

# ةب س ا ح م ل ا و ض ي و ف ت ل ا و ة ق د ا ص م ل ا ن ي و ك ت FDM ر ب ع F T D ي ل ع ن م آ ل ي م ع ل ( A A A )

## ت ا ي و ت ح م ل ا

---

[ة م د ق م ل ا](#)

[ة ي س ا س ا 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 ا 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 ن ي و ك ت ل ا](#)

[F T D ة ه ج ا و ن ي 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](#)

[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 3. ة و ط خ ل ا](#)

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

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

[ل ي ص و ت ل ا ف ي ص و ت ل ة ي ح ر ا خ ل ا ة ه ج ا و ل ا و ز ا ه ج ل ا ة ي و ه ة د ا ه ش ن ي و ك ت 6. ة و ط خ ل ا](#)

[ل ا ص ت ا ل ا ف ي ر ع ت ف ل م ل ة ن م آ ل ي م ع ة ر و ص ن ي و ك ت 7. 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 8. ة و ط خ ل ا](#)

[LocalIdentitySource ي ل ا م د خ ت س م ة ف ا ض ا 9. ة و ط خ ل ا](#)

[F T D ي ل ا C A ة ف ا ض ا 10. ة و ط خ ل ا](#)

[F T D ب ة ص ا خ ل ا \( C L I \) ر م ا و ا ل ا ر ط س ة ه 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](#)

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

[C A 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](#)

[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 V P N ة س ل ج د ي ك ا ت 2. ة و ط خ ل ا](#)

[م د ا خ ل ا ب ل ا ص ت ا ل ا د ي ك ا ت 3. ة و ط خ ل ا](#)

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

[ة ل ص ت ا ذ ت ا م و ل ع م](#)

---

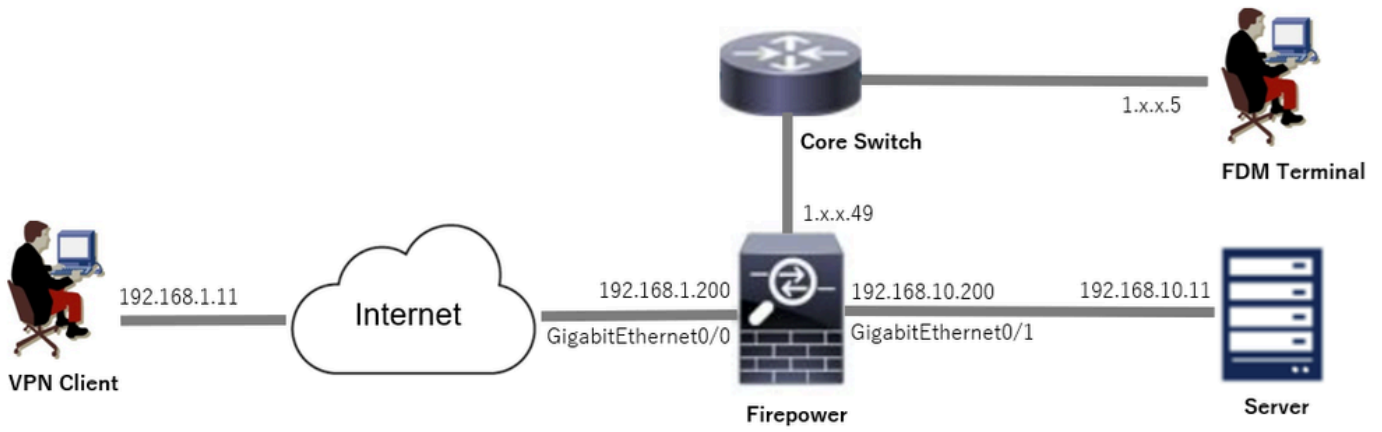
## ة م د ق م ل ا

ه ت ر ا د ا م ت ي ذ ل ا F T D ي ل ع S S L ر ب ع Cisco Secure Client ن ي و ك ت ت ا و ط خ د ن ت س م ل ا ا ذ ه ف ص ي ة د ا ه ش ل ا ة ق د ا ص م و ( A A A ) ة ب س ا ح م ل ا و ض ي و ف ت ل ا و ة ق د ا ص م ل ا م ا د خ ت س ا ب F D M ة ط س ا و ب

## ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا

[ت ا ب ل ط ت م ل ا](#)





ةكبش ل ل يطي طختال مسرلا

## تاني وكتال

### FDM ني وكتال

#### ة FTD هجاو ني وكت 1. ةوطخال

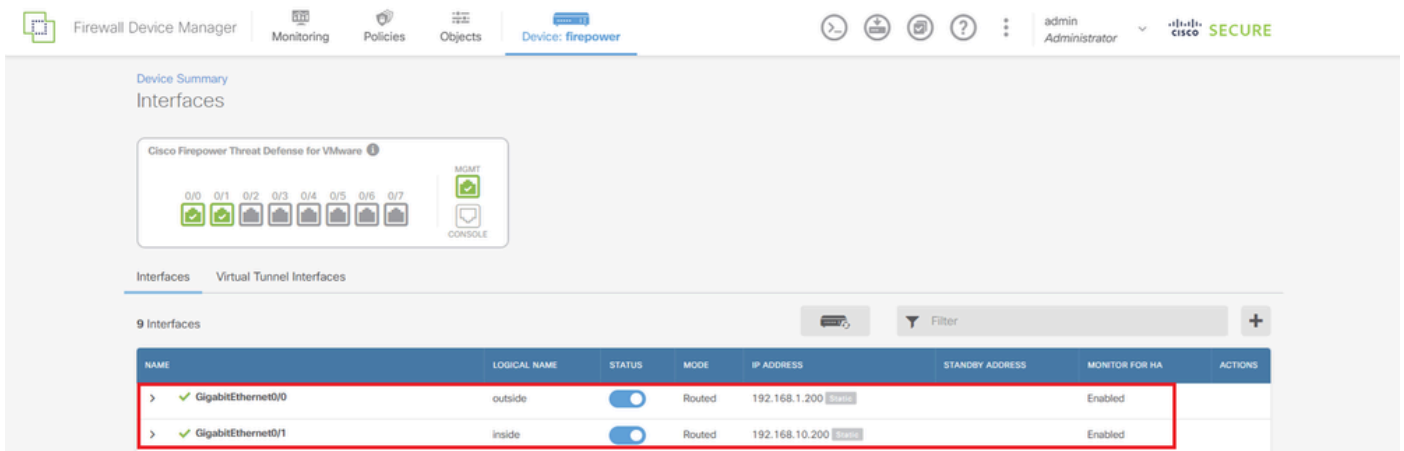
ل FTD ل ةي ج راخ لال او ةي ل خا دل ال ة هجاو ال ني وكت و ، تاهجاو ال عي م ج ضرع > تاهجاو ال > زا هجاو ال ل ل ل ق ت ن ا  
inInterfaceBaseAb.

#### ل GigabitEthernet0/0.

- ج راخ : مسال ال
- ة او ن ع IP: 192.168.1.200/24

#### ل GigabitEthernet0/1.

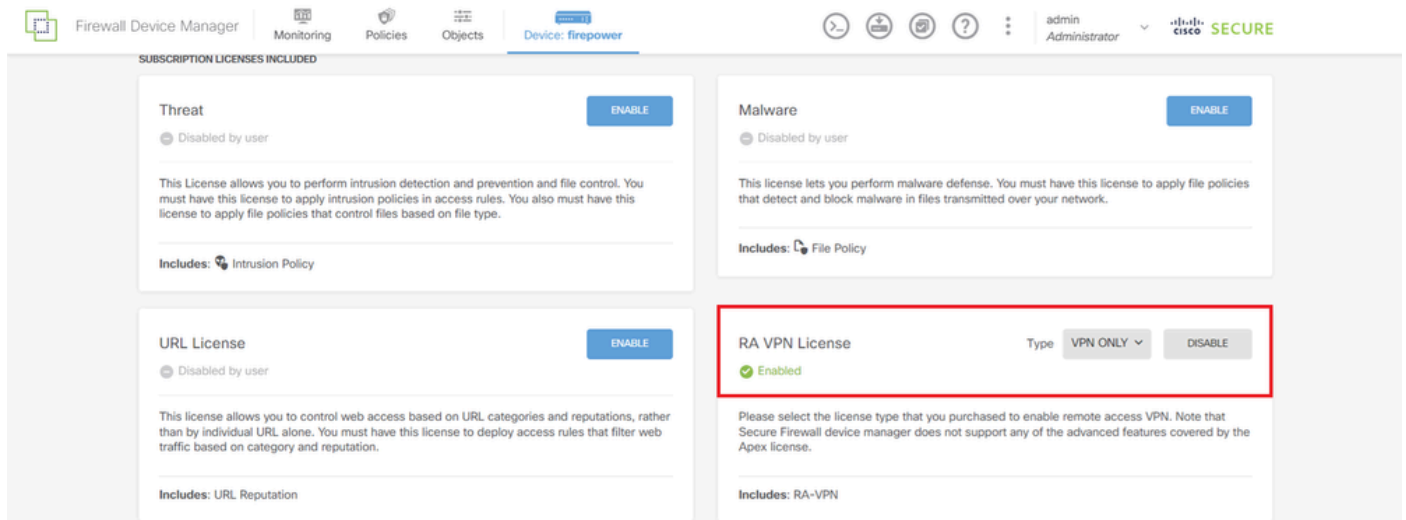
- ل خا دل : مسال ال
- ة او ن ع IP: 192.168.10.200/24



ة FTD هجاو

#### Cisco Secure Client صي خرت دي كأت 2. ةوطخال

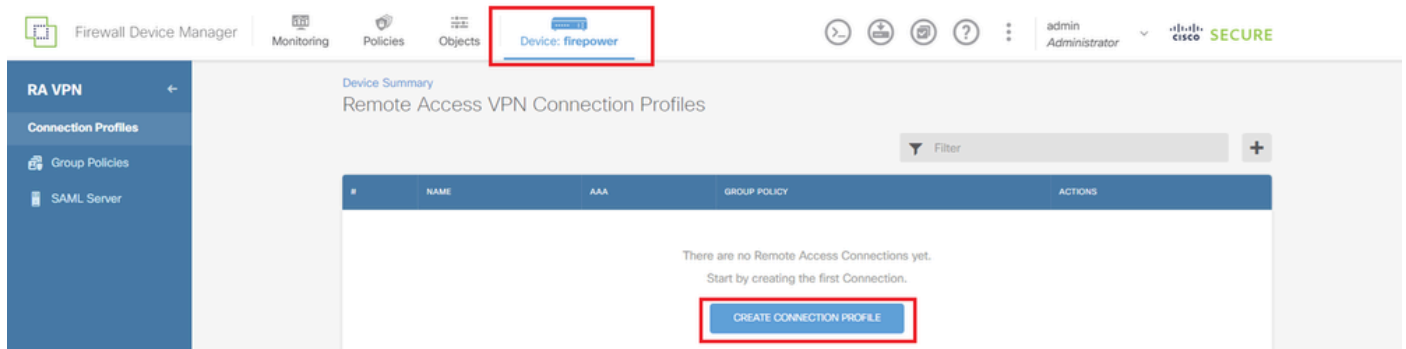
Cisco Secure Client صيخرت نم دكأتو، نيوكتال ضرع > يكدال صيخرتال > زاچال ال لقتنا في RA VPN LicenseItem.



نمأل لي عمل صيخرت

دعب نع لوصول VPN لاصتا فيرعت فلم ةفاضل 3. ةوطخل

View Configuration (ضرع) > Remote Access VPN (دعب نع لوصول) > زاچال ال لقتنا لاصتال فيرعت فلم ءاشن رز قوف رقنا، (نيوكتال).



دعب نع لوصول VPN لاصتا فيرعت فلم ةفاضل

في ديدج ةكبش رز ءاشن رز قوف رقنا لاصتال فيرعت فلم ة ضرورضال تامول عمل لخدأ IPv4 نيوانع عمجت رصنع

- لاصتال فيرعت فلم مسا: ftdvpn-aaa-cert-auth
- لي عمل ةداهش و (AAA) ةب ساجم لاو ضي وفت لاو ةقداصل ما: ةقداصل ما عون
- LocalIdentitySource: مدخت سمل ةقداصل ما لياسال ةي وهال ردصم
- ةذفان في ةدوجوم ال ةداهش ال نم Prefill مدخت سم مسا: لي عمل ةداهش ل ةمدقت ما ادادع ال مدخت سمل لوخد لي جست

## 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

ftdvpn-aaa-cert-auth

#### Group Alias (one per line, up to 5)

ftdvpn-aaa-cert-auth

#### Group URL (one per line, up to 5)

#### Primary Identity Source

##### Authentication Type

AAA and Client Certificate

##### Primary Identity Source for User Authentication

LocalIdentitySource

##### Fallback Local Identity Source

Please Select Local Identity Source

#### AAA Advanced Settings

##### Username from Certificate

##### Map Specific Field

##### Primary Field

CN (Common Name)

##### Secondary Field

OU (Organisational Unit)

##### Use entire DN (distinguished name) as username

#### Client Certificate Advanced Settings

Prefill username from certificate on user login window

Hide username in login window

#### Client Address Pool Assignment

##### IPv4 Address Pool

Endpoints are provided an address from this pool

+

Filter

- IPv4-Private-10.0.0.0-8 Network
- IPv4-Private-172.16.0.0-12 Network
- IPv4-Private-192.168.0.0-16 Network
- any-ipv4 Network

Create new Network

##### IPv6 Address Pool

Endpoints are provided an address from this pool

+

NEXT

OK

VPN لاصتا فيرعت فلم ليصافت

لاصتال فيرعت فلم نيوانع عمجة فاضا 4. ةوطخلا

يديجلا IPv4 نيوانع عمجة دح. ديج IPv4 نيوانع عمجة فاضال ةيروزضال تامولعمل لخدأ يلاتل رزقوف رقناو لاصتال فيرعت فلم هت فاضا تمت يذلا

- مسالا: ftdvpn-aaa-cert-pool
- قاطنلا: عونلا
- قاطن IP: 172.16.1.40-172.16.1.50

## Add Network Object



Name

ftdvpn-aaa-cert-pool

Description

Type



Network



Range

IP Range

172.16.1.40-172.16.1.50

e.g. 192.168.2.1-192.168.2.24 or 2001:068:0:CD30::10-2001:068:0:CD30::100

CANCEL

OK

IPv4 نيوانع عمجت ليصافت

لاصتال فيرعت فلملة وعمجملا جهن ةفاضلا 5 ةوطخلا

ةعمجملا جهن ضرع رصنع يف ديدج ةعمجم جهن عاشن ا قوف رقنا

### 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

Filter

DfltGrpPolicy

Create new Group Policy

DNS + BANNER

DNS Server: None

Banner Text for Authenticated Clients: None

SESSION SETTINGS

Maximum Connection Time / Alert Interval: Unlimited / 1 Minutes

BACK NEXT

ةعومحمل جهن ةفاضلا

جهن ددح. قفاوم رز قوف رقن او ديدج ةعومحمل جهن ةفاضلا ةرورضلا تامولعمل لاداب مق لاصتالا فيرعت فلمل ديدج فاضم ةعومحمل.

- مسالا: ftdvpn-aaa-cert-grp

### Edit Group Policy

Search for attribute

Name: ftdvpn-aaa-cert-grp

Description

DNS Server: CustomDNSServerGroup

Banner Text for Authenticated Clients

Default domain

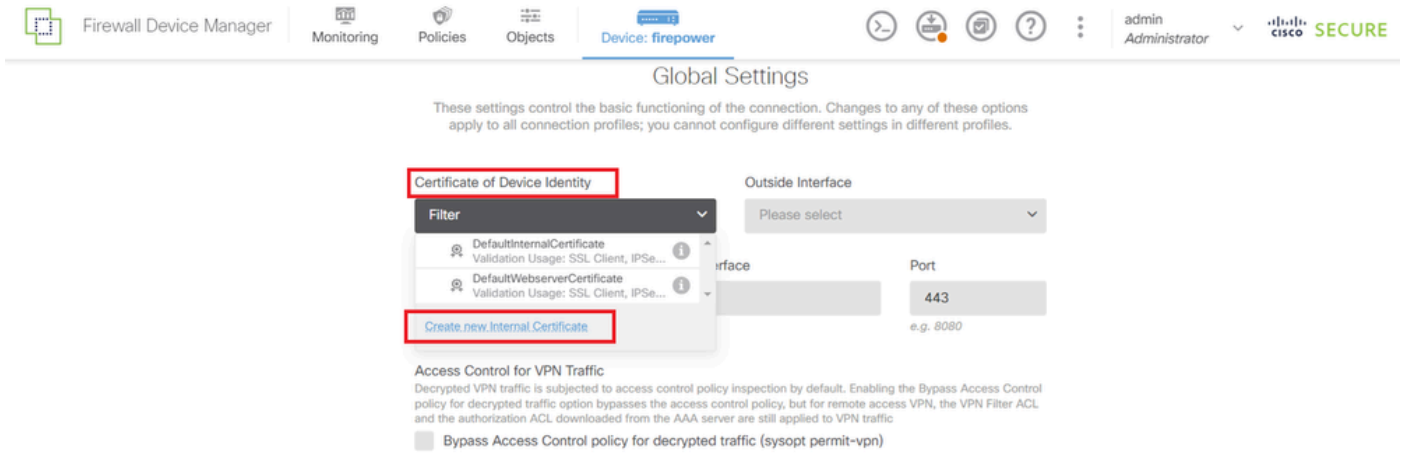
Secure Client profiles

CANCEL OK

ةومحمل جهن لي صافات

لي صوتل في صوتل ةي ج راخلال ةه ج اول او زاه جال ةي وه ةداهش ني وك ت 6 ةوطخال

زاه جال ةي وه رصنع ةداهش يف ةديج ةلخاد ةداهش ءاشنإ يل ع رقنا



ةلخاد ةداهش ةفاض

حات فملاو ةداهشلا لي محت يل ع 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.

حات فملاو ةداهشلا لي محت

نم صيخرت حات فملاو ةداهش داريت ساب مق م ت، FTD ةداهشل ةي رورضلا تامول عملا لخدأ  
ق فوم رز يل ع رقنا م ث يل حمللا رتوي بم كلال



- مسال: ftdvpn-cert
- مداخ: صخال تامدخلل ةحصلل نم ققحتل مادختسا

## Add Internal Certificate

Name

ftdvpn-cert

Certificate ftdCert.crt

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

```
-----BEGIN CERTIFICATE-----
MIIDfDCCAeSgAwIBAgIIIkE99YS2cmwDQYJKoZIhvcNAQELBQAwTELMakGA1UE
BhMCS1AxZDjAMBglNVBAgTBVRva31vMQ4wDAYDVQQHEwUub2t5bzEOMAwGA1UECjMF
O31vY30uZjAAMPMBAAQ0IBAwQDAAYDVR0DQHkE99YS2cmwDQYJKoZIhvcNAQELBQAw
-----
```

Certificate Key ftdCertKey.pem

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

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAxdn5eTUngo5+GUG2Ng2FjI/+xHRkRr-f6o20ccGdzLYK1tzw8
98wPu1YP0T/qwCffKXuMQ9DEVGWijLRX9nvXd8NoaKUbZVzc03qW3AjEB7p0h0t0
-----
```

Validation Usage for Special Services

SSL Server

CANCEL OK

ةلخالل ةداهشل لىصافت

VPN لاصتال ةيجراخلل ةهجالاول او زاهجال ةيوه ةداهش ددح

- زاهجال ةيوه ةداهش: ftdvpn-cert
- ةيجراخلل ةهجالاول: جراخ (GigabitEthernet0/0)

## 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	Outside Interface
ftdvpn-cert (Validation Usage: SSL Ser...)	outside (GigabitEthernet0/0)
Fully-qualified Domain Name for the Outside Interface	Port
e.g. ravn.example.com	443 e.g. 8080

ةمومعلا تادادعلا لىصافت

لاصتالا فىرعت فلمل ةنمآ لىمع ةروص نىوكت 7. ةوطخلا

مزلال رصنع فى Windows ددح

**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](https://software.cisco.com).  
You must have the necessary secure client software license.

Packages

UPLOAD PACKAGE

Windows

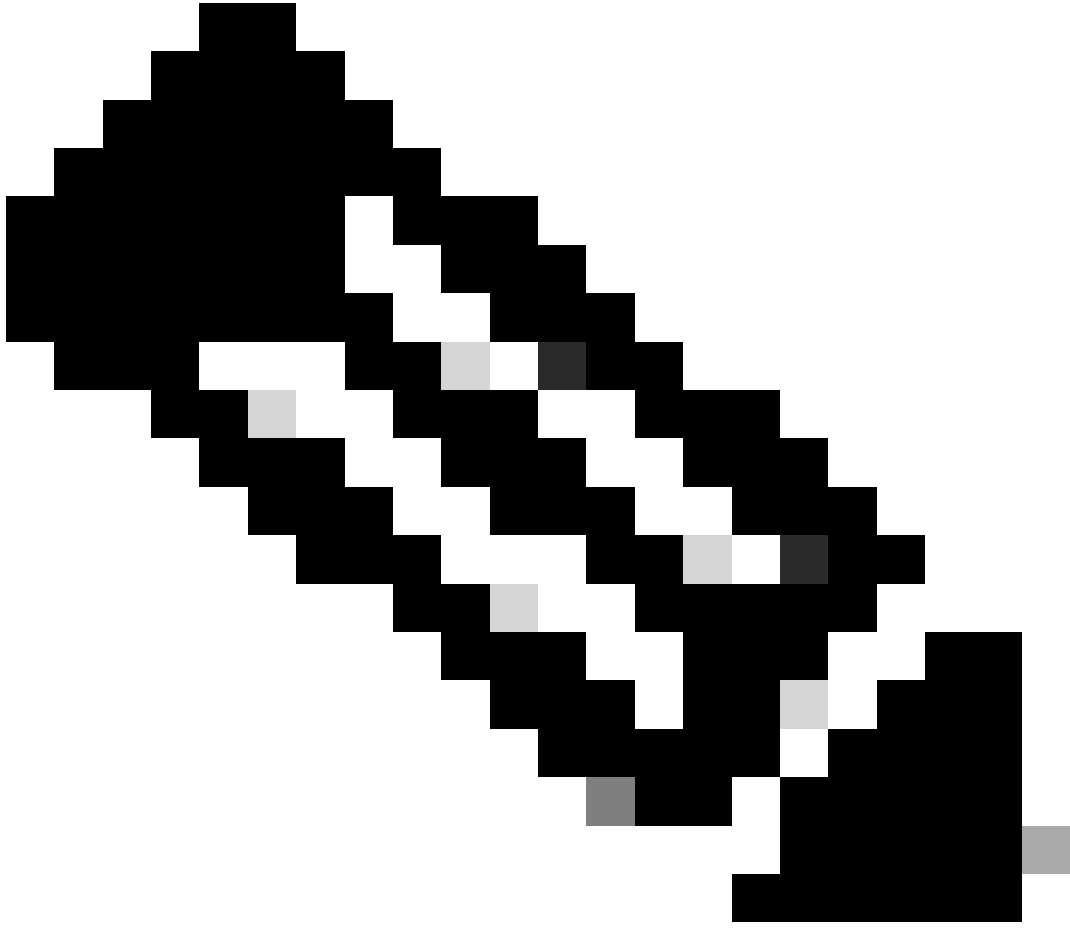
Mac

Linux

BACK NEXT

ةنمآلا لىمعلا ةروص ةمزل لىمحت

Nextbutton. قوف رقناو لىملا رتوي بمكلا نم ةنمآلا لىمعلا ةروص فلم لىمحت ب مق



م تي، يضا رتفا لك ش ب. دن تسم لا اذه يف NAT ءان ثت سا ة زيم لي طعت مت : ة طحال م  
اهري فشت ك ف مت ي التا رورم لا ة ك رحل يف اف التالال لوصول اب مكحت لال ة سايس لي طعت  
ع ضخت اهري فشت ك ف مت ي التا VPN رورم ة ك رح نأ ي نعي امم، (sysopt allowed-vpn)  
لوصولا يف مكحت لال ة سايس صر ح فل.

---

## 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](https://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

نمآل ليمعلا ةروص ةمزح ديدحت

لاصتال فيرعت فللمل صخلمل لديكأت 8. ةوطخل

FINISHbutton. قوف رقن او VPN لاصتال اهلإخدا مت يتلا تامولعمل دكأ

Summary

Review the summary of the Remote Access VPN configuration.

### Ftdvpn-Aaa-Cert-Auth

**STEP 1: CONNECTION AND CLIENT CONFIGURATION**

Primary Identity Source

Authentication Type: AAA and Client Certificate

Primary Identity Source: LocalIdentitySource

AAA Advanced Settings

Username from Certificate: Map Specific Field

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Client Certificate Advanced Settings

Secondary Identity Source

Secondary Identity Source for User Authentication: -

Fallback Local Identity Source: -

Advanced

Authorization Server

Accounting Server

Client Address Pool Assignment

IPv4 Address Pool: ftdvpn-aaa-cert-pool

IPv6 Address Pool: -

DHCP Servers: -

**STEP 2: GROUP POLICY**

Group Policy Name: ftdvpn-aaa-cert-grp

Banner + DNS Server

DNS Server: CustomDNSServerGroup

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: -

**STEP 3: GLOBAL SETTINGS**

Certificate of Device Identity: ftdvpn-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: GigabitEthernet0/0 (outside)

Inside Networks: -

Secure Client Package

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

Instructions

Instructions for your FTD (Firepower Threat Defense) configuration

BACK FINISH

```
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
!
interface GigabitEthernet0/1
speed auto
nameif inside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50

// Defines a local user
username sslVPNClientCN password ***** pbkdf2

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
enrollment terminal
keypair ftdvpn-cert
validation-usage ssl-server
crl configure

// Server Certificate
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
.....
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client ssl-server
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 enable
tunnel-group-list enable
cache
disable
error-recovery disable
```

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

```
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
dns-server value 64.x.x.245 64.x.x.184
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 none
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting
```

```
// Configures the tunnel-group to use the aaa & certificate authentication
```

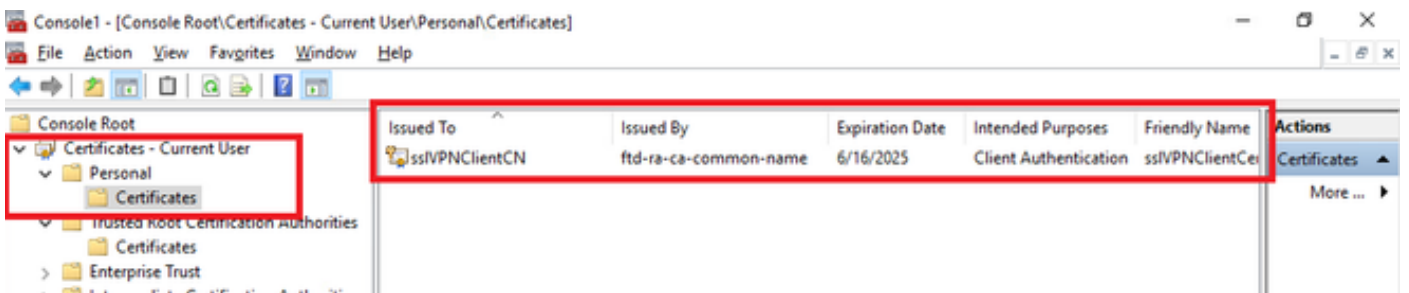
```
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
```

```
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

## VPN كابتش ليمع يف ديكتات

ليمعال اءاهش ديكتات 1. ءوطخال

ليمعال اءاهش نم ققحت ، اءاهش > يصخش > للاح مءختسم - اءاهشلا لىل لقتنا ءقءاصم لل ءمءختسملا

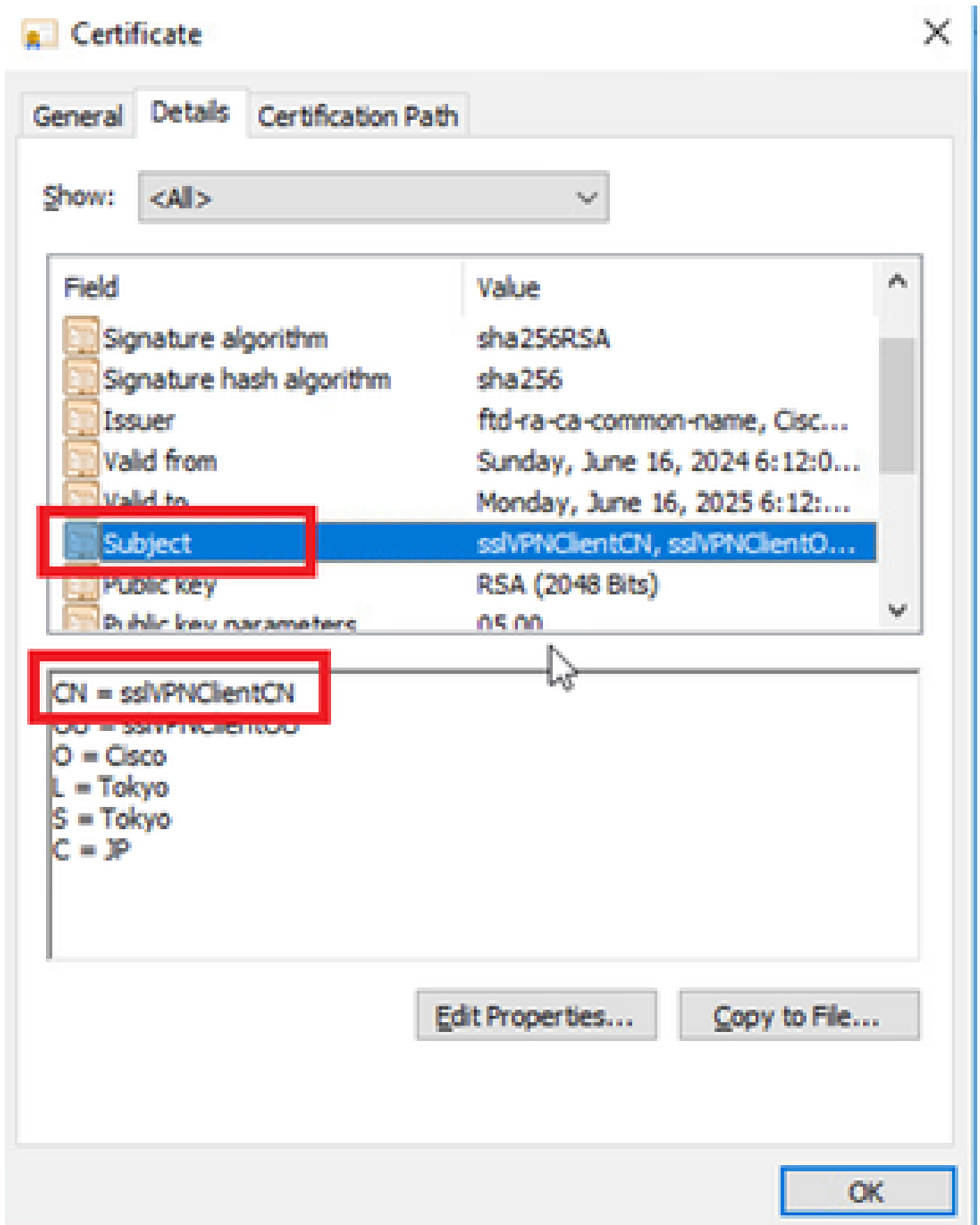


ليمعال اءاهش ديكتات

لوصاف نم ققحت مء ، Details لىل لقتنا مء ، ليمعال اءاهش قوف اءوزم ارقن رقنا ءوضوملا

- ءوضوملا : CN = ssIVPNClientCN





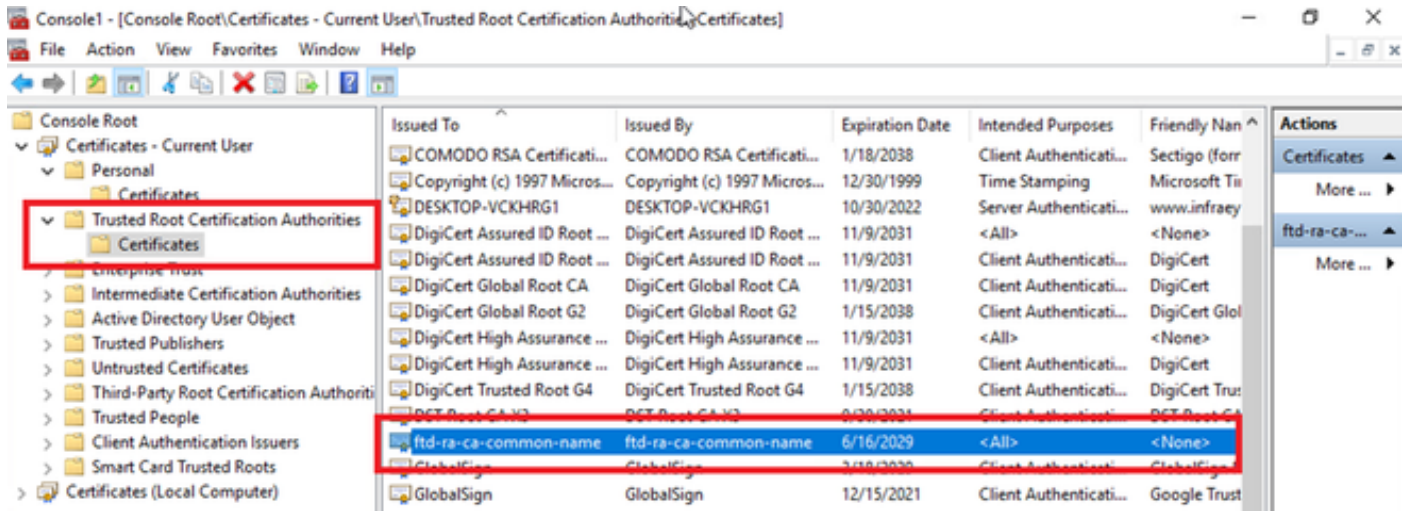
لي معال عدهاش لي صرافت

CA دي كات 2. ةوطخال

تاداهشال > اهب قو و نومال رذجال قي دصتال عجارم > يلال م دخت سمل - تاداهشال يلال لقتنا

ة. قداصل لمدختس م ل قداصل عجر م ل نم ققحت

- نع رداص : ftd-ra-ca-common-name

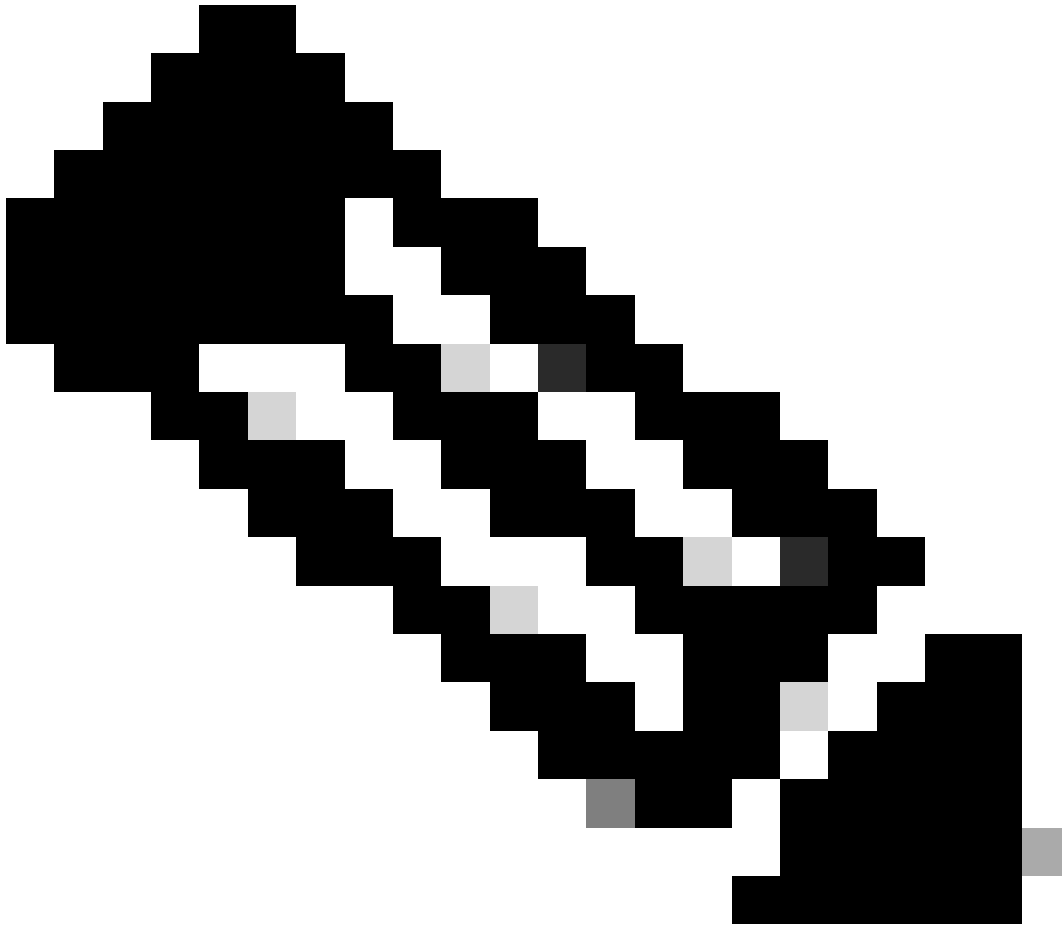


CA دي كأت

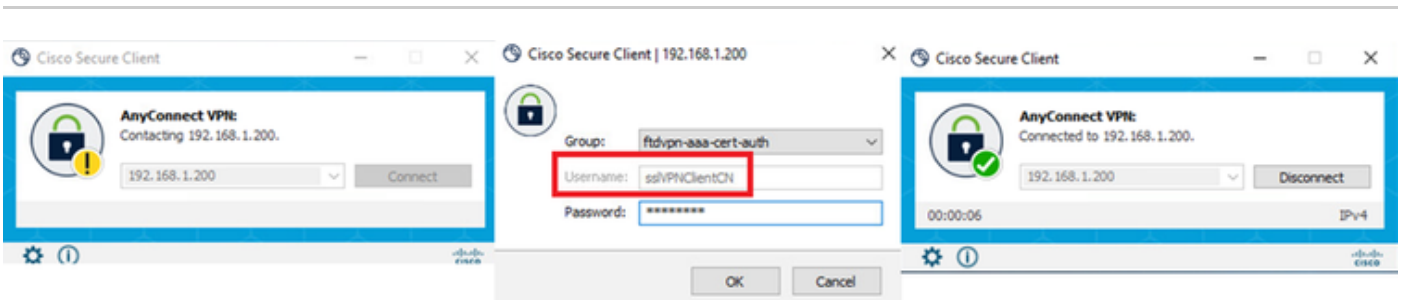
## ةحصل ل نم ققحت ل

VPN لاصتا ادب .1 ةوطخل

ةداهش نوبزل نم username ل تجرختسا Cisco Secure Client لاصتا ادب ،ةياهنلا ةطقن يل عة. ةيوه ةحص VPN ل ةمك ل لخدني نأ جاتحت تنأ



لي م عمل اءاهشل "(CN) عئاشل ل مسال" ل قح نم مدخت سمل مسال جارخت سا متي :ءظالم دن سمل اءه في



VPN لاصتا ادب

## 2. ةوطخل ف VPN ف FTD CLI ةسلج ديكأت

ةسلج VPN ل ا دكؤي نأ CLI (Lina) FTD في رمأ show vpn-sessiondb detail anyconnect لءغش

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

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 4  
Assigned IP : 172.16.1.40 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 : 29072 Bytes Rx : 44412  
Pkts Tx : 10 Pkts Rx : 442  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth  
Login Time : 11:47:42 UTC Sat Jun 29 2024  
Duration : 1h:09m:30s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 000000000004000667ff45e  
Security Grp : none Tunnel Zone : 0

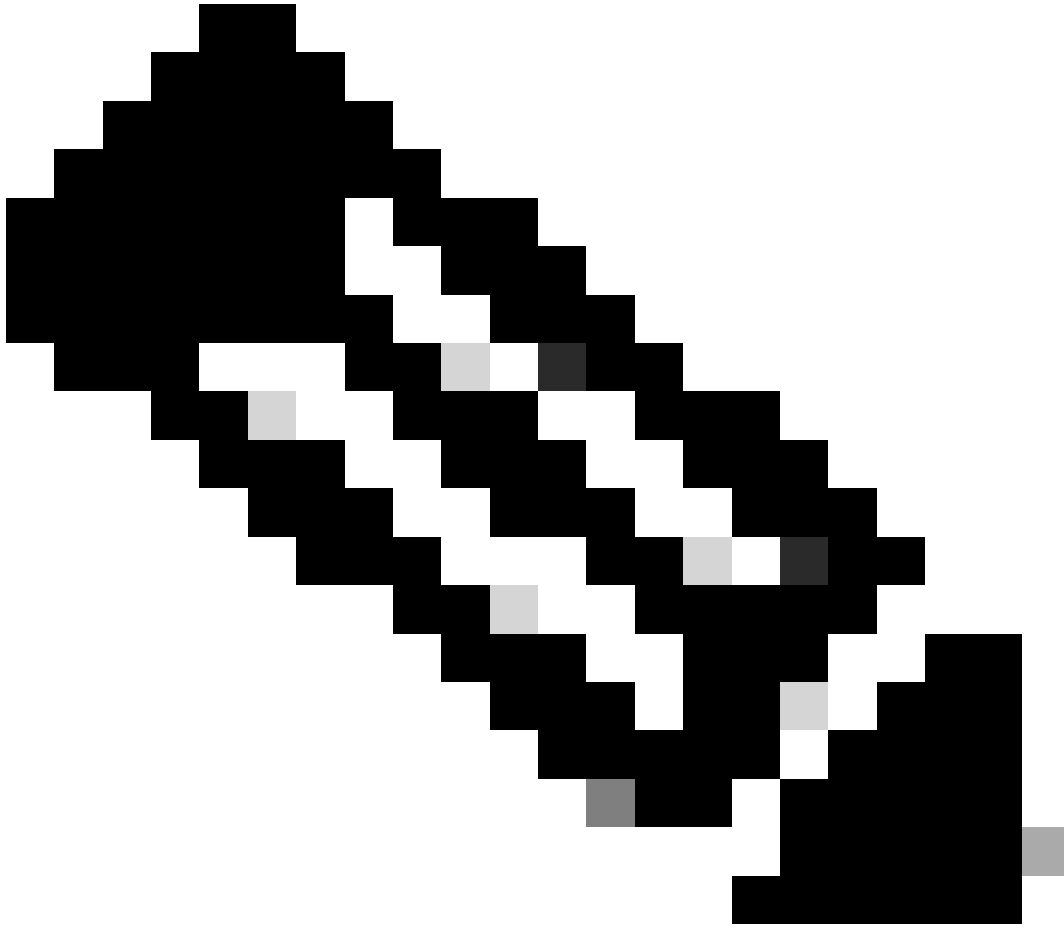
AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:  
Tunnel ID : 4.1  
Public IP : 192.168.1.11  
Encryption : none Hashing : none  
TCP Src Port : 49779 TCP Dst Port : 443  
Auth Mode : Certificate and userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 7 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 : 14356 Bytes Rx : 0  
Pkts Tx : 2 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:  
Tunnel ID : 4.3  
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384  
Encapsulation: TLSv1.2 TCP Src Port : 49788  
TCP Dst Port : 443 Auth Mode : Certificate and userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74  
Bytes Tx : 7178 Bytes Rx : 10358  
Pkts Tx : 1 Pkts Rx : 118  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

مداخل اب لاصتال دي كأت 3. ةوطخلال

ةكبشل لليمع ني ب لاصتال حاجن نم دكأتو ،مدخلال ل(VPN) ةيره اطلال ةصاخال ةكبشل لليمع نم لاصتال رابخل اءبا



اهري فشت ك ف متي لارورم لة كرحل يف افاف لالال لوصولا يف مكحتل رايل ليطعتل ارطن :ةظالم (sysopt allowed-vpn) نيوانع عمجت لوصول حمست يتل لوصولا يف مكحتل دعاوق عاشنا لىل ةجأب تن أف ، 7 ةوطا ل يف (vpn) مداخل لىل كيدل .

---

```
C:\Users\cisco>ping 192.168.10.11
```

```
Pinging 192.168.10.11 with 32 bytes of data:  
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128  
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128  
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128  
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128
```

```
Ping statistics for 192.168.10.11:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

لاصتال را بتخا حجن

ةمزل طاقتل ديكأتل (Lina) ل CLI ف capture in interface inside real-timeRunCommand

```
firepower# capture in interface inside real-time
```

Warning: using this option with a slow console connection may result in an excessive amount of non-displayed packets due to performance limitations.

Use ctrl-c to terminate real-time capture

```
1: 12:03:26.626691 172.16.1.40 > 192.168.10.11 icmp: echo request  
2: 12:03:26.627134 192.168.10.11 > 172.16.1.40 icmp: echo reply  
3: 12:03:27.634641 172.16.1.40 > 192.168.10.11 icmp: echo request  
4: 12:03:27.635144 192.168.10.11 > 172.16.1.40 icmp: echo reply  
5: 12:03:28.650189 172.16.1.40 > 192.168.10.11 icmp: echo request  
6: 12:03:28.650601 192.168.10.11 > 172.16.1.40 icmp: echo reply  
7: 12:03:29.665813 172.16.1.40 > 192.168.10.11 icmp: echo request  
8: 12:03:29.666332 192.168.10.11 > 172.16.1.40 icmp: echo reply
```

اهال صاوا عاطخأل فاشكتسا

زاهج لىل ع DART فلم ف و Lina engine نم syslog عاطخأل احيصت ف VPN ةقداصم لوح تامولعم لىل ع روتعلا ع قوت كنكم ف Windows رت و بيمك

Lina كرحم ف عاطخأل احيصت تالجم لىل ع لاثم اذه

```
// Certificate Authentication
```

```
Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
```

```
Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
```

```
Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=sslVPNClientCN
```

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

Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 3]

Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 3]

// AAA Authentication

Jun 29 2024 11:29:53: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN

Jun 29 2024 11:29:53: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN

Jun 29 2024 11:29:53: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN

اهم ادخستس كنكمي تامولعم رفوت يتالو، FTD ل فيصيصيخشش التال (CLI) رم اوألا رطس ةهجاو نم اطاخال هذه ليغشت نكمي  
اهحالص او نيوكتال اطاخال فاشكتس ال.

- debug crypto ca 14
- debug webVPN AnyConnect 255
- debug crypto ike-common 255

ةلص تاذا تامولعم

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

[FDM ةطس او ب ةرادملا FTD ل ع دع ب نع لوصول ل VPN ةكبش نيوكت](#)

[FirePOWER Device Manager في هتحص نم ققحتل او syslog نيوكت](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء نأ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة يرش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل 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 ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه 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 أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا