

لي م عمل اة ق داصم اة ق داصم ني وكت FDM 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 ا س آ ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ة ي س ا س آ ت ا م و ل ع م](#)

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

[ت ا ن ي و ك ت ل ا](#)

[FDM 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](#)

[ن ي و ن ع ع م ح ت ة ف ا ض ا 3. ة و ط خ ل ا](#)

[ن م آ ل ي م ع ف ي ر ع ت ف ل م ع ا ش ن ا 4. ة و ط خ ل ا](#)

[FDM ى ل ا ن م آ ل ا ل ي م ع ل ا ف ي ر ع ت ف ل م ل ي م ح ت 5. ة و ط خ ل ا](#)

[ة و م ج م ل ا ج ه ن ة ف ا ض ا 6. ة و ط خ ل ا](#)

[FTD ة د ا ه ش ة ف ا ض ا 7. ة و ط خ ل ا](#)

[FTD ى ل ا C A ة ف ا ض ا 8. ة و ط خ ل ا](#)

[د ع ب ن ع ل و ص و ل ل V P N ل ا ص ت ا ف ي ر ع ت ف ل م ة ف ا ض ا 9. ة و ط خ ل ا](#)

[ل ا ص ت ا ل 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](#)

[F T D ب ة ص ا خ ل ا \(C L I \) ر م ا و آ ل ا ر ط س ة و ج ا و ي ف د ي ك ا ت ل ا](#)

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

[V P N ل ي م ع ى ل ا ن م آ ل ا ل ي م ع ل ا ف ي ر ع ت ف ل م خ س ن 1. ة و ط خ ل ا](#)

[ل ي م ع ل ا ة د ا ه ش د ي ك ا ت 2. ة و ط خ ل ا](#)

[C A د ي ك ا ت 3. ة و ط خ ل ا](#)

[ة ح ص ل ا ن م ق ق ح ت ل ا](#)

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

[F T D C L I ي ف V P N ل م ع ت ا س ل ج د ي ك ا ت 2. 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](#)

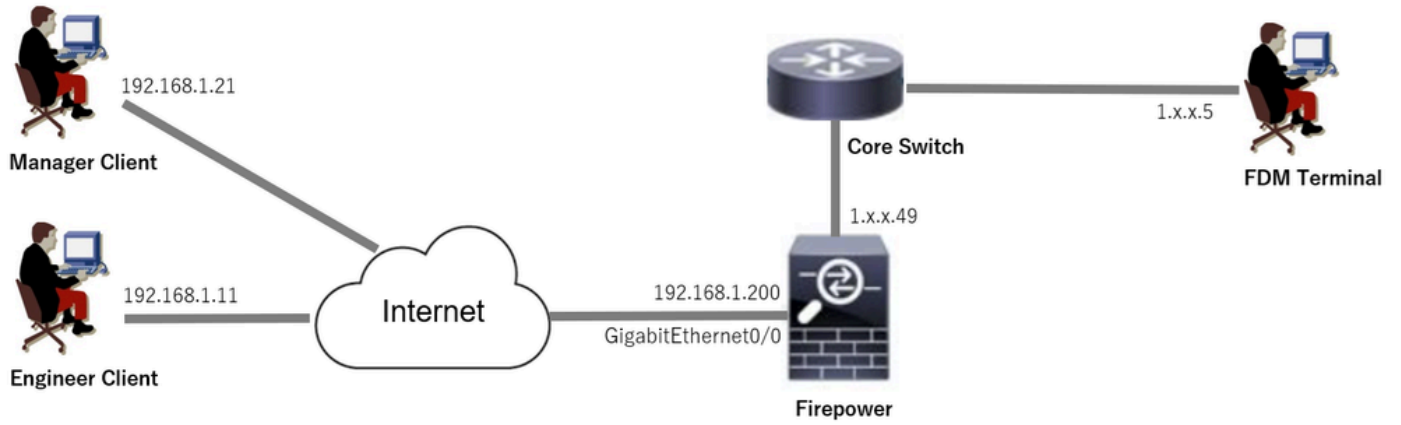
[ة ل ص ت ا ذ ت ا م و ل ع م](#)

ة م د ق م ل ا

م ا د خ ت س ا ب F D M ر ب ع F T D ى ل ع S S L ع م C i s c o S e c u r e C l i e n t د ا د ع ا ة ي ف ي ك د ن ت س م ل ا ا ذ ه ح ض و ي ة ق د ا ص م ل ل ة د ا ه ش ل ا ة ق ب ا ط م .

ة ي س ا س آ ل ا ت ا ب ل ط ت م ل ا

[ت ا ب ل ط ت م ل ا](#)



ةكبش لل ل يطيطخت التا مسرلا

تاني وكتلا

FDM في ني وكتلا

FTD هجاو ني وكت 1. ةوطخلا

ل ةي ج راخ لا و ةي ل خ ادلا هجاو لا ني وكت ب مقو ، تاه جاو لا ةي م ج ضرع > تاه جاو لا > زاه جا لا لا ل ل ق ت نا
 تاه جاو لا ب ي و ب ت لا ةم ال ع في FTD.

ل GigabitEthernet0/0.

- ج راخ : م س ال ا
- IP: 192.168.1.200/24 نا و ن ع

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ GigabitEthernet0/0	outside	Enabled	Routed	192.168.1.200		Enabled	

ة هجاو FTD

Cisco Secure Client صي خرت دي كأت 2. ةوطخلا

في Cisco Secure Client صي خرت دكأ ، ني وكت لا ضرع > ي ك ذ لا صي خرت لا > زاه جا لا لا ل ل ق ت نا
 ع RA VPN صي خرت رصنع.

The screenshot shows the 'SUBSCRIPTION LICENSES INCLUDED' section in the Cisco Firepower Device Manager. The 'RA VPN License' is highlighted with a red box. It is currently 'Enabled' and has a 'Type' dropdown set to 'VPN ONLY'. Other licenses shown include Threat, Malware, and URL License, all of which are 'Disabled by user'.

نمآل ليمعمل صيخرت

نيوانع عمجت ةفاضل 3. ةوطخل

رز + رقنا ، تالكبش > تانئاك ىل لقتنا

The screenshot shows the 'Objects' section in the Cisco Firepower Device Manager. The 'Networks' option in the 'Object Types' sidebar is highlighted with a red box. The main area shows a table of network objects, with one object listed: 'IPv4-Private-10.0.0.0-8'.

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	

نيوانع عمجت ةفاضل

قف اوام رزلا قوف رقنا . دي دج IPv4 نيوانع عمجت ةفاضل ةي رورضل تامولعمل لخدأ

- مسال: ftd-cert-match-pool
- قاطنل: عونل
- قاطن IP: 172.16.1.150-172.16.1.160

Add Network Object



Name

ftd-cert-match-pool

Description

Type



Network



Host



FQDN



Range

IP Range

172.16.1.150-172.16.1.160

e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100

CANCEL

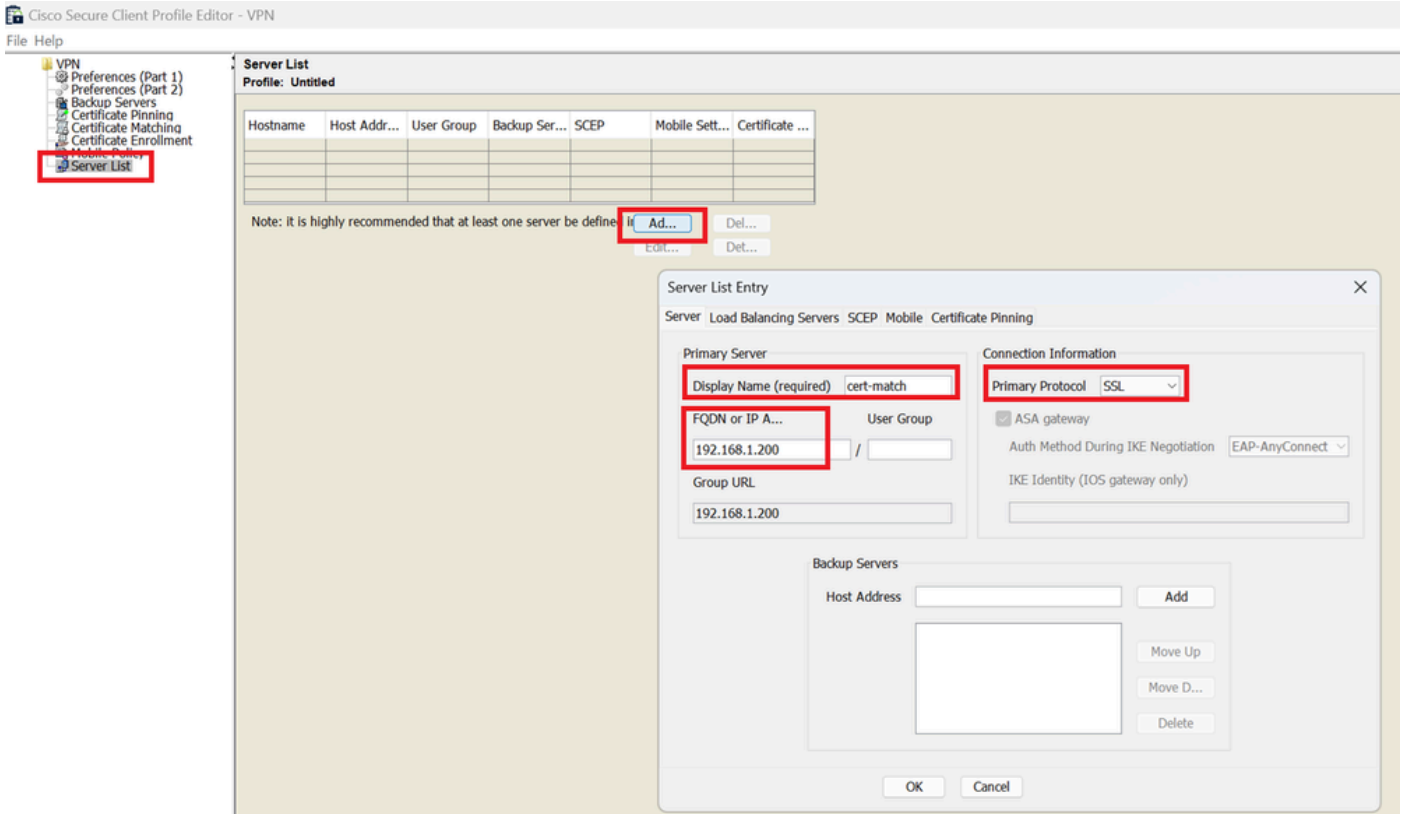
OK

IPv4 نڤوانع عمحت لڤصافت

نمآ لڤمعم فڤرعت فلم عاشنإ. 4 ةوطخلإ

لقتنا [Cisco Software](#) جمارب عقوم نم هتڤبثتو نمآلإ لڤمعلإ فڤرعت فلم ررحم لڤزننتب مق ةمئاق لاخذإ ةفاضلإ ةڤرورضلإ تامولعملإ لخدأ. رز ةفاضلإ قوف رقنا، مداوخلإ ةمئاق ىلإ قفاوم رزلا قوف رقناو مداوخلإ.

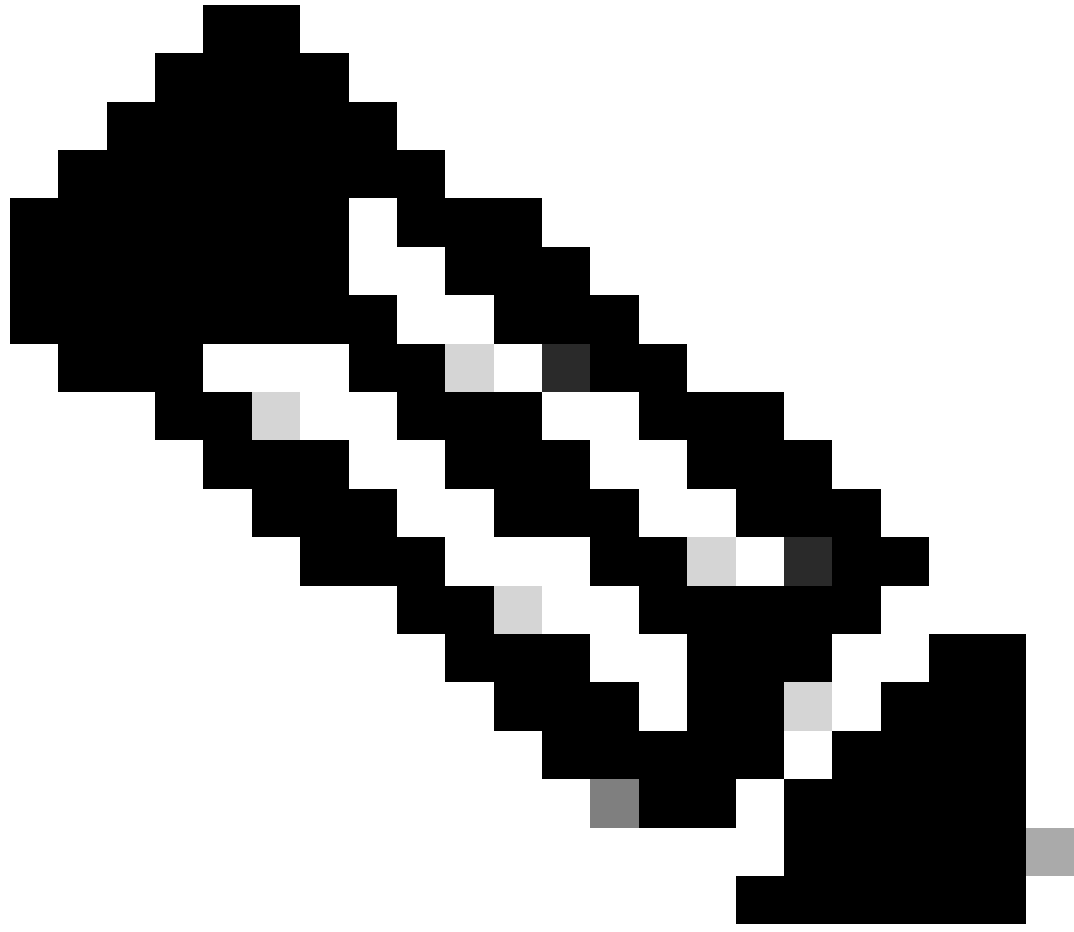
- ضرعلإ مسأ: cert-match
- IP: 192.168.1.200 ناوئع وأ FQDN
- SSL: ساسألأ لوكوتوربلا



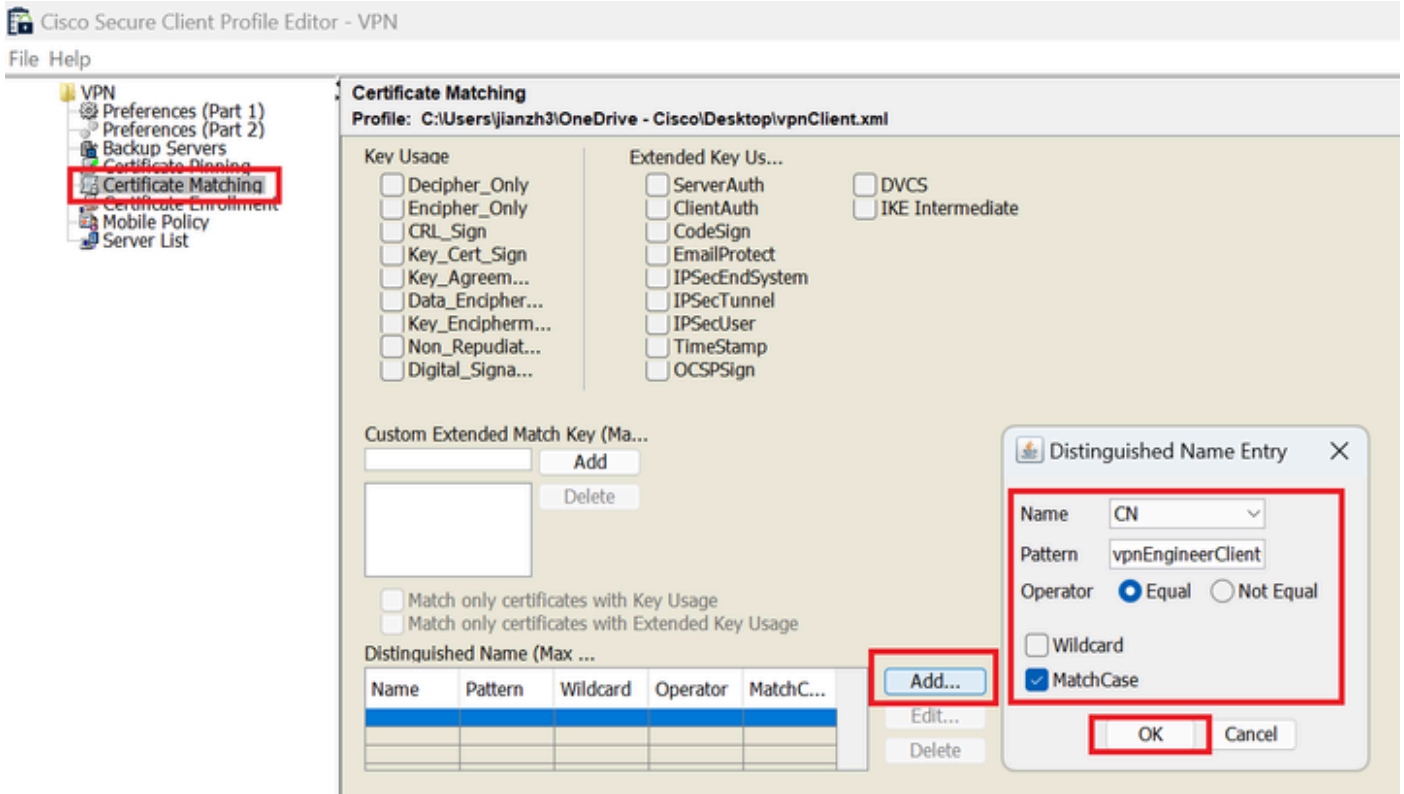
مداوخل ةمئاق لاخدا

لاخدا ةفاضل ةرورضلا تامولعمل لاخدا. رز ةفاضل قوف رقنا، ةداهشلا ةقباطم ىلإ لقتنا قفاوم رز ىلع رقنا وزيتم مسا.

- مرسال: CN
- طمنل: vpnEngineerClientCN
- يواسي: ليغشتلا لماع



دنتسملا اذه في MatchCase راڤخ نم ققحت :ةطحال م



زي مالم مسال لاد

فيري ل فلم لي صافات ديك اوتوي حل مالم رتوي بكم كالم لي ع نم آالم لي مالم فيري ل فلم ظفح

```

<CertificateMatch>
  <MatchOnlyCertsWithKLI>false</MatchOnlyCertsWithKLI>
  <DistinguishedName>
    <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled" MatchCase="Enabled">
      <Name>CN</Name>
      <Pattern>vpnEngineerClientCN</Pattern>
    </DistinguishedNameDefinition>
  </DistinguishedName>
</CertificateMatch>
<EnableAutomaticServerSelection UserControllable="false">
  false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false</RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>cert-match</HostName>
    <HostAddress>192.168.1.200</HostAddress>
  </HostEntry>
</ServerList>
</AnyConnectProfile>

```

نم آالم لي مالم فيري ل فلم

FDM الى نم آالم لي مالم فيري ل فلم لي محت 5 ة ووطخل

نم آالم لي مالم فيري ل فلم عاشن رز الى رقنا، نم آالم لي مالم فيري ل فلم > تانئاك الى لقتنا

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | cisco SECURE

Object Types ←

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profil...**
- Identity Sources

Secure Client Profiles

Filter

#	NAME	FILE NAME	ACTIONS
There are no Secure Client profile objects yet. Start by creating the first Secure Client profile object.			

CREATE SECURE CLIENT PROFILE

نم آ ليمع فيرعت فلم عاشنا

قفاوم رز قوف رقناو نم آ ليمع فيرعت فلم ةفاضال ةرورضال تامولعمل لخدأ

- اسم ال: secureClientProfile
- (يحمل ال رتوي بمك ال نم ليمحت) secureClientProfile.xml: نم آ ليمع ال فيرعت فلم

Add Secure Client Profile

Name

secureClientProfile

Description

Secure Client Profile

UPLOAD secureClientProfile.xml

CANCEL **OK**

نم آ ليمع فيرعت فلم ةفاضال

6. ةوطخل ءومءمءل ءهن ةفاضل

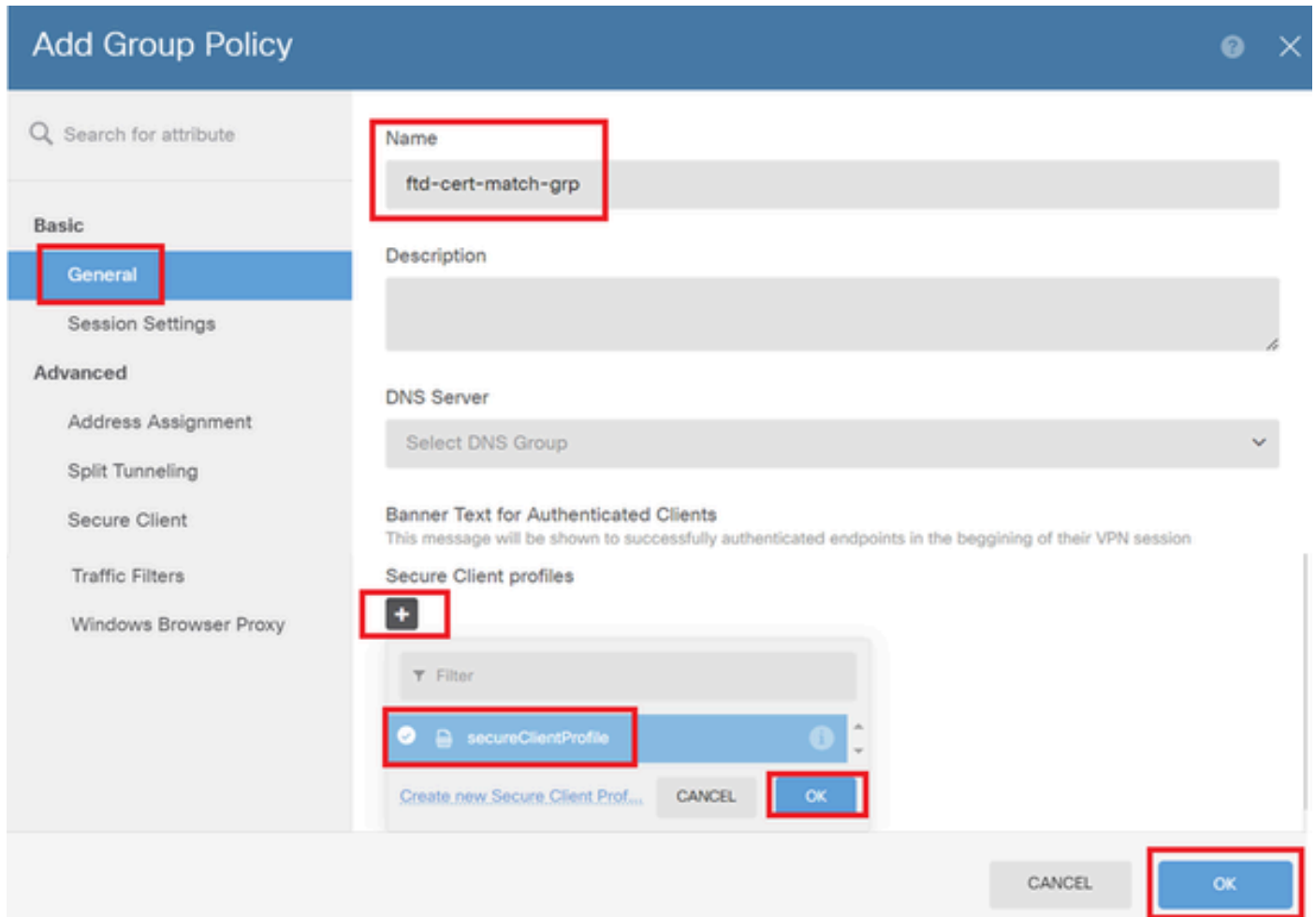
ءومءمءل ءهن ةفاضل > Remote Access VPN (ءءب نع لوصول) > View Configuration (ءرع) > Group Policy (ءومءمءل ءهن) > رز + قوف رقنا.



ءومءمءل ءهن ةفاضل

قفاوم رز قوف رقنا وءومءمءل ءهن ةفاضل ةرورءل ءامولءمءل لءءءب مق.

- مءسءل: ftd-cert-match-grp
- ءومءمءل ءهن ةفاضل: secureClientProfile



ءومءمءل ءهن ةفاضل

7. ةءاءش ةفاضل FTD

رءنع + نم ةلءءء ةءاءش ةفاضل رقنا، ءءءءء > ءءءءء لءءءب.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | CISCO SECURE

Object Types

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates**

Certificates

121 objects

Filter

Preset filters: System defined, User defined

#	NAME	TYPE	ACTIONS
1	AAA-Certificate-Services	Trusted CA Certificate	
2	ACCVRAIZ1	Trusted CA Certificate	
3	Actalis-Authentication-Root-CA	Trusted CA Certificate	
4	AffirmTrust-Commercial	Trusted CA Certificate	
5	AffirmTrust-Networking	Trusted CA Certificate	
6	AffirmTrust-Premium	Trusted CA Certificate	
7	AffirmTrust-Premium-ECC	Trusted CA Certificate	
8	Amazon-Root-CA-1	Trusted CA Certificate	
9	Amazon-Root-CA-2	Trusted CA Certificate	
10	Amazon-Root-CA-3	Trusted CA Certificate	
11	DefaultInternalCertificate	Internal Certificate	
12	DefaultWebserverCertificate	Internal Certificate	

Actions: Add Internal CA, Add Internal Certificate, Add Trusted CA Certificate

ةيلخاد ةداهش ةفاضل

حاتفملاو ةداهشلا ليمحت لىع رقنا

Choose the type of internal certificate you want to create

Upload Certificate and Key

Create a certificate from existing files. PEM and DER files are supported.

Self-Signed Certificate

Create a new certificate that is signed by the device.

حاتفملاو ةداهشلا ليمحت

نم صيخرت حاتفم و ةداهش داريتساب مق م، FTD ةداهش ل ةرورضلا تامولعمل لخدأ قفاوم رز لىع رقنا م يلىحمل رتوي بمكل

- مسالا: ftd-vpn-cert
- مداخ: SSL تامدخ لىع ةحصلا نم ققحتلا مادختسا

Add Internal Certificate



Name

ftd-vpn-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

ftdCert.crt

[Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----  
MIIDfDCCAmSgAwIBAgIIIkE99YS2cmwwDQYJKoZIhvcNAQELBQAwTELMAkGA1UE  
BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVub2t5bzEOMAwGA1UEChMF  
O11-V38-w4AMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVub2t5bzEOMAwGA1UEChMF
```

Certificate Key

Paste certificate key, or choose a file (KEY, PEM)

ftdCertKey.pem

[Upload Certificate Key](#)

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEogIBAAKCAQEAXdn5eTUngo5+GUG2Ng2FjI/+xHRkRrf6o2OccGdzLYK1tzw8  
98HPu1YP0T/qwCffKXuMQ9DEVGWijLRX9nvXd8NoaKUbZVzc03qW3Aje87p0h0t0  
+42b130M7a-0u01-1+1w03w-0+6YEE0+1u4140w-730w-T160wM/TVw0173A-0wVE-C
```

Validation Usage for Special Services

SSL Server

CANCEL

OK

ةيلخادلا ةداهشلا ليصرافت

FTD لي CA ةفاضلا 8 ةوطخلا

رصنع + نم ةقث ق دصم عجرم ةداهش ةفاضلا رقنا ، تاداهش > تانئاك لي لقتنا

Firewall Device Manager

Monitoring Policies **Objects** Device: firepower

admin Administrator

Application Filters

URLs

Geolocations

Syslog Servers

IKE Policies

IPSec Proposals

Secure Client Profiles

Identity Sources

Users

Certificates

Secret Keys

Certificates

120 objects

Filter

Preset filters: System defined, User defined

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	AAA-Certificate-Services	Trusted CA Certificate	
3	ACCVRAIZ1	Trusted CA Certificate	
4	Actalis-Authentication-Root-CA	Trusted CA Certificate	
5	AffirmTrust-Commercial	Trusted CA Certificate	
6	AffirmTrust-Networking	Trusted CA Certificate	
7	AffirmTrust-Premium	Trusted CA Certificate	

[Add Internal CA](#)
[Add Internal Certificate](#)
[Add Trusted CA Certificate](#)

وقت قدصم عجرم ةداهش ةفاضلا

يلحلل رتوي بمك ال ن م ةداهش دروت سا م ث ، CA ل ةمزال ال تامول عمل لخدأ

- مرسال : ftdvpn-ca-cert
- SSL ليمع : ةصاخ ال تامدخل ل ةحصل ال ن م ققحت ال م ادخت سا

Add Trusted CA Certificate

Name

ftdvpn-ca-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

ftd-ra-ca.crt

[Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----
MIIDbDCCA1SgAwIBAgIIUkKgLg229/0wDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE
BHMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDQgQEwVUub2t5bzEOMAwGA1UEChMF
Q31-V38-UjAMBgNVBAgTBVRva31vMQ4wDAYDQgQEwVUub2t5bzEOMAwGA1UEChMF
-----
```

Skip CA Certificate Check *i*

Validation Usage for Special Services

SSL Client

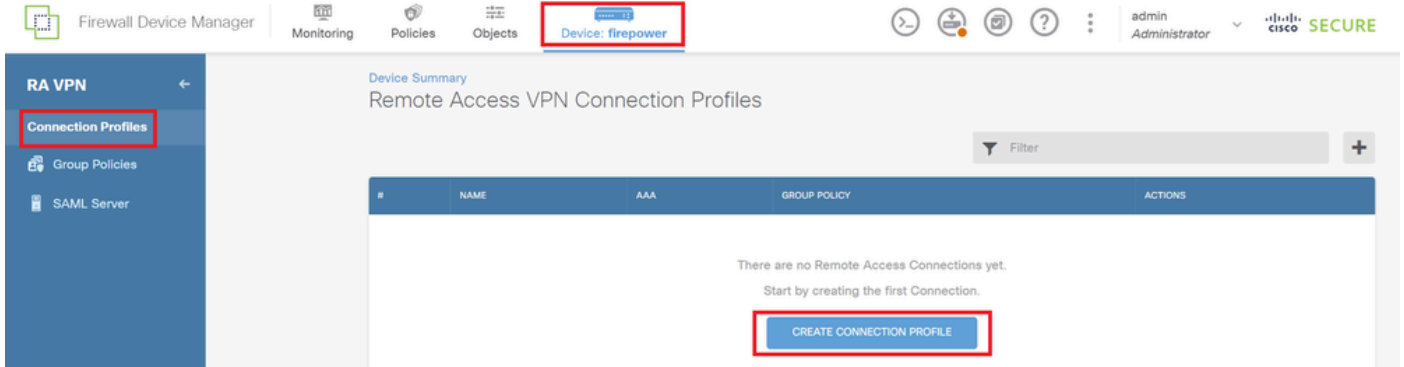
CANCEL

OK

ة قث لال ق دصم لال عجرم لال ة داهش ل ل صرافت

دع ب نع لوصول ل VPN لاصتال فيرعت فلم ة فاضا 9. ة وطلخال

ضرع (View Configuration > Remote Access VPN (دع ب نع لوصول) > زاوجل ال ل لقتنا
فيرعت فلم ءاشن ل رز قوف رقنا، (الاصتال فيرعت تافل) > Connection Profile (ني وكتال
الاصتال).



دع ب نع لوصول ل VPN لاصتال فيرعت فلم ة فاضا

ي لال رز ل رقنا و لاصتال فيرعت فلم ل ة رورضال تامول عمل ل ل خدأ

- لاصتال فيرعت فلم مسا : ftd-cert-match-vpn
- طقف ل ل عم لال ة داهش : ة ق داصم لال عون
- ن يي ع ل ل ددحم ل قح : ة داهش لال نم مدختسم لال مسا
- عئاش لال مسا لال) CN : ساس الال ل قح لال
- ة م يظنن لال ة دحولال) OU : يون اثلال ل قح لال
- IPv4 : ftd-cert-match-pool ن يوانع تاعمجت

Remote Access VPN | 1 Connection and Client Configuration | 2 Remote User Experience | 3 Global Settings | 4 Summary



Connection and Client Configuration

Specify how to authenticate remote users and the secure clients they can use to connect to the inside network.

Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

ftd-cert-match-vpn

Group Alias (one per line, up to 5)

ftd-cert-match-vpn

Group URL (one per line, up to 5)

Primary Identity Source

Authentication Type

Client Certificate Only

Username from Certificate

Map Specific Field

Primary Field: CN (Common Name) | Secondary Field: OU (Organisational Unit)

Use entire DN (distinguished name) as username

Advanced

Authorization Server

Please select

Accounting Server

Please select

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool

ftd-cert-match-pool

IPv6 Address Pool

Endpoints are provided an address from this pool

+

DHCP Servers

+

CANCEL | NEXT

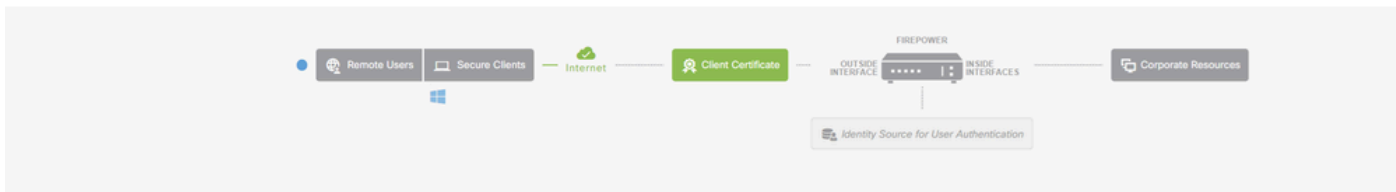
VPN لاصتا فيرعت فلم لي صافات

يالات رزلا قوف رقن او عوم جمل جهن لة رورضلا تام ول عمل ل اخداب مق

- عوم جمل جهن ضرع: ftd-cert-match-grp

Remote Access VPN

- 1 Connection and Client Configuration
- 2 Remote User Experience
- 3 Global Settings
- 4 Summary



Remote User Experience

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.

View Group Policy
ftd-cert-match-grp

Policy Group Brief Details

DNS + BANNER Edit

DNS Server None

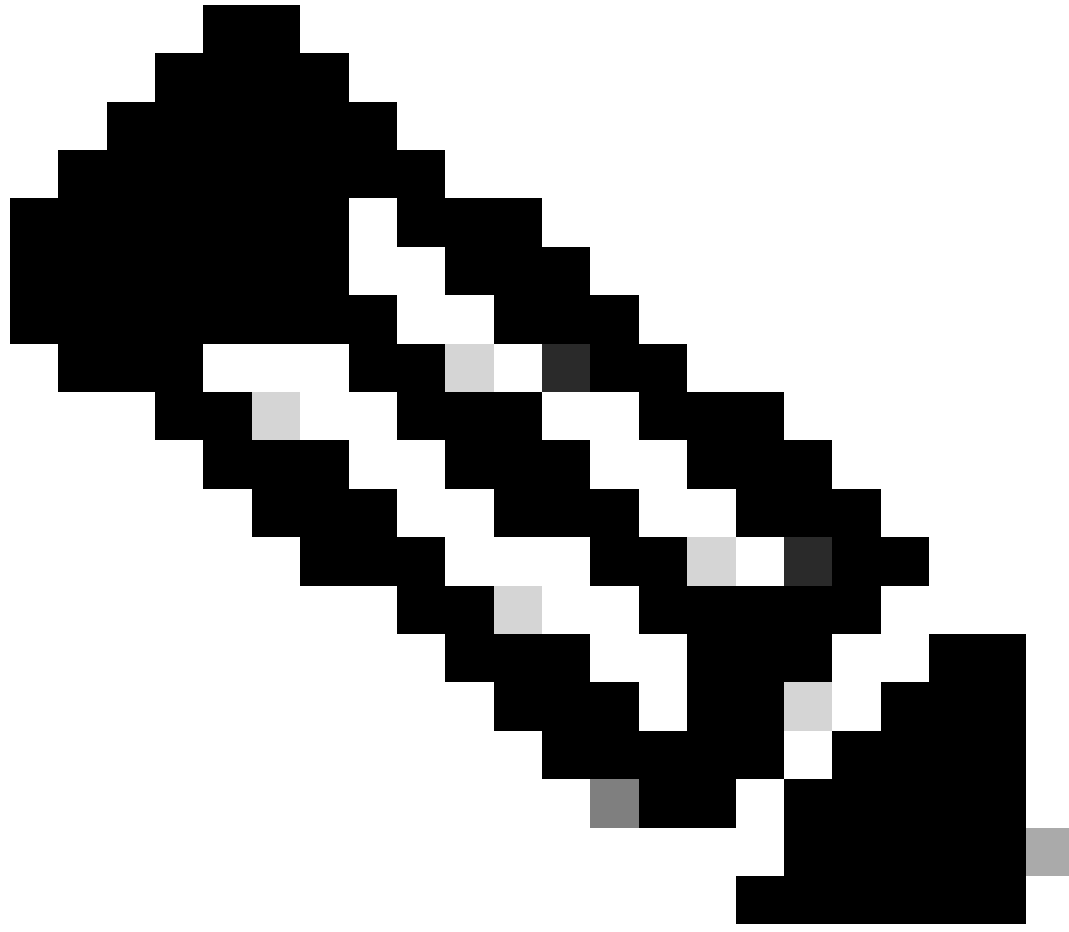
Banner Text for Authentication

BACK NEXT

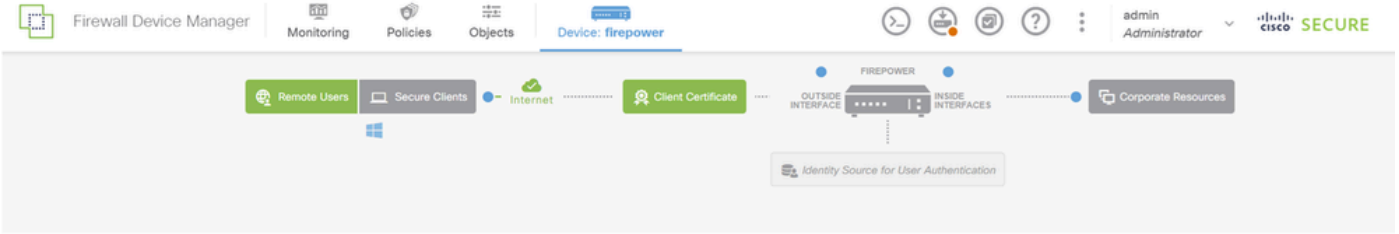
ةوعومحمل جهن ديدحت

VPN لاصتال ةنمآلا ليمعلا ةمزح، ةيجراخ ةهجاو، زاهجلا ةيوه ةداهش دح

- زاهجلا ةيوه ةداهش: ftd-vpn-cert
- ةيجراخلا ةهجاو: جراخ (GigabitEthernet0/0)
- ةنمآلا ليمعلا ةمزح: Cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



دنتسملا اذه يف لطمعلا NAT ءانثتسا ةزيم :ةظحالم



Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity
ftd-vpn-cert (Validation Usage: SSL Se...)

Outside Interface
outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface
e.g. ravn.example.com

Port
443
e.g. 8080

Access Control for VPN Traffic
Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT Exempt

Secure Client Package
If a user does not already have the right secure client package installed, the system will launch the secure client installer when the client authenticates for the first time. The user can then install the package from the system.
You can download secure client packages from software.cisco.com.
You must have the necessary secure client software license.

Packages
UPLOAD PACKAGE

Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK NEXT

ةيمومعلا تادادعلا لىصافت

لاصتالا فيرعت فللمل صخلمل ديكتأ 10 ةوطخلا

رز زاجنإ ةقطقو لىصوت VPN ل تلخد ةمولعمل تدكأ

^ Summary

Review the summary of the Remote Access VPN configuration.

Ftd-Cert-Match-Vpn

STEP 1: CONNECTION AND CLIENT CONFIGURATION

Primary Identity Source

Authentication Type: Client Certificate Only

Primary Identity Source: -

Fallback Local Identity Source: -

Username from Certificate: Map Specific Field

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Advanced

Authorization Server

Accounting Server

Client Address Pool Assignment

IPv4 Address Pool: ftd-cert-match-pool

IPv6 Address Pool: -

DHCP Servers: -

STEP 2: GROUP POLICY

Group Policy Name: ftd-cert-match-grp

Banner + DNS Server

DNS Server: -

Banner text for authenticated clients: -

Session Settings

Maximum Connection Time / Alert Interval: Unlimited / 1 minutes

Idle Timeout / Alert Interval: 30 / 1 minutes

Simultaneous Login per User: 3

Split Tunneling

IPv4 Split Tunneling: Allow all traffic over tunnel

IPv6 Split Tunneling: Allow all traffic over tunnel

Secure Client

Secure Client Profiles: secureClientProfile

STEP 3: GLOBAL SETTINGS

Certificate of Device Identity: ftd-vpn-cert

Outside Interface: GigabitEthernet0/0 (outside)

Fully-qualified Domain Name for the Outside Interface: -

Port: 443

Access Control for VPN Traffic: No

NAT Exempt

NAT Exempt: No

Inside Interfaces: -

Inside Networks: -

Secure Client Package

Packages: Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK FINISH

لاصتالال فيرعت فلمل صخلمللا ديكأت

FTD بة صاخلا (CLI) رماوالا رطس ةهجاويف ديكأتلا

FDM. نم رشنلا دعب FTD ل (CLI) رماوالا رطس ةهجاويف VPN لاصتالادادع ديكأت

```
// Defines IP of interface
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftd-vpn-cert
enrollment terminal
keypair ftd-vpn-cert
crl configure

// Server Certificate
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client
crl configure

// CA
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
```

```

group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles value secureClientProfile type user
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

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

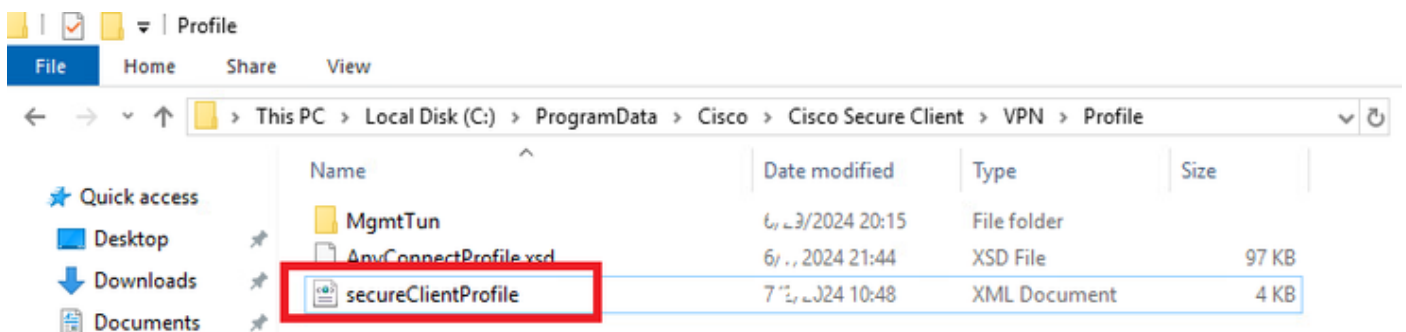
```

VPN كېڭىش لايىھىسىنىڭ تەرتىپى

VPN لايىھىسىنىڭ ئىشلىتىش تەرتىپىنىڭ 1. قىسمى

VPN لايىھىسىنىڭ ئىشلىتىش تەرتىپىنىڭ 2. قىسمى

Windows رتوي بيمك في نمآلا ليمعلا في رعت فلم ليلد: ةظحالم
C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



VPN ليمعلا لى نمآلا ليمعلا في رعت فلم خسن

ليمعلا ةداهش ديكأت 2. ةوطخلا

تاداهش > يصخش > يلاح مدختسم - تاداهشلا لى لوقتنا، ةيسدنهل VPN ةكبش ليمعلا في رعت، ةقداصم لل ةمدختسم لى ليمعلا ةداهش نم ققحت.



Engineer VPN ليمعمل عداهش لاديكأت

ليصافات نم ققحت م ث ، ليصافات لاد ل لقتنا م ث ، ليمعمل عداهش قوف اجودزم ارقن رقنا
عوضوملا

- عوضوملا : CN = vpnEngineerClientCN

Certificate



General Details Certification Path

Show: <All>

Field	Value
Valid to	Wednesday, June 18, 2025 5:...
Subject	vpnEngineerClientCN, vpnEngl...
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 = vpnEngineerClientCN

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

Edit Properties...

Copy to File...

OK

سندنهمل ليمع ةداهش ليرصافت

نم ققحت ،تاداهش > ي صخش > ي لاج مدختسم - تاداهشلا ىل لقتنا ، Manager VPN ليمع ي ف ةقداصم لل ةمدختسم ل ليمع ل ةداهش .



تلي ميعل ةداهش لل دي كأت VPN Manager

لي صافات نم ققحت م، لي صافات لل ل لقتنا م، لي ميعل ةداهش قوف اچودزم ارقن رقنا
عوضوم لل.

- عوضوم لل: CN = vpnManagerClientCN

Certificate



General Details Certification Path

Show: <All>

Field	Value
Issued To	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...

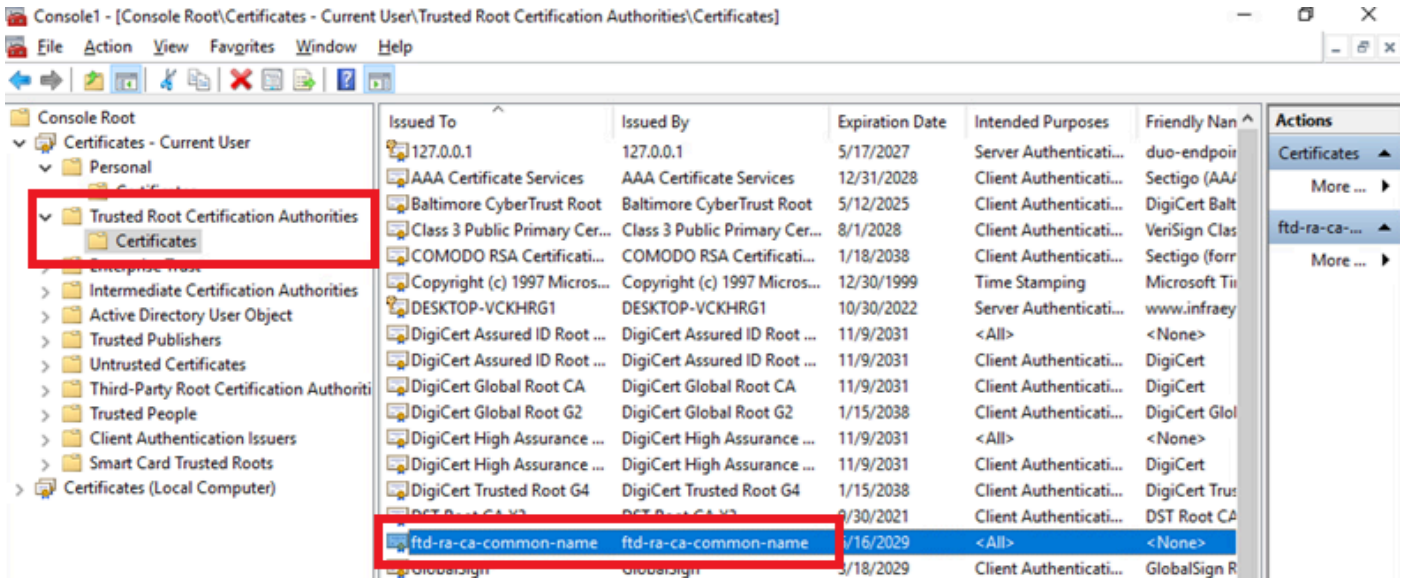
OK

ريدمال ليمع عدهاش ليصافات

CA دي كأت 3. ةوطخال

- 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 > يلاحلا مدختسملا ةقداصملا مدختسملا قداصملا

- نرداص : ftd-ra-ca-common-name

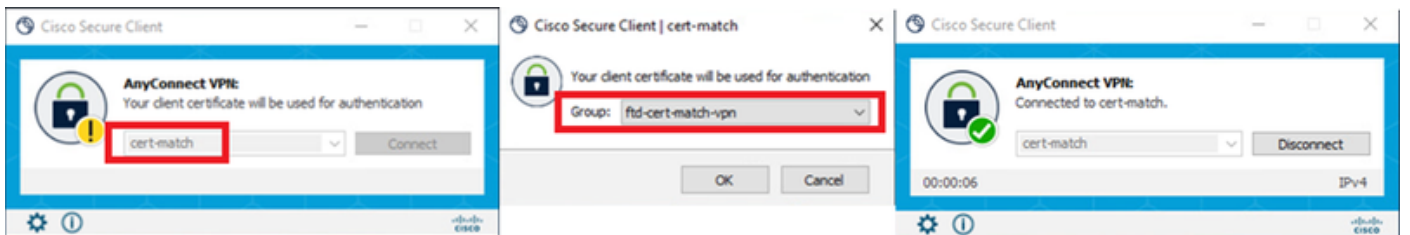


CA ديكتات

ةحصلا نم ققحتلا

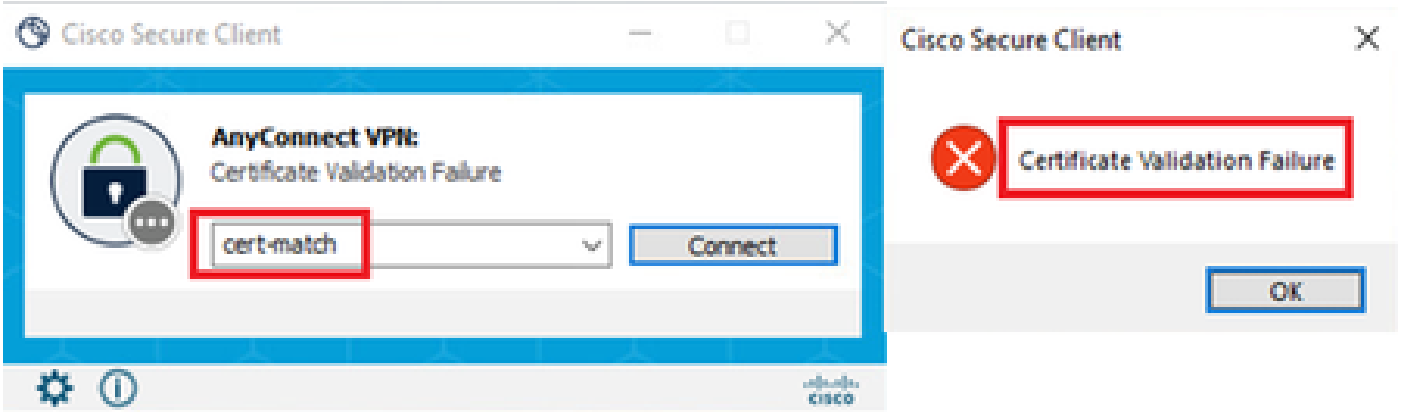
VPN لاصتا ادب 1. ةوطخل

ام Cisco نم نمآلا ليمعلا لاصتا ادبا ،سندنهملل (VPN) ةيرهظلا ةصاخلا ةكبشلا ليمع يف حاجن بطبري VPN ل ،ةملاك و username ل لخدي نأ ةجاج نم



VPN ليمعلا لاصتا حاجن

"Cisco" نم نمآلا ليمعلا "لاصتا ادبا ،"ريدملل (VPN) ةيرهظلا ةصاخلا ةكبشلا ليمع يف ةداهشلا ةحص نم ققحتلا لشف ببسب VPN ةكبش لاصتا لشف



VPN Manager ليمعمل VPN لاصتا لشرف

FTD CLI ف VPN لمع تاسلج ديكأت 2. ةوطخلال

سندنهم نم ةسلج VPN لادكؤي نأ CLI (Lina) FTD في رمأ show vpn-sessiondb detail anyconnect لغش

```
firepower# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx : 14718 Bytes Rx : 12919
Pkts Tx : 2 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn
Login Time : 05:42:03 UTC Tue Jul 2 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 00000000000200006683932b
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 32.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50170 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7359 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0

Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 32.2

Assigned IP : 172.16.1.150 Public IP : 192.168.1.11

Encryption : AES-GCM-256 Hashing : SHA384

Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384

Encapsulation: TLSv1.2 TCP Src Port : 50177

TCP Dst Port : 443 Auth Mode : Certificate

Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes

Client OS : Windows

Client Type : SSL VPN Client

Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74

Bytes Tx : 7359 Bytes Rx : 12919

Pkts Tx : 1 Pkts Rx : 51

Pkts Tx Drop : 0 Pkts Rx Drop : 0

اهحالص او اطاخال فاشكتسا

زاهج ىلع DART فلم في و Lina engine نم syslog اطاخال احيصت في VPN ةقداصم لوح تامولعم ىلع روثعلا عقوت كنكمي Windows رتوي بمك.

سدنهم لاليم نم VPN لاصتا اناثا كرحم Lina في اطاخال احيصت تالجس ىلع لاثم اذه.

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn

Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineClient

Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineClientCN

Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 session

ةلص تاذا تامولعم

[Firepower 2100 ل عبرملا في FDM ةرادا ةمدخ نيوكت](#)

[FDM ةطساوب ةرادملا FTD ىلع دعب نع لوصول ل VPN ةكبش نيوكت](#)

[FirePOWER Device Manager في هتحص نم ققحت لالو syslog نيوكت](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا