Configure AnyConnect VPN Client on FTD: Hairpin and NAT Exemption

Contents

Introduction

This document describes how to configure Cisco remote access VPN solution (AnyConnect) on Firepower Threat Defense (FTD), v6.3, managed by FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic remote access VPN, Secure Sockets Layer (SSL) and Internet Key Exchange (IKEv2) version 2 knowledge
- Basic Authentication, Authorization, and Accounting (AAA) and RADIUS knowledge
- Basic FMC knowledge
- Basic FTD knowledge

Components Used

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

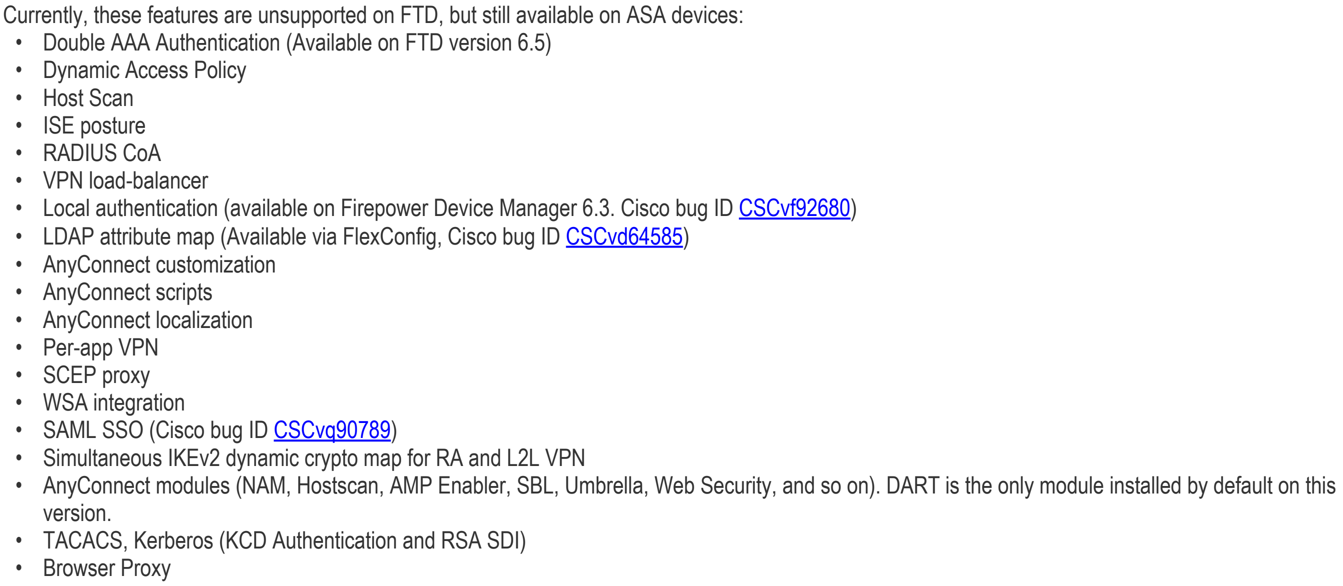
- Cisco FMC 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

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.

Background Information

This document is intended to cover the configuration on FTD devices. If you want the ASA configuration example, please refer to the document: Configure AnyConnect VPN Client U-turn Traffic on ASA 9.X

Limitations:



Currently, these features are unsupported on FTD, but still available on ASA devices:

- Double AAA Authentication (Available on FTD version 6.5)
- Dynamic Access Policy
- Host Scan
- ISE posture
- RADIUS CoA
- VPN load-balancer
- Local authentication (available on Firepower Device Manager 6.3. Cisco bug ID CSCvf92680)
- LDAP attribute map (Available via FlexConfig, Cisco bug ID CSCvd64585)
- AnyConnect customization
- AnyConnect scripts
- AnyConnect localization
- Per-app VPN
- SCEP proxy
- WSA integration
- SAML SSO (Cisco bug ID CSCvq90789)
- Simultaneous IKEv2 dynamic crypto map for RA and L2L VPN
- AnyConnect modules (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security, and so on). DART is the only module installed by default on this version.
- TACACS, Kerberos (KCD Authentication and RSA SDI)
- Browser Proxy

Configure

In order to go through the Remote Access VPN wizard in the FMC, these steps must be completed:

Step 1. Import an SSL Certificate

Certificates are essential when you configure AnyConnect. Only RSA based certificates are supported for SSL and IPSec. Elliptic Curve Digital Signature Algorithm (ECDSA) certificates are supported in IPSec, however, it is not possible to deploy a new AnyConnect package or XML profile when ECDSA based certificate is used. It can be used for IPSec, but you must pre-deploy the AnyConnect packages along with the XML profile, all the XML profile updates must be pushed manually on each client (Cisco bug ID CSCtx42595).

Additionally, the certificate must contain a Common Name (CN) extension with DNS name and/or IP address in order to avoid "Untrusted server certificate" errors in web browsers.

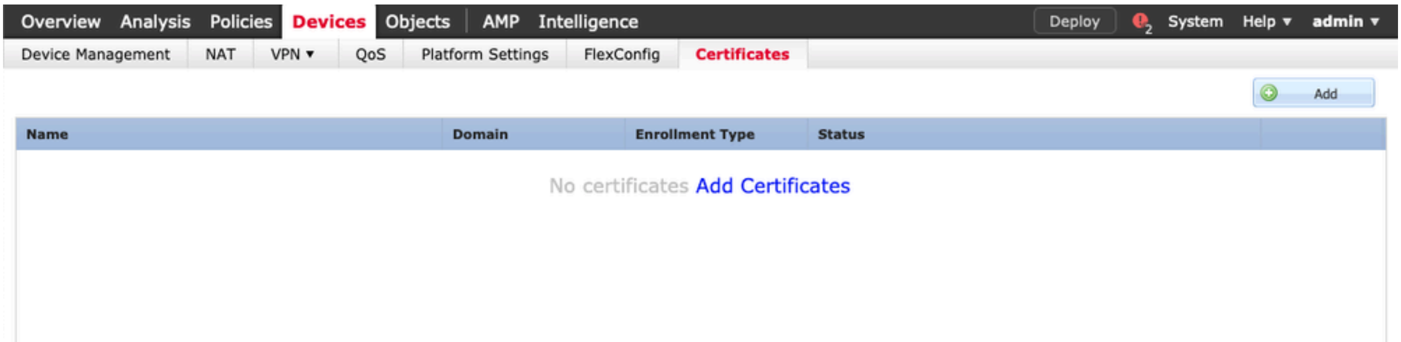
Note: On FTD devices, the Certificate Authority (CA) certificate is needed before the Certificate Signing Request (CSR) is generated.

- If the CSR is generated in an external server (such as Windows Server or OpenSSL), the manual enrollment method is intended to fail, since FTD does not support manual key enrollment.

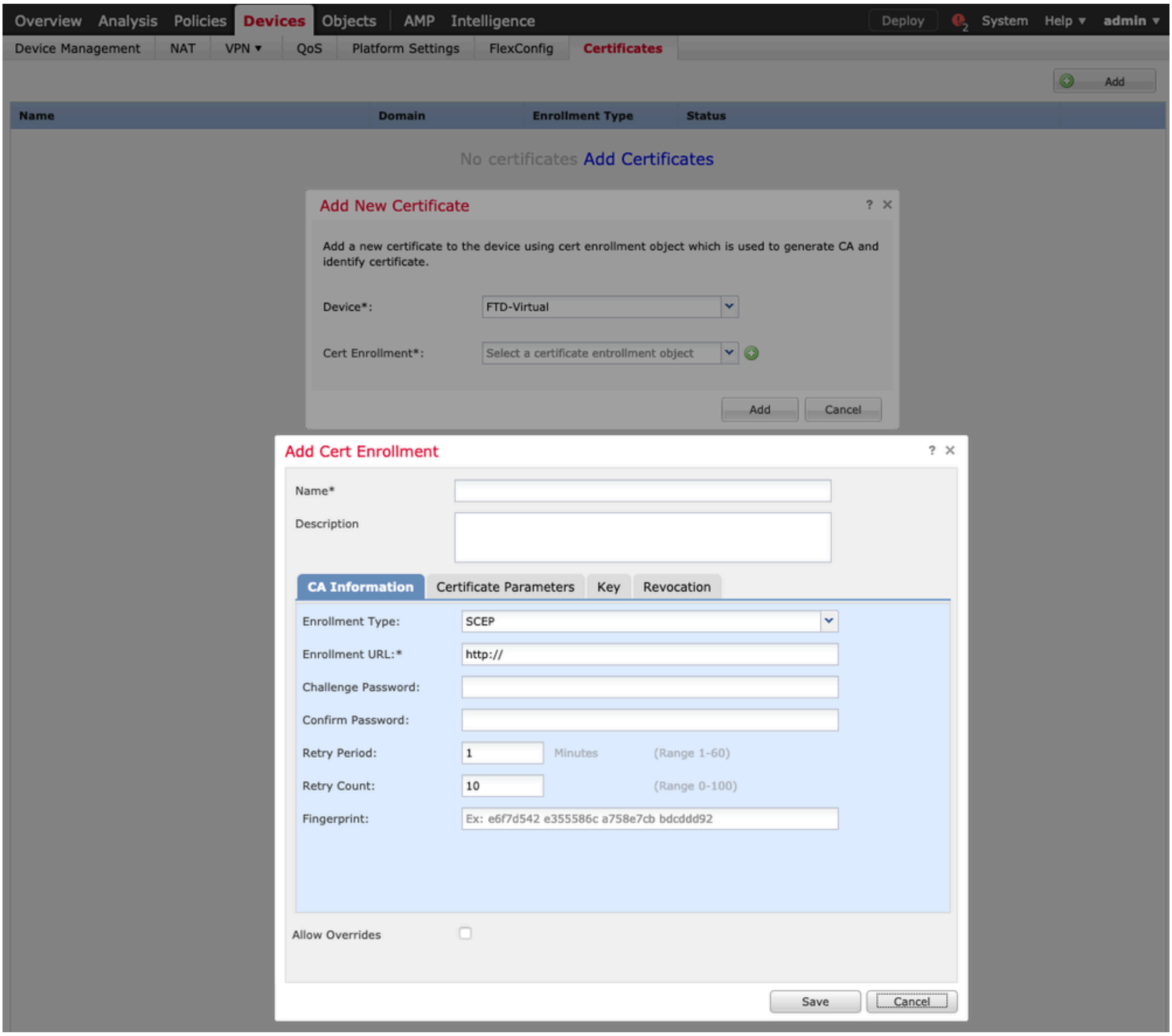
- A different method must be used such as PKCS12.

In order to get a certificate for the FTD appliance with the manual enrollment method, a CSR needs to be generated. Sign it with a CA and then import the identity certificate.

1. Navigate to **Devices** > **Certificates** and select **Add** as shown in the image.



2. Select the **Device** and add a new **Cert Enrollment** object as shown in the image.



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD-Virtual

Cert Enrollment*: Select a certificate entrollment object

Add Cert Enrollment

Name*

Description

Enrollment Type: SCEP

Enrollment URL:* http://

Challenge Password:

Confirm Password:

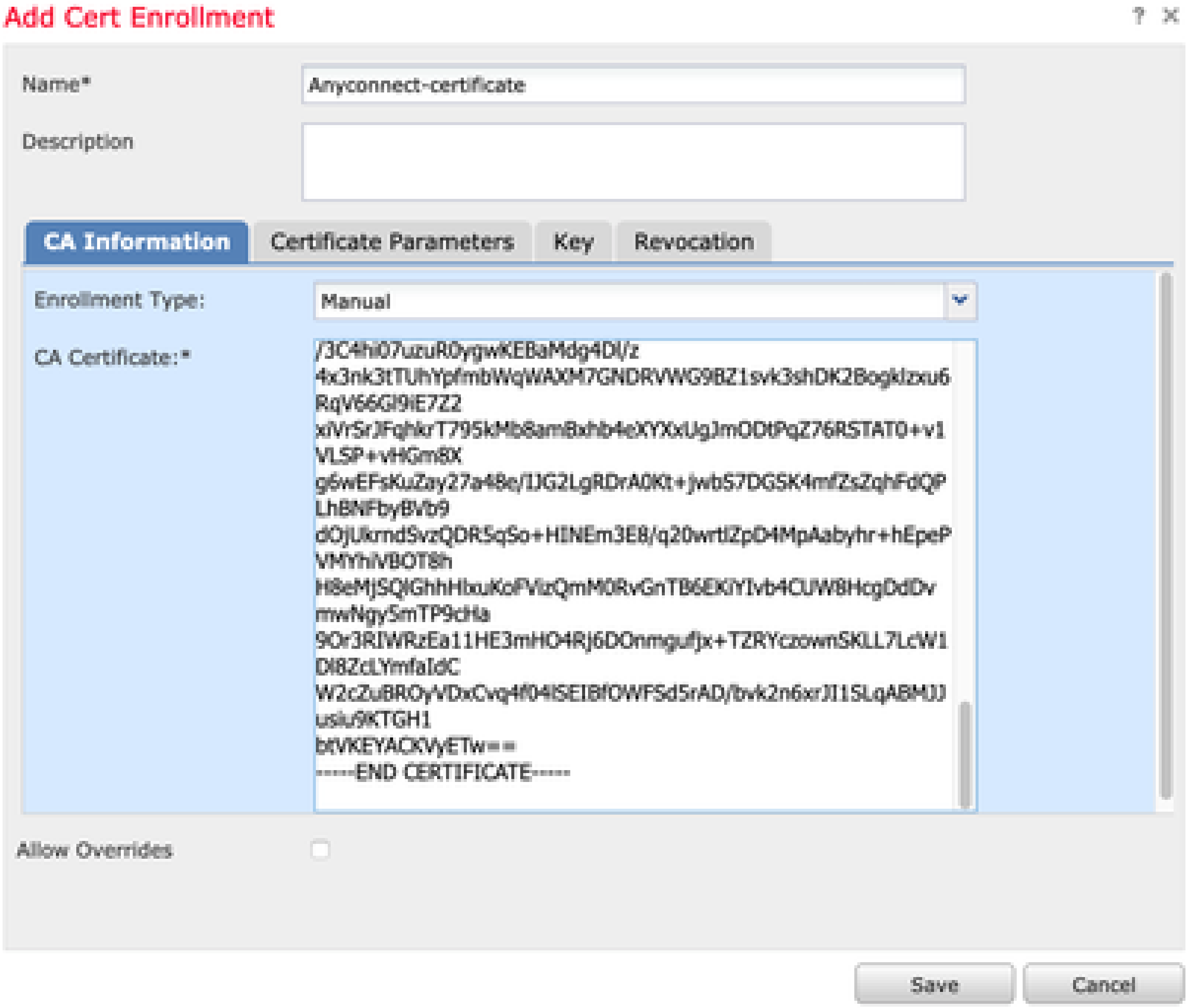
Retry Period: 1 Minutes (Range 1-60)

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7cb bdcddd92

Allow Overrides □

3. Select **manual Enrollment Type** and paste the CA certificate (the certificate which is intended to sign the CSR).



Add Cert Enrollment

Name* Anyconnect-certificate

Description

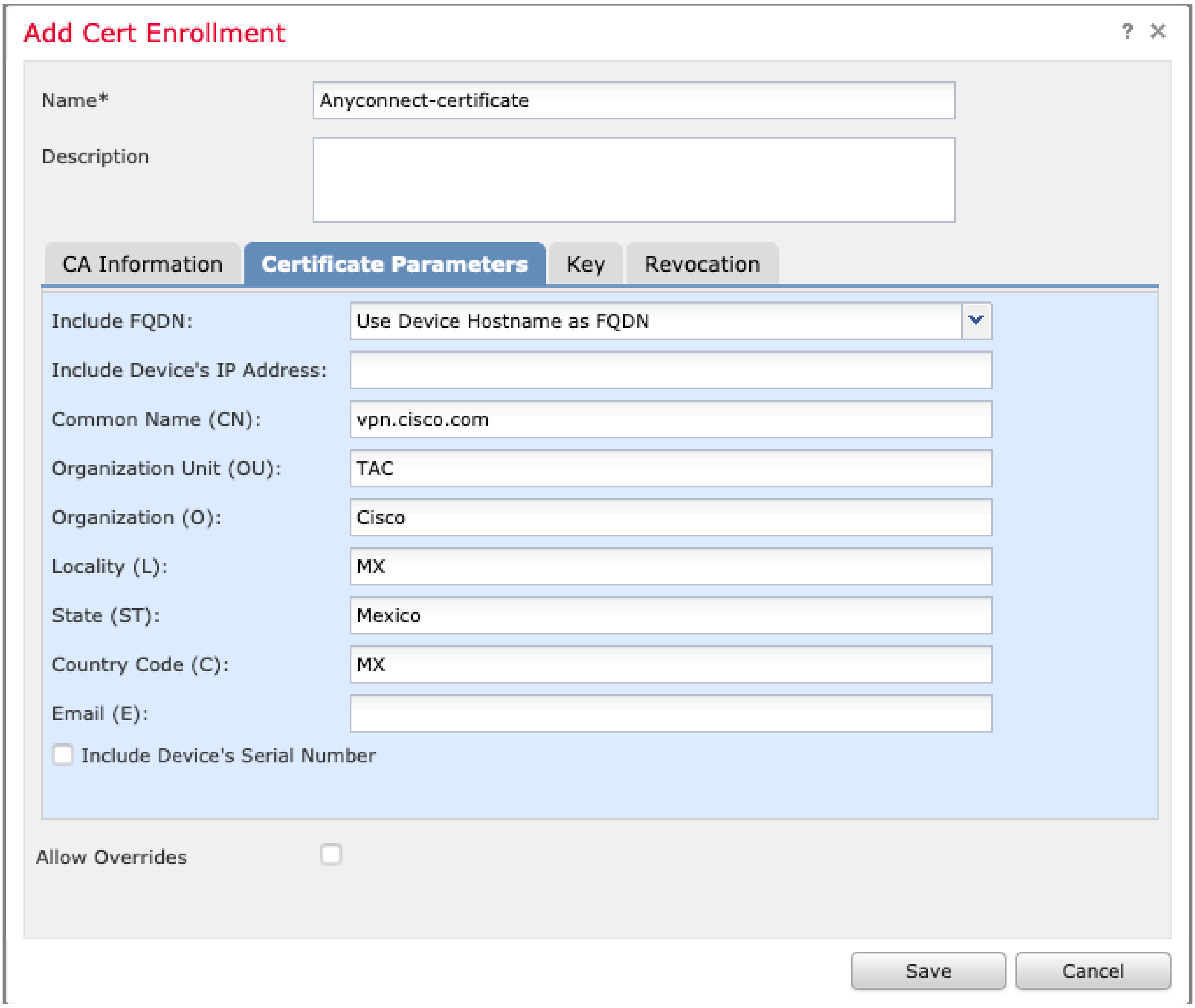
Enrollment Type: Manual

CA Certificate:*

```
/3C4hi07uzuR0ygwKEBaMdg4Dl/z
4x3nk3tTUhYpfmbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogklzxu6
RqV66GI9iE7Z2
xiVrSrJFqhkrT795kMb8amBxhb4eXYXxUgJmODtPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/1JG2LgRDrA0Kt+jwbS7DGSK4mfZsZqhFdQP
LhBNFbyBVb9
dOjUkrndSvzQDR5qSo+HINEm3E8/q20wrtlZpD4MpAabyhr+hEpeP
VMYhiVBOT8h
H8eMjSQlGhhHbuKoFVizQmM0RvGnTB6EKiYIvb4CUW8HcgDdDv
mwNgySmTP9cHa
9Or3RIWRzEa11HE3mHO4Rj6DOnmgufjx+TZRYczownSKLL7LcW1
Dl8ZcLYmfaIdC
W2cZuBROyVDxCvq4f04lSEIBfOWFSd5rAD/bvk2n6xrJI1SLqABMJJ
usiu9KTGH1
btVKEYACKVyETw==
-----END CERTIFICATE-----
```

Allow Overrides □

4. Select the **Certificate Parameters** tab and select **Custom FQDN** for the **Include FQDN** field and fill the certificate details a shown in the image.



Add Cert Enrollment

Name*: Anyconnect-certificate

Description:

Include FQDN: Use Device Hostname as FQDN

Include Device's IP Address:

Common Name (CN): vpn.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): MX

State (ST): Mexico

Country Code (C): MX

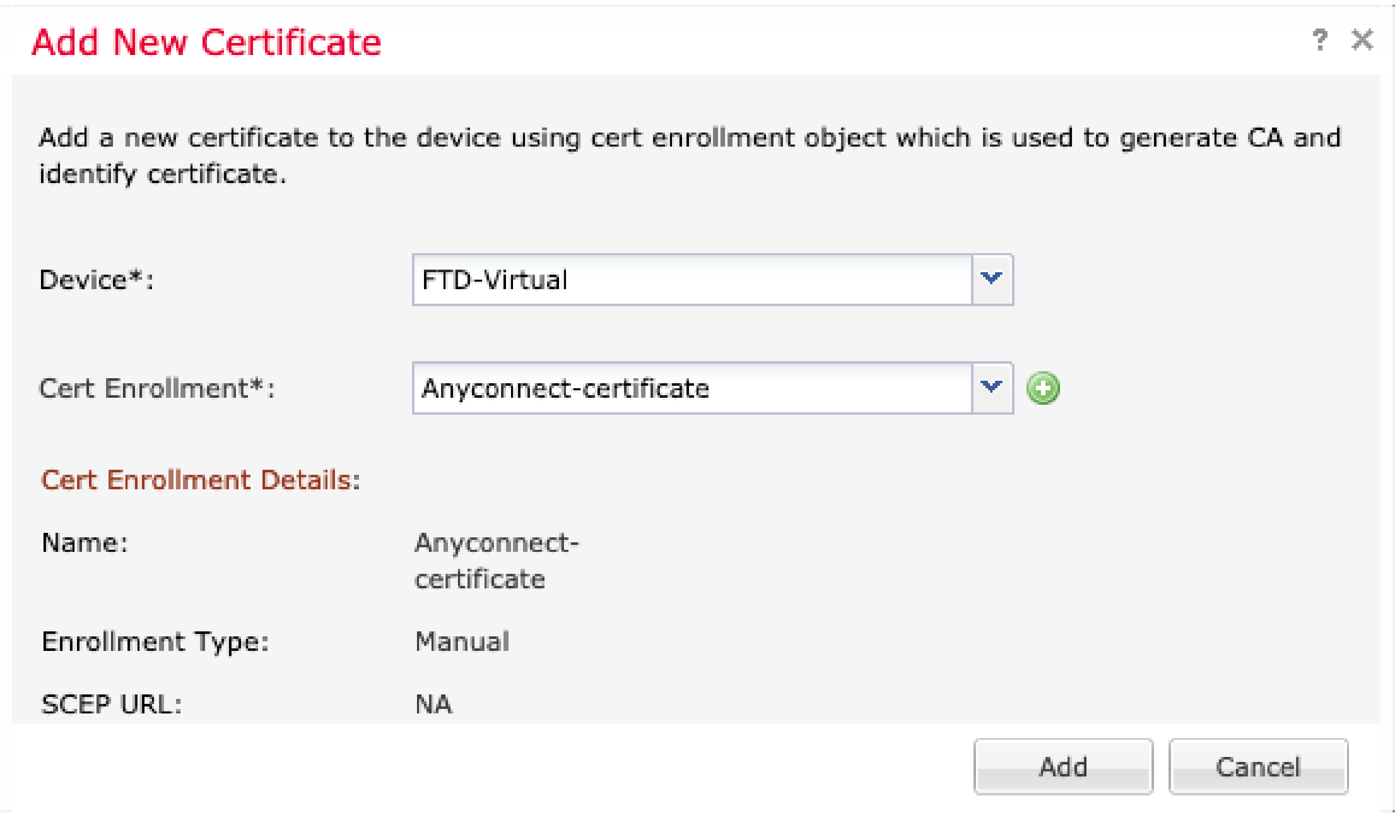
Email (E):

□ Include Device's Serial Number

Allow Overrides □

5. Select the **Key** tab, and select **key** type. You can choose name and size. For RSA, 2048 bytes is a minimum requirement.

6. Select **save**, confirm the **Device**, and under **Cert Enrollment** select the trustpoint which was just created. Select **Add** in order to deploy the certificate.



Add New Certificate

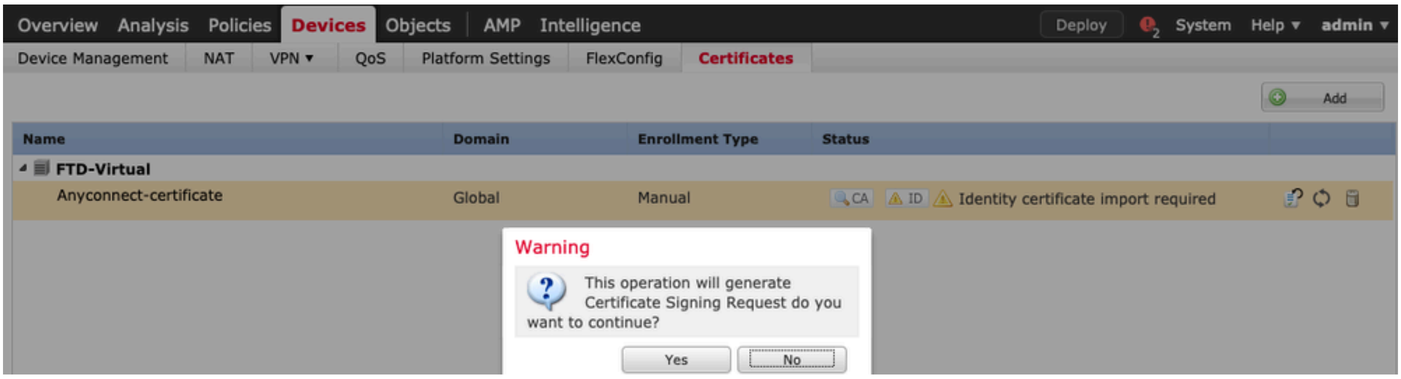
Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:	FTD-Virtual
Cert Enrollment*:	Anyconnect-certificate

Cert Enrollment Details:

Name:	Anyconnect-certificate
Enrollment Type:	Manual
SCEP URL:	NA

7. In the **Status** column, select the **ID** icon and select **Yes** to generate the CSR as shown in the image.



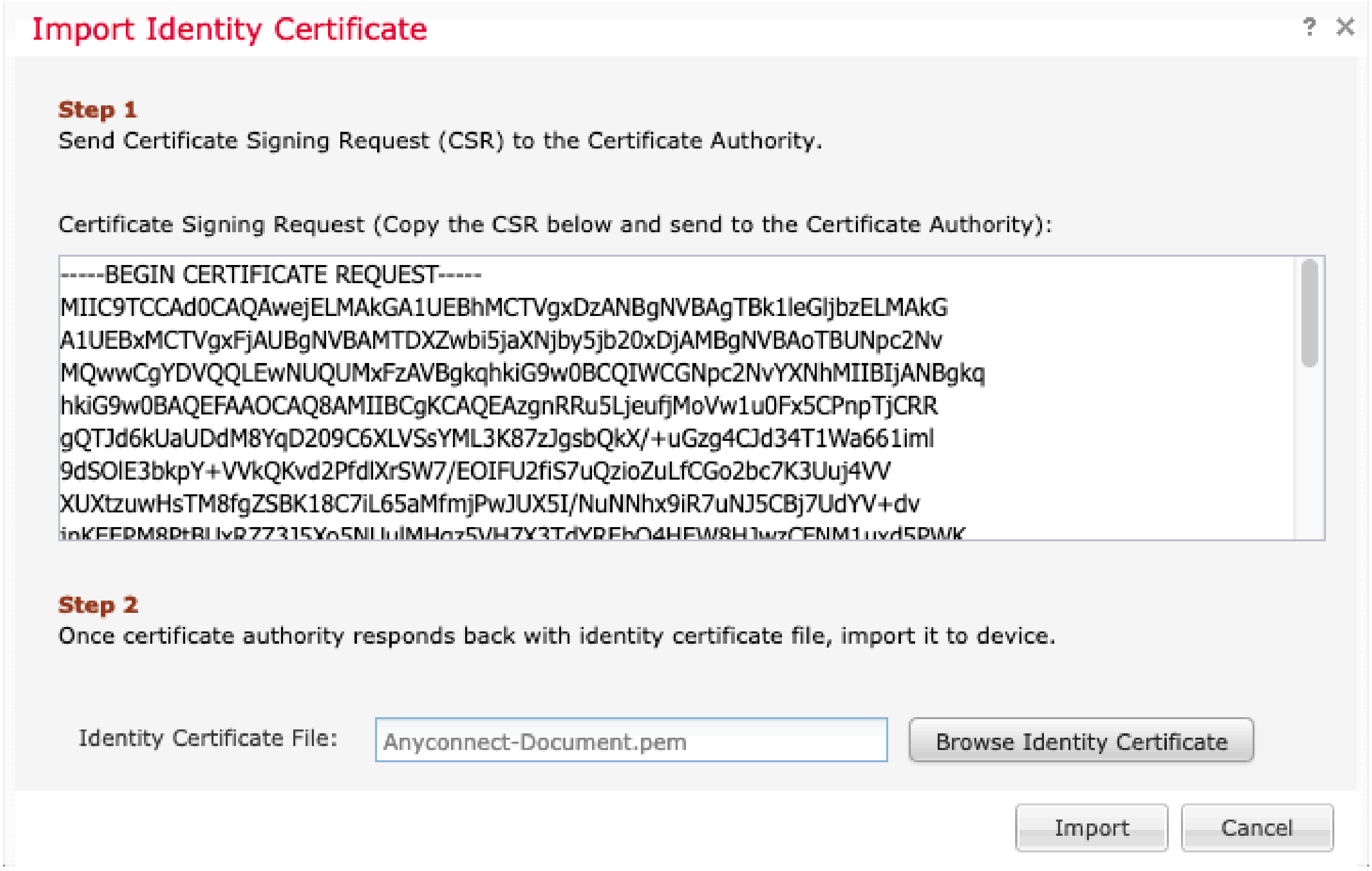
Name	Domain	Enrollment Type	Status
FTD-Virtual			
Anyconnect-certificate	Global	Manual	CA ID ⚠ Identity certificate import required

Warning

This operation will generate Certificate Signing Request do you want to continue?

8. Copy **CSR** and sign it with your preferred CA (for example, GoDaddy or DigiCert).

9. Once the identity certificate is received from the CA (which must be in base64 format), select **Browse Identity Certificate** and locate the certificate in the local computer. Select **Import**.



Step 1
Send Certificate Signing Request (CSR) to the Certificate Authority.

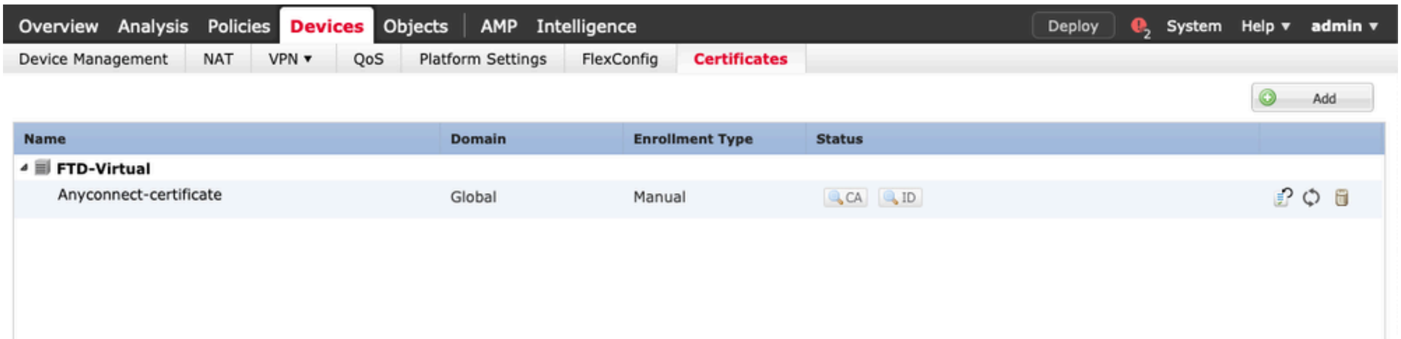
Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC9TCCAd0CAQAwejELMAkGA1UEBhMCTVgxDzANBgNVBAgTBk1leGljbzELMAkG
A1UEBxMCTVgxFjAUBgNVBAMTDXZwbi5jaXNjby5jb20xDjAMBgNVBAoTBUNpc2Nv
MQwwCgYDVQQLEwNUQUMxFzAVBgkqhkiG9w0BCQIWCGNpc2NvYXNhMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzgnRRu5LjeufjMoVw1u0Fx5CPnpTjCRR
gQTJd6kUaUDdM8YqD209C6XLVSsYML3K87zJgsbQkX/+uGzg4CJd34T1Wa661iml
9dSOlE3bkpY+VVkQKvd2PfdlXrSW7/EOIFU2fiS7uQzioZuLfCGo2bc7K3Uuj4VV
XUXtzuwHsTM8fgZSBK18C7iL65aMfmjPwJUX5I/NuNNhx9iR7uNJ5CBj7UdYV+dv
inKEFRM8PtBUxR77315Xo5NLUuIMHgz5VH7X3TdYREbO4HEW8HJwzCENM1uxd5RWK
```

Step 2
Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File: Anyconnect-Document.pem

10. Once imported, both CA and ID certificate details are available for display.

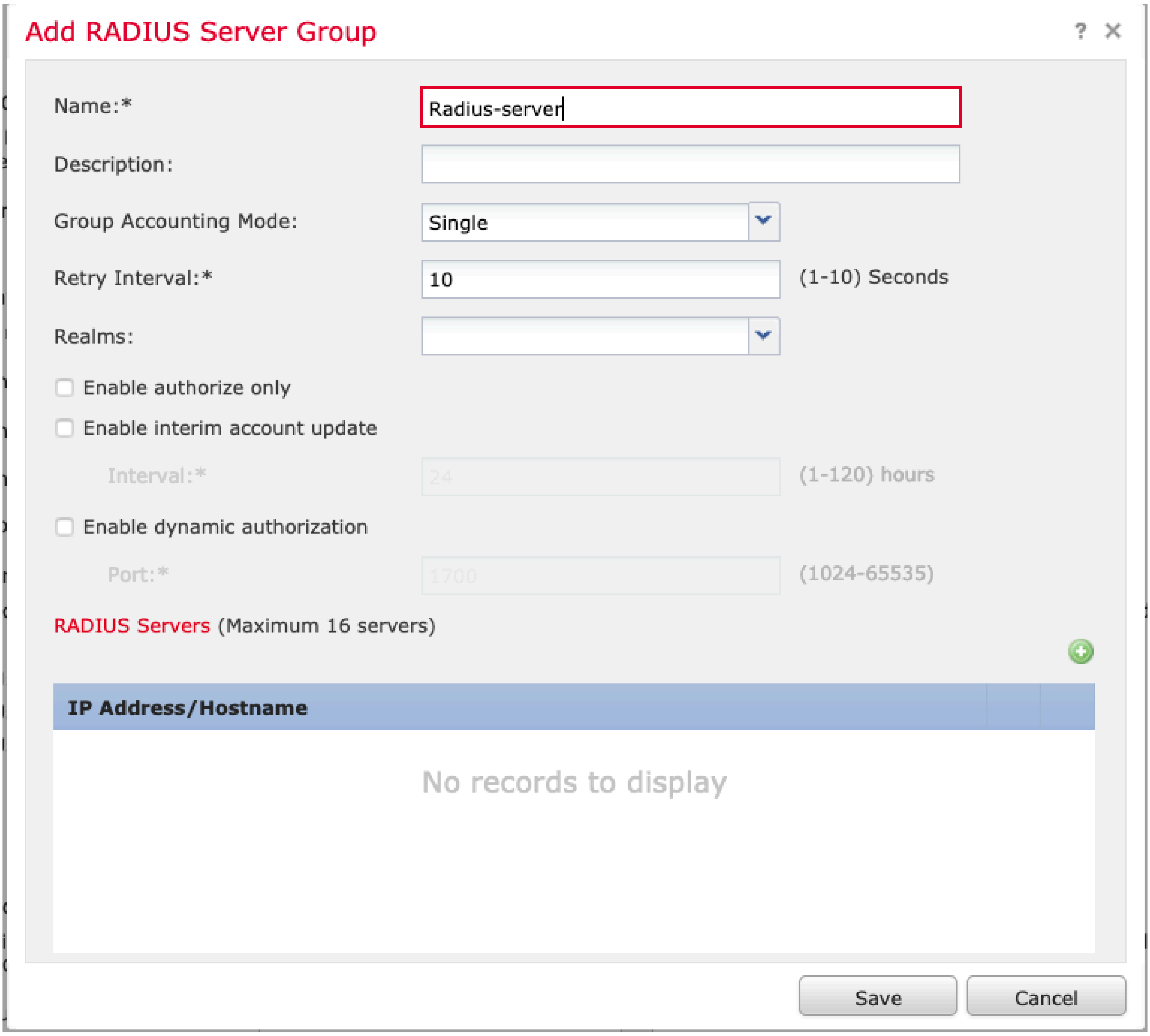


Name	Domain	Enrollment Type	Status
FTD-Virtual			
Anyconnect-certificate	Global	Manual	CA ID

Step 2. Configure a RADIUS Server

On FTD devices managed by FMC, the local user database is not supported. Another authentication method must be used, such as RADIUS or LDAP.

1. Navigate to **Objects** > **Object Management** > **RADIUS Server Group** > **Add RADIUS Server Group** as shown in the image.


Add RADIUS Server Group

Name:* Radius-server

Description:

Group Accounting Mode: Single

Retry Interval:* 10 (1-10) Seconds

Realms:

□ Enable authorize only

□ Enable interim account update

Interval:* 24 (1-120) hours

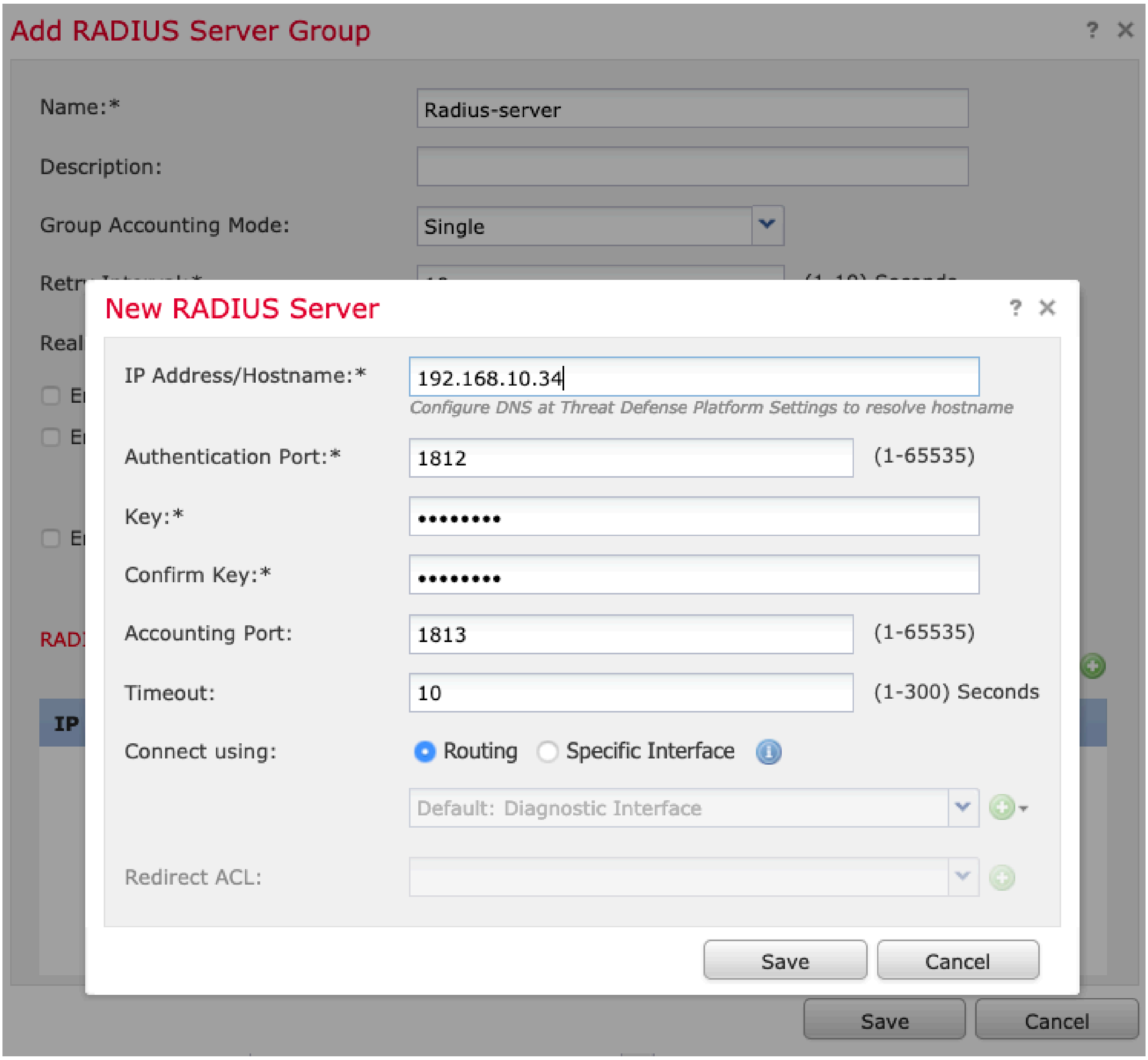
□ Enable dynamic authorization

Port:* 1700 (1024-65535)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

2. Assign a name to the **Radius Server Group** and add the **Radius server IP address** along with a shared secret (the shared secret is required to pair the FTD with the Radius server), select **Save** once this form is completed as shown in the image.



Add RADIUS Server Group

Name:* Radius-server

Description:

Group Accounting Mode: Single

New RADIUS Server

IP Address/Hostname:* 192.168.10.34

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* 1812 (1-65535)

Key:* ••••••••

Confirm Key:* ••••••••

Accounting Port: 1813 (1-65535)

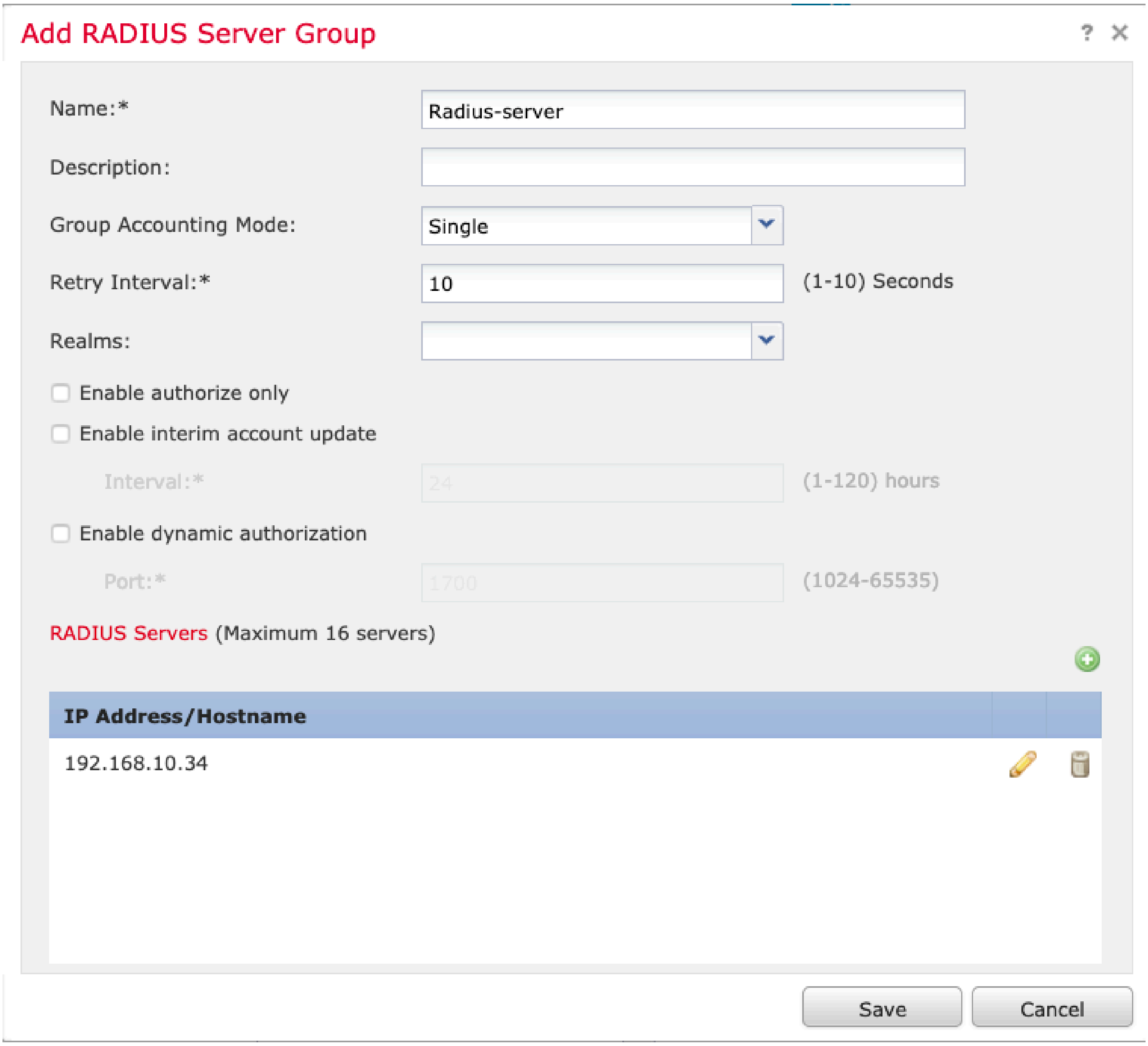
Timeout: 10 (1-300) Seconds

Connect using: ● Routing ○ Specific Interface

Default: Diagnostic Interface

Redirect ACL:

3. The RADIUS server information is now available in the Radius Server list as shown in the image.



Add RADIUS Server Group

Name:* Radius-server

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)

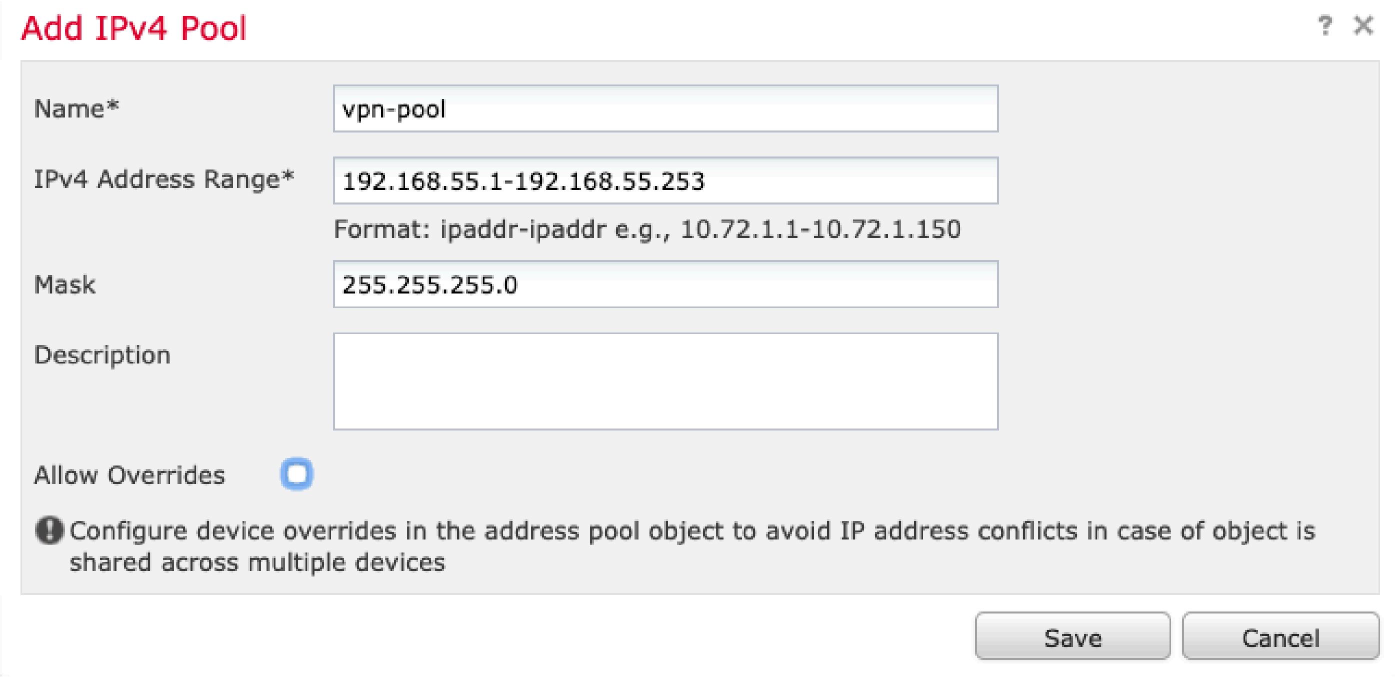
RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
192.168.10.34

Step 3. Create an IP Pool

1. Navigate to **Objects** > **Object Management** > **Address Pools** > **Add IPv4 Pools**.

2. Assign the **name** and r**ange of IP addresses**, Mask field is not required, but it can be specified as shown in the image.



Add IPv4 Pool

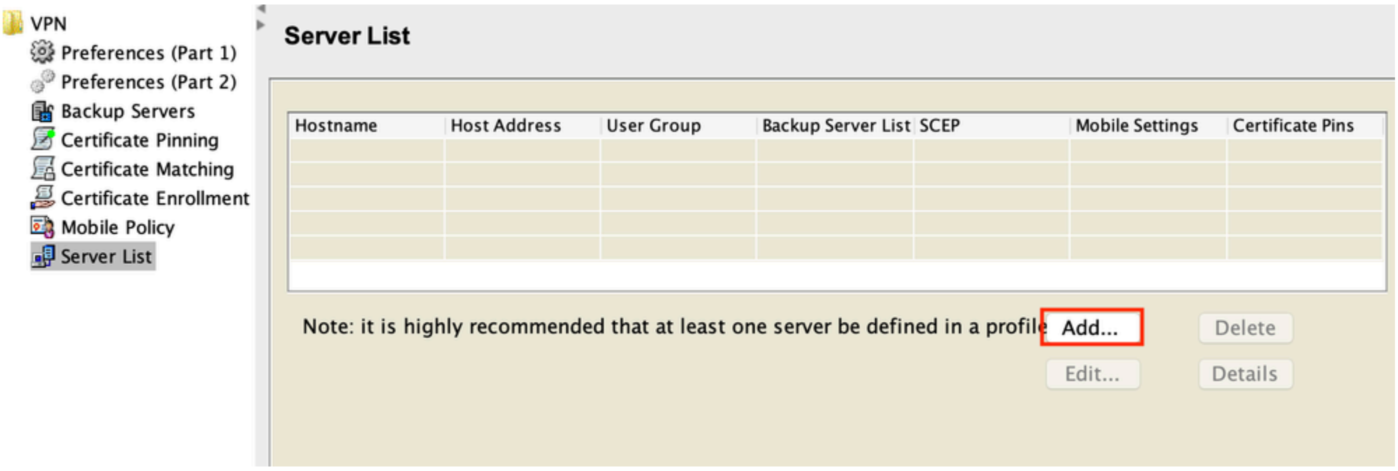
Name*	vpn-pool
IPv4 Address Range*	192.168.55.1-192.168.55.253 Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150
Mask	255.255.255.0
Description	
Allow Overrides	□

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

Step 4. Create an XML Profile

1. Download the **Profile Editor** tool from Cisco.com and run the application.

2. In the Profile Editor application, navigate to **Server List** and select **Add** as shown in the image.

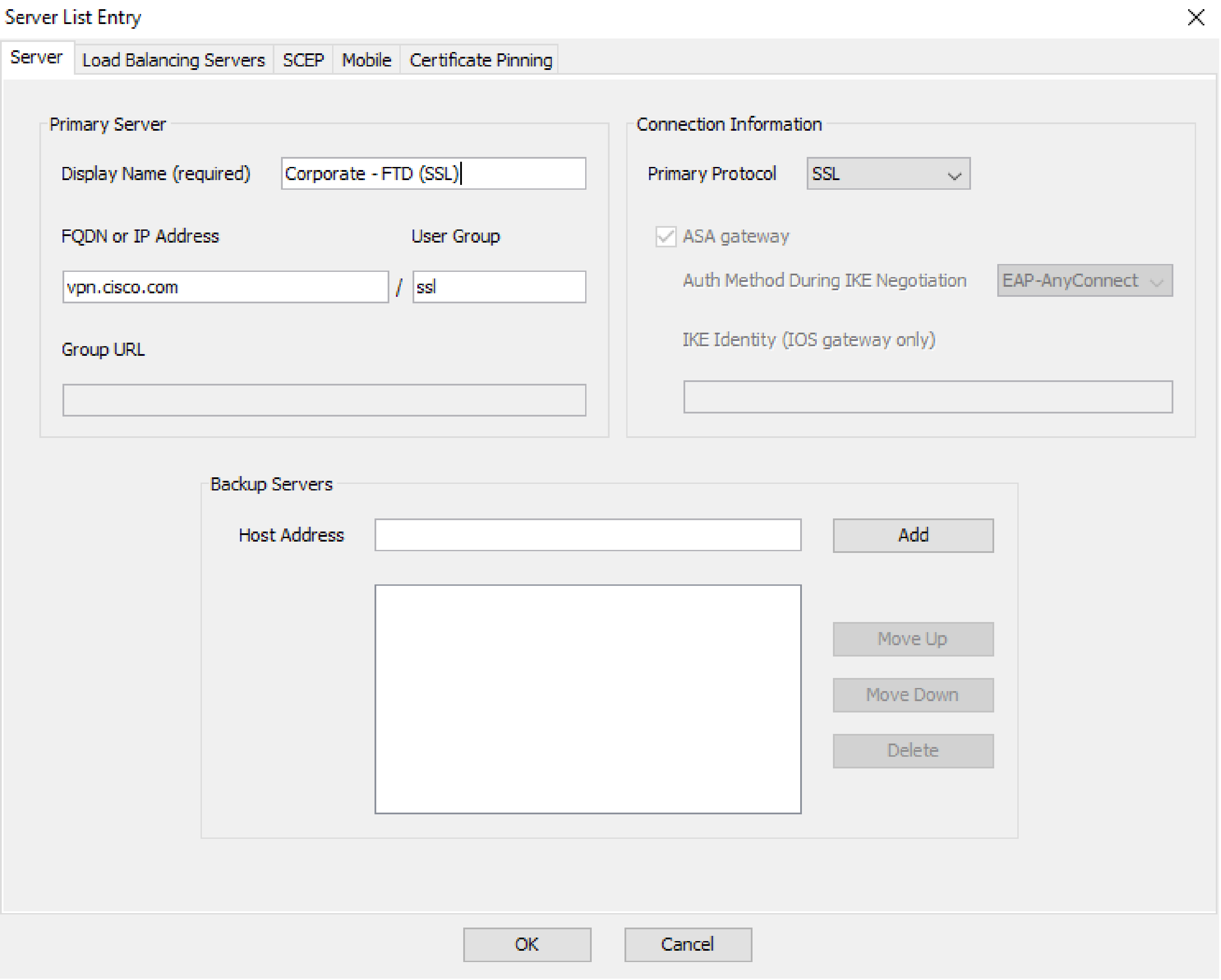


Server List

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins

Note: it is highly recommended that at least one server be defined in a profile

3. Assign a **Display Name, Fully Qualified Domain Name (FQDN) or IP Address** and select **OK** as shown in the image.



Primary Server

Display Name (required): Corporate - FTD (SSL)

FQDN or IP Address: vpn.cisco.com / User Group: ssl

Group URL:

Connection Information

Primary Protocol: SSL

☑ ASA gateway

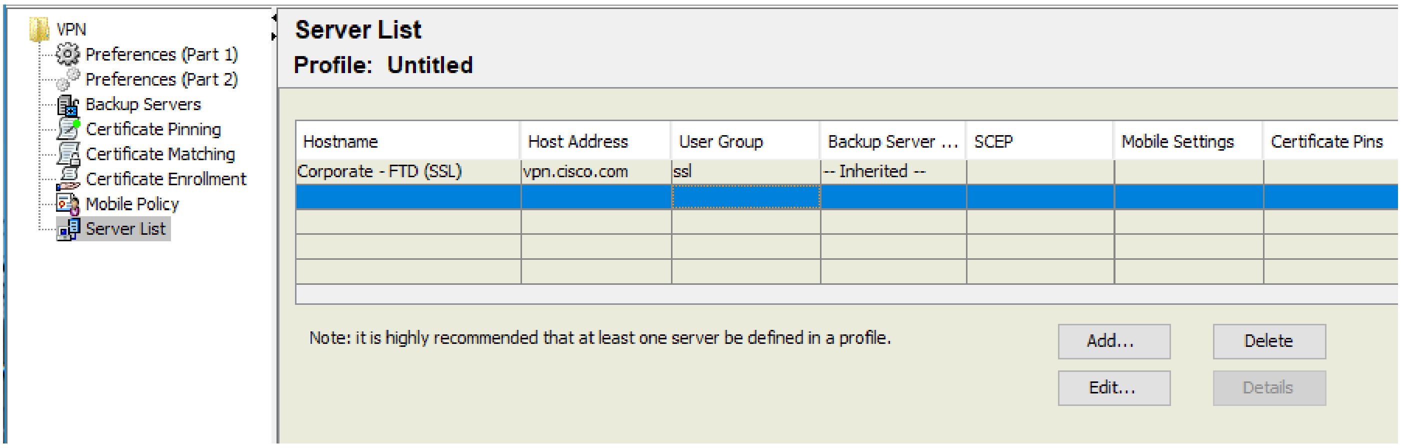
Auth Method During IKE Negotiation: EAP-AnyConnect

IKE Identity (IOS gateway only):

Backup Servers

Host Address:

4. The entry is now visible in the Server List menu:



Server List

Profile: Untitled

Hostname	Host Address	User Group	Backup Server ...	SCEP	Mobile Settings	Certificate Pins
Corporate - FTD (SSL)	vpn.cisco.com	ssl	-- Inherited --			

Note: it is highly recommended that at least one server be defined in a profile.

5. Navigate to **File** > **Save as**.

Note: Save the profile with an easily identifiable name with an extension.

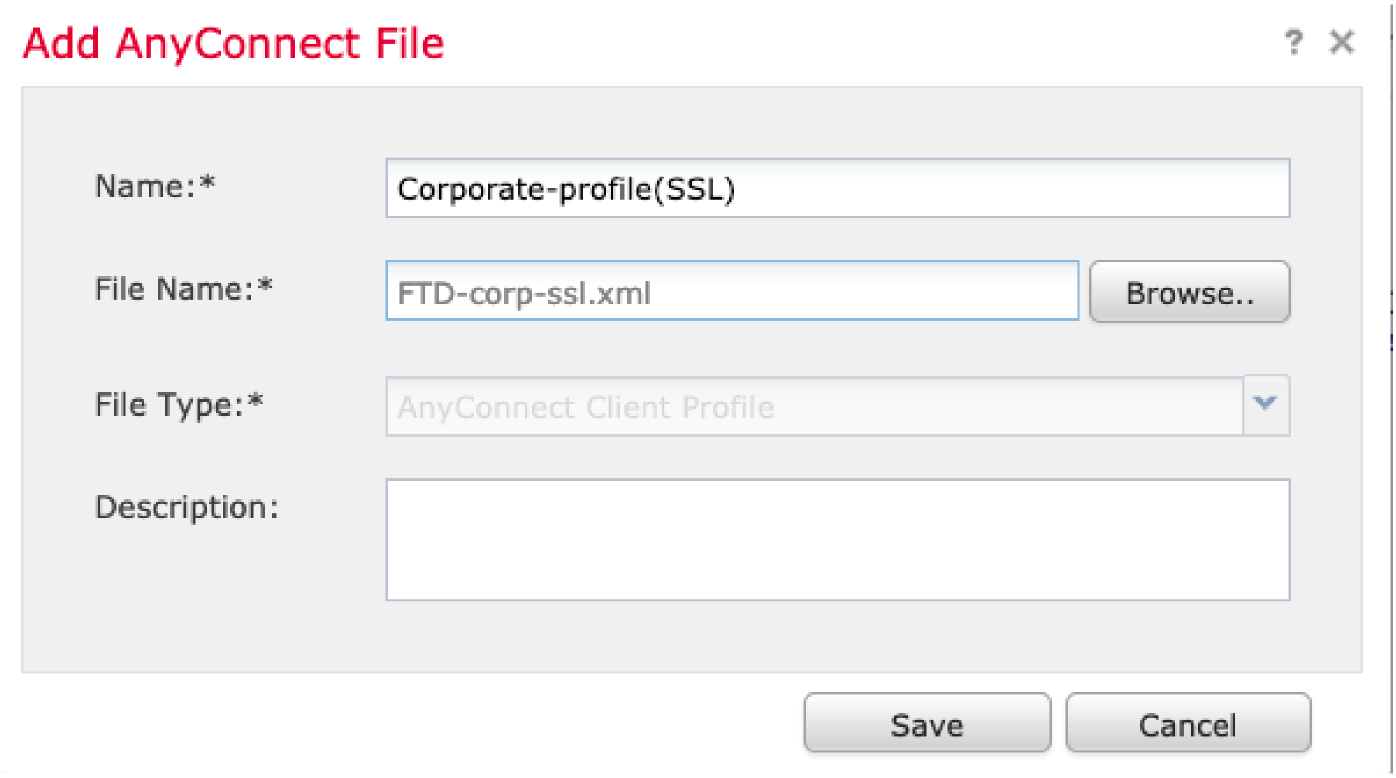
Step 5. Upload AnyConnect XML Profile

1. In the FMC, navigate to **Objects** > **Object Management** > **VPN** > **AnyConnect File** > **Add**

AnyConnect File.

2. Assign a **name** to the object and click **Browse**. Locate the client profile in your local system and select **Save**.

⚠ **Caution**: Ensure you select **AnyConnect Client Profile** as the file type.



Add AnyConnect File

Name:* Corporate-profile(SSL)

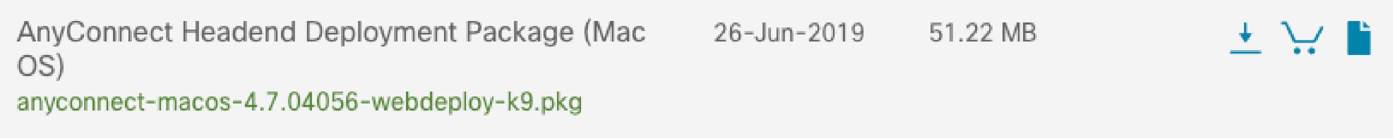
File Name:* FTD-corp-ssl.xml

File Type:* AnyConnect Client Profile

Description:

Step 6. Upload AnyConnect Images

1. Download the **webdeploy (.pkg)** images from the Cisco downloads webpage.



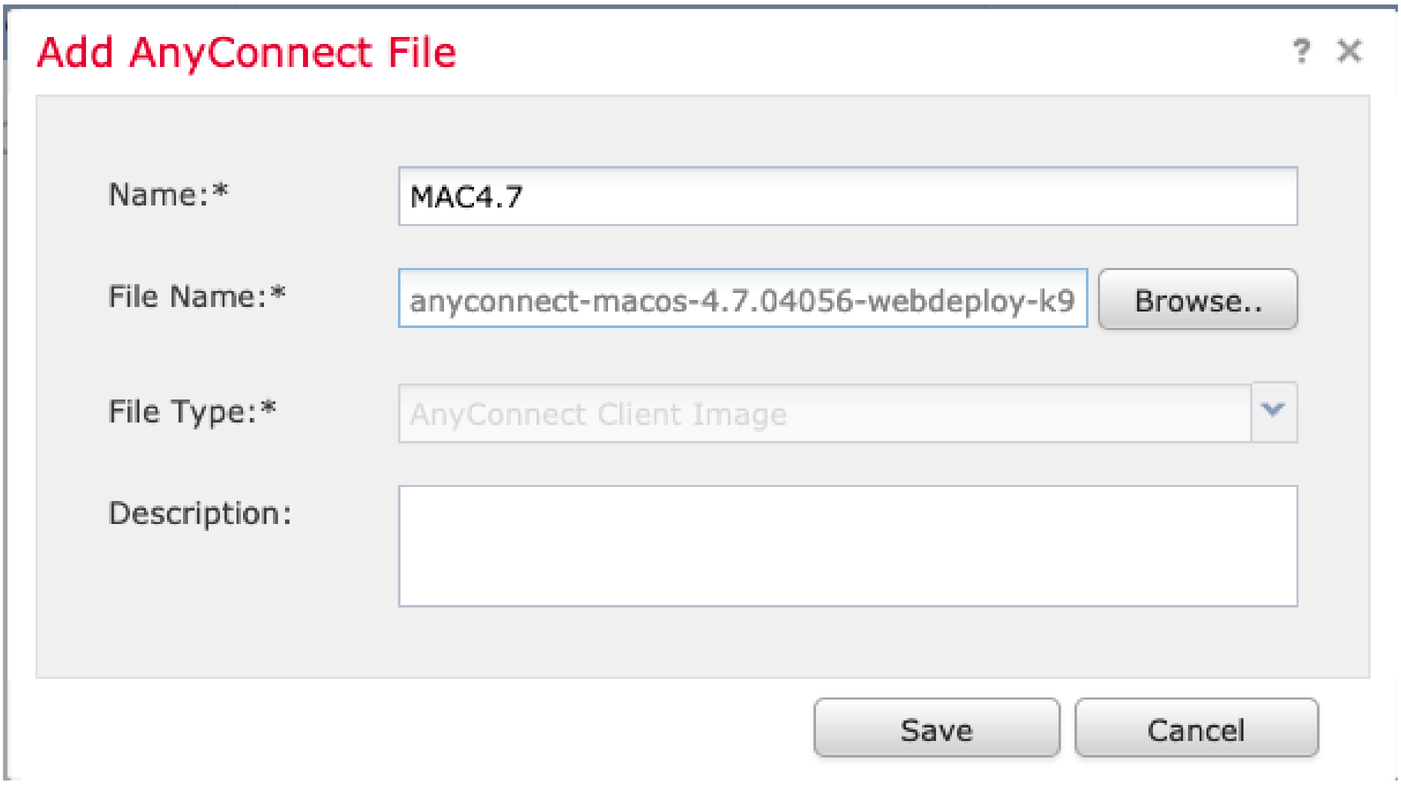
AnyConnect Headend Deployment Package (Mac OS) 26-Jun-2019 51.22 MB

anyconnect-macos-4.7.04056-webdeploy-k9.pkg

2. Navigate to **Objects** > **Object Management** > **VPN** > **AnyConnect File** > **Add AnyConnect File**.

3. Assign a name to the **AnyConnect package** file and select the **.pkg** file from your local system, once the file is selected.

4. Select **Save**.



Add AnyConnect File

Name:* MAC4.7

File Name:* anyconnect-macos-4.7.04056-webdeploy-k9

File Type:* AnyConnect Client Image

Description:

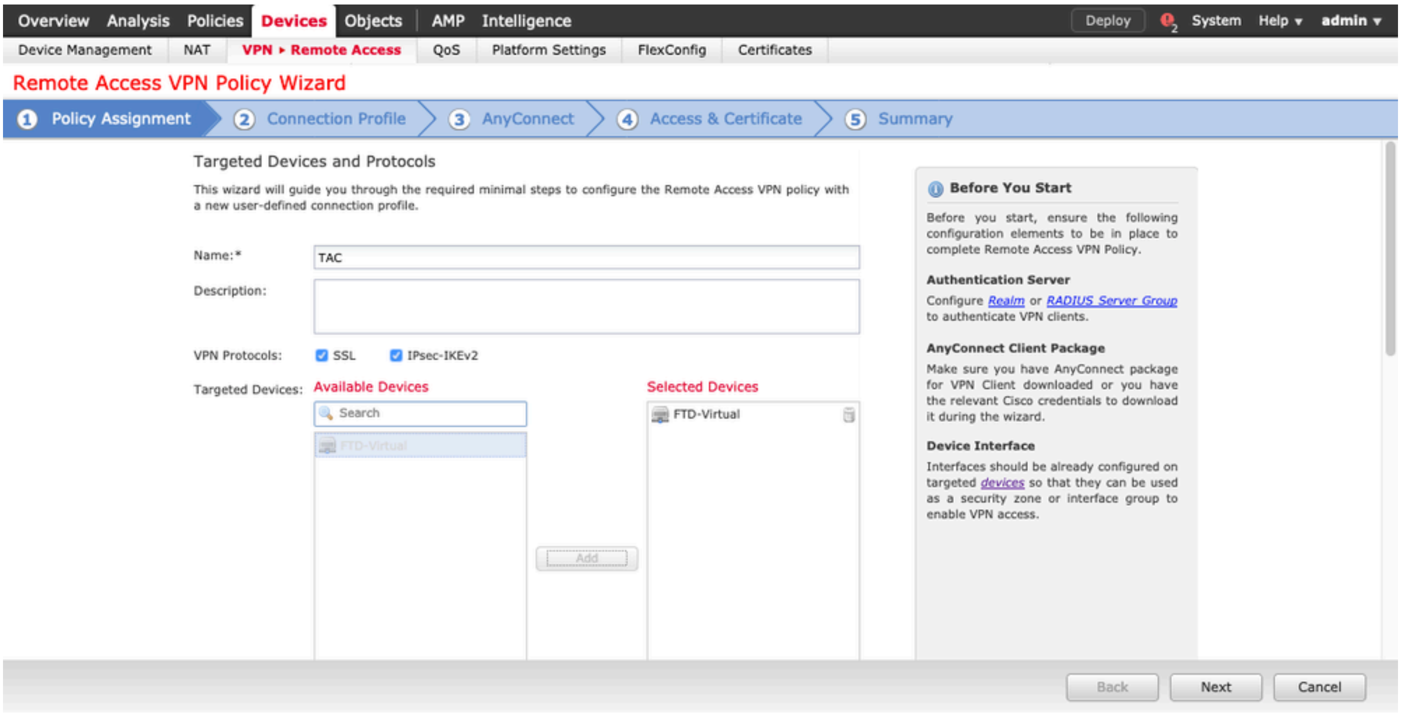
Note: Additional packages can be uploaded based on your requirements (Windows, MAS, Linux).

Step 7. Remote Access VPN Wizard

Based on the previous steps, the Remote Access Wizard can be followed accordingly.

1. Navigate to **Devices** > **VPN** > **Remote Access**.

2. Assign the **name** of the Remote Access policy and select an **FTD device** from the **Available Devices**.



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:* TAC

Description:

VPN Protocols: ☑ SSL ☑ IPsec-IKEv2

Targeted Devices: Available Devices: FTD-Virtual — Selected Devices: FTD-Virtual

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

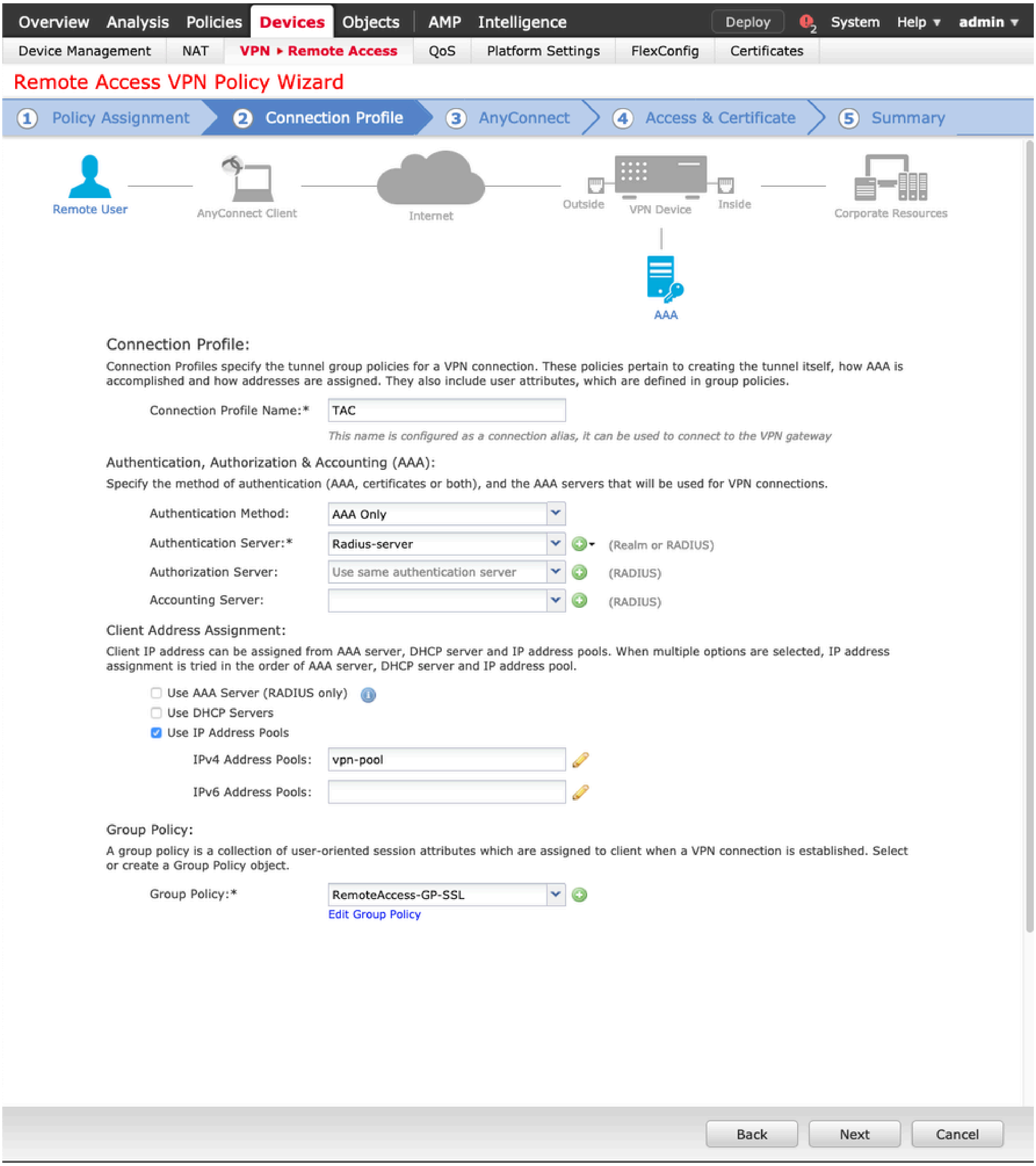
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

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.

3. Assign the **Connection Profile Name** (the Connection Profile Name is the tunnel-group name), select

Authentication Server and **Address Pools** as shown in the image.



Remote Access VPN Policy Wizard

Connection Profile:

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

Connection Profile Name:* TAC

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:* Radius-server (Realm or RADIUS)

Authorization Server: Use same authentication server (RADIUS)

Accounting Server: (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-pool

IPv6 Address Pools:

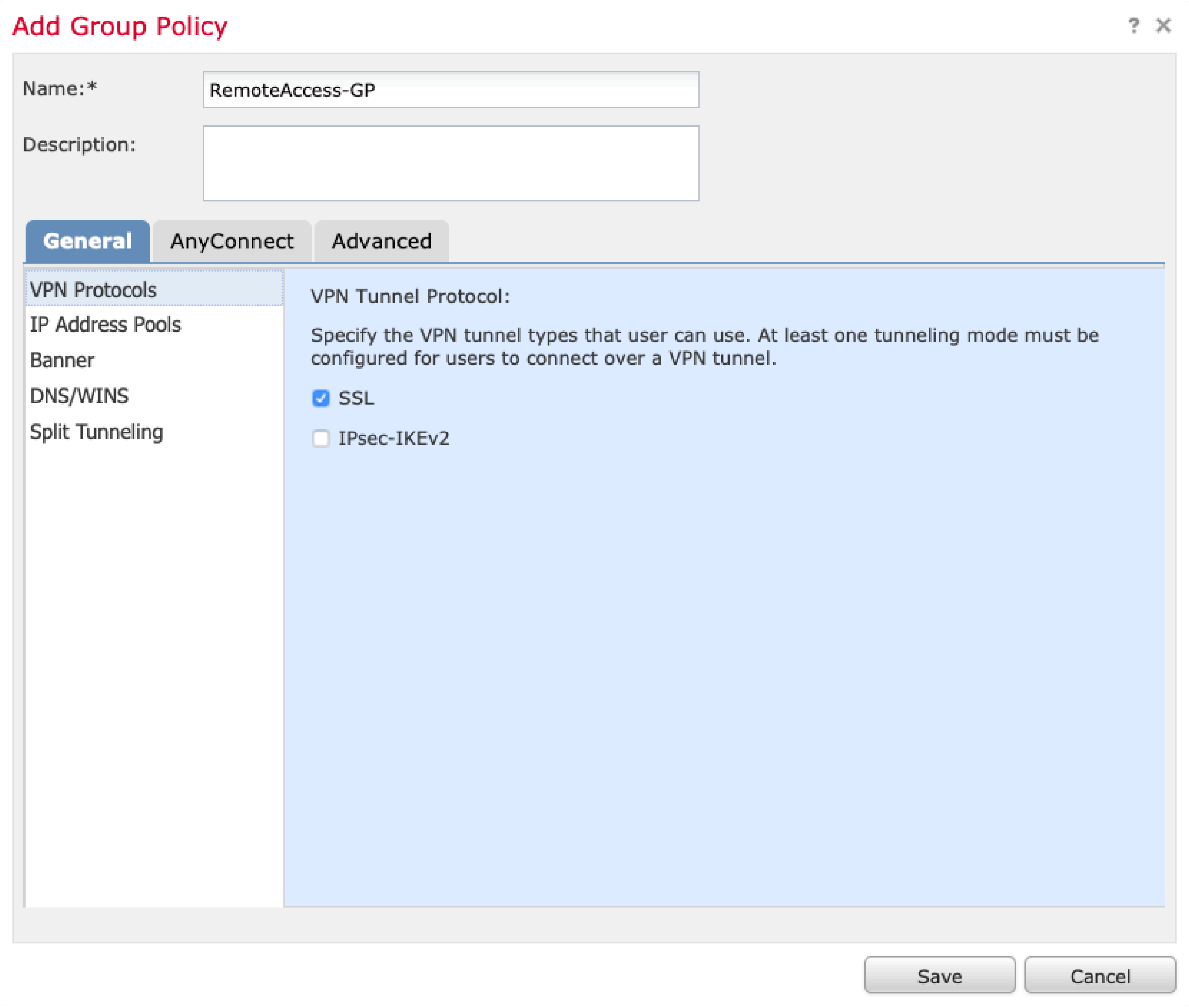
Group Policy:

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:* RemoteAccess-GP-SSL

Edit Group Policy

4. Select the + symbol in order to create **Group Policy**.



Add Group Policy

Name:* RemoteAccess-GP

Description:

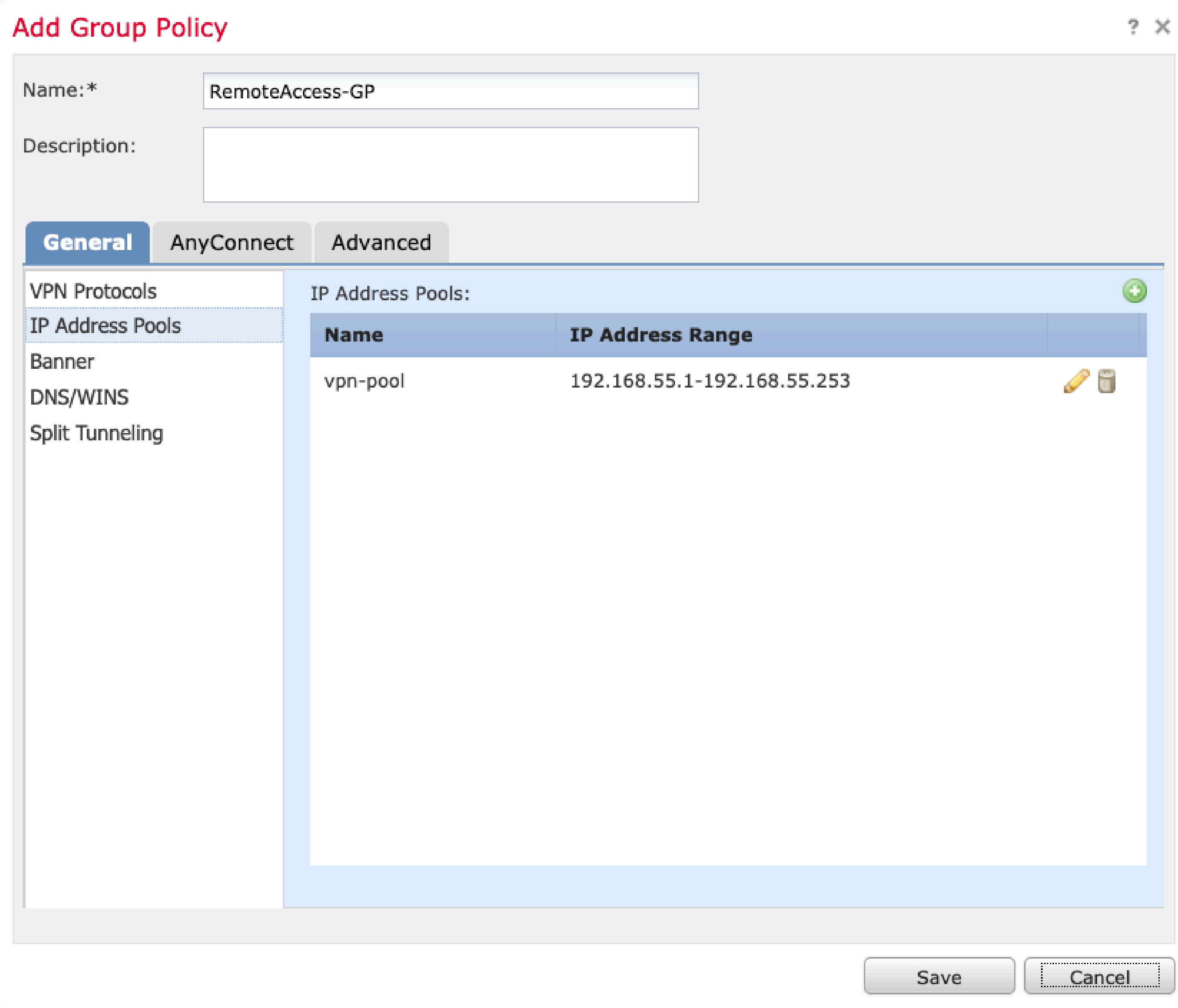
VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

☑ SSL

□ IPsec-IKEv2

5. (Optional) A local IP address pool can be configured in a group policy basis. If it is not configured, the pool is inherited from the pool configured in the Connection Profile (tunnel-group).



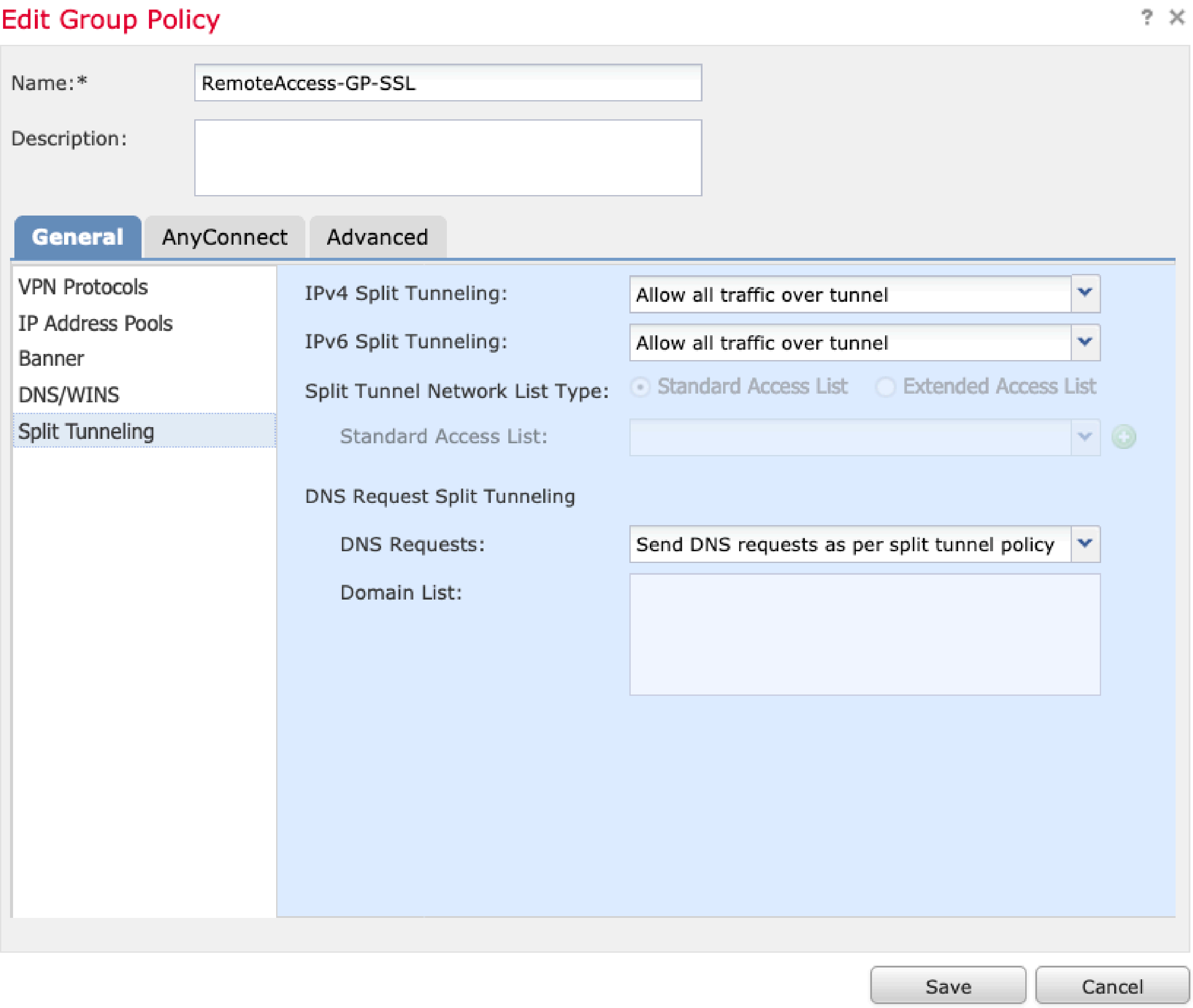
Add Group Policy

Name:* RemoteAccess-GP

Description:

Name	IP Address Range
vpn-pool	192.168.55.1-192.168.55.253

6. For this scenario, all the traffic is routed over the tunnel, **IPv4 Split Tunneling** policy is set to **Allow all traffic over the tunnel** as shown in the image.



Edit Group Policy

Name:* RemoteAccess-GP-SSL

Description:

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

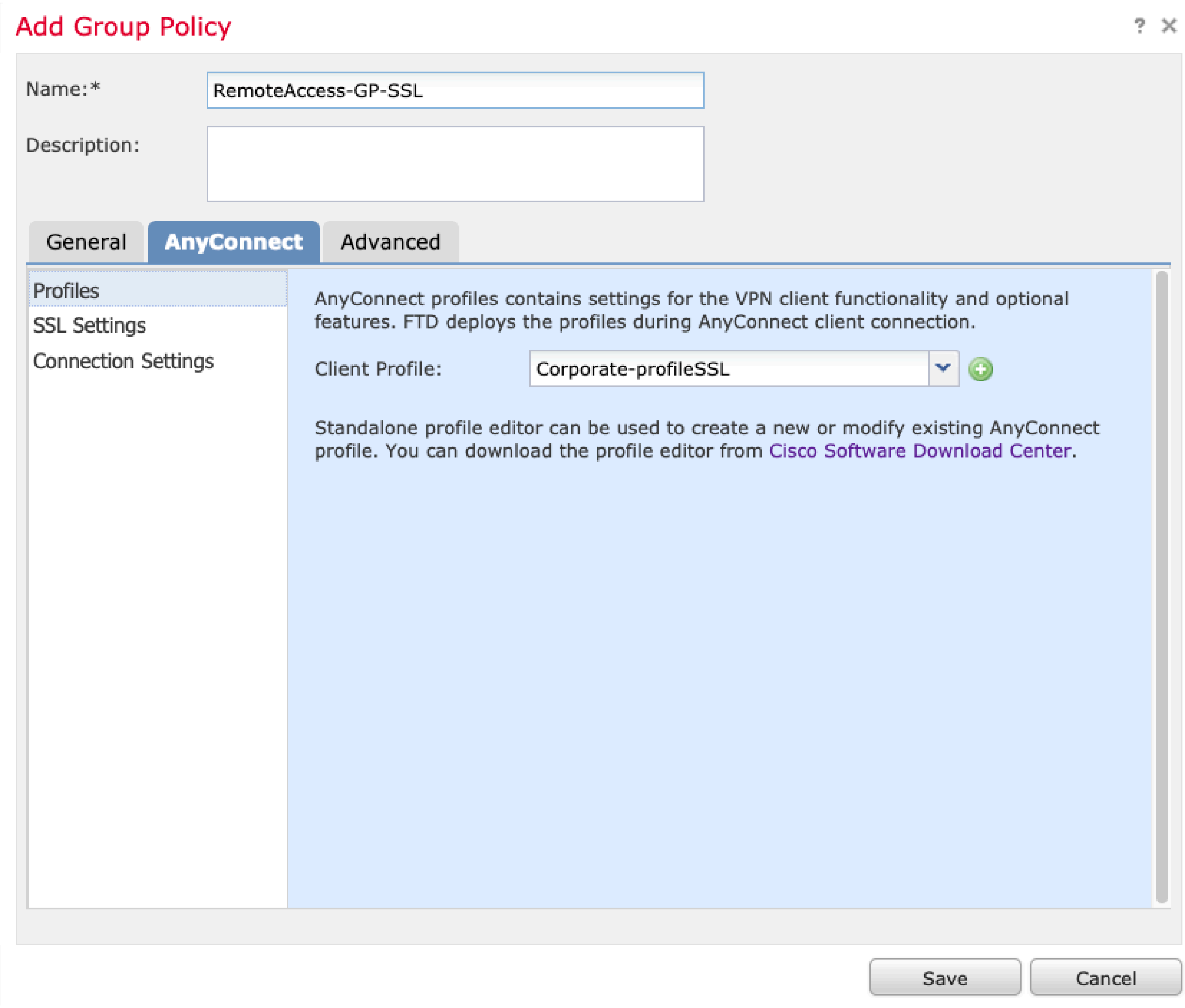
Standard Access List:

DNS Request Split Tunneling

DNS Requests: Send DNS requests as per split tunnel policy

Domain List:

7. Select the **.xml** profile for AnyConnect profile and select **Save** as shown in the image.



Add Group Policy

Name:* RemoteAccess-GP-SSL

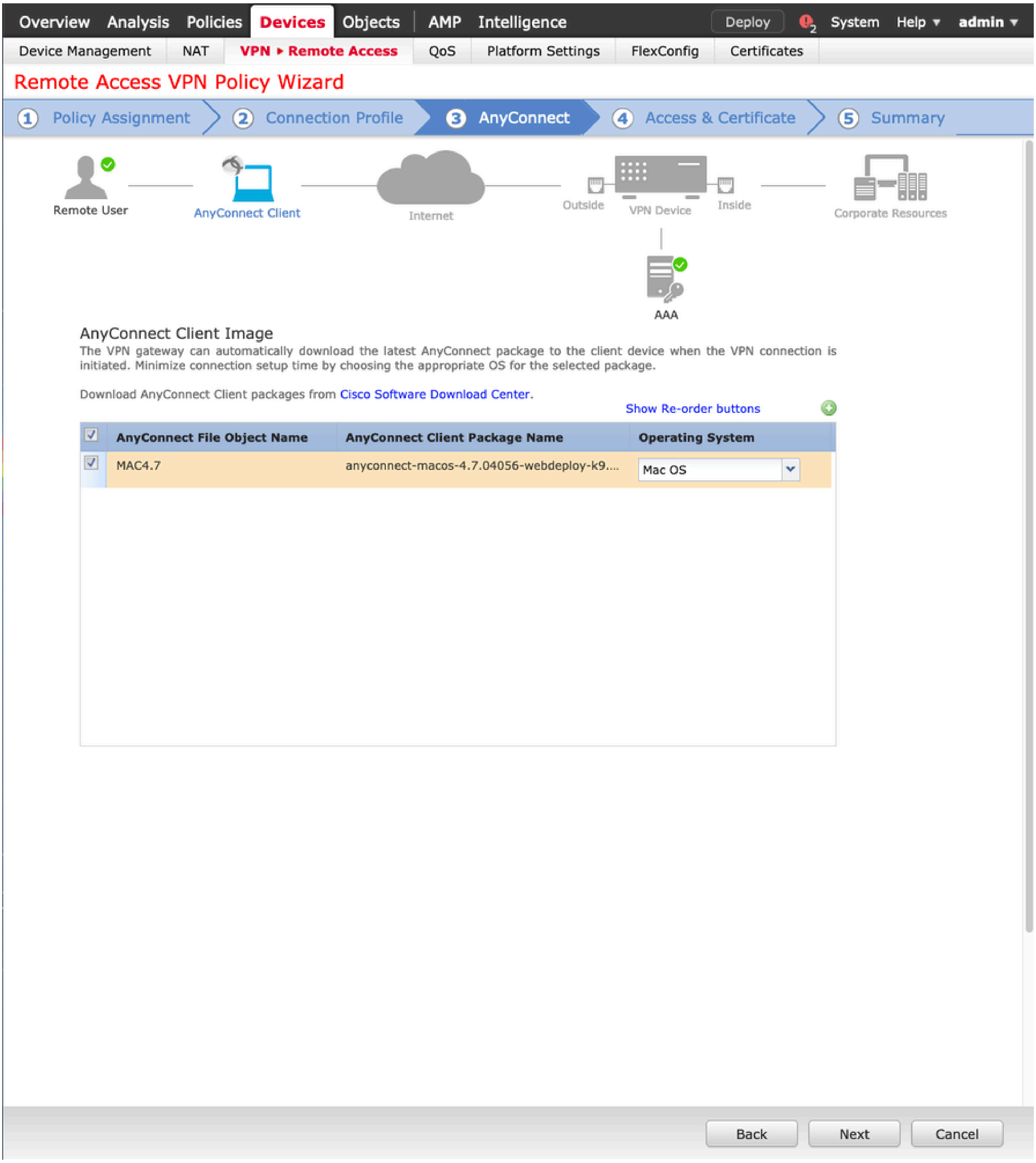
Description:

AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.

Client Profile: Corporate-profileSSL

Standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from Cisco Software Download Center.

8. Select the desired **AnyConnect images** based on the operative system requirements, select **Next** a shown in the image.



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.

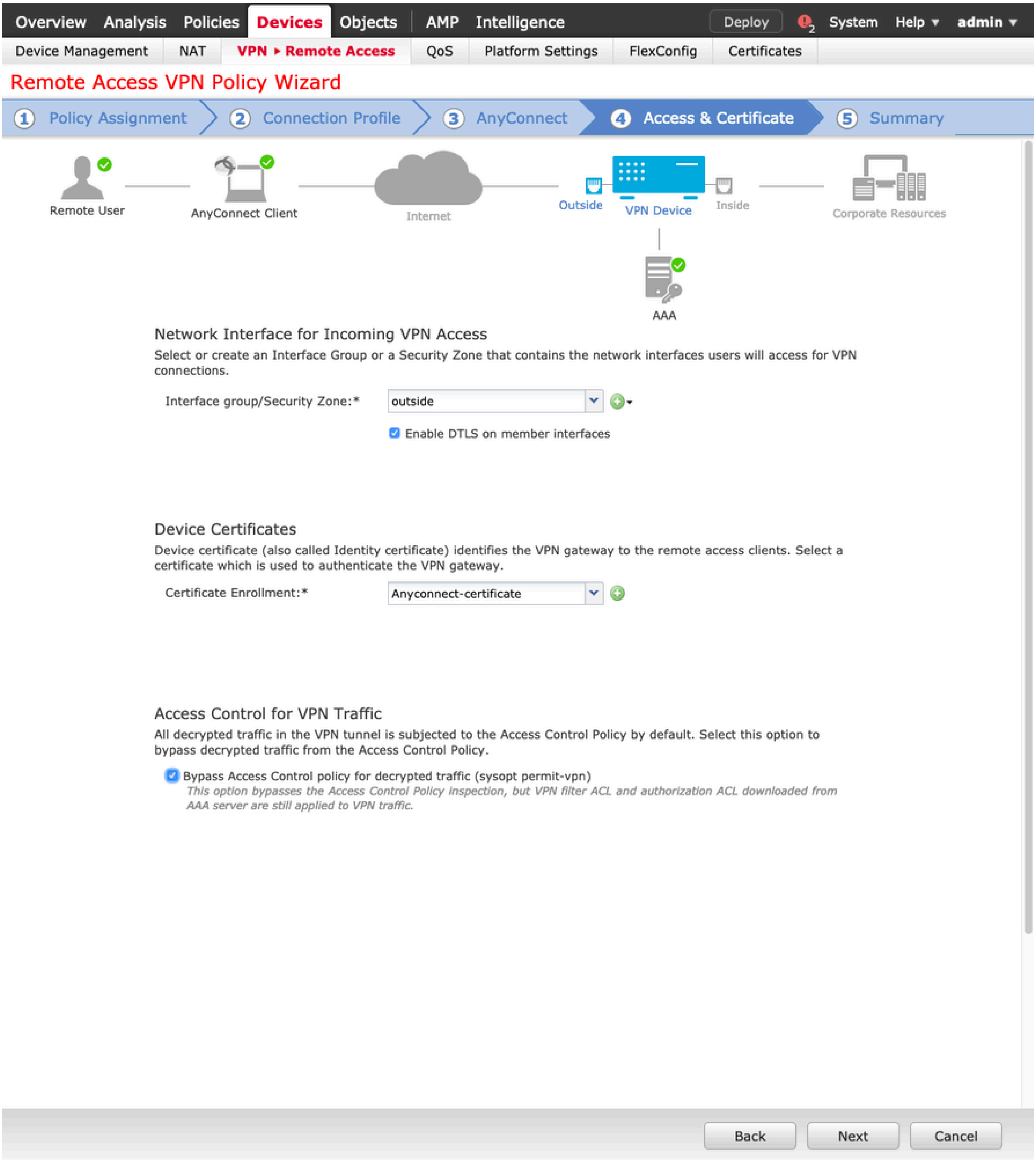
Download AnyConnect Client packages from Cisco Software Download Center.

☑	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
☑	MAC4.7	anyconnect-macos-4.7.04056-webdeploy-k9....	Mac OS

9. Select the **Security Zone** and **DeviceCertificates**:

- This configuration defines the interface on which the VPN terminates and the certificate that is presented upon an SSL connection.

Note: In this scenario, the FTD is configured to not inspect any VPN traffic, bypass the Access Control Policies (ACP) option is toggled.



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:* 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:* Anyconnect-certificate

Access Control for VPN Traffic

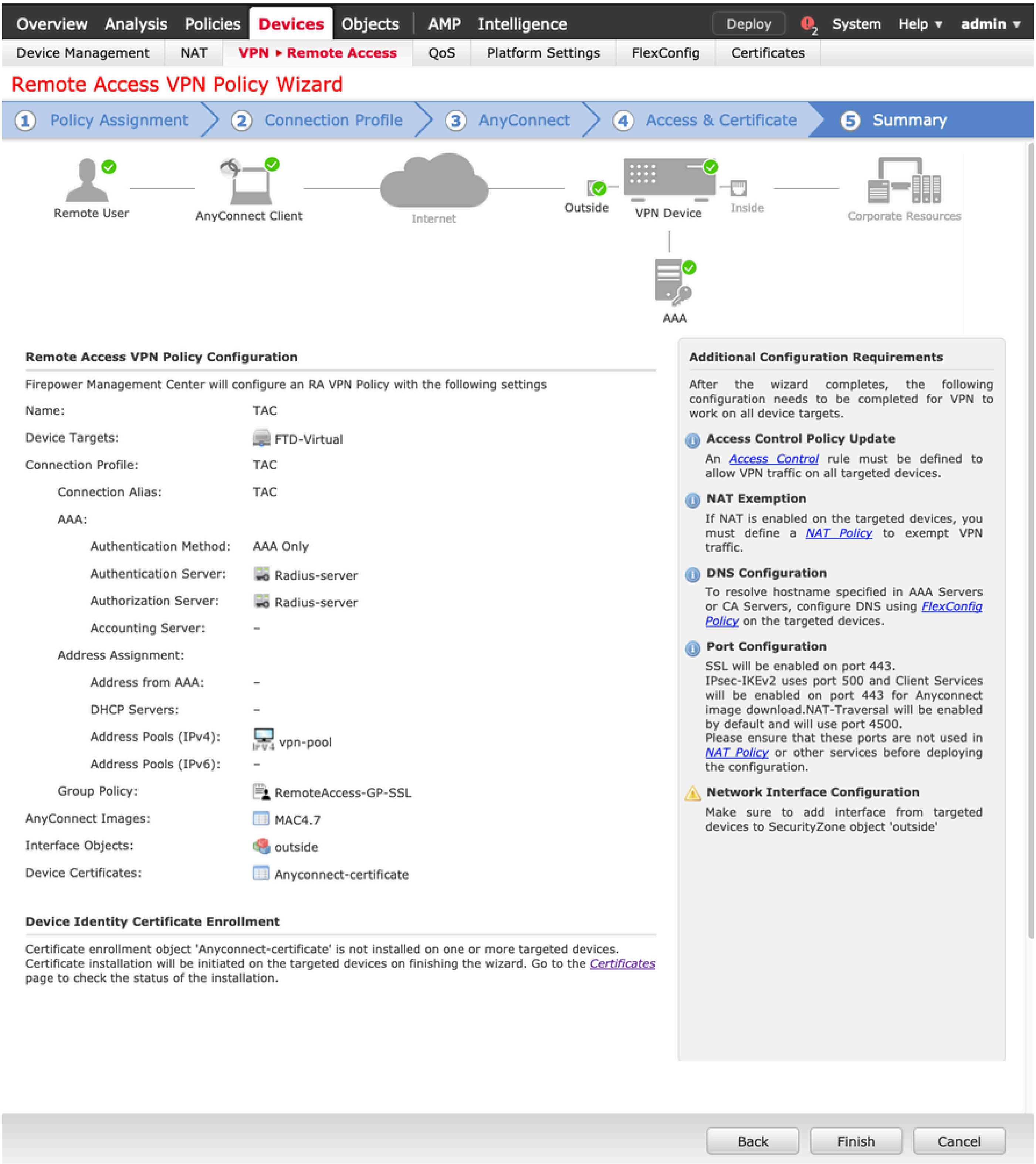
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

☑ 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.

10. Select **Finish** and **Deploy** the changes:

- All the configurations related to VPN, SSL certificates and AnyConnect packages are pushed via FMC Deploy as shown in the image.



Remote Access VPN Policy Wizard

Remote Access VPN Policy Configuration

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

Name:	TAC
Device Targets:	FTD-Virtual
Connection Profile:	TAC
Connection Alias:	TAC
AAA:	
Authentication Method:	AAA Only
Authentication Server:	Radius-server
Authorization Server:	Radius-server
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn-pool
Address Pools (IPv6):	-
Group Policy:	RemoteAccess-GP-SSL
AnyConnect Images:	MAC4.7
Interface Objects:	outside
Device Certificates:	Anyconnect-certificate

Device Identity Certificate Enrollment

Certificate enrollment object 'Anyconnect-certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the Certificates page to check the status of the installation.

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.
IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download.NAT-Traversal will be enabled by default and will use port 4500.
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 'outside'

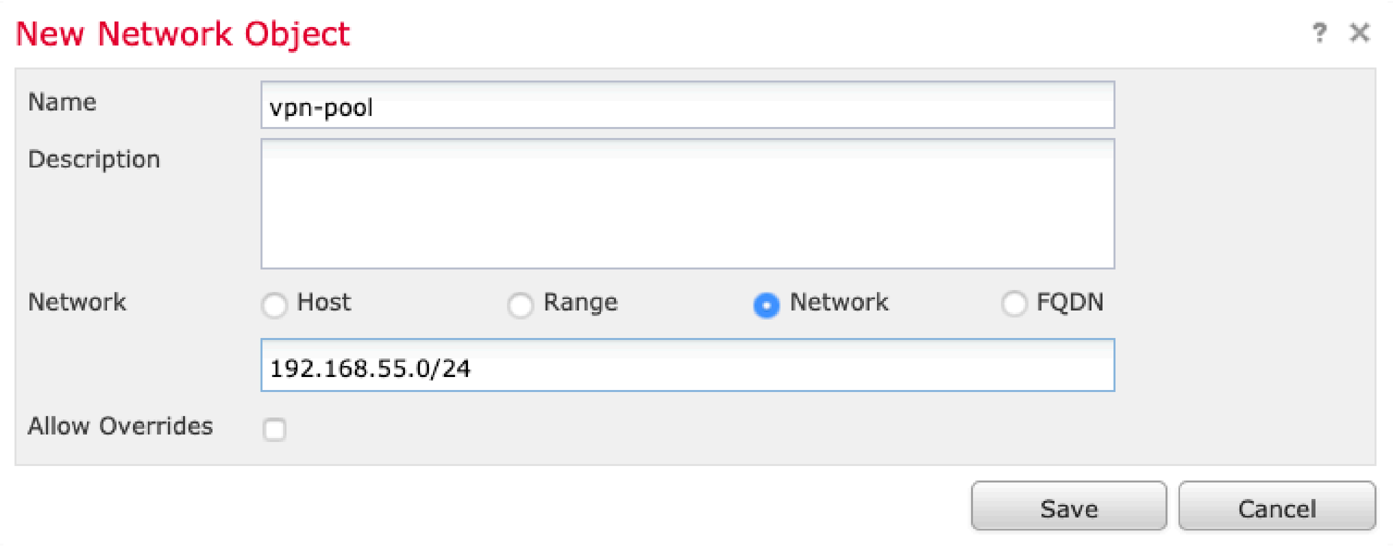
NAT Exemption and Hairpin

Step 1. NAT Exemption Configuration

The NAT exemption is a preferred translation method used to prevent traffic to be routed to the internet when it is intended to flow over a VPN tunnel (Remote Access or Site-to-Site).

This is needed when the traffic from your internal network is intended to flow over the tunnels without any translation.

1. Navigate to **Objects** > **Network** > **Add Network** > **Add Object** as shown in the image.



New Network Object

Name: vpn-pool

Description:

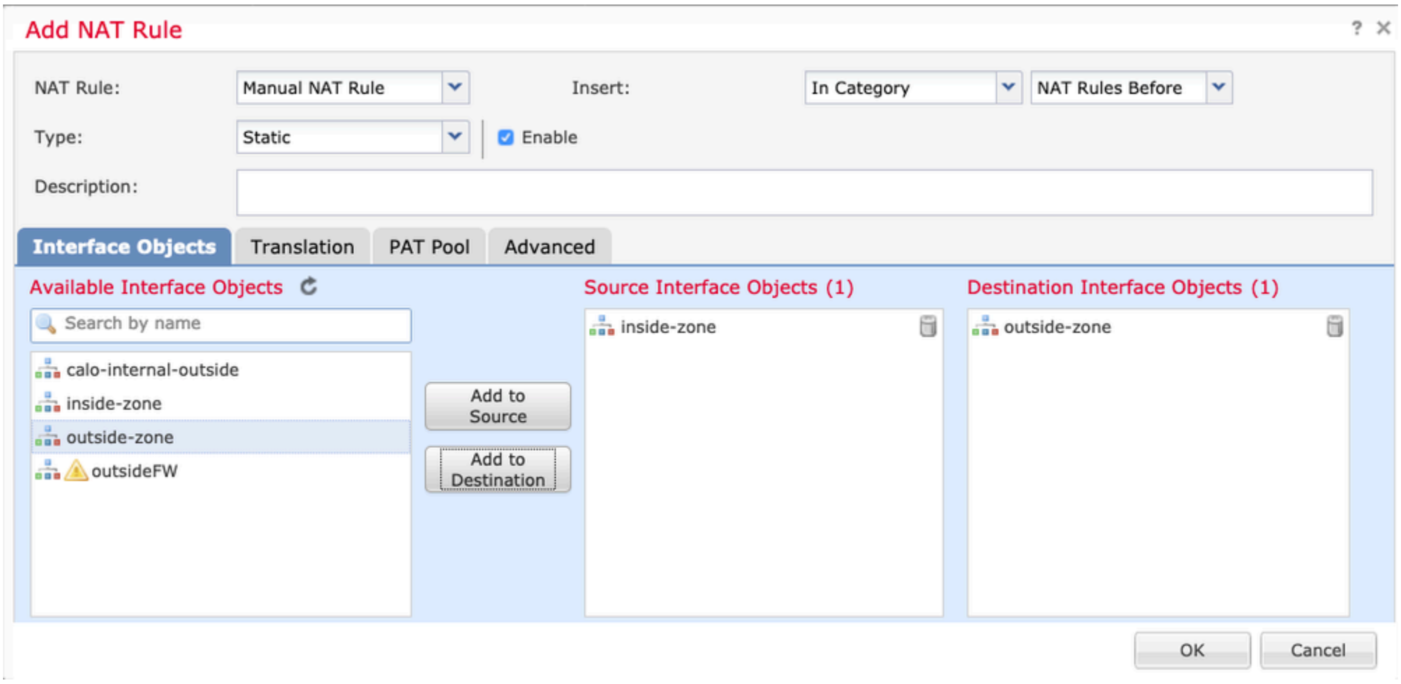
Network: ○ Host ○ Range ● Network ○ FQDN

192.168.55.0/24

Allow Overrides □

2. Navigate to **Device** > **NAT**, select the **NAT policy** that is used by the device in question, and create a **new statement.**

Note: The traffic flow goes from inside to outside.



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category; NAT Rules Before

Type: Static

☑ Enable

Description:

Interface Objects | Translation | PAT Pool | Advanced

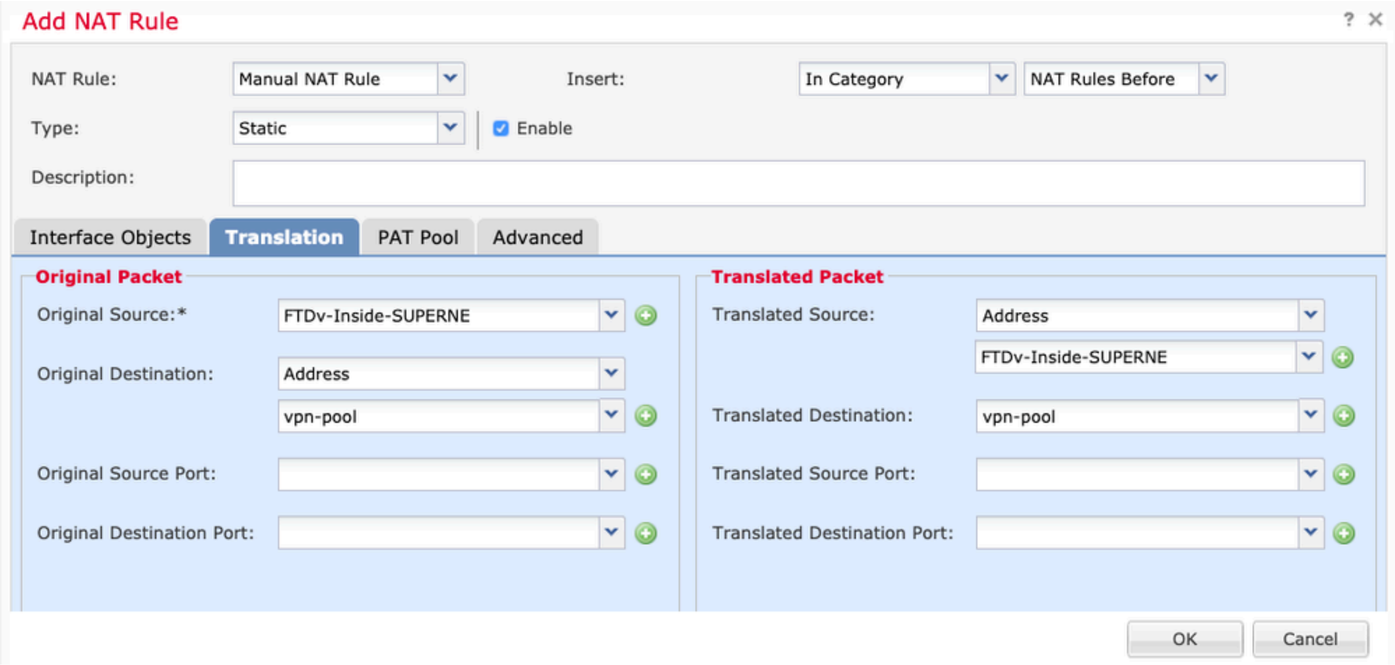
Available Interface Objects

- calo-internal-outside
- inside-zone
- outside-zone
- outsideFW

Source Interface Objects (1): inside-zone

Destination Interface Objects (1): outside-zone

3. Select the **internal resources** behind the FTD (**original source** and **translated source**) and the destination as the ip local pool for the AnyConnect users (**Original destination** and **translated destination**) as shown in the image.



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category — NAT Rules Before

Type: Static

☑ Enable

Description:

Original Packet

Original Source:* FTDv-Inside-SUPERNE

Original Destination: Address — vpn-pool

Original Source Port:

Original Destination Port:

Translated Packet

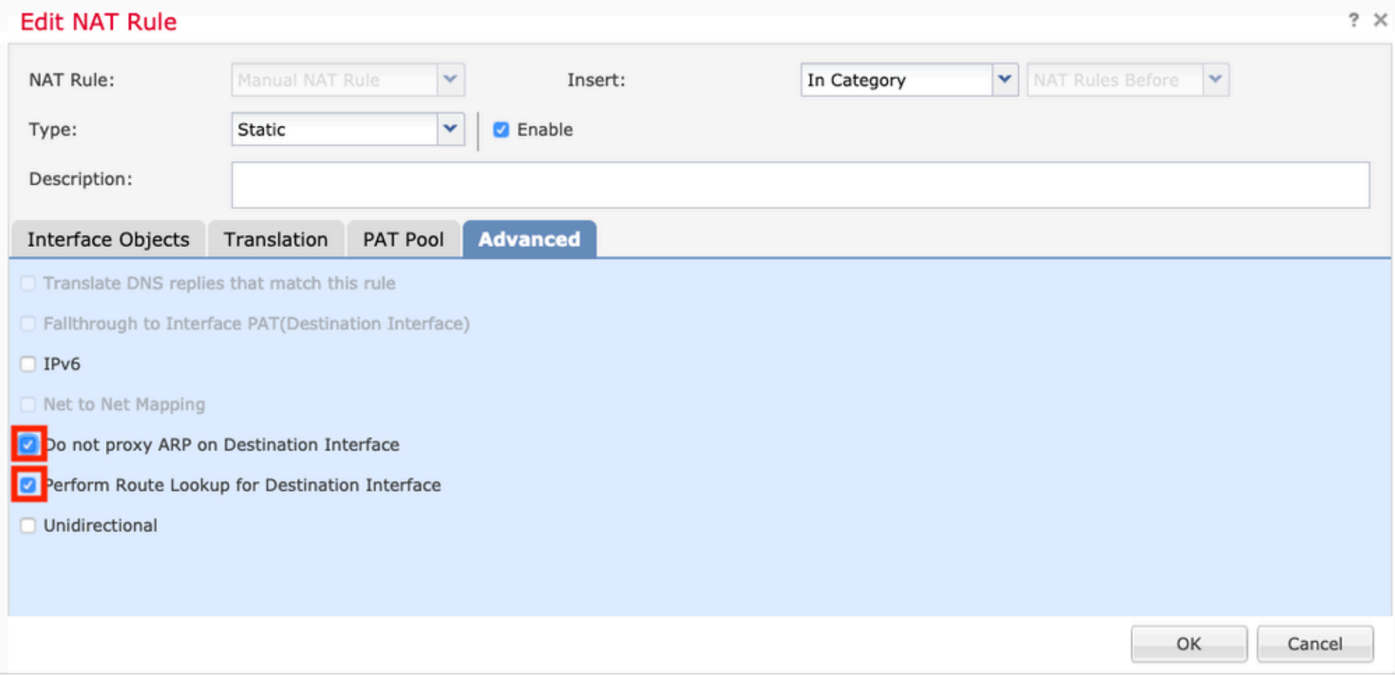
Translated Source: Address — FTDv-Inside-SUPERNE

Translated Destination: vpn-pool

Translated Source Port:

Translated Destination Port:

4. Ensure you toggle the options (as shown in the image), in order to enable **no-proxy-arp** and **route-lookup** in the NAT rule. Select **OK** as shown in the image.



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

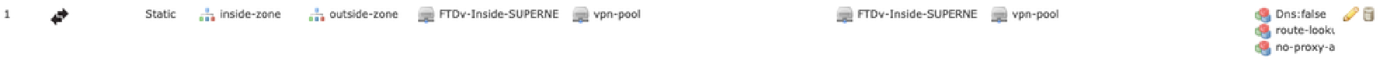
□ Net to Net Mapping

☑ Do not proxy ARP on Destination Interface

☑ Perform Route Lookup for Destination Interface

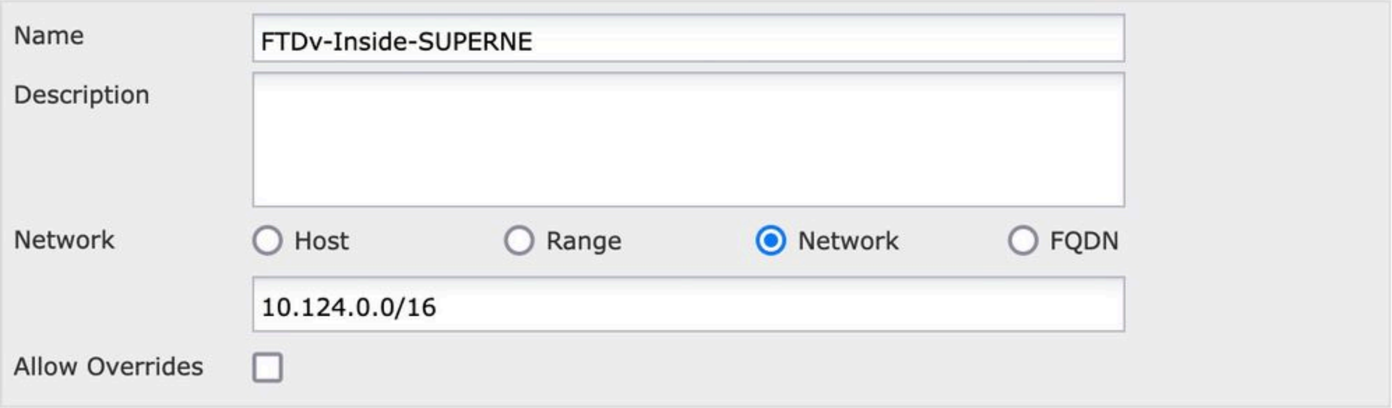
□ Unidirectional

5. This is the result of the NAT exemption configuration.



1 Static inside-zone outside-zone FTDv-Inside-SUPERNE vpn-pool FTDv-Inside-SUPERNE vpn-pool Dns:false route-looku no-proxy-a

The objects used in the previous section are the ones described below.



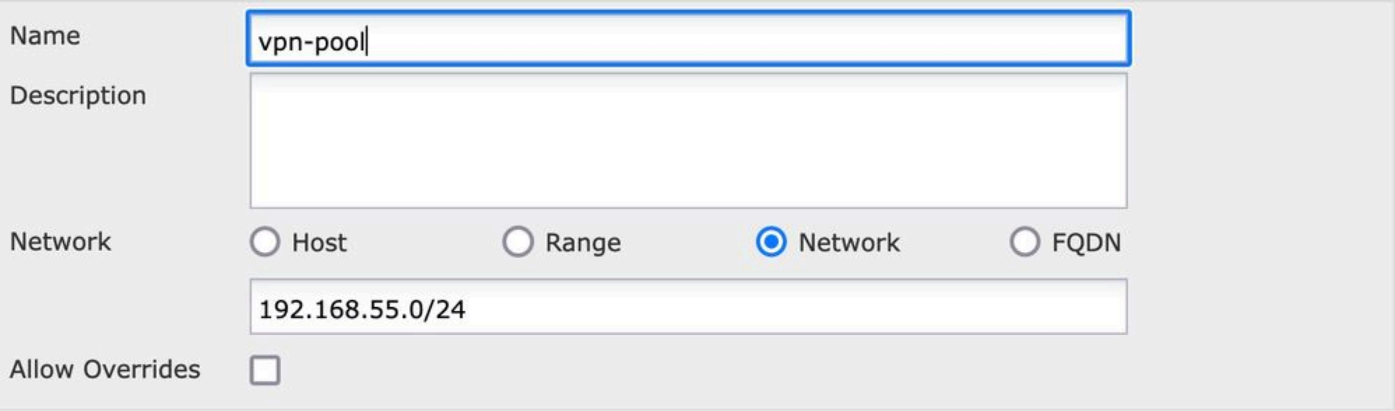
Name: FTDv-Inside-SUPERNE

Description:

Network: ○ Host ○ Range ● Network ○ FQDN

10.124.0.0/16

Allow Overrides □



Name: vpn-pool

Description:

Network: ○ Host ○ Range ● Network ○ FQDN

192.168.55.0/24

Allow Overrides □

Step 2. Hairpin Configuration

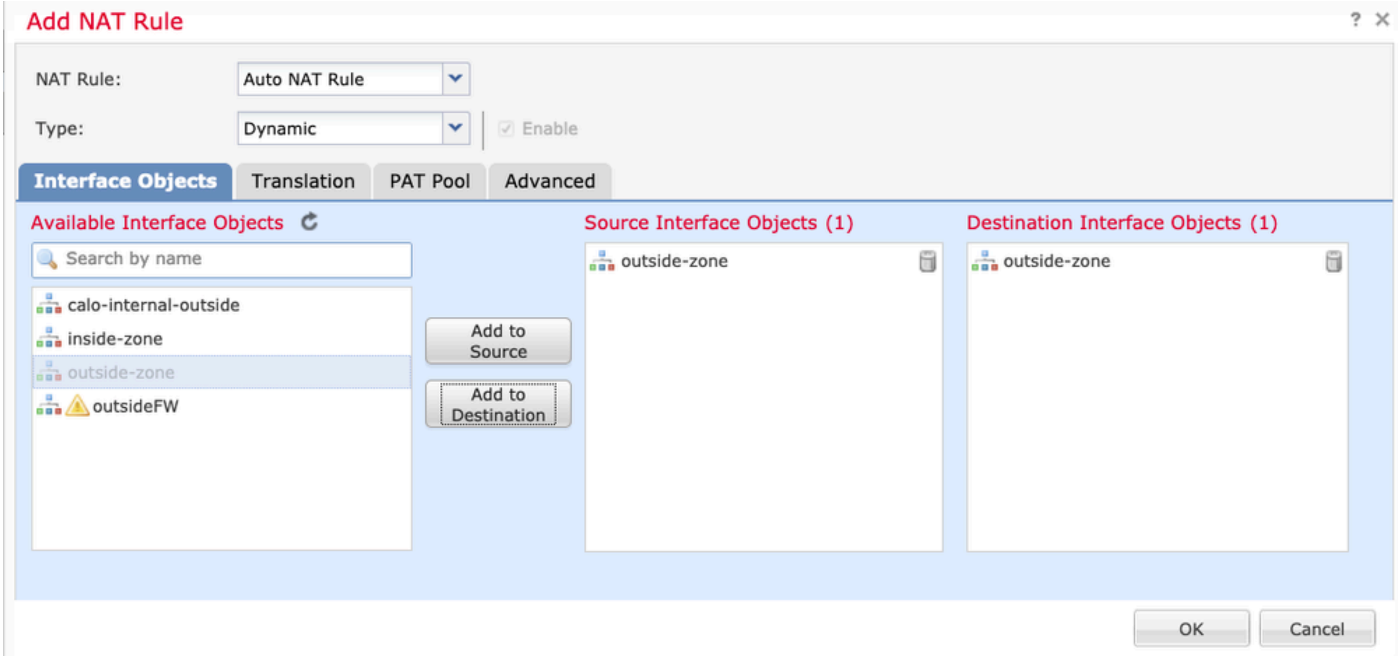
Also known as U-turn, this is a translation method that allows the traffic to flow over the same interface the traffic is received on.

For example, when AnyConnect is configured with a Full tunnel split-tunnel policy, the internal resources are accessed as per the NAT Exemption policy. If the AnyConnect client traffic is intended to reach an external site on internet, the hairpin NAT (or U-turn) is responsible to route the traffic from outside to outside.

A VPN pool object must be created before the NAT configuration.

1. Create a new **NAT statement**, select **Auto NAT Rule** in the **NAT Rule** field and select **Dynamic** as the **NAT** Type.

2. Select the same interface for the **source** and **destination** interface objects (outside):



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Available Interface Objects

- calo-internal-outside
- inside-zone
- outside-zone
- outsideFW

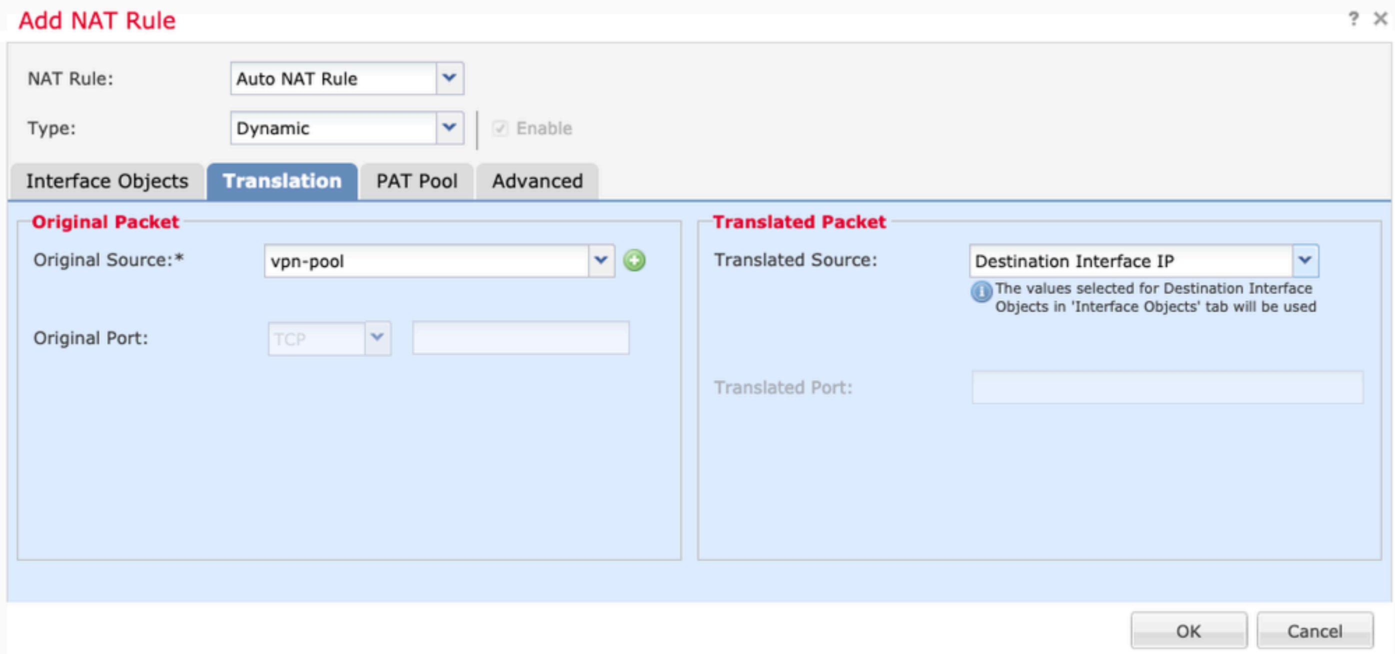
Source Interface Objects (1)

- outside-zone

Destination Interface Objects (1)

- outside-zone

3. In the **Translation** tab, select the **Original Source**, the **vpn-pool object**, and select **Destination Interface IP** as the **Translated Source**. Select **OK** as shown in the image.



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Original Packet

Original Source:* vpn-pool

Original Port: TCP

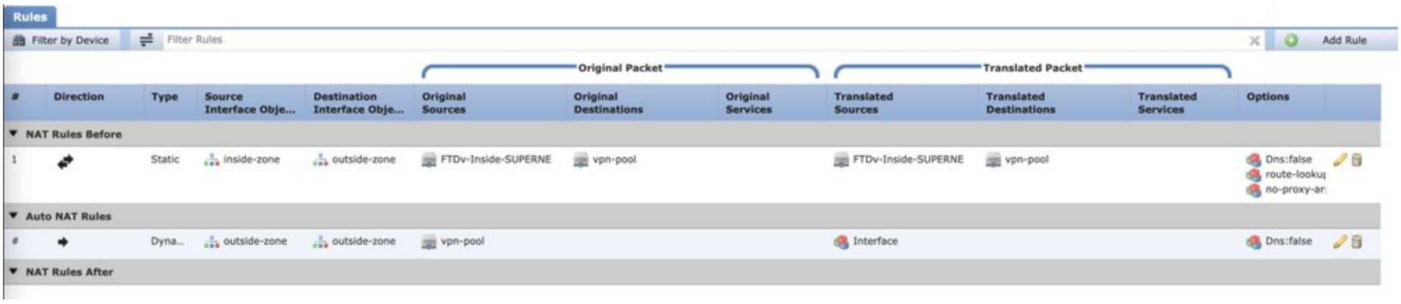
Translated Packet

Translated Source: Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

4. This is the summary of the NAT configuration as shown in the image.



					Original Packet			Translated Packet			
#	Direction	Type	Source Interface Obje...	Destination Interface Obje...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
1	⇄	Static	inside-zone	outside-zone	FTDv-Inside-SUPERNE	vpn-pool		FTDv-Inside-SUPERNE	vpn-pool		Dns:false route-looku no-proxy-ar
▼ Auto NAT Rules											
#	→	Dyna...	outside-zone	outside-zone	vpn-pool			Interface			Dns:false
▼ NAT Rules After											

5. Click **Save** and **Deploy** the changes.

Verify

Use this section to confirm that your configuration works properly.

Run these commands in the FTD command line.

- **sh crypto ca certificates**
- **show running-config ip local pool**
- **show running-config webvpn**
- **show running-config tunnel-group**
- **show running-config group-policy**
- **show running-config ssl**
- **show running-config nat**

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.