# FMC를 통해 FTD에서 보안 클라이언트에 대한 AAA 및 인증서 인증 구성

목차
<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
<u>배경 정보</u>
<u>네트워크 다이어그램</u>
<u>설정</u>
FMC의 컨피그레이션
<u>1단계. FTD 인터페이스 구성</u>
<u>2단계. Cisco Secure Client 라이센스 확인</u>
<u>3단계. 정책 할당 추가</u>
<u>4단계. 연결 프로파일에 대한 컨피그레이션 세부사항</u>
<u>5단계. 연결 프로파일에 대한 주소 풀 추가</u>
<u>6단계. 연결 프로파일에 대한 그룹 정책 추가</u>
<u>7단계. 연결 프로파일에 대한 보안 클라이언트 이미지 구성</u>
<u>8단계. 연결 프로파일용 컨피그레이션 액세스 및 인증서</u>
<u>9단계. 연결 프로파일에 대한 요약 확인</u>
<u>FTD CLI에서 확인</u>
<u>VPN 클라이언트에서 확인</u>
<u>1단계. 클라이언트 인증서 확인</u>
<u>2단계. CA 확인</u>
<u>다음을 확인합니다.</u>
<u>1단계. VPN 연결 시작</u>
<u>2단계. FMC에서 활성 세션 확인</u>
<u>3단계. FTD CLI에서 VPN 세션 확인</u>
<u>4단계. 서버와의 통신 확인</u>
<u>문제 해결</u>
<u>참조</u>

## 소개

이 문서에서는 FMC에서 AAA 및 인증서 인증을 사용하여 관리하는 FTD에서 SSL을 통한 Cisco Secure Client를 구성하는 단계를 설명합니다.

## 사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Firepower 관리 센터)
- 방화벽 FTD(Threat Defense Virtual)
- VPN 인증 흐름

사용되는 구성 요소

- firepower Cisco Domain Management Center for VMWare 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1
- Cisco Secure Client 5.1.3.62

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

조직에서 더욱 엄격한 보안 조치를 채택함에 따라 2FA(Two-Factor Authentication)와 인증서 기반 인증을 결합하는 것이 보안을 강화하고 무단 액세스를 차단하는 일반적인 관행이 되었습니다. 사용 자 경험 및 보안을 크게 개선할 수 있는 기능 중 하나는 Cisco Secure Client에서 사용자 이름을 미 리 채우는 기능입니다. 이 기능은 로그인 프로세스를 간소화하고 원격 액세스의 전반적인 효율성을 향상시킵니다.

이 문서에서는 미리 채워진 사용자 이름을 FTD의 Cisco Secure Client와 통합하여 사용자가 빠르고 안전하게 네트워크에 연결하는 방법에 대해 설명합니다.

이러한 인증서는 권한 부여 목적으로 사용되는 공통 이름을 포함합니다.

- CA: ftd-ra-ca-common-name
- 클라이언트 인증서: sslVPNClientCN
- 서버 인증서: 192.168.1.200

## 네트워크 다이어그램

이 그림에서는 이 문서의 예에 사용된 토폴로지를 보여줍니다.



네트워크 다이어그램

## 설정

### FMC의 컨피그레이션

1단계. FTD 인터페이스 구성

Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 Interfaces(인터페이스) 탭에 서 대상 FTD 디바이스, config inside and outside interface for FTD(FTD에 대한 인터페이스 내부 및 외부 인터페이스)를 수정합니다.

GigabitEthernet0/0,

- 이름 : 외부
- 보안 영역: outsideZone
- IP 주소: 192.168.1.200/24

GigabitEthernet0/1,

- 이름: inside
- 보안 영역: insideZone
- IP 주소: 192.168.10.200/24

Firewall Management C Devices / Secure Firewall Interface	es Overview	Analysis	Policies Devices	Objects Integration	t	Deploy Q 💕 🌣	∂ admin ∨ dua     cisc     cis	SECURE
1	ware	VTEP						Cancel
All Interfaces Virtual Tunnels					Q. Search by nam	e S	Add In	terfaces ¥
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	۹.4
GigabitEthernet0/0	outside	Physical	outsideZone		192.168.1.200/24(Static)	Disabled	Global	/
GigabitEthernet0/1	inside	Physical	insideZone		192.168.10.200/24(Static)	Disabled	Global	/
GigabitEthernet0/2		Physical				Disabled		/
GigabitEthernet0/3		Physical				Disabled		/

FTD 인터페이스

#### 2단계. Cisco Secure Client 라이센스 확인

Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 대상 FTD 디바이스를 편집 하고 Device(디바이스) 탭에서 Cisco Secure Client 라이센스를 확인합니다.

Firewall Management Center Devices / Secure Firewall Device Summary	iew Analys	sis Policies Devices	Objects Integration		Depk	oy Q 💕 🌣 🛛	admin ~ diada	SECURE
1		License		Ø				
Device Routing Interfaces Inline Sets DHC	P VTEP	License Types Performance Tier:	FTDv5 - 100 Mbps	×				
General	12	Essentials:			m		0	2
Name:	1. 1. 1.4	Export-Controlled Features:			:	Cisco Firepower Threat D	efense for VMware	•
Transfer Packets:	Ye	Malware Defense:					9A33F35ANSU	
Troubleshoot:	Download	IPS:				202	4-06-14 07:38:47	
Mode:	Route	Carrier:			ione:		UTC (UTC+0:00)	
Compliance Mode: Performance Profile:	Defaul	URL:			n: Zone setting for		7.4.1	
TLS Crypto Acceleration:	Disable	Secure Client Premier:			based Rules:		UTC (UTC+0:00)	
		Secure Client Advantage:						
Device Configuration: Import Exp	ort Download	Secure Client VPN Only:	0					
OnBoarding Method: Re	egistration Ke	If a device already has Secure Client VPI	N Only they cannot have					
Increasing Facility		has Secure Client Premier or Secure Client A has Secure Client Premier or Secure Clie have Secure Client VPN Only	ent Advantage it cannot		a com cont			
Inspection Engine					gement		/	
Inspection Engine:	Snort			Cancel Save	e Host Address:		1.114.0.49	,
Revert to Snort 2					dary Address:			

Secure Client 라이센스

#### 3단계. 정책 할당 추가

Devices(디바이스) > VPN > Remote Access(원격 액세스)로 이동하고 Add(추가) 버튼을 클릭합니다.

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

원격 액세스 VPN 추가

필요한 정보를 입력하고 Next(다음) 버튼을 클릭합니다.

- 이름: ftdvpn-aaa-cert-auth
- VPN 프로토콜: SSL
- 대상 장치: 1.x.x.49

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy Q 💕 🌣 🚳 admin ~ 🔤
Remote Access VPN Policy Wizard           Policy Assignment         2 Connection Profile         3 Secure Client         4 Access & Certificate         5 Summary		
Targeted Devices and Protocols         This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.         Imme:*	Before You Start Before you start, ensure the following configuration elements 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 Client downloaded or you have the relevant Cisco credentials to download it during the witzard. Device Interface Interfaces should be already configured on targeted devices should be already configured on targeted for interface group to enable VPN access.	
		Cancel Back Next

정책 할당

#### 4단계. 연결 프로파일에 대한 컨피그레이션 세부사항

연결 프로파일에 필요한 정보를 입력하고 로컬 영역 항목 옆에 있는 + 버튼을 클릭합니다.

- 인증 방법 : 클라이언트 인증서 및 AAA
- 인증 서버: LOCAL
- Username From Certificate(인증서의 사용자 이름): Map specific(맵) 필드
- 기본 필드: CN(공통 이름)
- 보조 필드: OU(조직 단위)

Remote Access VPN Policy Wizard	
1 Policy Assignment 6 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.* / ftdxpn-aaa-cert-auth	
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 & AAA	
Authentication Server:* LOCAL  (LOCAL or Reatin or RADIUS) +	
Local Realm.* v +	
Prefil usemame from certificate on user login window	
Username From  Map specific field  Vise entire DN (Distinguished Name) as username  Certificate:	
Primary Field: CN (Common Name)	
Secondary Field: OU (Organisational Unit)	

연결 프로파일 세부사항

Add Realm(영역 추가) 드롭다운 목록에서 Local(로컬)을 클릭하여 새 로컬 영역을 추가합니다.

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

로컬 영역 추가

로컬 영역에 필요한 정보를 입력하고 Save(저장) 버튼을 클릭합니다.

- 이름: LocalRealmTest
- 사용자 이름: sslVPNClientCN



#### 참고: 사용자 이름은 클라이언트 인증서 내의 공통 이름과 같습니다

Name*	Description
LocalRealmTest	
Local User Configuration	
∧ ssIVPNClientCN	
Username	
ssiVPNClientCN	
Password	Confirm Password

#### Add another local user

Save	Cancel

로컬 영역 세부 정보

#### 5단계. 연결 프로파일에 대한 주소 풀 추가

### IPv4 Address Pools(IPv4 주소 풀) 항목 옆에 있는 edit(수정) 버튼을 클릭합니다.

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

<ul> <li>Use AAA Server (Realm or RADIUS only)</li> </ul>	
Use DHCP Servers	
Jse IP Address Pools	
IPv4 Address Pools:	/
IPv6 Address Pools:	/

IPv4 주소 풀 추가

새 IPv4 주소 풀을 추가하는 데 필요한 정보를 입력합니다. 연결 프로파일에 대한 새 IPv4 주소 풀을 선택합니다.

- 이름: ftdvpn-aaa-cert-pool
- IPv4 주소 범위: 172.16.1.40-172.16.1.50

 $\mathbf{0} \times$ 

• 마스크: 255.255.255.0

### Add IPv4 Pool

Name* ftdvpn-aaa-cert-pool		
Description		
IPv4 Address Range* 172.16.1.40-172.16.1.50		
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150 Mask* 255.255.255.0		
<ul> <li>Allow Overrides</li> <li>Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices</li> </ul>		
<ul> <li>Override (0)</li> </ul>		
	Cancel	Save
IPv4 주소 풀 세부 정보 6단계. 연결 프로파일에 대한 그룹 정책 추가		
그룹 정책 항목 옆에 있는 + 단추를 클릭합니다. Group Policy: A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object. Group Policy: Edit Group Policy		
	Cancel	Back
그룹 정책 추가		

0

새 그룹 정책을 추가하는 데 필요한 정보를 입력합니다. 연결 프로파일에 대한 새 그룹 정책을 선택

### 합니다.

- 이름: ftdvpn-aaa-cert-grp
- VPN 프로토콜: SSL

### Add Group Policy

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

0



7단계. 연결 프로파일에 대한 보안 클라이언트 이미지 구성

보안 클라이언트 이미지 파일을 선택하고 Next(다음) 버튼을 클릭합니다.

Firewall Management Center Overview And Devices / VPN / Setup Wizard	alysis Policies Objects Integration	Deploy Q 🧳 🌣 🕲 admin 🗸 🐝 SECURE
Remote Access VPN Policy Wizard		
Policy Assignment 2 Connection Profile 3	Secure Client 4 Access & Certificate (5) Summary	
	Remote Secure Citent Internet Outside User Inside Corporate Resources	
	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-webdepto Windows 💌	



Secure Client Image(보안 클라이언트 이미지) 선택

#### 8단계. 연결 프로파일용 컨피그레이션 액세스 및 인증서

#### VPN 연결을 위한 보안 영역을 선택하고 인증서 등록 항목 옆에 있는 + 버튼을 클릭합니다.

• 인터페이스 그룹/보안 영역: outsideZone

Firewall Management Center Overview Analysis P	olicies Devices Objects Integration	Deploy Q 🗳 🌣 🔕 admin 🗸 號 SECURE
Remote Access VPN Policy Wizard   Policy Assignment  Connection Profile  Secure Clie	nt (§) Summary	
Remote	Cutsise User Inside Corporate Resources	
	Network Interface for Incoming VPN Access Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections. Interface group/Security Zone.* outsideZone + + Control C	
	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.*	

보안 영역 선택

#### FTD 인증서에 필요한 정보를 입력하고 로컬 컴퓨터에서 PKCS12 파일을 가져옵니다.

- 이름: ftdvpn-cert
- 등록 유형: PKCS12 파일

### Add Cert Enrollment

Nam ftc	ie* dvpn-cert						Î
Des	cription						
Ci	A Information	C	ertificate Paramet	ers Key	Revo	ocation	-
	Enrollment T	ype:	PKCS12 File		¥		
	PKCS12 F	File*:	ftdCert.pfx			Browse PKCS12 File	
	Passphra	se*:					
	Validation Us	age:	IPsec Client	SSL Client	<u>s</u>	SL Server	
			Skip Check fo	or CA flag in bas	sic con	nstraints of the CA Certificate	
							-
						Cancel Saw	D

FTD 인증서 추가

Access & Certificate(액세스 및 인증서) 마법사에서 입력한 정보를 확인하고 Next(다음) 버튼을 클 릭합니다.

0



참고: 암호 해독된 VPN 트래픽이 액세스 제어 정책 검사를 받지 않도록 암호 해독된 트래픽에 대해 Bypass Access Control 정책을 활성화합니다(sysopt permit-vpn).

Firewall Management Center Overview Analysis Polic Devices / VPN / Setup Wizard	ies Devices Objects Integration	Deploy Q 🧬 🌣 🕢 admin - 👘 SECURE
Remote Access VPN Policy Wizard		
1 Policy Assignment (2) Connection Profile (3) Secure Client	Access & Certificate 5 Summary	
Permote User	Secure Client Internet Outside United Inside Corporate Resources	
	Network Interface for Incoming VPN Access	
	Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections. Interface group/Security Zone.* outsideZone ++ Enable DTLS on member interfaces	
	▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.	
	Device Certificates	
	Device certificate (also called identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.	
	Certificate Enrollment.*  tdvpn-cert  +	
	Enroll the selected certificate object on the target devices	
	Access Control for VPN Traffic	
	All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.	
	Pippass Access Control policy for decrypted traffic (syspet permit-yph) This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.	
(		•
		Cancel Back Next

액세스 및 인증서의 설정 확인

#### 9단계. 연결 프로파일에 대한 요약 확인

### VPN 연결을 위해 입력한 정보를 확인하고 Finish(마침) 버튼을 클릭합니다.

![](_page_12_Picture_4.jpeg)

VPN 연결 설정 확인

#### 원격 액세스 VPN 정책의 요약을 확인하고 FTD에 설정을 구축합니다.

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects	Integration	Deploy Q 💕 🌣 🕻	admin ~ states SECURE
ftdvpn-aaa-cert-auth				Save Cancel
Enter Description				
				Policy Assignments (1)
Connection Brofile Access Interfaces Advanced			Local Realm: LocalRealmTest	Dynamic Access Policy: None
Connection Prome Access internaces Advanced				
				+
				Ŧ
Name	AAA	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DthOrpPolicy	_	/i
ftdvpn-aaa-cert-auth	Authentication: Client Certificate & LOCAL Authorization: None Accounting: None	B ftdvpn-aaa-cert-orp		/1

원격 액세스 VPN 정책 요약

### FTD CLI에서 확인

FMC에서 구축한 후 FTD CLI에서 VPN 연결 설정을 확인합니다.

// Defines IP of interface interface GigabitEthernet0/0 nameif outside security-level 0 ip address 192.168.1.200 255.255.255.0 interface GigabitEthernet0/1 nameif inside security-level 0 ip address 192.168.10.200 255.255.255.0 // Defines a pool of addresses ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0 // Defines a local user username sslVPNClientCN password \*\*\*\*\* encrypted // Defines Trustpoint for Server Certificate crypto ca trustpoint ftdvpn-cert keypair ftdvpn-cert crl configure // Server Certificate Chain crypto ca certificate chain ftdvpn-cert certificate 22413df584b6726c 3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7 . . . . . . quit certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 . . . . . . quit // Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client

enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows" anyconnect enable tunnel-group-list enable cache disable error-recovery disable // Bypass Access Control policy for decrypted traffic // This setting is displayed in the 'show run all' command output sysopt connection permit-vpn // Configures the group-policy to allow SSL connections group-policy ftdvpn-aaa-cert-grp internal group-policy ftdvpn-aaa-cert-grp attributes banner none wins-server none dns-server none dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-tunnel-network-list none default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable // Configures the tunnel-group to use the aaa & certificate authentication tunnel-group ftdvpn-aaa-cert-auth type remote-access tunnel-group ftdvpn-aaa-cert-auth general-attributes address-pool ftdvpn-aaa-cert-pool default-group-policy ftdvpn-aaa-cert-grp // These settings are displayed in the 'show run all' command output. Start authentication-server-group LOCAL secondary-authentication-server-group none

no accounting-server-group default-group-policy ftdvpn-aaa-cert-grp username-from-certificate CN OU secondary-username-from-certificate CN OU authentication-attr-from-server primary authenticated-session-username primary username-from-certificate-choice second-certificate secondary-username-from-certificate-choice second-certificate // These settings are displayed in the 'show run all' command output. End tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes authentication aaa certificate pre-fill-username client group-alias ftdvpn-aaa-cert-auth enable

## VPN 클라이언트에서 확인

1단계. 클라이언트 인증서 확인

Certificates - Current User > Personal > Certificates로 이동하여 인증에 사용되는 클라이언트 인증 서를 확인합니다.

🚘 Console1 - [Console Root\Certificates - Curren	t User\Personal\Certificates]				-	o ×
Eile Action View Favorites Window	Help					- 8 ×
🗢 🔶 🙇 📷 🛍 🔯 🔂 📷						
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Actions
Gertificates - Current User	SslVPNClientCN	ftd-ra-ca-common-name	6/16/2025	<b>Client Authentication</b>	ssIVPNClientCer	Certificates 🔺
Certificates						More 🕨
Inusted Koot Certification Authorities						
Certificates						
> interprise Trust						

클라이언트 인증서 확인

클라이언트 인증서를 두 번 클릭하고 Details(세부사항)로 이동하여 Subject(주체)의 세부사항을 확 인합니다.

• 제목: CN = sslVPNClientCN

## 🕵 Certificate

Seneral	Details	Certification Pa	sth	
Show:	<al></al>		$\sim$	
Field Sig Sig	nature al nature h	gorithm ash algorithm	Value sha256RSA sha256 ftd-ra-ca-common-	name, Cisc
Va Va	lid from lid to bject		Sunday, June 16, Monday, June 16, ssiVPNClientCN, ss RSA (2048 Bits)	2024 6: 12:0 2025 6: 12: VPNClientO
CN = s 0 = Ck L = Tok S = Tok C = JP	siVPNClier siVPNClier sive inclice sco sco syo kyo	ntCN	05.00	~
		[	Edit Properties	Copy to File
				OK

X

2단계. CA 확인

Certificates - Current User(인증서 - 현재 사용자) > Trusted Root Certification Authorities(신뢰할 수

있는 루트 인증 기관) > Certificates(인증서)로 이동하여 인증에 사용된 CA를 확인합니다.

• 발급자: ftd-ra-ca-common-name

📸 Console1 - [Console Root\Certificates - Current	t User\Trusted Root Certification A	uthoritie Certificates]			-	٥	×	<
File Action View Favorites Window	Help						- 8	×
🗢 🔶 🙇 📷 🐇 🗞 🗙 📾 🖬								
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Actions		
✓ G Certificates - Current User	COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	Certific	ates	
Personal     Certificates	Copyright (c) 1997 Micros	Copyright (c) 1997 Micros	12/30/1999	Time Stamping	Microsoft Til	Mo	ore	۲
Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	<all></all>	<none></none>	ftd-ra-o	a	•
2 Cincipise Trost	DigiCert Assured ID Root	DigiCert Assured ID Root DigiCert Global Root CA	11/9/2031	Client Authenticati	DigiCert	Me	ore	•
> Intermediate Certification Authorities > Intermediate Certification Authorities > Intermediate Directory User Object	DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati	DigiCert Glol			
> 🔛 Trusted Publishers	DigiCert High Assurance	DigiCert High Assurance	11/9/2031	<all></all>	<none></none>			
> Untrusted Certificates	DigiCert High Assurance	DigiCert High Assurance DigiCert Trusted Beet G4	11/9/2031	Client Authenticati	DigiCert DigiCert Tour			
> Inited Party Root Certification Authoriti > Inited People		DCT Rest CA X2	0/20/2021	Client Authenticati	DGT Deet CA			
> Client Authentication Issuers	🙀 ftd-ra-ca-common-name	ftd-ra-ca-common-name	6/16/2029	<all></all>	<none></none>			
> Smart Card Trusted Roots	ClobalCiga	ClobalCiga	2/10/2020	Clines Andhorstinut	ClobalCign I			
> 🙀 Certificates (Local Computer)	🔄 GlobalSign	GlobalSign	12/15/2021	Client Authenticati	Google Trust			

CA 확인

# 다음을 확인합니다.

1단계. VPN 연결 시작

엔드포인트에서 Cisco Secure Client 연결을 시작합니다. 사용자 이름은 클라이언트 인증서에서 추 출됩니다. VPN 인증을 위해 비밀번호를 입력해야 합니다.

![](_page_18_Picture_0.jpeg)

참고: 사용자 이름은 이 문서에 있는 클라이언트 인증서의 CN(Common Name) 필드에서 추출됩니다.

Sisco Secure Client		Q.	$\times$	Sisco Secure Client   192.168.1.200	S Cisco Secure Client   192.168.1.200 X		- 🗆 X
AnyConnect VPI: Contacting 192.168.1.200. 192.168.1.200	V	Connect		Group: ftdvpn-aaa-cert-auth	~	AnyConnect VPH: Connected to 192.168.1.200. 192.168.1.200	<ul> <li>Disconnect</li> </ul>
				Password:		00:00:07	IPv4
¢ ()			cisco			\$	-sh-sh- cisco
				OK Cancel			

VPN 연결 시작

2단계. FMC에서 활성 세션 확인

Analysis(분석) > Users(사용자) > Active Sessions(활성 세션)로 이동하여 활성 세션에서 VPN 인증 을 확인합니다.

ē	Firewall Managemen Analysis / Users / Active Sess	t Center Overview An	1 Overview Analysis Policies Devices Objects Integration Deploy Q, 🧬 Q 🕢 admin - d SECURE								SECURE					
Switch to legacy U									legacy UI							
<b>T</b>	lelect													×	Refresh	og Out
0	bowing the 1 and only session	<u>E</u>			_										15	
	LosinTime	Realm/Username	Last.Seen 4	Authentication Type	Current IP	Baales	Usemane	Exxt.Name	Last Name	Email	Department	Phone Number	Discovery. Application	Device		^
	2024-06-17 11:38:22	LocalRealmTest(ssIVPNClientCN	2024-06-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	ss/VPNC/ientCN						LDAP	1		

활성 세션 확인

#### 3단계. FTD CLI에서 VPN 세션 확인

FTDshow vpn-sessiondb detail anyconnect(Lina) CLI에서 명령을 실행하여 VPN 세션을 확인합니다.

ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384 Bytes Tx : 14780 Bytes Rx : 15386 Pkts Tx: 2 Pkts Rx: 37 Pkts Tx Drop: 0 Pkts Rx Drop: 0 Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth Login Time : 02:38:22 UTC Mon Jun 17 2024 Duration: 0h:01m:22s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : cb00718200007000666fa19e Security Grp: none Tunnel Zone: 0

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

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

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

DTLS-Tunnel: Tunnel ID : 7.3 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 56382 UDP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 0 Bytes Rx : 13094 Pkts Tx : 0 Pkts Rx : 34 Pkts Tx Drop : 0 Pkts Rx Drop : 0

4단계. 서버와의 통신 확인

VPN 클라이언트에서 서버로 ping을 시작하고 VPN 클라이언트와 서버 간의 통신이 성공했는지 확인합니다.

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

Ping 성공

FTD(capture in interface inside real-timeLina) CLI에서 명령을 실행하여 패킷 캡처를 확인합니다.

```
ftd702#
```

#### capture in interface inside real-time

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

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

#### 문제 해결

Lina 엔진의 디버그 syslog 및 Windows PC의 DART 파일에서 VPN 인증에 대한 정보를 찾을 수 있습니다.

Lina 엔진의 디버그 로그 예입니다.

#### // Certificate Authentication

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

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

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

// AAA Authentication

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

#### 이러한 디버그는 컨피그레이션 문제를 해결하기 위해 사용할 수 있는 정보를 제공하는 FTD의 진단 CLI에서 실행할 수 있습니다.

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

참조

모바일 액세스를 위한 Anyconnect 인증서 기반 인증 구성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.