# Configuración de AAA y autenticación de certificado para Secure Client en FTD a través de FMC

## Contenido

**Introducción Prerequisites Requirements** Componentes Utilizados **Antecedentes** Diagrama de la red **Configuraciones** Configuración en FMC Paso 1. Configuración de la interfaz FTD Paso 2. Confirmar licencia de cliente seguro de Cisco Paso 3. Agregar asignación de directiva Paso 4. Detalles de configuración para el perfil de conexión Paso 5. Agregar conjunto de direcciones para el perfil de conexión Paso 6. Agregar directiva de grupo para el perfil de conexión Paso 7. Configurar imagen de Secure Client para perfil de conexión Paso 8. Configurar acceso y certificado para el perfil de conexión Paso 9. Confirmar resumen para perfil de conexión Confirmar en CLI de FTD Confirmar en cliente VPN Paso 1. Confirmar certificado de cliente Paso 2. Confirmar CA Verificación Paso 1. Iniciar conexión VPN Paso 2. Confirmar sesiones activas en FMC Paso 3. Confirmar sesión VPN en CLI de FTD Paso 4. Confirmar comunicación con el servidor **Troubleshoot Referencia** 

## Introducción

Este documento describe los pasos para configurar Cisco Secure Client sobre SSL en FTD administrado por FMC con AAA y autenticación de certificados.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defence Virtual (FTD)
- Flujo de autenticación VPN

### **Componentes Utilizados**

- Cisco Firepower Management Center para VMWare 7.4.1
- Cisco Firewall Threat Defence Virtual 7.4.1
- Cisco Secure Client 5.1.3.62

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

A medida que las organizaciones adoptan medidas de seguridad más estrictas, la combinación de la autenticación de dos factores (2FA) con la autenticación basada en certificados se ha convertido en una práctica habitual para mejorar la seguridad y proteger frente al acceso no autorizado. Una de las funciones que puede mejorar significativamente la experiencia del usuario y la seguridad es la capacidad de rellenar previamente el nombre de usuario en Cisco Secure Client. Esta función simplifica el proceso de inicio de sesión y mejora la eficacia general del acceso remoto.

Este documento describe cómo integrar el nombre de usuario preconfigurado con Cisco Secure Client en FTD, asegurando que los usuarios puedan conectarse de forma rápida y segura a la red.

Estos certificados contienen un nombre común que se utiliza para fines de autorización.

- CA: ftd-ra-ca-common-name
- Certificado de cliente: sslVPNClientCN
- Certificado de servidor: 192.168.1.200

## Diagrama de la red

Esta imagen muestra la topología utilizada para el ejemplo de este documento.



Diagrama de la red

## Configuraciones

### Configuración en FMC

Paso 1. Configuración de la interfaz FTD

Navegue hasta Devices > Device Management, edite el dispositivo FTD de destino, configure la interfaz interna y externa para FTD en la pestaña Interfaces.

Para GigabitEthernet0/0,

- Nombre: externo
- · Zona de seguridad: outsideZone
- Dirección IP: 192.168.1.200/24

Para GigabitEthernet0/1,

- Nombre: inside
- Zona de seguridad: insideZone
- Dirección IP: 192.168.10.200/24

Firewall Management Center Devices / Secure Firewall Interfaces	Overview Overview	Analysis	Policies Devices	Objects Integration	De	ploy Q 🚱 🌣	∂ admin ∨ dual     cisc	SECURE
1 49 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets DHCP VTEP								
All Interfaces Virtual Tunnels					Q, Search by name	S	Add Int	erfaces ¥
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	۹.4
GigabitEthernet0/0	outside	Physical	outsideZone		192.168.1.200/24(Static)	Disabled	Global	/
GigabitEthernet0/1	inside	Physical	insideZone		192.168.10.200/24(Static)	Disabled	Global	/
GigabitEthernet0/2		Physical				Disabled		/
GigabitEthernet0/3		Physical				Disabled		/

Interfaz FTD

Paso 2. Confirmar licencia de cliente seguro de Cisco

Navegue hasta Devices > Device Management, edite el dispositivo FTD de destino, confirme la licencia de Cisco Secure Client en la pestaña Device.

Firewall Management Ce Devices / Secure Firewall Device S	enter Overview Analys Summary	is Policies Devices	Objects Integration		Depl	oy Q 💕 🌣 😧 admin ~ 🤐 sect
1	are	License			0	
Device Routing Interfaces	Inline Sets DHCP VTEP	License Types				
		Performance Tier:	FTDv5 - 100 Mbps			
General	12	Essentials:			m	<b>G</b> G
Name:	1.2171.4	Export-Controlled Features:				Cisco Firepower Threat Defense for VMware
Transfer Packets:	Ye	Malware Defense:	_			9A33F35ANSU
Troubleshoot:	Logs CLI Download	IPS:				2024-06-14 07:38:47
Mode:	Route				Zone:	UTC (UTC+0:00)
Compliance Mode:	None	Carrier:			n:	7.4.1
Performance Profile:	Defaul	URL:			Zone setting for	UTC (UTC+0:00)
TLS Crypto Acceleration:	Disable	Secure Client Premier:			based Rules:	
		Secure Client Advantage:				
Device Configuration:	Import Export Download	Secure Client VPN Only:				
OnBoarding Method:	Registration Ke	If a device already has Secure Client VPI Secure Client Deemler or Secure Client A	Only they cannot have			
		has Secure Client Premier or Secure Client A has Secure Client Premier or Secure Client have Secure Client VPN Only	nt Advantage it cannot			
Inspection Engine					gement	/
Inspection Engine:	Snort			Cancel	te Host Address:	1.1.1.1.49
Revert to Snort 2				Gancer	dary Address:	

Licencia de cliente seguro

#### Paso 3. Agregar asignación de directiva

Navegue hasta Devices > VPN > Remote Access, haga clic en el botón Add.

Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	¢	° 0	admin ~	cisco SECURE
													Add
Name				Status			Last Modified						
No configuration available Add a new configuration													

Agregar VPN de acceso remoto

Introduzca la información necesaria y haga clic en el botón Next.

- Nombre: ftdvpn-aaa-cert-auth
- Protocolos VPN: SSL
- Dispositivos objetivo: 1.x.x.49

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy	۹	<b>6</b> 0	admin ~	cisco SECURE
Overview Analysis Policies Devices Objects Integration      Remote Access VPN Policy Wizard     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*     Indivgn-aa-cert-auth     Description:     VPN Protocols:      VPN Protocols:	Before You Start Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Polcy. Authentication Server Configure LOCAL or Realm or RADUS 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 Clicoc	Deploy	Q		admin ∽	dere SECURE
✓ SSL         IPsec-KEv2         Targeted Devices:         Available Devices         Q. Search         1.1.4.9         Add	credentials to download it during the witzerd. 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.					
				Ca	ncel Bac	k Next

Asignación de políticas

#### Paso 4. Detalles de configuración para el perfil de conexión

Introduzca la información necesaria para el perfil de conexión y haga clic en el botón + situado junto al elemento Dominio local.

- Método de autenticación: certificado de cliente y AAA
- Servidor de autenticación: LOCAL
- · Nombre de usuario del certificado: campo específico de asignación
- Campo principal: CN (nombre común)
- Campo secundario: OU (unidad organizativa)

Firewall Management Center Overview Analysis	Policies Devices Objects Integration	Deploy	۹	<b>e</b> :	0	admin 🗸	esco SECURE
Remote Access VPN Policy Wizard							
1 Policy Assignment 2 Connection Profile 3 Secu	ure Client						
	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.* ftwon-aaa-cert-auth						
	This name is configured as a connection alias, it can be used to connect to the VPN gateway  Authoritization Authorization 8 Accounting (AAA):						
	Autoenucation, Autoenzation & Accounting (AVA):						
	Speciny the method or authentication (AAA, certificates or born), and the AAA servers that will be used for VPN connections.						
	Authentication Method: Client Certificate & AAA +						
	Authentication Server:* LOCAL   LOCAL    LOCAL						
	Local Realm.* +						
	Prefill username from certificate on user login window						
	Username From Certificate: Map specific field Use entire DN (Distinguished Name) as username						
	Primary Field: CN (Common Name)						
	Secondary Field: OU (Organisational Unit)						
Detalles del perfil de conexión							

Haga clic en Local de la lista desplegable Add Realm para agregar un nuevo rango local.

Firewall Management Center Integration / Other Integrations / Realms	Overview Analysis Policies Devices	Objects Integration			Deploy Q 🧬 🌣 🔕 admin 🗸 🖽 SECURE
Cloud Services Realms Identity Sources	High Availability eStreamer Host Input Client	Smart Software Manager On-Prem			
Realms Realm Sequences Sync Result	9				
					Compare Realms Add Realm 🗸
Name * Type	Description		Status O	Value	State
LocalRealmTest Local					Enabled Active Directory/LDAP

Agregar rango local

Introduzca la información necesaria para el rango local y haga clic en el botón Save.

- Nombre: LocalRealmTest
- Nombre de usuario: sslVPNClientCN



Nota: El nombre de usuario es igual al nombre común dentro del certificado del cliente

Name*	Description
LocalRealmTest	
Local User Configuration	
<ul> <li>ssIVPNClientCN</li> </ul>	
Username	
ssIVPNClientCN	
Password	Confirm Password

#### Add another local user

Save	Cancel

Detalles del rango local

#### Paso 5. Agregar conjunto de direcciones para el perfil de conexión

Haga clic en el botón edit junto al elemento IPv4 Address Pools.

Client Address Assignment:	
Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options ar selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.	8
Use AAA Server (Realm or RADIUS only)	
Use DHCP Servers	
Jse IP Address Pools	
IPv4 Address Pools:	
IPv6 Address Pools:	

Agregar conjunto de direcciones IPv4

Introduzca la información necesaria para agregar un nuevo conjunto de direcciones IPv4. Seleccione el nuevo conjunto de direcciones IPv4 para el perfil de conexión.

- Nombre: ftdvpn-aaa-cert-pool
- Intervalo de direcciones IPv4: 172.16.1.40-172.16.1.50

•	Máscara:	255.255.255.0
---	----------	---------------

### Add IPv4 Pool

Name* ftdvpn-aaa-cert-pool	
Description	
IPv4 Address Range*	
172.16.1.40-172.16.1.50	
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150	
Mask*	
255.255.255.0	
Allow Overrides	
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices	
<ul> <li>Override (0)</li> </ul>	
	Cancel Save
Detalles del conjunto de direcciones IPv4	
Dess 6. Agregor directive de grupe para el perfil de conevién	
Paso 6. Agregar directiva de grupo para el perm de conexión	
Haga clic en el botón + situado junto al elemento 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	
	Cancel Rack Next
	Canoor Dack Next

0

Agregar directiva de grupo

Introduzca la información necesaria para agregar una nueva directiva de grupo. Seleccione la

nueva directiva de grupo para el perfil de conexión.

- Nombre: ftdvpn-aaa-cert-grp
- Protocolos VPN: SSL

### Add Group Policy

Name:* ftdvpn-aaa-cert-grp	
Description:	
General Secure	Client Advanced
VPN Protocols IP Address Pools Banner DNS/WINS Split Tunneling	VPN Tunnel Protocol: Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel. SSL ☐ IPsec-IKEv2
	Cancel Save

0

Detalles de la directiva de grupo

Paso 7. Configurar imagen de Secure Client para perfil de conexión

Seleccione el archivo de imagen de cliente seguro y haga clic en el botón Next.



Seleccionar imagen de cliente seguro

#### Paso 8. Configurar acceso y certificado para el perfil de conexión

Seleccione Security Zone para la conexión VPN y haga clic en el botón + junto al elemento Certificate Enrollment.

· Grupo de interfaz/Zona de seguridad: outsideZone

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🌣 🚱 admin -> 🖓 dealer SECURE
Remote Access VPN Policy Wizard         1 Policy Assignment       2 Connection Profile         3 Secure Client       4 Access & Certificate         9 Summary	
Remote UserSecure ClientUterne	
AAA 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* outsideZone  + C 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.*	



Introduzca la información necesaria para el certificado de FTD e importe un archivo PKCS12 desde el equipo local.

- Nombre: ftdvpn-cert
- Tipo de inscripción: archivo PKCS12

### Add Cert Enrollment

Nam fto	ne* dvpn-cert				Î
Des	cription				
С	A Information	Certificate Paramet	ers Key Rev	ocation	
	Enrollment Type	e: PKCS12 File	*		
	PKCS12 File	* ftdCert.pfx		Browse PKCS12 File	
	Passphrase	·:			
	Validation Usage	e: 🗹 IPsec Client	- SSL Client 🗌 S	SSL Server	
		Skip Check f	or CA flag in basic co	nstraints of the CA Certificate	
					-
				Cancel Save	

Agregar certificado FTD

Confirme la información ingresada en el asistente Access & Certificate y haga clic en el botón Next.

0



Nota: habilite la política de omisión del control de acceso para el tráfico descifrado (sysopt permit-vpn), de modo que el tráfico VPN descifrado no esté sujeto a la inspección de la política de control de acceso.

Firewall Management Center Overview Analysis Po Devices / VPN / Setup Wizard	cies Devices Objects Integration	Deploy Q 🥩 🌣 🕢 admin 🗸 👘 SECURE
Remote Access VPN Policy Wizard		
1 Policy Assignment 2 Connection Profile 3 Secure Client	Access & Certificate S Summary	
Permote User	Secure Client Internet Outside VPN Corporate Resources	
	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:* outsideZone	
	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:* ftdvpn-cert +	
	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 (syspert permit-type) This option bypasses the Access Control Policy impection, but VPN fifter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.	
4		•
		Cancel Back Next

Confirmar configuración en Acceso y certificado

#### Paso 9. Confirmar resumen para perfil de conexión

Confirme la información introducida para la conexión VPN y haga clic en el botón Finish.



Confirmar configuración para la conexión VPN

Confirme el resumen de la directiva VPN de acceso remoto e implemente la configuración en FTD.

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects	Integration	Deploy Q 💕 🔅 🌘	admin ~ stude SECURE
ftdvpn-aaa-cert-auth				Save Cancel
Enter Description				
				Policy Assignments (1)
Connection Dealer Annual Interference Advanced			Local Realm: LocalRealmTest	Dynamic Access Policy: None
Connection Prome Access Interfaces Advanced				
				+
Name	AAA	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftrGrpPolicy	_	/1
ftdvpn-aaa-cert-auth	Authentication: Client Certificate & LOCAL Authorization: None Accounting: None	📑 ftdvpn-aaa-cert-grp		/1

Resumen de la directiva VPN de acceso remoto

### Confirmar en CLI de FTD

Confirme la configuración de la conexión VPN en la CLI de FTD después de la implementación desde el FMC.

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0
interface GigabitEthernet0/1
nameif inside
security-level 0
ip address 192.168.10.200 255.255.255.0
// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0
// Defines a local user
username sslVPNClientCN password ***** encrypted
// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
keypair ftdvpn-cert
crl configure
// Server Certificate Chain
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
. . . . . .
quit
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
. . . . . .
quit
// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
```

no preload hsts-client enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows" anyconnect enable tunnel-group-list enable cache disable error-recovery disable // Bypass Access Control policy for decrypted traffic // This setting is displayed in the 'show run all' command output sysopt connection permit-vpn // Configures the group-policy to allow SSL connections group-policy ftdvpn-aaa-cert-grp internal group-policy ftdvpn-aaa-cert-grp attributes banner none wins-server none dns-server none dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-tunnel-network-list none default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable // Configures the tunnel-group to use the aaa & certificate authentication tunnel-group ftdvpn-aaa-cert-auth type remote-access tunnel-group ftdvpn-aaa-cert-auth general-attributes address-pool ftdvpn-aaa-cert-pool default-group-policy ftdvpn-aaa-cert-grp // These settings are displayed in the 'show run all' command output. Start

authentication-server-group LOCAL secondary-authentication-server-group none no accounting-server-group default-group-policy ftdvpn-aaa-cert-grp username-from-certificate CN OU secondary-username-from-certificate CN OU authentication-attr-from-server primary authenticated-session-username primary username-from-certificate-choice second-certificate secondary-username-from-certificate-choice second-certificate // These settings are displayed in the 'show run all' command output. End tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes authentication aaa certificate pre-fill-username client group-alias ftdvpn-aaa-cert-auth enable

### Confirmar en cliente VPN

Paso 1. Confirmar certificado de cliente

Vaya a Certificates - Current User > Personal > Certificates, verifique el certificado de cliente utilizado para la autenticación.



Confirmar certificado de cliente

Haga doble clic en el certificado de cliente, navegue hasta Detalles, verifique los detalles de Asunto.

Asunto: CN = sslVPNClientCN

## 💼 Certificate

General	Details	Certification Pa	ath
Show:	<al></al>		$\sim$
Field			Value ^
Sig	nature al	gorithm	sha256RSA
Sig Sig	nature h	ash algorithm	sha256
	uer		ftd-ra-ca-common-name, Cisc
<b>Va</b>	id from		Sunday, June 16, 2024 6:12:0
1 Martine State	id to		Monday, June 16, 2025 6:12:
Su	bject	ana ana amin'ny sora	ssIVPNClientCN, ssIVPNClientO
Pu	blic key		RSA (2048 Bits)
Din Pu	hlir kev n	arameterc	05.00
CN = s O = Cis L = Tok S = Tok C = JP	siVPNClier sco cyo cyo	ntCN	Ч5
			Edit Properties
			OK

X

Detalles del certificado de cliente

### Paso 2. Confirmar CA

Navegue hasta Certificados - Usuario actual > Entidades de certificación raíz de confianza >

Certificados, verifique la CA utilizada para la autenticación.

• Emitido por : ftd-ra-ca-common-name

Console1 - [Console Root\Certificates - Curren File Action View Favorites Window (	t User\Trusted Root Certification A Help	Authoritid (Certificates)			-	-	× 8	×
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Actions		
Gertificates - Current User     Gertificates     Certificates     Gertificates     Gertificates     Gertificates     Gertificates	COMODO RSA Certificati Copyright (c) 1997 Micros ESKTOP-VCKHRG1 DigiCert Assured ID Root	COMODO RSA Certificati Copyright (c) 1997 Micros DESKTOP-VCKHRG1 DigiCert Assured ID Root	1/18/2038 12/30/1999 10/30/2022 11/9/2031	Client Authenticati Time Stamping Server Authenticati <all></all>	Sectigo (forr Microsoft Tii www.infraey <none></none>	Certificat Mor ftd-ra-ca	es 4	•
Cincerprise Trust     Cincerprise Trust     Cincerprise Trust     Cincerprise Trust     Cincerprise Trust     Cincerprise Trusted Publishers     Cincerprise Certificates     Cincerprise Certificates     Cincerprise People     Cincerprise Certification Authoritie     Cincerprise Certification Certification	DigiCert Assured ID Root DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance DigiCert High Assurance DigiCert Trusted Root G4	DigiCert Assured ID Root DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance DigiCert High Assurance DigiCert Trusted Root G4 DCT Root CA X2	11/9/2031 11/9/2031 1/15/2038 11/9/2031 11/9/2031 1/15/2038 0/30/2031	Client Authenticat Client Authenticati Client Authenticati Client Authenticati Client Authenticati	DigiCert DigiCert Glol <none> DigiCert DigiCert Tru: DCT Reat C</none>	Mor	e )	,
Client Authentication Issuers     Smart Card Trusted Roots     Great Card Trusted Computer)	GlobalSign	ftd-ra-ca-common-name ClobalSign GlobalSign	6/16/2029 2/19/2020 12/15/2021	Client Authenticati	ClobalCiga Google Trust			

## Verificación

Paso 1. Iniciar conexión VPN

En el terminal, inicie la conexión de Cisco Secure Client. El nombre de usuario se extrae del certificado del cliente, debe ingresar la contraseña para la autenticación VPN.



Nota: El nombre de usuario se extrae del campo CN (Common Name) del certificado de cliente en este documento.

Sisco Secure Client	- 0	$\times$	S Cisco Secure Client   192.168.1.200	×	Sisco Secure Client	×
AnyConnect VPI: Contacting 192.168.1.200. 192.168.1.200	✓ Connect		Group: ftdvpn-aaa-cert-auth ~		AnyConnect VPH: Connected to 192.168.1.200. 192.168.1.200	V Disconnect
			Password:		00:00:07	IPv4
<b>\$</b> ①		ulualu cisco		_	\$	altada CISCO
			OK Cancel			

Iniciar conexión VPN

Paso 2. Confirmar sesiones activas en FMC

Navegue hasta Análisis > Usuarios > Sesiones activas, verifique la sesión activa para la autenticación VPN.

þ	Eriewall Management Center Overview Analysis Desices Desices Objects Integration Deploy Q 💞 O 😦 admin v 🚓 SEL									SECURE							
															•	Switch	to legacy UI
T :	elect														×	efresh	Log Out
0	howing the 1 and only session	<u>+</u>															B
	Looin.Time	Realm/Username	Last.Seen 4	Authentication Type	Current.IP	Basics	Usemame	ExtName	Last.Name	Email	Department	Phone Number	Discovery Application	Device			^
	2024-06-17 11:38:22	LocalRealmTest(ssIVPNClientCN	2024-06-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	ssIVPNClientCN						LDAP	1.	149		

Confirmar sesión activa

### Paso 3. Confirmar sesión VPN en CLI de FTD

Ejecuteshow vpn-sessiondb detail anyconnect el comando en la CLI de FTD (Line) para confirmar la sesión VPN.

ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 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 : 14780 Bytes Rx : 15386 Pkts Tx: 2 Pkts Rx: 37 Pkts Tx Drop: 0 Pkts Rx Drop: 0 Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth Login Time : 02:38:22 UTC Mon Jun 17 2024 Duration : 0h:01m:22s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : cb00718200007000666fa19e Security Grp: none Tunnel Zone: 0

AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1

AnyConnect-Parent: Tunnel ID : 7.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 50035 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : win Client OS ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7390 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 7.2 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Encryption : AES-GCM-128 Hashing : SHA256 Ciphersuite : TLS\_AES\_128\_GCM\_SHA256 Encapsulation: TLSv1.3 TCP Src Port : 50042 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7390 Bytes Rx : 2292 Pkts Tx : 1 Pkts Rx : 3 Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel: Tunnel ID : 7.3 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 56382 UDP Dst Port : 443 Auth Mode : Certificate and 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 5.1.3.62 Bytes Tx : 0 Bytes Rx : 13094 Pkts Tx : 0 Pkts Rx : 34 Pkts Tx Drop : 0 Pkts Rx Drop : 0

Paso 4. Confirmar comunicación con el servidor

Inicie el ping desde el cliente VPN al servidor, confirme que la comunicación entre el cliente VPN y el servidor es exitosa.

C:\Users\CALO>ping 192.168.10.11
Pinging 192.168.10.11 with 32 bytes of data: Reply from 192.168.10.11: bytes=32 time=12ms TTL=128 Reply from 192.168.10.11: bytes=32 time=87ms TTL=128 Reply from 192.168.10.11: bytes=32 time=3ms TTL=128 Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Ping statistics for 192.168.10.11: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 3ms, Maximum = 87ms, Average = 26ms

Ping correcto

Ejecute capture in interface inside real-time el comando en la CLI de FTD (Line) para confirmar la captura de paquetes.

#### <#root>

```
ftd702#
```

#### capture in interface inside real-time

#### Use ctrl-c to terminate real-time capture

1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request 2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply 3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request 4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply 5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request 6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply 7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request 8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo request

#### Troubleshoot

Puede esperar encontrar información sobre la autenticación VPN en el registro del sistema de depuración del motor de línea y en el archivo DART en la PC con Windows.

Este es un ejemplo de los logs de debug en el motor Lina.

#### // Certificate Authentication

Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=ssIV Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked. Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=ssIVPNClientCL

#### // Extract username from the CN (Common Name) field

Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 5] Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 5]

// AAA Authentication

Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN

Estas depuraciones se pueden ejecutar desde la CLI de diagnóstico del FTD, que proporciona información que puede utilizar para solucionar problemas de configuración.

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

Configuración de la Autenticación Basada en Certificados de Anyconnect para el Acceso Móvil

### 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).