تنفيذ تدابير التعزيز لتأمين عميل AnyConnect VPN

المحتويات

المقدمة

يوضح هذا المستند كيفية تحسين أمان تنفيذ شبكة VPN للوصول عن بعد لديك.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco Secure Client AnyConnect VPN.

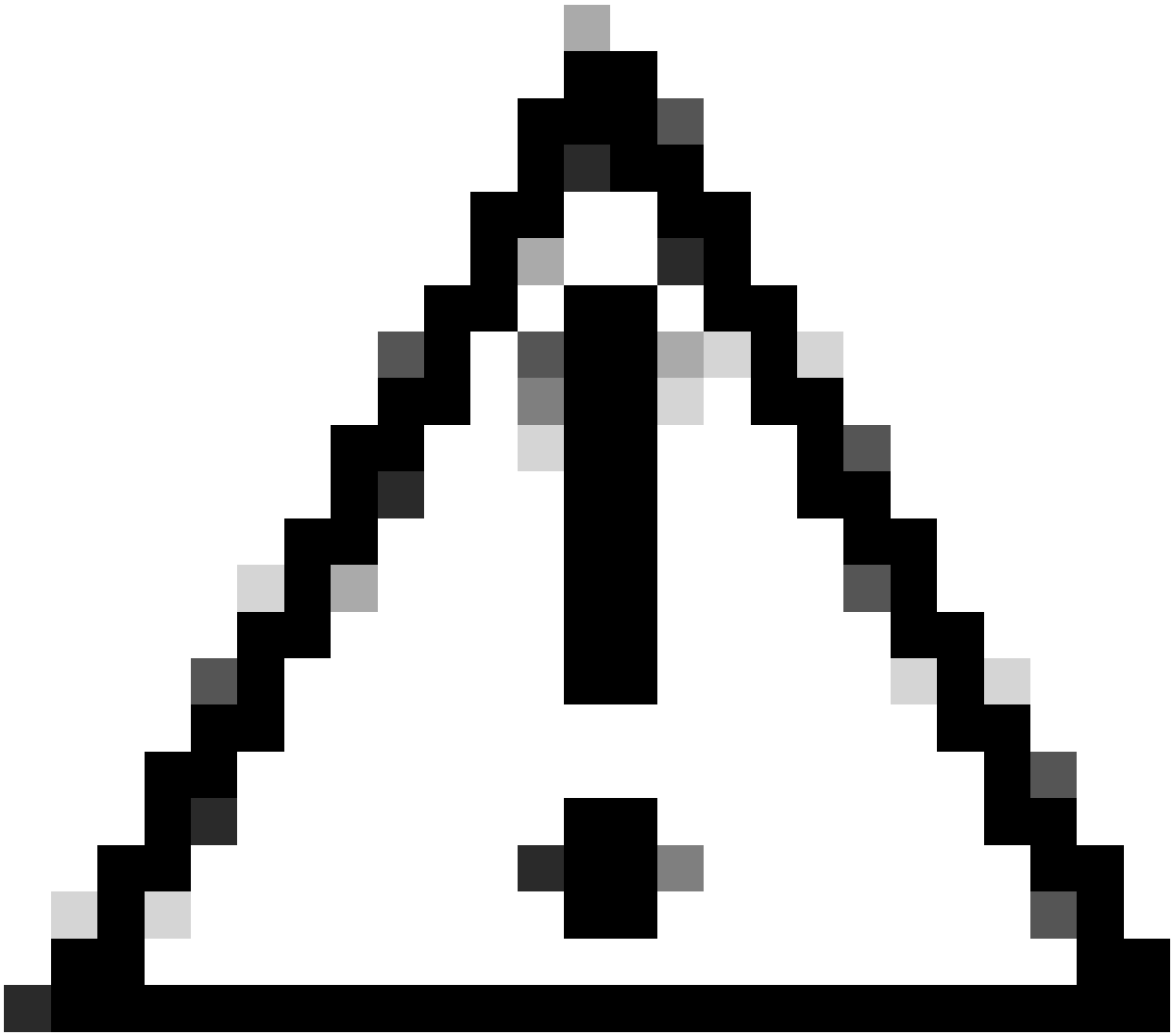
- تكوين الوصول عن بعد ASA/FTD.

المكونات المستخدمة

يستند دليل أفضل الممارسات إلى إصدارات الأجهزة والبرامج التالية:

- Cisco ASA 9.x
- برنامج الدفاع ضد تهديد Firepower 7.x / FMC 7.x

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.



تحذير: لا يحتوي هذا المستند على خطوات لإدارة أجهزة FirePOWER (FDM). يدعم FDM فقط. الرجاء إستخدام قوائم "الإعدادات العامة" لتغيير طريقة المصادقة على DefaultWEBVPNGroup في قسم مخصص في واجهة مستخدم FDM. يجب الاتصال بمركز المساعدة التحكم في الوصول لمستوى التحكم أو منفذ مخصص للوصول عن بعد داخل VPN للوصول على مزيد من المساعدة إذا لزم الأمر. Cisco (TAC) التقنية

معلومات أساسية

الغرض من هذا المستند هو ضمان التزام تكوين AnyConnect VPN الخاص بالعميل الآمن من Cisco بأفضل ممارسات الأمان في عالم حديث حيث تكون هجمات الأمان الإلكتروني شائعة.

عادة ما تتضمن هجمات القوة الغاشمة محاولات متكررة للوصول إلى مورد ما باستخدام مجموعات اسم المستخدم وكلمة المرور. يحاول المهاجمون إستخدام مستعرض الإنترنت الخاص بهم أو واجهة مستخدم العميل الآمن أو أدوات أخرى لإدخال العديد من أسماء المستخدمين وكلمات المرور على أمل مطابقتهم لمجموعة مشروعة في قاعدة بيانات المصادقة والتفويض والمحاسبة (AAA). عند إستخدام المصادقة والتفويض والمحاسبة (AAA) للمصادقة، نتوقع من المستخدم النهائي إدخال اسم المستخدم وكلمة المرور نظرا لأن هذا ضروري لإنشاء الاتصال. في الوقت نفسه، ال نتحقق من هوية المستخدم حتى يقوموا بإدخال بيانات الاعتماد الخاصة بهم. وهذا من شأنه بطبيعة الحال أن يسمح للمهاجمين بالاستفادة من هذه السيناريوهات:

1. كشف أسماء المجالات المؤهلة بالكامل لجدار حماية Cisco الآمن (خاصة عند إستخدام أسماء مستعارة جماعية في ملف تعريف الاتصال):
   - إذا اكتشف المهاجم FQDN لجدار حماية VPN الخاص بك، فسيكون لديهم بعد ذلك خيار تحديد مجموعة النفق باستخدام الاسم المستعار للمجموعة الذي يريدون بدء هجوم القوة الغاشمة فيه.

2. تم تكوين ملف تعريف الاتصال الافتراضي باستخدام AAA أو قاعدة البيانات المحلية:
   - إذا عثر المهاجم على FQDN لجدار حماية VPN، فيمكنه محاولة مهاجمة خادم AAA أو قاعدة البيانات المحلية بالقوة. يحدث هذا لأن الاتصال بحدود FQDN في ملف تعريف الاتصال الافتراضي، حتى في حالة عدم تحديد أسماء مستعارة للمجموعات.

3. إستهلاك الموارد على جدار الحماية أو على خوادم AAA:
   - يمكن للمهاجمين التغلب على خوادم AAA أو موارد جدار الحماية من خلال إرسال كميات كبيرة من طلبات المصادقة وإنشاء حالة قطع الخدمة (DoS).

المفاهيم

أسماء المجموعات المستعارة:

- اسم بديل يمكن لجدار الحماية من خلاله الرجوع إلى ملف تعريف الاتصال. بعد بدء اتصال بجدار الحماية، تظهر هذه الأسماء في قائمة منسدلة في واجهة مستخدم العميل الآمن للمستخدمين الذين سيتم تحديدهم. توفر إزالة الأسماء المستعارة للمجموعات إلى إزالة الوظيفة المنسدلة في واجهة مستخدم العميل الآمن.

عناوين URL الخاصة بالمجموعة:

- عنوان URL يمكن ربطه بملف تعريف اتصال بحيث يتم تعيين الاتصالات الواردة مباشرة إلى ملف تعريف اتصال مرغوب. ال توجد وظيفة منسدلة، حيث يمكن

للمستخدمين إدخال عنوان URL الكامل في واجهة مستخدم العميل الآمن، أو يمكن دمج عنوان URL مع 'اسم العرض' في ملف تعريف XML لإخفاء عنوان URL من المستخدم.

يكمن الاختلاف هنا في حالة تطبيق أسماء مستعارة جماعية، حيث يباشر المستخدم الاتصال to vpn_gateway.example.com ويقدم مع أسماء مستعارة لتحديد دفعهم إلى ملف تعريف اتصال. باستخدام عناوين URL الخاصة بالمجموعة، يدأ المستخدم الاتصال ب vpn_gateway.example.com/example_group ويقودهم مباشرة إلى ملف تعريف الاتصال بدون الحاجة إلى قائمة منسدلة أو خيار.

ممارسات تقوية العميل الآمن على جدار الحماية الآمن من Cisco:

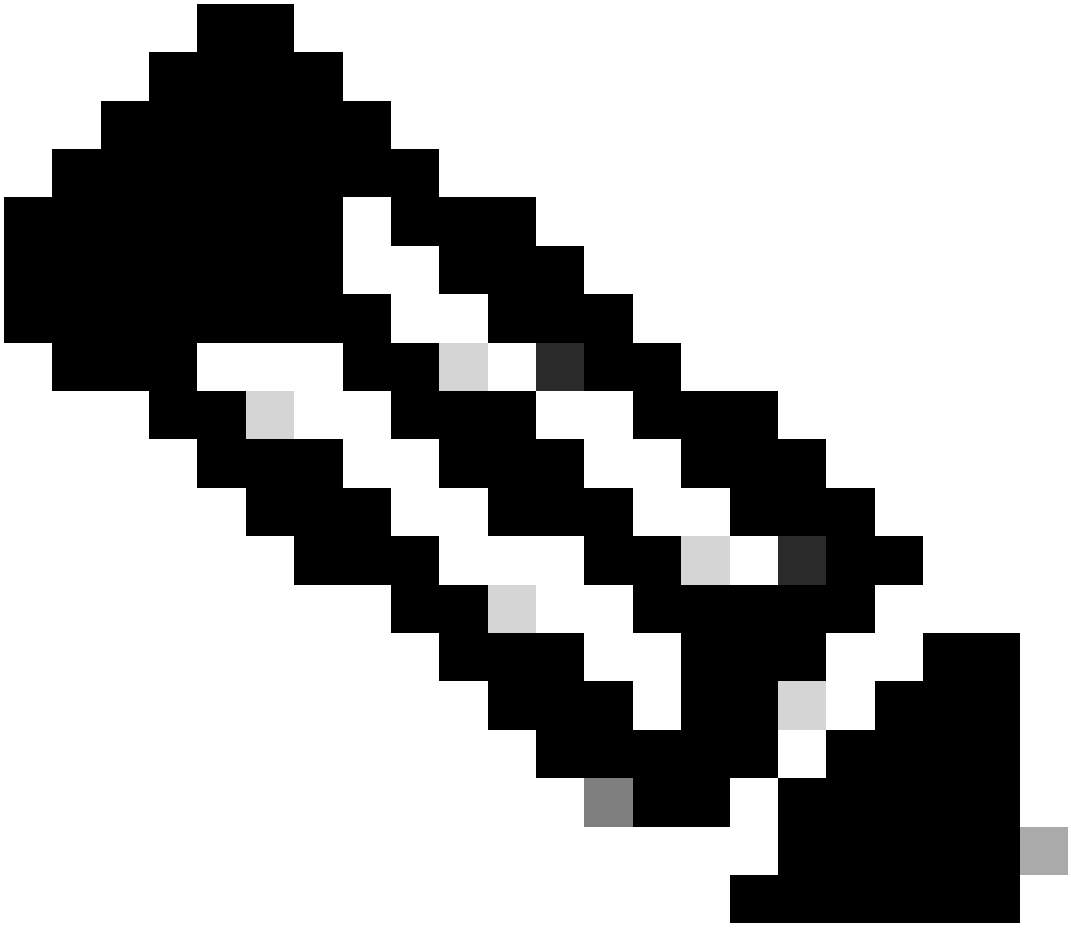
تعتمد هذه الطرق على تعيين المستخدمين الشرعيين لملفات تعريف الاتصال/مجموعات النفق المناسبة بينما يتم إرسال المستخدمين الضارين المحتملين إلى مجموعة نفق مالئمة نقوم بتكوينها لعدم السماح بتركيبات اسم المستخدم وكلمة المرور. وعلى الرغم من أنه ال يجب تنفيذ كافة التجميعات، إال أن تعطيل أسماء المجموعات المستعارة وتغيير طريقة المصادقة الخاصة ب DefaultRAGgroup و DefaultWEBvpngGroup مطلوبان لتنفيذ التوصيات بشكل فعال.

- قم بتعطيل أسماء المجموعات المستعارة واستخدم عنوان URL الخاص بالمجموعة فقط في تكوين ملف تعريف الاتصال، وهذا يسمح لك بامتالك FQDN مجدد لن يكون من السهل للمهاجم اكتشافه وتحديده نظرا ألن العمالء الذين لديهم FQDN المناسب هم فقط القادرون على بدء الاتصال. على سبيل المثال، vpn_gateway.example.com/example_group هو أكثر صعوبة للمهاجم من الكشف عن موقع vpn_gateway.example.com.

- قم بتعطيل مصادقة AAA في DefaultWEBvpngGroup و DefaultRAGgroup وتكوين مصادقة الشهادة، مما يجنبنا إمكانية فرض الأمر بشكل قاس على قاعدة البيانات المحلية أو خادم AAA. وسيواجه المهاجم في هذا السيناريو أخطاء فورية عند محاولة الاتصال. ال يوجد حقل اسم مستخدم أو كلمة مرور نظرا ألن المصادقة تستند إلى الشهادات، وبالتالي يتم إيقاف محاوالت القوة الغاشمة. خيار آخر وهو إنشاء خادم AAA بدون تكوين داعم لإنشاء حفرة للطلبات الضارة.

- إستخدام تعيين الشهادة لملف تعريف الاتصال. وهذا يسمح بتعيين الاتصاالت الواردة على توصيفات توصيل محددة استنادا إلى السمات المستلمة من الشهادات الموجودة على جهاز العميل. يتم تعيين المستخدمين الذين لديهم الشهادات المناسبة بشكل صحيح، بينما يتم إرسال المهاجمين الذين يخفقون في معايير التعيين إلى DefaultWEBVPNGgroup.

- يتسبب إستخدام IKEv2-IPSec بدال من SSL في اعتماد مجموعات النفق على تعيين محدد لمجموعة المستخدمين في ملف تعريف XML. بدون XML على جهاز المستخدم النهائي، يتم إرسال المستخدمين تلقائيا إلى مجموعة النفق االفتراضية.



ملاحظة: للحصول على مزيد من المعلومات حول وظيفة الاسم المستعار للمجموعة، راجع دليل تكوين ASA VPN وراقب 'الجدول 1. سمات ملف تعريف الاتصال ل SSL VPN'.

تحديد الهجمات باستخدام معرفات التسجيل و syslog

تمثل هجمات القوة الغاشمة الطريقة السائدة للتضحية بشبكات VPN الخاصة بالوصول عن بعد، واستغلال كلمات المرور الضعيفة للحصول على الدخول غير المصرح به. من المهم للغاية معرفة كيفية التعرف على علامات الهجوم من خلال الاستفادة من إستخدام تسجيل الدخول وتقييم syslog. معرفات syslogs الشائعة التي يمكن أن تشير إلى هجوم إذا تمت مواجهتها بوحدة تخزين غير عادية هي:

٪ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database : user = admin : user

٪ASA-6-113005

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =

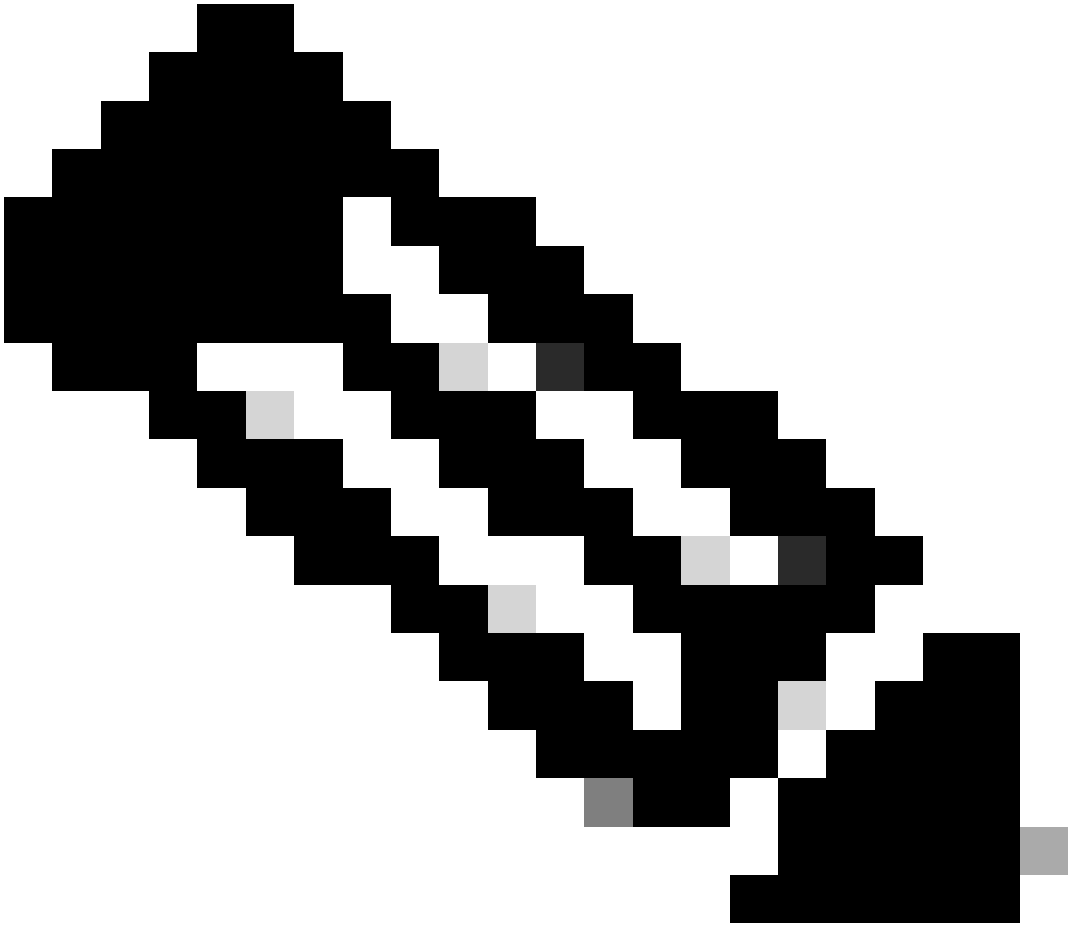
٪ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN

اسم المستخدم مخفي دائما حتى يتم تكوين الأمر no logging hide username على ASA.



ملاحظة: يوفر هذه معلومات حول ما إذا تم إنشاء مستخدمين صالحين أو معرفتهم من خلال عناوين IP المسيئة، يرجى توخي الحذر نظرا لظهور أسماء المستخدمين في السجلات.

تسجيل دخول ASA من Cisco:

دليل المستخدم لجدار حماية ASA الآمن
فصل التسجيل من دليل تكوين واجهة سطر الأوامر الخاصة بالعمليات العامة Cisco Secure Firewall ASA Series General Operations CLI

تسجيل الدخول إلى برنامج الإرسال فائق السرعة (FTD) من Cisco:

تكوين التسجيل على FTD عبر FMC

تكوين قسم syslog في فصل إعدادات النظام الأساسي من دليل تكوين جهاز مركز إدارة جدار الحماية الآمن من Cisco
تكوين syslog والتحقق من صحته في FirePOWER Device Manager

تكوين قسم إعدادات تسجيل النظام في فصل إعدادات النظام من دليل تكوين الدفاع عن تهديد FirePOWER ل FirePOWER

التحقق من الهجوم

للتحقق، قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) ASA أو FTD، ثم قم بتشغيل الأمر show aaa-server، وتحقق من عدد غير عادي من طلبات المصادقة التي تم المحاولة عليها أو رفضها إلى أي من خوادم AAA التي تم تكوينها:

```
<#root>

ciscoasa#

show aaa-server



Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 8473575 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
Number of rejects 8473574 - - - - - >>>> Unusual increments
```

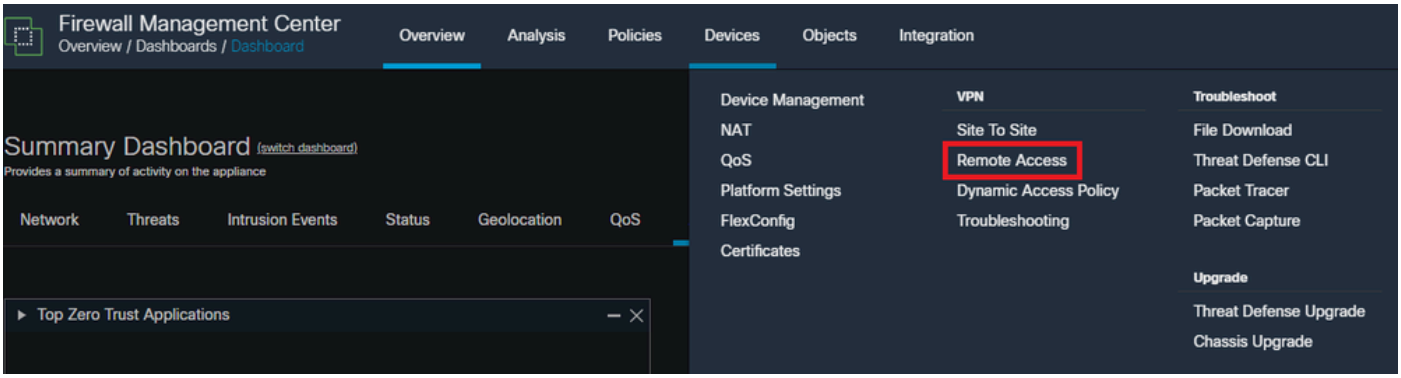
```
<#root>

ciscoasa#

show aaa-server



Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 2228536 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
Number of rejects 2225363 - - - - - >>>> Unusual increments
Number of challenges 0
Number of malformed responses 0
```

```
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```

أمثلة تكوين FMC

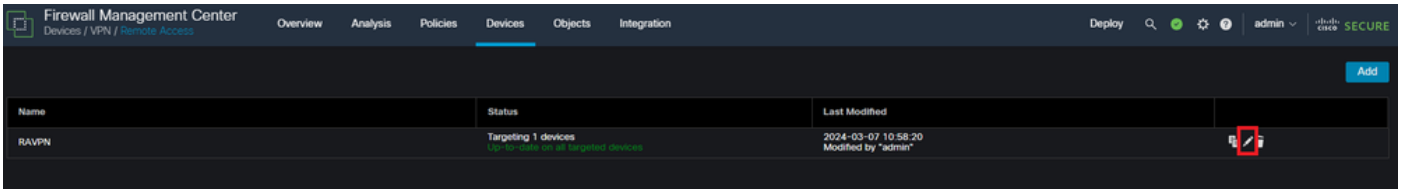
تعطيل مصادقة AAA في توصيفات توصيل DefaultWebVPNGroup و DefaultRagGroup

انتقل إلى الأجهزة > الوصول عن بعد.



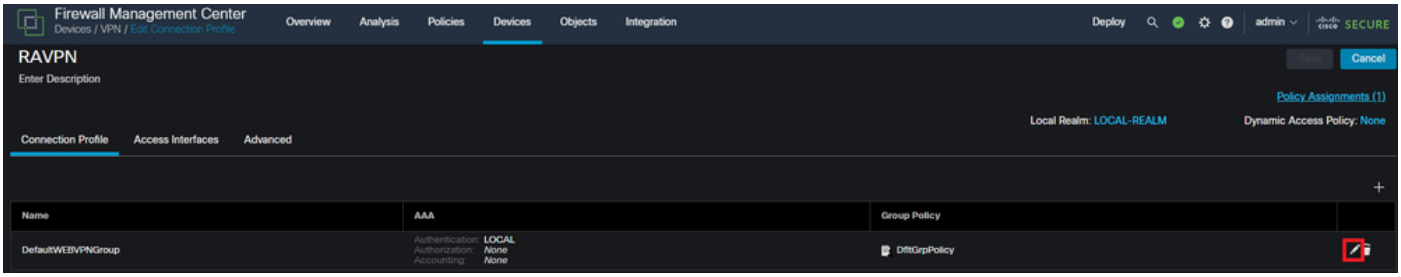
يعرض التنقل في واجهة المستخدم الرسومية (GUI) لـ FMC للوصول إلى تكوين نهج VPN للوصول عن بعد.

تحرير نهج VPN الموجود للوصول عن بعد وإنشاء ملف تعريف اتصال باسم 'DefaultRAGgroup'



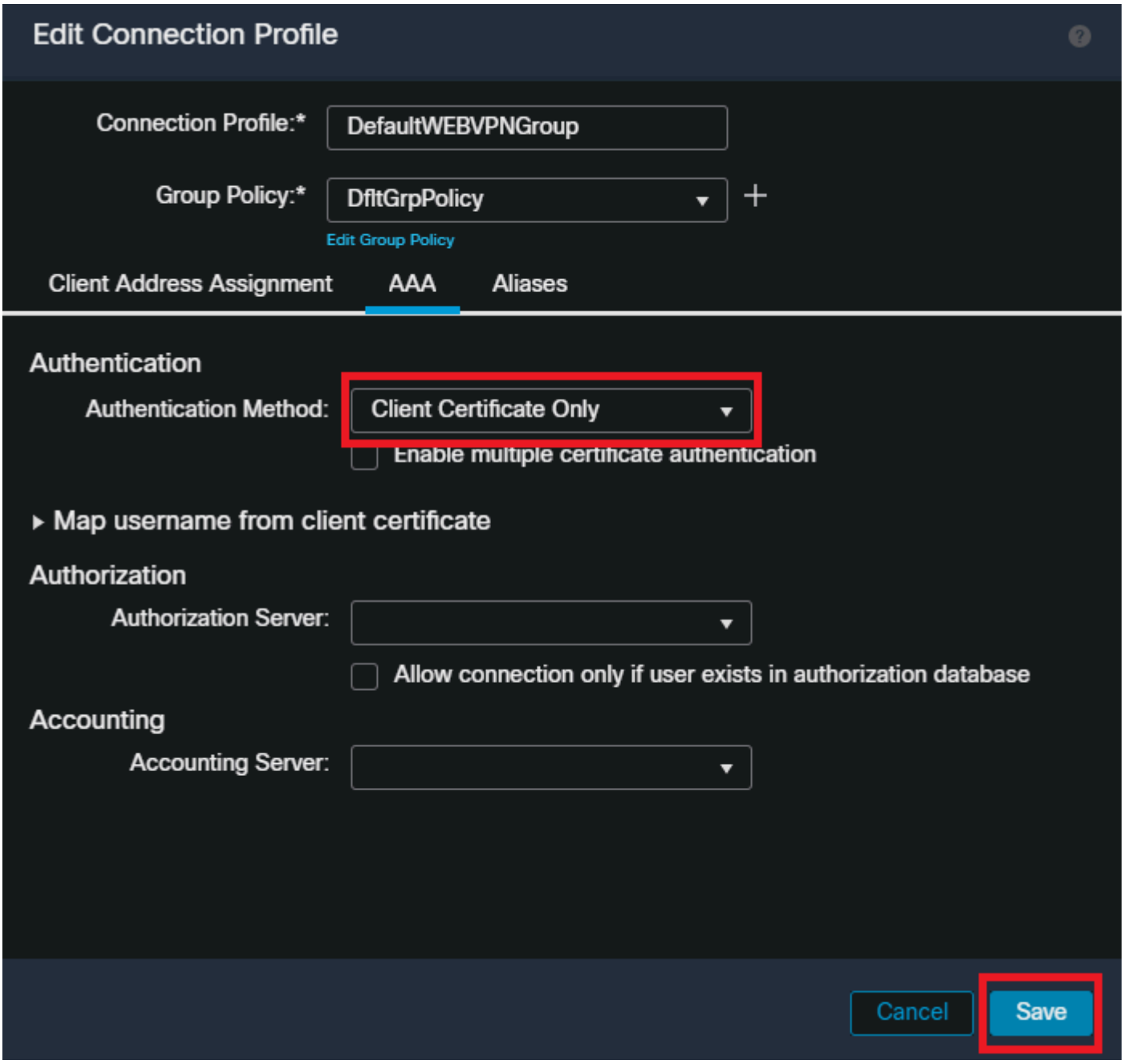
عرض كيفية تحرير نهج VPN للوصول عن بعد داخل واجهة مستخدم FMC.

تحرير ملفات تعريف الاتصال المسماة 'DefaultWEBVPNGroup' و'DefaultRAGroup'



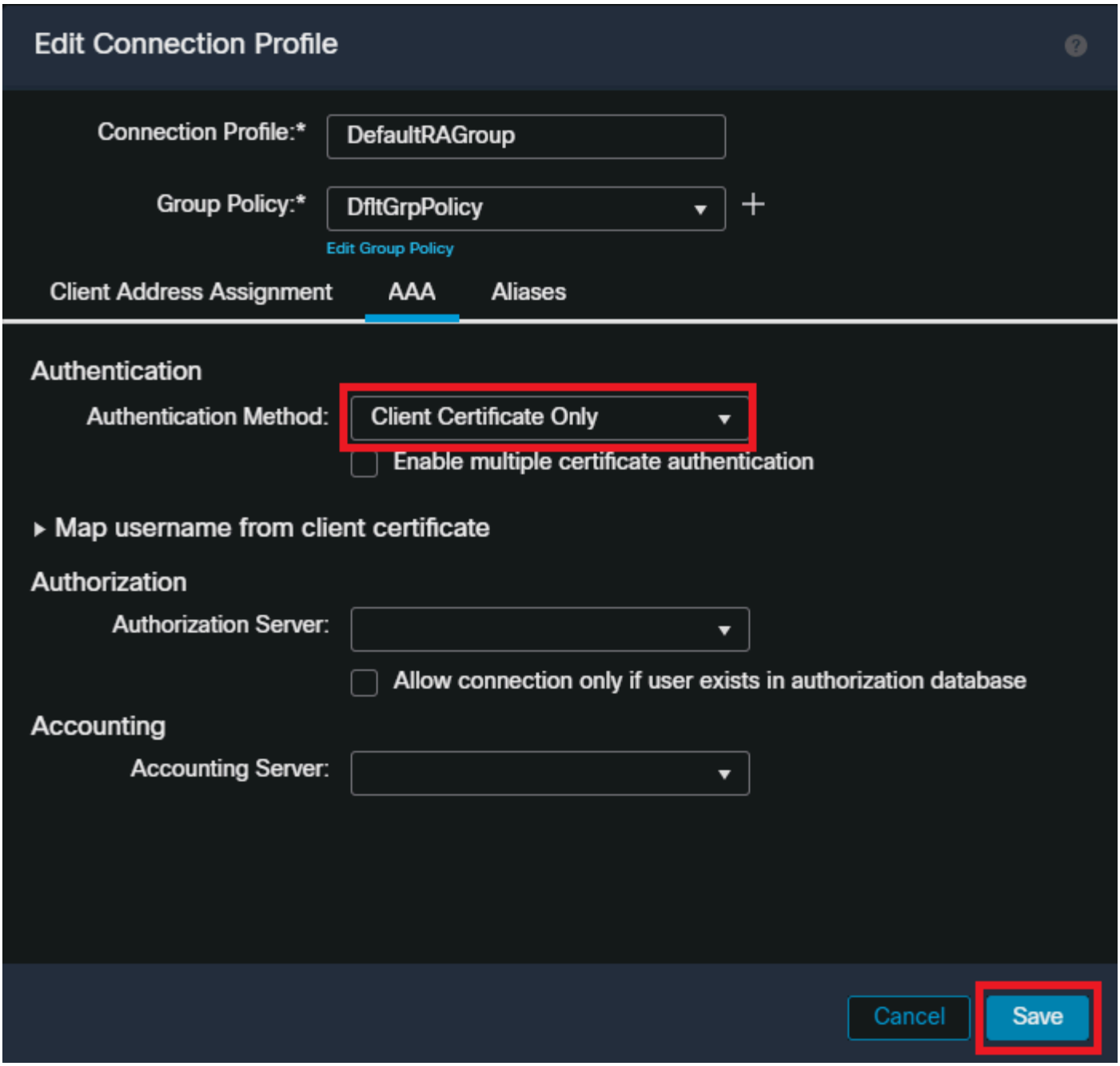
عرض كيفية تحرير DefaultWEBVPNGroup ضمن واجهة مستخدم FMC.

انتقل إلى علامة التبويب AAA وحدد القائمة المنسدلة أسلوب المصادقة. حدد 'شهادة العميل فقط' وحدد حفظ.

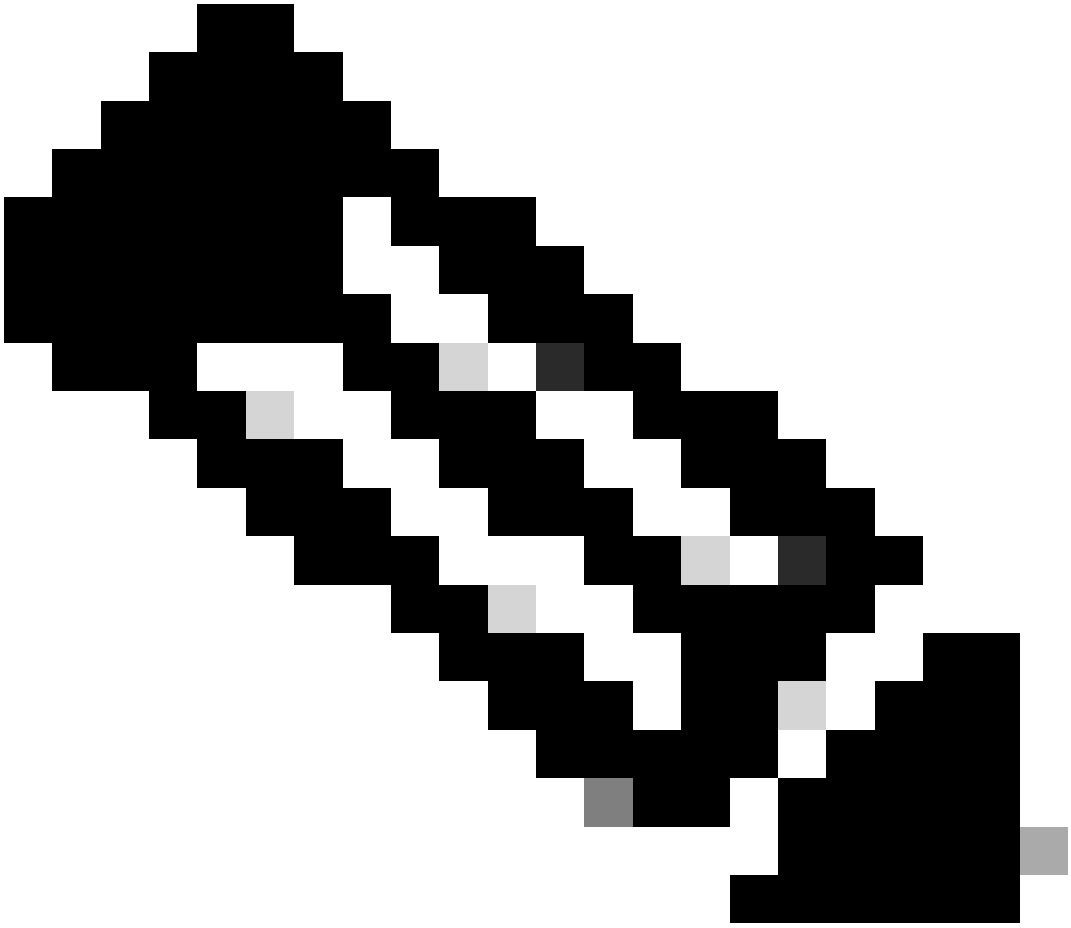


تغيير طريقة المصادقة إلى شهادة العميل فقط لـ DefaultWEBVPNGroup داخل واجهة مستخدم FMC.

قم بتحرير DefaultRAGgroup وانتقل إلى علامة التبويب AAA وحدد القائمة المنسدلة أسلوب المصادقة. حدد 'شهادة العميل فقط' وحدد حفظ.



تغيير طريقة المصادقة إلى شهادة العميل فقط لـ DefaultRAGroup داخل واجهة مستخدم FMC.

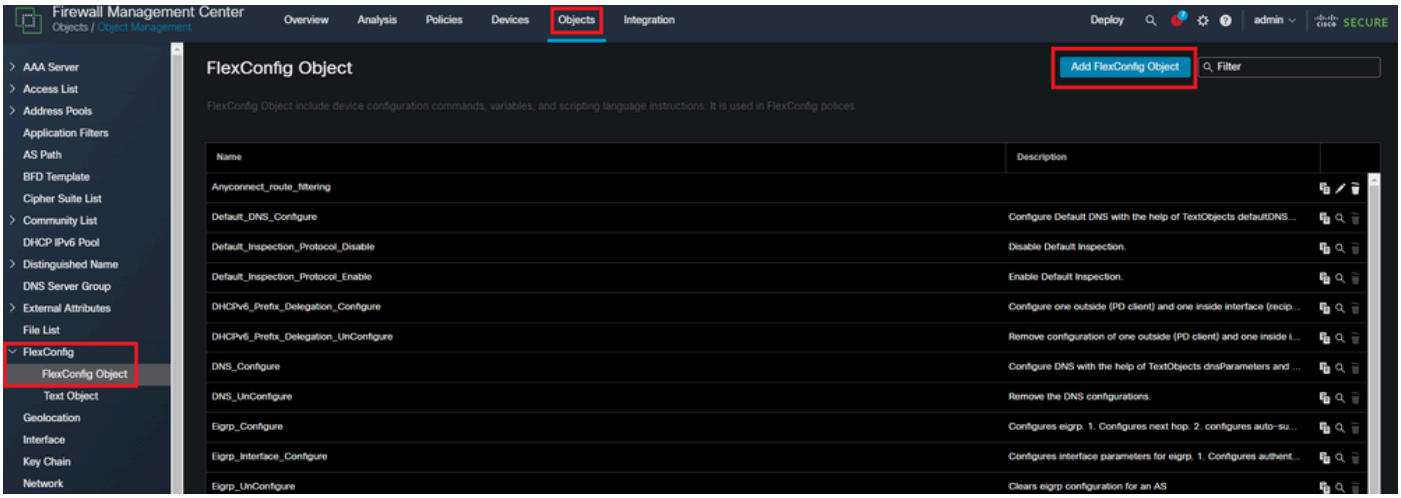


ملاحظة: يمكن أن يكون أسلوب المصادقة أيضا خادم AAA للفتحة الأخيرة. إذا تم إستخدام هذه الطريقة، فإن تكوين خادم AAA يكون مزيفا والي يعالج أي طلبات بالفعل. يجب أيضا تعريف تجمع VPN في عملية التبويب "تعيين عنوان العميل" لحفظ التغييرات.

تعطيل Hostscan / وضع جدار الحماية الآمن على DefaultWEBvpngGroup و DefaultRAGgroup (إختياري)

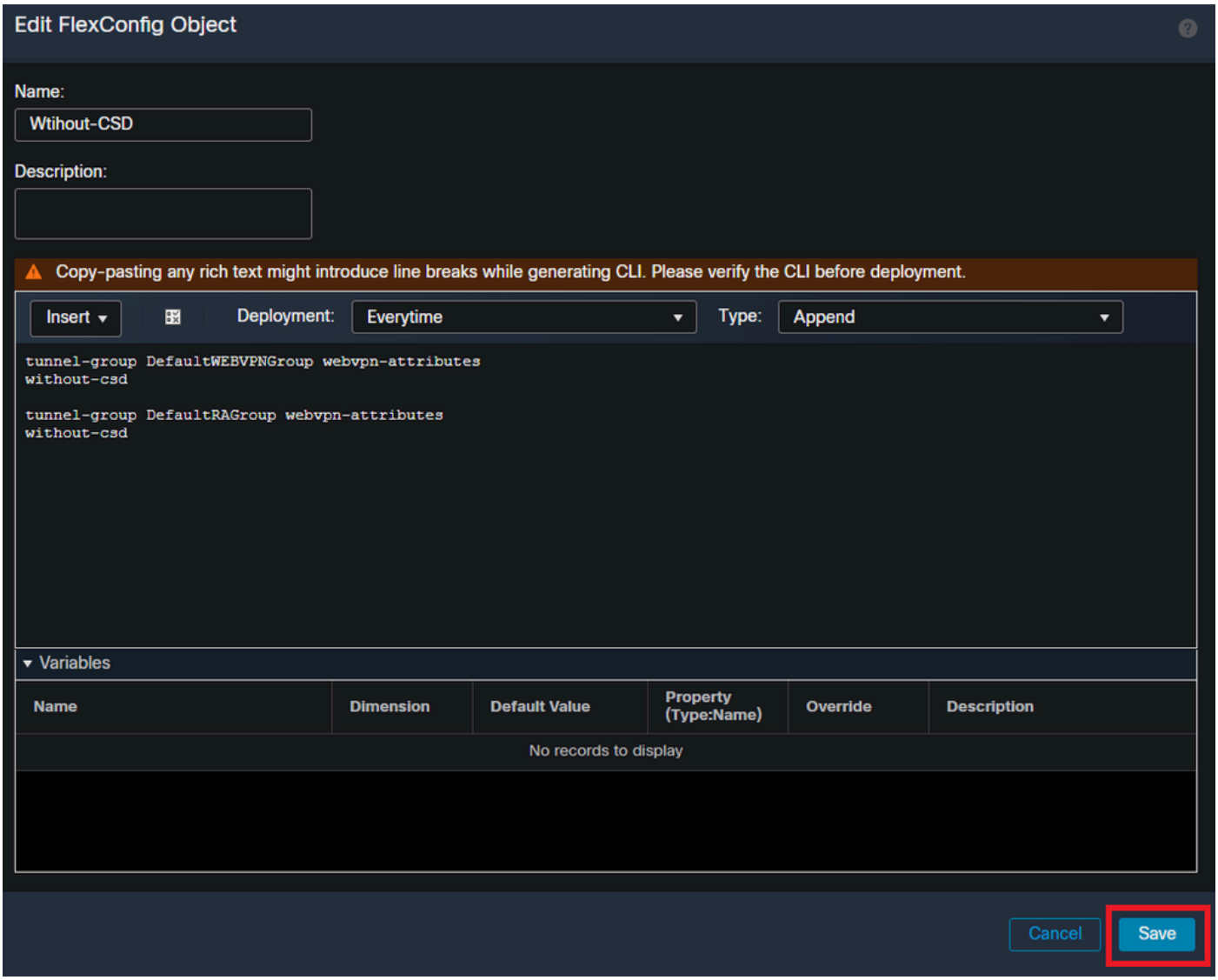
الي يكون هذا ضروريا إلا إذا كان لديك Hostscan / Secure Firewall Posture (وضعية جدار الحماية الآمنة) في بيئتك. تمنع هذه الخطوة المهاجمين من زيادة إستخدام الموارد على جدار الحماية بسبب عملية المسح الضوئي لنقطة النهاية. في FMC، يتم تحقيق ذلك من خلال إنشاء كائن FlexConfig باستخدام الأمر without-csd لتعطيل وظيفة المسح الضوئي لنقطة النهاية.

انتقل إلى الكائنات > إدارة الكائن > كائن FlexConfig > إضافة كائن FlexConfig.



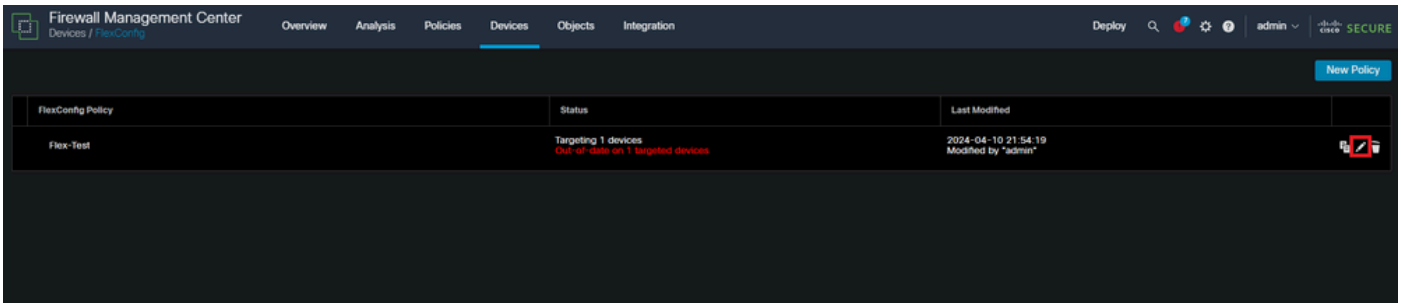
التنقل في واجهة مستخدم FMC لإنشاء كائن FlexConfig.

قم بتسمية الكائن FlexConfig، ثم قم بتعيين النشر على كل وقت باستخدام النوع Append. ثم أدخل الصياغة كما هو موضح تمامًا ثم احفظ الكائن.



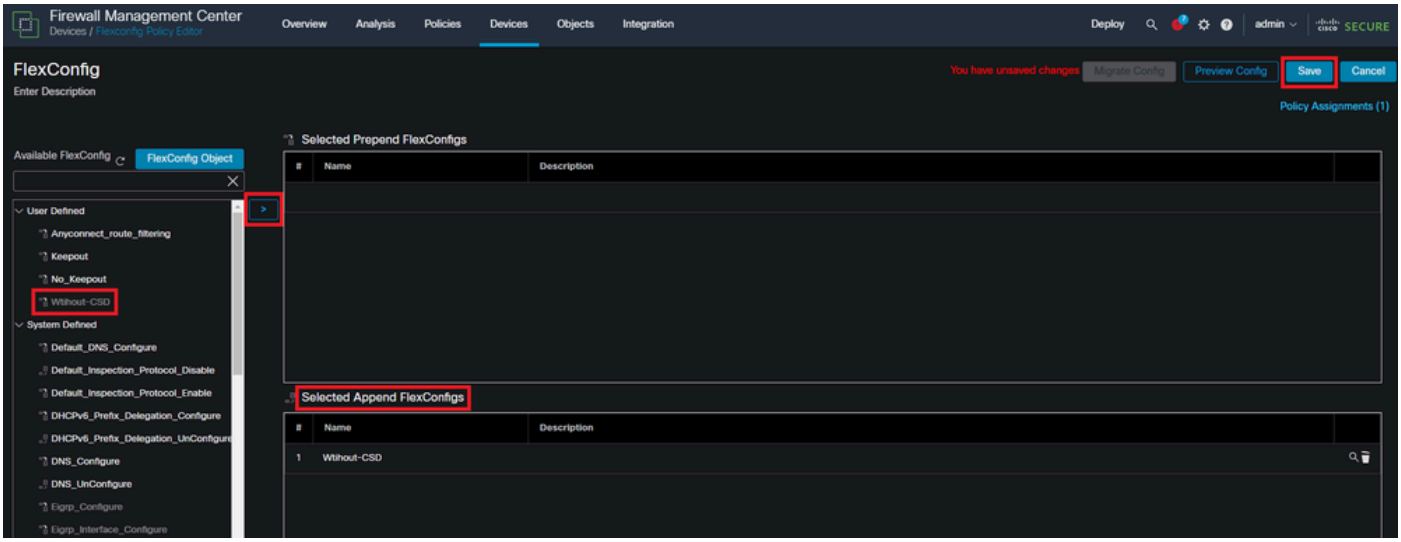
إنشاء كائن FlexConfig باستخدام 'without-csd'

انتقل إلى الأجهزة > FlexConfig ثم انقر فوق Cil لتحرير سياسة FlexConfig.



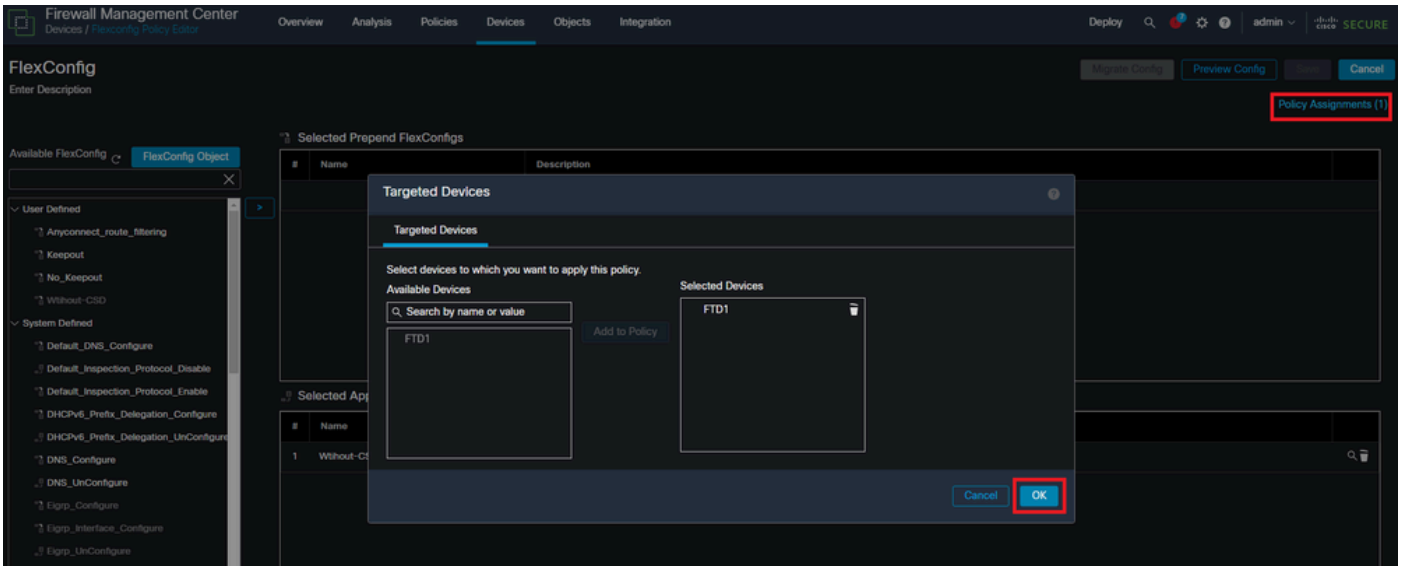
تحرير سياسة FlexConfig داخل FMC.

حدد موقع الكائن الذي قمت بإنشائه من القسم المعرف من قبل المستخدم. ثم حدد السهم للإضافته إلى Append FlexConfigs المحدد. أخيرا، حدد حفظ لحفظ نهج FlexConfig.



قم بإرفاق الكائن FlexConfig بسياسة FlexConfig.

حدد تعيينات النهج واختر FTD الذي تريد تطبيق نهج FlexConfig هذا عليه، ثم حدد موافق. حدد حفظ مرة أخرى إذا كان هذا هو تعيين FlexConfig جديد وقم بنشر التغييرات. التحقق من الصحة بمجرد النشر



قم بتخصيص سياسة FlexConfig لجهاز FirePOWER.

أدخل واجهة سطر أوامر (CLI) في FTD وأصدر الأمر show run tunnel-group لـ DefaultWEBvpngGroup و DefaultRagGroup. دقق أن دون csd الآن حاضر في التشكيل.

<#root>

FTD72#

show run tunnel-group DefaultRAGroup

```
tunnel-group DefaultRAGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultRAGroup webvpn-attributes
authentication certificate
```

without-csd

FTD72#

show run tunnel-group DefaultWEBVPNGroup

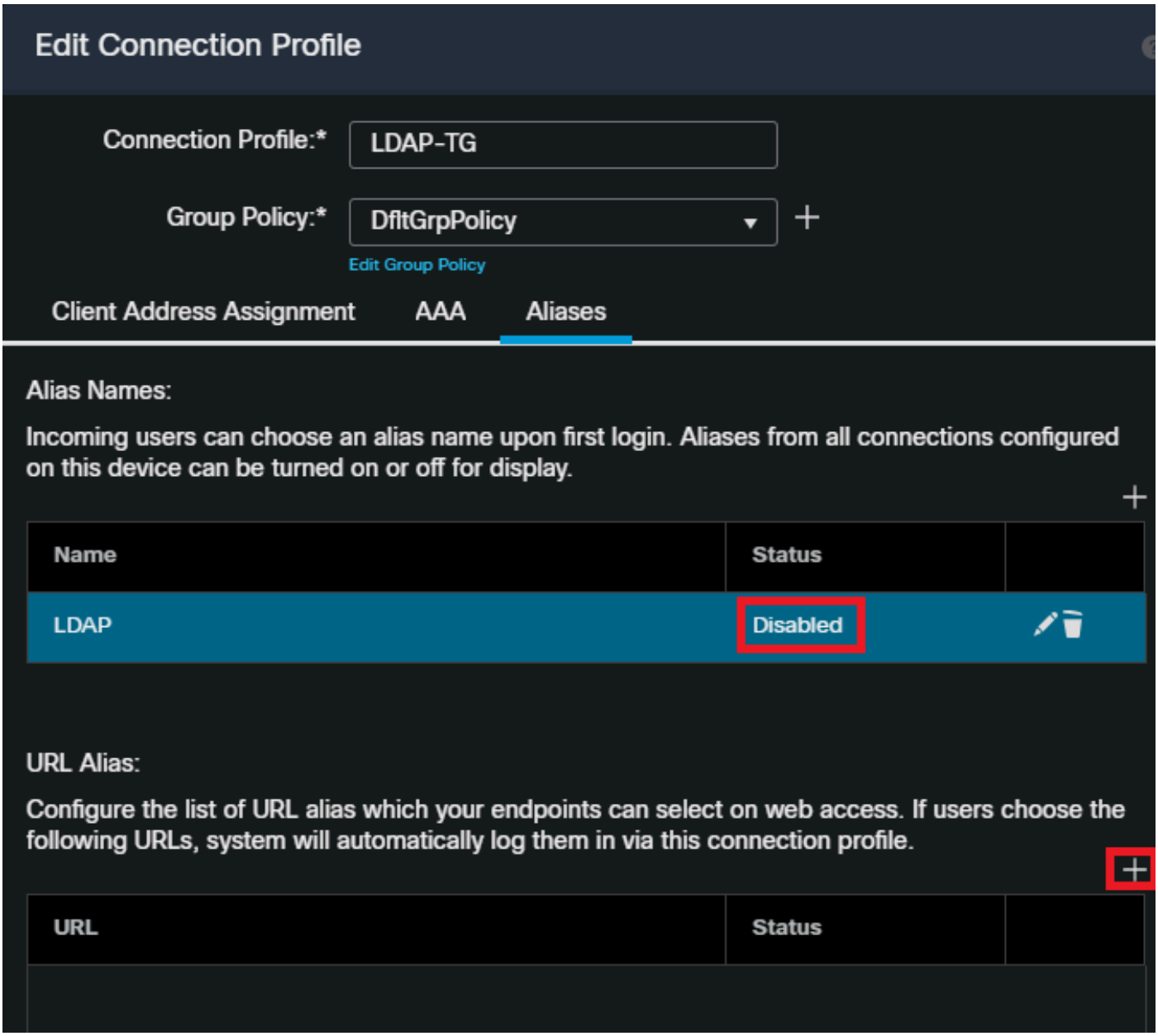
```
tunnel-group DefaultWEBVPNGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultWEBVPNGroup webvpn-attributes
authentication certificate
```

without-csd

تعطيل أسماء المجموعة المستعارة وتمكين عناوين URL الخاصة بالمجموعة

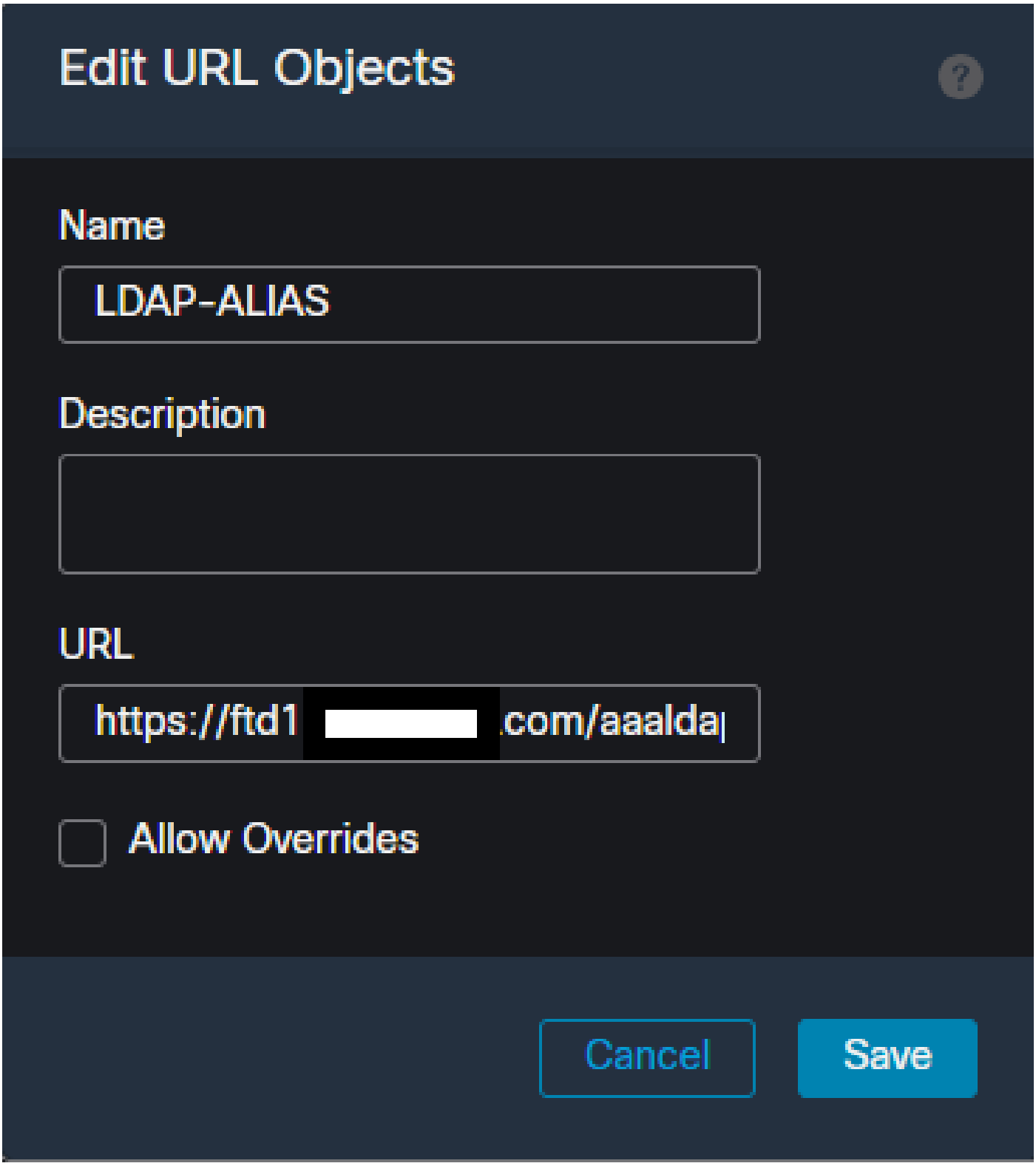
انتقل إلى ملف تعريف اتصال وحدد علامة التبويب أسماء مستعارة". قم بتعطيل أو حذف

الاسم المستعار للمجموعة، وانقر أيقونة زائد لإضافة اسم مستعار ل URL.



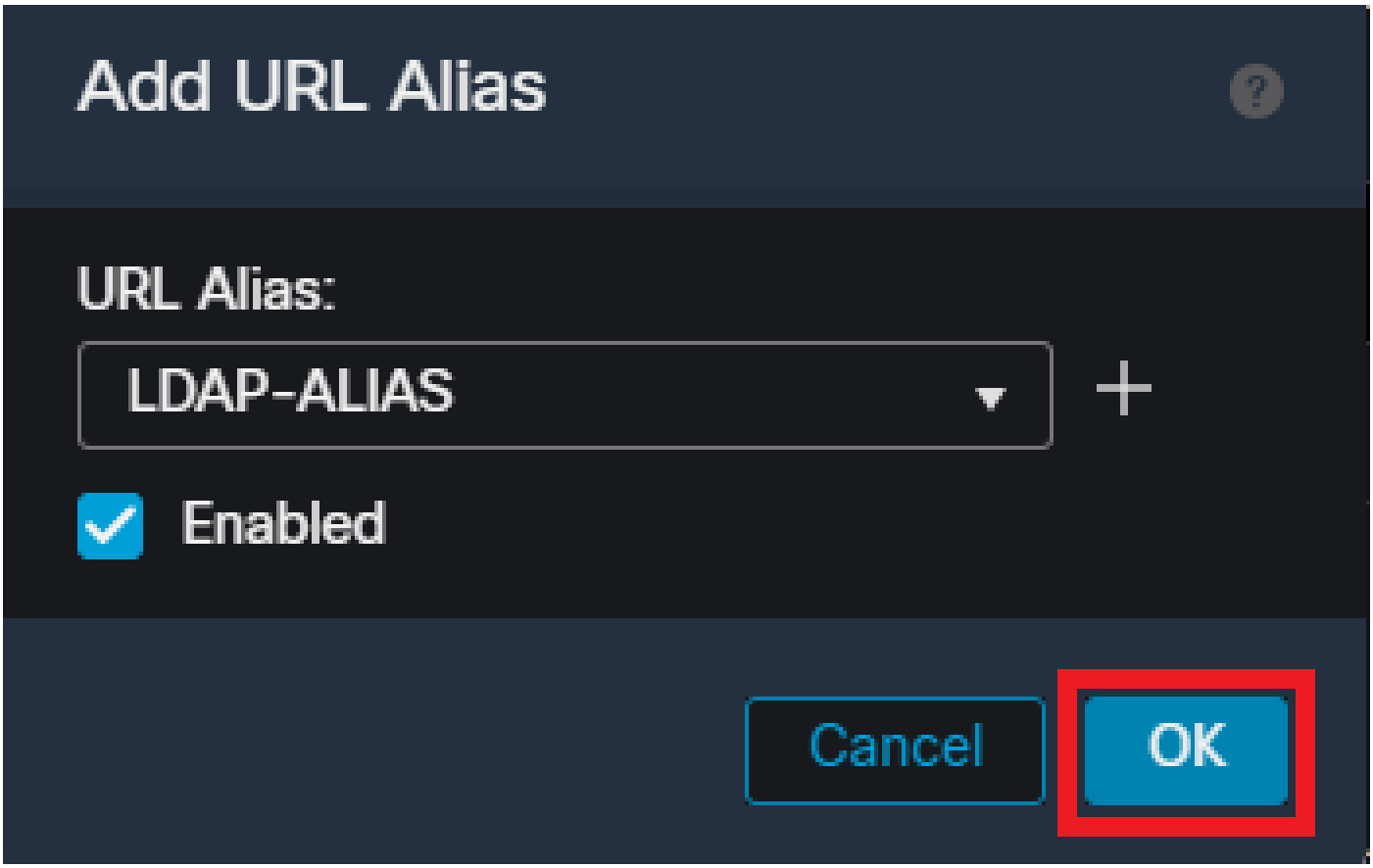
تعطيل خيار الاسم المستعار للمجموعة النفق داخل واجهة مستخدم FMC.

قم بتكوين اسم كائن للاسم المستعار لعنوان URL، وقم بتعبئة FQDN و/أو عنوان IP لجدار الحماية لعنوان URL، متبوعا بالاسم الذي تريد إقران ملف تعريف الاتصال به. في هذا المثال، اخترنا 'aaldap'. كلما كان مبهما أكثر، كلما كان أكثر أمانا، حيث يكون من غير المحتمل للمهاجمين تخمين عنوان URL الكامل حتى إذا كانوا قد حصلوا على FQDN الخاص بك. بمجرد الانتهاء، حدد حفظ.



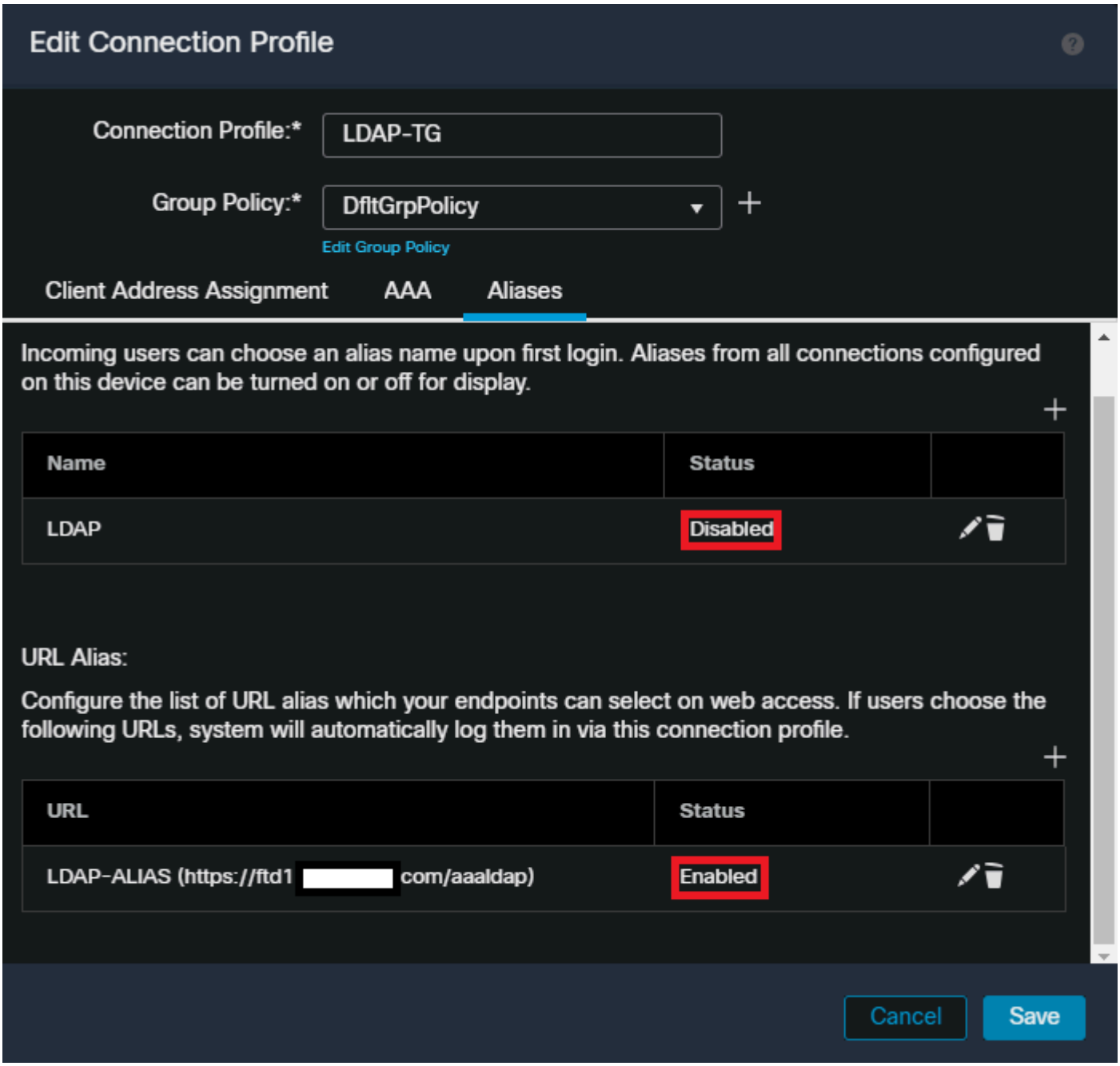
إنشاء كائن URL-Alias داخل واجهة مستخدم FMC.

حدد الاسم المستعار لعنوان URL من القائمة المنسدلة، وحدد المربع ممكن وحدد موافق.



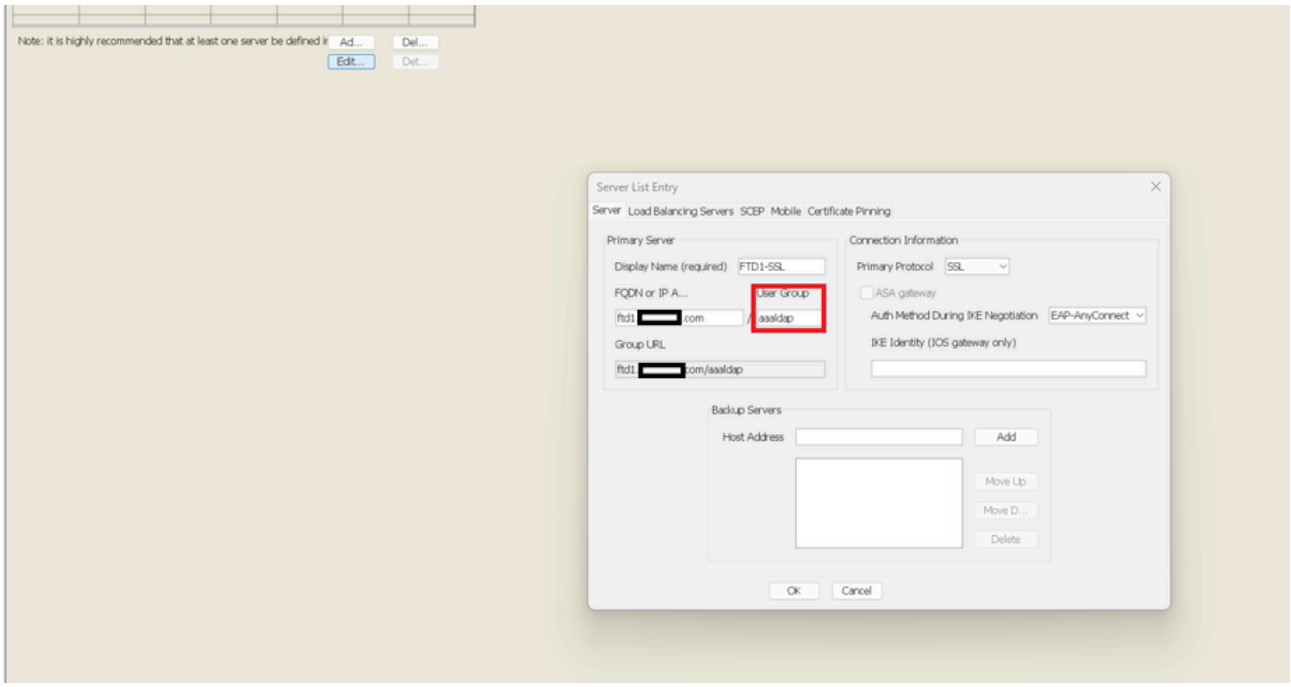
تأكد من تمكين الاسم المستعار لعنوان URL داخل واجهة مستخدم FMC.

تأكد من حذف الاسم المستعار للمجموعة أو تعطيله وتحقق من تمكين الاسم المستعار لعنوان URL الآن ثم حدد حفظ.



تمكين خيار الاسم المستعار لعنوان URL لمجموعة النفق ضمن واجهة مستخدم FMC.

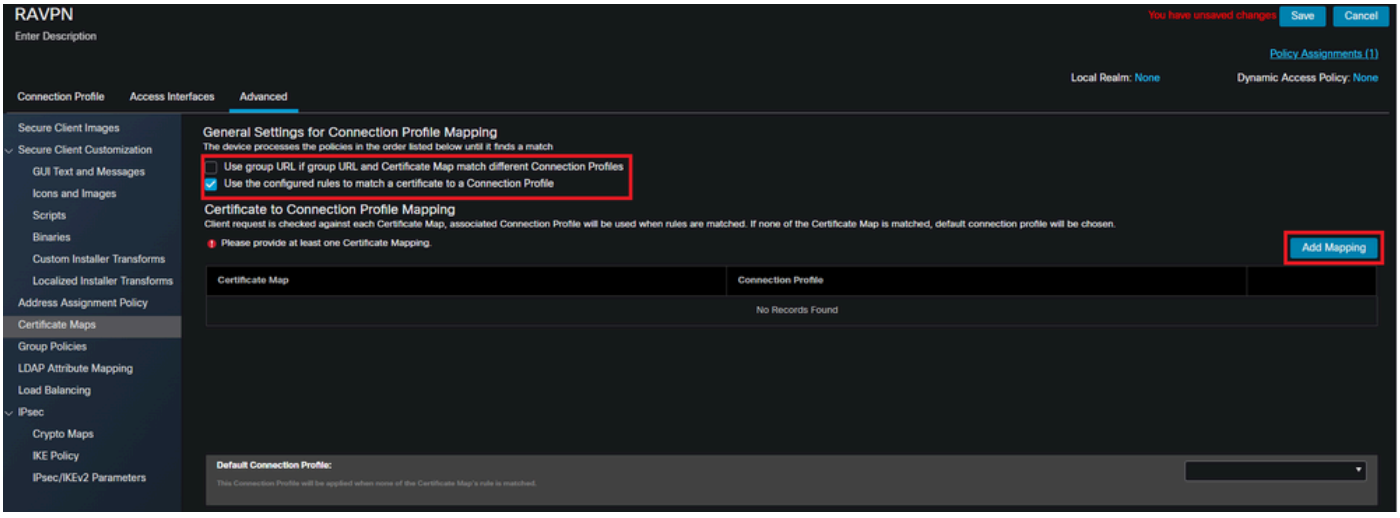
إذا رغبت، يمكن أيضا دفع أسماء URL المستعارة كجزء من XML. ويتم تحقيق ذلك من خلال تحرير XML باستخدام محرر ملف تعريف VPN أو محرر ملف تعريف ASA. للقيام بذلك، انتقل إلى علامة التبويب "قائمة الخوادم" وتأكد من تطابق حقل "مجموعة المستخدمين" مع الاسم المستعار لعنوان URL الخاص بملف تعريف الاتصال عند إستخدام SSL. بالنسبة ل IKEv2، تأكد من تطابق حقل مجموعة المستخدمين مع الاسم المحدد لملف تعريف الاتصال.



تحرير ملف تعريف XML للحصول على اسم مستعار ل URL لاتصالات SSL.

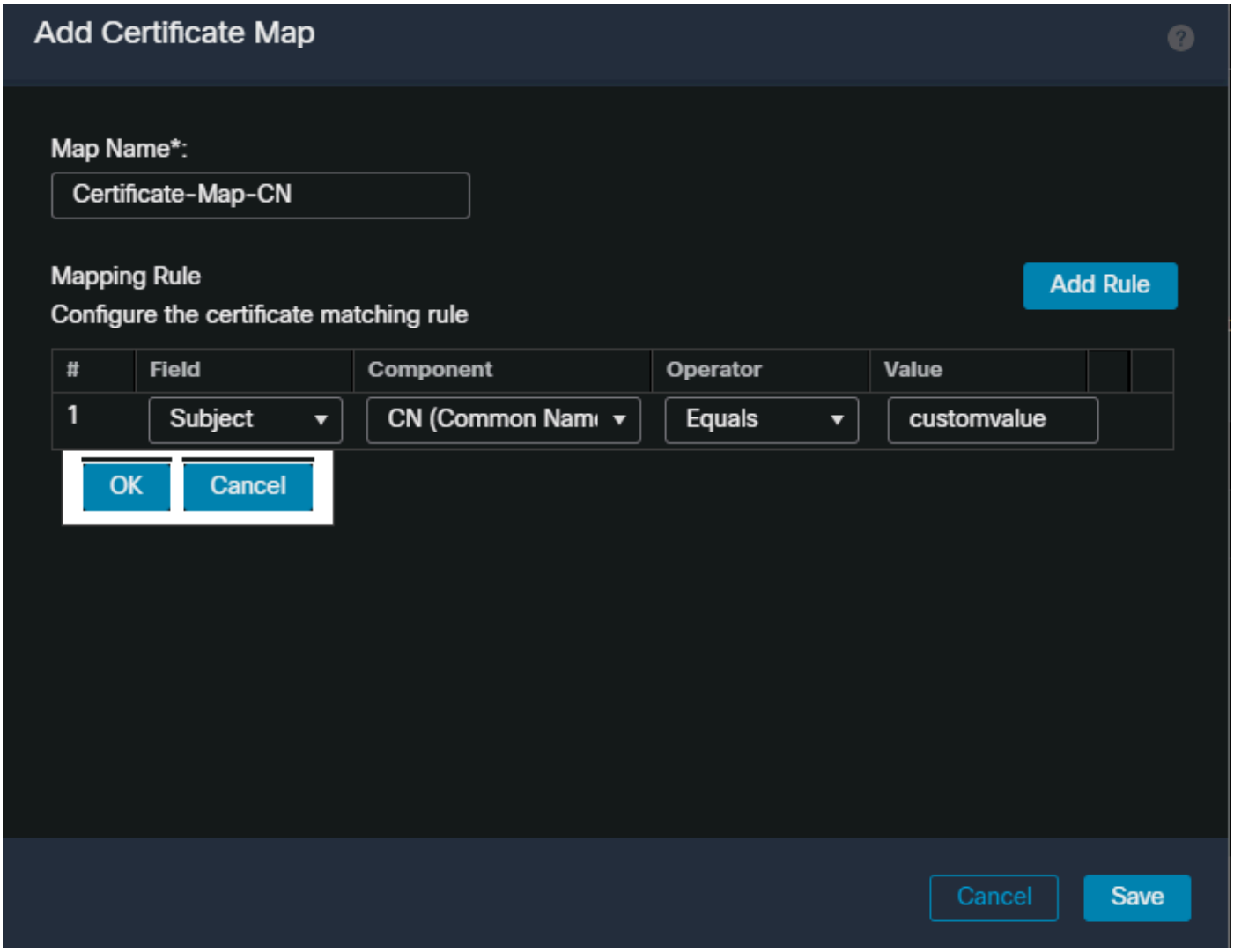
تعيين الشهادة

انتقل إلى علامة التبويب خيارات متقدمة ضمن نهج VPN للوصول عن بعد. أختر خيار إعداد عام بناء على التفضيل. بمجرد تحديده، حدد إضافة تخطيط.



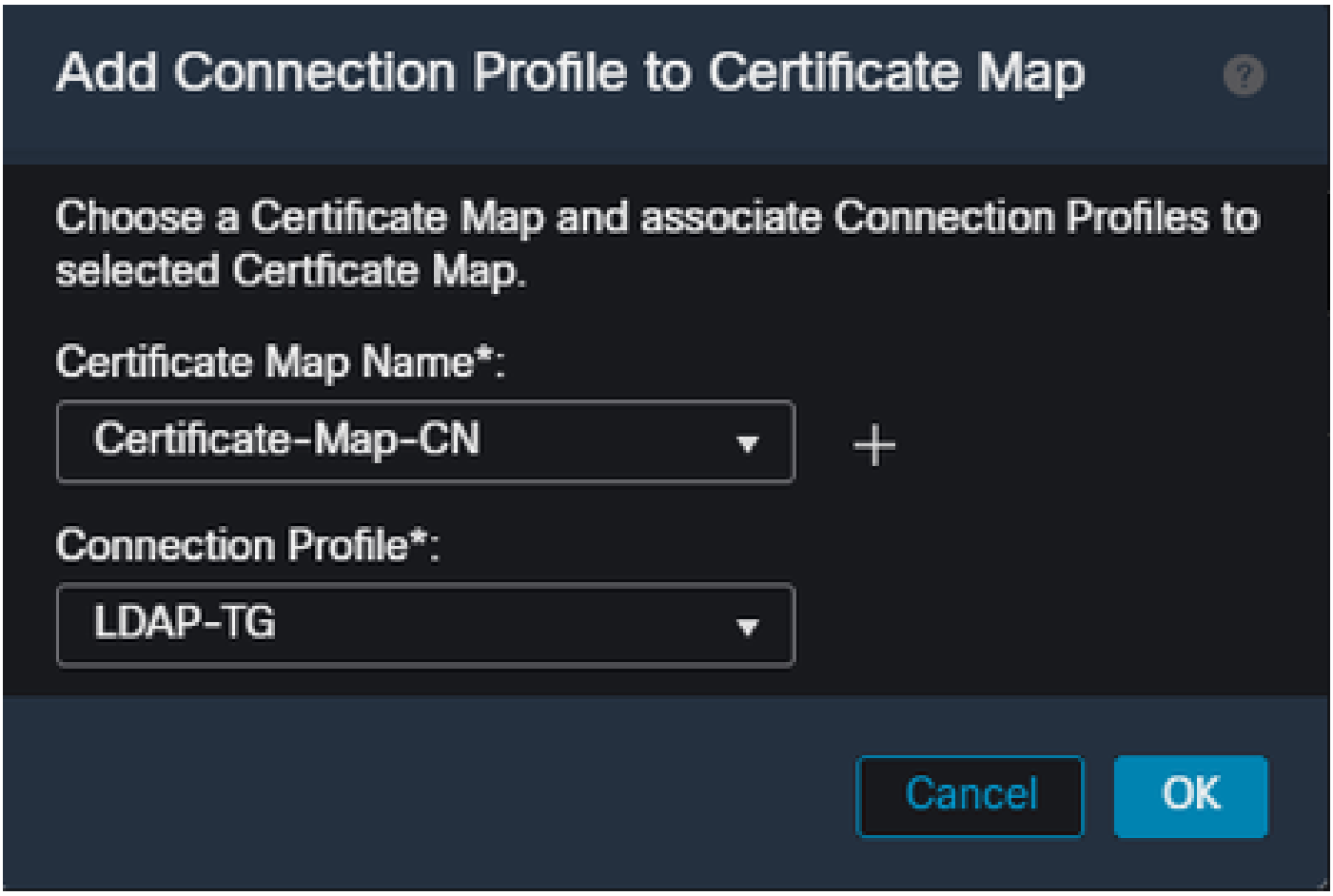
الانتقال إلى علامة التبويب خيارات متقدمة ضمن واجهة مستخدم FMC لإنشاء كائن خريطة ترخيص داخل واجهة مستخدم FMC.

قم بتسمية كائن خريطة الشهادة وحدد إضافة قاعدة. في هذه القاعدة، قم بتحديد خصائص الشهادة التي ترغب في تعريفها لتعيين المستخدم إلى ملف تعريف اتصال معين. بمجرد الانتهاء، حدد موافق ثم حدد حفظ.



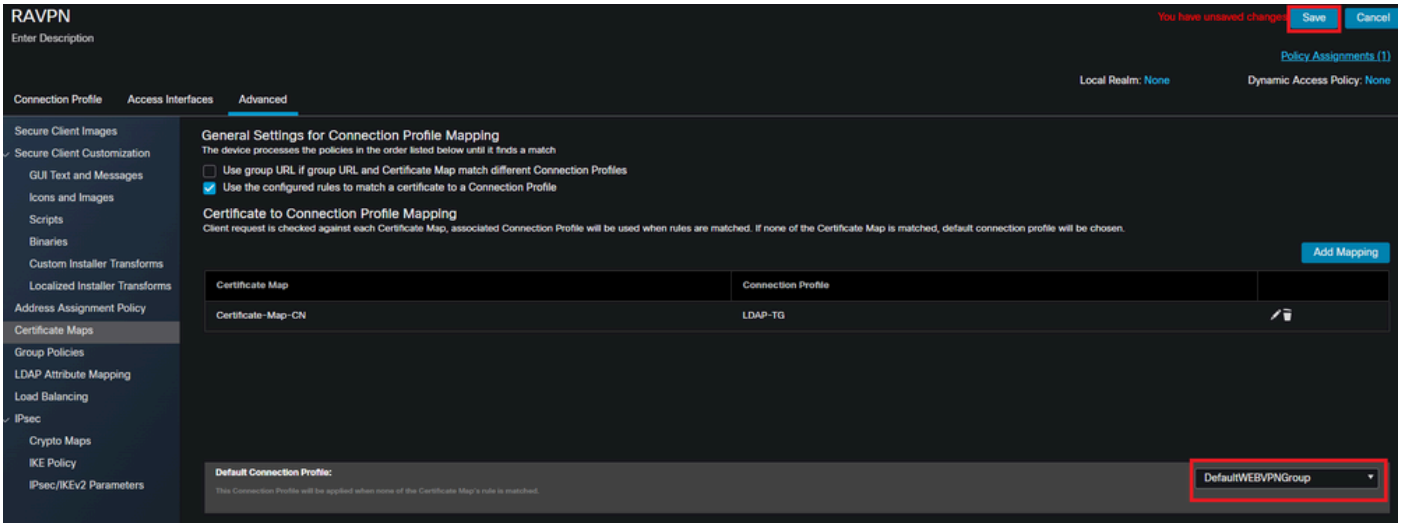
قم بإنشاء خريطة شهادة وإضافة معايير للخريطة داخل واجهة مستخدم FMC.

من القائمة المنسدلة، حدد كائن خريطة الشهادة، وتوصيف التوصيل الذي تريد أن يقترن به خريطة الشهادة. ثم حدد موافق.



قم بربط كائن خريطة الشهادة بمجموعة النفق المطلوبة داخل واجهة مستخدم FMC.

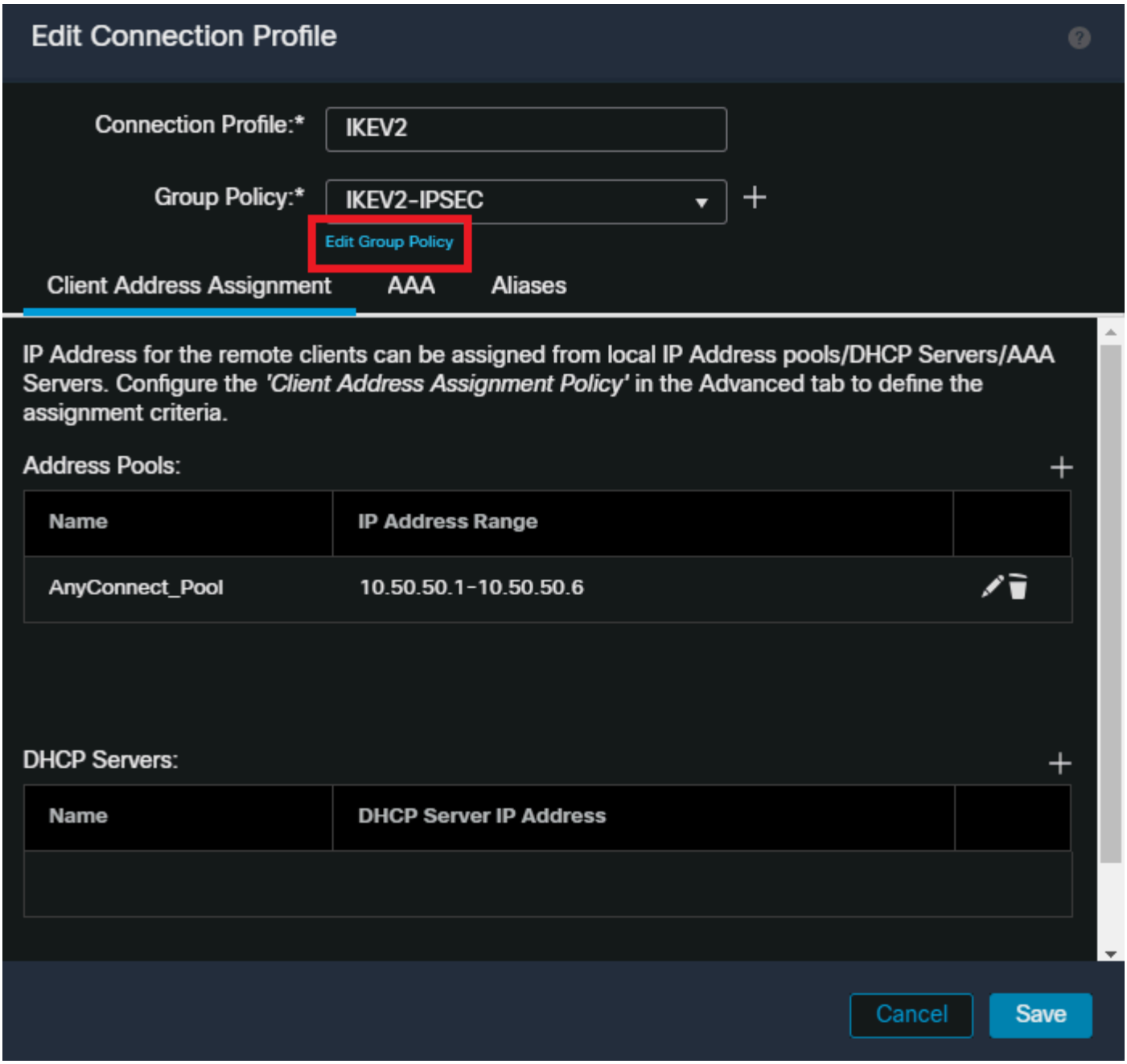
تأكد من تكوين ملف تعريف الاتصال الافتراضي ك DefaultWEBVPNGroup حتى إذا فشل المستخدم في التعيين يتم إرساله إلى DefaultWEBVPNGroup. بمجرد الانتهاء، حدد حفظ ونشر التغييرات.



قم بتغيير ملف تعريف الاتصال الافتراضي لتعيين الشهادة إلى DefaultWEBVPNGroup ضمن واجهة مستخدم FMC.

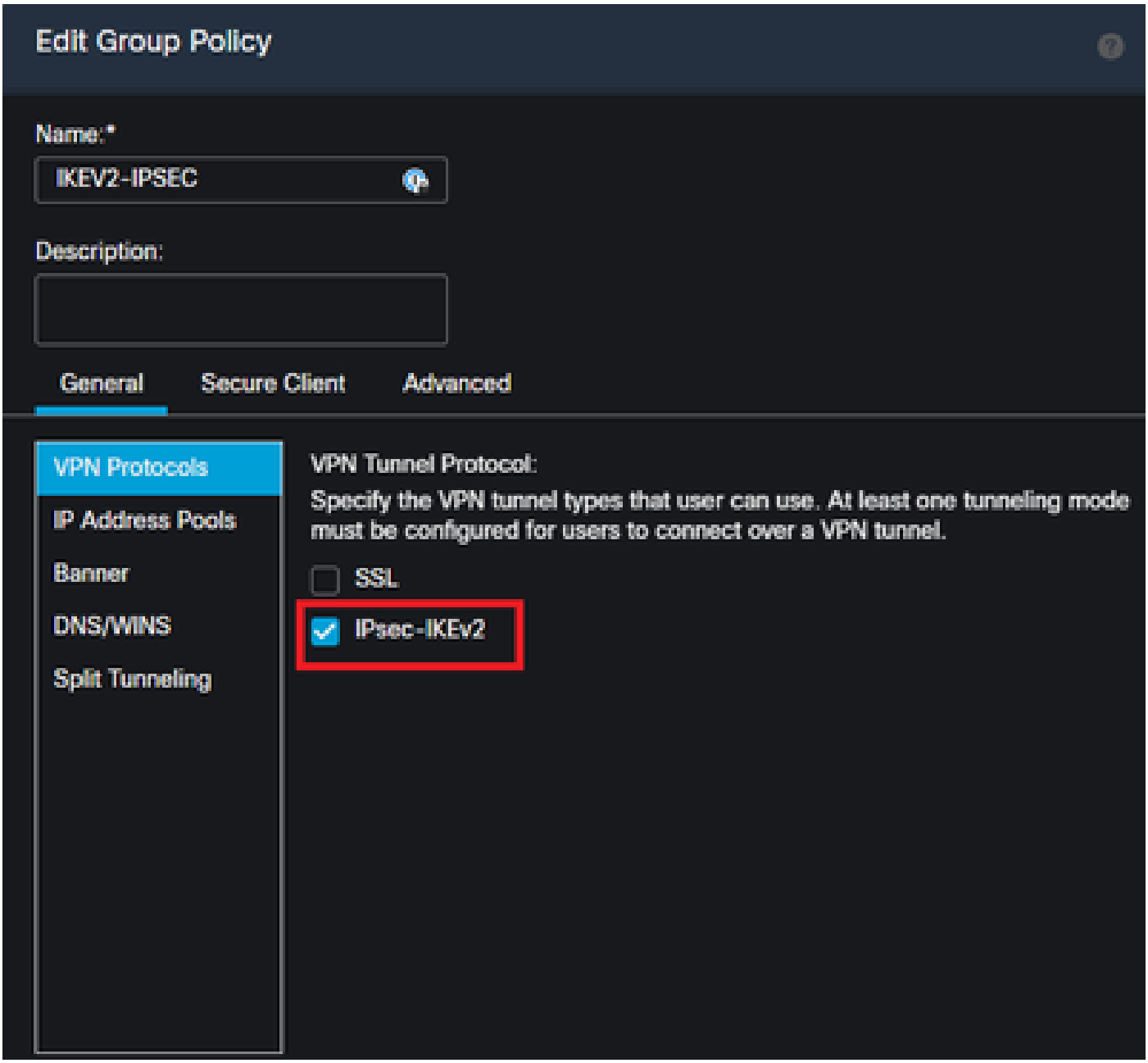
IPsec-IKEv2

حدد ملف تعريف اتصال IPsec-IKEv2 المطلوب، وانتقل إلى تحرير نهج المجموعة.



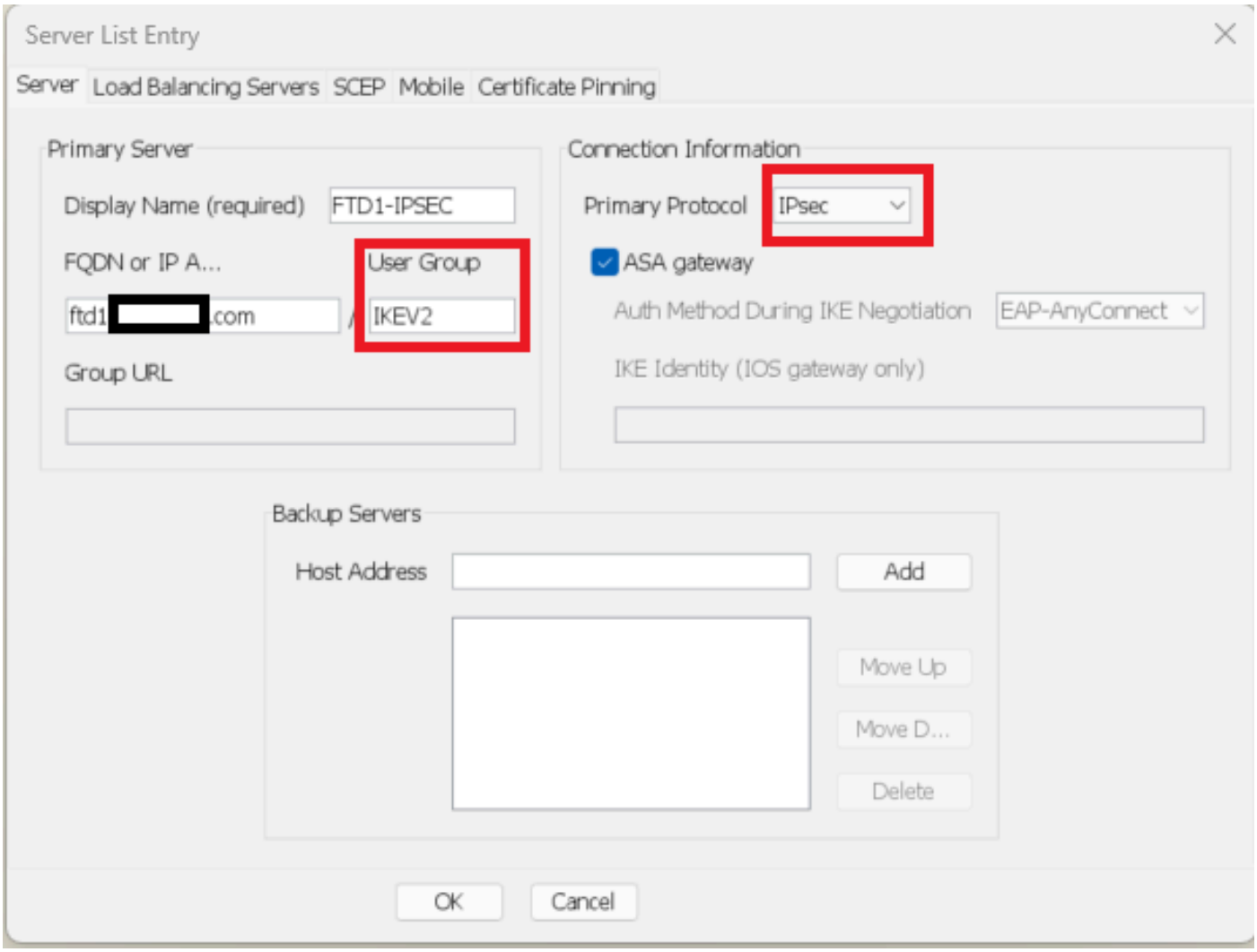
تحرير نهج مجموعة داخل واجهة مستخدم FMC.

في علامة التبويب عام، انتقل إلى قسم بروتوكولات VPN وتأكد من تحديد مربع IPsec-IKEv2.

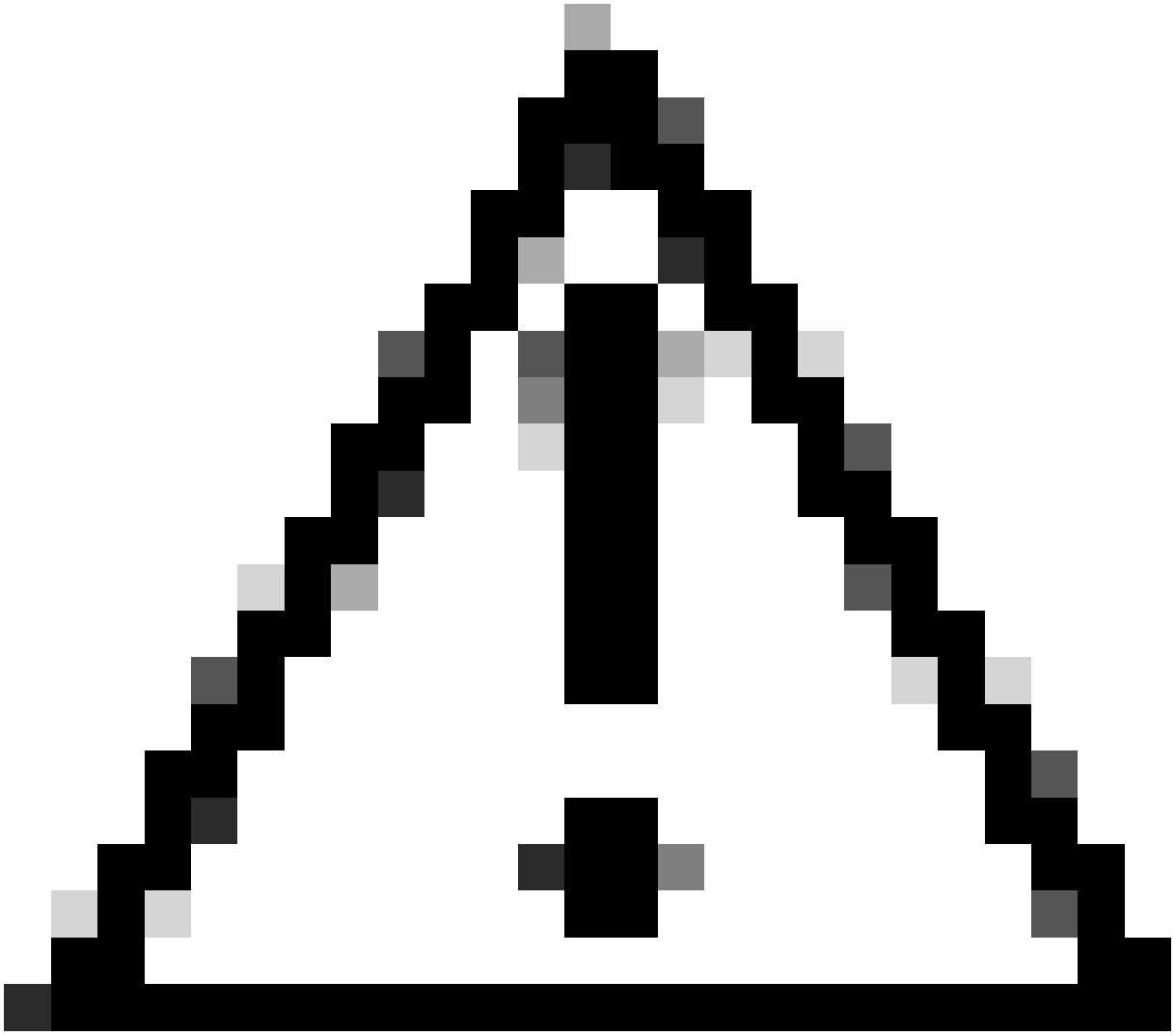


قم بتمكين IPsec-IKEv2 داخل نهج المجموعة في واجهة مستخدم FMC.

في محرر ملف تعريف VPN، أو محرر ملف تعريف ASA، انتقل إلى علامة التبويب قائمة الخوادم. يجب أن يكون اسم مجموعة المستخدمين مطابقا تماما لاسم ملف تعريف الاتصال الموجود على جدار الحماية. في هذا المثال، كان IKEV2 هو ملف تعريف الاتصال / اسم مجموعة المستخدمين. تم تكوين البروتوكول الأساسي ك IPsec. يتم عرض "اسم العرض" في واجهة مستخدم العميل الآمن عند إنشاء اتصال بملف تعريف الاتصال هذا.

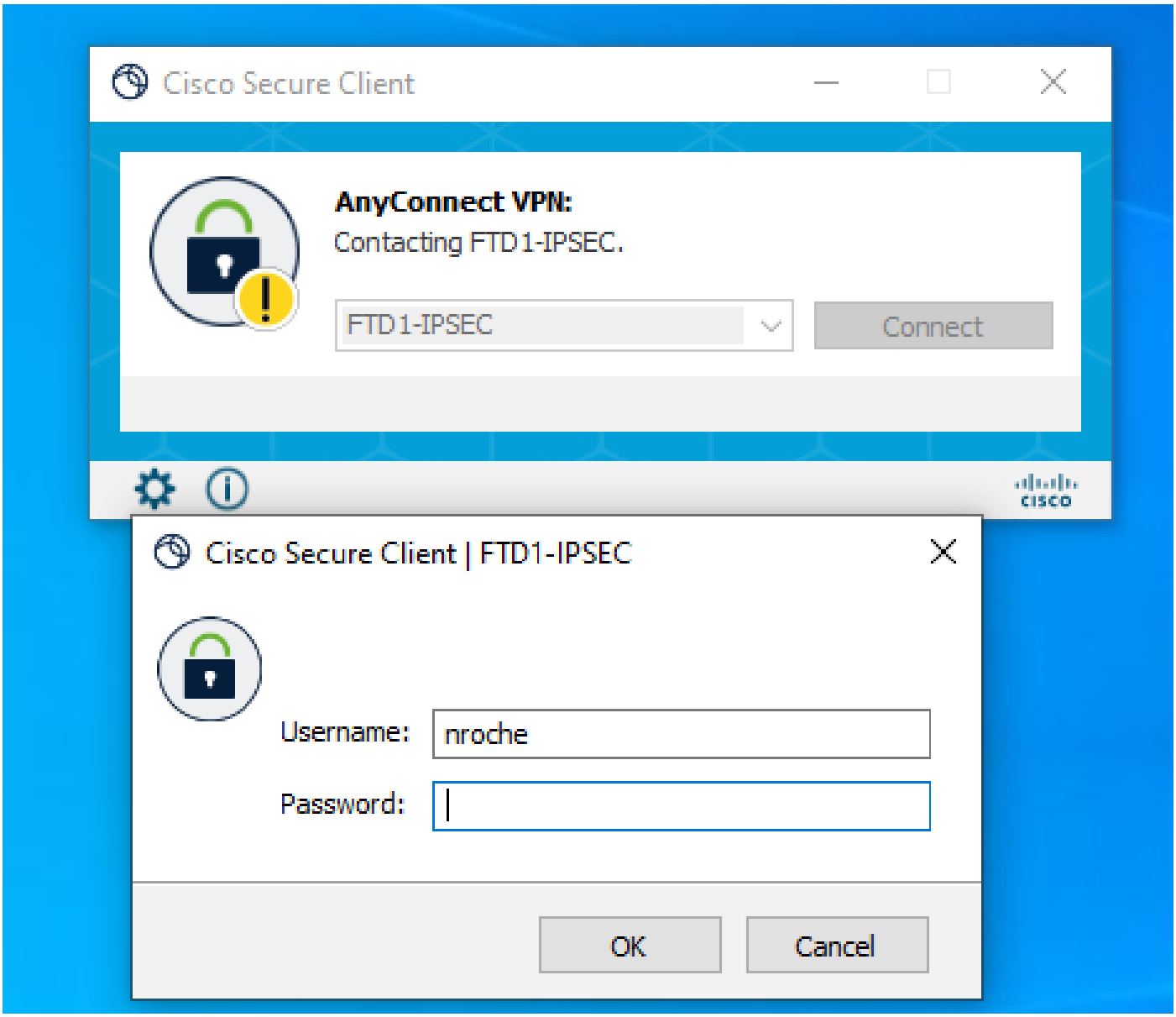


قم بتحرير ملف تعريف XML حتى يكون البروتوكول الأساسي IPsec، وتطابق مجموعة المستخدمين اسم ملف تعريف الاتصال.



تحذير: يلزم اتصال SSL لدفع توصيفات XML إلى العميل من جدار الحماية. عند إستخدام IKEV2-IPsec فقط، يجب دفع توصيفات XML إلى العملاء بطريقة خارج النطاق.

بمجرد دفع ملف تعريف XML إلى العميل، يستخدم Secure Client مجموعة المستخدمين من ملف تعريف XML للاتصال بملف تعريف اتصال IKEv2-IPsec.



طريقة عرض واجهة مستخدم العميل الآمنة لمحاولة اتصال الشبكة الفرعية IPsec-IKEv2.

أمثلة تكوين ASA

تعطيل مصادقة AAA في توصيفات توصيل DefaultWebVPNGroup و DefaultRagGroup

أدخل قسم سمات WebVPN لمجموعة النفق DefaultWEBvpngGroup وحدد المصادقة على أنها مستندة إلى شهادة. كرر هذه العملية لـ DefaultRAGgroup. يجبر المستخدمون الذين يحتوون على توصيفات التوصيل الافتراضية هذه على تقديم شهادة للمصادقة ولا تتاح لهم فرصة إدخال مسوغات اسم المستخدم وكلمة المرور.

```
ASA# configure terminal
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# authentication certificate

ASA# configure terminal
```

```
ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes
ASA(config-tunnel-webvpn)# authentication certificate
```

تعطيل Hostscan / وضع جدار الحماية الآمن على DefaultWEBvpngGroup و DefaultRAGgroup (إختياري)

لا يكون هذا ضروريا إلا إذا كان لديك Hostscan / Secure Firewall Posture (وضع جدار الحماية الآمن) في بيئتك. تمنع هذه الخطوة المهاجمين من زيادة إستخدام الموارد على جدار الحماية بسبب عملية المسح الضوئي لنقطة النهاية. أدخل قسم سمات webVPN ل DefaultWEBvpngGroup و DefaultRAGgroup وقم بتطبيق بدون-csd لتعطيل الاتصال وتعرف فاتورة المسح الضوئي لنقطة النهاية.

```
ASA# configure terminal
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# without-csd

ASA# configure terminal
ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes
ASA(config-tunnel-webvpn)# without-csd
```

تعطيل أسماء المجموعة المستعارة وتمكين عناوين URL الخاصة بالمجموعة

أدخل مجموعة مستخدمي مجموعة (مجموعات) النفق المتصلين بها. في حالة وجود اسم مستعار للمجموعة، قم بتعطيله أو إزالته. في هذا المثال، تم تعطيله. بمجرد اكتمال ذلك، قم بإنشاء عنوان URL للمجموعة باستخدام FQDN أو عنوان IP الخاص بواجهة إنهاء RAPN. يجب أن يكون الاسم الموجود في نهاية عنوان URL للمجموعة غامضا. تجنب القيم المشتركة مثل VPN، و AAA، و RADIUS، و LDAP حيث أن هذه تسهل على المهاجمين تخمين عنوان URL الكامل إذا حصلوا على FQDN. بدلا من ذلك، استخدم أسماء ذات أهمية داخلية تساعدك على تحديد مجموعة الأنفاق.

```
ASA# configure terminal
ASA(config)# tunnel-group NAME webvpn-attributes
ASA(config-tunnel-webvpn)# group-alias NAME disable
ASA(config-tunnel-webvpn)# group-url https://FQDN/name enable
```

تعيين الشهادة

من وضع التكوين العام، قم بإنشاء خريطة شهادات وقم بتعيين اسم ورقم تسلسلي لها. ثم حدد قاعدة يجب على المستخدمين مطابقتها لاستخدام التعيين. في هذا المثال، يجب على المستخدمين مطابقة معايير قيمة الاسم المشتركة التي تساوي "customValue". بعد ذلك، أدخل تكوين WebVPN وطبق خريطة الشهادة على مجموعة النفق المطلوبة. ما إن يتم،

ي DefaultWEBVPNGroup و يجعل هذا النفق-group الافتراضي للمستخدمين الذين
يخفقون في تعيين الشهادة. في حالة فشل المستخدمين في التعيين، يتم توجيههم
إلى DefaultWEBVPNGroup. بينما يتم تكوين DefaultWEBvpngGroup بمصادقة الشهادة، ال
يتوفر للمستخدمين خيار تمرير بيانات اعتماد اسم المستخدم وأ كلمة المرور.

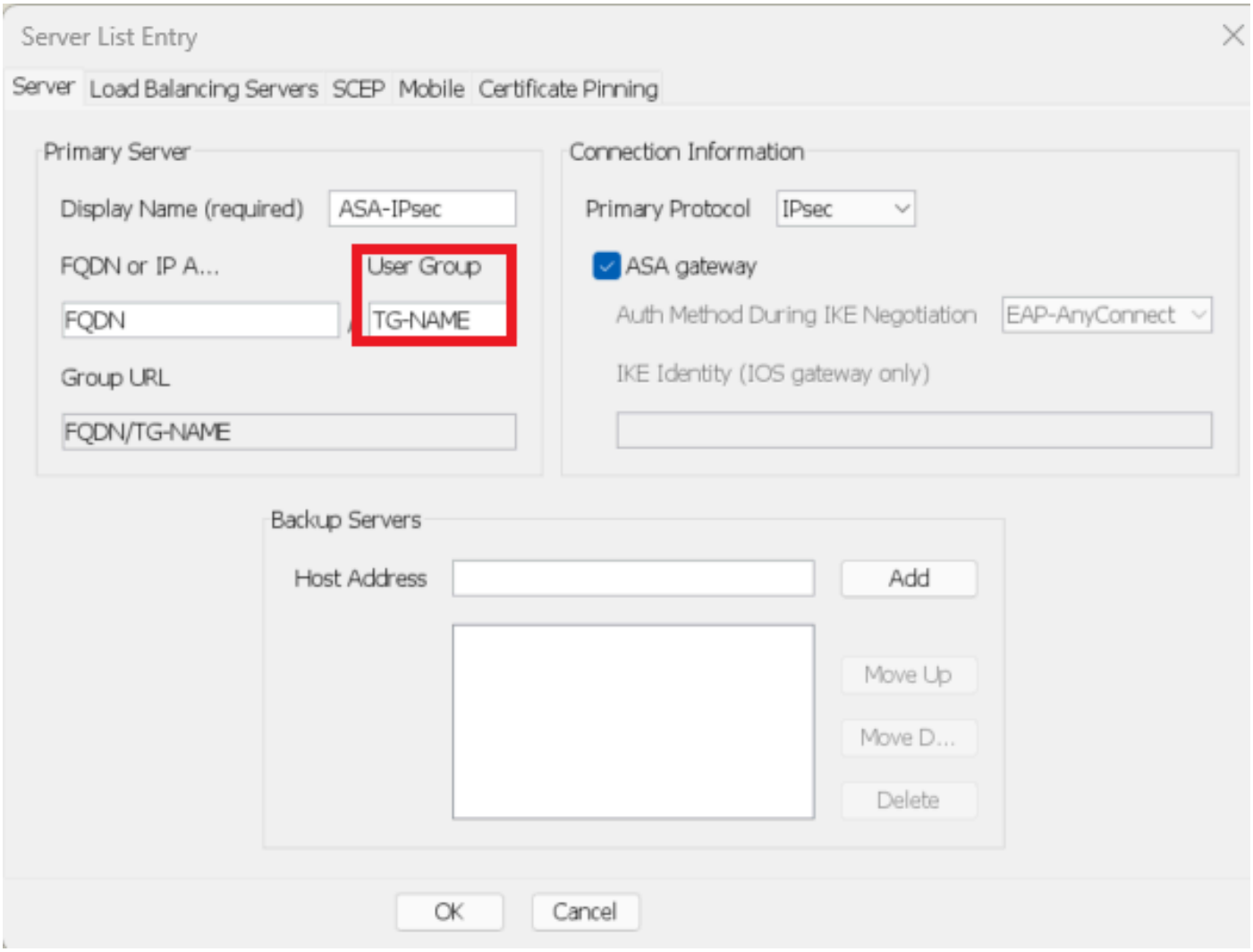
```
ASA(config)# crypto ca certificate map NAME 1
ASA(config-ca-cert-map)# subject-name attr cn eq customvalue

ASA(config)# webvpn
ASA(config-webvpn)# certificate-group-map NAME 1 TG-NAME

ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# tunnel-group-map default-group
```

IPsec-IKEv2

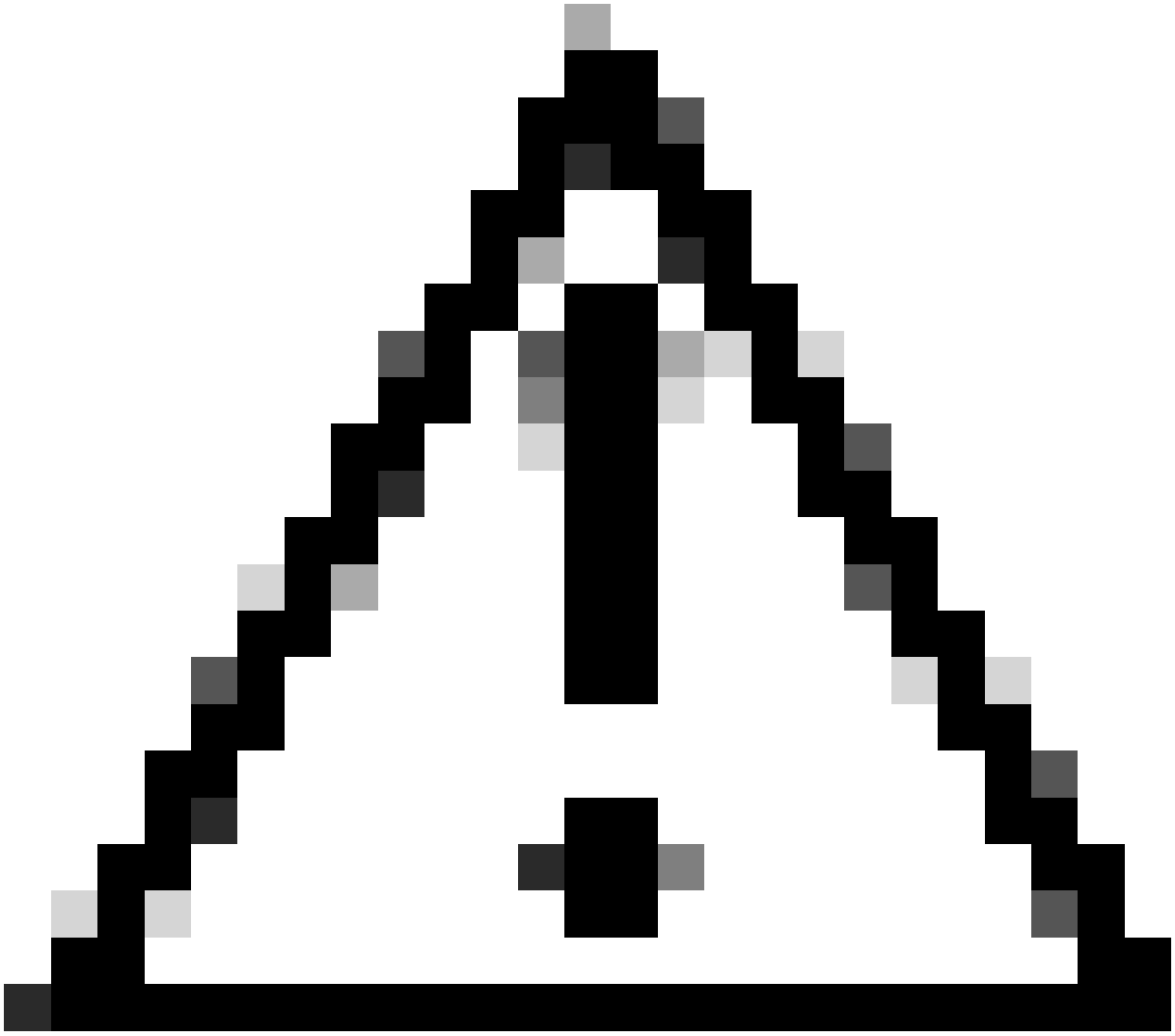
من وضع التكوين العام، يمكنك تحرير نهج مجموعة موجود أو إنشاء نهج مجموعة جديد وإدخال
السمات الخاصة بنهج المجموعة هذا. بمجرد أن تكون في قسم السمات، قم بتمكين IKEv2
كبروتوكول نفق VPN الوحيد. تأكد من ربط نهج المجموعة هذا بمجموعة أنفاق سيتم
إستخدامها اتصالات VPN للوصول عن بعد إلى IPsec-IKEV2. على غرار خطوات FMC، يجب
عليك تحرير ملف تعريف XML عبر محرر ملف تعريف VPN أو محرر ملف تعريف ASA وتغيير
حقل مجموعة المستخدمين ليطابق اسم مجموعة النفق على ASA، وتغيير البروتوكول إلى
IPsec.

```
ASA# configure terminal
ASA(config)# group-policy GP-NAME internal
ASA(config)# group-policy GP-NAME attributes
ASA(config-group-policy)# vpn-tunnel-protocol ikev2

ASA(config)# tunnel-group TG-NAME general-attributes
ASA(config-tunnel-general)# default-group-policy GP-NAME
```

في محرر ملف تعريف VPN، أو محرر ملف تعريف ASA، انتقل إلى علامة التبويب قائمة
الخوادم. يجب أن يكون اسم مجموعة المستخدمين مطابقا تماما لاسم ملف تعريف الاتصال
الموجود على جدار الحماية. تم تكوين البروتوكول الأساسي ك IPsec. يظهر اسم العرض
للمستخدم في واجهة مستخدم العميل الآمن عند إنشاء اتصال بملف تعريف الاتصال هذا.



قم بتحرير ملف تعريف XML حتى يكون اسم البروتوكول الأساسي هو IPsec وتطابق اسم مجموعة المستخدمين اسم مجموعة النفق الخاص ب ASA لاتصالات IPsec-IKEv2 RAPN.



تحذير: يلزم اتصال SSL لدفع توصيفات XML إلى العميل من جدار الحماية. عند إستخدام IKEV2-IPsec فقط، يجب دفع توصيفات XML إلى العملاء بطريقة خارج النطاق.

القرار

في الخلاصة، يتمثل الغرض من ممارسات التعزيز الواردة في هذا المستند في تعيين المستخدمين الشرعيين إلى ملفات تعريف اتصال مخصصة بينما يتم إجبار المهاجمين على DefaultWEBvpngGroup و DefaultRAGgroup. في تكوين محسن، ال يحتوي ملف تعريف التوصيل الافتراضي على أي تكوين خادم AAA مخصص للشريك القانوني. بالإضافة إلى ذلك، تمنع إزالة أسماء المجموعات المهاجمين من التعرف بسهولة على ملفات تعريف التوصيل المخصصة عن طريق إزالة إمكانية الرؤية المنسدلة عند التنقل إلى FQDN أو عنوان IP العام لجدار الحماية.

معلومات ذات صلة

[الدعم الفني والتنزيلات من Cisco]

[هجمات ذات كلمة المرور]

[الثغرات الأمنية للوصول غير المصرح به سبتمبر 2023]

[أدلة تكوين ASA]

[أدلة تكوين FMC / 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).