Configurer un RAVPN IPv6 avec authentification AAA sur FTD géré par FDM

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Diagramme du réseau
- Configurations sur FDM
- Configurations sur ISE

Vérifier

Dépannage

Informations connexes

Introduction

Ce document décrit les étapes de configuration d'un VPN d'accès à distance IPv6 avec authentification AAA sur FTD géré par FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firepower Device Manager (FDM) virtuel
- Cisco Secure Firewall Threat Defense (FTD) virtuel
- Flux d'authentification VPN

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure FDM Virtual 7.6.0
- Cisco Secure FTD Virtual 7.6.0
- Cisco Secure Client 5.1.6.103

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.

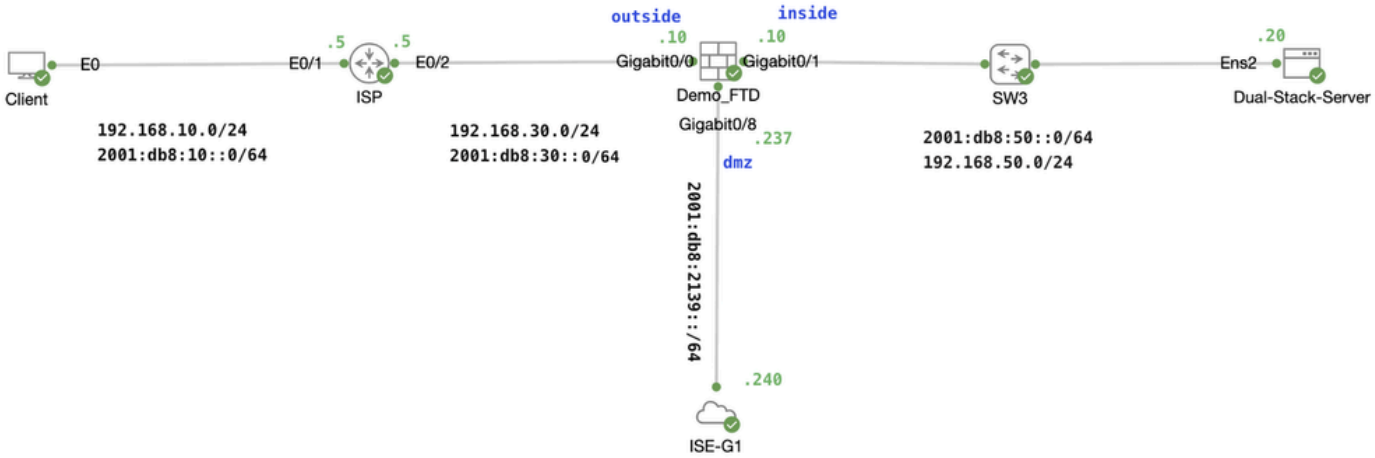
Informations générales

Le VPN d'accès à distance IPv6 (RAVPN) prend de plus en plus d'importance à mesure que le monde passe d'IPv4 à IPv6, les adresses IPv4 étant limitées et pratiquement épuisées, tandis que l'IPv6 offre un espace d'adressage pratiquement illimité, en s'adaptant au nombre croissant de périphériques connectés à Internet. À mesure que les réseaux et les services passent à l'IPv6, la capacité IPv6 garantit que votre réseau reste compatible et accessible. IPv6 RAVPN aide les entreprises à se préparer à l'avenir de la mise en réseau, en garantissant une connectivité à distance sécurisée et évolutive.

Dans cet exemple, le client communique avec la passerelle VPN à l'aide d'une adresse IPv6 fournie par le fournisseur de services, mais reçoit des adresses IPv4 et IPv6 des pools VPN, en utilisant Cisco Identity Service Engine (ISE) comme source d'identité d'authentification. ISE est configuré avec une adresse IPv6 uniquement. Le serveur interne est configuré avec des adresses IPv4 et IPv6, représentant des hôtes à double pile. Le client peut accéder aux ressources internes à l'aide de l'adresse VPN IPv4 ou IPv6, selon le cas.

Configurer

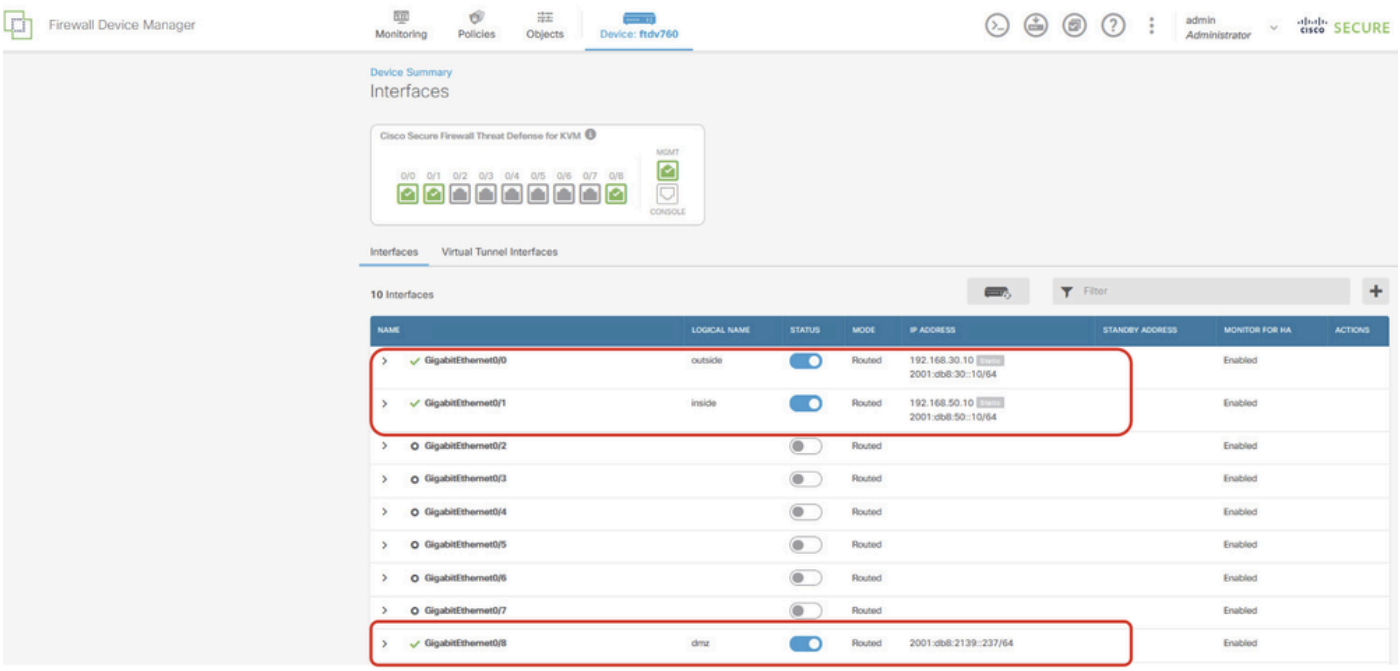
Diagramme du réseau



Topologie

Configurations sur FDM

Étape 1. Il est essentiel de s’assurer que la configuration préliminaire de l’interconnexion IPv4 et IPv6 entre les noeuds a été dûment effectuée. La passerelle du client et du FTD est l’adresse du FAI associée. La passerelle du serveur se trouve à l'intérieur de l'adresse IP de FTD. L'ISE se trouve dans la zone DMZ de FTD.



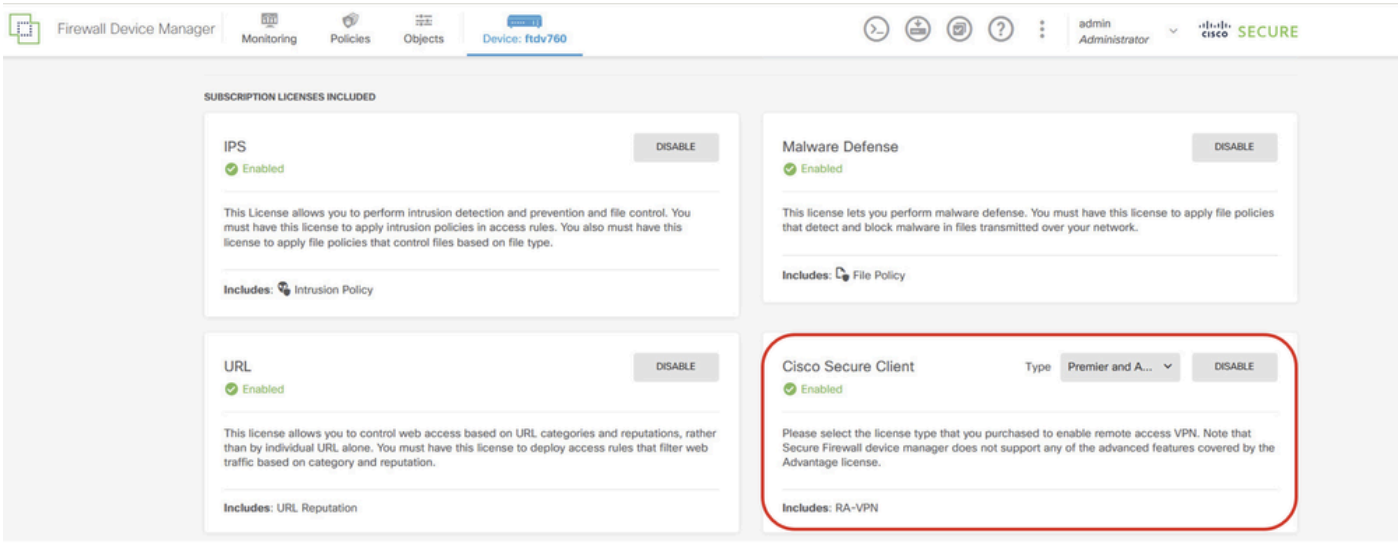
FTD_Interface_IP



FTD_Route_ParDéfaut

Étape 2. Téléchargez le package Cisco Secure Client nommé Cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg à partir de la page de téléchargement de logiciels Cisco et vérifiez que le fichier est correct après le téléchargement en confirmant que la somme de contrôle md5 du fichier téléchargé est identique à celle de la page de téléchargement de logiciels Cisco.

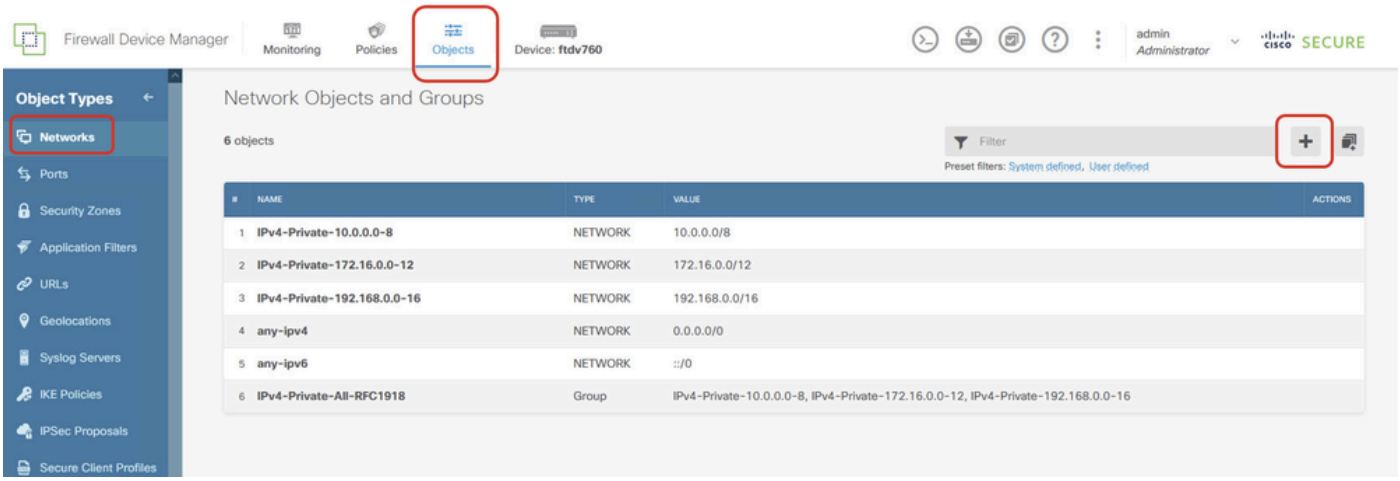
Étape 3 : vérification de l'activation des licences RAVPN sur le FTD



Licence_FDM

Étape 4 : création du pool d'adresses VPN

Étape 4.1. Créer un pool d'adresses IPv6 et IPv4 en créant des objets réseau. Accédez à Objets > Réseaux et cliquez sur le bouton +.

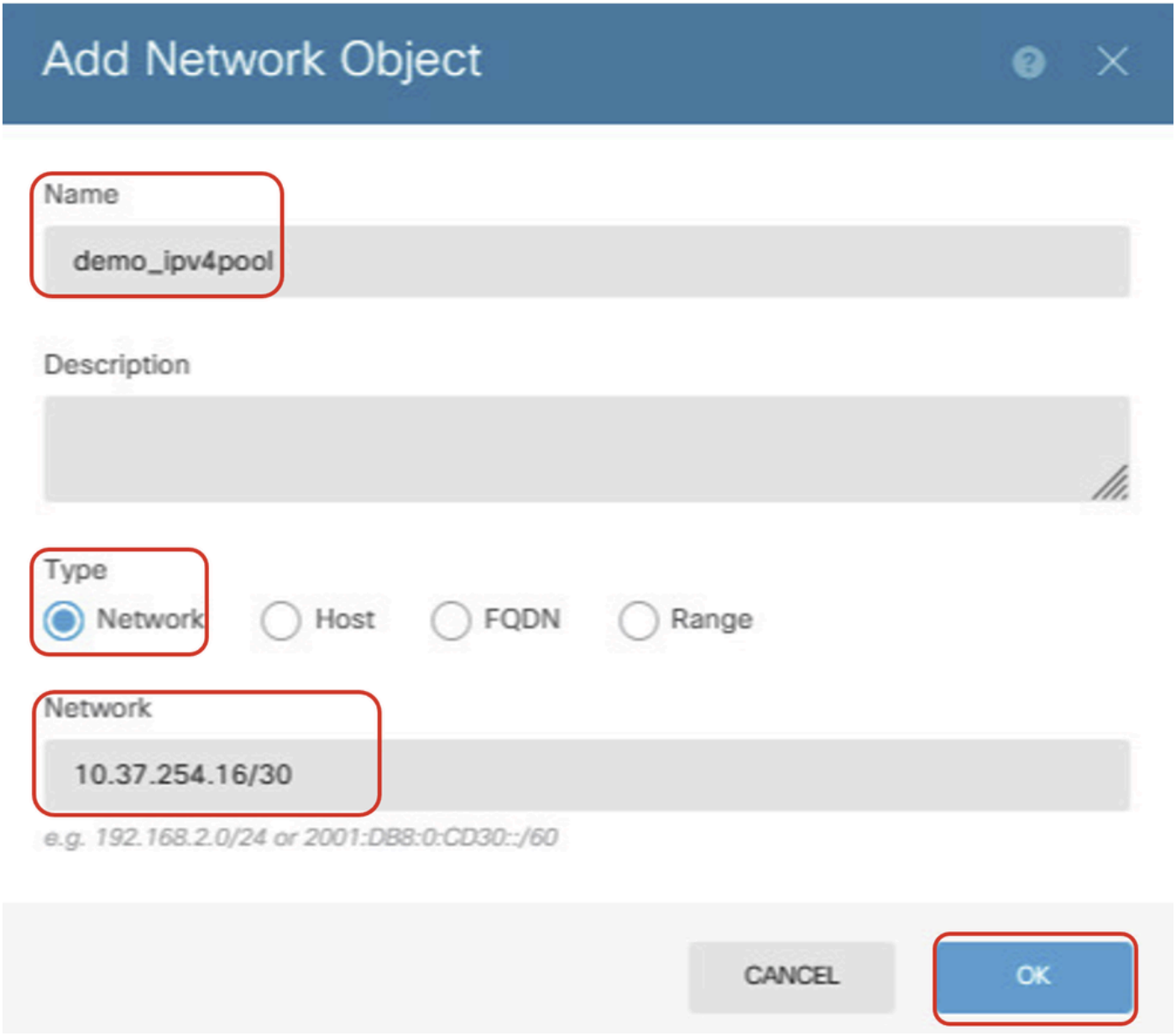


Create_VPN_Address_Pool_1

Étape 4.2. Fournissez les informations nécessaires sur chaque objet réseau. Cliquez sur le bouton OK.

Pour un pool IPv4, le type d'objet peut être choisi avec Réseau ou Plage. Dans cet exemple, le type d'objet Réseau est choisi à des fins de démonstration.

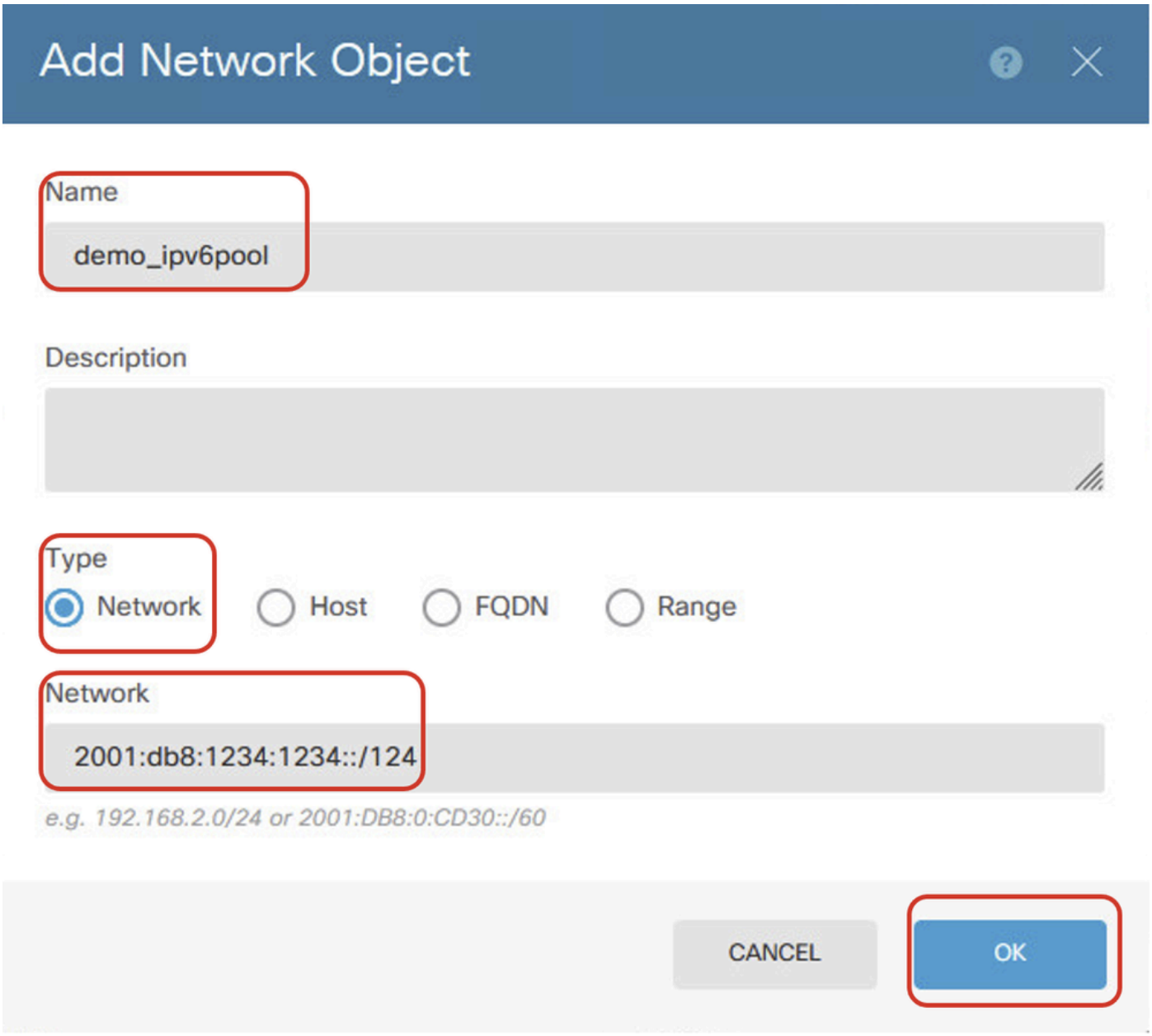
- Name : demo_ipv4pool
- type : Réseau
- Réseau: 10.37.254.16/30



Create_VPN_Address_Pool_2_IPv4

Pour le pool IPv6, le type d'objet ne peut être choisi qu'avec Network à partir de maintenant.

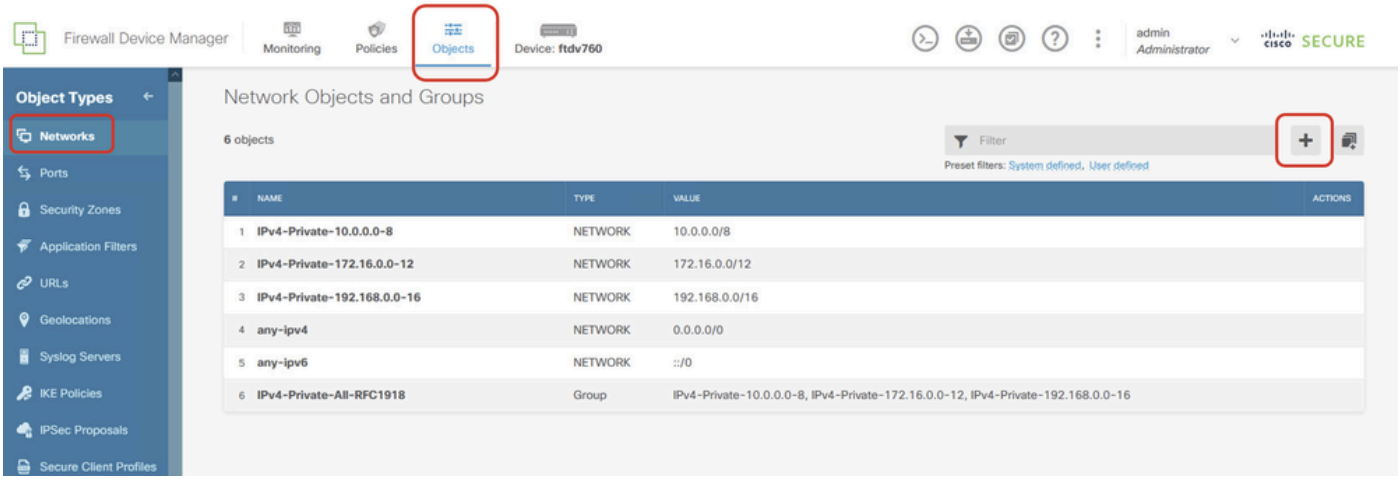
- Name : demo_ipv6pool
- type : Réseau
- Réseau: 2001:db8:1234:1234::/124



Create_VPN_Address_Pool_2_IPv6

Étape 5 : création du réseau interne pour l'exemption NAT

Étape 5.1. Accédez à Objets > Réseaux et cliquez sur le bouton +.

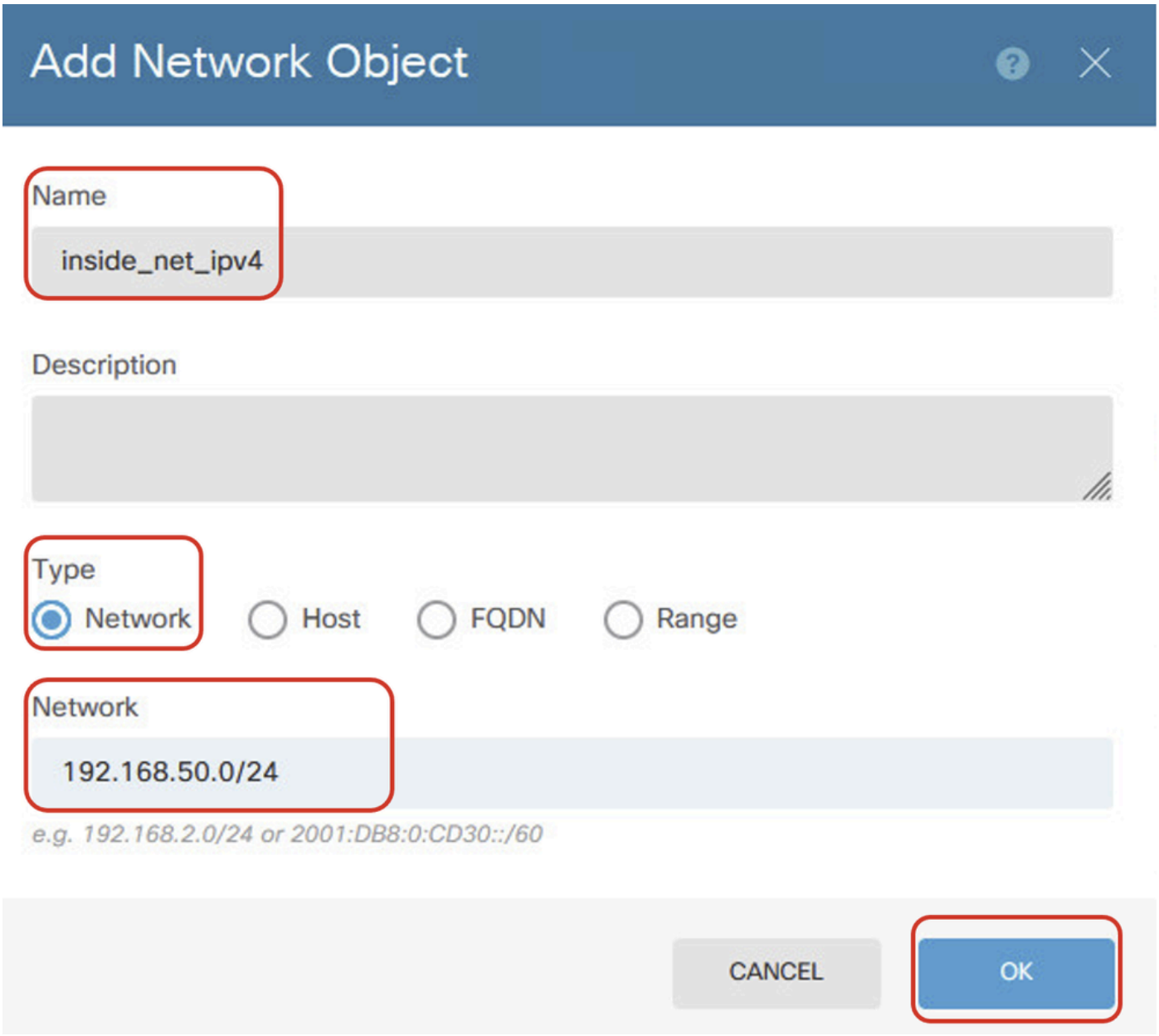


Créer_Réseau_Exempt_NAT_1

Étape 5.2. Fournissez les informations nécessaires pour chaque objet réseau. Cliquez sur le bouton OK.

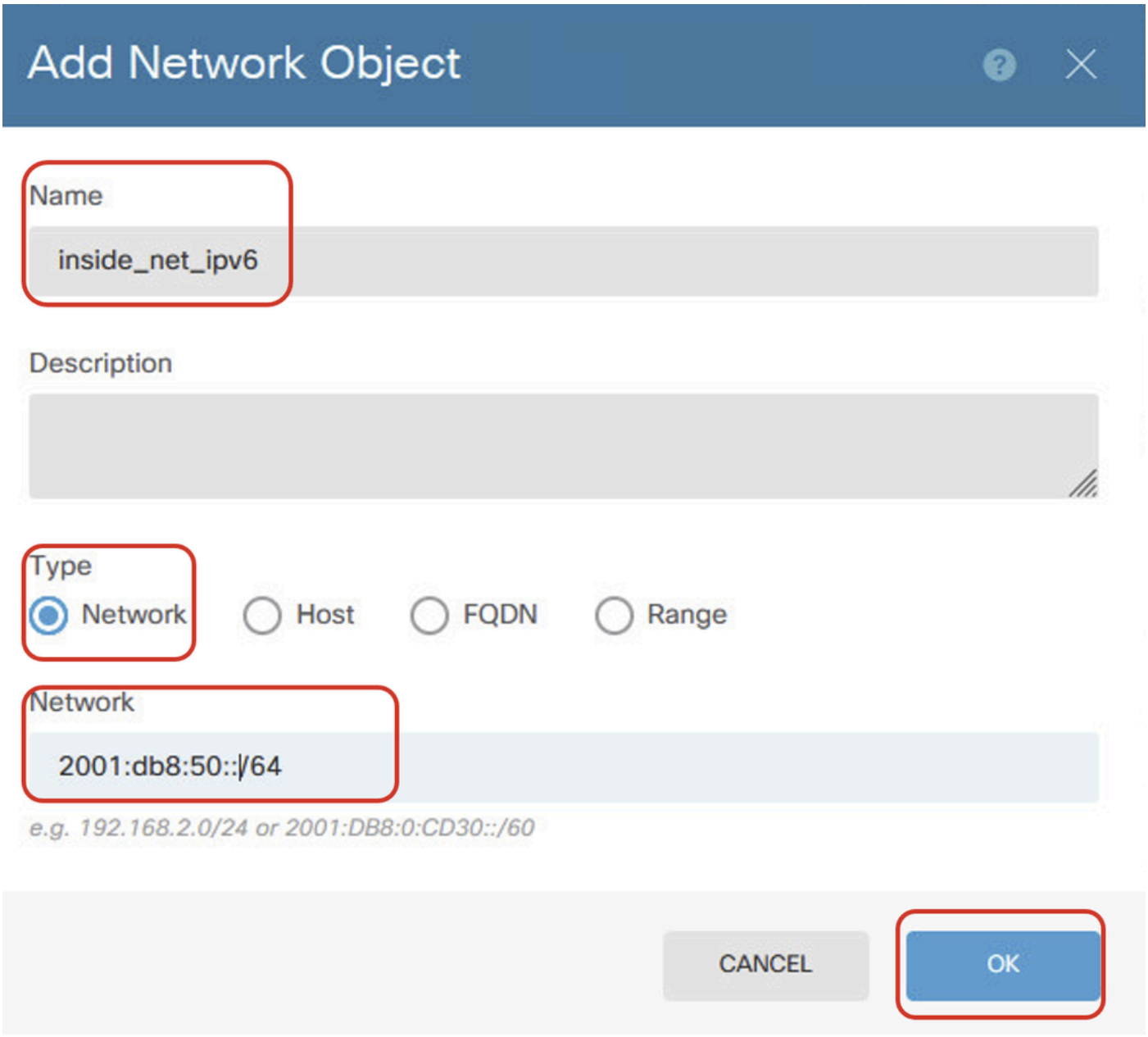
Dans cet exemple, les réseaux IPv4 et IPv6 sont tous deux configurés.

- Name : ipv4_réseau_intérieur
- type : Réseau
- Réseau: 192.168.50.0/24



Create_NAT_Exempt_Network_2_IPv4

- Name : inside_net_ipv6
- type : Réseau
- Réseau: 2001:db8:50::/64

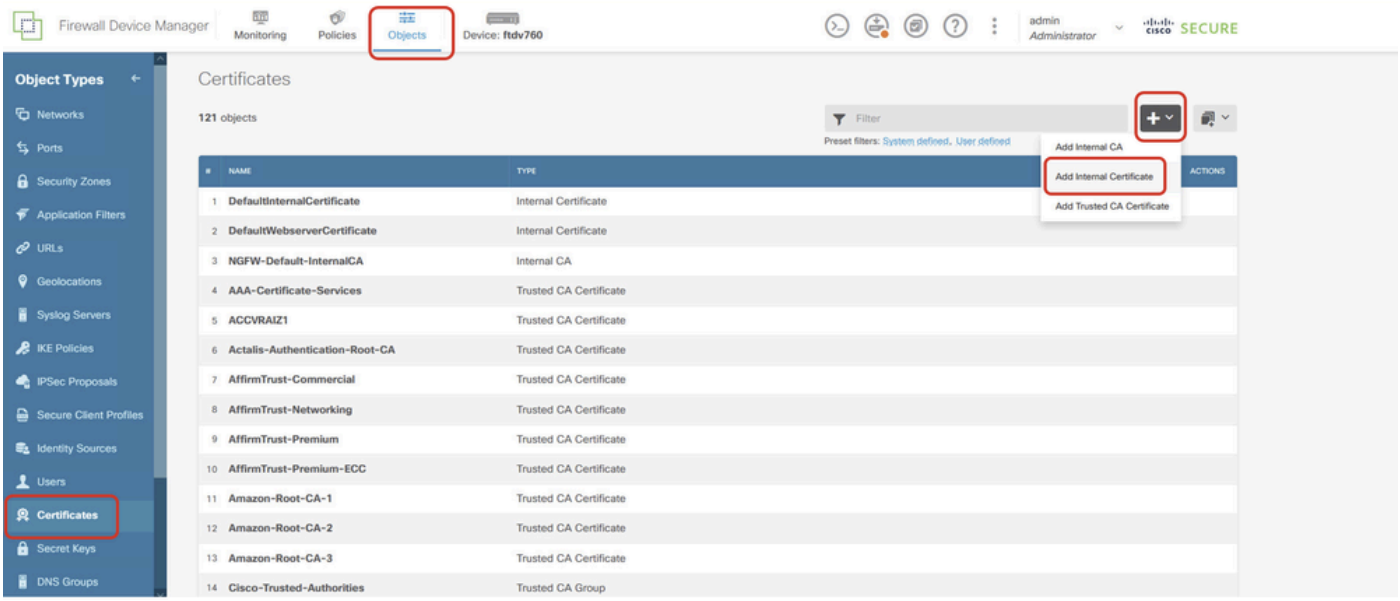


Create_NAT_Exempt_Network_2_IPv6

Étape 6 : création du certificat utilisé pour le protocole RAVPN Vous avez deux options : vous pouvez télécharger un certificat signé par une autorité de certification (CA) tierce ou générer un nouveau certificat auto-signé.

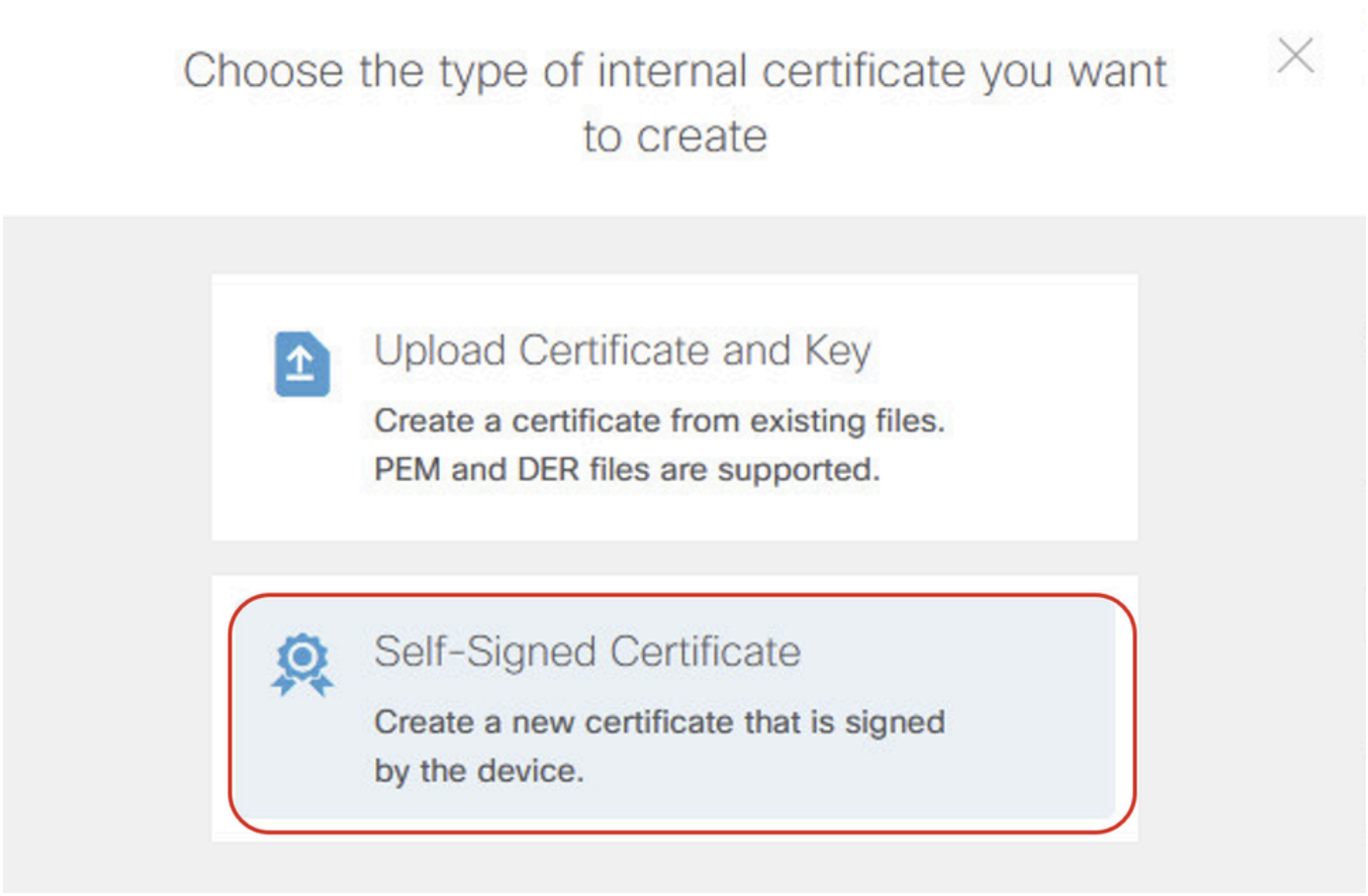
Dans cet exemple, un nouveau certificat auto-signé est utilisé avec le contenu personnalisé du certificat à des fins de démonstration.

Étape 6.1. Accédez à Objets > Certificats. Cliquez sur le bouton + et choisissez Ajouter un certificat interne.



Créer_Certificat_1

Étape 6.2. Cliquez sur Self-Signed Certificate.



Étape 6.3. Cliquez sur l'onglet Général et fournissez les informations nécessaires.

Name : démobiliser

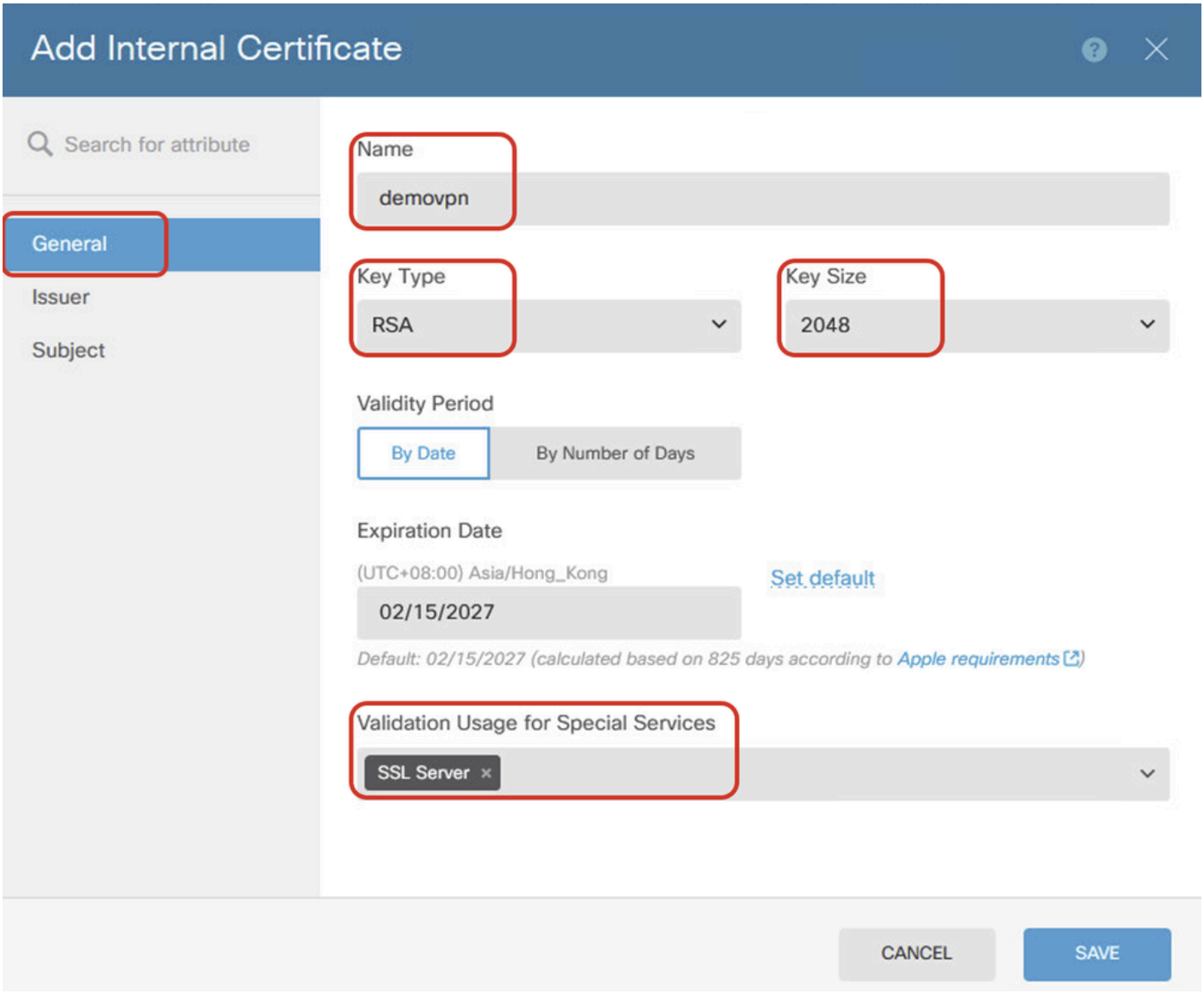
Type de clé : RSA

Taille de la clé : 2048

Période de validité : Défaut

Date d'expiration : Défaut

Utilisation de la validation pour les services spéciaux : Serveur SSL

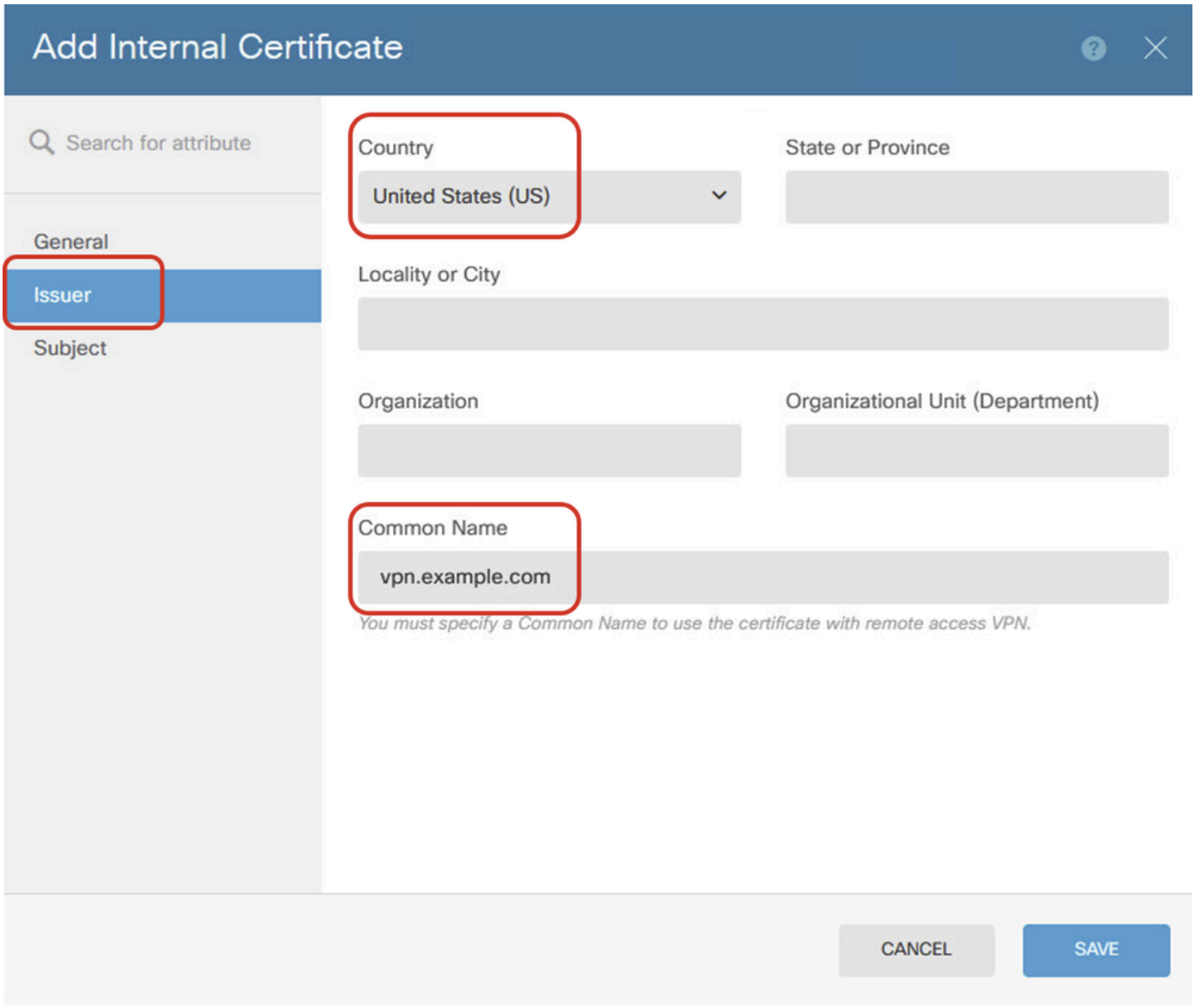


Créer_Certificat_3

Étape 6.4. Cliquez sur l'onglet Émetteur et fournissez les informations nécessaires.

Pays : États-Unis (US)

Nom commun : vpn.example.com

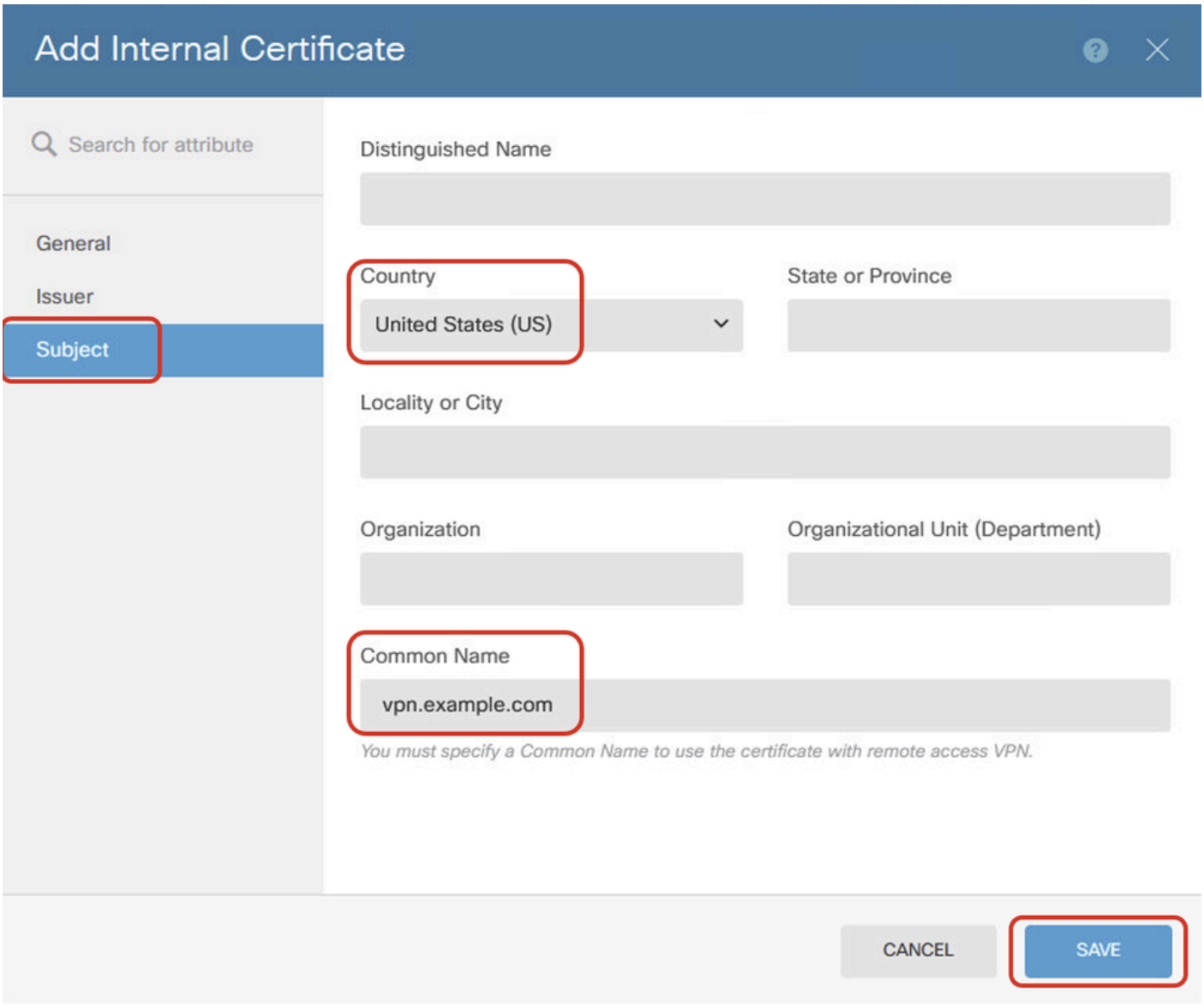


Créer_Certificat_4

Étape 6.5. Cliquez sur l'onglet Subject, fournissez les informations nécessaires, puis cliquez sur SAVE.

Pays : États-Unis (US)

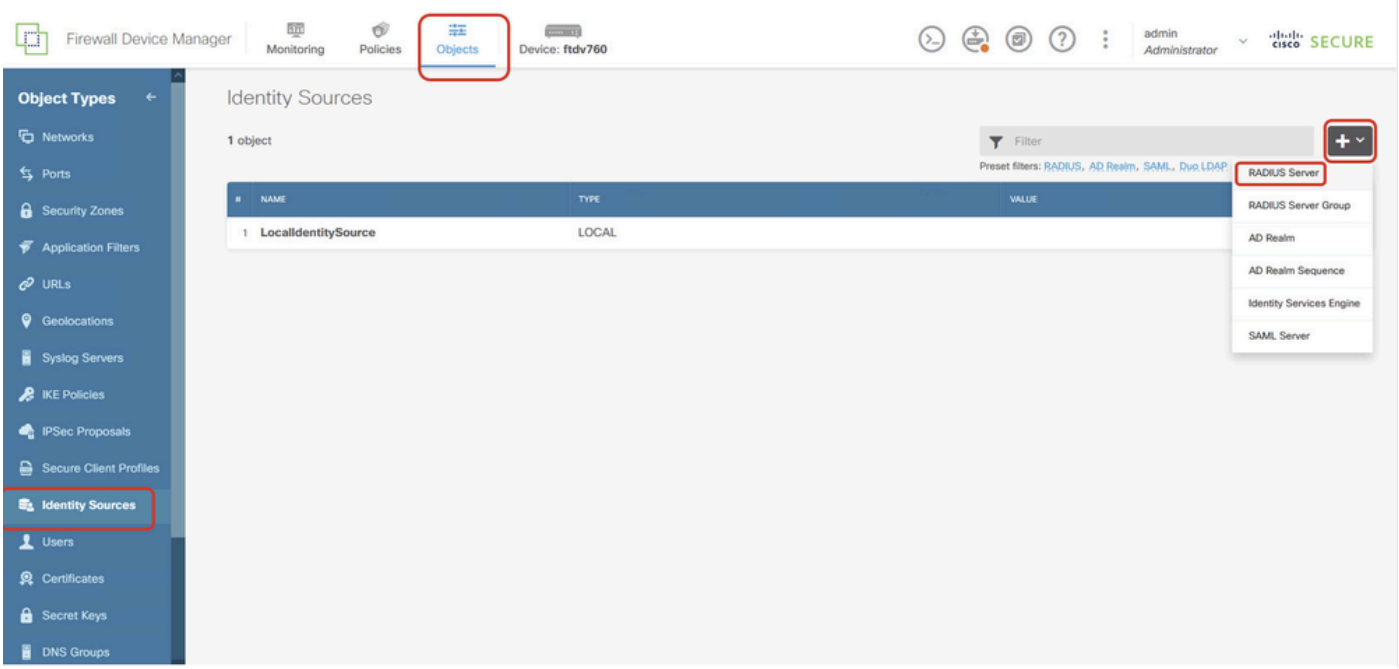
Nom commun : vpn.example.com



Créer_Certificat_5

Étape 7 : création de la source d'identité du serveur RADIUS

Étape 7.1. Accédez à Objets > Sources d'identité, cliquez sur le bouton + et choisissez Serveur RADIUS.



Créer_Source_Rayon_1

Étape 7.2. Fourniture des informations nécessaires sur le serveur RADIUS Cliquez sur le bouton OK.

Name : demo_ise

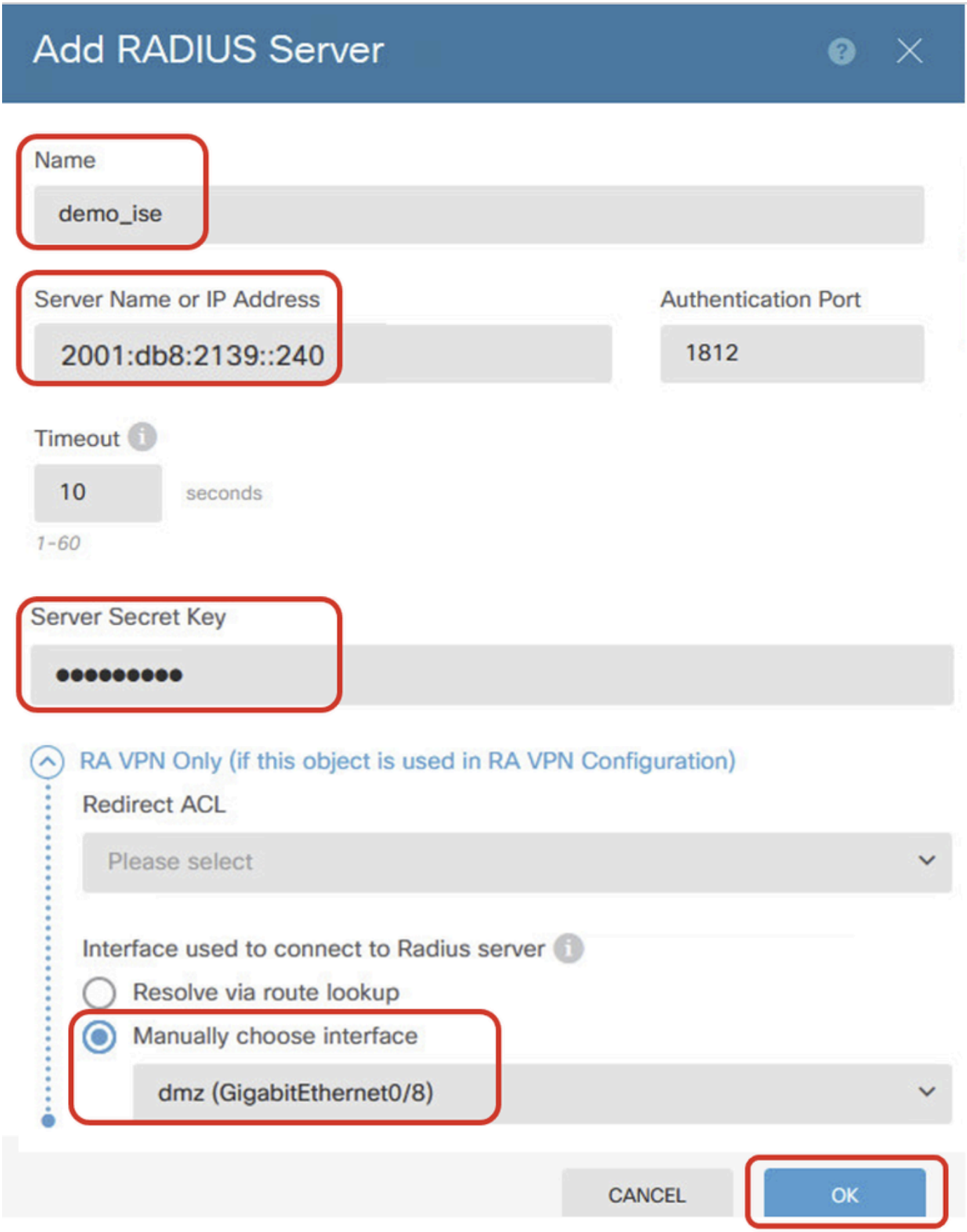
Nom ou adresse IP du serveur : 2001:db8:2139::240

Port d'authentification : 1812 (default)

timeout : 10 (default)

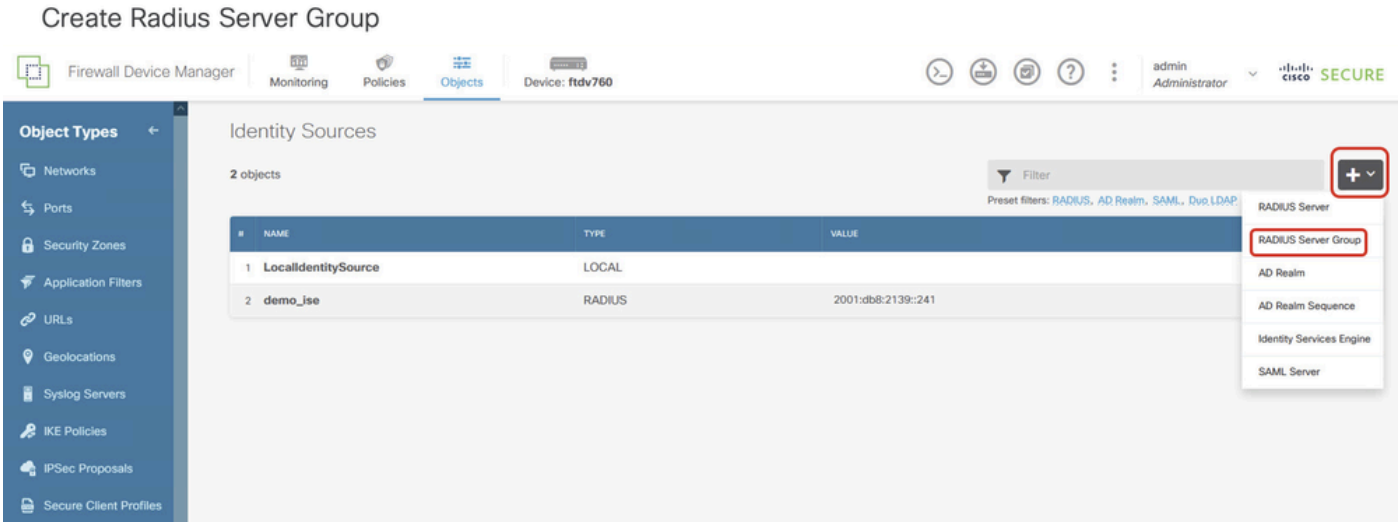
Clé secrète du serveur : cisco

Interface utilisée pour la connexion au serveur Radius : Sélectionnez manuellement l'interface. Dans cet exemple, choisissez dmz (GigabitEthernet0/8).



Créer_Source_Rayon_2

Étape 7.3. Accédez à Objets > Sources d'identité. Cliquez sur le bouton + et choisissez RADIUS Server Group.



Créer_Source_Rayon_3

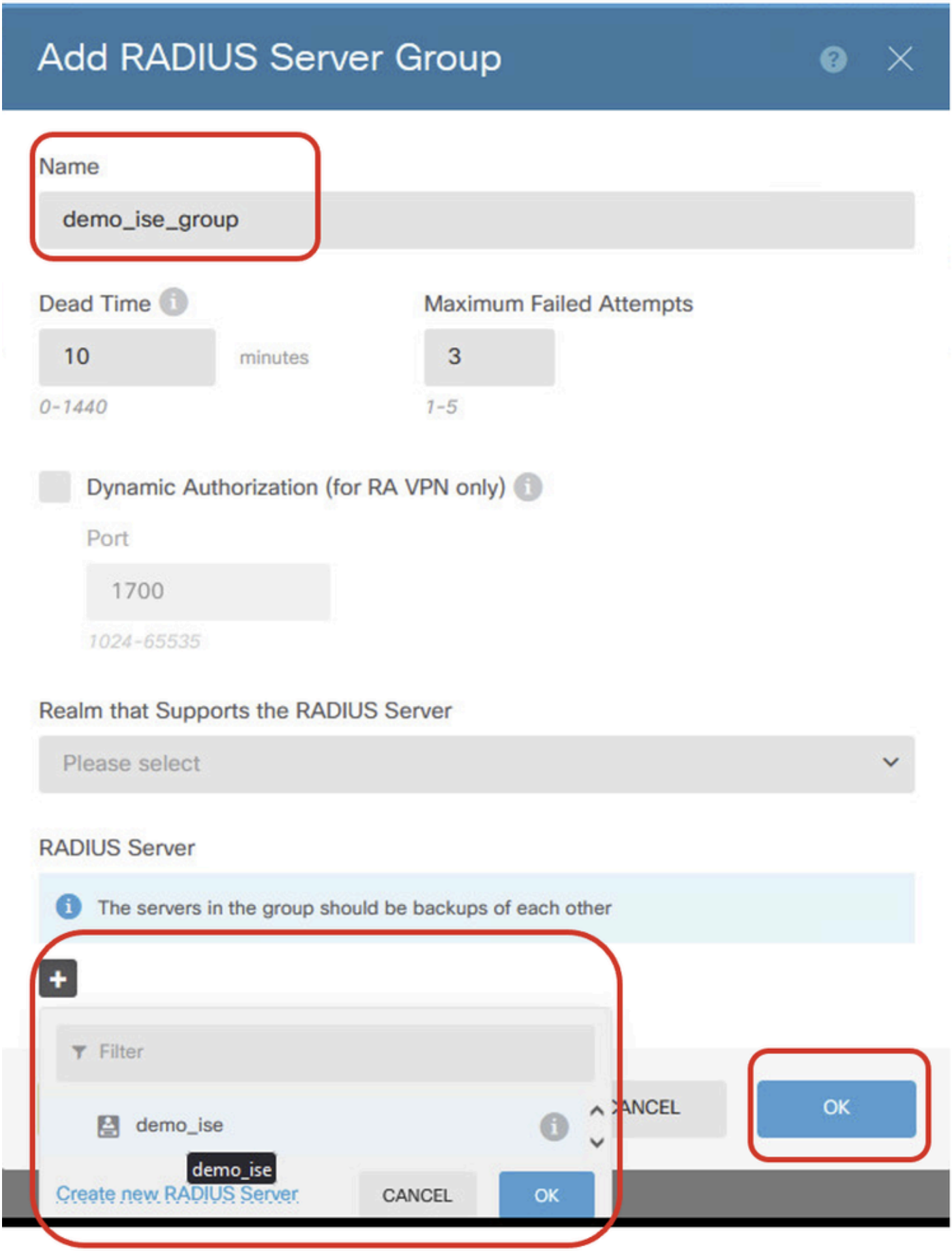
Étape 7.4. Fournissez les informations nécessaires sur le groupe de serveurs RADIUS. Cliquez sur le bouton OK.

Name : demo_ise_group

Heure d'arrêt : 10 (default)

Nombre maximal de tentatives infructueuses : 3 (default)

Serveur RADIUS : Cliquez sur le bouton +, sélectionnez le nom créé à l'étape 6.2. Dans cet exemple, il s'agit de demo_ise.



Créer_Source_Rayon_4

Étape 8 : création de la stratégie de groupe utilisée pour le réseau RAVPN Dans cet exemple, la bannière personnalisée et le paramètre de délai d'attente sont configurés à des fins de démonstration. Vous pouvez les modifier en fonction de vos besoins réels.

Étape 8.1. Accédez à Remote Access VPN > View Configuration. Cliquez sur Stratégies de groupe dans la barre latérale gauche, puis cliquez sur le bouton +.

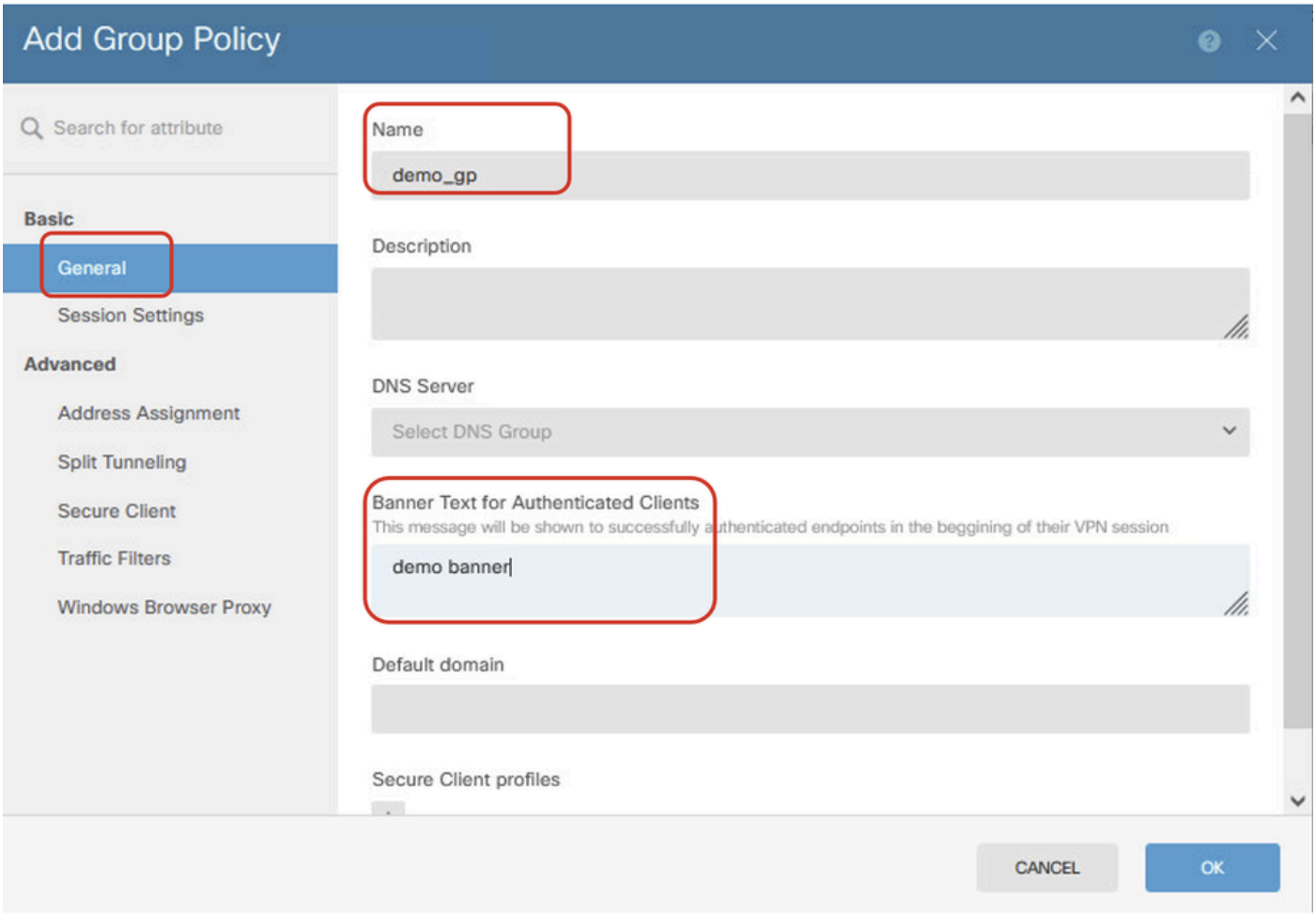


Créer_Stratégie_Groupe_1

Étape 8.2. Cliquez sur Général et fournissez les informations nécessaires.

Name : gp_démo

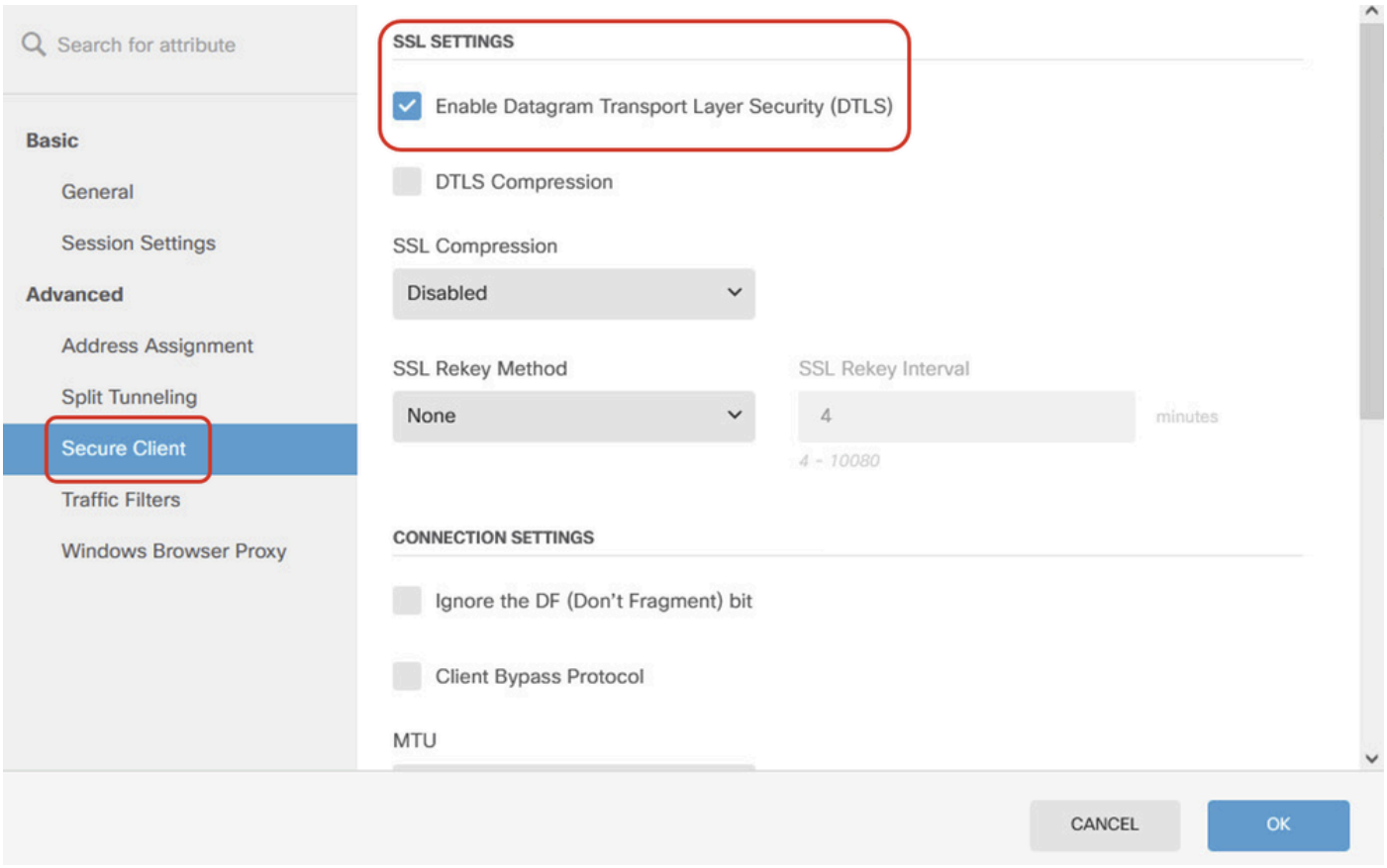
Texte de bannière pour les clients authentifiés : bannière de démonstration



Créer_Stratégie_Groupe_2

Étape 8.3. Cliquez sur Secure Client et fournissez les informations nécessaires.

Cochez Enable Datagram Transport Layer Security (DTLS).

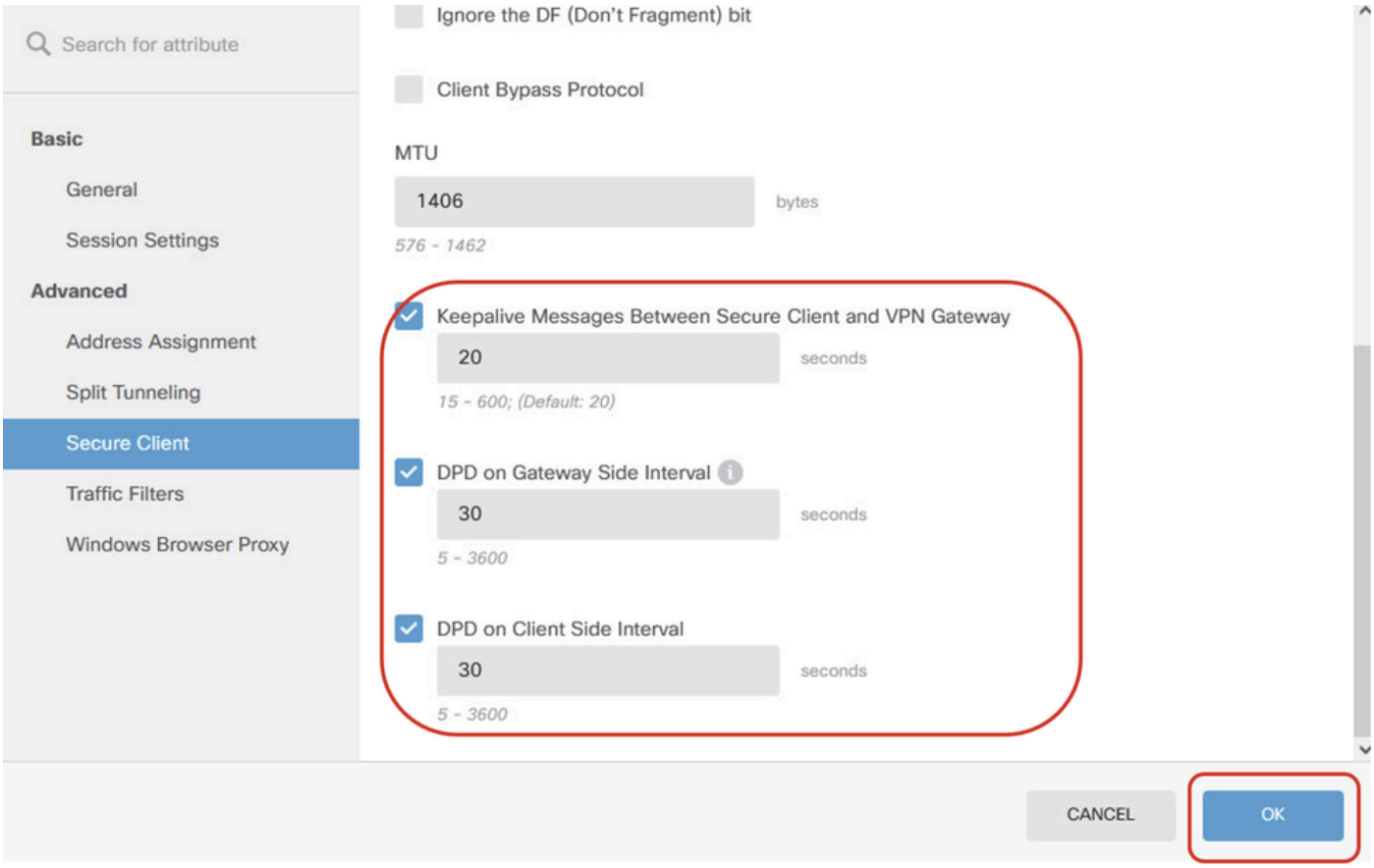


Créer_Stratégie_Groupe_3

Vérifiez les messages Keepalive entre le client sécurisé et la passerelle VPN (valeur par défaut).

Cochez DPD on Gateway Side Interval (valeur par défaut).

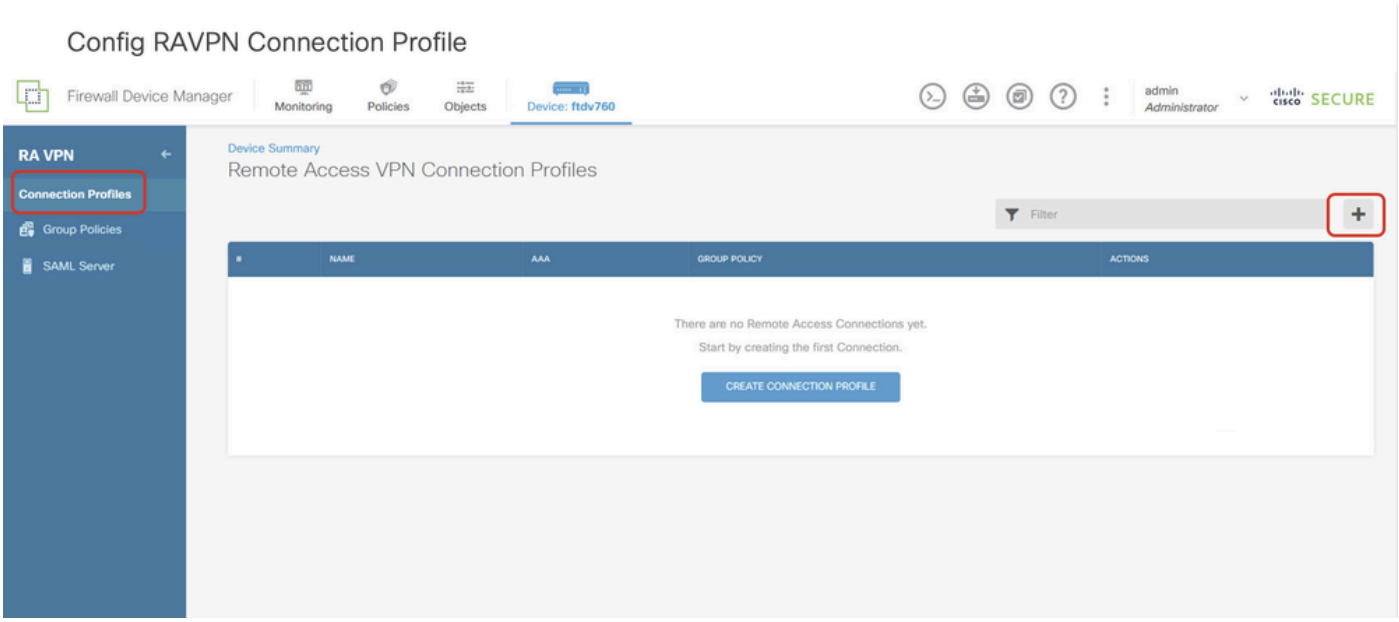
Cochez DPD on Client Side Interval (valeur par défaut).



Create_Group_Policy_3_Cont

Étape 9 : création d'un profil de connexion RAVPN

Étape 9.1. Accédez à Remote Access VPN > View Configuration. Cliquez sur Profil de connexion dans la barre latérale gauche, puis cliquez sur le bouton + afin de démarrer l'Assistant.

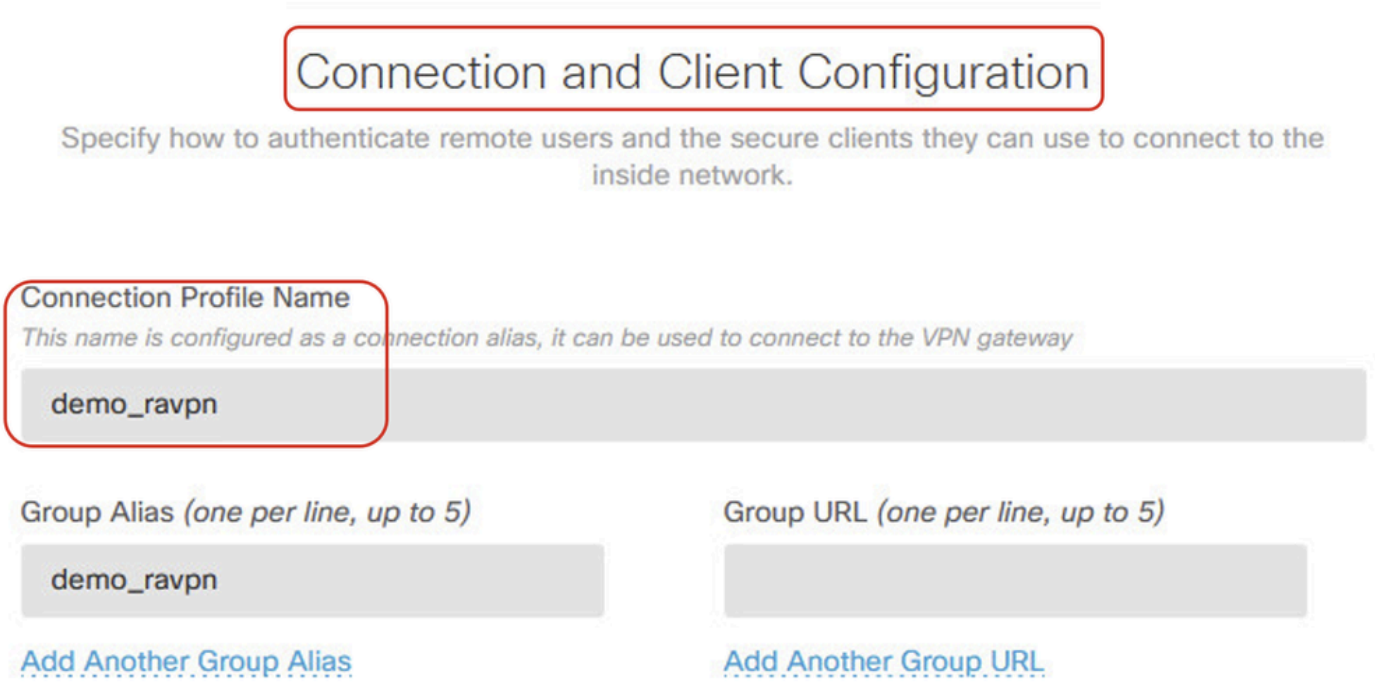


Assistant_Création_RAVPN_1

Étape 9.2. Fournissez les informations nécessaires dans la section Connection and Client Configuration et cliquez sur le bouton NEXT.

Nom du profil de connexion : démo_ravpn

Alias de groupe : démo_ravpn



Create_RAVPN_Wizard_2_Conn_Name

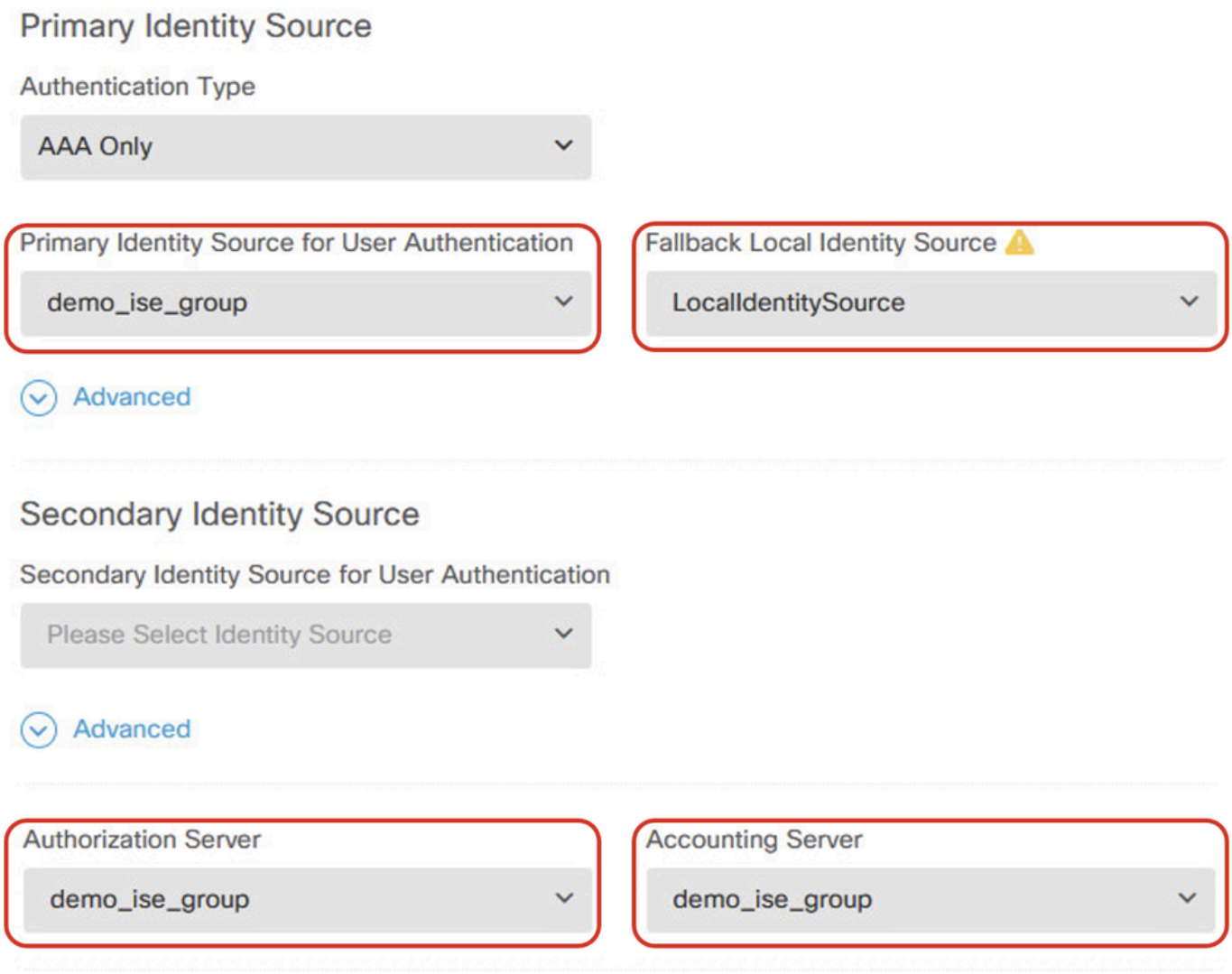
Source d'identité principale > Type d'authentification : AAA uniquement

Source d'identité principale > Source d'identité principale : demo_ise_group (nom configuré à l'étape 7.4.)

Source d'identité locale de secours : IdentitéLocaleSource

Serveur d'autorisation : demo_ise_group (nom configuré à l'étape 7.4.)

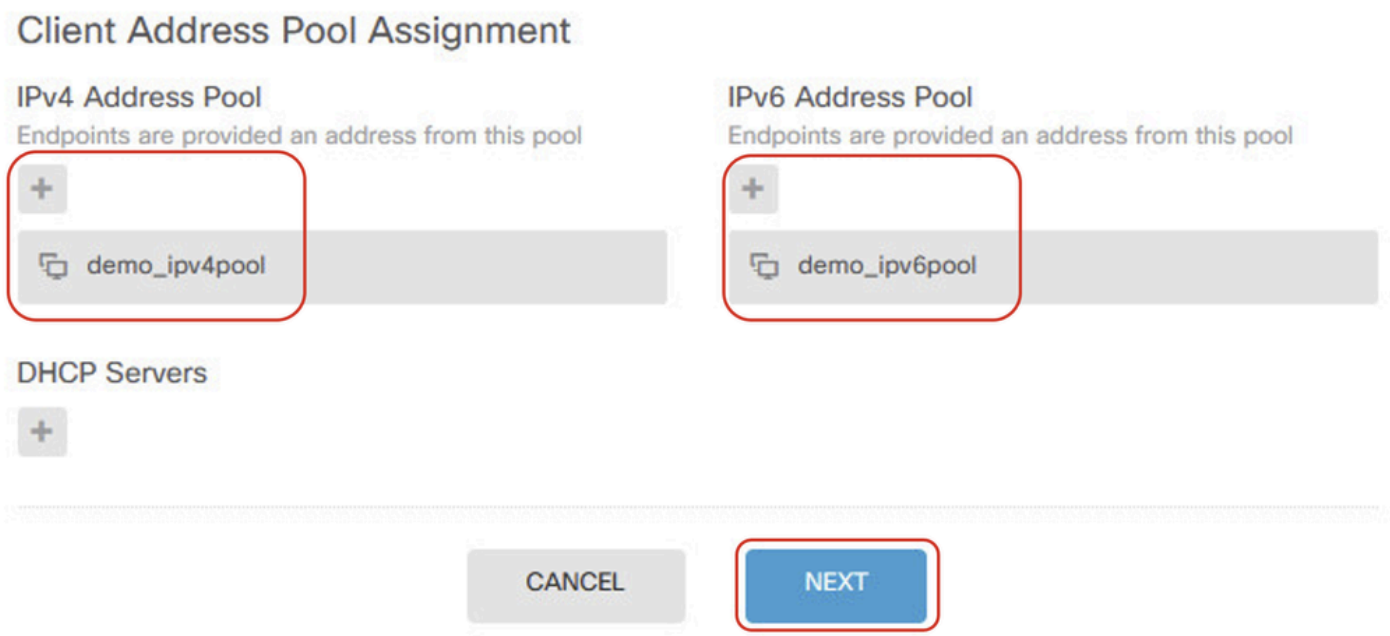
Serveur de comptabilité : demo_ise_group (nom configuré à l'étape 7.4.)



Create_RAVPN_Wizard_2_Identity_Source

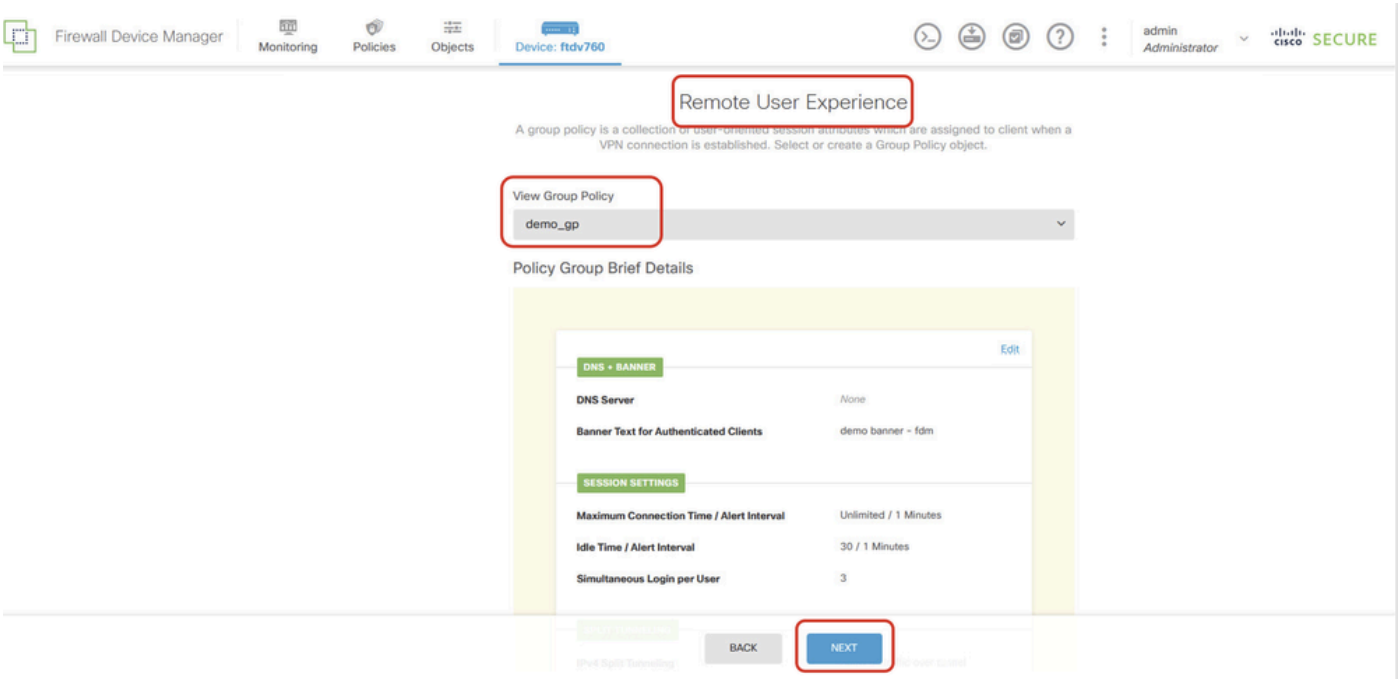
Pool d'adresses IPv4 : demo_ipv4pool (nom configuré à l'étape 4.2.)

Pool d'adresses IPv6 : demo_ipv6pool (nom configuré à l'étape 4.2.)



Create_RAVPN_Wizard_2_Address_Pool

Étape 9.3. Choisissez la stratégie de groupe configurée à l'étape 8.2. dans la section Expérience utilisateur à distance, et cliquez sur le bouton SUIVANT.

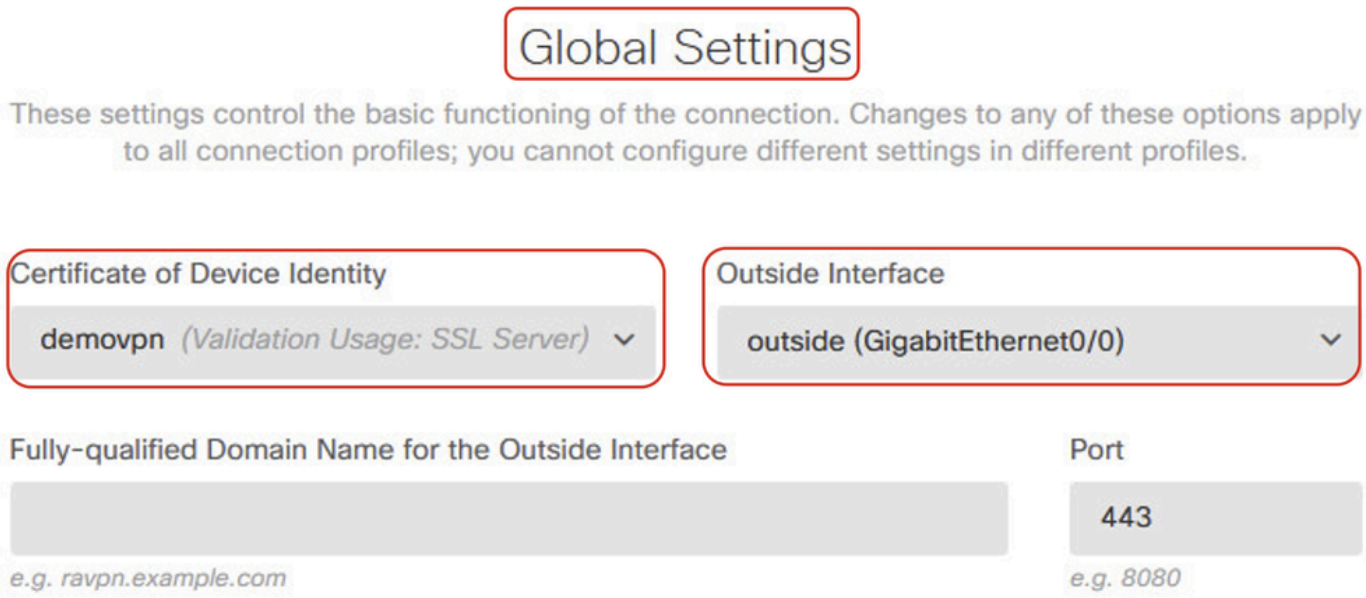


Assistant_Création_RAVPN_3

Étape 9.4. Fournissez les informations nécessaires dans la section Global Setting et cliquez sur le bouton NEXT.

Certificat d'identité du périphérique : demovpn (nom configuré à l'étape 6.3.)

Interface externe : extérieur



Assistant_Création_RAVPN_4

Contrôle d'accès pour le trafic VPN : Cochez la case Bypass Access Control policy for decrypted traffic (sysopt permit-vpn).

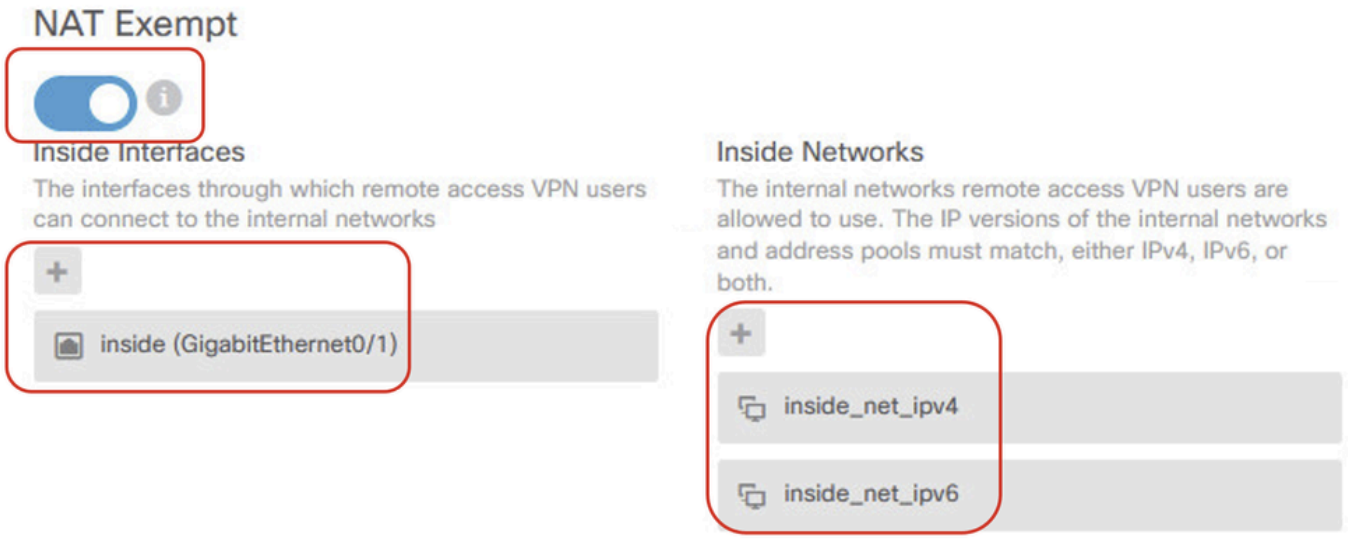


Create_RAVPN_Wizard_4_VPN_ACP

Exemption NAT : Cliquez sur le curseur jusqu'à la position Activé

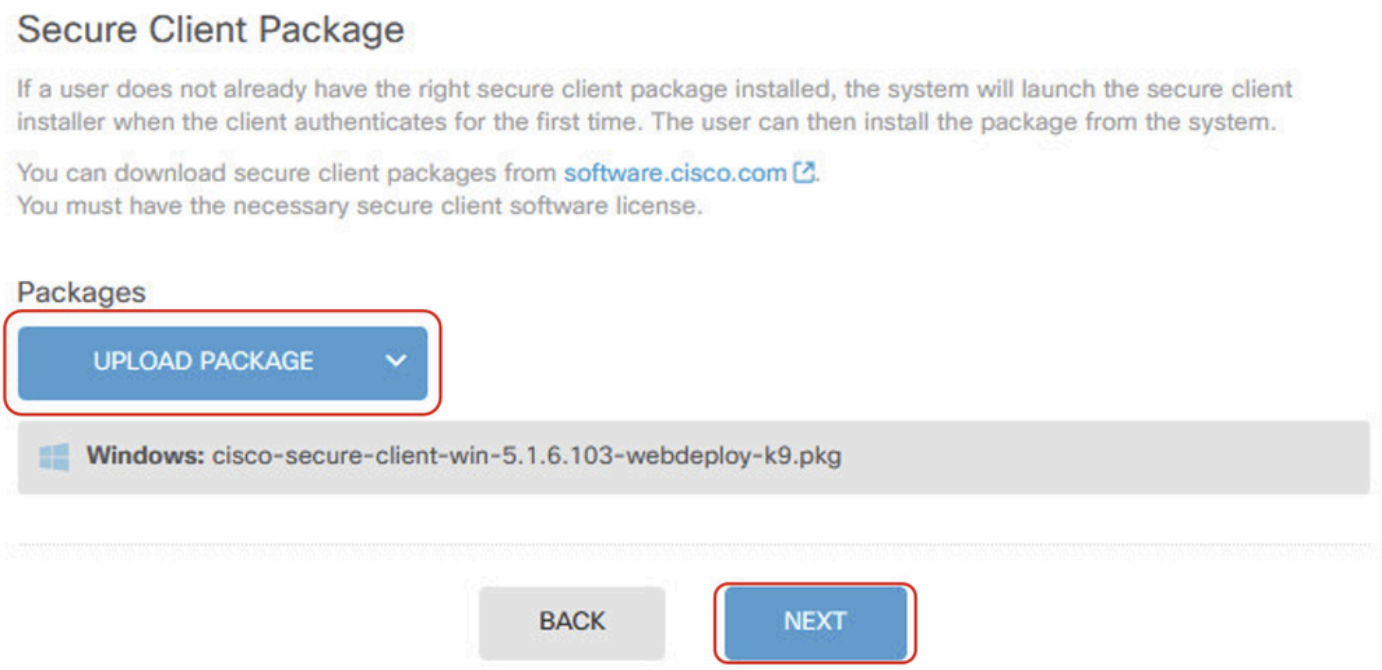
Interfaces internes : intérieur

Réseaux internes : inside_net_ipv4, inside_net_ipv6 (nom configuré à l'étape 5.2.)



Create_RAVPN_Wizard_4_VPN_NATExempt

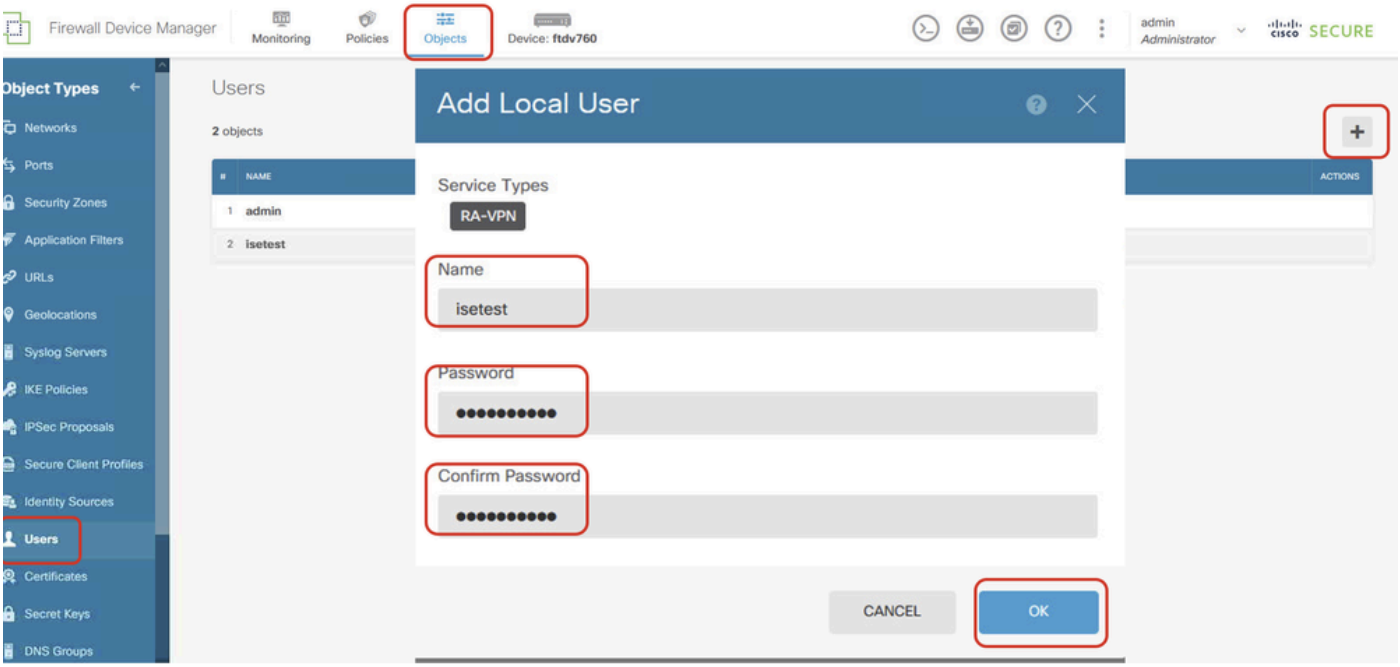
Package client sécurisé : Cliquez sur UPLOAD PACKAGE et téléchargez le package en conséquence. Dans cet exemple, le package Windows est téléchargé.



Create_RAVPN_Wizard_4_Image

Étape 9.5. Révision du résumé Si vous devez modifier quelque chose, cliquez sur le bouton BACK. Si tout va bien, cliquez sur le bouton FINISH.

Étape 10. Créez un utilisateur local si la source d'identité locale de secours est choisie avec LocalIdentitySource à l'étape 9.2. Le mot de passe de l'utilisateur local doit être le même que celui configuré sur ISE.



Créer_Utilisateur_Local

Étape 11. Déployez les modifications de configuration.

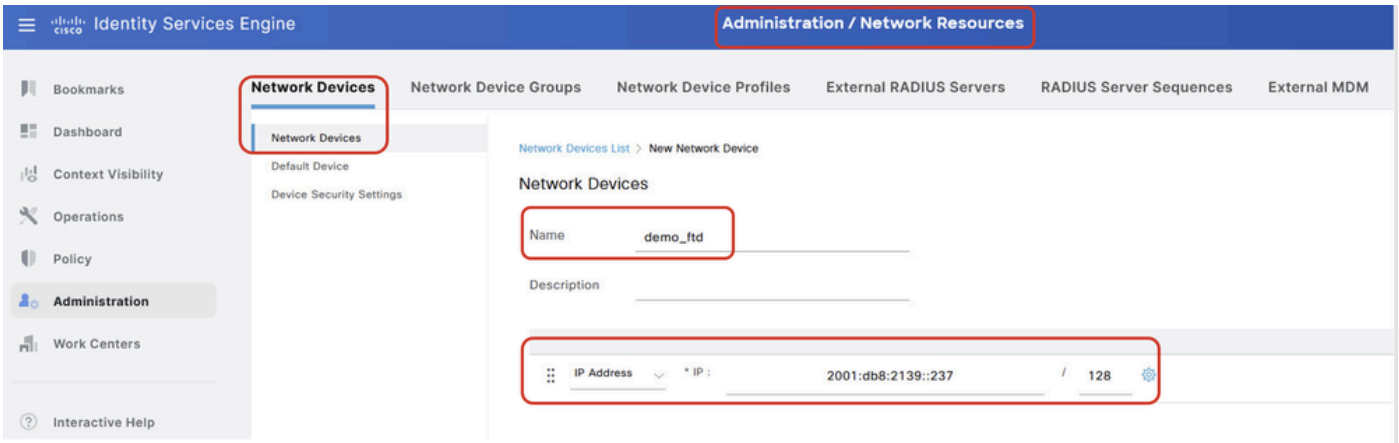


Déployer_les modifications

Configurations sur ISE

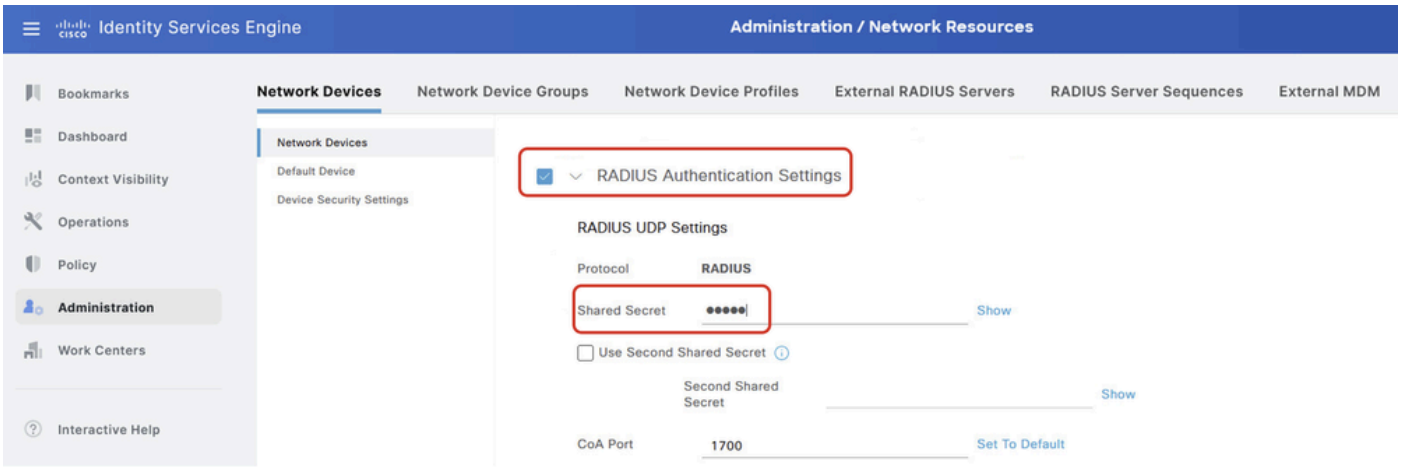
Étape 12. Création de périphériques réseau

Étape 12.1. Accédez à Administration > Network Resources > Network Devices, cliquez sur Add, fournissez le Name, IP Address et faites défiler la page vers le bas.



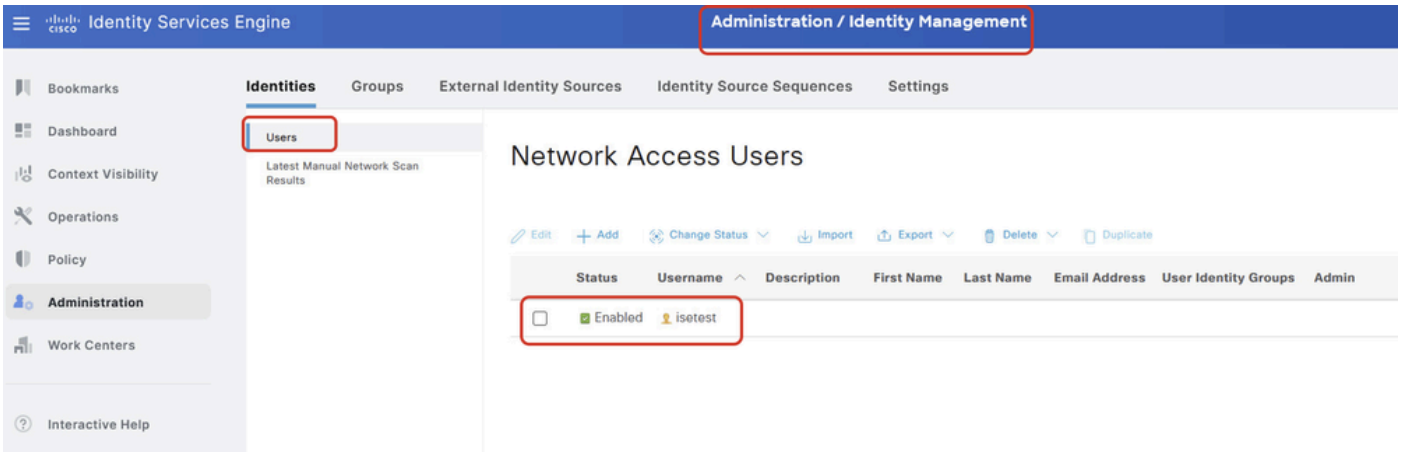
Périphériques_réseau_de_création

Étape 12.2. Cochez la case RADIUS Authentication Settings. Saisissez le secret partagé et cliquez sur Submit.



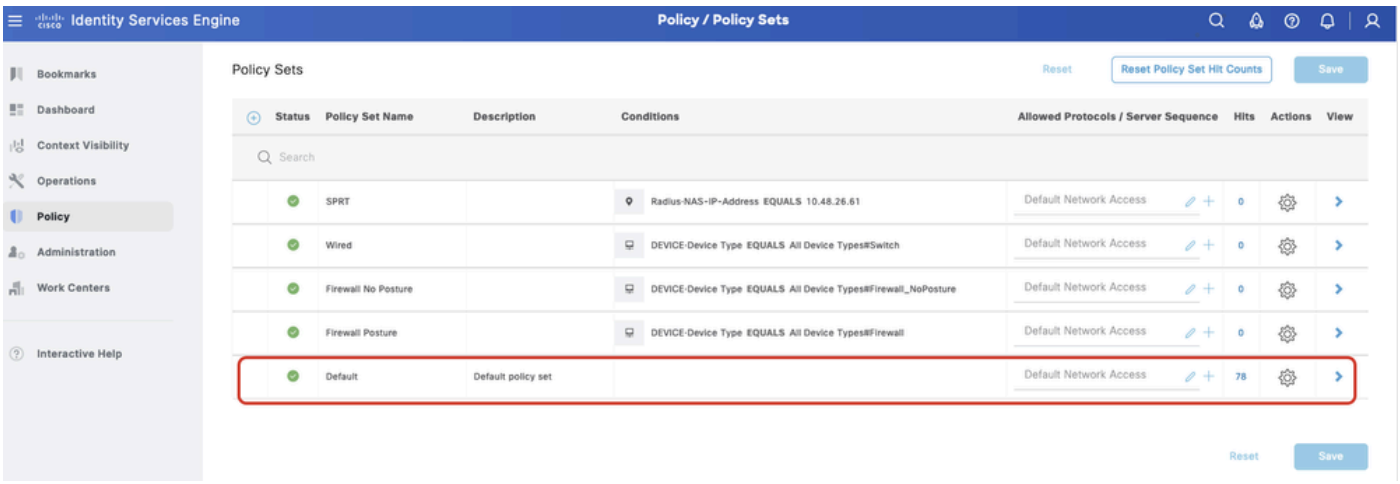
Create_Network_Devices_Cont

Étape 13. Créer des utilisateurs d'accès au réseau Accédez à Administration > Identity Management > Identities. Cliquez sur Add afin de créer un nouvel utilisateur. Le mot de passe est identique pour l'utilisateur local FDM créé à l'étape 10. afin de garantir le fonctionnement du secours.



Créer_Utilisateur_ISE

Étape 14. (Facultatif) Créez un nouvel ensemble de stratégies avec une règle d'authentification et une règle d'autorisation personnalisées. Dans cet exemple, le jeu de stratégies par défaut est utilisé à des fins de démonstration.

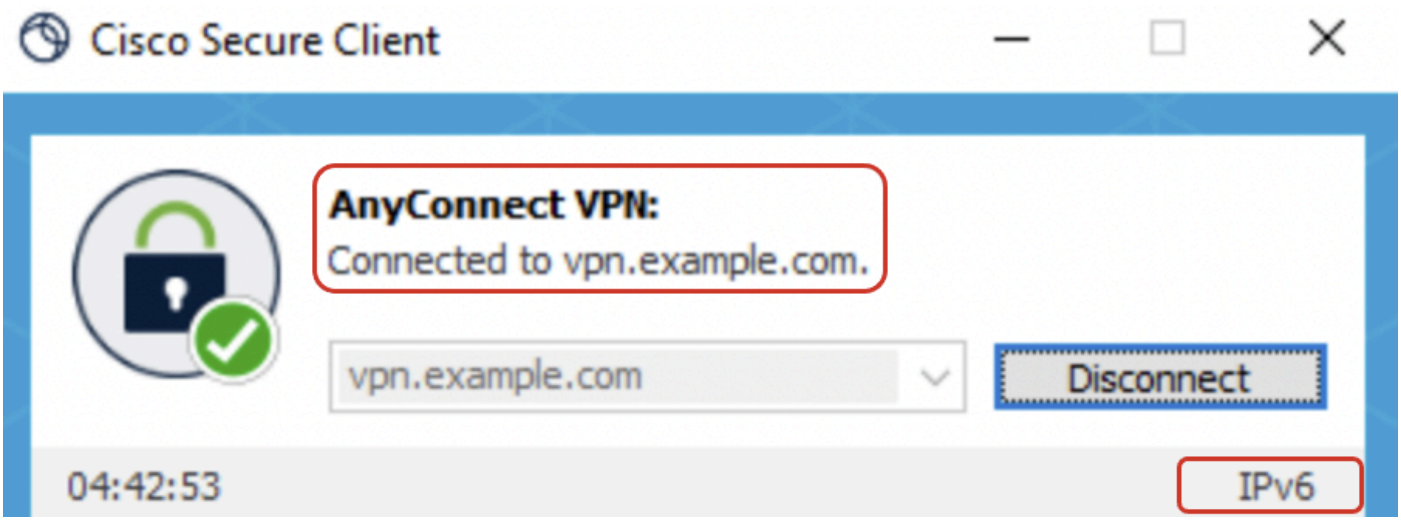


ISE_Default_Policy_Set

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 15. Connectez la passerelle VPN via l'adresse IPv6 sur le client. La connexion VPN a réussi.



Vérifier_Connexion_Réussite

Étape 16. Accédez à la CLI de FTD via SSH ou la console. Exécutez la commande show vpn-sessiondb detail anyconnect dans la CLI FTD (Lina) afin de vérifier les détails de la session VPN.

<#root>

```
ftdv760# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed
```

Username : isetest

Index : 2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 15402 Bytes Rx : 14883
Pkts Tx : 10 Pkts Rx : 78
Pkts Tx Drop : 0 Pkts Rx Drop : 10
Group Policy : demo_gp Tunnel Group : demo_ravpn
Login Time : 05:22:30 UTC Mon Dec 23 2024
Duration : 0h:05m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a81e0a000020006768f396
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 2.1

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Encryption : none Hashing : none
TCP Src Port : 58339 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes
Client OS : win
Client OS Ver: 10.0.19042
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 2.2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

```
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 58352
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 25 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 152
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 2.3
```

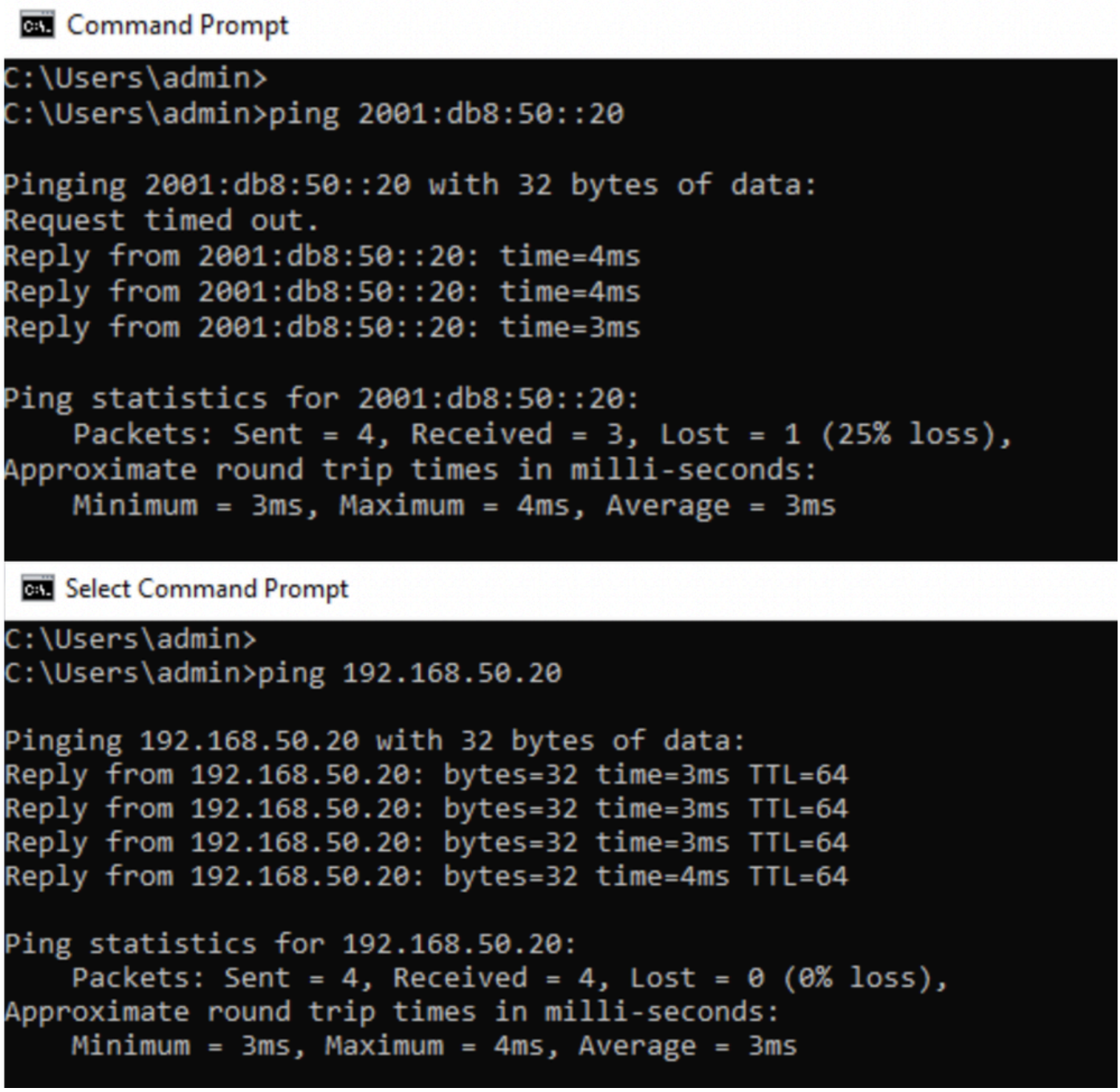
Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

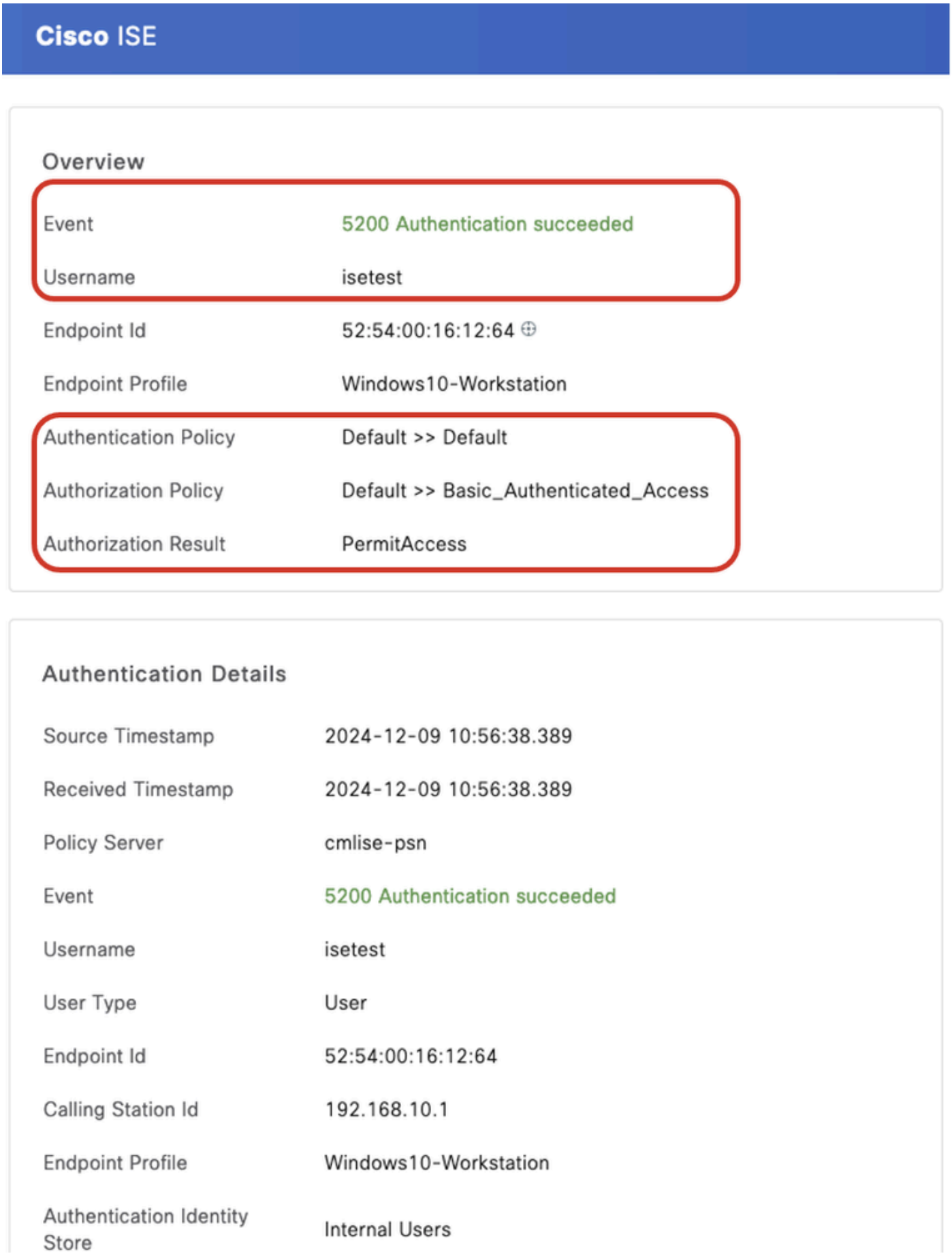
```
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 58191
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 560 Bytes Rx : 14731
Pkts Tx : 8 Pkts Rx : 76
Pkts Tx Drop : 0 Pkts Rx Drop : 10
```

Étape 17. Test Ping sur le client. Dans cet exemple, le client exécute avec succès une requête ping à la fois sur les adresses IPv4 et IPv6 du serveur.



Vérifier_Cisco_Secure_Client_Ping

Étape 18. Le journal en direct du rayon ISE indique une authentification réussie.



ISE_Authentication_Success_Log

Étape 19. Tester l’authentification FTD passe à LOCAL lorsque FTD ne peut pas atteindre ISE.

Étape 19.1. Lorsque l'authentification FTD passe à ISE, exécutez la commande show aaa-server dans l'interface de ligne de commande FTD (Lina) afin de vérifier les statistiques.

Dans cet exemple, il n'existe aucun compteur pour LOCAL et l'authentification est dirigée vers le serveur RADIUS.

<#root>

```
ftdv760# show aaa-server

Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 08:18:11 UTC Fri Dec 6 2024
Number of pending requests              0
Average round trip time                 0ms
Number of authentication requests       0
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       0
Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius


Server Address:  2001:db8:2139::240


Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 02:56:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms

Number of authentication requests       1  <== Increased


Number of authorization requests        1  <== Increased


Number of accounting requests           1  <== Increased


Number of retransmissions               0

Number of accepts                       2  <== Increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
```

Étape 19.2. Arrêtez l’interface ISE pour simuler que FTD ne peut pas recevoir de réponse d’ISE.

<#root>

```
ftdv760# ping 2001:db8:2139::240


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:2139::240, timeout is 2 seconds:
???
Success rate is 0 percent (0/3)
```

Étape 19.3. Le client lance la connexion VPN et entre le même nom d’utilisateur et mot de passe que celui créés à l’étape 10, la connexion VPN est toujours réussie.

Exécutez de nouveau la commande show aaa-server dans l'interface de ligne de commande FTD (Lina) afin de vérifier la statistique, l'authentification, l'autorisation et les compteurs d'acceptation pour LOCAL ont maintenant augmenté. Le compteur d'acceptation du serveur RADIUS n'a pas augmenté.

<#root>

```
ftdv760# show aaa-server
Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 03:36:26 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 0ms

Number of authentication requests       1  <== Increased


Number of authorization requests        1  <== Increased


Number of accounting requests           0
Number of retransmissions               0

Number of accepts                       2  <== Increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius

Server Address:  2001:db8:2139::240
Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 03:36:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms
```

```
Number of authentication requests       2
Number of authorization requests        1
Number of accounting requests           6
Number of retransmissions               0

Number of accepts                       2  <== Not increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      6
Number of unrecognized responses        0
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Vous pouvez exécuter ces commandes sur FTD Lina afin de dépanner la section VPN.

debug webvpn 255
debug webvpn anyconnect 255

Vous pouvez collecter un fichier DART auprès du client pour le dépannage VPN afin de déterminer si le problème provient du client sécurisé. Pour obtenir des conseils, reportez-vous au document CCO pertinent Collect DART Bundle for Secure Client.

Vous pouvez exécuter ces commandes sur FTD Lina afin de dépanner la section Radius.

```
ftdv760# debug radius ?

all      All debug options
decode   Decode debug option
dynamic-authorization CoA listener debug option
session  Session debug option
user     User debug option
<cr>
```

```
ftdv760# debug aaa ?

accounting
authentication
authorization
common
condition
internal
shim
```

```
url-redirect
<cr>
```

Vous pouvez les examiner afin de dépanner le problème lié au trafic après une connexion VPN réussie.

1. Capturez le trafic sur FTD Lina afin de voir si Lina abandonne le trafic, en vous reportant à ce document CCO ; Utilisez Firepower Threat Defense Captures et Packet Tracer - Cisco.
2. Vérifiez la stratégie de contrôle d'accès afin de vous assurer que le trafic VPN associé est autorisé à passer si la stratégie de contournement du contrôle d'accès pour le trafic déchiffré est désactivée.
3. Examiner l'exemption NAT afin de s'assurer que le trafic VPN est exclu de la NAT.

Informations connexes

- Guide de configuration FDM de RAVPN - Cisco
- Collecter l'offre groupée DART pour client sécurisé - Cisco
- Utiliser les captures Firepower Threat Defense et Packet Tracer - Cisco
- Dépannage de Cisco Secure Client - Cisco
- Assistance technique de Cisco et téléchargements

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.