Configuración de la posición de ISE en VPN de acceso remoto AnyConnect en FTD

Contenido

Introducción

Este documento describe cómo configurar Firepower Threat Defence (FTD) versión 6.4.0 para exponer a los usuarios de VPN frente a Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN de acceso remoto AnyConnect
- Configuración de VPN de acceso remoto en el FTD
- Identity Services Engine y servicios de estado

Componentes Utilizados

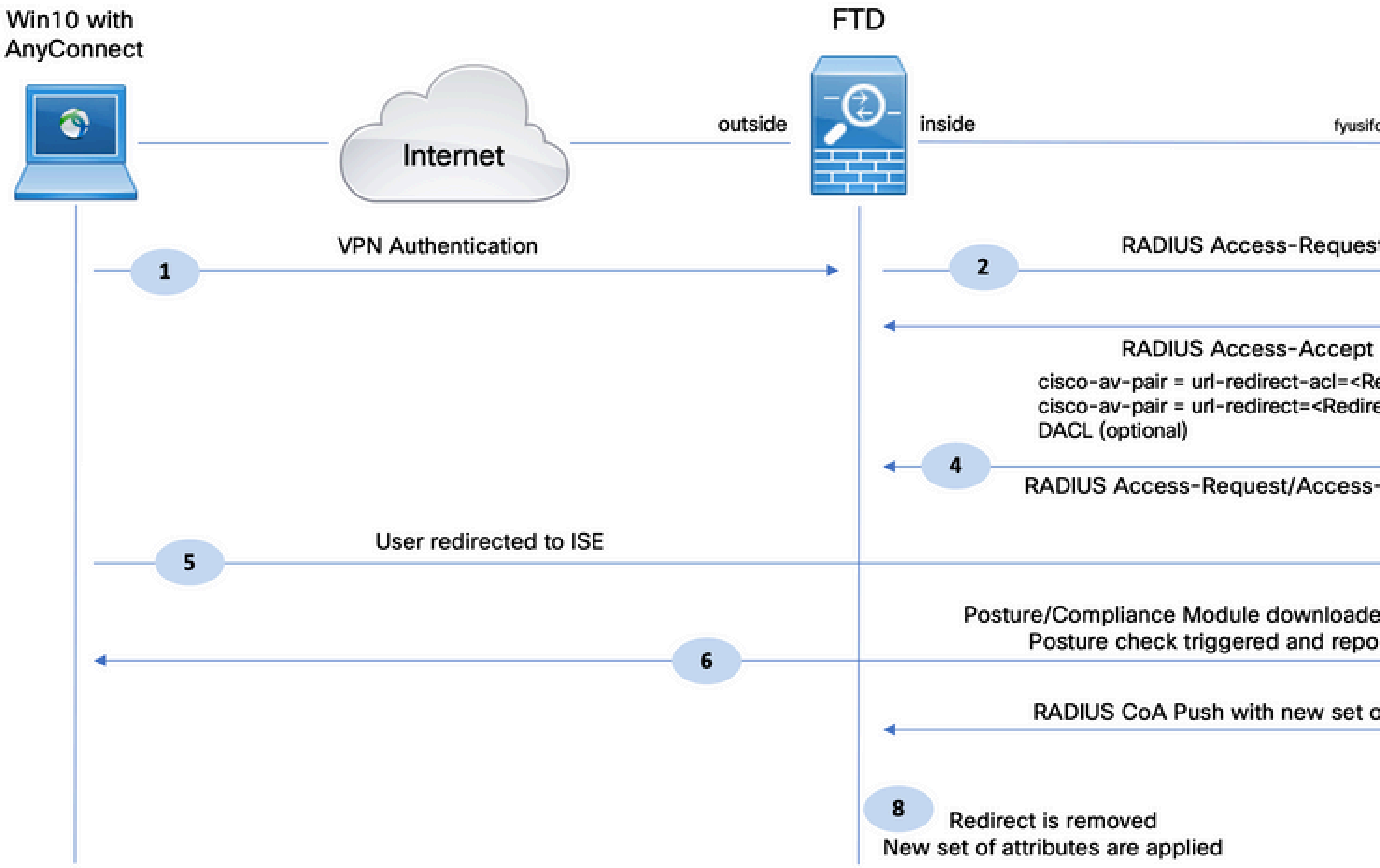
La información que contiene este documento se basa en estas versiones de software:

- Software Cisco Firepower Threat Defense (FTD), versiones 6.4.0
- Software Cisco Firepower Management Console (FMC) versión 6.5.0
- Microsoft Windows 10 con Cisco AnyConnect Secure Mobility Client versión 4.7
- Cisco Identity Services Engine (ISE) versión 2.6 con parche 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 red y flujo de tráfico


Win10 with AnyConnect
FTD
Internet
outside
inside
fyusifo
VPN Authentication
1
2
RADIUS Access-Request
RADIUS Access-Accept
cisco-av-pair = url-redirect-acl=<Re
cisco-av-pair = url-redirect=<Redire
DACL (optional)
4
RADIUS Access-Request/Access-
User redirected to ISE
5
Posture/Compliance Module downloade
Posture check triggered and repo
6
RADIUS CoA Push with new set o
8
Redirect is removed
New set of attributes are applied

1. El usuario remoto utiliza Cisco Anyconnect para el acceso VPN al FTD.

2. El FTD envía una solicitud de acceso RADIUS para ese usuario a ISE.

3. Esa solicitud llega a la política denominada **FTD-VPN-Posture-Unknown** en ISE. ISE envía una aceptación de acceso RADIUS con tres atributos:

- **cisco-av-pair = url-redirect-acl=fyusifovredirect** - Este es el nombre de la lista de control de acceso (ACL) que se define localmente en el FTD, que decide el tráfico que se redirige.
- cisco-av-pair = url-redirect=**https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp**: **URL a la que se redirige al usuario remoto.**
- **DACL = PERMIT_ALL_IPV4_TRAFFIC** - ACL descargable Este atributo es opcional. En esta situación, todo el tráfico está permitido en DACL)

4. Si se envía la DACL, se intercambia RADIUS Access-Request/Access-Accept para descargar el contenido de la DACL

5. Cuando el tráfico del usuario VPN coincide con la ACL definida localmente, se redirige al portal de aprovisionamiento de clientes de ISE. ISE aprovisiona el módulo de estado de AnyConnect y el módulo de conformidad.

6. Una vez instalado el agente en el equipo cliente, busca ISE con sondeos automáticamente. Cuando se

detecta ISE correctamente, se comprueban los requisitos de estado en el terminal. En este ejemplo, el agente comprueba si hay software antimalware instalado. A continuación, envía un informe de estado al ISE.

7. Cuando ISE recibe el informe de estado del agente, ISE cambia el estado de estado de esta sesión y activa el tipo de RADIUS CoA Push con nuevos atributos. Esta vez, se conoce el estado de postura y se aplica otra regla.

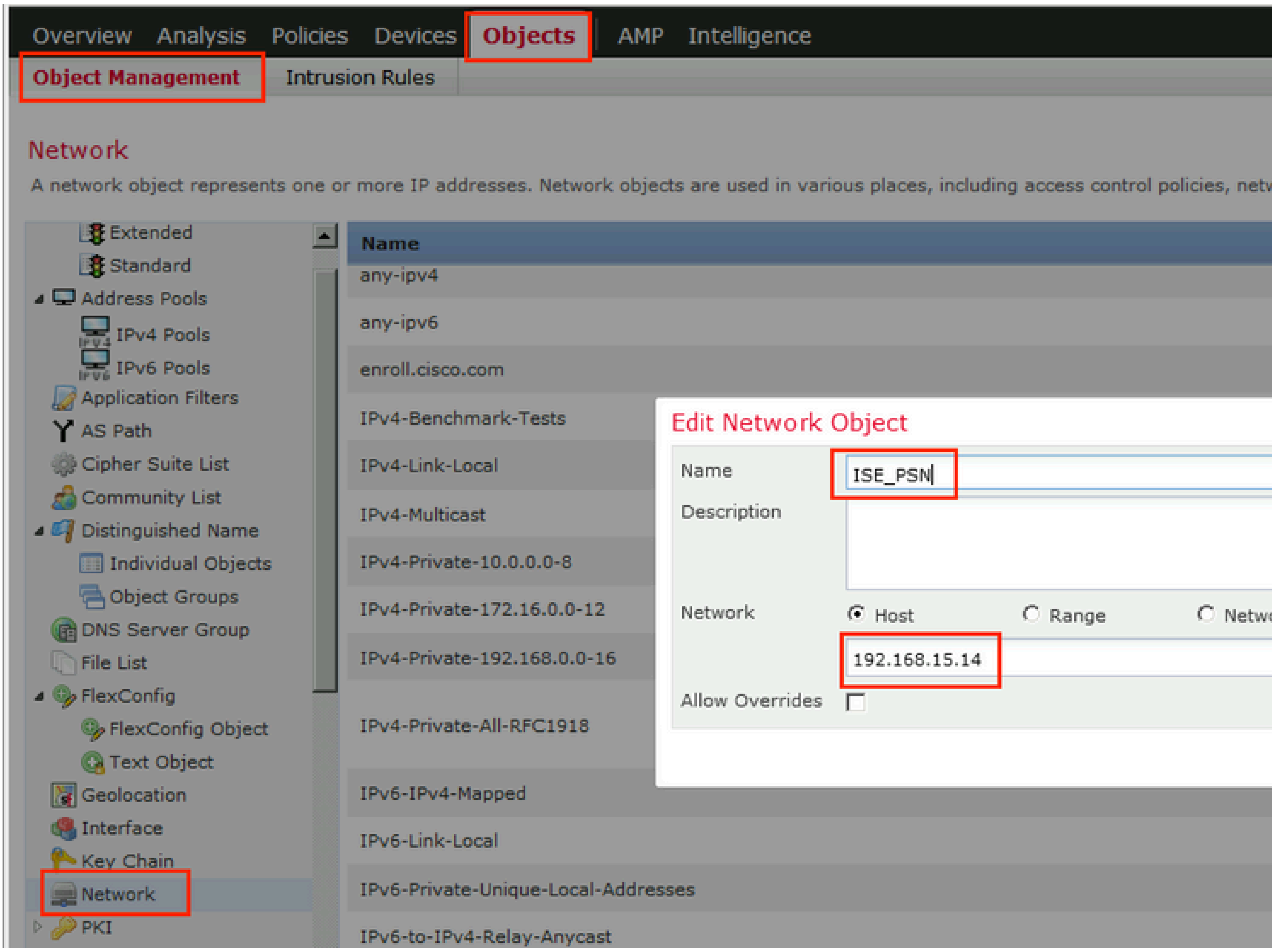
- Si el usuario cumple con la normativa, se envía un nombre de DACL que permite el acceso completo.
- Si el usuario no cumple con la normativa, se envía un nombre de DACL que permite el acceso limitado.

8. El FTD elimina la redirección. FTD envía Access-Request para descargar DACL desde ISE. La DACL específica se asocia a la sesión VPN.

Configuraciones

FTD/FMC

Paso 1. Crear un grupo de objetos de red para ISE y servidores de corrección (si los hay). Navegue hasta **Objetos > Administración de objetos > Red**.



Network

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, netw

Name
any-ipv4
any-ipv6
enroll.cisco.com
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8
IPv4-Private-172.16.0.0-12
IPv4-Private-192.168.0.0-16
IPv4-Private-All-RFC1918
IPv6-IPv4-Mapped
IPv6-Link-Local
IPv6-Private-Unique-Local-Addresses
IPv6-to-IPv4-Relay-Anycast

Edit Network Object

Name: ISE_PSN

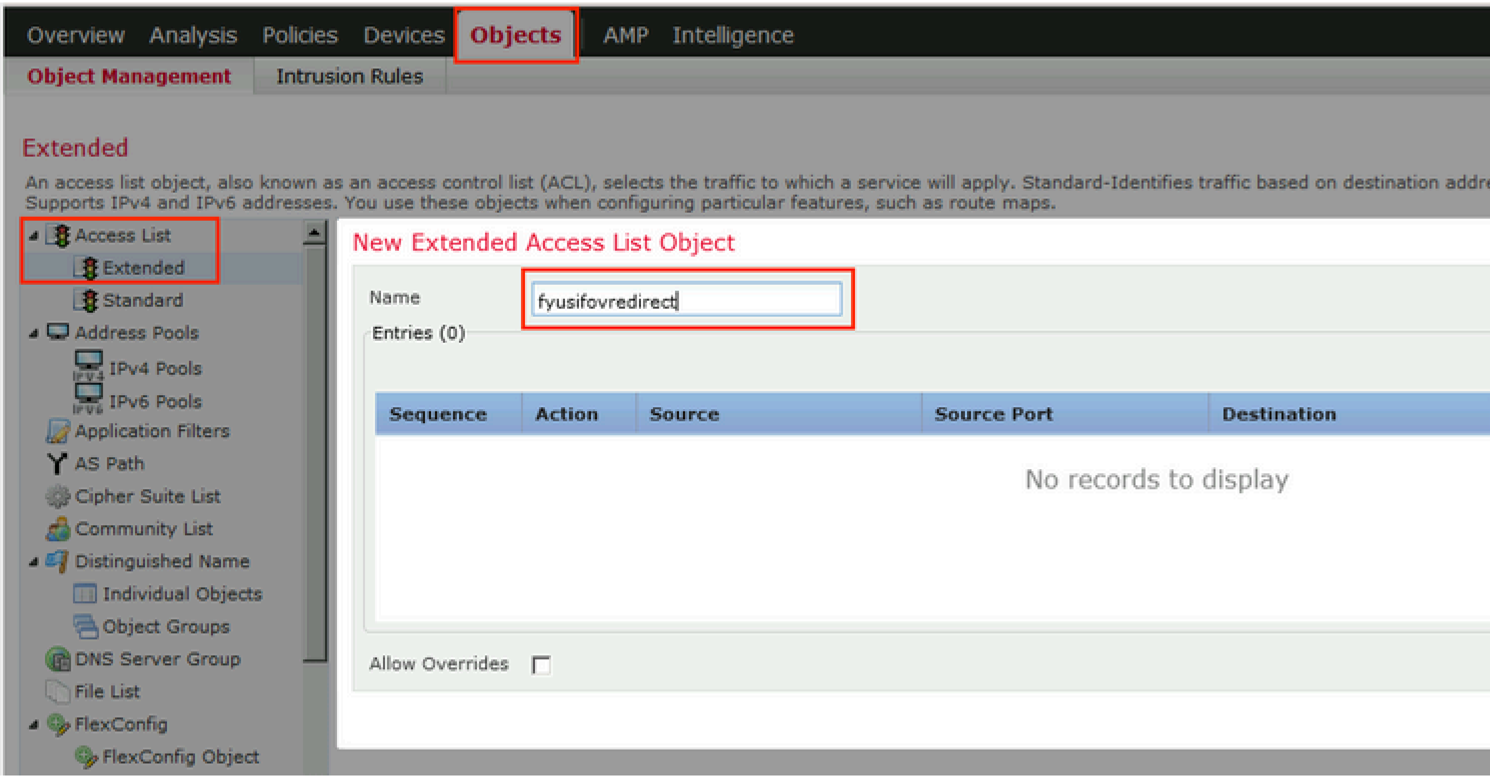
Description:

Network: ● Host ○ Range ○ Netw

192.168.15.14

Allow Overrides □

Paso 2. Crear ACL de redirección. Navegue hasta **Objetos** > **Administración de objetos** > **Lista de acceso** > **Extendida**. Haga clic en **Add Extended Access List** y proporcione el nombre de Redirect ACL. Este nombre debe ser el mismo que en el resultado de la autorización de ISE.



Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination addre
Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

New Extended Access List Object

Name: fyusifovredirect

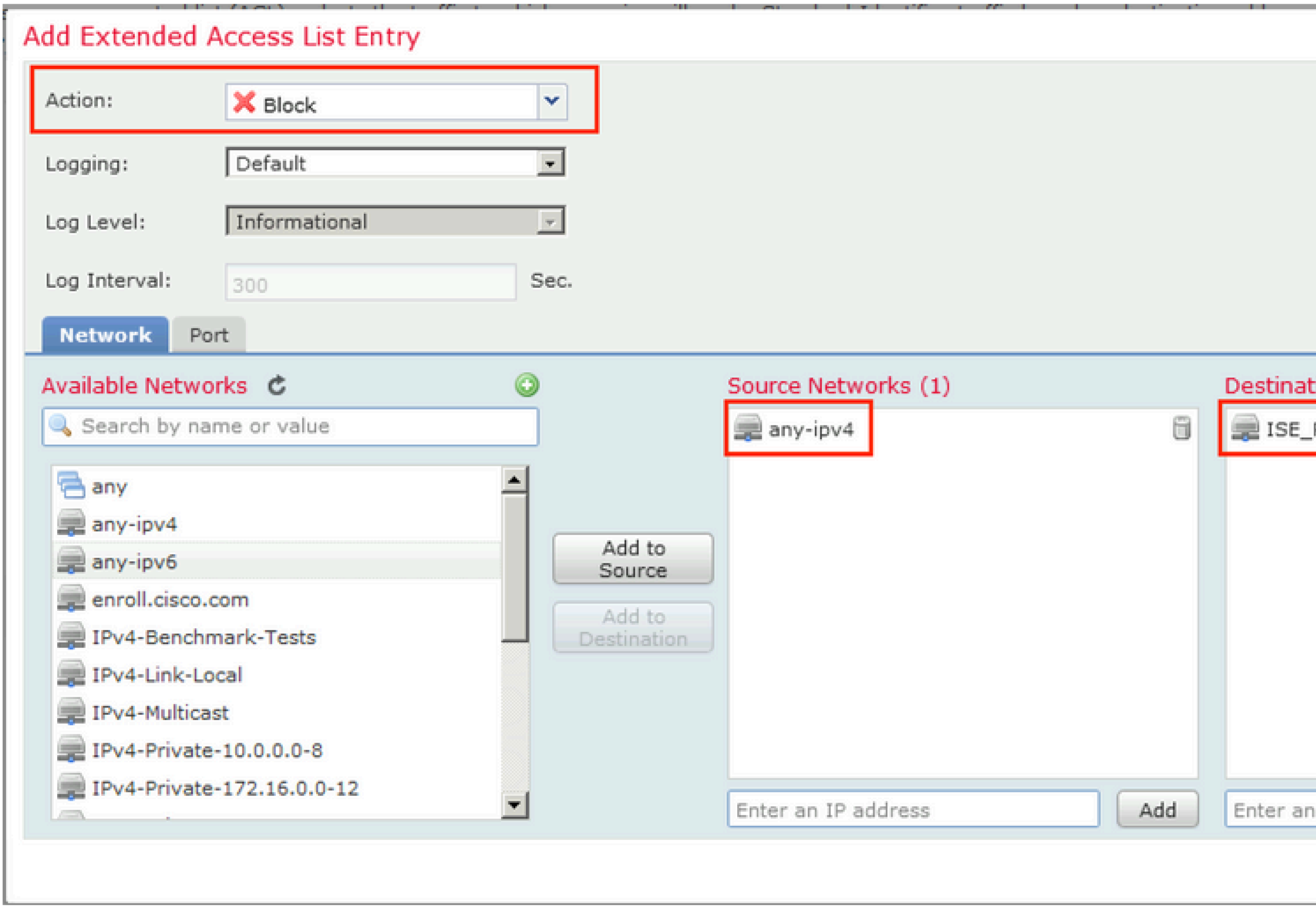
Entries (0)

Sequence	Action	Source	Source Port	Destination

No records to display

Allow Overrides □

Paso 3. Agregue entradas de ACL de redirección. â€˜Haga clic en el botón Add (Agregar).â€™ Bloquee el tráfico a DNS, ISE y a los servidores de corrección para excluirlos de la redirección. Permitir el resto del tráfico, esto activa la redirección (las entradas de ACL podrían ser más específicas si fueran necesarias).



Add Extended Access List Entry

Action: Block

Logging: Default

Log Level: Informational

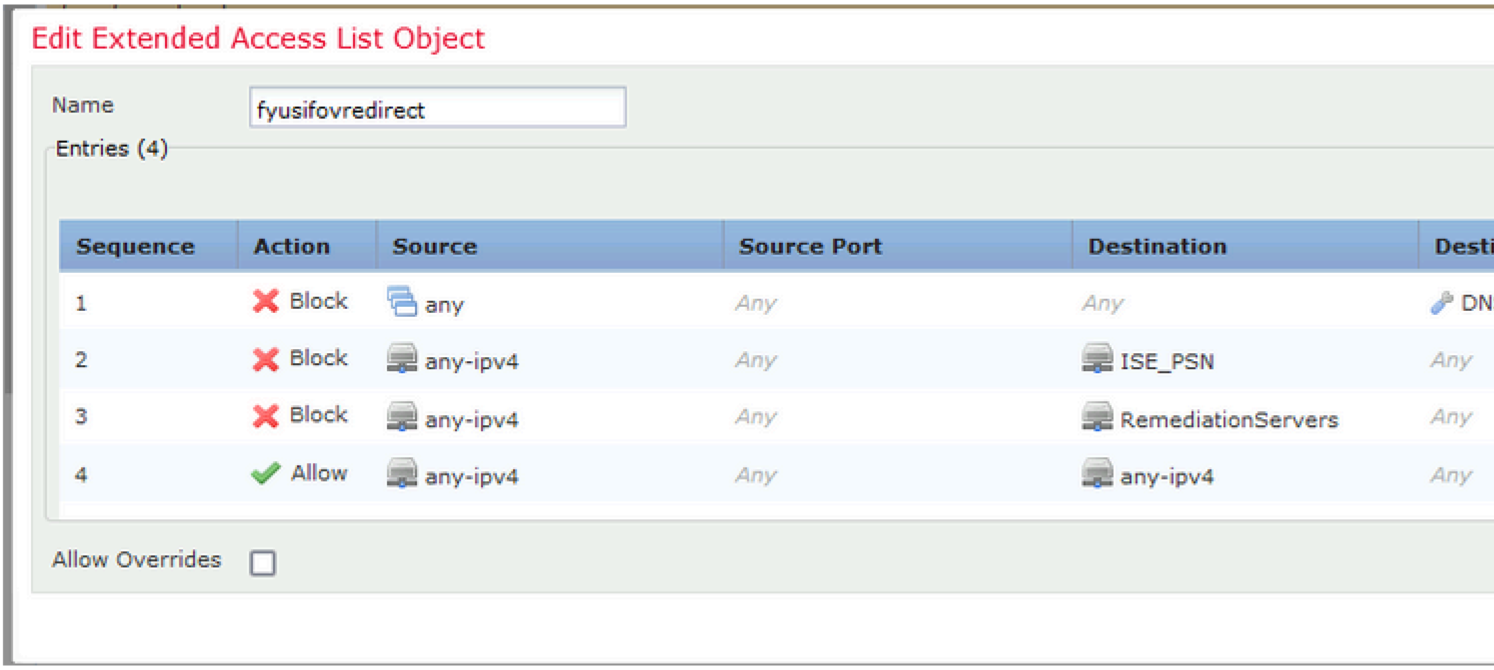
Log Interval: 300 Sec.

Source Networks (1)

any-ipv4

Destinat

ISE_



Edit Extended Access List Object

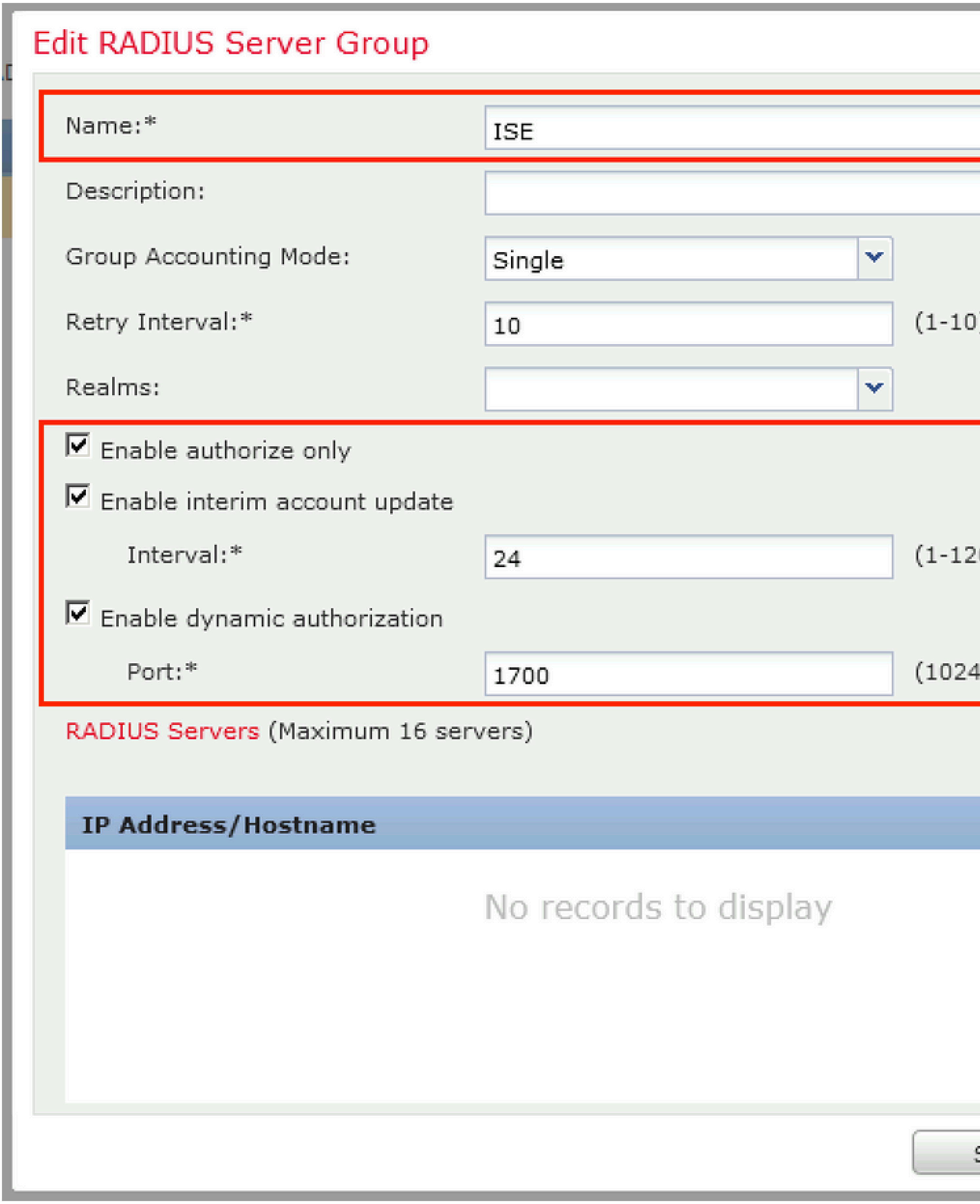
Name: fyusifovredirect

Entries (4)

Sequence	Action	Source	Source Port	Destination	Desti
1	✗ Block	any	Any	Any	DN
2	✗ Block	any-ipv4	Any	ISE_PSN	Any
3	✗ Block	any-ipv4	Any	RemediationServers	Any
4	✓ Allow	any-ipv4	Any	any-ipv4	Any

Allow Overrides □

Paso 4. Agregue nodos PSN de ISE. Navegue hasta **Objetos > Administración de objetos > Grupo de servidores RADIUS**. Haga clic en **Agregar grupo de servidores RADIUS**, luego indique el nombre, active todas las casillas de verificación y haga clic en el icono **más**.



Edit RADIUS Server Group

Name:* ISE

Description:

Group Accounting Mode: Single

Retry Interval:* 10 (1-10

Realms:

☑ Enable authorize only

☑ Enable interim account update

Interval:* 24 (1-12

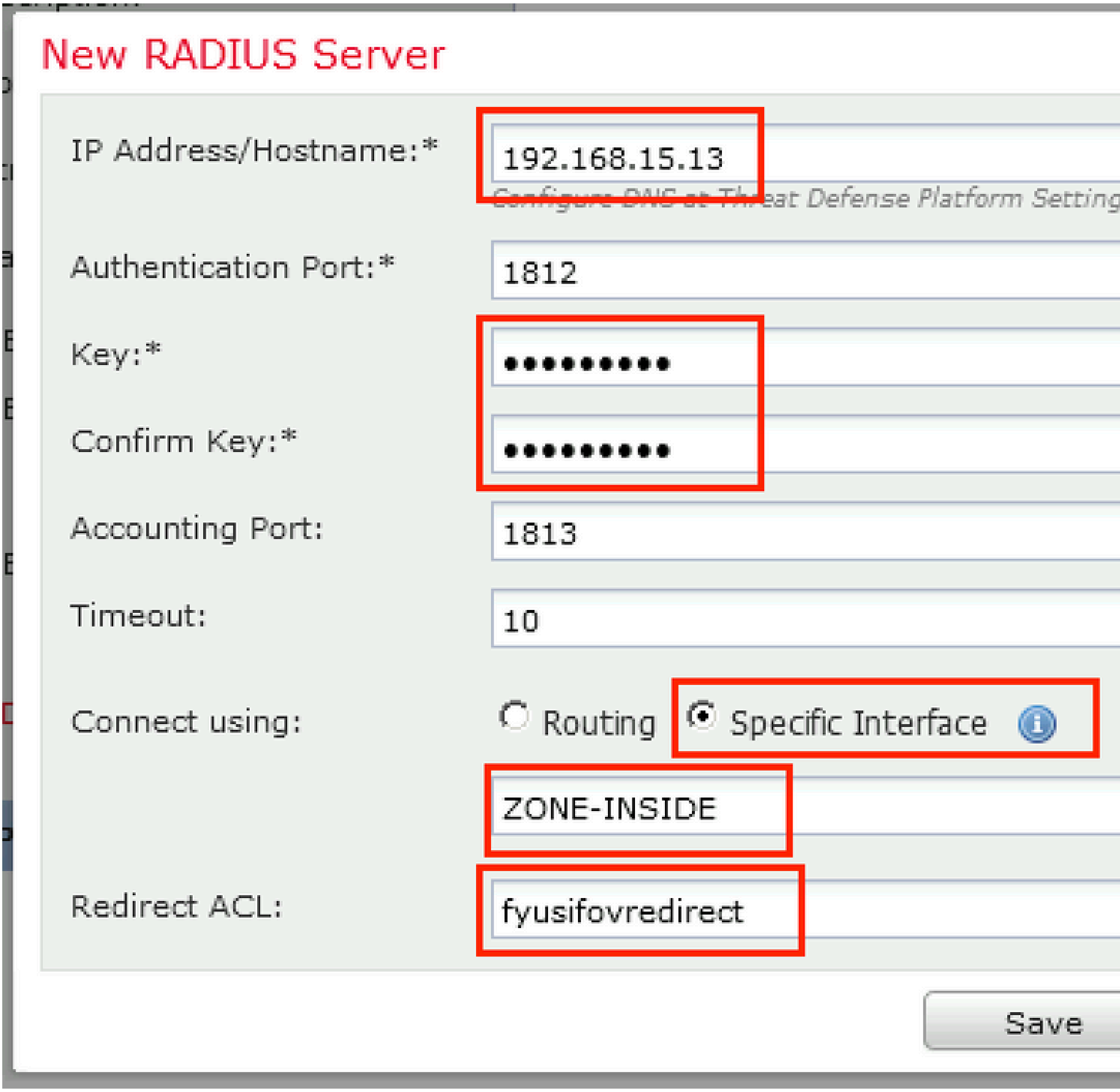
☑ Enable dynamic authorization

Port:* 1700 (1024

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

Paso 5. En la ventana abierta, proporcione la dirección IP PSN de ISE, la clave RADIUS, seleccione **Specific Interface** y seleccione la interfaz desde la que se puede alcanzar ISE (esta interfaz se utiliza como origen del tráfico RADIUS) y, a continuación, seleccione **Redirect ACL**, que se configuró anteriormente.



New RADIUS Server

IP Address/Hostname:* 192.168.15.13

Configure DNS at Threat Defense Platform Setting

Authentication Port:* 1812

Key:* ●●●●●●●●●●

Confirm Key:* ●●●●●●●●●●

Accounting Port: 1813

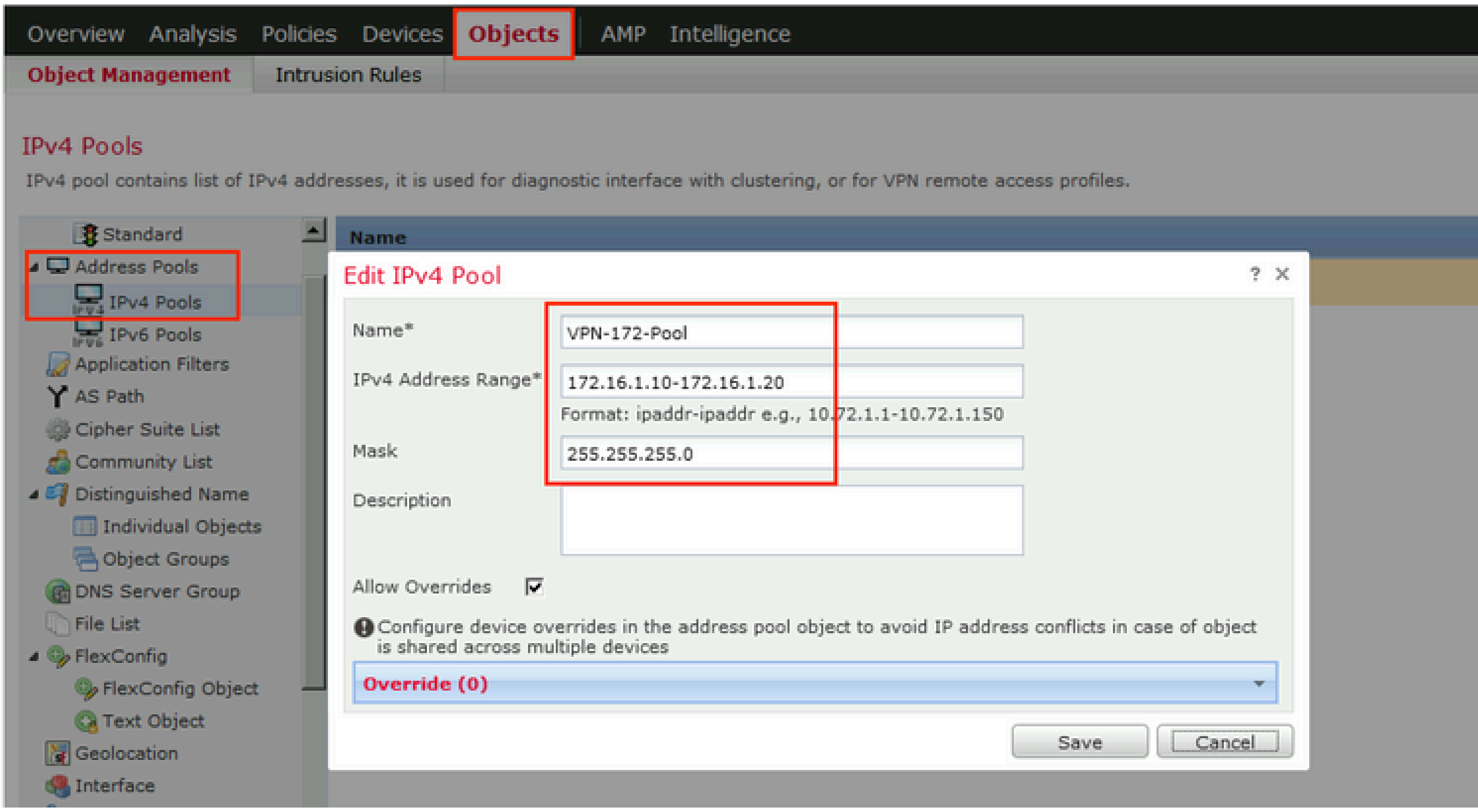
Timeout: 10

Connect using: ○ Routing ● Specific Interface

ZONE-INSIDE

Redirect ACL: fyusifovredirect

Paso 6. Crear conjunto de direcciones para usuarios de VPN. Navegue hasta **Objetos** > **Administración de objetos** > **Pools de direcciones** > **Pools IPv4**. Haga clic en **Add IPv4 Pools** y rellene los detalles.



IPv4 Pools

IPv4 pool contains list of IPv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles.

Edit IPv4 Pool

Name* VPN-172-Pool

IPv4 Address Range* 172.16.1.10-172.16.1.20

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask 255.255.255.0

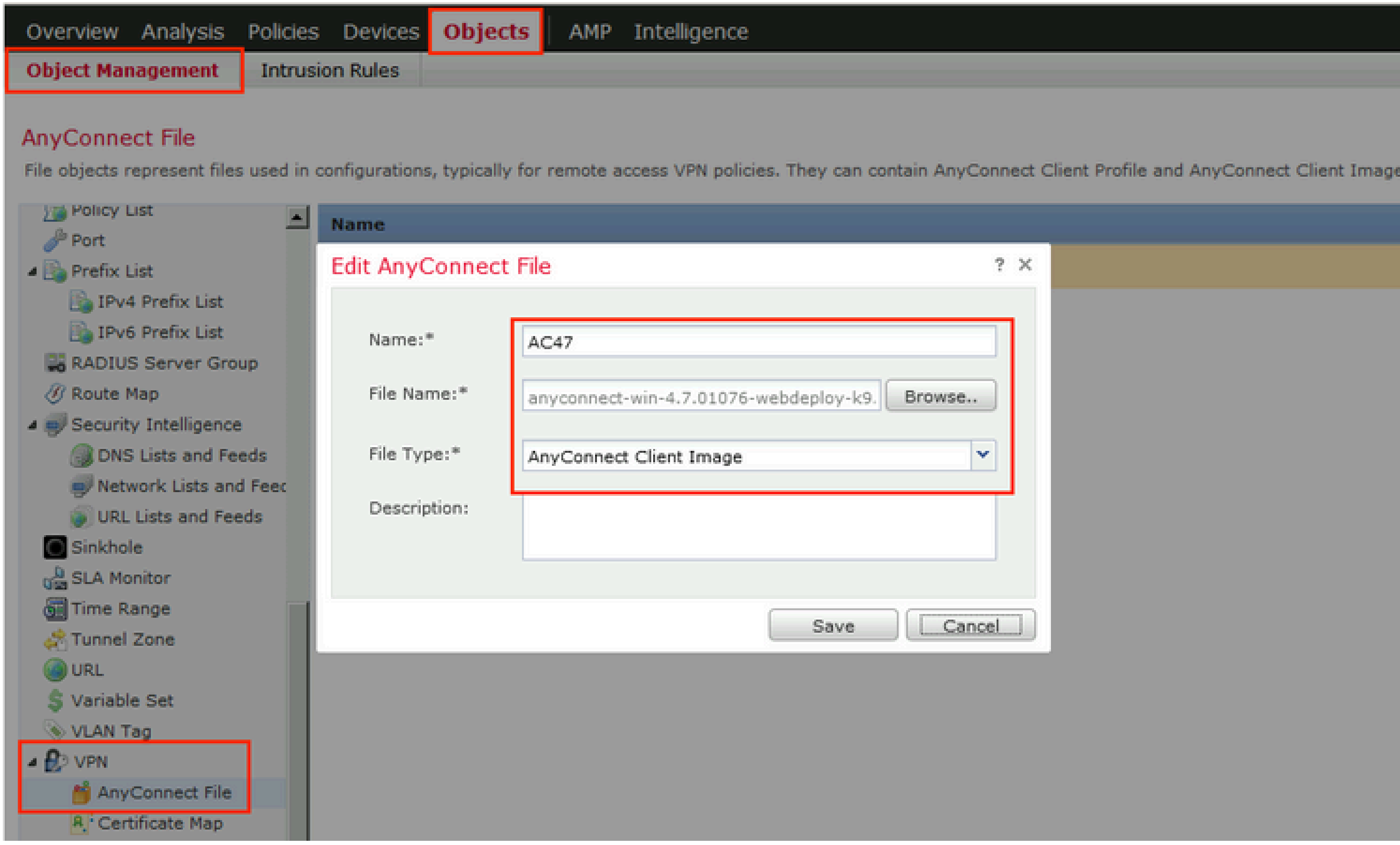
Description

Allow Overrides ☑

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Override (0)

Paso 7. Cree el paquete de AnyConnect. Navegue hasta **Objetos** > **Administración de objetos** > **VPN** > **Archivo de AnyConnect**. Haga clic en **Agregar archivo de AnyConnect**, proporcione el nombre del paquete, descargue el paquete de [Descarga de software de Cisco](#) y seleccione el tipo de archivo **Imagen de cliente de Anyconnect**.



AnyConnect File

File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image

Edit AnyConnect File

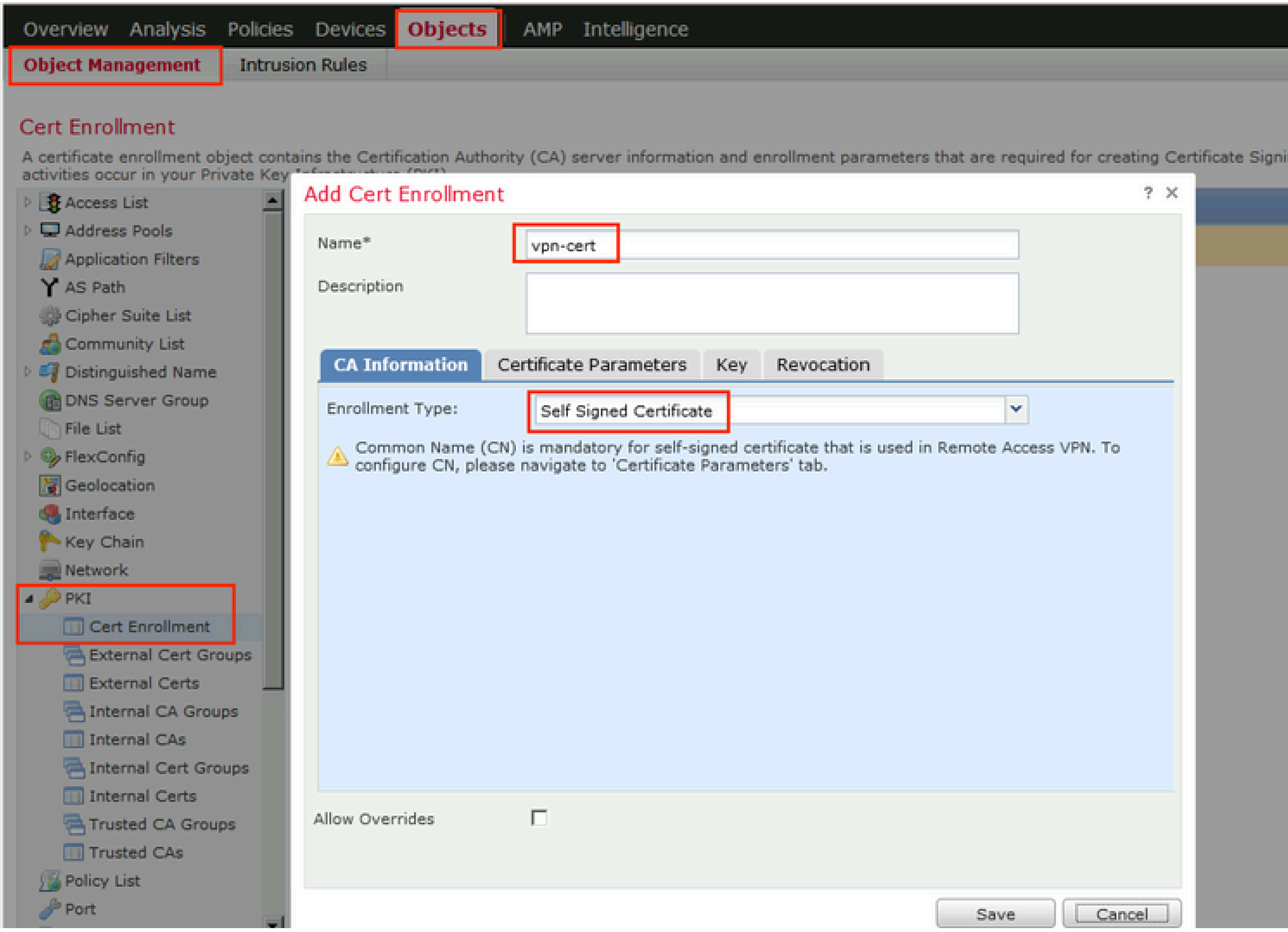
Name:* AC47

File Name:* anyconnect-win-4.7.01076-webdeploy-k9.

File Type:* AnyConnect Client Image

Description:

Paso 8. Navegue hasta **Objetos de certificado > Administración de objetos > PKI > Inscripción de certificado**. Haga clic en **Add Cert Enrollment**, proporcione el nombre y elija **Self Signed Certificate** en Enrollment Type. Haga clic en la ficha Parámetros de certificado y proporcione CN.



Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signi
activities occur in your Private Key

Add Cert Enrollment

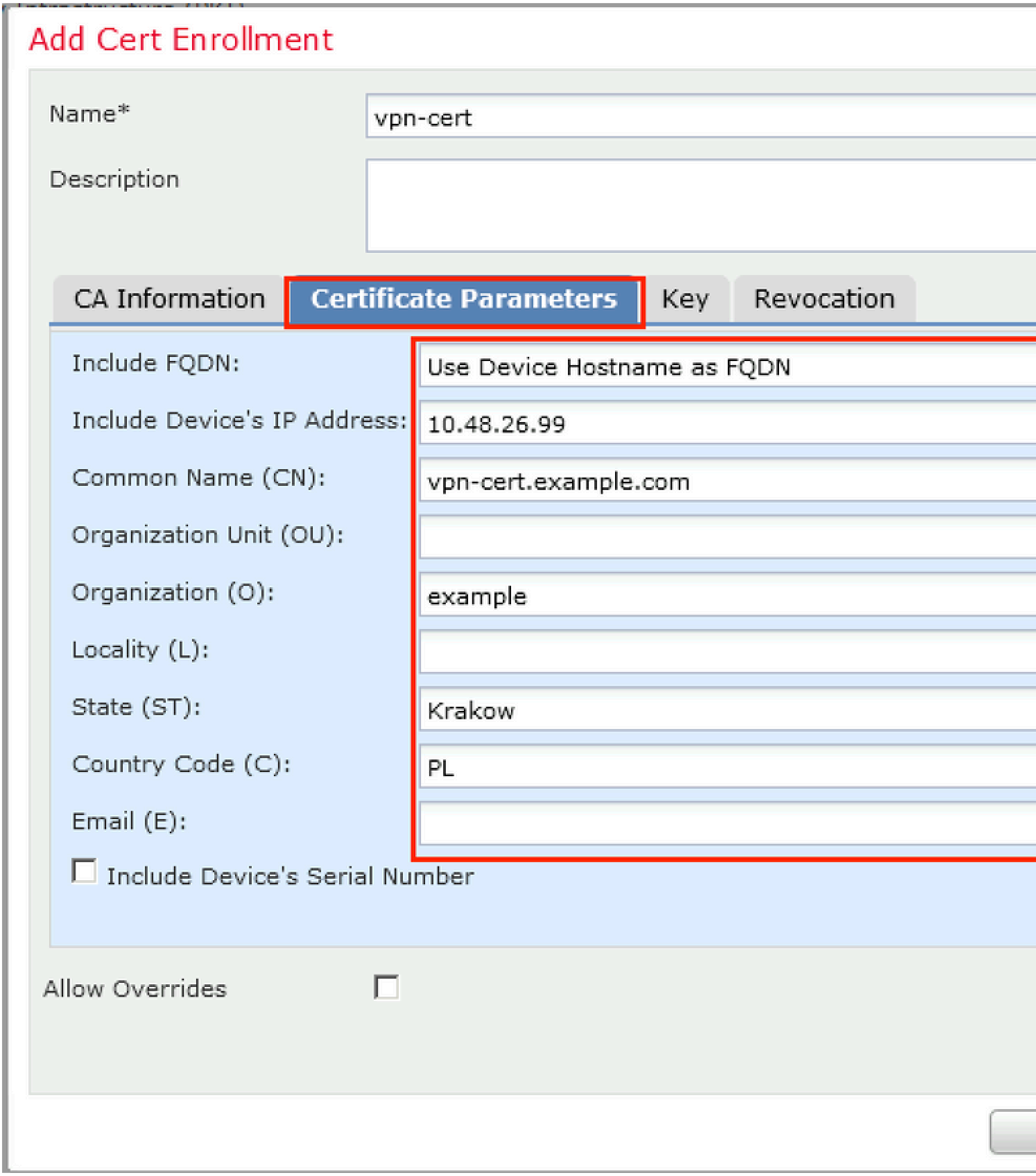
Name* vpn-cert

Description

Enrollment Type: Self Signed Certificate

⚠ Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.

Allow Overrides ☐



Add Cert Enrollment

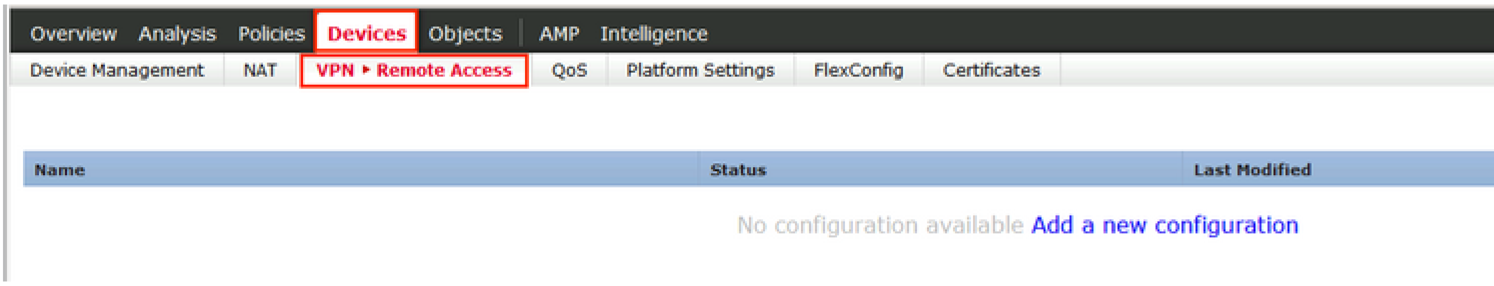
Name*	vpn-cert
Description	

Include FQDN:	Use Device Hostname as FQDN
Include Device's IP Address:	10.48.26.99
Common Name (CN):	vpn-cert.example.com
Organization Unit (OU):	
Organization (O):	example
Locality (L):	
State (ST):	Krakow
Country Code (C):	PL
Email (E):	

□ Include Device's Serial Number

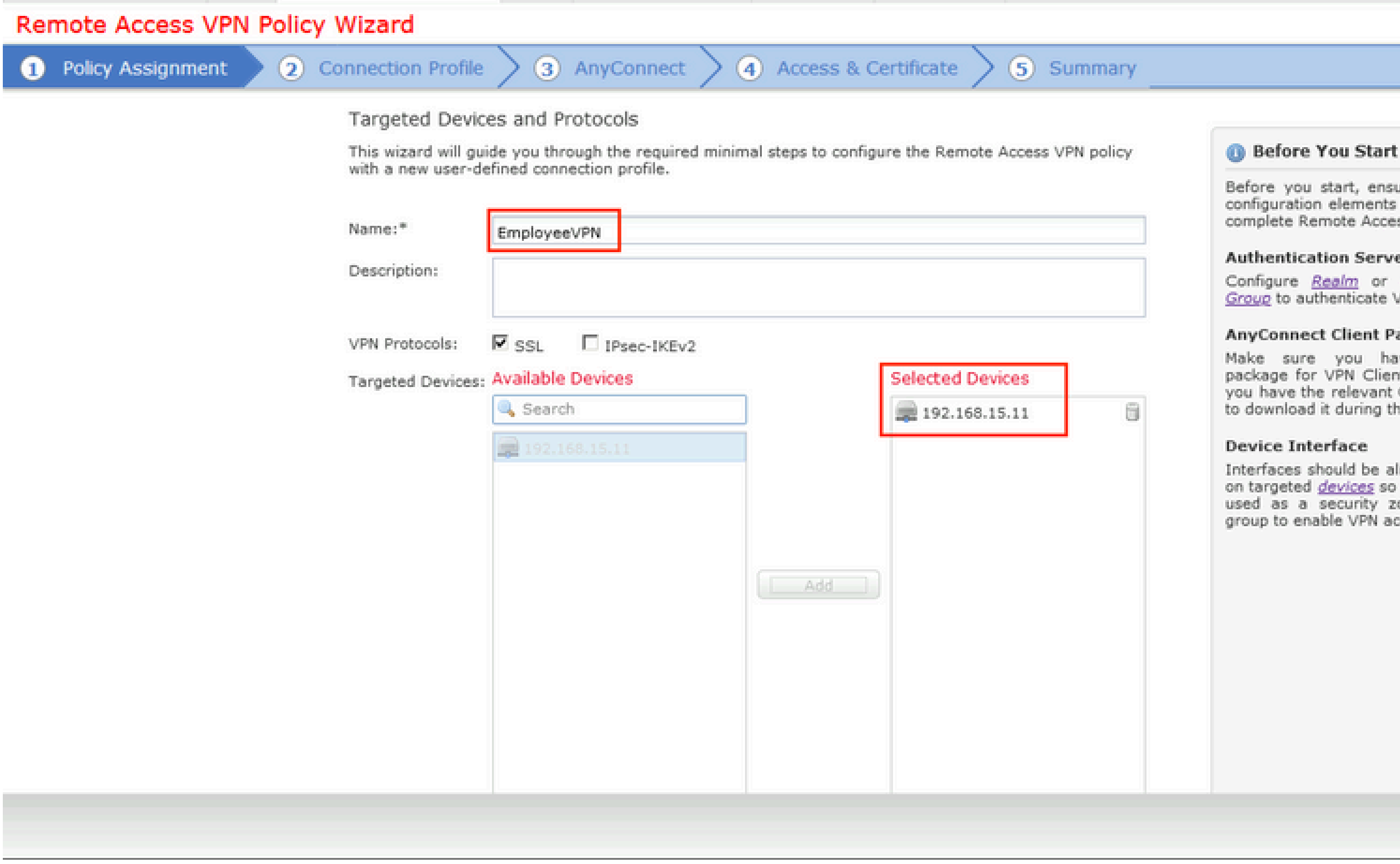
Allow Overrides □

Paso 9. Inicie el asistente para VPN de acceso remoto. Navegue hasta **Devices** > **VPN** > **Remote Access** y haga clic en **Add**.



No configuration available Add a new configuration

Paso 10. Proporcione el nombre, marque SSL como protocolo VPN, elija FTD que se utiliza como concentrador VPN y haga clic en **Next**.



Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:* EmployeeVPN

Description:

VPN Protocols: ☑ SSL □ IPsec-IKEv2

Targeted Devices: Available Devices: 192.168.15.11 — Selected Devices: 192.168.15.11

Before You Start

Before you start, ensu configuration elements complete Remote Acces

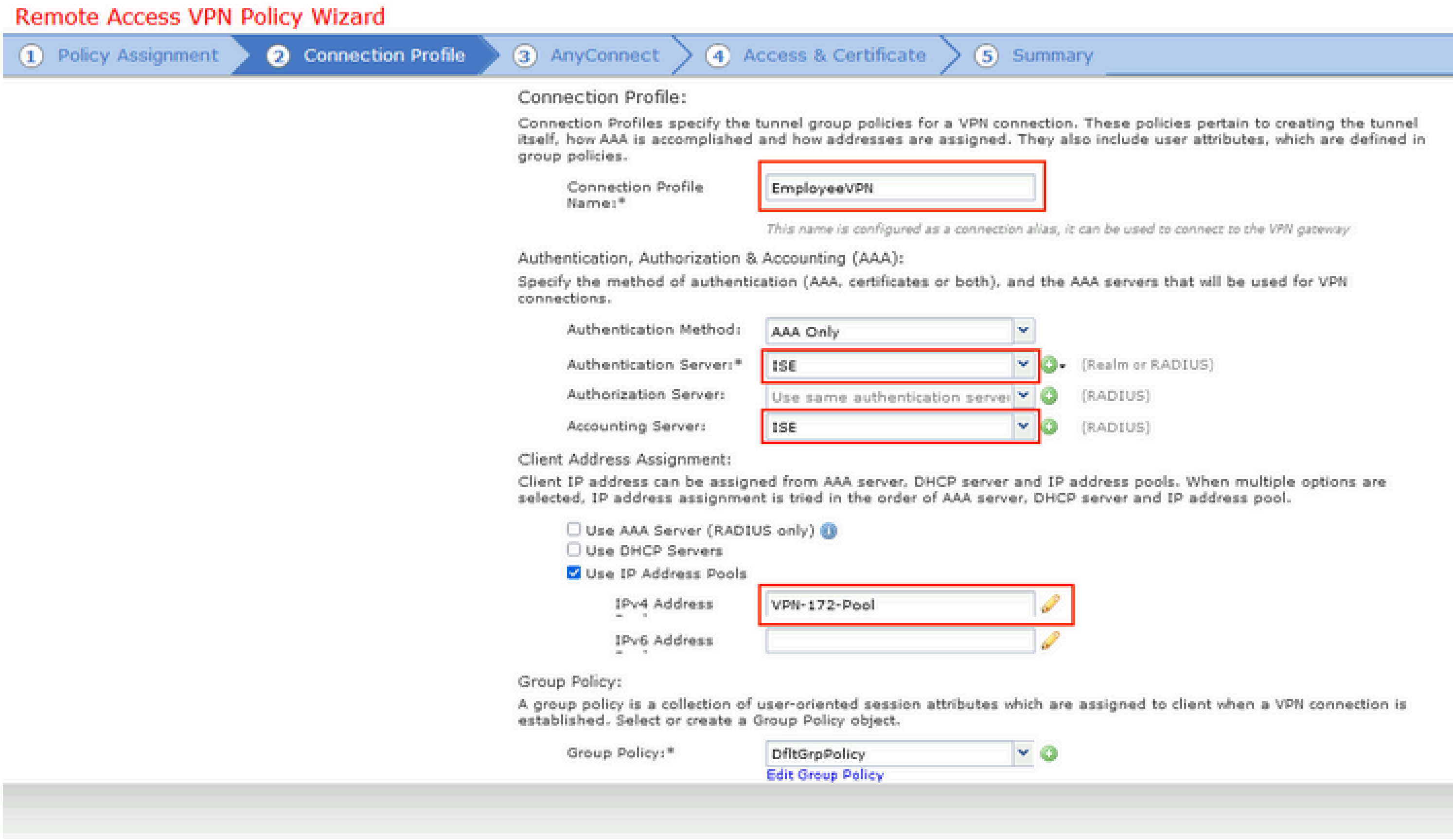
Authentication Serve
Configure Realm or Group to authenticate V

AnyConnect Client Pa
Make sure you ha package for VPN Clien you have the relevant to download it during th

Device Interface
Interfaces should be al on targeted devices so used as a security zo group to enable VPN ac

Paso 11. Proporcione el nombre del **perfil de conexión**, seleccione **Authentication/Accounting Servers**, seleccione el pool de direcciones que se configuró previamente y haga clic en **Next**.

> **Nota**: No seleccione el servidor de autorización. Activa dos solicitudes de acceso para un único usuario (una con la contraseña de usuario y la segunda con la contraseña de *cisco*).



Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* EmployeeVPN

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only

Authentication Server:* ISE (Realm or RADIUS)

Authorization Server: Use same authentication server (RADIUS)

Accounting Server: ISE (RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

☐ Use AAA Server (RADIUS only)
☐ Use DHCP Servers
☑ Use IP Address Pools

IPv4 Address Pools: VPN-172-Pool

IPv6 Address Pools:

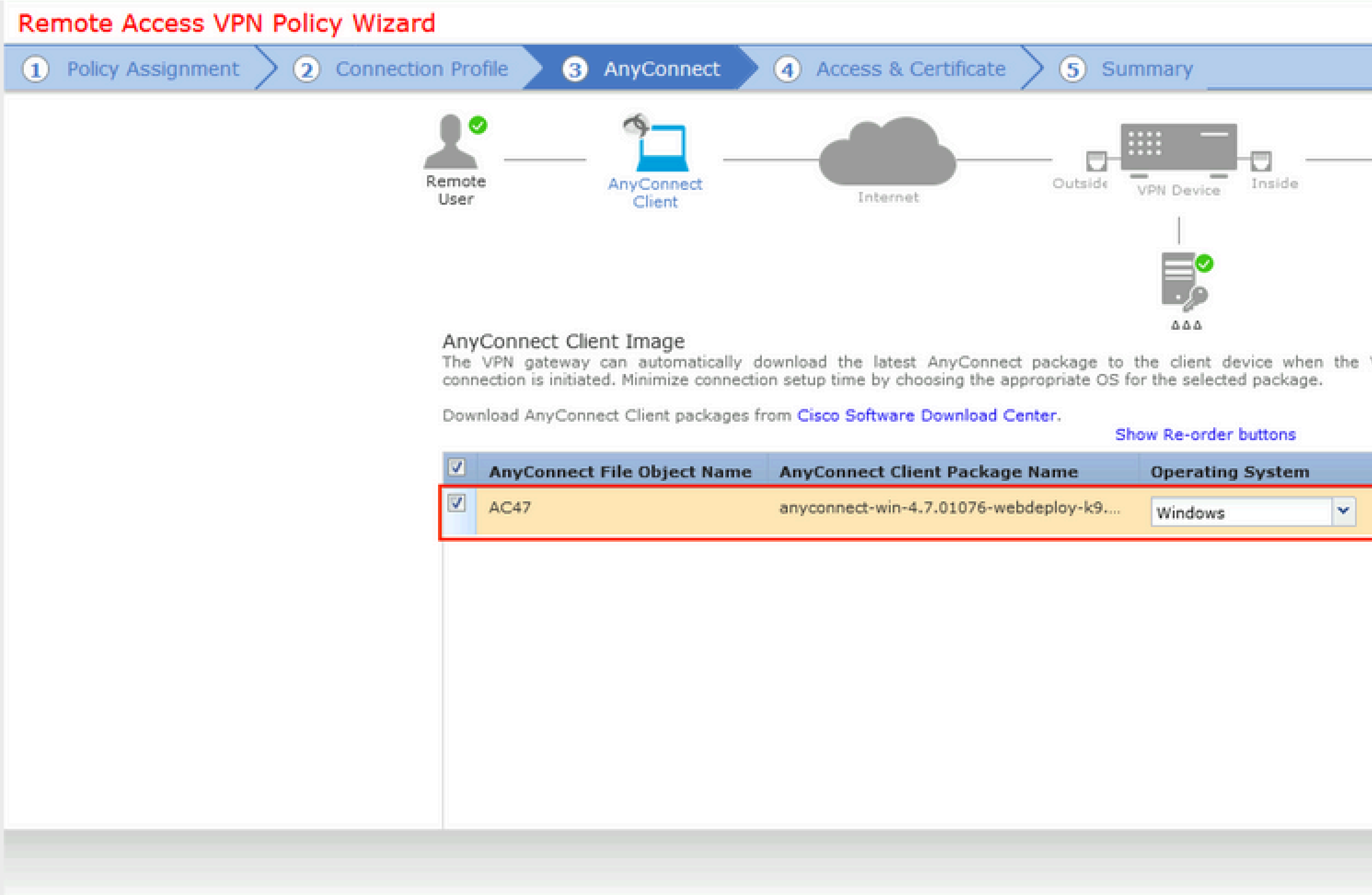
Group Policy:

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.

Group Policy:* DfltGrpPolicy

Edit Group Policy

Paso 12. Seleccione el paquete de AnyConnect que se configuró anteriormente y haga clic en **Next**.



AnyConnect Client Image

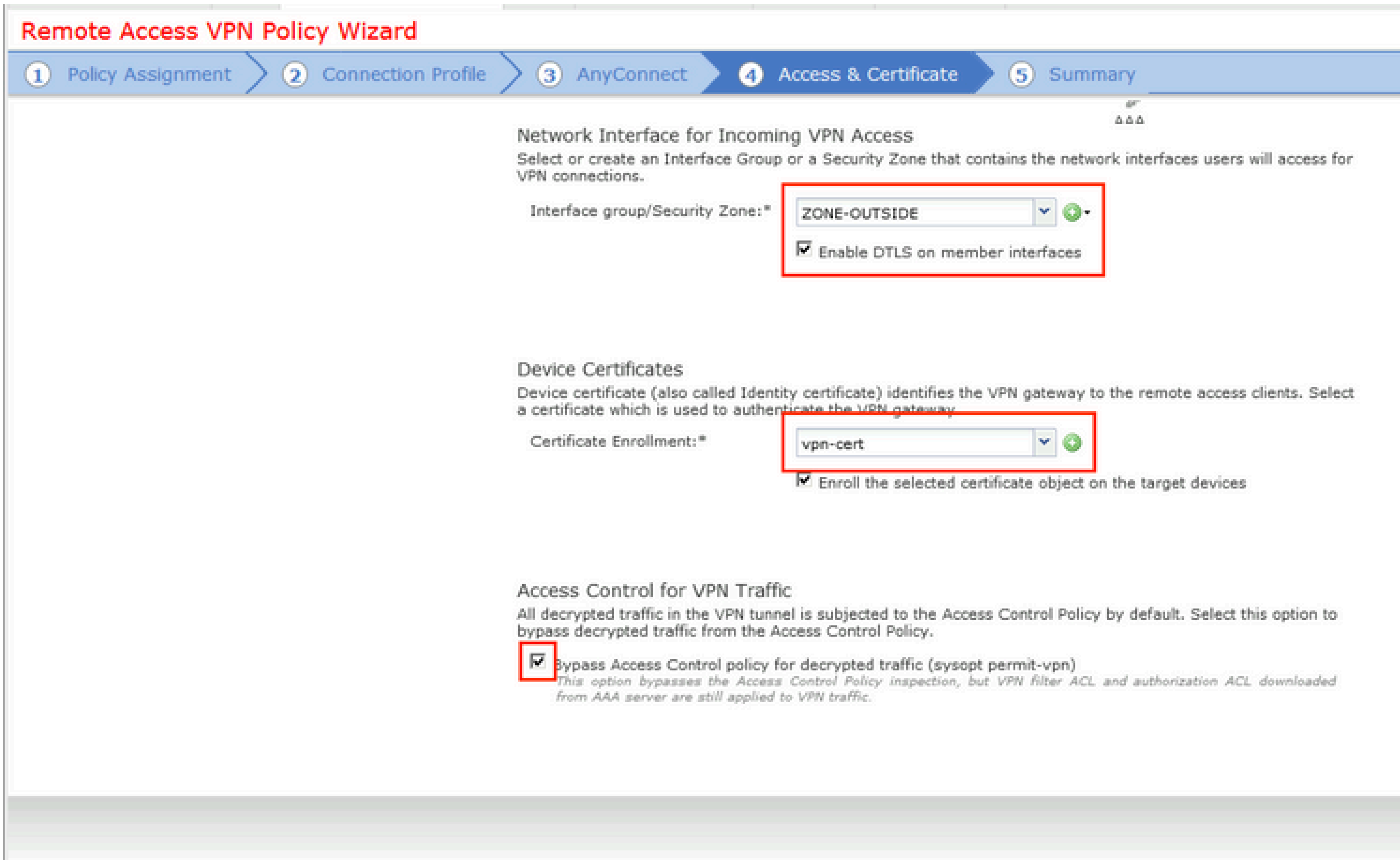
The VPN gateway can automatically download the latest AnyConnect package to the client device when the connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from Cisco Software Download Center.

Show Re-order buttons

☑	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
☑	AC47	anyconnect-win-4.7.01076-webdeploy-k9....	Windows

Paso 13. Seleccione la interfaz de la que se espera tráfico VPN, seleccione **Certificate Enrollment** que se configuró anteriormente y haga clic en **Next**.



Remote Access VPN Policy Wizard

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* ZONE-OUTSIDE

☑ Enable DTLS on member interfaces

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* vpn-cert

☑ Enroll the selected certificate object on the target devices

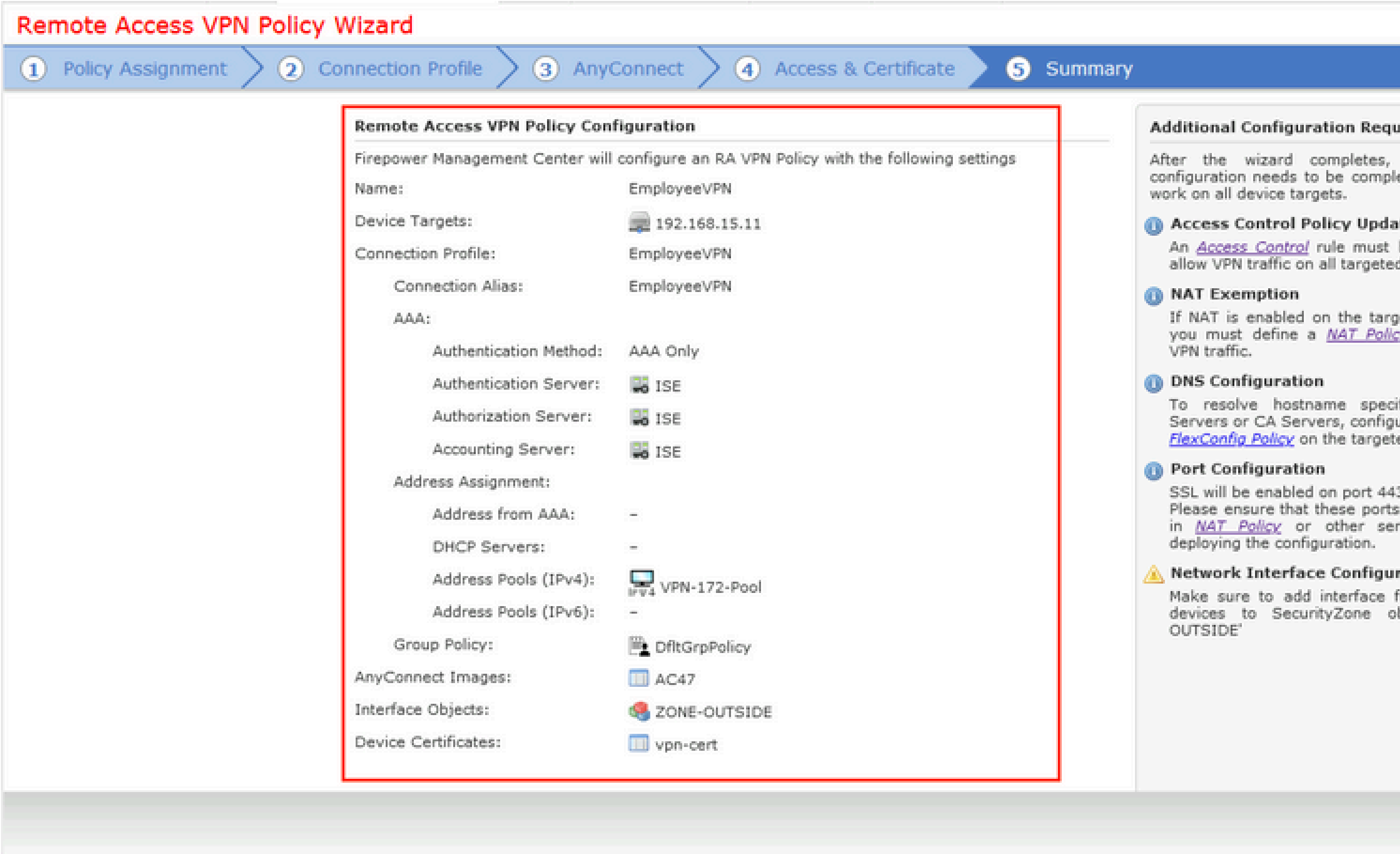
Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

☑ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Paso 14. Compruebe la página de resumen y haga clic en **Finalizar**.



Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: EmployeeVPN

Device Targets: 192.168.15.11

Connection Profile: EmployeeVPN

Connection Alias: EmployeeVPN

AAA:

Authentication Method: AAA Only

Authentication Server: ISE

Authorization Server: ISE

Accounting Server: ISE

Address Assignment:

Address from AAA: -

DHCP Servers: -

Address Pools (IPv4): VPN-172-Pool

Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images: AC47

Interface Objects: ZONE-OUTSIDE

Device Certificates: vpn-cert

Additional Configuration Requ

After the wizard completes, configuration needs to be comple work on all device targets.

Access Control Policy Upda

An Access Control rule must allow VPN traffic on all targeted

NAT Exemption

If NAT is enabled on the targ you must define a NAT Polic VPN traffic.

DNS Configuration

To resolve hostname speci Servers or CA Servers, configu FlexConfig Policy on the targete

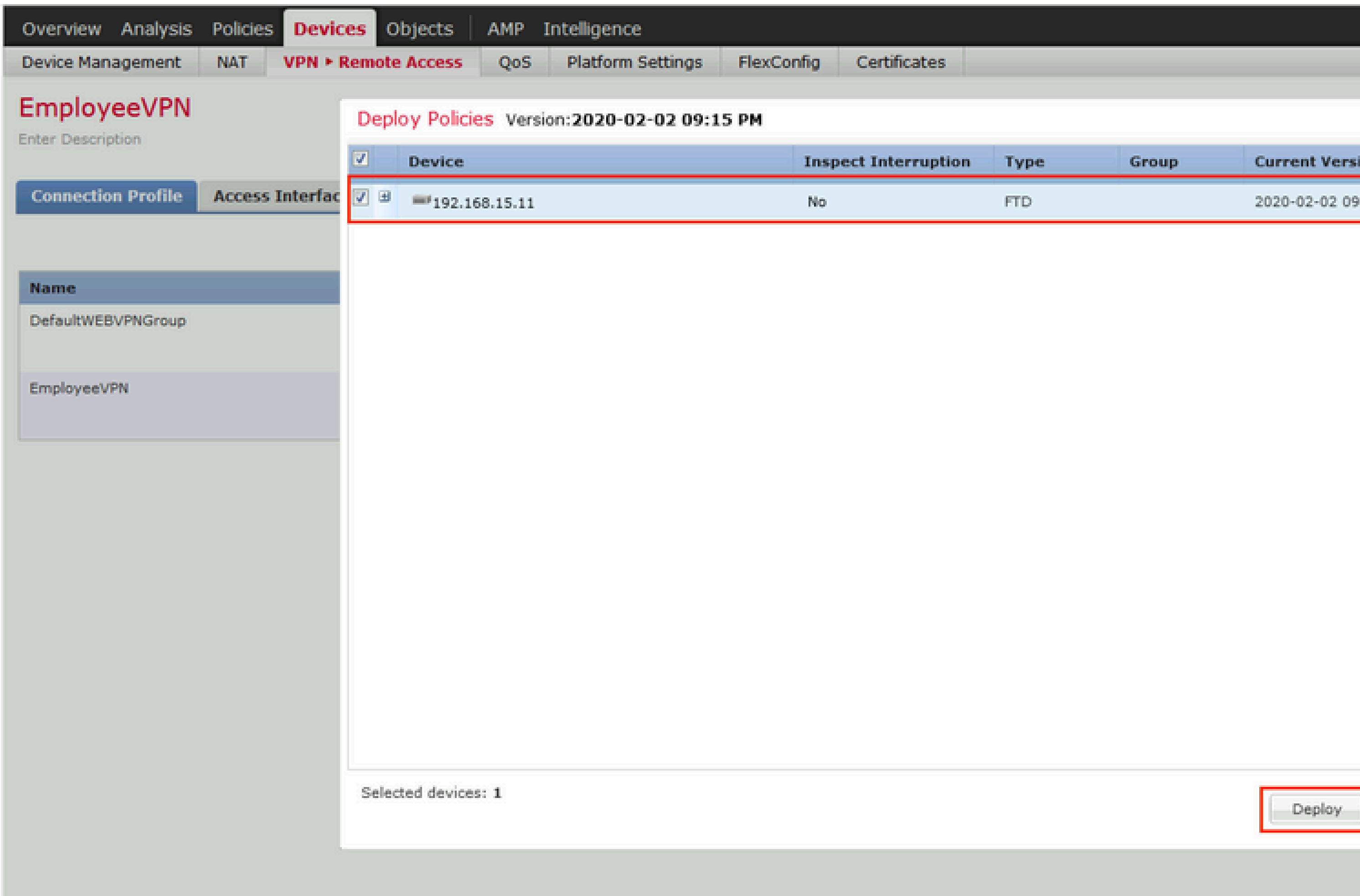
Port Configuration

SSL will be enabled on port 443 Please ensure that these ports in NAT Policy or other ser deploying the configuration.

Network Interface Configur

Make sure to add interface f devices to SecurityZone ol OUTSIDE'

Paso 15. Implemente la configuración en FTD. Haga clic en **Deploy** y seleccione **FTD** que se utiliza como concentrador VPN.



Deploy Policies Version:**2020-02-02 09:15 PM**

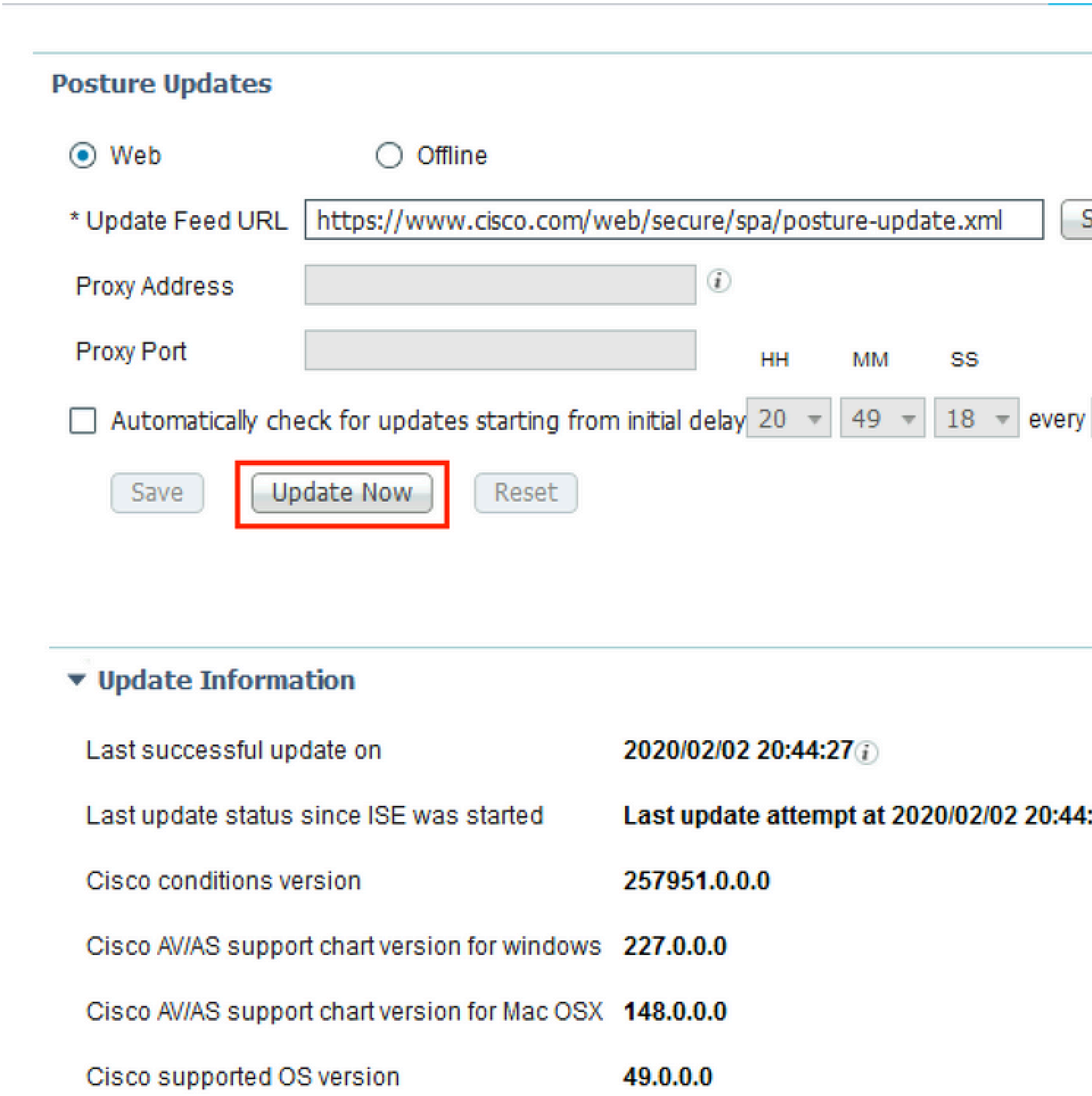
☑		Device	Inspect Interruption	Type	Group	Current Versi
☑	⊞	192.168.15.11	No	FTD		2020-02-02 09

Name
DefaultWEBVPNGroup
EmployeeVPN

Selected devices: **1**

ISE

Paso 1. Ejecutar actualizaciones de estado. Vaya a **Administration > System > Settings > Posture > Updates**.



Posture Updates

● Web ○ Offline

* Update Feed URL https://www.cisco.com/web/secure/spa/posture-update.xml

Proxy Address

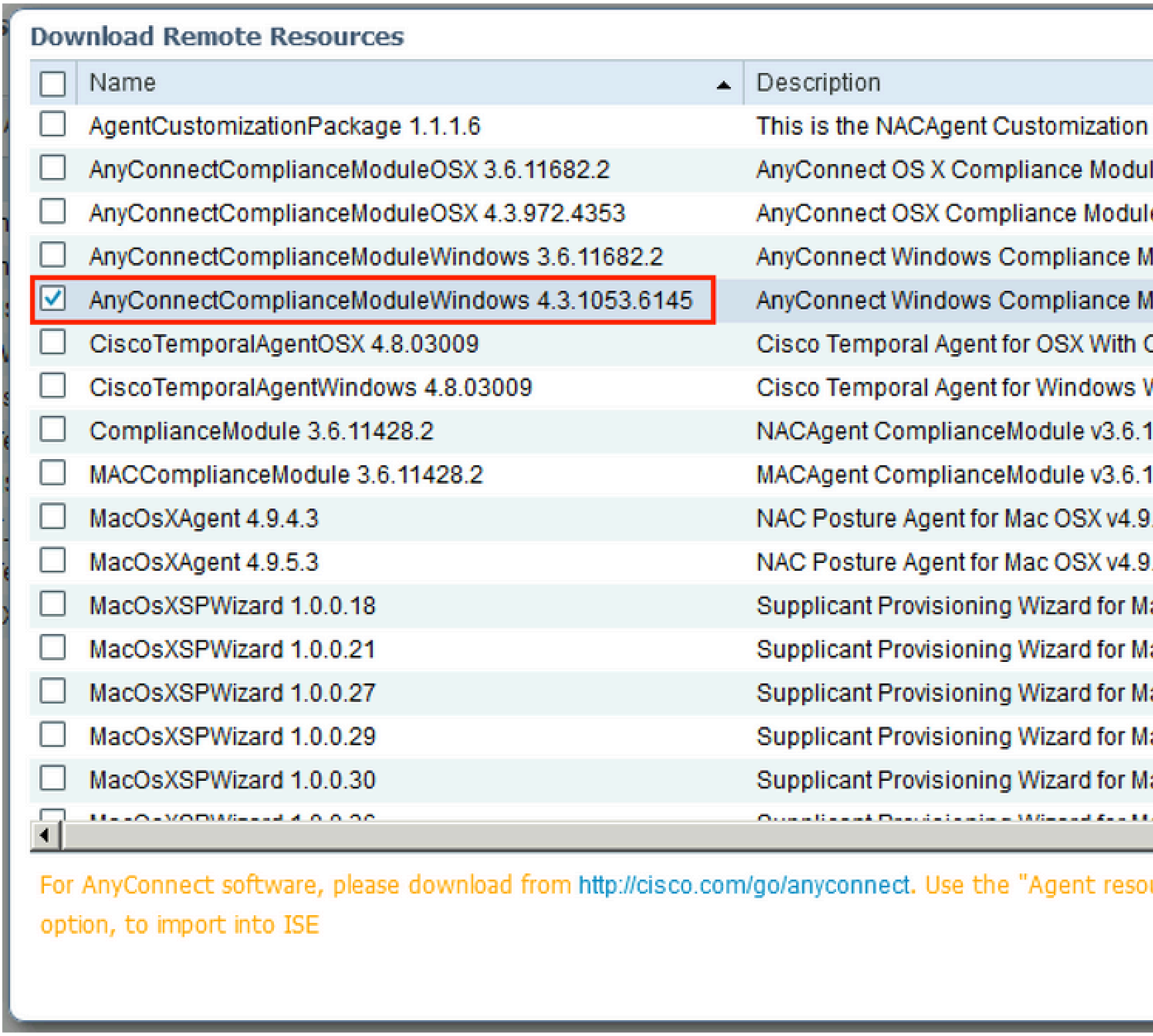
Proxy Port

□ Automatically check for updates starting from initial delay HH 20 MM 49 SS 18 every

Update Information

Last successful update on	2020/02/02 20:44:27
Last update status since ISE was started	Last update attempt at 2020/02/02 20:44:
Cisco conditions version	257951.0.0.0
Cisco AV/AS support chart version for windows	227.0.0.0
Cisco AV/AS support chart version for Mac OSX	148.0.0.0
Cisco supported OS version	49.0.0.0

Paso 2. Cargue el módulo de cumplimiento. Vaya a **Directiva** > **Elementos de directiva** > **Resultados** > **Aprovisionamiento de cliente** > **Recursos**. Haga clic en **Agregar** y seleccione **Recursos de agente del sitio de Cisco**



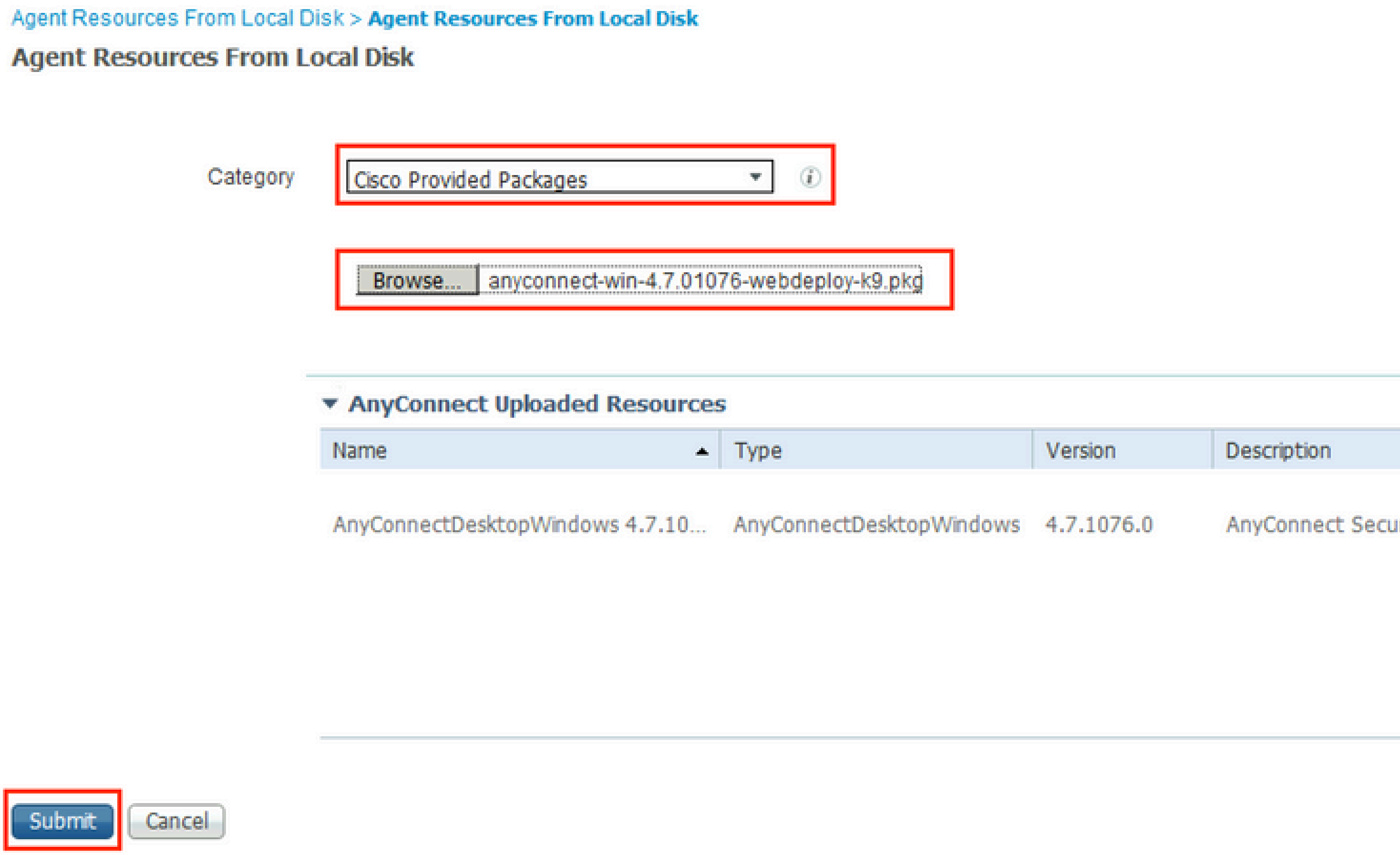
Download Remote Resources

□	Name	Description
□	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization
□	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Modul
□	AnyConnectComplianceModuleOSX 4.3.972.4353	AnyConnect OSX Compliance Modul
□	AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance M
☑	AnyConnectComplianceModuleWindows 4.3.1053.6145	AnyConnect Windows Compliance M
□	CiscoTemporalAgentOSX 4.8.03009	Cisco Temporal Agent for OSX With C
□	CiscoTemporalAgentWindows 4.8.03009	Cisco Temporal Agent for Windows W
□	ComplianceModule 3.6.11428.2	NACAgent ComplianceModule v3.6.1
□	MACComplianceModule 3.6.11428.2	MACAgent ComplianceModule v3.6.1
□	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9
□	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9
□	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Ma
□	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Ma
□	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Ma
□	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Ma
□	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Ma
□	MacOsXSPWizard 1.0.0.36	Supplicant Provisioning Wizard for Ma

For AnyConnect software, please download from http://cisco.com/go/anyconnect. Use the "Agent reso
option, to import into ISE

Paso 3. Descargue AnyConnect de [Cisco Software Download]() y cárguelo en ISE. Vaya a **Directiva > Elementos de directiva > Resultados > Aprovisionamiento de cliente > Recursos**.

Haga clic en **Add** y seleccione **Agent Resources From Local Disk**. Elija **Cisco Provided Packages** en **Category**, seleccione el paquete de AnyConnect del disco local y haga clic en **Submit**.



Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Cisco Provided Packages

Browse... anyconnect-win-4.7.01076-webdeploy-k9.pkg

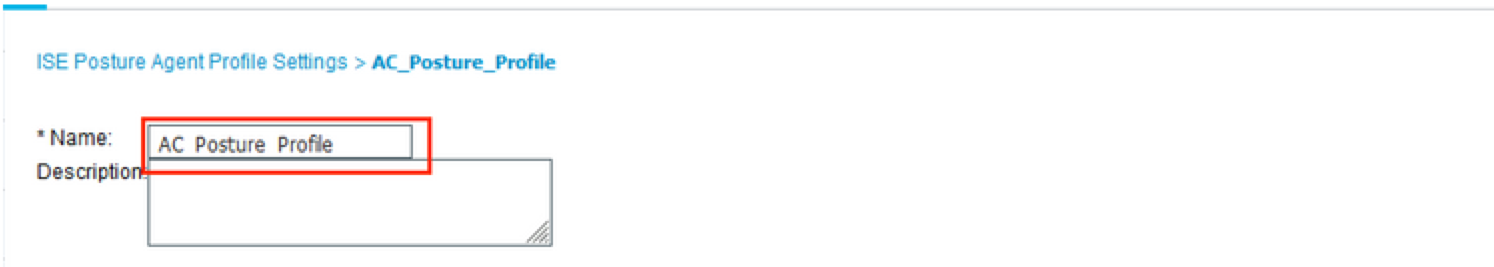
AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.7.10...	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secu

Paso 4. Crear perfil de postura de AnyConnect. Vaya a **Directiva** > **Elementos de directiva** > **Resultados** > **Aprovisionamiento de cliente** > **Recursos**.

Haga clic en **Agregar** y seleccione **Perfil de postura de AnyConnect**. Rellene el nombre y el protocolo de posición.

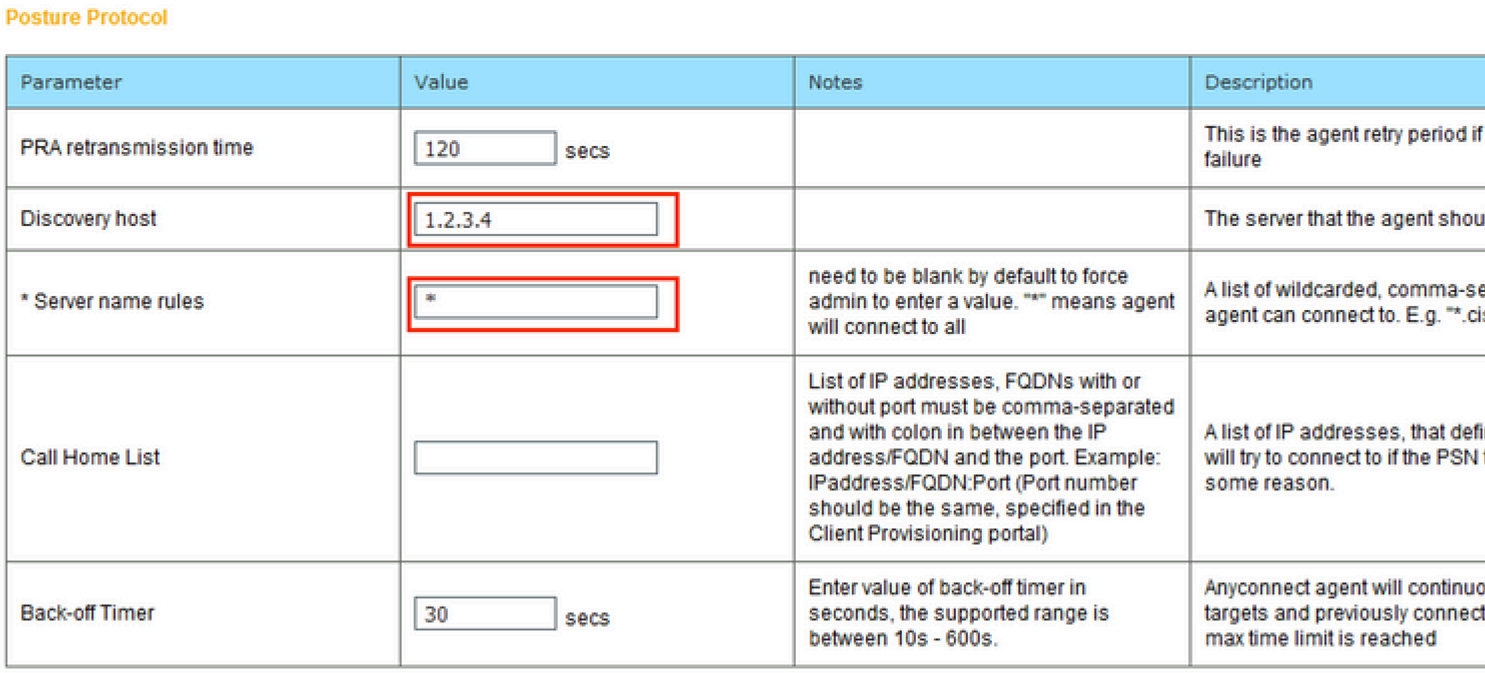
Bajo ***Server name rules** put ***** y put any dummy IP address under **Discovery host**.



ISE Posture Agent Profile Settings > AC_Posture_Profile

* Name: AC Posture Profile

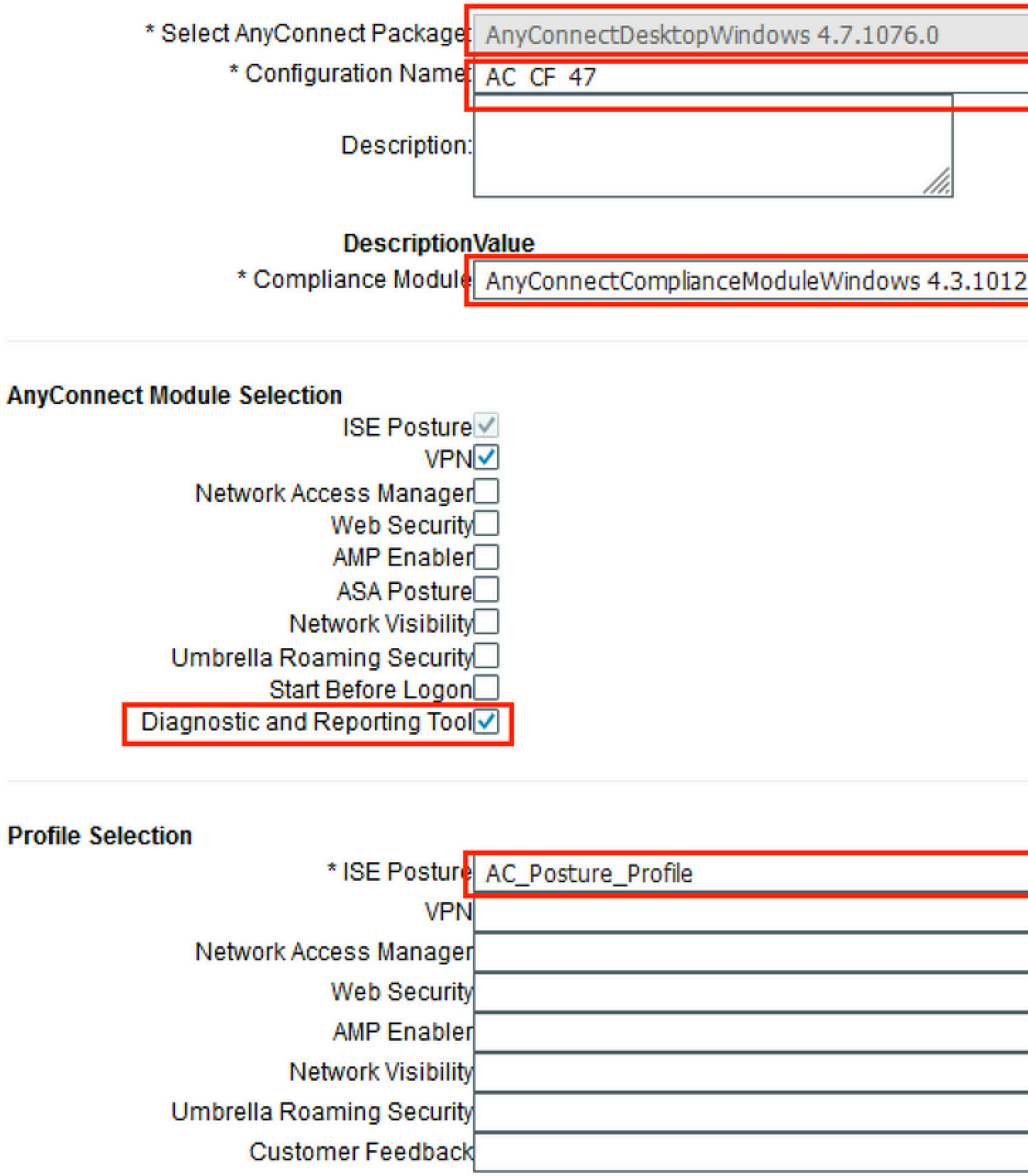
Description:



Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if failure
Discovery host	1.2.3.4		The server that the agent shou
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-se agent can connect to. E.g. "*.ci
Call Home List		List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defi will try to connect to if the PSN some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuo targets and previously connect max time limit is reached

Paso 5. Vaya a **Directiva > Elementos de directiva > Resultados > Aprovisionamiento de cliente > Recursos** y cree la **configuración de AnyConnect**. Haga clic en **Agregar** y seleccione **Configuración de AnyConnect**. Seleccione el paquete **AnyConnect**, proporcione el nombre de la configuración, seleccione el **módulo de cumplimiento**, verifique la herramienta de diagnóstico e informes, seleccione el perfil de postura y haga clic en Guardar**.**



* Select AnyConnect Package: AnyConnectDesktopWindows 4.7.1076.0

* Configuration Name: AC_CF_47

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 4.3.1012

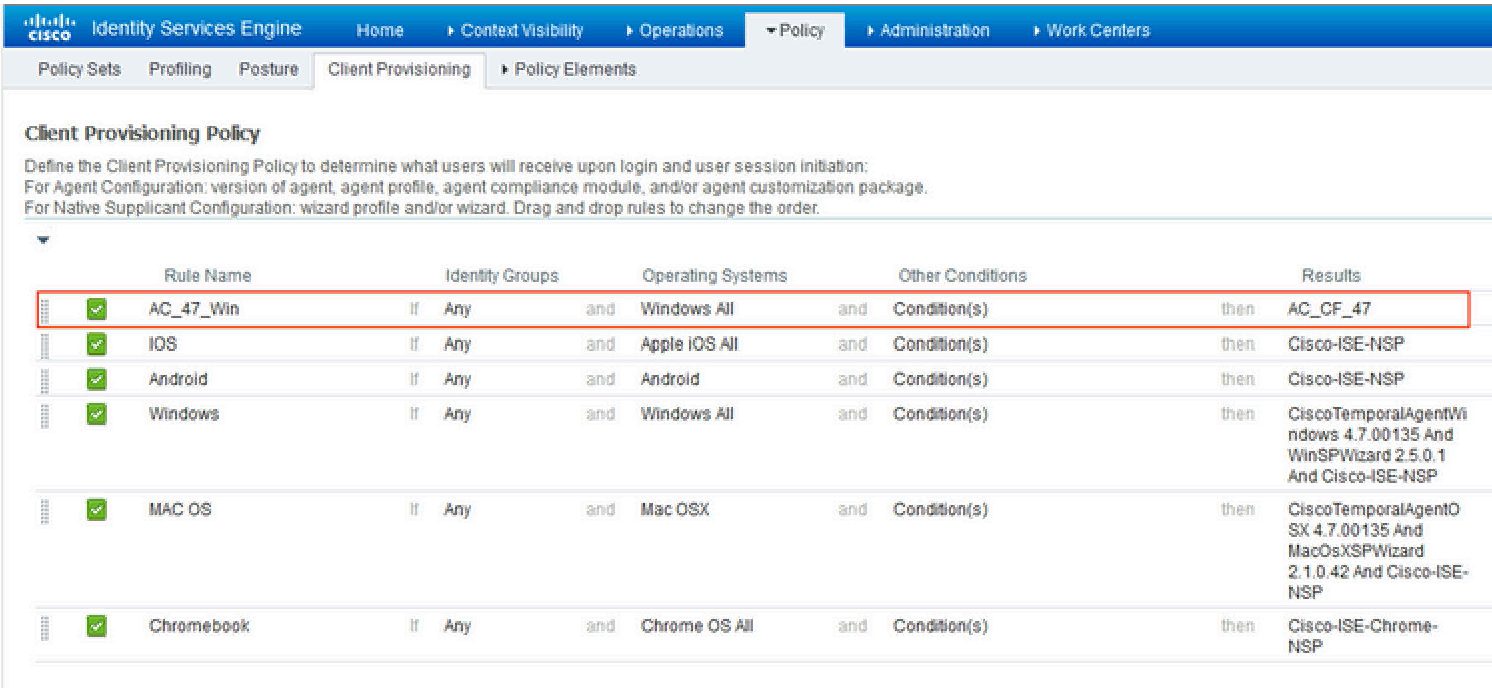
AnyConnect Module Selection

ISE Posture ☑
VPN ☑
Network Access Manager □
Web Security □
AMP Enabler □
ASA Posture □
Network Visibility □
Umbrella Roaming Security □
Start Before Logon □
Diagnostic and Reporting Tool ☑

Profile Selection

* ISE Posture: AC_Posture_Profile
VPN:
Network Access Manager:
Web Security:
AMP Enabler:
Network Visibility:
Umbrella Roaming Security:
Customer Feedback:

Paso 6. Navegue hasta **Policy > Client Provisioning** y cree **Client Provisioning Policy**. Haga clic en **Edit** y luego seleccione **Insert Rule Above**, proporcione el nombre, seleccione OS y elija **AnyConnect Configuration** que se creó en el paso anterior.



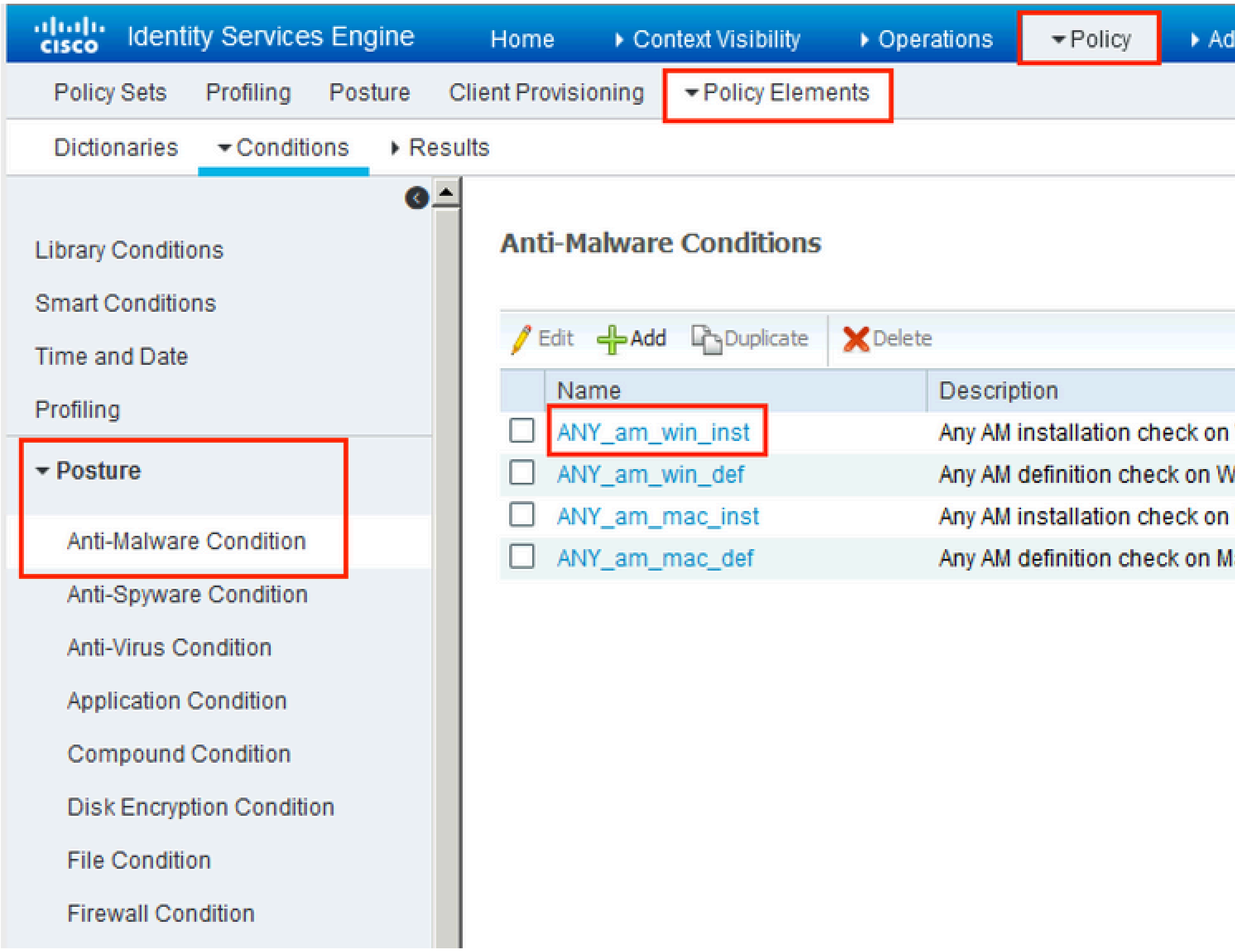
Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	AC_47_Win	If	Any	and	Windows All	and	Condition(s)	then	AC_CF_47
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	Cisco-ISE-NSP
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP
☑	Windows	If	Any	and	Windows All	and	Condition(s)	then	CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
☑	MAC OS	If	Any	and	Mac OSX	and	Condition(s)	then	CiscoTemporalAgentOSX 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE-NSP
☑	Chromebook	If	Any	and	Chrome OS All	and	Condition(s)	then	Cisco-ISE-Chrome-NSP

Paso 7. Cree la condición de postura en **Política** > **Elementos de política** > **Condiciones** > **Condición** > **Condición** > **Condición anti-malware**. En este ejemplo, se utiliza "ANY_am_win_inst" predefinido.

.

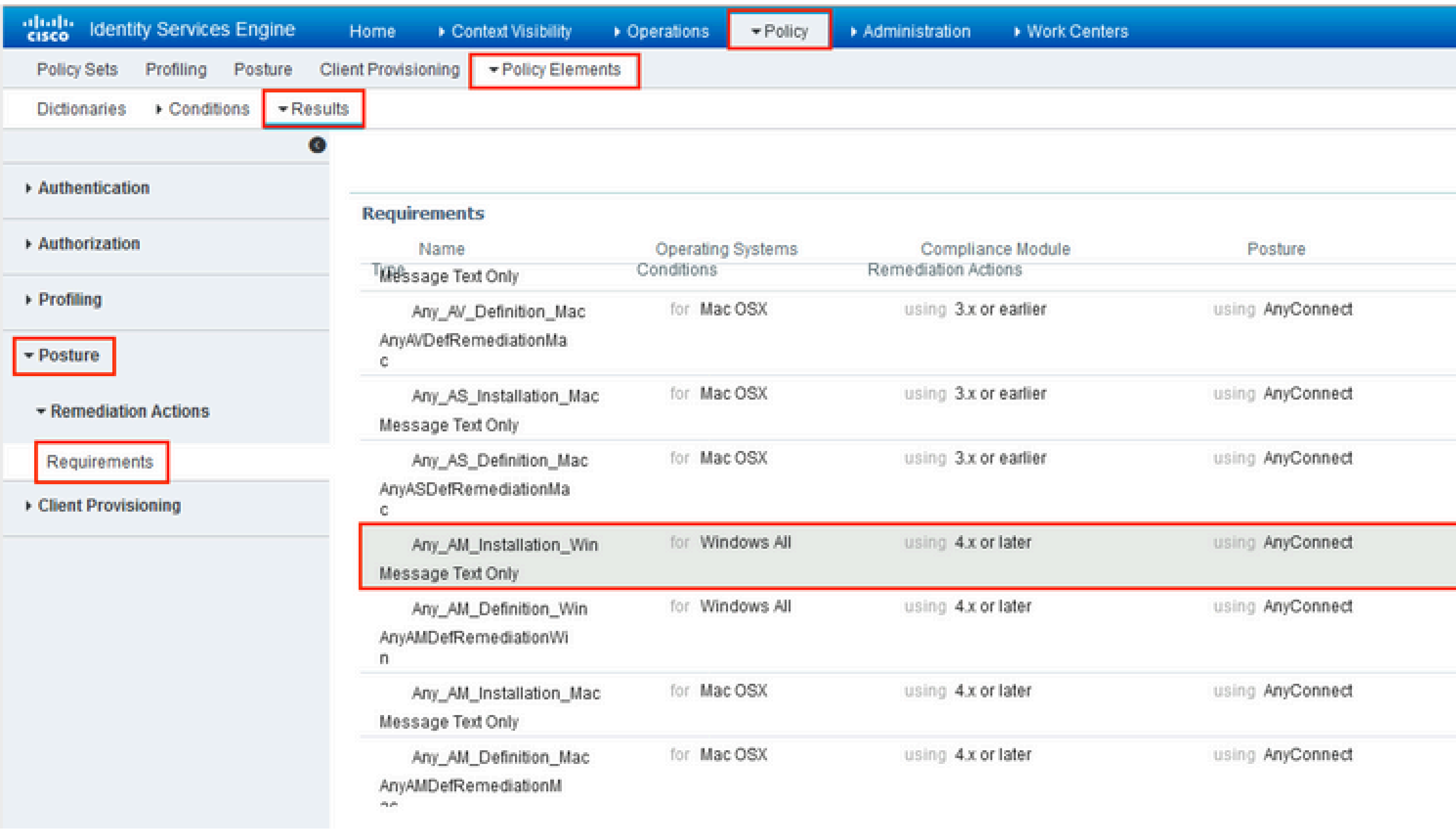


Anti-Malware Conditions

	Name	Description
☐	ANY_am_win_inst	Any AM installation check on
☐	ANY_am_win_def	Any AM definition check on W
☐	ANY_am_mac_inst	Any AM installation check on
☐	ANY_am_mac_def	Any AM definition check on M

Paso 8. Navegue hasta **Política** > **Elementos de política** > **Resultados** > **Postura** > **Acciones de remediación** y cree **remediación de postura**. En este ejemplo, se omite. La acción de remediación puede ser un mensaje de texto.

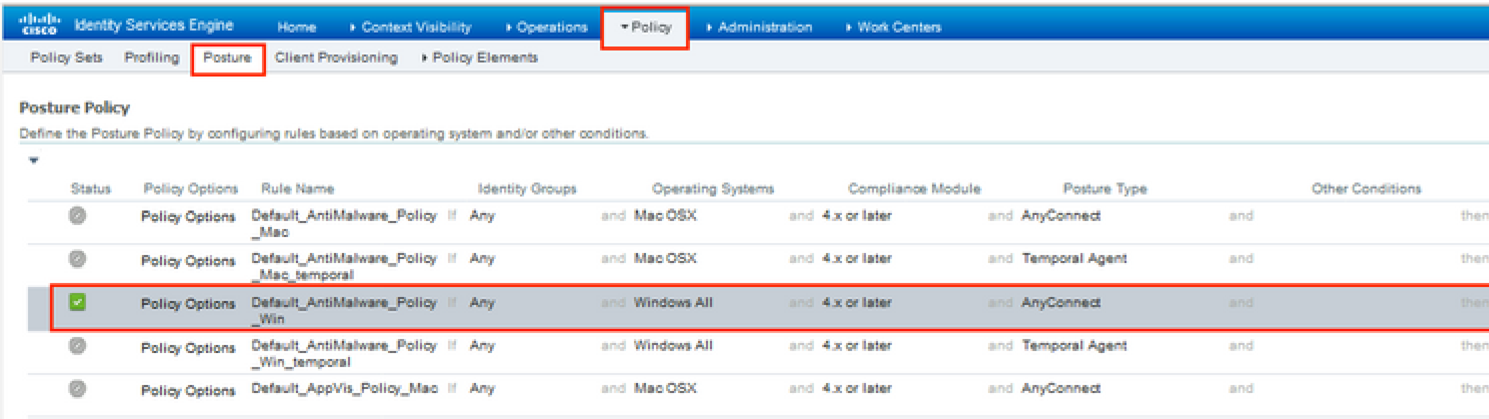
Paso 9. Navegue hasta **Política** > **Elementos de Política** > **Resultados** > **Postura** > **Requisitos** y cree **Requisitos de Postura**. Requisito predefinido Se utiliza Any_AM_Installation_Win.



Requirements

Name Remediation Actions		Operating Systems		Compliance Module		Posture
Any_AV_Definition_Mac AnyAVDefRemediationMac	for	Mac OSX	using	3.x or earlier	using	AnyConnect
Any_AS_Installation_Mac Message Text Only	for	Mac OSX	using	3.x or earlier	using	AnyConnect
Any_AS_Definition_Mac AnyASDefRemediationMac	for	Mac OSX	using	3.x or earlier	using	AnyConnect
Any_AM_Installation_Win Message Text Only	for	Windows All	using	4.x or later	using	AnyConnect
Any_AM_Definition_Win AnyAMDefRemediationWin	for	Windows All	using	4.x or later	using	AnyConnect
Any_AM_Installation_Mac Message Text Only	for	Mac OSX	using	4.x or later	using	AnyConnect
Any_AM_Definition_Mac AnyAMDefRemediationMac	for	Mac OSX	using	4.x or later	using	AnyConnect

Paso 10. Cree políticas de postura en **Políticas** > **Postura**. Se utiliza la política de estado predeterminada para cualquier comprobación de AntiMalware para el SO Windows.



Posture Policy

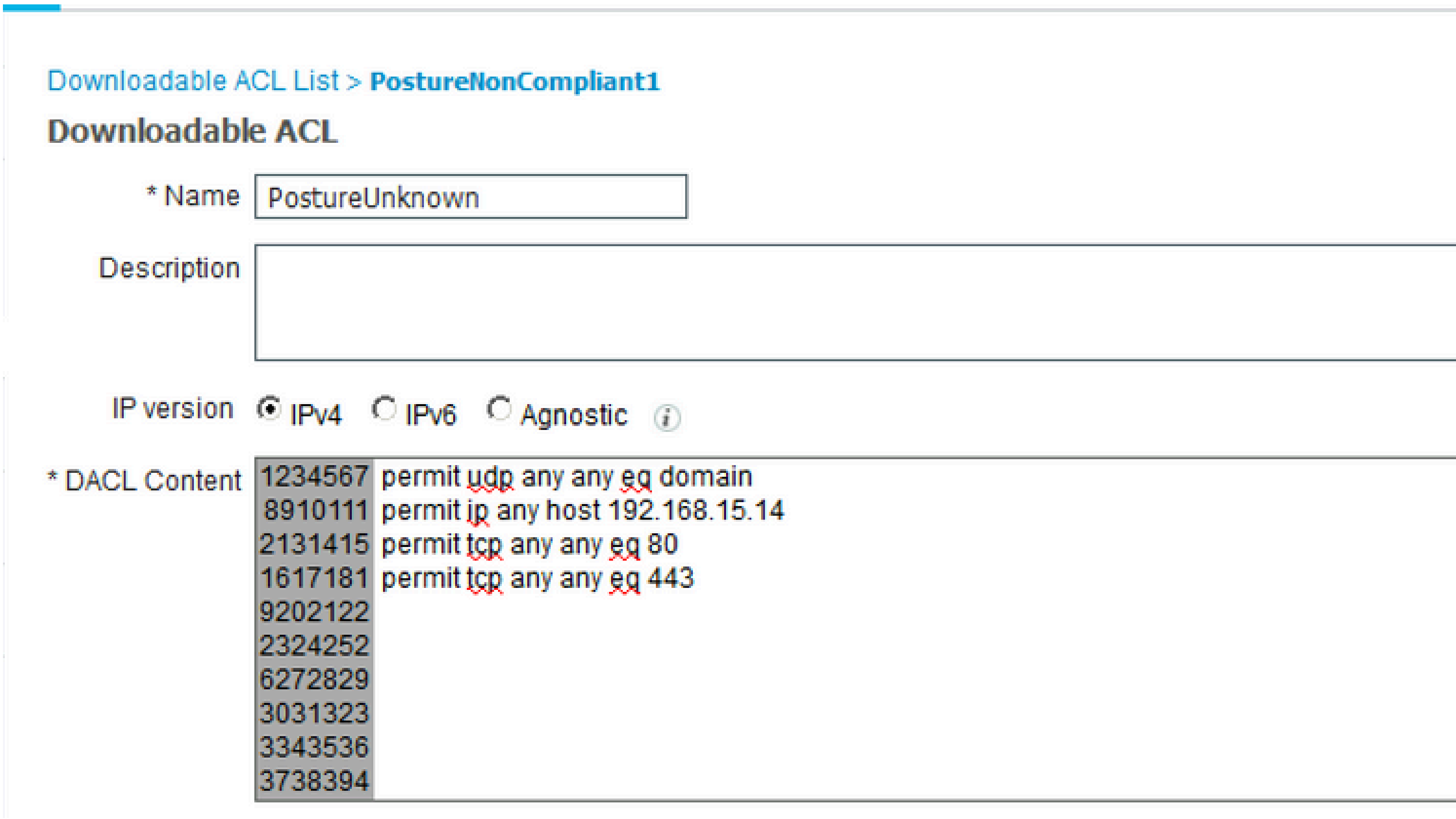
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions	
○	Policy Options	Default_AntiMalware_Policy_Mac	If	Any	and	Mac OSX	and	4.x or later	and	AnyConnect	and		then
○	Policy Options	Default_AntiMalware_Policy_Mac_temporal	If	Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and		then
✓	Policy Options	Default_AntiMalware_Policy_Win	If	Any	and	Windows All	and	4.x or later	and	AnyConnect	and		then
○	Policy Options	Default_AntiMalware_Policy_Win_temporal	If	Any	and	Windows All	and	4.x or later	and	Temporal Agent	and		then
○	Policy Options	Default_AppVis_Policy_Mac	If	Any	and	Mac OSX	and	4.x or later	and	AnyConnect	and		then

Paso 11. Navegue hasta **Política** > **Elementos de política** > **Resultados** > **Autorización** > **ACL descargables y** cree DACL para diferentes estados de estado.

En este ejemplo:

- DACL de estado desconocido: permite el tráfico a DNS, PSN y HTTP y HTTPS.
- DACL de condición no conforme: deniega el acceso a las subredes privadas y permite únicamente el tráfico de Internet.
- Permitir todas las DACL: permite todo el tráfico para el estado de cumplimiento de condición.



Downloadable ACL List > **PostureNonCompliant1**

Downloadable ACL

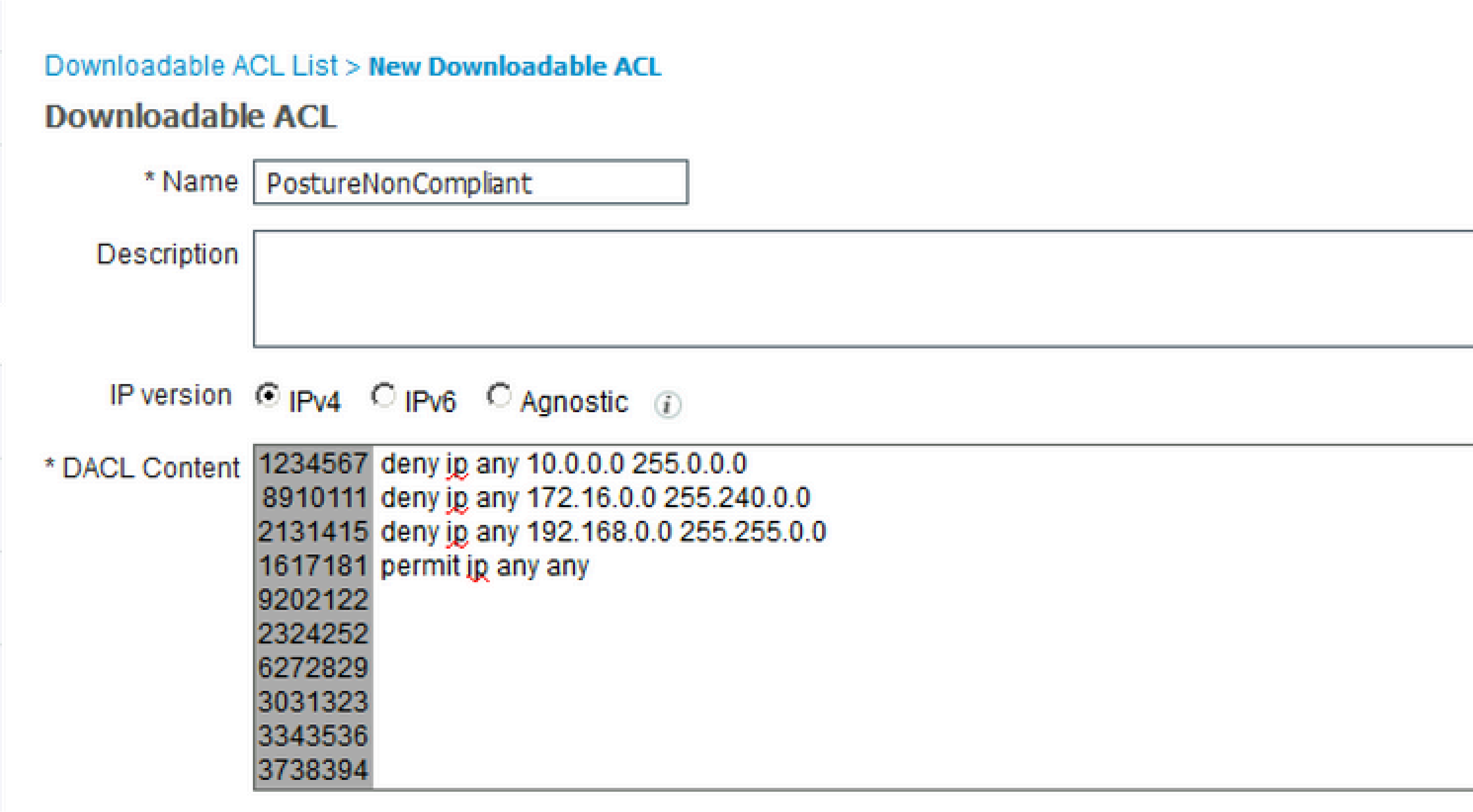
* Name: PostureUnknown

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit udp any any eq domain
permit ip any host 192.168.15.14
permit tcp any any eq 80
permit tcp any any eq 443
```



Downloadable ACL List > **New Downloadable ACL**

Downloadable ACL

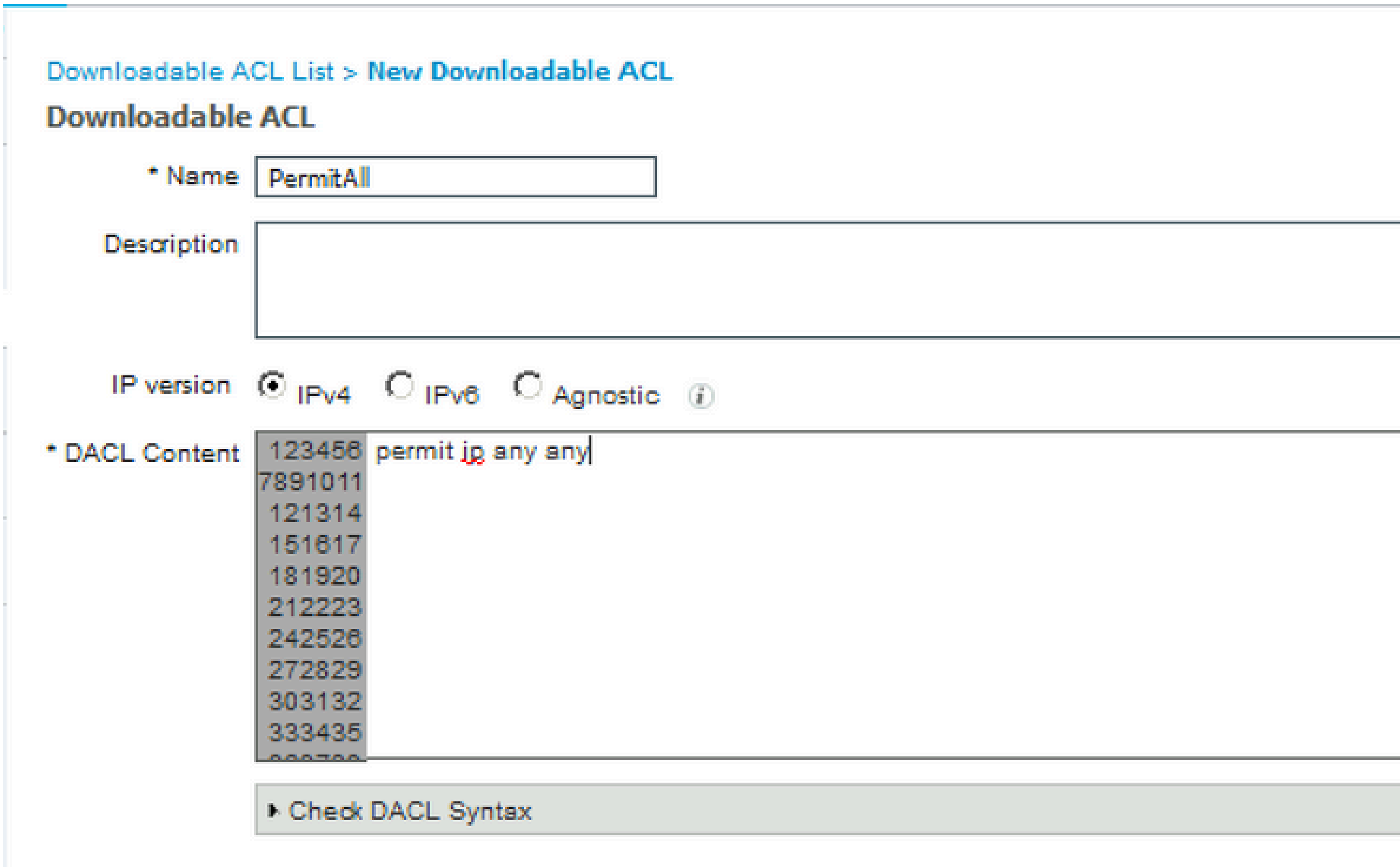
* Name: PostureNonCompliant

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
deny ip any 10.0.0.0 255.0.0.0
deny ip any 172.16.0.0 255.240.0.0
deny ip any 192.168.0.0 255.255.0.0
permit ip any any
```



Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name: PermitAll

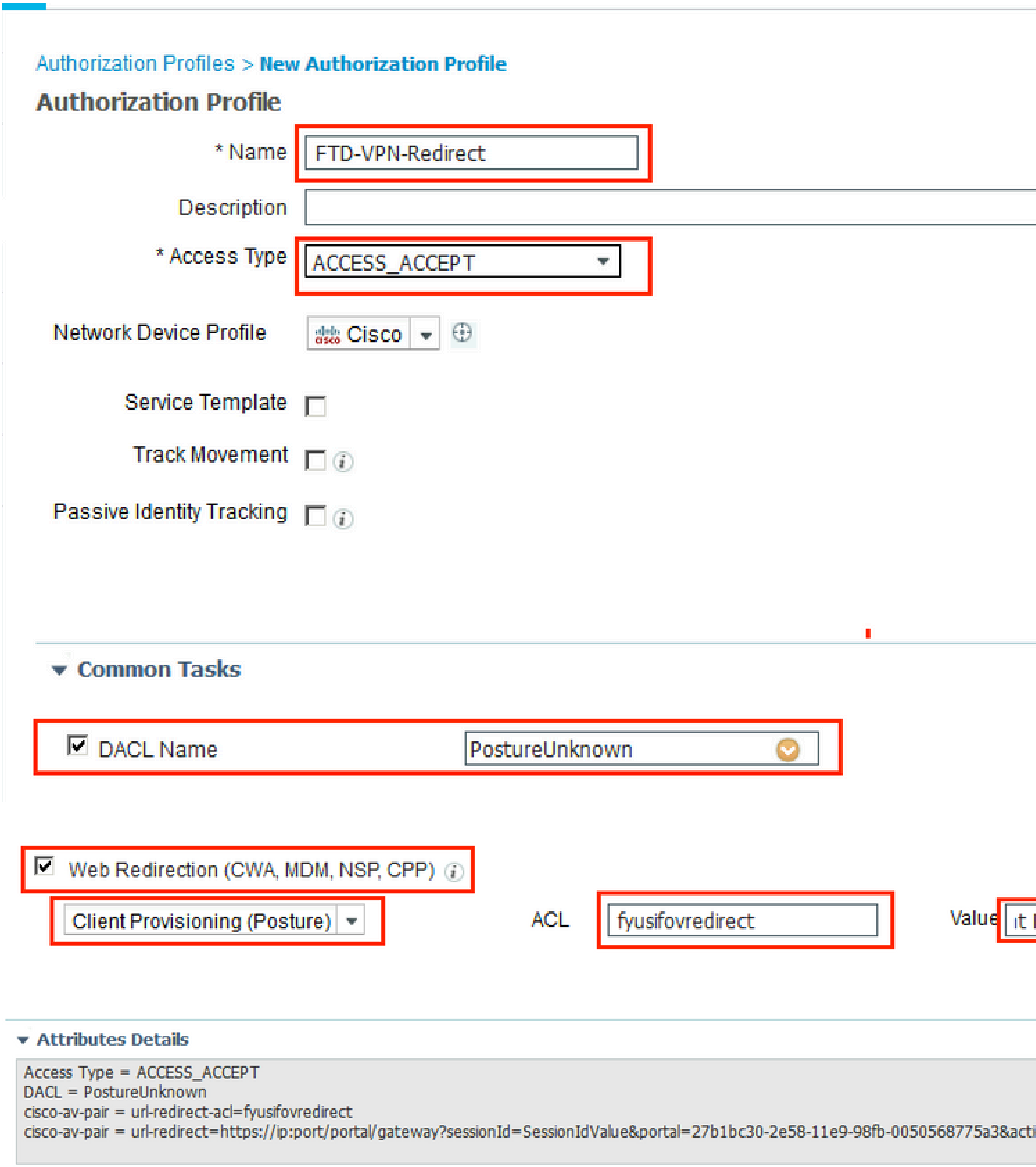
Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
123456 permit ip any any
7891011
121314
151617
181920
212223
242526
272829
303132
333435
```

Paso 12. Cree tres perfiles de autorización para los estados Postura desconocida, Postura no conforme y Postura conforme. Para hacerlo, navegue hasta **Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización**. En el perfil **Posture Unknown**, seleccione **Posture Unknown DACL**, verifique **Web Redirection**, seleccione **Client Provisioning**, proporcione un nombre de ACL de redirección (que se configura en FTD) y seleccione el portal.



Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name: FTD-VPN-Redirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

☑ DACL Name: PostureUnknown

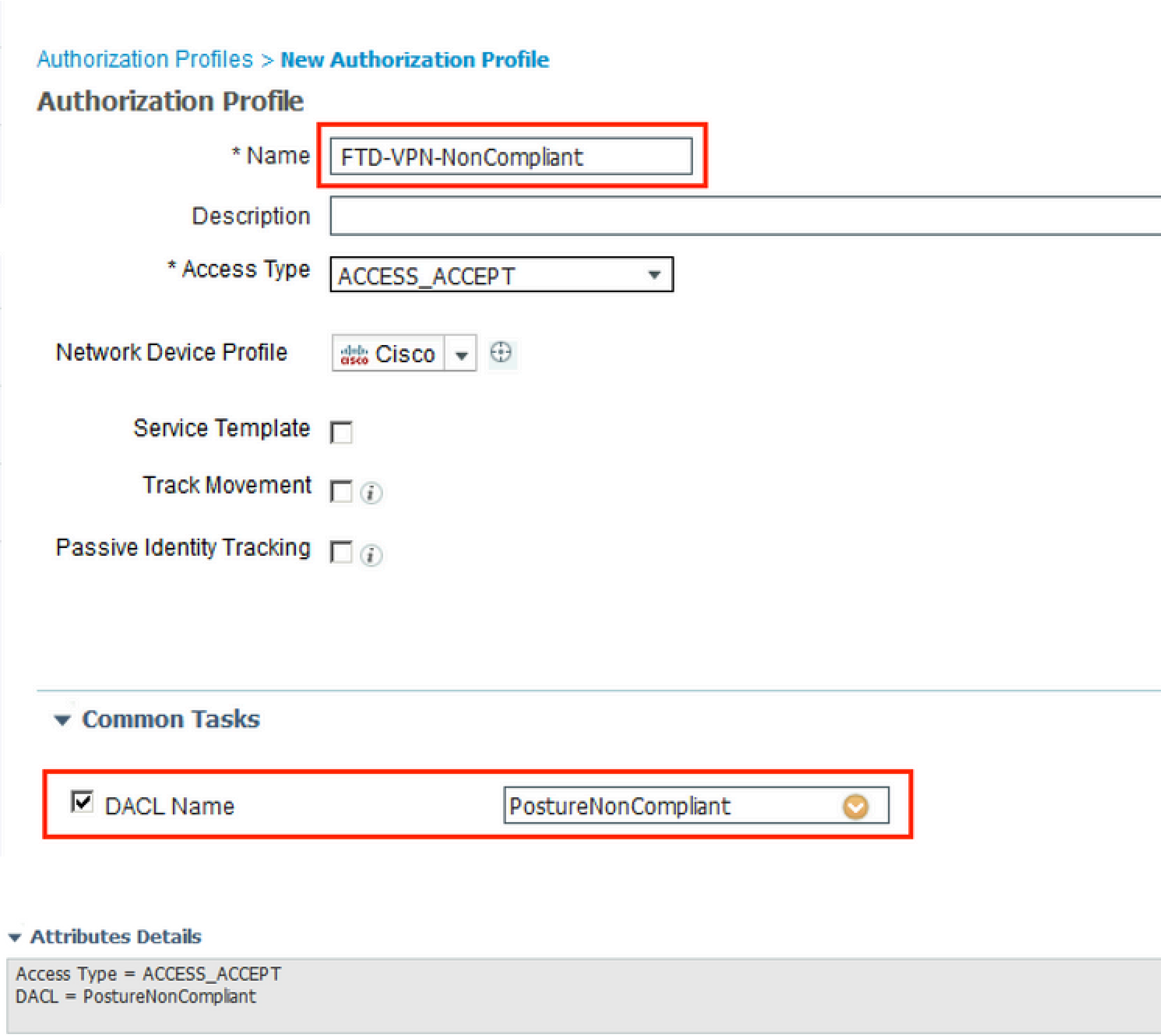
☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: fyusifovredirect Value: it

Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = PostureUnknown
cisco-av-pair = url-redirect-acl=fyusifovredirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&acti
```

En el perfil **Posture NonCompliant**, seleccione **DACL** para limitar el acceso a la red.



Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name: FTD-VPN-NonCompliant

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

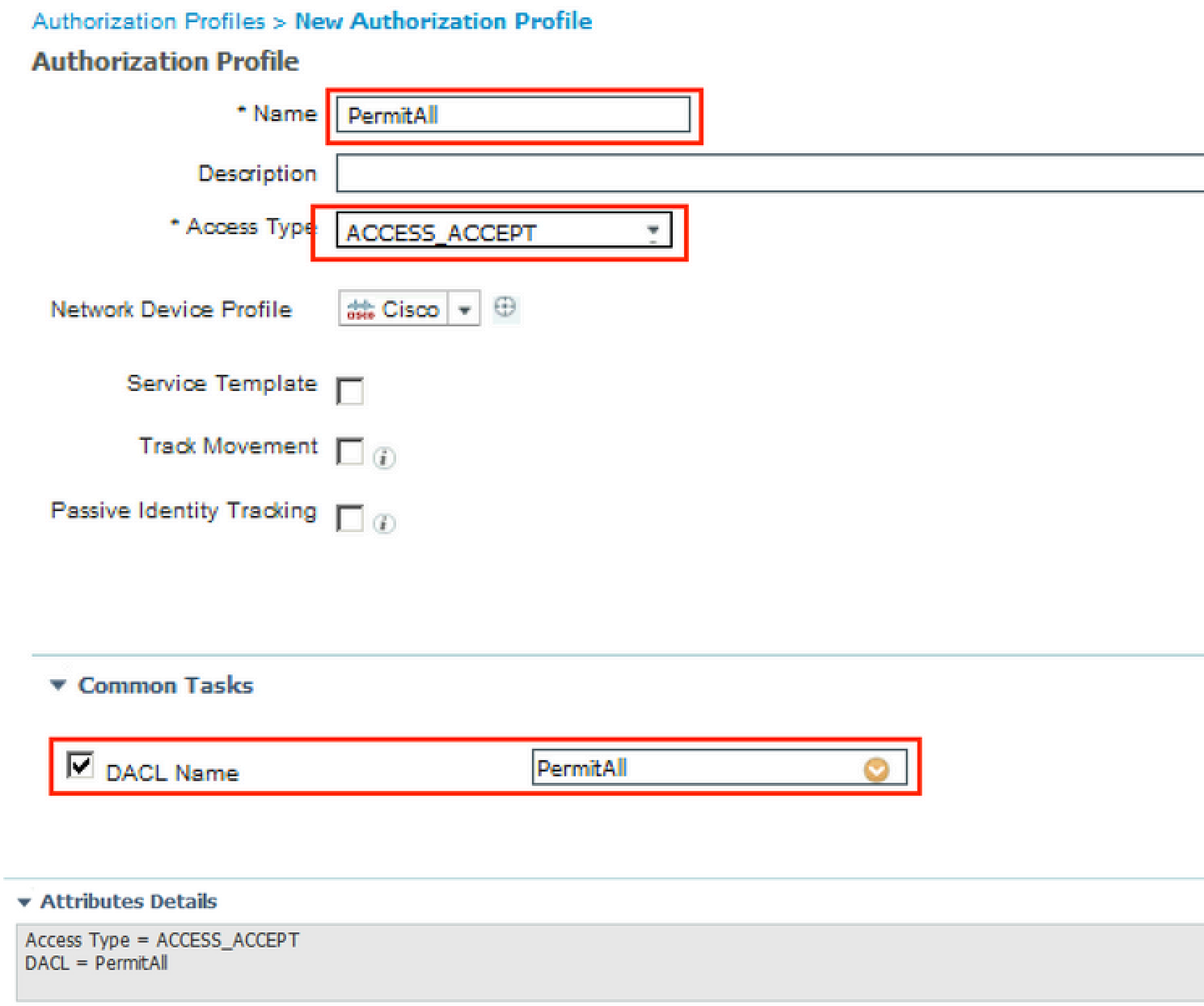
Common Tasks

☑ DACL Name: PostureNonCompliant

Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = PostureNonCompliant
```

En el perfil **Posture Compliant**, seleccione **DACL** para permitir el acceso completo a la red.


Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: PermitAll

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

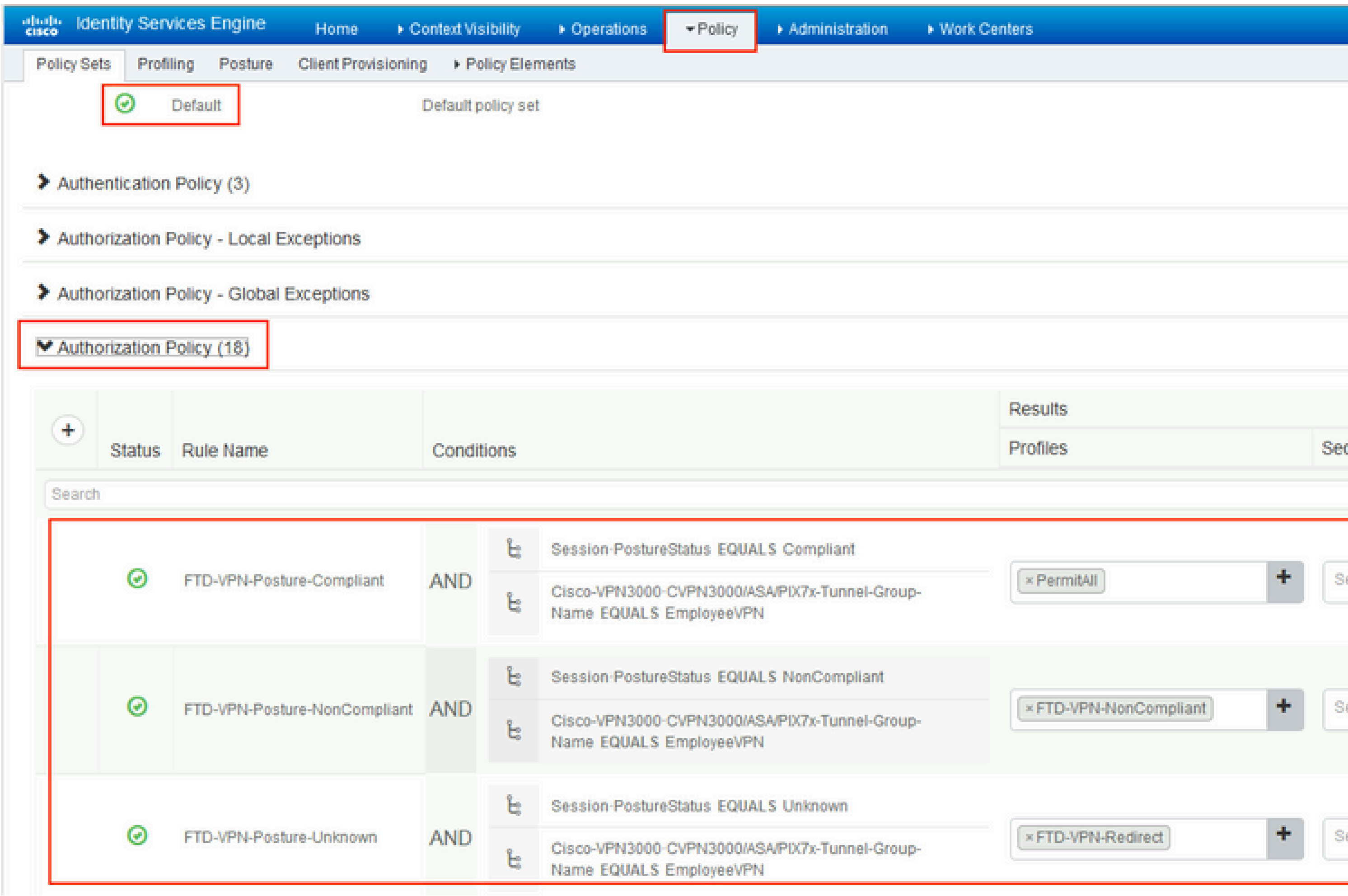
Common Tasks

☑ DACL Name: PermitAll

Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = PermitAll
```

Paso 13. Cree Políticas de Autorización en **Política** > **Conjuntos de Políticas** > **Predeterminado** > **Política de Autorización**. Como condición se utiliza Estado de postura y Nombre de grupo de túnel VPN.



Default — Default policy set

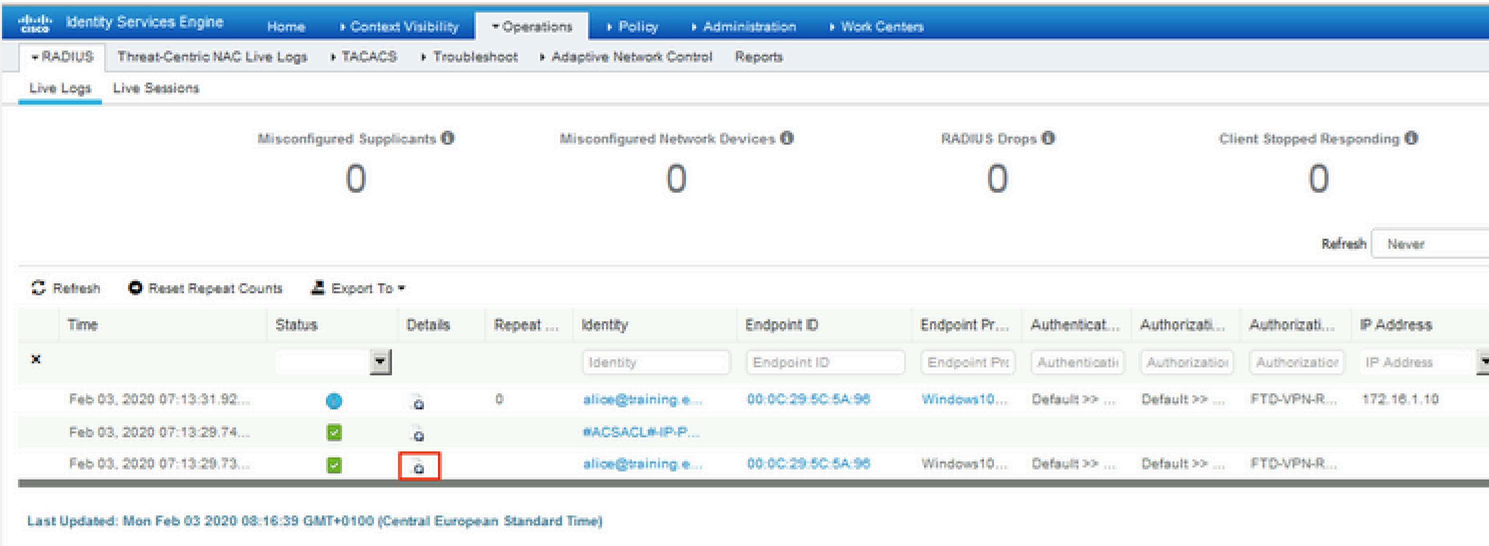
- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (18)

Status	Rule Name	Conditions		Profiles
✓	FTD-VPN-Posture-Compliant	AND	Session·PostureStatus EQUALS Compliant Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	PermitAll
✓	FTD-VPN-Posture-NonCompliant	AND	Session·PostureStatus EQUALS NonCompliant Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	FTD-VPN-NonCompliant
✓	FTD-VPN-Posture-Unknown	AND	Session·PostureStatus EQUALS Unknown Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	FTD-VPN-Redirect

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

En ISE, el primer paso de verificación es RADIUS Live Log. Vaya a **Operaciones > Registro de actividad de RADIUS**. Aquí, el usuario Alice está conectado y se selecciona la política de autorización esperada.



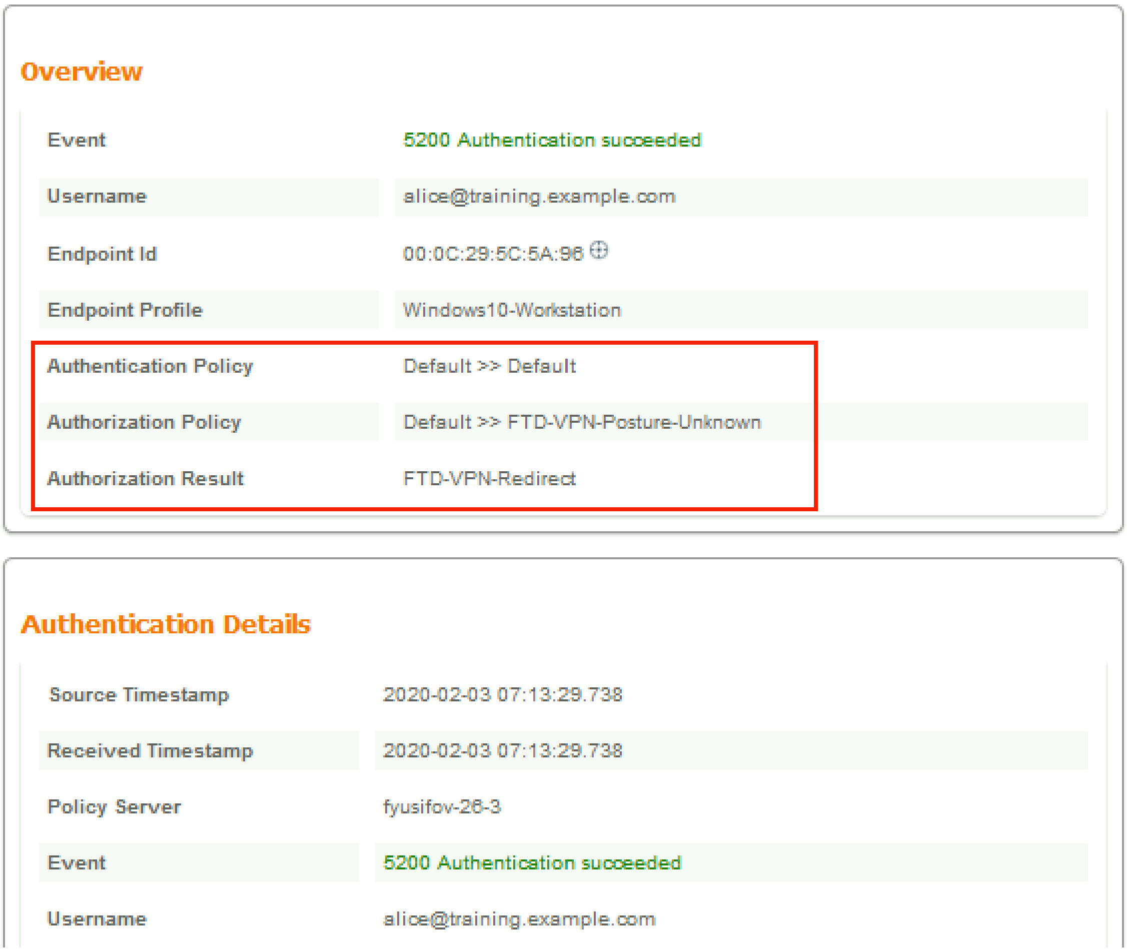
Misconfigured Supplicants 0 · Misconfigured Network Devices 0 · RADIUS Drops 0 · Client Stopped Responding 0

Refresh: Never

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizati...	Authorizati...	IP Address
Feb 03, 2020 07:13:31.92...	●		0	alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...	172.16.1.10
Feb 03, 2020 07:13:29.74...	✓			#ACSACL#-IP-P...						
Feb 03, 2020 07:13:29.73...	✓			alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...	

Last Updated: Mon Feb 03 2020 08:16:39 GMT+0100 (Central European Standard Time)

La política de autorización FTD-VPN-Posture-Unknown coincide y, como resultado, FTD-VPN-Profile se envía a FTD.



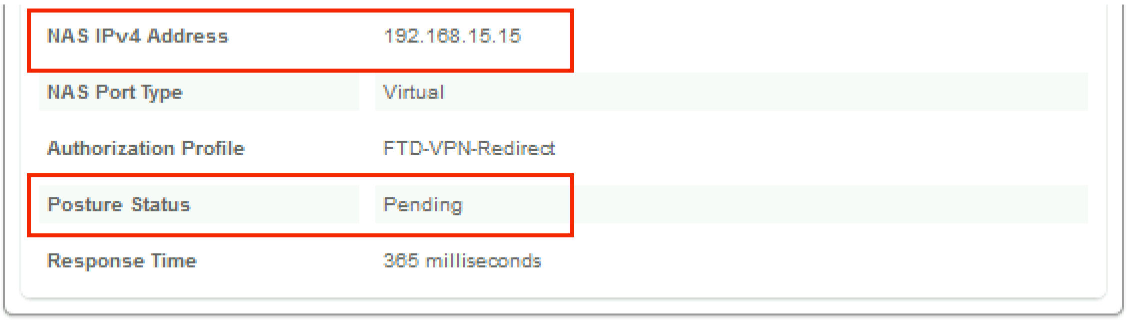
Overview

Event	5200 Authentication succeeded
Username	alice@training.example.com
Endpoint Id	00:0C:29:5C:5A:96 ⊕
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> FTD-VPN-Posture-Unknown
Authorization Result	FTD-VPN-Redirect

Authentication Details

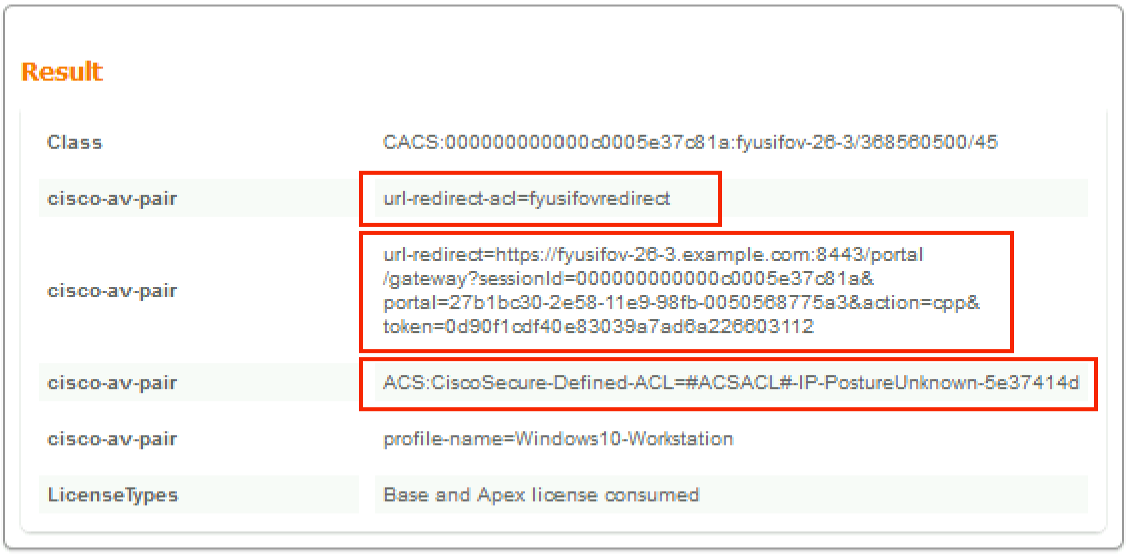
Source Timestamp	2020-02-03 07:13:29.738
Received Timestamp	2020-02-03 07:13:29.738
Policy Server	fyusifov-26-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

Estado de estado pendiente.



NAS IPv4 Address	192.168.15.15
NAS Port Type	Virtual
Authorization Profile	FTD-VPN-Redirect
Posture Status	Pending
Response Time	365 milliseconds

La sección Resultado muestra qué atributos se envían al FTD.



Result

Class	CACS:000000000000c0005e37c81a:fyusifov-26-3/368560500/45
cisco-av-pair	url-redirect-acl=fyusifovredirect

cisco-av-pair	url-redirect=https://fyusifov-26-3.example.com:8443/portal
	/gateway?sessionId=000000000000c0005e37c81a&
	portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp&
	token=0d90f1cdf40e83039a7ad6a226603112

cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PostureUnknown-5e37414d
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base and Apex license consumed

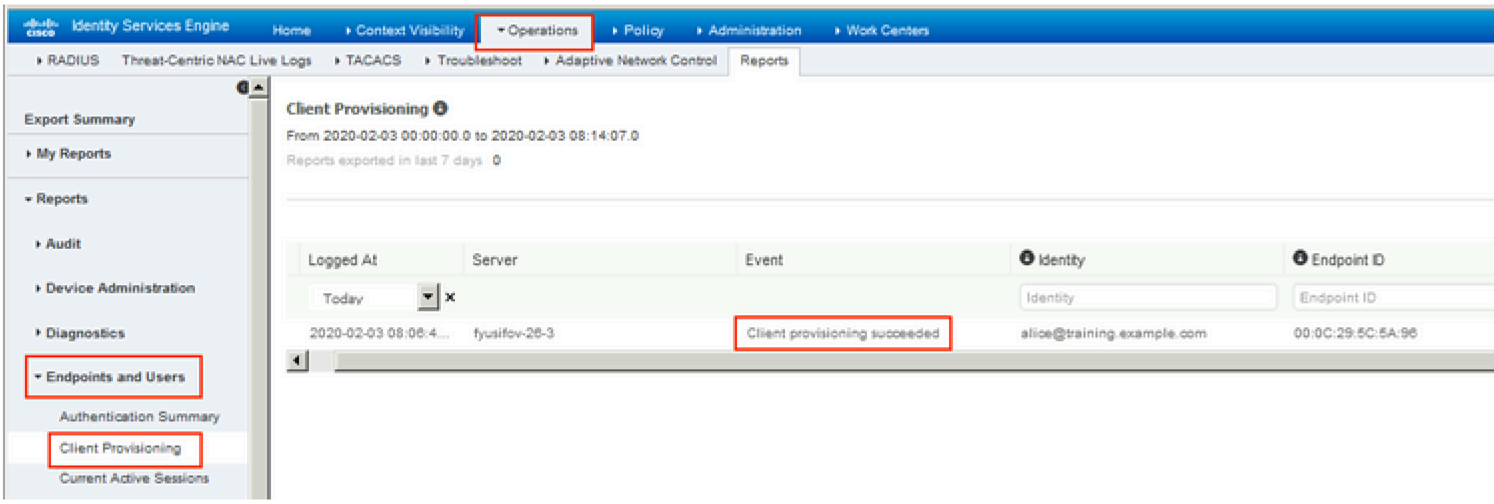
En FTD, para verificar la conexión VPN, SSH al equipo, ejecute **system support diagnostic-cli** y luego **show vpn-sessiondb detail anyconnect**. A partir de esta salida, verifique que los atributos enviados desde ISE se apliquen para esta sesión VPN.

<#root>

```
fyusifov-ftd-64#

show vpn-sessiondb detail anyconnect


Session Type: AnyConnect Detailed


Username     : alice@training.example.com

Index        : 12

Assigned IP  : 172.16.1.10

             Public IP    : 10.229.16.169
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15326                  Bytes Rx     : 13362
Pkts Tx      : 10                     Pkts Rx      : 49
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy

Tunnel Group : EmployeeVPN

Login Time   : 07:13:30 UTC Mon Feb 3 2020
Duration     : 0h:06m:43s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000c0005e37c81a
Security Grp : none                   Tunnel Zone  : 0

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

```
AnyConnect-Parent:
  Tunnel ID    : 12.1
  Public IP    : 10.229.16.169
  Encryption   : none                   Hashing      : none
  TCP Src Port : 56491                  TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 23 Minutes
  Client OS    : win
  Client OS Ver: 10.0.18363
  Client Type  : AnyConnect

Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.7.01076

  Bytes Tx     : 7663                   Bytes Rx     : 0
  Pkts Tx      : 5                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 12.2
  Assigned IP  : 172.16.1.10            Public IP    : 10.229.16.169
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 56495
  TCP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 23 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.7.01076
  Bytes Tx     : 7663                   Bytes Rx     : 592
  Pkts Tx      : 5                      Pkts Rx      : 7
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-PostureUnknown-5e37414d

DTLS-Tunnel:
  Tunnel ID    : 12.3
  Assigned IP  : 172.16.1.10            Public IP    : 10.229.16.169
  Encryption   : AES256                 Hashing      : SHA1
  Ciphersuite  : DHE-RSA-AES256-SHA
  Encapsulation: DTLSv1.0               UDP Src Port : 59396
  UDP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.7.01076
  Bytes Tx     : 0                      Bytes Rx     : 12770
  Pkts Tx      : 0                      Pkts Rx      : 42
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

 Filter Name  : #ACSACL#-IP-PostureUnknown-5e37414d


ISE Posture:
  Redirect URL : https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=000000000000c0005e37c81
  Redirect ACL : fyusifovredirect


fyusifov-ftd-64#
```

Se pueden verificar las políticas de aprovisionamiento de clientes. Vaya a **Operaciones > Informes > Terminales y usuarios > Aprovisionamiento del cliente**.



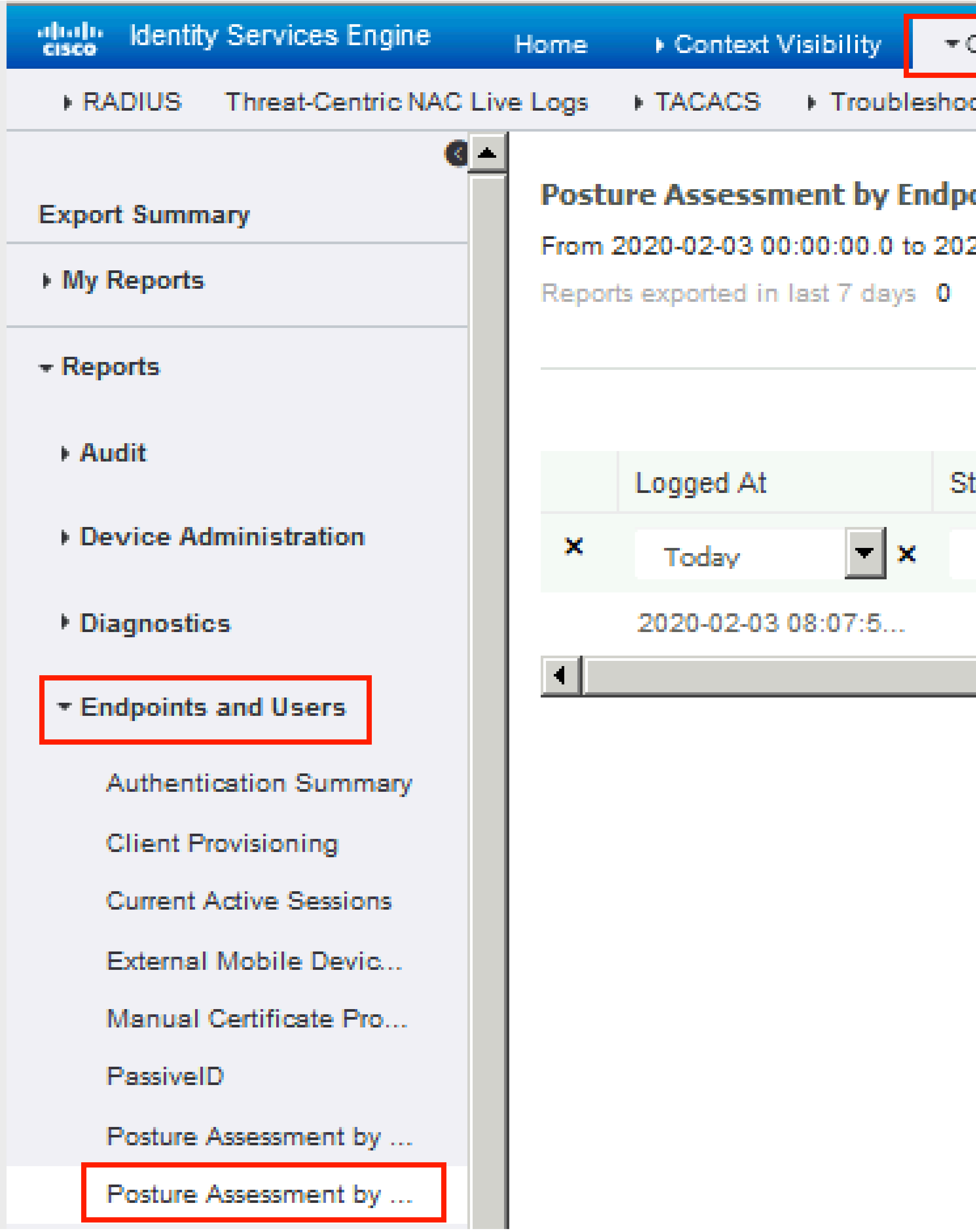
Client Provisioning

From 2020-02-03 00:00:00.0 to 2020-02-03 08:14:07.0

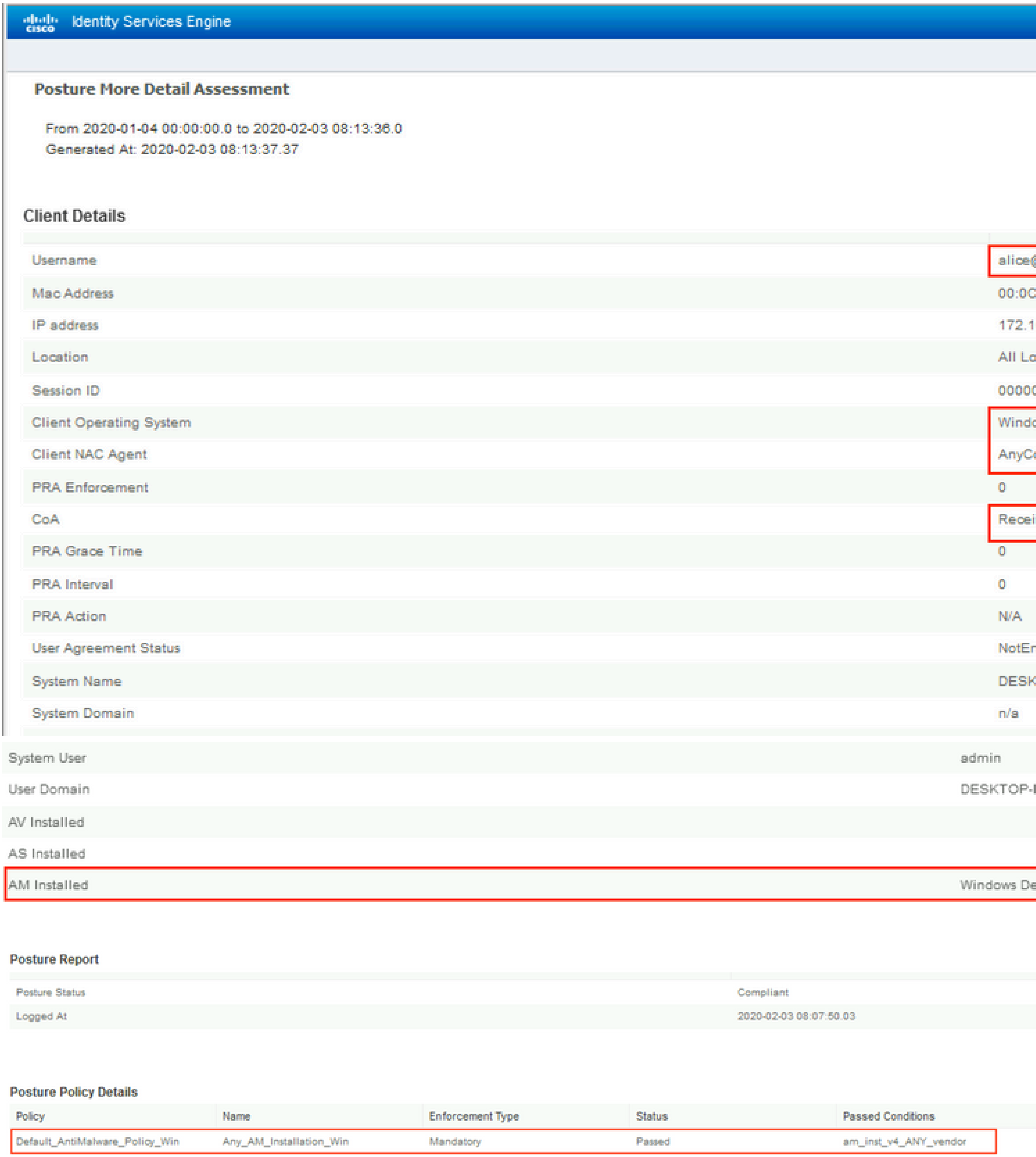
Reports exported in last 7 days 0

Logged At	Server	Event	Identity	Endpoint ID
Today			Identity	Endpoint ID
2020-02-03 08:06:4...	fyusifov-26-3	Client provisioning succeeded	alice@training.example.com	00:0C:29:5C:5A:96

El informe de estado enviado desde AnyConnect se puede comprobar. Vaya a **Operaciones > Informes > Terminales y usuarios > Evaluación de estado por terminal**.



Para ver más detalles sobre el informe de estado, haga clic en **Detalles**.



Posture More Detail Assessment

From 2020-01-04 00:00:00.0 to 2020-02-03 08:13:36.0
Generated At: 2020-02-03 08:13:37.37

Client Details

Username	alice@
Mac Address	00:0C
IP address	172.1
Location	All Lo
Session ID	00000
Client Operating System	Windo
Client NAC Agent	AnyCo
PRA Enforcement	0
CoA	Recei
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEn
System Name	DESK
System Domain	n/a
System User	admin
User Domain	DESKTOP-I
AV Installed	
AS Installed	
AM Installed	Windows De

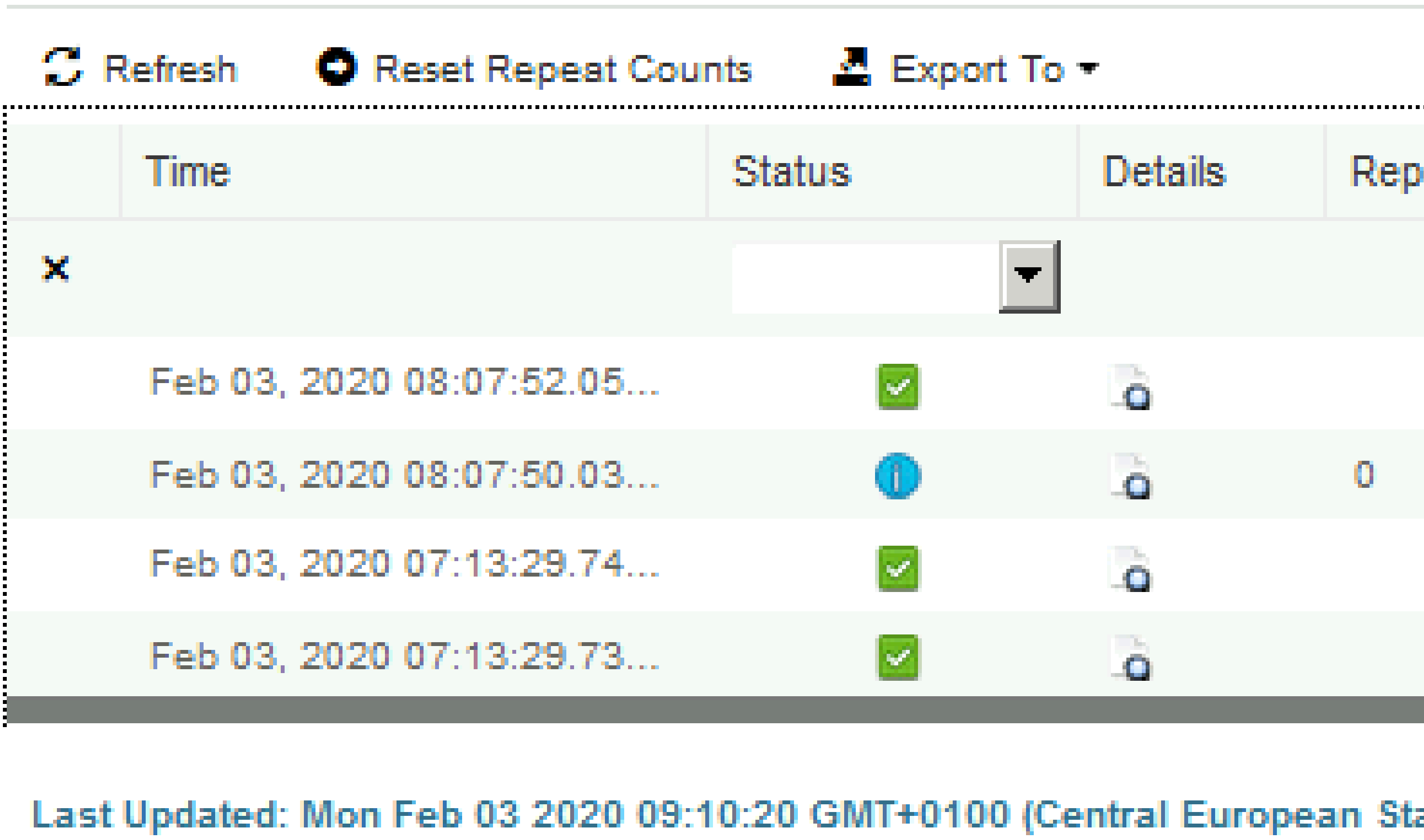
Posture Report

Posture Status	Compliant
Logged At	2020-02-03 08:07:50.03

Posture Policy Details

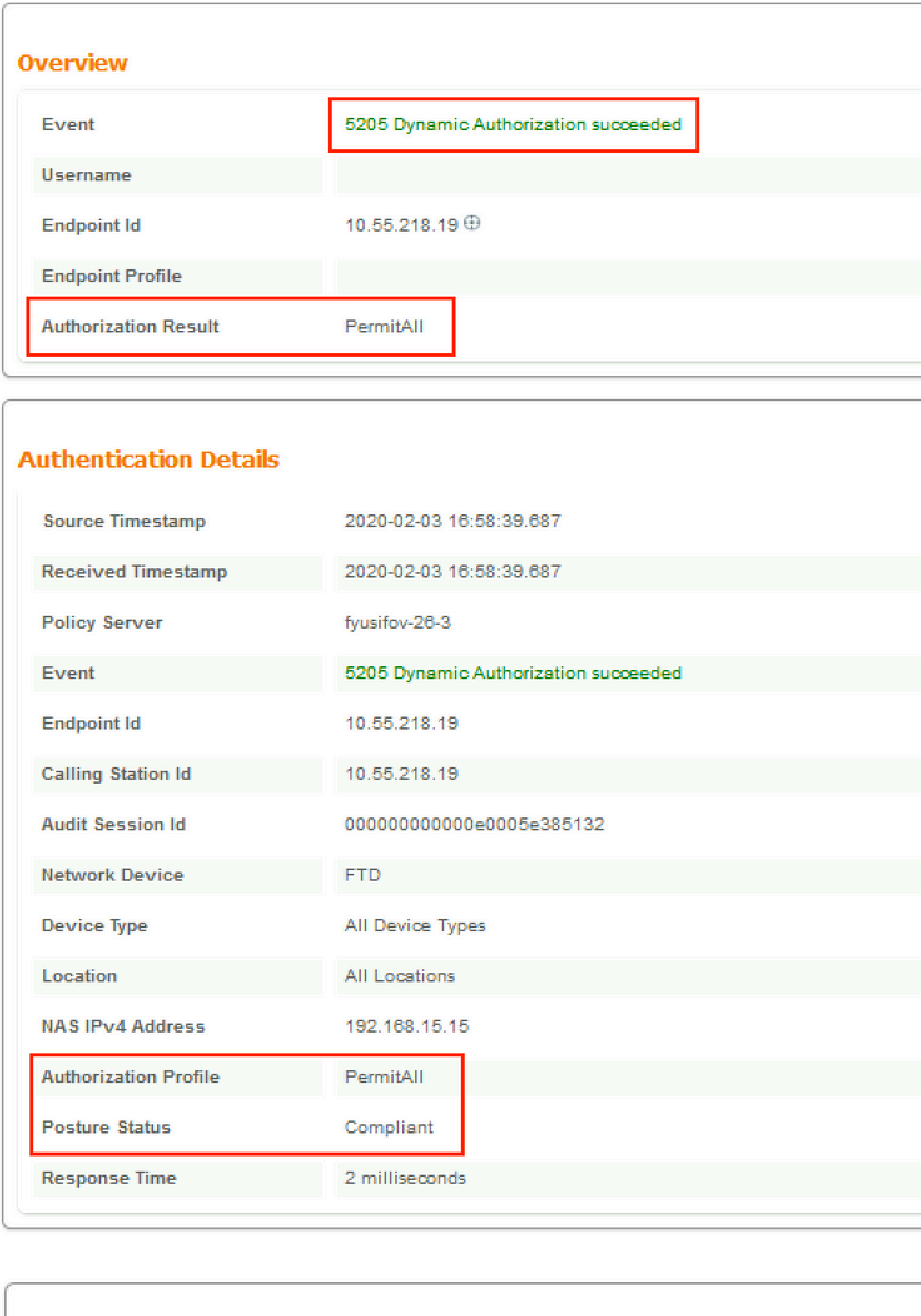
Policy	Name	Enforcement Type	Status	Passed Conditions
Default_AntiMalware_Policy_Win	Any_AM_Installation_Win	Mandatory	Passed	am_inst_v4_ANY_vendor

Una vez recibido el informe sobre ISE, se actualiza el estado. En este ejemplo, el estado de estado es compatible y CoA Push se activa con un nuevo conjunto de atributos.



	Time	Status	Details	Rep
×		▾		
	Feb 03, 2020 08:07:52.05...	✓	🔍	
	Feb 03, 2020 08:07:50.03...	ⓘ	🔍	0
	Feb 03, 2020 07:13:29.74...	✓	🔍	
	Feb 03, 2020 07:13:29.73...	✓	🔍	

Last Updated: Mon Feb 03 2020 09:10:20 GMT+0100 (Central European Sta



Overview

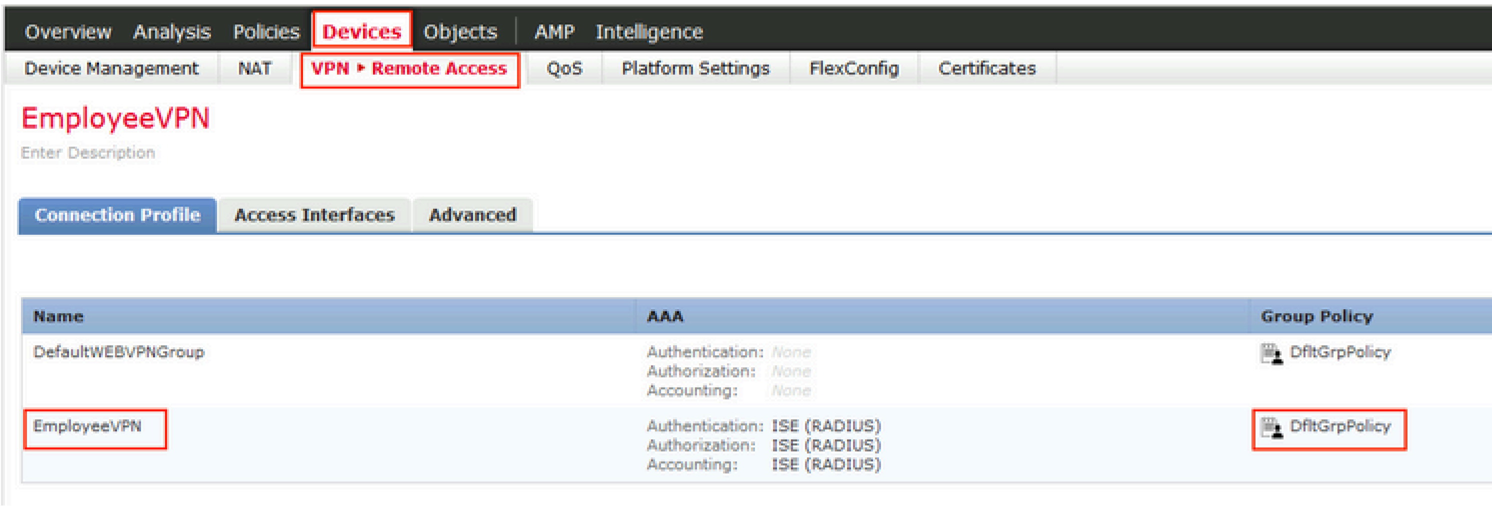
Event	5205 Dynamic Authorization succeeded
Username	
Endpoint Id	10.55.218.19
Endpoint Profile	
Authorization Result	PermitAll

Authentication Details

Source Timestamp	2020-02-03 16:58:39.687
Received Timestamp	2020-02-03 16:58:39.687
Policy Server	fyusifov-26-3
Event	5205 Dynamic Authorization succeeded
Endpoint Id	10.55.218.19
Calling Station Id	10.55.218.19
Audit Session Id	000000000000e0005e385132
Network Device	FTD
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.15.15
Authorization Profile	PermitAll
Posture Status	Compliant
Response Time	2 milliseconds

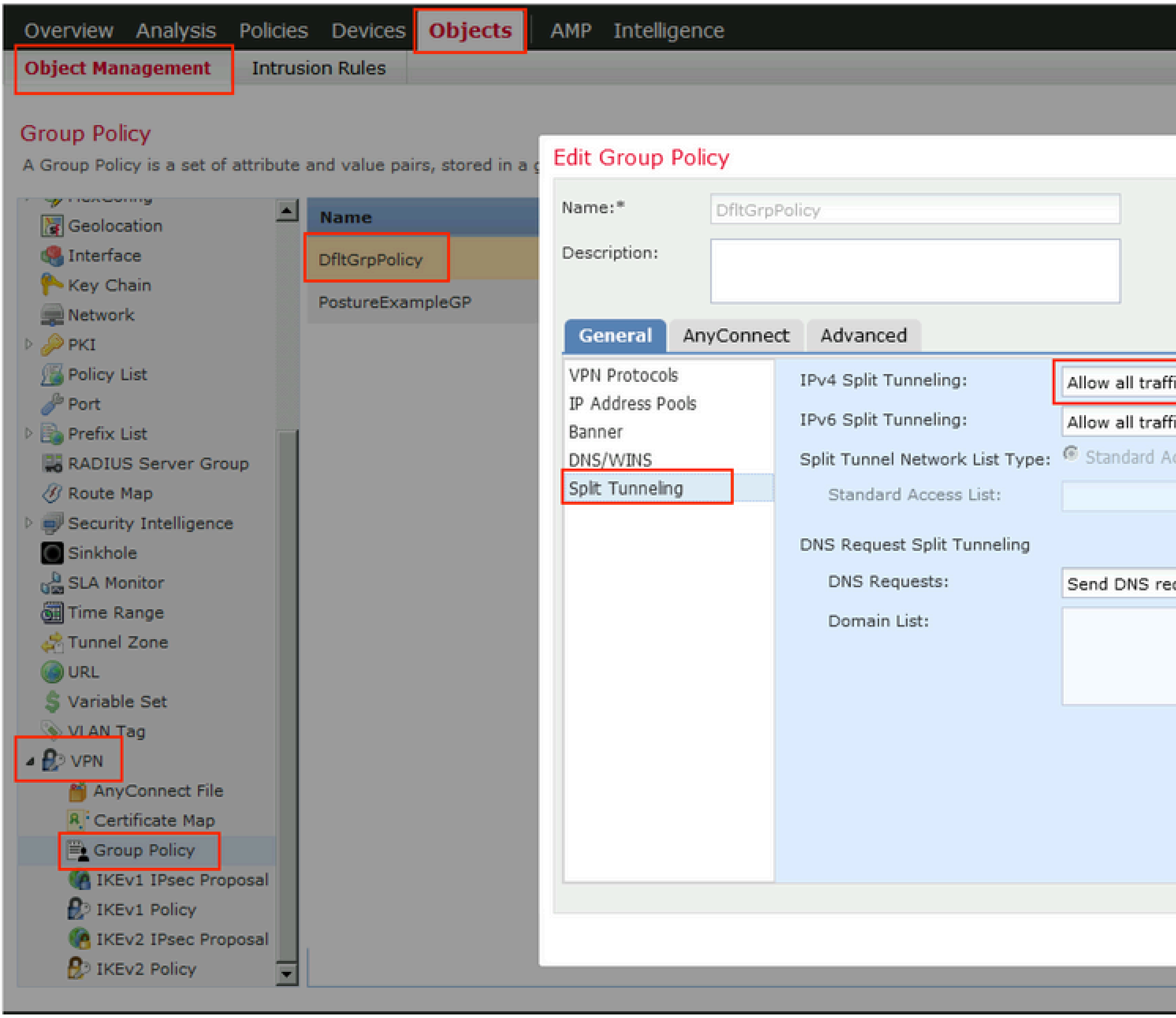
Uno de los problemas comunes, cuando hay un túnel de escupir se configura. En este ejemplo, se utiliza la directiva de grupo predeterminada, que establece túneles para todo el tráfico. En caso de que solo se tunelice tráfico específico, los sondeos de AnyConnect (enroll.cisco.com y host de detección) deben pasar a través del túnel, además del tráfico a ISE y otros recursos internos.

Para verificar la política de túnel en FMC, primero, verifique qué política de grupo se utiliza para la conexión VPN. Vaya a **Devices > VPN Remote Access**.



Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
EmployeeVPN	Authentication: ISE (RADIUS) Authorization: ISE (RADIUS) Accounting: ISE (RADIUS)	DfltGrpPolicy

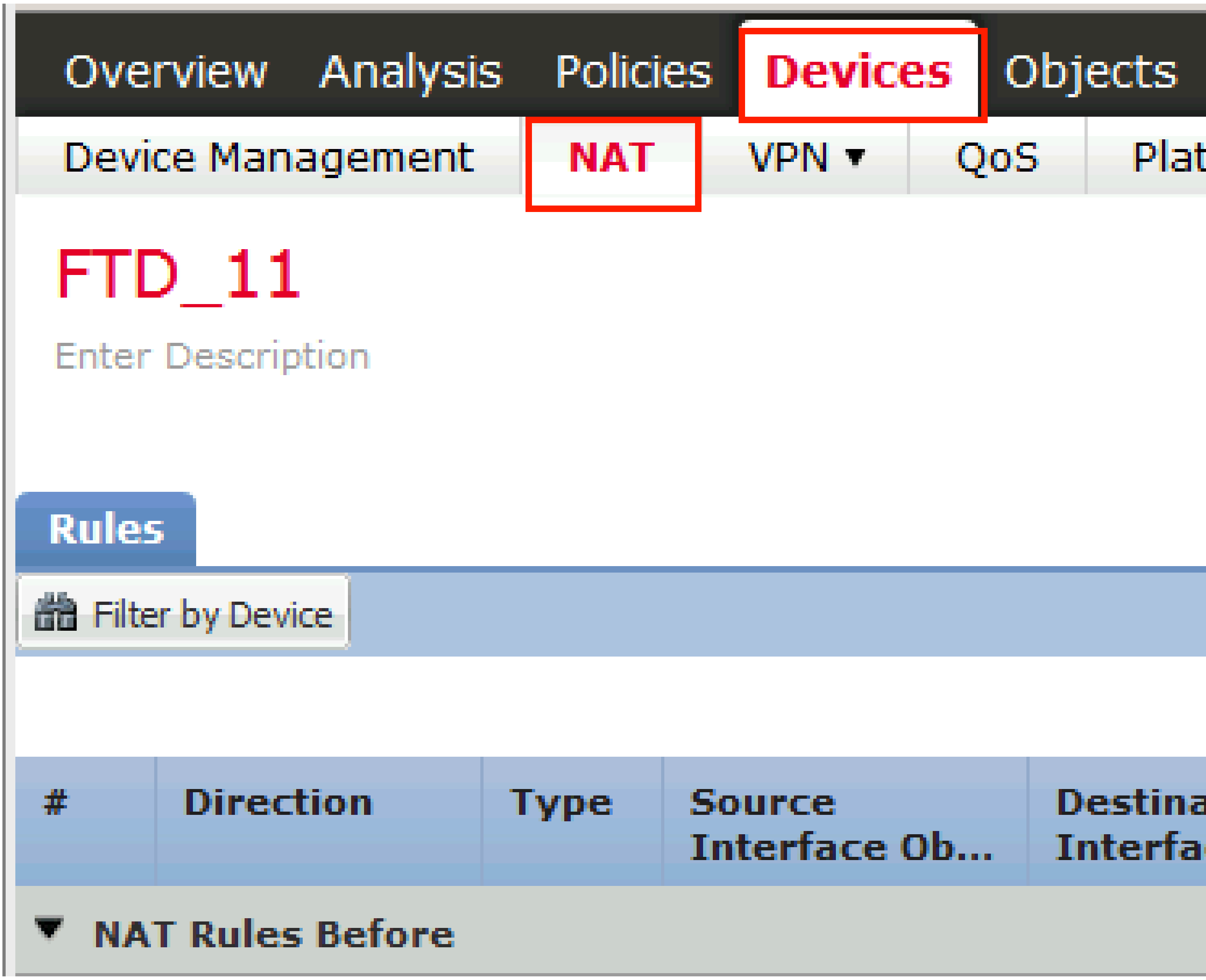
Luego, navegue hasta **Objetos > Administración de objetos > VPN > Política de grupo** y haga clic en **Política de grupo** configurada para VPN.



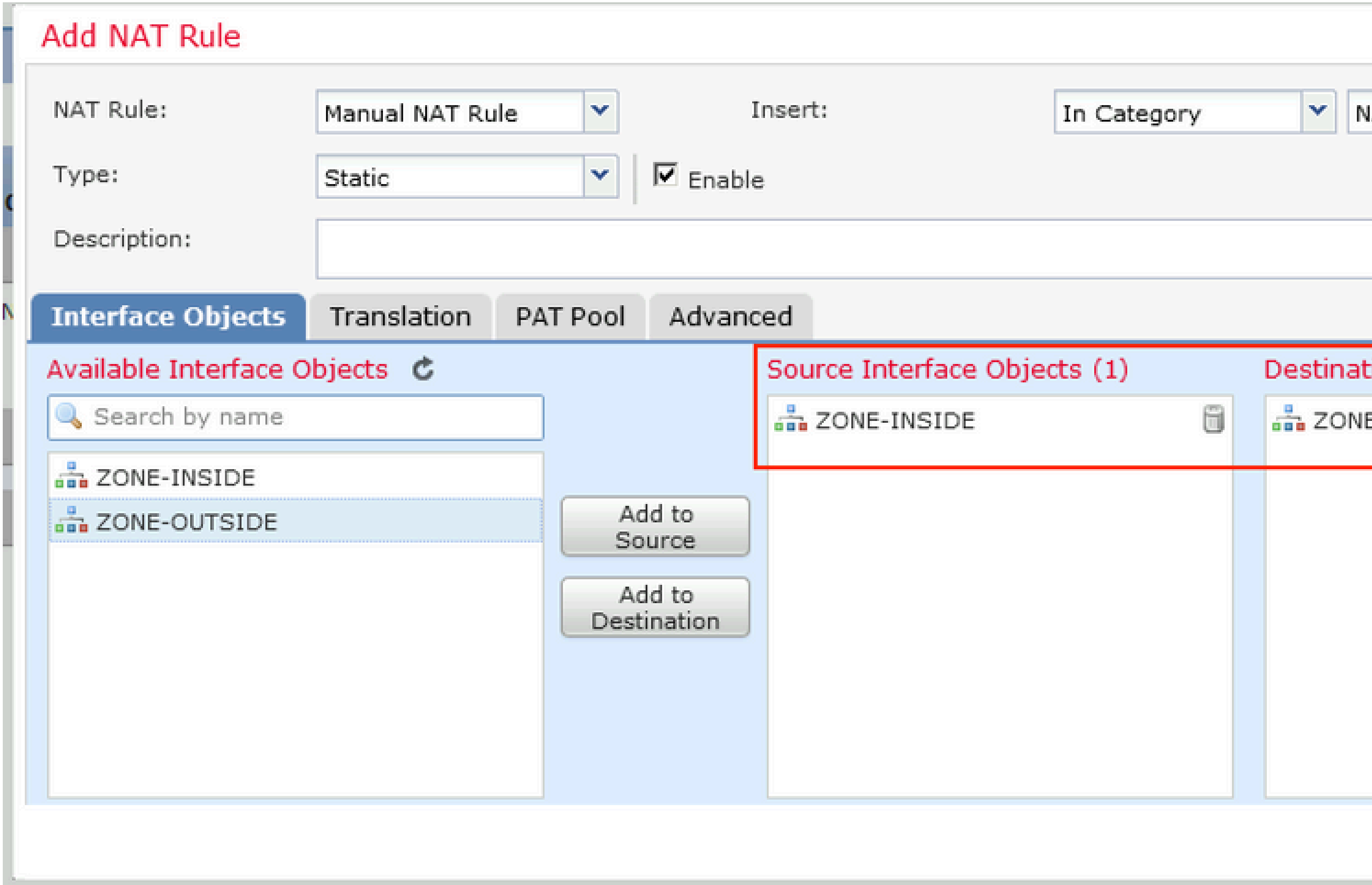
- Identidad NAT

Otro problema común, cuando el tráfico de retorno de los usuarios de VPN se traduce con el uso de una entrada de NAT incorrecta. Para solucionar este problema, la identidad NAT debe crearse en un orden apropiado.

Primero, verifique las reglas NAT para este dispositivo. Navegue hasta **Devices** > **NAT** y luego haga clic en **Add Rule** para crear una nueva regla.



En la ventana abierta, en la pestaña **Objetos de interfaz**, seleccione **Zonas de seguridad**. En este ejemplo, la entrada NAT se crea de **ZONE-INSIDE** a **ZONE-OUTSIDE**.



Add NAT Rule

NAT Rule: Manual NAT Rule

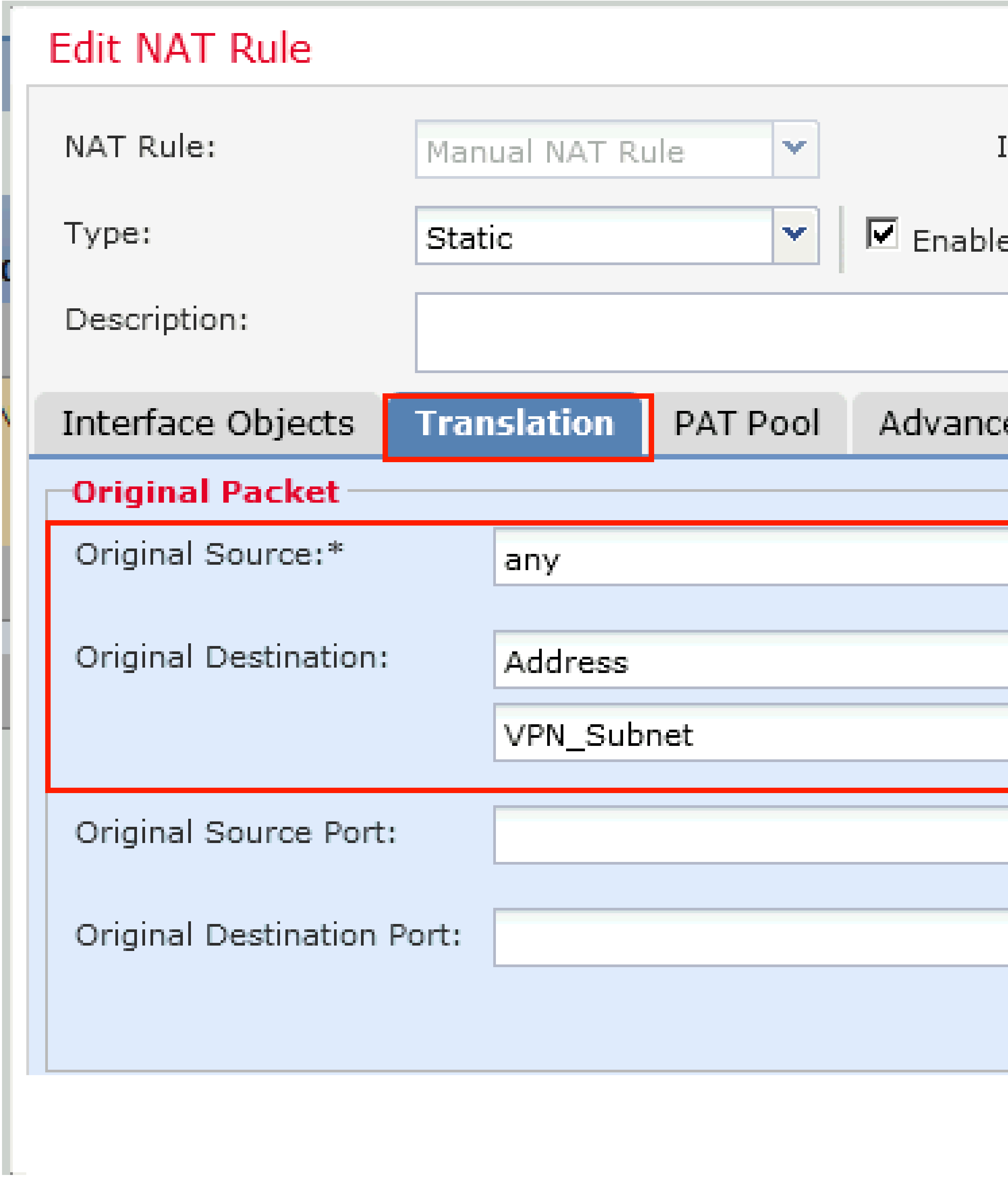
Insert: In Category

Type: Static

☑ Enable

Description:

En la pestaña **Translation**, seleccione los detalles del paquete original y traducido. Como es identidad NAT, el origen y el destino se mantienen sin cambios:



Edit NAT Rule

NAT Rule: Manual NAT Rule

Type: Static

☑ Enable

Description:

Original Packet

Original Source:* any

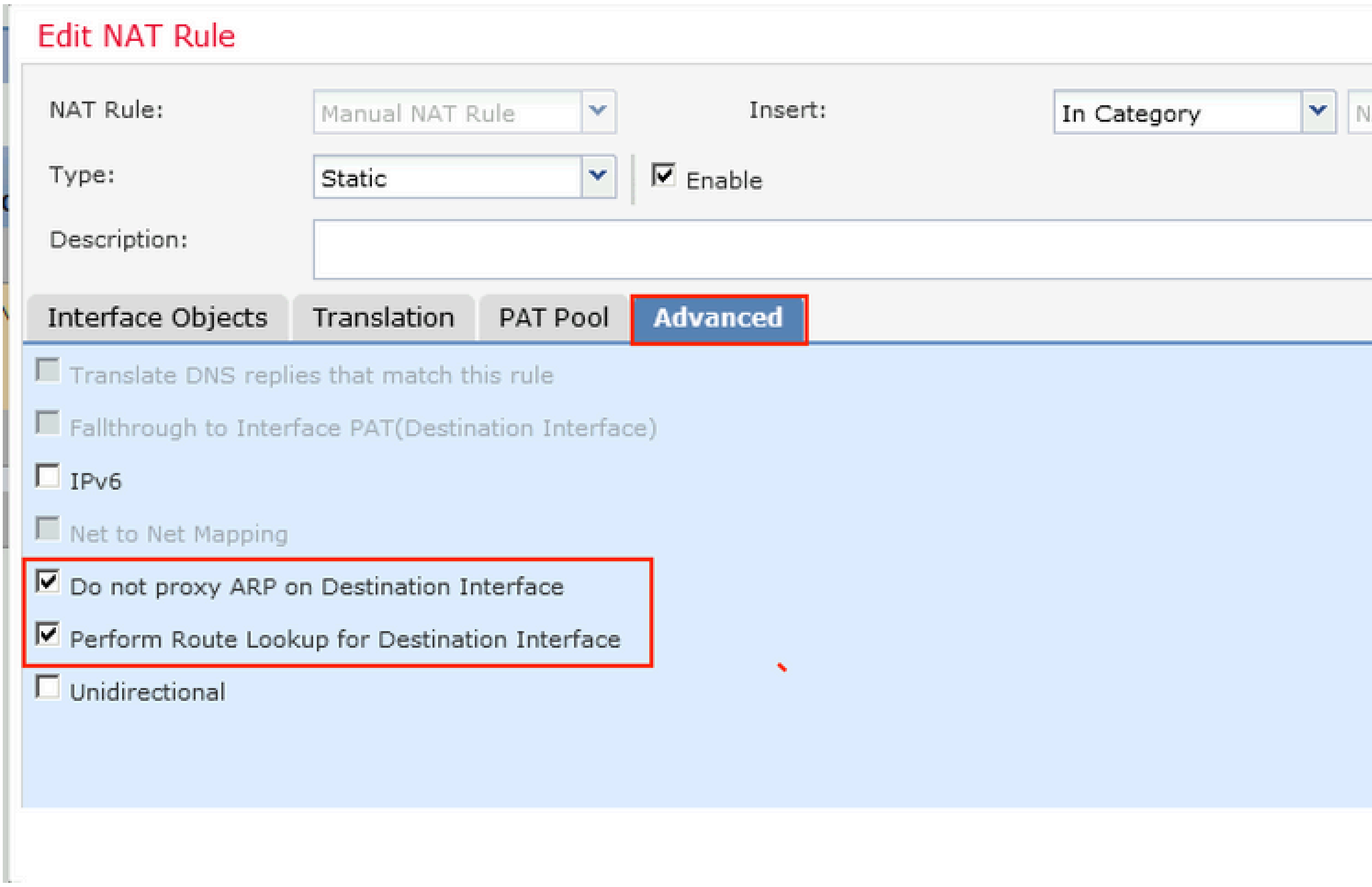
Original Destination: Address

VPN_Subnet

Original Source Port:

Original Destination Port:

En la pestaña **Advanced**, marque las casillas de verificación como se muestra en esta imagen:



Edit NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category

Type: Static

☑ Enable

Description:

□ Translate DNS replies that match this rule

□ Fallthrough to Interface PAT(Destination Interface)

□ IPv6

□ Net to Net Mapping

☑ Do not proxy ARP on Destination Interface

☑ Perform Route Lookup for Destination Interface

□ Unidirectional

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).