

Configure AnyConnect Remote Access VPN on FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configuration](#)

[1. Prerequisites](#)

[a\) Import the SSL Certificate](#)

[b\) Configure RADIUS Server](#)

[c\) Create a Pool of Addresses for VPN Users](#)

[d\) Create XML Profile](#)

[e\) Upload AnyConnect Images](#)

[2. Remote Access Wizard](#)

[Connection](#)

[Limitations](#)

[Security considerations](#)

[a\) Enable uRPF](#)

[b\) Enable sysopt connection permit-vpnOption](#)

[Related Information](#)

Introduction

This document describes a configuration for AnyConnect Remote Access VPN on FTD.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic VPN, TLS and IKEv2 knowledge
- Basic Authentication, Authorization, and Accounting (AAA) and RADIUS knowledge
- Experience with Firepower Management Center

Components Used

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

- Cisco FTD 7.2.0
- Cisco FMC 7.2.1
- AnyConnect 4.10

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 provides a configuration example for Firepower Threat Defense (FTD) version 7.2.0 and later, that allows remote access VPN to use Transport Layer Security (TLS) and Internet Key Exchange version 2 (IKEv2). As a client, Cisco AnyConnect can be used, which is supported on multiple platforms.

Configuration

1. Prerequisites

In order to go through Remote Access wizard in Firepower Management Center:

- Create a certificate used for server authentication.
- Configure RADIUS or LDAP server for user authentication.
- Create pool of addresses for VPN users.
- Upload AnyConnect images for different platforms.

a) Import the SSL Certificate

Certificates are essential when you configure AnyConnect. The certificate must have Subject Alternative Name extension with DNS name and/or IP address to avoid errors in web browsers.



Note: Only registered Cisco users have access to internal tools and bug information.

There are limitations for manual certificate enrollment:

- On FTD you need the CA certificate before you generate the CSR.
- If the CSR is generated externally, the manual method fails, a different method must be used (PKCS12).

There are several methods to obtain a certificate on FTD appliance, but the safe and easy one is to create a Certificate Signing Request (CSR), sign it with a Certificate Authority (CA) and then import certificate issued for public key, which was in CSR. Here is how to do that:

- Go to Objects > Object Management > PKI > Cert Enrollment , click **Add Cert Enrollment**.

Add Cert Enrollment



Name*

vpntestbbed.cisco.com

Description

|

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
Ep0WYTGngteb6JFITIn..StZxr  
YfPCilB7g  
BMAV7Gzdc4VspS6lJrAhbiiaw  
dBiIQmsBeFz9JkF4..b3l8Bo  
GN+qMa56Y  
lt8una2gY4l2O//on88r5IWJlm  
1L0oA8e4fR2yrBHX..adsGeFK  
kyNrwGi/  
7vQMfXdGsRrXNGRGnX+vWD  
Z3/zWl0joDtCkNnqEpVn..HoX  
-----END CERTIFICATE-----
```

Validation Usage: IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Allow Overrides

Cancel

Save

- Select Enrollment Type and paste Certificate Authority (CA) certificate (the certificate which is used to sign the CSR).
- Then go to second tab and select Custom FQDN and fill all necessary fields, for example:

Add Cert Enrollment



Name*

vpntestbbed.cisco.com

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN:

Use Device Hostname as FQDN ▾

Include Device's IP Address:

Common Name (CN):

vpntestbed.cisco.com

Organization Unit (OU):

TAC

Organization (O):

Mexico

Locality (L):

MX

State (ST):

CDMX

Country Code (C):

MX

Email (E):

tac@cisco.com

Include Device's Serial Number

Allow Overrides

Cancel

Save

- On the third tab, select Key Type, choose name and size. For RSA, 2048 bits is minimum.
- Click save and go to Devices > Certificates > Add > New Certificate.
- Then select Device, and under Cert Enrollment select the trustpoint which you just created, click Add:

Add New Certificate



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

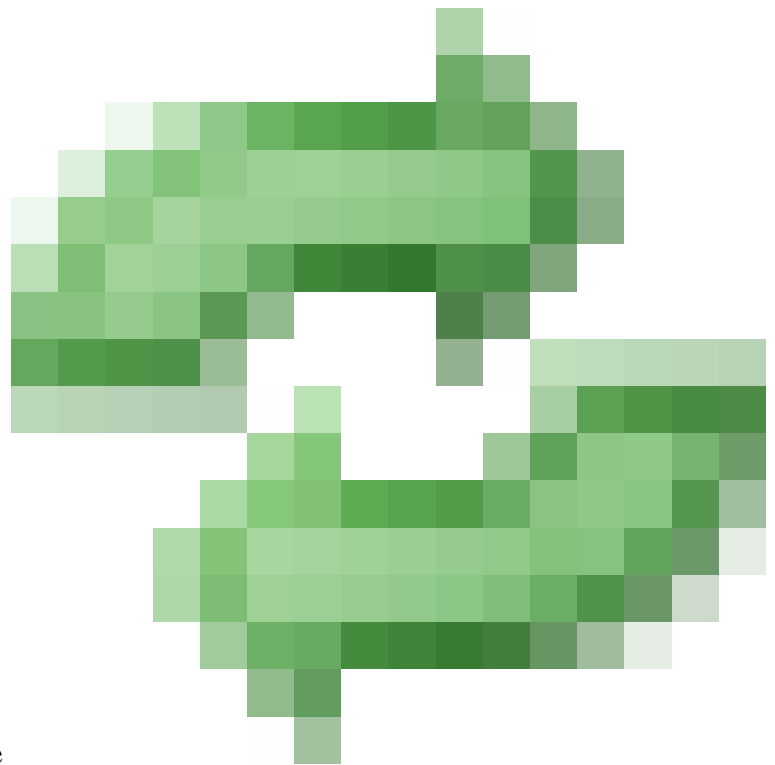
Device*:

Cert Enrollment*:

 +

Cert Enrollment Details:

Name: vpntestbed.cisco.com



- Later, next to the trustpoint name, click the icon, then Yes, and after that copy CSR to CA and sign it. Certificate must have attributes the same as normal a HTTPS server.
- After you received the certificate from CA in base64 format, select it from the disk and click Import. When this succeeds, you see:

| Name | Domain | Enrollment Type | Status | |
|----------------------|--------|-----------------|--------|-----------------------|
| FTD | | | | |
| vpntestbed.cisco.com | Global | Self-Signed | CA ID | Import Refresh Delete |

b) Configure RADIUS Server

- Go to Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group.

- Fill out the name and add IP address along with shared secret, click Save:

Edit RADIUS Server



IP Address/Hostname:*

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

Key:*

Confirm Key:*

Accounting Port: (1-65535)


Timeout: (1-300) Seconds

Connect using:

Routing Specific Interface 

Default: Management/Diagnostic  +



Redirect ACL:

  +

Cancel

Save

- After that you see the server on the list:

| Name | Value | |
|--------------|----------|---|
| RadiusServer | 1 Server |   |

c) Create a Pool of Addresses for VPN Users

- Go to **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- Put the name and range, mask is not needed:

Name*

vpn_pool

IPv4 Address Range*

10.72. -10.72.

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Specify a netmask in X.X.X.X format

Description

Allow Overrides

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

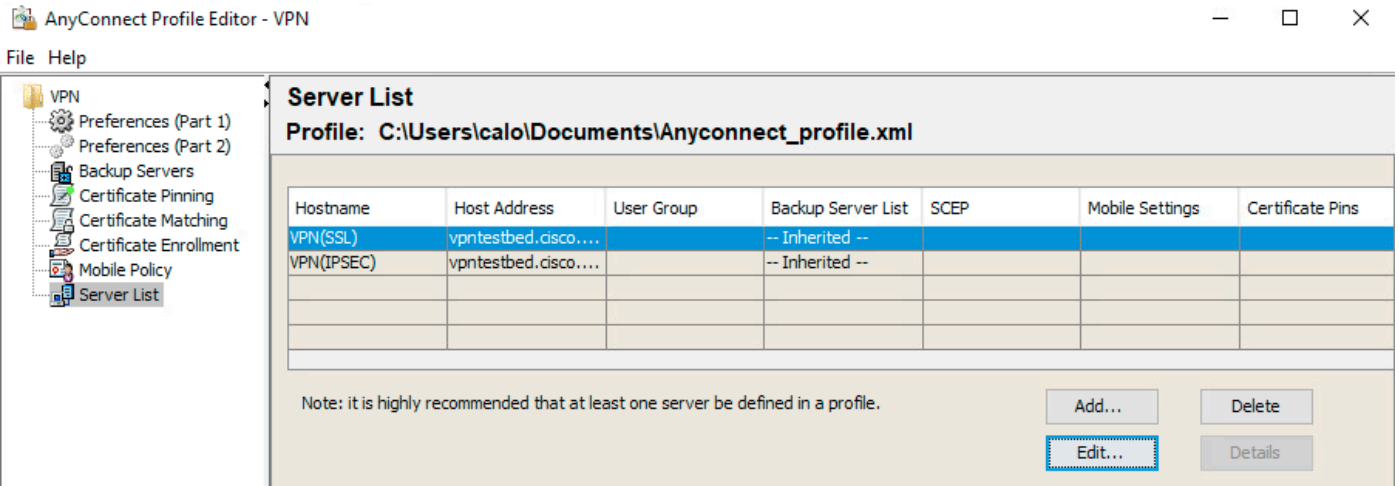
► Override (0)

Cancel

OK

d) Create XML Profile

- Download the Profile Editor from Cisco site and open it.
- Go to **Server List > Add...**
- Put Display Name and FQDN. You see entries in Server List:



- Click OK and **File > Save as...**

e) Upload AnyConnect Images

- Download pkg images from Cisco site.
- Go to **Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.**
- Type the name and select PKG file from disk, click **Save:**

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

- Add more packages based on your own requirements.

2. Remote Access Wizard

- Go to Devices > VPN > Remote Access > Add a new configuration.
- Name the profile and select FTD device:

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:*

Description:

VPN Protocols:

SSL

IPsec-IKEv2


Targeted Devices:

Available Devices

| |
|-----|
| FTD |
|-----|

Add

Selected Devices

| |
|---|
| FTD  |
|---|

- In Connection Profile step, type Connection Profile Name, select the **Authentication Server** and Address Pools that you created earlier:

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:*

i 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:* +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server: +

(Realm or 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 (Realm or RADIUS only) **i**

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. Select or create a Group Policy object.

Group Policy:* +

[Edit Group Policy](#)

- Click on **Edit Group Policy** and on the tab AnyConnect, select Client Profile, then click Save:

Name:*

DfltGrpPolicy

Description:

General **AnyConnect** Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

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

Client Profile:

Anyconnect_profile ▾ +

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](#).

- On the next page, select AnyConnect images and click Next.

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](#).

Show Re-order buttons +

| <input checked="" type="checkbox"/> | AnyConnect File Object Name | AnyConnect Client Package Name | Operating System |
|-------------------------------------|-----------------------------|--|------------------|
| <input checked="" type="checkbox"/> | Anyconnectmac4.10 | anyconnect-macos-4.10.06079-webdeploy... | Mac OS ▾ |

- On the next screen, select **Network Interface and Device Certificates**:

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

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

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.

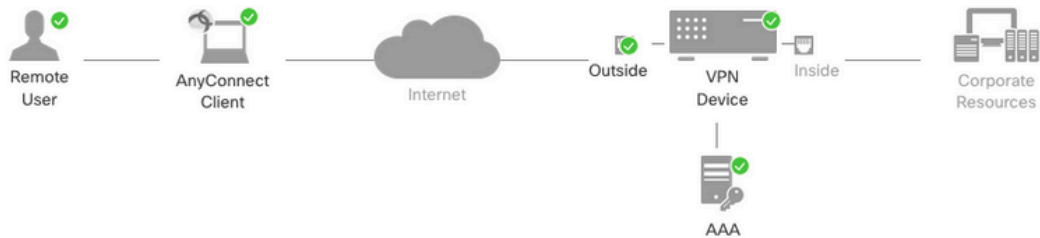
Certificate Enrollment:* +

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.

- When everything is configured correctly, you can click **Finish** and then **Deploy**:



Remote Access VPN Policy Configuration

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

| | |
|------------------------|-----------------------|
| Name: | Anyconnect_RA |
| Device Targets: | FTD |
| Connection Profile: | Anyconnect_RA |
| Connection Alias: | Anyconnect_RA |
| AAA: | |
| Authentication Method: | AAA Only |
| Authentication Server: | RadiusServer (RADIUS) |
| Authorization Server: | RadiusServer (RADIUS) |
| Accounting Server: | - |
| Address Assignment: | |
| Address from AAA: | - |
| DHCP Servers: | - |
| Address Pools (IPv4): | vpn_pool |
| Address Pools (IPv6): | - |
| Group Policy: | DfltGrpPolicy |
| AnyConnect Images: | Anyconnectmac4.10 |
| Interface Objects: | Outsied |
| Device Certificates: | vpntestbed.cisco.com |

Device Identity Certificate Enrollment

Certificate enrollment object 'vpntestbed.cisco.com' 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.

1 Access Control Policy Update

An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.

2 NAT Exemption

If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.

3 DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.

4 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 'Outsied'

- This copies the whole configuration along with certificates and AnyConnect packages to FTD appliance.

Connection

To connect to FTD you need to open a browser, type DNS name or IP address that points to the outside interface. You then log in with credentials stored in RADIUS server and do the instructions on the screen. Once AnyConnect installs, you then need to put the same address in AnyConnect window and click Connect.

Limitations

Currently unsupported on FTD, but available on ASA:

- FTDposture VPN does not support group policy change through dynamic authorization or RADIUS change of authorization (CoA).
- AnyConnect customization (Enhancement: Cisco bug ID [CSCvq87631](#))
- AnyConnect scripts (Enhancement: Cisco bug ID [CSCvt58044](#)).
- AnyConnect localization.

- WSA integration.
- Simultaneous IKEv2 dynamic crypto map for RA and L2L VPN (Enhancement: Cisco bug ID [CSCvr52047](#)).
- TACACS, Kerberos - KCD Authentication and RSA SDI (Enhancement: Cisco bug ID [CSCvx55859](#)).
- Browser Proxy.

Security considerations

By default, the `sysopt connection permit-vpnoption` is disabled. This means, that you need to allow the traffic that comes from the pool of addresses on outside interface via Access Control Policy. Although the pre-filter or access-control rule is added to allow VPN traffic only, if clear-text traffic happens to match the rule criteria, it is erroneously permitted.

There are two approaches to this problem. First, TAC recommended option, is to enable Anti-Spoofing (on ASA it was known as Unicast Reverse Path Forwarding - uRPF) for outside interface, and secondly, is to enable `sysopt connection permit-vpn` to bypass Snort inspection completely. The first option allows a normal inspection of the traffic that goes to and from VPN users.

a) Enable uRPF

- Create a null route for the network used for remote access users, defined in section C. Go to `Devices > Device Management > Edit > Routing > Static Route` and select `Add route`

Add Static Route Configuration



Type: IPv4 IPv6

Interface*

Null0

(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Search

Add

any-ipv4
FMC
GW
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast

Selected Network

objvpnusers 

Gateway*

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

Cancel

OK

- Next, enable uRPF on the interface where the VPN connections terminate. To find this, navigate to **Devices > Device Management > Edit > Interfaces > Edit > Advanced > Security Configuration > Enable Anti Spoofing**.

| | | | | | | |
|-------------|------|------------------------|-----------------|------------------------|----------------|----------|
| General | IPv4 | IPv6 | Path Monitoring | Hardware Configuration | Manager Access | Advanced |
| Information | ARP | Security Configuration | | | | |

Enable Anti Spoofing:

Allow Full Fragment Reassembly:

Override Default Fragment Setting:

Cancel OK

When a user is connected, the 32-bit route is installed for that user in the routing table. Clear the text traffic sourced from the other, unused IP addresses from the pool is dropped by uRFP. To see a description of **Anti-Spoofing** refer to [Set Security Configuration Parameters on Firepower Threat Defense](#).

b) Enable `sysopt connection permit-vpn` Option

- There is an option to do it with the wizard or under `Devices > VPN > Remote Access > VPN Profile > Access Interfaces`.

Access Control for VPN Traffic

- Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`)**
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Related Information

- [Cisco Technical Support & Downloads](#)