

Configurar Autenticação de Certificado de Cliente Seguro no FTD Gerenciado pelo FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[a. Criar/Importar um Certificado Usado para Autenticação do Servidor](#)

[b. Adicionar um Certificado CA Confiável/Interno](#)

[c. Configure o pool de endereços para usuários de VPN](#)

[d. Fazer upload de imagens de cliente seguras](#)

[e. Criar e fazer upload do perfil XML](#)

[Configuração de VPN de acesso remoto](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve o processo de configuração da VPN de acesso remoto no Firepower Threat Defense (FTD) gerenciado pelo Firepower Management Center (FMC) com autenticação de certificado.

Contribuição de Dolly Jain e Rishabh Aggarwal, engenheiro do Cisco TAC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Registro manual de certificados e noções básicas de SSL FMC
- Conhecimento básico de autenticação para VPN de acesso remoto
- Autoridade de Certificação (CA) de terceiros, como Entrust, Geotrust, GoDaddy, Thawte e VeriSign

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Secure Firepower Threat Defense versão 7.4.1
- Firepower Management Center (FMC) versão 7.4.1
- Secure Client versão 5.0.05040
- Microsoft Windows Server 2019 como servidor de autoridade de certificação

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.

Configurar

Diagrama de Rede

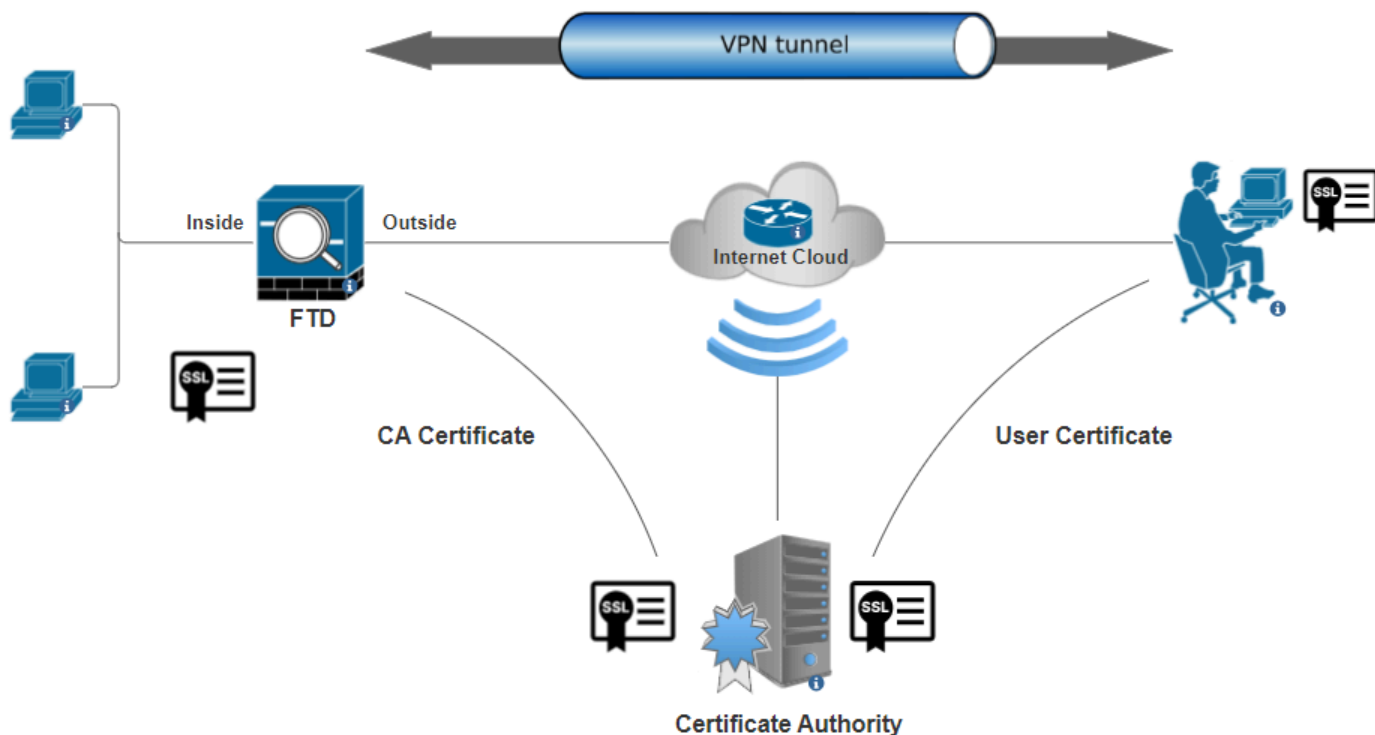


Diagrama de Rede

Configurações

a. Criar/Importar um Certificado Usado para Autenticação do Servidor



Observação: no FMC, um certificado CA é necessário antes que você possa gerar o CSR. Se o CSR for gerado de uma fonte externa (OpenSSL ou terceiros), o método manual falhará e o formato do certificado PKCS12 deverá ser usado.

Etapa 1. Navegue até `Devices > Certificat` e clique em `Add`. Selecione `Device` e clique no sinal de mais (+) em `Cert Enrollment`.

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

Adicionar registro de certificado

Etapa 2. Em CA Information, selecione o Tipo de inscrição como Manual e cole o certificado da Autoridade de certificação (CA) usado para assinar o 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:

```
HQYDVQQDEZXIeWRyYw50S
UQgU2VydMvYlENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID-7...
```

Validation Usage:

IPsec Client SSL Client SSL Server

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

Cancel

Save

Adicionar informações da autoridade de certificação

Etapa 3. Em Uso da Validação, selecione IPsec Client, SSL Client e Skip Check for CA flag in basic constraints of the CA Certificate.

Etapa 4. Em Certificate Parameters, preencha os detalhes do nome do assunto.

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):

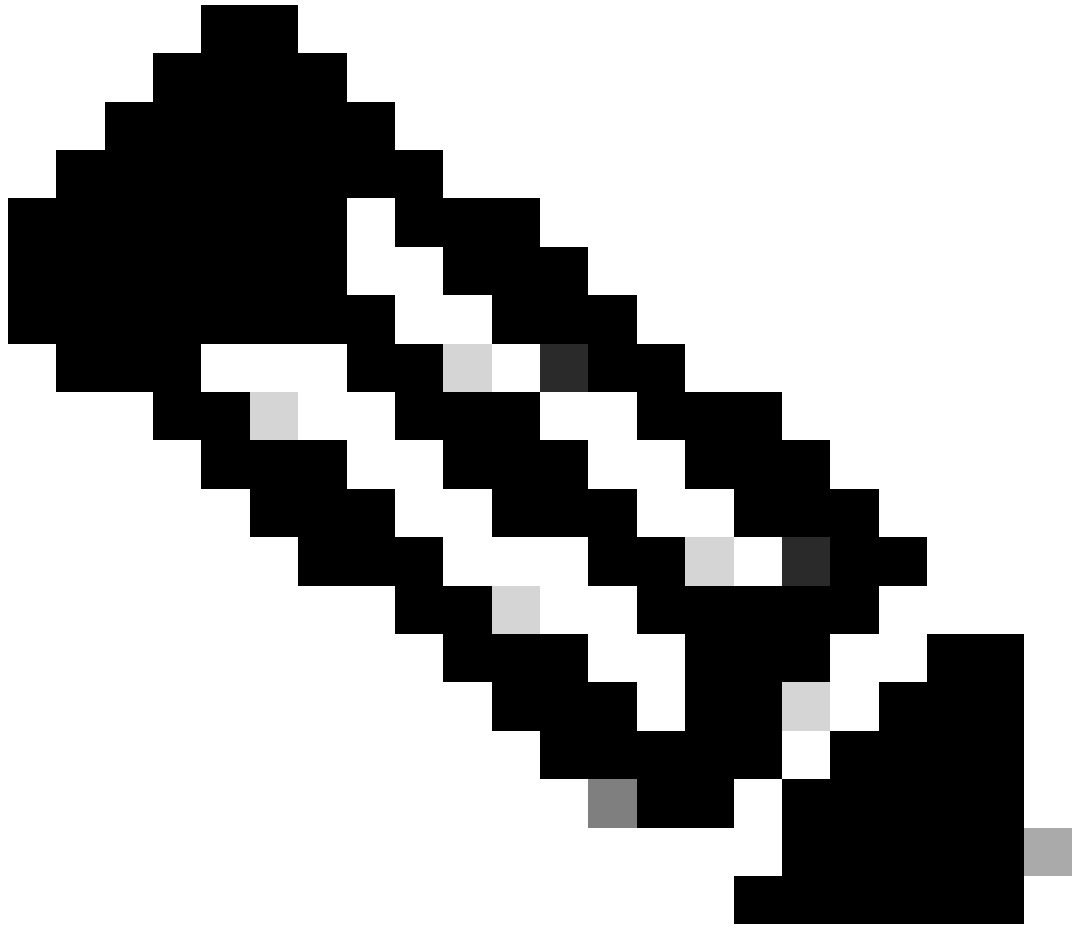
Include Device's Serial Number

Cancel

Save

Adicionar Parâmetros de Certificado

Etapa 5. Em Keyselecione o tipo de chave como RSA com um nome de chave e tamanho. Clique em Save.



Observação: para o tipo de chave RSA, o tamanho mínimo da chave é 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**

Adicionar chave RSA

Etapa 6. Em Cert Enrollment, selecione o ponto de confiança no menu suspenso que acabou de ser criado e clique em 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*:

FTD-A-7.4.1

Cert Enrollment*:

ssl_certificate +

Cert Enrollment Details:

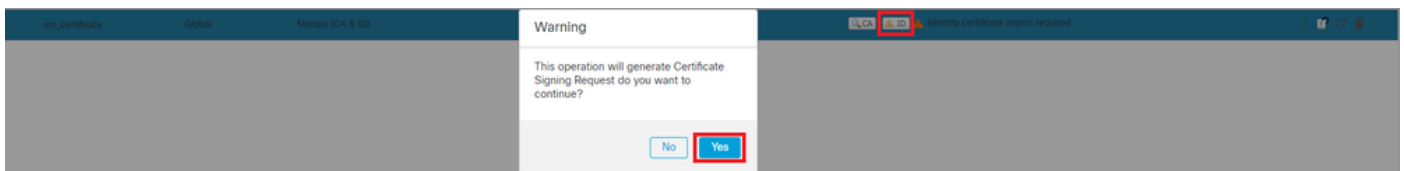
Name: ssl_certificate
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Cancel

Add

Adicionar novo certificado

Passo 7. Clique em ID e, em seguida, clique em Yes no prompt seguinte para gerar o CSR.



Gerar CSR

Etapa 8. Copie o CSR e assine-o pela autoridade de certificação. Assim que o certificado de identidade for emitido pela CA, importe-o clicando em Browse Identity Certificate e clique em 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/e3PDccc3eC57e+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



Observação: se a emissão do certificado de ID demorar, você poderá repetir a Etapa 7 mais tarde. Isso gerará o mesmo CSR e podemos importar o certificado de ID.

b. Adicionar um Certificado CA Confiável/Interno



Observação: se a Autoridade de Certificação (CA) usada na etapa (a), "**Criar/Importar um Certificado Usado para Autenticação de Servidor**" também emitir certificados de usuário, você poderá ignorar a etapa (b), "**Adicionar um Certificado de CA Confiável/Interno**". Não há necessidade de adicionar o mesmo certificado CA novamente e ele também deve ser evitado. Se o mesmo certificado CA for adicionado novamente, o ponto confiável é configurado com "validation-usage none", o que pode afetar a autenticação do certificado para RAVPN.

Etapa 1. Navegue até Devices > Certificates e clique em Add.

Selecione Device e clique no sinal de mais (+) em Cert Enrollment.

Aqui, "auth-risaggar-ca" é usado para emitir certificados de identidade/usuário.

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

Etapa 2. Insira um nome de ponto confiável e selecione Manual como o tipo de inscrição em CA information.

Etapa 3. Marque CA Only e cole o certificado CA confiável/interno no formato pem.

Etapa 4. Marque **Skip Check for CA flag in basic constraints of the CA Certificate** clique em Save.

Add Cert Enrollment ?

Internal_CA

Description

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type: Manual

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

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
--  
MIIG1jCCBL6gAwIBAgIQQAFu  
+wogXPrr4Y9x1zq7eDANBgk  
qhkiG9w0BAQsFADBK  
MQswCQYDVQQGEwJVUzES  
MBAGA1UEChMJSWRlbiRydX  
N0MScwJQYDVQQDEw5JZGVu  
u  
VHJ1c3QgQ29tbWV5Y2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage: IPsec Client SSL Client SSL Server

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

Cancel Save

Adicionar ponto confiável

Etapa 5. Em Cert Enrollment, selecione o ponto de confiança no menu suspenso que acabou de ser criado e clique em 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

Adicionar CA interna

Etapa 6. O certificado adicionado anteriormente é mostrado como:

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

Certificado Adicionado

c. Configure o pool de endereços para usuários de VPN

Etapa 1. Navegue até Objects > Object Management > Address Pools > IPv4 Pools .

Etapa 2. Insira o nome e o intervalo de endereços IPv4 com uma 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

Adicionar Pool de IPv4

d. Fazer upload de imagens de cliente seguras

Etapa 1. Faça o download de imagens de cliente seguras de implantação na Web conforme o SO do site do [software Cisco](#).

Etapa 2. Navegue até Objects > Object Management > VPN > Secure Client File > Add Secure Client File .

Etapa 3. Digite o nome e selecione o arquivo do Secure Client no disco.

Etapa 4. Selecione o tipo de arquivo como Secure Client Image e clique em Save.

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

Adicionar Imagem de Cliente Segura

e. Criar e fazer upload do perfil XML

Etapa 1. Faça o download e instale o Secure Client Profile Editor a partir do [site do Cisco Software](#).

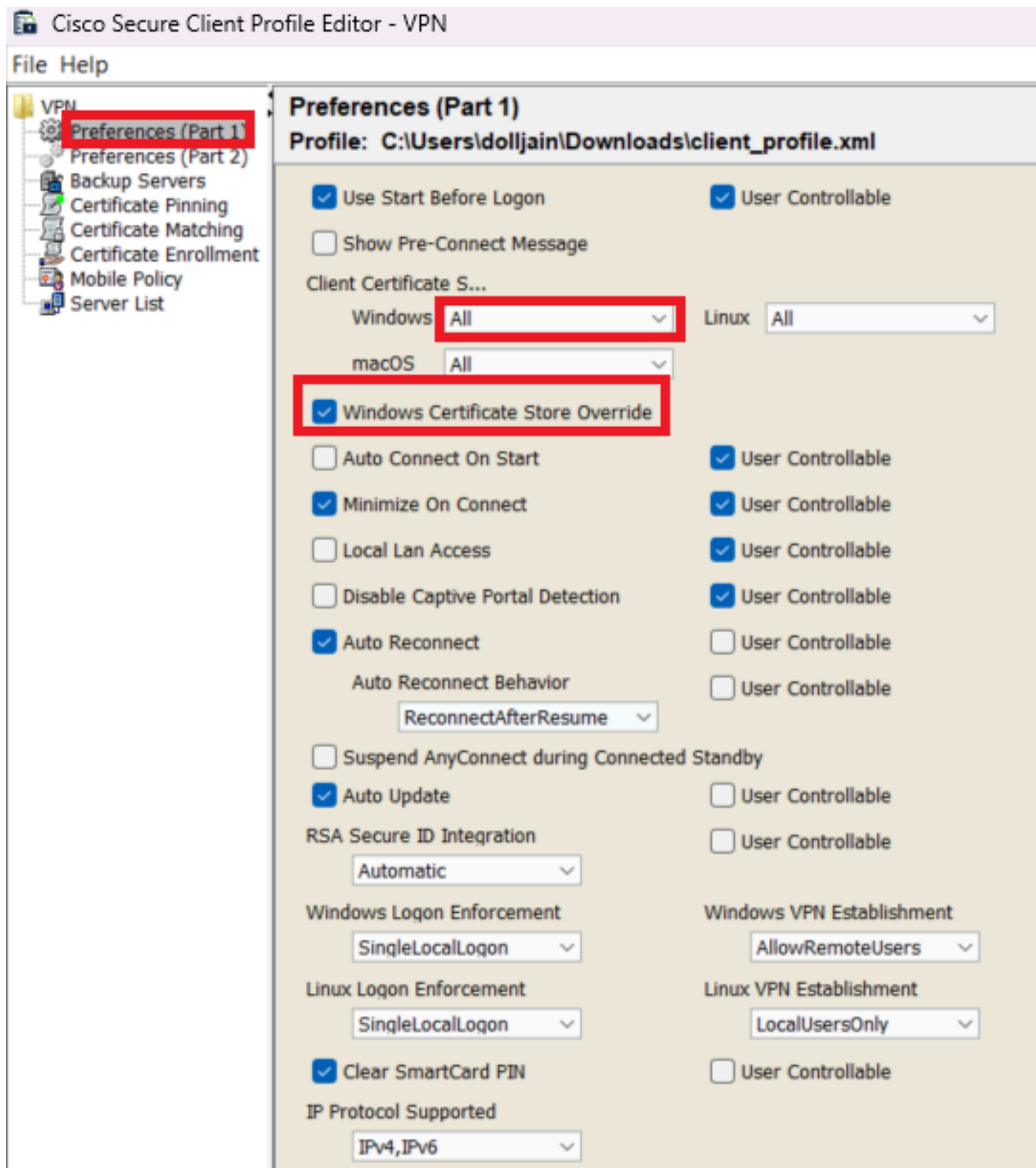
Etapa 2. Crie um novo perfil e selecione All no menu suspenso Seleção de certificado do cliente. Ele controla principalmente quais armazenamentos de certificados o Secure Client pode usar para armazenar e ler certificados.

Duas outras opções disponíveis são:

- **Computador** - o Cliente Seguro está restrito à pesquisa de certificado no repositório de certificados do computador local do Windows.
- **Usuário** - o Cliente Seguro está restrito à pesquisa de certificado no repositório local de certificados de usuário do Windows.

Definir Substituição de Repositório de Certificados como True .

Isso permite que um administrador instrua o Cliente Seguro a utilizar certificados no armazenamento de certificados da máquina Windows (Sistema Local) para autenticação de certificado de cliente. A Substituição do armazenamento de certificados aplica-se somente ao SSL, onde a conexão é iniciada, por padrão, pelo processo da interface do usuário. Ao usar IPsec/IKEv2, esse recurso no perfil de cliente seguro não é aplicável.



Adicionar preferências (Parte1)

Etapa 3. (Opcional) Desmarque a opção Disable Automatic Certificate Selection, pois ela evita que o usuário solicite que selecione o certificado de autenticação.

- 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

Untrusted Network Policy

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

Allow Captive Portal Remediation

Remediation Timeout (min.)

Apply Last VPN Local Resource Rules

Captive Portal Remediation Browser Failover

Allow Manual Host Input

PPP Exclusion

User Controllable

PPP Exclusion Server IP

User Controllable

Enable Scripting

User Controllable

Terminate Script On Next Event

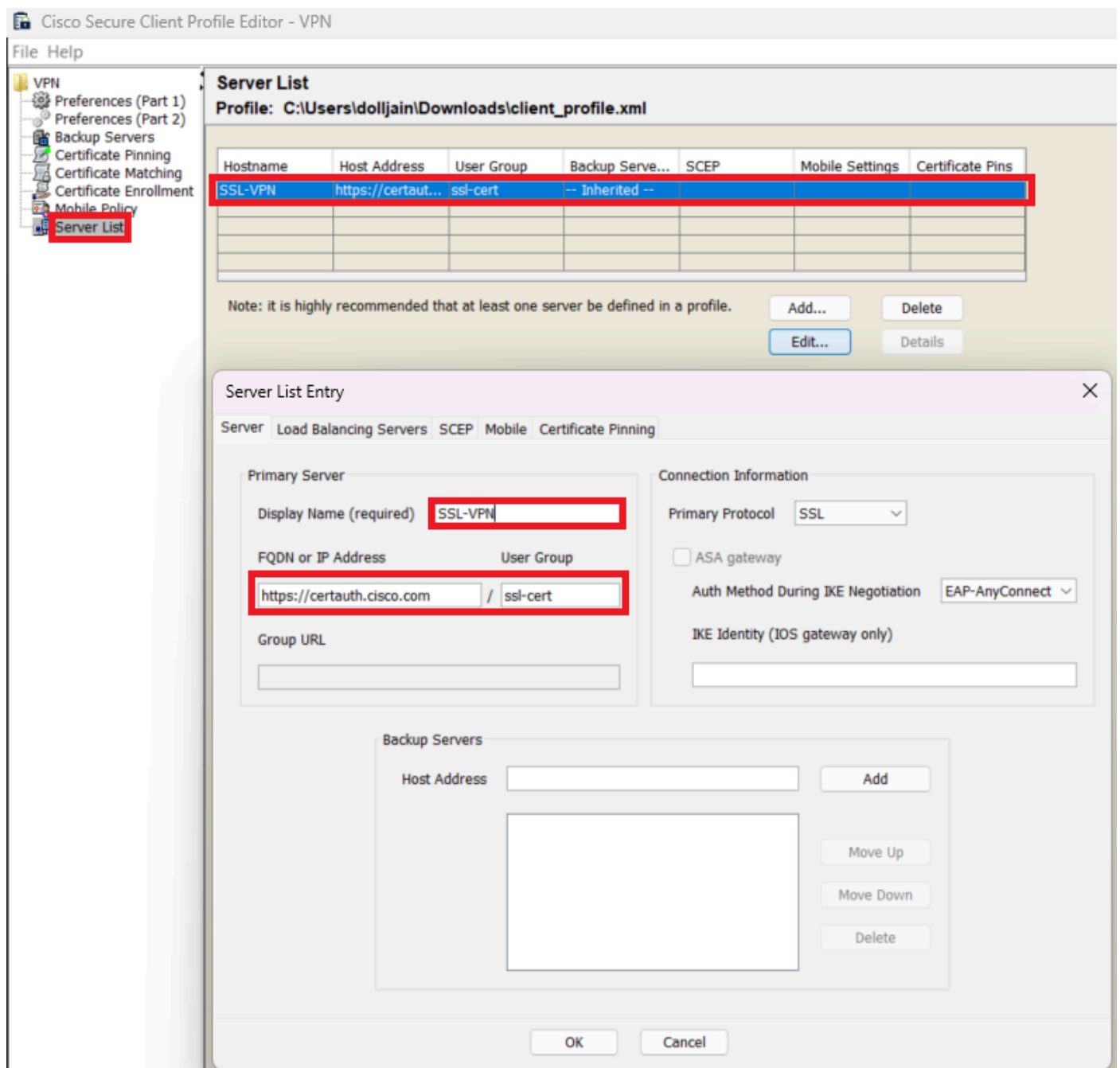
Enable Post SBL On Connect Script

Retain VPN on Logoff

User Enforcement

Authentication Timeout (seconds)

Server List Entry para configurar um perfil no Secure Client VPN fornecendo group-alias e group-url na Lista de servidores e salve o perfil XML.



Adicionar lista de servidores

Etapa 5. Finalmente, o perfil XML está pronto para uso.

```

<?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>All</CertificateStoreAll>
    <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 SecurID Integration UserControllable="false">Automatic</RSA SecurID Integration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVFNEstablishment>AllowRemoteUsers</WindowsVFNEstablishment>
    <LinuxVFNEstablishment>LocalUsersOnly</LinuxVFNEstablishment>
    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
    <PPPEXclusion UserControllable="false">Disable
      <PPPEXclusionServerIP UserControllable="false"></PPPEXclusionServerIP>
    </PPPEXclusion>
    <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

Local dos perfis XML para vários sistemas operacionais:

- **Windows** - C:\ProgramData\Cisco\Cisco Cliente seguro\VPN\Perfil
- **MacOS** - /opt/cisco/anyconnect/profile
- **Linux** - /opt/cisco/anyconnect/profile

Etapa 6. Navegue até Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile .

Digite o nome do arquivo e clique em Browse para selecionar o perfil XML. Clique em Save.

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

Adicionar perfil de VPN de cliente seguro

Configuração de VPN de acesso remoto

Etapa 1. Criar uma ACL de acordo com o requisito para permitir acesso a recursos internos.

Navegue até Objects > Object Management > Access List > Standard e clique em 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

Adicionar ACL padrão



Observação: essa ACL é usada pelo Secure Client para adicionar rotas seguras aos recursos internos.

Etapa 2. Navegue até `Devices > VPN > Remote Access` e clique em `Add`.

Etapa 3. Digite o nome do perfil, selecione o dispositivo FTD e clique em `Avançar`.

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.

Adicionar nome de perfil

Etapa 4. Insira o Connection Profile Name e selecione o Método de autenticação como Client Certificate Only em Authentication, Authorization and Accounting (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)

Selecionar método de autenticação

Etapa 5. Clique em Use IP Address Pools em Client Address Assignment e selecione o pool de endereços IPv4 criado 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: 

Selecionar Atribuição de Endereço de Cliente

Etapa 6. Edite a Diretiva 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 Política de Grupo

Passo 7. Navegue até General > Split Tunneling , selecione Tunnel networks specified below e selecione Standard Access List em Tipo de lista de rede de túnel dividido.

Selecione a ACL criada 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

Adicionar tunelamento dividido

Etapa 8. Navegue até Secure Client > Profile , selecione o Client Profile e clique em 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](#).

Adicionar perfil de cliente seguro

Etapa 9. Clique em Next, selecione o Secure Client Image e clique em 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 ▾

Adicionar Imagem de Cliente Segura

Etapa 10. Selecione a Interface de rede para acesso VPN, escolha a opção Device Certificates e marque sysopt permit-vpn e clique em 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.

Adicionar Controle de Acesso para Tráfego VPN

Etapa 11. Finalmente, revise todas as configurações e clique em 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.

Configuração da Política de VPN de Acesso Remoto

Etapa 12. Quando a configuração inicial da VPN de acesso remoto estiver concluída, edite o Perfil de conexão criado e vá para Aliases.

Etapa 13. Configure group-alias clicando no ícone de adição (+).

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 do grupo

Etapa 14. Configure group-url clicando no ícone de adição (+). Use a mesma URL de grupo configurada anteriormente no Perfil do 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 do grupo

Etapa 15. Navegue até Interfaces de acesso. Selecione Interface Trustpoint e nas SSL Global Identity Certificate configurações de SSL.

RAVPN

Enter Description

Local Realm: cisco-local 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

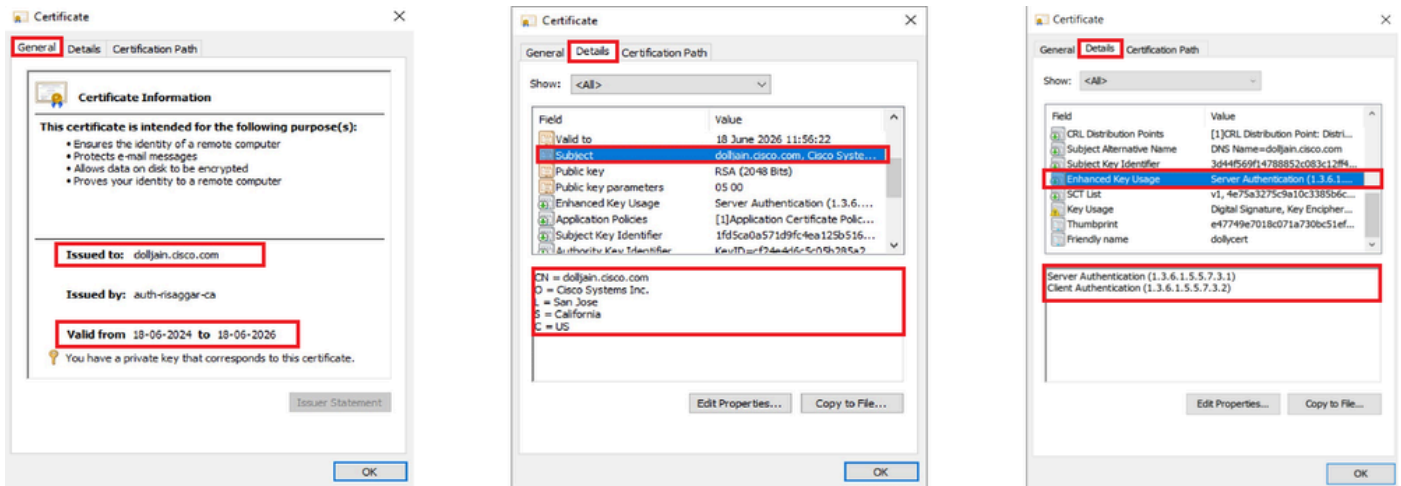
Editar interfaces de acesso

Etapa 16. CliqueSave e implante essas alterações.

Verificar

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

1. O PC cliente seguro deve ter o certificado instalado com uma data, assunto e ECU válidos no PC do usuário. Este certificado deve ser emitido pela CA cujo certificado está instalado no FTD, como mostrado anteriormente. Aqui, a identidade ou o certificado do usuário é emitido por "auth-risaggar-ca".

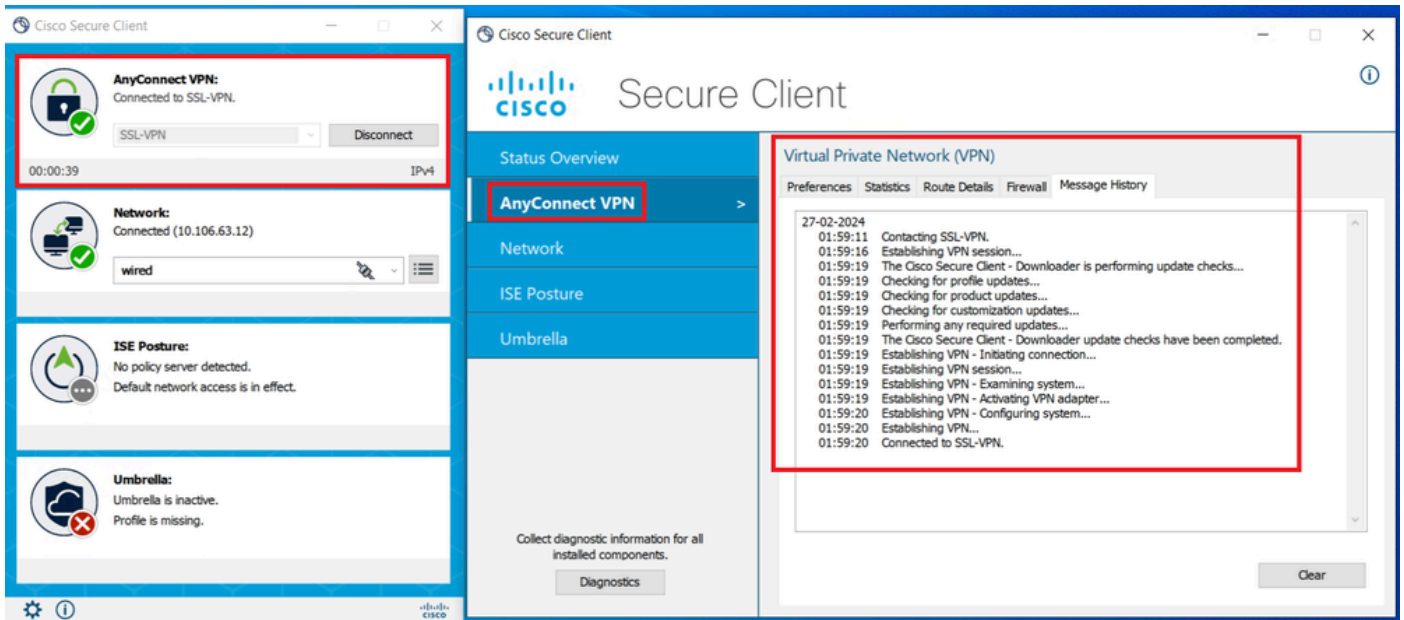


Destaques do certificado



Observação: o certificado do cliente deve ter o EKU (Enhanced Key Usage) de "Autenticação do cliente".

2. O Cliente Seguro deve estabelecer a conexão.



Conexão de Cliente Seguro Bem-sucedida

3. Execute `show vpn-sessiondb anyconnect` para confirmar os detalhes de conexão do usuário ativo no grupo de túneis usado.

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

Troubleshooting

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

1. As depurações podem ser executadas a partir da CLI de diagnóstico do FTD:

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

2. Consulte este [guia](#) para obter informações sobre problemas comuns.

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.