

Configurez Anyconnect VPN Client sur FTD : Serveur DHCP pour l'attribution d'adresses

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Étape 1. Configurer l'étendue DHCP dans le serveur DHCP](#)

[Étape 2. Configurer Anyconnect](#)

[Étape 2.1. Configurer le profil de connexion](#)

[Étape 2.2. Configurez la stratégie de groupe](#)

[Étape 2.3. Configurer la stratégie d'attribution d'adresses](#)

[Scénario d'assistance IP](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document fournit un exemple de configuration pour Firepower Threat Defense (FTD) sur la version 6.4, qui permet aux sessions VPN d'accès à distance d'obtenir une adresse IP attribuée par un serveur DHCP (Dynamic Host Configuration Protocol) tiers.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- 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.

Informations générales

Ce document ne décrit pas l'ensemble de la configuration de l'accès à distance, juste la configuration requise dans le FTD afin de passer du pool d'adresses locales à l'affectation d'adresses DHCP.

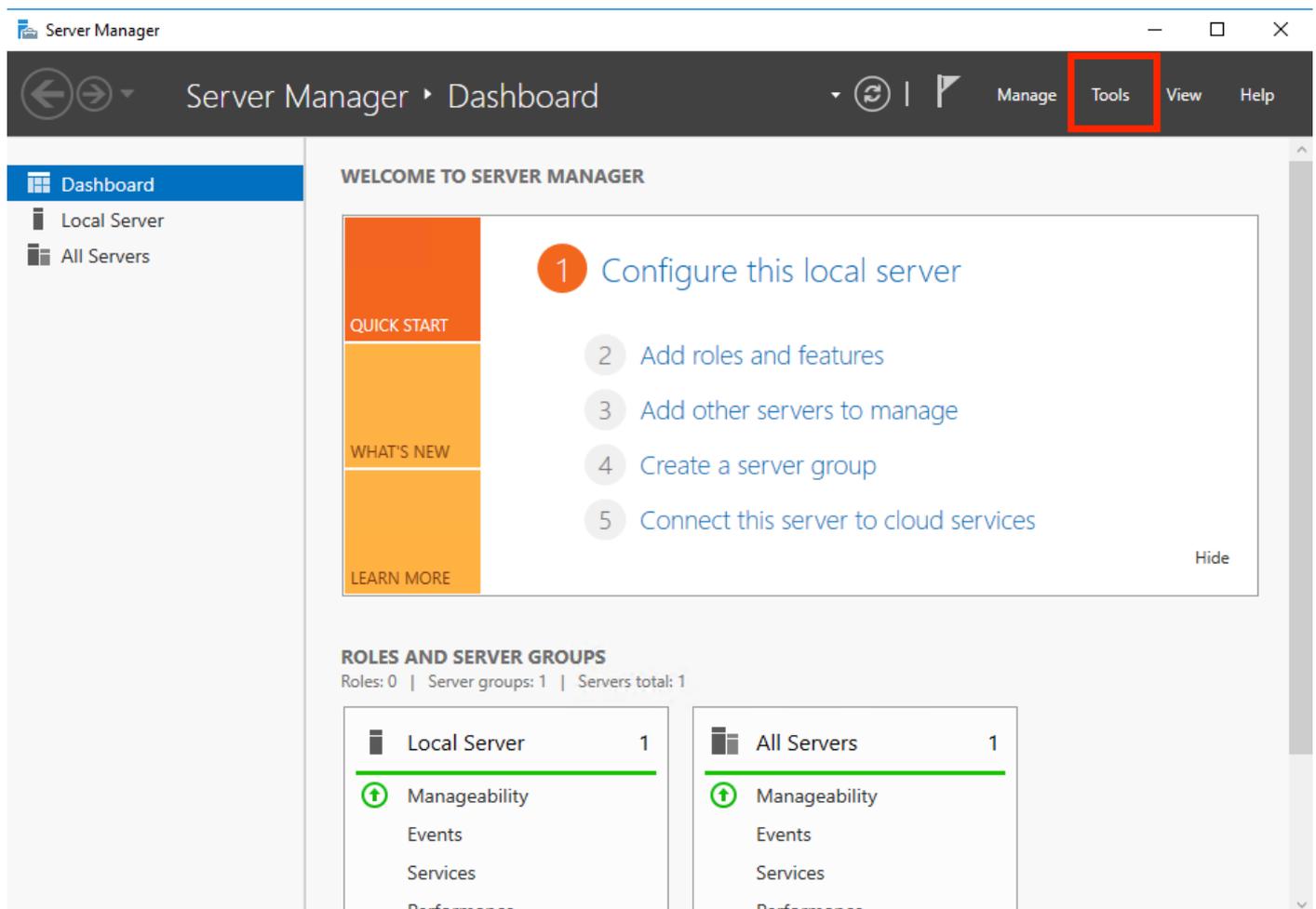
Si vous recherchez un exemple de document de configuration Anyconnect, reportez-vous à Configurer AnyConnect VPN Client sur FTD : Hairpinning and NAT Exemption ».

Configuration

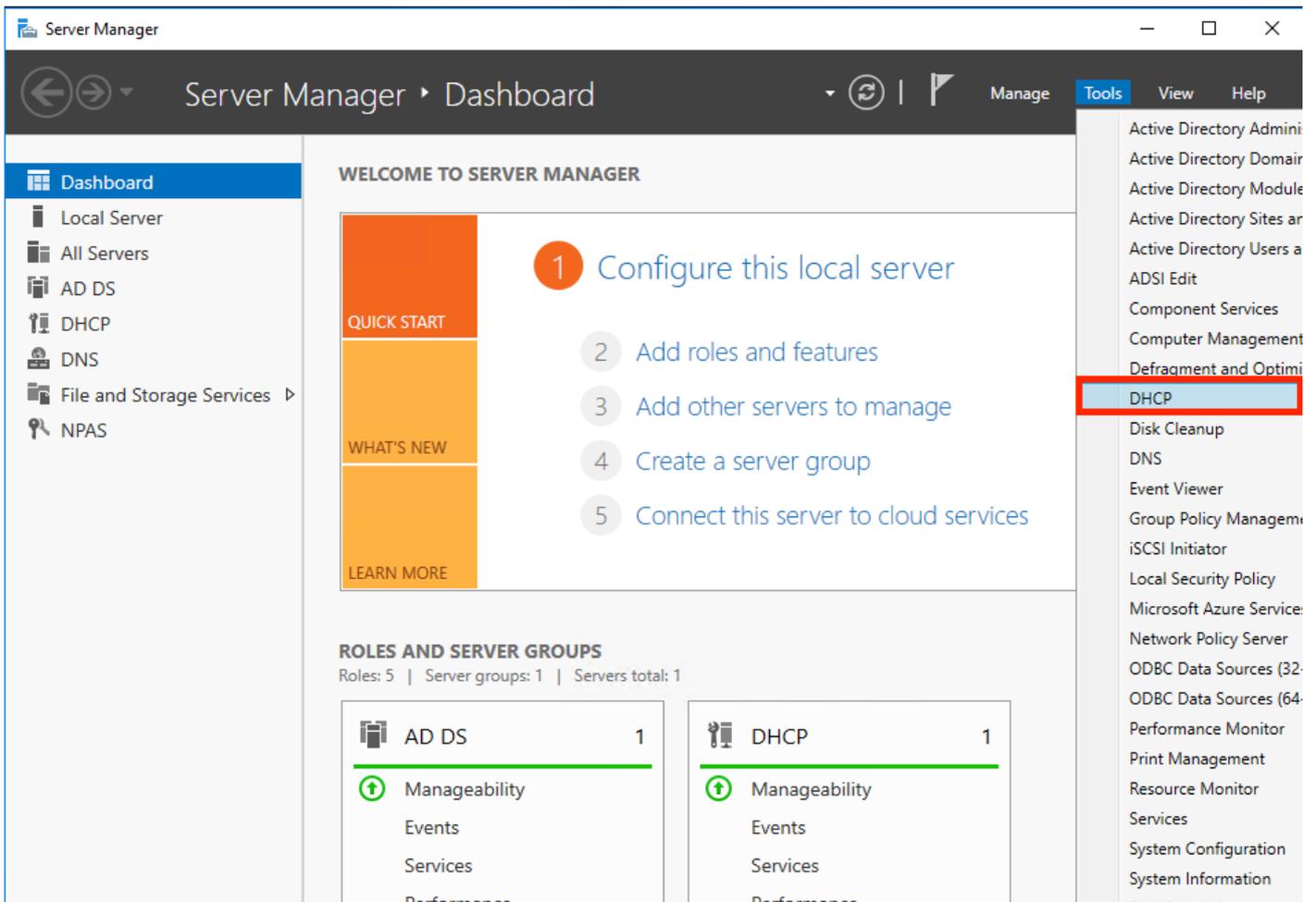
Étape 1. Configurer l'étendue DHCP dans le serveur DHCP

Dans ce scénario, le serveur DHCP est situé derrière l'interface interne du FTD.

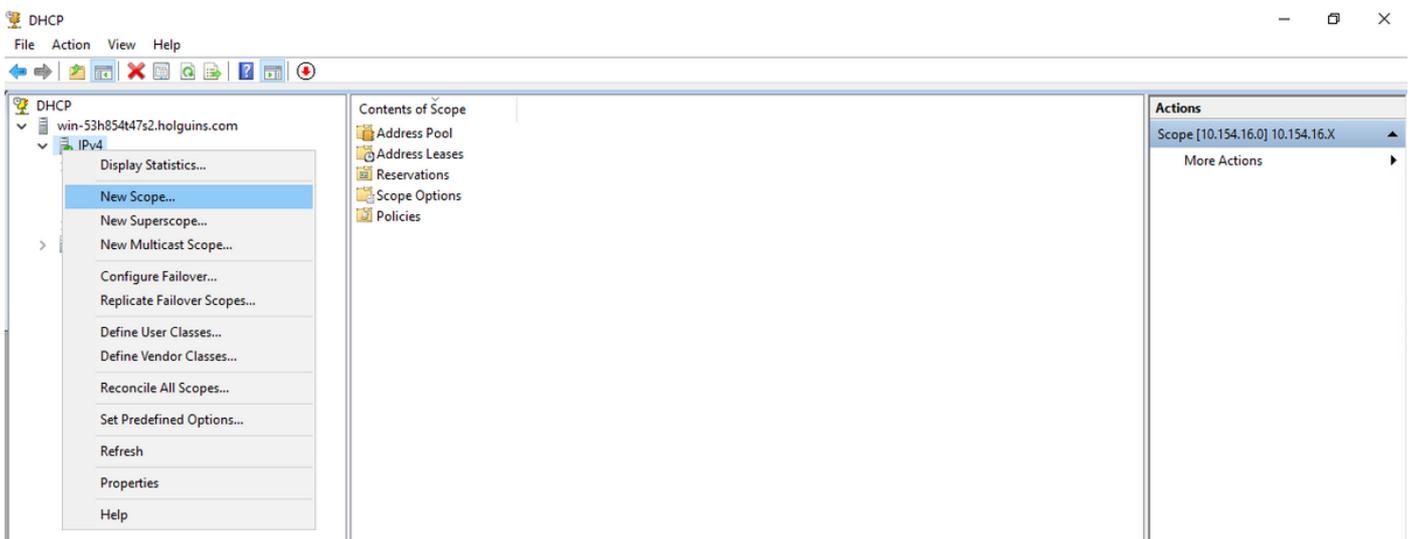
1. Ouvrez le Gestionnaire de serveur dans Windows Server et sélectionnez **Outils** comme indiqué dans l'image.



2. Sélectionnez DHCP :



3. Sélectionnez IPv4, cliquez dessus avec le bouton droit et sélectionnez **Nouvelle étendue** comme indiqué dans l'image.



4. Suivez l'**Assistant** comme indiqué dans l'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. Attribuez un nom à l'étendue comme indiqué dans l'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. Configurez la plage d'adresses comme indiqué dans l'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. (Facultatif) Configurez les exclusions comme indiqué dans l'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. Configurez la **durée du bail** comme indiqué dans l'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. (Facultatif) Configurez les options d'étendue DHCP :

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

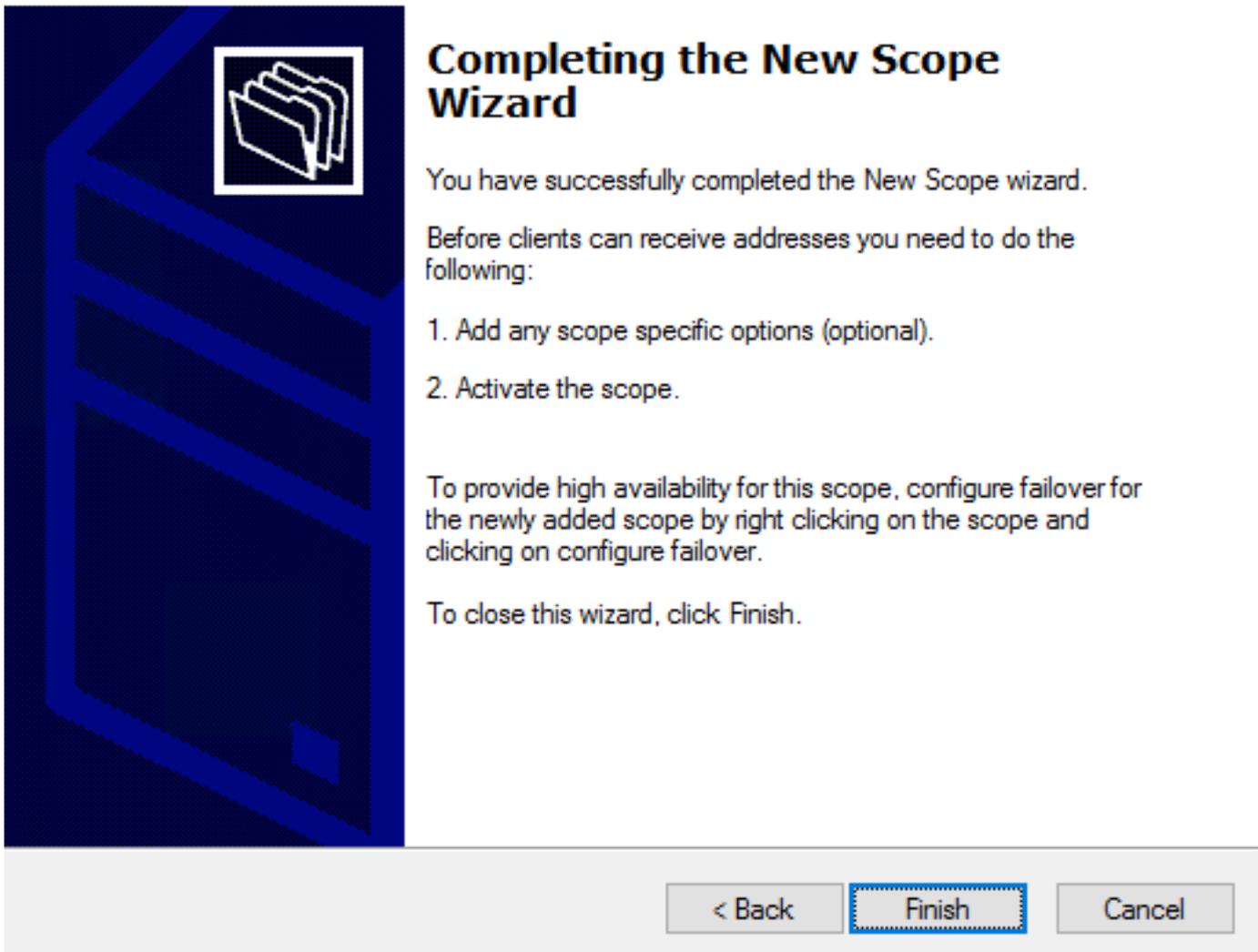
< Back

Next >

Cancel

10: Sélectionnez **Terminer** comme indiqué dans l'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:

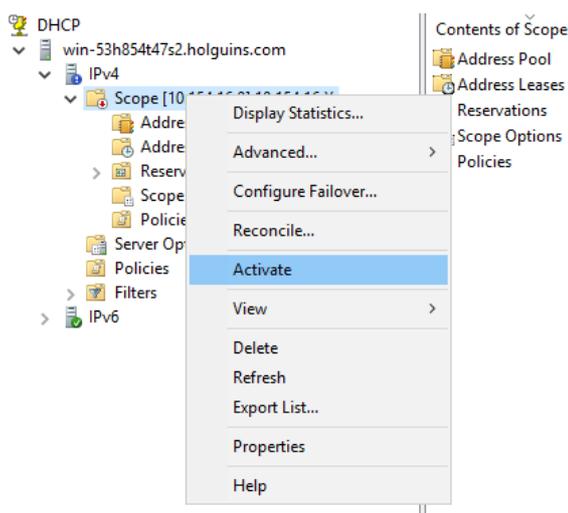
1. Add any scope specific options (optional).
2. Activate the scope.

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: Cliquez avec le bouton droit de la souris dans l'étendue que vous venez de créer et sélectionnez **Activer** comme indiqué dans l'image.



Étape 2. Configurer Anyconnect

Une fois l'étendue DHCP configurée et activée, la procédure suivante se déroule dans le FMC.

Étape 2.1. Configurer le profil de connexion

1. Dans la section DHCP Servers, sélectionnez  et créer un objet avec l'adresse IP du serveur DHCP.

2. Sélectionnez l'objet en tant que serveur DHCP afin de demander une adresse IP à partir de comme indiqué dans l'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

Étape 2.2. Configurez la stratégie de groupe

1. Dans le menu Stratégie de groupe, accédez à **General > DNS/WINS**, il existe une section **étendue réseau DHCP** comme illustré dans l'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:

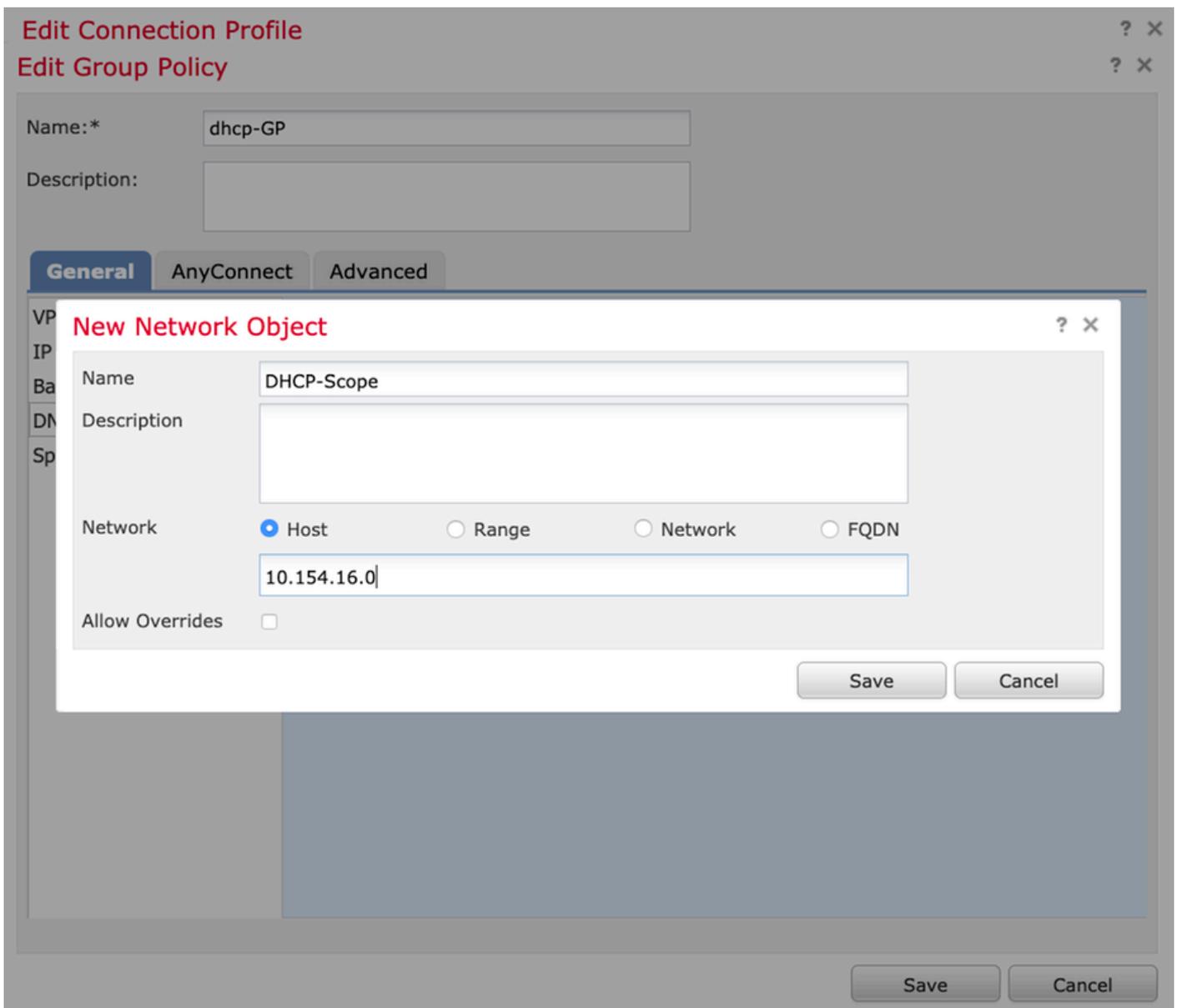
DHCP Network Scope:
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Save Cancel

2. Créez un nouvel objet, qui doit avoir la même étendue réseau que celle du serveur DHCP.

Note: Il doit s'agir d'un objet hôte et non d'un sous-réseau.



3. Sélectionnez l'objet de portée DHCP et sélectionnez **Enregistrer** comme indiqué dans l'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

Étape 2.3. Configurer la stratégie d'attribution d'adresses

1. Accédez à **Advanced > Address Assignment Policy** et assurez-vous que l'option **Use DHCP** est basculée comme indiqué dans l'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

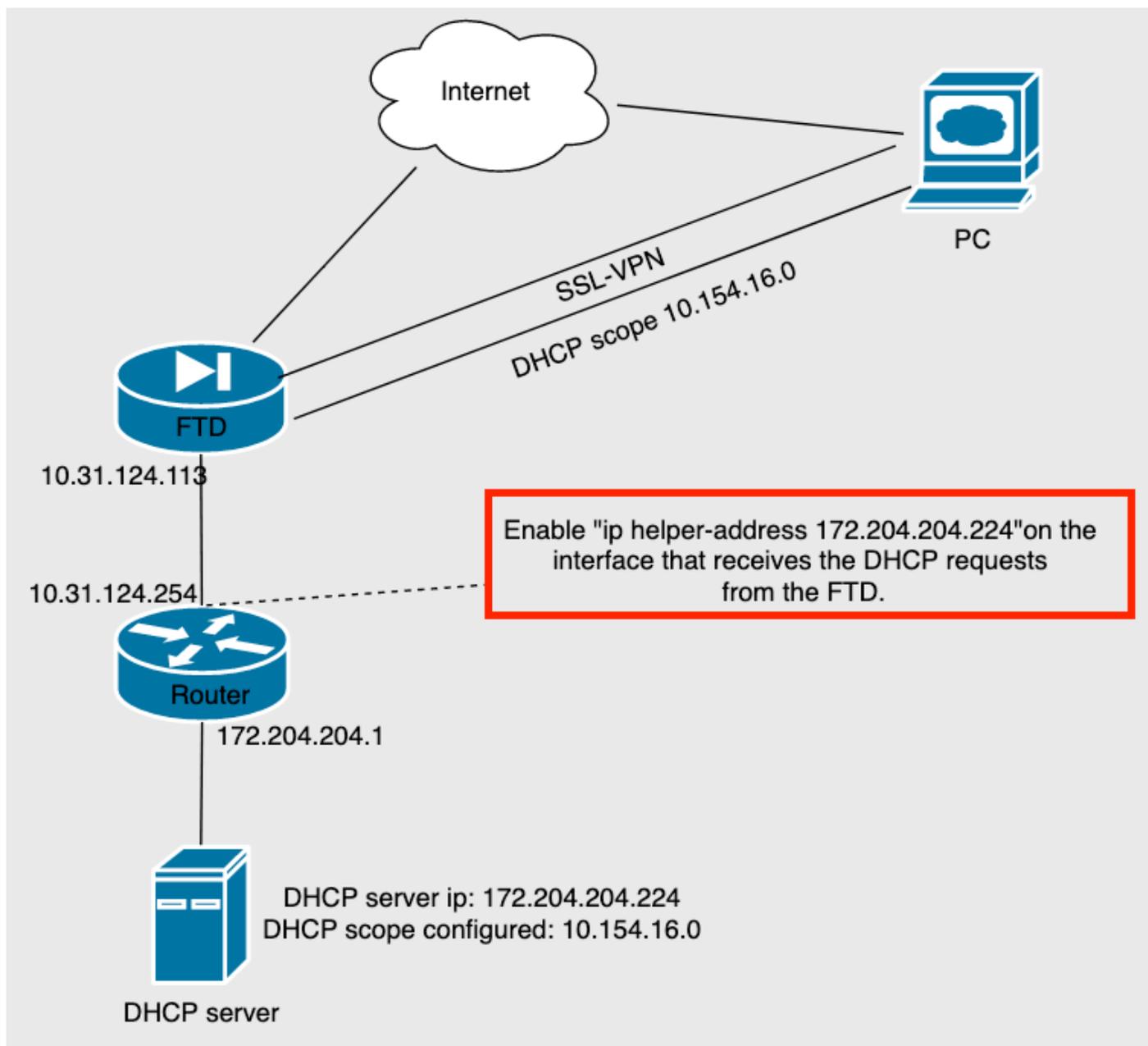
- Use authorization server (RADIUS Only)
- Use internal address pools

2. Enregistrez les modifications et déployez la configuration.

Scénario d'assistance IP

Lorsque le serveur DHCP se trouve derrière un autre routeur du réseau local (LAN), une assistance IP est nécessaire pour transmettre les requêtes au serveur DHCP.

Comme l'illustre l'image, une topologie illustre le scénario et les modifications nécessaires dans le réseau.



Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Cette section décrit les paquets DHCP échangés entre le serveur FTD et le serveur DHCP.

- Découverte : Il s'agit d'un paquet de monodiffusion envoyé de l'interface interne du FTD au

serveur DHCP. Dans la charge utile, une **adresse IP de l'agent de relais** spécifie l'étendue du serveur DHCP comme indiqué dans l'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
```

- Offre : Ce paquet est une réponse du serveur DHCP, qui vient avec la source du serveur DHCP et la destination de l'étendue DHCP dans le FTD.
- Demande : Il s'agit d'un paquet de monodiffusion envoyé de l'interface interne de FTD au serveur DHCP.
- ACK : Ce paquet est une réponse du serveur DHCP, qui vient avec la source du serveur DHCP et la destination de l'étendue DHCP dans le FTD.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Étape 1. Téléchargez et activez Wireshark sur le serveur DHCP.

Étape 2. Appliquez DHCP comme filtre de capture, comme illustré dans l'image.

No.	Time	Source	Destination	Protocol	Length	Info
						Number

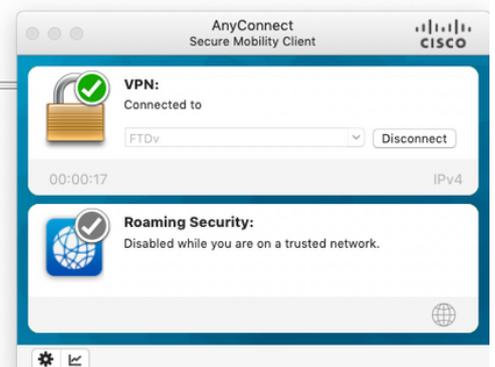


Étape 3. Connectez-vous à Anyconnect, la négociation DHCP doit être vue comme indiqué dans l'image.

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...-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  .....
```



Informations connexes

- Cette vidéo fournit un exemple de configuration pour FTD, qui permet aux sessions VPN d'accès à distance d'obtenir une adresse IP attribuée par un serveur DHCP tiers.
- [Support et documentation techniques - Cisco Systems](#)