ISE-houding configureren via AnyConnect Remote Access VPN op FTD

Inhoud

Inleiding

Dit document beschrijft hoe u Firepower Threat Defence (FTD) versie 6.4.0 moet configureren om VPN-gebruikers aan te stellen tegen Identity Services Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- AnyConnect externe toegang tot VPN
- Configuratie van VPN voor externe toegang op de FTD
- Identity Services Engine en postuur

Gebruikte componenten

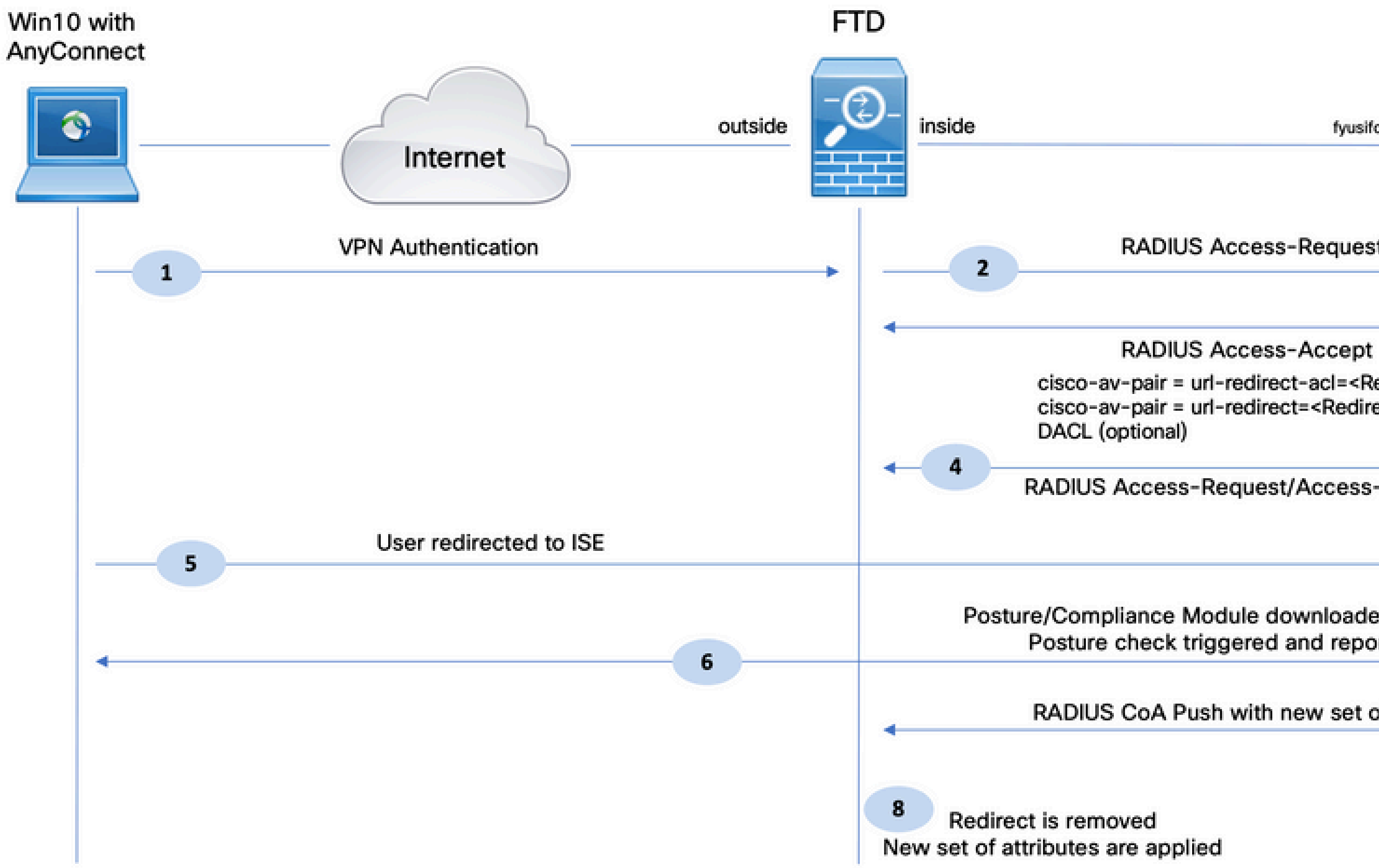
De informatie in dit document is gebaseerd op de volgende softwareversies:

- Software voor Cisco Firepower Threat Defence (FTD), versie 6.4.0
- Software voor Cisco Firepower Management Console (FMC), versie 6.5.0
- Microsoft Windows 10 met Cisco AnyConnect Secure Mobility-client versie 4.7
- Cisco Identity Services Engine (ISE) versie 2.6 met Patch 3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram en verkeersstroom


Win10 with AnyConnect
Internet
FTD
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-
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. De externe gebruiker gebruikt Cisco AnyConnect voor VPN-toegang tot de FTD.

2. De FTD stuurt een RADIUS-toegangsverzoek voor die gebruiker naar de ISE.

3. Dat verzoek raakt het beleid genaamd **FTD-VPN-Posture-Unknown** op de ISE. De ISE stuurt een RADIUS-toegangsgoedkeuring met drie kenmerken:

- **Cisco-av-paar = url-redirect-acl=fyusifovredirect** - Dit is de naam van de toegangscontrolelijst (ACL) die lokaal op de FTD is gedefinieerd, die beslist welk verkeer wordt omgeleid.
- **Cisco-av-pair = url-redirect=**[https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp]() - Dit is de URL waarnaar de externe gebruiker wordt doorgestuurd.
- **DACL = PERMIT_ALL_IPV4_TRAFFIC** - downloadbare ACL Dit kenmerk is optioneel. In dit scenario is al het verkeer toegestaan in DACL)

4. Als DACL wordt verzonden, wordt RADIUS-toegangsverzoek/toegangsgoedkeuring uitgewisseld om de inhoud van DACL te downloaden

5. Wanneer het verkeer van de VPN-gebruiker overeenkomt met de lokaal gedefinieerde ACL, wordt het omgeleid naar ISE-clientprovisioningportal. ISE-bepalingen AnyConnect-postermodule en nalevingsmodule.

6. Nadat de agent op de clientmachine is geïnstalleerd, zoekt hij automatisch naar ISE met sondes. Wanneer ISE met succes is gedetecteerd, worden de houdingsvereisten gecontroleerd op het eindpunt. In dit voorbeeld controleert de agent op geïnstalleerde anti-malware software. Vervolgens stuurt het een postuur verslag naar de ISE.

7. Wanneer ISE het postuur rapport van de agent ontvangt, verandert ISE Positie Status voor deze sessie en activeert RADIUS CoA type Push met nieuwe eigenschappen. Ditmaal is de status van de houding bekend en wordt er een andere regel geraakt.

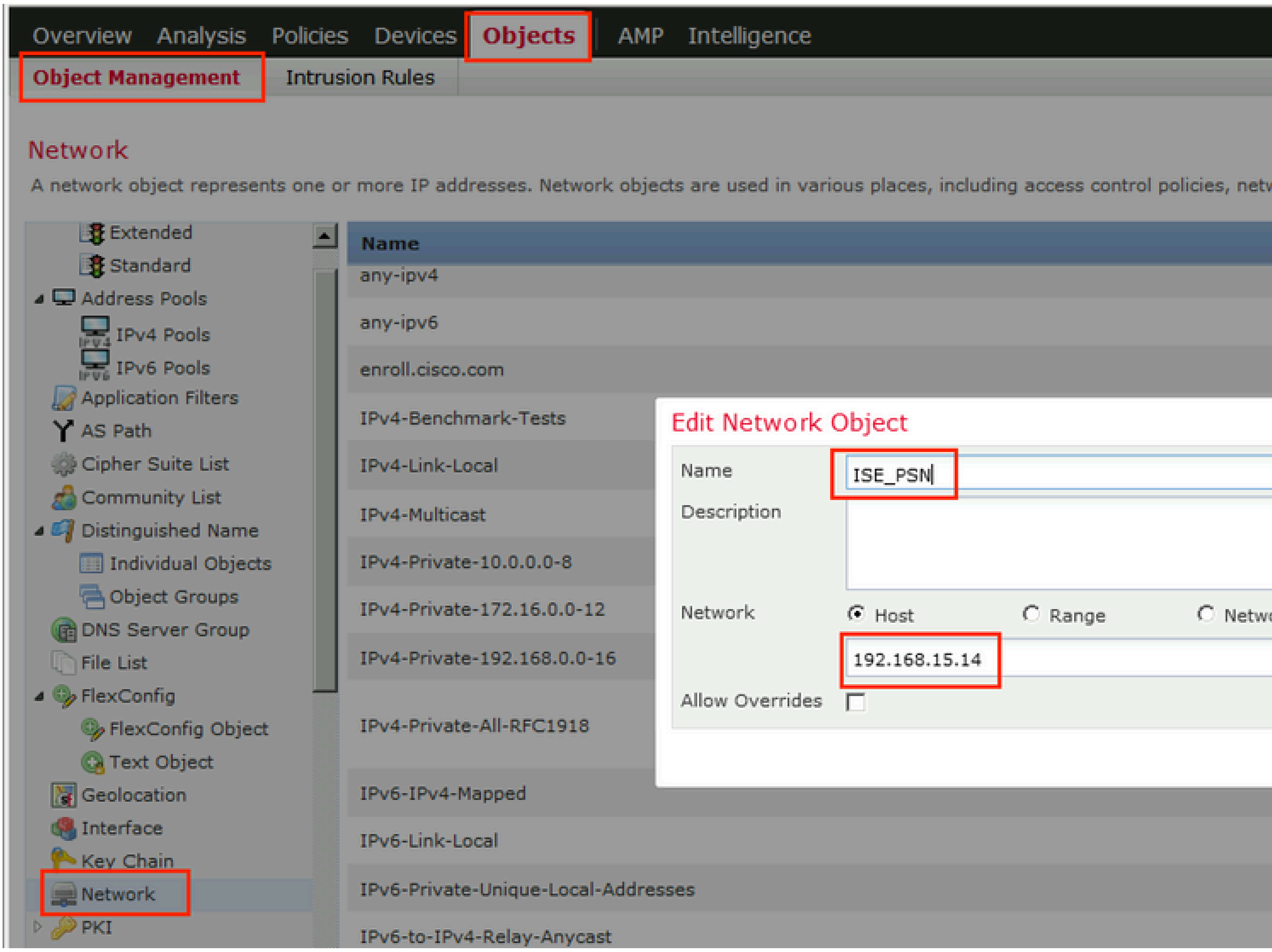
- Als de gebruiker volgzaam is, dan wordt een DACL naam die volledige toegang toelaat verzonden.
- Als de gebruiker niet-compatibel is, wordt een DACL-naam die beperkte toegang toestaat verzonden.

8. Het FTD verwijdert de omleiding. FTD stuurt een toegangsaanvraag om DACL van de ISE te downloaden. De specifieke DACL is gekoppeld aan de VPN-sessie.

Configuraties

FTD/FMC

Stap 1. Maak een netwerkobjectgroep voor ISE- en herstelservers (indien aanwezig). Ga naar **Objecten > Objectbeheer > Netwerk**.



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:

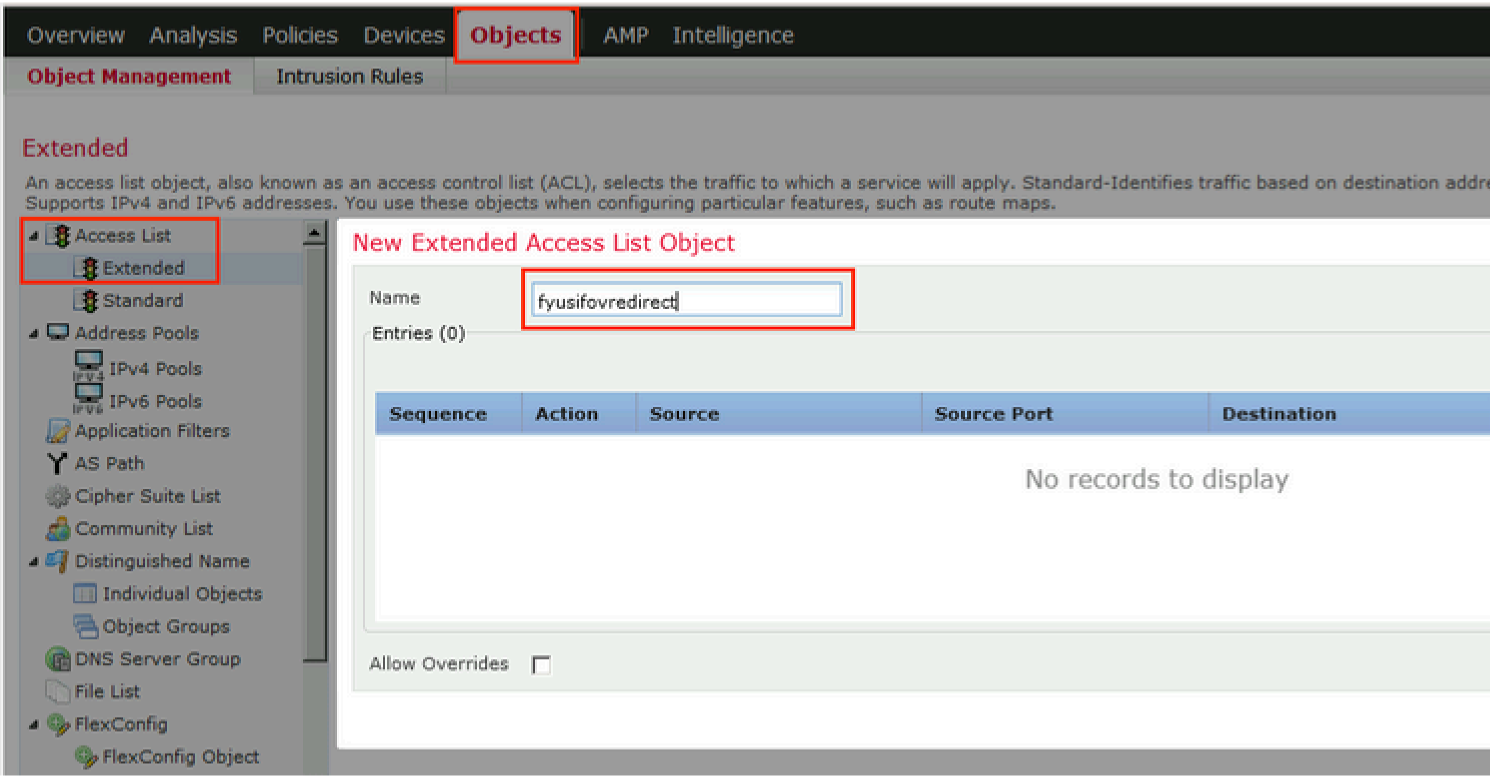
Network: ● Host ○ Range ○ Netw

192.168.15.14

Allow Overrides □

Stap 2. Omleiden ACL maken Navigeer naar **Objecten > Objectbeheer > Toegangslijst > Uitgebreid**.

Klik op **Uitgebreide toegangslijst toevoegen** en geef de naam op van ACL-omleiding. Deze naam moet dezelfde zijn als in het resultaat van de ISE-autorisatie.



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

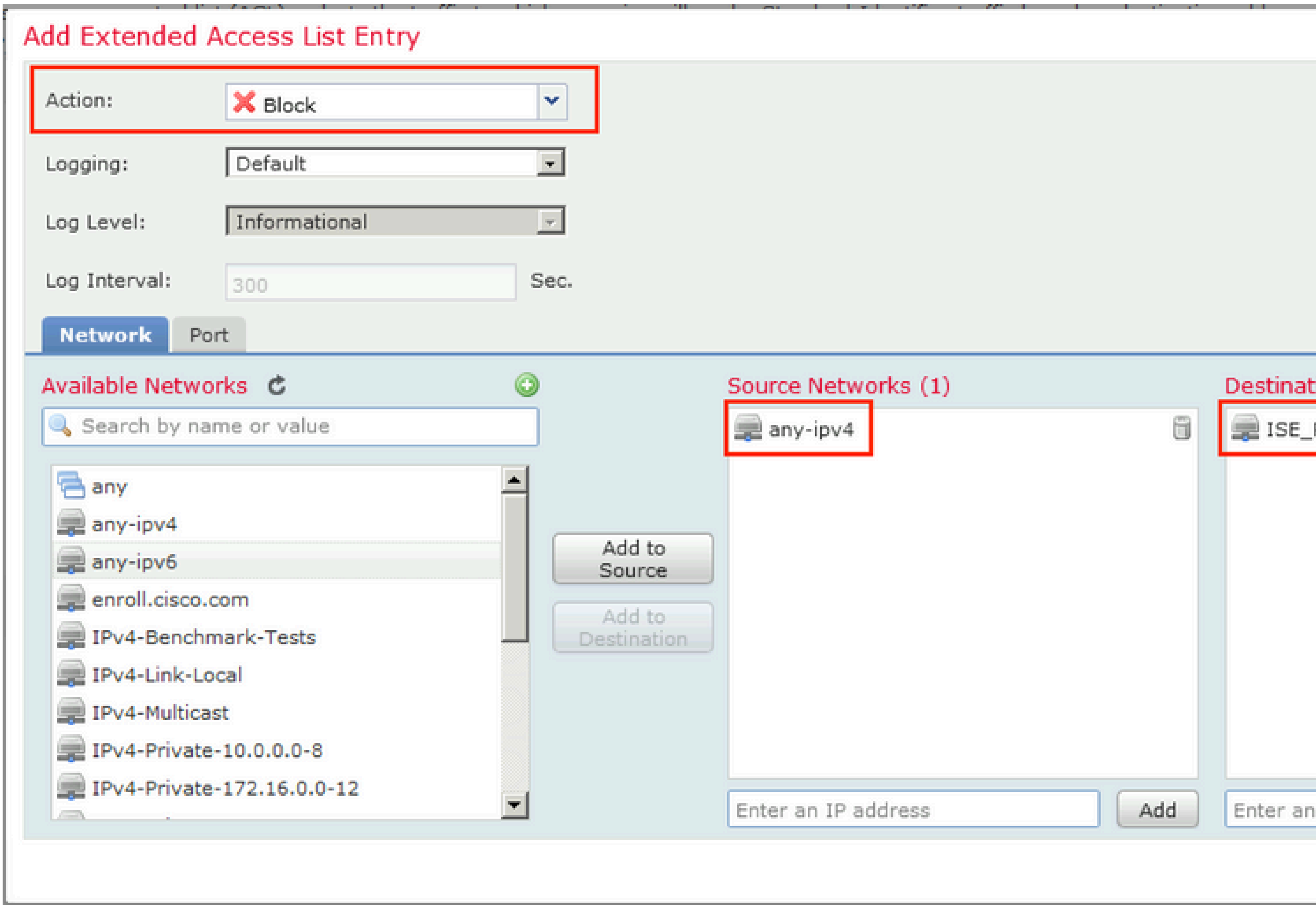
Entries (0)

Sequence	Action	Source	Source Port	Destination

No records to display

Allow Overrides □

Stap 3. Vermeldingen in ACL-omleiding toevoegen. Klik op de knop **Toevoegen**. Blokkeer verkeer naar DNS, ISE en de herstelservers om deze uit te sluiten van omleiding. Laat de rest van het verkeer toe, dit activeert omleiding (ACL-vermeldingen kunnen specifieker zijn indien nodig).



Add Extended Access List Entry

Action: Block

Logging: Default

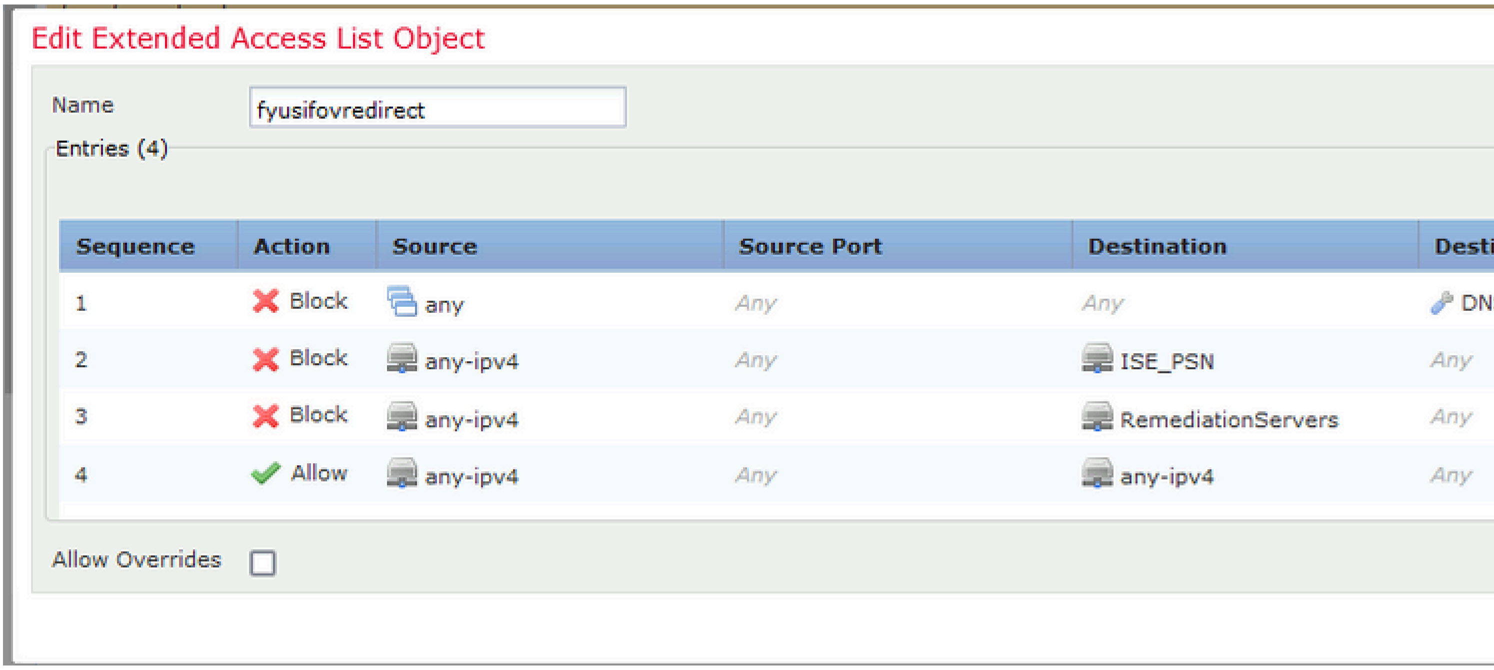
Log Level: Informational

Log Interval: 300 Sec.

Source Networks (1)

any-ipv4

ISE_



Edit Extended Access List Object

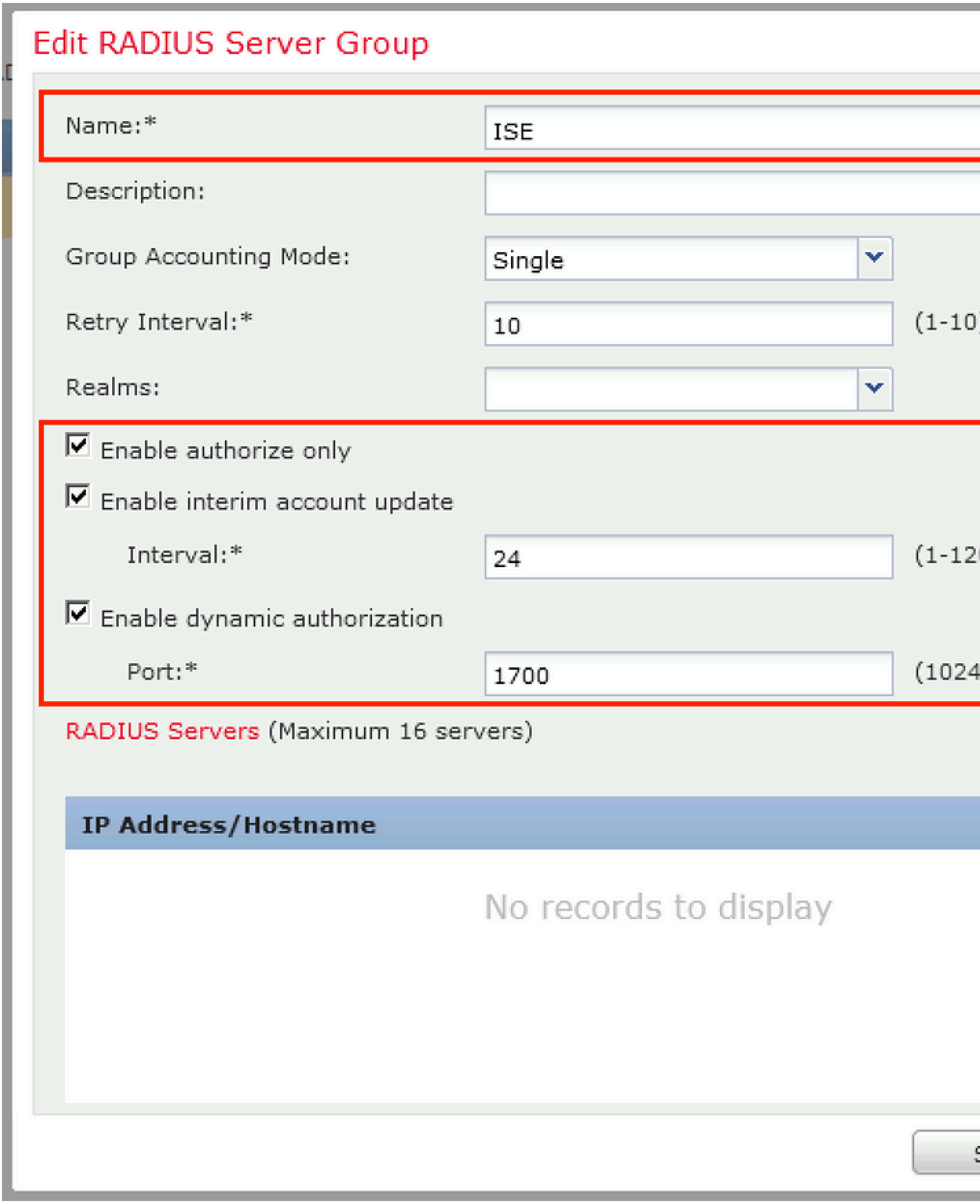
Name: fyusifovredirect

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 □

Stap 4. Voeg ISE-PSN-knooppunt/knooppunten toe. Ga naar **Objecten** > **Objectbeheer** > **RADIUS-servergroep**. Klik op **RADIUS-servergroep toevoegen**, geef de naam op, schakel alle selectievakjes in en klik op het pictogram **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

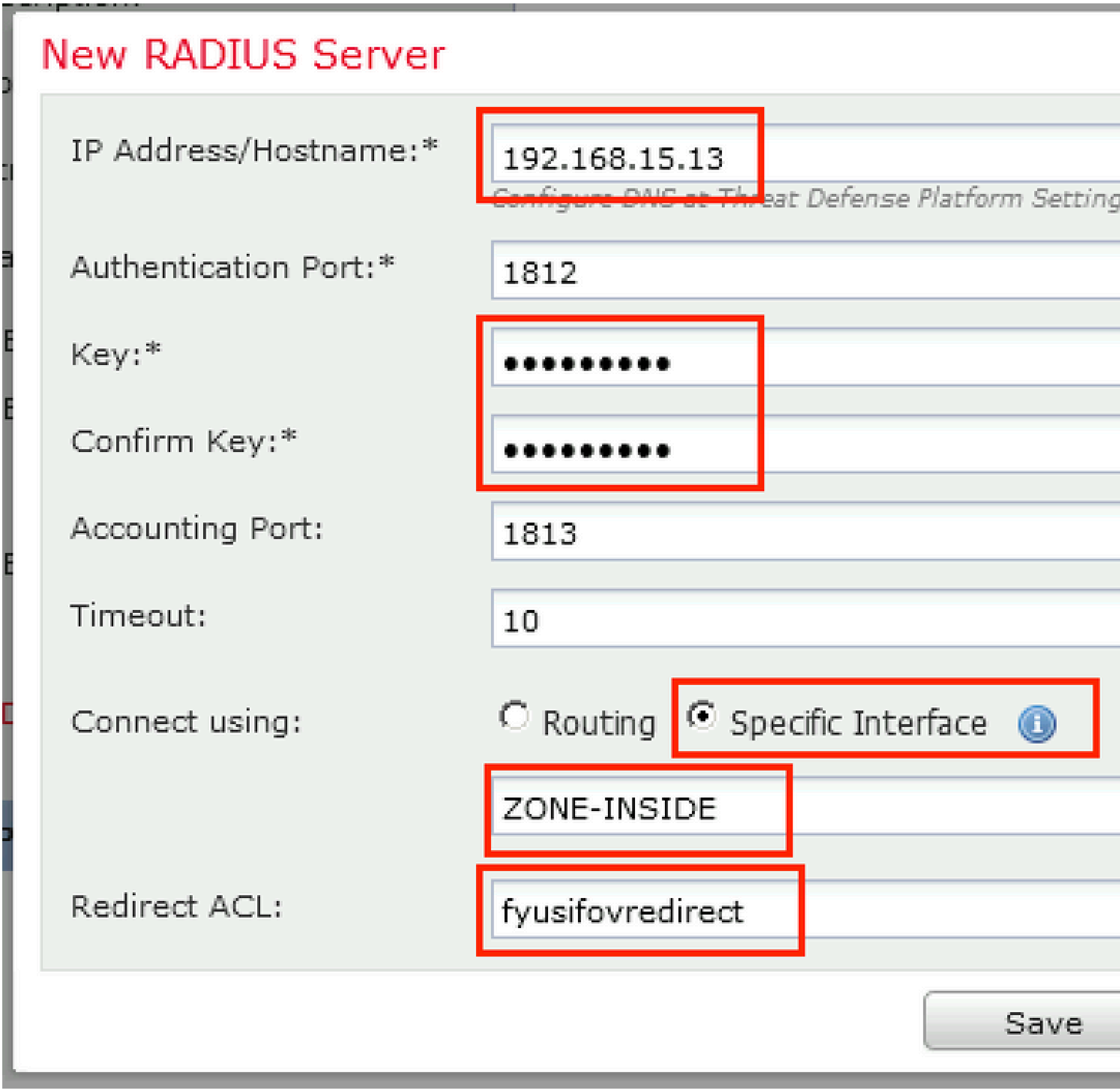
☑ Enable dynamic authorization

Port:* 1700 (1024

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

Stap 5. Typ in het geopende venster ISE-PSN IP-adres, RADIUS-sleutel, selecteer **Specifieke interface** en selecteer de interface waaruit ISE bereikbaar is (deze interface wordt gebruikt als bron van RADIUS-verkeer) en selecteer vervolgens **ACL-omleiding** die eerder is geconfigureerd.



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

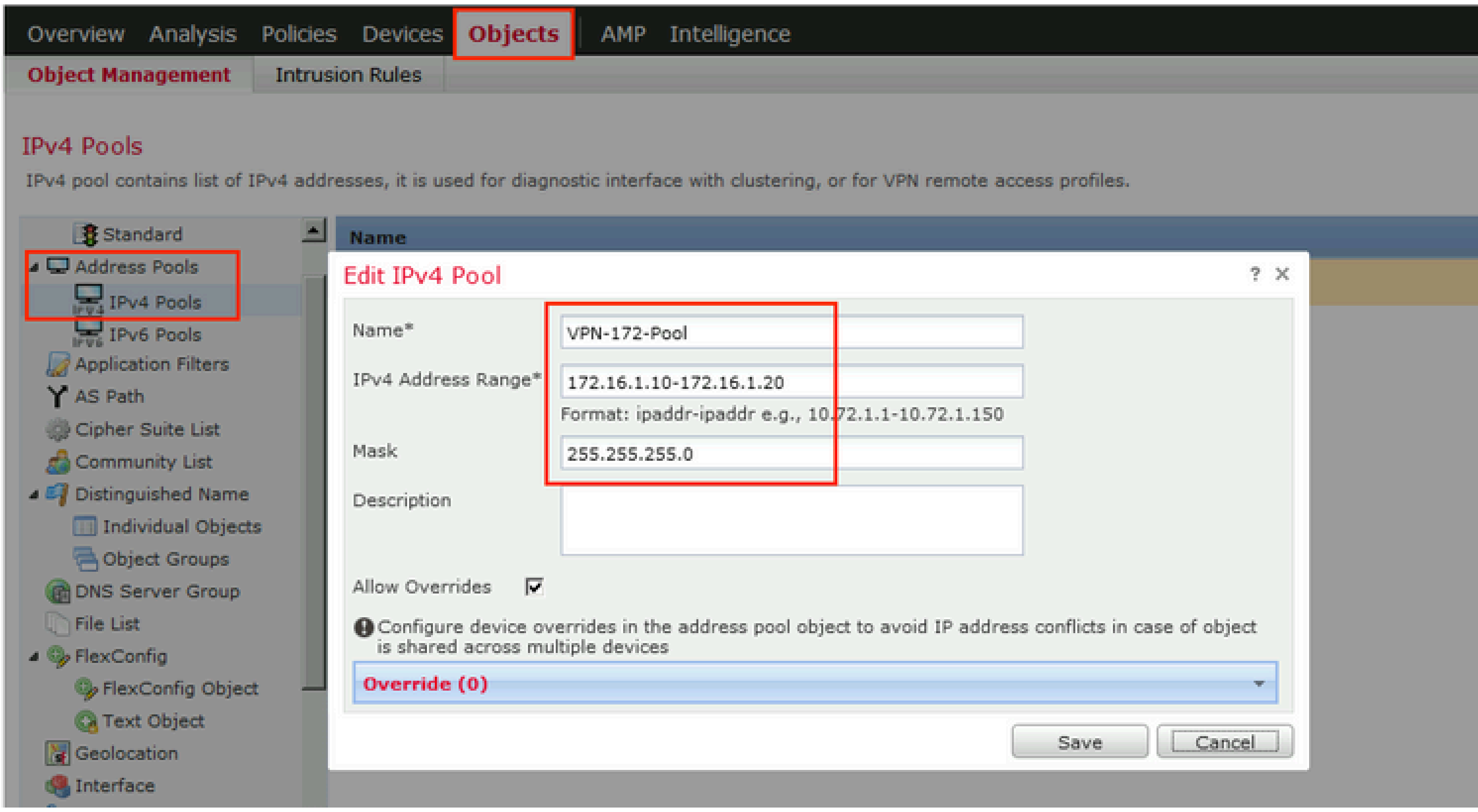
Timeout: 10

Connect using: ○ Routing ● Specific Interface

ZONE-INSIDE

Redirect ACL: fyusifovredirect

Stap 6. Adresgroep maken voor VPN-gebruikers. Ga naar **Objecten** > **Objectbeheer** > **Adrespools** > **IPv4-pools**. Klik op **IPv4-pools toevoegen** en vul de gegevens in.



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

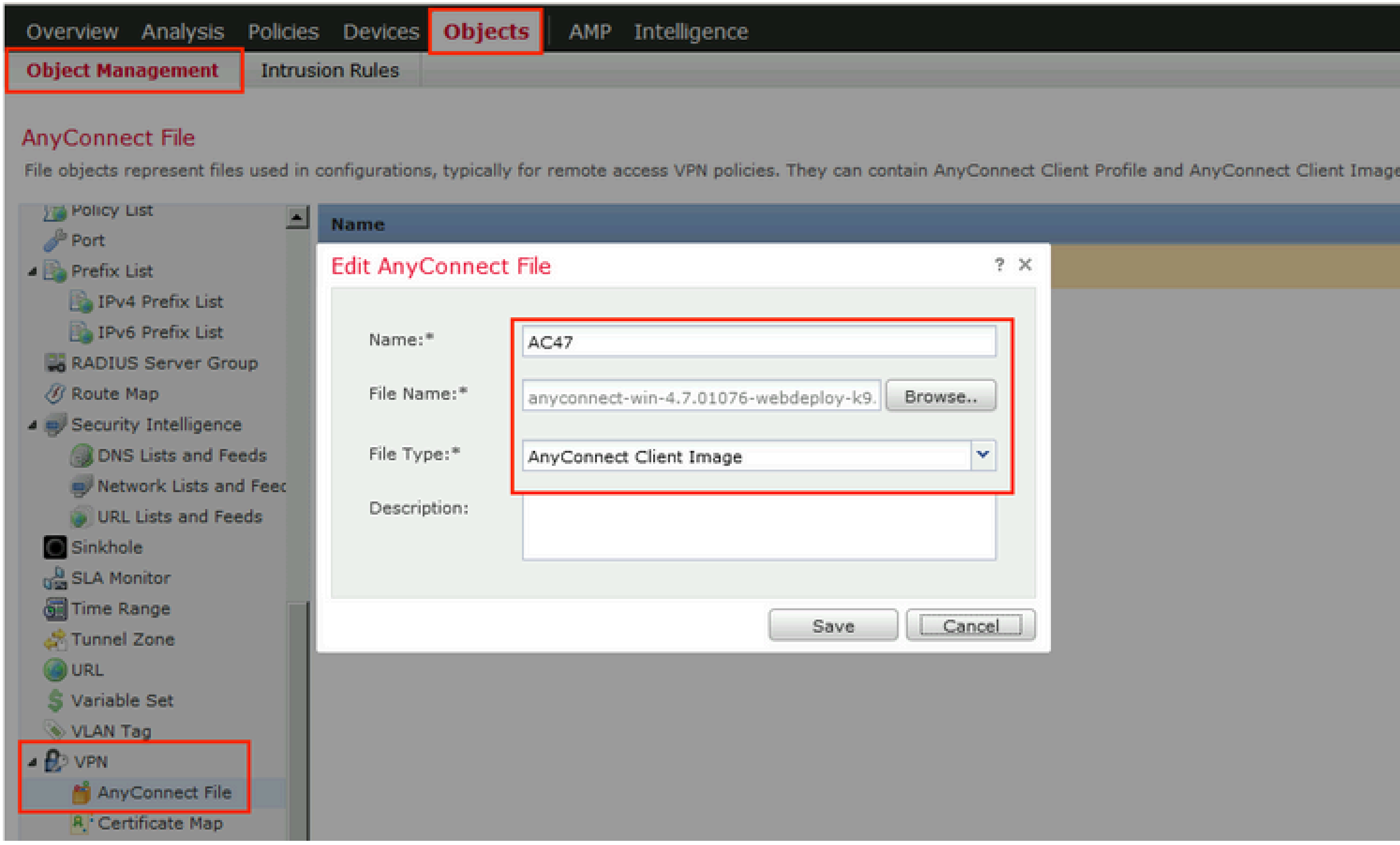
Description

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)

Stap 7. Maak een AnyConnect-pakket. Navigeer naar **Objecten** > **Objectbeheer** > **VPN** > **AnyConnect File**. Klik op **Add AnyConnect File**, geef de pakketnaam op, download het pakket van Cisco Software Download en selecteer **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

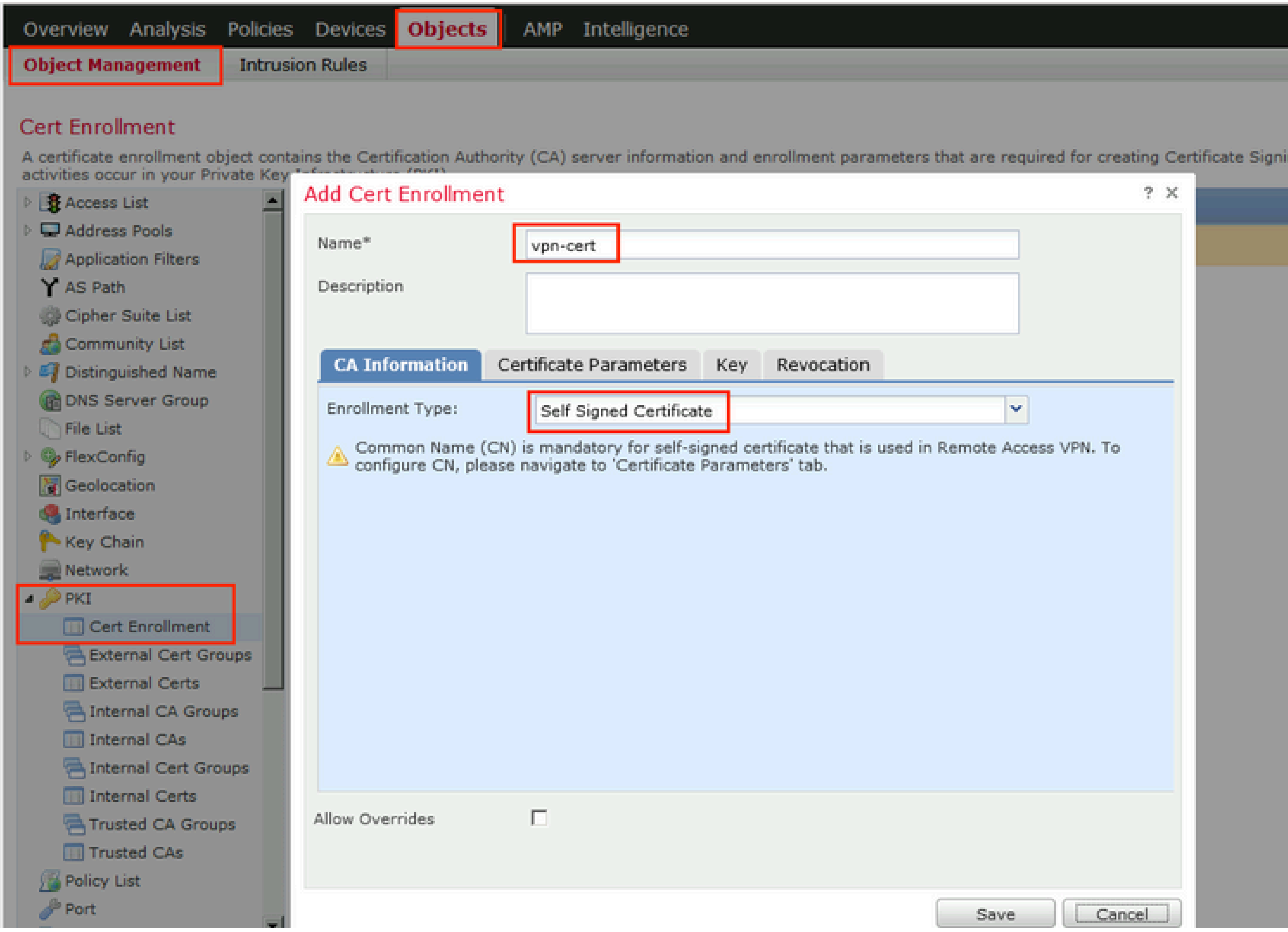
Name:* AC47

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

File Type:* AnyConnect Client Image

Description:

Stap 8. Navigeer naar **certificaatobjecten > Objectbeheer > PKI > Cert-inschrijving**. Klik op **Add Cert Inschrijving**, geef naam op en kies **Self Signed Certificate** in Inschrijftype. Klik op het tabblad Certificaatparameters en geef de GN op.



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

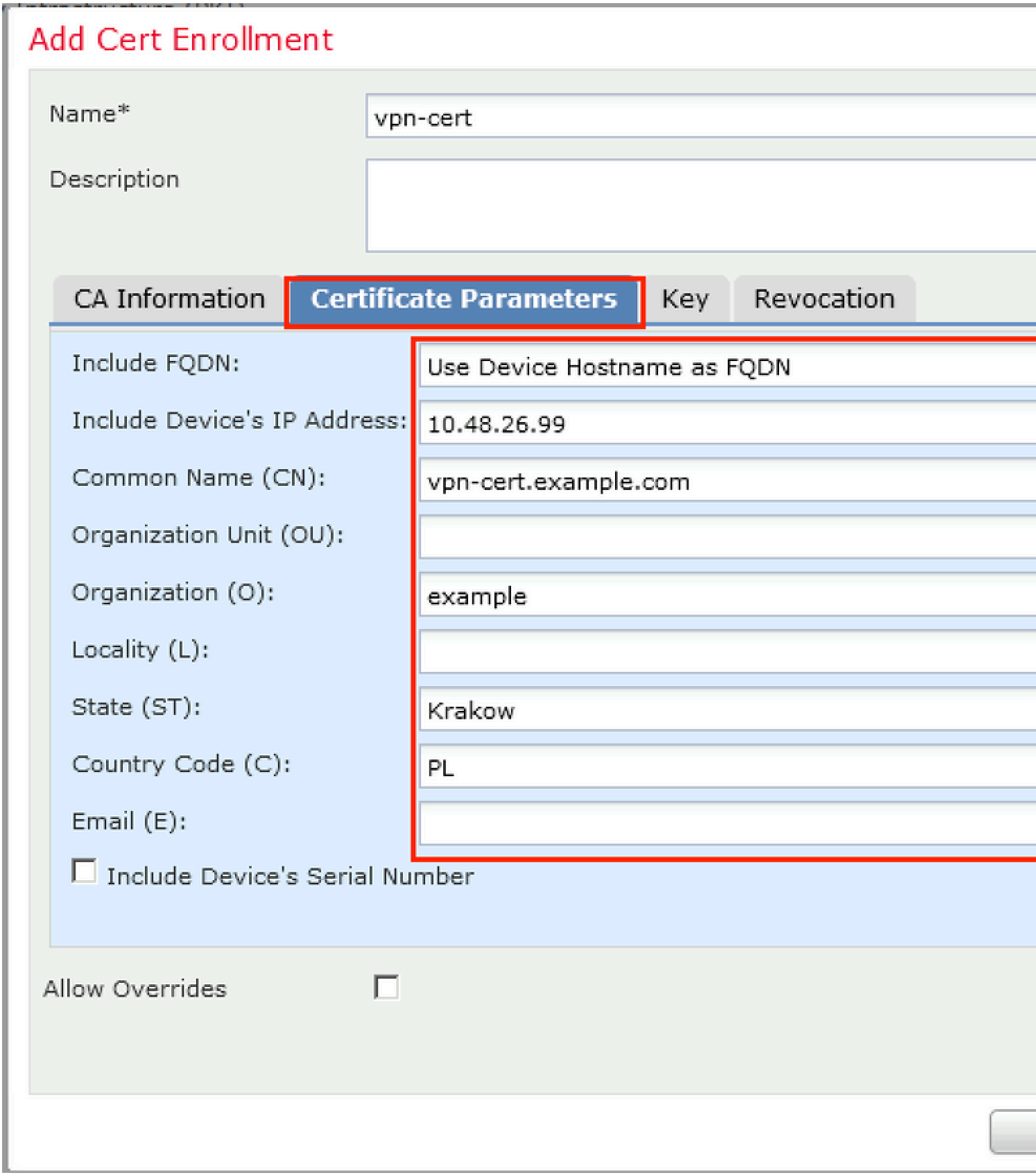
Name* vpn-cert

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

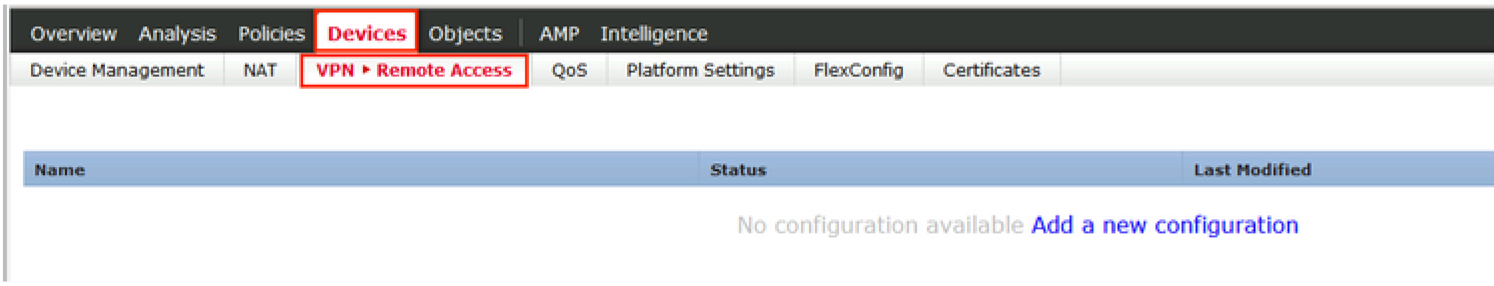
Name*	vpn-cert
Description	

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):	

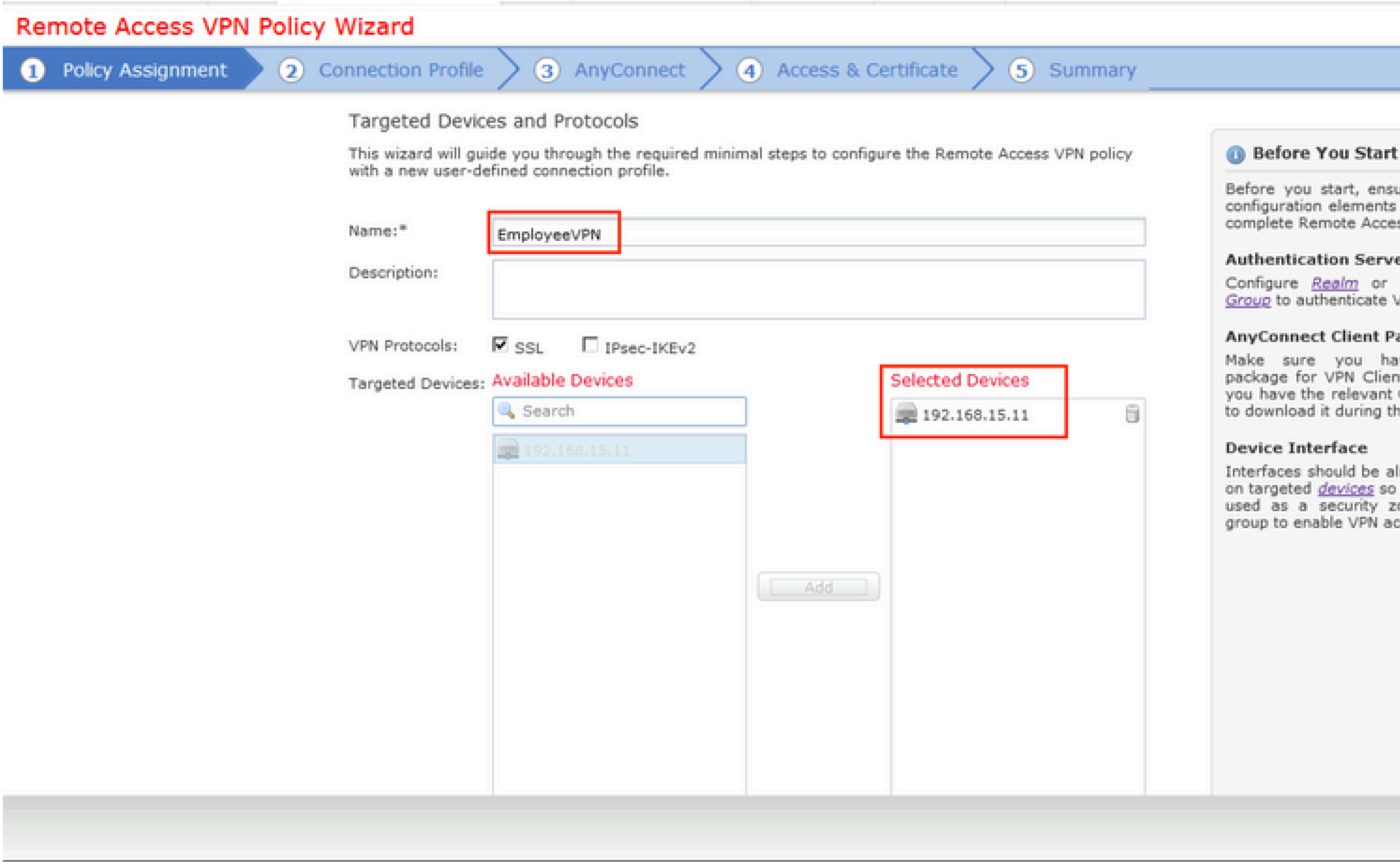
□ Include Device's Serial Number

Allow Overrides □

Stap 9. Start de wizard Externe toegang tot VPN. Navigeer naar **Apparaten** > **VPN** > **Externe toegang** en klik op **Toevoegen**.



Stap 10. Vermeld de naam, controleer SSL als VPN Protocol, kies FTD die als VPN concentrator wordt gebruikt en klik op **Volgende**.



Remote Access VPN Policy Wizard

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

Before You Start

Before you start, ensu configuration elements complete Remote Acces

Authentication Serve

Configure Realm or Group to authenticate V

AnyConnect Client Pa

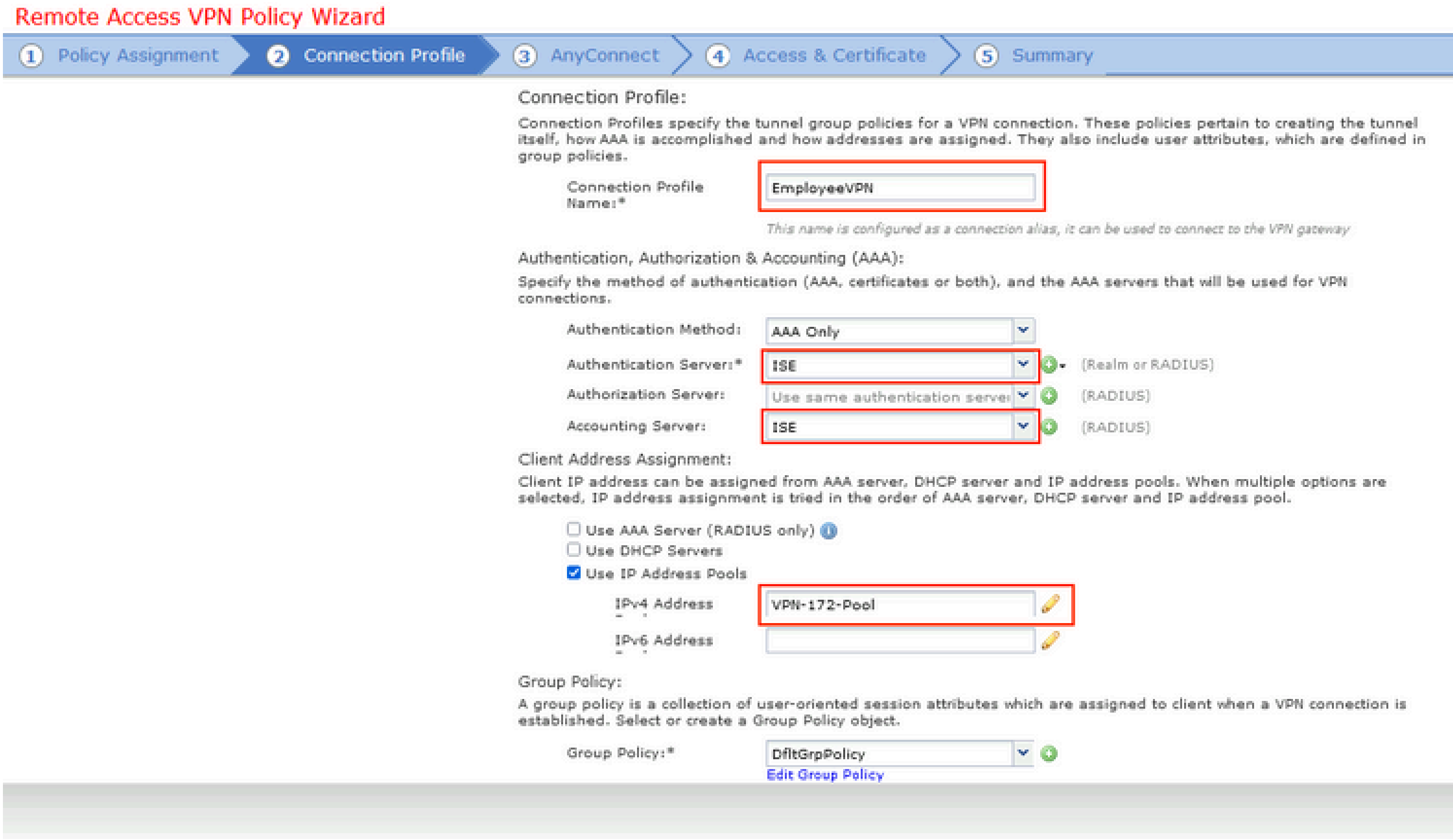
Make sure you ha package for VPN Clien you have the relevant to download it during th

Device Interface

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

Stap 11. Geef **de** naam van het **verbindingsprofiel op**, selecteer **Verificatie-**/boekhoudservers, selecteer de adrespool die eerder is geconfigureerd en klik op **Volgende**.

Opmerking: selecteer de autorisatieserver niet. Het brengt twee toegangsaanvragen voor één gebruiker (eenmaal met het gebruikerswachtwoord en de tweede keer met wachtwoord *cisco*).



Remote Access VPN Policy Wizard

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:

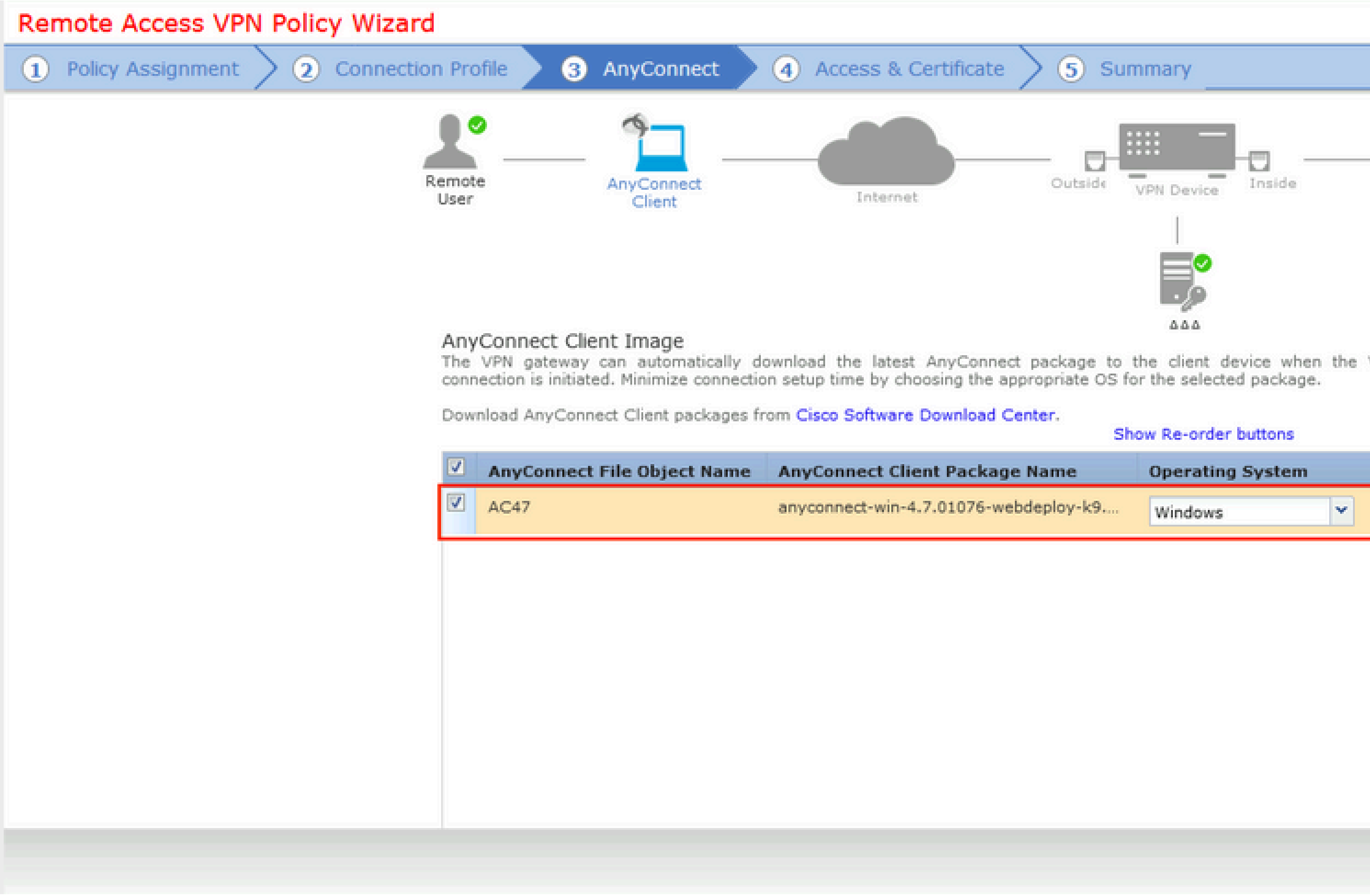
Group Policy:

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

Stap 12. Selecteer AnyConnect-pakket dat eerder is geconfigureerd en klik op **Volgende**.



Remote Access VPN Policy Wizard

AnyConnect Client Image

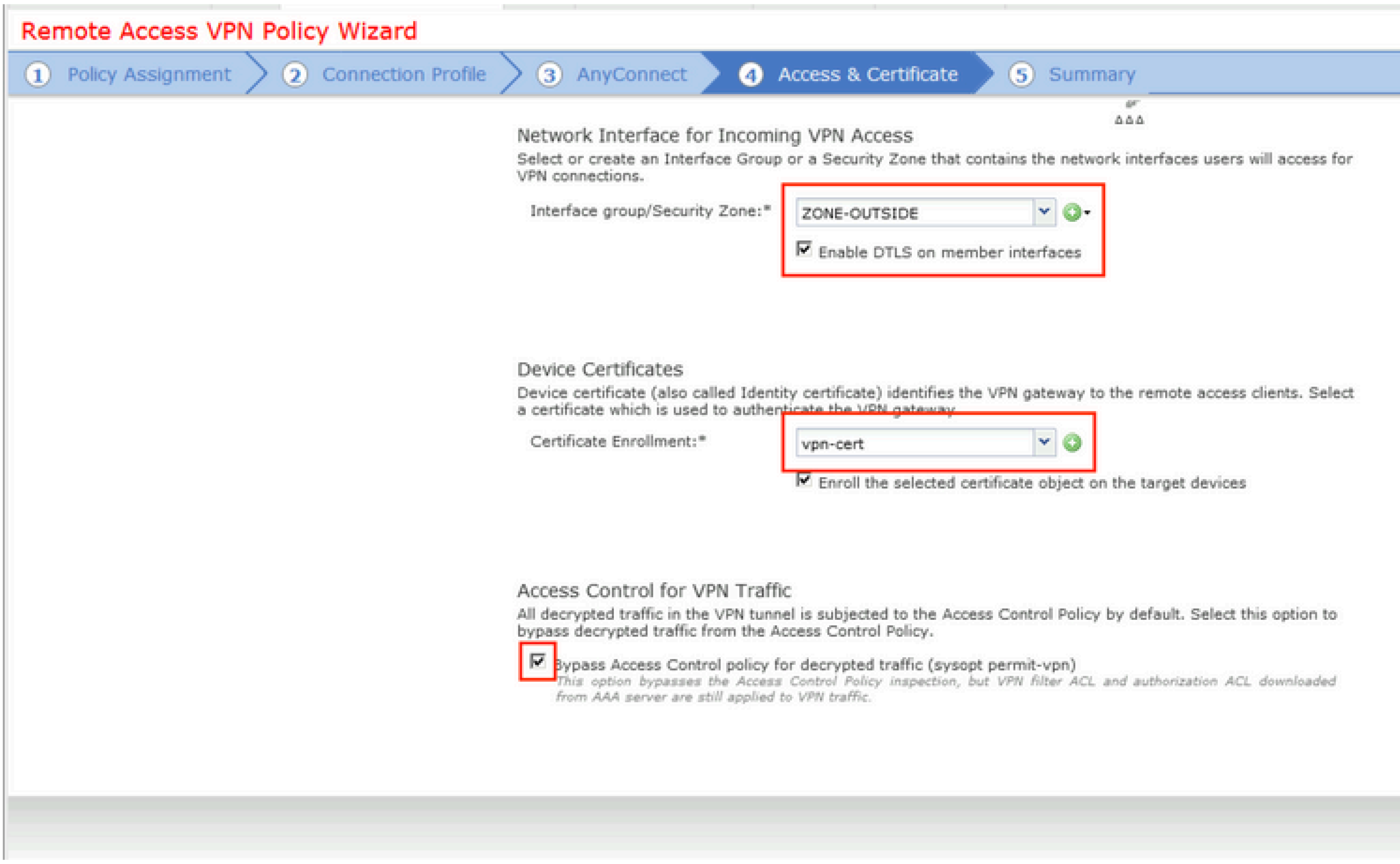
The VPN gateway can automatically download the latest AnyConnect package to the client device when the connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

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

Stap 13. Selecteer de interface waarvan VPN-verkeer wordt verwacht, selecteer **Certificaatinschrijving** die eerder is geconfigureerd en klik op **Volgende**.



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

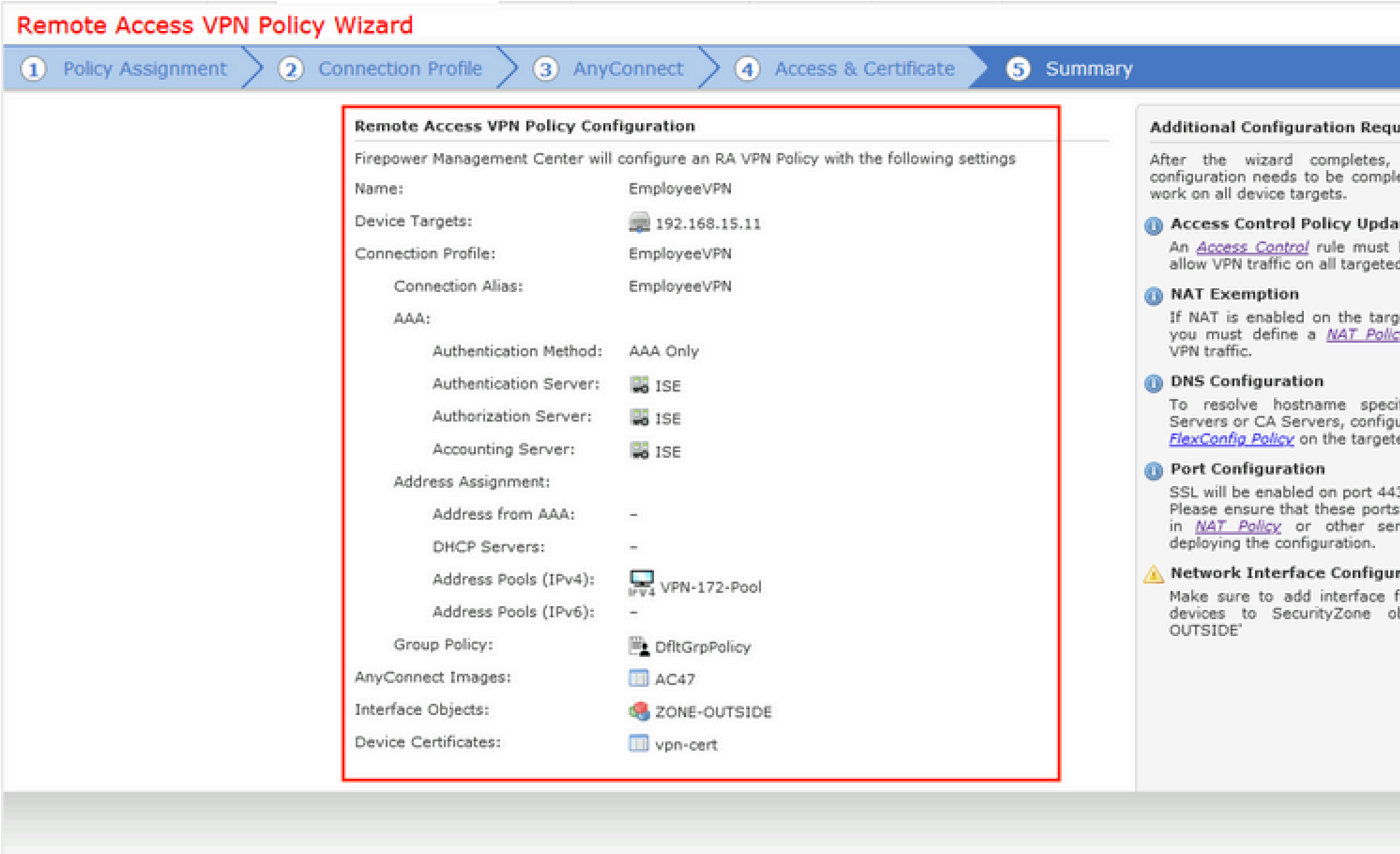
Access Control for VPN Traffic

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.

Stap 14. Controleer de overzichtspagina en klik op **Voltooien**.



Remote Access VPN Policy Wizard

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

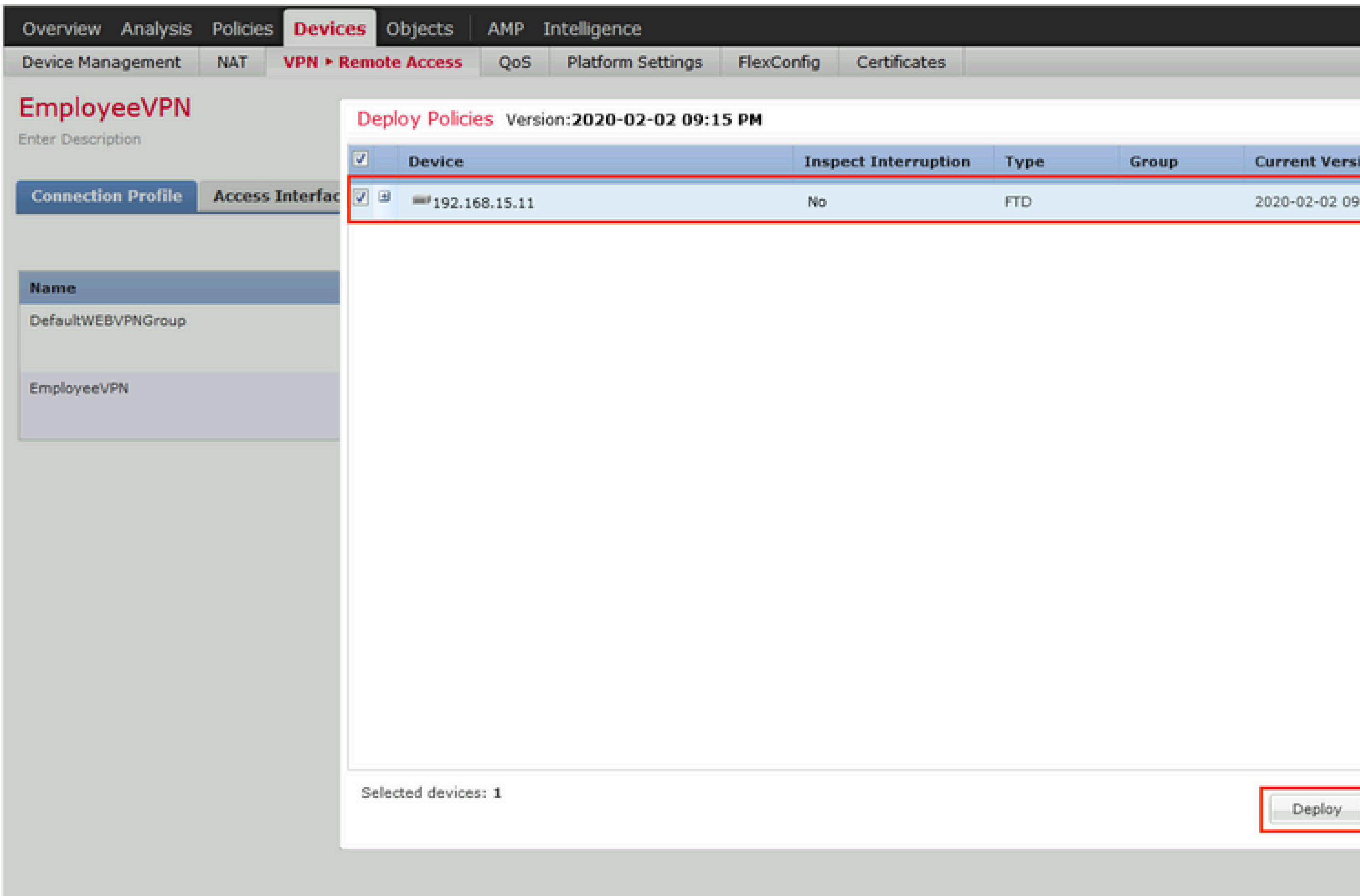
NAT Exemption
If NAT is enabled on the targ you must define a *NAT Polic* VPN traffic.

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

Port Configuration
SSL will be enabled on port 44 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'

Stap 15. Configuratie in FTD implementeren. Klik op **Implementeren** en selecteer **FTD** die wordt gebruikt als VPN-concentrator.



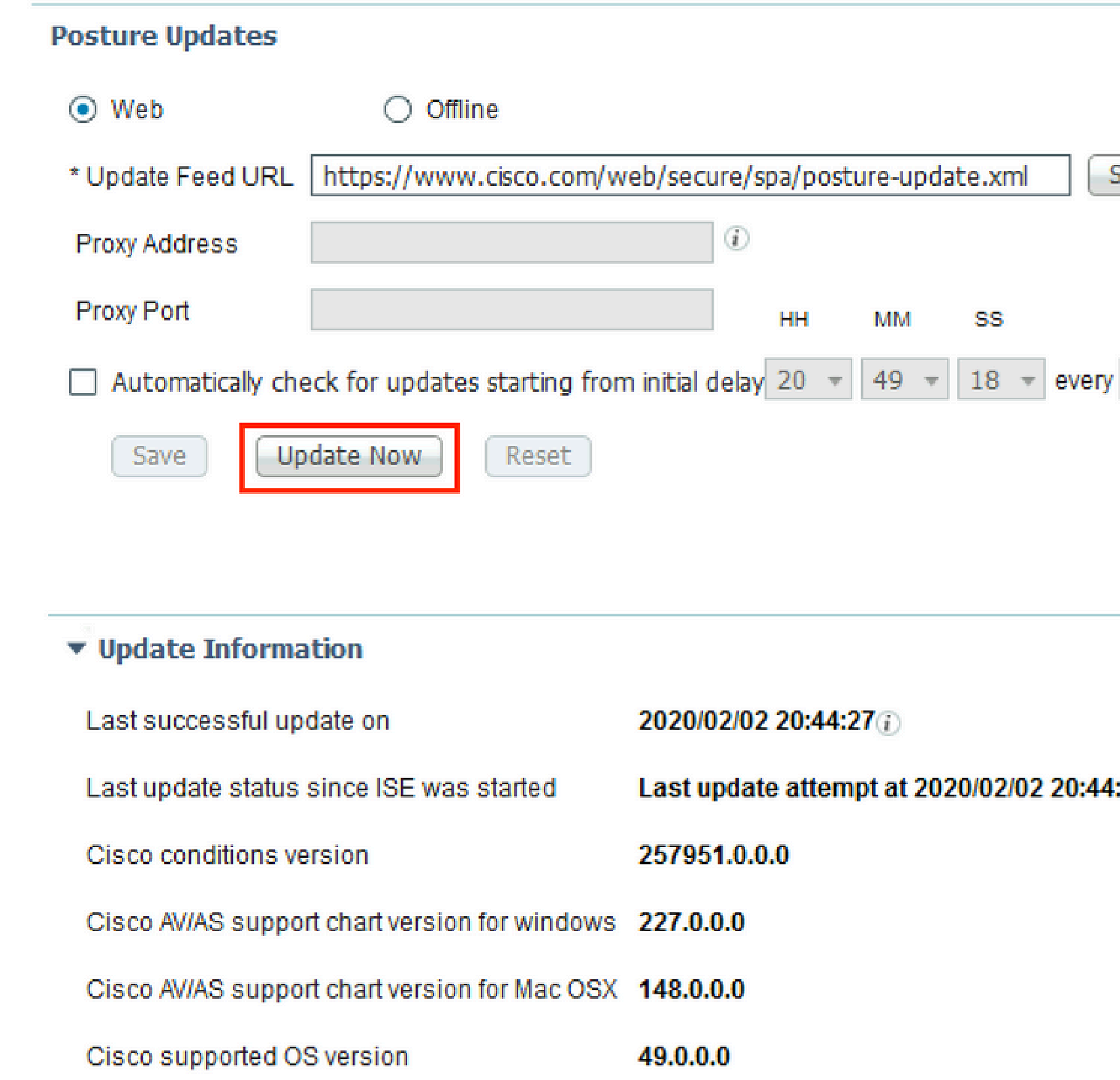
Deploy Policies Version:**2020-02-02 09:15 PM**

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

Selected devices: **1**

ISE

Stap 1. Werk de houding bij. Ga naar **Beheer > Systeem > Instellingen > Houding > 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 20 (HH) 49 (MM) 18 (SS) 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:

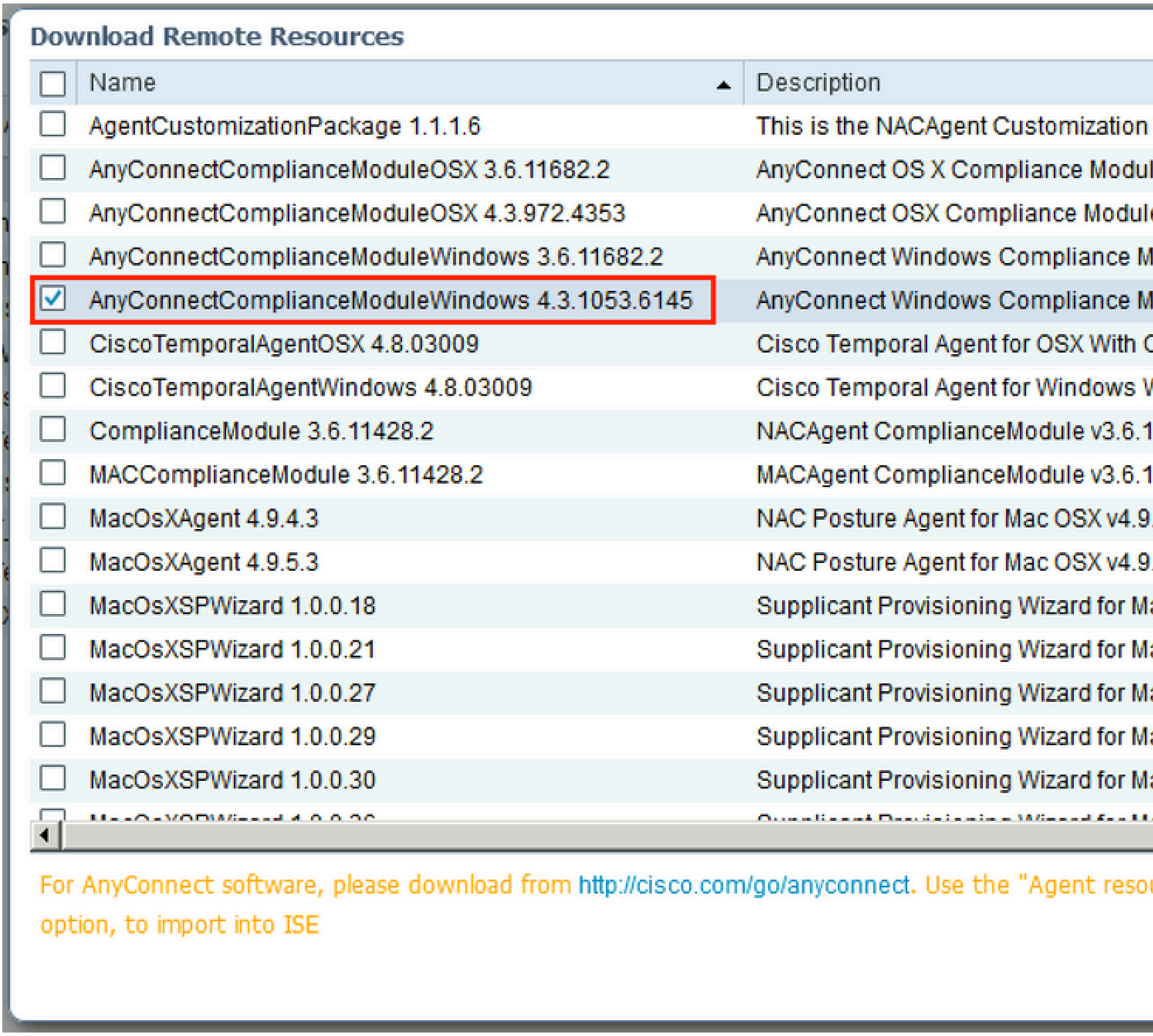
Cisco conditions version 257951.0.0.0

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

Stap 2. Nalevingsmodule voor uploaden. Ga naar **Beleid** > **Beleidselementen** > **Resultaten** > **Clientprovisioning** > **Resources**. Klik op **Add** en selecteer **Agent resources vanaf Cisco-site**



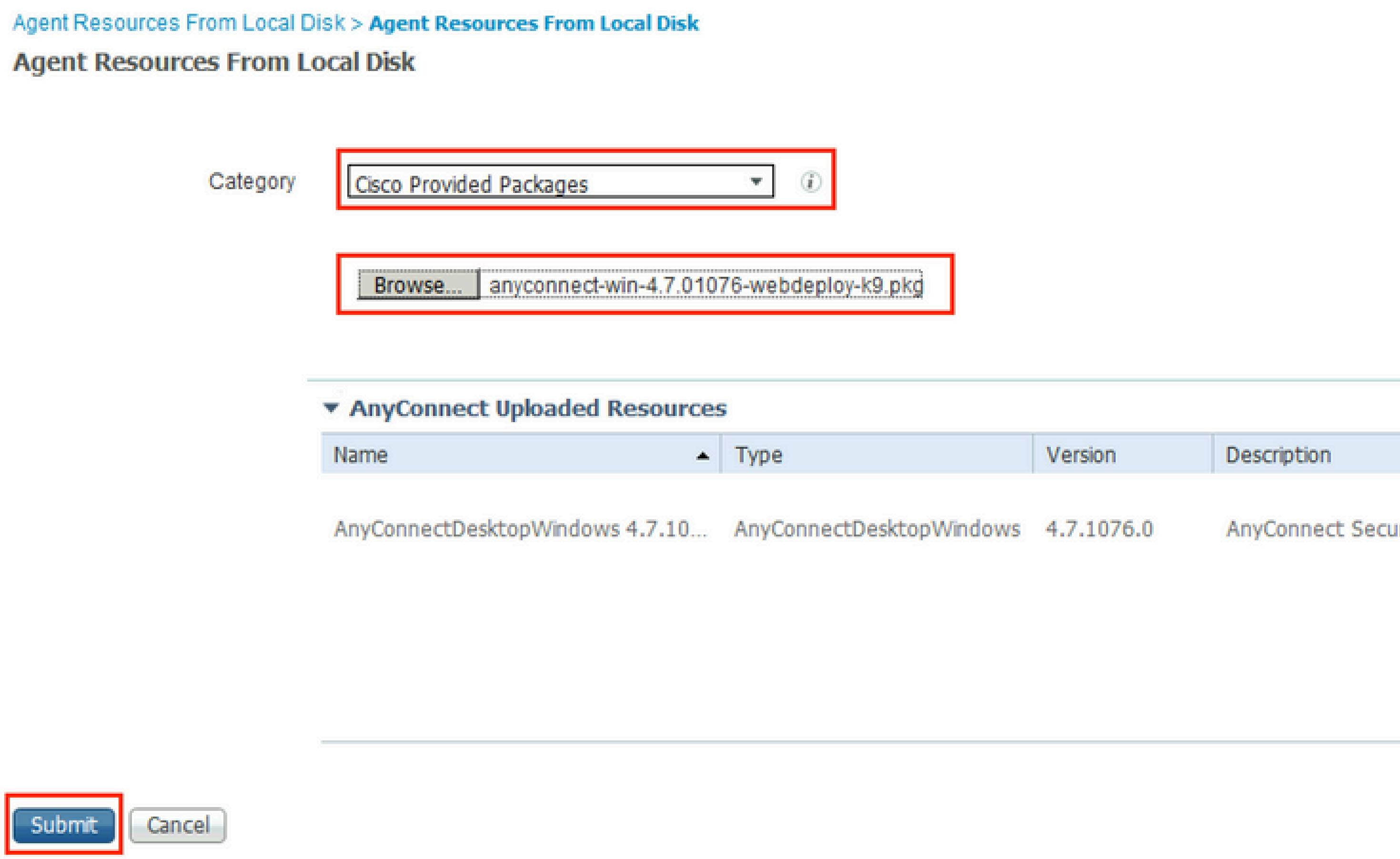
Download Remote Resources

□	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 M
□	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for M
□	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for M
□	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for M
□	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for M
□	MacOsXSPWizard 1.0.0.36	Supplicant Provisioning Wizard for M

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

Stap 3. Download AnyConnect van [Cisco Software Download]() en upload het vervolgens naar ISE. Ga naar **Beleid** > **Beleidselementen** > **Resultaten** > **Clientprovisioning** > **Resources**.

Klik op **Add** en selecteer **Agent Resources from Local Disk**. Kies **Cisco Provided Packages** onder **Category**, selecteer AnyConnect-pakket op de lokale schijf en klik op **Indienen**.



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

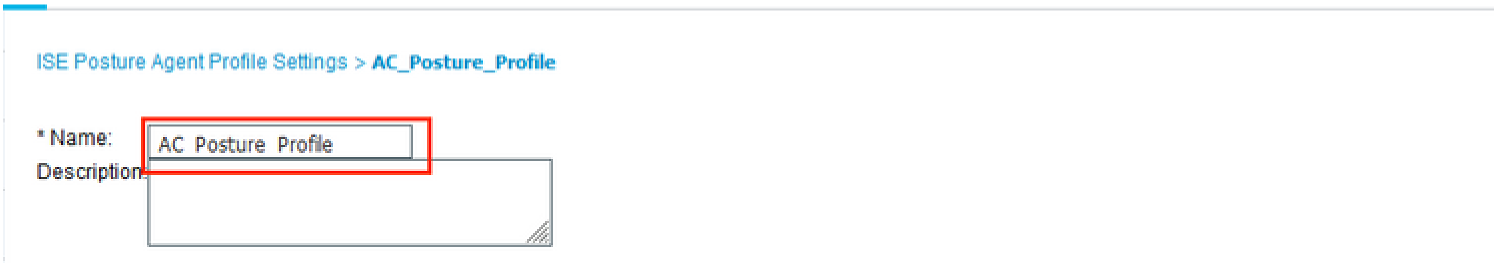
AnyConnect Uploaded Resources

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

Stap 4. Een profiel voor AnyConnect maken. Ga naar **Beleid** > **Beleidselementen** > **Resultaten** > **Clientprovisioning** > **Resources**.

Klik op **Add** en selecteer **AnyConnect Posture Profile**. Vul de naam en het protocol in.

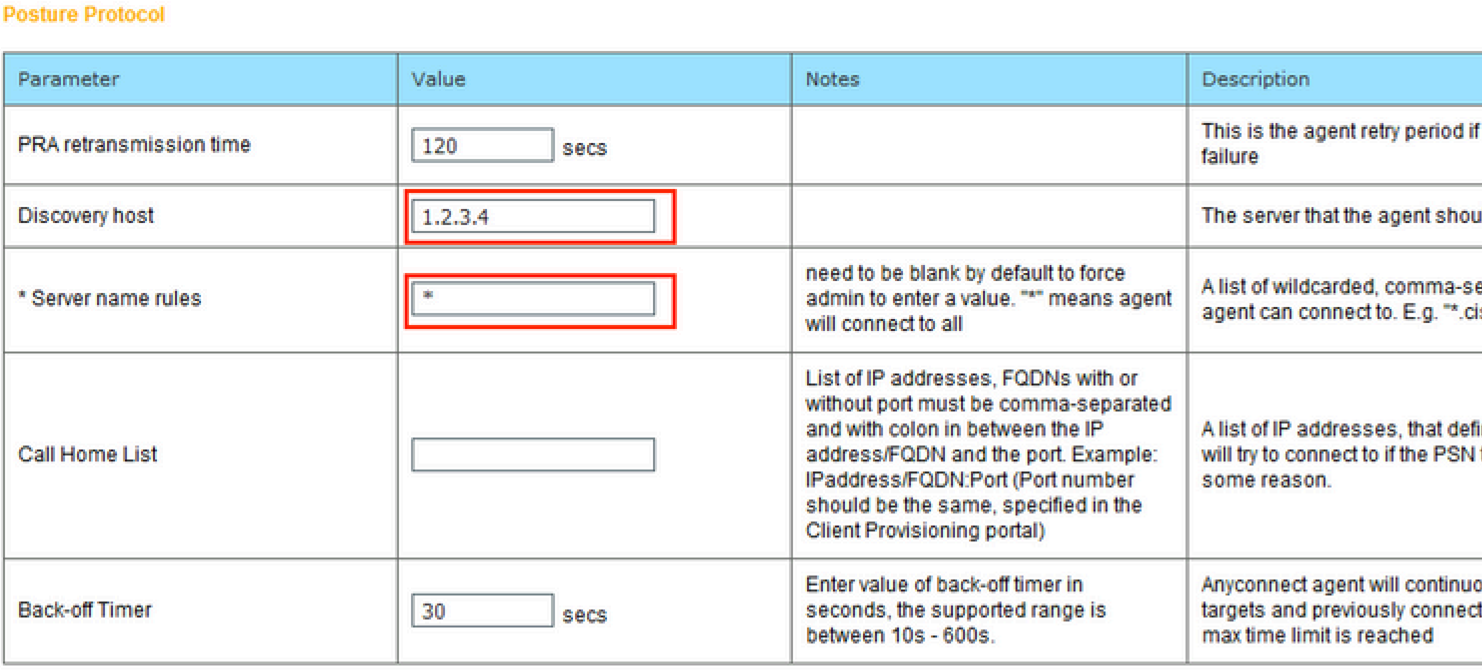
Onder ***Server naam regels** zet * en zet een dummy IP-adres onder **Discovery host**.



ISE Posture Agent Profile Settings > **AC_Posture_Profile**

* Name: AC_Posture_Profile

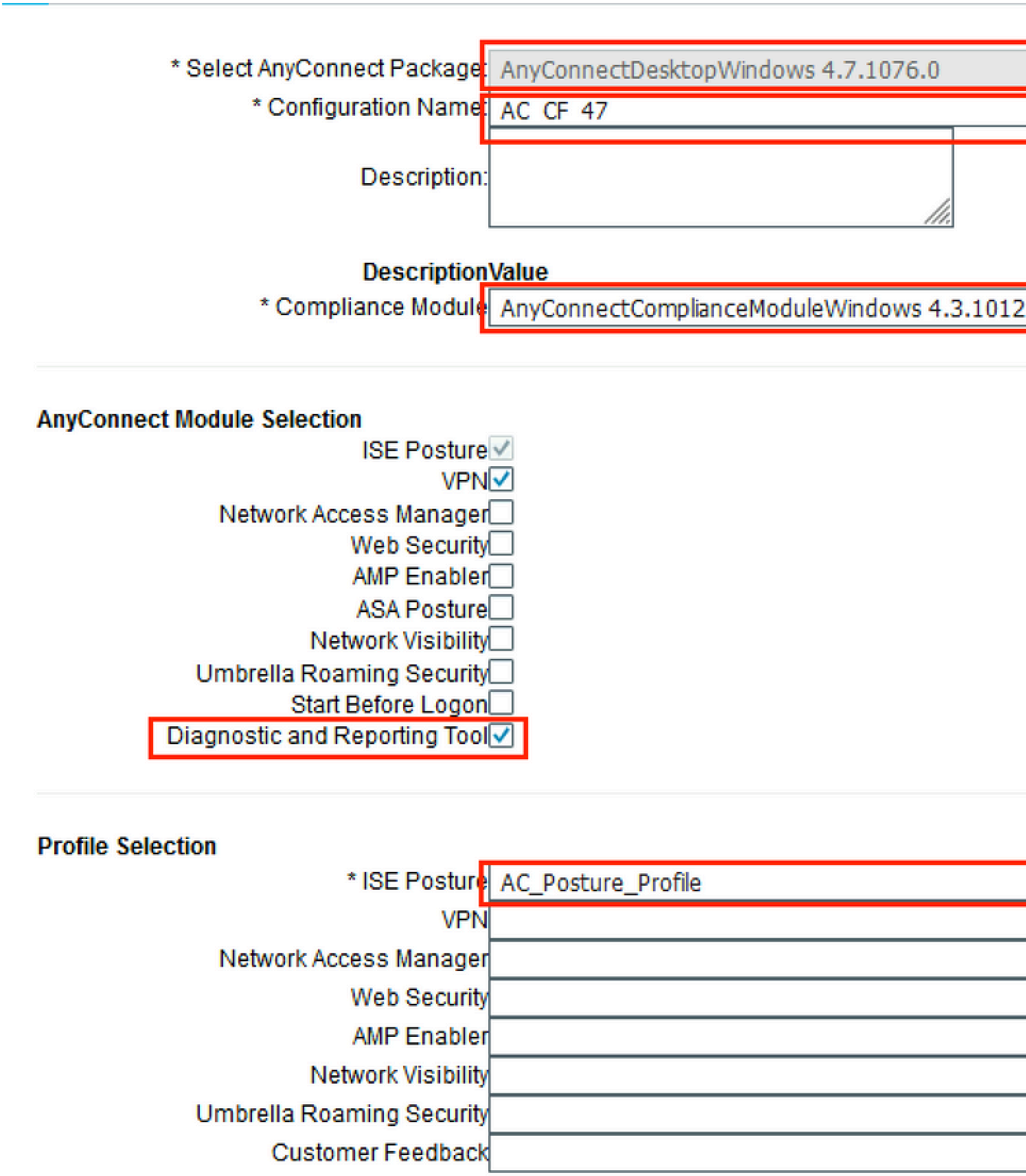
Description:



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

Stap 5. Navigeren naar **Beleid > Beleidselementen > Resultaten > Clientprovisioning > Resources** en **AnyConnect Configuration** maken. Klik op **Add** en selecteer **AnyConnect Configuration**. Selecteer **AnyConnect-pakket**, geef de configuratienaam op, selecteer **compliancemodule**, controleer het diagnostische en rapportageprogramma, selecteer **Profiel houding** en klik op **Opslaan**.



* 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:

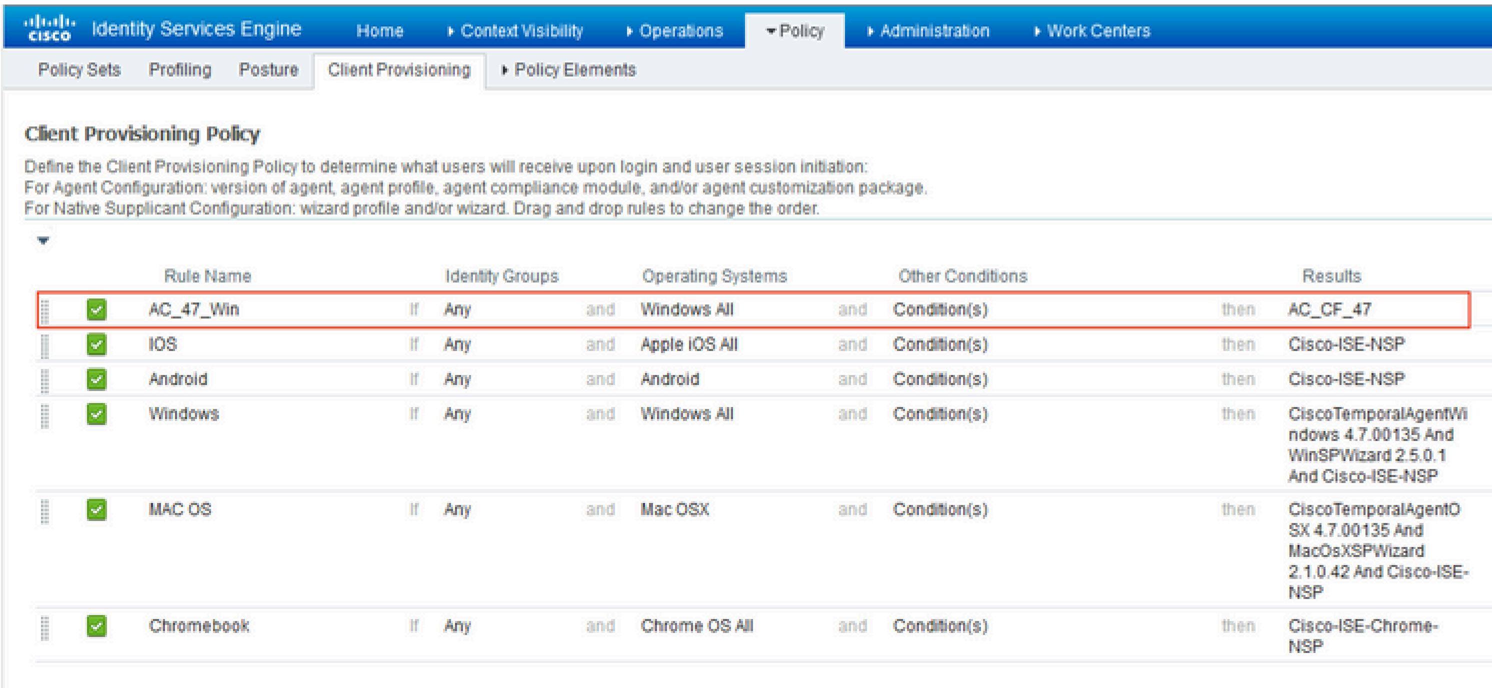
AMP Enabler:

Network Visibility:

Umbrella Roaming Security:

Customer Feedback:

Stap 6. Navigeer naar **Beleid** > **Clientprovisioning** en maak een **clientprovisioningbeleid**. Klik op **Bewerken** en selecteer vervolgens **Regel invoegen hierboven**, geef naam op, selecteer het besturingssysteem en kies **AnyConnect Configuration** die in de vorige stap is gemaakt.



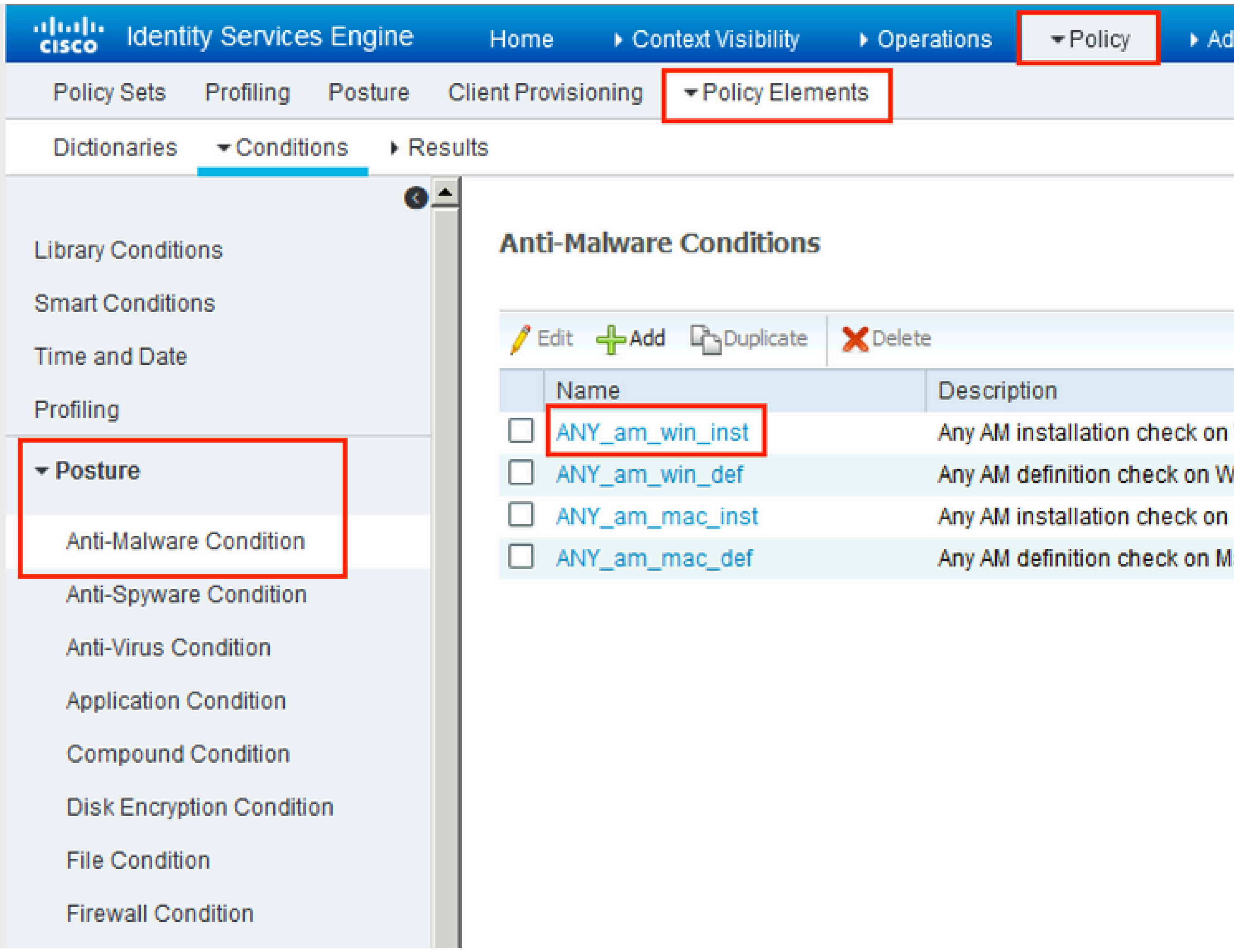
Client Provisioning Policy

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

Stap 7. Houdbaarheid aanmaken onder **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Anti-Malware Condition**. In dit voorbeeld, wordt "ANY_am_win_inst" vooraf gedefinieerd.

.

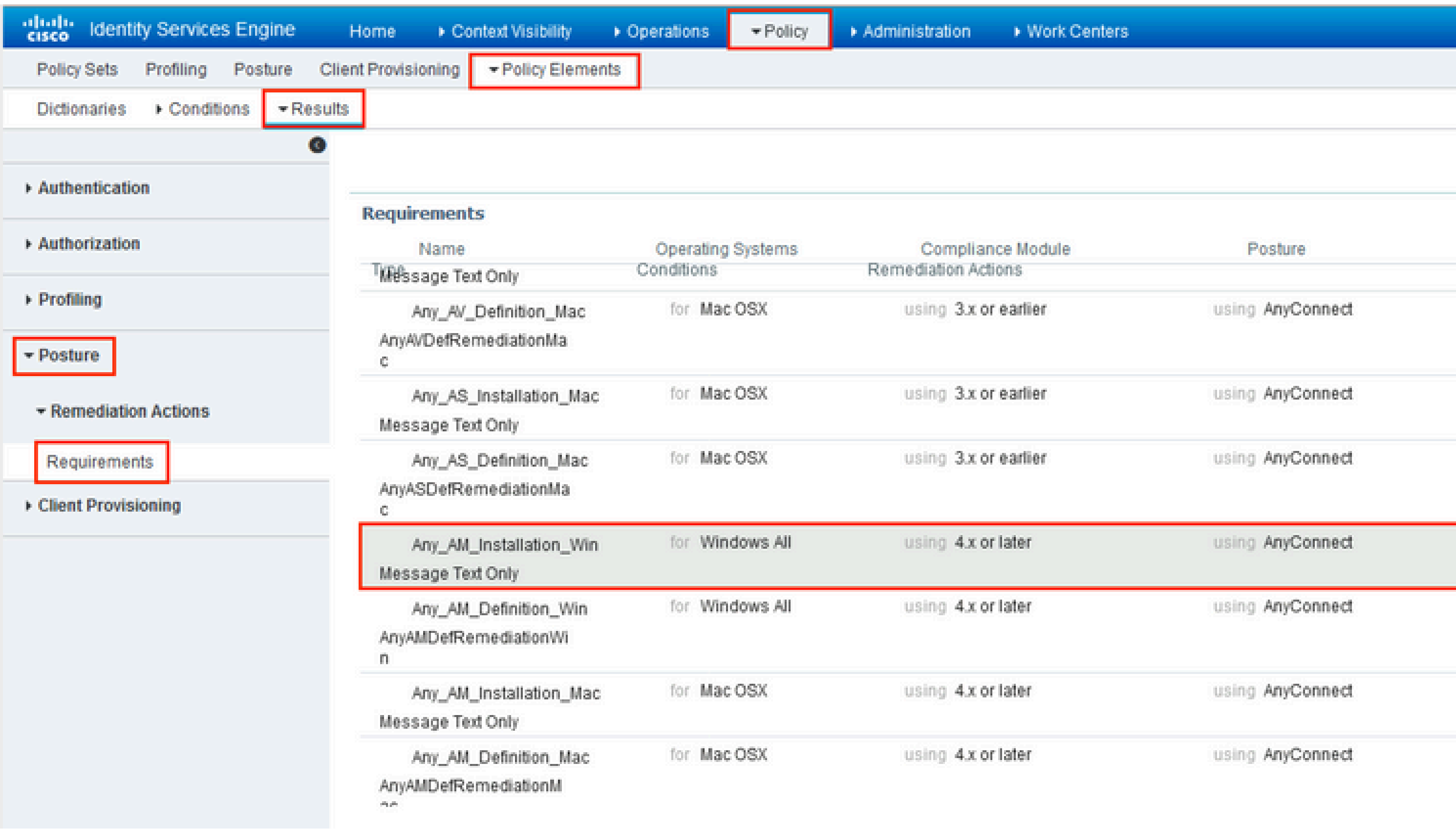


Anti-Malware Conditions

	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

Stap 8. Ga naar **Beleid** > **Beleidselementen** > **Resultaten** > **Houding** > **Herstelmaatregelen** en creëer **Posture Remediation**. In dit voorbeeld wordt het overgeslagen. Oplossingsactie kan een tekstbericht zijn.

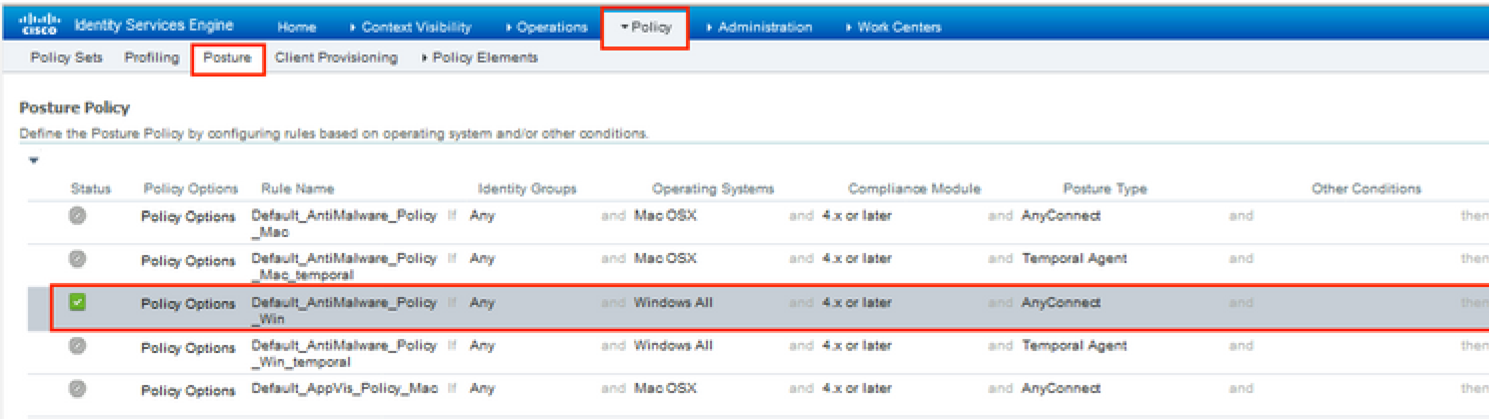
Stap 9. Navigeer naar **Beleid** > **Beleidselementen** > **Resultaten** > **Houding** > **Vereisten** en creëer **Houding Vereisten**. Vooraf gedefinieerde vereiste Any_AM_Installatie_Win wordt gebruikt.



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

Stap 10. Posterijen onder **Beleid** > **Posterijen** maken. Standaard posterbeleid voor alle AntiMalware Check voor Windows OS wordt gebruikt.



Posture Policy

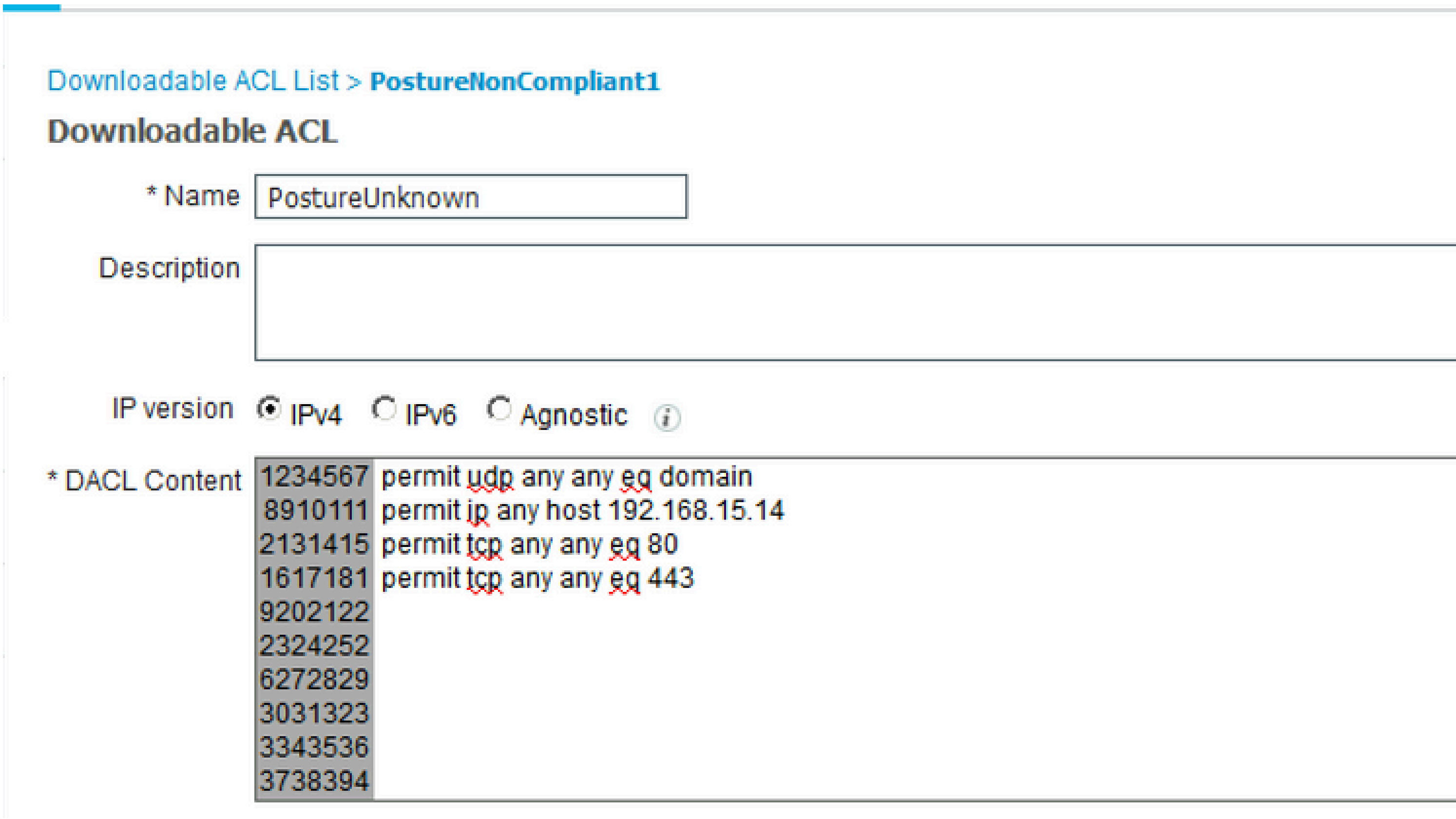
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

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

Stap 11. Navigeer naar **Beleid** > **Beleidselementen** > **Resultaten** > **Autorisatie** > **Downloadbare ACLS en** maak DACL's voor verschillende postuur-statussen.

In dit voorbeeld:

- Posture Unknown DACL - maakt verkeer mogelijk naar DNS-, PSN- en HTTP- en HTTPS-verkeer.
- Posture NonCompliant DACL - ontzegt toegang tot Private Subnets en staat alleen internetverkeer toe.
- Laat Alle DACL toe - staat al verkeer voor Posture Volgzame Status toe.



Downloadable ACL List > **PostureNonCompliant1**

Downloadable ACL

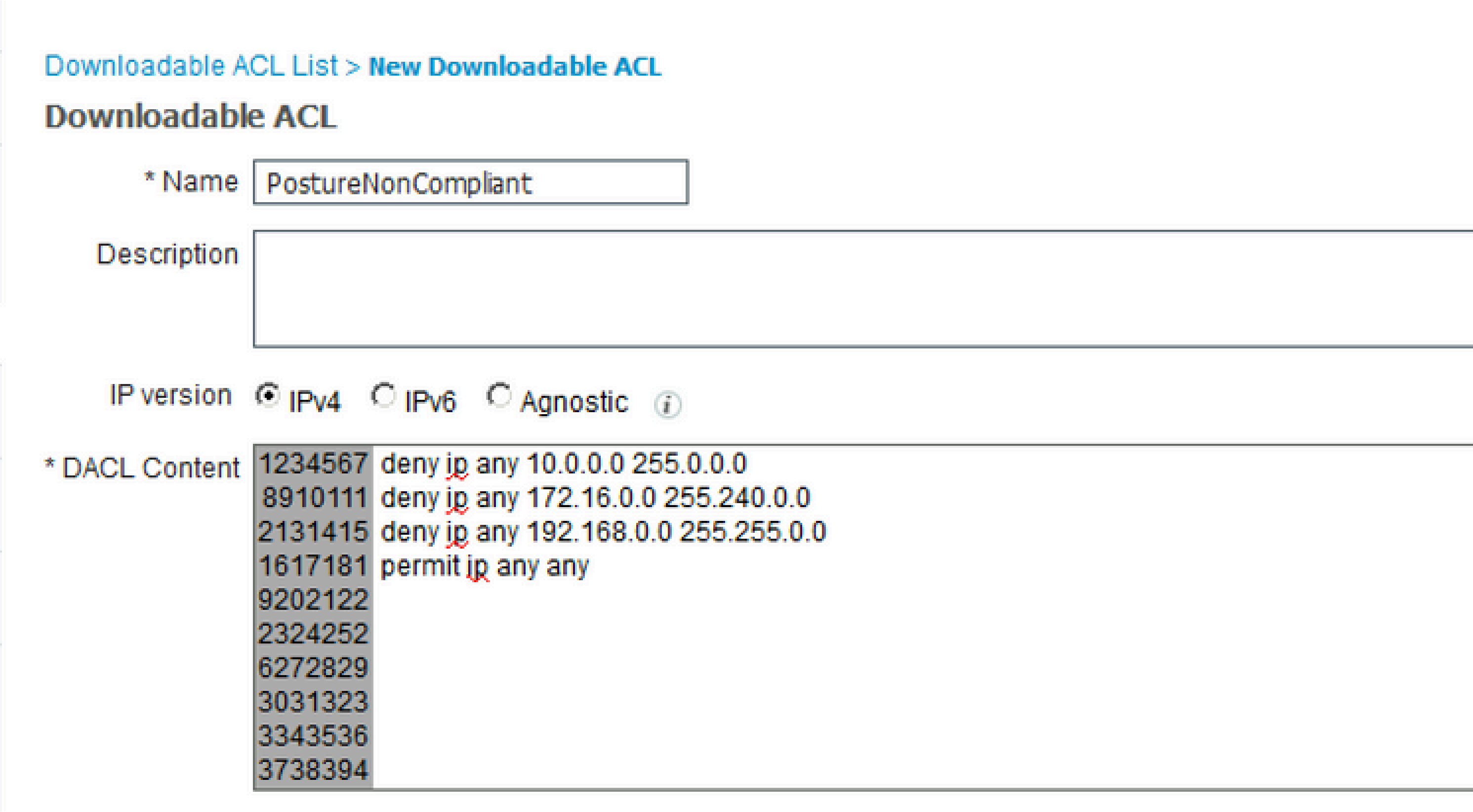
* Name: PostureUnknown

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

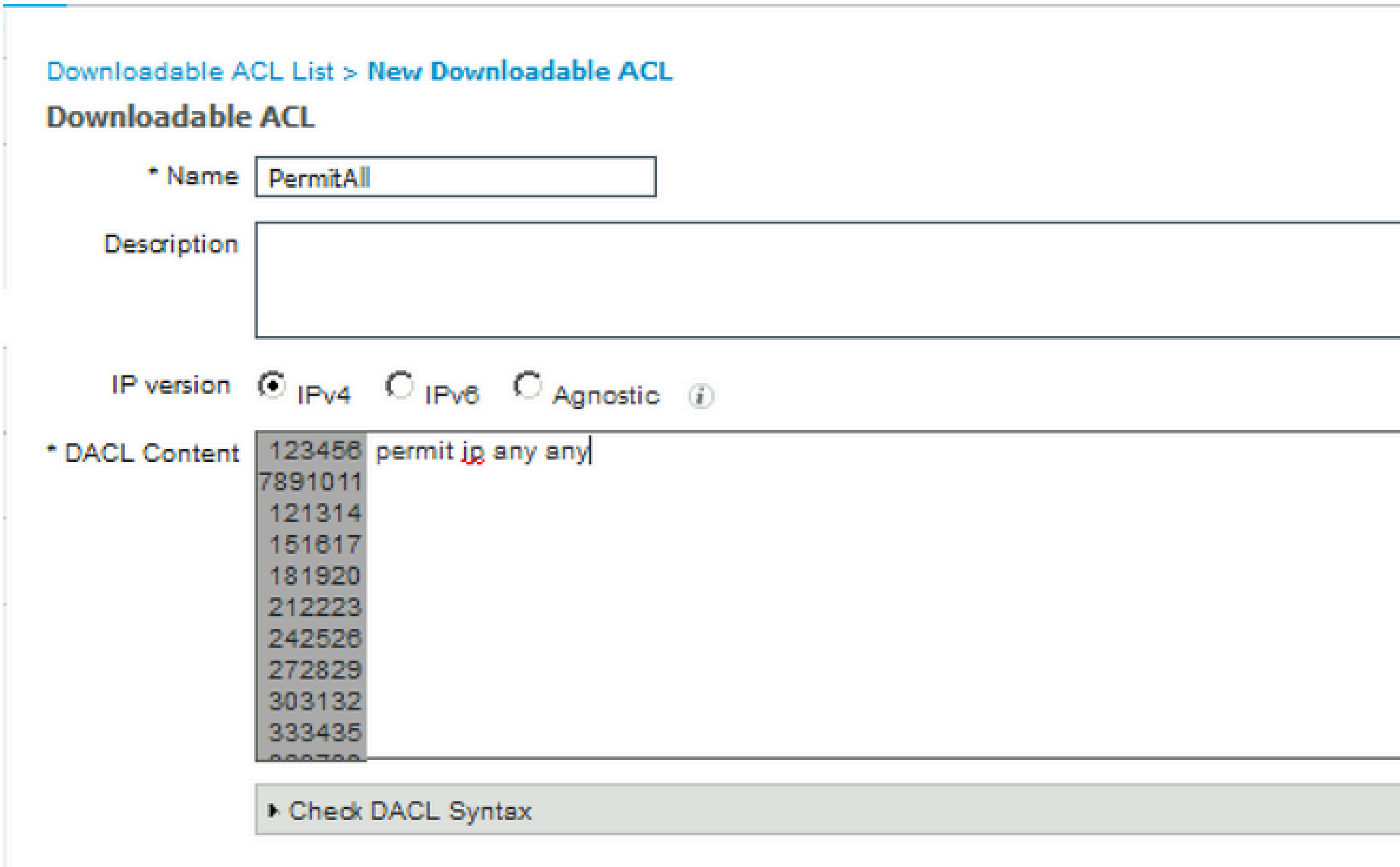
* Name: PostureNonCompliant

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
```



* Name PermitAll

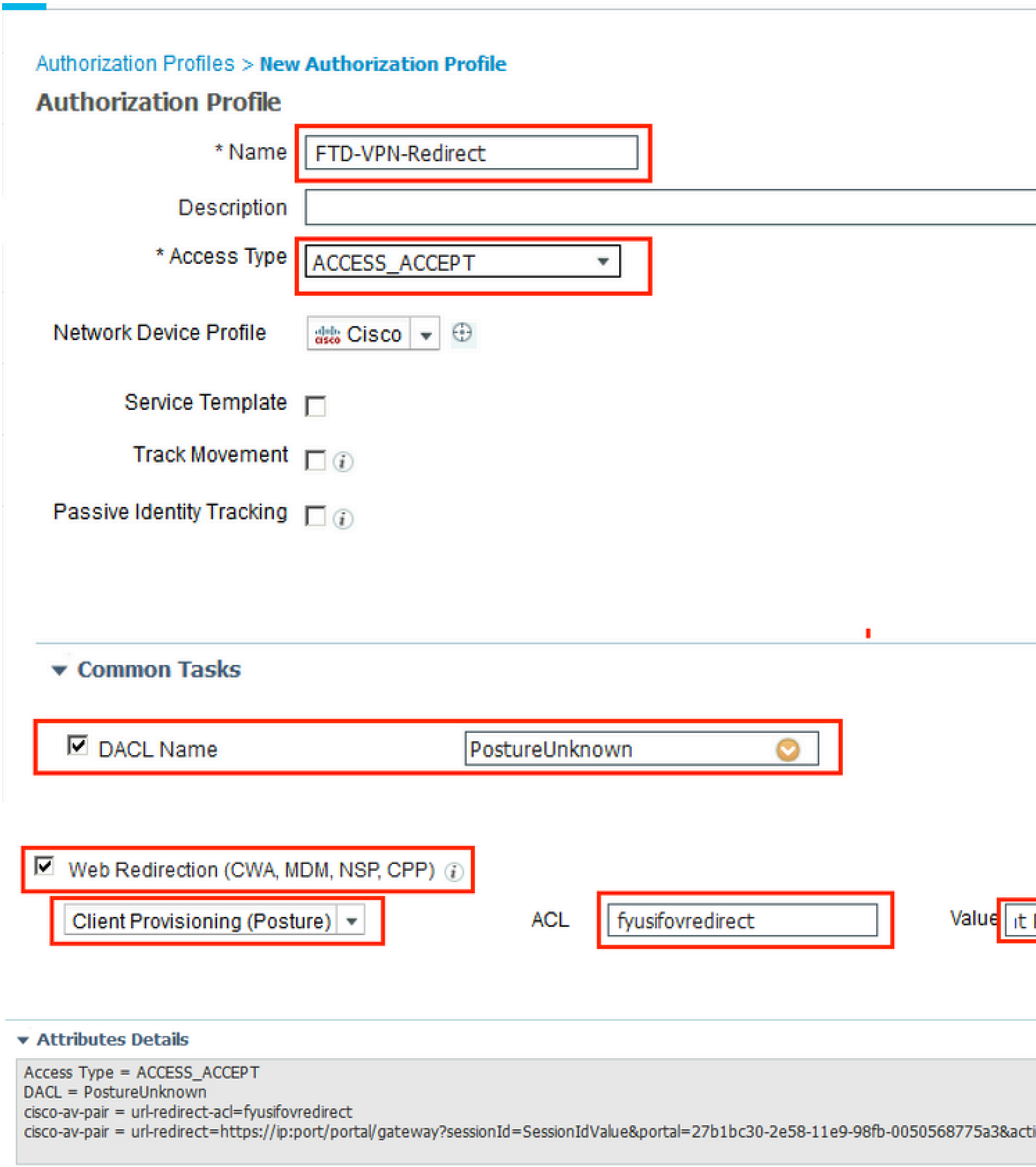
Description

IP version ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content

```
permit ip any any
```

Stap 12. Maak drie autorisatieprofielen voor de status Onbekend, niet-conform en niet-conform. Hiervoor bladert u naar **Policy > Policy Elements > Results > Authorisation > Authorisation Profiles**. Selecteer in het profiel **Onbekend** maken van de **houding**, selecteer **Onbekend DACL van de houding**, controleer **webomleiding**, selecteer **Clientprovisioning**, geef Redirect ACL-naam (die op FTD is geconfigureerd) en selecteer de 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

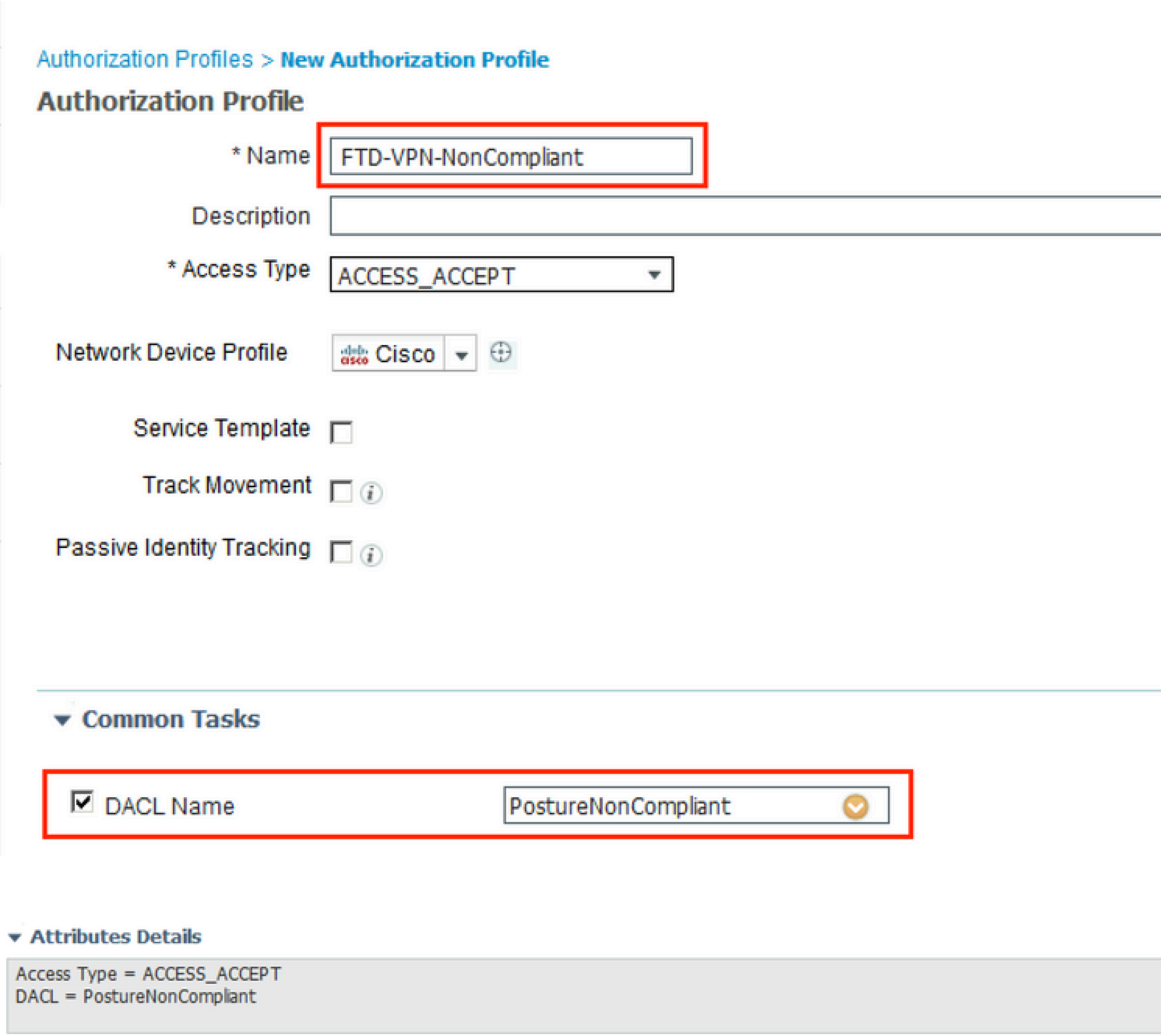
☑ Web Redirection (CWA, MDM, NSP, CPP)

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

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
```

Selecteer in het profiel **Posture NonCompliant DACL** om de toegang tot het netwerk te beperken.



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 □

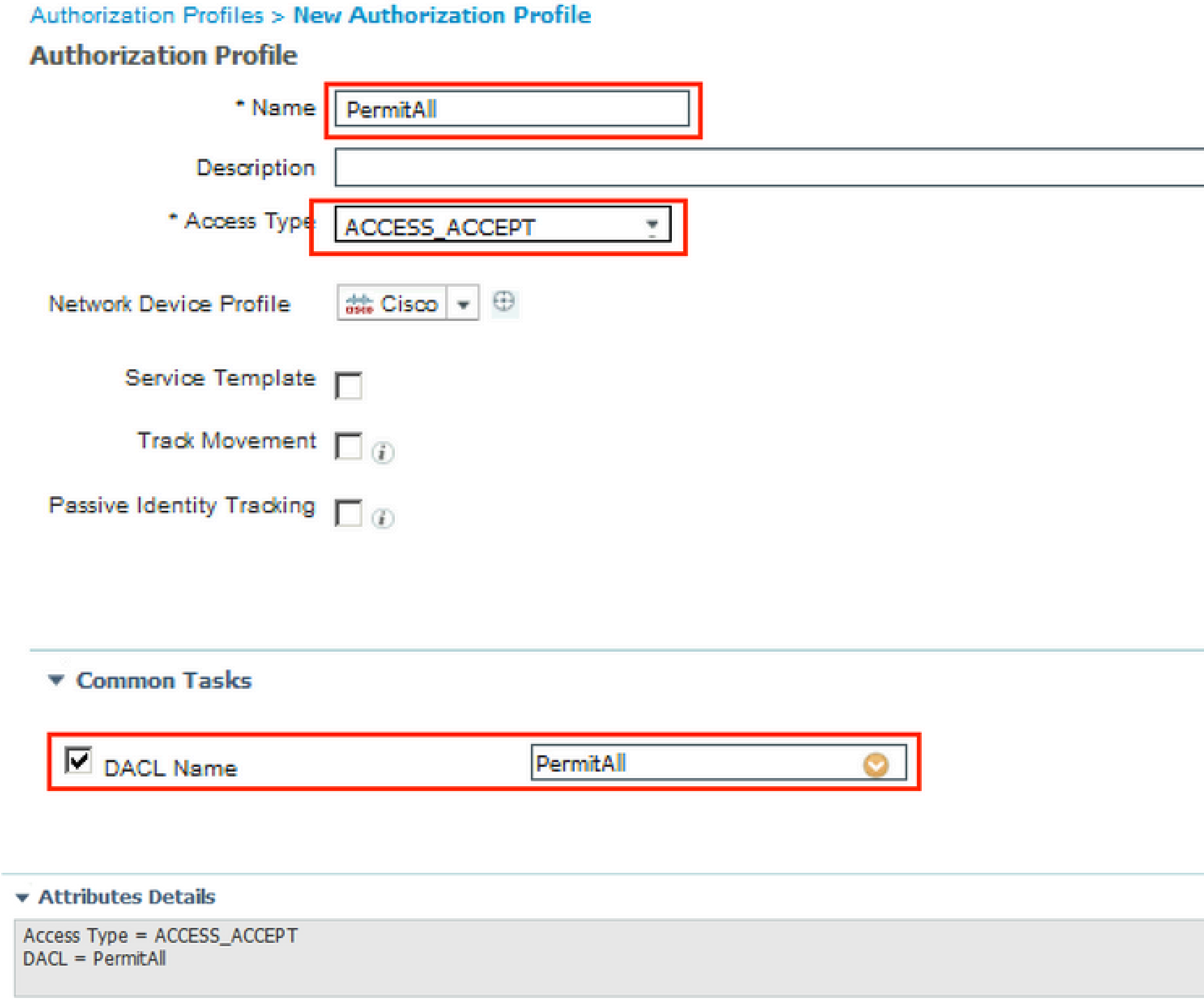
Common Tasks

☑ DACL Name: PostureNonCompliant

Attributes Details

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

Selecteer in het profiel **Posture Compliant DACL** om volledige toegang tot het netwerk mogelijk te maken.



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 □

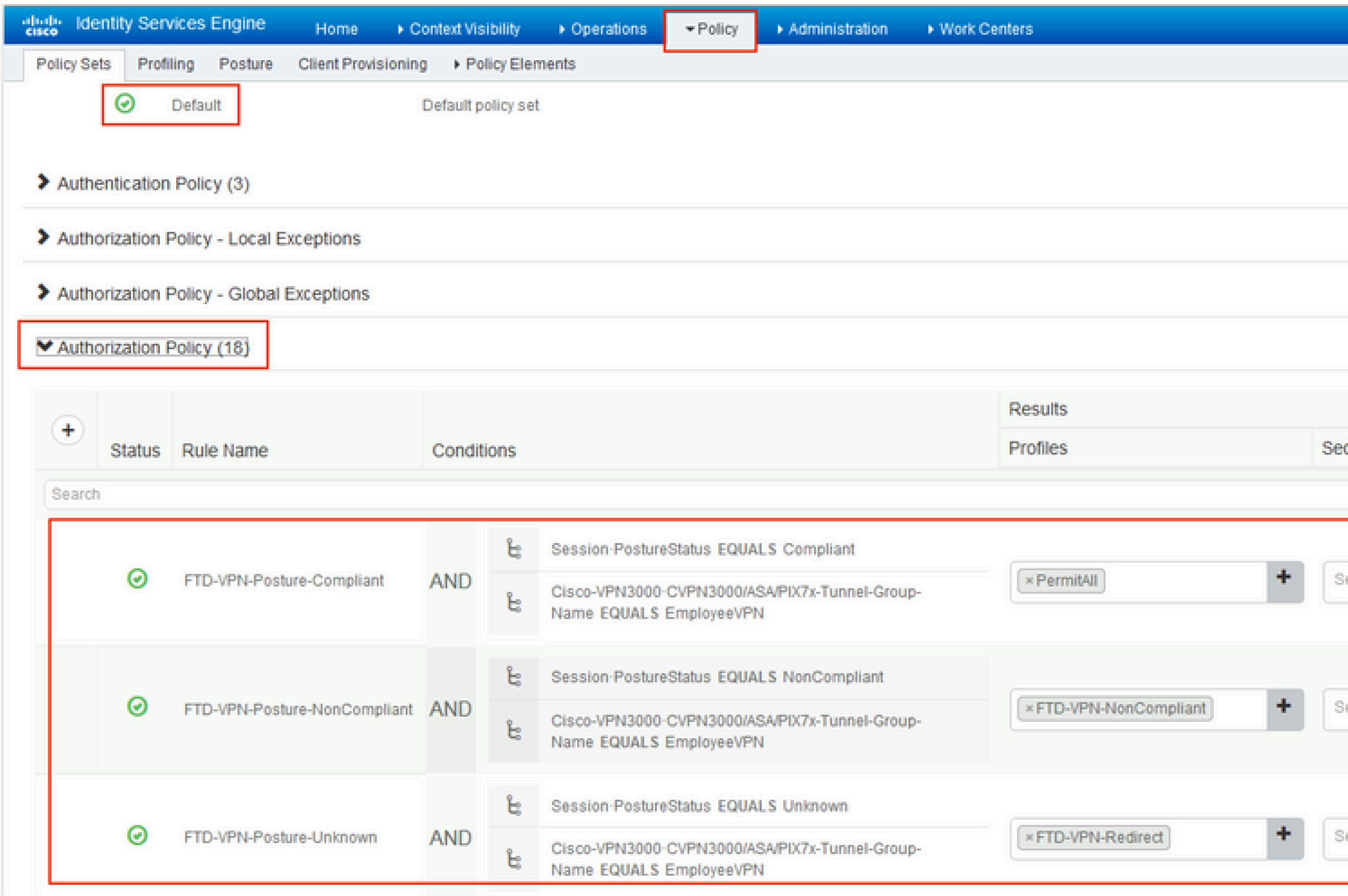
Common Tasks

☑ DACL Name: PermitAll

Attributes Details

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

Stap 13. Creëer autorisatiebeleid onder **Beleid** > **Beleidssets** > **Standaard** > **Autorisatiebeleid**. Als conditie Positie Status en VNP TunnelGroup Naam wordt gebruikt.



Default — Default policy set

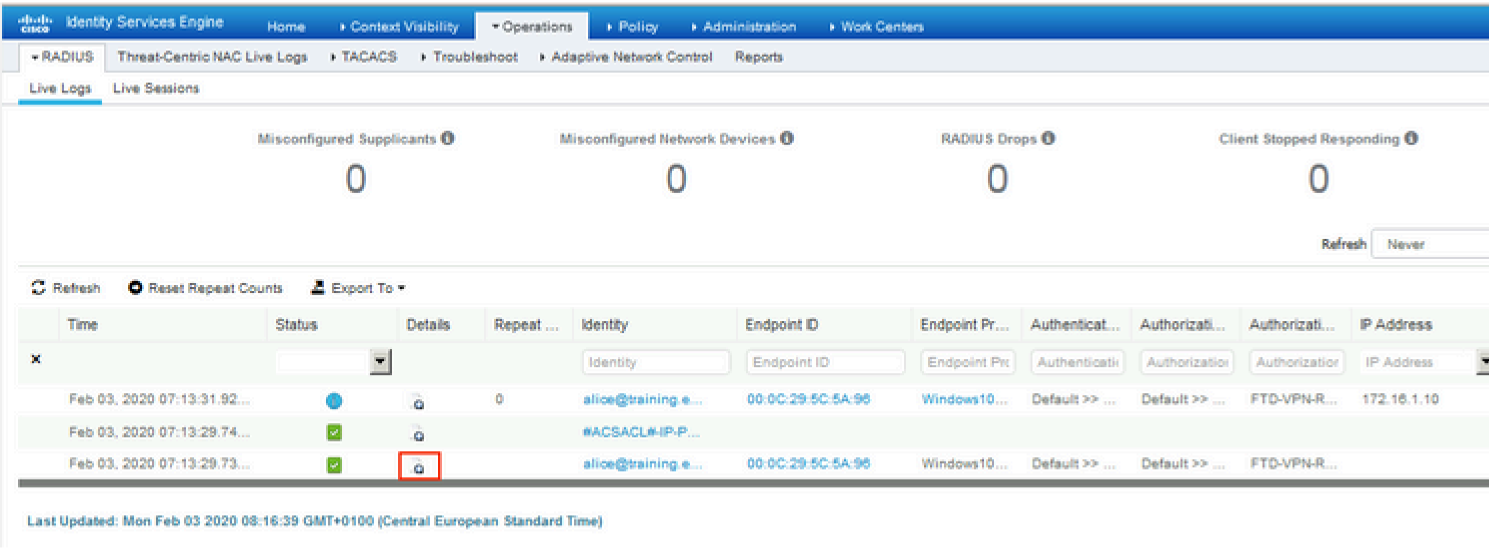
- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (18)

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

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Op ISE is de eerste verificatiestap RADIUS Live Log. Navigeer naar **Operations** > **RADIUS Live Log**. Hier is de gebruiker Alice verbonden en wordt het verwachte autorisatiebeleid geselecteerd.

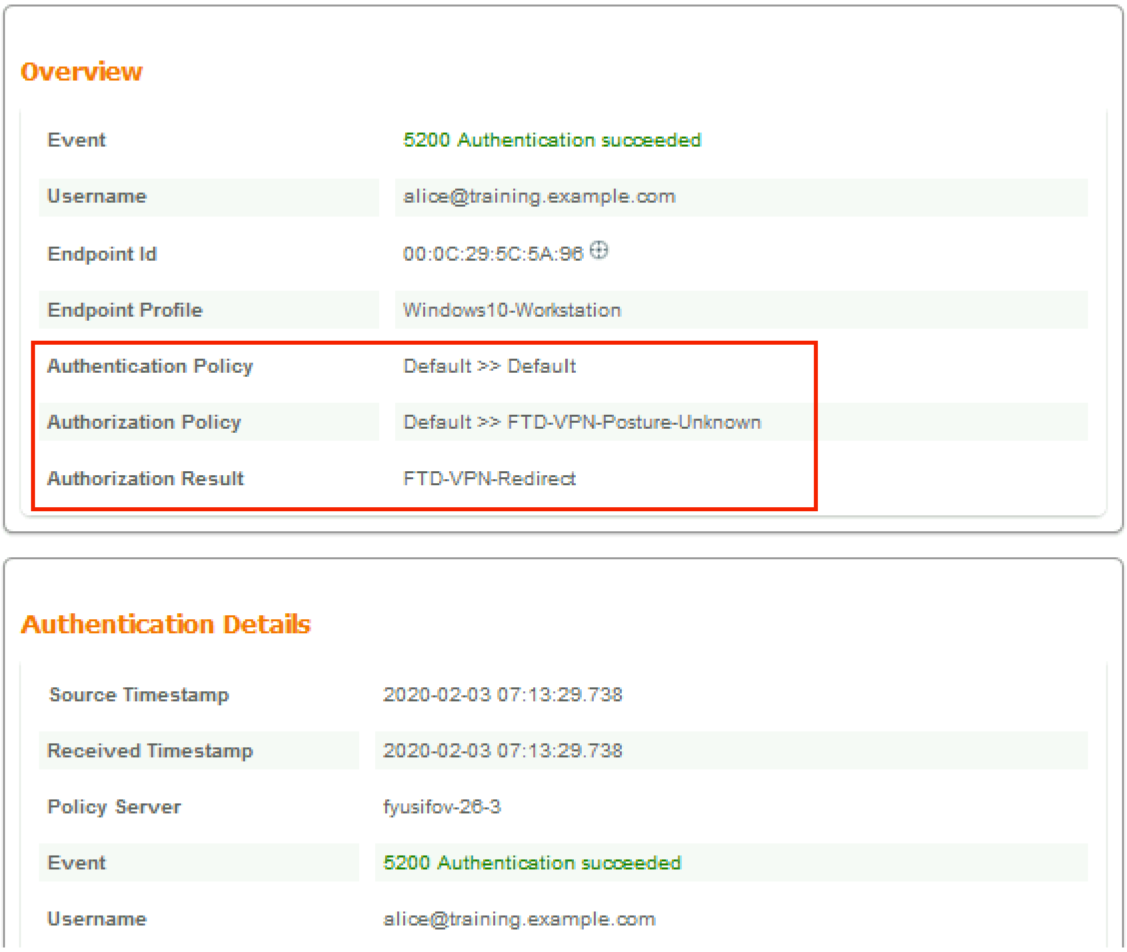


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding
0	0	0	0

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)

Het FTD-VPN-Posture-Unknown autorisatiebeleid wordt gematched en als gevolg daarvan wordt het FTD-VPN-Profiel naar FTD verzonden.



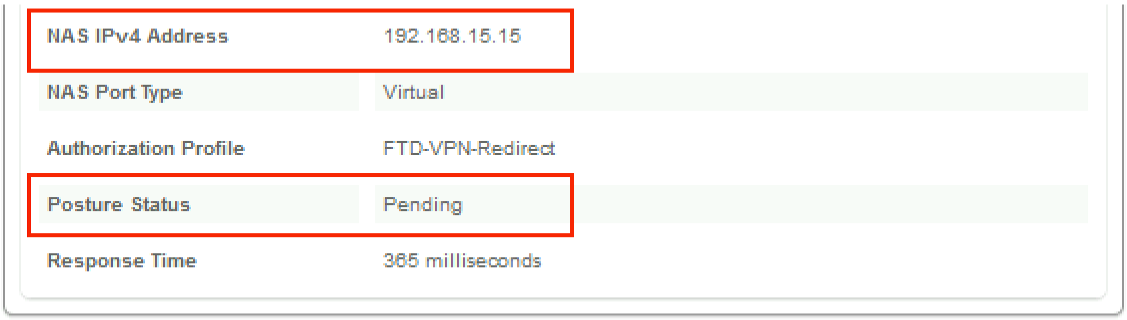
Overview

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

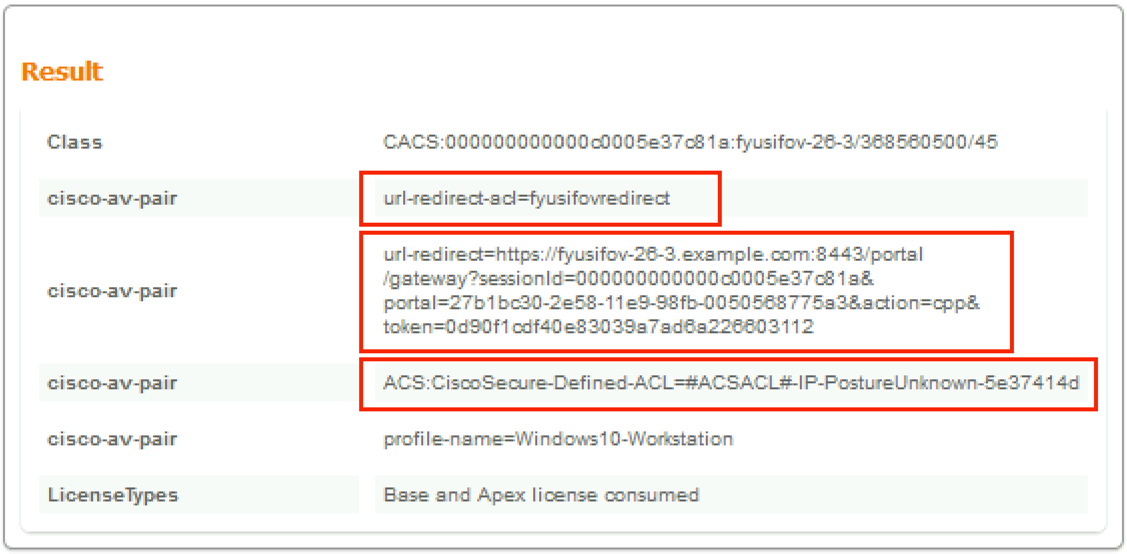
Source Timestamp	2020-02-03 07:13:29.738
Received Timestamp	2020-02-03 07:13:29.738
Policy Server	fyusifov-26-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

Houdbaarheid status in behandeling.



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

De sectie Resultaat toont welke eigenschappen naar FTD worden verzonden.



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

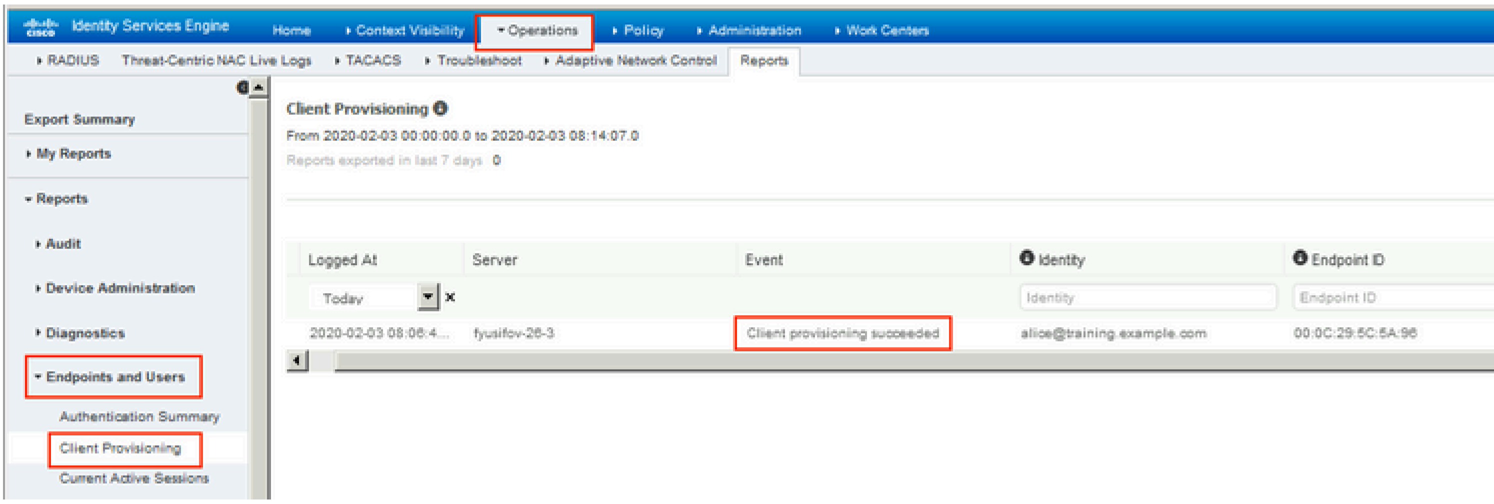
Op FTD, om de verbinding van VPN te verifiëren, SSH aan het vakje, voer **systeemsteun kenmerkend-cli uit** en **toon** dan **vpn-sessiondb detail om het even welk verbinden**. Van deze output, verifieer dat de attributen die van ISE worden verzonden voor deze VPN zitting worden toegepast.

<#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#
```

Het beleid voor clientprovisioning kan worden geverifieerd. Ga naar **Operations > Rapporten > Endpoints en gebruikers > Clientprovisioning**.



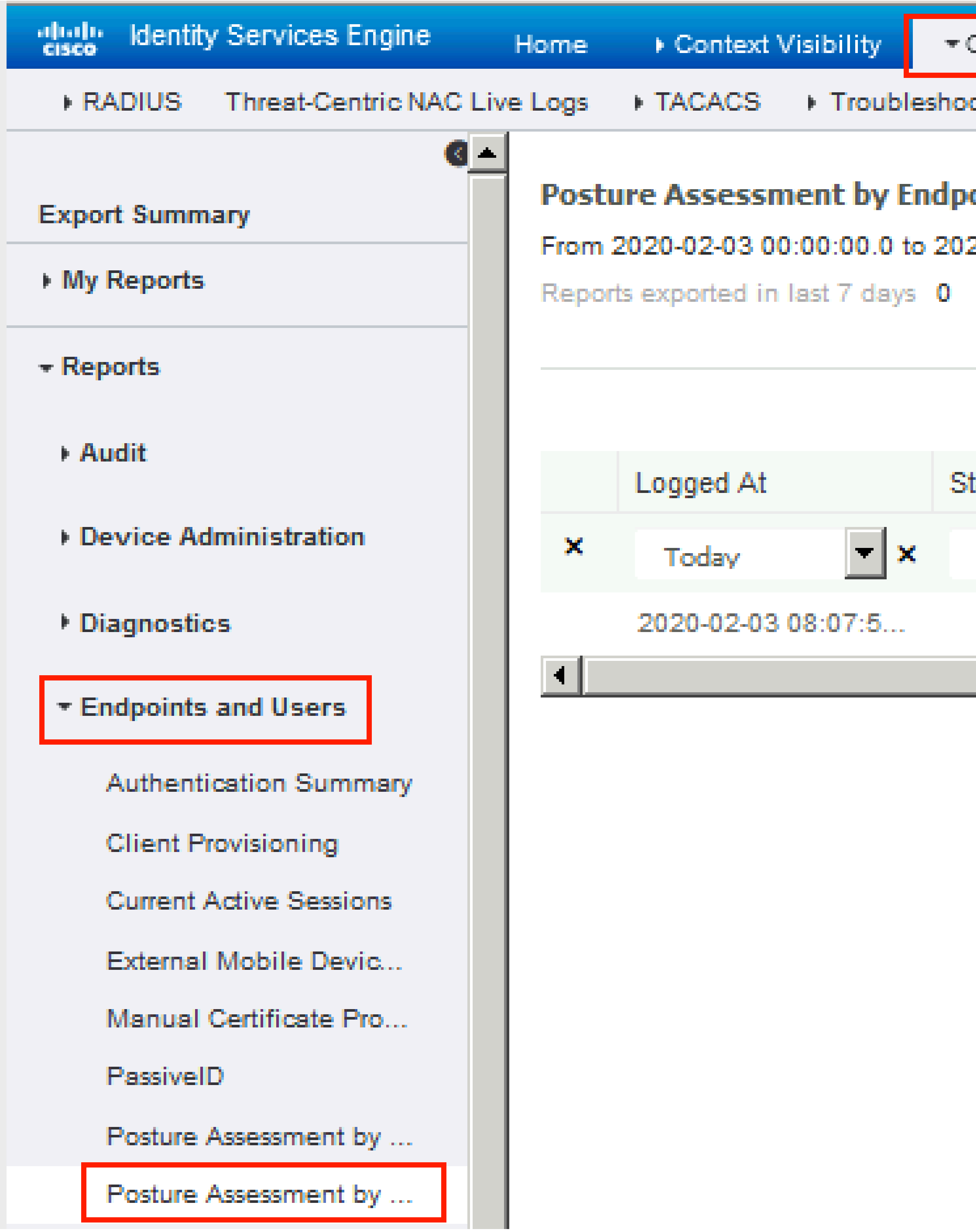
Client Provisioning

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

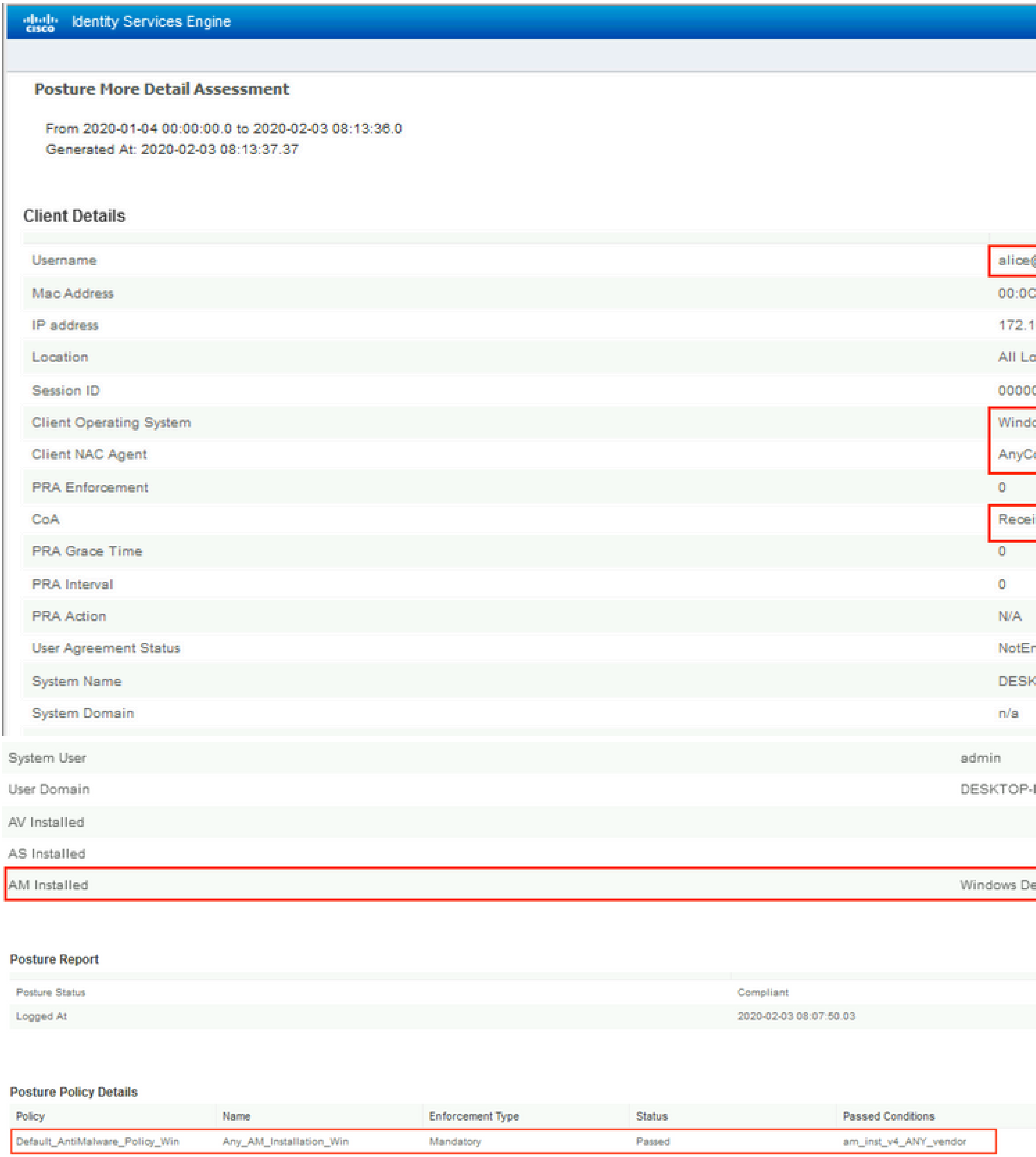
Reports exported in last 7 days 0

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

Het rapport van de houding dat van AnyConnect wordt verzonden kan worden gecontroleerd. Ga naar **Operations > Rapporten > Eindpunten en gebruikers > Posture Assessment by Endpoint**.



Klik op **Details** om meer details te zien in het poortrapport.



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

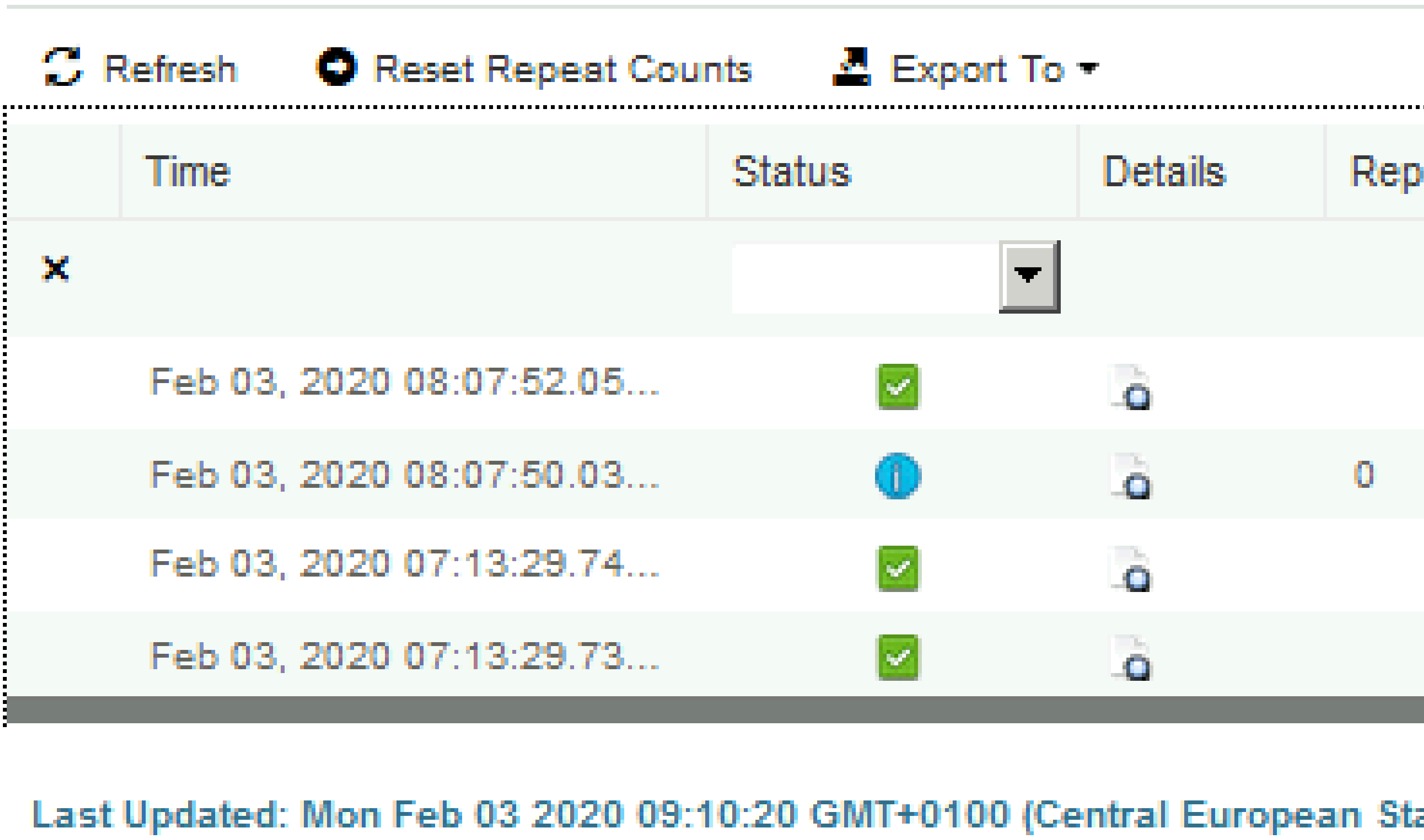
Posture Report

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

Posture Policy Details

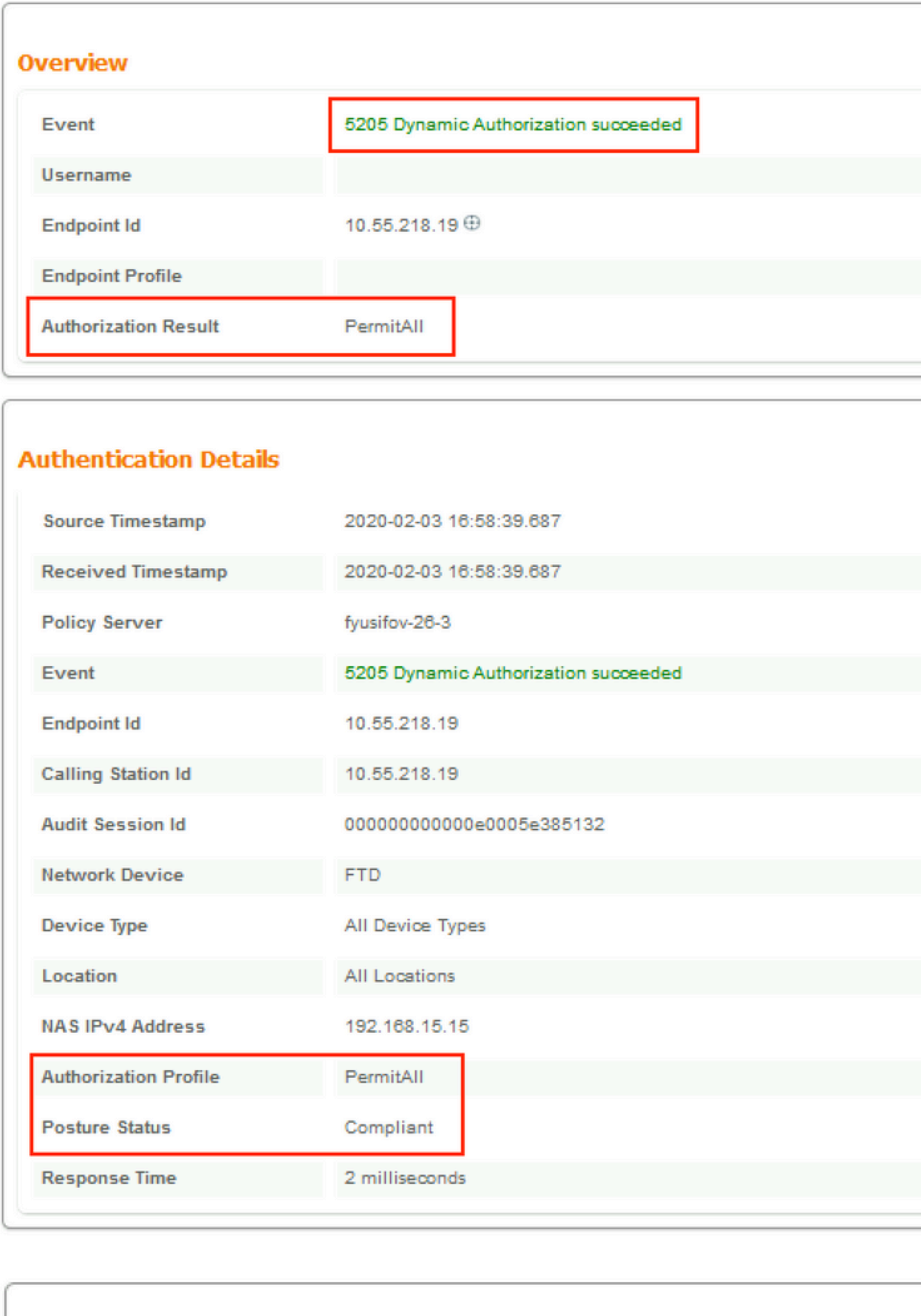
Policy	Name	Enforcement Type	Status	Passed Conditions
Default_AntiMalware_Policy_Win	Any_AM_Installation_Win	Mandatory	Passed	am_inst_v4_ANY_vendor

Nadat het rapport is ontvangen op ISE, wordt de postuur status bijgewerkt. In dit voorbeeld is de postuur status compatibel en CoA Push wordt geactiveerd met een nieuwe reeks kenmerken.



	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

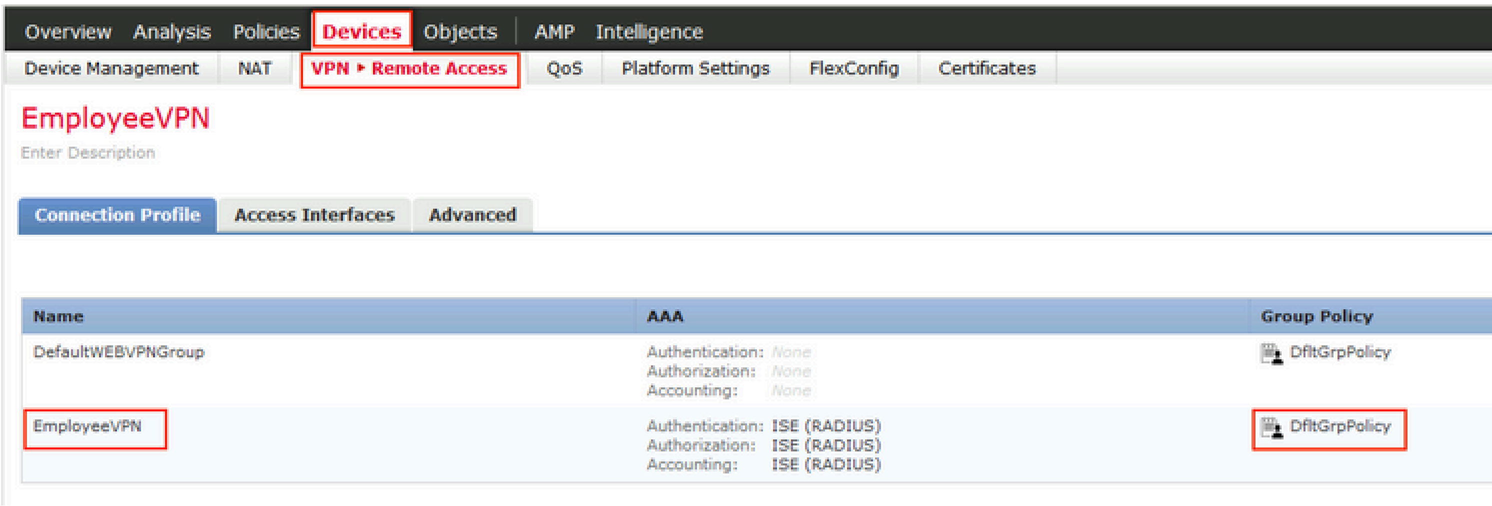
Event	5205 Dynamic Authorization succeeded
Username	
Endpoint Id	10.55.218.19 ⊕
Endpoint Profile	
Authorization Result	PermitAll

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

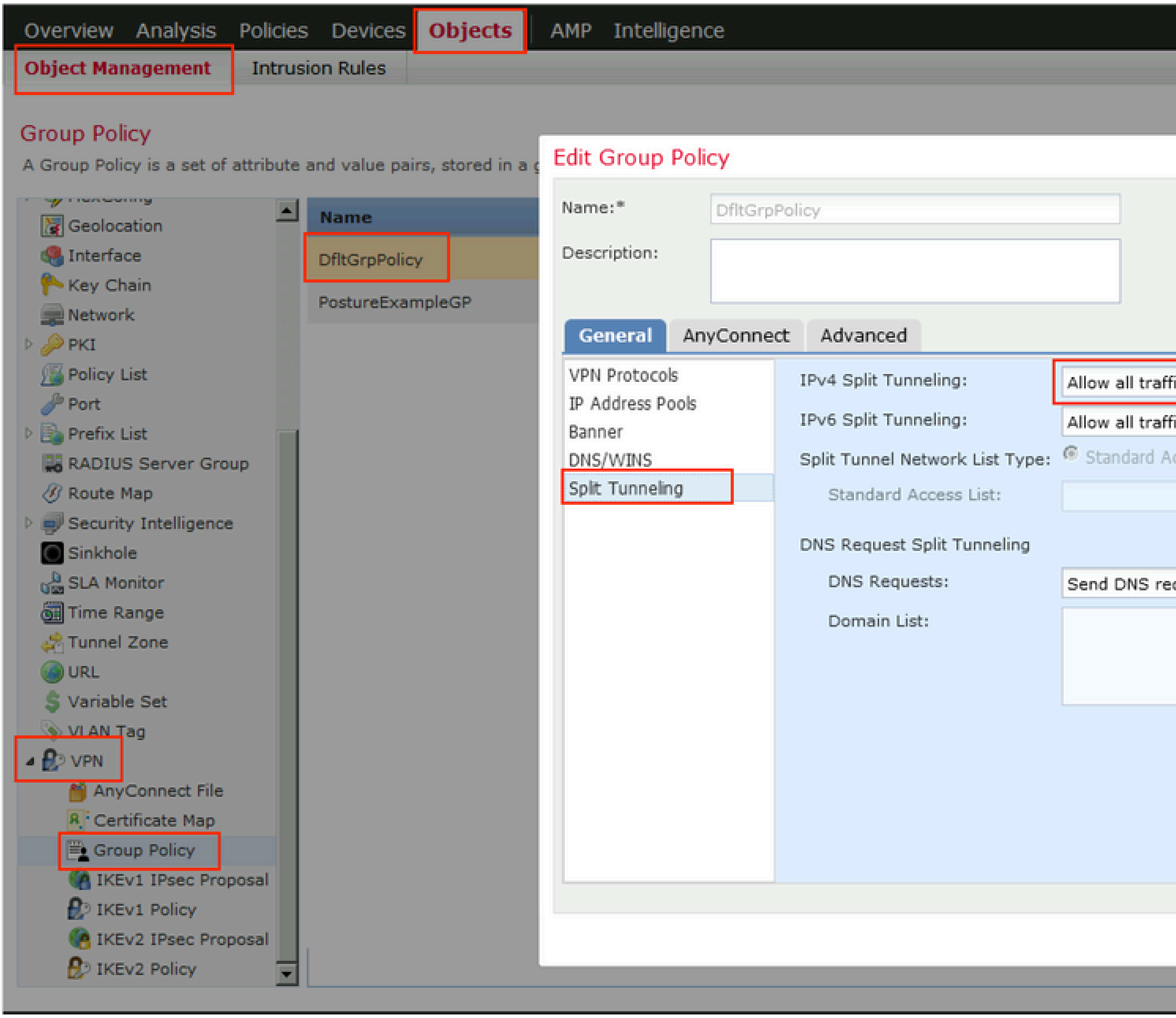
Een van de meest voorkomende problemen, wanneer er een spit tunnel is ingesteld. In dit voorbeeld wordt standaard groepsbeleid gebruikt, dat alle verkeer tunnelt. In het geval dat alleen het specifieke verkeer wordt getunneld, dan moeten AnyConnect-sondes (enroll.cisco.com en discovery host) door de tunnel gaan, naast het verkeer naar ISE en andere interne bronnen.

Om het tunnelbeleid op FMC te controleren, controleer eerst welk groepsbeleid wordt gebruikt voor VPN-verbinding. Navigeer naar **Apparaten > 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

Ga vervolgens naar **Objecten > Objectbeheer > VPN > Groepsbeleid** en klik op **Groepsbeleid** geconfigureerd voor 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:

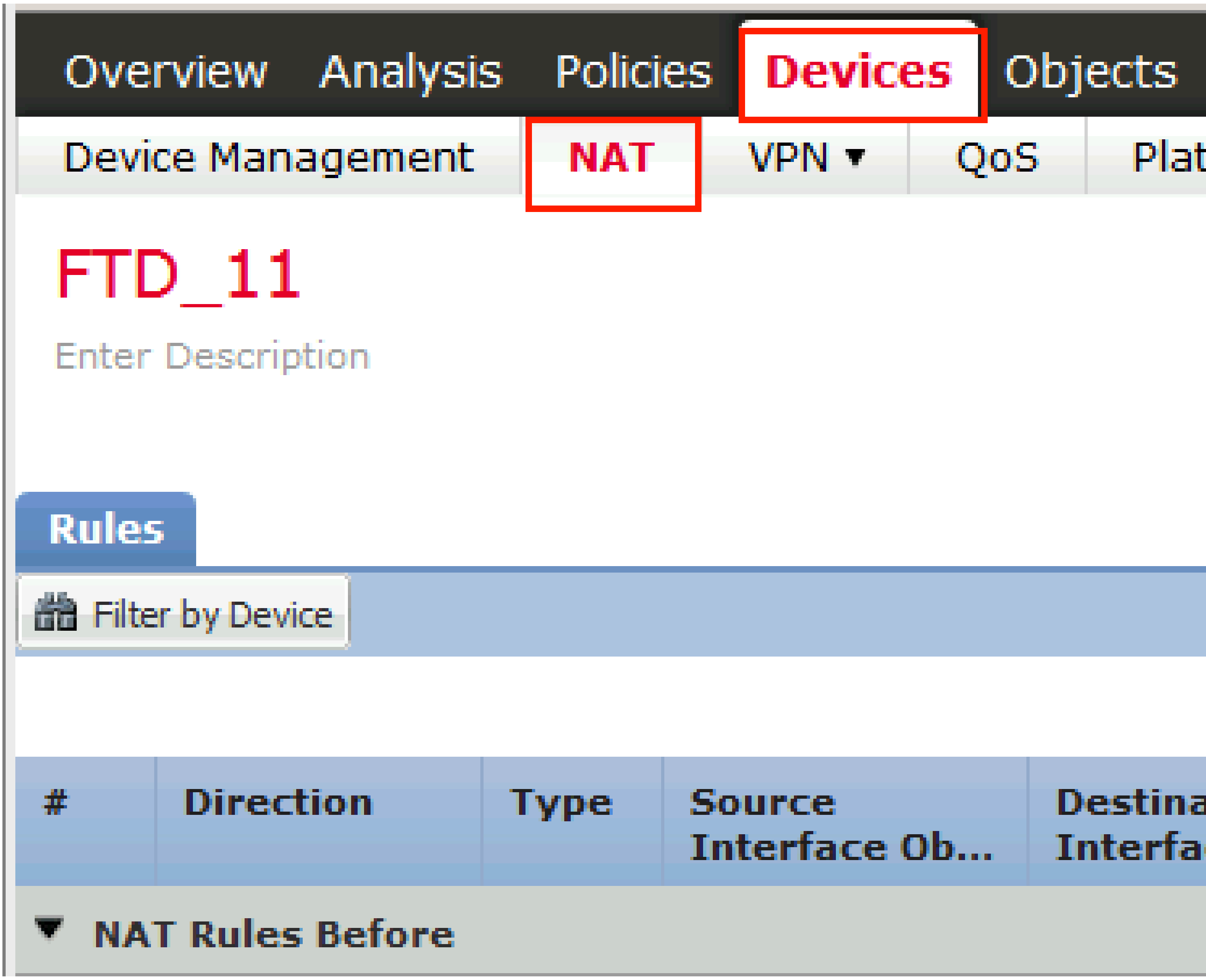
DNS Requests: Send DNS rec

Domain List:

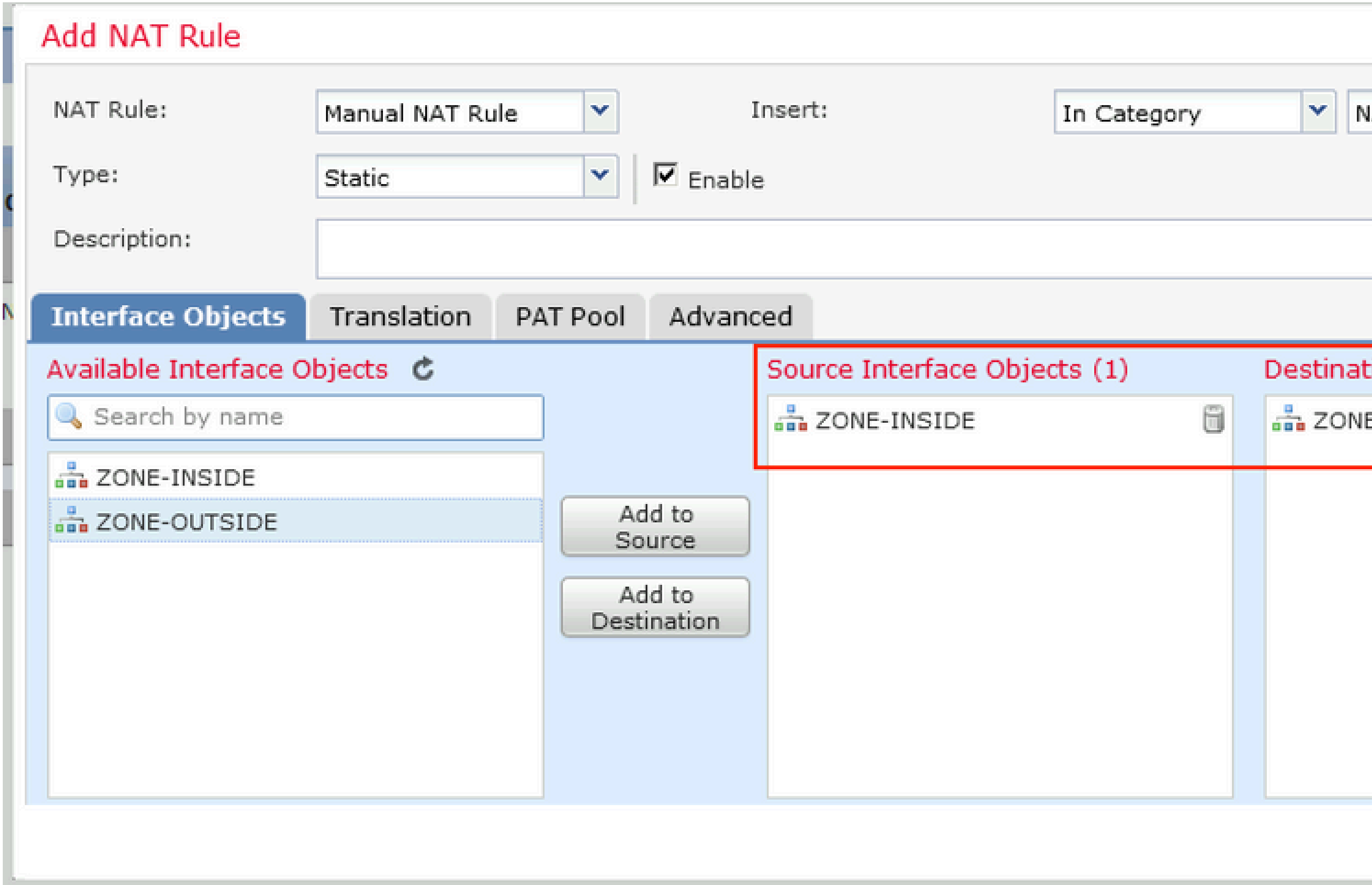
- Identity NAT

Een ander veelvoorkomend probleem is wanneer het retourverkeer van VPN-gebruikers wordt vertaald met het gebruik van een onjuiste NAT-ingang. Om dit probleem op te lossen, moet Identity NAT in een juiste volgorde worden gemaakt.

Controleer eerst NAT-regels voor dit apparaat. Navigeer naar **Apparaten** > **NAT** en klik vervolgens op **Regel toevoegen** om een nieuwe regel te maken.



Selecteer in het geopende venster op het tabblad **Interfaceobjecten de** optie **Beveiligingszones**. In dit voorbeeld, wordt de NAT ingang gemaakt van **streek-BINNENKANT** aan **streek-buitenkant**.



Add NAT Rule

NAT Rule: Manual NAT Rule

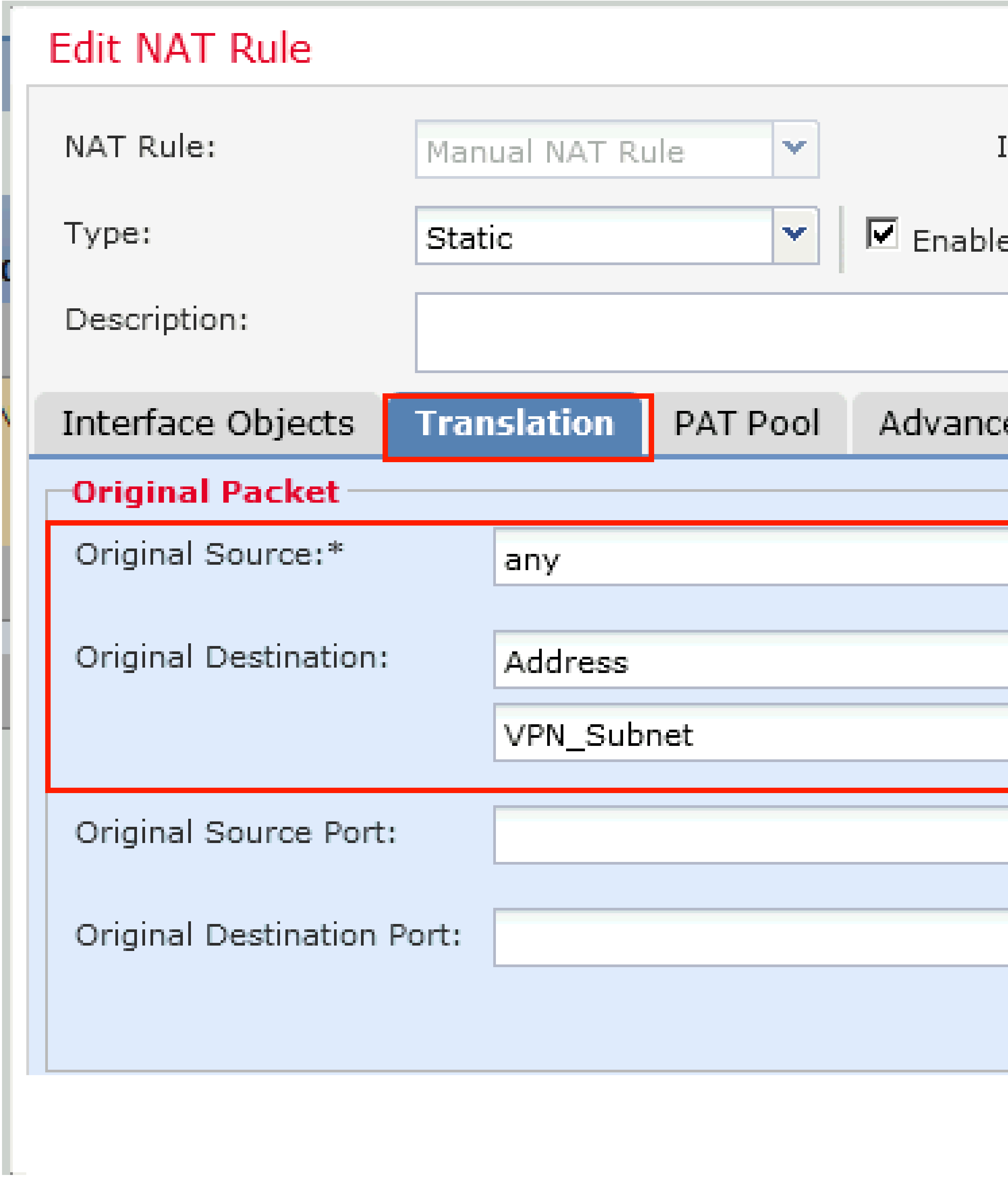
Insert: In Category

Type: Static

☑ Enable

Description:

Selecteer onder het tabblad **Vertaling** de optie oorspronkelijke en vertaalde pakketdetails. Aangezien het Identity NAT is, worden de bron en de bestemming onveranderd gehouden:



Edit NAT Rule

NAT Rule: Manual NAT Rule

Type: Static

☑ Enable

Description:

Original Packet

Original Source:* any

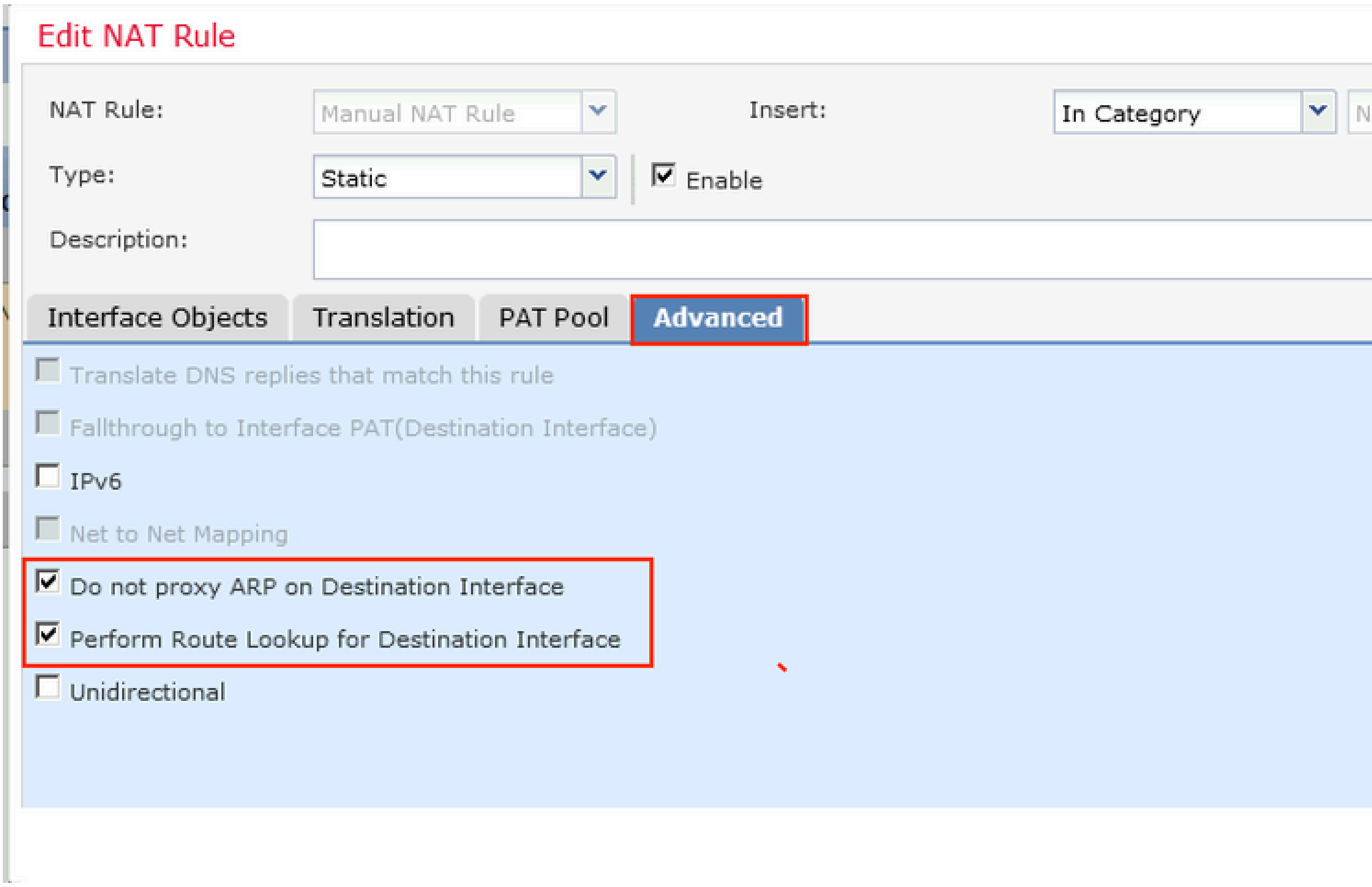
Original Destination: Address

VPN_Subnet

Original Source Port:

Original Destination Port:

Schakel in het tabblad **Geavanceerd** de selectievakjes in zoals in deze afbeelding:



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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.