

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

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background information](#)

[Configure](#)

[Step 1. Configure DHCP Scope in the DHCP Server](#)

[Step 2. Configure Anyconnect](#)

[Step 2.1. Configure Connection Profile](#)

[Step 2.2. Configure Group Policy](#)

[Step 2.3. Configure the Address Assignment Policy](#)

[IP Helper Scenario](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

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.

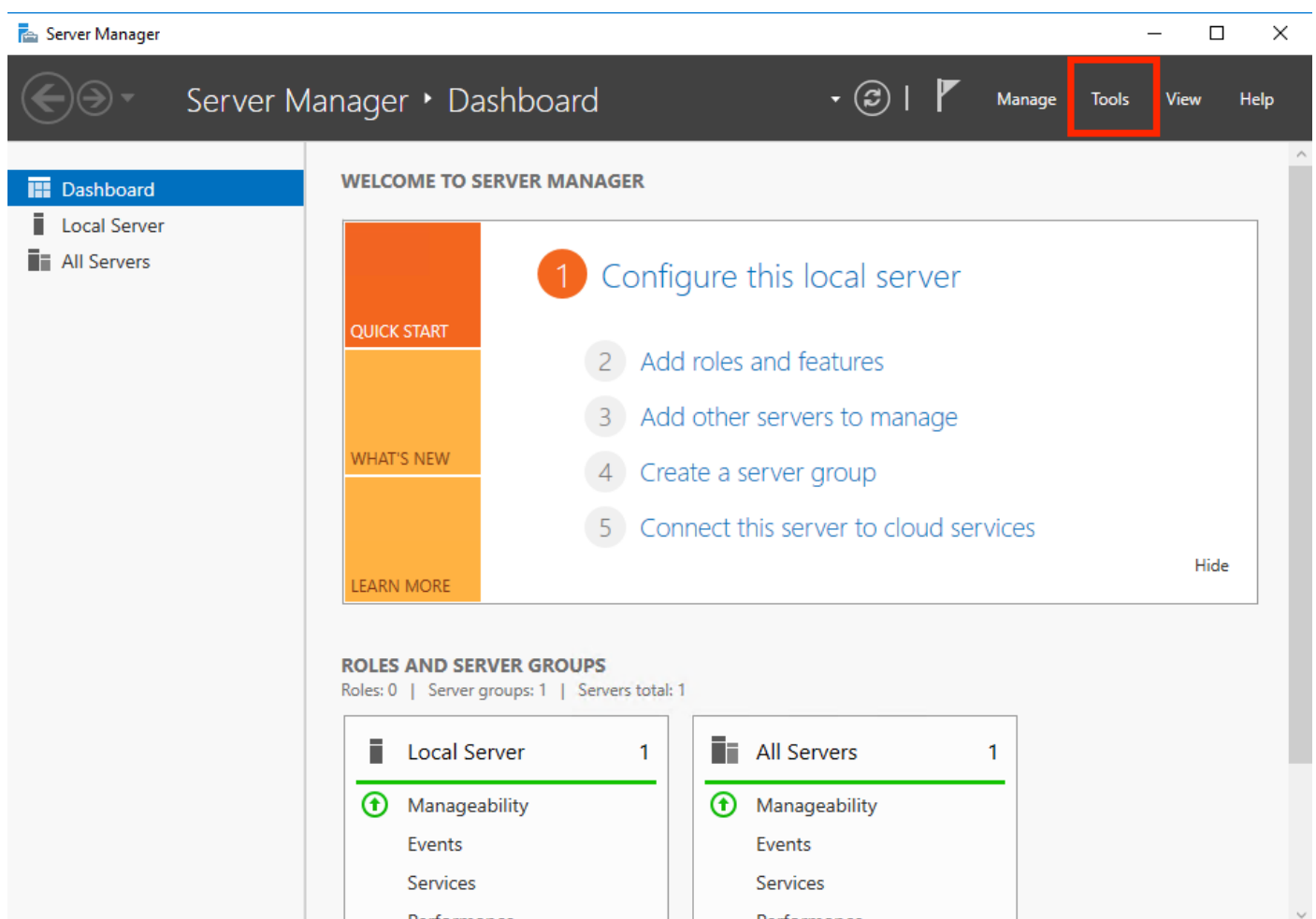
If you are looking for the Anyconnect configuration example document, please refer to "Configure AnyConnect VPN Client on FTD: Hairpinning and NAT Exemption" document.

Configure

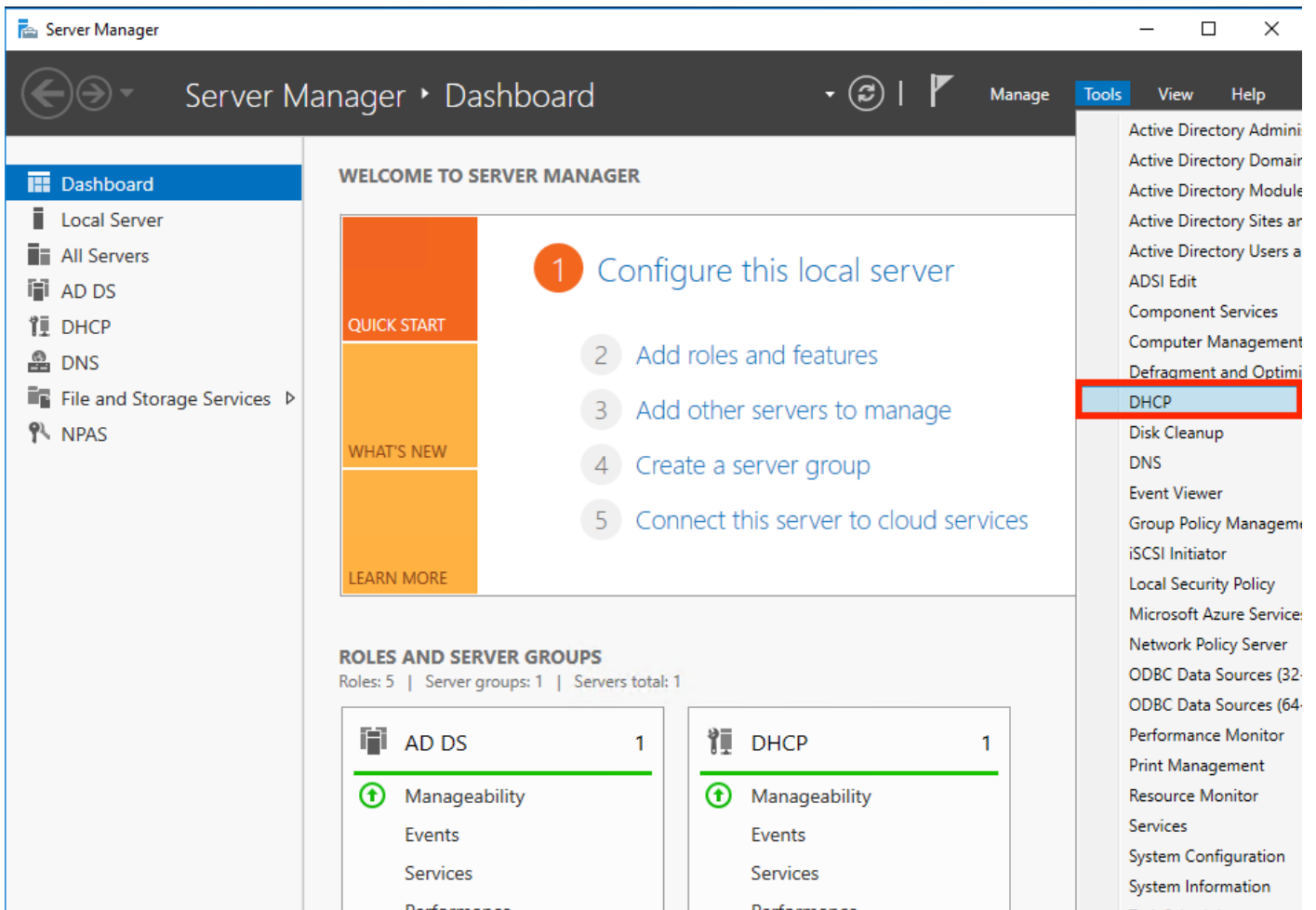
Step 1. Configure DHCP Scope in the DHCP Server

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

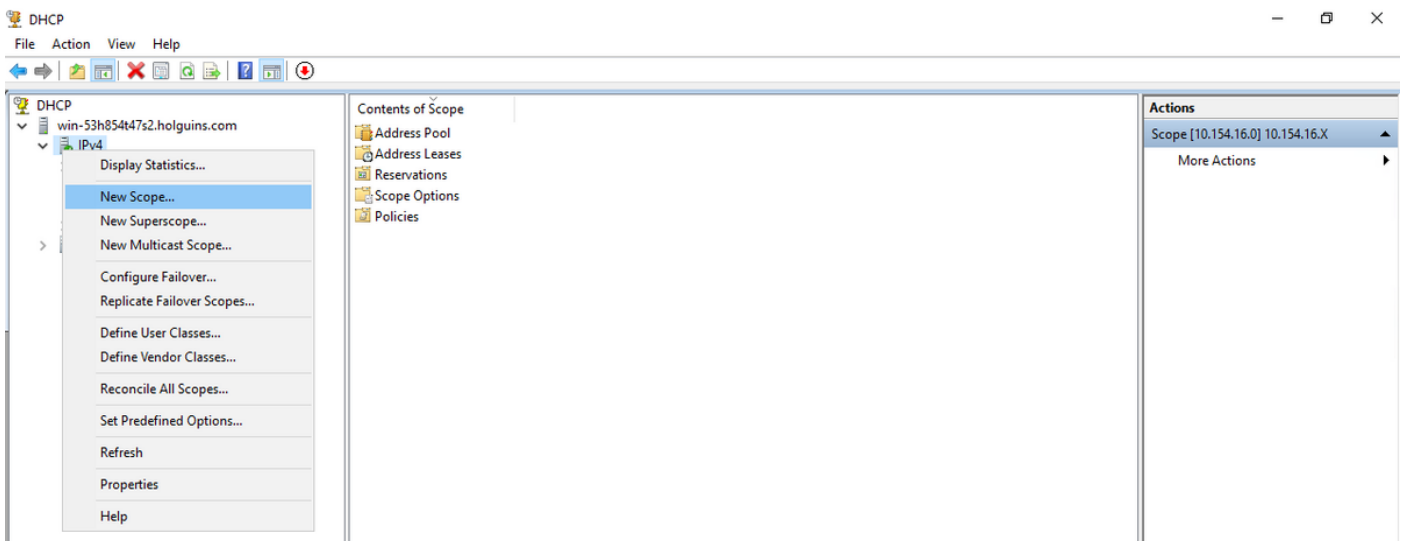
1. Open the Server Manager in the Windows Server and select **Tools** as shown in the image.



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.

New Scope Wizard



Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

< Back

Next >

Cancel

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

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back

Next >

Cancel

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

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back Next > Cancel

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

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Remove

Subnet delay in milli second:

< Back

Next >

Cancel

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

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back

Next >

Cancel

9. (Optional) Configure DHCP scope options:

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

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

New Scope Wizard



Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

Before clients can receive addresses you need to do the following:

1. Add any scope specific options (optional).
2. Activate the scope.

To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

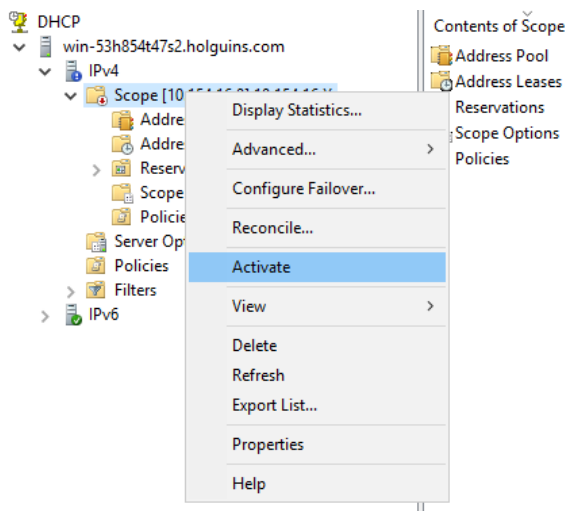
To close this wizard, click Finish.

< Back

Finish

Cancel

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.

Edit Connection Profile ? x

Connection Profile:*

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

Client Address Assignment AAA Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the '*Client Address Assignment Policy*' in the Advanced tab to define the assignment criteria.

Address Pools: + v

Name	IP Address Range
------	------------------

DHCP Servers: +

Name	DHCP Server IP Address
DC-holguins-172.204.206.224	172.204.206.224 🗑

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

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.

Edit Group Policy



Name: *

Description:

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

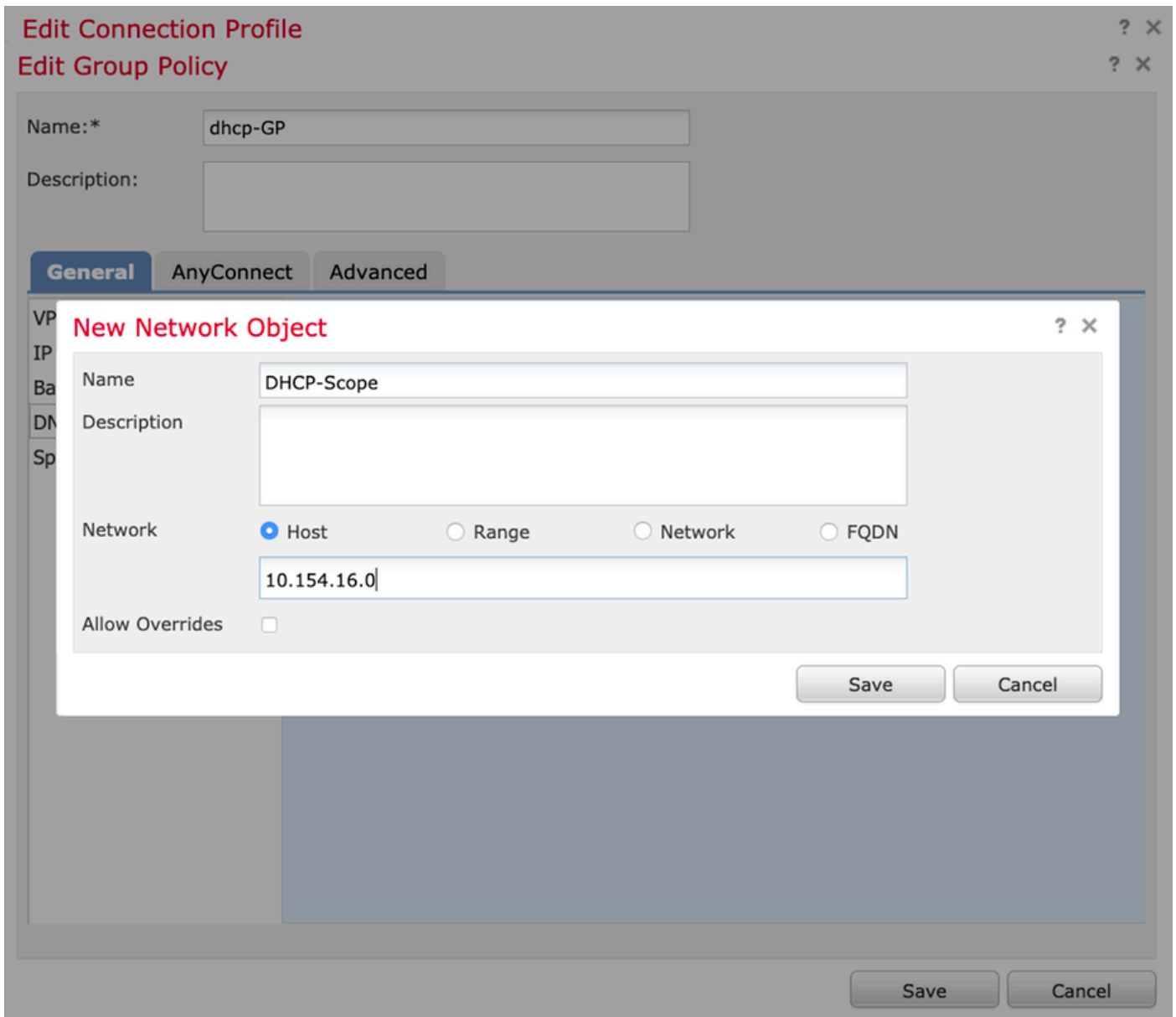
Secondary WINS Server:

DHCP Network Scope:
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

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.

Edit Group Policy



Name:*

Description:

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

Primary DNS Server: +

Secondary DNS Server: +

Primary WINS Server: +

Secondary WINS Server: +

DHCP Network Scope: +

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Save Cancel

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.

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

Anyconnect-FTD

Policy Assignments (1)

Connection Profile **Access Interfaces** **Advanced**

AnyConnect Client Images
Address Assignment Policy
Certificate Maps
Group Policies
IPsec
Crypto Maps
IKE Policy
IPsec/IKEV2 Parameters

Address Assignment Policy
Client address assignment criteria for all connection profiles. For incoming VPN client, the following options are tried in order, until an address is found.

IPv4 Policy

- Use authorization server (RADIUS Only)
- Use DHCP** ←
- Use internal address pools

Reuse an IP address: minutes until session released. (0 - 480 mins)

IPv6 Policy

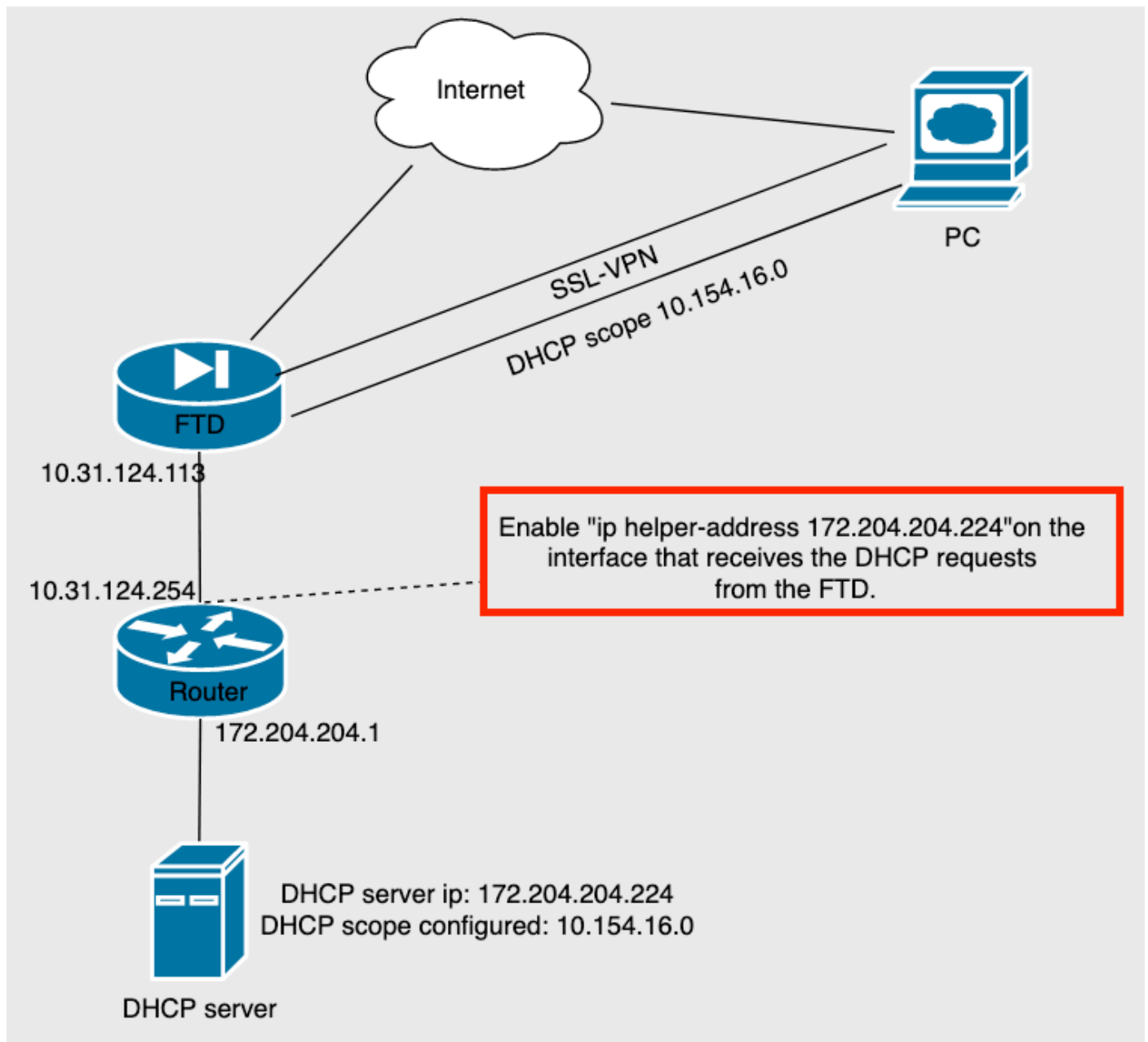
- Use authorization server (RADIUS Only)
- Use internal address pools

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.

```
Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x0765c988
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 10.154.16.0
  Client MAC address: Vmware_96:d1:70 (00:50:56:96:d1:70)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
```

- 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.

No.	Time	Source	Destination	Protocol	Length	Info
						Number

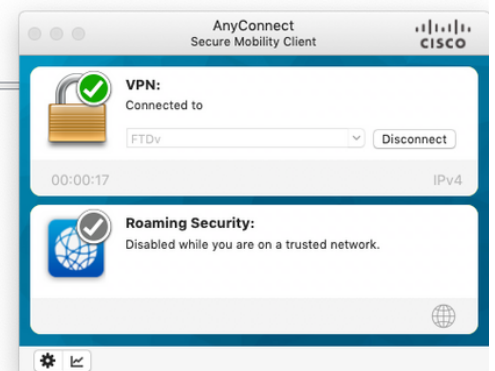


Step 3. Log in to Anyconnect, the DHCP negotiation should be seen as shown in the image.

No.	Time	Source	Destination	Protocol	Length	Info
4125	211.109079	10.31.124.113	172.204.204.224	DHCP	590	DHCP Discover - Transaction ID 0x765c988
4126	211.109321	172.204.204.224	10.154.16.0	DHCP	342	DHCP Offer - Transaction ID 0x765c988
4127	211.111245	10.31.124.113	172.204.204.224	DHCP	590	DHCP Request - Transaction ID 0x765c988
4128	211.111514	172.204.204.224	10.154.16.0	DHCP	342	DHCP ACK - Transaction ID 0x765c988

```
> Frame 4125: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{B27A96D9-4596-4DC3-A4C6-58020274134D}, id 0
> Ethernet II, Src: Cisco_d1:2d:30 (28:6f:7f:d1:2d:30), Dst: Vmware_96:23:b6 (00:50:56:96:23:b6)
> Internet Protocol Version 4, Src: 10.31.124.113, Dst: 172.204.204.224
> User Datagram Protocol, Src Port: 67, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

0000	00	50	56	96	23	b6	28	6f	7f	d1	2d	30	08	00	45	00	..PV.#-(o---0--E
0010	02	40	1f	99	00	00	00	11	18	d7	0a	1f	7c	71	ac	cc	@..... q-
0020	cc	e0	00	43	00	43	02	2c	cb	e4	01	01	06	00	07	65	..C.C.,.....e
0030	c9	88	00	00	00	00	00	00	00	00	00	00	00	00	00	00P.V.-p...
0040	00	00	0a	9a	10	00	00	50	56	96	d1	70	00	00	00	00
0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00b0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00c0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00d0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00e0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00f0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00



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](#)