

Configurer la correspondance de certificat pour l'authentification client sécurisée sur FTD via FDM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration dans FDM](#)

[Étape 1. Configurer l'interface FTD](#)

[Étape 2. Confirmer la licence Cisco Secure Client](#)

[Étape 3. Ajouter un pool d'adresses](#)

[Étape 4. Créer un profil client sécurisé](#)

[Étape 5. Télécharger le profil client sécurisé vers FDM](#)

[Étape 6. Ajouter une stratégie de groupe](#)

[Étape 7. Ajouter un certificat FTD](#)

[Étape 8. Ajouter une AC au FTD](#)

[Étape 9. Ajouter un profil de connexion VPN d'accès à distance](#)

[Étape 10. Confirmer le résumé du profil de connexion](#)

[Confirmer dans FTD CLI](#)

[Confirmer dans le client VPN](#)

[Étape 1. Copier le profil de client sécurisé vers le client VPN](#)

[Étape 2. Confirmer le certificat client](#)

[Étape 3. Confirmer CA](#)

[Vérifier](#)

[Étape 1. Initiation de la connexion VPN](#)

[Étape 2. Confirmer les sessions VPN dans FTD CLI](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer Cisco Secure Client avec SSL sur FTD via FDM en utilisant la correspondance de certificat pour l'authentification.

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
- Éditeur de profil (Windows) 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

CertificateMatch est une fonctionnalité qui permet aux administrateurs de configurer des critères que le client doit utiliser pour sélectionner un certificat client pour l'authentification avec le serveur VPN. Cette configuration est spécifiée dans le profil client, qui est un fichier XML pouvant être géré à l'aide de l'Éditeur de profil ou modifié manuellement. La fonctionnalité CertificateMatch peut être utilisée pour améliorer la sécurité des connexions VPN en s'assurant que seul un certificat avec des attributs spécifiques est utilisé pour la connexion VPN.

Ce document décrit comment authentifier le client sécurisé Cisco en utilisant le nom commun d'un certificat SSL.

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

- CA : ftd-ra-ca-common-name
- Certificat du client VPN de l'ingénieur : vpnEngineerClientCN
- Certificat du client VPN du gestionnaire : vpnManagerClientCN
- Certificat du serveur : 192.168.1.200

Diagramme du réseau

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

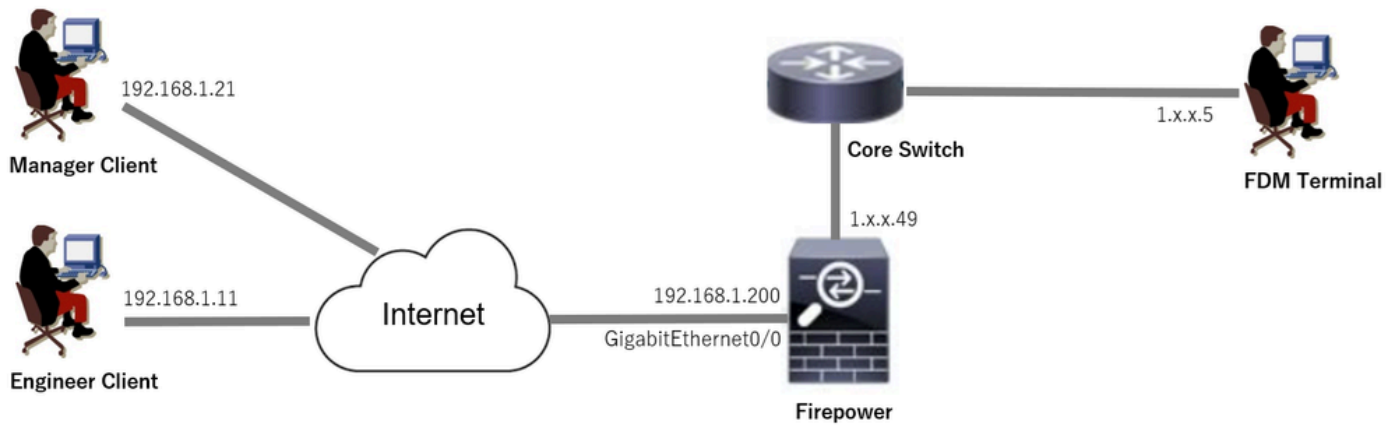


Diagramme du réseau

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

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ GigabitEthernet0/0	outside	<input checked="" type="checkbox"/>	Routed	192.168.1.200/24		Enabled	

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.

The screenshot shows the 'SUBSCRIPTION LICENSES INCLUDED' section in the Cisco Secure Firewall Device Manager. The 'RA VPN License' is highlighted with a red box. It is currently 'Enabled' and has a 'Type' dropdown set to 'VPN ONLY'. Other licenses shown include Threat, Malware, and URL License, all of which are disabled by the user.

Licence client sécurisée

Étape 3. Ajouter un pool d'adresses

Accédez à Objets > Réseaux, cliquez sur + bouton.

The screenshot shows the 'Object Types' section in the Cisco Secure Firewall Device Manager. The 'Networks' option is highlighted with a red box. The 'Objects' tab is also highlighted with a red box. A table of network objects is visible, with one object listed: 'IPv4-Private-10.0.0.0-8'.

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	

Ajouter un pool d'adresses

Entrez les informations nécessaires pour ajouter un nouveau pool d'adresses IPv4. Cliquez sur le bouton OK.

- Nom : ftd-cert-match-pool
- Type : Plage
- Plage IP : 172.16.1.150-172.16.1.160

Add Network Object



Name

ftd-cert-match-pool

Description

Type



Network



Host



FQDN



Range

IP Range

172.16.1.150-172.16.1.160

e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100

CANCEL

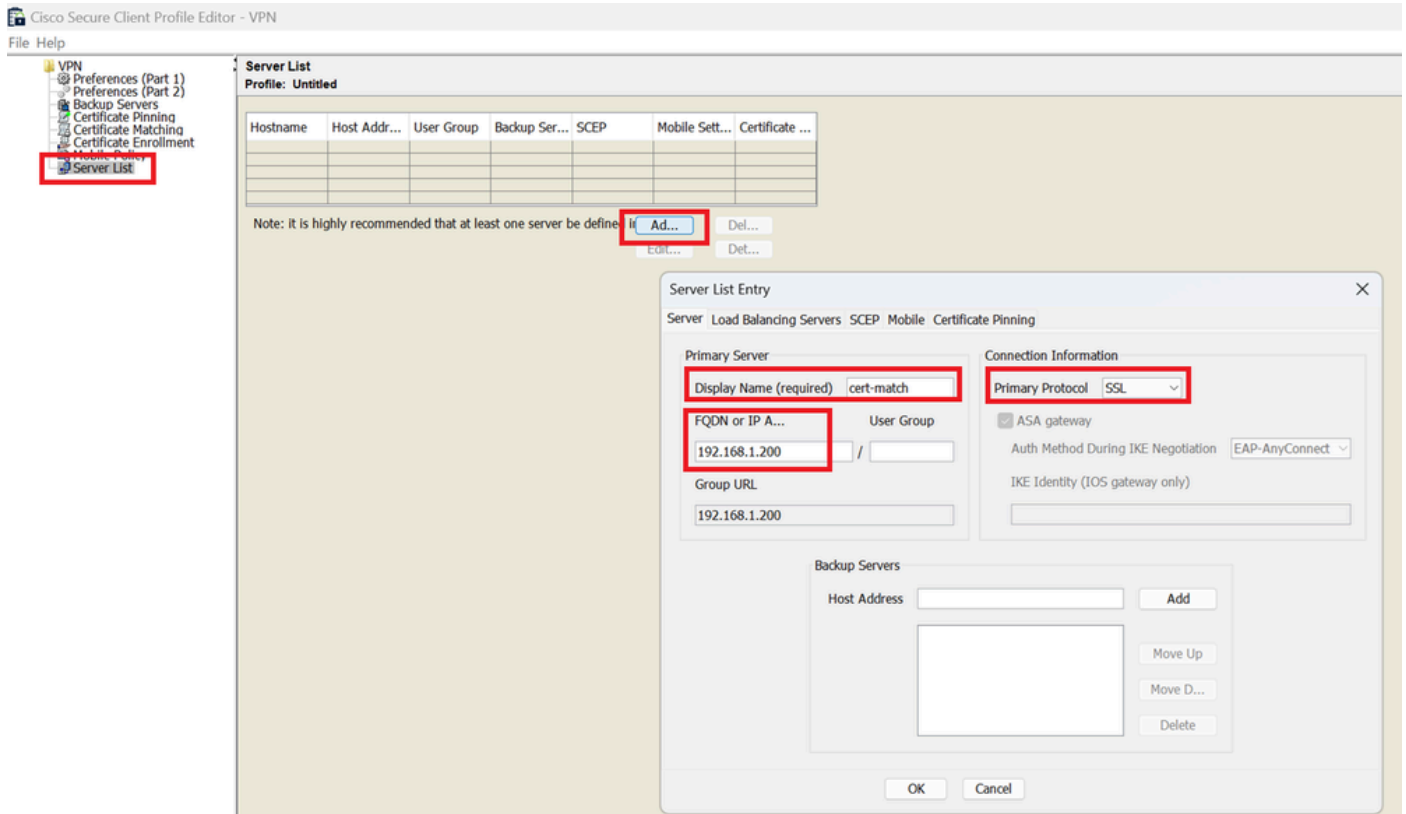
OK

Détail du pool d'adresses IPv4

Étape 4. Créer un profil client sécurisé

Téléchargez et installez Secure Client Profile Editor à partir du site [Cisco Software](#). Accédez à Server List, cliquez sur Add button. Entrez les informations nécessaires pour ajouter une entrée de liste de serveurs et cliquez sur le bouton OK.

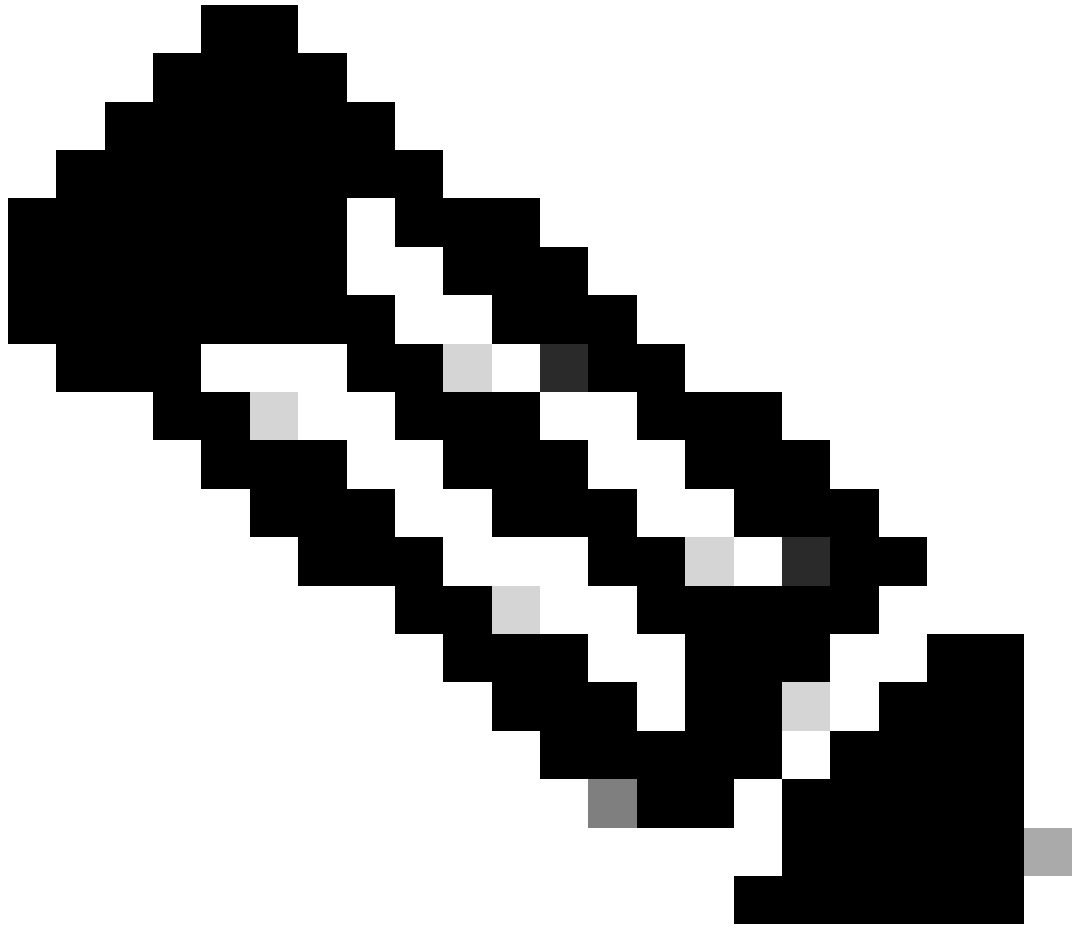
- Nom d'affichage : cert-match
- Nom de domaine complet ou adresse IP : 192.168.1.200
- Protocole principal : SSL



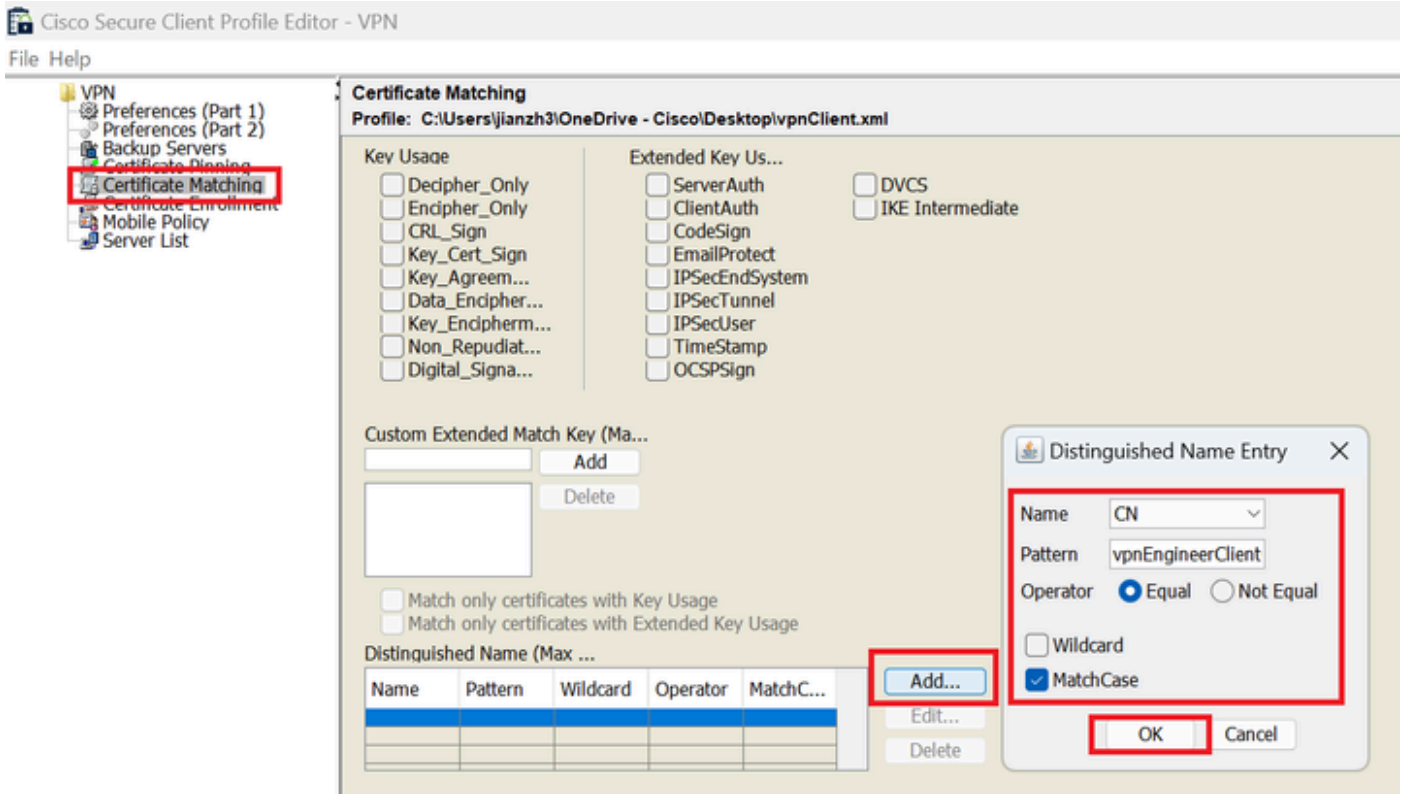
Entrée de liste de serveurs

Accédez à Certificate Matching, cliquez sur Add button. Entrez les informations nécessaires pour ajouter une entrée de nom unique et cliquez sur le bouton OK.

- Nom : CN
- Modèle : vpnEngineerClientCN
- Opérateur : égal



Remarque : cochez l'option MatchCase dans ce document.



Entrée de nom distinctif

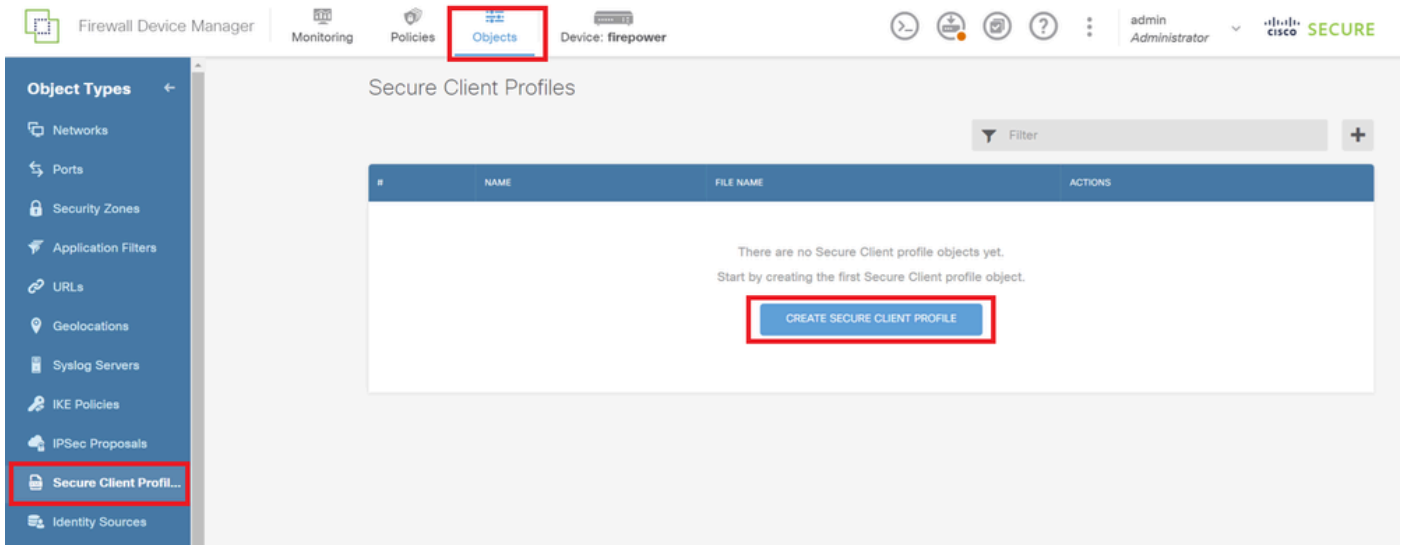
Enregistrez le profil client sécurisé sur l'ordinateur local et confirmez les détails du profil.



Profil client sécurisé

Étape 5. Télécharger le profil client sécurisé vers FDM

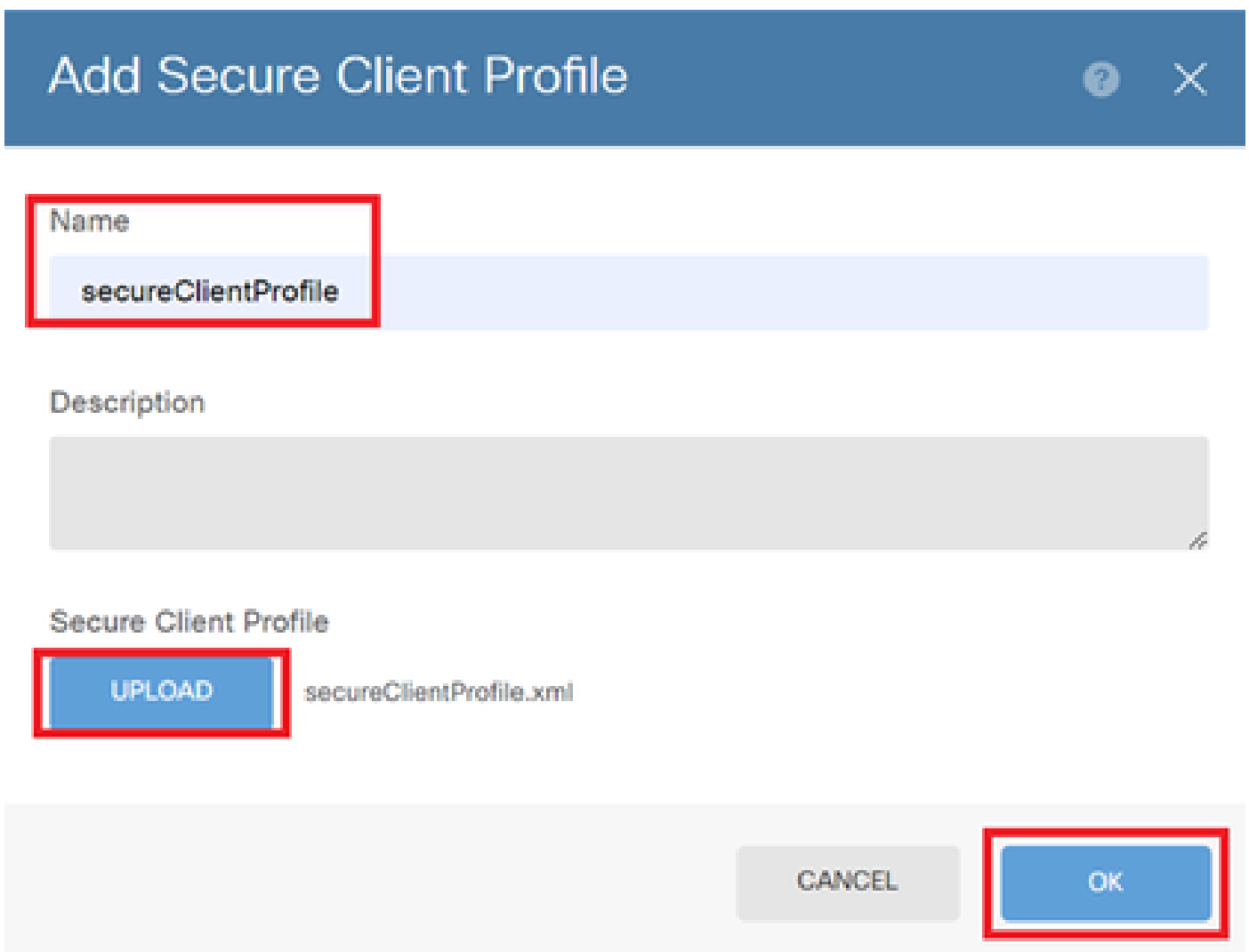
Accédez à Objets > Profil client sécurisé, cliquez sur le bouton CREATE SECURE CLIENT PROFILE.



Créer un profil client sécurisé

Entrez les informations nécessaires pour ajouter un profil client sécurisé et cliquez sur le bouton OK.

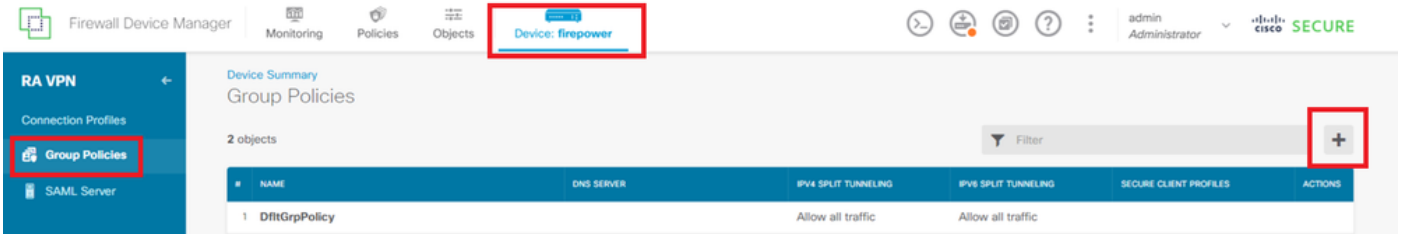
- Nom : secureClientProfile
- Profil client sécurisé : secureClientProfile.xml (téléchargement à partir de l'ordinateur local)



Ajouter un profil client sécurisé

Étape 6. Ajouter une stratégie de groupe

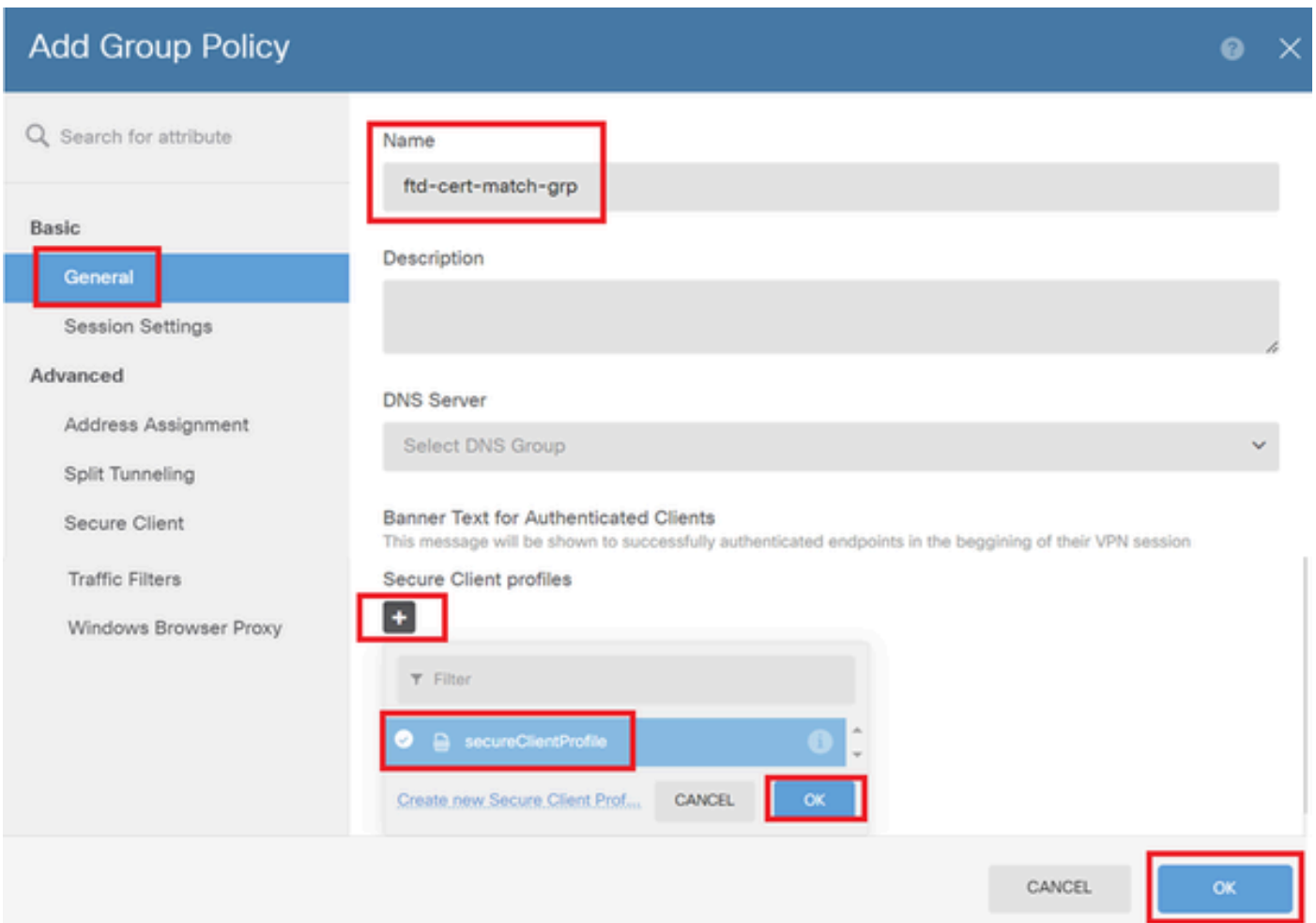
Accédez à Device > Remote Access VPN > View Configuration > Group Policies, cliquez sur + button.



Ajouter une stratégie de groupe

Entrez les informations nécessaires pour ajouter une stratégie de groupe et cliquez sur OK.

- Nom : ftd-cert-match-grp
- Profils clients sécurisés : secureClientProfile



Détails de la stratégie de groupe

Étape 7. Ajouter un certificat FTD

Accédez à Objets > Certificats, cliquez sur Ajouter un certificat interne à partir de l'élément +.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | cisco SECURE

Object Types ←

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates**

Certificates

121 objects

Filter

Preset filters: System defined, User defined

#	NAME	TYPE	ACTIONS
1	AAA-Certificate-Services	Trusted CA Certificate	
2	ACCVRAIZ1	Trusted CA Certificate	
3	Actalis-Authentication-Root-CA	Trusted CA Certificate	
4	AffirmTrust-Commercial	Trusted CA Certificate	
5	AffirmTrust-Networking	Trusted CA Certificate	
6	AffirmTrust-Premium	Trusted CA Certificate	
7	AffirmTrust-Premium-ECC	Trusted CA Certificate	
8	Amazon-Root-CA-1	Trusted CA Certificate	
9	Amazon-Root-CA-2	Trusted CA Certificate	
10	Amazon-Root-CA-3	Trusted CA Certificate	
11	DefaultInternalCertificate	Internal Certificate	
12	DefaultWebserverCertificate	Internal Certificate	

Actions: Add Internal CA, **Add Internal Certificate**, Add Trusted CA Certificate

Ajouter un certificat interne

Cliquez sur Télécharger le certificat et la clé.

Choose the type of internal certificate you want to create

Upload Certificate and Key
Create a certificate from existing files.
PEM and DER files are supported.

Self-Signed Certificate
Create a new certificate that is signed by the device.

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 : ftd-vpn-cert
- Utilisation de la validation pour les services spéciaux : serveur SSL

Add Internal Certificate

Name

ftd-vpn-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

[Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----
MIIDfDCCAmSgAwIBAgIIIkE99YS2cmwDQYJKoZIhvcNAQELBQAwTELMAkGA1UE
BhMCS1AxOjQjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUB2t5bzEOMAwGA1UE
ChMF
O31-V38-w04AMP-wBDA-TBIAkx78k-MQ4-UAYDQCEwUw4C9t-wEwY3EwY3QwKLD...
```

Certificate Key

Paste certificate key, or choose a file (KEY, PEM)

[Upload Certificate Key](#)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAxdn5eTUngo5+GUG2Ng2FjI/+xHRkR-f6o20ccGdzLYK1tzwB
98HPu1YP0T/qwCfFKXuMQ9DEVGMIjLRX9nvXdBNoakUbZVzc03qM3AjE87p0h0t0
+42b1MPTw-0u41-1-1-w03-wE-wY6E9-1u4140-73E-wT4E-wM-73w-773A-w8wE-wE...
```

Validation Usage for Special Services

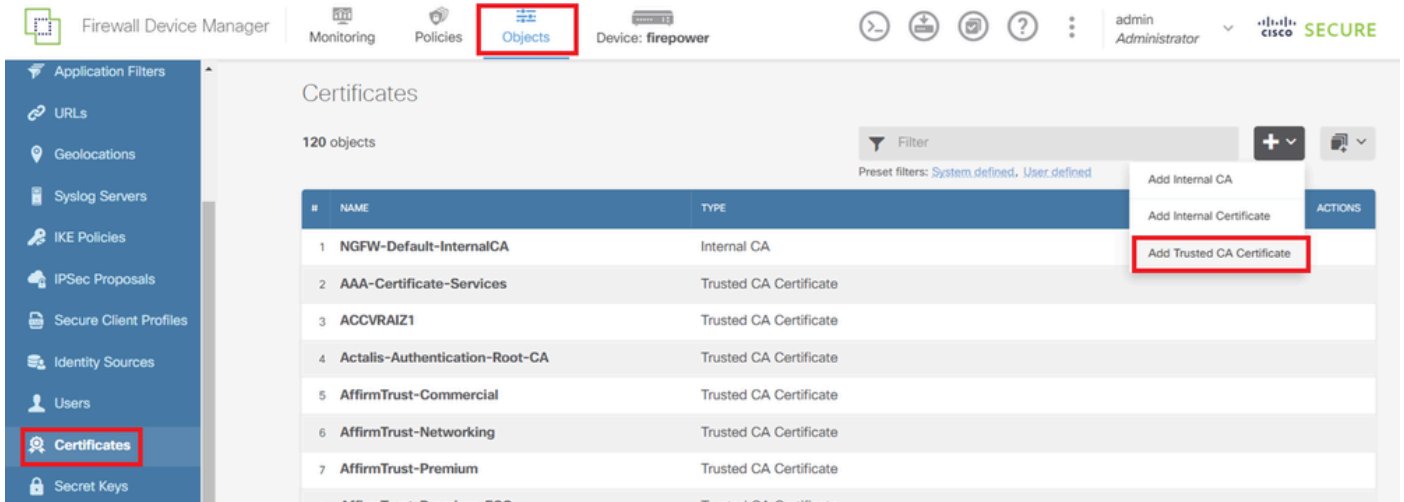
SSL Server

CANCEL OK

Détails du certificat interne

Étape 8. Ajouter une AC au FTD

Accédez à Objets > Certificats, cliquez sur Ajouter un certificat CA approuvé à partir de l'élément +.



Ajouter un certificat CA approuvé

Entrez les informations nécessaires pour l'autorité de certification, importez un certificat depuis l'ordinateur local.

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

Add Trusted CA Certificate



Name

ftdvpn-ca-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

ftd-ra-ca.crt

Upload Certificate

```
-----BEGIN CERTIFICATE-----
MIIDbDCCA1SgAwIBAgIIUkKgLG229/0wDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE
BHMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUub2t5bzEOMAwGA1UE
CChMFo31vMQ4wDAYDVQIYbTBRb2t5bzEwDQYJKoZIhvcNAQEFBQAwYzEwDQYJ
```

Skip CA Certificate Check

Validation Usage for Special Services

SSL Client

CANCEL

OK

Détails du certificat CA approuvé

Étape 9. Ajouter un profil de connexion VPN d'accès à distance

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

Firewall Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator | cisco SECURE

RA VPN

Connection Profiles

Group Policies

SAML Server

Device Summary

Remote Access VPN Connection Profiles

#	NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.				

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 Next .

- Nom du profil de connexion : ftd-cert-match-vpn
- Type d'authentification : certificat client uniquement
- Nom d'utilisateur du certificat : champ spécifique au mappage
- Champ principal : CN (nom commun)
- Champ secondaire : OU (Unité organisationnelle)
- Pools d'adresses IPv4 : ftd-cert-match-pool

Remote Access VPN

1 Connection and Client Configuration 2 Remote User Experience 3 Global Settings 4 Summary

Remote Users Secure Clients Internet Client Certificate FIREPOWER OUTSIDE INTERFACES INSIDE INTERFACES Corporate Resources Identity Source for User Authentication

Connection and Client Configuration

Specify how to authenticate remote users and the secure clients they can use to connect to the inside network.

Connection Profile Name
This name is configured as a connection alias, it can be used to connect to the VPN gateway
ftd-cert-match-vpn

Group Alias (one per line, up to 5)
ftd-cert-match-vpn

Group URL (one per line, up to 5)

Primary Identity Source
Authentication Type
Client Certificate Only

Username from Certificate
Map Specific Field
Primary Field: CN (Common Name) Secondary Field: OU (Organisational Unit)
Use entire DN (distinguished name) as username
Advanced

Authorization Server
Please select

Accounting Server
Please select

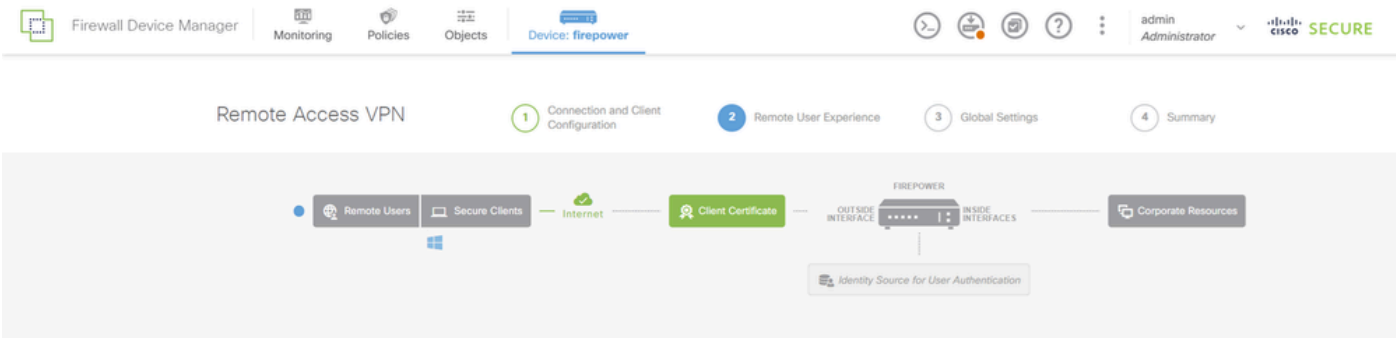
Client Address Pool Assignment
IPv4 Address Pool
Endpoints are provided an address from this pool
ftd-cert-match-pool
DHCP Servers

CANCEL NEXT

Détails du profil de connexion VPN

Entrez les informations nécessaires à la stratégie de groupe et cliquez sur Next .

- Afficher la stratégie de groupe : ftd-cert-match-grp



Remote User Experience

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

View Group Policy

ftd-cert-match-grp

Policy Group Brief Details

DNS + BANNER Edit

DNS Server None

Banner Text for Authentication

BACK NEXT

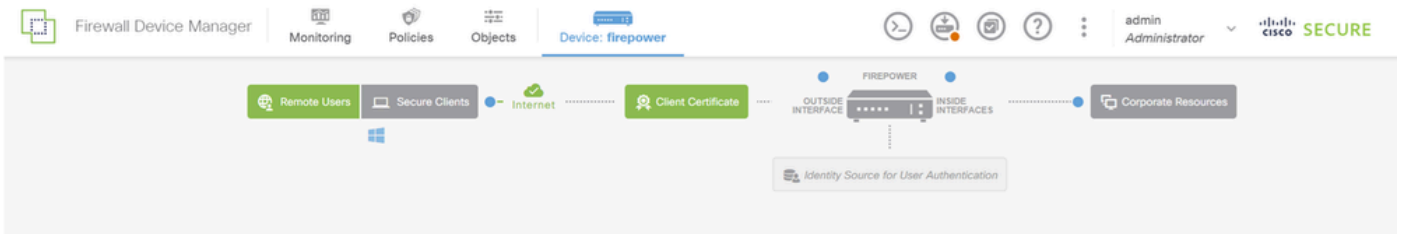
Sélectionner une stratégie de groupe

Sélectionnez Certificate of Device Identity, Outside Interface, Secure Client Package pour la connexion VPN.

- Certificat d'identité du périphérique : ftd-vpn-cert
- Interface externe : externe (GigabitEthernet0/0)
- Package client sécurisé : cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



Remarque : fonction NAT Exempt désactivée dans ce document.



Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity
ftd-vpn-cert (Validation Usage: SSL Se...)

Outside Interface
outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface
Port
e.g. ravn.example.com 443
e.g. 8080

Access Control for VPN Traffic
Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic.
 Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT Exempt

Secure Client Package
If a user does not already have the right secure client package installed, the system will launch the secure client installer when the client authenticates for the first time. The user can then install the package from the system.
You can download secure client packages from software.cisco.com.
You must have the necessary secure client software license.

Packages
UPLOAD PACKAGE
Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK NEXT

Détails des paramètres globaux

Étape 10. Confirmer le résumé du profil de connexion

Confirmez les informations entrées pour la connexion VPN et cliquez sur le bouton FINISH.

^ Summary

Review the summary of the Remote Access VPN configuration.

Ftd-Cert-Match-Vpn

STEP 1: CONNECTION AND CLIENT CONFIGURATION

Primary Identity Source

Authentication Type: Client Certificate Only

Primary Identity Source: -

Fallback Local Identity Source: -

Username from Certificate: Map Specific Field

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Advanced

Authorization Server

Accounting Server

Client Address Pool Assignment

IPv4 Address Pool: ftd-cert-match-pool

IPv6 Address Pool: -

DHCP Servers: -

STEP 2: GROUP POLICY

Group Policy Name: ftd-cert-match-grp

Banner + DNS Server

DNS Server: -

Banner text for authenticated clients: -

Session Settings

Maximum Connection Time / Alert Interval: Unlimited / 1 minutes

Idle Timeout / Alert Interval: 30 / 1 minutes

Simultaneous Login per User: 3

Split Tunneling

IPv4 Split Tunneling: Allow all traffic over tunnel

IPv6 Split Tunneling: Allow all traffic over tunnel

Secure Client

Secure Client Profiles: secureClientProfile

STEP 3: GLOBAL SETTINGS

Certificate of Device Identity: ftd-vpn-cert

Outside Interface: GigabitEthernet0/0 (outside)

Fully-qualified Domain Name for the Outside Interface: -

Port: 443

Access Control for VPN Traffic: No

NAT Exempt

NAT Exempt: No

Inside Interfaces: -

Inside Networks: -

Secure Client Package

Packages: Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK FINISH

Confirmer le résumé du profil de connexion

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 FDM.

```
// Defines IP of interface
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

// Defines a pool of addresses
ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftd-vpn-cert
enrollment terminal
keypair ftd-vpn-cert
cr1 configure

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

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client
cr1 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 profiles secureClientProfile disk0:/anyconnprofs/secureClientProfile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable
```

```
// Configures the group-policy to allow SSL connections
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
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 value secureClientProfile type user
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting
```

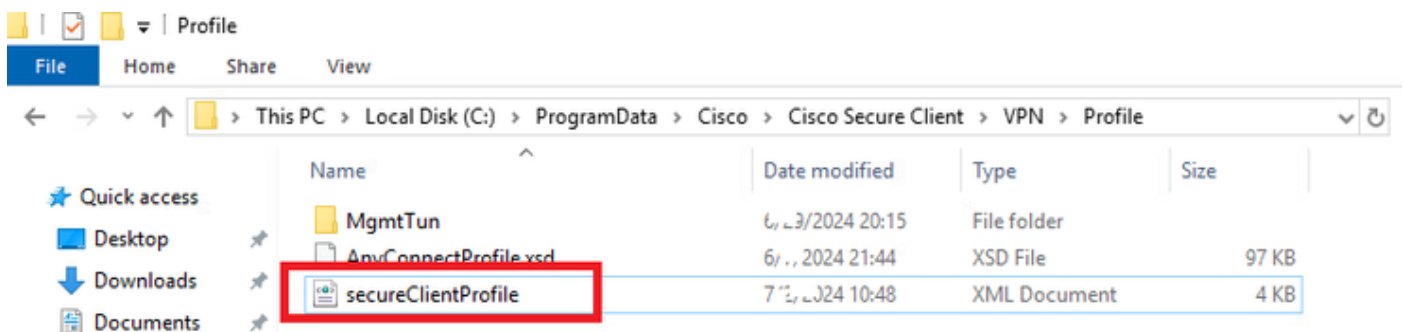
```
// Configures the tunnel-group to use the certificate authentication
tunnel-group ftd-cert-match-vpn type remote-access
tunnel-group ftd-cert-match-vpn general-attributes
address-pool ftd-cert-match-pool
default-group-policy ftd-cert-match-grp
tunnel-group ftd-cert-match-vpn webvpn-attributes
authentication certificate
group-alias ftd-cert-match-vpn enable
```

Confirmer dans le client VPN

Étape 1. Copier le profil de client sécurisé vers le client VPN

Copiez le profil client sécurisé pour concevoir le client VPN et le client VPN du manager.

Remarque : le répertoire du profil client sécurisé sur l'ordinateur Windows :
C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



Copier le profil de client sécurisé vers le client VPN

Étape 2. Confirmer le certificat client

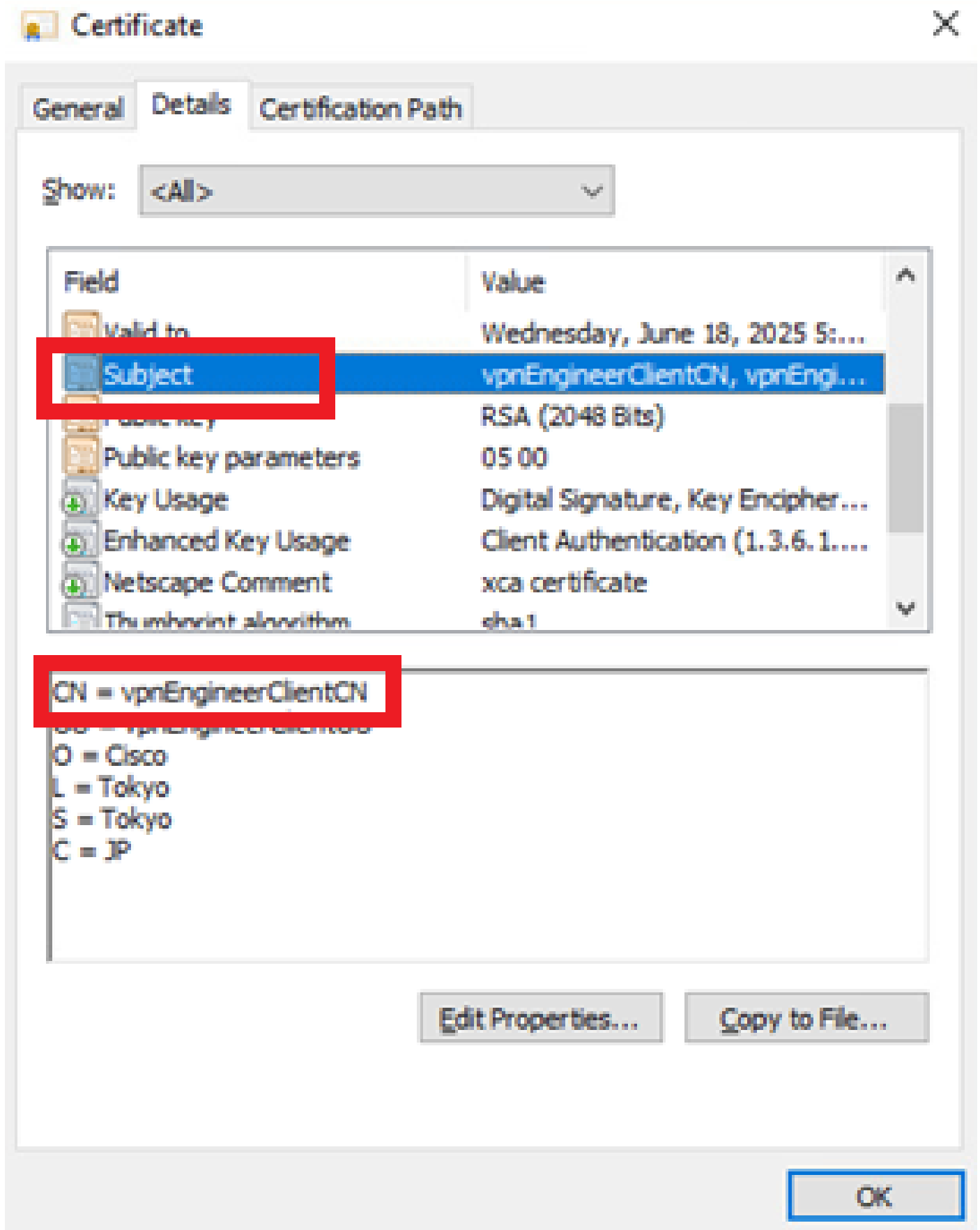
Dans Engineer VPN Client, accédez à Certificates - Current User > Personal > Certificates, vérifiez le certificat client utilisé pour l'authentification.



Confirmer le certificat du client VPN de l'ingénieur

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

- Objet : CN = vpnEngineerClientCN



Détails du certificat du client ingénieur

Dans le client VPN du gestionnaire, naviguez vers Certificates - Current User > Personal > Certificates, vérifiez le certificat client utilisé pour l'authentification.



Confirmer le certificat pour le client VPN Manager

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

- Objet : CN = vpnManagerClientCN

Certificate



General Details Certification Path

Show: <All>

Field	Value
Issued To	Thursday, June 19, 2025 9:41...
Subject	vpnManagerClientCN, vpnMan...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Comment	xca certificate
Thumbprint algorithm	sha1

CN = vpnManagerClientCN
O = Cisco
L = Tokyo
S = Tokyo
C = JP

Edit Properties... Copy to File...

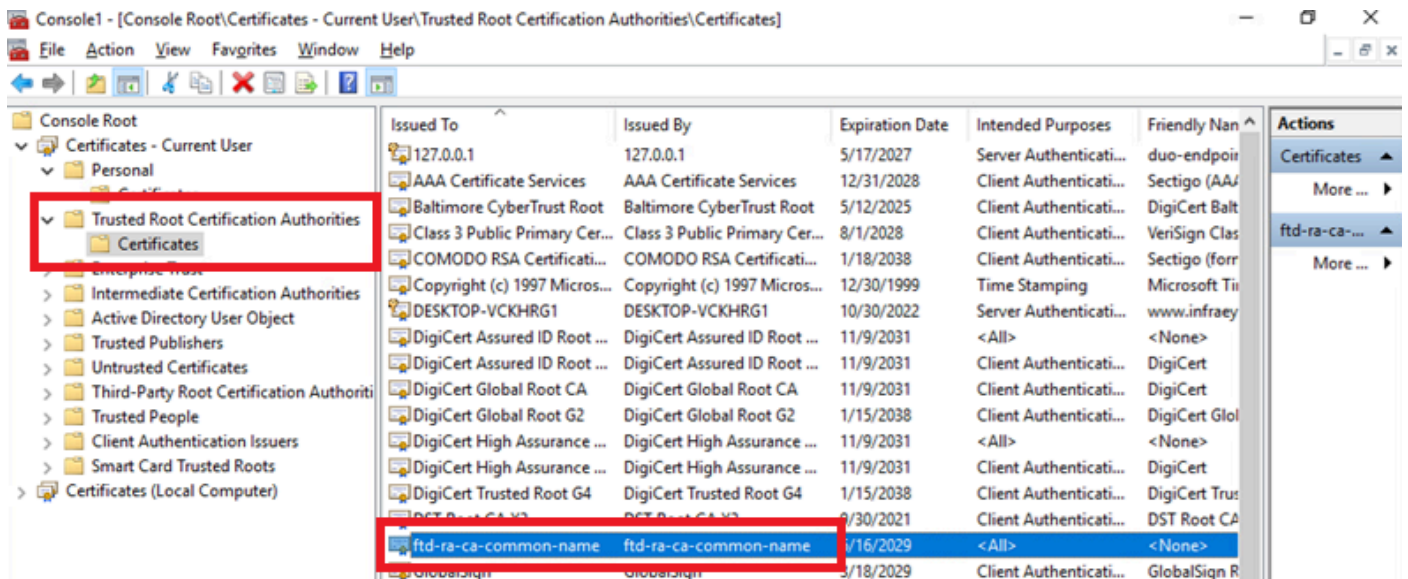
OK

Détails du certificat client du manager

Étape 3. Confirmer CA

Dans le client VPN ingénieur et le client VPN gestionnaire, naviguez vers Certificates - Current User > Trusted Root Certification Authorities > Certificates, vérifiez l'autorité de certification utilisée pour l'authentification.

- Émis par : ftd-ra-ca-common-name

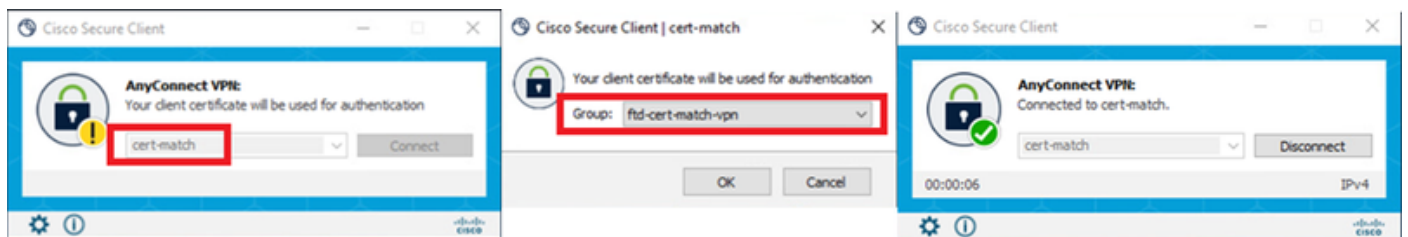


Confirmer CA

Vérifier

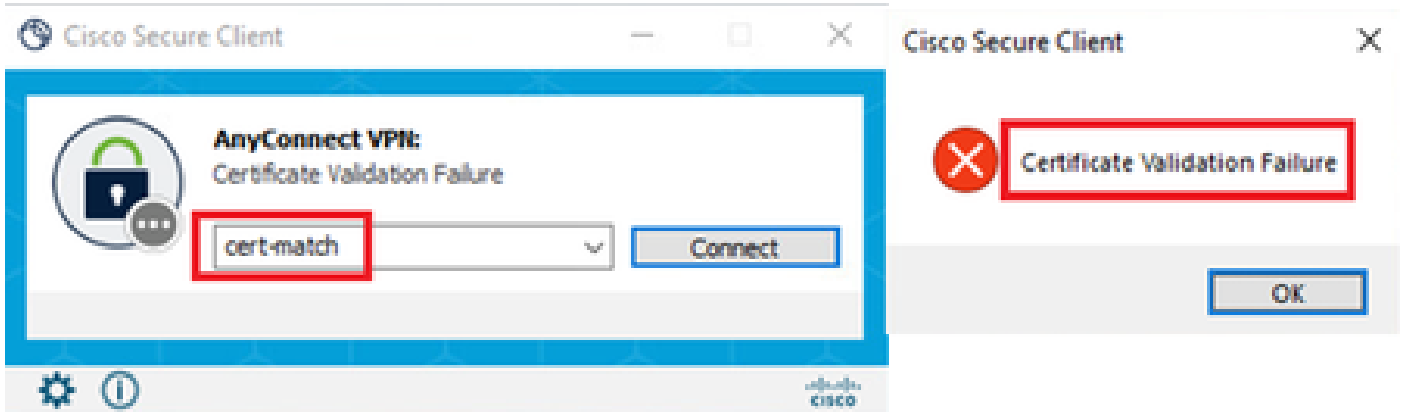
Étape 1. Initiation de la connexion VPN

Dans Engineer VPN Client, initiez la connexion Cisco Secure Client. Pas besoin d'entrer le nom d'utilisateur et le mot de passe, le VPN s'est connecté avec succès.



Connexion VPN réussie pour le client VPN de l'ingénieur

Dans le client VPN du gestionnaire, initiez la connexion du client sécurisé Cisco. Le VPN connecté a échoué en raison d'un échec de validation du certificat.



Échec de la connexion VPN pour le client VPN Manager

Étape 2. Confirmer les sessions VPN dans FTD CLI

Exécutez la commande `show vpn-sessiondb detail anyconnect` dans l'interface de ligne de commande FTD (Lina) pour confirmer les sessions VPN de l'ingénieur.

```
firepower# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username : vpnEngineerClientCN Index : 32
Assigned IP : 172.16.1.150 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 : 14718 Bytes Rx : 12919
Pkts Tx : 2 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn
Login Time : 05:42:03 UTC Tue Jul 2 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0000000000200006683932b
Security Grp : none Tunnel Zone : 0
```

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

AnyConnect-Parent:

```
Tunnel ID : 32.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50170 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 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 : 7359 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 32.2
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 50177
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7359 Bytes Rx : 12919
Pkts Tx : 1 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0

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.

Ceci est un exemple de journaux de débogage dans le moteur Lina pendant la connexion VPN du client ingénieur.

```
Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN
Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN
Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN
Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 session
```

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.