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

المحتويات

المقدمة

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

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

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

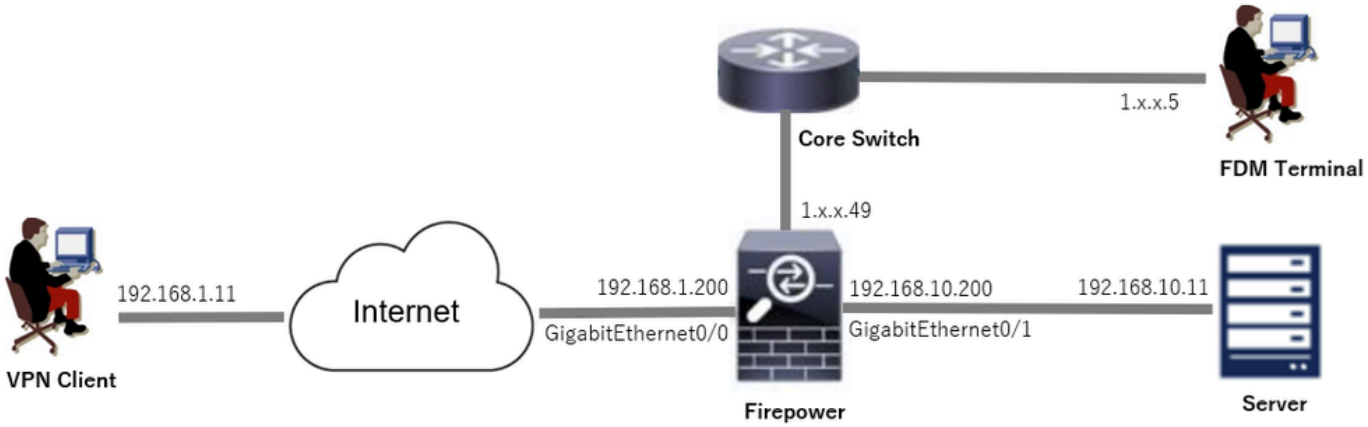
مدير أجهزة Firepower (FDM) هو واجهة إدارة مبسطة قائمة على الويب تستخدم لإدارة أجهزة الدفاع عن تهديد الحماية (FTD) من Cisco. تسمح إدارة أجهزة FirePOWER لمسؤولي الشبكة بتكوين أجهزة FTD الخاصة بهم وإداراتها دون إستخدام مركز إدارة FirePOWER (FMC) الأكثر تعقيدا. يوفر FDM واجهة مستخدم سهلة الاستخدام للعمليات الأساسية مثل إعداد واجهات الشبكة ومناطق الأمان وسياسات التحكم في الوصول والشبكات الخاصة الظاهرية (VPN)، بالإضافة إلى مراقبة أداء الجهاز وأحداث الأمان. وهو مناسب لعمليات النشر الصغيرة إلى متوسطة الحجم حيث تكون الإدارة المبسطة مطلوبة.
يوضح هذا المستند كيفية دمج أسماء المستخدمين المعبأة مسبقا مع عميل Cisco Secure Client على FTD الذي تتم إدارته بواسطة FDM.
إذا كنت تقوم بإدارة FTD باستخدام FMC، فيرجى الرجوع إلى دليل تكوين المصادقة والتفويض والمحاسبة (AAA) ومصادقة الوحدة النمطية للعميل الآمن على FTD عبر FMC.

هذه هي سلسلة الشهادات التي لها الاسم الشائع لكل شهادة مستخدمة في المستند.

- أ ك: ftd-ra-ca-name الشائع
- 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 FDM

الخطوة 1. تكوين واجهة FTD

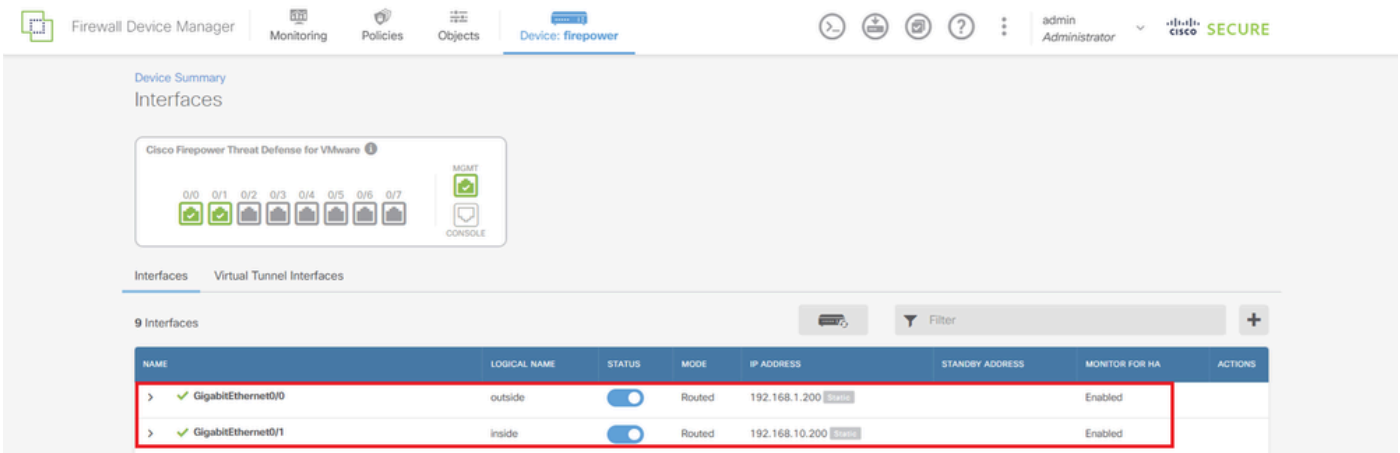
انتقل إلى الجهاز > الواجهات > عرض جميع الواجهات، وتكوين الواجهة الداخلية والخارجية ل FTD inInterfaceBaseAb.

ل GigabitEthernet0/0،

- الاسم: خارج
- عنوان IP: 192.168.1.200/24

ل GigabitEthernet0/1،

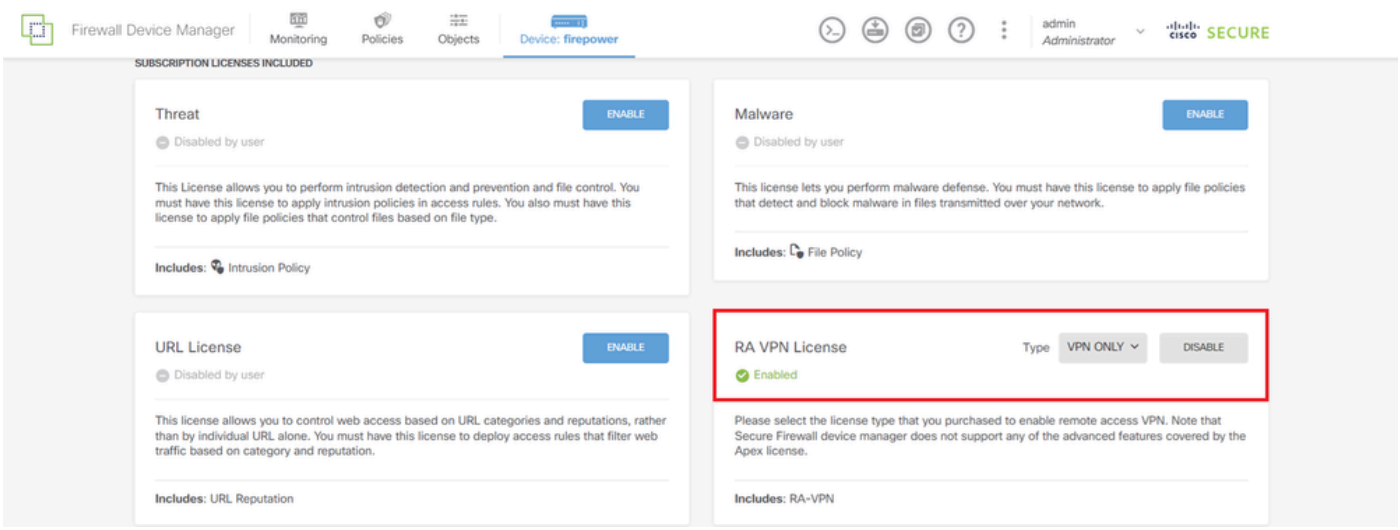
- الاسم: الداخل
- عنوان IP: 192.168.10.200/24



واجهة FTD

الخطوة 2. تأكيد ترخيص Cisco Secure Client

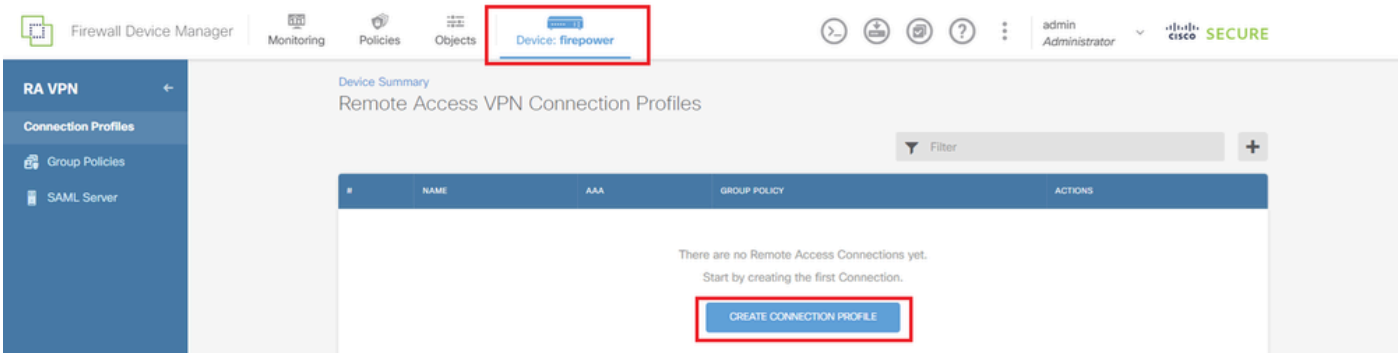
انتقل إلى الجهاز > الترخيص الذكي > عرض التكوين، وتأكد من ترخيص Cisco Secure Client في RA VPN LicenseItem.



ترخيص العميل الآمن

الخطوة 3. إضافة ملف تعريف اتصال VPN للوصول عن بعد

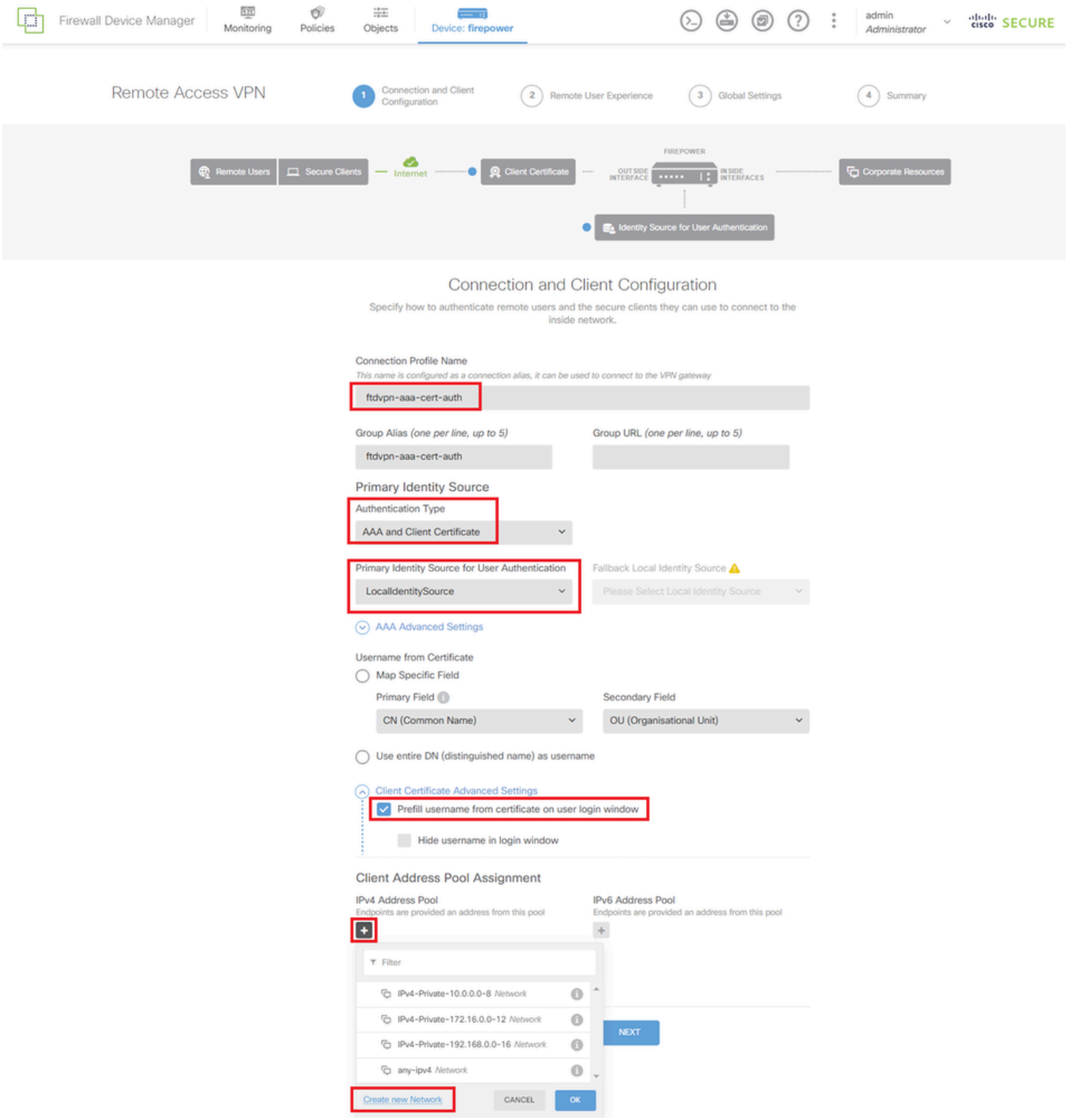
انتقل إلى الجهاز > Remote Access VPN (الوصول عن بعد) > View Configuration (عرض التكوين)، انقر فوق زر إنشاء ملف تعريف الاتصال.



إضافة ملف تعريف اتصال VPN للوصول عن بعد

أدخل المعلومات الضرورية لملف تعريف الاتصال وانقر فوق إنشاء زر شبكة جديد في عنصر تجمع عناوين IPv4.

- اسم ملف تعريف الاتصال: ftdvpn-aaa-cert-auth
- نوع المصادقة: المصادقة والتفويض والمحاسبة (AAA) وشهادة العميل
- مصدر الهوية الأساسي لمصادقة المستخدم: LocalIdentitySource
- الإعدادات المتقدمة لشهادة العميل: اسم مستخدم Prefill من الشهادة الموجودة في نافذة تسجيل دخول المستخدم

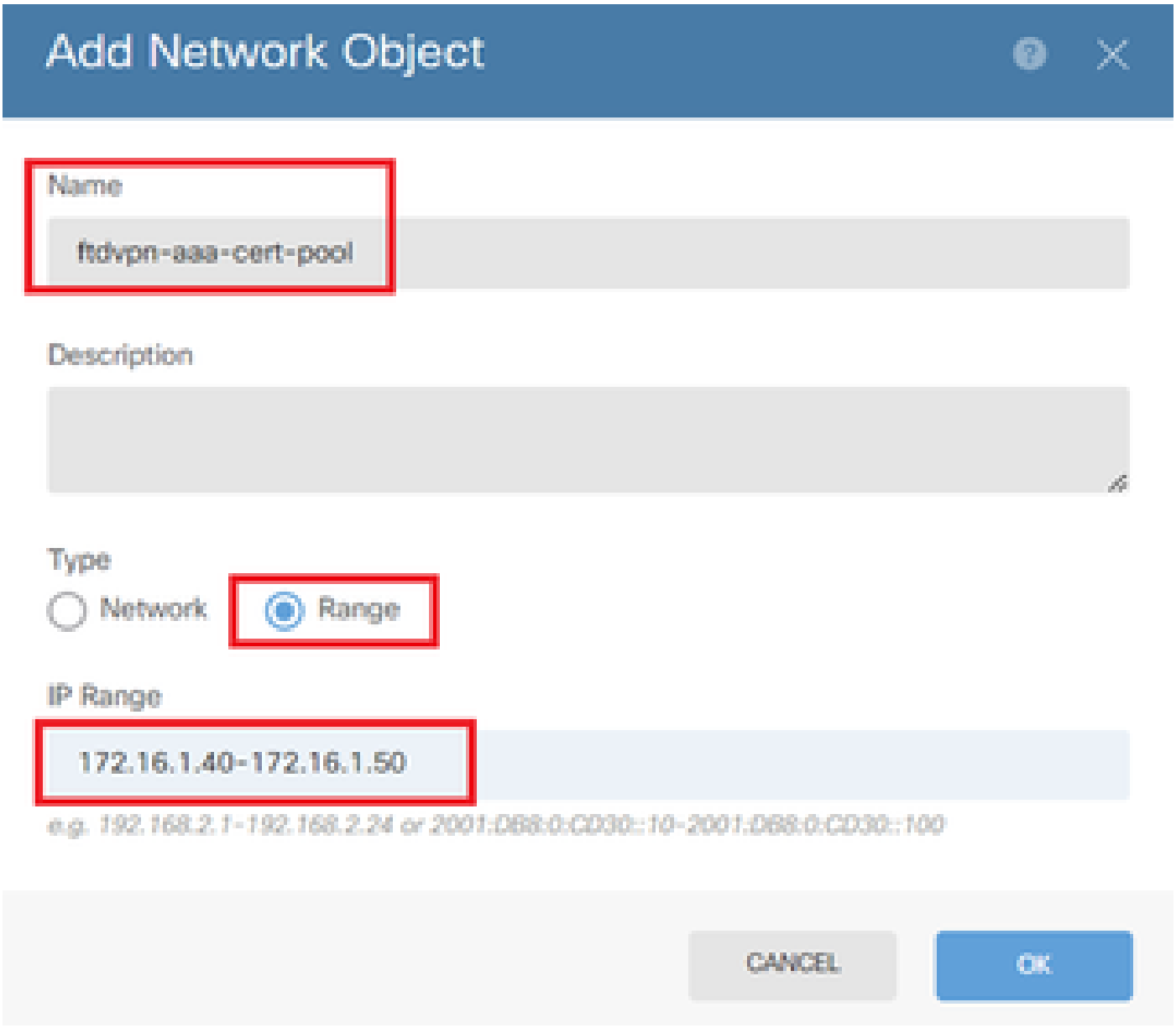


تفاصيل ملف تعريف اتصال VPN

الخطوة 4. إضافة تجمع عناوين لملف تعريف الاتصال

أدخل المعلومات الضرورية لإضافة تجمع عناوين IPv4 جديد. حدد تجمع عناوين IPv4 الجديد الذي تمت إضافته لملف تعريف الاتصال وانقر فوق زر التالي.

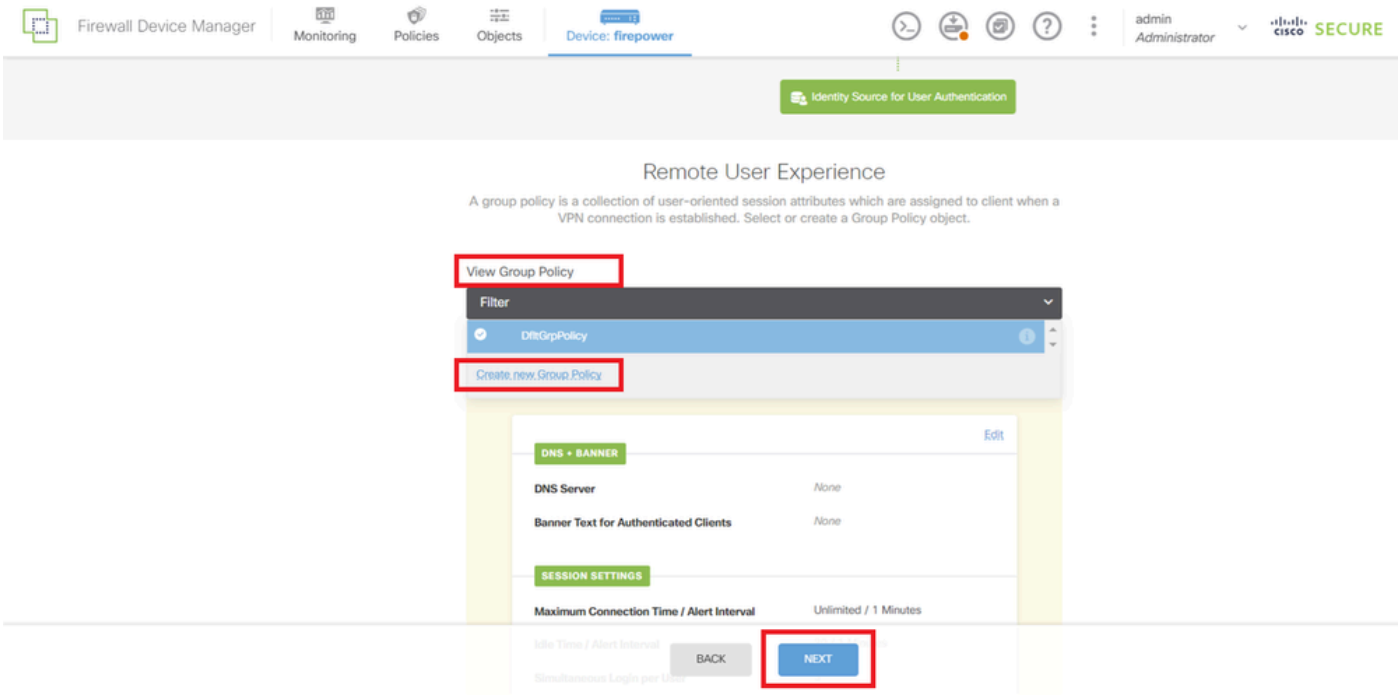
- الاسم: ftdvpn-aaa-cert-pool
- النوع: النطاق
- نطاق IP: 172.16.1.40-172.16.1.50



تفاصيل تجمع عناوين IPv4

الخطوة 5. إضافة نهج المجموعة لملف تعريف الاتصال

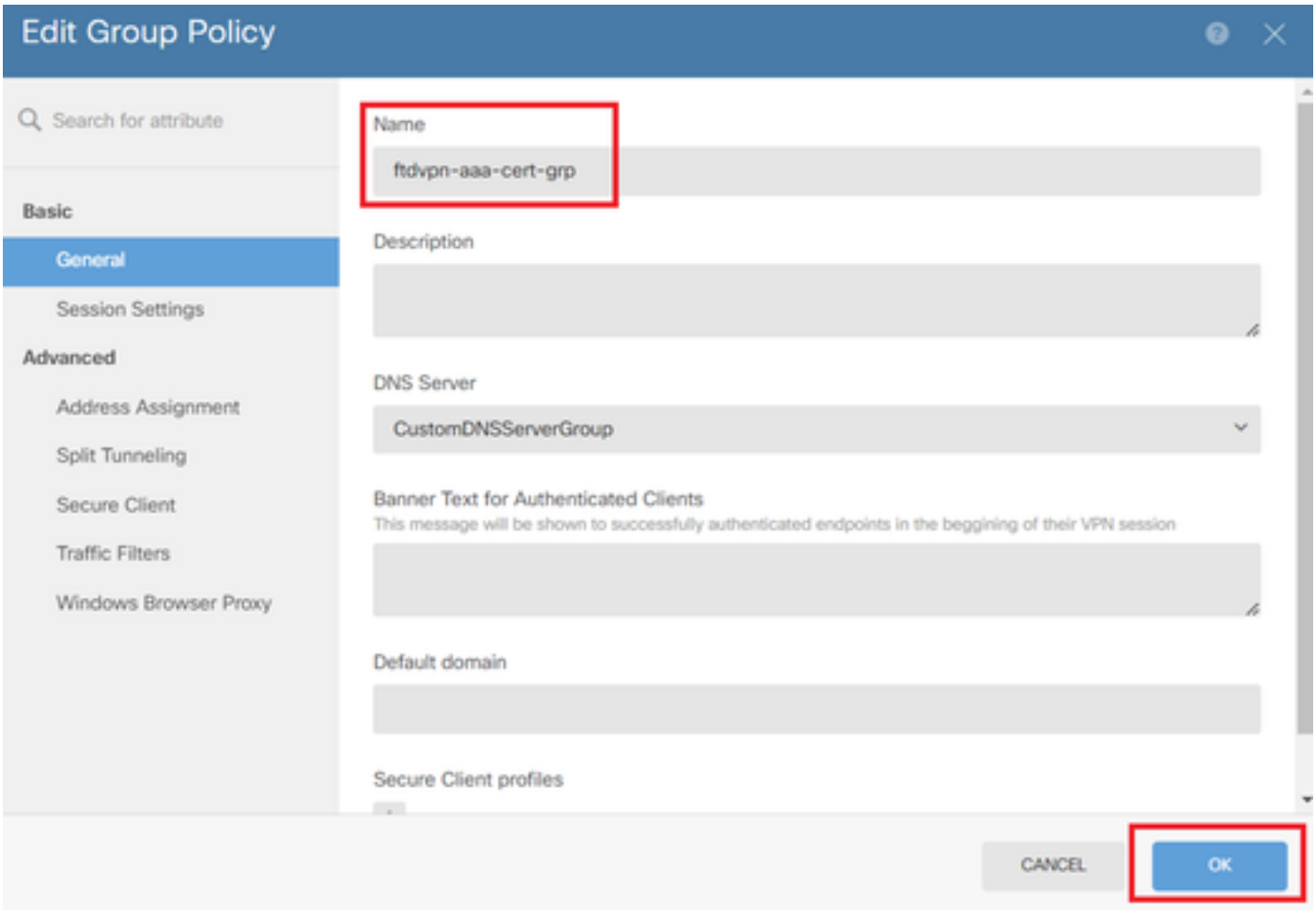
انقر فوق إنشاء نهج مجموعة جديد في عنصر عرض نهج المجموعة.



اضافة نهج المجموعة

قم بإدخال المعلومات الضرورية لإضافة نهج مجموعة جديد وانقر فوق زر موافق. حدد نهج مجموعة مضاف جديد لملف تعريف الاتصال.

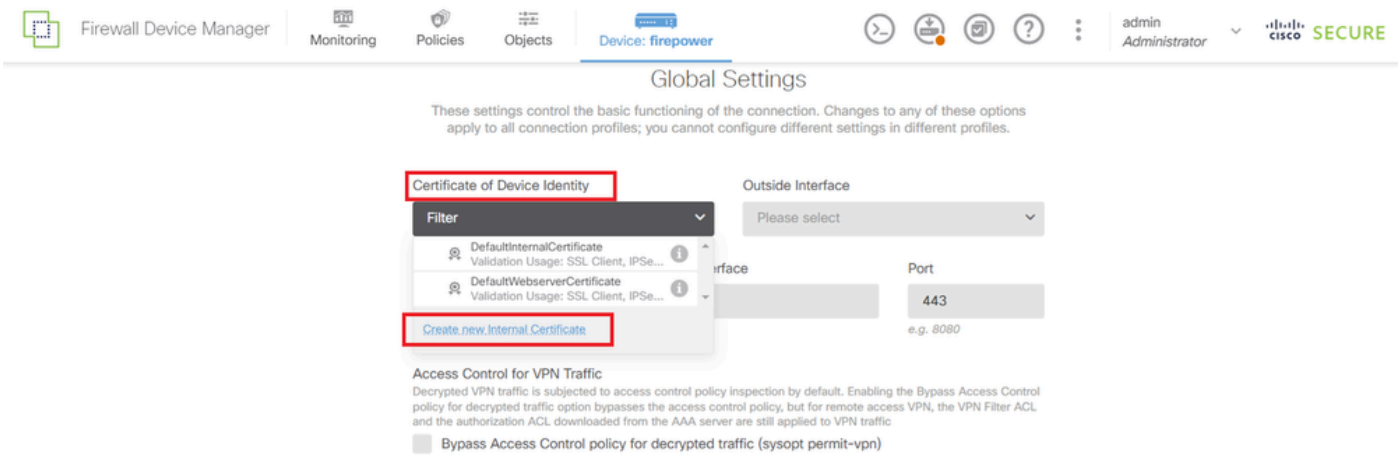
- الاسم: ftdvpn-aaa-cert-grp



تفاصيل نهج المجموعة

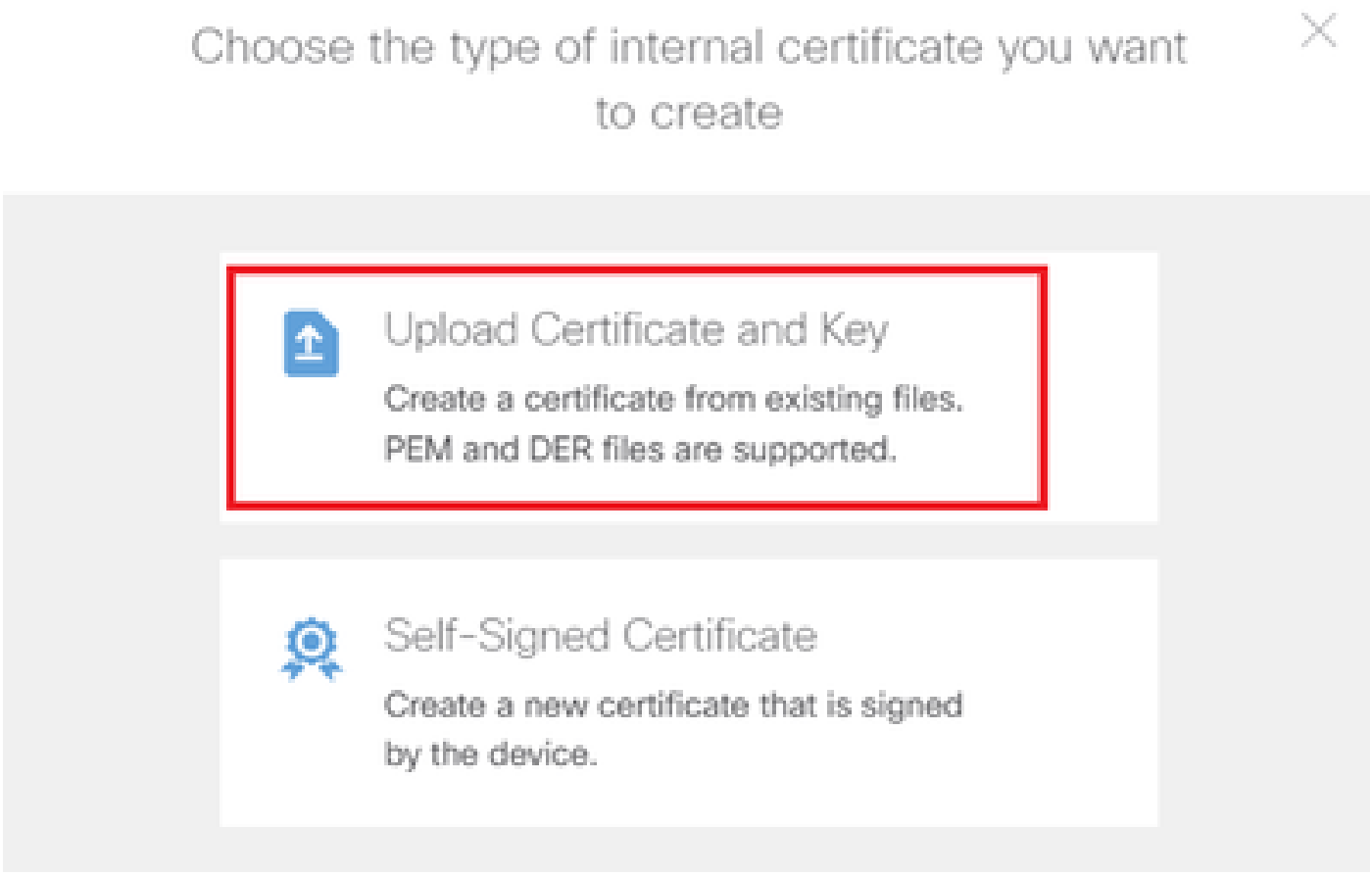
الخطوة 6. تكوين شهادة هوية الجهاز والواجهة الخارجية لتوصيف التوصيل

انقر على إنشاء شهادة داخلية جديدة في شهادة عنصر هوية الجهاز.



إضافة شهادة داخلية

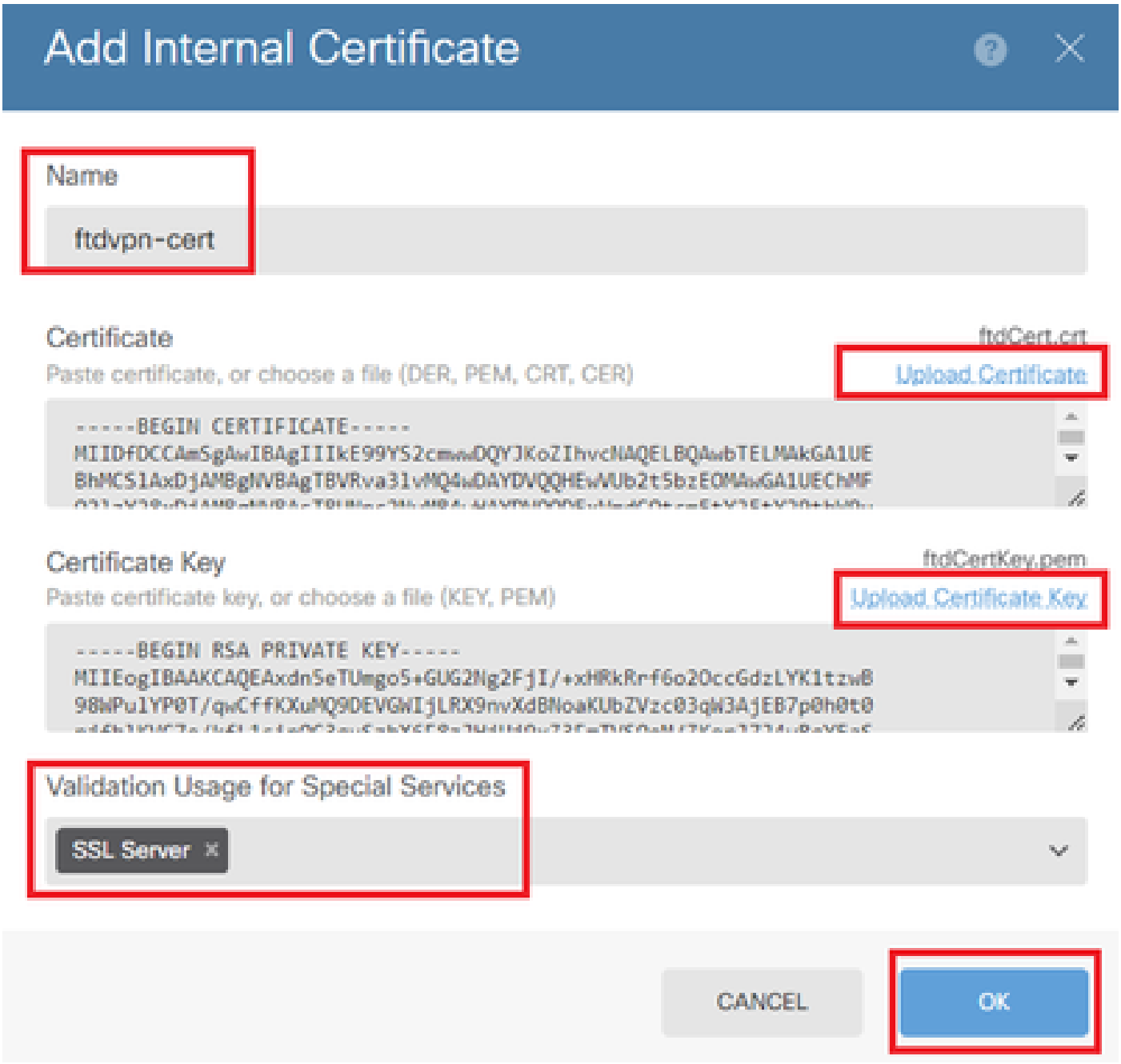
انقر على تحميل الشهادة والمفتاح.



تحميل الشهادة والمفتاح

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

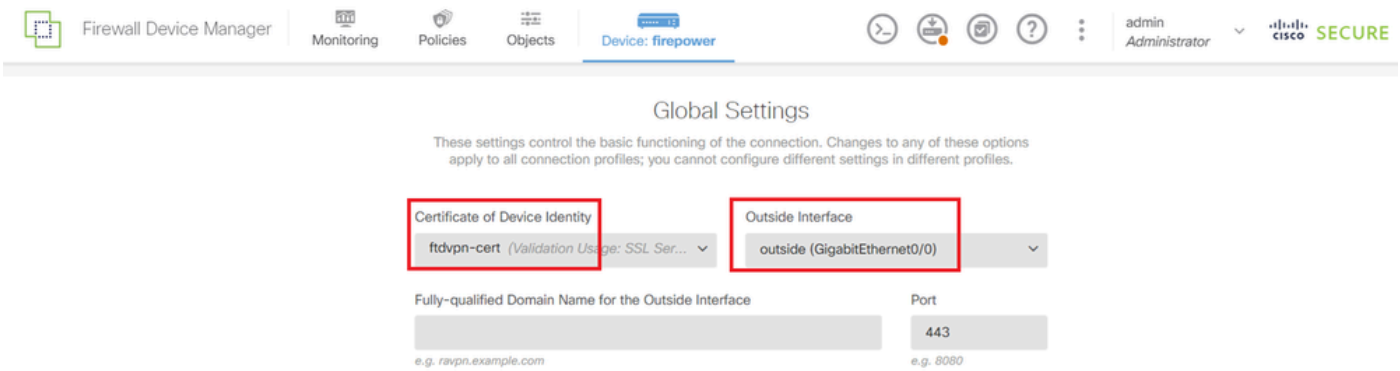
- الاسم: ftdvpn-cert
- إستخدام التحقق من الصحة للخدمات الخاصة: خادم SSL



تفاصيل الشهادة الداخلية

حدد شهادة هوية الجهاز والواجهة الخارجية لاتصال VPN.

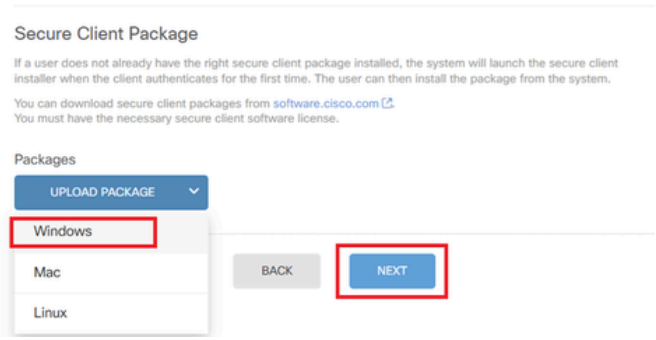
- شهادة هوية الجهاز: ftdvpn-cert
- الواجهة الخارجية: خارج (GigabitEthernet0/0)



تفاصيل الإعدادات العمومية

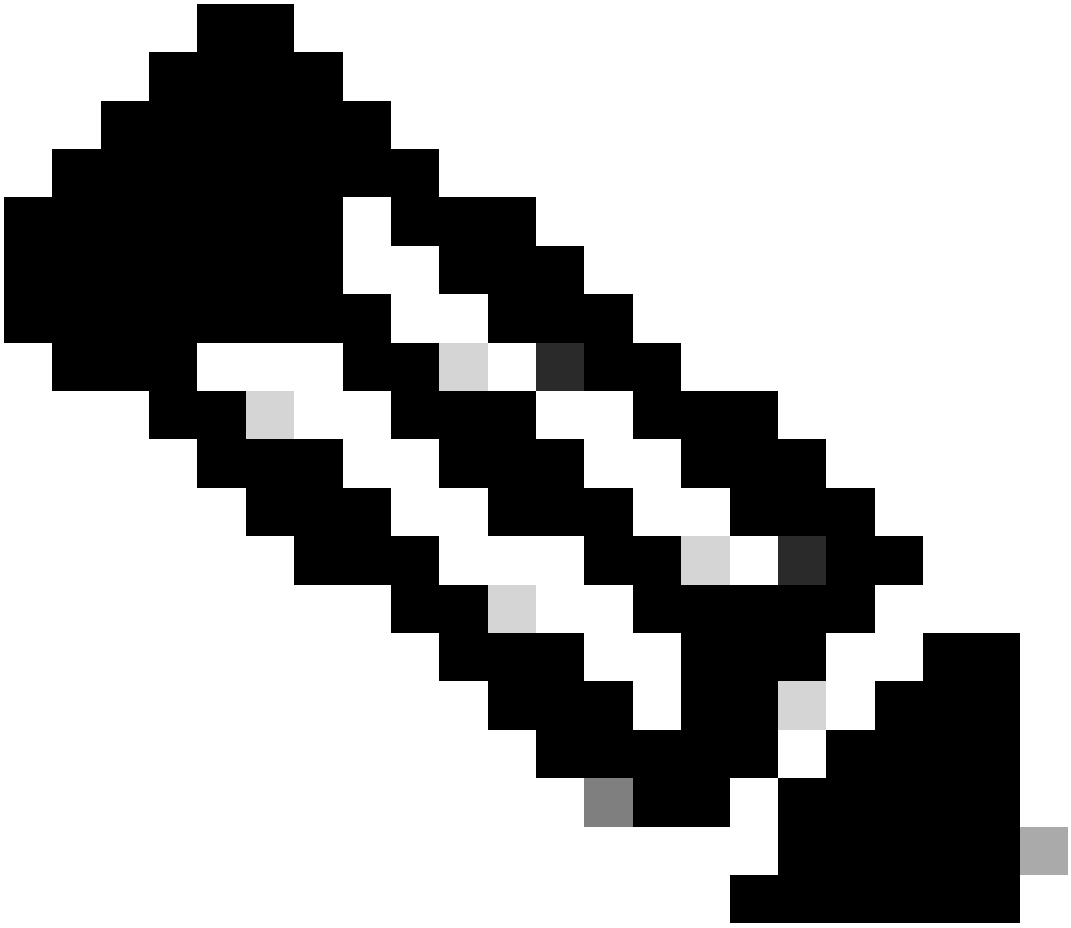
الخطوة 7. تكوين صورة عميل آمنة لملف تعريف الاتصال

حدد Windows في عنصر الحزم

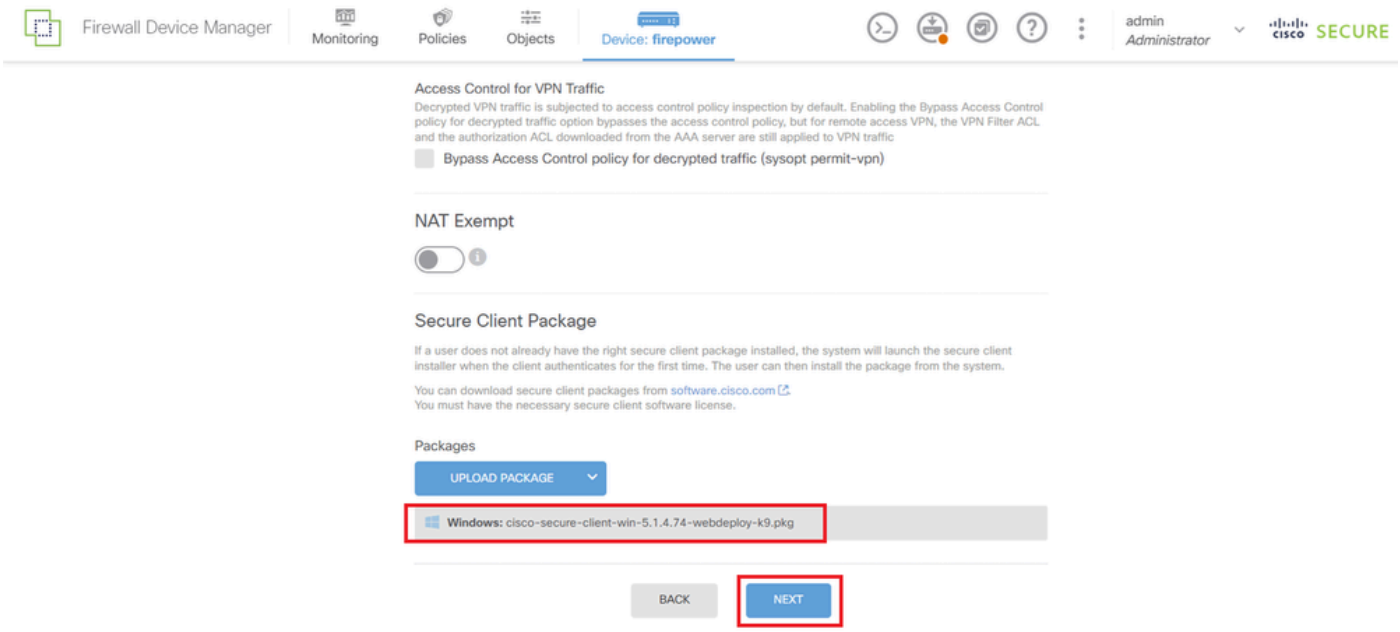


تحميل حزمة صورة العميل الآمنة

قم بتحميل ملف صورة العميل الآمنة من الكمبيوتر المحلي وانقر فوق Nextbutton.



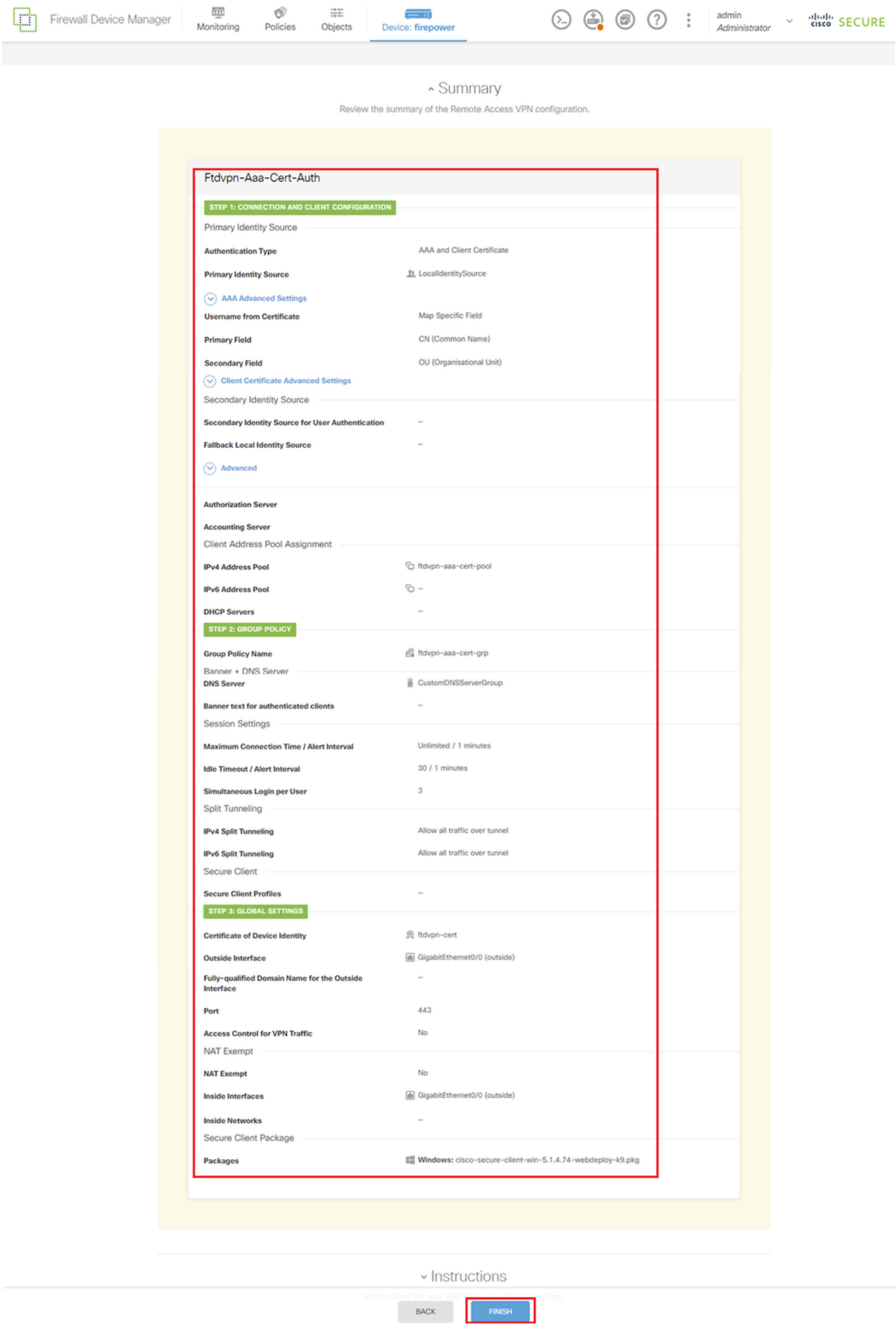
ملاحظة: تم تعطيل ميزة إستثناء NAT في هذا المستند. بشكل افتراضي، يتم تعطيل سياسة التحكم بالوصول الالتفافي لحركة المرور التي تم فك تشفيرها (sysopt allowed-vpn)، مما يعني أن حركة مرور VPN التي تم فك تشفيرها تخضع لفحص سياسة التحكم في الوصول.



تحديد حزمة صورة العميل الآمنة

الخطوة 8. تأكيد الملخص لملف تعريف الاتصال

أكد المعلومات التي تم إدخالها لاتصال VPN وانقر فوق FINISHbutton.



تأكيد الإعدادات لتوصيف التوصيل

```
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
```

تأكيد في عميل شبكة VPN

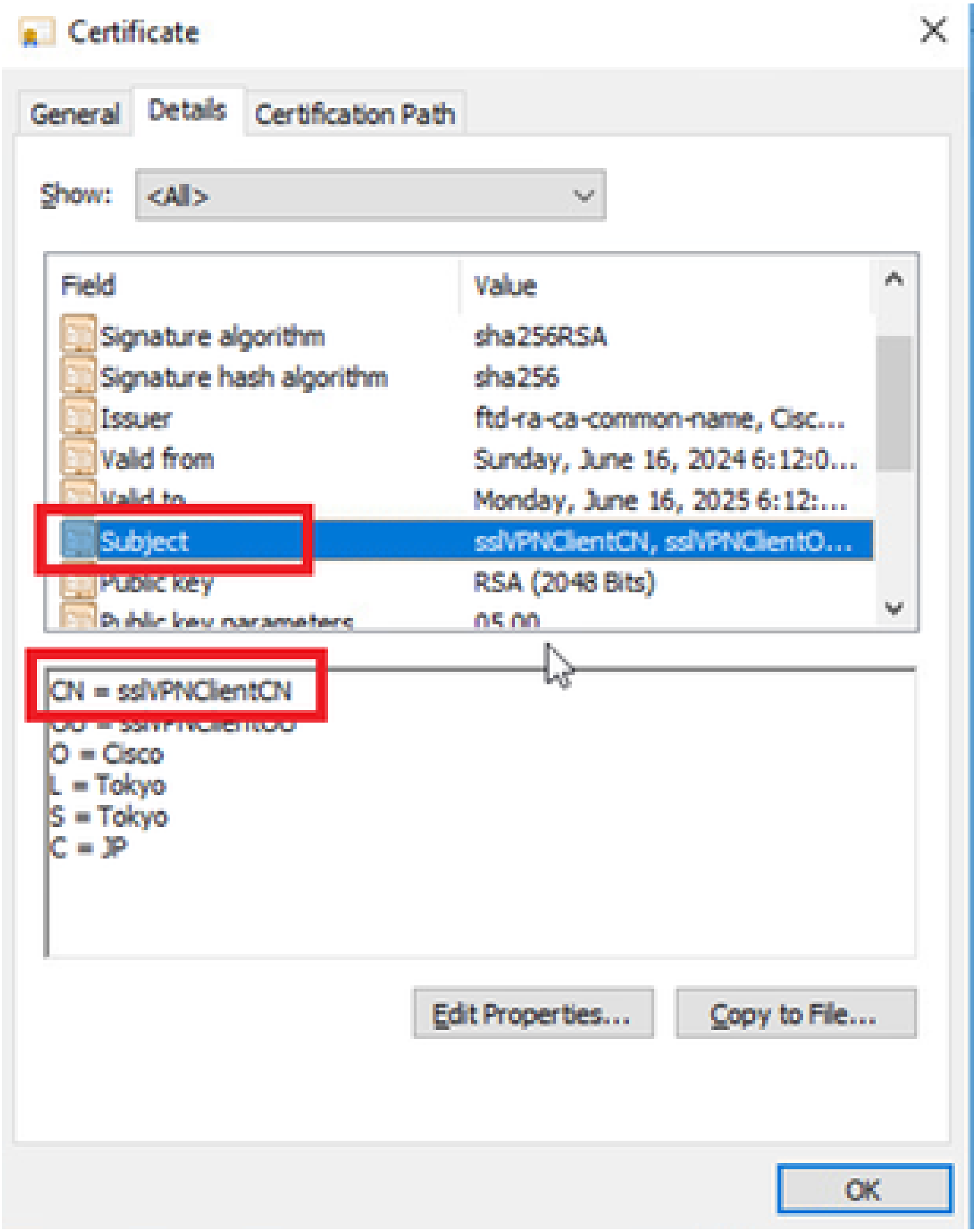
الخطوة 1. تأكيد شهادة العميل

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

تأكيد شهادة العميل

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

- الموضوع: CN = sslVPNClientCN



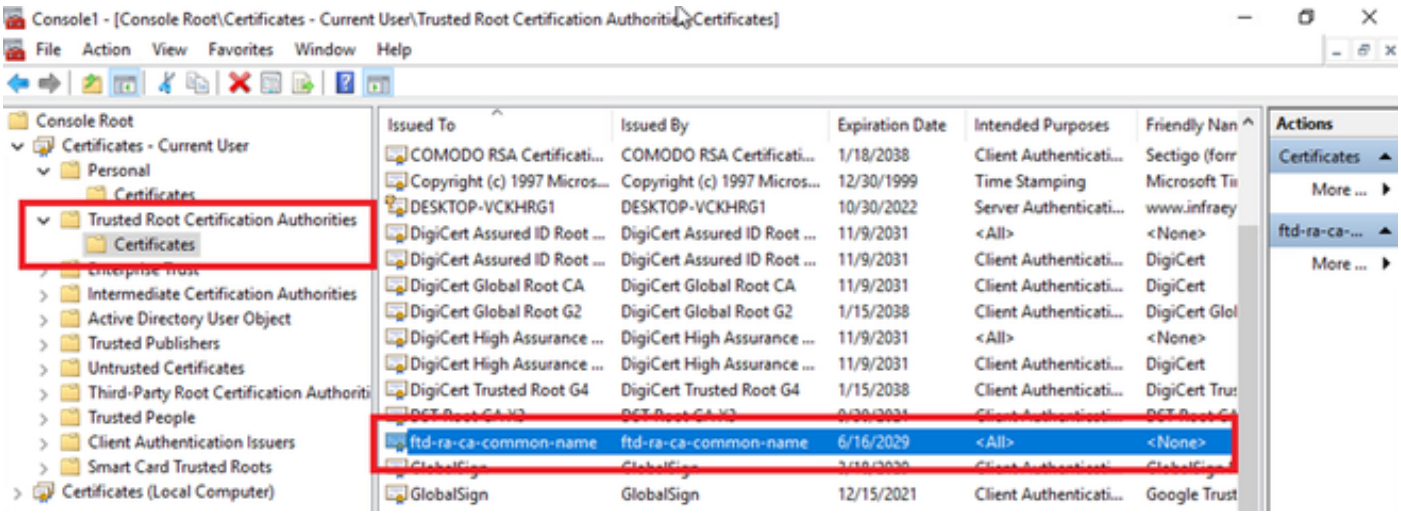
تفاصيل شهادة العميل

الخطوة 2. تأكيد CA

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

تحقق من المرجع المصدق المستخدم للمصادقة.

- صادر عن: ftd-ra-ca-common-name

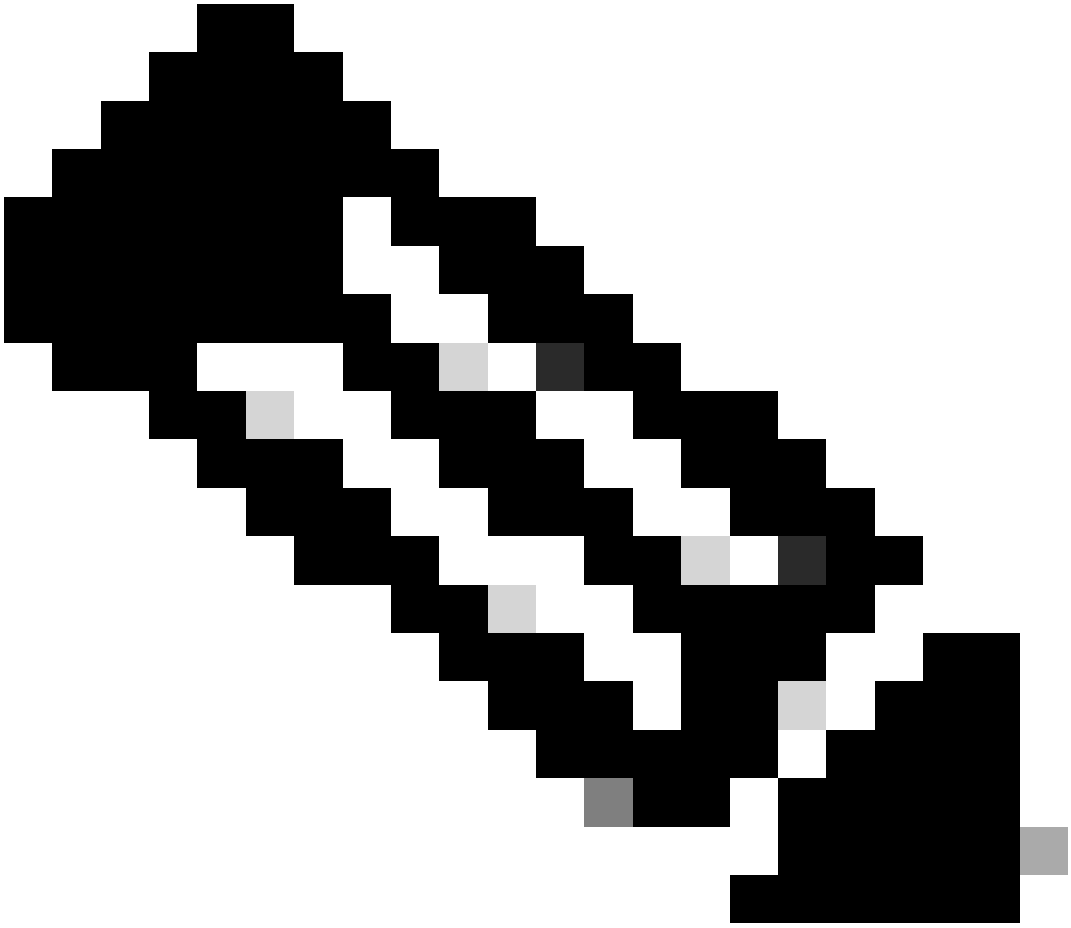


تأكيد CA

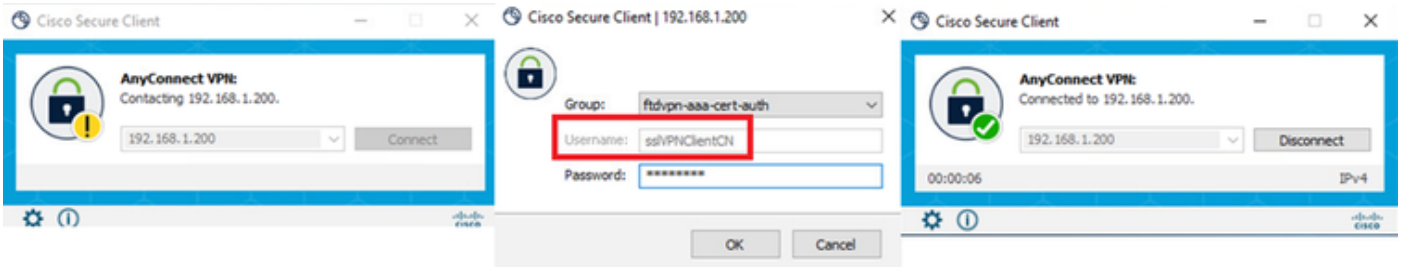
التحقق من الصحة

الخطوة 1. بدء اتصال VPN

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



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



بدء اتصال VPN

الخطوة 2. تأكيد جلسة VPN في FTD CLI

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

```
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 : 00000000000004000667ff45e
Security Grp : none Tunnel Zone : 0

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

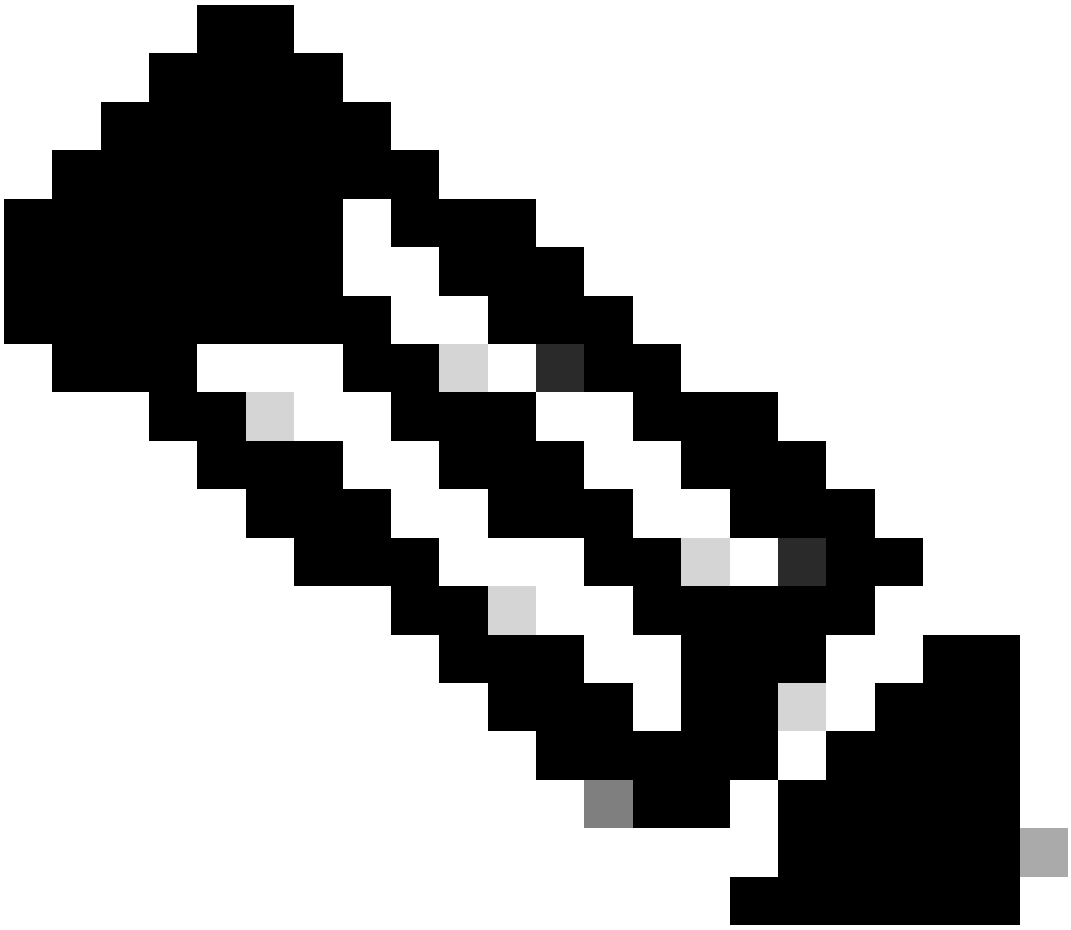
AnyConnect-Parent:
Tunnel ID : 4.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 49779 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 7 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : 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

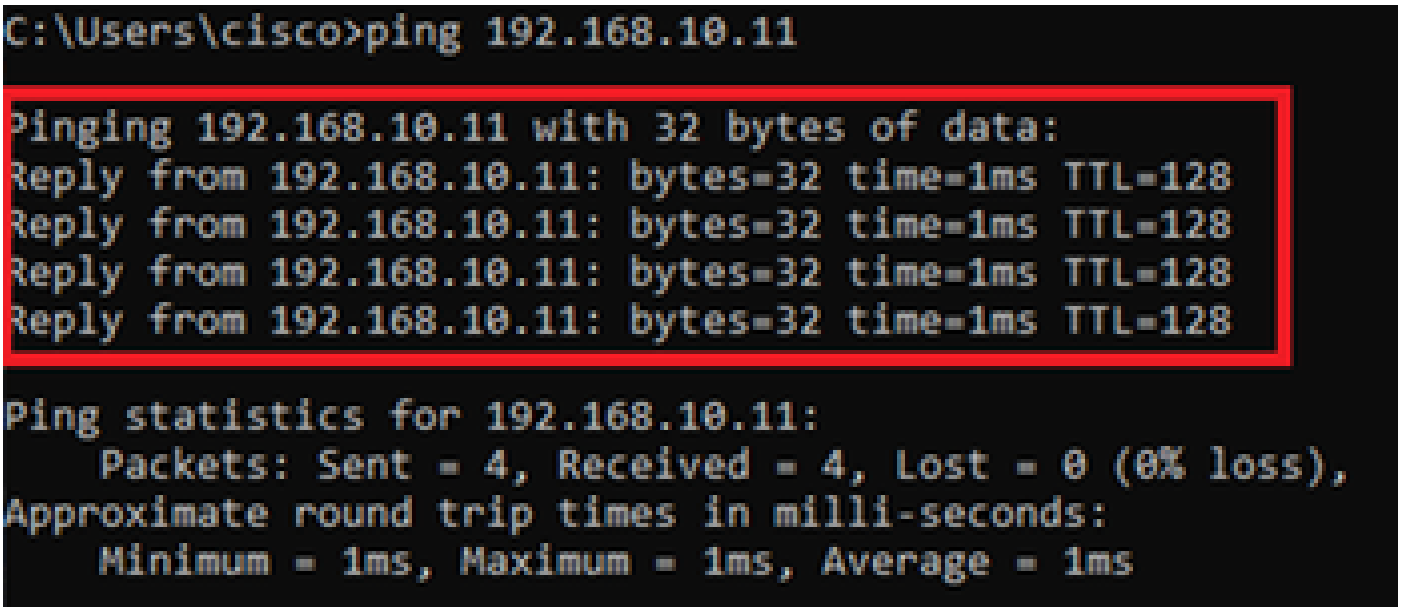
الخطوة 3. تأكيد الاتصال بالخادم

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

الخاصة الظاهرية (VPN) والخادم.



ملاحظة: نظرا لتعطيل خيار التحكم في الوصول الالتفافي لحركة المرور التي تم فك تشفيرها (sysopt allowed-vpn) في الخطوة 7، فأنت بحاجة إلى إنشاء قواعد التحكم في الوصول التي تسمح بوصول تجمع عناوين IPv4 لديك إلى الخادم.



لجن إختبار الاتصال

capture in interface inside real-timeRunCommand في CLI ل FTD (Lina) لتأكيد التقاط الحزمة.

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

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 محرك Lina.

// 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

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

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

معلومات ذات صلة

تكوين خدمة إدارة FDM في الهروب لـ Firepower 2100

تكوين شبكة 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).