Configure Cert Matching for Secure Client Auth on FTD via FDM

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Network Diagram
Configurations
Configuration in FDM
Step 1. Configure FTD Interface
Step 2. Confirm Cisco Secure Client License
Step 3. Add Address Pool
Step 4. Create Secure Client Profile
Step 5. Upload Secure Client Profile to FDM
Step 6. Add Group Policy
Step 7. Add FTD Certificate
Step 8. Add CA to FTD
Step 9. Add Remote Access VPN Connection Profile
Step 10. Confirm Summary for Connection Profile
Confirm in FTD CLI
Confirm in VPN Client
Step 1. Copy Secure Client Profile to VPN Client
Step 2. Confirm Client Certificate
Step 3. Confirm CA
Verify
Step 1. Initiate VPN Connection
Step 2. Confirm VPN Sessions in FTD CLI
Troubleshoot
Related Information

Introduction

This document describes how to set up Cisco Secure Client with SSL on FTD via FDM using certificate matching for authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firepower Device Manager (FDM) Virtual
- Firewall Threat Defense (FTD) Virtual
- VPN Authentication Flow

Components Used

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8
- Cisco Secure Client 5.1.4.74
- Profile Editor (Windows) 5.1.4.74

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

CertificateMatch is a feature that allows administrators to configure criteria that the client must use to select a client certificate for authentication with the VPN server. This configuration is specified in the client profile, which is an XML file that can be managed using the Profile Editor or manually edited. The CertificateMatch feature can be used to enhance the security of VPN connections by ensuring that only a certificate with specific attributes is used for the VPN connection.

This document describes how to authenticate the Cisco Secure Client using the common name from an SSL certificate.

These certificates contain a common name within them, which is used for authorization purposes.

- CA: ftd-ra-ca-common-name
- Engineer VPN Client Certificate: vpnEngineerClientCN
- Manager VPN Client Certificate: vpnManagerClientCN
- Server Certificate: 192.168.1.200

Network Diagram

This image shows the topology that is used for the example of this document.



Configurations

Configuration in FDM

Step 1. Configure FTD Interface

Navigate to **Device > Interfaces > View All Interfaces**, configure inside and outside interface for FTD in **Interfaces** tab.

For GigabitEthernet0/0,

- Name: outside
- IP Address: 192.168.1.200/24

Firewall D	Device Manager	Monitoring	Ø Policies	Dbjects	Device: firepowe	r		0) ()	?	:	admin A <i>dministrator</i>	~	cisco SECURE
	Device Summary Interfaces														
	Cisco Firepower Threat I 0/0 0/1 0/2	0/3 0/4 0/5	0/6 0/7	CONSOLE											
-	interraces virtual tu	nnerinterraces													
	9 Interfaces							-	1 723	T F	ilter				+
	NAME			LO	GICAL NAME S	TATUS	MODE	IP ADDRESS			STANDBY AD	ORESS	MONITO	R FOR HA	ACTIONS
	> 🗸 GigabitEtherne	t0/0		ou	tside		Routed	192.168.1.200	Static				Enabled	ł	

FTD Interface

Step 2. Confirm Cisco Secure Client License

Navigate to **Device > Smart License > View Configuration**, confirm the Cisco Secure Client license in **RA VPN License** item.





Step 3. Add Address Pool

Navigate to **Objects > Networks**, click + button.

Firewall Device Mana	ger Monitoring Policies Objects Device:	firepower	((+	۵	?	:	admin Administrator	cisco SECURE
Object Types ←	Network Objects and Groups									
C Networks	7 objects			1	y Filte	er.				+ 🕫
S Ports				Pre	eset filten	s: <u>Syster</u>	n defined.	. <u>User de</u>	efined	
G Security Zones	# NAME	TYPE	VALUE							ACTIONS
T Application Elitere	1 IPv4-Private-10.0.0.0-8	NETWORK	10.0.0/8							

Input necessary information to add a new IPv4 address pool. click **OK** button.

- Name: ftd-cert-match-pool
- Type: Range
- IP Range: 172.16.1.150-172.16.1.160

Add Network Object	0	×
Name ftd-cert-match-pool		
Description		
		1.
Type Network Host FQDN Range		
IP Range		
172.16.1.150-172.16.1.160		



Add Address Pool

Step 4. Create Secure Client Profile

Download and install the Secure Client Profile Editor from <u>Cisco Software</u> site. Navigate to **Server List**, click **Add** button. Input necessary information to add a **Server List Entry** and click **OK** button.

- Display Name: cert-match
- FQDN or IP Address: 192.168.1.200
- Primary Protocol: SSL



Server List Entry

Navigate to Certificate Matching, click Add button. Input necessary information to add a Distinguished Name Entry and click OK button.

- Name: CN
- Pattern: vpnEngineerClientCN
- Operator: Equal



Note: Check the MatchCase option in this document.

e Help							
VPN Preferences (Part 1) Preferences (Part 2)	Certificate Profile: C:	Matching Users\jianzh:	3\OneDrive	- Cisco\Des	sktop\vpnCli	ent.xml	
Preferences (Part 2) Backup Servers Certificate Dinning Certificate Enrolment Mobile Policy Server List	Key Usao Deci Enci CRL Key Data Key Non Digi	e pher_Only _Sign _Cert_Sign _Agreem _Encipher _Rencipherm _Repudiat tal_Signa	Extended Key Us Inly ServerAuth DVCS Inly ClientAuth IKE Intermediate CodeSign EmailProtect In IPSecEndSystem her IPSecUser liat TimeStamp Ia OCSPSign				ate
	Custom E	xtended Mato	h Key (Ma. Add Delete				Distinguished Name Entry X Name CN Pattern vpnEngineerClient Operator O Equal O Not Equal
	Distinguis	h only certifi hed Name (N	cates with E lax	Extended Ke	y Usage		Wildcard
	Name	Pattern	Wildcard	Operator	MatchC	Add	MatchCase
						Edit	

Distinguished Name Entry

Save the secure client profile to local computer and confirm the details of profile.



Secure Client Profile

Step 5. Upload Secure Client Profile to FDM

Navigate to **Objects > Secure Client Profile**, click **CREATE SECURE CLIENT PROFILE** button.

Firewall Device Manager Monitoring	Policies Objects	Device: firepower	So admin Administrato	r · · · · · · · · SECURE
Object Types ←	Secure Client Prof	iles		
C Networks			Filter	+
S Ports	# NAME	FILE NAME	ACTIONS	
G Security Zones				_
🐬 Application Filters		There are n	o Secure Client profile objects yet.	
€ ² URLs		Start by creatin	g the first Secure Client profile object.	
© Geolocations		CRE	ATE SECURE CLIENT PROFILE	
Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
Secure Client Profil				
Sa Identity Sources				

Create Secure Client Profile

Input necessary information to add a secure client profile and click **OK** button.

- Name: secureClientProfile
- Secure Client Profile: secureClientProfile.xml (upload from local computer)

Add Secure Client Profile		6	×
Name secureClientProfile			
Description			
			4
Secure Client Profile UPLOAD secureClientProfile.xml			
	CANCEL	0	к

Add Secure Client Profile

Step 6. Add Group Policy

Navigate to **Device > Remote Access VPN > View Configuration > Group Policies**, click + button.

Firewall Device M	anager Monitoring Policies Objects	Device: firepower	(Σ_{-})	۵? :	admin Administrator	seco SECURE
RA VPN ←	Device Summary Group Policies					
Connection Profiles	2 objects			Y Filter		+
SAML Server	# NAME	DNS SERVER	IPV4 SPLIT TUNNELING	IPV6 SPLIT TUNNELING	SECURE CLIENT PROFILES	ACTIONS
	1 DfltGrpPolicy		Allow all traffic	Allow all traffic		



Input necessary information to add a group policy and click **OK** button.

- Name: ftd-cert-match-grp
- Secure Client profiles: secureClientProfile

Add Group Policy		0	×
Q. Search for attribute	Name ftd-cert-match-gro		
Basic General Session Settings	Description		
Advanced Address Assignment	DNS Server Select DNS Group		1
Secure Client Traffic Filters	Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session Secure Client profiles		
Windows Browser Proxy	T Filter		
	Create new Secure Client Prof CANCEL OK	04	
	CANCEL	~	

Details of Group Policy

Step 7. Add FTD Certificate

Navigate to **Objects > Certificates**, click **Add Internal Certificate** from + item.

Firewall Device Mar	ager Monitoring Policies Objects Device f	irepower	O → Ø ○ : ad Ad	imin Iministrator
Object Types ←	Certificates			
C Networks	121 objects		Y Filter	+ - 🔊
S Ports			Preset filters: System defined, User defined	Add Internal CA
8 Security Zones	B NAME	туре		Add Internal Certificate ACTIONS
Application Filters	1 AAA-Certificate-Services	Trusted CA Certificate		Add Trusted CA Certificate
A 1101 ★	2 ACCVRAIZ1	Trusted CA Certificate		
Co URLS	3 Actalis-Authentication-Root-CA	Trusted CA Certificate		
Geolocations	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		
Lisors	10 Amazon-Root-CA-3	Trusted CA Certificate		
	11 DefaultInternalCertificate	Internal Certificate		
및 Certificates	12 DefaultWebserverCertificate	Internal Certificate		

Add Internal Certificate

Click Upload Certificate and Key.



Upload Certificate and Key

Input necessary information for FTD certificate, import a certificate and a certificate key from local computer and then Click **OK** button.

- Name: ftd-vpn-cert
- Validation Usage for Special Services: SSL Server

Add Internal Certificate



Ø

Х

Details of Internal Certificate

Step 8. Add CA to FTD

Navigate to **Objects > Certificates**, click **Add Trusted CA Certificate** from + item.

Firewall Device Manager	Monitoring Policies Objects Device: firepow	ver	ECURE
🐬 Application Filters	Cartificates		
🖉 URLs	Certificates		
Geolocations	120 objects	▼ Filter + ✓	. ~
Suslog Servers		Preset inters: System defined. User defined Add Internal CA	
	# NAME	TYPE 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	- Alfantin Product FOO	T 04 0	



Input necessary information for CA, import a certificate from local computer.

- Name: ftdvpn-ca-cert
- Validation Usage for Special Services: SSL Client

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

Step 9. Add Remote Access VPN Connection Profile

Navigate to **Device > Remote Access VPN > View Configuration > Connection Profiles**, click **CREATE CONNECTION PROFILE** button.

Firewall Device M	anager Monitoring	🔊 Policies Ot	Dbjects Device: firepower		۵ 🖨	2	* admin * Administrator	eisco SECURE
RA VPN ←		Device Summary Remote Acc	cess VPN Connectio	on Profiles				
Group Policies						T Filter		+
SAML Server		# NAME	AAA	GROUP POLICY			ACTIONS	
				There are no Remote a	Access Connection	ns yet.		
				Start by creating t	the first Connection	n.		
				CREATE CONN	NECTION PROFILE			

Add Remote Access VPN Connection Profile

Input necessary information for connection profile and click Next button.

- Connection Profile Name: ftd-cert-match-vpn
- Authentication Type: Client Certificate Only
- Username From Certificate: Map specific field
- Primary Field: CN (Common Name)
- Secondary Field: OU (Organizational Unit)
- IPv4 Address Pools: ftd-cert-match-pool

Firewall Device Manager Monitoring Policies Objects Device: firepower	Section 2 → Secure 3 → Secure
Remote Access VPN 1 Connection and Client 2 Remote User Experience	3 Global Settings 4 Summary
Remote Users 🗖 Secure Clients — internet	ANDOR NEDRACES Corporate Resources
Connection and Client Confi Specify how to authenticate remote users and the secure clients inside network.	guration they 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 ftd-cert-match-vpn	i VPN gateway
Group Alias (one per line, up to 5) Group URL (or ftd-cert-match-vpn	ne per line, up to 5)
Primary Identity Source Authentication Type Client Certificate Only	
Username from Certificate (Map Specific Field	
Primary Field Secondary Fiel CN (Common Name) V OU (Organisa	ld ational Unit) 🗸
Use entire DN (distinguished name) as username	
⊙ Advanced	
Authorization Server Accounting Server	or
Please select V Please select	
Client Address Pool Assignment IPv4 Address Pool Endpoints are provided an address from this pool + C find-cent-match-pool	ol ded an address from this pool
DHCP Servers +	
CANCEL	

Details of VPN Connection Profile

Input necessary information for group policy and click **Next** button.

• View Group Policy: 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 — OUT Set	INFORMACES	Corporate Resources
	Remote User Experience A group policy is a collection of user-oriented session attributes whi VPN connection is established. Select or create a Gro View Group Policy ftd-cert-match-grp Policy Group Brief Details	e th are assigned to client when a up Policy object.	
	Banour Text for Authentic BACK		

Select Group Policy

Select Certificate of Device Identity, Outside Interface, Secure Client Package for VPN connection.

- Certificate of Device Identity: ftd-vpn-cert
 Outside Interface: outside (GigabitEthernet0/0)
 Secure Client Package: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



Note: Disabled NAT Exempt feature in this document.

Firewall Device Manager Monitoring Policies	Objects Device: firepower	> 🚔 🗐	? admin Administrator	cisco SECURE
Remote Users	Clients - Internet Q Client Certificate	OUTSIDE INTERVACE	Corporate Resources	
	Global S These settings control the basic functioning of th apply to all connection profiles; you cannot co	ettings e connection. Changes to any of these opti nfigure different settings in different profiles	ions	
	Certificate of Device Identity Itd-vpn-cert (Validation Usinge: SSL Se > Fully-qualified Domain Name for the Outside Interfan e.g. ravpn.example.com Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy of and the autorization ACL downloaded from the AAA server Bypass Access Control policy for decrypted traffic NAT Exempt () () ()	Outside Interface outside (GigabitEthernet0/0) ce Port 443 e.g. 8080 uspection by default. Enabling the Bypass Access of policy, but for remote access VPA, the VPN Filte are still applied to VPM traffic ffic (aysopt permit-vpn)	Control r ACL	
	Secure Client Package If a user does not already have the right secure client package instaler when the client authenticates for the first time. The Vou can download secure client packages from software clients to use thewe the necessary secure client software license. Packages UPLOAD PACKAGE Windows: clico-secure-client-win-5.1.4.74-webdepi	ve installed, the system will launch the secure clien user can then install the package from the system. too.com (2.	a	

Details of Global Settings

Step 10. Confirm Summary for Connection Profile

Confirm the information entered for VPN connection and click **FINISH** button.

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

Summary

Review the summary of the Remote Access VPN configuration.

Advanced	
Authorization Server	
Accounting Server	
Client Address Pool Assignment	
IPv4 Address Pool	C ftd-cert-match-pool
IPv6 Address Pool	°o -
DHCP Servers	-
STEP 2: GROUP POLICY	
Banner + DNS Server	fie un-ceit-maicu-âtb
DNS Server	1 -
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
Secure Client	Prover an Denic Oran Ionian
Secure Client Profiles	SecureClientProfile
STEP 3: GLOBAL SETTINGS	
Certificate of Device Identity	옷 ftd-vpn-cert
Outside Interface	GigsbitEthernet0/0 (outside)
Fully-qualified Domain Name for the Outside Interface	-
Port	443
Access Control for VPN Traffic	No
NAT Exempt	
NAT Exempt	No
Inside Interfaces	-
Inside Networks	-
Secure Client Package	

Confirm Summary for Connection Profile

Confirm in FTD CLI

Confirm the VPN connection settings in the FTD CLI after deployment from the 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

Confirm in VPN Client

Step 1. Copy Secure Client Profile to VPN Client

Copy secure client profile to engineer VPN client and manager VPN client.



Note: The directory of secure client profile in Windows computer : C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

📕 🗹 🛃 🗢 🕴 Profile	e			
File Home	Share View			
← → • ↑ 📙	> This PC > Local Disk (C:) > ProgramDa	ata > Cisco > Cisco Secure Clie	nt > VPN > Profile	ٽ ~
	Name	Date modified	Туре	Size
Quick access	MgmtTun	€, <u>-</u> 3/2024 20:15	File folder	
Desktop	AnyConnectProfile ysd	6/., 2024 21:44	XSD File	97 KB
Documents	✓ secureClientProfile	7 12, 2024 10:48	XML Document	4 KB



Step 2. Confirm Client Certificate

In engineer VPN client, navigate to **Certificates - Current User > Personal > Certificates**, check the client certificate used for authentication.



Confirm Certificate for Engineer VPN Client

Double click the client certificate, navigate to **Details**, check the detail of **Subject**.

• Subject: CN = vpnEngineerClientCN

Certificate	×
General Details Certification	Path
Show: <all></all>	\sim
Field	Value Wednesday, June 18, 2025 5:
Public key parameters	RSA (2048 Bits) 05 00
 Key Usage Enhanced Key Usage Netscape Comment 	Digital Signature, Key Encipher Client Authentication (1.3.6.1 xca certificate
CN = vpnEngineerClientCN O = Cisco L = Tokyo S = Tokyo C = JP	ona 1
I	Edit Properties Copy to File
	OK

Details of Engineer Client Certificate

In manager VPN client, navigate to **Certificates - Current User > Personal > Certificates**, check the client certificate used for authentication.



Confirm Certificate for Manager VPN Client

Double click the client certificate, navigate to **Details**, check the detail of **Subject**.

• Subject: CN = vpnManagerClientCN

eneral Details Certification	Path	
how: <all></all>	\sim	
Field	Value '	~
- total	Thursday, June 19, 2025 9:41	
Subject	vpnManagerClientCN, vpnMan	
Public 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	cha1	۴.
CN = vpnManagerClientCN O = Cisco L = Tokyo S = Tokyo C = JP	-	I
	Edit Properties Copy to File	
	OK	

×

Details of Manager Client Certificate

Step 3. Confirm CA

💼 Certificate

In both engineer VPN client and manager VPN client, navigate to **Certificates - Current User > Trusted Root Certification Authorities > Certificates**, check the CA used for authentication.

• Issued By: ftd-ra-ca-common-name

🜇 Console1 - [Console Root\Certificates - Current	t User\Trusted Root Certification A	Authorities\Certificates]			()	or ×
Eile Action View Favorites Window	Help					- 8 ×
🗢 🔶 🙇 📷 🐇 🛍 🗙 🖼 🖬						
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Actions
 Certificates - Current User 	Sal 127.0.0.1	127.0.0.1	5/17/2027	Server Authenticati	duo-endpoir	Certificates 🔺
V Personal	AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati	Sectigo (AA/	More >
🗤 🧐 Trusted Poot Cartification Authorities	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati	DigiCert Balt	indic in F
Certificates	🔄 Class 3 Public Primary Cer	Class 3 Public Primary Cer	8/1/2028	Client Authenticati	VeriSign Clas	ftd-ra-ca 🔺
Ceruncates	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	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>	
> 🛄 Untrusted Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	Client Authenticati	DigiCert	
> Chird-Party Root Certification Authoriti	🔄 DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati	DigiCert	
> 🧮 Trusted People	🔄 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>	
> 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 Trus	
		DCT D CA YO	9/30/2021	Client Authenticati	DST Root CA	
	🙀 ftd-ra-ca-common-name	ftd-ra-ca-common-name	/16/2029	<all></all>	<none></none>	
		olooabign	3/18/2029	Client Authenticati	GlobalSign R	

Confirm CA

Verify

Step 1. Initiate VPN Connection

In engineer VPN client, initiate the Cisco Secure Client connection. No need to input the username and password, the VPN connected successfully.

S Cisco Secure Client − □ ×	S Cisco Secure Client cert-match X	Sisco Secure Client	– 🗆 X
AnyConnect VPIE Your clent certificate will be used for authentication cert-match Connect	Your clent certificate will be used for authentication Group: ftd-cert-match-vpn	AnyConnect VPIE Connected to cert-match.	Disconnect
	OK Cancel	00:00:06	IPv4
🗘 🕕 dhabe		\$ ()	-shudo. Cisco

VPN connection succeeded for Engineer VPN Client

In manager VPN client, initiate the Cisco Secure Client connection. the VPN connected failed due to certificate validation failure.

S Cisco Secure Client			\times	Cisco Secure Client	Х
Certificate Validation Failure	~	Connect		Certificate Validation Failure]
				OK	
\$ ①			-deade. cisco		

Step 2. Confirm VPN Sessions in FTD CLI

Run show vpn-sessiondb detail anyconnect command in FTD (Lina) CLI to confirm the VPN sessions of engineer.

```
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 : 000000000000006683932b
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

You can expect to find information about VPN authentication in the debug syslog of Lina engine and in the DART file on Windows computer.

This is an example of debug logs in the Lina engine during VPN connection from engineer client.

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial num Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50

Related Information

Configure FDM On-Box Management Service for Firepower 2100 Configure Remote Access VPN on FTD Managed by FDM Configure and Verify Syslog in Firepower Device Manager