تكوين شبكة VPN للوصول عن بعد على FTD المدارة بواسطة FDM

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نشر شبكة RA VPN على FTD تتم إدارتها بواسطة مدير FDM الموجود في المربع الذي يشغل الإصدار 6.5.0 والإصدارات الأحدث.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بتكوين شبكة الوصول عن بعد الخاصة الظاهرية (RA VPN) على FirePOWER Device Manager (FDM).

الترخيص

- تم تسجيل خدمة الدفاع عن تهديد Firepower (FTD) مع بوابة الترخيص الذكي مع تمكين الميزات التي يتم التحكم فيها في التصدير (للسماح بتمكين عالمة التبويب "تكوين RA VPN")

- أي من ترا خيص AnyConnect التي تم تمكينها (APEX، Plus، أو VPN فقط)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج FTD من Cisco الذي يشغل الإصدار 6.5.0-115
- Cisco AnyConnect Secure Mobility Client، الإصدار 4.7.01076

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.

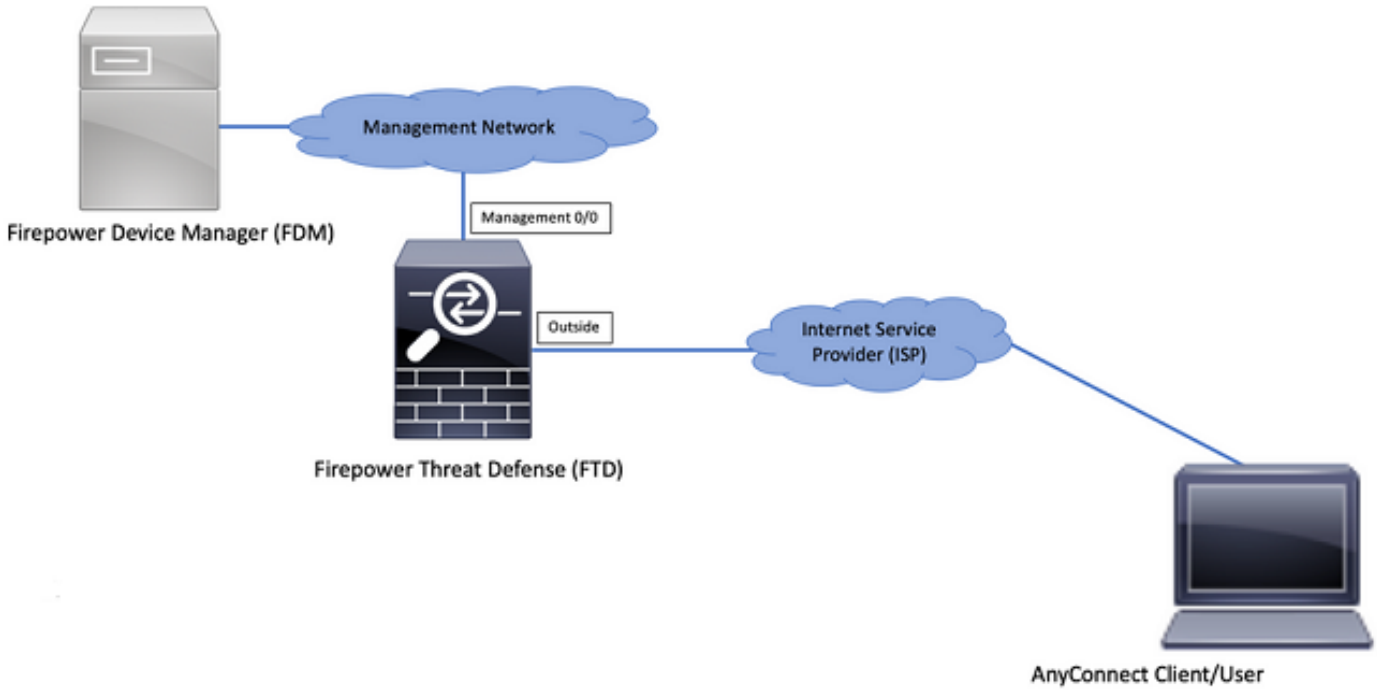
معلومات أساسية

يواجه تكوين بروتوكول FTD من خلال FDM صعوبات عند محاولة إنشاء إتصالات لعملاء AnyConnect من خلال الواجهة الخارجية أثناء الوصول إلى الإدارة من خلال الواجهة نفسها. هذا قيد معروف على إدارة fdm. تم تصنيف طلب التعزيز CSCvm76499 لهذه المشكلة.

التكوين

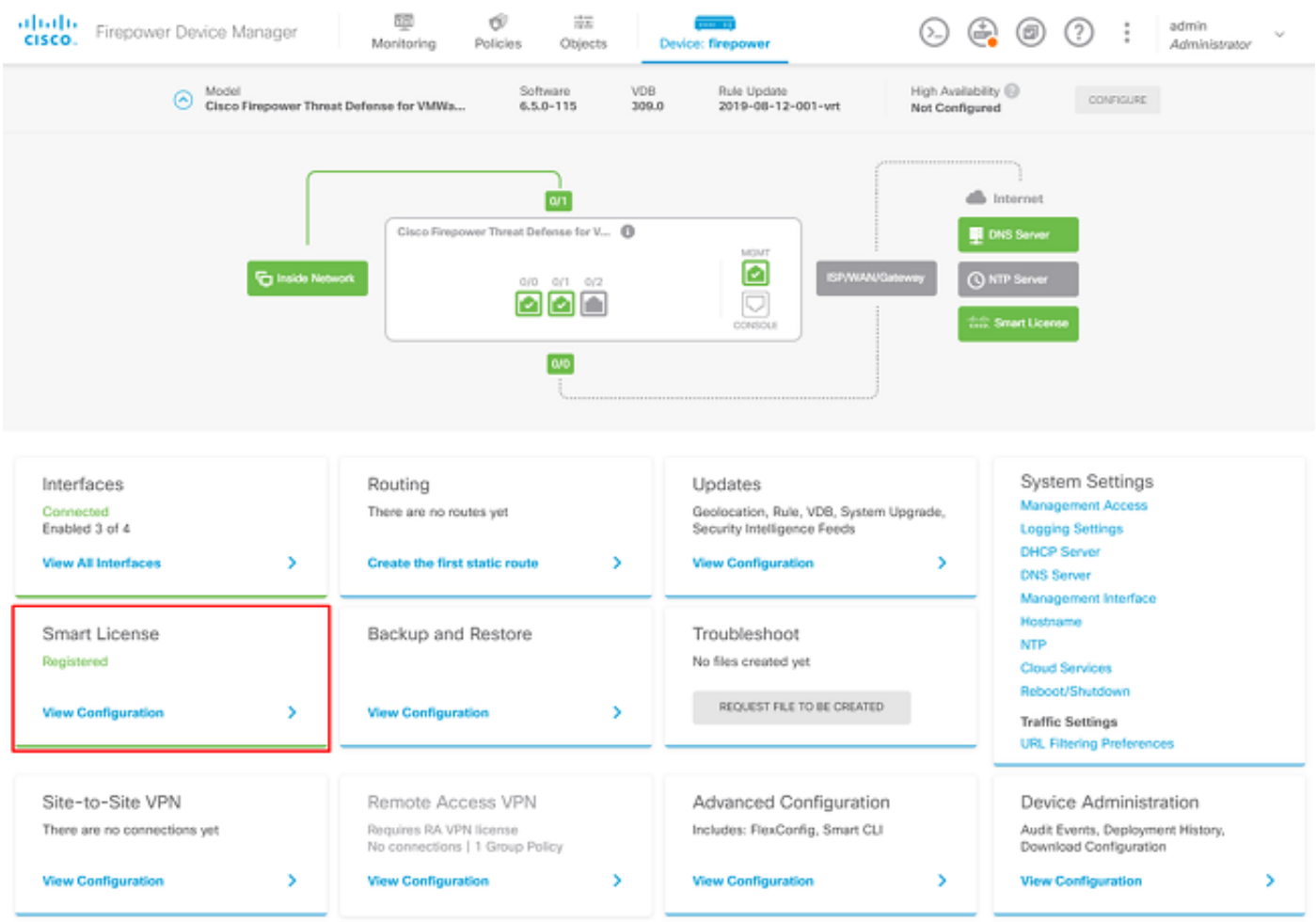
الرسم التخطيطي للشبكة

مصادقة AnyConnect Client باستخدام المحلية.

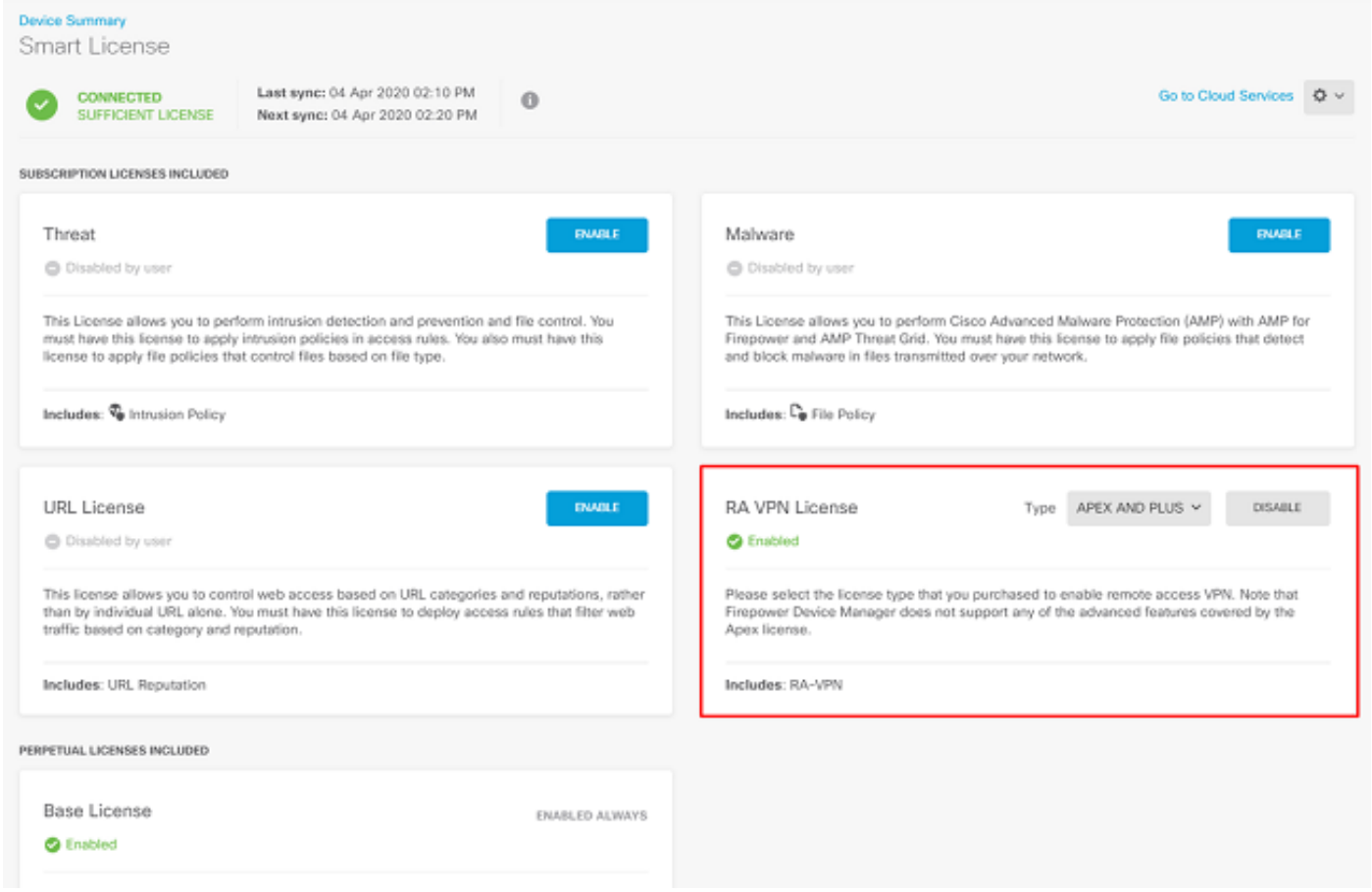


التحقق من الترخيص على FTD

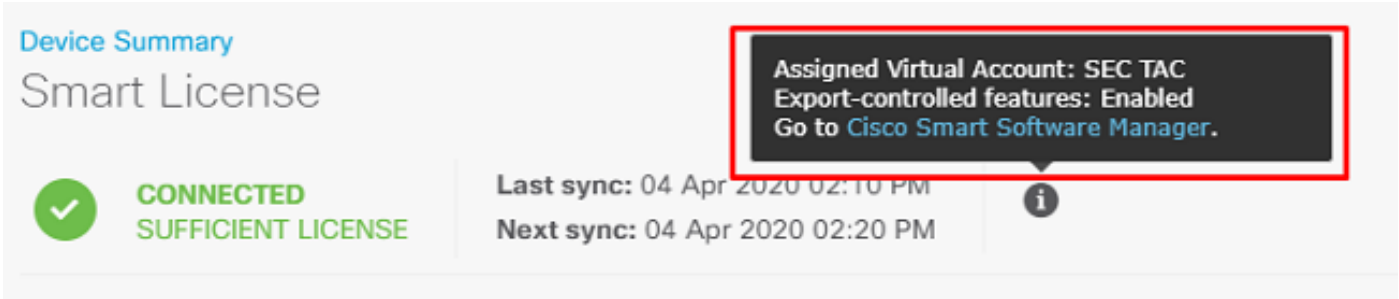
الخطوة 1. تحقق من تسجيل الجهاز في "الترخيص الذكي" كما هو موضح في الصورة:



الخطوة 2. تحقق من تمكين ترخيص AnyConnect على الجهاز كما هو موضح في الصورة.

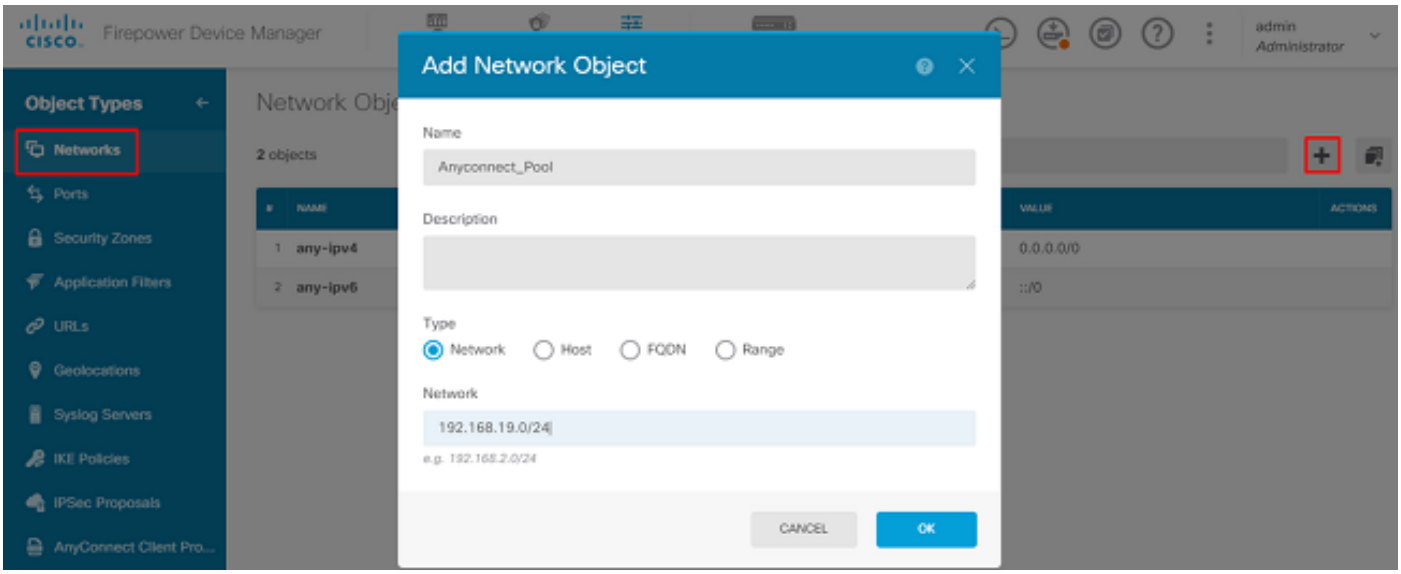


الخطوة 3. تحقق من تمكين المميزات التي تتحكم في التصدير في الرمز المميز كما هو موضح في الصورة:

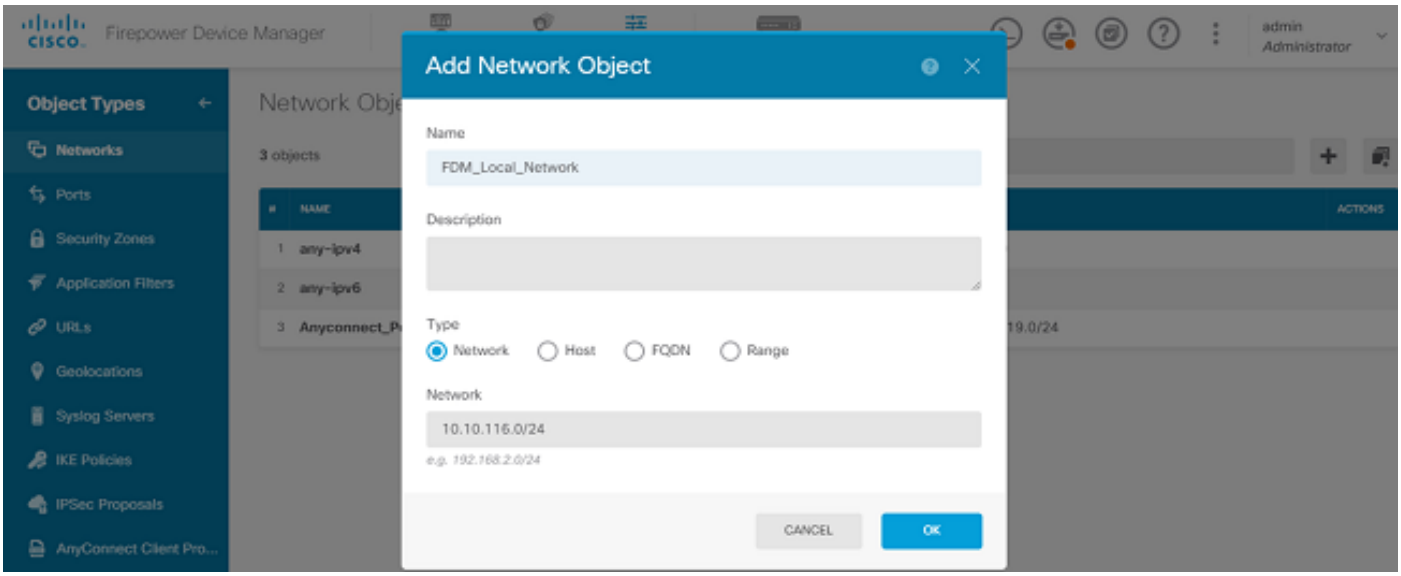


تعريف الشبكات المحمية

انتقل إلى Objects > Networks > Add new Network. تكوين تجمع VPN وشبكات LAN من واجهة المستخدم الرسومية (GUI) ل FDM. قم بإنشاء تجمع VPN لكي يتم إستخدامه لتعيين العنوان المحلي لمستخدمي AnyConnect كما هو موضح في الصورة:

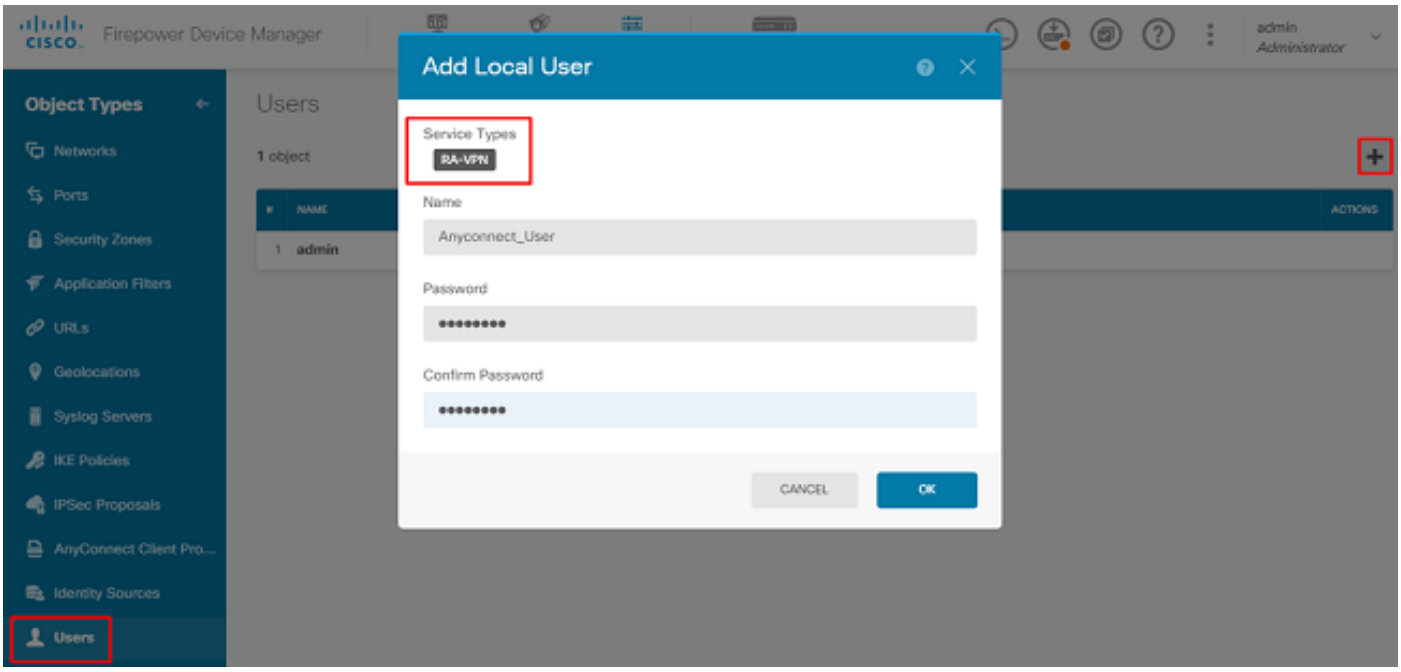


قم بإنشاء كائن للشبكة المحلية خلف جهاز FDM كما هو موضح في الصورة:



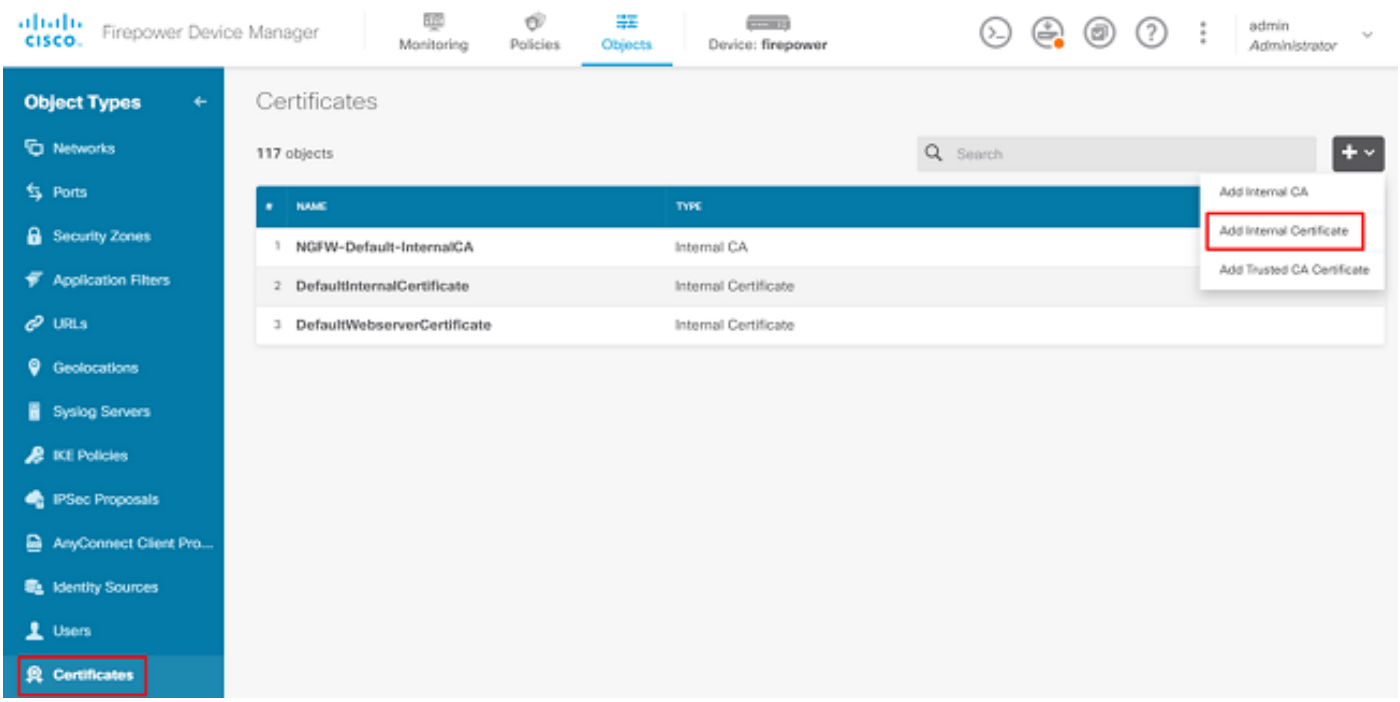
إنشاء مستخدمين محليين

انتقل إلى Objects > Users > Add User. إضافة المستخدمين المحليين لشبكة VPN الذين يقومون بالاتصال ب FTD من خلال AnyConnect. قم بإنشاء مستخدمين محليين كما هو موضح في الصورة:

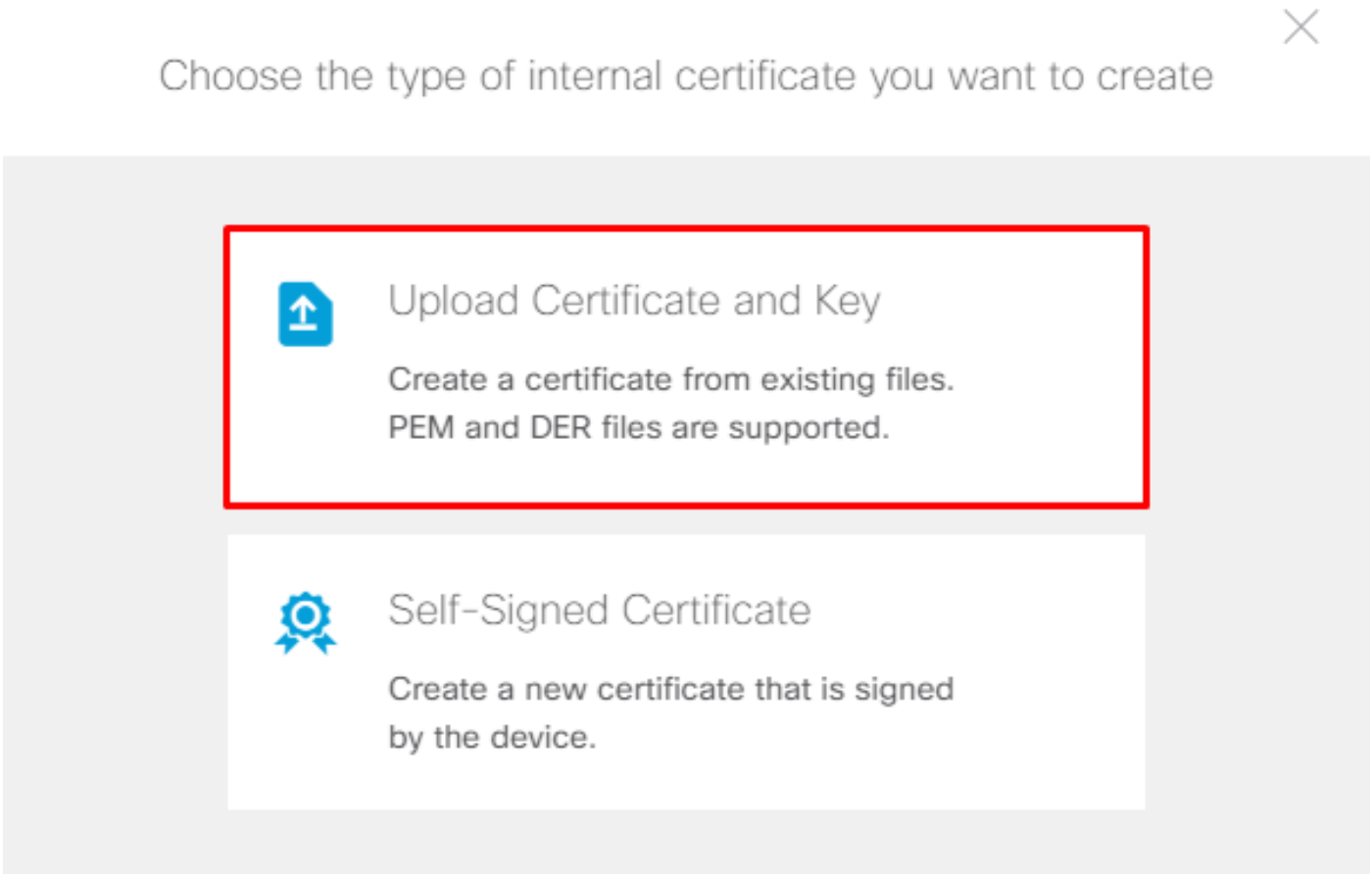


إضافة شهادة

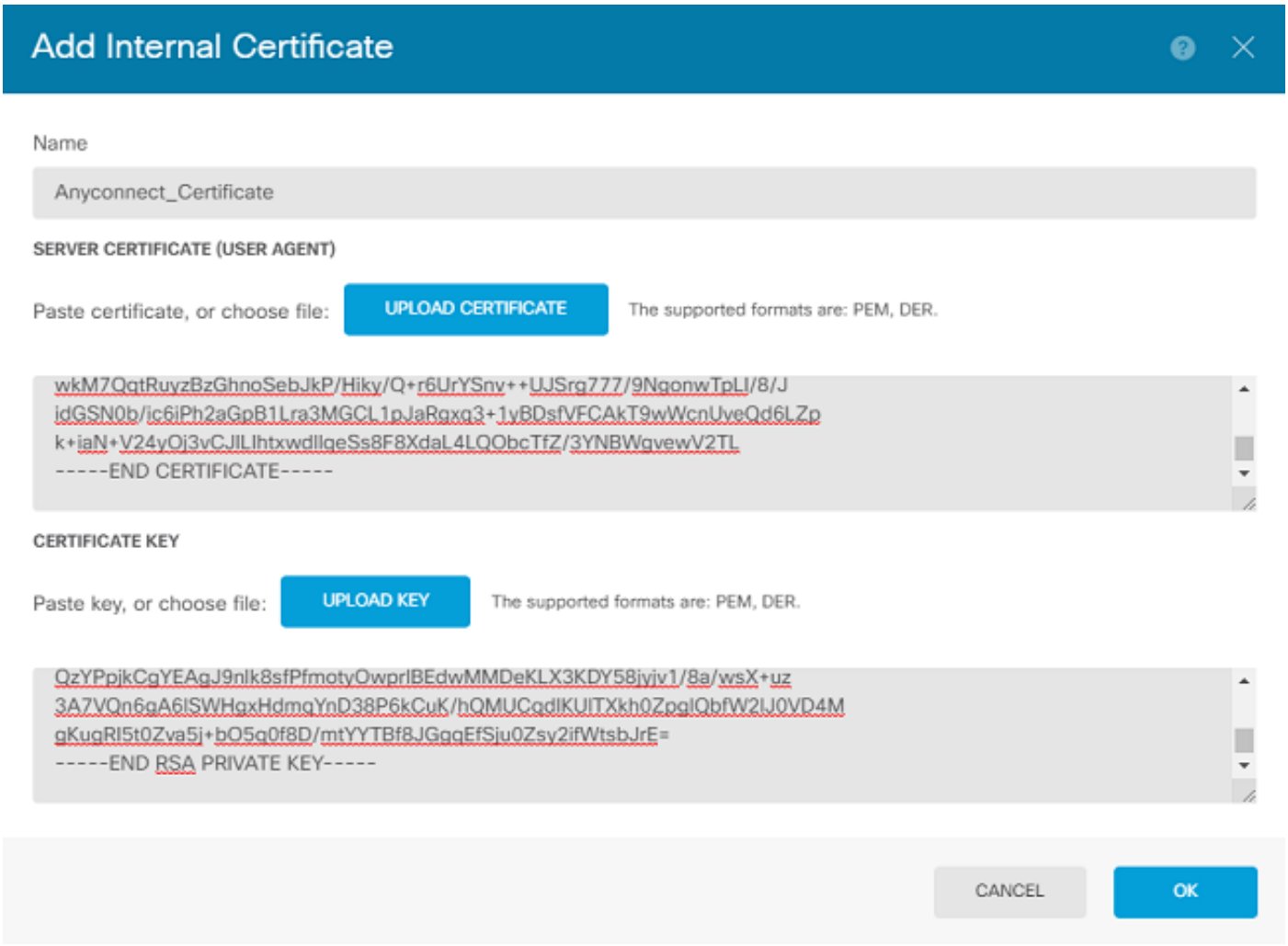
انتقل إلى Objects > Certificates > Add Internal Certificate. قم بتكوين شهادة كما هو موضح في الصورة:



قم بتحميل كل من الشهادة والمفتاح الخاص كما هو موضح في الصورة:

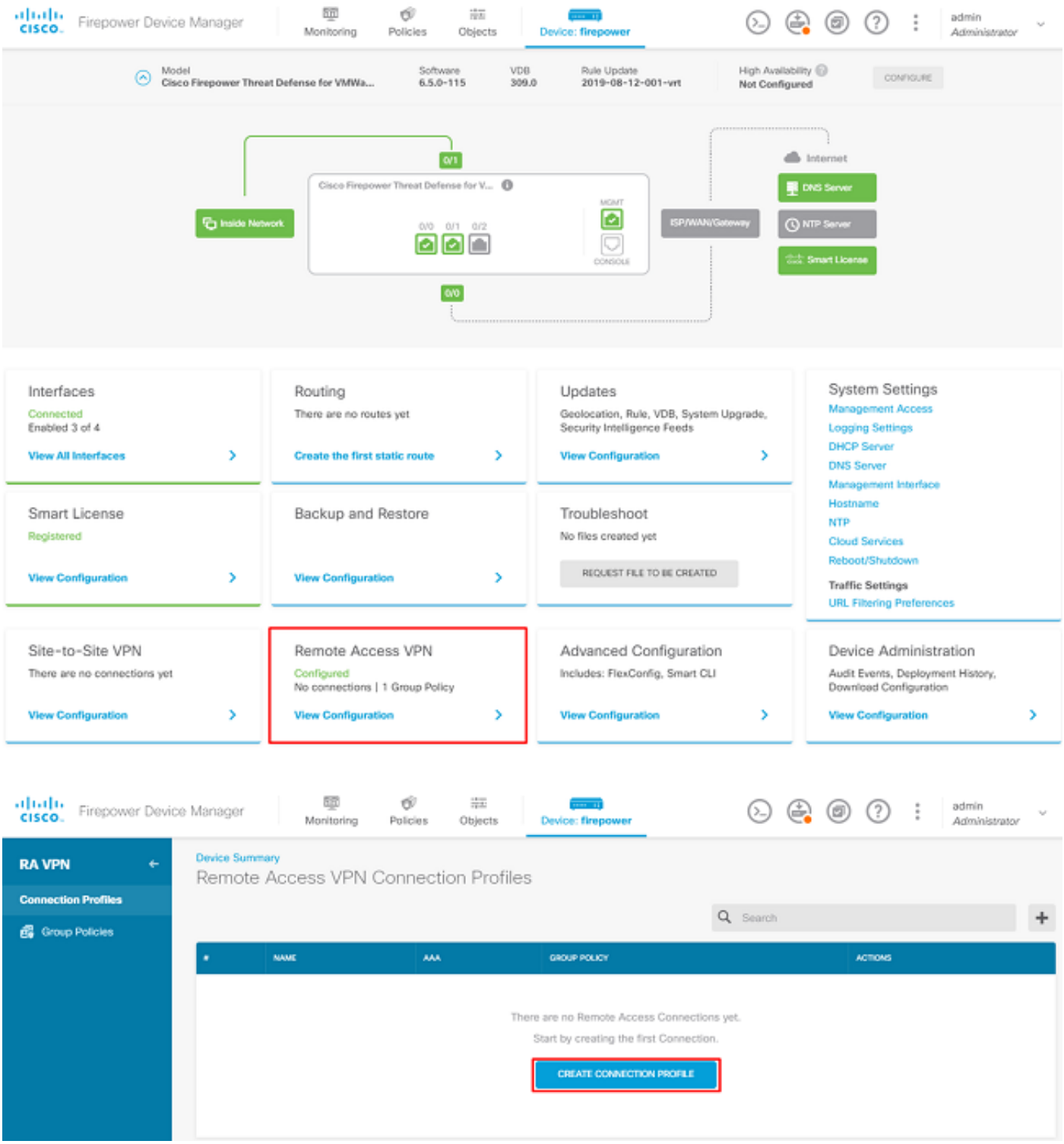


يمكن تحميل الشهادة والمفتاح عن طريق النسخ واللصق أو زر التحميل لكل ملف كما هو موضح في الصورة:

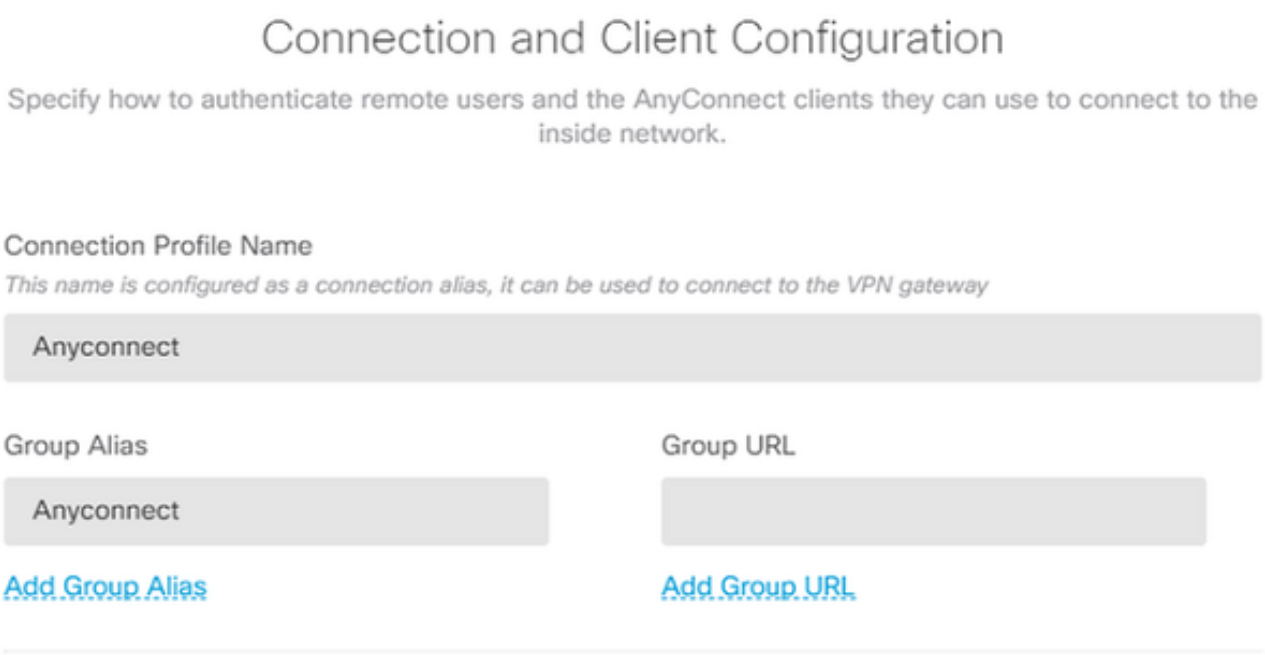


تكوين شبكة VPN للوصول عن بعد

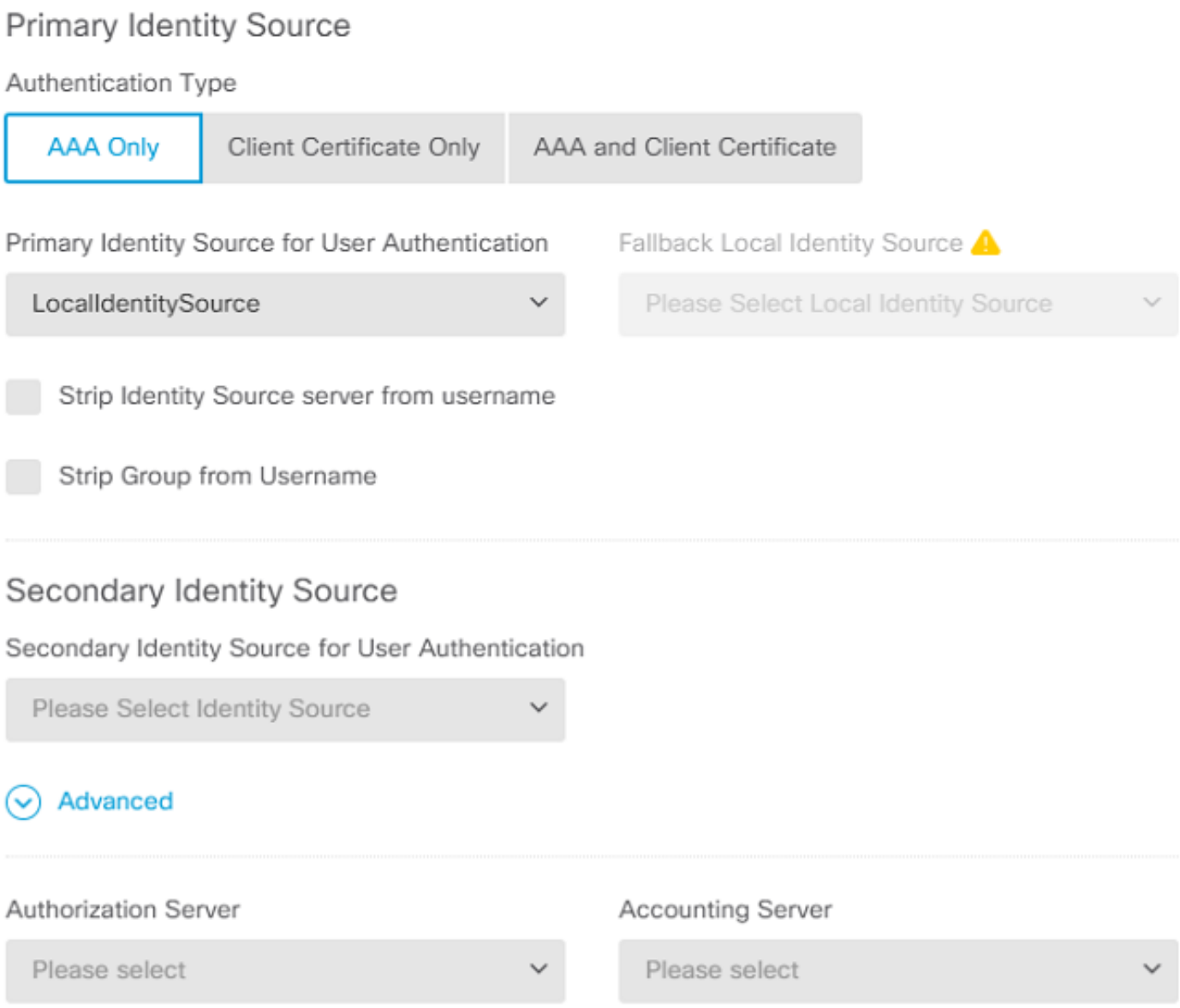
انتقل إلى Remote Access VPN > Create Connection Profile. انتقل عبر معالج RA VPN على FDM كما هو موضح في الصورة:



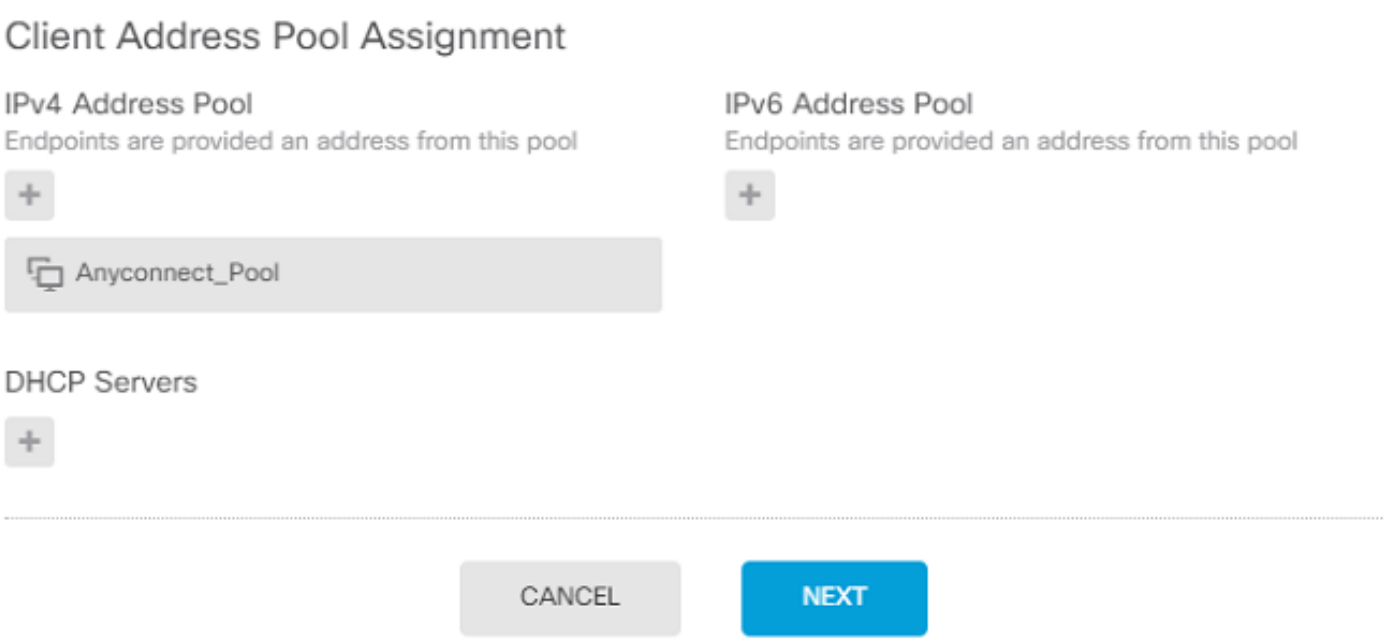
إنشاء توصيف توصيل وبدء التكوين كما هو موضح في الصورة:



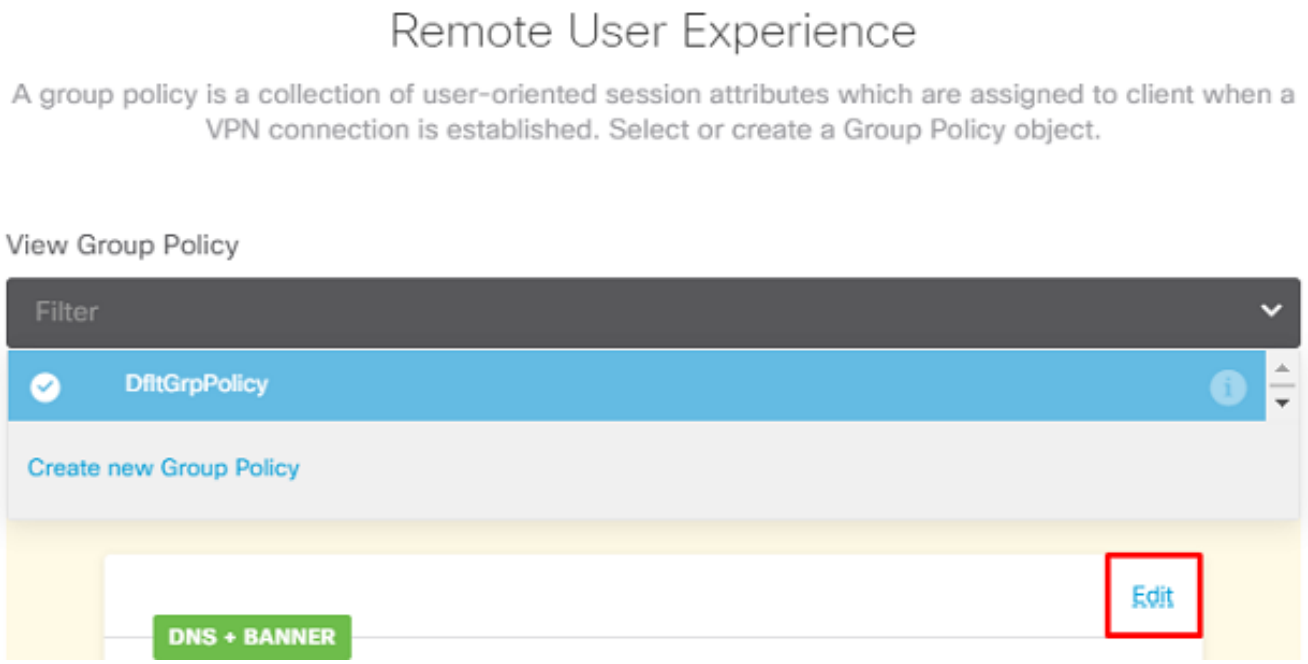
أختر طرق المصادقة كما هو موضح في الصورة. يستخدم هذا الدليل المصادقة المحلية.



أختر Anyconnect_Pool كائن كما هو موضح في الصورة:

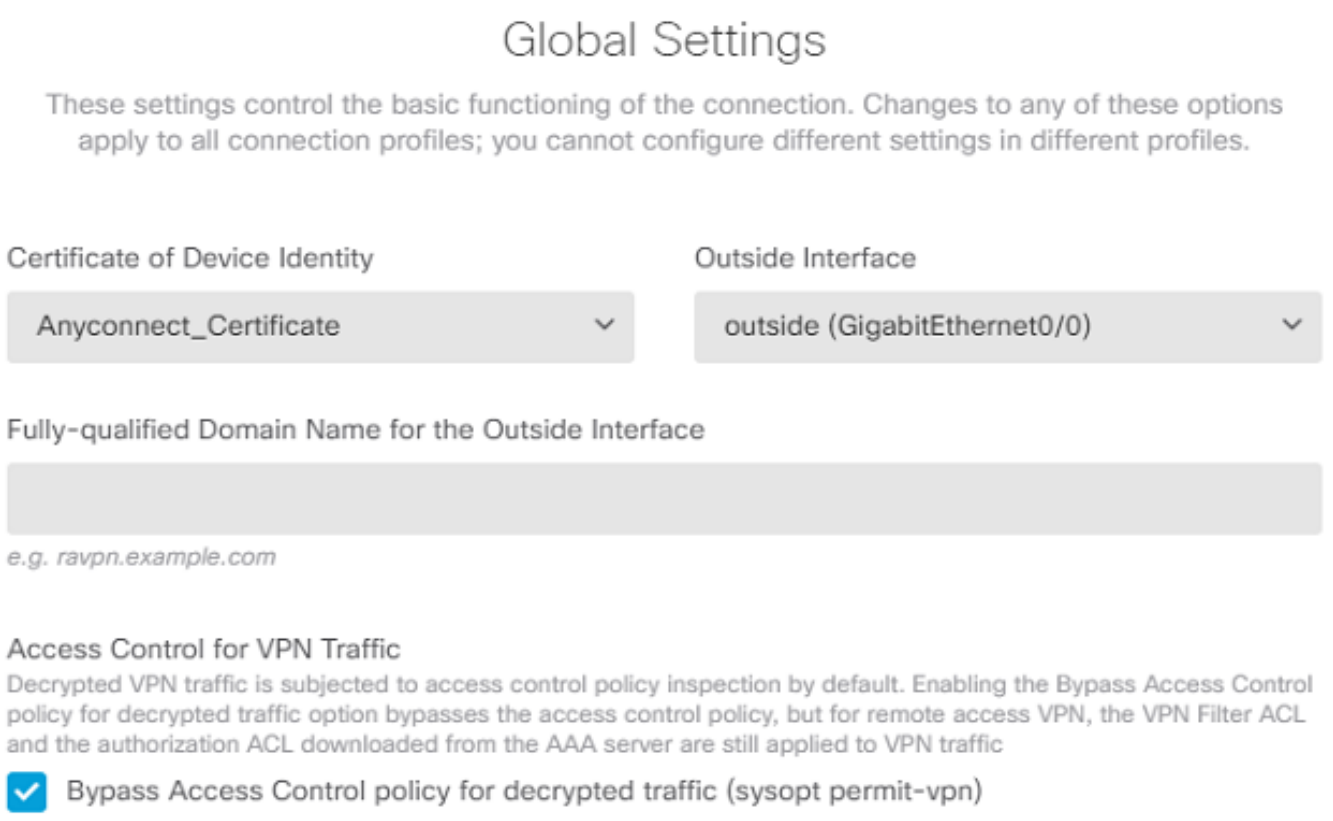


يتم عرض ملخص لنهج المجموعة الافتراضي في الصفحة التالية. يمكن إنشاء نهج مجموعة جديد عند الضغط على القائمة المنسدلة واختيار الخيار إلى Create a new Group Policy. لهذا الدليل، يتم إستخدام "نهج المجموعة" الافتراضي. أختر خيار التحرير في أعلى السياسة كما هو موضح في الصورة:

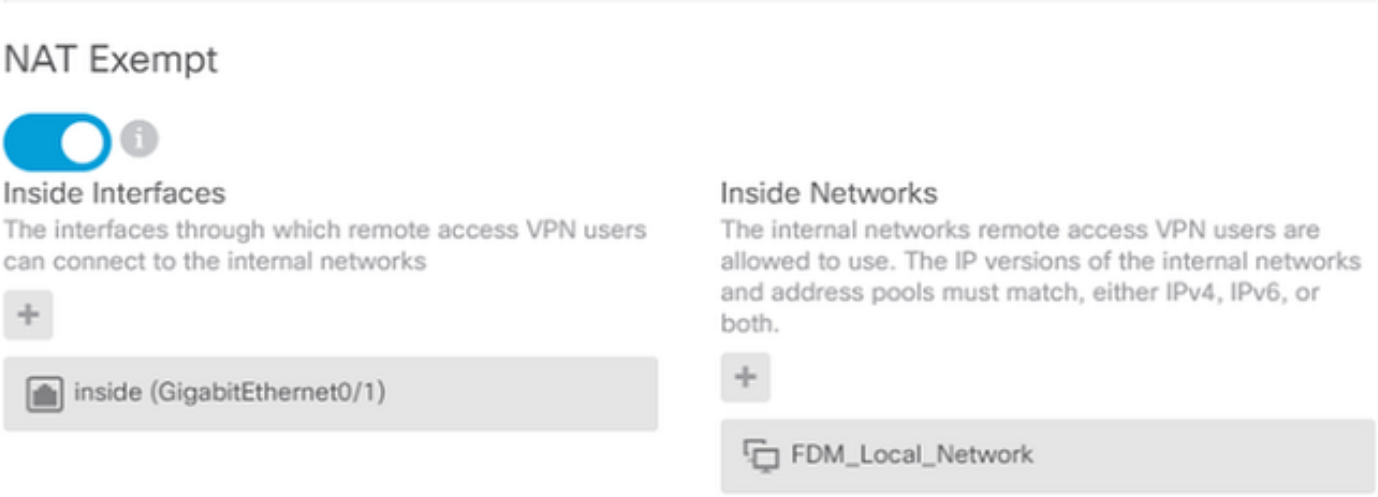


في نهج المجموعة، أضف تقسيم الاتصال النفقي حتى يقوم المستخدمون المتصلون ب AnyConnect بإرسال حركة مرور البيانات الموجهة إلى شبكة FTD الداخلية عبر عميل AnyConnect فقط بينما تخرج جميع حركة مرور البيانات الأخرى من اتصال ISP للمستخدم كما هو موضح في الصورة:

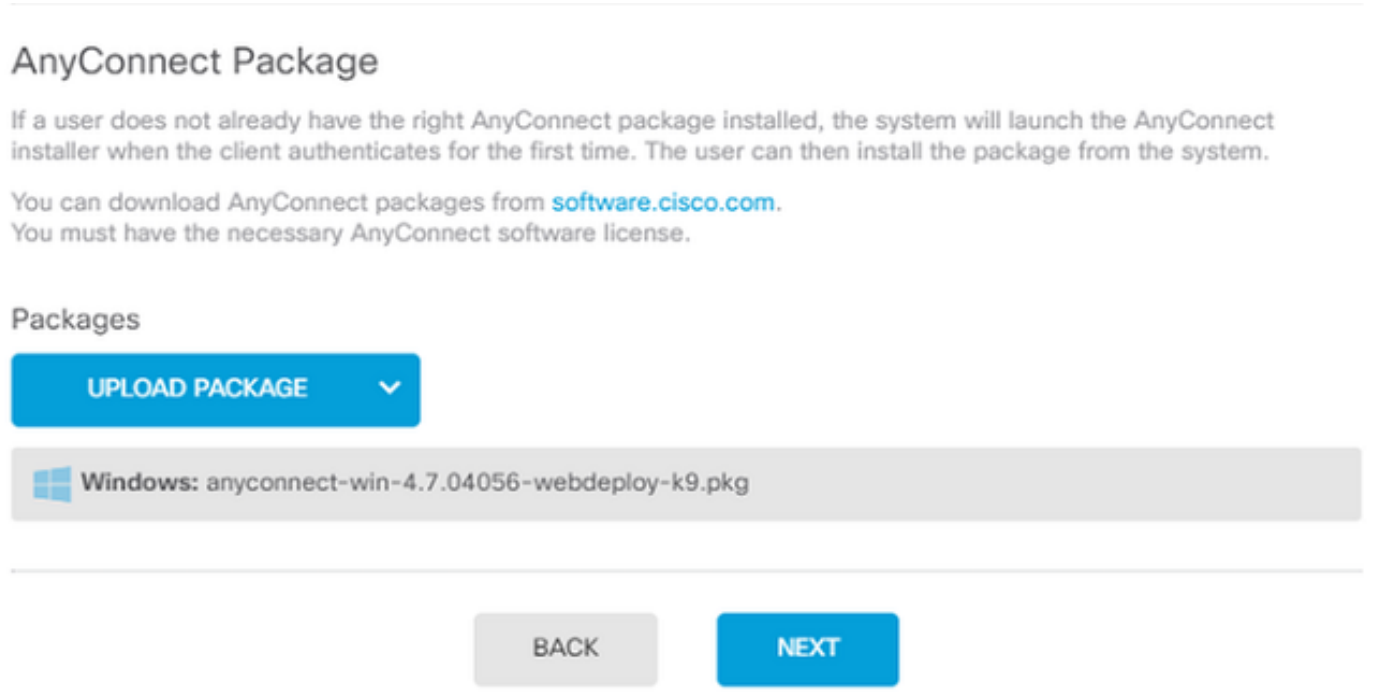
في الصفحة التالية، أختر Anyconnect_Certificate تمت إضافتها في قسم الشهادات. بعد ذلك، أختر الواجهة التي يسمع FTD عليها إتصالات AnyConnect. أختر نهج التحكم في الوصول الالتفافي لحركة المرور التي تم فك تشفيرها (sysopt permit-vpn). هذا أمر إختياري إذا sysopt permit-vpn غير مختار. يجب إنشاء سياسة التحكم في الوصول التي تسمح لحركة المرور من عملاء AnyConnect بالوصول إلى الشبكة الداخلية كما هو موضح في الصورة:



يمكن تكوين إستثناء NAT يدويا تحت Policies > NAT أو يمكن تكوينه تلقائيا بواسطة المعالج. أختر الواجهة الداخلية والشبكات التي يحتاج إليها عملاء AnyConnect للوصول كما هو موضح في الصورة.



أختر حزمة AnyConnect لكل نظام تشغيل (Windows/Mac/Linux) يمكن للمستخدمين الاتصال به، كما هو موضح في الصورة.



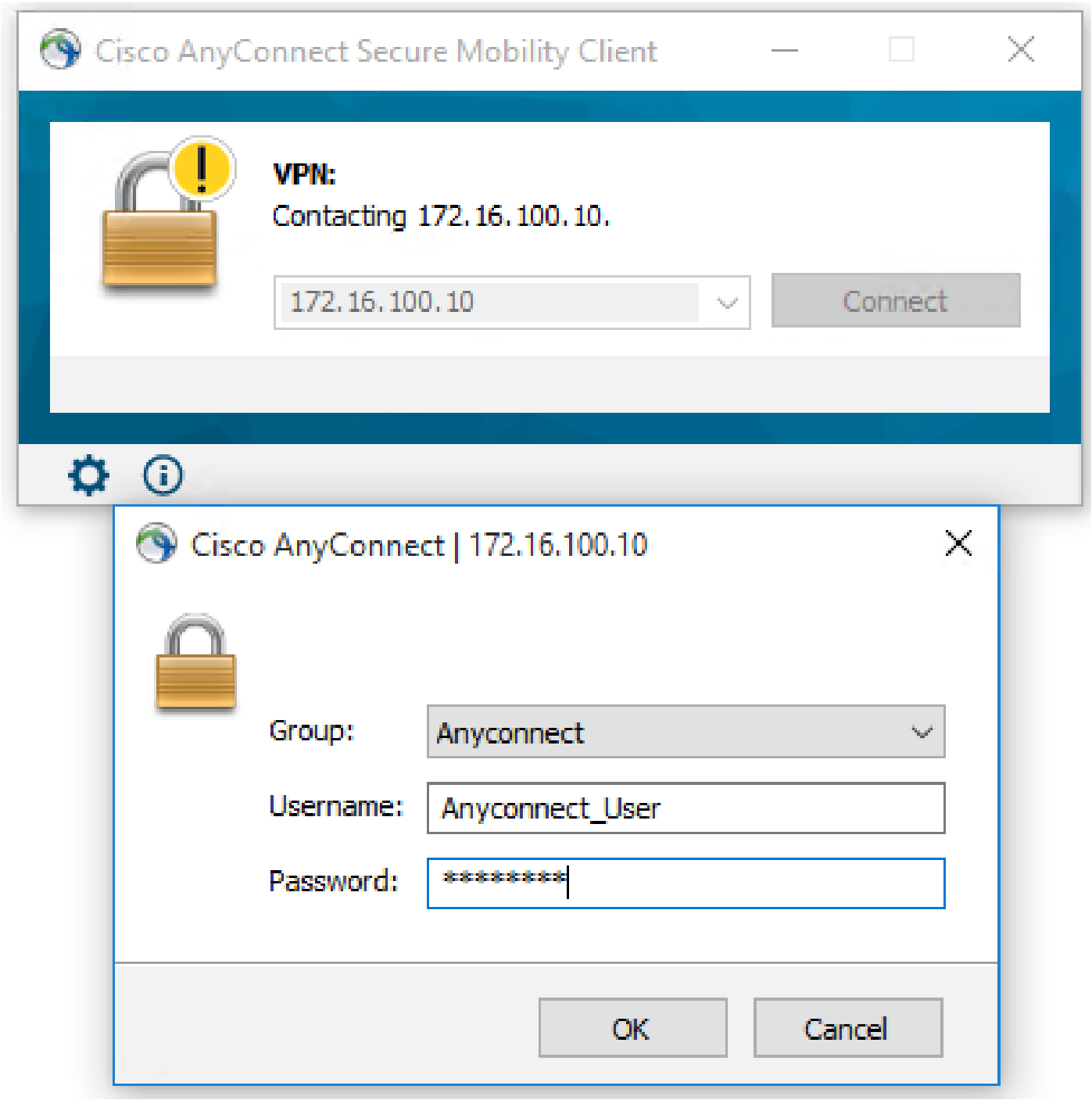
تعطي الصفحة الأخيرة ملخصا للتكوين بأكمله. تأكد من تعيين المعلمات الصحيحة واضغط على الزر "إنهاء" ونشر التكوين الجديد.

التحقق من الصحة

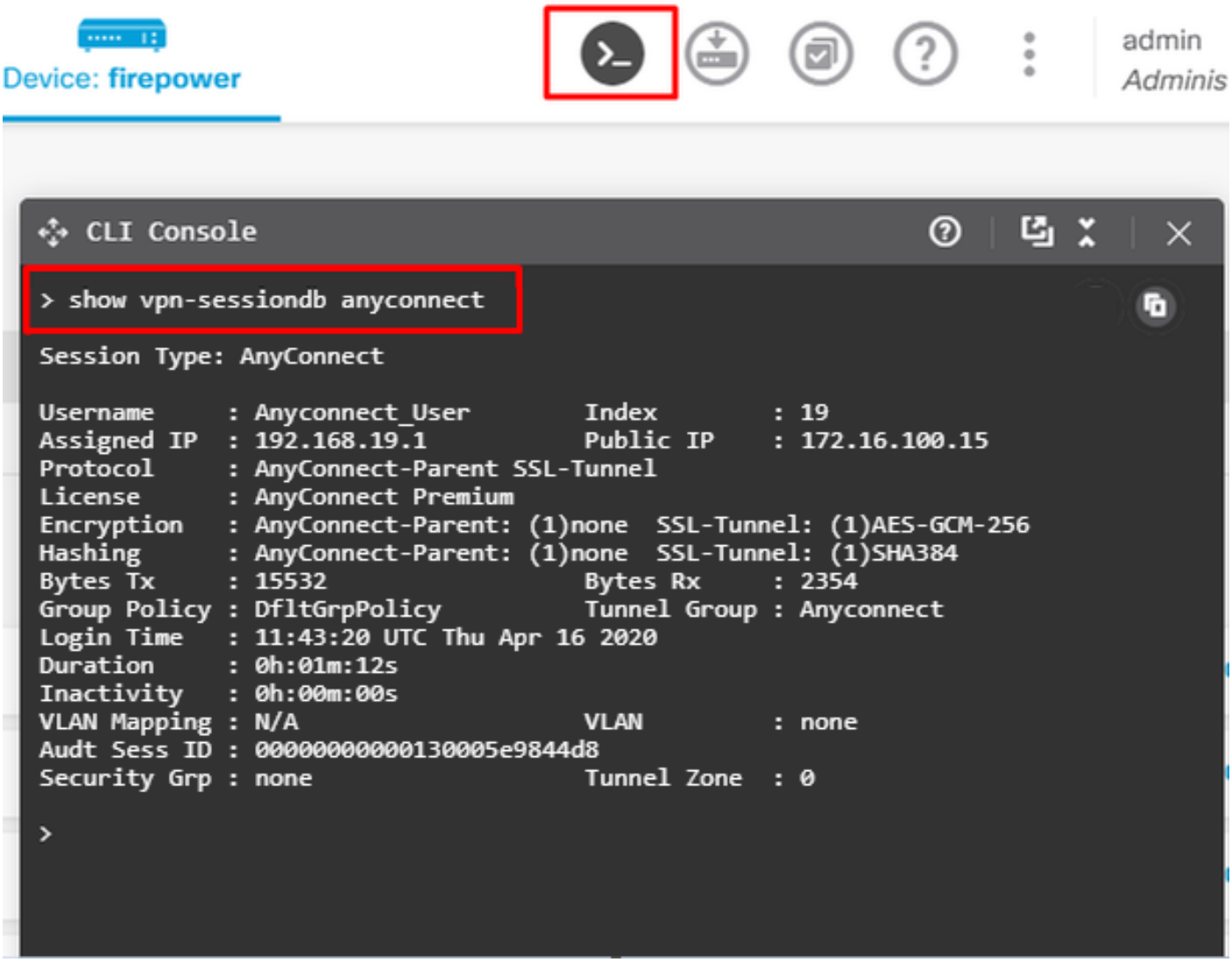
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

بمجرد نشر التكوين، حاول الاتصال. إذا كانت لديك شبكة FQDN تقوم بالحل إلى IP الخارجي الخاص ب FTD، فأدخل الشبكة في مربع اتصال AnyConnect. في هذا المثال، يتم إستخدام عنوان IP الخارجي ل FTD. أستخدم اسم المستخدم/كلمة المرور التي تم إنشاؤها في قسم

الكائنات في FDM كما هو موضح في الصورة.



اعتبارا من FDM 6.5.0، ال توجد طريقة لمراقبة مستخدمي AnyConnect من خلال واجهة المستخدم الرسومية (GUI) ل FDM. الخيار الوحيد هو مراقبة مستخدمي AnyConnect عبر CLI (واجهة سطر الأوامر). يمكن إستخدام وحدة تحكم واجهة سطر الأوامر (CLI) الخاصة بواجهة المستخدم الرسومية (GUI) ل FDM كذلك للتحقق من اتصال المستخدمين. أستخدم هذا الأمر، Show vpn-sessiondb anyconnect.



يمكن تشغيل الأمر نفسه مباشرة من واجهة سطر الأوامر (CLI).

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Anyconnect_User        Index        : 15
Assigned IP  : 192.168.19.1           Public IP    : 172.16.100.15
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     : 38830                  Bytes Rx     : 172
Group Policy : DfltGrpPolicy          Tunnel Group : Anyconnect
Login Time   : 01:08:10 UTC Thu Apr 9 2020
Duration     : 0h:00m:53s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000f0005e8e757a
Security Grp : none                   Tunnel Zone  : 0
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم المعلومات التي يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إذا تعذر على المستخدم الاتصال بـ FTD باستخدام SSL، فقم بتنفيذ الخطوات التالية لعزل مشكلة تفاوض SSL:

1. تحقق من إمكانية إدخال عنوان IP الموجود خارج FTD من خلال كمبيوتر المستخدم.
2. أستخدم sniffer خارجي للتحقق مما إذا كانت مصافحة TCP الثلاثية ناجحة.

مشكل عميل AnyConnect

يوفر هذا القسم إرشادات لاستكشاف أخطاء AnyConnect VPN العميلة الأكثر شيوعا وإصلاحها. يمكن العثور على دليل أستكشاف الأخطاء وإصلاحها لعميل AnyConnect هنا: دليل أستكشاف أخطاء عميل AnyConnect VPN وإصلاحها.

مشكلات الاتصال الأولية

إذا كان لدى مستخدم مشكل اتصال أولية، قم بتمكين تصحيح الأخطاء webvpn AnyConnect على FTD وتحليل رسائل تصحيح الأخطاء. يجب تشغيل تصحيح الأخطاء على CLI (واجهة سطر الأوامر) الخاصة بـ FTD. استخدم الأمر debug webvpn anyconnect 255.

قم بتجميع حزمة DART من جهاز العميل للحصول على السجلات من AnyConnect. يمكن الاطلاع على تعليمات حول كيفية تجميع حزمة DART هنا: تجميع حزم DART.

المشاكل الخاصة بحركة المرور

إذا نجح اتصال ولكن فشل حركة مرور البيانات عبر نفق SSL VPN، فراجع إحصائيات حركة مرور البيانات على العميل للتحقق من تلقي حركة مرور البيانات ونقلها بواسطة العميل. تتوفر إحصائيات تفصيلية حول العملاء في جميع إصدارات AnyConnect. إذا أظهر العميل أنه تم إرسال حركة المرور واستقبالها، فتحقق من FTD بحثا عن حركة المرور المسلمة والمحولة. إذا كان FTD يطبق عامل تصفية، يتم عرض اسم المرشح ويمكنك مراجعة إدخالات قائمة التحكم في الوصول للتحقق مما إذا كانت حركة المرور الخاصة بك يتم إسقاطها. المشاكل الشائعة لحركة المرور التي يواجهها المستخدمون هي:

- مشكل التوجيه خلف FTD - يتعذر على الشبكة الداخلية توجيه الحزم مرة أخرى إلى عناوين IP المخصصة وعملاء VPN
- قوائم التحكم في الوصول التي تمنع حركة المرور
- ال يتم تجاوز ترجمة عنوان الشبكة لحركة مرور VPN

للحصول على مزيد من المعلومات حول شبكات VPN للوصول عن بعد على FTD الذي تتم إدارته بواسطة FDM، ابحث عن دليل التكوين الكامل هنا: برنامج FTD للوصول عن بعد الذي تتم إدارته بواسطة FDM.

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).