

Configure AnyConnect VPN Client on FTD: Hairpin and NAT Exemption

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Step 1. Import an SSL Certificate](#)

[Step 2. Configure a RADIUS Server](#)

[Step 3. Create an IP Pool](#)

[Step 4. Create an XML Profile](#)

[Step 5. Upload Anyconnect XML Profile](#)

[Step 6. Upload AnyConnect Images](#)

[Step 7. Remote Access VPN Wizard](#)

[NAT Exemption and Hairpin](#)

[Step 1. NAT Exemption Configuration](#)

[Step 2. Hairpin Configuration](#)

[Verify](#)

[Troubleshoot](#)

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 version 2 (IKEv2) 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

This document describes the procedure to configure Cisco remote access VPN solution (AnyConnect) on Firepower Threat Defense (FTD), version 6.3, managed by Firepower Management Center (FMC).

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 seek the ASA configuration example, please refer to the document: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

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](#)).

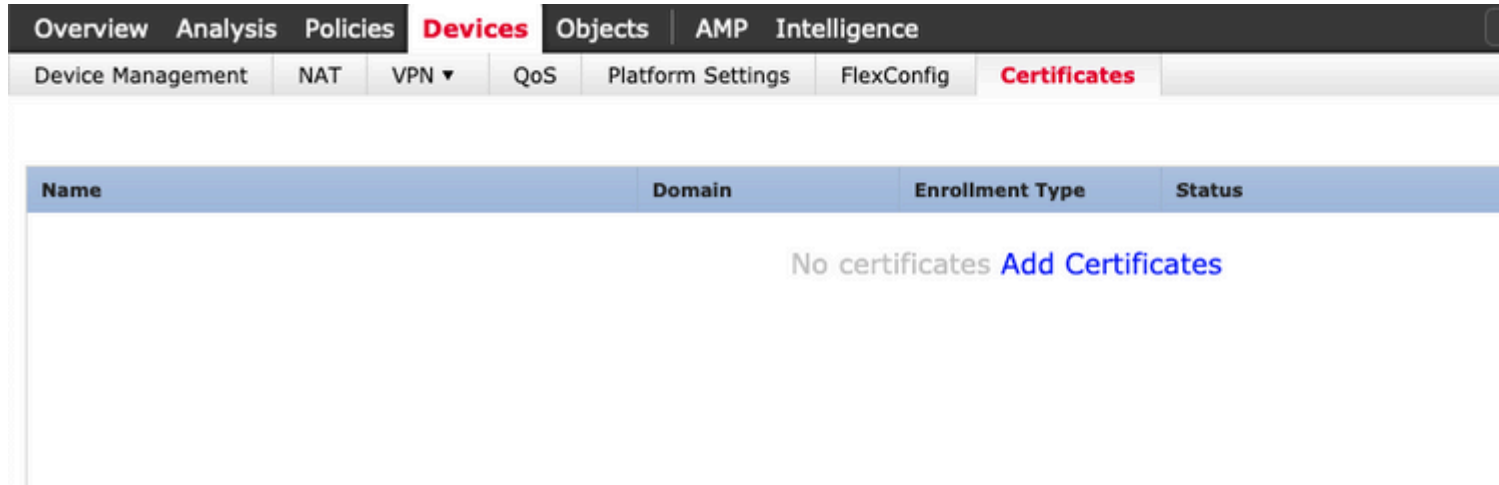
Additionally, the certificate must contain a Common Name (CN) extension with DNS name and/or IP address in order to avoid "Untrusted server certificate" errors in web browsers.

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.

Overview Analysis Policies **Devices** Objects AMP Intelligence

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

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

Add New Certificate

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

Device*:

Cert Enrollment*:

Add Cert Enrollment

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

Enrollment URL:*

Challenge Password:

Confirm Password:

Retry Period: Minutes (Range 1-60)

Retry Count: (Range 0-100)

Fingerprint:

Allow Overrides

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

Add Cert Enrollment

? X

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate: *

```
/3C4h07uzuRDyggwKEBaMdg4DI/z
4x3nk3tTUhyppmbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogkzou6
RqV66G9IE7Z2
xiVrSrJFqhrT795kMb8amBxhb4eXYXUjJmODTPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/IJG2LgRDrA0Kt+jwb57DGSK4mfZsZqhFdQP
LhBNFbyBVb9
dOjUkmd5vzQDR5qSo+HINEm3E8/q20wrtIzP4MpAabyhr+hEpeP
VMYhIVBOT8h
H8eMJSQjGhhHkuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDv
mwNgy5mTP9chla
9Or3RIWRzEa11HE3mHO4Rj6DOngufjx+TZRYczownSKLL7LcW1
D8ZcLYmfaIdC
W2CZuBR0yVDxQv4#04ISEIBFOWFSd5rAD/bvk2n6xrJI1SLqABMJ
uslu9KTGH1
bIVKEYACKVYETw==
-----END CERTIFICATE-----
```

Allow Overrides

Save Cancel

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

Add Cert Enrollment

? X

Name*

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

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 ? x

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

Add Cancel

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

Overview Analysis Policies **Devices** Objects AMP Intelligence

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

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

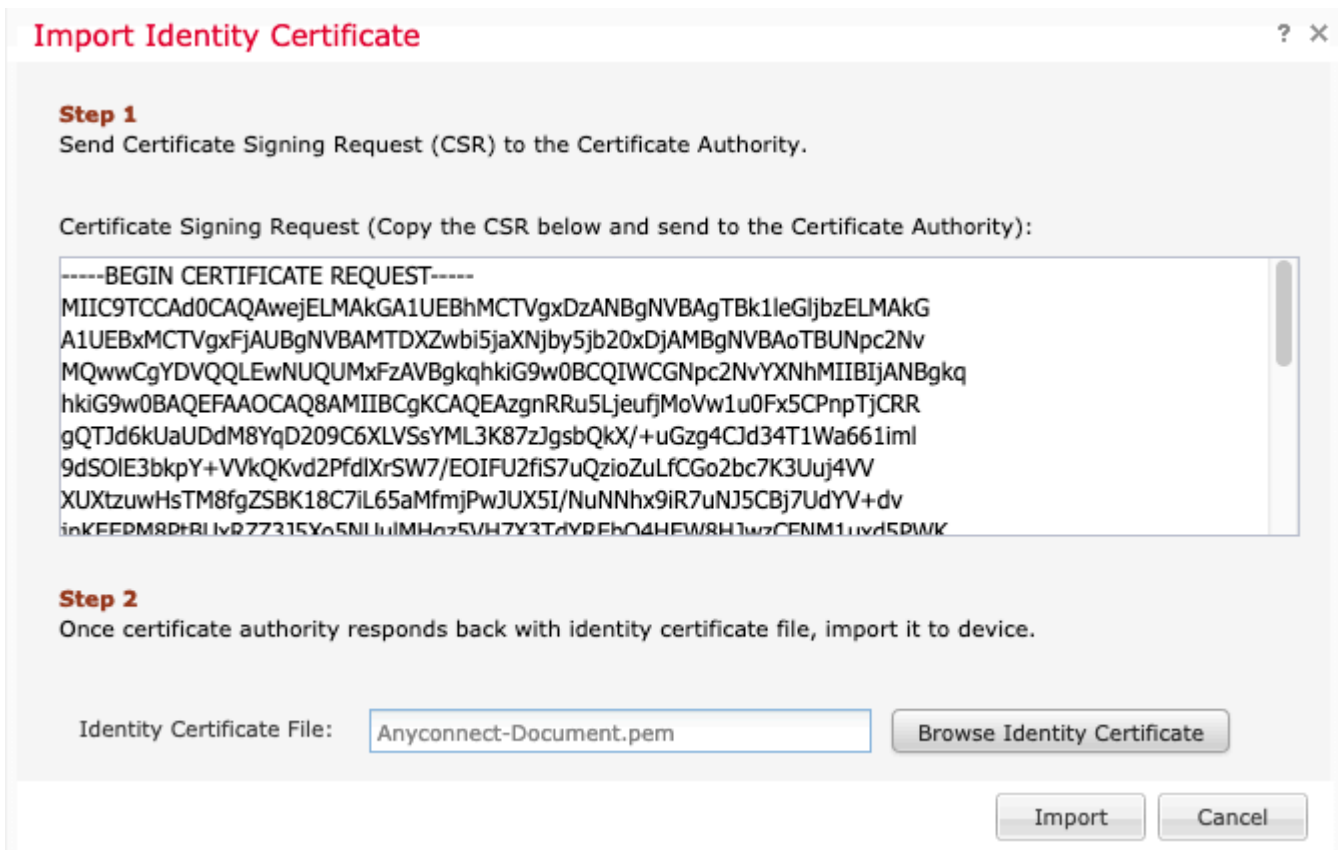
Warning

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

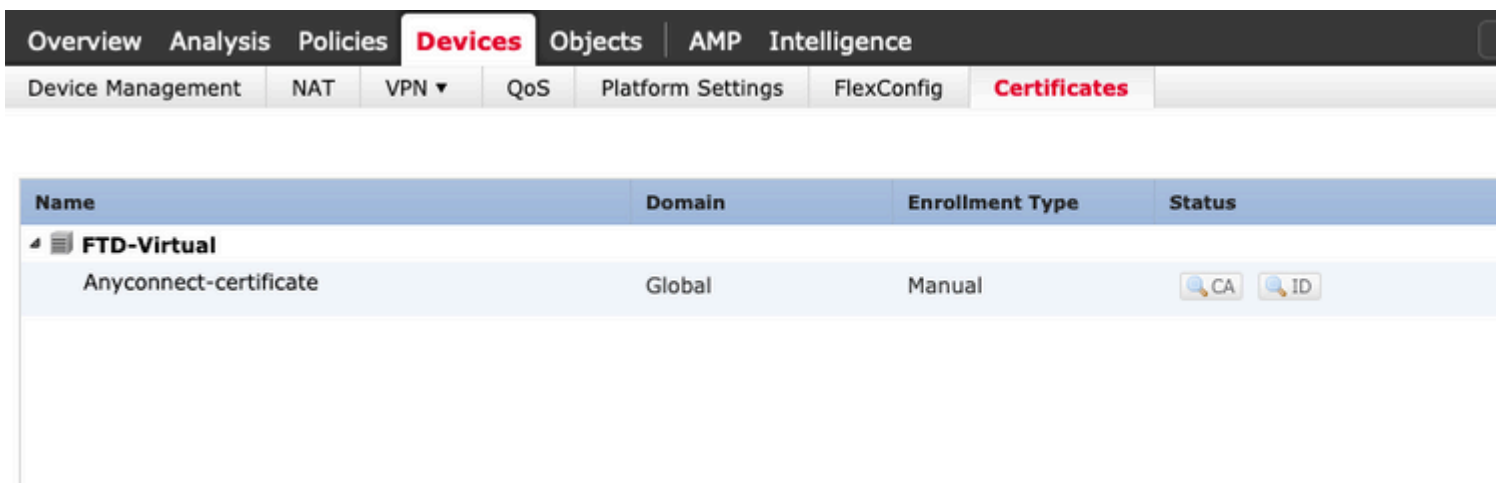
Yes No

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**.



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



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:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼


Enable authorize only

Enable interim account update

Interval:* (1-120) hours

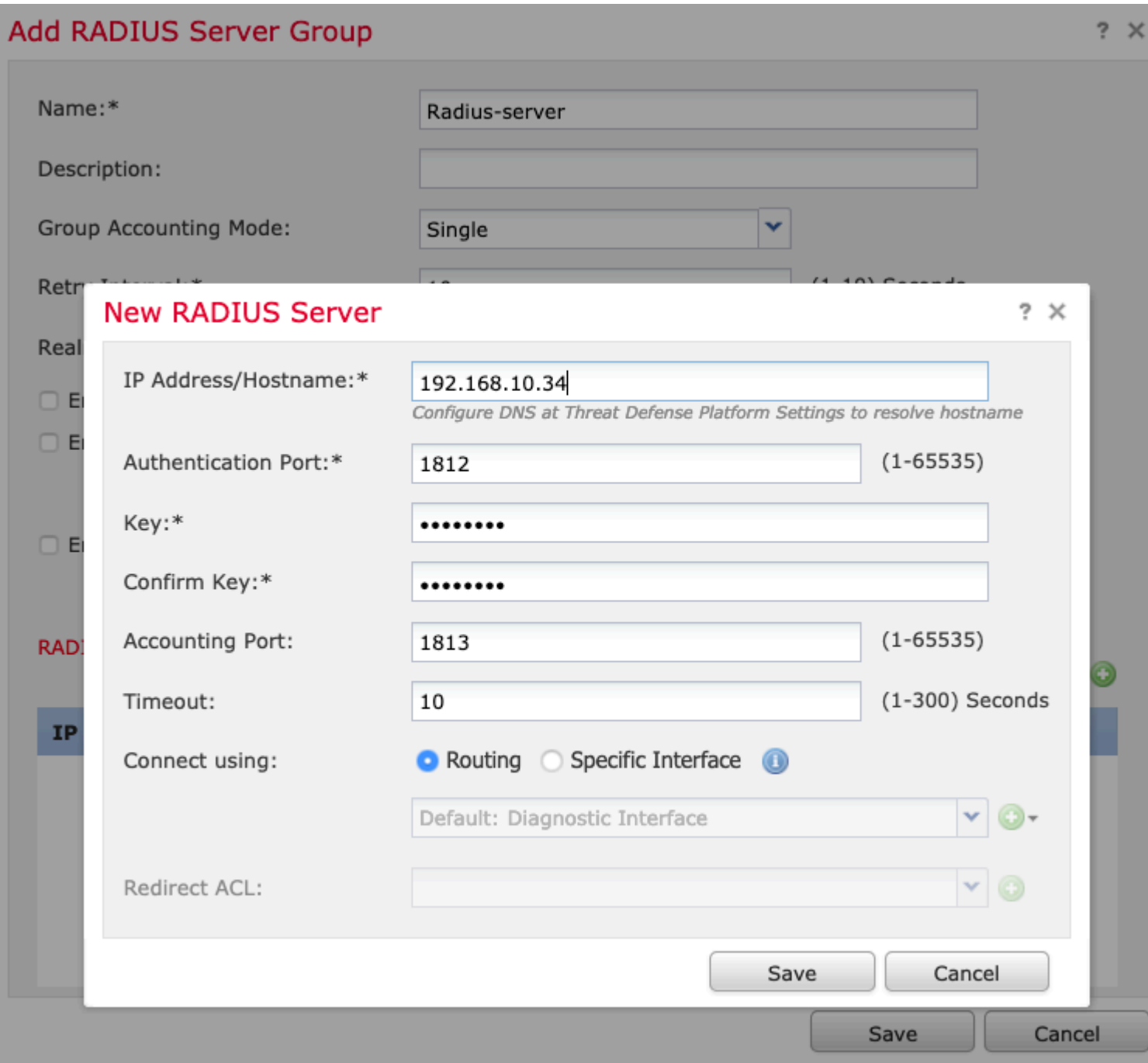
Enable dynamic authorization

Port:* (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.



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

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

192.168.10.34



Save

Cancel

Step 3. Create an IP Pool

1. Navigate to **Objects > Object Management > Address Pools > Add IPv4 Pools**.
2. Assign the name and range of IP addresses, **Mask** field is not required but it can be specified as shown in the image.

Add IPv4 Pool

Name*

IPv4 Address Range*
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

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.

The screenshot shows the Profile Editor application interface. On the left is a navigation pane with a tree view under 'VPN' containing: Preferences (Part 1), Preferences (Part 2), Backup Servers, Certificate Pinning, Certificate Matching, Certificate Enrollment, Mobile Policy, and Server List (which is highlighted). The main area is titled 'Server List' and contains a table with the following columns: Hostname, Host Address, User Group, Backup Server List, and SCEP. The table is currently empty. Below the table, a note states: '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.

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required)

FQDN or IP Address / User Group

Group URL

Connection Information

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

Backup Servers

Host Address

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

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Profile: Untitled

Hostname	Host Address	User Group	Backup Server ...	SCEP	Mobil
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 a **.xml** 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 ? X

Name:*

File Name:*

File Type:* ▼

Description:

Note: Additional packages can be uploaded, based on your requirements (Windows, Mac, 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**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 **Connection Profile** 3 AnyConnect 4 Access & Certificate 5 Summary

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

Search

FTD-Virtual

Add

Selected Devices

FTD-Virtual

Before You Start

Before you start, configuration elements must be complete Remote Access VPN.

Authentication Server

Configure [Realm](#) or to authenticate VPN.

AnyConnect Client

Make sure you have for VPN Client download the relevant Cisco client during the wizard.

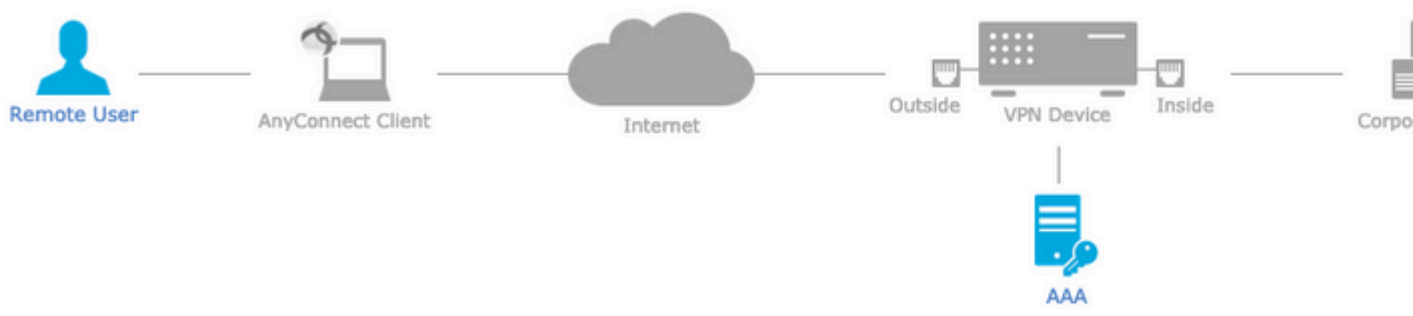
Device Interface

Interfaces should be targeted [devices](#) so as a security zone 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

1 Policy Assignment 2 **Connection Profile** 3 AnyConnect 4 Access & Certificate 5



Connection Profile:

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

Connection Profile Name:*

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: ▼
 Authentication Server:* ▼ + (Realm or RADIUS)
 Authorization 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: ✎
 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. or create a Group Policy object.

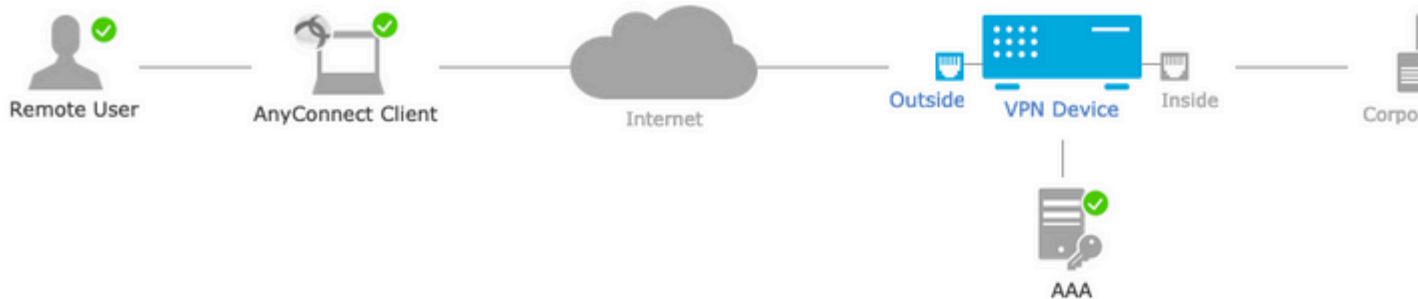
Group Policy:* ▼ +
[Edit Group Policy](#)

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

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

Remote Access VPN Policy Wizard

1 Policy Assignment > 2 Connection Profile > 3 AnyConnect > **4 Access & Certificate** > 5



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:* +

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:* +

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.

Back

Next

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

All the configuration related to VPN, SSL certificates and AnyConnect packages is pushed via FMC

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

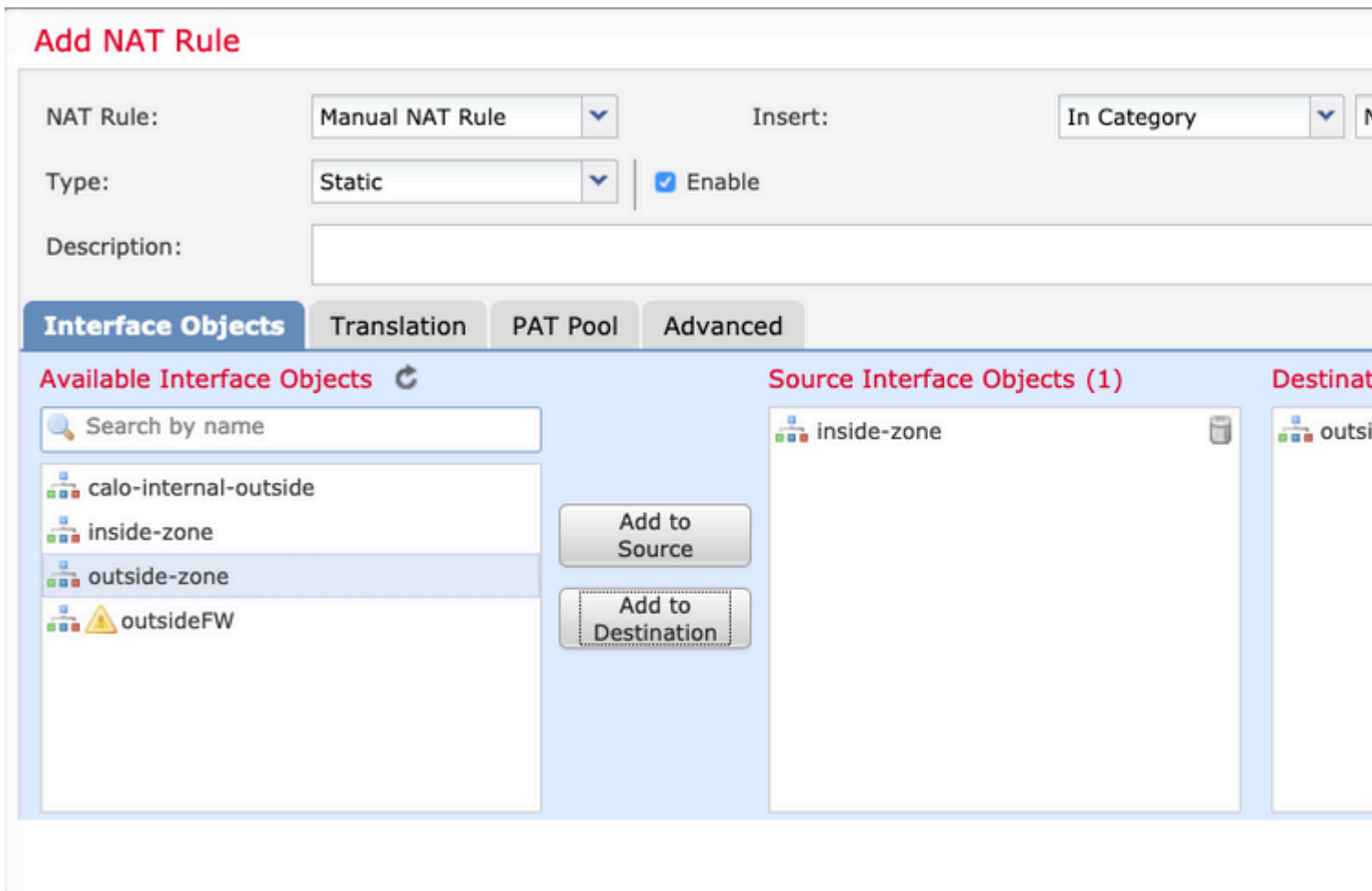
192.168.55.0/24

Allow Overrides:

Save Cancel

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.



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

Type:

Static

Enable

Description:

Interface Objects

Translation

PAT Pool

Advanced

Original Packet

Original Source:*

FTDv-Inside-SUPERNE

Original Destination:

Address

vpn-pool

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source:

Translated Destination:

Translated Source Port:

Translated Destination Port:

4. Ensure to 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: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

- 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

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

Name

Description

Network Host Range Network

Allow Overrides

Name	<input type="text" value="vpn-pool"/>
Description	<input type="text"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input checked="" type="radio"/> Network <input type="radio"/>
	<input type="text" value="192.168.55.0/24"/>
Allow Overrides	<input type="checkbox"/>

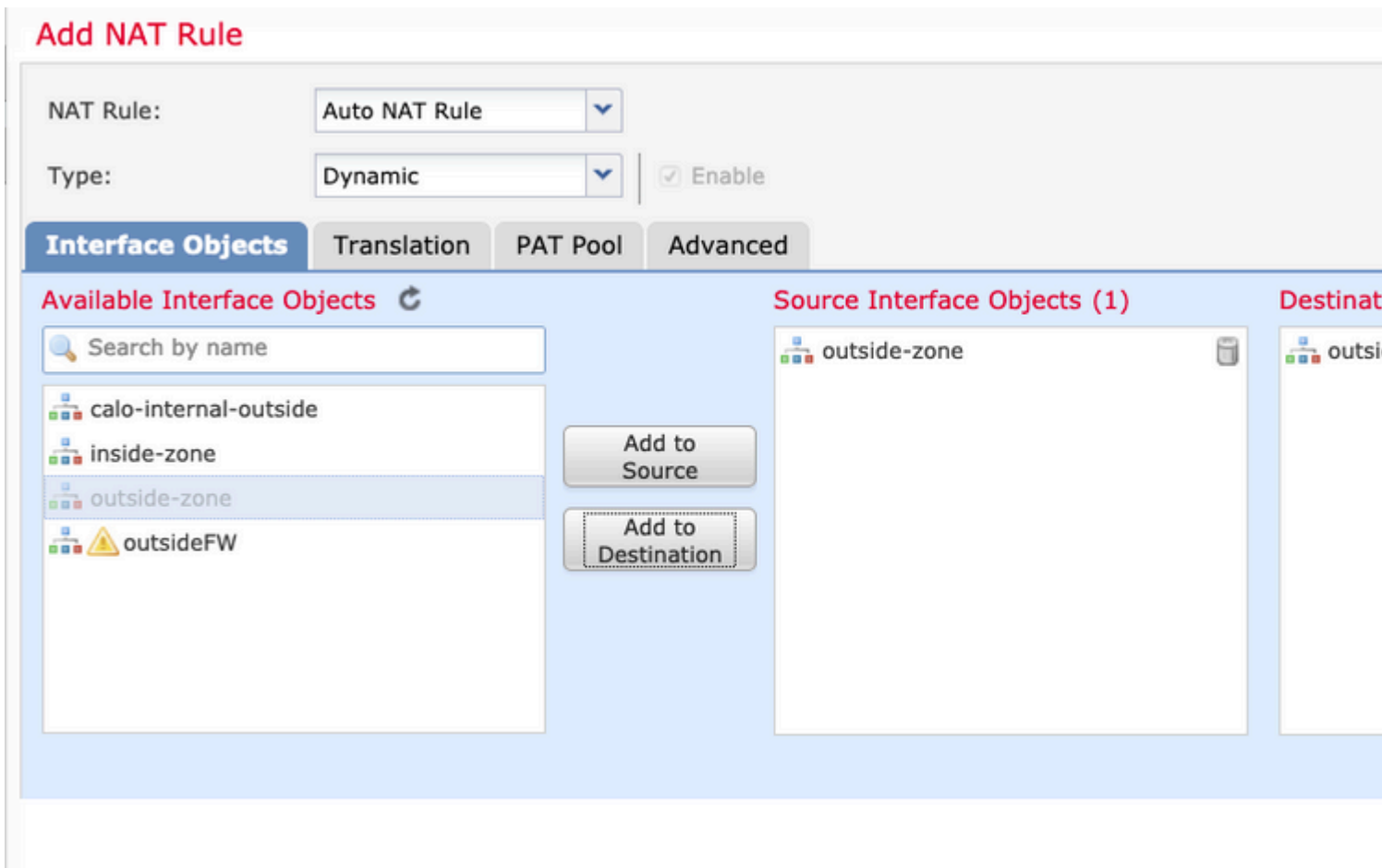
Step 2. Hairpin Configuration

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):



3. In the **Translation** tab, select as 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: ▼

Type: ▼ Enable

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* ▼ +

Original Port: ▼

Translated Packet

Translated Source: ▼ i The va Object

Translated Port:

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

Rules									
Filter by Device Filter Rules									
#	Direction	Type	Source Interface Obje...	Destination Interface Obje...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destination
▼ NAT Rules Before									
1	↔	Static	inside-zone	outside-zone	FTDv-Inside-SUPERNE	vpn-pool		FTDv-Inside-SUPERNE	vpn-pool
▼ Auto NAT Rules									
#	→	Dyna...	outside-zone	outside-zone	vpn-pool			Interface	
▼ 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.</>