Configuración de la condición de VPN de Linux con ISE 3.3

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Configurar

- Diagrama de la red
- Configuraciones en FMC/FTD
- Configuraciones en ISE
- Configuraciones en Ubuntu

Verificación

Troubleshoot

Información Relacionada

Introducción

Este documento describe cómo configurar el estado de la VPN Linux con Identity Services Engine (ISE) y Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cliente seguro de Cisco
- VPN de acceso remoto en Firepower Threat Defence (FTD)
- Identity Services Engine (ISE)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

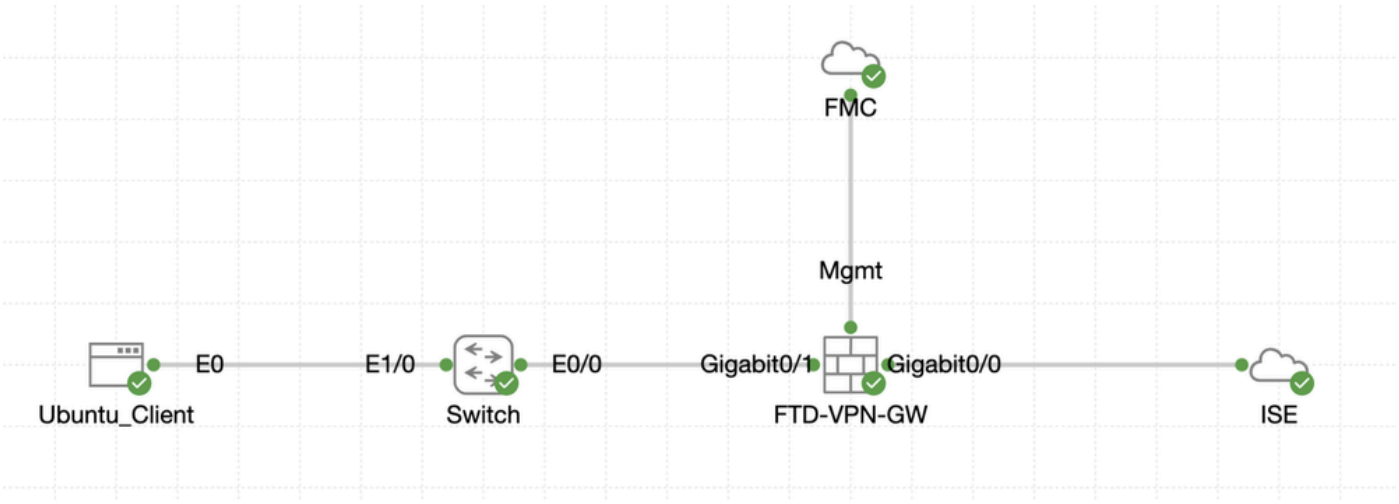
- Ubuntu 22,04
- Cisco Secure Client 5.1.3.62

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



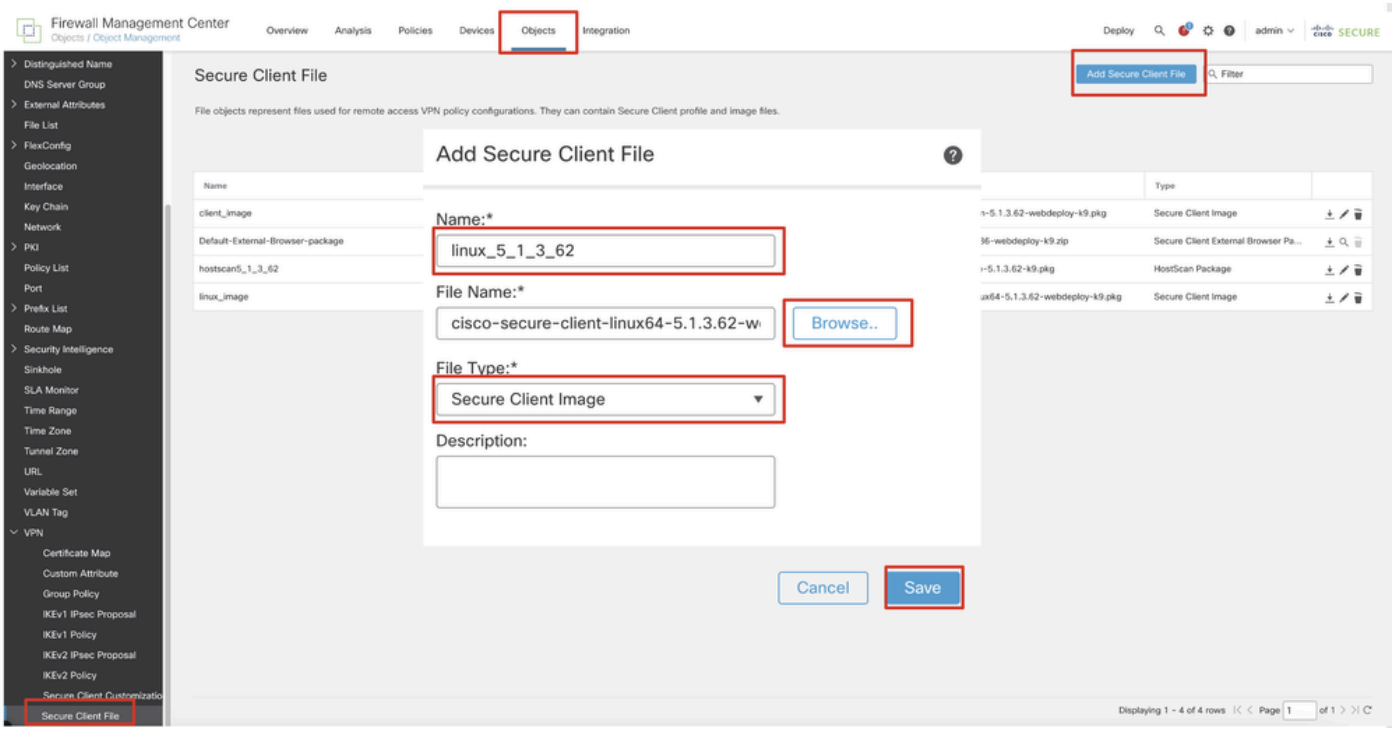
Topología

Configuraciones en FMC/FTD

Paso 1. La conectividad entre el cliente, FTD, FMC e ISE se ha configurado correctamente. Como enroll.cisco.com se utiliza para los terminales que hacen sondeos para redirección (consulte los documentos de CCO sobre el flujo de postura Comparación del estilo de postura ISE para versiones anteriores y posteriores a la 2.2 para obtener más información). Asegúrese de que la ruta para el tráfico a enroll.cisco.com en FTD esté configurada correctamente.

Paso 2. Descargue el nombre del paquete cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg de Descarga de Software de Cisco y asegúrese de que el archivo sea bueno después de la descarga confirmando que la suma de comprobación md5 del archivo descargado es la misma que la página de Descarga de Software de Cisco.

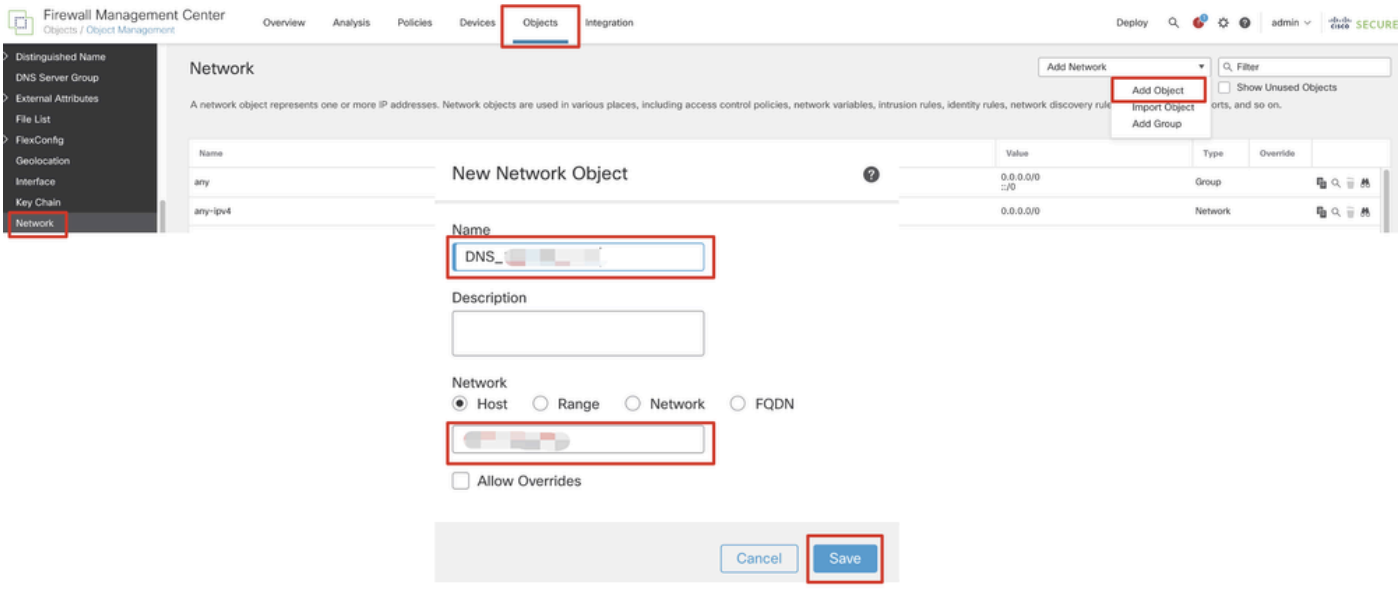
Paso 3. Desplácese hasta Objects > Object Management > VPN > Secure Client File. Haga clic en Add Secure Client File, proporcione el nombre, navegue File Name para seleccionar cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg, seleccione Secure Client Image en la lista desplegableFile Type. A continuación, haga clic en Save.



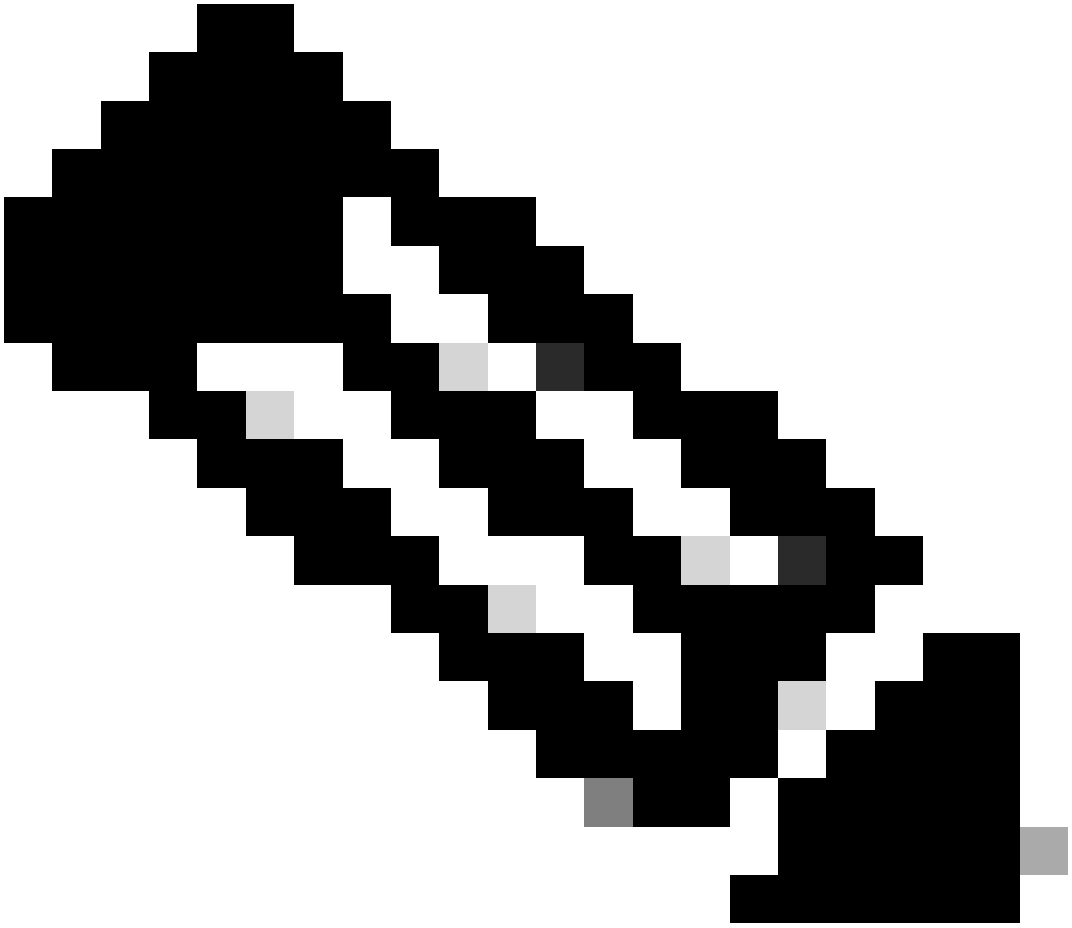
FMC_Upload_Secure_Client_Image

Paso 4. Desplácese hasta Objects > Object Management > Network.

Paso 4.1. Cree un objeto para el servidor DNS. Haga clic en Add Object, indique el nombre y la dirección IP de DNS disponible. Haga clic en Save.

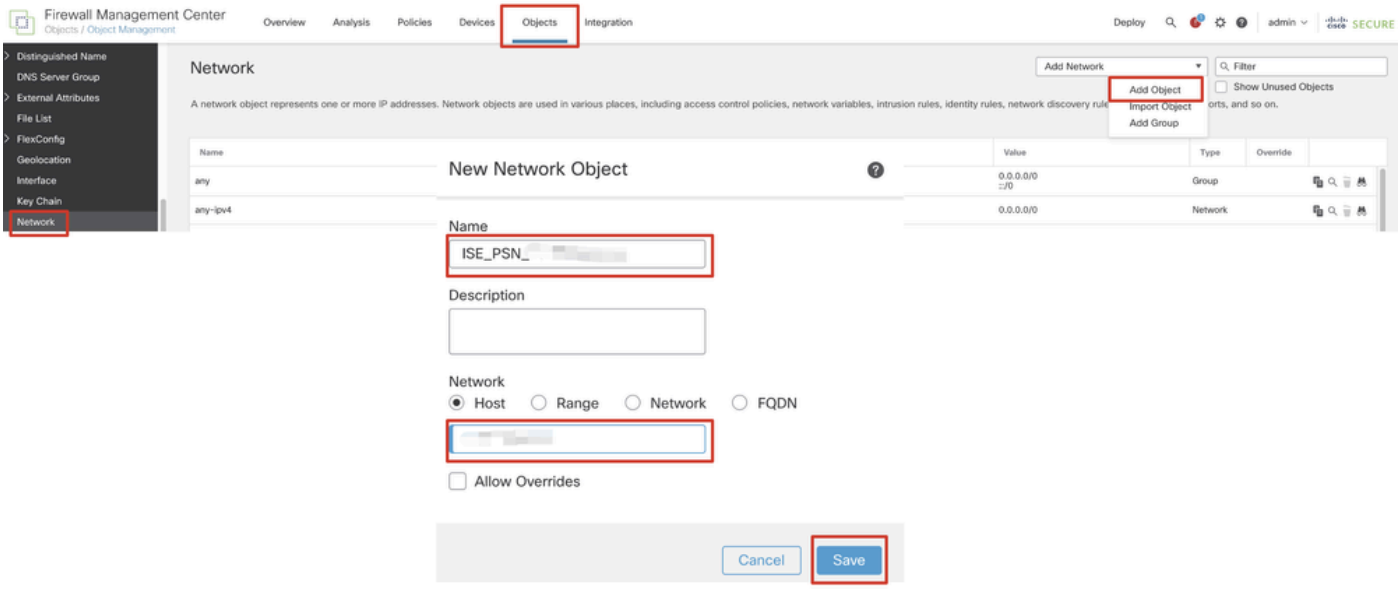


FMC_Add_Object_DNS



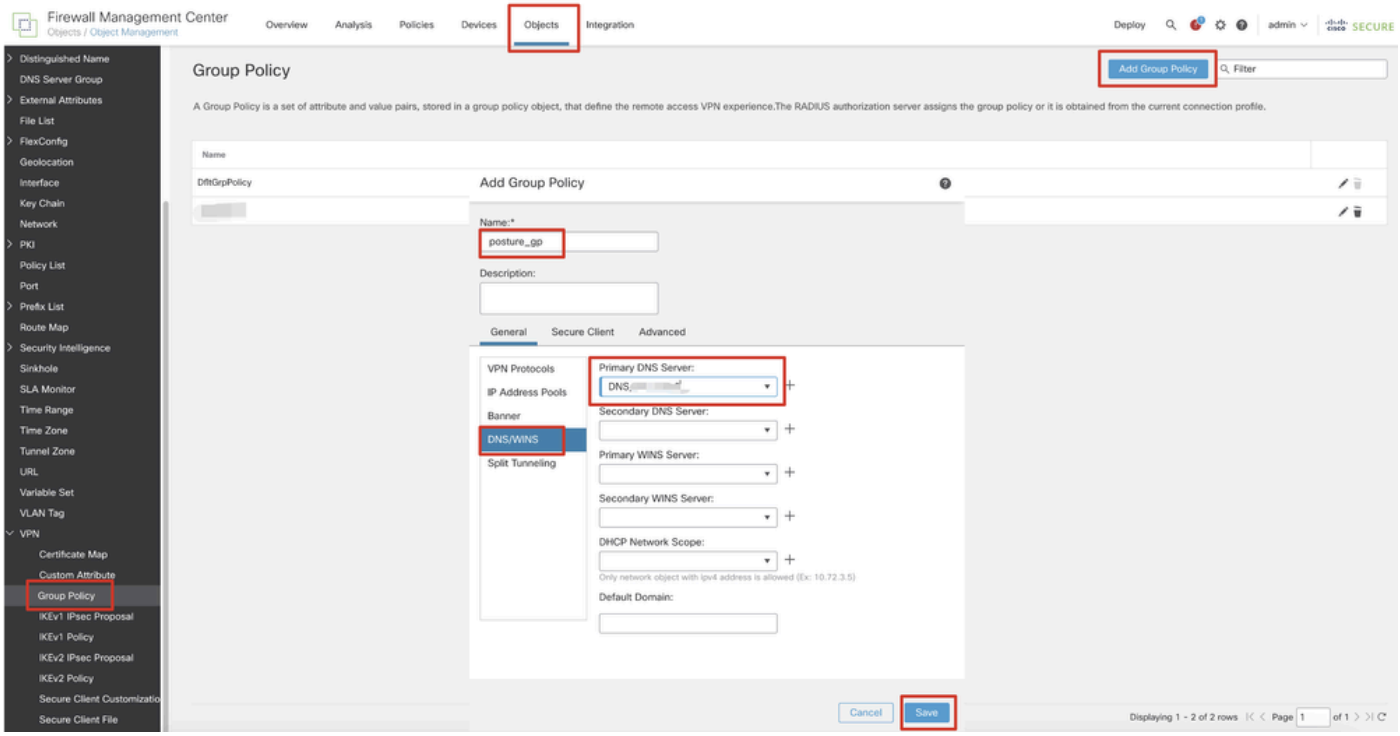
Nota: El servidor DNS configurado aquí se debe utilizar para los usuarios de VPN.

Paso 4.2. Cree un objeto para ISE PSN. Haga clic en Add Object, introduzca el nombre y la dirección IP PSN de ISE disponible. Haga clic en Save.

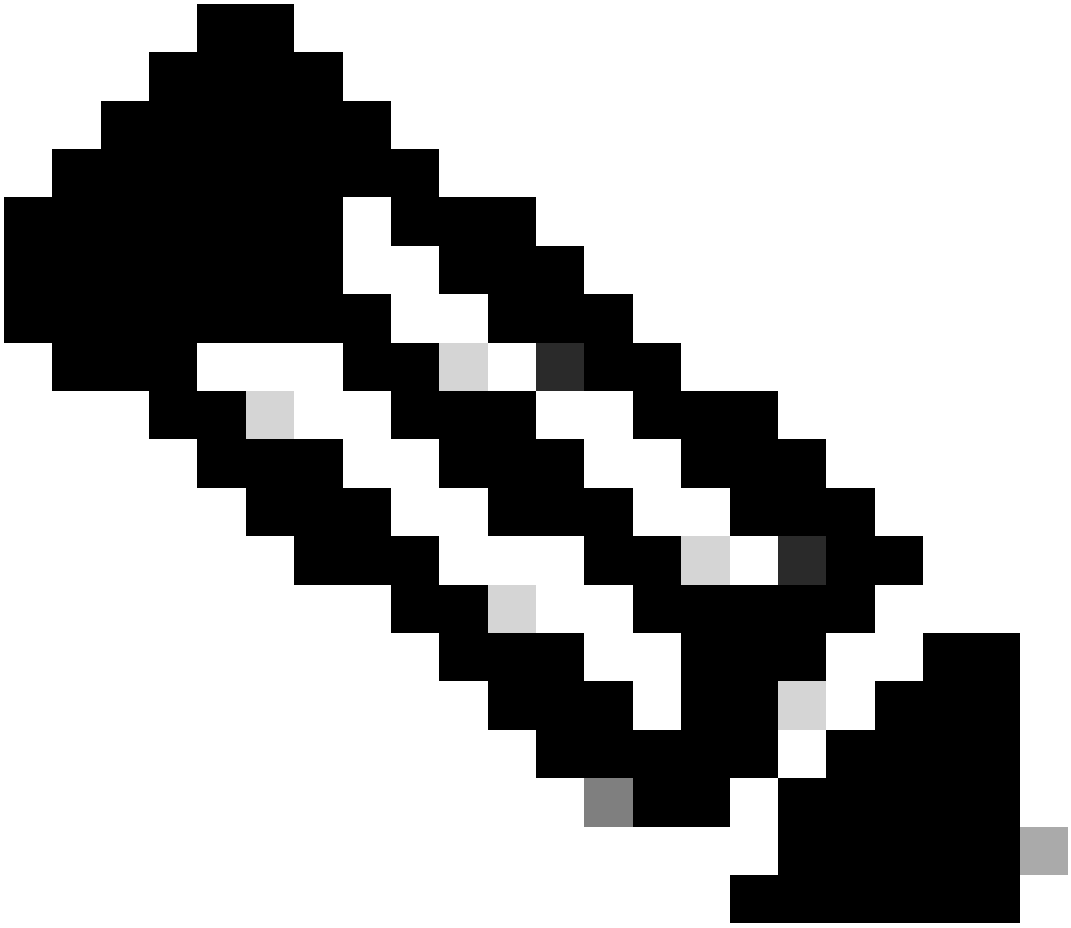


FMC_Add_Object_ISE

Paso 5. Desplácese hasta Objects > Object Management > VPN > Group Policy. Haga clic en Add Group Policy. Haga clic en DNS/WINS, seleccione el objeto del servidor DNS en Primary DNS Server. A continuación, haga clic en Save.

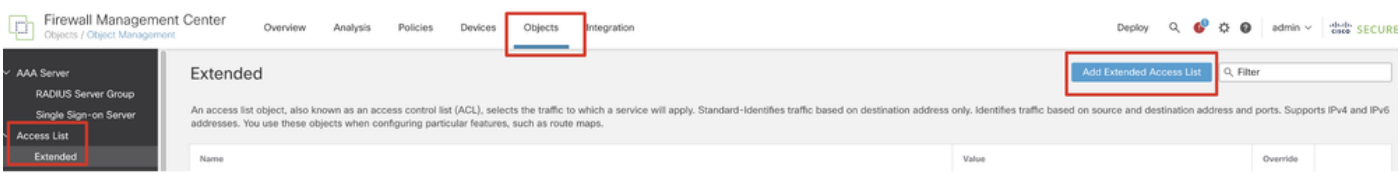


FMC_Add_Group_Policy



Nota: asegúrese de que el servidor DNS utilizado en la política de grupo VPN puede resolver el FQDN y enroll.cisco.com del portal de aprovisionamiento de clientes de ISE.

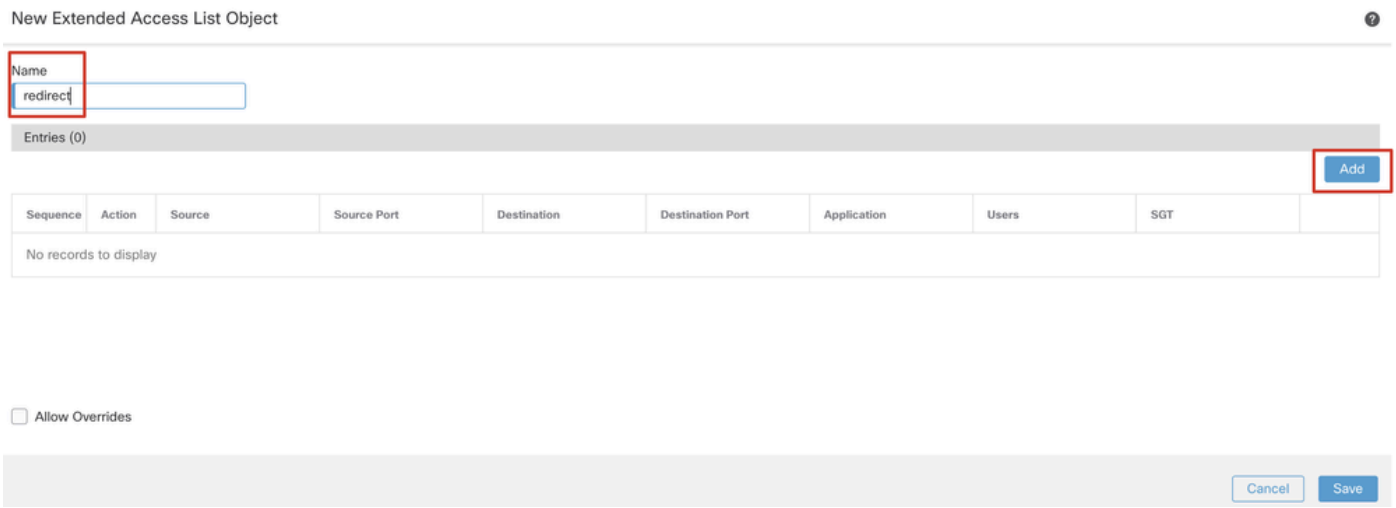
Paso 6. Desplácese hasta Objects > Object Management > Access List > Extended. Haga clic en Add Extended Access List.



FMC_Add_Redirect_ACL

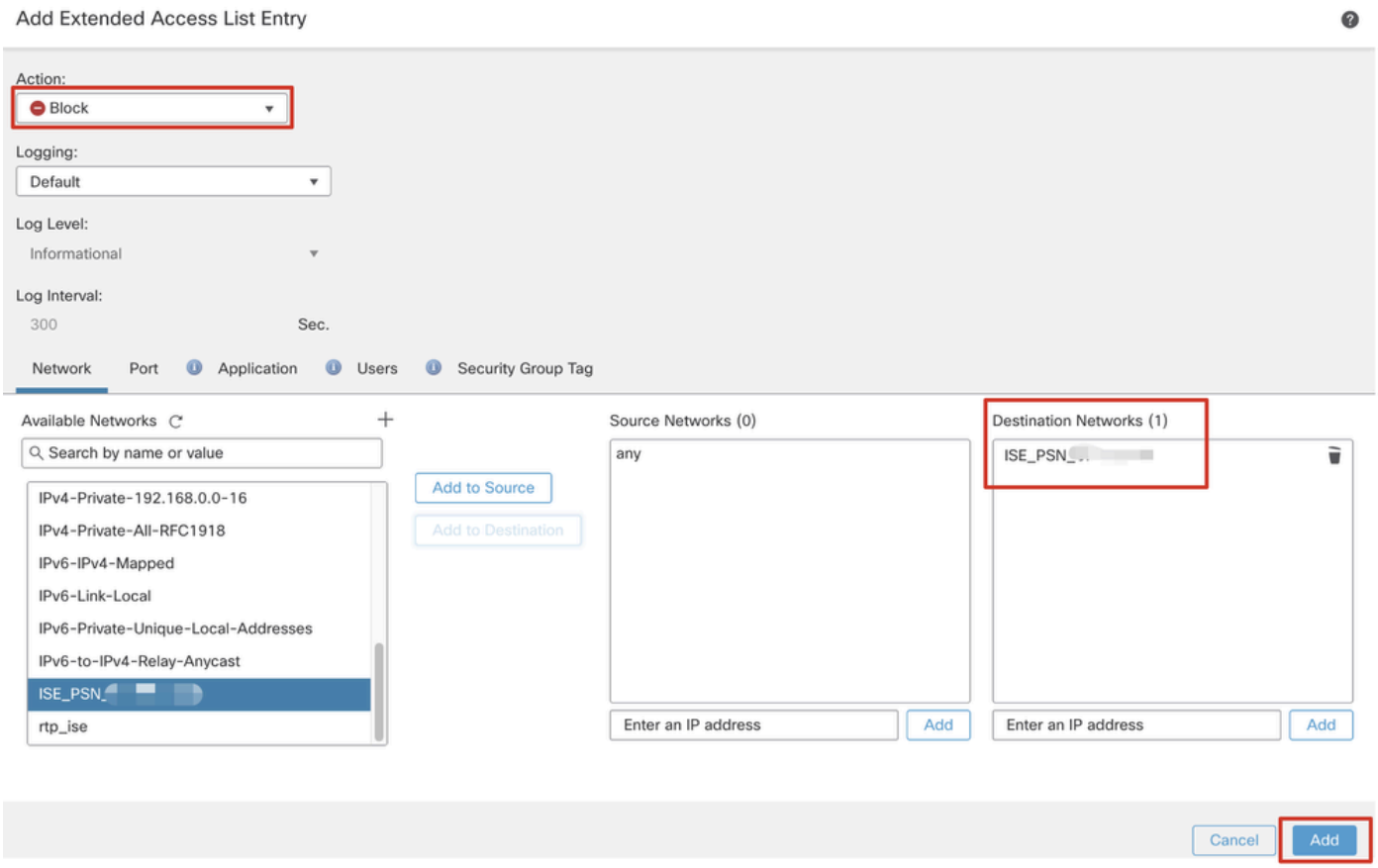
Paso 6.1. Proporcione el nombre de la ACL de redirección. Este nombre debe ser el mismo que en el perfil de autorización de ISE. Haga clic en

Add.

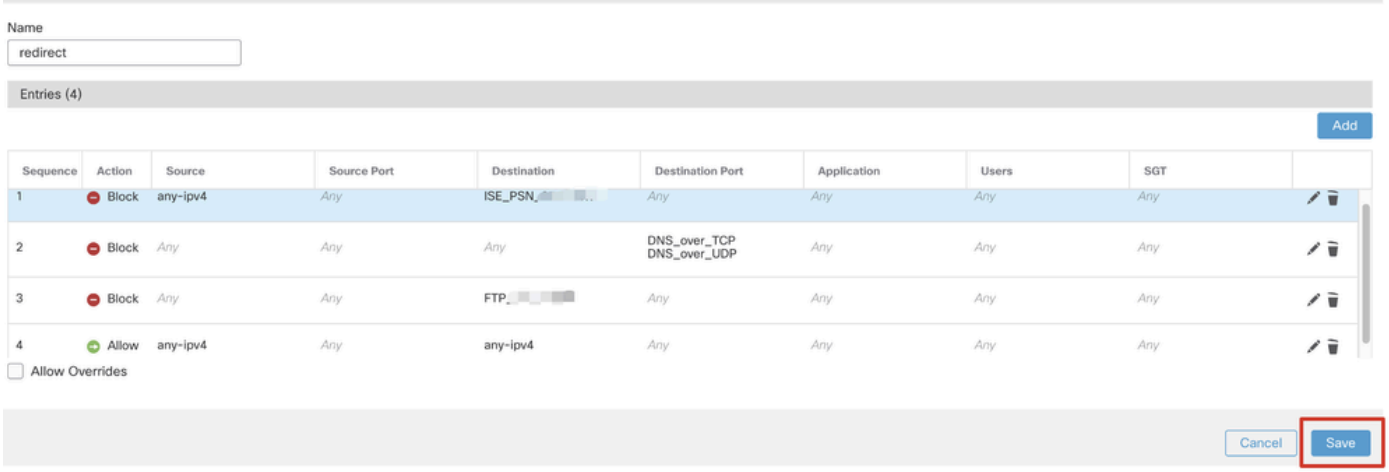


FMC_Add_Redirect_ACL_Part_1

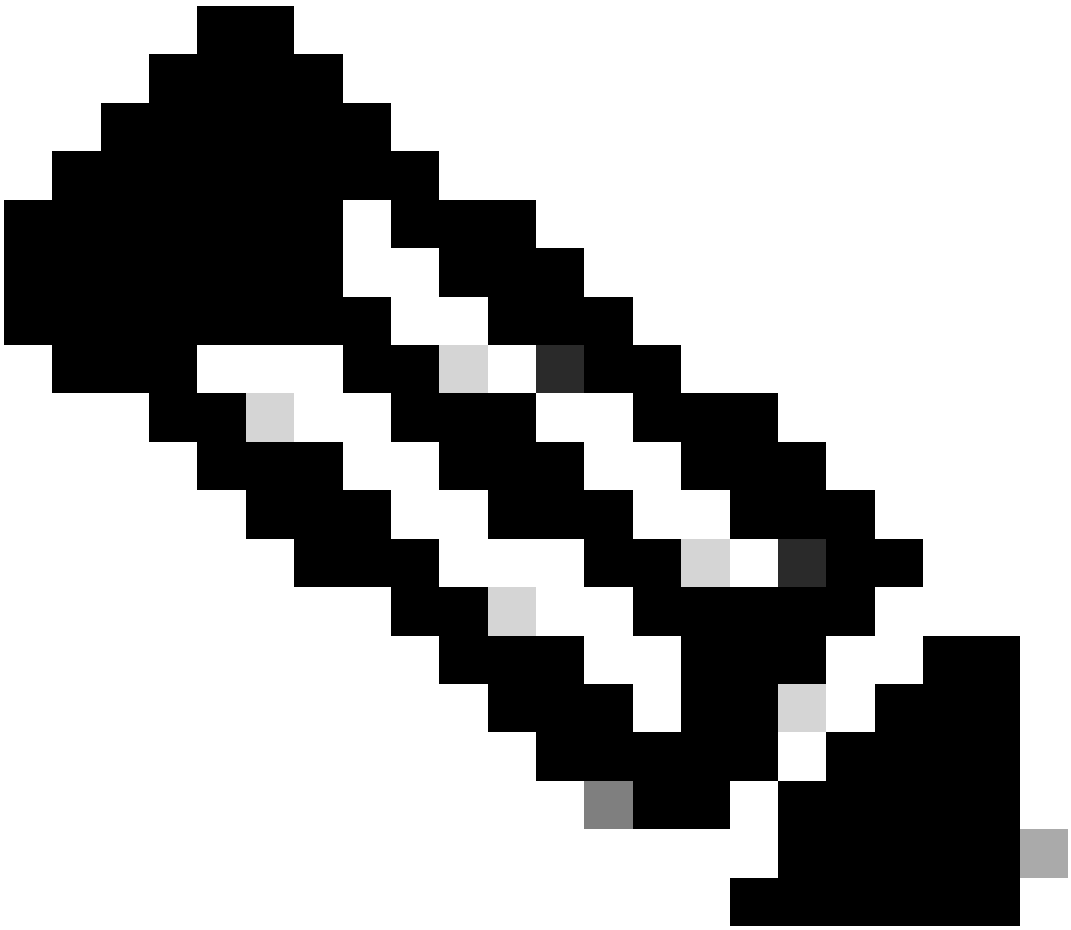
Paso 6.2. Bloquee el tráfico DNS, el tráfico a la dirección IP PSN de ISE y los servidores de corrección para excluirlos de la redirección. Permitir el resto del tráfico. Esto activa la redirección. Haga clic en Save.



FMC_Add_Redirect_ACL_Part_2

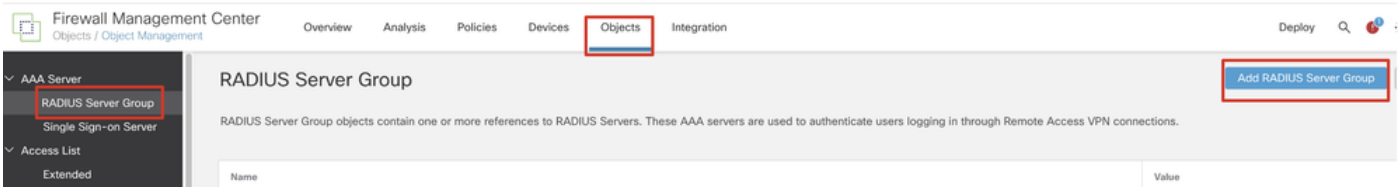


FMC_Add_Redirect_ACL_Part_3



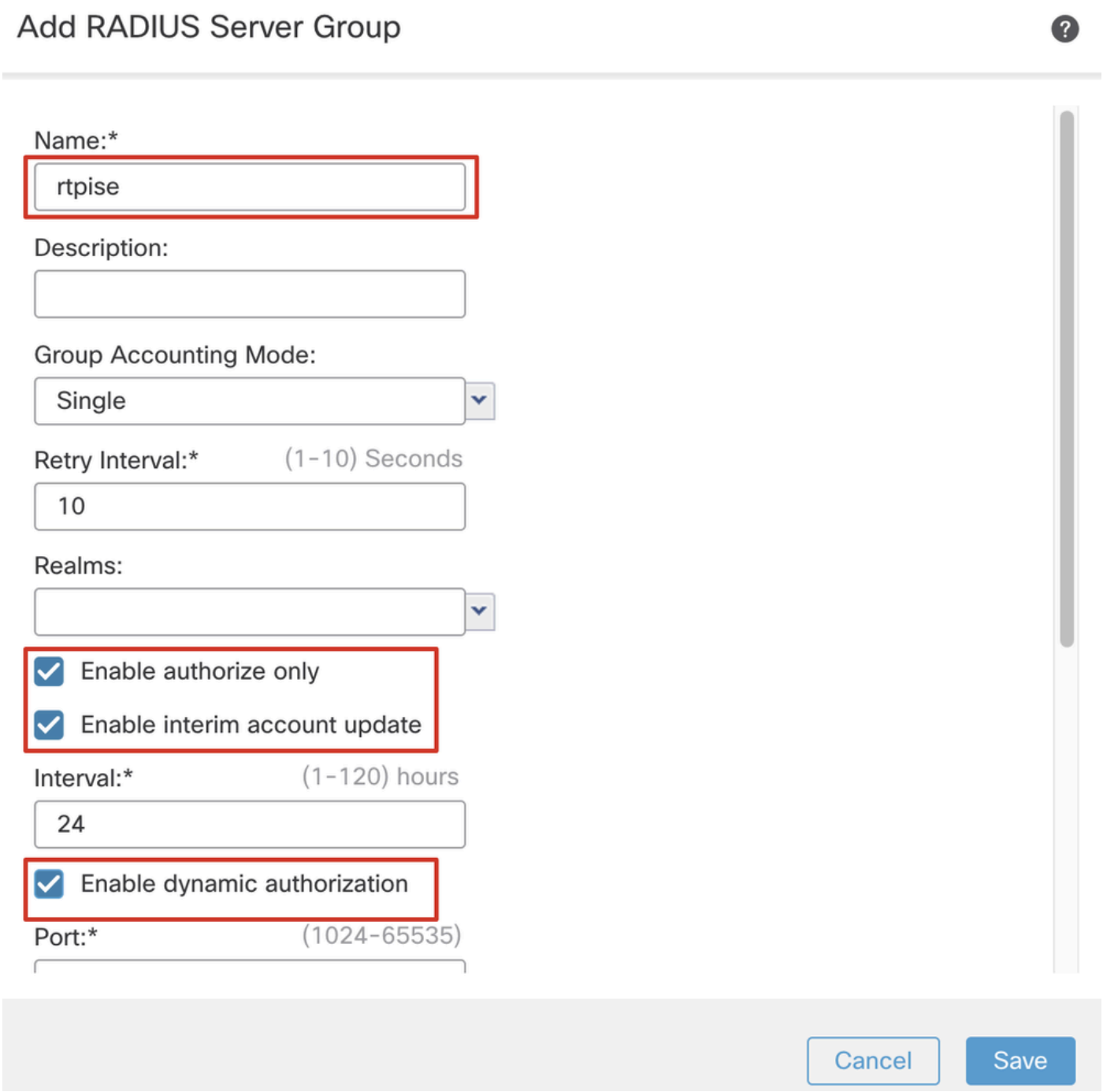
Nota: El FTP de destino en este ejemplo de ACL de redirección se utiliza como ejemplo de servidor de corrección.

Paso 7. Desplácese hasta Objects > Object Management > RADIUS Server Group. Haga clic en Add RADIUS Server Group.



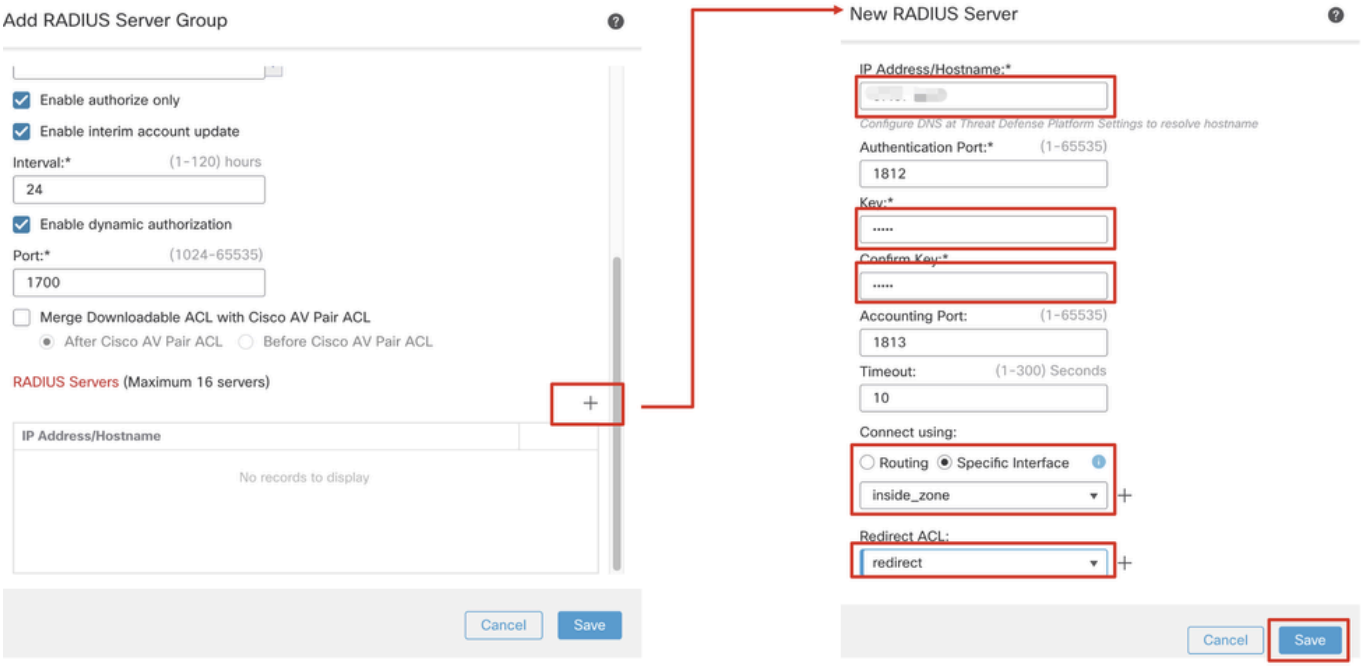
FMC_Add_New_Radius_Server_Group

Paso 7.1. Proporcione el nombre, la comprobación Enable authorize only, la comprobación Enable interim account update, la comprobación Enable dynamic authorization.



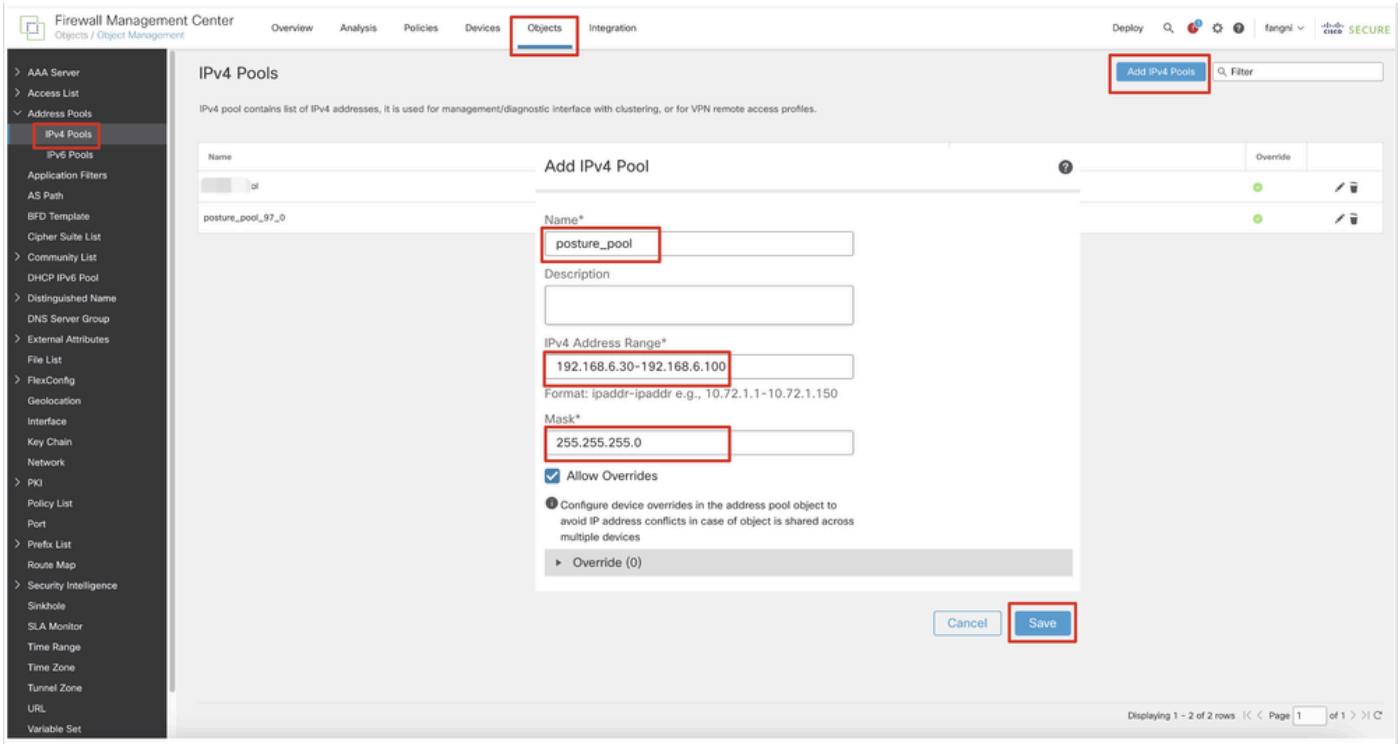
FMC_Add_New_Radius_Server_Group_Part_1

Paso 7.2. Haga clic en el Plus icono para agregar un nuevo servidor RADIUS. Proporcione el ISE PSN IP Address/Hostname, Key. Seleccione el specific interface para conectarse. Seleccione el Redirect ACL. A continuación, haga clic Savepara guardar el nuevo servidor RADIUS. A continuación, haga clic Save de nuevo para guardar el nuevo grupo de servidores RADIUS.



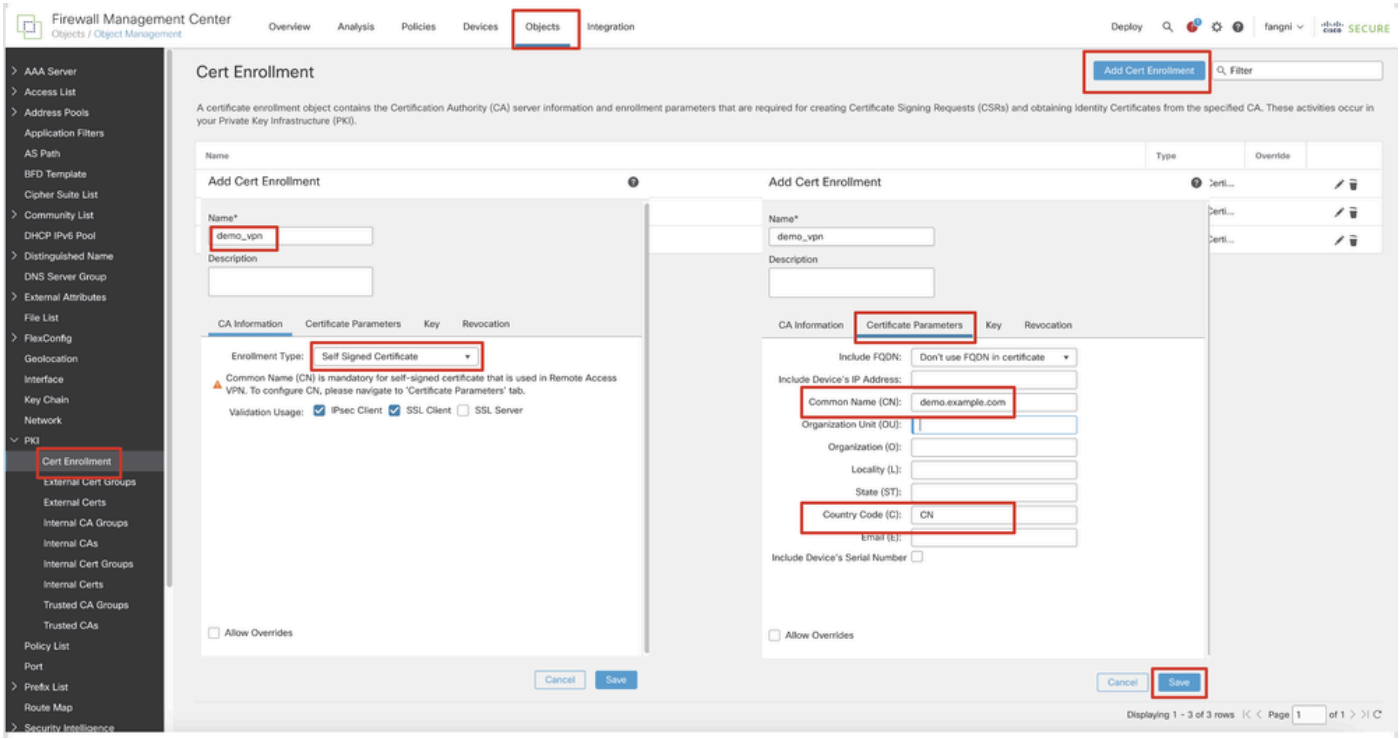
FMC_Add_New_Radius_Server_Group_Part_2

Paso 8. Desplácese hasta Objects > Object Management > Address Pools > IPv4 Pools. Haga clic en Add IPv4 Pools y proporcione el **Name, IPv4 Address Range**y Mask. A continuación, haga clic en Save.



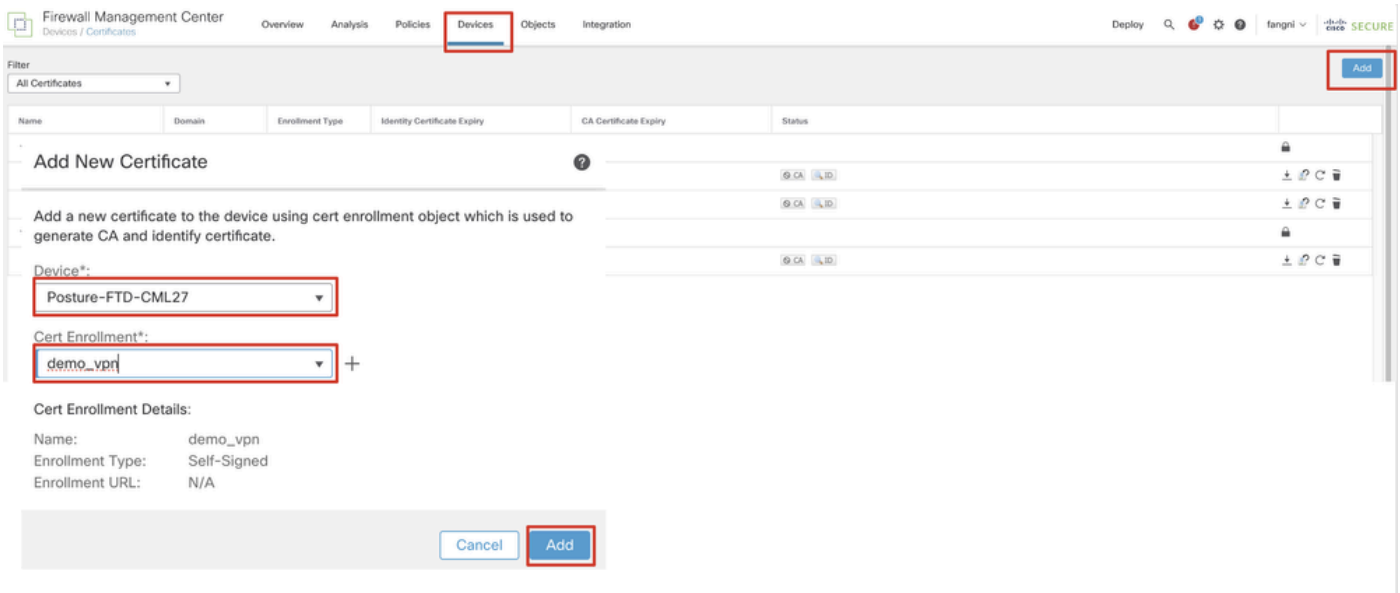
FMC_Add_New_Pool

Paso 9. Desplácese hasta Certificate Objects > Object Management > PKI > Cert Enrollment. Haga clic en Add Cert Enrollment, proporcione un nombre y seleccione Self Signed Certificateen Enrollment Type. Haga clic en la Certificate Parameters ficha y proporcione Common Name y Country Code. A continuación, haga clic en Save.



FMC_Add_New_Cert_Enroll

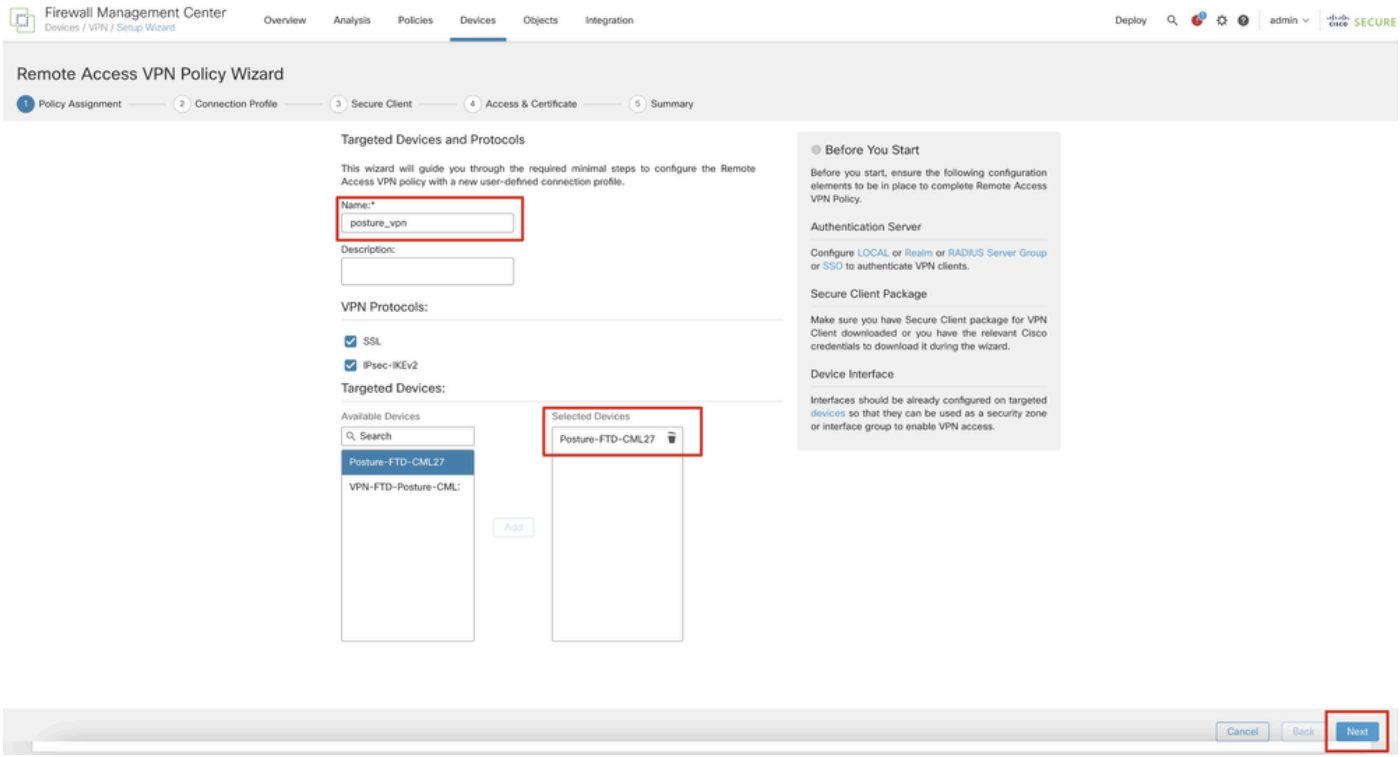
Paso 10. Desplácese hasta Devices > Certificates. Haga clic en Add, seleccione el nombre de FTD en Device, seleccione la inscripción configurada anterior en Cert Enrollment. Haga clic en Add.



FMC_Add_New_Cert_To_FTD

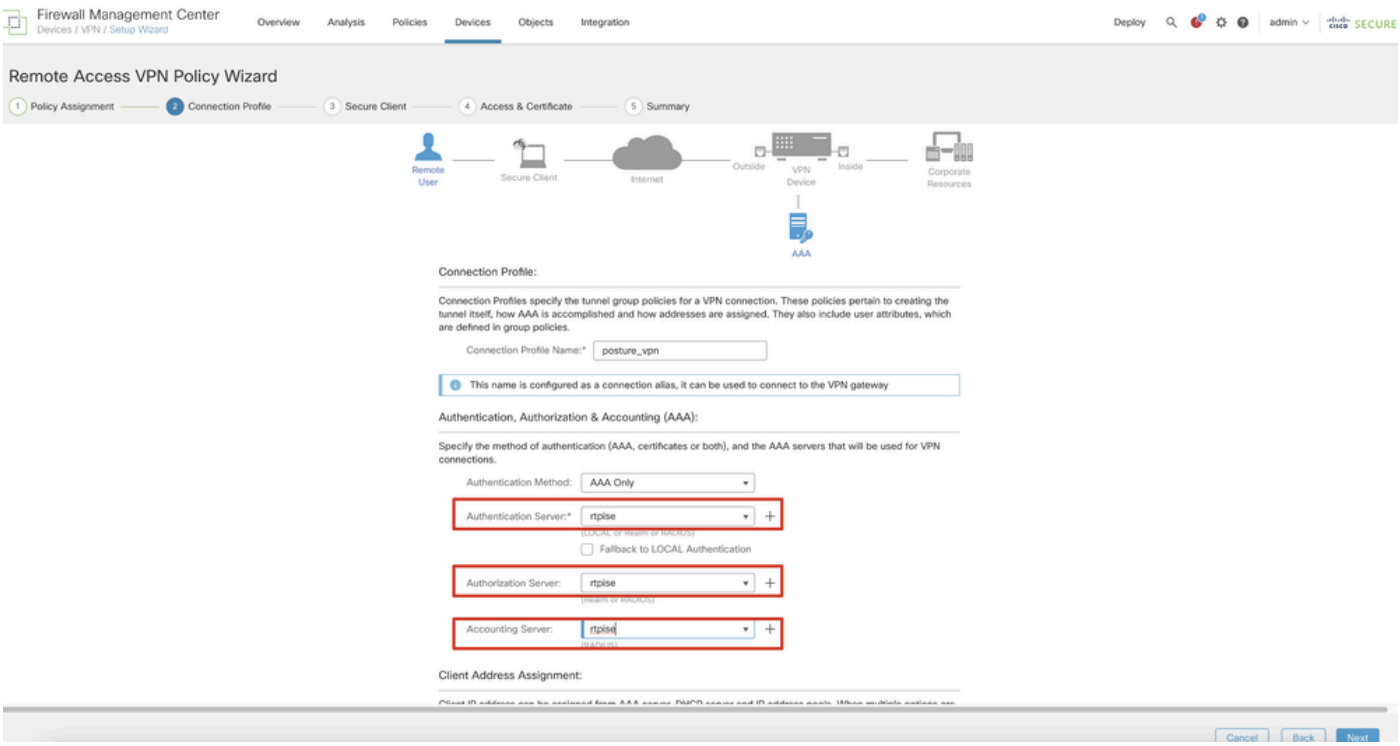
Paso 11. Desplácese hasta Devices > VPN > Remote Access. Haga clic en Add.

Paso 11.1. Proporcione el nombre y añada el FTD a Selected Devices. Haga clic en Next.



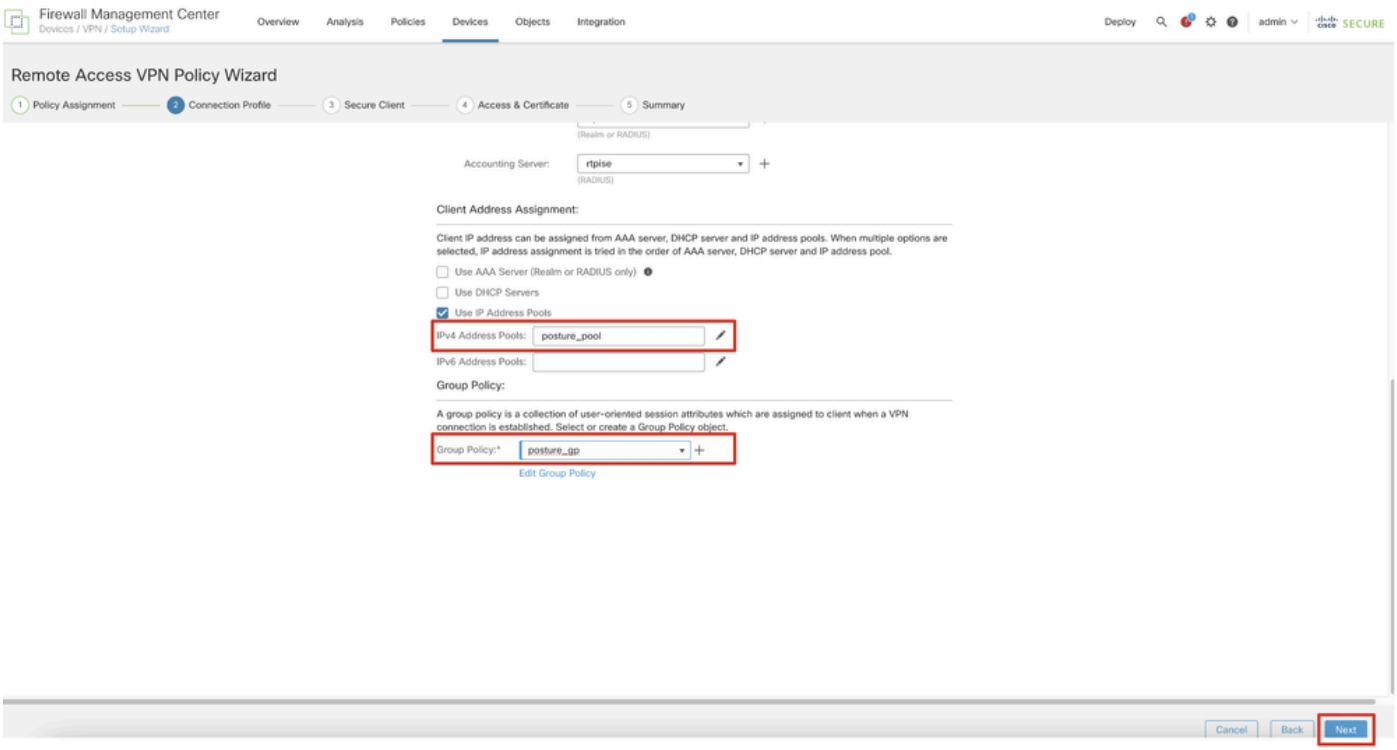
FMC_New_RAVPN_Wizard_1

Paso 11.2. Seleccione el grupo de servidores RADIUS configurado anteriormente en la Authentication Server, Authorization Server, Accounting Server. Desplácese hacia abajo en la página.



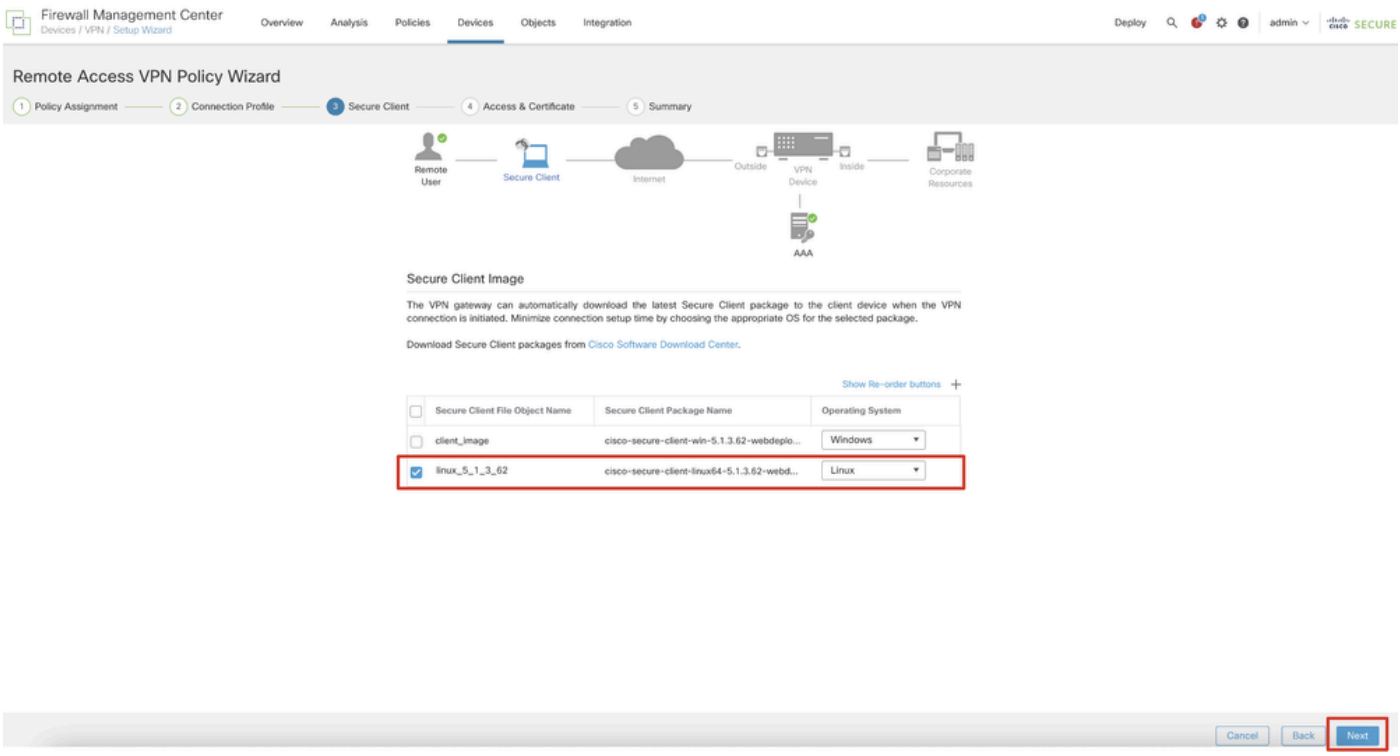
FMC_New_RAVPN_Wizard_2

Paso 11.3. Seleccione el nombre de conjunto configurado anteriormente en IPv4 Address Pools. Seleccione la política de grupo configurada anteriormente en Group Policy. Haga clic en Next.



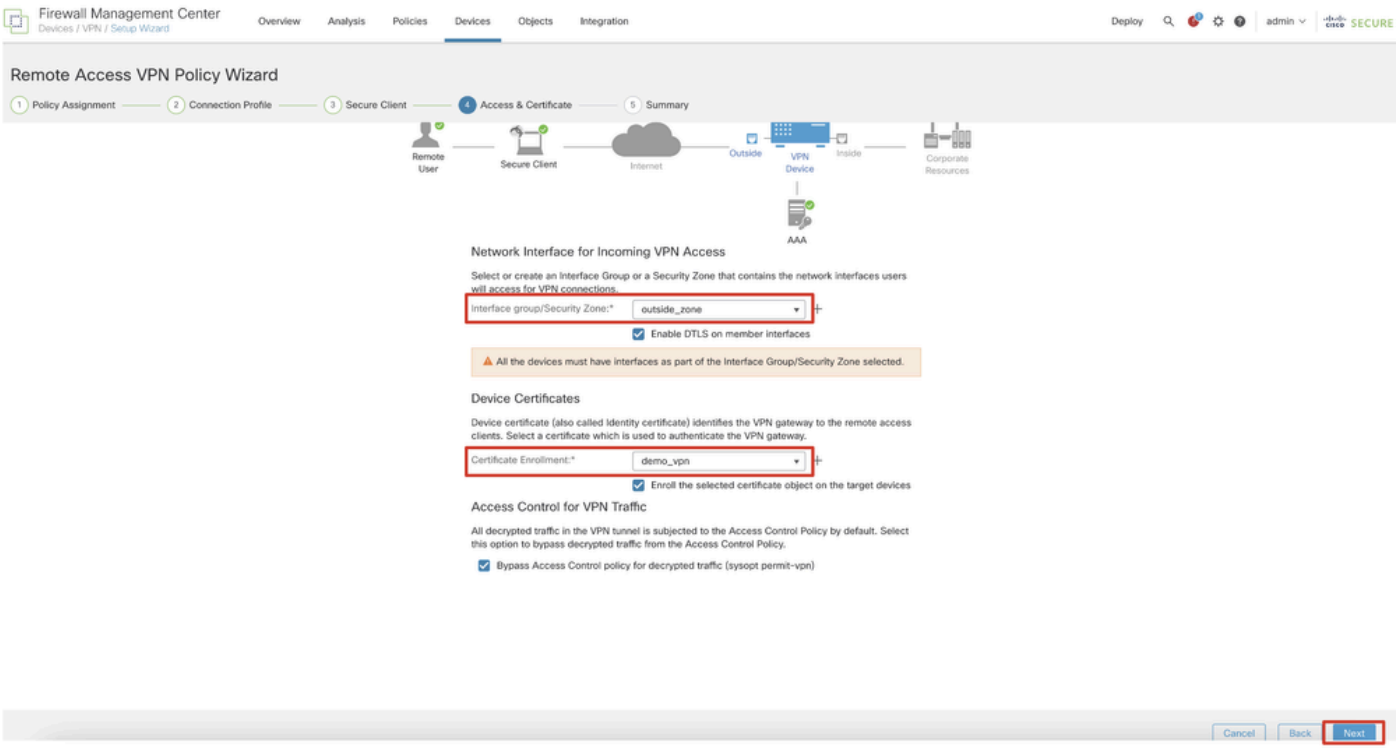
FMC_New_RAVPN_Wizard_3

Paso 11.4. Marque la casilla de la imagen de Linux. Haga clic en Next.



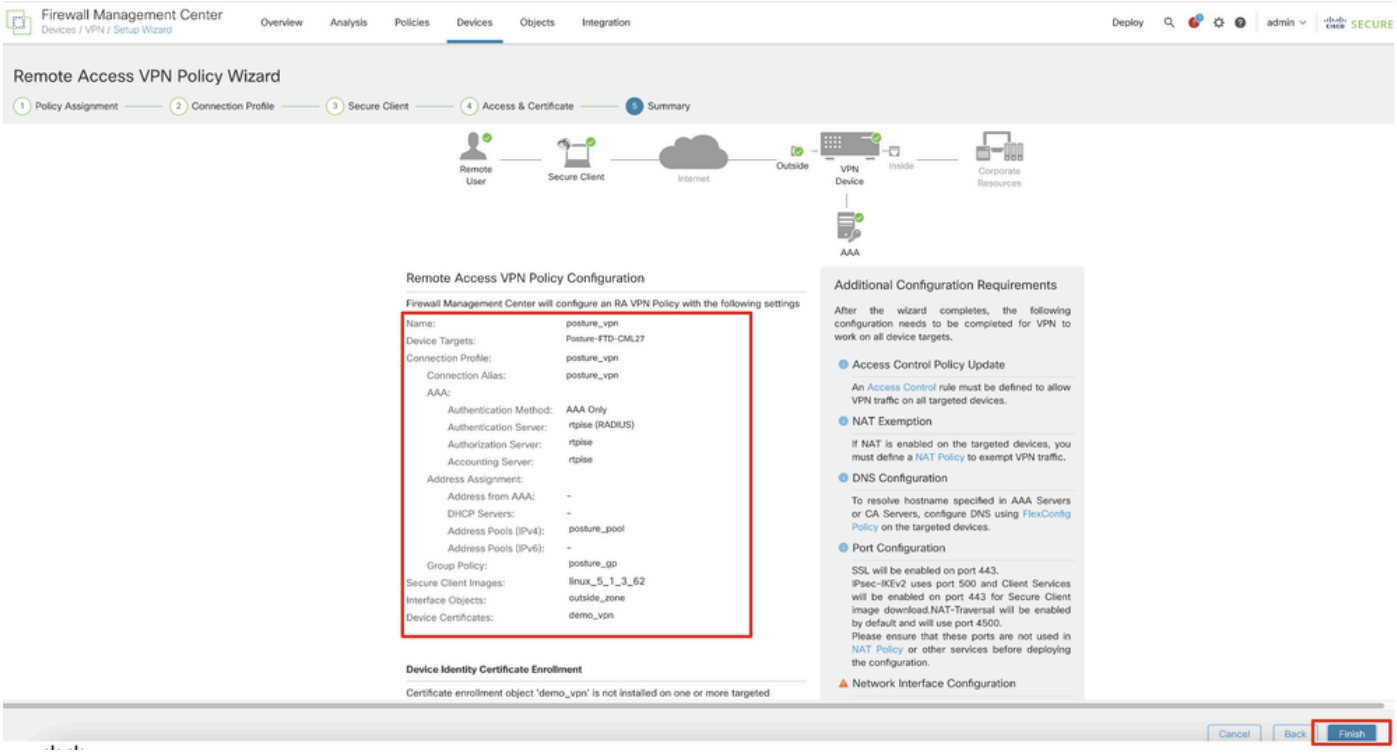
FMC_New_RAVPN_Wizard_4

Paso 11.5. Seleccione la interfaz de la interfaz VPN. Seleccione la inscripción de certificados que se inscribió en el FTD en el paso 9. Haga clic en Next.



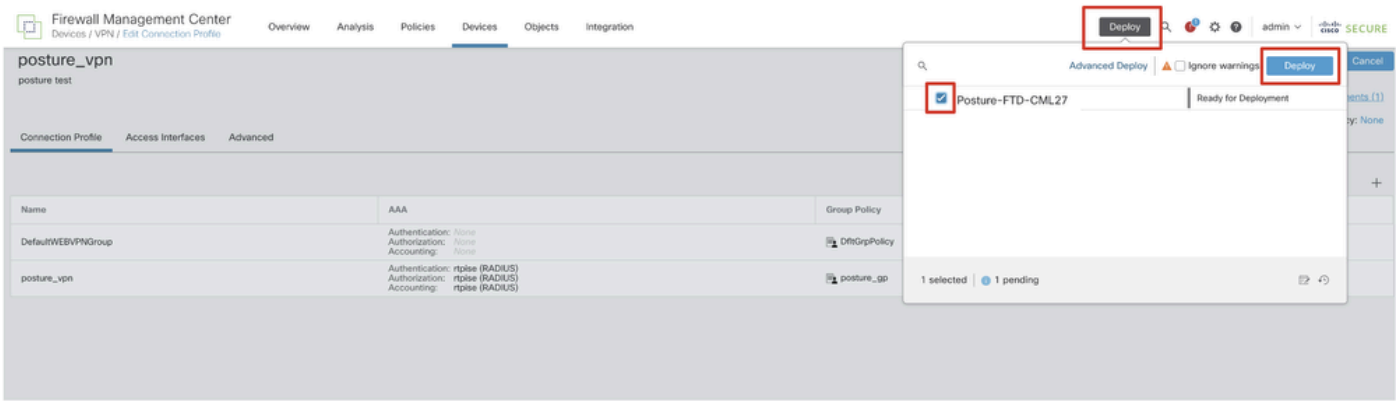
FMC_New_RAVPN_Wizard_5

Paso 11.6. Confirme la información relacionada en la página de resumen. Si todo está bien, haga clic en Finish. Si necesita modificar algo, haga clic en Back.



FMC_New_RAVPN_Wizard_6

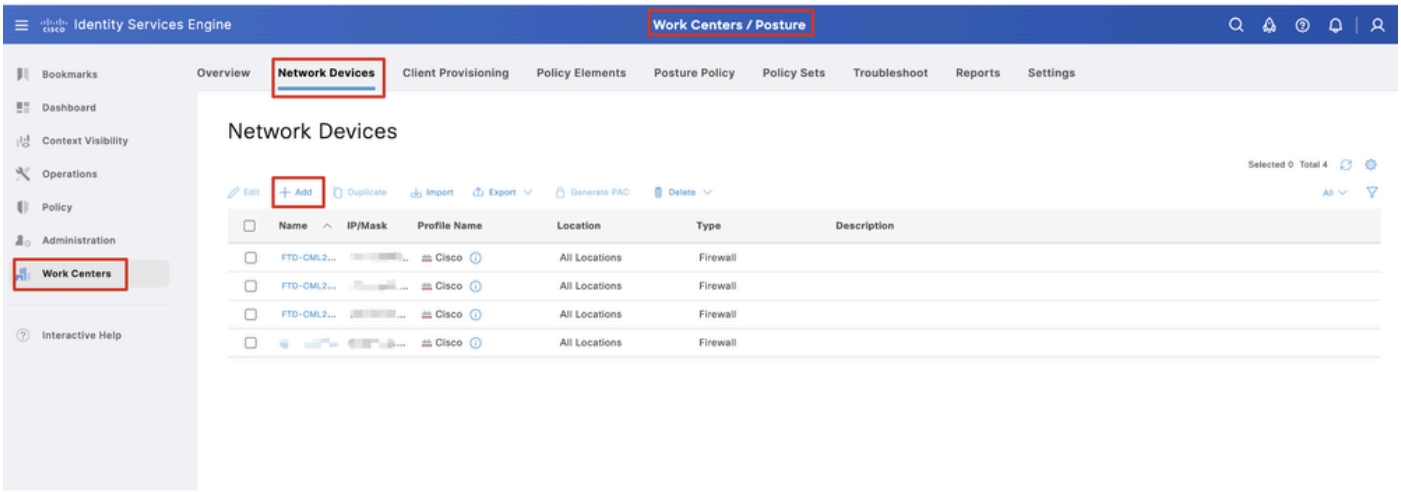
Paso 12. Implemente la nueva configuración en FTD para completar la configuración de VPN de acceso remoto.



FMC_Deploy_FTD

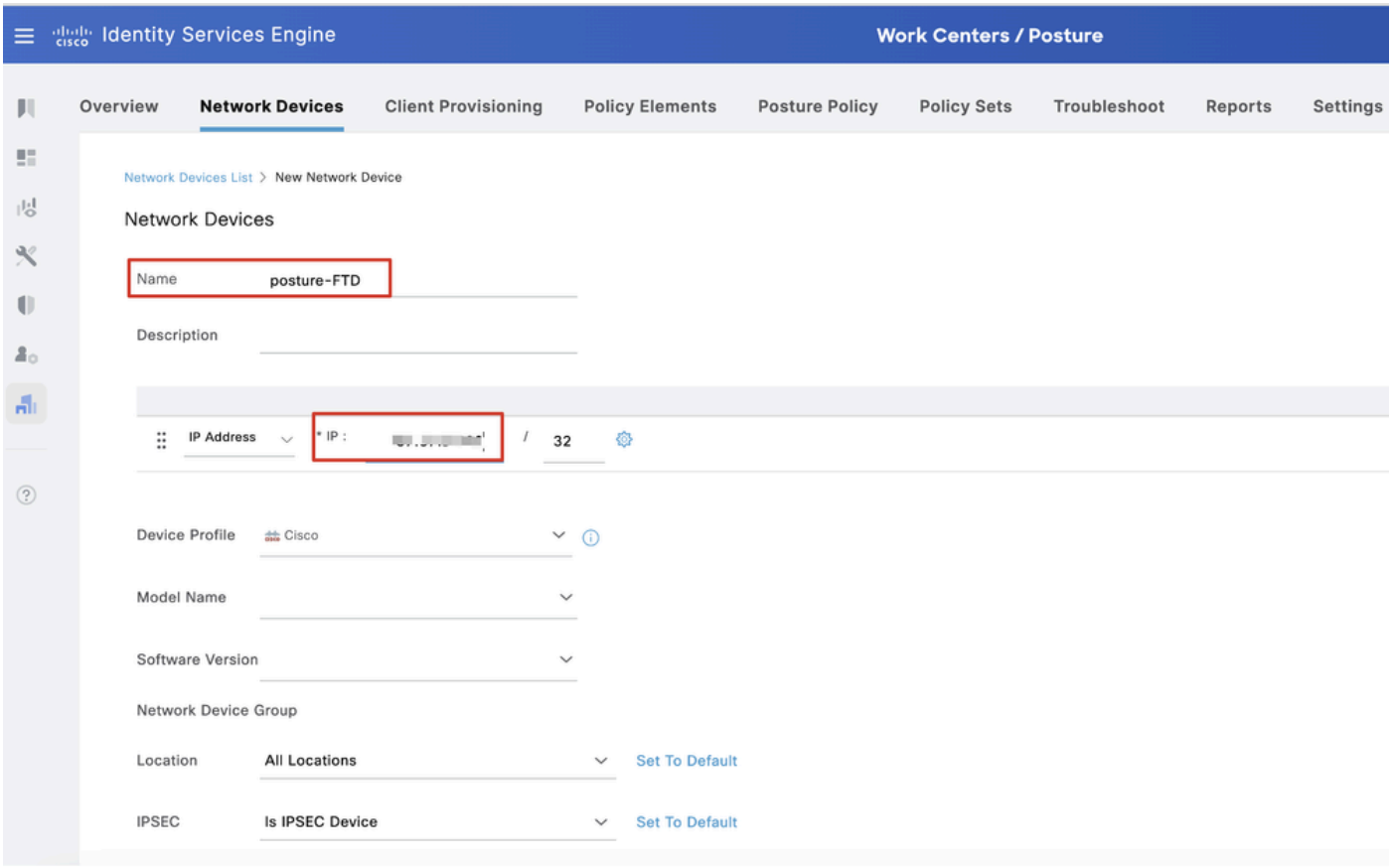
Configuraciones en ISE

Paso 13. Desplácese hasta Work Centers > Posture > Network Devices. Haga clic en Add.



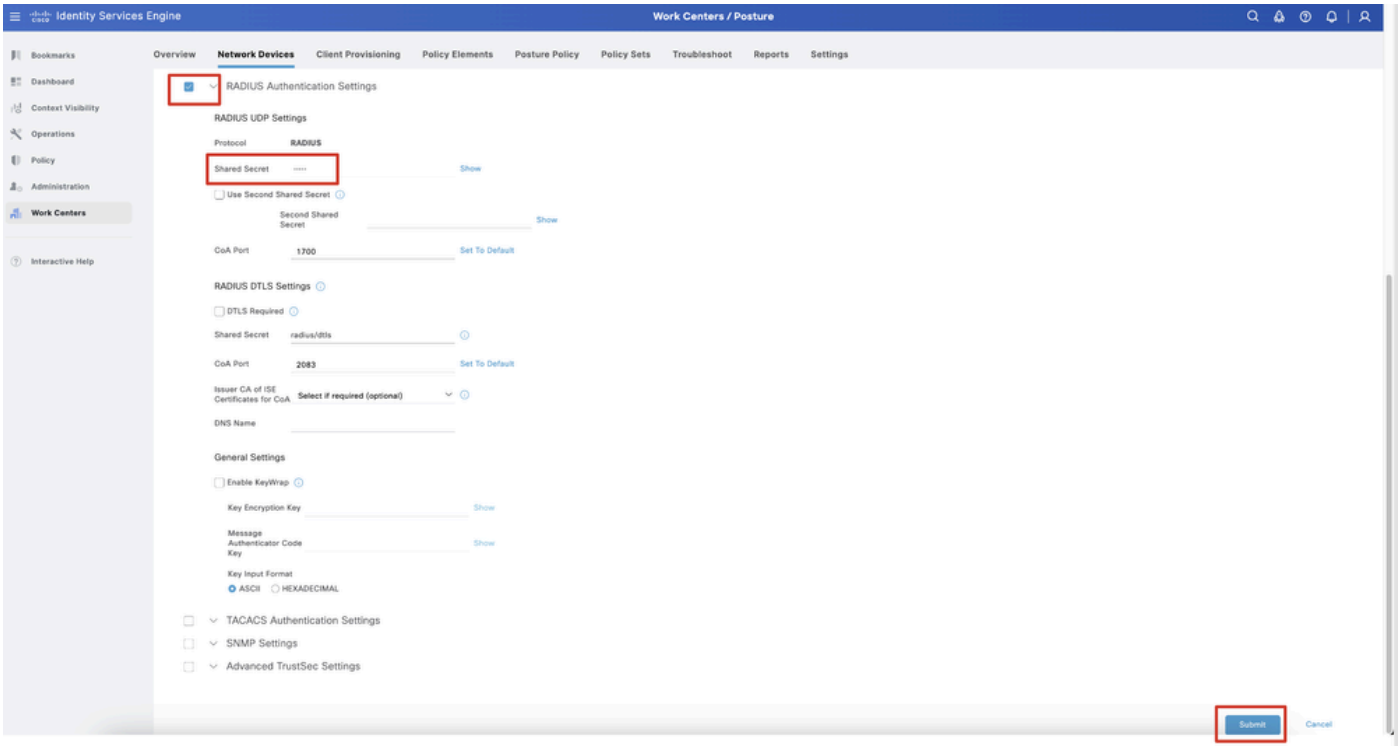
ISE_Add_New_Devices

Paso 13.1. Proporcione el Name, IP Addressy desplácese hacia abajo por la página.



ISE_Add_New_Devices_1

Paso 13.2. Marque la casilla de verificación de RADIUS Authentication Settings. Proporcione el Shared Secret. Haga clic en Submit.

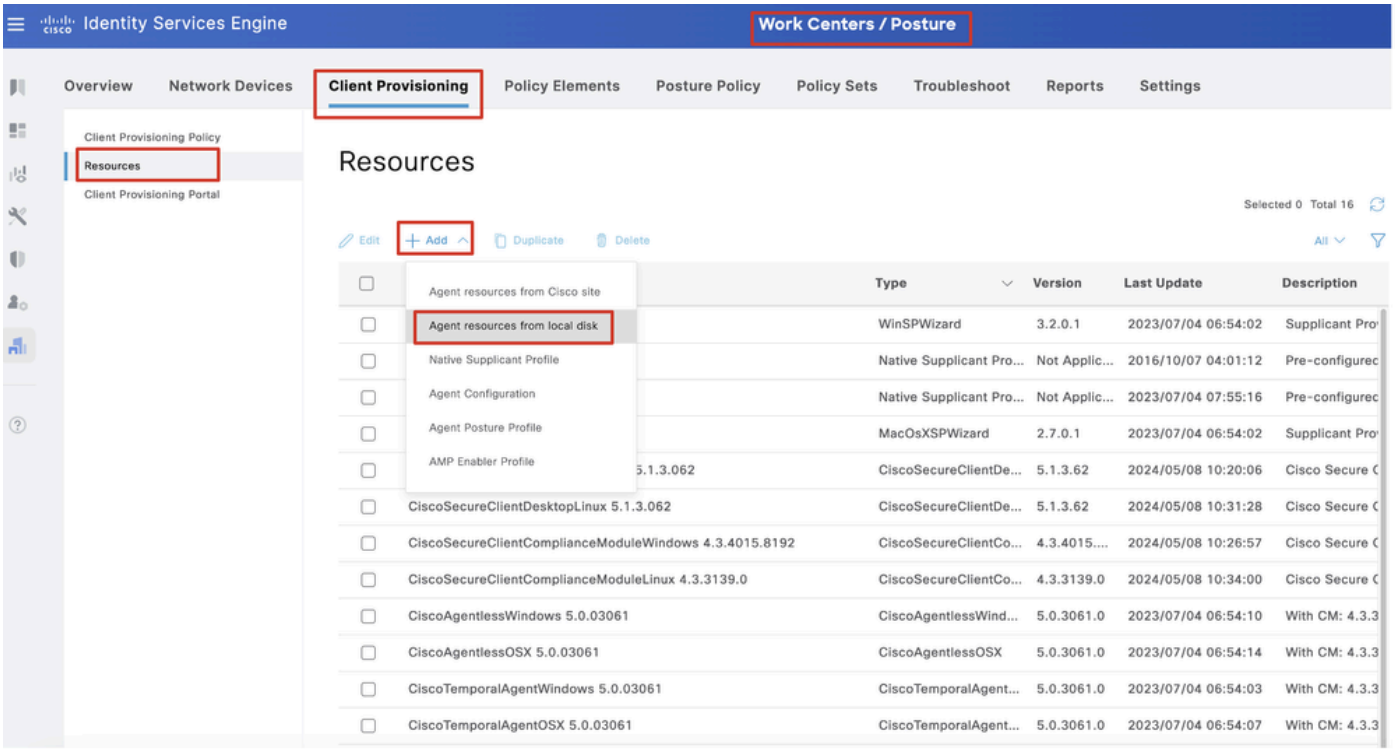


ISE_Add_New_Devices_2

Paso 14. Descargue el nombre del paquete cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg de Descarga de Software de Cisco y asegúrese de que el archivo sea bueno confirmando que la suma de comprobación md5 del archivo descargado es la misma que la página

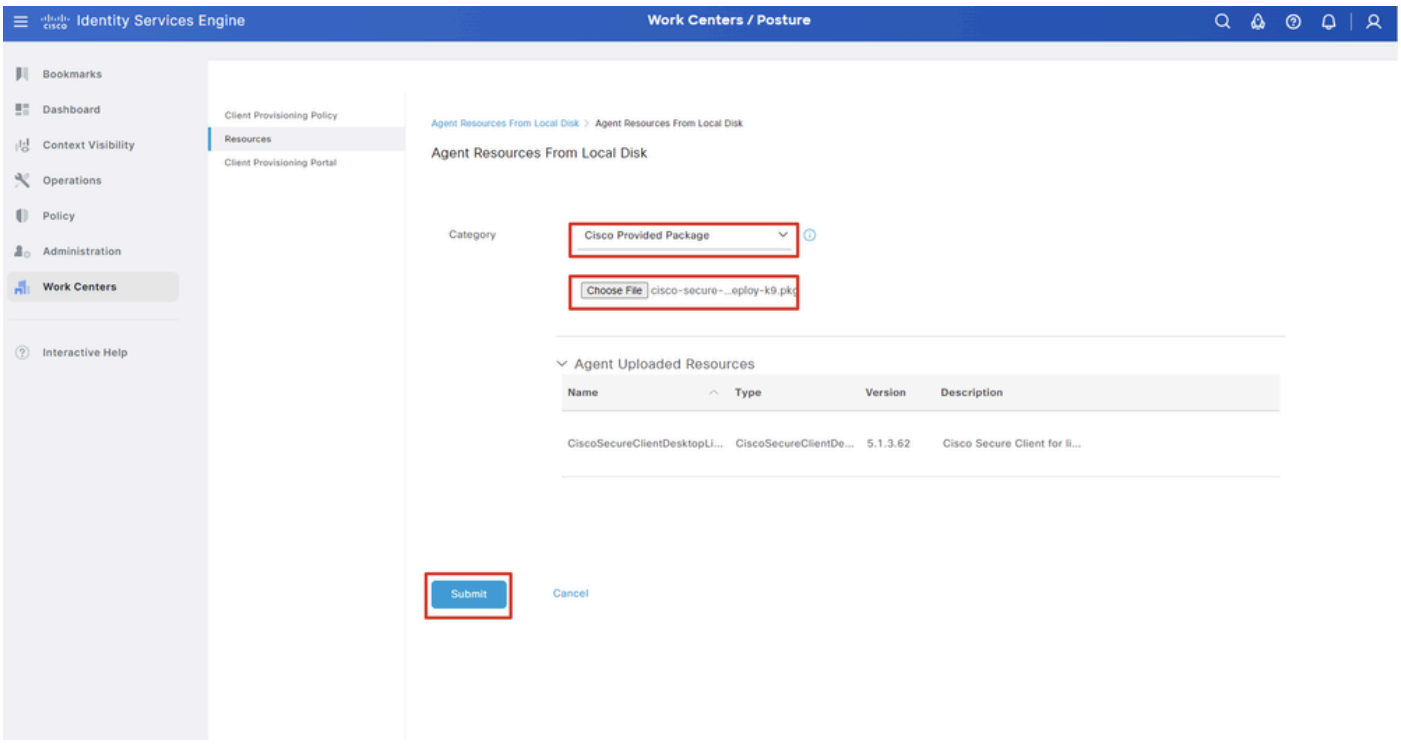
de Descarga de Software de Cisco. El nombre del paquete cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg se ha descargado correctamente en el paso 1.

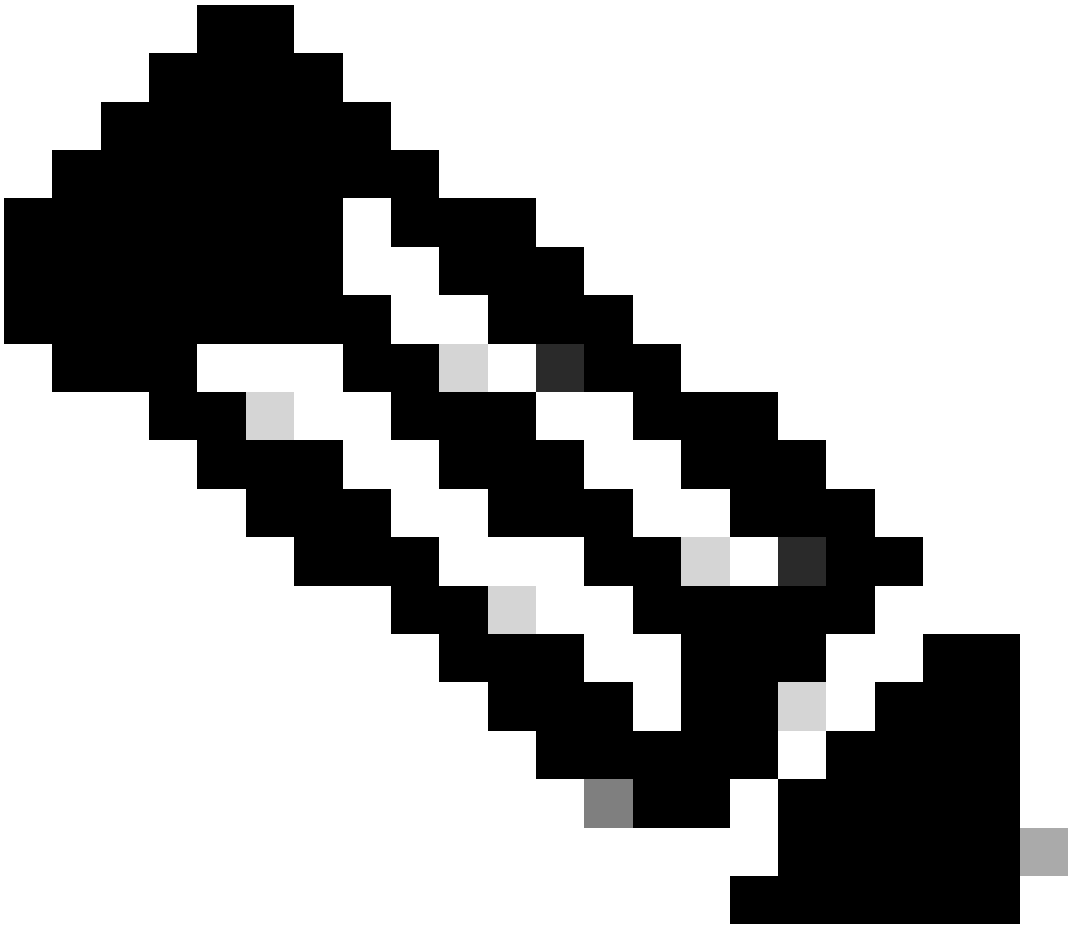
Paso 15. Desplácese hasta Work Centers > Posture > Client Provisioning > Resources. Haga clic en Add. Seleccione Agent resources from local disk.



ISE_Upload_Resource

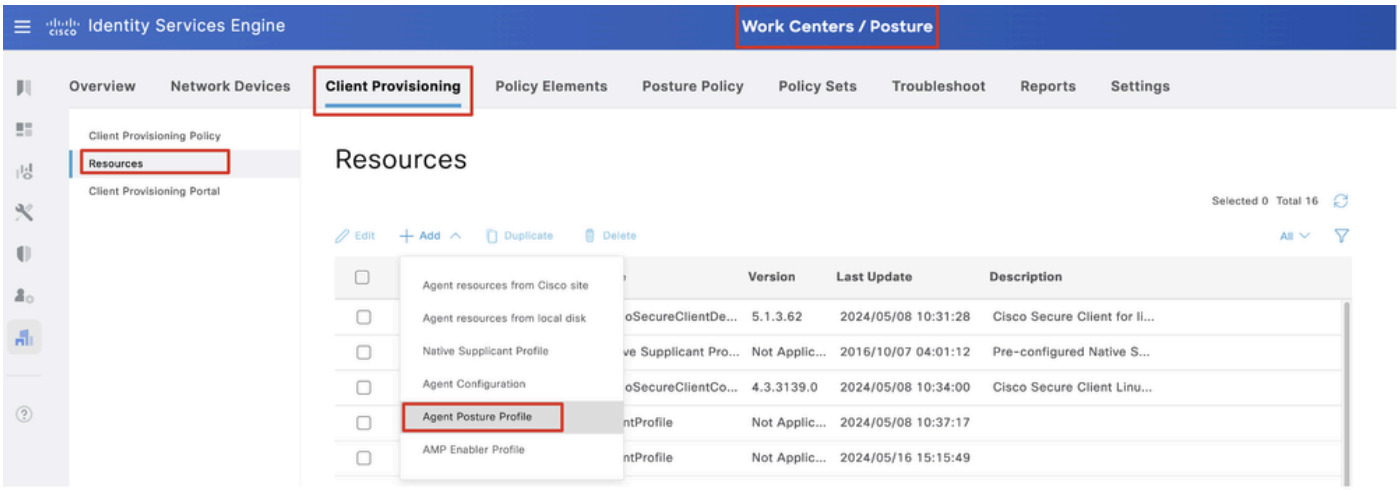
Paso 15.1. Seleccione Cisco Provided Package. Haga clic Choose File para cargar cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Haga clic en Submit.





Nota: Repita el paso 14 para cargar cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg .

Paso 16. Desplácese hasta Work Centers > Posture > Client Provisioning > Resources. Haga clic en Add. Seleccione Agent Posture Profile.

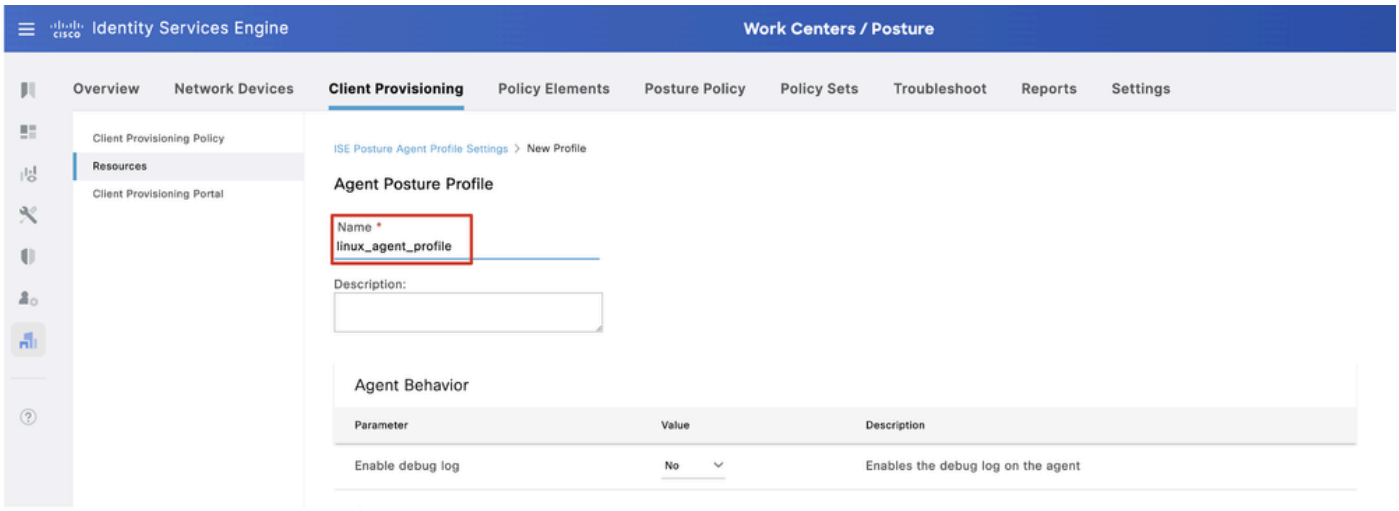


ISE_Add_Agent_Posture_Profile

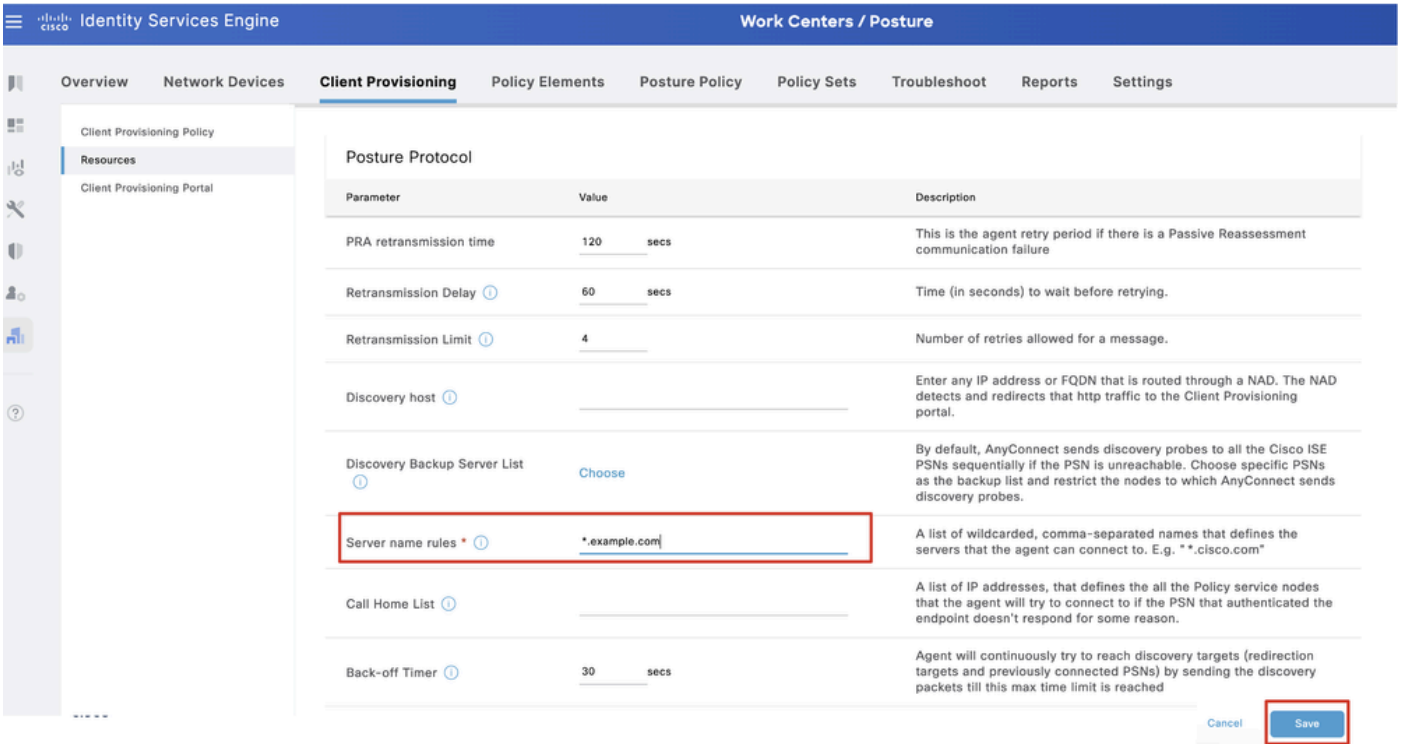
Paso 16.1. Proporcione el Name, Server name rules y mantenga el resto como predeterminado. Haga clic en Save.

Nombre: linux_agent_profile

Reglas de nombre de servidor: *.example.com

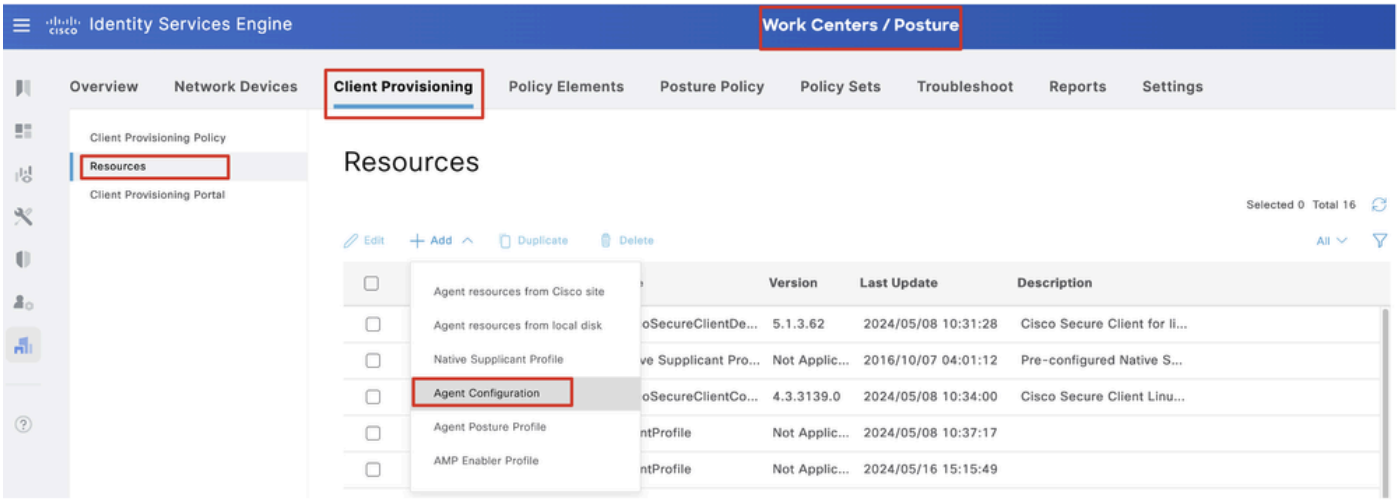


ISE_Add_Agent_Posture_Profile_1



ISE_Add_Agent_Posture_Profile_2

Paso 17. Desplácese hasta Work Centers > Posture > Client Provisioning > Resources. Haga clic en Add. Seleccione Agent Configuration.



ISE_Add_Agent_Configuration

Paso 17.2. Configure los detalles:

Seleccionar paquete de agente: CiscoSecureClientDesktopLinux 5.1.3.062

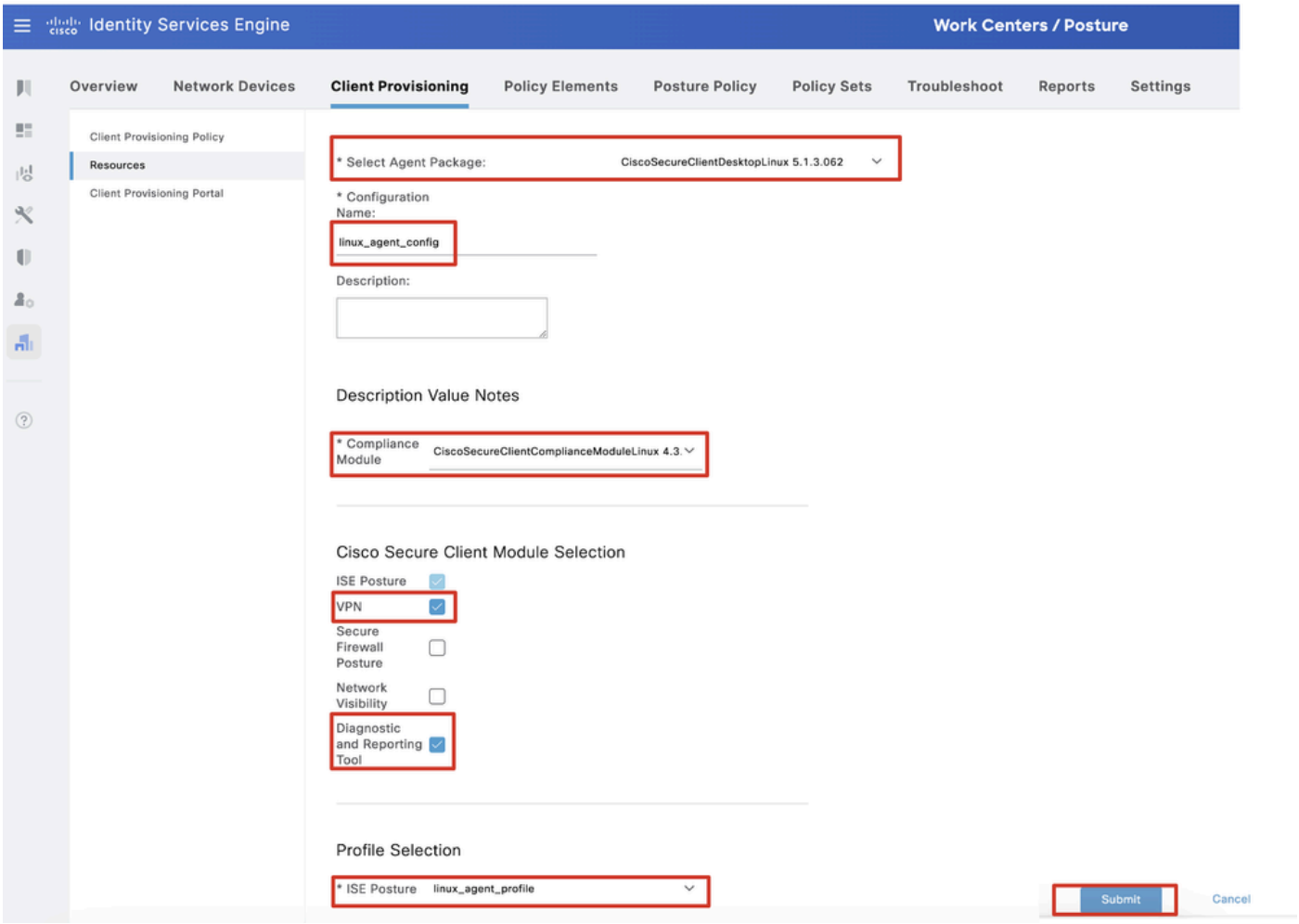
Nombre: linux_agent_config

Módulo de cumplimiento: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Marque la casilla de verificación de VPN, Diagnostic and Reporting Tool

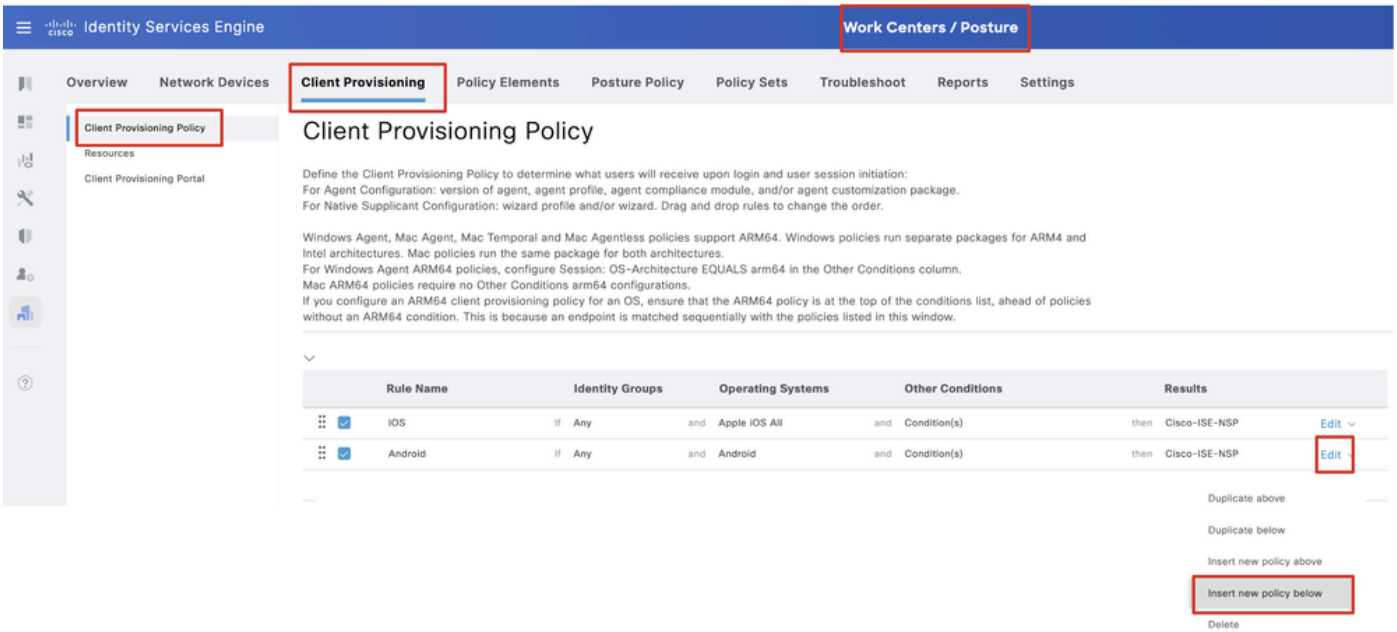
Posición de ISE para la selección de perfiles: linux_agent_profile

Haga clic en Submit.



ISE_Add_Agent_Configuration_1

Paso 18. Desplácese hasta Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Haga clic Edit al final de cualquier nombre de regla. Seleccione Insert new policy below.



ISE_Add_New_Provisioning_Policy

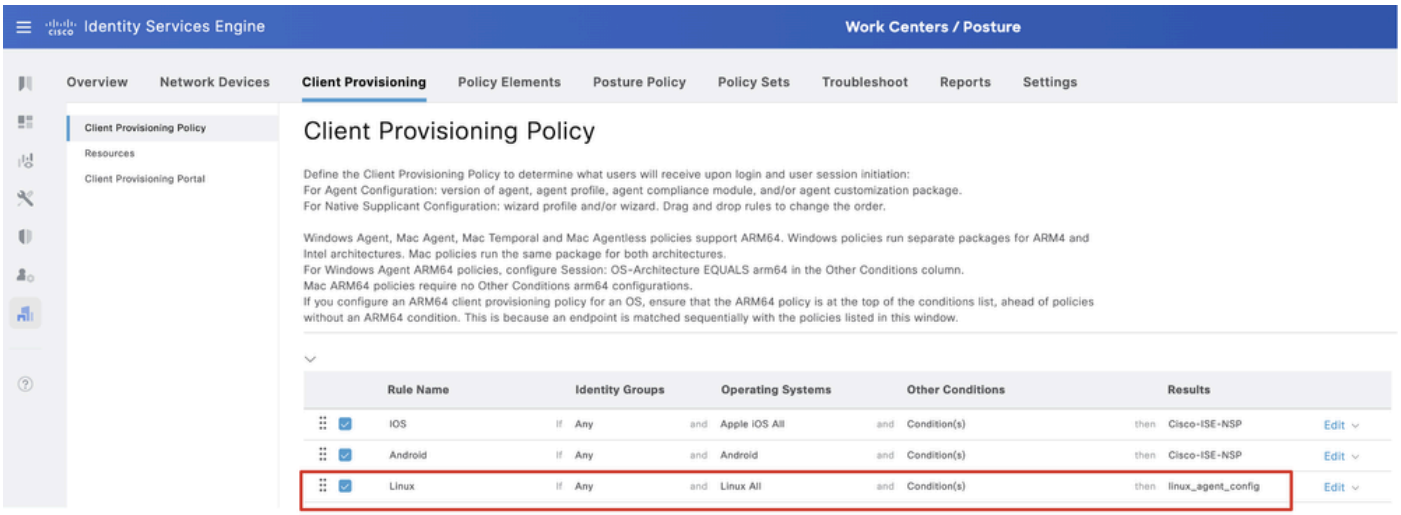
Paso 18.1. Configure los detalles:

Nombre de regla: Linux

Sistemas operativos: Linux All

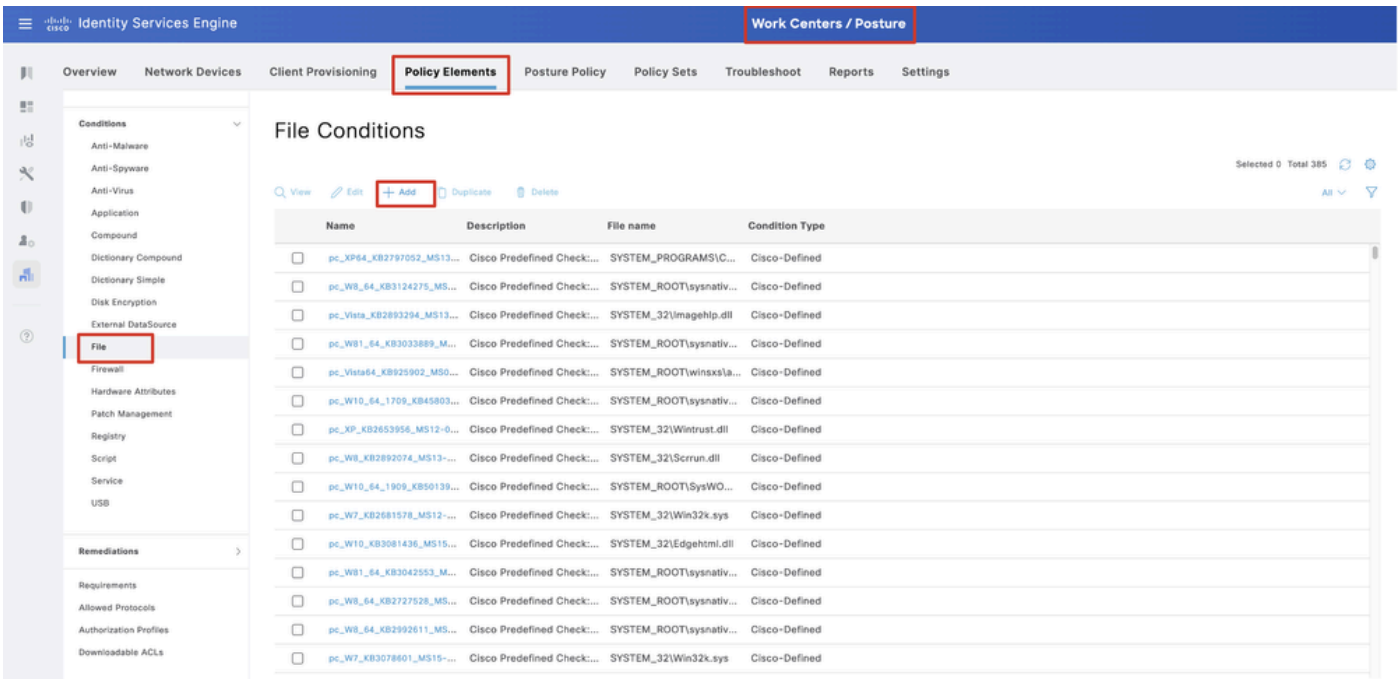
Resultados: linux_agent_config

Haga clic en Done y Save.



ISE_Add_New_Provisioning_Policy_1

Paso 19. Desplácese hasta Work Centers > Posture > Policy Elements > Conditions > File. Haga clic en Add.



ISE_Add_New_File_Condition

Paso 19.1. Configure los detalles:

Nombre: linux_demo_file_exist

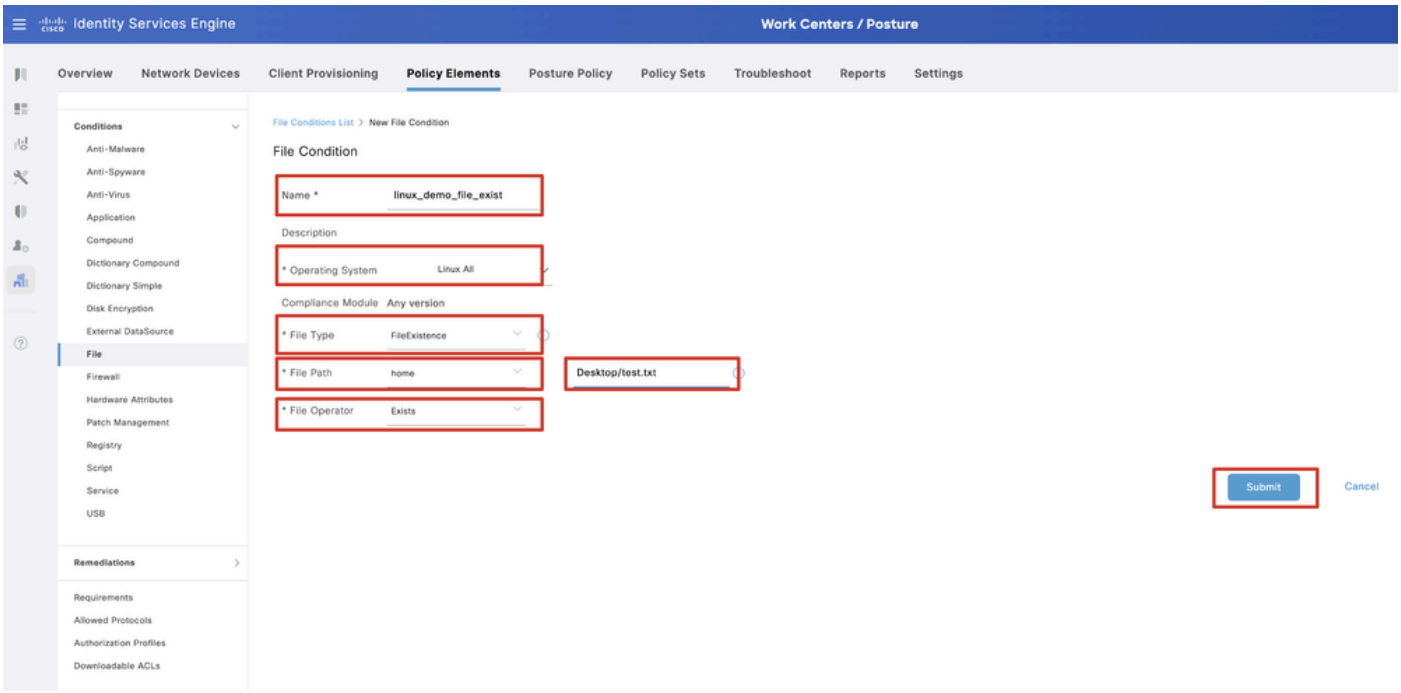
Sistemas operativos: Linux All

Tipo de archivo: FileExistence

Ruta del archivo: inicio, Desktop/test.txt

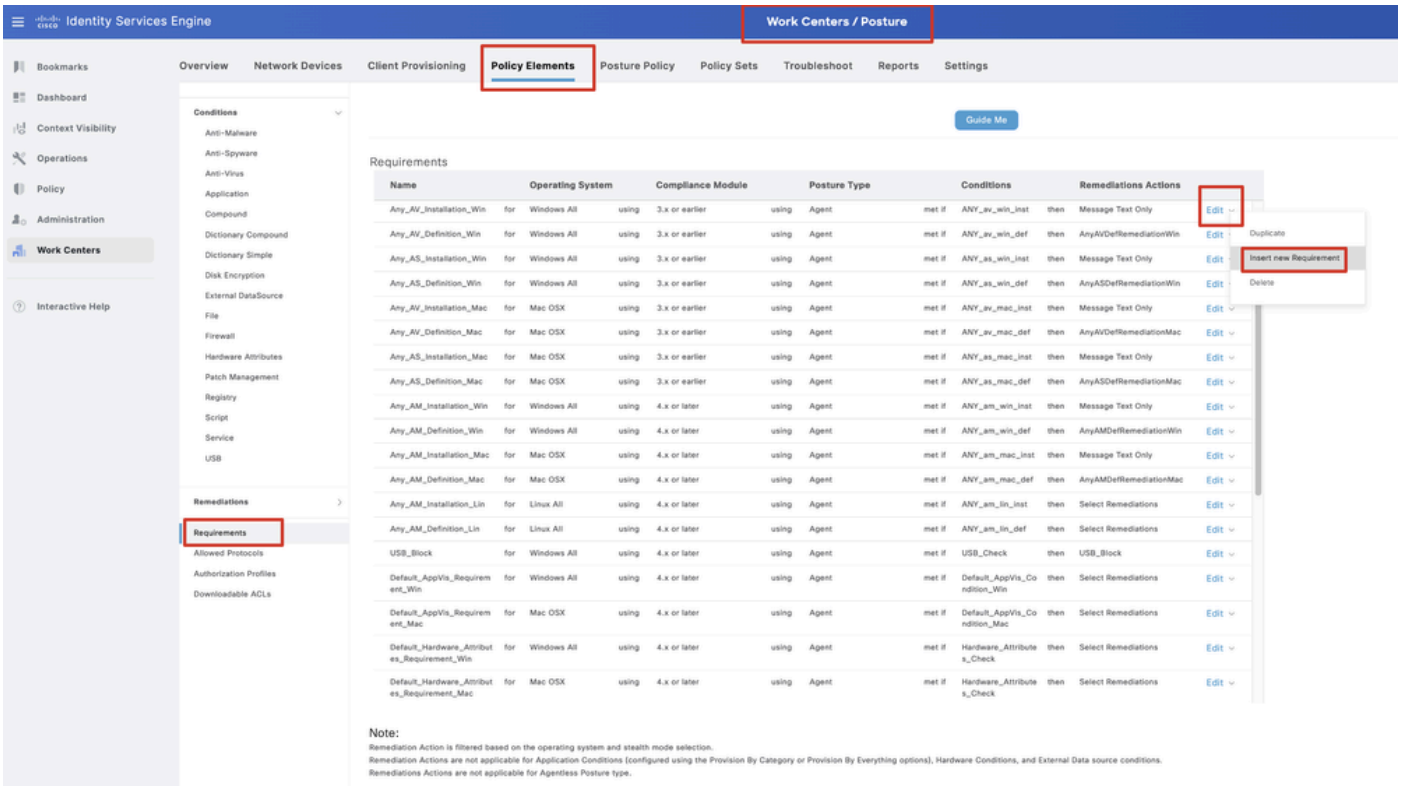
Operador de archivos: existe

Haga clic en Submit.



ISE_Add_New_File_Condition_1

Paso 20. Desplácese hasta Work Centers > Posture > Policy Elements > Requirements. Haga clic Edit al final de cualquier nombre de regla. Seleccione Insert new Requirement.



ISE_Add_New_Posture_Requirement

Paso 20.1. Configure los detalles:

Nombre: Test_exist_linux

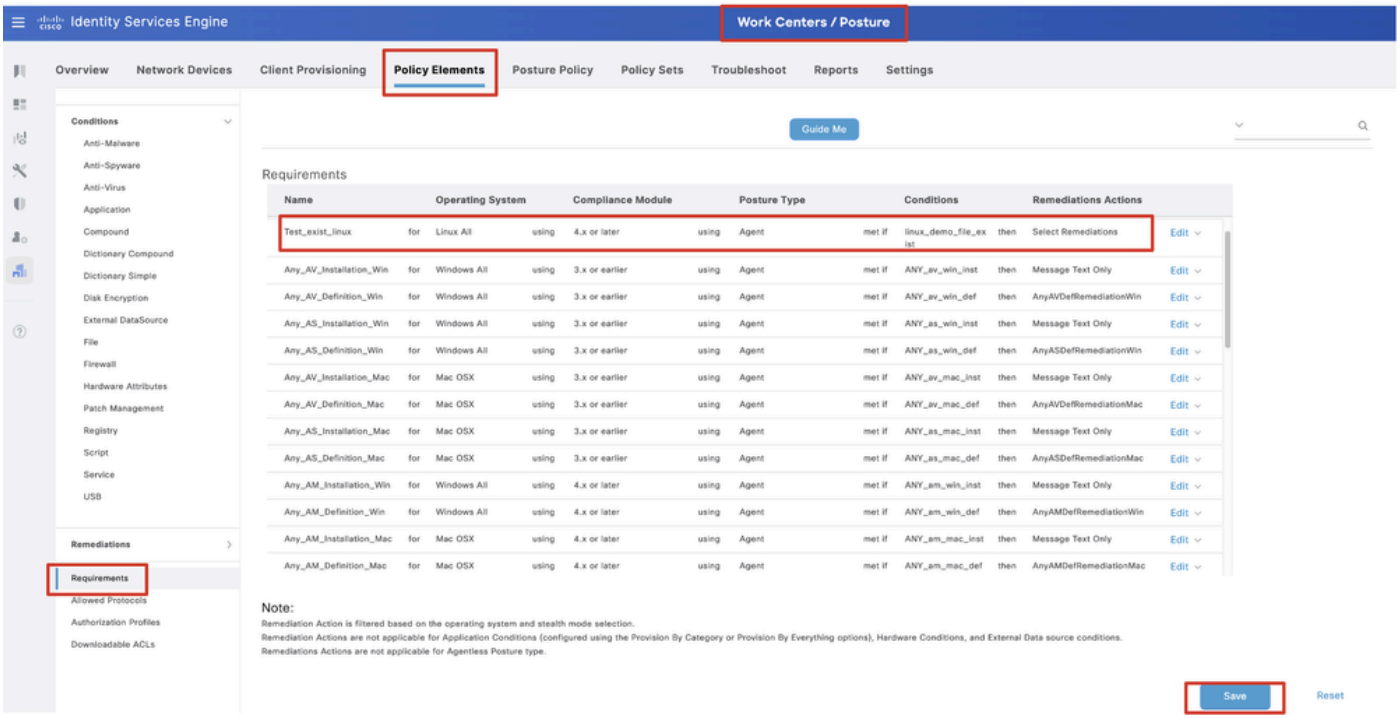
Sistemas operativos: Linux All

Módulo de cumplimiento: 4.x o posterior

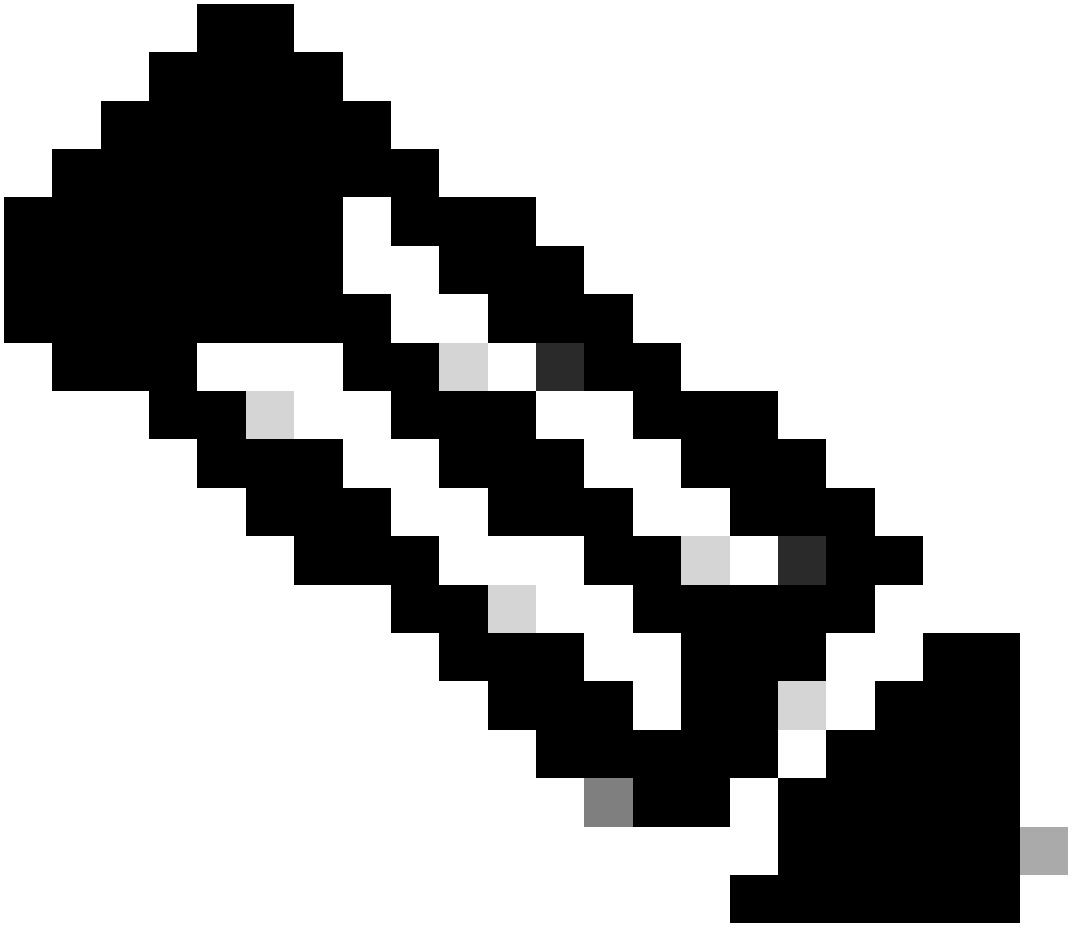
Tipo de postura: Agente

Condiciones: linux_demo_file_exist

Haga clic en Done y Save.



ISE_Add_New_Posture_Requirement_1



Nota: A partir de ahora, sólo se admiten scripts de shell para los agentes Linux como solución.

Paso 21. Desplácese hasta Work Centers > Posture > Policy Elements > Authorization Profiles. Haga clic en Add.

Paso 21.1. Configure los detalles:

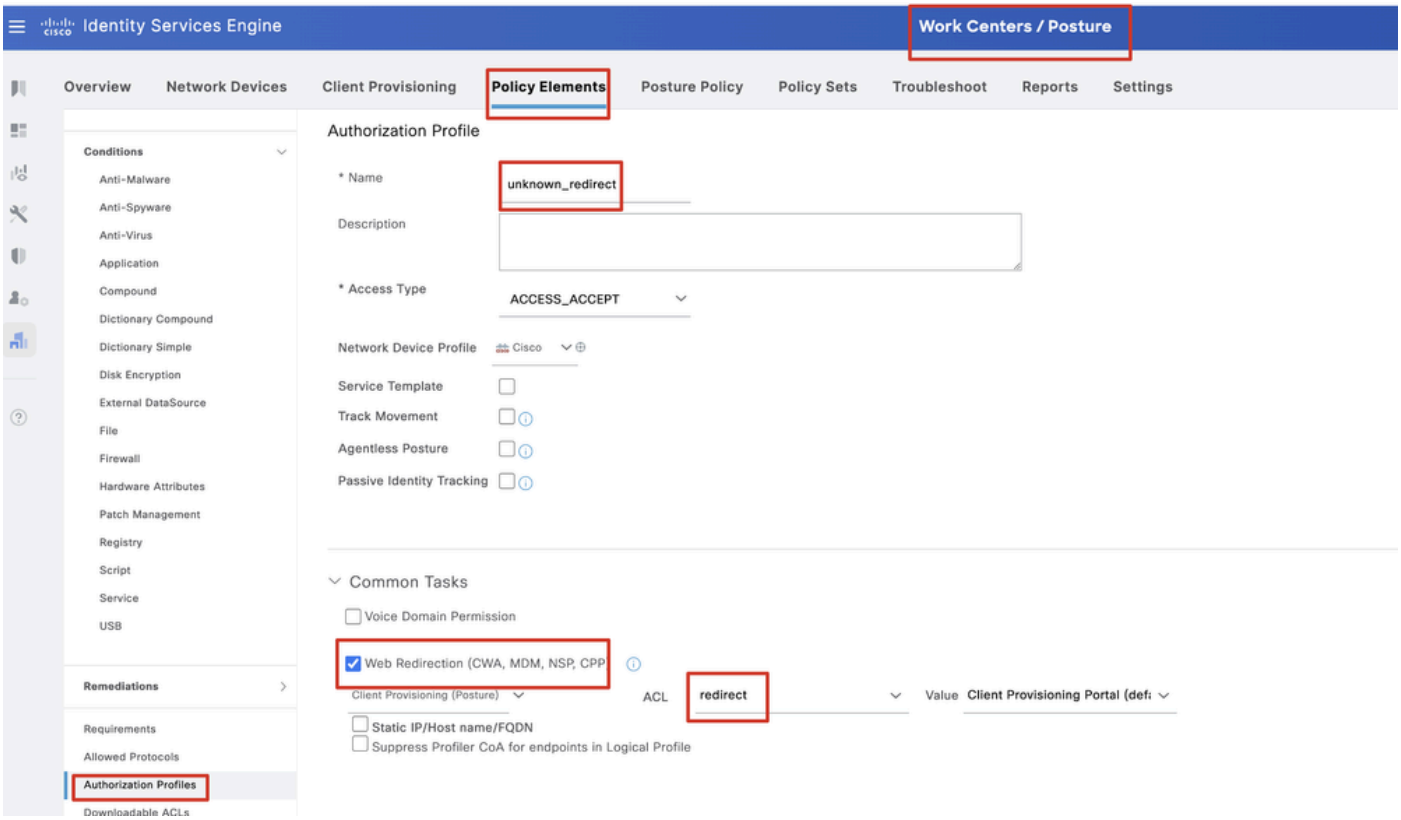
Nombre: unknown_redirect

Marque la casilla de verificación de Web Redirection(CWA,MDM,NSP,CPP)

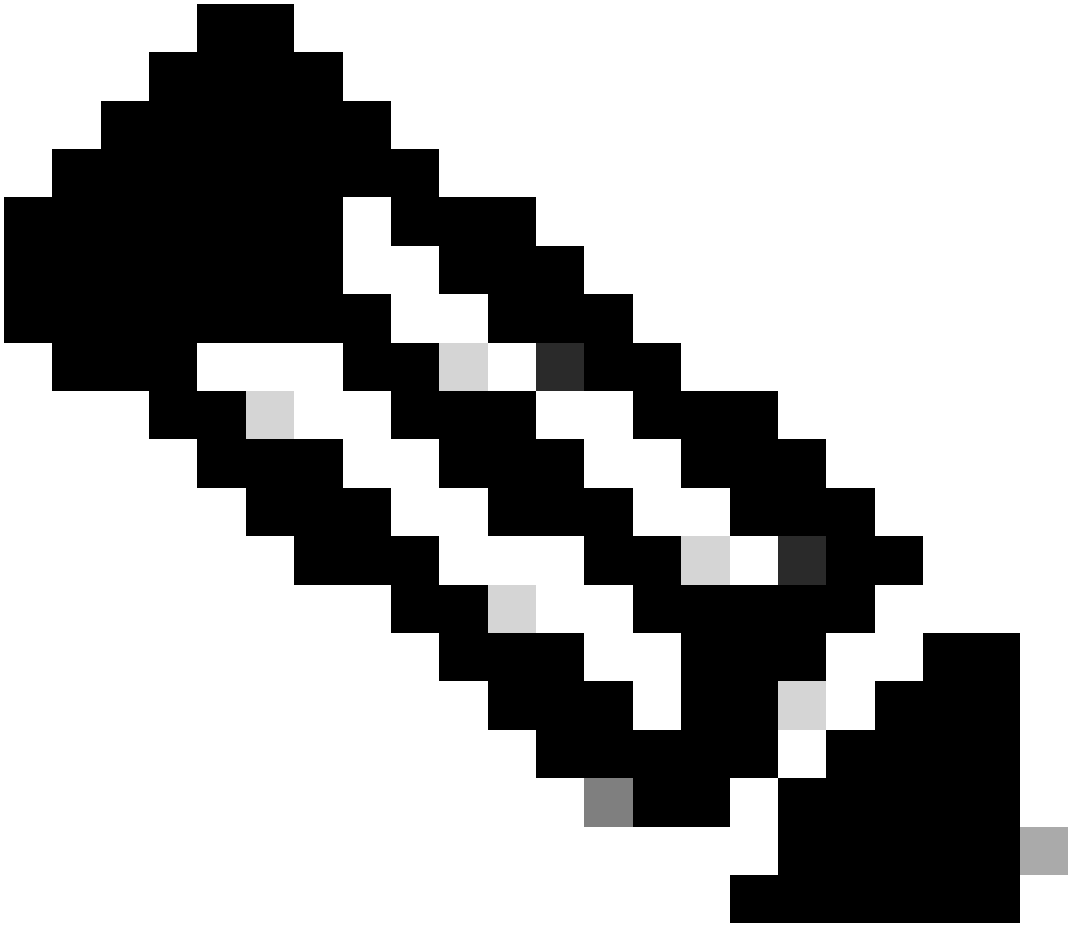
Seleccionar Client Provisioning(Posture)

ACL: redirección

Valor: Client Provisioning Portal (predeterminado)



ISE_Add_New_Authorization_Profile_Redirect_1



Nota: Esta redirección de nombre de ACL debe coincidir con el nombre de ACL correspondiente configurado en FTD.

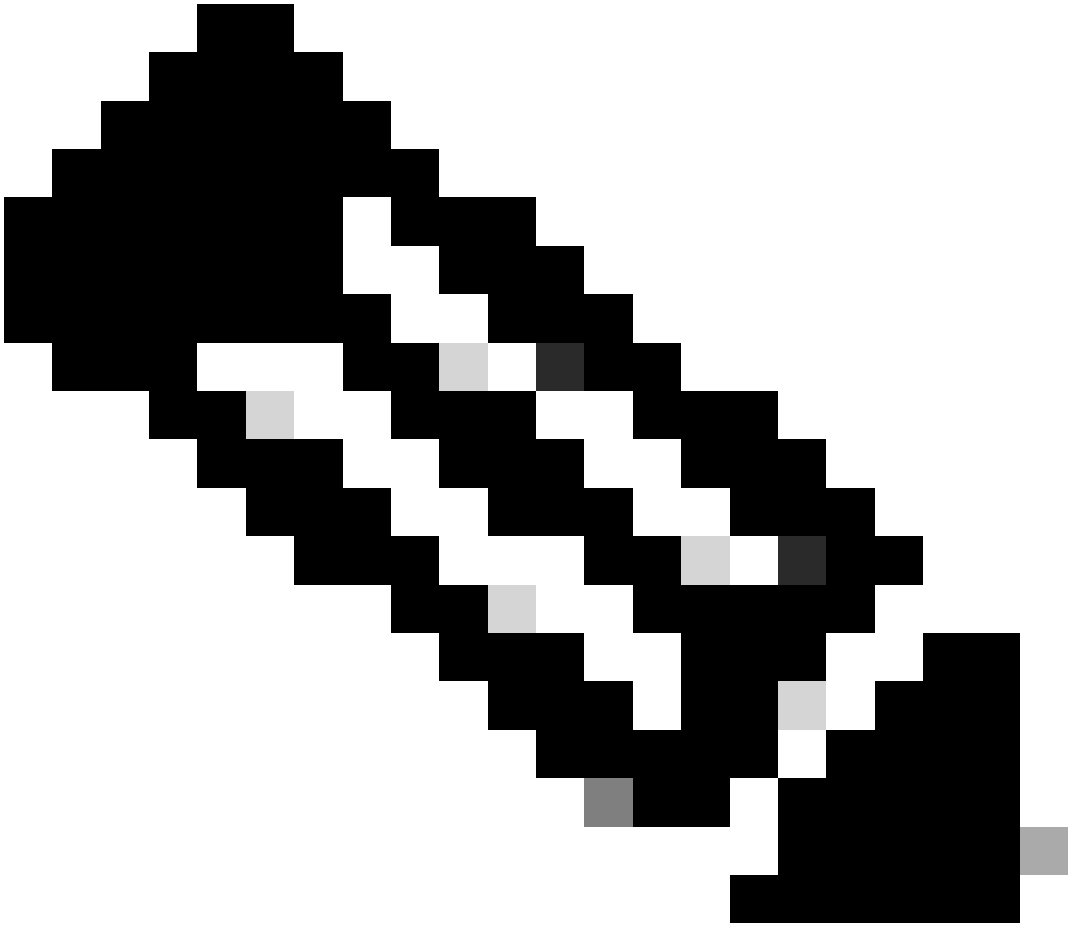
Paso 21.2. Repita el Add para crear otros dos perfiles de autorización para terminales no conformes y conformes con los detalles.

Nombre: non_compliance_profile

Nombre de DACL: DENY_ALL_IPv4_TRAFFIC

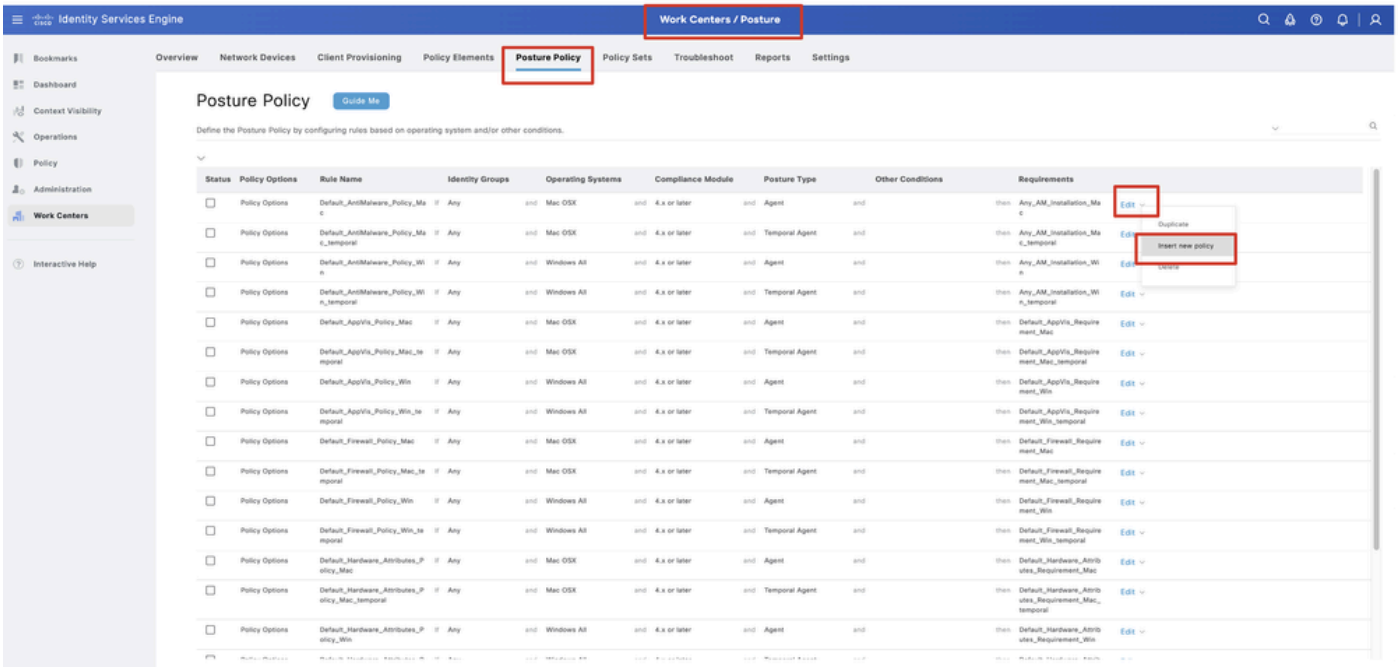
Nombre: compliance_profile

Nombre de DACL: PERMIT_ALL_IPv4_TRAFFIC



Nota: La DACL para terminales conformes o no conformes debe configurarse según los requisitos reales.

Paso 22. Desplácese hasta Work Centers > Posture > Posture Policy. Haga clic Edit al final de las reglas. Seleccione Insert new policy.



ISE_Add_New_Posture_Policy

Paso 22.1. Configure los detalles:

Nombre de regla: Demo_test_exist_linux

Grupos de identidades: Cualquiera

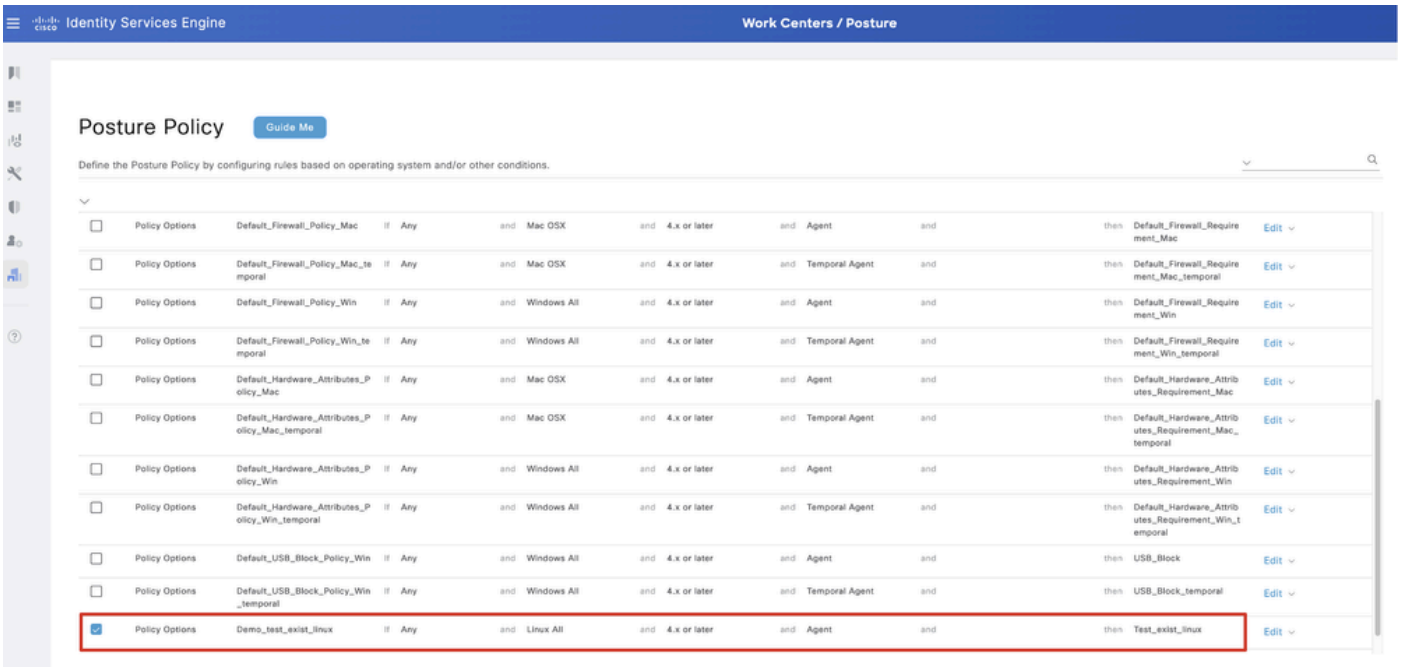
Sistemas operativos: Linux All

Módulo de cumplimiento: 4.x o posterior

Tipo de postura: Agente

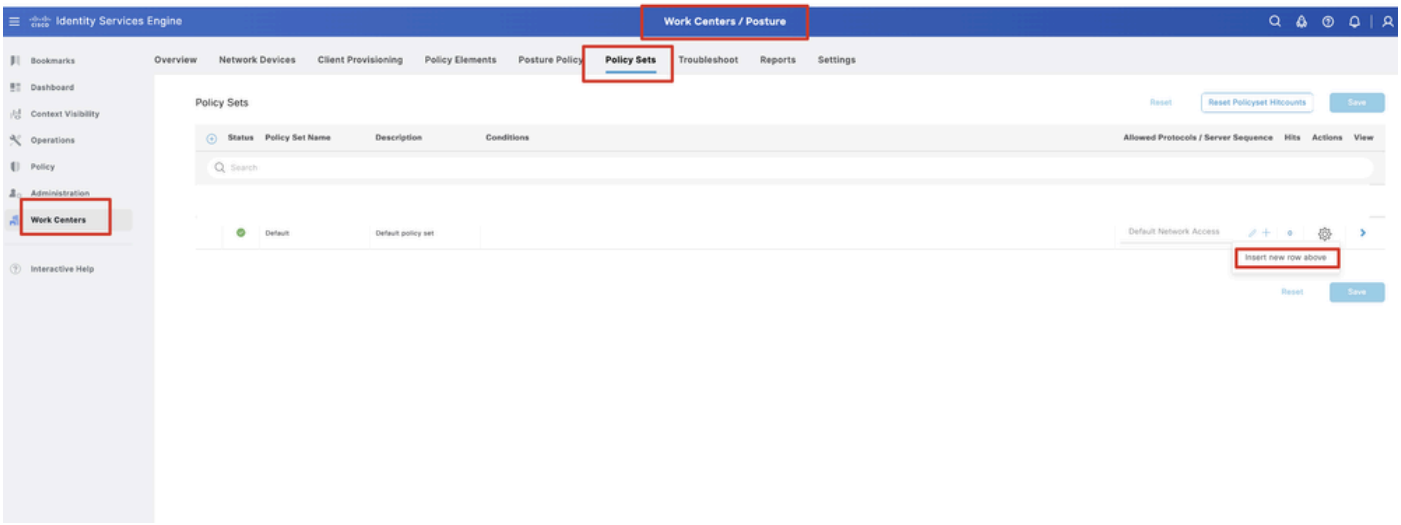
Requisitos: Test_exist_linux

Haga clic en Done y Save.



ISE_Add_New_Posture_Policy_1

Paso 23. Desplácese hasta Work Centers > Posture > Policy Sets. Haga clic para Insert new row above.



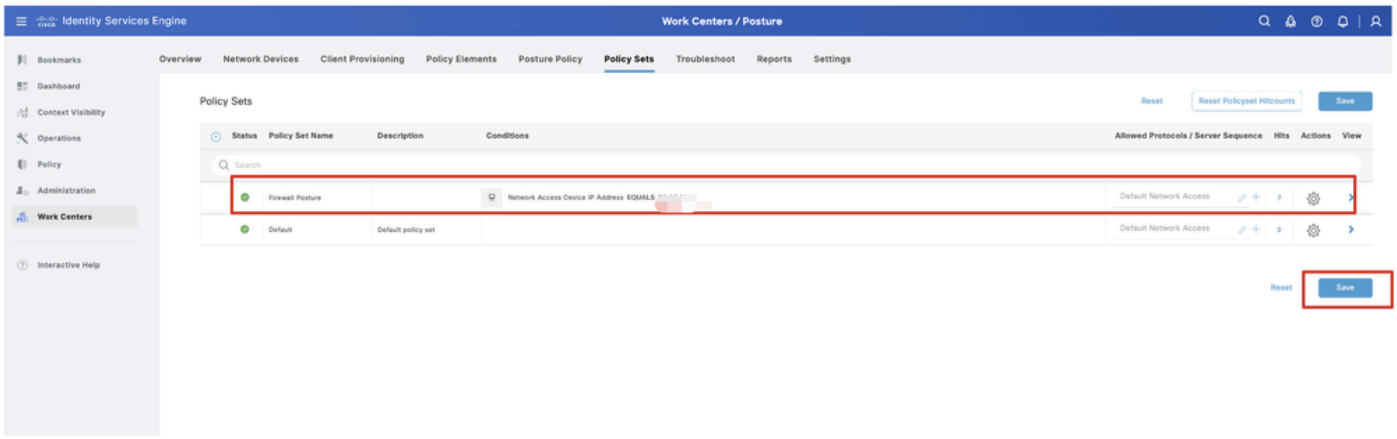
ISE_Add_New_Policy_Set

Paso 23.1. Configure los detalles:

Nombre del conjunto de políticas: Estado del firewall

Condiciones: Dispositivo de acceso a la red Dirección IP EQUALs [Dirección IP FTD]

Haga clic Save .



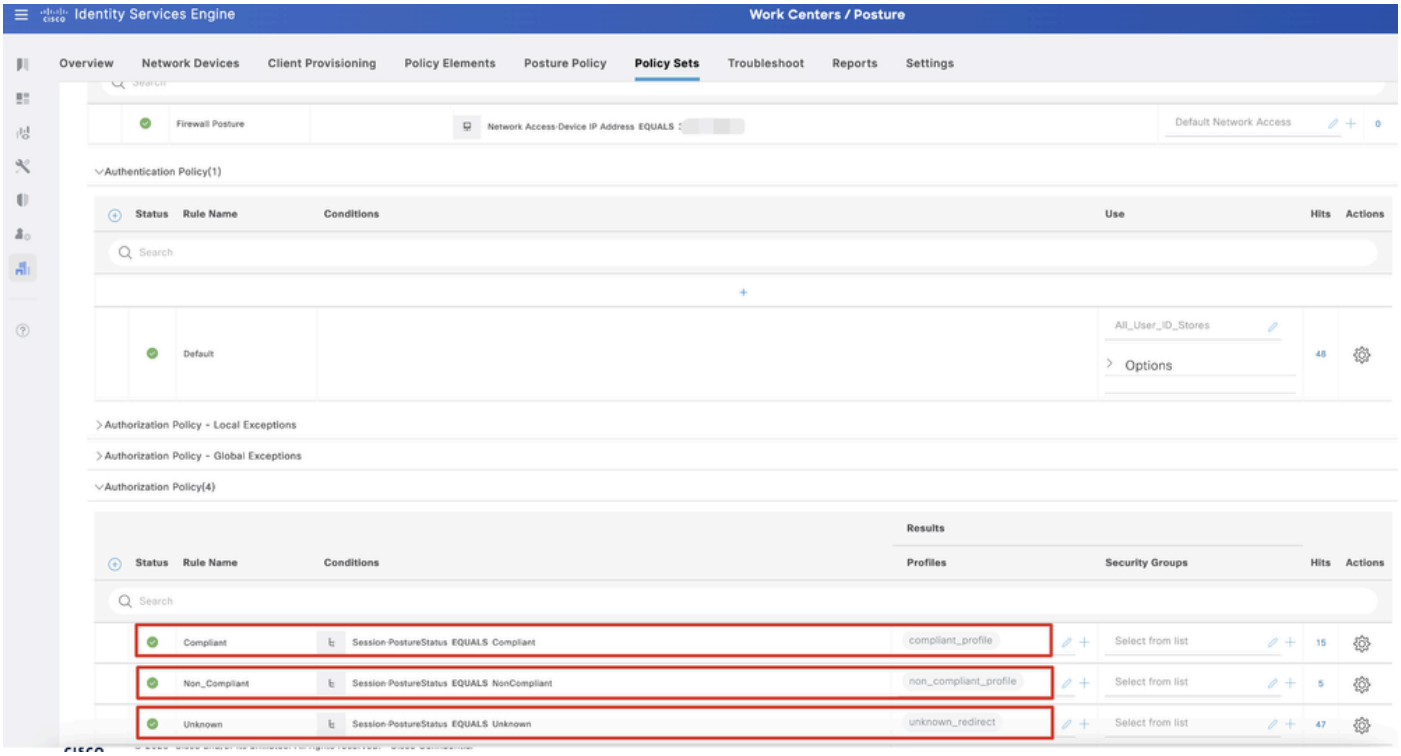
ISE_Add_New_Policy_Set_1

Paso 23.2. Haga clic > para introducir el conjunto de políticas. Crear nuevas reglas de autorización para estados conformes al estado, no conformes y desconocidos. Haga clic en Save.

De conformidad con compliance_profile

No conforme con non_compliance_profile

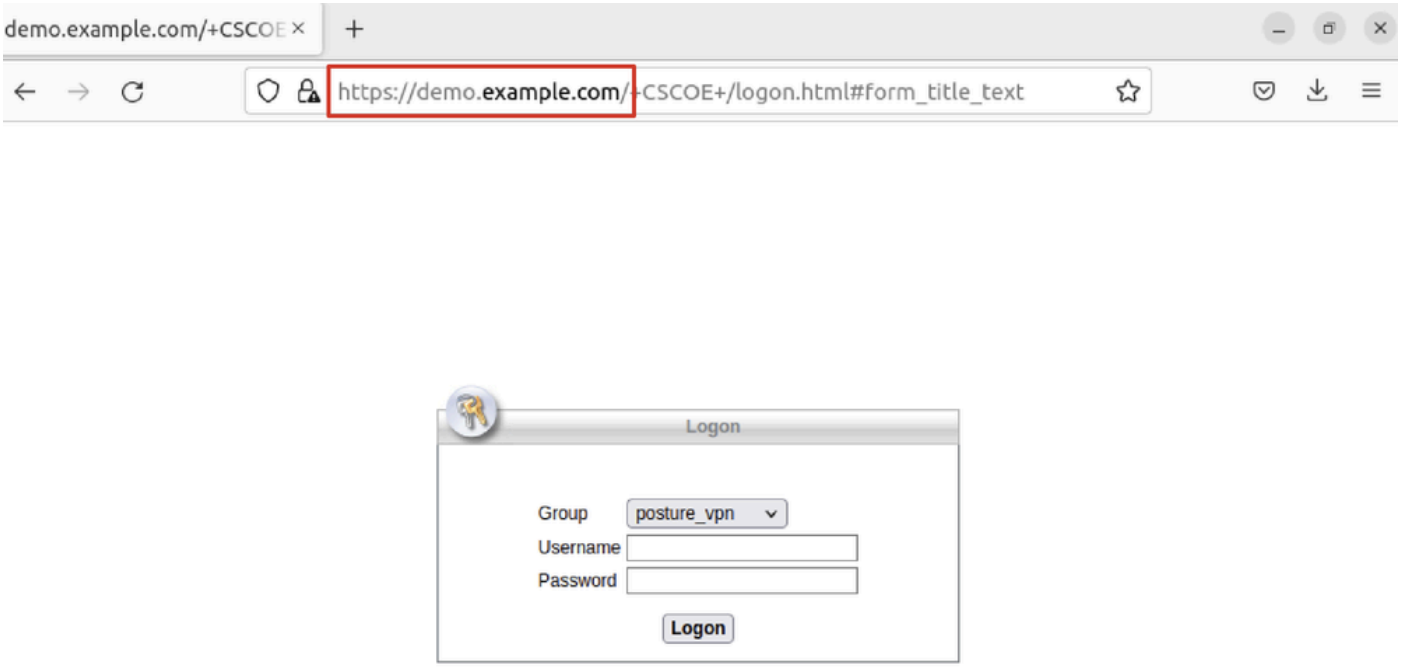
Desconocido con unknown_redirect



ISE_Add_New_Policy_Set_2

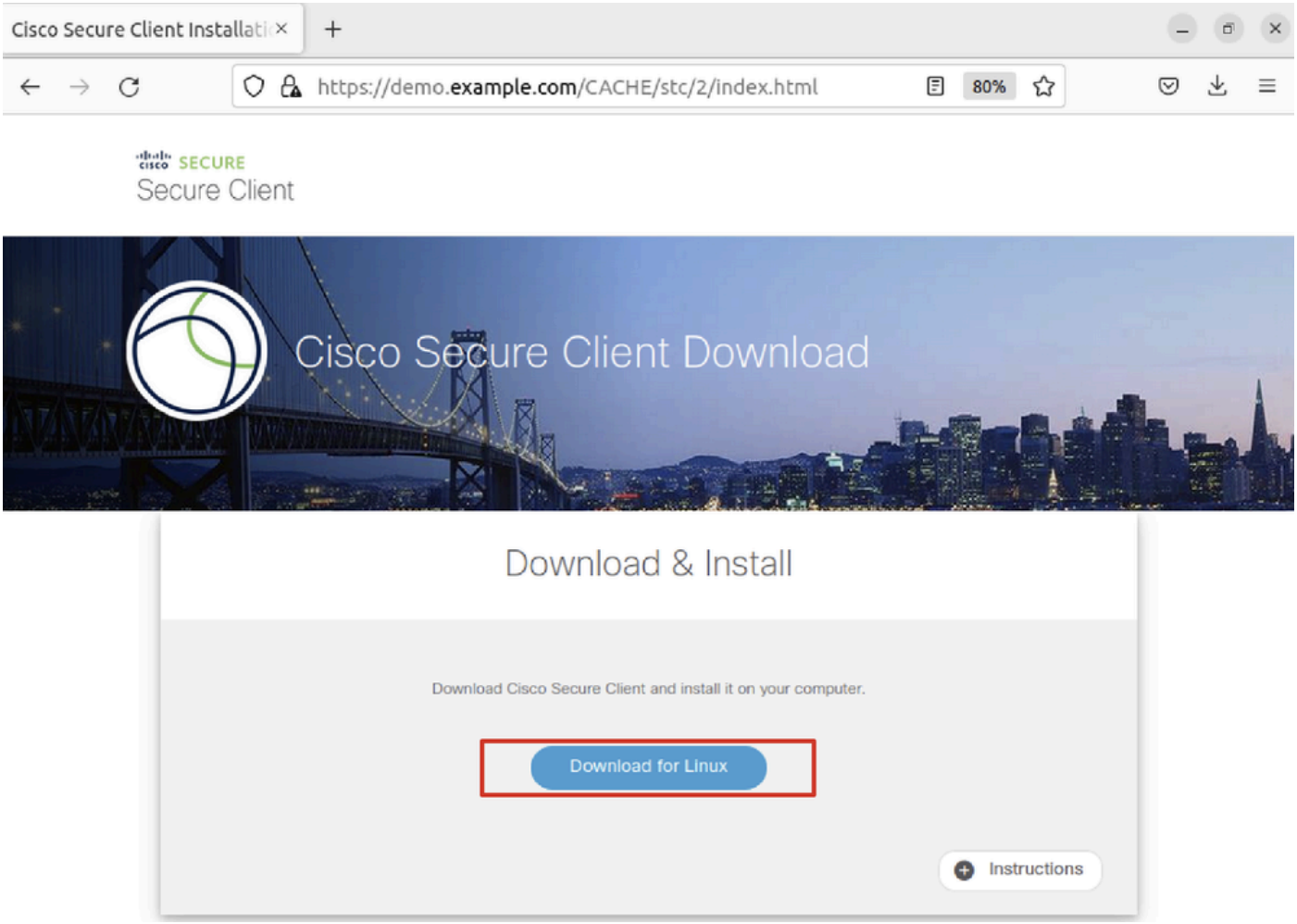
Configuraciones en Ubuntu

Paso 24. Inicie sesión en el cliente Ubuntu mediante la GUI. Abra el explorador para iniciar sesión en el portal VPN. En este ejemplo, es demo.example.com.



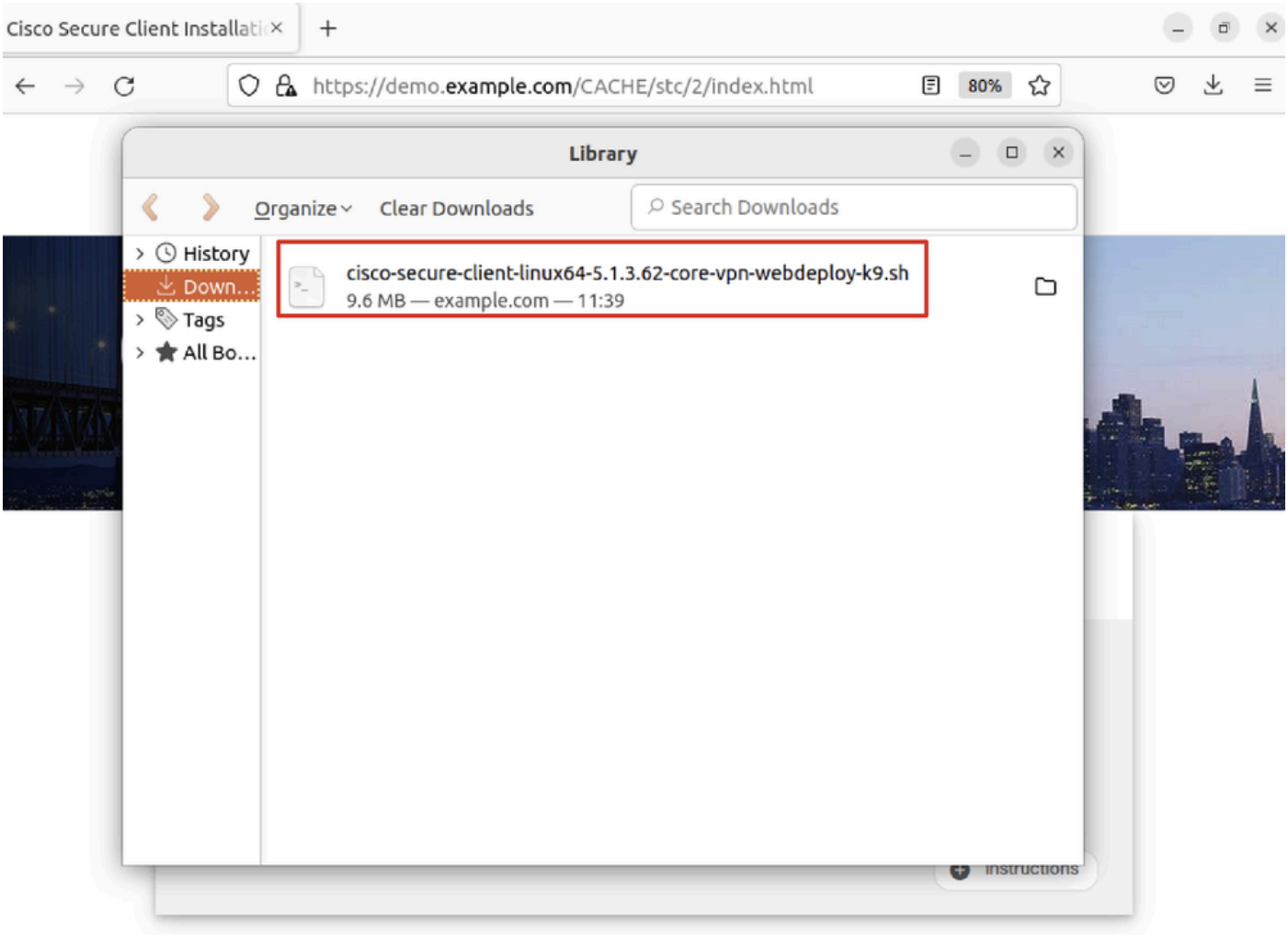
Ubuntu_Browser_VPN_Login

Paso 25. Haga clic en Download for Linux.



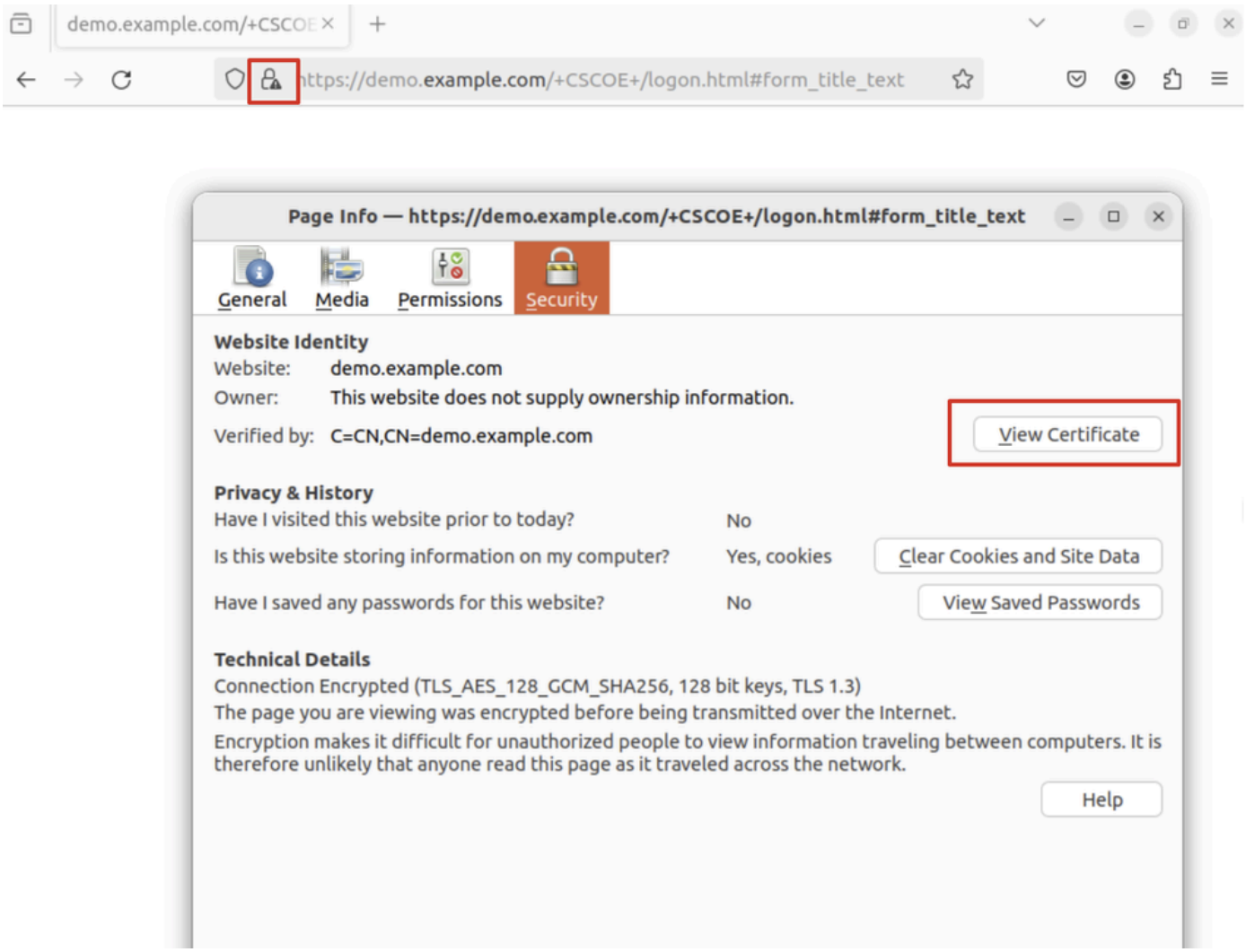
Ubuntu_Browser_VPN_Download_1

El nombre del archivo descargado es cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu_Browser_VPN_Download_2

Paso 26. Descargue el certificado VPN a través del navegador y cambie el nombre del archivo a <certificate>.crt. Este es el ejemplo de cómo usar firefox para descargar el certificado.



Ubuntu_Browser_VPN_Cert_Download

Paso 27. Abra el terminal en el cliente Ubuntu. Desplácese hasta path home/user/Downloads/ para instalar 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$
```

Paso 28. Confíe en el certificado del portal VPN en el cliente 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

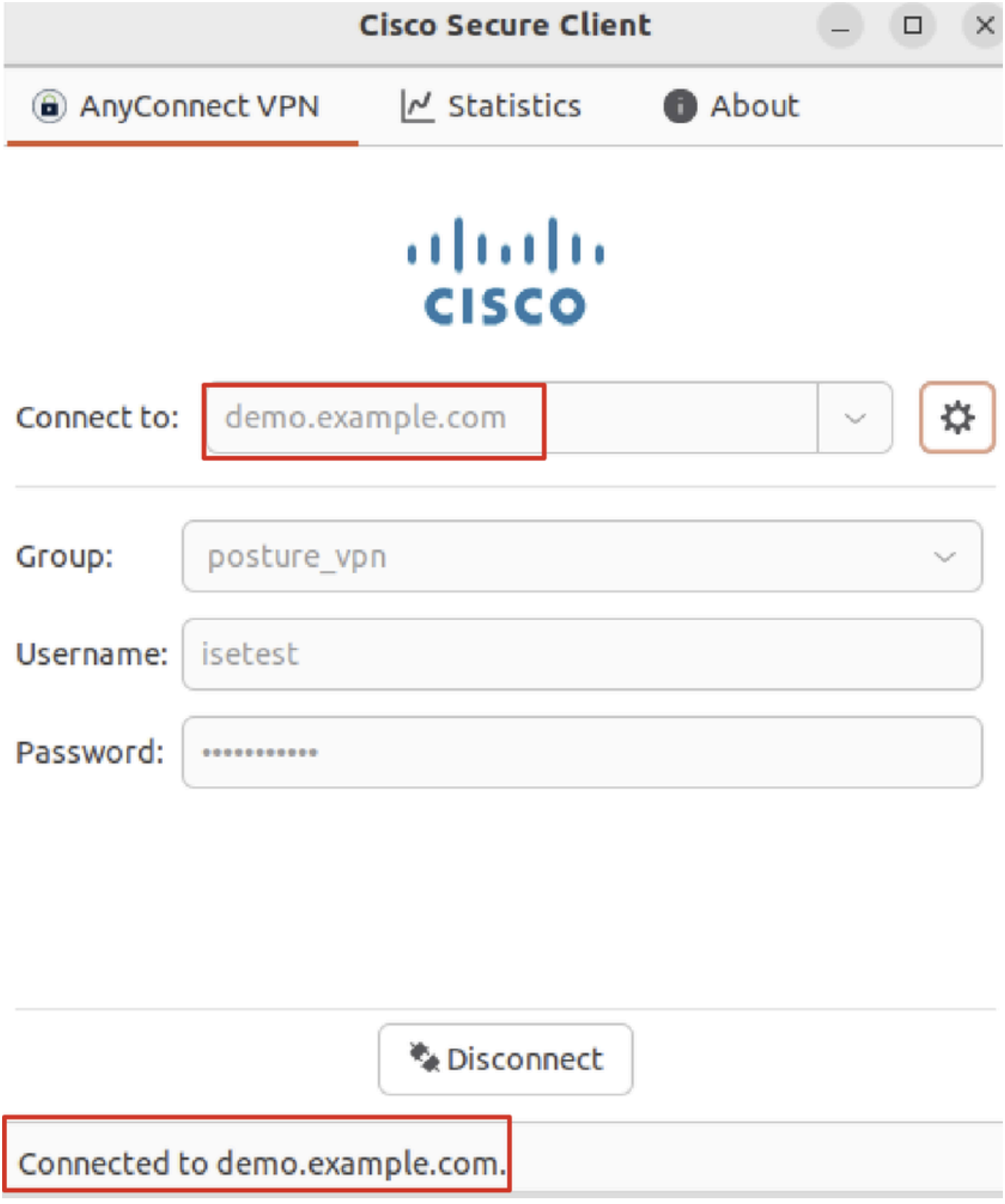
```
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
```

1 added

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

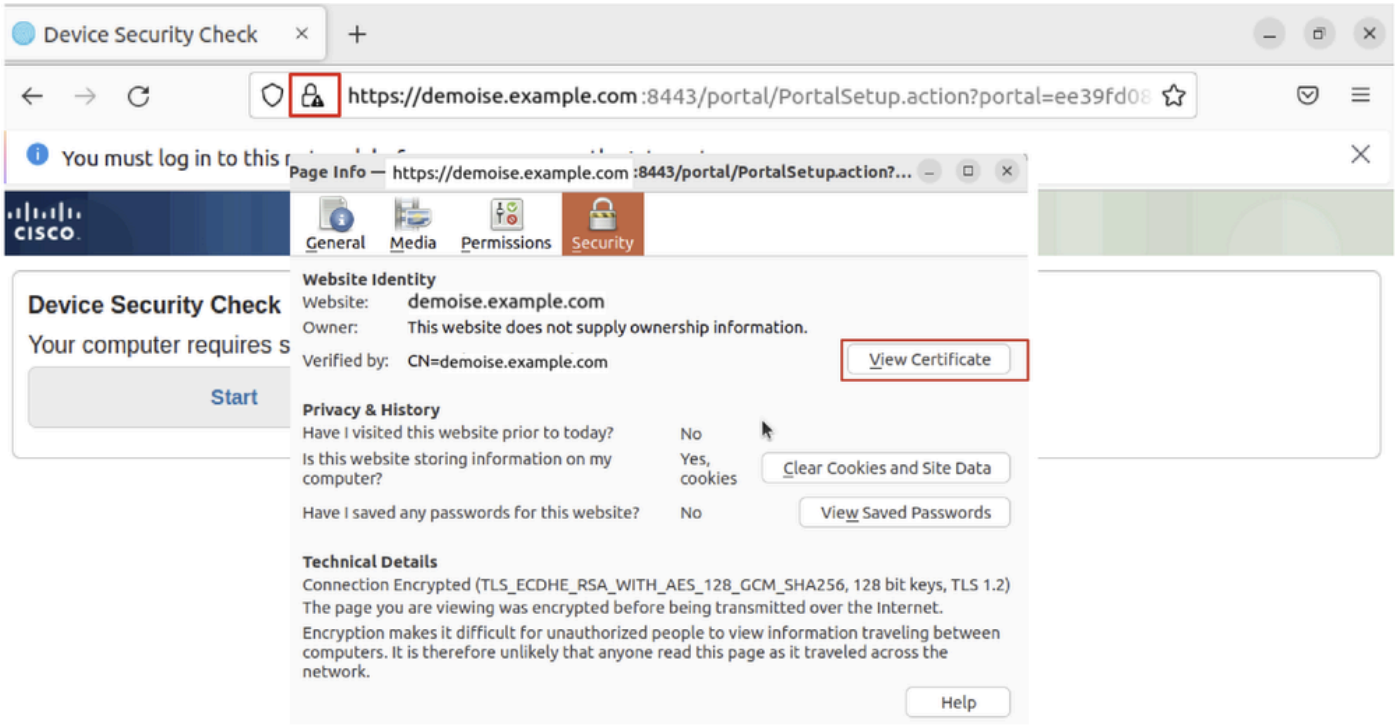
```
user@ubuntu22-desktop:~/Downloads$
openssl verify demo-example-com.crt

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

Paso 29. Abra Cisco Secure Client en el cliente Ubuntu y conecte VPN a demo.example.com correctamente.



Ubuntu_Secure_Client_Connected

Paso 30. Abra el navegador para acceder a cualquier sitio web que active la redirección al portal ISE CPP. Descargue el certificado del portal ISE CPP y cambie el nombre del archivo a <certificate>.crt. Este es un ejemplo del uso de Firefox para la descarga.



Ubuntu_Browser_CPP_Cert_Download

Paso 30.1. Confíe en el certificado del portal CPP de ISE en el cliente 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$

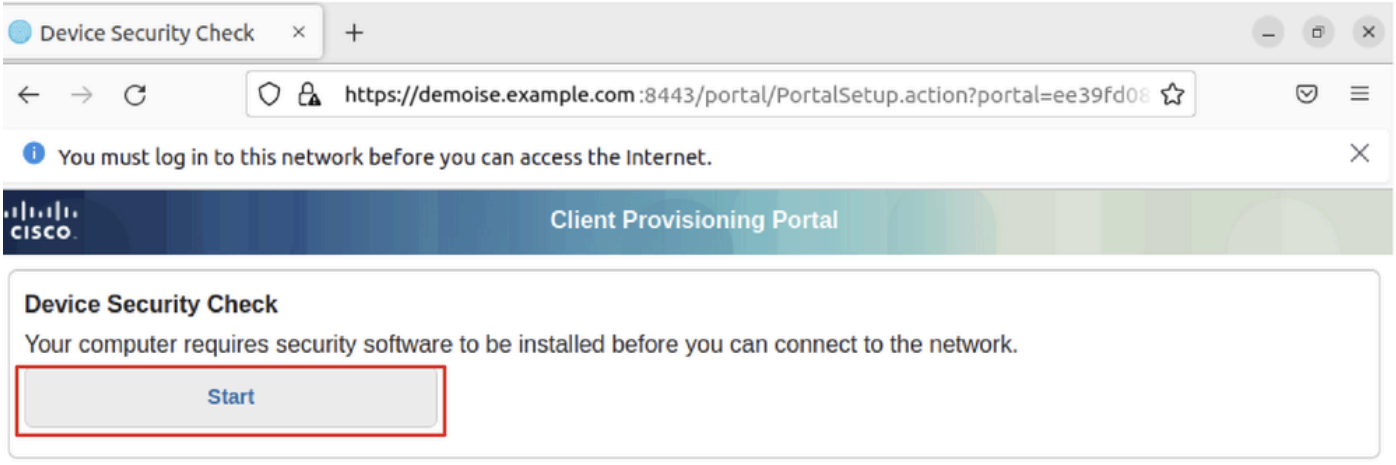
sudo update-ca-certificates

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.

Paso 31. Haga clic Start en el portal de ISE CPP.



Ubuntu_Browser_CPP_Start

Paso 32. Click here to download and install Agent.

Ubuntu_Browser_CPP_Download_Posture

Paso 33. Abra el terminal en el cliente Ubuntu. Vaya a la ruta home/user/Downloads/ para instalar el módulo de estado.

```
<#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.
```

Paso 34. En la interfaz de usuario del cliente de Ubuntu, salga de Cisco Secure Client y vuelva a abrirlo. El módulo de estado de ISE se ha instalado y se ha ejecutado correctamente.

Ubuntu_Secure_Client_ISE_Posture_Installed

Paso 35. Abra el terminal en el cliente Ubuntu. Navegue hasta rutahome/user/Desktop , cree un test.txt archivo para cumplir con la condición de archivo configurada en ISE.

<#root>

user@ubuntu22-desktop:~$

cd Desktop/

user@ubuntu22-desktop:~/Desktop$

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

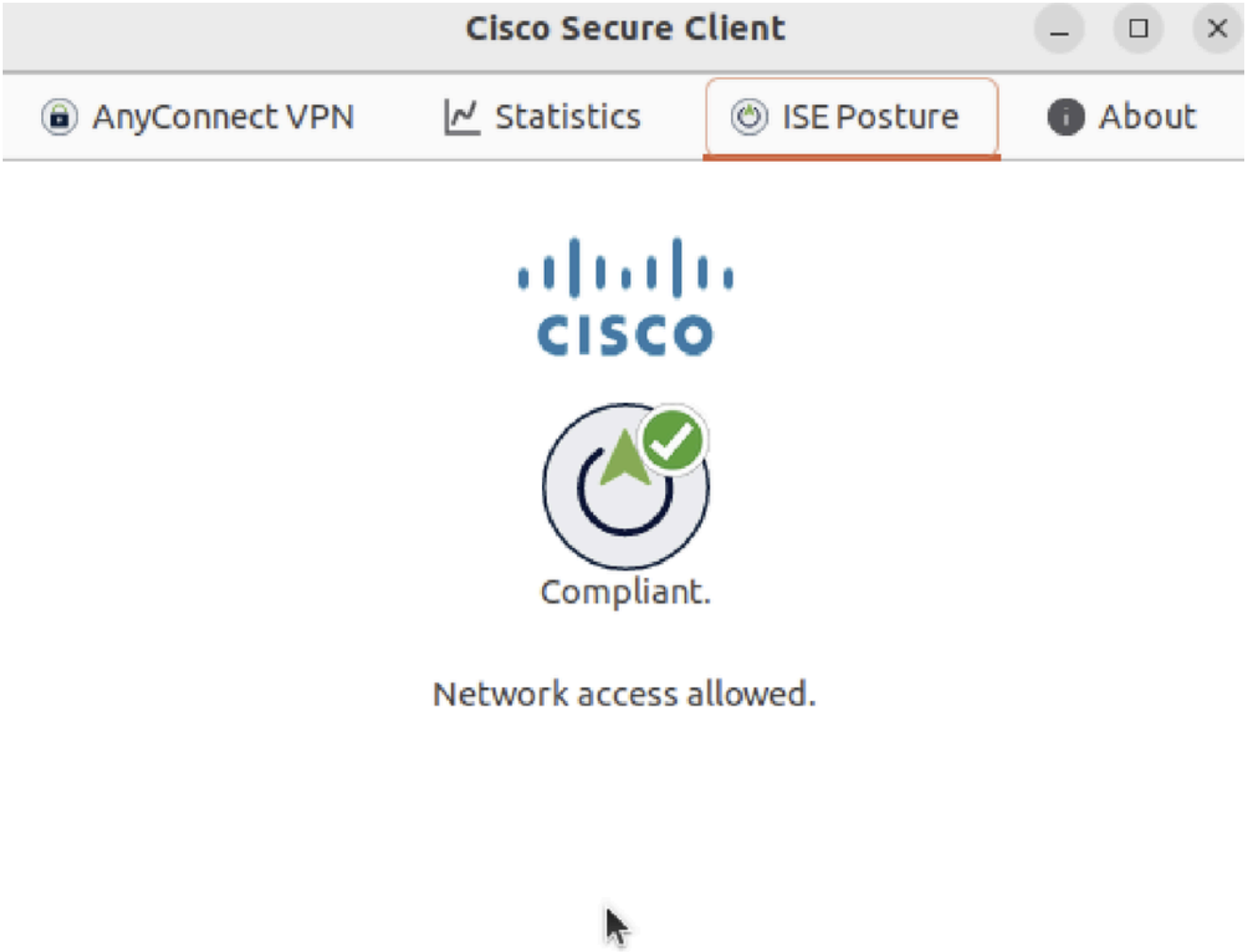
Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Conecte VPN a demo.example.com en el cliente Ubuntu.

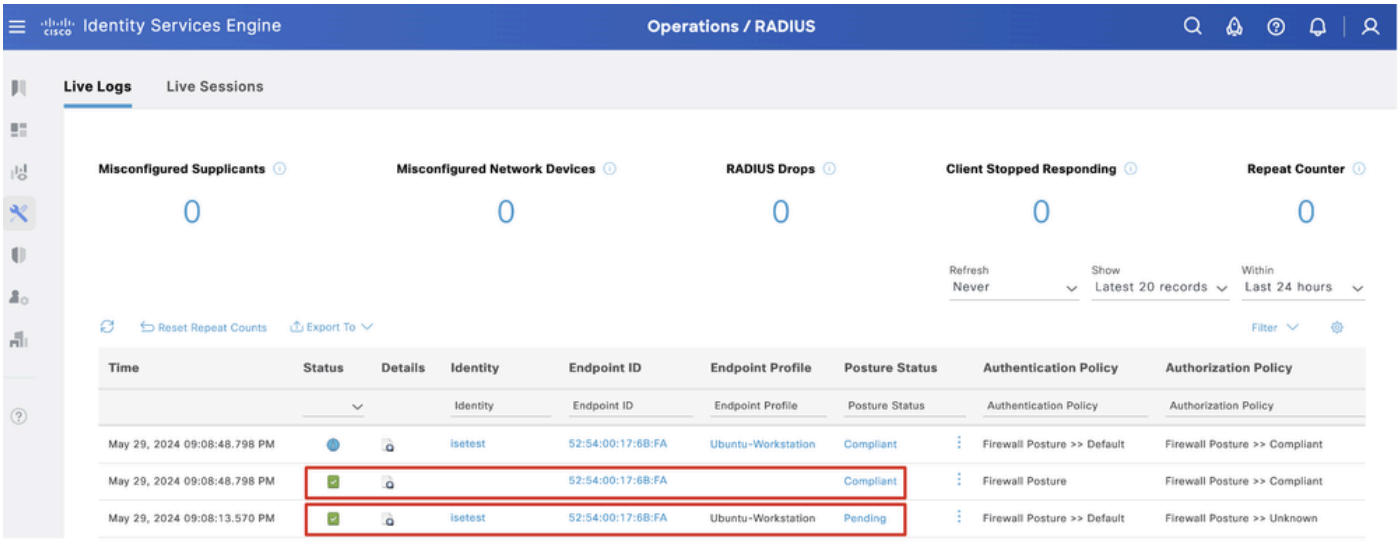
Verify_Ubuntu_Secure_Client_Connected

Paso 2. Compruebe el estado de ISE en el cliente Ubuntu.



Verify_Ubuntu_Secure_Client_Compliant

Paso 3. Marque Radius Live Log en ISE. Desplácese hasta Operations > RADIUS Live Log.



Paso 4. Vaya a FTD CLI mediante SSH o la consola.

```
<#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 : cb007182000210006659d871
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
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para ver el flujo de estado y la resolución de problemas de Cisco Secure Client e ISE, consulte los **documentos de** CCO**ISE Posture Style Comparison for Pre and Post 2.2** y **Troubleshooting de ISE Session Management and Posture.**

Información Relacionada

- Compatibilidad de componentes de red de Cisco Identity Services Engine, versión 3.3

- Guía del administrador de Cisco Identity Services Engine, versión 3.3
- **Soporte técnico y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).