# 透過FMC在FTD上設定安全使用者端驗證的憑證 對應

目錄
<u>必要條件</u>
<u>採用元件</u>
背景資訊
·····································
FMC中的配置
<u>步驟 1.設定FTD介面</u>
步驟2.確認思科安全客戶端許可證
<u>步驟 3.增加IPv4地址池</u>
<u>步驟 4.增加組策略</u>
<u>步驟 5.新增FTD憑證</u>
<u>步驟 6.為工程師連線配置檔案增加策略分配</u>
步驟7.設定工程師連線設定檔的詳細資訊
<u>步驟 8.為工程師連線配置檔案配置安全客戶端映像</u>
步驟 9.配置工程師連線配置檔案的訪問和證書 
步驟 10.確認工程師連線設定檔摘要
步驟 11.為Manager VPN客戶端增加連線配置檔案
<u>步驟 12.增加證書對映</u>
步驟 13.將證書對映繫結到連線配置檔案
在FTD CLI中確認
在VPN客戶端中確認
<u>步驟 1.確認使用者端憑證</u>
步驟 2.確認CA
<u>驗證</u>
步驟 1.啟動VPN連線
步驟 2.確認FMC中的活動會話
步驟 3.在FTD CLI中確認VPN作業階段
<u>疑難排解</u>
相關資訊

# 簡介

本檔案介紹如何使用憑證對應進行驗證,透過FMC在FTD上設定具有SSL的Cisco Secure Client。

# 必要條件

### 需求

思科建議您瞭解以下主題:

- Cisco Firepower管理中心(FMC)
- 防火牆威脅防禦(FTD)虛擬
- VPN身份驗證流程

採用元件

- 適用於VMWare的Cisco Firepower管理中心7.4.1
- 思科防火牆威脅防禦虛擬7.4.1
- 思科安全使用者端5.1.3.62

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

## 背景資訊

憑證對映是在VPN連線中使用的方法,其中使用者端憑證對映至本機使用者帳戶,或使用憑證內的 屬性進行授權。這是使用數位憑證作為辨識使用者或裝置的方式。透過使用證書對映,它利用 SSL協定對使用者進行身份驗證,而無需他們輸入憑證。

本文檔介紹如何使用SSL證書中的公用名稱對Cisco Secure Client進行身份驗證。

這些憑證中包含用於授權目的的通用名稱。

- CA : ftd-ra-ca-common-name
- 工程師VPN客戶端證書:vpnEngineerClientCN
- Manager VPN客戶端證書: vpnManagerClientCN
- 伺服器證書: 192.168.1.200

## 網路圖表

下圖顯示本文檔示例中使用的拓撲。



網路圖表

# 組態

## FMC中的配置

### 步驟 1.設定FTD介面

導覽至Devices > Device Management,編輯目標FTD裝置,然後為FTD設定外部介面 inInterfacestab。

對於GigabitEthernet0/0,

- 名稱: outside
- 安全區域: outsideZone
- IP地址: 192.168.1.200/24

Firewall Management Cente Devices / Secure Firewall Interfaces	Overview	Analysis	Policies	Devices	Objects	Integration		De	ploy Q	¢ 🖗	o admin	n ∨ duala cisco	SECURE
1.승규	Cancel     Save     Cancel       Soco Firepower Threat Defense for VMware     Device     Routing     Interfaces     Inline Sets     DHCP     VTEP												
All Interfaces Virtual Tunnels								Q, Search by name			ync Device	Add Inte	erfaces 💌
Interface	Logical Name	Туре	Security	Zones	MAC Add	ress (Active/Standby)	IP Address		Path N	lonitoring	Virtual Rout	er	
Management0/0	management	Physical							Disabl	be	Global		०. ⊲
GigabitEthernet0/0	outside	Physical	outsideZ	one			192.168.1.20	0/24(Static)	Disabl	bd	Global		/

FTD介面

### 步驟 2.確認思科安全客戶端許可證

導航到裝置>裝置管理,編輯目標FTD裝置,在裝置頁籤中確認Cisco安全客戶端許可證。

Firewall Management Center Devices / Secure Firewall Device Summary	y Overview Analys	sis Policies Devices	Objects Integration		Deploy	९ 💣 🔅 🛛	admin ~	cisco SECURE
1.5.49 Cisco Firepower Threat Defense for VMware		License		Ø				
Device Routing Interfaces Inline	Sets DHCP VTEP	License Types						
		Performance Tier:	FTDv5 - 100 Mbps	•				
General	12	Essentials:		m				© G
Name:	1.7671.4	Export-Controlled Features:	2	-	Ci	sco Firepower Threat	Defense for VM	ware
Transfer Packets:	Ye	Mahuara Defense:					9A33F35A	INSU
Troubleshoot:	Logs CLI Download	Maiware Detense.				2	024-06-14 07:3	8:47
Mode:	Route	IPS:		Zone:			UTC (UTC+)	0:00)
Compliance Mode:	None	Carrier:		n:				7.4.1
Performance Profile:	Defaul	URL:		Zone	setting for		UTC (UTC+)	0:00)
TLS Crypto Acceleration:	Disable	Secure Client Premier:		based	i Rules:			
		Secure Client Advantage:						
Device Configuration:	Import Export Download	Secure Client VPN Only:						
OnBoarding Method:	Registration Ke	If a device already has Secure Client VPN	Only they cannot have					
		Secure Client Premier or Secure Client A has Secure Client Premier or Secure Clie	dvantage. If a device int Advantage it cannot					
Inspection Engine		have Secure Client VPN Only		gem	nent		1	
Inspection Engine:	Snort			te Ho	st Address:		1.100	
Revert to Snort 2				Cancel Save dary	Address:			

安全使用者端授權

### 步驟 3.增加IPv4地址池

導航到對象>對象管理>地址池> IPv4池,點選Add IPv4池按鈕。

Firewall Manageme Objects / Object Manageme	ent Center Overview	Analysis Policies	Devices Objects I	ntegration	Deploy Q 🚱 🌣 🌘	admin ~ thethe SECUR
> AAA Server	IPv4 Pools				Add IPv4 Pools Q Fi	ter
> Access List	IPv4 pool contains list of IPv4	addresses, it is used for m	anagement/diagnostic interface	with clustering, or for VPN remote access profiles.		
IPv4 Pools						
IPv6 Pools	Name				Value	Override
Application Filters				No records to display		
AJ Faul						

增加IPv4地址池

輸入必要資訊,為工程師VPN客戶端建立IPv4地址池。

- 名稱: ftd-vpn-engineer-pool
- IPv4地址範圍: 172.16.1.100-172.16.1.110
- 掩碼: 255.255.255.0



0

- 名稱:ftd-vpn-manager-pool
- IPv4地址範圍: 172.16.1.120-172.16.1.130
- 掩碼: 255.255.255.0

Itd-vpn-manager-pool   Description   IPv4 Address Range*   172.16.1.120-172.16.1.130   Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150   Mask*   255.255.255.0]   Ilow Overrides   Image: Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices Image: VPN&F # with Pool Cancel Sove Manager VPN&F # with Pool Image: VPN&F # VPOol Im	Name*		
Description  Pv4 Address Range* 172.16.1.120-172.16.1.130 Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150  Mask* 255.255.255.0  Allow Overrides  Allow Overrides  Allow Overrides  Cancel Save  Anager VPN&F #wb/Pv4.#ut.#u  Engering Market Save  Anager VPN&F #wb/Pv4.#ut.#u  Engering Market Save  Anager VPN&F #wb/Pv4.#ut.#u  Engering Market Save  Description  Pv4 Pols  Pvare Description  Pv	ftd-vpn-manager-pool		
<pre> Prv4 Address Range* 172.16.1.120-172.16.1.130 Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150 Mask* 255.255.255.0  ✓ Allow Overrides    Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices    Concel Save  Vanager VPN&amp;F F\u00ethBitPv4\u00ethBut     Cancel Save  Vanager VPN&amp;F F\u00ethBitPv4\u00ethBut    Cancel Save  Vanager VPN&amp;F F\u00ethBitPv4\u00ethBut    Cancel Save  Vanager VPN&amp;F F\u00ethBitPv4\u00ethBut    Cancel Save  Vanager VPN&amp;F F\u00ethBitPv4\u00ethBut    Cancel Save  Vanager VPN&amp;F F\u00ethBitPv4\u00ethBut    Cancel Save  Vanager VPN&amp;F F\u00ethBitPv4\u00ethBut    Cancel Save  Vanager VPN&amp;F F\u00ethBitPv4\u00ethBut    Cancel Save  Vanager VPN&amp;F F\u00ethBitPv4\u00ethBitBitPv4\u00ethBitBitPv4\u00ethBitBitBitPv4\u00ethBitBitPv4\u00ethBitBitBitBitBitPv4\u00ethBitBitBitBitBitBitBitBitBitBitBitBitBitB</pre>	Description		
Image: VPN& Address Range*         172.16.1.120-172.16.1.130         Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150         Image: VPN@ Space         Image: VPN@ FightiPv4tstable			
IPv4 Address Range*         172.16.1.120-172.16.1.130         Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150         Mask*         255.255.255.0]         Image: Allow Overrides         Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices         Image: VPN客戶端的IPv4地址池         Rask*         Deverride (0)         Image: VPN客戶端的IPv4地址池         Image: VPN客戶端的IPv4地址池         Image: VPN客戶端的IPv4地址池         Image: VPN客戶端的IPv4地址池         Image: VPN客戶端的IPv4地址池         Image: VPN客戶端的IPv4地址池			
172.16.1.120-172.16.1.130         Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150         Mask*         25.255.255.0]         ✓ Allow Overrides         ● Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices         ● Override (0)         Cancel Save         Wanager VPN客戶端的IPv4地址池         EBS新的IPv4地址池         Prover Management Center Over Allow and a construction of the address conflicts in case of object is shared across multiple devices         Vanager VPN客戶端的IPv4地址池         EBS新的IPv4地址池         Cancel Network and the address conflicts in case of object is not and the address conflicts in case of object is shared across multiple devices	IPv4 Address Range*		
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150  Mask* 255.255.255.q  ✓ Allow Overrides  Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices  • Override (0)  Cancel Save Vanager VPN® F # objPv4 # # # # # # # # # # # # # # # # # # #	172.16.1.120-172.16.1.130		
Mask*         255.255.255.0]         Image: Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices         Image: Override (0)         Image: VPN客戶端的IPv4地址池         arage: VPN客戶端的IPv4地址池         East Absorber Veture to the address	Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150		
255.255.255.0 ✓ Allow Overrides ● Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices ► Override (0) Cancel Save Vanager VPN客戶端的IPv4地址池 客認新的IPv4地址池 Cancel Save Vanager VPN客戶端的IPv4地址池 Cancel Save	Mask*		
Allow Overrides Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices • Override (0) Cancel Save Vanager VPN客戶端的IPv4地址池 Rational DIPv4地址社 Cancel Save Vanager VPN客戶端的IPv4地址: Vanager VPN客戶端的IPv4地址: Cancel Save Vanager VPN客戶端的IPv4地址: Cancel Save Vanager VPN客戶端的IPv4地址: Vanager VPN客戶端的IPv4地址: Vanager VPN客戶端的IPv4地址: Cancel Save Vanager VPN客戶端的IPv4地址: Vanager VPN客戶端的IPv4地址: Vanager VPN客戶端的IPv4地址: Vanager VPN客戶端的IPv4地址: Vanager VPN客戶端的IPv4世社: Vanager VPN客戶端的IPv4世社: Vanager VPN客戶端的IPv4世社: Vanager VPN客戶端的IPv4世社: Vanager VPN客戶端的IPv4世社: Vanager VPN客戶端 Vanager VPN客戶 Vanager VPN名 <p< td=""><td>255.255.255.0</td><td></td><td></td></p<>	255.255.255.0		
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices I Override (0) Cancel Save Vanager VPNs FpishiPv4地址池 Ransert VPNs FpishiPv4地址池 Preval Management Center over a ways are over a grant over a gr	Allow Overrider		
● Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices          • Override (0)          Cancel Save          Verride (0)          Cancel Save          Verride (0)          Verr			
► Override (0) Cancel Save Vanager VPN客戶端的IPv4地址池 客認新的IPv4地址池 Concel Save Vanager VPN客戶端的IPv4地址池 Concel Save Vanager VPN客戶端 Vanager VPN Kenter Concel Conce	Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices		
Cancel Save Manager VPN客戶端的IPv4地址池 審認新的IPv4地址池。 Frewall Management Center Oppects / Oppect Management Center Oppects	<ul> <li>Override (0)</li> </ul>		
Cencel Save Manager VPN客戶端的IPv4地址池 審認新的IPv4地址池。			
Cancel Save Manager VPN客戶端的IPv4地址池 確認新的IPv4地址池。			_
Manager VPN客戶端的IPv4地址池。 定 Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy Q I Integration		Cancel	Save
確認新的IPv4地址	Manager VPN客戶端的IPv4地址池		
Firewall Management Overview Analysis Policies Devices Objects Integration Deploy © © admin "tests SECURE"	確認新的IPv4地址池。		
> AAA Server       Add IPv4 Pools       Q. Filter         > Access List       IPv4 Pools       IPv4 pools       Q. Filter         IPv4 Pools       IPv4 pools       IPv4 pools       IPv4 pools         IPv6 Pools       Name       Value       Override         IPv6 Pools       Itd-vpn-engineer-pool       Itd-vpn-engineer-pool       Itd-vpn-manager-pool         BFD Template       Itd-vpn-engineer-pool       Itd-vpn-engineer-pool       Itd-vpn-engineer-pool	Firewall Management Center Objects / Objects / Objects / Objects Integration	Deploy Q 💕 🌣	admin v diulu SECURE
Address Pools     IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.       IPv4 Pools       IPv6 Pools       Application Filters       AS Path       BFD Template       Iftd-vpn-manager-pool	> AAA Server IPv4 Pools	Add IPv4 Pools	ilter
IPv6 Pools         Name         Value         Override           Application Filters         ftd-vpn-engineer-pool	Address Pools     IPv4 Pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.     IPv4 Pools		
AS Path         ftd-vpn-engineer-pool         172.16.1.100-172.16.1.10         · · · · · ·           BFD Template         ftd-vpn-manager-pool         172.16.1.120-172.16.1.130         · · · · · · ·	IPv6 Pools Name Application Filters	Value	Override
	AS Path BFD Template ftd-vpn-engineer-pool	172.16.1.100-172.16.1.110	• /1

新的IPv4地址池

步驟 4.增加組策略

導航到對象>對象管理> VPN >組策略,點選增加組策略按鈕。

0

Firewall Management ( Objects / Object Management	Center Overview	Analysis Polic	es Devices	Objects	Integration	Deploy Q 💕 🌣 🞯	admin ~ stude SECURE
> PKI •	Group Policy					Add Group Policy Q. Filte	15
> Prefix List Route Map	A Group Policy is a set of att current connection profile.	ribute and value pairs,	tored in a group	policy object, the	at define the remote access VPN experience.The RAI	DIUS authorization server assigns the group po	licy or it is obtained from the
> Security Intelligence	Name						
Sinkhole SLA Monitor	DfltGrpPolicy						11
Time Range							
Time Zone Tunnel Zone							
URL							
Variable Set VLAN Tag							
V VPN							
Certificate Map Custom Attribute Group Policy							

增加組策略

### 輸入為工程師VPN客戶端建立組策略所需的資訊。

- 名稱: ftd-vpn-engineer-grp
- VPN協定:SSL

## Add Group Policy

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

0

### 輸入為管理器VPN客戶端建立組策略所需的資訊。

- 名稱: ftd-vpn-manager-grp
- VPN協定:SSL

# Add Group Policy

Name:*	
ftd-vpn-manager-gr	
Description:	
General Secure	Client Advanced
VPN Protocols	VPN Tunnel Protocol:
IP Address Pools	Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.
Banner	SSL SSL
DNS/WINS	IPsec-IKEv2
Split Tunneling	
lanager VPN客戶端的組策略	

## 確認新的群組原則。

Firewall Management	t Center Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	¢	¢ 0	admin $\sim$	cisco SECURE
> PKI												
Policy List	Group Policy						Add Gr	oup Po	licy	Q, Filte	r	
Port												
> Prefix List	A Group Policy is a set of current connection profile	attribute and value	ue pairs, stored	f in a group p	olicy object, th	at define the remote access VPN experience. The RADIUS authoriz	ation serve	r assig	ns the ç	roup po	licy or it is ob	ained from the
Route Map	current connection prome											
> Security Intelligence	Name											
Sinkhole	DftGroPolicy											1=
SLA Monitor	ontoip: oney	_										· · ·
Time Range	ftd-vpn-engineer-grp											11
Time Zone	ftd-vpn-manager-grp											11
Tunnel Zone		-										

新增群組原則

## 步驟 5.新增FTD憑證

導航到對象>對象管理> PKI >證書註冊,點選增加證書註冊按鈕。

Firewall Management Objects / Object Management	Center Overview	Analysis	Policies	Devices	Objects	Integration	Deploy (	Q 🔮 🕸	🕜 admin 🗸	cisco SECURE
Cipher Suite List							A HI OLD From			
> Community List	Cert Enrollment						Add Cert Enro	liment	Ļ	
DHCP IPv6 Pool	A certificate enrollment obje	t contains the C	ertification Au	thority (CA)	) server informa	tion and enrollment parameters that are required for creating C	ertificate Signing	Requests (C	SRs) and obtaining	Identity
> Distinguished Name	Certificates from the specifie	d CA. These acti	vities occur i	n your Priva	te Key Infrastruc	ture (PKI).				
DNS Server Group										
> External Attributes	Name							Туре	Override	
File List						No records to display				
> FlexConfig										
Geolocation										
Interface										
Key Chain										
Network										
∨ PKI										
Cert Enrollment										
External Cert Groups										

0

輸入FTD憑證的必要資訊,並從本機電腦匯入PKCS12檔案。

- 名稱:ftd-vpn-cert
- 註冊型別: PKCS12檔案

# Add Cert Enrollment

Name* ftd-vpn-cert Description
This certificate is already enrolled on devices.Remove the enrolment from Device>Certificate page to edit/delete this Certificate. CA Information Certificate Parameters Key Revocation
Enrollment Type:       PKCS12 File         PKCS12 File*:       ftdCert.pfx         Passphrase*:          Validation Usage:       IPsec Client       SSL Client       SSL Server         Skip Check for CA flag in basic constraints of the CA Certificate
Cancel Save 證書註冊詳細資訊 確認新的憑證註冊。
Firewall Management Center   Objects / Object Management     Objects / Object Management     Cipher Suite List     Community List   DHCP IPv6 Pool   > Distinguished Name   DNS Server Group   > External Attributes   Fie List     Index        Name        Type

0

新憑證註冊

## 導航到裝置>證書,點選增加按鈕。

Firewall Management Center Devices / Certificates	Overview Analysis	Policies Devices Objects	Integration	Deploy	० 🎸 🌣 🙆 ः	admin ~ alterite SECURE
Filter All Certificates						Add
Name Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status		
		No certificates	Add Certificates			*

新增FTD憑證

輸入將新憑證註冊連結到FTD的必要資訊。

- 裝置:1.x.x.49
- 證書註冊:ftd-vpn-cert

Add	New	Cert	ificate
-----	-----	------	---------



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

¥	
¥	
	Ψ Ψ

Cert Enrollment Details:

Name:	ftd-vpn-cert
Enrollment Type:	PKCS12 file
Enrollment URL:	N/A



將憑證連結到FTD

確認憑證繫結的狀態。

Ę	Firewall Manageme	nt Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	¢	0	admin $\sim$	cisco SE	CURE
Filt	ter All Certificates	¥													Ad	d
	Name	Domain	Enrollment T	Гуре	Identity Certifica	te Expiry		CA Certificate Expiry	Status							
ſ	∨ <b>m=</b> 1,53 k.J.49													<b></b>		^
	ftd-vpn-cert	Global	PKCS12 file		Jun 16, 2025			Jun 16, 2029	CA CID					± 🖉	C 🛢	

憑證繫結的狀態

### 步驟 6.為工程師連線配置檔案增加策略分配

### 導航到Devices > VPN > Remote Access, Addbutton。

Firewall Management Center Ove	erview Analysis F	Policies Devices Objects	Integration	Deploy	९ 💕 🌣 🛛	admin ~ dude SECURE
						Add
Name		Status	Last Modif	fied		
		No configuration availa	ble Add a new configuration			

增加遠端訪問VPN

### 輸入必要資訊,然後按一下「下一步」按鈕。

- 名稱: ftd-vpn-engineer
- VPN協定:SSL
- 目標裝置:1.x.x.49

Firewall Management Center Devices / VPN / Setup Wizard Overview Analysis Policies Devices Objects Integration	Deploy Q 🎸 :	to admin v altaba S	ECURE
Remote Access VPN Policy Wizard         Policy Assignment          ② Connection Profile          ③ Secure Client          ④ Access & Certificate          ⑤ Summer (S) Su	mary		
Targeted Devices and Protocols         This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.         Name:*         Ifd-vpn-engineer         Description:         Description:         Image:	Before You Start     Before you start, ensure the following configuration     levents to be in place to complete Remote Access     VPN Policy.     Authentication Server     Configure LOCAL or Realm or RADIUS Server Group     or SSO to authenticate VPN clients.     Secure Client Package     Make sure you have Secure Client package for VPN     Ciredentiats to download it during the witzard.     Device Interface     Interfaces should be already configured on targeted     devices so that they can be used as a security zone     or interface group to enable VPN access.		
		Cancel Back Ner	ext

策略分配

步驟 7.設定工程師連線設定檔的詳細資訊

輸入必要資訊,然後按一下「下一步」按鈕。

- 驗證方法:僅使用者端憑證
- 來自證書的使用者名稱: 對映特定欄位

- 主要欄位: CN (一般名稱)
- 次要欄位: OU (組織單位)
- IPv4地址池:ftd-vpn-engineer-pool
- 組策略:ftd-vpn-engineer-grp

Firewall Management Center Overview	Analysis Policies Devices Objects Integration	Deploy	٩	¢	° 0	admin ~	eisco SECURE
Remote Access VPN Policy Wizard							
1 Policy Assignment 2 Connection Profile	3 Secure Client 4 Access & Certificate 5 Summary						
	Connection Profile:						
	Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.						
	Connection Profile Name:* ftd-vpn-engineer						
	This name is configured as a connection alias, it can be used to connect to the VPN gateway						
	Authentication, Authorization & Accounting (AAA):						
	Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.						
	Authentication Method: Client Certificate Only						
	Username From Certificate:   Map specific field Jse entire DN (Distinguished Name) as username						
	Primary Field: CN (Common Name)						
	Secondary Field: OU (Organisational Unit)						
	Authorization Server: (Realm or RADIUS) +						
	Accounting Server: (RADIUS) +						
	Client Address Assignment:						
	Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are						
	Use AAA Server (Realm or RADIUS only)						
	Use DHCP Servers						
	Use IP Address Pools						
	IPv4 Address Pools: ftd-vpn-engineer-pool						
	IPv6 Address Pools:						
	Group Policy:						
	A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.						
	Group Policy:* [td-vpn-engineer-grp +						
	Edit Group Policy						
							•
					Cance	Back	Next

連線設定檔的詳細資訊

步驟 8.為工程師連線配置檔案配置安全客戶端映像

選擇安全客戶端映像檔案,然後按一下Nextbutton。

Firewall Management Center Ove	view Analysis Policies Devices Objects Integration	Deploy	۹	¢	0	admin $\sim$	cisco SECURE
Remote Access VPN Policy Wizard							
1 Policy Assignment 2 Connection Profile	3 Secure Client 4 Access & Certificate 5 Summary						
	Remote User Secure Client Internet Outside Upp Inside Corporate Resources						
	AAA Secure Client Image The VPN gateway can automatically download the latest. Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package. Download Secure Client packages from Cisco Software Download Center.						
	Show Re-order buttons +     Secure Client File Object Name     Secure Client Package Name     Operating System						
[	cisco-secure-client-win-5.1.3.6 cisco-secure-client-win-5.1.3.62-webdeplo Windows						
٠		_			0		

選取安全使用者端

### 步驟 9.配置工程師連線配置檔案的訪問和證書

為介面組/安全區域和證書註冊項選擇值,然後按一下下一步按鈕。

- 介面組/安全區域:outsideZone
- 憑證註冊:ftd-vpn-cert

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy Q	° 0	admin $\vee$	diale SECURE
Remote Access VPN Policy Wizard			
1 Policy Assignment ② Connection Profile ③ Secure Client ④ Access & Certificate ⑤ Summary			
Network Interface for Incoming VPN Access			
Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for URM connections			
Interface group/Security Zone:* outsideZone +			
Z Enable DTLS on member interfaces			
▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.			
Device Certificates			
Device certificate (also called identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.			
Certificate Enrollment:* ftd-vpn-cert +			
Access Control for VPN Traffic			
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.			
✓ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) The nation humseese the Access Control Policy Instantion but VPN filter ACL and			-

訪問和證書的詳細資訊

### 步驟 10.確認工程師連線設定檔摘要

確認輸入的遠端訪問VPN策略資訊,然後按一下Finish按鈕。

Firewall Management Center Devices / VPN / Setup Wizard	r Overview Analysis Po	licies Devices Objects Integration	Deploy	Q 🔮 🌣 🚱 admin ~ dude SECURE
Remote Access VPN Policy 1 Policy Assignment (2) Conner	/ Wizard	t ④ Access & Certificate ⑤	Summary	
	Firewall Management Center will conf Firewall Management Center will conf Name: Device Targets: Connection Profile: Connection Allas: AAA: Authentication Method:	Hornguration Hours an RA VPN Policy with the following settings ftd-vpn-engineer ftd-vpn-engineer ftd-vpn-engineer Client Certificate Only	Additional Configuration Requirements After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.  Access Control Policy Update An Access Control rule must be defined to allow VPN traffic on all targeted devices.  NAT Examplifice	
	Username From Certificate: Authorization Server: Accounting Server: Address Assignment: Address from AAA: DHCP Servers: Address Pools (IPv4): Address Pools (IPv6):	- - - fid-vpn-engineer-pool	IN ALL composition     IN NAT Exemption     IN NAT is enabled on the targeted devices, you     must define a NAT Policy to exempt VPN traffic.     DNS Configuration     To resolve hostname specified in AAA Servers     or CA Servers, configure DNS using FlexConfig     Policy on the targeted devices.     Port Configuration	
4	Group Policy: Secure Client Images: Interface Objects: Device Certificates:	ftd-vpn-engineer-grp cisco-secure-client-win-5.1.3.62-webdeploy-k9.pk g outsideZone ftd-vpn-cert	SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Secure Client image download.NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in NAT Policy or other services before deploving	Cancel Back Finlah

遠端訪問VPN策略的詳細資訊

## 步驟 11.為Manager VPN客戶端增加連線配置檔案

導航到Devices > VPN > Remote Access > Connection Profile,按一下+按鈕。

Firewall Management Center Devices / VPN / Edit Connection Profile	Analysis Policies Devices Objects Integration	Deploy Q 💕 🌣 🙆 admin 🗸 🐇	cisco SECURE
ftd-vpn-engineer			e Cancel
Enter Description			
		Policy A:	ssignments (1)
Connection Profile Assess Interfaces Advanced		Local Realm: None Dynamic Acces	s Policy: None
Connection Prome Access interfaces Advanced			
			+
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy	/1
ftd-vpn-engineer	Authentication: Client Certificate Only Authorization: None Accounting: None	■ ftd-vpn-engineer-grp	/1

為Manager VPN客戶端增加連線配置檔案

輸入連線配置檔案的必要資訊,然後按一下Save按鈕。

- 名稱:ftd-vpn-manager
- 組策略: ftd-vpn-manager-grp
- IPv4地址池:ftd-vpn-manager-pool

## Add Connection Profile

Connection Profile:*	ftd-vpn-manager	
Group Policy:*	ftd-vpn-manager-grp	• +
Client Address Assignment	AAA Aliases	

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA. Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools:

Name	IP Address Range	
ftd-vpn-manager-pool	172.16.1.120-172.16.1.130	ftd-vpn-manager-pool

# DHCP Servers: + Name DHCP Server IP Address

Manager VPN客戶端的連線配置檔案的詳細資訊

### 確認新增的連線設定檔。

Firewall Management Center Devices / VPN / Edit Connection Profile	Analysis Policies Devices	Objects Integration		Deploy Q 💕 🌣 🕻	admin ~ durity SECURE
ftd-vpn-engineer		_		You have unsav	ved changes Save Cancel
Enter Description			Lo	cal Realm: None	Policy Assignments (1) Dynamic Access Policy: None
Connection Profile Access Interfaces Advanced					
					+
Name	AAA		Group Policy		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None		DfltGrpPolicy		/1
ftd-vpn-engineer	Authentication: Client Certificate Only Authorization: None Accounting: None		📑 ftd-vpn-engineer-grp		/1
ftd-vpn-manager	Authentication: Client Certificate Only Authorization: None Accounting: None		ttd-vpn-manager-grp		/1

確認增加的連線配置檔案

+

Cancel

Save

### 步驟 12.增加證書對映

導航到對象>對象管理> VPN >證書對映,點選增加證書對映按鈕。

Firewall Management	t Center Overview	Analysis Policies	Devices Object	Integration	Deploy Q	🕼 🌣 🔞 🛛 admin 🗸	disdo SECURE
> PKI						_	
Policy List	Certificate Map				Add Certificate Ma	p Q	
Port						_	
> Prefix List	Certificate Map Object is use connection is associated wit	ed to provide an association the specified connection of	between a received cert profile.	ficate and a Remote Access VPN connection p	rofile.If a received certificate matches the n	ules contained in the certif	icate map, the
Route Map		n ore opposition controller p					
> Security Intelligence	Name					Value	
Sinkhole							
SLA Monitor				No records to display			
Time Range							
Time Zone							
Tunnel Zone							
URL							
Variable Set							
VLAN Tag							
V VPN							
Certificate Map							
Custom Attribute							

增加證書對映

輸入工程師VPN客戶端的證書對映所需的資訊,然後按一下Save按鈕。

- 對映名稱:cert-map-engineer
- 對映規則:CN(公用名)等於vpnEngineerClientCN

Map Name*:
cert-map-engineer

### Mapping Rule

Add Rule

Configure the certificate matching rule

#	Field	Component	Operator	Value	
1	Subject	CN (Common Name)	Equals	vpnEngineerClie	/ 1



Engineer Client的證書對映

為管理器VPN客戶端的證書對映輸入必要資訊,然後按一下Save按鈕。

- 對映名稱:cert-map-manager
- 對映規則:CN(公用名)等於vpnManagerClientCN

0

Map Name*:
cert-map-manager

### Mapping Rule

Configure the certificate matching rule

#	Field	Component	Operator	Value		
1	Subject	CN (Common Name)	Equals	vpnManagerClie	/	Ì

	Cancel	Save
Manager客戶端的證書對映		

## 確認新增的憑證對應。

Firewall Managemer	: Center Overview Analysis Policies Devices Objects Integration Deploy Q	🖓 🌣 🞯 🛛 admin 🦄	cisco SECURE
PKI     Policy List     Post	Certificate Map Add Certificate Map	٩	
Prefix List     Route Map	Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile. If a received certificate matches the rule connection is associated with the specified connection profile.	es contained in the cert	ificate map, the
> Security Intelligence	Name	Value	
Sinkhole	cert-map-engineer	1 Criteria	13
SLA Monitor	cert-man-mananer	1 Criteria	
Time Range	(diranehaneha)	r Grivena	/ I

新憑證對應

步驟 13.將證書對映繫結到連線配置檔案

導覽至Devices > VPN > Remote Access,編輯ftd-vpn-engineer。 然後,導航到高級>證書對映 ,點選增加對映按鈕。

0

Add Rule



繫結證書對映

將證書對映繫結到工程師VPN客戶端的連線配置檔案。

- 證書對映名稱: cert-map-engineer
- 連線Profile: ftd-vpn-engineer

# Add Connection Profile to Certificate Map

Choose a Certificate Map and associate Connection Profiles to selected Certificate Map.

2



工程師VPN客戶端的繫結證書對映

將證書對映繫結到管理器VPN客戶端的連線配置檔案。

- 證書對映名稱:cert-map-manager
- 連線配置檔案:ftd-vpn-manager

Choose a Certificate Map and associate Connection Profiles to selected Certficate Map.



確認憑證繫結

在FTD CLI中確認

從FMC部署後,在FTD CLI中確認VPN連線設定。

// Defines IP of interface
interface GigabitEthernet0/0

nameif outside security-level 0 ip address 192.168.1.200 255.255.255.0 // Defines a pool of addresses ip local pool ftd-vpn-engineer-pool 172.16.1.100-172.16.1.110 mask 255.255.255.0 ip local pool ftd-vpn-manager-pool 172.16.1.120-172.16.1.130 mask 255.255.255.0 // Defines Trustpoint for Server Certificate crypto ca trustpoint ftd-vpn-cert keypair ftd-vpn-cert crl configure // Server Certificate Chain crypto ca certificate chain ftd-vpn-cert certificate 22413df584b6726c 3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7 quit certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 . . . . . . quit // Defines Certificate Map for Engineer VPN Clients crypto ca certificate map cert-map-engineer 10 subject-name attr cn eq vpnEngineerClientCN // Defines Certificate Map for Manager VPN Clients crypto ca certificate map cert-map-manager 10 subject-name attr cn eq vpnManagerClientCN // Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows" anyconnect enable tunnel-group-list enable cache disable certificate-group-map cert-map-engineer 10 ftd-vpn-engineer certificate-group-map cert-map-manager 10 ftd-vpn-manager error-recovery disable // Configures the group-policy to allow SSL connections from manager VPN clients group-policy ftd-vpn-manager-grp internal group-policy ftd-vpn-manager-grp attributes banner none wins-server none dns-server none

dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ikev2 ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-tunnel-network-list none default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable // Configures the group-policy to allow SSL connections from engineer VPN clients group-policy ftd-vpn-engineer-grp internal group-policy ftd-vpn-engineer-grp attributes banner none wins-server none dns-server none dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-tunnel-network-list none default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20

anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable

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

// Configures the tunnel-group to use the certificate authentication for manager VPN clients
tunnel-group ftd-vpn-manager type remote-access
tunnel-group ftd-vpn-manager general-attributes
address-pool ftd-vpn-manager-pool
default-group-policy ftd-vpn-manager-grp
tunnel-group ftd-vpn-manager webvpn-attributes
authentication certificate

### 在VPN客戶端中確認

步驟 1.確認使用者端憑證

在工程VPN客戶端中,導航到證書- Current User > Personal > Certificates,檢查用於身份驗證的 客戶端證書。



確認工程師VPN客戶端的證書

按兩下客戶端證書,導航至詳細資訊,檢查主題的詳細資訊。

主題:CN = vpnEngineerClientCN

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

工程師客戶端證書的詳細資訊

在Manager VPN客戶端中,導航到Certificates - Current User > Personal > Certificates,檢查用於 身份驗證的客戶端證書。 Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

🚡 Eile Action View Favorites Window Help

🗢 🔿 🙍 📆 🛍 🔯 🕞 📓 🗖	D					
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Actions	
Certificates - Current User	Supprime Strength Str	ftd-ra-ca-common-name	6/19/2025	<b>Client Authentication</b>	Certificates	
Certificates					More Actions	٠
Certificates Certificates Enterprise Trust						

or ×

- 8 ×

\_

確認Manager VPN客戶端的證書

按兩下客戶端證書,導航至詳細資訊,檢查主題的詳細資訊。

• 主題: CN = vpnManagerClientCN

Ce	rtifi	cate

General	Details	Certification Pa	th					
Show:	<al></al>		$\sim$					
Field			Value	^				
(B)			Thursday, June 19, 2025 9:41					
E Su	bject		vpnManagerClientCN, vpnMan					
EL PO	ALC NOY		RSA (2048 Bits)	- 10				
E Put	blic key p	arameters	05 00					
Ke	y Usage		Digital Signature, Key Encipher.					
Enhanced Key Usage			Client Authentication (1.3.6.1					
Netscape Comment			Client Authentication (1.3.6.1 xca certificate					
(C) Th	mhorint	aloorithm	dha 1	¥				
CN = V O = Cis L = Tok S = Tok C = JP	pnManag co cyo cyo	erClientCN		I				
			Edit Properties Copy to File	t				
				OK				

х

Manager客戶端證書的詳細資訊

步驟 2.確認CA

在工程VPN客戶端和管理器VPN客戶端中,導航到證書-當前使用者>受信任的根證書頒發機構>證 書,檢查用於身份驗證的CA。

### • 頒發者:ftd-ra-ca-common-name

Eile Action View Favorites Window	Help					- 8 3
• 🔶 🖄 📷 🐇 🖦 🗶 🖼 🔒 🖬	1					
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Actions
Certificates - Current User	<b>2</b> 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 1
- Tourted Post Cartification Authorities	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati	DigiCert Balt	indic
Cartificater	Class 3 Public Primary Cer	Class 3 Public Primary Cer	8/1/2028	Client Authenticati	VeriSign Clas	ftd-ra-ca 🔺
Certificates	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 Til	
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>	
> Dutrusted Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	Client Authenticati	DigiCert	
> 🔛 Third-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>	
> 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:	
	CONT D CA Y2	DOT DUILO A VO	9/30/2021	Client Authenticati	DST Root CA	
	🙀 ftd-ra-ca-common-name	ftd-ra-ca-common-name	/16/2029	<all></all>	<none></none>	
	cap orobarsign	olooaloigii	3/18/2029	Client Authenticati	GlobalSign R	1

# 驗證

0

步驟 1.啟動VPN連線

在工程VPN客戶端中,啟動Cisco Secure Client連線。無需輸入使用者名稱和密碼,VPN連線成功

Cisco Secur	-		×		
	AnyConnect VPN: Connected to 192.168.1.200. 192.168.1.200	~		Disconnect	
00:01:00				IP	∿4
\$ ①					altalta cisco

從工程師客戶端啟動VPN連線

在Manager VPN客戶端中,啟動Cisco Secure Client連線。無需輸入使用者名稱和密碼,VPN連線 成功。



```
從管理器客戶端啟動VPN連線
```

### 步驟 2.確認FMC中的活動會話

### 導航到Analysis > Users > Active Sessions,檢查VPN身份驗證的活動會話。

Firewall Management Center Overview Analysis / Users / Active Sessions Overview Analysis / Users / Active Sessions Objects Integration Deploy Q & 🚱 🌣 🕢 admin 🗸 the secure									
Switch to legacy UI									
<b>▼</b> s	Y Select X Refresh Log Out								
⊘ Showing all 2 sessions ±									
	Login Time	Realm\Username	Last Seen	Authentication Type	Current IP	Realm	<u>Username</u> ↓	FirstName	Last Nar
	2024-06-19 11:01:19	Discovered Identities\vpnManagerClientCN	2024-06-19 11:01:19	VPN Authentication	172.16.1.120	Discovered Identities	vpnManagerClientCN		
	2024-06-19 <b>11:00:35</b>	Discovered Identities\vpnEngineerClientCN	2024-06-19 <b>11:00:35</b>	VPN Authentication	172.16.1.101	Discovered Identities	vpnEngineerClientCN		

確認活動會話

### 步驟 3.在FTD CLI中確認VPN作業階段

在FTD (Lina) CLI中執行show vpn-sessiondb detail anyconnect命令,以確認工程師和管理員的VPN作業階段。

ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 13 Assigned IP : 172.16.1.101 Public IP : 192.168.1.11 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384 Bytes Tx : 14782 Bytes Rx : 12714 Pkts Tx : 2 Pkts Rx : 32 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : ftd-vpn-engineer-grp Tunnel Group : ftd-vpn-engineer Login Time : 02:00:35 UTC Wed Jun 19 2024 Duration : 0h:00m:55s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : cb0071820000d00066723bc3 Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent: Tunnel ID : 13.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 50225 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7391 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 13.2 Assigned IP : 172.16.1.101 Public IP : 192.168.1.11 Encryption : AES-GCM-128 Hashing : SHA256 Ciphersuite : TLS\_AES\_128\_GCM\_SHA256 Encapsulation: TLSv1.3 TCP Src Port : 50232 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7391 Bytes Rx : 1775 Pkts Tx : 1 Pkts Rx : 2 Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel: Tunnel ID : 13.3 Assigned IP : 172.16.1.101 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 50825 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 0 Bytes Rx : 10939 Pkts Tx : 0 Pkts Rx : 30 Pkts Tx Drop : 0 Pkts Rx Drop : 0

Username : vpnManagerClientCN Index : 14 Assigned IP : 172.16.1.120 Public IP : 192.168.1.21 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384 Bytes Tx : 14782 Bytes Rx : 13521 Pkts Tx : 2 Pkts Rx : 57 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : ftd-vpn-manager-grp Tunnel Group : ftd-vpn-manager Login Time : 02:01:19 UTC Wed Jun 19 2024 Duration : 0h:00m:11s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : cb0071820000e00066723bef Security Grp : none Tunnel Zone : 0 AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1

SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1

AnyConnect-Parent: Tunnel ID : 14.1 Public IP : 192.168.1.21 Encryption : none Hashing : none TCP Src Port : 49809 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7391 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 14.2 Assigned IP : 172.16.1.120 Public IP : 192.168.1.21 Encryption : AES-GCM-128 Hashing : SHA256 Ciphersuite : TLS\_AES\_128\_GCM\_SHA256 Encapsulation: TLSv1.3 TCP Src Port : 49816 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7391 Bytes Rx : 3848 Pkts Tx : 1 Pkts Rx : 25 Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel: Tunnel ID : 14.3 Assigned IP : 172.16.1.120 Public IP : 192.168.1.21 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 65501 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 0 Bytes Rx : 9673 Pkts Tx : 0 Pkts Rx : 32 Pkts Tx Drop : 0 Pkts Rx Drop : 0

### 疑難排解

您可以期待在Lina引擎的調試系統日誌和Windows PC上的DART檔案中找到有關VPN身份驗證的資訊。

這是來自工程師客戶端的VPN連線期間Lina引擎中的調試日誌示例。

### <#root>

Jun 19 2024 02:00:35: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpr Jun 19 2024 02:00:35: %FTD-6-717022:

### Certificate was successfully validated

. serial number: 7AF1C78ADCC8F941, subject name:

#### CN=vpnEngineerClientCN

,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP. Jun 19 2024 02:00:35: %FTD-7-717038: Tunnel group match found.

### Tunnel Group: ftd-vpn-engineer

, Peer certificate: serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN,OU=vpnEnginee Jun 19 2024 02:00:35: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-engineer-grp) for user Jun 19 2024 02:00:46: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50

下面是來自管理器客戶端的VPN連線期間Lina引擎中的調試日誌示例。

### <#root>

Jun 19 2024 02:01:19: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 1AD1B5EAE28C6D3C, subject name: CN=vp Jun 19 2024 02:01:19: %FTD-6-717022:

### Certificate was successfully validated

. serial number: 1AD1B5EAE28C6D3C, subject name:

### CN=vpnManagerClientCN

,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP. Jun 19 2024 02:01:19: %FTD-7-717038: Tunnel group match found.

### Tunnel Group: ftd-vpn-manager

, Peer certificate: serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN,OU=vpnManagerC Jun 19 2024 02:01:19: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-manager-grp) for user Jun 19 2024 02:01:25: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.21/65 <u>為行動存取配置基於Anyconnect證書的身份驗證</u>

### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。