUsersOnly</LinuxVFNEstablishment>
    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
    <PPPEExclusion UserControllable="false">Disable
      <PPPEExclusionServerIP UserControllable="false"></PPPEExclusionServerIP>
    </PPPEExclusion>
    <EnableScripting UserControllable="false">false</EnableScripting>
    <EnableAutomaticServerSelection UserControllable="false">false
      <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
      <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
    </EnableAutomaticServerSelection>
    <RetainVpnOnLogoff>false
      </RetainVpnOnLogoff>
    <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
    <AllowManualHostInput>true</AllowManualHostInput>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>SSL-VPN</HostName>
      <HostAddress>https://certauth.cisco.com</HostAddress>
      <UserGroup>ssl-cert</UserGroup>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>

```

Perfil XML

Ubicación de perfiles XML para varios sistemas operativos:

- **Windows** - C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile
- **MacOS**: /opt/cisco/anyconnect/profile
- **Linux**: /opt/cisco/anyconnect/profile

Paso 6. Vaya a Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile .

Introduzca el nombre del archivo y haga clic en Browse para seleccionar el perfil XML. Haga clic en Save.

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

Agregar perfil VPN de cliente seguro

Configuración de VPN de acceso remoto

Paso 1. Cree una ACL según los requisitos para permitir el acceso a los recursos internos.

Desplácese hasta Objects > Object Management > Access List > Standard y haga clic en Add Standard Access List.

Edit Standard Access List Object



Name

Split_ACL

▼ Entries (1)

Add

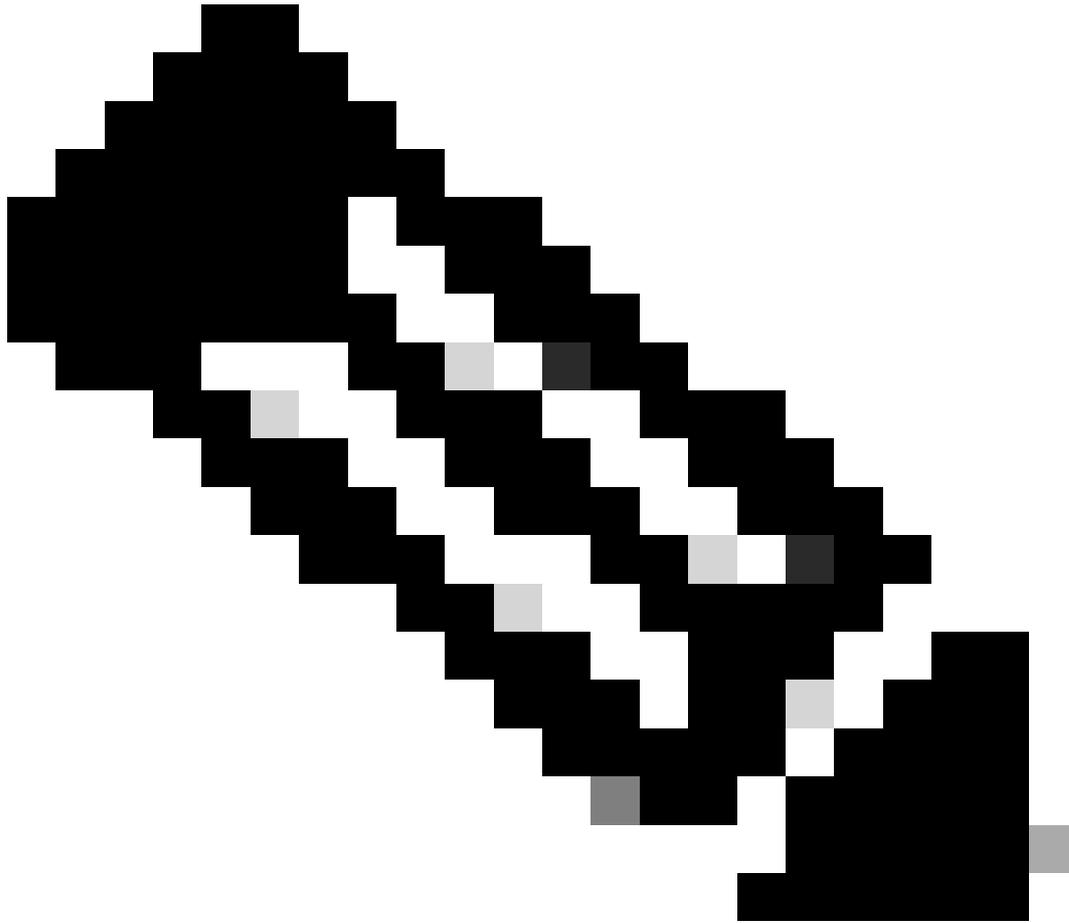
Sequence No	Action	Network	
1	Allow	split_acl	

Allow Overrides

Cancel

Save

Agregar ACL estándar



Nota: Secure Client utiliza esta ACL para agregar rutas seguras a los recursos internos.

Paso 2. Desplácese hasta `Devices > VPN > Remote Access` y haga clic en `Add`.

Paso 3. Introduzca el nombre del perfil, seleccione el dispositivo FTD y haga clic en `Next (Siguiente)`.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*

RAVPN

Description:

VPN Protocols:

- SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Q Search"/>	FTD-A-7.4.1
FTD-A-7.4.1	
FTD-B-7.4.0	
FTD-ZTNA-7.4.1	
<input type="button" value="Add"/>	

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure [LOCAL](#) or [Realm](#) or [RADIUS Server Group](#) or [SSO](#) to authenticate VPN clients.

Secure Client Package

Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

Agregar nombre de perfil

Paso 4. Introduzca el Connection Profile Name y seleccione el método de autenticación como Client Certificate Only en Autenticación, autorización y contabilidad (AAA).

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* RAVPN-CertAuth

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

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: Client Certificate Only

Username From Certificate: Map specific field Use entire DN (Distinguished Name) as username

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Authorization Server: +
(Realm or RADIUS)

Accounting Server: +
(RADIUS)

Seleccionar método de autenticación

Paso 5. Haga clic Use IP Address Pools en Asignación de dirección de cliente y seleccione el pool de direcciones IPv4 creado anteriormente.

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

Seleccionar asignación de dirección de cliente

Paso 6. Edite la directiva de grupo.

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* ▼ +

[Edit Group Policy](#)

Editar directiva de grupo

Paso 7. Desplácese hasta General > Split Tunneling , seleccione Tunnel networks specified below y seleccione Standard Access List en Tipo de lista de red de túnel dividido.

Seleccione la ACL creada anteriormente.

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

Tunnel networks specified below ▼

IPv6 Split Tunneling:

Allow all traffic over tunnel ▼

Split Tunnel Network List Type:

Standard Access List Extended Access List

Standard Access List:

Split_ACL ▼ +

DNS Request Split Tunneling

DNS Requests:

Send DNS requests as per split t ▼

Domain List:

Cancel

Save

Agregar túnel dividido

Paso 8. Desplácese hasta Secure Client > Profile , seleccione el Client Profile y haga clic en Save.

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

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

Client Profile:

Anyconnect_Profile-5-0-05040 ▾ +

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

Agregar perfil de cliente seguro

Paso 9. Haga clic en Next, seleccione el Secure Client Image y haga clic en Next.

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

<input type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyconnectWin-5.0.05040	cisco-secure-client-win-5.0.05040-webde...	Windows ▾

Agregar imagen de cliente seguro

Paso 10. Seleccione la interfaz de red para el acceso VPN, elija el Device Certificates y marque sysopt permit-vpn y haga clic en Next.

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +
 Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +
 Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

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

Agregar control de acceso para tráfico VPN

Paso 11. Por último, revise todas las configuraciones y haga clic en Finish.

Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	FTD-B-7.4.0
Connection Profile:	RAVPN-CertAuth
Connection Alias:	RAVPN-CertAuth
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
Secure Client Images:	AnyconnectWin-5.0.05040
Interface Objects:	outside-zone
Device Certificates:	ssl_certificate

Device Identity Certificate Enrollment

Certificate enrollment object 'ssl_certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Configuración de la directiva VPN de acceso remoto

Paso 12. Una vez finalizada la configuración inicial de la VPN de acceso remoto, edite el perfil de conexión creado y vaya a Aliases.

Paso 13. Configure group-alias haciendo clic en el icono más (+).

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth

Group Policy:* DfltGrpPolicy +

[Edit Group Policy](#)

Client Address Assignment AAA **Aliases**

Alias Names:

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

Name	Status	
ssl-cert	Enabled	

URL Alias:

Configure the list of UR following URLs, system

URL	
-----	--

Edit Alias Name

Alias Name:

 Enabled

Cancel OK

Cancel Save

Editar alias de grupo

Paso 14. Configure group-url haciendo clic en el icono más (+). Utilice la misma URL de grupo configurada anteriormente en el perfil de cliente.

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth

Group Policy:* DfltGrpPolicy [Edit Group Policy](#)

Client Address Assignment AAA **Aliases**

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

Edit URL Alias

URL Alias:

certauth

Enabled

[Cancel](#) [OK](#)

URL Alias:

Configure the list of URL Aliases for this connection profile. If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status
certauth (https://certauth.cisco.com/ssl-cert)	Enabled

[Cancel](#) [Save](#)

Editar URL de grupo

Paso 15. Vaya a Interfaces de acceso. Seleccione Interface Trustpoint y SSL Global Identity Certificate en la configuración de SSL.

RAVPN

Enter Description

Local Realm: cisco-local Policy Assignments (1) Dynamic Access Policy: None

Connection Profile **Access Interfaces** Advanced

Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2
outside-zone	ssl_certificate	●	●	●

Access Settings

Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:* 443

DTLS Port Number:* 443

SSL Global Identity Certificate: **ssl_certificate**

Note: Ensure the port used in VPN configuration is not used in other services

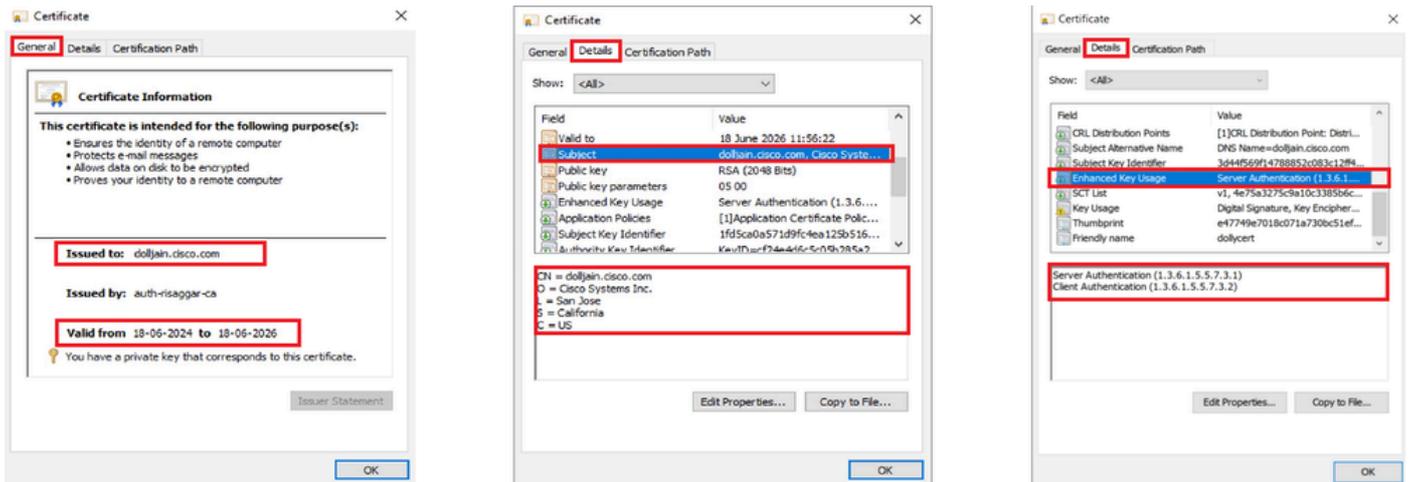
Editar interfaces de acceso

Paso 16. HagaSave clic e implemente estos cambios.

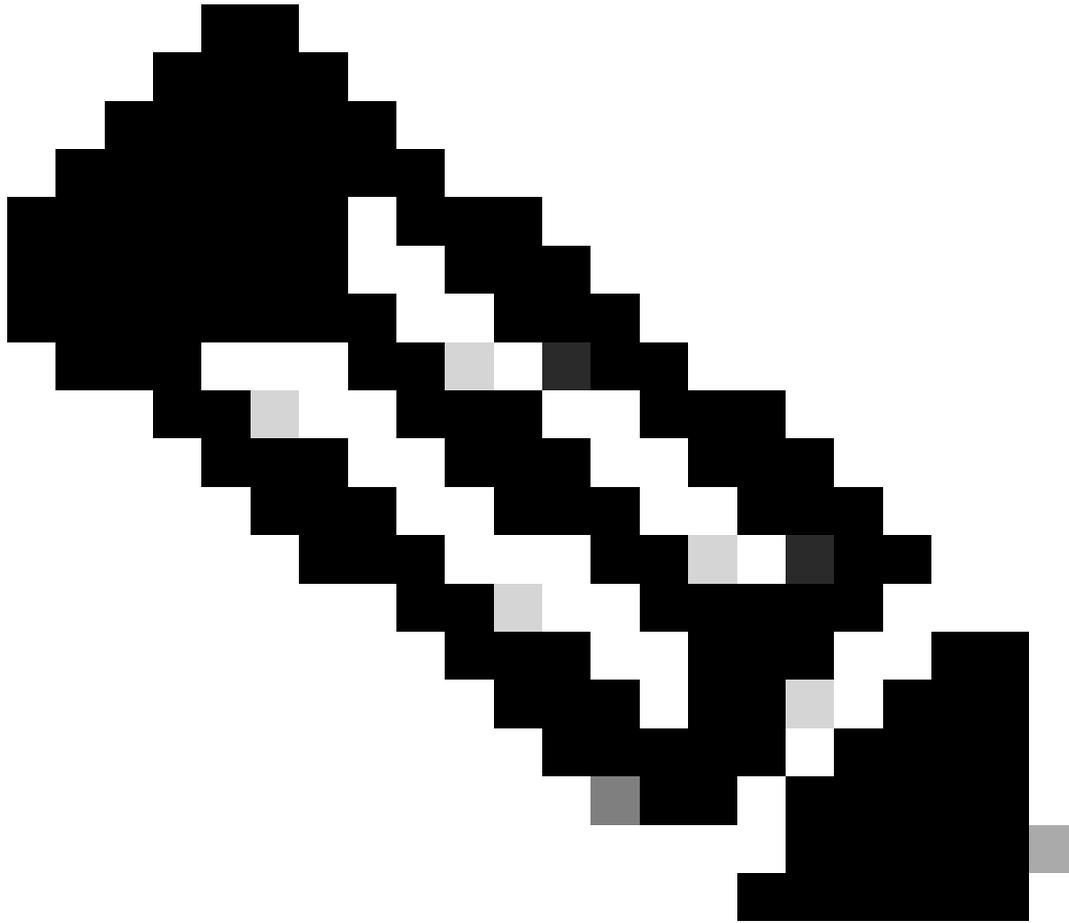
Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. El equipo cliente seguro debe tener el certificado instalado con una fecha, asunto y EKU válidos en el equipo del usuario. Este certificado debe ser emitido por la CA cuyo certificado esté instalado en FTD, como se muestra anteriormente. Aquí, la identidad o el certificado de usuario es emitido por "auth-risaggar-ca".

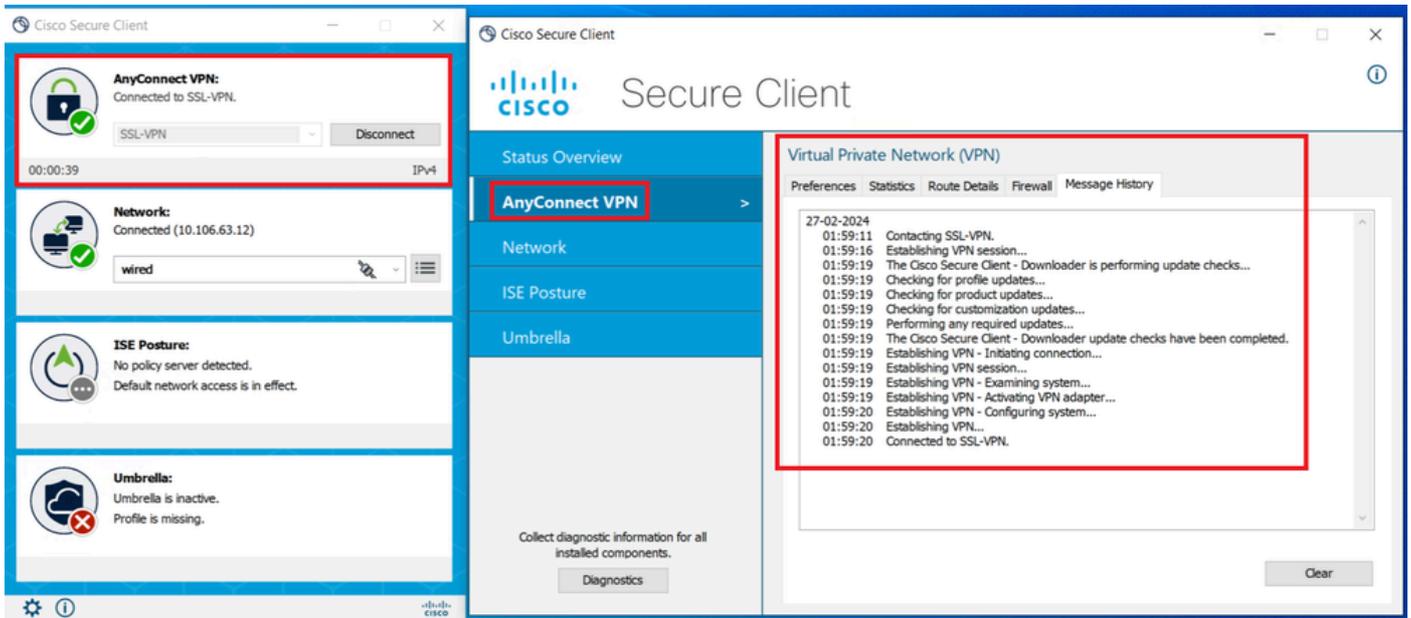


Características del certificado



Nota: el certificado de cliente debe tener el uso mejorado de claves (EKU) de "autenticación de cliente".

2. Secure Client debe establecer la conexión.



Conexión de cliente segura correcta

3. Ejecute `show vpn-sessiondb anyconnect` para confirmar los detalles de conexión del usuario activo en el grupo de túnel utilizado.

```
firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dolljain.cisco.com Index :
```

Troubleshoot

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

1. Las depuraciones se pueden ejecutar desde la CLI de diagnóstico del FTD:

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2. Consulte esta [guía](#) para obtener información sobre problemas comunes.

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).