

# AnyConnect VPN-client op FTD configureren DHCP-server voor adrestoewijzing

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Stap 1. Configureer de DHCP-werkruimte in de DHCP-server](#)

[Stap 2. Steekweg](#)

[Stap 2.1. Configuratieprofiel](#)

[Stap 2.2. Groepsbeleid configureren](#)

[Stap 2.3. Het beleid voor adrestoewijzing configureren](#)

[IP-Helper-scenario](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document biedt een configuratievoorbeeld voor Firepower Threat Defense (FTD) op versie 6.4, waardoor VPN-sessies op afstand een IP-adres kunnen verkrijgen dat is toegewezen door een DHCP-server van 3rd party Dynamic Host Configuration Protocol (DHCP).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

### Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- MC65,5
- FTD 6.5
- Windows Server 2016

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Achtergrondinformatie

Dit document beschrijft niet de hele configuratie van de Externe Toegang, alleen de gewenste configuratie in het FTD om van lokale adrestoewijzing naar DHCP-adrestoewijzing te veranderen.

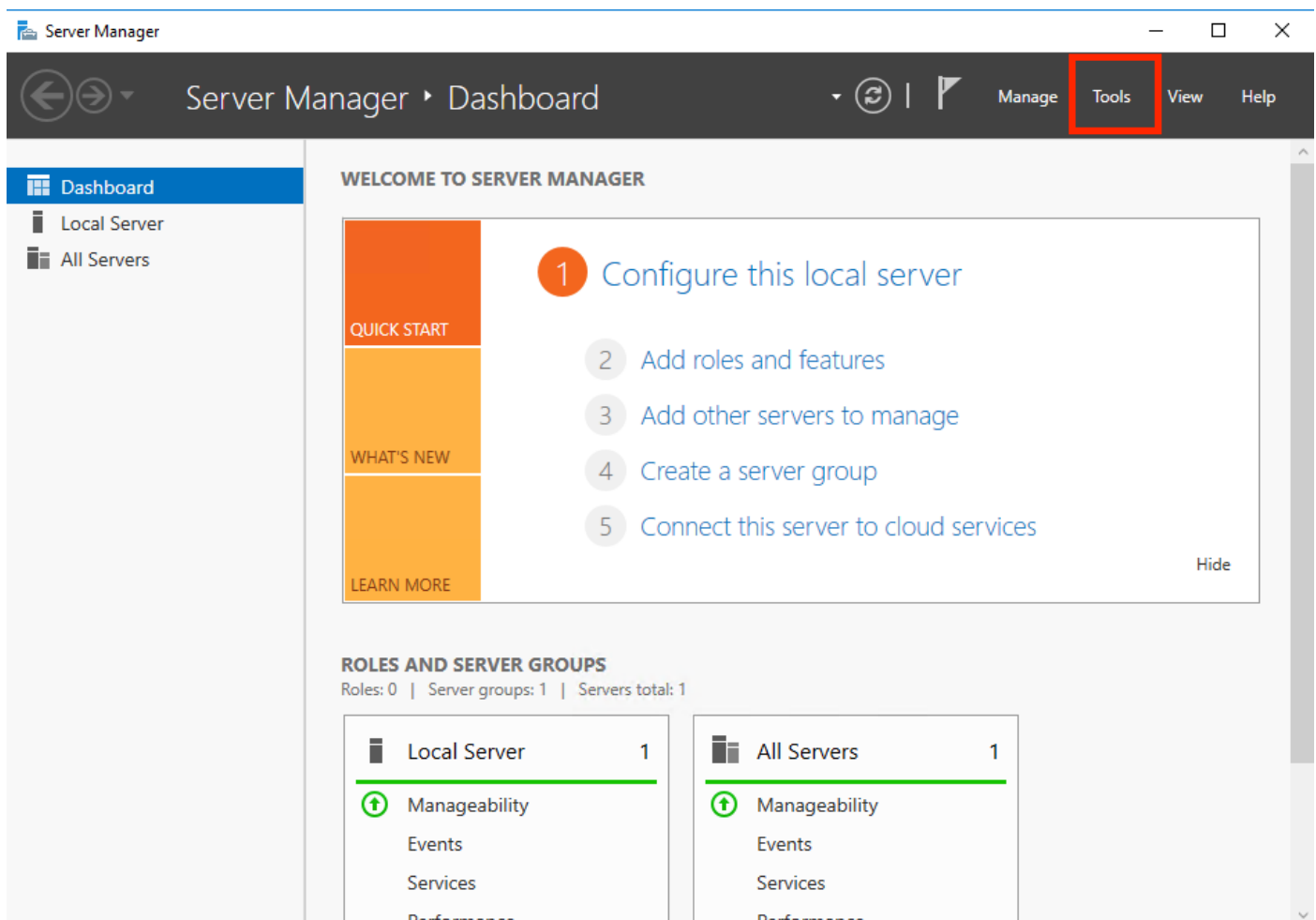
Als u het AnyConnect-configuratievoorbeelddocument zoekt, raadpleegt u "AnyConnect VPN-client configureren op FTD: HAAIEN EN NAT-vrijstellingsdocument".

## Configureren

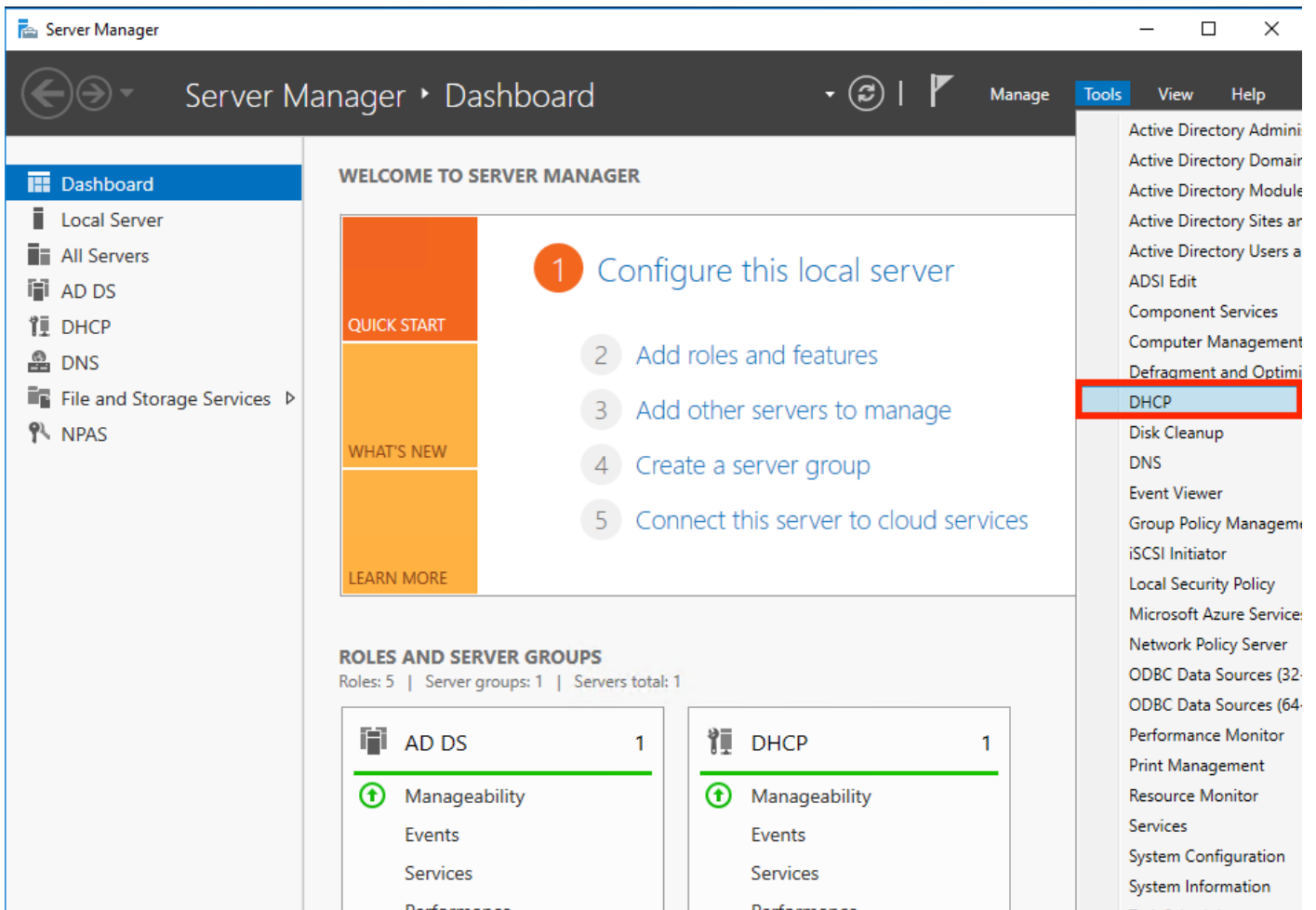
### Stap 1. Configureer de DHCP-werkruimte in de DHCP-server

In dit scenario bevindt de DHCP-server zich achter de FTD's interne interface.

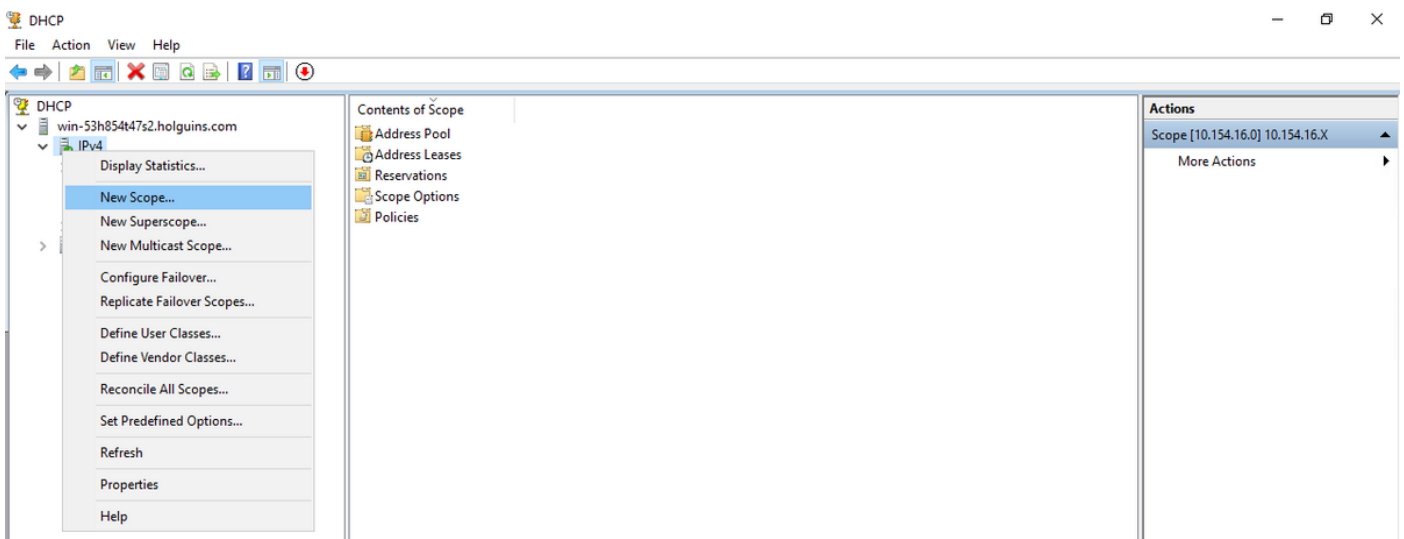
1. Open de Server Manager in Windows Server en selecteer **Gereedschappen** zoals in de afbeelding.



2. Selecteer DHCP:



3. Selecteer IPv4, klik met de rechtermuisknop op het gebied en selecteer **Nieuw bereik** zoals in de afbeelding.



4. Volg de **Wizard** zoals in de afbeelding.

## 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. Pas een naam aan het bereik toe zoals in de afbeelding wordt getoond.

## 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. Configureer het bereik van de adressen zoals in de afbeelding.

## 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. (Optioneel) Het configureren van de uitsluitingen zoals in de afbeelding weergegeven.

### 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. Het instellen **van de** tijdslimiet **is** een voorbeeld van hoe deze in de afbeelding wordt weergegeven.

## 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. (Optioneel) DHCP-opties instellen:



## 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

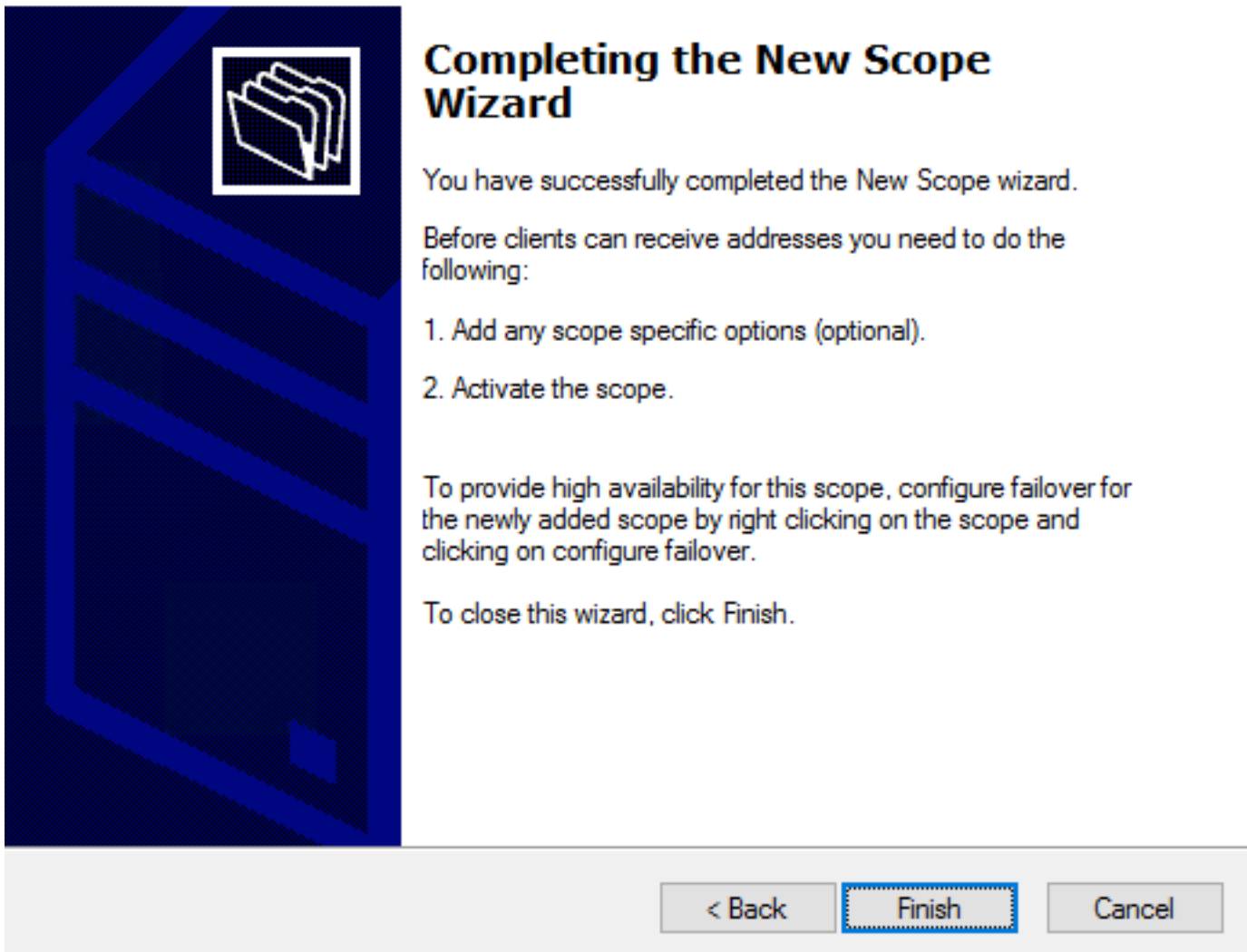
< Back

Next >

Cancel

10: Selecteer **Voltoeien** zoals in de afbeelding.

## 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:

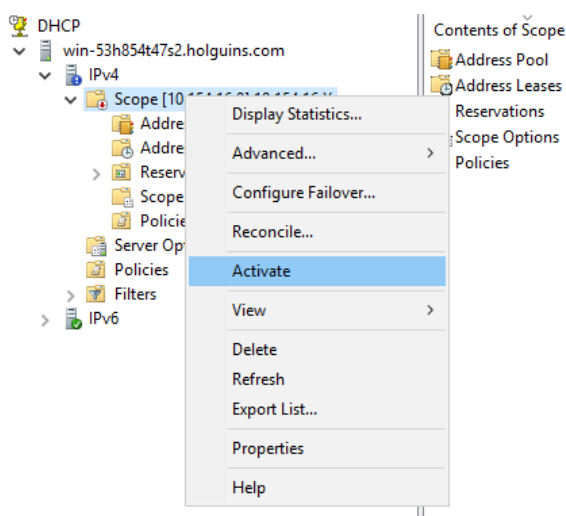
1. Add any scope specific options (optional).
2. Activate the scope.

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: Klik met de rechtermuisknop op de geselecteerde tekst en kies **Activeren** zoals in de afbeelding.



## Stap 2. Steekweg

Nadat het DHCP-bereik is ingesteld en geactiveerd, vindt de volgende procedure plaats in het FMC.


## Stap 2.1. Configuratieprofiel

1. Selecteer in het gedeelte DHCP-servers de  symbool en maak een object met het IP-adres van de DHCP-server.

2. Selecteer het object als de DHCP-server om een IP-adres aan te vragen, zoals in de afbeelding.


### Edit Connection Profile

Connection Profile:\*


Group Policy:\*    
[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: 

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

## Stap 2.2. Groepsbeleid configureren

1. In het menu Groepsbeleid, navigeer naar **Algemeen > DNS/WINS**, dan is er een gedeelte **DHCP-netwerkbereik** zoals in de afbeelding.

## 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:

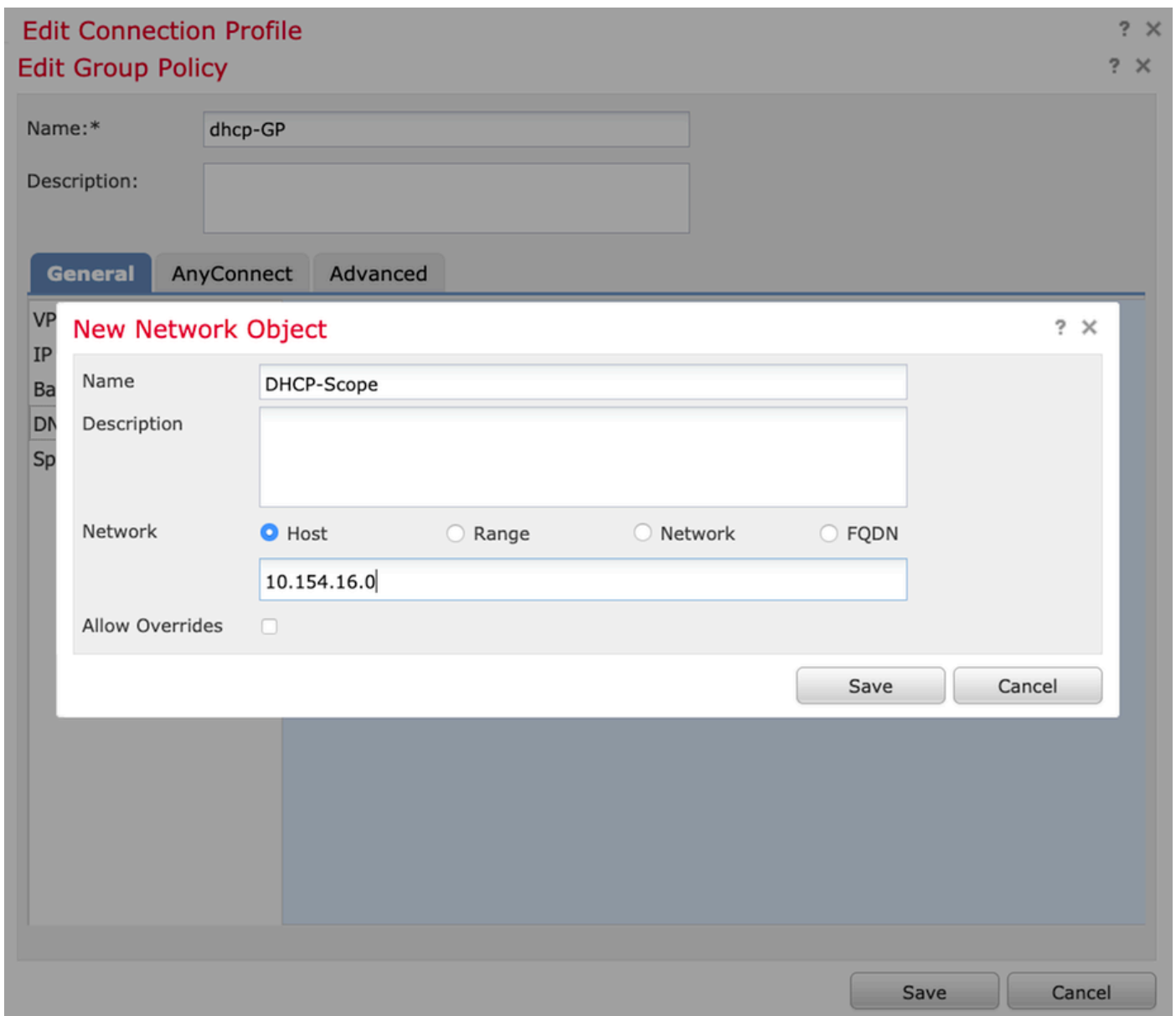
**DHCP Network Scope:**    
*Only network object with ipv4 address is allowed (Ex: 10.72.3.5)*

Default Domain:

Save Cancel

2. Maak een nieuw object, dit moet dezelfde netwerk grootte hebben als de DHCP-server.

**Opmerking:** Dit moet een host-object zijn, geen subtype.



3. Selecteer het object DHCP-bereik en selecteer **Opslaan** zoals in de afbeelding.

## 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

### Stap 2.3. Het beleid voor adrestoewijzing configureren

1. Navigeer naar **Geavanceerd > Adviezenbeleid** en controleer of de optie **DHCP gebruiken** is ingeschakeld zoals in de afbeelding.

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**

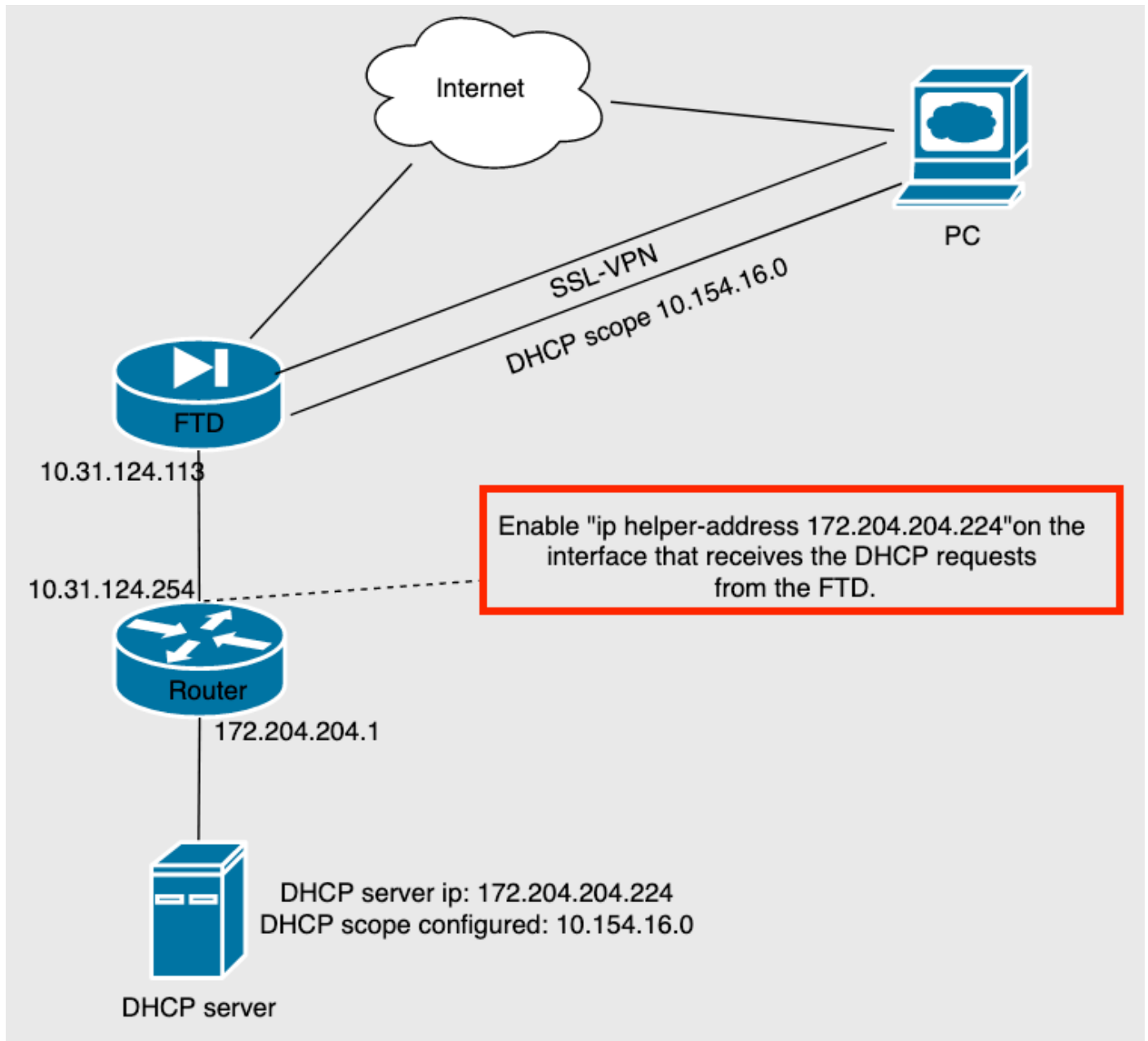
- Use authorization server (RADIUS Only)
- Use internal address pools

2. Sla de wijzigingen op en stel de configuratie in.

## IP-Helper-scenario

Wanneer de DHCP-server achter een andere router in het Local Area Network (LAN) staat, is een "IP-helpster" nodig om de verzoeken naar de DHCP-server te kunnen doorsturen.

Zoals in het beeld wordt getoond, illustreert een topologie het scenario en de noodzakelijke veranderingen in het netwerk.



## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

In deze sectie worden de DHCP-pakketten beschreven die tussen de FTD en de DHCP-server worden uitgewisseld.

- Detectie: Dit is een uniek pakket dat van de FTD's binneninterface naar de DHCP-server wordt verzonden. In de lading, specificeert een **Relay Agent IP adres** het bereik van de DHCP-server zoals in de afbeelding getoond.

```
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: 0000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
```

- Aanbod: Dit pakket is een reactie van de server van DHCP, dit komt met de de serverbron van DHCP en de bestemming van het gebied van DHCP in de FTD.
- Aanvraag: Dit is een uniek pakket dat van FTD's binnen interface naar de DHCP-server wordt verzonden.
- ACK: Dit pakket is een reactie van de server van DHCP, dit komt met de de serverbron van DHCP en de bestemming van het gebied van DHCP in de FTD.

## Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Stap 1. Download en schakelt wireshark in de DHCP-server in.

Stap 2. Pas DHCP toe als het opnamefilter zoals in de afbeelding.



No.	Time	Source	Destination	Protocol	Length	Info

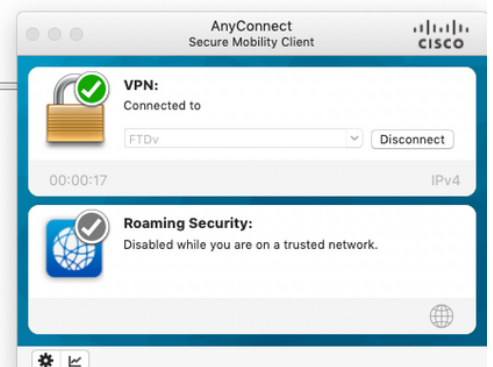


Step 3. Meld u aan bij AnyConnect. De DHCP-onderhandeling moet worden gezien zoals in de afbeelding.

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...-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  .C.C.....
0040 00 00 0a 9a 10 00 00 50 56 96 d1 70 00 00 00 00  .P.V.p.....
0050 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  .....
0070 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  .....
0090 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  .....
00b0 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  .....
00d0 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  .....
00f0 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  .....
```



## Gerelateerde informatie

- Deze video geeft het configuratievoorbeeld voor FTD, dat externe VPN-sessies om een IP-adres te verkrijgen dat toegewezen is door een DHCP-server van een derde partij.
- [Technische ondersteuning en documentatie – Cisco Systems](#)