Configurer AAA et l'authentification certifiée pour le client sécurisé sur FTD via FDM

Table des matières

Introduction

Ce document décrit les étapes de configuration de Cisco Secure Client sur SSL sur FTD géré par FDM avec AAA et authentification de certificat.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Device Manager (FDM) virtuel
- Défense contre les menaces de pare-feu (FTD) virtuelle
- Flux d'authentification VPN

Composants utilisés

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8

- Cisco Secure Client 5.1.4.74

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

Firepower Device Manager (FDM) est une interface de gestion Web simplifiée utilisée pour gérer les périphériques Cisco Firepower Threat Defense (FTD). Le Gestionnaire de périphériques Firepower permet aux administrateurs réseau de configurer et de gérer leurs appareils FTD sans utiliser le centre de gestion Firepower (FMC), plus complexe. FDM fournit une interface utilisateur intuitive pour les opérations de base telles que la configuration des interfaces réseau, des zones de sécurité, des politiques de contrôle d'accès et des VPN, ainsi que pour la surveillance des performances des périphériques et des événements de sécurité. Il est adapté aux déploiements de petite et moyenne taille pour lesquels une gestion simplifiée est souhaitée.
Ce document décrit comment intégrer des noms d'utilisateur pré-remplis avec Cisco Secure Client sur FTD géré par FDM.
Si vous gérez FTD avec FMC, veuillez vous reporter au guide Configurer AAA et authentification certifiée pour client sécurisé sur FTD via FMC.

Il s'agit de la chaîne de certificats avec le nom commun de chaque certificat utilisé dans le document.

- CA : ftd-ra-ca-common-name
- Certificat client : sslVPNClientCN
- Certificat du serveur : 192.168.1.200

Diagramme du réseau

Cette image présente la topologie utilisée pour l'exemple de ce document.

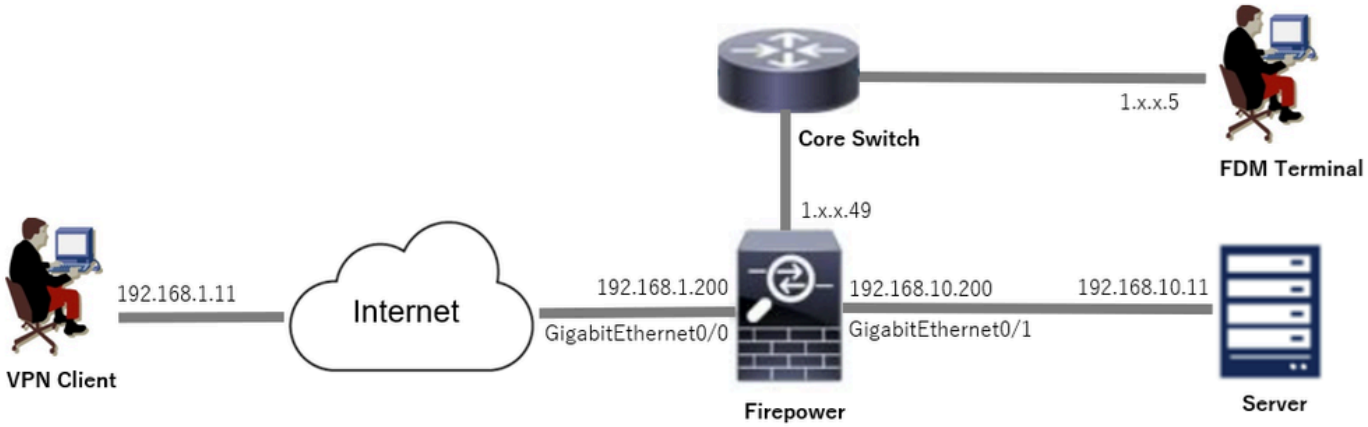


Diagramme du réseau

Configurations

Configuration dans FDM

Étape 1. Configurer l'interface FTD

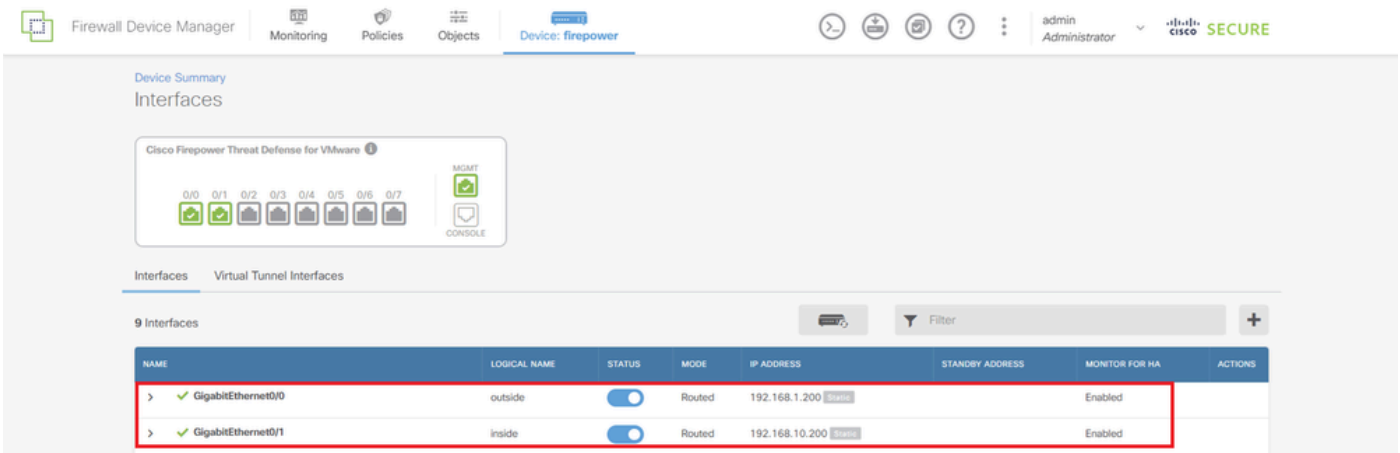
Accédez à Device > Interfaces > View All Interfaces, configurez l'interface interne et externe pour FTD dans l'onglet Interfaces.

Pour GigabitEthernet0/0,

- Nom : extérieur
- Adresse IP : 192.168.1.200/24

Pour GigabitEthernet0/1,

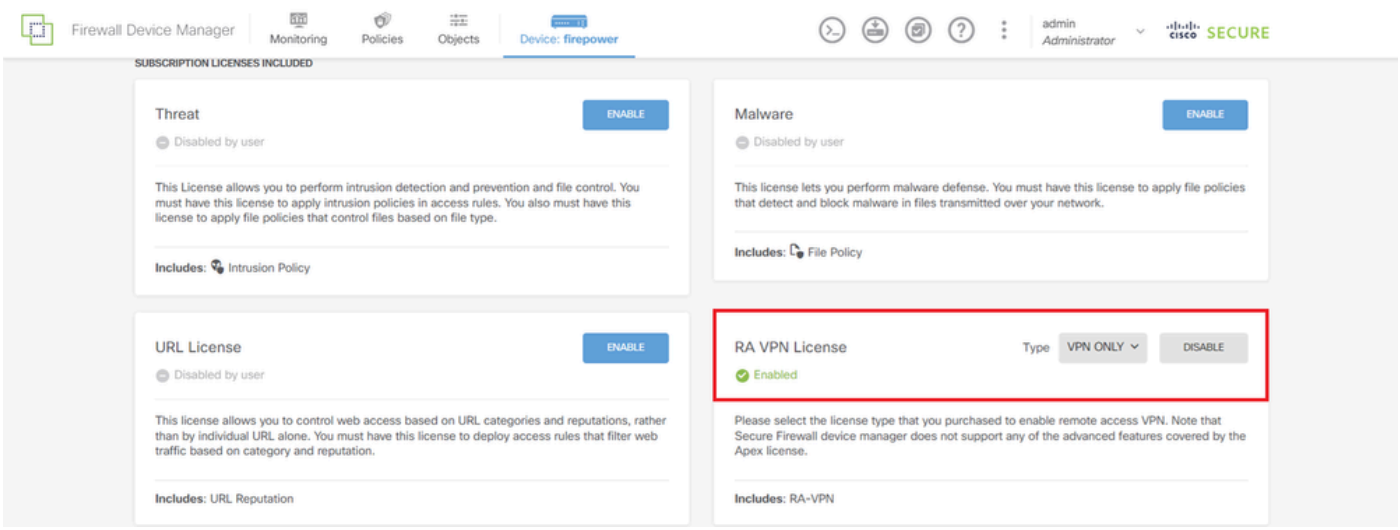
- Nom : à l'intérieur
- Adresse IP : 192.168.10.200/24



Interface FTD

Étape 2. Confirmer la licence Cisco Secure Client

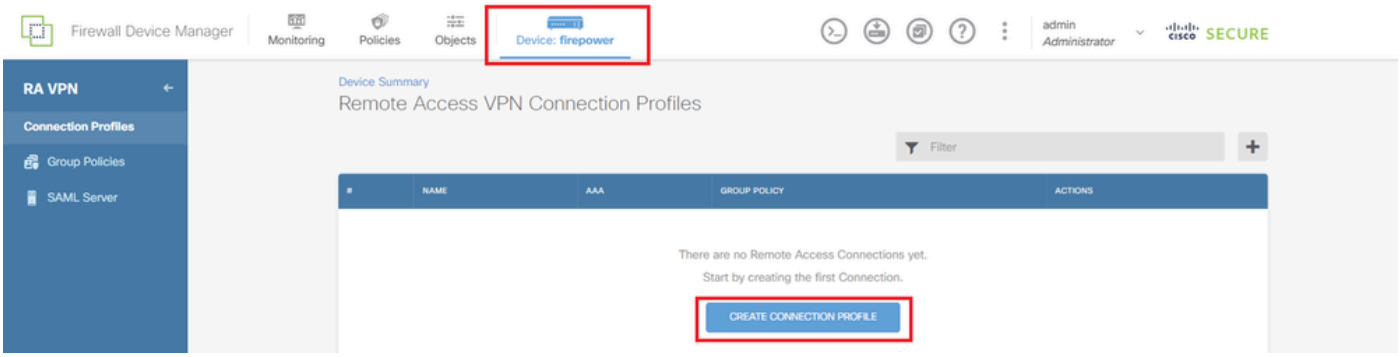
Accédez à Device > Smart License > View Configuration, confirmez la licence Cisco Secure Client dans l'élément RA VPN License.



Licence client sécurisée

Étape 3. Ajouter un profil de connexion VPN d'accès à distance

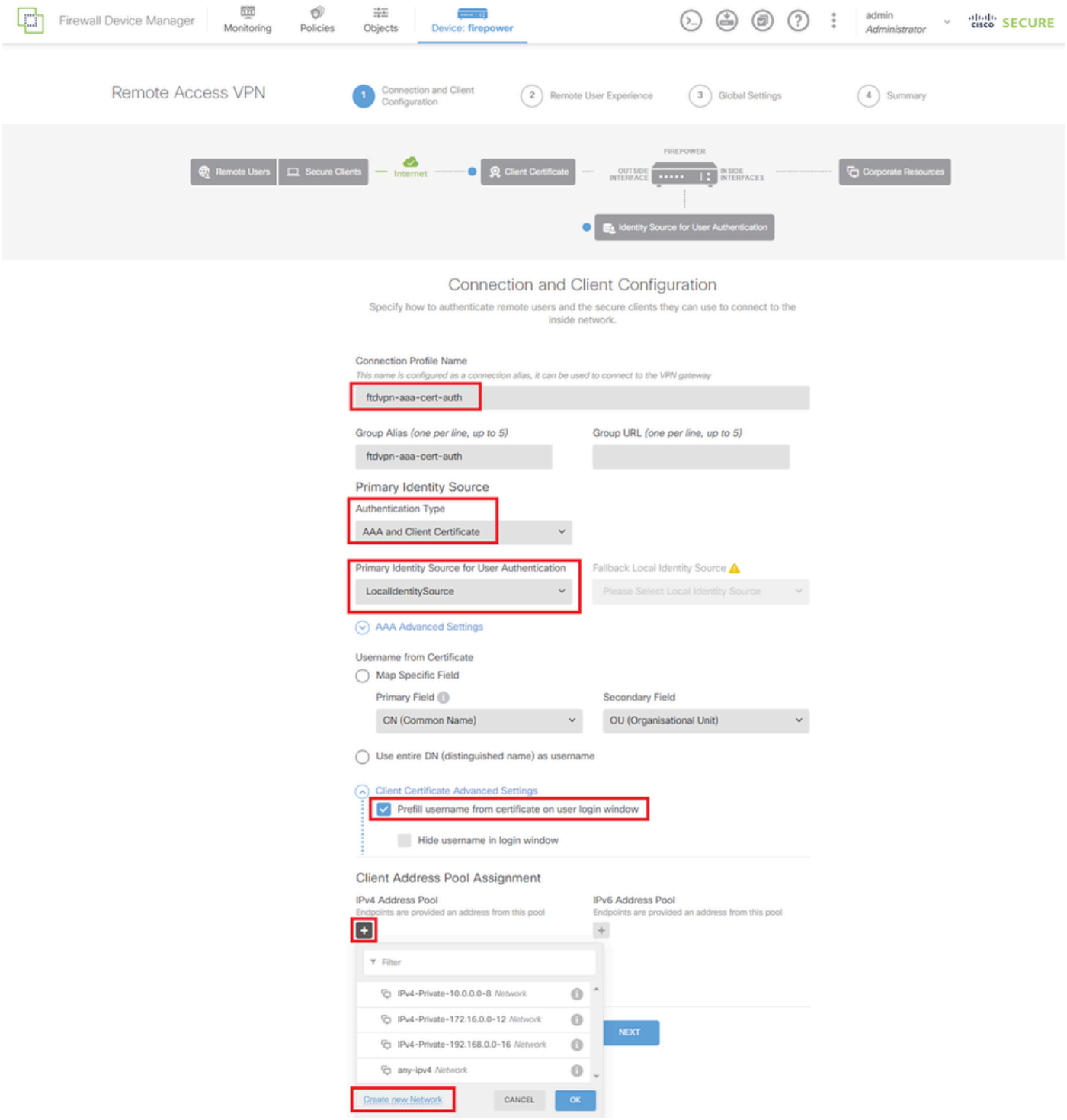
Accédez à Device > Remote Access VPN > View Configuration, cliquez sur le bouton CREATE CONNECTION PROFILE.



Ajouter un profil de connexion VPN d'accès à distance

Entrez les informations nécessaires pour le profil de connexion et cliquez sur le bouton Create new Network dans l'élément IPv4 Address Pool.

- Nom du profil de connexion : ftdvpn-aaa-cert-auth
- Type d'authentification : AAA et certificat client
- Source d'identité principale pour l'authentification utilisateur : LocalIdentitySource
- Paramètres avancés du certificat client : Préremplir le nom d'utilisateur à partir du certificat dans la fenêtre de connexion utilisateur

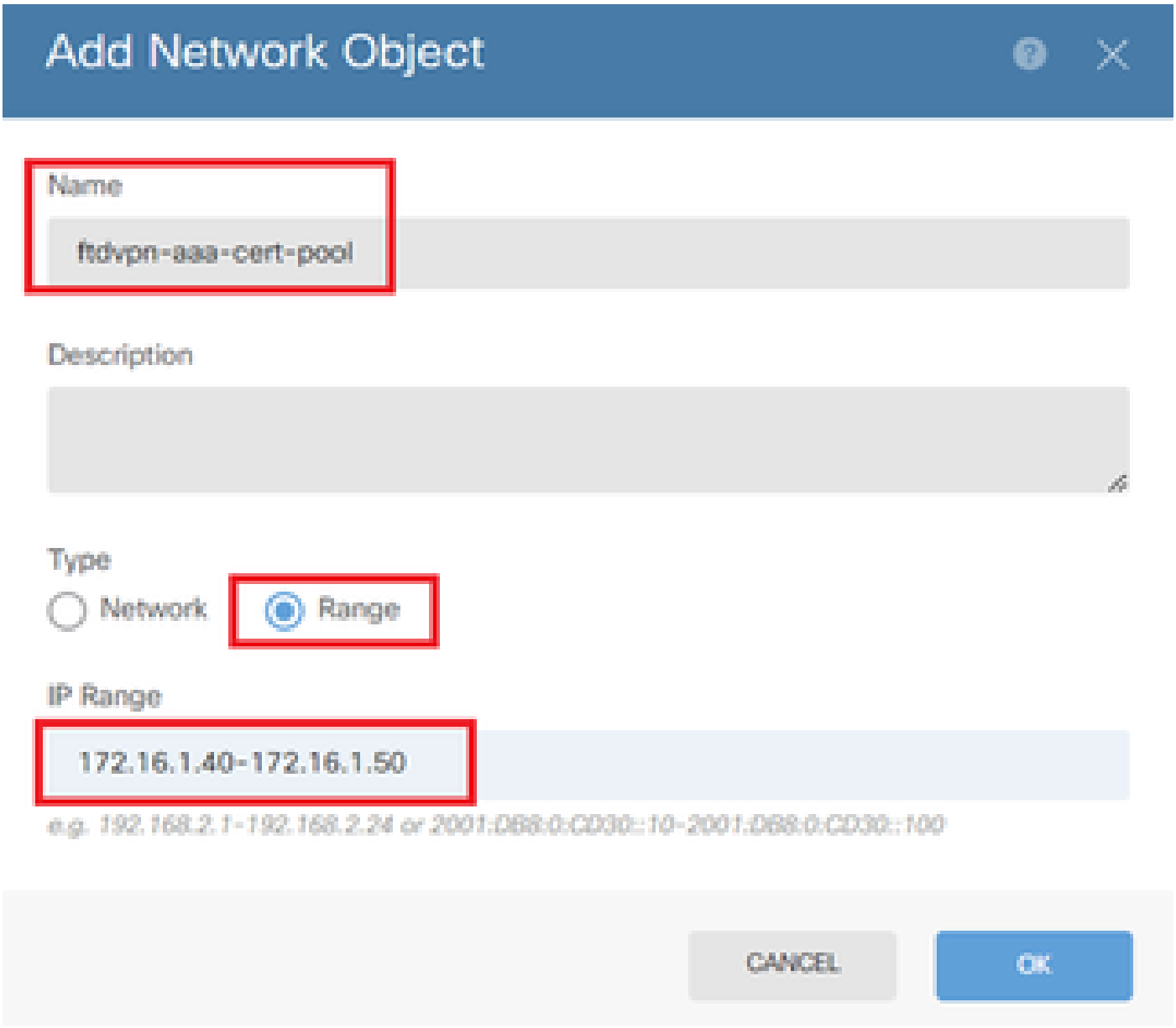


Détails du profil de connexion VPN

Étape 4. Ajouter un pool d'adresses pour le profil de connexion

Entrez les informations nécessaires pour ajouter un nouveau pool d'adresses IPv4. Sélectionnez le nouveau pool d'adresses IPv4 ajouté pour le profil de connexion et cliquez sur Next.

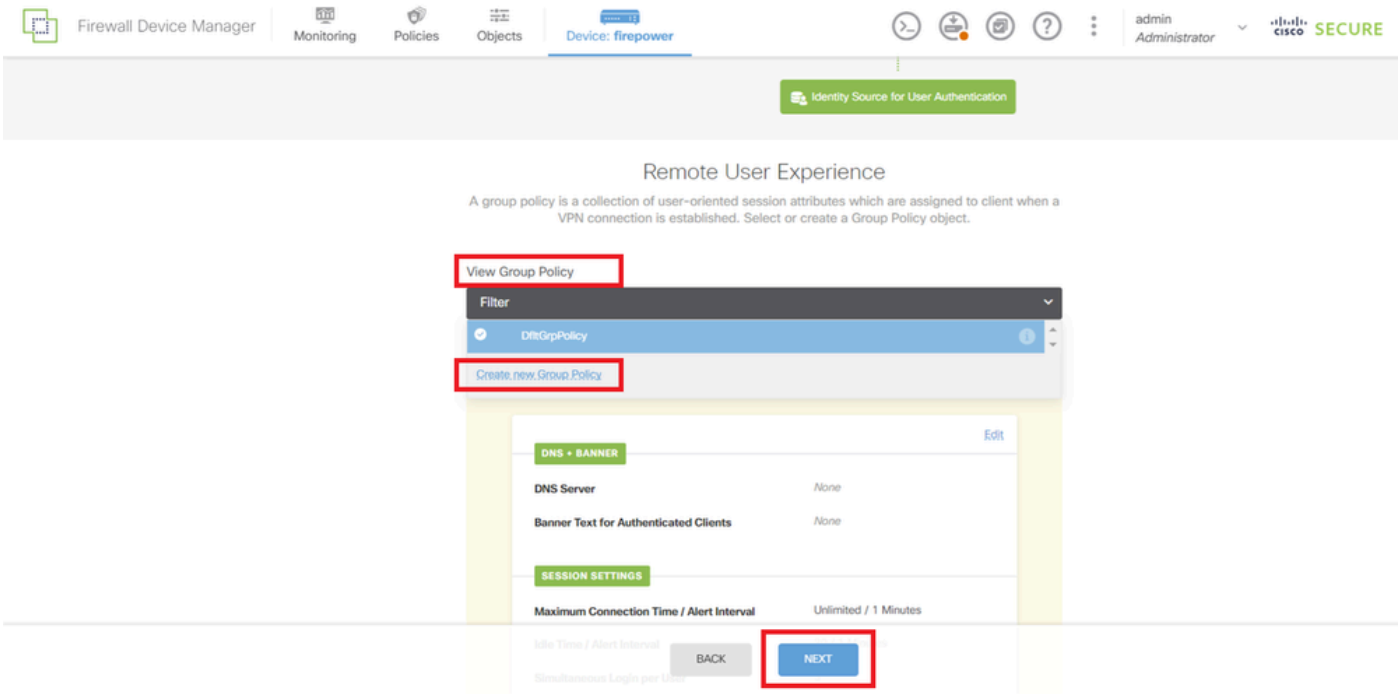
- Nom : ftdvpn-aaa-cert-pool
- Type : Plage
- Plage IP : 172.16.1.40-172.16.1.50



Détails du pool d'adresses IPv4

Étape 5. Ajouter une stratégie de groupe pour le profil de connexion

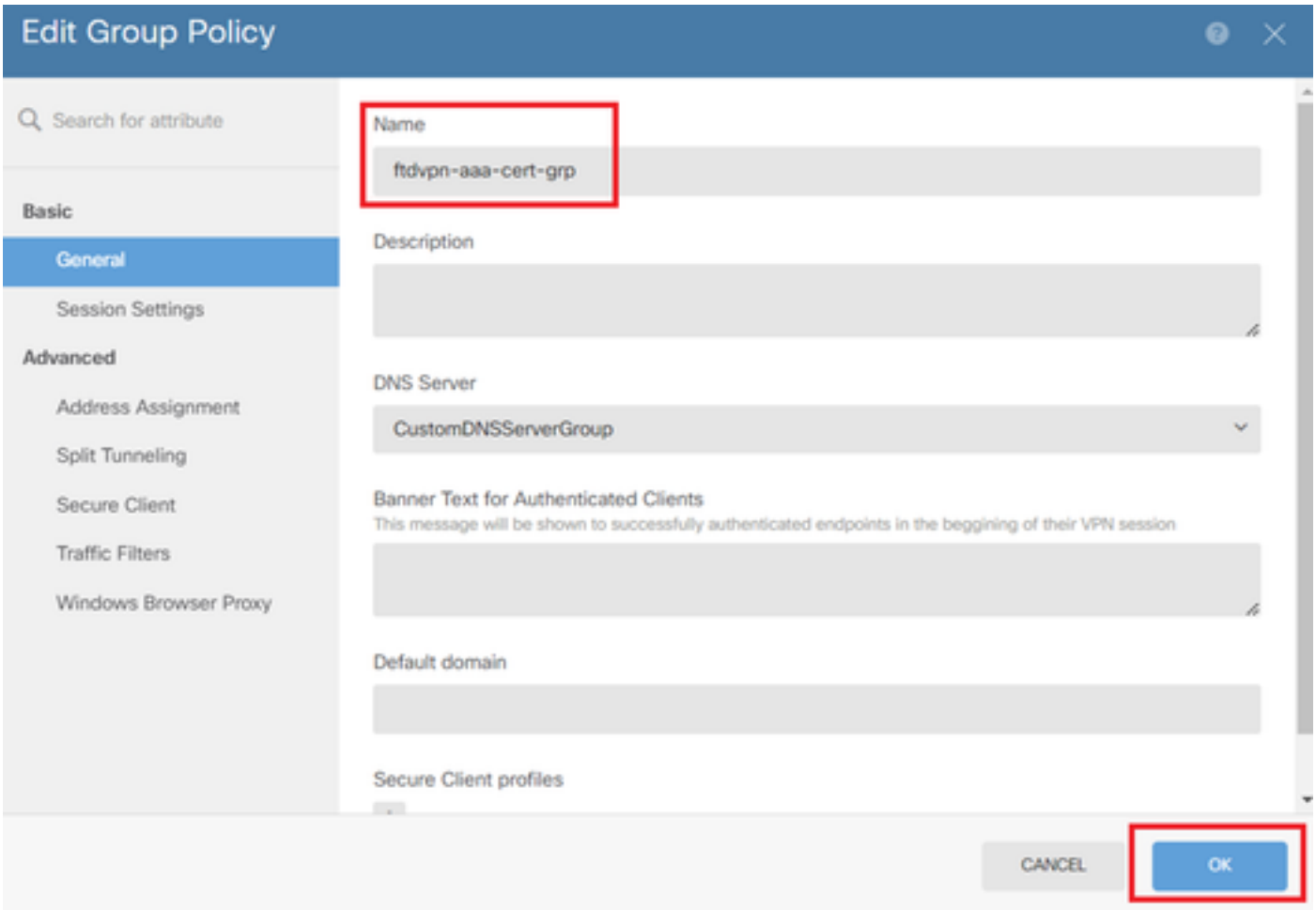
Cliquez sur Créer une nouvelle stratégie de groupe dans l'élément Afficher la stratégie de groupe.



Ajouter une stratégie de groupe

Entrez les informations nécessaires pour ajouter une nouvelle stratégie de groupe et cliquez sur OK bouton. Sélectionnez une nouvelle stratégie de groupe ajoutée pour le profil de connexion.

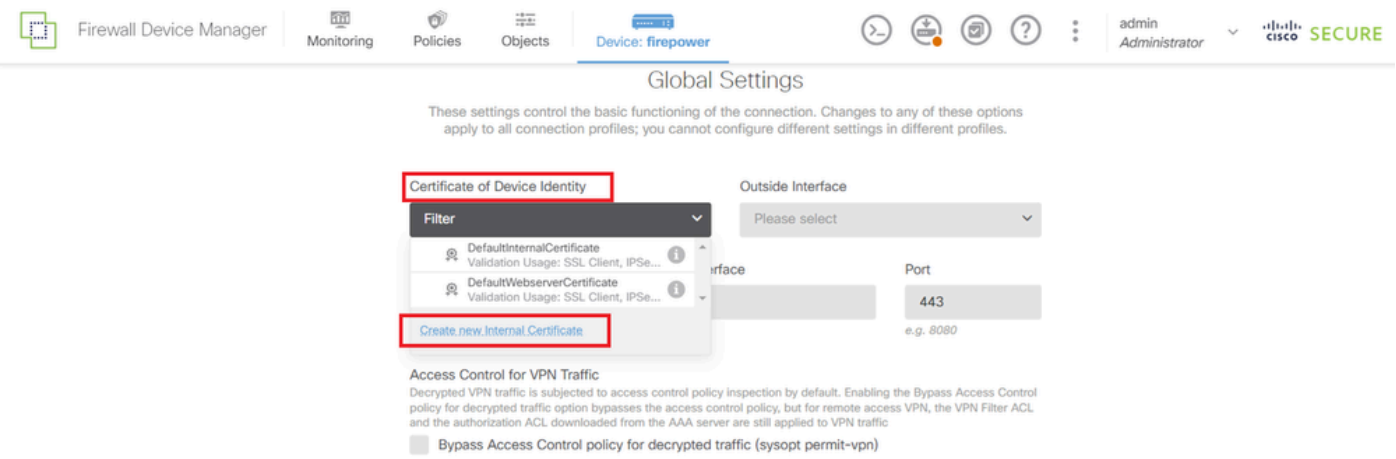
- Nom : ftdvpn-aaa-cert-grp



Détails de la stratégie de groupe

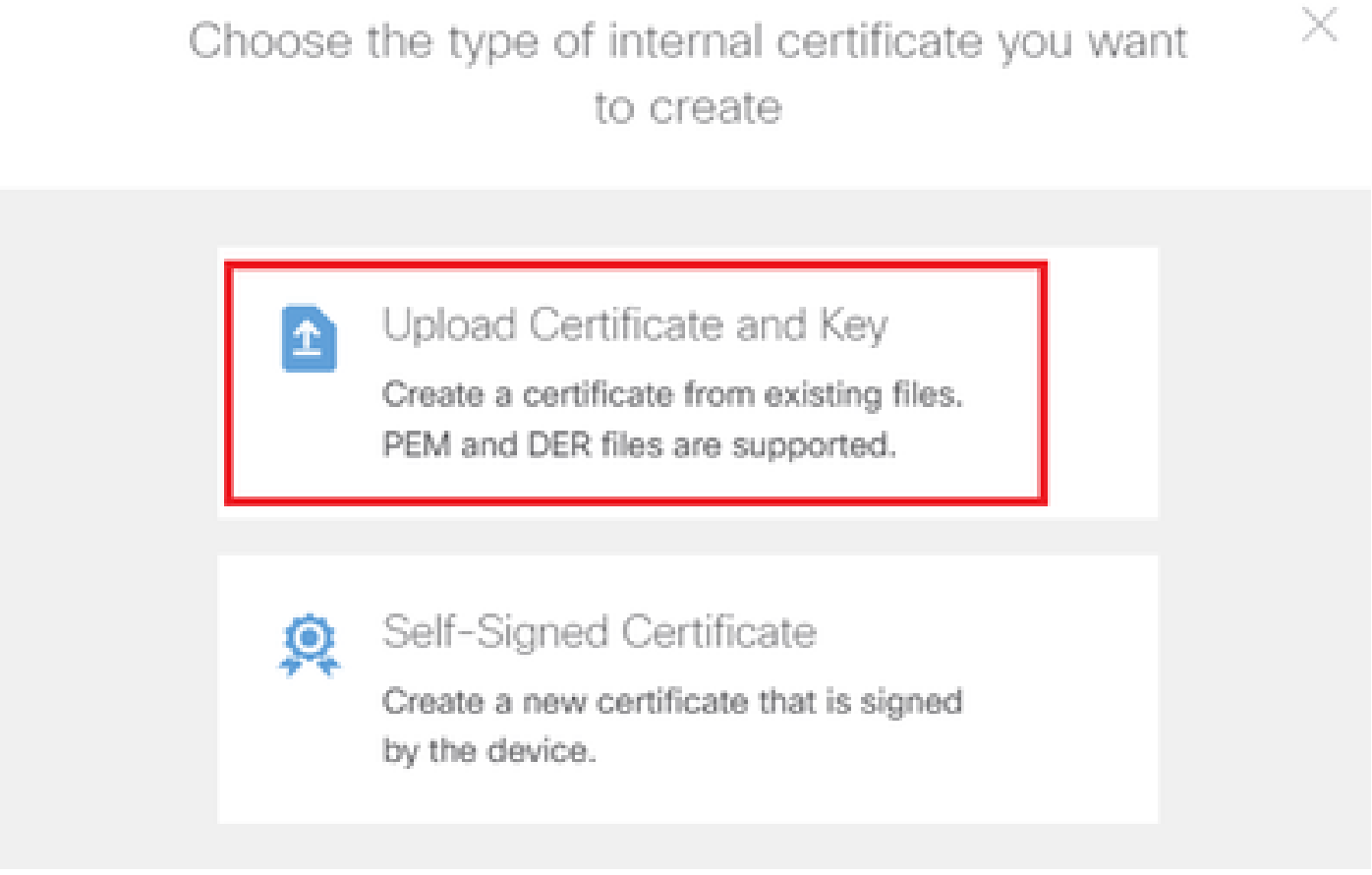
Étape 6. Configurer le certificat d'identité de périphérique et l'interface externe pour le profil de connexion

Cliquez sur Créer un nouveau certificat interne dans l'élément Certificat d'identité de périphérique.



Ajouter un certificat interne

Cliquez sur Télécharger le certificat et la clé.

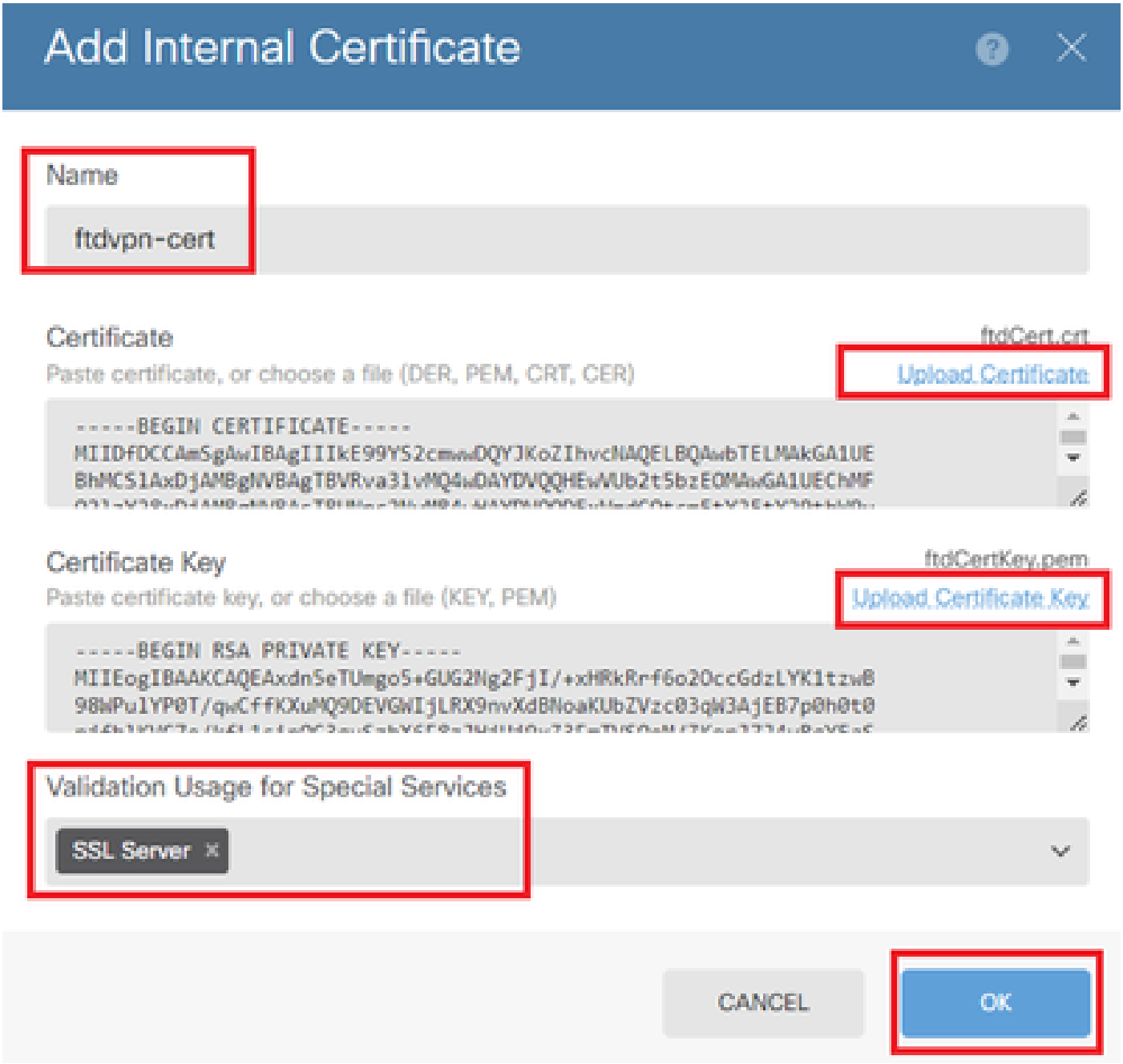


Télécharger le certificat et la clé

Entrez les informations nécessaires pour le certificat FTD, importez un certificat et une clé de

certificat depuis l'ordinateur local, puis cliquez sur le bouton OK.

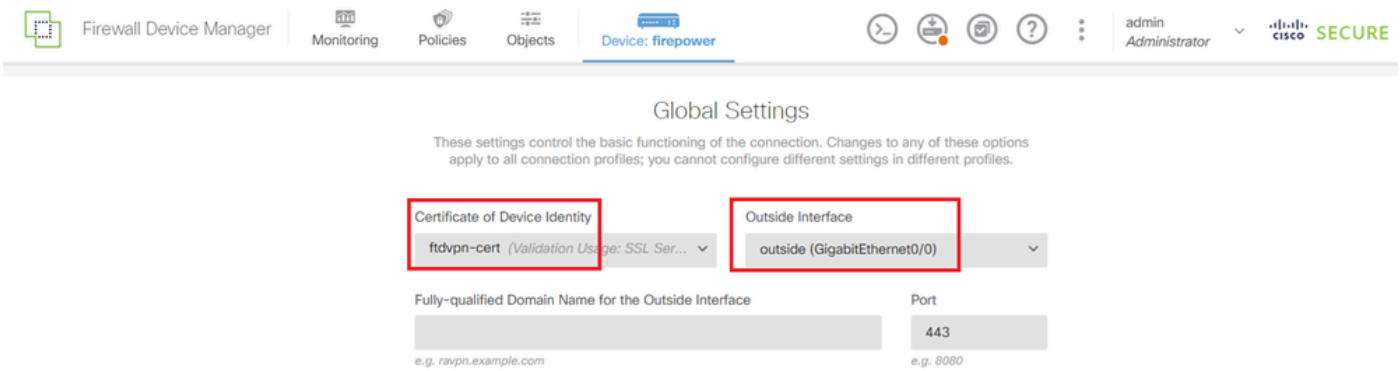
- Nom : ftdvpn-cert
- Utilisation de la validation pour les services spéciaux : serveur SSL



Détails du certificat interne

Sélectionnez Certificate of Device Identity et Outside Interface pour la connexion VPN.

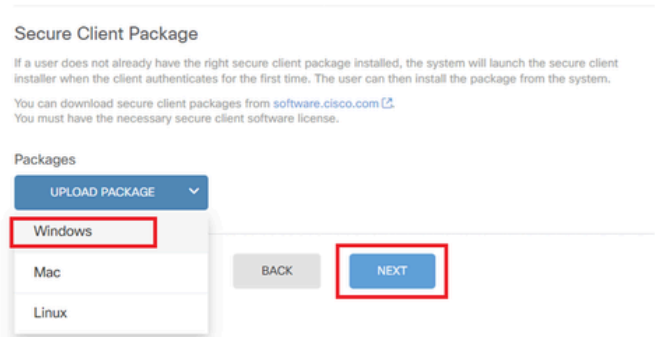
- Certificat d'identité du périphérique : ftdvpn-cert
- Interface externe : externe (GigabitEthernet0/0)



Détails des paramètres globaux

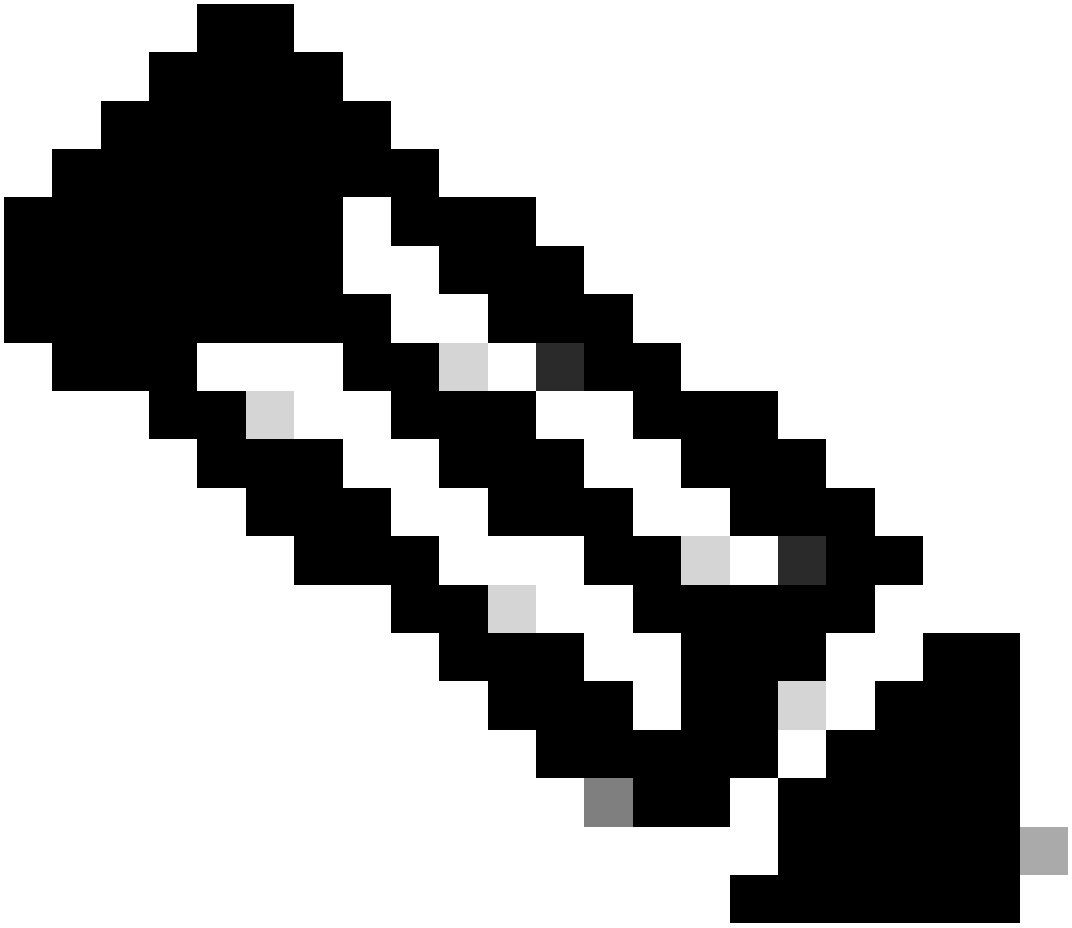
Étape 7. Configurer l'image du client sécurisé pour le profil de connexion

Sélectionner l'élément Windows dans les packages

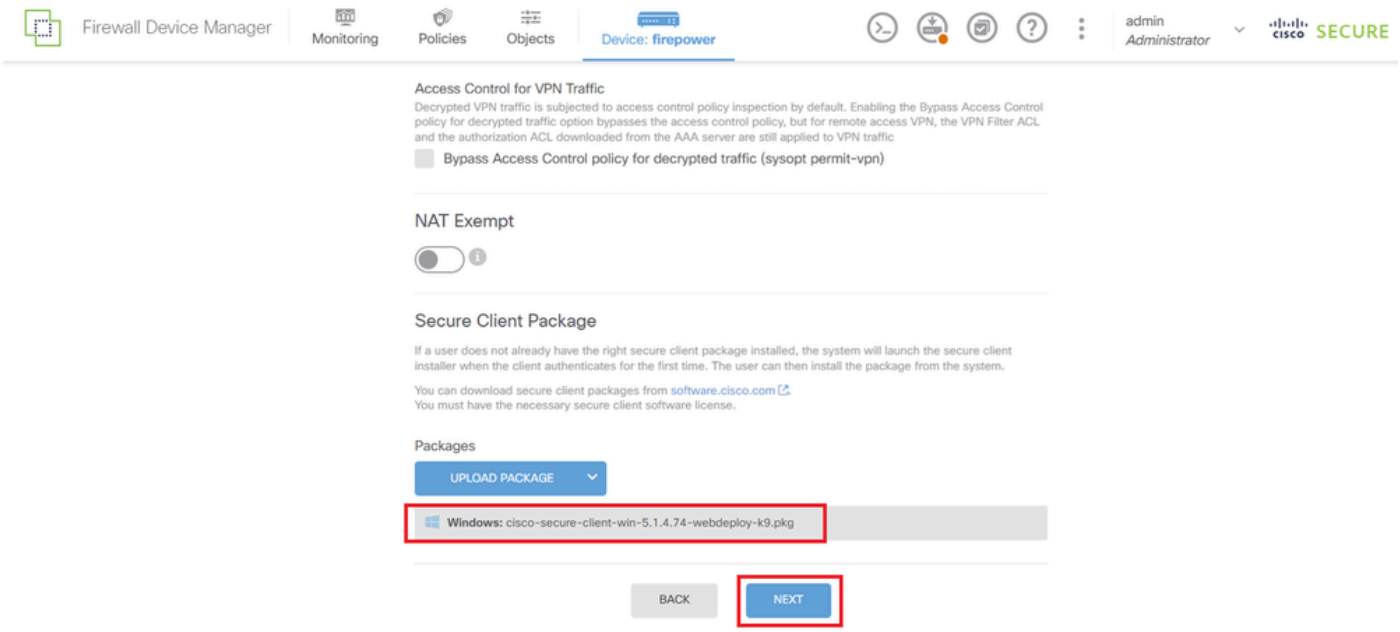


Télécharger le package d'image client sécurisé

Téléchargez le fichier d'image client sécurisé depuis l'ordinateur local et cliquez sur Suivant.



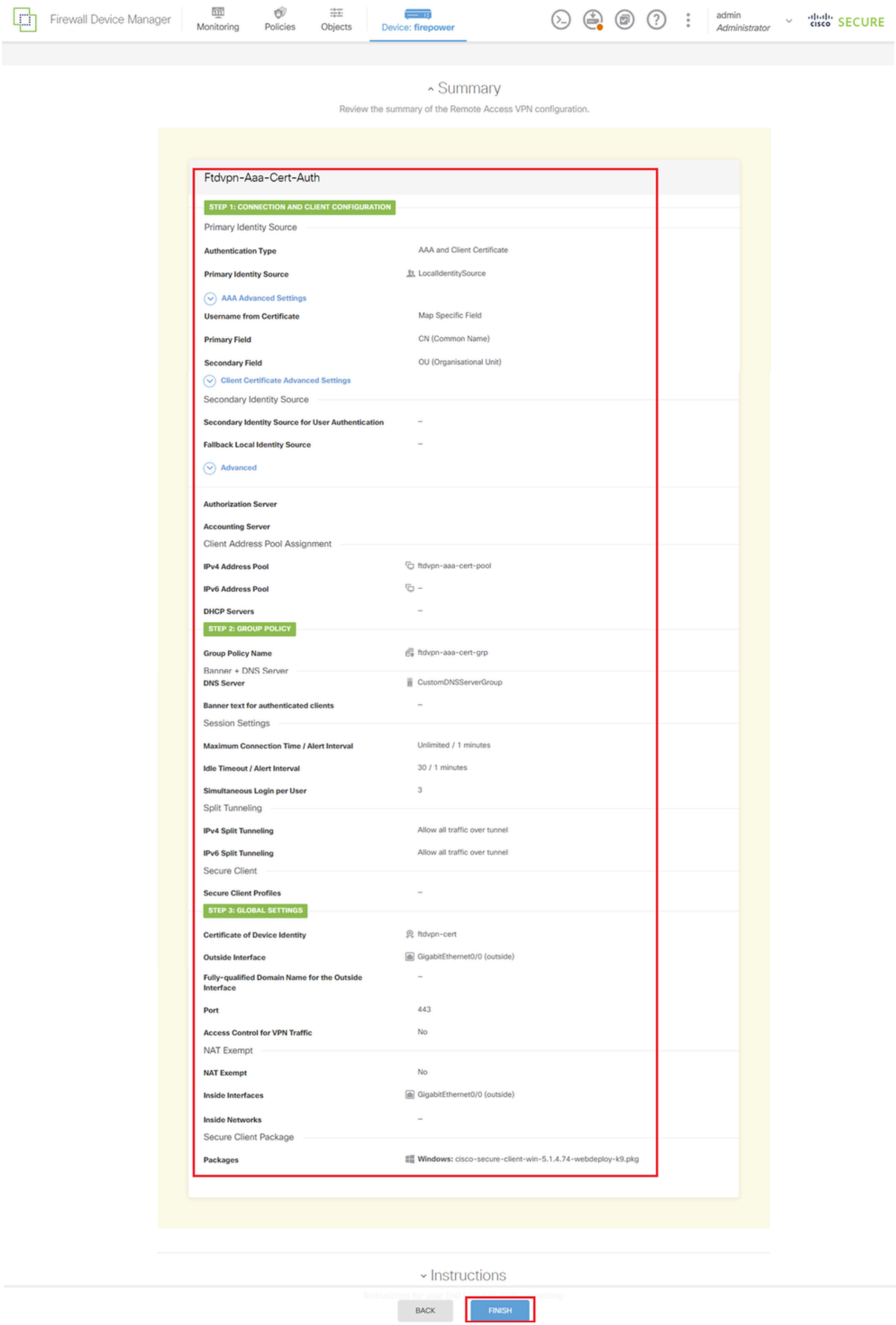
Remarque : la fonctionnalité NAT Exempt est désactivée dans ce document. Par défaut, l'option Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) est désactivée, ce qui signifie que le trafic VPN décrypté est soumis à l'inspection de la politique de contrôle d'accès.



Sélectionner un package d'image client sécurisé

Étape 8. Confirmer le résumé du profil de connexion

Confirmez les informations entrées pour la connexion VPN et cliquez sur FINISHbutton.



Confirmer les paramètres du profil de connexion

```
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0
!
interface GigabitEthernet0/1
speed auto
nameif inside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50

// Defines a local user
username sslVPNClientCN password ***** pbkdf2

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
enrollment terminal
keypair ftdvpn-cert
validation-usage ssl-server
crl configure

// Server Certificate
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
......
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client ssl-server
crl configure

// CA
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
```

```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
dns-server value 64.x.x.245 64.x.x.184
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles none
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
```

```
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

Confirmer dans le client VPN

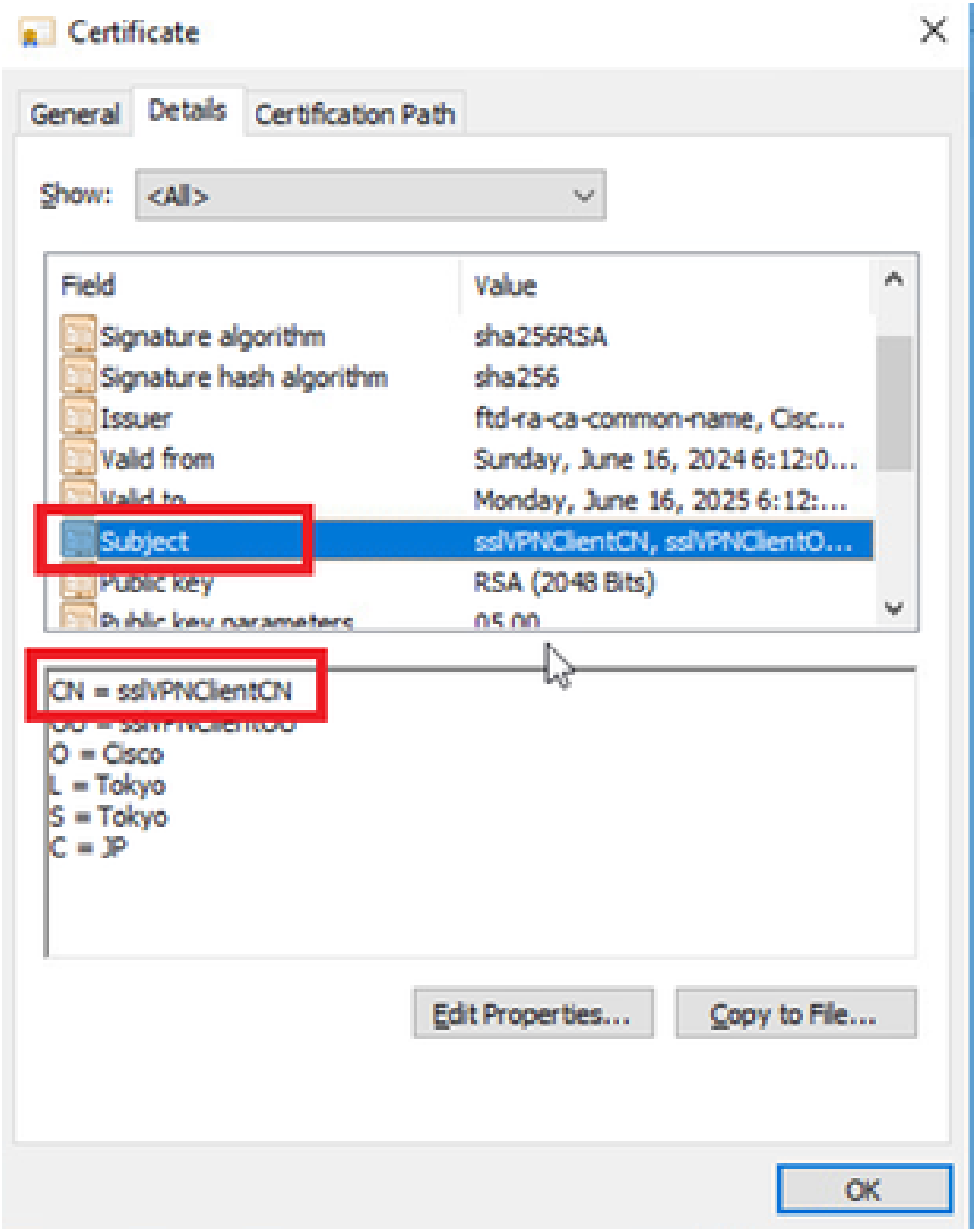
Étape 1. Confirmer le certificat client

Accédez à Certificates - Current User > Personal > Certificates, vérifiez le certificat client utilisé pour l'authentification.

Confirmer le certificat client

Double-cliquez sur le certificat client, accédez à Détails, vérifiez les détails de Objet.

- Objet : CN = sslVPNClientCN



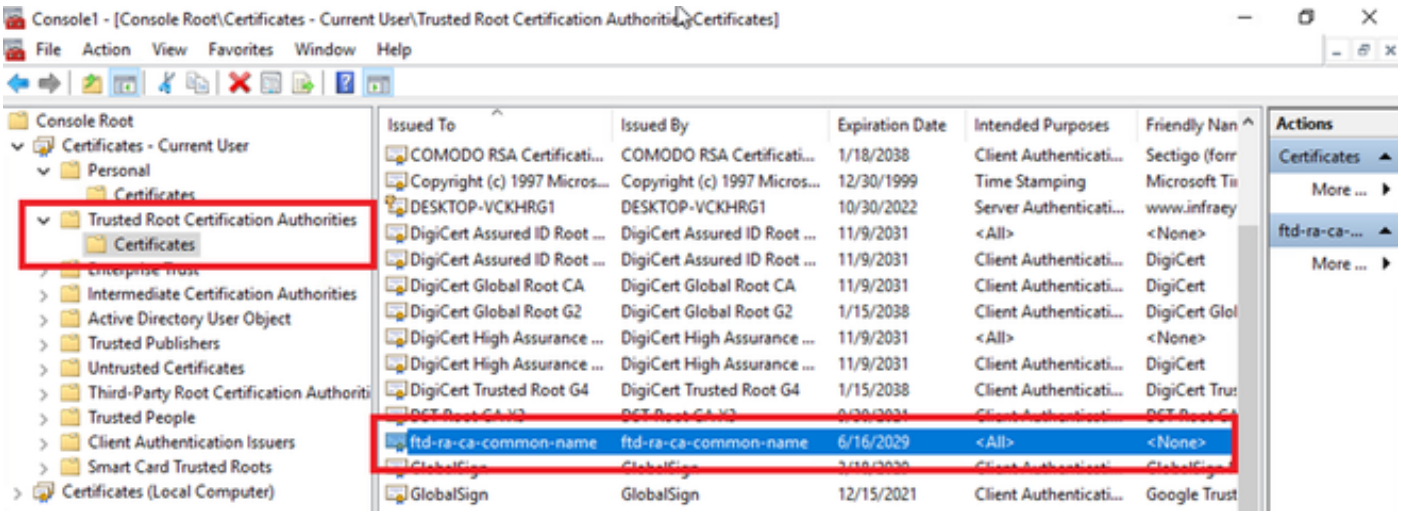
Détails du certificat client

Étape 2. Confirmer CA

Accédez à Certificates - Current User > Trusted Root Certification Authorities > Certificates,

cochez la CA utilisée pour l'authentification.

- Émis par : ftd-ra-ca-common-name

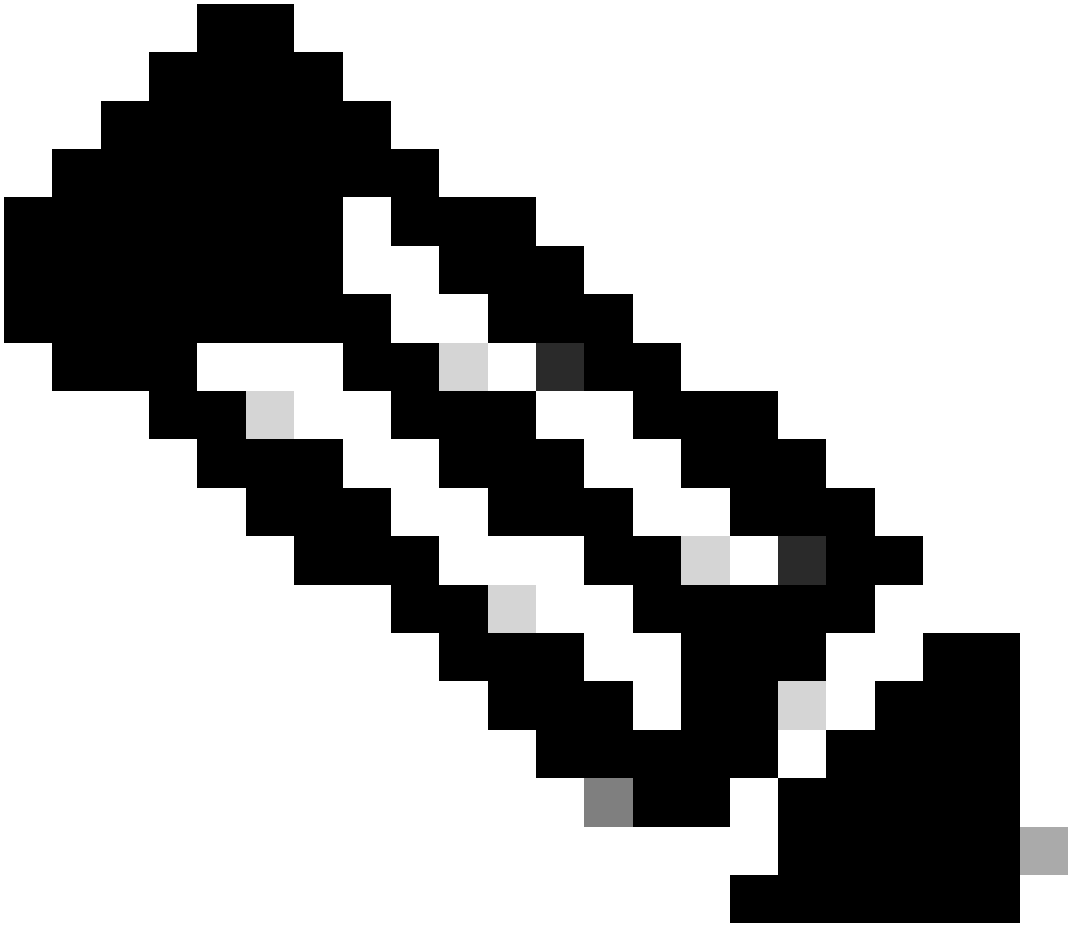


Confirmer CA

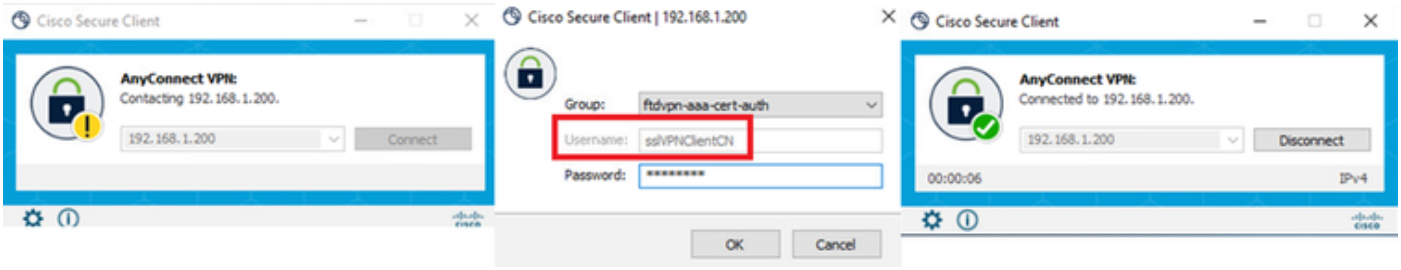
Vérifier

Étape 1. Initiation de la connexion VPN

Sur le terminal, lancez la connexion Cisco Secure Client. Le nom d'utilisateur est extrait du certificat client, vous devez entrer le mot de passe pour l'authentification VPN.



Remarque : le nom d'utilisateur est extrait du champ Nom commun (CN) du certificat client dans ce document.



Initiation de la connexion VPN

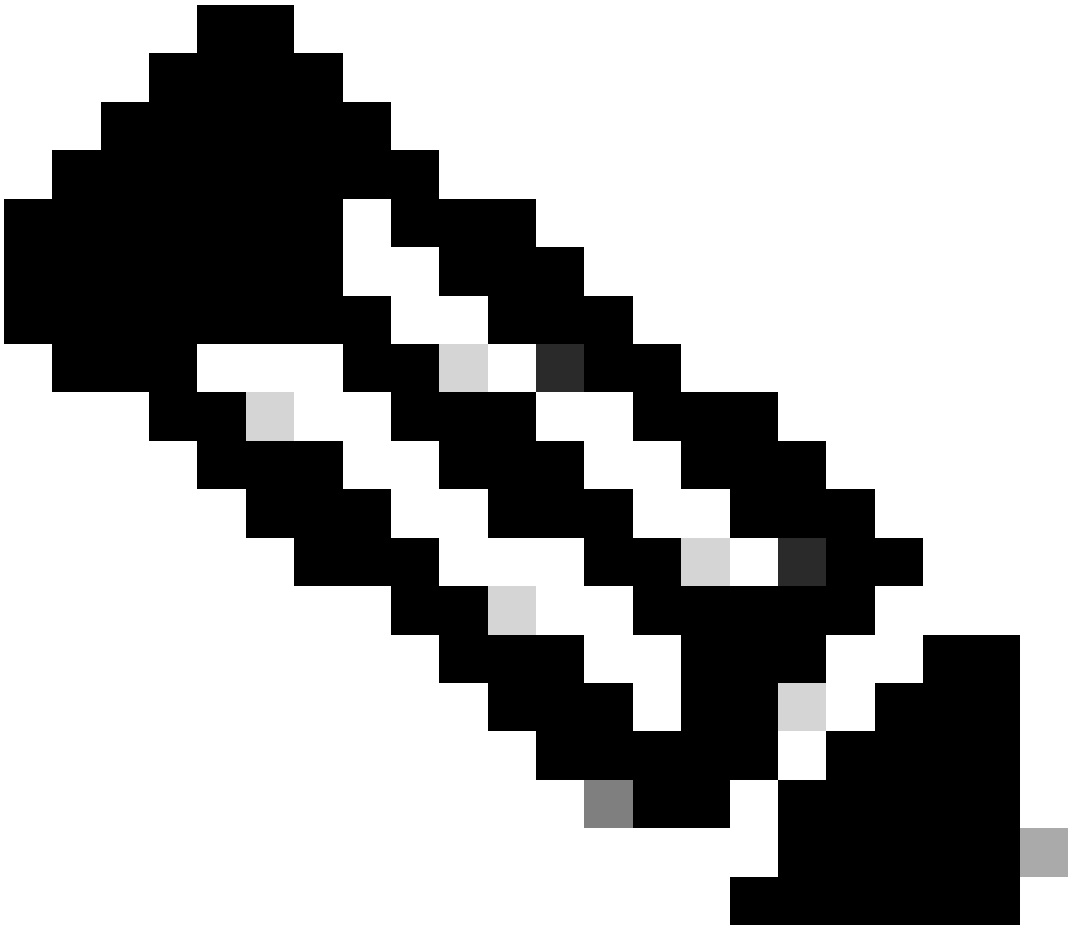
Étape 2. Confirmer la session VPN dans FTD CLI

Exécutezshow vpn-sessiondb detail anyconnect la commande dans l'interface de ligne de commande FTD (Lina) pour confirmer la session VPN.

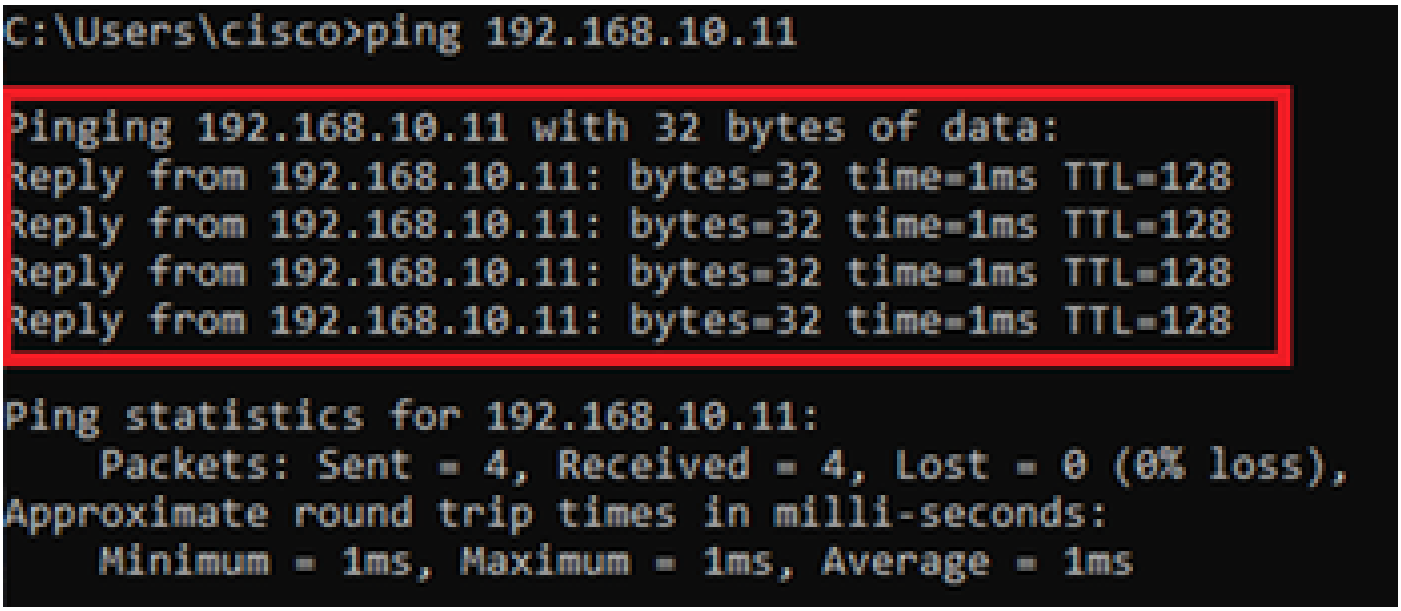
```
firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 4
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx : 29072 Bytes Rx : 44412
Pkts Tx : 10 Pkts Rx : 442
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 11:47:42 UTC Sat Jun 29 2024
Duration : 1h:09m:30s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000004000667ff45e
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 4.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 49779 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 7 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 14356 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 4.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 49788
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7178 Bytes Rx : 10358
Pkts Tx : 1 Pkts Rx : 118
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Étape 3. Confirmer la communication avec le serveur

Lancez une requête ping à partir du client VPN vers le serveur, confirmez que la communication entre le client VPN et le serveur a réussi.



Remarque : comme l'option Ignorer la stratégie de contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn) est désactivée à l'étape 7, vous devez créer des règles de contrôle d'accès qui permettent à votre pool d'adresses IPv4 d'accéder au serveur.



Ping réussi

capture in interface inside real-timeExécutez la commande dans l'interface de ligne de commande FTD (Lina) pour confirmer la capture des paquets.

firepower# capture in interface inside real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture

1: 12:03:26.626691 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 12:03:26.627134 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 12:03:27.634641 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 12:03:27.635144 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 12:03:28.650189 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 12:03:28.650601 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 12:03:29.665813 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 12:03:29.666332 192.168.10.11 > 172.16.1.40 icmp: echo reply

Dépannage

Vous pouvez vous attendre à trouver des informations sur l'authentification VPN dans le syslog de débogage du moteur Lina et dans le fichier DART sur l'ordinateur Windows.

Voici un exemple de journaux de débogage dans le moteur Lina.

// Certificate Authentication
Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.

Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=sslVPNClientCN

// Extract username from the CN (Common Name) field
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 3]
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 3]

// AAA Authentication
Jun 29 2024 11:29:53: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN

Ces débogages peuvent être exécutés à partir de l'interface de ligne de commande de diagnostic du FTD, qui fournit des informations que vous pouvez utiliser afin de dépanner votre configuration.

- debug crypto ca 14
- debug webvpn anyconnect 255
- debug crypto ike-common 25

Informations connexes

Configuration du service de gestion prêt à l'emploi FDM pour Firepower 2100

Configurer un VPN d'accès à distance sur FTD géré par FDM

Configuration et vérification de Syslog dans le Gestionnaire de périphériques Firepower

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.