

لیمعل ا ئقداصمل CERT نیييعت نیوکت رمع ئلیع ئنماـلا FMC

تاي وتحملـا

قـمـدـقـمـلـا

قـيـسـاسـأـلـاـ تـابـلـطـتـمـلـا

تابـلـطـتـمـلـا

قـمـدـخـتـسـمـلـاـتـانـوـكـمـلـا

قـيـسـاسـأـتـامـوـلـعـمـ

قـكـبـشـلـلـيـطـيـطـخـتـلـاـ مـسـرـلـا

تـانـيـوـكـتـلـا

قـيـفـنـيـوـكـتـلـاـ FMC

قـهـجـاوـنـيـوـكـتـلـاـ FTD

قـصـيـخـرـتـ دـيـكـأـنـ Cisco Secure Client

قـنـيـوـانـعـعـمـجـتـ فـفـاضـأـنـ IPv4

قـعـوـمـجـمـلـاـجـهـنـ فـفـاضـأـنـ 4. قـوـطـخـلـا

قـدـاهـشـ فـفـاضـأـنـ 5. قـوـطـخـلـا

سـدـنـهـمـلـاـلـاـصـتـاـ فـيـرـعـتـ فـلـمـلـجـهـنـ نـيـيـعـتـ فـفـاضـأـنـ 6. قـوـطـخـلـا

سـدـنـهـمـلـاـلـاـصـتـاـ فـيـرـعـتـ فـلـمـلـ لـيـصـافـتـ نـيـوـكـتـ 7. قـوـطـخـلـا

سـدـنـهـمـلـاـلـاـصـتـاـ فـيـرـعـتـ فـلـمـلـ قـبـمـآـلـيـعـ قـرـوـصـ نـيـوـكـتـ 8. قـوـطـخـلـا

سـدـنـهـمـلـاـلـاـصـتـاـ فـيـرـعـتـ فـلـمـلـ قـدـاهـشـلـاـلـاـلـوـصـلـاـنـيـوـكـتـ 9. قـوـطـخـلـا

سـدـنـهـمـلـاـلـاـصـتـاـ فـيـرـعـتـ فـلـمـلـ صـخـلـمـلـاـ دـيـكـأـنـ 10. قـوـطـخـلـا

لـيـمـعـلـلـاـلـاـصـتـاـ فـيـرـعـتـ فـلـمـلـ فـاضـأـنـ 11. قـوـطـخـلـا

تـادـاهـشـ قـطـيـخـ فـفـاضـأـنـ 12. قـوـطـخـلـا

لـاـصـتـاـلـاـ فـيـرـعـتـ فـلـمـبـ قـدـاهـشـلـاـلـاـطـطـخـمـ طـبـرـ 13. قـوـطـخـلـا

قـبـ قـصـاخـلـاـ (CLI) رـمـاـلـاـرـطـسـ قـهـجـاوـيـفـ دـيـكـأـنـلـاـ FTD

قـكـبـشـ لـيـمـعـيـفـ دـيـكـأـنـ VPN

لـيـمـعـلـاـ قـدـاهـشـ دـيـكـأـنـ 1. قـوـطـخـلـا

دـيـكـأـنـ 2. قـوـطـخـلـا CA

قـحـصـلـاـتـمـ قـقـحـتـلـا

لـاـصـتـاـعـدـ 1. قـوـطـخـلـا VPN

قـيـفـ قـطـشـنـلـاـنـاسـلـجـلـاـ دـيـكـأـنـ 2. قـوـطـخـلـا FMC

قـيـفـ قـمـعـتـاسـلـجـ دـيـكـأـنـ 3. قـوـطـخـلـا VPN FTD CLI

اهـحـالـصـ اوـعـاطـخـأـلـاـ فـاشـكـتـسـا

قـلـصـ تـاذـتـامـوـلـعـمـ

قـمـدـقـمـلـا

مـاـدـخـتـسـابـ FTD ئـلـعـ SSLـعـ Cisco Secure Clientـمـ دـنـتـسـمـلـاـ اـذـهـ حـضـوـيـ

قـيـسـاسـأـلـاـ تـابـلـطـتـمـلـا

تابل طتملا

ةيلاتلا عيضاوملا بفرعم كيدل نوكت نأب Cisco يصوت:

- Cisco FireSIGHT (FMC) نم ةرادا زكرم
- يرهاظلا (FTD) ةيامحلا رادج ديدهت دض عافدلا
- VPN ةقداصم قفدت

ةمدختسملا تانوكمل

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

ةصالخ ةيلمعم ةئيب يف ةدوچوملا ۆزهچألا نم دنتسملا اذه يف ةدواولا تامولعملاءاشنإ مت
تناك اذا .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ۆزهچألا عيجمج تأدب
رمأ يأ لمحتملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةيساسأ تامولعم

ىلع ليمع ةداهش نيعت متي ثيح VPN تالاصتا يف مدختست ۆقيرطي ە ةداهشلا طيطخت
ةيلمع ەذه.لىوختلا ضارغأ ەداهشلا لخاد تامسلا مادختسا متى وأ ،يلحم مادختسم باسح
نيعت مادختساب .زاهج وأ مادختسم فيرعتل ۆليسوک ۆيمقرلا ەداهشلا مادختسا اهييف متى
تانايب لاخدا ىلا ۆجاحللا نود نيمدختسملا ۆقادصم SSL لوكوتورب لغتسى ھنإف ،ةداهشلا
دامتعالا.

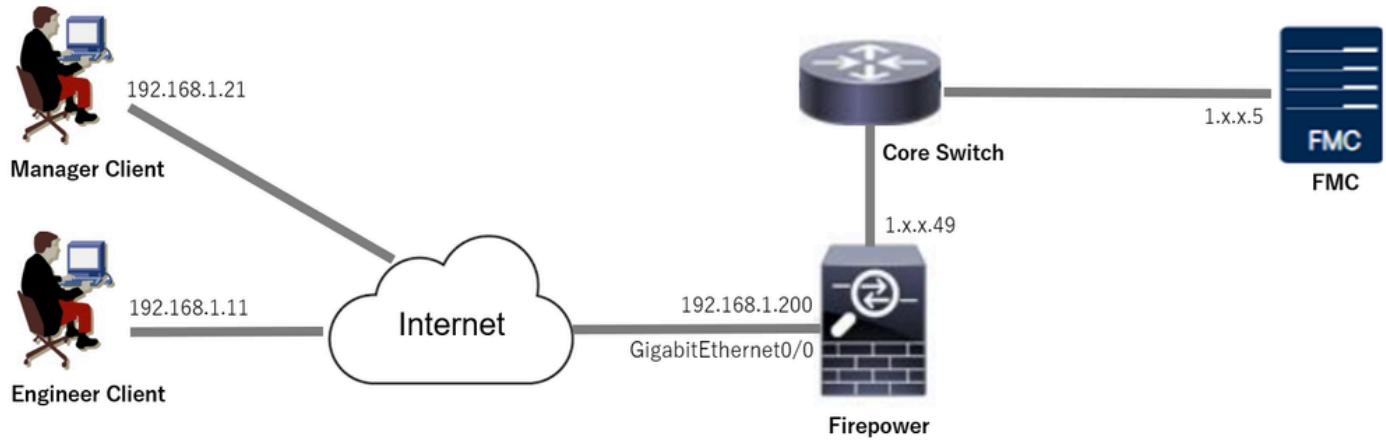
ةداهش نم عئاشلا مسالا مادختساب نمآل Cisco ليمع ۆقادصم ةيفيك دنتسملا اذه حضوي
SSL.

لىوختلا ضارغأ ھمادختسا متى ،اھلخادب كرتشم مسا ىلع تاداهشلا ھذه يوتحت.

- ftd-ra-ca-name : ەراشلا
- vpnEngineerClientCN : سدنھملل VPN ۆكبش ليمع ەداهش
- vpnManagerClientCN : ەداهش ليمع Manager VPN
- 192.168.1.200 : مداخلا ەداهش

ةكبشلل یطيطختلا مسربلا

دنتسملا اذه لاثمل ھمادختسا متى يذلا ططخملا ۆروصلما ھذه ضرعى.



ةكبشلل يطي طختلا مس رلا

تاني وكتلا

يف نيوكتلا FMC

ةهج او نيوكت 1. وةوطخل

ل ئيجراخلا ئهجاولى نيوكتب مقو، فدهلـا FTD زاهج ررحـو، ئزهـجـأـلـا ئـرـادـا > ئـزـهـجـأـلـا ئـلـا لـقـتـنـا inInterfacestab.

لـ GigabitEthernet0/0،

- جراخ: مسالا
- ئقطنمـلـا جـراـخـ: ئـيـنـمـأـلـا ئـقـطـنـمـلـا
- IP: 192.168.1.200/24 نـاـونـعـ

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

او جـهـجـلـا FTD

صـيـخـرـتـ دـيـكـأـتـ 2. وةوطـخـلـا Cisco Secure Client

صـيـخـرـتـ نـمـ دـكـأـتـ وـ، فـدـهـلـا FTD زـاهـجـ رـرحـوـ، ئـزـهـجــأـلـا ئـرـادـا > ئـزـهـجــأـلـا ئـلـا لـقـتـنـا Cisco Secure Client DeviceTab يـفـ.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices' (which is underlined), 'Objects', and 'Integration'. On the right, there are 'Deploy' and search icons, along with user information 'admin' and the Cisco logo.

The main content area has two tabs: 'Device' (selected) and 'Routing'. Below these are sections for 'General', 'Inspection Engine', and 'Logs'. The 'General' section contains fields for 'Name', 'Transfer Packets', 'Troubleshoot', 'Mode', 'Compliance Mode', 'Performance Profile', 'TLS Crypto Acceleration', 'Device Configuration', and 'OnBoarding Method'. Buttons for 'Import', 'Export', and 'Download' are also present.

A modal window titled 'License' is open, showing 'License Types' and a dropdown for 'Performance Tier' set to 'FTDv5 - 100 Mbps'. Under 'Essentials', 'Export-Controlled Features', and 'IPS' checkboxes are checked. Under 'Carrier', 'URL', and 'Secure Client Premier' (which is highlighted with a red box), checkboxes are unchecked. Under 'Secure Client Advantage', the checkbox is checked. A note at the bottom states: 'If a device already has Secure Client VPN Only they cannot have Secure Client Premier or Secure Client Advantage. If a device has Secure Client Premier or Secure Client Advantage it cannot have Secure Client VPN Only.'

The right side of the screen shows a summary of the device configuration, including the device name 'Cisco Firepower Threat Defense for VMware 9A33F35ANSU', its last update time '2024-06-14 07:38:47', and its zone 'UTC (UTC+0:00)'. It also lists 'Zone setting for based Rules' and their respective times.

نەمآلە لىيەمۇلە صېخىرت

3. ةوطخلا نيوانع عمجمت ةفاضا IPv4

مزمحة قافلاً رزلاً قوف رقناً، IPv4 تابع مجت **>** نیوانعلماً تابع مجت **>** نیاکلاً ڦارداً **>** Object یلإ لقتنا IPv4.

The screenshot shows the Firewall Management Center interface. The left sidebar has a tree view with 'Address Pools' expanded, showing 'IPv4 Pools' selected. The main content area is titled 'IPv4 Pools' and contains a table with one column: 'Name'. A message below the table says 'No records to display'. At the top, there are tabs for Overview, Analysis, Policies, Devices, Objects (which is highlighted with a red box), and Integration. To the right of the tabs are buttons for Deploy, a search icon, and settings. The top right corner shows the user 'admin' and a 'Cisco SECURE' badge.

Name	Value	Override

IPv4 فاصله عجمت وانی

سدن 5 مل ل VPN لیمعل IPv4 نیوانع عمجمت عاشن ایل ۆیرورض للا تامولعملالاخداپ مق

- مس الـ ftd-vpn-engineer-pool
 - ناونع قاطن IPv4: 172.16.1.100-172.16.1.110
 - عانقـاـ 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

● 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

سدنەمەل لیمعل VPN نیوانع عمجت

ریدملاب صاخلا لیمعل VPN نیوانع عمجت ئاشنال ئيوررضلا تامولعملالا لخدا.

- مسالا: ftd-vpn-manager-pool
- IPv4: 172.16.1.120-172.16.1.130
- عانقلالا: 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

● 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

ریدمبل VPN لیمعل نیوانع مجت

ڈی Jal IPv4 نیوانع تاعمجت دی کات

The screenshot shows the Firewall Management Center interface with the 'Objects' tab selected. On the left, a sidebar lists various objects like AAA Server, Access List, Address Pools, and IPv4 Pools. The 'IPv4 Pools' section is currently active. The main area displays a table of IPv4 pools. The first pool, 'ftd-vpn-engineer-pool', has its 'Value' row highlighted with a red box. The second pool, 'ftd-vpn-manager-pool', also has its 'Value' row highlighted with a red box. Both rows contain the IP range '172.16.1.100-172.16.1.110' and '172.16.1.120-172.16.1.130' respectively. The table includes columns for Name, Value, and Override.

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"/>

ڈی Jal IPv4 نیوانع تاعومجم

4. ڈو طخلا ڈی جہن ڈفاضا

ڈی وو مجملا جھن ڈفاضا رز قوف رقنا، ڈی وو مجملا جھن > نئا کل اورادی > VPN > Object لیا لقتنا.

Firewall Management Center

Overview Analysis Policies Devices Objects Integration

Add Group Policy

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

ساعده مل جهن فاصا

لدي معلم عوامجي مل جهن ايشن إل ئيرورضلا تامولعمل لاخداب مق

- مسالا: ftd-vpn-engineer-grp
- تالوكوتورب VPN: SSL

Add Group Policy

Name:

Description:

General Secure Client Advanced

VPN Protocols

IP Address Pools

Banner SSL

DNS/WINS IPsec-IKEv2

Split Tunneling

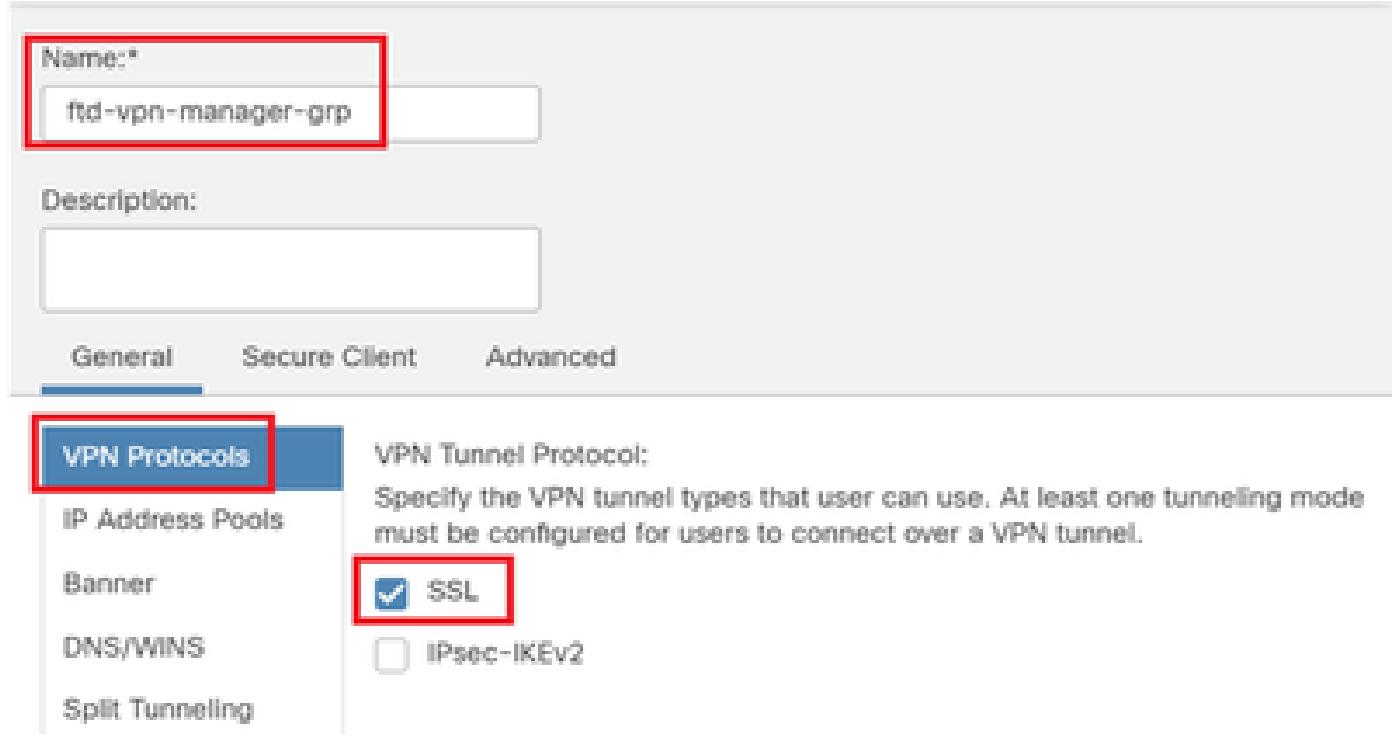
VPN Tunnel Protocol:
Specify the VPN tunnel types that user can use. At least one tunnelling mode must be configured for users to connect over a VPN tunnel.

سدنهم لـ VPN ليمعل عوامجي مل جهن

ريدملاپ صاخلا VPN ليمعل عوامجي مل جهن ايشن إل ئيرورضلا تامولعمل لخدا.

- مسالا: ftd-vpn-manager-grp
- تالوكوتورب VPN: SSL

Add Group Policy



لیمعل ةعومجملا جن Manager VPN

ةـدـيـدـجـلـاـةـعـوـمـجـمـلـاـجـهـنـدـيـكـأـتـ.

ڏيڍو ڦومجم ج٥٥

٥. وظخا فاضا داهش ة

لیجسٽ ڦفاضا رزلما ڦوپ رقنا ،عاطتق والا لیجسٽ > PKI > نئاکلا ڦرادا > Object ىلما لقتنا عاطتق والا.

Firewall Management Center

Overview Analysis Policies Devices Objects Integration

Add Cert Enrollment

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

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		

ةداهش لـ FTD او FDS او PKCS12 فـمل داريتس او لـاخـداـب مـقـ.

- مـسـالـاـ: ftd-vpn-cert
- فـمل PKCS12 لـيجـسـتـلـاـ عـونـ

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

ةداهشل لايچس ت

دي دجل ا ةداهشل لايچس ت ديكأ.

The screenshot shows the 'Cert Enrollment' page in the Firewall Management Center. On the left, there's a sidebar with various object management options like Cipher Suite List, Community List, DHCP IPv6 Pool, etc. The main area has a table with one row. The first column is 'Name' with the value 'ftd-vpn-cert' highlighted with a red box. The second column is 'Type' with the value 'PKCS12 File' also highlighted with a red box. At the top right, there's a 'Add Cert Enrollment' button and a search bar.

دي دج ةداهش لايچس ت

ةفاصن رز قوف رقنا ، تاداهشل > ةزهجأ لىا لقتنا.

The screenshot shows the 'Devices' page in the Firewall Management Center. The 'Devices' tab is selected. There's a 'Filter' dropdown set to 'All Certificates'. A large red box highlights the 'Add' button at the top right. Below it is a table with columns: Name, Domain, Enrollment Type, Identity Certificate Expiry, CA Certificate Expiry, and Status. The table currently displays 'No certificates'.

ةداهش ةفاصن FTD

ب ةدجل ا ةداهشل لايچس ت طبرل ئي رورضل ا تامولعمل ا لخدا.

- زاهجلا 1.x.x.49
- ةداهشل لايچس ت: FTD-VPN-CERT

Add New Certificate



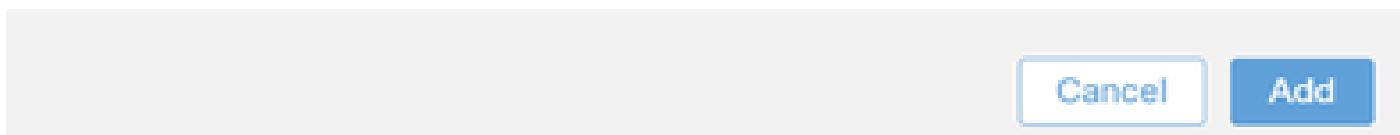
Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

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



ب ةداهشلما طبر

ةداهشلما طبر ٖ لاح ديكأت.

Firewall Management Center						Deploy	Q	⟳	✖	admin	SECURE
Devices / Certificates						Overview	Analysis	Policies	Devices	Objects	Integration
Filter						All Certificates					
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							

ةداهشلما طبر ٖ لاح

سدنهملا لاصتا فيرعت فلمل جهن نيعي ةفاضا 6. ٖ ووطخلا

قفوف رقنا ، دعب نع لوصولما > VPN > زهجألا ىلإ لقتنا AddButton.

Firewall Management Center						Deploy	Q	⟳	✖	admin	SECURE
Devices / VPN / Remote Access						Overview	Analysis	Policies	Devices	Objects	Integration
						Add					
Name	Status	Last Modified	No configuration available Add a new configuration								

دعب نع لوصولل VPN ةكبش ةفاضا

قفوف رقنا او ةيرورضلما تامولعملاب مدق Nextbutton.

- مسالا: ftd-vpn-engineer
- تالوكوتورب VPN: SSL
- ةفدهتس ملا ةزهجأا 1.x.49

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies Devices Objects Integration Deploy 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: *

Description:

VPN Protocols:

SSL IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
Search 1.1.1.49	Selected Devices 1.1.1.49

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

جنهنلا نيعي

سدنهملالا لاصتا فيرعت فلم ليصافت نيوكت 7. ووطخل

قوف رقناو ةيرورضلاتامولعملالاخداب مق Nextbutton.

- طقف ليجعلها ةداهش: ئقاداصملابولسا
- نيعتيلل ددجم لقح: ةداهشلا نم مدخلتس ملا مسا
- عئاشلا مسالا CN: يساسالا لقحلا
- (ةيميظنتلا ةدحولا) OU: يوناثلا لقحلا
- IPv4: ftd-vpn-engineer-pool
- عومجملالا جن: 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:

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](#)

للاصت الـا في رعـت فـلم لـيـص اـفت

سدن هملا لاصتا فيرعت فلمل ٰنما ليمع ٰروص نيوكت ٠٨ ووطخلا

قف رقناو نم آلیم ع ۃروص فلم ددح Nextbutton.

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 +

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-webdeplo...	Windows ▾

Next

نـمـآـلـيـمـعـ دـيـدـحـتـ

سدنهملا لاصتا فيرعت فلملل ةداهشل ولوصلولا نيوكت 9 ةوطخل

يـلـاتـلـا رـزـلـا قـوـفـ رـقـنـا ، ةـدـاهـشـلـا لـيـجـسـتـ رـصـانـعـ وـنـامـأـلـا ةـقـطـنـمـ / ةـهـجـاـولـا ةـعـوـمـجـمـ لـ ةـمـيـقـ دـدـحـ

- قطنملاراخ ناماڭلا قطنم/ەجأولاقۇمچىم
 - ftd-vpn-cert: داداھشىلارىچىسىت

Remote Access VPN Policy Wizard

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

 AAA

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: +
 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: +

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 (syspt permit-vpn)
This option bypasses the Access Control Online inspection, but VPN filter ACP and

Next

ةداهشل او لوصول ا ليصافت

سدن همل لاصتا في رع فلمل صخل ملا دي كأ. 10. ووط خلا

عاهنإ رز قوف رقن او دعب نع لوص ولل VPN جهـنـل اـهـلـاخـدـا مـتـ يـتـلـا تـامـوـلـعـمـلـا نـمـ دـكـأـتـ

Firewall Management Center

Devices / VPN / Setup Wizard

Overview Analysis Policies Devices Objects Integration Deploy Q E S admin cisco SECURE

Remote Access VPN Policy Wizard

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

Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	ftd-vpn-engineer
Device Targets:	1.1.1.1 J.49
Connection Profile:	ftd-vpn-engineer
Connection Alias:	ftd-vpn-engineer
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	ftd-vpn-engineer-pool
Address Pools (IPv6):	-
Group Policy:	ftd-vpn-engineer-grp
Secure Client Images:	cisco-secure-client-win-5.1.3.62-webdeploy-k9.pk
Interface Objects:	g outsideZone
Device Certificates:	ftd-vpn-cert

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 Exemption**
If 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**
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 deploying.

دع ب نع لوص ولل VPN جهن ليص افت

Manager VPN لـ معمل لاصـتـالـا فـيـرـعـتـ فـلـمـ ةـفـاضـاـ 11. ةـوـطـخـلـا

رز + قوف رقنا ، لاصتالا فيرعت فلم > دعب نع لوصولا > ڦجهجألا ىلإ لقتنا.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices (which is highlighted with a red box), Objects, and Integration. On the far right, there are Deploy, Search, and Admin options. The main content area is titled 'ftd-vpn-engineer' and shows a table for 'Connection Profile'. The table has three columns: Name, AAA, and Group Policy. It lists two entries: 'DefaultWEBVPNGroup' and 'ftd-vpn-engineer'. The 'ftd-vpn-engineer' entry has 'Authentication: Client Certificate Only', 'Authorization: None', and 'Accounting: None'. The 'Group Policy' column shows 'DfltGrpPolicy' for the first entry and 'ftd-vpn-engineer-grp' for the second. At the bottom right of the table, there is a red box around a '+' button. Above the table, there are buttons for 'Save' and 'Cancel'.

لیمعل لاصتالا فيرعت فلم ظفاحا Manager VPN

ظفح رز ىلع رقنا او لاصتالا فيرعت فلممل ٿيرو رضلا تامولعمل ا لخدا.

- مسالا: ftd-vpn-manager
- ڦجهجملان: ftd-vpn-manager-grp
- IPv4 نیوانع تاعمجت: ftd-vpn-manager-pool

Add Connection Profile



Connection Profile:^{*} ftd-vpn-manager

Group Policy:^{*} ftd-vpn-manager-grp



[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	

[Cancel](#)

[Save](#)

لیمعل لاصتالا فیرعت فلم ليصافت Manager VPN

فاضم ةديج ليصوت تافيصوت ديكت.

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis Policies Devices Objects Integration Deploy admin 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
DefaultWEBVPNGroup	AAA	Group Policy
ftd-vpn-engineer	Authentication: Client Certificate Only Authorization: None Accounting: None	DfltGrpPolicy
ftd-vpn-manager	Authentication: Client Certificate Only Authorization: None Accounting: None	ftd-vpn-engineer-grp
		ftd-vpn-manager-grp

فاضمل ا ليصوتلا تافيصوت ديكت

تاداھش ۋە ئەنۋەرخ ئەفاضى 12. ۋە ئەنۋەرخ

ئەفاضى ۋە ئەنۋەرخ رز قوف رقنا، ئەدەشلى ئەنۋەرخ > نىڭلارا ئەنۋەرخ > تانئاكلى ئەنۋەرخ > تانئاكلى ئەنۋەرخ.

The screenshot shows the Cisco Firewall Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects (which is highlighted with a red box), and Integration. On the far right, there are Deploy, Search, Settings, and User admin options. The main content area is titled "Certificate Map". A sub-header explains that a Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile. It states that if a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile. Below this is a table with columns "Name" and "Value", which currently displays "No records to display". At the top right of the main content area is a blue "Add Certificate Map" button, also highlighted with a red box. The left sidebar lists various object types under the "Objects" category, with "Certificate Map" being the selected item, also highlighted with a red box. Other listed items include PKI, Policy List, Port, Prefix List, Route Map, Security Intelligence, Sinkhole, SLA Monitor, Time Range, Time Zone, Tunnel Zone, URL, Variable Set, VLAN Tag, and VPN.

تاداھش ۋە ئەنۋەرخ ئەفاضى

رز قوف رقناو VPN لىمۇب ئەنۋەرخ ئەنۋەشلى ئەنۋەرخ ئەنۋەشلى ئامولۇملا لىخدا ظفح.

- ئەنۋەرخ سىدىنەم - رېبىخ: ئەنۋەرخ مىسا
- يواسى (عىاشلى مىسالا) CN: vpnEngineerClientCN

Add Certificate Map



Map Name*:

cert-map-engineer

Mapping Rule

Configure the certificate matching rule

Add Rule

#	Field	Component	Operator	Value	edit	trash
1	Subject	CN (Common Name)	Equals	vpnEngineerCle...		

Cancel

Save

سدنەملا لىيەنلەنەشلىا ئەطىەخ

ظفح رز قوف رقناو Manager VPN لىيەنلەنەشلىا ئەطىەخ ئەرورضلا تامولۇملا لىخدا.

- ئەطىەخلا مسا: cert-map-manager
- يواسى (عئاشلىا مسالا) CN: نىيىعەتلىا ئەدعاق vpnManagerClientCN

Add Certificate Map

1

Map Name*:

Mapping Rule

Configure the certificate matching rule

Add Rule

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

لیمعل ڈاہش لانی یعنی Manager

دی دجله ڈاک اسٹیشن کا نام تاطخم دیکھتے۔

The screenshot shows the Firewall Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects (which is the active tab), and Integration. On the right, there are buttons for Deploy, a search icon, and user admin settings. A sidebar on the left lists categories like PKI, Policy List, Port, Prefix List, Route Map, Security Intelligence, Sinkhole, SLA Monitor, and Time Range. The main content area is titled "Certificate Map" and contains a description: "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." Below this is a table with two rows:

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

ةدیج تاداھش طیارخ

لاصتا فى رعد فلمب ڈاہشلا ططخم طبر 13 ڈو طخل

Firewall Management Center

Devices / VPN / Edit Advanced

Devices **Devices** Objects Integration Deploy admin cisco SECURE

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.

Please provide at least one Certificate Mapping.

Add Mapping

Certificate Map	Connection Profile
	No Records Found

ةداهشلا ةطيرخ طبر

سدنهم لـ VPN ليجعل لاصتالا فيرعت فلمب ةداهشلـ ةطيرخ طبر.

- ةداهشلـ ةطيرخ 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

ليجعل ةداهشلـ ةطيرخ طبر Engineer VPN

ريـ دـ مـ لـ اـ بـ صـ اـ خـ لـ اـ فـ يـ رـ عـ تـ فـ لـ مـ بـ ةـ دـاهـ شـ لـ ةـ طـ يـ رـ طـ بـ رـ.

- ةداهشلـ ةطيرخ مسا: cert-map-manager
- لاصتالـ ةيـ رـ عـ تـ فـ لـ مـ: 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

لیمعل ۋە داداشلار ئەطىرخ طېرى

ۋە داداشلار ئەطىرخ دىكأت.

Firewall Management Center
Devices / VPN / Edit Advanced

Overview Analysis Policies Devices Objects Integration Deploy 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.

Add Mapping

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

ۋە داداشلار ئەطىرخ دىكأت

ب ئەصاخلا (CLI) رەم اۋالا رەتس ۋە جاۋىف دىكأتلا

نم رشنىلا دعب VPN لاصىتا تادادعى دىكأت

```
// 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
htts-server
enable
max-age 31536000
include-sub-domains
no preload
htts-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

```

ةكبش ليمع يف ديڪاتن

ليمعلا ةداهش ديڪاتن 1. ٽوطخلا

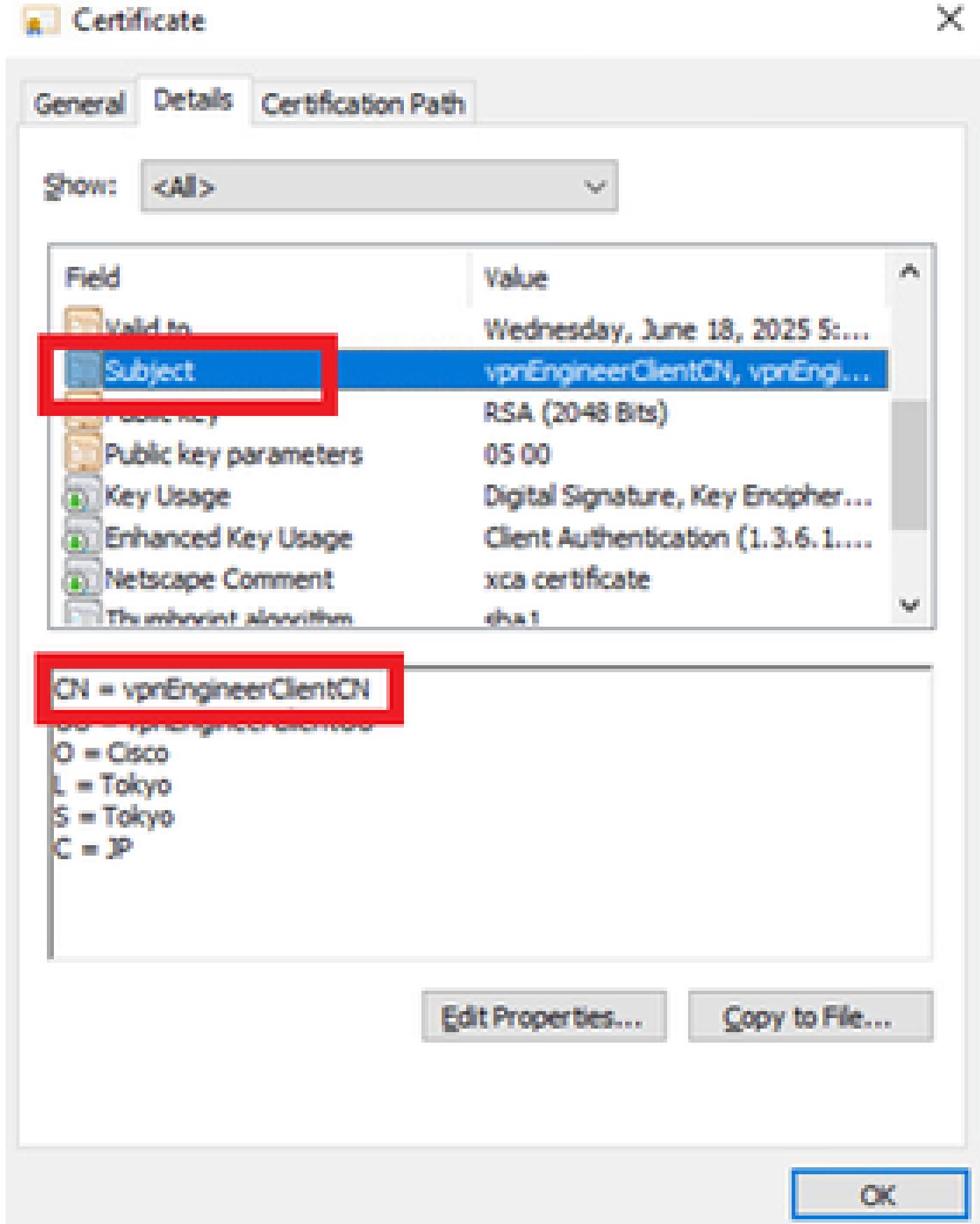
تاداهش > يصخش > يلاح مدخلتسم - تاداهشلا ىلإ لقتنا، ئيسدنەلـا ةكبش ليمع يف، قداصملـل ٽمدختسمـلـا لـيمـعـلـا ةـدـاهـشـ نـمـ قـقـحـتـ.



ليـمعـلـا ةـدـاهـشـ لـيمـعـلـا دـيـڪـاتـنـ

ليـصـافـتـ نـمـ قـقـحـتـ مـثـ، ليـمعـلـا ةـدـاهـشـ قـوـفـ اـجـوـذـمـ اـرـقـنـ رـقـنـاـ عـوـضـوـمـلـاـ.

- عـوـضـوـمـلـاـ: CN = vpnEngineerClientCN



سدن هملا ليمع ةداهش ليصافت



لـيـصـافـتـ نـمـ قـقـحـتـ مـثـ، لـيـمـعـلـاـ مـثـ، لـيـمـعـلـاـ ةـدـاهـشـ قـوـفـ اـجـوـذـمـ اـرـقـنـ رـقـنـاـ عـوـضـوـمـلـاـ.

- عـوـضـوـمـلـاـ: CN = vpnManagerClientCN

Certificate

General Details Certification Path

Show: <All>

Field	Value
Not before	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

ريدملا لمي مع دادهش ليصافت

ديكأت 2. ووطخل CA

- تاداھش لى لىقتنا، ريدملى VPN ئەكپش لىيمع و سدنەملى ئەكپش لىيمع نم لى يف عجرملى نم ققحت، تاداھش لىا > اھي ف قوڭوملا رذجلارىدىتلىا عچارم > يلاحلا مىختىسىمىلا ئەقاداصمىلى مىختىسىمىلا قىدىمىلا.

- نۇع رداش • ftd-ra-ca-common-name

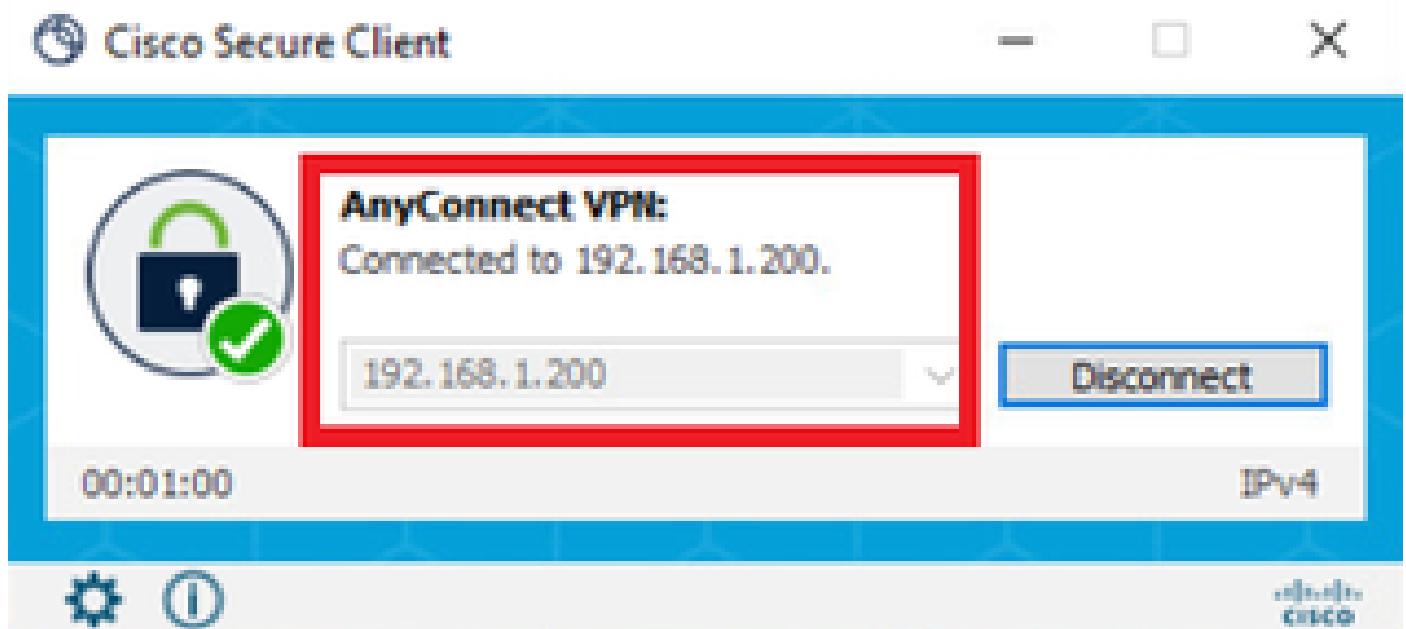
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
127.0.0.1	127.0.0.1	5/17/2027	Server Authentication	duo-endpoint
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authentication	Sectigo (AA)
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authentication	DigiCert Balt...
Class 3 Public Primary Cer...	Class 3 Public Primary Cer...	8/1/2028	Client Authentication	VeriSign Clas...
COMODO RSA Certificati...	COMODO RSA Certificati...	1/18/2038	Client Authentication	Sectigo (form...
Copyright (c) 1997 Micros...	Copyright (c) 1997 Micros...	12/30/1999	Time Stamping	Microsoft Tim...
DESKTOP-VCKHRG1	DESKTOP-VCKHRG1	10/30/2022	Server Authentication	www.infraey...
DigiCert Assured ID Root ...	DigiCert Assured ID Root ...	11/9/2031	<All>	<None>
DigiCert Assured ID Root ...	DigiCert Assured ID Root ...	11/9/2031	Client Authentication	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authentication	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authentication	DigiCert Glob...
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	<All>	<None>
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	Client Authentication	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authentication	DigiCert Trus...
DST Root CA V3	DST Root CA V3	9/30/2021	Client Authentication	DST Root CA
ftd-ra-ca-common-name	ftd-ra-ca-common-name	1/16/2029	<All>	<None>
GlobalSign	GlobalSign	3/18/2029	Client Authentication	GlobalSign R...

دىكأت CA

ۋەھىچىلما نم ققحتلا

لاصتا عدب 1. ۋەھىچىلما VPN

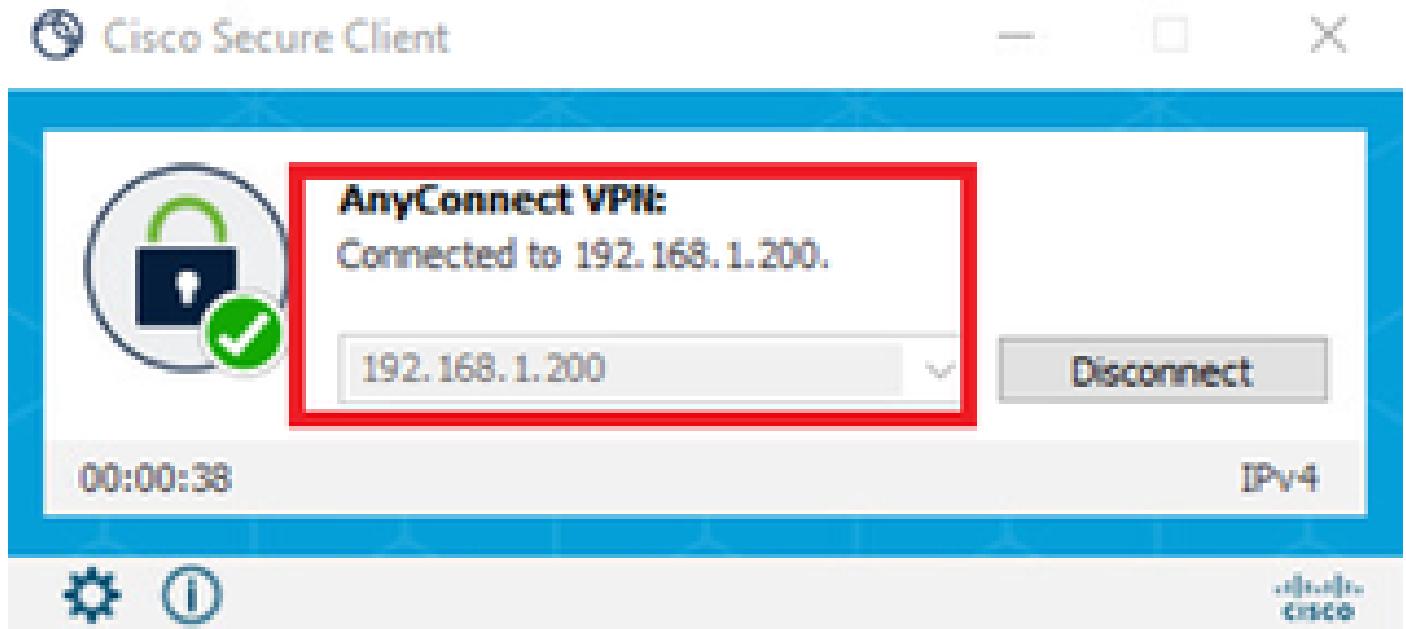
ام Cisco نم نەمآلما لىيمىغا لاصتا أدبا، سدنەملى (VPN) ئېرها ئەنلا ئەكساخلىا ئەكپش لىا لىيمىع يف حاجنب طبىرى لىا، ۋەملىك و لىخدى نأ ۋەھىچىلما نم.



سدنەملى ئەكپش لىيمىع نم لاصتا عدب

، ۋەملىك و لىخدى نأ ۋەھىچىلما نم Cisco Secure Client لاصتا أدبا، In Manager VPN، لىيمىع.

جانب طبري لـ VPN.



قرادإلا ليمع نم VPN لاصتا عدب

يف ظشنل ا تاسلجل ديكأت 2. ووطخلا

لمعلا تاسلجل (Analysis > Users > نومدخلاتسملا) لىا لقتنا ظداصمل ظشنل ا تاسلجل ديكأت VPN.

The screenshot shows the FMC interface under the Analysis tab. It displays two active sessions in a table:

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		

ظشنل ا لماعل ا ظسلج ديكأت

يف VPN لمع تاسلجل ديكأت 3. ووطخلا

ريدمو سدنهم نم ظسلج VPN لـ FTD (Lina) CLI يف رمأ show vpn-sessiondb detail anyconnect.

```
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
Audit 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
Audit 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

اوهالص او عاطخألا فاشكتسا

رتويبمك زاحج ىلع فلم يفو لينا DART Debug syslog لوح تامولعم ىلع روثعلا عقوت كنكمي Windows.

سدنهملا ليمع نم VPN لاصتا عانثأك رحم Lina يف عاطخألا حيיחصت 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=vpnEngineerClientCN,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.  
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:192.168.1.11/500
```

ريدم ليمع نم VPN لاصتا عانثأك رحم Lina يف عاطخألا حيיחصت 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=vpnManagerClientCN,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.  
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:192.168.1.21/65535
```

مولي اتم تاذ صل

[لقطة لـ AnyConnect ملائمة لـ وصل ولـ اتصال](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).