تكوين تعيين CERT لمصادقة العميل الآمنة على FTD عبر FMC

المحتويات

المقدمة

يوضح هذه المستند كيفية إعداد Cisco Secure Client مع SSL على FTD عبر FMC باستخدام تعيين الشهادة للمصادقة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة FireSIGHT (FMC) من Cisco
- الدفاع ضد تهديد جدار الحماية (FTD) الظاهري
- 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

تخطيط الشهادة هي طريقة تستخدم في إتصالات VPN حيث يتم تعيين شهادة عميل على حساب مستخدم محلي، أو يتم إستخدام السمات داخل الشهادة لأغراض التخويل.هذه عملية يتم فيها إستخدام الشهادة الرقمية كوسيلة لتعريف مستخدم أو جهاز. باستخدام تعيين الشهادة، فإنه يستغل بروتوكول SSL لمصادقة المستخدمين دون الحاجة إلى إدخال بيانات الاعتماد.

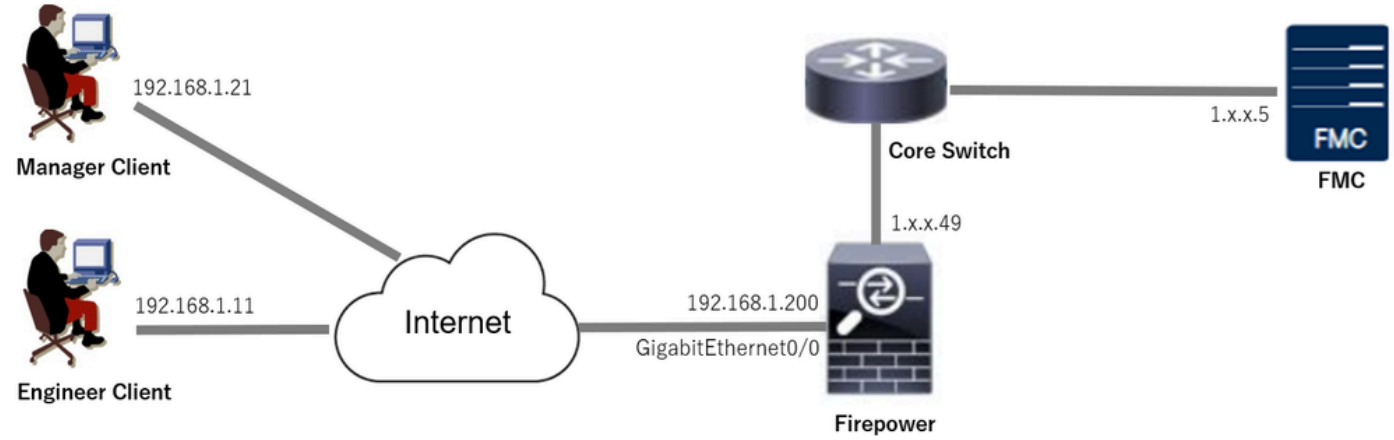
يوضح هذا المستند كيفية مصادقة عميل Cisco الآمن باستخدام الاسم الشائع من شهادة SSL.

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

- ك أ: ftd-ra-ca-name الشائع
- شهادة عميل شبكة VPN للمهندس: vpnEngineerClientCN
- شهادة عميل Manager VPN: vpnManagerClientCN
- شهادة الخادم: 192.168.1.200

الرسم التخطيطي للشبكة

تعرض هذه الصورة المخطط الذي يتم إستخدامه لمثال هذا المستند.



الرسم التخطيطي للشبكة

التكوينات

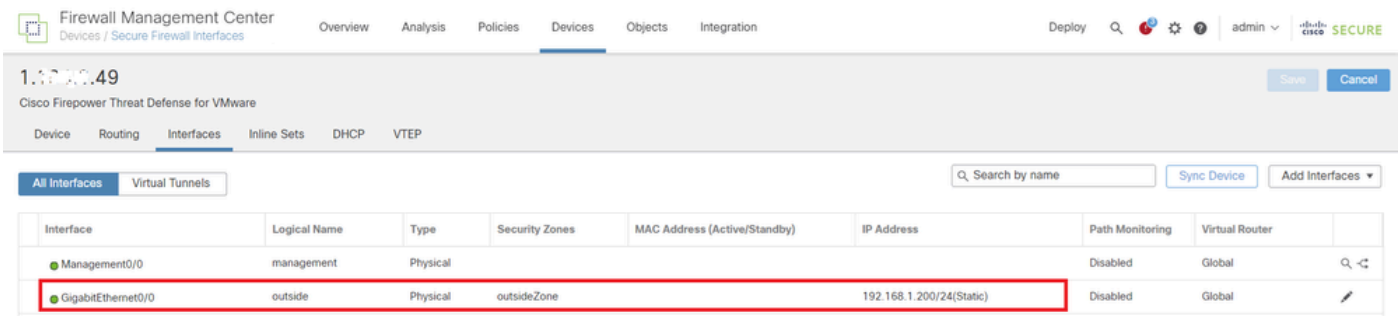
التكوين في FMC

الخطوة 1. تكوين واجهة FTD

انتقل إلى الأجهزة > إدارة الأجهزة، وحرر جهاز FTD الهدف، وقم بتكوين الواجهة الخارجية ل FTD inInterfacestab.

ل GigabitEthernet0/0،

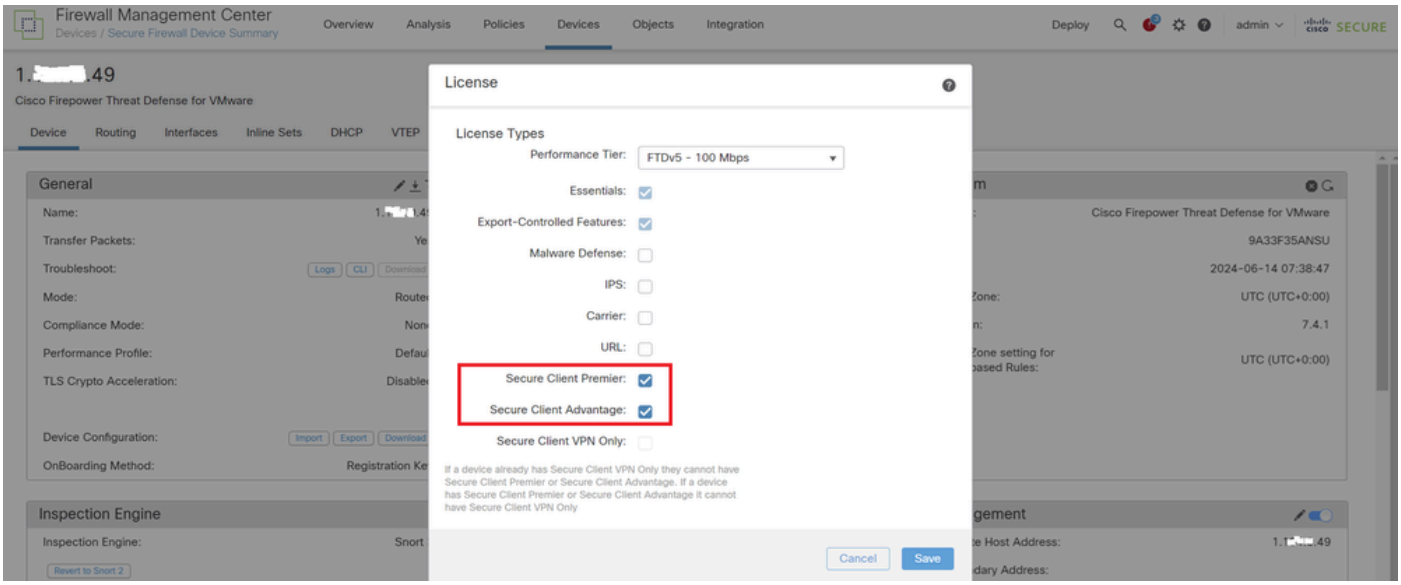
- الاسم: خارج
- المنطقة الأمنية: خارج المنطقة
- عنوان IP: 192.168.1.200/24



واجهة FTD

الخطوة 2. تأكيد ترخيص Cisco Secure Client

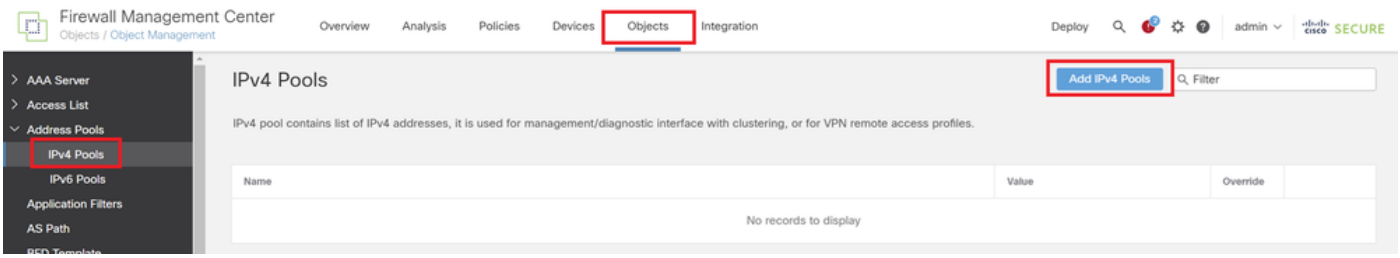
انتقل إلى الأجهزة > إدارة الأجهزة، وحرر جهاز FTD الهدف، وتأكد من ترخيص Cisco Secure Client في DeviceTab.



ترخيص العميل الآمن

الخطوة 3. إضافة تجمع عناوين IPv4

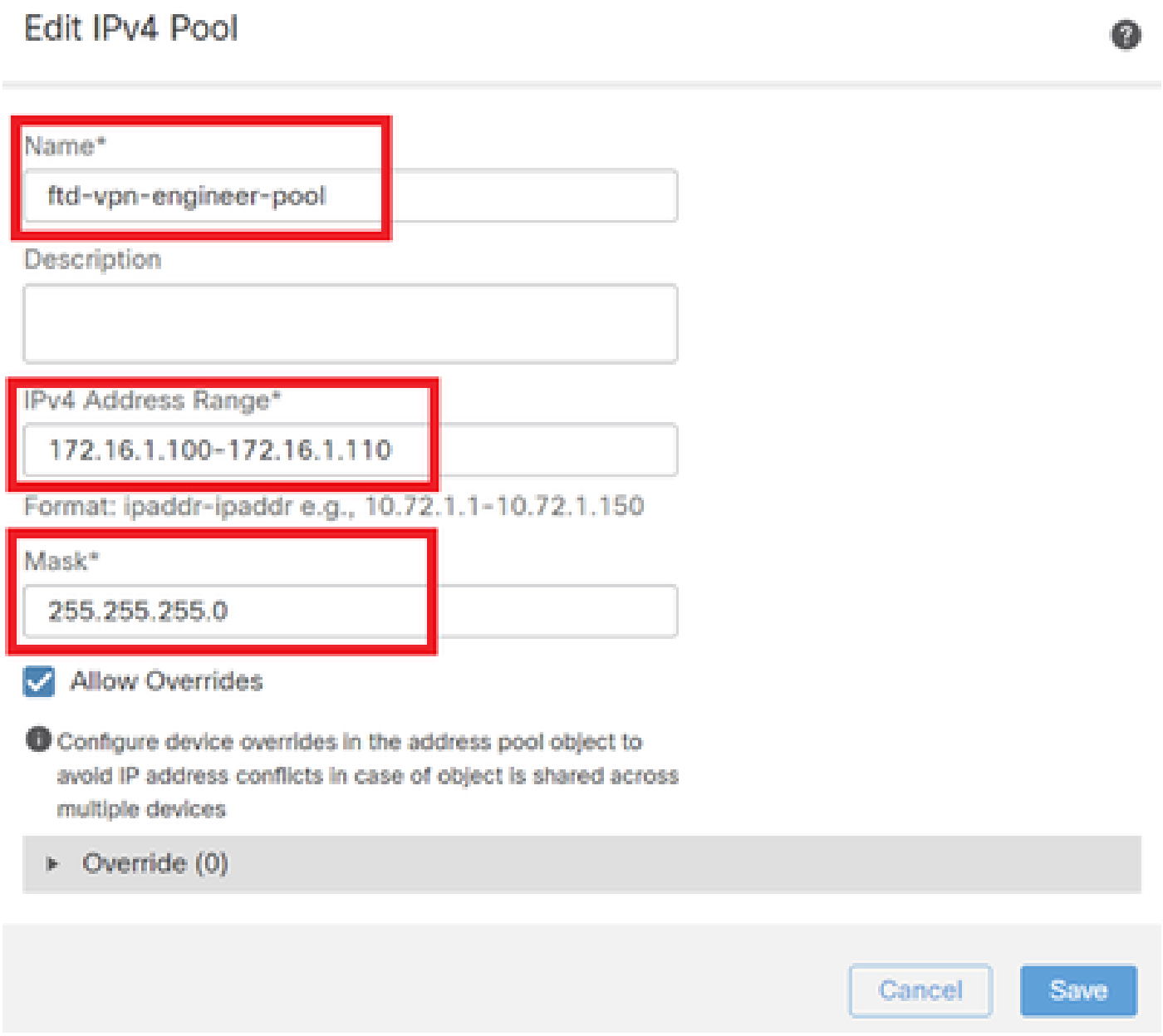
انتقل إلى Object > إدارة الكائن > تجمعات العناوين > تجمعات IPv4، انقر فوق الزر إضافة حزم IPv4.



إضافة تجمع عناوين IPv4

قم بإدخال المعلومات الضرورية لإنشاء تجمع عناوين IPv4 لعميل VPN للمهندس.

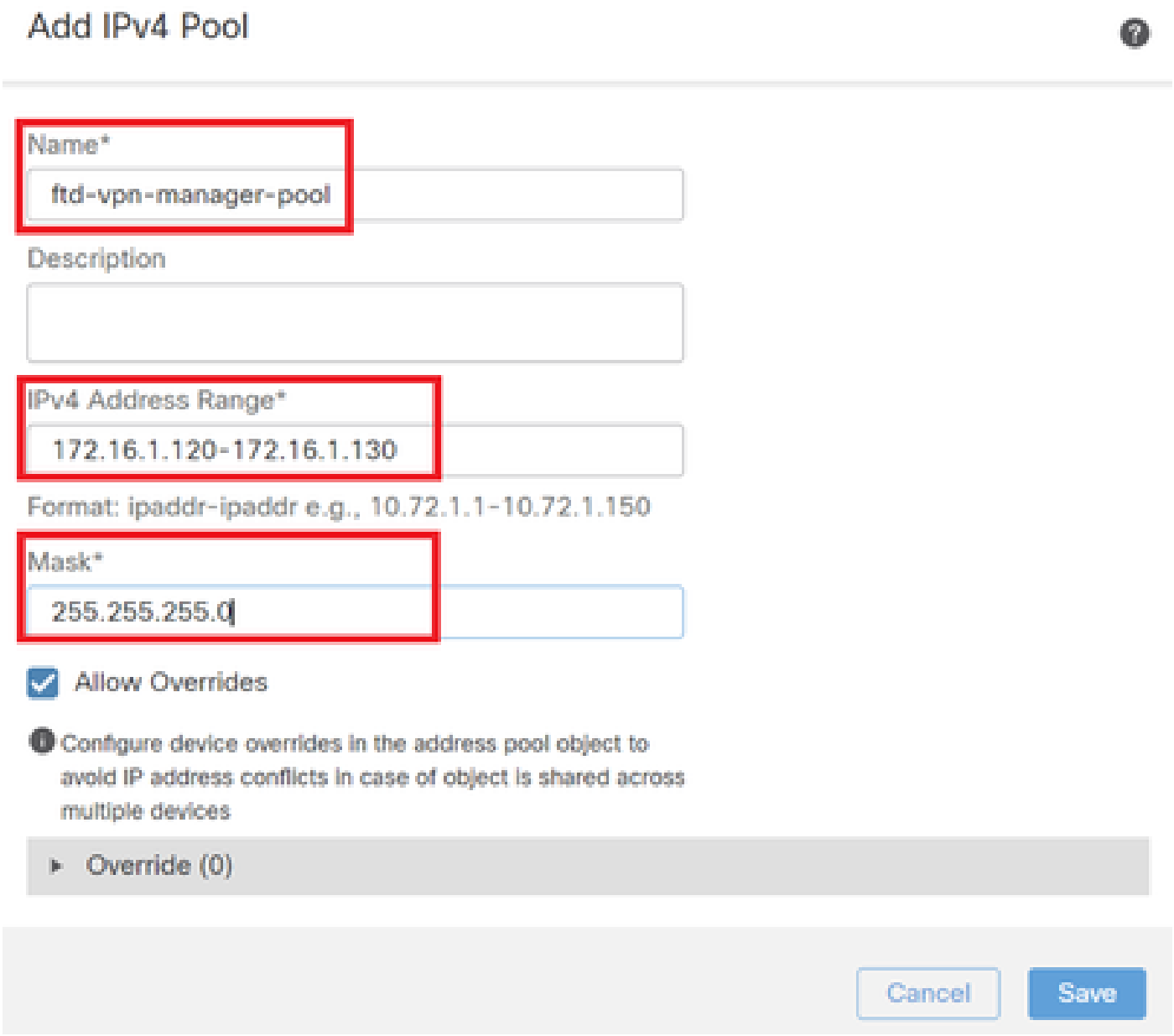
- الاسم: ftd-vpn-engineer-pool
- نطاق عنوان IPv4: 172.16.1.100-172.16.1.110
- القناع: 255.255.255.0



تجمع عناوين IPv4 لعميل VPN للمهندس

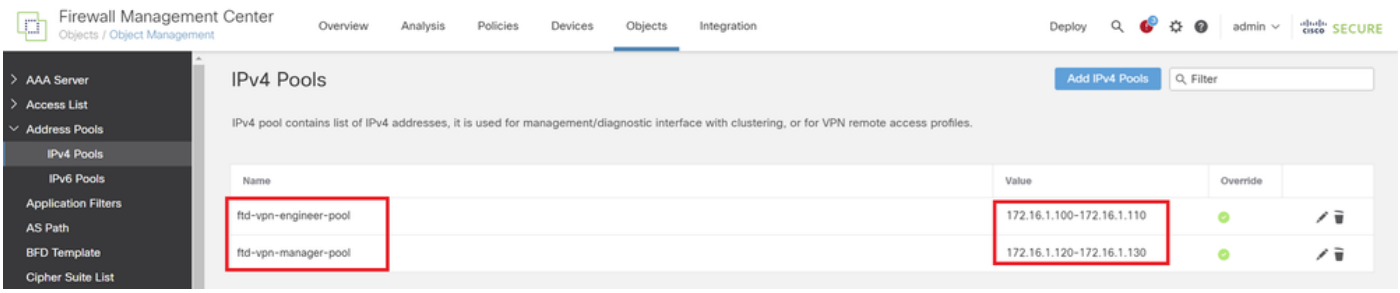
أدخل المعلومات الضرورية لإنشاء تجمع عناوين IPv4 لعميل VPN الخاص بالمدير.

- الاسم: ftd-vpn-manager-pool
- نطاق عناوين IPv4: 172.16.1.120-172.16.1.130
- القناع: 255.255.255.0



تجمع عناوين IPv4 لعميل VPN للمدير

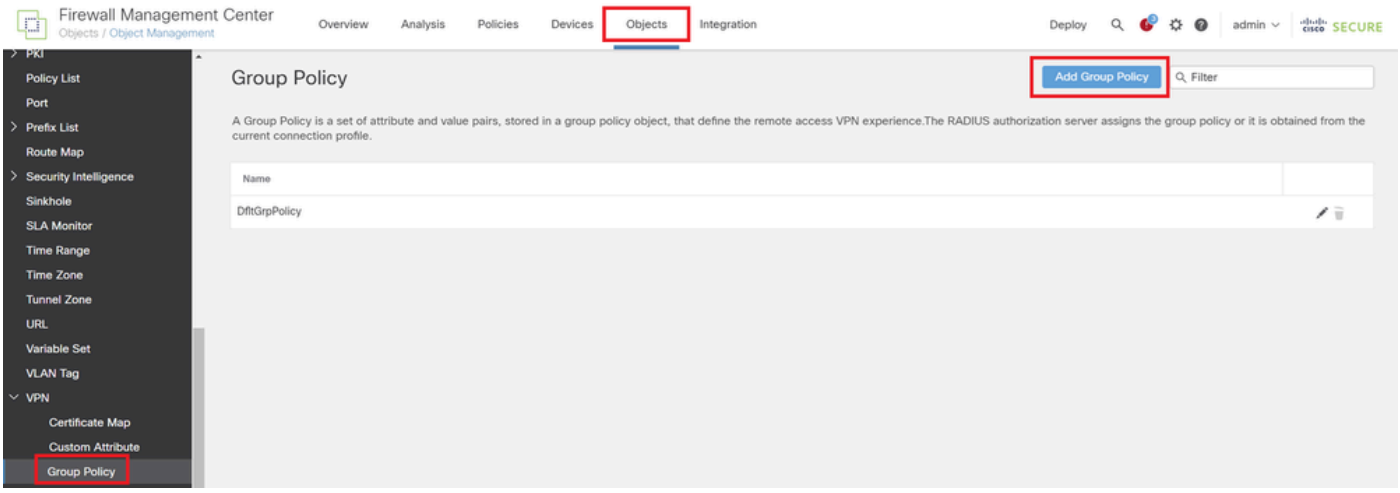
تأكيد تجمعات عناوين IPv4 الجديدة.



مجموعات عناوين IPv4 الجديدة

الخطوة 4. إضافة نمج المجموعة

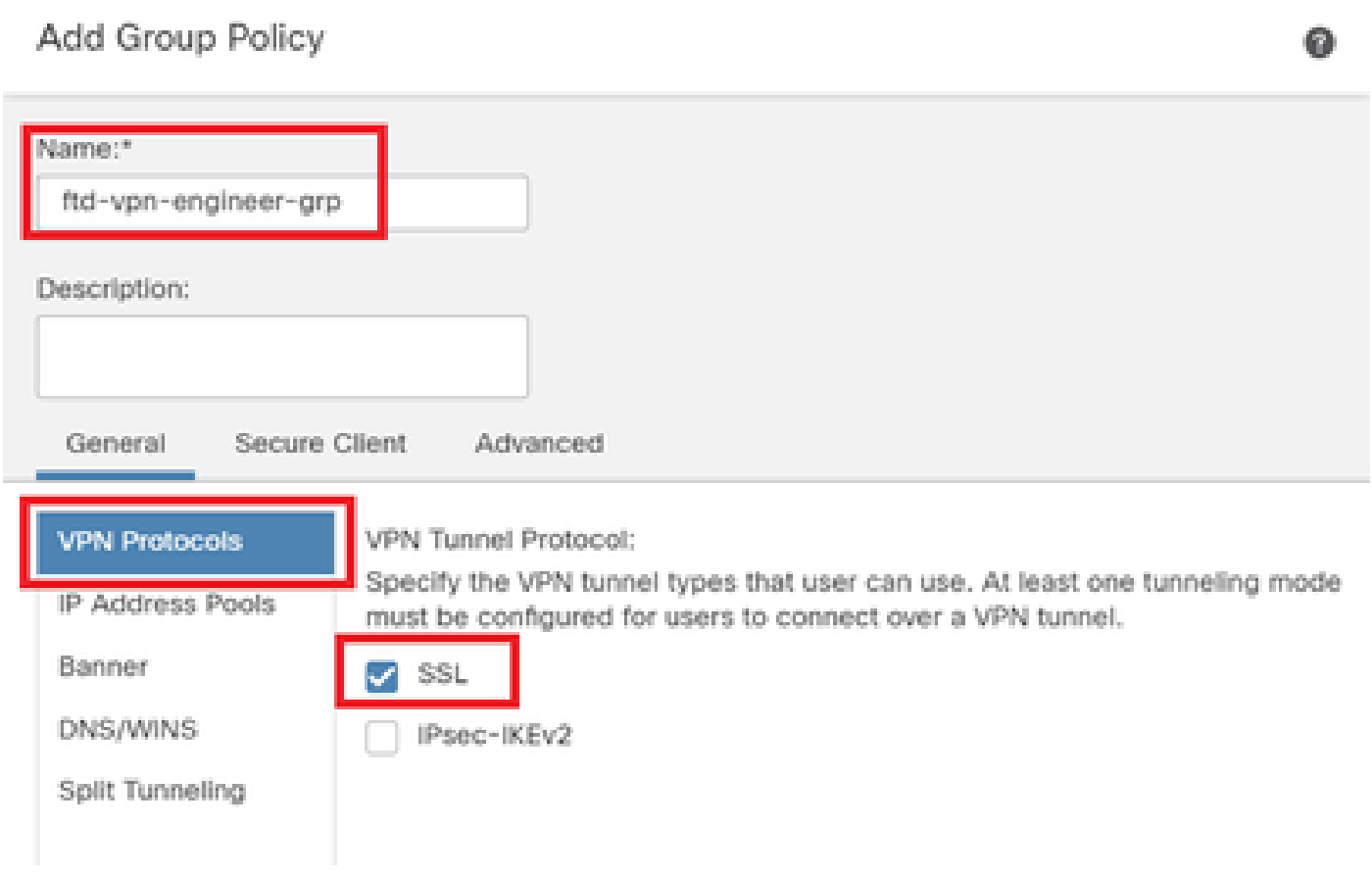
انتقل إلى Object > إدارة الكائن > VPN > نمج المجموعة، انقر فوق زر إضافة نمج المجموعة.



اضافة نهج المجموعة

قم بإدخال المعلومات الضرورية لإنشاء سياسة مجموعة لعميل Engineer VPN.

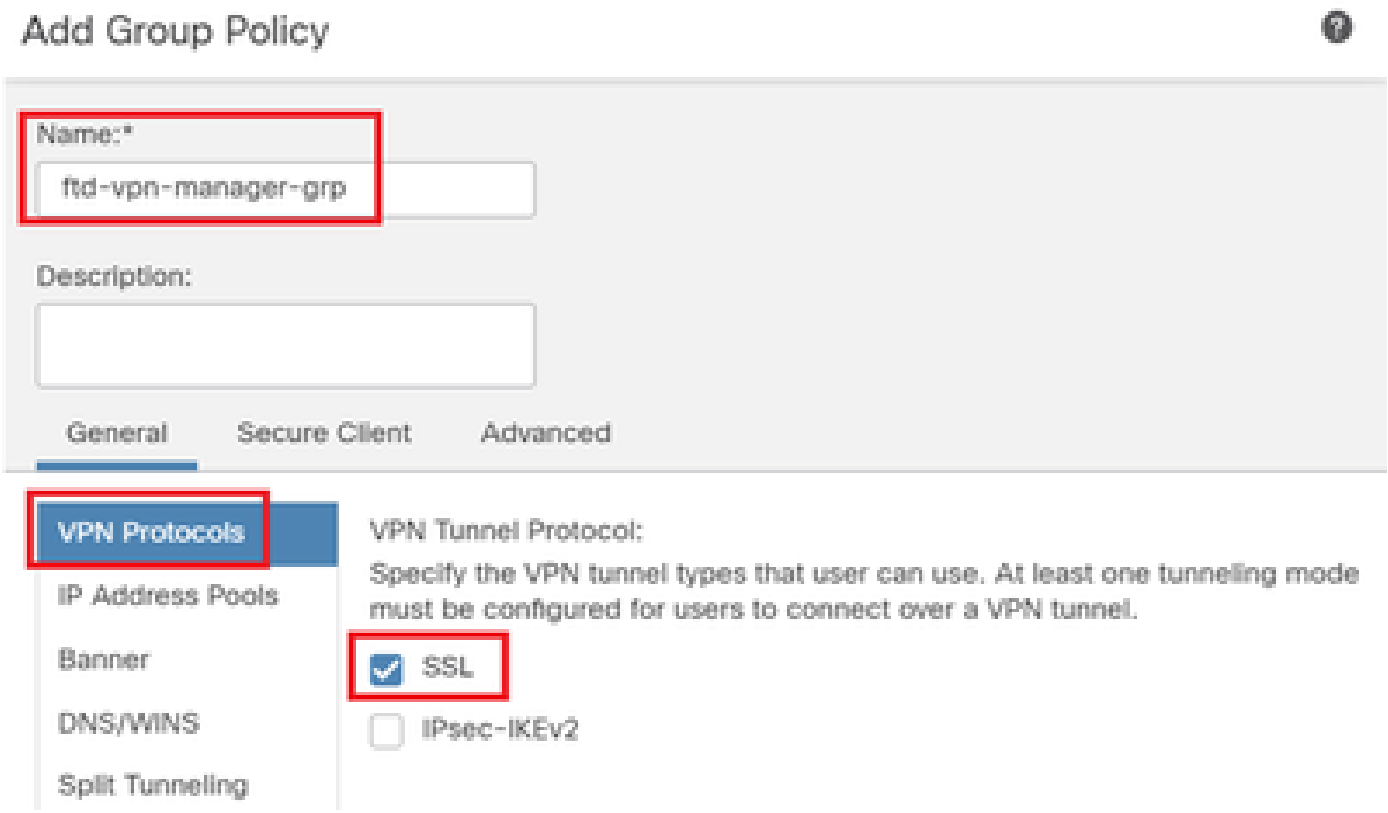
- الاسم: ftd-vpn-engineer-grp
- بروتوكولات VPN: SSL



نهج المجموعة لعميل شبكة VPN للمهندس

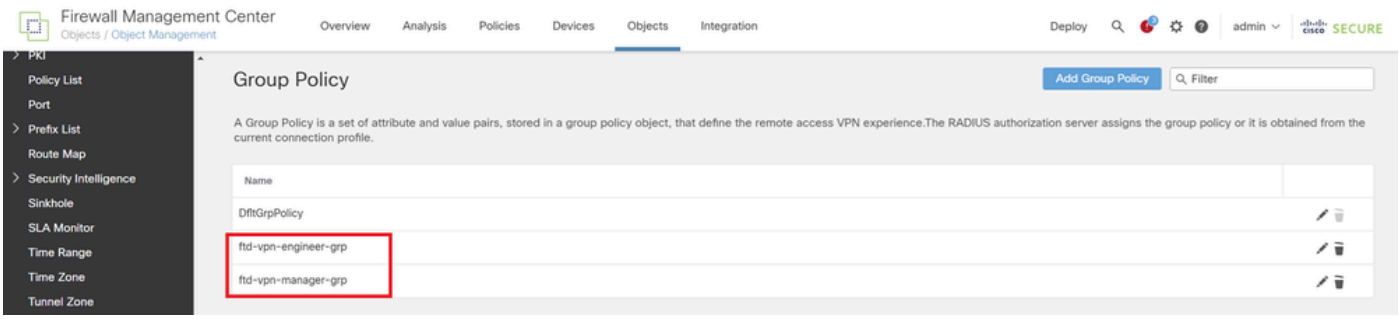
أدخل المعلومات الضرورية لإنشاء سياسة مجموعة لعميل VPN الخاص بالمدير.

- الاسم: ftd-vpn-manager-grp
- بروتوكولات VPN: SSL



نهج المجموعة لعميل Manager VPN

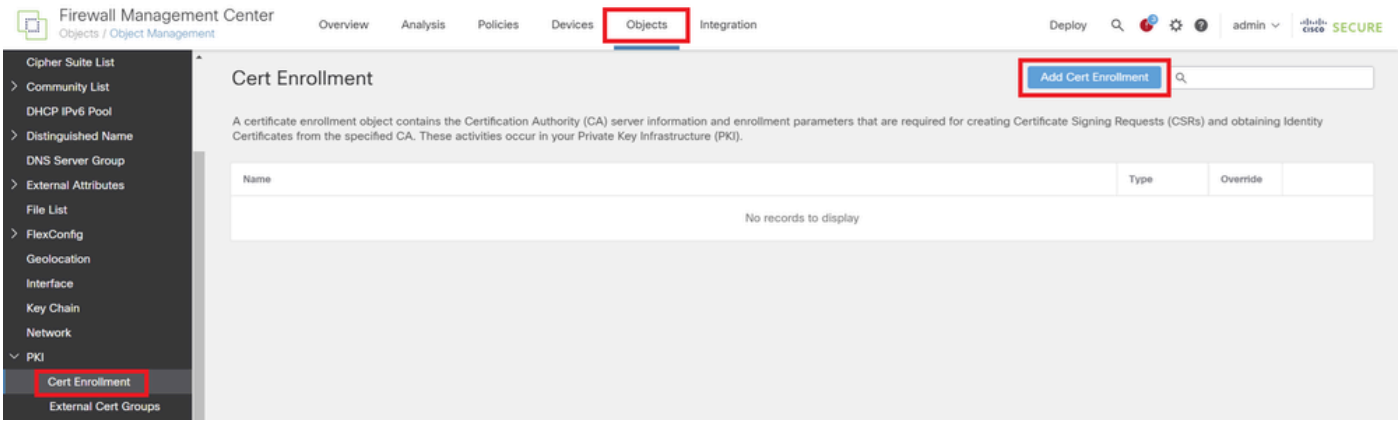
تأكيد نهج المجموعة الجديدة.



نهج مجموعة جديدة

الخطوة 5. إضافة شهادة FTD

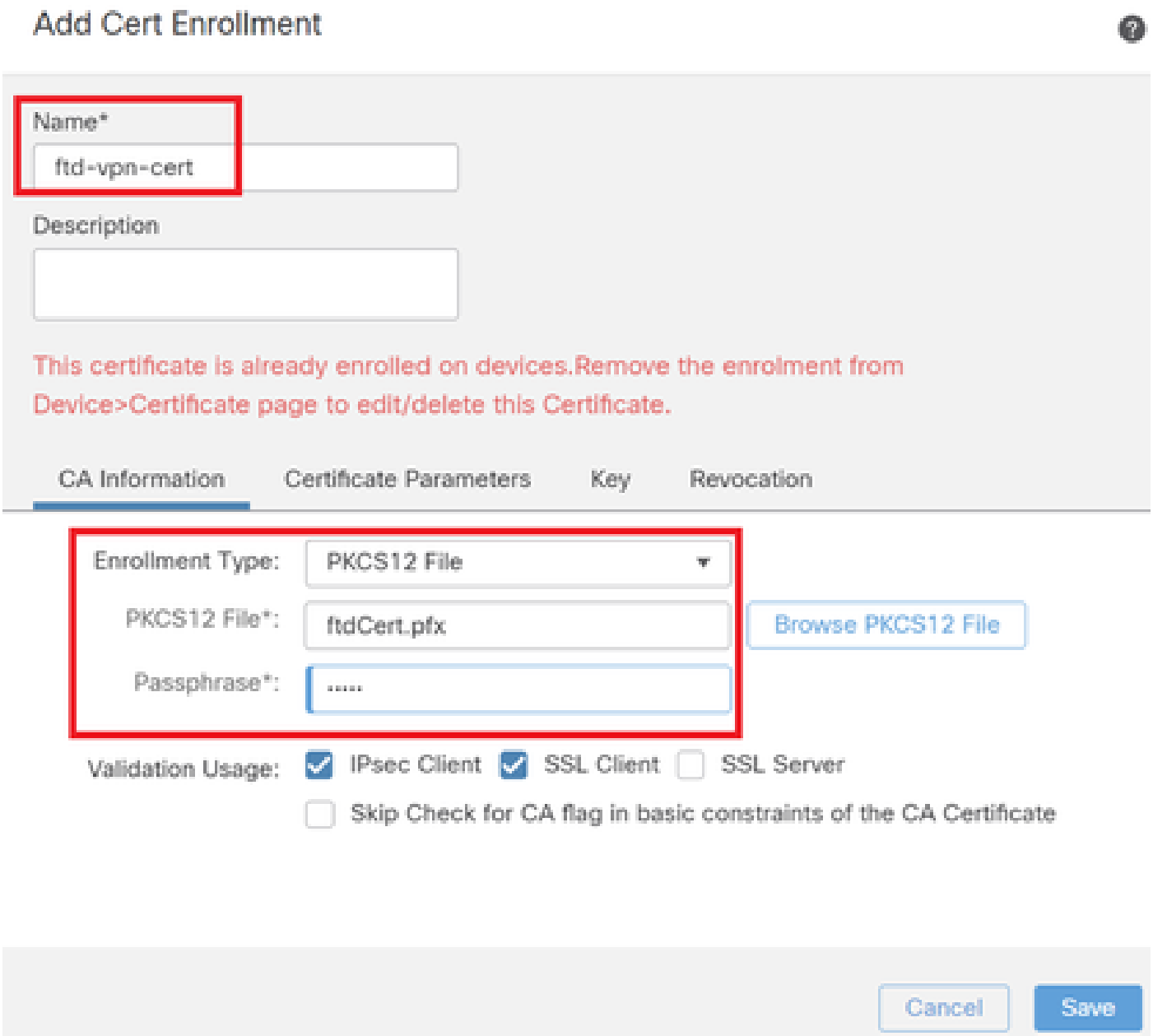
انتقل إلى Object > إدارة الكائن > PKI > تسجيل القاطع، انقر فوق الزر إضافة تسجيل القاطع.



إضافة تسجيل الشهادة

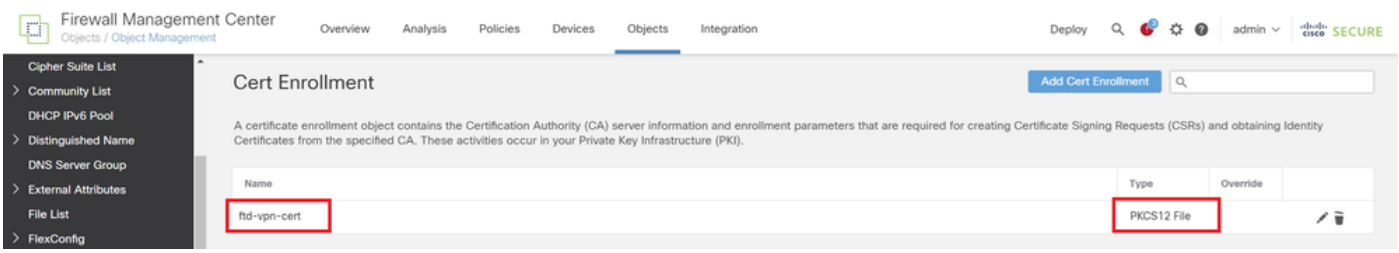
قم بإدخال المعلومات الضرورية لشهادة FTD واستيراد ملف PKCS12 من حاسب محلي.

- الاسم: ftd-vpn-cert
- نوع التسجيل: ملف PKCS12



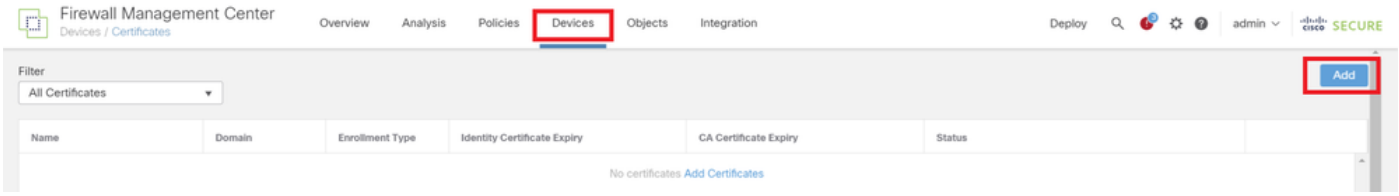
تفاصيل تسجيل الشهادة

تأكيد تسجيل الشهادة الجديد.



تسجيل شهادة جديد

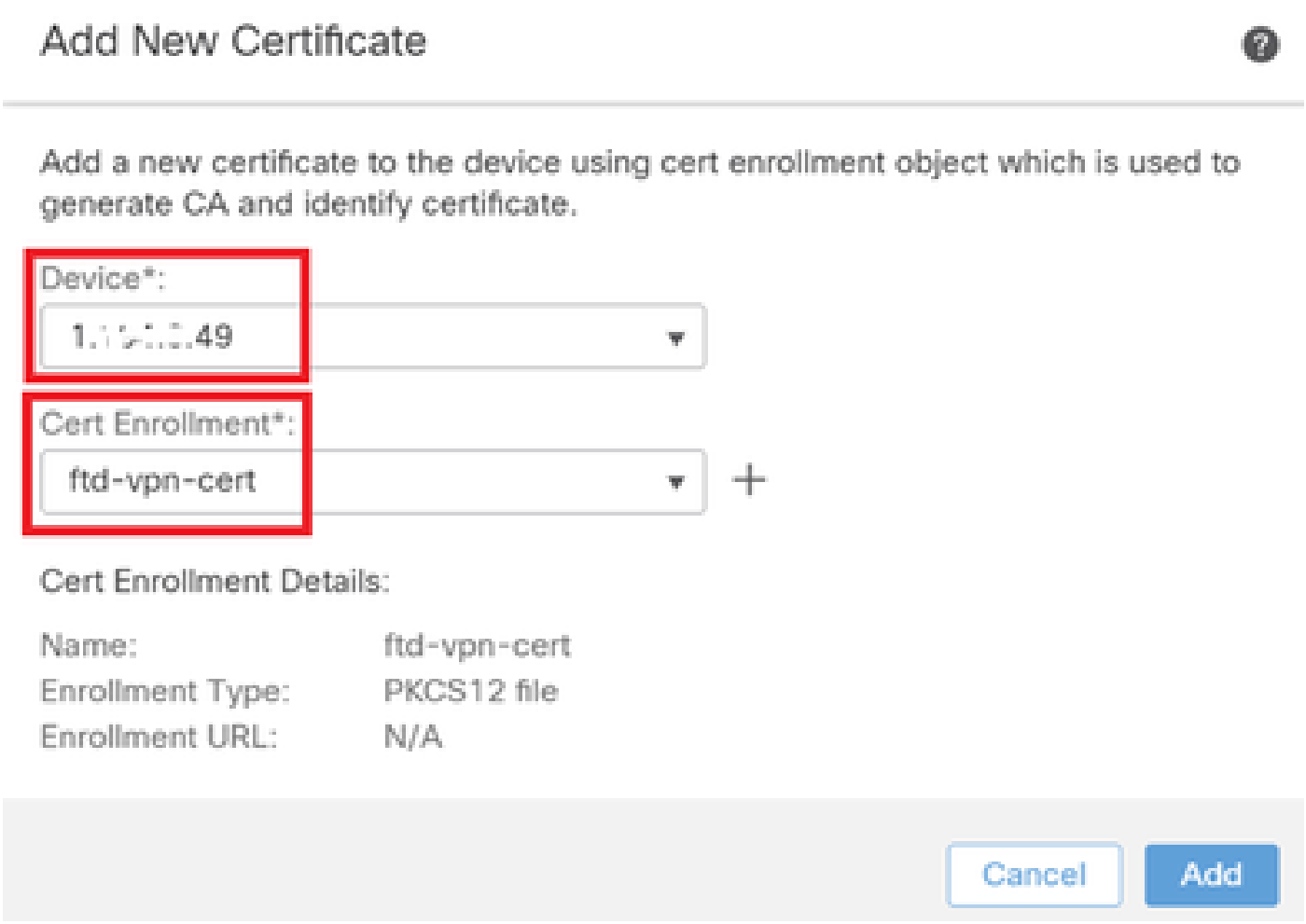
انتقل إلى الأجهزة > الشهادات، انقر فوق زر إضافة.



إضافة شهادة FTD

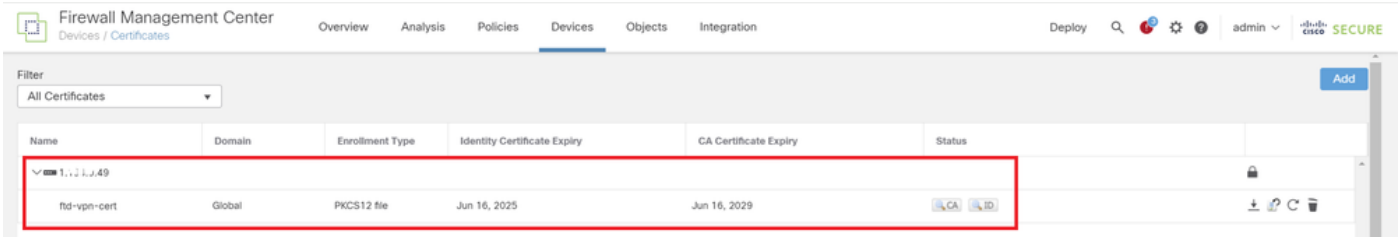
أدخل المعلومات الضرورية لربط تسجيل الشهادة الجديدة ب FTD.

- الجهاز: 1.x.x.49
- تسجيل الشهادة: FTD-VPN-CERT



ربط الشهادة ب FTD

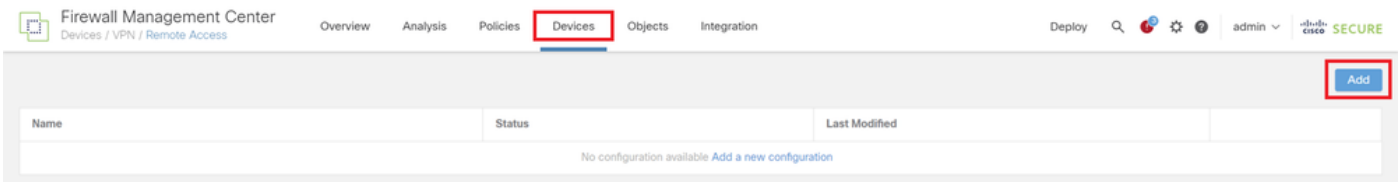
تأكيد حالة ربط الشهادة.



حالة ربط الشهادة

الخطوة 6. إضافة تعيين نهج لملف تعريف اتصال المهندس

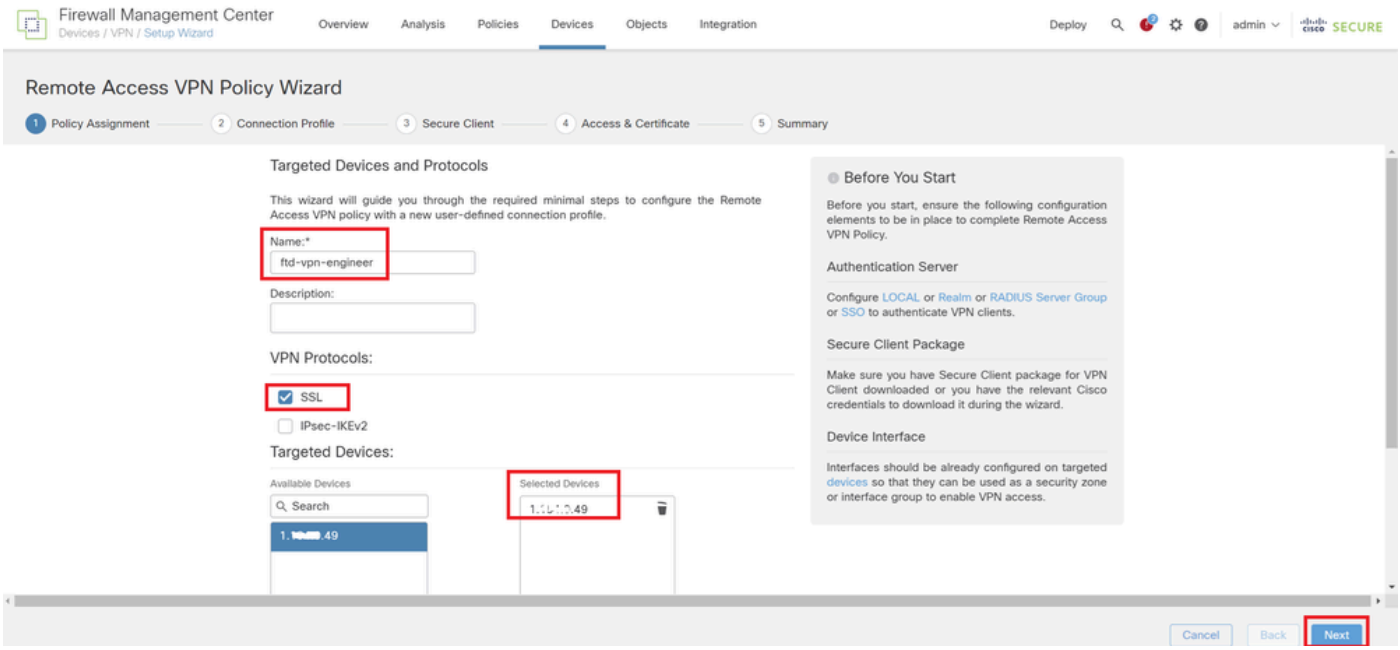
انتقل إلى الأجهزة > VPN > الوصول عن بعد، انقر فوق AddButton.



إضافة شبكة VPN للوصول عن بعد

قم بإدخال المعلومات الضرورية وانقر فوق Nextbutton.

- الاسم: ftd-vpn-engineer
- بروتوكولات VPN: SSL
- الأجهزة المستهدفة: 1.x.49



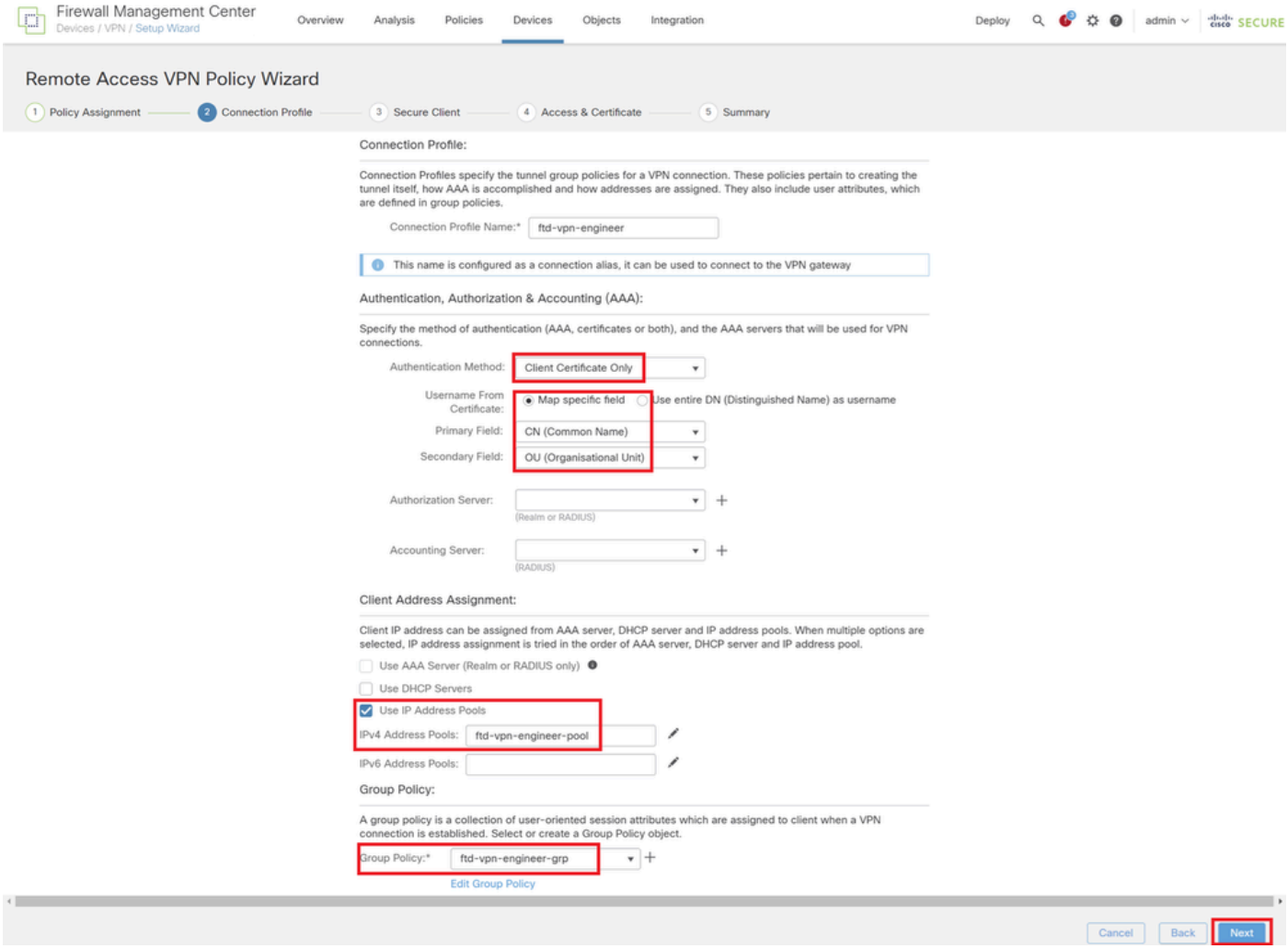
تعيين النهج

الخطوة 7. تكوين تفاصيل ملف تعريف اتصال المهندس

قم بإدخال المعلومات الضرورية وانقر فوق Nextbutton.

- أسلوب المصادقة: شهادة العميل فقط
- اسم المستخدم من الشهادة: حقل محدد للتعيين
- الحقل الأساسي: CN (الاسم الشائع)
- الحقل الثانوي: OU (الوحدة التنظيمية)

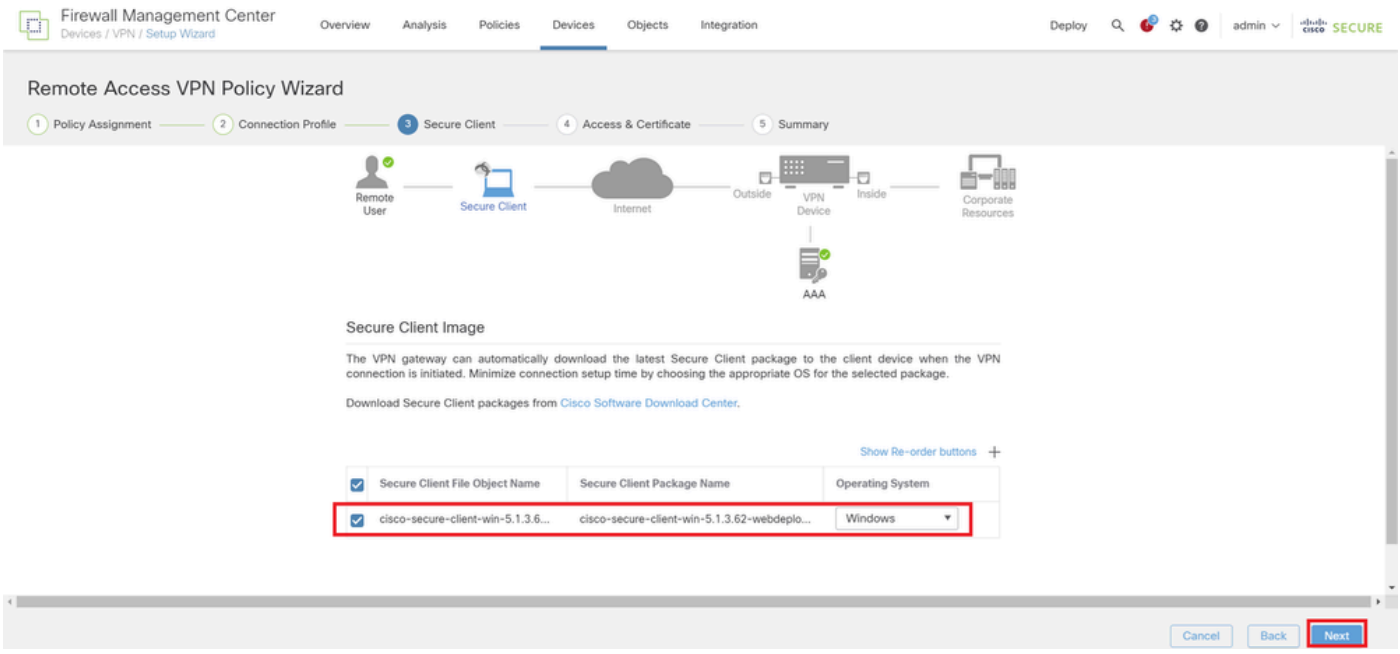
- تجمعات عناوين IPv4: ftd-vpn-engineer-pool
- نهج المجموعة: ftd-vpn-engineer-grp



تفاصيل ملف تعريف الاتصال

الخطوة 8. تكوين صورة عميل آمنة لملف تعريف اتصال المهندس

حدد ملف صورة عميل آمن وانقر فوق Nextbutton.

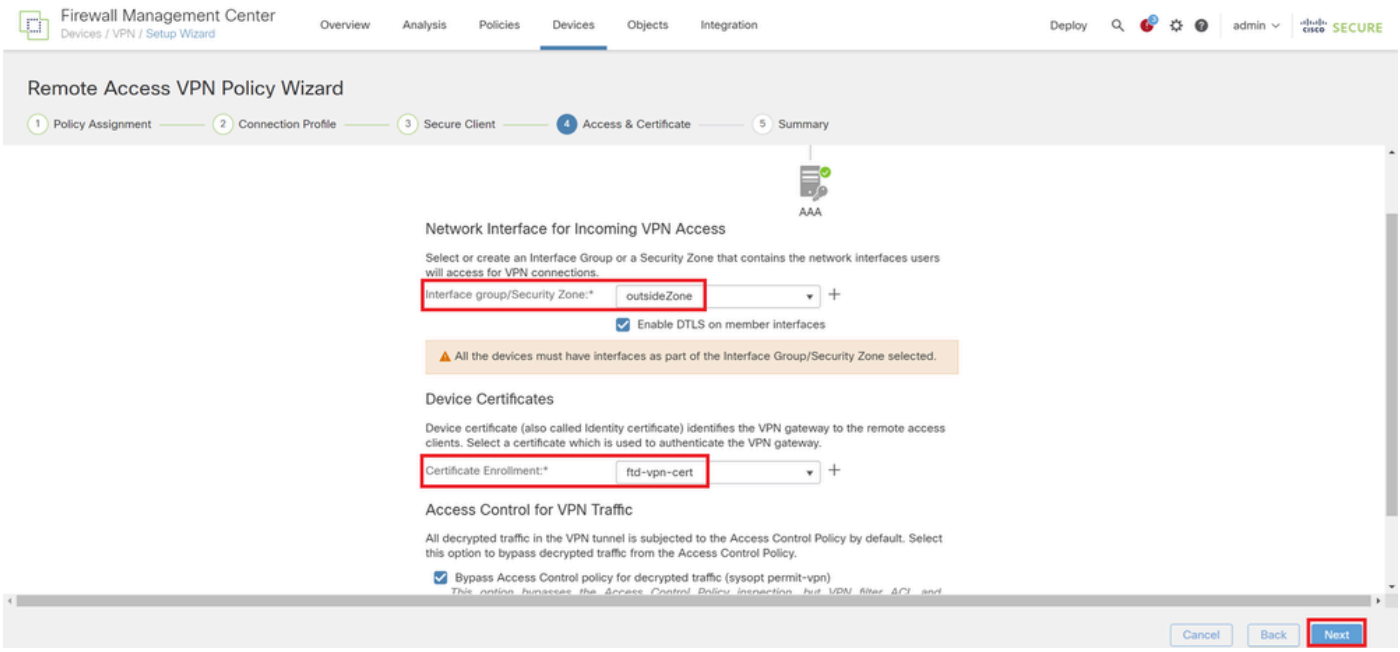


تحديد عميل آمن

الخطوة 9. تكوين الوصول والشهادة لملف تعريف اتصال المهندس

حدد قيمة ل مجموعة الواجهة/منطقة الأمان وعناصر تسجيل الشهادة، انقر فوق الزر التالي.

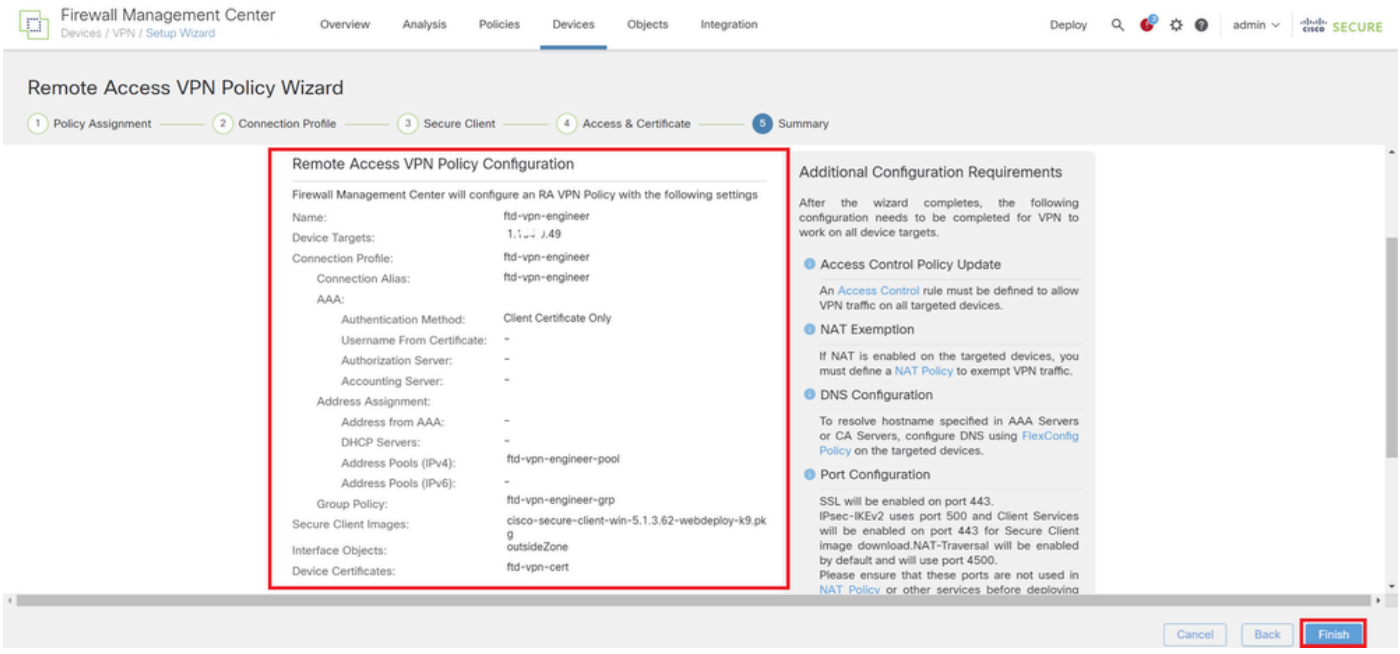
- مجموعة الواجهة/منطقة الأمان: خارج المنطقة
- تسجيل الشهادة: ftd-vpn-cert



تفاصيل الوصول والشهادة

الخطوة 10. تأكيد الملخص لملف تعريف اتصال المهندس

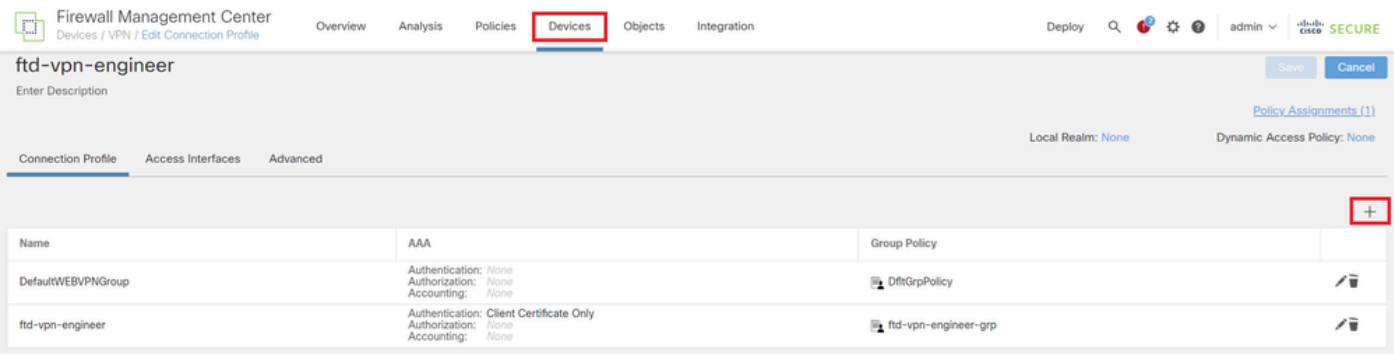
تأكد من المعلومات التي تم إدخالها لنهج VPN للوصول عن بعد وانقر فوق زر إنهاء.



تفاصيل نهج VPN للوصول عن بعد

الخطوة 11. إضافة ملف تعريف الاتصال لعميل Manager VPN

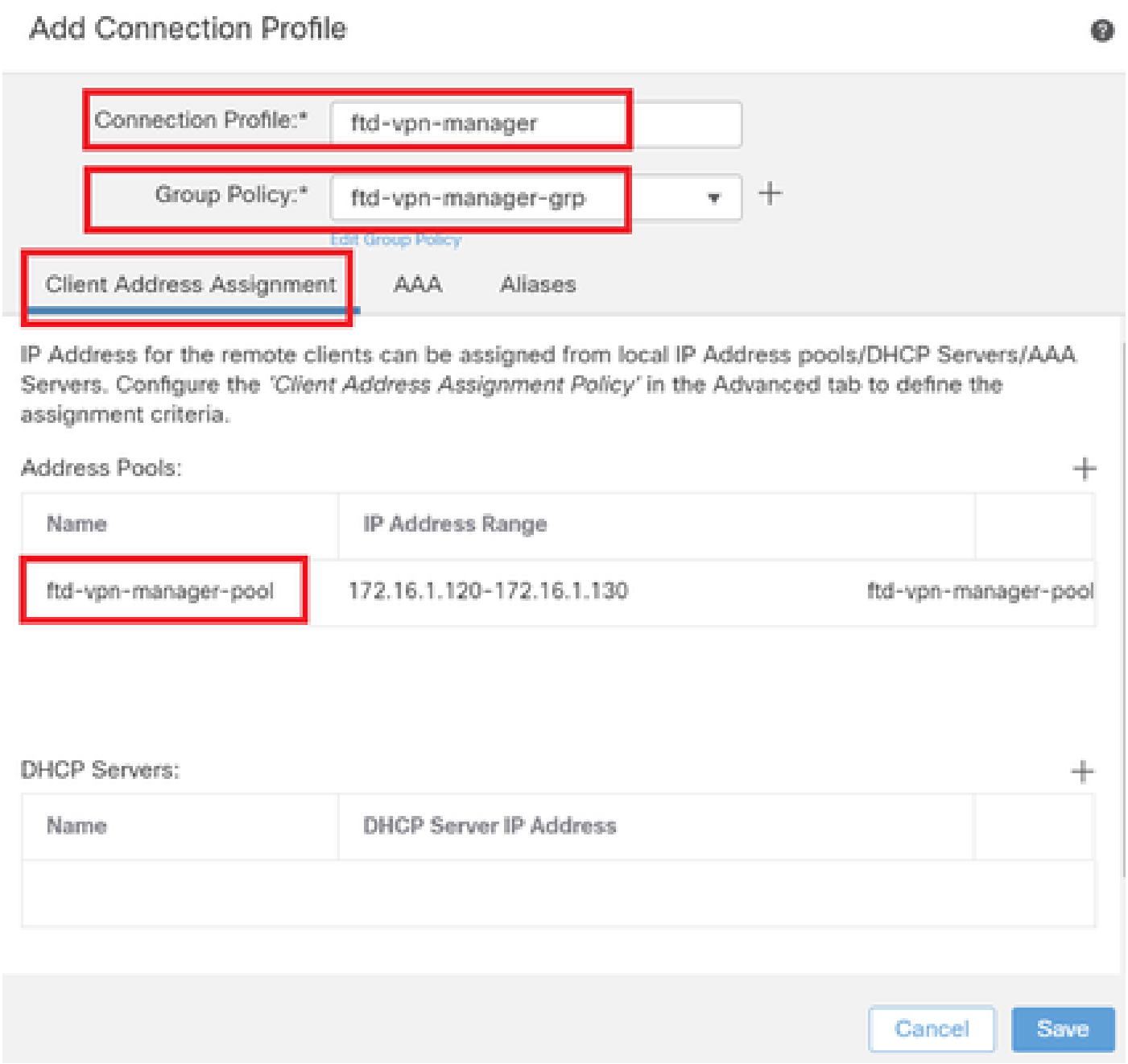
انتقل إلى الأجهزة > VPN > الوصول عن بعد > ملف تعريف الاتصال، انقر فوق + زر.



إضافة ملف تعريف الاتصال لعميل Manager VPN

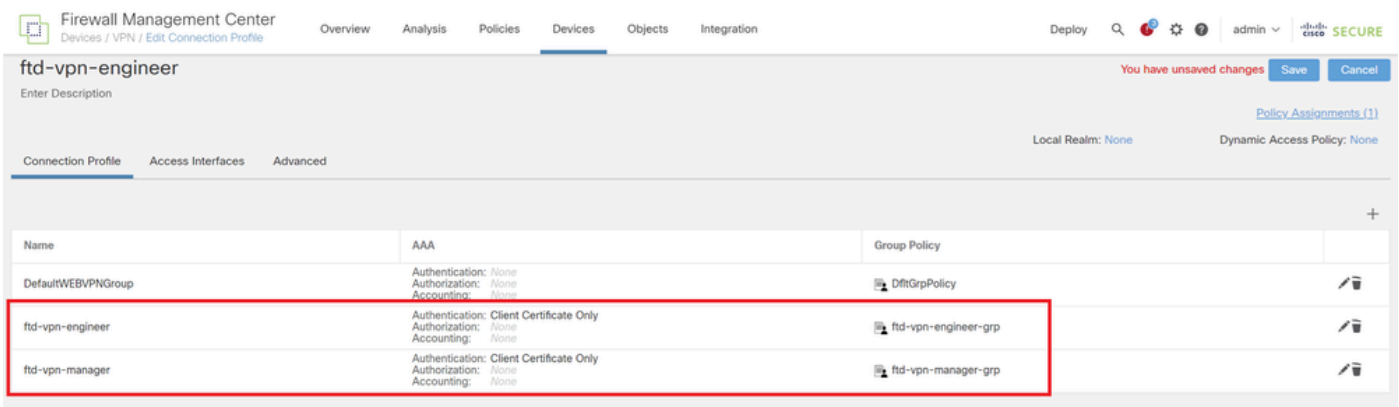
أدخل المعلومات الضرورية لملف تعريف الاتصال وانقر على زر حفظ.

- الاسم: ftd-vpn-manager
- نهج المجموعة: ftd-vpn-manager-grp
- تجمعات عناوين IPv4: ftd-vpn-manager-pool



تفاصيل ملف تعريف الاتصال لعميل Manager VPN

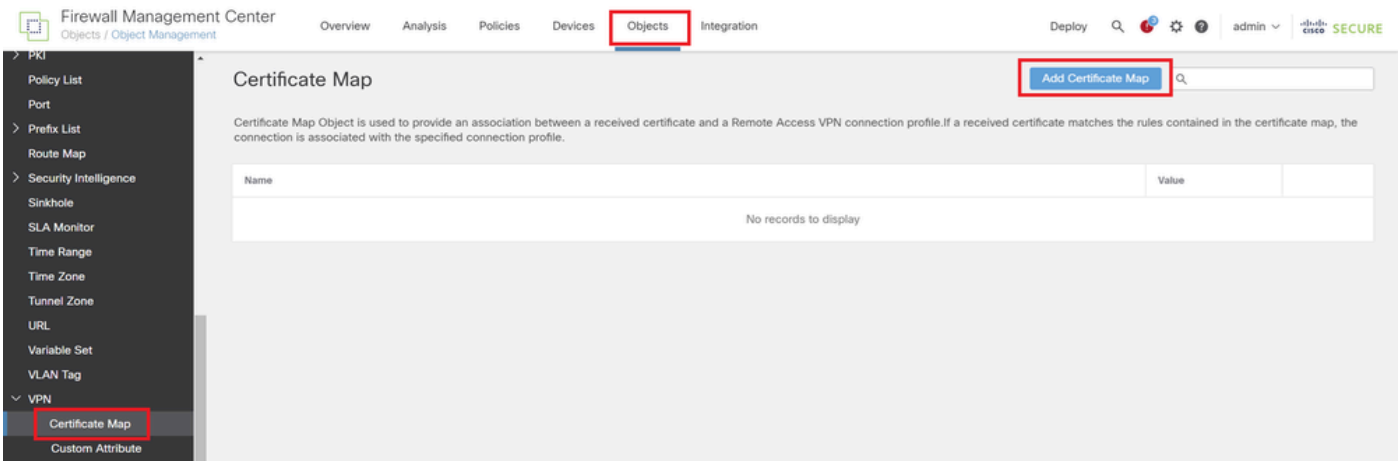
تأكيد توصيفات توصيل جديدة مضافة.



تأكيد توصيفات التوصيل المضافة

الخطوة 12. إضافة خريطة شهادات

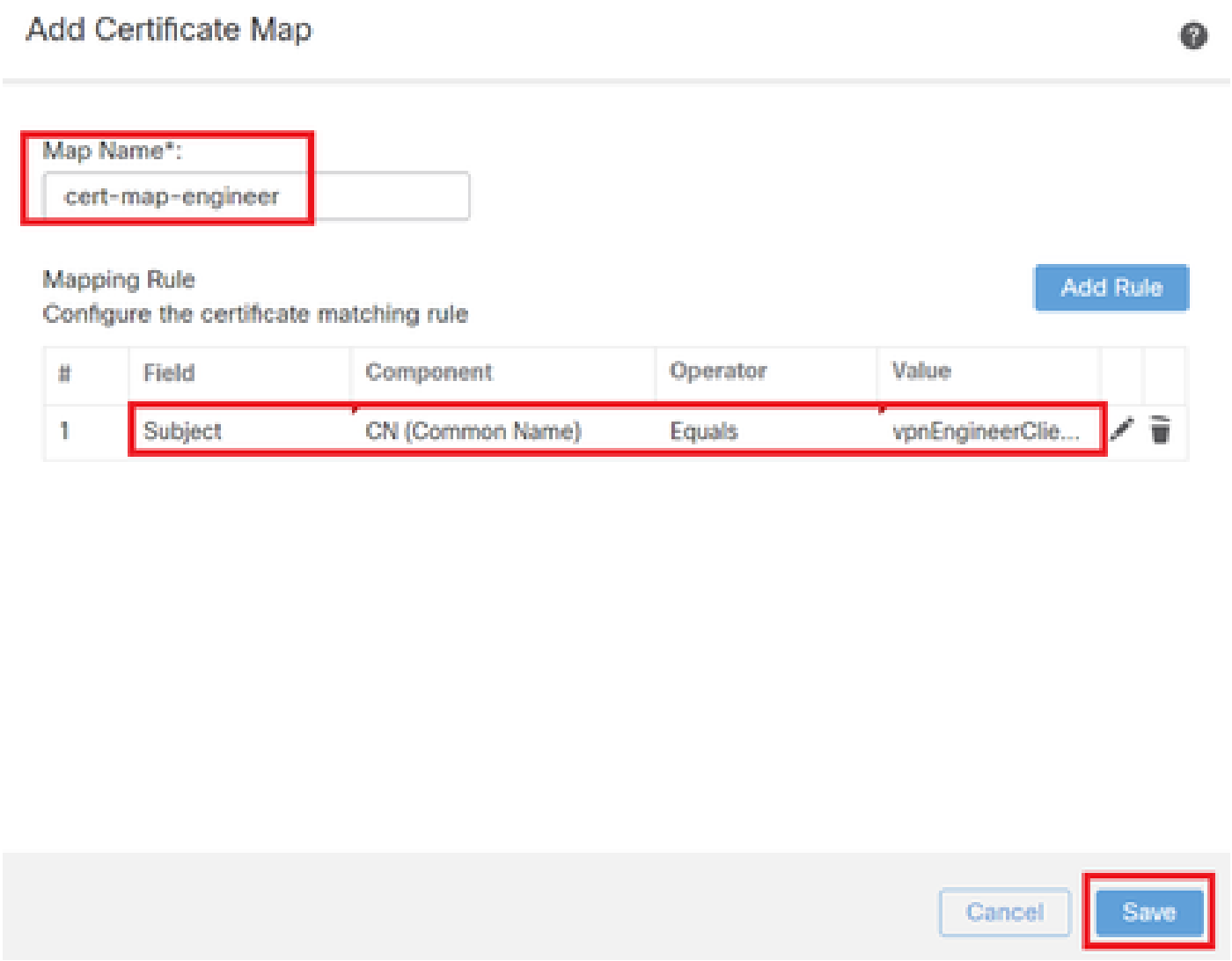
انتقل إلى كائنات > إدارة الكائن > VPN > خريطة الشهادة، انقر فوق زر خريطة إضافة الشهادة.



إضافة خريطة شهادات

أدخل المعلومات الضرورية لخريطة الشهادات الخاصة بعميل Engineer VPN وانقر فوق زر حفظ.

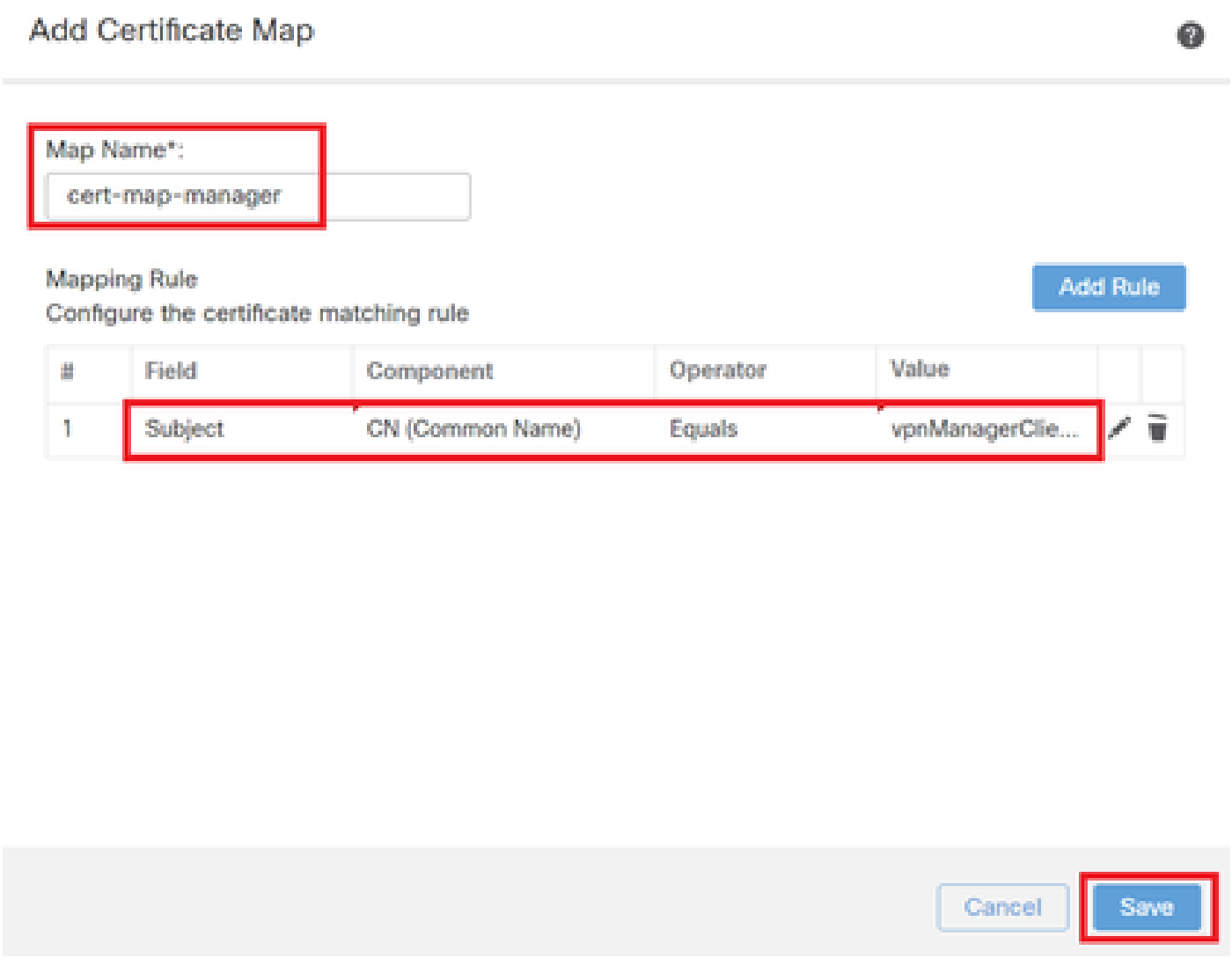
- اسم الخريطة: خبير - مهندس الخريطة
- قاعدة التعيين: CN (الاسم الشائع) يساوي vpnEngineerClientCN



خريطة الشهادات لعميل المهندس

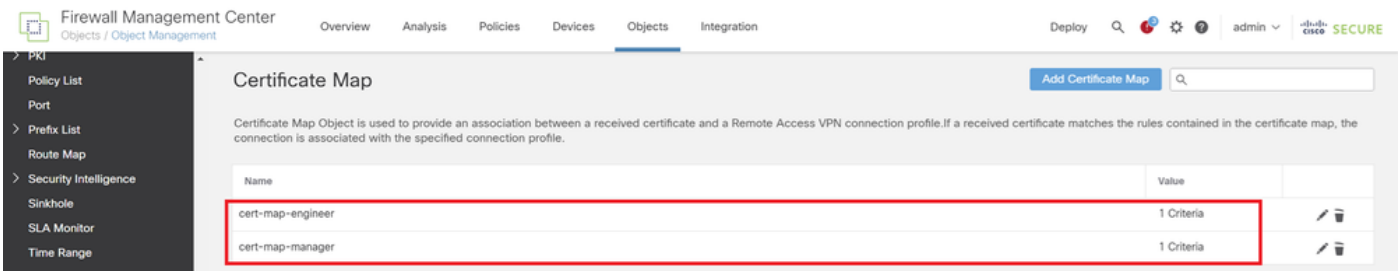
أدخل المعلومات الضرورية لخريطة الشهادة لعميل Manager VPN وانقر فوق زر حفظ.

- اسم الخريطة: cert-map-manager
- قاعدة التعيين: CN (الاسم الشائع) يساوي vpnManagerClientCN



تعيين الشهادة لعميل Manager

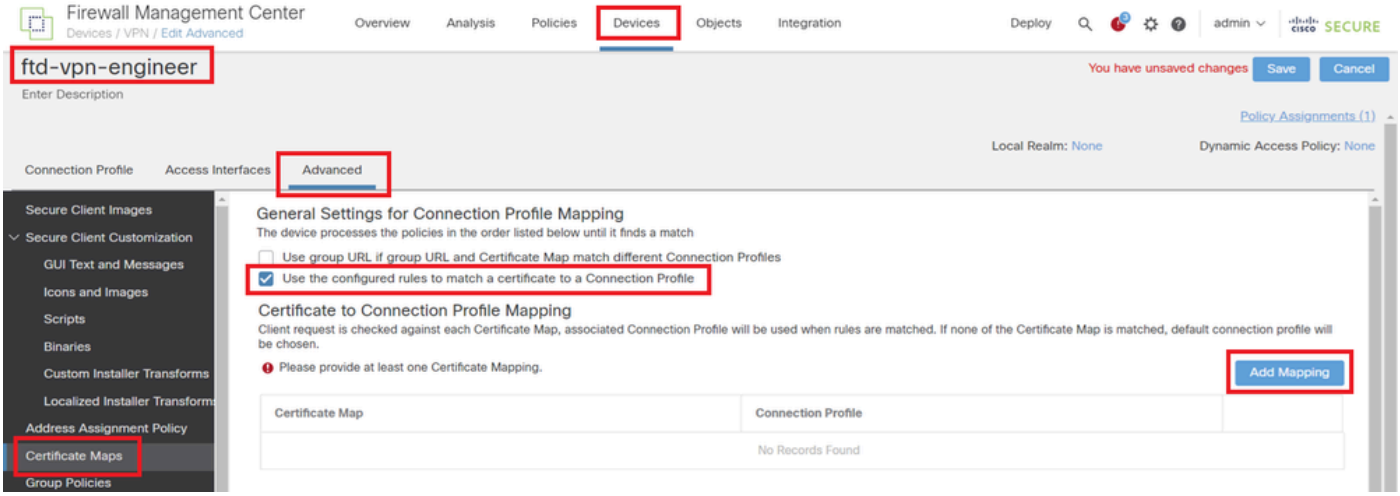
تأكيد مخططات الشهادات المضافة الجديدة.



خرائط شهادات جديدة

الخطوة 13. ربط مخطط الشهادة بملف تعريف الاتصال

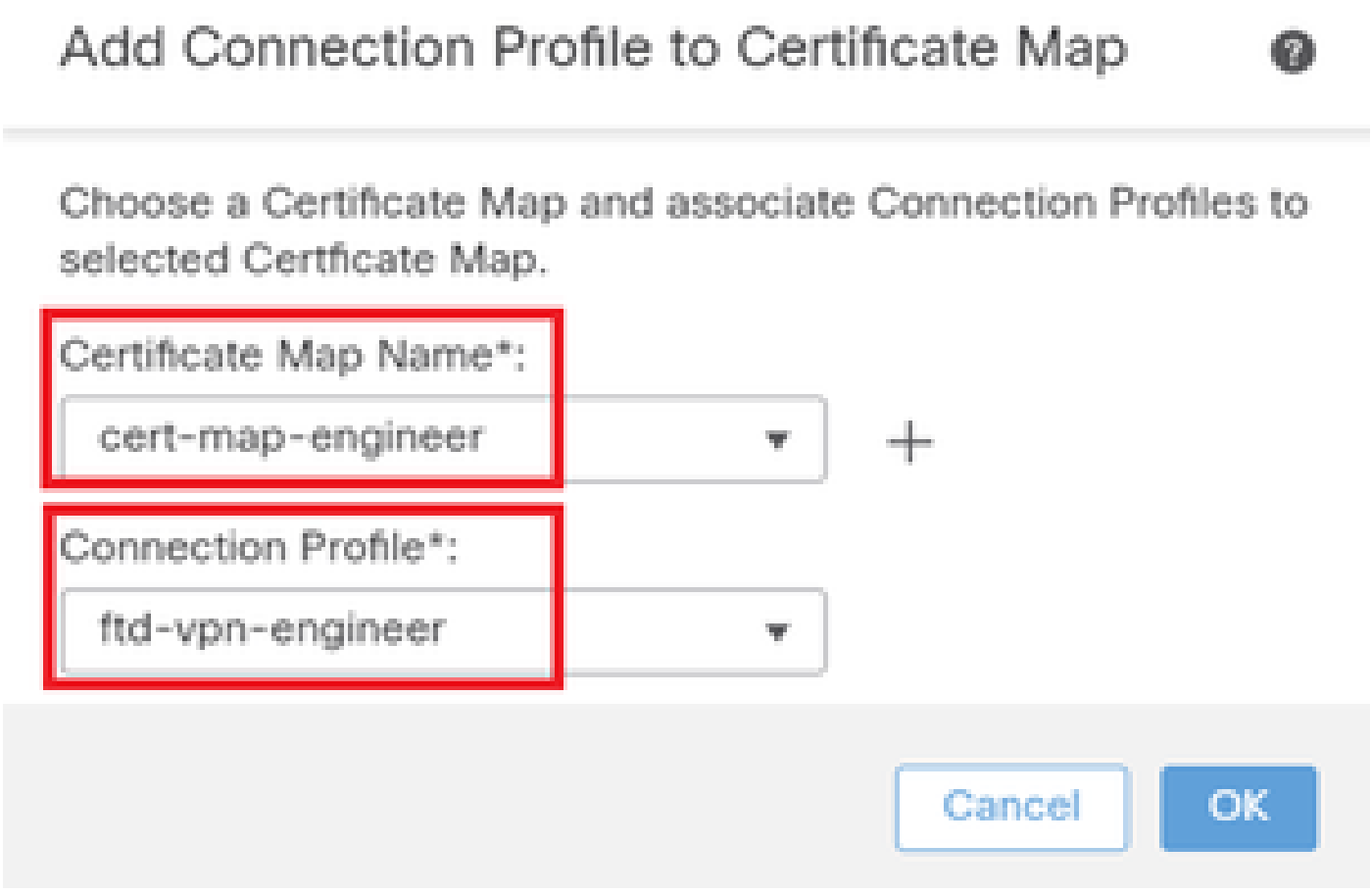
انتقل إلى الأجهزة > VPN > الوصول عن بعد، وحرر FTD-VPN-engineer. ثم، انتقل إلى متقدم > خرائط الترخيص، انقر زر إضافة تخطيط.



ربط خريطة الشهادة

ربط خريطة الشهادة بملف تعريف الاتصال لعميل VPN للمهندس.

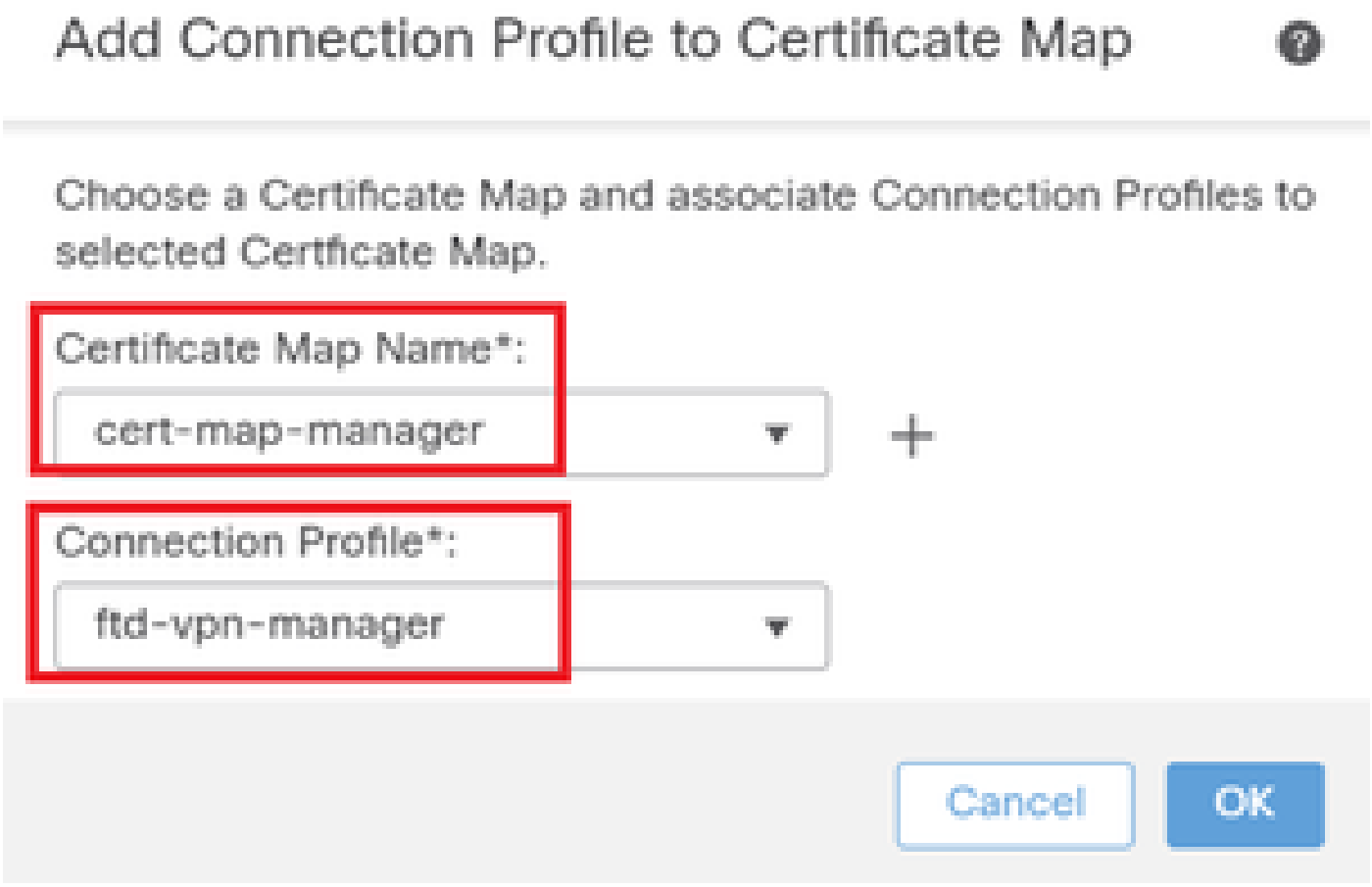
- اسم خريطة الشهادة: cert-map-engineer
- Connection Profile: ftd-vpn-engineer



ربط خريطة الشهادة لعميل Engineer VPN

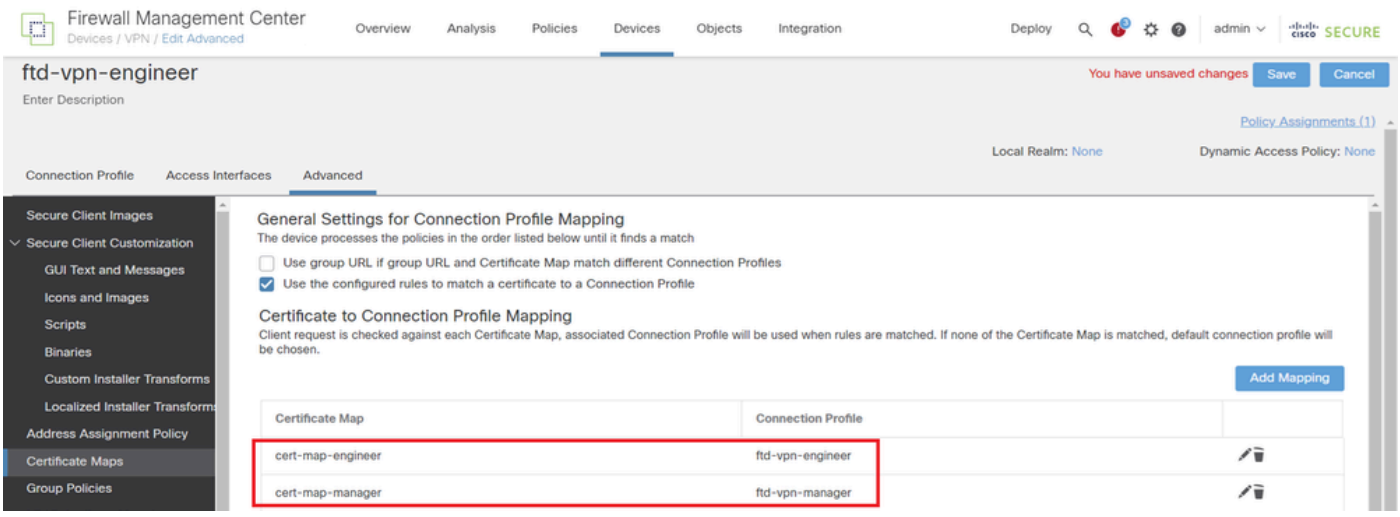
ربط خريطة الشهادة بملف تعريف الاتصال لعميل VPN الخاص بالمدير.

- اسم خريطة الشهادة: cert-map-manager
- ملف تعريف الاتصال: ftd-vpn-manager



ربط خريطة الشهادة لعميل Manager VPN

تأكيد إعداد ربط الشهادة.



تأكيد ربط الشهادة

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

// Defines a pool of addresses
ip local pool ftd-vpn-engineer-pool 172.16.1.100-172.16.1.110 mask 255.255.255.0
ip local pool ftd-vpn-manager-pool 172.16.1.120-172.16.1.130 mask 255.255.255.0

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

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

certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Defines Certificate Map for Engineer VPN Clients
crypto ca certificate map cert-map-engineer 10
subject-name attr cn eq vpnEngineerClientCN

// Defines Certificate Map for Manager VPN Clients
crypto ca certificate map cert-map-manager 10
subject-name attr cn eq vpnManagerClientCN

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert-map-engineer 10 ftd-vpn-engineer
certificate-group-map cert-map-manager 10 ftd-vpn-manager
error-recovery disable

// Configures the group-policy to allow SSL connections from manager VPN clients
group-policy ftd-vpn-manager-grp internal
group-policy ftd-vpn-manager-grp attributes
banner none
wins-server none
dns-server none
```

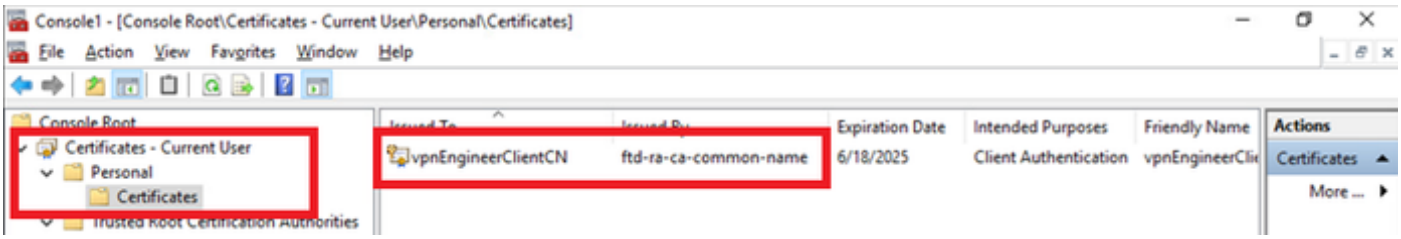
```
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// Configures the group-policy to allow SSL connections from engineer VPN clients
group-policy ftd-vpn-engineer-grp internal
group-policy ftd-vpn-engineer-grp attributes
banner none
wins-server none
dns-server none
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
```

```
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

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

// Configures the tunnel-group to use the certificate authentication for manager VPN clients
tunnel-group ftd-vpn-manager type remote-access
tunnel-group ftd-vpn-manager general-attributes
address-pool ftd-vpn-manager-pool
default-group-policy ftd-vpn-manager-grp
tunnel-group ftd-vpn-manager webvpn-attributes
authentication certificate
```

تأكيد في عميل شبكة VPN

الخطوة 1. تأكيد شهادة العميل

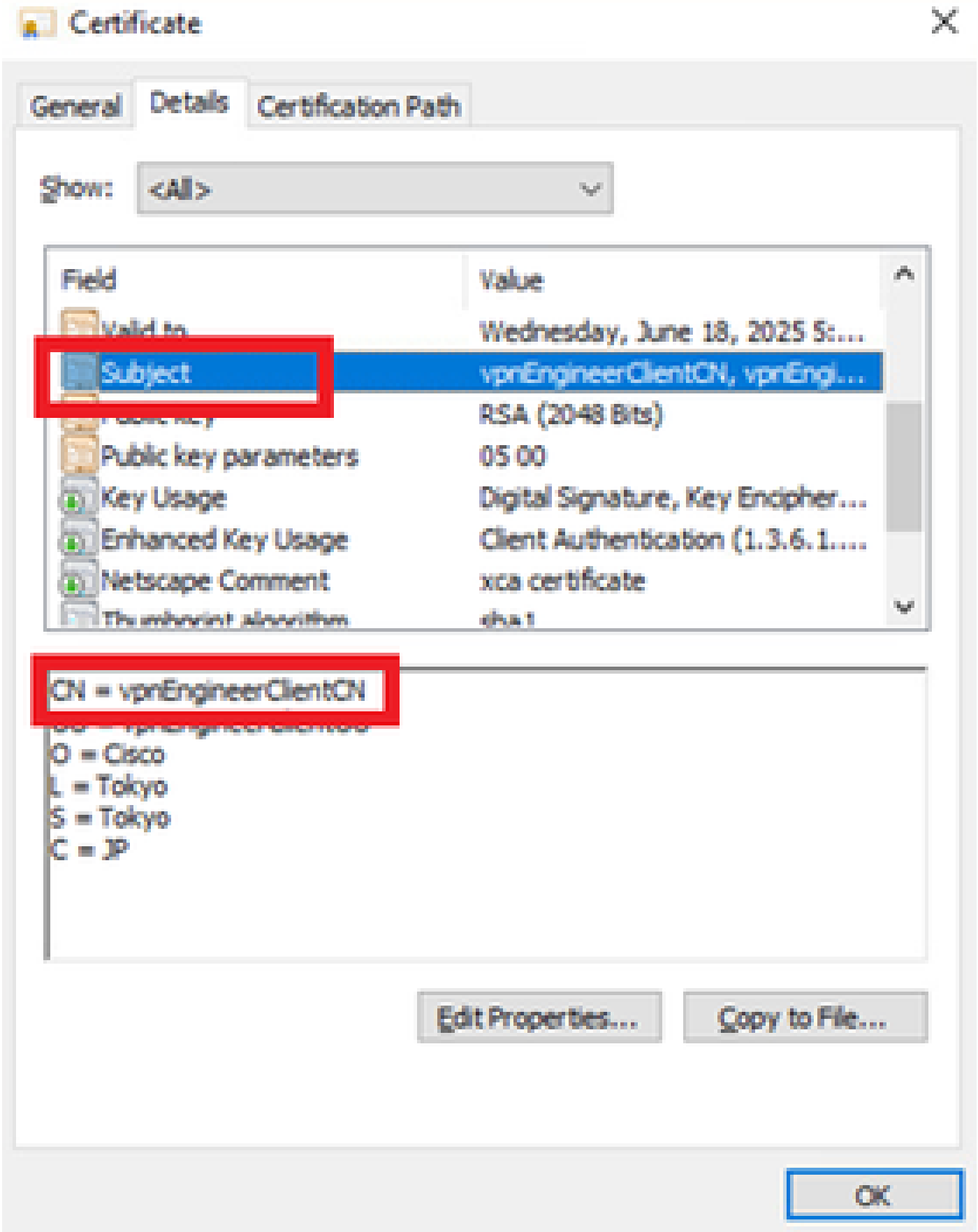
في عميل شبكة VPN الهندسية، انتقل إلى الشهادات - مستخدم حالي > شخصي > شهادات، تحقق من شهادة العميل المستخدمة للمصادقة.



تأكيد الشهادة لعميل Engineer VPN

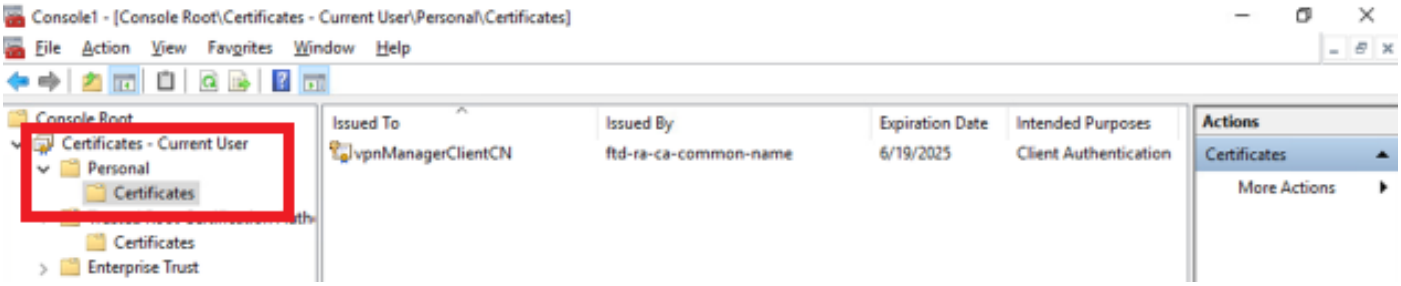
انقر نقرا مزدوجا فوق شهادة العميل، ثم انتقل إلى Details، ثم تحقق من تفاصيل الموضوع.

- الموضوع: CN = vpnEngineerClientCN



تفاصيل شهادة عميل المهندس

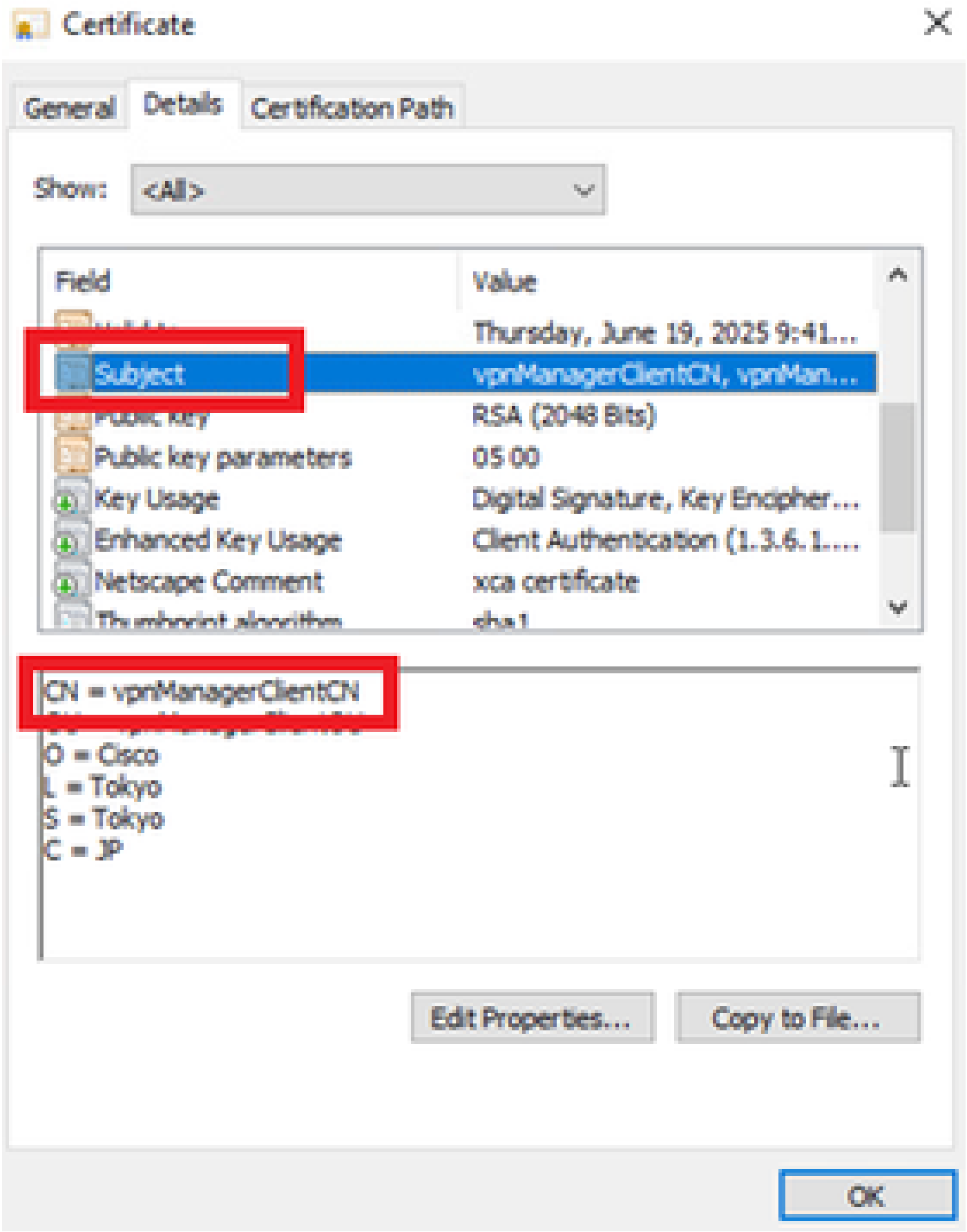
في عميل Manager VPN، انتقل إلى الشهادات - مستخدم حالي > شخصي > شهادات، تحقق من شهادة العميل المستخدمة للمصادقة.



تأكيد الشهادة لعميل Manager VPN

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

- الموضوع: CN = vpnManagerClientCN

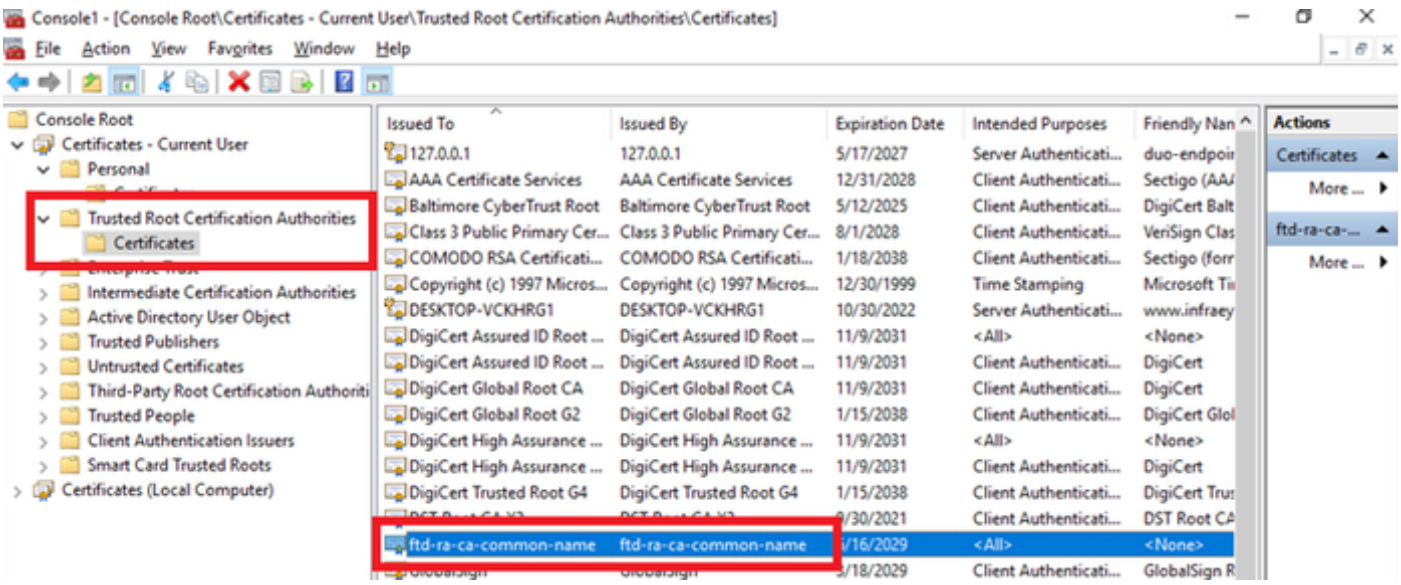


تفاصيل شهادة عميل المدير

الخطوة 2. تأكيد CA

في كل من عميل شبكة VPN للمهندس و عميل شبكة VPN للمدير، انتقل إلى الشهادات - المستخدم الحالي > مراجع التصديق الجذر الموثوق فيها > الشهادات، تحقق من المرجع المصدق المستخدم للمصادقة.

- صادر عن: ftd-ra-ca-common-name

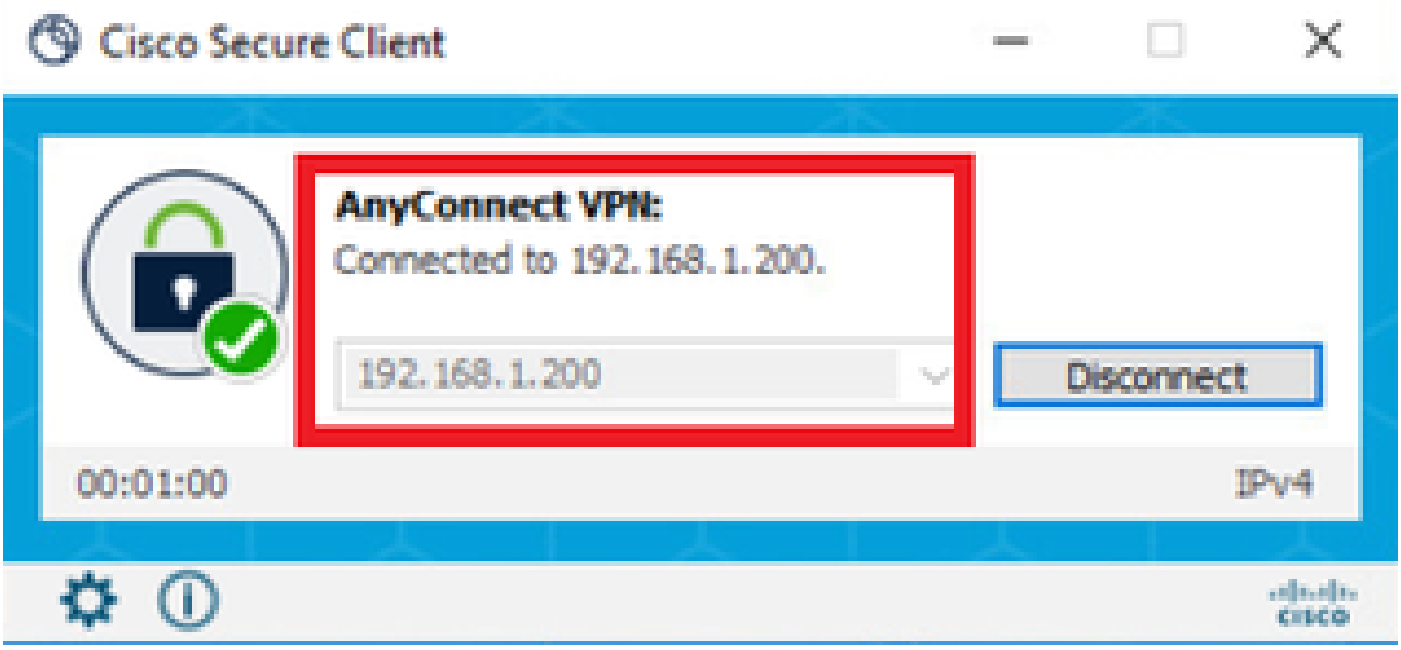


تأكيد CA

التحقق من الصحة

الخطوة 1. بدء اتصال VPN

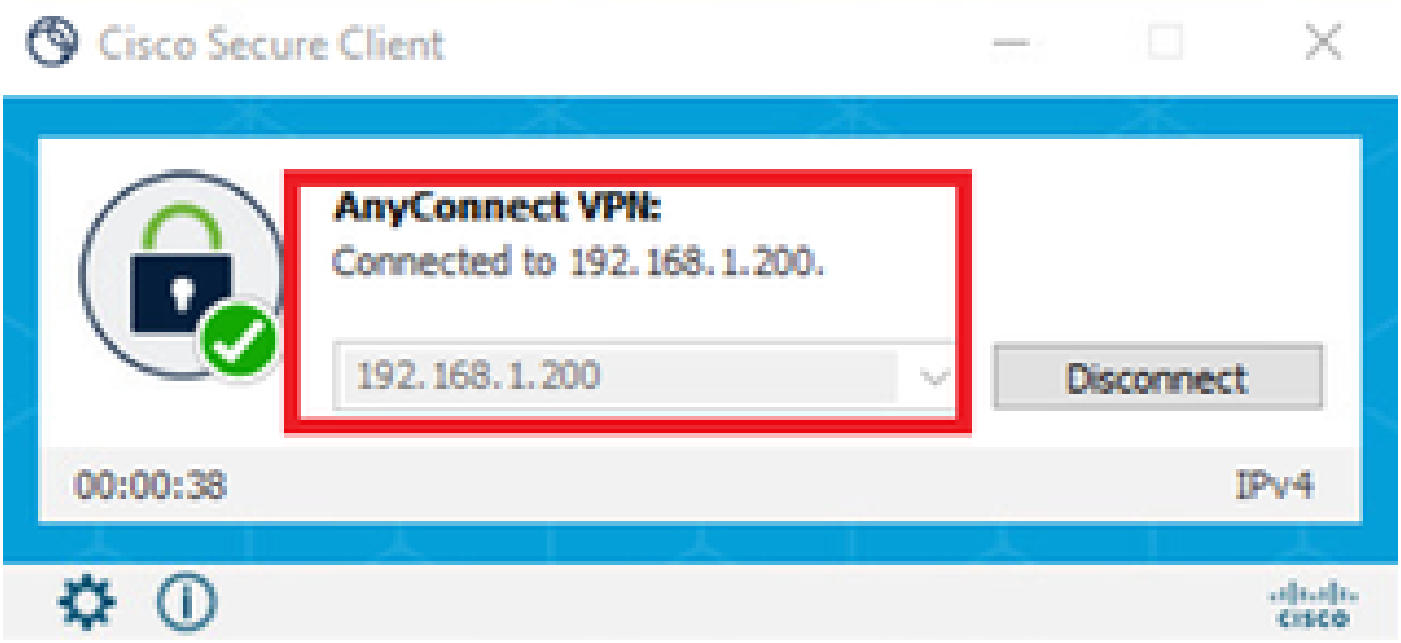
في عميل الشبكة الخاصة الظاهرية (VPN) للمهندس، ابدأ اتصال العميل الآمن من Cisco. ما من حاجة أن يدخل ال username وكلمة، ال VPN يربط بنجاح.



بدء اتصال VPN من عميل المهندس

عميل In Manager VPN، ابدأ اتصال Cisco Secure Client. ما من حاجة أن يدخل ال username وكلمة،

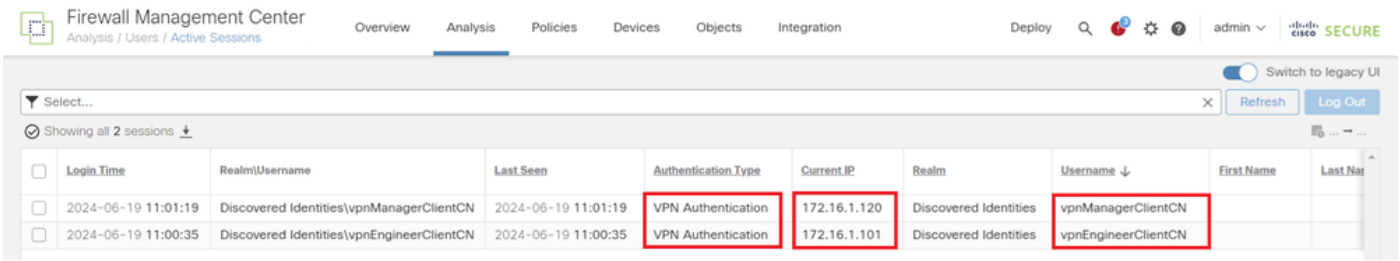
ال VPN يربط بنجاح.



بدء اتصال VPN من عميل الإدارة

الخطوة 2. تأكيد الجلسات النشطة في FMC

انتقل إلى Analysis (التحليل) > Users (المستخدمون) > Active Session (جلسات العمل النشطة)، تحقق من الجلسة النشطة لمصادقة VPN.



تأكيد جلسة العمل النشطة

الخطوة 3. تأكيد جلسات عمل VPN في FTD CLI

شغلshow vpn-sessiondb detail anyconnect أمر في FTD (Lina) CLI أن يؤكد ال VPN جلسة من مهندس ومدير.

```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 13
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14782 Bytes Rx : 12714
```

Pkts Tx : 2 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-engineer-grp Tunnel Group : ftd-vpn-engineer
Login Time : 02:00:35 UTC Wed Jun 19 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000d00066723bc3
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 13.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50225 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 13.2
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50232
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 1775
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 13.3
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 50825
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 0 Bytes Rx : 10939
Pkts Tx : 0 Pkts Rx : 30
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Username : vpnManagerClientCN Index : 14
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14782 Bytes Rx : 13521
Pkts Tx : 2 Pkts Rx : 57
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-manager-grp Tunnel Group : ftd-vpn-manager
Login Time : 02:01:19 UTC Wed Jun 19 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000e00066723bef
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 14.1
Public IP : 192.168.1.21
Encryption : none Hashing : none
TCP Src Port : 49809 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 14.2
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 49816
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 3848
Pkts Tx : 1 Pkts Rx : 25
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 14.3
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 65501
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes

Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 0 Bytes Rx : 9673
Pkts Tx : 0 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0

اهحالصإو ءاطخألا فاشكتسا

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 Lina محرك أثناء اتصال VPN من عميل المهندس.

<#root>

Jun 19 2024 02:00:35: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn
Jun 19 2024 02:00:35: %FTD-6-717022:

Certificate was successfully validated

. serial number: 7AF1C78ADCC8F941, subject name:

CN=vpnEngineerClientCN

,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
Jun 19 2024 02:00:35: %FTD-7-717038: Tunnel group match found.

Tunnel Group: ftd-vpn-engineer

, Peer certificate: serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN,OU=vpnEnginee
Jun 19 2024 02:00:35: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-engineer-grp) for user
Jun 19 2024 02:00:46: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50

هذا مثال على سجلات تصحيح الأخطاء في Lina محرك أثناء اتصال VPN من عميل مدير.

<#root>

Jun 19 2024 02:01:19: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 1AD1B5EAE28C6D3C, subject name: CN=vp
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=vpnManagerC
Jun 19 2024 02:01:19: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-manager-grp) for user
Jun 19 2024 02:01:25: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.21/65

معلومات ذات صلة

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).