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

Contenu

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.

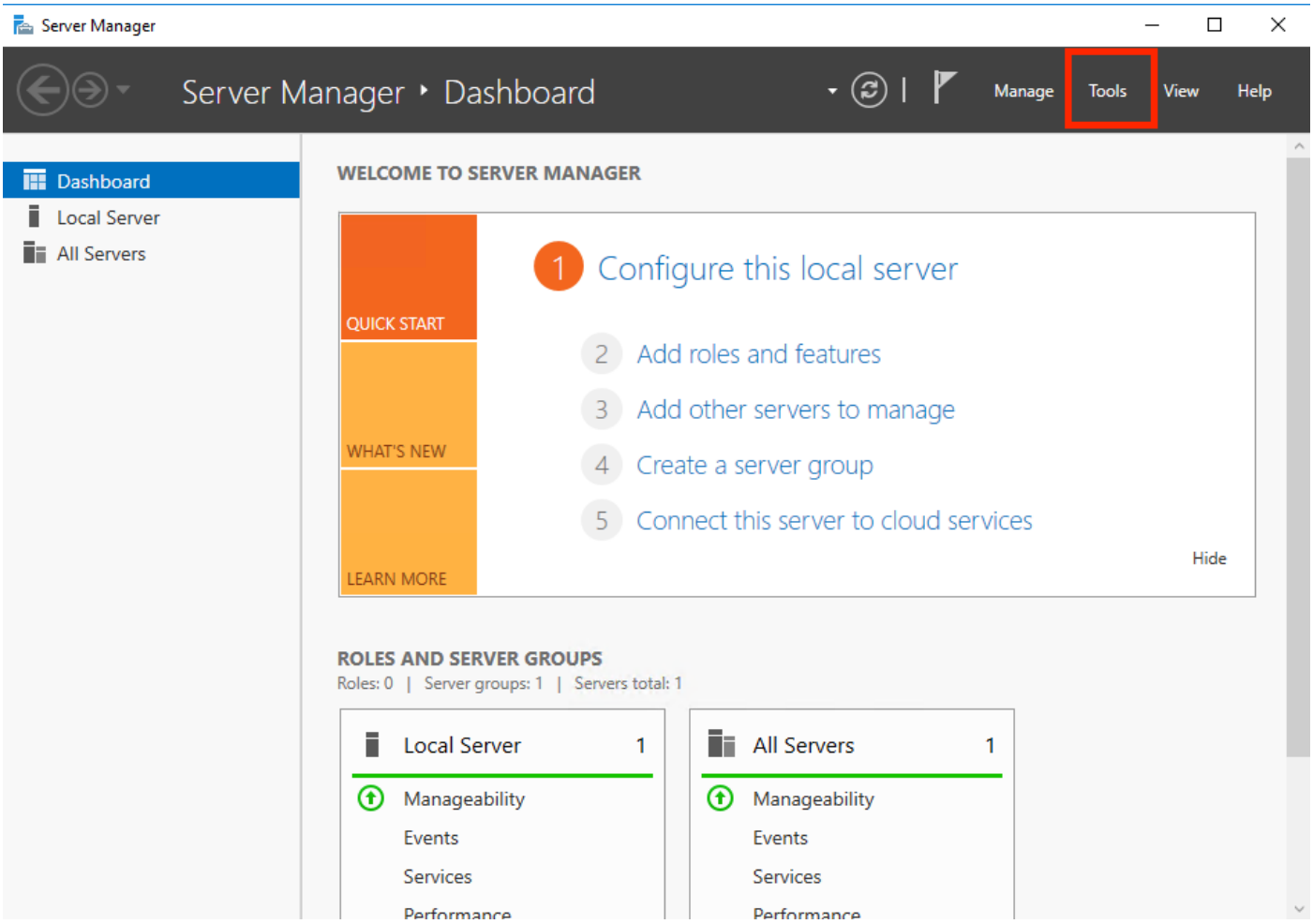
Si vous recherchez un exemple de document de configuration Anyconnect, reportez-vous à Configurer AnyConnect VPN Client sur FTD : Hairpining and NAT Exemption ».

Configuration

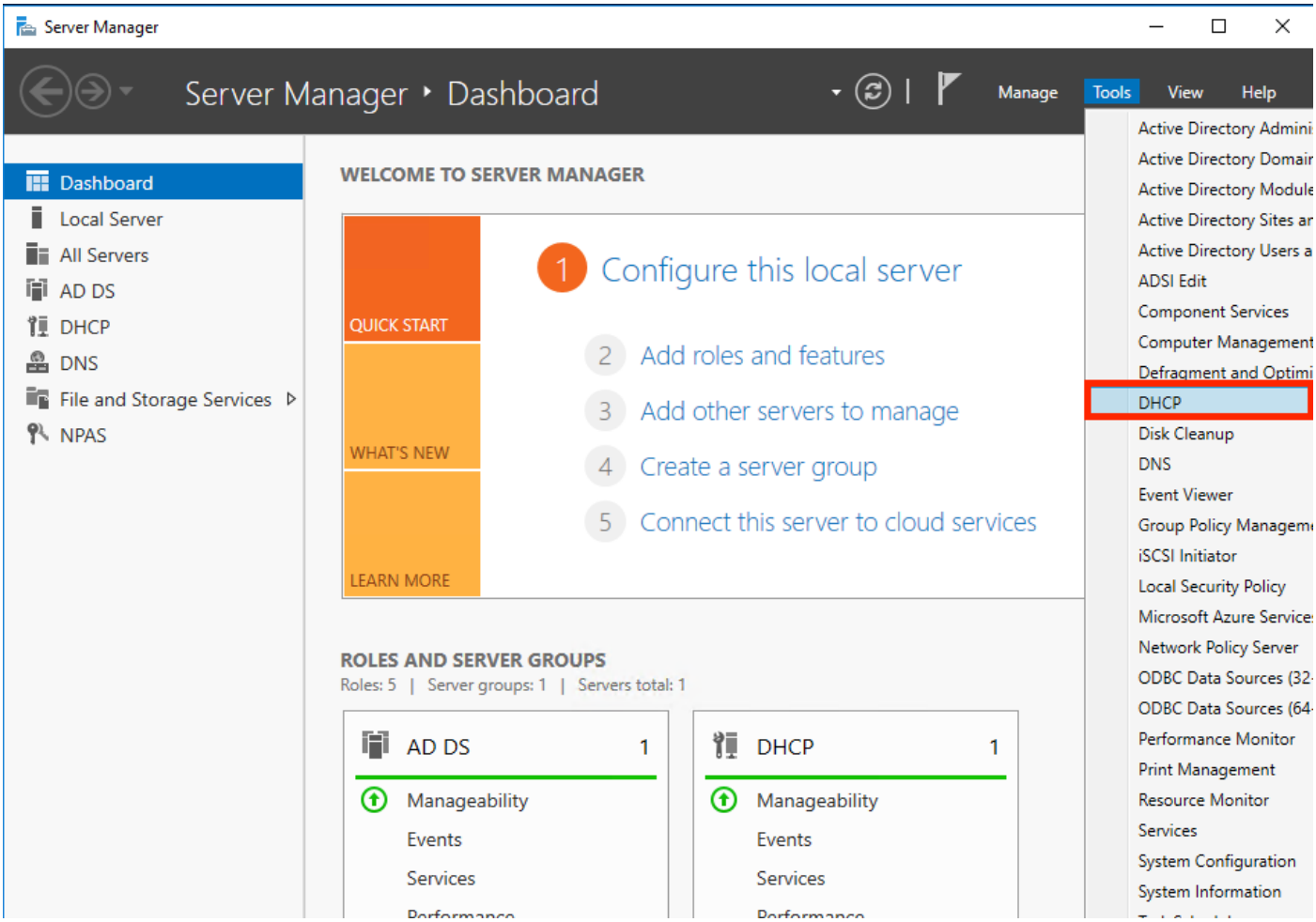
Étape 1. Configurer l'étendue DHCP dans le serveur DHCP

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

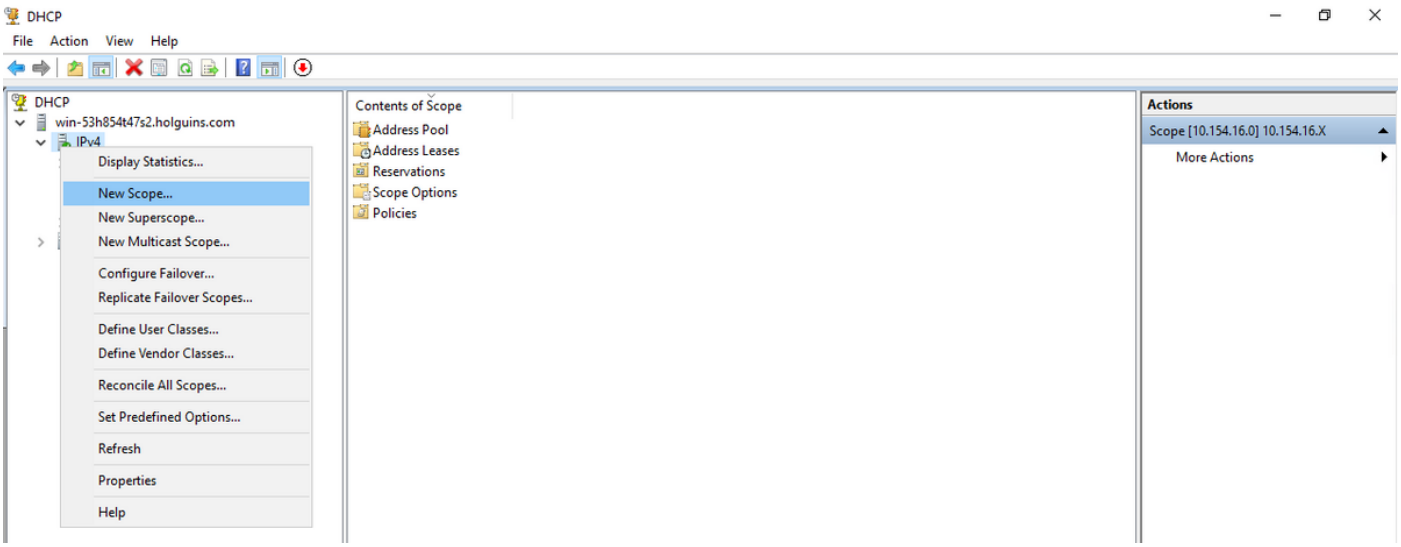
1. Ouvrez le Gestionnaire de serveur dans Windows Server et sélectionnez **Outils** comme indiqué dans l'image.



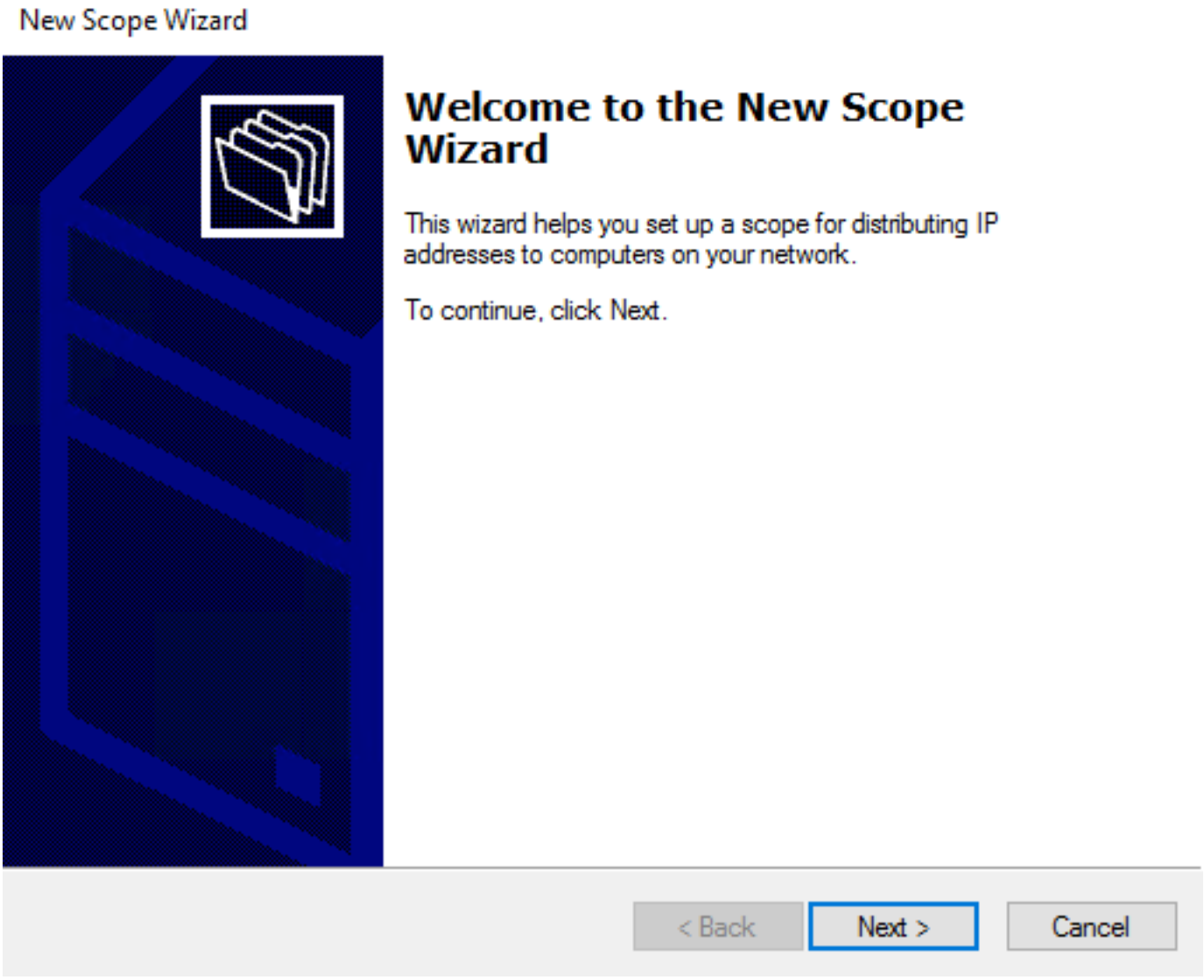
2. Sélectionnez DHCP :



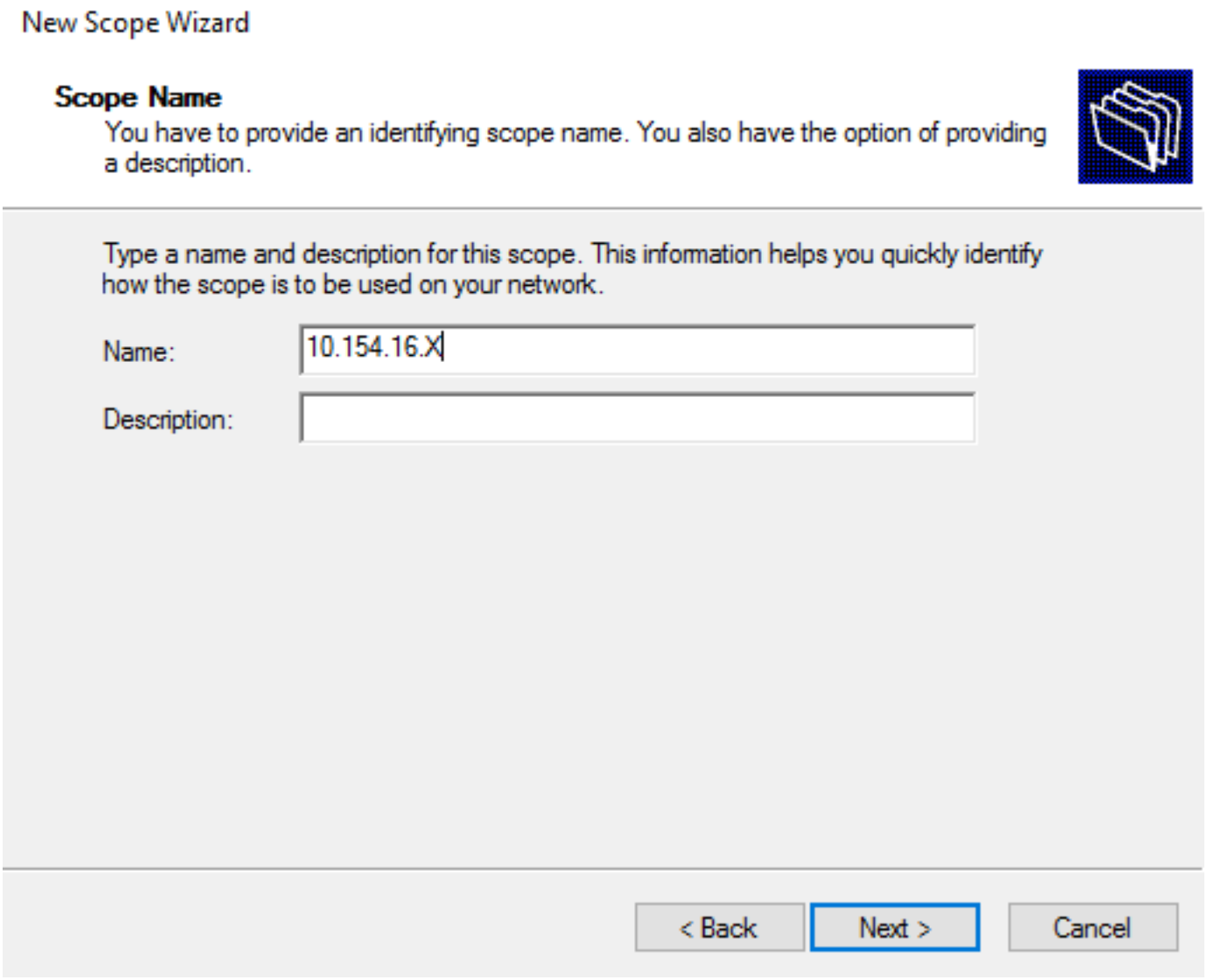
3. Sélectionnez IPv4, cliquez dessus avec le bouton droit et sélectionnez **Nouvelle étendue** comme indiqué dans l'image.



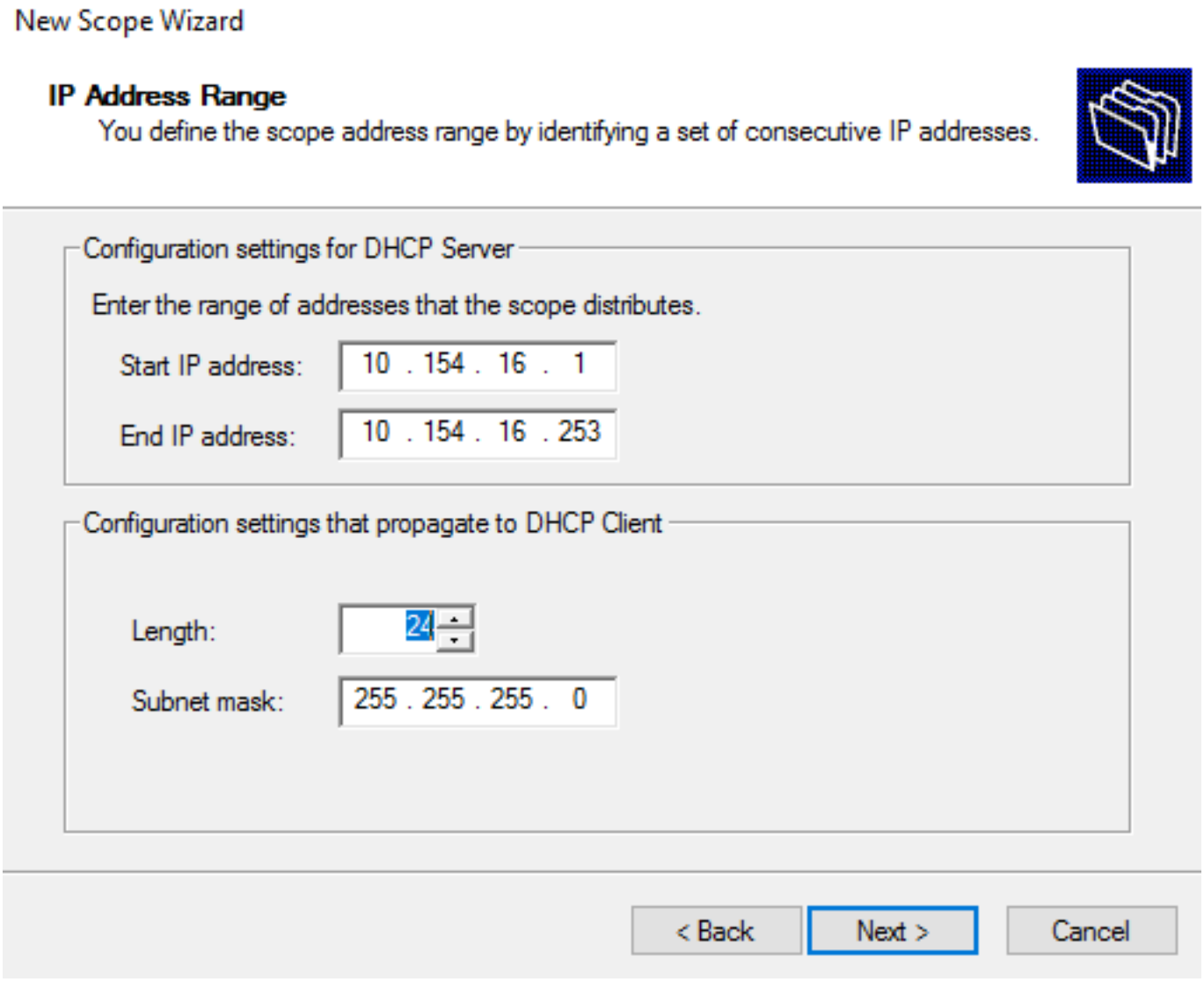
4. Suivez l'**Assistant** comme indiqué dans l'image.



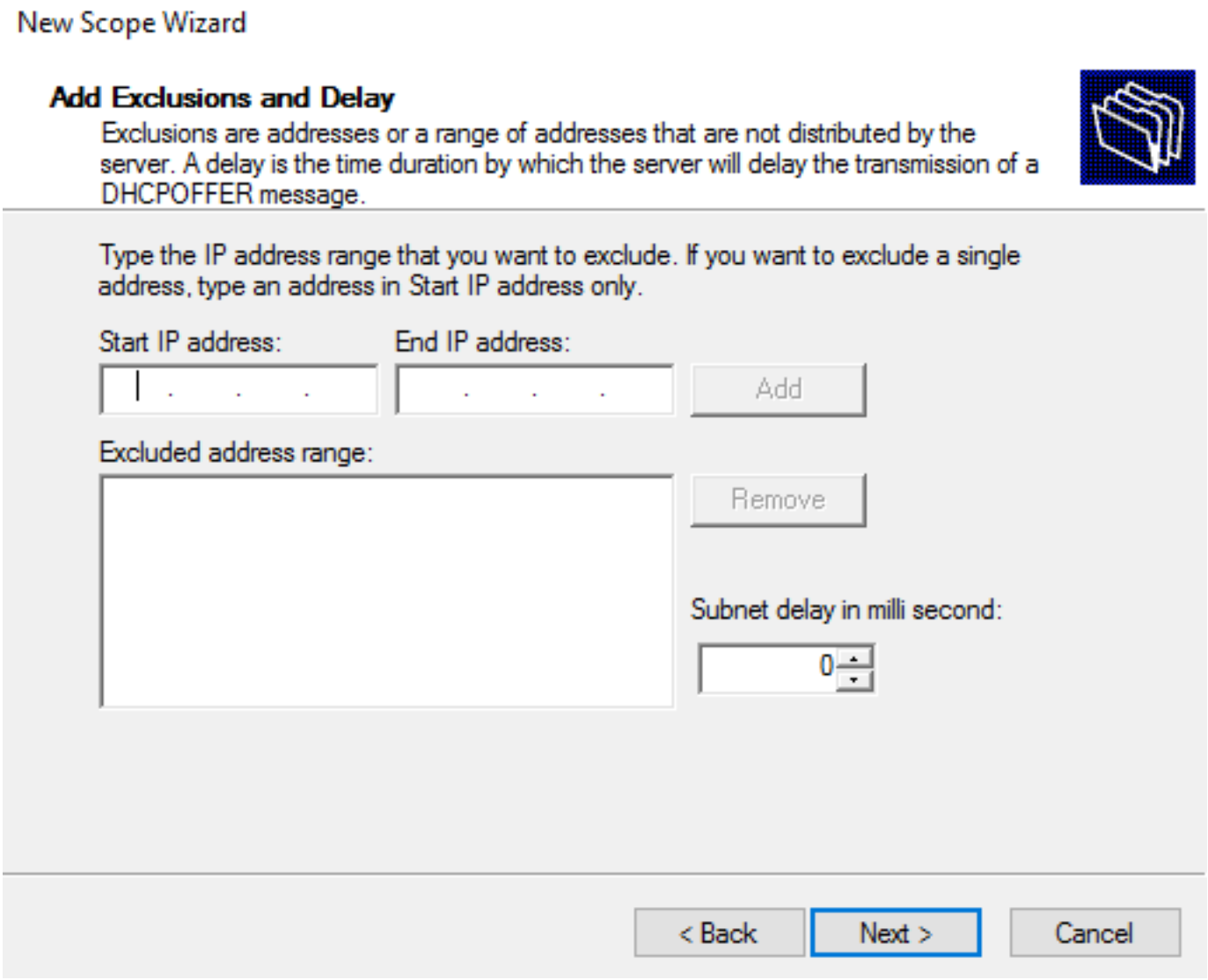
5. Attribuez un nom à l'étendue comme indiqué dans l'image.



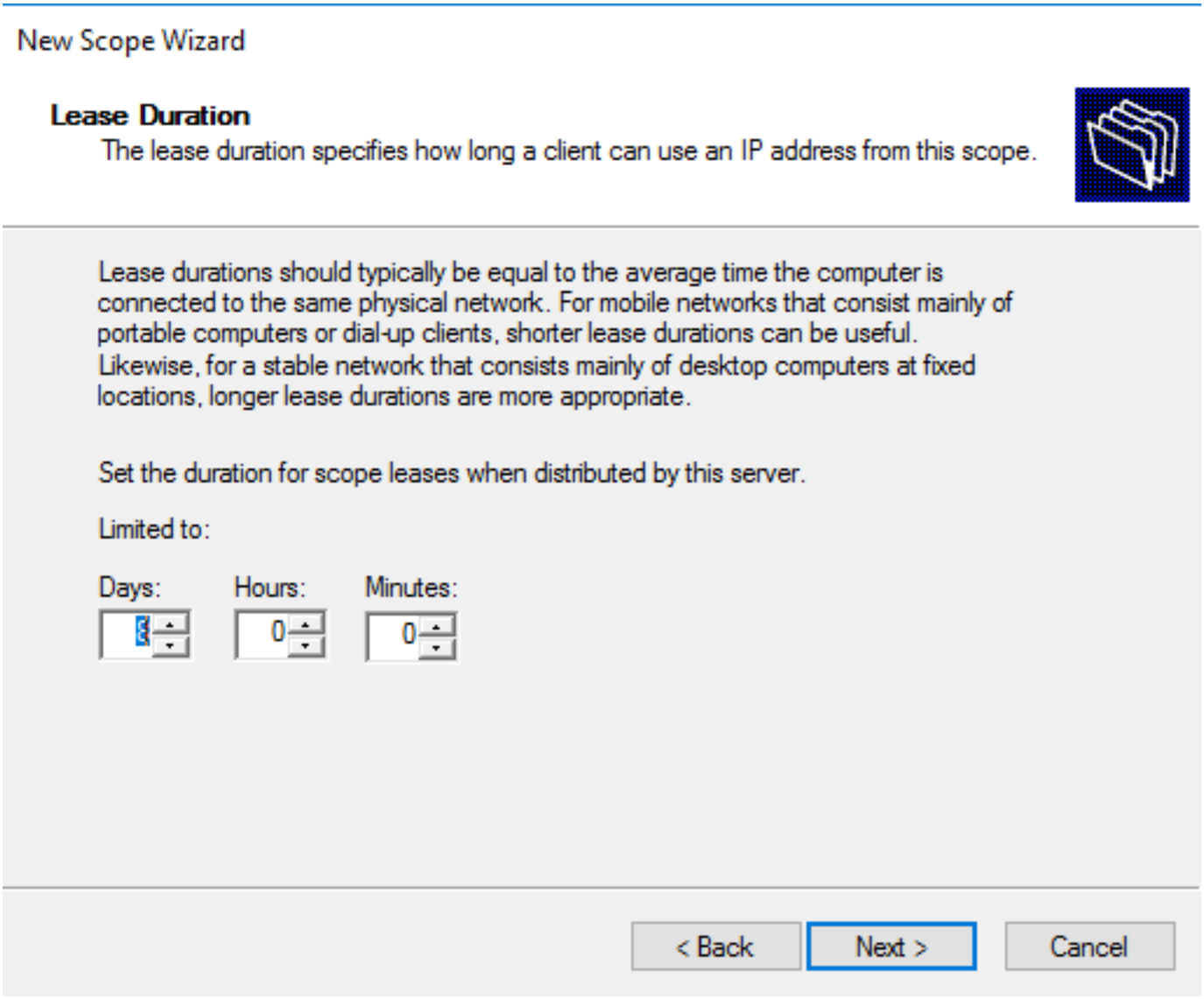
6. Configurez la plage d’adresses comme indiqué dans l’image.



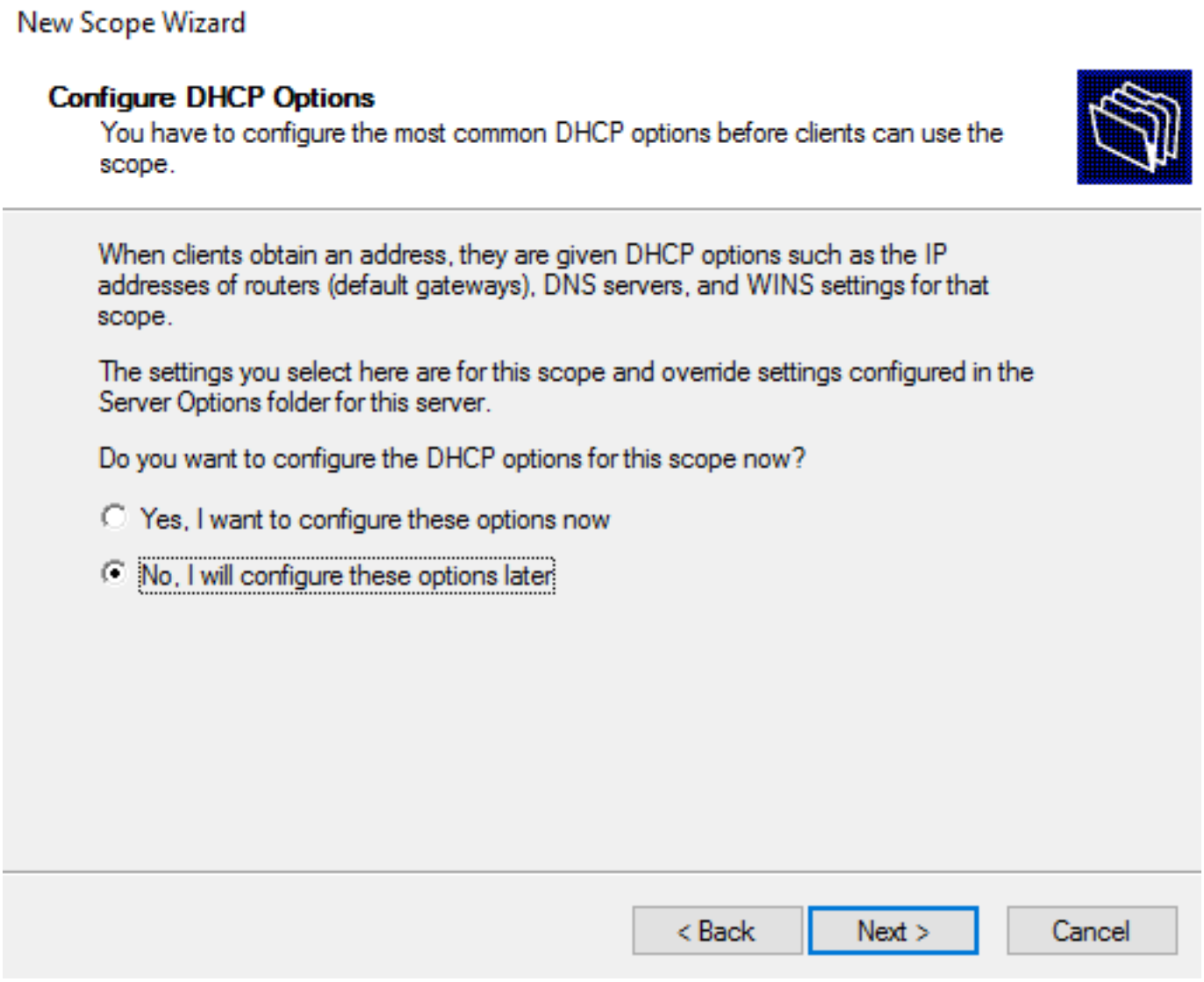
7. (Facultatif) Configurez les exclusions comme indiqué dans l'image.



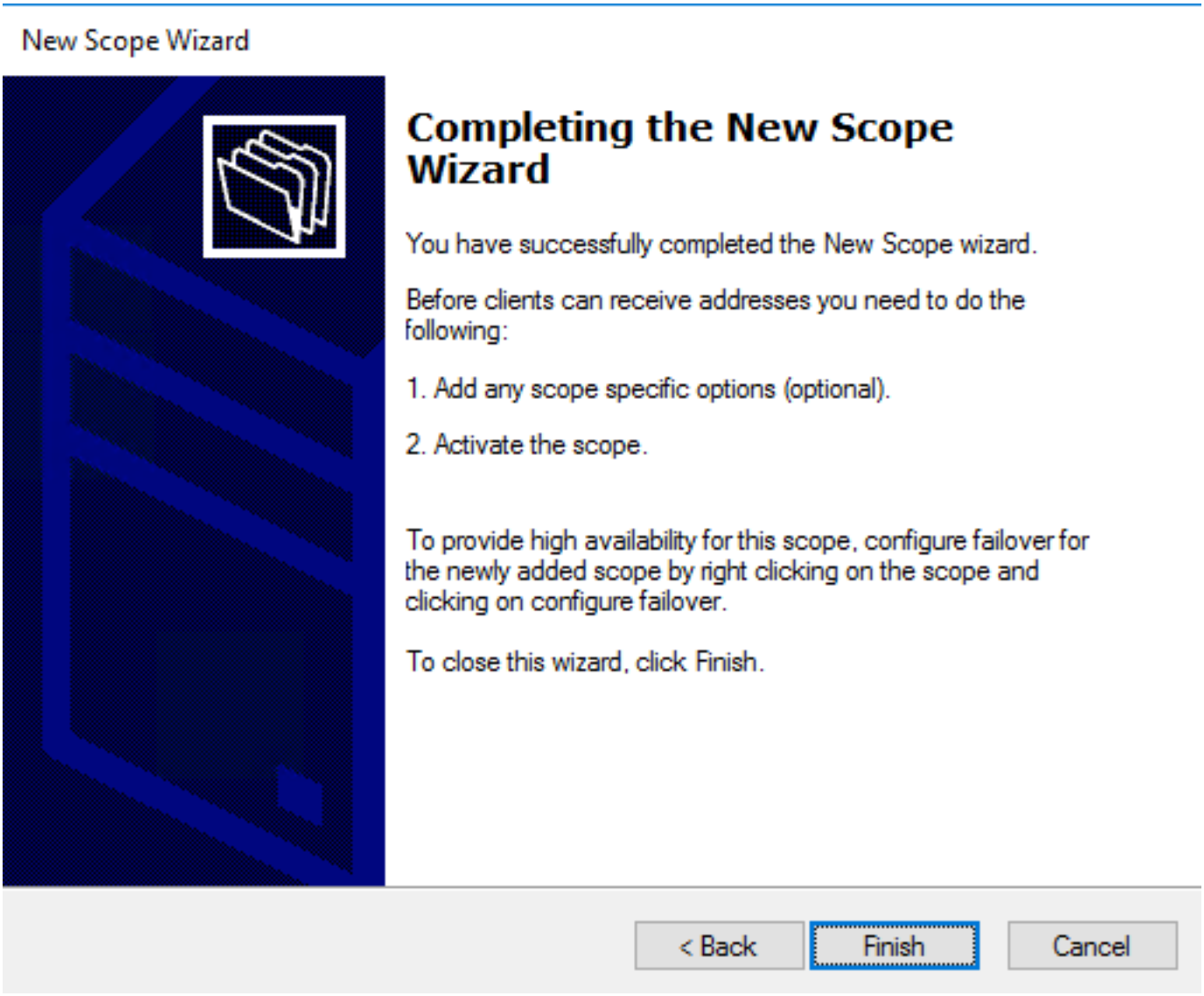
8. Configurez la **durée du bail** comme indiqué dans l'image.



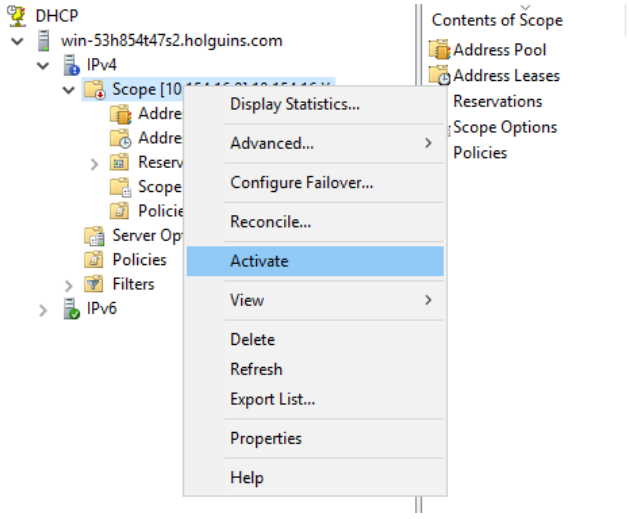
9. (Facultatif) Configurez les options d'étendue DHCP :



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



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.



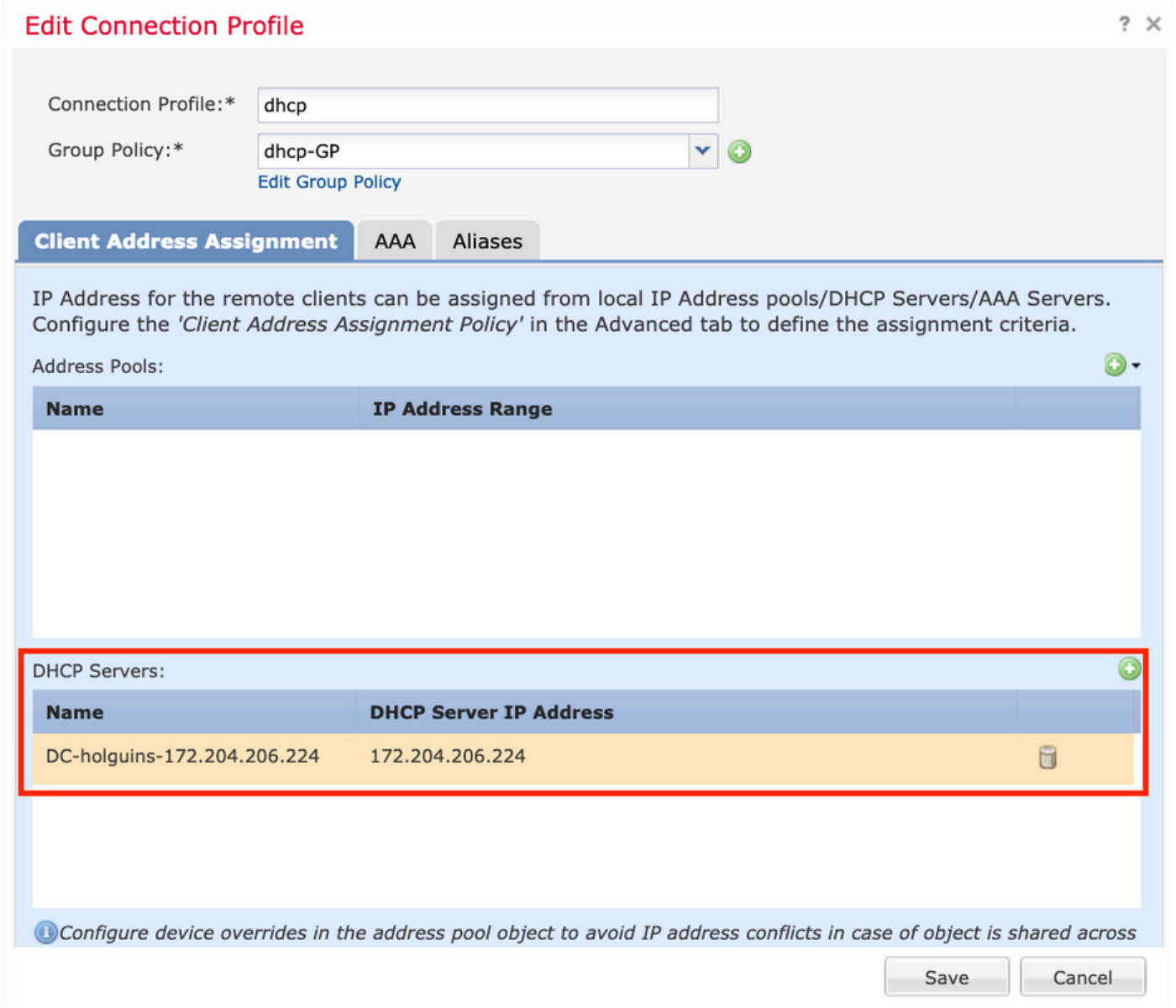
Étape 2. Configurer Anyconnect

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

Étape 2.1. Configurer le profil de connexion

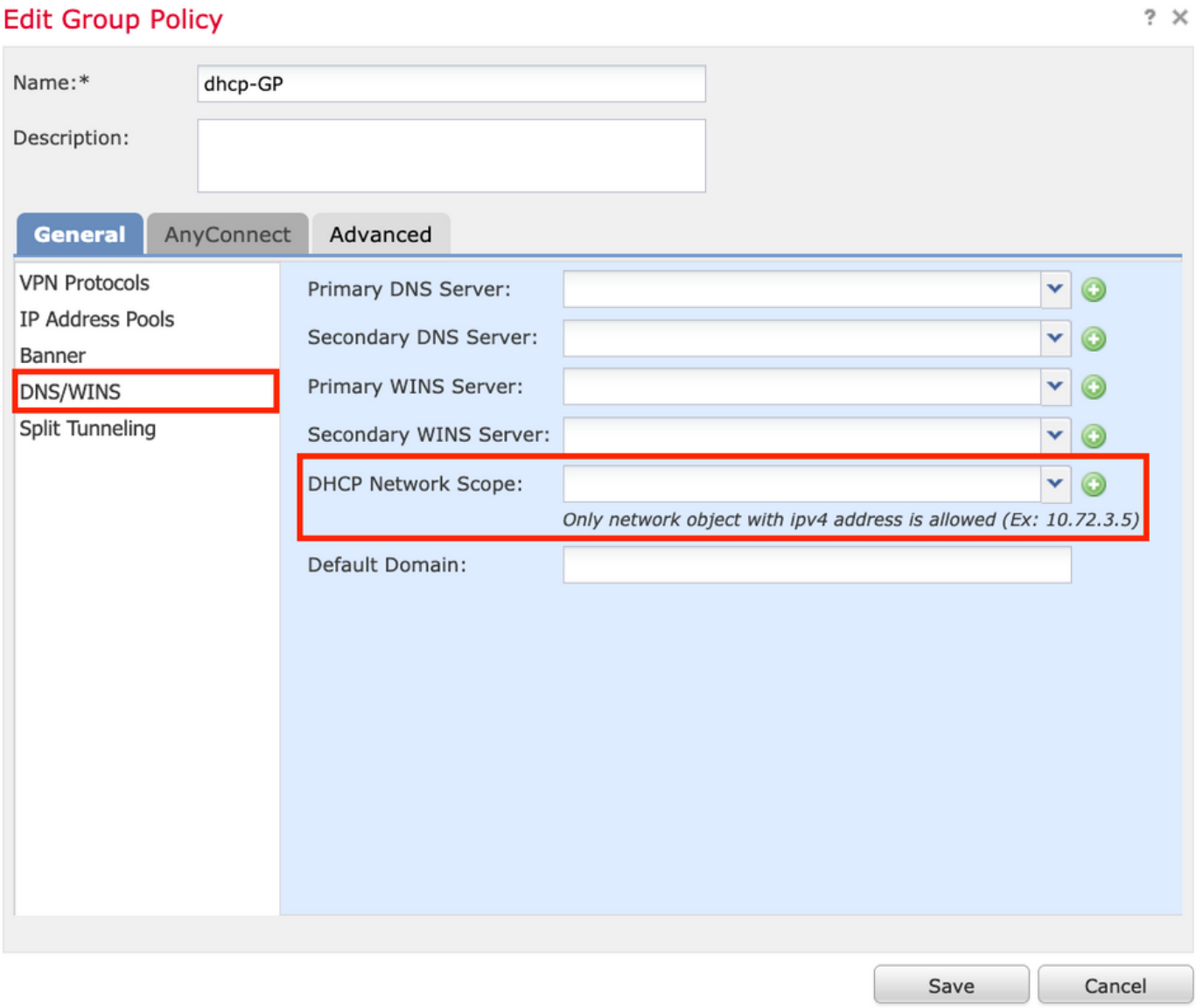
1. Dans la section DHCP Servers, sélectionnez  et créer un objet avec l'adresse IP du serveur DHCP.

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



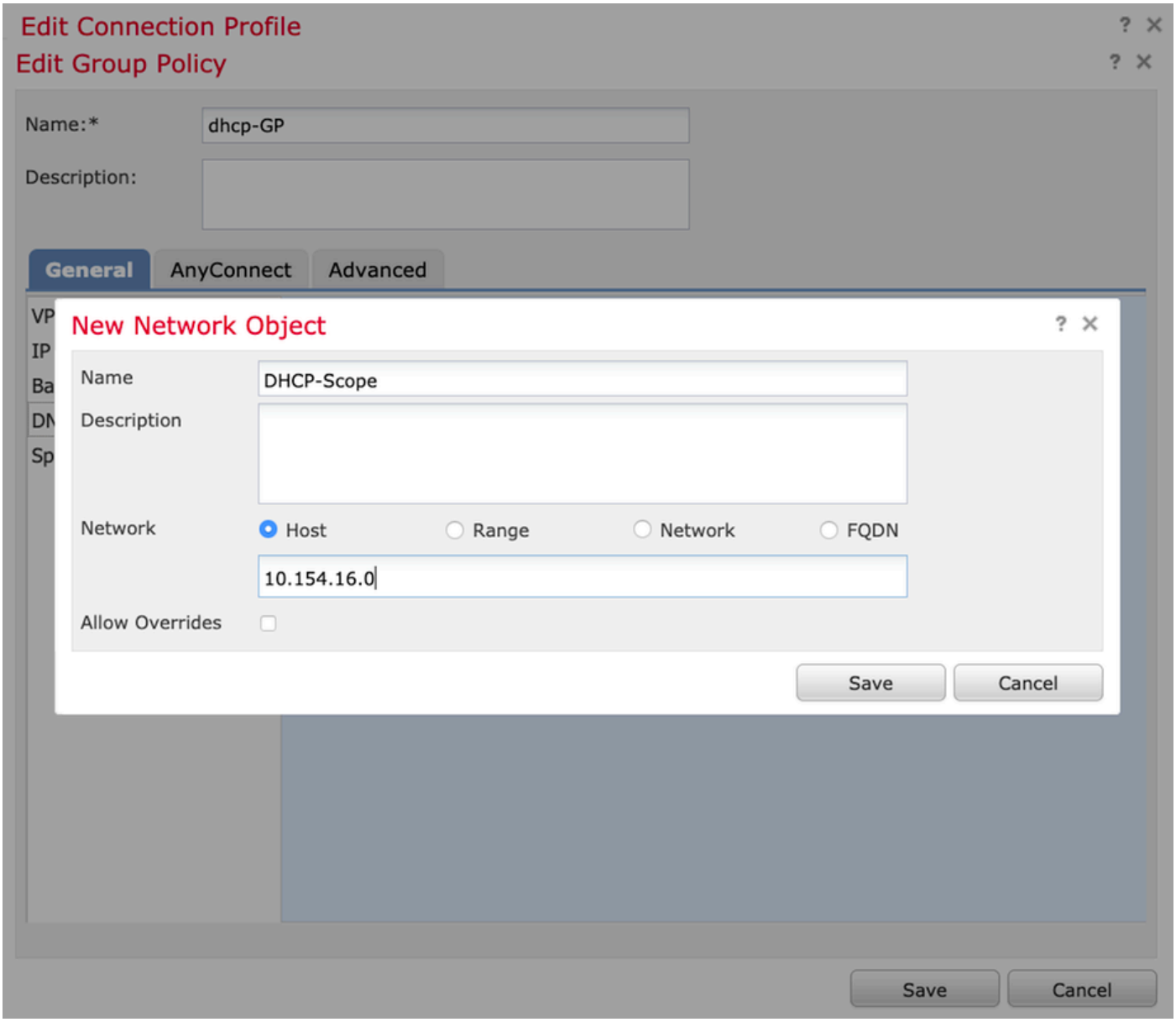
Étape 2.2. Configurez la stratégie de groupe

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

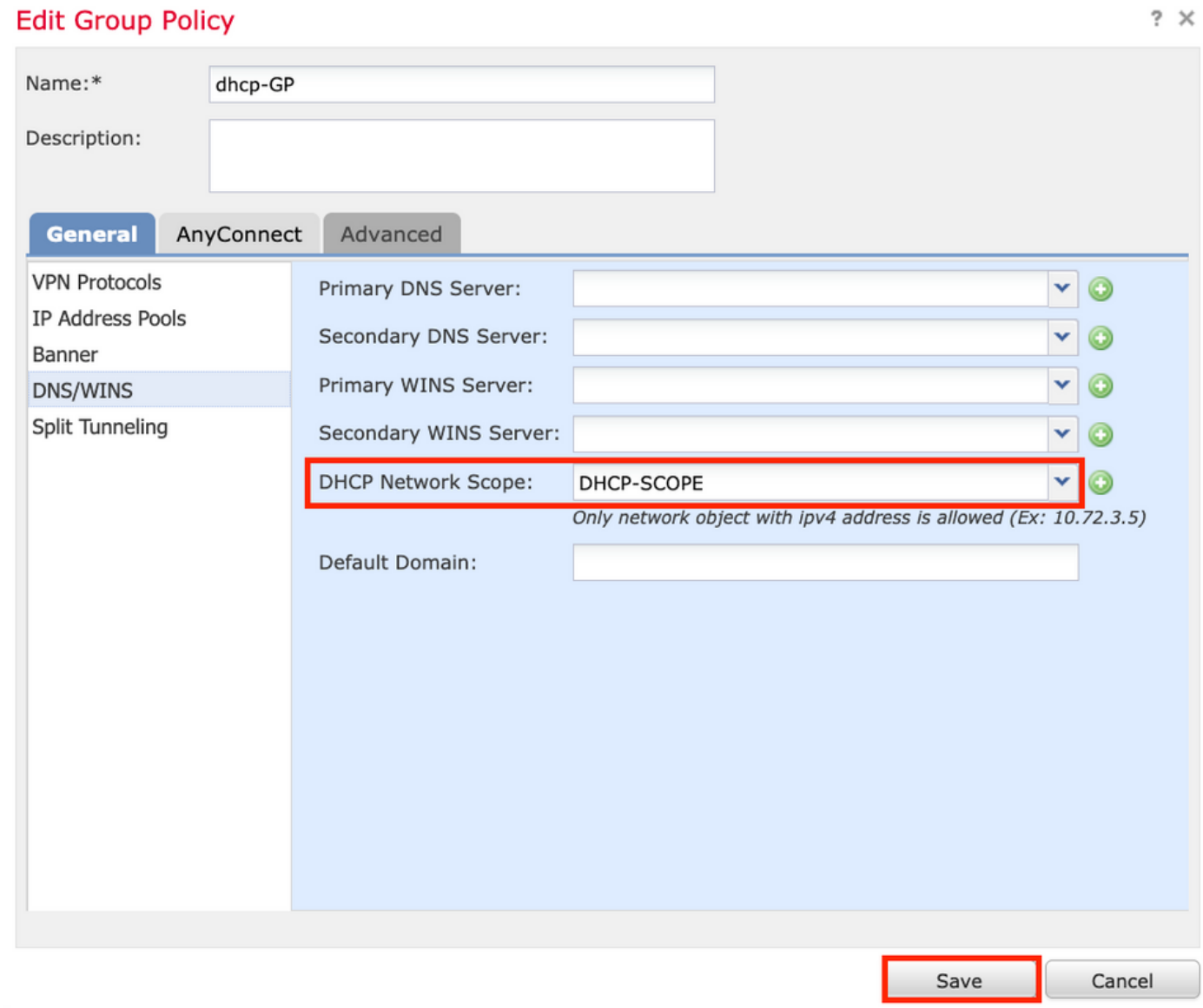


2. Créez un nouvel objet, qui doit avoir la même étendue réseau que celle du serveur DHCP.

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

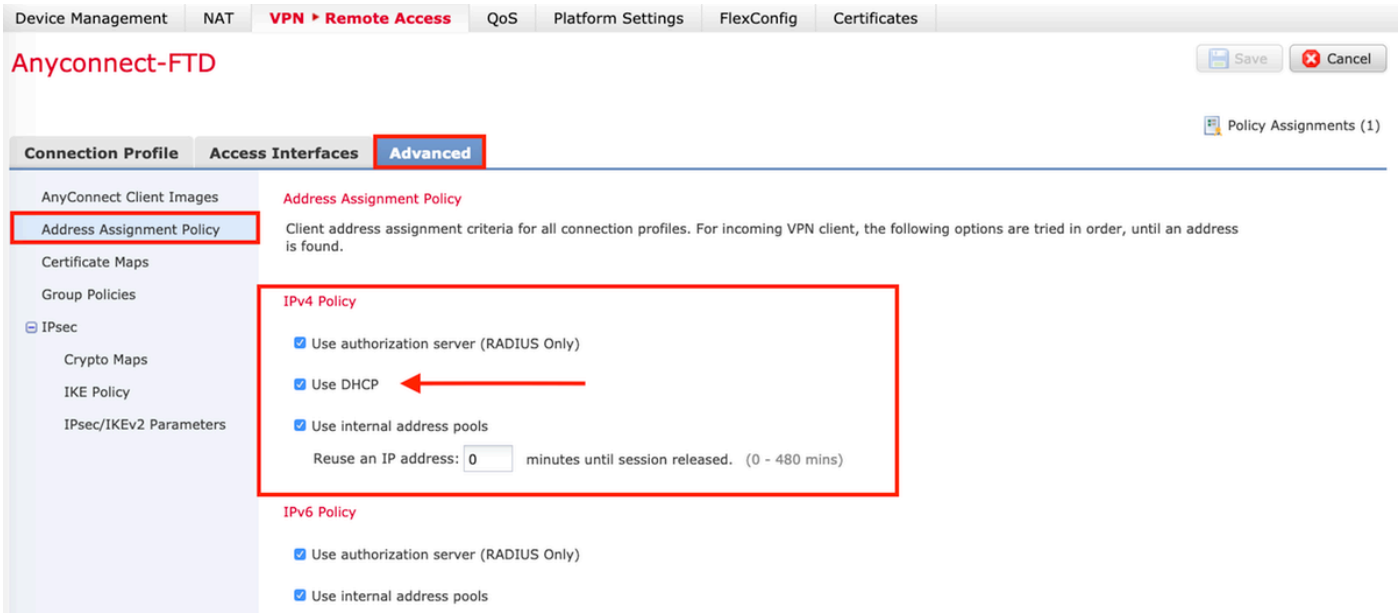


3. Sélectionnez l'objet de portée DHCP et sélectionnez **Enregistrer** comme indiqué dans l'image.



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.

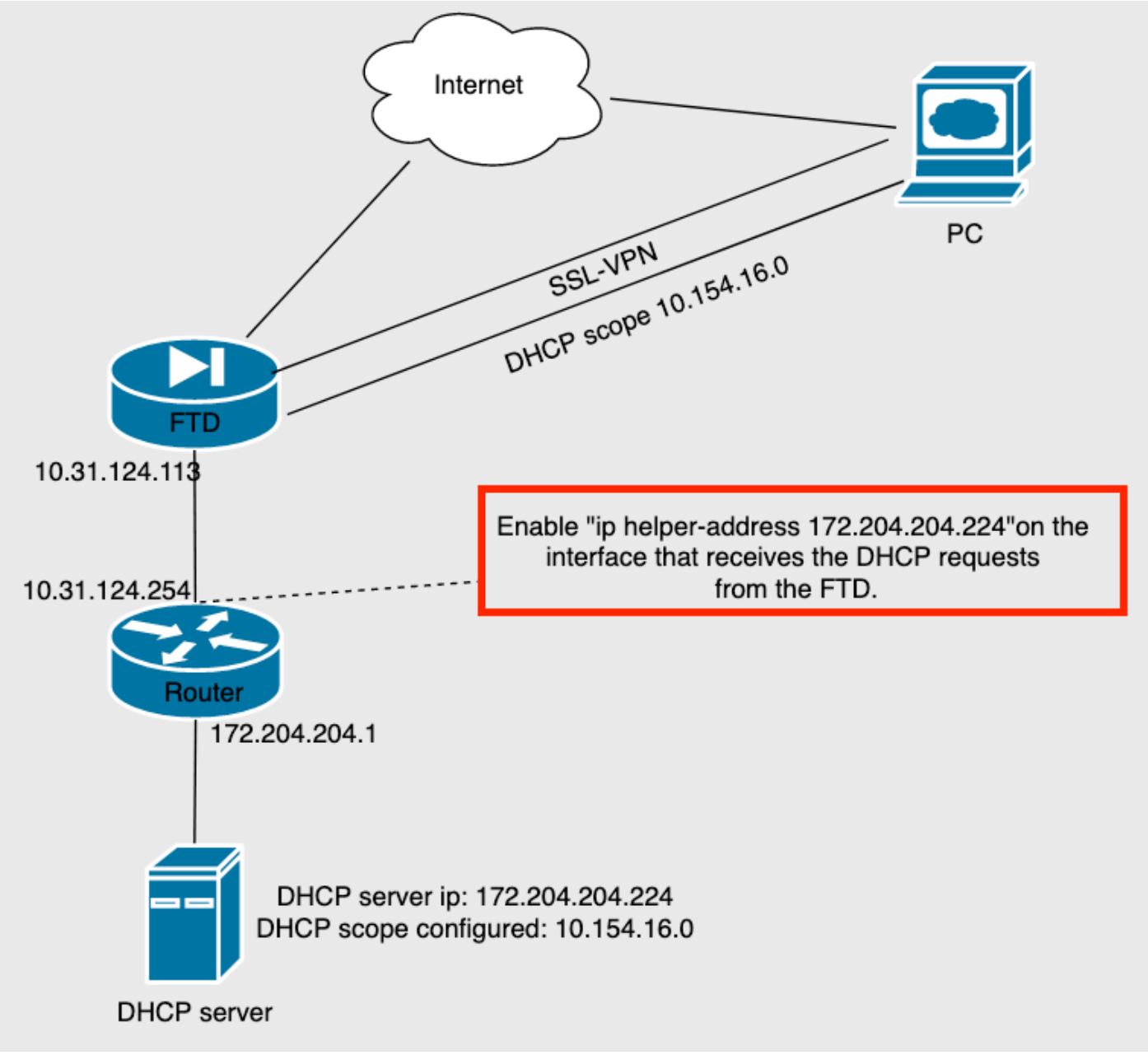


2. Enregistrez les modifications et déployez la configuration.

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.



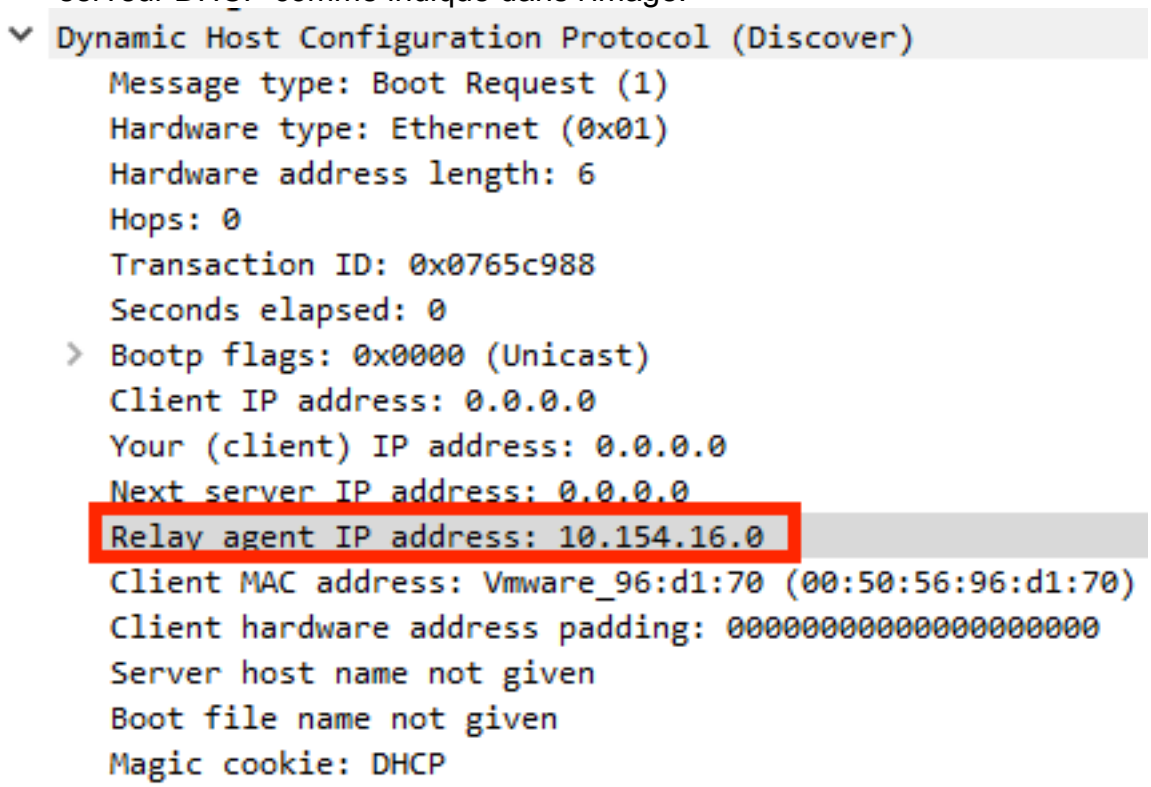
Vérification

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.



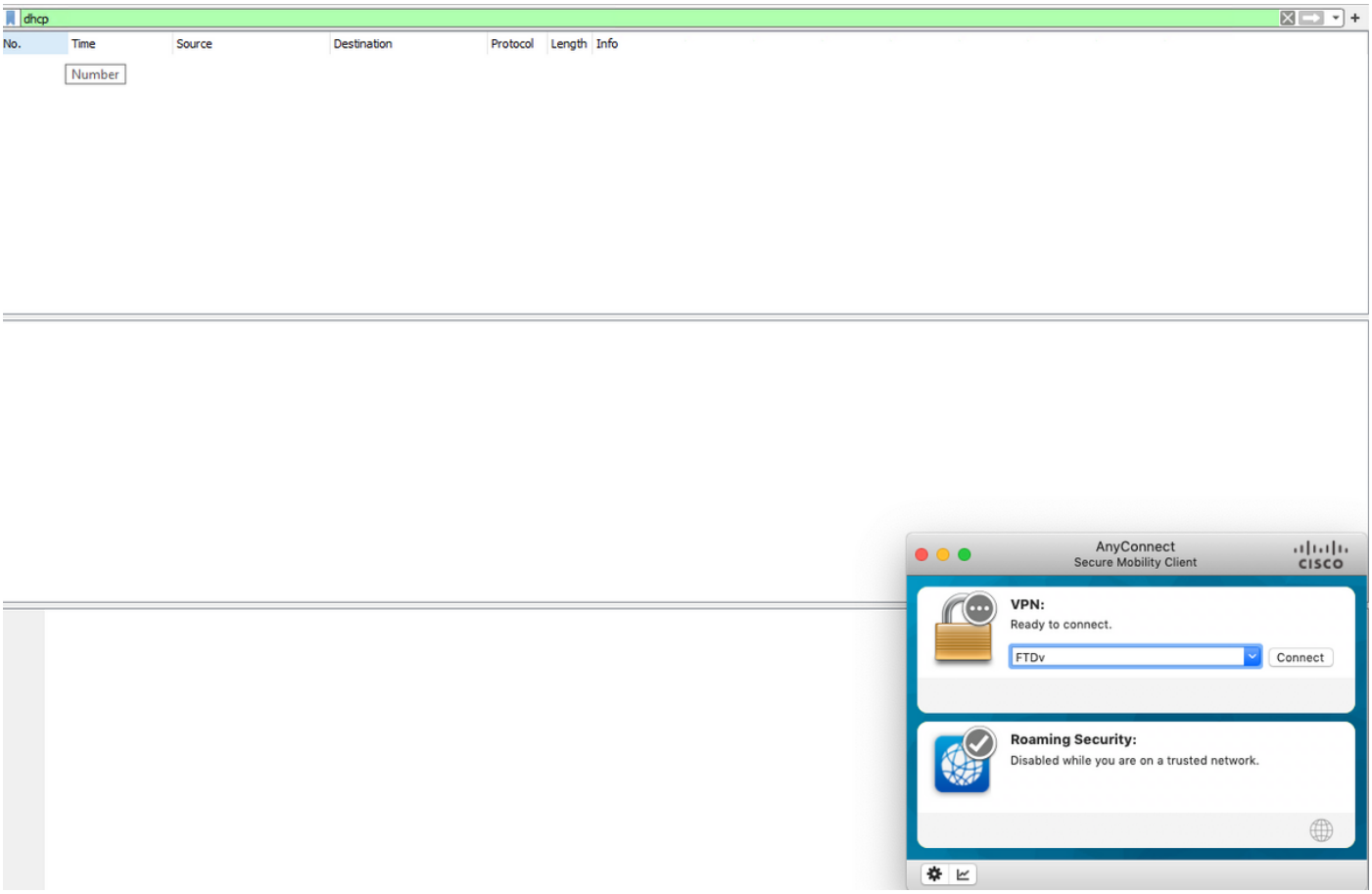
- Offre : Ce paquet est une réponse du serveur DHCP, qui vient avec la source du serveur DHCP et la destination de l'étendue DHCP dans le FTD.
- Demande : Il s'agit d'un paquet de monodiffusion envoyé de l'interface interne de FTD au serveur DHCP.
- ACK : Ce paquet est une réponse du serveur DHCP, qui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

Dépannage

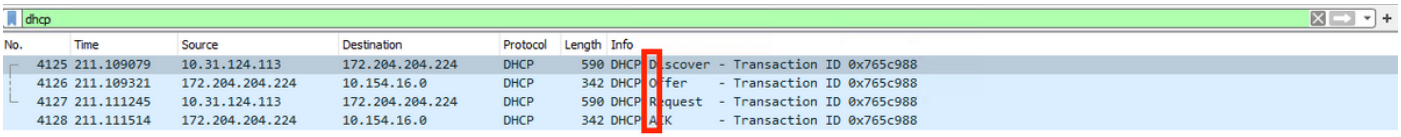
Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

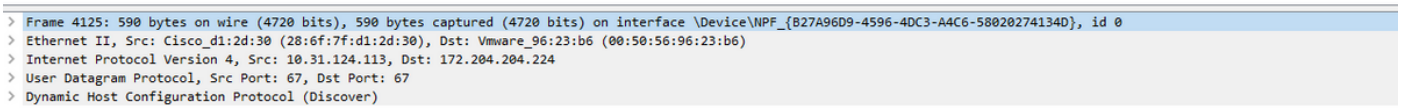
Étape 1. Téléchargez et activez Wireshark sur le serveur DHCP.

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



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





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