# Configuration de la position VPN Linux avec ISE 3.3

## Table des matières



## Introduction

Ce document décrit comment configurer la position VPN Linux avec Identity Services Engine (ISE) et Firepower Threat Defense (FTD).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Client sécurisé Cisco
- VPN d'accès à distance sur Firepower Threat Defense (FTD)
- Identity Services Engine (ISE)

### Composants utilisés

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

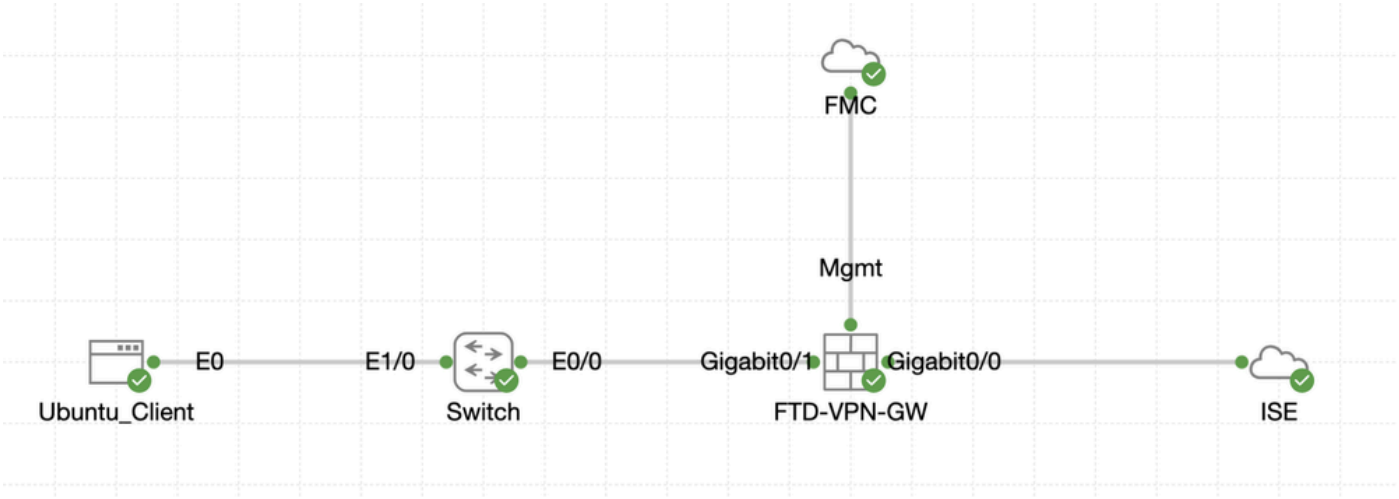
- Ubuntu 22.04
- Cisco Secure Client 5.1.3.62

- Cisco Firepower Threat Defense (FTD) 7.4.1
- Cisco Firepower Management Center (FMC) 7.4.1
- Cisco Identity Services Engine (ISE) 3.3

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.

# Configurer

## Diagramme du réseau



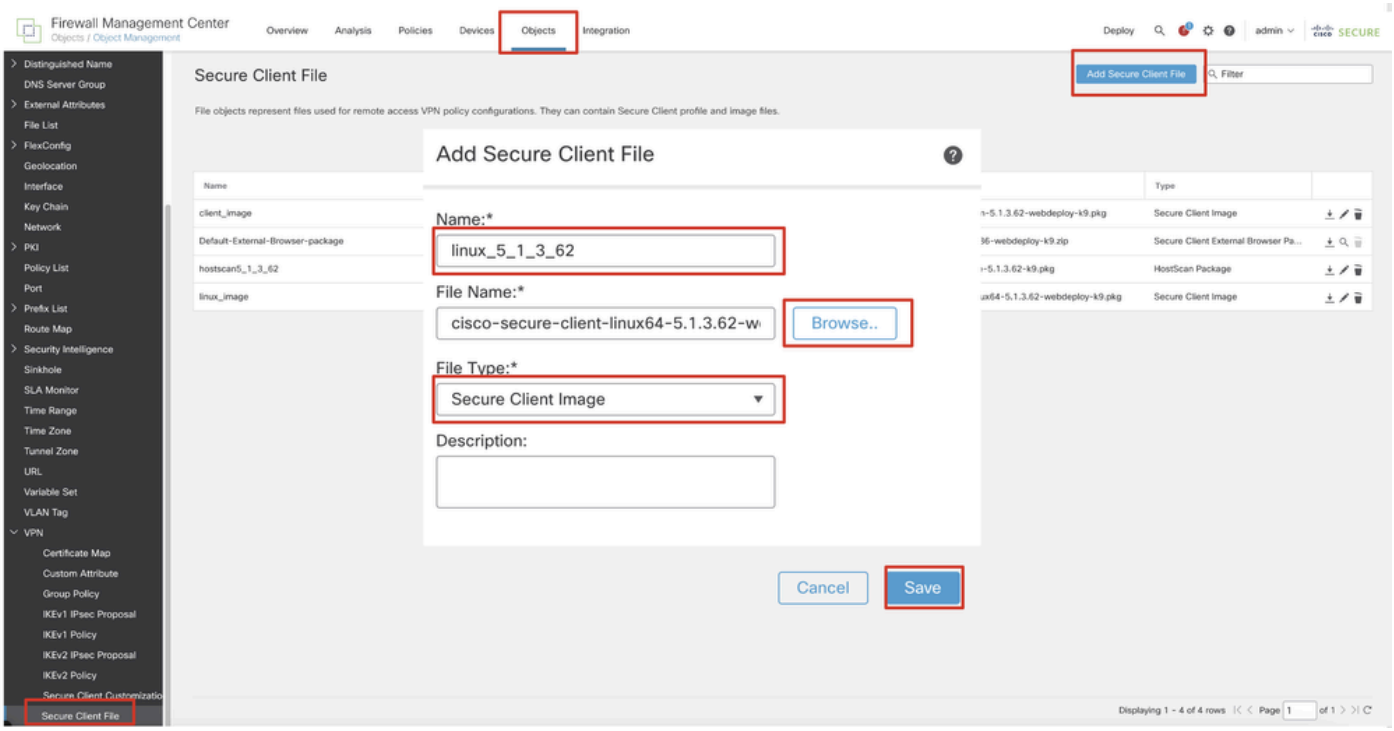

Topologie

## Configurations sur FMC/FTD

Étape 1. La connectivité entre le client, FTD, FMC et ISE a été correctement configurée. Comme enroll.cisco.com est utilisé pour les terminaux qui effectuent des tests de redirection (référez-vous aux documents CCO de flux de postureComparaison de style de posture ISE pour Pre et Post 2.2 pour plus de détails). Assurez-vous que la route du trafic vers enroll.cisco.com sur FTD est correctement configurée.

Étape 2. Téléchargez le nom cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg du package à partir de Cisco Software Download et assurez-vous 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 Cisco Software Download.

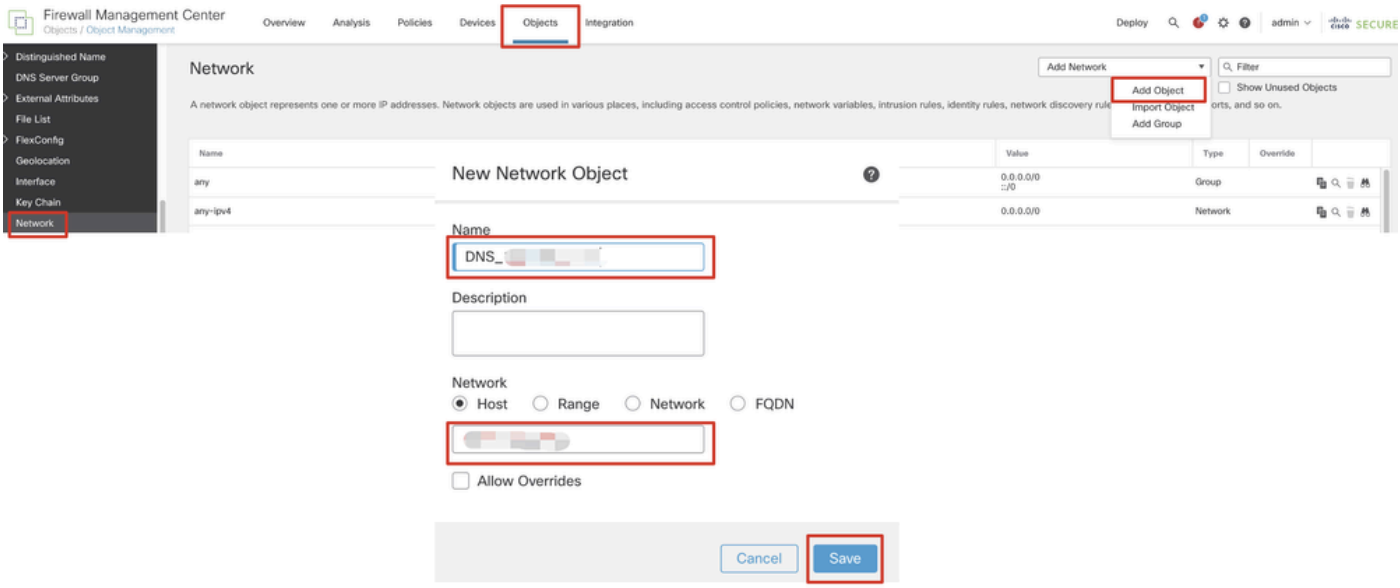
Étape 3. Accédez à Objects > Object Management > VPN > Secure Client File. Cliquez sur Add Secure Client File, indiquez le nom, recherchez File Name pour sélectionner cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg, sélectionnez Secure Client Image dans la liste déroulanteFile Type. Cliquez ensuite sur Save.



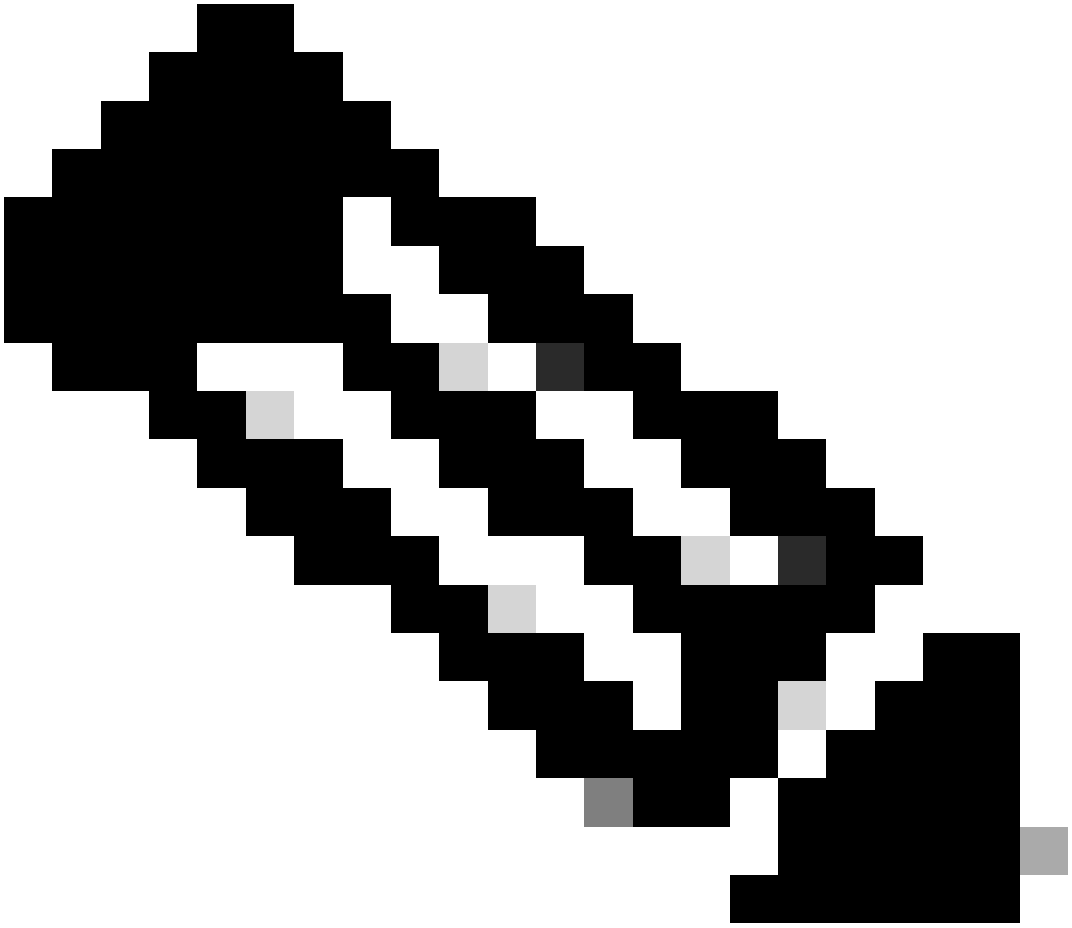

*Image_Client_Sécurisé_Téléchargement_FMC*

Étape 4. Accédez à Objects > Object Management > Network.

Étape 4.1. Créez un objet pour le serveur DNS. Cliquez sur Add Object, indiquez le nom et l'adresse IP DNS disponible. Cliquez sur Save.

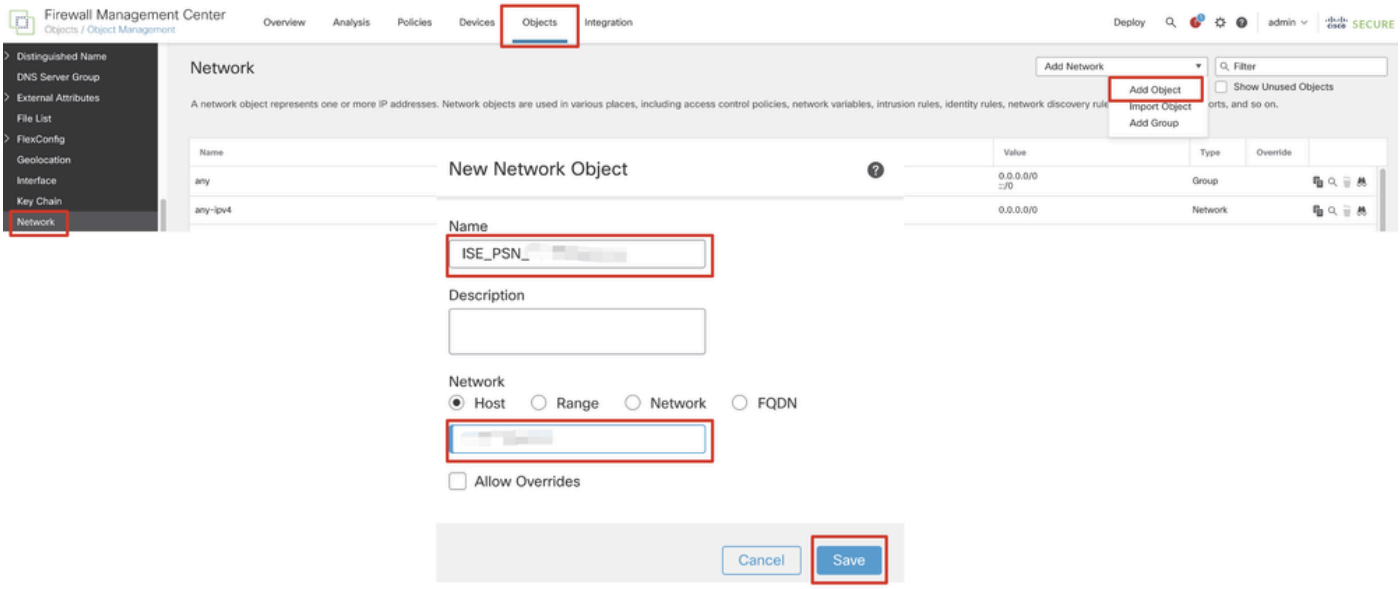



*FMC_Add_Object_DNS*



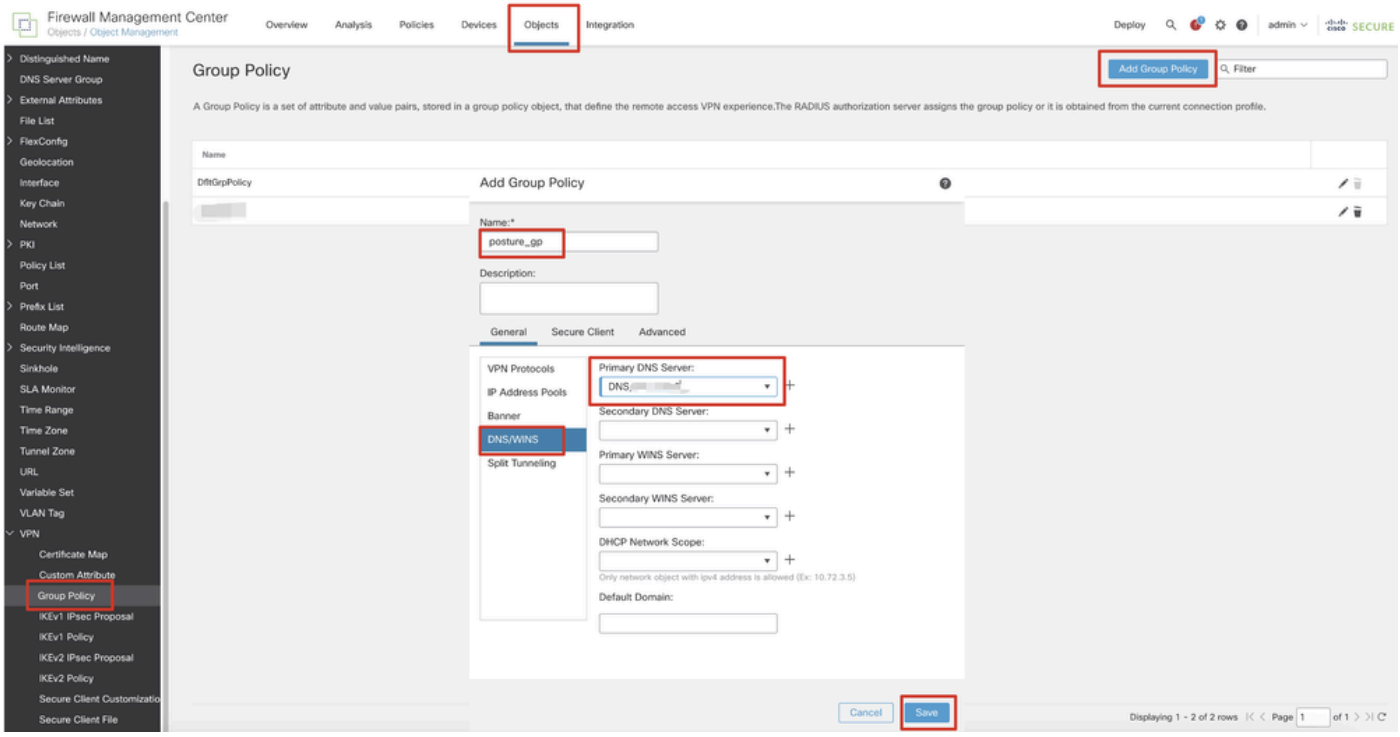
**Remarque** : le serveur DNS configuré ici doit être utilisé pour les utilisateurs VPN.

Étape 4.2. Créez un objet pour ISE PSN. Cliquez sur Add Object, indiquez le nom et l'adresse IP PSN ISE disponible. Cliquez sur Save.

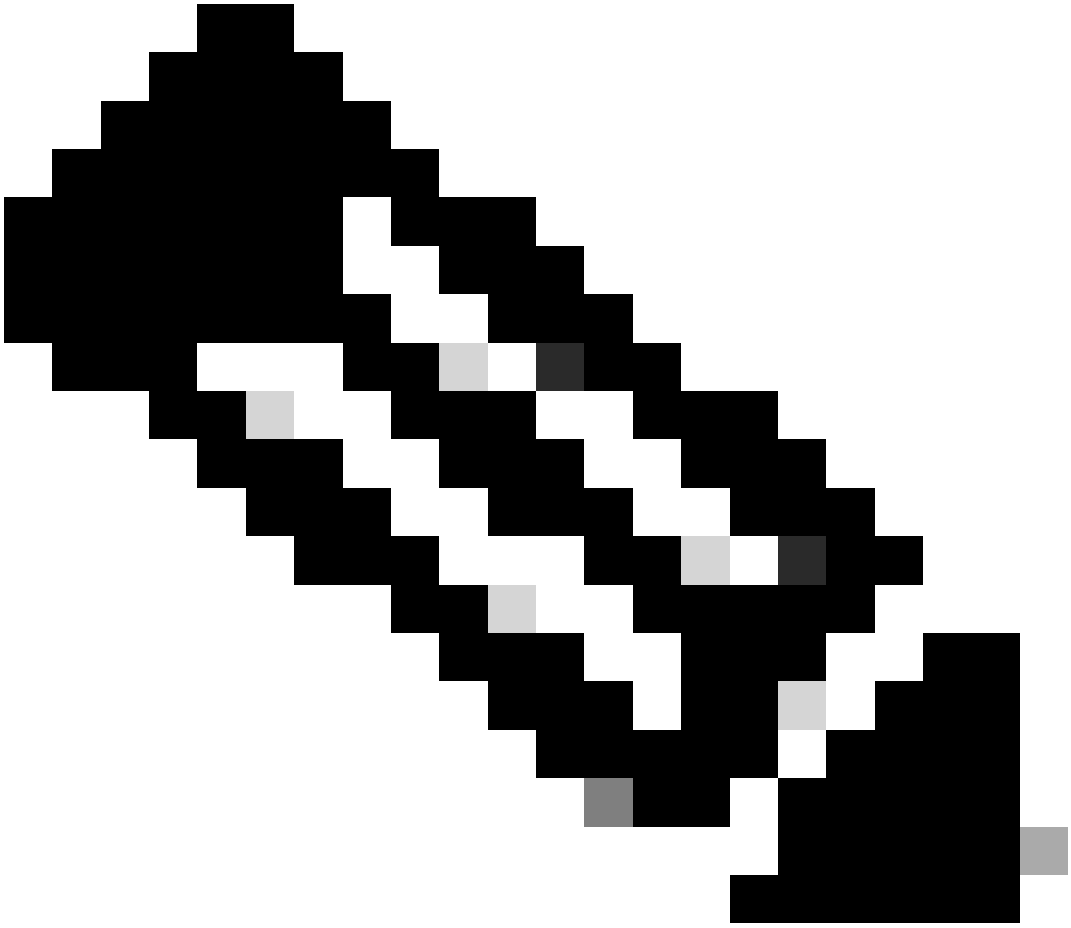



*FMC_Add_Object_ISE*

Étape 5. Accédez à Objects > Object Management > VPN > Group Policy. Cliquez sur Add Group Policy. Cliquez sur DNS/WINS, sélectionnez l'objet du serveur DNS dans Primary DNS Server. Cliquez ensuite sur Save.

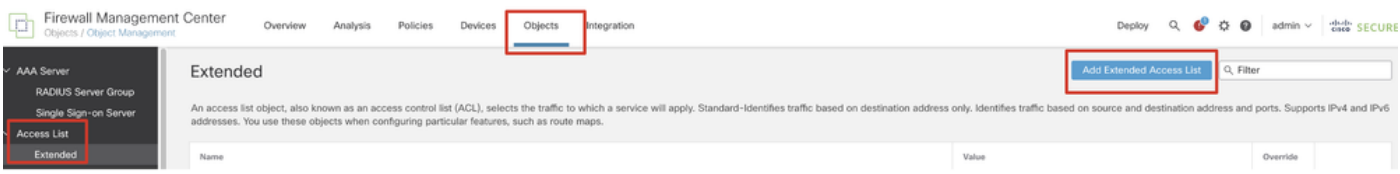



*FMC_Add_Group_Policy*



**Remarque** : assurez-vous que le serveur DNS utilisé dans la stratégie de groupe VPN peut résoudre le FQDN et le enroll.cisco.com du portail d'approvisionnement du client ISE.

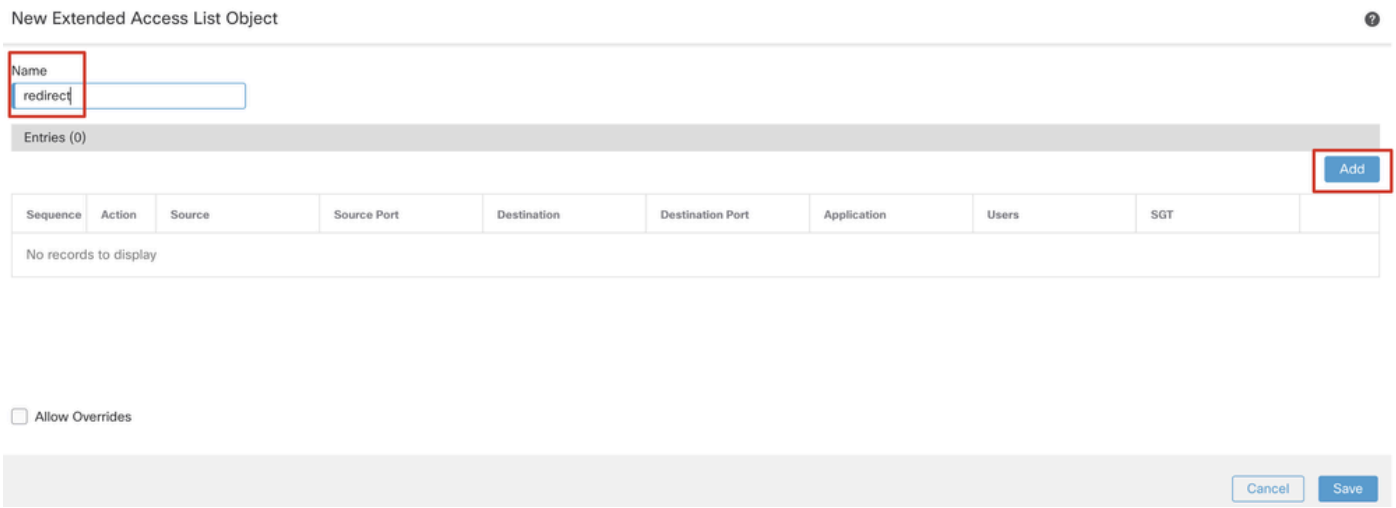
Étape 6. Accédez à Objects > Object Management > Access List > Extended. Cliquez sur Add Extended Access List.




*FMC_Add_Redirect_ACL*

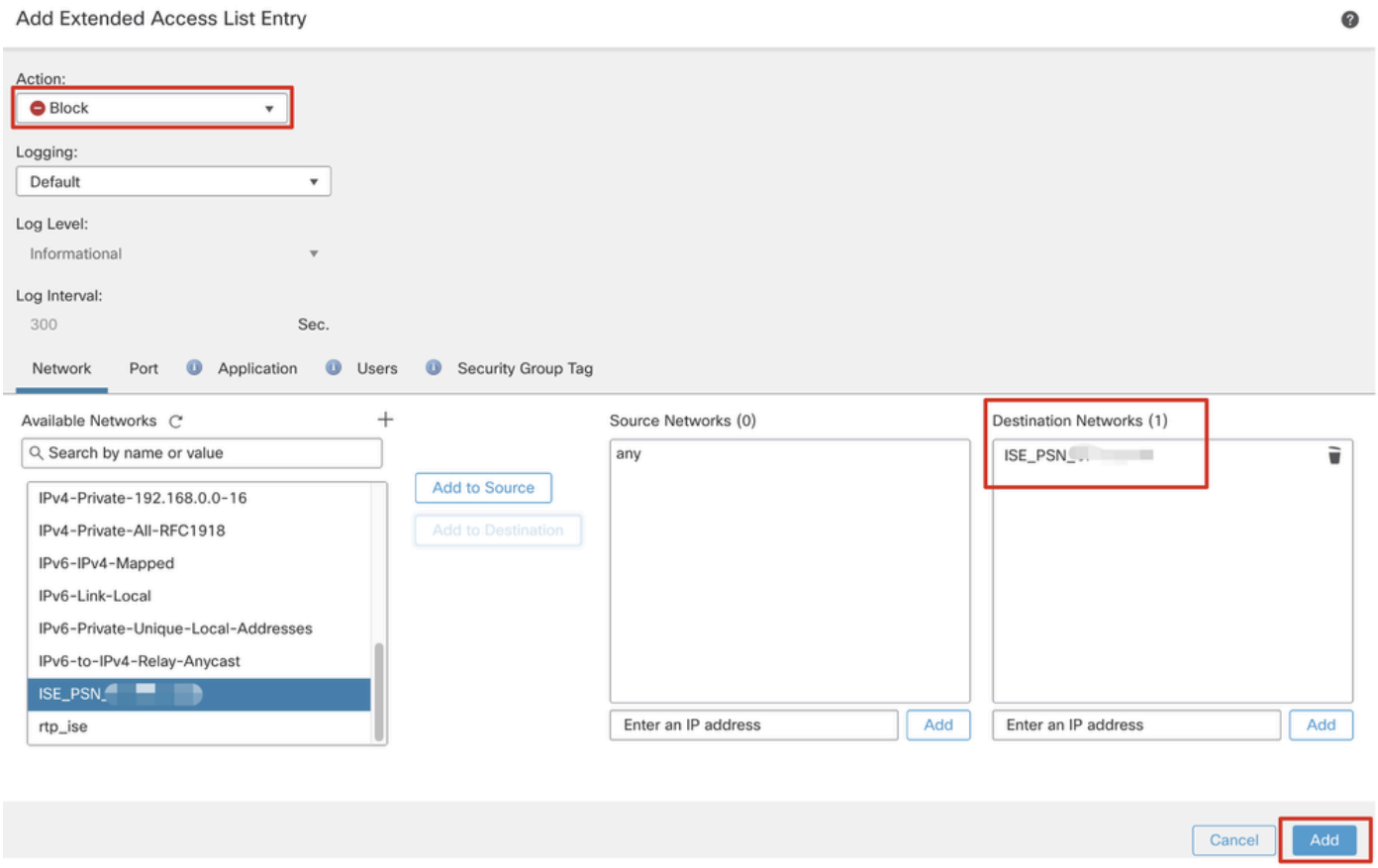
Étape 6.1. Indiquez le nom de la liste de contrôle d’accès de redirection. Ce nom doit être le même que dans le profil d'autorisation ISE. Cliquez

sur Add.

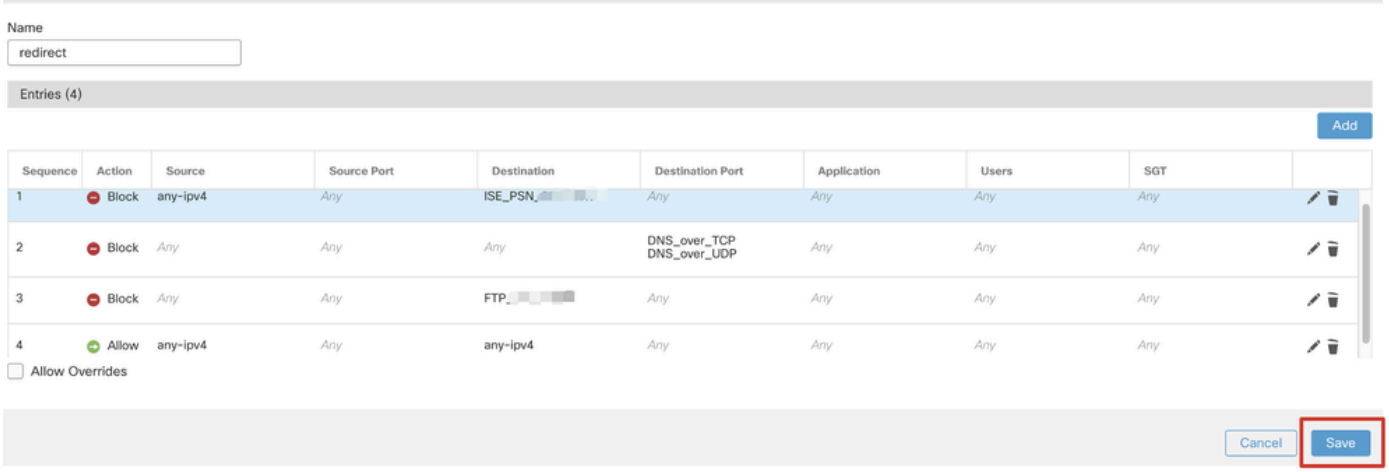



*FMC_Add_Redirect_ACL_Part_1*

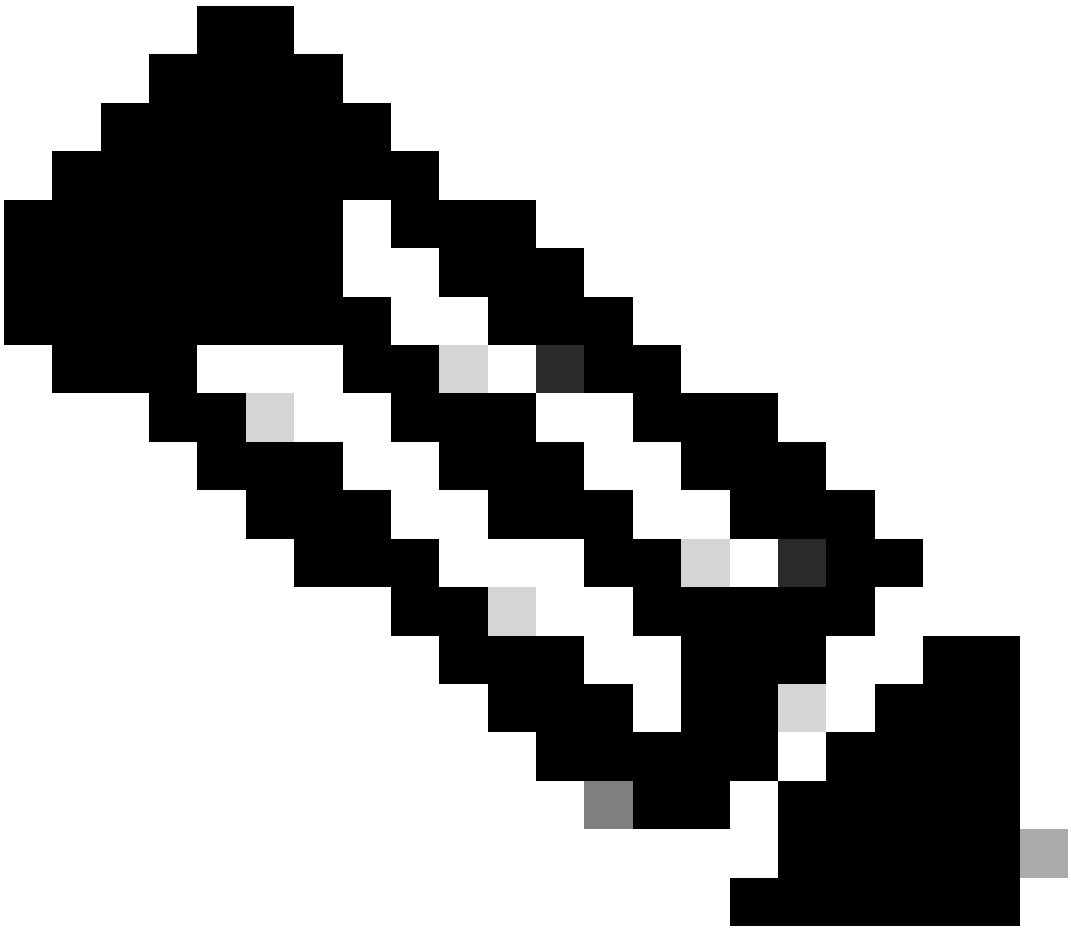
Étape 6.2. Bloquez le trafic DNS, le trafic vers l'adresse IP PSN ISE et les serveurs de conversion pour les exclure de la redirection. Autorisez le reste de la circulation. Cela déclenche la redirection. Cliquez sur Save.




*FMC_Add_Redirect_ACL_Part_2*



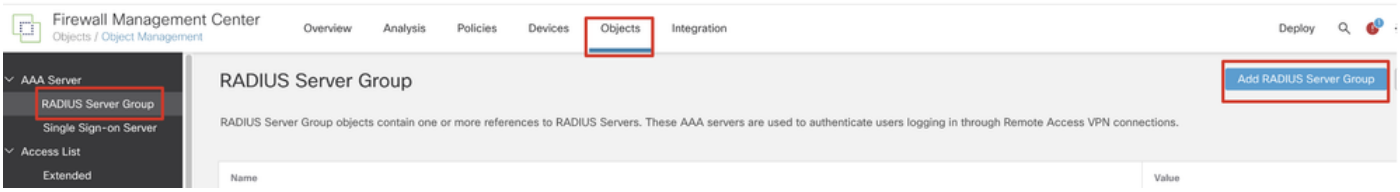

*FMC_Add_Redirect_ACL_Part_3*



**Remarque** : le FTP de destination dans cet exemple de liste de contrôle d'accès de redirection est utilisé comme exemple de serveur

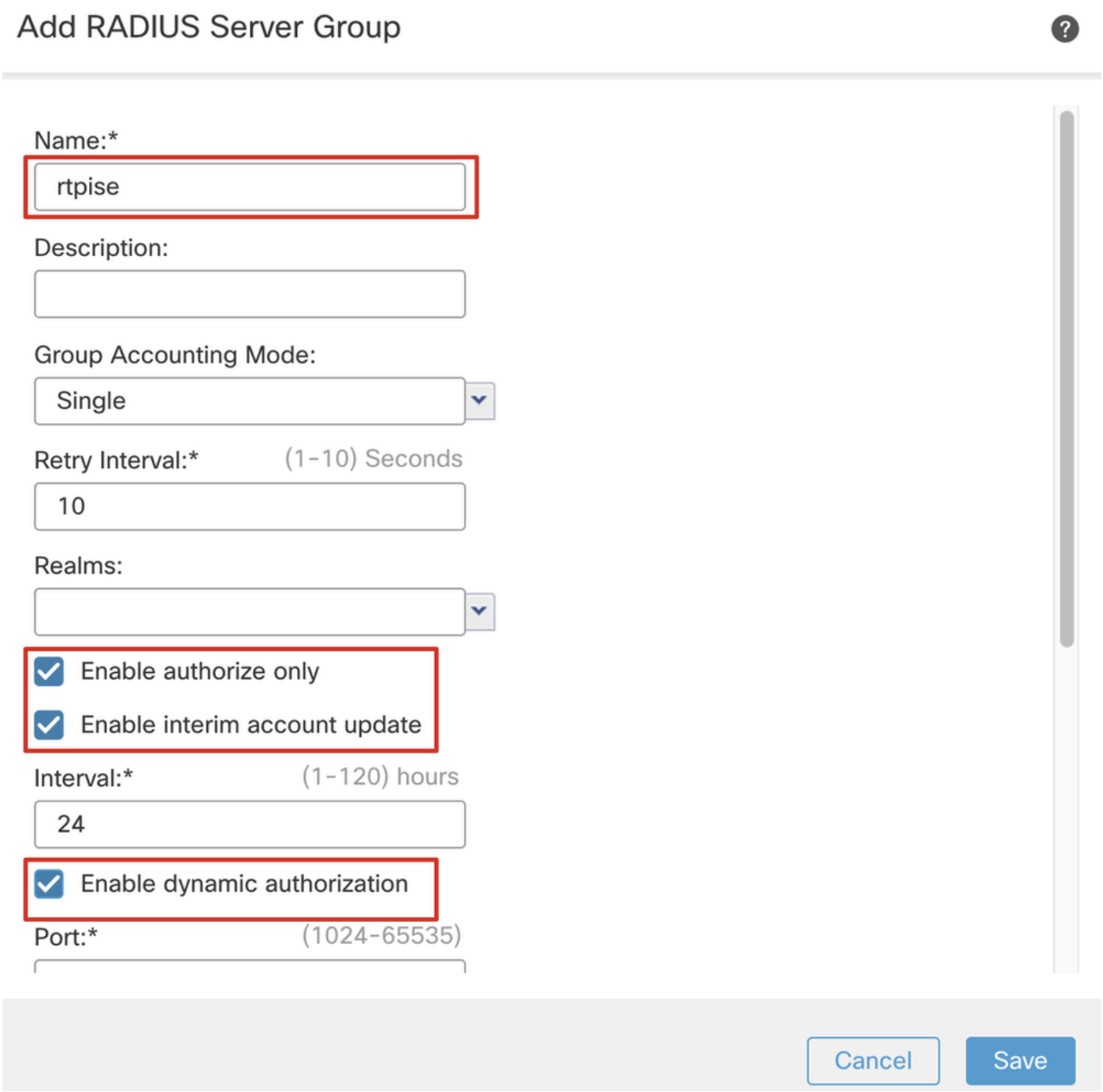
de conversion.

Étape 7. Accédez à Objects > Object Management > RADIUS Server Group. Cliquez sur Add RADIUS Server Group.



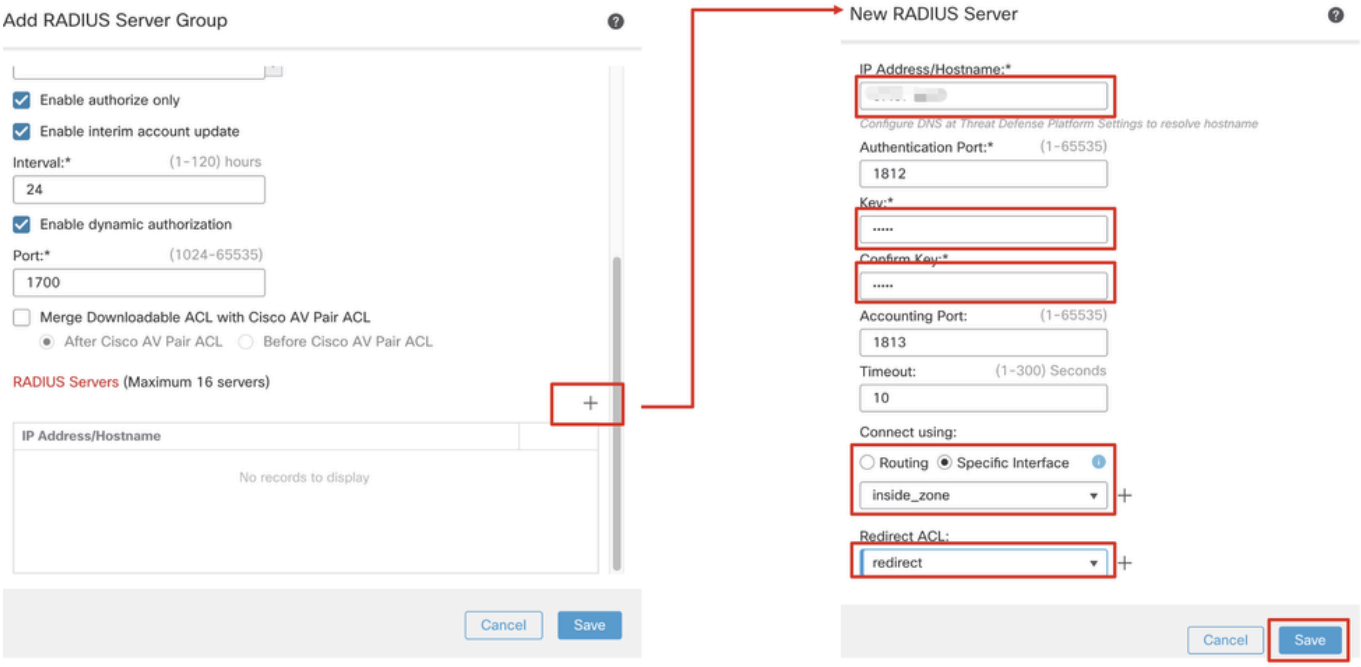

*FMC_Add_New_Radius_Server_Group*

Étape 7.1. Indiquez le nom, la vérification Enable authorize only, la vérification Enable interim account update, la vérification Enable dynamic authorization.



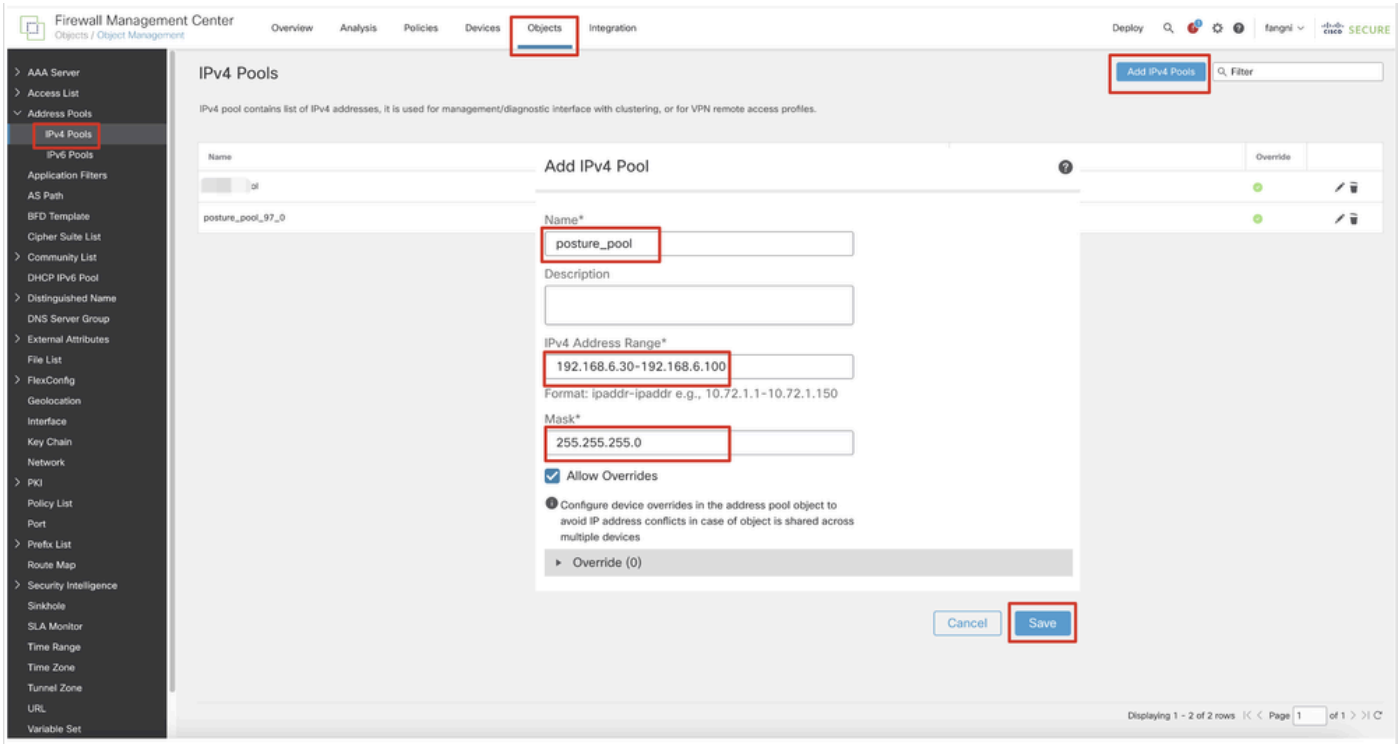

*FMC_Add_New_Radius_Server_Group_Part_1*

Étape 7.2. Cliquez sur l'Plus icône pour ajouter un nouveau serveur RADIUS. Fournissez le PSN ISE IP Address/Hostname, Key. Sélectionnez le specific interface pour la connexion. Sélectionnez la Redirect ACL. Cliquez ensuite sur Savepour enregistrer le nouveau serveur RADIUS. Cliquez ensuite Save à nouveau sur pour enregistrer le nouveau groupe de serveurs RADIUS.



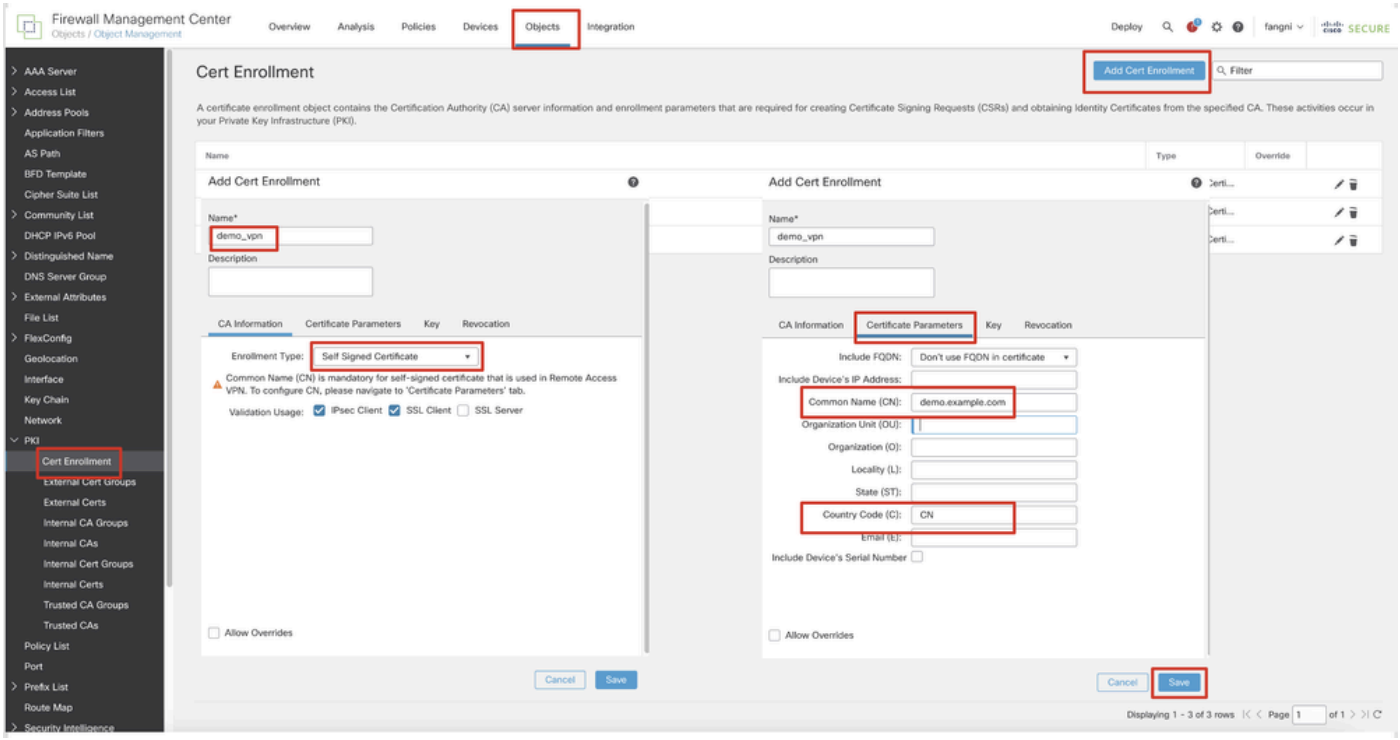

*FMC_Add_New_Radius_Server_Group_Part_2*

Étape 8. Accédez à Objects > Object Management > Address Pools > IPv4 Pools. Cliquez sur Add IPv4 Pools et indiquez les **Name, IPv4 Address Range**et Mask. Cliquez ensuite sur Save.



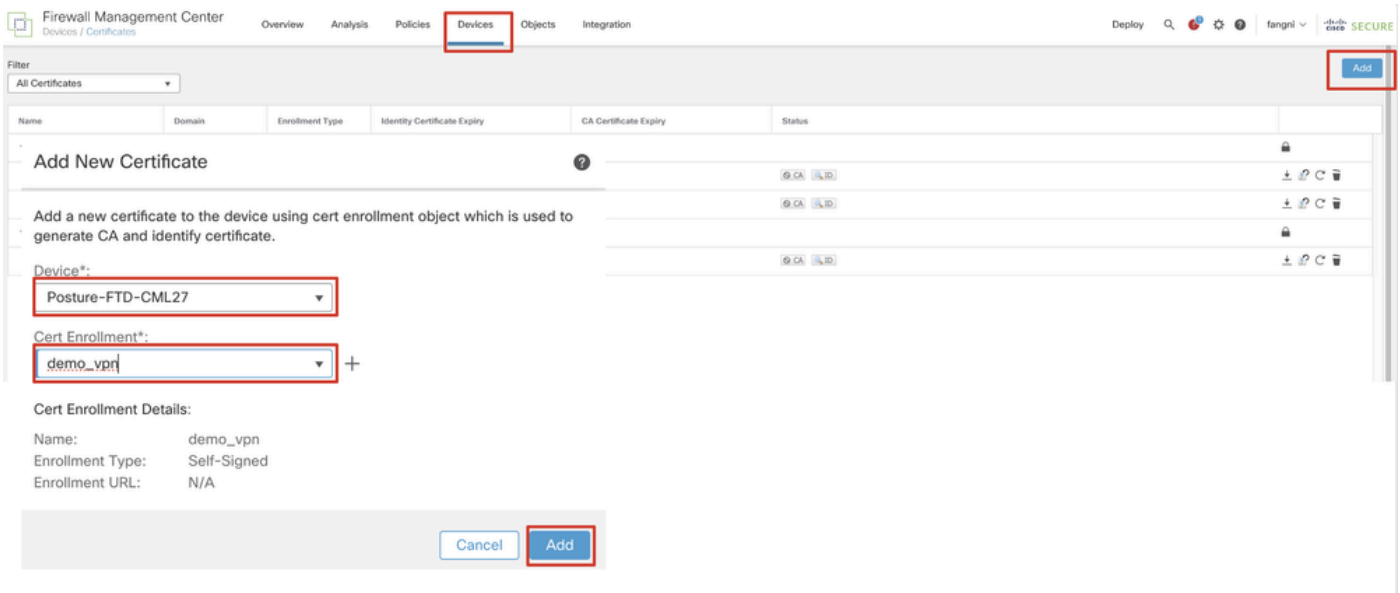

*FMC_Add_New_Pool*

Étape 9. Accédez à Certificate Objects > Object Management > PKI > Cert Enrollment. Cliquez sur Add Cert Enrollment, indiquez un nom, puis sélectionnez Self Signed Certificatedans Enrollment Type. Cliquez sur l'Certificate Parameters onglet et indiquez Common Name et Country Code. Cliquez ensuite sur Save.




*FMC_Add_New_Cert_Enroll*

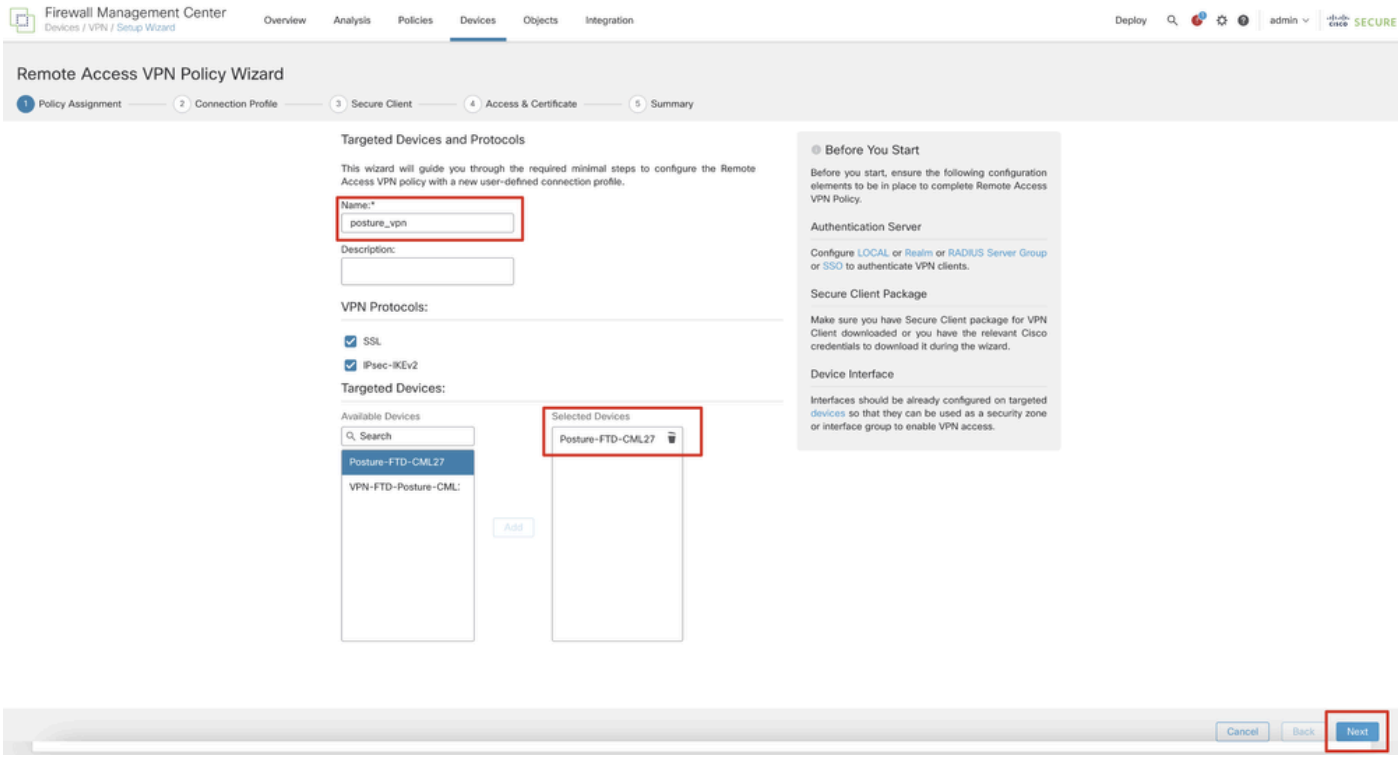
Étape 10. Accédez à Devices > Certificates. Cliquez sur Add, sélectionnez le nom FTD sous Device, sélectionnez l'inscription configurée précédente sous Cert Enrollment. Cliquez sur Add.




*FMC_Add_New_Cert_To_FTD*

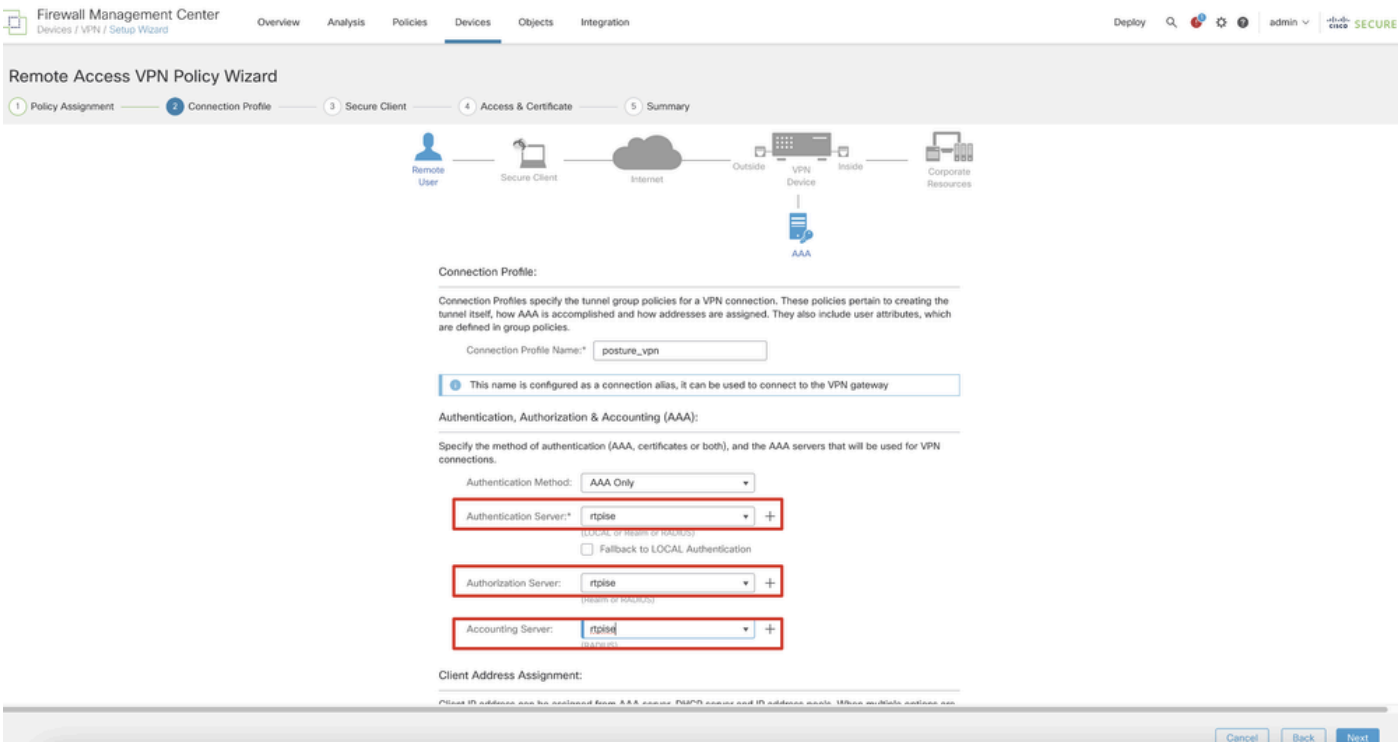
Étape 11. Accédez à Devices > VPN > Remote Access. Cliquez sur Add.

Étape 11.1. Saisissez le nom et ajoutez le FTD à Selected Devices. Cliquez sur Next.



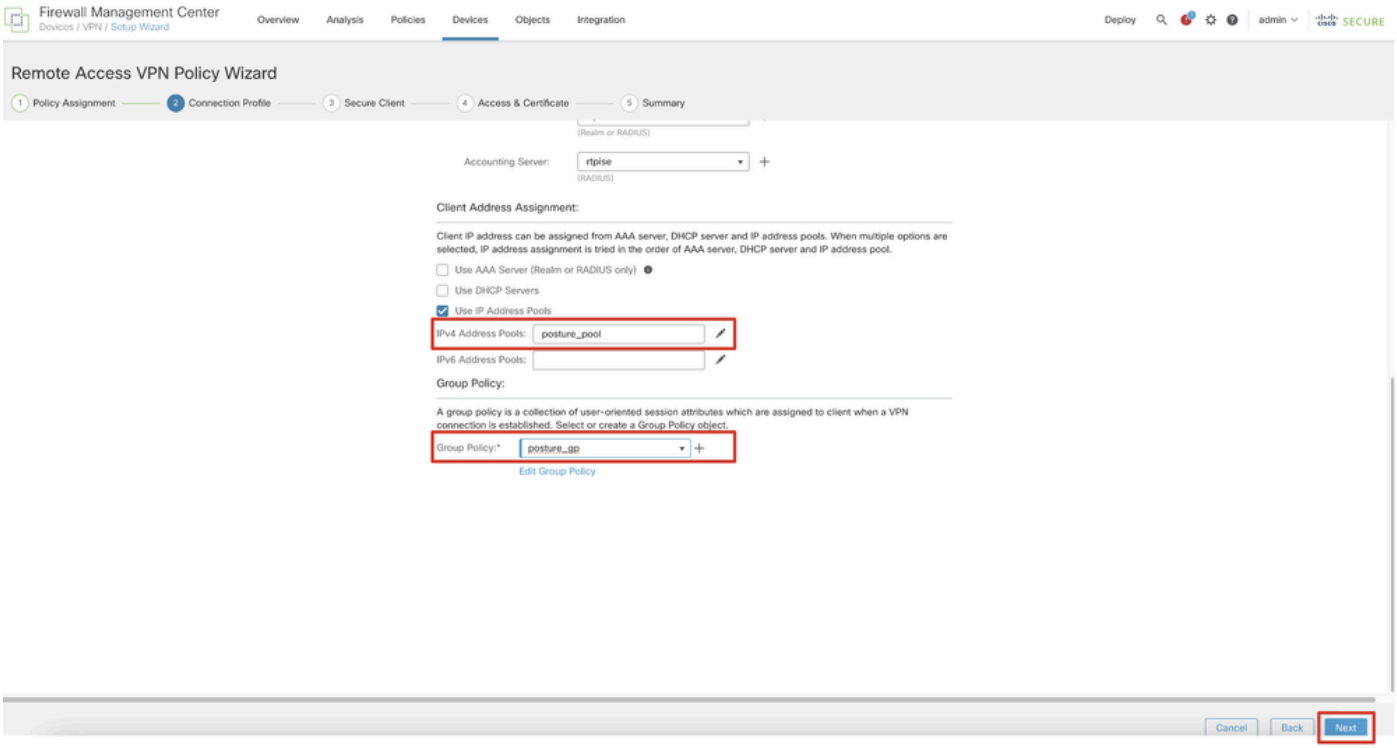

*FMC_New_RAVPN_Wizard_1*

Étape 11.2. Sélectionnez le groupe de serveurs RADIUS précédemment configuré dans la Authentication Server, Authorization Server, Accounting Server. Faites défiler la page.



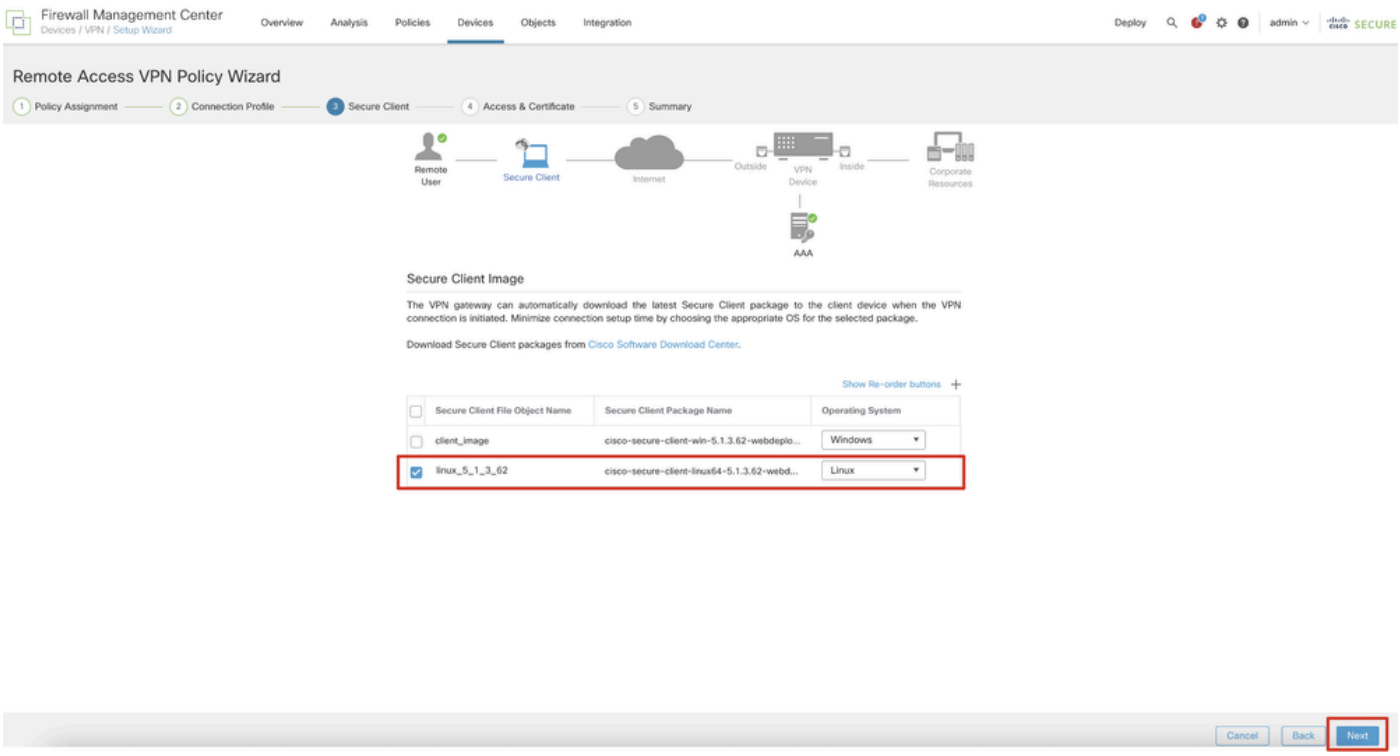

*FMC_New_RAVPN_Wizard_2*

Étape 11.3. Sélectionnez le nom du pool précédemment configuré dans IPv4 Address Pools. Sélectionnez la stratégie de groupe précédemment configurée dans Group Policy. Cliquez sur Next.



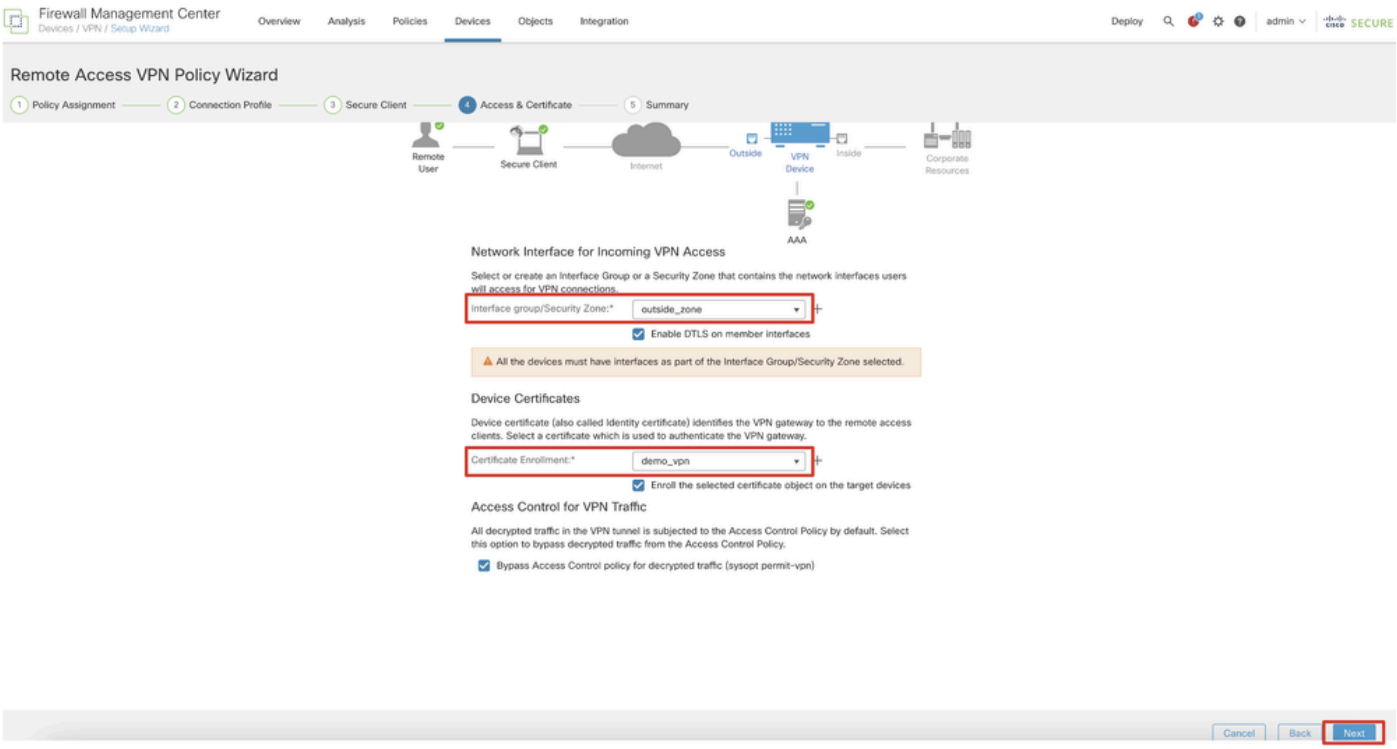

*FMC_New_RAVPN_Wizard_3*

Étape 11.4. Cochez la case de l'image Linux. Cliquez sur Next.



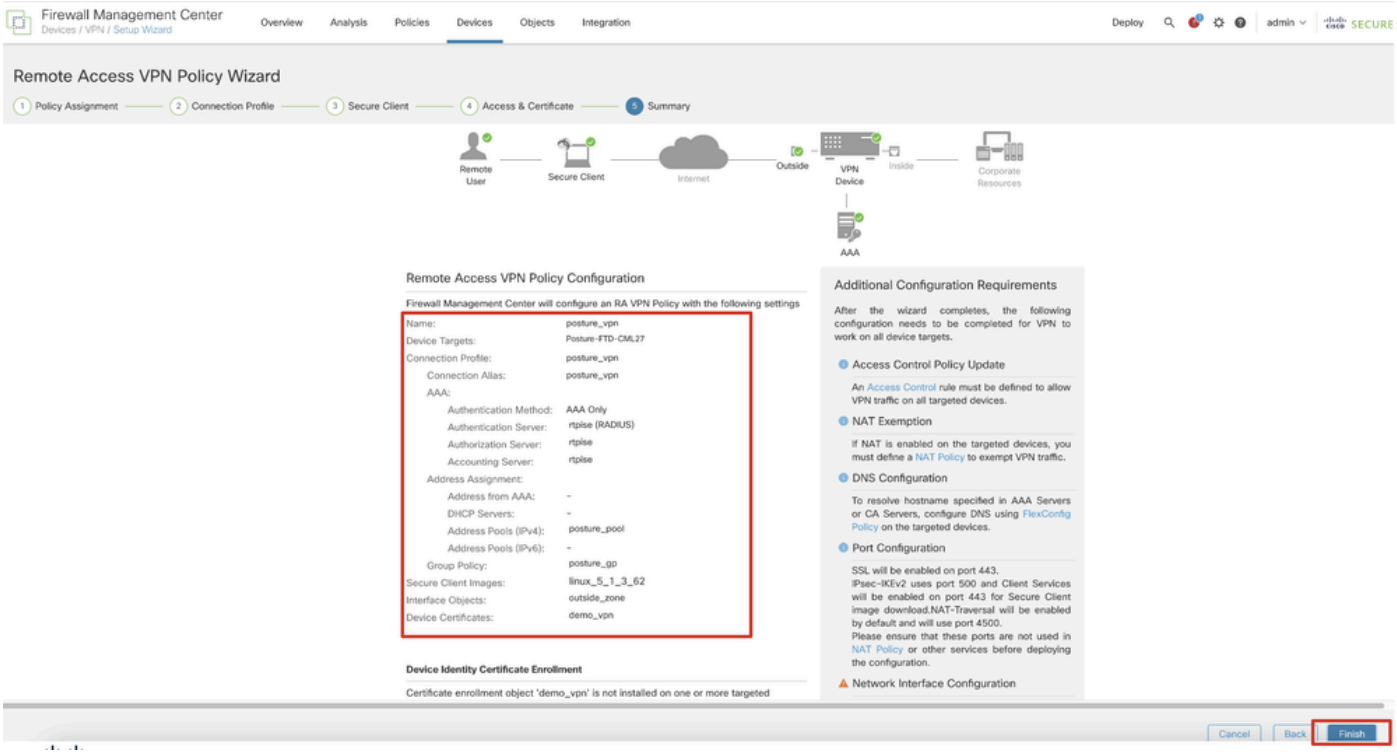

*FMC_New_RAVPN_Wizard_4*

Étape 11.5. Sélectionnez l'interface de l'interface VPN. Sélectionnez l'inscription de certificat qui s'est inscrite sur FTD à l'étape 9. Cliquez sur Next.



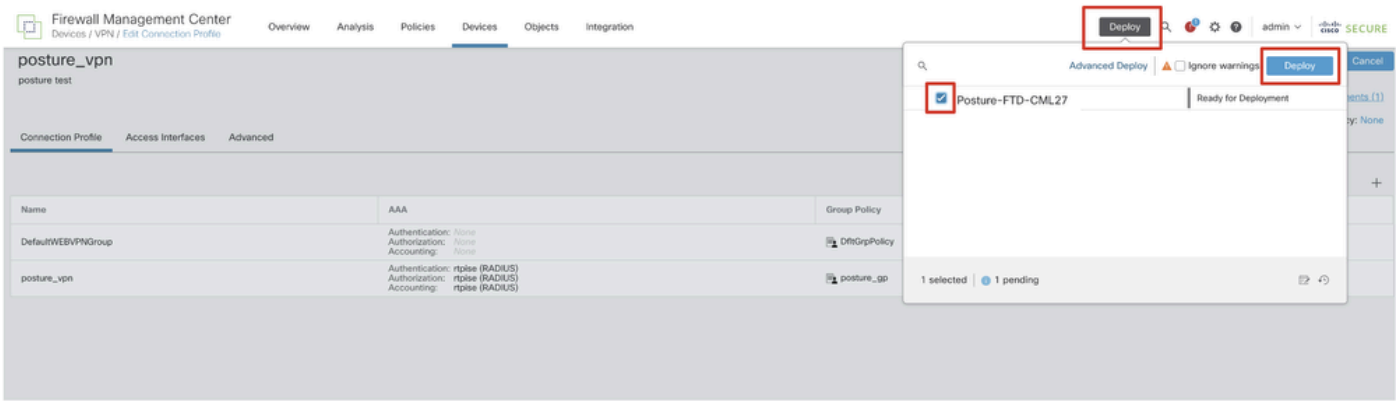

*FMC_New_RAVPN_Wizard_5*

Étape 11.6. Double-confirmez les informations associées sur la page de résumé. Si tout va bien, cliquez sur Finish. Si vous devez modifier quelque chose, cliquez sur Back.




*FMC_New_RAVPN_Wizard_6*

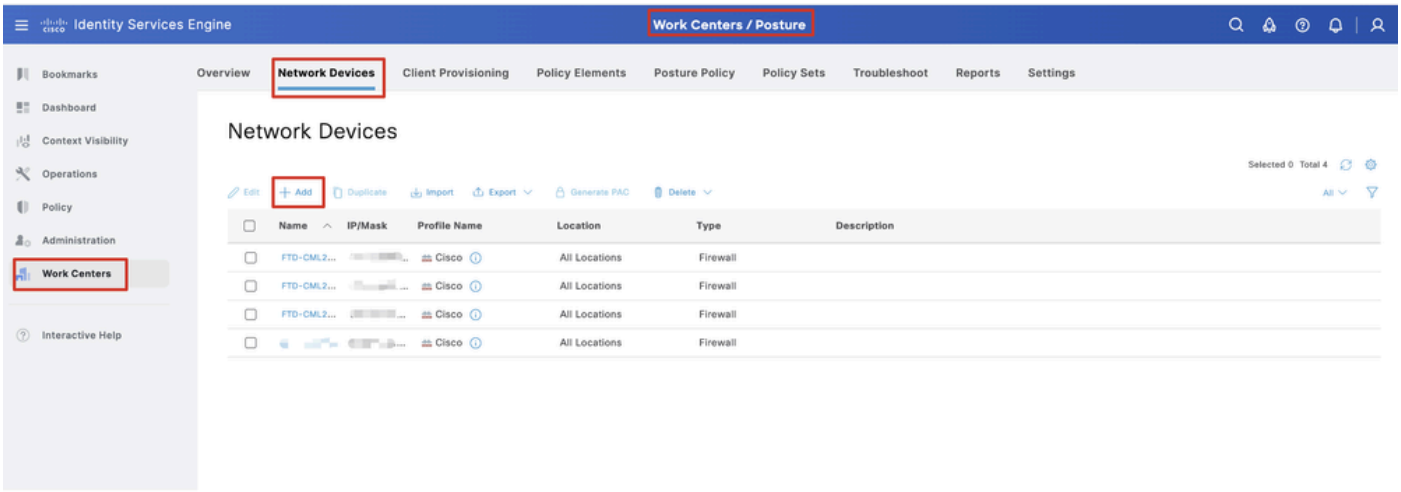
Étape 12. Déployez la nouvelle configuration sur FTD pour terminer la configuration VPN d'accès à distance.




*FMC_Deploy_FTD*

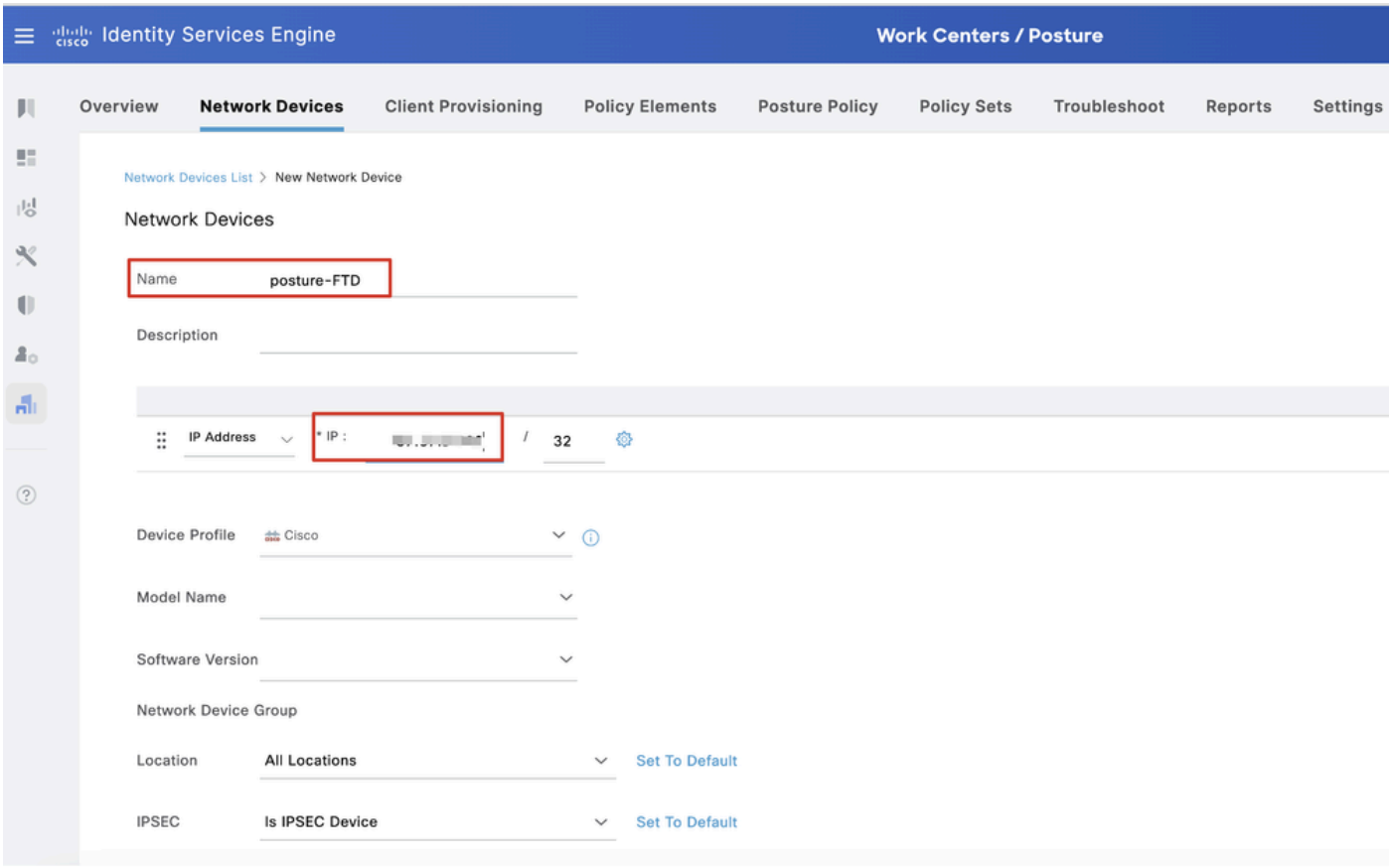
Configurations sur ISE

Étape 13. Accédez à Work Centers > Posture > Network Devices. Cliquez sur Add.



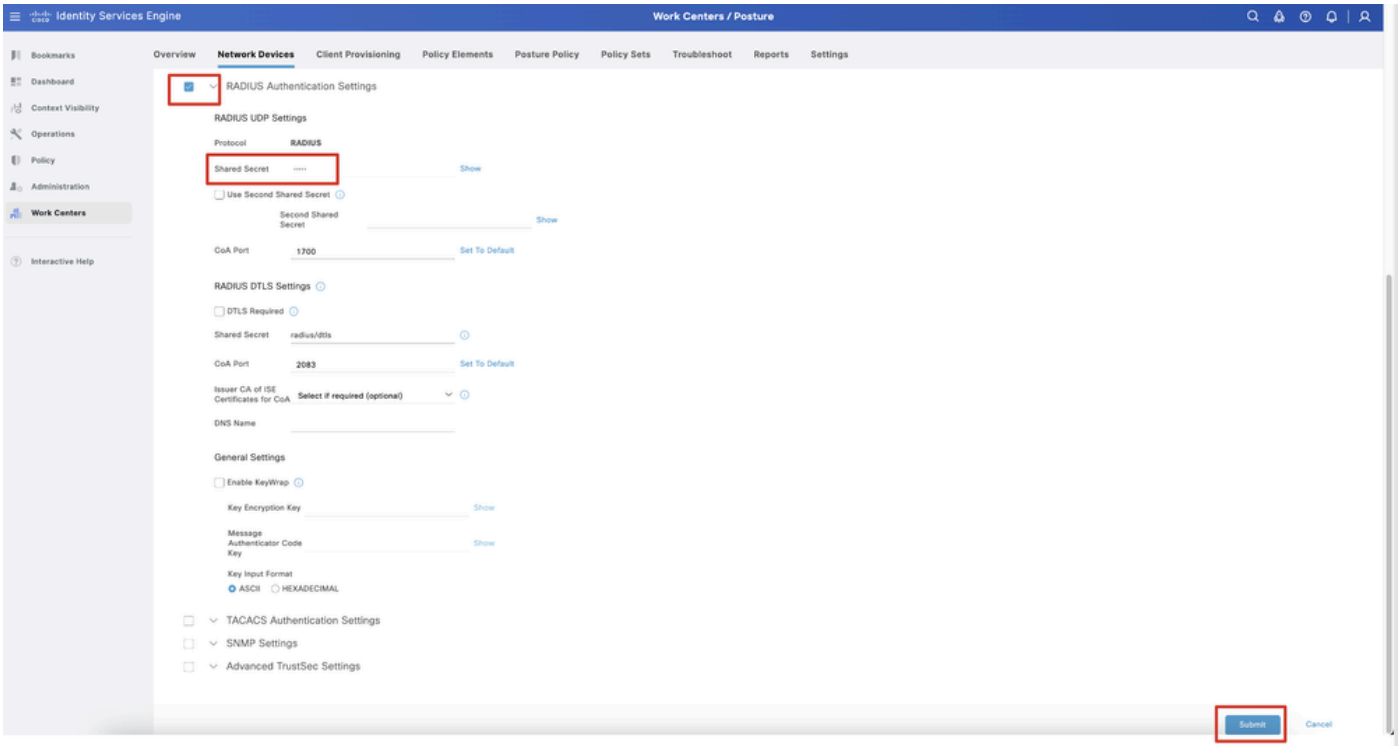

*ISE_Add_New_Devices*

Étape 13.1. Fournissez le Name, IP Addresset faites défiler la page vers le bas.




*ISE_Add_New_Devices_1*

Étape 13.2. Cochez la case de RADIUS Authentication Settings. Fournissez le Shared Secret. Cliquez sur Submit.

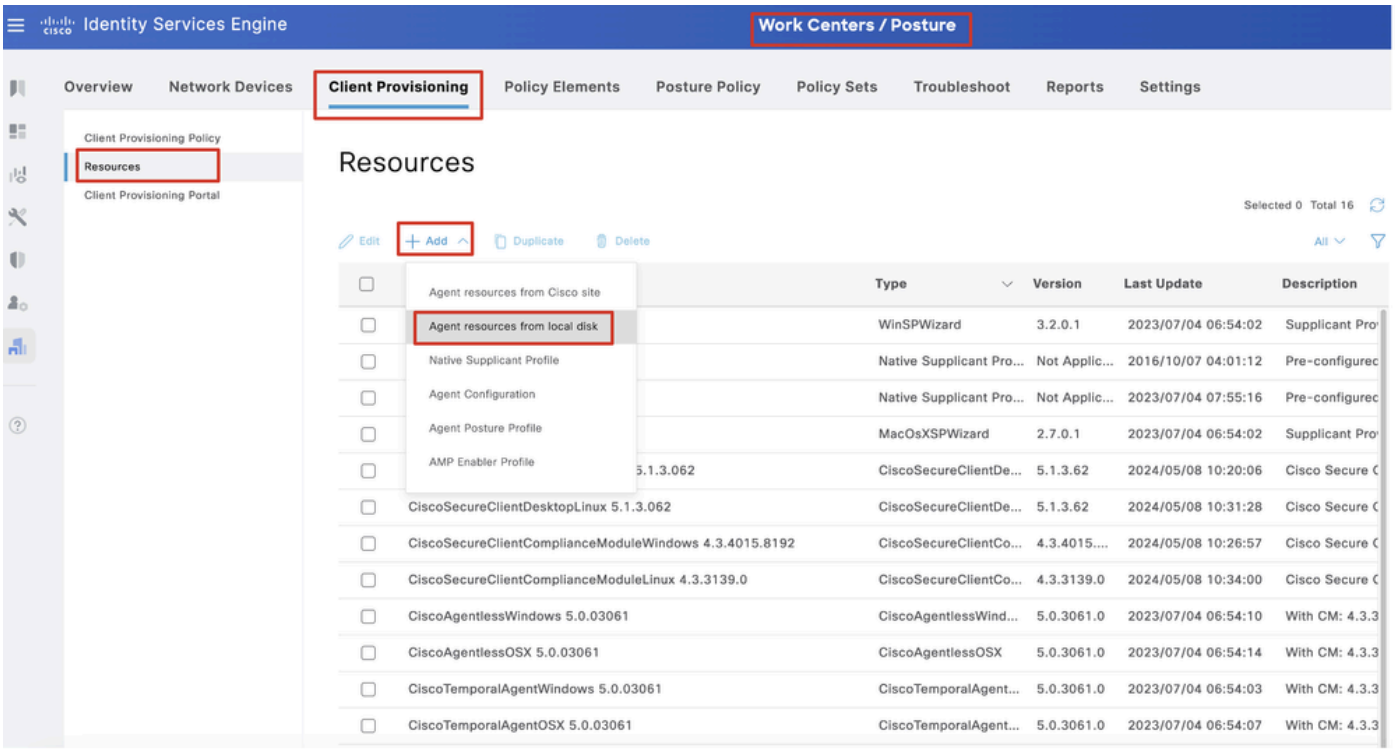



*ISE_Add_New_Devices_2*

Étape 14. Téléchargez le nom cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg du package à partir de Téléchargement de logiciel Cisco et assurez-vous que le fichier est correct en confirmant que la somme de contrôle md5 du fichier téléchargé est identique à la

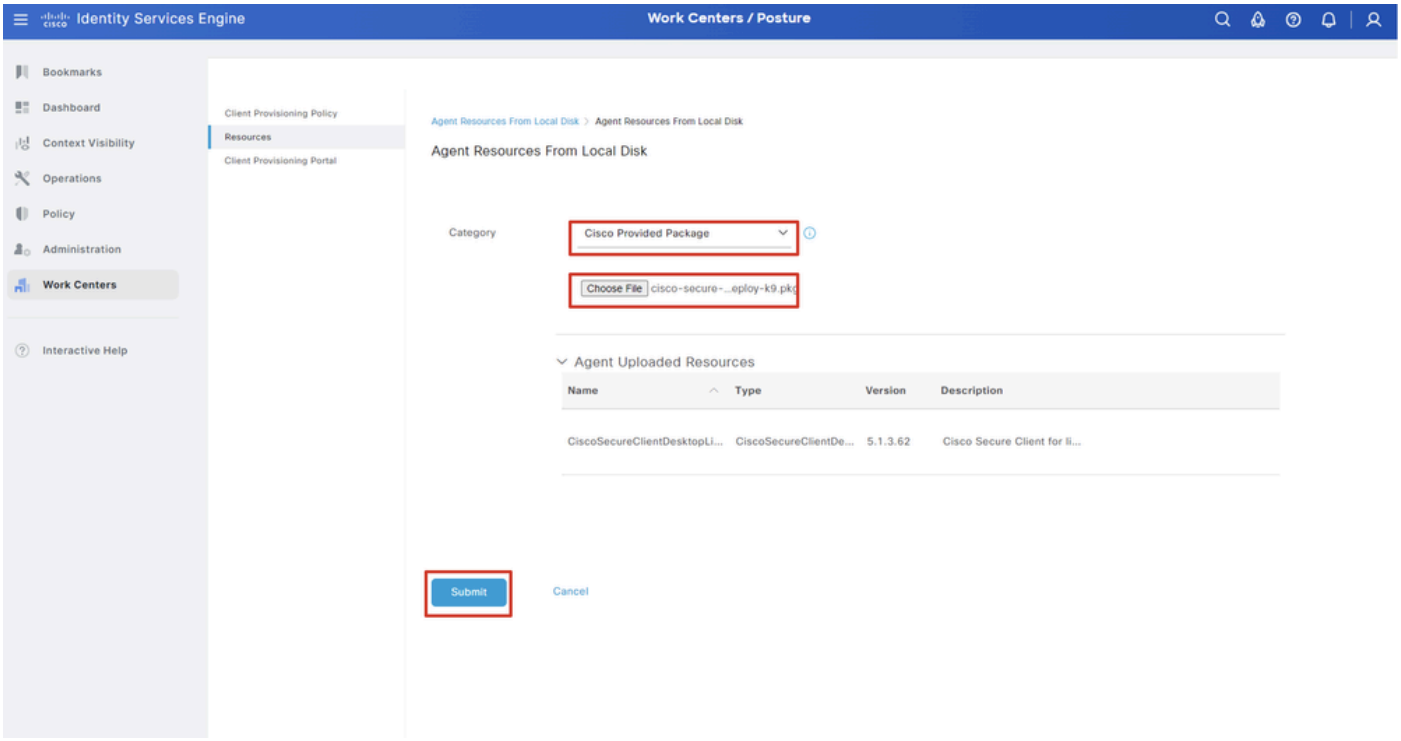
page Téléchargement de logiciel Cisco. Le nom du package cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg a été téléchargé à l'étape 1.

Étape 15. Accédez à Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add. Sélectionnez Agent resources from local disk.

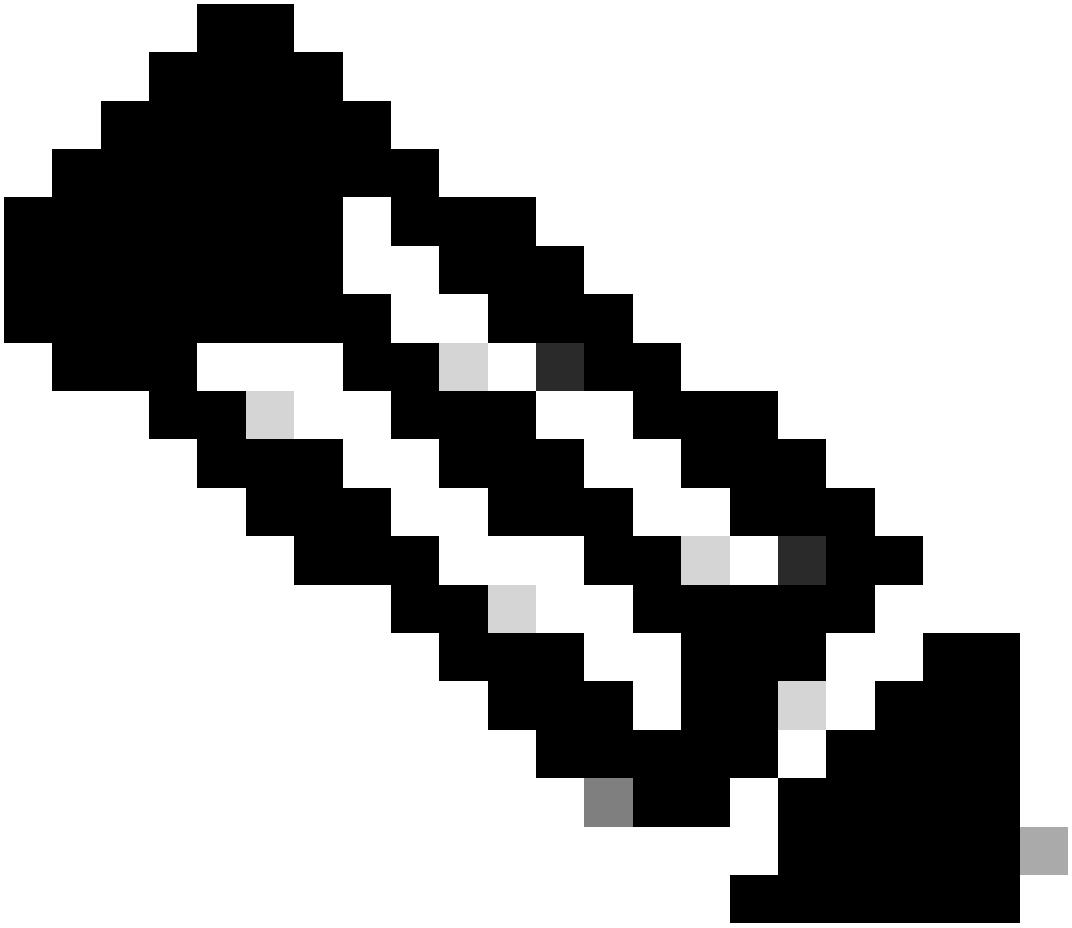



*Ressource_Téléchargement_ISE*

Étape 15.1. Sélectionnez Cisco Provided Package. Cliquez sur Choose File cette option pour télécharger cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Cliquez sur Submit.

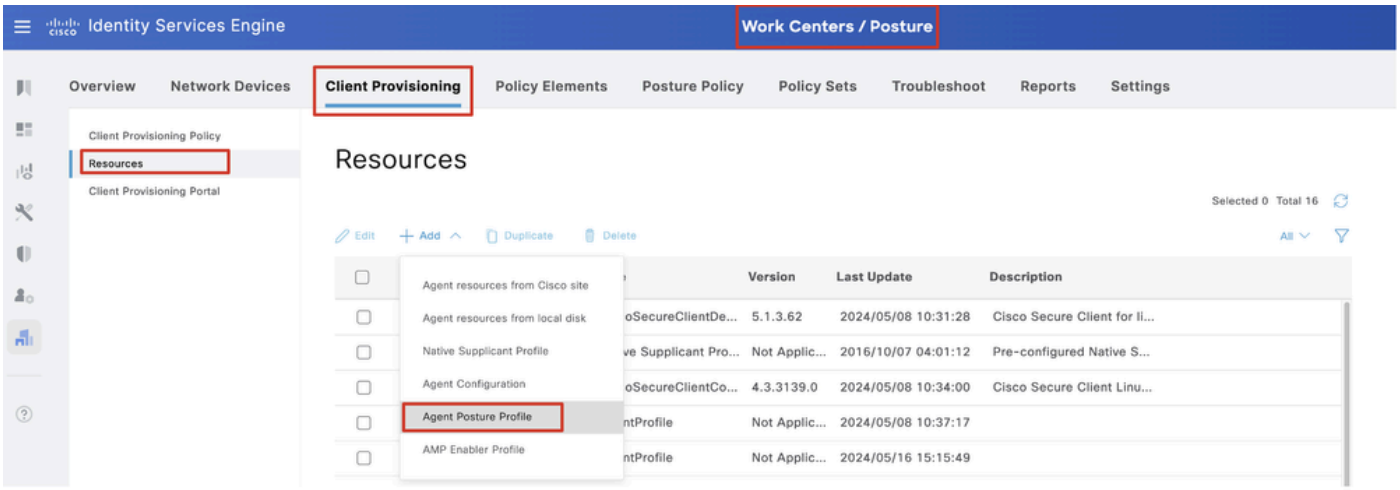



*ISE_Upload_Resources_1*



**Remarque** : répétez l'étape 14. pour télécharger cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg .

Étape 16. Accédez à Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add. Sélectionnez Agent Posture Profile.

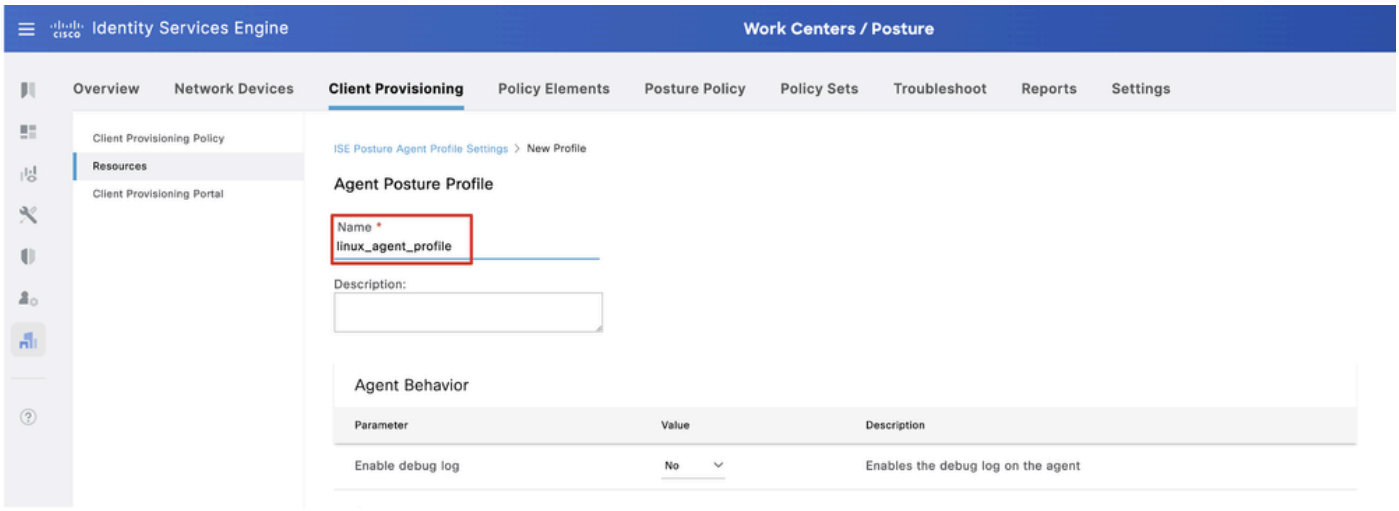



*Profil_Posture_Agent_Ajout_ISE*

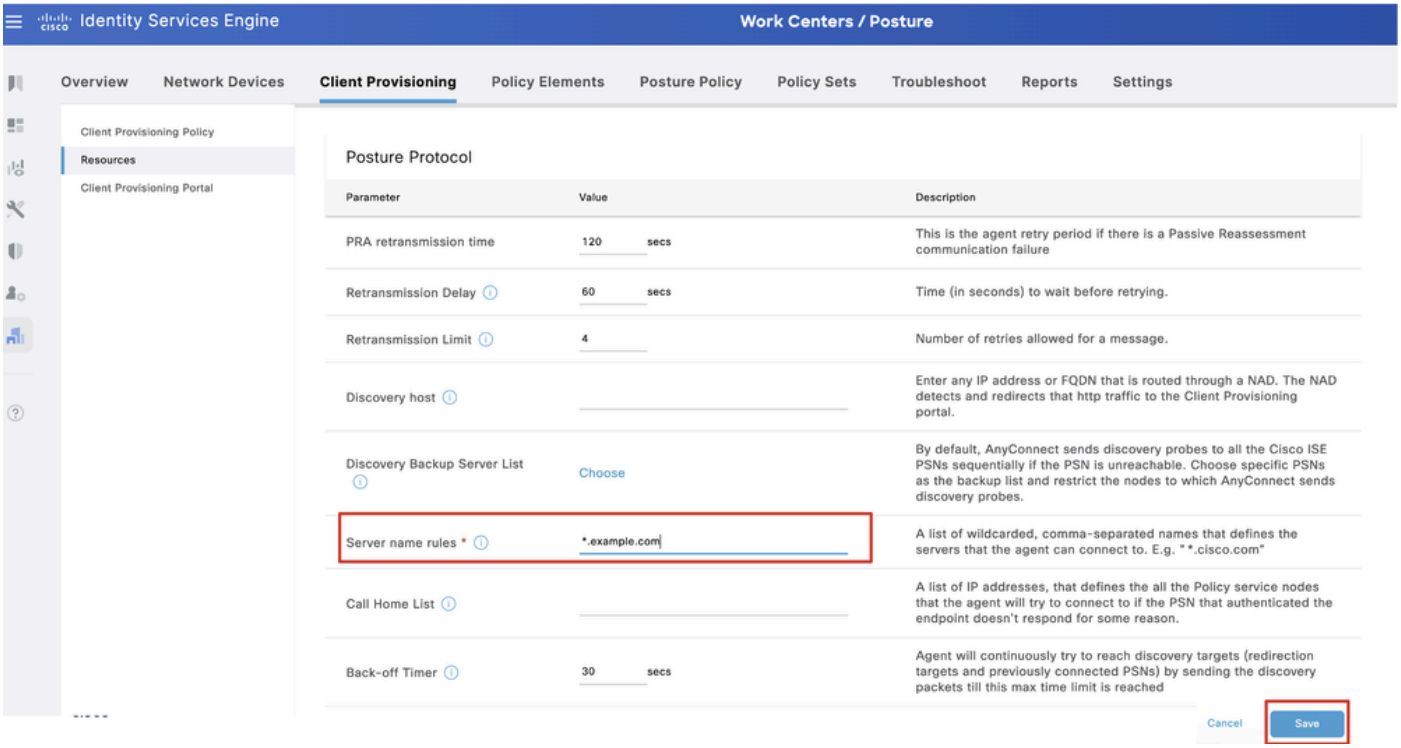
Étape 16.1. Fournissez le Name, Server name rules et conservez le reste par défaut. Cliquez sur Save.

Nom : linux_agent_profile

Règles de nom de serveur : *.example.com

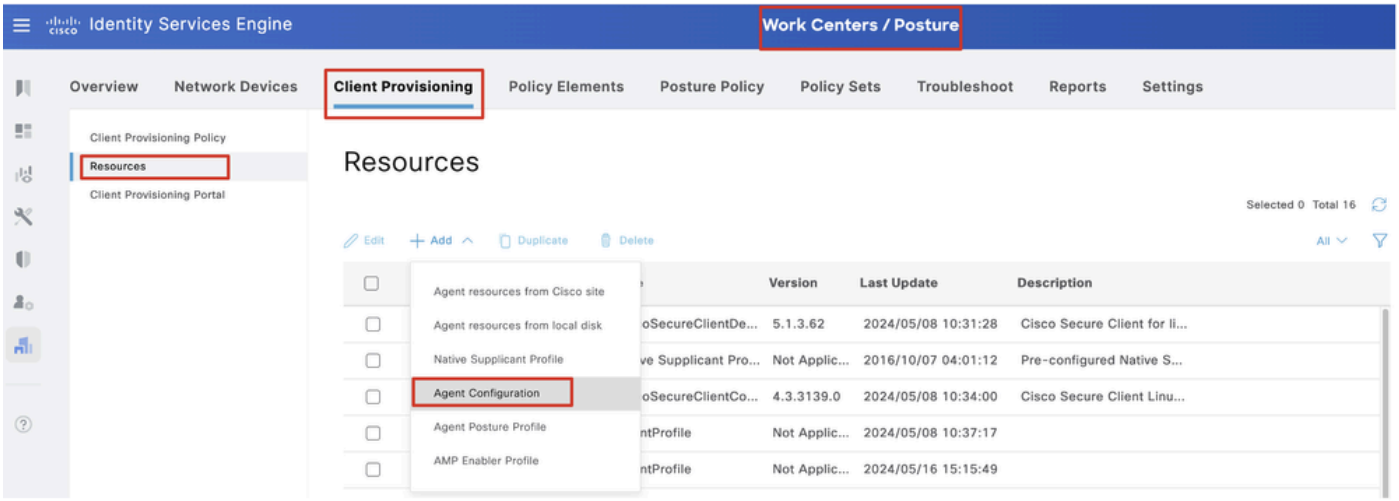



*ISE_Add_Agent_Posture_Profile_1*




*ISE_Add_Agent_Posture_Profile_2*

Étape 17. Accédez à Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add. Sélectionnez Agent Configuration.




*ISE_Add_Agent_Configuration*

Étape 17.2. Configurez les détails :

Package Select Agent : CiscoSecureClientDesktopLinux 5.1.3.062

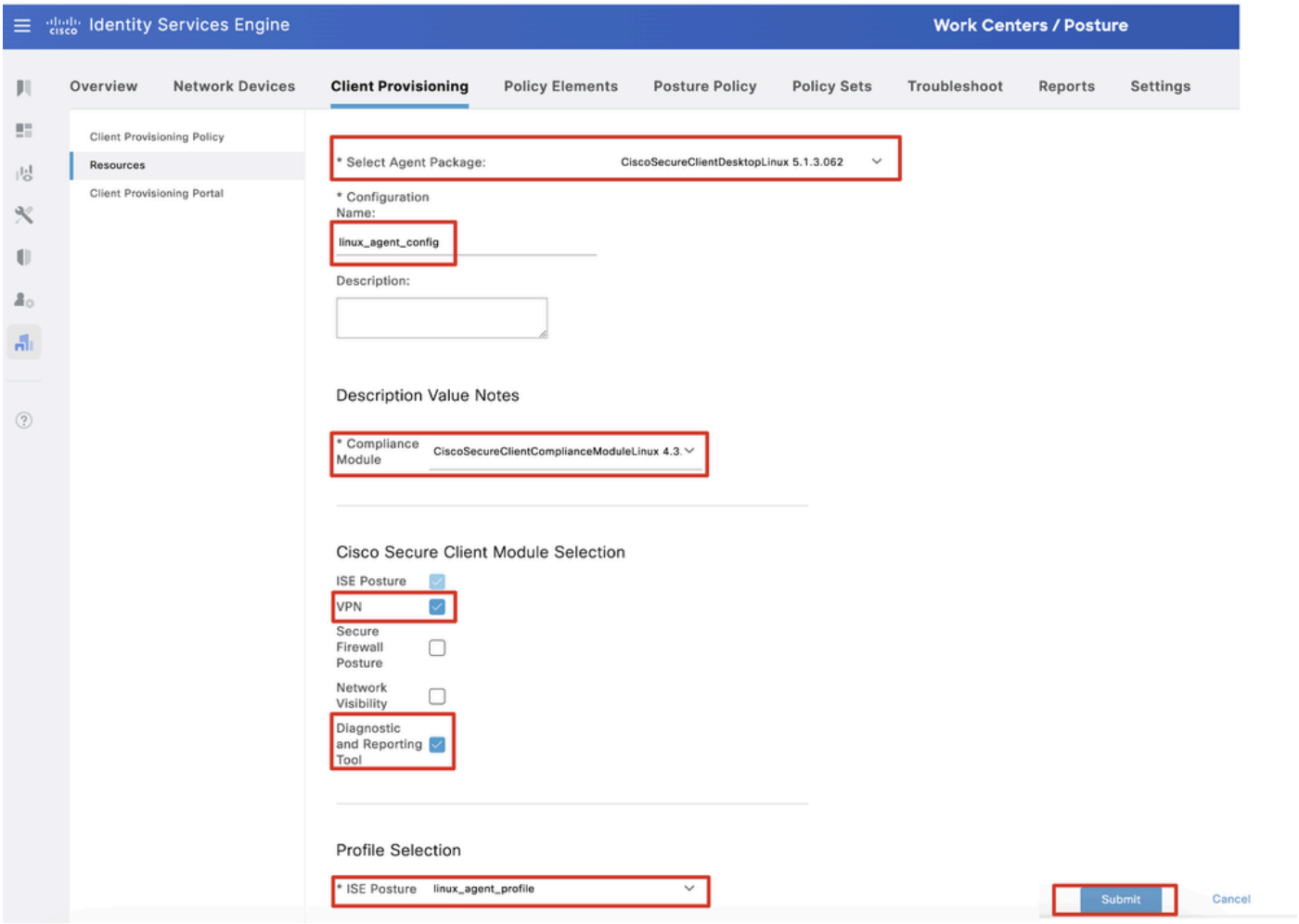
Nom : linux_agent_config

Module de conformité : CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Cochez la case de VPN, Diagnostic and Reporting Tool

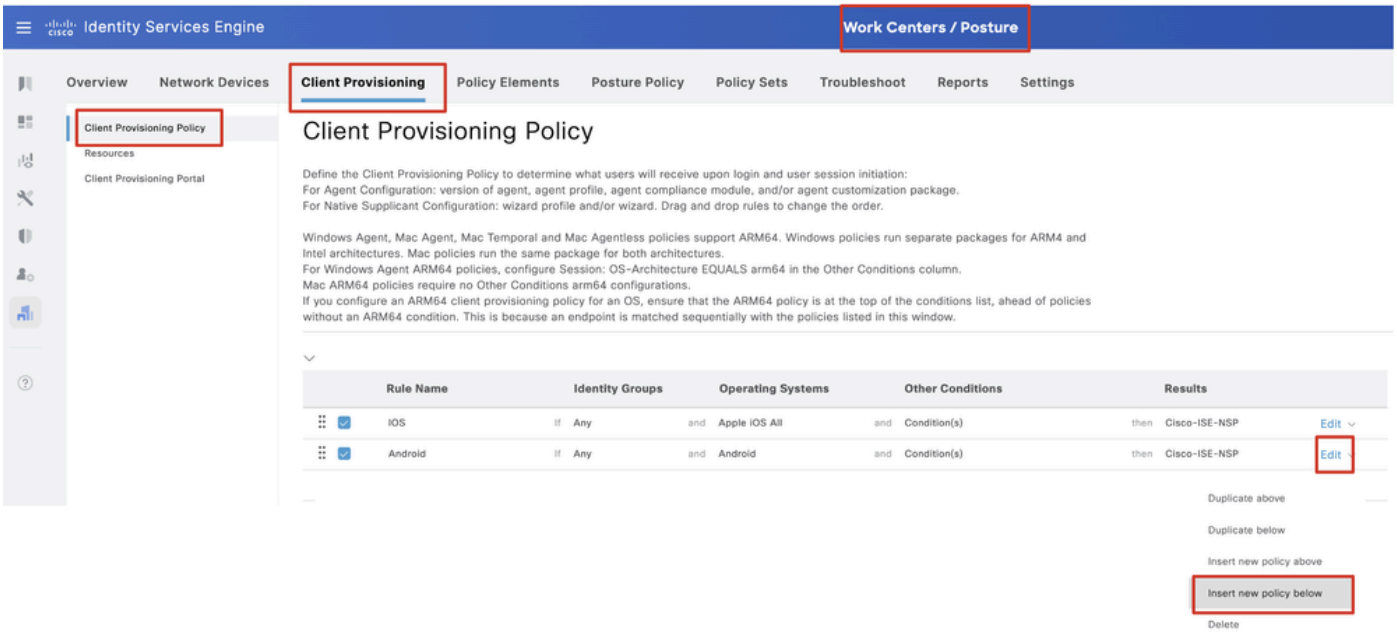
Position ISE de sélection de profil : linux_agent_profile

Cliquez sur Submit.




*ISE_Add_Agent_Configuration_1*

Étape 18. Accédez à Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Cliquez Edit à la fin du nom d'une règle. Sélectionnez Insert new policy below.




*ISE_Add_New_Provisioning_Policy*

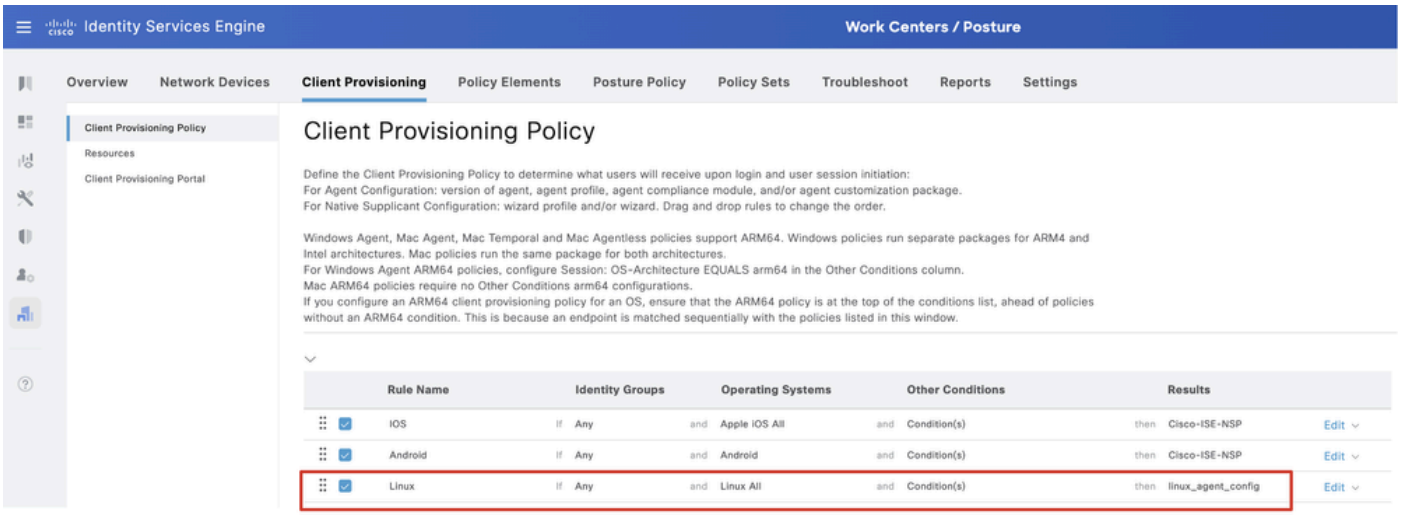
Étape 18.1. Configurez les détails :

Nom de la règle : Linux

Systèmes d'exploitation : Linux All

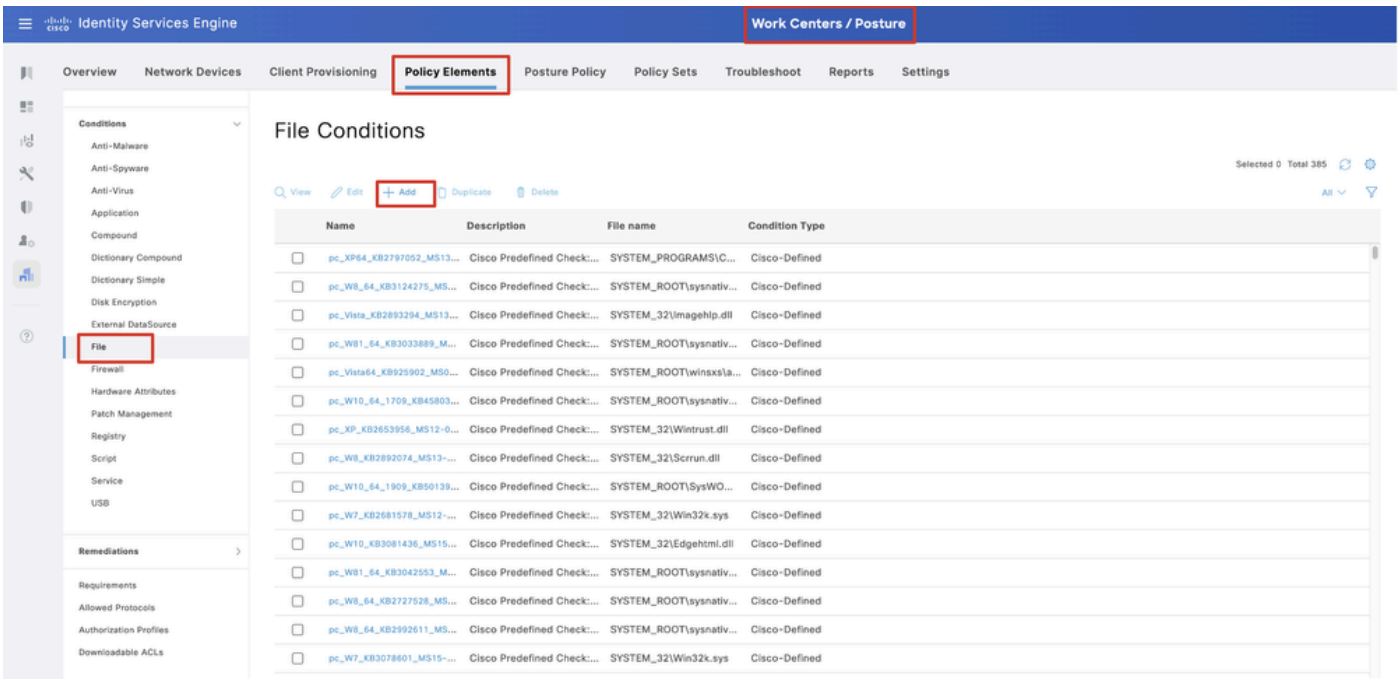
Résultats : linux_agent_config

Cliquez sur Done et Save.




*ISE_Add_New_Provisioning_Policy_1*

Étape 19. Accédez à Work Centers > Posture > Policy Elements > Conditions > File. Cliquez sur Add.




*ISE_Add_New_File_Condition*

Étape 19.1. Configurez les détails :

Nom : linux_demo_file_existing

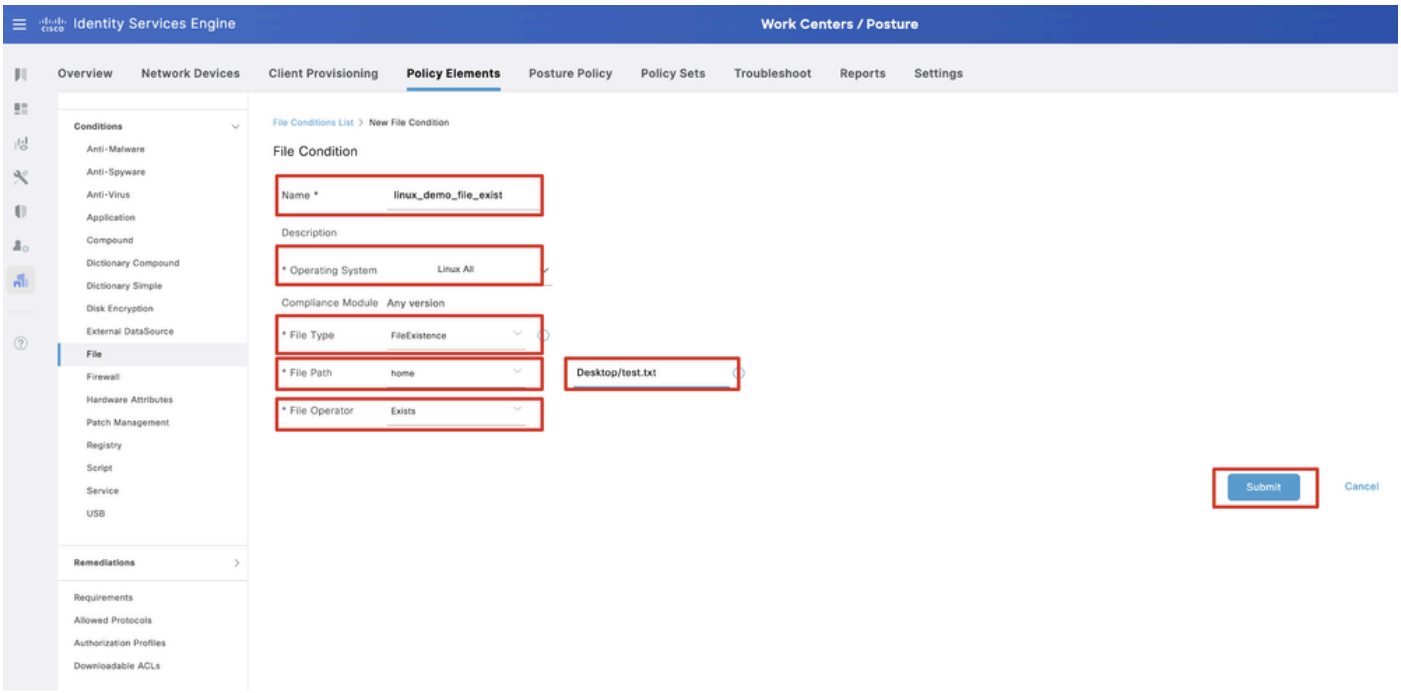
Systèmes d'exploitation : Linux All

Type de fichier : FileExistence

Chemin d'accès au fichier : home, Desktop/test.txt

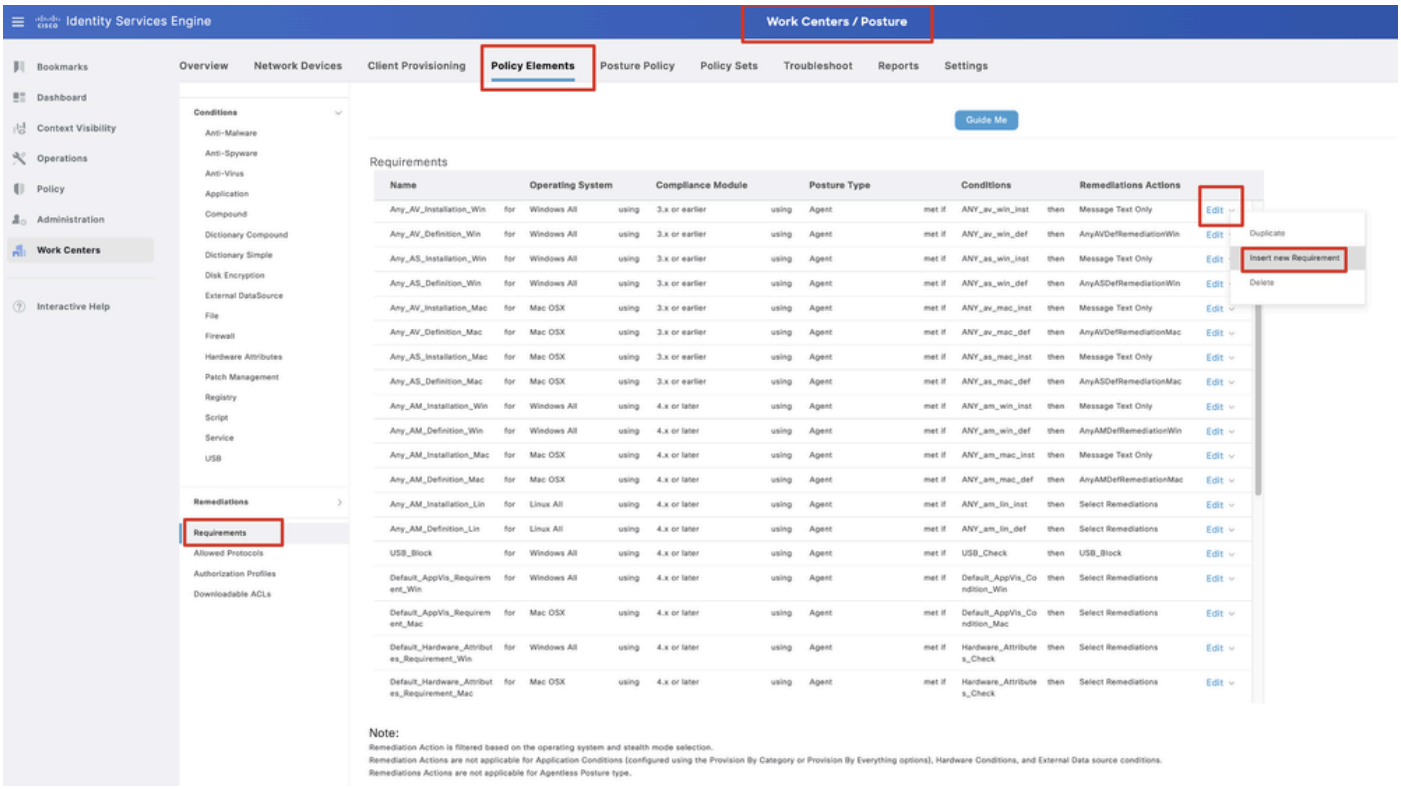
Opérateur de fichier : existe

Cliquez sur Submit.




*ISE_Add_New_File_Condition_1*

Étape 20. Accédez à Work Centers > Posture > Policy Elements > Requirements. Cliquez Edit à la fin du nom d'une règle. Sélectionnez Insert new Requirement.




*ISE_Add_New_Posture_Requirement*

Étape 20.1. Configurez les détails :

Nom : Test_existing_linux

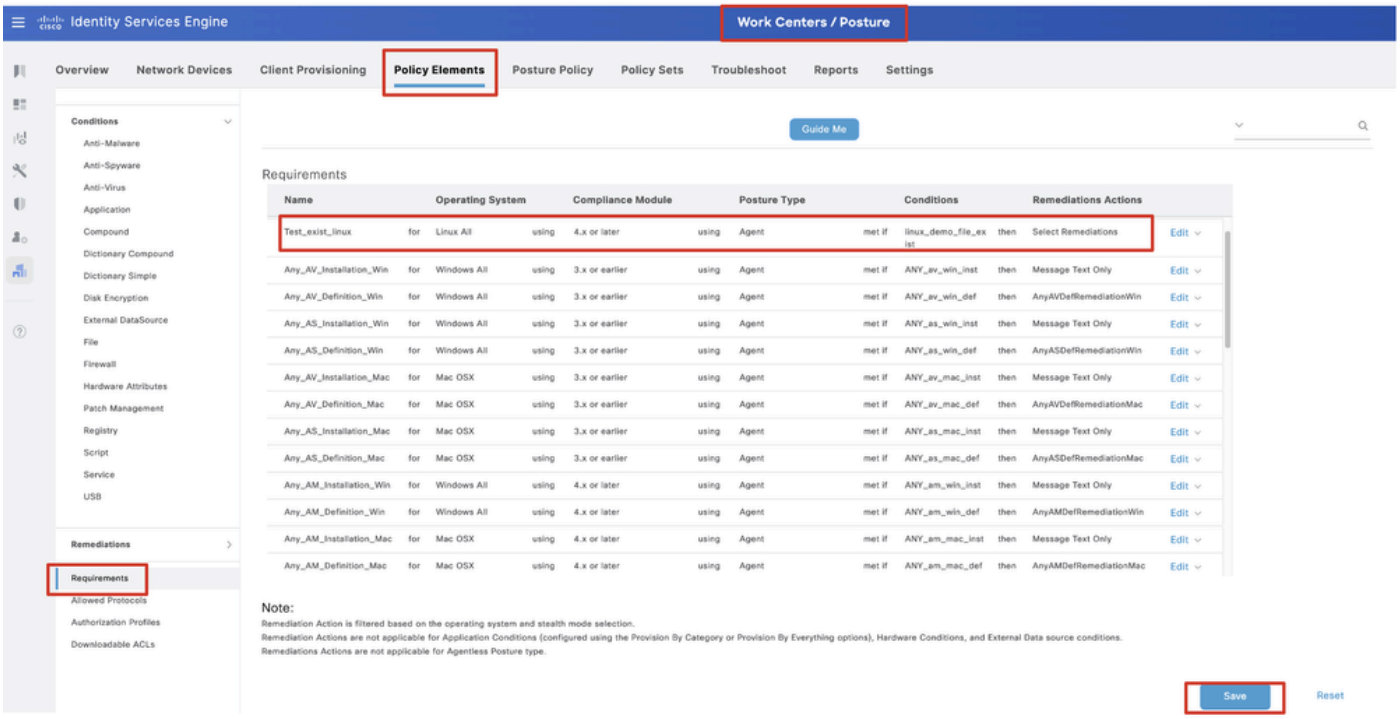
Systèmes d'exploitation : Linux All

Module de conformité : version 4.x ou ultérieure

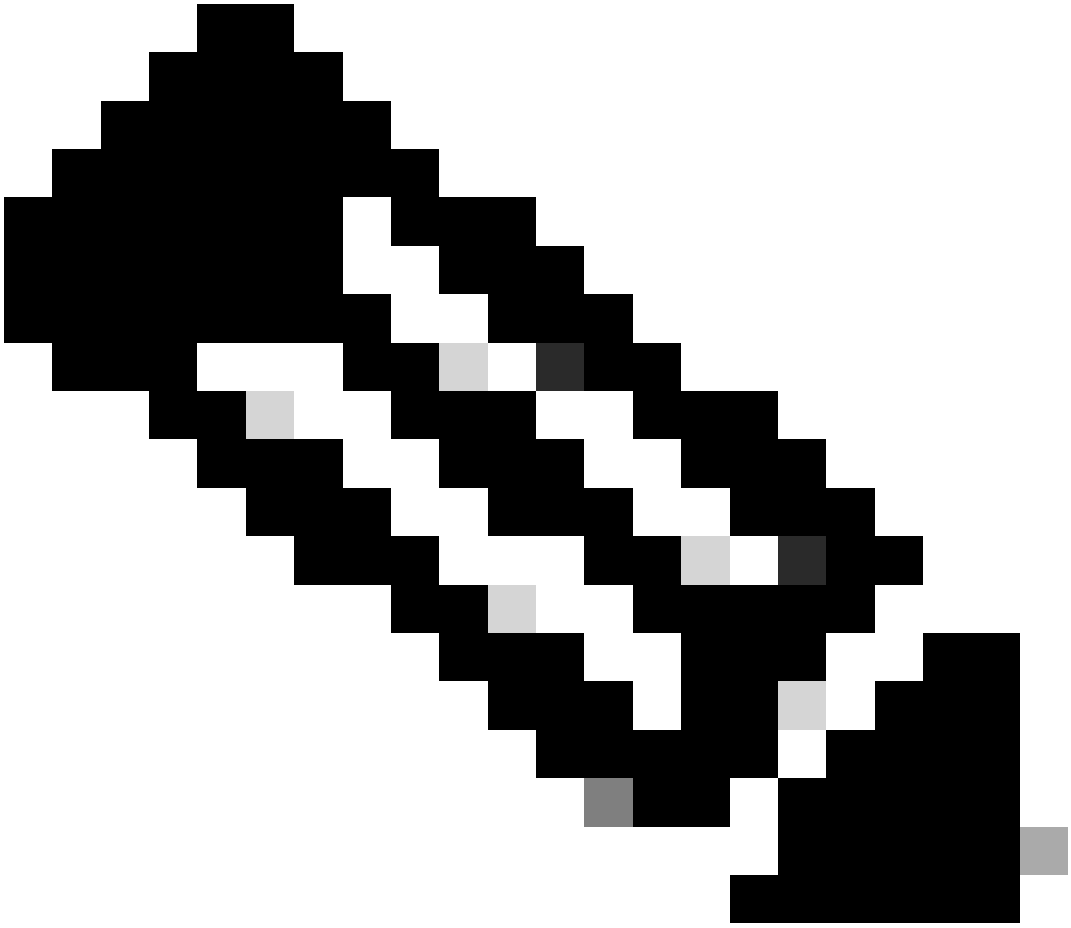
Type de posture : Agent

Conditions : linux_demo_file_existing

Cliquez sur Done et Save.




*ISE_Add_New_Posture_Requirement_1*



**Remarque** : actuellement, seuls les scripts shell sont pris en charge pour les agents Linux en tant que correction.

---

Étape 21. Accédez à Work Centers > Posture > Policy Elements > Authorization Profiles. Cliquez sur Add.

Étape 21.1. Configurez les détails :

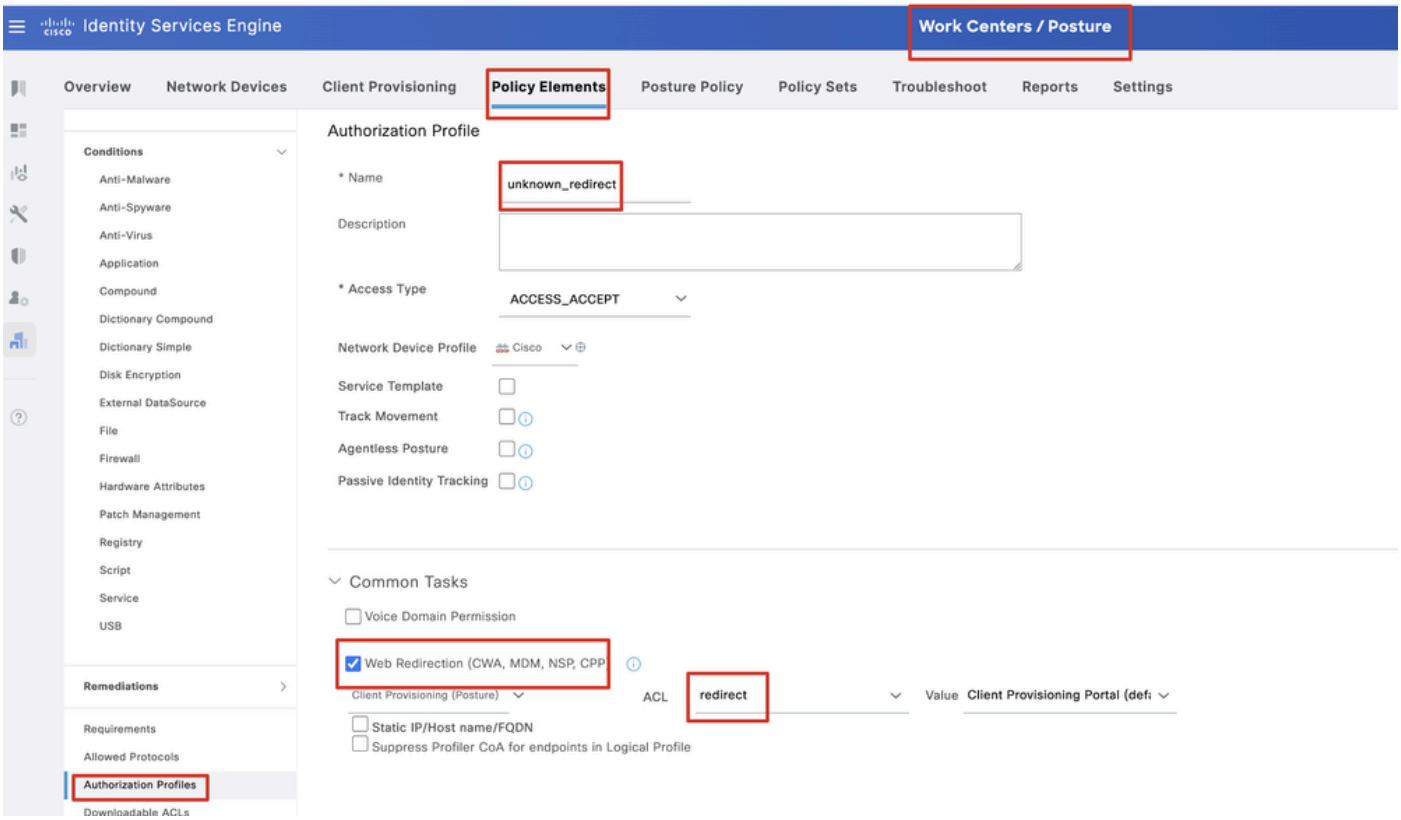
Nom : unknown_redirect

Cochez la case de Web Redirection(CWA,MDM,NSP,CPP)

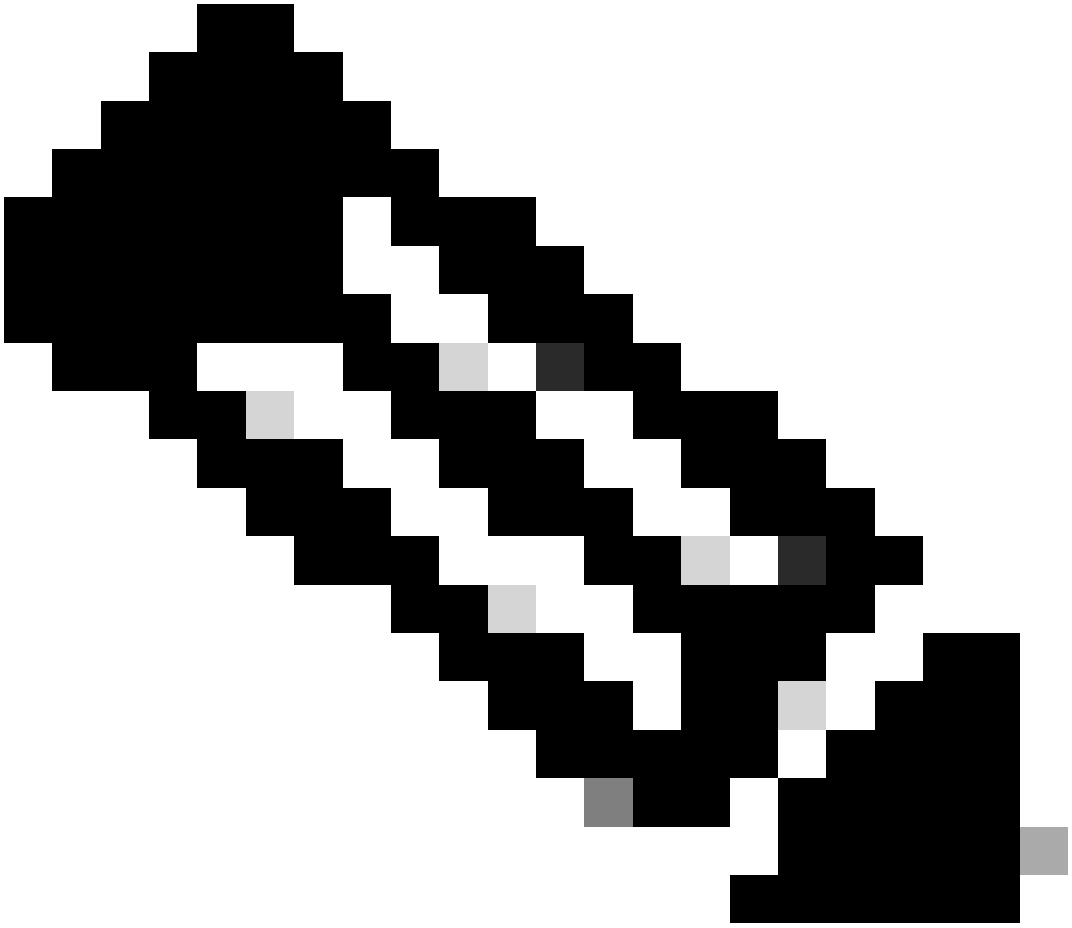
Sélectionner Client Provisioning(Posture)

ACL : redirection

Valeur : Client Provisioning Portal (par défaut)




*ISE_Add_New_Authorization_Profile_Redirect_1*



**Remarque** : cette redirection de nom de liste de contrôle d'accès doit correspondre au nom de liste de contrôle d'accès correspondant configuré sur FTD.

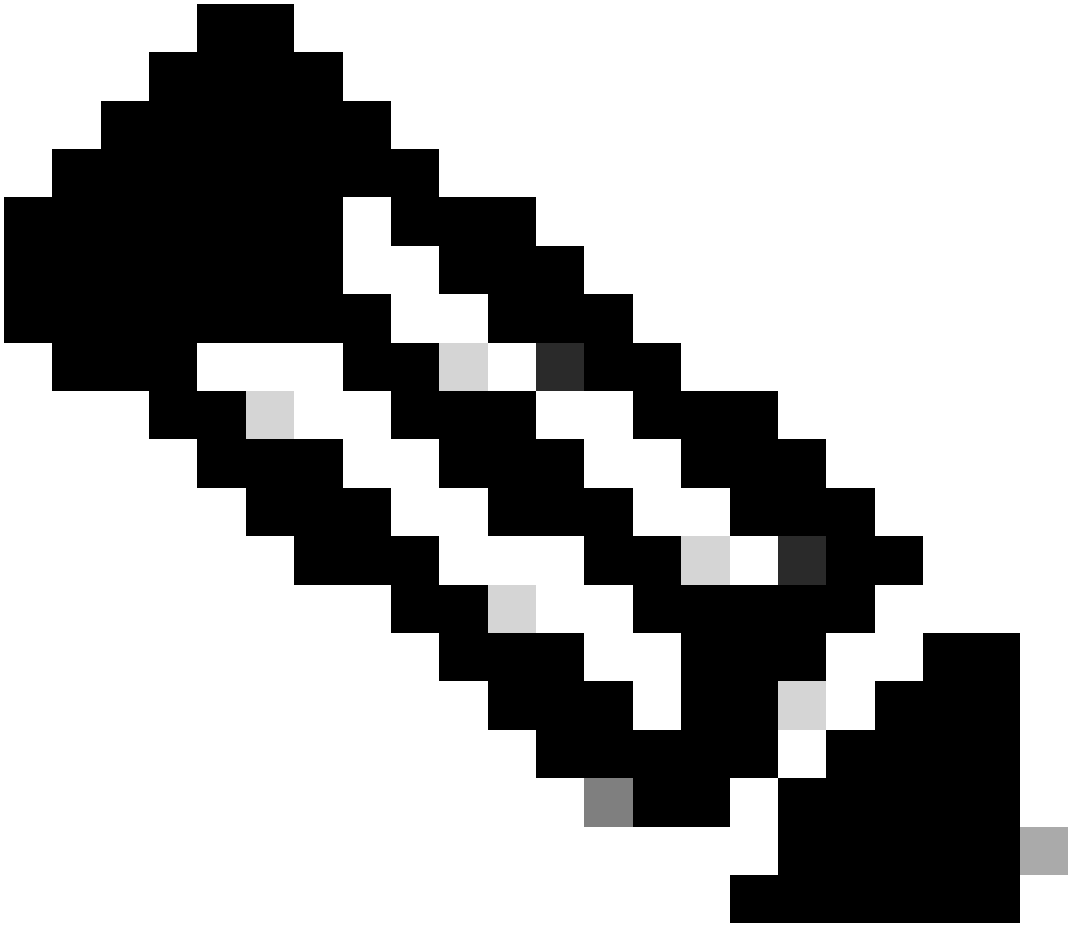
Étape 21.2. Répétez l' Add pour créer deux autres profils d'autorisation pour les terminaux non conformes et conformes avec les détails.

Nom : non_compliance_profile

Nom DACL : DENY_ALL_IPv4_TRAFFIC

Nom : compliance_profile

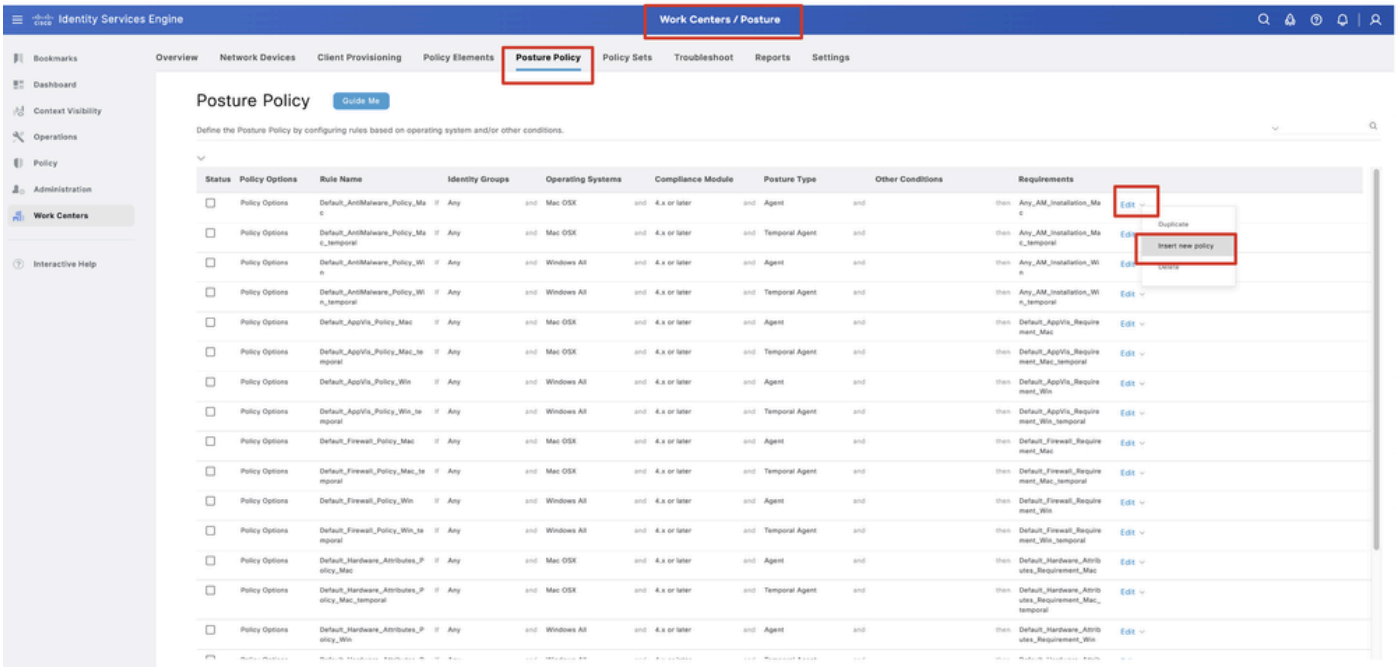
Nom DACL : PERMIT_ALL_IPv4_TRAFFIC



**Remarque** : la liste de contrôle d'accès pour les terminaux conformes ou non conformes doit être configurée en fonction des exigences réelles.

---

Étape 22. Accédez à Work Centers > Posture > Posture Policy. Cliquez sur Edit à la fin des règles. Sélectionnez Insert new policy.




*Politique_Nouvelle_Posture_Ajout_ISE*

Étape 22.1. Configurez les détails :

Nom de la règle : Demo_test_existing_linux

Groupes d'identités : Tous

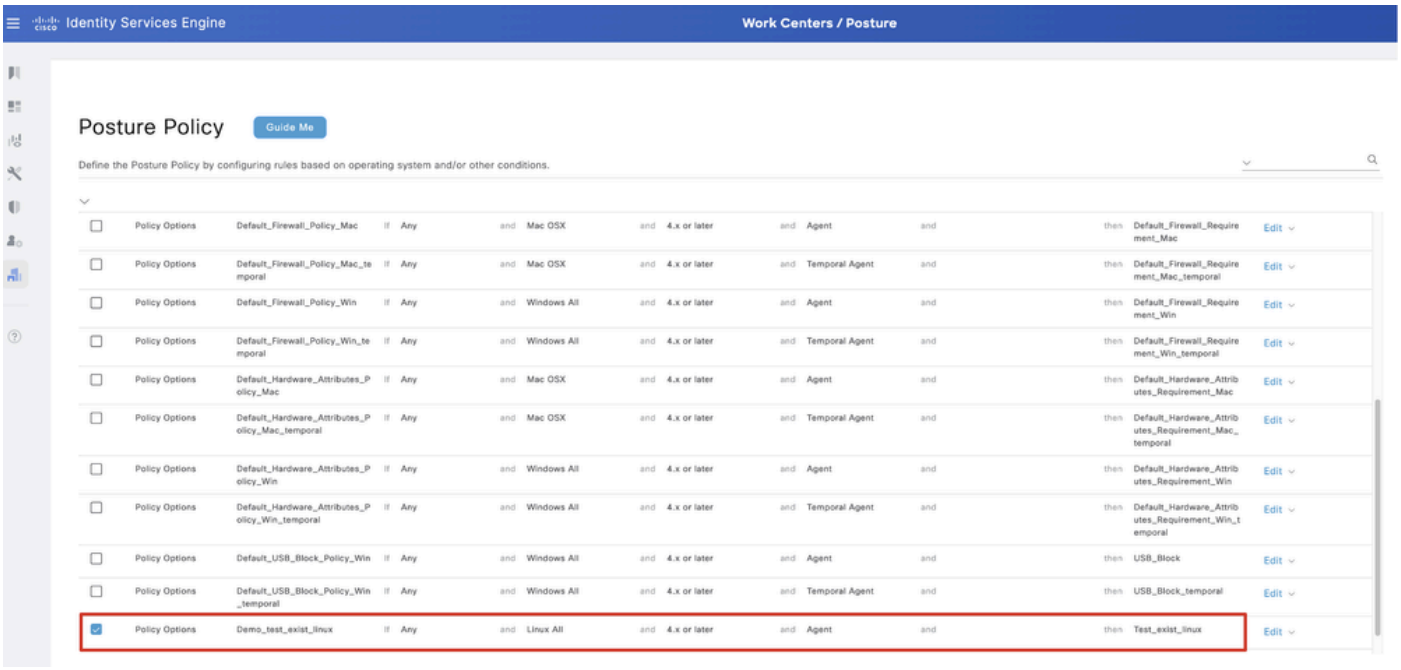
Systèmes d'exploitation : Linux All

Module de conformité : version 4.x ou ultérieure

Type de posture : Agent

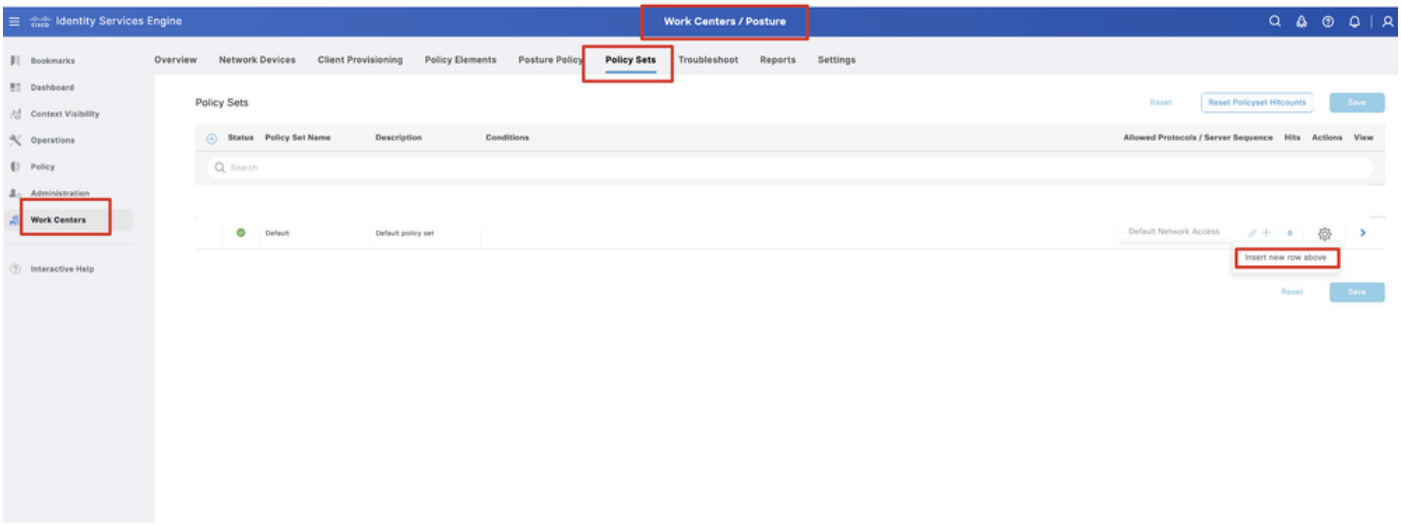
Configuration requise : Test_existing_linux

Cliquez sur Done et Save.




*ISE_Add_New_Posture_Policy_1*

Étape 23. Accédez à Work Centers > Posture > Policy Sets. Cliquez pour Insert new row above.



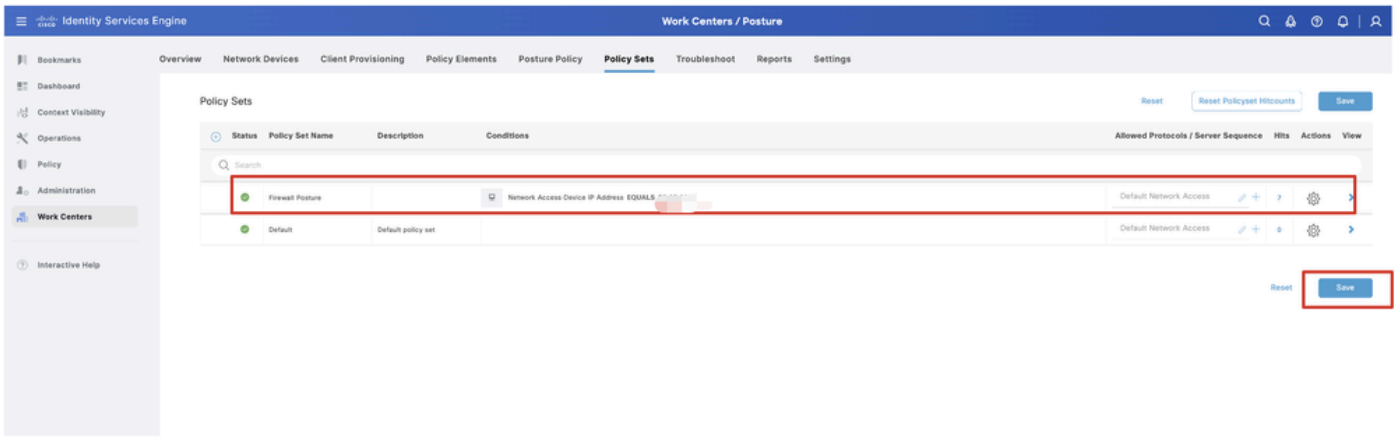

*ISE_Add_New_Policy_Set*

Étape 23.1. Configurez les détails :

Nom du jeu de stratégies : Position du pare-feu

Conditions : ÉGAL à l'adresse IP du périphérique d'accès réseau [FTD IP Address]

Cliquez sur Save .



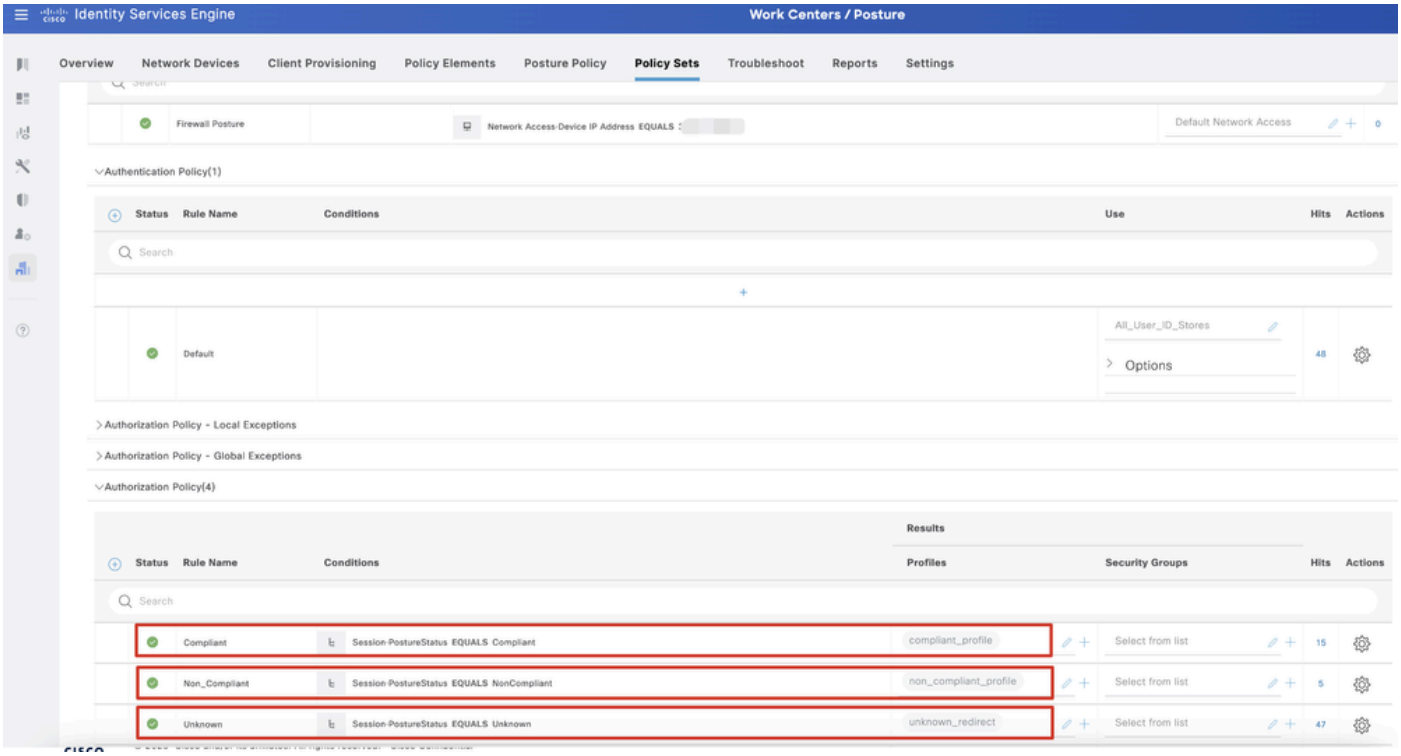

*ISE_Add_New_Policy_Set_1*

Étape 23.2. Cliquez sur > pour entrer le jeu de stratégies. Créez de nouvelles règles d'autorisation pour l'état conforme à la position, non conforme et inconnu. Cliquez sur Save.

Conforme à compliance_profile

Non conforme avec non_compliance_profile

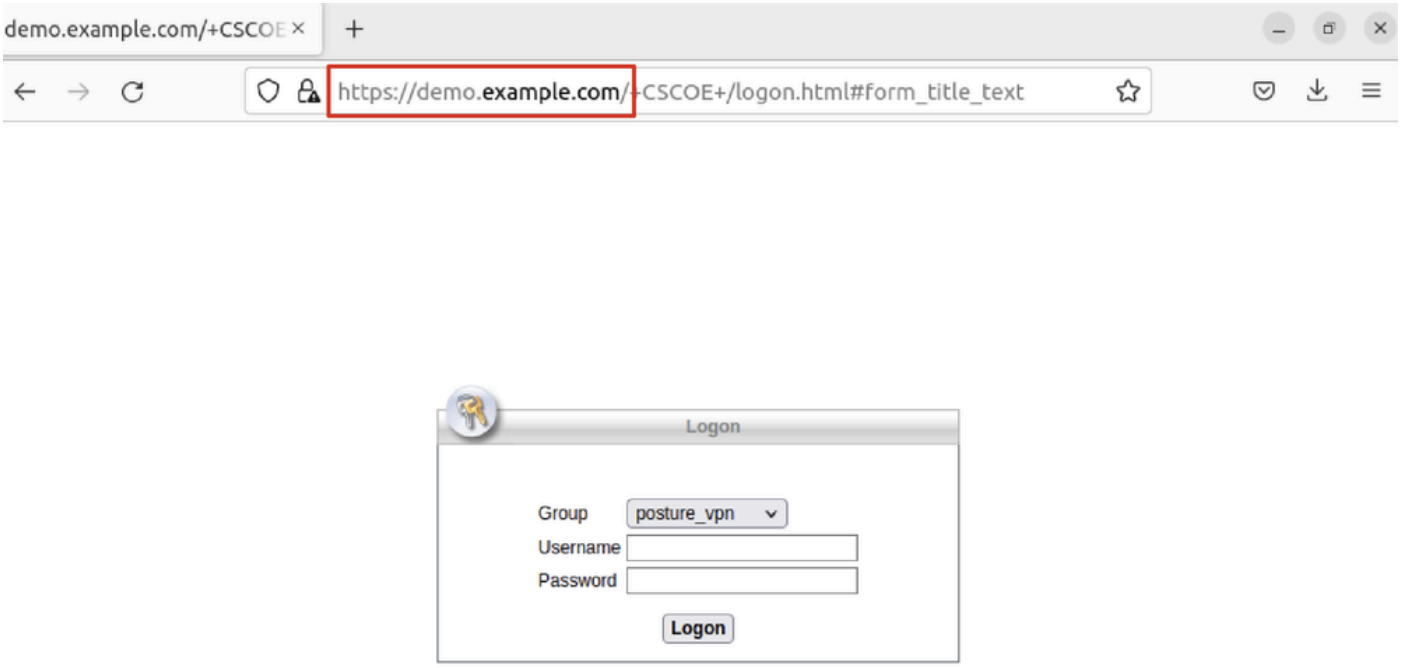
Inconnu avec unknown_redirect




*ISE_Add_New_Policy_Set_2*

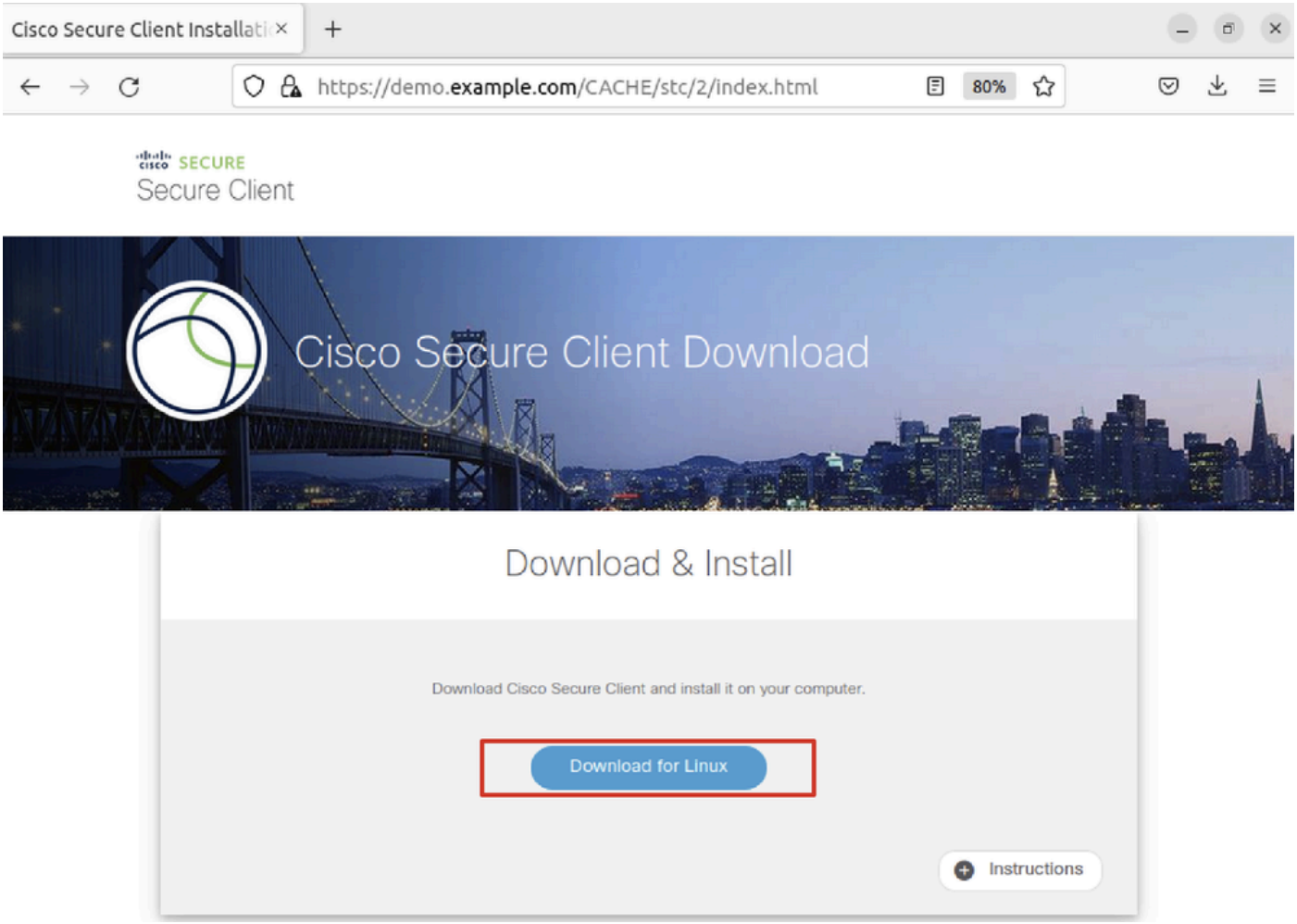
Configurations sur Ubuntu

Étape 24. Connectez-vous au client Ubuntu via l'interface utilisateur graphique. Ouvrez le navigateur pour vous connecter au portail VPN. Dans cet exemple, il s'agit de demo.example.com.



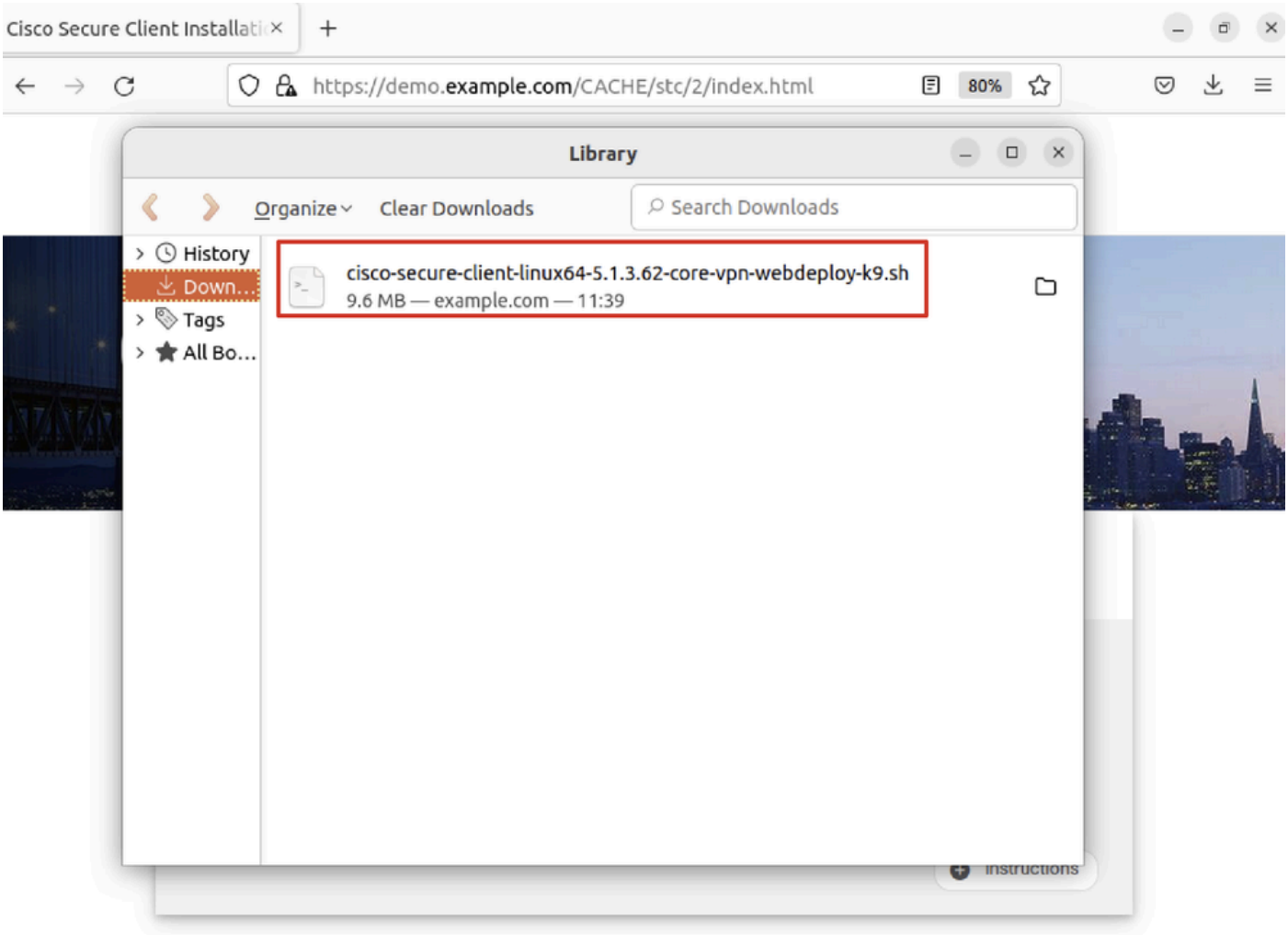

*Ubuntu_Browser_VPN_Login*

Étape 25. Cliquez sur Download for Linux.



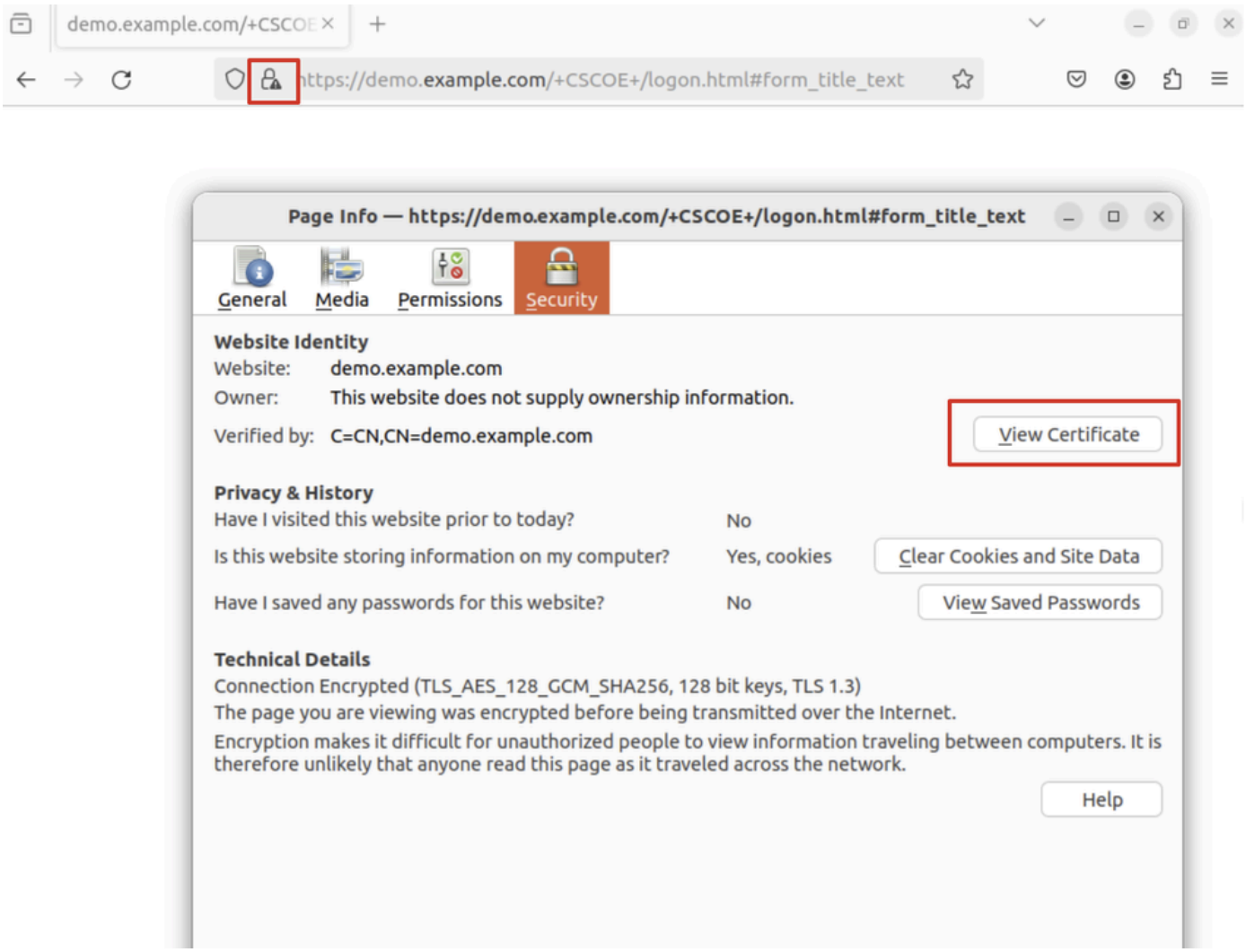

*Ubuntu_Browser_VPN_Download_1*

Le nom du fichier téléchargé est cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.




*Ubuntu_Browser_VPN_Download_2*

Étape 26. Téléchargez le certificat VPN via le navigateur et renommez le fichier en <certificate>.crt. Voici l'exemple d'utilisation de firefox pour télécharger le certificat.




*Ubuntu_Browser_VPN_Cert_Download*

Étape 27. Ouvrez le terminal sur le client Ubuntu. Accédez à pourpath home/user/Downloads/ installer Cisco Secure Client.

<#root>

user@ubuntu22-desktop:~$

**cd Downloads/**

user@ubuntu22-desktop:~/Downloads$

**ls**

**cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh**

demo-example-com.crt

user@ubuntu22-desktop:~/Downloads$

**chmod +x cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh**

user@ubuntu22-desktop:~/Downloads$

**sudo ./cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh**

```
[sudo] password for user:
Installing Cisco Secure Client...
Migrating /opt/cisco/anyconnect directory to /opt/cisco/secureclient directory
Extracting installation files to /tmp/vpn.zaeAZd/vpninst959732303.tgz...
Unarchiving installation files to /tmp/vpn.zaeAZd...
Starting Cisco Secure Client Agent...
Done!
Exiting now.
user@ubuntu22-desktop:~/Downloads$
```

Étape 28. Faites confiance au certificat du portail VPN sur le client Ubuntu.

<#root>

user@ubuntu22-desktop:~$

**cd Downloads/**

```
user@ubuntu22-desktop:~/Downloads$
```

**ls**

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

**demo-example-com.crt**

```
user@ubuntu22-desktop:~/Downloads$
```

**openssl verify demo-example-com.crt**

```
CN = demo.example.com, C = CN
error 18 at 0 depth lookup: self-signed certificate
Error demo-example-com.crt:
```

**verification failed**

```
user@ubuntu22-desktop:~/Downloads$
```

**sudo cp demo-example-com.crt /usr/local/share/ca-certificates/**

```
user@ubuntu22-desktop:~/Downloads$
```

**sudo update-ca-certificates**

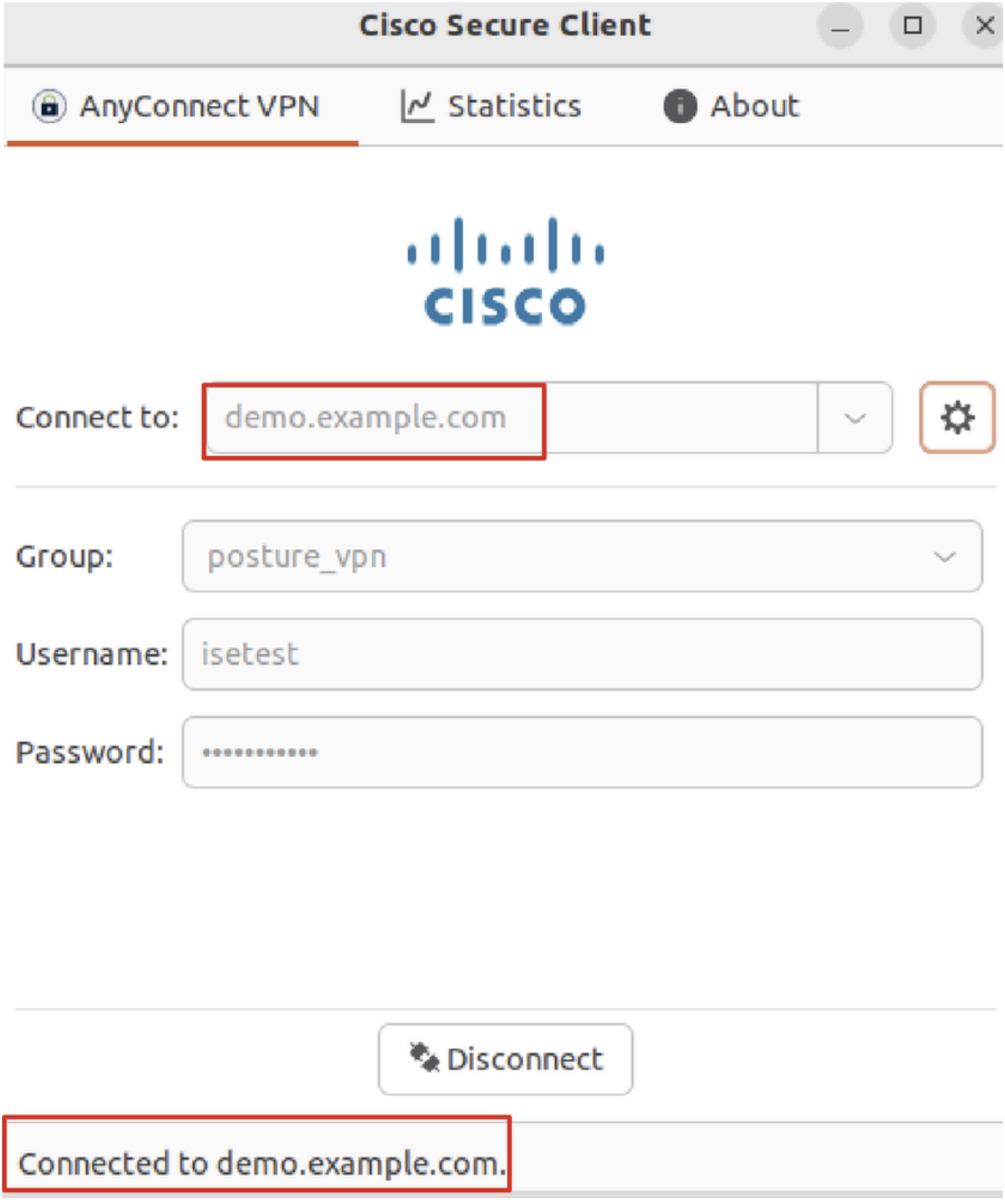
```
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
```

**1 added**

```
, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

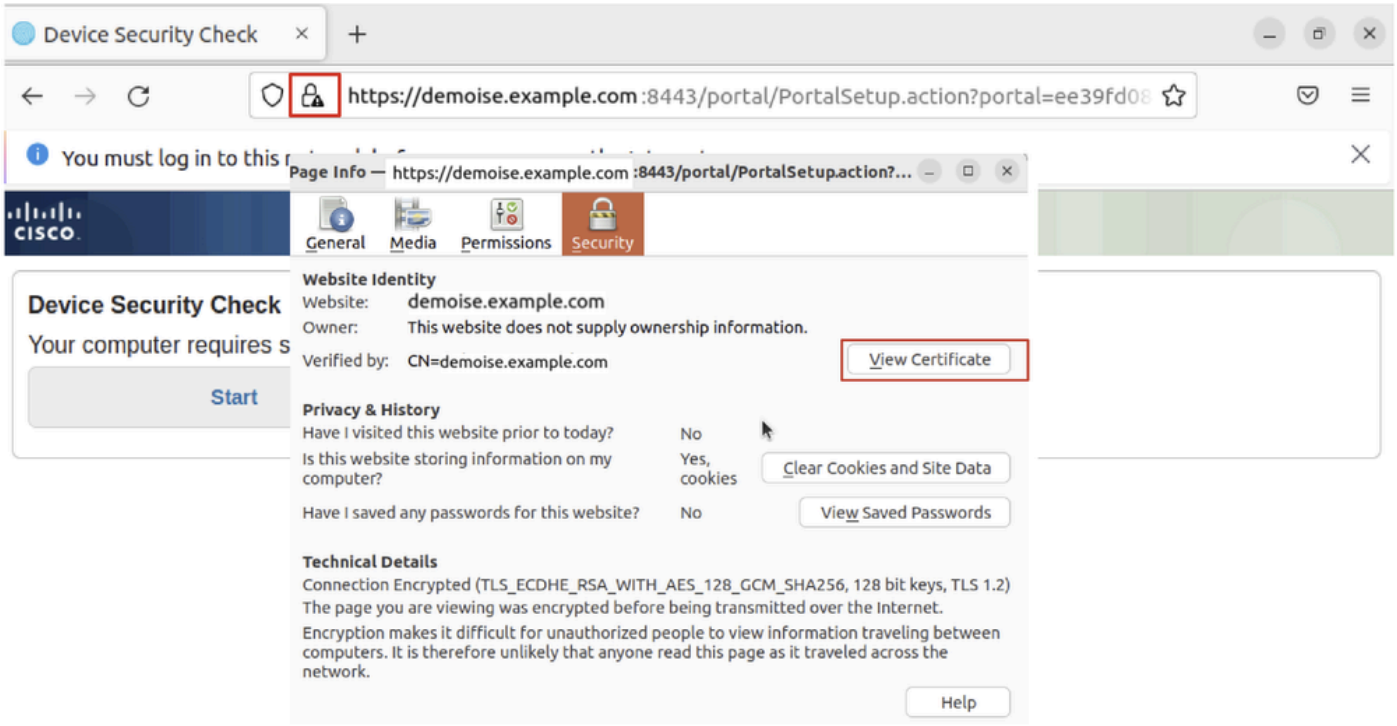
```
user@ubuntu22-desktop:~/Downloads$
openssl verify demo-example-com.crt

demo-example-com.crt: OK
```

Étape 29. Ouvrez Cisco Secure Client sur le client Ubuntu et connectez le VPN à demo.example.com avec succès.




*Ubuntu_Secure_Client_Connected*

Étape 30. Ouvrez le navigateur pour accéder à tout site Web déclenchant la redirection vers le portail CPP ISE. Téléchargez le certificat à partir du portail CPP ISE et renommez le fichier <certificate>.crt. Voici un exemple d'utilisation de Firefox pour le téléchargement.




*Ubuntu_Browser_CPP_Cert_Download*

Étape 30.1. Faites confiance au certificat du portail CPP ISE sur le client Ubuntu.

## <#root>

user@ubuntu22-desktop:~/Downloads$ ls
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
demo-example-com.crt

**ise-cert.crt**

user@ubuntu22-desktop:~/Downloads$

**sudo cp ise-cert.crt /usr/local/share/ca-certificates/**

user@ubuntu22-desktop:~/Downloads$

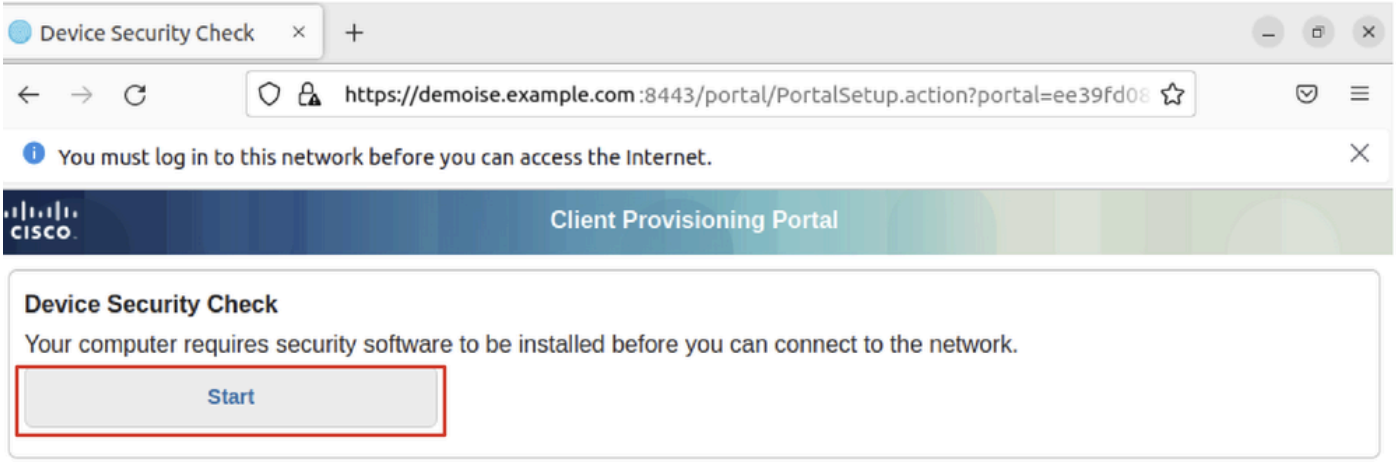
**sudo update-ca-certificates**

Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL

**1 added**

, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.

Étape 31. Cliquez Start sur le portail CPP ISE.




*Ubuntu_Browser_CPP_Start*

Étape 32. Click here to download and install Agent.


*Ubuntu_Browser_CPP_Download_Posture*

Étape 33. Ouvrez le terminal sur le client Ubuntu. Accédez au chemin home/user/Downloads/ d'installation du module de posture.

<#root>

user@ubuntu22-desktop:~/Downloads$ ls

**cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6HoLmL**

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
demo-example-com.crt
ise-cert.crt

user@ubuntu22-desktop:~/Downloads$
```

**chmod +x cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfy**

```
user@ubuntu22-desktop:~/Downloads$
user@ubuntu22-desktop:~/Downloads$
user@ubuntu22-desktop:~/Downloads$
```

**./cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6HoL**

```
Cisco Network Setup Assistant
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
Cisco ISE Network Setup Assistant started. Version - 5.1.3.62
Trusted and Secure Connection
You are connected to

demoise.example.com

whose identity has been certified. Your connection to this website is encrypted.
Downloading Cisco Secure Client...
Downloading remote package...
Running Cisco Secure Client - Downloader...
Installation is completed.
```

Étape 34. Sur l'interface utilisateur du client Ubuntu, quittez le client sécurisé Cisco et rouvrez-le. Le module de posture ISE est installé et s'exécute correctement.


*Ubuntu_Secure_Client_ISE_Posture_Installed*

Étape 35. Ouvrez le terminal sur le client Ubuntu. Accédez à path home/user/Desktop , créez un fichiertest.txt pour répondre à la condition de fichier configurée sur ISE.

<#root>

user@ubuntu22-desktop:~$

**cd Desktop/**

```
user@ubuntu22-desktop:~/Desktop$
```

```
echo test > test.txt
```

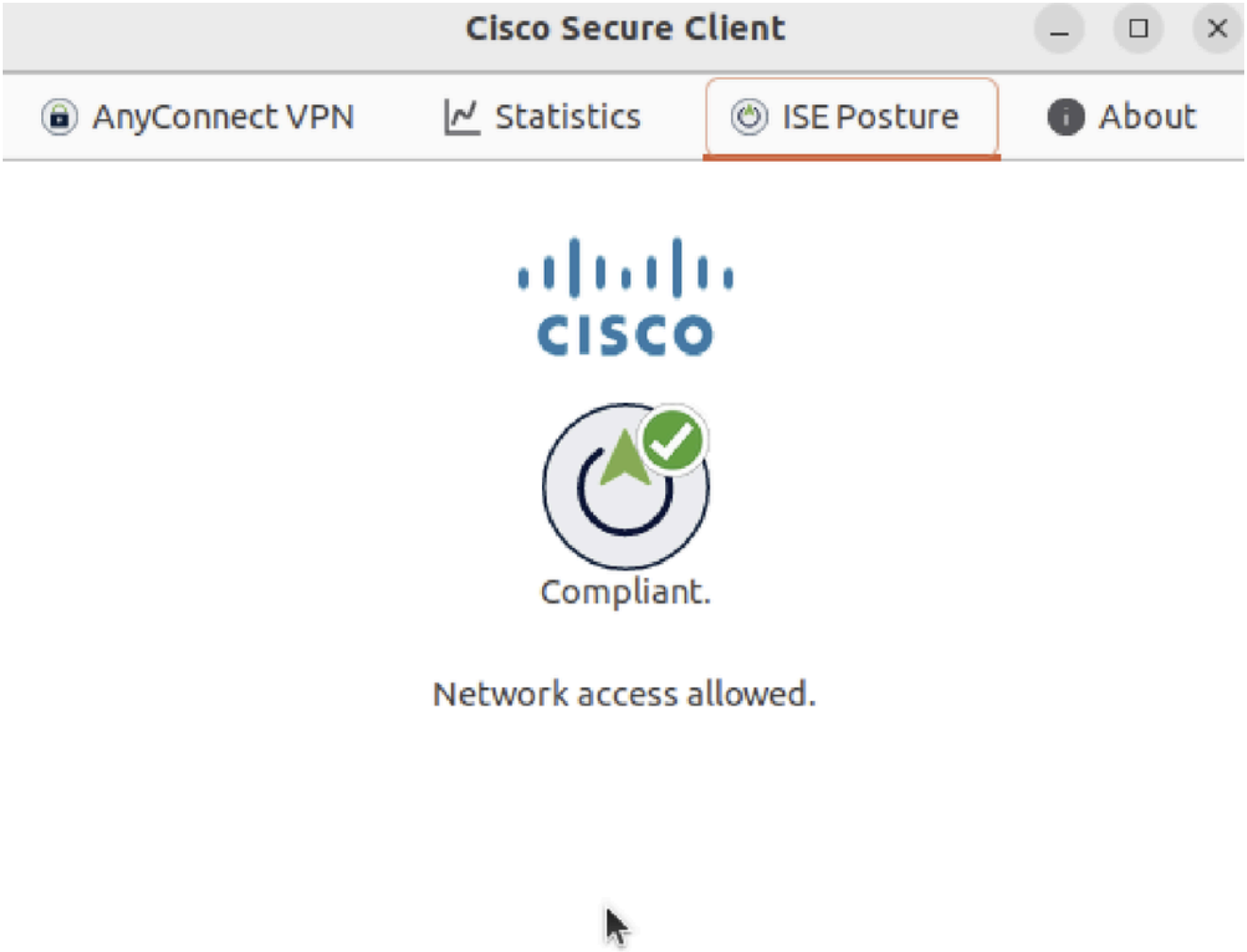
Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Connectez le VPN à demo.example.com sur le client Ubuntu.

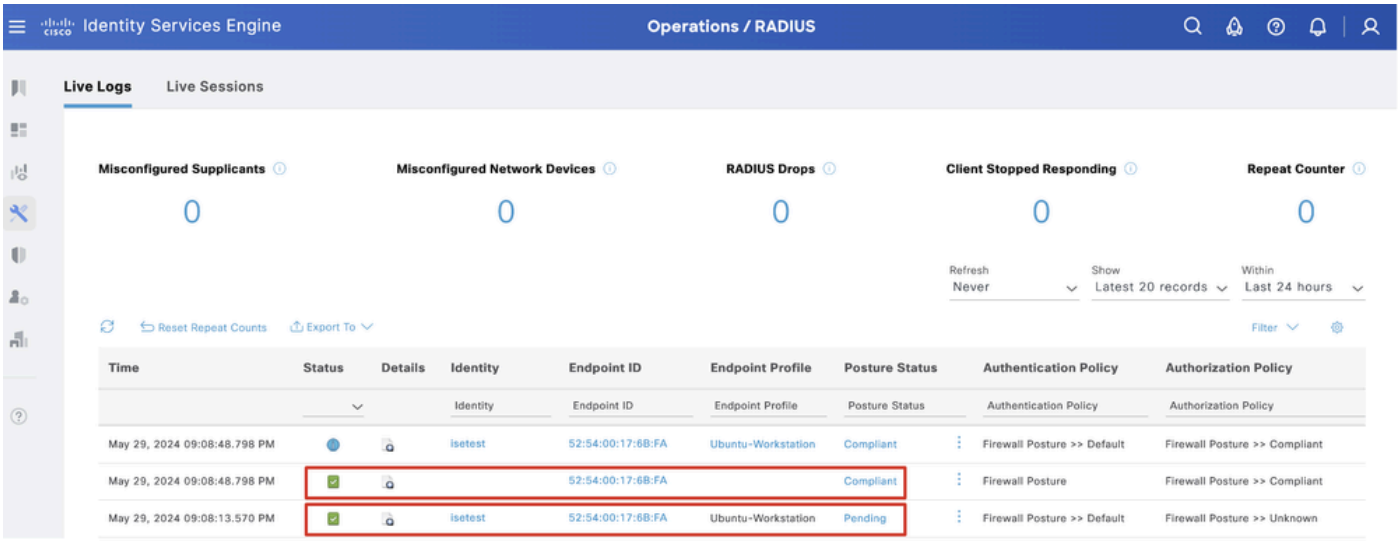

*Vérifier_Ubuntu_Secure_Client_Connected*

Étape 2. Vérifiez l'état de la position ISE sur le client Ubuntu.




*Vérifier_Ubuntu_Secure_Client_Compliant*

Étape 3. Cochez Radius Live Log sur ISE. Accédez à Operations > RADIUS Live Log.



Étape 4. Accédez à FTD CLI via SSH ou la console.

```
<#root>

>
>

system support diagnostic-cli


Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv741>

enable


Password:
ftdv741#
ftdv741#

show vpn-sessiondb detail anyconnect



Session Type: AnyConnect Detailed

Username : isetest Index : 33
Assigned IP : 192.168.6.30 Public IP : 192.168.10.13
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 : 51596 Bytes Rx : 17606
Pkts Tx : 107 Pkts Rx : 136
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : posture_gp Tunnel Group : posture_vpn
Login Time : 14:02:25 UTC Fri May 31 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820002100006659d871
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 33.1
Public IP : 192.168.10.13
Encryption : none Hashing : none
TCP Src Port : 59180 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : linux-64

Client OS Ver: Ubuntu 22.04 LTS 22.04 (Jammy Jellyfish)
```

```
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62

Bytes Tx : 6364 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 33.2
Assigned IP :192.168.6.30 Public IP : 192.168.10.13
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 59182
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Linux_64
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62
Bytes Tx : 6364 Bytes Rx : 498
Pkts Tx : 1 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

DTLS-Tunnel:
Tunnel ID : 33.3
Assigned IP :192.168.6.30 Public IP : 192.168.10.13
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56078
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Linux_64
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62
Bytes Tx : 38868 Bytes Rx : 17108
Pkts Tx : 105 Pkts Rx : 130
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
```

## Dépannage

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

Pour le flux de posture et le dépannage de Cisco Secure Client et ISE, consultez les **documents** CCO**Comparaison des styles de posture ISE pour les versions antérieures et postérieures à 2.2** et **Dépannage de la gestion et de la posture des sessions ISE.**

## Informations connexes

- Compatibilité des composants réseau de Cisco Identity Services Engine, version 3.3

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.3
- **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.