Configure Remote Access VPN on FTD Managed by FDM

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Licensing

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 RAVPN 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 (RAVPN) configuration on Firepower Device Manager (FDM).

Components Used

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

- Cisco Firepower Threat Defense (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.

Licensing

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

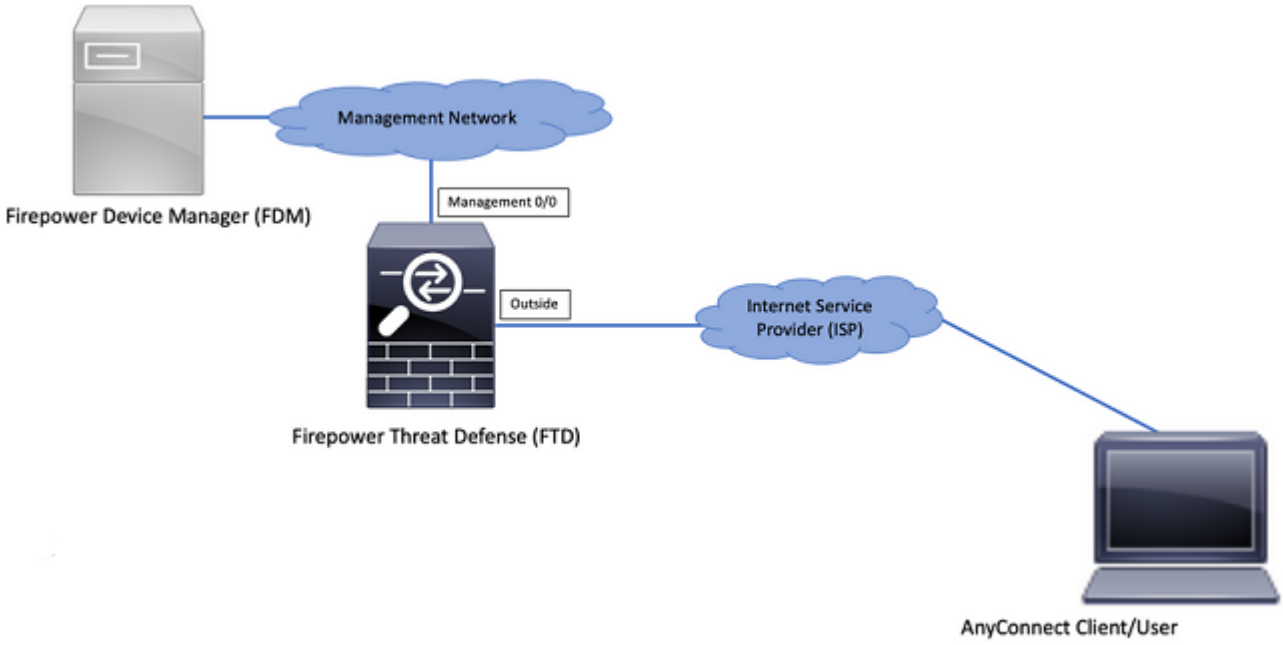
Background Information

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 Cisco bug ID CSCvm76499 has been filed for this issue.

Configure

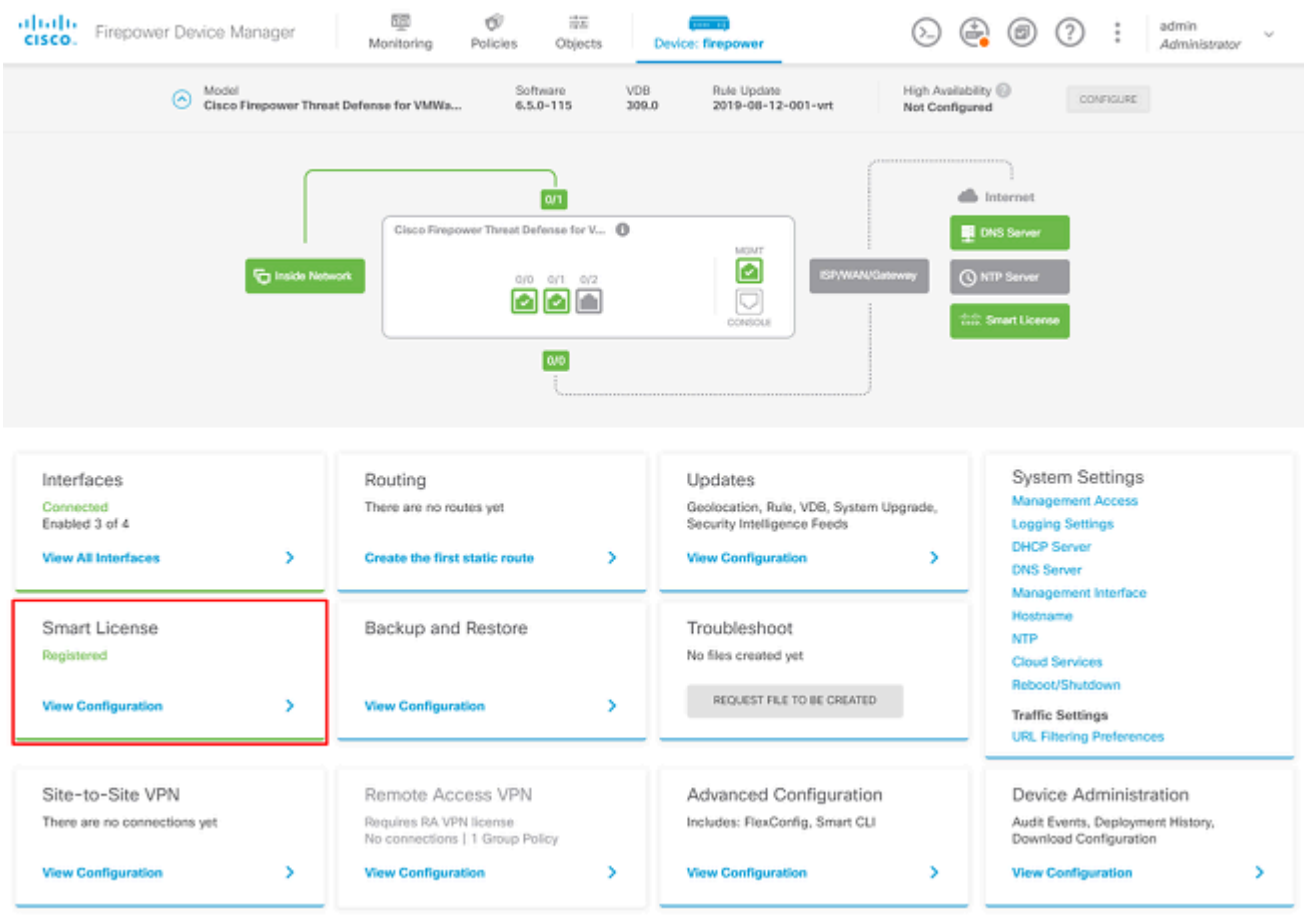
Network Diagram

AnyConnect Client Authentication with the use of Local.

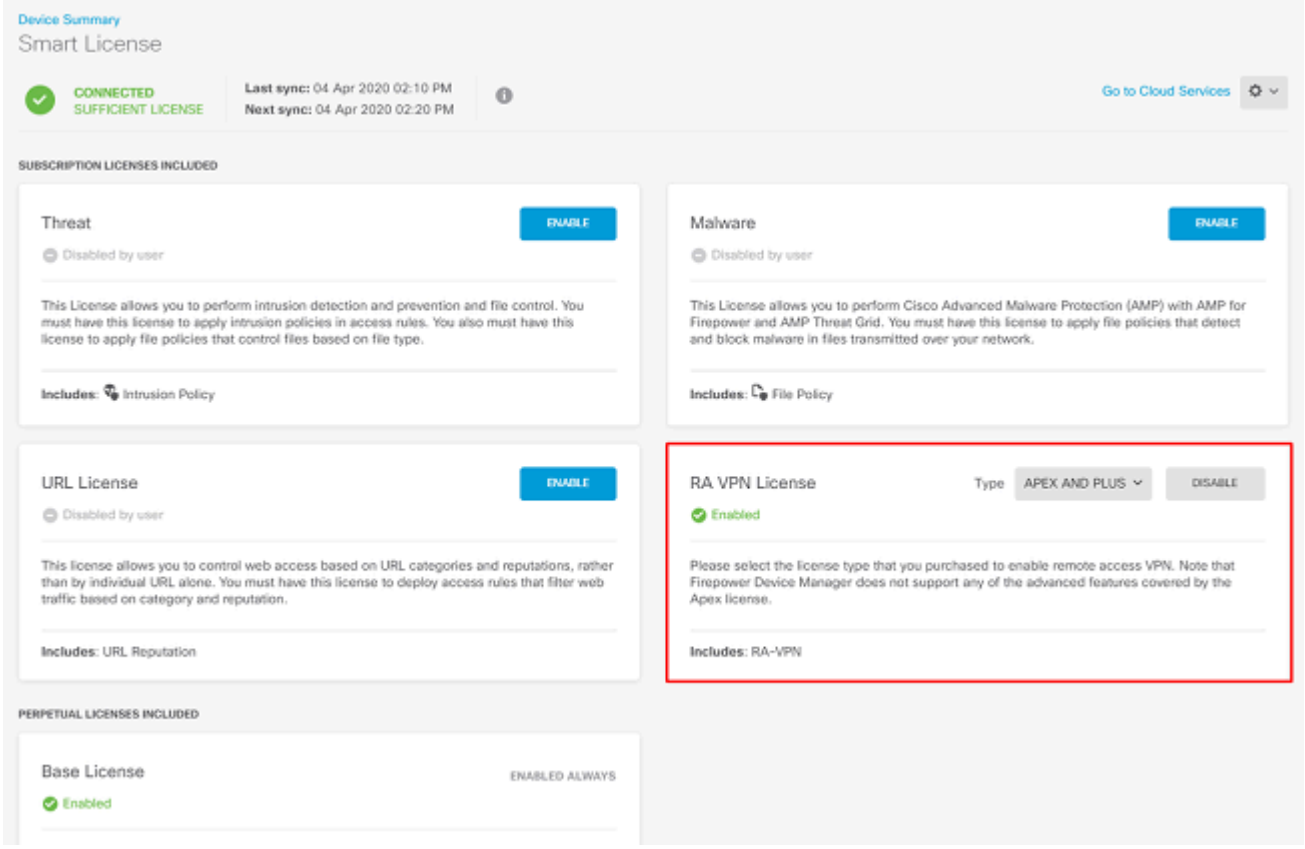


Verify Licensing on the FTD

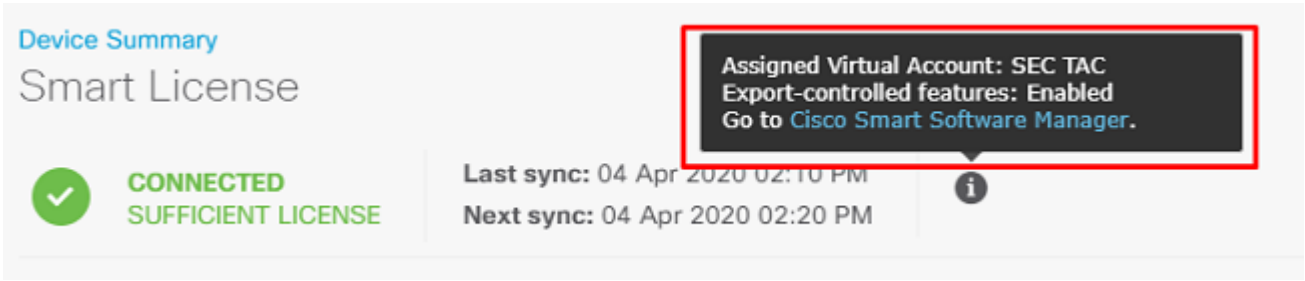
Step 1. Verify the device is registered to Smart Licensing as shown in the image.



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

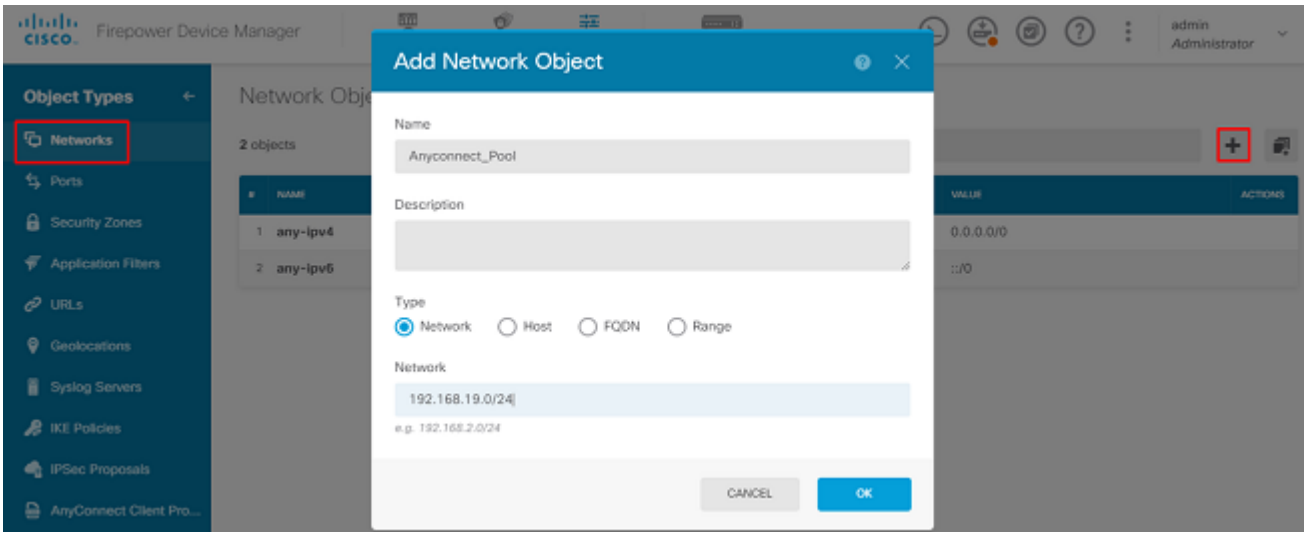


Step 3. Verify that Export-controlled Features are enabled in the token as shown in the image.

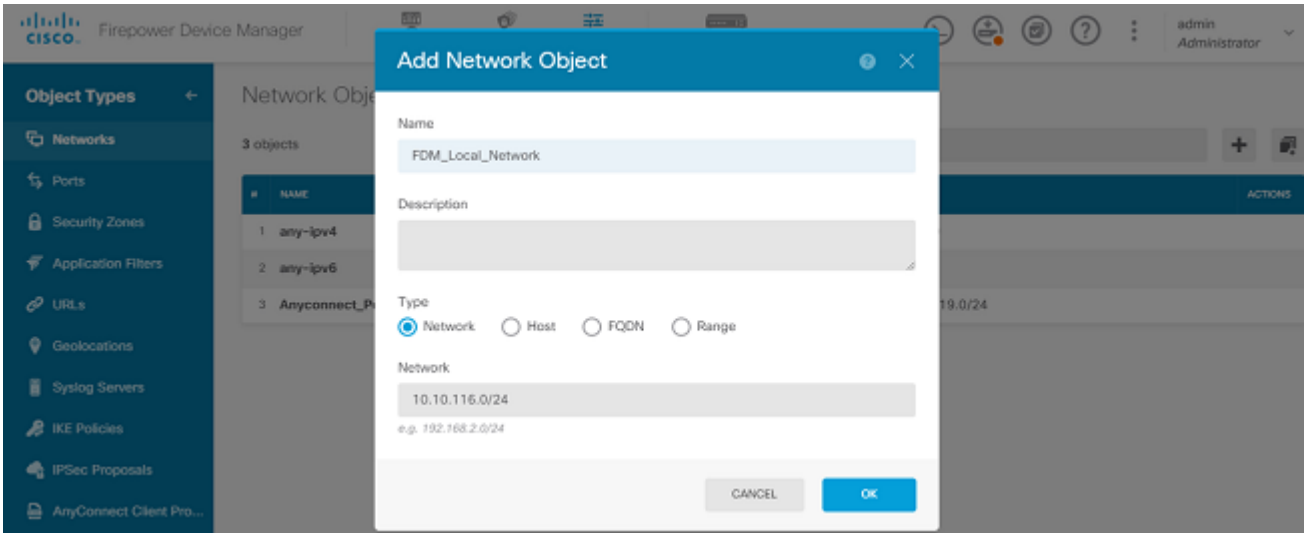


Define Protected Networks

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.

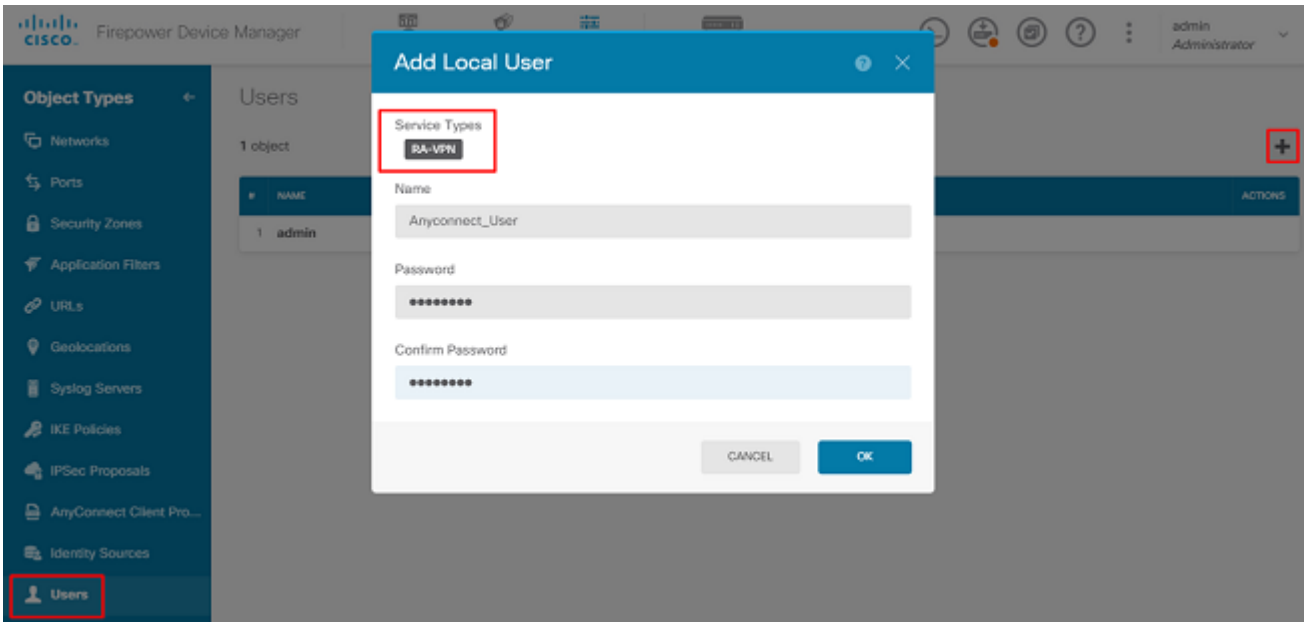


Create an **object** for the local network behind the FDM device as shown in the image.



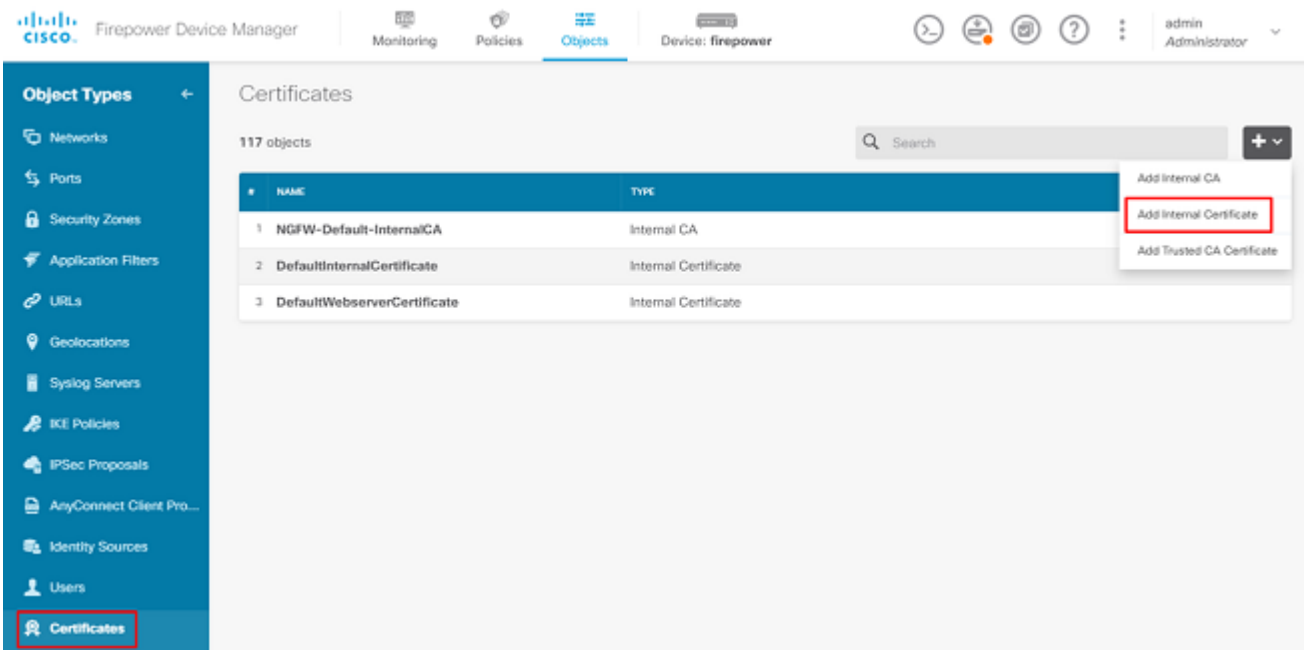
Create Local Users

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

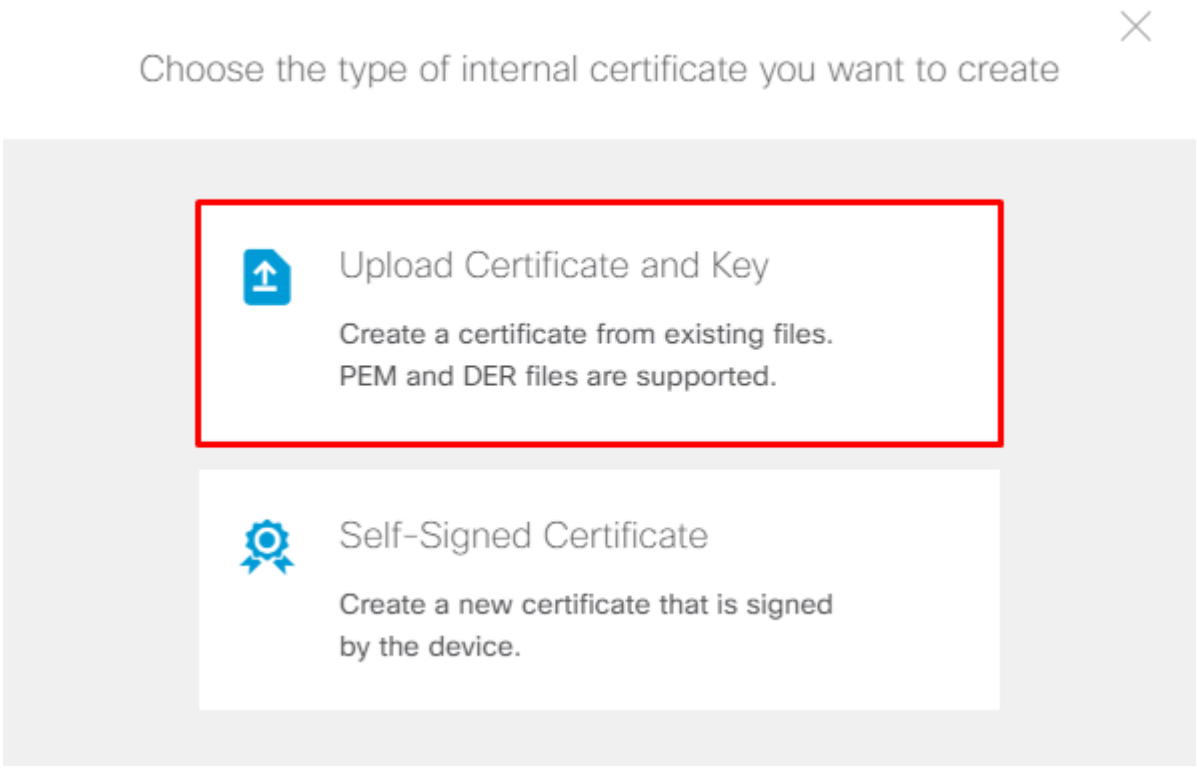


Add Certificate

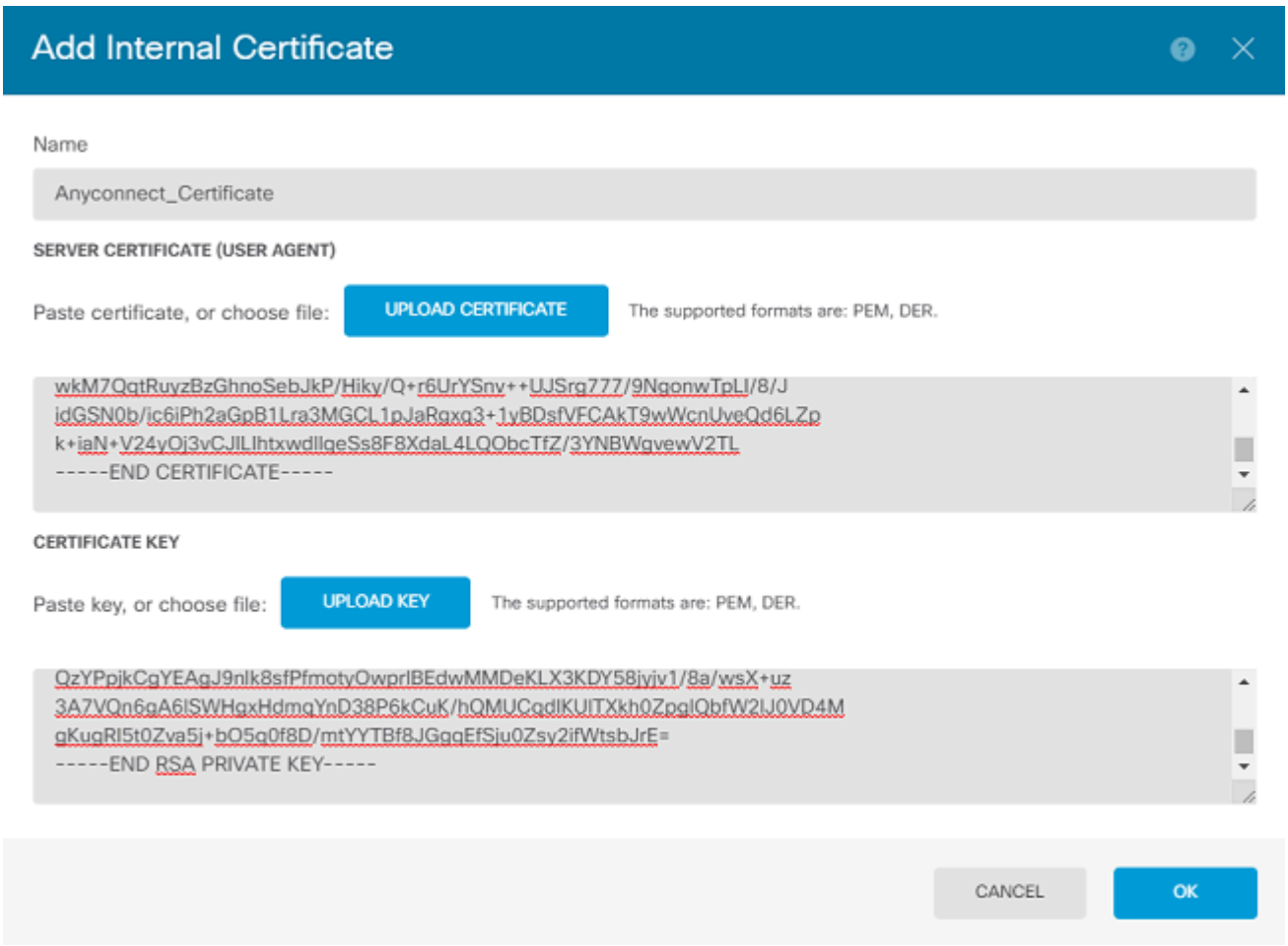
Navigate to Objects > Certificates > Add Internal Certificate. Configure a **certificate** as shown in the image.



Upload both the **certificate** and the **private key** as shown in the image.

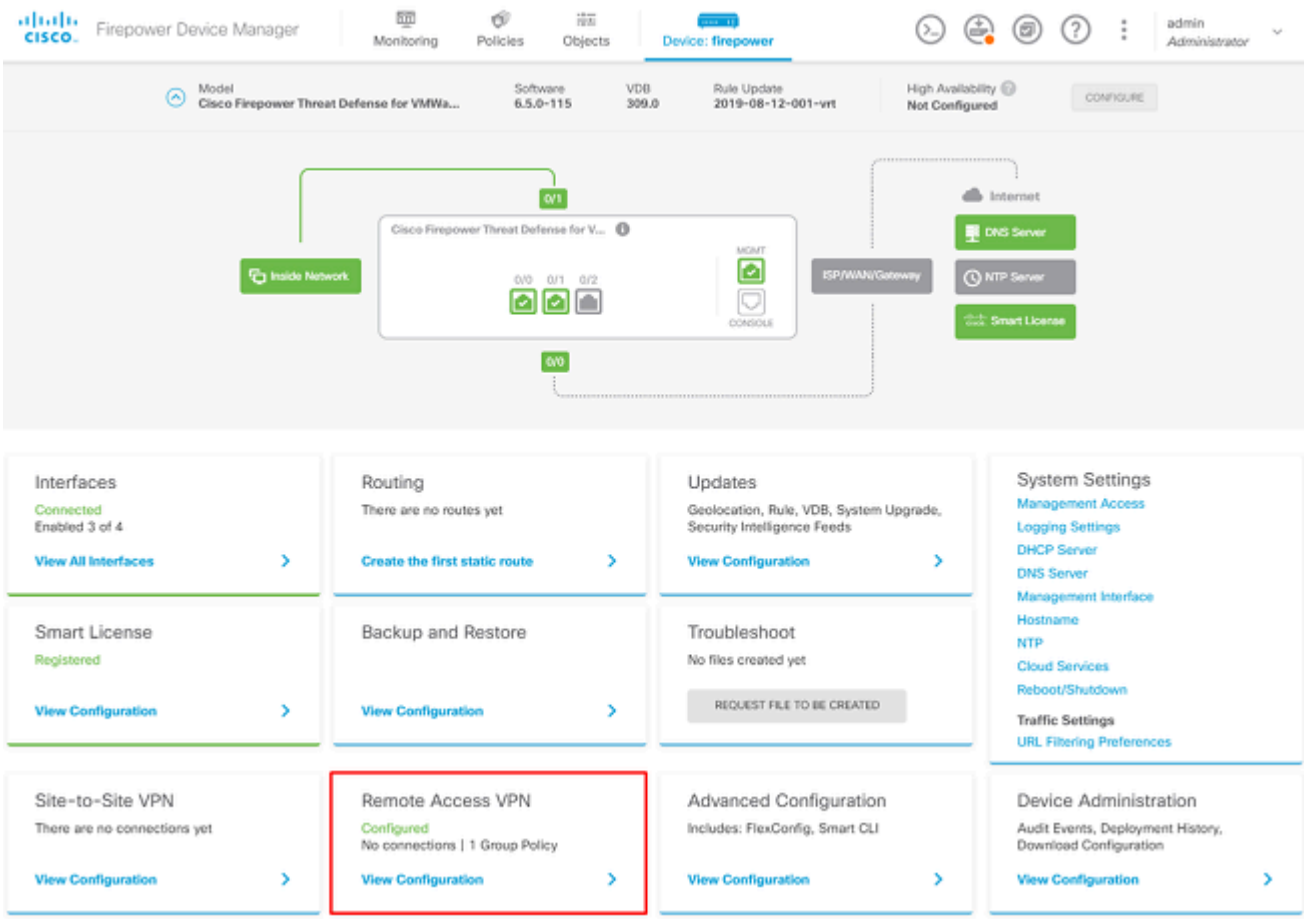


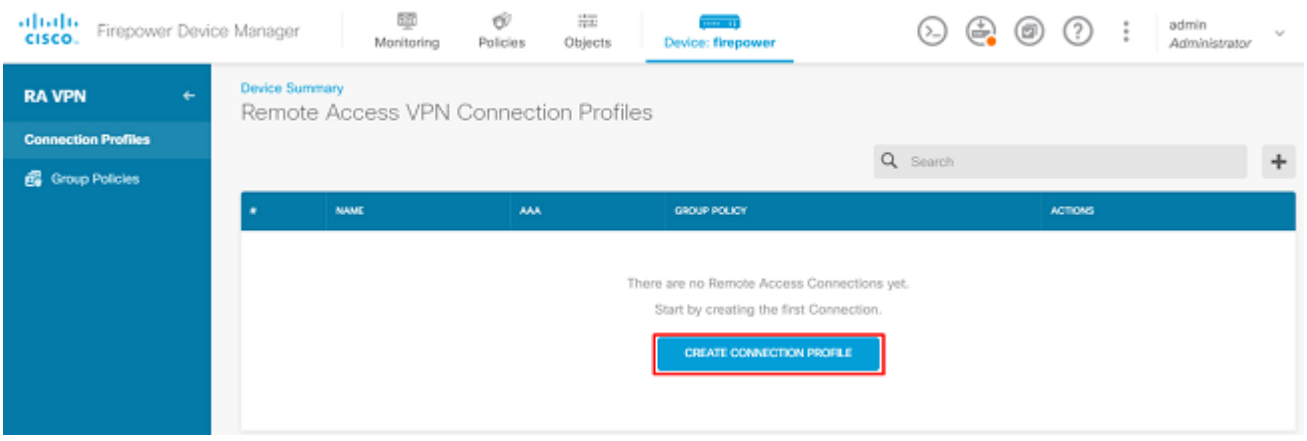
The certificate and key can be uploaded by copy and paste, or the upload button for each file as shown in the image.



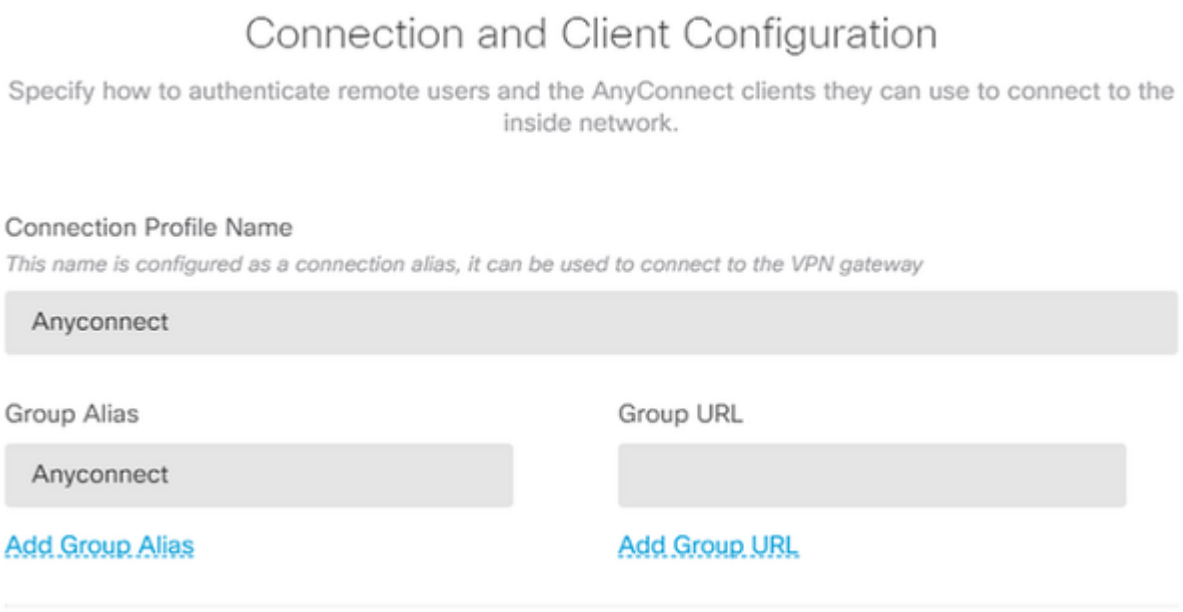
Configure Remote Access VPN

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

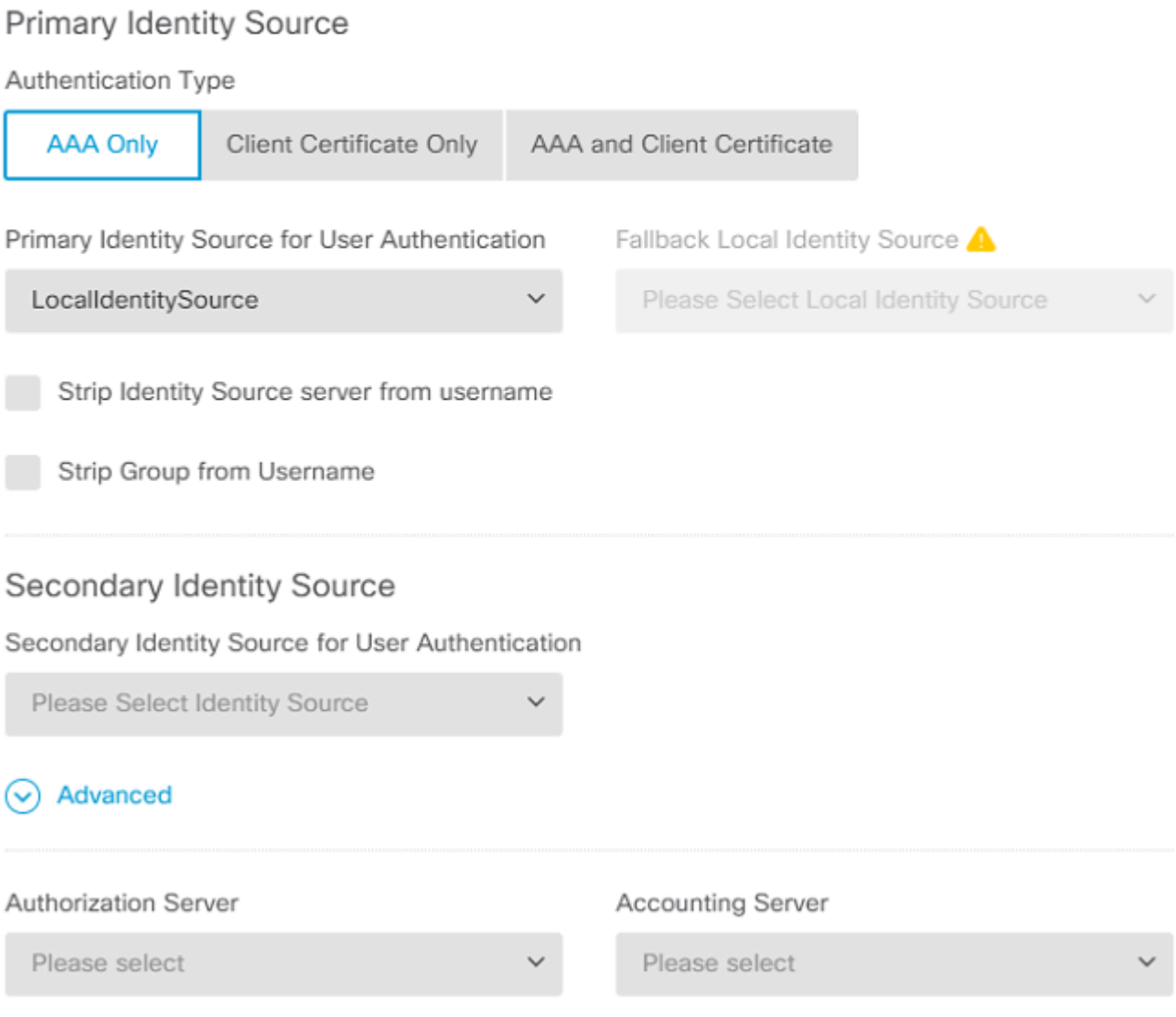




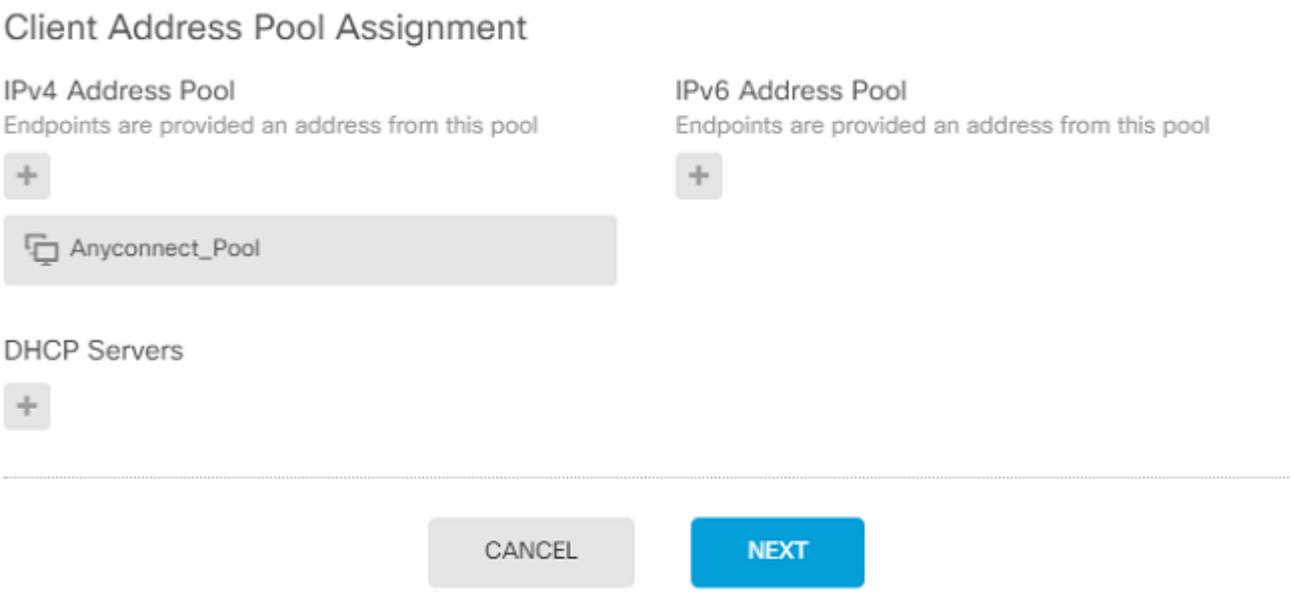
Create a **connection profile** and start the **configuration** as shown in the image.



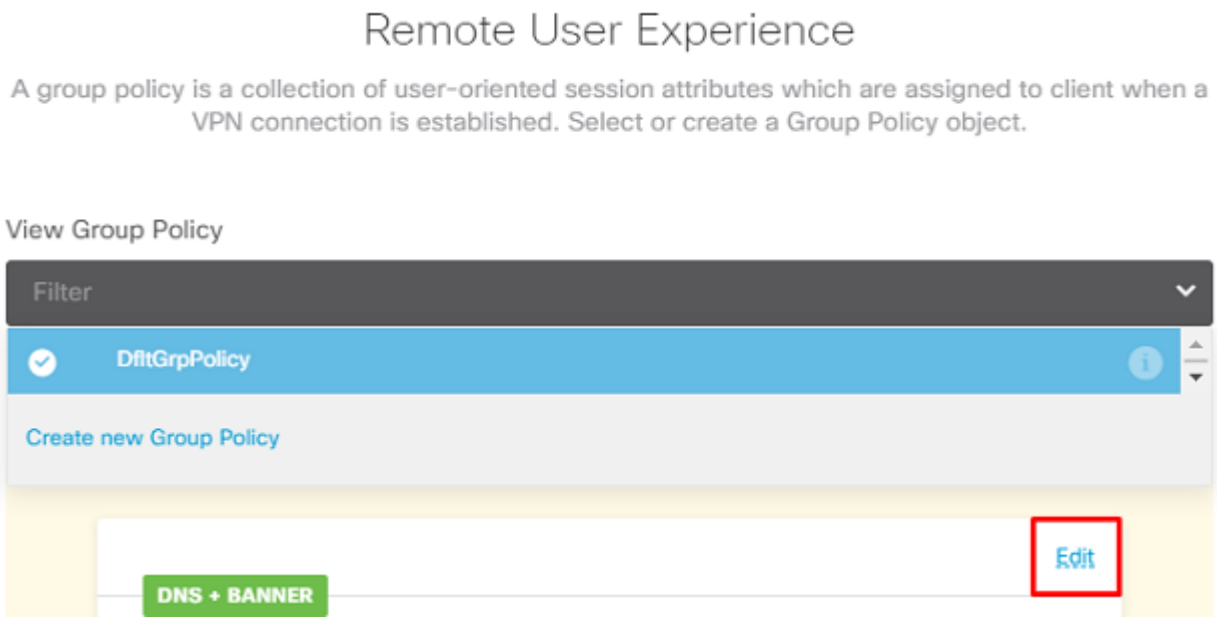
Choose the authentication methods as shown in the image. This guide uses Local Authentication.



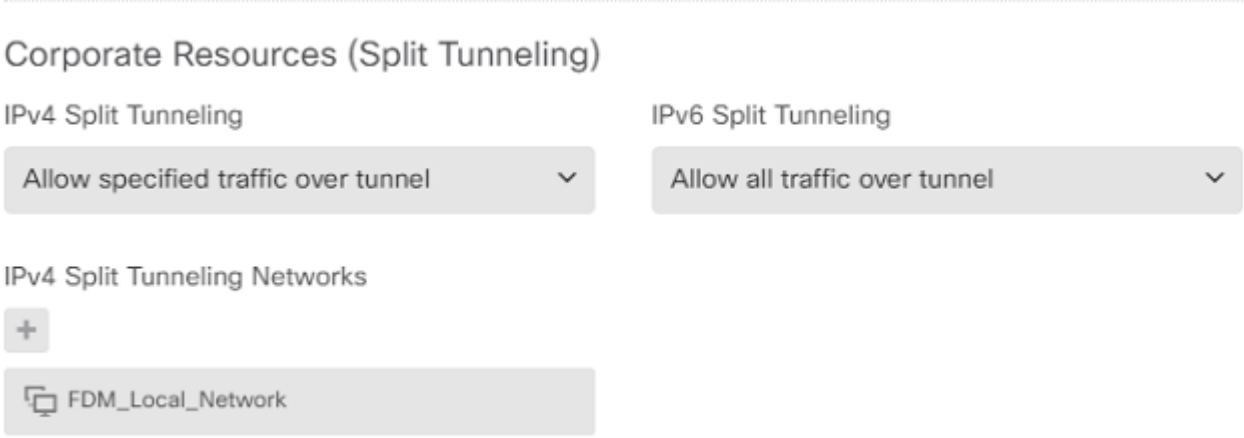
Choose the Anyconnect_Pool object as shown in the image.



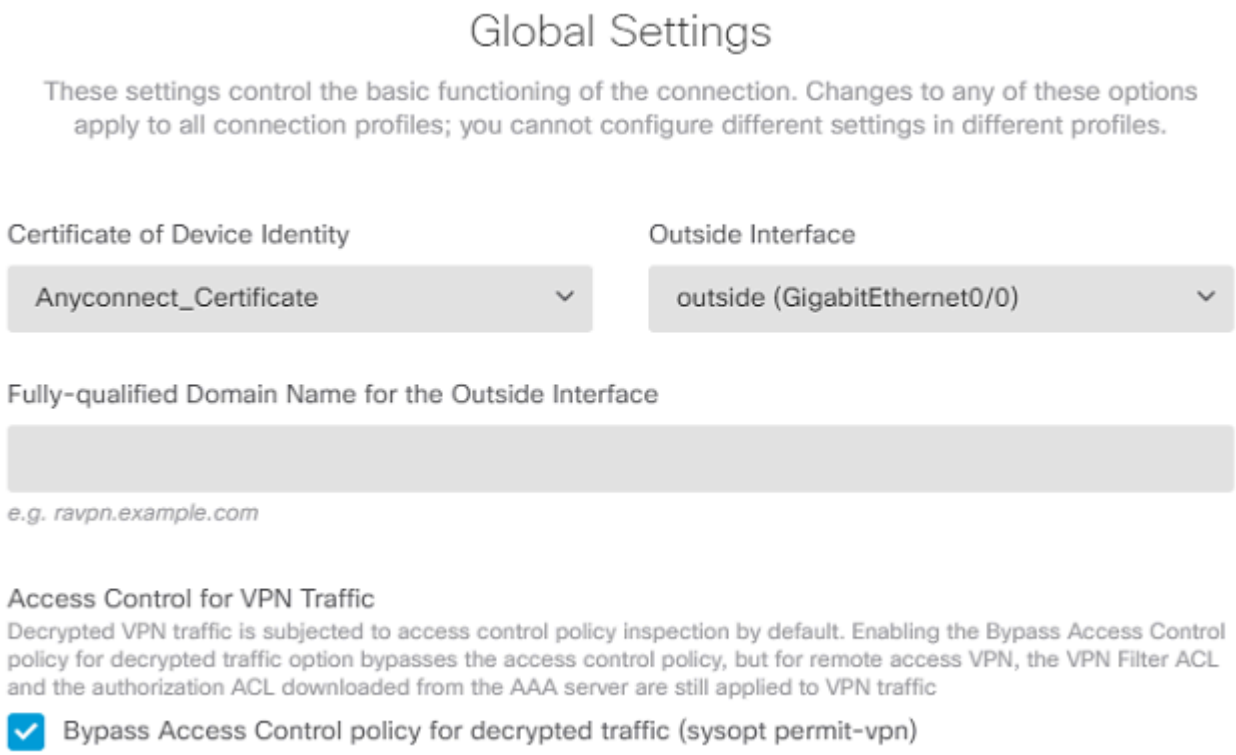
A summary of the default Group Policy is displayed on the next page. A new group policy can be created when you hit the drop-down and choose the option to Create a new Group Policy. For this guide, the default Group Policy is used. Choose the **edit** option at the top of the policy as shown in the image.



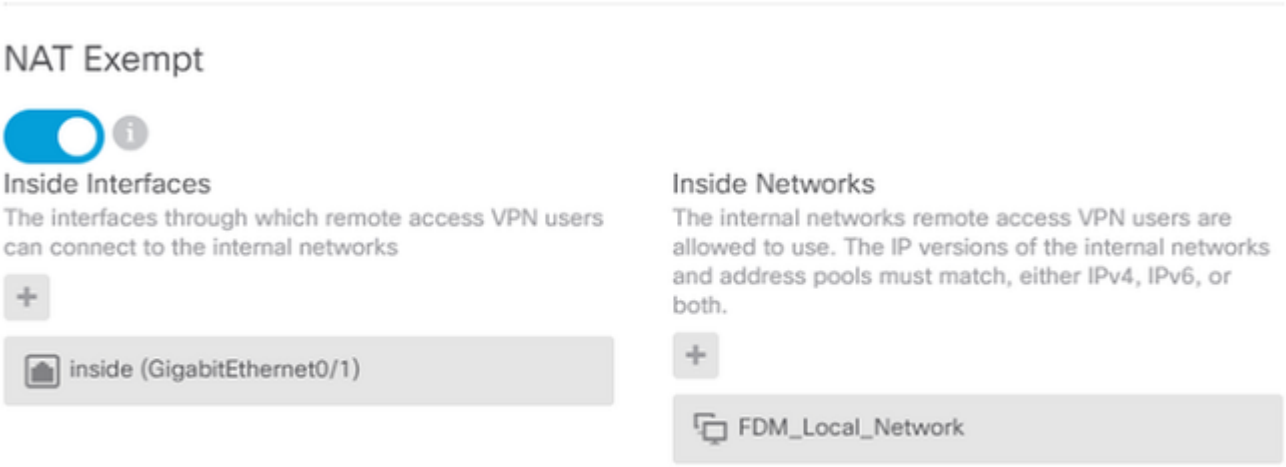
In the group policy, add **Split tunneling** so users connected to AnyConnect only send traffic that is destined to the internal FTD network over the AnyConnect client while all other traffic goes out of the ISP connection of the user as shown in the image.



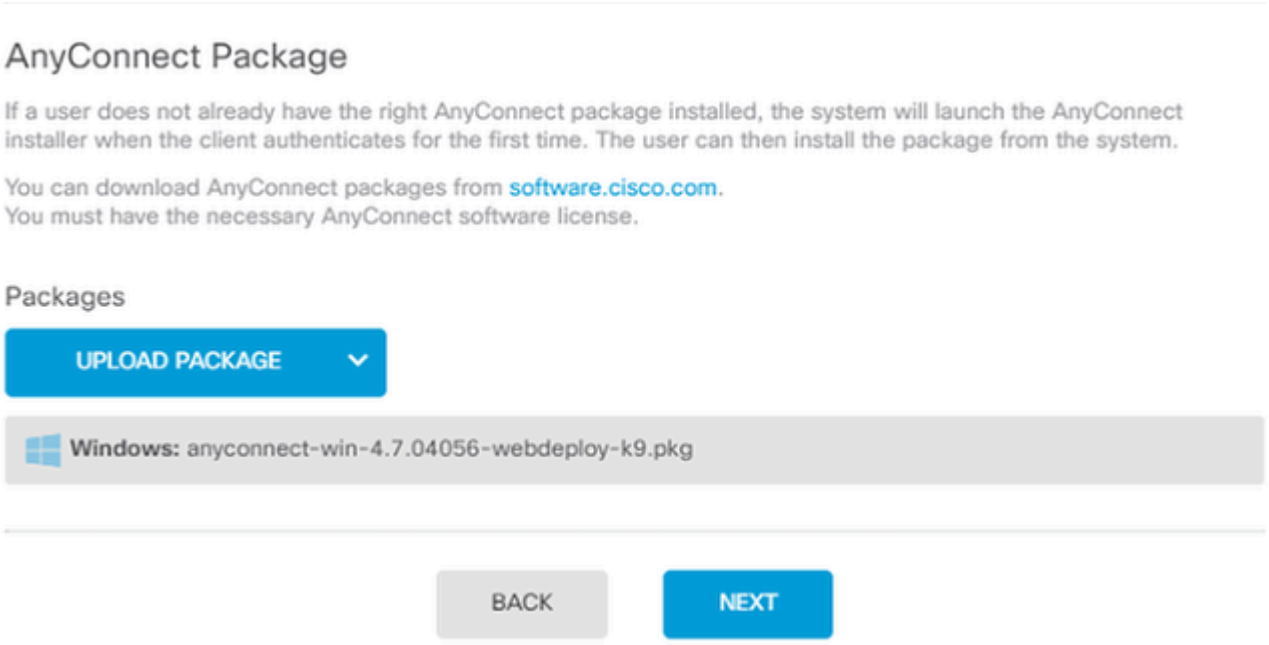
On the next page, choose the Anyconnect_Certificate added in the certificate section. Next, choose the **interface** on which the FTD listens for AnyConnect connections. Choose the **Bypass Access Control policy** for decrypted traffic (sysopt permit-vpn). This is an optional command if the sysopt permit-vpn 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.



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.



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



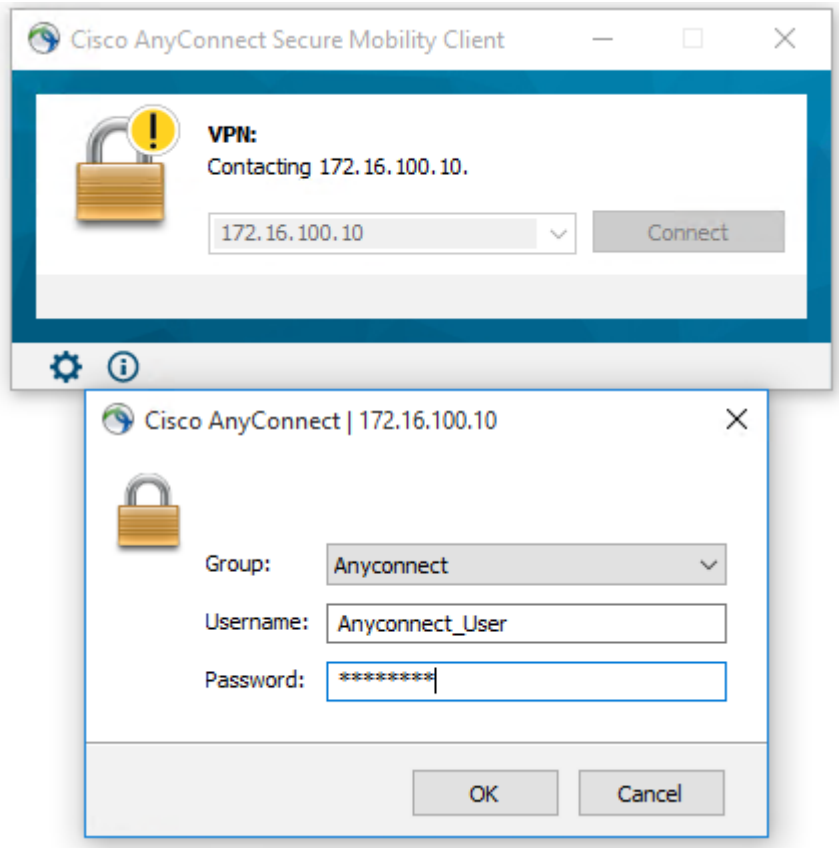
The last page gives a summary of the entire configuration. Confirm that the correct parameters have been set and hit the **Finish** Button and **Deploy** the new configuration.

Verify

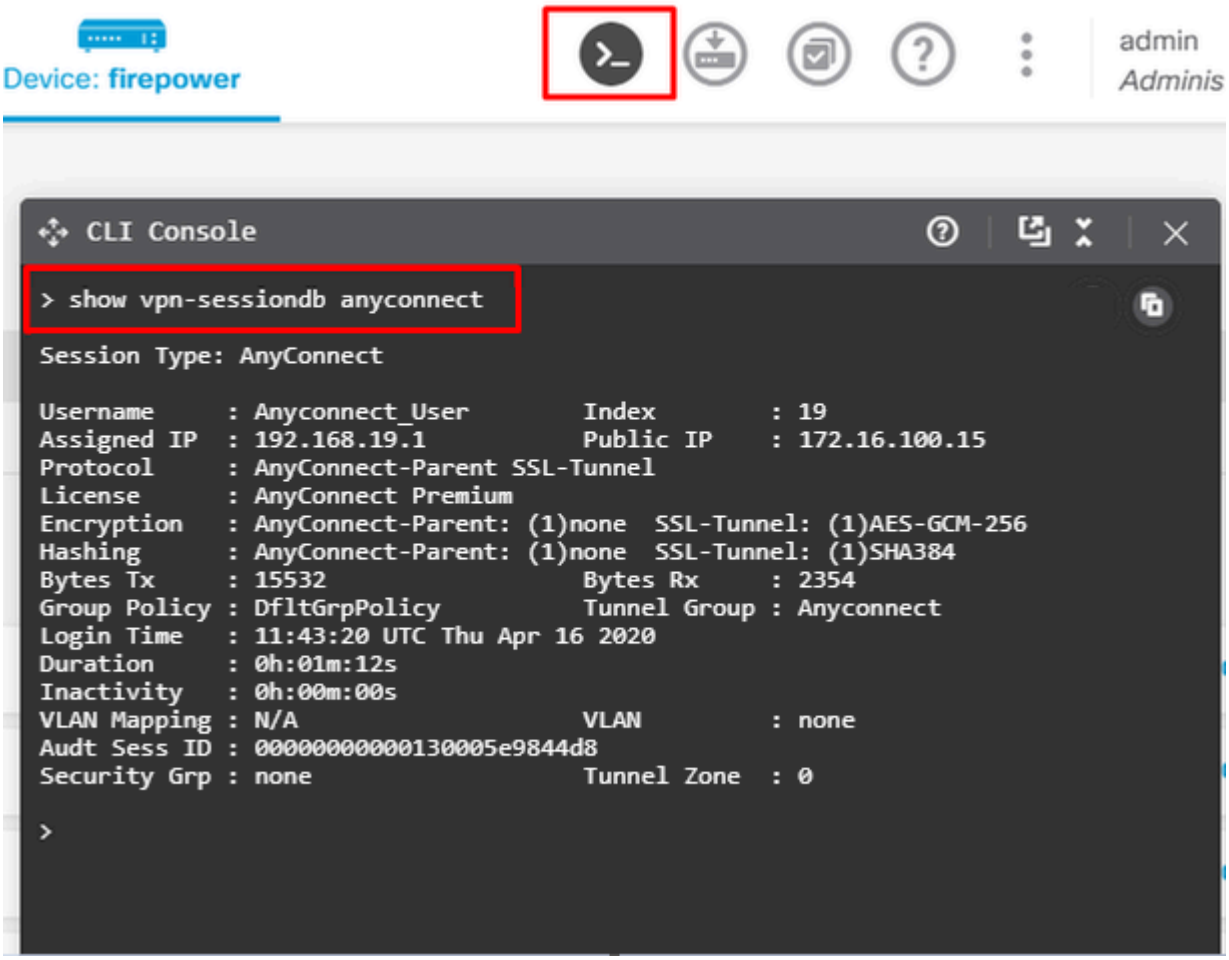
Use this section in order to confirm that your configuration works properly.

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.