

Configure Remote Access VPN on FTD Managed by FDM

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Licensing](#)
[Components Used](#)
[Background Information](#)
[Configure](#)
[Network Diagram](#)
[Verify Licensing on the FTD](#)
[Define Protected Networks](#)
[Create Local Users](#)
[Add Certificate](#)
[Configure Remote Access VPN](#)
[Verify](#)
[Troubleshoot](#)
[AnyConnect Client Issues](#)
[Initial Connectivity Issues](#)
[Traffic-Specific Issues](#)

Introduction

This document describes how to configure the deployment of a RA VPN on FTD managed by the on-box manager FDM that runs version 6.5.0 and later.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Remote Access Virtual Private Network (RA VPN) configuration on Firepower Device Manager (FDM).

Licensing

- Firepower Threat Defense (FTD) registered with the smart licensing portal with Export Controlled Features enabled (in order to allow the RA VPN configuration tab to be enabled)
- Any of the AnyConnect Licenses enabled (APEX, Plus, or VPN-Only)

Components Used

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

- Cisco FTD that runs version 6.5.0-115
- Cisco AnyConnect Secure Mobility Client version 4.7.01076

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.

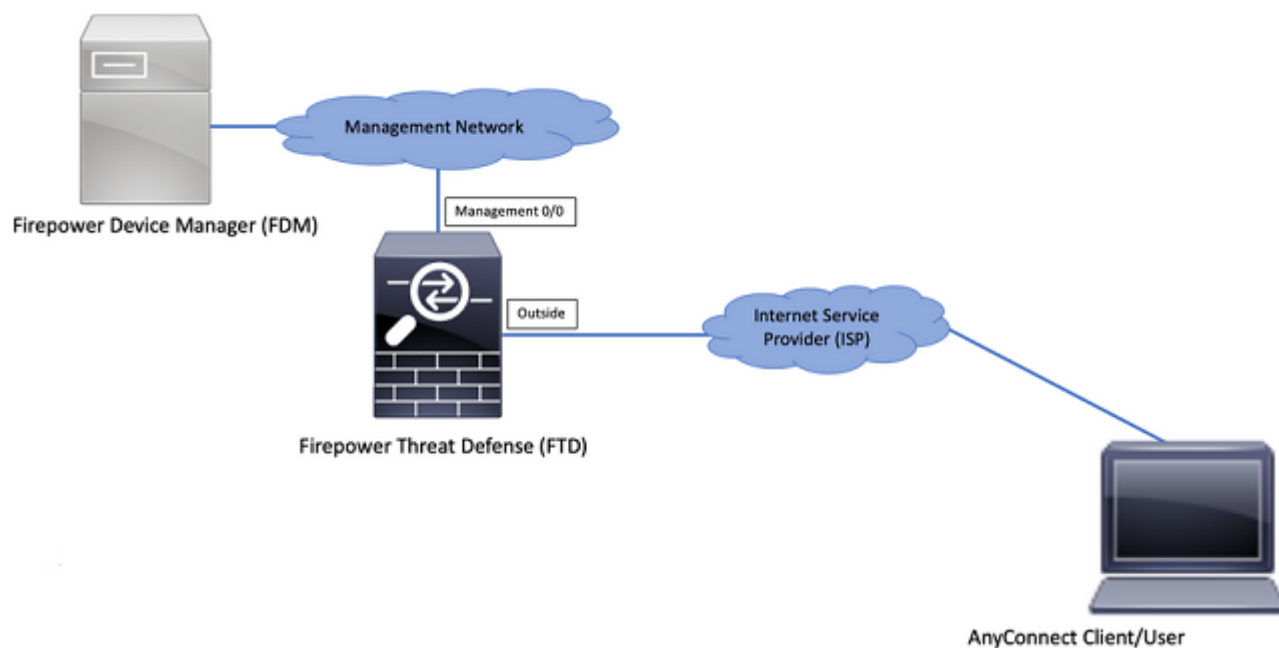
Background Information

Configuration of FTD through FDM poses difficulties when you attempt to establish connections for AnyConnect clients through the external interface while management is accessed through the same interface. This is a known limitation of FDM. Enhancement request [CSCvm76499](#) has been filed for this issue.

Configure

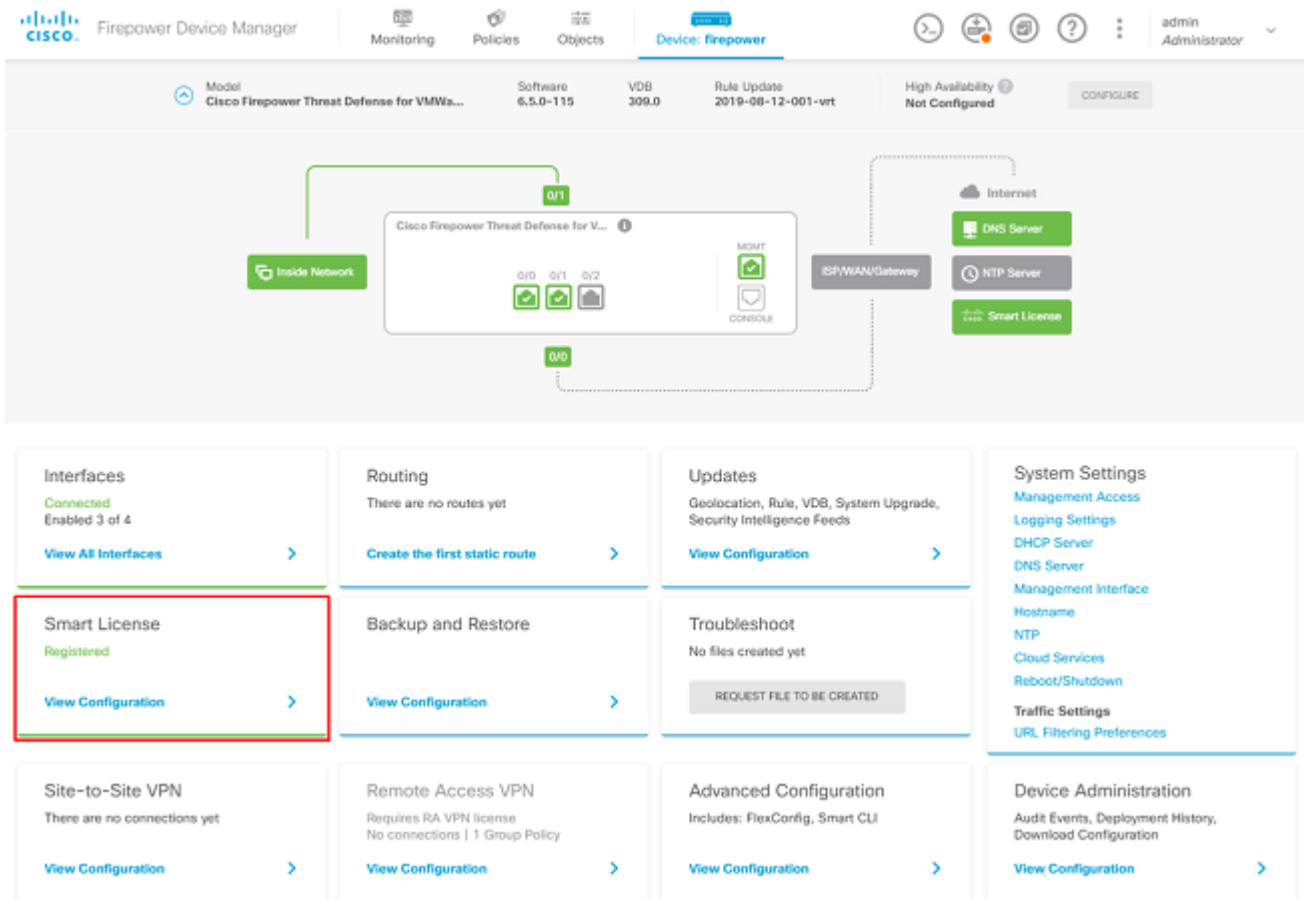
Network Diagram

AnyConnect Client Authentication with the use of Local.

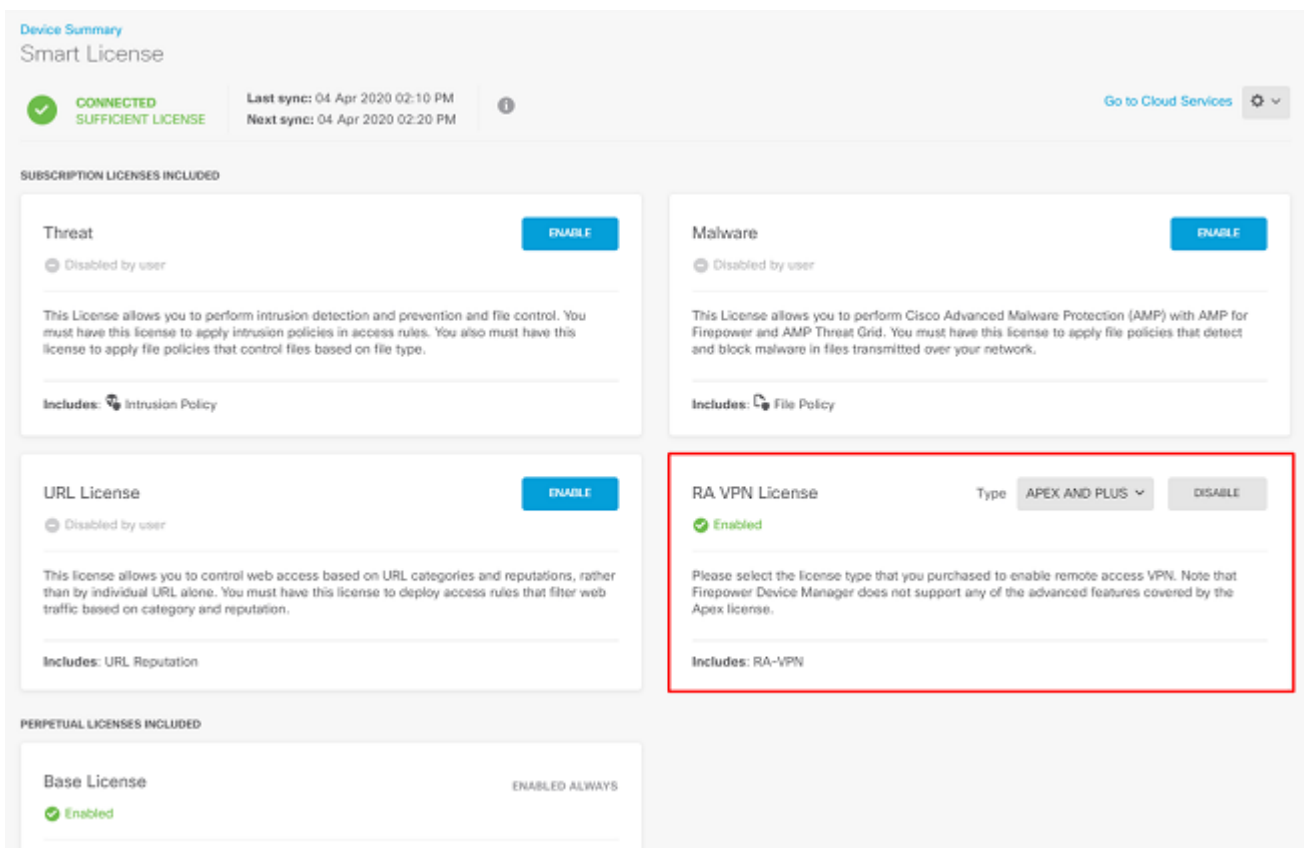


Verify Licensing on the FTD

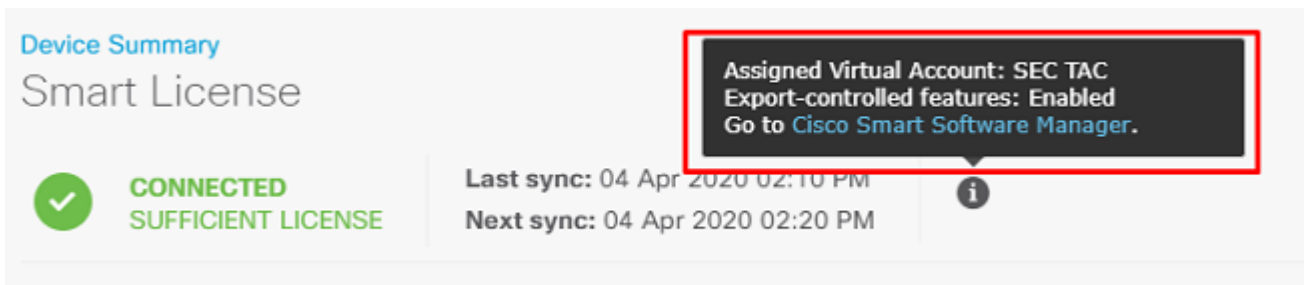
Step 1. Verify the device is registered to Smart Licensing as shown in the image:



Step 2. Verify that AnyConnect licenses are enabled on the device as shown in the image.

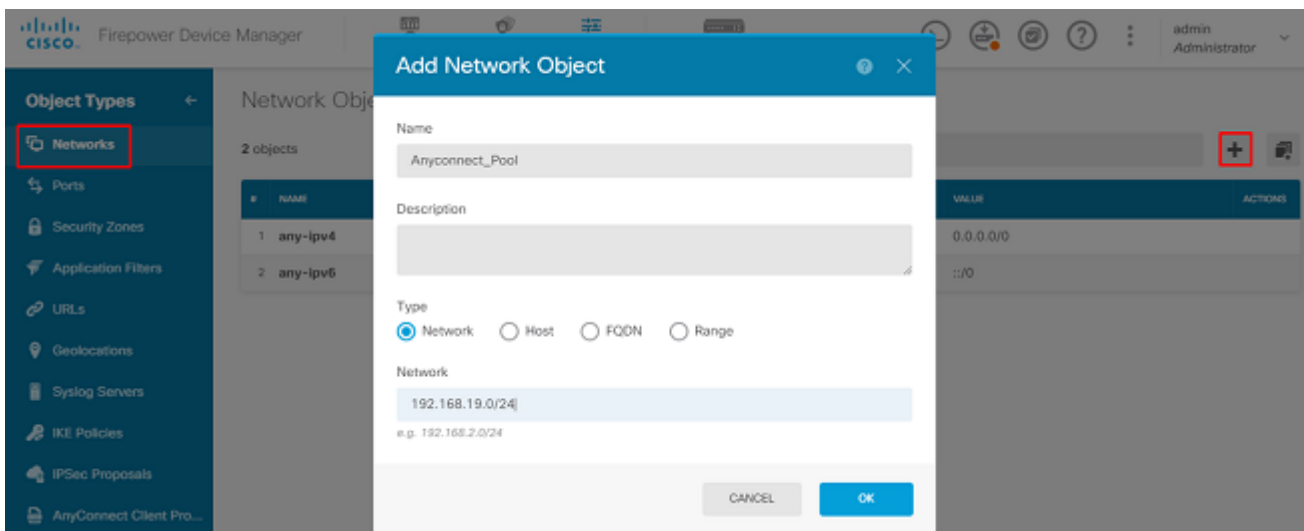


Step 3. Verify that Export-controlled Features are enabled in the token as shown in the image:

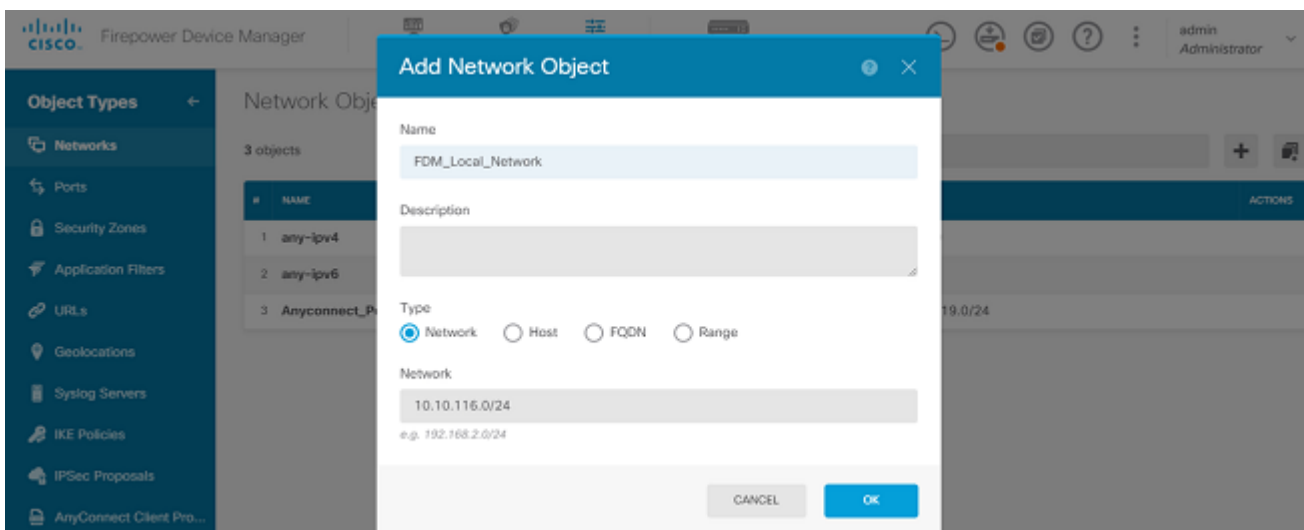


Define Protected Networks

Navigate to Objects > Networks > Add new Network. Configure VPN Pool and LAN Networks from FDM GUI. Create a VPN Pool in order to be used for Local Address Assignment to AnyConnect Users as shown in the image:

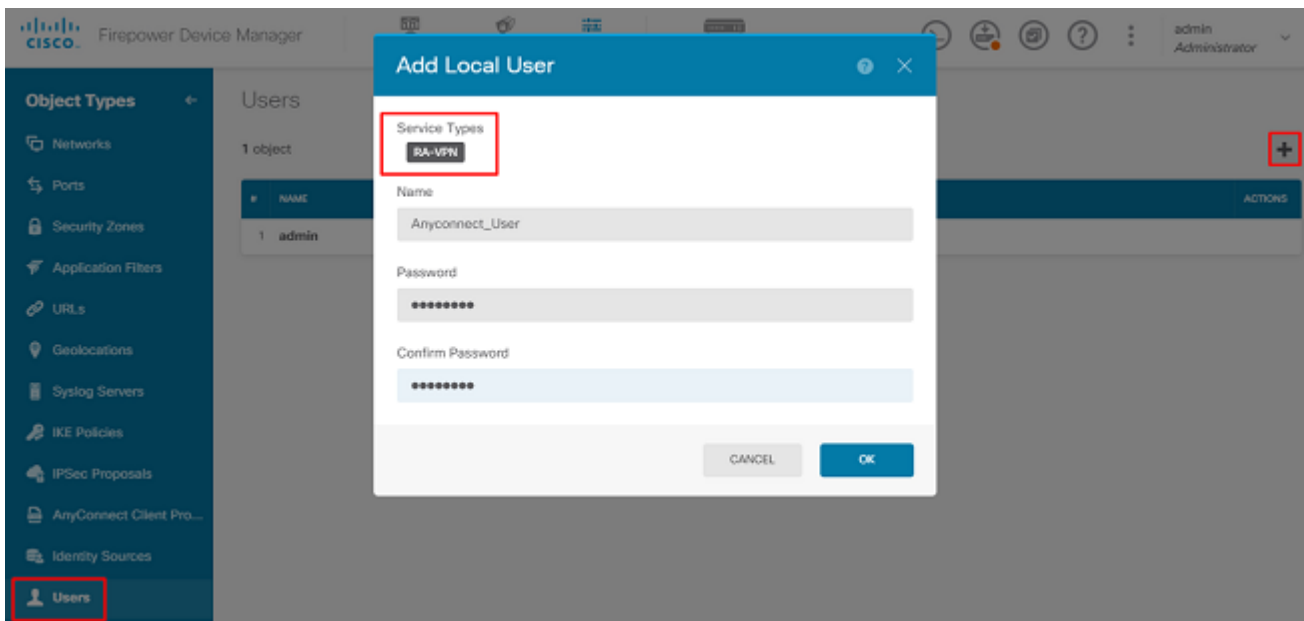


Create an object for the local network behind the FDM device as shown in the image:



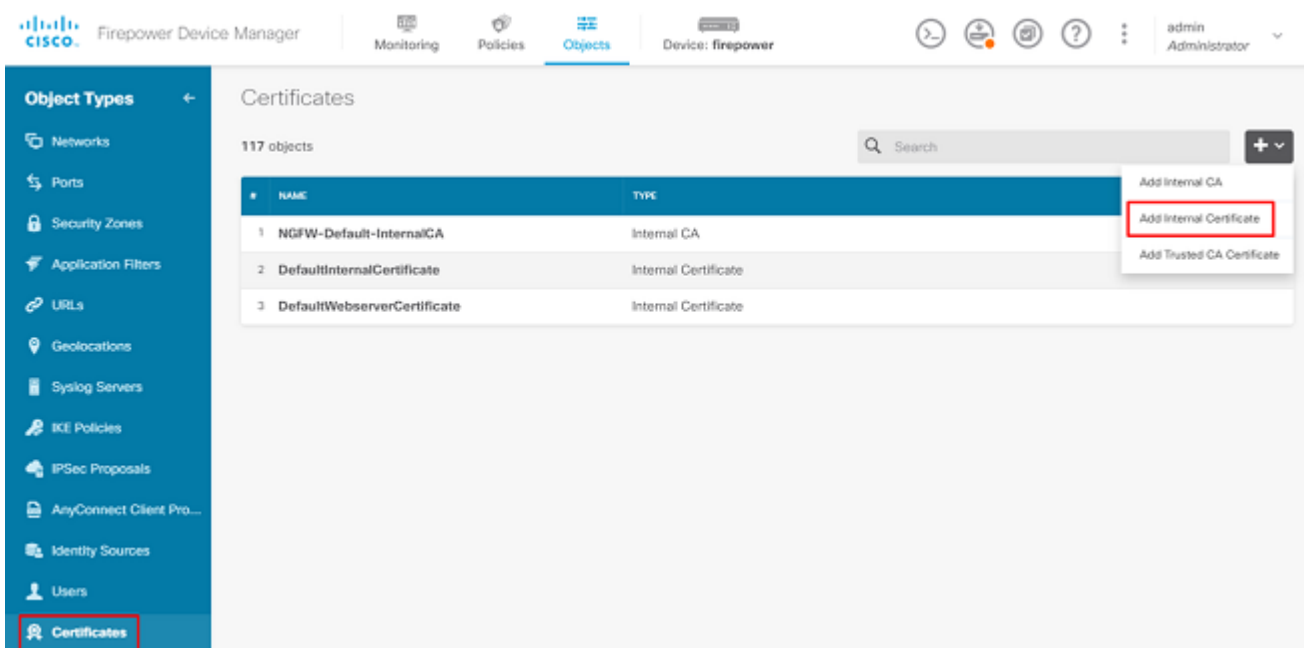
Create Local Users

Navigate to Objects > Users > Add User. Add VPN Local users that connect to FTD via Anyconnect. Create local Users as shown in the image:



Add Certificate

Navigate to Objects > Certificates > Add Internal Certificate. Configure a certificate as shown in the image:



Upload both the certificate and the private key as shown in the image:

Choose the type of internal certificate you want to create



Upload Certificate and Key

Create a certificate from existing files.
PEM and DER files are supported.



Self-Signed Certificate

Create a new certificate that is signed
by the device.

The certificate and key can be uploaded by copy and paste or the upload button for each file as shown in the image:

Add Internal Certificate

Name

Anyconnect_Certificate

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file: **UPLOAD CERTIFICATE** The supported formats are: PEM, DER.

```
wkM7QqtRuyzBzGhnoSebJkP/Hiky/Q+r6UrYSnv++UJSrq777/9NgonwTpLI/8/J  
idGSN0b/ic6iPh2aGpB1Lra3MGCL1pJaRqxq3+1vBDsfVFCaKt9wWcnUveQd6LZp  
k+iaN+V24yOj3vCJILlhtxwdllqeSs8F8XdaL4LQObcTfZ/3YNBWqvevV2TL  
-----END CERTIFICATE-----
```

CERTIFICATE KEY

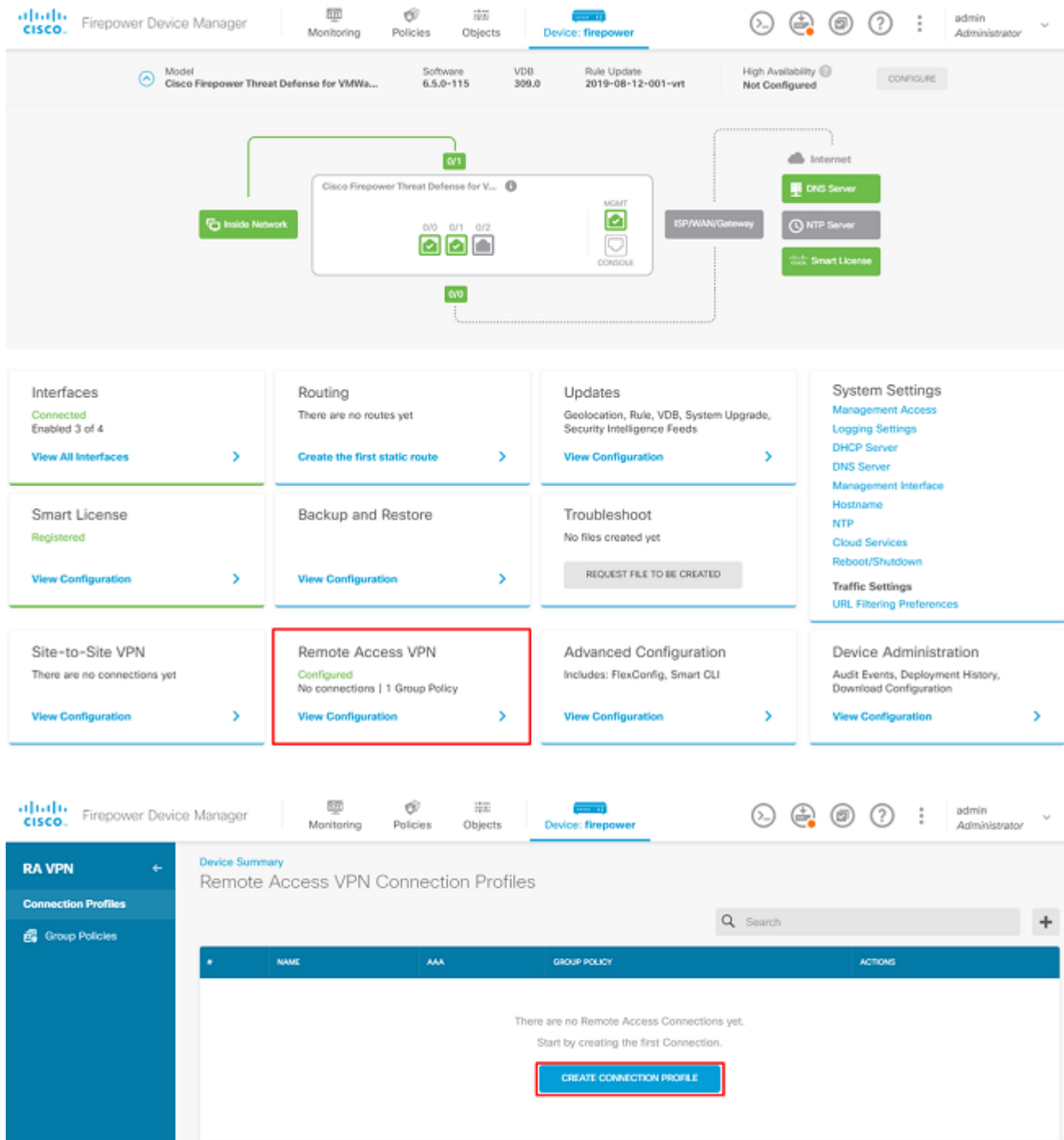
Paste key, or choose file: **UPLOAD KEY** The supported formats are: PEM, DER.

```
QzYPpikCgYEAgJ9nlk8sfPfmotyQwprlBEdwMMDeKLX3KDY58jiv1/8a/wsX+uz  
3A7VQn6gA6iSWHqxHdmgYnD38P6kCuK/hQMUcadiKUITXkh0ZpglQbfW2lJ0VD4M  
gKugRI5t0Zva5j+bO5q0f8D/mtYYTBf8JGggEfSju0Zsy2ifWtsbJrE=  
-----END RSA PRIVATE KEY-----
```

CANCEL **OK**

Configure Remote Access VPN

Navigate to Remote Access VPN > Create Connection Profile. Navigate through the RA VPN Wizard on FDM as shown in the image:



Create a connection profile and start the configuration as shown in the image:

Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

Connection Profile Name

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

Anyconnect

Group Alias

Anyconnect

[Add Group Alias](#)

Group URL

[Add Group URL](#)

Choose the authentication methods as shown in the image. This guide uses Local Authentication.

Primary Identity Source

Authentication Type

AAA Only

Client Certificate Only

AAA and Client Certificate

Primary Identity Source for User Authentication

LocalIdentitySource

Fallback Local Identity Source

Please Select Local Identity Source

Strip Identity Source server from username

Strip Group from Username

Secondary Identity Source

Secondary Identity Source for User Authentication

Please Select Identity Source

Advanced

Authorization Server

Please select

Accounting Server

Please select

Choose the Anyconnect_Pool object as shown in the image:

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool



Anyconnect_Pool

IPv6 Address Pool

Endpoints are provided an address from this pool



DHCP Servers



CANCEL

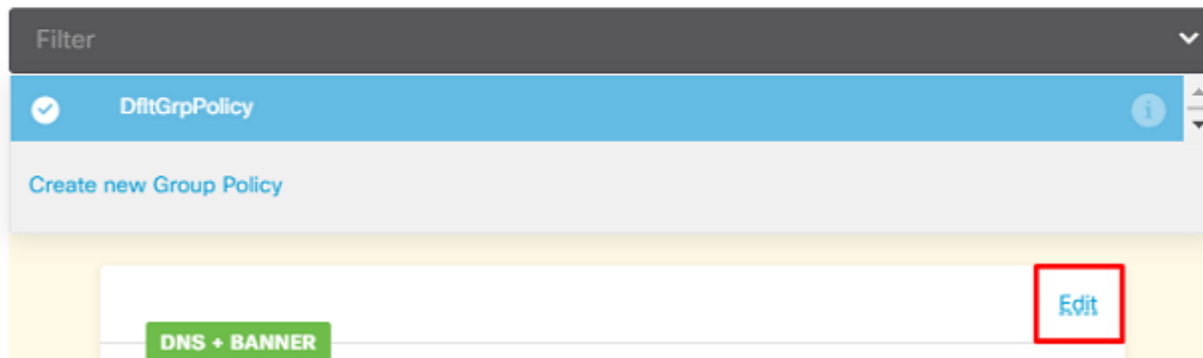
NEXT

A summary of the default Group Policy is displayed on the next page. A new group policy can be created when you hit the drop-down and choose the option to Create a new Group Policy. For this guide, the default Group Policy is used. Choose the edit option at the top of the policy as shown in the image:

Remote User Experience

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.

View Group Policy



In the group policy, add Split tunneling so users connected to Anyconnect only send traffic that is destined to the internal FTD network over the Anyconnect client while all other traffic goes out of the ISP connection of the user as shown in the image:

Corporate Resources (Split Tunneling)

IPv4 Split Tunneling

Allow specified traffic over tunnel



IPv6 Split Tunneling

Allow all traffic over tunnel



IPv4 Split Tunneling Networks



FDM_Local_Network

On the next page, choose the `Anyconnect_Certificate` added in the certificate section. Next, choose the interface on which the FTD listens for AnyConnect connections. Choose the Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`). This is an optional command if the `sysopt permit-vpn` is not chosen. An access control policy must be created that allows traffic from the Anyconnect clients to access the internal network as shown in the image:

Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity

Anyconnect_Certificate



Outside Interface

outside (GigabitEthernet0/0)



Fully-qualified Domain Name for the Outside Interface

e.g. `ravpn.example.com`

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`)

NAT exemption can be configured manually under `Policies > NAT` or it can be configured automatically by the wizard. Choose the inside interface and the networks that Anyconnect clients need in order to access as shown in the image.

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



FDM_Local_Network

Choose the Anyconnect Package for each operating system (Windows/Mac/Linux) that users can connect with, as shown in the image.

AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from software.cisco.com. You must have the necessary AnyConnect software license.

Packages

UPLOAD PACKAGE



Windows: anyconnect-win-4.7.04056-webdeploy-k9.pkg

BACK

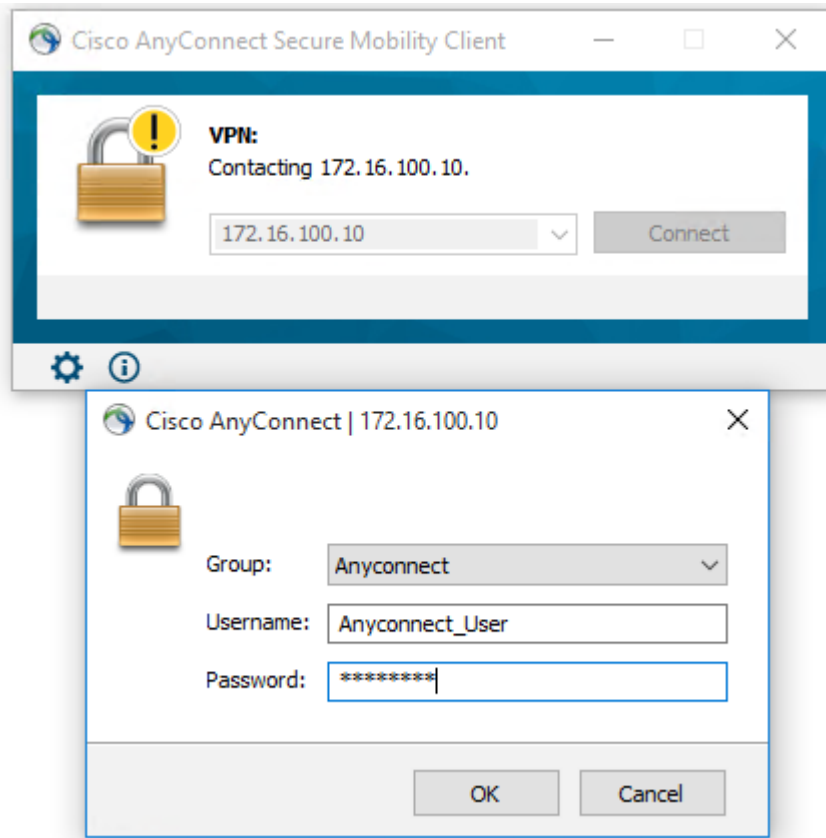
NEXT

The last page gives a summary of the entire configuration. Confirm that the correct parameters have been set and hit the Finish Button and Deploy the new configuration.

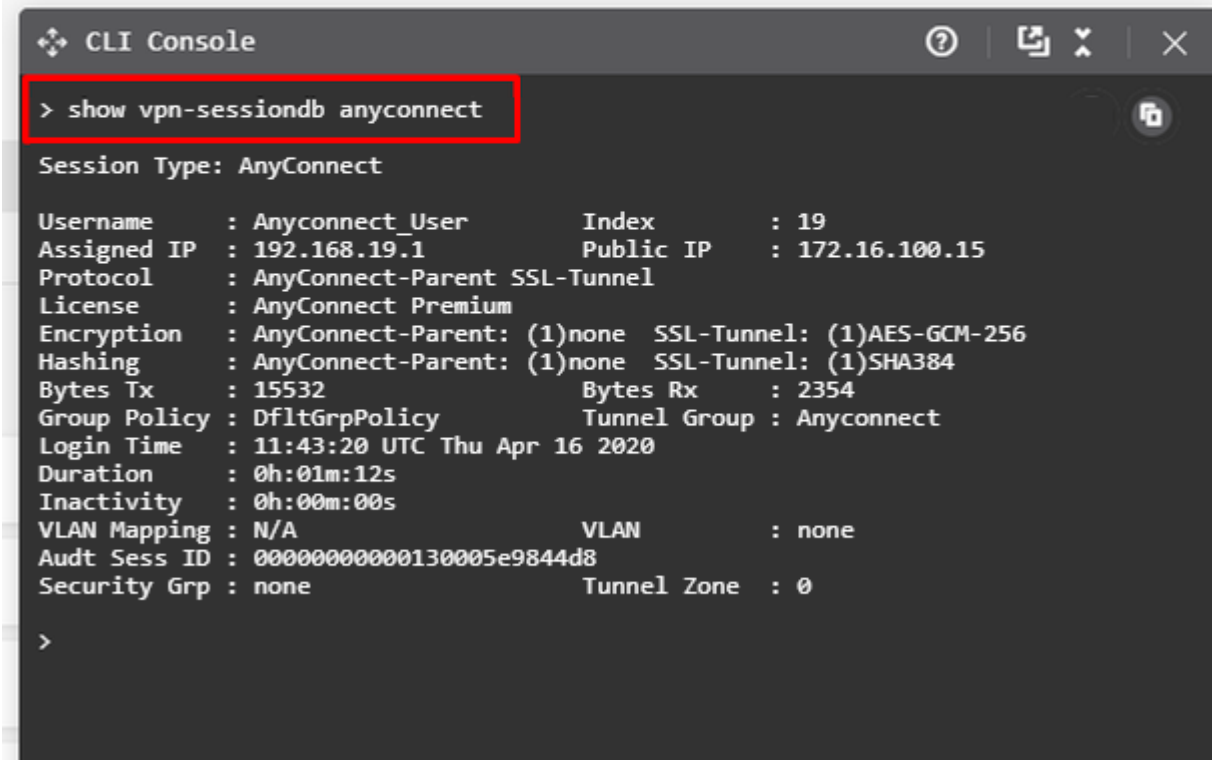
Verify

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

Once the configuration is deployed, attempt to connect. If you have an FQDN that resolves to the outside IP of the FTD, enter it in the Anyconnect connection box. In this example, the outside IP address of the FTD is used. Use the username/password created in the objects section of FDM as shown in the image.



As of FDM 6.5.0, there is no way to monitor the Anyconnect users through the FDM GUI. The only option is to monitor the Anyconnect users via CLI. The CLI console of the FDM GUI can be used as well to verify users are connected. Use this command, `Show vpn-sessiondb anyconnect`.



The same command can be run directly from the CLI.

```
> show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

```
Username      : Anyconnect_User      Index       : 15
Assigned IP   : 192.168.19.1          Public IP   : 172.16.100.15
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx      : 38830                Bytes Rx    : 172
Group Policy  : DfltGrpPolicy        Tunnel Group : Anyconnect
Login Time    : 01:08:10 UTC Thu Apr 9 2020
Duration      : 0h:00m:53s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN        : none
Audt Sess ID  : 000000000000f0005e8e757a
Security Grp  : none                  Tunnel Zone : 0
```

Troubleshoot

This section provides the information you can use to troubleshoot your configuration.

If a user is unable to connect to the FTD with SSL, perform these steps in order to isolate the SSL negotiation issues:

1. Verify that the IP address outside FTD can be pinged through the computer of the user.
2. Use an external sniffer in order to verify whether the TCP three-way handshake is successful.

AnyConnect Client Issues

This section provides guidelines to troubleshoot the two most common AnyConnect VPN client issues. A troubleshooting guide for the AnyConnect client can be found here: [AnyConnect VPN Client Troubleshooting Guide](#).

Initial Connectivity Issues

If a user has initial connectivity issues, enable debug `webvpn AnyConnect` on the FTD and analyze the debug messages. Debugs must be run on the CLI of the FTD. Use the command `debug webvpn anyconnect 255`.

Collect a DART bundle from the client machine in order to get the logs from AnyConnect. Instructions on how to collect a DART bundle can be found here: [Collecting DART bundles](#).

Traffic-Specific Issues

If a connection is successful but traffic fails over the SSL VPN tunnel, look at the traffic statistics on the client to verify that traffic is being received and transmitted by the client. Detailed client statistics are available in all versions of AnyConnect. If the client shows that traffic is being sent and received, check the FTD for received and transmitted traffic. If the FTD applies a filter, the filter name is shown and you can look at the ACL entries in order to check whether your traffic is being dropped. Common traffic issues that users experience are:

- Routing issues behind the FTD - the internal network is unable to route packets back to the assigned IP addresses and VPN clients
- Access control lists blocking traffic
- Network Address Translation not being bypassed for VPN traffic

For further information about remote access VPNs on the FTD managed by FDM, find the full configuration guide here: [Remote Access FTD managed by FDM](#).