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

Table des matières

Introduction

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

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Management Center (FMC)
- Protection contre les menaces virtuelles (FTD)
- Flux d'authentification VPN

Composants utilisés

- Cisco Firepower Management Center pour VMWare 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1

- Cisco Secure Client 5.1.3.62

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

À mesure que les entreprises adoptent des mesures de sécurité plus strictes, l'association de l'authentification à deux facteurs (2FA) et de l'authentification basée sur certificat est devenue une pratique courante pour améliorer la sécurité et protéger contre les accès non autorisés. L'une des fonctionnalités permettant d'améliorer de manière significative l'expérience utilisateur et la sécurité est la possibilité de préremplir le nom d'utilisateur dans le client sécurisé Cisco. Cette fonctionnalité simplifie le processus de connexion et améliore l'efficacité globale de l'accès à distance.
Ce document décrit comment intégrer un nom d'utilisateur pré-rempli avec Cisco Secure Client sur FTD, afin de garantir que les utilisateurs peuvent se connecter rapidement et en toute sécurité au réseau.

Ces certificats contiennent un nom commun qui est utilisé à des fins d’autorisation.

- 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.

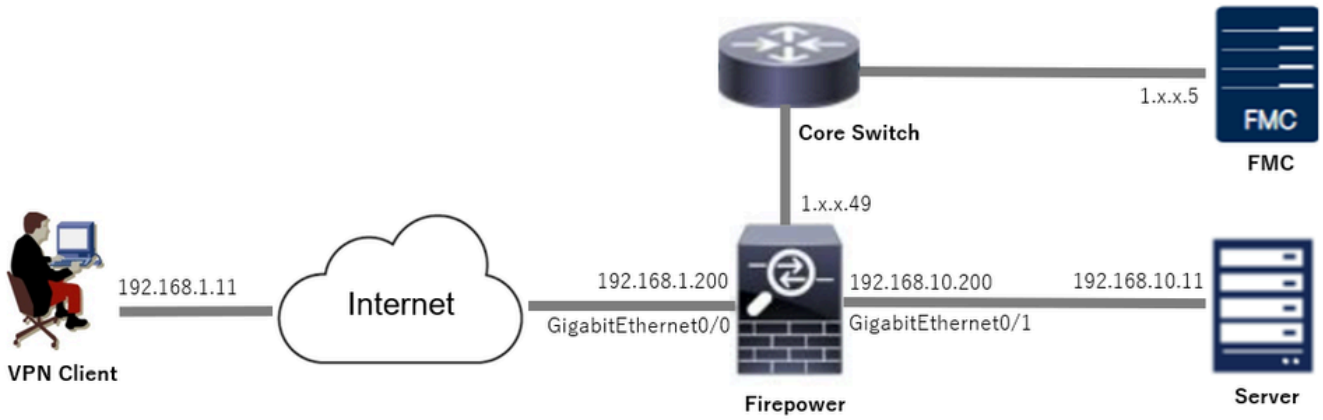


Diagramme du réseau

Configurations

Configuration dans FMC

Étape 1. Configurer l'interface FTD

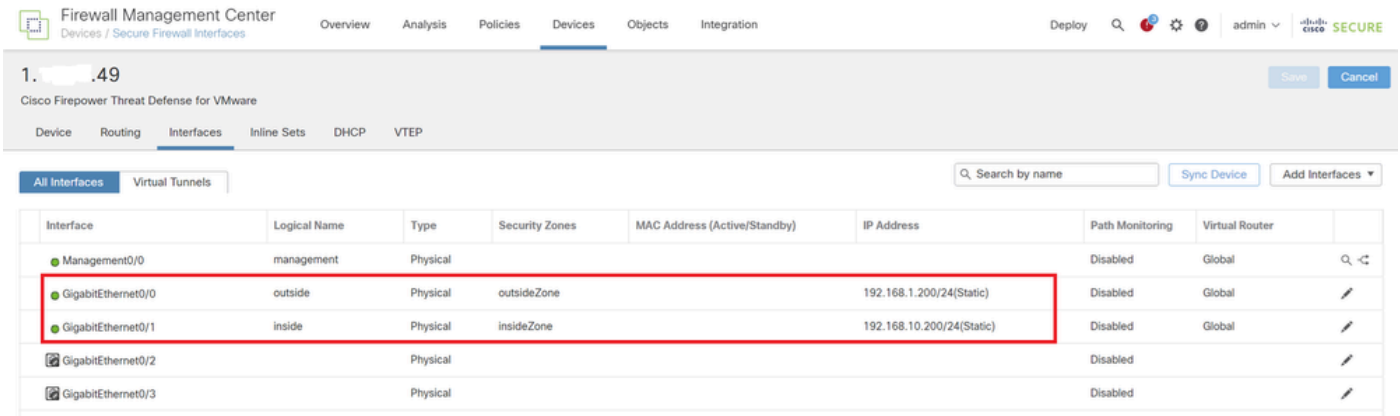
Accédez à Devices > Device Management, modifiez le périphérique FTD cible, configurez l'interface interne et externe pour FTD dans l'onglet Interfaces.

Pour GigabitEthernet0/0,

- Nom : externe
- Zone de sécurité : outsideZone
- Adresse IP : 192.168.1.200/24

Pour GigabitEthernet0/1,

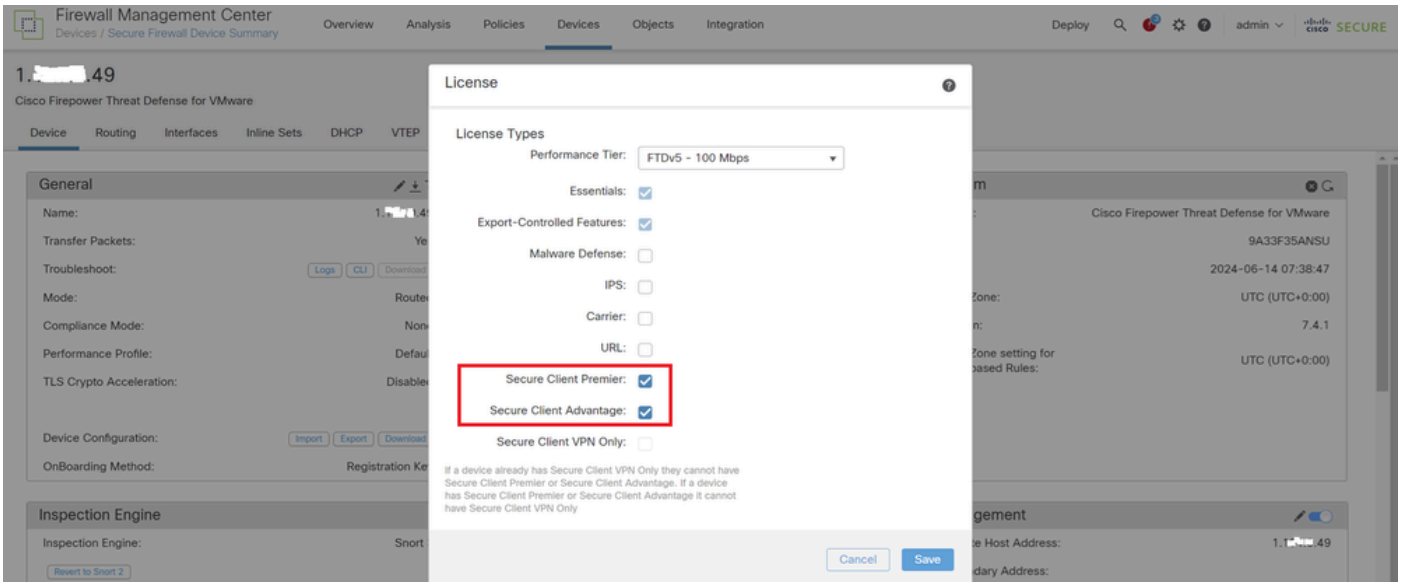
- Nom : interne
- Zone de sécurité : insideZone
- Adresse IP : 192.168.10.200/24



Interface FTD

Étape 2. Confirmer la licence Cisco Secure Client

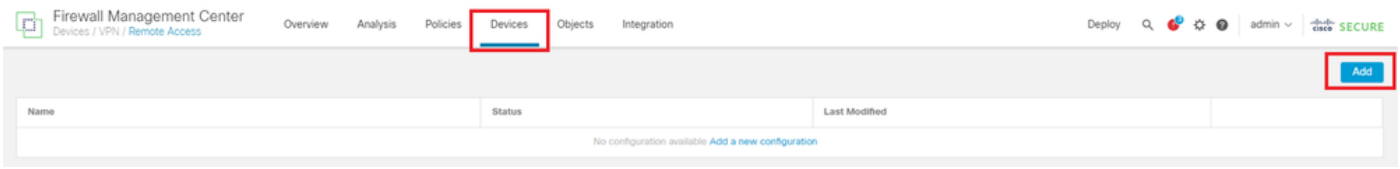
Accédez à Devices > Device Management, modifiez le périphérique FTD cible, confirmez la licence Cisco Secure Client dans l'onglet Device.



Licence client sécurisée

Étape 3. Ajouter une affectation de stratégie

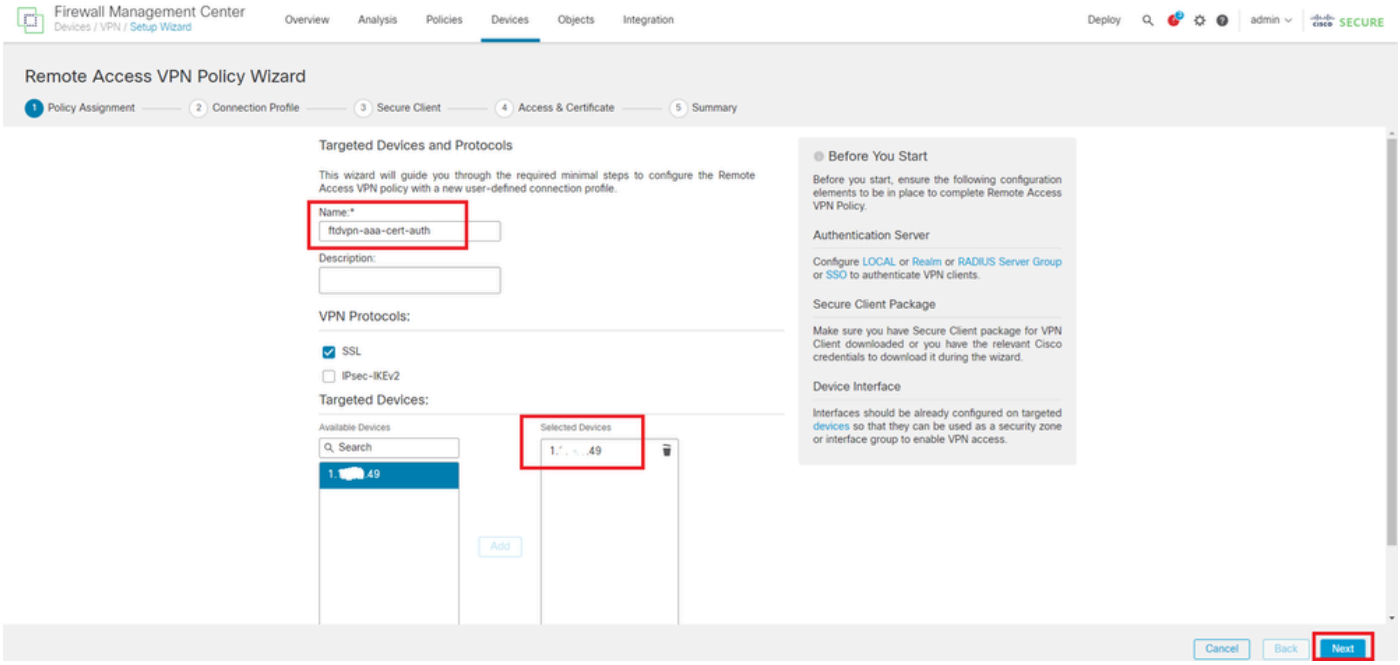
Accédez à Devices > VPN > Remote Access, cliquez sur Add button.



Ajouter un VPN d'accès à distance

Saisissez les informations nécessaires et cliquez sur Next button.

- Nom : ftdvpn-aaa-cert-auth
- Protocoles VPN : SSL
- Périphériques cibles : 1.x.x.49

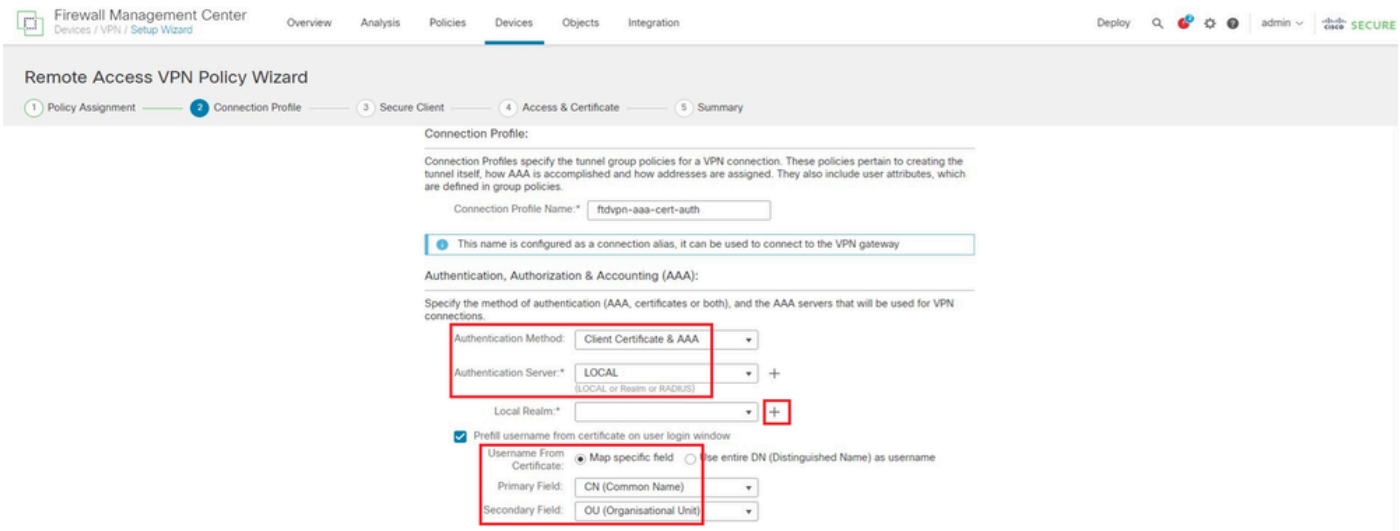


Affectation de stratégie

Étape 4. Détails de configuration du profil de connexion

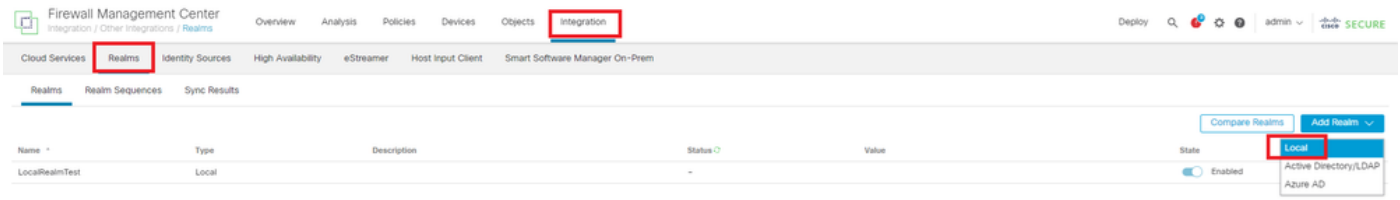
Entrez les informations nécessaires pour le profil de connexion et cliquez sur le bouton + en regard de l'élément Domaine local.

- Méthode d'authentification : certificat client et AAA
- Serveur d'authentification : LOCAL
- Nom d'utilisateur du certificat : champ spécifique au mappage
- Champ principal : CN (nom commun)
- Champ secondaire : OU (unité organisationnelle)



Détails du profil de connexion

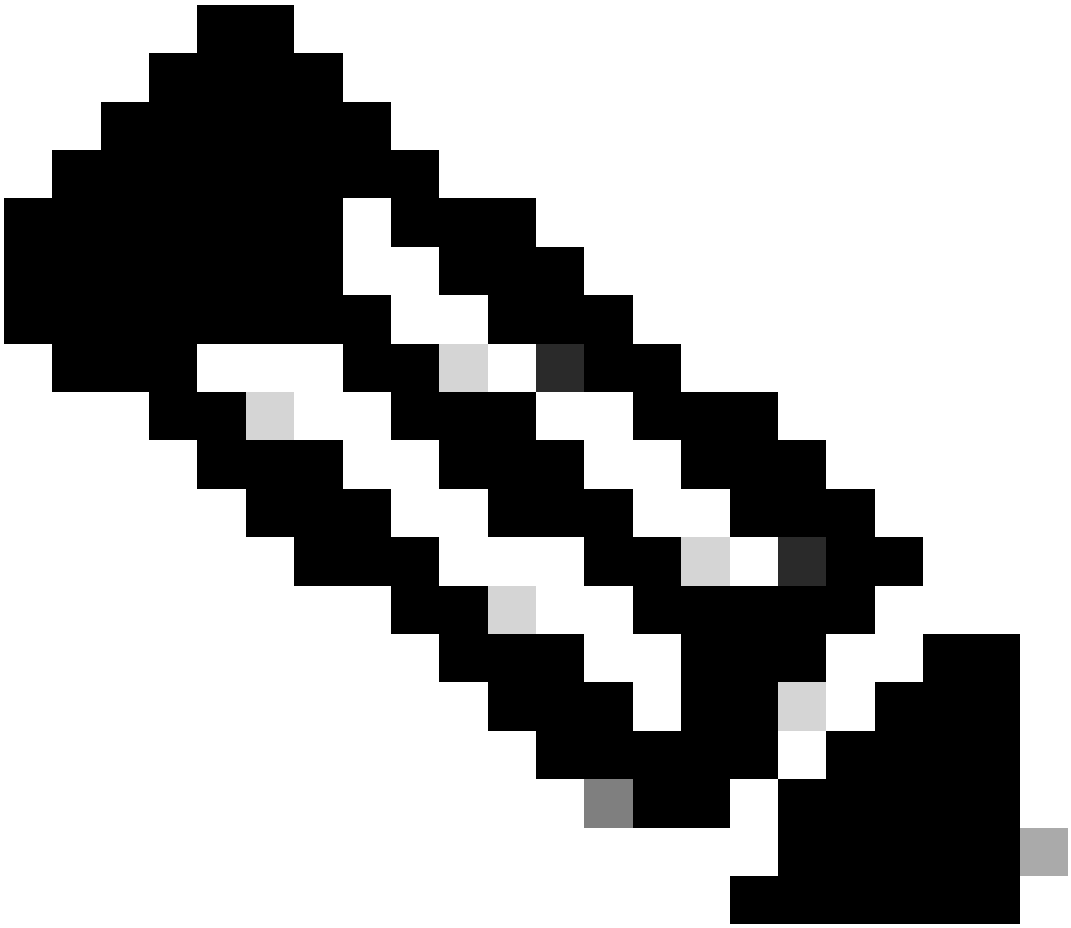
Cliquez sur Local dans la liste déroulante Add Realm pour ajouter un nouveau domaine local.



Ajouter un domaine local

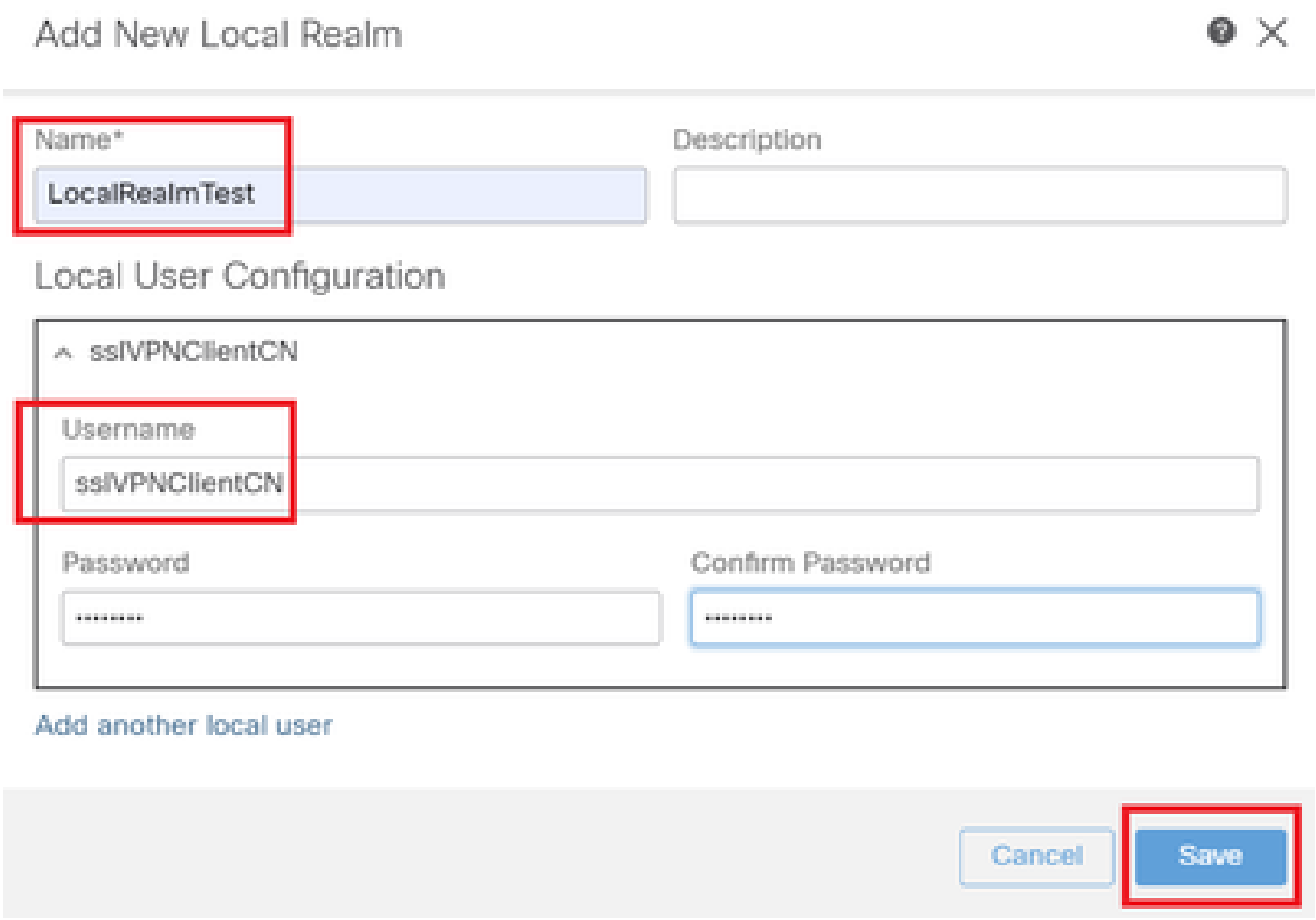
Entrez les informations nécessaires pour le domaine local et cliquez sur le bouton Enregistrer.

- Nom : LocalRealmTest
- Nom d'utilisateur : sslVPNClientCN



Remarque : le nom d'utilisateur est le nom commun du certificat client

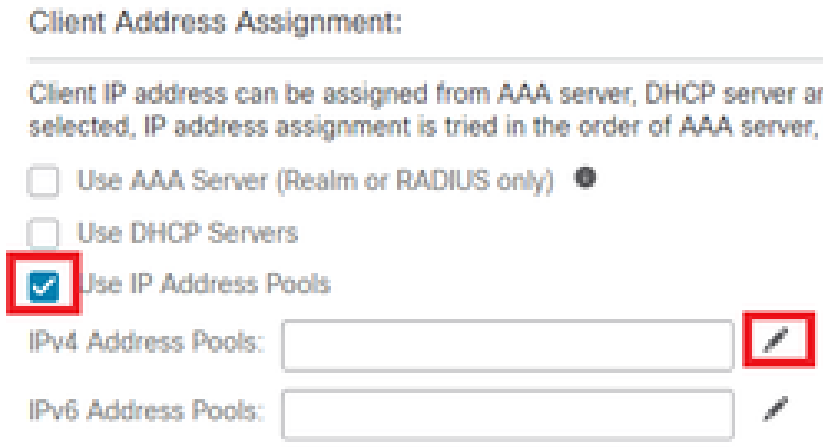
---



Détails du domaine local

Étape 5. Ajouter un pool d'adresses pour le profil de connexion

Cliquez sur le bouton Edit en regard de l'élément IPv4 Address Pools.

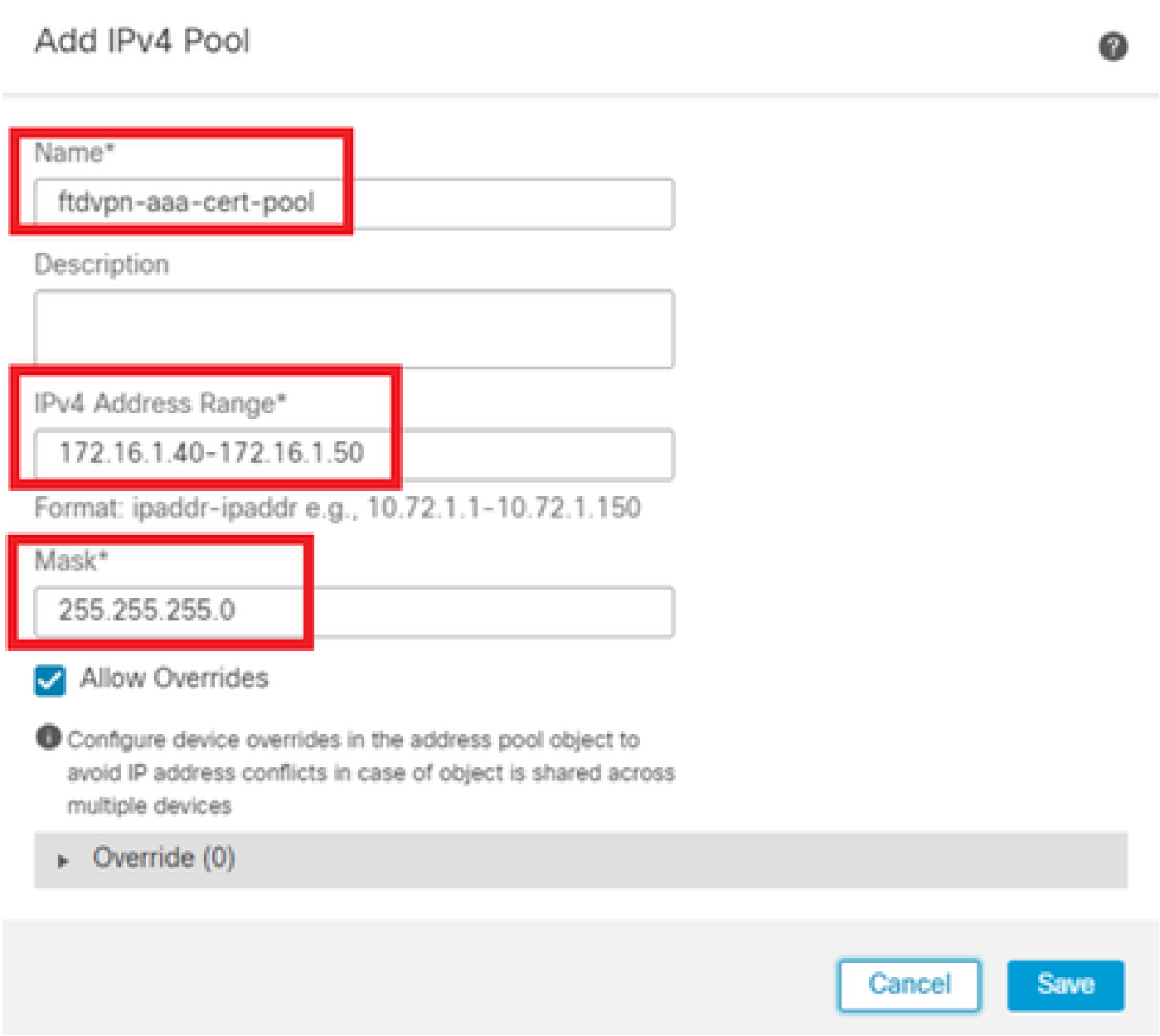


Ajouter un pool d'adresses IPv4

Entrez les informations nécessaires pour ajouter un nouveau pool d'adresses IPv4. Sélectionnez le nouveau pool d'adresses IPv4 pour le profil de connexion.

- Nom : ftdvpn-aaa-cert-pool
- Plage d'adresses IPv4 : 172.16.1.40-172.16.1.50

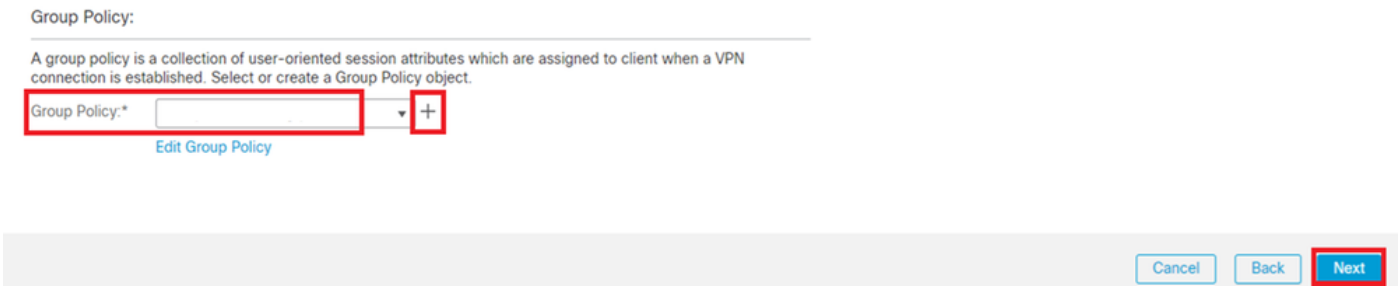
- Masque : 255.255.255.0



Détails du pool d'adresses IPv4

Étape 6. Ajouter une stratégie de groupe pour le profil de connexion

Cliquez sur le bouton + en regard de l'élément Stratégie de groupe.

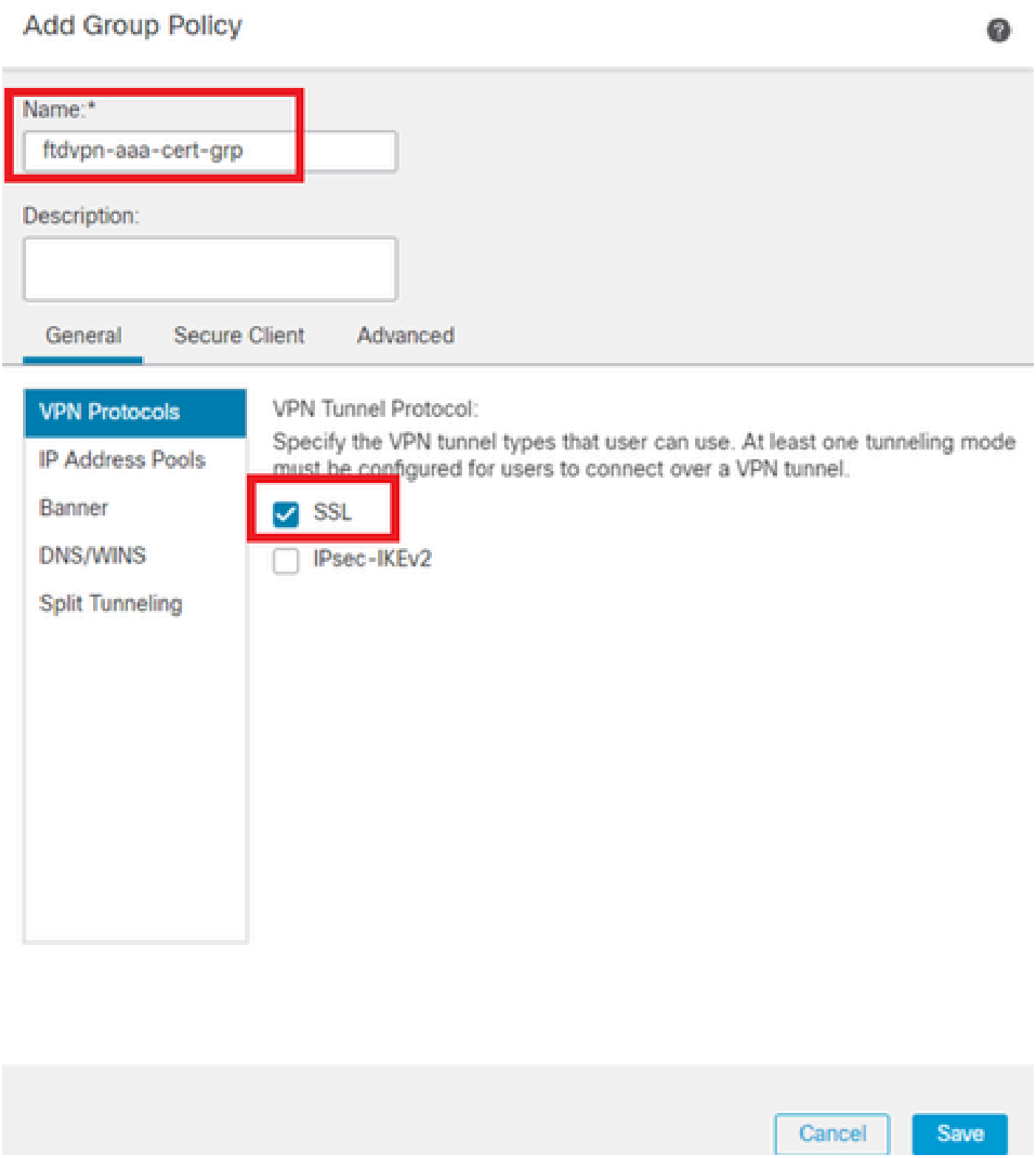


Ajouter une stratégie de groupe

Entrez les informations nécessaires pour ajouter une nouvelle stratégie de groupe. Sélectionnez la

nouvelle stratégie de groupe pour le profil de connexion.

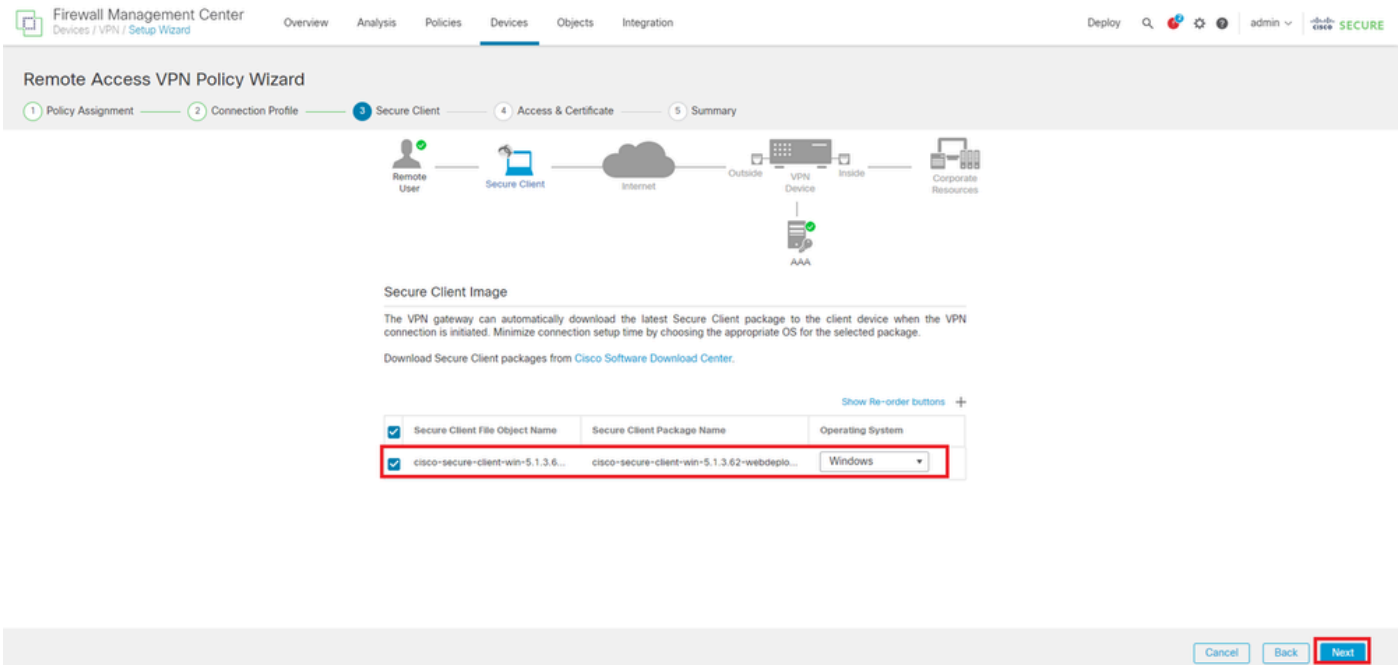
- Nom : ftdvpn-aaa-cert-grp
- Protocoles VPN : SSL



Détails de la stratégie de groupe

Étape 7. Config Image du client sécurisé pour le profil de connexion

Sélectionnez le fichier image client sécurisé et cliquez sur Next.

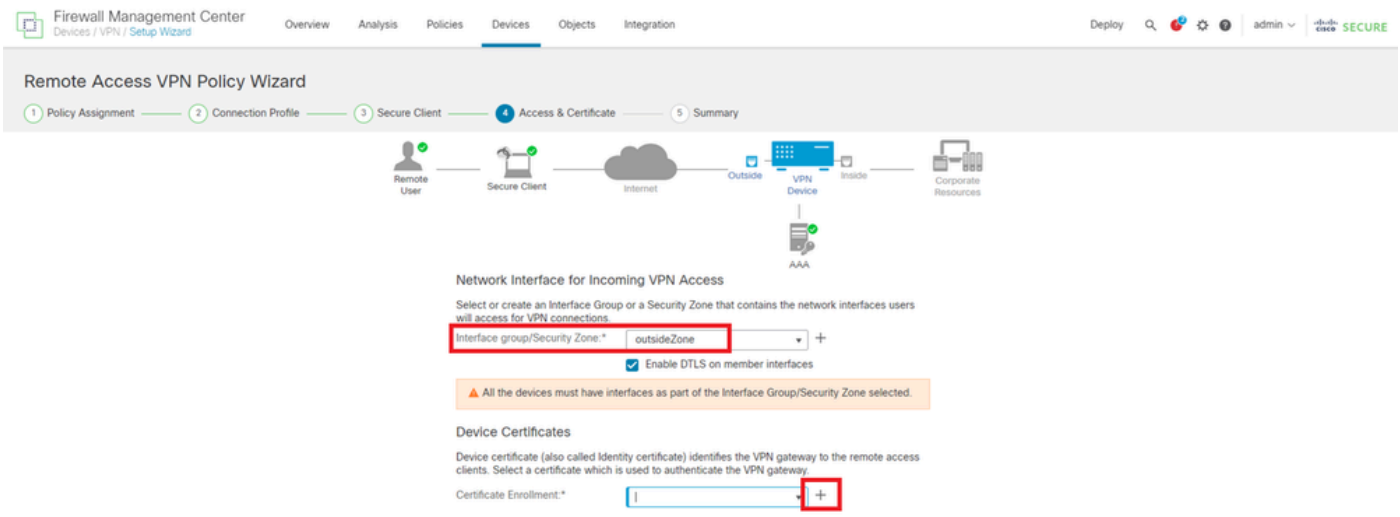


Sélectionner l'image client sécurisée

Étape 8. Accès et certificat de configuration pour le profil de connexion

Sélectionnez Security Zone for VPN connection et cliquez sur le bouton + en regard de l'élément Certificate Enrollment.

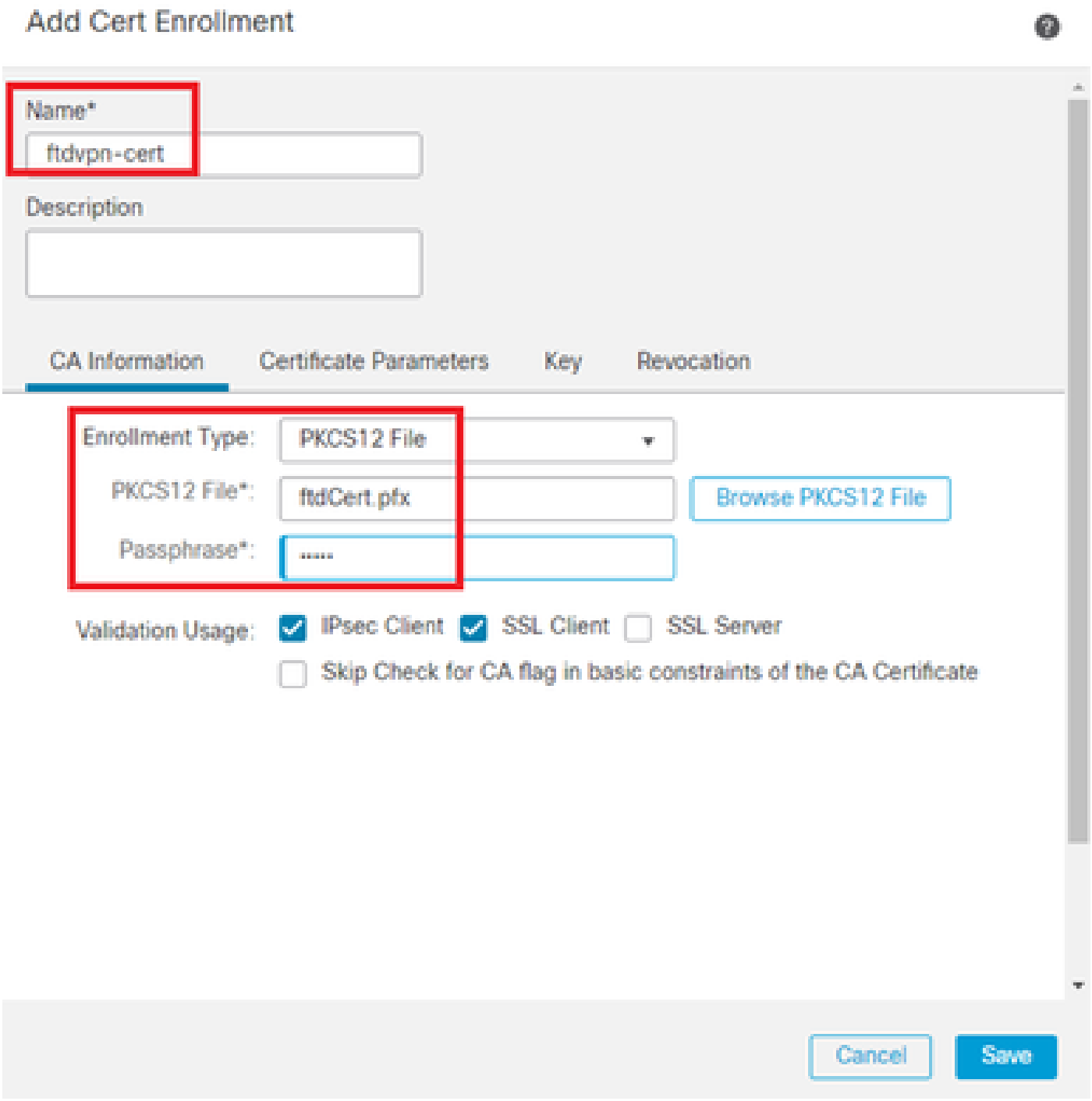
- Groupe d'interfaces/Zone de sécurité : outsideZone



Sélectionner une zone de sécurité

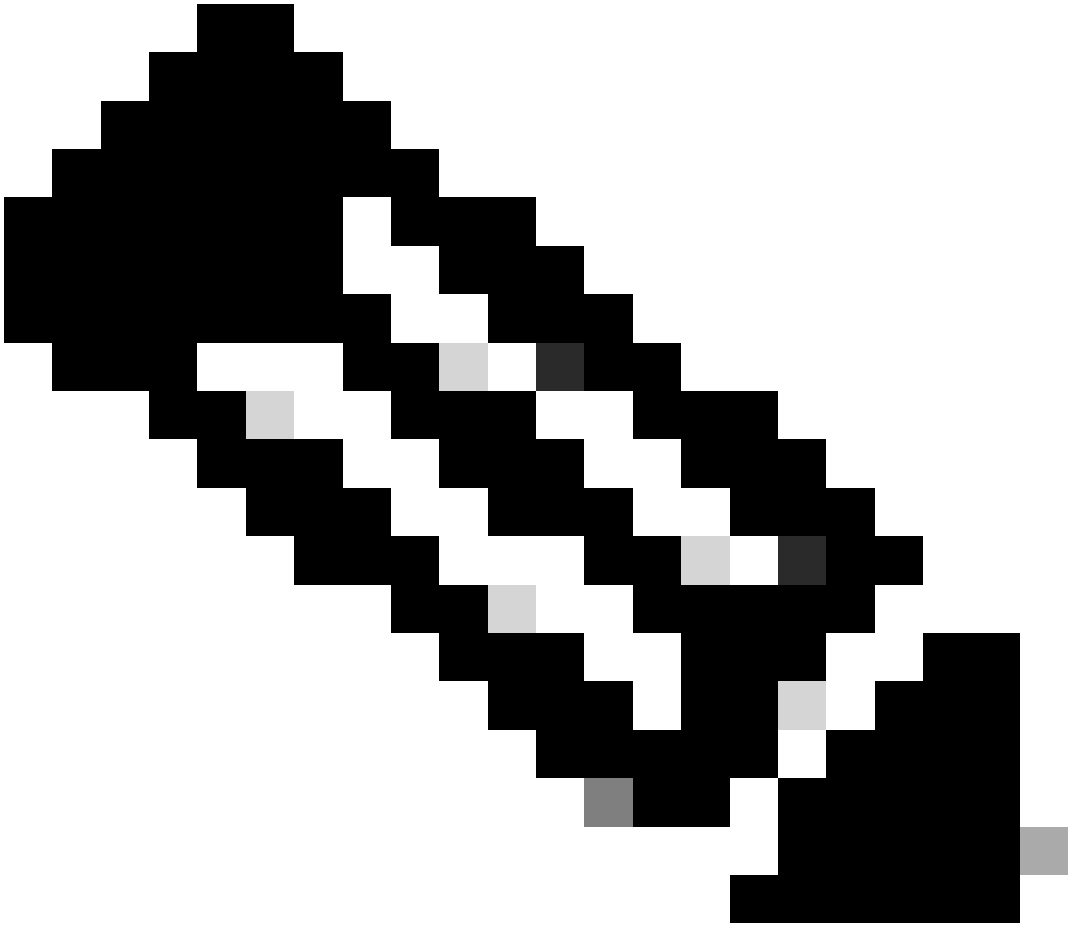
Entrez les informations nécessaires pour le certificat FTD et importez un fichier PKCS12 depuis l'ordinateur local.

- Nom : ftdvpn-cert
- Type d'inscription : fichier PKCS12

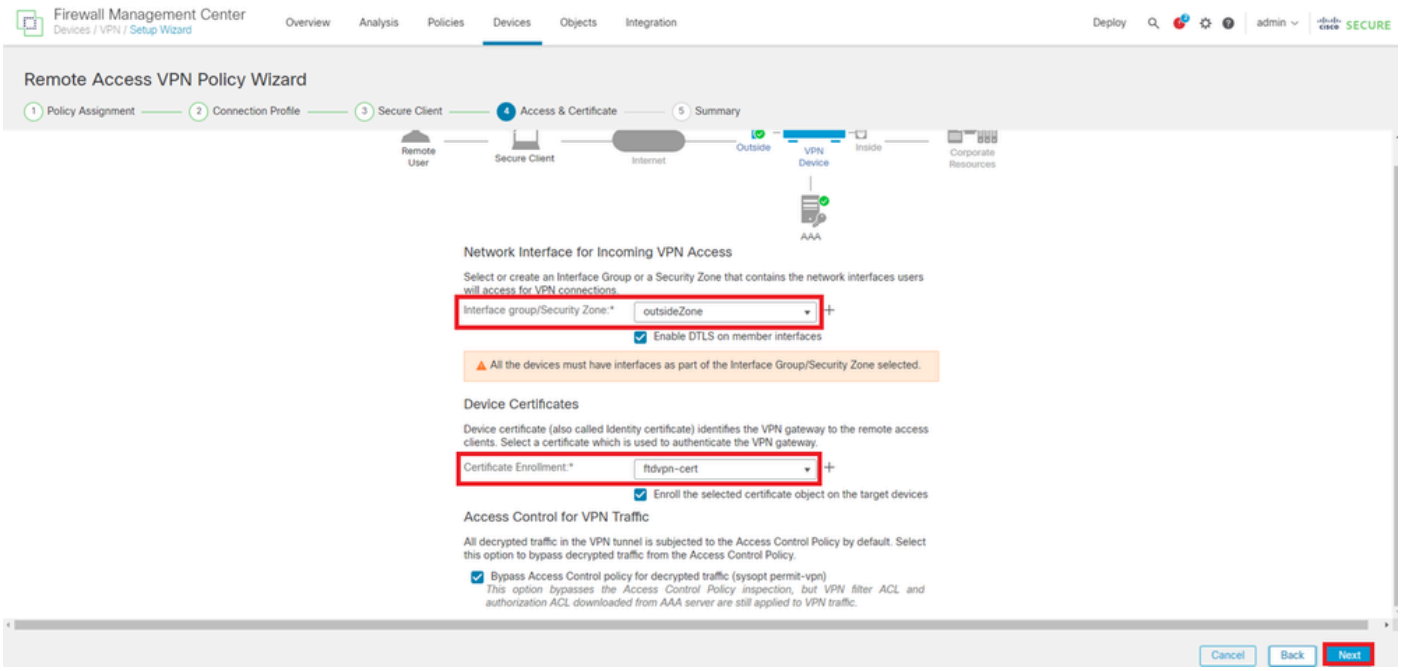


Ajouter un certificat FTD

Confirmez les informations saisies dans l'Assistant Accès et certificat et cliquez sur Suivant.



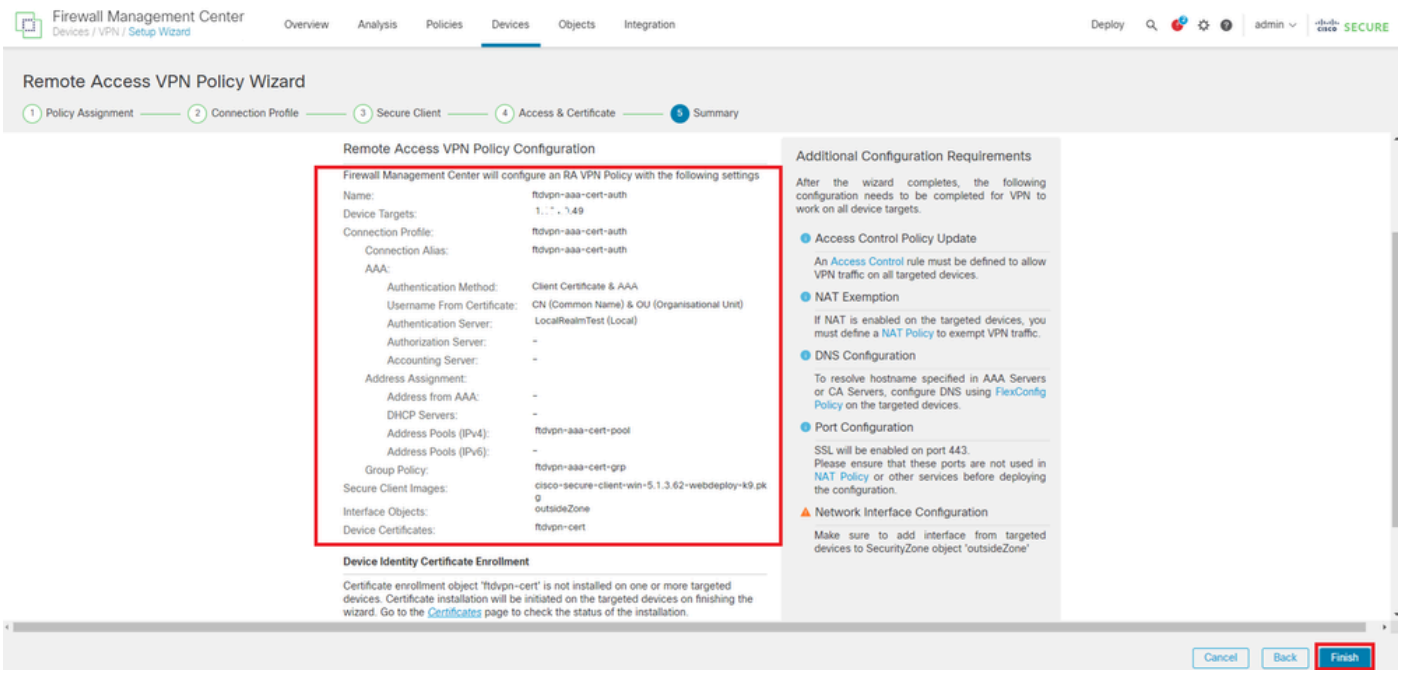
Remarque : activez la politique de contournement du contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn), de sorte que le trafic VPN déchiffré ne soit pas soumis à l'inspection de la politique de contrôle d'accès.



Confirmer les paramètres dans Access & Certificate

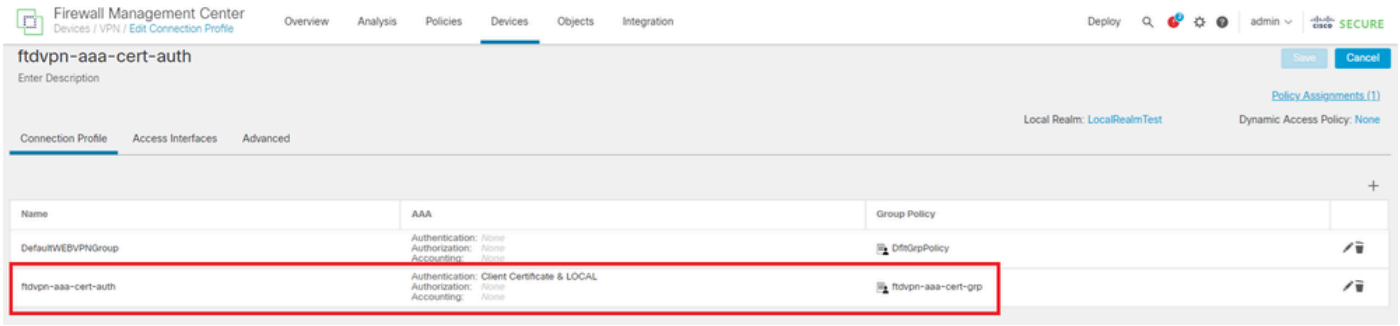
Étape 9. Confirmer le résumé du profil de connexion

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



Confirmer les paramètres de connexion VPN

Confirmez le résumé de la stratégie VPN d'accès à distance et déployez les paramètres sur FTD.



Résumé de la stratégie VPN d'accès à distance

Confirmer dans FTD CLI

Confirmez les paramètres de connexion VPN dans l'interface de ligne de commande du FTD après le déploiement à partir du FMC.

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0
interface GigabitEthernet0/1
nameif inside
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 mask 255.255.255.0

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

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
keypair ftdvpn-cert
crl configure

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

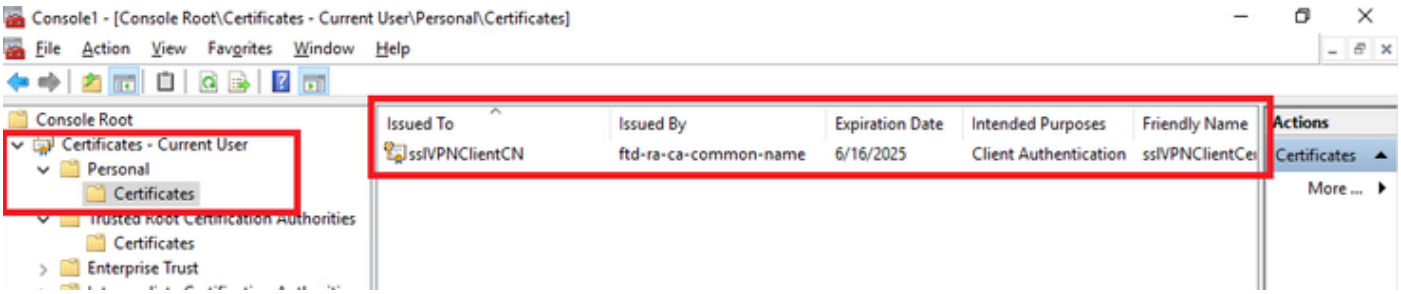
```
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
banner none
wins-server none
dns-server none
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-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// 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

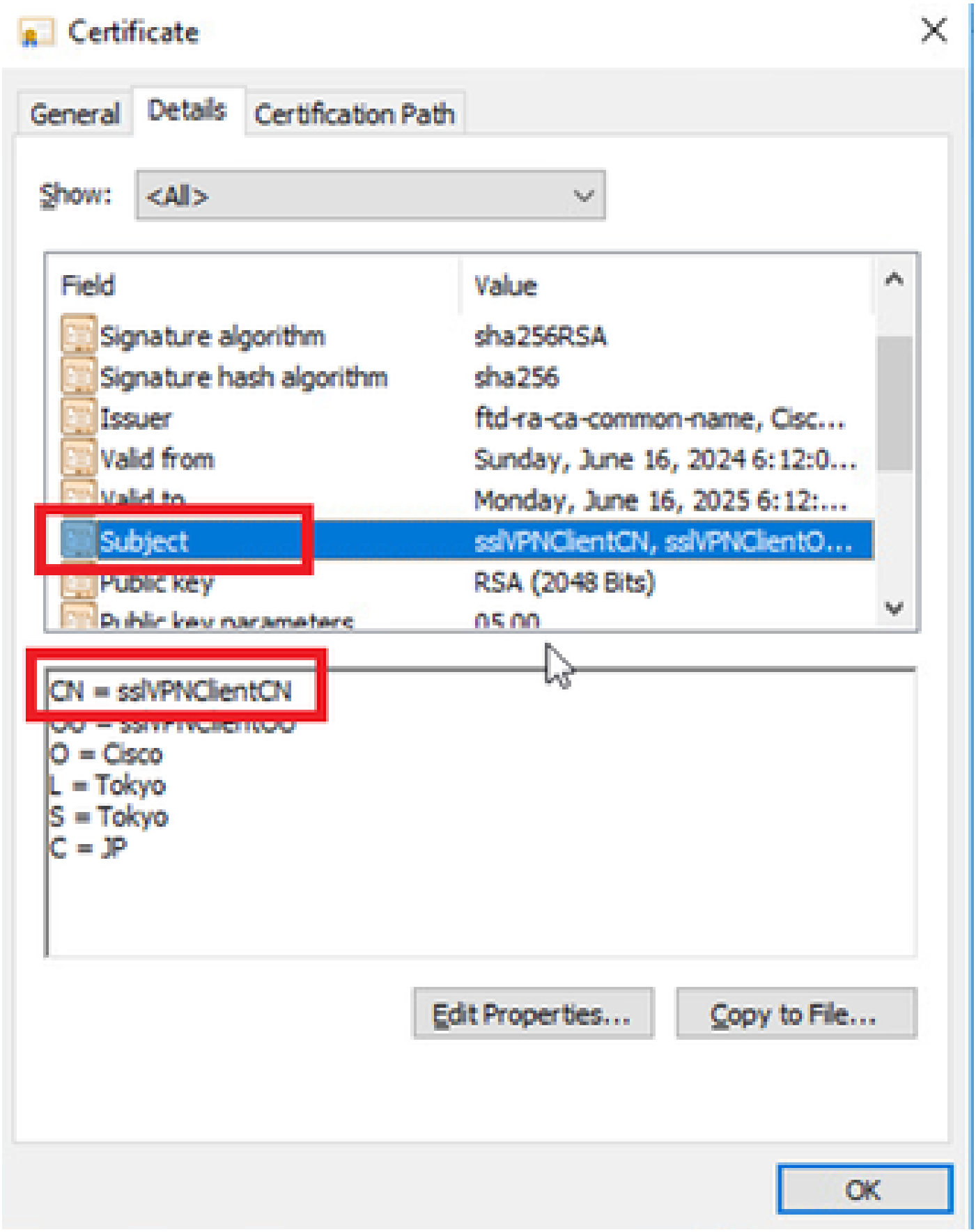
Accédez à Certificates - Current User > Personal > Certificates, vérifiez le certificat client utilisé pour l'authentification.



Confirmer le certificat client

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

- Objet : CN = sslVPNClientCN



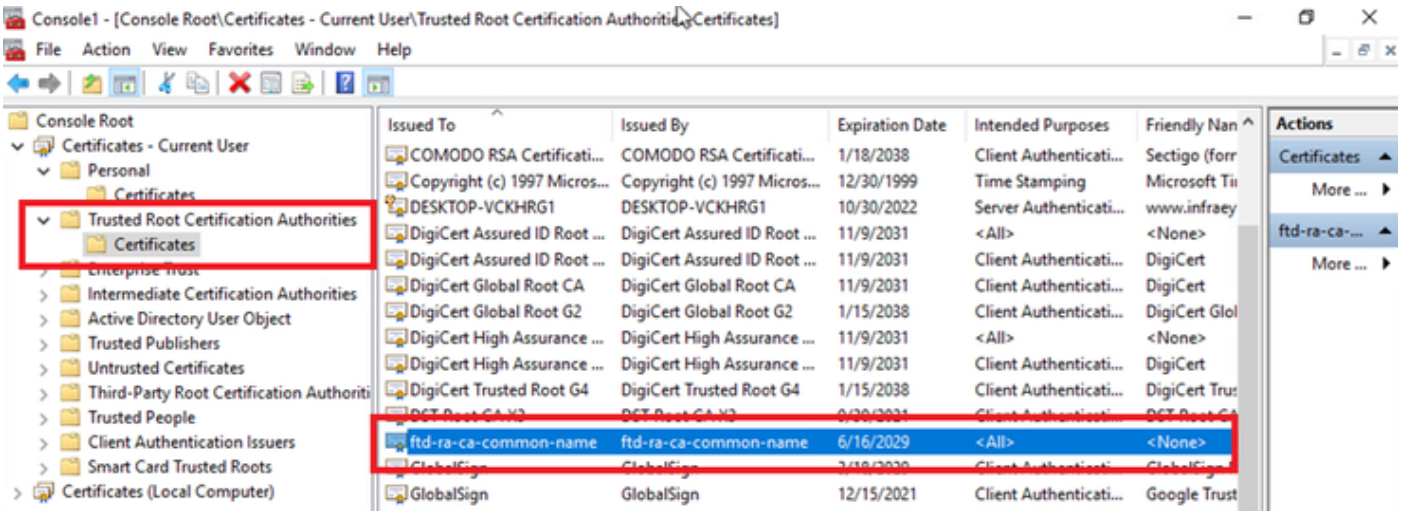
Détails du certificat client

Étape 2. Confirmer CA

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

vérifiez l'autorité de certification utilisée pour l'authentification.

- Émis par : ftd-ra-ca-common-name

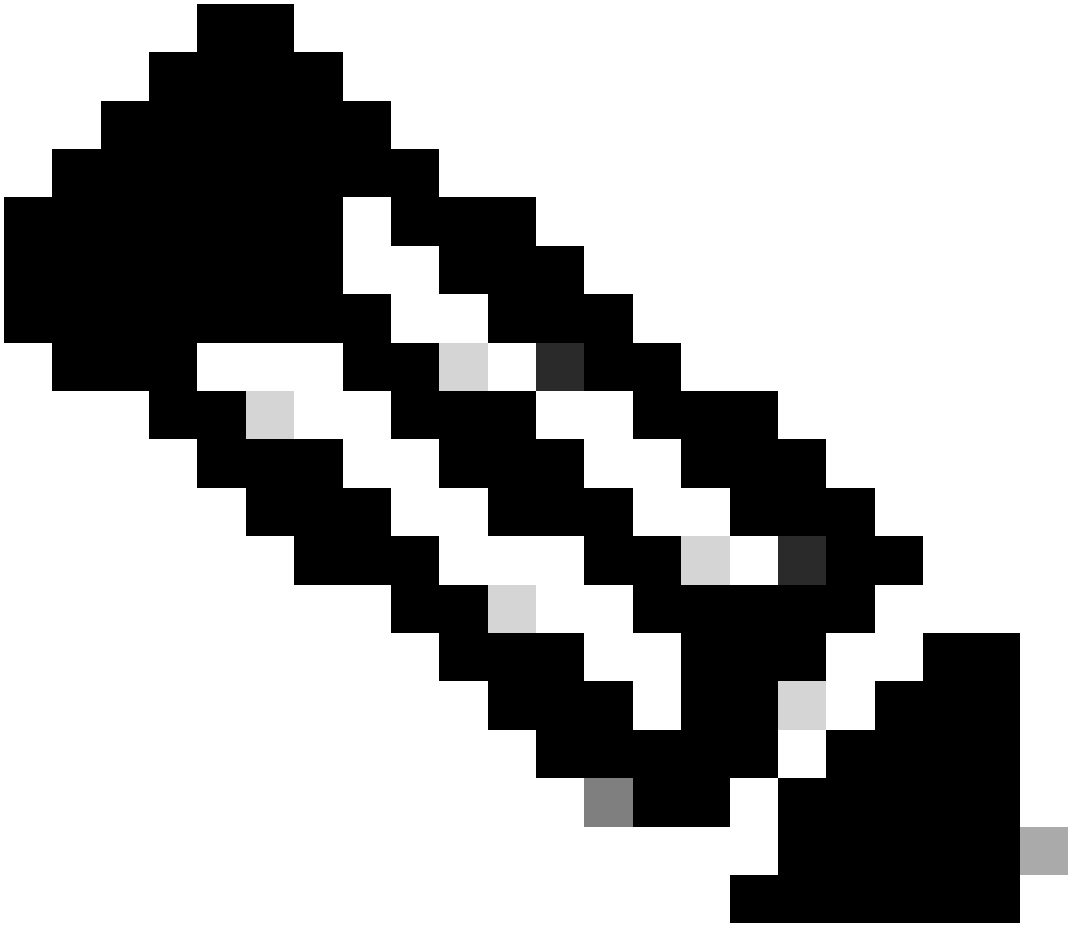


Confirmer CA

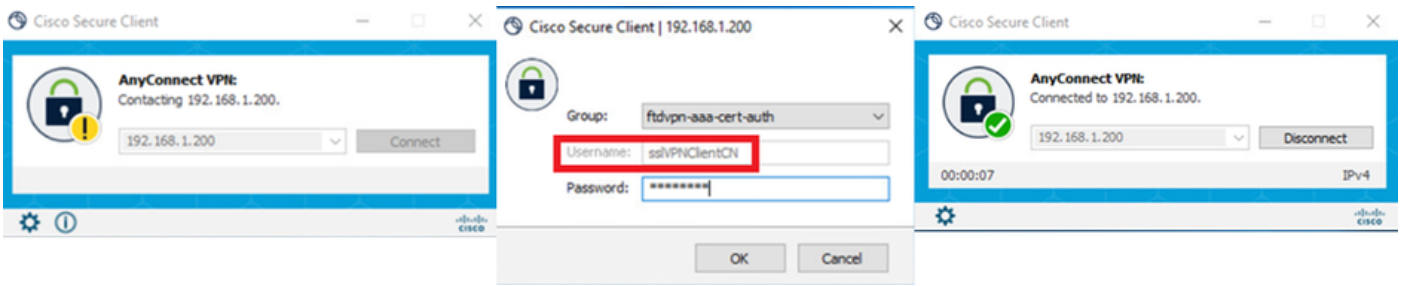
Vérifier

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.



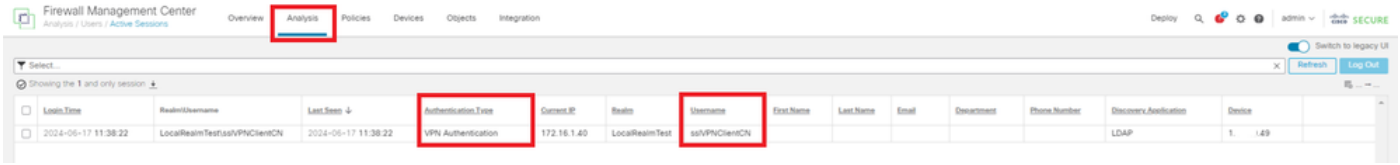
Remarque : le nom d'utilisateur est extrait du champ CN (Common Name) du certificat client dans ce document.



Initiation de la connexion VPN

Étape 2. Confirmer les sessions actives dans FMC

Naviguez jusqu'à Analysis > Users > Active Sessions, vérifiez la session active pour l'authentification VPN.



Confirmer la session active

Étape 3. 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.

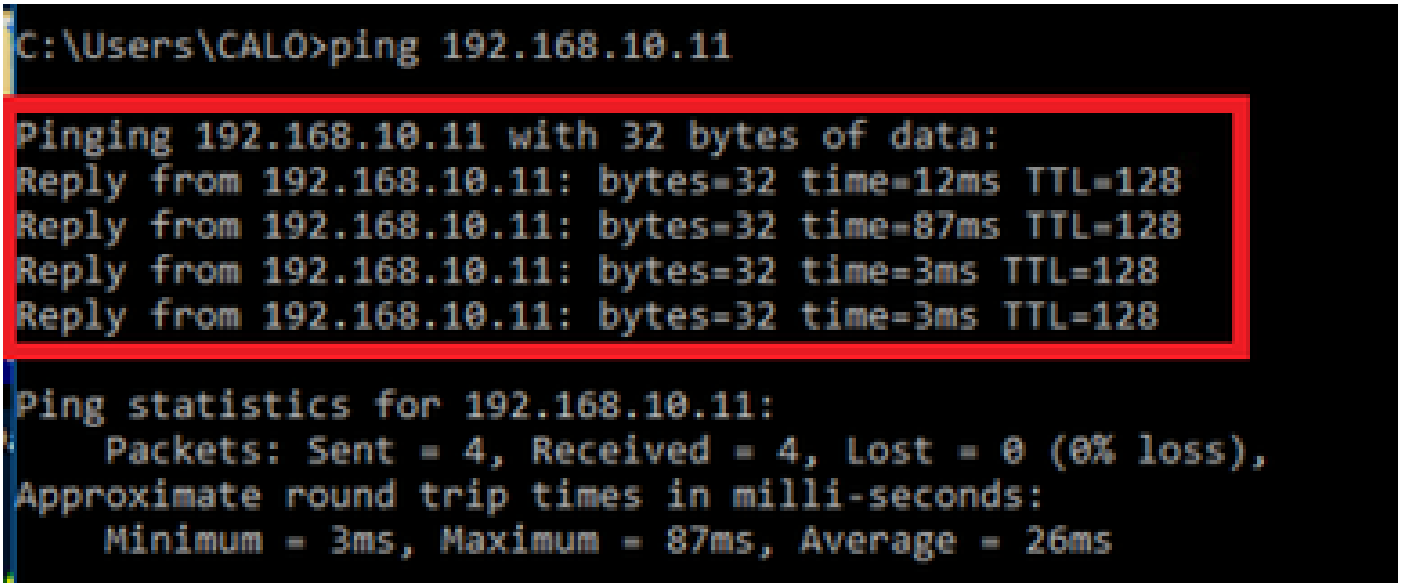
```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
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 : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb00718200007000666fa19e
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 7.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50035 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
```

Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 2292
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 7.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56382
UDP Dst Port : 443 Auth Mode : Certificate and 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 5.1.3.62
Bytes Tx : 0 Bytes Rx : 13094
Pkts Tx : 0 Pkts Rx : 34
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Étape 4. 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.



Ping réussi

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

<#root>

ftd702#

capture in interface inside real-time

```
Use ctrl-c to terminate real-time capture

1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 03:39:28.808399 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 le PC Windows.

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

```
// Certificate Authentication
Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name:  CN=sslVPNClientCl

// Extract username from the CN (Common Name) field
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested.  [Request 5]
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed.  [Request 5]

// AAA Authentication
Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 17 2024 02:38:22: %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

Référence

Configuration d'AnyConnect Remote Access VPN sur FTD

Configurer l'authentification basée sur certificat Anyconnect pour l'accès mobile

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.