

لي م عمل اة ق داصم ل CERT ني ني عت ني وكت FMC ربع FTD ىل ع ن م آلا

تا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س اس آلا تا ب ل ط ت م ل ا](#)

[تا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا تا ن و ك م ل ا](#)

[ة ي س اس آ تا م و ل ع م](#)

[ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[تا ن ي و ك ت ل ا](#)

[FMC ي ف ني و ك ت ل ا](#)

[FTD ة و ج ا و ني و ك ت 1. ة و ط خ ل ا](#)

[Cisco Secure Client ص ي خ ر ت د ي ك ا ت 2. ة و ط خ ل ا](#)

[IPv4 ني و ن ع ع م ج ت ة ف ا ض ا 3. ة و ط خ ل ا](#)

[ة و م و ح م ل ا ج و ن ة ف ا ض ا 4. ة و ط خ ل ا](#)

[FTD ة د ا ه ش ة ف ا ض ا 5. ة و ط خ ل ا](#)

[س د ن ه م ل ا ل ا ص ت ا ف ي ر ع ت ف ل م ل ج و ن ني ي ع ت ة ف ا ض ا 6. ة و ط خ ل ا](#)

[س د ن ه م ل ا ل ا ص ت ا ف ي ر ع ت ف ل م ل ي ص ا ف ت ني و ك ت 7. ة و ط خ ل ا](#)

[س د ن ه م ل ا ل ا ص ت ا ف ي ر ع ت ف ل م ل ة ت م آ ل ي م ع ة ر و ص ني و ك ت 8. ة و ط خ ل ا](#)

[س د ن ه م ل ا ل ا ص ت ا ف ي ر ع ت ف ل م ل ة د ا ه ش ل ا و ل و ص و ل ا ني و ك ت 9. ة و ط خ ل ا](#)

[س د ن ه م ل ا ل ا ص ت ا ف ي ر ع ت ف ل م ل ص خ ل م ل ا د ي ك ا ت 10. ة و ط خ ل ا](#)

[VPN م ا ن ا ج ل ل ا ص ت ا ل ا ف ي ر ع ت ف ل م ة ف ا ض ا 11. ة و ط خ ل ا](#)

[تا د ا ه ش ة ط ي ر خ ة ف ا ض ا 12. ة و ط خ ل ا](#)

[ل ا ص ت ا ل ا ف ي ر ع ت ف ل م ب ة د ا ه ش ل ا ط ط خ م ط ب ر 13. ة و ط خ ل ا](#)

[FTD ب ة ص ا خ ل ا \(CLI\) ر م ا و آ ل ا ر ط س ة و ج ا و ي ف د ي ك ا ت ل ا](#)

[VPN ة ك ب ش ل ي م ع ي ف د ي ك ا ت](#)

[ل ي م ع ل ا ة د ا ه ش د ي ك ا ت 1. ة و ط خ ل ا](#)

[CA د ي ك ا ت 2. ة و ط خ ل ا](#)

[ة ح ص ل ا ن م ق ق ح ت ل ا](#)

[VPN ل ا ص ت ا ع د ب 1. ة و ط خ ل ا](#)

[FMC ي ف ة ط ش ن ل ا ت ا س ل ج ل ا د ي ك ا ت 2. ة و ط خ ل ا](#)

[FTD CLI ي ف VPN ل م ع ت ا س ل ج د ي ك ا ت 3. ة و ط خ ل ا](#)

[ا ه ج ا ل ص ا و ع ا ط خ آ ل ا ف ا ش ك ت س ا](#)

[ة ل ص ت ا ذ تا م و ل ع م](#)

ة م د ق م ل ا

م ا د خ ت س ا ب FMC ربع FTD ىل ع SSL ع م Cisco Secure Client د ا د ع ا ي ف ي ك د ن ت س م ل ا ا ذ ه ح و ي ة ق د ا ص م ل ل ة د ا ه ش ل ا ني ي ع ت .

ة ي س اس آلا تا ب ل ط ت م ل ا

تاب لطلت مل

ة لالتل عيضاوم لابل ة فرعم كيدل نوكت نأب Cisco ي صوت

- Cisco نم FireSIGHT (FMC) ةراد زكرم
- يرهاظلا (FTD) ةياملال رادج ديهت دض عافدلا
- VPN ةقداصم قفدت

ةمدختس مل تانوك مل

- Cisco Firepower ل VMWare 7.4.1 ةراد زكرم
- Cisco Firewall Threat Defense Virtual 7.4.1
- Cisco Secure Client 5.1.3.62

ةصاخ ةيلمعم ةئي ب ي ةدووم ل ةزهأل نم دنتس مل اذ ي ةدراول تامولعمل ءاشن ا مت تنك اذ ا. (يضا رتفا) حوسمم نيوك تب دنتس مل اذ ي ةمدختس مل ةزهأل عي م ج ت اد ب رم أ ي آل لم ت حمل ري ثأ تل ل كم هف نم دكأت ف، لي غش تل دي ق ك تك ب ش

ةيساس ا تامولعم

يلع لي مع ةداهش ني يع ت متي ثي ح VPN تالاصت ا ي ف مدختست ةقيرط يه ةداهش ل طي طخت ةيلمع هذه. لي وختل ضارغأل ةداهش ل ل خاد تامس ل ا م ادختس ا متي و ا، ي ل حم مدختس م باس ح ني يع ت م ادختس اب. زاهج و ا م دختس م في رع تل ةلي سو ك ةيم قرل ا ةداهش ل ا م ادختس ا ه ي ف متي ت ا نا ي ب ل ا خ د ا ي ل ة ج ا ح ل ل ن و د ني م دختس م ل ا ة ق د ا ص م ل SSL لو ك و ت و ر ب ل غ ت س ي ه ن ا ف، ة د ا ه ش ل ا د ا م ت ع ا ل ا

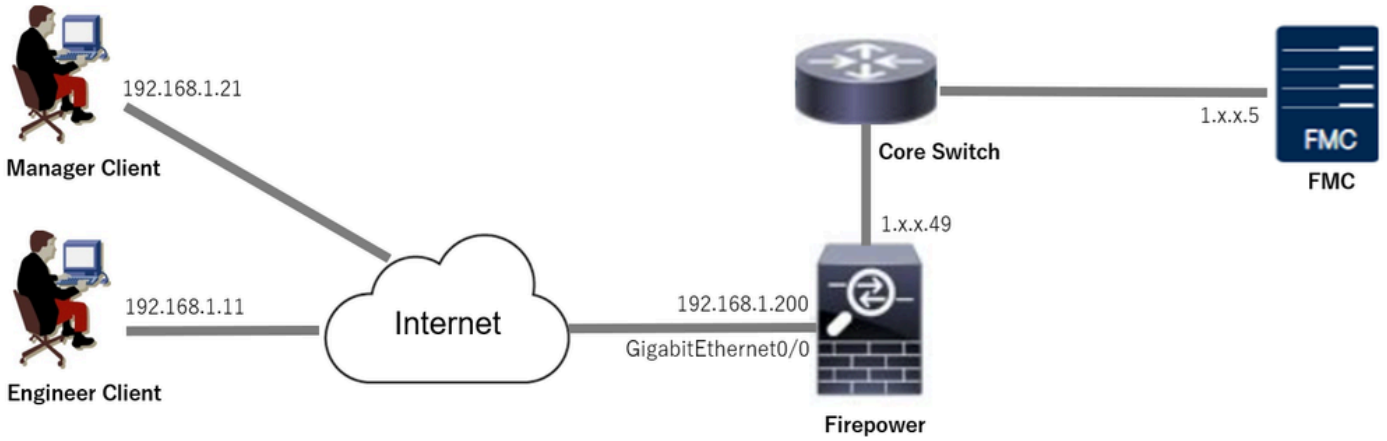
ةداهش نم عئاشل ل م س ا ل ا م ادختس اب نم آل Cisco لي مع ةقداصم ةي ف ي ك دنتس مل اذ ي ح ض و ي SSL.

لي وختل ل ضارغأل هم ادختس ا متي، اهل خاد ب كرتشم م س ا ي ل ع ت ا د ا ه ش ل ا ه ذ ي و ت ح ت

- عئاشل ل ftd-ra-ca-name: أ ك
- س دن هم ل ل VPN ةك ب ش لي مع ةداهش: vpnEngineerClientCN
- م ا د خ ت س م ل ل م ا د خ ت س م ل ل م a n a g e r V P N : vpnManagerClientCN
- م د ا خ ل ا ة د ا ه ش : 192.168.1.200

ةك ب ش ل ل ي ط ي ط خ ت ل م س ر ل ا

دنتس مل اذ ي ل ا ث م ل هم ادختس ا متي ي ذل ا ط ط خ م ل ا ة ر و ص ل ا ه ذ ي ض ر ع ت



ةكبش ل ل يطيطختل مسرلا

تانيوكتلا

FMC في نيوكتلا

ةهجاو نيوكت 1. ةوطخلا

ل FTD ل ةيچراخل ةهجاو نيوكت ب مقو، فدهل FTD زاهاج رحو، ةزهجال ةرادا > ةزهجالا ل ل لقتنا inInterfacestab.

ل GigabitEthernet0/0.

- چراخ: مسالا
- ةقطنملا چراخ: ةني نمألا ةقطنملا
- IP: 192.168.1.200/24 ناو نع

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies Devices Objects Integration

Deploy Search admin

1.17.1.49 Save Cancel

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

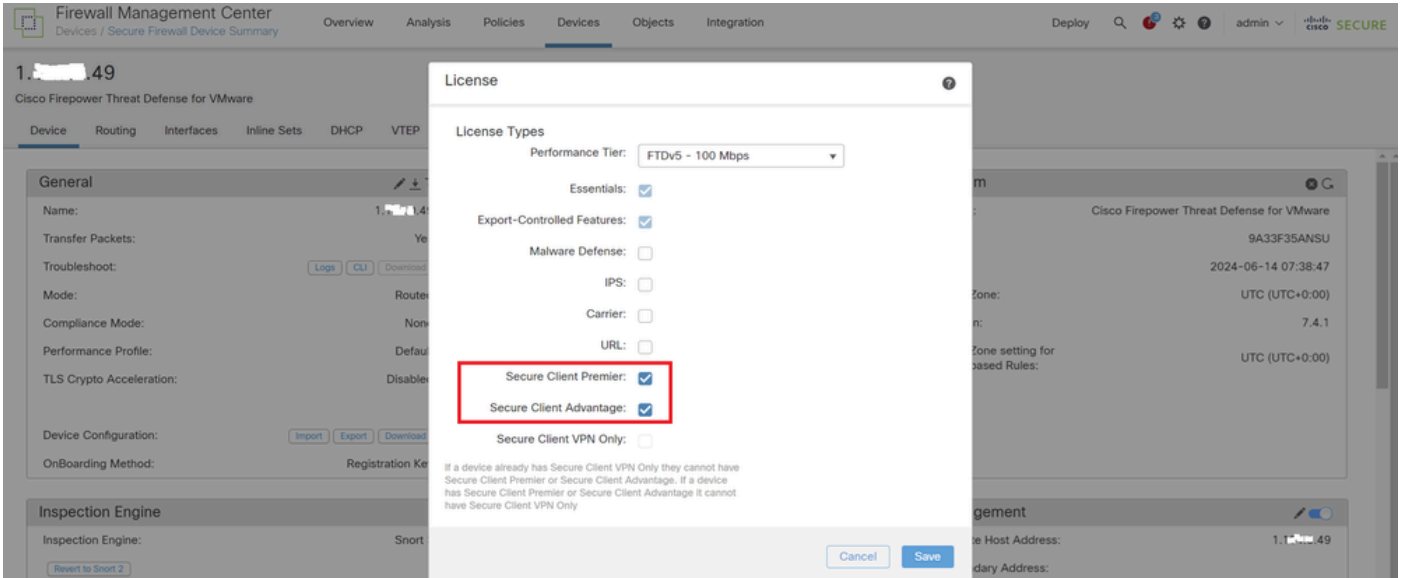
All Interfaces Virtual Tunnels Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical	outsideZone		192.168.1.200/24(Static)	Disabled	Global

ةهجاو FTD

Cisco Secure Client صيخرت ديكأت 2. ةوطخلا

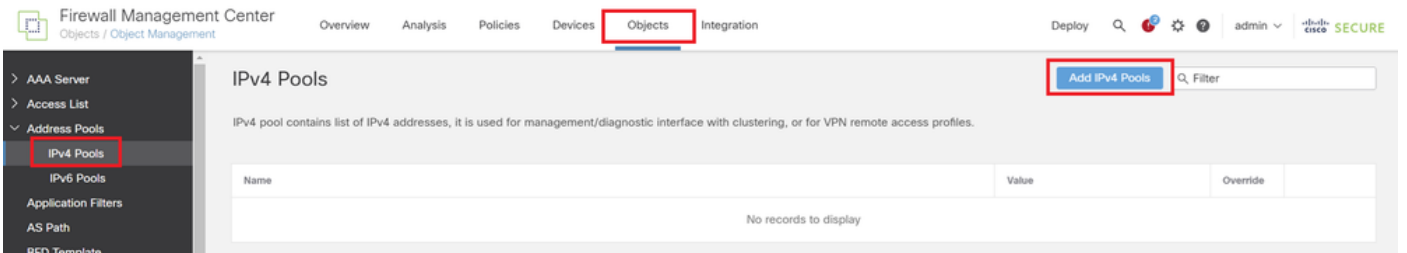
ل Cisco Secure Client صيخرت نم دكأتو، فدهل FTD زاهاج رحو، ةزهجالا ةرادا > ةزهجالا ل لقتنا في DeviceTab.



نمآل ليمعلا صيخرت

IPv4 نيوانع عمجت ةفاضل 3 ةوطخل

مرح ةفاضل رزل قوف رقنا، IPv4 تاعمجت > نيوانعلا تاعمجت > نئاكل اقراد > Object لى لقتنا IPv4.



IPv4 نيوانع عمجت ةفاضل

سندنهملل VPN ليمعلا IPv4 نيوانع عمجت ءاشنال ةيروضلل تامولعمللا لخداب مق

- مرسال: ftd-vpn-engineer-pool
- ناوئع قاطن IPv4: 172.16.1.100-172.16.1.110
- عانقل: 255.255.255.0

Edit IPv4 Pool



Name*

ftd-vpn-engineer-pool

Description

IPv4 Address Range*

172.16.1.100-172.16.1.110

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

255.255.255.0

Allow Overrides

i 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

سندنهملل VPN ليمعمل IPv4 نيوانع عمجت

ريدملاب صاخال VPN ليمعمل IPv4 نيوانع عمجت عاشنال ةرورضال تامولعمل لخدأ

- مسال: ftd-vpn-manager-pool
- IPv4 نيوانع قاطن: 172.16.1.120-172.16.1.130
- عانقال: 255.255.255.0

Add IPv4 Pool



Name*

ftd-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

Allow Overrides

i 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

ريدم ل VPN لي م عمل IPv4 ني وان ع م ع م ح ت

ة دي د ج ل IPv4 ني وان ع م ح ت دي ك أ ت .

Name	Value	Override	
ftd-vpn-engineer-pool	172.16.1.100-172.16.1.110	<input checked="" type="checkbox"/>	
ftd-vpn-manager-pool	172.16.1.120-172.16.1.130	<input checked="" type="checkbox"/>	

ة دي د ج ل IPv4 ني وان ع م ح ت

ة ع م ح ل ا ج ه ن ة ف ا ض ا . 4 ة و ط خ ل ا

ة ع م ح ل ا ج ه ن ة ف ا ض ا ر ز ق و ف ر ق ن ا ، ة ع م ح ل ا ج ه ن > VPN > ن ئ ا ك ل ا ة ر ا د ا > Object ل ل ل ق ت ن ا

Firewall Management Center

Overview Analysis Policies Devices **Objects** Integration

Deploy Filter admin

Objects / Object Management

PKI
Policy List
Port
Prefix List
Route Map
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable Set
VLAN Tag
VPN
Certificate Map
Custom Attribute
Group Policy

Add Group Policy Filter

Group Policy

A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

Name: DftGrpPolicy

ةوعومجم لآ جهن ةفاضلآ

Engineer VPN لآ لآ عمل ةوعومجم ةسلس ءاشنل ءل ءرورضلل ءاملول عمل لآ ءءءب مق

- ملسال: ftd-vpn-engineer-grp
- VPN: SSL ءالوك وءورب

Add Group Policy

Name:*

ftd-vpn-engineer-grp

Description:

General Secure Client Advanced

VPN Protocols

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

IP Address Pools
Banner
DNS/WINS
Split Tunneling

سءنهملل VPN ءكبش لآ لآ عمل ةوعومجم لآ جهن

رآءمل ءب صءءل VPN لآ لآ عمل ةوعومجم ةسلس ءاشنل ءل ءرورضلل ءاملول عمل لآ ءءءب

- ملسال: ftd-vpn-manager-grp
- VPN: SSL ءالوك وءورب

Add Group Policy



Name:*

Description:

General Secure Client Advanced

VPN Protocols

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

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Manager ليمعمل وعومحمل جهن

ةدي دجالا وعومحمل جهن دي كأت.

Firewall Management Center

Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Help admin

PKI

Policy List

Port

Prefix List

Route Map

Security Intelligence

Sinkhole

SLA Monitor

Time Range

Time Zone

Tunnel Zone

Group Policy

Add Group Policy Filter

A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

Name	
DfltGrpPolicy	
ftd-vpn-engineer-grp	
ftd-vpn-manager-grp	

ةدي دج وعومحمل جهن

FTD ةداهش ةفاضلا 5. ةوطخل

ليجست ةفاضلا رزلا قوف رقنا، اعاطتقالا ليجست > PKI > نئاللا ةرادا > Object > لى لقتنا اعاطتقالا.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ ⓘ admin 🔽 Cisco SECURE

Cert Enrollment

[Add Cert Enrollment](#)

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Name	Type	Override
No records to display		

Navigation: Cipher Suite List, Community List, DHCP IPv6 Pool, Distinguished Name, DNS Server Group, External Attributes, File List, FlexConfig, Geolocation, Interface, Key Chain, Network, PKI, **Cert Enrollment**, External Cert Groups

داهشل ليجست ةفاضل

يلحم بساح نم PKCS12 فلم داري ت ساو FTD داهشل ةرورضلا تامولعمل ل اخداب مق

- م سال: ftd-vpn-cert
- فلم: ليجست ل عون PKCS12

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 [Browse PKCS12 File](#)

Passphrase*:

Validation Usage: IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

[Cancel](#) [Save](#)

ةداهش لىجست لىصافت

ديدل ةداهش لىجست دىكأت

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Help admin Cisco SECURE

Cert Enrollment

Add Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Name	Type	Override
ftd-vpn-cert	PKCS12 File	

ديج ةداهش لىجست

ةفاضل رز قوف رقنا ، تاداهش لى > ةزهأل لى لىقتنا

Firewall Management Center
Devices / Certificates

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Help admin Cisco SECURE

Devices

Filter: All Certificates

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
------	--------	-----------------	-----------------------------	-----------------------	--------

No certificates Add Certificates

Add

ةداهش ةفاضل

ب FTD ةديدل ةداهش لىجست طبرل ةرورض لى تامول عمل لىخدأ

- زاهل: 1.x.x.49
- ةداهش لىجست: FTD-VPN-CERT

Add New Certificate



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

Device*:
1.1.1.1.49

Cert Enrollment*:
ftd-vpn-cert

Cert Enrollment Details:

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

Cancel

Add

FTD بةداهشلا طبر

ةداهشلا طبر ةلاح ديكأت.

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
1.1.1.1.49					
ftd-vpn-cert	Global	PKCS12 file	Jun 16, 2025	Jun 16, 2029	CA, ID

ةداهشلا طبر ةلاح

سدنهملا لاصتا فيرعت فلمل جهن نييعت ةفاضلا 6 ةوطخلا

AddButton قوف رقنا، دعب نع لوصولا > VPN > ةزهجألا لىل لقتنا

Name	Status	Last Modified
No configuration available Add a new configuration		

دعب نع لوصولا VPN ةكبش ةفاضلا

Nextbutton قوف رقناو ةرورضلا تامولعملا لاداب مق

- ماسال: ftd-vpn-engineer
- VPN: SSL تالوكوتورب
- ةفدهتسمل ةزهجال: 1.x.49

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Help admin cisco SECURE

Remote Access VPN Policy Wizard

1 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.

Name:*
ftd-vpn-engineer

Description:

VPN Protocols:

SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices: 1.x.49

Selected Devices: 1.x.49

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 wizard.

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 Next

جهنل نبيعت

سدنهملا لاصتا فيرعت فلم ليصافت نيوكت 7 ةوطخلا

Nextbutton قوف رقناو ةرورضلا تامولعملال لاختاب مق

- طقف ليمعلا ةداهش: ةقداصملا بولسا
- نبيعتلل دحم لقح: ةداهشلل نم مدختسملا مسا
- (عئاشلا ماسالا) CN: يساسالا لقحلا
- (ةيميظنتلا ةدحوالا) OU: يوناتلا لقحلا
- IPv4 نيوانع تاعمجت: ftd-vpn-engineer-pool
- ةومجملا جهن: ftd-vpn-engineer-grp

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:*

i 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:

Username From Certificate: Map specific field Use entire DN (Distinguished Name) as username

Primary Field:

Secondary Field:

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 selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

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:*

[Edit Group Policy](#)

Cancel Back **Next**

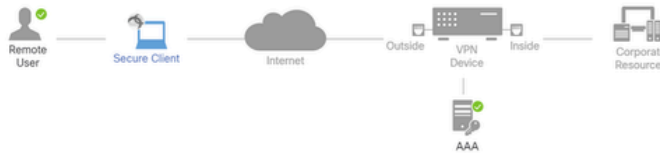
لاصتالال فيرعت فلم لىصافت

سدنهملا لاصتالال فيرعت فلم لىصافت نم لىصافت ةروص نيوكت 8 ةوطخلا

Nextbutton قوف رقاو نم لىصافت ةروص فلم دح

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **Secure Client** 4 Access & Certificate 5 Summary



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](#) +

<input checked="" type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	cisco-secure-client-win-5.1.3.6...	cisco-secure-client-win-5.1.3.62-webdepl...	Windows

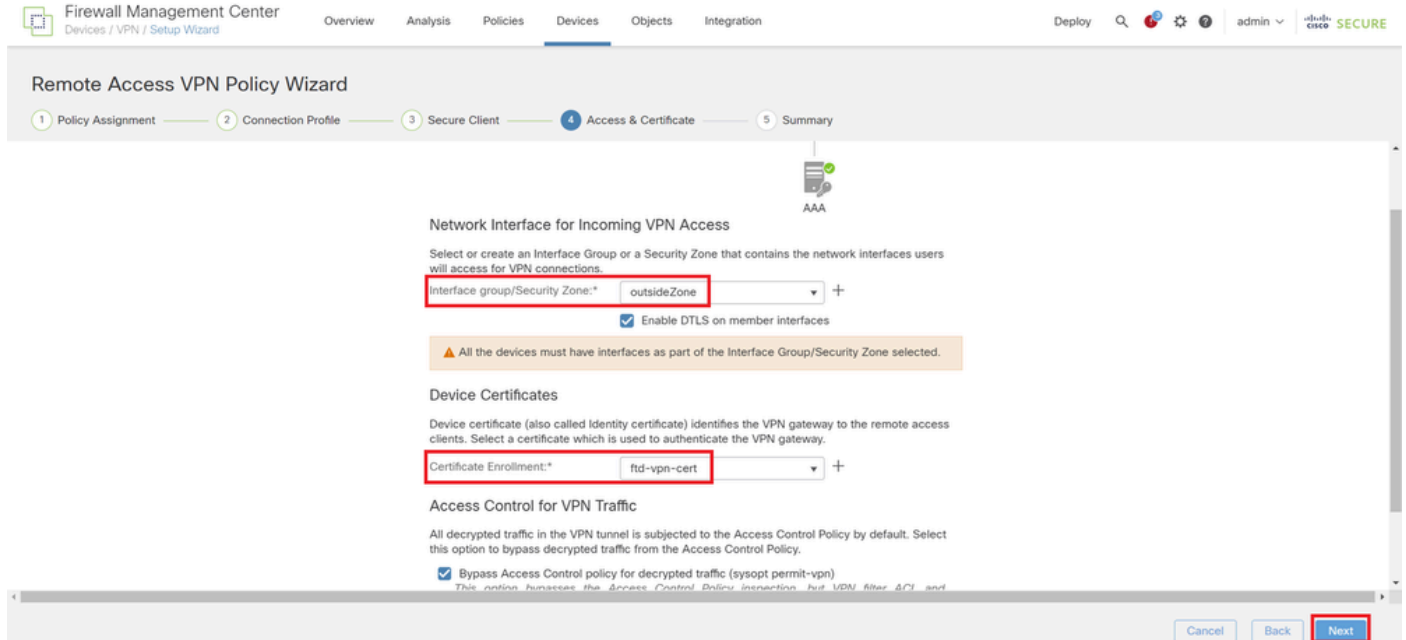
Cancel Back **Next**

نم لىصافت دح

سندهم لاصتا فيرعت فلمل ةداهشلاو لوصول نيوكت 9. ةوطخل

يلال رزلا قوف رقنا، ةداهشلا ليجست رصانعو نامألا ةقطنم/ةهجاولا ةعومجم ل ةميق دح

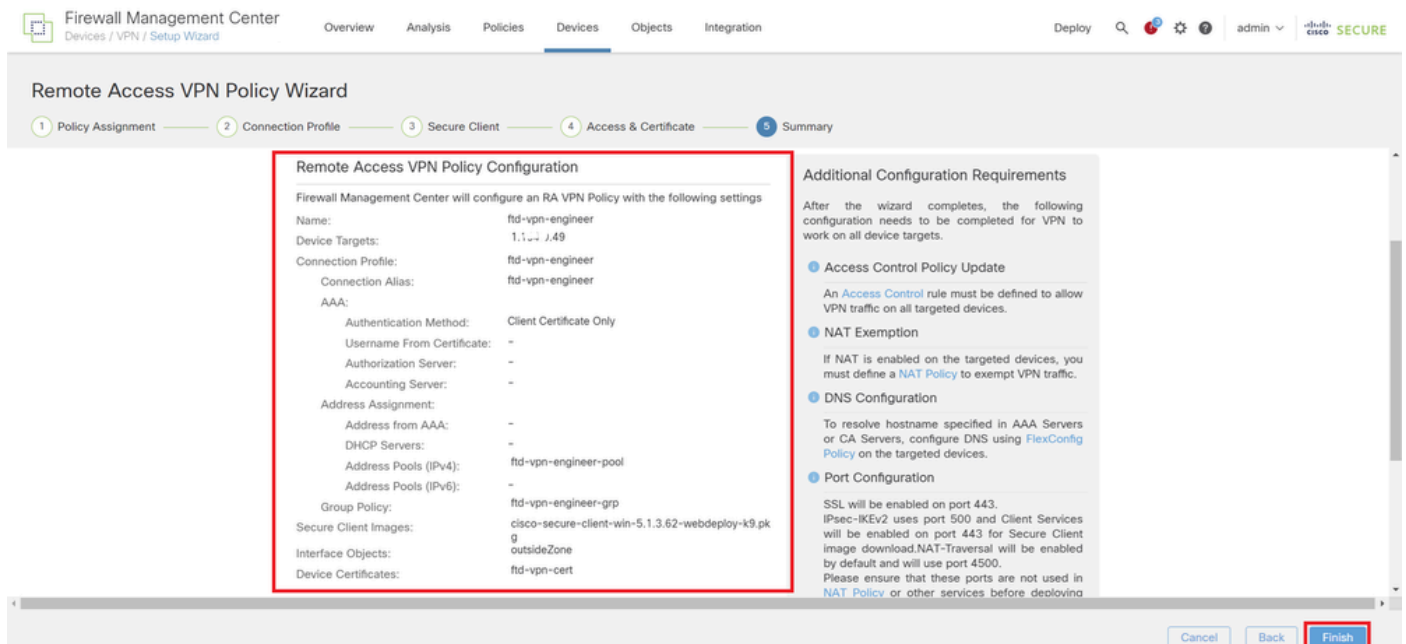
- ةقطنم ل جراخ: نامألا ةقطنم/ةهجاولا ةعومجم
- ةداهشلا ليجست: ftd-vpn-cert



ةداهشلاو لوصول لياصافت

سندهم لاصتا فيرعت فلمل صخلمل ديكأت 10. ةوطخل

ءاهن رز قوف رقناو دعب نع لوصول VPN جهنل اهلاخدإ مت يتلا تامولعمل نم دكأت



دعب نع لوصول VPN جهن لياصافت

VPN Manager ليعمل لاصتال فيرعت فلمل ةفاضل 11. ةوطخل

رز + قوف رونا، لاصتال فيرعت فلم > دعب نع لوصول > VPN > ةزهجالا لىل لقتنا

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices' (highlighted with a red box), 'Objects', and 'Integration'. The main content area is titled 'ftd-vpn-engineer' and has tabs for 'Connection Profile', 'Access Interfaces', and 'Advanced'. A table lists the configuration details for the VPN connection profile.

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
ftd-vpn-engineer	Authentication: Client Certificate Only Authorization: None Accounting: None	ftd-vpn-engineer-grp

لعمل لاصتال فيرعت فلم ةفاضل VPN Manager

ظفح رز لىل روناو لاصتال فيرعت فلم ل ةرورضال تامولعمل لخدأ

- مرسال: ftd-vpn-manager
- ةومحمل جهن: ftd-vpn-manager-grp
- نىوانع اعمجت IPv4: ftd-vpn-manager-pool

Add Connection Profile



Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

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 لي عمل لاصتاللا في رعت فلم لي صرافت

ة فاضم ة دي دج لي صوت تاف صوت دي كأت

Firewall Management Center
Devices / VPN / Edit Connection Profile

Overview Analysis Policies **Devices** Objects Integration

Deploy admin **SECURE**

ftd-vpn-engineer You have unsaved changes

Enter Description [Policy Assignments \(1\)](#)

Local Realm: None Dynamic Access Policy: None

Connection Profile | Access Interfaces | Advanced

Name	AAA	Group Policy	
DefaultWEBVPGGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy	<input type="button" value="Delete"/>
ftd-vpn-engineer	Authentication: Client Certificate Only Authorization: None Accounting: None	ftd-vpn-engineer-grp	<input type="button" value="Delete"/>
ftd-vpn-manager	Authentication: Client Certificate Only Authorization: None Accounting: None	ftd-vpn-manager-grp	<input type="button" value="Delete"/>

ة فاضم ل لاصتاللا تاف صوت دي كأت

تاداهش ةطيخ ةفاضل 12. ةوطخل

ةفاضل ةطيخ رز قوف رقا ،ةداهشل ةطيخ > VPN > نئال ةرادل > تانئال لىل لقتن ةداهشل.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ ⚠️ admin | Cisco Secure

PKI
Policy List
Port
Prefix List
Route Map
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable Set
VLAN Tag
VPN
Certificate Map
Custom Attribute

Certificate Map

Add Certificate 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 rules contained in the certificate map, the connection is associated with the specified connection profile.

Name	Value
No records to display	

تاداهش ةطيخ ةفاضل

رز قوف رقا و VPN Engineer لىمعب ةصاخلا تاداهشل ةطيخل ةرورضل تامولعمل لخدأ ظفح.

- ةطيخل سدنه م - رىبخ :ةطيخل مسا
- نىيىتلا ةدعاق : CN (عئاشل م سال) vpnEngineerClientCN

Add Certificate Map



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...		

Cancel

Save

سندنهمل ليمعمل تاداهش لة طيرخ

ظفح رز قوف رقن او Manager VPN ليمعمل ةداهش لة طيرخ لة رورض لة تامول عمل لخدأ

- ةطيرخ لة مس ا : cert-map-manager
- نيةت لة ةدعاق : CN (عئاش لة مسال) : vpnManagerClientCN

Add Certificate Map



Map Name*:

cert-map-manager

Mapping Rule

Configure the certificate matching rule

Add Rule

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

Cancel

Save

Manager ليمعمل عداهشال نييعت

ةديجال ةفاضل تاداهشال تاطخم ديكأت.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy admin **SECURE**

Certificate Map

Add Certificate 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 rules contained in the certificate map, the connection is associated with the specified connection profile.

Name	Value		
cert-map-engineer	1 Criteria		
cert-map-manager	1 Criteria		

ةديج تاداهش طئارخ

لاصتالا فيرعت فلمب ةداهشال طاطخم طبر. 13 ةوطخال

> م دقتم الى لقتنا، مث. FTD-VPN-engineer رحو، دعب نع لوصولو > VPN > ةزهجال الى لقتنا
طيطخت ةفاضل رزقنا، صيخرتال طئارخ

Firewall Management Center
Devices / VPN / Edit Advanced

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin | Cisco SECURE

ftd-vpn-engineer You have unsaved changes Save Cancel

Enter Description Policy Assignments (1)
Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces **Advanced**

Secure Client Images
Secure Client Customization
GUI Text and Messages
Icons and Images
Scripts
Binaries
Custom Installer Transforms
Localized Installer Transforms
Address Assignment Policy
Certificate Maps
Group Policies

General Settings for Connection Profile Mapping
The device processes the policies in the order listed below until it finds a match

Use group URL if group URL and Certificate Map match different Connection Profiles
 Use the configured rules to match a certificate to a Connection Profile

Certificate to Connection Profile Mapping
Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are matched. If none of the Certificate Map is matched, default connection profile will be chosen.

Please provide at least one Certificate Mapping. Add Mapping

Certificate Map	Connection Profile
No Records Found	

ةداهشلا ةطيخ طبر

س.ندنهملل VPN ليمعمل لاصتالا فيرعت فلمب ةداهشلا ةطيخ طبر

- ةداهشلا ةطيخ مسا : cert-map-engineer
- Connection Profile: ftd-vpn-engineer

Add Connection Profile to Certificate Map ?

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

Certificate Map Name*:
cert-map-engineer

Connection Profile*:
ftd-vpn-engineer

Cancel OK

Engineer VPN ليمعمل ةداهشلا ةطيخ طبر

ريدملاب صاخلا VPN ليمعمل لاصتالا فيرعت فلمب ةداهشلا ةطيخ طبر

- ةداهشلا ةطيخ مسا : cert-map-manager
- لاصتالا فيرعت فلم : ftd-vpn-manager

Add Connection Profile to Certificate Map



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

Certificate Map Name*:
cert-map-manager

+

Connection Profile*:
ftd-vpn-manager

Cancel OK

طبر VPN Manager ليعمل عداهشال عطيخ طبر

ةداهشال طبر دادع ديكات

Firewall Management Center
Devices / VPN / Edit Advanced

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Help admin | Cisco SECURE

ftd-vpn-engineer

Enter Description

You have unsaved changes Save Cancel

Policy Assignments (1)

Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

Secure Client Images
Secure Client Customization
GUI Text and Messages
Icons and Images
Scripts
Binaries
Custom Installer Transforms
Localized Installer Transforms
Address Assignment Policy
Certificate Maps
Group Policies

General Settings for Connection Profile Mapping
The device processes the policies in the order listed below until it finds a match

Use group URL if group URL and Certificate Map match different Connection Profiles
 Use the configured rules to match a certificate to a Connection Profile

Certificate to Connection Profile Mapping
Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are matched. If none of the Certificate Map is matched, default connection profile will be chosen.

Certificate Map	Connection Profile	
cert-map-engineer	ftd-vpn-engineer	
cert-map-manager	ftd-vpn-manager	

Add Mapping

ةداهشال طبر ديكات

FTD بةصاخال (CLI) رماوالا رطس ةهجاوي ف ديكاتال

FMC نم رشنال دع ب FTD CLI ف VPN لاصتا تادادع ديكات

```
// 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

```

VPN كابت ليمع في دي كأت

ليمعال ةداهش دي كأت 1. ةوطخال

تاداهش > يصخش > لياج مدختسم - تاداهش لى لى لقتنا، ةيس دنه لى VPN كابت ليمع في ةق قحت ةقداصم لى لى مدختسم لى لى ةداهش نم ققحت



ليمعال ةداهش لى لى Engineer VPN كأت

ليمعال ةداهش قوف اچودزم ارقن رقنا لى لى ققحت نم ققحت م، Details لى لى لقتنا م، لى لى ةداهش قوف اچودزم ارقن رقنا لى لى ققحت نم ققحت م.

- ةوضومال: CN = vpnEngineerClientCN



تلي م ل ع ا ه ش ل ل ا د ي ك أ ت VPN Manager

ل ي ص ا ف ت ن م ق ق ح ت م ث . Details ل ل ل ق ت ن ا م ث ، ل ي م ل ع ا ه ش ق و ف ا ج و د ز م ا ر ق ن ر ق ن ا ع و و م ل ا .

- ع و و م ل ا : CN = vpnManagerClientCN

Certificate



General Details Certification Path

Show: <All>

Field	Value
Issued	Thursday, June 19, 2025 9:41...
Subject	vpnManagerClientCN, vpnMan...
Public Key	RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Comment	xca certificate
Thumbprint algorithm	sha1

CN = vpnManagerClientCN

O = Cisco
L = Tokyo
S = Tokyo
C = JP

Edit Properties...

Copy to File...

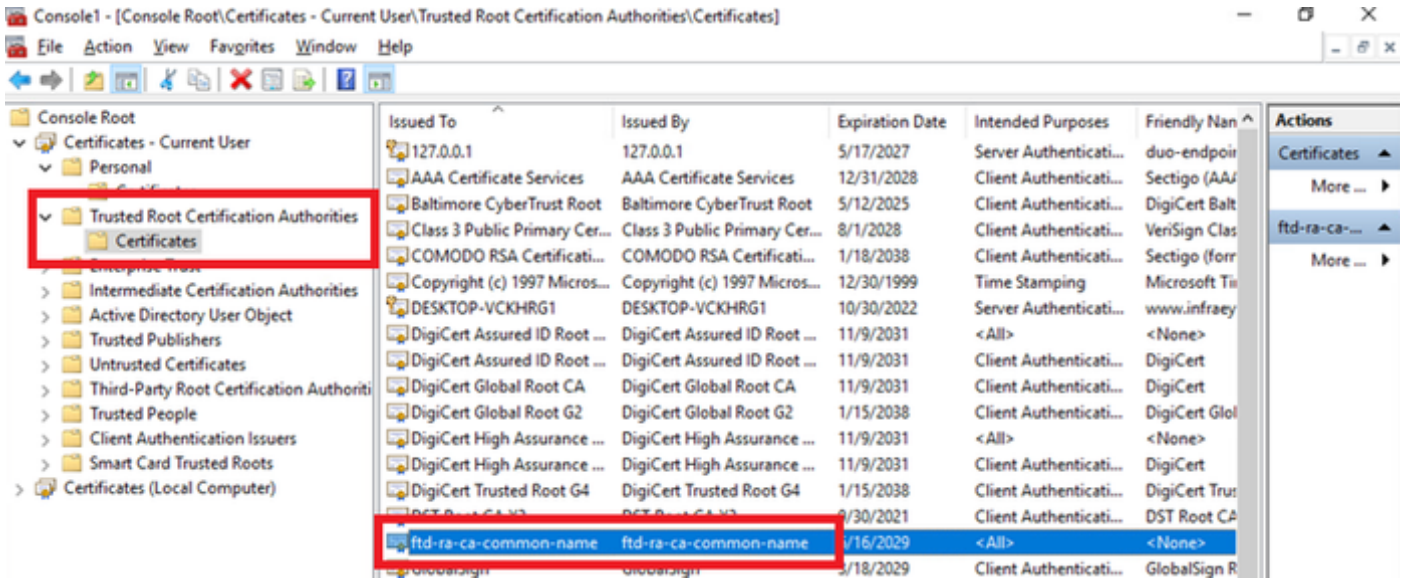
OK

رېدمال لېم مع ٻڌاش لېصافت

CA ډيڪاټ 2. ٻوطلالا

- تاداهشلا إلى لقتنا ،ريدملل VPN ةكبش ليمع و سندنهملل VPN ةكبش ليمع نم لك يف
عجرملا نم ققحت ،تاداهشلا > اهيف قوئوملا روجللا قي دصتلا عجارم > يلاجل مدختسملا
ةقداصملا مدختسملا قداصملا

- نرداص : ftd-ra-ca-common-name

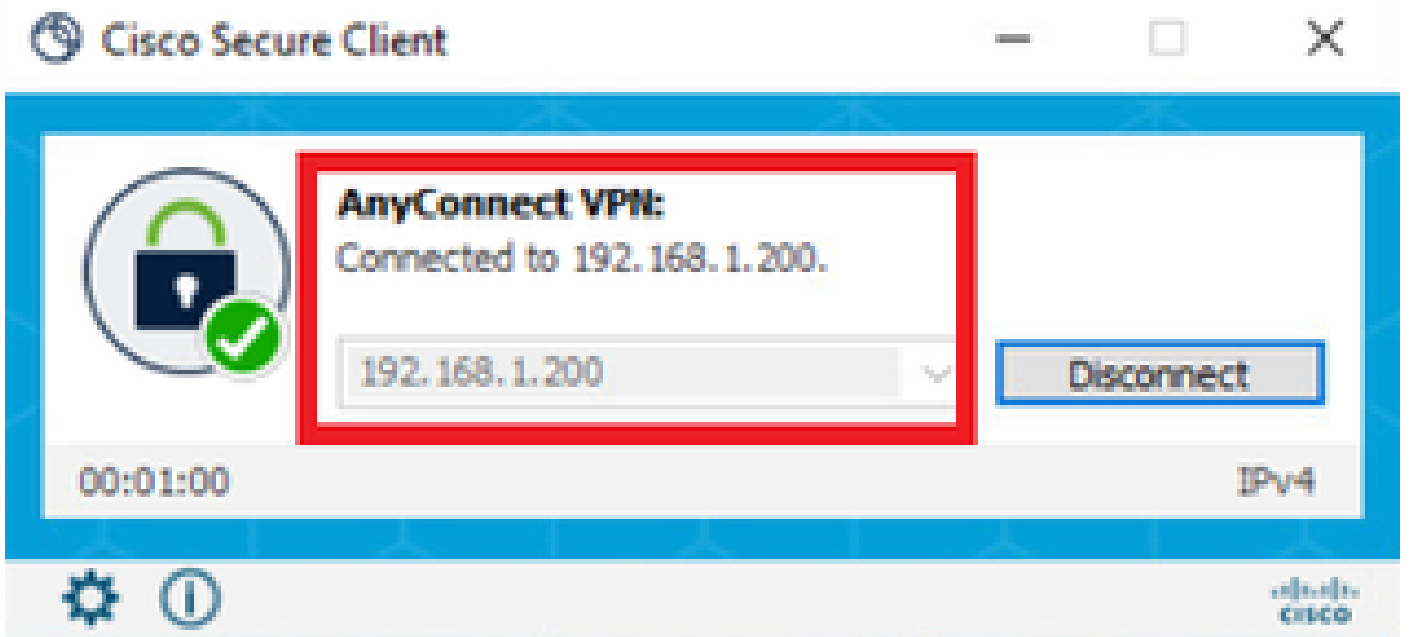


CA ديكتات

ةحصللا نم ققحتلا

VPN لاصتا ادب 1. ةوطخل

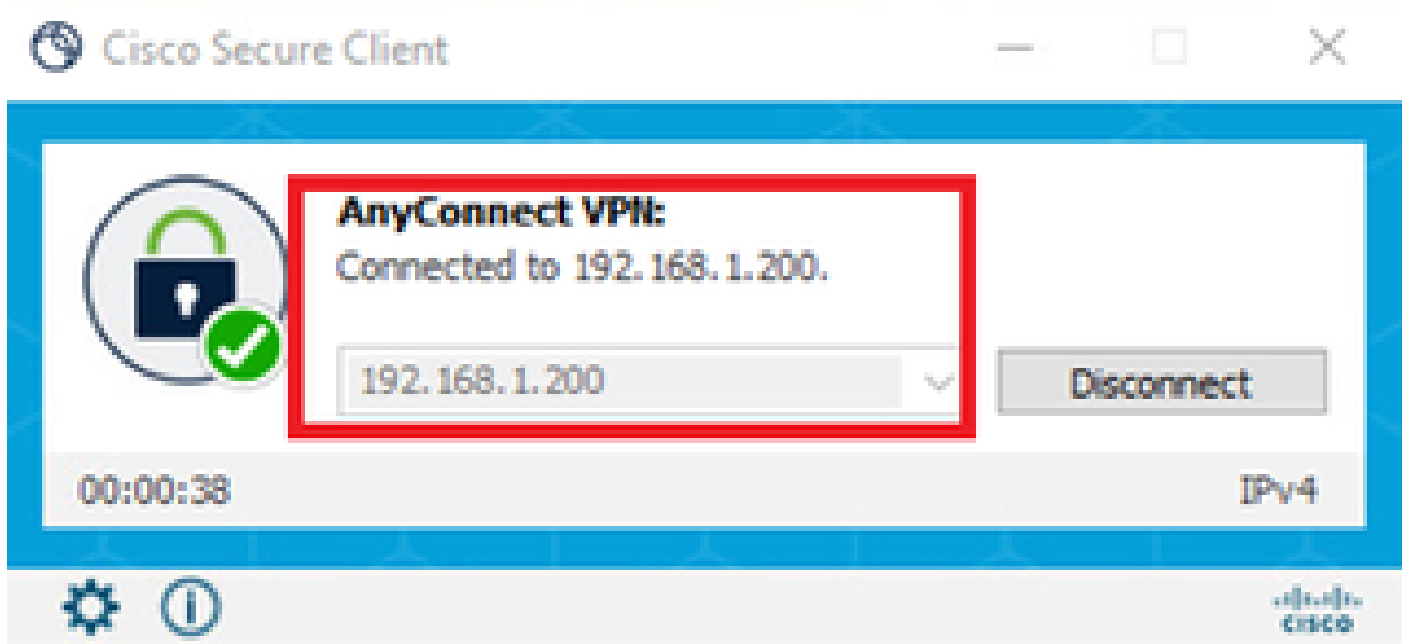
ام Cisco نم نم آلا ليمعلا لاصتا ادبا ،سندنهملل (VPN) ةيرهظلا ةصاخلا ةكبشلا ليمع يف
حاجنب طبري VPN ل ،ةملاك و username ل لخدي نأ ةجاج نم



سندنهملا ليمع نم VPN لاصتا ادب

ةملاك و username ل لخدي نأ ةجاج نم ام Cisco Secure Client لاصتا ادبا ، In Manager VPN ليمع

حاجن ب طبري VPN ل



قرا دل ليمع نم VPN لاصتا ادب

FMC يف عطشننلا تاسلجل ديكتأت 2. ةوطخل

لمعل تاسلجل (Active Session) > Users (نوم دختسم ل) > Analysis (ل لحتل) ل لقتنا
VPN. ةقداصل مل عطشننلا ةسلجل نم ققحت، (ةطشننلا)

The screenshot shows the Firewall Management Center (FMC) interface. The top navigation bar includes "Overview", "Analysis", "Policies", "Devices", "Objects", and "Integration". The "Analysis" tab is selected. The main content area shows a table of active sessions. The table has columns for "Login Time", "Realm/Username", "Last Seen", "Authentication Type", "Current IP", "Realm", "Username", "First Name", and "Last Name". Two sessions are listed, both with "VPN Authentication" type. The "Current IP" and "Username" columns for both sessions are highlighted with red boxes.

Login Time	Realm/Username	Last Seen	Authentication Type	Current IP	Realm	Username	First Name	Last Name
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 11:00:35	Discovered Identities/vpnEngineerClientCN	2024-06-19 11:00:35	VPN Authentication	172.16.1.101	Discovered Identities	vpnEngineerClientCN		

ةطشننلا لمعل ةسلجل ديكتأت

FTD CLI يف VPN لمعل تاسلجل ديكتأت 3. ةوطخل

ريدم و سدنهم نم ةسلجل VPN ل دكؤي نأ CLI (Lina) FTD يف رمأ show vpn-sessiondb detail anyconnect ل غش

```
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
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

ههالصلوا عاطخألا فاشكتسا

رتويبمك زاهج ىلع DART فلم يف و Lina كرحم ل Debug syslog يف VPN ةقداصم لوح تامولعم ىلع روثعل عقوت كنكمري Windows.

سدنهم ل ليمع نم VPN لاصلتا اناثأ كرحم ل Lina يف عاطخألا حيحصت تالجس ىلع لاثم اذه

<#root>

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

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=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.

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

ريدم ل ليمع نم VPN لاصلتا اناثأ كرحم ل Lina يف عاطخألا حيحصت تالجس ىلع لاثم اذه

<#root>

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

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=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.

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

ةلص تاذا تامولعم

[للقننللا عانثأ لوص ولل AnyConnect ةداهش للا ةدننلس للا ةقداص مللا نيوكت](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل