Implémenter des mesures de renforcement pour le VPN AnyConnect Secure Client

Table des matières

Introduction

Ce document décrit comment améliorer la sécurité de votre implémentation VPN d'accès à distance.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

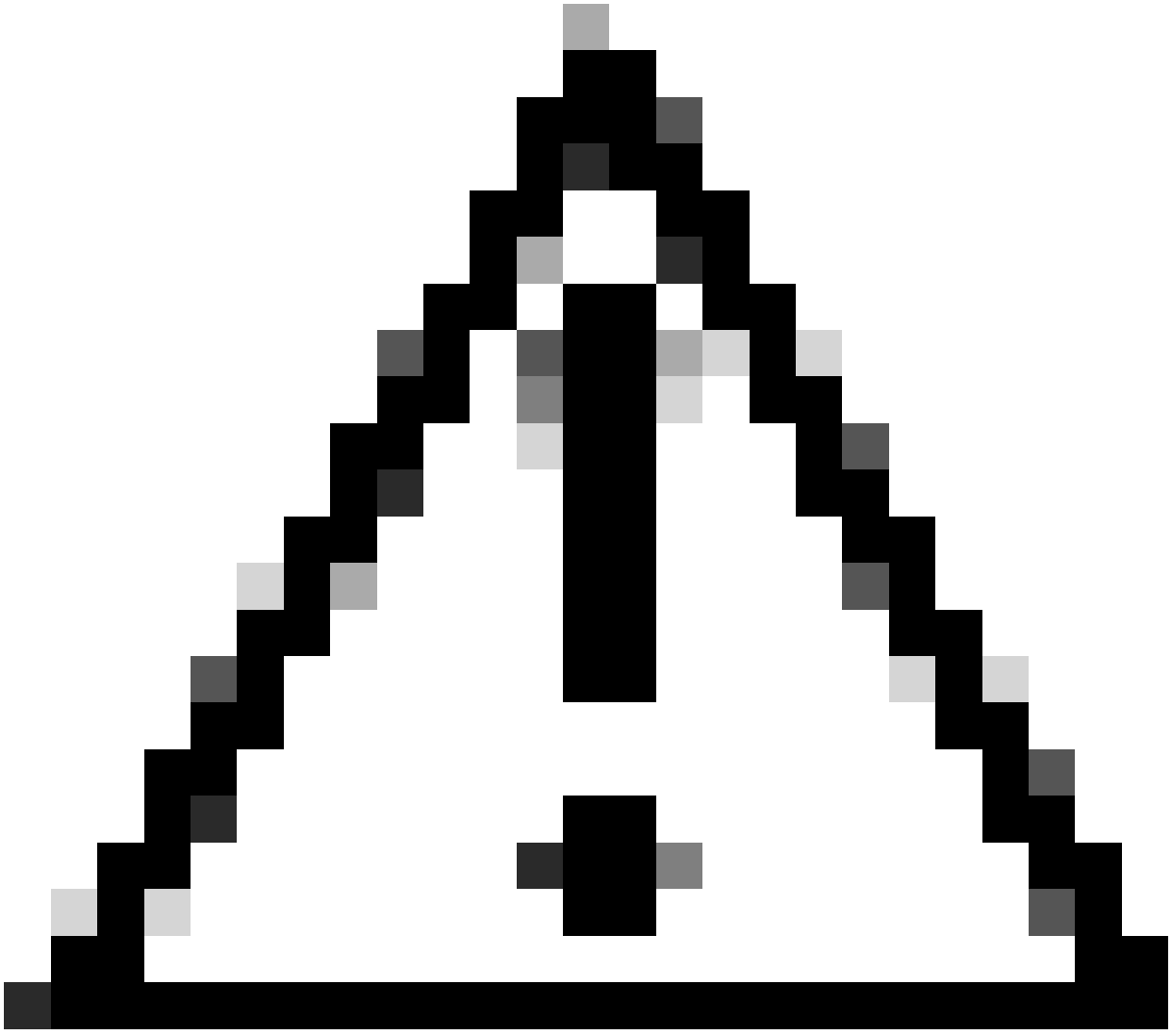
- VPN AnyConnect Cisco Secure Client.
- Configuration de l'accès à distance ASA/FTD.

Composants utilisés

Le guide des meilleures pratiques est basé sur les versions matérielles et logicielles suivantes :

- Cisco ASA 9.x
- Firepower Threat Defense 7.x / FMC 7.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.



Attention : ce document ne contient pas d'étapes pour Firepower Device Manager (FDM). FDM prend uniquement en charge la modification de la méthode d'authentification sur DefaultWEBVPNGroup. Utilisez des listes de contrôle d'accès du plan de contrôle ou un port personnalisé dans la section « Paramètres globaux » du VPN d'accès à distance

---

dans l'interface utilisateur de FDM. Veuillez contacter le centre d'assistance technique Cisco (TAC) pour obtenir de l'aide si nécessaire.

Informations générales

L'objectif de ce document est de garantir que la configuration VPN AnyConnect du client sécurisé Cisco respecte les meilleures pratiques de sécurité dans un monde moderne où les attaques de cybersécurité sont courantes.

Les attaques de force brutale impliquent généralement des tentatives répétées d'accès à une ressource à l'aide de combinaisons de nom d'utilisateur et de mot de passe. Les pirates tentent d'utiliser leur navigateur Internet, l'interface utilisateur du client sécurisé ou d'autres outils pour entrer plusieurs noms d'utilisateur et mots de passe en espérant qu'ils correspondent à une combinaison légitime dans une base de données AAA. Lorsque vous utilisez AAA pour l'authentification, nous attendons de l'utilisateur final qu'il entre son nom d'utilisateur et son mot de passe, car cela est nécessaire pour établir la connexion. En même temps, nous ne vérifions pas qui est l'utilisateur tant qu'il n'a pas saisi ses informations d'identification. Par nature, cela permet aux pirates de tirer parti des scénarios suivants :

1. Noms de domaine complets exposés pour le pare-feu sécurisé Cisco (en particulier lorsque vous utilisez un groupe d'alias dans le profil de connexion) :
    - Si le pirate détecte le nom de domaine complet de votre pare-feu VPN, il a alors la possibilité de sélectionner le groupe de tunnels à l'aide de l'alias de groupe dans lequel il veut lancer l'attaque en force brute.

2. Profil de connexion par défaut configuré avec AAA ou base de données locale :
    - Si le pirate trouve le nom de domaine complet du pare-feu VPN, il peut tenter d'attaquer en force le serveur AAA ou la base de données locale. Cela se produit parce que la connexion au FQDN atterrit sur le profil de connexion par défaut, même si aucun alias de groupe n'est spécifié.

3. Épuisement des ressources sur le pare-feu ou sur les serveurs AAA :
    - Les pirates peuvent submerger les serveurs AAA ou les ressources du pare-feu en envoyant de grandes quantités de demandes d'authentification et en créant une condition de déni de service (DoS).

Concepts

Alias de groupe :

- Autre nom par lequel le pare-feu peut faire référence à un profil de connexion. Après avoir initié une connexion au pare-feu, ces noms apparaissent dans un menu déroulant de l'interface utilisateur Secure Client pour que les utilisateurs puissent les sélectionner. La suppression des alias de groupe supprime la fonctionnalité de liste déroulante dans

l'interface utilisateur du client sécurisé.

URL de groupe :

- URL pouvant être liée à un profil de connexion de sorte que les connexions entrantes soient directement mappées à un profil de connexion souhaité. Il n'y a pas de fonctionnalité de liste déroulante, car les utilisateurs peuvent entrer l'URL complète dans l'interface utilisateur du client sécurisé, ou l'URL peut être intégrée avec un « nom d'affichage » dans le profil XML pour masquer l'URL de l'utilisateur.

La différence ici est que lorsque des groupes d'alias sont implémentés, un utilisateur lance une connexion to vpn_gateway.example.com et se voit présenter des alias pour les sélectionner afin de les diriger vers un profil de connexion. Avec les URL de groupe, un utilisateur établit une connexion à vpn_gateway.example.com/example_group et les dirige directement vers le profil de connexion sans avoir besoin d'un menu déroulant.

Pratiques de sécurisation renforcée des clients sur Cisco Secure Firewall :

Ces méthodes reposent sur le mappage d'utilisateurs légitimes à des groupes de tunnels/profils de connexion appropriés tandis que des utilisateurs potentiellement malveillants sont envoyés à un groupe de tunnels de déroutement que nous configurons pour ne pas autoriser les combinaisons de nom d'utilisateur et de mot de passe. Bien que toutes les combinaisons ne doivent pas être implémentées, la désactivation des alias de groupe et la modification de la méthode d'authentification de DefaultWEBVPNGroup et DefaultRAGroup sont nécessaires pour que les recommandations fonctionnent efficacement.

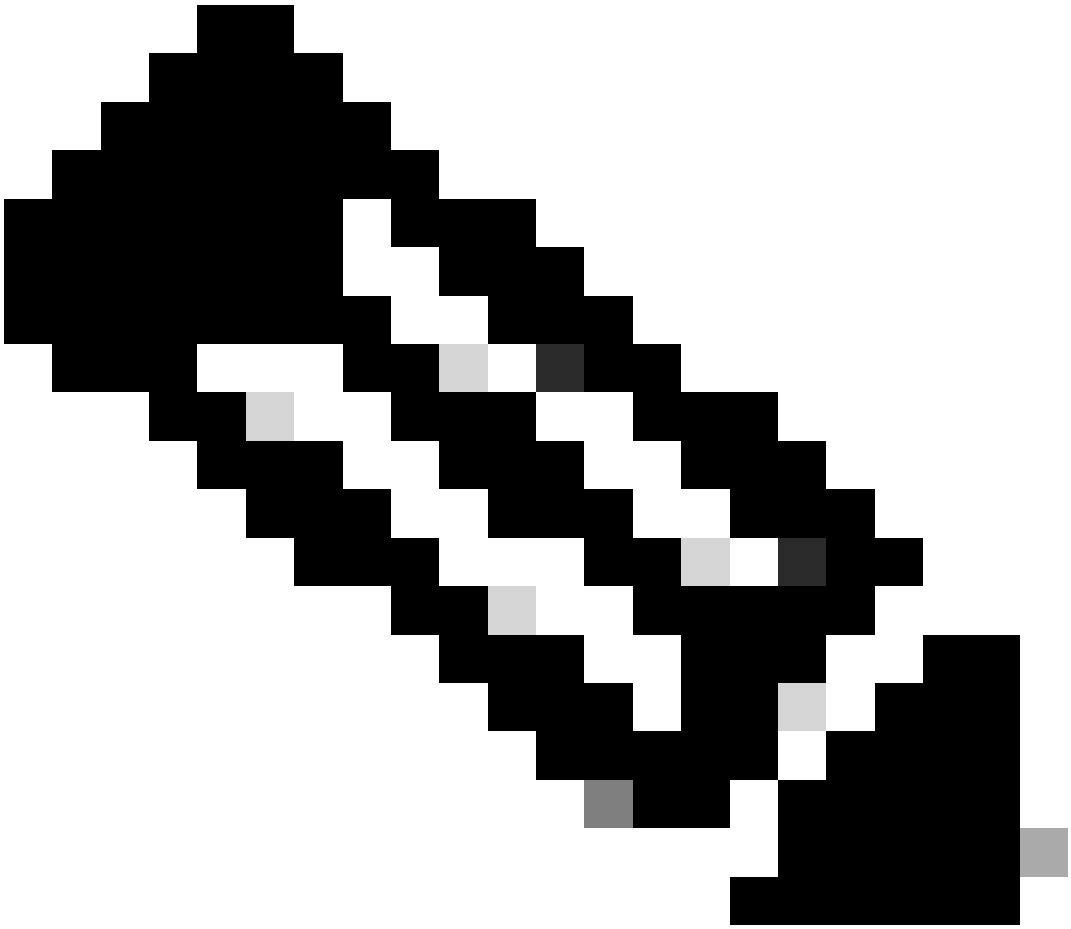
- Désactivez les alias de groupe et n'utilisez que group-url dans la configuration du profil de connexion, ce qui vous permet d'avoir un nom de domaine complet spécifique qui ne sera pas facile à détecter et à sélectionner pour un attaquant puisque seuls les clients avec le nom de domaine complet approprié sont en mesure d'initier la connexion. Par exemple, vpn_gateway.example.com/example_group est plus difficile à détecter pour un pirate que vpn_gateway.example.com.

- Désactivez l'authentification AAA dans DefaultWEBVPNGroup et DefaultRAGroup et configurez l'authentification de certificat, ce qui évite une force brute possible contre la base de données locale ou le serveur AAA. Dans ce scénario, le pirate rencontrerait des erreurs immédiates lors de sa tentative de connexion. Il n'existe aucun champ de nom d'utilisateur ou de mot de passe car l'authentification est basée sur des certificats, ce qui permet d'arrêter les tentatives en force. Une autre option consiste à créer un serveur AAA sans configuration de prise en charge afin de créer un goulot d'étranglement pour les requêtes malveillantes.

- Utilisez le mappage de certificat pour le profil de connexion. Cela permet de mapper les connexions entrantes à des profils de connexion spécifiques en fonction des attributs reçus

des certificats sur le périphérique client. Les utilisateurs qui possèdent les certificats appropriés sont mappés correctement, tandis que les pirates qui ne répondent pas aux critères de mappage sont envoyés au DefaultWEBVPNGroup.

- L'utilisation d'IKEv2-IPSec à la place de SSL amène les groupes de tunnels à s'appuyer sur un mappage de groupe d'utilisateurs spécifique dans le profil XML. Sans ce code XML sur l'ordinateur de l'utilisateur final, les utilisateurs sont automatiquement envoyés au groupe de tunnels par défaut.



Remarque : pour plus d'informations sur la fonctionnalité group-alias, consultez le Guide de configuration VPN ASA et observez le « Tableau 1. Attributs de profil de connexion pour VPN SSL'.

Identifier les attaques en utilisant les ID de journalisation et Syslog

Les attaques brutales représentent la méthode prédominante de compromission des VPN d'accès à distance, exploitant des mots de passe faibles pour obtenir une entrée non autorisée. Il est essentiel de savoir reconnaître les signes d'une attaque en exploitant l'utilisation de la journalisation et en évaluant les syslogs. Les ID Syslog courants qui peuvent indiquer une attaque en cas de volume anormal sont les suivants :

%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 =

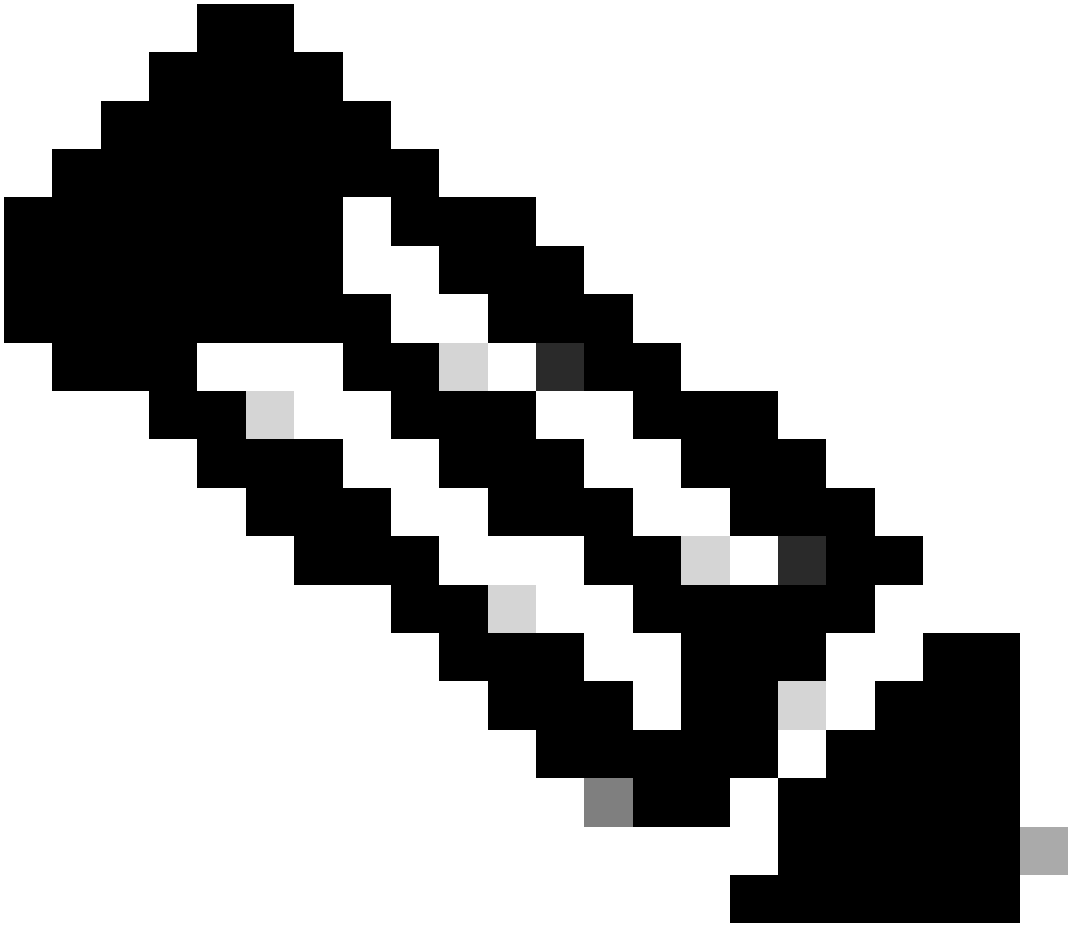
%ASA-6-716039

<#root>

%ASA-6-716039

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

Le nom d'utilisateur est toujours masqué jusqu'à ce que la commande no logging hide username soit configurée sur ASA.



Remarque : Remarque : ceci permet de savoir si des utilisateurs valides sont générés ou connus par des adresses IP incorrectes. Cependant, soyez prudent car les noms d'utilisateurs sont visibles dans les journaux.

Journalisation Cisco ASA :

Guide de l'utilisateur de Secure ASA Firewall
Chapitre Journalisation du Guide de configuration de l'interface de ligne de commande des opérations générales de Cisco Secure Firewall ASA

Journalisation FTD Cisco :

Configurez la connexion sur Cisco FTD à l'aide de Cisco FMC

Section Configure Syslog du chapitre Platform Settings du Guide de configuration des périphériques de Cisco Secure Firewall Management Center
Configuration et vérification de Syslog dans le Gestionnaire de périphériques Firepower

Section Configuration des paramètres de journalisation système du chapitre Paramètres système du Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager

Vérification des attaques

Pour vérifier, connectez-vous à l'interface de ligne de commande (CLI) ASA ou FTD, exécutez la commande show aaa-server et recherchez un nombre inhabituel de demandes d'authentification tentées et rejetées vers l'un des serveurs AAA configurés :

<#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

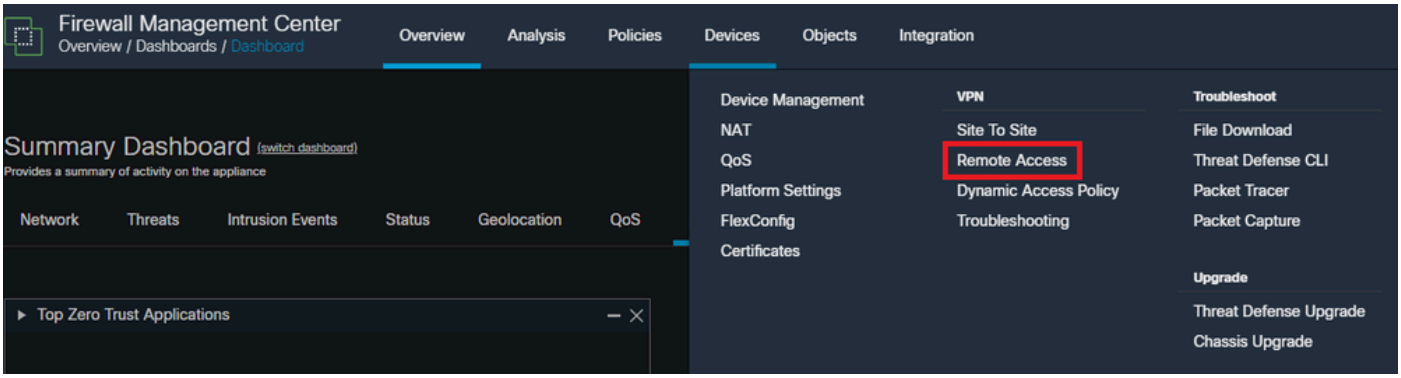
```
Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
Number of 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
```

Exemples de configuration FMC

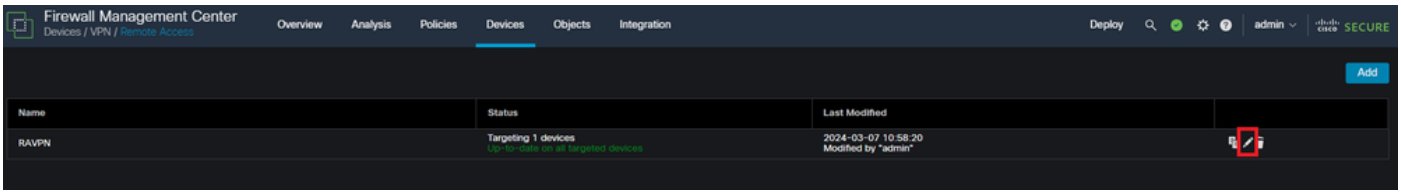
Désactiver l'authentification AAA dans les profils de connexion DefaultWEBVPNGroup et DefaultRAGroup

Accédez à Périphériques > Accès à distance.



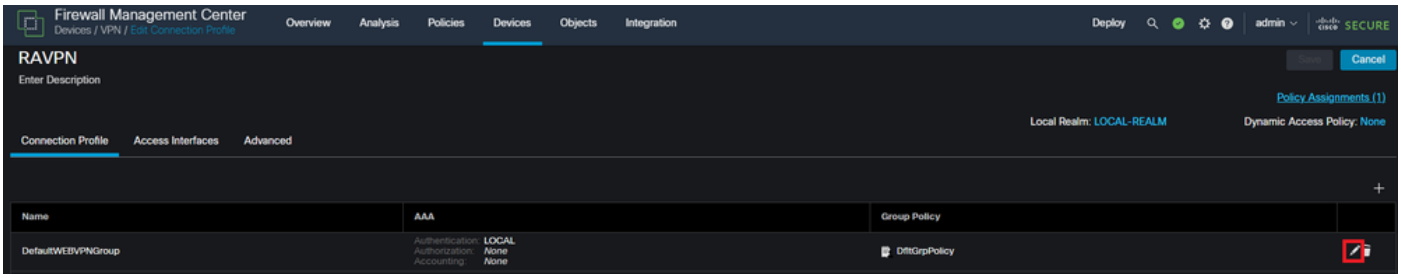
Affiche la navigation dans l'interface utilisateur graphique FMC pour accéder à la configuration de la stratégie VPN d'accès à distance.

Modifiez la stratégie VPN d'accès à distance existante et créez un profil de connexion nommé « DefaultRAGroup »



Indique comment modifier la stratégie VPN d'accès à distance dans l'interface utilisateur FMC.

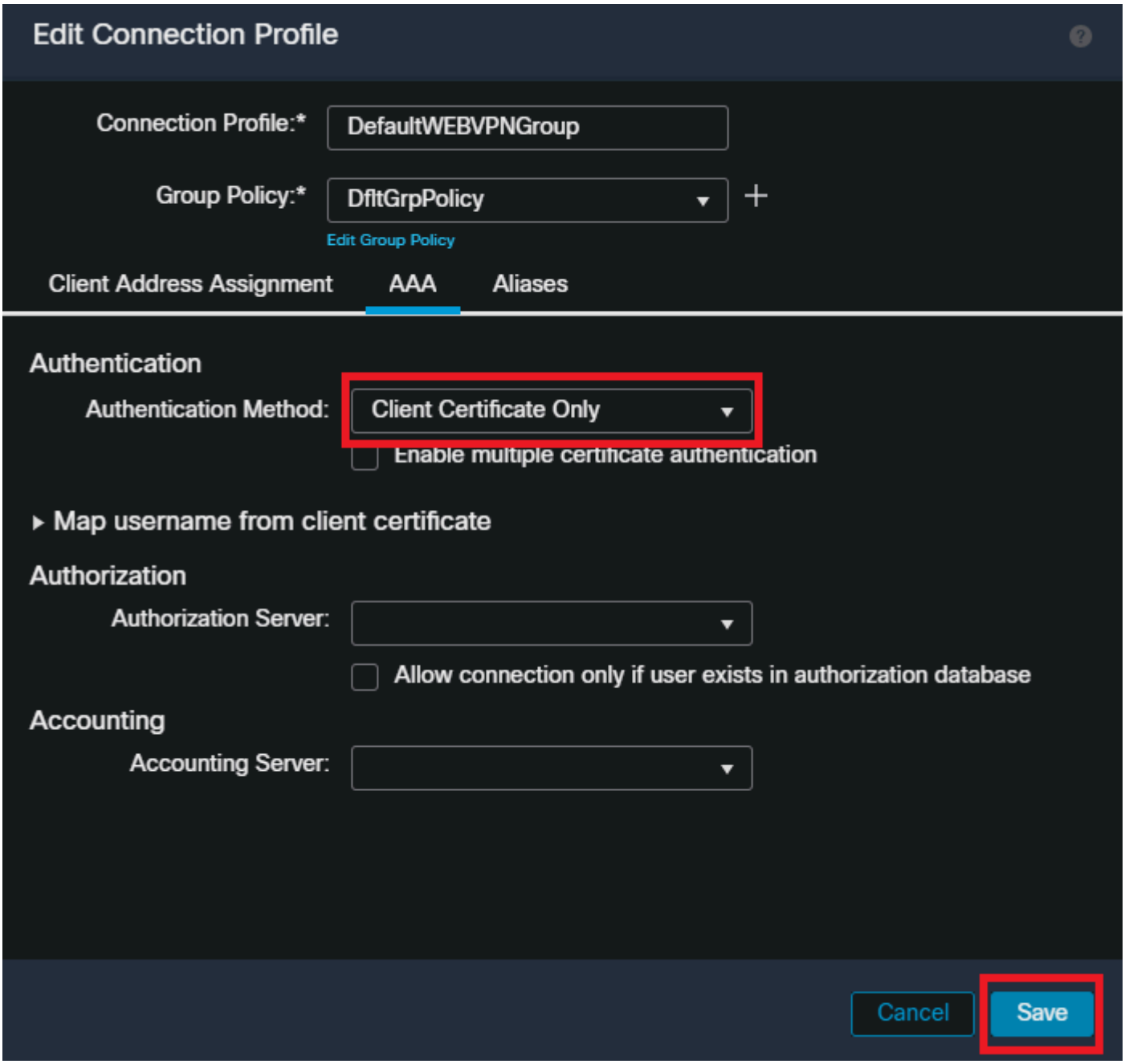
Modifier les profils de connexion nommés 'DefaultWEBVPNGroup' et 'DefaultRAGroup'



Indique comment modifier le groupeWEBVPNGroupParDéfaut dans l'interface utilisateur FMC.

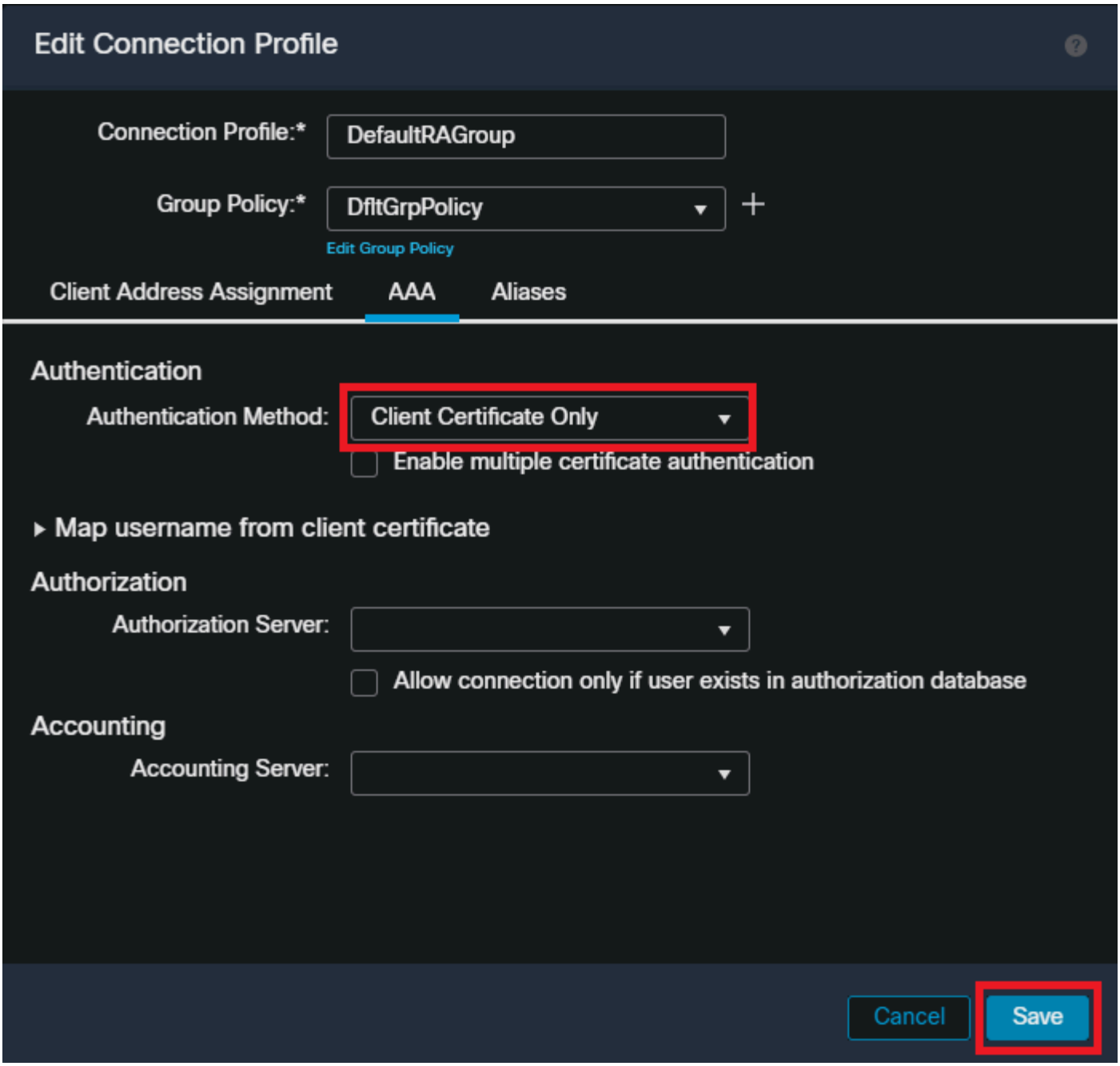
Accédez à l'onglet AAA et sélectionnez la liste déroulante Authentication Method. Sélectionnez

'Client Certificate Only' et sélectionnez Save.

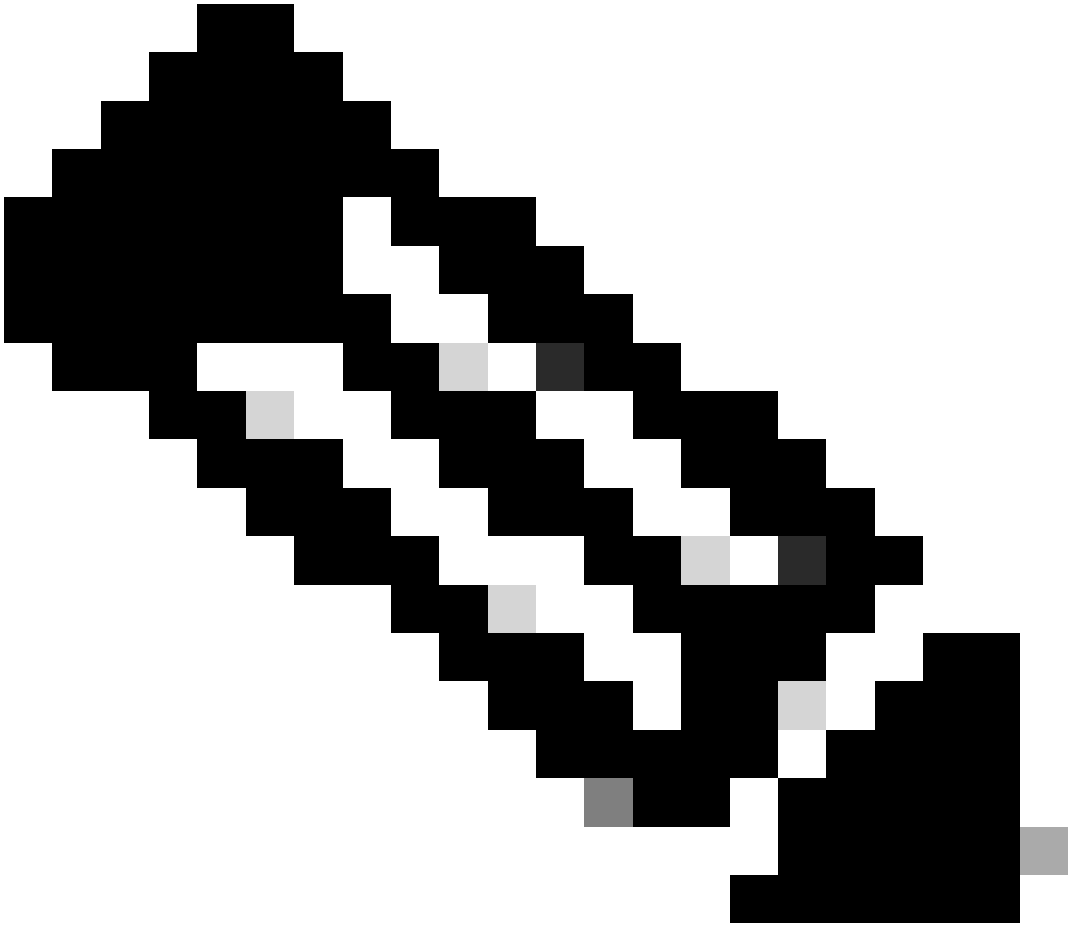


Changement de la méthode d'authentification en certificat client uniquement pour DefaultWEBVPNGroup dans l'interface utilisateur FMC.

Modifiez le DefaultRAGroup et accédez à l'onglet AAA et sélectionnez la liste déroulante Authentication Method. Sélectionnez 'Client Certificate Only' et sélectionnez Save.



Modification de la méthode d'authentification en certificat client uniquement pour le DefaultRAGroup dans l'interface utilisateur FMC.

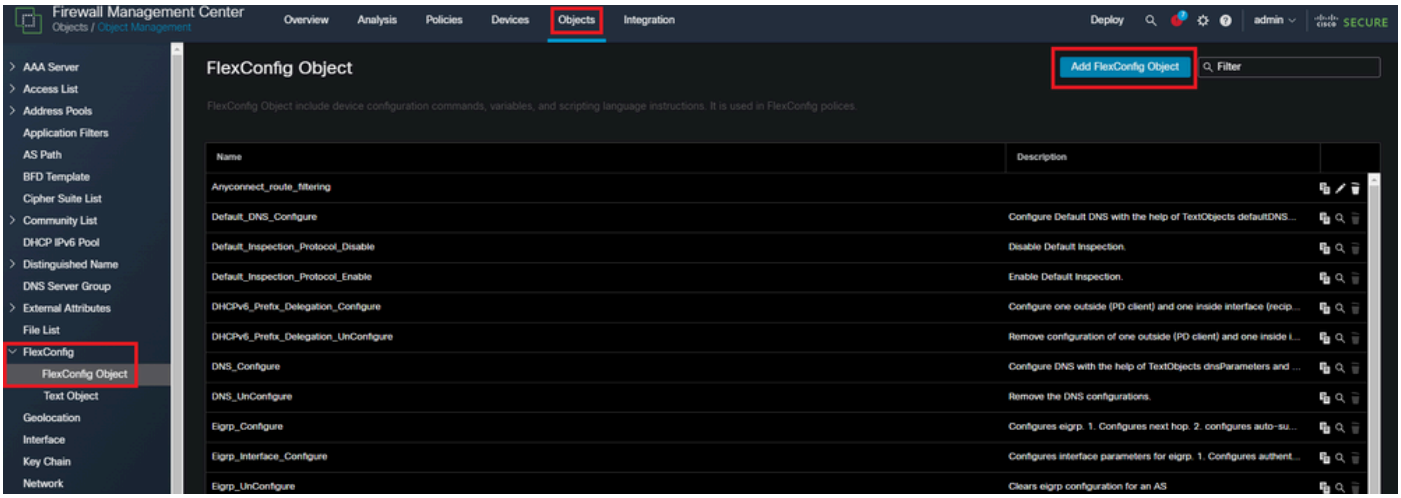


Remarque : la méthode d'authentification peut également être un serveur AAA de type « sinkhole ». Si cette méthode est utilisée, la configuration du serveur AAA est fausse et ne traite aucune requête. Un pool VPN doit également être défini dans l'onglet « Client Address Assignment » pour enregistrer les modifications.

Désactiver la position de Hostscan / Secure Firewall sur DefaultWEBVPNGroup et DefaultRAGroup (facultatif)

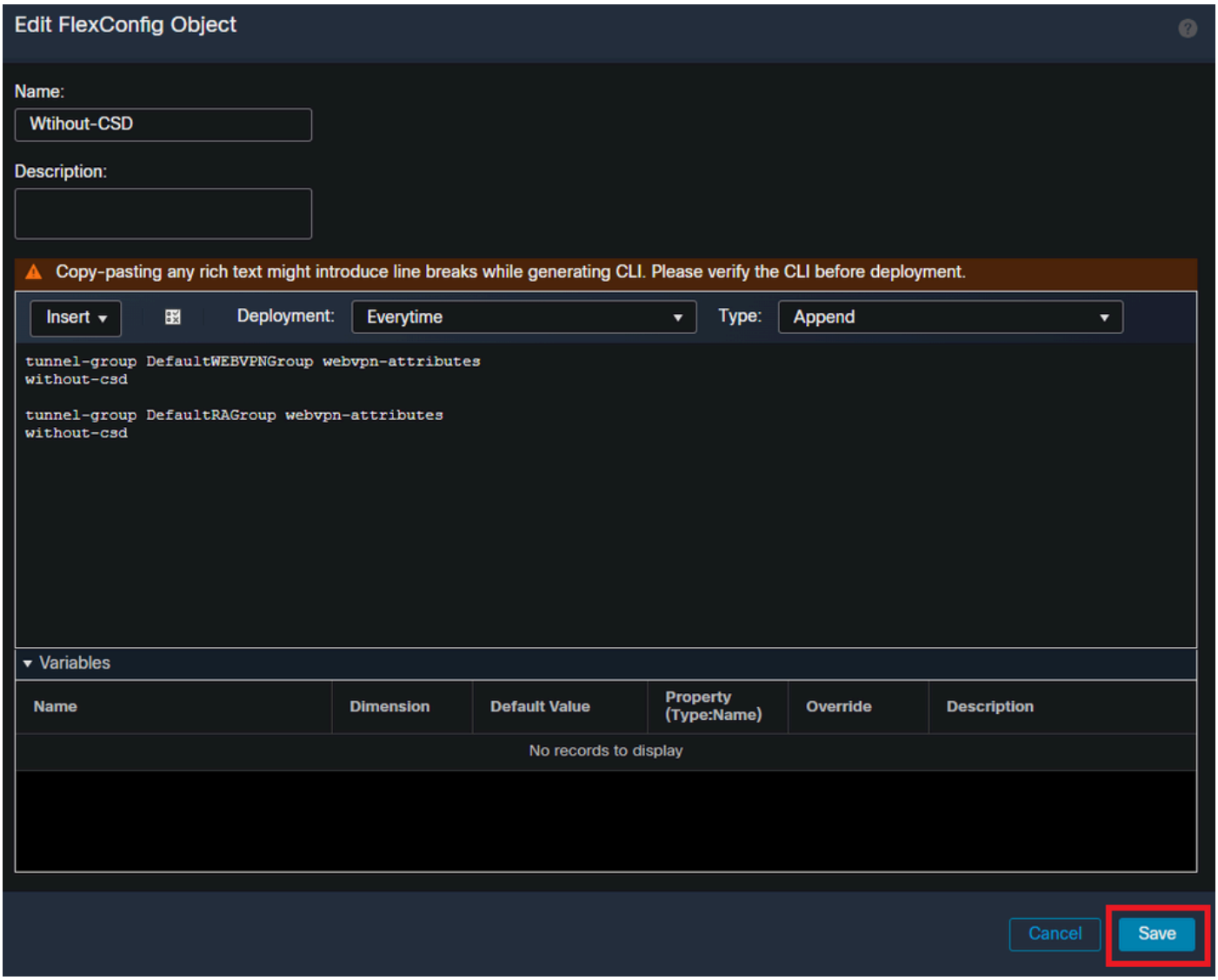
Ceci n'est nécessaire que si vous avez Hostscan / Secure Firewall Posture dans votre environnement. Cette étape empêche les pirates d'augmenter l'utilisation des ressources sur le pare-feu causée par le processus d'analyse des terminaux. Dans le FMC, ceci est réalisé en créant un objet FlexConfig avec la commande without-csd pour désactiver la fonctionnalité d'analyse de point de terminaison.

Accédez à Objets > Gestion des objets > Objet FlexConfig > Ajouter un objet FlexConfig.



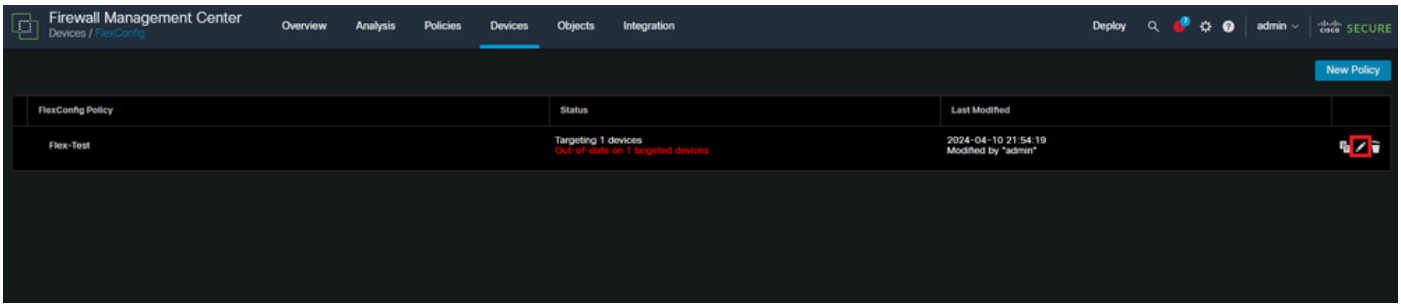
Navigation dans l'interface utilisateur FMC pour créer un objet FlexConfig.

Nommez l'objet FlexConfig, définissez le déploiement sur Everytime avec le type Append. Ensuite, entrez la syntaxe exactement comme indiqué et enregistrez l'objet.



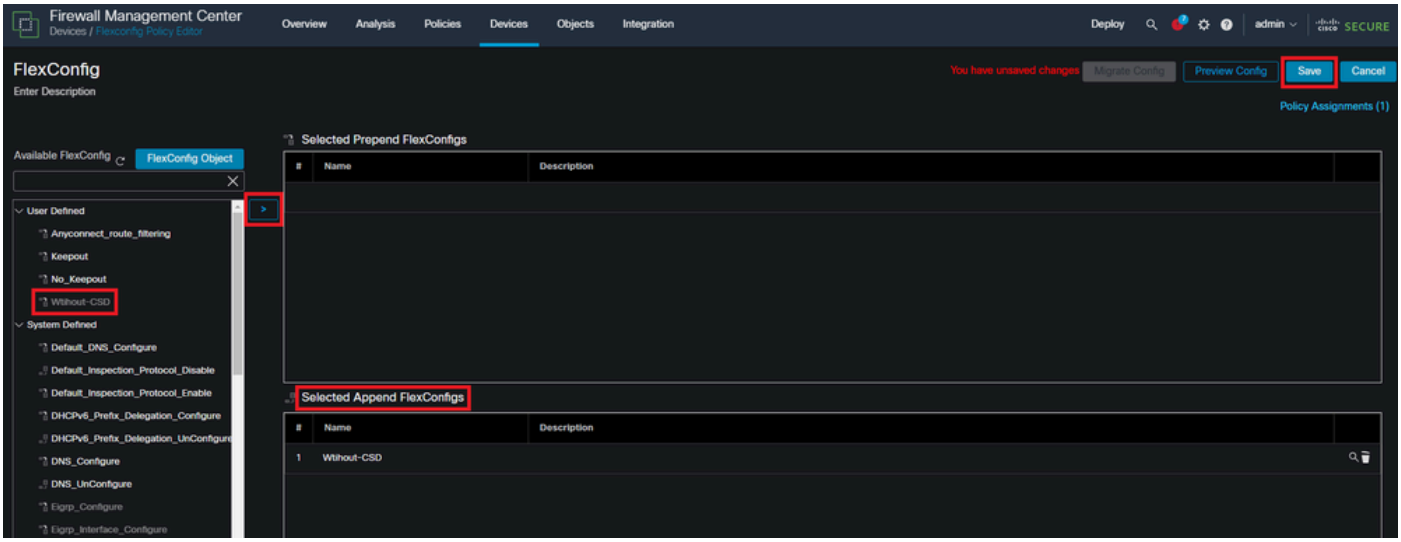
Création d'un objet FlexConfig avec « without-csd »

Accédez à Devices > FlexConfig, puis cliquez sur le crayon pour modifier la politique FlexConfig.



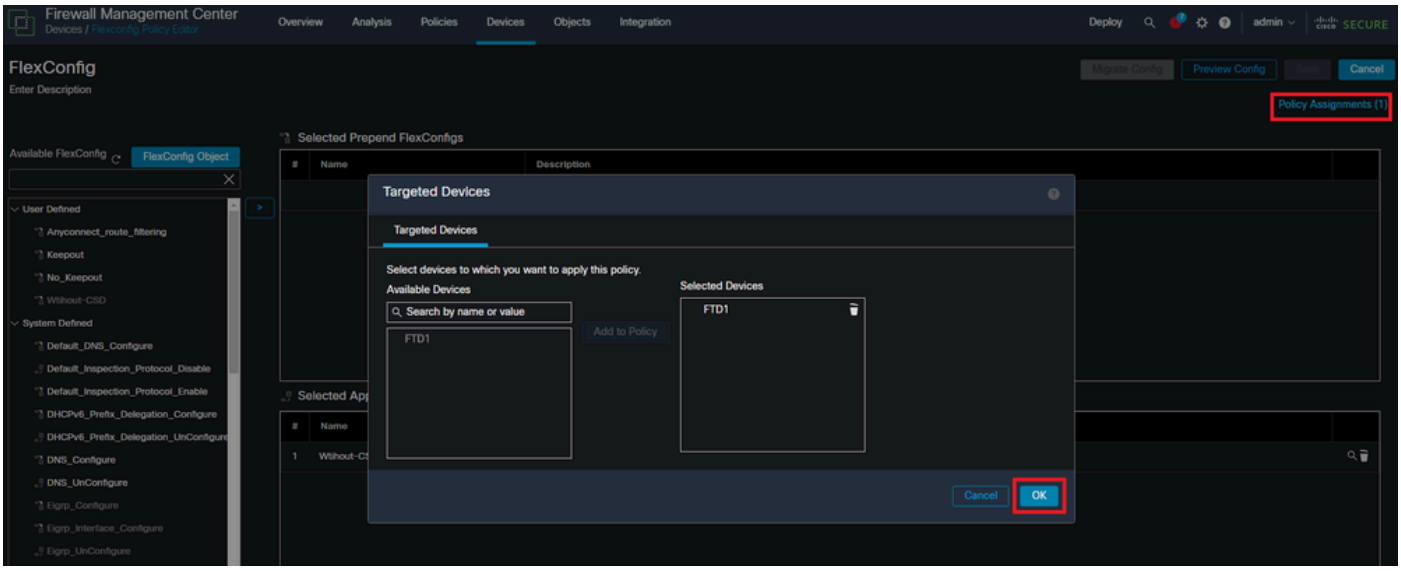
Modification de la stratégie FlexConfig dans le FMC.

Localisez l'objet que vous avez créé à partir de la section Défini par l'utilisateur. Sélectionnez ensuite la flèche pour l'ajouter aux FlexConfigs d'ajout sélectionnés. Enfin, sélectionnez Save pour enregistrer la stratégie FlexConfig.



Associez l'objet FlexConfig à la stratégie FlexConfig.

Sélectionnez Policy Assignments et choisissez le FTD auquel vous souhaitez appliquer cette stratégie FlexConfig, puis sélectionnez OK. Sélectionnez à nouveau Save s'il s'agit d'une nouvelle affectation FlexConfig et déployez les modifications. Une fois déployé, vérifiez



Attribuez la politique FlexConfig à un périphérique FirePOWER.

Entrez la CLI FTD et émettez la commande show run tunnel-group pour DefaultWEBVPNGroup et DefaultRAGroup. Vérifiez que without-csd est maintenant présent dans la configuration.

<#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

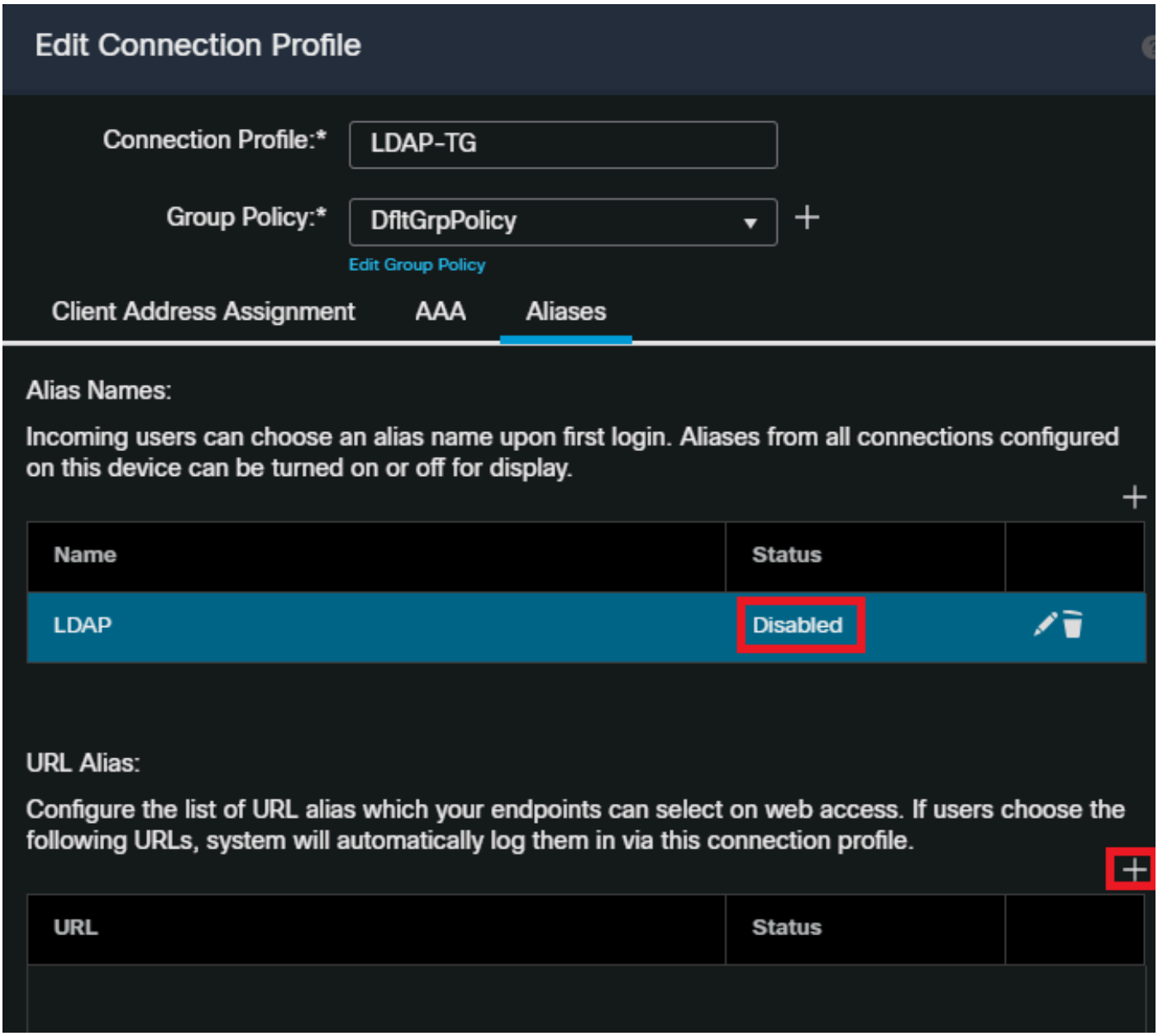
```
tunnel-group DefaultWEBVPNGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultWEBVPNGroup webvpn-attributes
authentication certificate
```

without-csd

Désactiver les alias de groupe et activer les URL de groupe

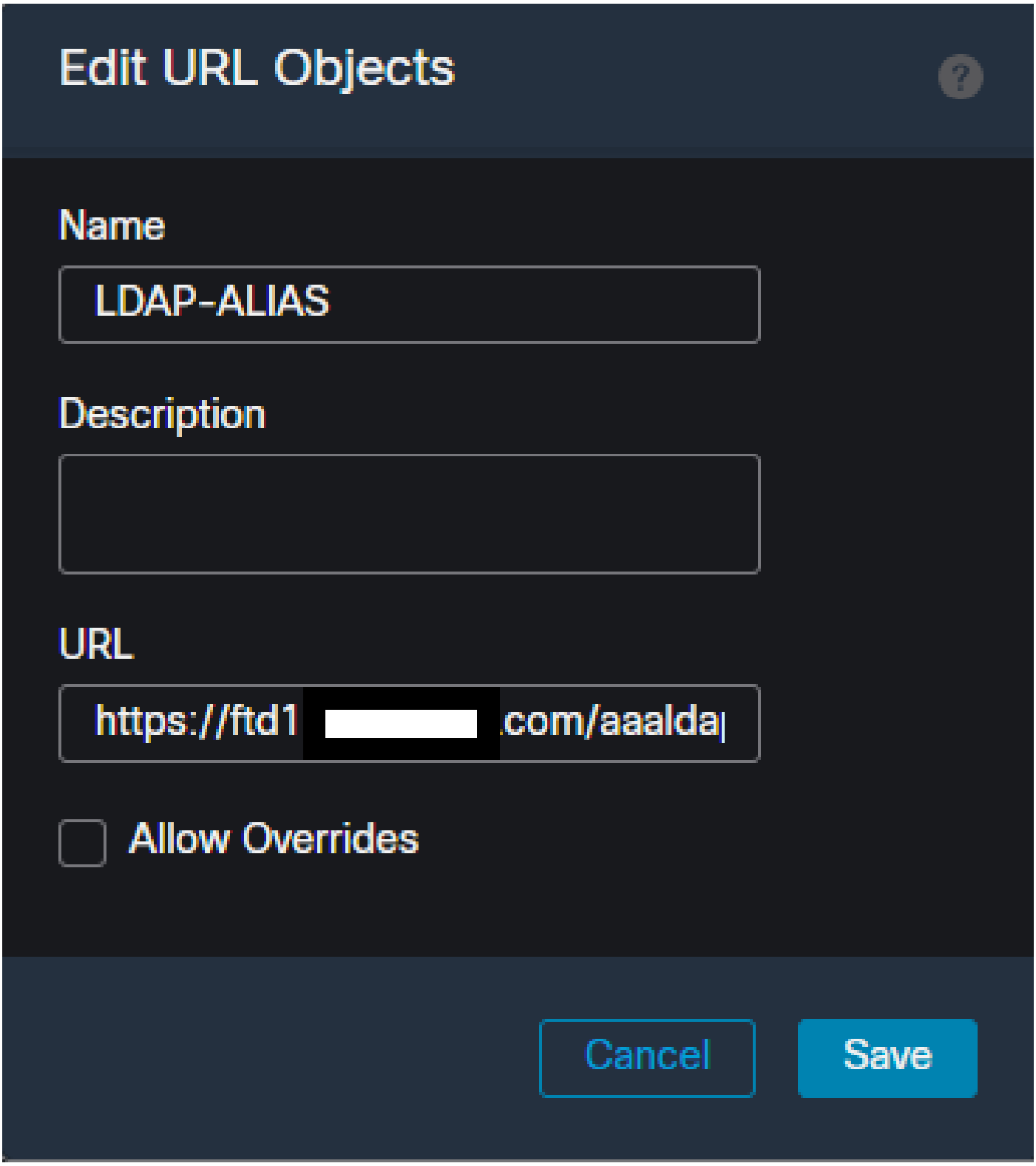
Accédez à un profil de connexion et sélectionnez l'onglet Alias. Désactivez ou supprimez l'alias-

groupe, puis cliquez sur l'icône plus pour ajouter un alias d'URL.



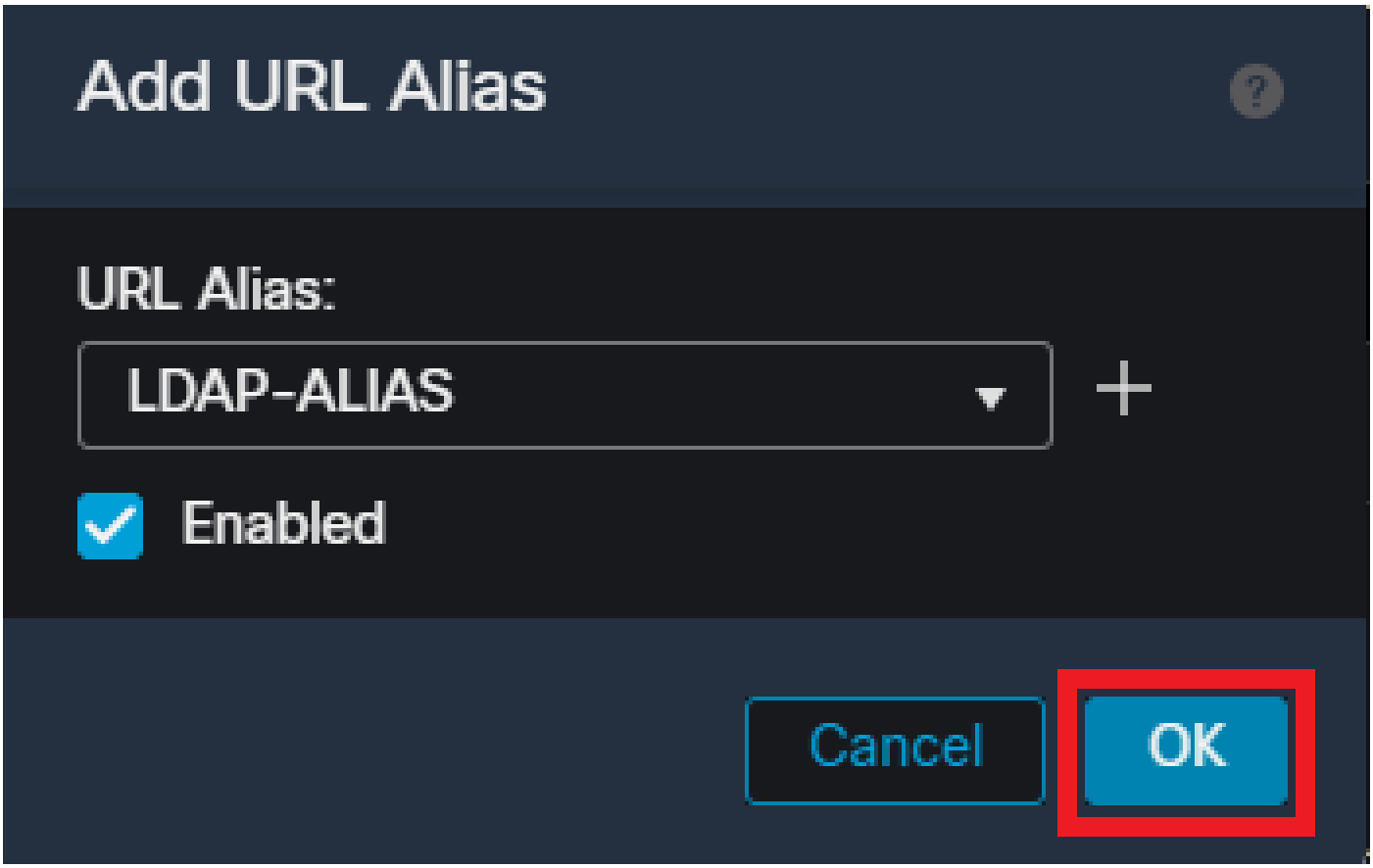
Désactivation de l'option group-alias pour un groupe de tunnels dans l'interface utilisateur FMC.

Configurez un nom d'objet pour l'alias d'URL, et complétez le nom de domaine complet et/ou l'adresse IP du pare-feu pour l'URL, suivi du nom auquel vous voulez associer le profil de connexion. Dans cet exemple, nous avons choisi « aaaldap ». Plus l'URL est obscure, plus elle est sécurisée, car il est moins probable que les pirates devinent l'URL complète même s'ils ont obtenu votre nom de domaine complet. Une fois terminé, sélectionnez Enregistrer.



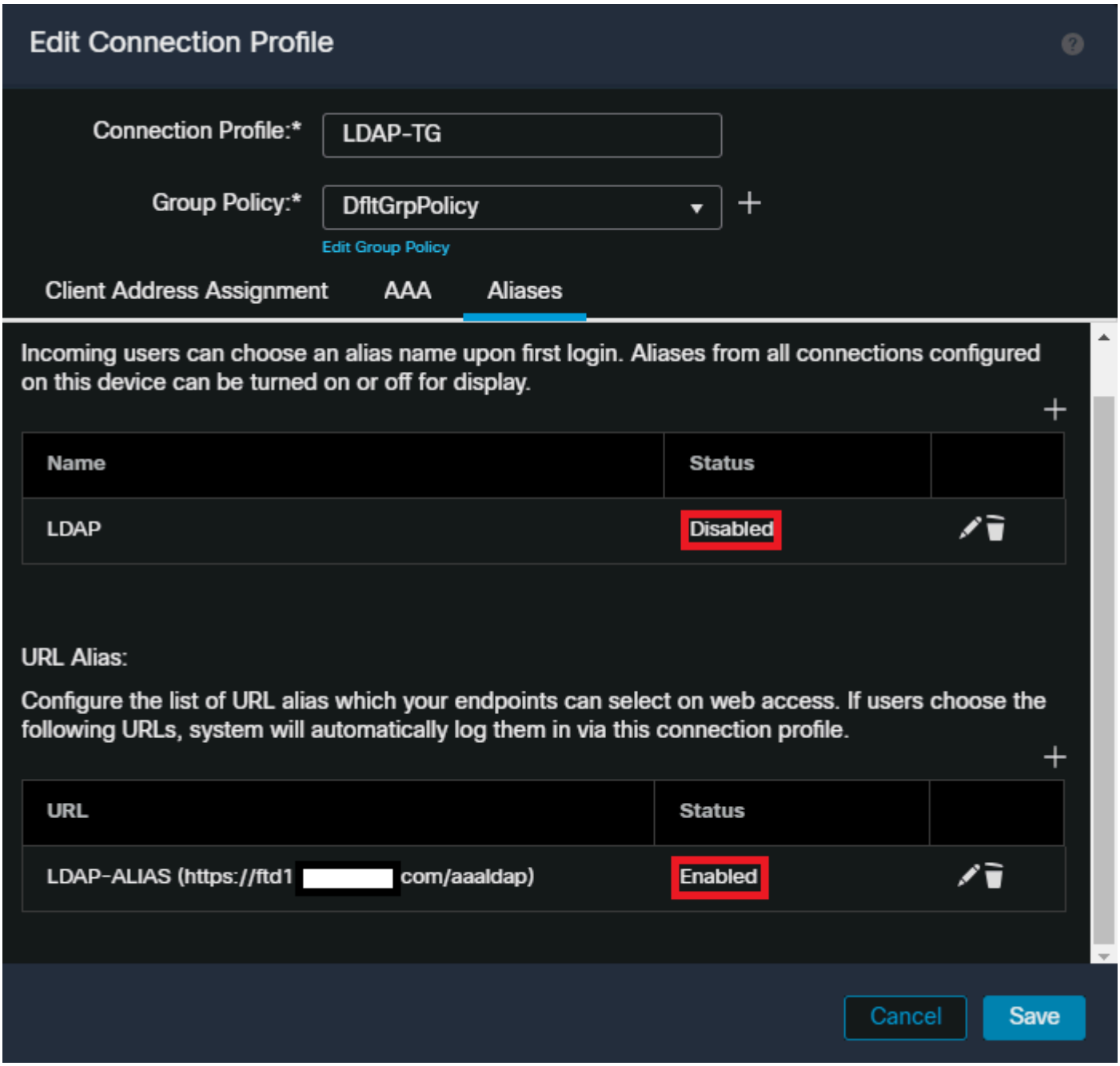
Création d'un objet URL-Alias dans l'interface utilisateur FMC.

Sélectionnez l'alias d'URL dans la liste déroulante, cochez la case Enabled et sélectionnez OK.



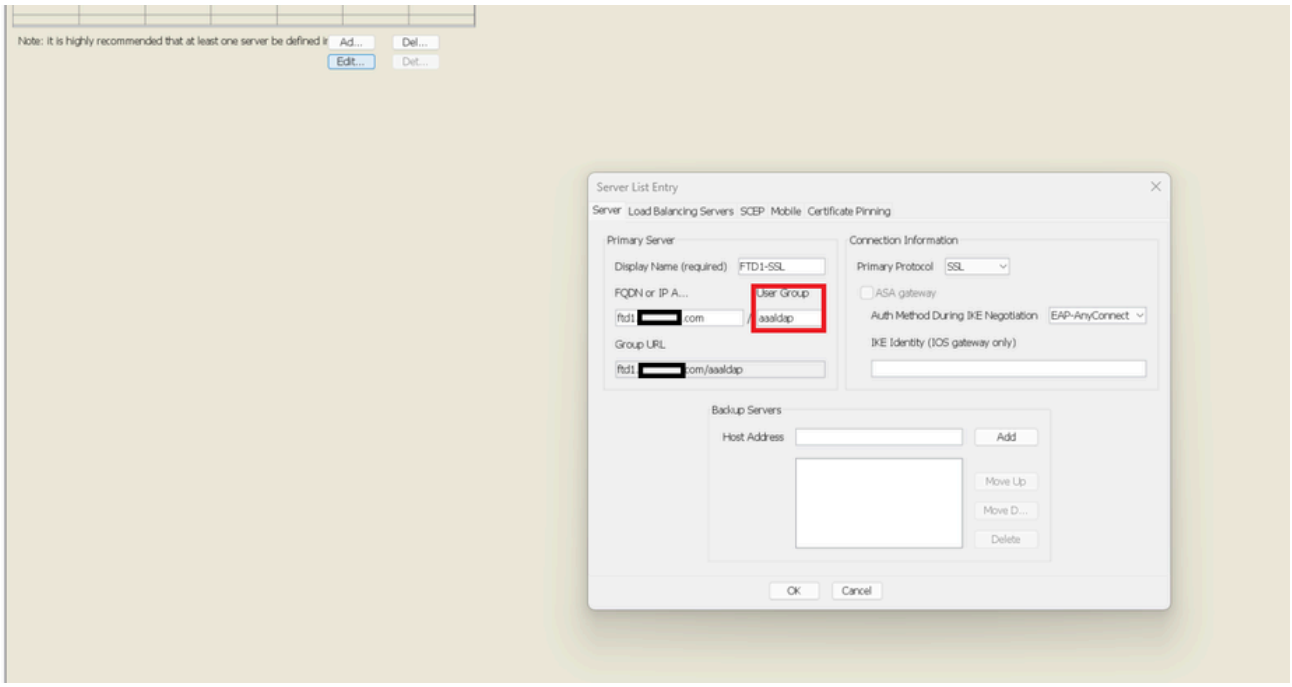
Assurez-vous que l'alias d'URL est activé dans l'interface utilisateur FMC.

Assurez-vous que l'alias de groupe est supprimé ou désactivé et vérifiez que votre alias d'URL est maintenant activé, puis sélectionnez Enregistrer.



Activation de l'option URL-Alias pour un groupe de tunnels dans l'interface utilisateur FMC.

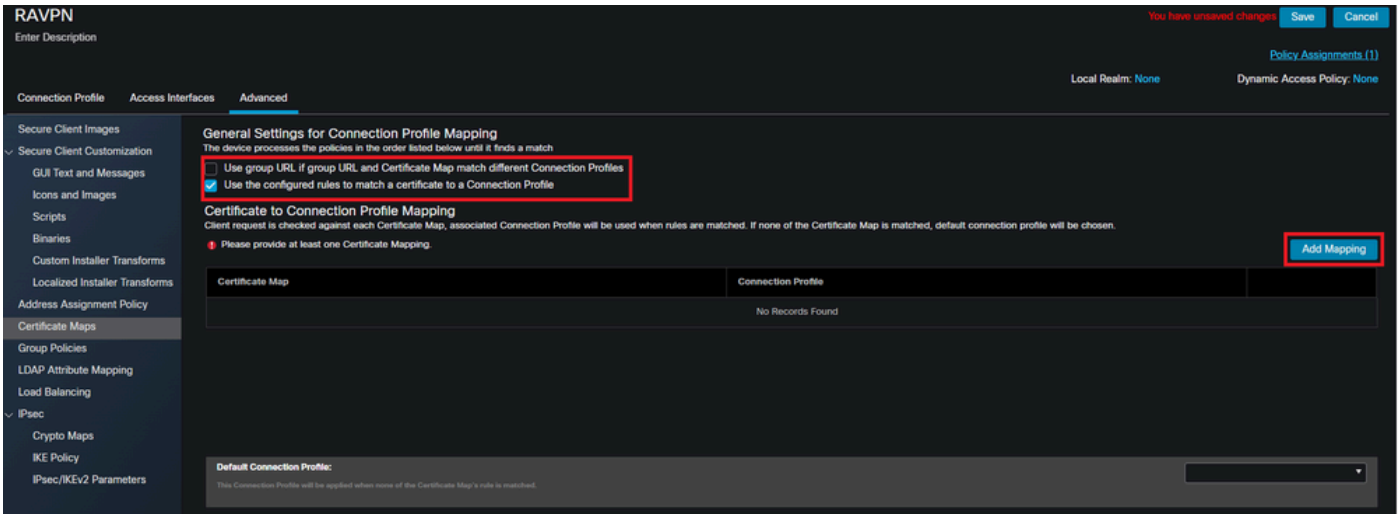
Si vous le souhaitez, les alias d'URL peuvent également être envoyés dans le cadre du code XML. Pour ce faire, modifiez le code XML à l'aide de l'Éditeur de profil VPN ou de l'Éditeur de profil ASA. Pour ce faire, accédez à l'onglet Liste des serveurs et assurez-vous que le champ Groupe d'utilisateurs correspond à l'alias d'URL du profil de connexion lors de l'utilisation de SSL. Pour IKEv2, assurez-vous que le champ User Group (Groupe d'utilisateurs) correspond au nom exact du profil de connexion.



Modification du profil XML pour obtenir un alias d'URL pour les connexions SSL.

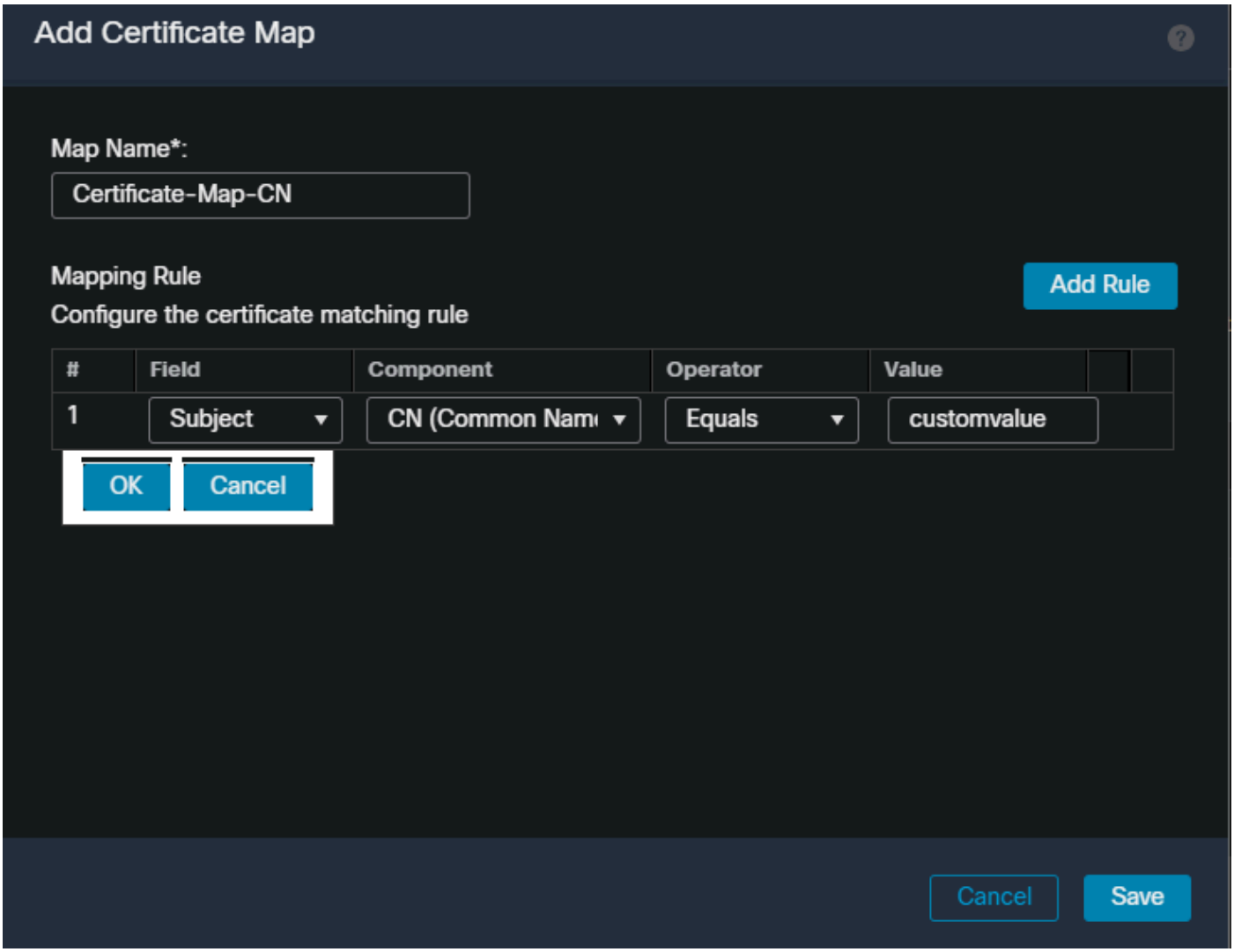
Mappage de certificat

Accédez à l'onglet Advanced dans la stratégie VPN d'accès à distance. Choisissez une option de paramètre général en fonction de vos préférences. Une fois sélectionné, sélectionnez Ajouter un mappage.



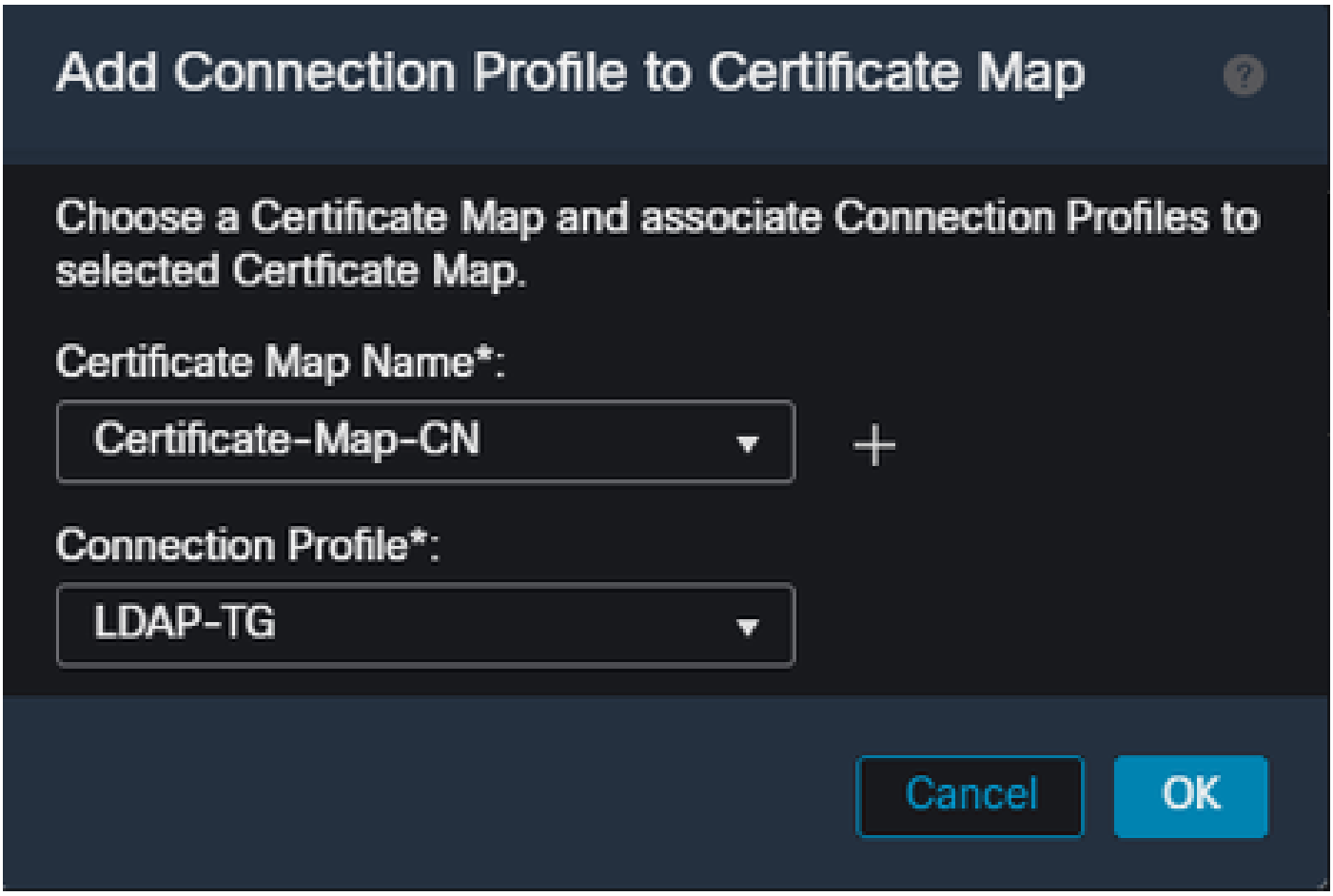
Accédez à l'onglet Avancé dans l'interface utilisateur FMC pour créer un objet de mappage de certificat dans l'interface utilisateur FMC.

Nommez l'objet de mappage de certificat et sélectionnez Ajouter une règle. Dans cette règle, définissez les propriétés du certificat que vous souhaitez identifier pour mapper l'utilisateur à un certain profil de connexion. Une fois terminé, sélectionnez OK, puis Save.



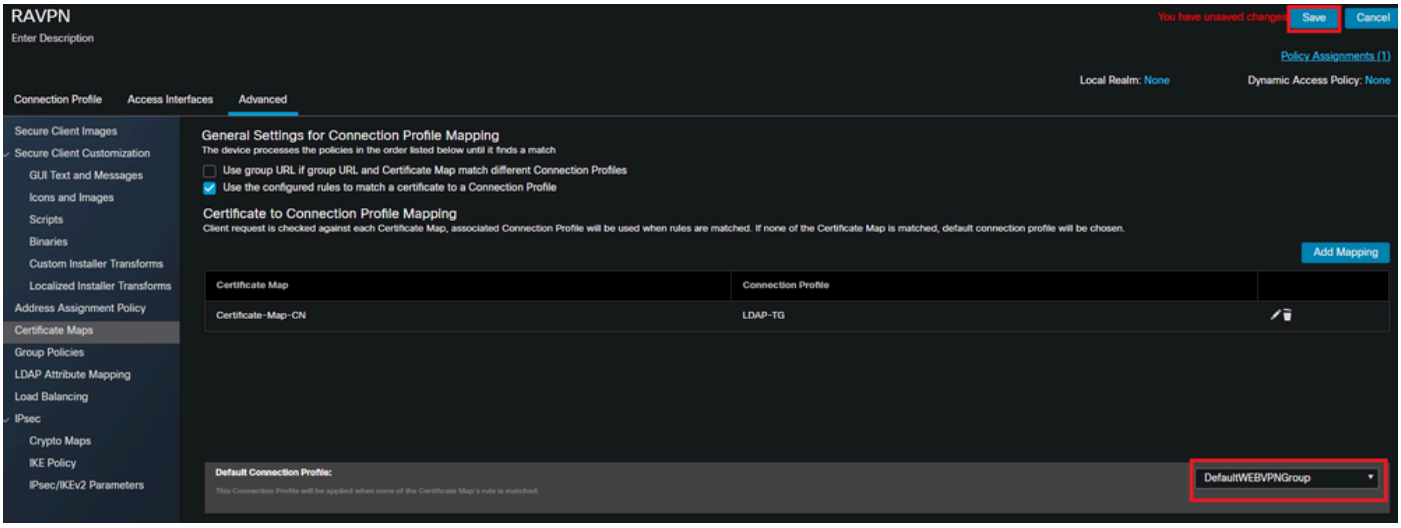
Créez un mappage de certificat et ajoutez des critères pour le mappage dans l'interface utilisateur FMC.

Dans la liste déroulante, sélectionnez l'objet de mappage de certificat et le profil de connexion auquel vous souhaitez associer le mappage de certificat. Sélectionnez ensuite OK.



Liez l'objet de mappage de certificat au groupe de tunnels souhaité dans l'interface utilisateur FMC.

Assurez-vous que le profil de connexion par défaut est configuré en tant que DefaultWEBVPNGroup afin que si un utilisateur échoue le mappage, il soit envoyé au DefaultWEBVPNGroup. Une fois terminé, sélectionnez Save et déployez les modifications.

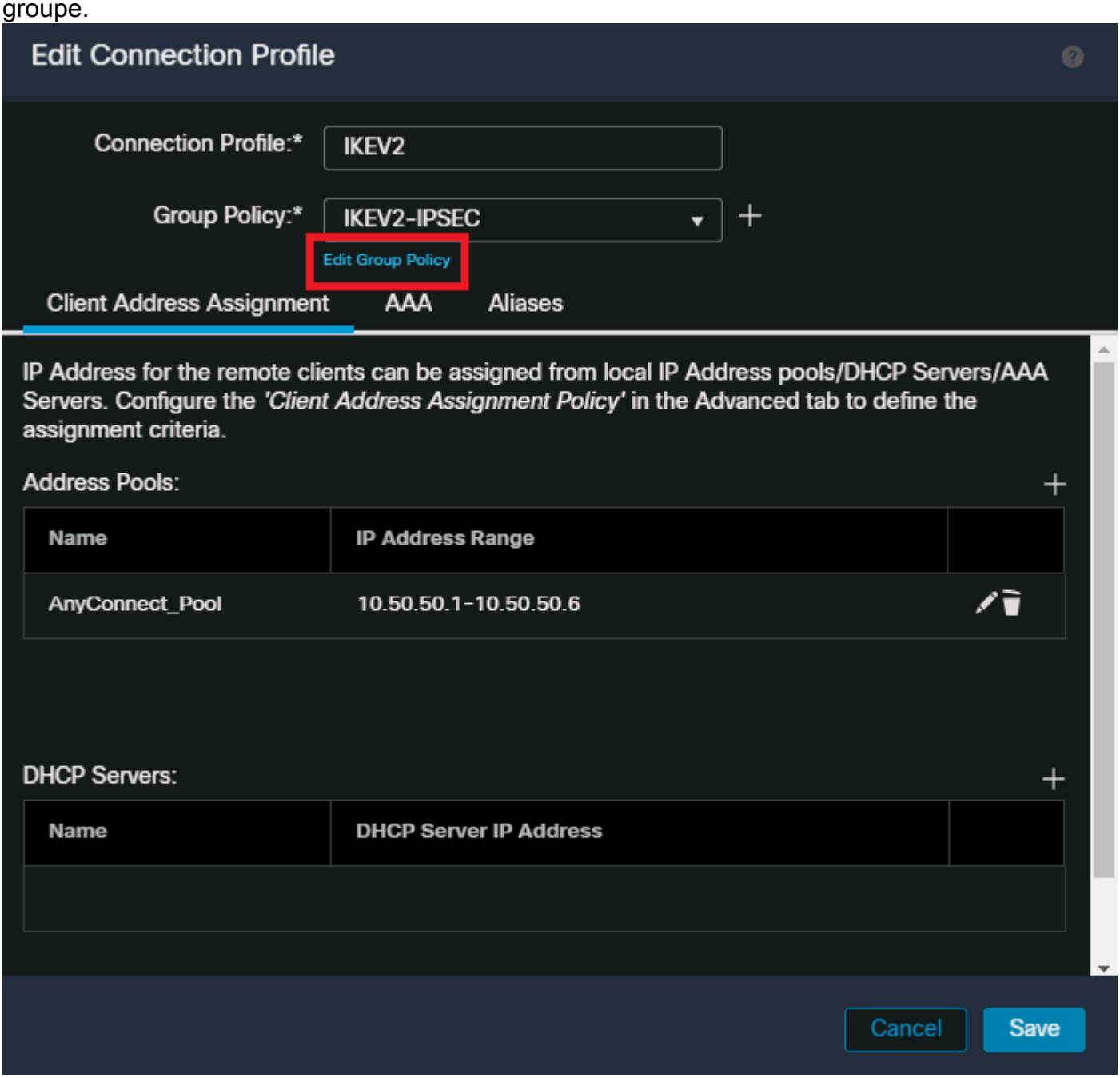


Modifiez le profil de connexion par défaut pour le mappage de certificat vers DefaultWEBVPNGroup dans l'interface utilisateur FMC.

IPsec-IKEv2

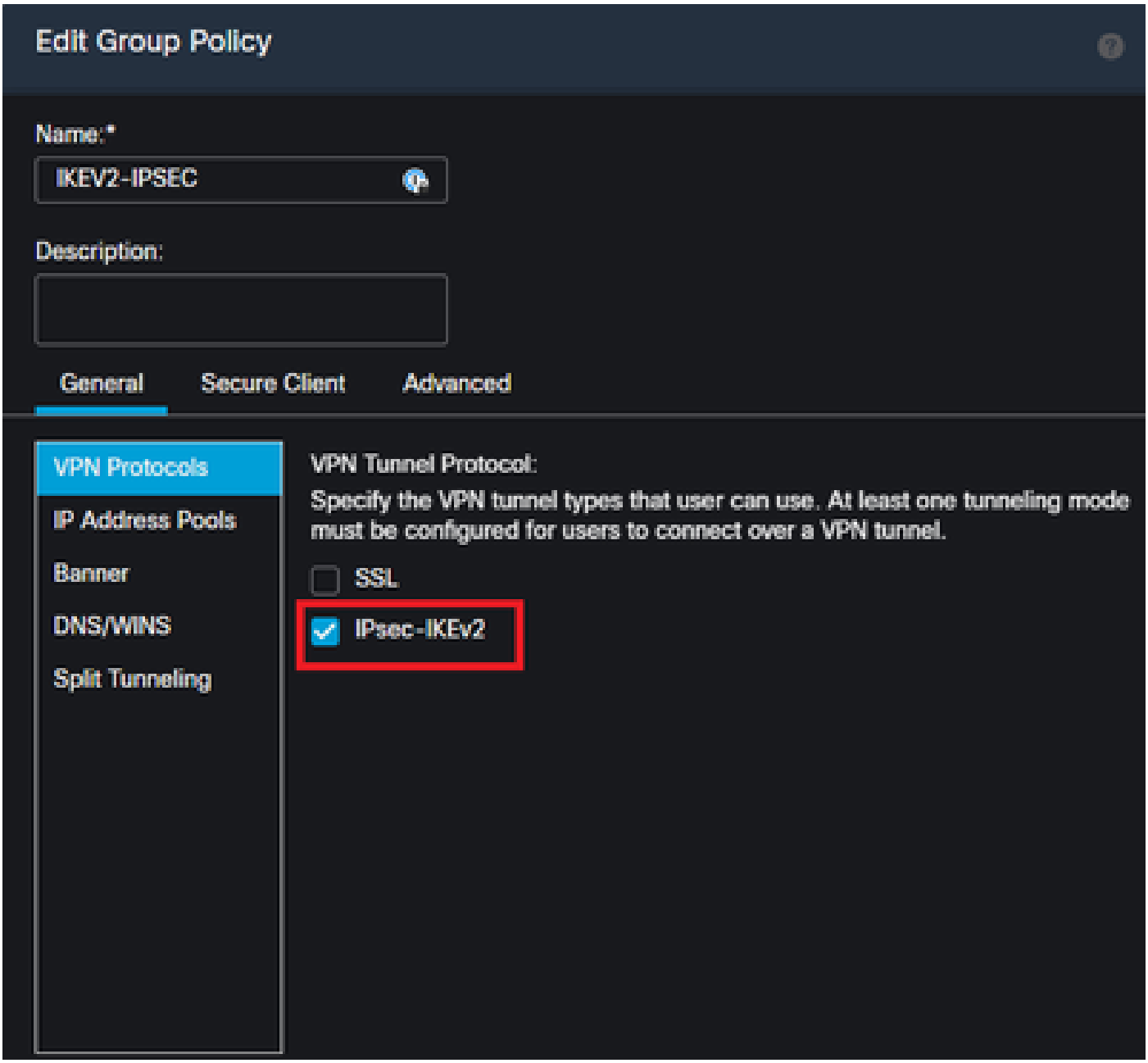
Sélectionnez le profil de connexion IPsec-IKEv2 souhaité, puis accédez à Modifier la stratégie de

groupe.



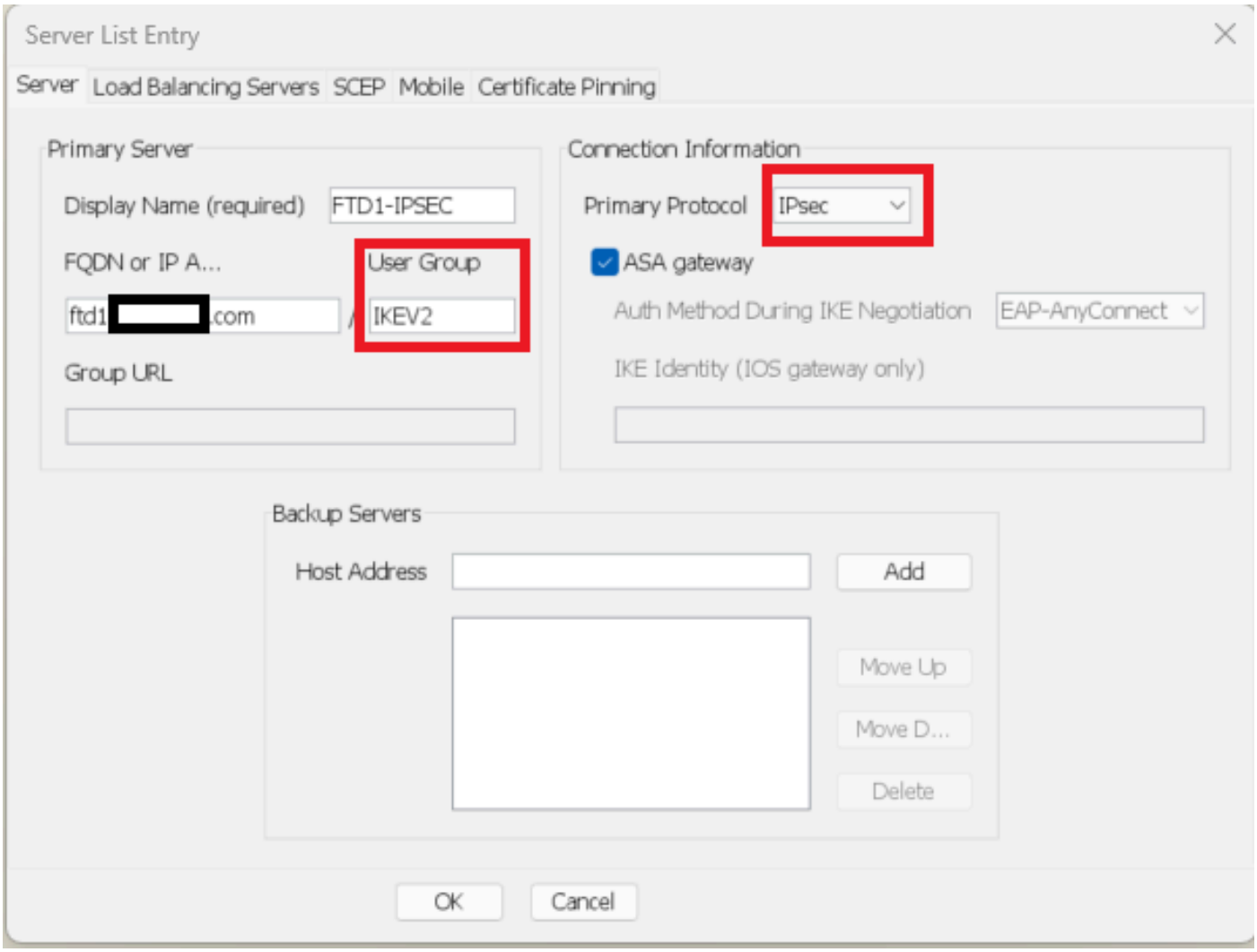
Modifiez une stratégie de groupe dans l'interface utilisateur FMC.

Dans l'onglet General, accédez à la section VPN Protocols et vérifiez que la case IPsec-IKEv2 est cochée.

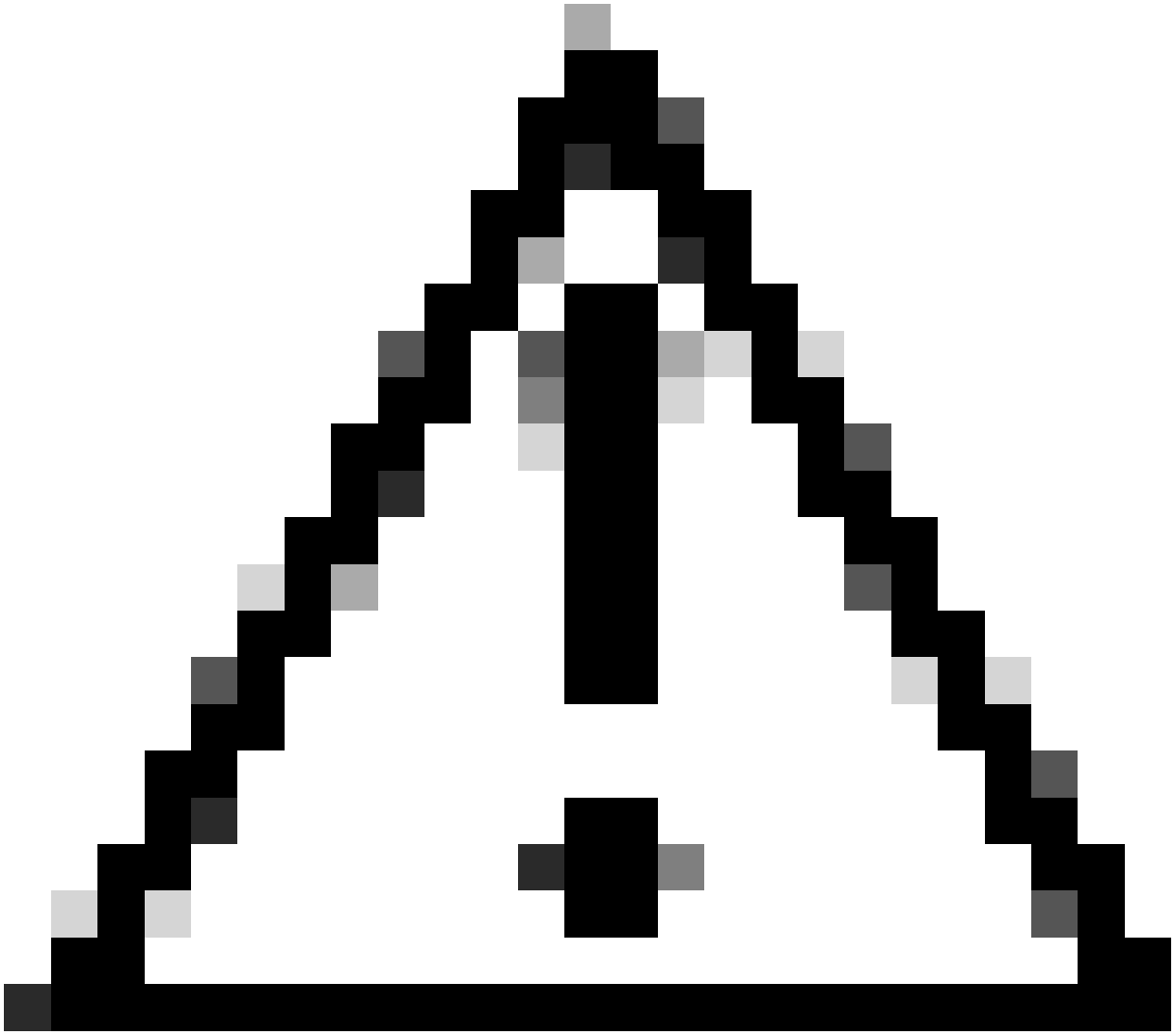


Activez IPsec-IKEv2 dans une stratégie de groupe dans l'interface utilisateur FMC.

Dans l'Éditeur de profil VPN ou l'Éditeur de profil ASA, accédez à l'onglet Liste des serveurs. Le nom du groupe d'utilisateurs DOIT correspondre exactement au nom du profil de connexion sur le pare-feu. Dans cet exemple, IKEV2 était le profil de connexion / nom du groupe d'utilisateurs. Le protocole principal est configuré comme IPsec. Le nom d'affichage de l' est affiché pour l'utilisateur dans l'interface utilisateur du client sécurisé lors de l'établissement d'une connexion à ce profil de connexion.

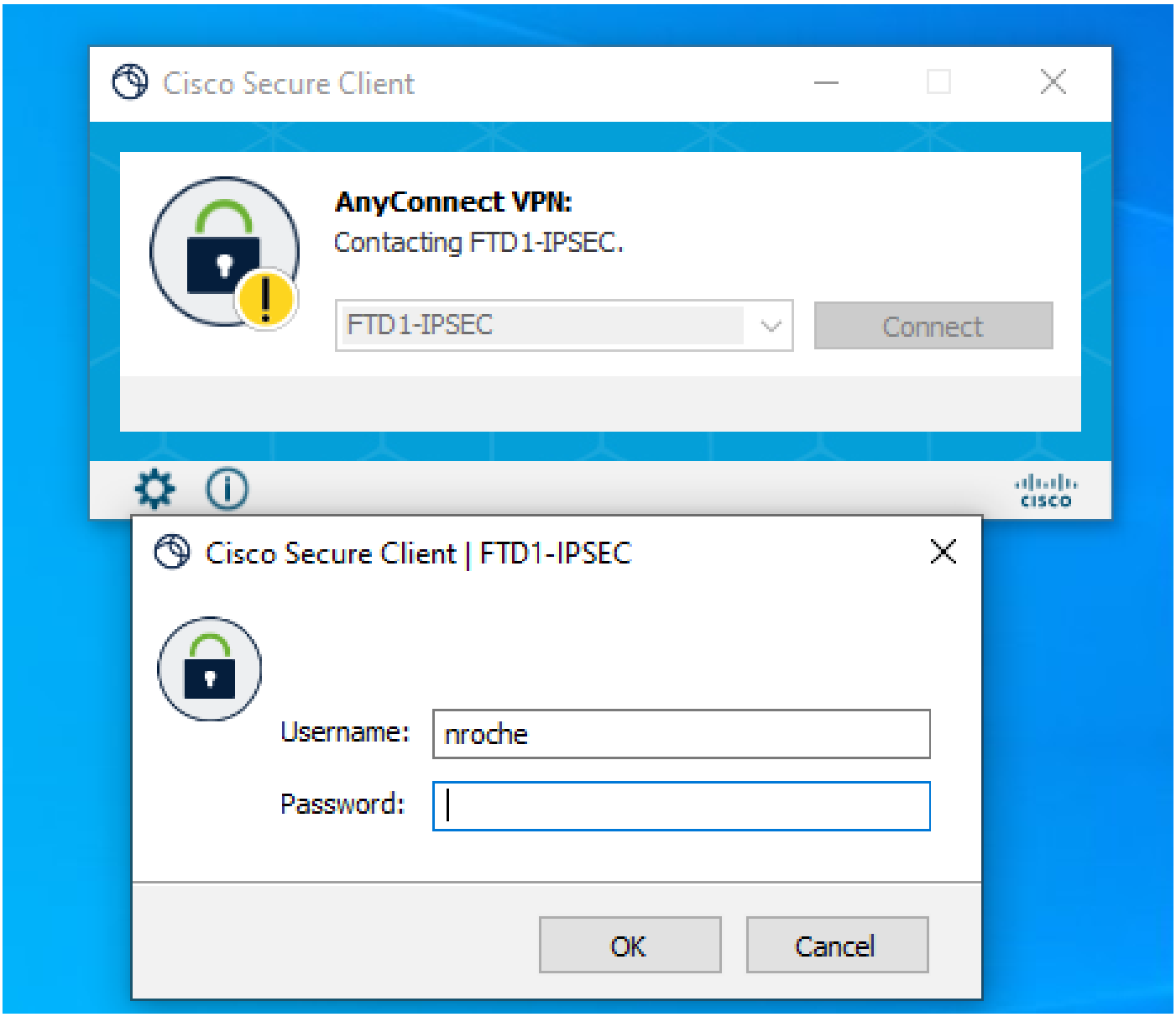


Modifiez le profil XML de sorte que le protocole principal soit IPsec et que le groupe d'utilisateurs corresponde au nom du profil de connexion.



Attention : une connexion SSL est requise pour transmettre des profils XML au client à partir du pare-feu. Lorsque vous utilisez uniquement IKEV2-IPsec, les profils XML doivent être envoyés aux clients via une méthode hors bande.

Une fois le profil XML envoyé au client, le client sécurisé utilise le groupe d'utilisateurs du profil XML pour se connecter au profil de connexion IKEV2-IPsec.



Affichage de l'interface utilisateur du client sécurisé de la tentative de connexion RAVPN IPsec-IKEv2.

Exemples de configuration ASA

Désactiver l'authentification AAA dans les profils de connexion DefaultWEBVPNGroup et DefaultRAGroup

Entrez la section webvpn-attributes pour tunnel-group DefaultWEBVPNGroup et spécifiez l'authentification comme étant basée sur un certificat. Répétez cette procédure pour le DefaultRAGroup. Les utilisateurs qui accèdent à ces profils de connexion par défaut sont obligés de présenter un certificat pour l'authentification et n'ont pas la possibilité d'entrer un nom d'utilisateur et un mot de passe.

```
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
```

Désactiver la position de Hostscan / Secure Firewall sur DefaultWEBVPNGroup et DefaultRAGroup (facultatif)

Ceci n'est nécessaire que si vous avez Hostscan / Secure Firewall Posture dans votre environnement. Cette étape empêche les pirates d'augmenter l'utilisation des ressources sur le pare-feu causée par le processus d'analyse des terminaux. Entrez la section webvpn-attributes pour les profils DefaultWEBVPNGroup et DefaultRAGroup et de connexion et implémentez without-csd pour désactiver la fonctionnalité d'analyse des points de terminaison.

```
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
```

Désactiver les alias de groupe et activer les URL de groupe

Entrez le ou les groupes de tunnels auxquels les utilisateurs se connectent. Si un alias de groupe existe déjà, désactivez-le ou supprimez-le. Dans cet exemple, il est désactivé. Une fois cette opération terminée, créez une URL de groupe à l'aide du nom de domaine complet ou de l'adresse IP de l'interface de terminaison RAVPN. Le nom à la fin de l'URL du groupe doit être obscur. Évitez les valeurs courantes telles que VPN, AAA, RADIUS, LDAP, car elles permettent aux pirates de deviner plus facilement l'URL complète s'ils obtiennent le nom de domaine complet. Utilisez plutôt des noms significatifs en interne qui vous aident à identifier le groupe de tunnels.

```
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
```

Mappage de certificat

À partir du mode de configuration globale, créez un mappage de certificat et attribuez-lui un nom et un numéro d'ordre. Définissez ensuite une règle à laquelle les utilisateurs doivent correspondre pour utiliser le mappage. Dans cet exemple, les utilisateurs doivent répondre aux critères d'une

valeur de nom commun égale à « customvalue ». Entrez ensuite la configuration webvpn et appliquez le mappage de certificat au groupe de tunnels souhaité. Une fois terminé, entrez DefaultWEBVPNGroup et définissez ce groupe de tunnels comme valeur par défaut pour les utilisateurs qui ne parviennent pas à mapper le certificat. Si le mappage échoue, les utilisateurs sont dirigés vers DefaultWEBVPNGroup. Bien que DefaultWEBVPNGroup soit configuré avec l'authentification par certificat, les utilisateurs n'ont pas la possibilité de transmettre des informations d'identification de nom d'utilisateur ou de mot de passe.

```
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
```

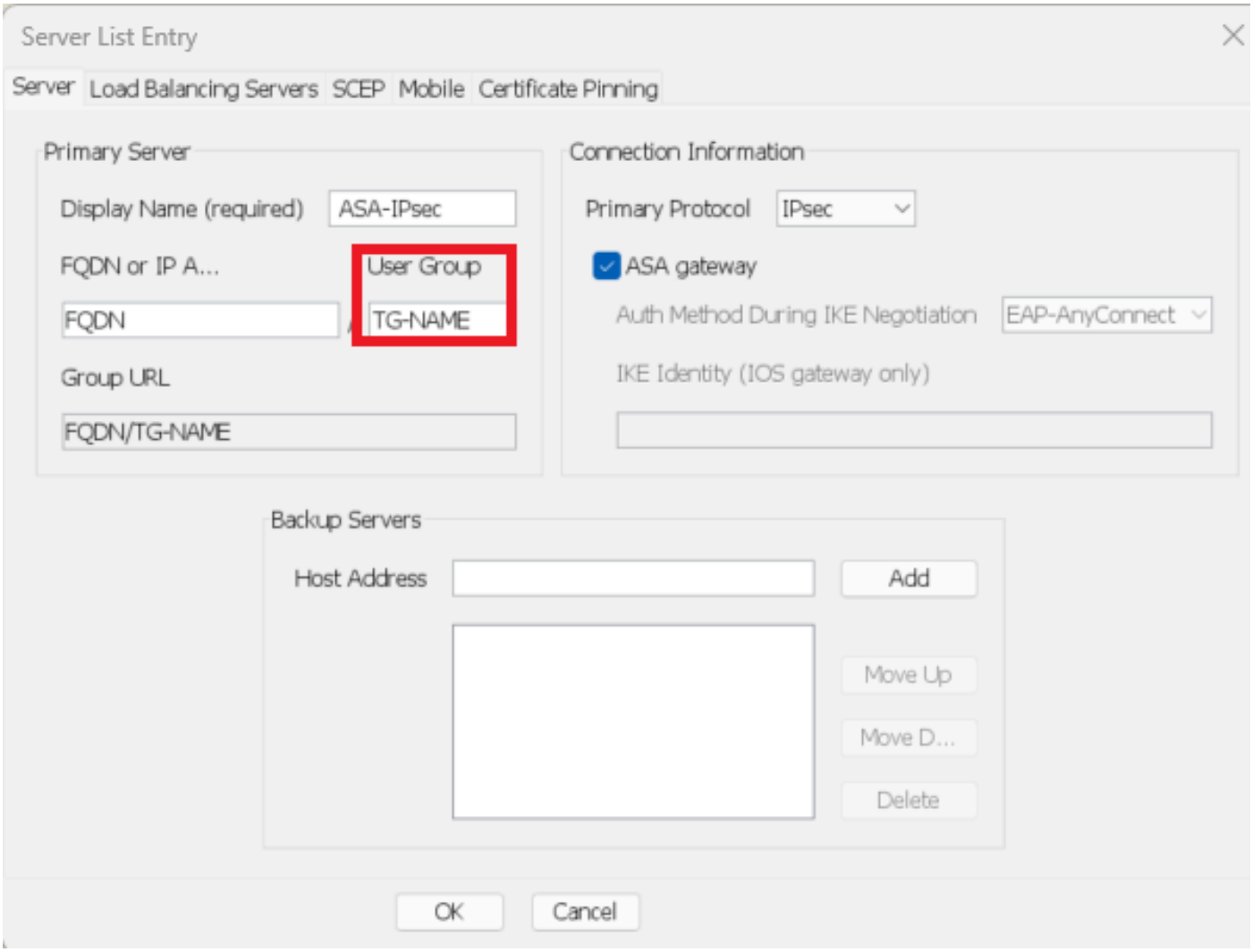
IPsec-IKEv2

En mode de configuration globale, vous pouvez modifier une stratégie de groupe existante ou en créer une nouvelle et entrer les attributs de cette stratégie de groupe. Une fois que vous êtes dans la section des attributs, activez IKEv2 en tant que seul protocole de tunnel VPN. Assurez-vous que cette stratégie de groupe est liée à un groupe de tunnels qui sera utilisé pour les connexions VPN d'accès à distance IPsec-IKEV2. Comme pour les étapes FMC, vous devez modifier le profil XML via l'Éditeur de profil VPN ou l'Éditeur de profil ASA et modifier le champ User Group pour qu'il corresponde au nom du groupe de tunnels sur l'ASA, et changer le protocole en IPsec.

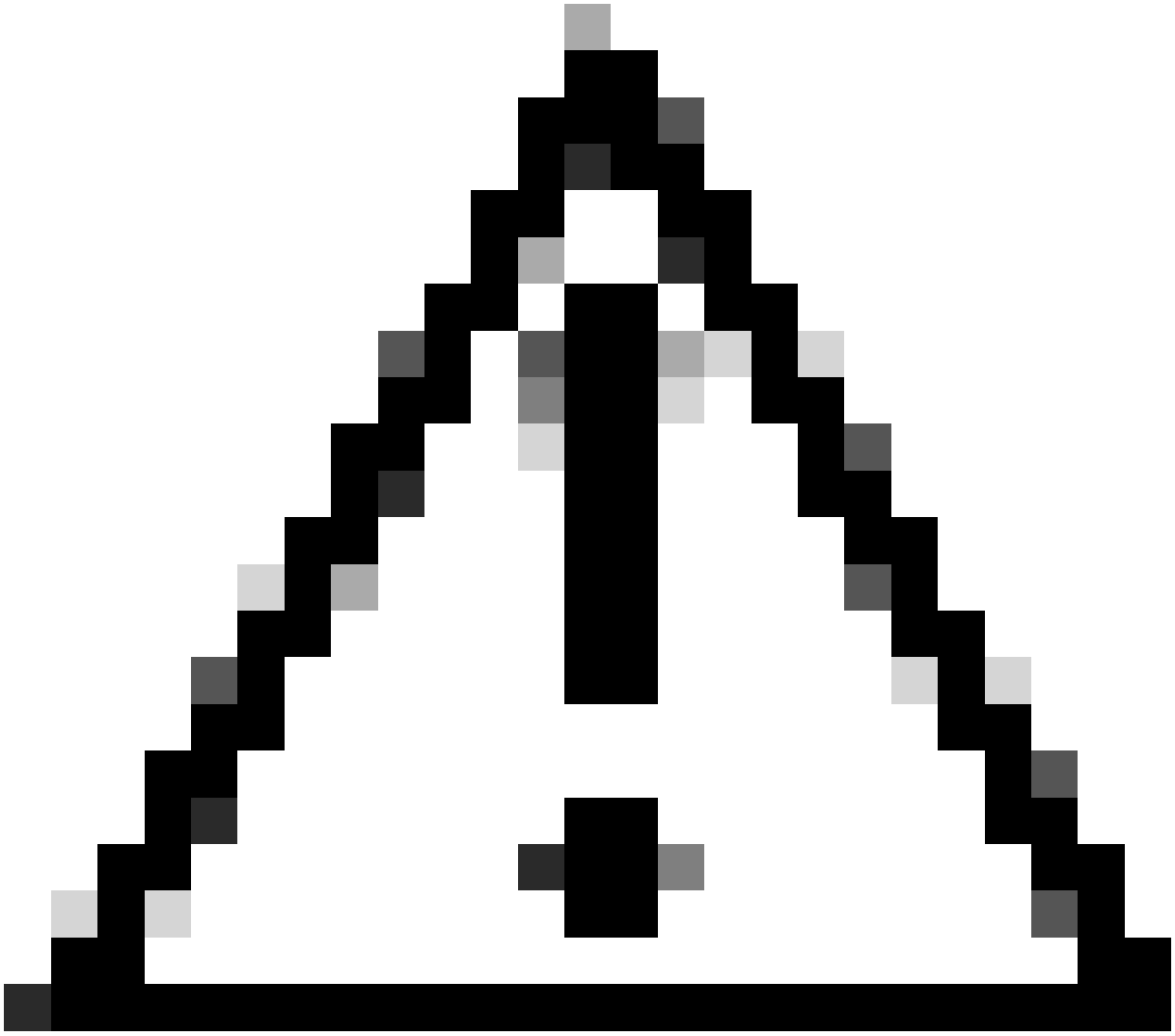
```
ASA# configure terminal
ASA(config)# group-policy GP-NAME internal
ASA(config)# group-policy GP-NAME attributes
ASA(config-group-policy)# vpn-tunnel-protocol ikev2

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

Dans l'Éditeur de profil VPN ou l'Éditeur de profil ASA, accédez à l'onglet Liste des serveurs. Le nom du groupe d'utilisateurs DOIT correspondre exactement au nom du profil de connexion sur le pare-feu. Le protocole principal est configuré comme IPsec. Le nom d'affichage apparaît à l'utilisateur dans l'interface utilisateur Secure Client lors de l'établissement d'une connexion à ce profil de connexion.



Modifiez le profil XML afin que le nom du protocole principal soit IPsec et que le nom du groupe d'utilisateurs corresponde au nom du groupe de tunnels de l'ASA pour les connexions RAVPN IPsec-IKEv2.



Attention : une connexion SSL est requise pour transmettre des profils XML au client à partir du pare-feu. Lorsque vous utilisez uniquement IKEV2-IPsec, les profils XML doivent être envoyés aux clients via une méthode hors bande.

Conclusion

En résumé, l'objectif des pratiques de renforcement de ce document est de mapper des utilisateurs légitimes à des profils de connexion personnalisés tandis que les agresseurs sont forcés d'accéder au DefaultWEBVPNGroup et au DefaultRAGroup. Dans une configuration optimisée, les deux profils de connexion par défaut n'ont pas de configuration de serveur AAA personnalisée légitime. En outre, la suppression des alias de groupe empêche les pirates d'identifier facilement les profils de connexion personnalisés en supprimant la visibilité de la liste déroulante lors de la navigation vers le nom de domaine complet ou l'adresse IP publique du pare-feu.

Informations connexes

Assistance technique de Cisco et téléchargements

Attaques par pulvérisation de mot de passe

Vulnérabilité d'accès non autorisé Septembre 2023

Guides de configuration ASA

Guides de configuration FMC / FDM

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.