Configure Anyconnect VPN Client on FTD: DHCP Server for Address Assignment

Contents

Introduction

This document provides a configuration example for Firepower Threat Defense (FTD) on version 6.4, that allows remote access VPN sessions to get an IP address assigned by a 3rd party Dynamic Host Configuration Protocol (DHCP) server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FTD
- Firepower Management Center (FMC).
- DHCP

Components Used

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

- FMC 6.5
- FTD 6.5
- Windows Server 2016

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, make sure that you understand the potential impact of any command.

Background information

This document will not describe the whole Remote Access configuration, just the required configuration in the FTD in order to change from local address pool to DHCP address assignment.

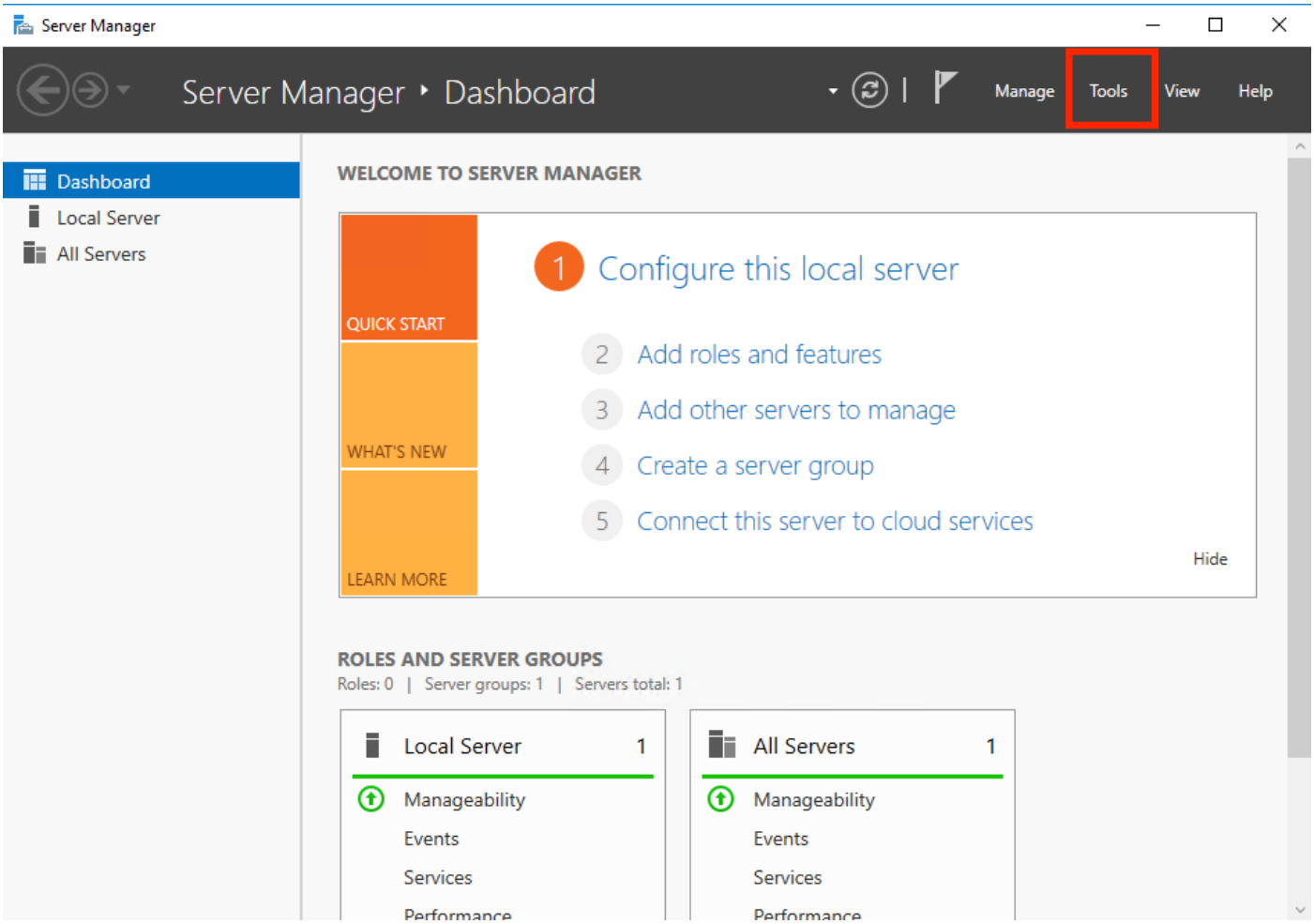
If you are looking for the Anyconnect configuration example document, please refer to "Configure AnyConnect VPN Client on FTD: Hairpining and NAT Exemption" document.

Configure

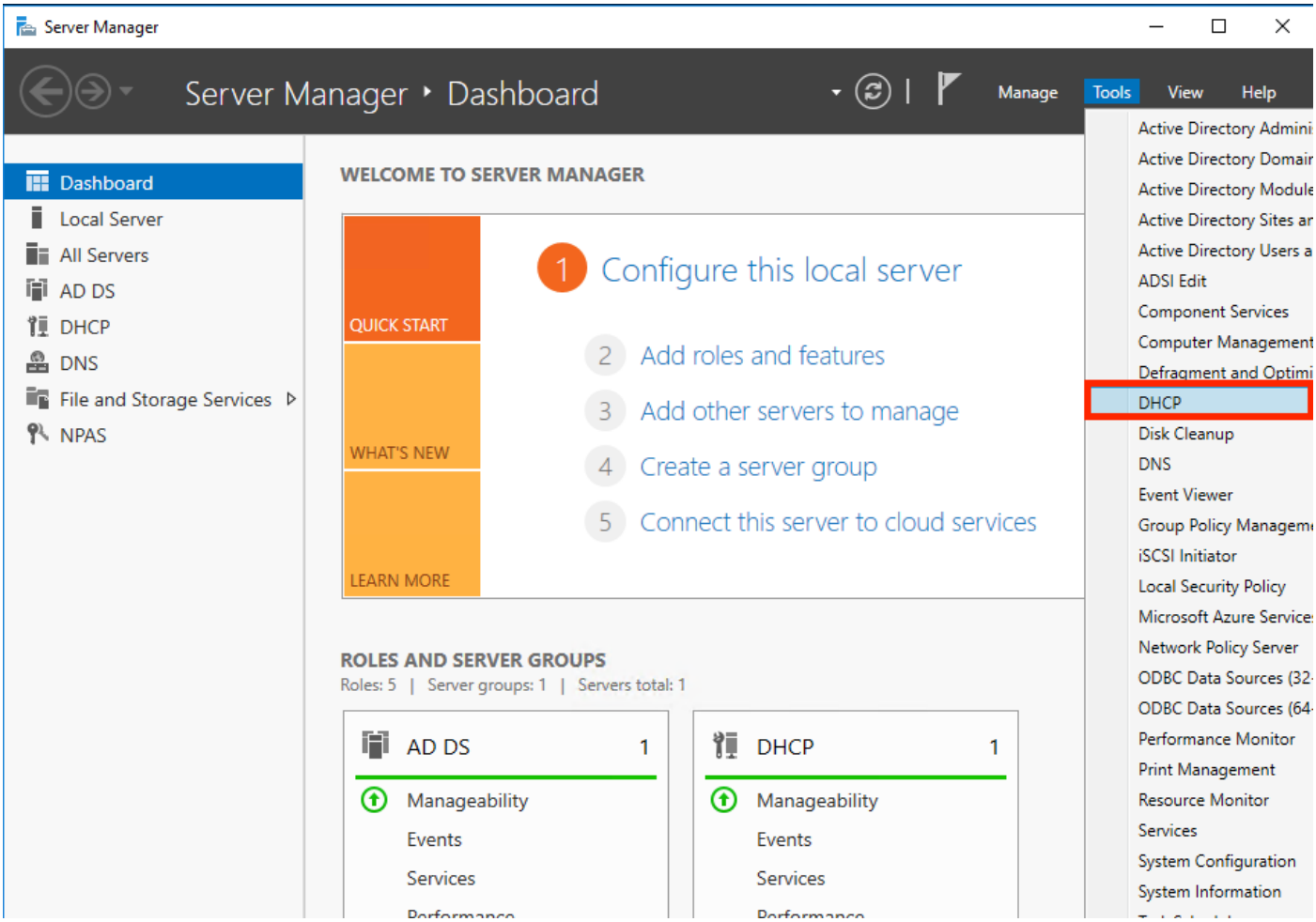
Step 1. Configure DHCP Scope in the DHCP Server

In this scenario, the DHCP server is located behind the FTD's inside interface.

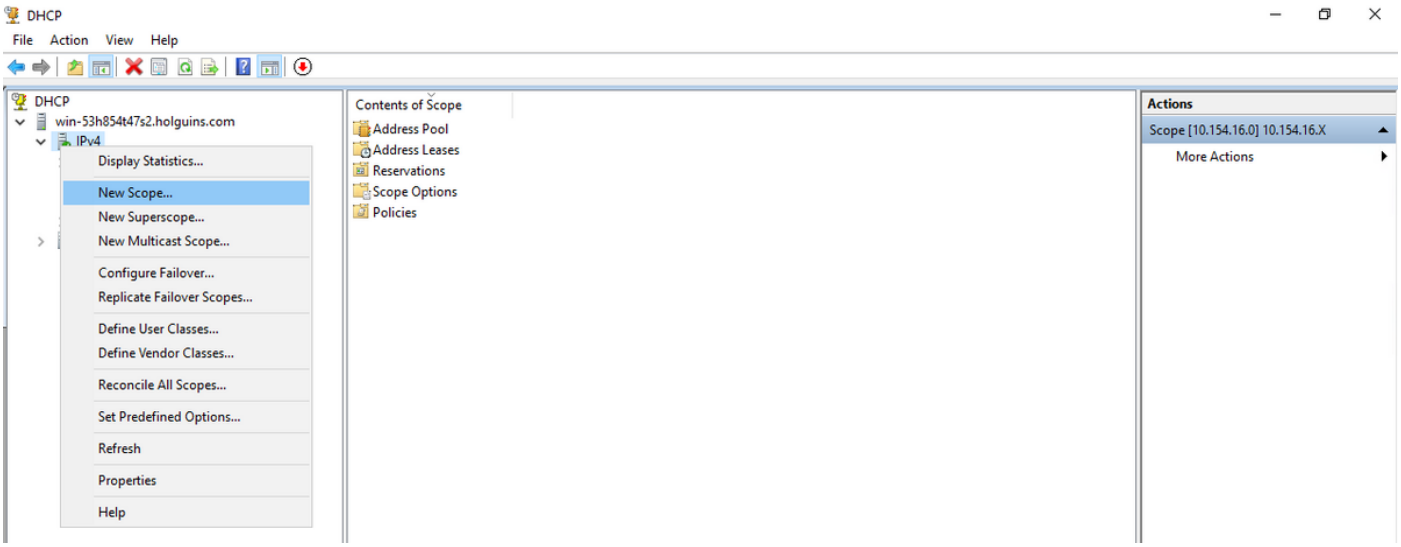
1. Open the Server Manager in the Windows Server and select **Tools** as shown in the image.



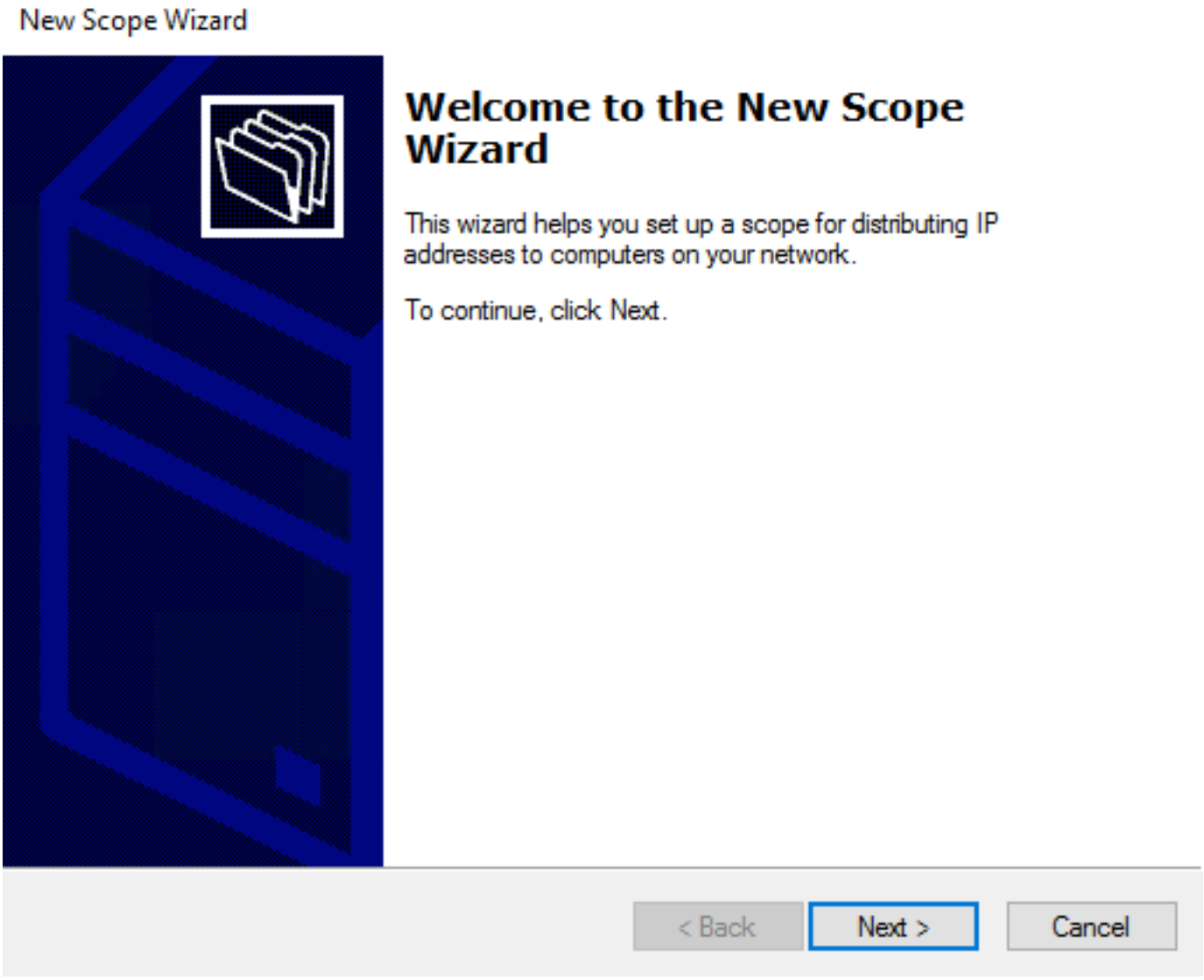
2. Select DHCP:



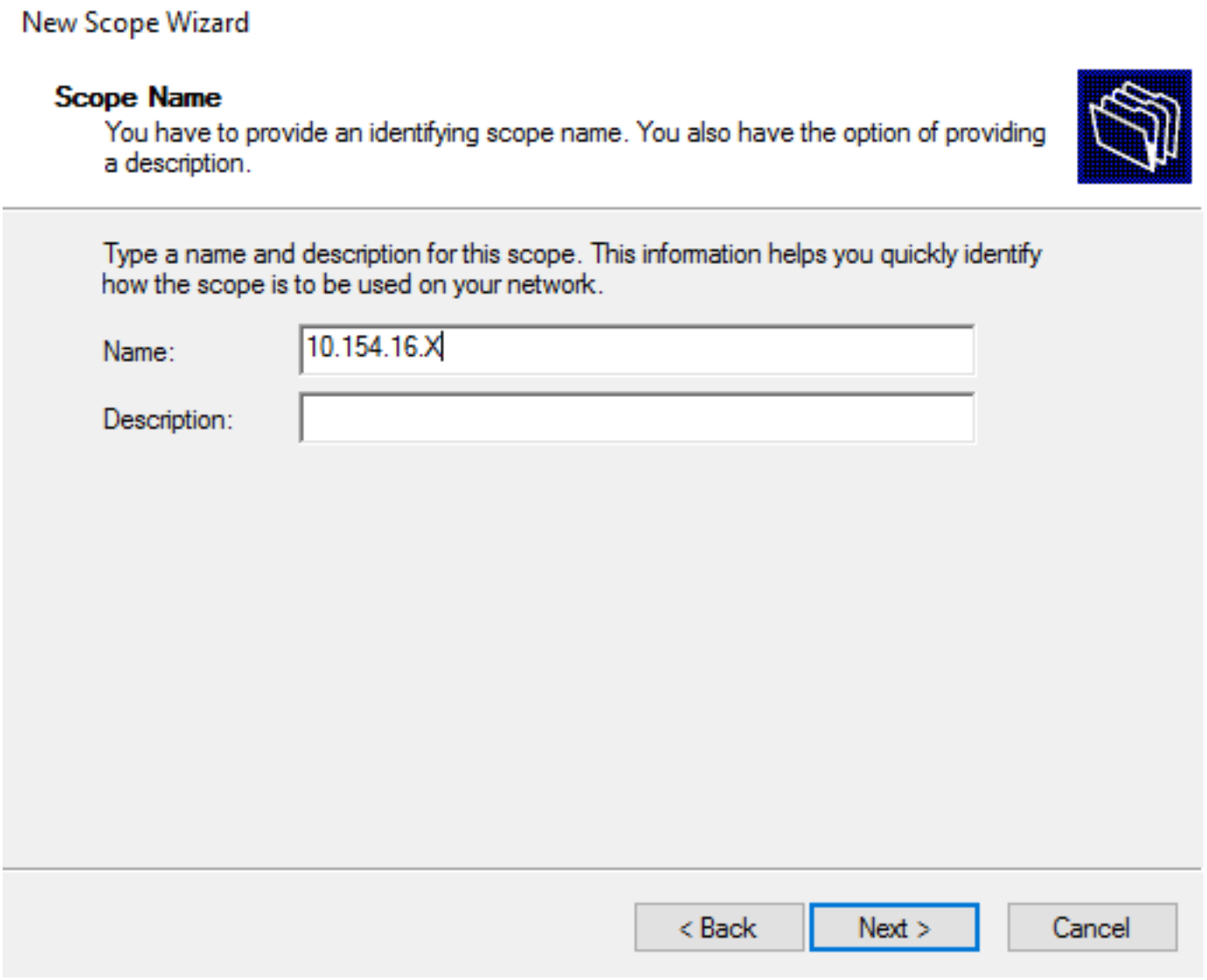
3. Select IPv4, right-click on it and select **New Scope** as shown in the image.



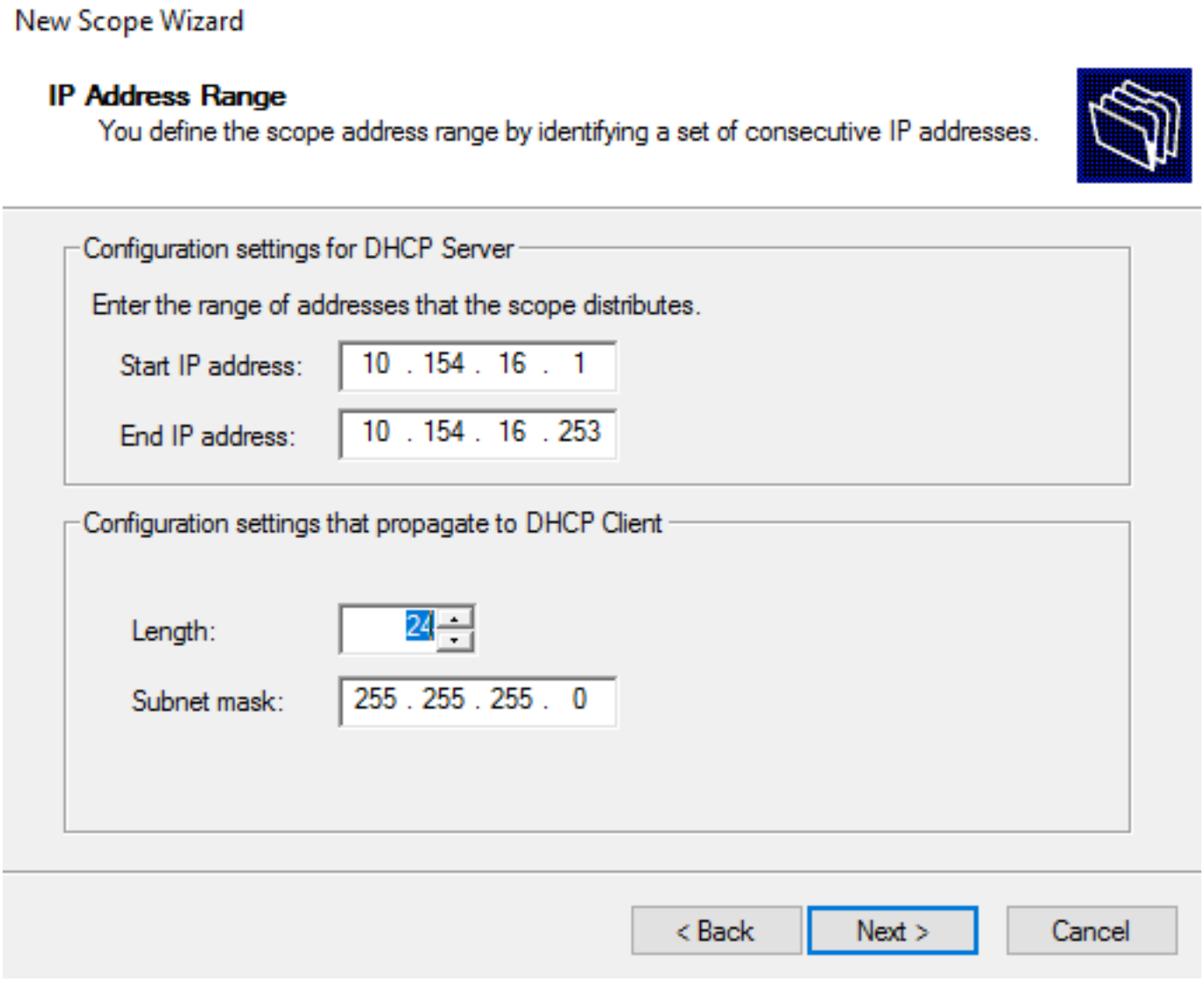
4. Follow the **Wizard** as shown in the image.



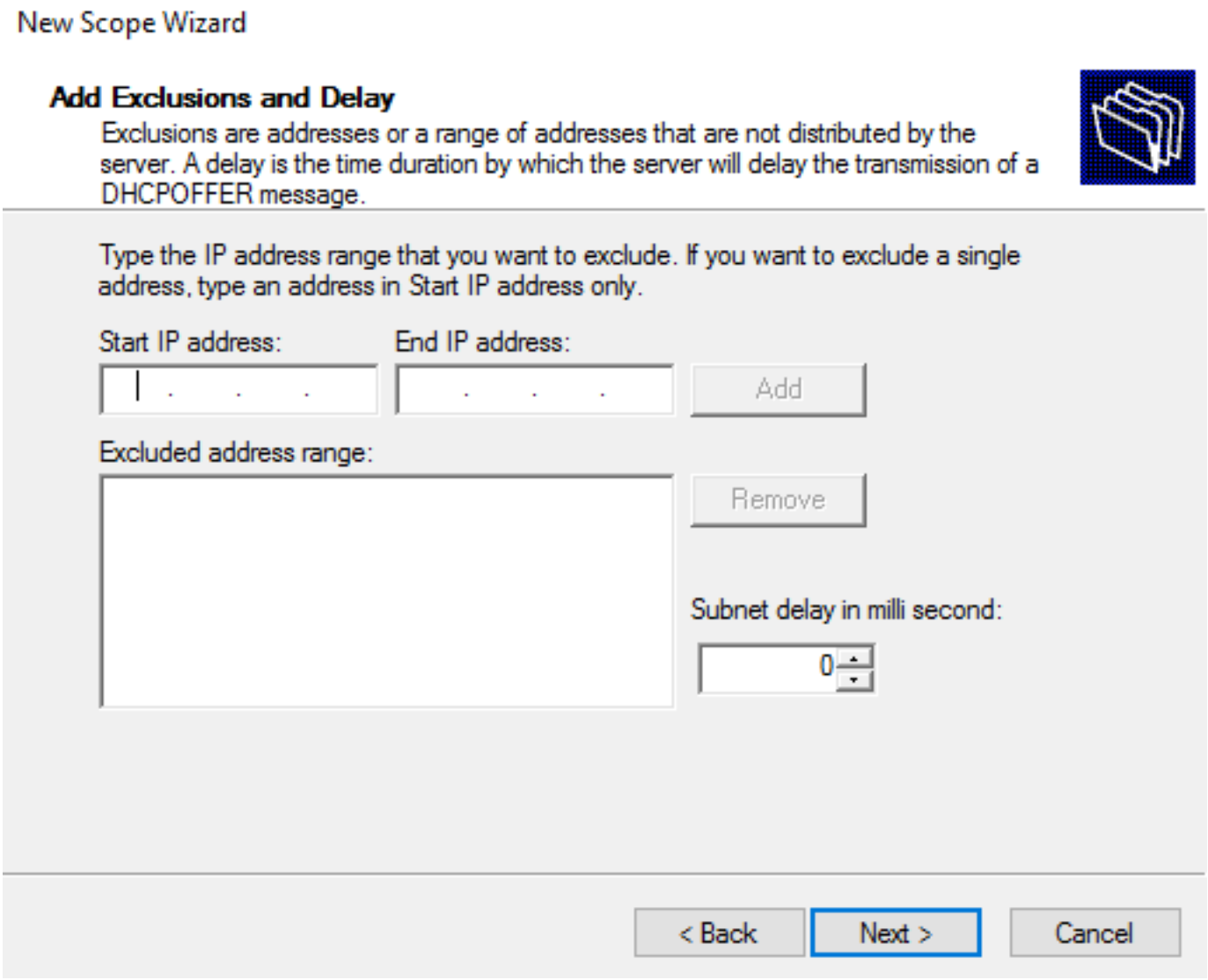
5. Assign a name to the scope as shown in the image.



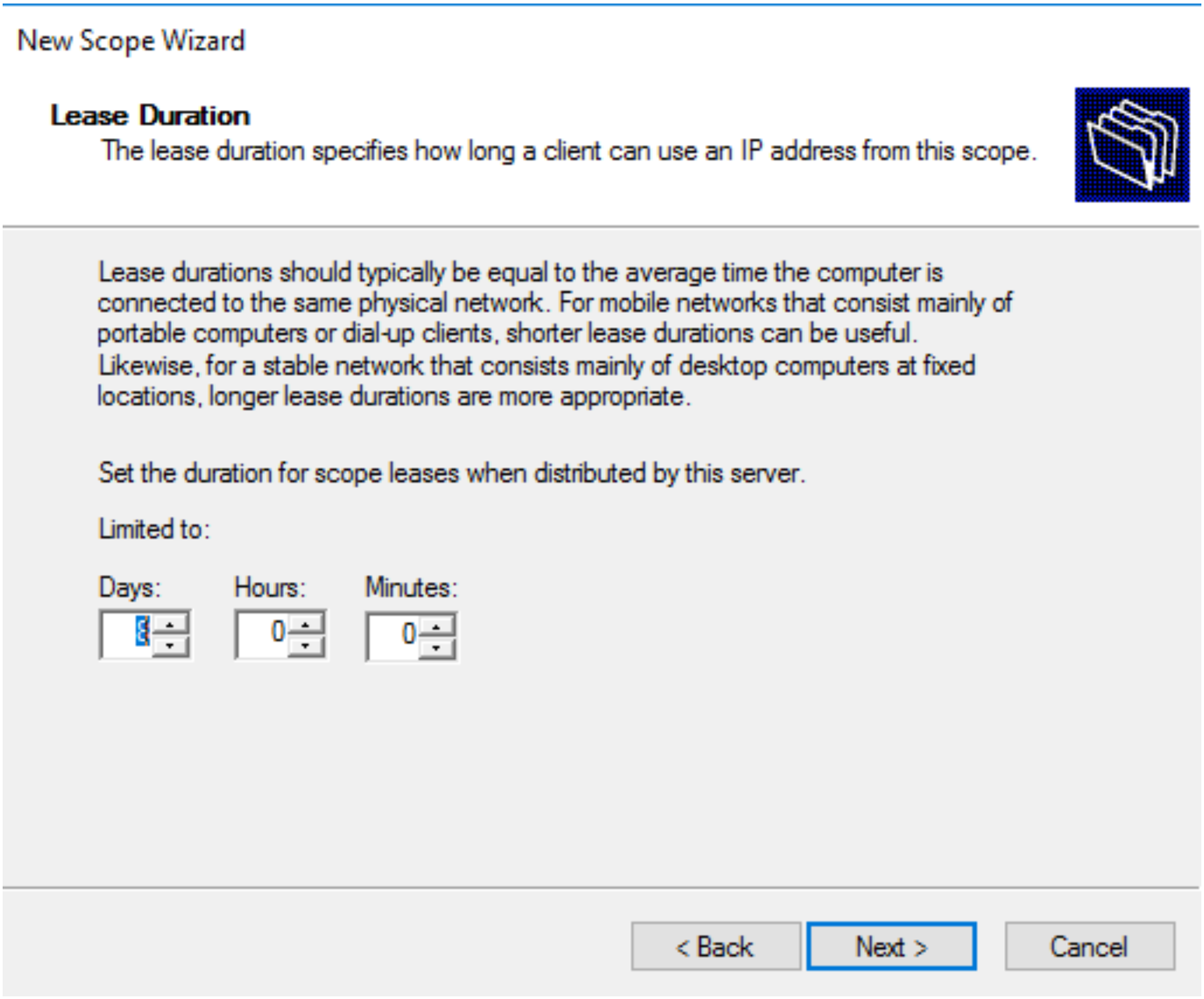
6. Configure the range of addresses as shown in the image.



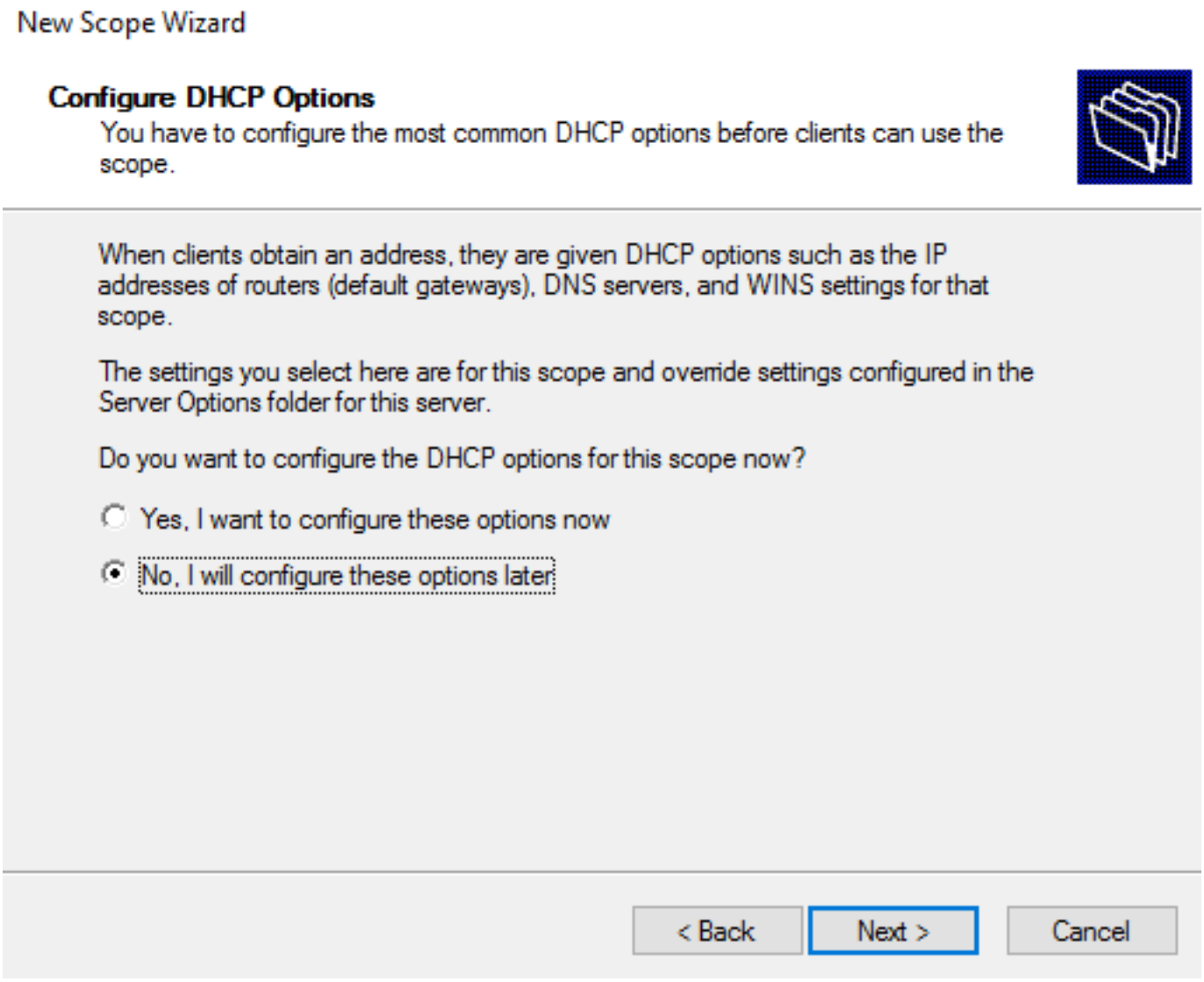
7. (Optional) Configure the exclusions as shown in the image.



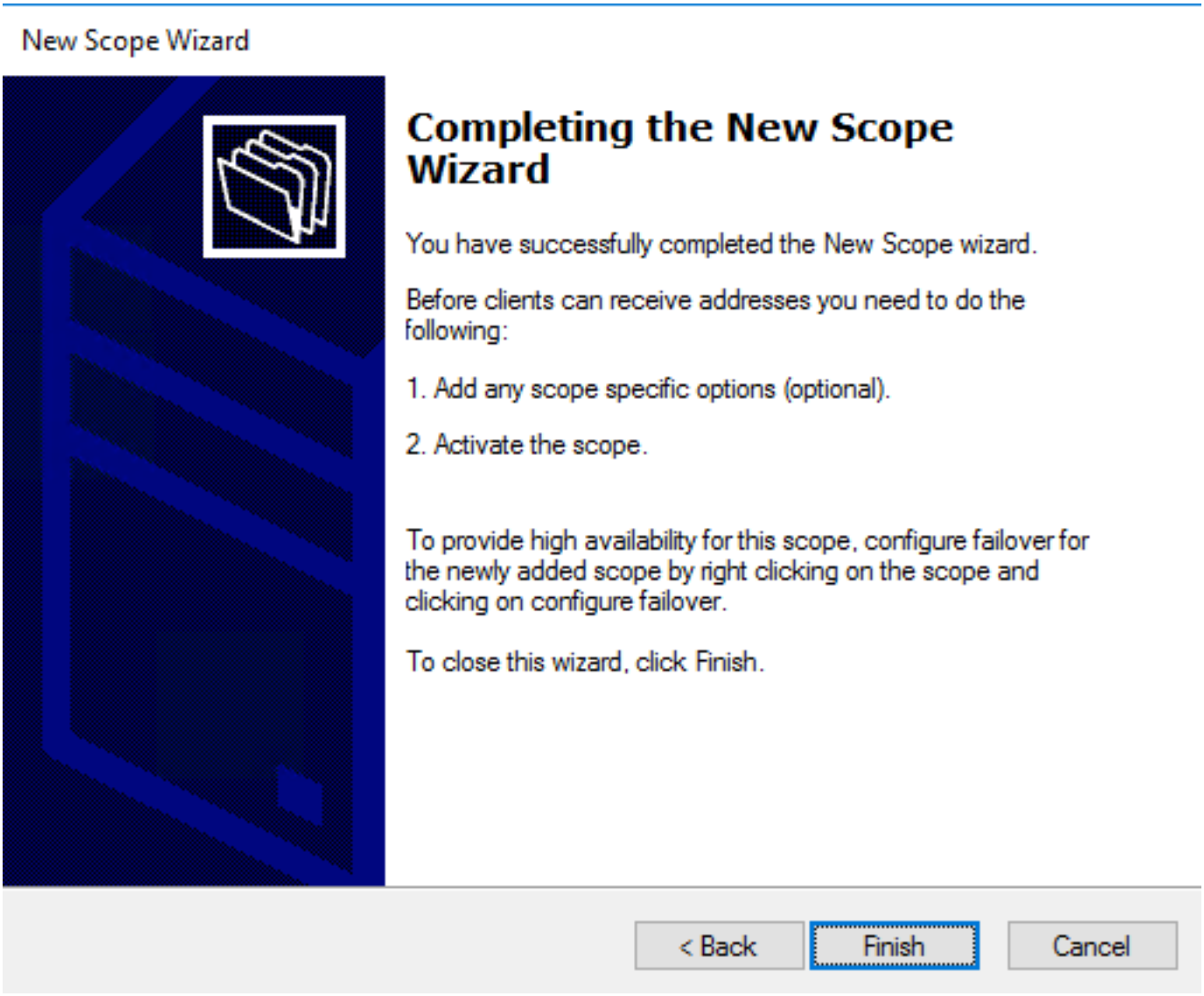
8. Configure **Lease Duration** as shown in the image.



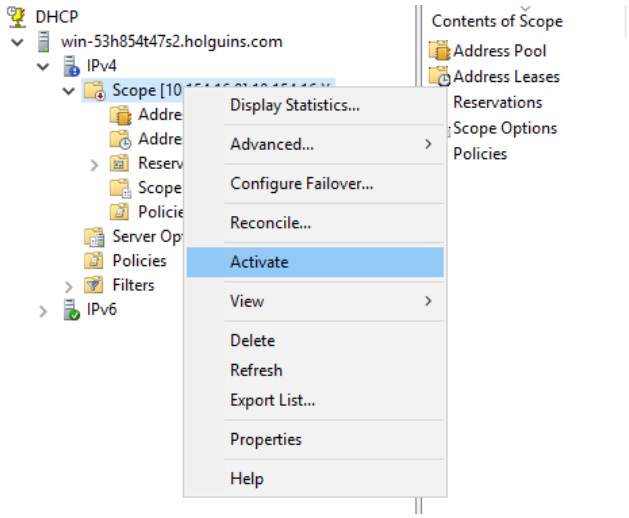
9. (Optional) Configure DHCP scope options:



10: Select **Finish** as shown in the image.



11: Right-click in the scope just created and select **Activate** as shown in the image.



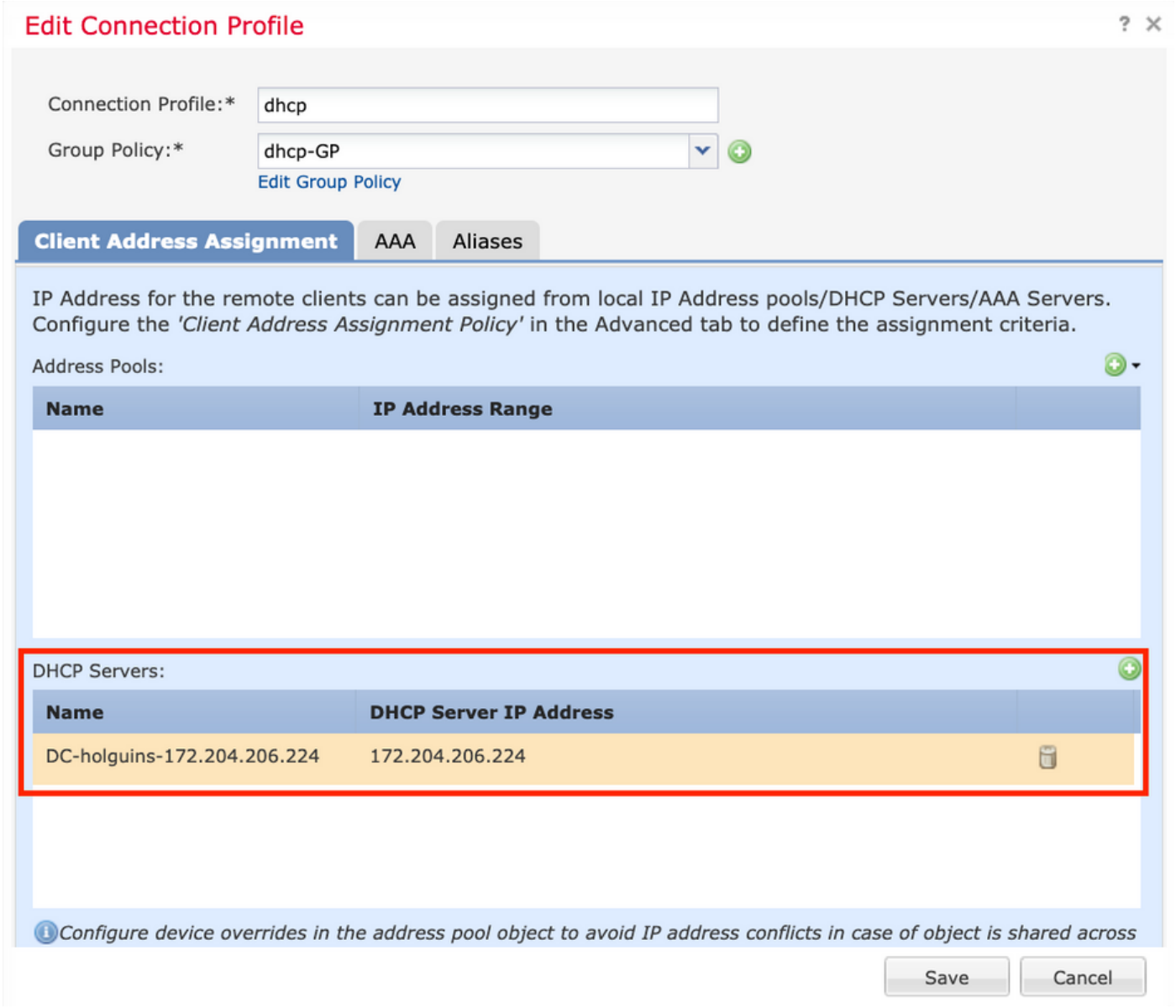
Step 2. Configure Anyconnect

Once the DHCP scope is configured and activated, the next procedure takes place in the FMC.

Step 2.1. Configure Connection Profile

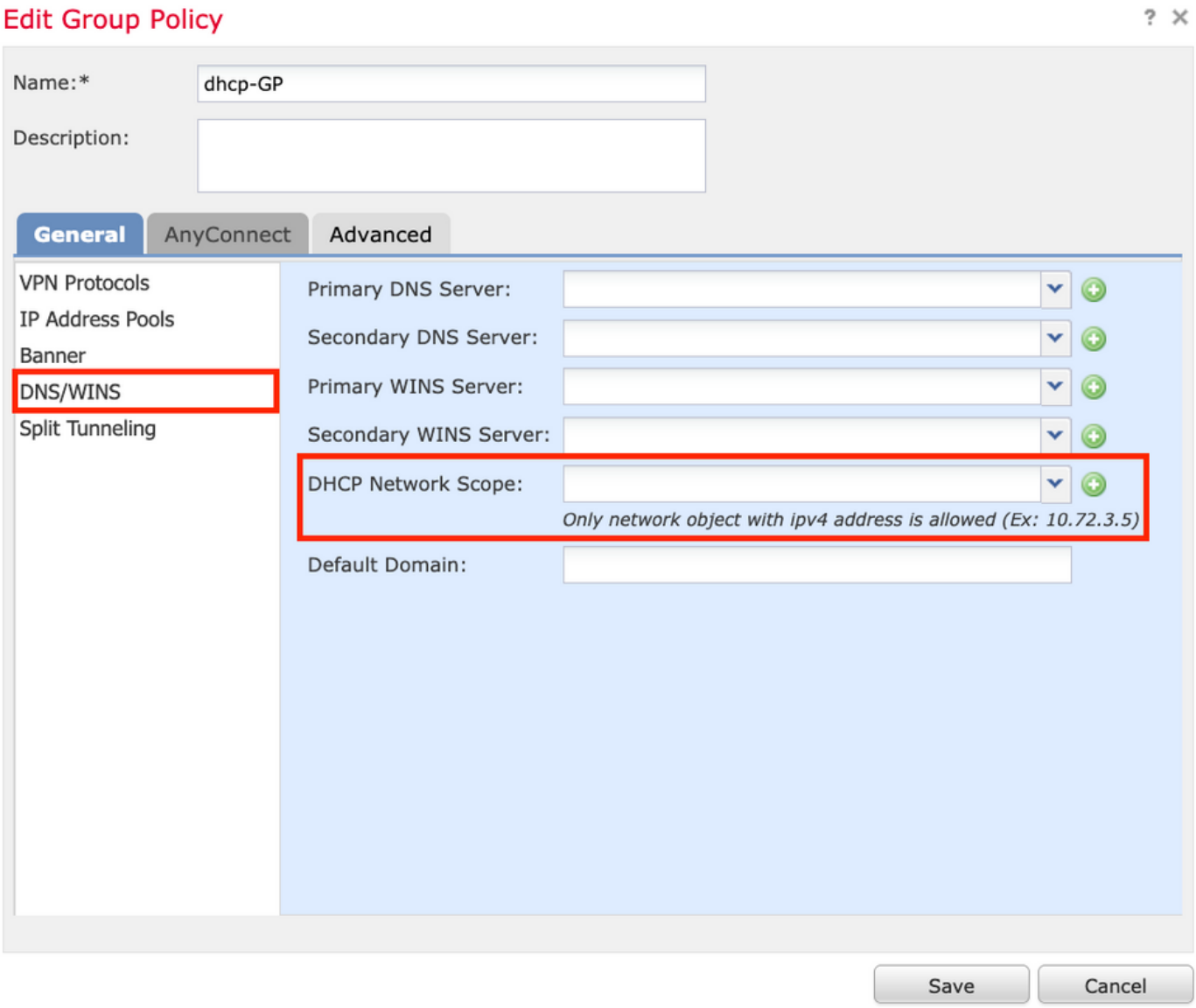
1. In the DHCP Servers section, select the symbol and create an object with the DHCP server's IP address.

2. Select the object as the DHCP server in order to request an IP address from as shown in the image.



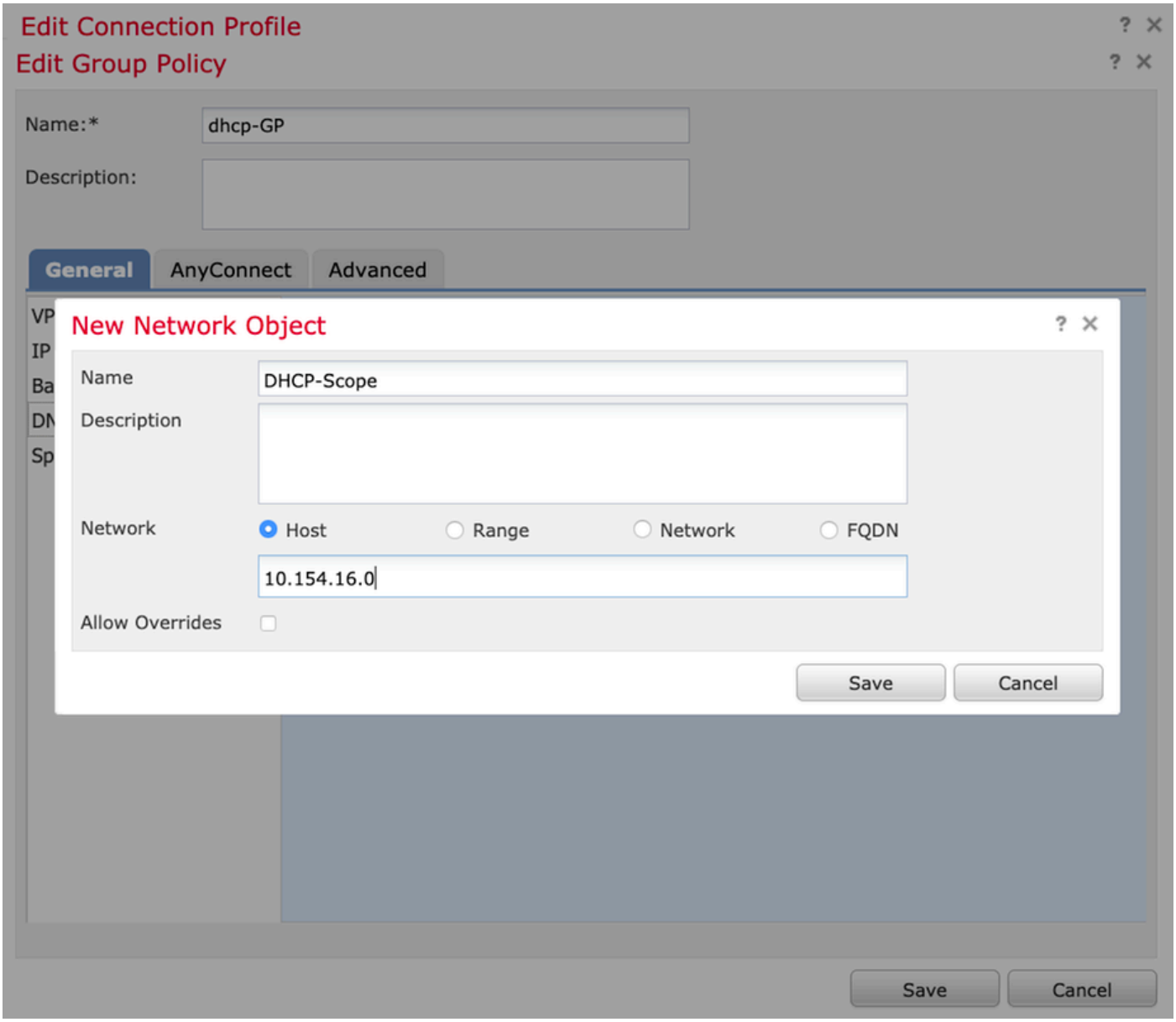
Step 2.2. Configure Group Policy

1. Inside the Group Policy menu, navigate to **General > DNS/WINS**, there is a **DHCP Network Scope** section as shown in the image.

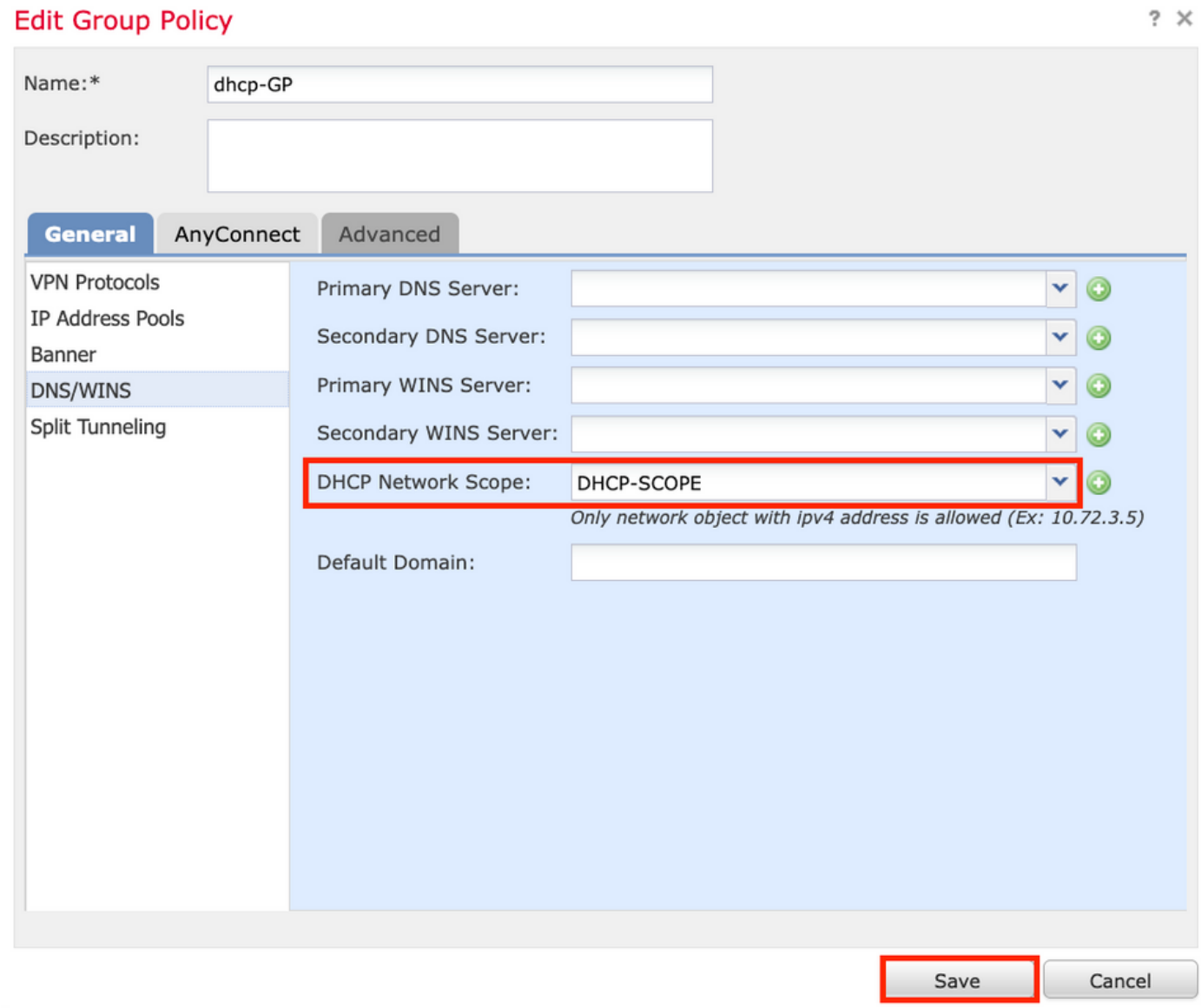


2. Create a new object, this must have the same network scope that the DHCP server has.

Note: This must be a host object, not a subnet.

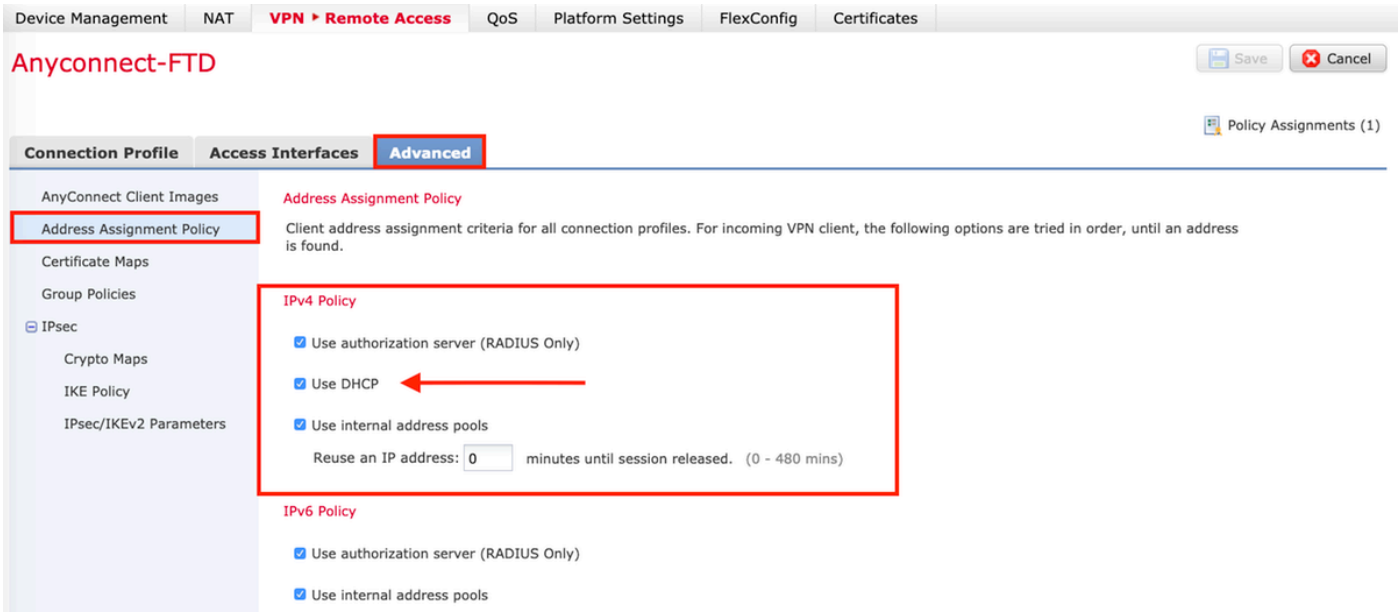


3. Select the DHCP scope object and select **Save** as shown in the image.



Step 2.3. Configure the Address Assignment Policy

1. Navigate to **Advanced** > **Address Assignment Policy** and ensure the **Use DHCP** option is toggled as shown in the image.

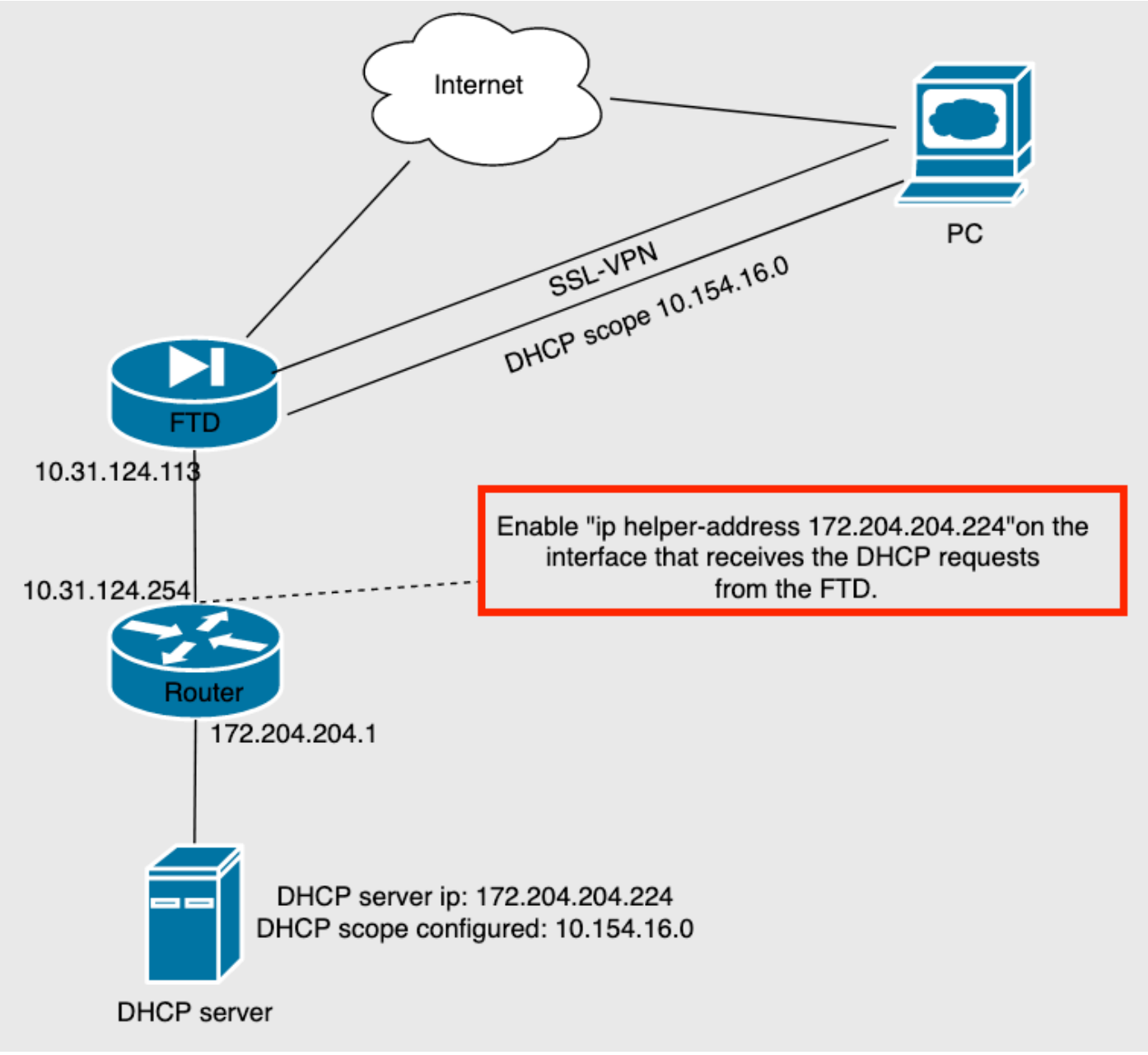


2. Save the changes and deploy the configuration.

IP Helper Scenario

When the DHCP server is behind another router in the Local Area Network (LAN), an "IP helper" is needed in order to forward the requests to the DHCP Server.

As shown in the image, a topology illustrates the scenario and the necessary changes in the network.



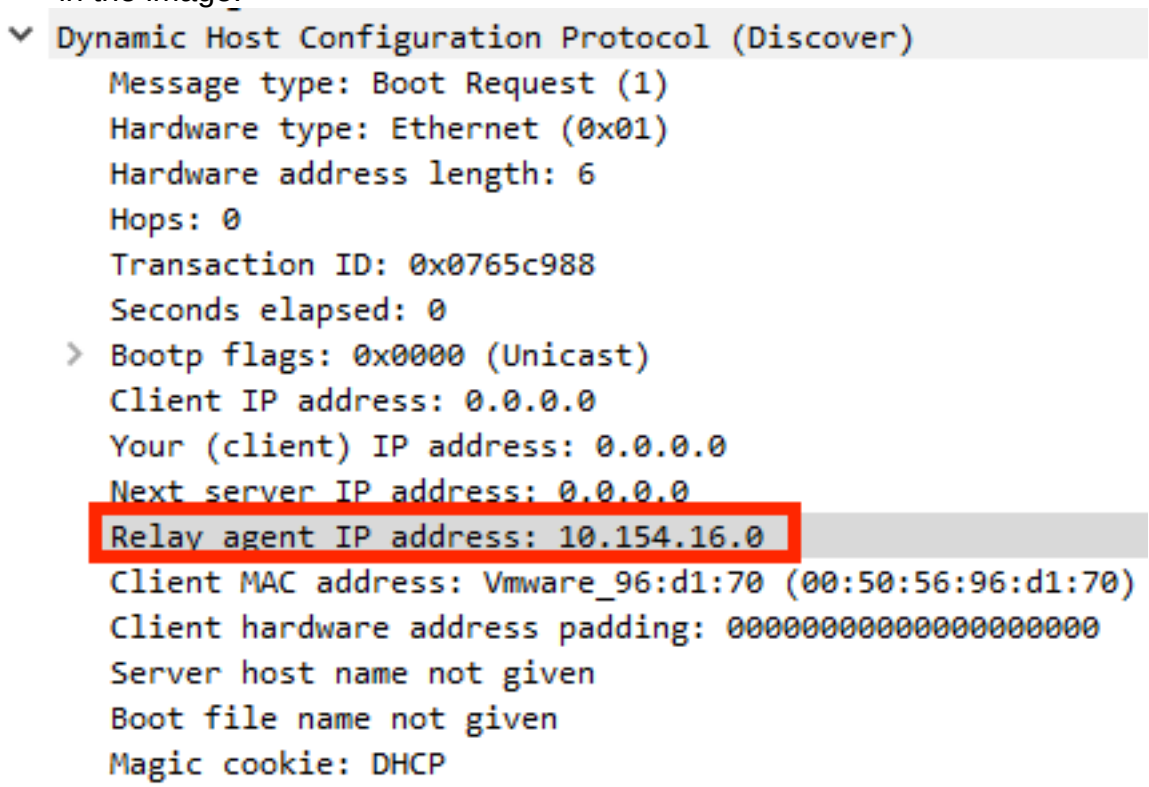
Verify

Use this section to confirm that your configuration works properly.

This section describes the DHCP packets exchanged between the FTD and the DHCP server.

- Discovery: This is a unicast packet sent from the FTD's inside interface to the DHCP Server.

In the payload, a **Relay agent IP address** specifies the scope of the DHCP server as shown in the image.



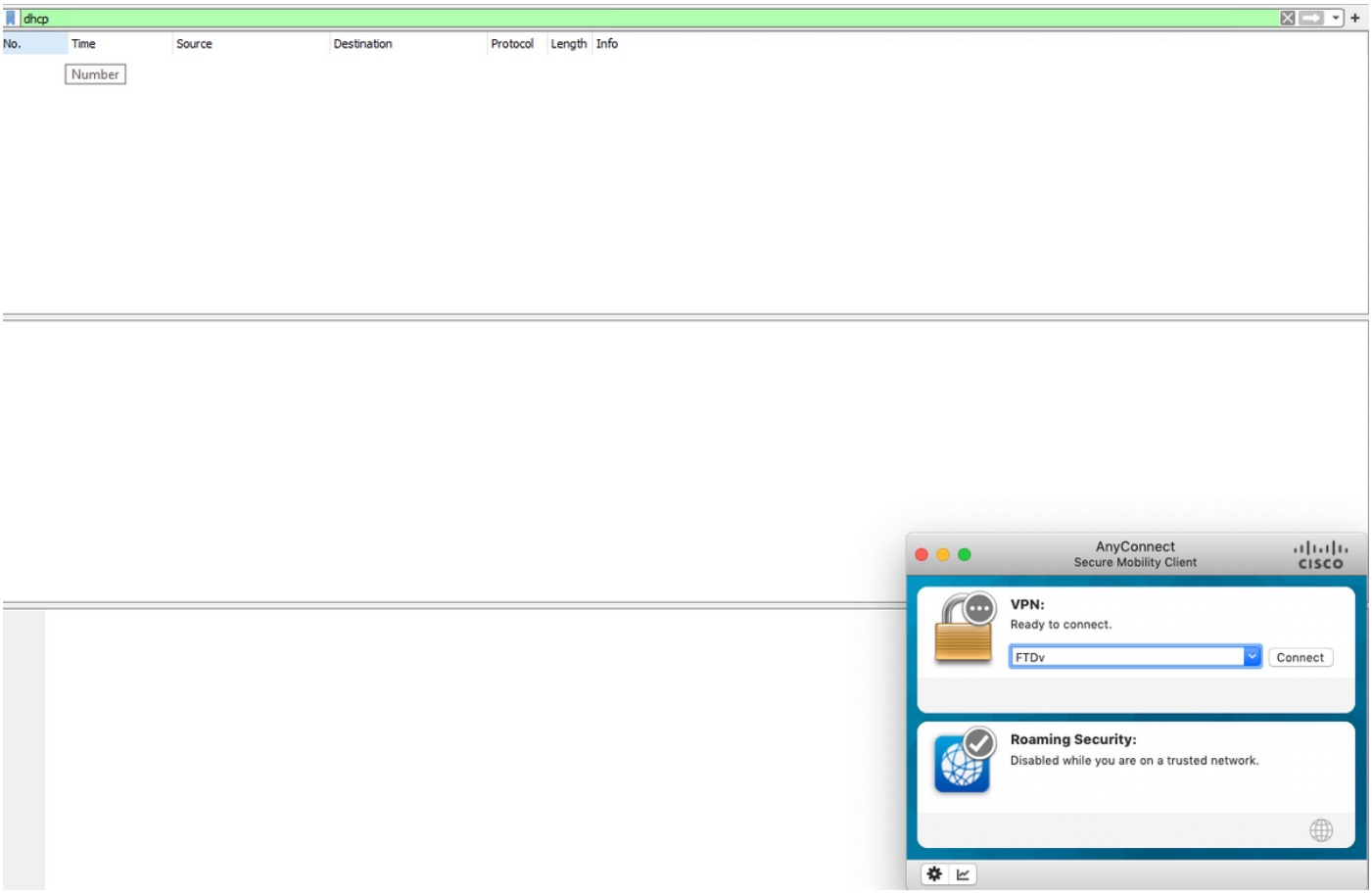
- Offer: This packet is a response from the DHCP server, this comes with the DHCP server source and the destination of the DHCP Scope in the FTD.
- Request: This is a unicast packet sent from FTD's inside interface to the DHCP Server.
- ACK: This packet is a response from the DHCP server, this comes with the DHCP server source and the destination of the DHCP Scope in the FTD.

Troubleshoot

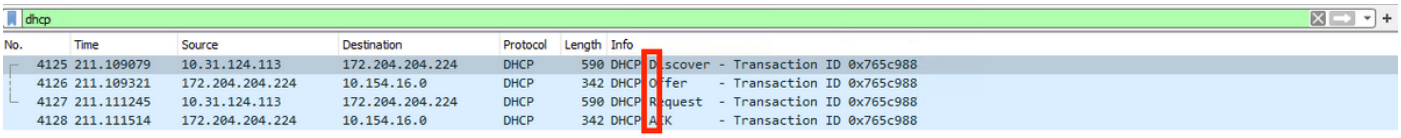
This section provides information you can use to troubleshoot your configuration.

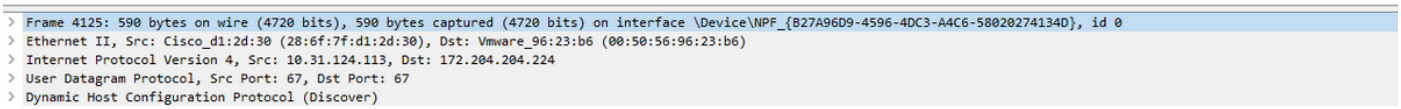
Step 1. Download and enable wireshark in the DHCP server.

Step 2. Apply DHCP as the capture filter as shown in the image.



Step 3. Log in to Anyconnect, the DHCP negotiation should be seen as shown in the image.





Related Information

- This video provides the configuration example for FTD, that allows remote access VPN sessions to get an IP address assigned by a 3rd party DHCP server.
- **Technical Support & Documentation - Cisco Systems**