Configurar a postura do ISE sobre a VPN de acesso remoto do AnyConnect no FTD

Contents

Introdução

Este documento descreve como configurar o Firepower Threat Defense (FTD) versão 6.4.0 para posicionar usuários de VPN contra o Identity Services Engine (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN de acesso remoto AnyConnect
- Configuração da VPN de acesso remoto no FTD
- Identity Services Engine e serviços de postura

Componentes Utilizados

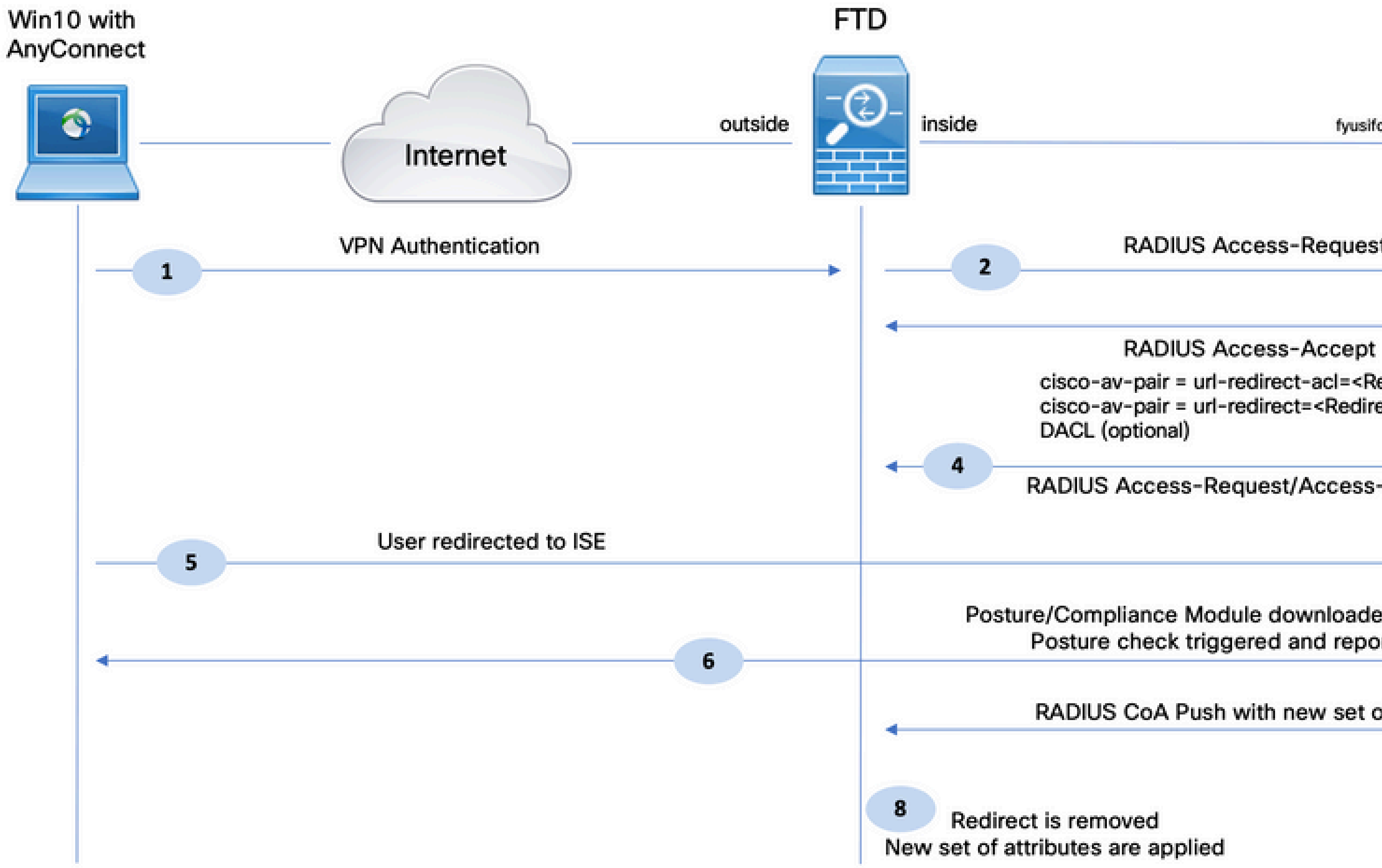
As informações neste documento são baseadas nestas versões de software:

- Software Cisco Firepower Threat Defense (FTD) versões 6.4.0
- Software Cisco Firepower Management Console (FMC) versão 6.5.0
- Microsoft Windows 10 com Cisco AnyConnect Secure Mobility Client versão 4.7
- Cisco Identity Services Engine (ISE) versão 2.6 com Patch 3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de rede e fluxo de tráfego


Win10 with AnyConnect
Internet
FTD
outside
inside
fyusifo
1
VPN Authentication
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-
5
User redirected to ISE
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. O usuário remoto usa o Cisco Anyconnect para acesso VPN ao FTD.

2. O FTD envia uma Solicitação de Acesso RADIUS para esse usuário ao ISE.

3. Essa solicitação atinge a política chamada **FTD-VPN-Posture-Unknown** no ISE. O ISE envia um Access-Accept RADIUS com três atributos:

- **cisco-av-pair = url-redirect-acl=fyusifovredirect** - Este é o nome da Lista de Controle de Acesso (ACL) definida localmente no FTD, que decide o tráfego que é redirecionado.
- cisco-av-pair = url-redirect=**https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp** **- Este é o URL para qual o usuário remoto é redirecionado.**
- **DACL = PERMIT_ALL_IPV4_TRAFFIC** - ACL para download Esse atributo é opcional. Neste cenário, todo o tráfego é permitido em DACL)

4. Se o DACL for enviado, RADIUS Access-Request/Access-Accept será trocado para baixar o conteúdo do DACL

5. Quando o tráfego do usuário da VPN corresponde à ACL definida localmente, ele é redirecionado para o ISE Client Provisioning Portal. O ISE provisiona o AnyConnect Posture Module e o Compliance Module.

6. Depois que o agente é instalado na máquina cliente, ele procura automaticamente pelo ISE com testes. Quando o ISE é detectado com êxito, os requisitos de postura são verificados no endpoint. Neste exemplo, o

agente verifica se há algum software antimalware instalado. Em seguida, ele envia um relatório de postura ao ISE.

7. Quando o ISE recebe o relatório de postura do agente, ele altera o Status da postura para esta sessão e aciona o tipo de CoA RADIUS Enviar com novos atributos. Desta vez, o status da postura é conhecido e outra regra é atingida.

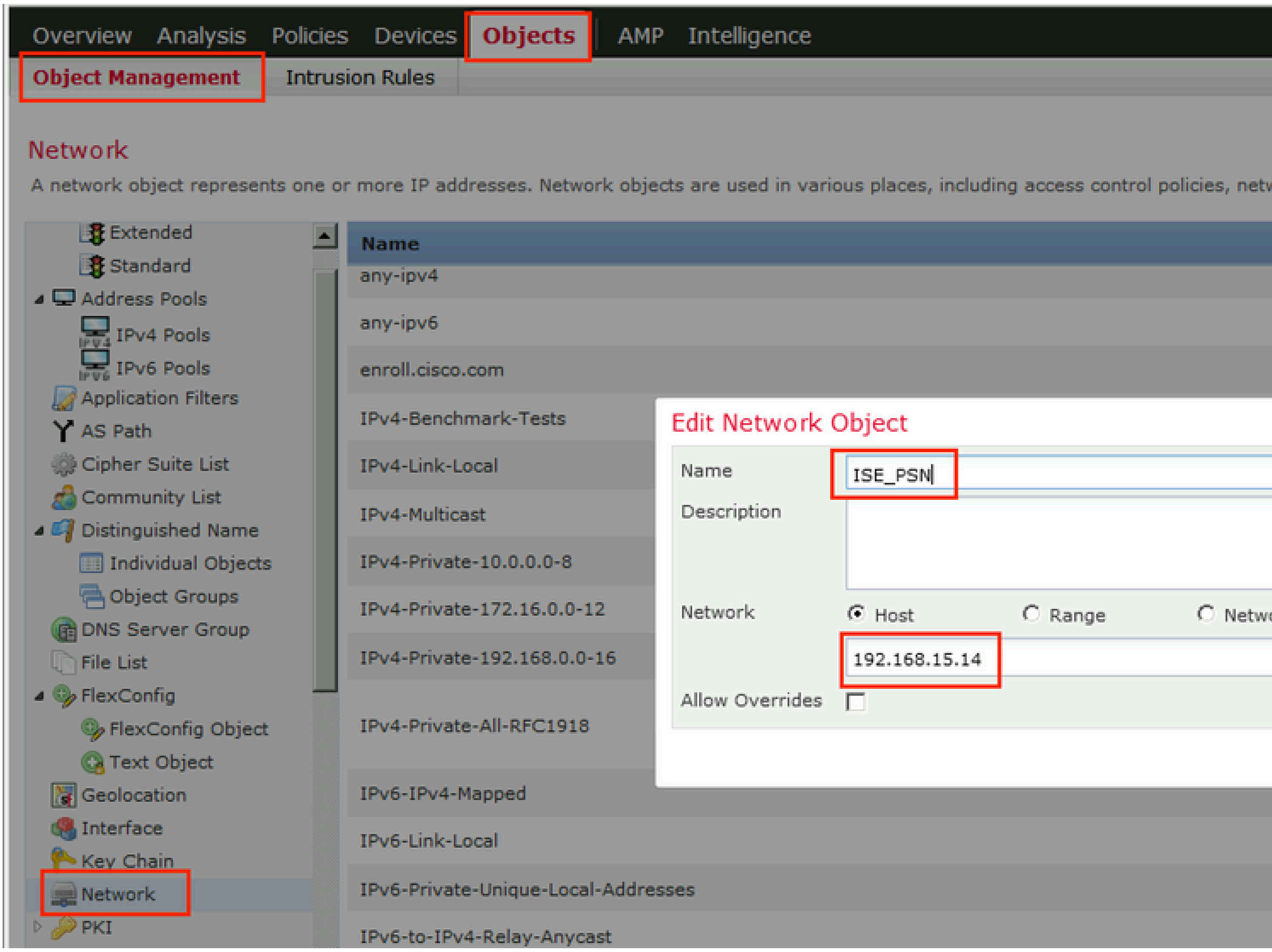
- Se o usuário for compatível, um nome de DACL que permita acesso total será enviado.
- Se o usuário não for compatível, um nome de DACL que permita acesso limitado será enviado.

8. O FTD remove o redirecionamento. O FTD envia a solicitação de acesso para baixar o DACL do ISE. O DACL específico é anexado à sessão VPN.

Configurações

FTD/FMC

Etapa 1. Crie um grupo de objetos de rede para o ISE e servidores de remediação (se houver). Navegue até **Objetos > Gerenciamento de objetos > Rede**.



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

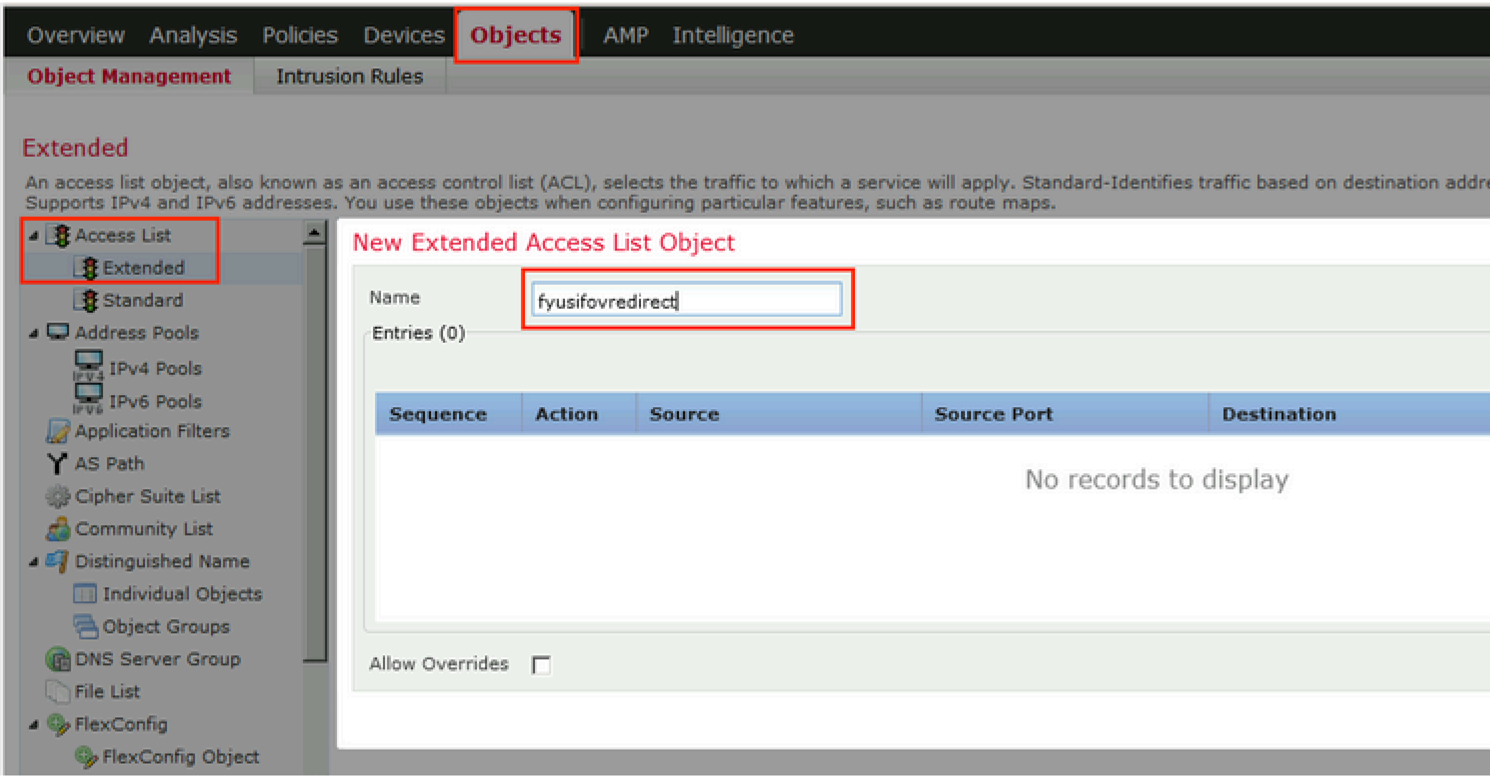
Description:

Network: ● Host ○ Range ○ Netw

192.168.15.14

Allow Overrides □

Etapa 2. Criar ACL de redirecionamento. Navegue até **Objetos > Gerenciamento de objetos > Lista de acesso > Estendido**. Clique em **Add Extended Access List** e forneça o nome de Redirect ACL. Esse nome deve ser o mesmo do resultado de autorização do 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

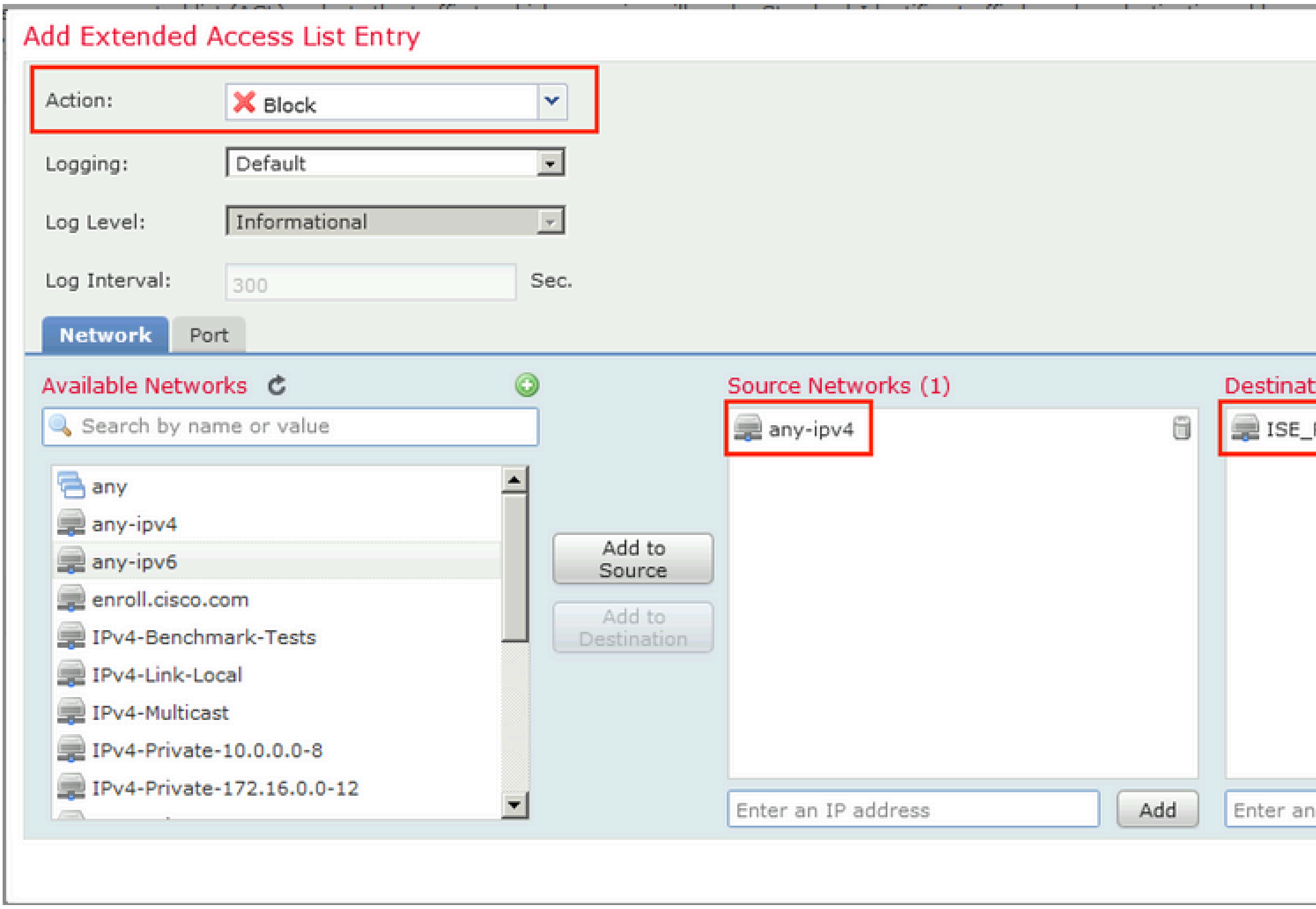
Name: fyusifovredirect

Entries (0)

No records to display

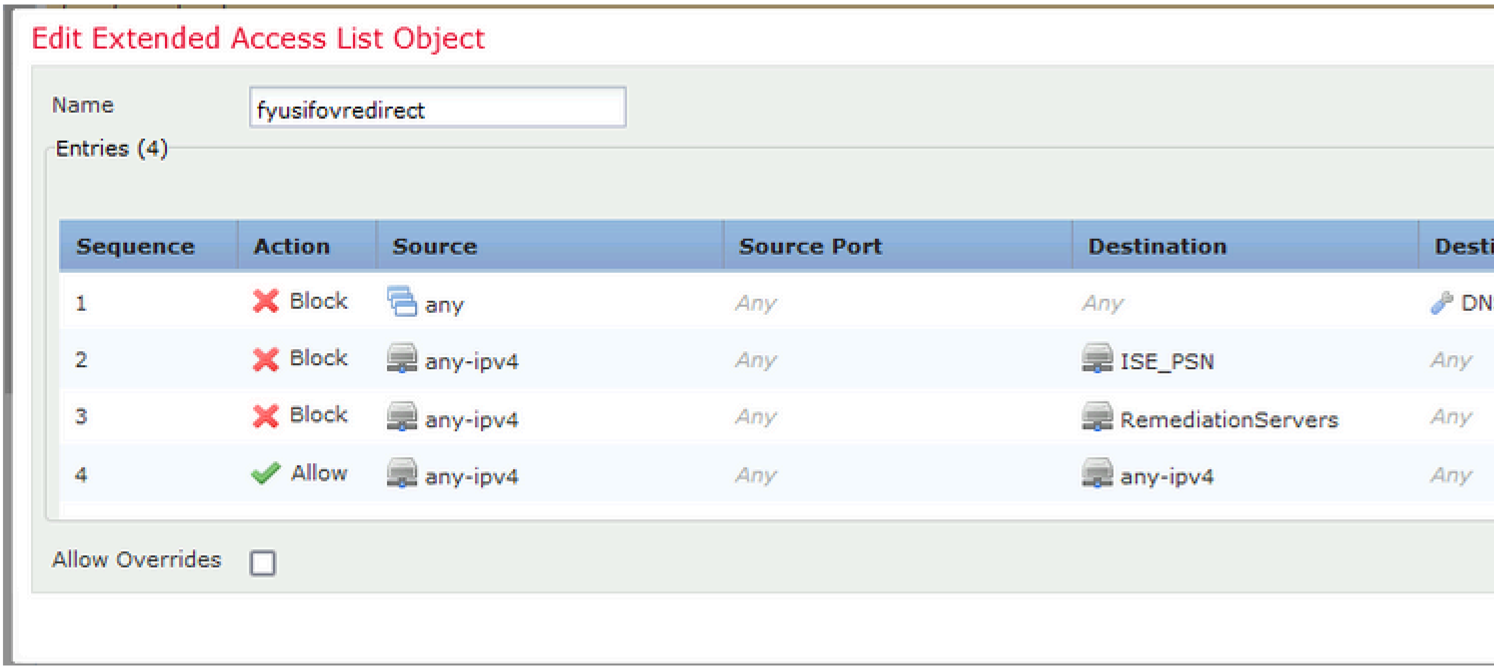
Allow Overrides □

Etapa 3. Adicionar entradas ACL de redirecionamento. Clique no botão Adicionar. Bloqueie o tráfego para DNS, ISE e para os servidores de remediação para excluí-los do redirecionamento. Permita o restante do tráfego, isso dispara o redirecionamento (as entradas de ACL podem ser mais específicas, se necessário).



Add Extended Access List Entry

Action:	Block
Logging:	Default
Log Level:	Informational
Log Interval:	300 Sec.



Edit Extended Access List Object

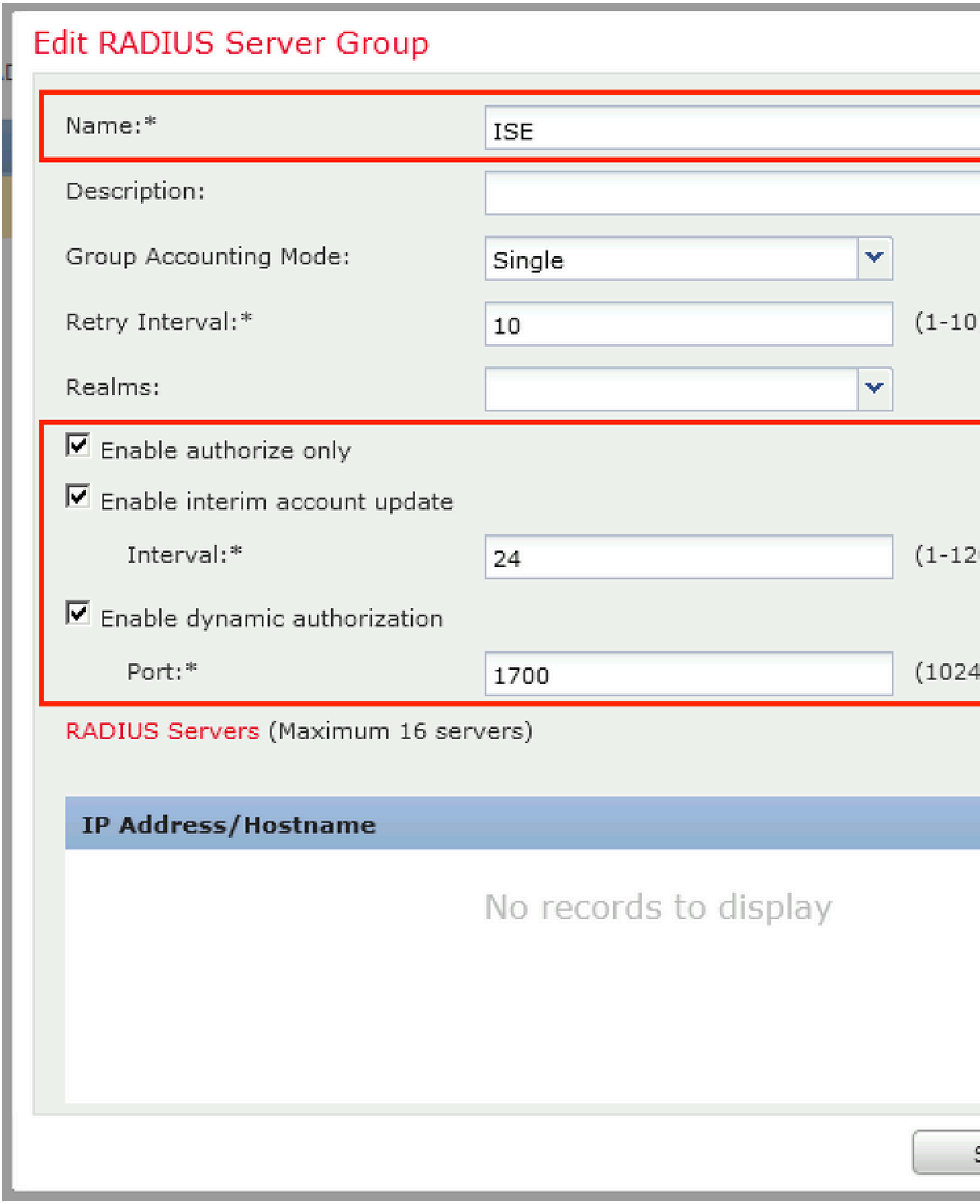
Name: fyusifovredirect

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 ☐

Etapa 4. Adicionar nó/nós PSN do ISE. Navegue até **Objetos > Gerenciamento de objetos > Grupo de servidores RADIUS**. Clique em **Add RADIUS Server Group**, forneça o nome, ative todas as caixas de seleção e clique no ícone **plus**.



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

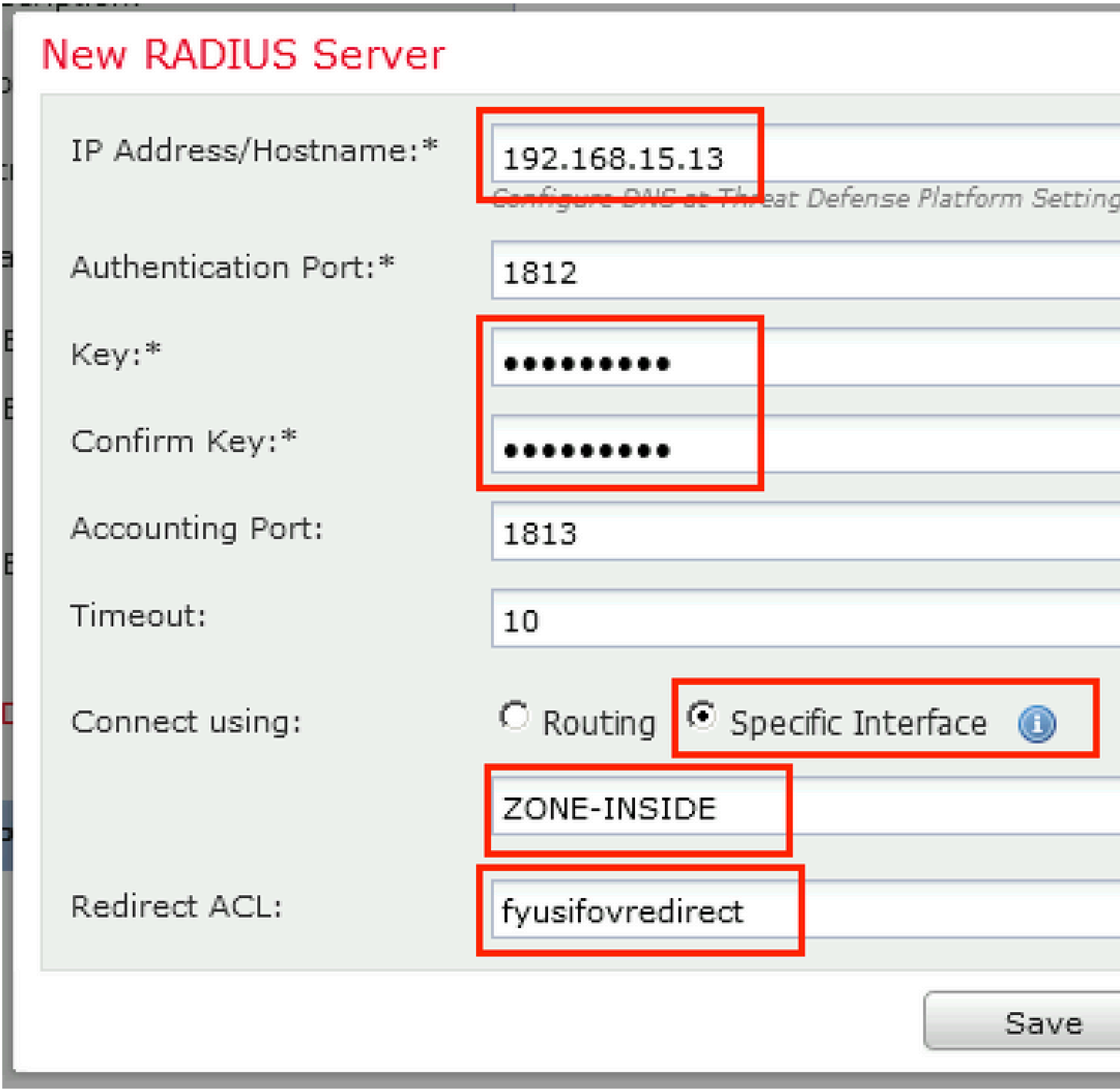
☑ Enable dynamic authorization

Port:*	1700	(1024

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

Etapa 5. Na janela aberta, forneça o endereço IP PSN do ISE, a chave RADIUS, selecione **Specific Interface** e selecione a interface a partir da qual o ISE pode ser alcançado (essa interface é usada como origem do tráfego RADIUS); em seguida, selecione **Redirect ACL**, que foi configurado 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

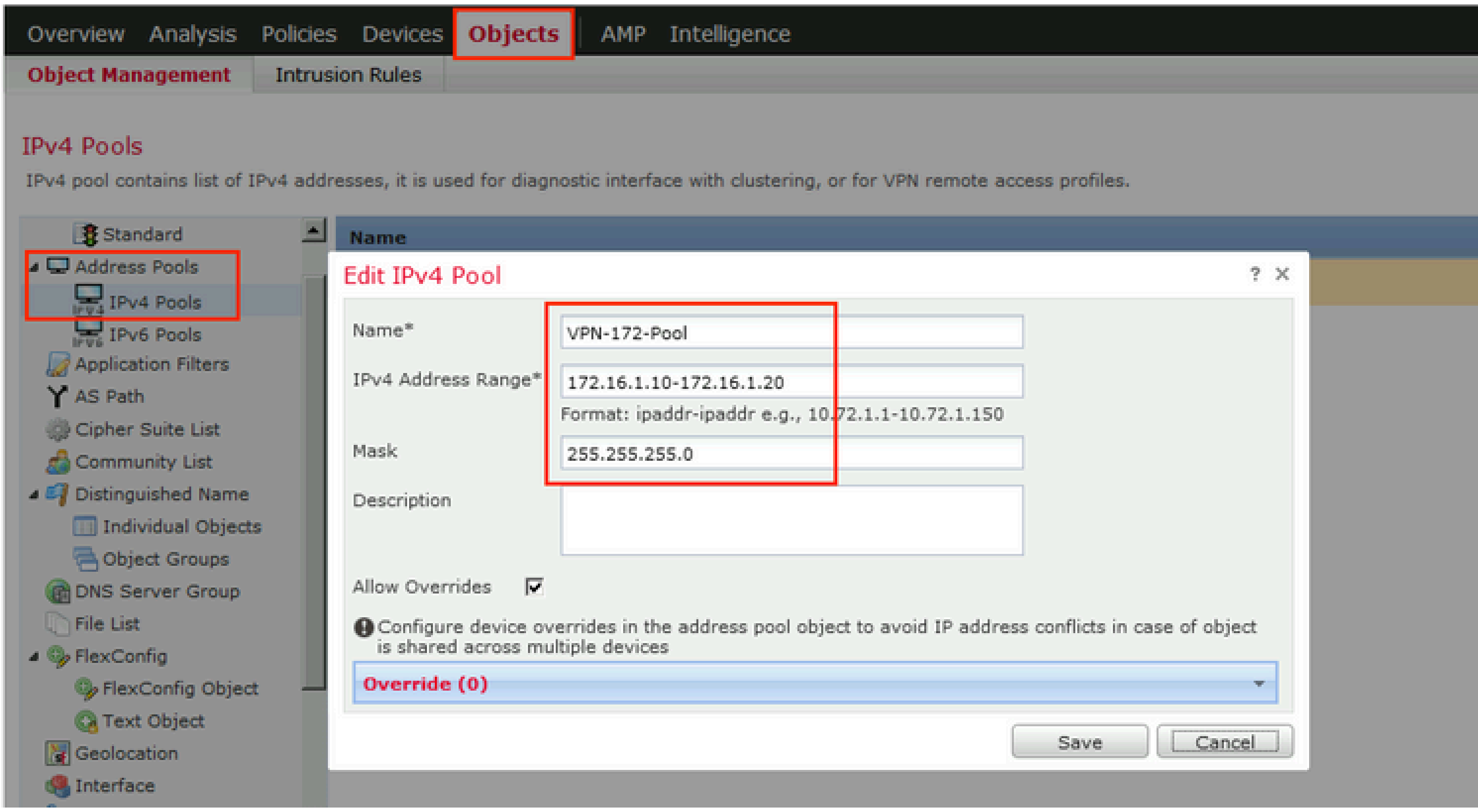
Timeout: 10

Connect using: ○ Routing ● Specific Interface

ZONE-INSIDE

Redirect ACL: fyusifovredirect

Etapa 6. Crie um pool de endereços para usuários VPN. Navegue até **Objects** > **Object Management** > **Address Pools** > **IPv4 Pools**. Clique em **Add IPv4 Pools** e preencha os detalhes.



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

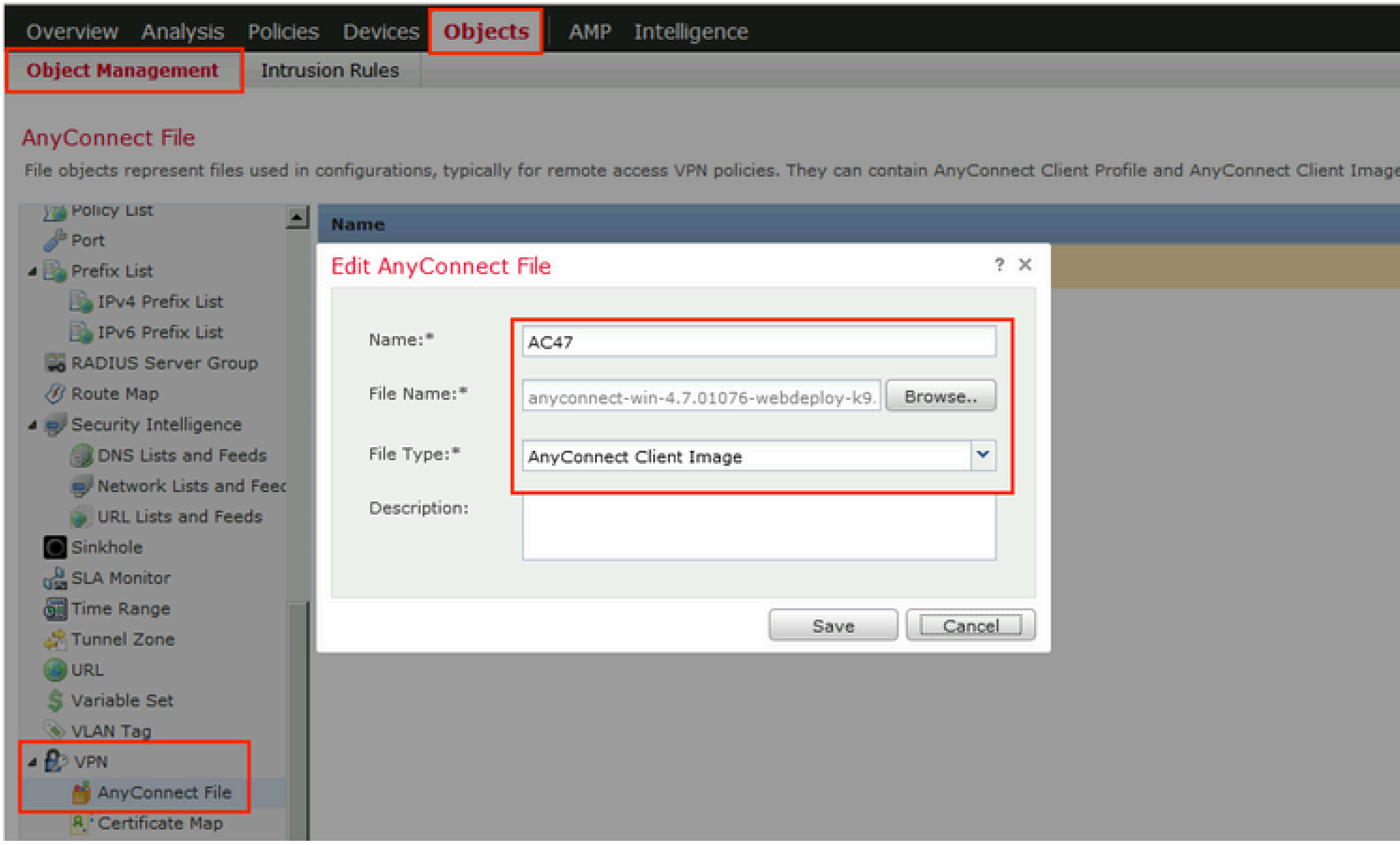
Description

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)

Passo 7. Criar pacote do AnyConnect. Navegue até **Objetos** > **Gerenciamento de objetos** > **VPN** > **Arquivo AnyConnect**. Clique em **Add AnyConnect File**, forneça o nome do pacote, faça o download do pacote em Cisco Software Download e selecione **Anyconnect Client Image** File Type.



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

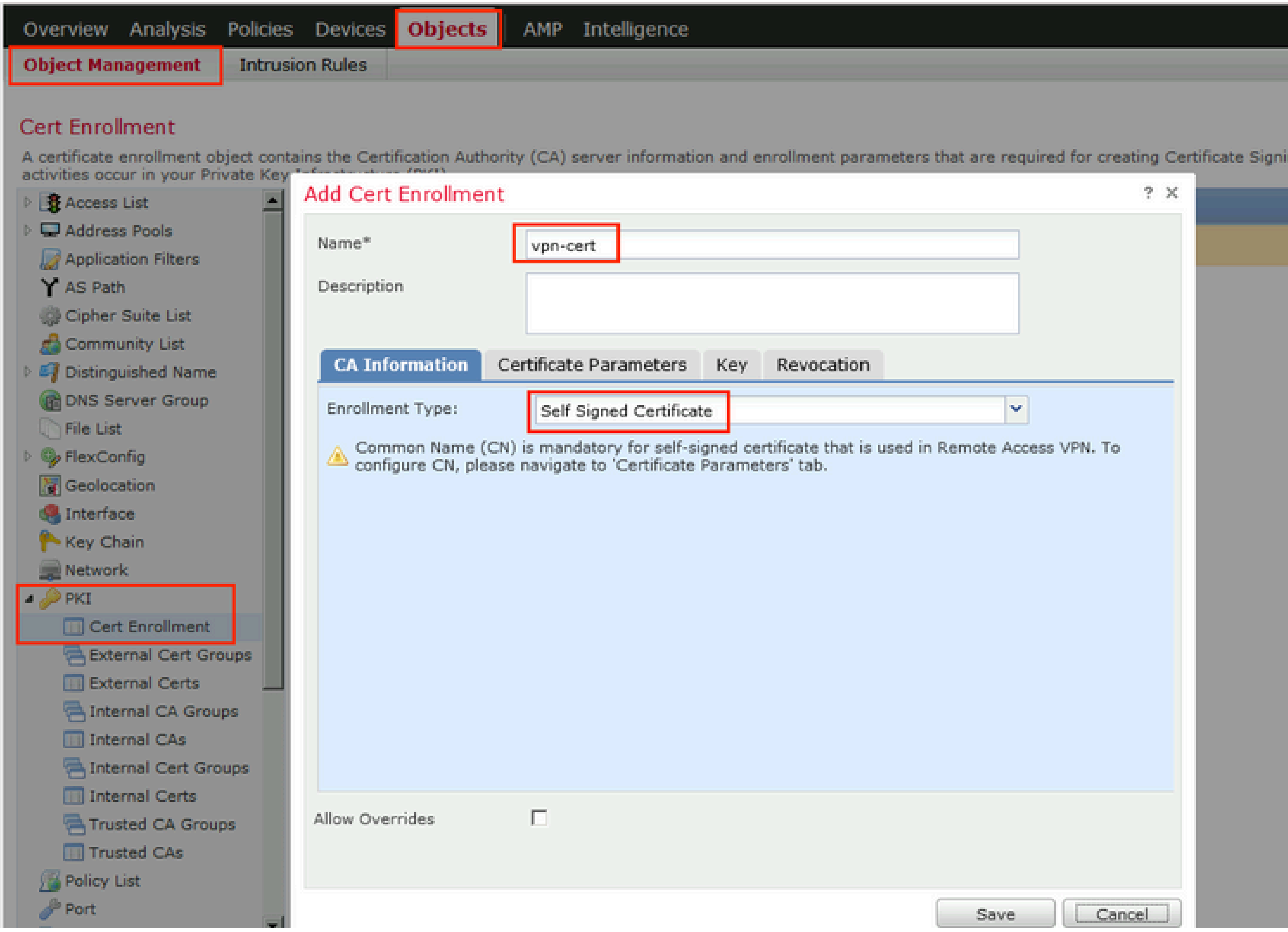
Name:* AC47

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

File Type:* AnyConnect Client Image

Description:

Etapa 8. Navegue até **Objetos de certificado > Gerenciamento de objetos > PKI > Registro de certificado**. Clique em **Add Cert Enrollment**, forneça o nome, escolha **Self Signed Certificate** em Enrollment Type. Clique na guia Parâmetros do certificado e forneça CN.



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 Infrastructure (PKI).

Add Cert Enrollment

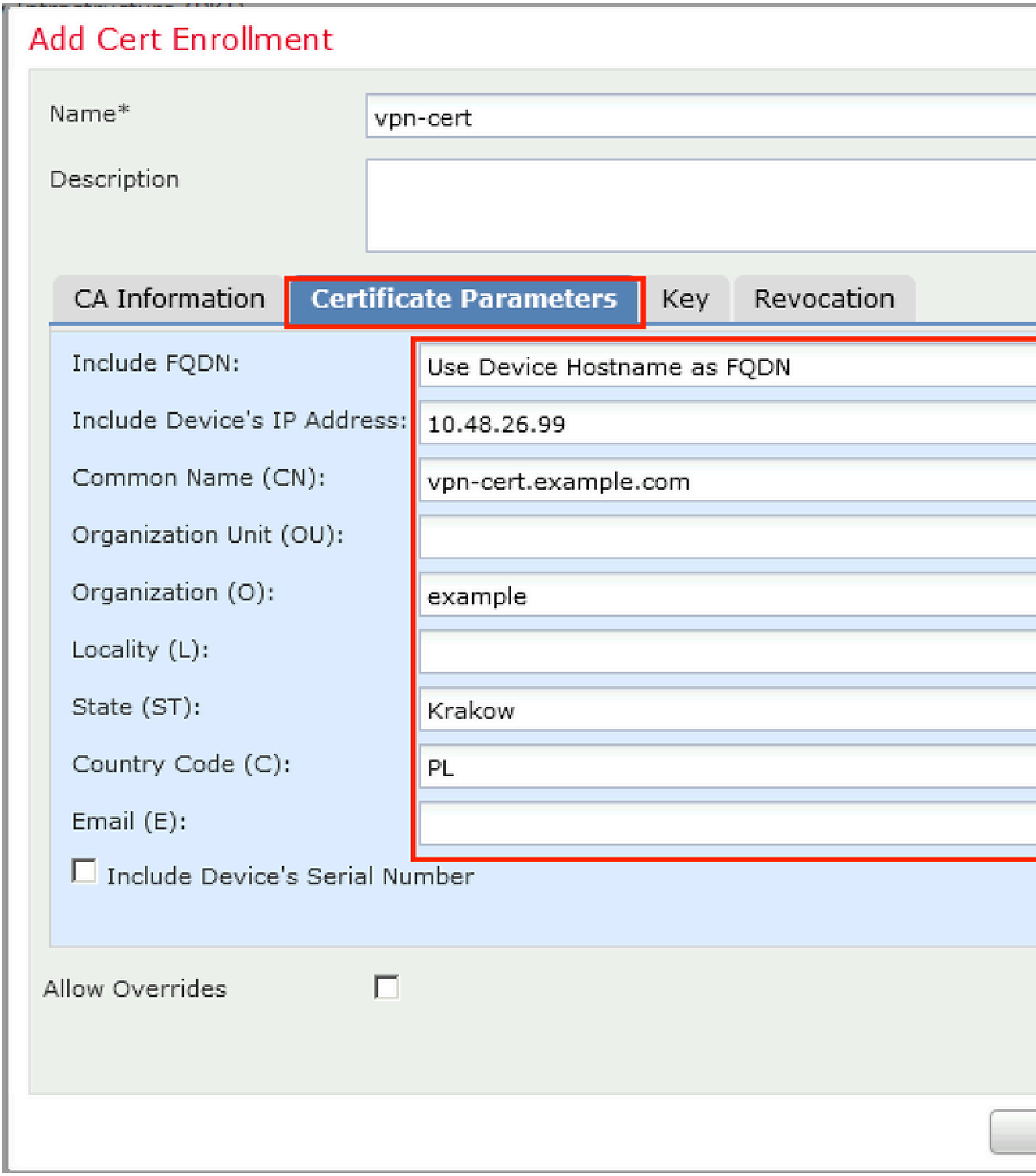
Name* vpn-cert

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

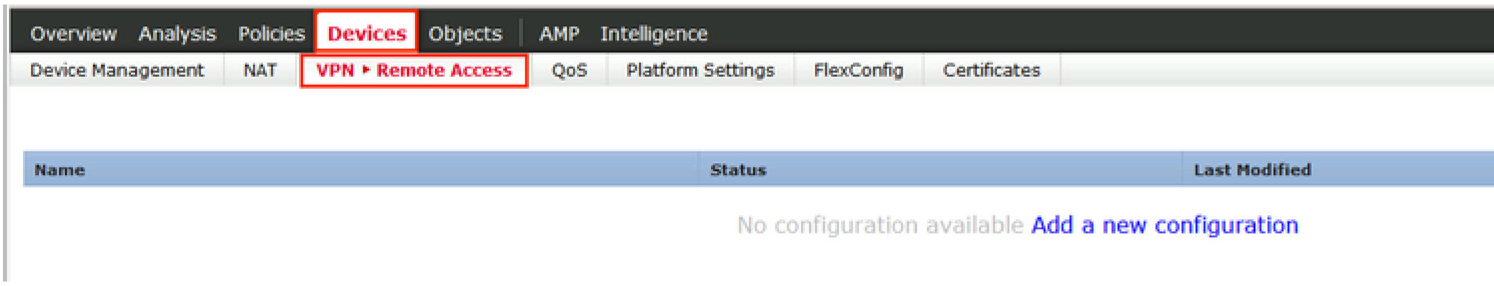
Description:

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 □

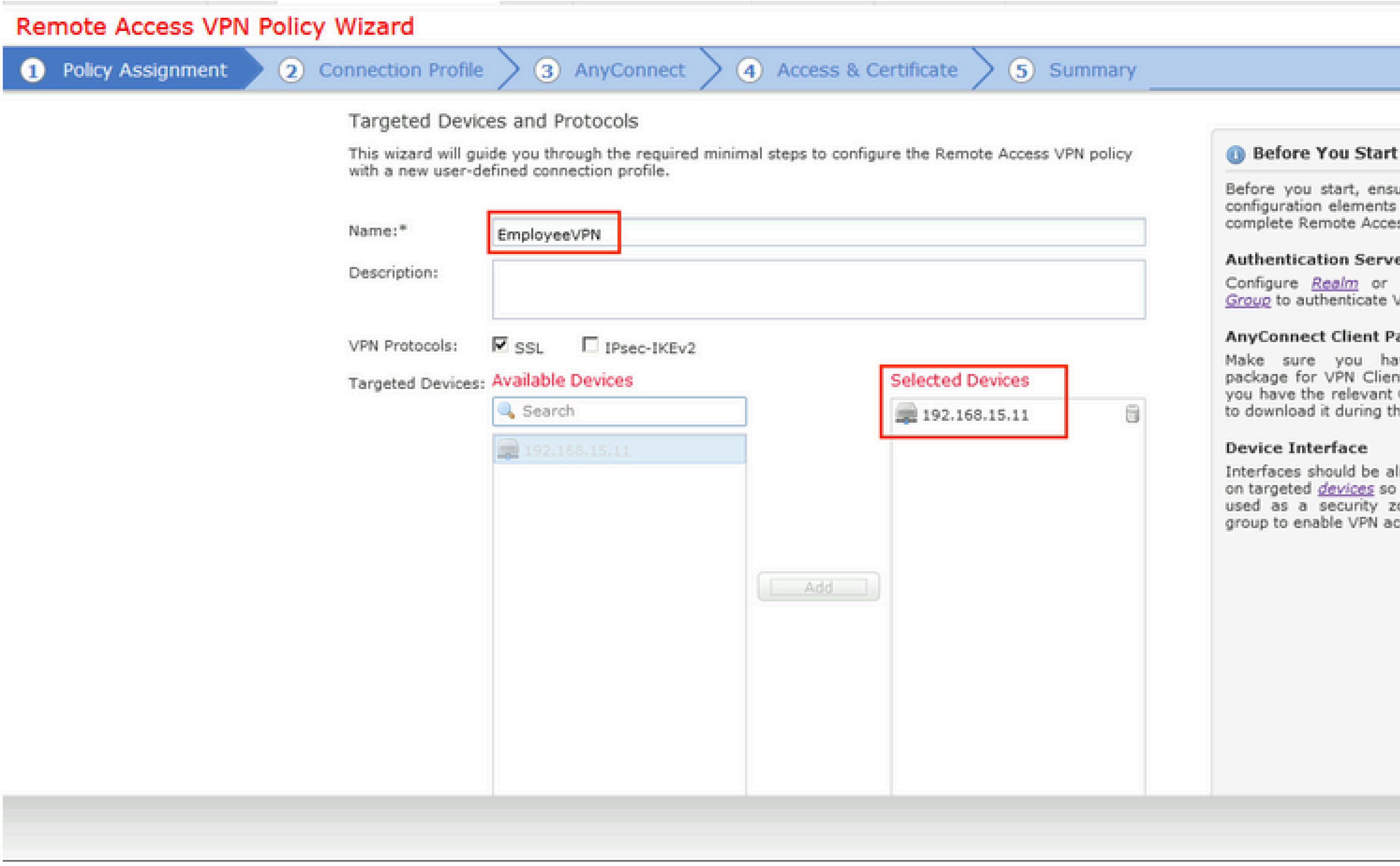
Etapa 9. Inicie o assistente de VPN de acesso remoto. Navegue até **Devices** > **VPN** > **Remote Access** e clique em **Add**.



Name	Status	Last Modified

No configuration available Add a new configuration

Etapa 10. Forneça o nome, marque SSL como VPN Protocol, escolha FTD que é usado como VPN concentrator e clique em **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

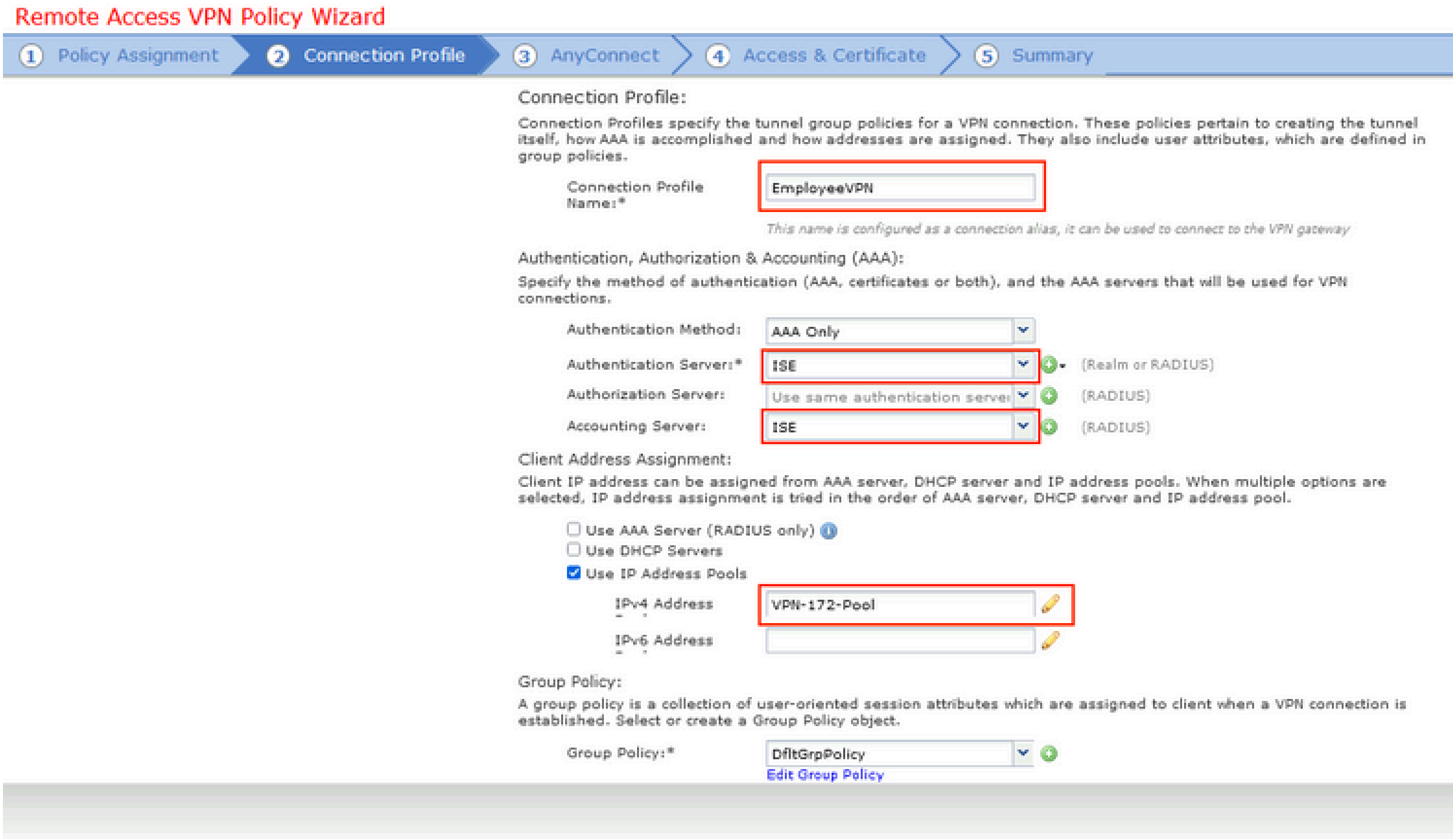
Authentication Serve
Configure Realm or
Group to authenticate V

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 z
group to enable VPN ac

Etapa 11. Forneça o nome do **Perfil de Conexão**, selecione **Servidores de Autenticação/Contabilização**, selecione o pool de endereços que foi configurado anteriormente e clique em **Avançar**.

> **Observação**: não selecione o servidor de autorização. Ele aciona duas solicitações de acesso para um único usuário (uma vez com a senha do usuário e a segunda vez com a senha *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: VPN-172-Pool

IPv6 Address:

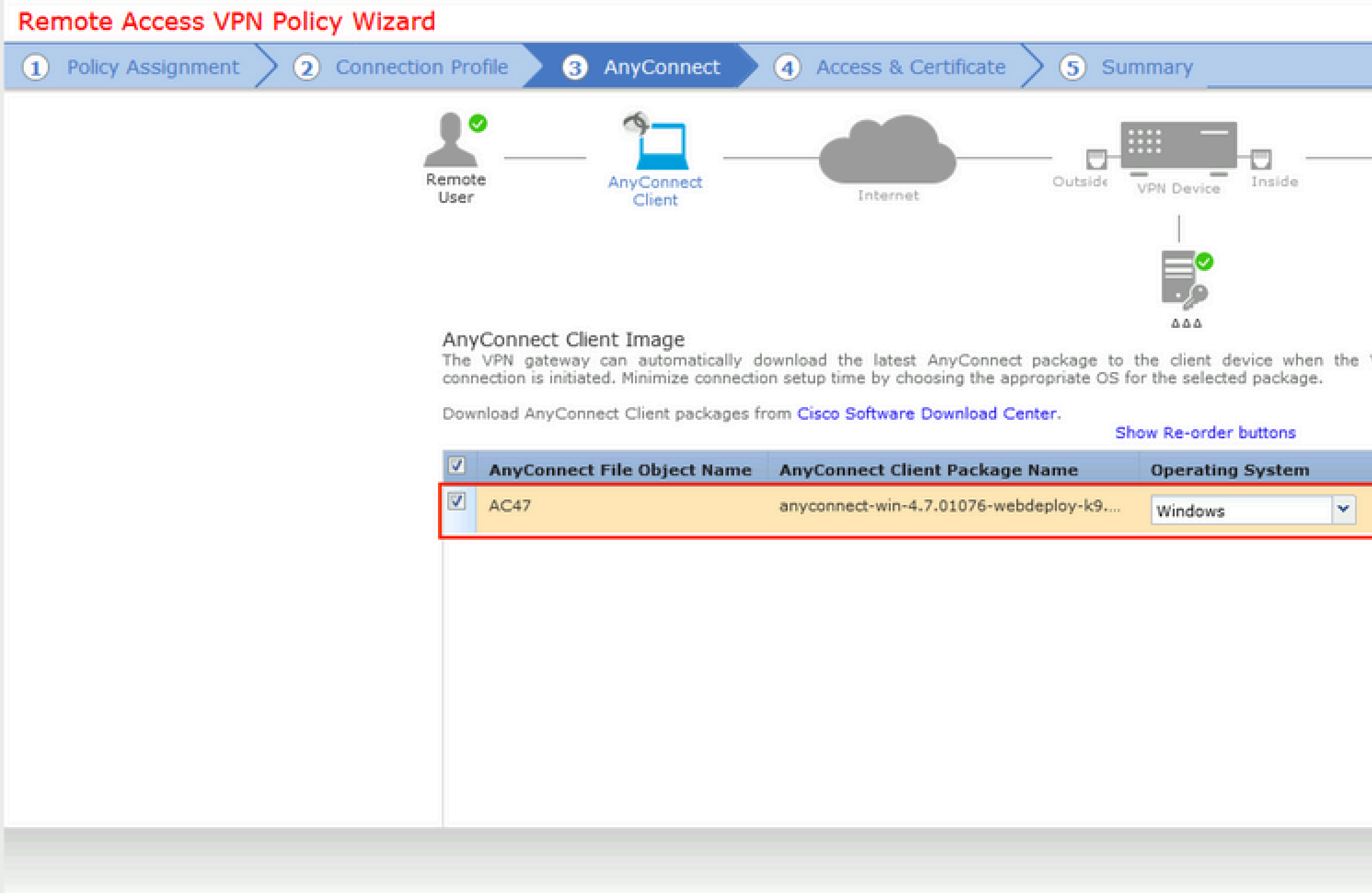
Group Policy:

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

Etapa 12. Selecione o pacote do AnyConnect que foi configurado anteriormente e clique em **Avançar**.



AnyConnect Client Image

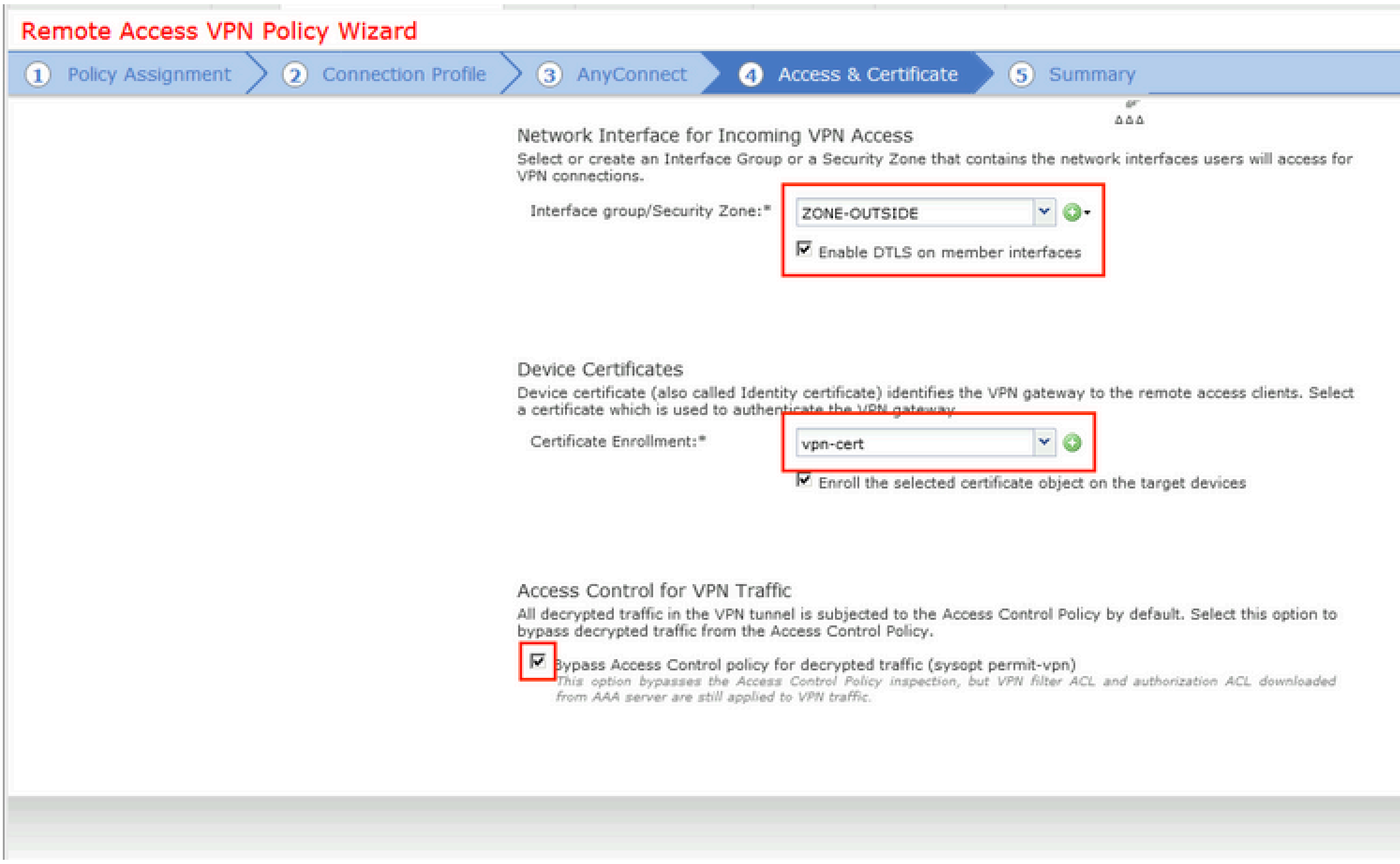
The VPN gateway can automatically download the latest AnyConnect package to the client device when the connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

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

Etapa 13. Selecione a interface da qual o tráfego VPN é esperado, selecione **Certificate Enrollment** que foi configurado anteriormente e clique em **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

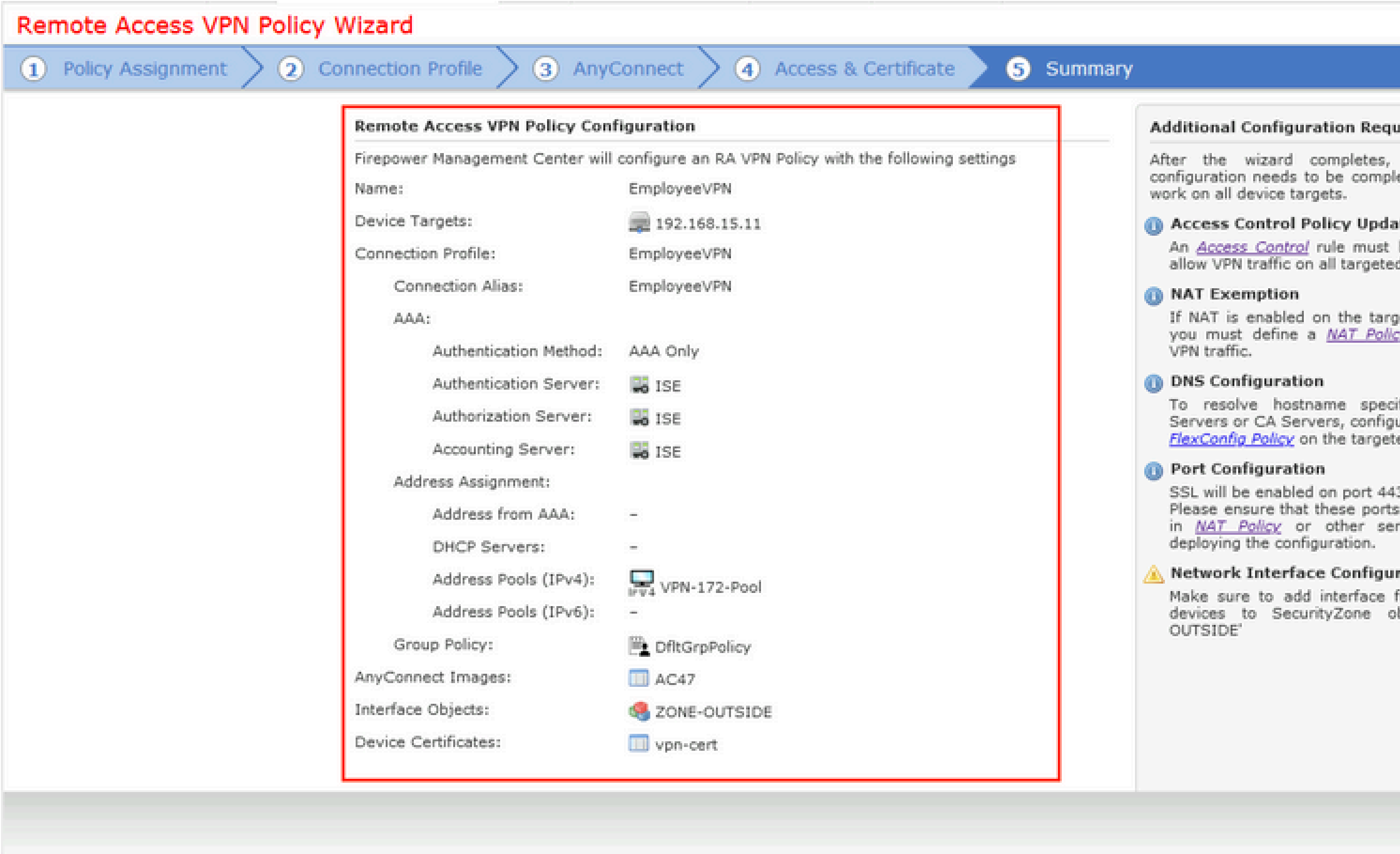
Access Control for VPN Traffic

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.

Etapa 14. Verifique a página de resumo e clique em **Finish**.



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

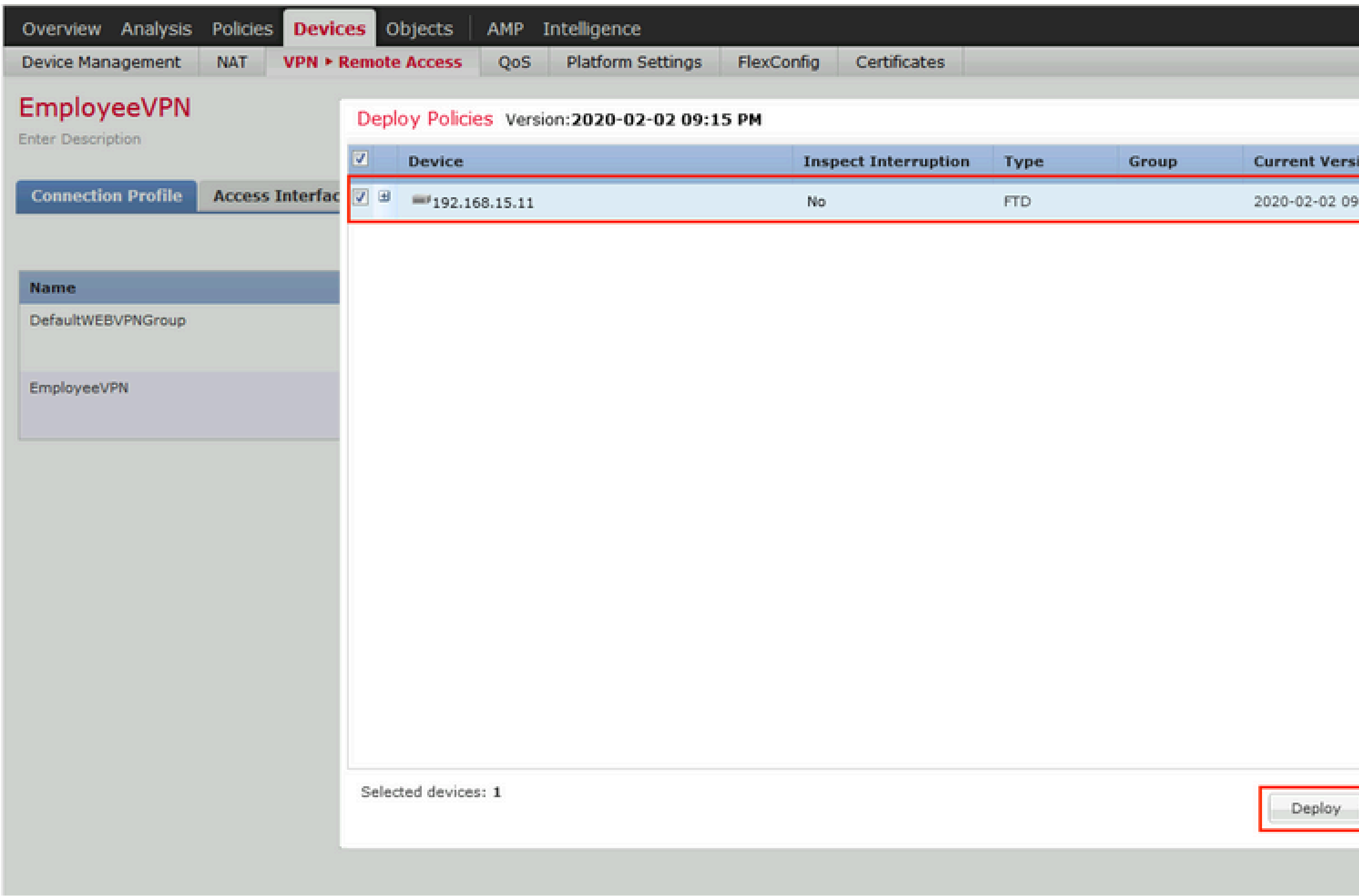
Port Configuration

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'

Etapa 15. Implante a configuração no FTD. Clique em **Deploy** e selecione **FTD** que é usado como um concentrador de VPN.



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

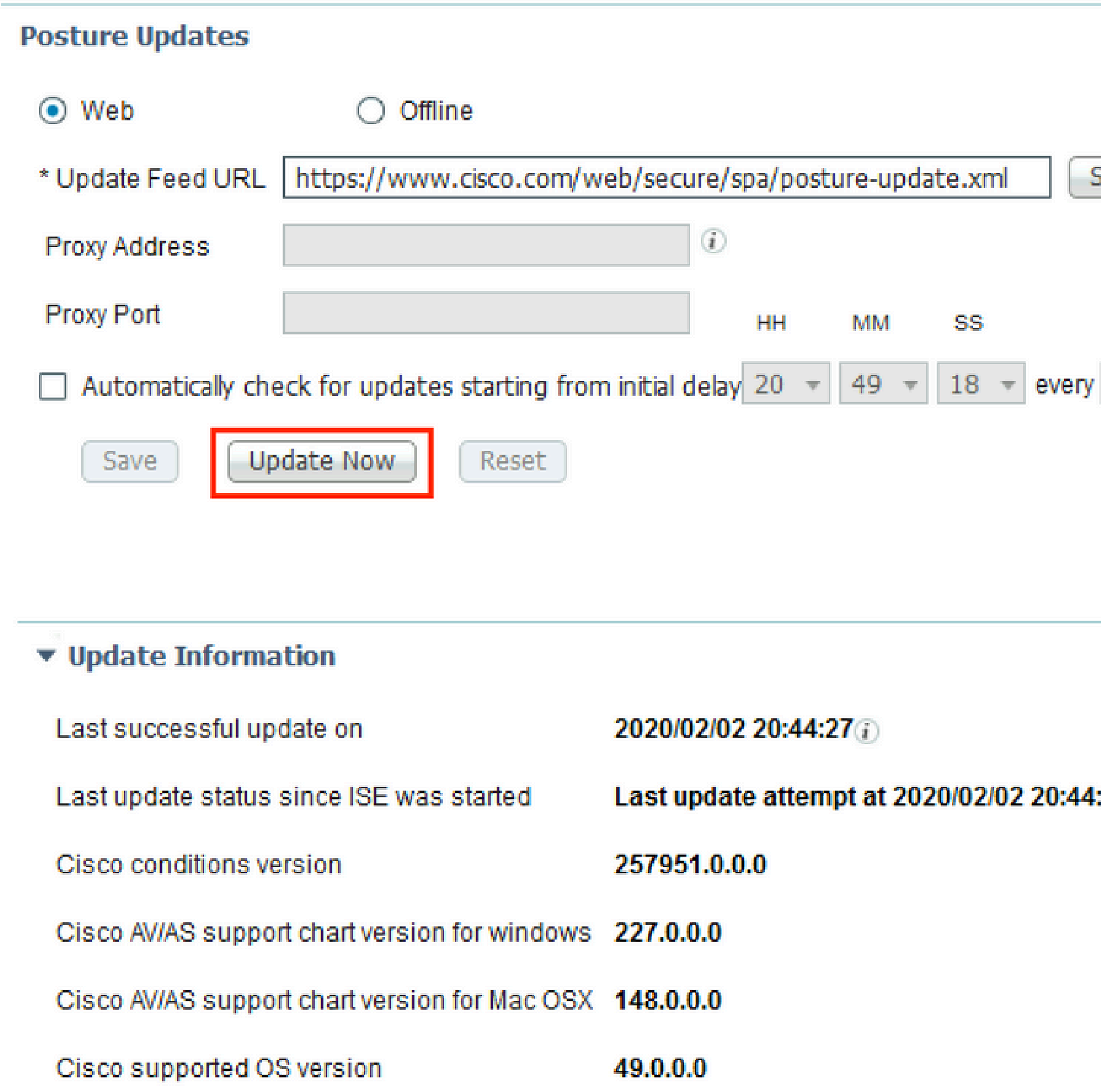
☑		Device	Inspect Interruption	Type	Group	Current Versi
☑	⊞	192.168.15.11	No	FTD		2020-02-02 09

Name
DefaultWEBVPNGroup
EmployeeVPN

Selected devices: 1

ISE

Etapa 1. Execute atualizações de postura. Navegue até **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:

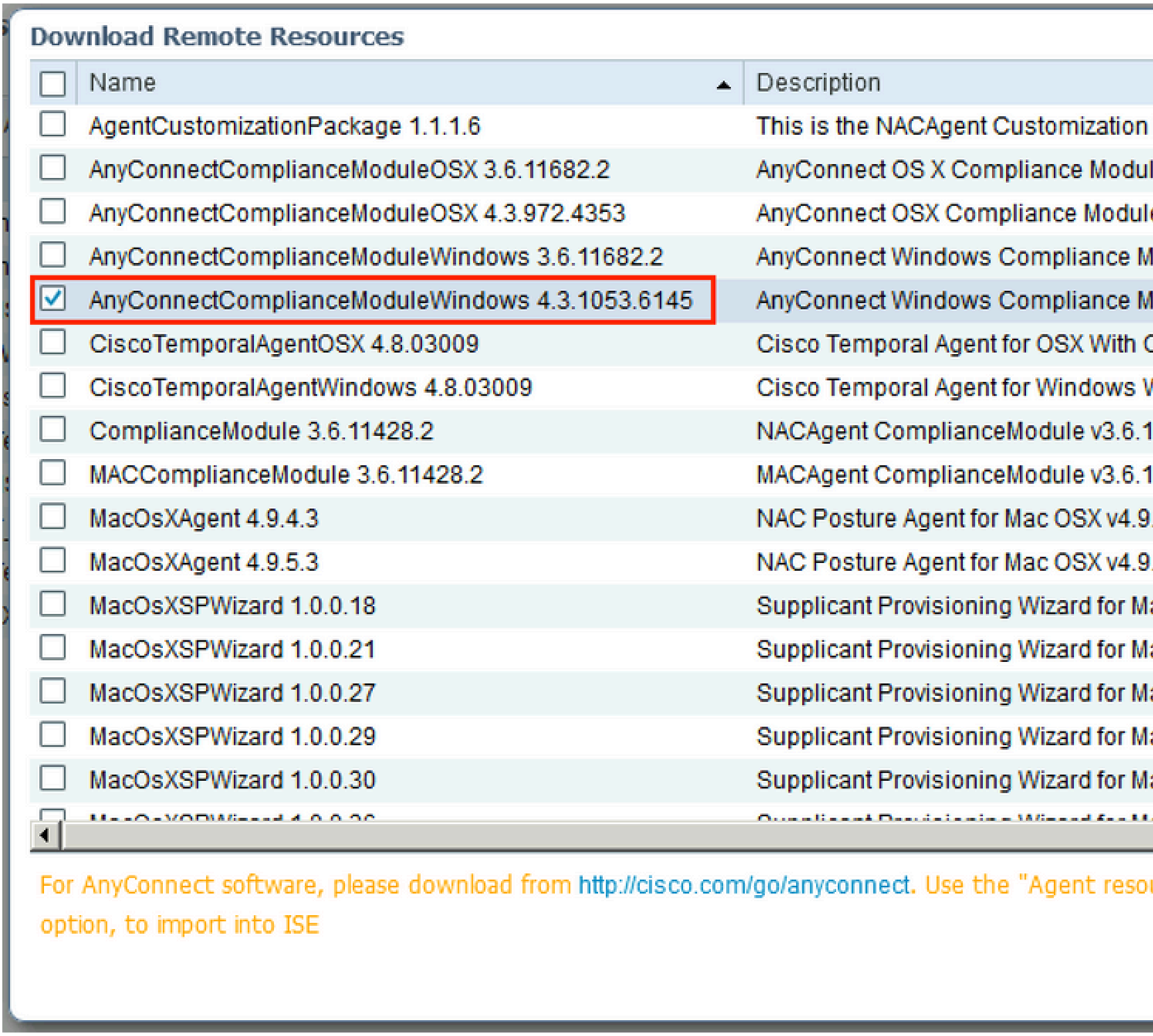
☐ Automatically check for updates starting from initial delay HH 20 MM 49 SS 18 every

Save | Update Now | Reset

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

Etapa 2. Upload Compliance Module (Módulo de conformidade de carregamento). Navegue até **Policy > Policy Elements > Results > Client Provisioning > Resources**. Clique em **Adicionar** e selecione **Recursos do agente no site da Cisco**



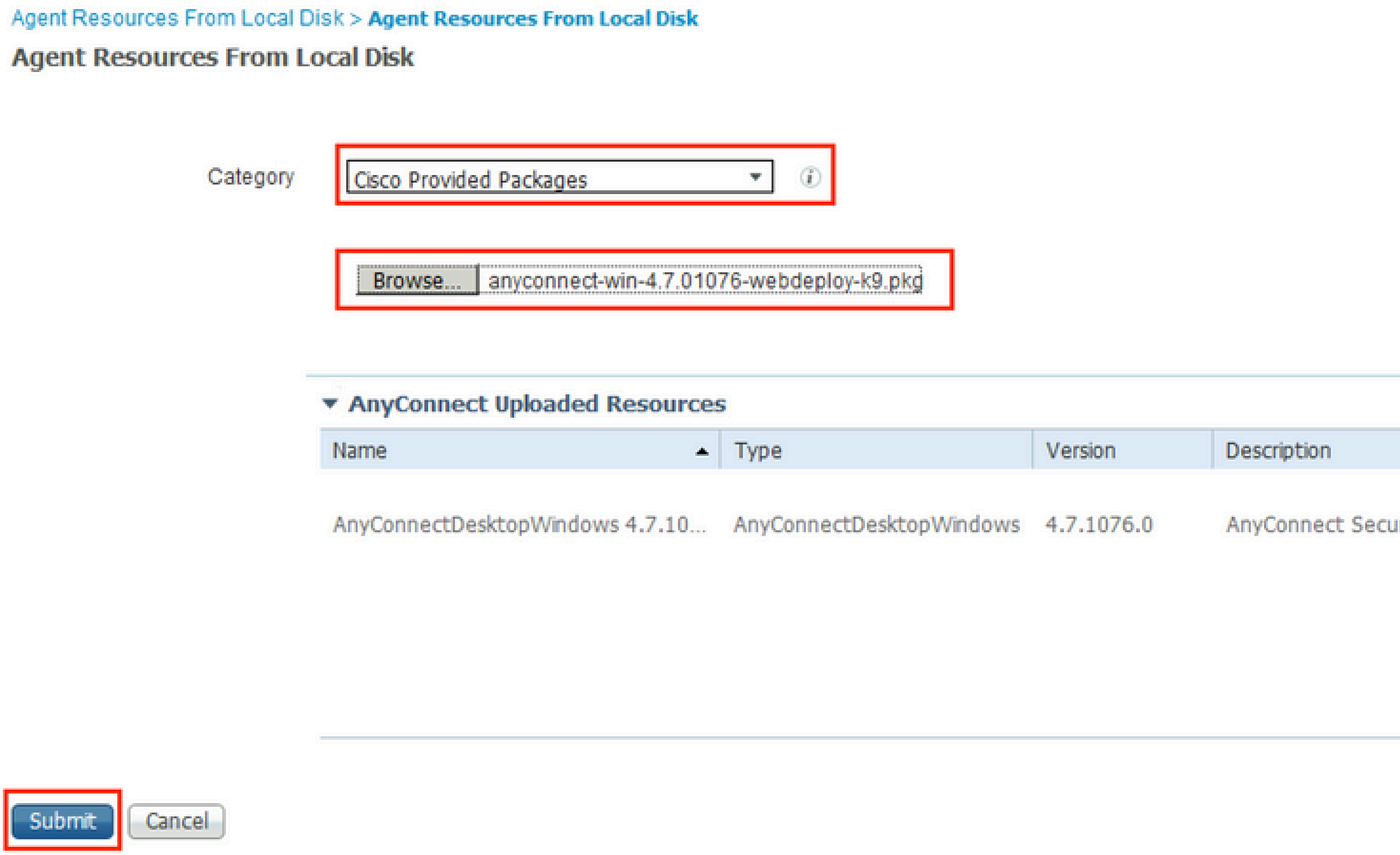
Download Remote Resources

☐	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

Etapa 3. Baixe o AnyConnect do download do software Cisco e carregue-o no ISE. Navegue até **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Clique em **Add** e selecione **Agent Resources From Local Disk**. Escolha **Cisco Provided Packages** em **Category**, selecione o pacote do AnyConnect no disco local e clique em **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

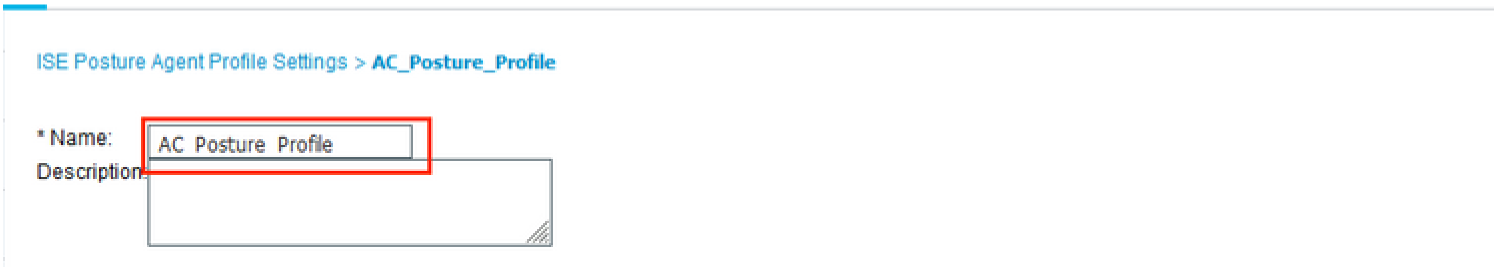
AnyConnect Uploaded Resources

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

Etapa 4. Criar perfil de postura do AnyConnect. Navegue até **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Clique em **Adicionar** e selecione **Perfil de postura do AnyConnect**. Preencha o nome e o protocolo de postura.

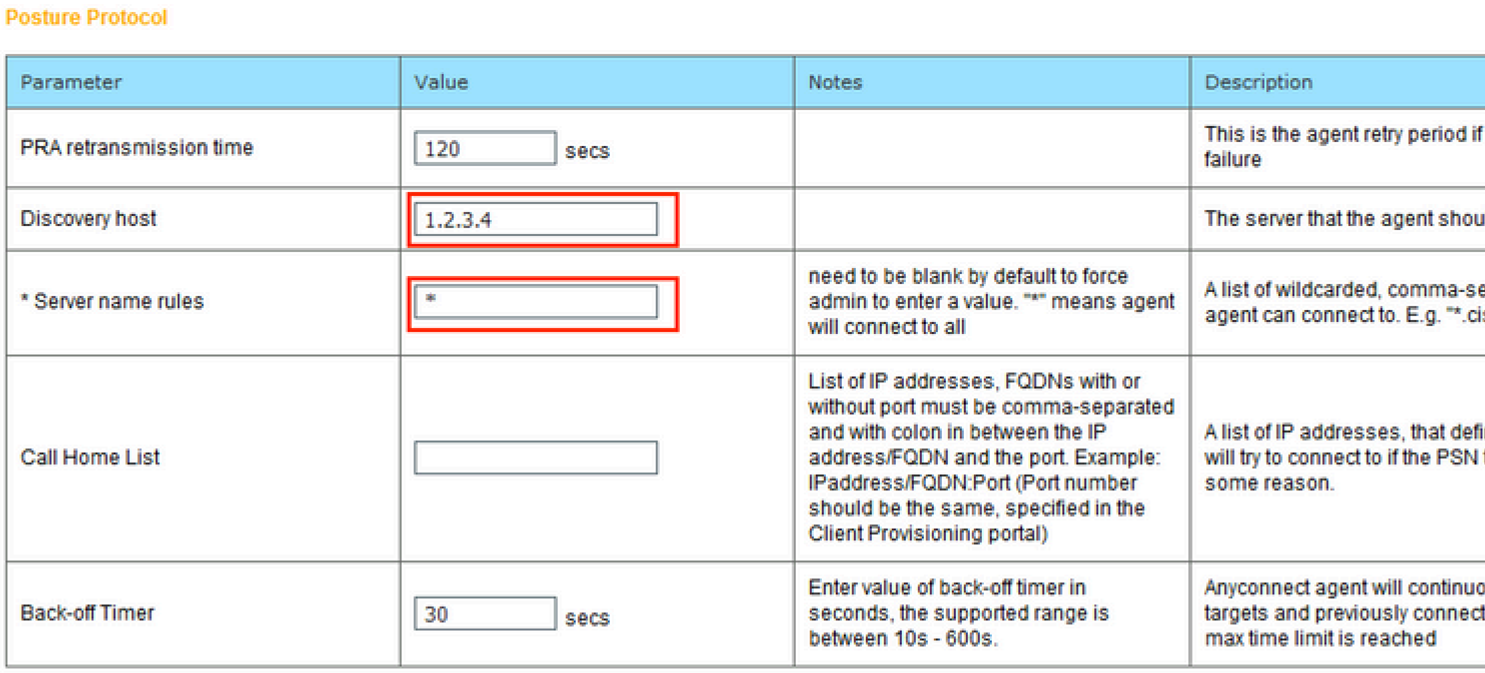
Em ***Server name rules**, coloque ***** e coloque qualquer endereço IP fictício em **Discovery host**.



ISE Posture Agent Profile Settings > **AC_Posture_Profile**

* Name: AC_Posture_Profile

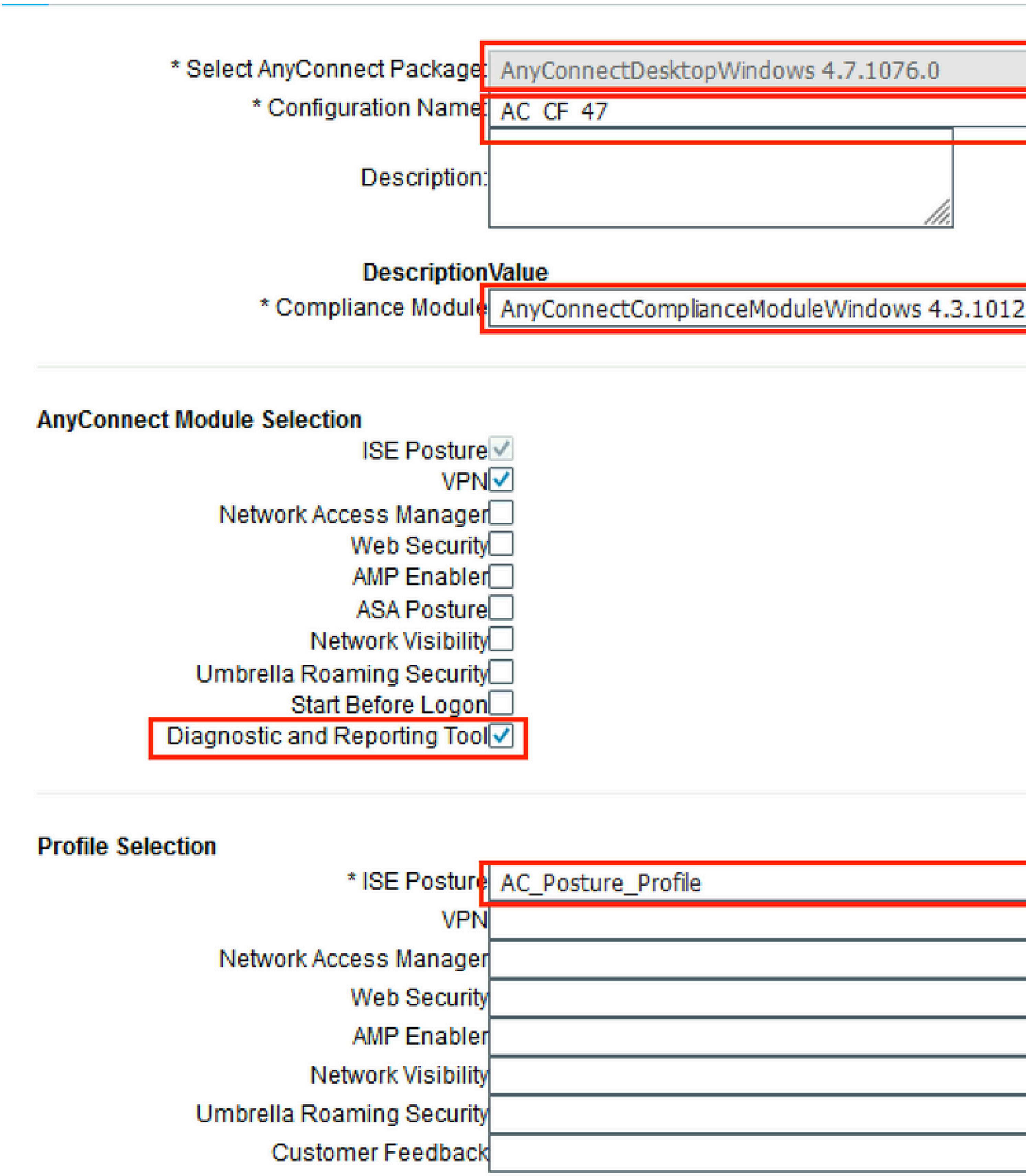
Description:



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

Etapa 5. Navegue para **Policy > Policy Elements > Results > Client Provisioning > Resources** e crie **AnyConnect Configuration**. Clique em **Adicionar** e selecione **Configuração do AnyConnect**. Selecione **AnyConnect** Package**, forneça o nome da configuração, selecione Compliance Module, marque Diagnostic and Reporting Tool, selecione** Posture Profile **e clique em** Save.



* Select AnyConnect Package: AnyConnectDesktopWindows 4.7.1076.0

* Configuration Name: AC_CF_47

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 4.3.1012

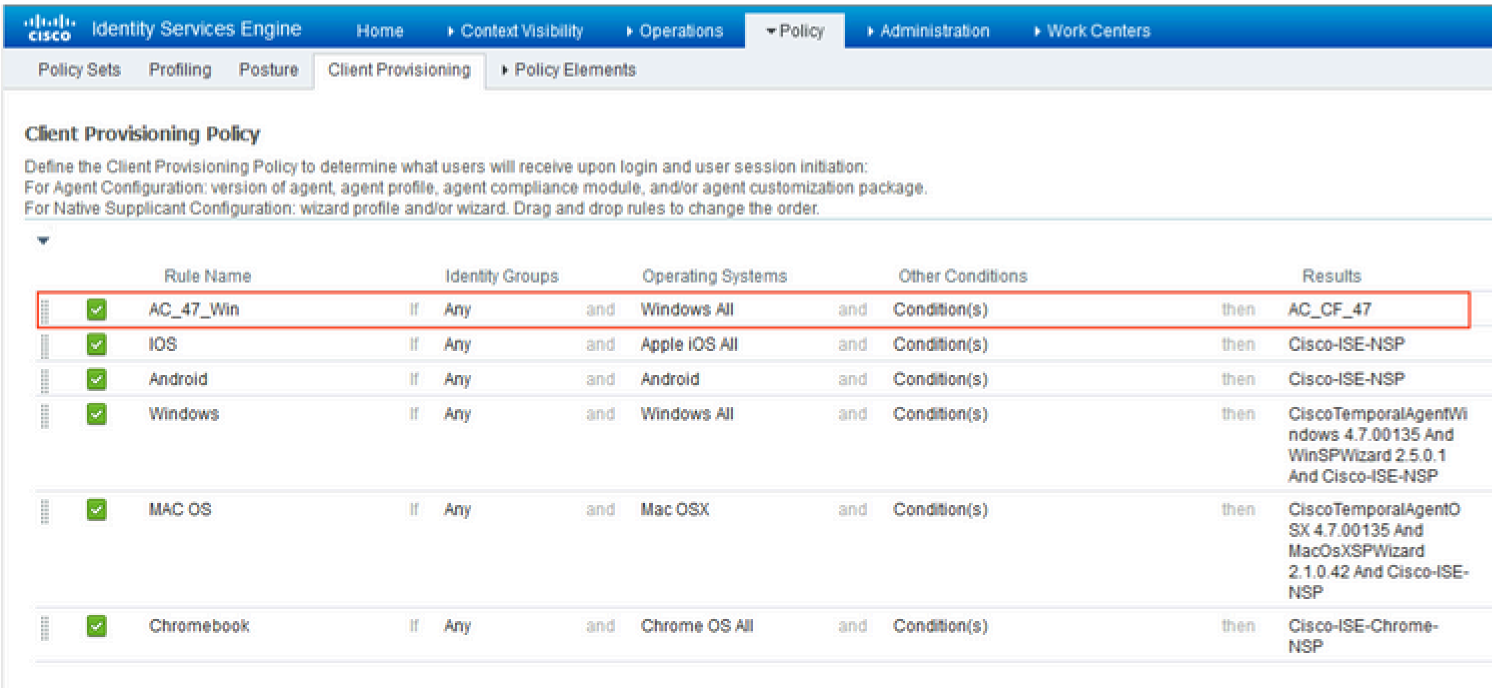
AnyConnect Module Selection

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:

Etapa 6. Navegue até **Policy** > **Client Provisioning** e crie **Client Provisioning Policy**. Clique em **Editar** e selecione **Inserir regra acima**, forneça o nome, selecione SO e escolha **Configuração do AnyConnect** que foi criada na etapa anterior.



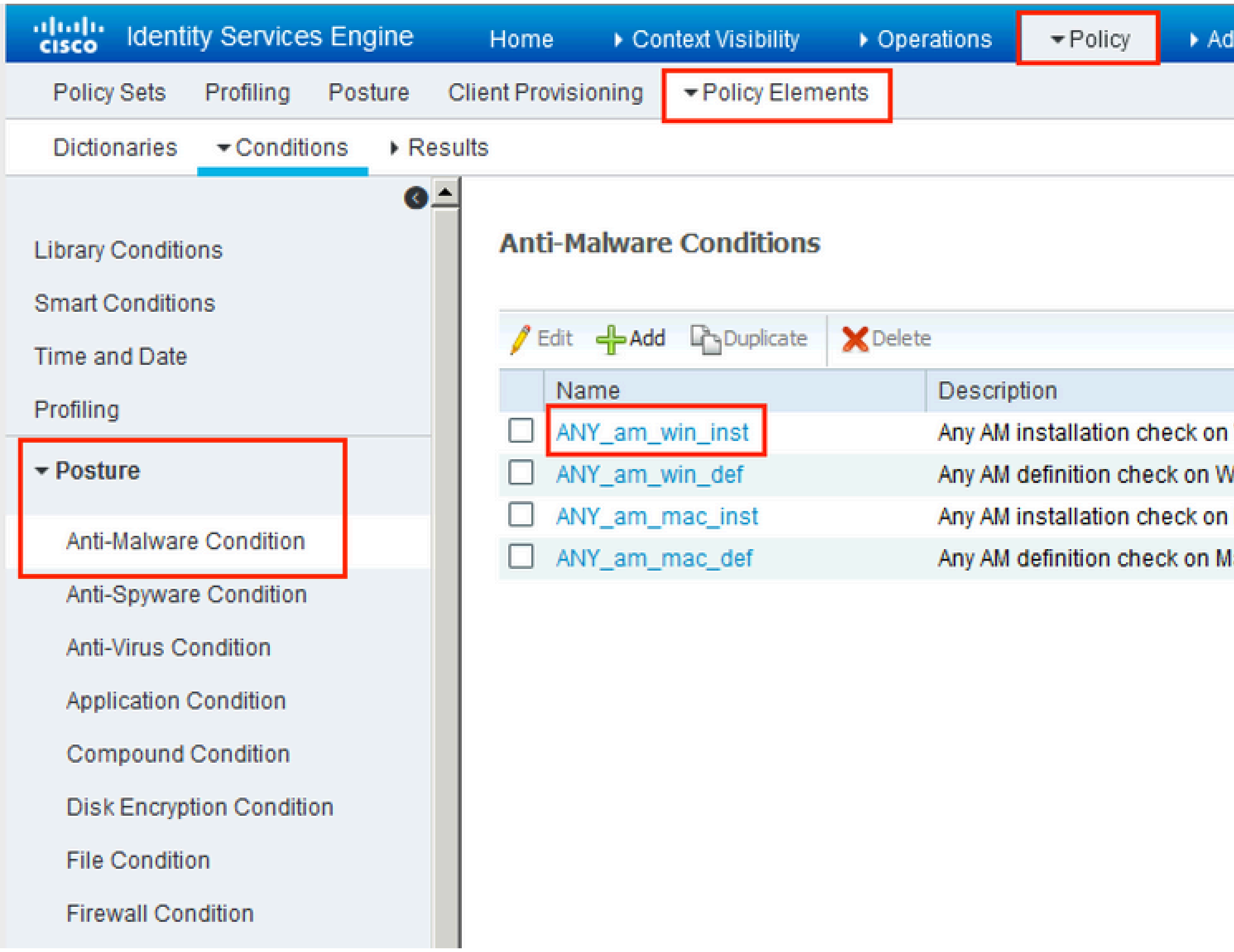
Client Provisioning Policy

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

Passo 7. Crie uma condição de postura em **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Anti-Malware Condition**. Neste exemplo, é usado o predefinido "ANY_am_win_inst".

.

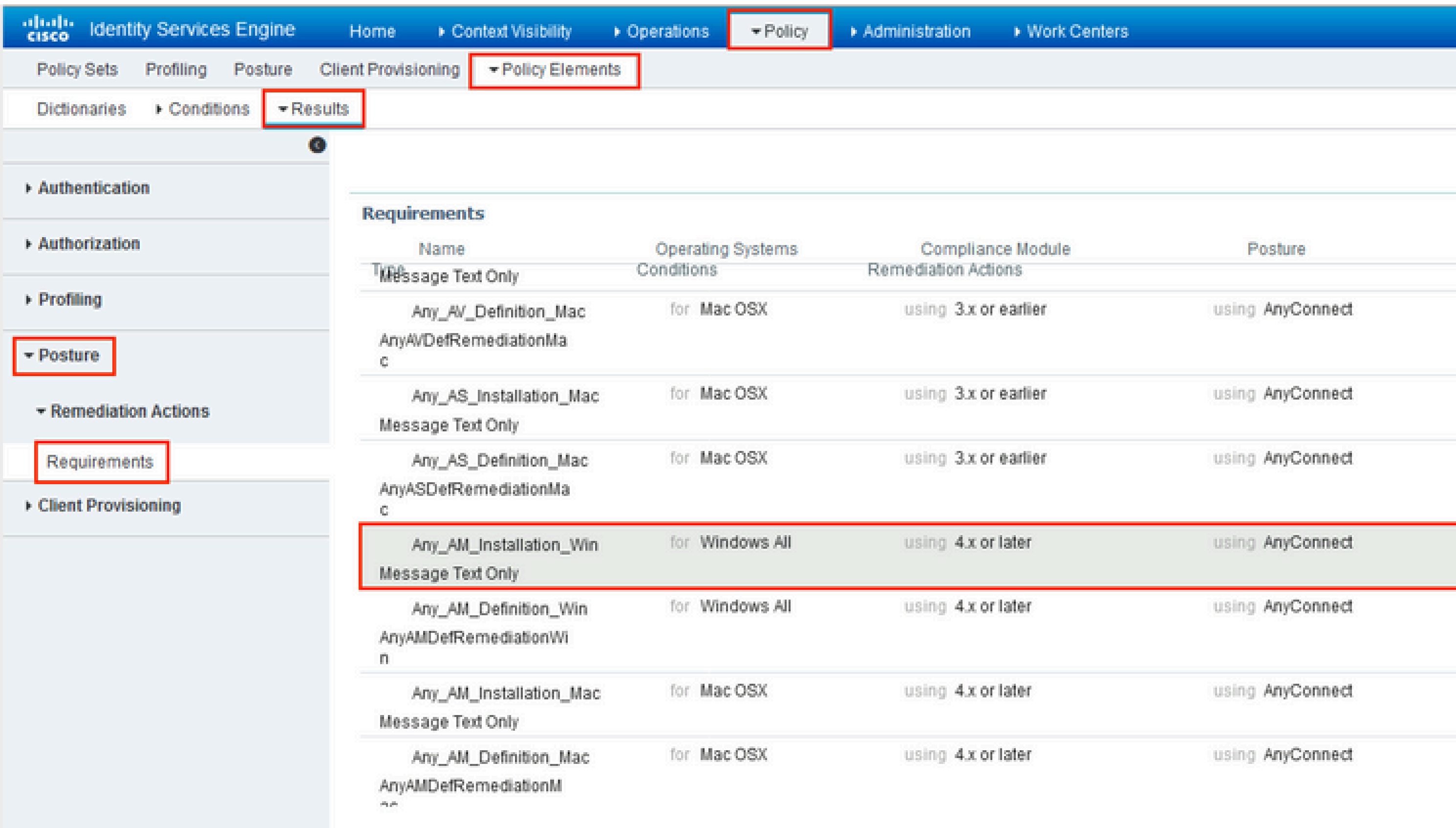


Anti-Malware Conditions

	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

Etapa 8. Navegue para **Política** > **Elementos de política** > **Resultados** > **Postura** > **Ações de correção** e crie **Remediação de postura**. Neste exemplo, ele é ignorado. A ação de correção pode ser uma mensagem de texto.

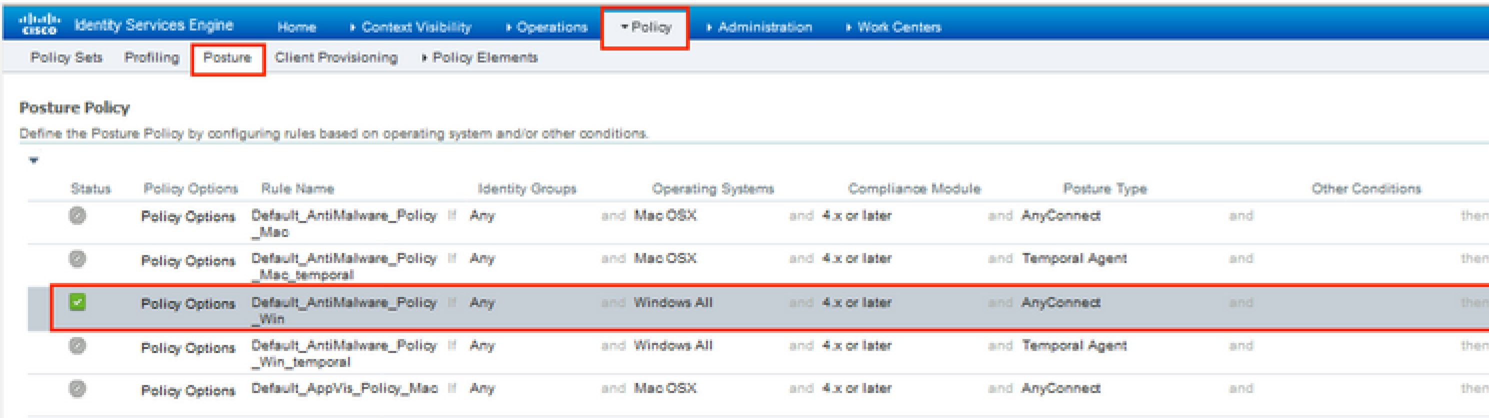
Etapa 9. Navegue para **Política** > **Elementos de política** > **Resultados** > **Postura** > **Requisitos** e crie **Requisitos de postura**. Requisito predefinido Any_AM_Installation_Win é usado.



Requirements

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

Etapa 10. Crie políticas de postura em **Policies** > **Posture**. A política de postura padrão para qualquer verificação de antimalware para o sistema operacional Windows é usada.



Posture Policy

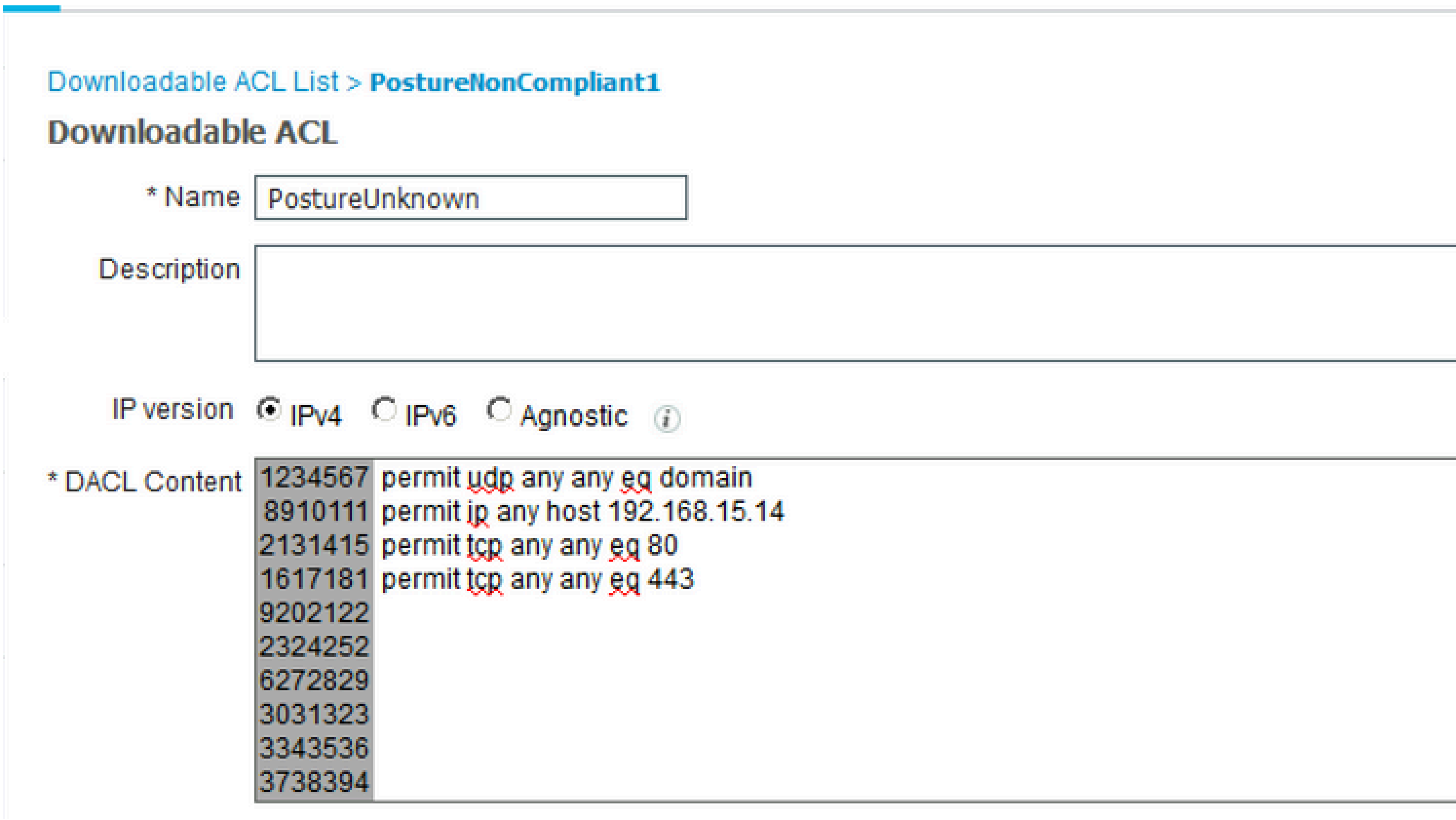
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

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

Etapa 11. Navegue até **Policy** > **Policy Elements** > **Results** > **Authorization** > **Downlodable ACLS e** crie DACLs para diferentes status de postura.

Neste exemplo:

- Posture Unknown DACL - permite o tráfego para DNS, PSN e tráfego HTTP e HTTPS.
- Posture NonCompliant DACL - nega o acesso a sub-redes privadas e permite apenas o tráfego da Internet.
- Permit All DACL (Permitir todos os DACLs) - permite todo o tráfego para o Status de conformidade com a postura.



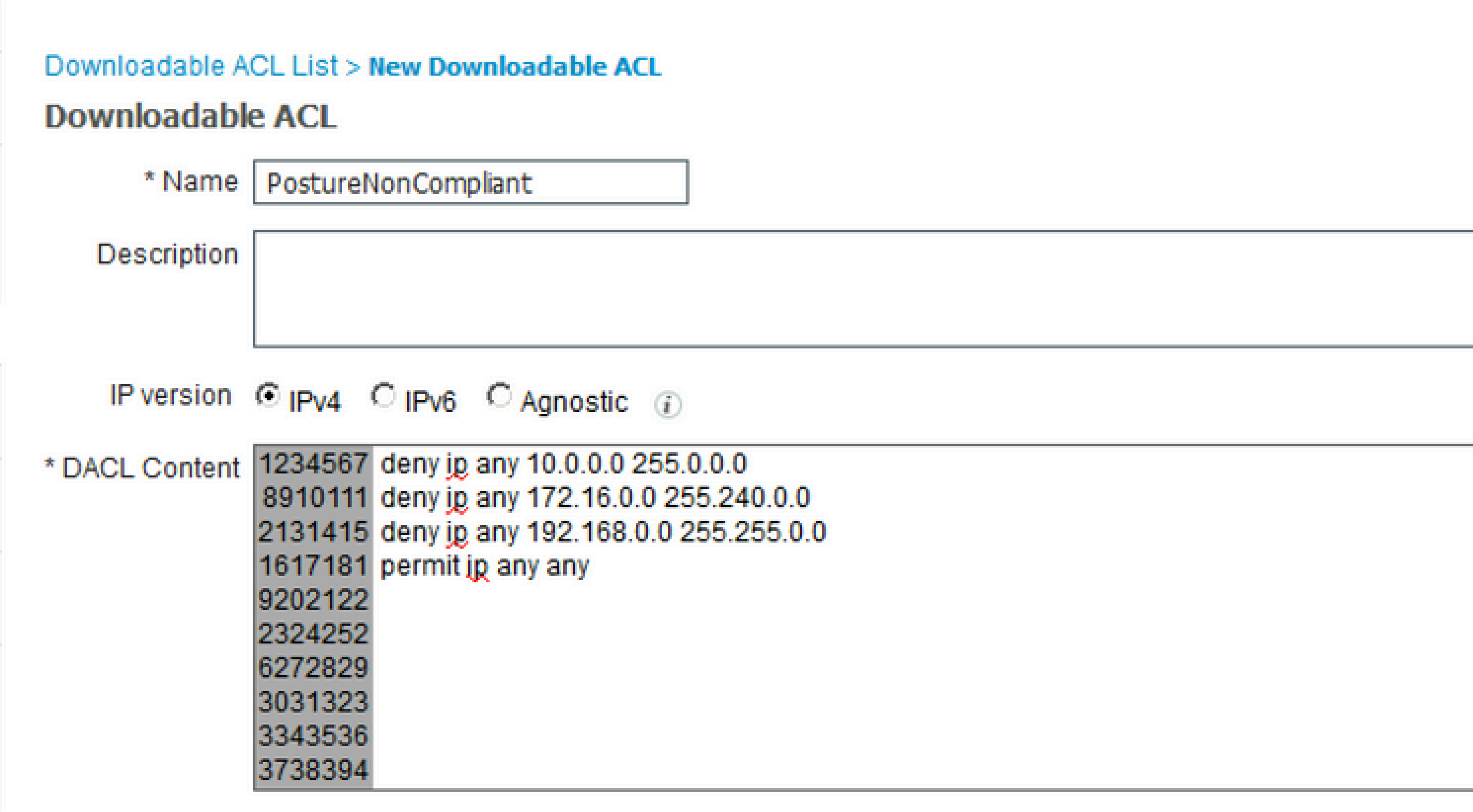
Downloadable ACL List > **PostureNonCompliant1**

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
```



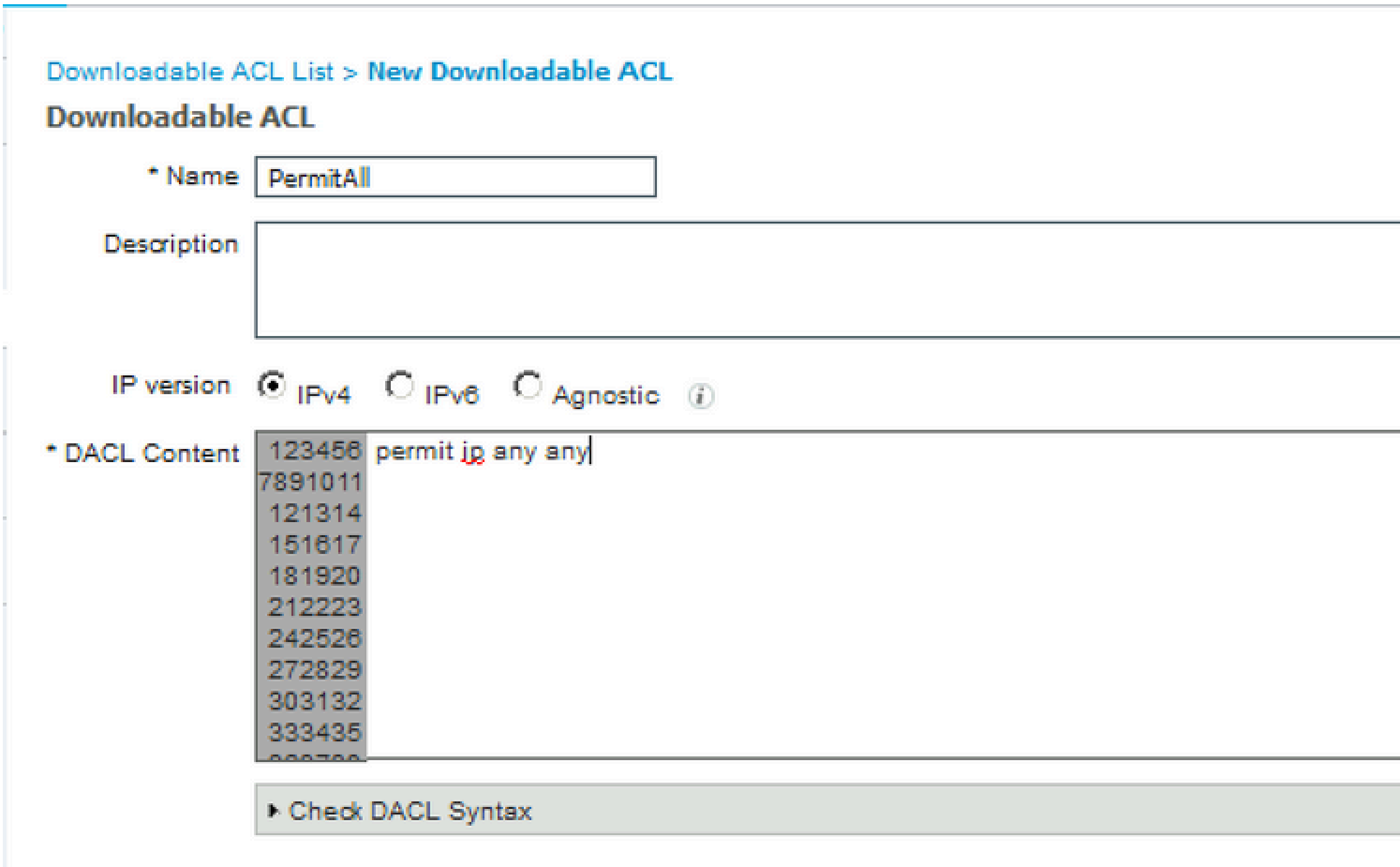
Downloadable ACL List > **New Downloadable ACL**

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

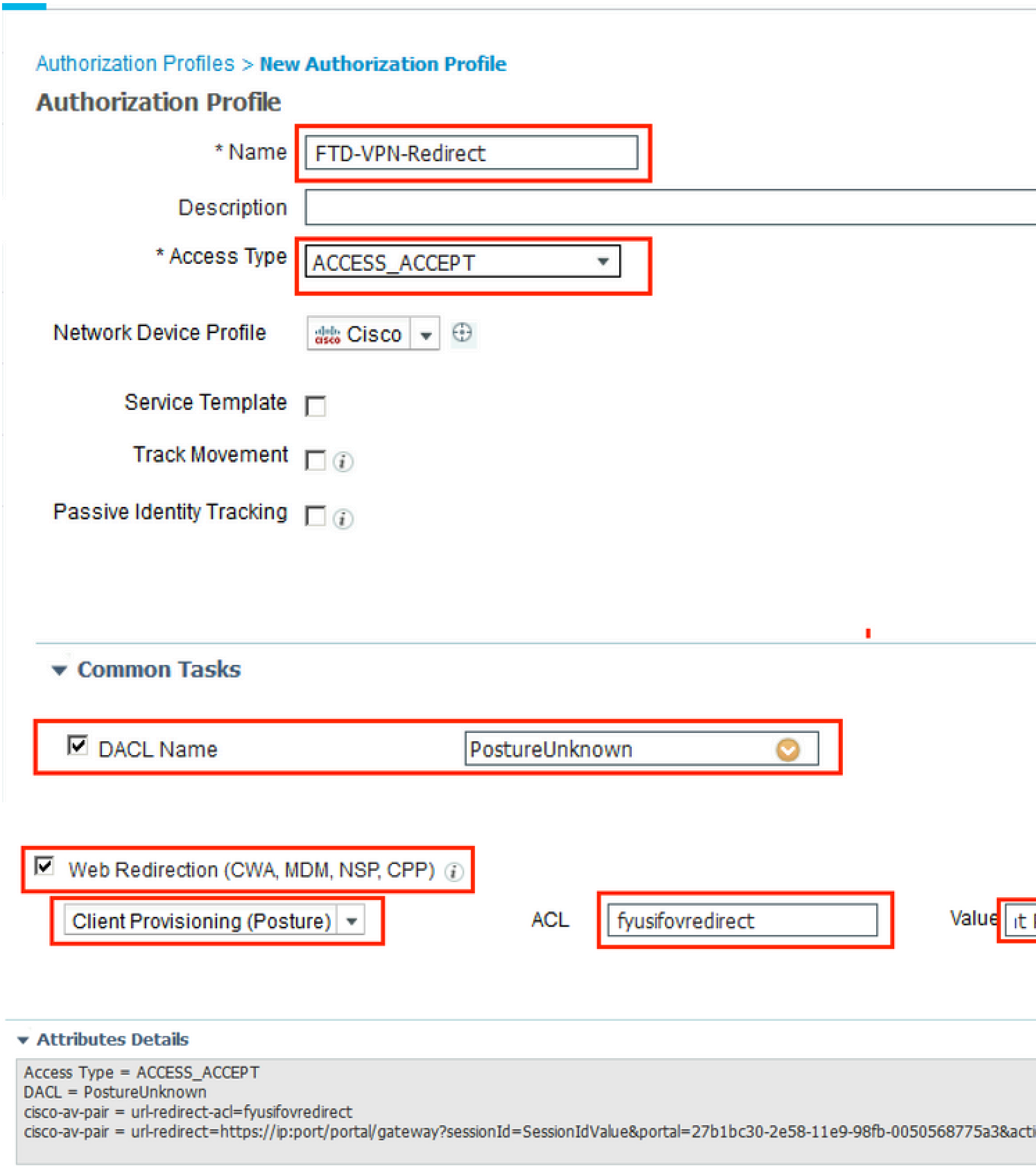
Description

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

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

Etapa 12. Crie três perfis de autorização para os status Posture Unknown, Posture NonCompliant e Posture Compliant. Para fazer isso, navegue para **Política** > **Elementos de política** > **Resultados** > **Autorização** > **Perfis de autorização**. No perfil **Posture Unknown**, selecione **Posture Unknown DACL**, marque **Web Redirection**, selecione **Client Provisioning**, forneça o nome da ACL de redirecionamento (que está configurado no FTD) e selecione o 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

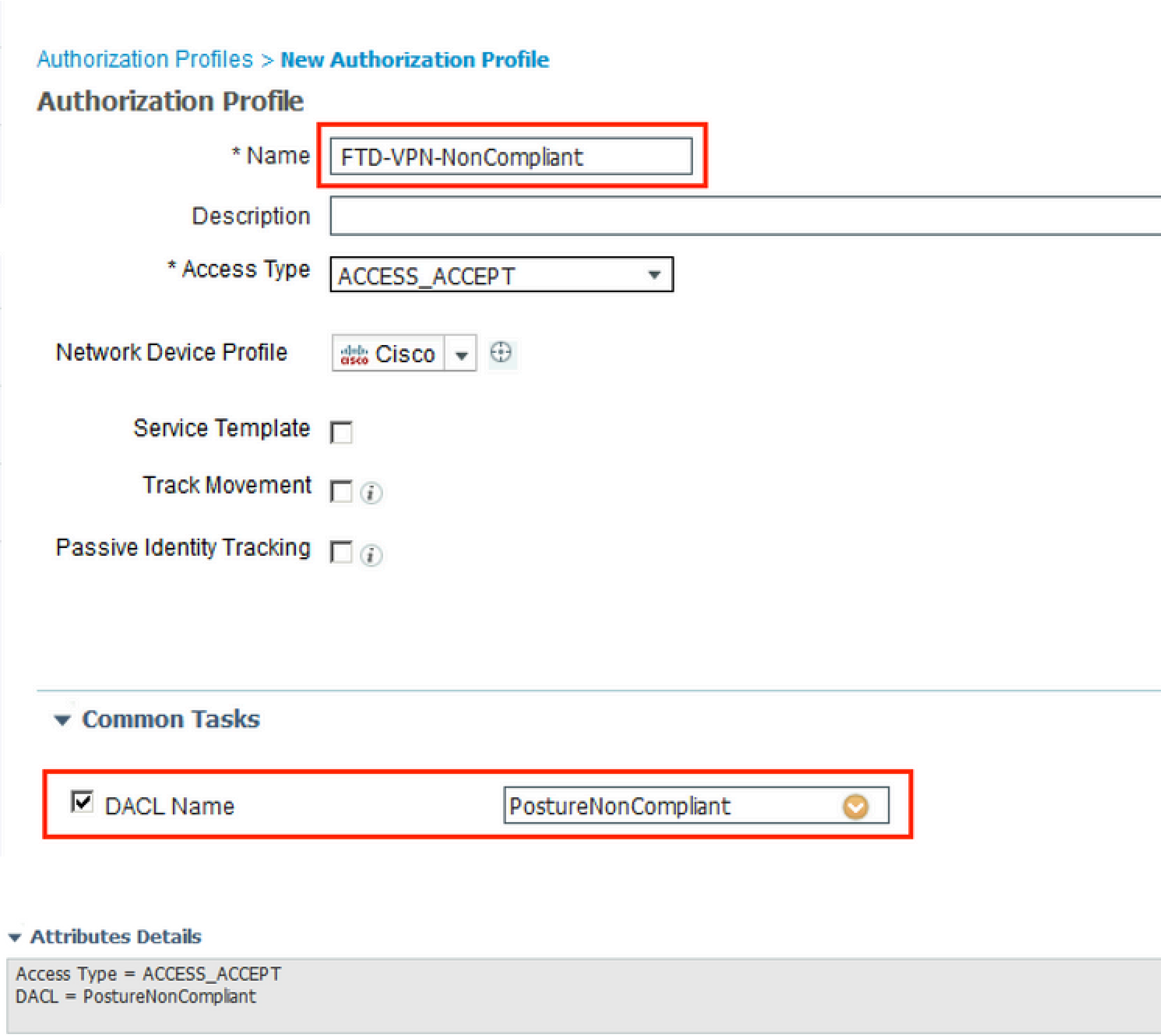
☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: fyusifovredirect Value: it I

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
```

No perfil **Posture NonCompliant**, selecione **DACL** para limitar o acesso à rede.



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 □

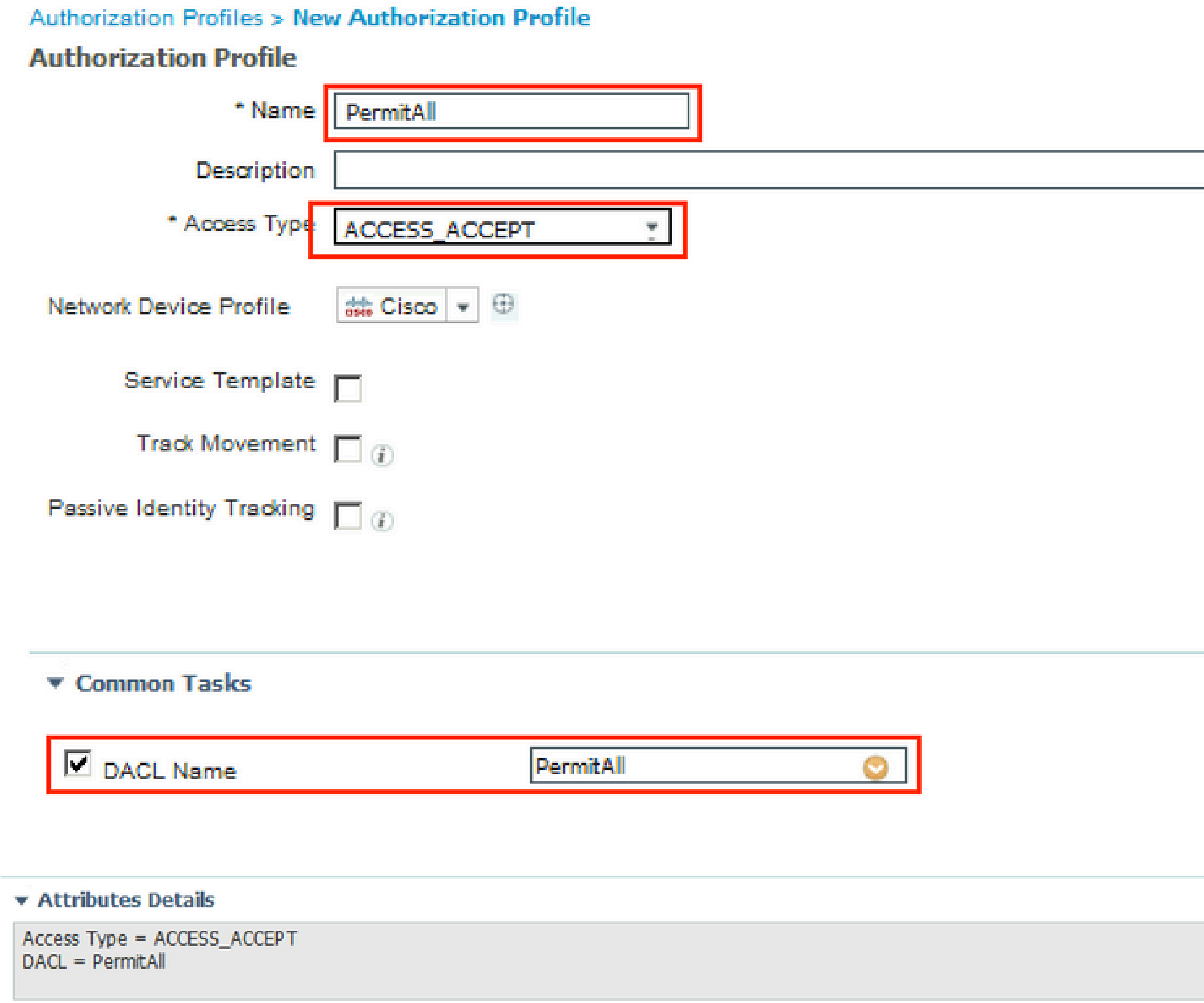
Common Tasks

☑ DACL Name: PostureNonCompliant

Attributes Details

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

No perfil **Posture Compliant**, selecione **DACL** para permitir acesso total à rede.



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: □

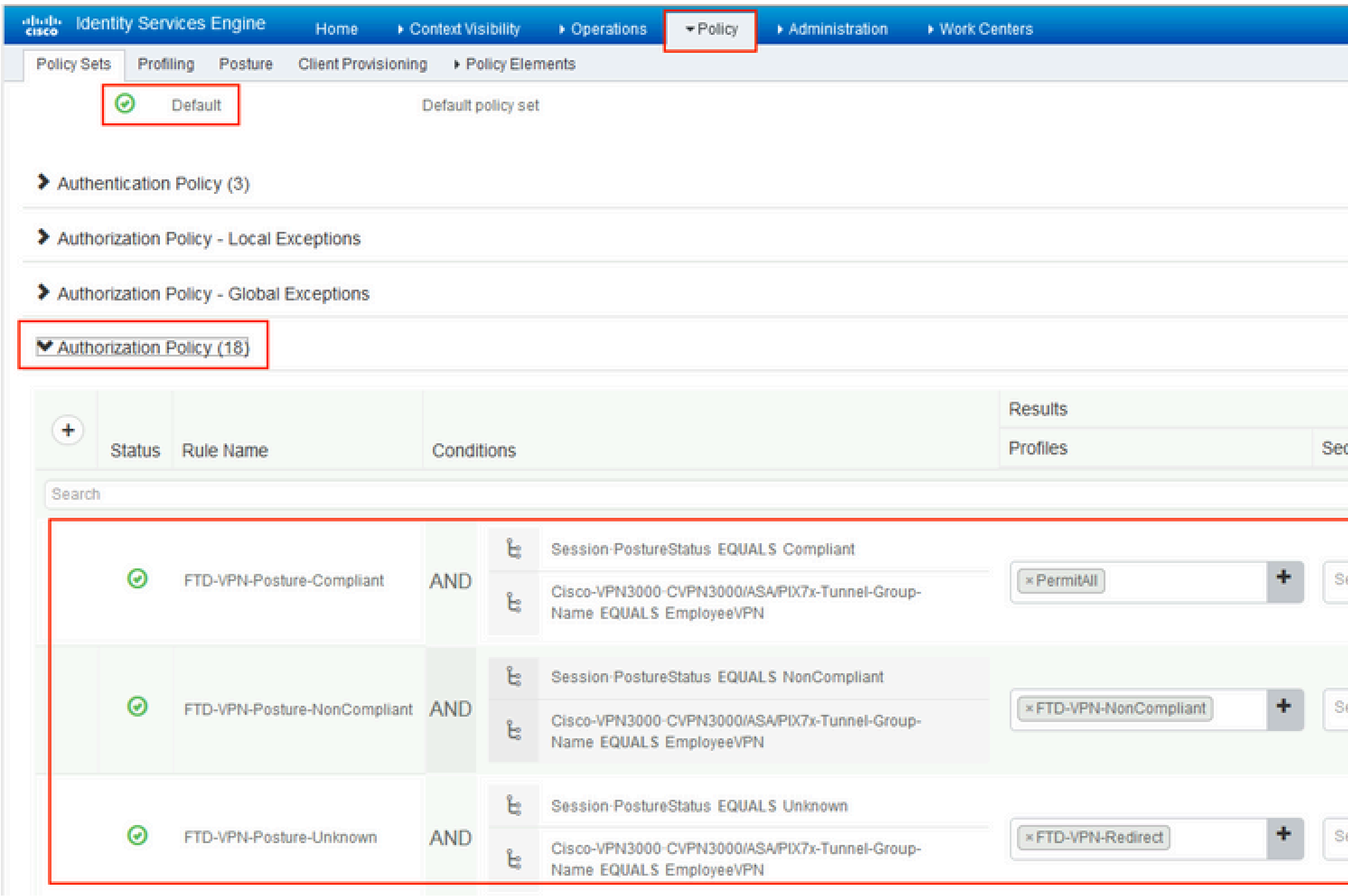
Common Tasks

☑ DACL Name: PermitAll

Attributes Details

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

Etapa 13. Crie políticas de autorização em **Policy** > **Policy Sets** > **Default** > **Authorization Policy**. Como condição, o Status da postura e o Nome do grupo de túneis VPN são usados.



Default — Default policy set

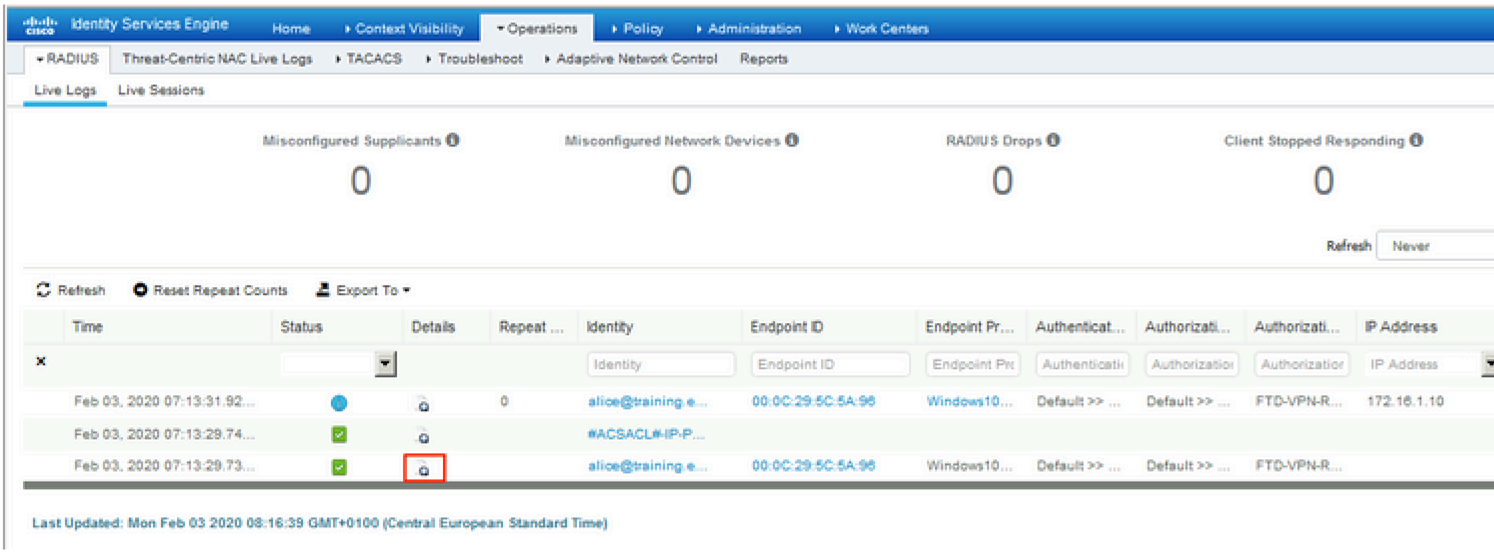
- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (18)

Status	Rule Name	Conditions		Results: 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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

No ISE, a primeira etapa de verificação é o RADIUS Live Log. Navegue até **Operations** > **RADIUS Live Log**. Aqui, o usuário Alice está conectado e a política de autorização esperada está selecionada.



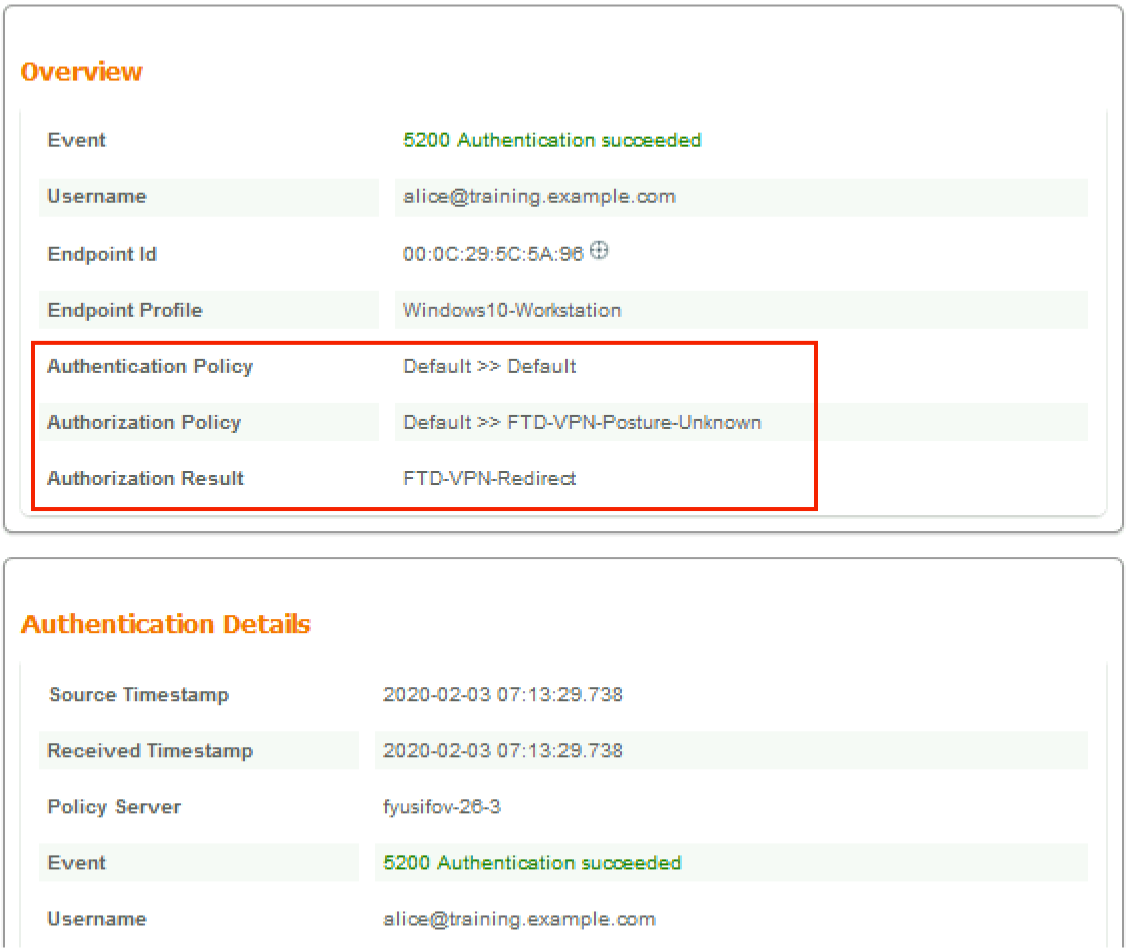
Misconfigured Supplicants 0 — Misconfigured Network Devices 0 — RADIUS Drops 0 — Client Stopped Responding 0

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)

A política de autorização FTD-VPN-Posture-Unknown é correspondida e, como resultado, FTD-VPN-Profile é enviado para FTD.



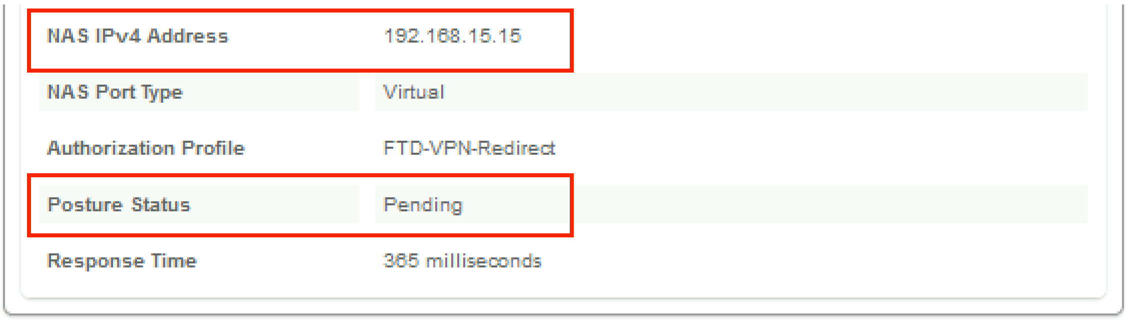
Overview

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

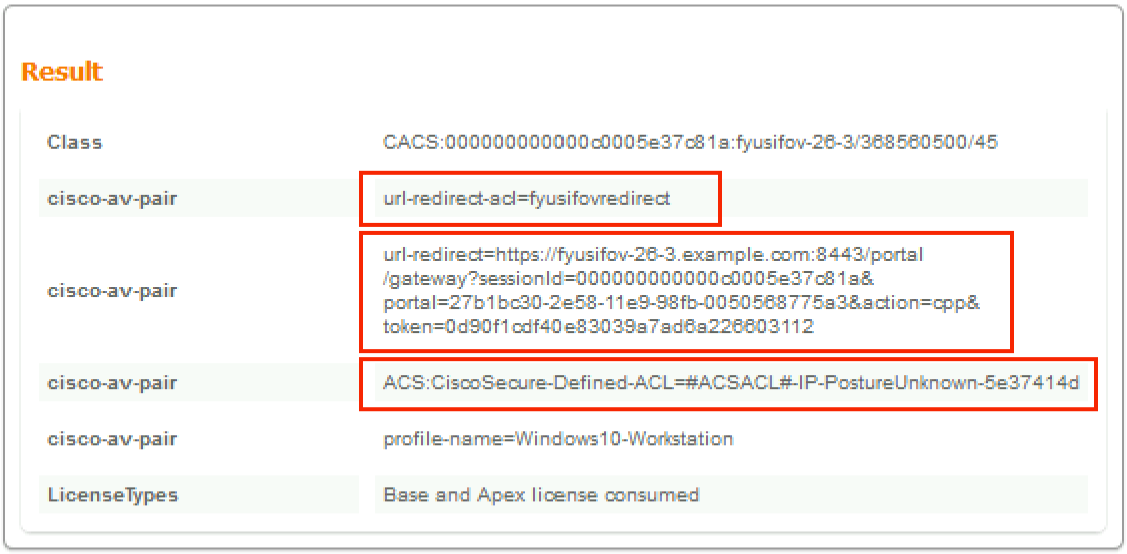
Source Timestamp	2020-02-03 07:13:29.738
Received Timestamp	2020-02-03 07:13:29.738
Policy Server	fyusifov-26-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

Status de postura pendente.



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

A seção Resultado mostra quais atributos são enviados ao 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

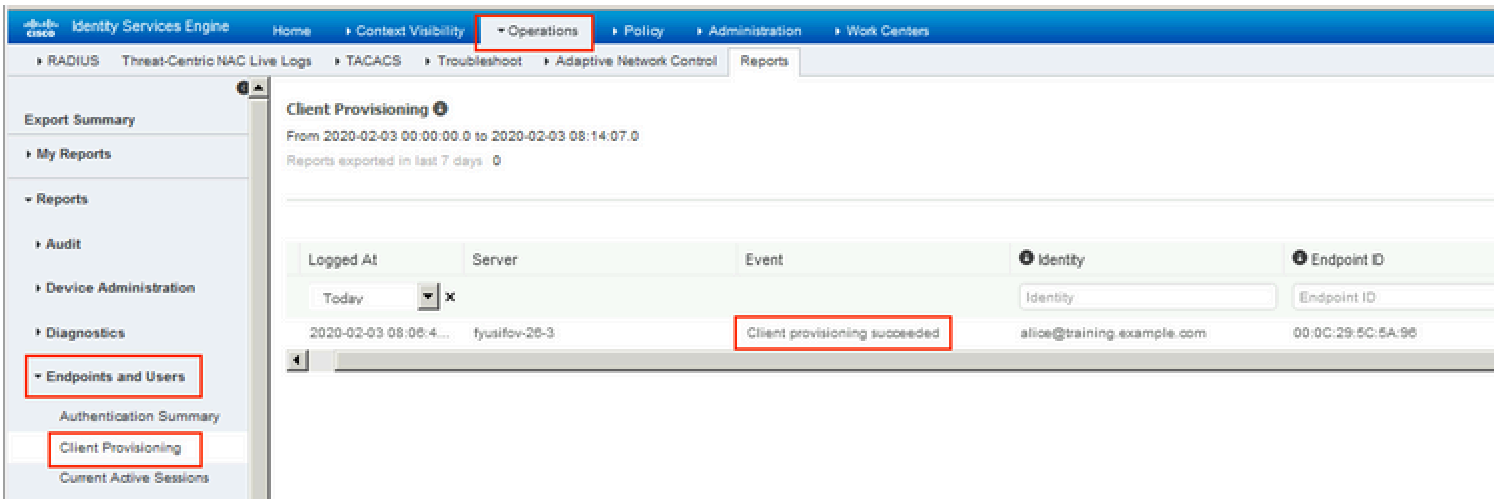
No FTD, para verificar a conexão VPN, execute SSH para a caixa, execute **system support diagnostic-cli** e, em seguida, **show vpn-sessiondb detail anyconnect**. A partir dessa saída, verifique se os atributos enviados do ISE são aplicados a essa sessão VPN.

<#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#
```

As políticas de provisionamento de clientes podem ser verificadas. Navegue até **Operações > Relatórios > Pontos de extremidade e Usuários > Provisionamento de cliente**.



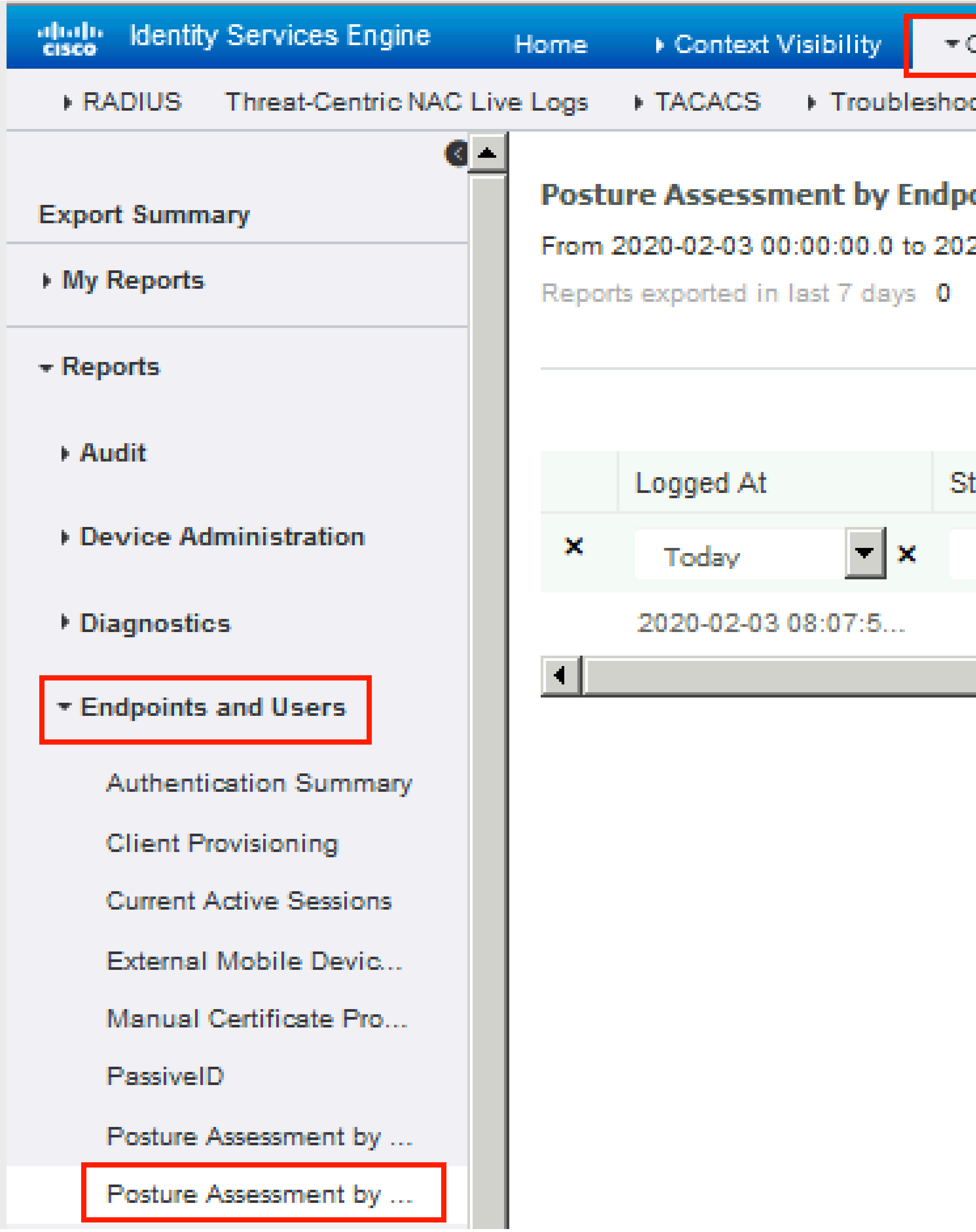
Client Provisioning

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

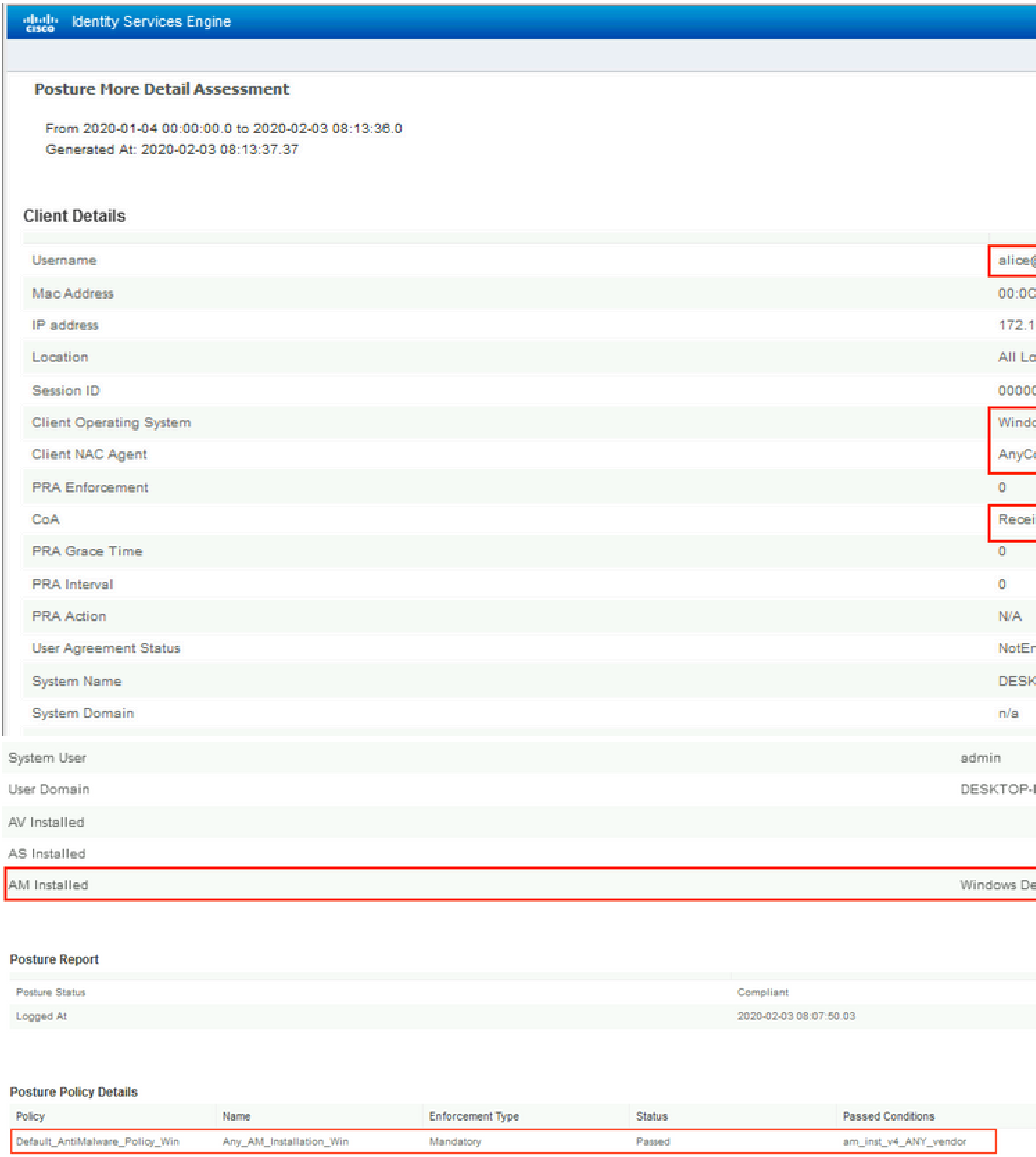
Reports exported in last 7 days 0

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

O relatório de postura enviado do AnyConnect pode ser verificado. Navegue até **Operations > Reports > Endpoints and Users > Posture Assessment by Endpoint**.



Para ver mais detalhes sobre o relatório de postura, clique em **Detalhes**.



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	0000C
Client Operating System	Windo
Client NAC Agent	AnyC
PRA Enforcement	0
CoA	Recei
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEr
System Name	DESK
System Domain	n/a
System User	admin
User Domain	DESKTOP-I
AV Installed	
AS Installed	
AM Installed	Windows De

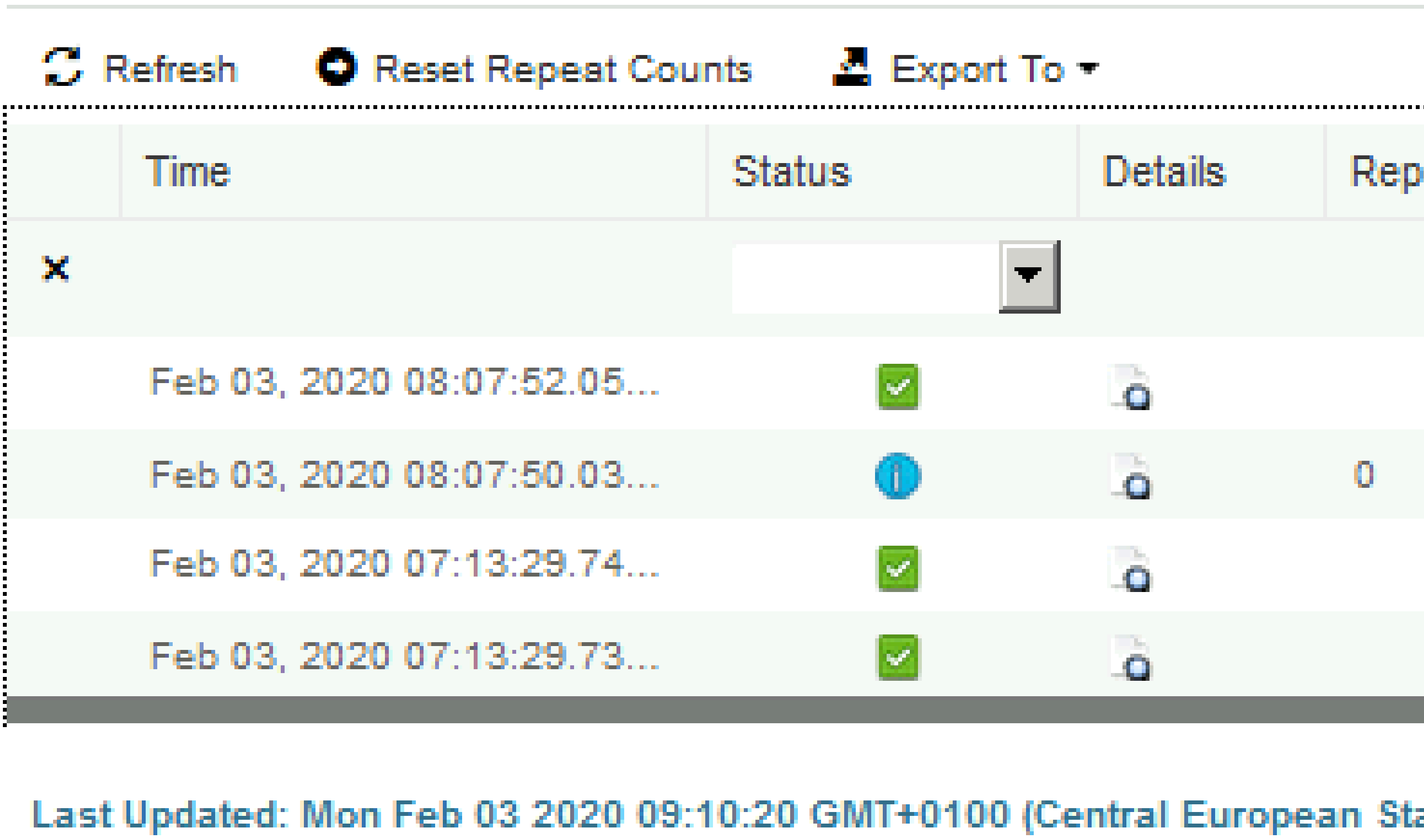
Posture Report

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

Posture Policy Details

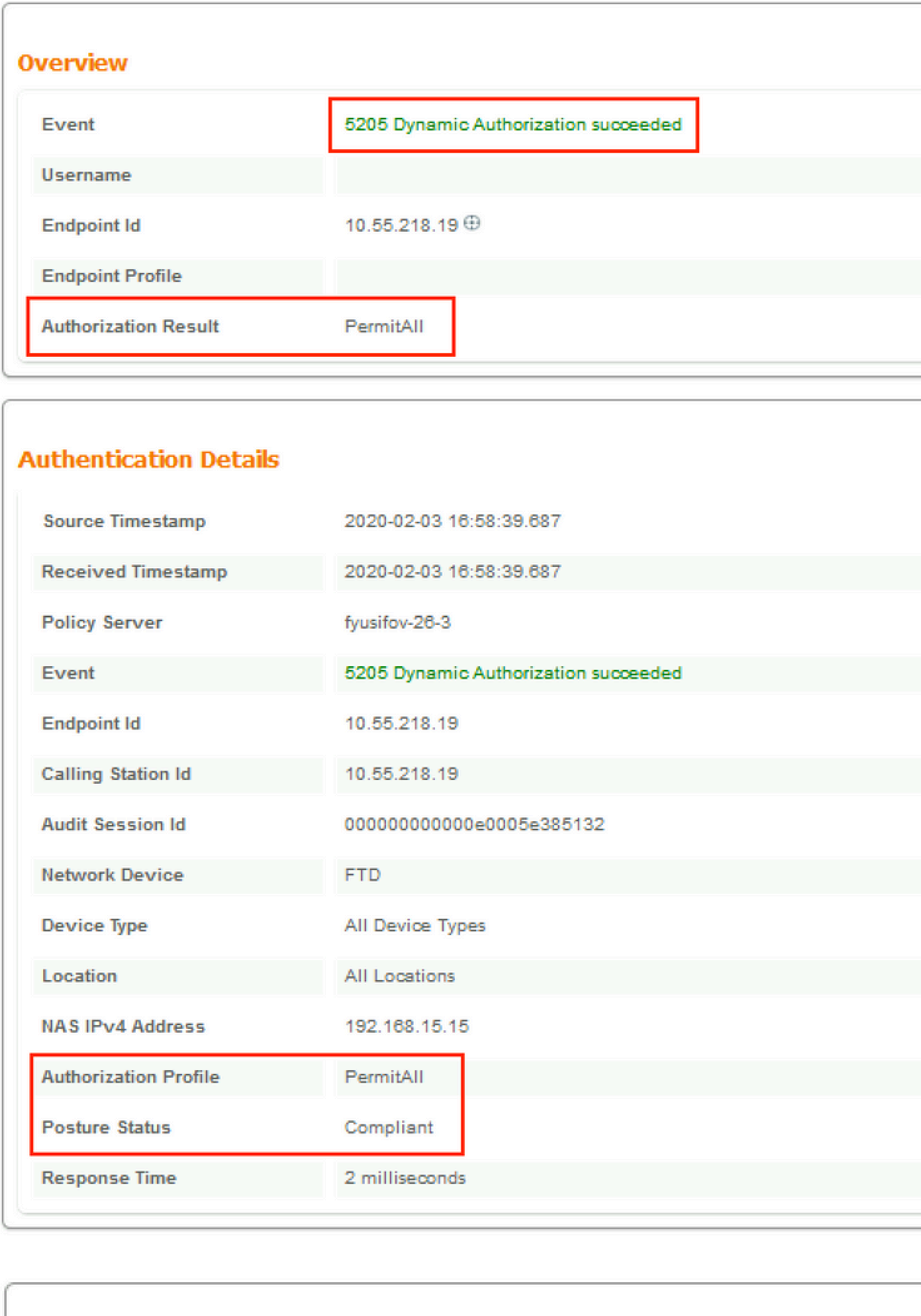
Policy	Name	Enforcement Type	Status	Passed Conditions
Default_AntiMalware_Policy_Win	Any_AM_Installation_Win	Mandatory	Passed	am_inst_v4_ANY_vendor

Depois que o relatório é recebido no ISE, o status da postura é atualizado. Neste exemplo, o status da postura está em conformidade e a Submissão de CoA é acionada com um novo 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

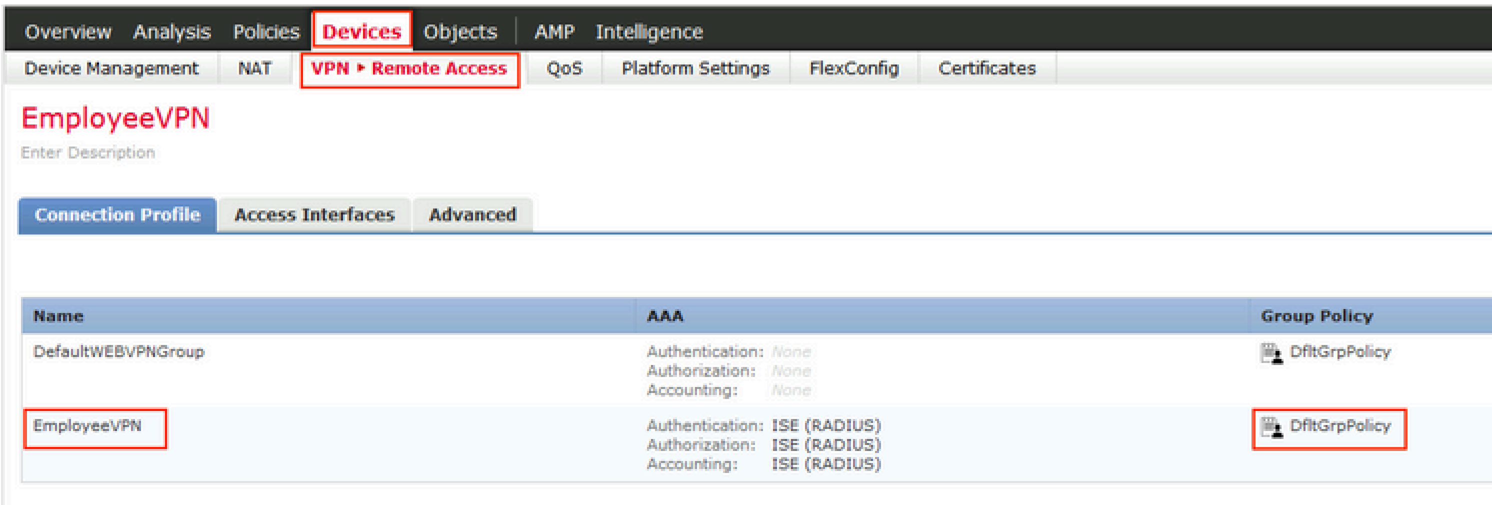
Authentication Details

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

- Túnel dividido

Um dos problemas comuns, quando há um túnel de divisão, é configurado. Neste exemplo, a Política de grupo padrão é usada, o que faz o encapsulamento de todo o tráfego. Caso apenas o tráfego específico seja encapsulado, os testes do AnyConnect (enroll.cisco.com e host de descoberta) devem passar pelo túnel, além do tráfego para o ISE e outros recursos internos.

Para verificar a política de túnel no FMC, primeiro, verifique qual Política de Grupo é usada para a conexão VPN. Navegue até **Devices > VPN Remote Access**.

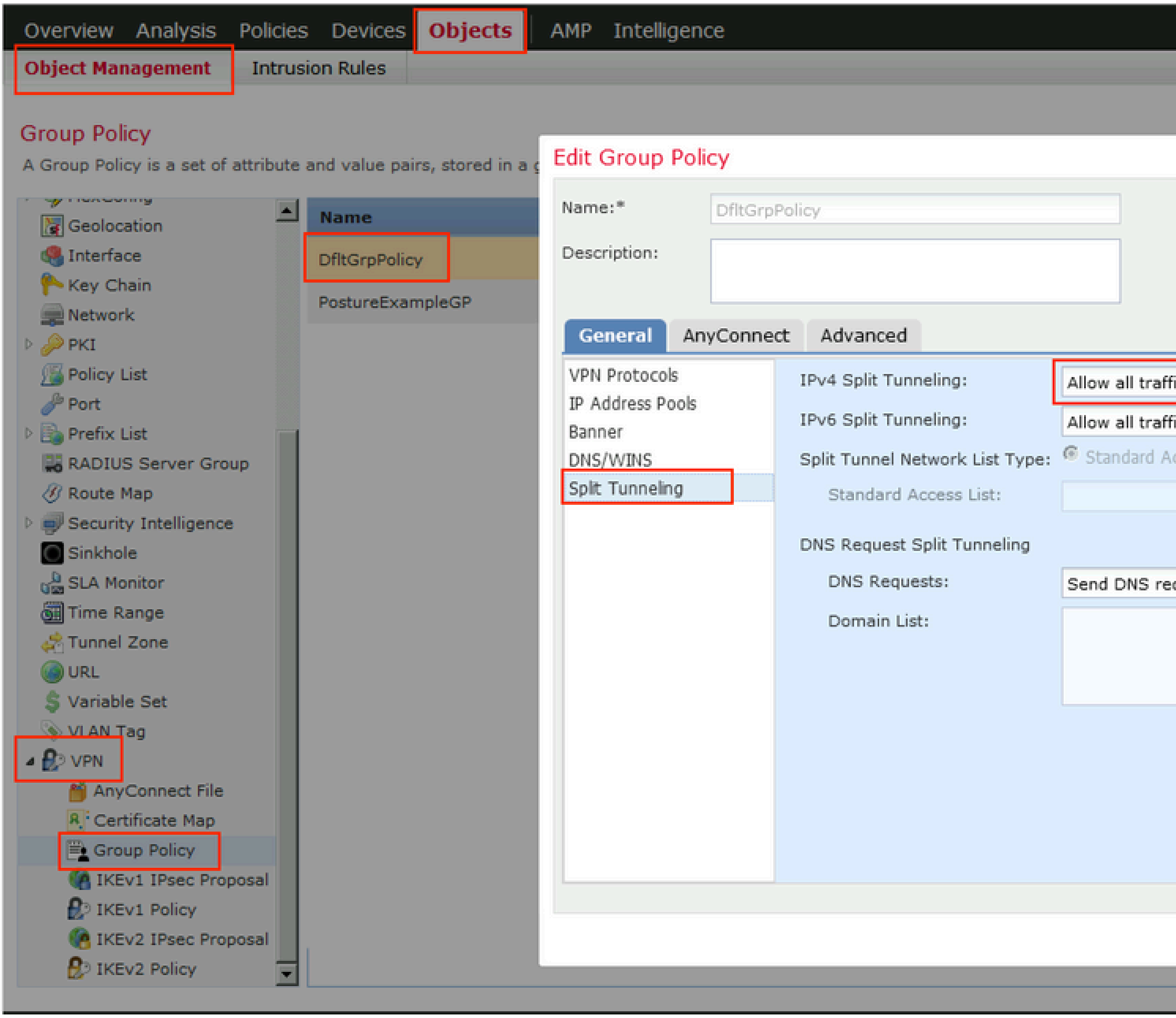


EmployeeVPN

Enter Description

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

Em seguida, navegue para **Objects** > **Object Management** > **VPN** > **Group Policy** e clique em **Group Policy** configurado para VPN.



Name:* DfltGrpPolicy

Description:

IPv4 Split Tunneling: Allow all traffi

IPv6 Split Tunneling: Allow all traffi

Split Tunnel Network List Type: ○ Standard Ac

Standard Access List:

DNS Request Split Tunneling

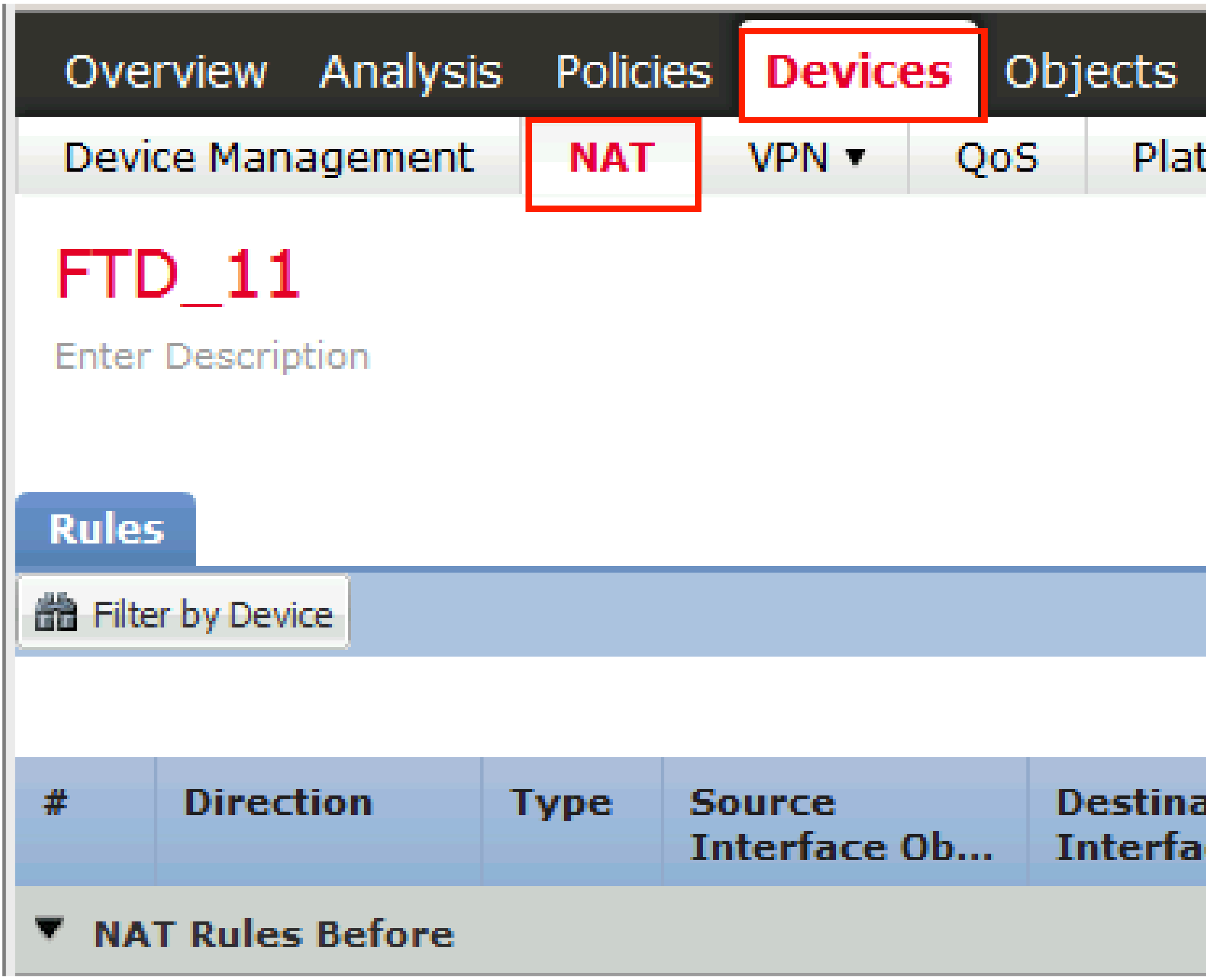
DNS Requests: Send DNS rec

Domain List:

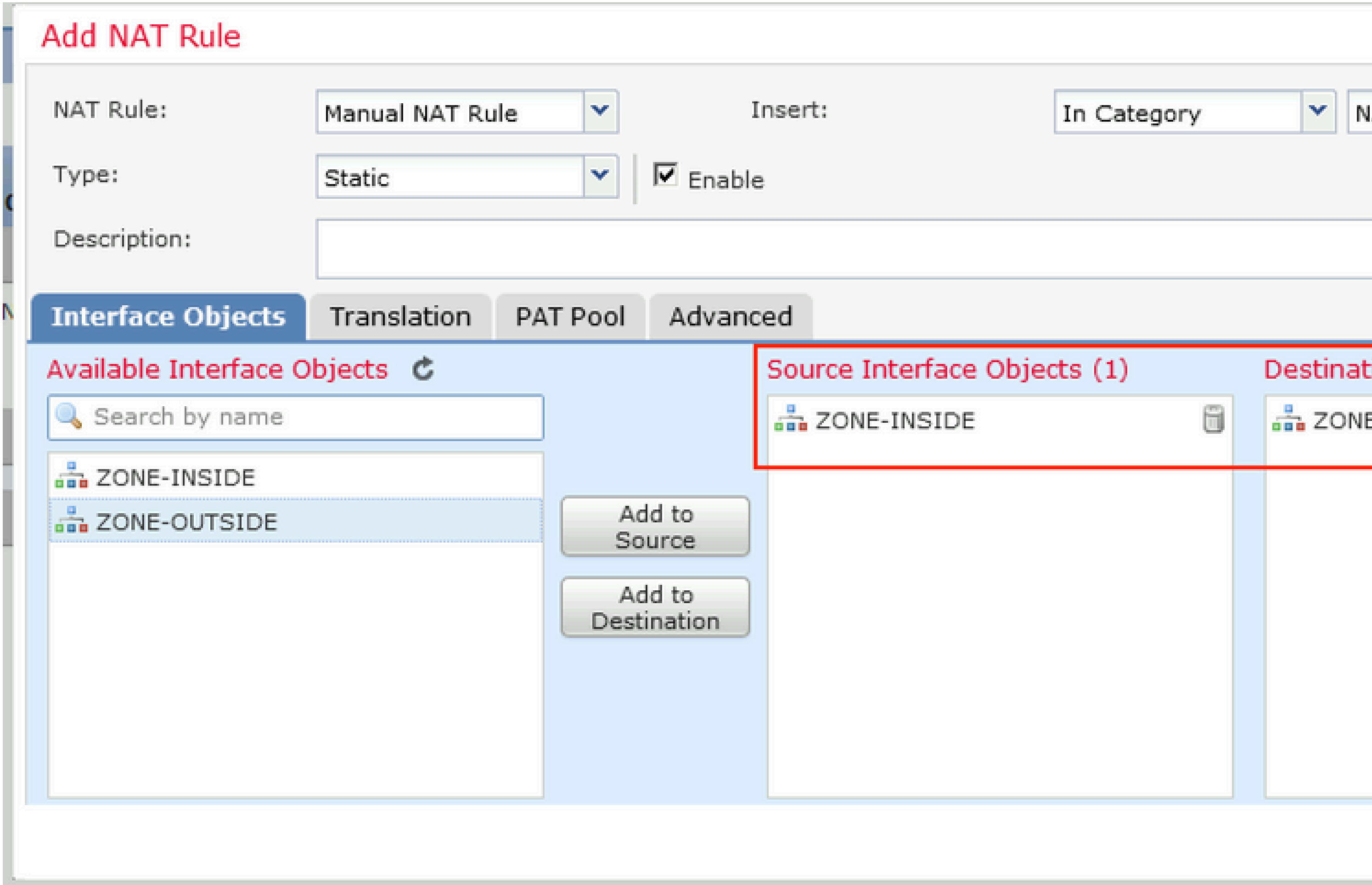
- NAT de identidade

Outro problema comum, quando o tráfego de retorno dos usuários da VPN é convertido com o uso de entrada de NAT incorreta. Para corrigir esse problema, o NAT de identidade deve ser criado em uma ordem apropriada.

Primeiro, verifique as regras de NAT para este dispositivo. Navegue até **Devices > NAT** e clique em **Add Rule** para criar uma nova regra.



Na janela aberta, na guia **Interface Objects**, selecione **Security Zones**. Neste exemplo, a entrada NAT é criada de **ZONE-INSIDE** para **ZONE-OUTSIDE**.



Add NAT Rule

NAT Rule: Manual NAT Rule

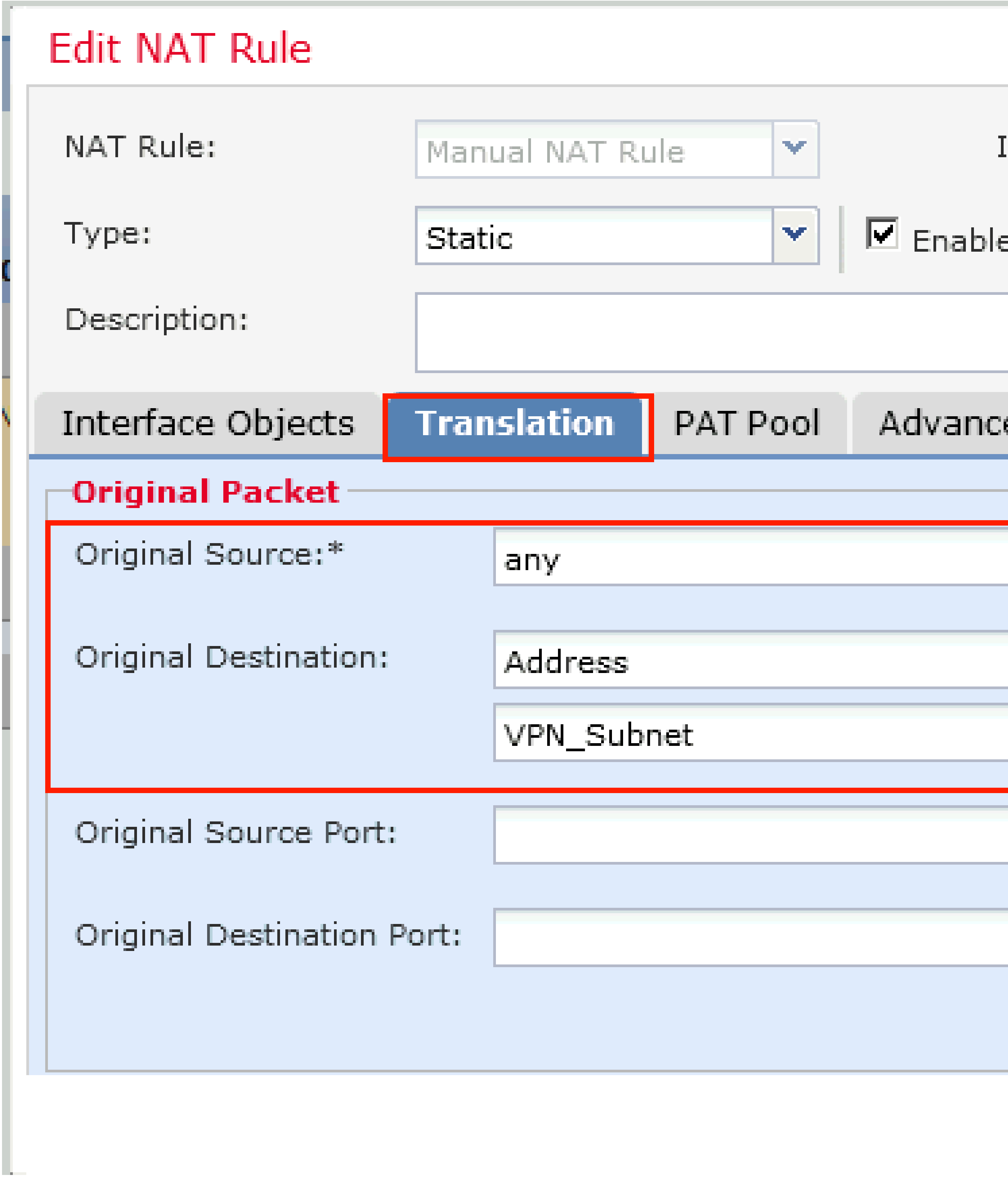
Insert: In Category

Type: Static

☑ Enable

Description:

Na guia **Translation**, selecione os detalhes do pacote original e traduzido. Como é o NAT de identidade, a origem e o destino são mantidos inalterados:



Edit NAT Rule

NAT Rule: Manual NAT Rule

Type: Static ☑ Enable

Description:

Original Packet

Original Source:* any

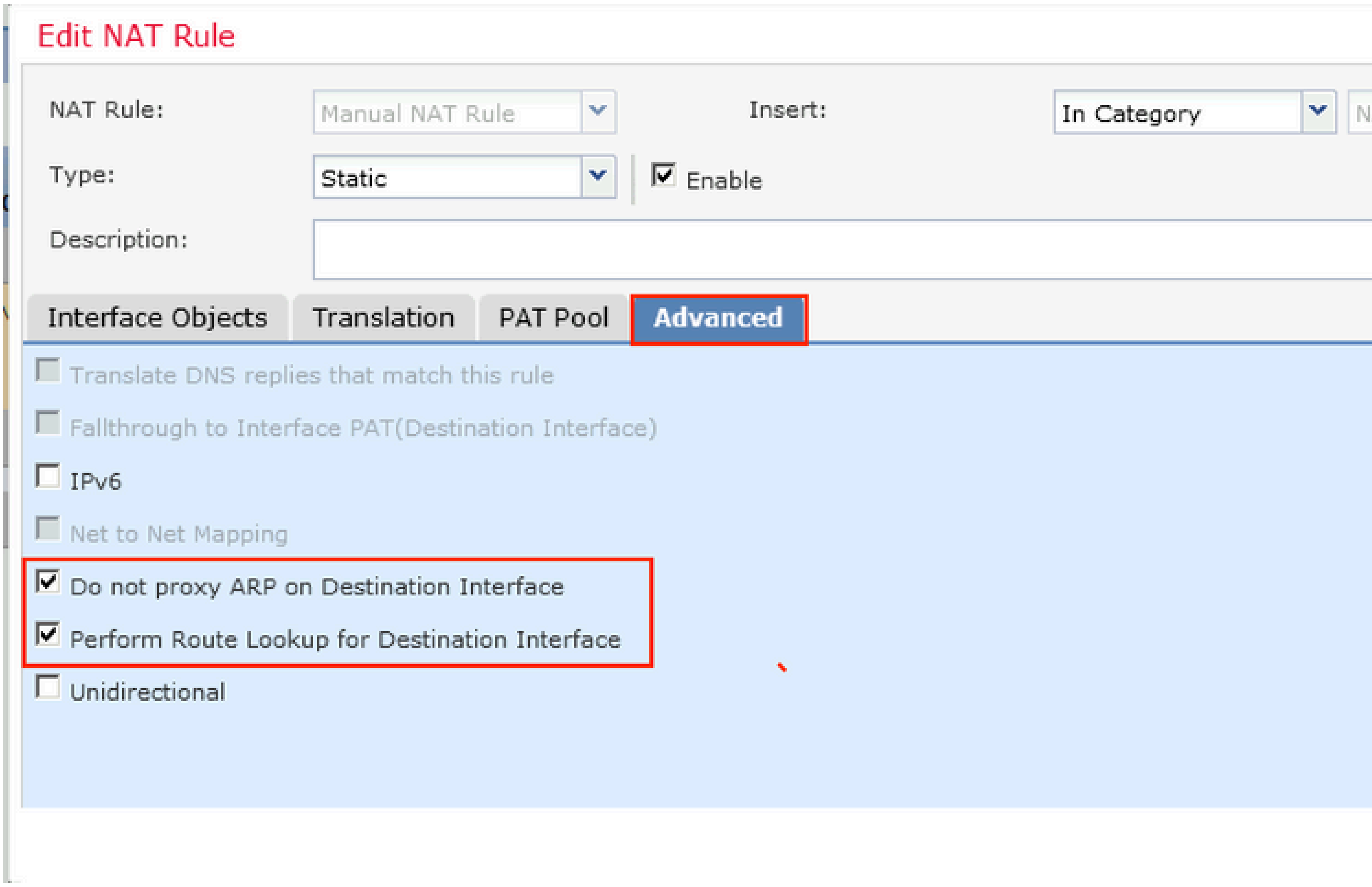
Original Destination: Address

VPN_Subnet

Original Source Port:

Original Destination Port:

Na guia **Advanced**, marque as caixas de seleção como mostrado nesta imagem:



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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.