تكوين عميل AnyConnect VPN على FTD: إستثناء HAIRpin و NAT

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين حل VPN للوصول عن بعد إلى Cisco (AnyConnect) على FirePOWER Threat Defense (FTD)، الإصدار 6.3، الذي تتم إدارته بواسطة FMC.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الشبكة الخاصة الظاهرية (VPN) الأساسية للوصول عن بعد ومعرفة طبقة مآخذ التوصيل الآمنة (SSL) وتبادل مفاتيح الإنترنت الإصدار 2 (IKEv2)
- المصادقة والتفويض والمحاسبة (AAA) الأساسية ومعرفة RADIUS
- معرفة FMC الأساسية
- معرفة أساسية ببروتوكول FTD

المكونات المستخدمة

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

- Cisco FMC، الإصدار 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

يصف هذه المستند إجراء تكوين حل VPN للوصول عن بعد إلى Cisco (AnyConnect) على الدفاع عن تهديد FirePOWER (FTD)، الإصدار 6.3، المدار بواسطة مركز إدارة FirePOWER (FMC).

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

معلومات أساسية

يهدف هذه المستند إلى تغطية التكوين على أجهزة FTD. إذا كنت تبحث عن مثال تكوين ASA، فيرجى الرجوع إلى المستند: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html

القيود:

حاليا، هذه سمة ال يسانده على FTD، غير أن بعد يتوفر على ASA أداة:
- مصادقة AAA مزدوجة (متوفرة على الإصدار 6.5 من FTD)
- سياسة الوصول الديناميكي
- فحص المضيف
- ISE Posture
- RADIUS COa
- موازن حمل VPN
- المصادقة المحلية (متوفرة على FirePOWER Device Manager، الإصدار 6.3. معرف تصحيح الأخطاء من Cisco CSCvf92680)
- خريطة سمة LDAP (متوفرة عبر FlexConfig، معرف تصحيح الأخطاء من Cisco CSCvd64585)
- تخصيص AnyConnect
- برامج AnyConnect النصية
- تعريب AnyConnect
- شبكة VPN لكل تطبيق
- وكيل SCEP
- تكامل WSA
- SAML SSO (معرف الأخطاء من Cisco CSCvq90789)
- خريطة التشفير الديناميكية المتزامنة IKEv2 ل RA و L2L VPN
- وحدات AnyConnect (NAM و Hostscan و AMP Enabler و SBL و Umbrella وأمان الويب وما إلى ذلك). DART هو الوحدة النمطية الوحيدة المثبتة بشكل افتراضي على هذا الإصدار.
- TACACS، Kerberos (مصادقة KCD و RSA SDI)
- وكيل المستعرض

التكوين

للانتقال من خلال معالج Remote Access VPN في FMC، يجب إكمال الخطوات التالية:

الخطوة 1. إستيراد شهادة SSL

الشهادات ضرورية عند تكوين AnyConnect. يتم دعم الشهادات المستندة إلى RSA فقط لـ SSL و IPSec.

شهادات خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA) مدعومة في IPSec، ومع ذلك، لا يمكن نشر حزمة AnyConnect جديدة أو توصيف XML عند إستخدام شهادة تستند إلى ECDSA.

يمكن إستخدامه ل IPSec، ولكن يجب عليك النشر المسبق لحزم AnyConnect مع ملف تعريف XML، ويجب دفع جميع تحديثات ملف تعريف XML يدويا على كل عميل (معرف تصحيح الأخطاء من Cisco CSCtx42595).

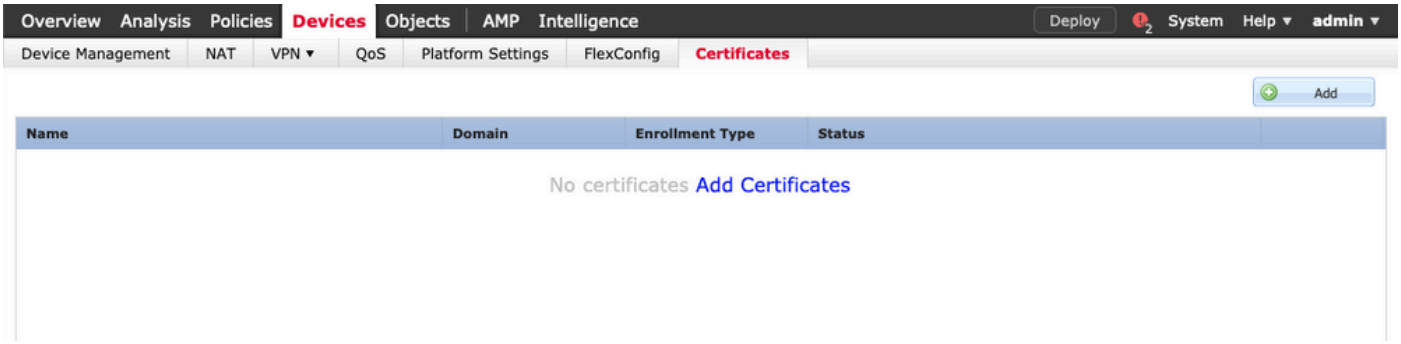
بالإضافة إلى ذلك، يجب أن تحتوي الشهادة على ملحق اسم مشترك (CN) باسم DNS و/أو عنوان IP لتجنب أخطاء "شهادة خادم غير موثوق بها" في مستعرضات الويب.

ملاحظة: في أجهزة FTD، يلزم وجود شهادة المرجع المصدق (CA) قبل إنشاء طلب توقيع الشهادة (CSR).

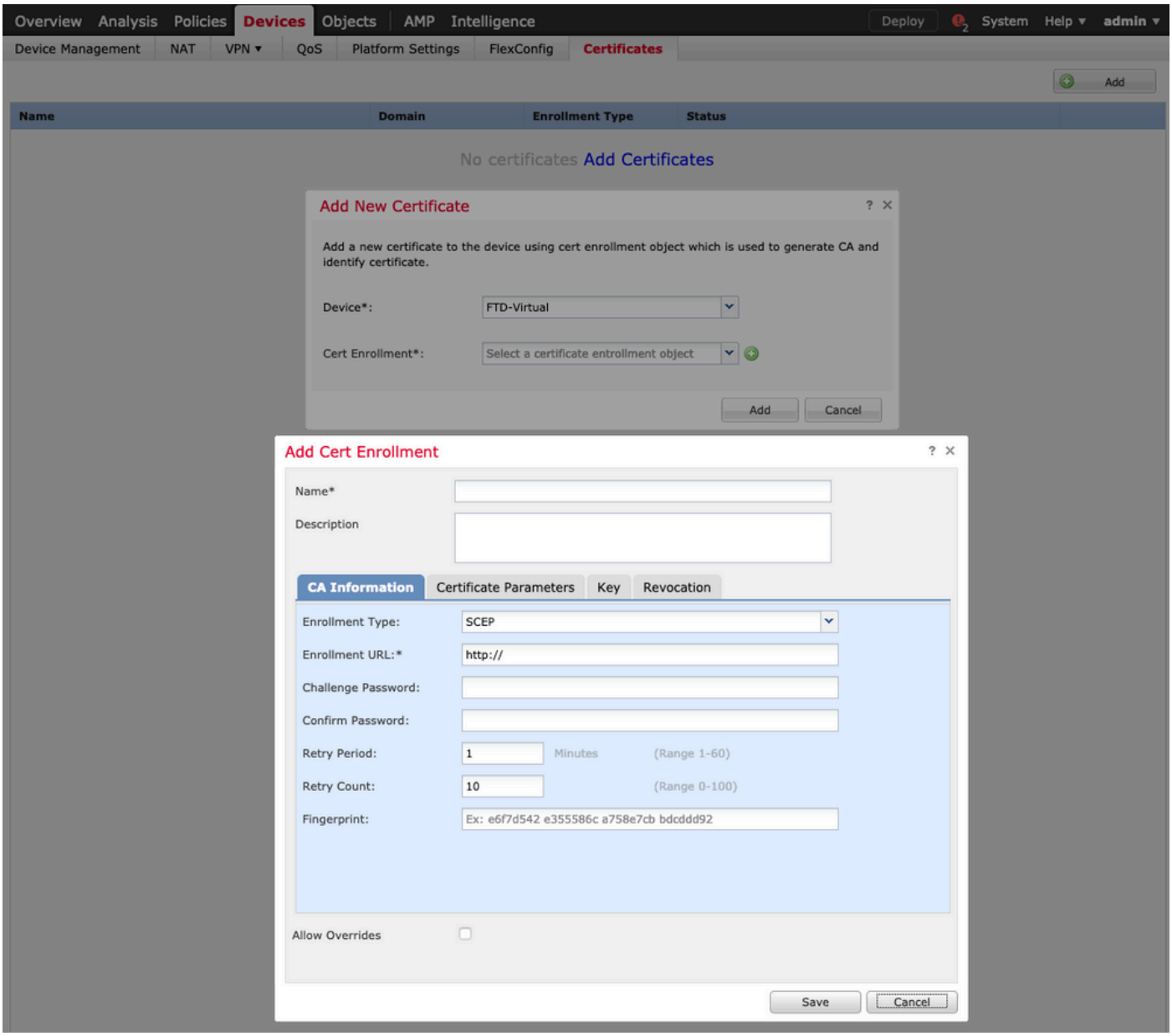
- إذا تم إنشاء CSR في خادم خارجي (مثل Windows Server أو OpenSSL)، فيقصد من طريقة التسجيل اليدوي الفشل، نظرا لأن FTD لا يدعم تسجيل المفاتيح يدويا.
- يجب إستخدام أسلوب مختلف مثل PKCS12.

للحصول على شهادة لجهاز FTD باستخدام طريقة التسجيل اليدوي، يلزم إنشاء CSR، وتوقيعه باستخدام CA ثم إستيراد شهادة الهوية.

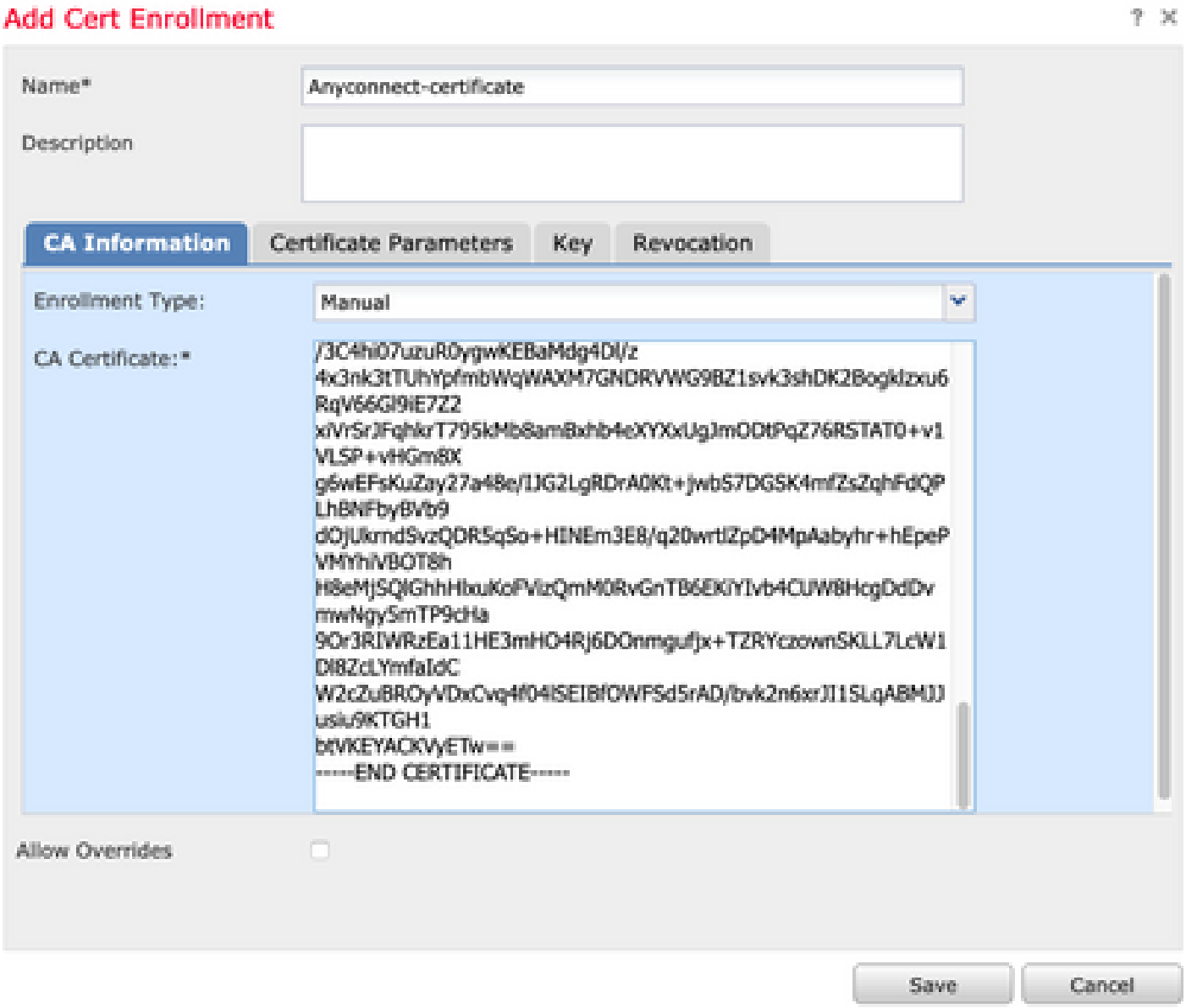
1. انتقل إلى الأجهزة > الشهادات وحدد إضافة كما هو موضح في الصورة.



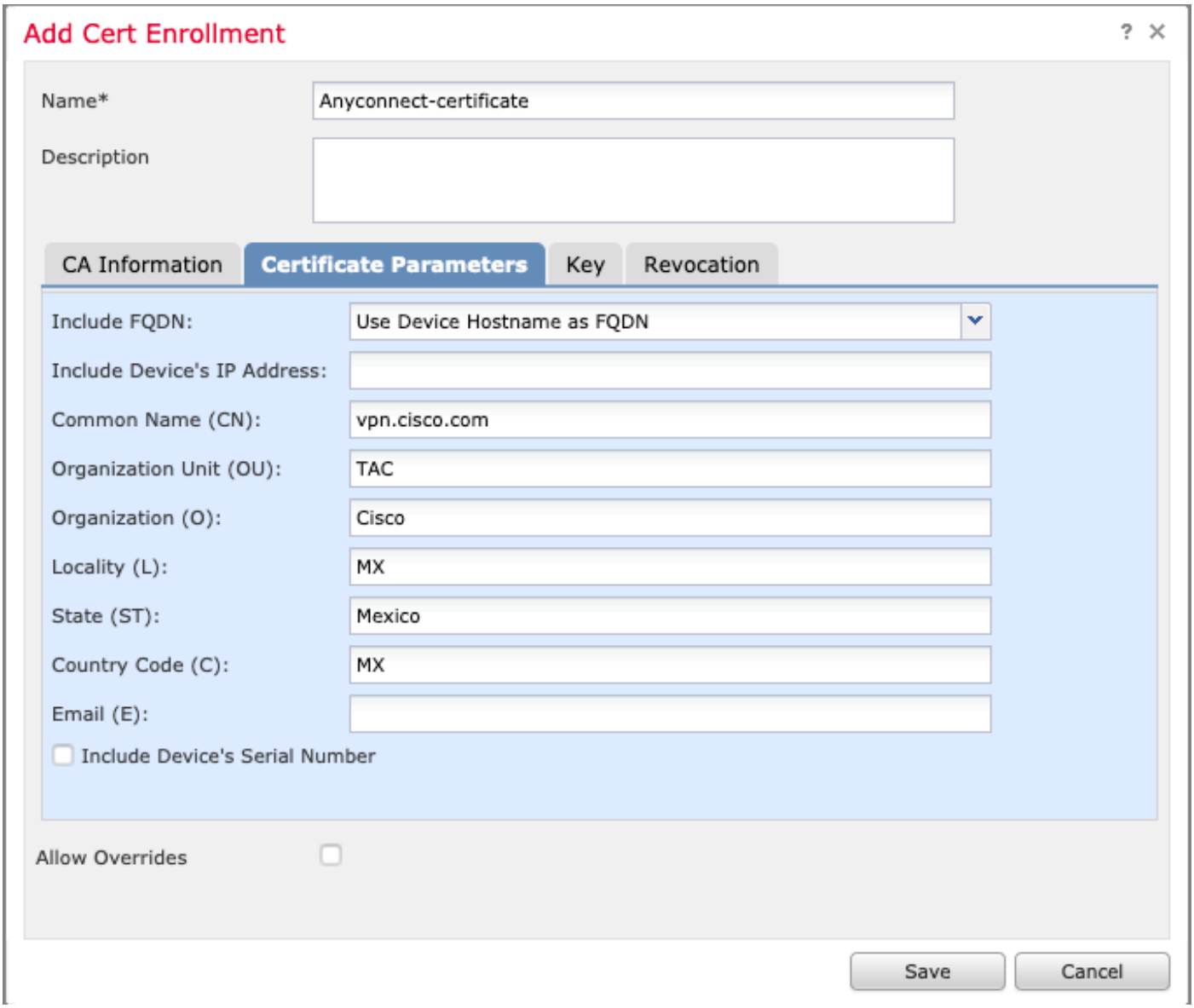
2. حدد الجهاز وأضف كائن تسجيل شهادة جديد كما هو موضح في الصورة.



3. حدد نوع التسجيل اليدوي ولصق شهادة CA (الشهادة التي يقصد منها توقيع CSR).

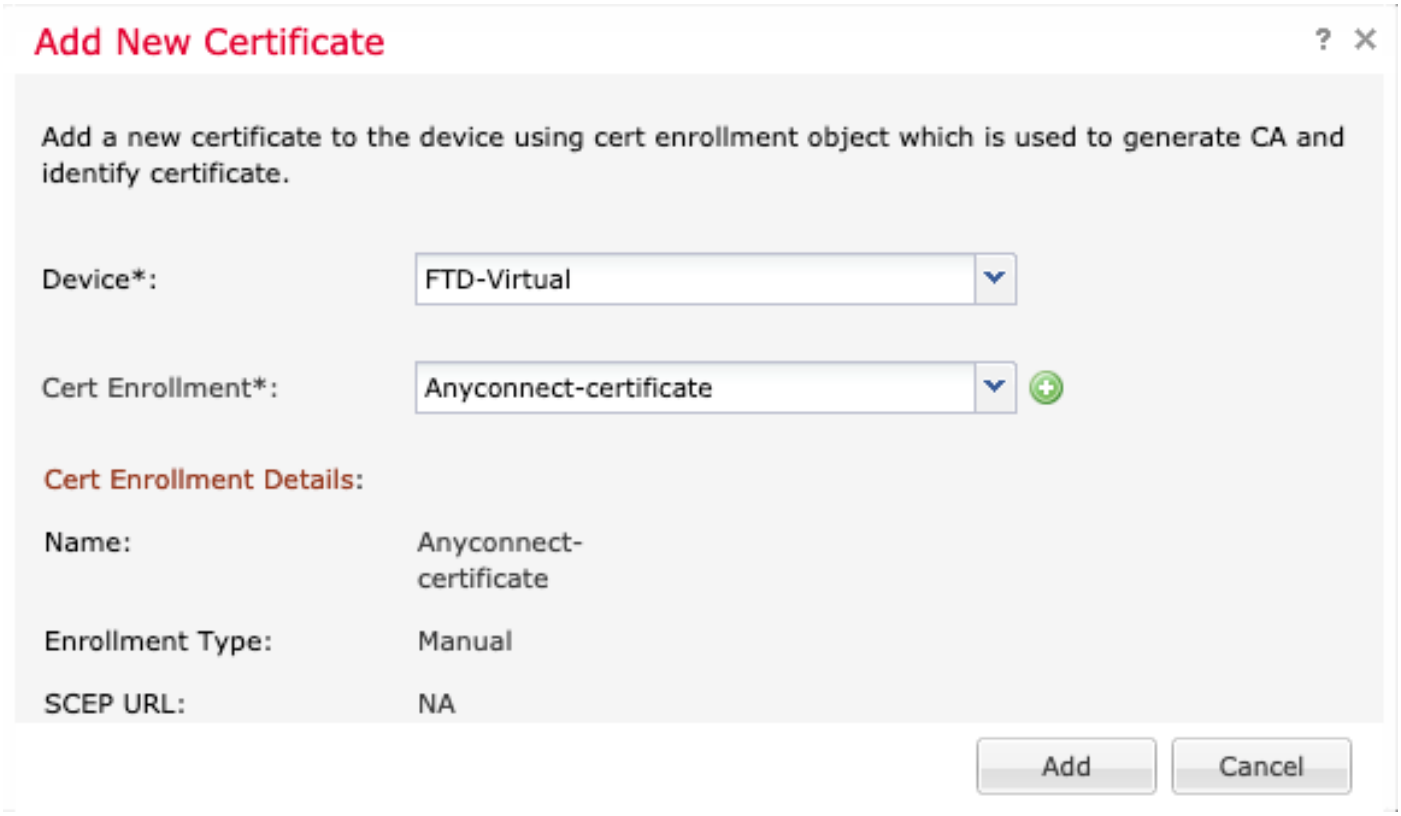


4. حدد علامة التبويب معلمات الشهادة وحدد "FQDN المخصص" لحقل تضمين FQDN وقم بتعبئة تفاصيل الشهادة الموضحة في الصورة.

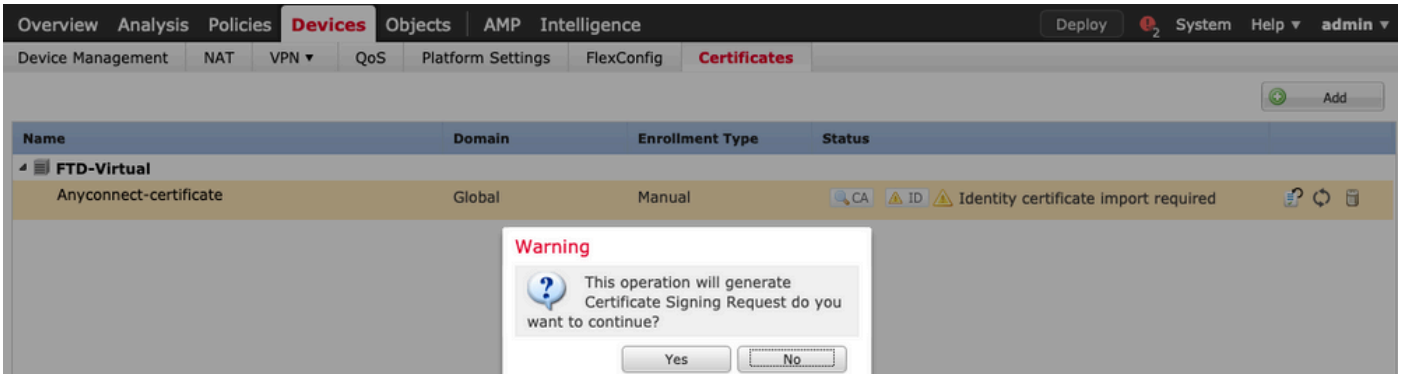


5. حدد علامة التبويب مفتاح، وحدد نوع المفتاح، يمكنك إختيار الاسم والحجم. بالنسبة إلى RSA، يعد 2048 بايت متطلبا أدنى.

6. حدد حفظ، تأكد من الجهاز، ثم حدد ضمن تسجيل الثقة TrustPoint الذي تم إنشاؤه للتو، حدد إضافة لنشر الشهادة.

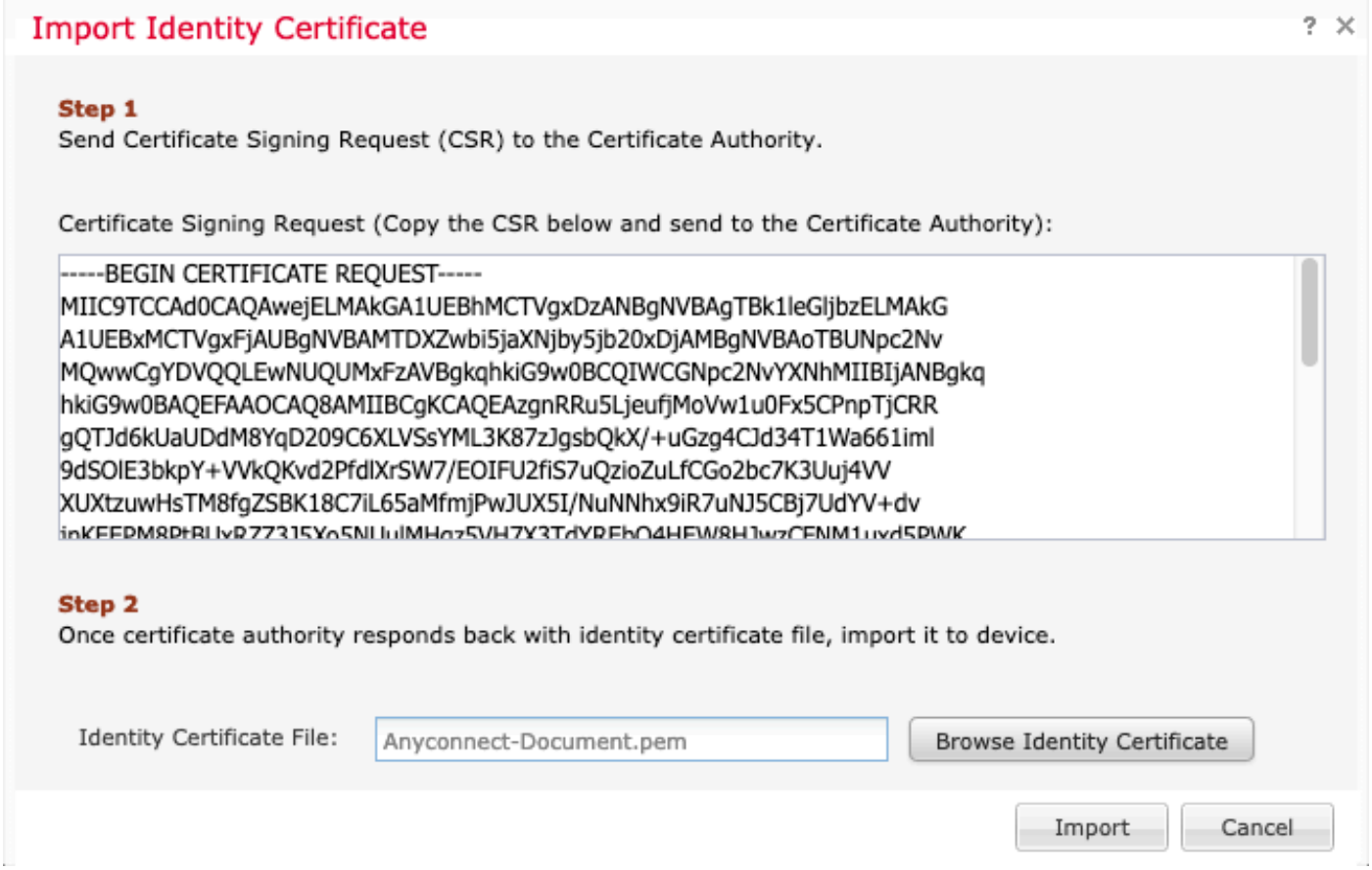


7. في عمود الحالة، حدد أيقونة المعرف وحدد نعم لإنشاء CSR كما هو موضح في الصورة.

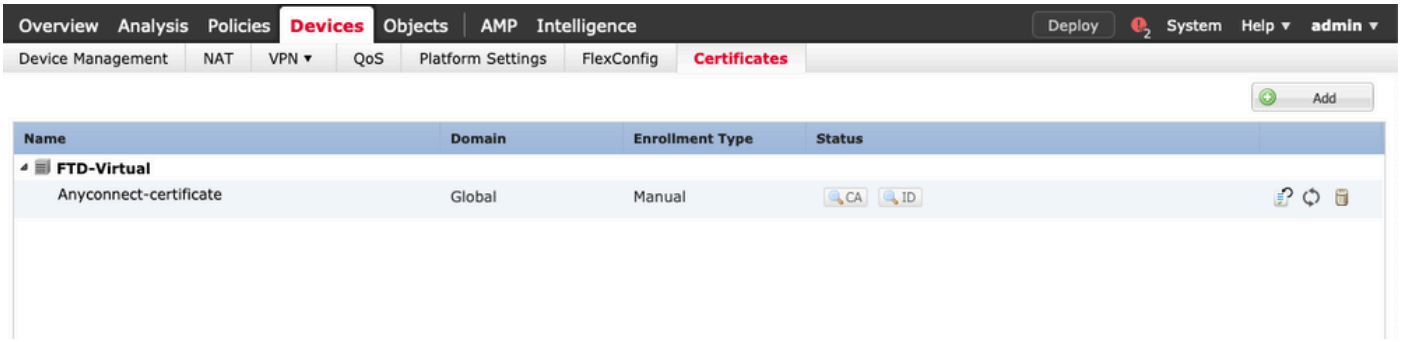


8. انسخ CSR وتوقيعه مع CA المفضل لديك (على سبيل المثال GoDaddy أو DigiCert).

9. بمجرد إستلام شهادة الهوية من المرجع المصدق (والذي يجب أن يكون بتنسيق base64)، حدد إستعراض شهادة الهوية وحدد مكان الشهادة في الكمبيوتر المحلي. حدد إستيراد.



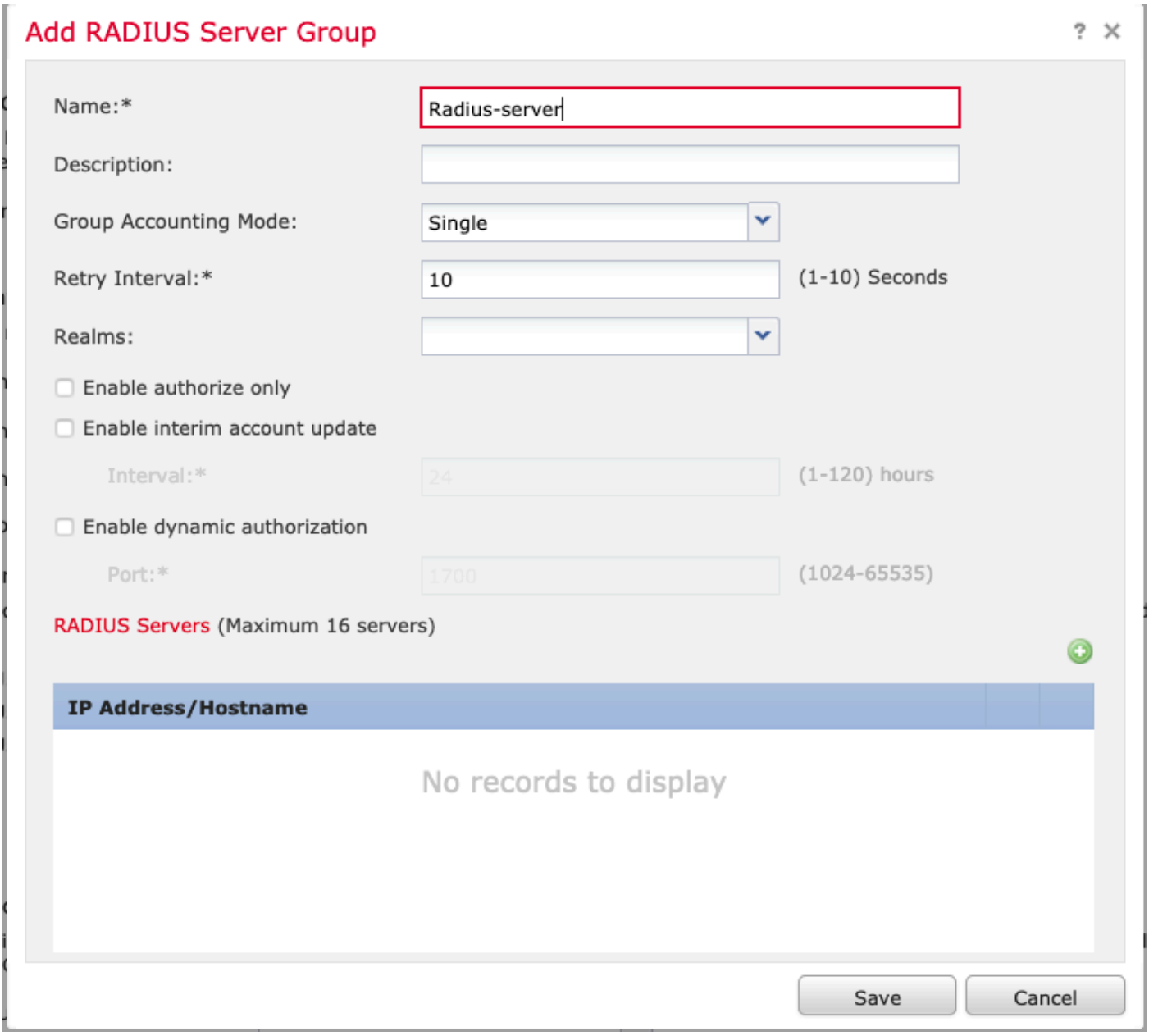
10. بمجرد الاستيراد، ستتوفر تفاصيل شهادة مرجع مصدق ومعرف الهوية على حد سواء للعرض.



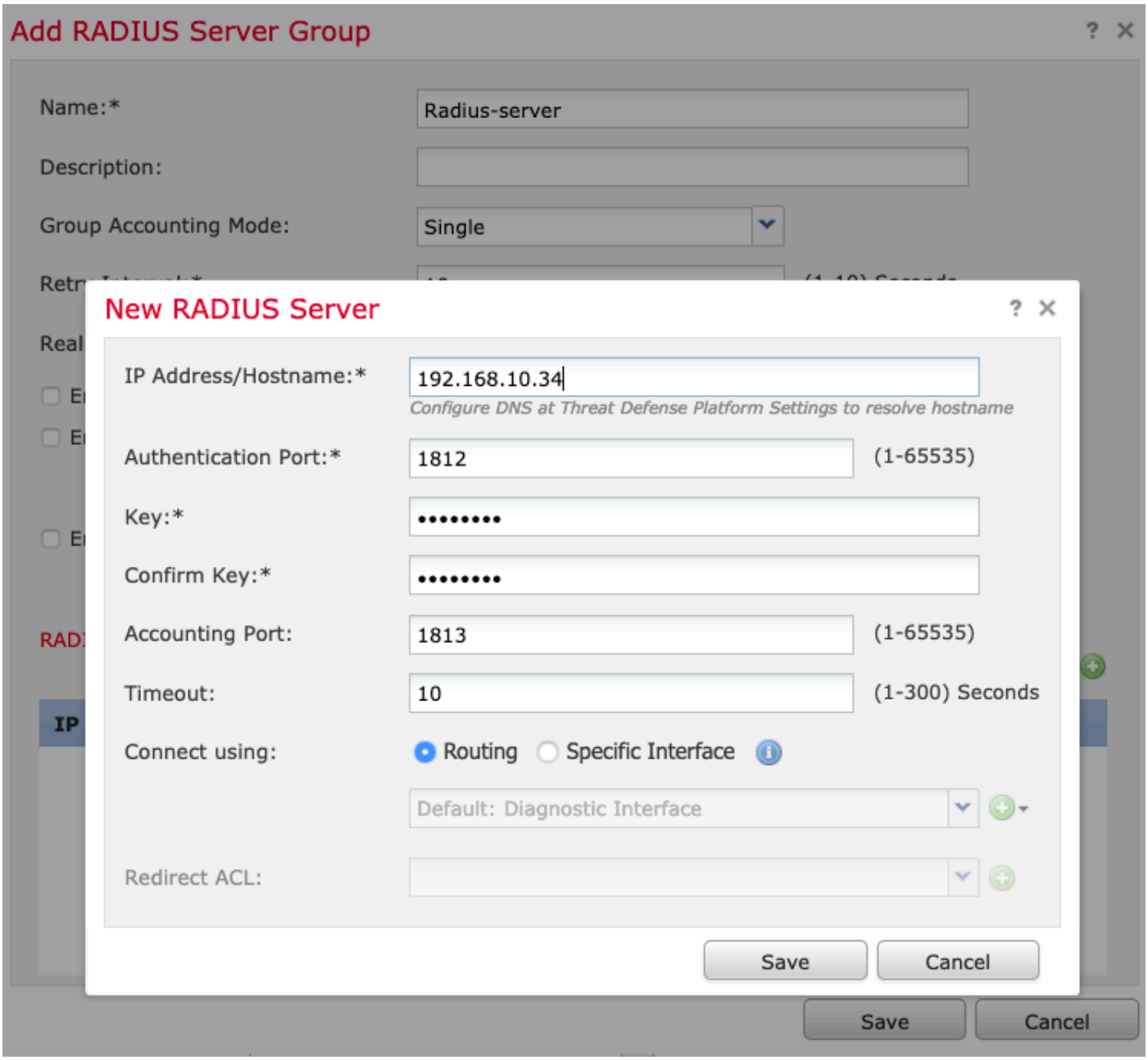
الخطوة 2. تكوين خادم RADIUS

في أجهزة FTD المدارة بواسطة FMC، قاعدة بيانات المستخدم المحلية غير مدعومة، يجب إستخدام طريقة مصادقة أخرى، مثل RADIUS أو LDAP.

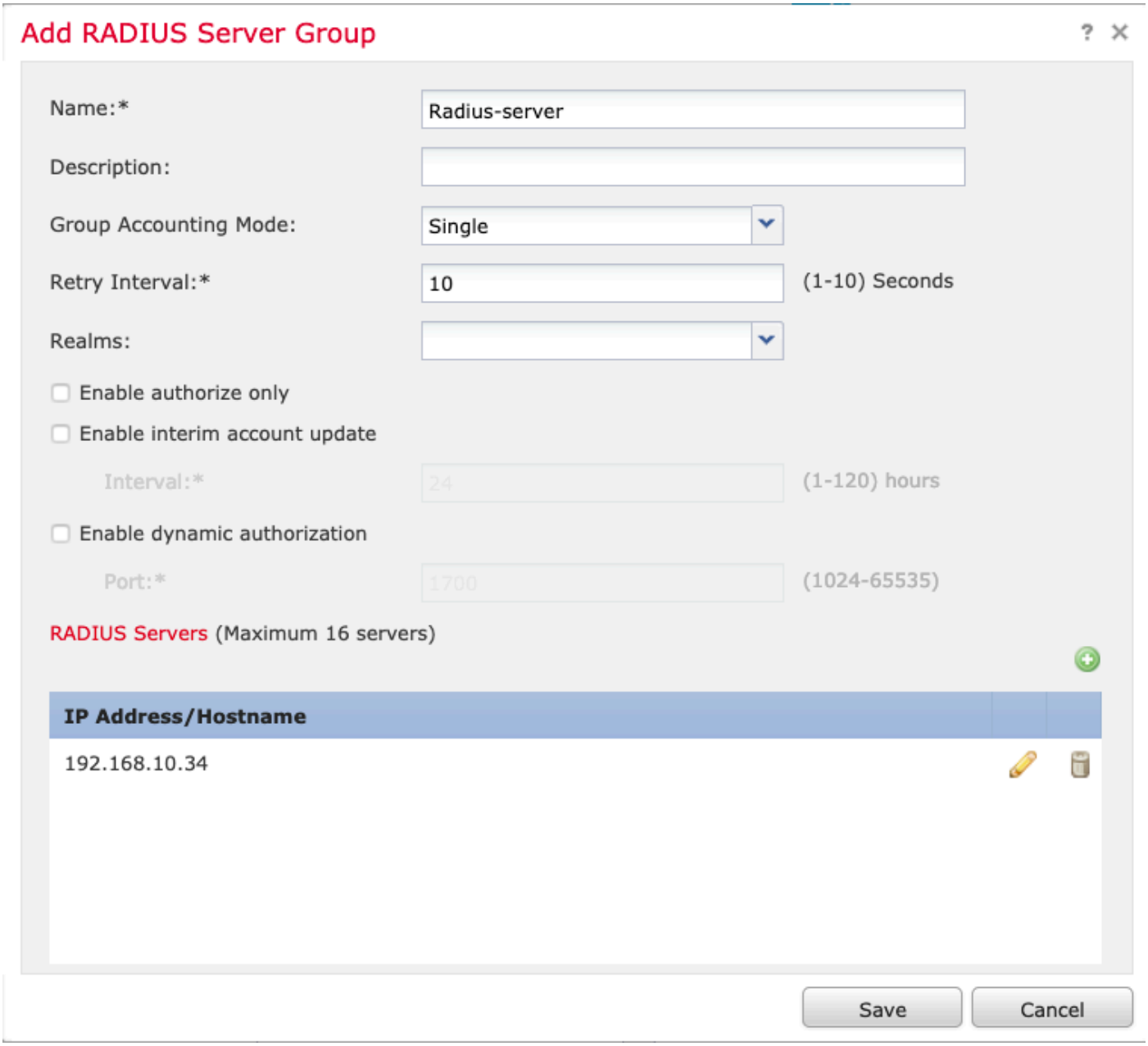
1. انتقل إلى الكائنات > إدارة الكائن > مجموعة خوادم RADIUS > إضافة مجموعة خوادم RADIUS كما هو موضح في الصورة.



2. قم بتعيين اسم إلى مجموعة خوادم RADIUS وأضف عنوان IP لخادم RADIUS مع سر مشترك (السر المشترك مطلوب لإقران FTD مع خادم RADIUS)، وحدد حفظ بمجرد اكتمال هذا النموذج كما هو موضح في الصورة.



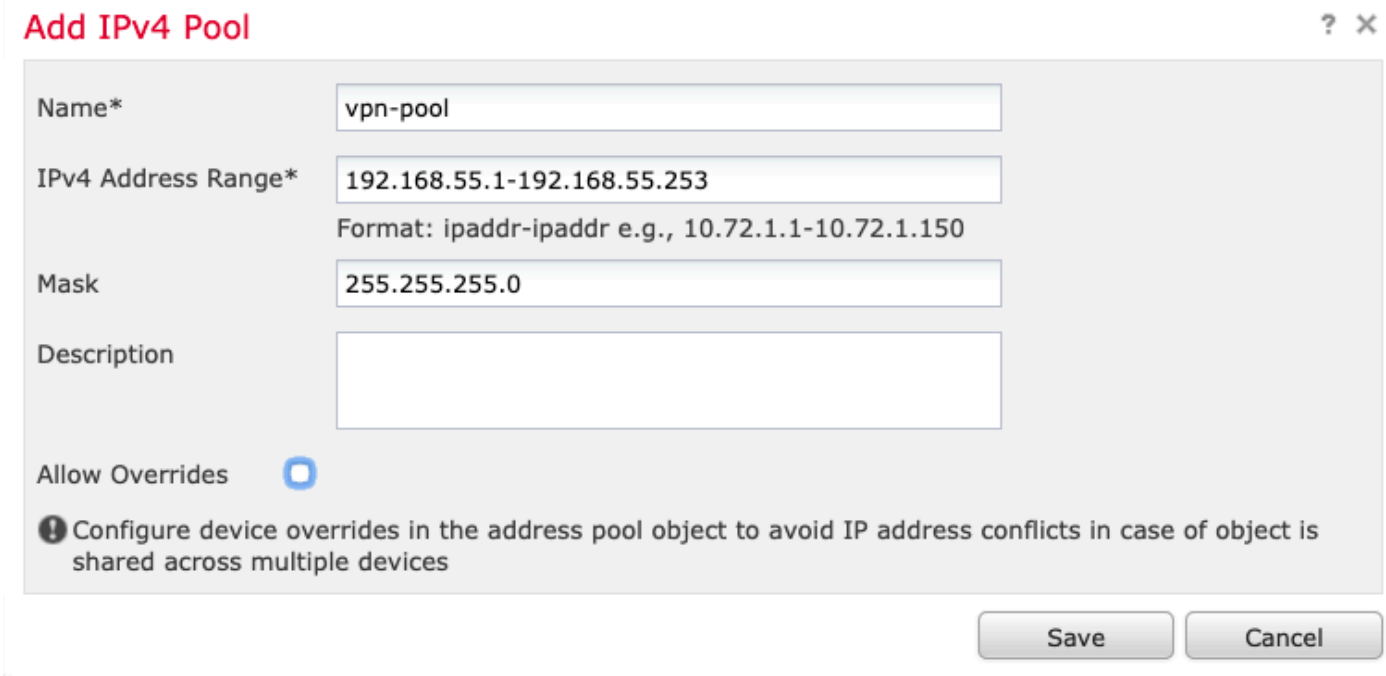
3. تتوفر الآن معلومات خادم RADIUS في قائمة خادم RADIUS كما هو موضح في الصورة.



الخطوة 3. إنشاء تجمع IP

1. انتقل إلى الكائنات > إدارة الكائنات > تجمعات العناوين > إضافة تجمعات IPv4.

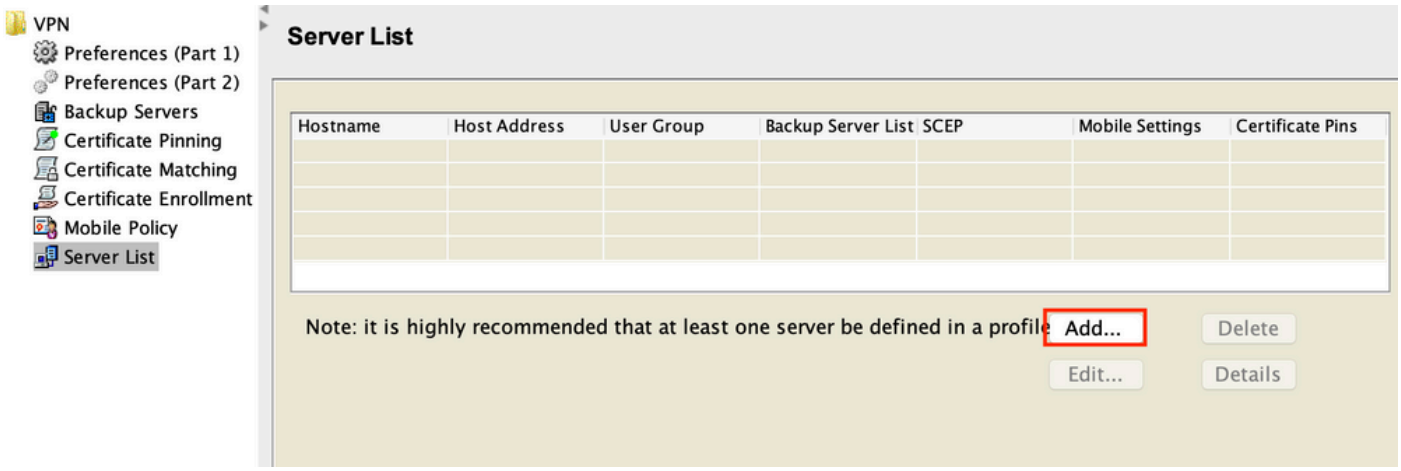
2. قم بتعيين اسم ونطاق عناوين IP، لا يكون حقل القناع مطلوبا ولكن يمكن تحديده كما هو موضح في الصورة.



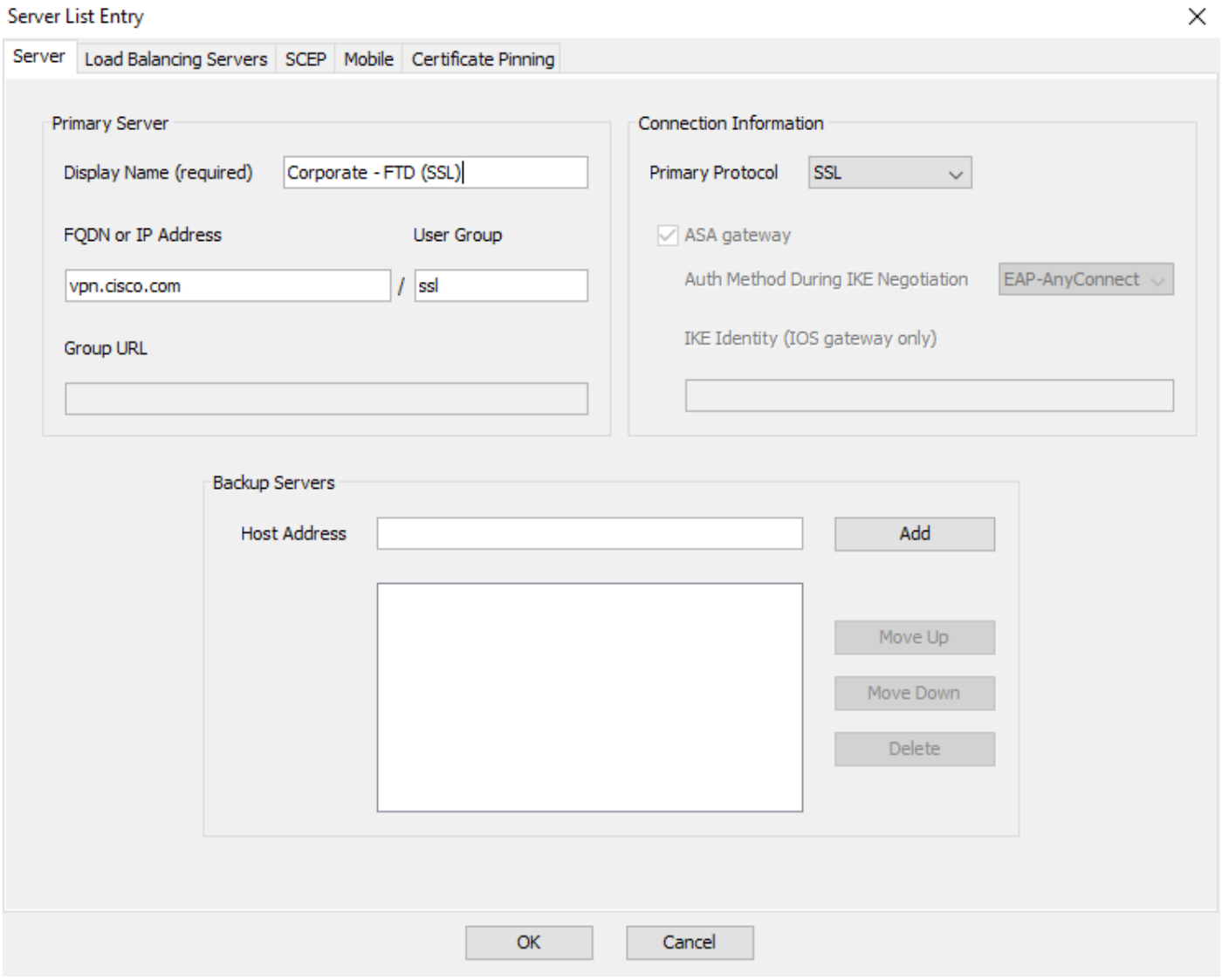
الخطوة 4. إنشاء ملف تعريف XML

1. قم بتنزيل أداة محرر ملفات التعريف من موقع الويب Cisco.com وقم بتشغيل التطبيق.

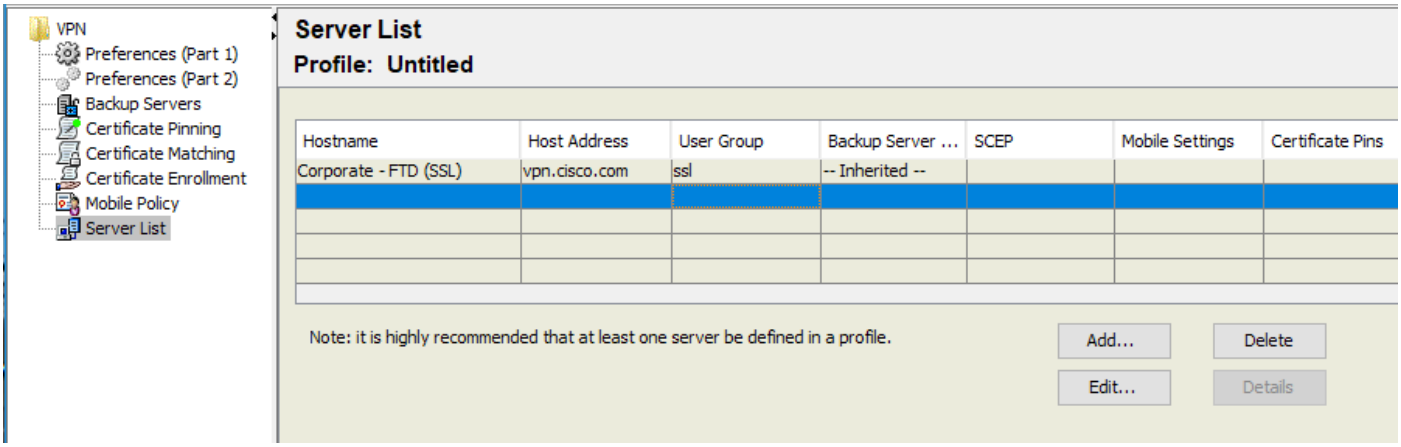
2. في تطبيق محرر ملف التعريف، انتقل إلى قائمة الخوادم وحدد إضافة كما هو موضح في الصورة.



3. قم بتعيين اسم عرض أو اسم مجال مؤهل بالكامل (FQDN) أو عنوان IP وحدد موافق كما هو موضح في الصورة.



4. يظهر الإدخال الآن في قائمة الخوادم :



5. انتقل إلى ملف > حفظ باسم.

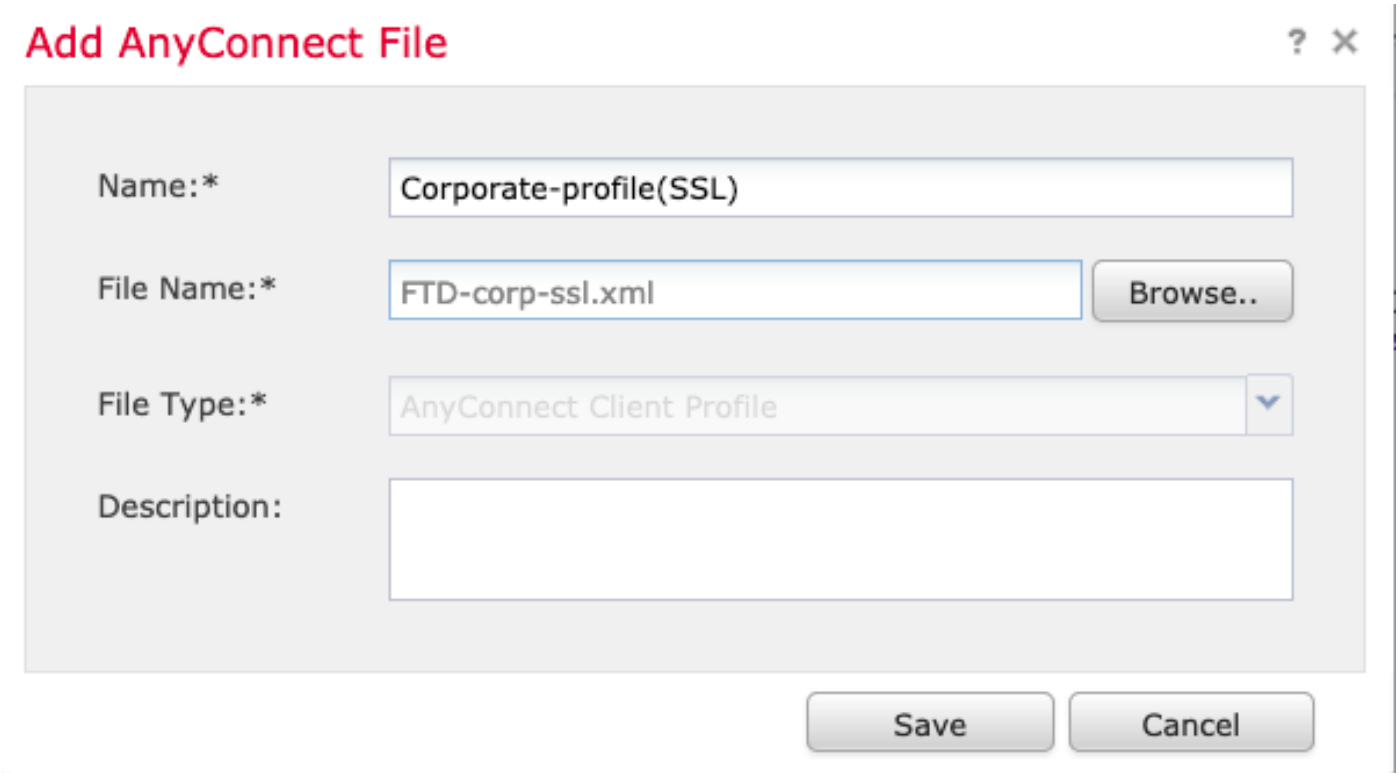
ملاحظة: احفظ ملف التعريف باسم يمكن التعرف عليه بسهولة باستخدام ملحق .xml.

الخطوة 5. تحميل ملف تعريف AnyConnect XML

1. في FMC، انتقل إلى كائنات > إدارة الكائن > VPN > ملف AnyConnect > إضافة ملف AnyConnect.

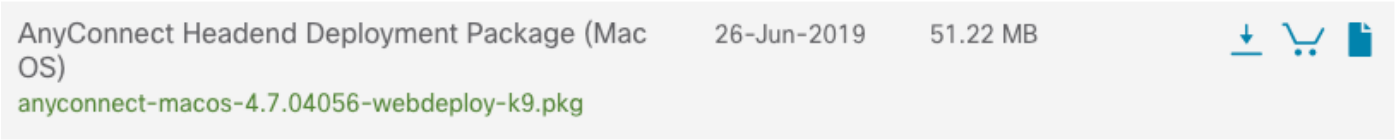
2. قم بتعيين اسم للكائن وانقر فوق إستعراض، وحدد ملف تعريف العميل في نظامك المحلي وحدد حفظ.

⚠ تحذير: تأكد من تحديد ملف تعريف عميل AnyConnect كنوع الملف.



الخطوة 6. تحميل صور AnyConnect

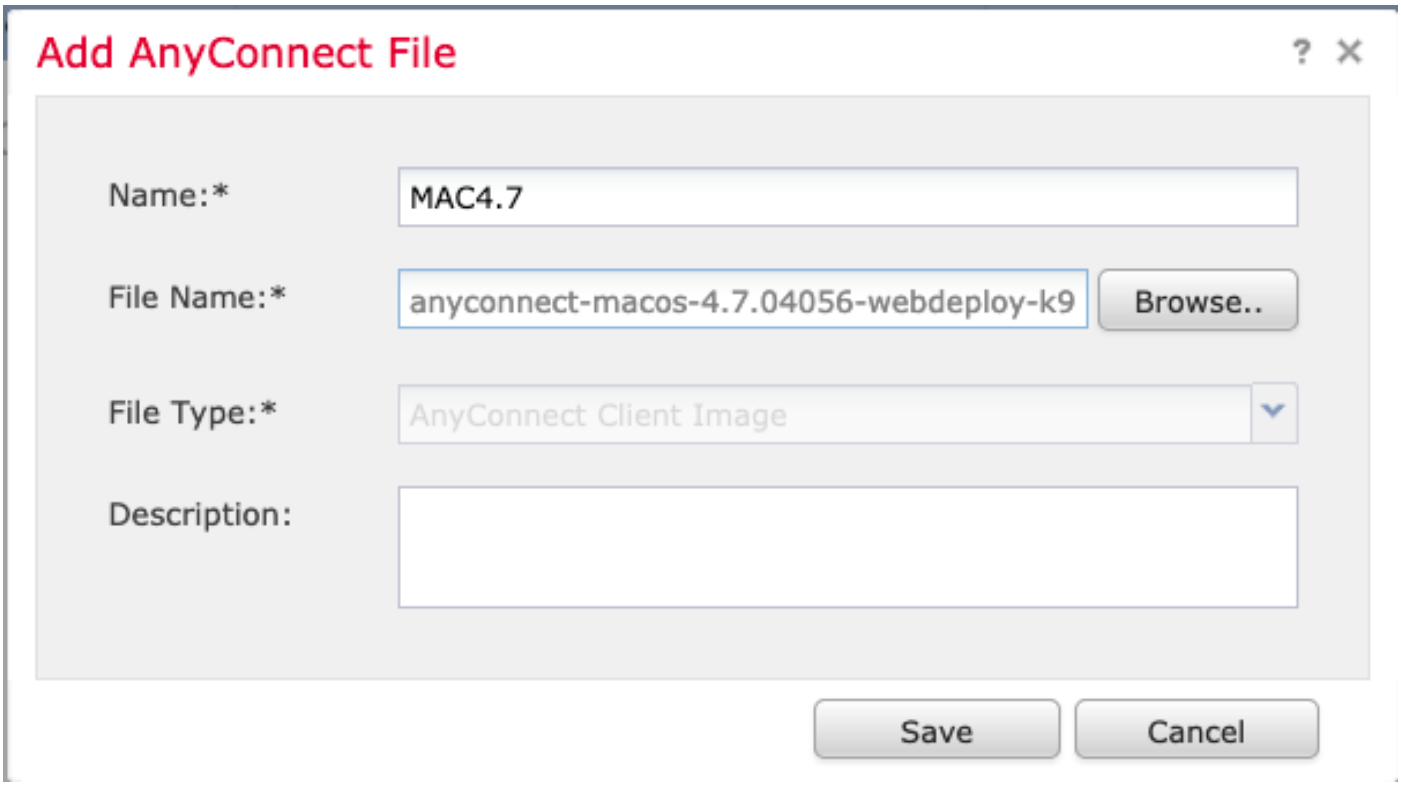
1. تنزيل صور النشر عبر الويب (.pkg) من صفحة الويب الخاصة بتنزيلات Cisco.



2. انتقل إلى كائنات > إدارة الكائن > VPN > ملف AnyConnect > إضافة ملف AnyConnect.

3. قم بتعيين اسم لملف حزمة AnyConnect وحدد ملف .pkg من نظامك المحلي، بمجرد تحديد الملف.

4. حدد حفظ.



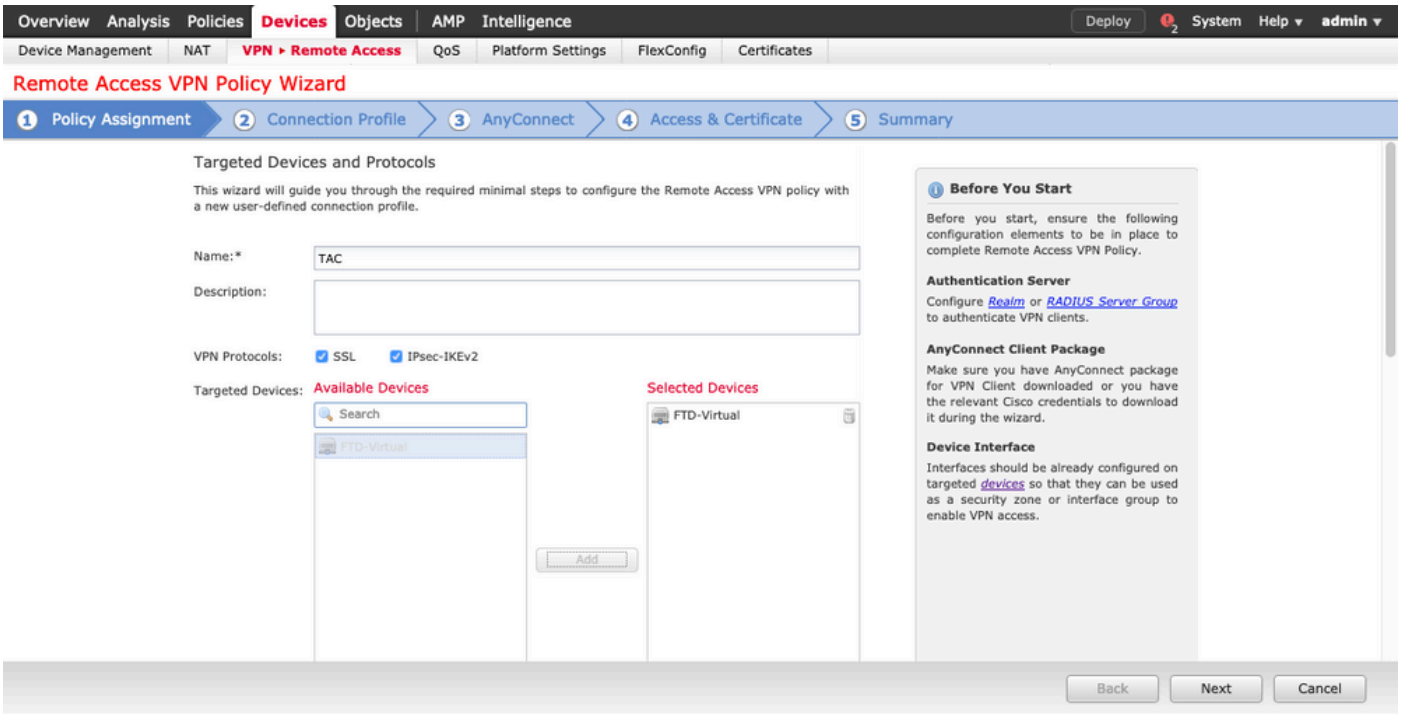
ملاحظة: يمكن تحميل حزم إضافية استنادا إلى متطلباتك (نظام التشغيل Windows و Mac و Linux).

الخطوة 7. معالج Remote Access VPN

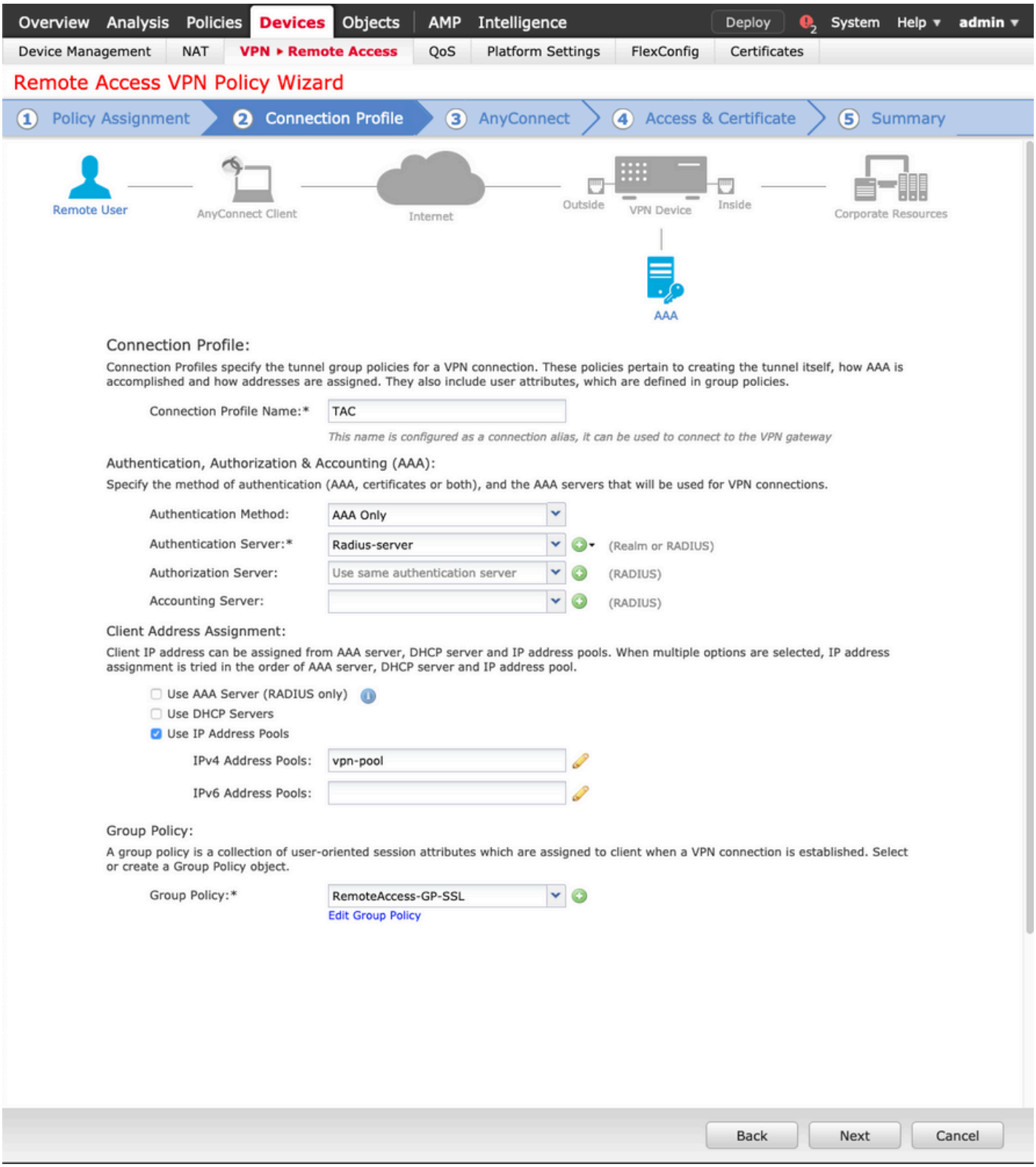
استنادا إلى الخطوات السابقة، يمكن اتباع "معالج الوصول عن بعد" وفقا لذلك.

1. انتقل إلى الأجهزة > VPN > الوصول عن بعد.

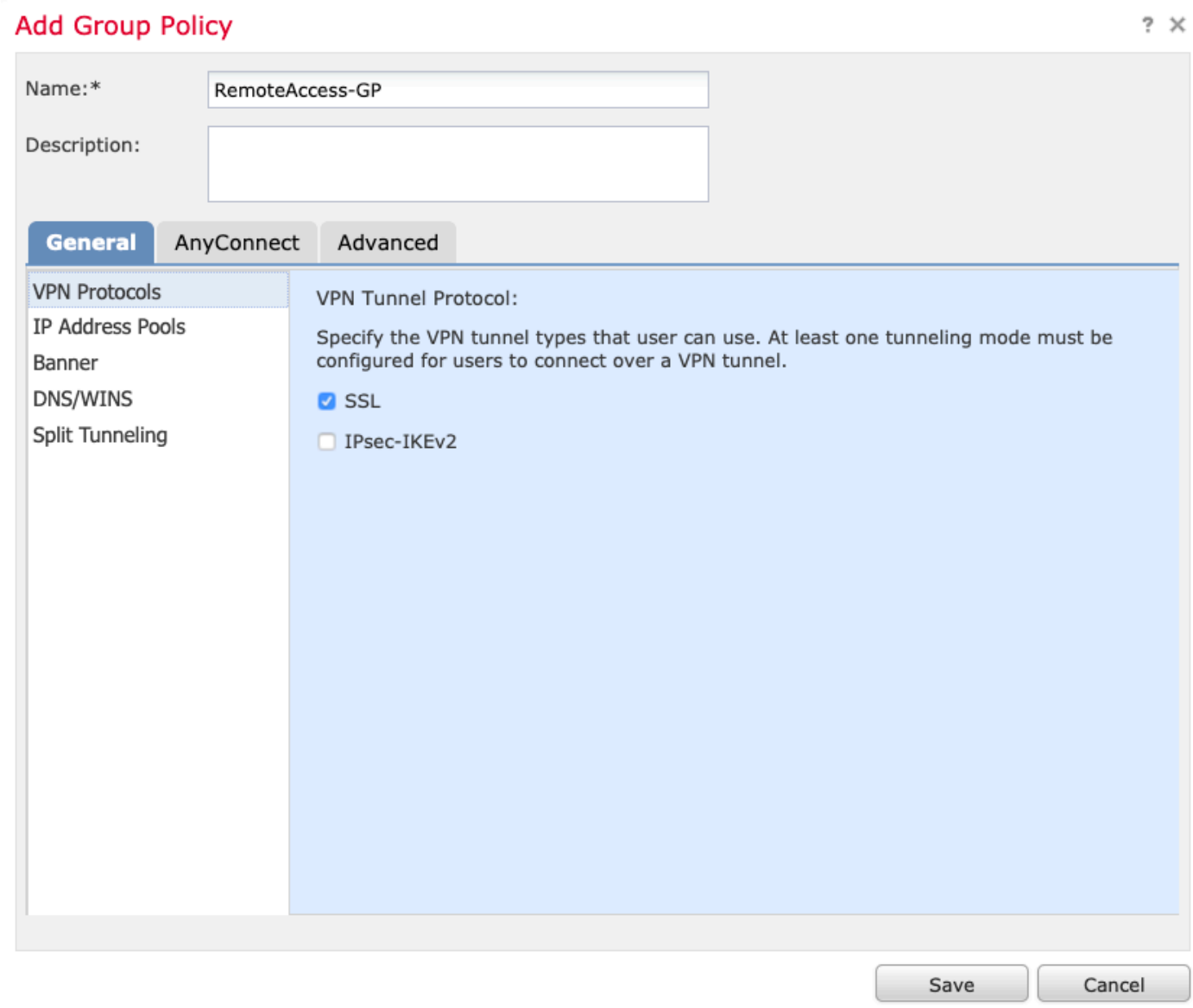
2. قم بتعيين اسم نهج الوصول عن بعد وحدد جهاز FTD من الأجهزة المتاحة.



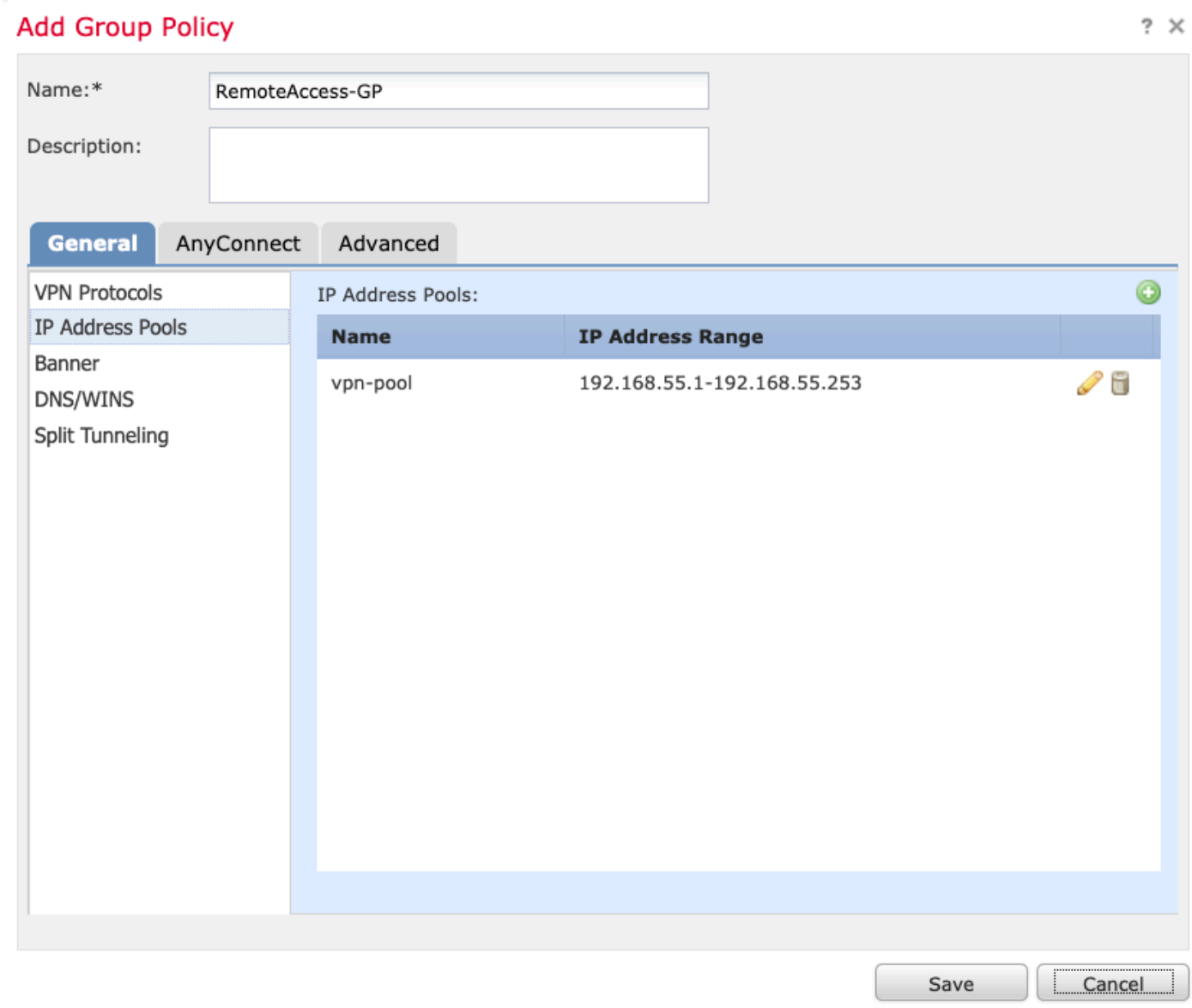
3. قم بتعيين اسم ملف تعريف الاتصال (اسم ملف تعريف الاتصال هو اسم مجموعة النفق)، حدد خادم المصادقة وتجمعات العناوين كما هو موضح في الصورة.



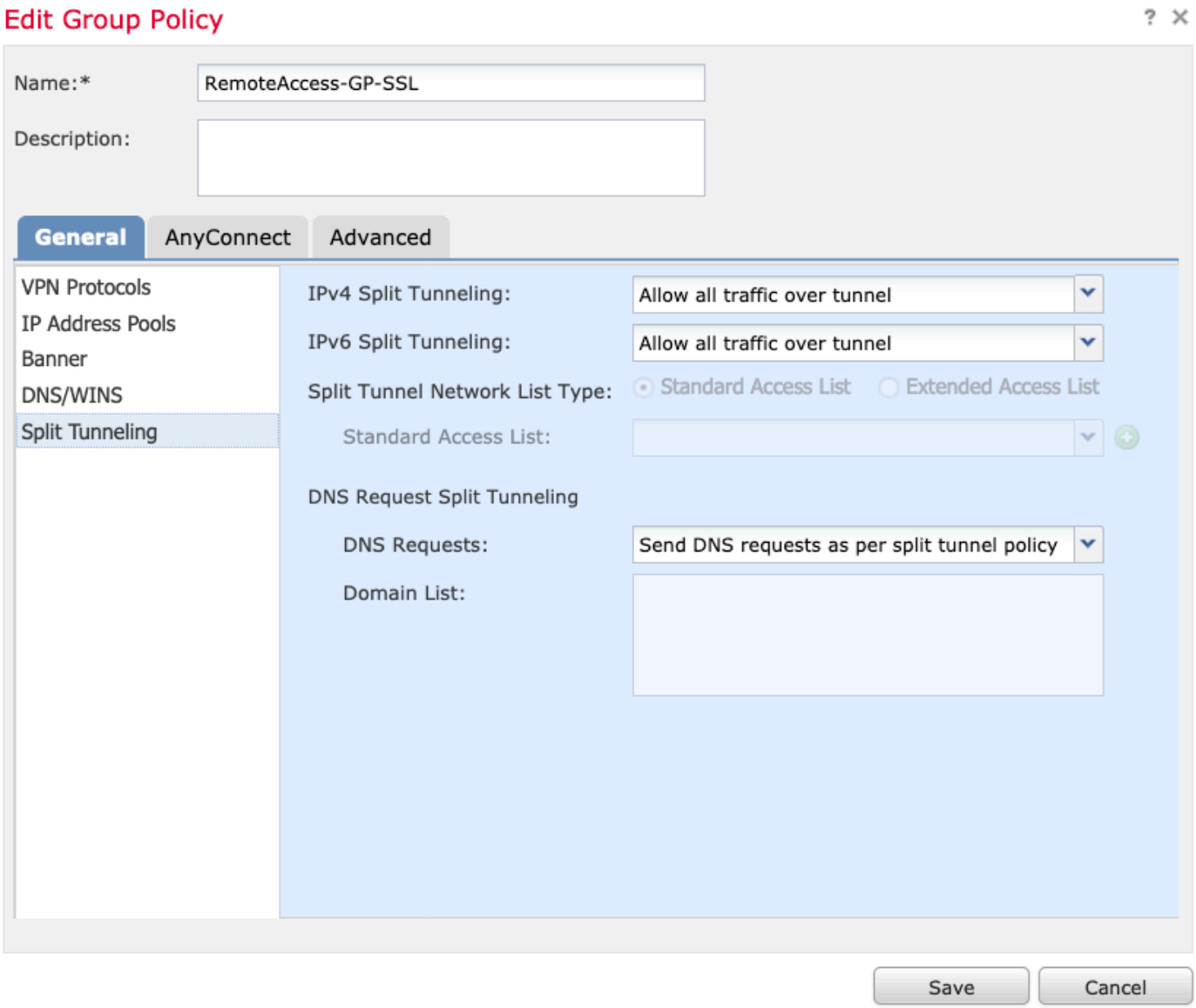
4. حدد + الرمز لإنشاء نهج المجموعة.



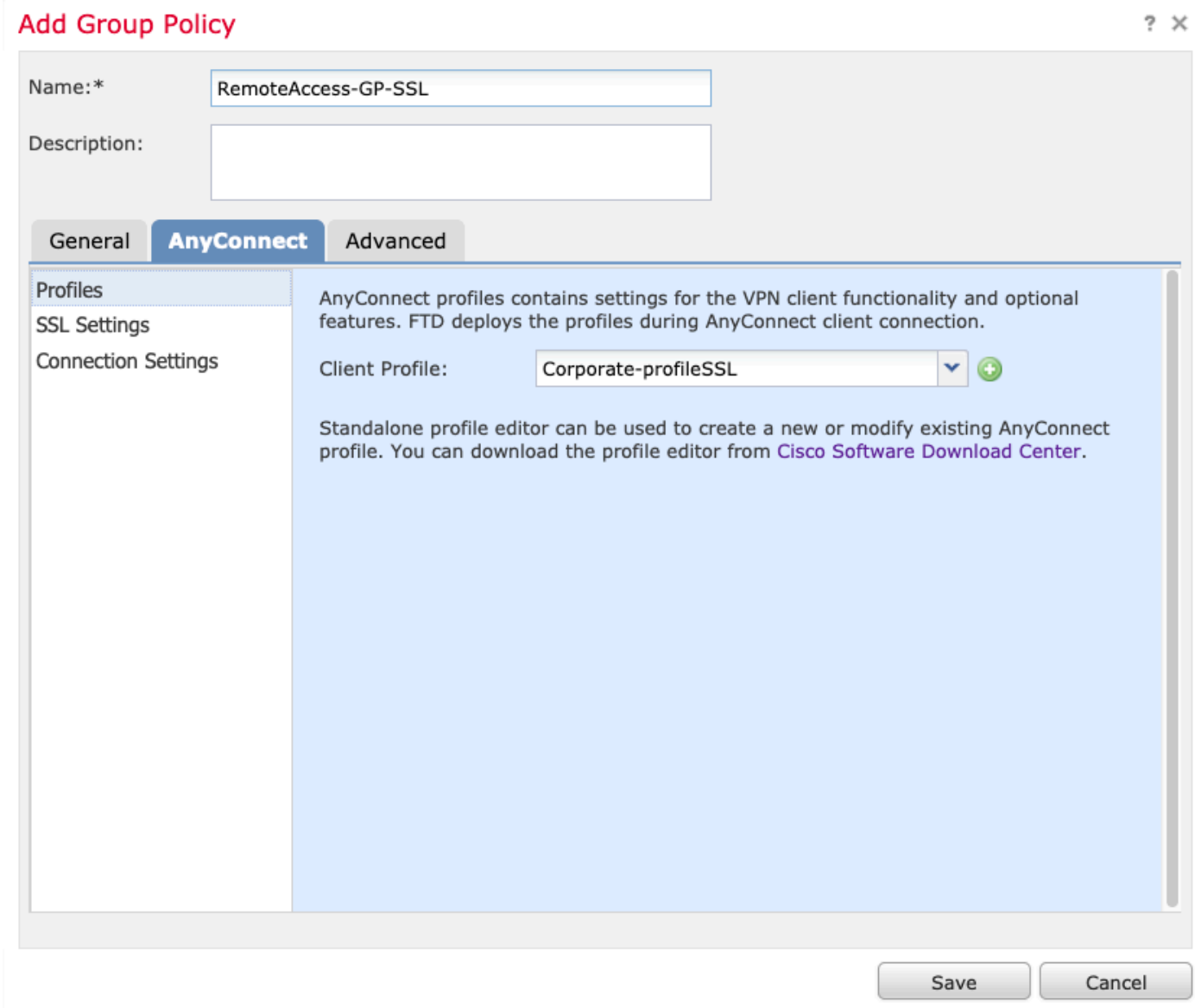
5. (إختياري) يمكن تكوين تجمع عناوين IP محلي في أساس سياسة المجموعة. في حالة عدم تكوينها، يتم توريث التجمع من التجمع الذي تم تكوينه في ملف تعريف الاتصال (مجموعة النفق).



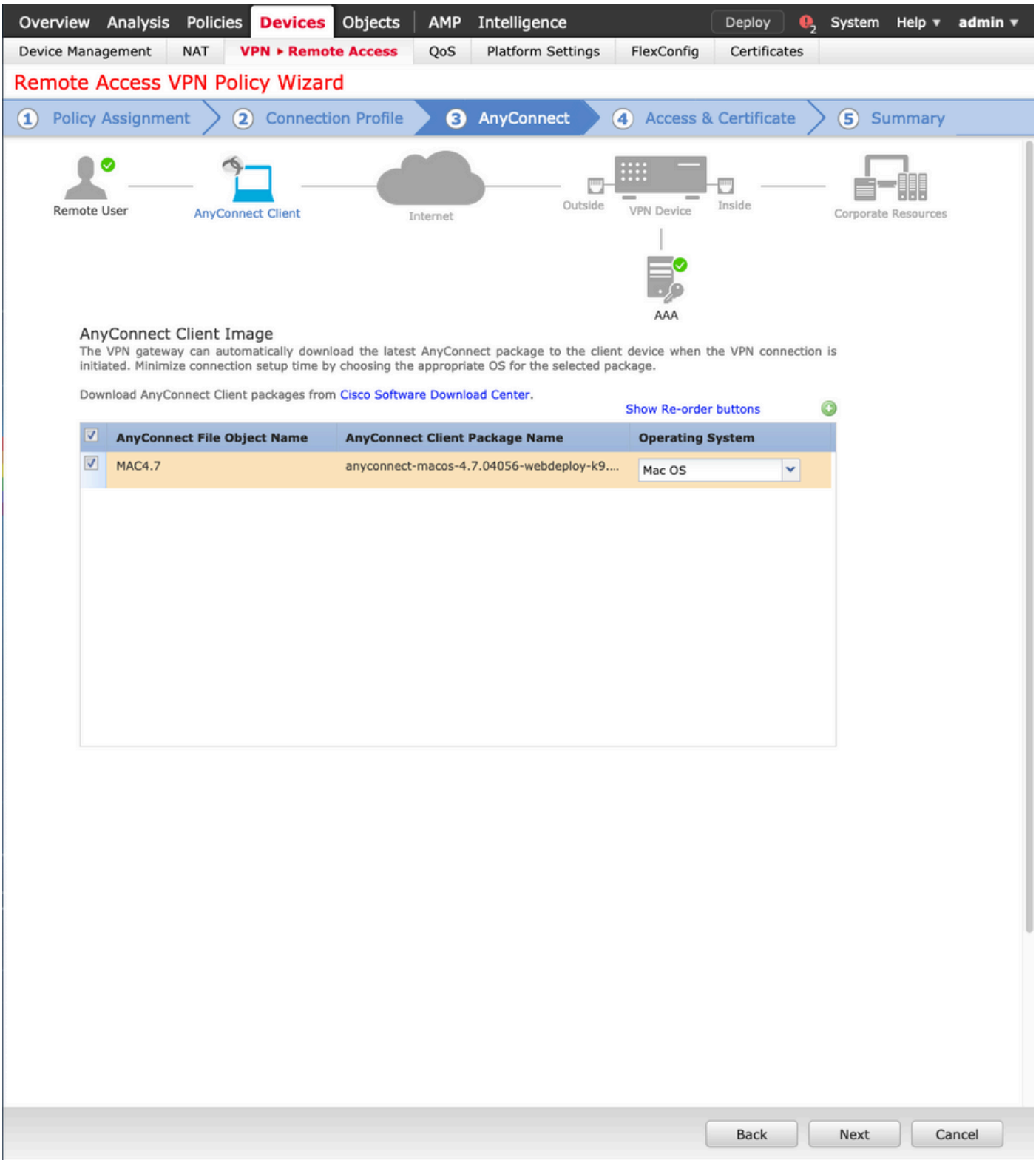
6. لهذا السيناريو، يتم توجيه حركة مرور البيانات بالكامل عبر النفق، ويتم تعيين سياسة اتصال IPv4 النفقي المقسم للسماح لجميع حركة المرور عبر النفق كما هو موضح في الصورة.



7. حدد ملف تعريف .xml لملف تعريف AnyConnect وحدد حفظ كما هو موضح في الصورة.



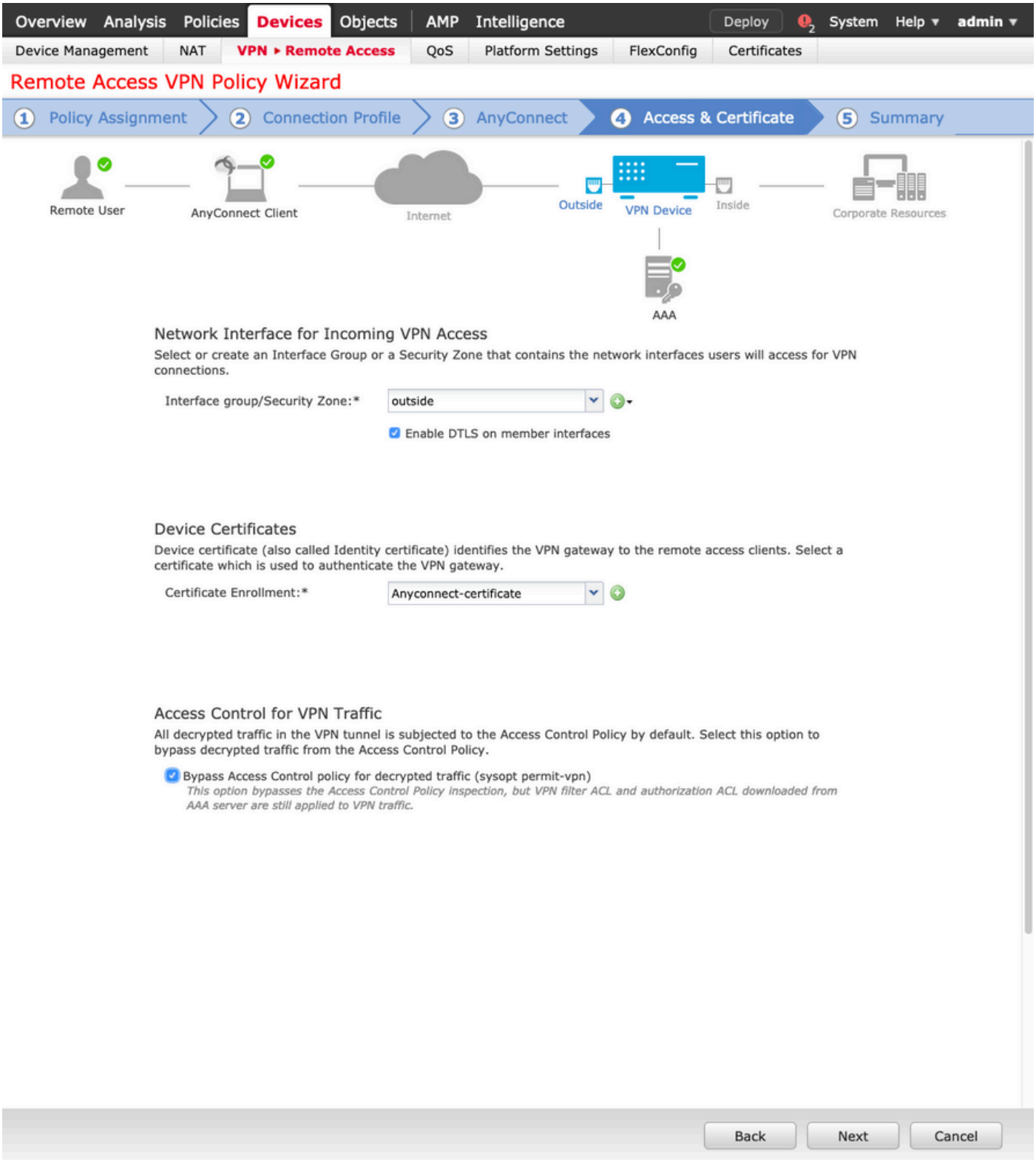
8. حدد صور AnyConnect المطلوبة استنادا إلى متطلبات النظام التشغيلي، حدد التالي في الصورة.



9. حدد منطقة الأمان وDeviceCertificates:

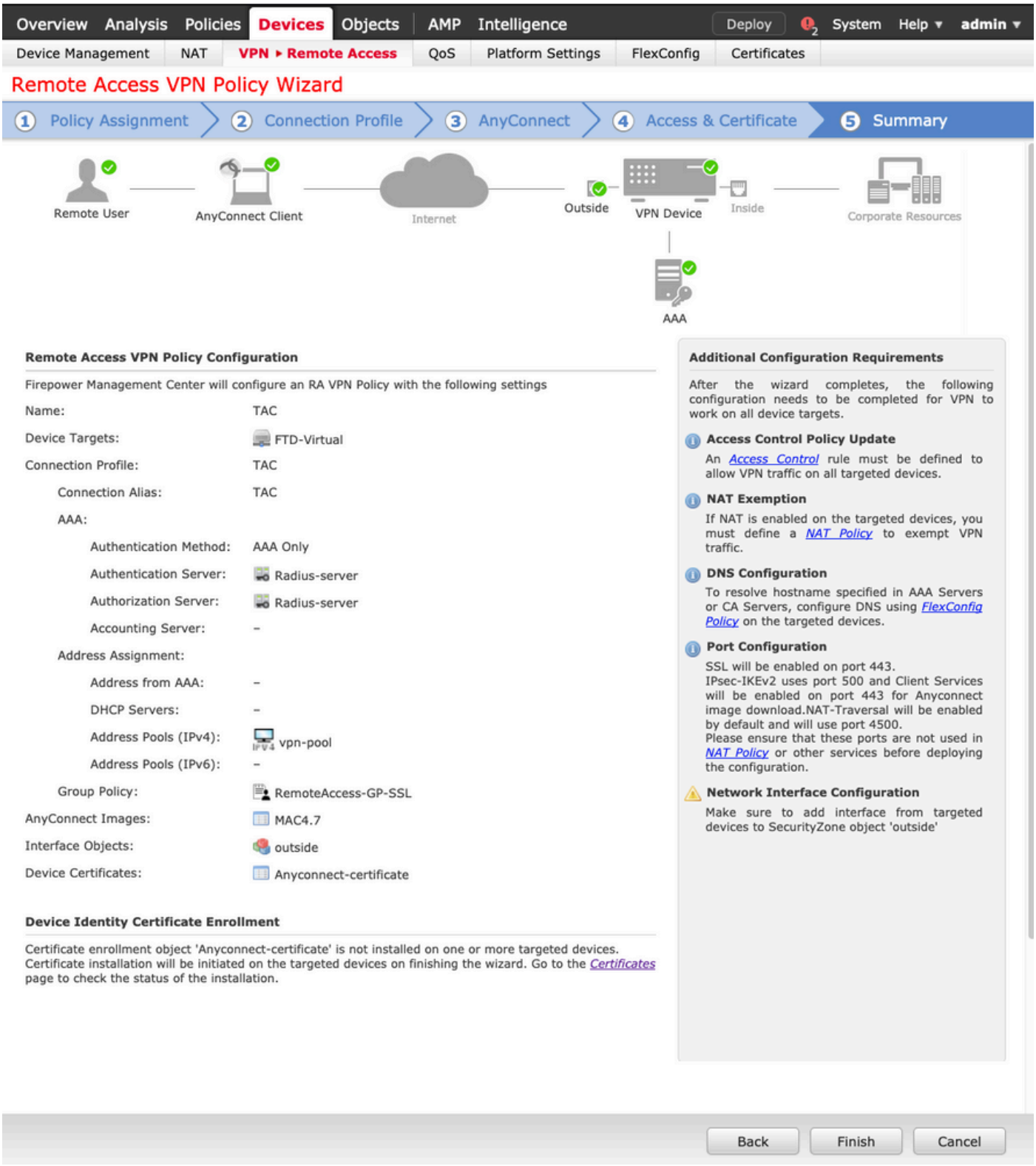
- يعين هذا تشكيل القارن على أي ال VPN ينهي والشهادة أن يكون قدمت على SSL توصيل.

ملاحظة: في هذا السيناريو، يتم تكوين FTD لعدم فحص أي حركة مرور VPN، وتجاوز خيار سياسات التحكم في الوصول (ACP) الذي تم تغيير خطوطه.



10. حدد إنهاء ونشر التغييرات:

- يتم دفع جميع التكوين المرتبط بشبكة VPN وشهادات SSL وحزم AnyConnect عبر نشر وحدة التحكم في الوصول عن بعد (FMC) كما هو موضح في الصورة.



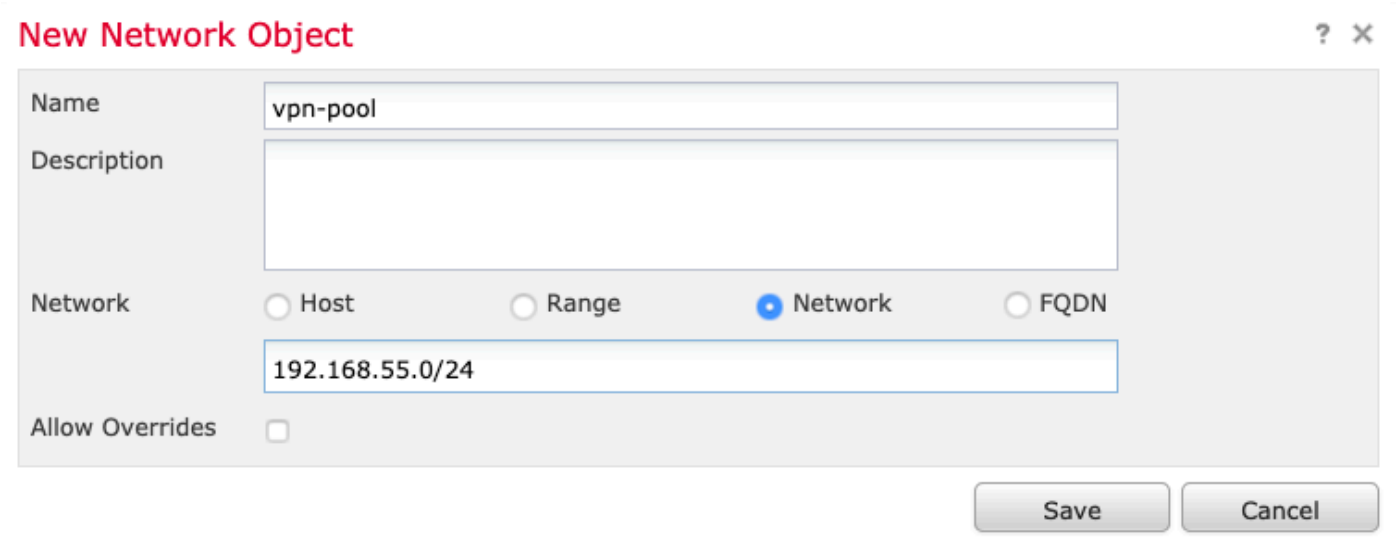
إعفاء NAT و HairPin

الخطوة 1. تكوين إستثناء NAT

إعفاء nat هو طريقة ترجمة مفضلة تستخدم لمنع حركة المرور التي سيتم توجيهها إلى الإنترنت عندما يكون المقصود هو التدفق عبر نفق VPN (الوصول عن بعد أو الوصول من موقع إلى موقع).

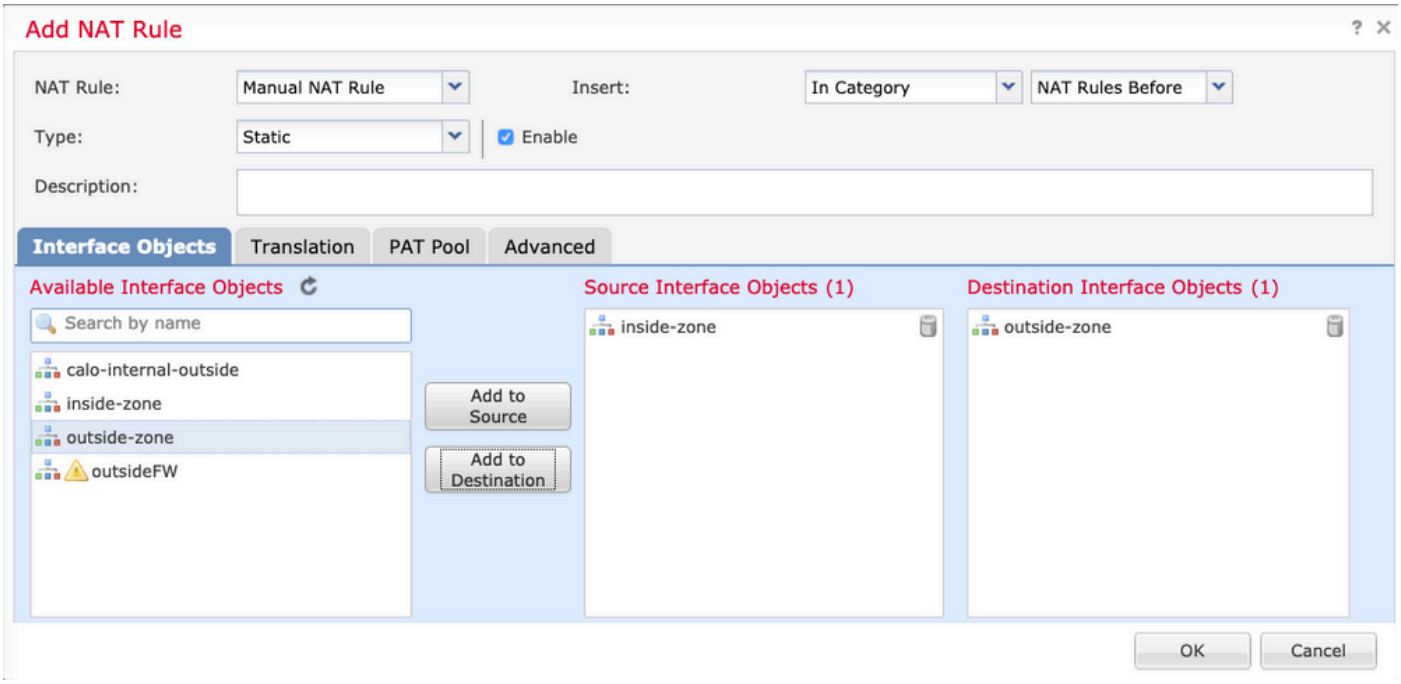
هذا يكون ضروريا عندما يكون من المفترض أن تتدفق حركة مرور البيانات من شبكتك الداخلية عبر الأنفاق دون أي ترجمة.

1. انتقل إلى الكائنات> الشبكة > إضافة شبكة > إضافة كائن كما هو موضح في الصورة.

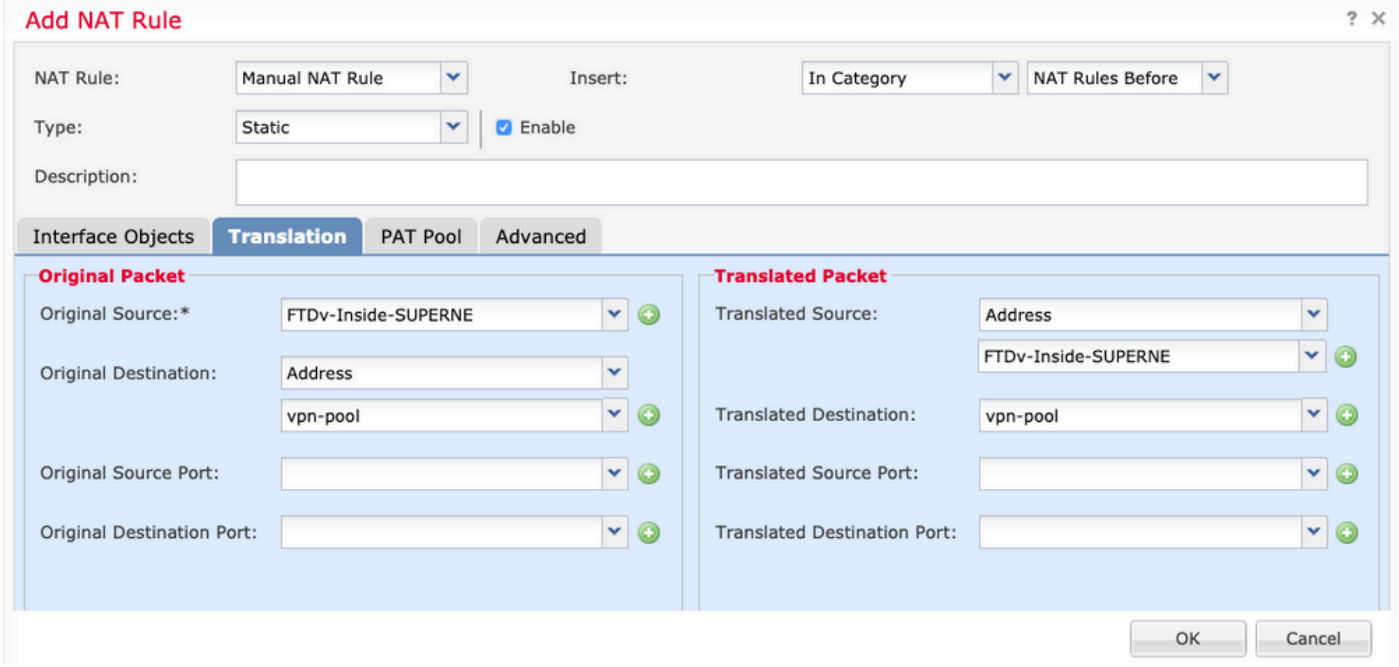


2. انتقل إلى جهاز > NAT، وحدد سياسة NAT التي يتم إستخدامها من قبل الجهاز المعني وقم بإنشاء جملة جديدة.

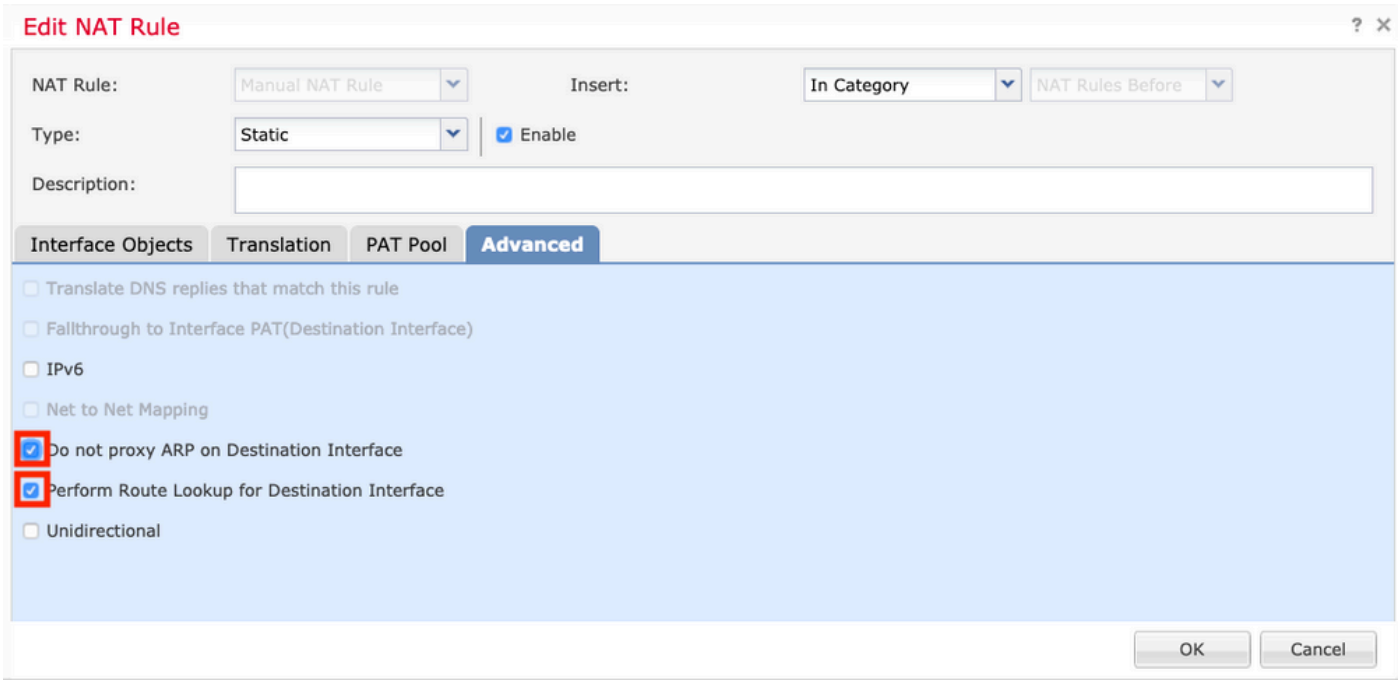
ملاحظة: ينتقل تدفق حركة المرور من الداخل إلى الخارج.



3. حدد الموارد الداخلية خلف FTD (المصدر الأصلي والمصدر المترجم) والوجهة كتجمع IP المحلي لمستخدمي AnyConnect (الوجهة الأصلية والوجهة المترجمة) كما هو موضح في الصورة.

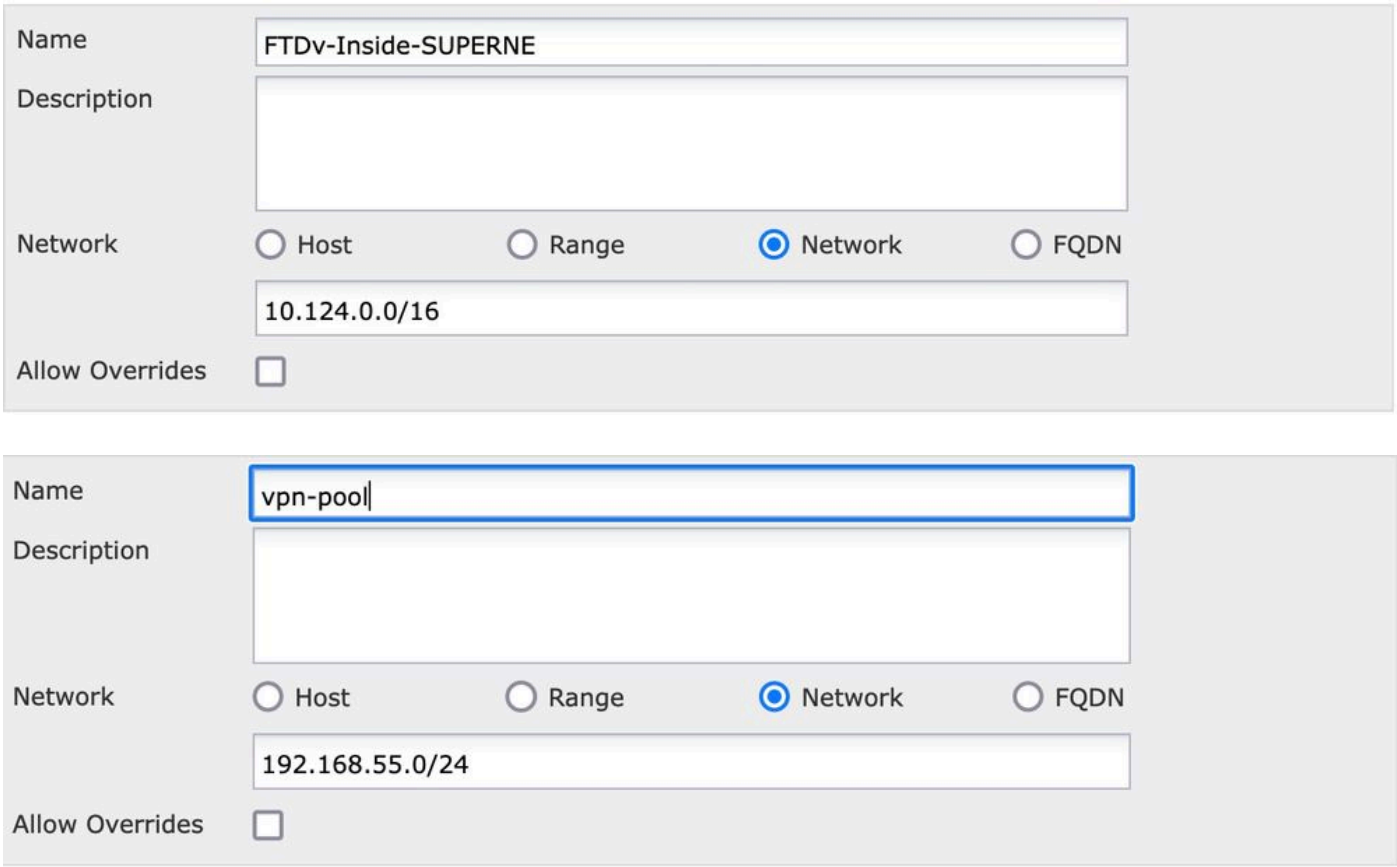


4. تأكد من تبديل الخيارات (كما هو موضح في الصورة)، لتمكين "no-proxy-arp" و"route-lookup" في قاعدة NAT، حدد ok كما هو موضح في الصورة.



5. هذا هو نتيجة لتكوين إستثناء NAT.

الكائنات المستخدمة في القسم السابق هي الكائنات الموضحة أدناه.



الخطوة 2. تكوين دبوس الشعر

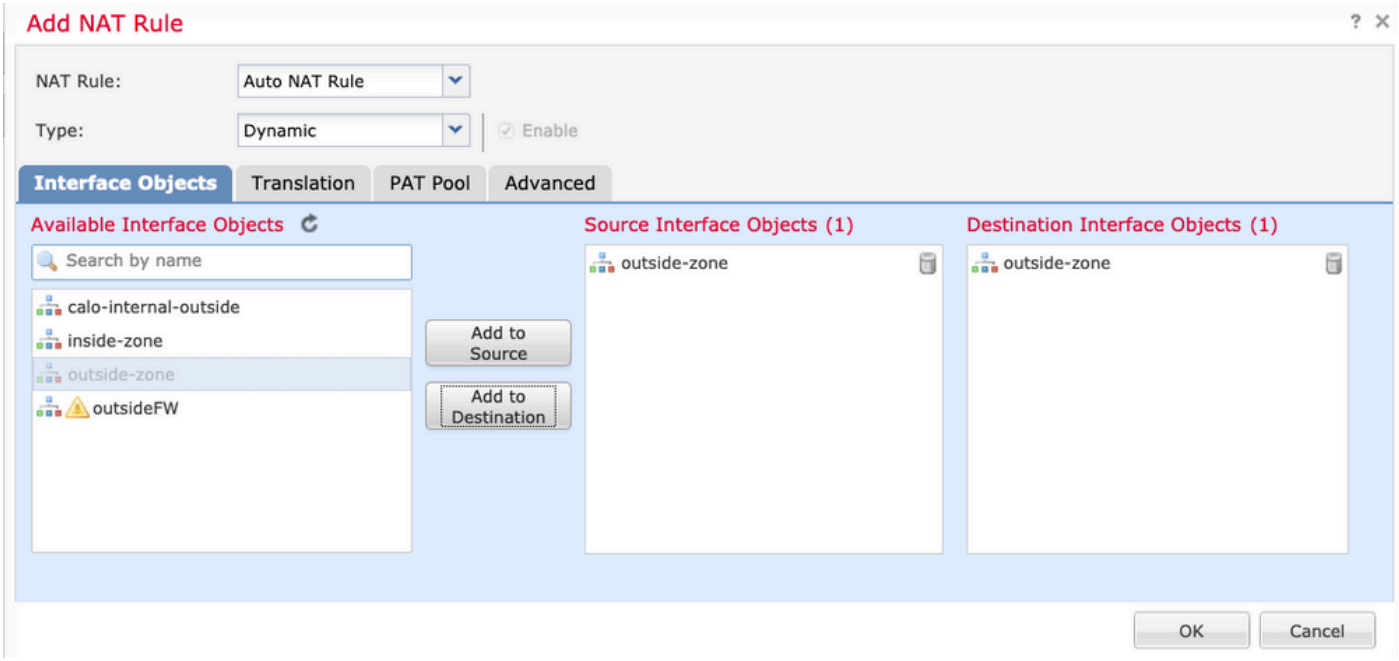
يعرف أيضا U-turn، هذا ترجمة طريقة أن يسمح الحركة مرور أن يتدفق عبر ال نفسه قارن إستلمت حركة مرور يكون على.

على سبيل المثال، عند تكوين AnyConnect بسياسة نفق كامل، يتم الوصول إلى الموارد الداخلية وفقا لسياسة إستثناء NAT. إذا كان المقصود من حركة مرور عميل AnyConnect الوصول إلى موقع خارجي على الإنترنت، فإن NAT (أو U-turn) القاصر مسؤول عن توجيه حركة المرور من الخارج إلى الخارج.

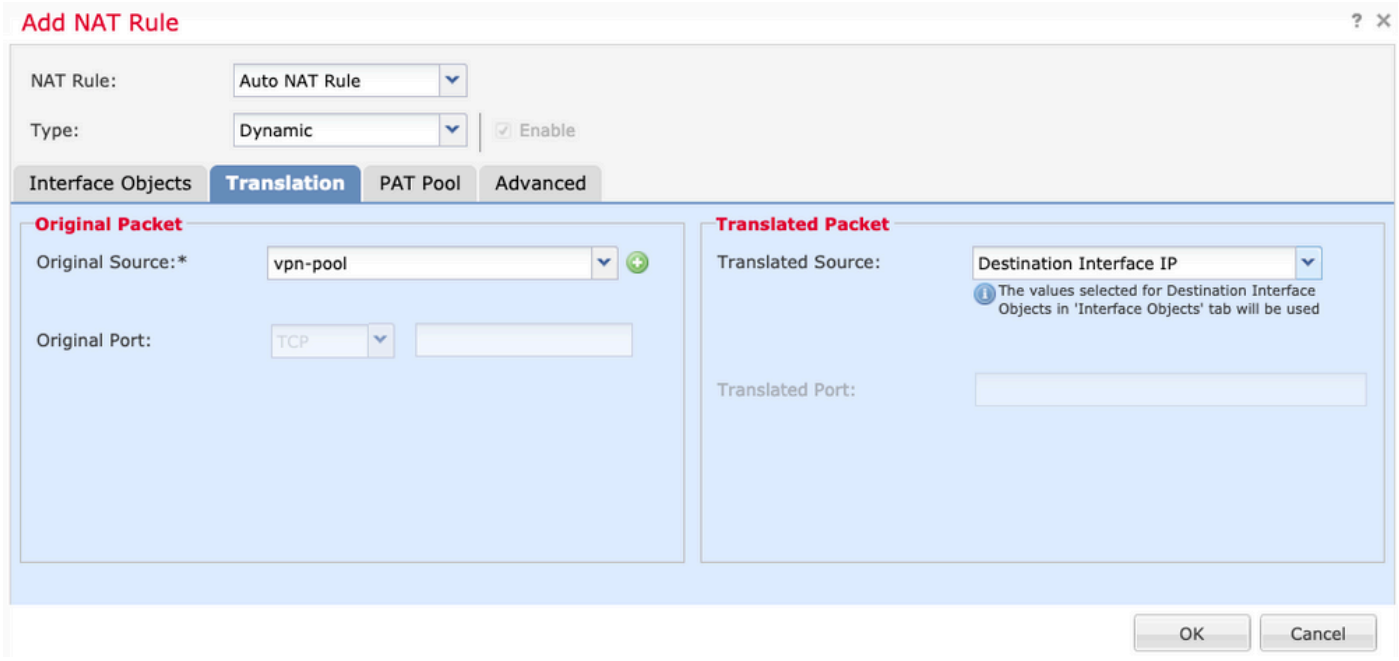
يجب إنشاء كائن تجمع VPN قبل تكوين NAT.

1. قم بإنشاء عبارة NAT جديدة، وحدد قاعدة NAT التلقائية في حقل قاعدة NAT وحدد ديناميكي ك NATtype.

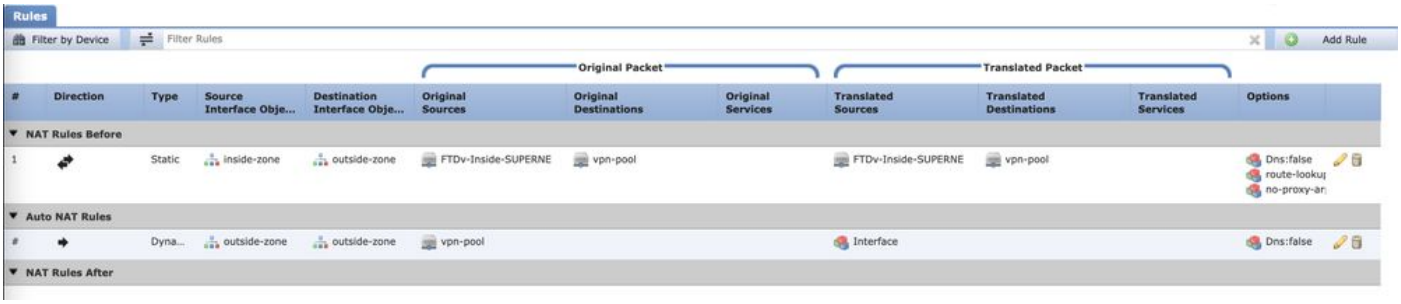
2. حدد نفس الواجهة لكائنات الواجهة المصدر والوجهة (خارج):



3. في علامة التبويب ترجمة، حدد كمصدر أصلي كائن تجمع VPN وحدد واجهة الوجهة IP كمصدر مترجم، حدد موافق كما هو موضح في الصورة.



4. هذا هو ملخص تكوين NAT كما هو موضح في الصورة.



5. انقر فوق حفظ ونشر التغييرات.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

قم بتشغيل هذه الأوامر في سطر أوامر FTD.

- شهادات SH crypto CA
- show running-config ip ip pool المحلي
- show running-config webVPN
- show running-config tunnel-group
- show running-config group-policy
- show running-config ssl
- show running-config nat

استكشاف الأخطاء وإصلاحها

لا توجد حاليا أي معلومات خاصة باستكشاف الأخطاء وإصلاحها متوفرة لهذا التكوين.

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).