Configure ISE Posture over AnyConnect Remote Access VPN on FTD

Contents

Introduction

This document describes how to configure Firepower Threat Defense (FTD) version 6.4.0 to posture VPN users against Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- AnyConnect Remote Access VPN
- Remote Access VPN configuration on the FTD
- Identity Services Engine and posture services

Components Used

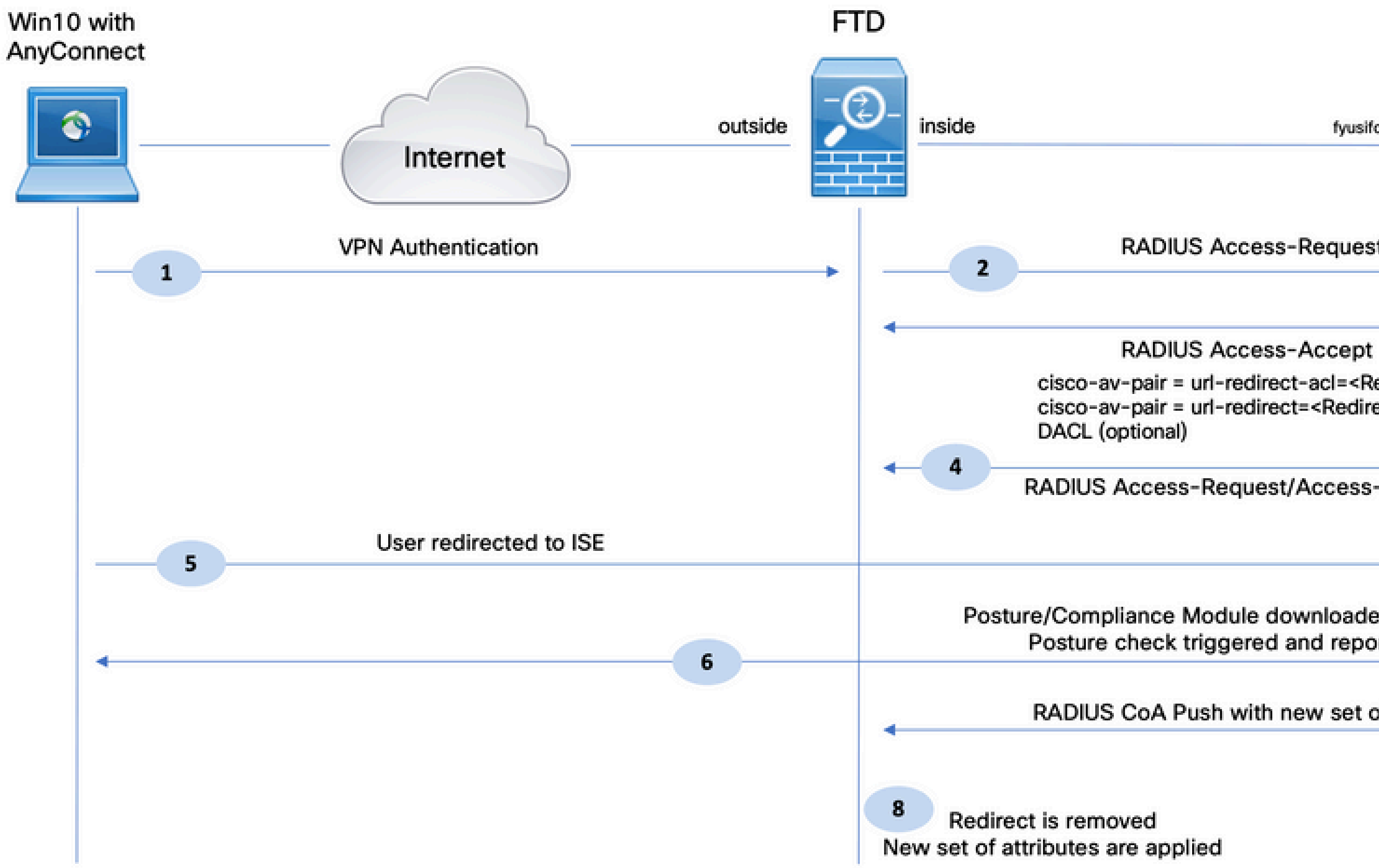
The information in this document is based on these software versions:

- Cisco Firepower Threat Defense (FTD) software versions 6.4.0
- Cisco Firepower Management Console (FMC) software version 6.5.0
- Microsoft Windows 10 with Cisco AnyConnect Secure Mobility Client Version 4.7
- Cisco Identity Services Engine (ISE) version 2.6 with Patch 3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram and Traffic Flow


Win10 with AnyConnect
Internet
outside
FTD
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. The remote user uses Cisco Anyconnect for VPN access to the FTD.

2. The FTD sends a RADIUS Access-Request for that user to the ISE.

3. That request hits the policy named **FTD-VPN-Posture-Unknown** on the ISE. The ISE sends a RADIUS Access-Accept with three attributes:

- **cisco-av-pair = url-redirect-acl=fyusifovredirect** - This is the Access Control List (ACL) name that is defined locally on the FTD, which decides the traffic that is redirected.
- **cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp** - This is the URL to which the remote user is redirected.
- **DACL = PERMIT_ALL_IPV4_TRAFFIC** - downloadable ACL Tthis attribute is optional. In this scenario, all traffic is permitted in DACL)

4. If DACL is sent, RADIUS Access-Request/Access-Accept is exchanged in order to download content of the DACL

5. When the traffic from the VPN user matches the locally-defined ACL, it is redirected to ISE Client Provisioning Portal. ISE provisions AnyConnect Posture Module and Compliance Module.

6. After the agent is installed on the client machine, it automatically searches for ISE with probes. When ISE is detected successfully, posture requirements are checked on the endpoint. In this example, the agent checks for any installed anti-malware software. Then it sends a posture report to the ISE.

7. When ISE receives the posture report from the agent, ISE changes Posture Status for this session and triggers RADIUS CoA type Push with new attributes. This time, the posture status is known and another rule is hit.

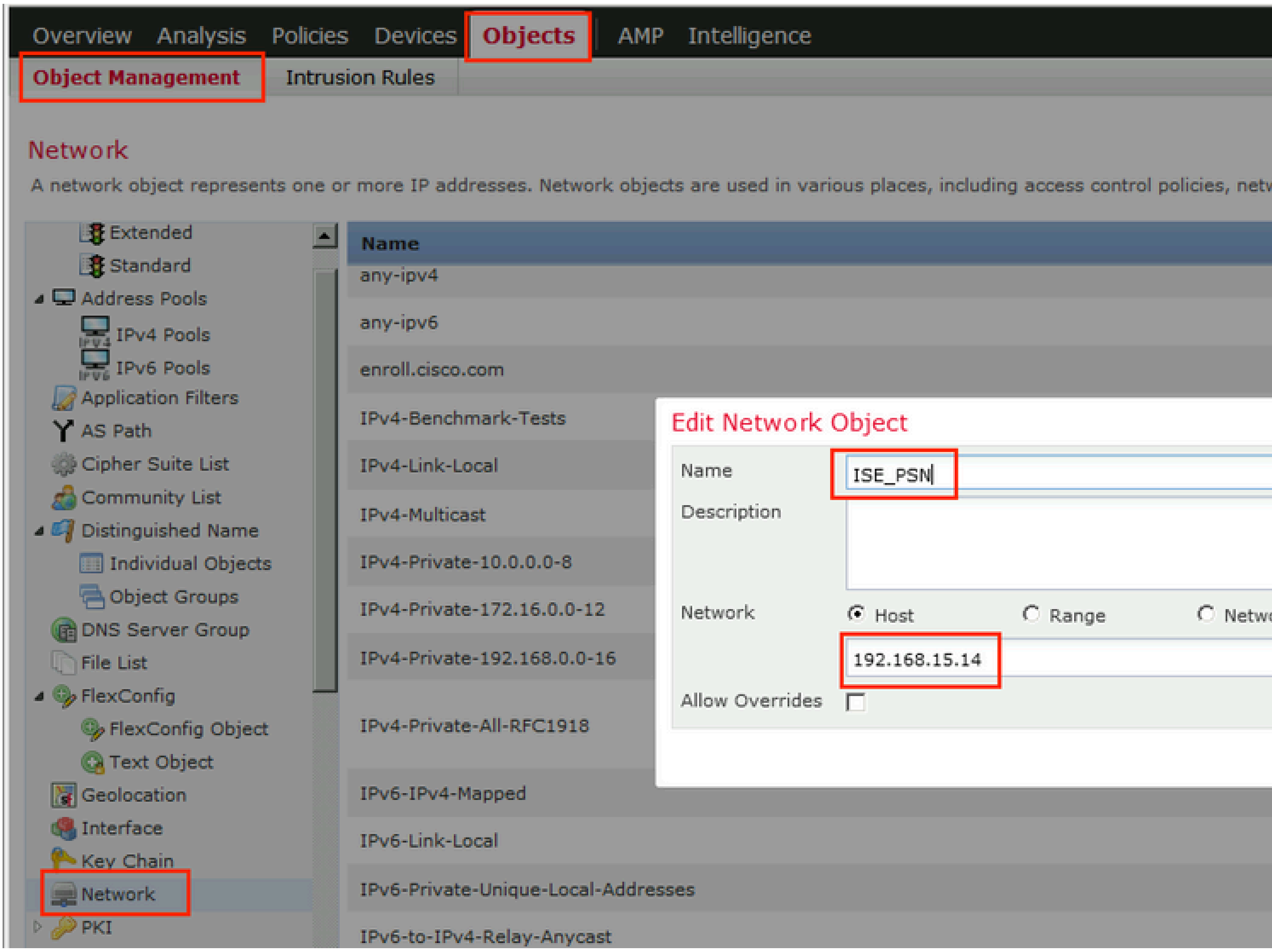
- If the user is compliant, then a DACL name that permits full access is sent.
- If the user is non-compliant, then a DACL name that permits limited access is sent.

8. The FTD removes the redirection. FTD sends Access-Request in order to download DACL from the ISE. The specific DACL is attached to the VPN session.

Configurations

FTD/FMC

Step 1. Create Network Object Group for ISE and Remediation Servers (if any). Navigate to **Objects > Object Management > Network**.



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

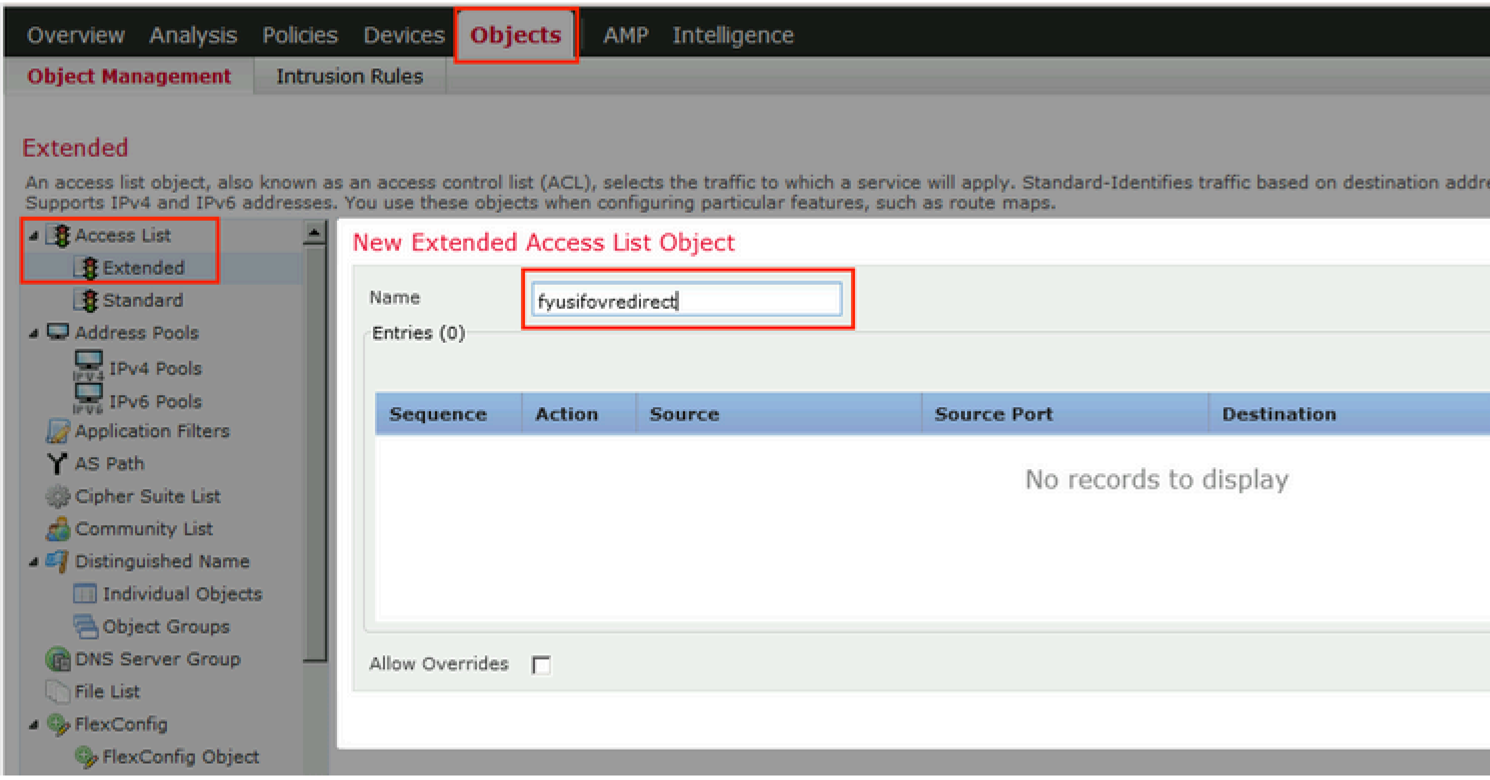
Description:

Network: ● Host ○ Range ○ Netw

192.168.15.14

Allow Overrides □

Step 2. Create Redirect ACL. Navigate to **Objects > Object Management > Access List > Extended**. Click **Add Extended Access List** and provide the name of Redirect ACL. This name must be the same as in the ISE authorization result.



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

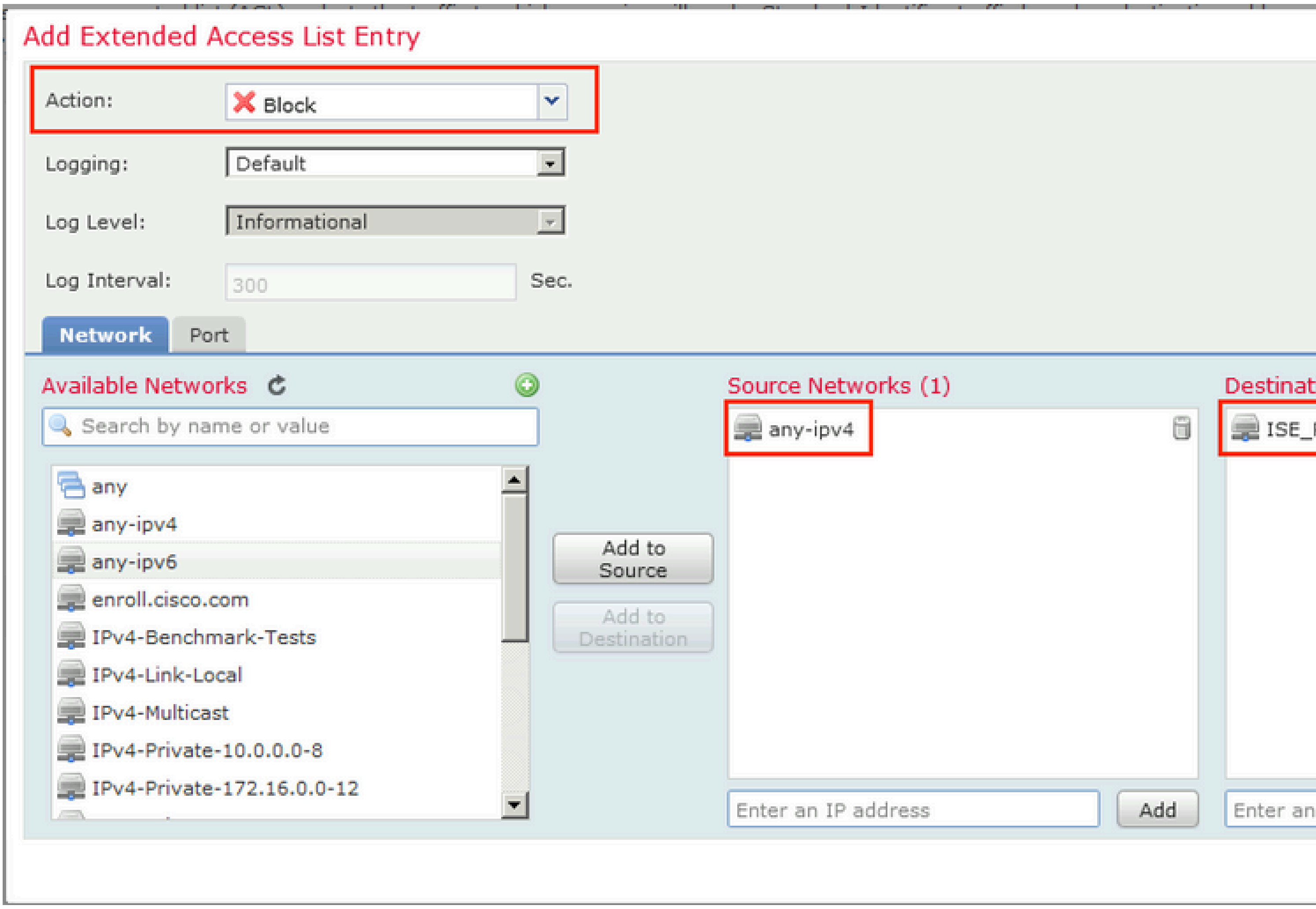
Entries (0)

Sequence	Action	Source	Source Port	Destination

No records to display

Allow Overrides □

Step 3. Add Redirect ACL Entries. Click the **Add** button. Block traffic to DNS, ISE, and to the remediation servers to exclude them from redirection. Allow the rest of the traffic, this triggers redirection (ACL entries could be more specific if needed).



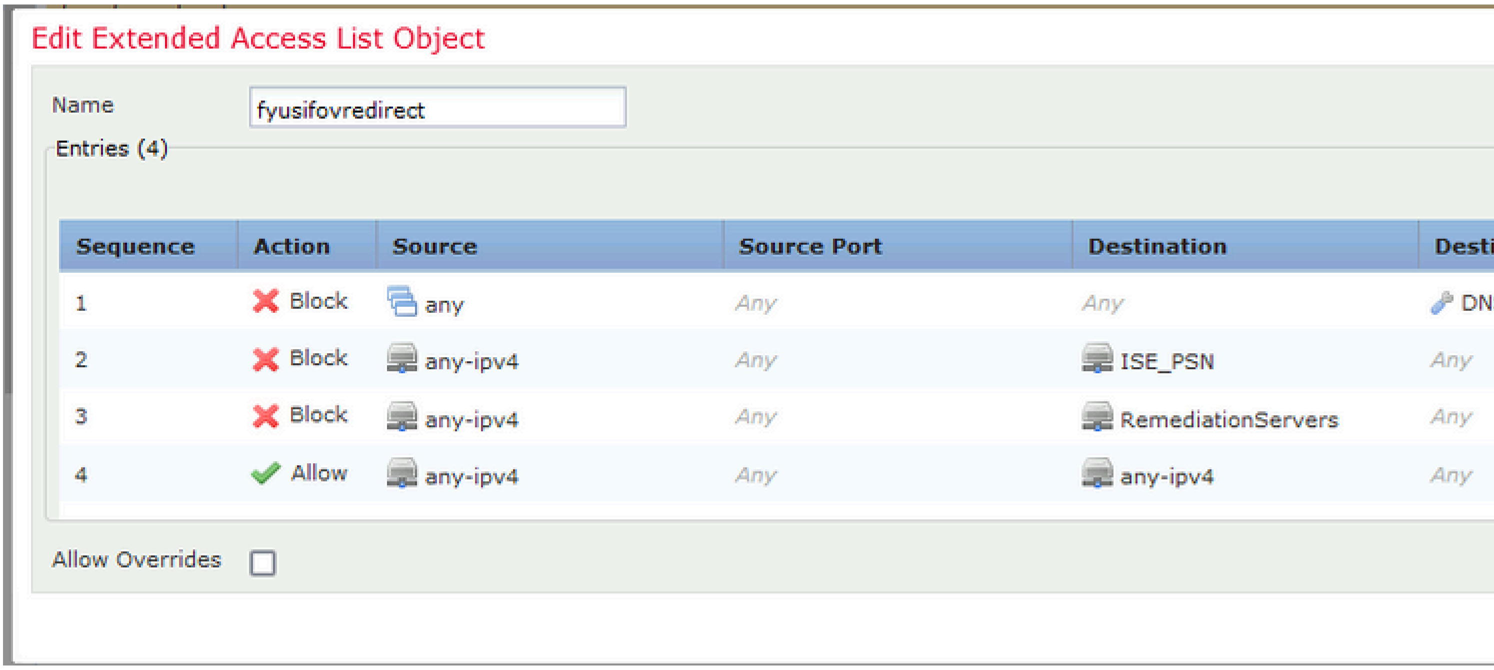
Add Extended Access List Entry

Action: Block

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.



Edit Extended Access List Object

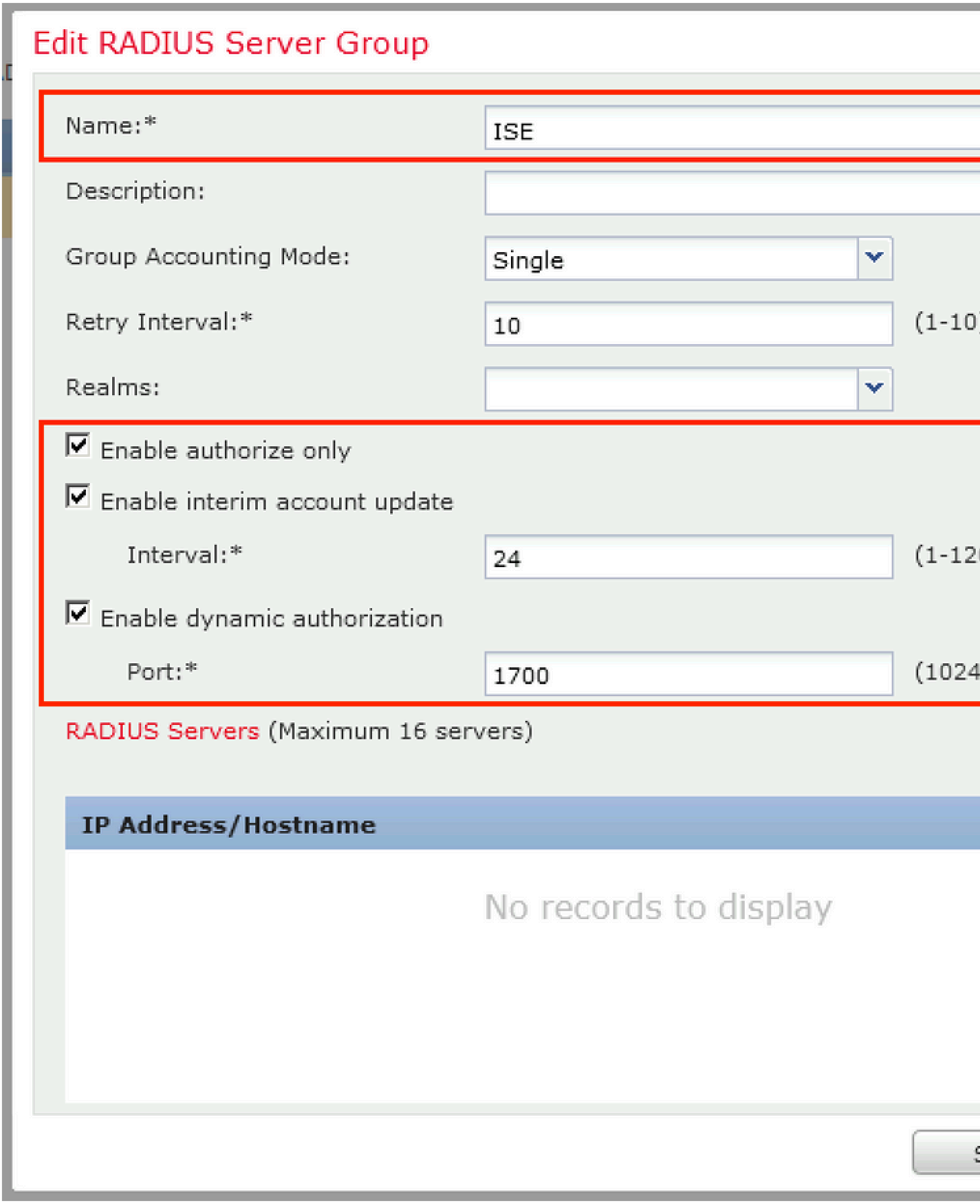
Name: fyusifovredirect

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 □

Step 4. Add ISE PSN node/nodes. Navigate to **Objects** > **Object Management** > **RADIUS Server Group**. Click **Add RADIUS Server Group**, then provide name, enable check all checkboxes and click the **plus** icon.



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

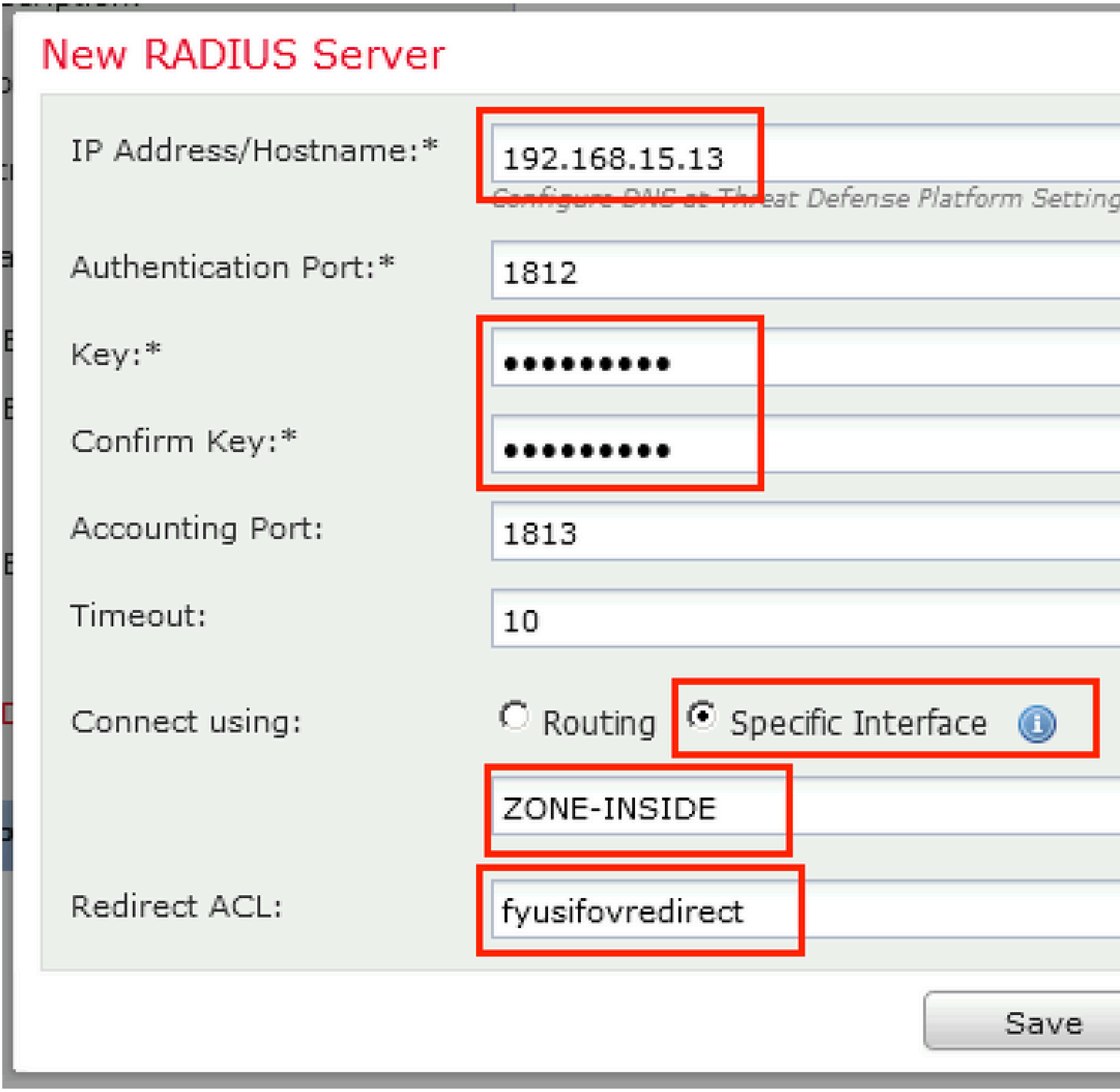
☑ Enable dynamic authorization

Port:* 1700 (1024

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

Step 5. In the opened window, provide ISE PSN IP address, RADIUS Key, select **Specific Interface** and select interface from which ISE is reachable (this interface is used as a source of RADIUS traffic) then select **Redirect ACL** which was configured previously.



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

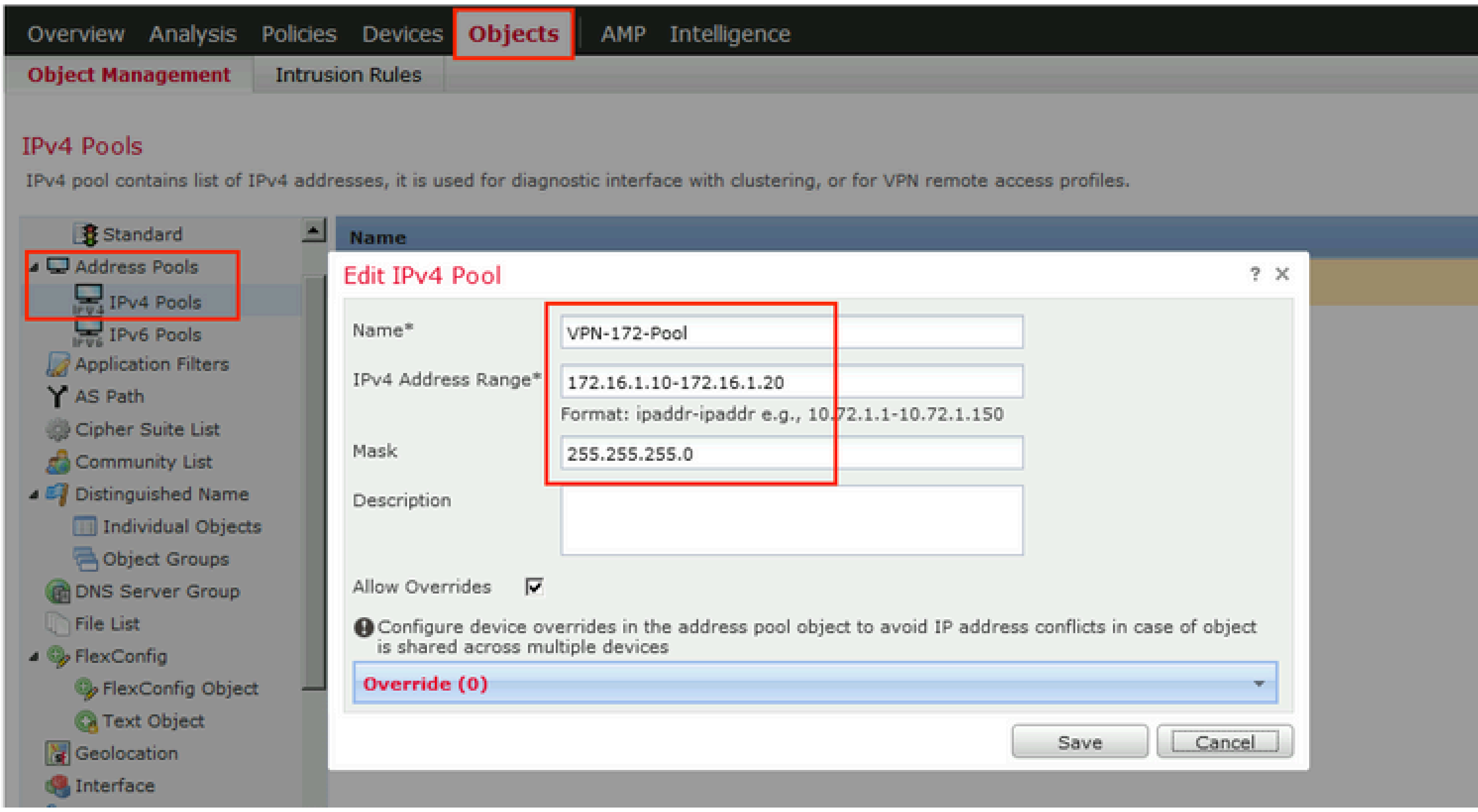
Timeout: 10

Connect using: ○ Routing ● Specific Interface

ZONE-INSIDE

Redirect ACL: fyusifovredirect

Step 6. Create Address Pool for VPN users. Navigate to **Objects > Object Management > Address Pools > IPv4 Pools**. Click **Add IPv4 Pools** and fill the in details.



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

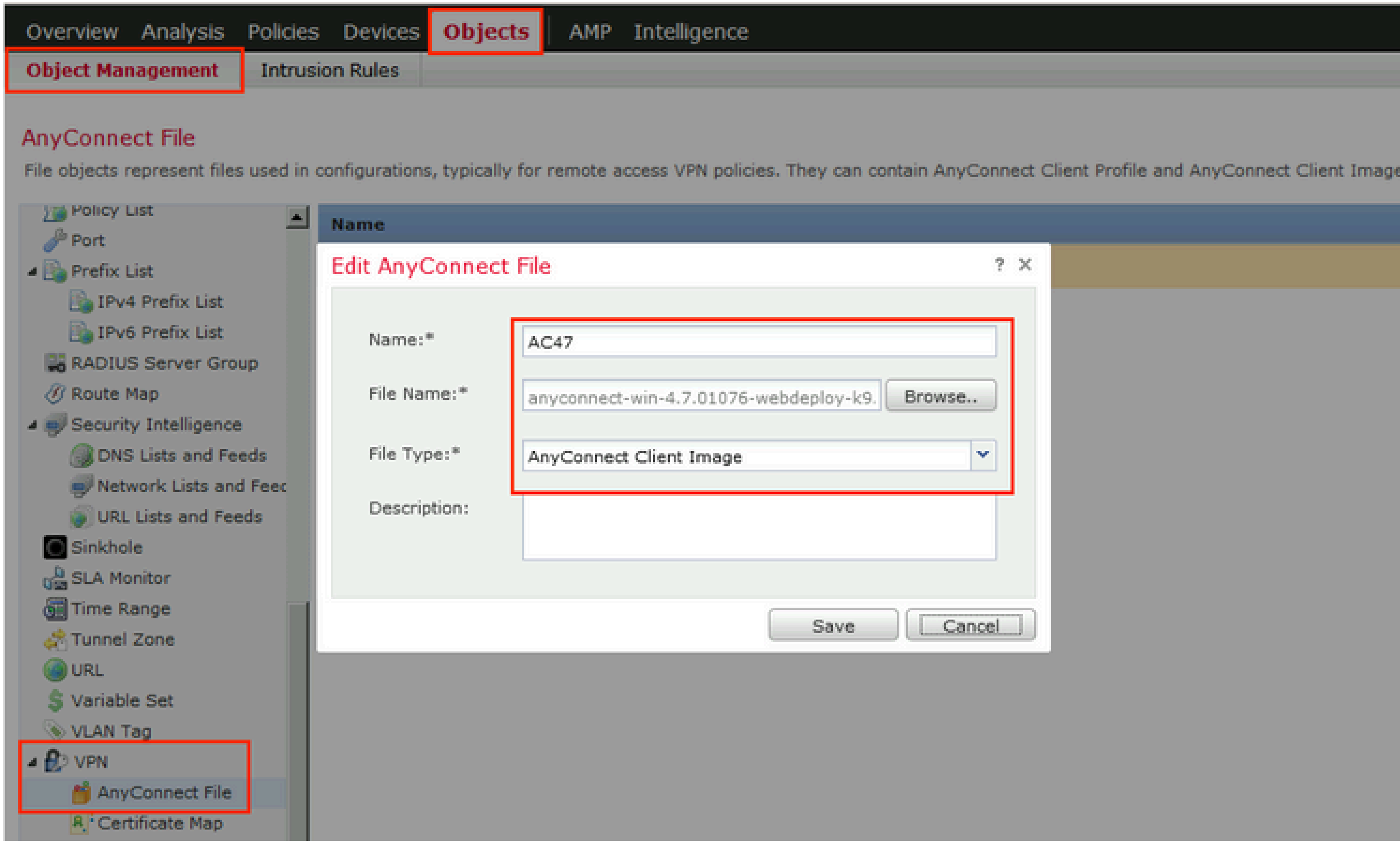
Mask 255.255.255.0

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

Step 7. Create AnyConnect package. Navigate to **Objects** > **Object Management** > **VPN** > **AnyConnect File**. Click **Add AnyConnect File**, provide the package name, download the package from Cisco Software Download and select **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

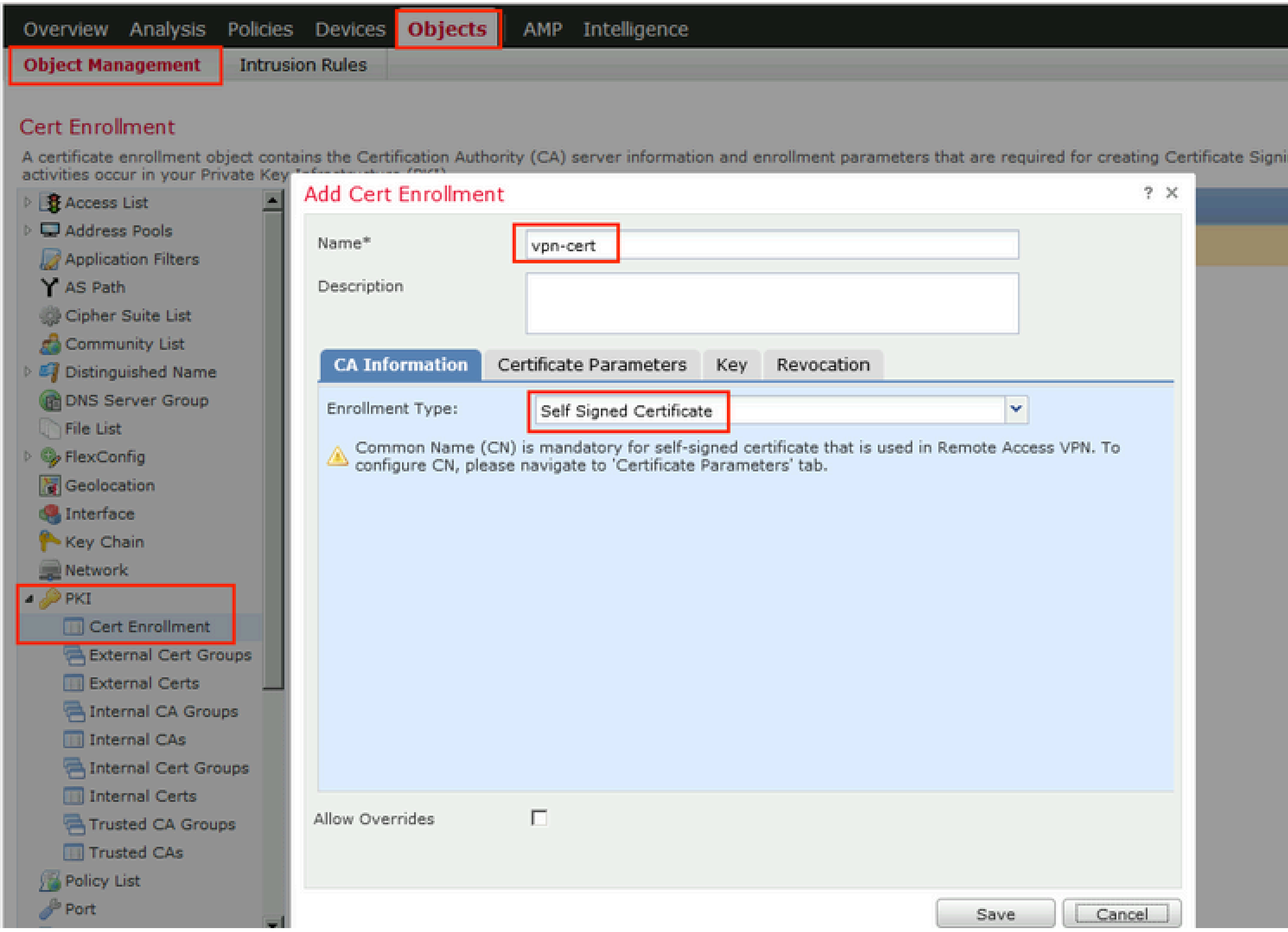
Name:* AC47

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

File Type:* AnyConnect Client Image

Description:

Step 8. Navigate to **Certificate Objects > Object Management > PKI > Cert Enrollment**. Click **Add Cert Enrollment**, provide name, choose **Self Signed Certificate** in Enrollment Type. Click the Certificate Parameters tab and provide CN.



Cert Enrollment

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

Add Cert Enrollment

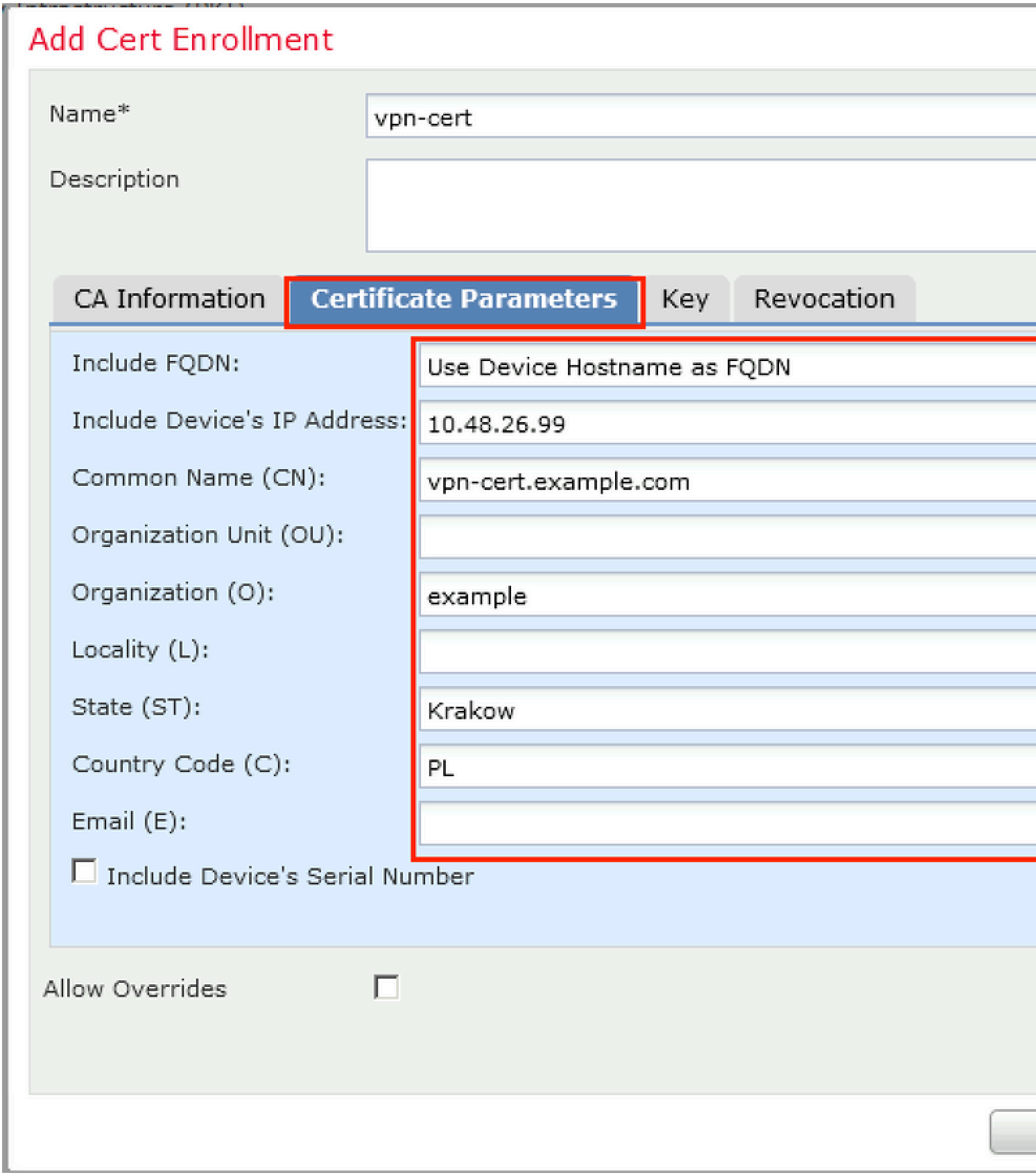
Name* vpn-cert

Description

Enrollment Type: Self Signed Certificate

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

Allow Overrides □



Add Cert Enrollment

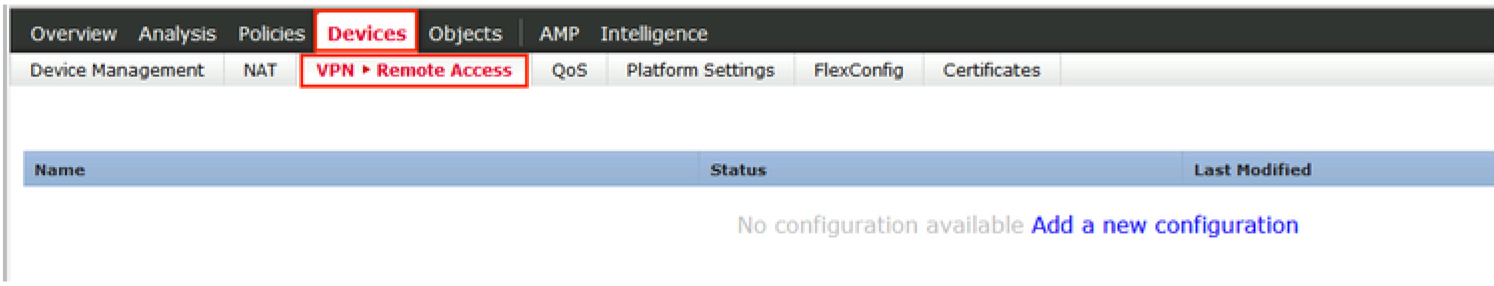
Name*	vpn-cert
Description	

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

□ Include Device's Serial Number

Allow Overrides □

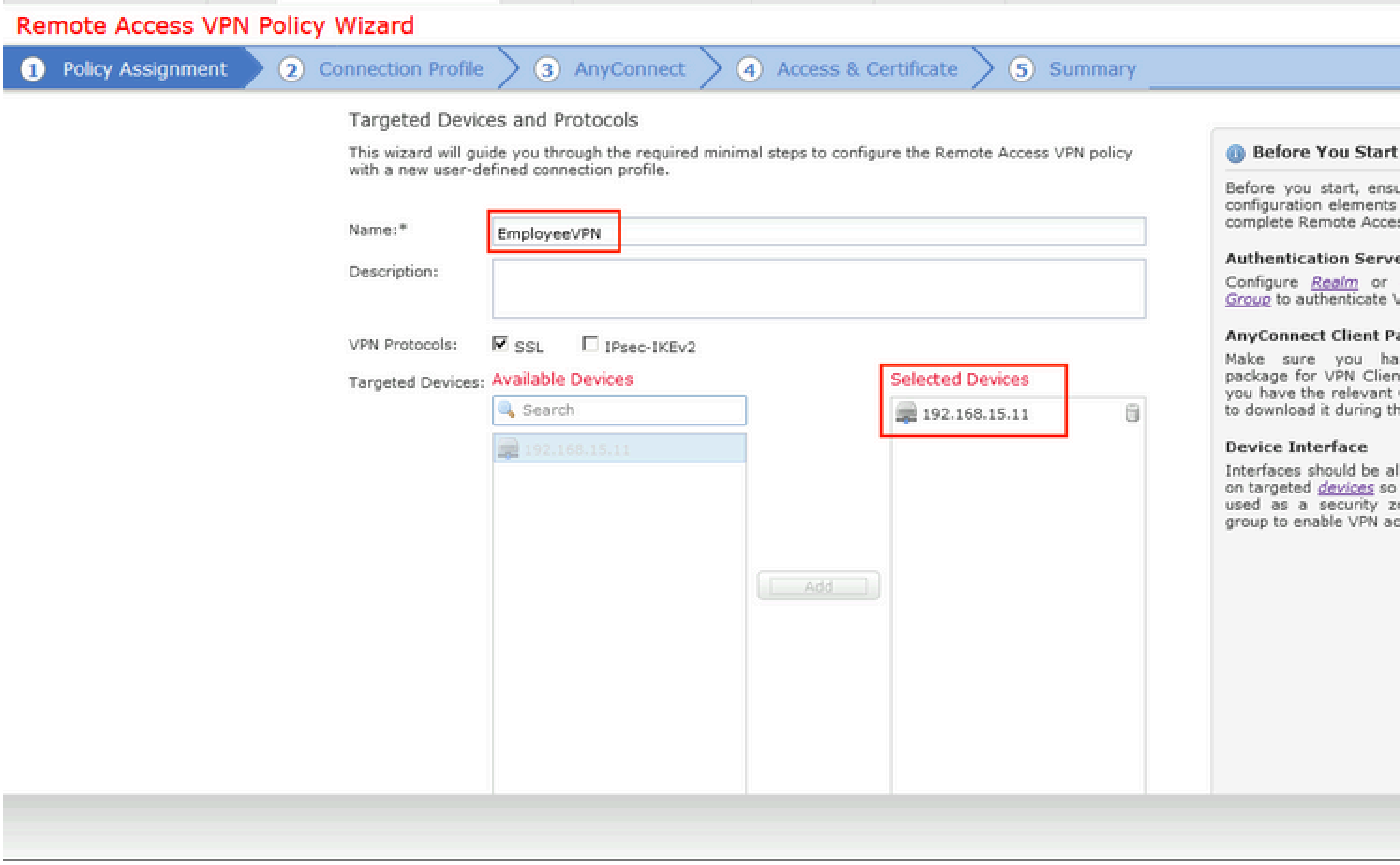
Step 9. Launch Remote Access VPN wizard. Navigate to **Devices** > **VPN** > **Remote Access** and click **Add**.



Name	Status	Last Modified

No configuration available Add a new configuration

Step 10. Provide the name, check SSL as VPN Protocol, choose FTD which is used as VPN concentrator and click **Next**.



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

Selected Devices

192.168.15.11

Before You Start

Before you start, ensu configuration elements complete Remote Acce

Authentication Serve

Configure Realm or Group to authenticate V

AnyConnect Client Pa

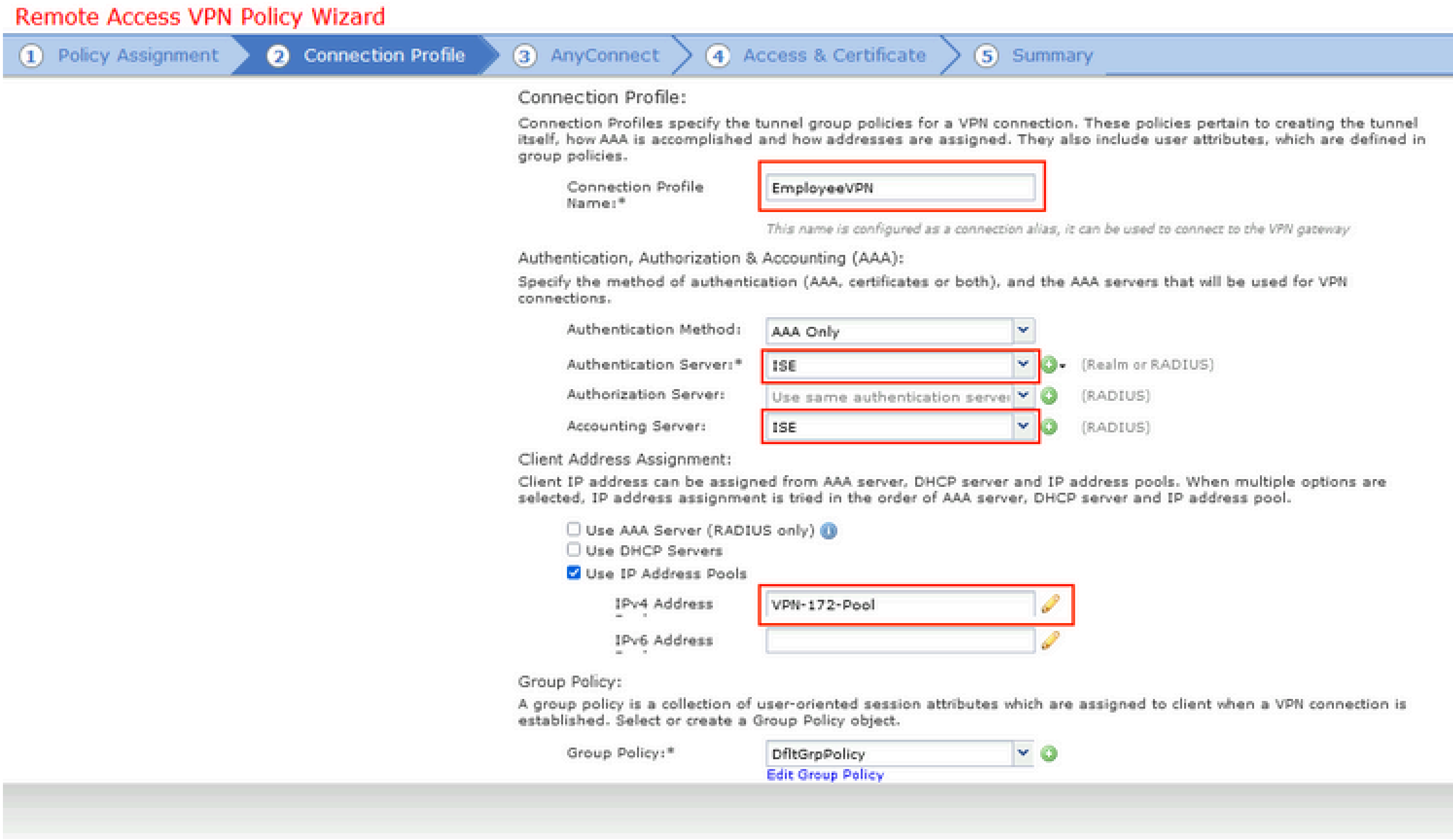
Make sure you ha package for VPN Clien you have the relevant to download it during th

Device Interface

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

Step 11. Provide **Connection Profile** name, select **Authentication/Accounting Servers**, select the address pool which was configured previously and click **Next**.

Note: Do not select the authorization server. It triggers two Access Requests for a single user (once with the user password and the second time with password *cisco*).



Connection Profile:

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

Connection Profile Name:* EmployeeVPN

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

Authentication, Authorization & Accounting (AAA):

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

Authentication Method: AAA Only

Authentication Server:* ISE (Realm or RADIUS)

Authorization Server: Use same authentication server (RADIUS)

Accounting Server: ISE (RADIUS)

Client Address Assignment:

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

☐ Use AAA Server (RADIUS only)

☐ Use DHCP Servers

☑ Use IP Address Pools

IPv4 Address Pools: VPN-172-Pool

IPv6 Address Pools:

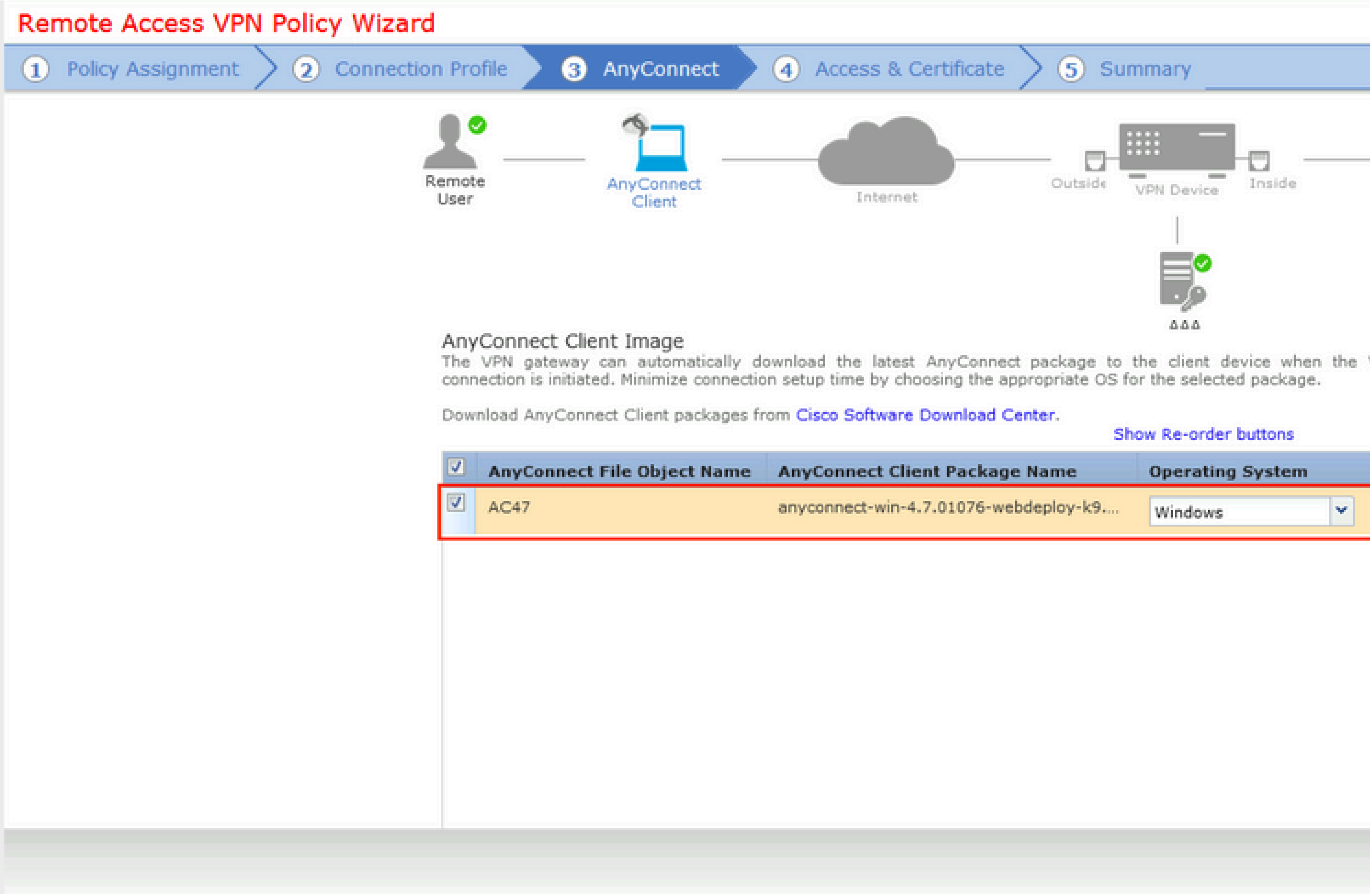
Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* DfltGrpPolicy

Edit Group Policy

Step 12. Select AnyConnect package that was configured previously and click **Next**.



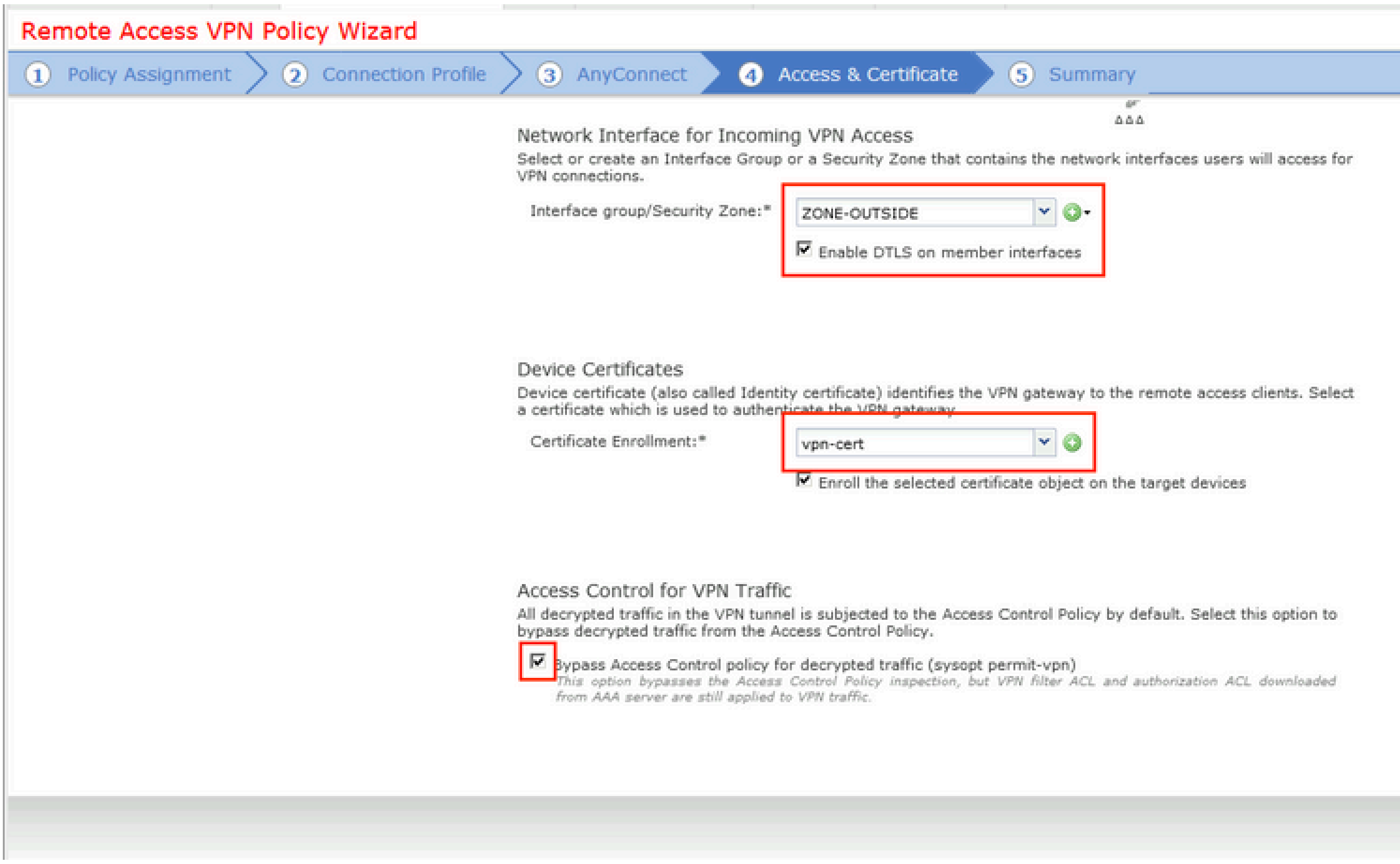
AnyConnect Client Image

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

Download AnyConnect Client packages from Cisco Software Download Center.

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

Step 13. Select interface from which VPN traffic is expected, select **Certificate Enrollment** that was configured previously and click **Next**.



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

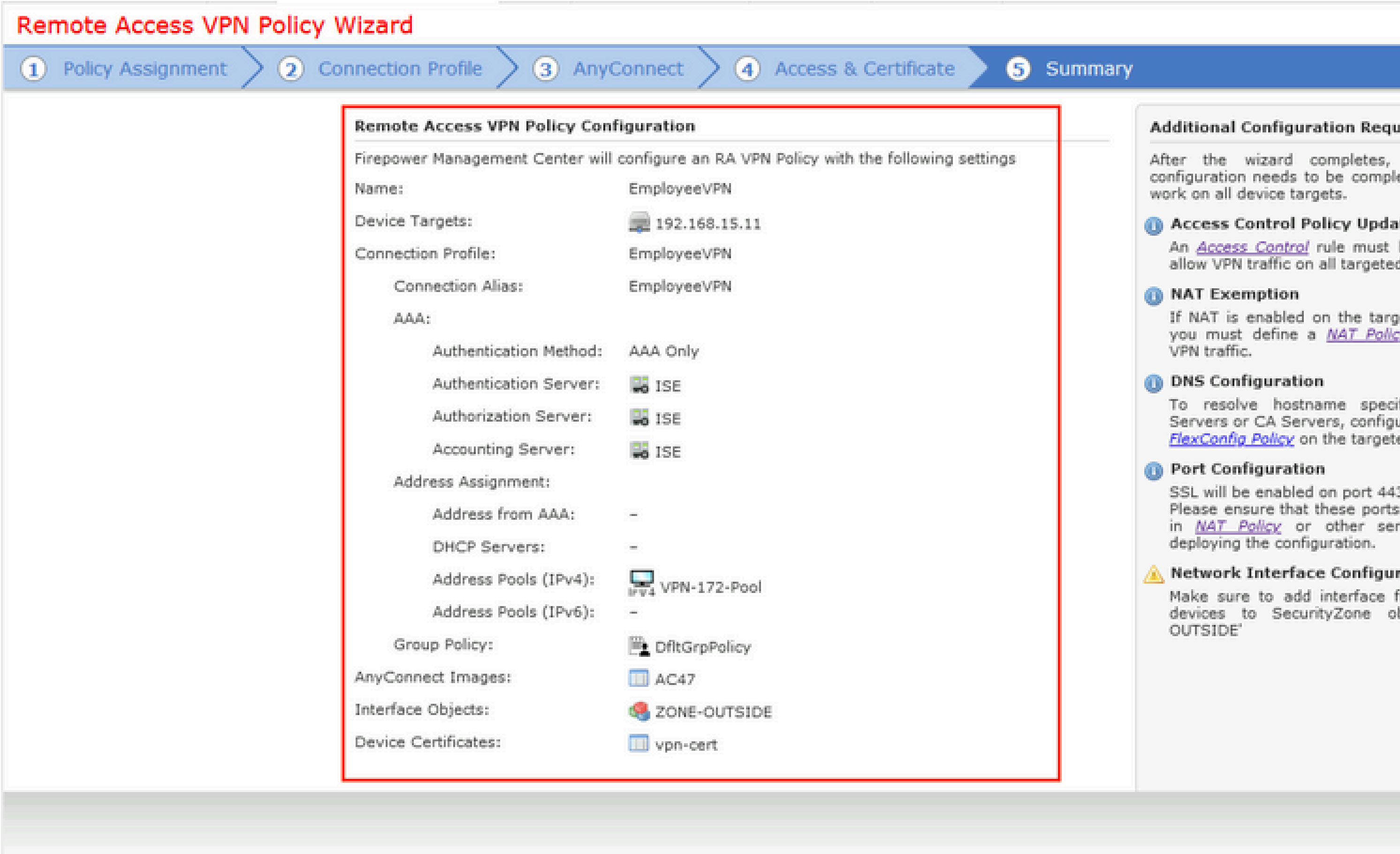
Access Control for VPN Traffic

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.

Step 14. Check the summary page and click **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

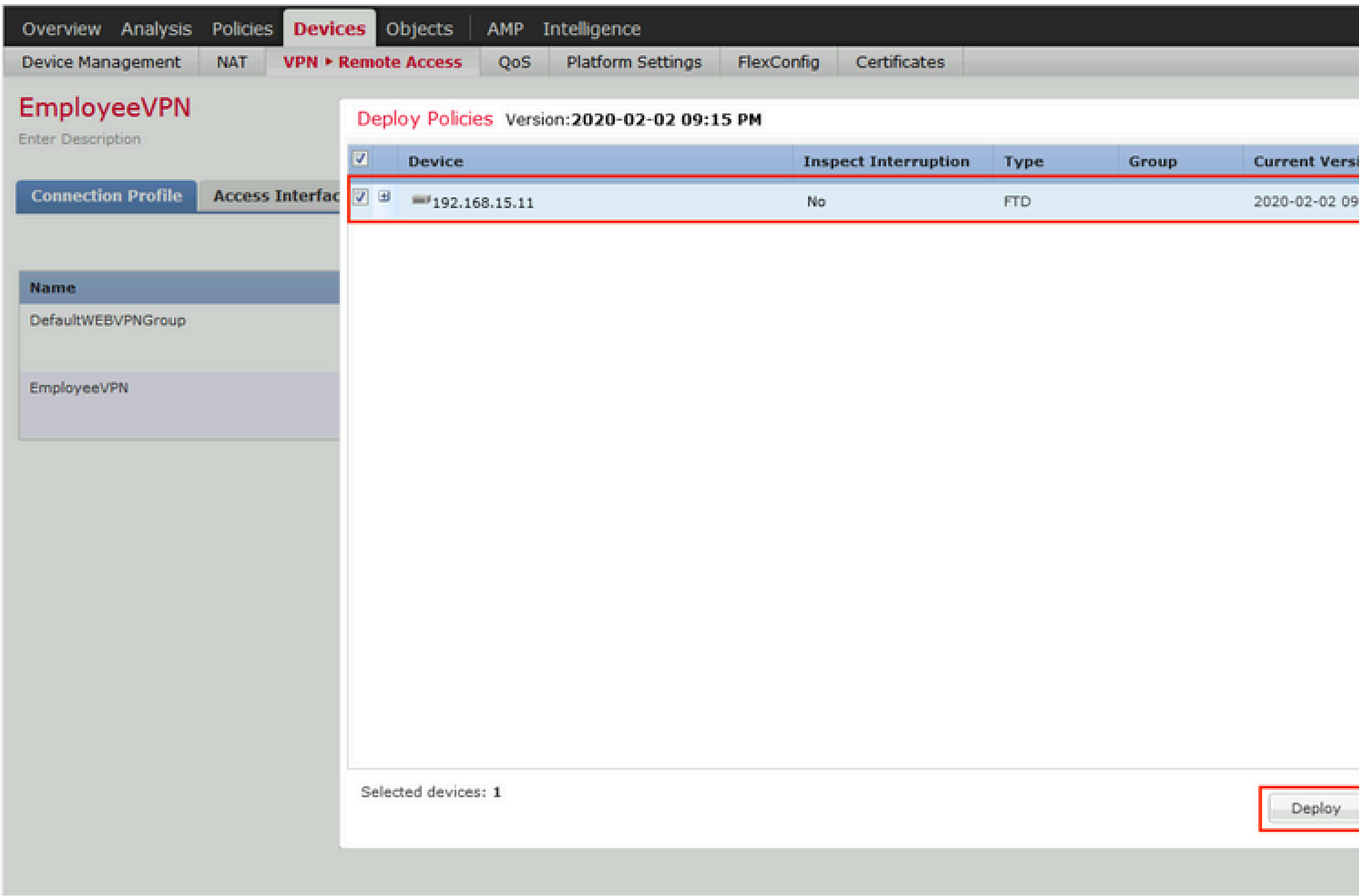
Port Configuration

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'

Step 15. Deploy configuration to FTD. Click **Deploy** and select **FTD** that is used as a VPN concentrator.



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

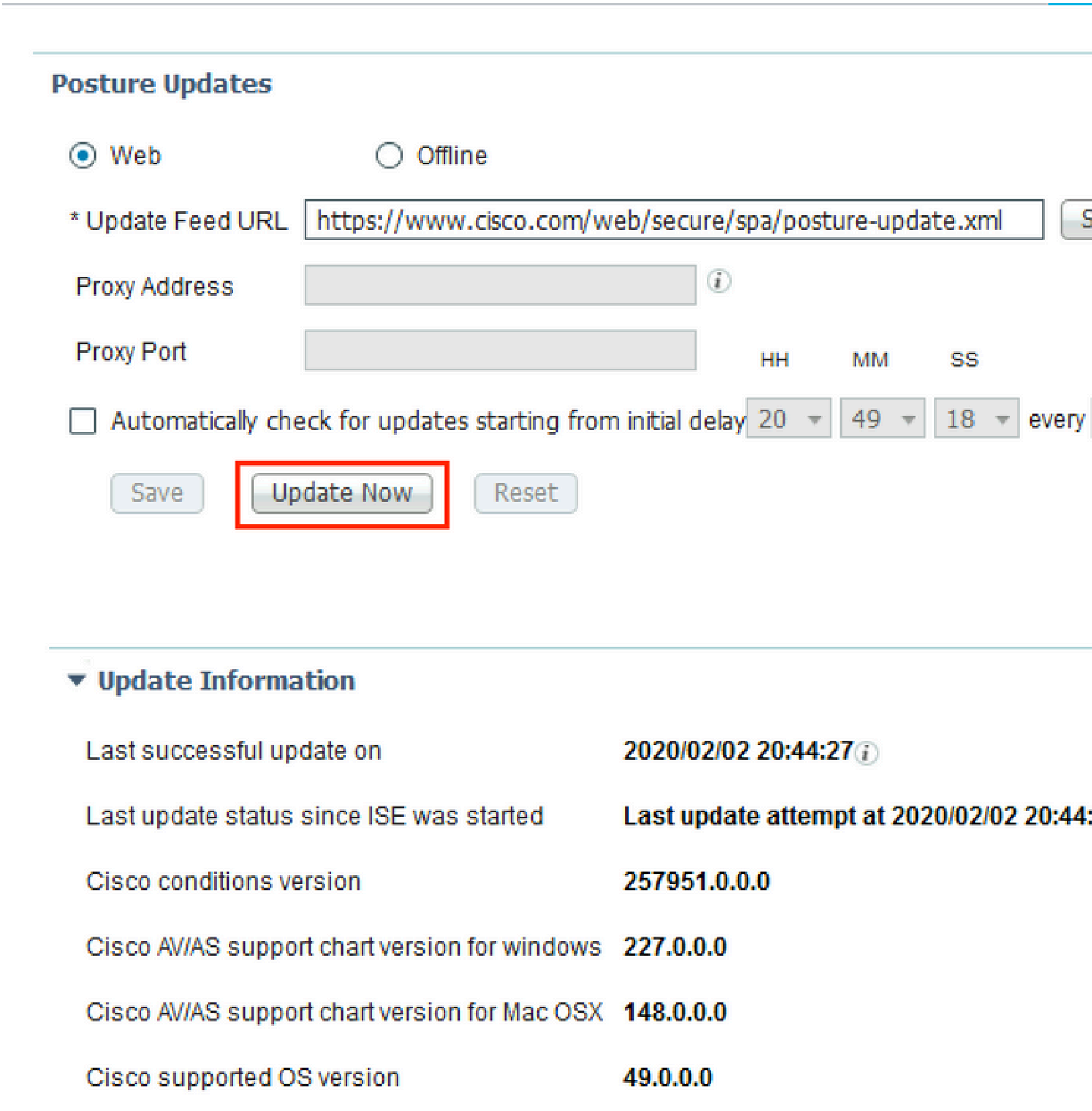
		Device	Inspect Interruption	Type	Group	Current Versi
☑	⊞	192.168.15.11	No	FTD		2020-02-02 09

Name
DefaultWEBVPNGroup
EmployeeVPN

Selected devices: 1

ISE

Step 1. Run Posture Updates. Navigate to **Administration** > **System** > **Settings** > **Posture** > **Updates**.



Posture Updates

● Web ○ Offline

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

Proxy Address:

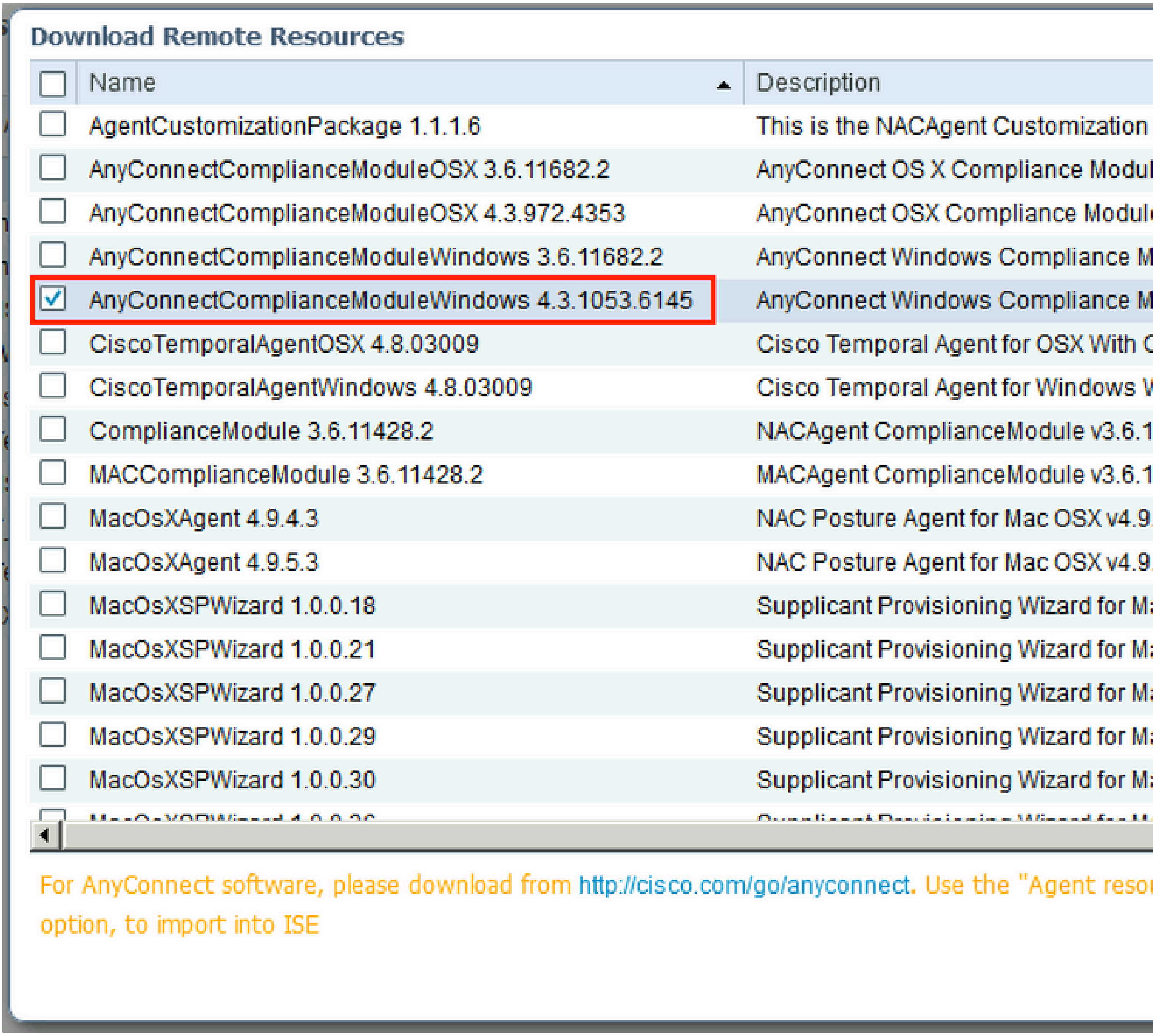
Proxy Port:

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

Update Information

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

Step 2. Upload Compliance Module. Navigate to **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**. Click **Add** and select **Agent resources from Cisco site**



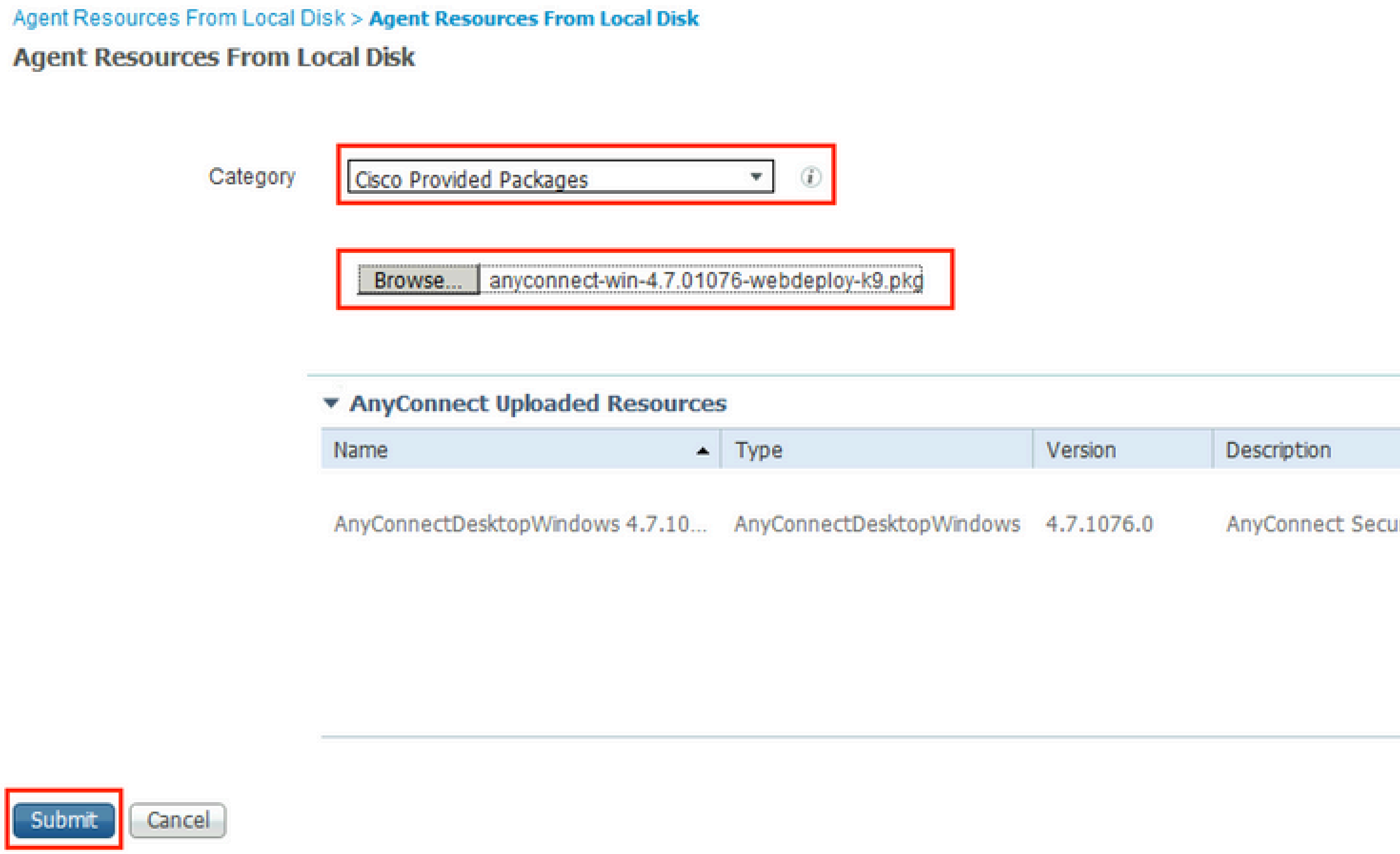
Download Remote Resources

□	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 V
□	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

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

Step 3. Download AnyConnect from Cisco Software Download, then upload it to ISE. Navigate to **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Click **Add** and select **Agent Resources From Local Disk**. Choose **Cisco Provided Packages** under **Category**, select AnyConnect package from local disk and click **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

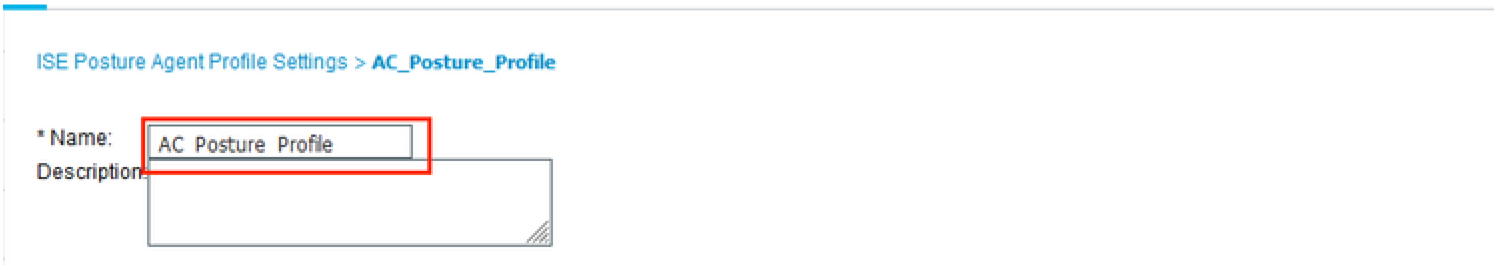
AnyConnect Uploaded Resources

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

Step 4. Create AnyConnect Posture Profile. Navigate to **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Click **Add** and select **AnyConnect Posture Profile**. Fill in the name and Posture Protocol.

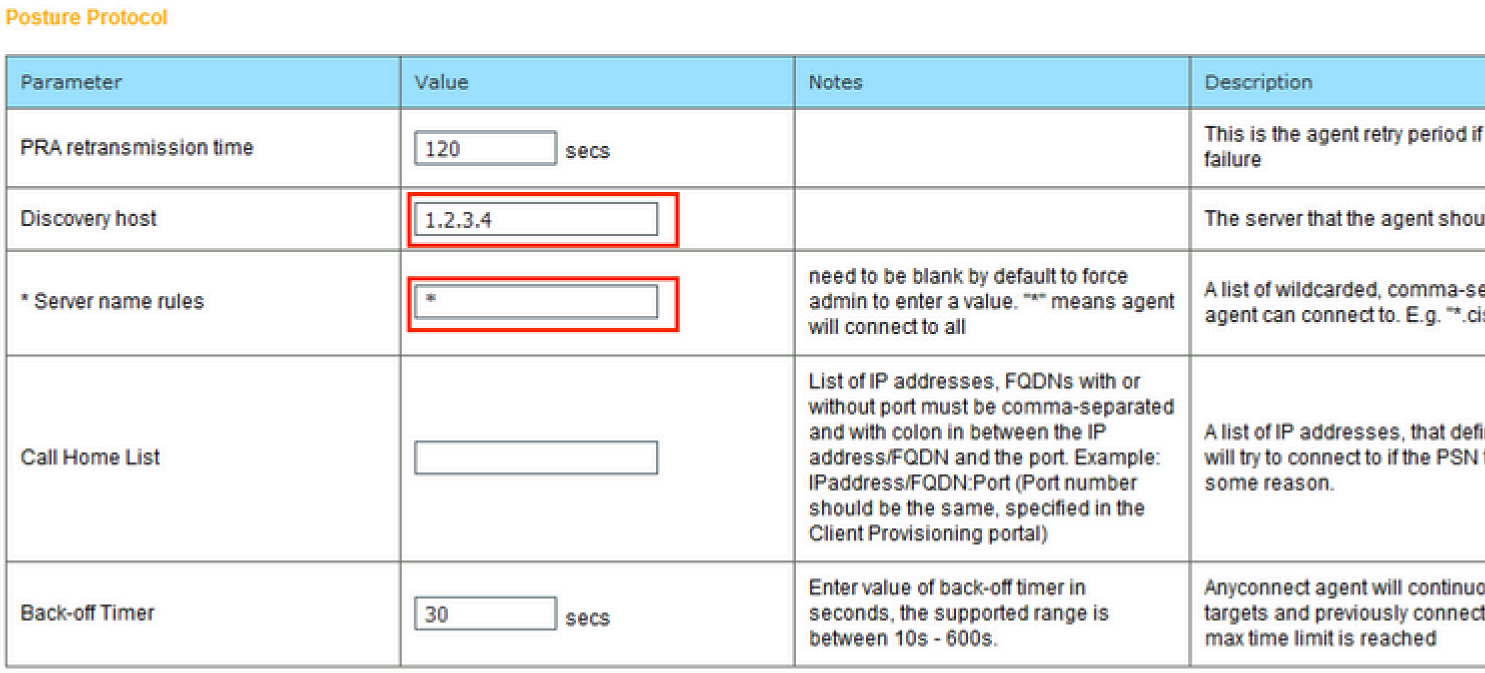
Under ***Server name rules** put ***** and put any dummy IP address under **Discovery host**.



ISE Posture Agent Profile Settings > AC_Posture_Profile

* Name: AC Posture Profile

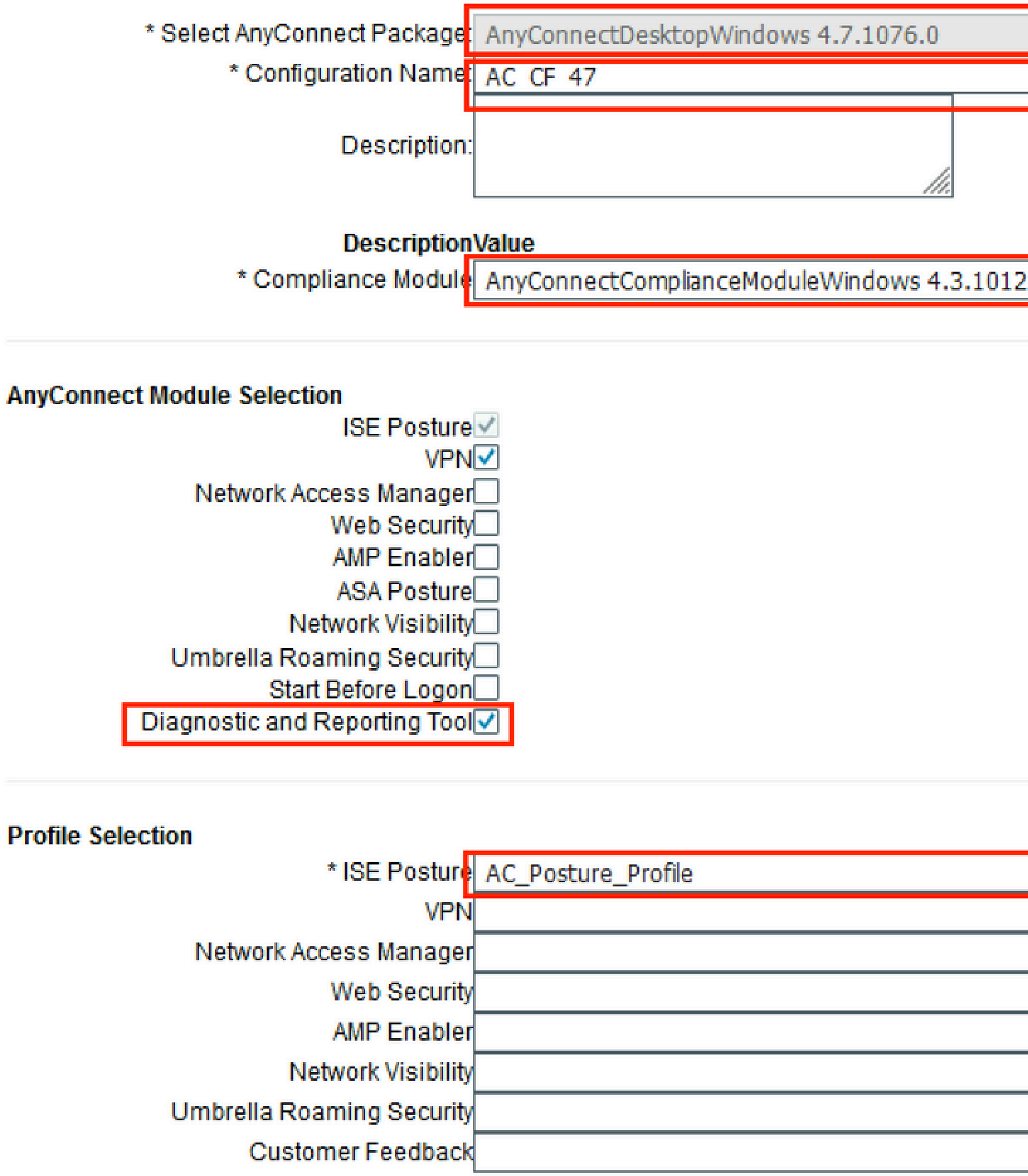
Description:



Posture Protocol

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

Step 5. Navigate to **Policy > Policy Elements > Results > Client Provisioning > Resources** and create **AnyConnect Configuration**. Click **Add** and select **AnyConnect Configuration**. Select **AnyConnect Package**, provide Configuration Name, select **Compliance Module**, check Diagnostic and Reporting Tool, select **Posture Profile** and click **Save**.



* Select AnyConnect Package: AnyConnectDesktopWindows 4.7.1076.0

* Configuration Name: AC_CF_47

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 4.3.1012

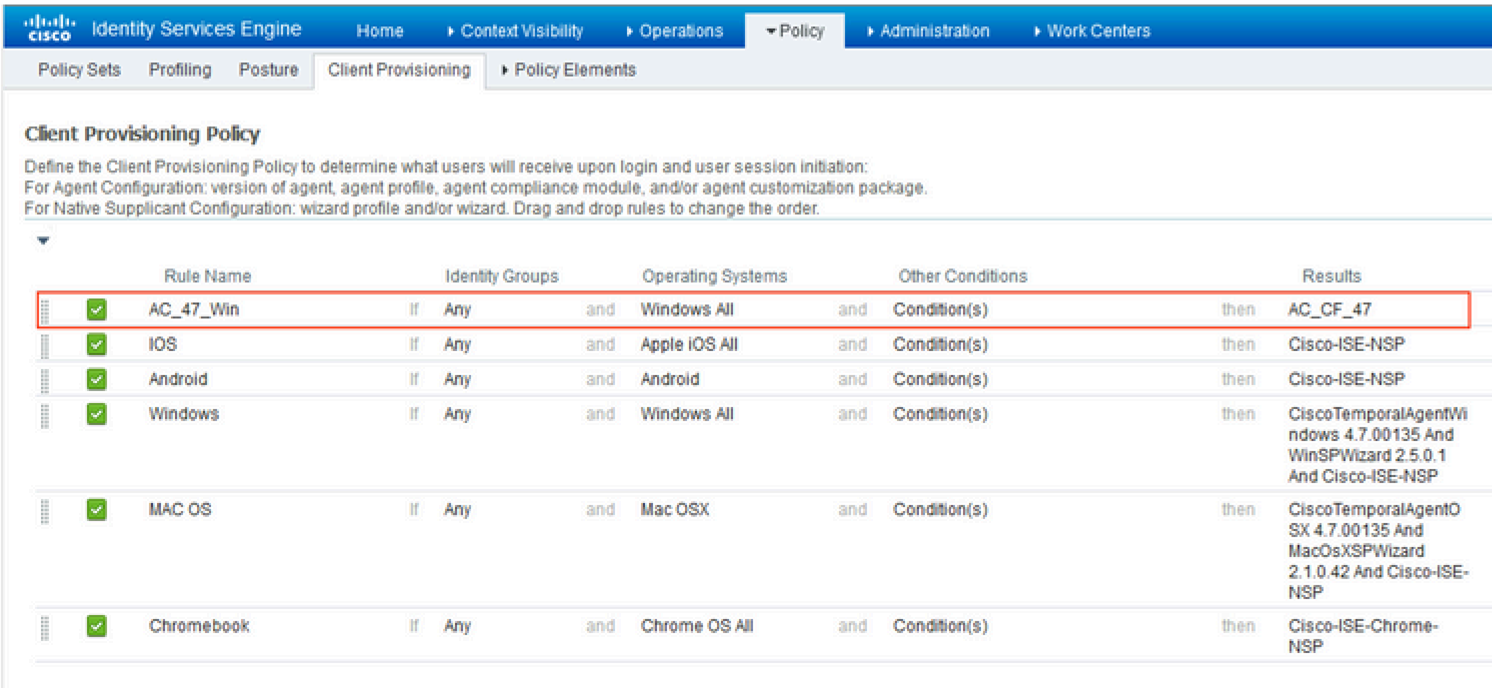
AnyConnect Module Selection

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:

Step 6. Navigate to **Policy** > **Client Provisioning** and create **Client Provisioning Policy**. Click **Edit** and then select **Insert Rule Above**, provide name, select OS, and choose **AnyConnect Configuration** that was created in the previous step.



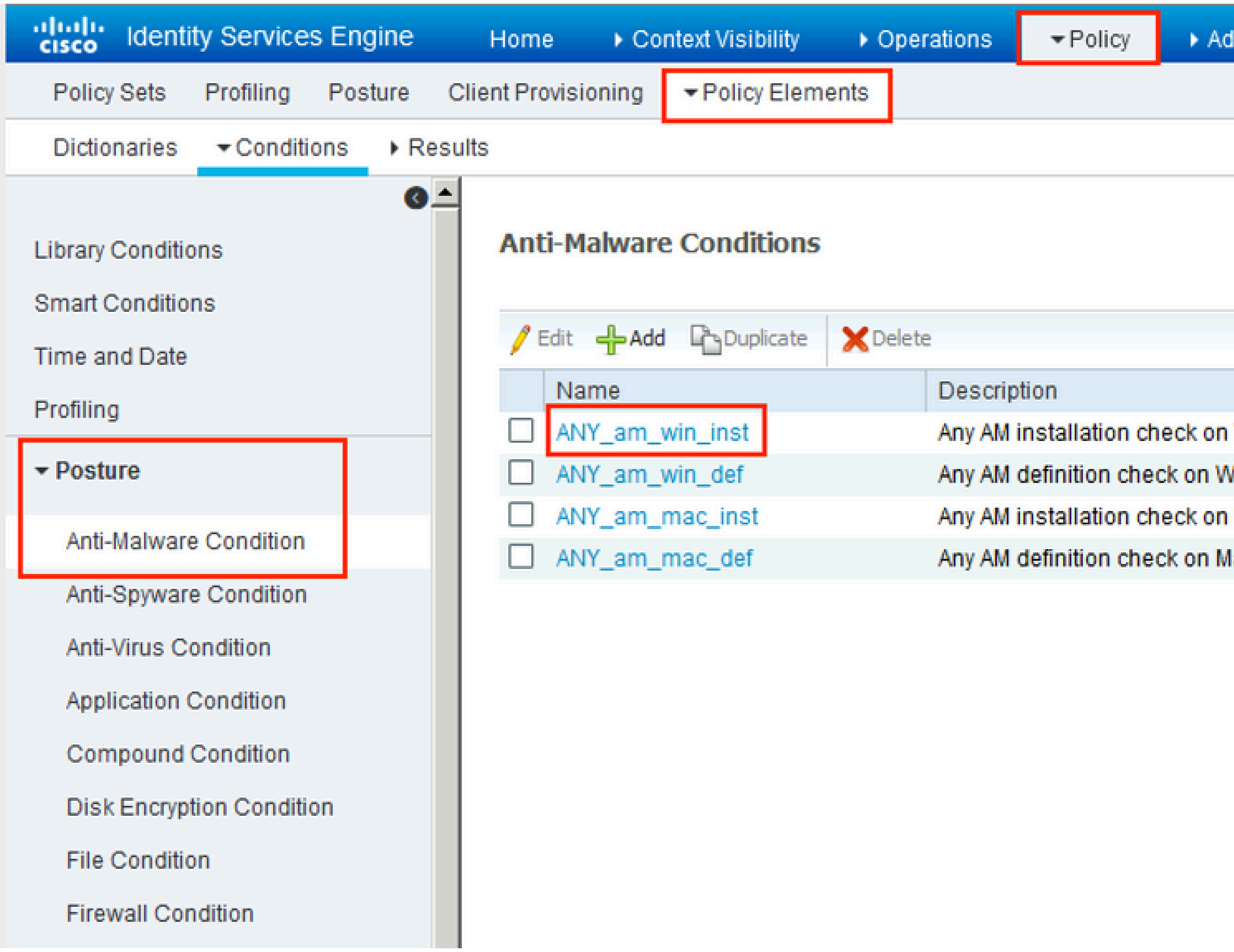
Client Provisioning Policy

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

Step 7. Create Posture Condition under **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Anti-Malware Condition**. In this example, predefined "ANY_am_win_inst" is used.

.

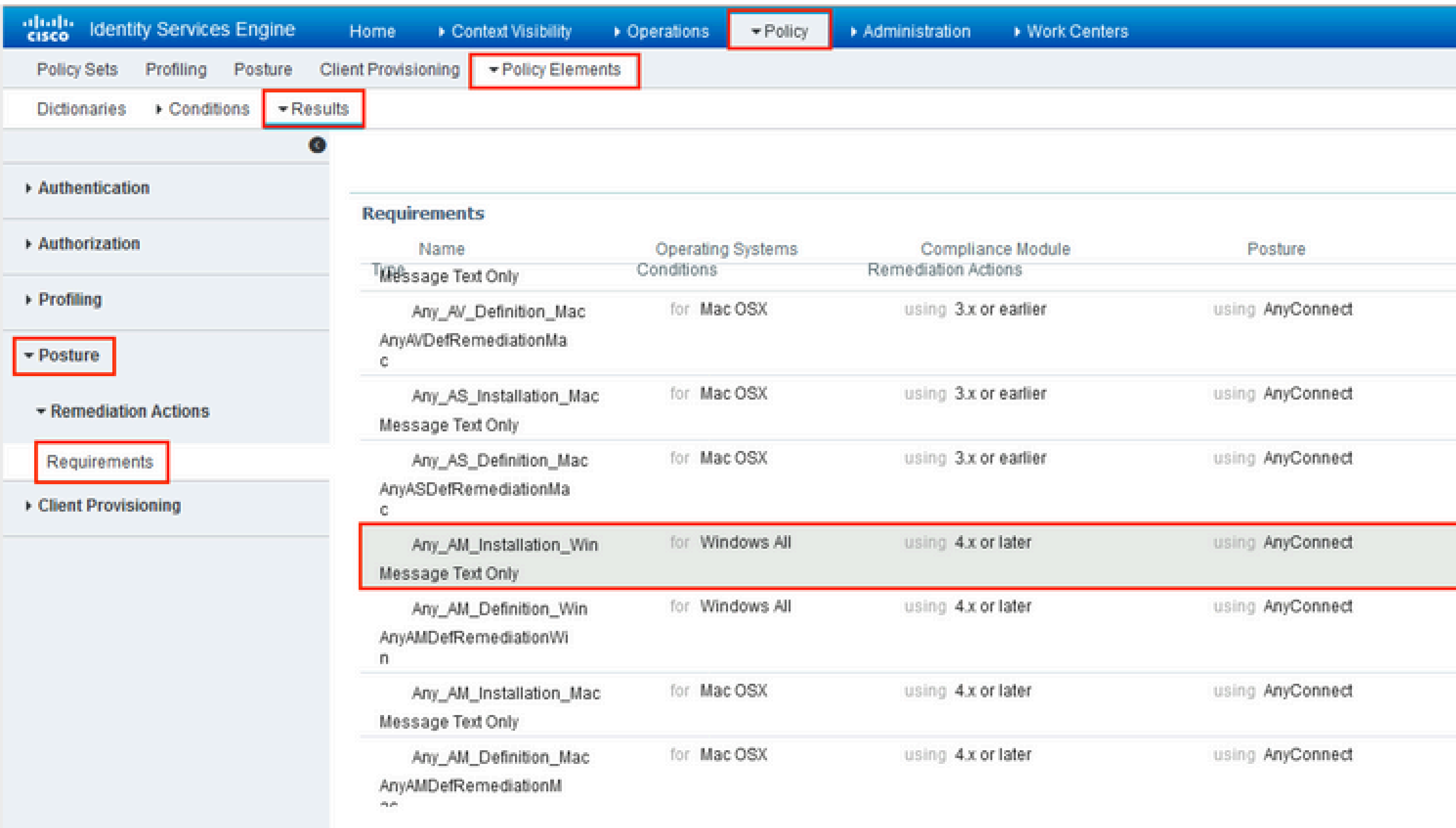


Anti-Malware Conditions

	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

Step 8. Navigate to **Policy** > **Policy Elements** > **Results** > **Posture** > **Remediation Actions** and create **Posture Remediation**. In this example, it is skipped. Remediation Action can be a Text Message.

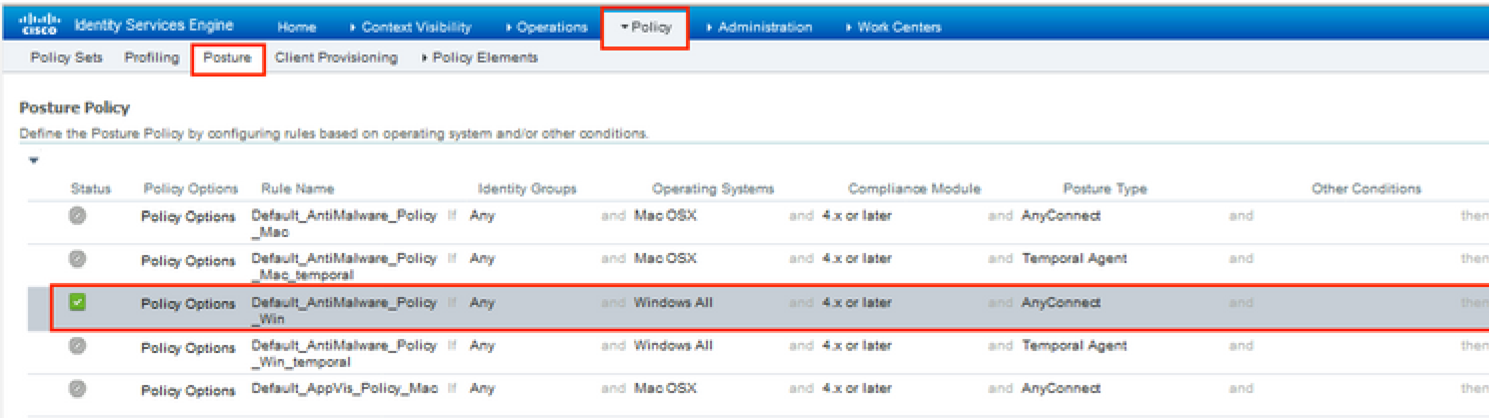
Step 9. Navigate to **Policy** > **Policy Elements** > **Results** > **Posture** > **Requirements** and create **Posture Requirements**. Predefined requirement Any_AM_Installation_Win is used.



Requirements

Name	Operating Systems	Compliance Module	Posture Type	Conditions	Remediation Actions
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

Step 10. Create Posture Policies under **Policies** > **Posture**. Default posture policy for any AntiMalware Check for Windows OS is used.



Posture Policy

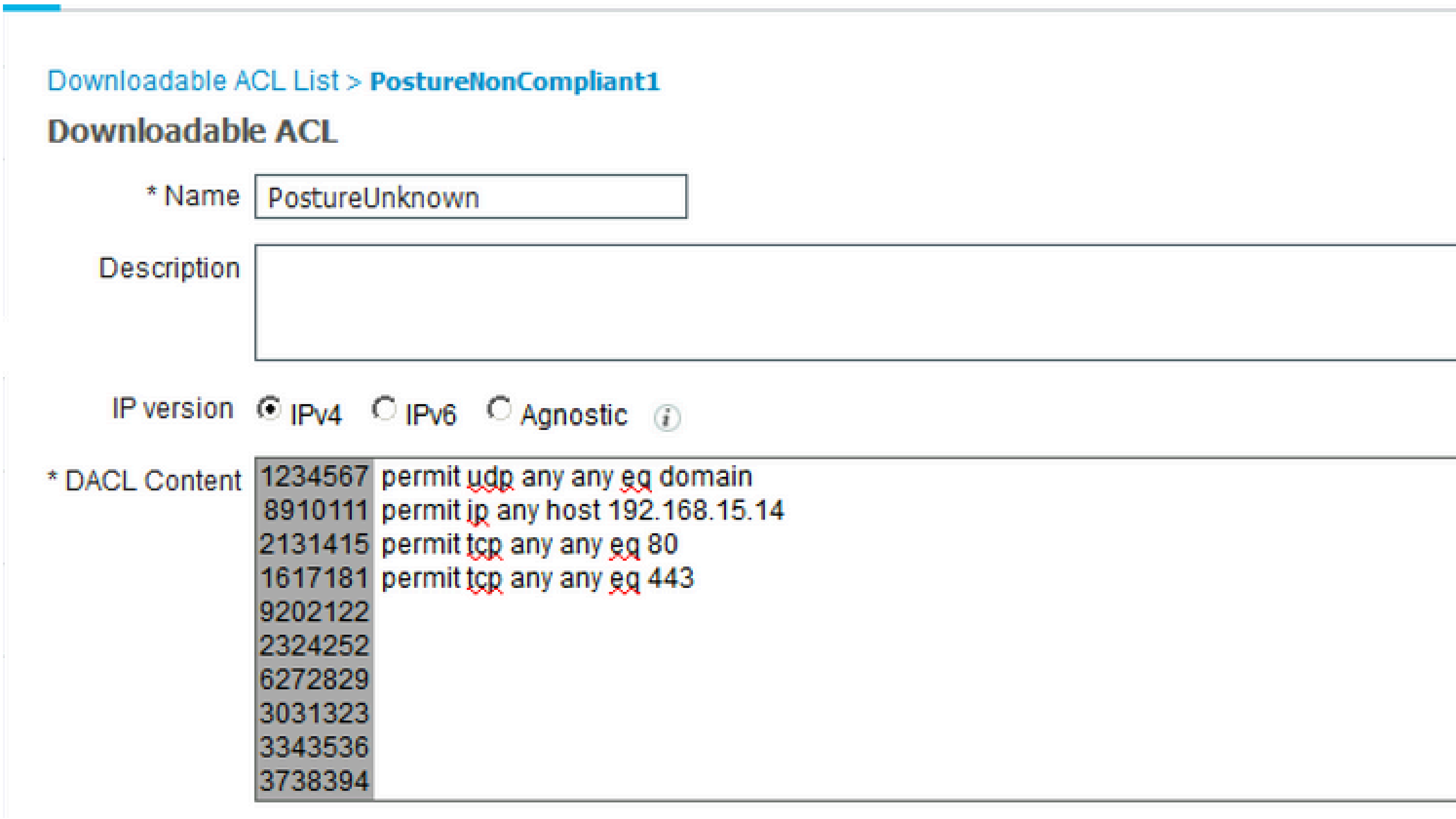
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

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

Step 11. Navigate to **Policy** > **Policy Elements** > **Results** > **Authorization** > **Downloadable ACLS and** create DACLs for different posture statuses.

In this example:

- Posture Unknown DACL - allows traffic to DNS, PSN and HTTP and HTTPS traffic.
- Posture NonCompliant DACL - denies access to Private Subnets and allow only internet traffic.
- Permit All DACL - allows all traffic for Posture Compliant Status.

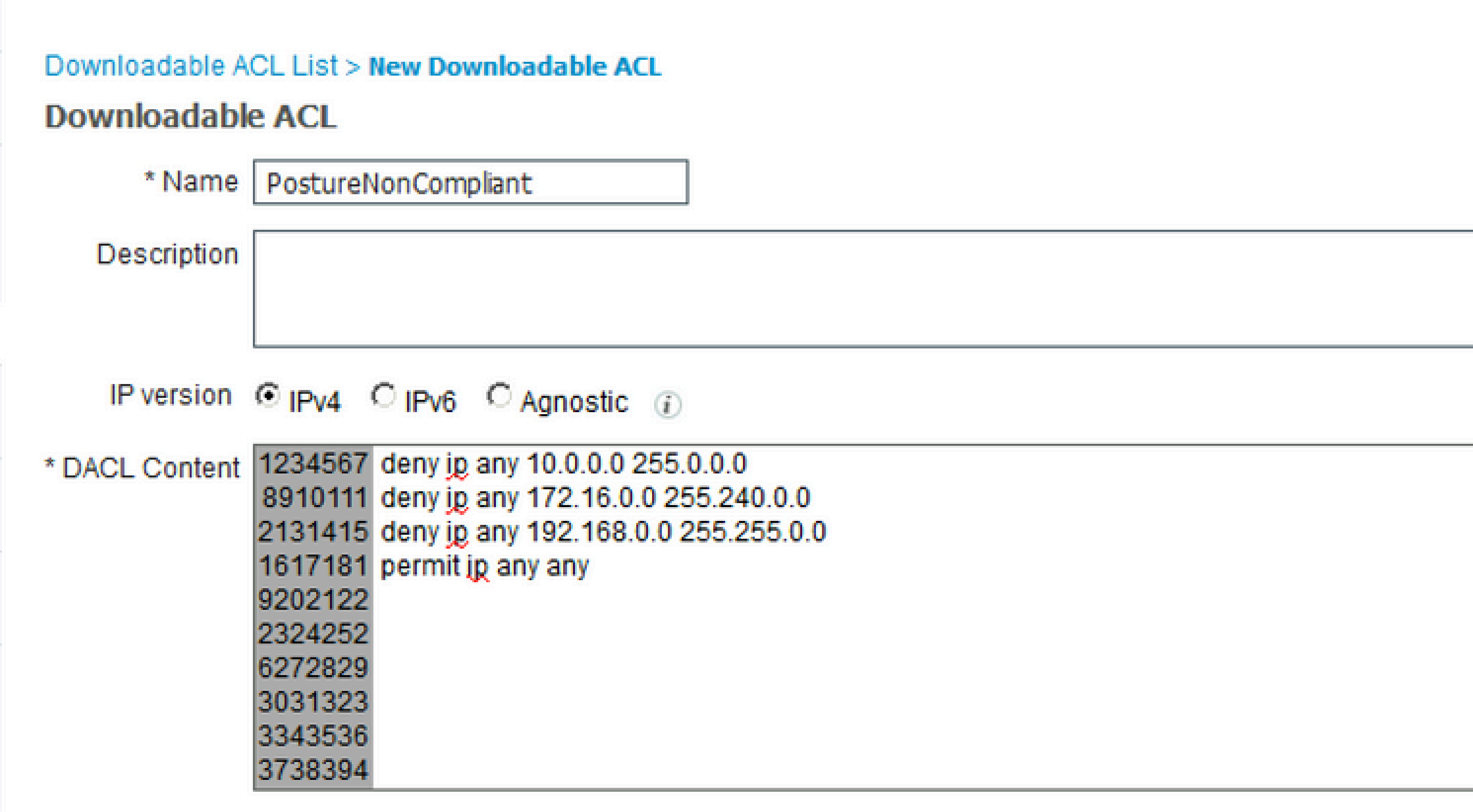


Downloadable ACL List > **PostureNonCompliant1**

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
```

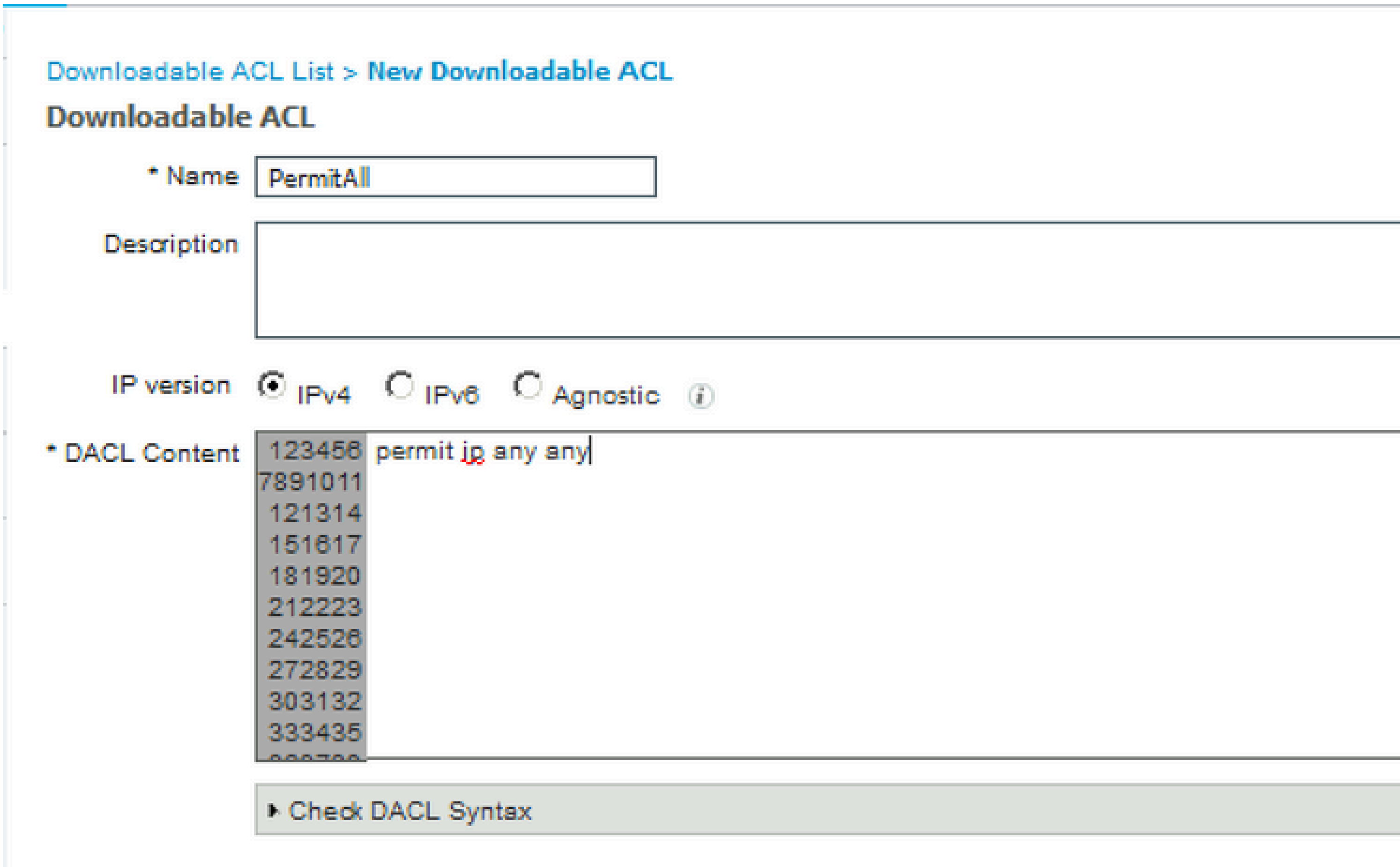


Downloadable ACL List > **New Downloadable ACL**

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

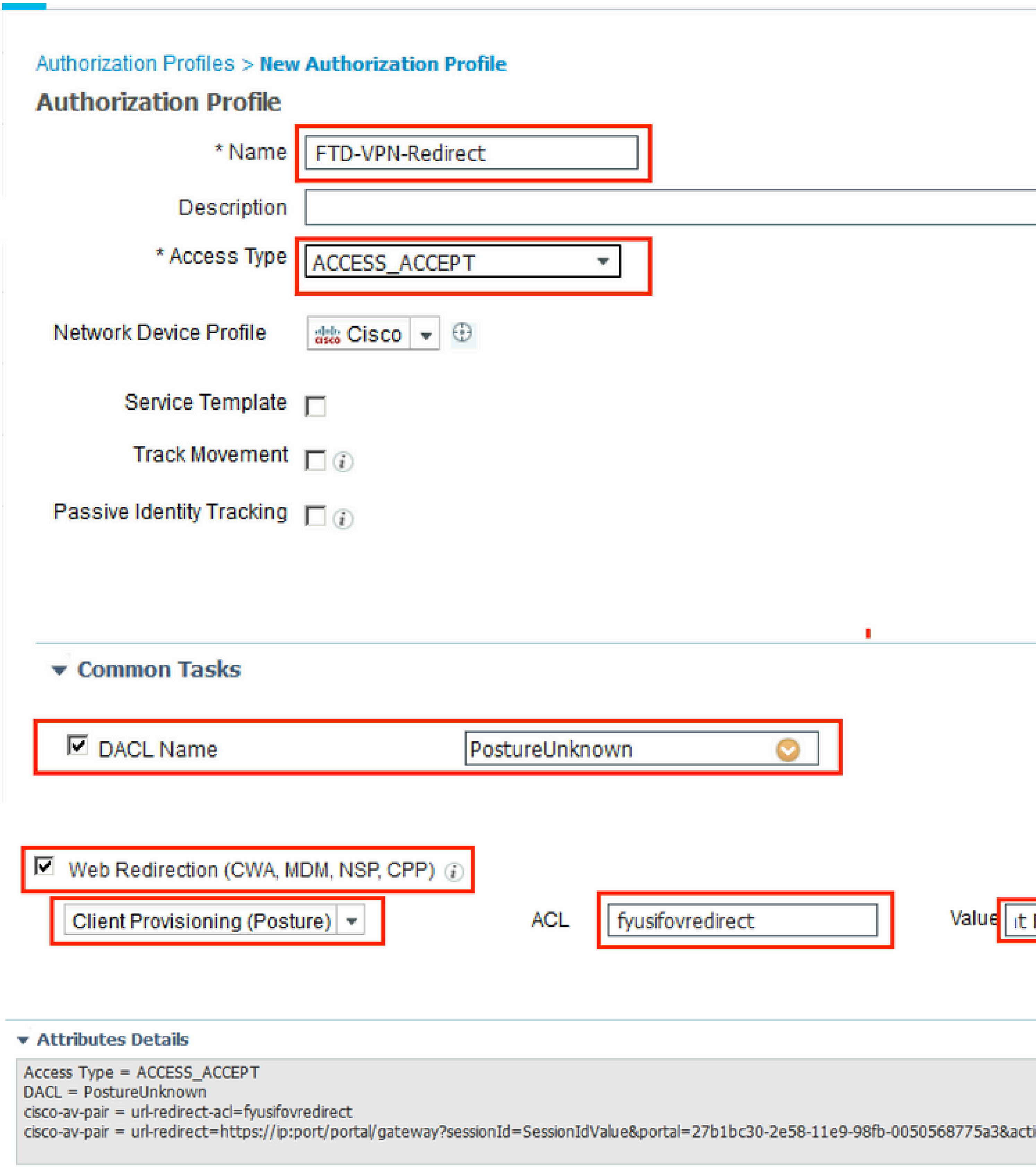
* Name: PermitAll

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content: permit ip any any

Step 12. Create three Authorization Profiles for Posture Unknown, Posture NonCompliant and Posture Compliant statuses. In order to do so, navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. In the **Posture Unknown** profile, select **Posture Unknown DACL**, check **Web Redirection**, select **Client Provisioning**, provide Redirect ACL name (that is configured on FTD) and select the 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

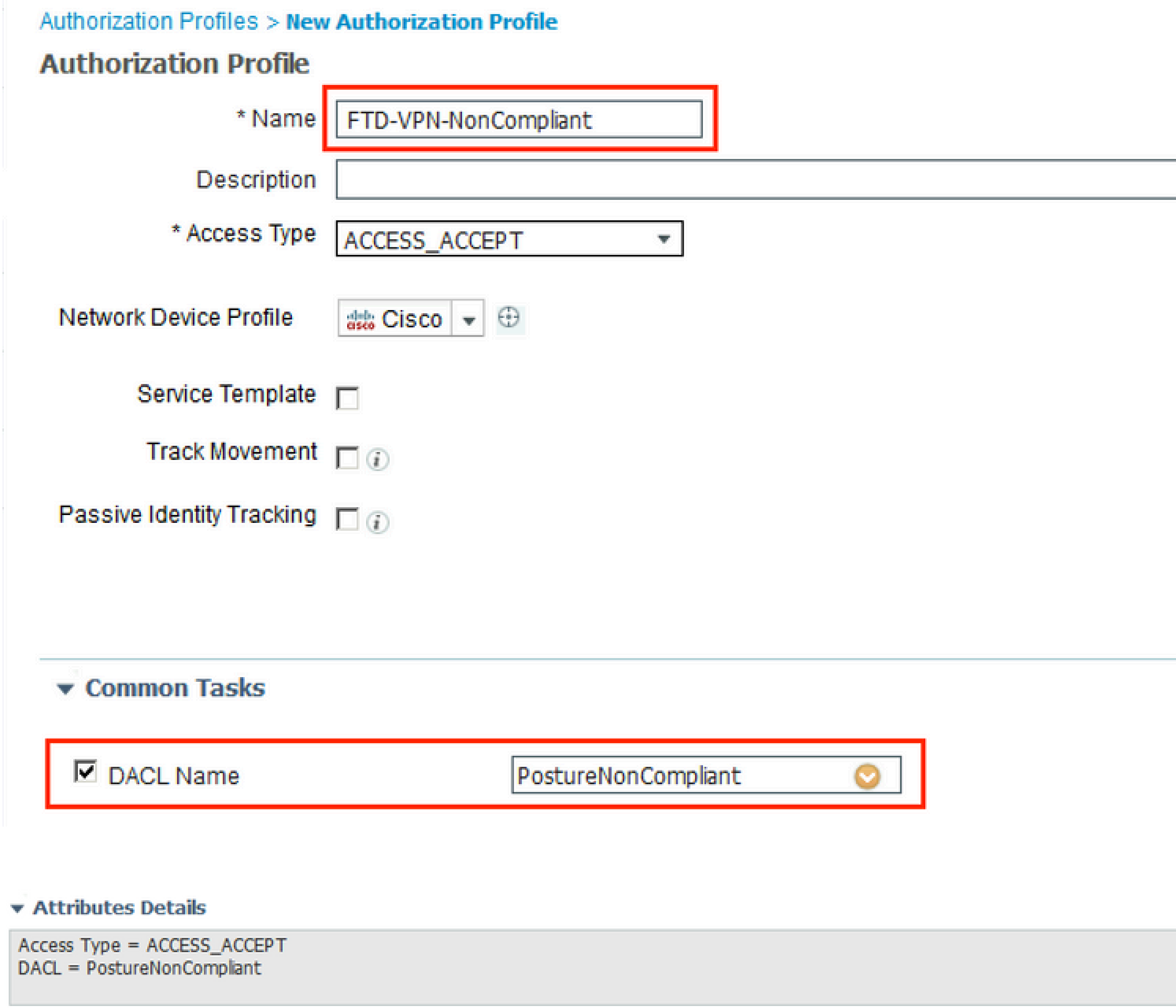
☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: fyusifovredirect Value: ıt 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
```

In the **Posture NonCompliant** profile, select **DACL** in order to limit access to the network.



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	□

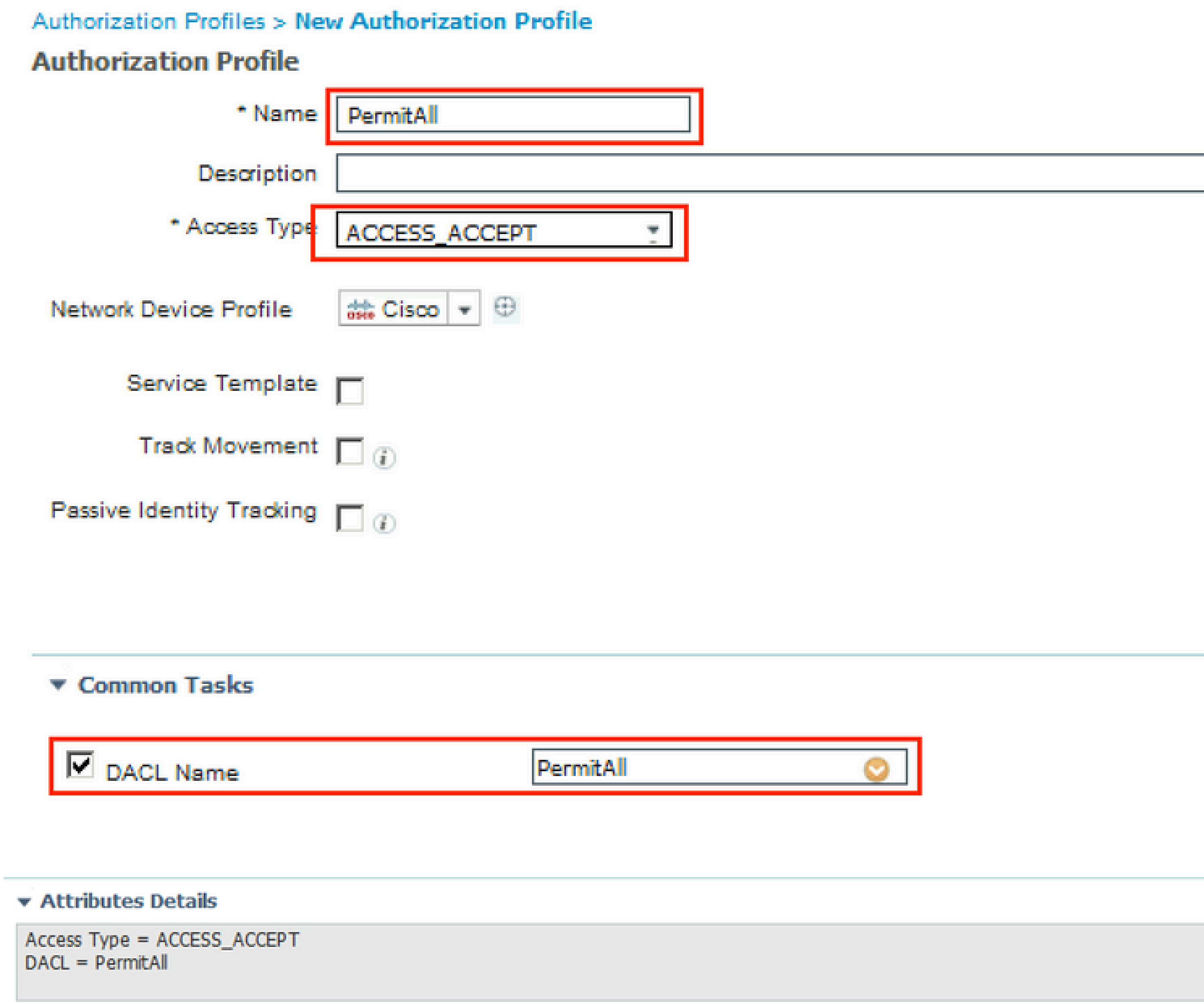
Common Tasks

☑ DACL Name PostureNonCompliant

Attributes Details

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

In the **Posture Compliant** profile, select **DACL** in order to allow full access to the network.



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 □

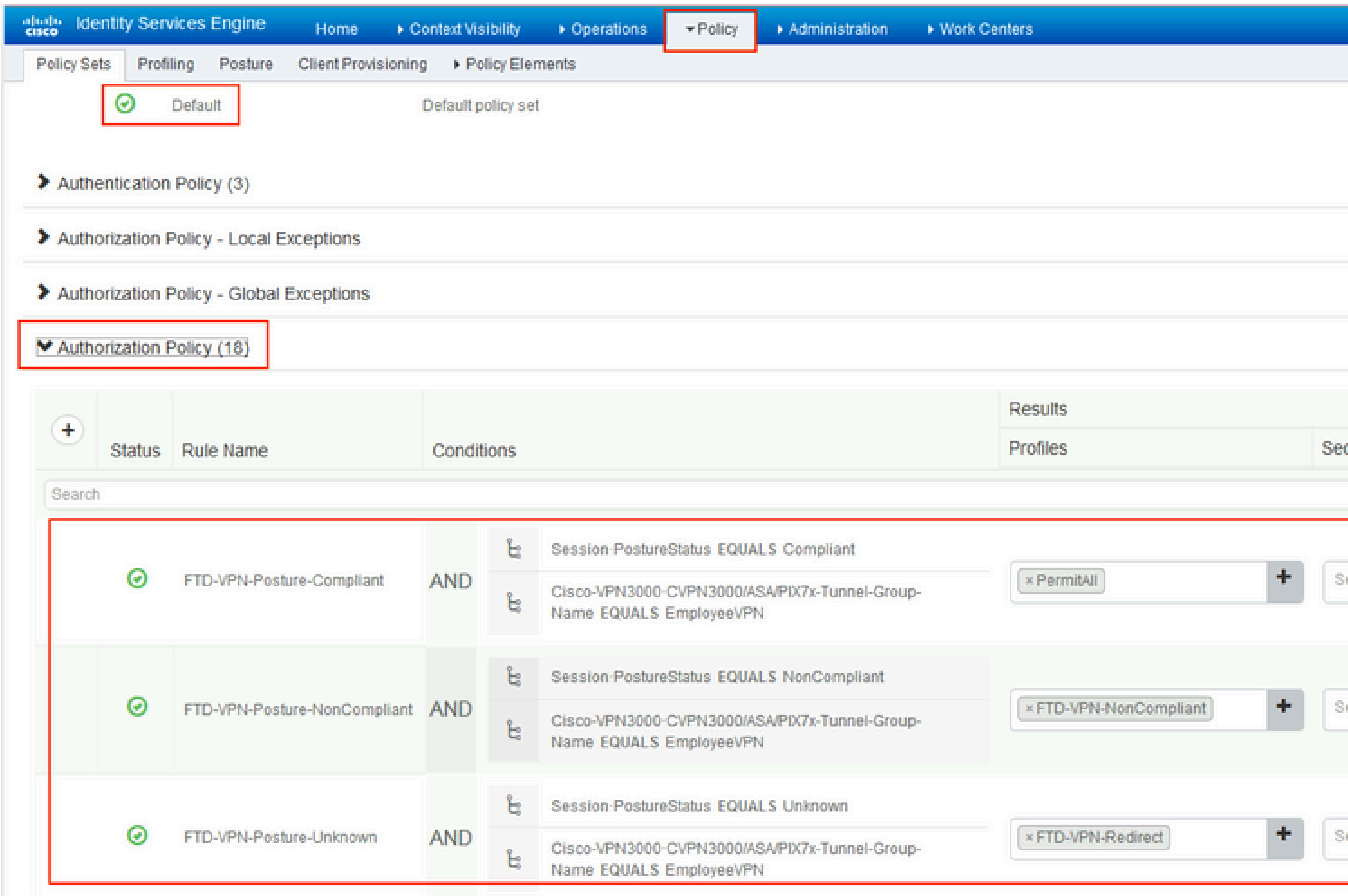
Common Tasks

☑ DACL Name: PermitAll

Attributes Details

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

Step 13. Create Authorization Policies under **Policy** > **Policy Sets** > **Default** > **Authorization Policy**. As condition Posture Status and VNP TunnelGroup Name is used.



Default | Default policy set

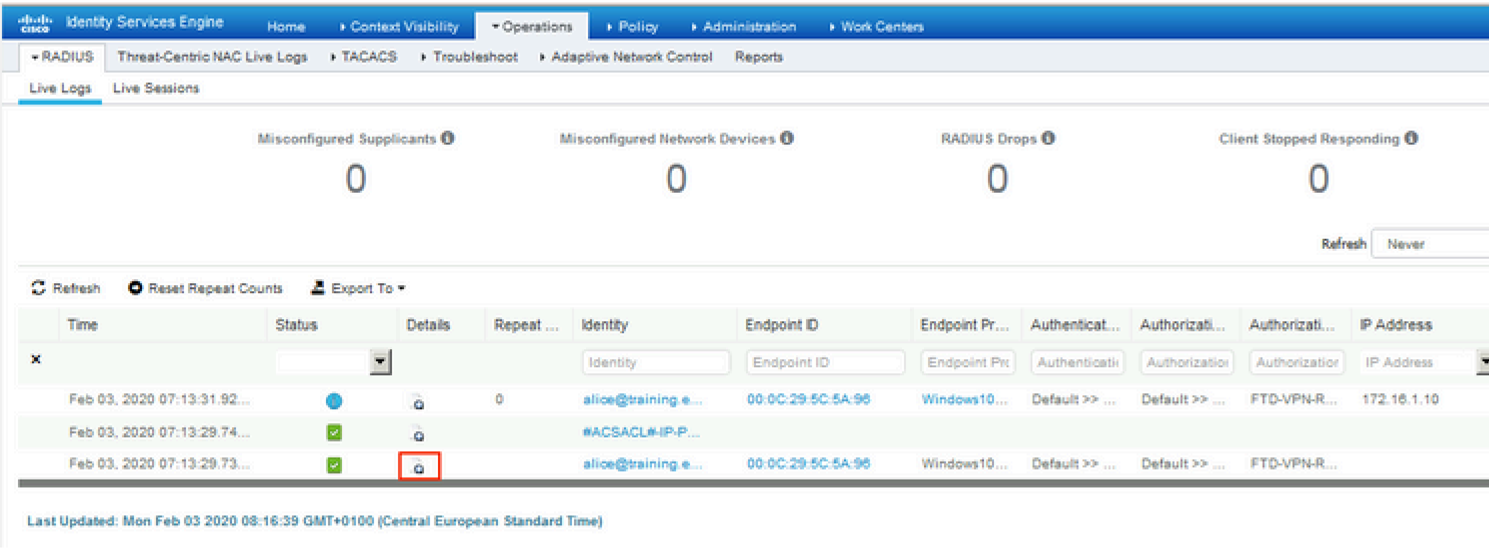
- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (18)

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

Verify

Use this section in order to confirm that your configuration works properly.

On ISE, the first verification step is RADIUS Live Log. Navigate to **Operations** > **RADIUS Live Log**. Here, user Alice is connected and the expected authorization policy is selected.

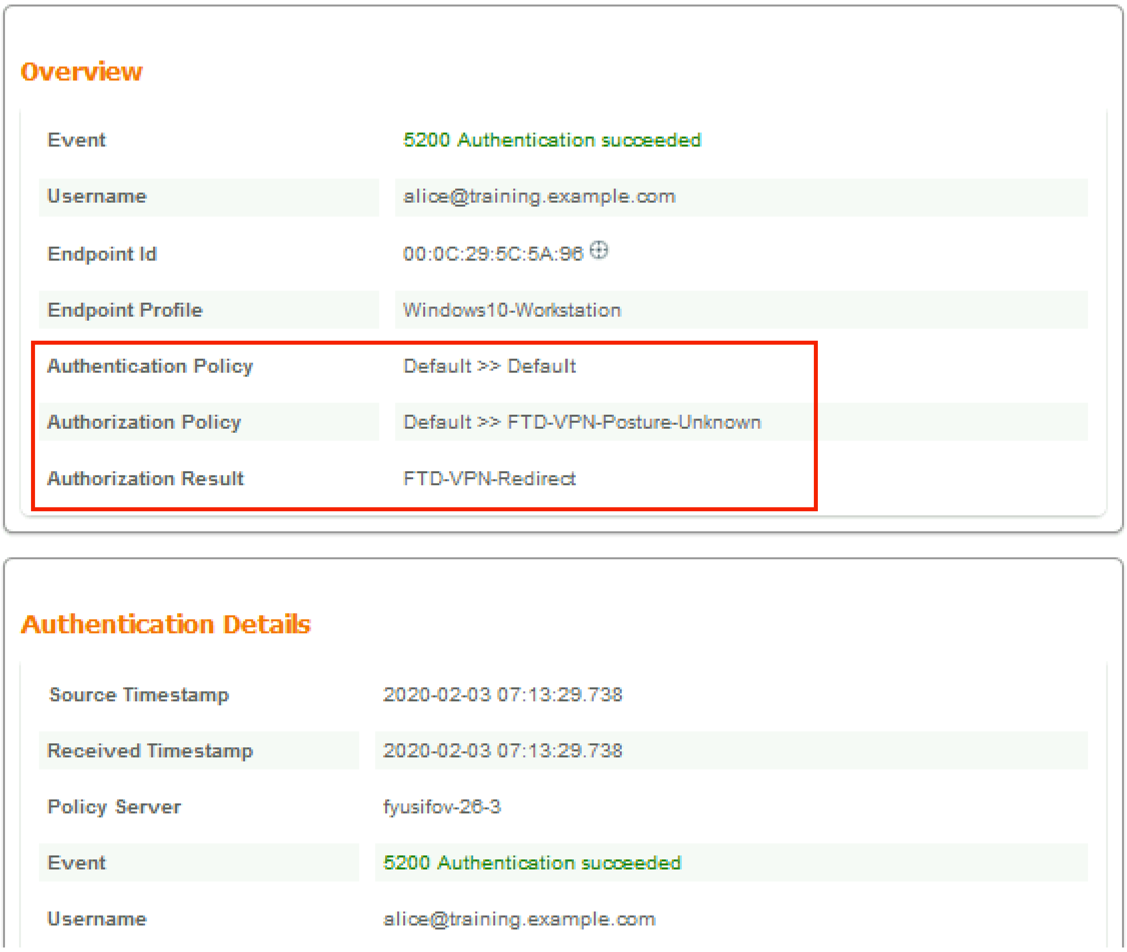


Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 0 | Client Stopped Responding 0

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)

Authorization policy FTD-VPN-Posture-Unknown is matched and as result, FTD-VPN-Profile is sent to FTD.



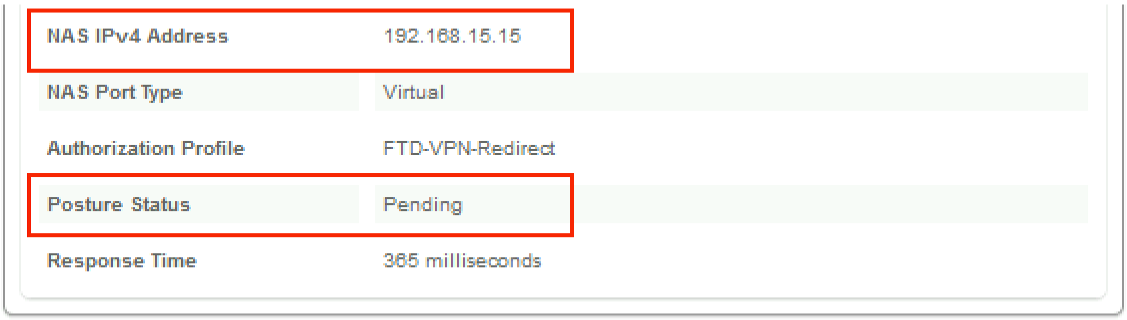
Overview

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

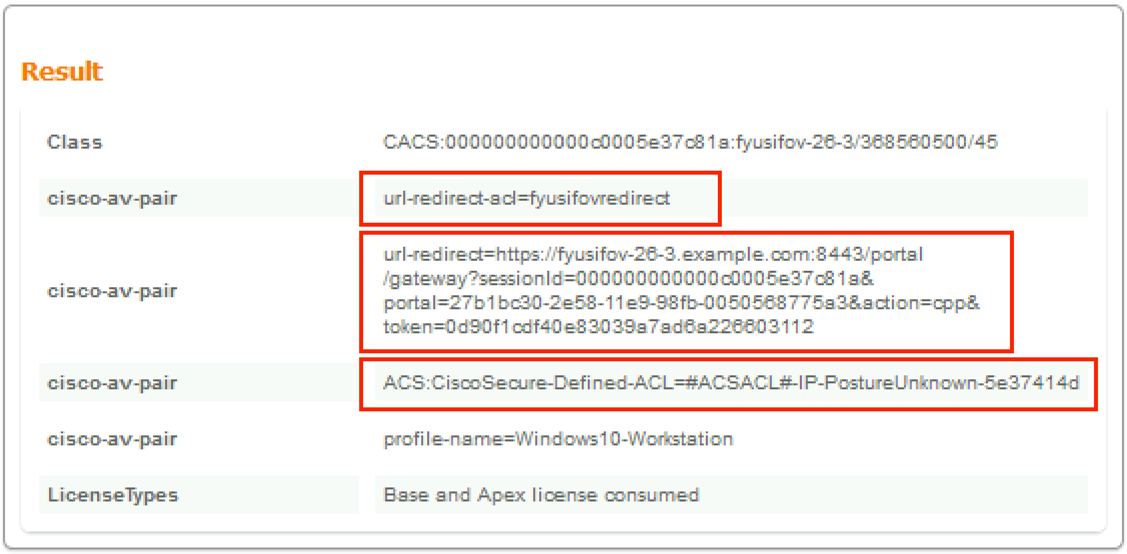
Source Timestamp	2020-02-03 07:13:29.738
Received Timestamp	2020-02-03 07:13:29.738
Policy Server	fyusifov-26-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

Posture Status Pending.



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

The Result section shows which attributes are sent to 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

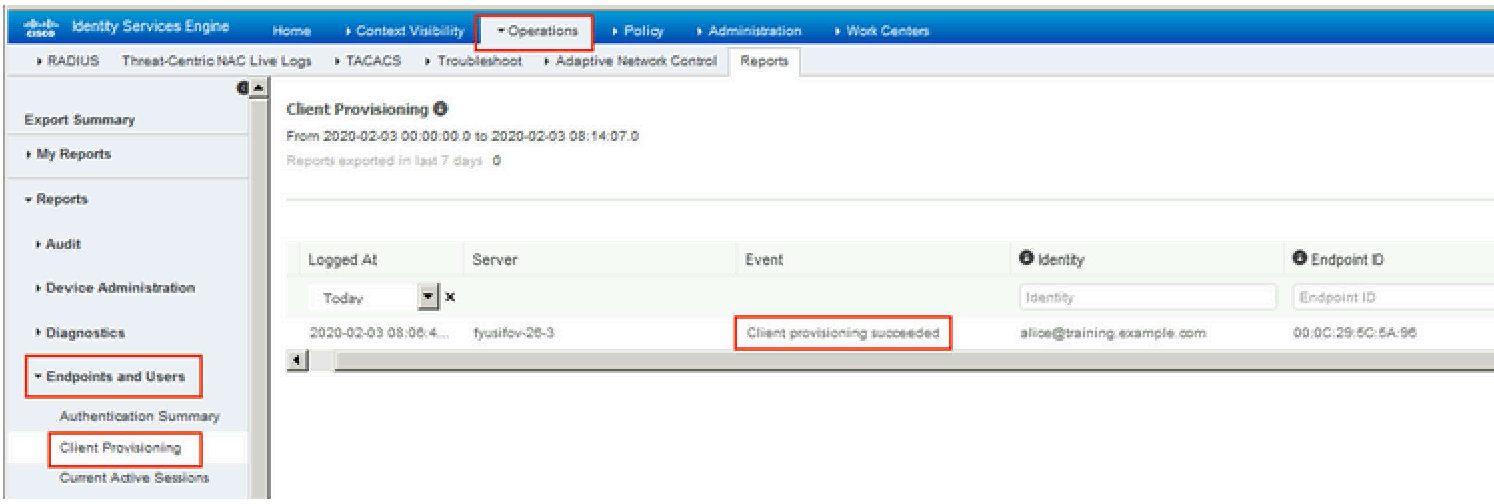
On FTD, in order to verify VPN connection, SSH to the box, execute **system support diagnostic-cli** and then **show vpn-sessiondb detail anyconnect**. From this output, verify that attributes sent from ISE are applied for this VPN session.

<#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#
```

Client Provisioning policies can be verified. Navigate to **Operations > Reports > Endpoints and Users > Client Provisioning**.



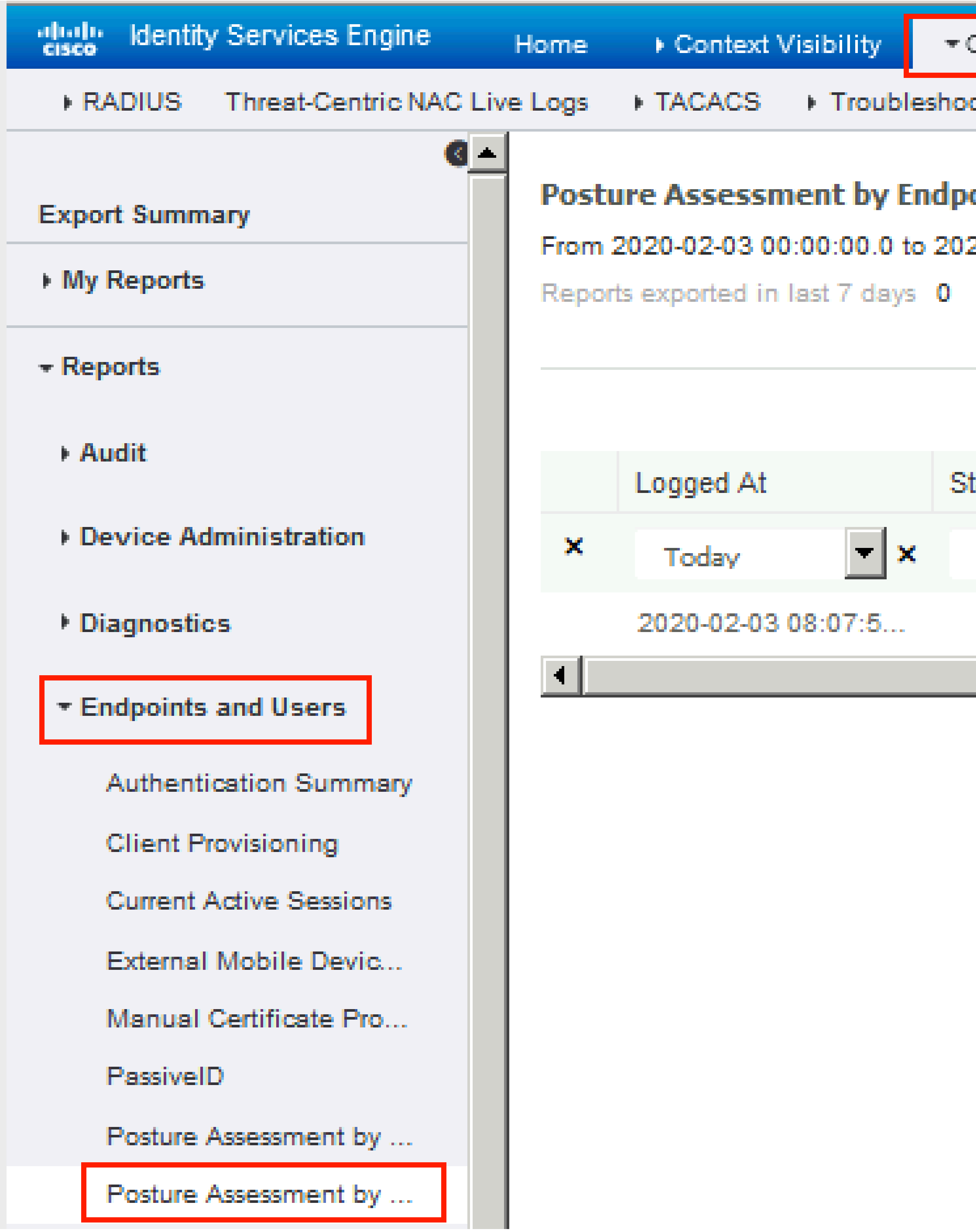
Client Provisioning

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

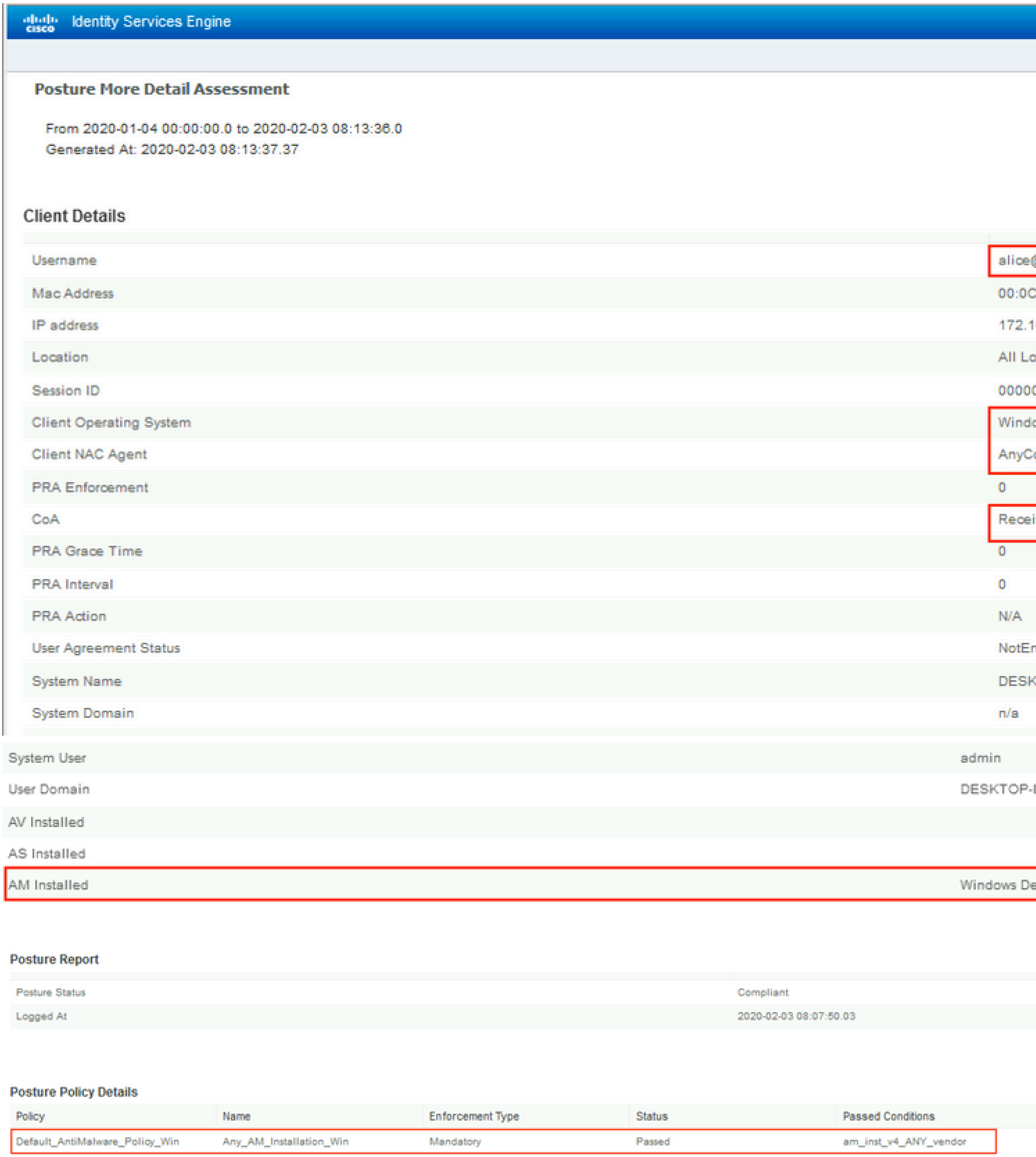
Reports exported in last 7 days 0

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

Posture Report sent from AnyConnect can be checked. Navigate to **Operations > Reports > Endpoints and Users > Posture Assessment by Endpoint**.



In order to see more details on the posture report, click **Details**.



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	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

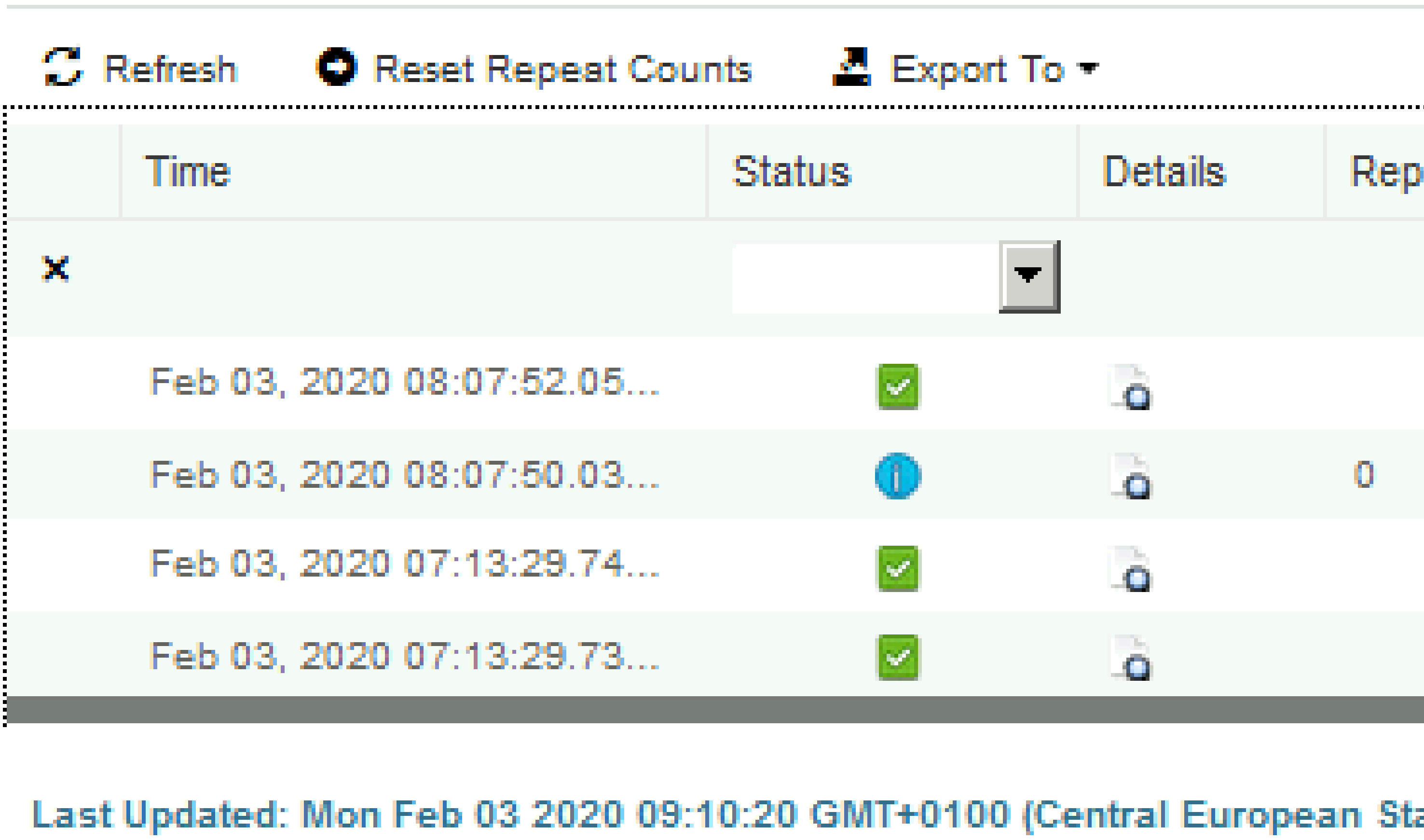
Posture Report

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

Posture Policy Details

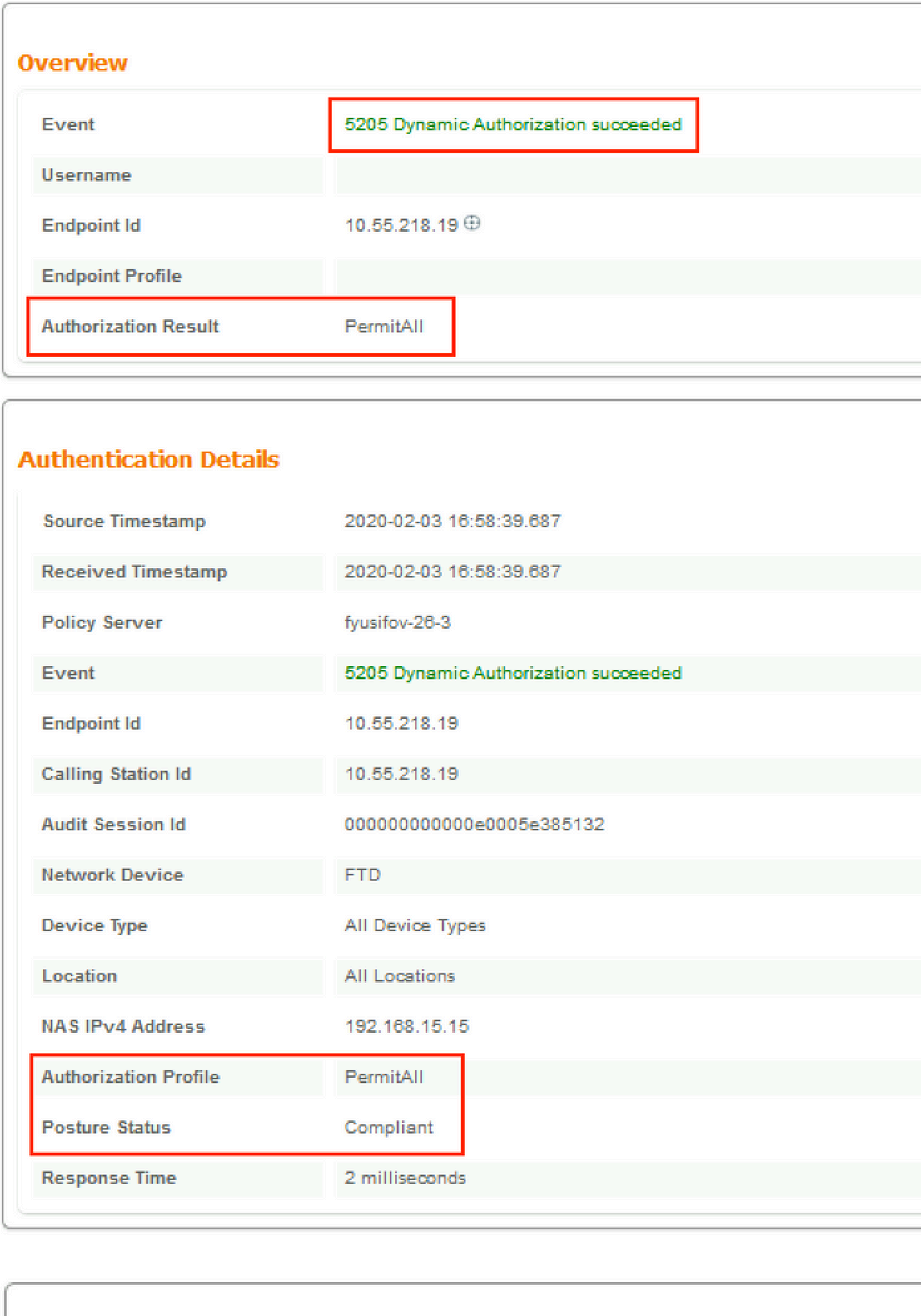
Policy	Name	Enforcement Type	Status	Passed Conditions
Default_AntiMalware_Policy_Win	Any_AM_Installation_Win	Mandatory	Passed	am_inst_v4_ANY_vendor

After the report is received on ISE, posture status is updated. In this example, posture status is compliant and CoA Push is triggered with a new set of attributes.



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

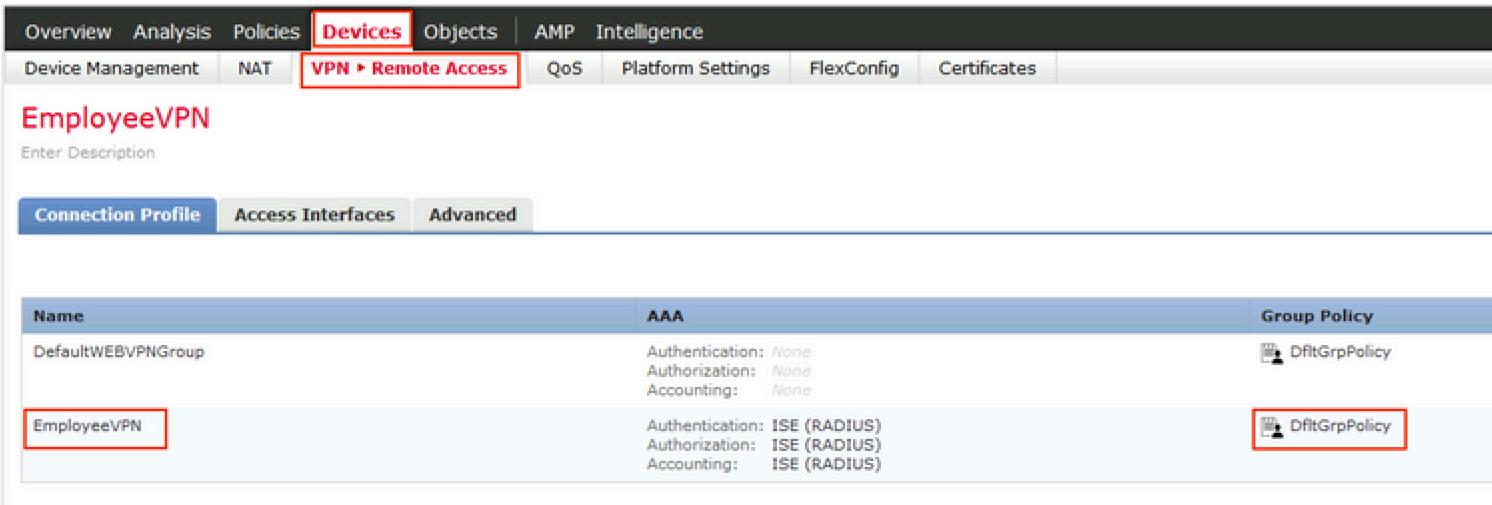
Authentication Details

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

- Spilt Tunnel

One of the common issues, when there is a spit tunnel is configured. In this example, default Group Policy is used, which tunnels all traffic. In case if only specific traffic is tunnelled, then AnyConnect probes (enroll.cisco.com and discovery host) must go through the tunnel in addition to traffic to ISE and other internal resources.

In order to check the tunnel policy on FMC, first, check which Group Policy is used for VPN connection. Navigate to **Devices > VPN Remote Access**.

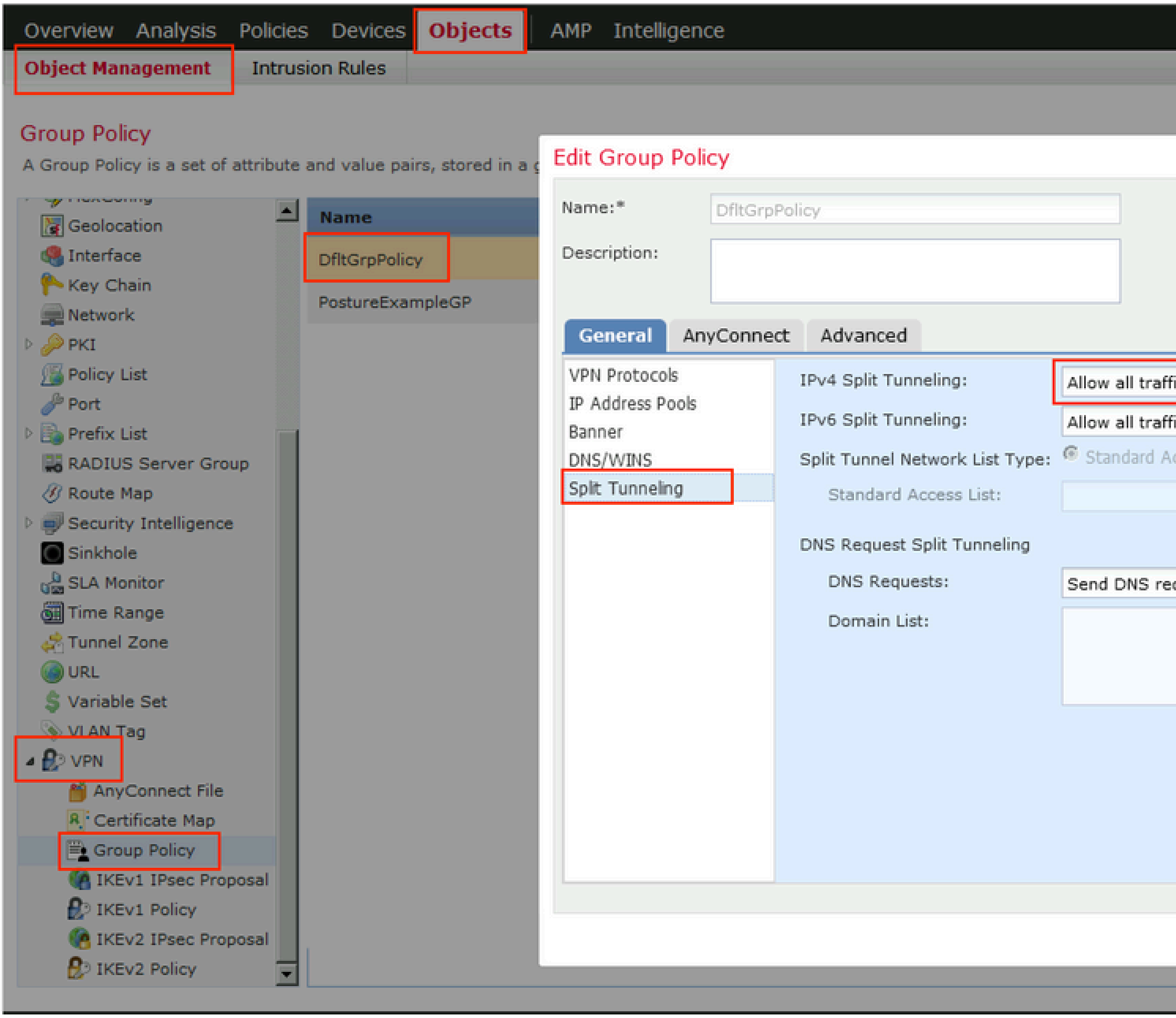


EmployeeVPN

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

Then, navigate to **Objects** > **Object Management** > **VPN** > **Group Policy** and click on **Group Policy** configured for VPN.



Name:* DfltGrpPolicy

Description:

IPv4 Split Tunneling: Allow all traffi

IPv6 Split Tunneling: Allow all traffi

Split Tunnel Network List Type: ○ Standard A

Standard Access List:

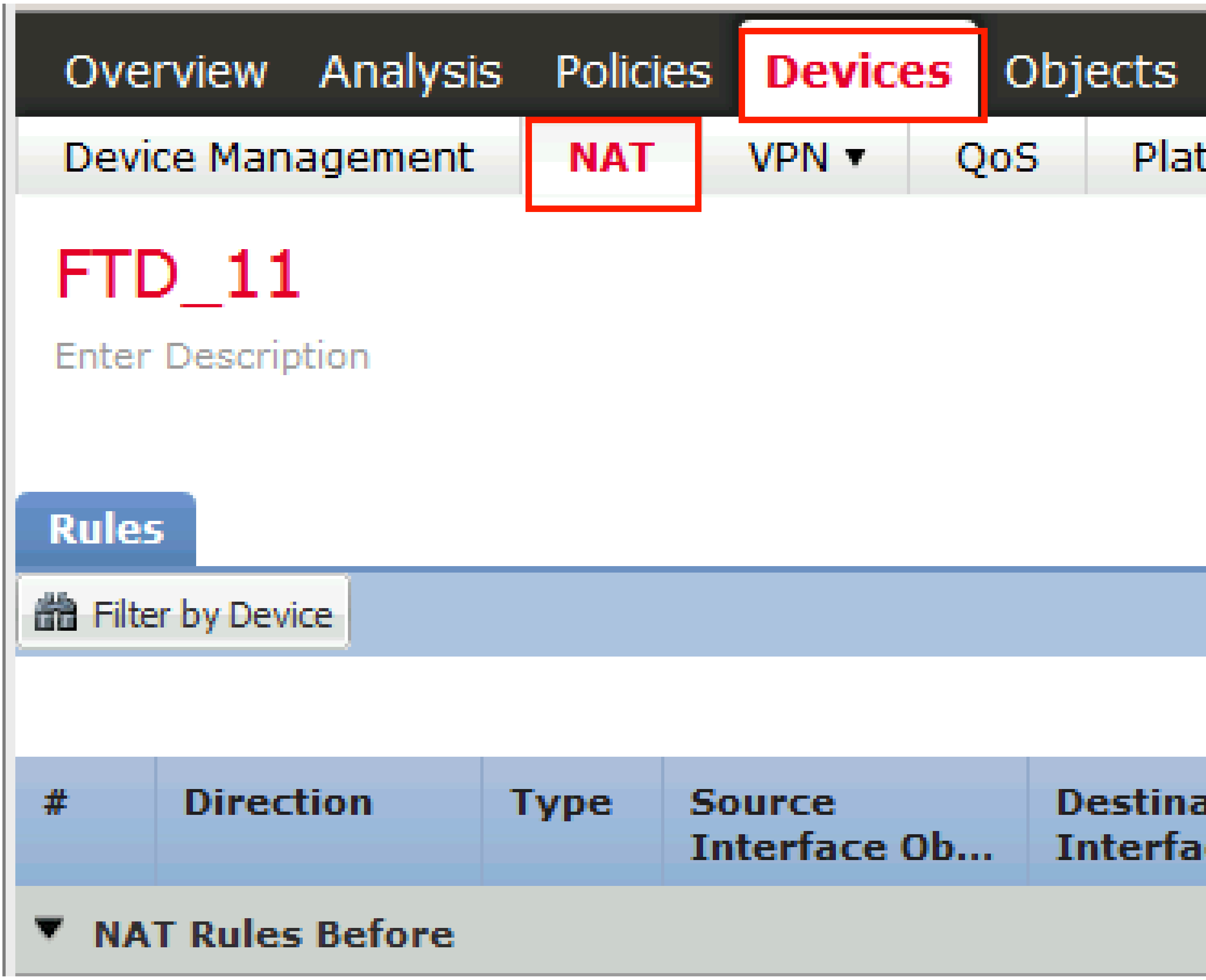
DNS Requests: Send DNS rec

Domain List:

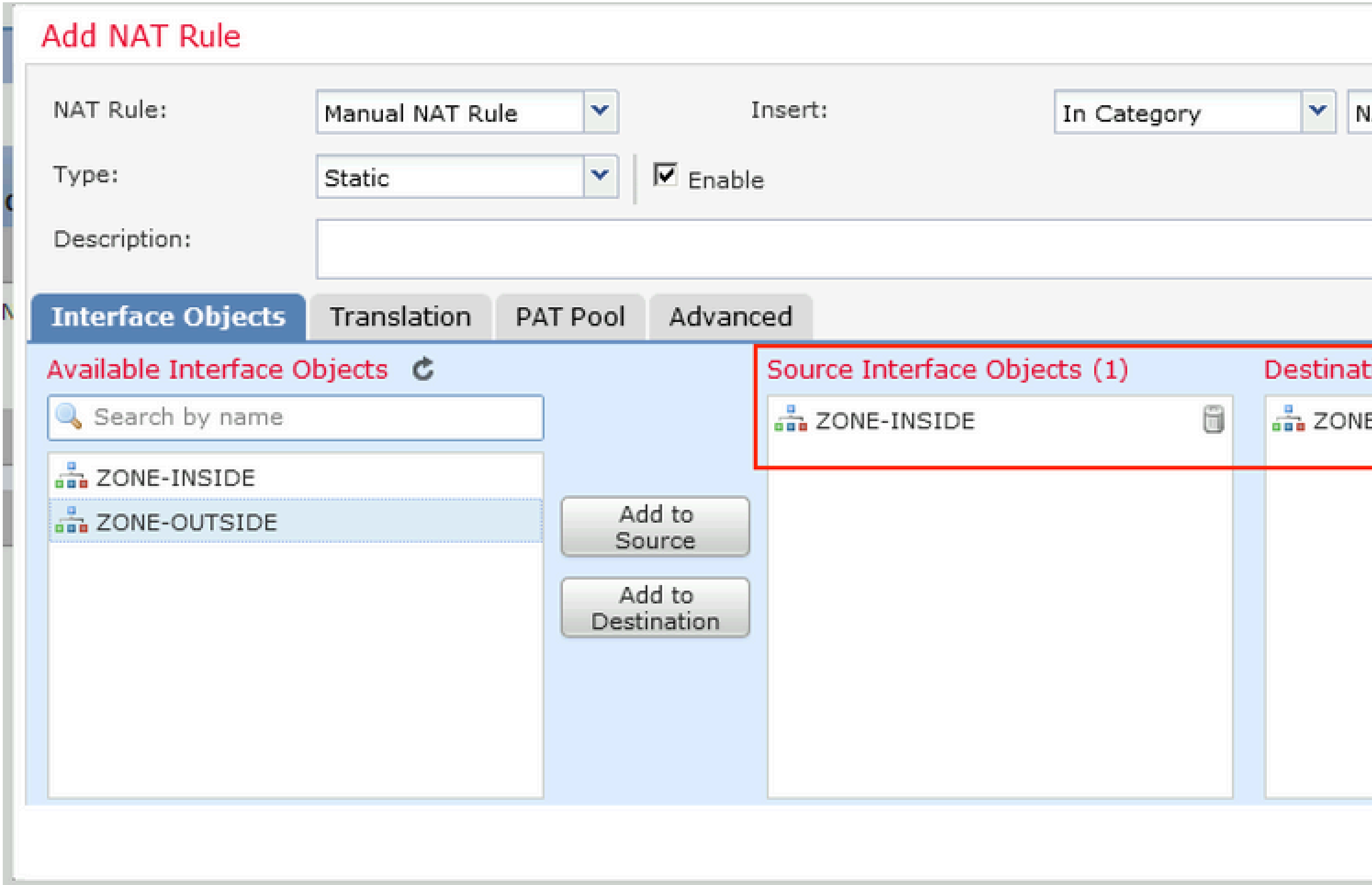
- Identity NAT

Another common issue, when VPN usersâ€™ return traffic gets translated with the use of incorrect NAT entry. In order to fix this issue, Identity NAT must be created in an appropriate order.

First, check NAT rules for this device. Navigate to **Devices > NAT** and then click **Add Rule** to create a new rule.



In the opened window, under the **Interface Objects** tab, select **Security Zones**. In this example, NAT entry is created from **ZONE-INSIDE** to **ZONE-OUTSIDE**.



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category

Type: Static

☑ Enable

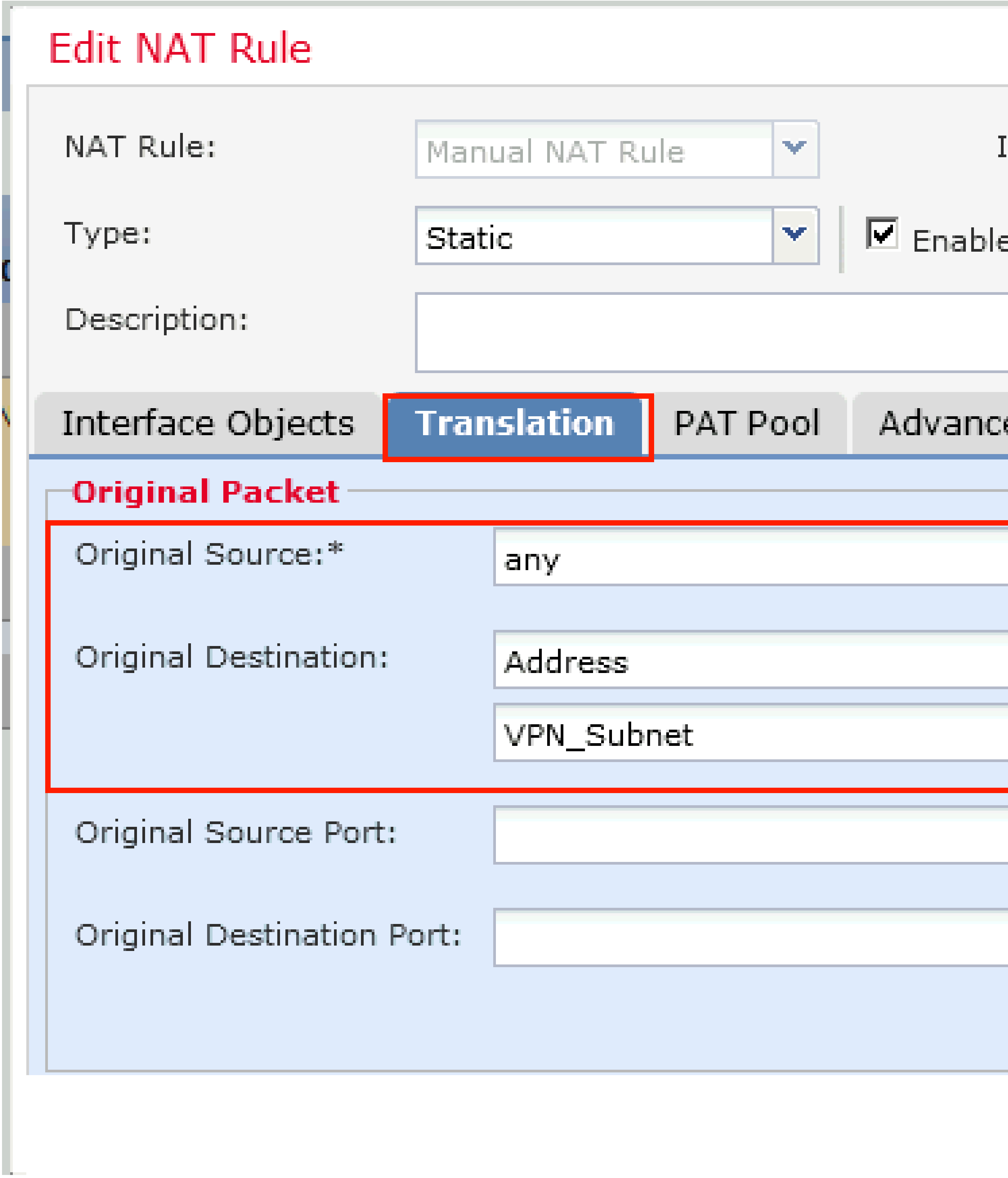
Description:

Available Interface Objects

Source Interface Objects (1)

ZONE-INSIDE

Under the **Translation** tab, select original and translated packet details. As it is Identity NAT, source and destination are kept unchanged:



Edit NAT Rule

NAT Rule: Manual NAT Rule

Type: Static

☑ Enable

Description:

Original Packet

Original Source:* any

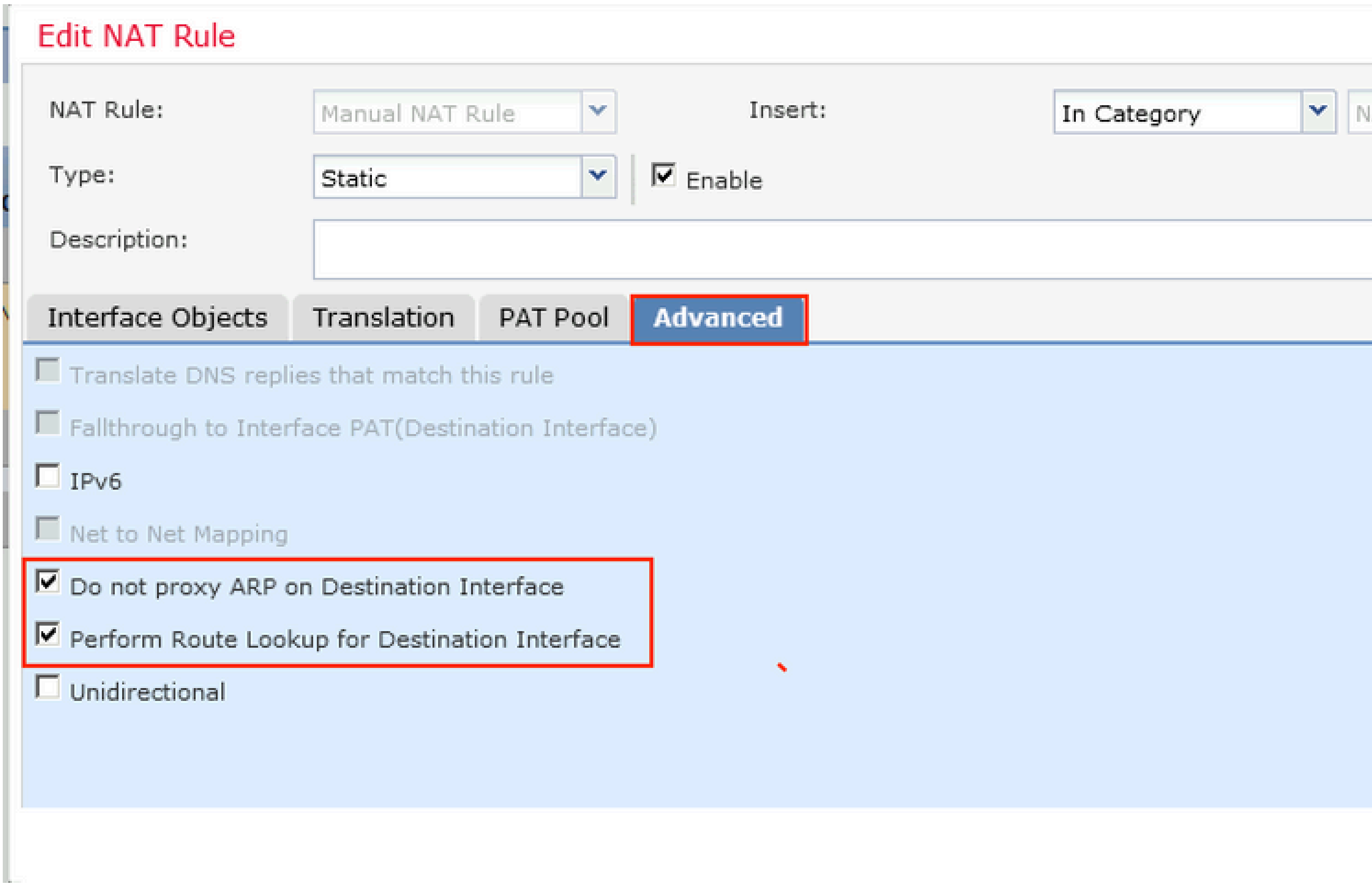
Original Destination: Address

VPN_Subnet

Original Source Port:

Original Destination Port:

Under the **Advanced** tab, check checkboxes as shown in this image:



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