FTD에서 AnyConnect 원격 액세스 VPN을 통한 ISE 상태 구성

목차

- 소개
- 사전 요구 사항
  - 요구 사항
  - 사용되는 구성 요소
- 구성
  - 네트워크 다이어그램 및 트래픽 흐름
  - 설정
    - FTD/FMC
    - ISE
- 다음을 확인합니다.
- 문제 해결

소개

이 문서에서는 ISE(Identity Services Engine)에 대한 VPN 사용자 상태를 파악하기 위해 FTD(Firepower Threat Defense) 버전 6.4.0을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AnyConnect 원격 액세스 VPN
- FTD의 원격 액세스 VPN 구성
- ISE(Identity Services Engine) 및 상태 서비스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

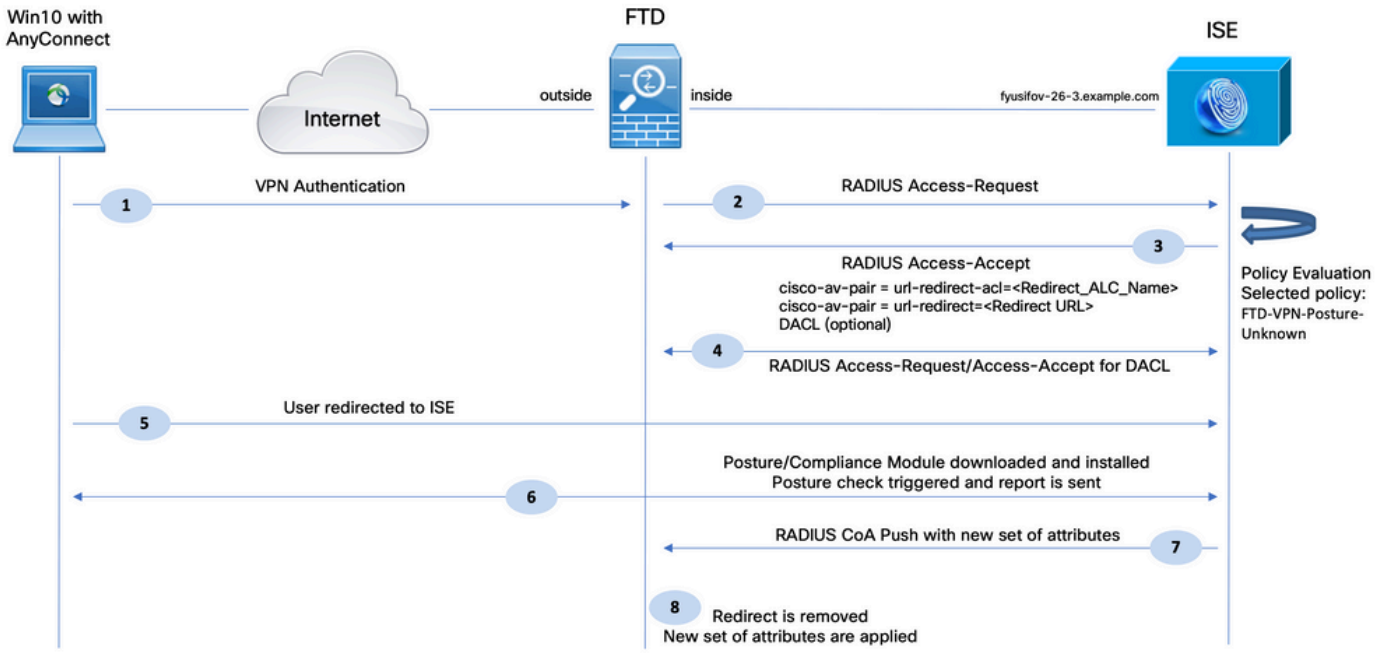
- Cisco FTD(Firepower Threat Defense) 소프트웨어 버전 6.4.0
- Cisco FMC(Firepower Management Console) 소프트웨어 버전 6.5.0
- Microsoft Windows 10(Cisco AnyConnect Secure Mobility Client 버전 4.7 포함)
- Cisco ISE(Identity Services Engine) 버전 2.6 및 패치 3

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램 및 트래픽 흐름


Win10 with AnyConnect
Internet
FTD
outside
inside
fyusifov-26-3.example.com
ISE
1
VPN Authentication
2
RADIUS Access-Request
3
RADIUS Access-Accept
cisco-av-pair = url-redirect-acl=<Redirect_ALC_Name>
cisco-av-pair = url-redirect=<Redirect URL>
DACL (optional)
Policy Evaluation
Selected policy:
FTD-VPN-Posture-Unknown
4
RADIUS Access-Request/Access-Accept for DACL
5
User redirected to ISE
Posture/Compliance Module downloaded and installed
Posture check triggered and report is sent
6
RADIUS CoA Push with new set of attributes
7
8
Redirect is removed
New set of attributes are applied

1. 원격 사용자가 FTD에 대한 VPN 액세스를 위해 Cisco Anyconnect를 사용합니다.

2. FTD가 해당 사용자에 대한 RADIUS 액세스 요청을 ISE에 전송합니다.

3. 해당 요청이 ISE의 FTD-VPN-Posture-Unknown이라는 정책에 도달합니다. ISE는 세 가지 특성을 가진 RADIUS Access-Accept를 전송합니다.

- cisco-av-pair = url-redirect-acl=fyusifovredirect - FTD에 로컬로 정의된 ACL(Access Control List) 이름으로, 리디렉션되는 트래픽을 결정합니다.
- cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp - 원격 사용자가 리디렉션되는 URL입니다.
- DACL = PERMIT_ALL_IPV4_TRAFFIC - 다운로드 가능한 ACL 이 속성은 선택 사항입니다. 이 시나리오에서는 모든 트래픽이 DACL에서 허용됨)

4. DACL이 전송 된 경우, RADIUS 액세스 요청/액세스 수락 DACL의 내용을 다운로드 하기 위해 교환 됩니다

5. VPN 사용자의 트래픽이 로컬로 정의된 ACL과 일치하면 ISE 클라이언트 프로비저닝 포털로 리디렉션됩니다. ISE는 AnyConnect Posture Module 및 Compliance Module을 프로비저닝합니다.

6. 에이전트는 클라이언트 시스템에 설치된 후 프로브를 사용하여 ISE를 자동으로 검색합니다. ISE가 성공적으로 탐지되면 엔드포인트에서 포스처 요건이 점검됩니다. 이 예에서 에이전트는 설

치된 모든 안티멀웨어 소프트웨어를 확인합니다. 그런 다음 ISE에 상태 보고서를 보냅니다.

7. ISE가 에이전트로부터 포스처 보고서를 수신하면 ISE는 이 세션에 대한 포스처 상태를 변경하고 RADIUS CoA 유형 Push를 새 속성으로 트리거합니다. 이번에는 포스처 상태를 알고 다른 규칙을 맞춥니다.

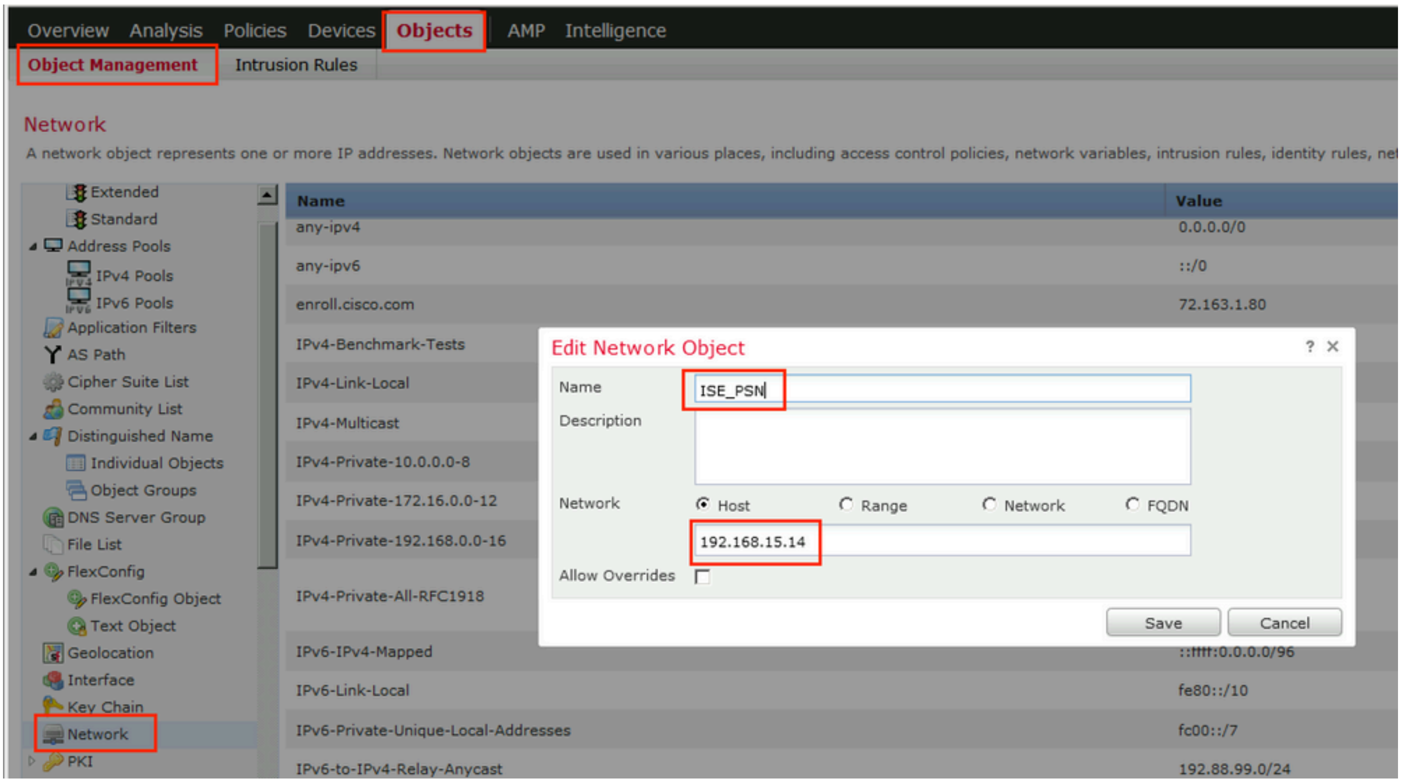
- 사용자가 규정을 준수하는 경우 전체 액세스를 허용하는 DACL 이름이 전송됩니다.
- 사용자가 규정을 준수하지 않으면 제한된 액세스를 허용하는 DACL 이름이 전송됩니다.

8. FTD에서 리디렉션을 제거합니다. FTD는 ISE에서 DACL을 다운로드하기 위해 Access-Request를 전송합니다. 특정 DACL은 VPN 세션에 연결됩니다.

설정

FTD/FMC

1단계. ISE 및 리미디에이션 서버에 대한 네트워크 객체 그룹을 생성합니다(있는 경우). Objects(개체) > Object Management(개체 관리) > Network(네트워크)로 이동합니다.



Network

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, net

Name	Value
any-ipv4	0.0.0.0/0
any-ipv6	::/0
enroll.cisco.com	72.163.1.80
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	::ffff:0.0.0.0/96
IPv6-Link-Local	fe80::/10
IPv6-Private-Unique-Local-Addresses	fc00::/7
IPv6-to-IPv4-Relay-Anycast	192.88.99.0/24

Edit Network Object

Name: ISE_PSN

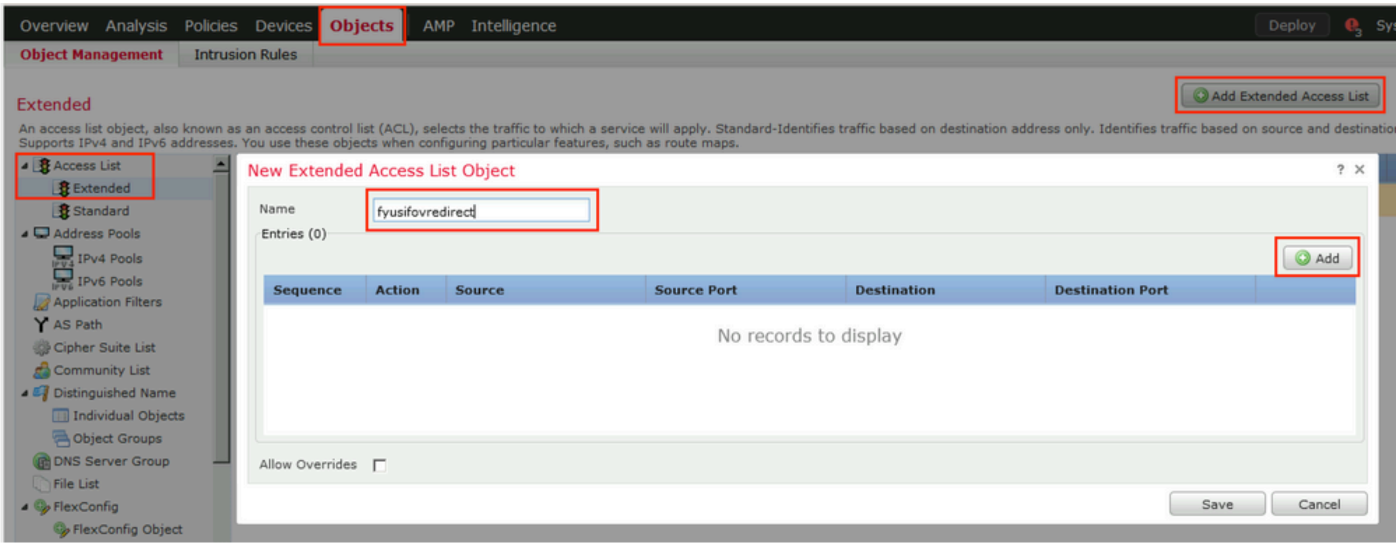
Description:

Network: ● Host ○ Range ○ Network ○ FQDN

192.168.15.14

Allow Overrides □

2단계. 리디렉션 ACL을 생성합니다. Objects(개체) > Object Management(개체 관리) > Access List(액세스 목록) > Extended(확장)로 이동합니다. Add Extended Access List(확장 액세스 목록 추가)를 클릭하고 리디렉션 ACL의 이름을 제공합니다. 이 이름은 ISE 권한 부여 결과와 동일해야 합니다.



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 address only. Identifies traffic based on source and destinatio
Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

New Extended Access List Object

Name: fyusifovredirect

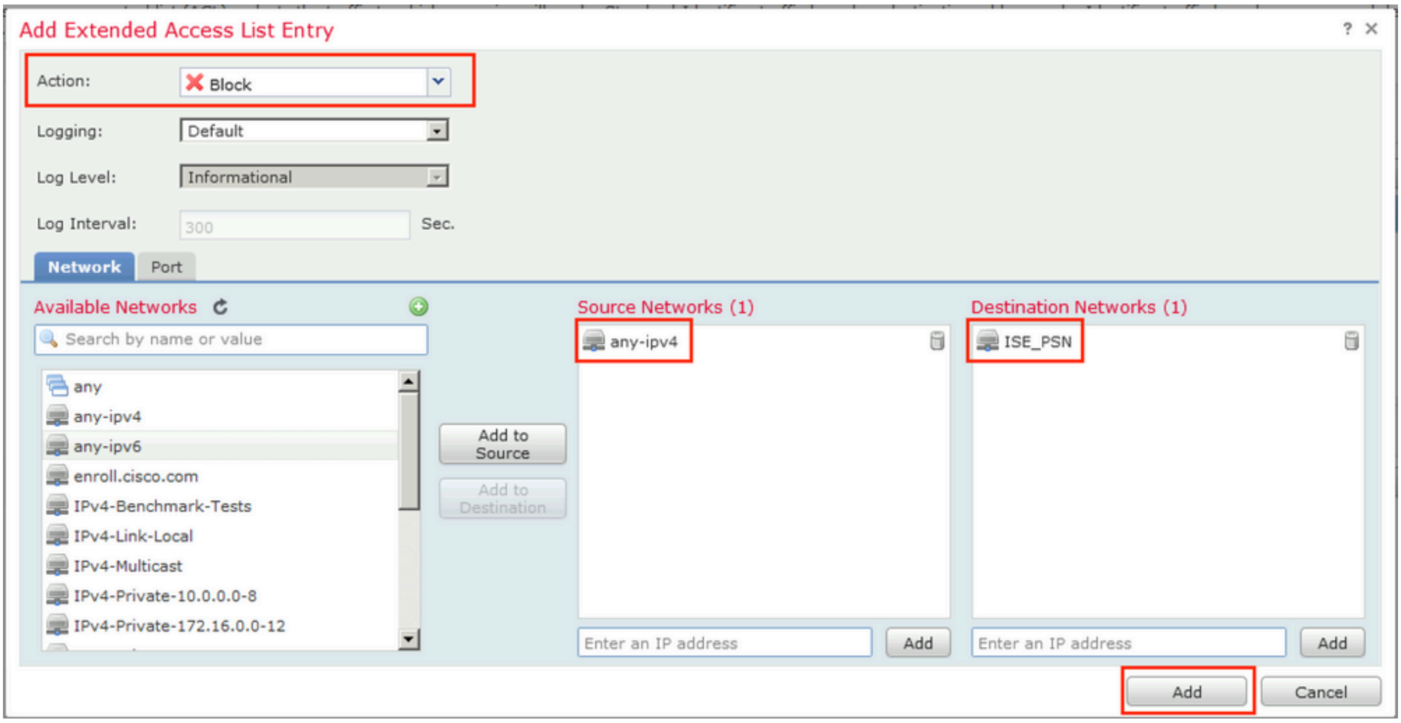
Entries (0)

Sequence	Action	Source	Source Port	Destination	Destination Port

No records to display

Allow Overrides ☐

3단계. 리디렉션 ACL 항목을 추가합니다. Add(추가) 버튼을 클릭합니다. 리디렉션에서 제외하기 위해 DNS, ISE 및 리미디에이션 서버에 대한 트래픽을 차단합니다. 나머지 트래픽을 허용하면 리디렉션이 트리거됩니다(필요한 경우 ACL 항목이 더 구체화될 수 있음).



Add Extended Access List Entry

Action: Block

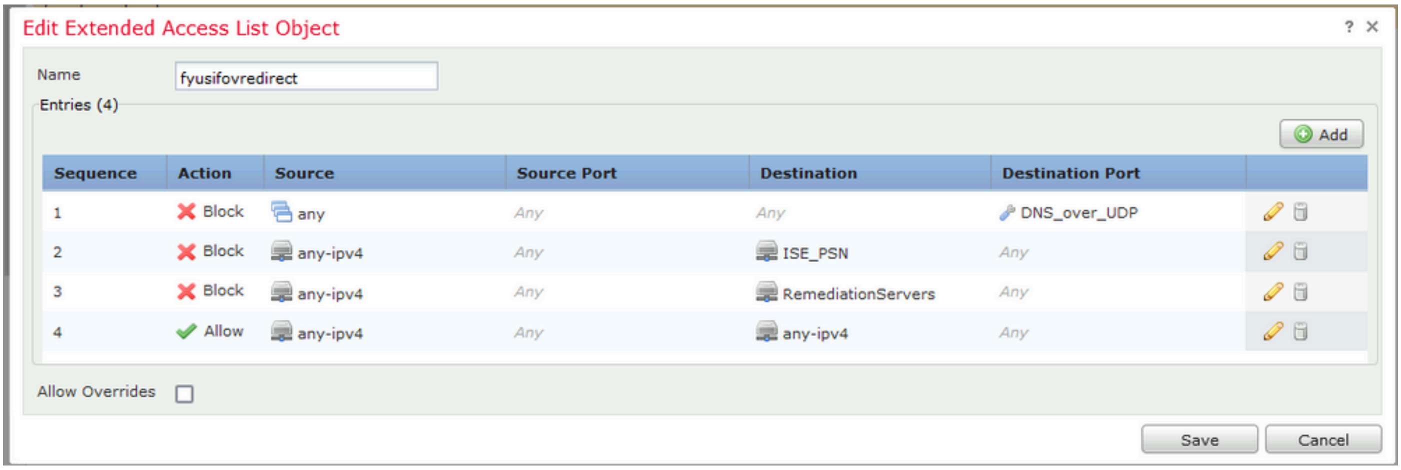
Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Source Networks (1): any-ipv4

Destination Networks (1): ISE_PSN



Edit Extended Access List Object

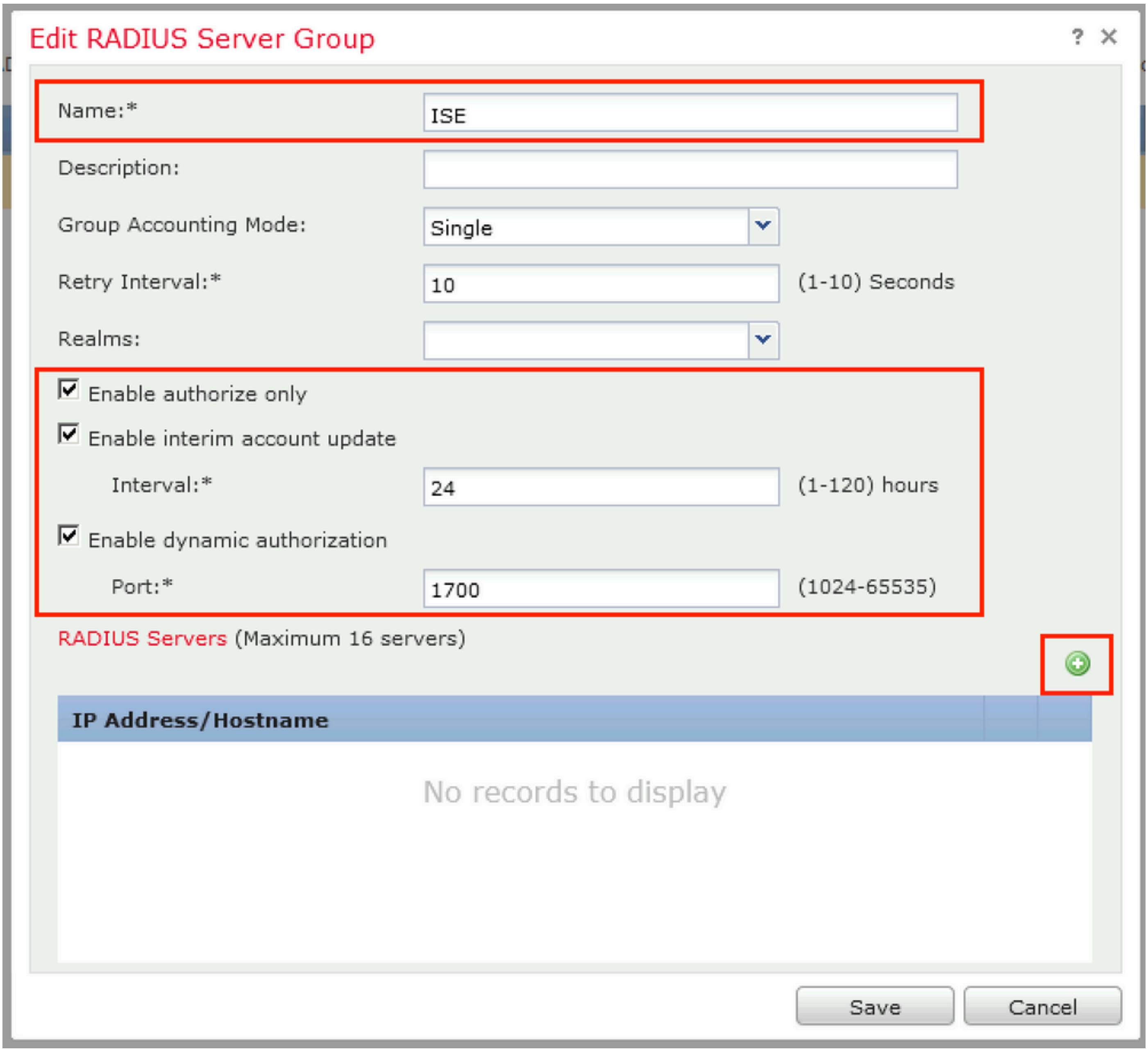
Name: fyusifovredirect

Entries (4)

Sequence	Action	Source	Source Port	Destination	Destination Port	
1	✗ Block	any	Any	Any	DNS_over_UDP	✎ 🗑
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 □

4단계. ISE PSN 노드/노드를 추가합니다. Objects(개체) > Object Management(개체 관리) > RADIUS Server Group(RADIUS 서버 그룹)으로 이동합니다. Add RADIUS Server Group(RADIUS 서버 그룹 추가)을 클릭한 다음 이름을 입력하고 check all(모두 선택) 확인란을 활성화한 다음 더하기 아이콘을 클릭합니다.



Edit RADIUS Server Group

Name:*	ISE
Description:	
Group Accounting Mode:	Single
Retry Interval:*	10 (1-10) Seconds
Realms:	

☑ Enable authorize only

☑ Enable interim account update

Interval:* 24 (1-120) hours

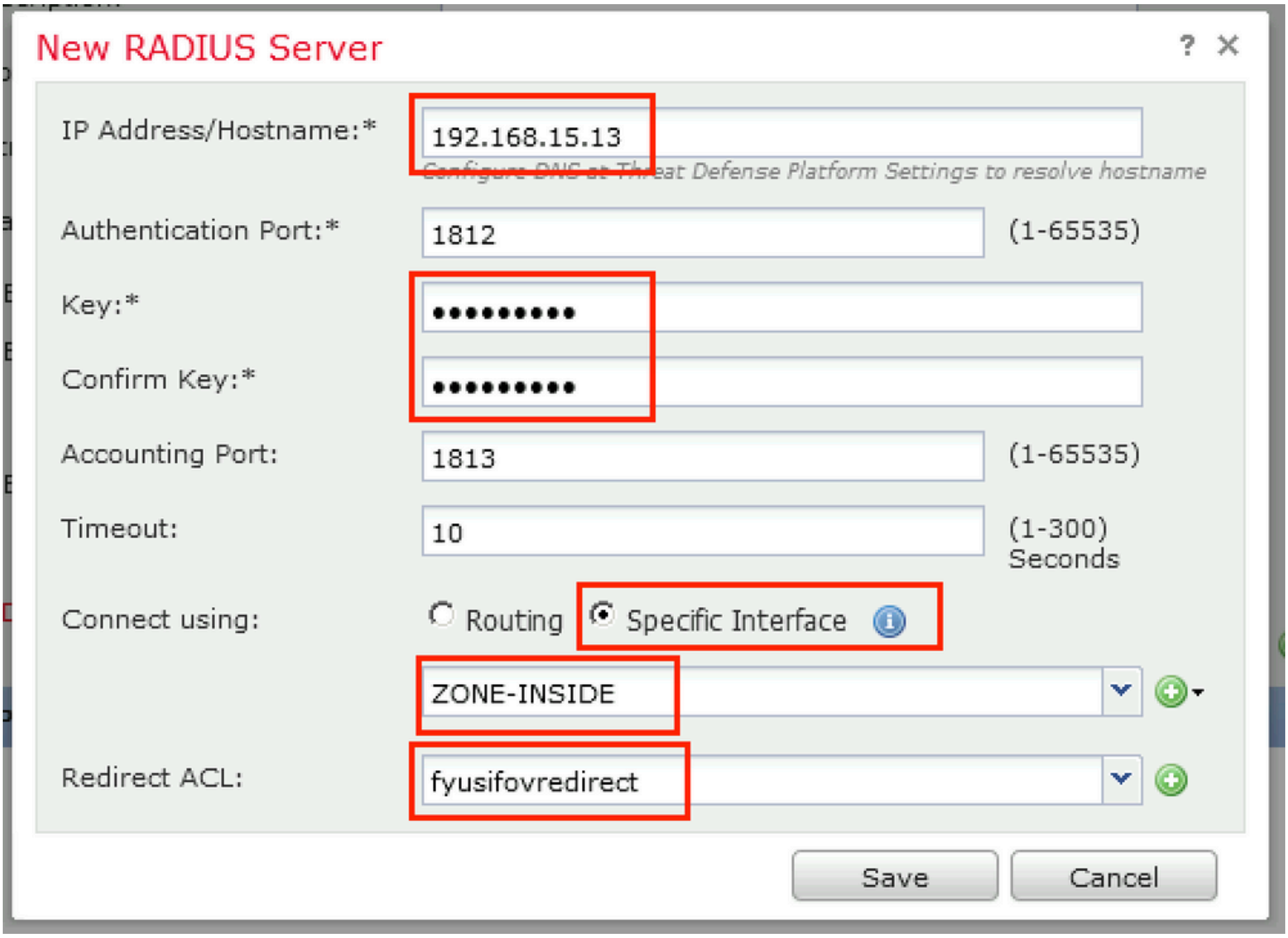
☑ Enable dynamic authorization

Port:* 1700 (1024-65535)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

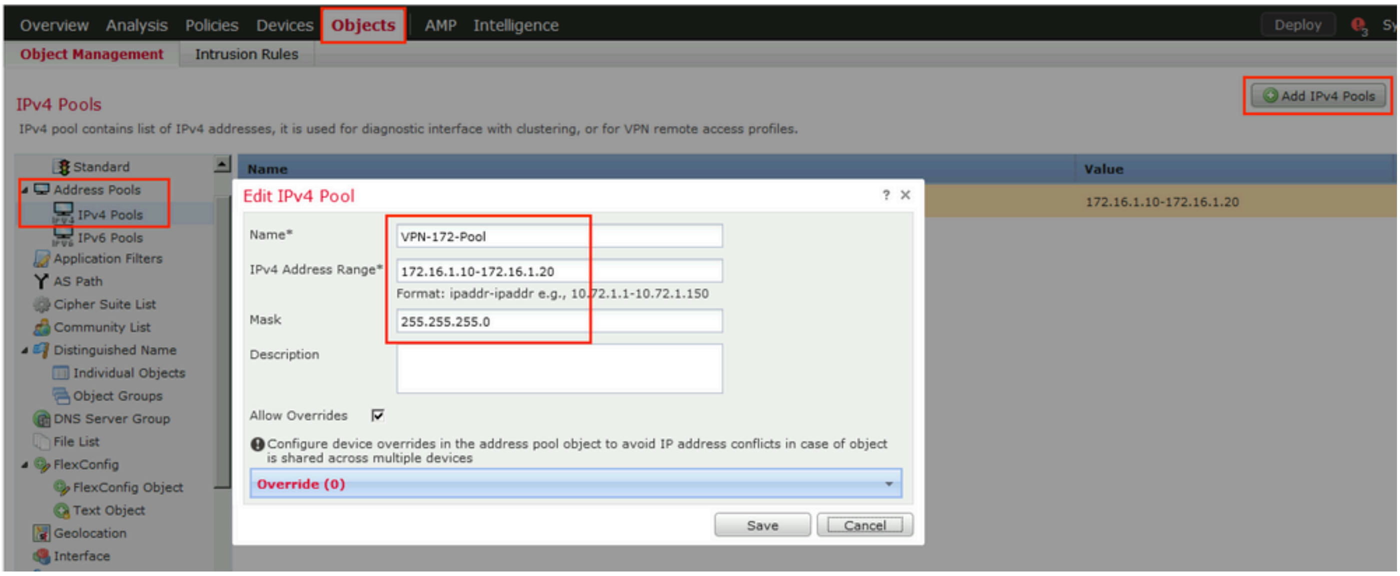
5단계. 열린 창에서 ISE PSN IP 주소, RADIUS 키를 제공하고 Specific Interface를 선택한 다음 ISE에 연결할 수 있는 인터페이스(이 인터페이스는 RADIUS 트래픽의 소스로 사용됨)를 선택한 다음 이전에 구성된 Redirect ACL을 선택합니다.



New RADIUS Server

IP Address/Hostname:*	192.168.15.13 Configure DNS at Threat Defense Platform Settings to resolve hostname	
Authentication Port:*	1812	(1-65535)
Key:*	●●●●●●●●●	
Confirm Key:*	●●●●●●●●●	
Accounting Port:	1813	(1-65535)
Timeout:	10	(1-300) Seconds
Connect using:	○ Routing ● Specific Interface	
	ZONE-INSIDE	
Redirect ACL:	fyusifovredirect	

6단계. VPN 사용자를 위한 주소 풀을 생성합니다. Objects(개체) > Object Management(개체 관리) > Address Pools(주소 풀) > IPv4 Pools(IPv4 풀)로 이동합니다. Add IPv4 Pools(IPv4 풀 추가)를 클릭하고 세부 정보를 입력합니다.



IPv4 Pools

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

Name	Value
	172.16.1.10-172.16.1.20

Edit IPv4 Pool

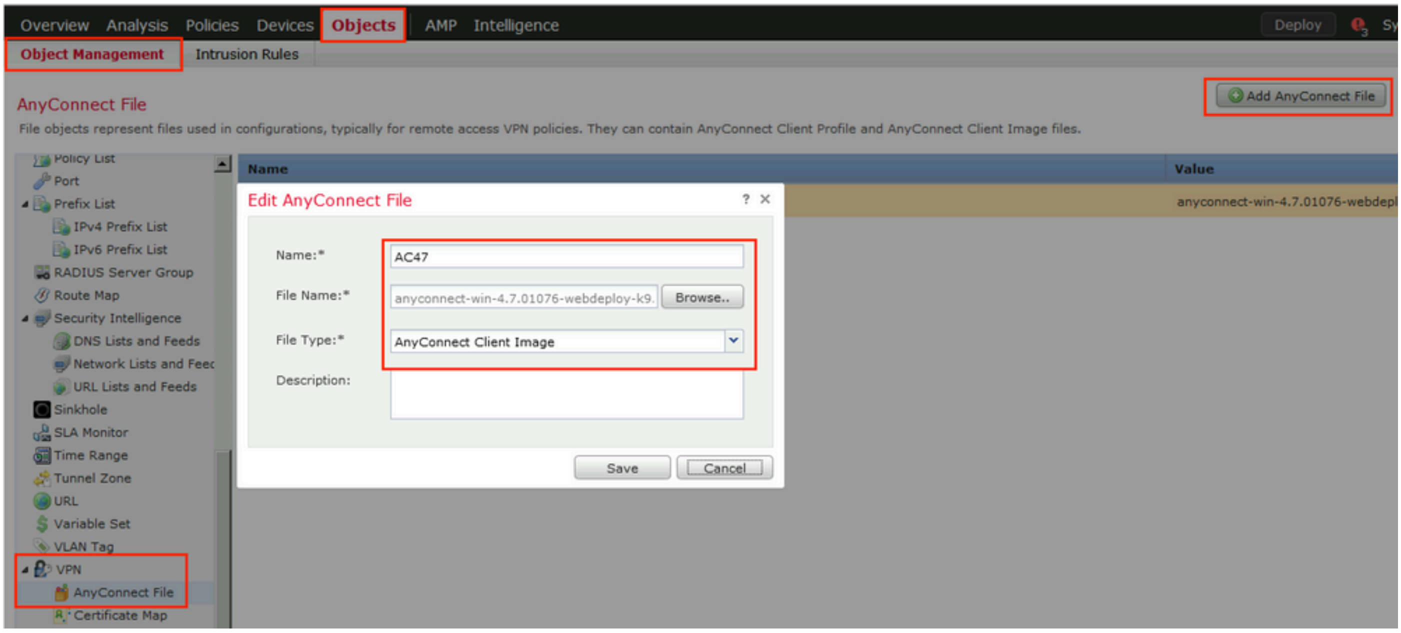
Name*	VPN-172-Pool
IPv4 Address Range*	172.16.1.10-172.16.1.20 Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150
Mask	255.255.255.0
Description	
Allow Overrides	☑

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

Override (0)

7단계. AnyConnect 패키지를 만듭니다. Objects(개체) > Object Management(개체 관리) > VPN >

AnyConnect File(AnyConnect 파일)로 이동합니다. Add AnyConnect File(AnyConnect 파일 추가)을 클릭하고 패키지 이름을 제공한 다음 Cisco Software Download(Cisco 소프트웨어 다운로드)에서 패키지를 다운로드하고 Anyconnect Client Image File Type(Anyconnect 클라이언트 이미지 파일 유형)을 선택합니다.



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 files.

Value: anyconnect-win-4.7.01076-webdepl

Edit AnyConnect File

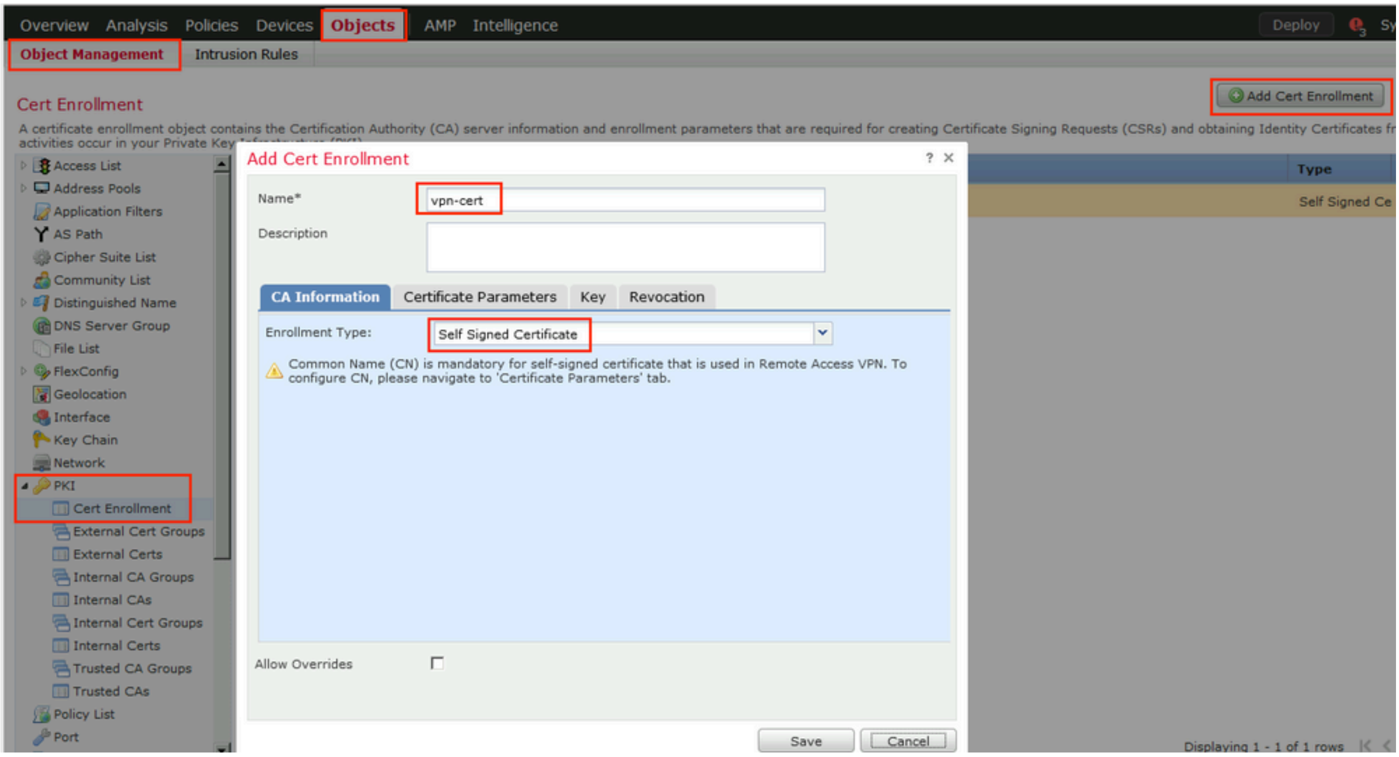
Name:* AC47

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

File Type:* AnyConnect Client Image

Description:

8단계. Certificate Objects(인증서 객체) > Object Management(객체 관리) > PKI > Cert Enrollment(인증서 등록)로 이동합니다. Add Cert Enrollment(인증서 등록 추가)를 클릭하고 이름을 입력한 다음 Enrollment Type(등록 유형)에서 Self Signed Certificate(자체 서명 인증서)를 선택합니다. Certificate Parameters(인증서 매개변수) 탭을 클릭하고 CN을 제공합니다.



Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates fr activities occur in your Private Key Infrastructure (PKI).

Type: Self Signed Ce

Add Cert Enrollment

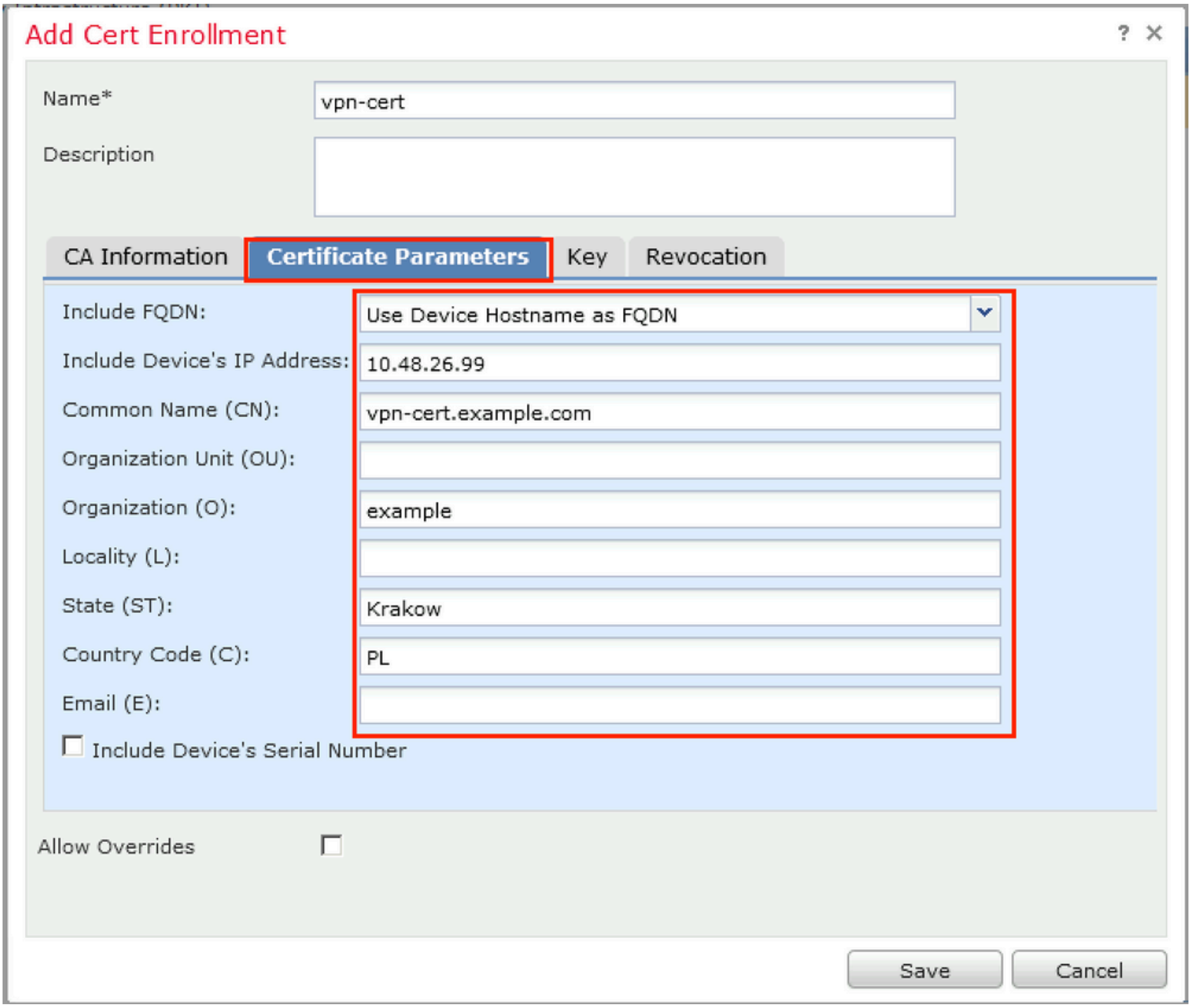
Name* vpn-cert

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

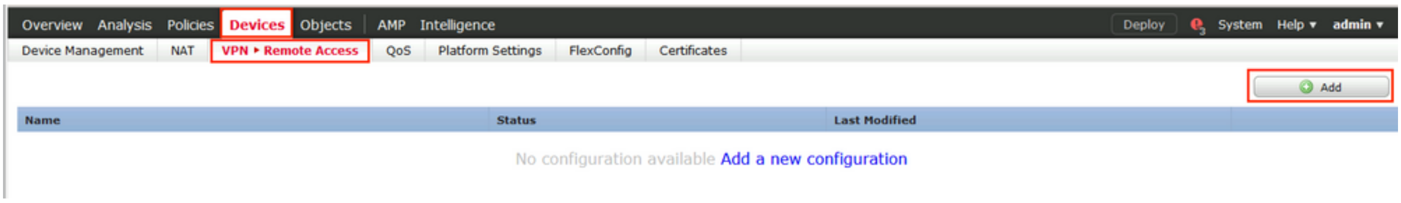
Name*	vpn-cert
Description	

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 ☐

9단계. 원격 액세스 VPN 마법사를 시작합니다. Devices(디바이스) > VPN > Remote Access(원격 액세스)로 이동하고 Add(추가)를 클릭합니다.

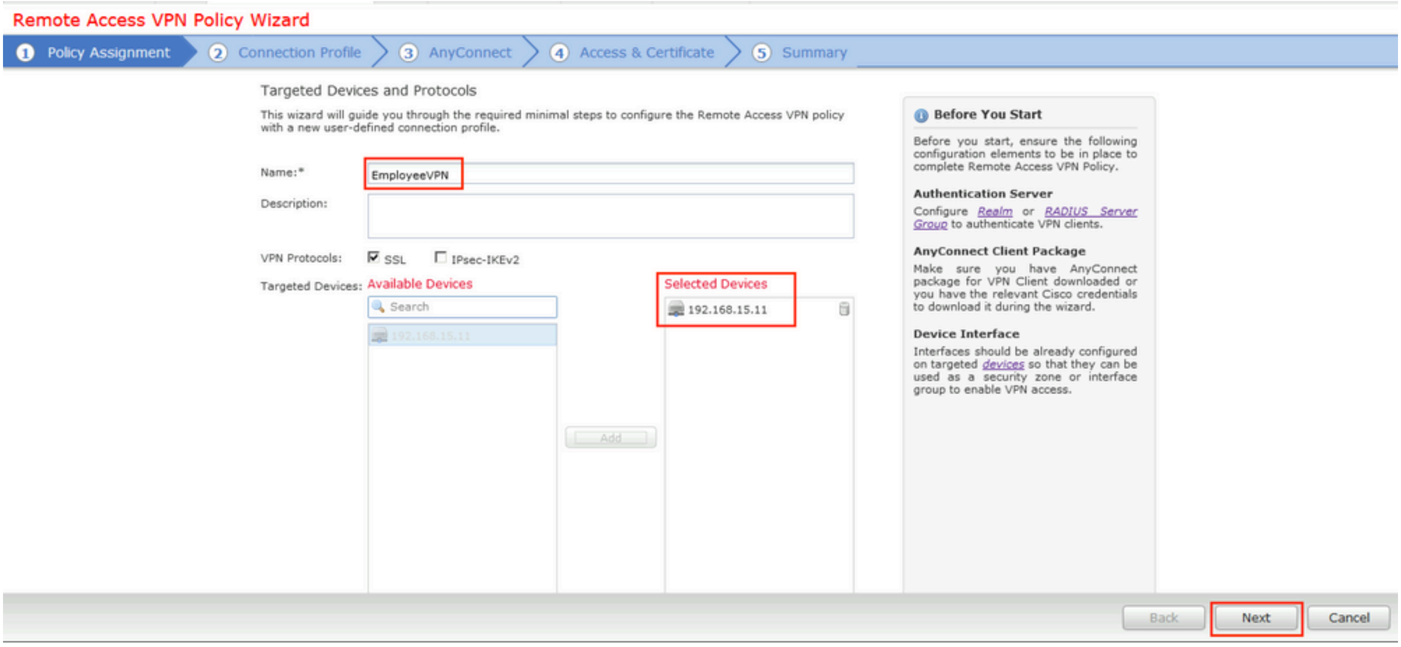


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▸ Remote Access QoS Platform Settings FlexConfig Certificates
Add

Name	Status	Last Modified

No configuration available Add a new configuration

10단계. 이름을 입력하고 SSL을 VPN Protocol(VPN 프로토콜)로 선택하고 VPN Concentrator로 사용되는 FTD를 선택한 후 Next(다음)를 클릭합니다.



Targeted Devices and Protocols

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

Name:* EmployeeVPN

Description:

VPN Protocols: ☑ SSL □ IPsec-IKEv2

Targeted Devices: Available Devices 192.168.15.11 | Selected Devices 192.168.15.11

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure Realm or RADIUS Server Group to authenticate VPN clients.

AnyConnect Client Package

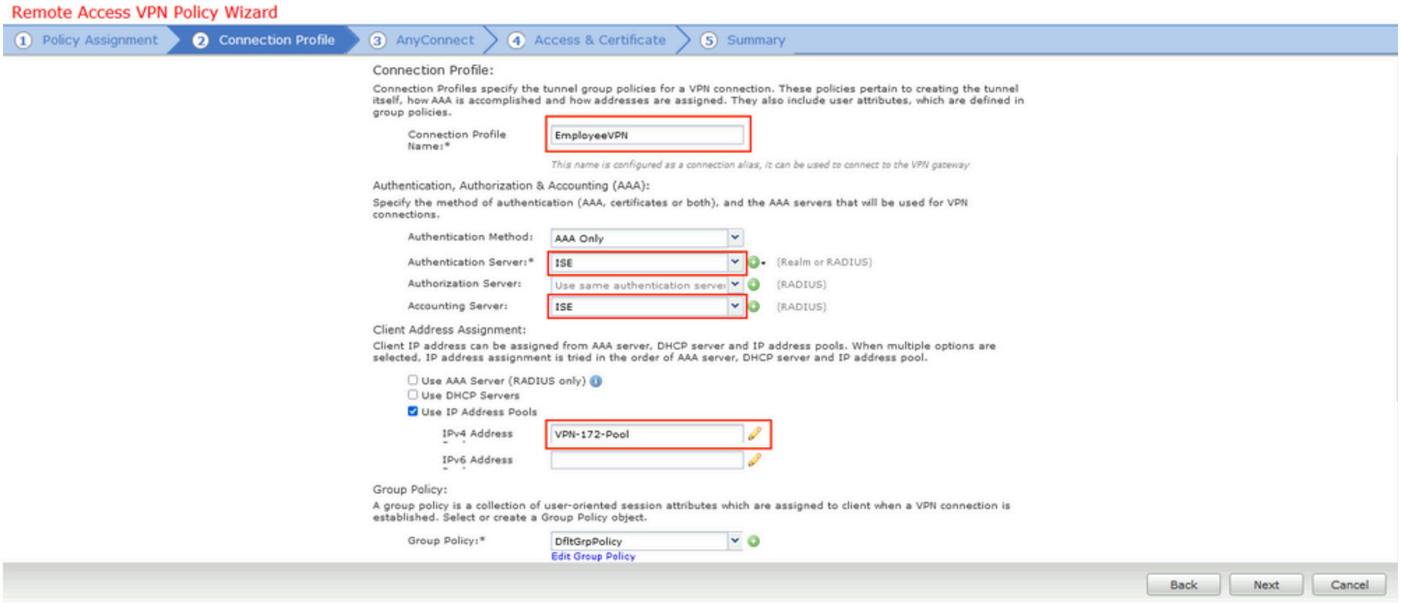
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

11단계. Connection Profile name(연결 프로파일 이름)을 입력하고 Authentication/Accounting Servers(인증/어카운팅 서버)를 선택한 다음 이전에 구성한 주소 풀을 선택하고 Next(다음)를 클릭합니다.

참고: 권한 부여 서버를 선택하지 마십시오. 단일 사용자에 대해 두 개의 액세스 요청을 트리거합니다(사용자 비밀번호로 한 번, 비밀번호 cisco로 두 번).



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:

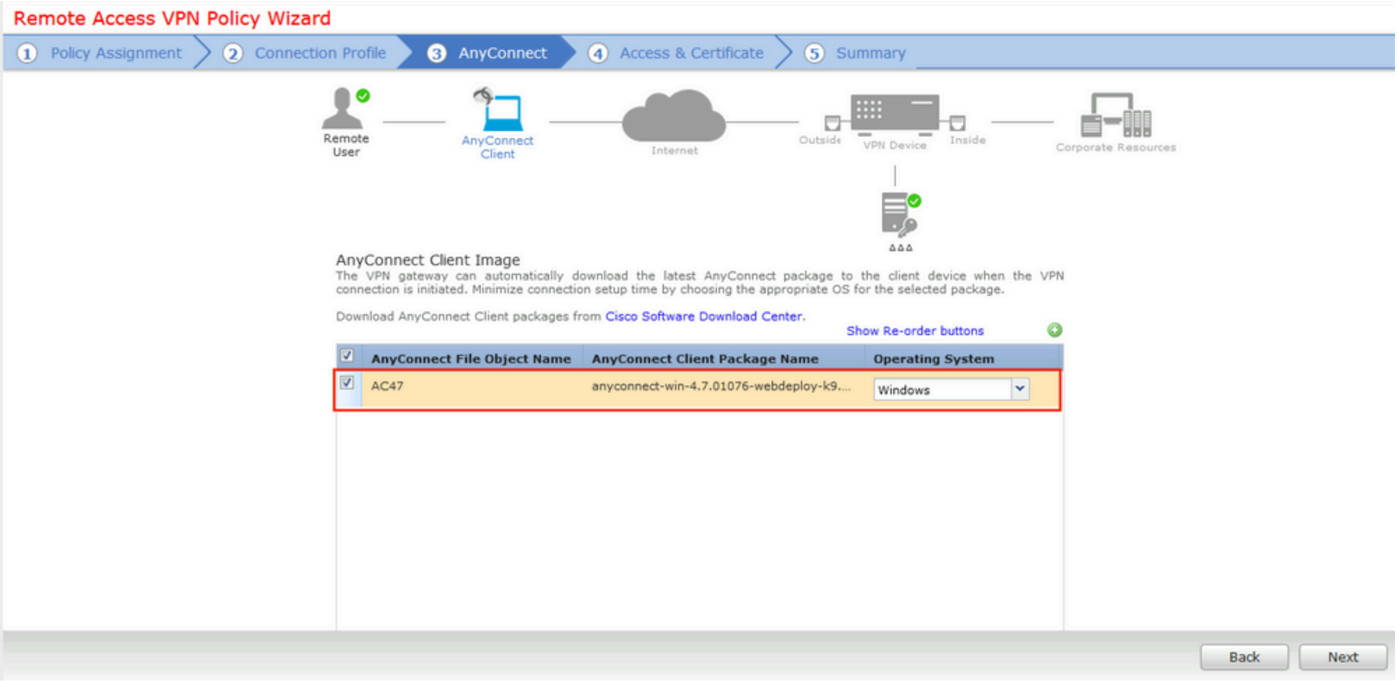
Group Policy:

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

12단계. 이전에 구성된 AnyConnect 패키지를 선택하고 Next(다음)를 클릭합니다.



Remote Access VPN Policy Wizard

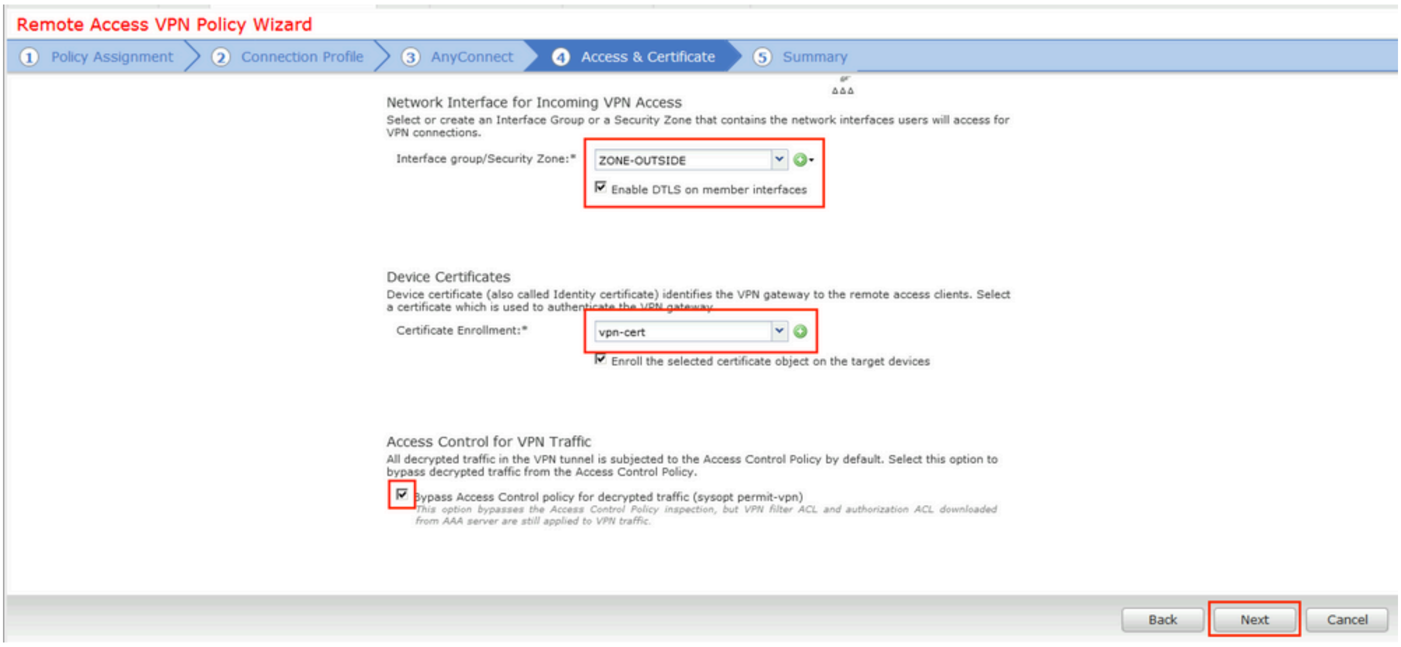
AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN 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

13단계. VPN 트래픽이 예상되는 인터페이스를 선택하고 이전에 구성된 Certificate Enrollment를 선택한 후 Next(다음)를 클릭합니다.



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

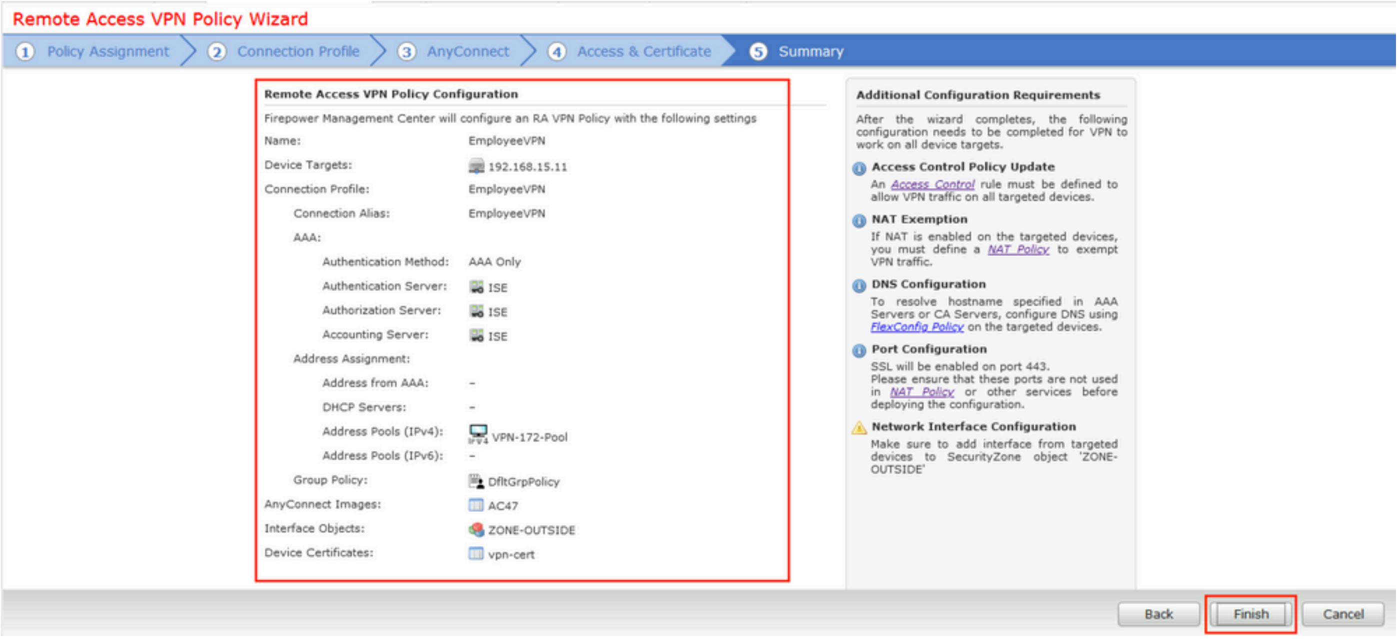
Access Control for VPN Traffic

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.

14단계. 요약 페이지를 확인하고 마침을 클릭합니다.



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 Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

Access Control Policy Update
An Access Control rule must be defined to allow VPN traffic on all targeted devices.

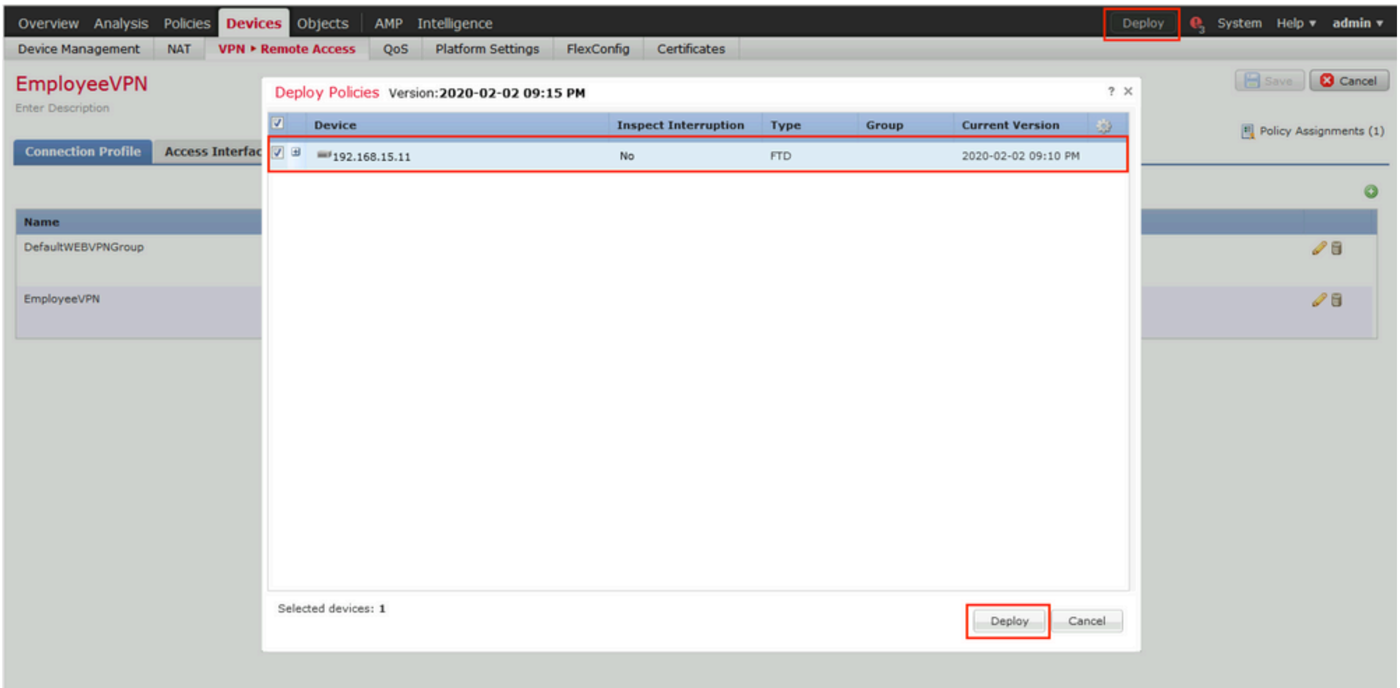
NAT Exemption
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.

DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.

Port Configuration
SSL will be enabled on port 443.
Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

Network Interface Configuration
Make sure to add interface from targeted devices to SecurityZone object 'ZONE-OUTSIDE'

15단계. FTD에 컨피그레이션 구축 Deploy(구축)를 클릭하고 VPN Concentrator로 사용되는 FTD를 선택합니다.



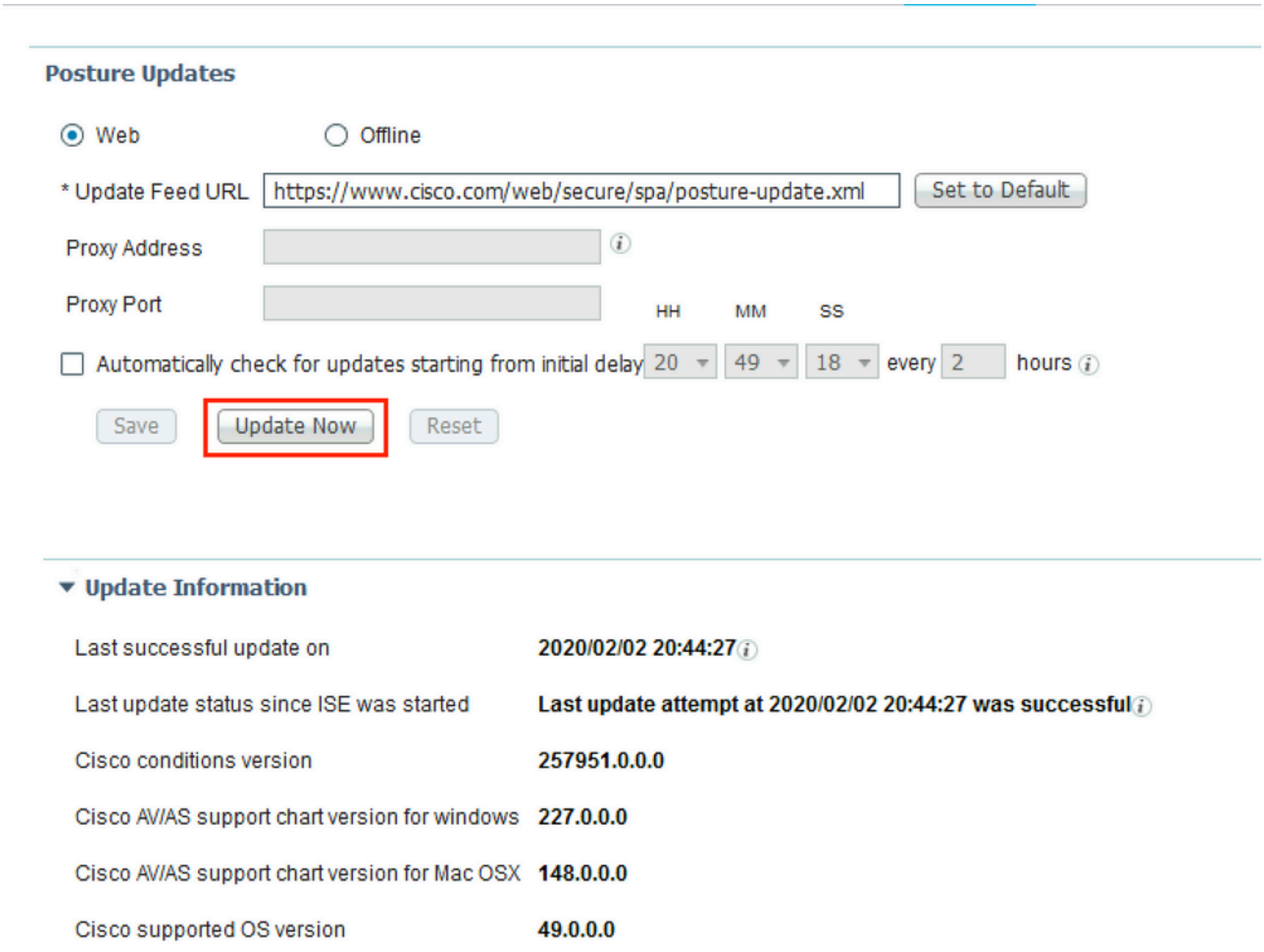
Deploy Policies Version:2020-02-02 09:15 PM

☑	Device	Inspect Interruption	Type	Group	Current Version
☑ ⊞	192.168.15.11	No	FTD		2020-02-02 09:10 PM

Selected devices: 1

ISE

1단계. 상태 업데이트를 실행 합니다. Administration(관리) > System(시스템) > Settings(설정) > Posture(상태) > Updates(업데이트)로 이동합니다.



Posture Updates

● Web ○ Offline

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

Proxy Address:

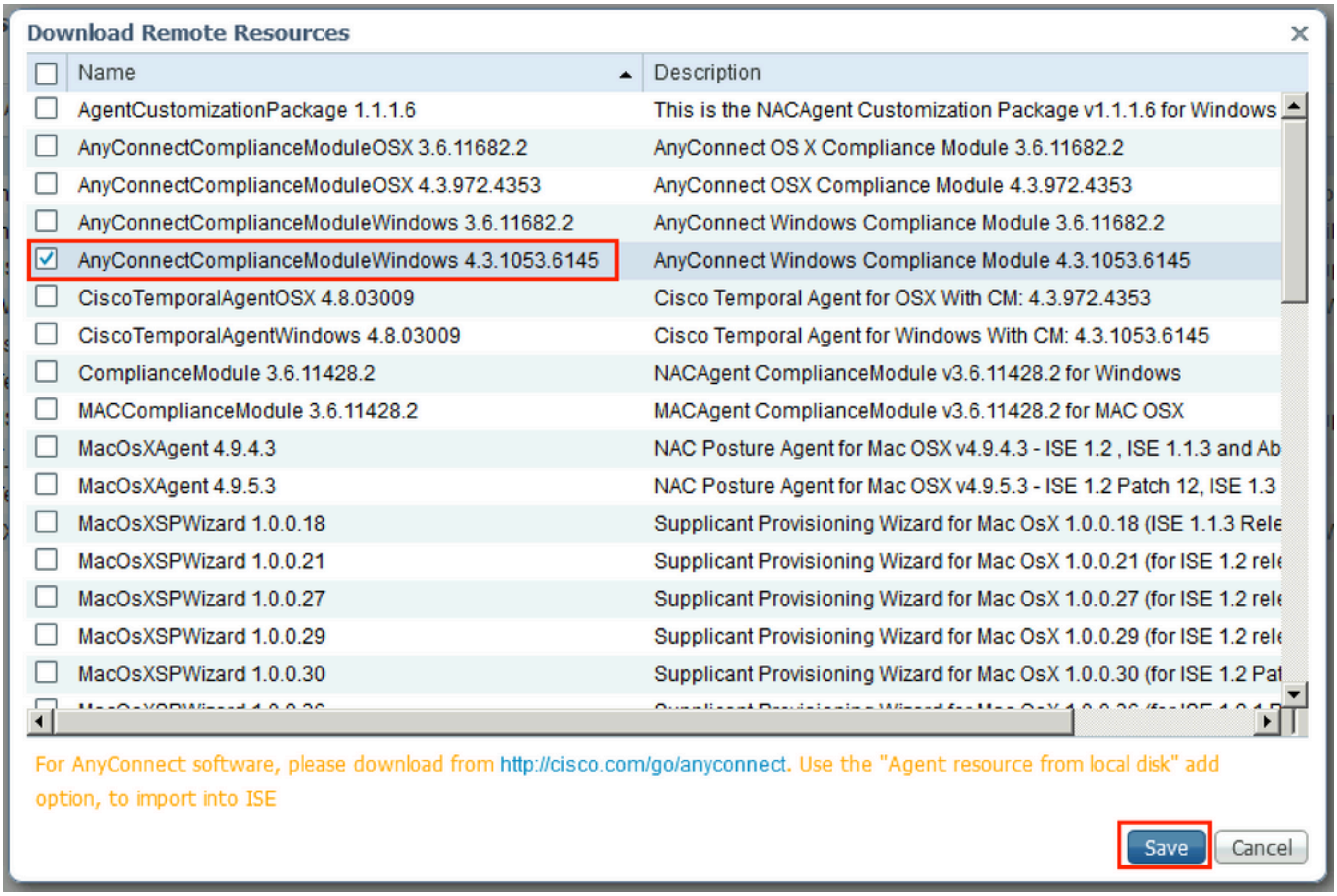
Proxy Port:

□ Automatically check for updates starting from initial delay HH 20 MM 49 SS 18 every 2 hours

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 20:44:27 was successful**
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**

2단계. Upload Compliance Module(규정 준수 모듈 업로드). Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동합니다. Add(추가)를 클릭하고 Cisco 사이트에서 Agent resources(에이전트 리소스)를 선택합니다



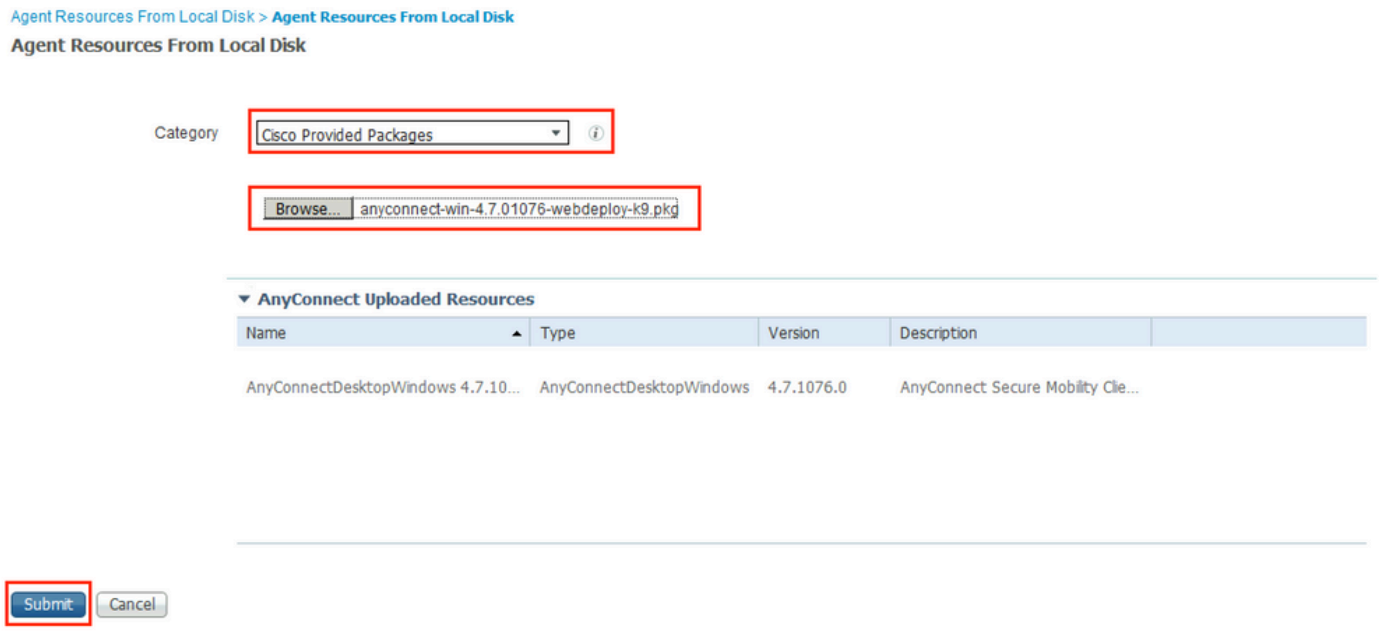
Download Remote Resources

☐	Name	Description
☐	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
☐	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2
☐	AnyConnectComplianceModuleOSX 4.3.972.4353	AnyConnect OSX Compliance Module 4.3.972.4353
☐	AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance Module 3.6.11682.2
☑	AnyConnectComplianceModuleWindows 4.3.1053.6145	AnyConnect Windows Compliance Module 4.3.1053.6145
☐	CiscoTemporalAgentOSX 4.8.03009	Cisco Temporal Agent for OSX With CM: 4.3.972.4353
☐	CiscoTemporalAgentWindows 4.8.03009	Cisco Temporal Agent for Windows With CM: 4.3.1053.6145
☐	ComplianceModule 3.6.11428.2	NACAgent ComplianceModule v3.6.11428.2 for Windows
☐	MACComplianceModule 3.6.11428.2	MACAgent ComplianceModule v3.6.11428.2 for MAC OSX
☐	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Ab
☐	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3
☐	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Rele
☐	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 rel
☐	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 rel
☐	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 rel
☐	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE 1.2 Pat
☐	MacOsXSPWizard 1.0.0.36	Supplicant Provisioning Wizard for Mac OsX 1.0.0.36 (for ISE 1.2 P

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

3단계. Cisco Software Download에서 AnyConnect를 다운로드한 다음 ISE에 업로드합니다. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동합니다.

Add(추가)를 클릭하고 Agent Resources From Local Disk(로컬 디스크의 에이전트 리소스)를 선택합니다. Category(카테고리)에서 Cisco Provided Packages(Cisco 제공 패키지)를 선택하고 AnyConnect package from local disk(로컬 디스크에서 AnyConnect 패키지)를 선택한 후 Submit(제출)을 클릭합니다.



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

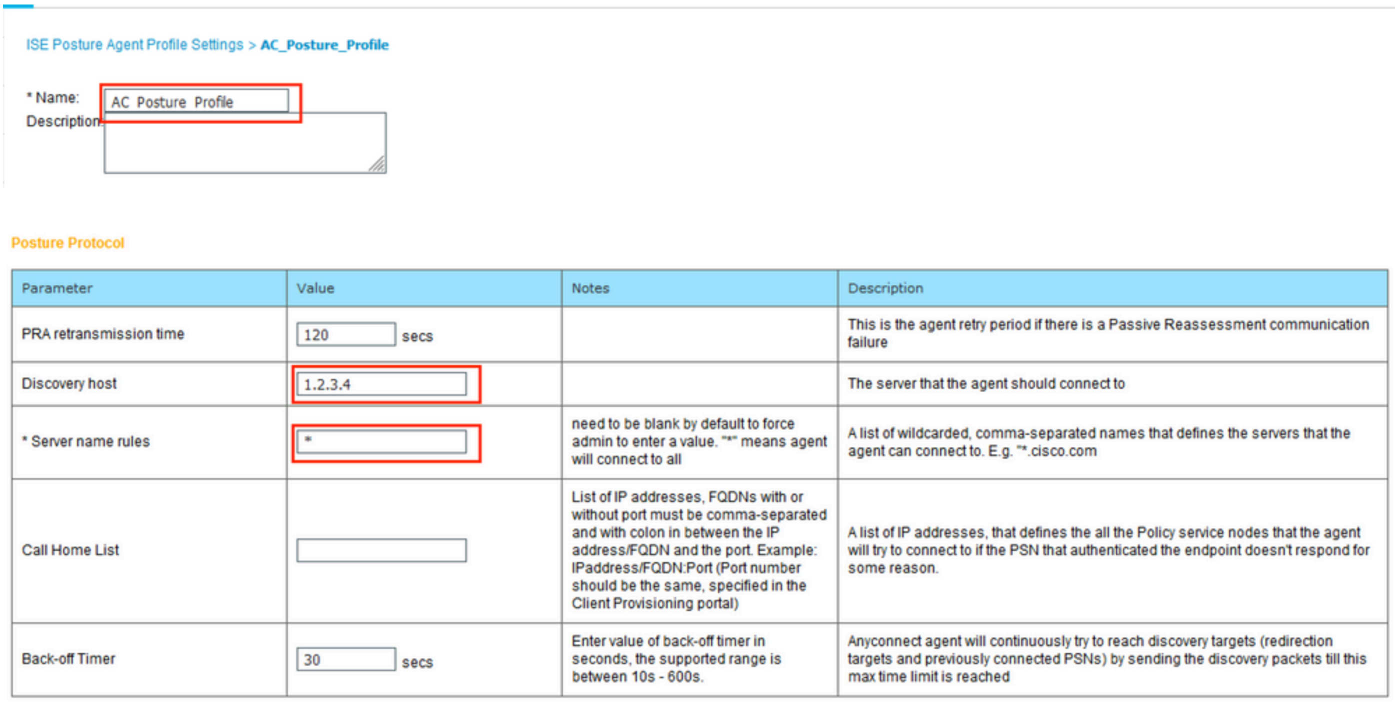
AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.7.10...	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secure Mobility Clie...

4단계. AnyConnect Posture 프로파일을 생성합니다. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동합니다.

Add(추가)를 클릭하고 AnyConnect Posture Profile(AnyConnect 포스처 프로파일)을 선택합니다. 이름과 Posture Protocol을 입력합니다.

*Server name 규칙 아래에는 *를 입력하고 Discovery host 아래에 임의의 더미 IP 주소를 입력합니다.



ISE Posture Agent Profile Settings > **AC_Posture_Profile**

* Name: AC_Posture_Profile

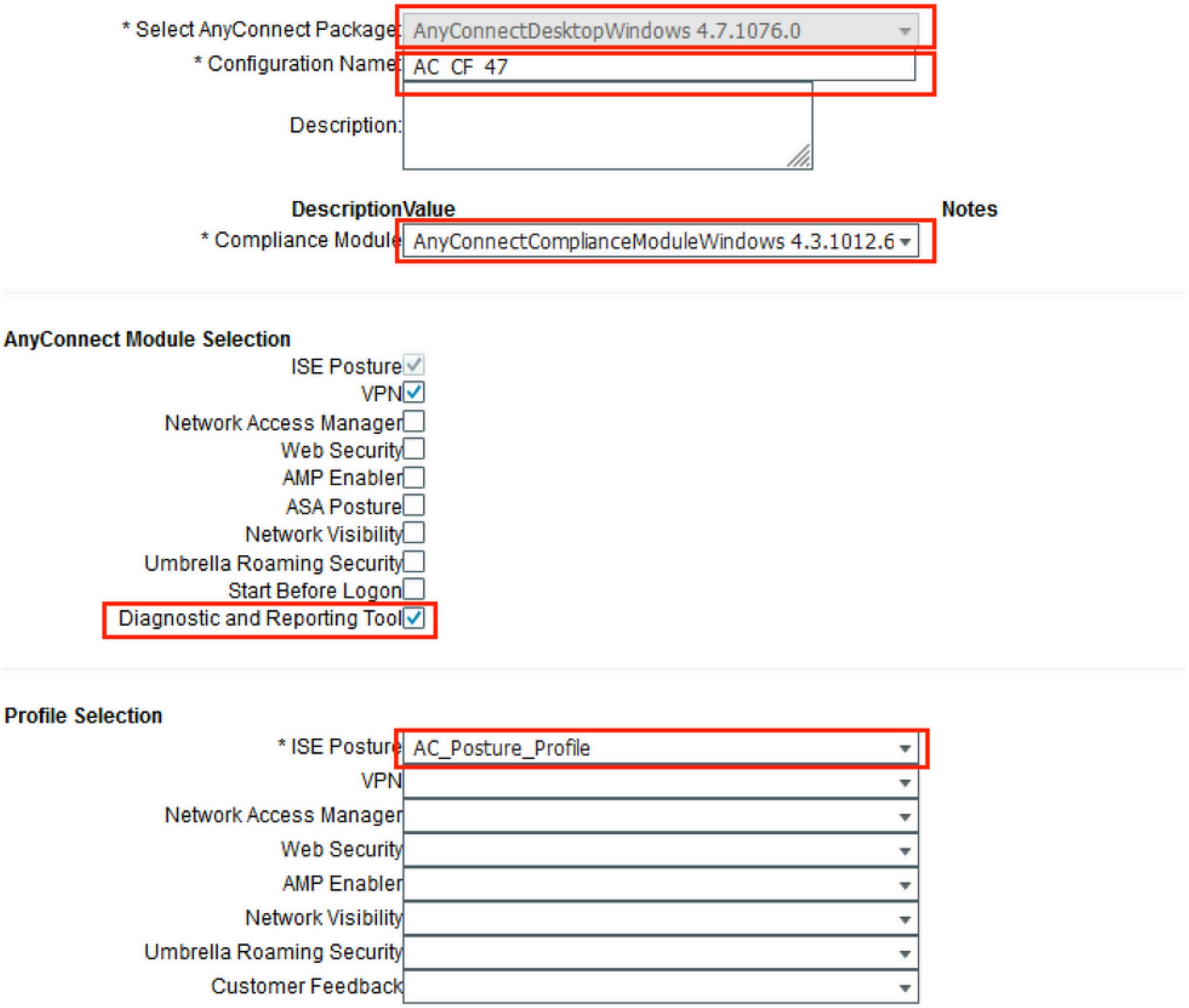
Description:

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host	1.2.3.4		The server that the agent should connect to
* 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-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com
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 defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for 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 continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

5단계. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하여 AnyConnect 컨피그레이션을 생성합니다. Add(추가)를 클릭하고 AnyConnect Configuration(AnyConnect 컨피그레이션)을 선택합니다. AnyConnect

Package(AnyConnect 패키지)를 선택하고 Configuration Name(컨피그레이션 이름)을 제공하며 Compliance Module(컴플라이언스 모듈)을 선택하고 Diagnostic and Reporting Tool(진단 및 보고 툴)을 선택한 다음 Posture Profile(포스처 프로파일)을 선택하고 Save(저장)를 클릭합니다.



* Select AnyConnect Package: AnyConnectDesktopWindows 4.7.1076.0

* Configuration Name: AC_CF_47

Description:

Description	Value	Notes
* Compliance Module	AnyConnectComplianceModuleWindows 4.3.1012.6	

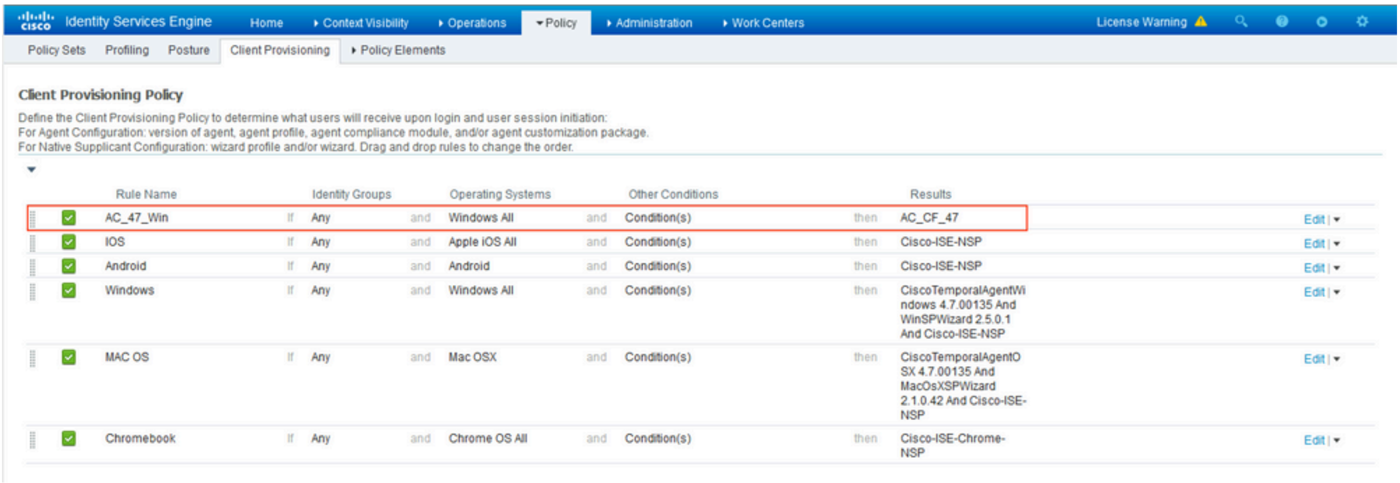
AnyConnect Module Selection

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:

6단계. Policy(정책) > Client Provisioning(클라이언트 프로비저닝)으로 이동하고 Client Provisioning Policy(클라이언트 프로비저닝 정책)를 생성합니다. Edit(편집)를 클릭한 다음 Insert Rule Above(위에 규칙 삽입)를 선택하고, 이름을 입력하고, OS를 선택한 다음 이전 단계에서 생성한 AnyConnect Configuration(AnyConnect 컨피그레이션)을 선택합니다.



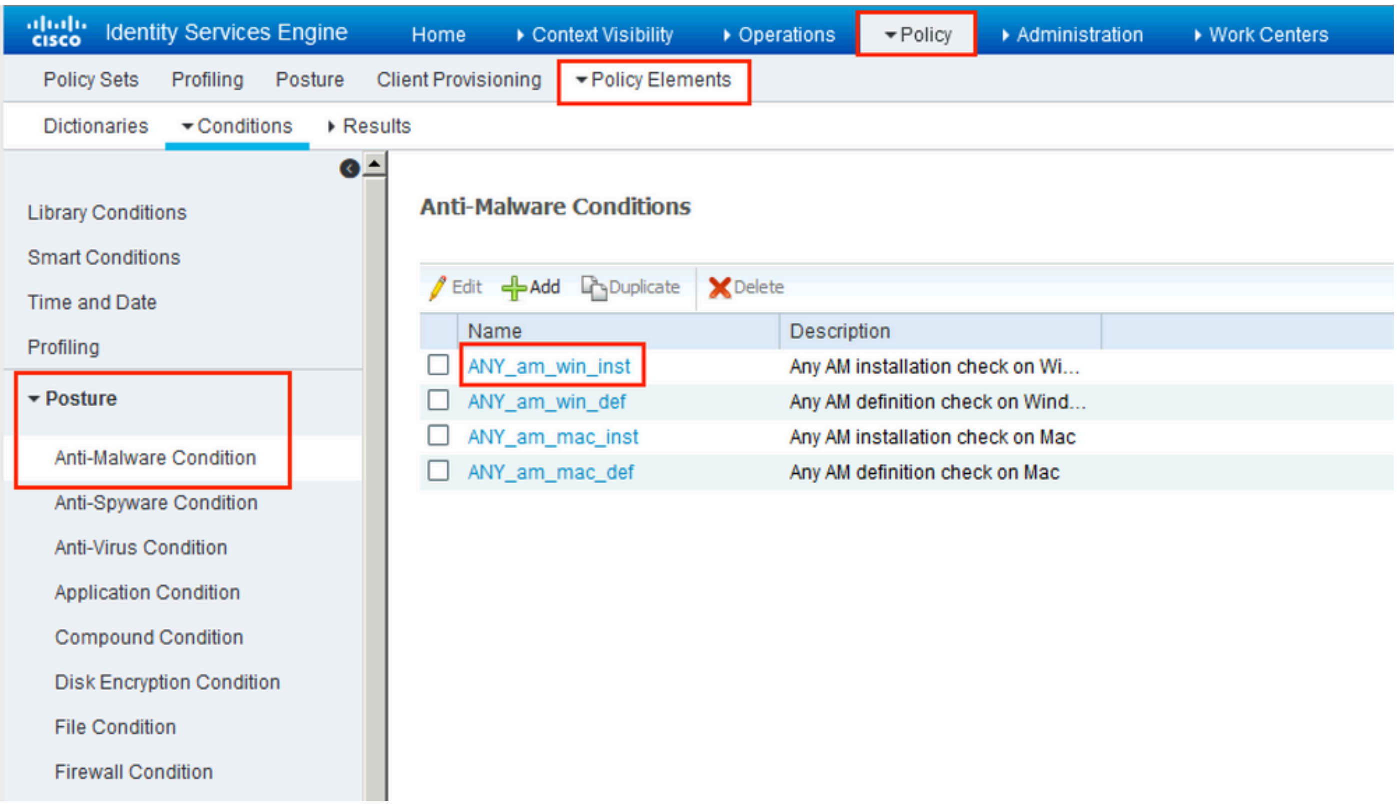
Client Provisioning Policy

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	Edit | ▾
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	Cisco-ISE-NSP	Edit | ▾
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	Edit | ▾
☑	Windows	If	Any	and	Windows All	and	Condition(s)	then	CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP	Edit | ▾
☑	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	Edit | ▾
☑	Chromebook	If	Any	and	Chrome OS All	and	Condition(s)	then	Cisco-ISE-Chrome-NSP	Edit | ▾

7단계. Policy(정책) > Policy Elements(정책 요소) > Conditions(조건) > Posture(포스처) > Anti-Malware Condition(안티멀웨어 조건)에서 포스처 조건을 생성합니다. 이 예에서는 사전 정의된 "ANY_am_win_inst"가 사용됩니다.

.

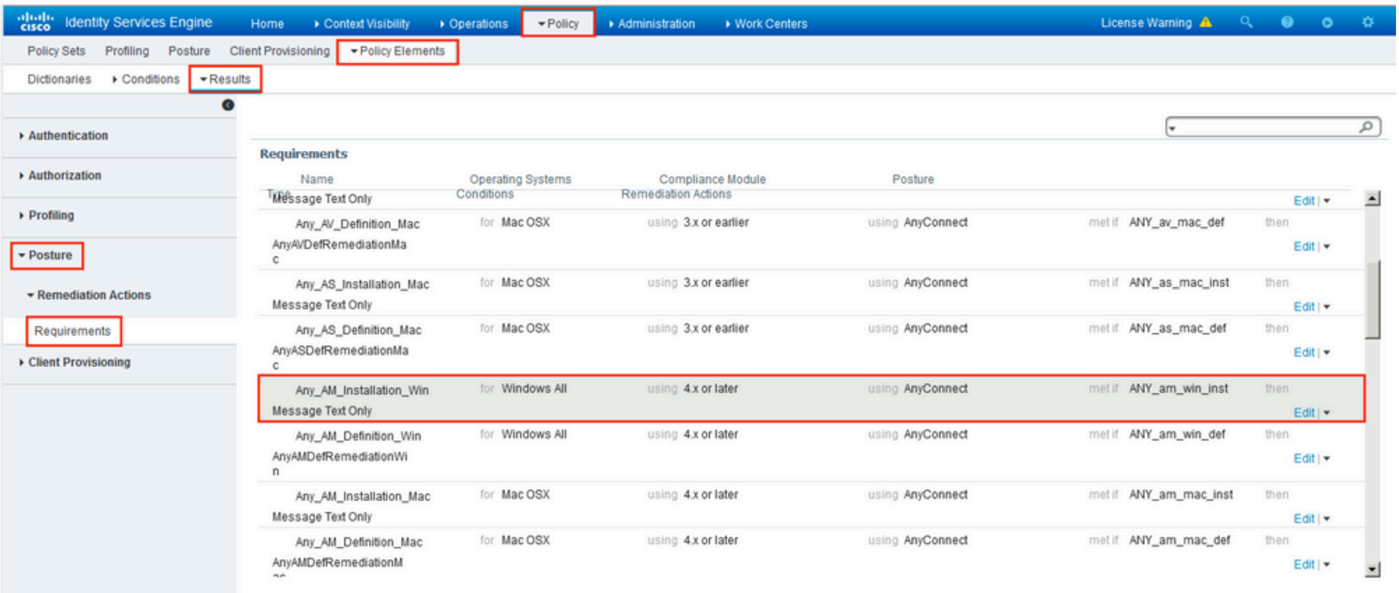


Anti-Malware Conditions

	Name	Description
□	ANY_am_win_inst	Any AM installation check on Wi...
□	ANY_am_win_def	Any AM definition check on Wind...
□	ANY_am_mac_inst	Any AM installation check on Mac
□	ANY_am_mac_def	Any AM definition check on Mac

8단계. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Posture(포스처) > Remediation Actions(교정 작업)로 이동하고 Posture Remediation(포스처 교정)을 생성합니다. 이 예에서는 건너뜁니다. 교정 작업은 텍스트 메시지일 수 있습니다.

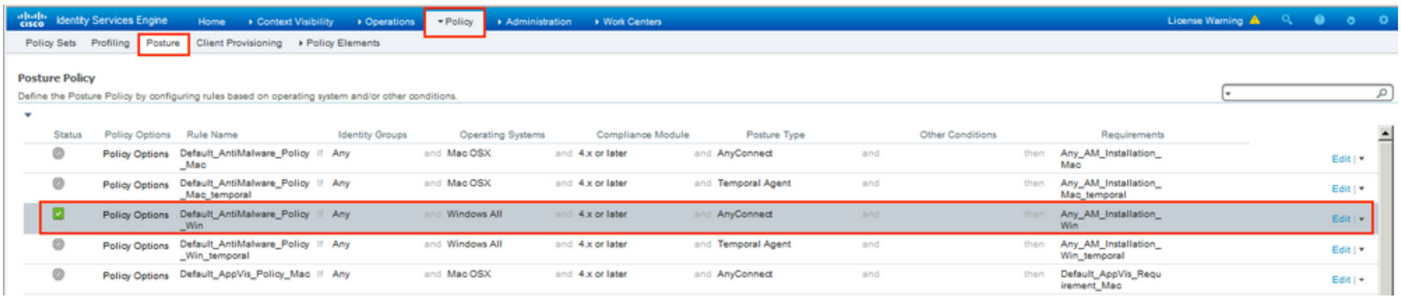
9단계. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Posture(포스처) > Requirements(요건)로 이동하고 Posture Requirements(포스처 요건)를 생성합니다. 사전 정의된 요구 사항 Any_AM_Installation_Win이 사용됩니다.



Requirements

Name	Operating Systems	Compliance Module	Posture	Conditions	Remediation Actions
					Message Text Only
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_av_mac_def	then AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_inst	then Message Text Only
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_def	then AnyASDefRemediationMac
Any_AM_Installation_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_inst	then Message Text Only
Any_AM_Definition_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_def	then AnyAMDefRemediationWin
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_inst	then Message Text Only
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_def	then AnyAMDefRemediationM

10단계. Policies(정책) > Posture(포스처)에서 Posture Policies(포스처 정책)를 생성합니다. Windows OS에 대한 안티멀웨어 검사에 대한 기본 포스처 정책이 사용됩니다.



Posture Policy

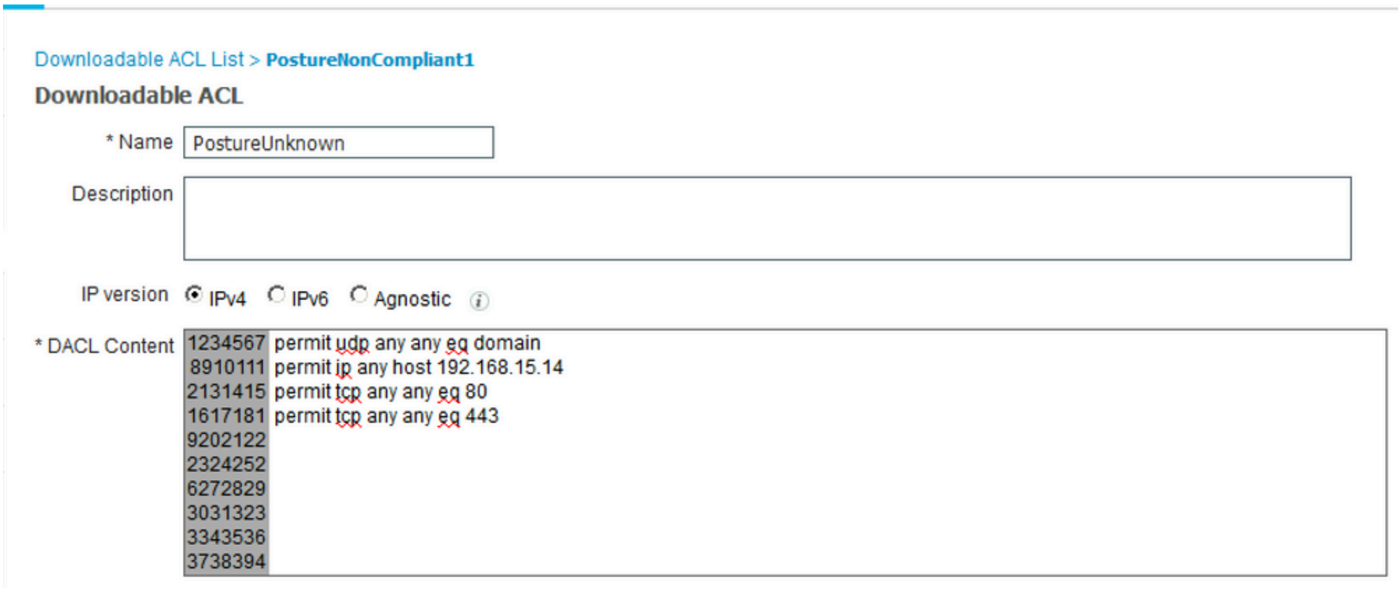
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

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

11단계. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Downloadable ACLS(다운로드 가능한 ACL)로 이동하고 여러 포스처 상태에 대한 DACL을 생성합니다.

이 예에서는 다음을 수행합니다.

- Posture Unknown DACL - DNS, PSN 및 HTTP/HTTPS 트래픽에 대한 트래픽을 허용합니다.
- Posture NonCompliant DACL - 프라이빗 서브넷에 대한 액세스를 거부하고 인터넷 트래픽만 허용합니다.
- Permit All DACL(모든 DACL 허용) - 포스처 호환 상태에 대한 모든 트래픽을 허용합니다.



Downloadable ACL List > **PostureNonCompliant1**

Downloadable ACL

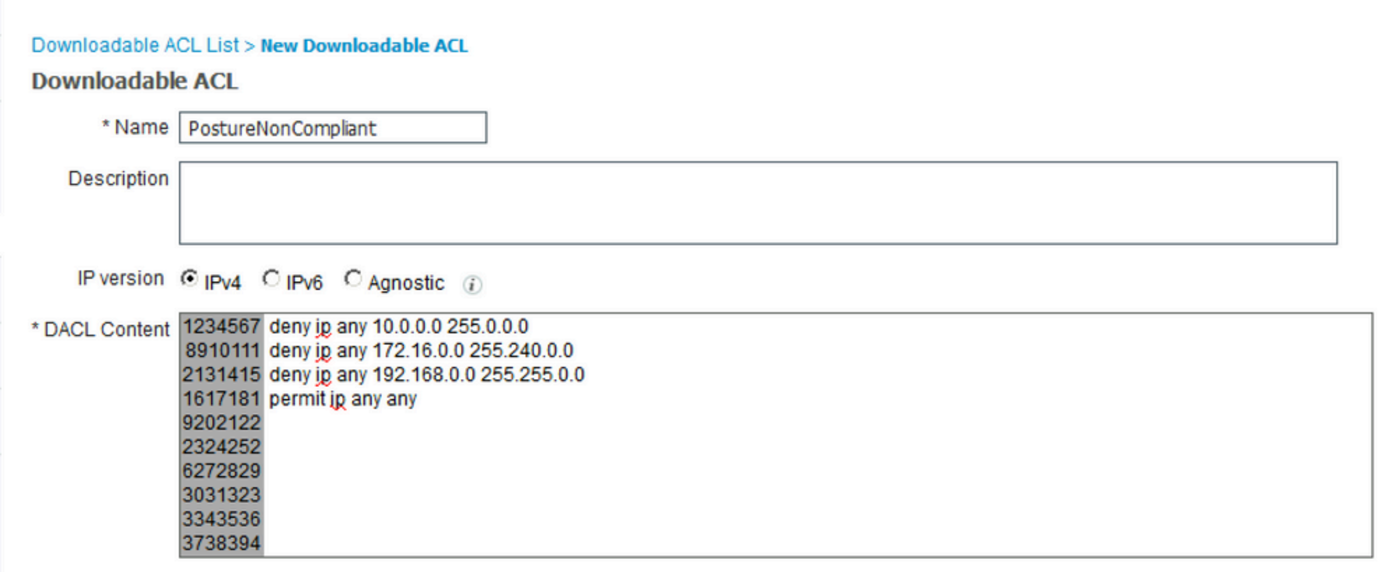
* Name: PostureUnknown

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

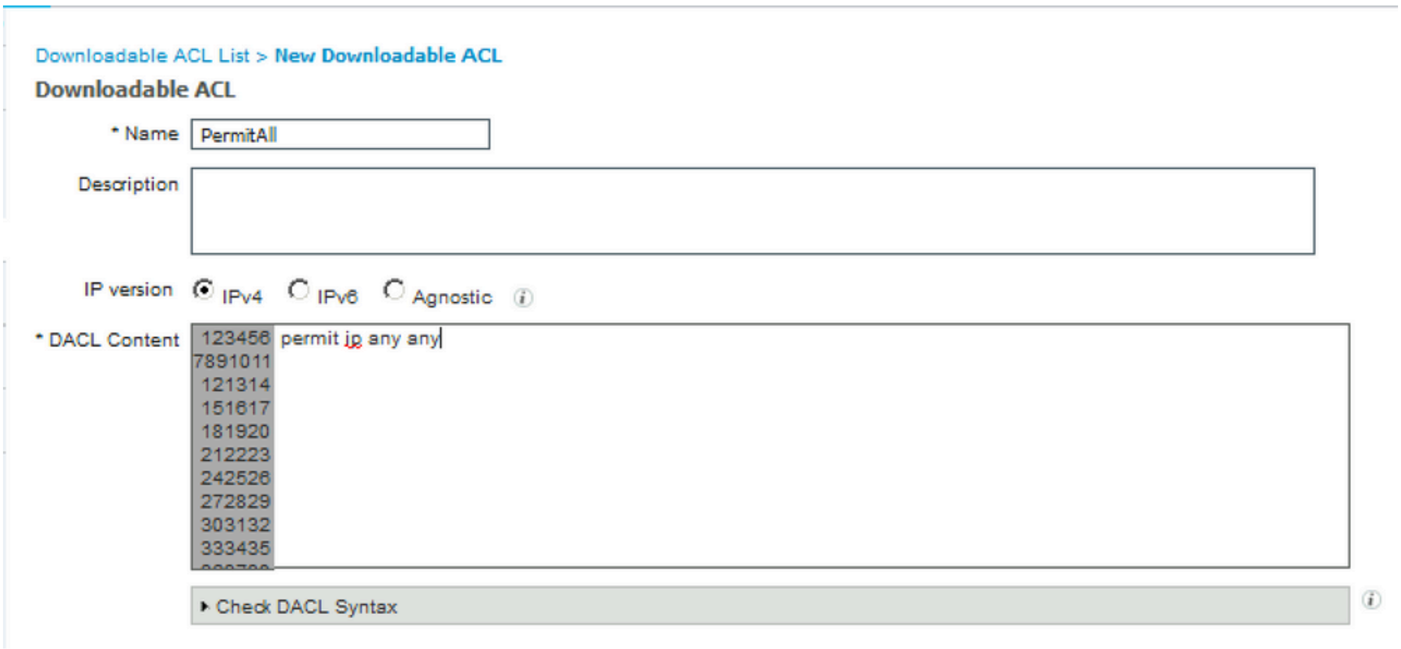
* Name: PostureNonCompliant

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:

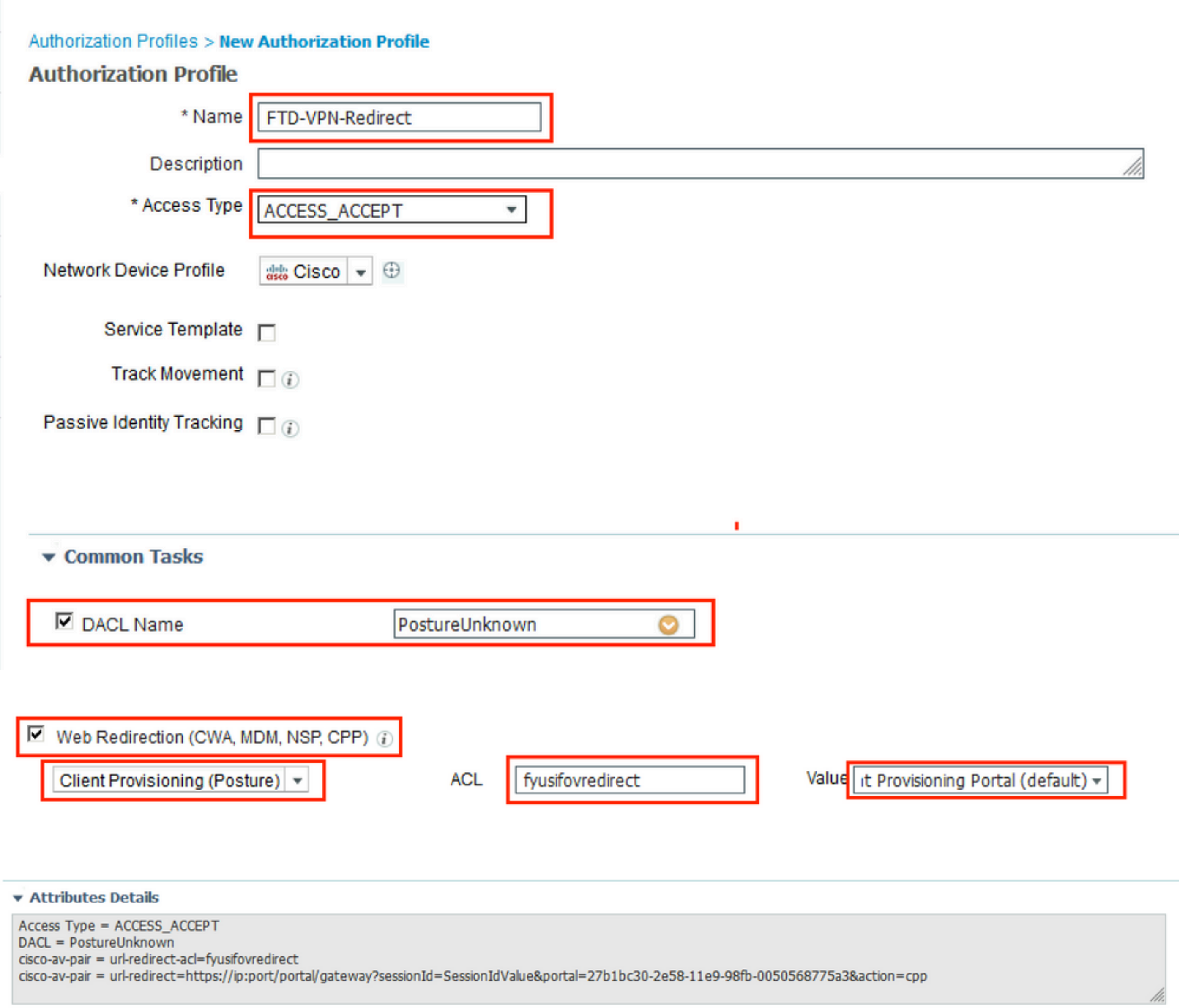
IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit ip any any
```

12단계. Posture Unknown, Posture NonCompliant 및 Posture Compliant 상태에 대한 3가지 권한

부여 프로파일을 생성합니다. 이렇게 하려면 정책 > 정책 구성 요소 > 결과 > 인증 > 인증 프로파일로 이동 합니다. Posture Unknown 프로필에서 Posture Unknown DACL을 선택하고 Web Redirection을 선택한 다음 Client Provisioning을 선택하고, Redirect ACL name(FTD에서 구성됨)을 제공하고 포털을 선택합니다.



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

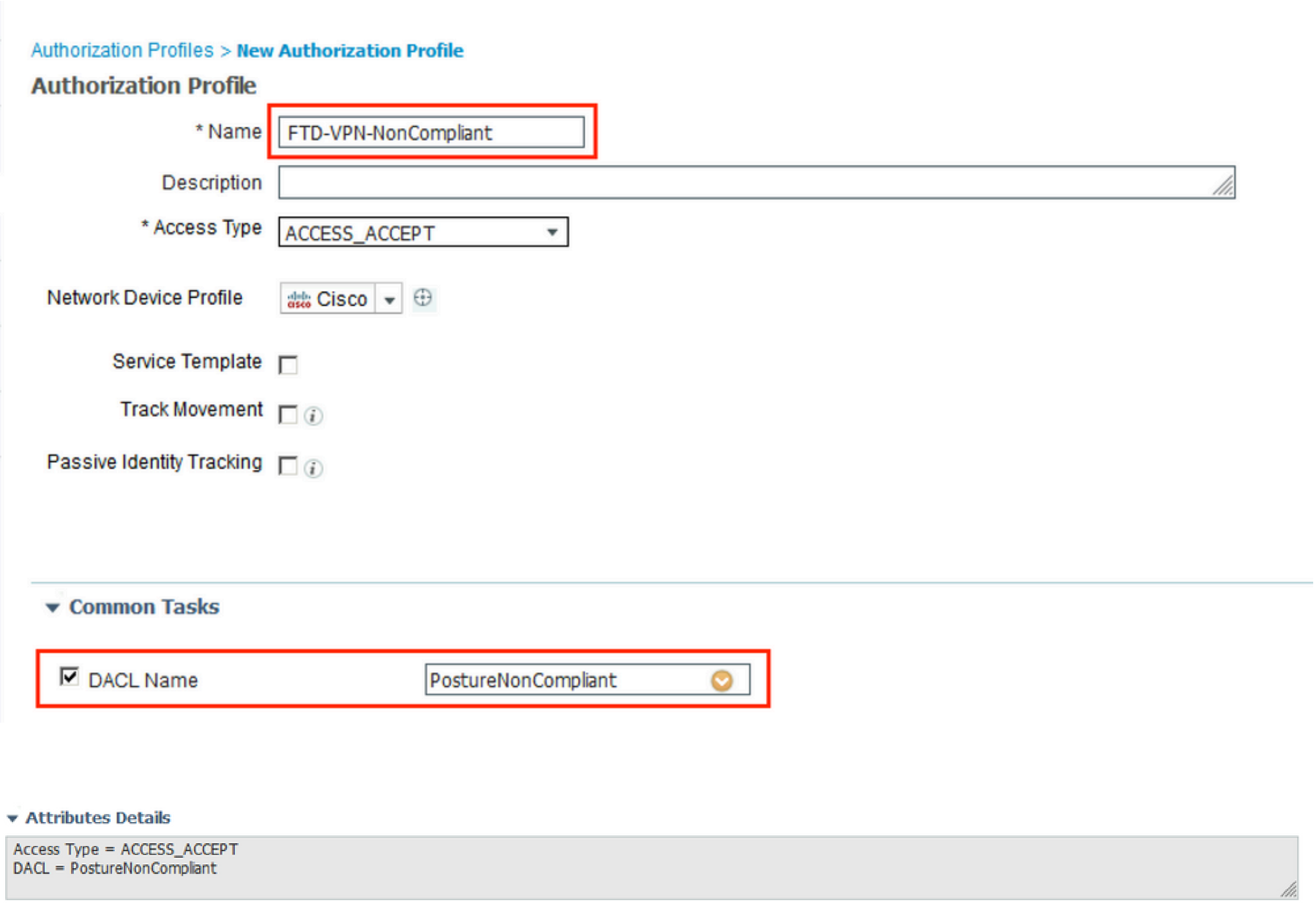
☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: fyusifovredirect Value: ıt Provisioning Portal (default)

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&action=cpp
```

Posture NonCompliant 프로파일에서 DACL을 선택하여 네트워크에 대한 액세스를 제한합니다.



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 □

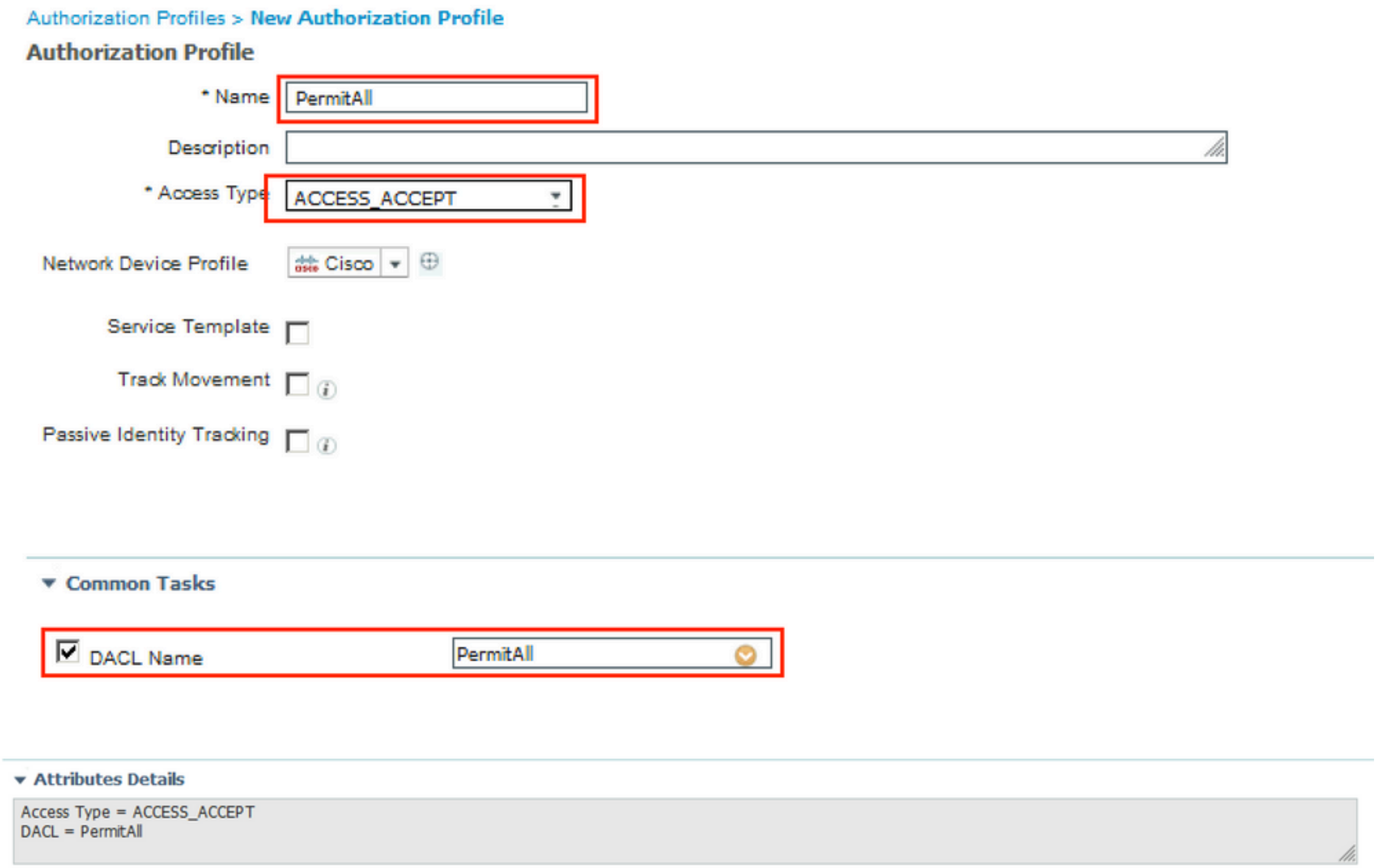
▾ Common Tasks

☑ DACL Name: PostureNonCompliant

▾ Attributes Details

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

Posture Compliant Profile에서 DACL을 선택하여 네트워크에 대한 전체 액세스를 허용합니다.



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 □

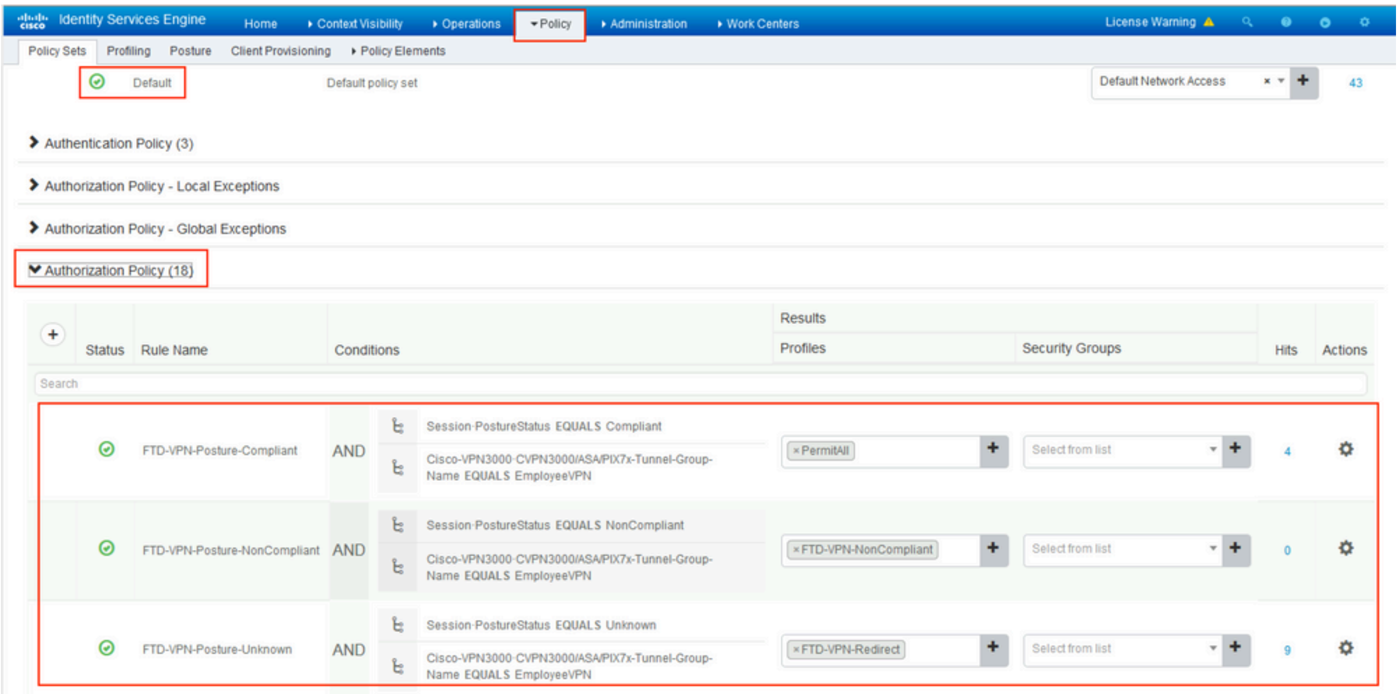
▾ Common Tasks

☑ DACL Name: PermitAll

▾ Attributes Details

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

13단계. Policy(정책) > Policy Sets(정책 집합) > Default(기본값) > Authorization Policy(권한 부여 정책)에서 권한 부여 정책을 생성합니다. As 조건 Posture Status 및 VNP TunnelGroup Name이 사용됩니다.

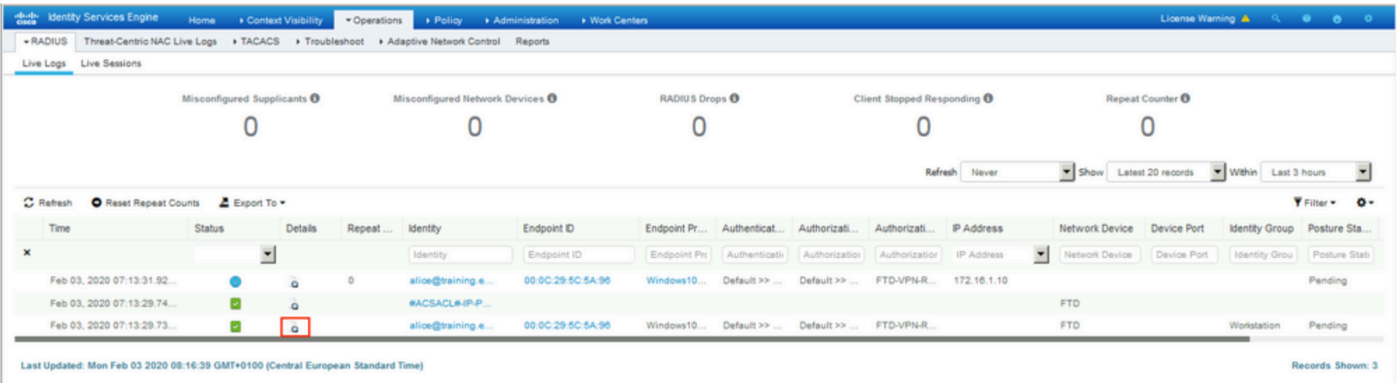


Status	Rule Name	Conditions		Results: Profiles	Security Groups	Hits	Actions
✓	FTD-VPN-Posture-Compliant	AND	Session·PostureStatus EQUALS Compliant Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	×PermitAll	Select from list	4	⚙
✓	FTD-VPN-Posture-NonCompliant	AND	Session·PostureStatus EQUALS NonCompliant Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	×FTD-VPN-NonCompliant	Select from list	0	⚙
✓	FTD-VPN-Posture-Unknown	AND	Session·PostureStatus EQUALS Unknown Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	×FTD-VPN-Redirect	Select from list	9	⚙

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

ISE에서 첫 번째 확인 단계는 RADIUS Live Log입니다. Operations(작업) > RADIUS Live Log(RADIUS 라이브 로그)로 이동합니다. 여기서 사용자 Alice가 연결되고 예상 권한 부여 정책이 선택됩니다.



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

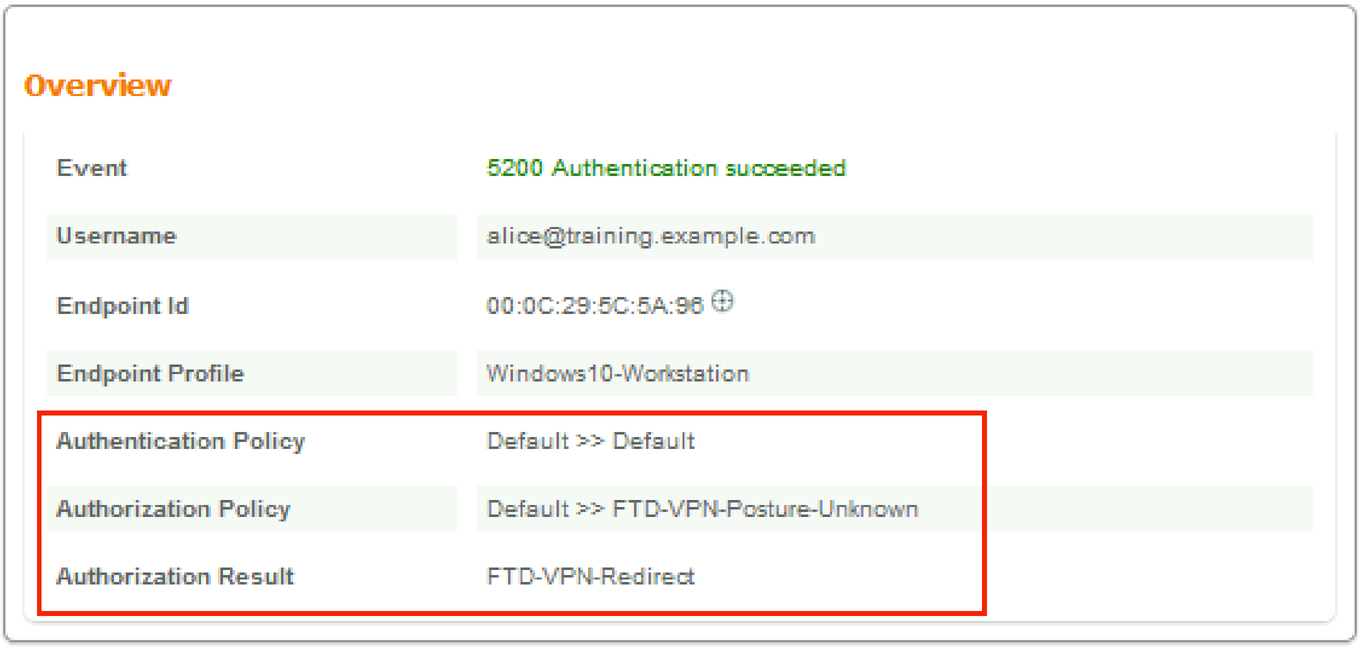
Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture Sta...
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				Pending
Feb 03, 2020 07:13:29.74...	✓	🔍		#ACSACL#-IP-P...							FTD			
Feb 03, 2020 07:13:29.73...	✓	🔍		alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...		FTD		Workstation	Pending

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

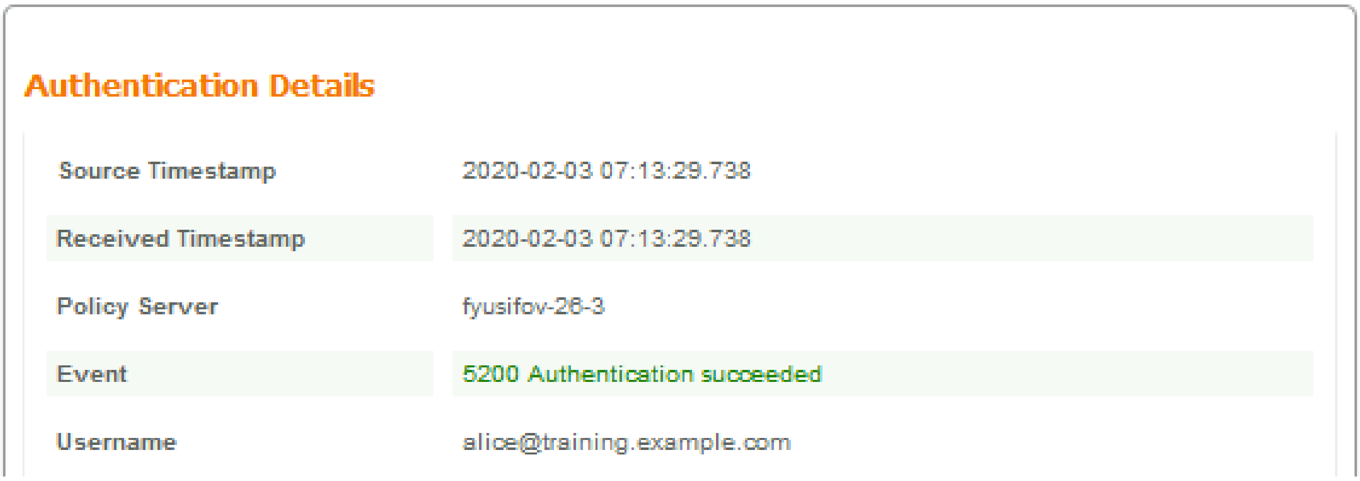
Records Shown: 3

권한 부여 정책 FTD-VPN-Posture-Unknown이 일치하고 그 결과 FTD-VPN-Profile이 FTD로 전송됩니다.



Overview

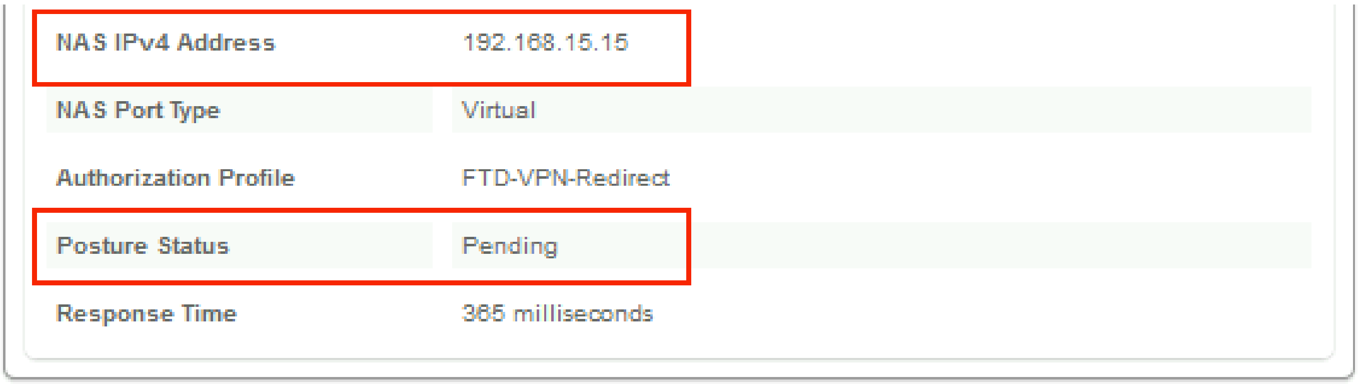
Event	5200 Authentication succeeded
Username	alice@training.example.com
Endpoint Id	00:0C:29:5C:5A:96 ⊕
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> FTD-VPN-Posture-Unknown
Authorization Result	FTD-VPN-Redirect



Authentication Details

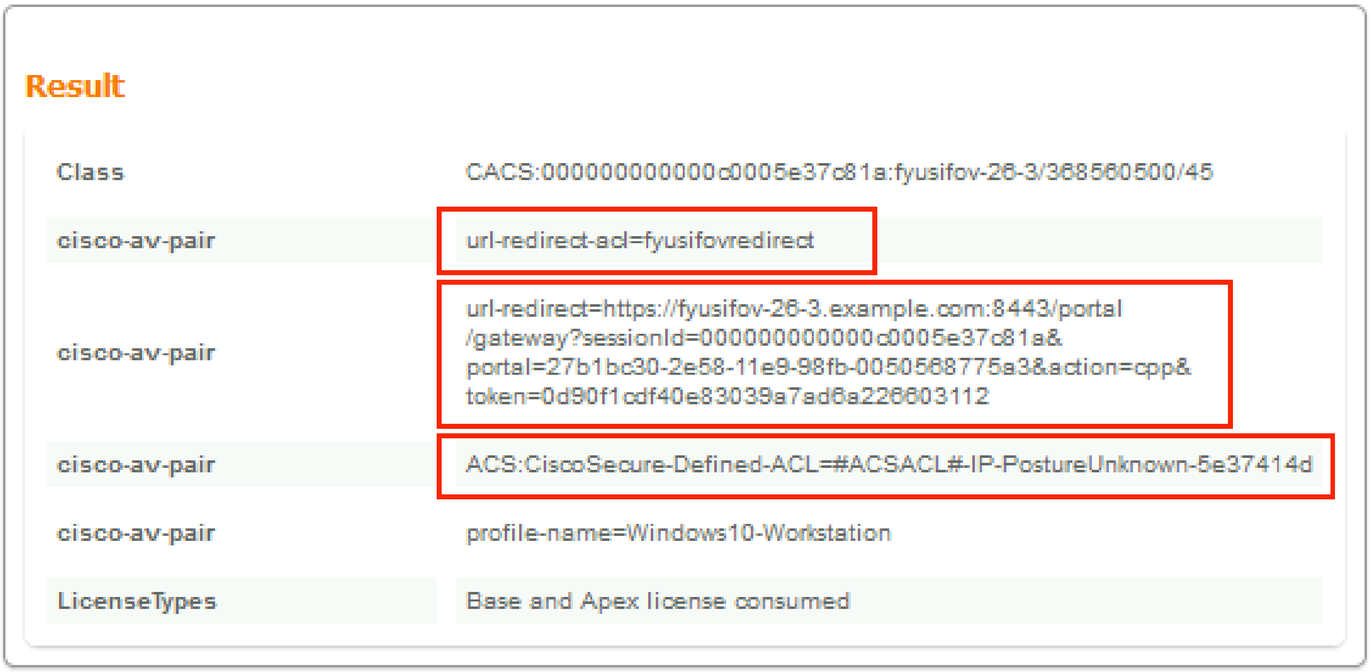
Source Timestamp	2020-02-03 07:13:29.738
Received Timestamp	2020-02-03 07:13:29.738
Policy Server	fyusifov-26-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

상태 보류 중.



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

Result(결과) 섹션에는 FTD로 전송되는 속성이 표시됩니다.



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

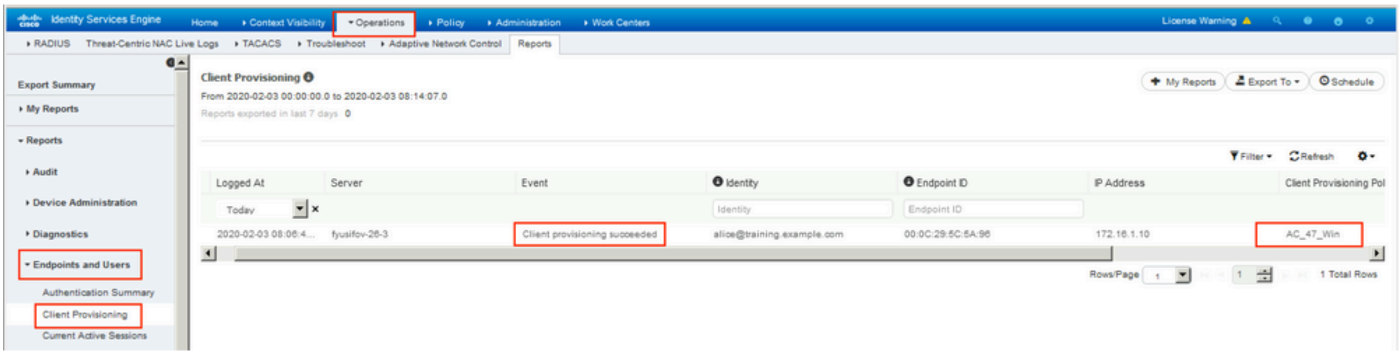
FTD에서 VPN 연결을 확인하려면 SSH를 상자에 입력하고 시스템 지원 diagnostic-cli를 실행한 다음 vpn-sessiondb detail anyconnect를 표시합니다. 이 출력에서 ISE에서 전송된 특성이 이 VPN 세션에 적용되는지 확인합니다.

<#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#
```

클라이언트 프로비저닝 정책을 확인할 수 있습니다. Operations(운영) > Reports(보고서) > Endpoints and Users(엔드포인트 및 사용자) > Client Provisioning(클라이언트 프로비저닝)으로 이동합니다.



Client Provisioning

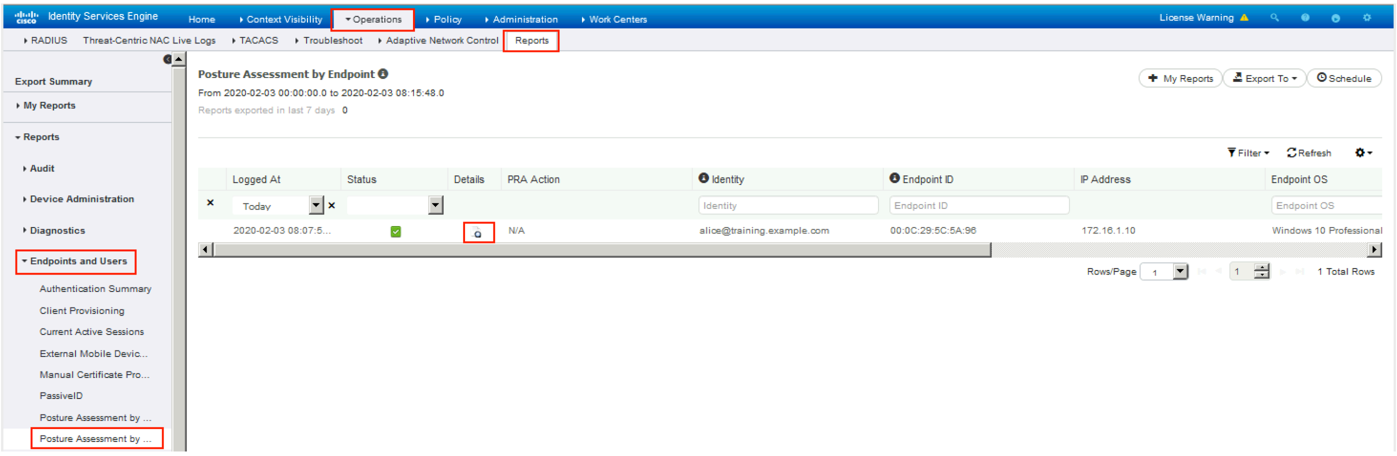
From 2020-02-03 00:00:00.0 to 2020-02-03 08:14:07.0

Reports exported in last 7 days 0

Logged At	Server	Event	Identity	Endpoint ID	IP Address	Client Provisioning Pol
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	172.16.1.10	AC_47_Win

Rows/Page 1 1 1 Total Rows

AnyConnect에서 전송된 상태 보고서를 확인할 수 있습니다. Operations(운영) > Reports(보고서) > Endpoints and Users(엔드포인트 및 사용자) > Posture Assessment by Endpoint(엔드포인트별 상태 평가)로 이동합니다.



Posture Assessment by Endpoint

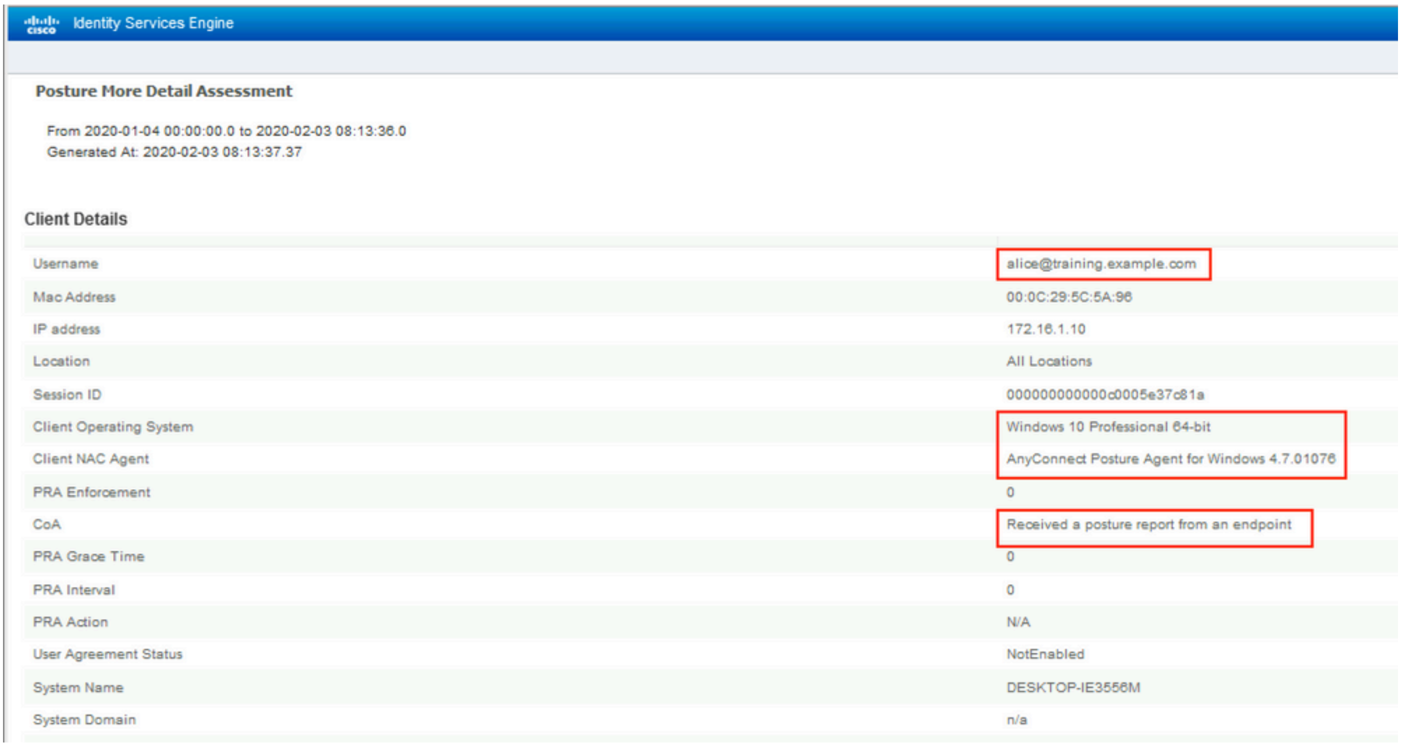
From 2020-02-03 00:00:00.0 to 2020-02-03 08:15:48.0

Reports exported in last 7 days 0

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address	Endpoint OS
Today				Identity	Endpoint ID		Endpoint OS
2020-02-03 08:07:5...	✓		N/A	alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	Windows 10 Professional

Rows/Page 1 1 1 Total Rows

상태 보고서에 대한 자세한 내용을 보려면 Details를 클릭합니다.



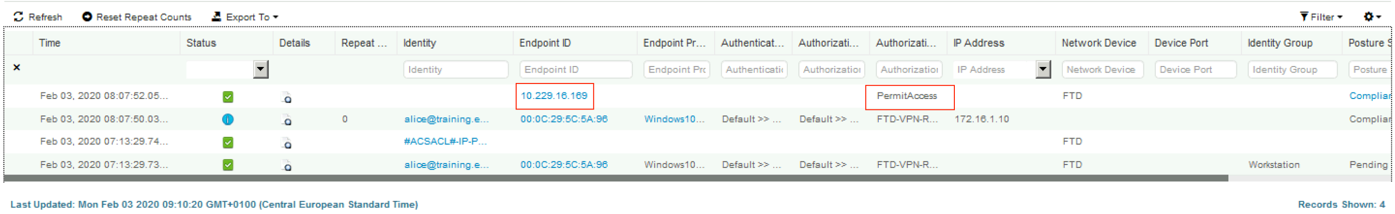
Posture More Detail Assessment

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@training.example.com
Mac Address	00:0C:29:5C:5A:96
IP address	172.16.1.10
Location	All Locations
Session ID	000000000000c0005e37c81a
Client Operating System	Windows 10 Professional 64-bit
Client NAC Agent	AnyConnect Posture Agent for Windows 4.7.01076
PRA Enforcement	0
CoA	Received a posture report from an endpoint
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEnabled
System Name	DESKTOP-IE3556M
System Domain	n/a

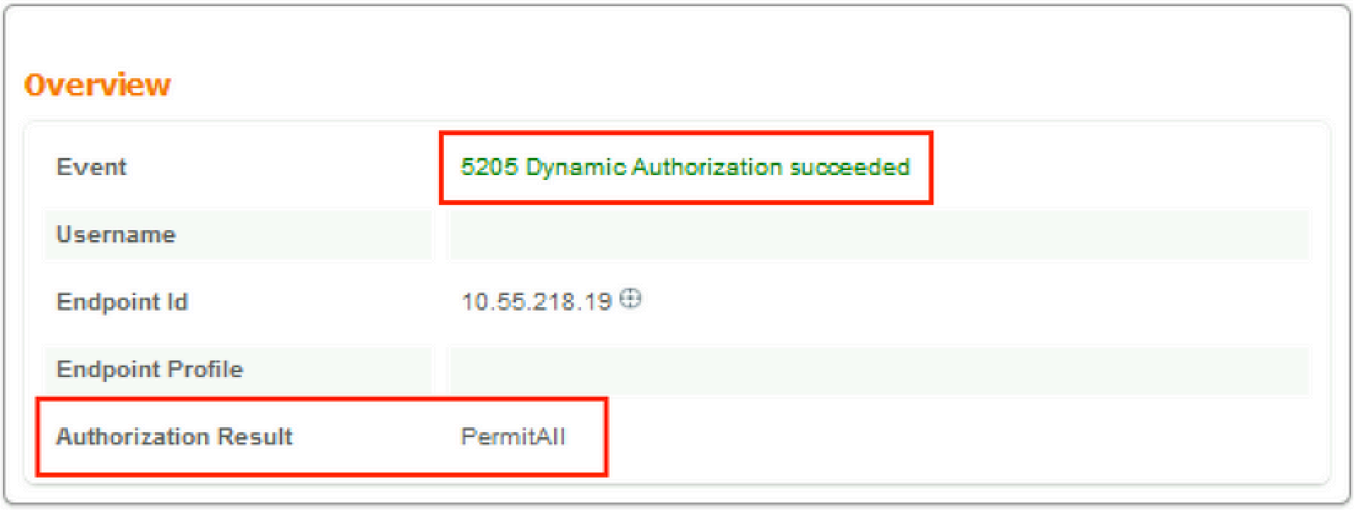
ISE에서 보고서를 받으면 포스처 상태가 업데이트됩니다. 이 예에서 포스처 상태는 규정준수 상태이며 CoA Push는 새 특성 집합으로 트리거됩니다.



Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture S
Feb 03, 2020 08:07:52.05...	✓				10.229.16.169				PermitAccess		FTD			Complian
Feb 03, 2020 08:07:50.03...	●		0	alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...	172.16.1.10				Complian
Feb 03, 2020 07:13:29.74...	✓			#ACSACL#-IP-P...							FTD			
Feb 03, 2020 07:13:29.73...	✓			alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...		FTD		Workstation	Pending

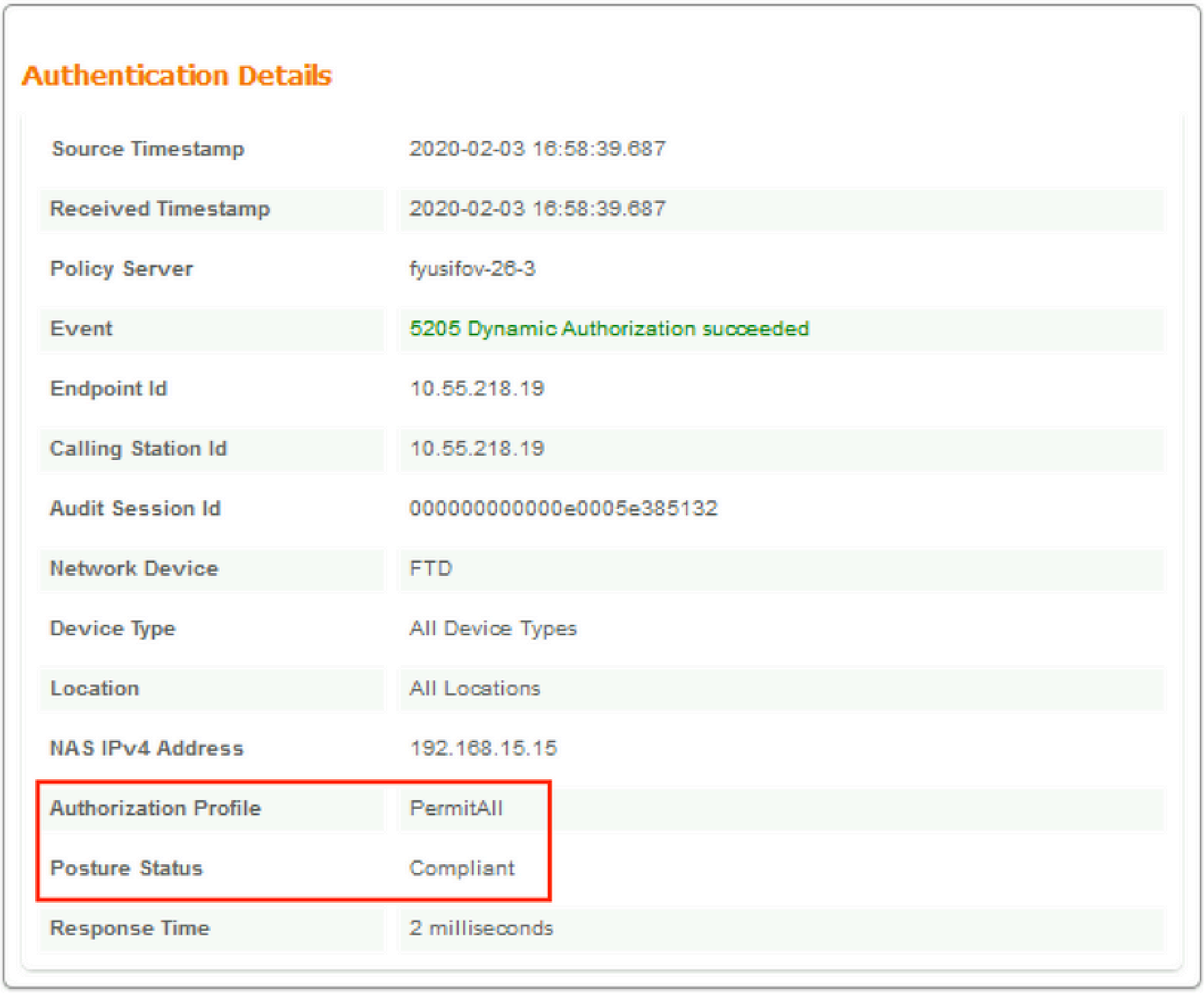
Last Updated: Mon Feb 03 2020 09:10:20 GMT+0100 (Central European Standard Time)

Records Shown: 4



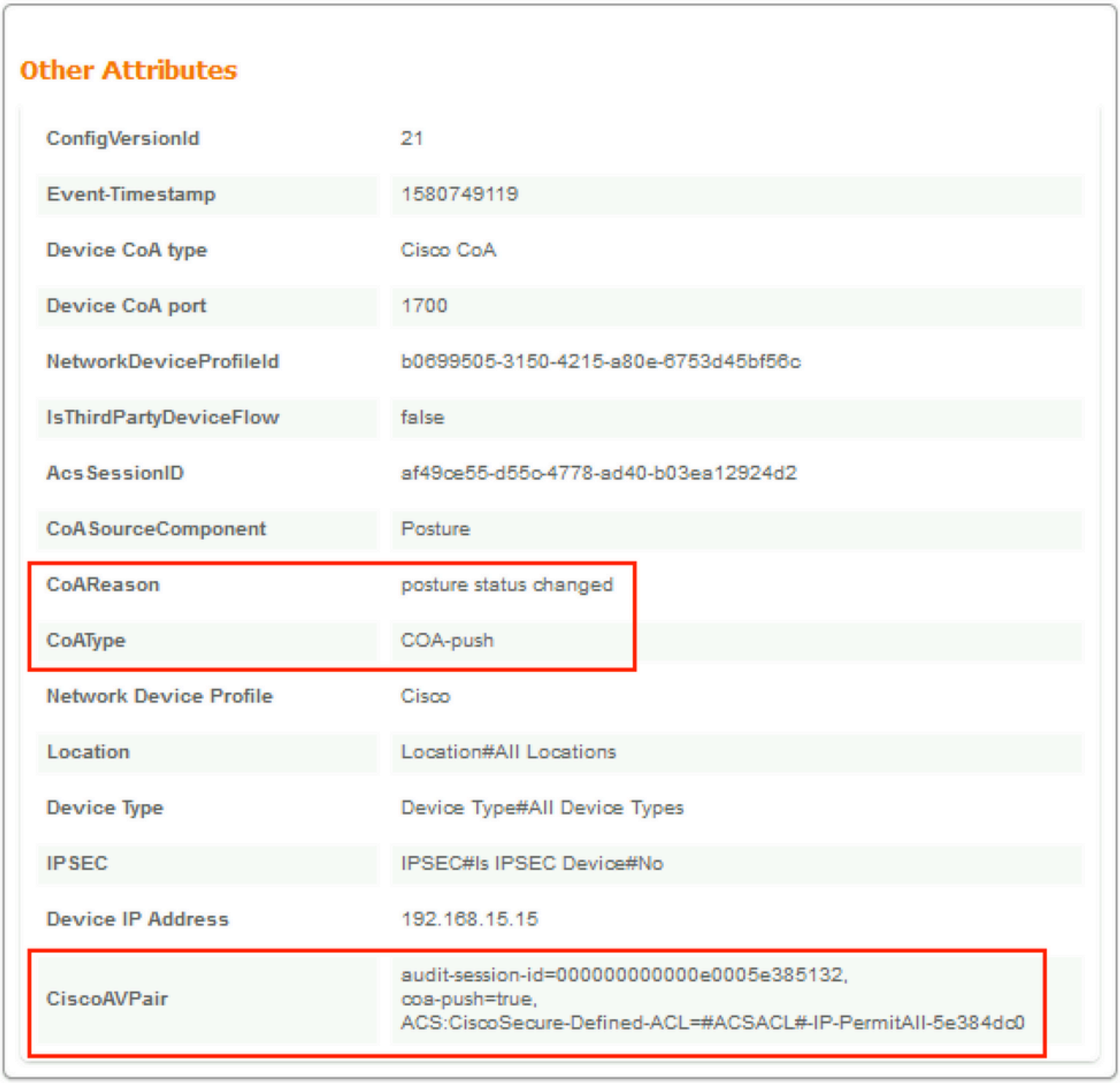
Overview

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



Other Attributes

ConfigVersionId	21
Event-Timestamp	1580749119
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	af49ce55-d55c-4778-ad40-b03ea12924d2
CoASourceComponent	Posture
CoAReason	posture status changed
CoAType	COA-push
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
Device IP Address	192.168.15.15

CiscoAVPair	audit-session-id=000000000000e0005e385132,
	coa-push=true,
	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PermitAll-5e384dc0

FTD에서 새 리디렉션 ACL 및 리디렉션 URL이 VPN 세션에 대해 제거되고 PermitAll DACL이 적용되는지 확인합니다.

<#root>

```
fyusifov-ftd-64#

show vpn-sessiondb detail anyconnect


Session Type: AnyConnect Detailed

Username     :

alice@training.example.com

Index        : 14
Assigned IP  : 172.16.1.10            Public IP    : 10.55.218.19
```

```
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     : 53990                  Bytes Rx     : 23808
Pkts Tx      : 73                     Pkts Rx      : 120
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group :

EmployeeVPN

Login Time   : 16:58:26 UTC Mon Feb 3 2020
Duration     : 0h:02m:24s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000e0005e385132
Security Grp : none                   Tunnel Zone  : 0

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

AnyConnect-Parent:
  Tunnel ID    : 14.1
  Public IP    : 10.55.218.19
  Encryption   : none                   Hashing      : none
  TCP Src Port : 51965                  TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 27 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    : 14.2
  Assigned IP  : 172.16.1.10            Public IP    : 10.55.218.19
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 51970
  TCP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.7.01076
  Bytes Tx     : 7715                   Bytes Rx     : 10157
  Pkts Tx      : 6                      Pkts Rx      : 33
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  :

#ACSACL#-IP-PermitAll-5e384dc0


DTLS-Tunnel:
  Tunnel ID    : 14.3
  Assigned IP  : 172.16.1.10            Public IP    : 10.55.218.19
  Encryption   : AES256                 Hashing      : SHA1
  Ciphersuite  : DHE-RSA-AES256-SHA
  Encapsulation: DTLSv1.0               UDP Src Port : 51536
  UDP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes            Idle TO Left : 28 Minutes
  Client OS     : Windows
  Client Type   : DTLS VPN Client
  Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.7.01076
  Bytes Tx      : 38612                Bytes Rx      : 13651
  Pkts Tx       : 62                   Pkts Rx       : 87
  Pkts Tx Drop : 0                     Pkts Rx Drop : 0
  Filter Name   :

#ACSACL#-IP-PermitAll-5e384dc0


fyusifov-ftd-64#
```

문제 해결

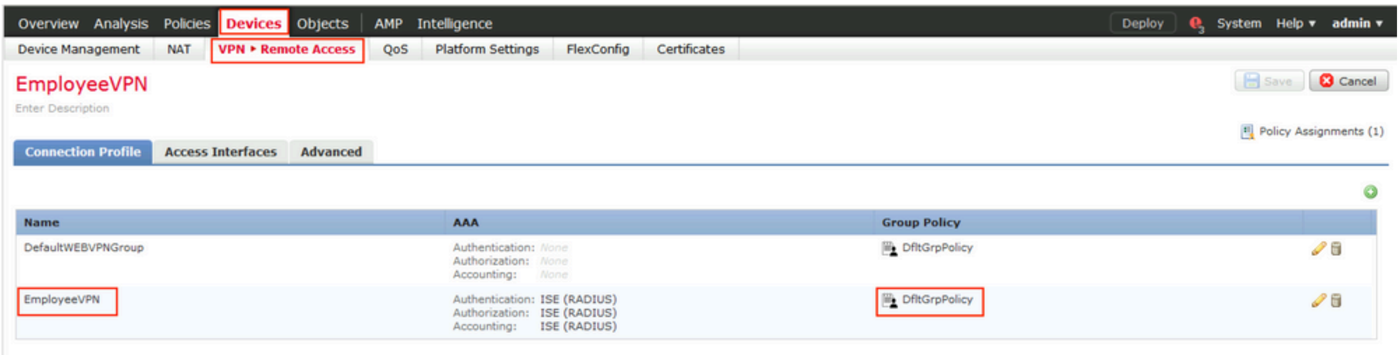
이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

자세한 상태 흐름 및 AnyConnect 및 ISE 문제를 해결하려면 다음 링크를 확인하십시오. ISE Posture Style Comparison for Pre and Post 2.2

- 스플릿 터널

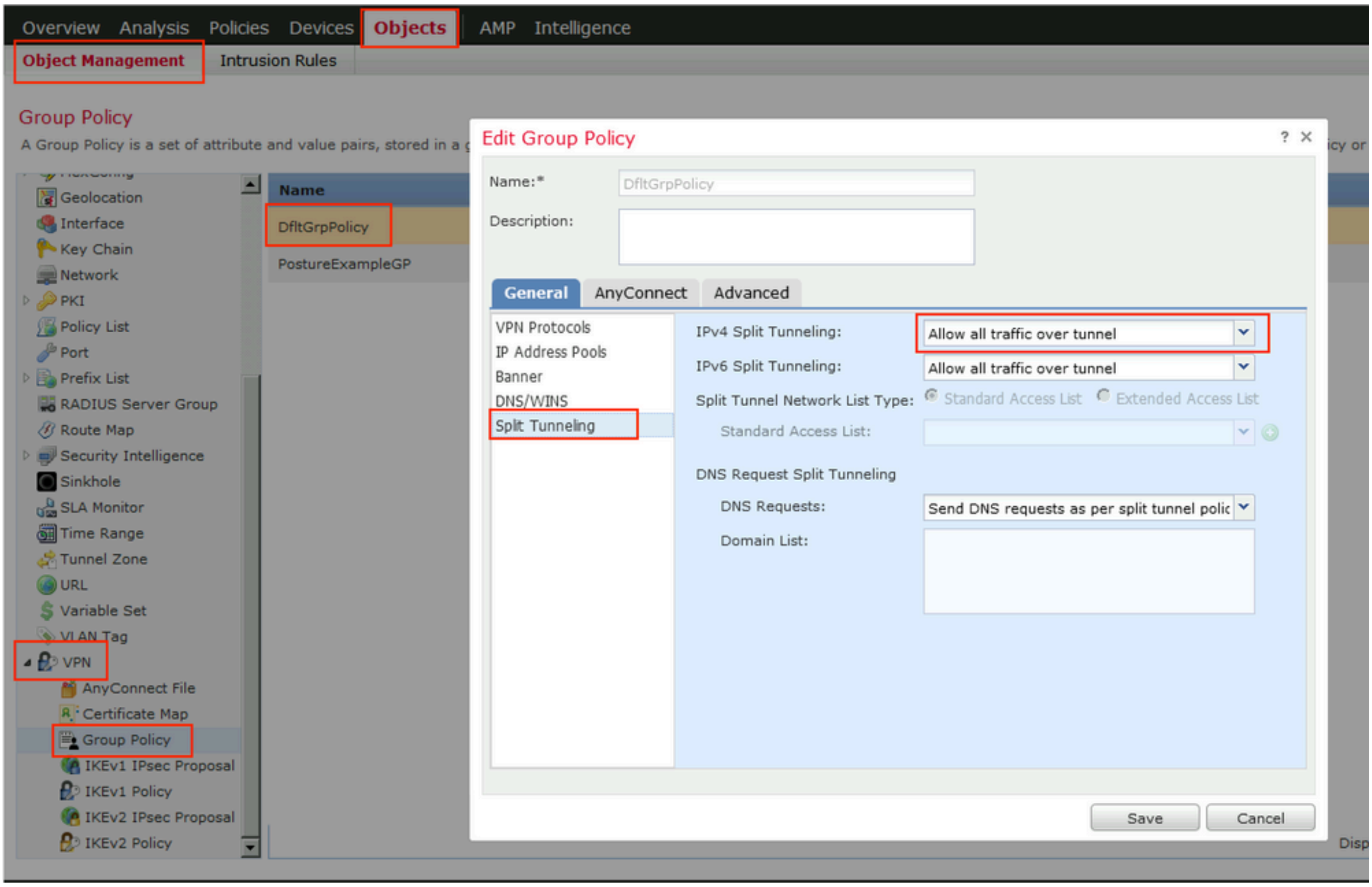
일반적인 문제 중 하나는 spit 터널이 구성된 경우입니다. 이 예에서는 모든 트래픽을 터널링하는 기본 그룹 정책이 사용됩니다. 특정 트래픽만 터널링되는 경우 AnyConnect 프로브(enroll.cisco.com 및 검색 호스트)는 ISE 및 기타 내부 리소스에 대한 트래픽 외에도 터널을 통과해야 합니다.

FMC에서 터널 정책을 확인하려면 먼저 VPN 연결에 어떤 그룹 정책이 사용되는지 확인하십시오. Devices(디바이스) > VPN Remote Access(VPN 원격 액세스)로 이동합니다.



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

그런 다음 Objects(개체) > Object Management(개체 관리) > VPN > Group Policy(그룹 정책)로 이동하고 VPN에 대해 구성된 Group Policy(그룹 정책)를 클릭합니다.



Overview Analysis Policies Devices **Objects** AMP Intelligence

Object Management Intrusion Rules

Group Policy

A Group Policy is a set of attribute and value pairs, stored in a g…

Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
RADIUS Server Group
Route Map
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Tunnel Zone
URL
Variable Set
VLAN Tag
VPN
AnyConnect File
Certificate Map
Group Policy
IKEv1 IPsec Proposal
IKEv1 Policy
IKEv2 IPsec Proposal
IKEv2 Policy

Name: DfltGrpPolicy, PostureExampleGP

Edit Group Policy

Name:* DfltGrpPolicy

Description:

General | AnyConnect | Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

IPv4 Split Tunneling: Allow all traffic over tunnel

IPv6 Split Tunneling: Allow all traffic over tunnel

Split Tunnel Network List Type: ● Standard Access List ○ Extended Access List

Standard Access List:

DNS Request Split Tunneling

DNS Requests: Send DNS requests as per split tunnel polic

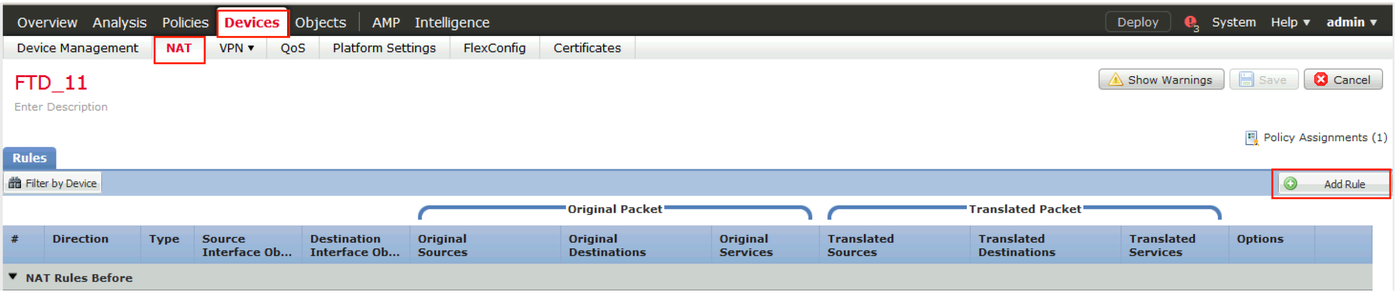
Domain List:

Save Cancel

- 아이덴티티 NAT

또 다른 일반적인 문제는 VPN 사용자의 반환 트래픽이 잘못된 NAT 항목을 사용하여 변환되는 경우입니다. 이 문제를 해결하려면 ID NAT를 적절한 순서로 생성해야 합니다.

먼저 이 디바이스에 대한 NAT 규칙을 확인합니다. Devices(디바이스) > NAT로 이동한 다음 Add Rule(규칙 추가)을 클릭하여 새 규칙을 생성합니다.



Overview Analysis Policies **Devices** Objects AMP Intelligence | Deploy System Help ▾ admin ▾

Device Management **NAT** VPN ▾ QoS Platform Settings FlexConfig Certificates

FTD_11

Enter Description

Show Warnings Save Cancel

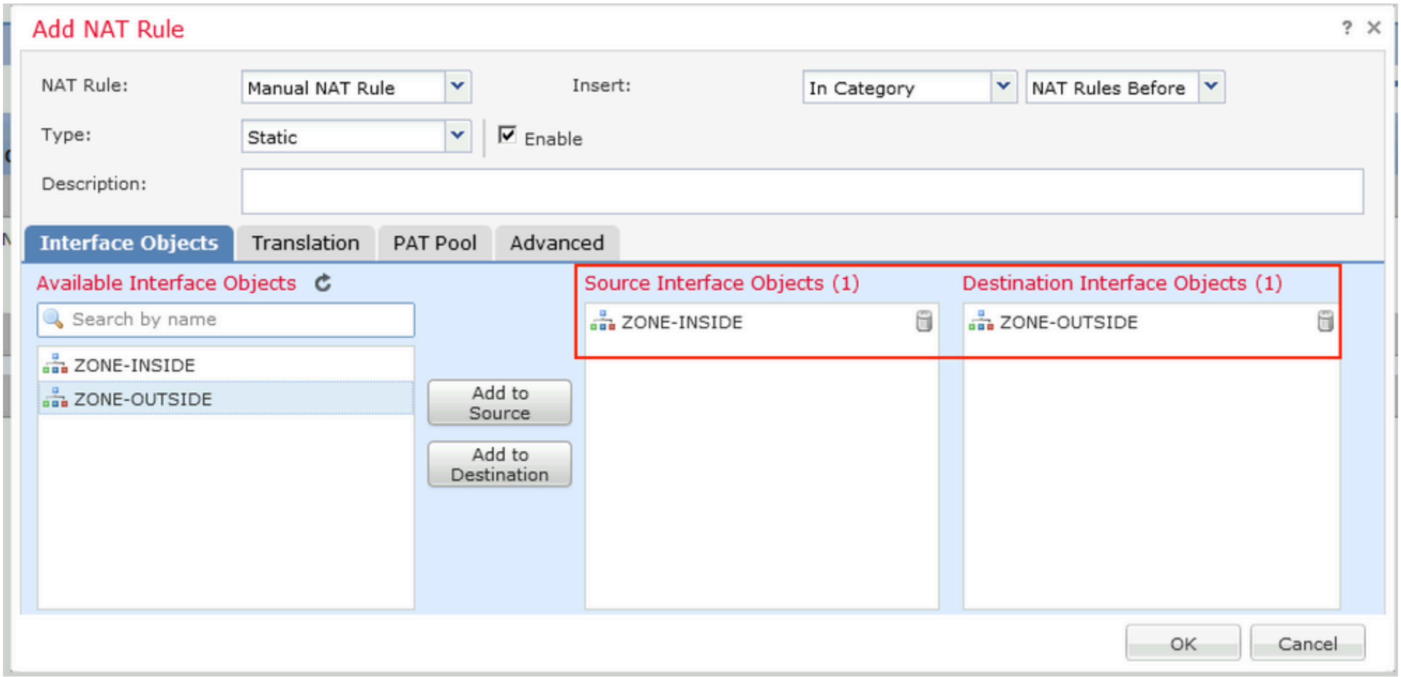
Policy Assignments (1)

Rules

Filter by Device | Add Rule

					Original Packet			Translated Packet			
#	Direction	Type	Source Interface Ob...	Destination Interface Ob...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											

열려 있는 창의 Interface Objects 탭 아래에서 Security Zones를 선택합니다. 이 예에서는 NAT 항목이 ZONE-INSIDE에서 ZONE-OUTSIDE로 생성됩니다.



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Static ☑ Enable

Description:

Interface Objects | Translation | PAT Pool | Advanced

Available Interface Objects

Search by name

- ZONE-INSIDE
- ZONE-OUTSIDE

Add to Source

Add to Destination

Source Interface Objects (1)

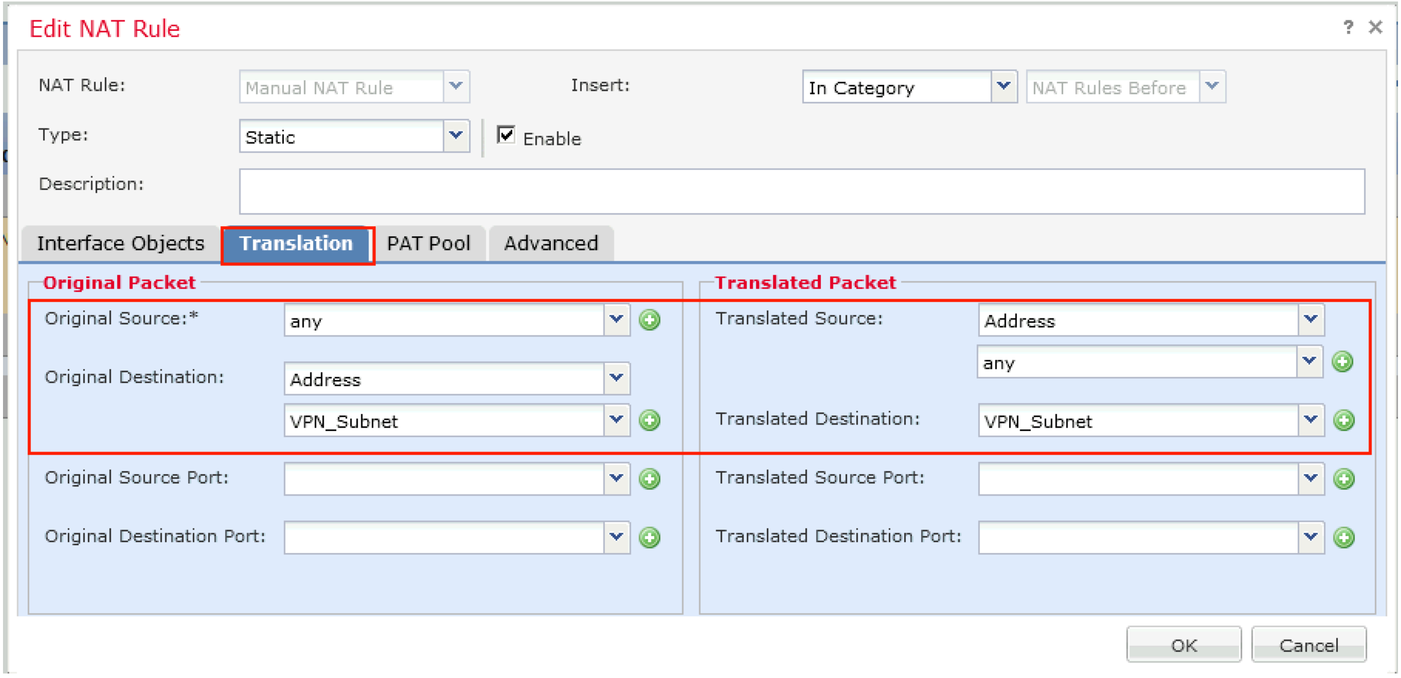
- ZONE-INSIDE

Destination Interface Objects (1)

- ZONE-OUTSIDE

OK | Cancel

Translation(변환) 탭에서 original(원본) 및 translated(변환된) 패킷 세부 정보를 선택합니다. ID NAT이므로 소스와 대상은 변경되지 않습니다.



Edit NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Static ☑ Enable

Description:

Interface Objects | Translation | PAT Pool | Advanced

Original Packet

Original Source:* any

Original Destination: Address

VPN_Subnet

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address

any

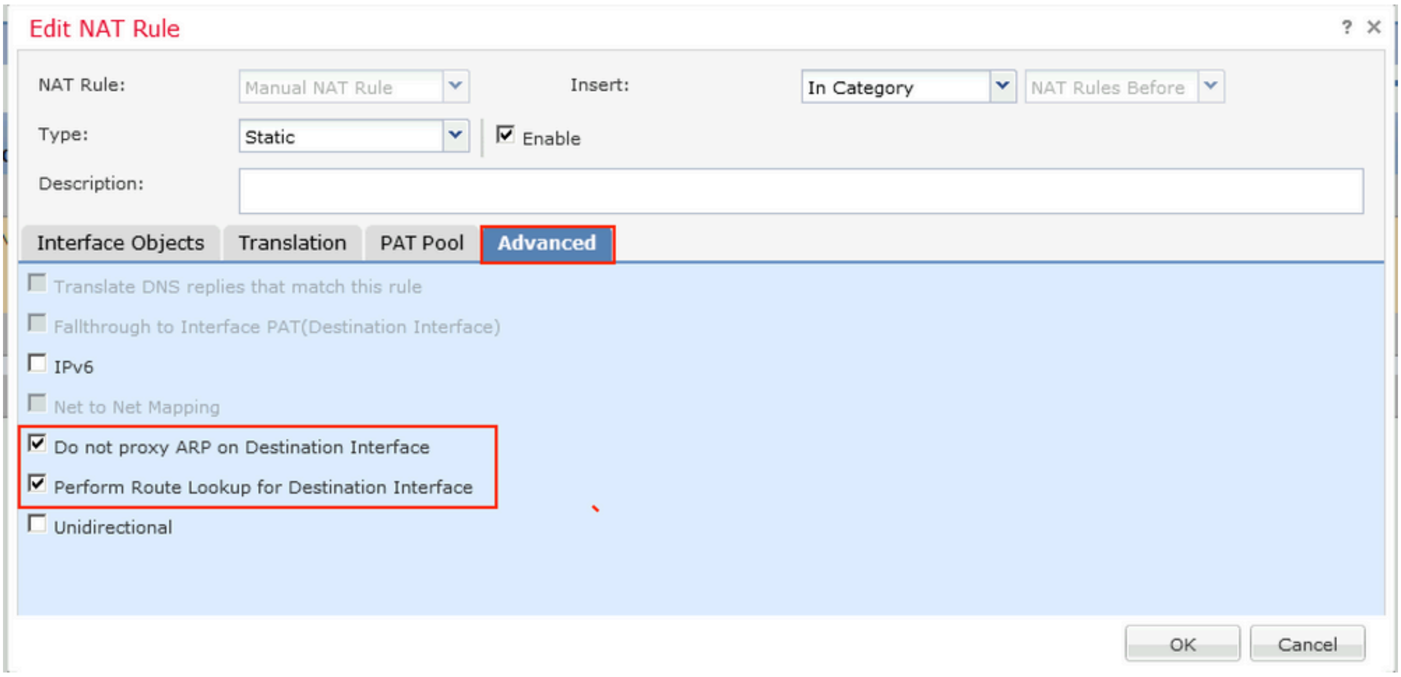
Translated Destination: VPN_Subnet

Translated Source Port:

Translated Destination Port:

OK | Cancel

Advanced(고급) 탭에서 이 이미지에 표시된 대로 확인란을 선택합니다.



Edit NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.