Configure AAA and Cert Auth for Secure Client 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 Remote Access VPN Connection Profile
Step 4. Add Address Pool for Connection Profile
Step 5. Add Group Policy for Connection Profile
Step 6. Configure Certificate of Device Identity and Outside Interface for Connection Profile
Step 7. Configure Secure Client Image for Connection Profile
Step 8. Confirm Summary for Connection Profile
Step 9. Add User to LocalIdentitySource
Step 10. Add CA to FTD
Confirm in FTD CLI
Confirm in VPN Client
Step 1. Confirm Client Certificate
Step 2. Confirm CA
Verify
Step 1. Initiate VPN Connection
Step 2. Confirm VPN Session in FTD CLI
Step 3. Confirm Communication with Server
Troubleshoot
Related Information

Introduction

This document describes the steps for configuring Cisco Secure Client over SSL on FTD managed by FDM with AAA and certificate 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

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

Firepower Device Manager (FDM) is a simplified, web-based management interface used for managing Cisco Firepower Threat Defense (FTD) devices. The Firepower Device Manager allows network administrators to configure and manage their FTD appliances without using the more complex Firepower Management Center (FMC). FDM provides an intuitive user interface for basic operations such as setting up network interfaces, security zones, access control policies, and VPNs, as well as for monitoring the device performance and security events. It is suitable for small to medium-sized deployments where simplified management is desired.

This document describes how to integrate pre-filled usernames with Cisco Secure Client on FTD managed by FDM.

If you are managing FTD with FMC, please refer to the <u>Configure AAA and Cert Auth for Secure Client on</u> <u>FTD via FMC</u> guide.

This is the certificate chain with the common name of each certificate used in the document.

- CA: ftd-ra-ca-common-name
- Client Certificate: sslVPNClientCN
- 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

For GigabitEthernet0/1,

- Name: inside
- IP Address: 192.168.10.200/24

all Device Manager Monitoring Policies Objects	Device: firepower) @ ? : adr Ad	nin vi ministrator c	isco SECURE
Device Summary Interfaces						
Cisco Firepower Threat Defense for VMware Cisco Firepower Threat Defense for VMware Cisco Firepower Threat Defens						
9 Interfaces				T Filter		+
NAME	LOGICAL NAME STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> V GigabitEthernet0/0	outside	Routed	192.168.1.200 State		Enabled	

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.

Firewall Device Manager Monitoring Policies Objects Device: firepower	S→ (a) (?) : admin Administrator ✓ theth SECURE
SUBSCRIPTION LICENSES INCLUDED	
Threat EVABLE Disabled by user	Malware ENABLE © Disabled by user
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.	This license lets you perform malware defense. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: 🖗 Intrusion Policy	Includes: C ₀ File Policy
URL License ENABLE	RA VPN License Type VPN ONLY ~ DISABLE
Disabled by user	S Enabled
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.	Please select the license type that you purchased to enable remote access VPN. Note that Secure Firewall device manager does not support any of the advanced features covered by the Apex license.
Includes: URL Reputation	Includes: RA-VPN

Step 3. Add Remote Access VPN Connection Profile

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

Firewall Device M	anager Monitoring	Ø Policies	iiii Objects	Device: firepower		>		* admin * Administrator	cisco SECURE				
RA VPN ←		Device Summa Remote	Access V	PN Connection Prot	iles								
Connection Profiles							¥ Filter		+				
SAML Server		•	NAME	***	GROUP POLICY			ACTIONS					
		There are no Remote Access Connections yet. Start by creating the first Connection. CREATE CONNECTION PROFILE											

Add Remote Access VPN Connection Profile

Input necessary information for connection profile and click **Create new Network** button in the **IPv4 Address Pool** item.

- Connection Profile Name: ftdvpn-aaa-cert-auth
- Authentication Type: AAA and Client Certificate
- Primary Identity Source for User Authentication: LocalIdentitySource
- Client Certificate Advanced Settings: Prefill username from certificate on user login window

Firewall Device Manager Monitoring Policies	Objects Device: firepower		* admin * Administrator * **********************************
Remote Access VPN	Connection and Client Configuration Configuration Configuration	User Experience 3 Global Settings	(4) Summary
Remote Users 🗖 Secure Ci	ients — Internet	FIREPOWER	Corporate Resources
	Connection and C Specify how to authenticate remote users and the inside n	ient Configuration e secure clients they can use to connect to the twork.	
	Connection Profile Name This name is configured as a connection alias, it can be use ftdvpn-aaa-cert-auth	d to connect to the VPN gateway	
	Group Alias (one per line, up to 5) ftdvpn-aaa-cert-auth	Group URL (one per line, up to 5)	
	Primary Identity Source Authentication Type AAA and Client Certificate		
	Primary Identity Source for User Authentication LocalIdentitySource	Fallback Local Identity Source	
	Username from Certificate Map Specific Field	Secondary Field	
	CN (Common Name)	OU (Organisational Unit) ~	
	Use entire DN (distinguished name) as usernar Client Certificate Advanced Settings Prefill username from certificate on user le Hide username in login window	ne Igin window	
	Client Address Pool Assignment IPv4 Address Pool Endpoints are provided an address from this pool	IPv6 Address Pool Endpoints are provided an address from this pool	
	Filter Filter Pr4-Private-10.0.0-8 Network IPv4-Private-172.16.0.0-12 Network	•	
	IPv4-Private-192.168.0.0-16 Network I any-ipv4 Network Create new Network CANCEL C	- ND(T	



Step 4. Add Address Pool for Connection Profile

Input necessary information to add a new IPv4 address pool. Select new added IPv4 address pool for connection profile and click **Next** button.

- Name: ftdvpn-aaa-cert-pool
- Type: Range
- IP Range: 172.16.1.40-172.16.1.50

Add Network Object

Name		
ftdvpn-aaa-cert-pool		
Description		
		4
Туре		
Network Network		
IP Range		
172.16.1.40-172.16.1.50		
e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-	2001:D68:0:CD30::100	
	CANCEL	ок

Θ

 \times

Details of IPv4 Address Pool

Step 5. Add Group Policy for Connection Profile

Click Create new Group Policy in the View Group Policy item.

Firewall Device Manager Monitoring Policies Obje	Ects Device: firepower $\textcircled{\begin{tabular}{c} \hline \hline$
	Identity Source for User Authentication
A gro	Remote User Experience sup 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.
View	Group Policy er V
© Grow	DhitGrapPolicy O
	Edit DHS + BANNER DNS Server None
	Banner Text for Authenticated Clients None SESSION SETTINGS
	Maximum Connection Time / Alert Interval Unlimited / 1 Minutes Idle Time / Alert Interval BACK NEXT
	Simultaneous Legin per User

Add Group Policy

Input necessary information to add a new group policy and click **OK** button. Select new added group policy for connection profile.

• Name: ftdvpn-aaa-cert-grp

Edit Group Policy			×
Q. Search for attribute	Name		Í
Basic	novpn-aaa-cent-grp		
General	Description		
Session Settings			4
Advanced Address Assignment Split Tunneling	DNS Server CustomDNSServerGroup	~	
Secure Client Traffic Filters Windows Browser Proxy	Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session		fe
	Default domain Secure Client profiles		1
	CANCEL	ОК	

Step 6. Configure Certificate of Device Identity and Outside Interface for Connection Profile

Click Create new Internal certificate in the Certificate of Device Identity item.

Firewall Device Manager	Monitoring	Policies	⊖bjects	Device: firepowe	r	(Σ_{-})			?	:	admin Administrator	Ŷ	-ili-ili- cisco	SECURE
				Globa	l Settings									
These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.														
		Certificate	of Device Identi	ty	Outside Interface									
		Filter		~	Please select				~					
		₽ Vi	efaultInternalCertifi alidation Usage: SS	cate EL Client, IPSe 6	rface		Port							
		₽ Vi	Validation Usage: SSL Client, IPSe				443							
		Greate.nev	v.Internal Certificat	R			e.g. 808	0						
		Access Co Decrypted VI policy for de- and the author Bypass	ntrol for VPN Tra PN traffic is subjec crypted traffic opti- orization ACL down s Access Contro	Iffic ted to access control po in bypasses the access aloaded from the AAA s al policy for decrypte	licy inspection by default. E control policy, but for remo erver are still applied to VPN d traffic (sysopt permit-	nabling ti te access I traffic Vpn)	he Bypass s VPN, the	Access VPN Filt	Control er ACL					

```
Add Internal Certificate
```

Click 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: ftdvpn-cert
- Validation Usage for Special Services: SSL Server

Add Internal Certificate	Ø	\times
Name ftdvpn-cert		
Certificate Paste certificate, or choose a file (DER, PEM, CRT, CER) UpBEGIN CERTIFICATE MIIDfDCCAmSgAwIBAgIIIkE99YS2cmwDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwNUb2t5bzEOMAwGA1UEChMF OD1-v29vD4AMP=hNPA+TBIN	ftdCe load.Certif	rt.crt icate
Certificate Key Paste certificate key, or choose a file (KEY, PEM) Upload UploadBEGIN RSA PRIVATE KEY MIIEogIBAAKCAQEAxdnSeTUmgoS+GUG2Ng2FjI/+xHRkRrf6o2OccGdzLYK1tzw8 98WPu1YP0T/qwCffKXuNQ9DEVGWIjLRX9nvXdBNoaKUbZVzc03qW3AjEB7p0h0t0 e46b3P0/C7a (b61te1e0C2auSebYCF2a3b4Ub0u72F=DrSOaM77Kaa3734uPaYEas	tdCertKey Certificate	EKex
Validation Usage for Special Services SSL Server ×		~
		_

Details of Internal Certificate

Select Certificate of Device Identity and Outside Interface for VPN connection.

- Certificate of Device Identity: ftdvpn-cert
- Outside Interface: outside (GigabitEthernet0/0)



Details of Global Settings

Step 7. Configure Secure Client Image for Connection Profile

Select Windows in Packages item

a user does not already have to staller when the client authenti	he right secure client package installed, the system will launch the secure client cates for the first time. The user can then install the package from the system.
bu can download secure client bu must have the necessary se	packages from software.cisco.com
ackages	
UPLOAD PACKAGE	~
UPLOAD PACKAGE Windows	×
UPLOAD PACKAGE Windows Mac	BACK NEXT

Upload Secure Client Image Package

Upload secure client image file from local computer and clickNextbutton.



Note: The NAT Exempt feature is disabled in this document. By default, the Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) option is disabled, which means that decrypted VPN traffic is subjected to access control policy inspection.

Firewall Device Manager	Monitoring	© Policies	Objects	Device: firepower	(Σ_{-})			?	•	admin Administrator	Y	.1 1.1 1. cisco	SECURE
		Access Cor Decrypted VF policy for dec and the author Bypass	ntrol for VPN Tr N traffic is subject rypted traffic opt rization ACL dow CACCESS Contr	raffic cted to access control policy inspection tion bypasses the access control policy, inloaded from the AAA server are still a ol policy for decrypted traffic (sys-	by default. Enabling the but for remote access oplied to VPN traffic opt permit-vpn)	he Bypass VPN, the	Access VPN Filte	Control er ACL					
		NAT Exer	mpt										
		Secure C	lient Packa	ge									
		If a user does installer when	not already have the client auther	a the right secure client package installe nticates for the first time. The user can t	d, the system will laun hen install the packag	ch the se e from the	cure clier e system.	it.					
		You can down You must hav	e the necessary :	nt packages from software.cisco.com secure client software license.									
		Packages		_									
		UPLOA	D PACKAGE	×.									
		🗮 Window	ws: cisco-secure	-client-win-5.1.4.74-webdeploy-k9.pk	9								
				BACK	хт								

Select Secure Client Image Package

Step 8. Confirm Summary for Connection Profile

Confirm the information entered for VPN connection and click FINISHbutton.



Monitoring

Ø Policies

∰≣ Objects

Summary

Review the summary of the Remote Access VPN configuration.

BTDP II CONNECTION AND CLEAR CONTROLATION Image: Control Clear Certificate withmay identity Source AAA and Clier Certificate withmay identity Source ALA carditerity Source AAA And Clier Certificate Map Specific Field vithmay identity Source Control Certificate vithmay identity Source Control Certificate Advanced Settings certificate Advanced Settings - certificate Server - certificate Server - vith Address Pool Assignment - vith Address Pool Assignment </th <th></th> <th></th> <th></th>			
htmary identify Source	STEP 1: CONNECTION AND CLIENT CONFIGURATION		
Automication Type AAA and Client Certificate In Localiterity Source International Settings May Specific Field International Unity Prinary Field CM (Common Name) International Unity Secondary Field Field Address Food International Unity International Server Field Address Food Assignment International Unity Priod Address Food Assignment Field Address Food Assignment Field Address Food Assignment Priod Address Food Assignment Field Address Food Assignment Field Address Food Assignment Priod Field Address Food Assignment Field Address Food Assignment Field Address Food Assignment Priod Address Food	Primary Identity Source		
Primary Identity Source AL LocatitientlySource Image (Compose) Warname from Certificate Map Specific Field Primary Field OU [Organisational Unit) Socodary Identity Source - - - Socodary Identity Source for User Authentication - - - Socodary Identity Source for User Authentication - - - Socodary Identity Source for User Authentication - - - Socodary Identity Source for User Authentication - - - Socodary Identity Source for User Authentication - - - Socodary Identity Source for User Authentication - - - Autocation Server - - - - Socodary Identity Source for User Authentication - </td <td>Authentication Type</td> <td>AAA and Client Certificate</td> <td></td>	Authentication Type	AAA and Client Certificate	
WAAA Anvenced Settings Map Specific Field Finany Field OU (Dogenisational Unit) Secondary Identity Source - - - Autorated - - - - Other Certificate Advanced Settings - - - - Secondary Identity Source of User Autoentication - <t< td=""><td>Primary Identity Source</td><td>北 LocalidentitySource</td><td></td></t<>	Primary Identity Source	北 LocalidentitySource	
tuennen from Certificate Map Specific Field Cit/Common Name) Secondary Identity Source Secondary Identity Secondary Identity	AAA Advanced Settings		
Parlangy Field CNI (Common Name) Secondary Kindt OUI (Organisational Unit) Socondary Kindthy Source (Secondary Kindthy Source (Secondary Kindthy Source (Secondary Kindthy Source) - Secondary Kindthy Source (Secondary Kindthy Source) - Secondary Kindthy Source (Secondary Kindthy Source) - Socondary Kindthy Source (Secondary Kindthy Source) - Secondary Kindthy Source - Secondary Kindthy Source (Secondary Kindthy Source) - Secondary Kindthy Source (Secondary Kindthy Kindt	Username from Certificate	Map Specific Field	
Secondary Field OU (Organisational Unit) Secondary Identity Source Gettings Secondary Identity Source Our Autoentication - Falback Local Identity Source - Falback Local Identity Source - Pathockation Server Accounting Server Client Address Pool Assignment Pr4 Agbit Tunneling Pr4 Address I Ender Pool (outside) Pr4 Agbit Tunneling Pr4 Address Control FVPN Tr4ffic No NaT Exempt Na Feenergt Na Fe	Primary Field	CN (Common Name)	
O cleare Contribute Advanced Settings - Secondary Identity Source for User Authentication - Faltback Local Identity Source - Call Identity Source - Authorization Server - Accounting Server - Client Address Pool Assignment - IPPA Server - Group Policy Name CustomDNSServerGroup Banner to DS Server - Session Settings - Session Settings - Setting - Setting - Setting - Setting - Setting Settings -	Secondary Field	OU (Organisational Unit)	
Secondary Identity Source Secondary Identity Source for User Authentication Fallisek Local Identity Source Fallisek Local Identity Fallice Fallisek Local Identity Fallisek Local Ide	Client Certificate Advanced Settings		
Secondary identity Source for User Authentication Fallback Local Identity Source Fallback Local Identity Fallback Local Identity Fallback Fallback Local Identity Fallback Local Id	Secondary Identity Source		
Fallback Local Identity Source - Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Pith 2:040040 POLICY Advanced Banner text for authenticated clients - Section Server Box Server Banner text for authenticated clients - Section Solip per User 30 / 1 minutes Situraneous Login per User 30 / 1 minutes Secure Client Profiles Adva	Secondary Identity Source for User Authentication	-	
Advanced Athorization Server Accounting Server Image: Server Client Address Pool Assignment Image: Server Pr4 Address Pool Image: Server Pr4 Address Pool Image: Server DitC Servers - Brit 2: Gloud De OutCot Image: Server Group Policy Name Image: Server Banner + DNS Sarver Image: Custom DNSServerGroup Banner tof or authenticated clients - Session Settings Image: Custom DNSServerGroup Banner tof nauthenticated clients - Stattaneous Login per User 30 / 1 minutes Simutaneous Login per User Allow all traffic over tunnel Pr4 Signt Tunneling Allow all traffic over tunnel Port Addres Allow Storuer Client Profiles - Storuer Client Profiles - Port 443 Access Control for VPN Traffic	Fallback Local Identity Source	-	
Aktorization Server Accounting Server Client Address Pool Assignment Thorpn-aas-cert-pool Pv4 Address Pool To 1 Pv6 Address Pool To - DifD Servers - Strip 2 GlobU PooLCO To - Group Policy Name Eff forgn-aas-cert-grp Banner + DNS Sarver CustomDNSServerGroup Banner + DNS Sarver - Session Settings - Maximum Connection Time / Alert Interval Unimited / 1 minutes Statianeous Login per User 3 Split Tunneling Allow all traffic over tunnel Port Split Tunneling Allow all traffic over tunnel State Interval Signatific over tunnel Split Tunneling - Port of Dustific Alert Interval Signatific over tunnel Port of Split Tunneling - State Interval Signatific over tunnel Port of Dustific Alert Interval Signatific over tunnel Port of Dustific Alert Interval Signatific over tunnel Port of Dustific Alert Interval Globalitithernet0/0 (outside) Fully capatified Domain Name for the Outside - No	Advanced		
Accounting Server Client Address Pool Assignment Pr4 Address Pool Pr6 for thypn-aas-cert-pool Pr6 Address Pool Pr6 Address Pool Pr6 Address Pool Pr6 Address Pool Pr6 Point Pr6 Address Pool Pr6 Point Pr6 Poi	Authorization Sequer		
Client Address Pool Assignment Pr4 Address Pool Sind Address Pool	Accounting Conjug		
IPv4 Address Pool IPv6 Address Pool IP	Client Address Pool Assignment		
Pro6 Address Pool □ Pro6 □ Pro7 □ Port □ Pro7 □ Pr	IPv4 Address Pool	G ftdvpn-aaa-cert-pool	
DHCP Servers - STEP 2: GROUP POLICY Group POLICY Group POLICY Group POLICY Group POLICY Composition COMPOSITION COMPOSITION C	IPv6 Address Pool	6 -	
STIP 2: GROUP POLICY Image: Creating and the set of t	DHCP Servers	_	
Group Policy Name for the Outside Interface Inte	STEP 2: GROUP POLICY		
Banner + DNS Server Banner + DNS Server CustomDNSServerGroup Banner text for authenticated clients - Session Settings Maximum Connection Time / Alert Interval Unlimited / 1 minutes Idel Timeout / Alert Interval 20 / 1 minutes Simultaneous Login per User 3 Split Tunneling PV4 Split Tunneling IPV4 Split Tunneling Allow all traffic over tunnel Secure Client Secure Client Secure Client Secure Client Profiles - StrEP 3: GLOBAL SETTINGS Certificate of Device Identity Rull regifice Operation Rull regifice Operation Rull regifice Client Secure Client No NAT Exempt NAT Exempt No Secure Client Package -	Group Policy Name	₫₽ ftdvpn-aaa-cert-grp	
DNS Server Custom/DNSServerGroup Banner text for authenticated clients - Session Settings - Maximum Connection Time / Alert Interval Unlimited / 1 minutes Idle Timeout / Alert Interval 20 / 1 minutes Simultaneous Login per User 3 Split Tunneling Allow all traffic over tunnel IPv6 Split Tunneling Allow all traffic over tunnel Secure Client - Secure Client Porfiles - Strip 3: GLOBAL SETTINOS - Certificate of Device Identity Natifier Acces GigabitEthernet0/0 (outside) Fully-qualified Domain Name for the Outside Interface No NAT Exempt No NAT Exempt No NAT Exempt - No ElizabitEthernet0/0 (outside) -	Banner + DNS Server		
Banner text for authenticated clients – Session Settings Maximum Connection Time / Alert Interval Unlimited / 1 minutes Simultaneous Login per User 3 Split Tunneling 3 IPv4 Split Tunneling Allow all traffic over tunnel IPv6 Split Tunneling Allow all traffic over tunnel Secure Client Secure Client Profiles – STEP 3: GLOBAL SETTINOS Certificate of Device Identity @ ftdvpn-cert Outside Interface @ GigabitEthernet0/0 (outside) Fully-qualified Domain Name for the Outside – Interface No NAT Exempt No NAT Exempt No Inside Interface GigabitEthernet0/0 (outside) Inside Inter	DNS Server	CustomDNSServerGroup	
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 - StEP 3: GLOBAL SETTINOS @ GigabitEthermet0/0 (outside) Puty-qualified Domain Name for the Outside - NAT Exempt No NAT Exempt No NAT Exempt No Inside Interfaces — GigabitEthermet0/0 (outside) Inside Interfaces — GigabitEthermet0/0 (outside) Inside Interfaces — GigabitEthermet0/0 (outside)	Banner text for authenticated clients	-	
Idle Timeout / Alert Interval 30 / 1 minutes Simultaneous Login per User 3 Split Tunneling Allow all traffic over tunnel IPv4 Split Tunneling Allow all traffic over tunnel Secure Client - Secure Client Profiles - Strep 3: GLOBAL SETTINGS GigabitEthernet0/0 (outside) Certificate of Device Identity 443 Access Control for VPN Traffic No NAT Exempt No NAT Exempt No Inside Interfaces - Secure Client Package -	Maximum Connection Time / Alert Interval	Unlimited / 1 minutes	
Simultaneous Login per User 3 Split Tunneling IIPv4 Split Tunneling Allow all traffic over tunnel IPv4 Split Tunneling Allow all traffic over tunnel Secure Client Secure Client Profiles – Secure	His Timonut / Alast Interval	30 / 1 minutes	
Simulations Login per user S Split Tunneling Allow all traffic over tunnel IPv4 Split Tunneling Allow all traffic over tunnel Secure Client Profiles - S Secure Clie		2	
IPv4 Split Tunneling Allow all traffic over tunnel IPv6 Split Tunneling Allow all traffic over tunnel Secure Client Secure Client Profiles StEP 3: CLOBAL SETTINOS - Certificate of Device Identity R ftdvpn-cert Outside Interface I gigabitEthernet0/0 (outside) Fully-qualified Domain Name for the Outside - Port 443 Access Control for VPN Traffic No NAT Exempt No Inside Interfaces I gigabitEthernet0/0 (outside)	Split Tunneling	J	
IPv6 Split Tunneling Allow all traffic over tunnel Secure Client Secure Client Profiles StEP 3: GLOBAL SETTINGS - Certificate of Device Identity R ftdvpn-cert Outside Interface GigabitEthernet0/0 (outside) Port 443 Access Control for VPN Traffic No NAT Exempt No NAT Exempt No Inside Interfaces GigabitEthernet0/0 (outside) Inside Interfaces GigabitEthernet0/0 (outside)	IPv4 Split Tunneling	Allow all traffic over tunnel	
Secure Client Profiles - Secure Client Profile	IPv6 Split Tunneling	Allow all traffic over tunnel	
Secure Client Profiles - STEP 3: GLOBAL SETTINGS Certificate of Device Identity R fdvpn-cert Outside Interface IsigabitEthernet0/0 (outside) Fully-qualified Domain Name for the Outside - Port 443 Access Control for VPN Traffic No NAT Exempt No Inside Interfaces IsigabitEthernet0/0 (outside) Inside Interfaces - Secure Client Package -	Secure Client		
STEP 3: GLOBAL SETTINGS Certificate of Device Identity fudupn-cert Outside Interface GigabitEthernet0/0 (outside) Fully-qualified Domain Name for the Outside - Port 443 Access Control for VPN Traffic No NAT Exempt No Inside Interfaces GigabitEthernet0/0 (outside) Inside Interfaces GigabitEthernet0/0 (outside) Inside Networks – Secure Client Package –	Secure Client Profiles	-	
Certificate of Device Identity R ftdypn-cert Outside Interface Image: Certificate of Downin Name for the Outside Fully-qualified Domain Name for the Outside - Port 443 Access Control for VPN Traffic No NAT Exempt No Inside Interfaces GigabitEthernet0/0 (outside) Inside Interfaces - Secure Client Package -	STEP 3: GLOBAL SETTINGS		
Outside Interface GigabitEthernet0/0 (outside) Fully-qualified Domain Name for the Outside Interface - Port 443 Access Control for VPN Traffic No NAT Exempt No Inside Interfaces @ GigabitEthernet0/0 (outside) Inside Interfaces @ GigabitEthernet0/0 (outside) Secure Client Package -	Certificate of Device Identity	R ftdvpn-cert	
Fully-qualified Domain Name for the Outside Interface - Port 443 Access Control for VPN Traffic No NAT Exempt No Inside Interfaces GigabitEthernet0/0 (outside) Inside Networks - Secure Client Package -	Outside Interface	GigabitEthernet0/0 (outside)	
Port 443 Access Control for VPN Traffic No NAT Exempt No Inside Interfaces GigabitEthermet0/0 (outside) Inside Networks – Secure Client Package	Fully-qualified Domain Name for the Outside Interface	-	
Access Control for VPN Traffic No NAT Exempt No Inside Interfaces I GigabitEthermet0/0 (outside) Inside Networks – Secure Client Package	Port	443	
NAT Exempt No No Inside Interfaces GigabitEthernet0/0 (outside) Inside Networks – Secure Client Package	Access Control for VPN Traffic	No	
NAT Exempt No Inside Interfaces GigabitEthernet0/0 (outside) Inside Networks – Secure Client Package	NAT Exempt		
Inside Interfaces GigabitEthermet0/0 (outside) Inside Networks - Secure Client Package	NAT Exempt	No	
Inside Networks – Secure Client Package	Inside Interfaces	GigabitEthernet0/0 (outside)	
Secure Client Package	Inside Networks	_	
	Secure Client Package		
Packages Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg	Packages	Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg	

 Instructions

BACK

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 1 interface GigabitEthernet0/1 speed auto nameif inside cts manual propagate sgt preserve-untag policy static sgt disabled trusted 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 // Defines a local user username sslVPNClientCN password ***** pbkdf2 // Defines Trustpoint for Server Certificate crypto ca trustpoint ftdvpn-cert enrollment terminal keypair ftdvpn-cert validation-usage ssl-server crl configure // Server Certificate crypto ca certificate chain ftdvpn-cert certificate 22413df584b6726c 3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7 quit // Defines Trustpoint for CA crypto ca trustpoint ftdvpn-ca-cert enrollment terminal validation-usage ssl-client ssl-server 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 enable tunnel-group-list enable cache disable error-recovery disable // Configures the group-policy to allow SSL connections group-policy ftdvpn-aaa-cert-grp internal group-policy ftdvpn-aaa-cert-grp attributes dns-server value 64.x.x.245 64.x.x.184 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 none anyconnect ssl df-bit-ignore disable always-on-vpn profile-setting // 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
```

Confirm in VPN Client

Step 1. Confirm Client Certificate

Navigate to**Certificates - Current User > Personal > Certificates**, check the client certificate used for authentication.



Confirm Client Certificate

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

• Subject: CN = sslVPNClientCN

💼 Certificate

General	Details	Certification	Path
Show:	<ai></ai>		\sim
Field Sig Sig Iss Val	nature al nature ha uer id from id to bject blic key blic key o	gorithm ash algorithm	Value sha256RSA sha256 ftd-ra-ca-common-name, Cisc Sunday, June 16, 2024 6:12:0 Monday, June 16, 2025 6:12: ssiVPNClientCN, ssiVPNClientO RSA (2048 Bits) 05 00
CN = st O = Cis L = Tok S = Tok C = JP	sivervelier soo co cyo cyo	ntCN	Edit Properties Copy to File
			OK

х

Details of Client Certificate

Step 2. Confirm CA

Navigate to Certificates - Current User > Trusted Root Certification Authorities > Certificates, check

the CA used for authentication.

• Issued By: ftd-ra-ca-common-name

à	Console1 - [Console Root\Certificates - Current	User\Trusted Root Certification A	uthoritie Certificates]			-	σ	>	ζ
œ.	File Action View Favorites Window	Help						- 8	х
٠	🔶 🖄 🚾 🔏 🗞 🗶 🔝 🕞 🖬	1					_		
	Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Action	s	
~	Certificates - Current User	COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	Certific	cates	•
5	Certificates	Copyright (c) 1997 Micros	Copyright (c) 1997 Micros DESKTOP-VCKHRG1	12/30/1999 10/30/2022	Time Stamping Server Authenticati	Microsoft Tii www.infraey	м	ore	۲
1	 Trusted Root Certification Authorities Certificates 	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	<all></all>	<none></none>	ftd-ra-	ca	•
Ľ,	7 Conceptise Trust	DigiCert Assured ID Root DigiCert Global Root CA	DigiCert Assured ID Root DigiCert Global Root CA	11/9/2031 11/9/2031	Client Authenticati Client Authenticati	DigiCert DigiCert	м	ore	۲
	Active Directory User Object	DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati	DigiCert Glol			
	S Invited Publishers D Intrusted Certificates	DigiCert High Assurance	DigiCert High Assurance DigiCert High Assurance	11/9/2031	< All> Client Authenticati	<none> DigiCert</none>			
	> Third-Party Root Certification Authoriti	DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati	DigiCert Tru:			
	Client Authentication Issuers	📑 ftd-ra-ca-common-name	ftd-ra-ca-common-name	6/16/2029	<all></all>	<none></none>			
	Smart Card Trusted Roots	Clabellige	ClobalCiga	2/10/2020	Class Authoritant	Claboling			
>	Certificates (Local Computer)	GlobalSign	GlobalSign	12/15/2021	Client Authenticati	Google Trust			

Confirm CA

Verify

Step 1. Initiate VPN Connection

On the endpoint, initiate the Cisco Secure Client connection. The username is extracted from the client certificate, you need to input the password for VPN authentication.



Note: The username is extracted from the Common Name (CN) field of the client certificate in this document.

O Cisco Secure Client		S Cisco Secure Client 192.168.1.200 ×		S Cisco Secure Client	-		×			
	AnyConnect VPN: Contacting 192.168.1.200. 192.168.1.200	~	Connect		Group: ftdvpn-aaa-cert-auth	~	AnyConnect VPN: Connected to 192.168.1.200.	~	Disconnect	
					Password:		00:00:06		B	Pv4
\$ (1)				dudu cisco	OK Can	cel	\$ ()			adaada CISCO

Initiate VPN Connection

Step 2. Confirm VPN Session in FTD CLI

Runshow vpn-sessiondb detail anyconnect command in FTD (Lina) CLI to confirm the VPN session.

Session Type: AnyConnect Detailed Username : sslVPNClientCN Index : 4 Assigned IP : 172.16.1.40 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 : 29072 Bytes Rx : 44412 Pkts Tx : 10 Pkts Rx : 442 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth Login Time : 11:47:42 UTC Sat Jun 29 2024 Duration : 1h:09m:30s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000000667ff45e Security Grp : none Tunnel Zone : 0 AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 4.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 49779 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 7 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 : 14356 Bytes Rx : 0 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 4.3 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 49788 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7178 Bytes Rx : 10358 Pkts Tx : 1 Pkts Rx : 118 Pkts Tx Drop : 0 Pkts Rx Drop : 0

Step 3. Confirm Communication with Server

Initiate ping from VPN client to the Server, confirm that communication between the VPN client and the server is successful.



Note: Because the Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) option is disabled in step 7, you need to create access control rules that allow your IPv4 address pool access to the server.

C:\Users\cisco>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data: Reply from 192.168.10.11: bytes=32 time=1ms TTL=128 Reply from 192.168.10.11: bytes=32 time=1ms TTL=128 Reply from 192.168.10.11: bytes=32 time=1ms TTL=128 Reply from 192.168.10.11: bytes=32 time=1ms 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 = 1ms, Maximum = 1ms, Average = 1ms
```

Ping Succeeded

Runcapture in interface inside real-timecommand in FTD (Lina) CLI to confirm packet capture.

firepower# capture in interface inside real-time

Warning: using this option with a slow console connection may result in an excessive amount of non-displayed packets due to performance limitations.

Use ctrl-c to terminate real-time capture

```
1: 12:03:26.626691 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 12:03:26.627134 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 12:03:27.634641 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 12:03:27.635144 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 12:03:28.650189 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 12:03:28.650601 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 12:03:29.665813 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 12:03:29.666332 192.168.10.11 > 172.16.1.40 icmp: echo request
```

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.

```
// Certificate Authentication
Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial num
Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocat
Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B23
```

```
// Extract username from the CN (Common Name) field
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has been reques
```

Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed.

```
// AAA Authentication
Jun 29 2024 11:29:53: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVP
Jun 29 2024 11:29:53: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user
Jun 29 2024 11:29:53: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN
```

These debugs can be run from the diagnostic CLI of the FTD, which provides information you can use in order to troubleshoot your configuration.

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

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