تكوين المصادقة والتفويض والمحاسبة (AAA) لعميل آمن على FTD عبر FMC

المحتويات

المقدمة

يصف هذا المستند خطوات تكوين Cisco Secure Client عبر SSL على FTD الذي تتم إدارته بواسطة FMC باستخدام المصادقة والتفويض والمحاسبة (AAA) ومصادقة الشهادة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة FireSIGHT (FMC) من Cisco
- النظام الظاهري للدفاع ضد تهديد جدار الحماية (FTD)
- تدفق مصادقة VPN

المكونات المستخدمة

- مركز إدارة Cisco Firepower ل VMWare 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1

- Cisco Secure Client 5.1.3.62

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

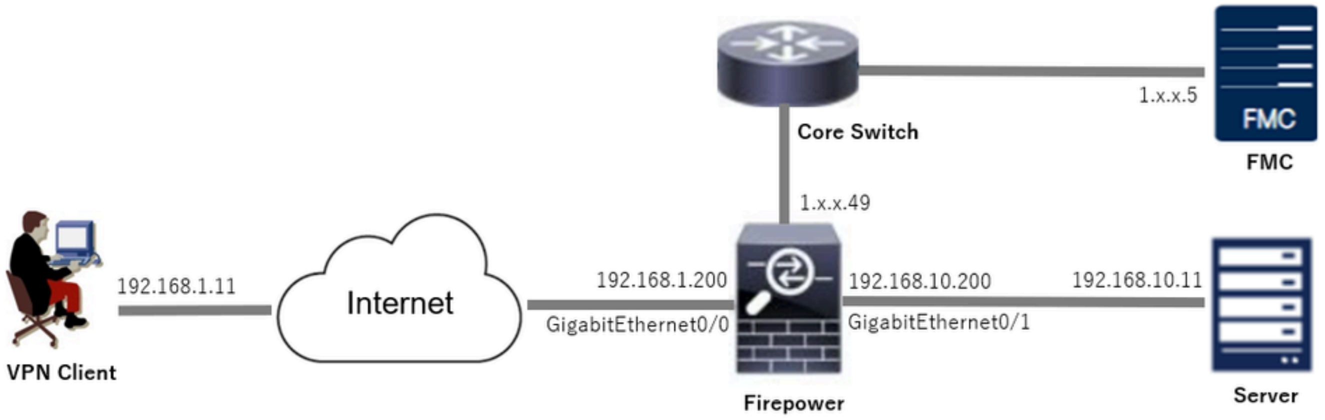
ومع اعتماد المؤسسات لتدابير أمنية أكثر صرامة، أصبح الجمع بين المصادقة ذات العاملين (2FA) والمصادقة القائمة على الشهادة ممارسة شائعة لتعزيز الأمن والحماية من الوصول غير المصرح به. إحدى الميزات التي يمكنها تحسين تجربة المستخدم وأمانه بشكل كبير هي القدرة على ملء اسم المستخدم مسبقا في عميل Cisco الآمن. تعمل هذه الميزة على تبسيط عملية تسجيل الدخول وتحسين الكفاءة الكلية للوصول عن بعد. يوضح هذا المستند كيفية دمج اسم المستخدم المعبأ مسبقا مع عميل Cisco الآمن على FTD، مما يضمن إمكانية اتصال المستخدمين بالشبكة بسرعة وأمان.

تحتوي هذه الشهادات على اسم مشترك بداخلها، يتم إستخدامه لأغراض التخويل.

- ك.أ: ftd-ra-ca-common-name
- شهادة العميل: sslVPNClientCN
- شهادة الخادم: 192.168.1.200

الرسم التخطيطي للشبكة

تعرض هذه الصورة المخطط الذي يتم إستخدامه لمثال هذا المستند.



الرسم التخطيطي للشبكة

التكوينات

التكوين في FMC

الخطوة 1. تكوين واجهة FTD

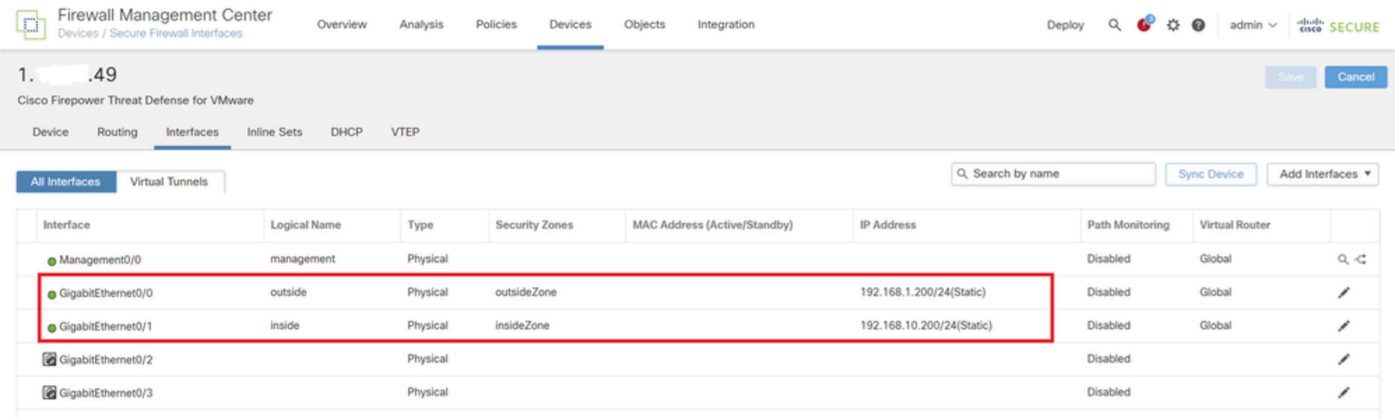
انتقل إلى الأجهزة > إدارة الأجهزة، وحرر جهاز FTD الهدف، وقم بتكوين الواجهة الداخلية والخارجية ل FTD في علامة التبويب الواجهات.

ل GigabitEthernet0/0،

- الاسم : خارج
- المنطقة الأمنية: خارج المنطقة
- عنوان IP: 192.168.1.200/24

ل GigabitEthernet0/1،

- الاسم :
- المنطقة الأمنية: داخلZone
- عنوان IP: 192.168.10.200/24



1.[redacted].49

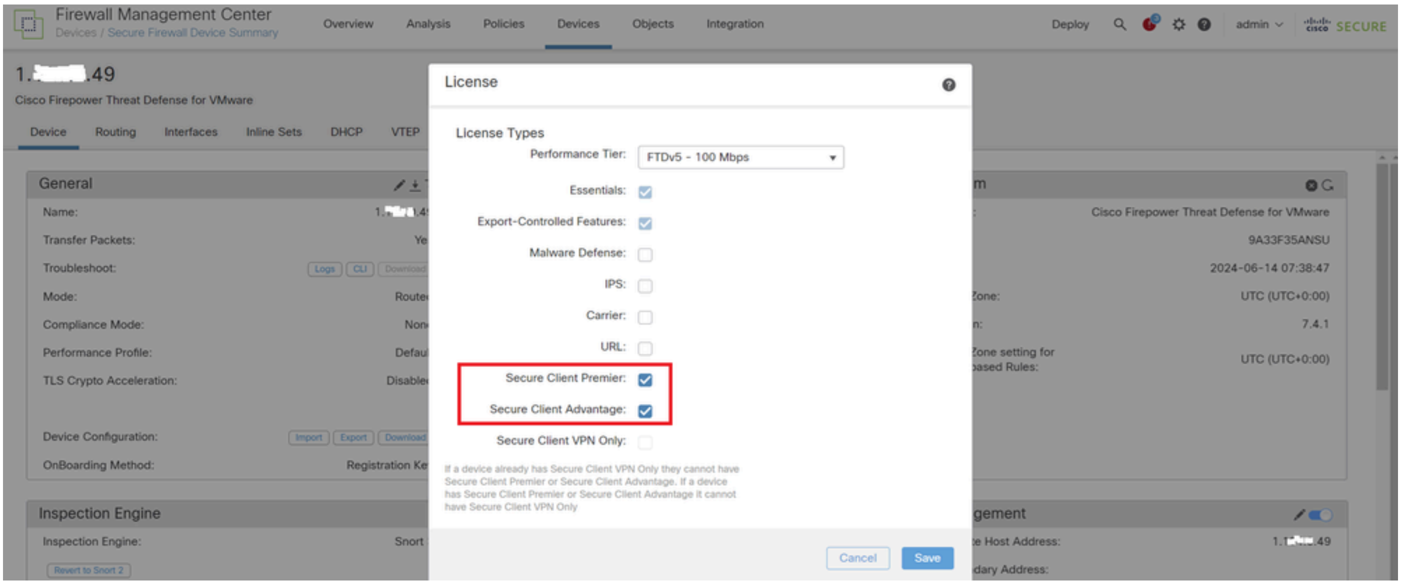
Cisco Firepower Threat Defense for VMware

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
GigabitEthernet0/1	inside	Physical	insideZone		192.168.10.200/24(Static)	Disabled	Global
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	

واجهة FTD

الخطوة 2. تأكيد ترخيص Cisco Secure Client

انتقل إلى الأجهزة > إدارة الأجهزة، وقم بتحرير جهاز FTD الهدف، وتأكيد ترخيص Cisco Secure Client في علامة التبويب الجهاز.



License

License Types

Performance Tier: FTDv5 - 100 Mbps

Essentials: ☑

Export-Controlled Features: ☑

Malware Defense: □

IPS: □

Carrier: □

URL: □

Secure Client Premier: ☑

Secure Client Advantage: ☑

Secure Client VPN Only: □

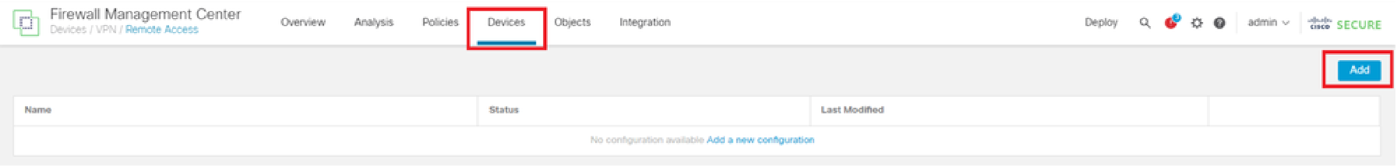
If a device already has Secure Client VPN Only they cannot have Secure Client Premier or Secure Client Advantage. If a device has Secure Client Premier or Secure Client Advantage it cannot have Secure Client VPN Only

Cancel | Save

ترخيص العميل الآمن

الخطوة 3. إضافة تعيين نهج

انتقل إلى الأجهزة > VPN > الوصول عن بعد، انقر فوق زر إضافة.

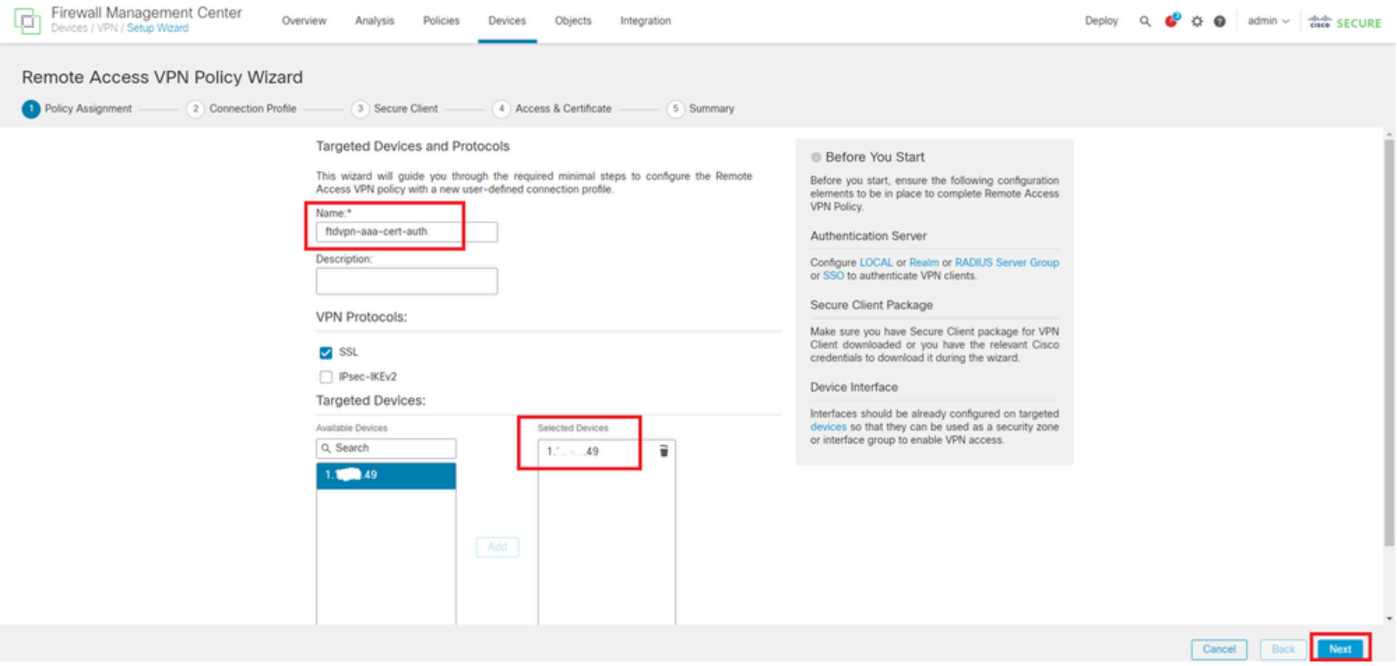


Name	Status	Last Modified
No configuration available Add a new configuration		

إضافة شبكة VPN للوصول عن بعد

أدخل المعلومات الضرورية وانقر فوق الزر التالي.

- الاسم: ftdvpn-aaa-cert-auth
- بروتوكولات VPN : SSL
- الأجهزة المستهدفة: 1.x.49



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:* ftdvpn-aaa-cert-auth

Description:

VPN Protocols:

☑ SSL

□ IPsec-IKEv2

Targeted Devices:

Available Devices: 1.[redacted].49

Selected Devices: 1.[redacted].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

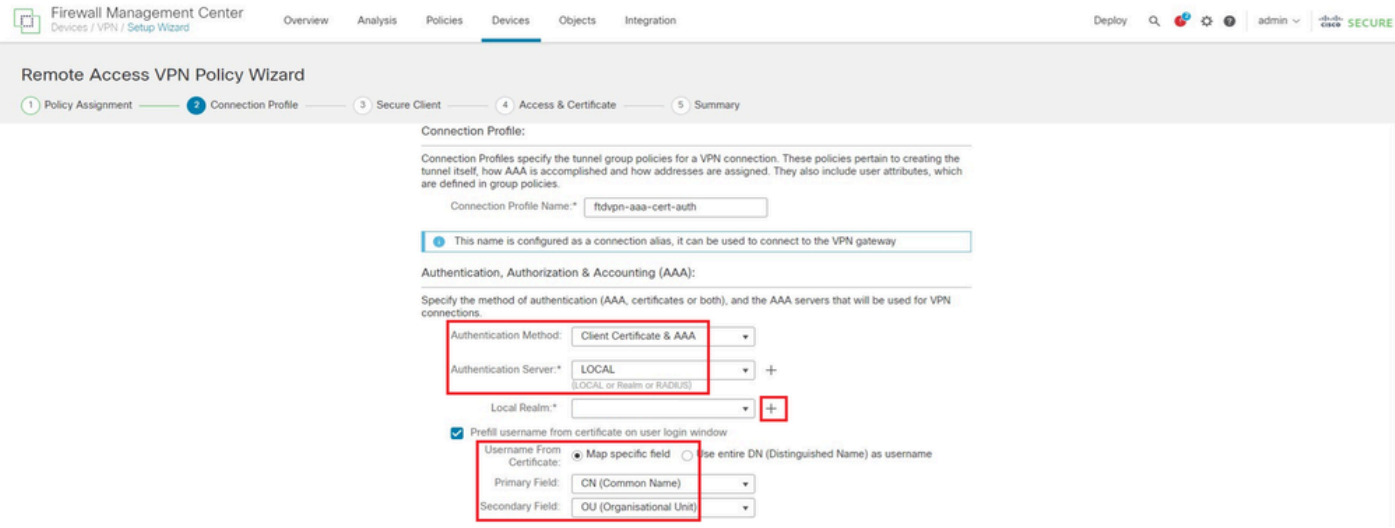
Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

تعيين النهج

الخطوة 4. تفاصيل التكوين لملف تعريف الاتصال

أدخل المعلومات الضرورية لملف تعريف الاتصال وانقر فوق + زر بجوار عنصر النطاق المحلي.

- أسلوب المصادقة: شهادة العميل و AAA
- خادم المصادقة: محلي
- اسم المستخدم من الشهادة: حقل تعيين محدد
- الحقل الأساسي: CN (الاسم الشائع)
- الحقل الثانوي: OU (الوحدة التنظيمية)



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:* ftdvpn-aaa-cert-auth

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

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: Client Certificate & AAA

Authentication Server:* LOCAL +
(LOCAL or Realm or RADIUS)

Local Realm:* +

☑ Prefill username from certificate on user login window

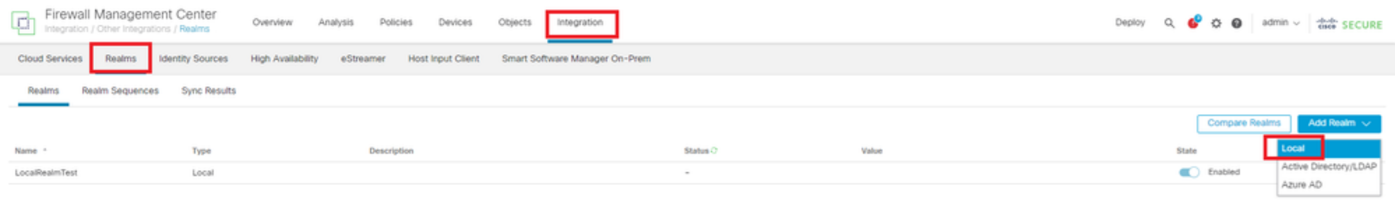
Username From Certificate: ● Map specific field ○ Use entire DN (Distinguished Name) as username

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

تفاصيل ملف تعريف الاتصال

انقر فوق محلي من القائمة المنسدلة إضافة حيز لإضافة نطاق محلي جديد.



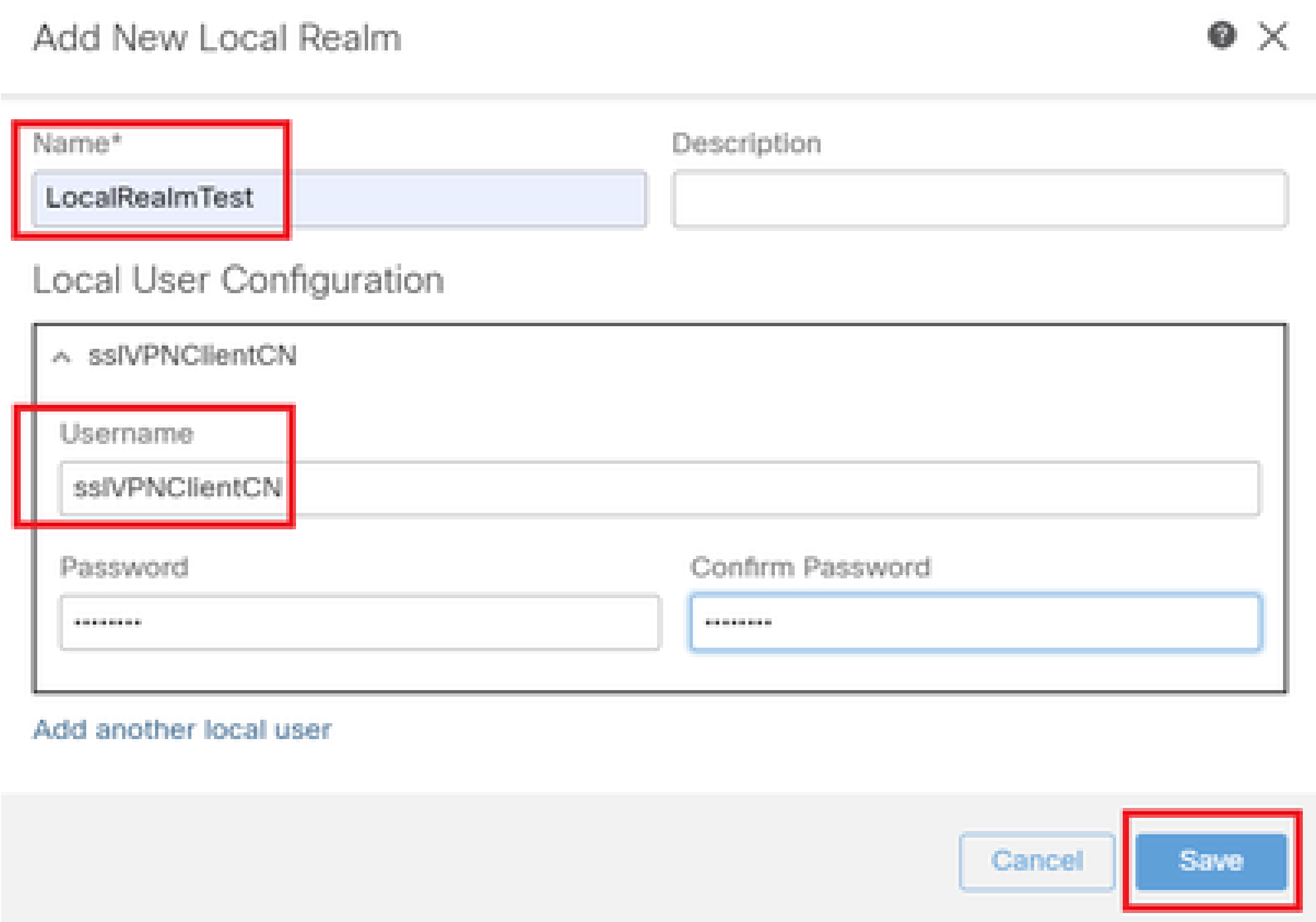
Name	Type	Description	Status	Value	State
LocalRealmTest	Local		-		Enabled

إضافة نطاق محلي

أدخل المعلومات الضرورية للحيز المحلي وانقر فوق زر حفظ.

- الاسم: LocalRealmTest
- اسم المستخدم: sslVPNClientCN

ملاحظة: اسم المستخدم يساوي الاسم الشائع داخل شهادة العميل



Add New Local Realm

Name*: LocalRealmTest

Description:

Local User Configuration

ssIVPNClientCN

Username: ssIVPNClientCN

Password: ·········

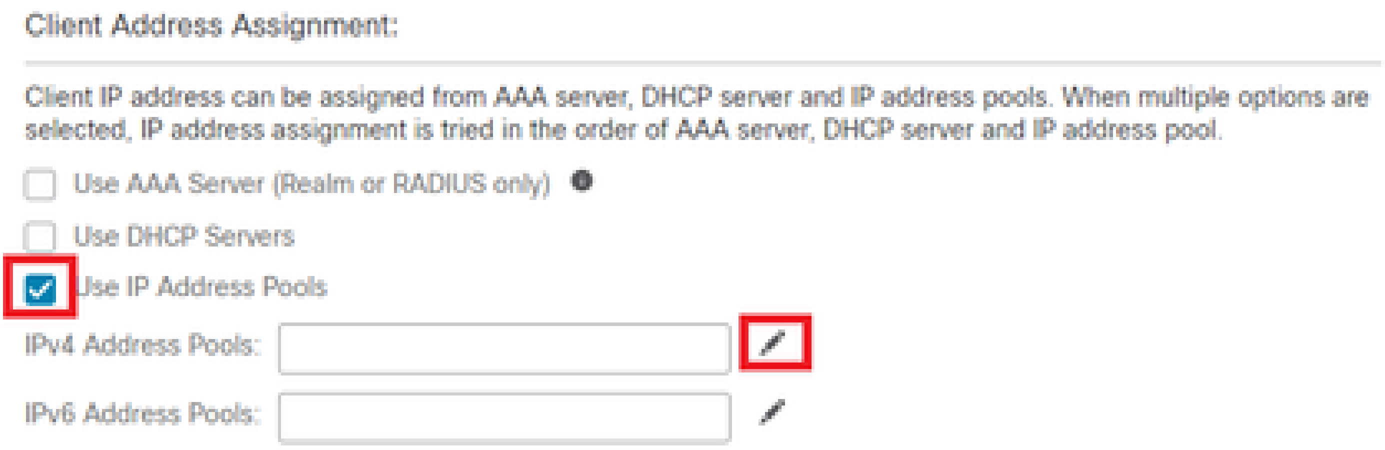
Confirm Password: ········

Add another local user

تفاصيل النطاق المحلي

الخطوة 5. إضافة تجمع عناوين لملف تعريف الاتصال

انقر فوق زر تحرير الموجود بجوار عنصر تجمعات عناوين IPv4.



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:

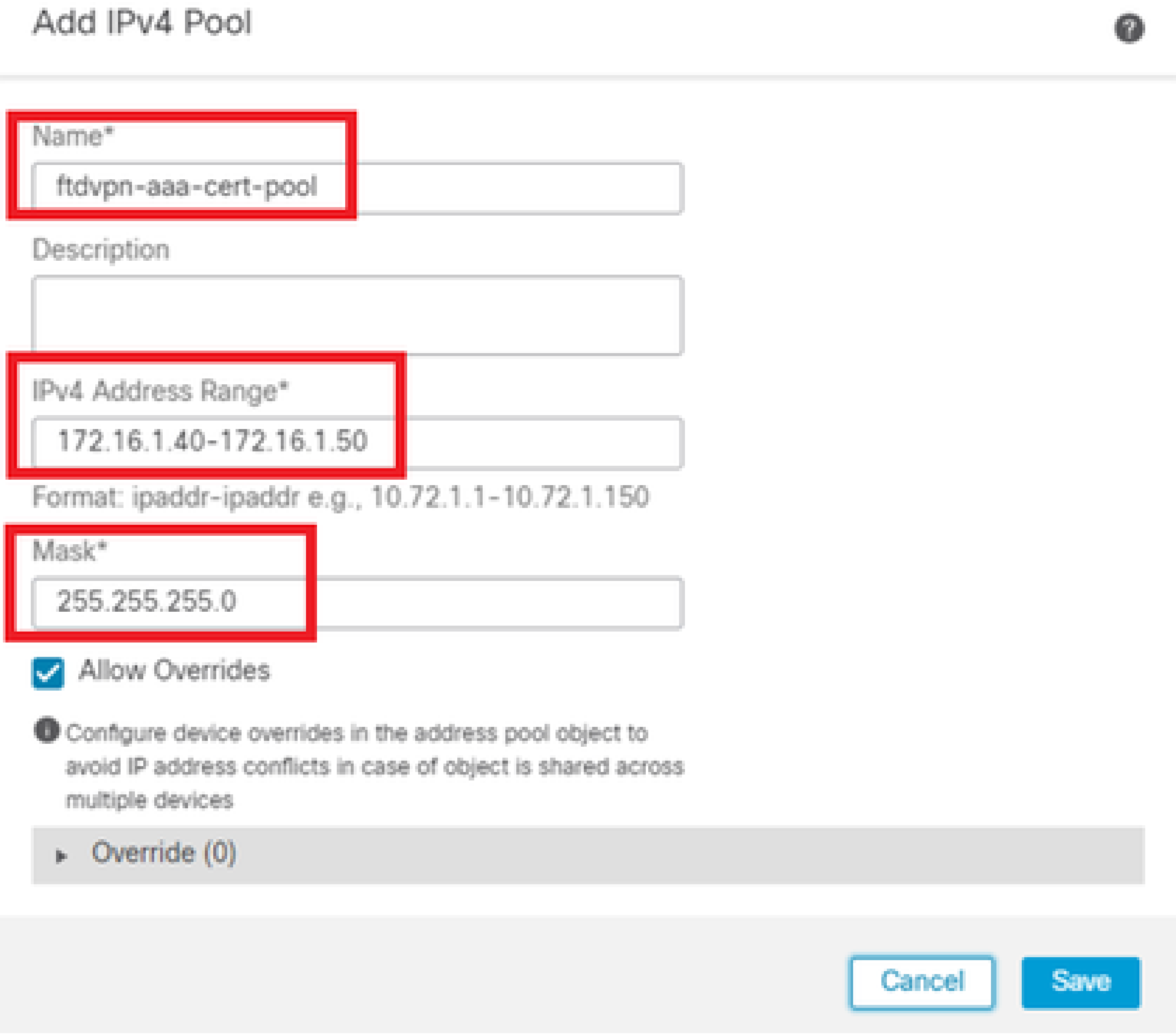
IPv6 Address Pools:

إضافة تجمع عناوين IPv4

أدخل المعلومات الضرورية لإضافة تجمع عناوين IPv4 جديد. حدد تجمع عناوين IPv4 الجديد لملف تعريف الاتصال.

- الاسم: ftdvpn-aaa-cert-pool
- نطاق عنوان IPv4: 172.16.1.40-172.16.1.50

- القناع: 255.255.255.0



Add IPv4 Pool

Name*
ftdvpn-aaa-cert-pool

Description

IPv4 Address Range*
172.16.1.40-172.16.1.50
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*
255.255.255.0

☑ Allow Overrides

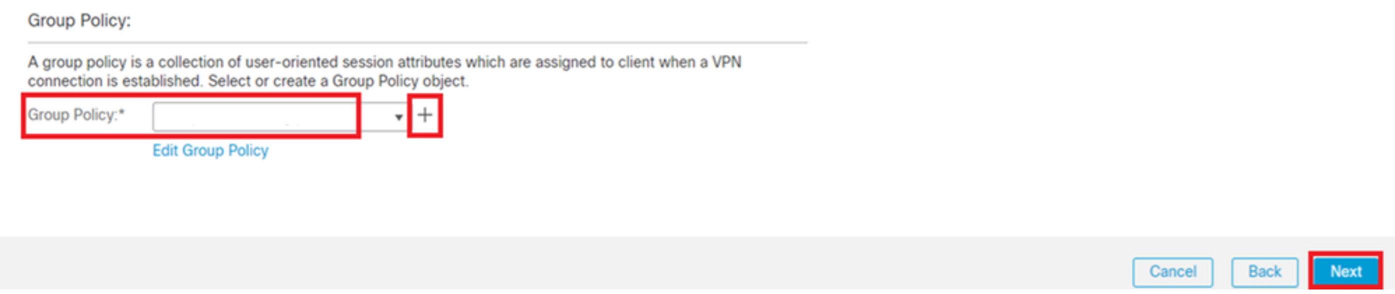
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▸ Override (0)

تفاصيل تجمع عناوين IPv4

الخطوة 6. إضافة نهج المجموعة لملف تعريف الاتصال

انقر فوق + زر بجوار عنصر نهج المجموعة.



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.

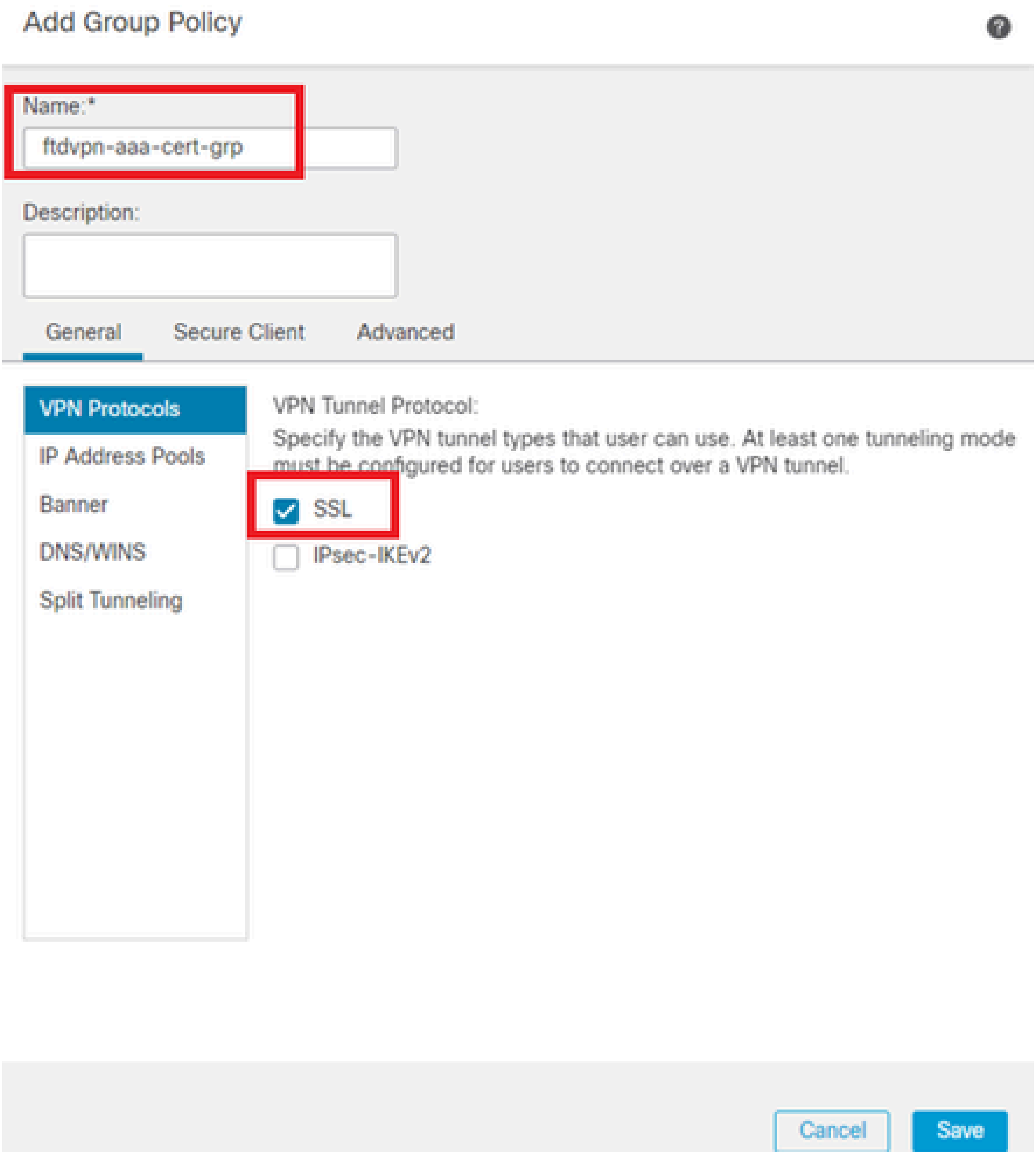
Group Policy:*

إضافة نهج المجموعة

قم بإدخال المعلومات الضرورية لإضافة نهج مجموعة جديد. حدد نهج المجموعة الجديد لملف

تعريف الاتصال.

- الاسم: ftdvpn-aaa-cert-grp
- بروتوكولات VPN : SSL



Add Group Policy

Name:* ftdvpn-aaa-cert-grp

Description:

VPN Tunnel Protocol:

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

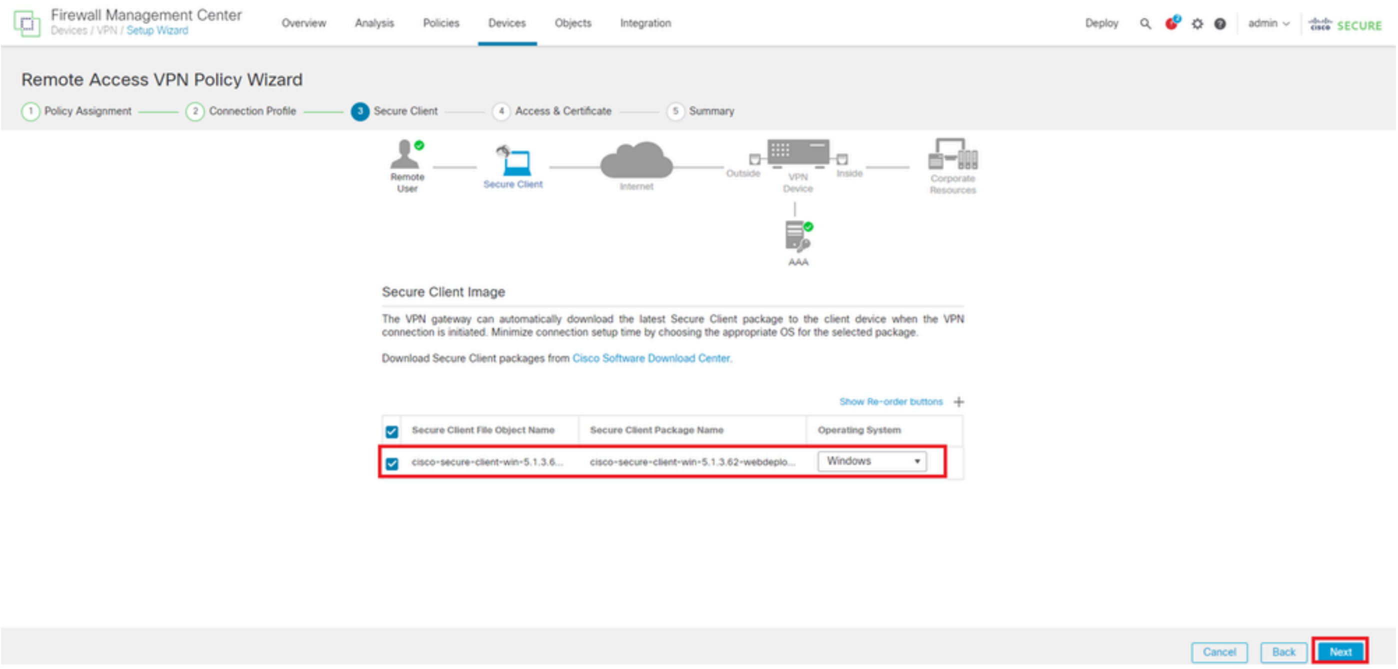
☑ SSL

□ IPsec-IKEv2

تفاصيل نهج المجموعة

الخطوة 7. تكوين صورة عميل آمنة لملف تعريف الاتصال

حدد ملف صورة عميل آمن وانقر فوق الزر التالي.



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
☑	cisco-secure-client-win-5.1.3.6...	cisco-secure-client-win-5.1.3.62-webdeplo...	Windows

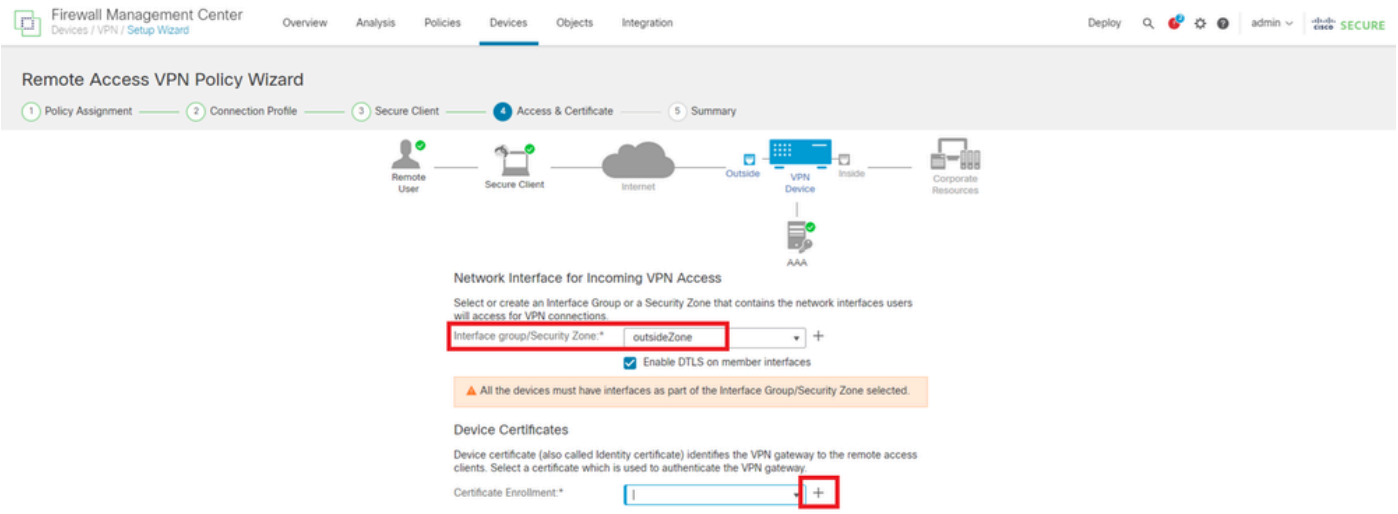
Cancel Back Next

تحديد صورة عميل آمنة

الخطوة 8. تكوين الوصول والشهادة لملف تعريف الاتصال

حدد منطقة الأمان لاتصال VPN وانقر فوق + زر بجوار صنف تسجيل الشهادة.

- مجموعة الواجهة/منطقة الأمان : خارج المنطقة



Remote Access VPN Policy Wizard

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

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* outsideZone +

☑ Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

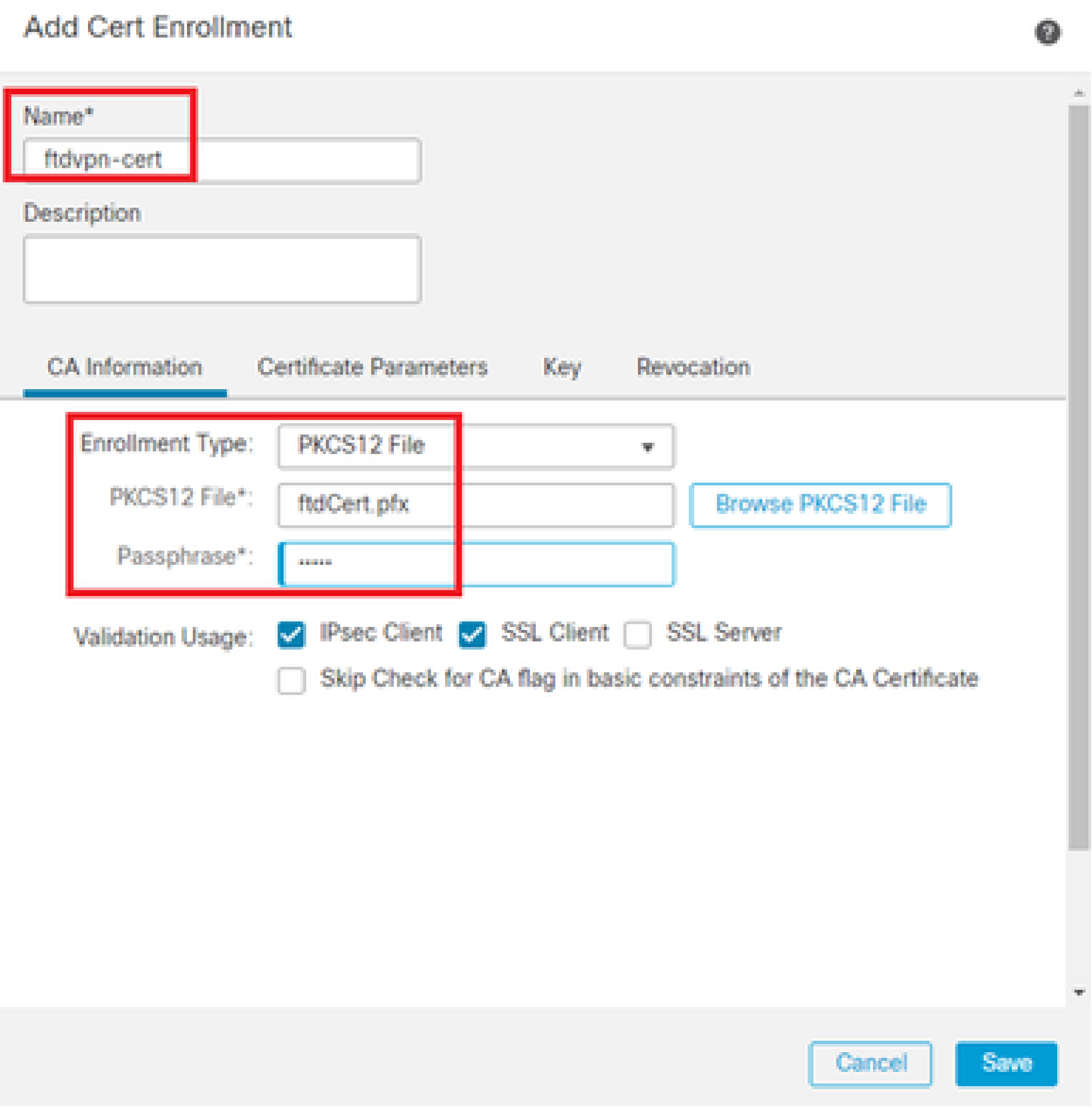
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

تحديد منطقة الأمان

قم بإدخال المعلومات الضرورية لشهادة FTD واستيراد ملف PKCS12 من حاسب محلي.

- الاسم: ftdvpn-cert
- نوع التسجيل: ملف PKCS12



Add Cert Enrollment

Name*

ftdvpn-cert

Description

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: ftdCert.pfx

Passphrase*: ......

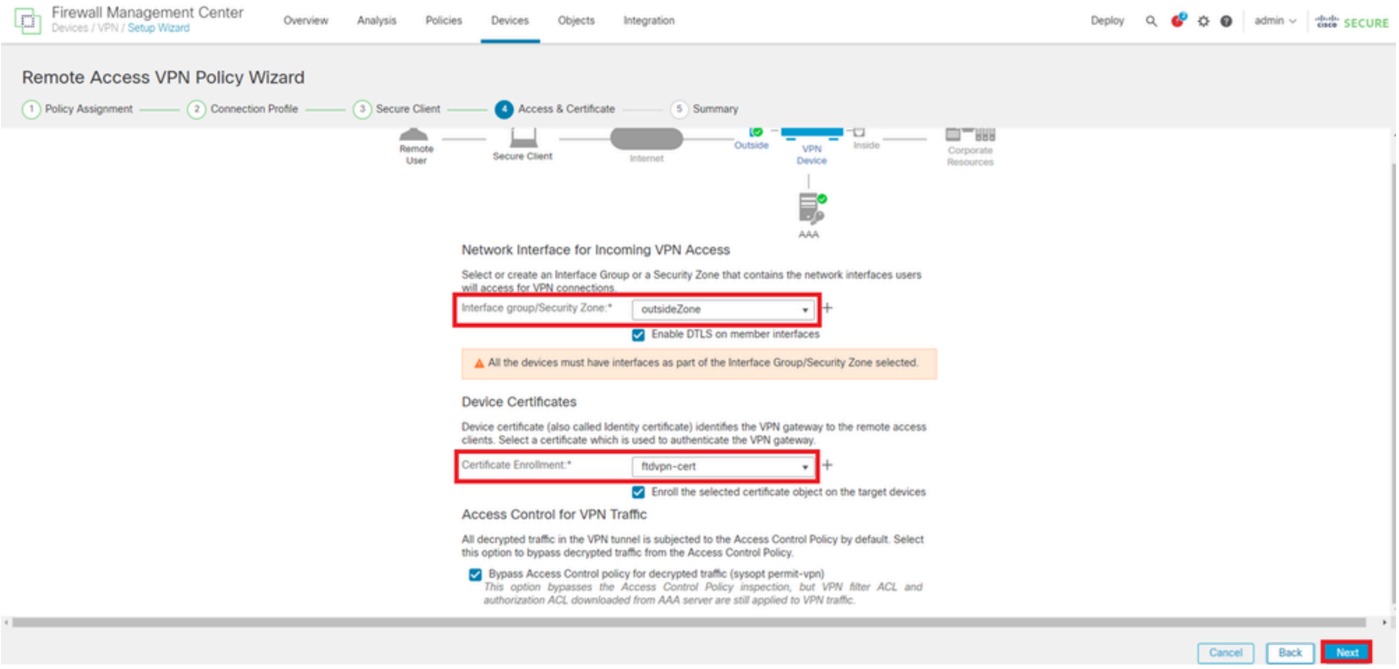
Validation Usage: ☑ IPsec Client ☑ SSL Client □ SSL Server

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

إضافة شهادة FTD

تأكد من المعلومات التي تم إدخالها في معالج الوصول والشهادة وانقر فوق التالي.

ملاحظة: تمكين سياسة التحكم في الوصول الالتفافي لحركة المرور التي تم فك تشفيرها (sysopt allowed-vpn)، حتى لا تخضع حركة مرور VPN التي تم فك تشفيرها إلى فحص سياسة التحكم في الوصول.



Remote Access VPN Policy Wizard

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

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* outsideZone

☑ Enable DTLS on member interfaces

All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* ftdvpn-cert

☑ Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

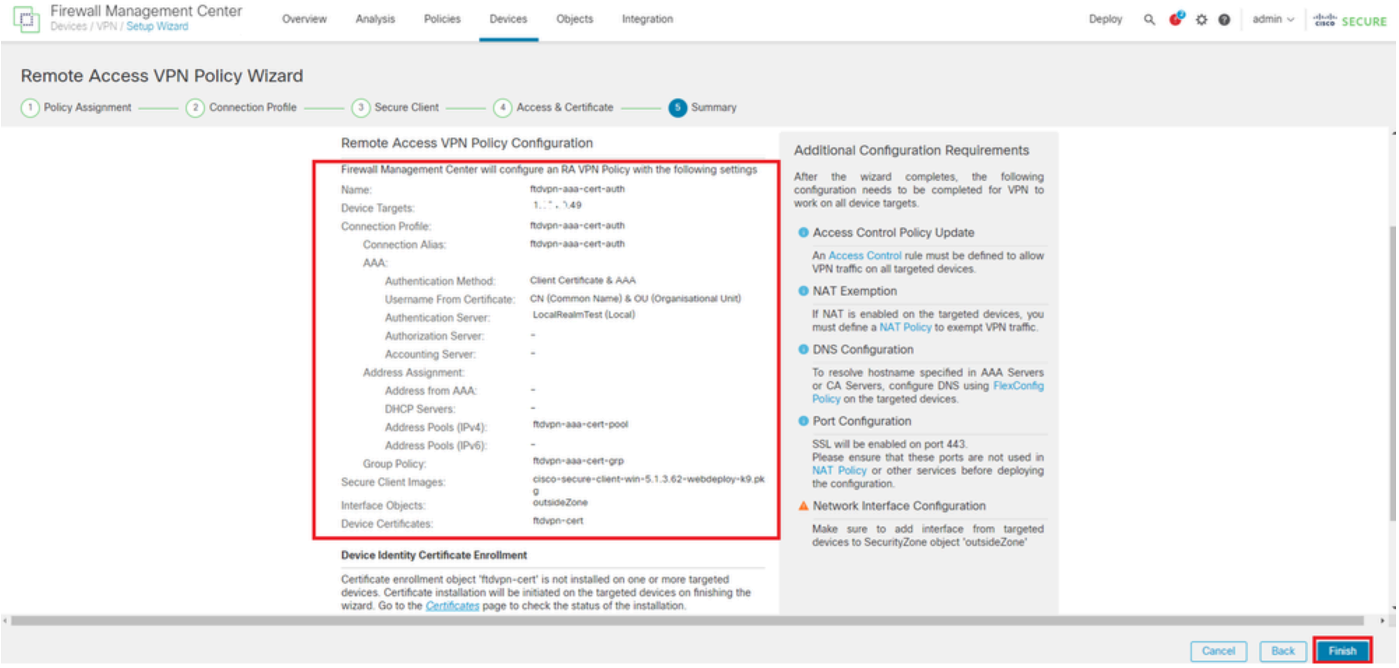
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

☑ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

تأكيد الإعدادات في Access & Certificate

الخطوة 9. تأكيد الملخص لملف تعريف الاتصال

أكدت المعلومة دخلت ل VPN توصيل وطقطقة إنجاز زر.



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:	ftdvpn-aaa-cert-auth
Device Targets:	1.[redacted].49
Connection Profile:	ftdvpn-aaa-cert-auth
Connection Alias:	ftdvpn-aaa-cert-auth
AAA:	
Authentication Method:	Client Certificate & AAA
Username From Certificate:	CN (Common Name) & OU (Organisational Unit)
Authentication Server:	LocalRealmTest (Local)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	ftdvpn-aaa-cert-pool
Address Pools (IPv6):	-
Group Policy:	ftdvpn-aaa-cert-grp
Secure Client Images:	cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg
Interface Objects:	outsideZone
Device Certificates:	ftdvpn-cert

Device Identity Certificate Enrollment

Certificate enrollment object 'ftdvpn-cert' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the Certificates page to check the status of the installation.

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

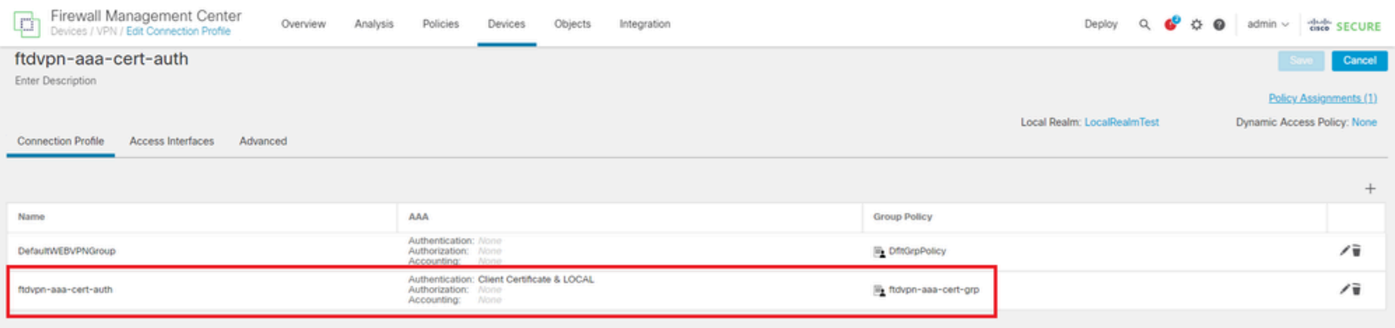
SSL will be enabled on port 443.
Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

Network Interface Configuration

Make sure to add interface from targeted devices to SecurityZone object 'outsideZone'

تأكيد إعدادات اتصال VPN

تأكيد ملخص نهج VPN للوصول عن بعد ونشر الإعدادات على FTD.



ftdvpn-aaa-cert-auth

Enter Description

Local Realm: LocalRealmTest

Dynamic Access Policy: None

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
ftdvpn-aaa-cert-auth	Authentication: Client Certificate & LOCAL Authorization: None Accounting: None	ftdvpn-aaa-cert-grp

ملخص نهج VPN للوصول عن بعد

التأكيد في واجهة سطر الأوامر (CLI) الخاصة ب FTD

تأكيد إعدادات اتصال VPN في FTD CLI بعد النشر من FMC.

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0
interface GigabitEthernet0/1
nameif inside
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0

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

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
keypair ftdvpn-cert
crl configure

// Server Certificate Chain
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
......
quit
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
```

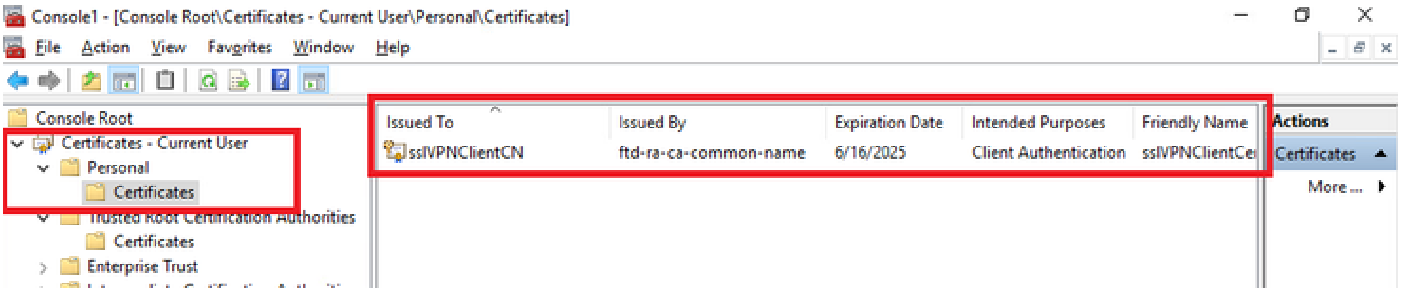
```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
banner none
wins-server none
dns-server none
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
```

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

تأكيد في عميل شبكة VPN

الخطوة 1. تأكيد شهادة العميل

انتقل إلى الشهادات - المستخدم الحالي > شخصي > شهادات، تحقق من شهادة العميل المستخدمة للمصادقة.



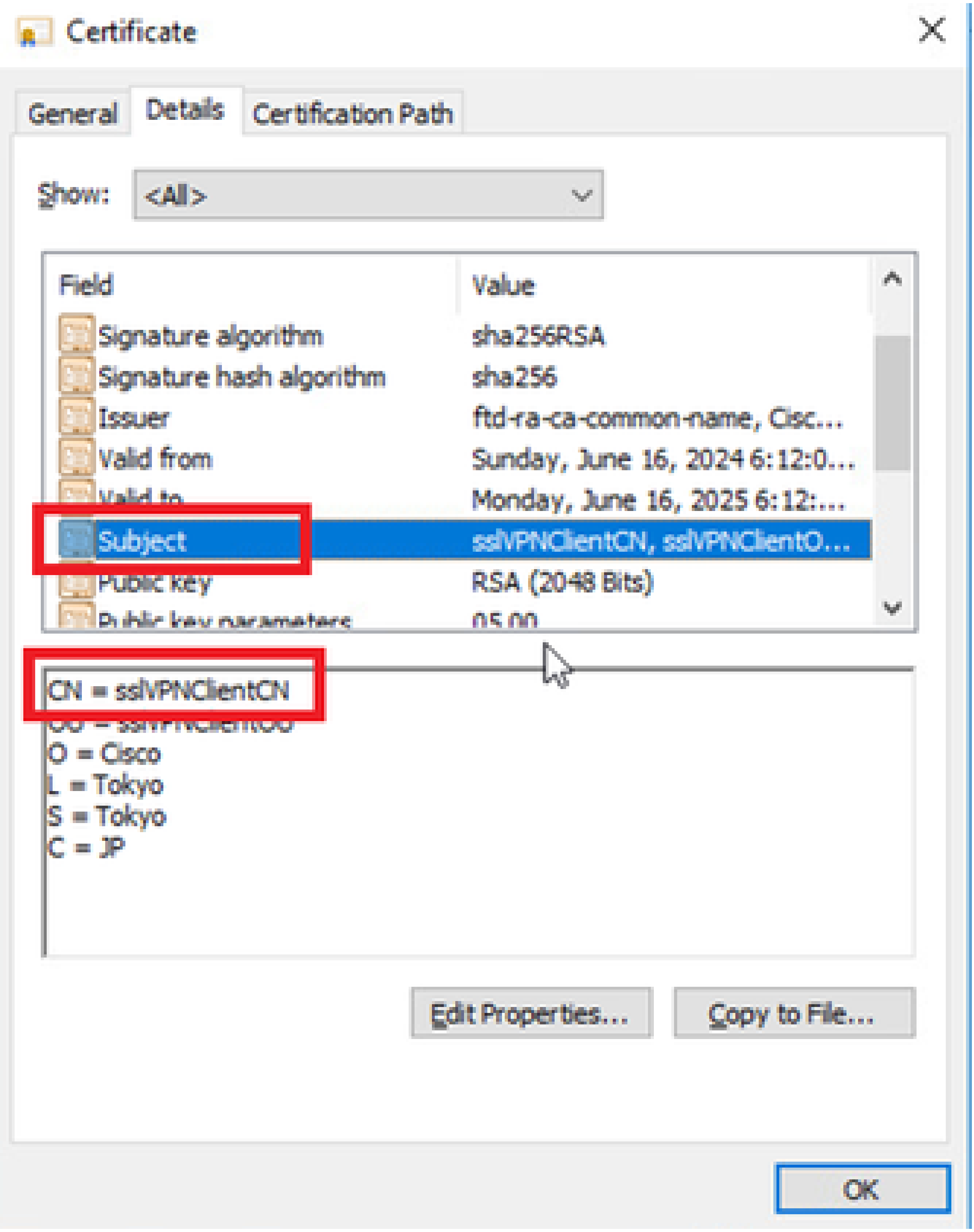
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
sslVPNClientCN	ftd-ra-ca-common-name	6/16/2025	Client Authentication	sslVPNClientCe

تأكيد شهادة العميل

انقر نقرا مزدوجا فوق شهادة العميل، ثم انتقل إلى التفاصيل، ثم تحقق من تفاصيل الموضوع.

- الموضوع: CN = sslVPNClientCN



Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ftd-ra-ca-common-name, Cisc...
Valid from	Sunday, June 16, 2024 6:12:0...
Valid to	Monday, June 16, 2025 6:12:...
Subject	sslVPNClientCN, sslVPNClientO...
Public key	RSA (2048 Bits)
Public key parameters	05 00

```
CN = sslVPNClientCN
OU = sslVPNClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP
```

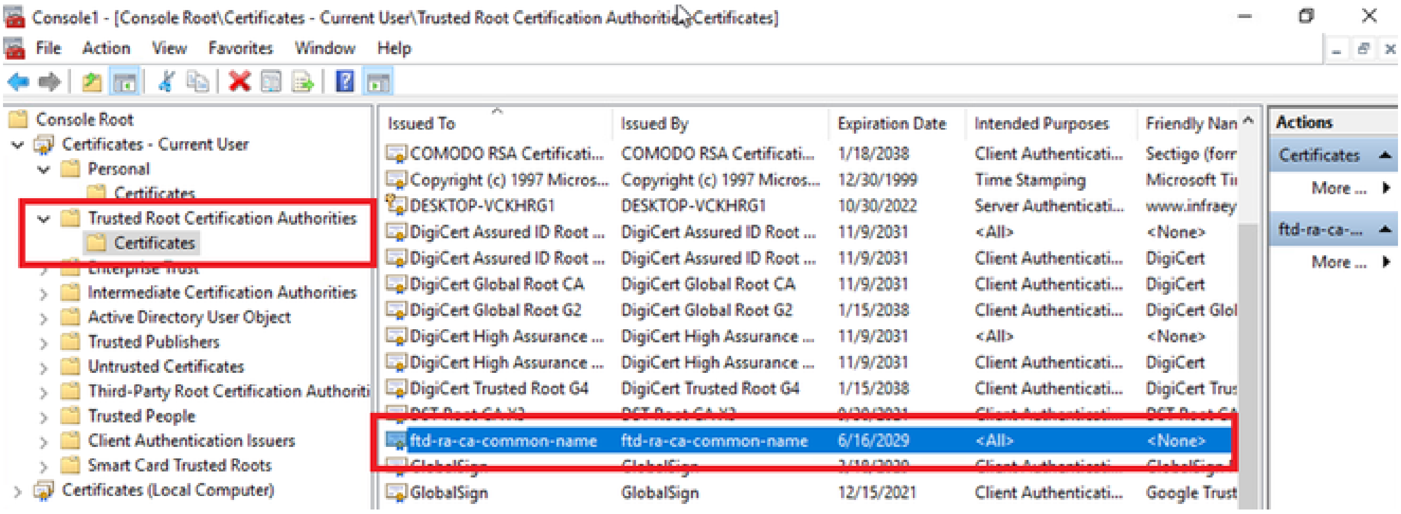
تفاصيل شهادة العميل

الخطوة 2. تأكيد CA

انتقل إلى الشهادات - المستخدم الحالي > مراجع التصديق الجذر الموثوق بها > الشهادات،

تحقق من المرجع المصدق المستخدم للمصادقة.

- صدر عن : ftd-ra-ca-common-name


Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots
Certificates (Local Computer)
Actions
Certificates
More ...
ftd-ra-ca-...
More ...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan
COMODO RSA Certificati...	COMODO RSA Certificati...	1/18/2038	Client Authenticati...	Sectigo (forr
Copyright (c) 1997 Micros...	Copyright (c) 1997 Micros...	12/30/1999	Time Stamping	Microsoft Ti
DESKTOP-VCKHRG1	DESKTOP-VCKHRG1	10/30/2022	Server Authenticati...	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 Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Glol
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	<All>	<None>
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	Client Authenticati...	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati...	DigiCert Trus
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...	DST Root CA
ftd-ra-ca-common-name	ftd-ra-ca-common-name	6/16/2029	<All>	<None>
GlobalSign	GlobalSign	3/18/2029	Client Authenticati...	GlobalSign
GlobalSign	GlobalSign	12/15/2021	Client Authenticati...	Google Trust

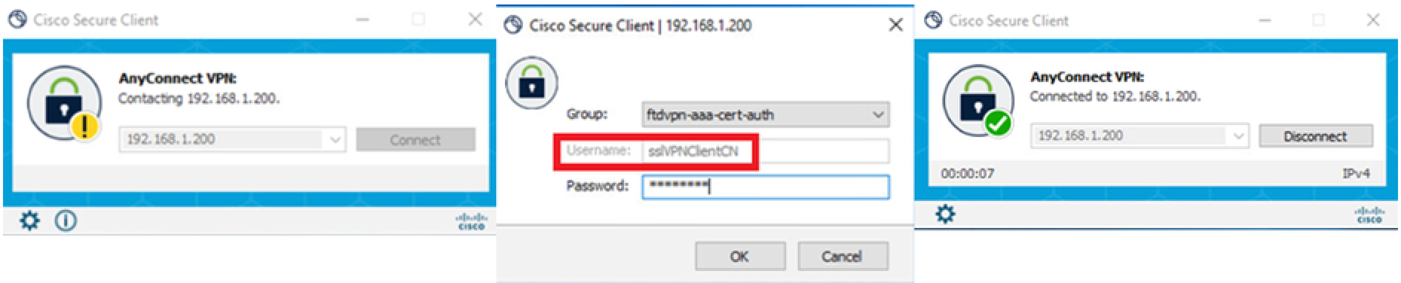
تأكيد CA

التحقق من الصحة

الخطوة 1. بدء اتصال VPN

على نقطة النهاية، ابدأ اتصال Cisco Secure Client. استخرجت ال username من الزبون شهادة، أنت تحتاج أن يدخل الكلمة ل VPN صحة هوية.

ملاحظة: يتم إستخراج اسم المستخدم من حقل CN (الاسم الشائع) لشهادة العميل في هذا المستند.


Cisco Secure Client

AnyConnect VPN:
Contacting 192.168.1.200.

192.168.1.200

Cisco Secure Client | 192.168.1.200

Group: ftdvpn-aaa-cert-auth

Username: sslVPNClientCN

Password: ********

Cisco Secure Client

AnyConnect VPN:
Connected to 192.168.1.200.

192.168.1.200

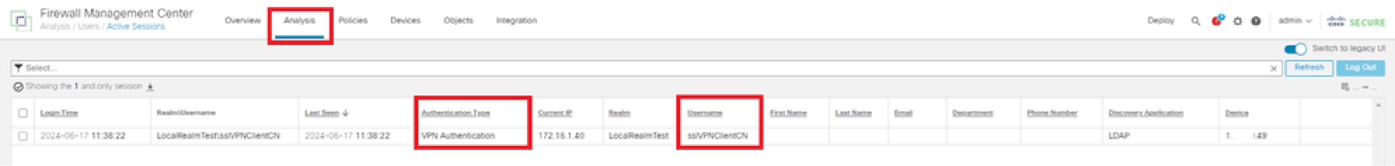
00:00:07

IPv4

بدء اتصال VPN

الخطوة 2. تأكيد الجلسات النشطة في FMC

انتقل إلى تحليل > مستخدمون > جلسات عمل نشطة، تحقق من الجلسة النشطة لمصادقة VPN.



☐	Login Time	Realm\Username	Last Seen ↓	Authentication Type	Current IP	Realm	Username	First Name	Last Name	Email	Department	Phone Number	Discovery Application	Device
☐	2024-06-17 11:38:22	LocalRealmTest\sslVPNClientCN	2024-06-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	sslVPNClientCN						LDAP	1. .49

تأكيد جلسة العمل النشطة

الخطوة 3. تأكيد جلسة VPN في FTD CLI

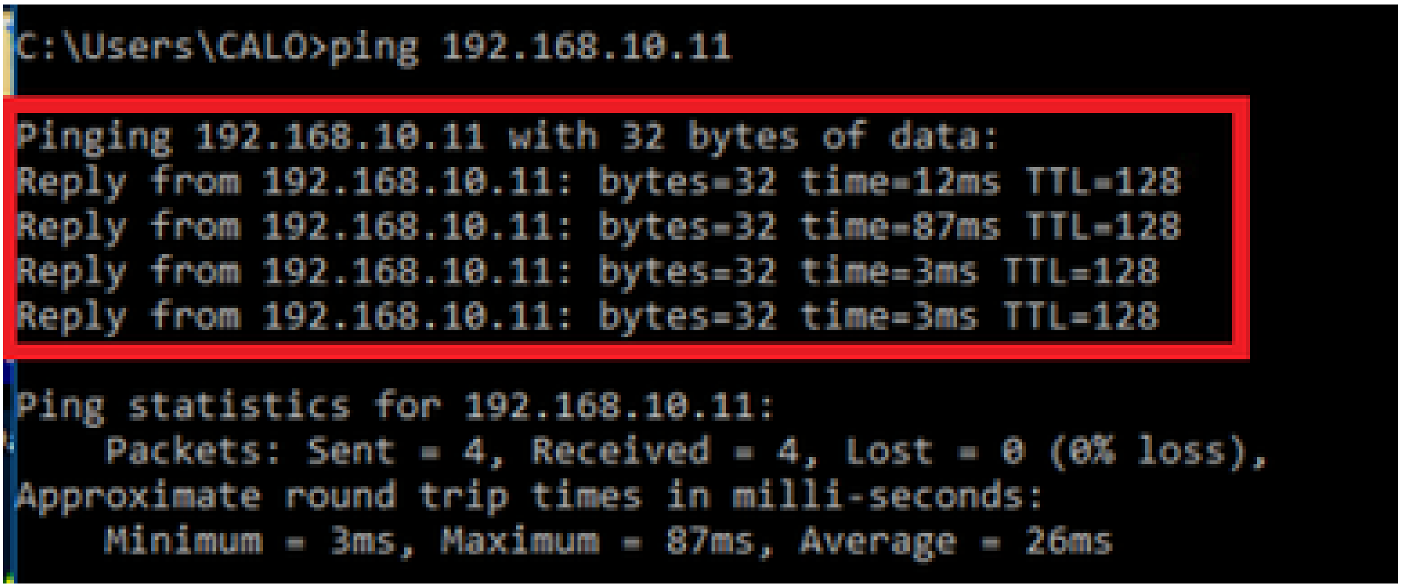
شغلshow vpn-sessiondb detail anyconnect أمر في FTD (Lina) CLI أن دكؤي لا VPN جلسة.

```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000700066 6fa19e
Security Grp : none Tunnel Zone : 0

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

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

SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
```

```
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 2292
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

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

الخطوة 4. تأكيد الاتصال بالخادم

ابدأ إختبار الاتصال من عميل الشبكة الخاصة الظاهرية (VPN) إلى الخادم، وتأكد من نجاح الاتصال بين عميل الشبكة الخاصة الظاهرية (VPN) والخادم.



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

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=12ms TTL=128
Reply from 192.168.10.11: bytes=32 time=87ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 87ms, Average = 26ms
```

نجح إختبار الاتصال

قم بتشغيل capture in interface inside real-time الأمر في FTD (Lina) CLI لتأكيد التقاط الحزمة.

<#root>

```
ftd702#

capture in interface inside real-time


Use ctrl-c to terminate real-time capture

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

استكشاف الأخطاء وإصلاحها

يمكنك توقع العثور على معلومات حول مصادقة VPN في Debug syslog لمحرك Lina وفي ملف DART على جهاز كمبيوتر Windows.

هذا مثال على سجلات تصحيح الأخطاء في محرك Lina.

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

// Extract username from the CN (Common Name) field
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested.  [Request 5]
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed.  [Request 5]

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

يمكن تشغيل هذه الأخطاء من واجهة سطر الأوامر (CLI) التشخيصية ل FTD، والتي توفر معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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

المرجع

تكوين AnyConnect Remote Access VPN على FTD

تكوين المصادقة المستندة إلى شهادة AnyConnect للوصول أثناء التنقل

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية
والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم
بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما
هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco
Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى
المستند الإنجليزي الأصلي (الرابط متوفر).