تكوين مصادقة مصادقة مصادقة العميل الآمن على FTD عبر FDM

المحتويات

المقدمة

يوضح هذا المستند كيفية إعداد Cisco Secure Client مع SSL على FTD عبر FDM باستخدام مطابقة الشهادة للمصادقة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالموضوع التالية:

- مدير جهاز FirePOWER الظاهري (FDM) من Cisco
- الدفاع ضد تهديد جدار الحماية (FTD) الظاهري
- تدفق مصادقة VPN

المكونات المستخدمة

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8

- Cisco Secure Client 5.1.4.74
- محرر ملف التعريف (Windows) 5.1.4.74

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

CertificateMatch هي ميزة تسمح للمسؤولين بتكوين المعايير التي يجب على العميل إستخدامها لتحديد شهادة عميل للمصادقة مع خادم VPN. ويتم تحديد هذا التكوين في ملف تعريف العميل، وهو ملف XML يمكن إدارته باستخدام محرر ملف التعريف أو تحريره يدويا. يمكن إستخدام ميزة CertificateMatch لتعزيز أمان إتصالات VPN عن طريق ضمان إستخدام شهادة ذات سمات محددة فقط لاتصال VPN.

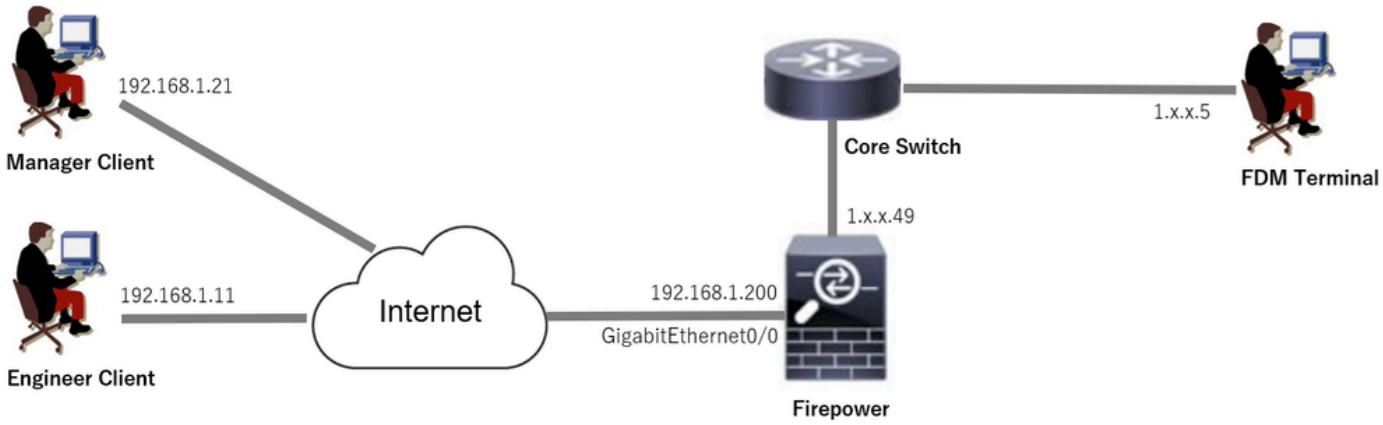
يوضح هذا المستند كيفية مصادقة عميل Cisco الآمن باستخدام الاسم الشائع من شهادة SSL.

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

- أ ك: 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 FDM

الخطوة 1. تكوين واجهة FTD

انتقل إلى الجهاز > الواجهات > عرض جميع الواجهات، وقم بتكوين الواجهة الداخلية والخارجية لـ FTD في علامة التبويب الواجهات.

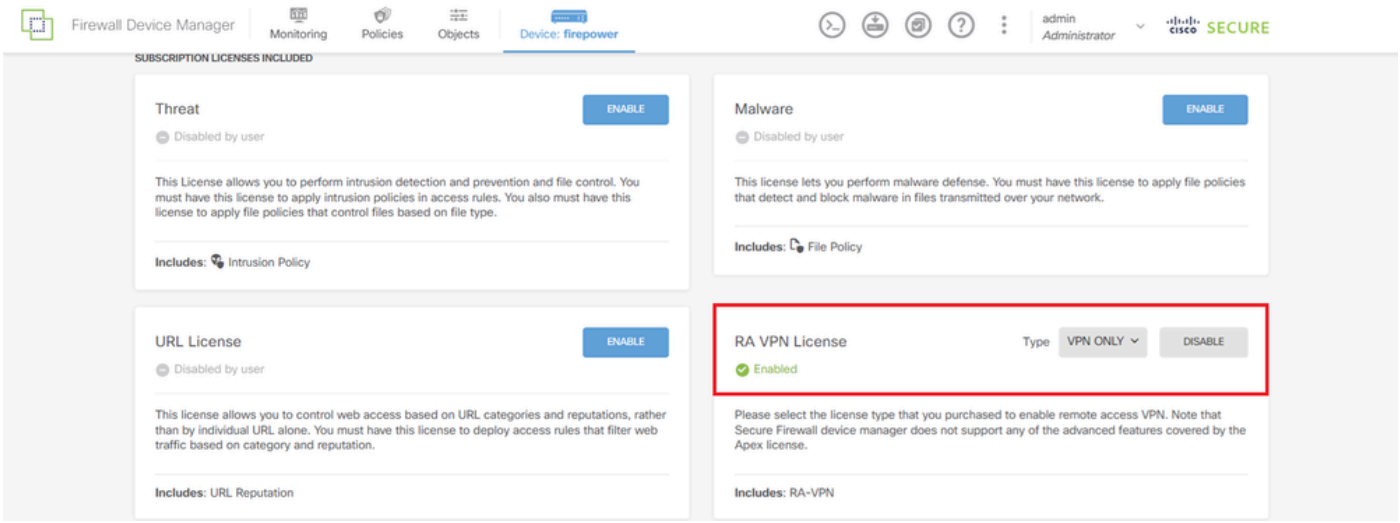
لـ GigabitEthernet0/0،

- الاسم: خارج
- عنوان IP: 192.168.1.200/24

واجهة FTD

الخطوة 2. تأكيد ترخيص Cisco Secure Client

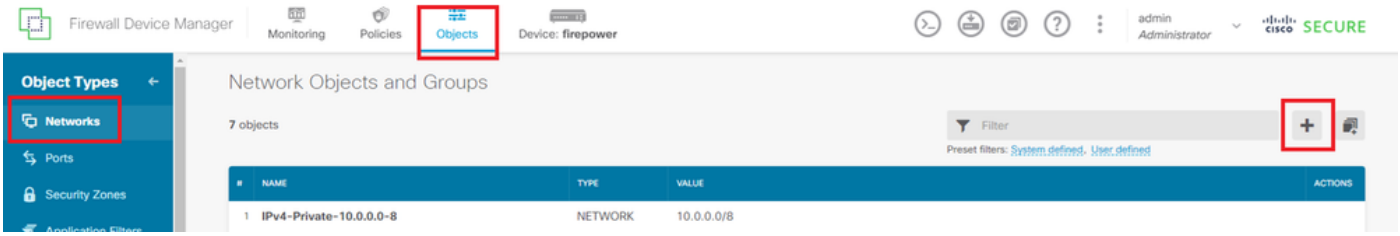
انتقل إلى الجهاز > الترخيص الذكي > عرض التكوين، أكد ترخيص Cisco Secure Client في عنصر ترخيص RA VPN.



ترخيص العميل الآمن

الخطوة 3. إضافة تجمع عناوين

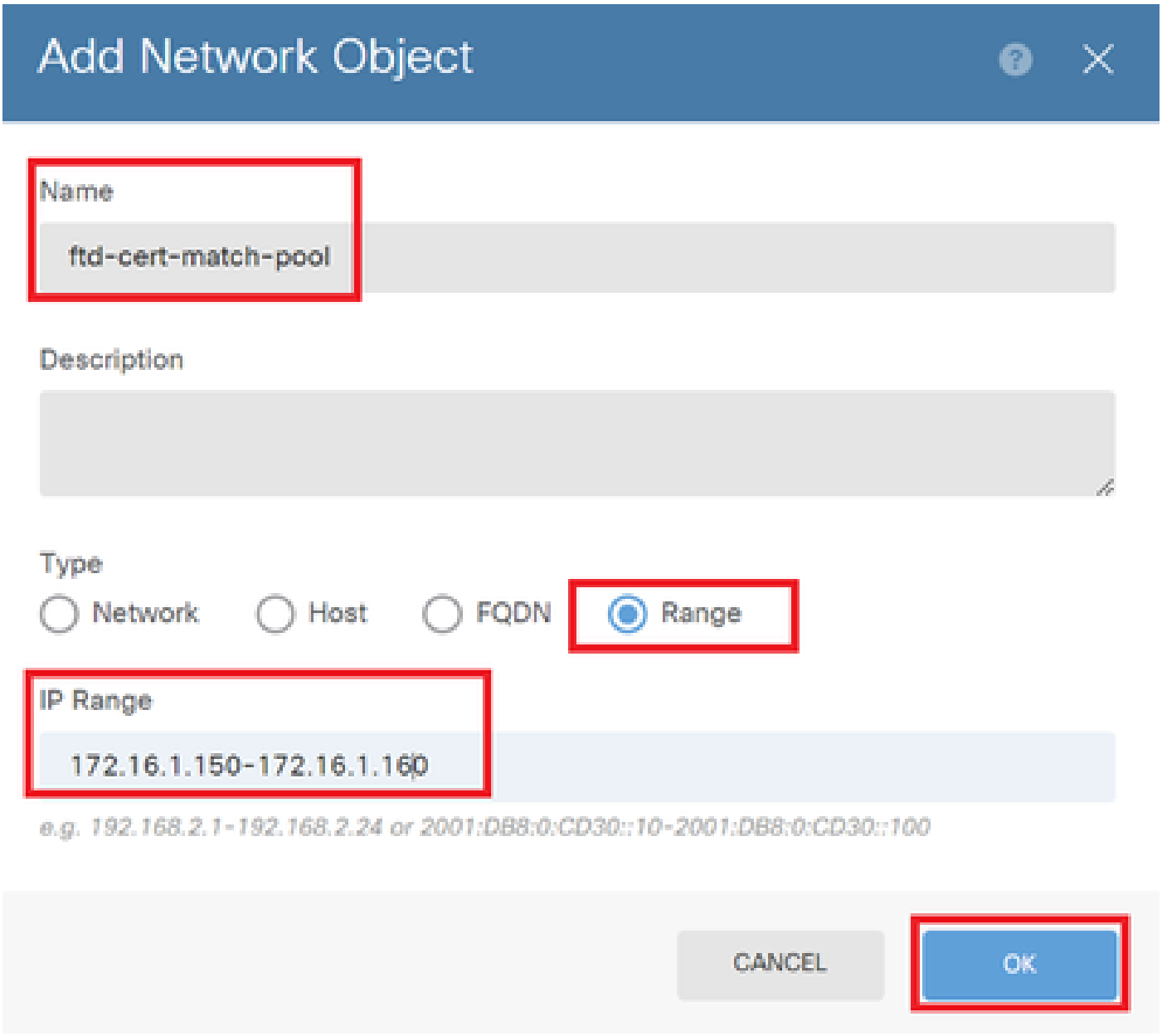
انتقل إلى كائنات > شبكات، انقر + زر.



إضافة تجمع عناوين

أدخل المعلومات الضرورية لإضافة تجمع عناوين IPv4 جديد. انقر فوق الزر موافق.

- الاسم: ftd-cert-match-pool
- النوع: النطاق
- نطاق IP: 172.16.1.150-172.16.1.160

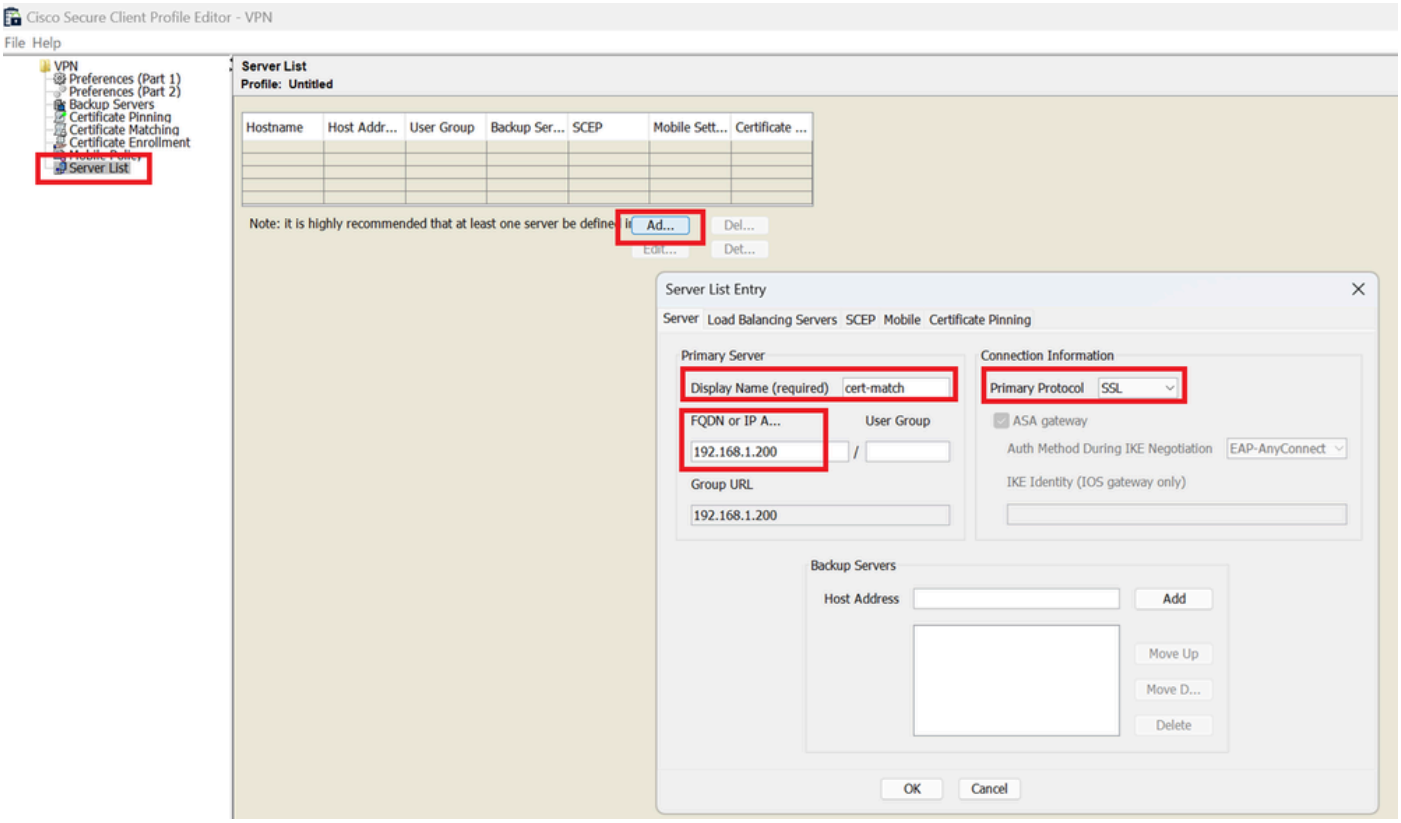


تفاصيل تجمع عناوين IPv4

الخطوة 4. إنشاء ملف تعريف عميل آمن

قم بتنزيل محرر ملف تعريف العميل الآمن وتثبيته من موقع برامج Cisco Software. انتقل إلى قائمة الخوادم، انقر فوق إضافة زر. أدخل المعلومات الضرورية لإضافة إدخال قائمة الخوادم وانقر فوق الزر موافق.

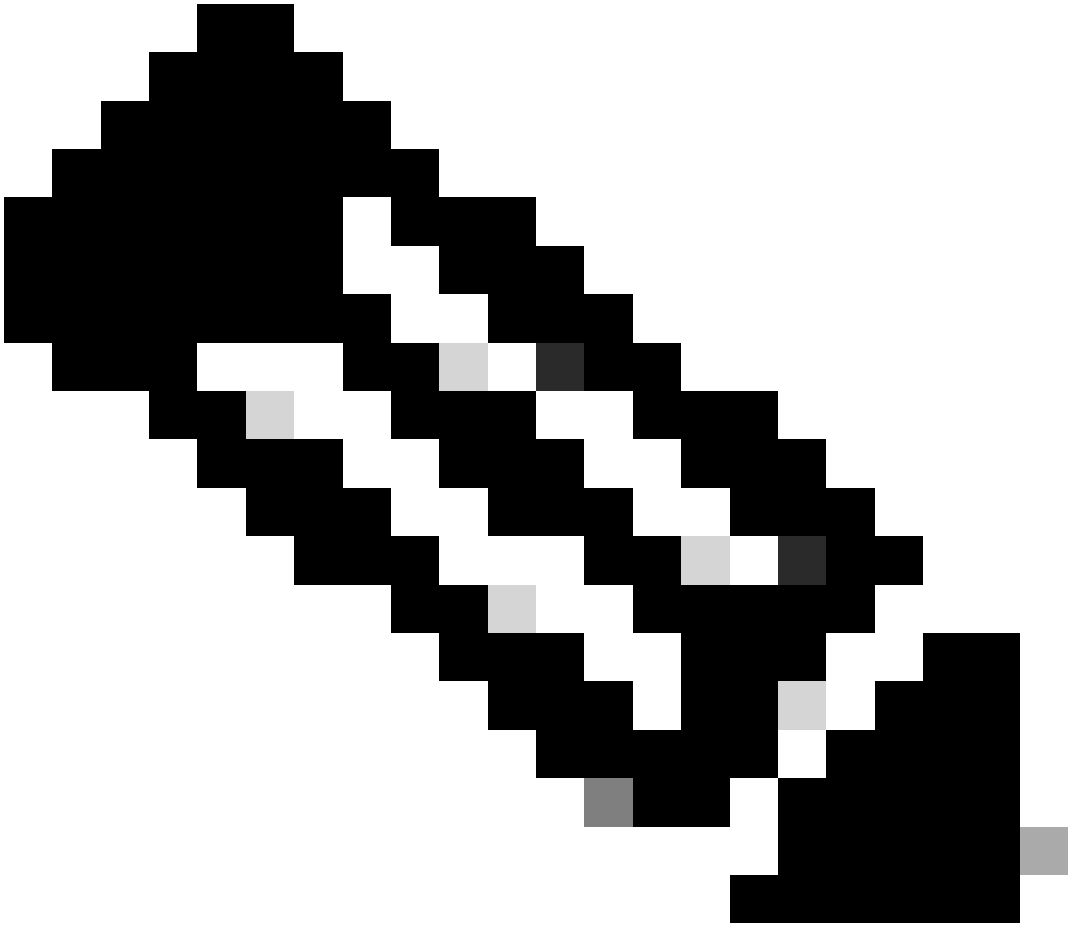
- اسم العرض: cert-match
- FQDN أو عنوان IP: 192.168.1.200
- البروتوكول الأساسي: SSL



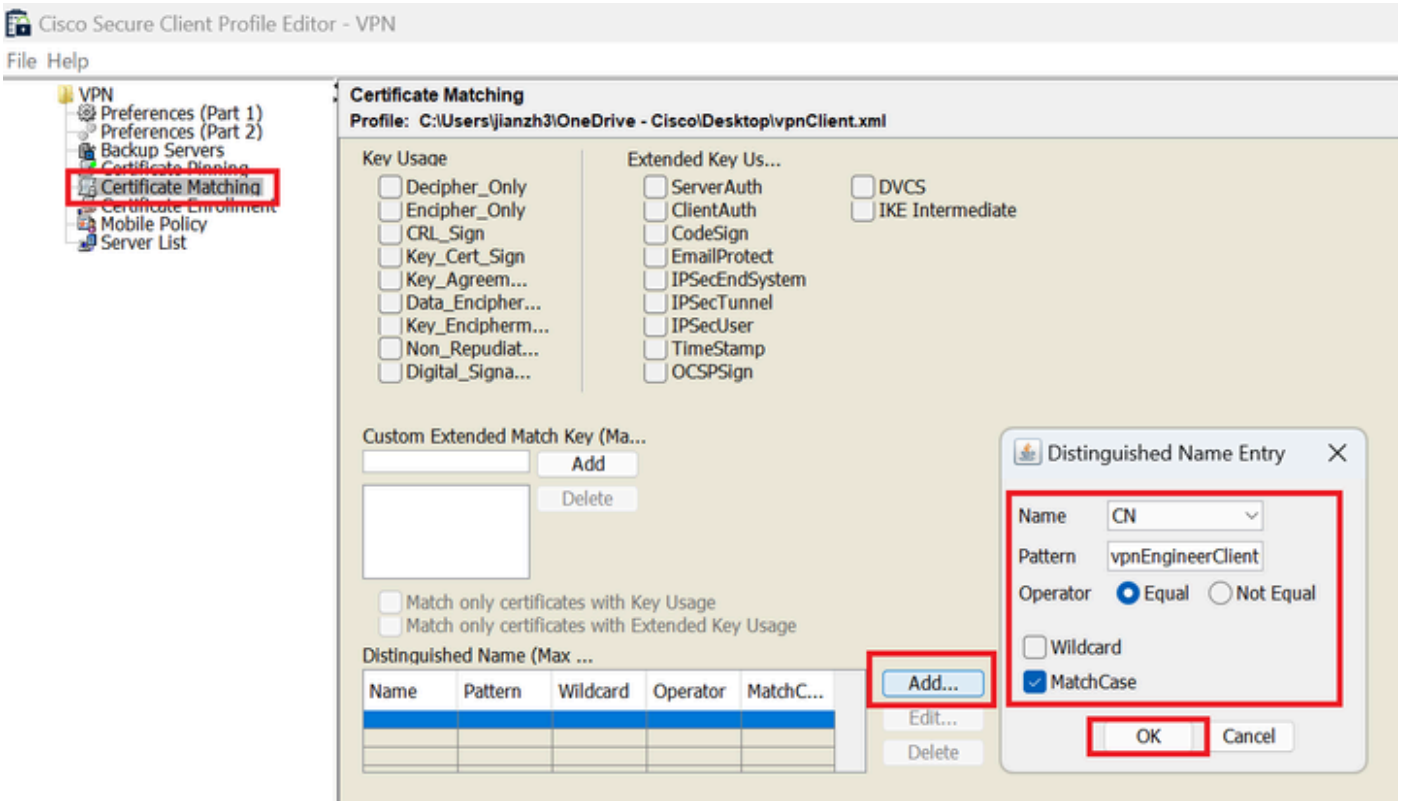
إدخال قائمة الخوادم

انتقل إلى مطابقة الشهادة، انقر فوق إضافة زر. أدخل المعلومات الضرورية لإضافة إدخال اسم مميز وانقر على زر موافق.

- الاسم: CN
- النمط: vpnEngineerClientCN
- عامل التشغيل: يساوي



ملاحظة: تحقق من خيار MatchCase في هذا المستند.



ادخال الاسم المميز

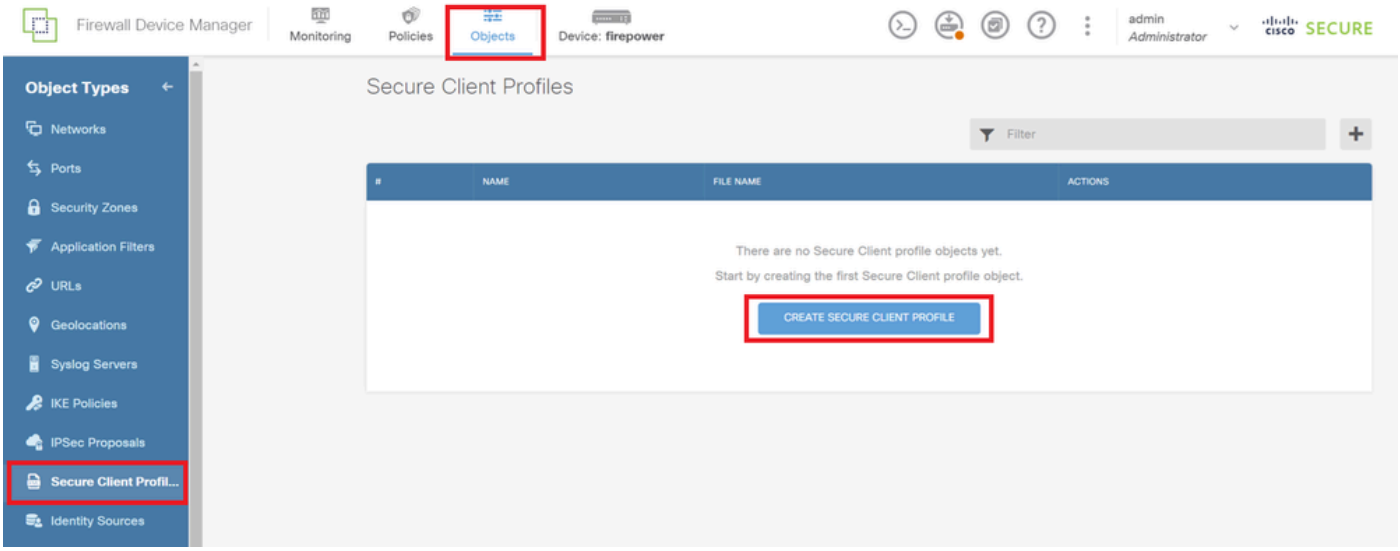
حفظ ملف تعريف العميل الآمن على الكمبيوتر المحلي وتأكيد تفاصيل ملف التعريف.

```
<CertificateMatch>
  <MatchOnlyCertsWithKU>false</MatchOnlyCertsWithKU>
  <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>
```

ملف تعريف العميل الآمن

الخطوة 5. تحميل ملف تعريف العميل الآمن إلى FDM

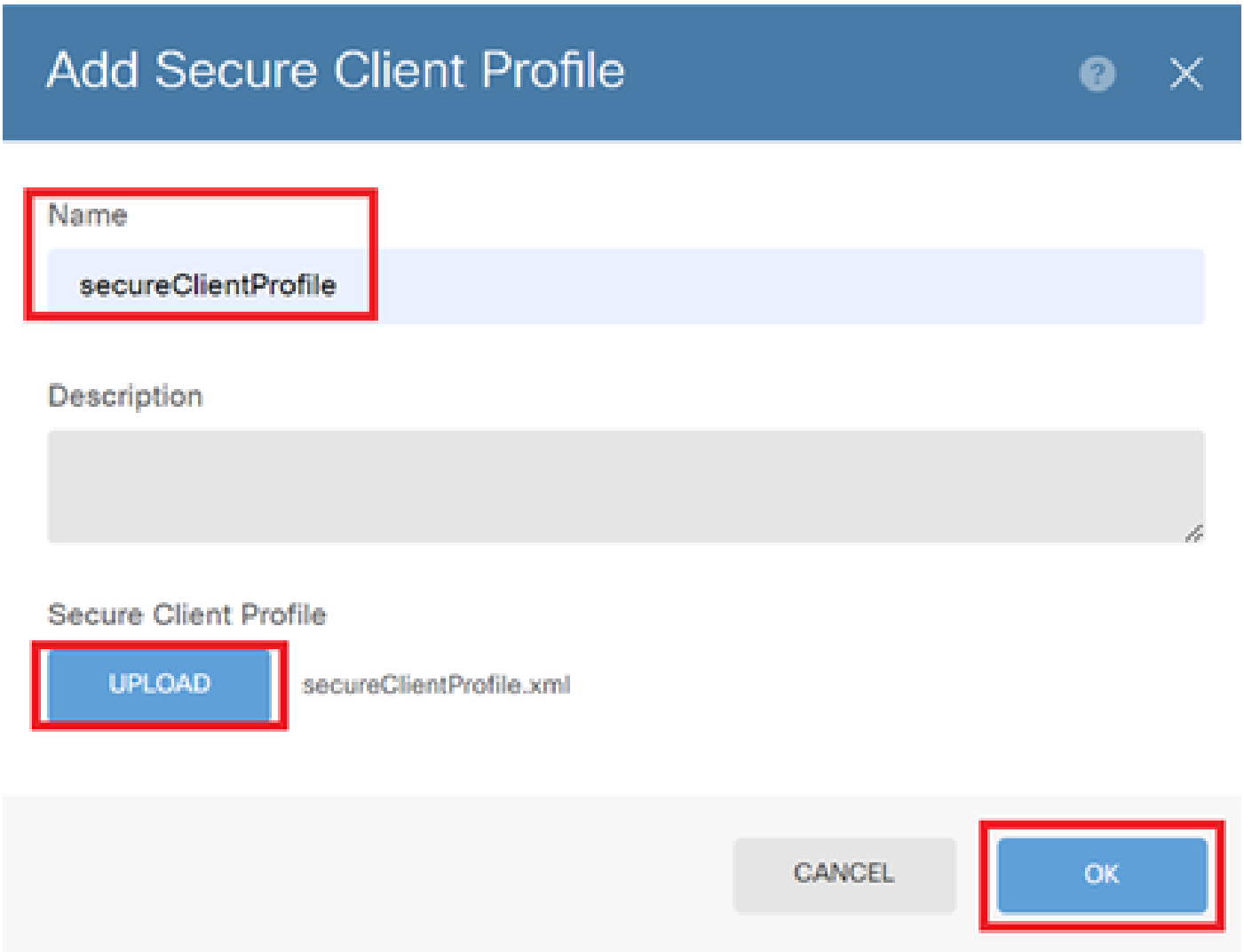
انتقل إلى كائنات > ملف تعريف عميل آمن، انقر على زر إنشاء ملف تعريف عميل آمن.



إنشاء ملف تعريف عميل آمن

أدخل المعلومات الضرورية لإضافة ملف تعريف عميل آمن وانقر فوق زر موافق.

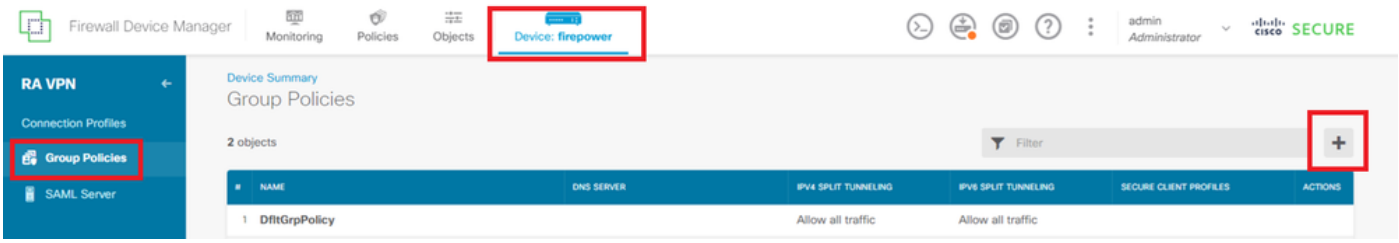
- الاسم: secureClientProfile
- ملف تعريف العميل الآمن: secureClientProfile.xml (تحميل من الكمبيوتر المحلي)



إضافة ملف تعريف عميل آمن

الخطوة 6. إضافة نهج المجموعة

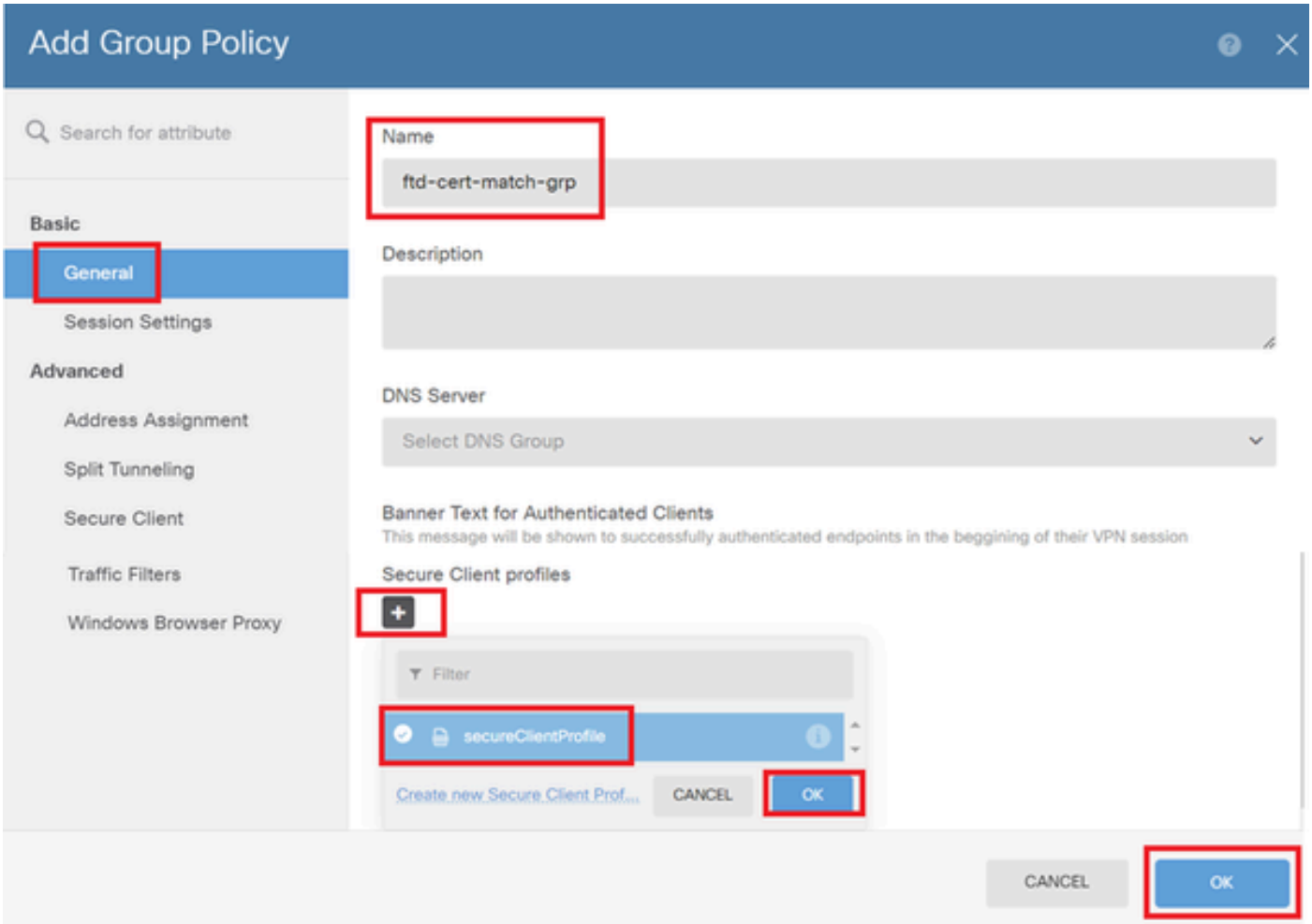
انتقل إلى الجهاز > Remote Access VPN (الوصول عن بعد) > View Configuration (عرض التكوين) > Group Policy (نهج المجموعة)، انقر فوق + زر.



إضافة نهج المجموعة

قم بإدخال المعلومات الضرورية لإضافة نهج مجموعة وانقر فوق زر موافق.

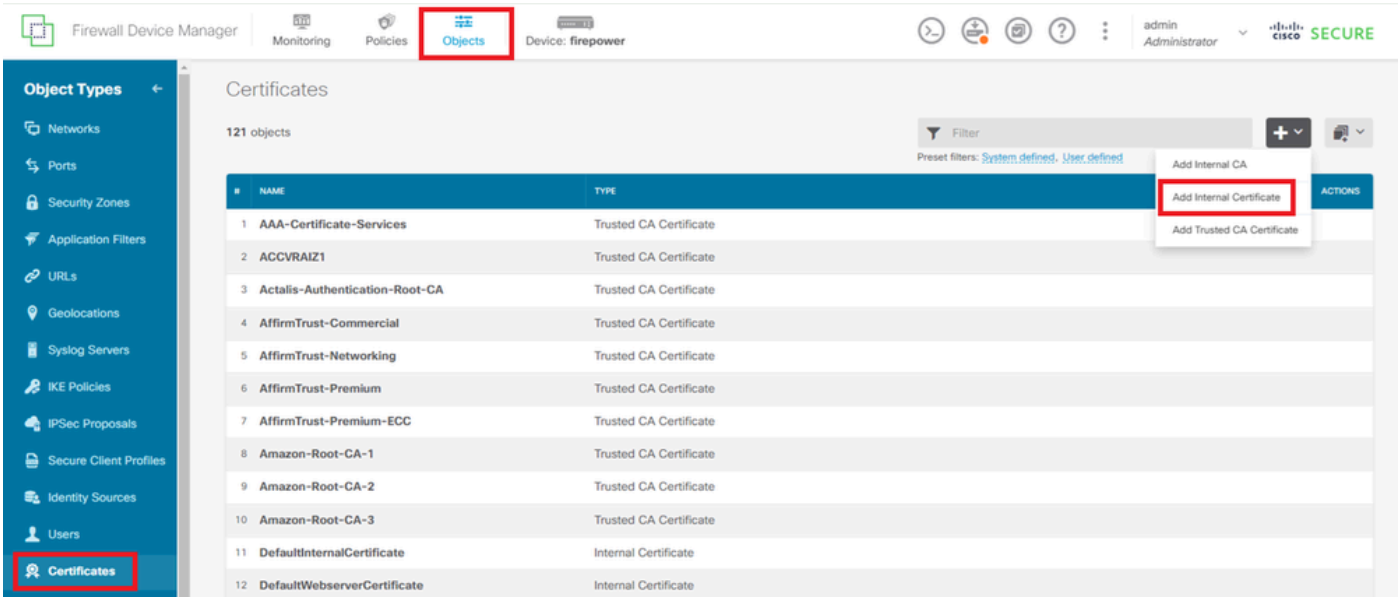
- الاسم: ftd-cert-match-grp
- ملفات تعريف العميل الآمنة: secureClientProfile



تفاصيل نهج المجموعة

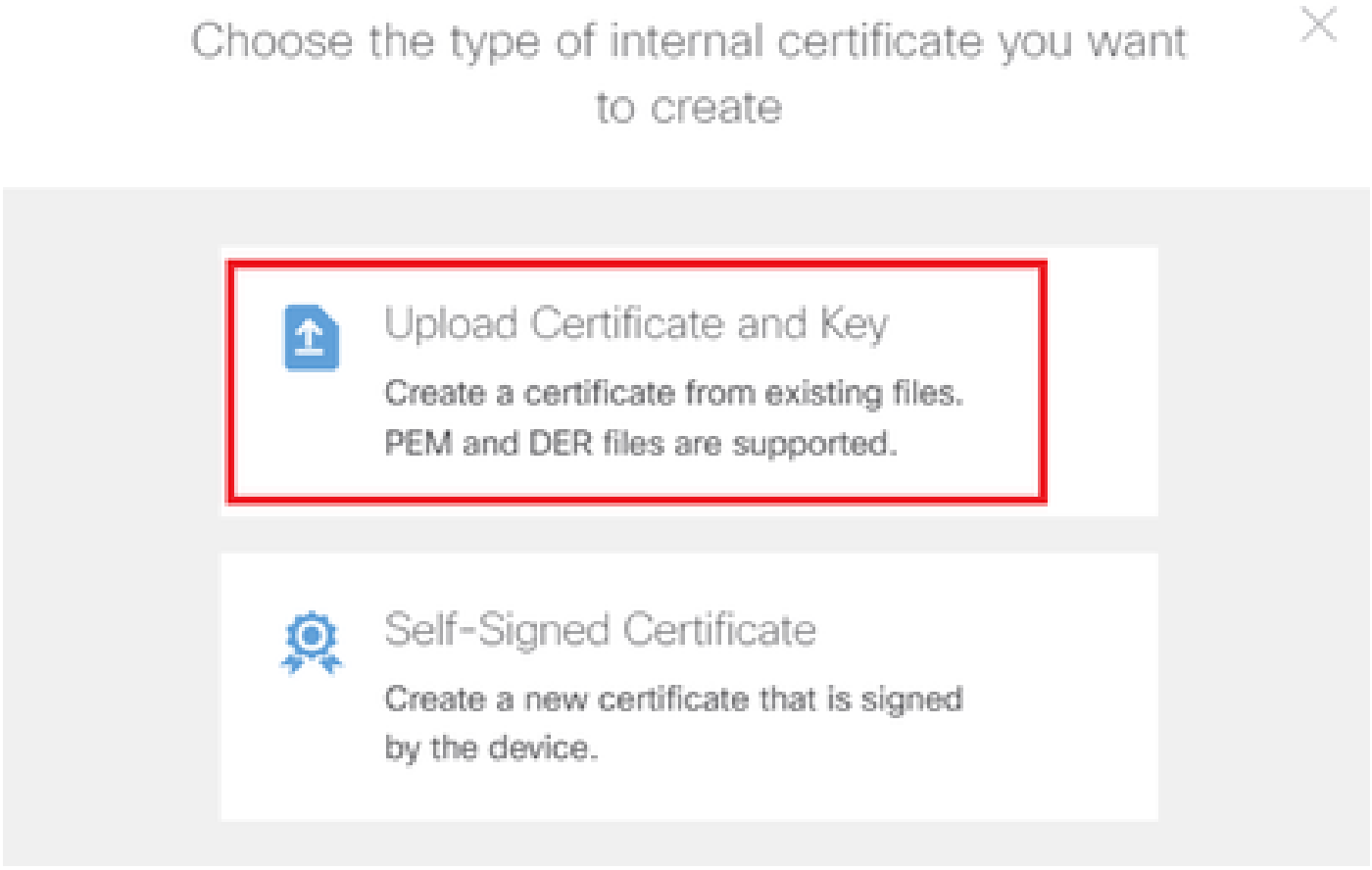
الخطوة 7. إضافة شهادة FTD

انتقل إلى كائنات > شهادات، انقر إضافة شهادة داخلية من + عنصر.



إضافة شهادة داخلية

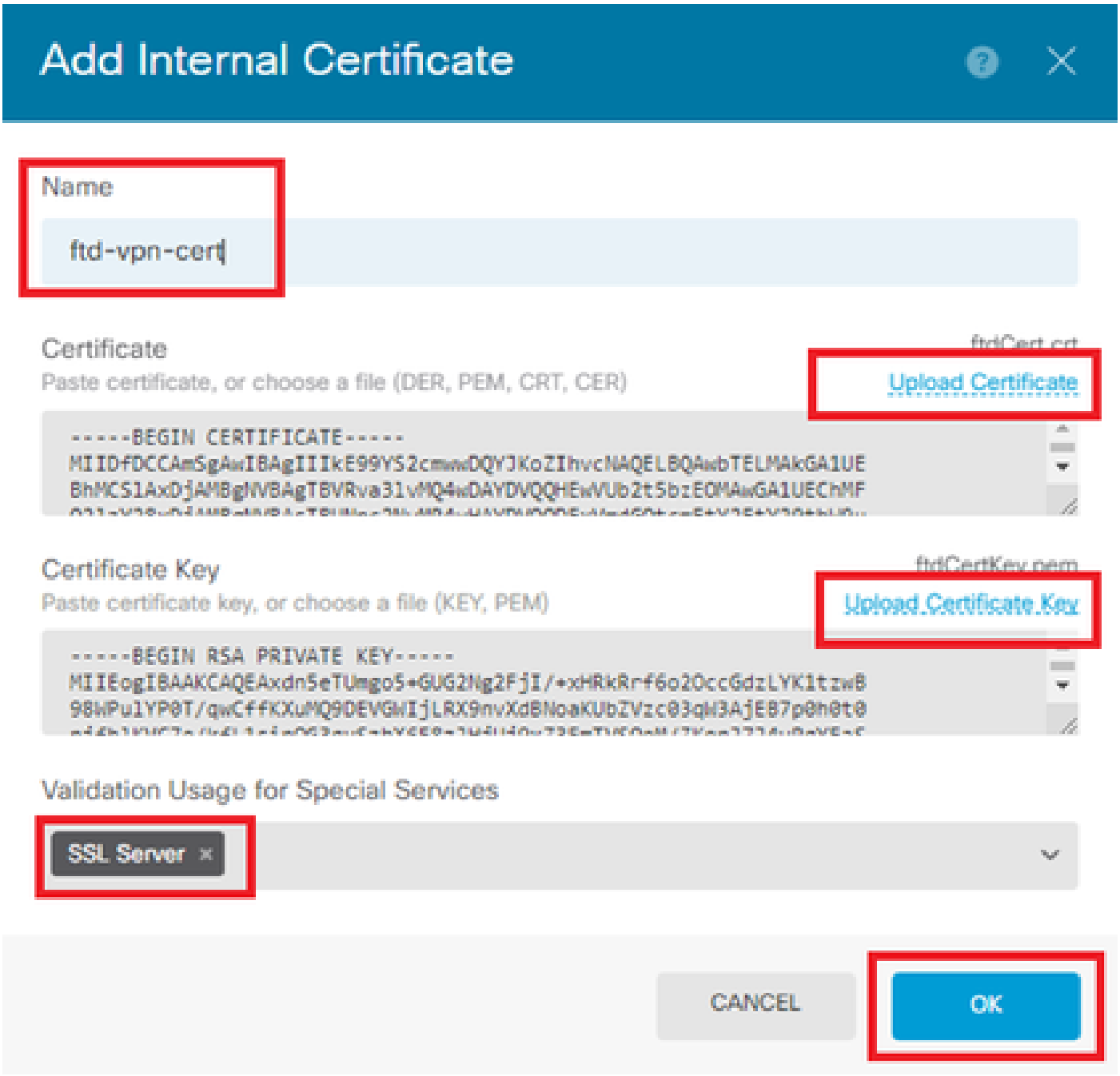
انقر على تحميل الشهادة والمفتاح.



تحميل الشهادة والمفتاح

أدخل المعلومات الضرورية لشهادة FTD، ثم قم باستيراد شهادة ومفتاح ترخيص من الكمبيوتر المحلي ثم انقر على زر موافق.

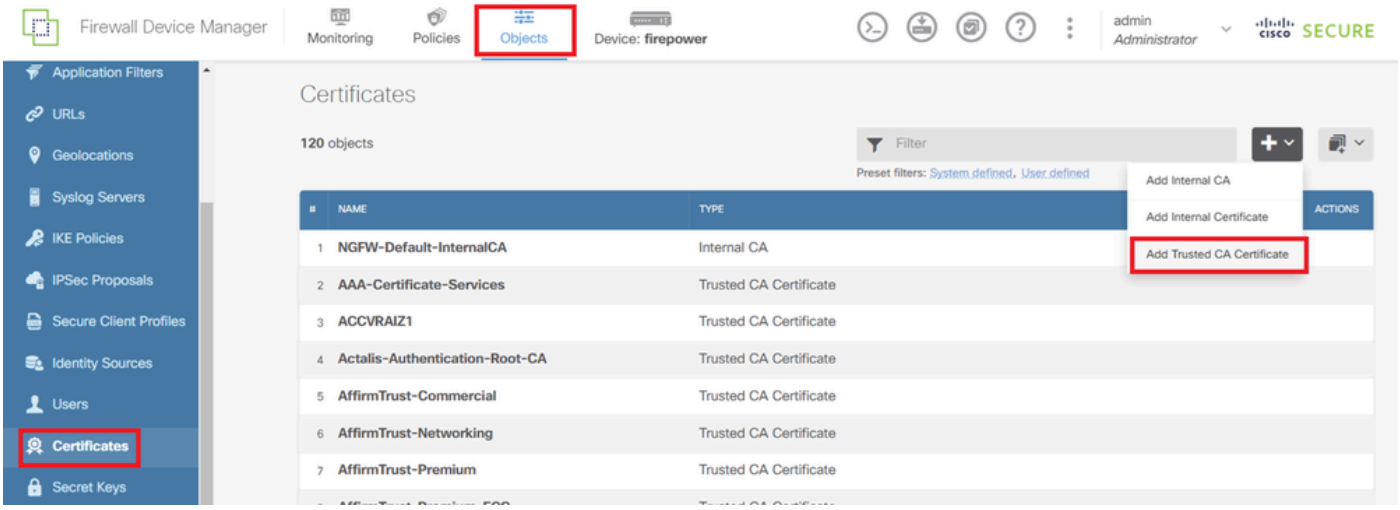
- الاسم: ftd-vpn-cert
- إستخدام التحقق من الصحة للخدمات الخاصة: خادم SSL



تفاصيل الشهادة الداخلية

الخطوة 8. إضافة CA إلى FTD

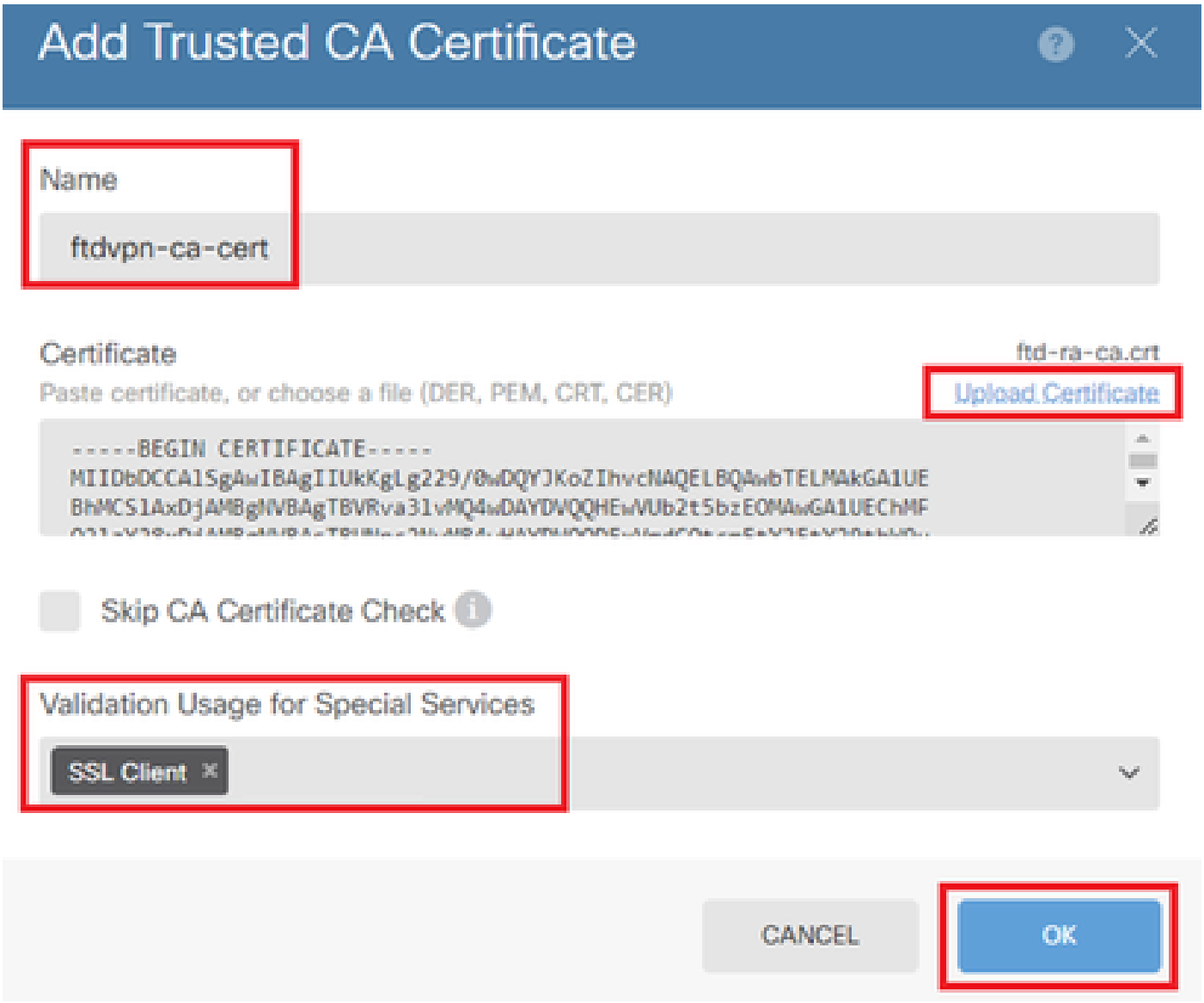
انتقل إلى كائنات > شهادات، انقر إضافة شهادة مرجع مصدق ثقة من + عنصر.



إضافة شهادة مرجع مصدق ثقة

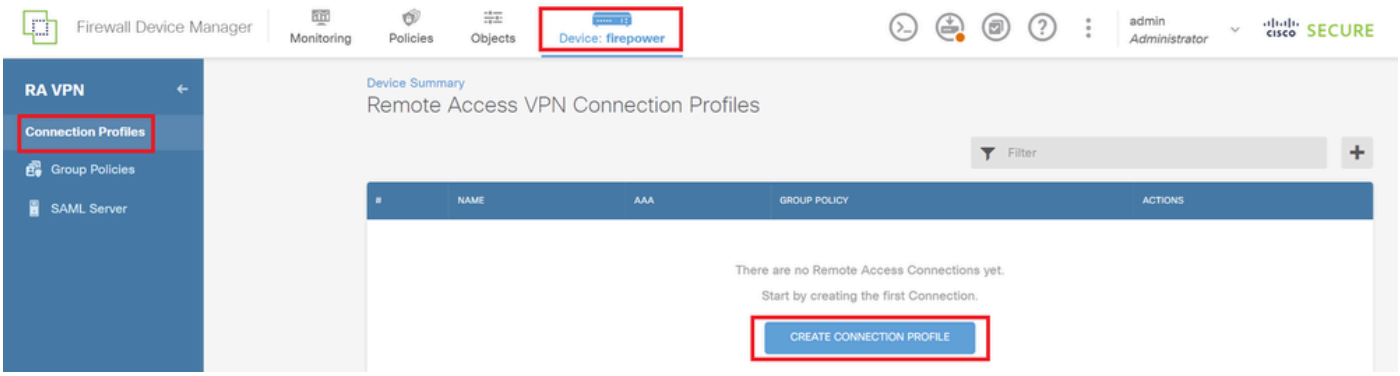
أدخل المعلومات اللازمة لـ CA، ثم استورد شهادة من الكمبيوتر المحلي.

- الاسم: ftdvpn-ca-cert
- إستخدام التحقق من الصحة للخدمات الخاصة: عميل SSL



الخطوة 9. إضافة ملف تعريف اتصال VPN للوصول عن بعد

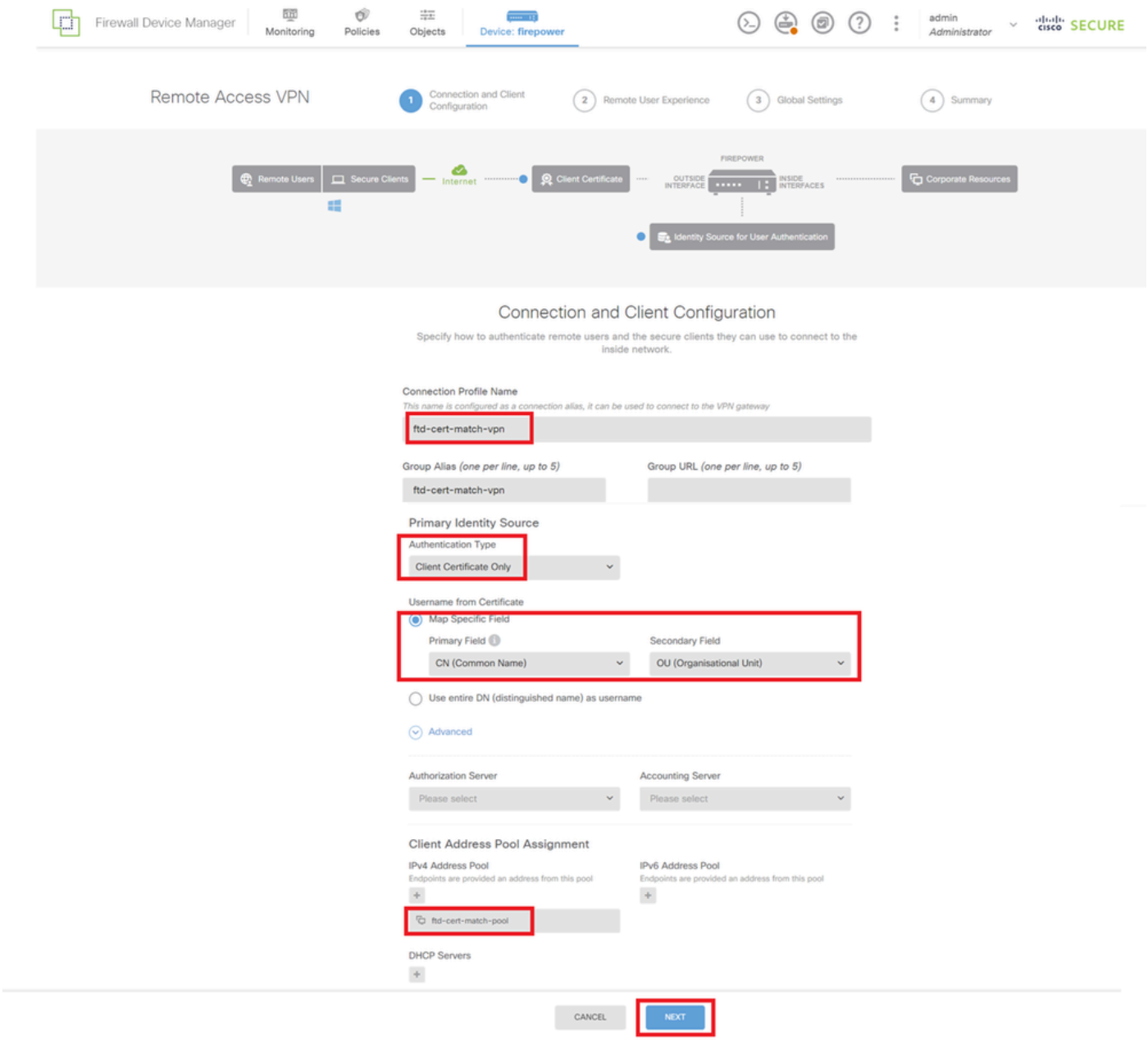
انتقل إلى الجهاز > Remote Access VPN (الوصول عن بعد) > View Configuration (عرض التكوين) > Connection Profile (ملفات تعريف الاتصال)، انقر فوق زر إنشاء ملف تعريف الاتصال.



إضافة ملف تعريف اتصال VPN للوصول عن بعد

أدخل المعلومات الضرورية لملف تعريف الاتصال وانقر على زر التالي.

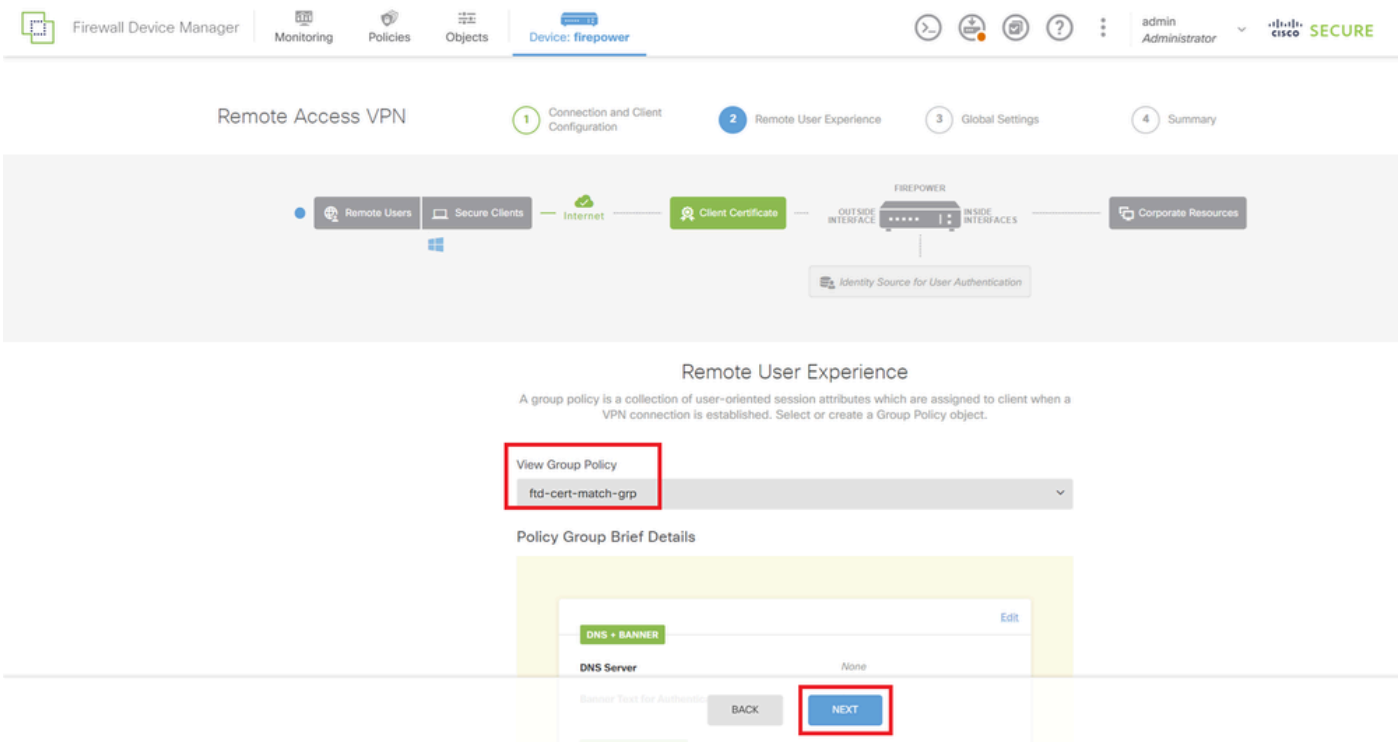
- اسم ملف تعريف الاتصال: ftd-cert-match-vpn
- نوع المصادقة: شهادة العميل فقط
- اسم المستخدم من الشهادة: حقل محدد للتعيين
- الحقل الأساسي: CN (الاسم الشائع)
- الحقل الثانوي: OU (الوحدة التنظيمية)
- تجمعات عناوين IPv4: ftd-cert-match-pool



تفاصيل ملف تعريف اتصال VPN

قم بإدخال المعلومات الضرورية لنهج المجموعة وانقر فوق الزر التالي.

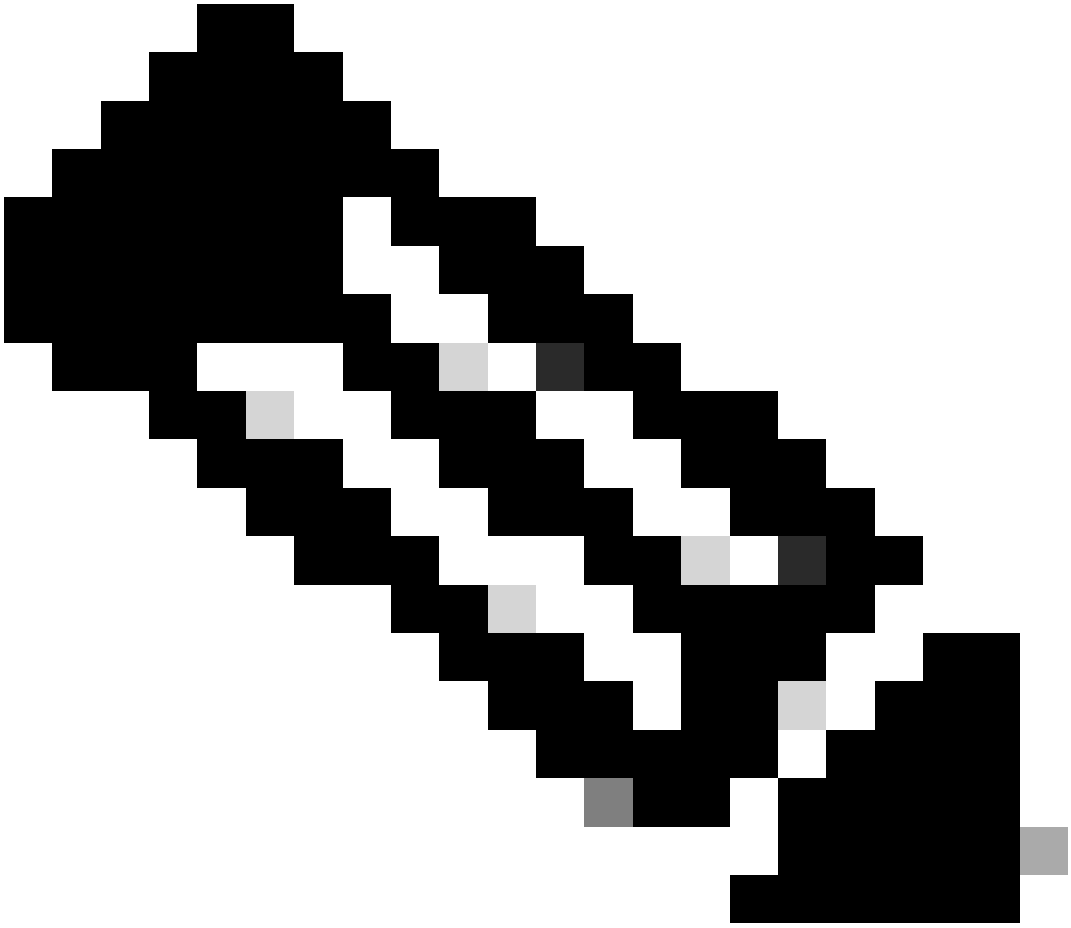
- عرض نهج المجموعة: ftd-cert-match-grp



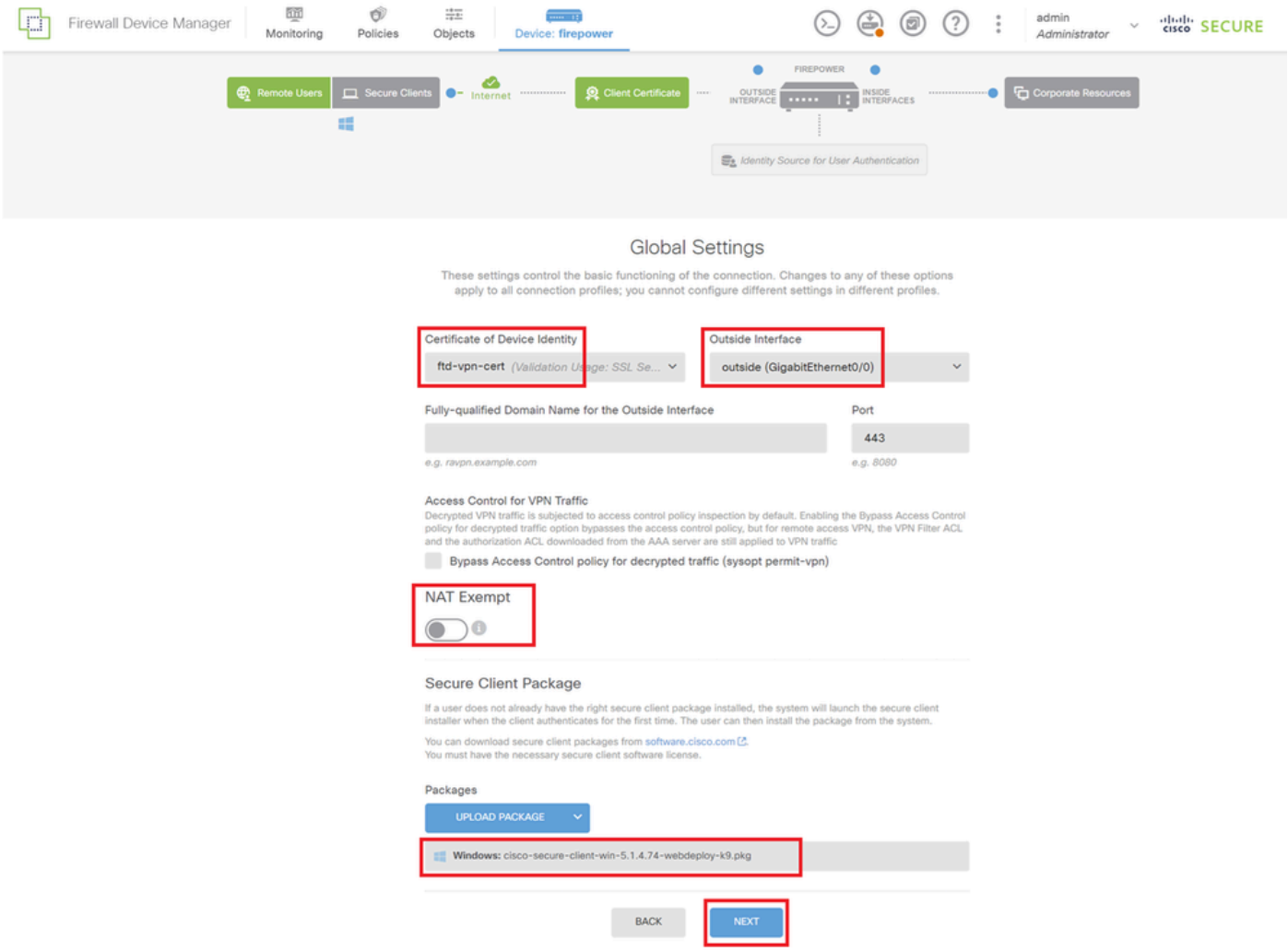
تحديد نهج المجموعة

حدد شهادة هوية الجهاز، واجهة خارجية، حزمة العميل الآمنة لاتصال VPN.

- شهادة هوية الجهاز: ftd-vpn-cert
- الواجهة الخارجية: خارج (GigabitEthernet0/0)
- حزمة العميل الآمنة: Cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



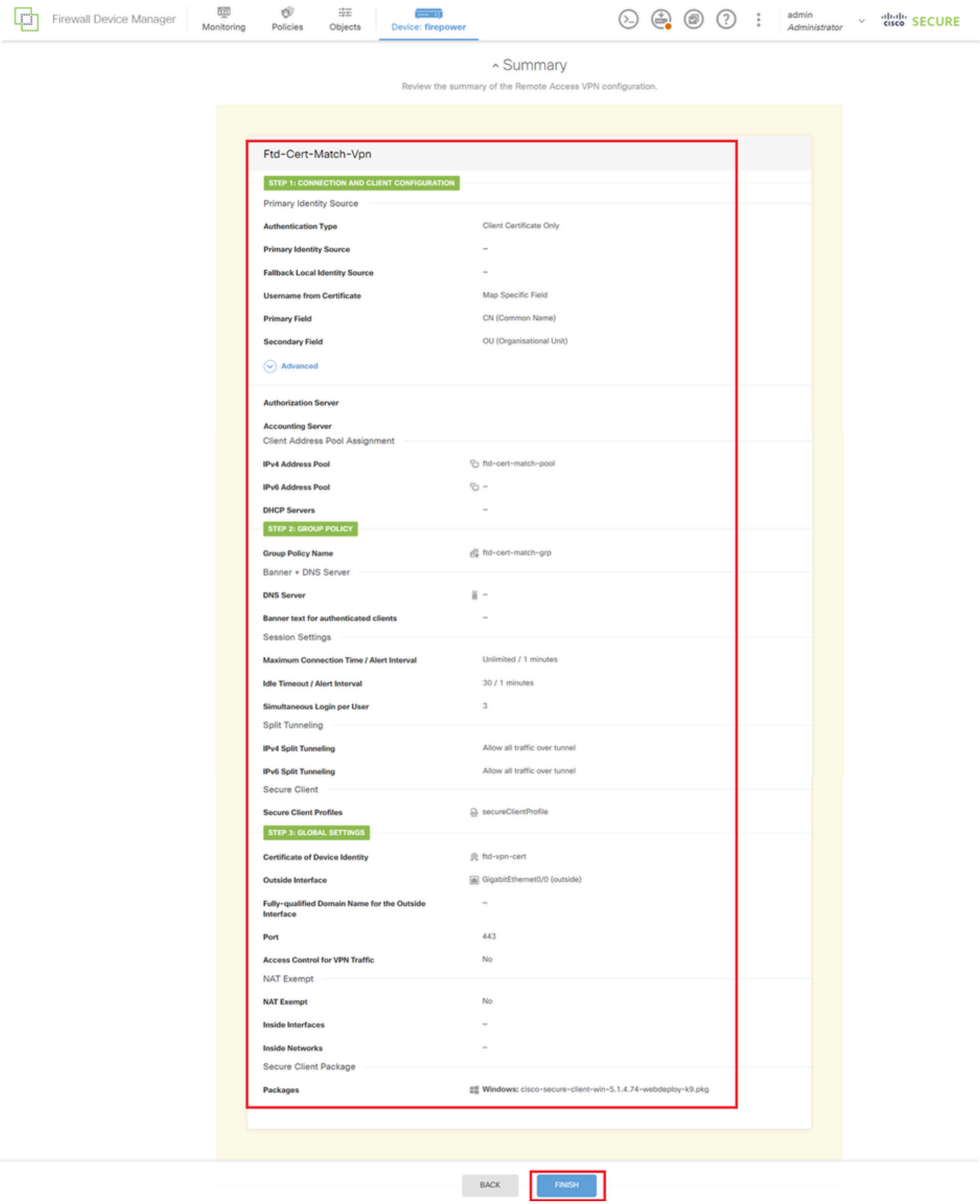
ملاحظة: ميزة إستثناء NAT المعطل في هذا المستند.



تفاصيل الإعدادات العمومية

الخطوة 10. تأكيد الملخص لملف تعريف الاتصال

أكدت المعلومة دخلت ل VPN توصيل وطقطقة إنجاز زر.



تأكيد الملخص لملف تعريف الاتصال

التأكيد في واجهة سطر الأوامر (CLI) الخاصة ب FTD

تأكيد إعدادات اتصال VPN في واجهة سطر الأوامر (CLI) ل FTD بعد النشر من FDM.

```
// 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
```

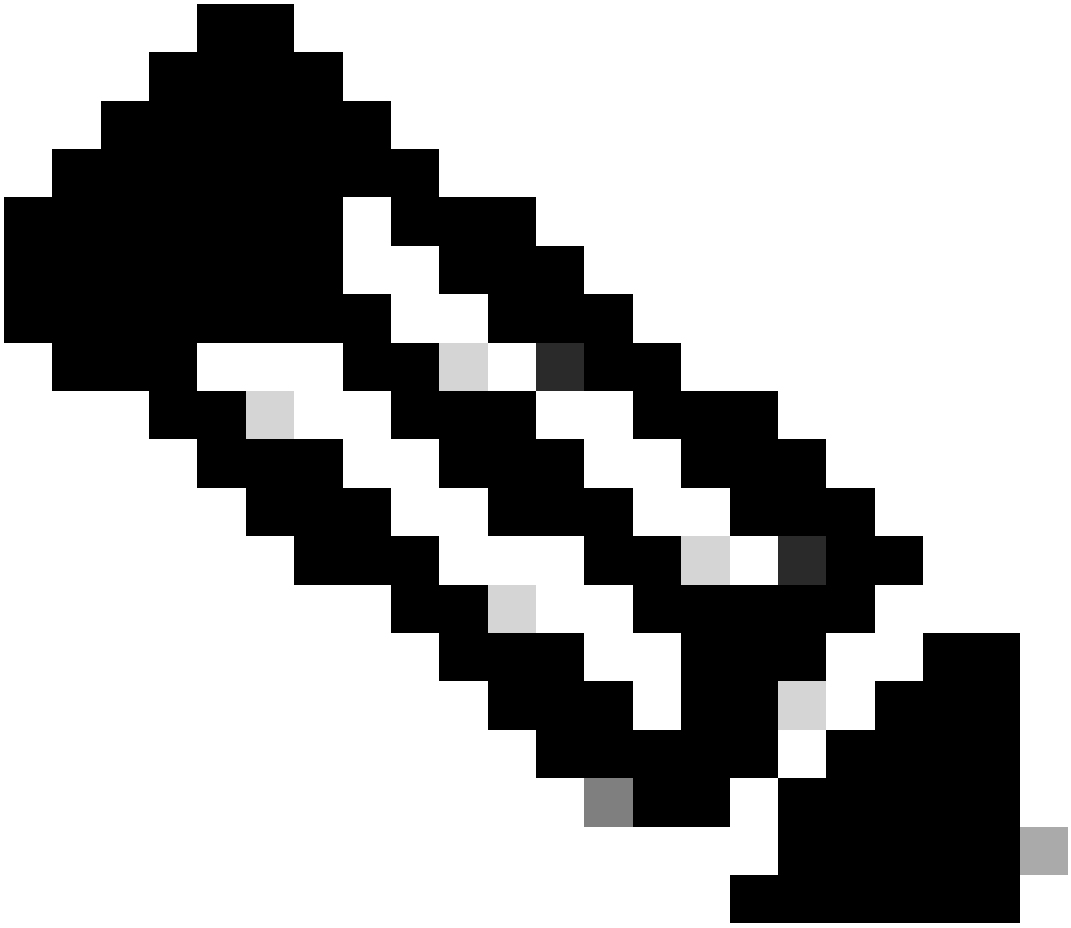
```
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
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
```

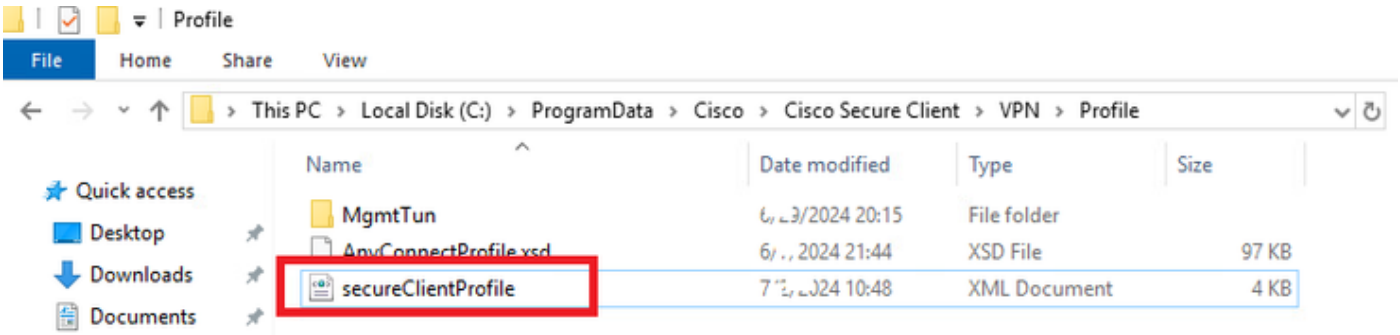
أتأكيد في عميل شبكة VPN

الخطوة 1. نسخ ملف تعريف العميل الآمن إلى عميل VPN

انسخ ملف تعريف العميل الآمن إلى عميل VPN للمهندس وعميل VPN للمدير.



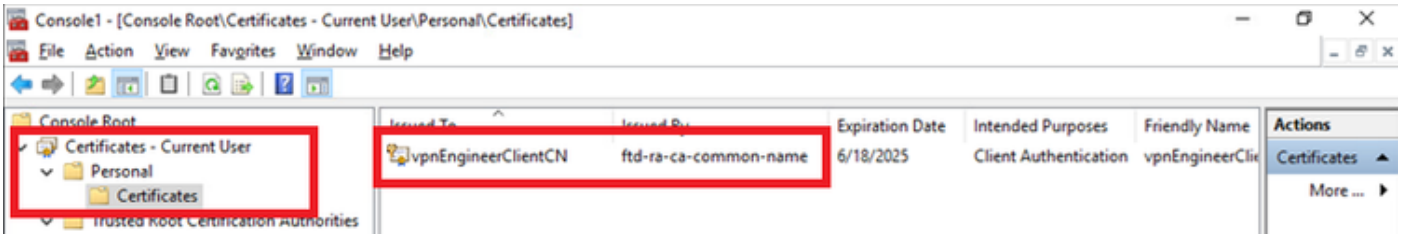
ملاحظة: دليل ملف تعريف العميل الآمن في كمبيوتر Windows: C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



نسخ ملف تعريف العميل الآمن إلى عميل VPN

الخطوة 2. تأكيد شهادة العميل

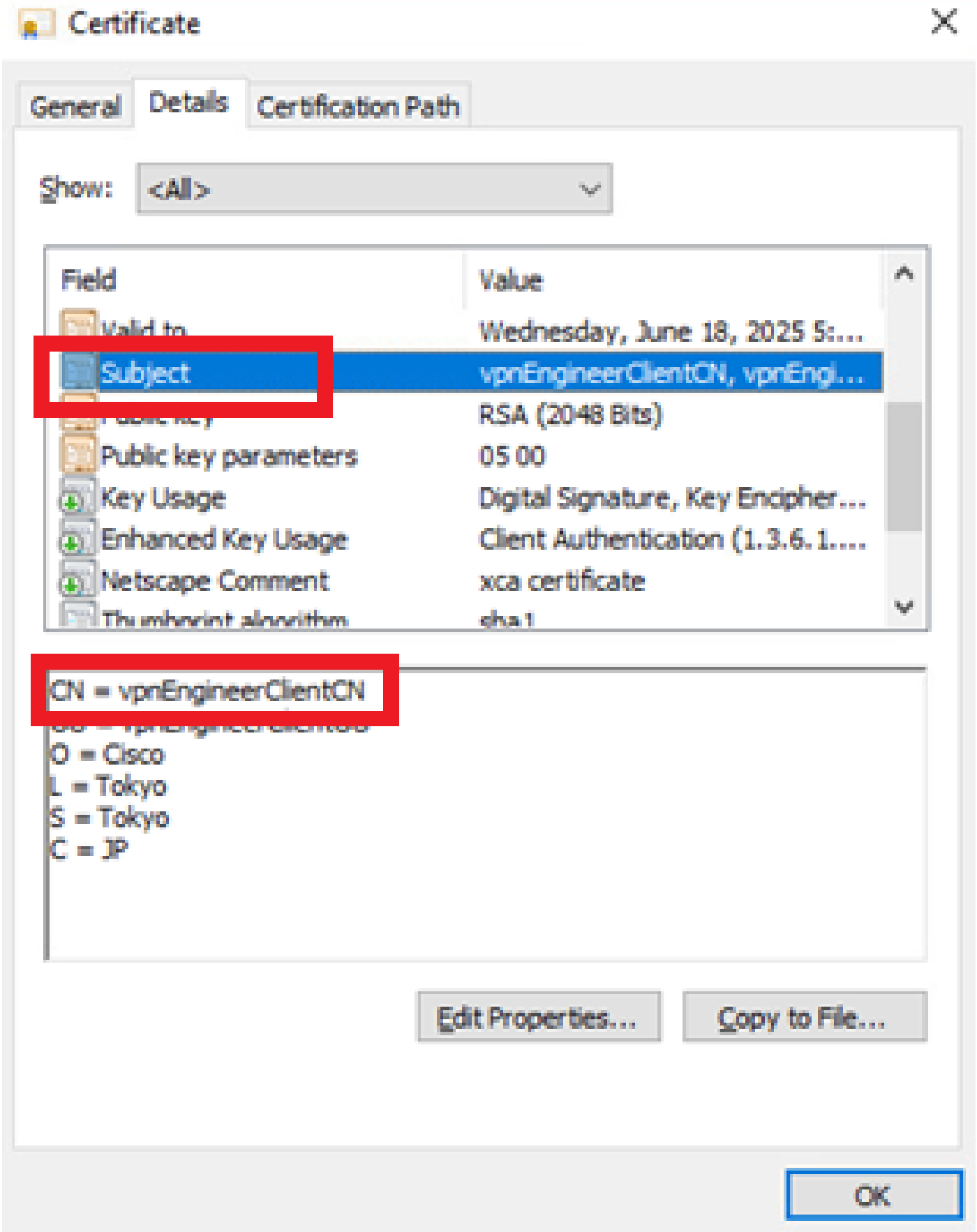
في عميل شبكة VPN الهندسية، انتقل إلى الشهادات - مستخدم حالي > شخصي > شهادات، تحقق من شهادة العميل المستخدمة للمصادقة.



تأكيد الشهادة لعميل Engineer VPN

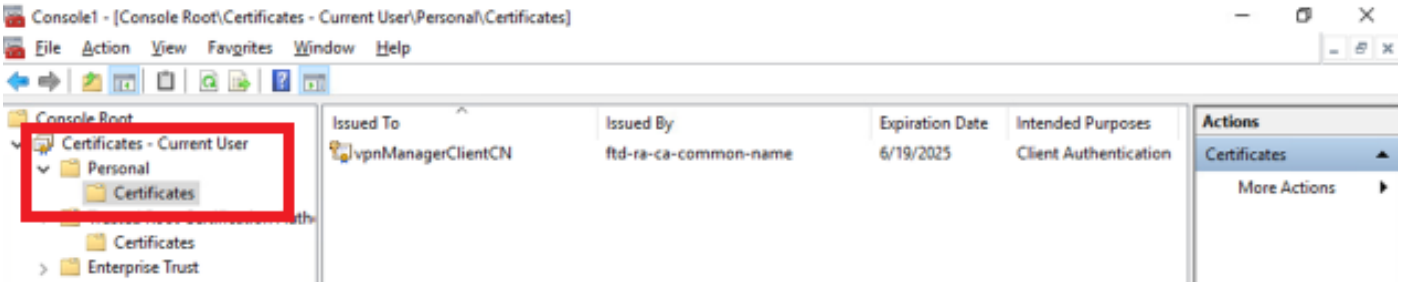
انقر نقرا مزدوجا فوق شهادة العميل، ثم انتقل إلى التفاصيل، ثم تحقق من تفاصيل الموضوع.

- الموضوع: CN = vpnEngineerClientCN



تفاصيل شهادة عميل المهندس

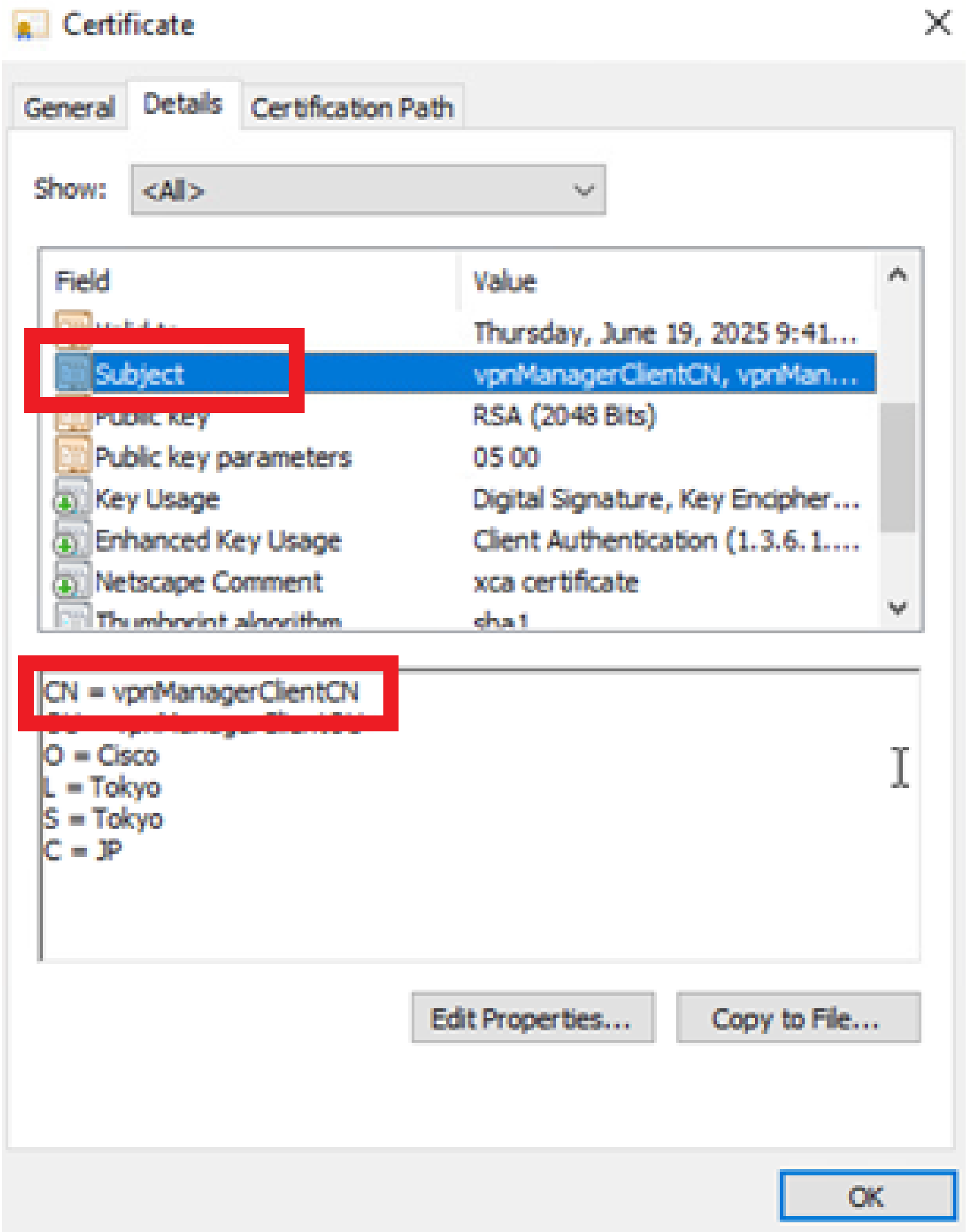
في عميل Manager VPN، انتقل إلى الشهادات - مستخدم حالي > شخصي > شهادات، تحقق من شهادة العميل المستخدمة للمصادقة.



تأكيد الشهادة لعميل Manager VPN

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

- الموضوع: CN = vpnManagerClientCN

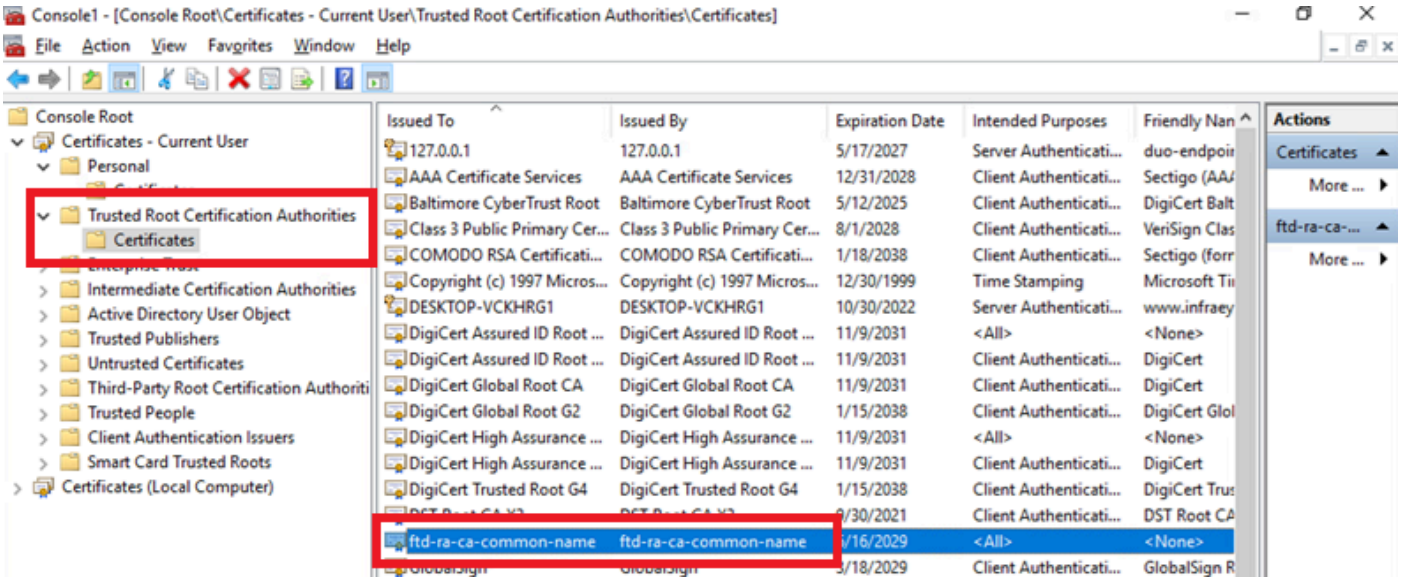


تفاصيل شهادة عميل المدير

الخطوة 3. 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

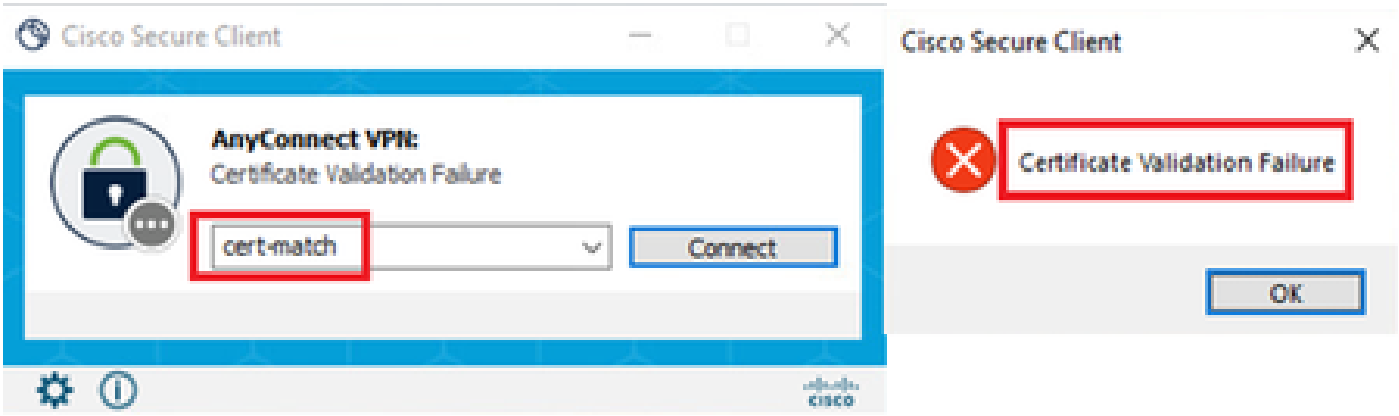
التحقق من الصحة

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.

نجح اتصال VPN لعميل Engineer VPN

في عميل "الشبكة الخاصة الظاهرية (VPN) للمدير"، ابدأ اتصال "العميل الآمن من Cisco". فشل اتصال شبكة VPN بسبب فشل التحقق من صحة الشهادة.



فشل اتصال VPN لعميل Manager VPN

الخطوة 2. تأكيد جلسات عمل VPN في FTD CLI

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

```
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 : 0000000000200006683932b
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

استكشاف الأخطاء وإصلاحها

يمكنك توقع العثور على معلومات حول مصادقة VPN في تصحيح الأخطاء syslog من Lina engine وفي ملف DART على جهاز كمبيوتر Windows.

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

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

معلومات ذات صلة

تكوين خدمة إدارة FDM في الحرم لـ Firepower 2100
تكوين شهادة VPN للوصول عن بعد على FTD المدارة بواسطة FDM
تكوين syslog والتحقق من صحته في FirePOWER Device Manager

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).