تكوين نفق AnyConnect للتقسيم الديناميكي على FTD الذي تتم إدارته بواسطة FMC

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

القيود

التكوين

الخطوة 1. تحرير مجموعة استخدام نفق التقسيم الديناميكي

الخطوة 2. تكوين سمة AnyConnect المخصصة

الخطوة 3. تحقق من التكوين، ثم احفظ وانشر

التحقق من الصحة

استكشاف الأخطاء وإصلاحها

المشكلة

الحل

معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية تكوين نفق AnyConnect المقسم الديناميكي على الدفاع عن تهديد FirePOWER (FTD) المدار بواسطة مركز إدارة FirePOWER.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco AnyConnect
- معرفة أساسية بمركز إدارة FirePOWER (FMC)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- FMC، الإصدار 7.0

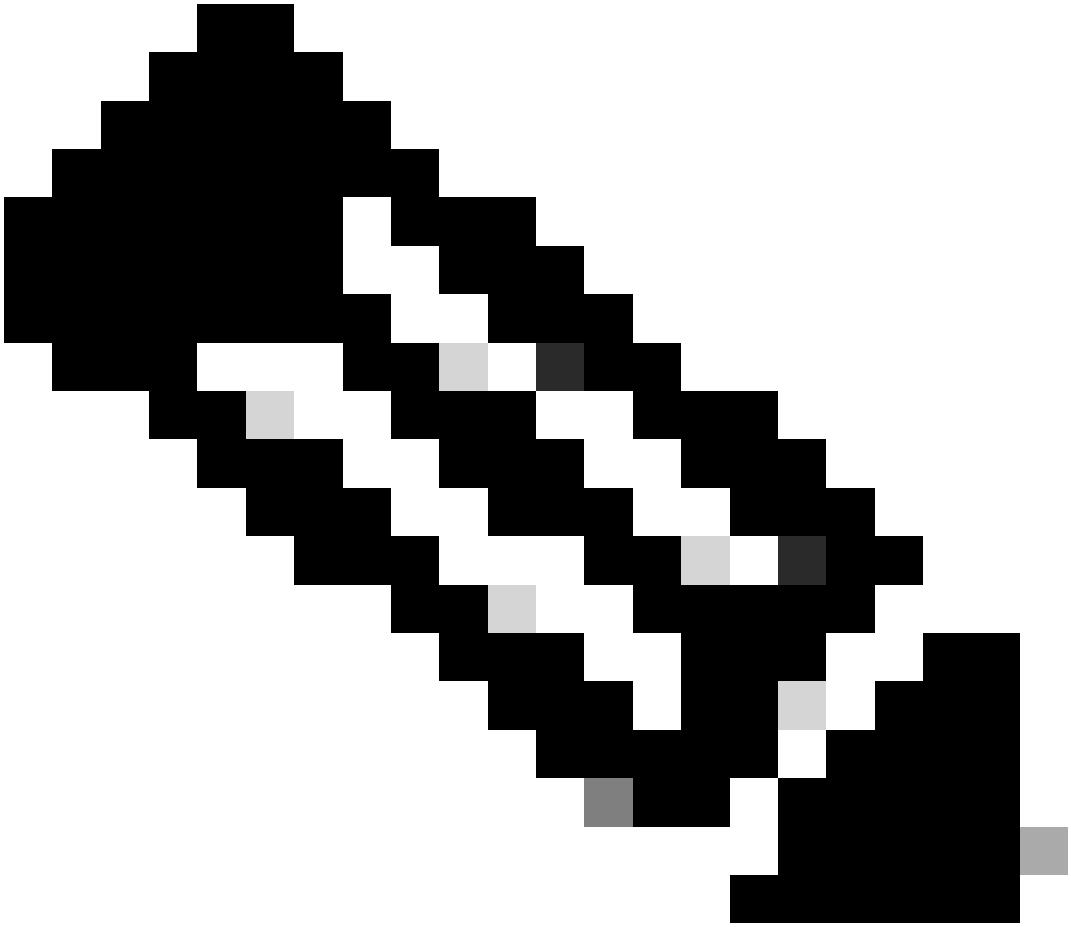
- FTD الإصدار 7.0

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

يتوفر تكوين AnyConnect Dynamic Split Tunnel على FTD الذي تتم إدارته بواسطة FMC بالكامل على الإصدار 7.0 من FMC والإصدارات الأحدث. إذا قمت بتشغيل إصدار أقدم، فأنت بحاجة إلى تكوينه عبر FlexConfig كما هو موضح في عمليات نشر AnyConnect VPN المتقدمة للدفاع عن تهديد FirePOWER باستخدام FMC.

باستخدام تكوين "نفق التقسيم الديناميكي"، يمكنك ضبط تكوين نفق التقسيم بدقة استنادا إلى أسماء مجالات DNS. نظرا لإمكانية تغيير عناوين IP المرتبطة بأسماء المجالات المؤهلة بالكامل (FQDN)، يوفر تكوين النفق المقسم القائم على أسماء DNS تعريفا أكثر ديناميكية لحركة مرور البيانات التي يتم أو لا يتم تضمينها في نفق شبكة الوصول عن بعد الخاصة الظاهرية (VPN). إن أي عنوان مرتجع لأسماء مجال مستبعد يكون ضمن العنوان بركة يتضمن في ال VPN، أن عنوان بعد ذلك استثنيت. لم يتم حظر المجالات المستبعدة. بدل من ذلك، أبقيت حركة مرور إلى أن مجال خارج ال VPN نفق.



ملاحظة: أنت يستطيع أيضا شكلت انقسام حركي نفق أن يعين مجال أن يتضمن في النفق أن بخلاف ذلك كنت سيستبعد يؤسس على عنوان.

القيود

حاليا، هذا سمة بعد ال يساند:

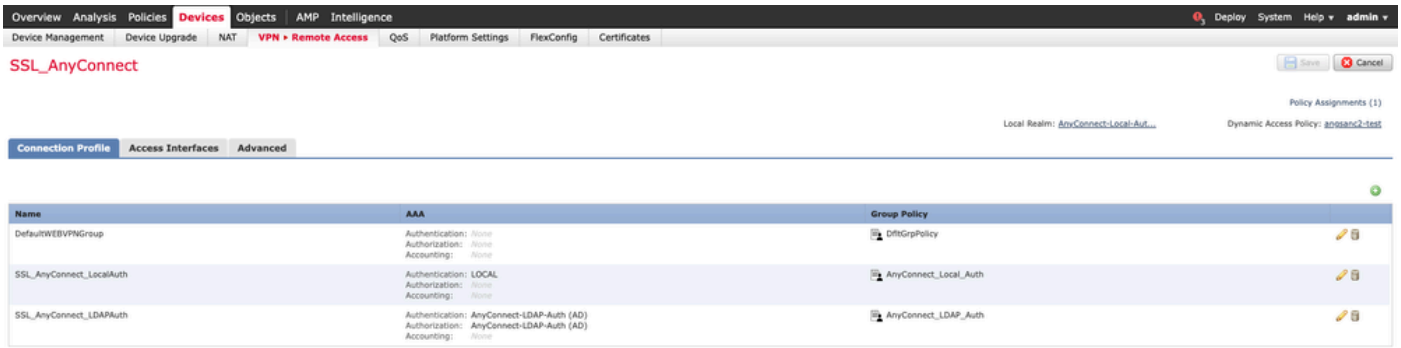
- نفق التقسيم الديناميكي غير مدعوم على أجهزة Cisco iOS. راجع معرف تصحيح الأخطاء من Cisco CSCvr54798
- ال يتم دعم نفق التقسيم الديناميكي على عملاء AnyConnect Linux. راجع Cisco IDCSCvt64988

التكوين

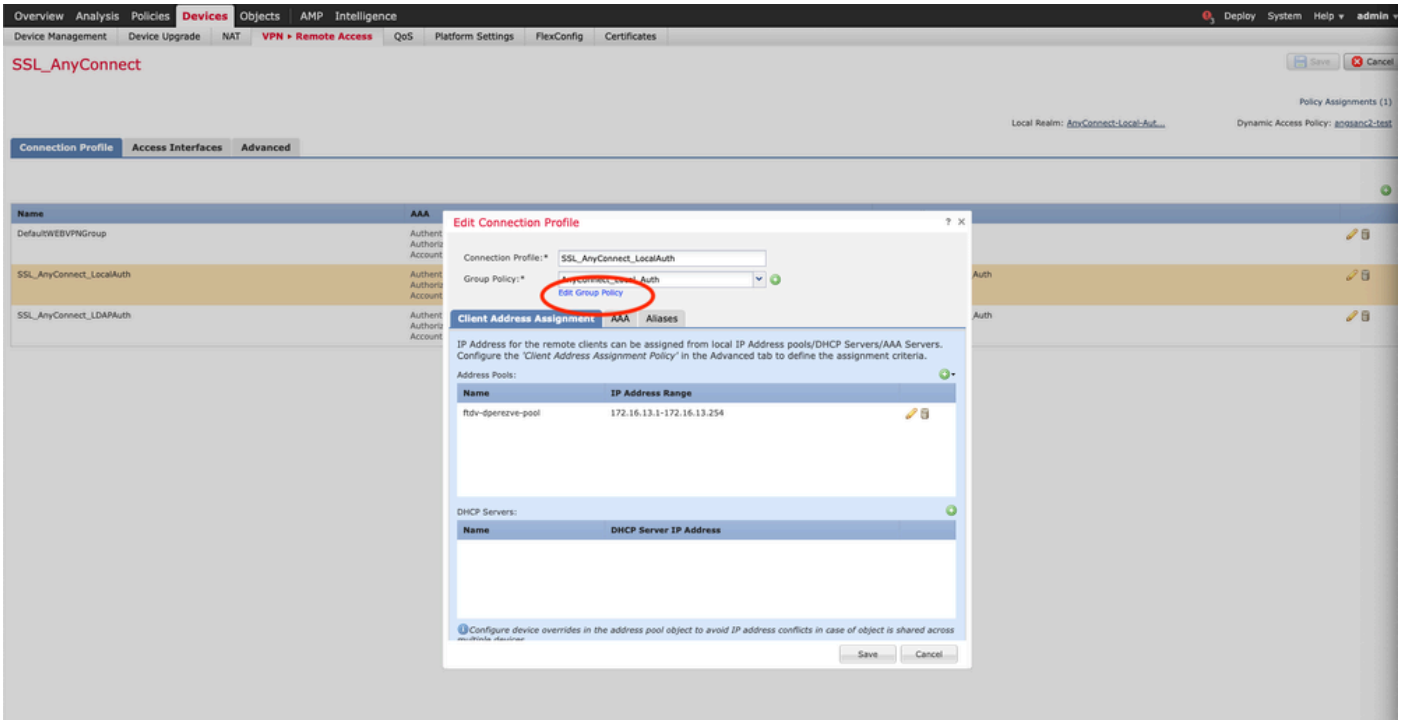
يوضح هذا القسم كيفية تكوين نفق AnyConnect للتقسيم الديناميكي على FTD الذي تتم إدارته بواسطة FMC.

الخطوة 1. تحرير نهج المجموعة لاستخدام نفق التقسيم الديناميكي

1. في FMC، انتقل إلى الأجهزة > VPN > الوصول عن بعد، ثم حدد ملف تعريف الاتصال الذي تريد تطبيق التكوين:

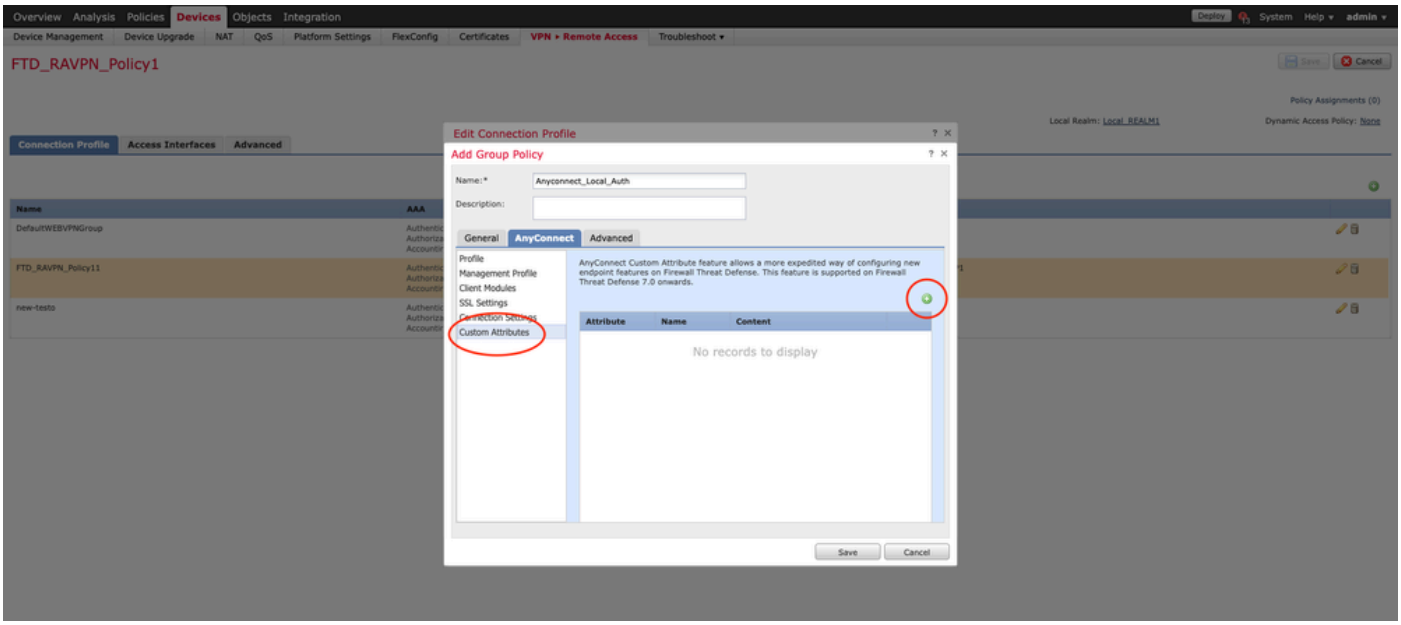


2. حدد تحرير نهج المجموعة لتعديل أحد نهج المجموعة التي تم إنشاؤها بالفعل.

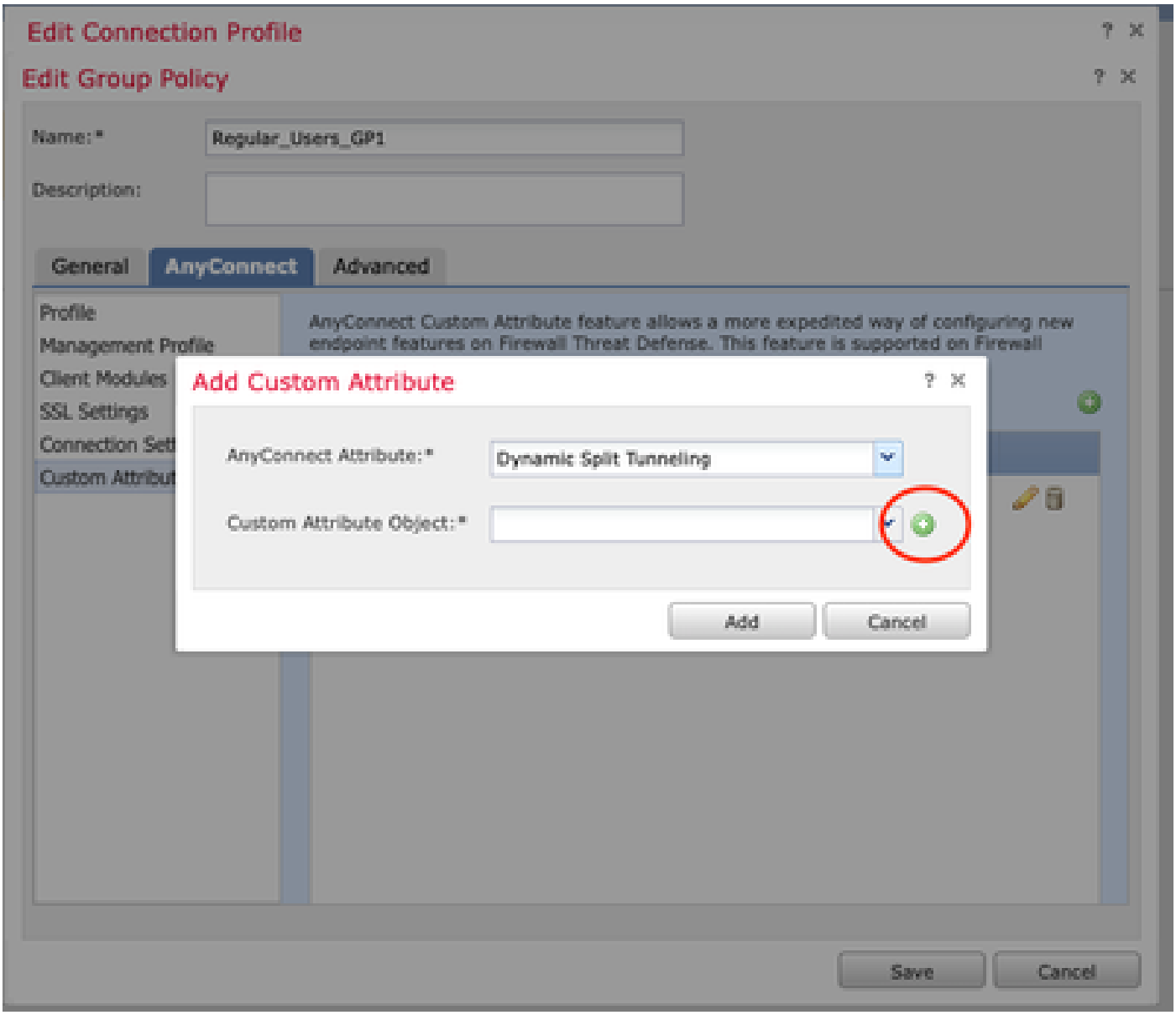


الخطوة 2. تكوين سمة AnyConnect المخصصة

1. ضمن تكوين "نهج المجموعة"، انتقل إلى AnyConnect > سمات مخصصة، انقر فوق الزر إضافة (+):

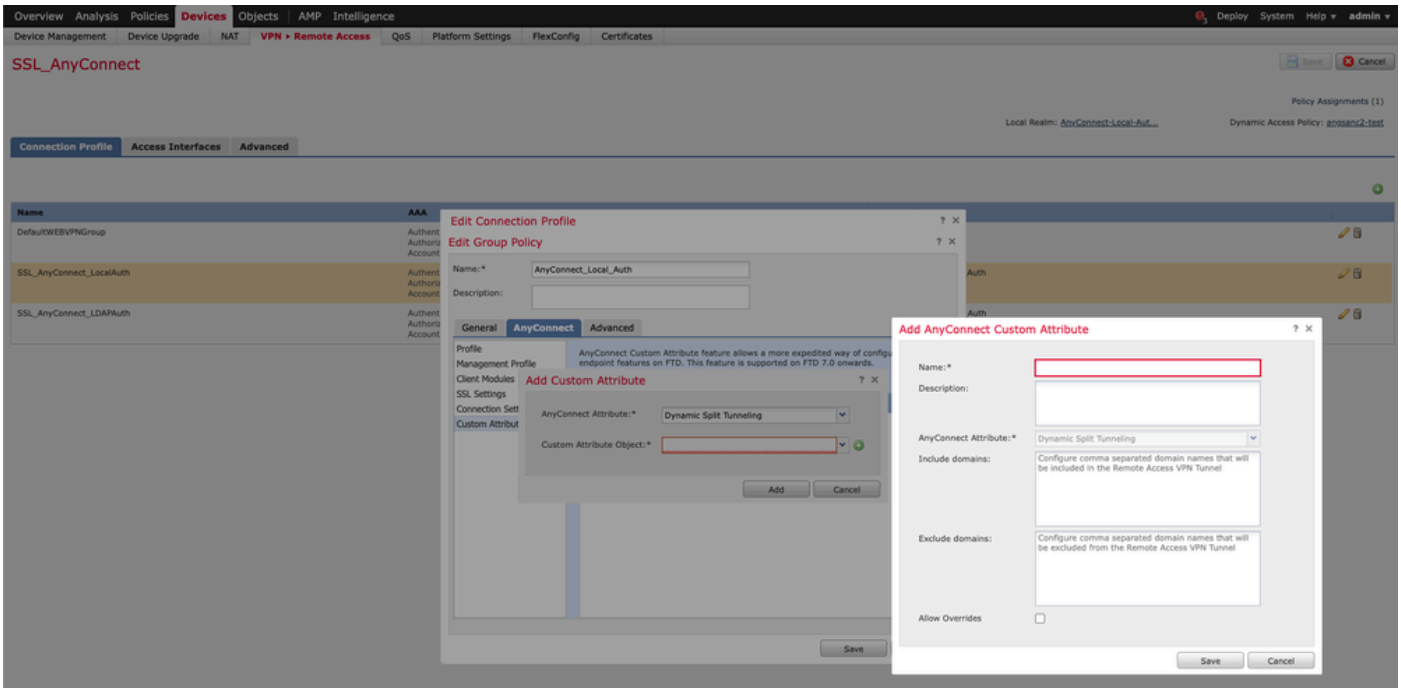


2. حدد سمة AnyConnect الخاصة بتقسيم ديناميكي للنفق، وانقر فوق الزر إضافة (+) لإنشاء كائن سمة مخصصة جديد:

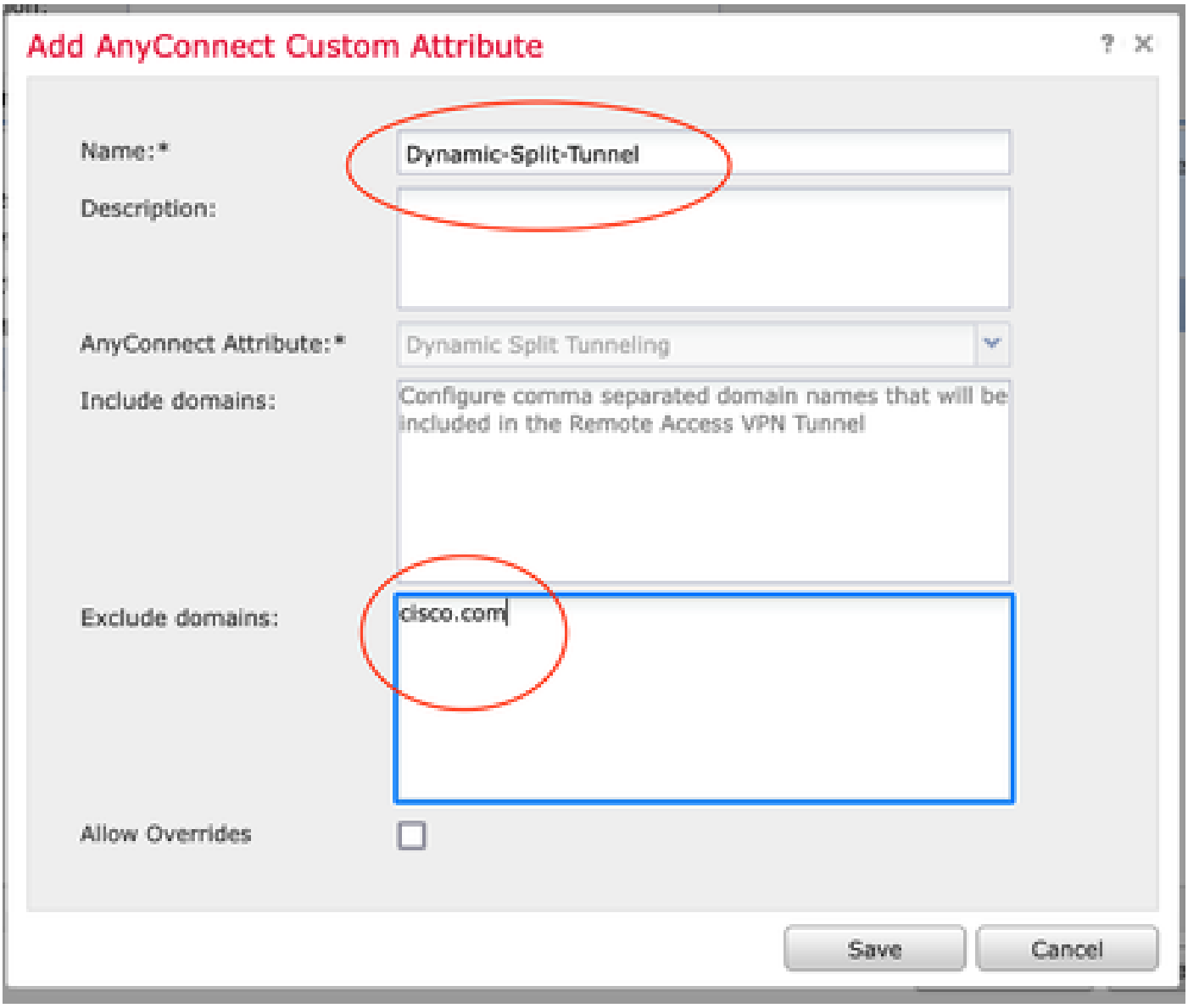


3. أدخل اسم سمة AnyConnect المخصصة وقم بتكوين المجالات المراد تضمينها أو إستبعادها بشكل ديناميكي.

ملاحظة: يمكنك تكوين إما مجالات التضمين أو مجالات الاستبعاد فقط.

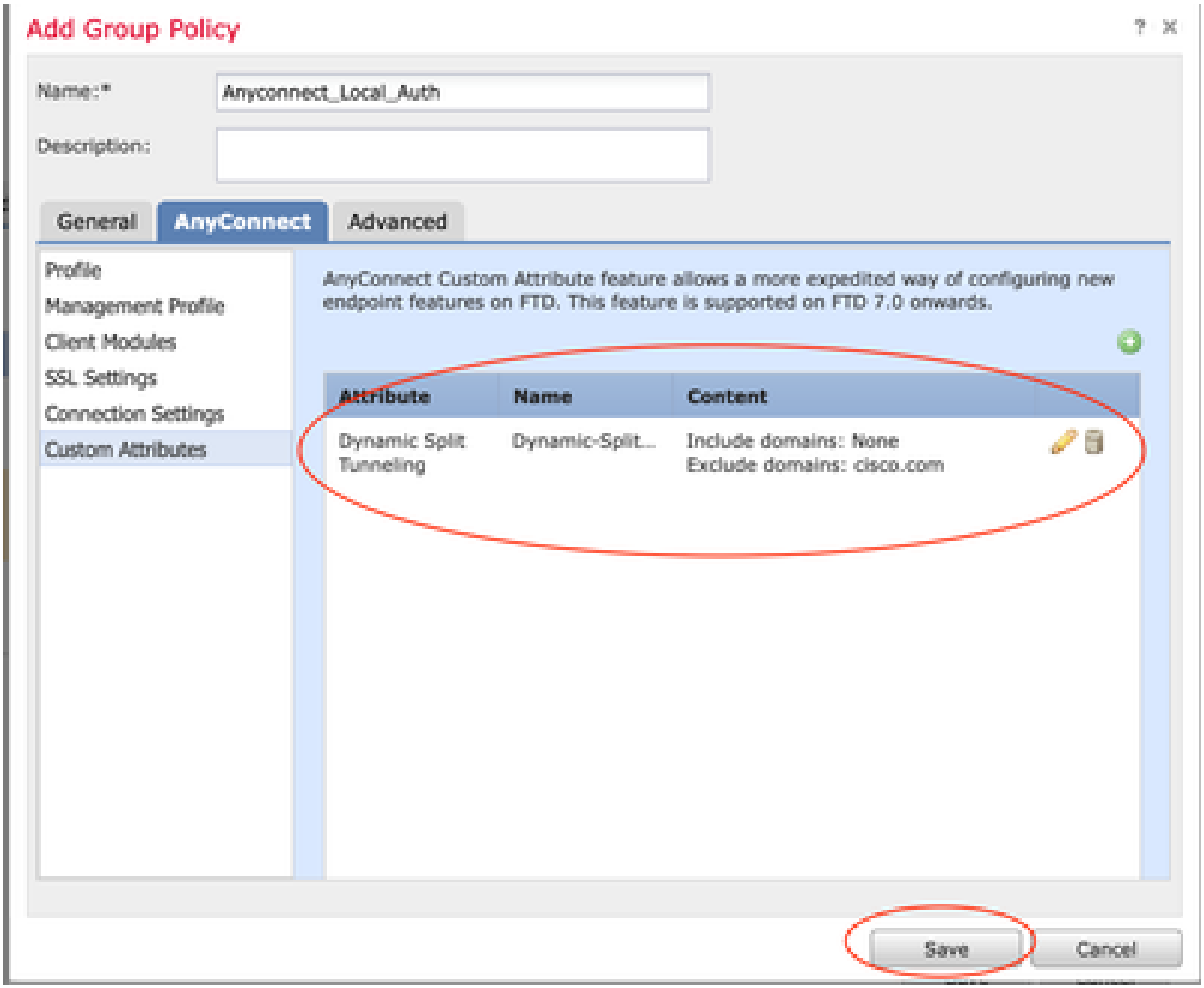


في هذا المثال، قمت بتكوين cisco.com كمجال ليتم إستبعاده، وعينت السمة المخصصة Dynamic-Split-Tunnel، كما هو موضح في الصورة:



الخطوة 3. تحقق من التكوين، ثم احفظ وانشر

تحقق من صحة السمة المخصصة التي تم تكوينها، ثم احفظ التكوين، ثم قم بنشر التغييرات إلى FTD المعني.



التحقق من الصحة

أنت يستطيع رضت هذا أمر على ال FTD عن طريق أمر خط قارن (CLI) أن يؤكد ال حركي انقسام نفق تشكيل:

- show running-config webVPN
- show running-config AnyConnect-custom-data
- show running-config group-policy <name of the group-policy>

في هذا المثال، التكوين هو:

<#root>

```
ftd# show run group-policy AnyConnect_Local_Auth
```

```
group-policy AnyConnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list value AC_networks
Default-domain none
split-dns none
address-pools value AC_pool
```

anyconnect-custom dynamic-split-exclude-domains value cisco.com

```
anyconnect-custom dynamic-split-include-domains none
```

ftd# show run webvpn

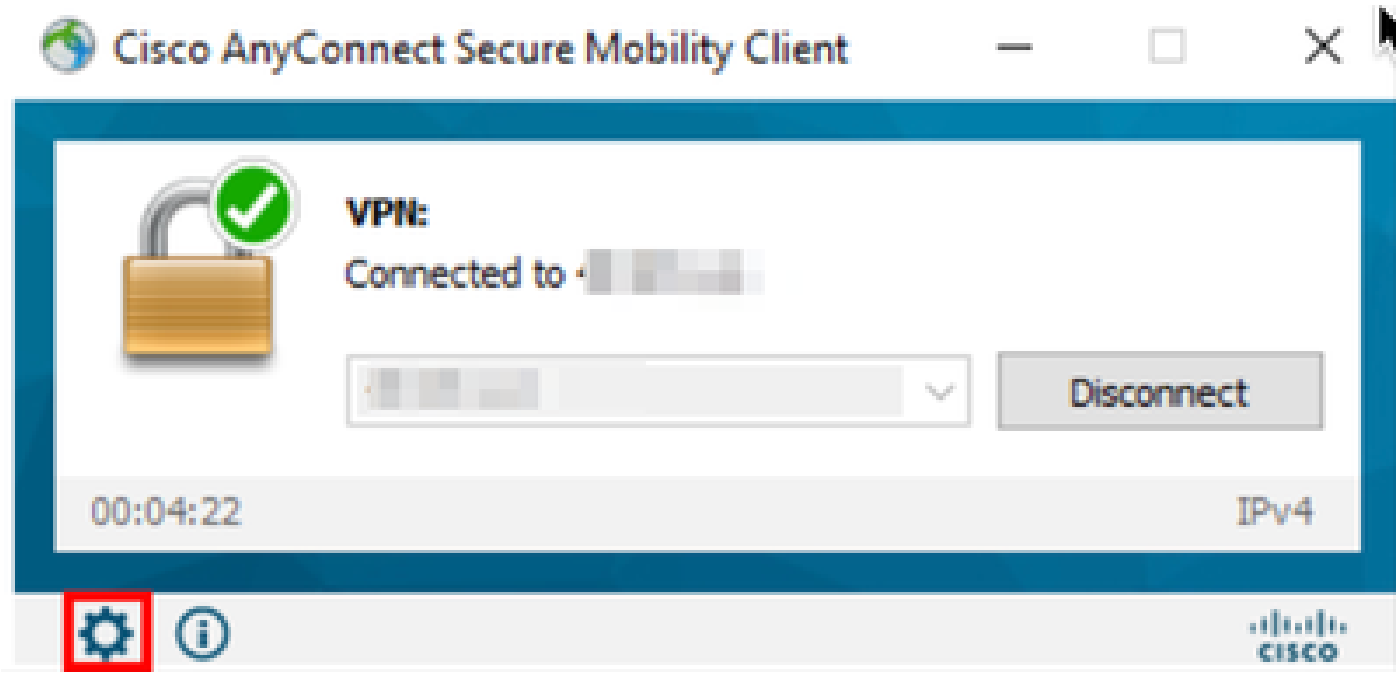
```
webvpn
enable outside
```

anyconnect-custom-attr dynamic-split-exclude-domains

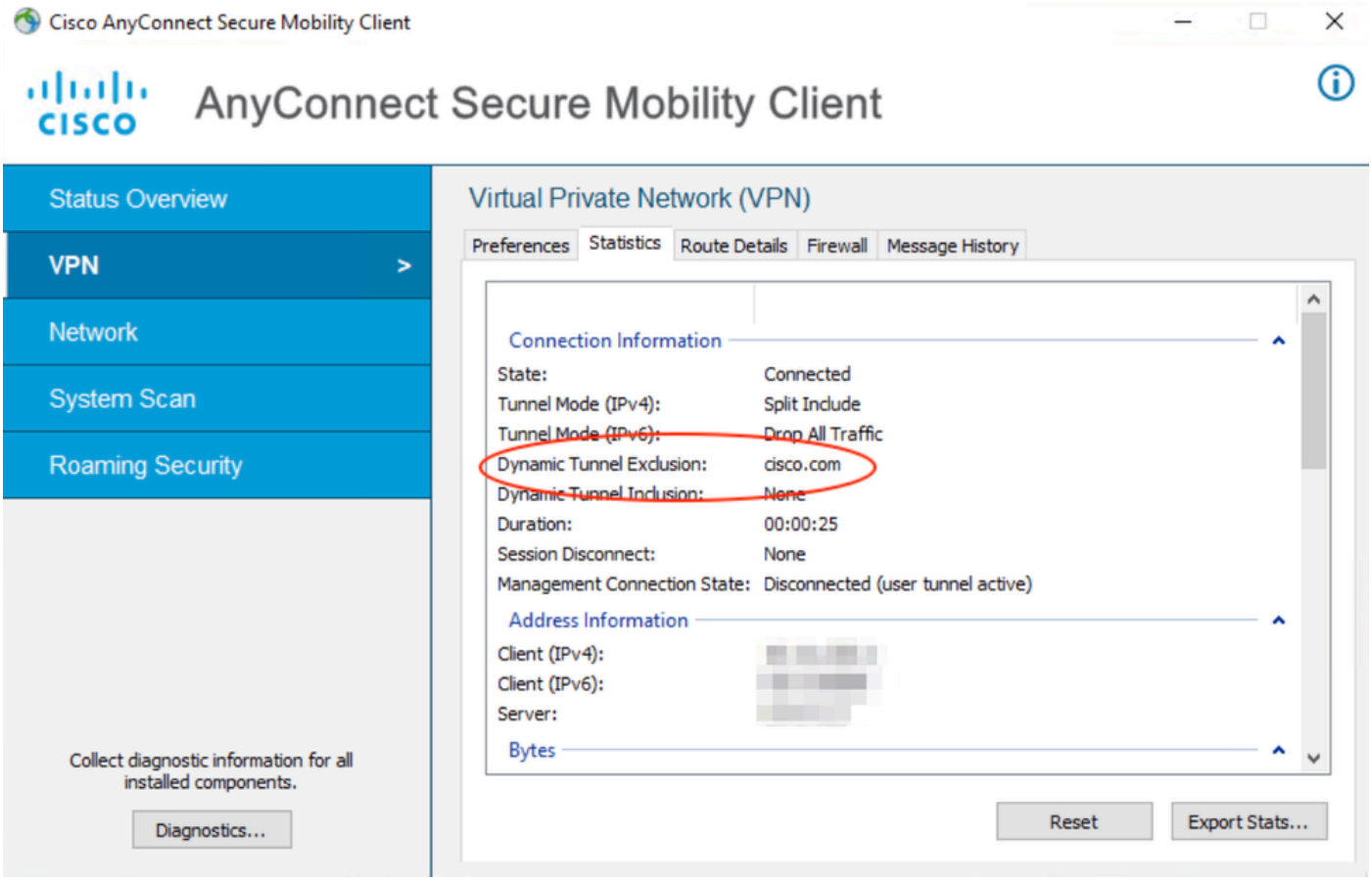
```
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert_map_test 10 cert_auth
error-recovery disable
```

للتحقق من استبعادات النفق الديناميكي التي تم تكوينها على العميل:

1. قم بتشغيل برنامج AnyConnect وانقر فوق رمز التروس، كما هو موضح بالصورة:



2. انتقل إلى VPN > الإحصاءات، وأكد المجالات المعروضة تحت إستبعاد/تضمين التقسيم الديناميكي:



استكشاف الأخطاء وإصلاحها

يمكنك إستخدام أداة تقارير وتشخيصات AnyConnect (DART) لجمع البيانات المفيدة لاستكشاف أخطاء تثبيت وتوصيل AnyConnect وإصلاحها.

تجمع DART السجلات والحالة والمعلومات التشخيصية لتحليل مركز المساعدة الفنية (TAC) من Cisco ولا تتطلب امتيازات المسؤول لتشغيلها على جهاز العميل.

المشكلة

إذا تم تكوين حرف بدل في السمات المخصصة ل AnyConnect، على سبيل المثال، *.cisco.com، فسيتم قطع اتصال جلسة عمل AnyConnect.

الحل

يمكنك إستخدام قيمة مجال cisco.com للسماح بديل حرف البدل. يتيح لك هذا التغيير إما تضمين مجالات أو إستبعادها مثل www.cisco.com and tools.cisco.com.

معلومات ذات صلة

- للحصول على مساعدة إضافية، اتصل بمركز المساعدة التقنية (TAC). يلزم عقد دعم صالح: جهات اتصال الدعم العالمية من Cisco
- يمكنك أيضا زيارة مجتمع VPN من Cisco.

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 دائماً إلى المستند الإنجليزي الأصلي (الرابط متوفر).