Configurar la coincidencia de certificados para la autenticación de cliente seguro en FTD a través de FDM

Contenido

Introducción Prerequisites Requirements Componentes Utilizados **Antecedentes** Diagrama de la red **Configuraciones** Configuración en FDM Paso 1. Configuración de la interfaz FTD Paso 2. Confirmar licencia de cliente seguro de Cisco Paso 3. Agregar conjunto de direcciones Paso 4. Crear perfil de cliente seguro Paso 5. Cargar perfil de cliente seguro en FDM Paso 6. Agregar directiva de grupo Paso 7. Agregar certificado FTD Paso 8. Agregar CA al FTD Paso 9. Agregar perfil de conexión VPN de acceso remoto Paso 10. Confirmar resumen para perfil de conexión Confirmar en CLI de FTD Confirmar en cliente VPN Paso 1. Copiar perfil de cliente seguro en cliente VPN Paso 2. Confirmar certificado de cliente Paso 3. Confirmar CA **Verificación** Paso 1. Iniciar conexión VPN Paso 2. Confirmar sesiones VPN en CLI de FTD **Troubleshoot** Información Relacionada

Introducción

Este documento describe cómo configurar Cisco Secure Client con SSL en FTD a través de FDM mediante la coincidencia de certificados para la autenticación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defence Virtual 7.2.8
- Cisco Secure Client 5.1.4.74
- Editor de perfiles (Windows) 5.1.4.74

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

CertificateMatch es una función que permite a los administradores configurar criterios que el cliente debe utilizar para seleccionar un certificado de cliente para la autenticación con el servidor VPN. Esta configuración se especifica en el perfil de cliente, que es un archivo XML que se puede administrar mediante el Editor de perfiles o editarse manualmente. La función CertificateMatch se puede utilizar para mejorar la seguridad de las conexiones VPN asegurándose de que sólo se utilice un certificado con atributos específicos para la conexión VPN.

Este documento describe cómo autenticar Cisco Secure Client utilizando el nombre común de un certificado SSL.

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

- CA: ftd-ra-ca-common-name
- Certificado de cliente VPN del ingeniero: vpnEngineerClientCN
- Certificado de cliente VPN del administrador: vpnManagerClientCN
- 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 FDM

Paso 1. Configuración de la interfaz FTD

Navegue hasta Device > Interfaces > View All Interfaces, configure la interfaz interna y externa para FTD en la pestaña Interfaces.

Para GigabitEthernet0/0,

- Nombre: fuera
- Dirección IP: 192.168.1.200/24

Firewall Device Manager Monitoring Po	Dicies Objects	Device: firepower				? : at	dmin dministrator	cisco SECURE
Device Summary Interfaces								
Cisco Firepower Threat Defense for VMware (0/0 0/1 0/2 0/3 0/4 0/5 0/6 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	0/7							
Interfaces Virtual Tunnel Interfaces								
9 Interfaces					T Filb	er		+
NAME	LOGICA	AL NAME STATUS	S MODE	IP ADDRESS		STANDBY ADDRESS		ACTIONS
> 🗸 GigabitEthernet0/0	outside	le C	Routed	192.168.1.200 Static			Enabled	

Interfaz FTD

Paso 2. Confirmar licencia de cliente seguro de Cisco

Vaya a Device > Smart License > View Configuration, confirme la licencia de Cisco Secure Client en el elemento RA VPN License.



Licencia de cliente seguro

Paso 3. Agregar conjunto de direcciones

Navegue hasta Objetos > Redes, haga clic en el botón +.

Firewall Device Manag	ger Monitoring Policies Objects Device	:: firepower	(>) (a) (a) (?) (admin Administrator	cisco SECURE
Ôbject Types ←	Network Objects and Groups			
C Networks	7 objects		T Filter	+ 🕫
S Ports			Preset filters: System defined, User defined	
Security Zones	* NAME	TYPE VALUE		ACTIONS
Application Siltere	1 IPv4-Private-10.0.0.0-8	NETWORK 10.0.0/8		

Agregar conjunto de direcciones

Introduzca la información necesaria para agregar un nuevo conjunto de direcciones IPv4. haga clic en el botón Aceptar.

- Nombre: ftd-cert-match-pool
- · Tipo: Rango
- Intervalo IP: 172.16.1.150-172.16.1.160

Add Network Object

Name	
ftd-cert-match-pool	
Description	
	h
Туре	
○ Network ○ Host ○ FQDN	
IP Range	
172.16.1.150-172.16.1.160	
e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::	:100
CANCEL	~~~

ค

Detalle del pool de direcciones IPv4

Paso 4. Crear perfil de cliente seguro

Descargue e instale Secure Client Profile Editor desde el sitio <u>Cisco Software</u>. Navegue hasta Lista de servidores, haga clic en el botón Agregar. Introduzca la información necesaria para agregar una entrada de lista de servidores y haga clic en el botón Aceptar.

- Nombre para mostrar: cert-match
- FQDN o dirección IP: 192.168.1.200
- · Protocolo principal: SSL

VPN Preferences (Part 1) Preferences (Part 2)	Server List Profile: Untitled		
Backup Server's Certificate Printing Certificate Platching Certificate Incolliment	Hostname Host Addr User Group Backup Se	r SCEP Mobile Sett Certificate er be define II Ad Del Edit Det	
		Server List Entry	la Cartificata Dinaina
		Primary Server Display Name (required) cert-match FQDN or IP A User Gri 192.168.1.200 / Group URL 192.168.1.200	Connection Information Primary Protocol SSL Dup ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only)
		Backup Servers Host Address	Add Move Up Move D Delete
			K Cancel

Entrada de lista de servidores

Navegue hasta Coincidencia de certificado, haga clic en el botón Agregar. Introduzca la información necesaria para agregar una entrada de nombre distinguido y haga clic en el botón Aceptar.

- Nombre: CN
- Patrón: vpnEngineerClientCN
- Operador: Equal



Nota: Marque la opción MatchCase en este documento.

Cisco Secure Client Profile Editor	- VPN								
VPN	Certificate Matching Profile: C:\Users\jianzh3\OneDrive - Cisco\Desktop\vpnClient.xml								
Preferences (Part 2) Reackup Servers Certificate Disolog Certificate Matching Mobile Policy Server List	Key Usag Dec End CRL Key Data Key Non Digi	e jpher_Only jher_Only _Sign _Cert_Sign _Agreem _Encipher _Encipherm _Repudiat tal_Signa		te					
	Custom E	ch only certifi	cates with K cates with K	Key Usage Extended Ke	y Usage		Distinguished Name Entry Name CN Pattern VpnEngineerClient Operator Equal Not Equal Wildcard		
	Distinguis	hed Name (N	fax			Add	MatchCase		
	Name	Pattern	wiidcard	Operator	MatchC	Edit Delete	OK Cancel		

Entrada de nombre distinguido

Guarde el perfil de cliente seguro en el equipo local y confirme los detalles del perfil.

▼ <certificatematch> <matchoplycertswithku>false< MatchOplyCerts</matchoplycertswithku></certificatematch>	sWi+bK115
<pre></pre>	qual" Wildcard="Disabled" MatchCase="Enabled">
	hlo="foloo"\
* senableAutomaticServerSelection UserControlia false	able= talse 2
<pre><autoserverselectionimprovement>20</autoserverselectionimprovement></pre>	rverSelectionImprovement>
<autoserverselectionsuspendtime>4</autoserverselectionsuspendtime> 444 <th>verSelectionSuspendTime></th>	verSelectionSuspendTime>
<retainvpnunlogoff>false <th></th></retainvpnunlogoff>	
 CaptivePortalRemediationBrowserFailover>tals 	se
<pre><allowmanualhostinput <="" allowmanualhostin="" clientinitialization="" true<=""></allowmanualhostinput></pre>	nput/
Cerverlist>	
▼ (HostEntry)	
<hostname>cert-match</hostname>	
<pre><hostaddress>192.168.1.200</hostaddress></pre>	
(AselverList)	
AnyConnectProf Lle2</td <th></th>	

Perfil de cliente seguro

Paso 5. Cargar perfil de cliente seguro en FDM

Navegue hasta Objetos > Perfil de cliente seguro, haga clic en el botón CREAR PERFIL DE CLIENTE SEGURO.

Firewall Device Manager Monitoring	Policies Objects Device: firepower	S. 🚑 🗐 ? : admin	sco SECURE
Object Types ←	Secure Client Profiles		
C Networks		Y Filter	+
S Ports	# NAME	FILE NAME ACTIONS	
G Security Zones			_
🐬 Application Filters		There are no Secure Client profile objects yet.	
C ⁹ URLs		Start by creating the first Secure Client profile object.	
© Geolocations		CREATE SECURE CLIENT PROFILE	
Syslog Servers			
✗ IKE Policies			
🔹 IPSec Proposals			
Secure Client Profil			
S Identity Sources			

Crear perfil de cliente seguro

Introduzca la información necesaria para agregar un perfil de cliente seguro y haga clic en el botón Aceptar.

- Nombre: secureClientProfile
- Perfil de cliente seguro: secureClientProfile.xml (carga desde el equipo local)

Add Secure Client Profile						
Name secureClientProfile						
Description						
		4				
Secure Client Profile UPLOAD secureClientProfile.xml						
CANCEL	ОК					

Agregar perfil de cliente seguro

Paso 6. Agregar directiva de grupo

Vaya a Device > Remote Access VPN > View Configuration > Group Policies, haga clic en el botón +.

Firewall Device M	anager Monitor	ing Policies	註 Objects	Device: fi	repower	(5.) 🖨	0	?	÷	admin Administrator	×	cisco SECURE
RA VPN ←	Device Summa Group Po	n plicies											
Connection Profiles	2 objects							T P	ilter				+
SAML Server	• NAME				DNS SERVER	IPV4 SPLIT TUNNELING	IPV6	SPLIT TUN	NELING		SECURE CLIENT PROF	ILES	ACTIONS
	1 DfltGrpF	olicy				Allow all traffic	Alk	w all traf	fic				

Agregar directiva de grupo

Introduzca la información necesaria para agregar una directiva de grupo y haga clic en el botón Aceptar.

- Nombre: ftd-cert-match-grp
- Perfiles de Secure Client: secureClientProfile

Add Group Policy		0	×
Q Search for attribute	Name		
Basic	ftd-cert-match-grp Description		
Session Settings			10
Advanced Address Assignment	DNS Server Select DNS Group		,
Split Tunneling Secure Client	Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session		
Traffic Filters Windows Browser Proxy	Secure Client profiles		
	▼ Filter		
	secureClientProfile Create new Secure Client Prof CANCEL OK		
	CANCEL	ок	

Detalles de la directiva de grupo

Paso 7. Agregar certificado FTD

Navegue hasta Objetos > Certificados, haga clic en Agregar certificado interno desde el elemento +.

Firewall Device Mana	ager Monitoring Policies Objects Device:	(interview)	o 🖨 🗐 🖓 🗄	admin Administrator Y the SECURE
Object Types ←	Certificates			
C Networks	121 objects		T Filter	+ × 👩 ×
S Ports			Preset filters: System defined, User defined	Add Internal CA
8 Security Zones	N NAME	туре		Add Internal Certificate ACTIONS
🐬 Application Filters	1 AAA-Certificate-Services	Trusted CA Certificate		Add Trusted CA Certificate
C URLs	2 ACCVRAIZ1	Trusted CA Certificate		
Geolocations	3 Actalis-Authentication-Root-CA	Trusted CA Certificate		
	4 AffirmTrust-Commercial	Trusted CA Certificate		
Syslog Servers	5 AffirmTrust-Networking	Trusted CA Certificate		
🔏 IKE Policies	6 AffirmTrust-Premium	Trusted CA Certificate		
🛶 IPSec Proposals	7 AffirmTrust-Premium-ECC	Trusted CA Certificate		
Secure Client Profiles	8 Amazon-Root-CA-1	Trusted CA Certificate		
💼 Identity Sources	9 Amazon-Root-CA-2	Trusted CA Certificate		
1 Users	10 Amazon-Root-CA-3	Trusted CA Certificate		
Cartificator	11 DefaultInternalCertificate	Internal Certificate		
and the second s	12 DefaultWebserverCertificate	Internal Certificate		

Agregar certificado interno

Haga clic en Cargar certificado y clave.



Cargar certificado y clave

Introduzca la información necesaria para el certificado FTD, importe un certificado y una clave de certificado desde el equipo local y, a continuación, haga clic en el botón Aceptar.

- Nombre: ftd-vpn-cert
- Uso de validación para servicios especiales: servidor SSL



Detalles del certificado interno

Paso 8. Agregar CA al FTD

Navegue hasta Objetos > Certificados, haga clic en Agregar certificado de CA de confianza desde el elemento +.

Firewall Device Manager	Monitoring Policies Objects Device: fireport	wer (>_ (@) (?) :	admin Administrator
🐬 Application Filters	Cortificator		
🖉 URLs	Certificates		
Geolocations	120 objects	T Filter	+ - 🛃 -
E Durley Desum		Preset filters: System defined. User defined	Add Internal CA
Syslog Servers	# NAME	туре	Add Internal Certificate ACTIONS
🔎 IKE Policies	1 NGFW-Default-InternalCA	Internal CA	Add Trusted CA Certificate
🛖 IPSec Proposals	2 AAA-Certificate-Services	Trusted CA Certificate	
Secure Client Profiles	3 ACCVRAIZ1	Trusted CA Certificate	
🚉 Identity Sources	4 Actalis-Authentication-Root-CA	Trusted CA Certificate	
1 Users	5 AffirmTrust-Commercial	Trusted CA Certificate	
Q Certificates	6 AffirmTrust-Networking	Trusted CA Certificate	
	7 AffirmTrust-Premium	Trusted CA Certificate	
- Secret Keys	- ME-T Possible FOO	T	

Agregar certificado de CA de confianza

Introduzca la información necesaria para la CA e importe un certificado desde el equipo local.

- Nombre: ftdvpn-ca-cert
- Uso de validación para servicios especiales: cliente SSL

Add Trusted CA Certificate	0 ×
Name ftdvpn-ca-cert	
Certificate Paste certificate, or choose a file (DER, PEM, CRT, CER)	ftd-ra-ca.crt Upload.Certificate
BEGIN CERTIFICATE MIIDbDCCA1SgAwIBAgIIUkKgLg229/0wDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUb2t5bzEOMAwGA1UEChMF	•
Skip CA Certificate Check	
Validation Usage for Special Services	
SSL Client ×	~
CANCEL	ОК

Paso 9. Agregar perfil de conexión VPN de acceso remoto

Vaya a Device > Remote Access VPN > View Configuration > Connection Profiles, haga clic en el botón CREATE CONNECTION PROFILE.

Firewall Device M	anager Monitoring	Policies	33. Objects	Device: firepower	(Σ)			e admin e Administrator	 diale SECURE
RA VPN ←		Device Summary Remote A	, ccess V	/PN Connection Profiles					
Group Policies							T Filter		+
SAML Server		•	NAME	AAA	GROUP POLICY			ACTIONS	
				There	e are no Remote Access Co Start by creating the first Co	nnection	s yet.		
					CREATE CONNECTION PR	OFILE			

Agregar perfil de conexión VPN de acceso remoto

Introduzca la información necesaria para el perfil de conexión y haga clic en el botón Next.

- Nombre del perfil de conexión: ftd-cert-match-vpn
- Tipo de autenticación: sólo certificado de cliente
- · Nombre de usuario del certificado: campo específico de asignación
- Campo principal: CN (nombre común)
- Campo secundario: OU (unidad organizativa)
- Conjuntos de direcciones IPv4: ftd-cert-match-pool

Firewall Device Manager Monitoring Policies	Objects Device: firepower	Section 2 → Secure admin admin administrator
Remote Access VPN	Connection and Client (2) Remote User Experience	3 Global Settings 4 Summary
Remote Users 🔲 Secure Cli	ients — Internet ········· Q Client Certificate ···· CUTISE	ree For User Authentication
	Connection and Client Config Specify how to authenticate remote users and the secure clients the inside network.	juration hey can use to connect to the
	Connection Profile Name This name is configured as a connection alias, it can be used to connect to the V ftd-cert-match-vpn	PM gateway
	Group Allas (one per line, up to 5) Group URL (one ftd-cert-match-vpn	per line, up to 5)
	Primary Identity Source Authentication Type Client Certificate Only	
	Username from Certificate Map Specific Field Primary Field CN (Common Name) V OU (Organisation OU (OU (Organisation OU (OU (OU (OU (OU (OU (OU (OU (OU (OU (onal Unit) 🗸
	 Use entire DN (distinguished name) as username Advanced 	
	Authorization Server Accounting Server Please select V Please select	~
	Client Address Pool Assignment IPv4 Address Pool Endpoints are provided an address from this pool * Control to the second and the second	d an address from this pool
	DHCP Servers CANCEL	

Detalles del perfil de conexión VPN

Introduzca la información necesaria para la política de grupo y haga clic en el botón Next.

• Ver directiva de grupo: ftd-cert-match-grp

Firewall Device Manager Monitoring Policies Objects	Device: firepower	> 🔮 🐵 ?	admin Administrator
Remote Access VPN	Connection and Client Configuration Remote User Experience	3 Global Settings	(4) Summary
Remote Users E Secure Cli	ents — Internet — R Client Certificate — BIELSYACE	INTEGRACES	Corporate Resources
	Remote User Experience A group policy is a collection of user-oriented session attributes which VPN connection is established. Select or create a Group View Group Policy Itd-cert-match-grp Policy Group Brief Details	e th are assigned to client when a up Policy object.	
	Banner Text for Authendia BACK		

Seleccionar directiva de grupo

Seleccione Certificate of Device Identity, Outside Interface, Secure Client Package para la conexión VPN.

- Certificado de identidad del dispositivo: ftd-vpn-cert
- Interfaz externa: externa (GigabitEthernet0/0)
- Paquete Secure Client: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



Nota: la función NAT Exempt inhabilitada en este documento.

Firewall Device Manager Monitoring Policies	Objects Device: firepower	> 🖨 🙆 🤅	? * admin Administrator	cisco SECURE
Remote Users 📃 Secure Clien	nts - Internet R Client Certificate	UTSIDE FIREPOWER	Corporate Resources	
	Global Setting	gs		
	These settings control the basic functioning of the conne apply to all connection profiles; you cannot configure of	iction. Changes to any of these options different settings in different profiles.		
	Certificate of Device Identity Outsid ftd-vpn-cert (Validation Us sge: SSL Se ~ outs	e Interface ilde (GigabitEthernet0/0)	~	
	Fully-qualified Domain Name for the Outside Interface	Port		
		443		
[Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy inspection policy for decrypted traffic objects and the access control policy, and the authorization ACL downloaded from the AAA server are still a Bypass Access Control policy for decrypted traffic (syst NAT Exempt	e.g. oueu i by default. Enabling the Bypass Access Contr but for remote access VPN, the VPN Filter AC pplied to VPN traffic opt permit-vpn)	rol J.	
	Secure Client Package	ad the system will launch the secure client		
	Installer when the client authenticates for the first time. The user can to You can download secure client packages from software.cisco.com (2) You must have the necessary secure client software license.	then install the package from the system.		
	Packages			
	UPLOAD PACKAGE 🗸			
	Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pk	9		
	BACK	TR		

Detalles de la configuración global

Paso 10. Confirmar resumen para perfil de conexión

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

þ	Firewall Device Manager	1回 Monitoring	Policies	Dbjects	Device: firepower	\odot	٢	۲	?	÷	admin Administrator	Ý	cisco SECURE

Summary

Review the summary of the Remote Access VPN configuration.

STEP 1: CONNECTION AND CLIENT CONFIGURATION	N	
Primary Identity Source	_	
Authentication Type	Client Certificate Only	
Primary Identity Source	-	
Fallback Local Identity Source	_	
Username from Certificate	Man Snerific Field	
Disemante from Cerunicate	CN (Common News)	
Primary Field	GN (Common Name)	
Secondary Field	OU (Organisational Unit)	
Advanced		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		
IPv4 Address Pool	C ftd-cert-match-pool	
IPv6 Address Pool	·	
DHCP Servers	-	
STEP 2: GROUP POLICY		
Group Policy Name	₫ [®] ftd-cert-match-grp	
Banner + DNS Server		
DNS Server	i -	
Banner text for authenticated clients	-	
Session Settings		
Maximum Connection Time / Alert Interval	Unlimited / 1 minutes	
Idle Timeout / Alert Interval	30 / 1 minutes	
Simultaneous Login per User	3	
Split Tunneling		
IPv4 Split Tunneling	Allow all traffic over tunnel	
IPv6 Split Tunneling	Allow all traffic over tunnel	
Secure Client		
Secure Client Profiles	a secureClientProfile	
STEP 3: GLOBAL SETTINGS		
Certificate of Device Identity	옷 ftd-vpn-cert	
Outside Interface	GigabitEthernet0/0 (outside)	
Fully-qualified Domain Name for the Outside	-	1
Port	443	1
Access Control for VPN Traffic	No	
NAT Exempt		_
NAT Exempt	No	
Inside Interfaces	-	
Inside Naturados		
Secure Client Package		
Dackages	## Windows ciscousacian/Santusio-5.1.4.74-unbulante-10-sta	
Packages	all windows: cisco-secure-cient-win-5.1.4.74-webdeploy-k9.pkg	1

Confirmar resumen para perfil de conexión

Confirmar en CLI de FTD

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

// Defines IP of interface interface GigabitEthernet0/0 speed auto nameif outside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.1.200 255.255.255.0 // Defines a pool of addresses ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160 // Defines Trustpoint for Server Certificate crypto ca trustpoint ftd-vpn-cert enrollment terminal keypair ftd-vpn-cert crl configure // Server Certificate crypto ca certificate chain ftdvpn-ca-cert certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 quit // Defines Trustpoint for CA crypto ca trustpoint ftdvpn-ca-cert enrollment terminal validation-usage ssl-client crl configure // CA crypto ca certificate chain ftdvpn-ca-cert 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:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2 anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml anyconnect enable tunnel-group-list enable cache disable error-recovery disable

// Configures the group-policy to allow SSL connections group-policy ftd-cert-match-grp internal group-policy ftd-cert-match-grp attributes 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-dns none split-tunnel-all-dns disable client-bypass-protocol disable msie-proxy method no-modify vlan none address-pools none ipv6-address-pools none webvpn anyconnect ssl dtls none anyconnect mtu 1406 anyconnect ssl keepalive none anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client none anyconnect dpd-interval gateway none anyconnect ssl compression none anyconnect dtls compression none anyconnect modules none anyconnect profiles value secureClientProfile type user anyconnect ssl df-bit-ignore disable always-on-vpn profile-setting

// Configures the tunnel-group to use the certificate authentication tunnel-group ftd-cert-match-vpn type remote-access tunnel-group ftd-cert-match-vpn general-attributes address-pool ftd-cert-match-pool default-group-policy ftd-cert-match-grp tunnel-group ftd-cert-match-vpn webvpn-attributes authentication certificate group-alias ftd-cert-match-vpn enable

Confirmar en cliente VPN

Paso 1. Copiar perfil de cliente seguro en cliente VPN

Copie el perfil de cliente seguro para diseñar el cliente VPN y el cliente VPN administrador.



Nota: El directorio del perfil de cliente seguro en el equipo con Windows: C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

📕 🛛 🛃 🗸 🕴 Profile	•				
File Home	Share View				
← → · ↑ 📙	> This PC > Loc	al Disk (C:) → ProgramData	> Cisco > Cisco Secure Clie	nt > VPN > Profile	ٽ ~
- Quick access	Name	^	Date modified	Туре	Size
Desktop	🖌 📙 Mgm	tTun	€, _3/2024 20:15	File folder	
Downloads	AnvC	onnectProfile vsd	6/., 2024 21:44	XSD File	97 KB
🛱 Documents	∦ secur	eClientProfile	7 1, J24 10:48	XML Document	4 KB



Paso 2. Confirmar certificado de cliente

En Engineer VPN Client, navegue hasta Certificates - Current User > Personal > Certificates, verifique el certificado de cliente utilizado para la autenticación.



Confirmar certificado para cliente de VPN de ingeniero

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

• Asunto: CN = vpnEngineerClientCN

Certificate	>
General Details Certification	Path
Show: <all></all>	\sim
Field	Value
Valid to	Wednesday, June 18, 2025 5:
Subject	vpnEngineerClientCN, vpnEngi
Contraction (RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher
Enhanced Key Usage	Client Authentication (1.3.6.1
Netscape Comment	xca certificate
Thumborint algorithm	cha1 Y
CN = vpnEngineerClientCN O = Cisco L = Tokyo S = Tokyo C = JP	
	Edit Properties Copy to File
	OK

Detalles del certificado de cliente de ingeniero

En manager VPN client, navegue hasta Certificates - Current User > Personal > Certificates, verifique el certificado de cliente utilizado para la autenticación.



Confirmar certificado para Manager VPN Client

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

• Asunto: CN = vpnManagerClientCN

how: <all></all>	\sim	
Field	Value	^
must day.	Thursday, June 19, 2025 9:41	
Subject Subject	vpnManagerClientCN, vpnMan	
PUDIC KEY	RSA (2048 Bits)	
Public key parameters	05 00	
🔊 Key Usage	Digital Signature, Key Encipher	
Enhanced Key Usage	Client Authentication (1.3.6.1	
Netscape Comment	xca certificate	
Thumhorint algorithm	cha 1	Ŷ
CN = vpnManagerClientCN O = Cisco L = Tokyo S = Tokyo C = JP		I
	Edit Properties Copy to File	

×

Detalles del certificado de cliente del administrador

Paso 3. Confirmar CA

💼 Certificate

En el cliente VPN del ingeniero y en el cliente VPN del administrador, navegue hasta Certificados - Usuario actual > Autoridades de certificación raíz de confianza > Certificados, verifique la CA utilizada para la autenticación.

• Emitido por: ftd-ra-ca-common-name

🜇 Console1 - [Console Root\Certificates - Current	t User\Trusted Root Certification A	Authorities\Certificates]				o x
🚡 Eile Action View Favorites Window	Help					- 8 ×
🗢 🔿 🖄 🚾 🐇 🗞 💥 📾 🛛 🖉						
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Actions
Certificates - Current User	² 127.0.0.1	127.0.0.1	5/17/2027	Server Authenticati	duo-endpoir	Certificates 🔺
Personal	AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati	Sectigo (AA/	More >
Trusted Root Certification Authorities	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati	DigiCert Balt	
Certificates	🔄 Class 3 Public Primary Cer	Class 3 Public Primary Cer	8/1/2028	Client Authenticati	VeriSign Clas	ftd-ra-ca 🔺
	COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	More >
> Intermediate Certification Authorities	Copyright (c) 1997 Micros	Copyright (c) 1997 Micros	12/30/1999	Time Stamping	Microsoft Tii	
> Active Directory User Object	CONTRACTOR DESKTOP-VCKHRG1	DESKTOP-VCKHRG1	10/30/2022	Server Authenticati	www.infraey	
> Trusted Publishers	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	<all></all>	<none></none>	
> Intrusted Certificates	🔄 🔄 DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	Client Authenticati	DigiCert	
> Inird-Party Root Certification Authoriti	🔄 🔄 DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati	DigiCert	
> Constant Second Se	🔄 DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati	DigiCert Glol	
> Client Authentication Issuers	DigiCert High Assurance	DigiCert High Assurance	11/9/2031	<all></all>	<none></none>	
> Smart Card Trusted Roots	DigiCert High Assurance	DigiCert High Assurance	11/9/2031	Client Authenticati	DigiCert	
> 🙀 Certificates (Local Computer)	DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati	DigiCert Tru:	
		DCT D CA YA	2/30/2021	Client Authenticati	DST Root CA	
	🙀 ftd-ra-ca-common-name	ftd-ra-ca-common-name	/16/2029	<all></all>	<none></none>	
	egronobaloign	olooabign	3/18/2029	Client Authenticati	GlobalSign R	
Confirmer CA						

Confirmar CA

Verificación

Paso 1. Iniciar conexión VPN

En el cliente de ingeniería VPN, inicie la conexión de Cisco Secure Client. No es necesario introducir el nombre de usuario y la contraseña, ya que la VPN se ha conectado correctamente.

S Cisco Secure Client − □ ×	S Cisco Secure Client cert-match X	Sisco Secure Client	– 🗆 X
AnyConnect VPH: Your client certificate will be used for authentication cert-match	Your clent certificate will be used for authentication Group: [ftd-cert-match-vpn ~]	AnyConnect VPI: Connected to cert-match. cert-match	Disconnect
	OK Cancel	00:00:06	IPv4
O dudu cate		\$ ()	rijnajn Cisco

Conexión VPN correcta para Engineer VPN Client

En el cliente VPN del administrador, inicie la conexión de Cisco Secure Client. La VPN conectada falló debido a un error en la validación del certificado.



Error en la conexión VPN para el cliente VPN del administrador

Paso 2. Confirmar sesiones VPN en CLI de FTD

Ejecute show vpn-sessiondb detail anyconnect el comando en la CLI de FTD (Line) para confirmar las sesiones VPN del ingeniero.

firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32 Assigned IP: 172.16.1.150 Public IP: 192.168.1.11 Protocol : AnyConnect-Parent SSL-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 Bytes Tx : 14718 Bytes Rx : 12919 Pkts Tx: 2 Pkts Rx: 51 Pkts Tx Drop: 0 Pkts Rx Drop: 0 Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn Login Time : 05:42:03 UTC Tue Jul 2 2024 Duration: 0h:00m:11s Inactivity: 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000200006683932b Security Grp: none Tunnel Zone: 0

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

AnyConnect-Parent: Tunnel ID : 32.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 50170 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.17763 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7359 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0

Pkts Tx Drop: 0 Pkts Rx Drop: 0

SSL-Tunnel: Tunnel ID : 32.2 Assigned IP : 172.16.1.150 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 50177 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7359 Bytes Rx : 12919 Pkts Tx : 1 Pkts Rx : 51 Pkts Tx Drop : 0 Pkts Rx Drop : 0

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 el equipo con Windows.

Este es un ejemplo de los registros de depuración en el motor de línea durante la conexión VPN desde el cliente de ingeniería.

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClient Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi

Información Relacionada

Configuración del servicio de gestión integrada de FDM para Firepower 2100 Configurar VPN de acceso remoto en FTD administrado por FDM Configuración y verificación de Syslog en el administrador de dispositivos Firepower

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).