設定FTD上的Anyconnect VPN使用者端：用於地址分配的DHCP伺服器

目錄

簡介

本檔案將提供6.4版上的Firepower威脅防禦(FTD)組態範例，其中允許遠端存取VPN作業階段取得由第三方動態主機設定通訊協定(DHCP)伺服器指派的IP位址。

必要條件

需求

思科建議您瞭解以下主題：

- FTD
- Firepower管理中心(FMC)。
- DHCP

採用元件

本檔案中的資訊是根據以下軟體版本：

- FMC 6.5
- FTD 6.5
- Windows Server 2016

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

本檔案將不會說明整個遠端存取組態，而只是FTD中從本機位址池變更為DHCP位址指定所需的組態。

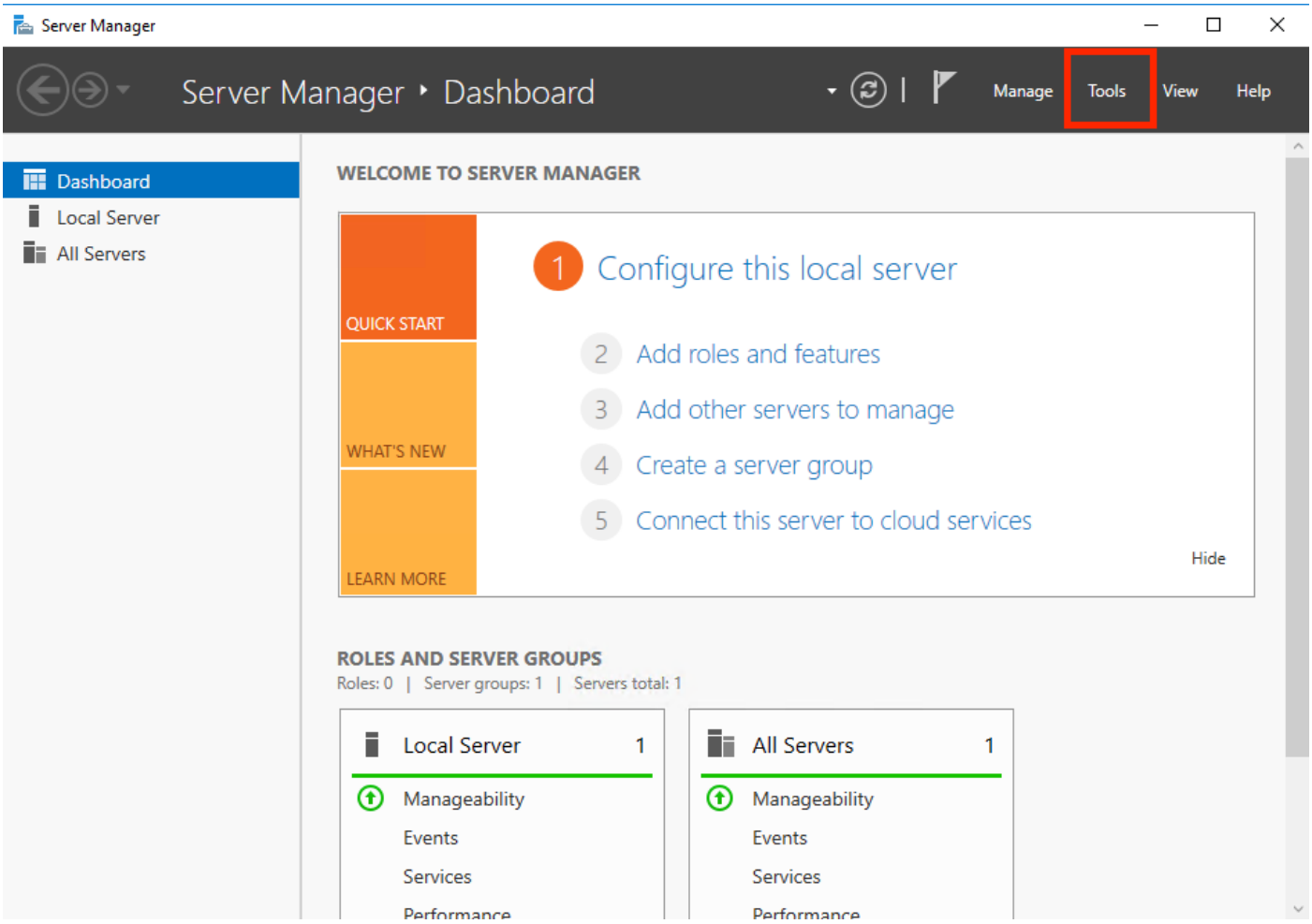
如果您正在查詢Anyconnect配置示例文檔，請參閱「在FTD上配置AnyConnect VPN客戶端：髮型和NAT免除」文檔。

設定

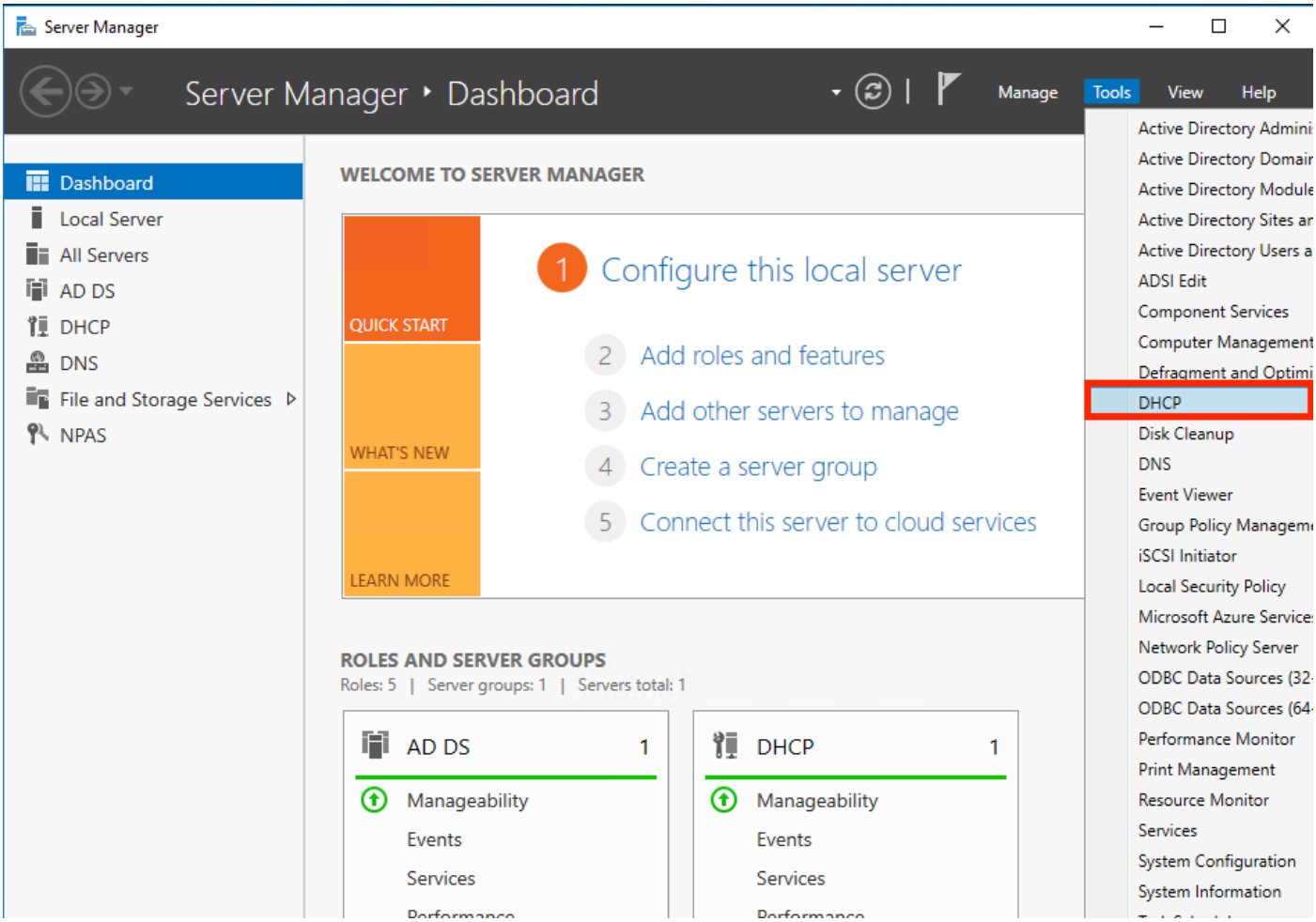
步驟1.在DHCP伺服器中配置DHCP作用域

在此案例中，DHCP伺服器位於FTD的內部介面後面。

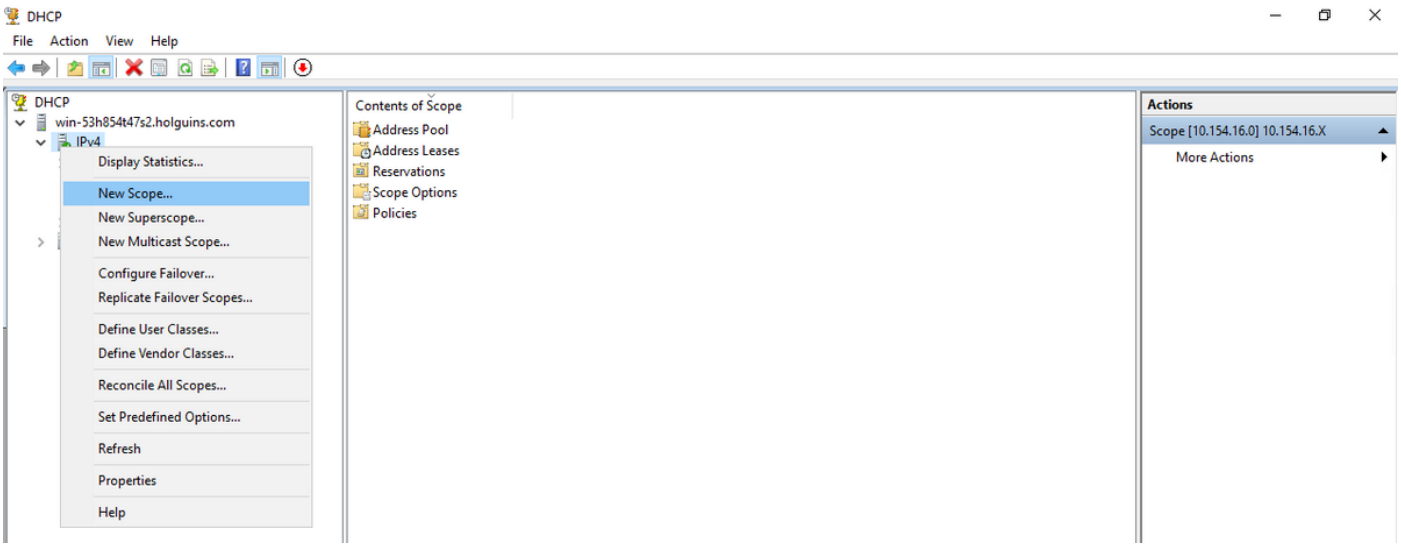
1.在Windows伺服器中開啟「伺服器管理器」，然後選擇**「工具」**，如下圖所示。



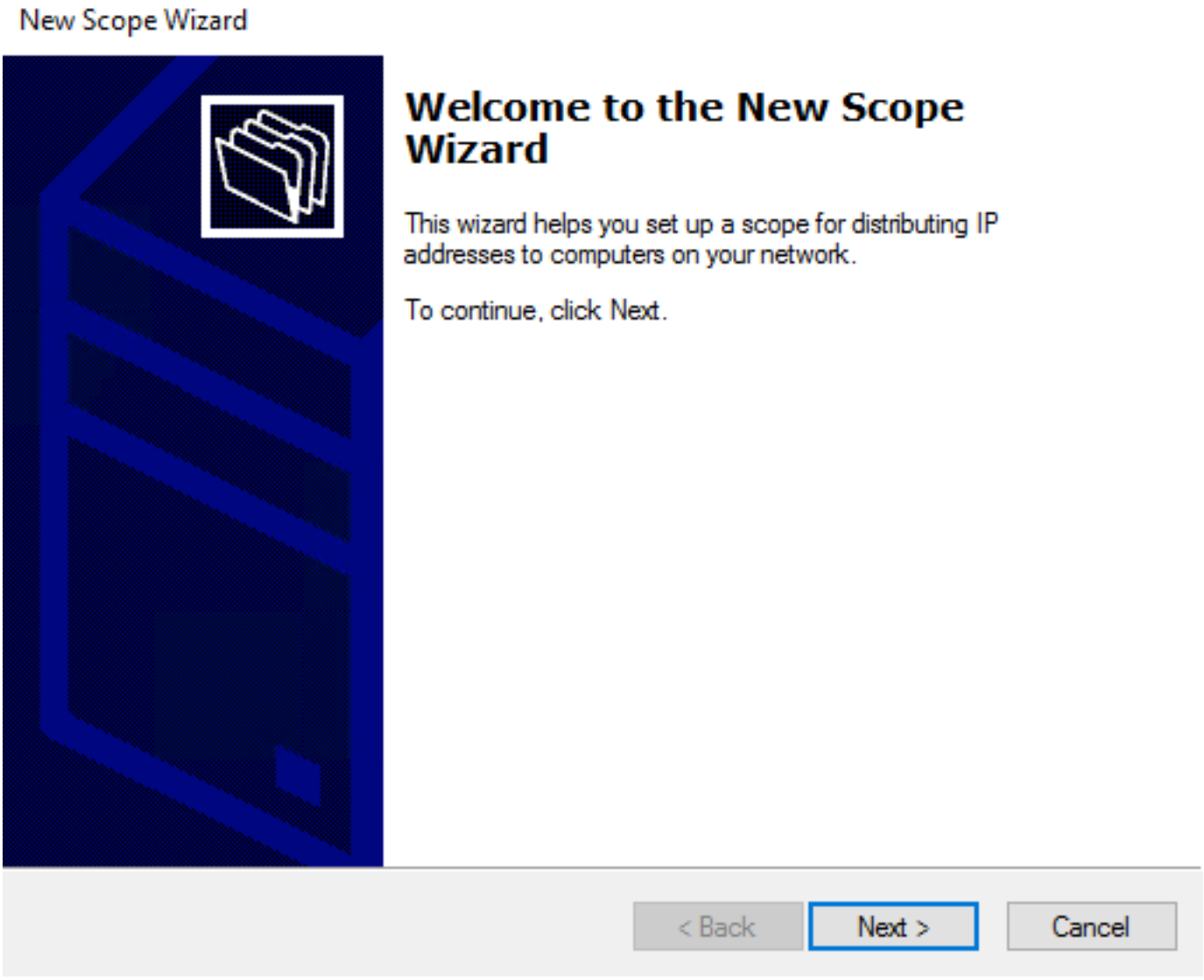
2.選擇DHCP:



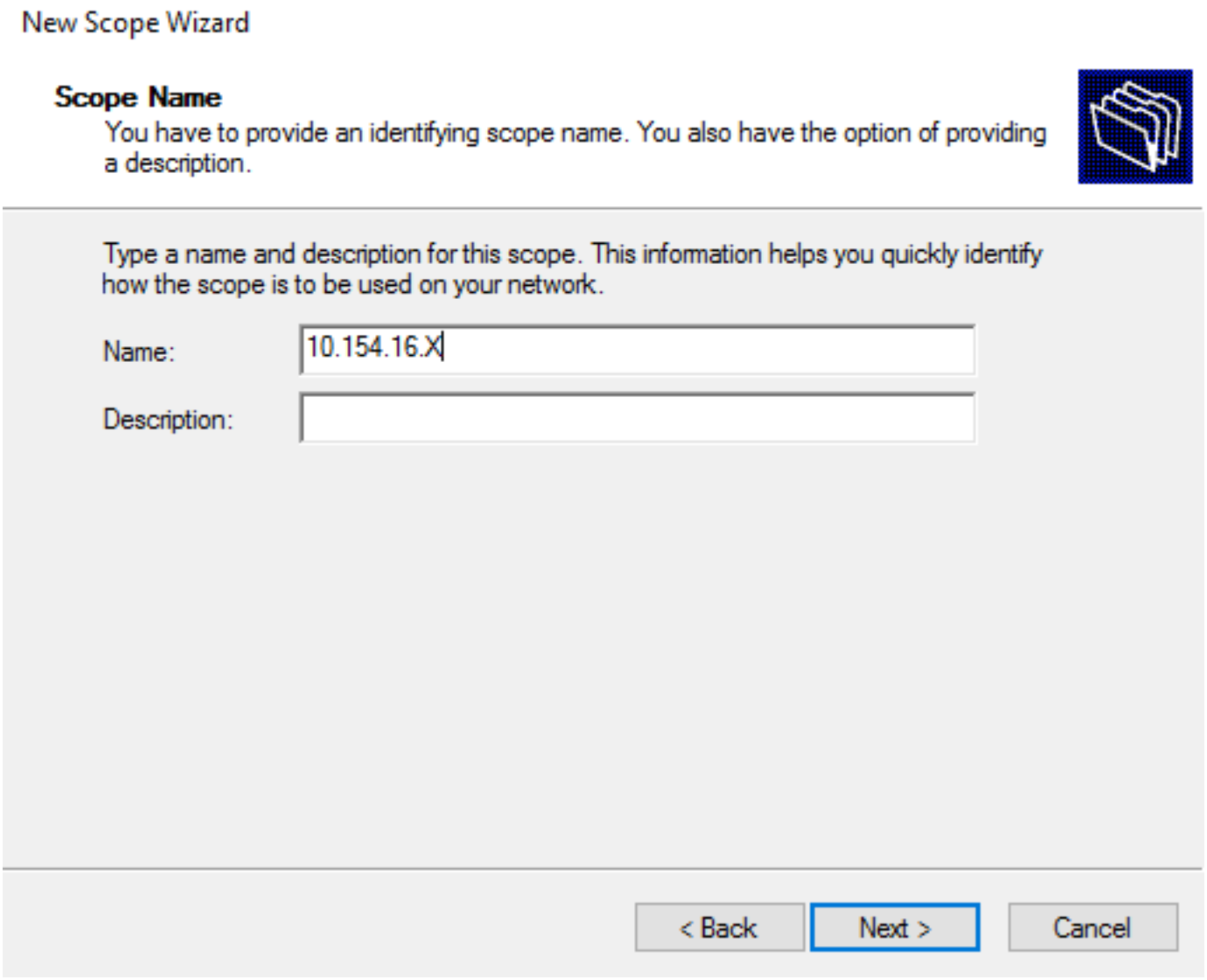
3.選擇IPv4，按一下右鍵並選擇**New Scope**，如下圖所示。



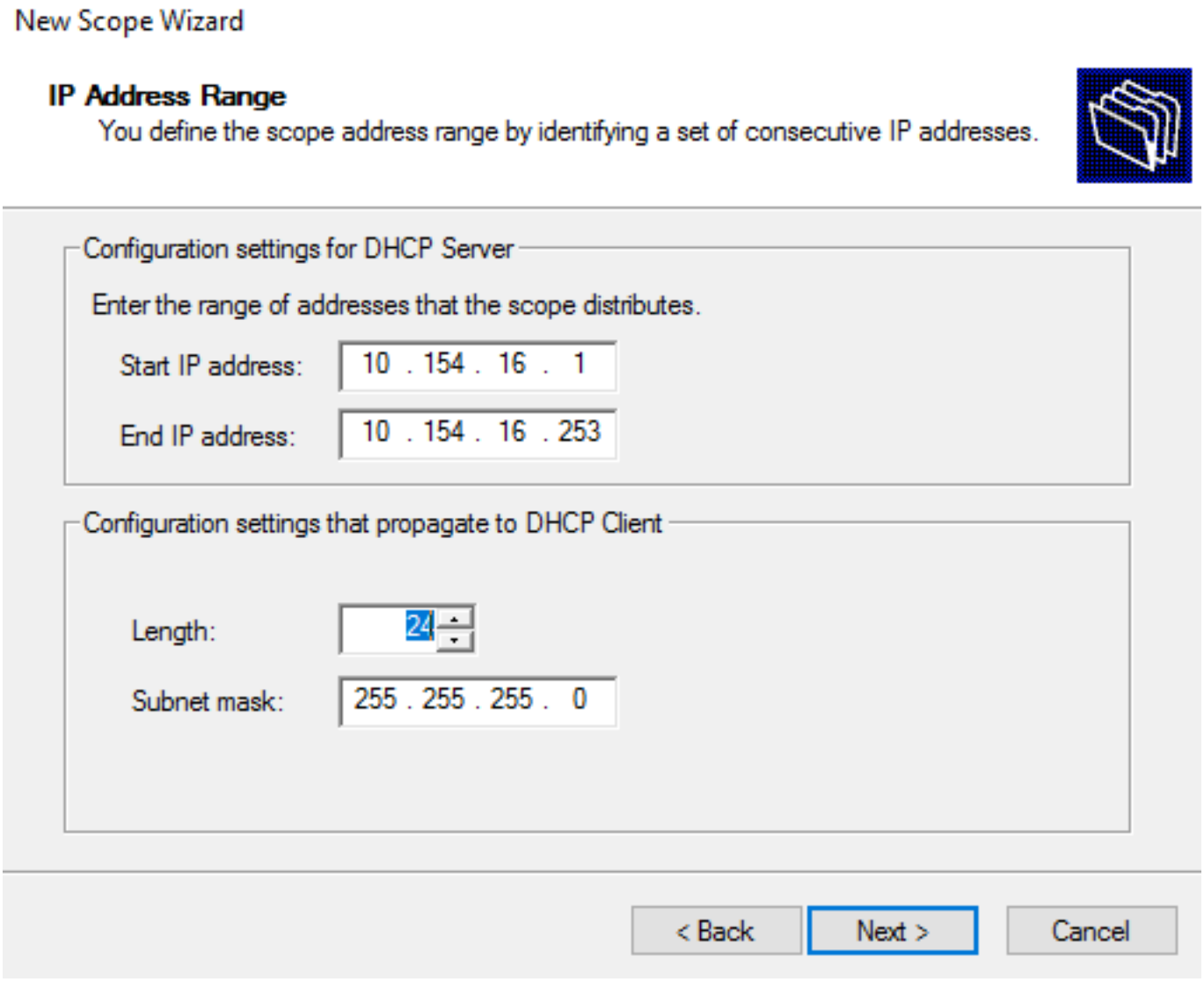
4.按照**嚮導**操作，如下圖所示。



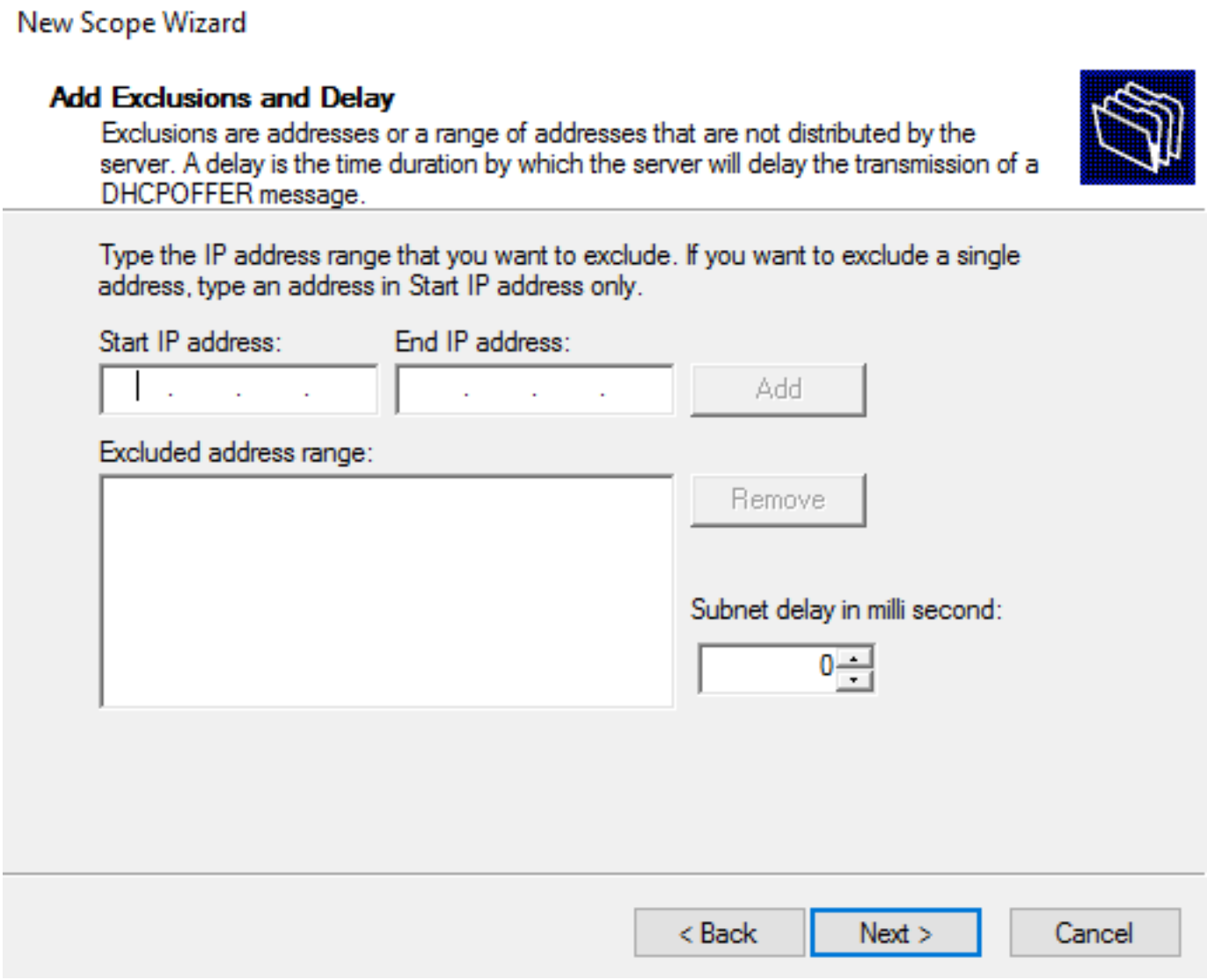
5.為作用域指定一個名稱，如下圖所示。



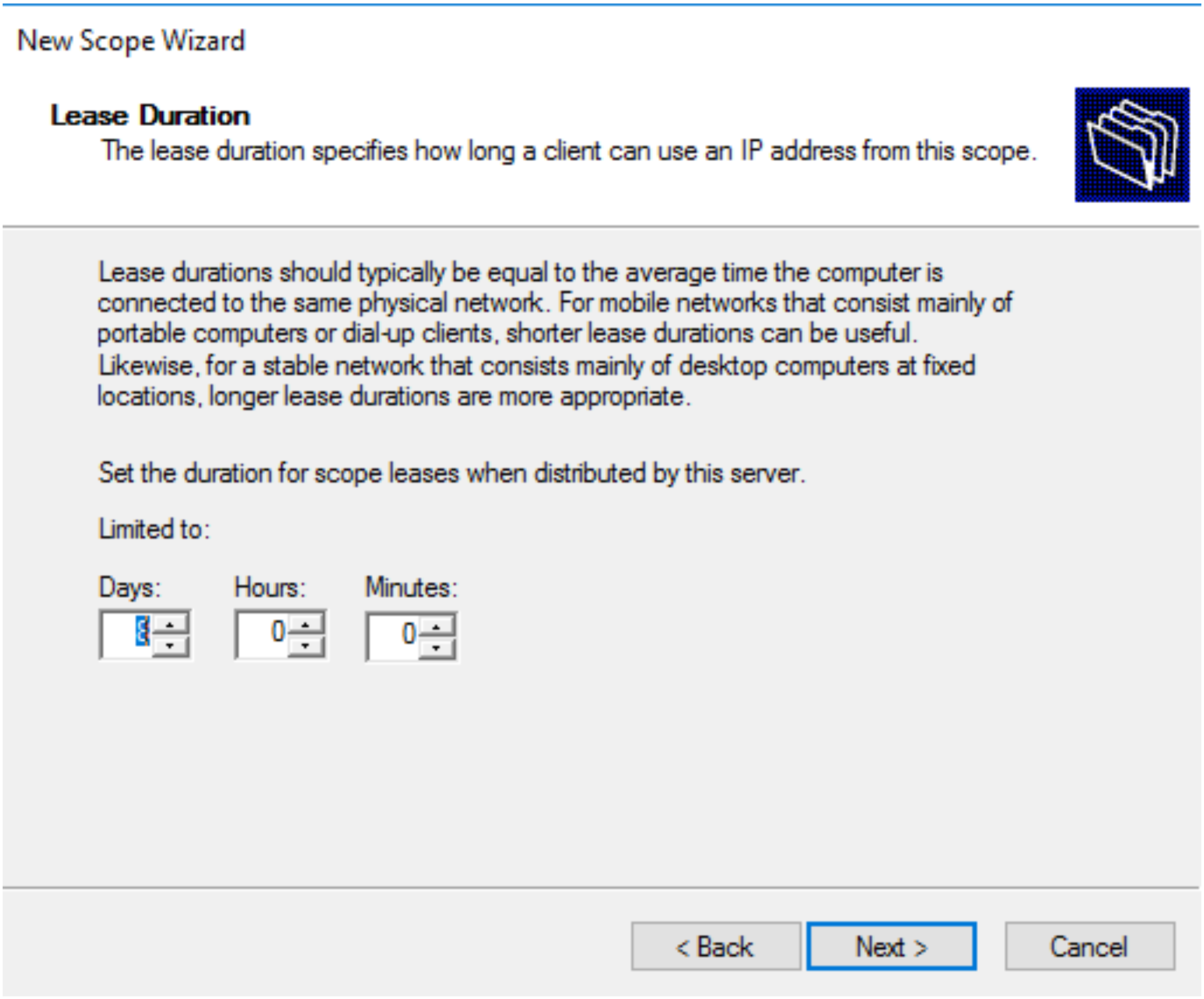
6.設定位址範圍，如下圖所示。



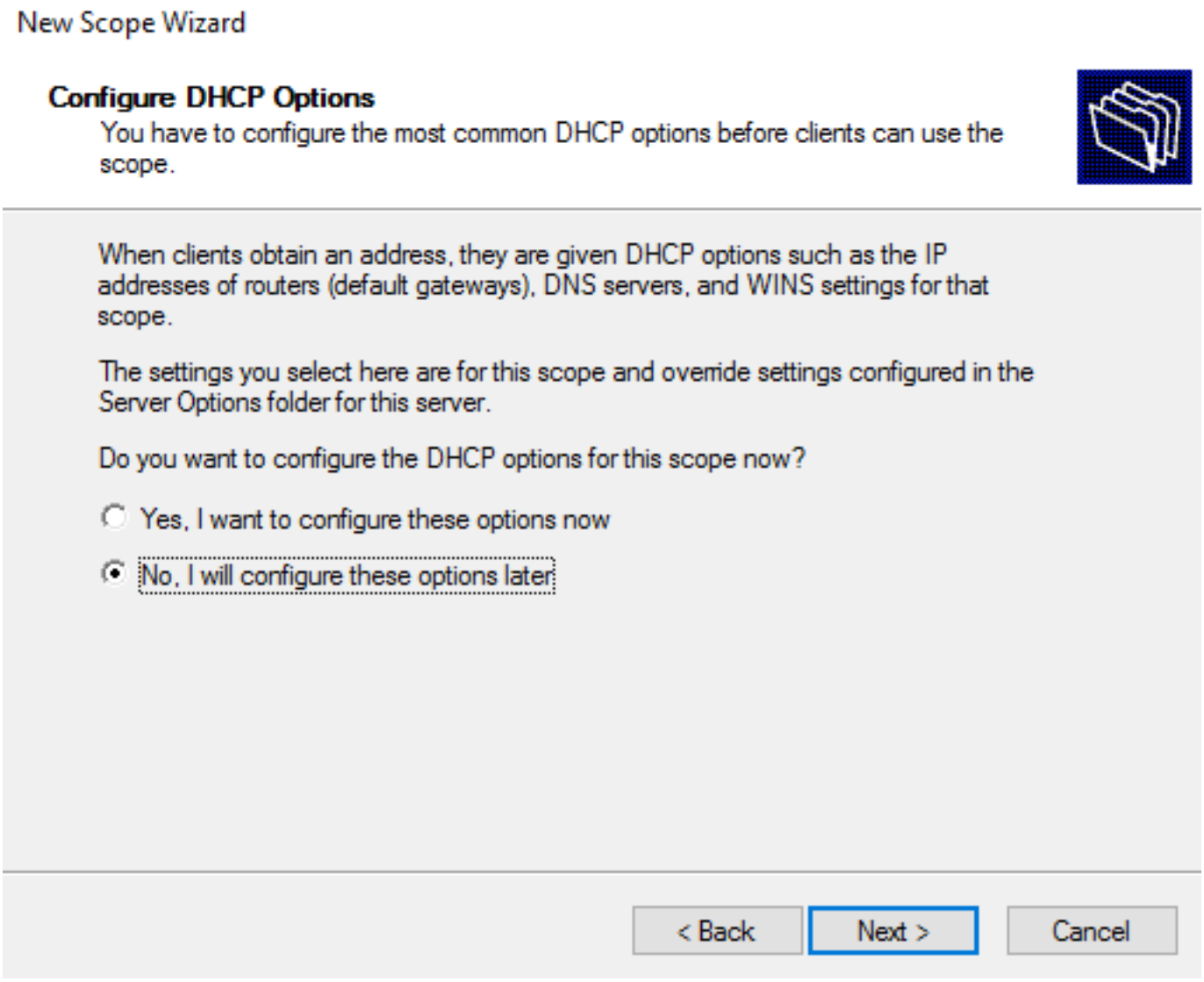
7.（可選）設定排除，如下圖所示。



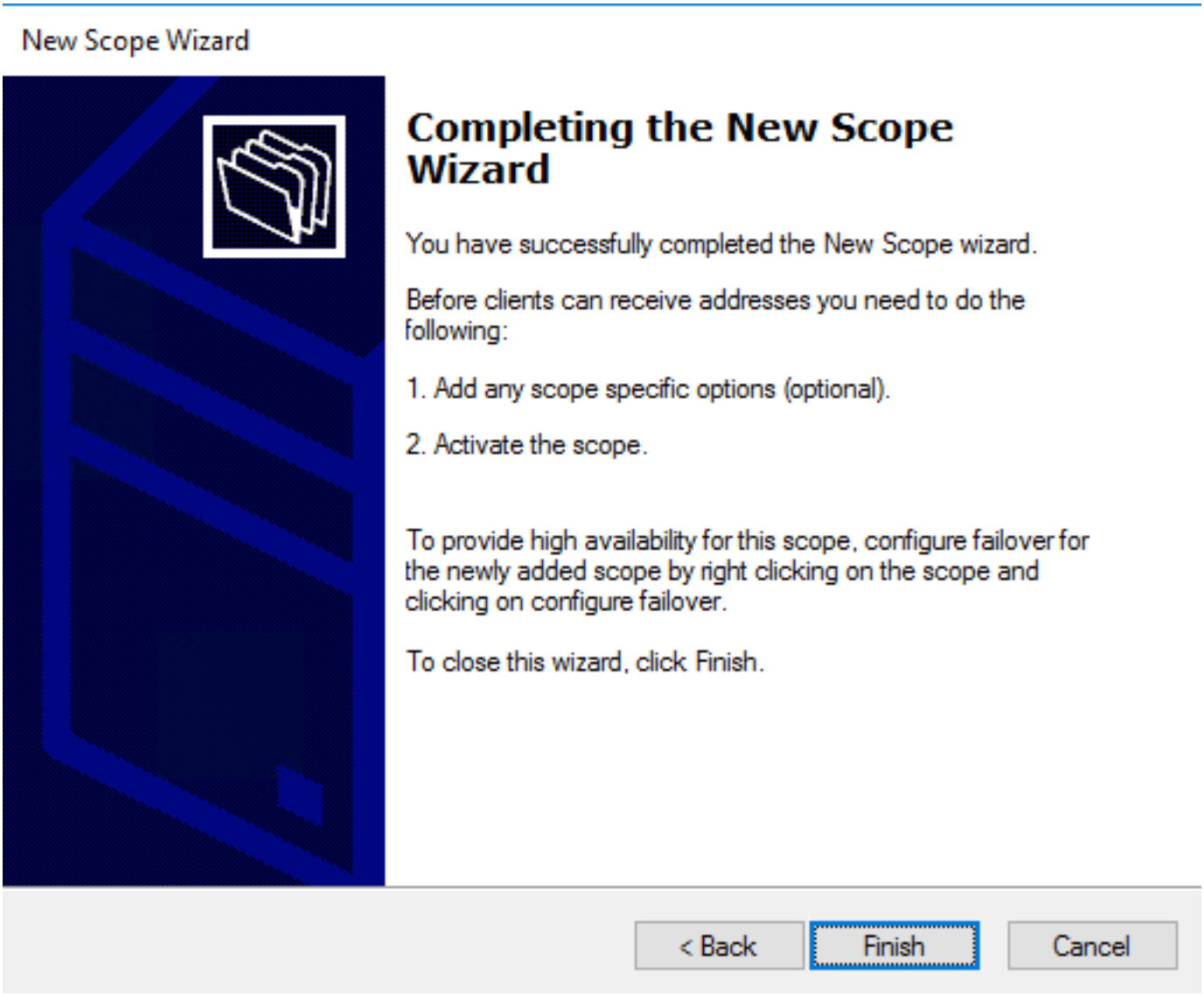
8.配置**租用期限**，如下圖所示。



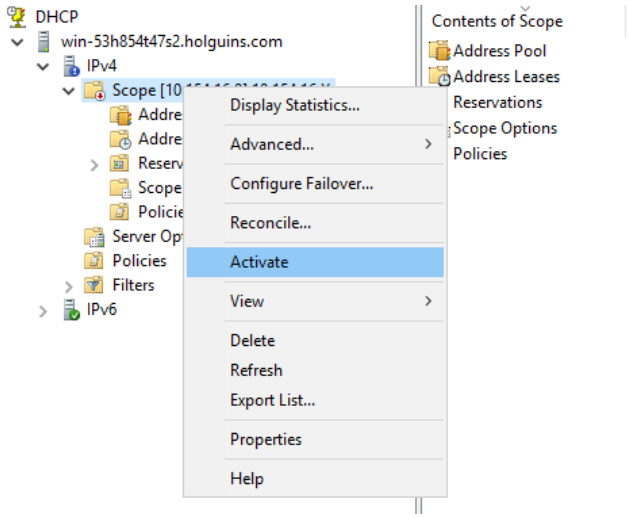
9.（可選）配置DHCP作用域選項：



10:選擇**完成**，如下圖所示。



11:在剛建立的範圍內按一下右鍵，然後選擇**Activate**，如下圖所示。



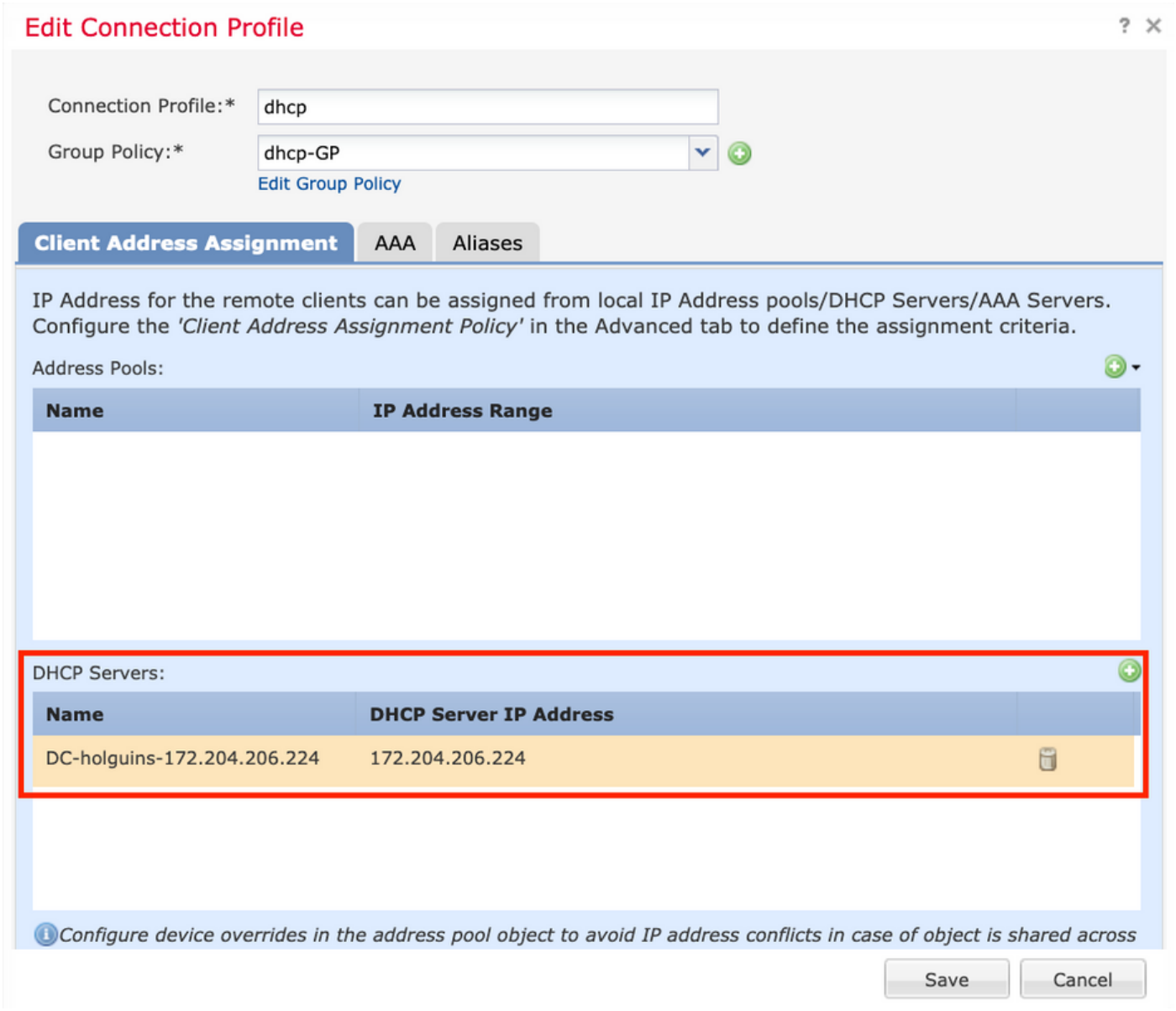
步驟2.配置Anyconnect

配置並啟用DHCP作用域後，下一個過程將在FMC中進行。

步驟2.1.配置連線配置檔案

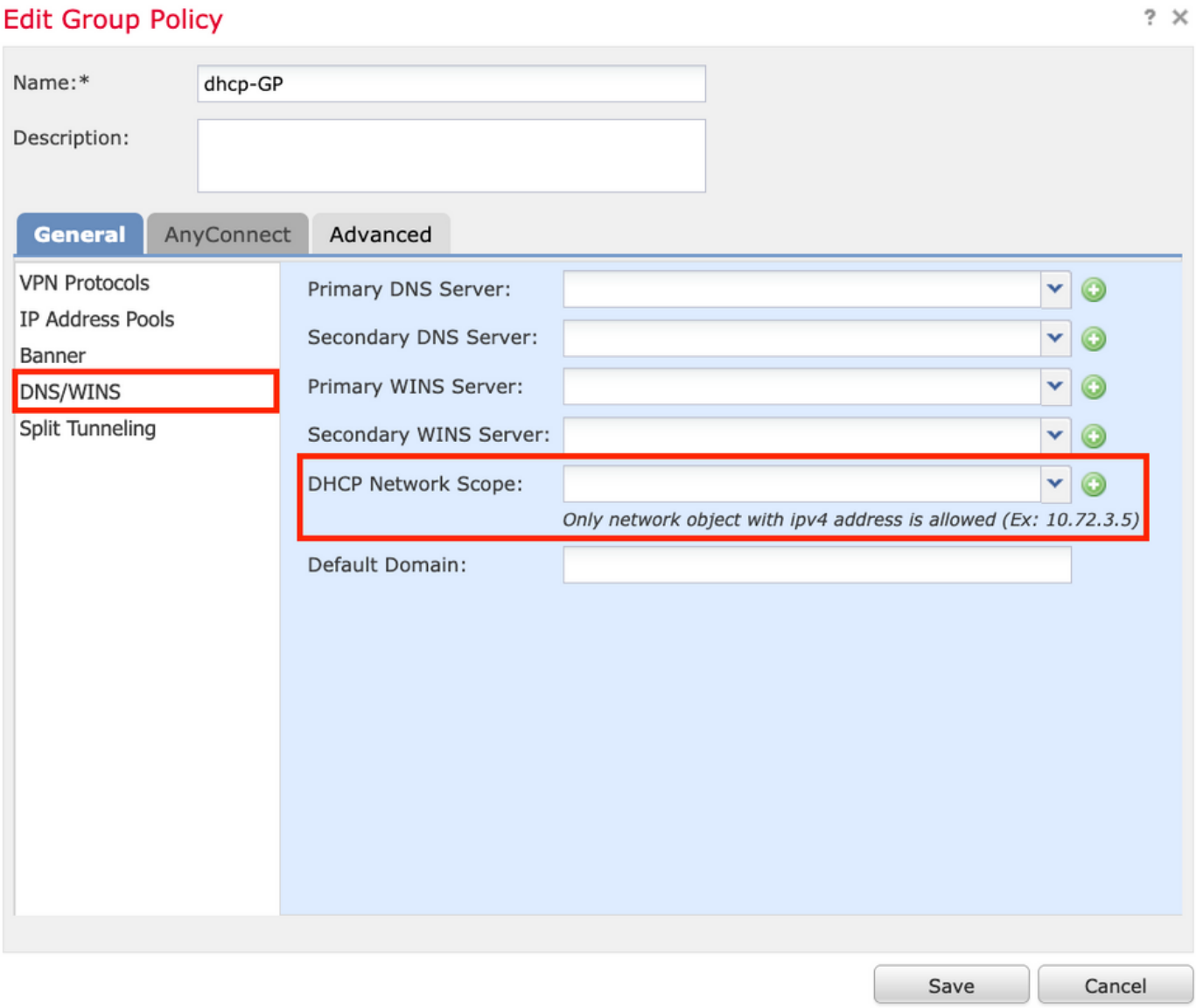
1.在DHCP伺服器部分，選擇  符號並使用DHCP伺服器的IP地址建立對象。

2.選擇對象作為DHCP伺服器，以便從中請求IP地址，如下圖所示。



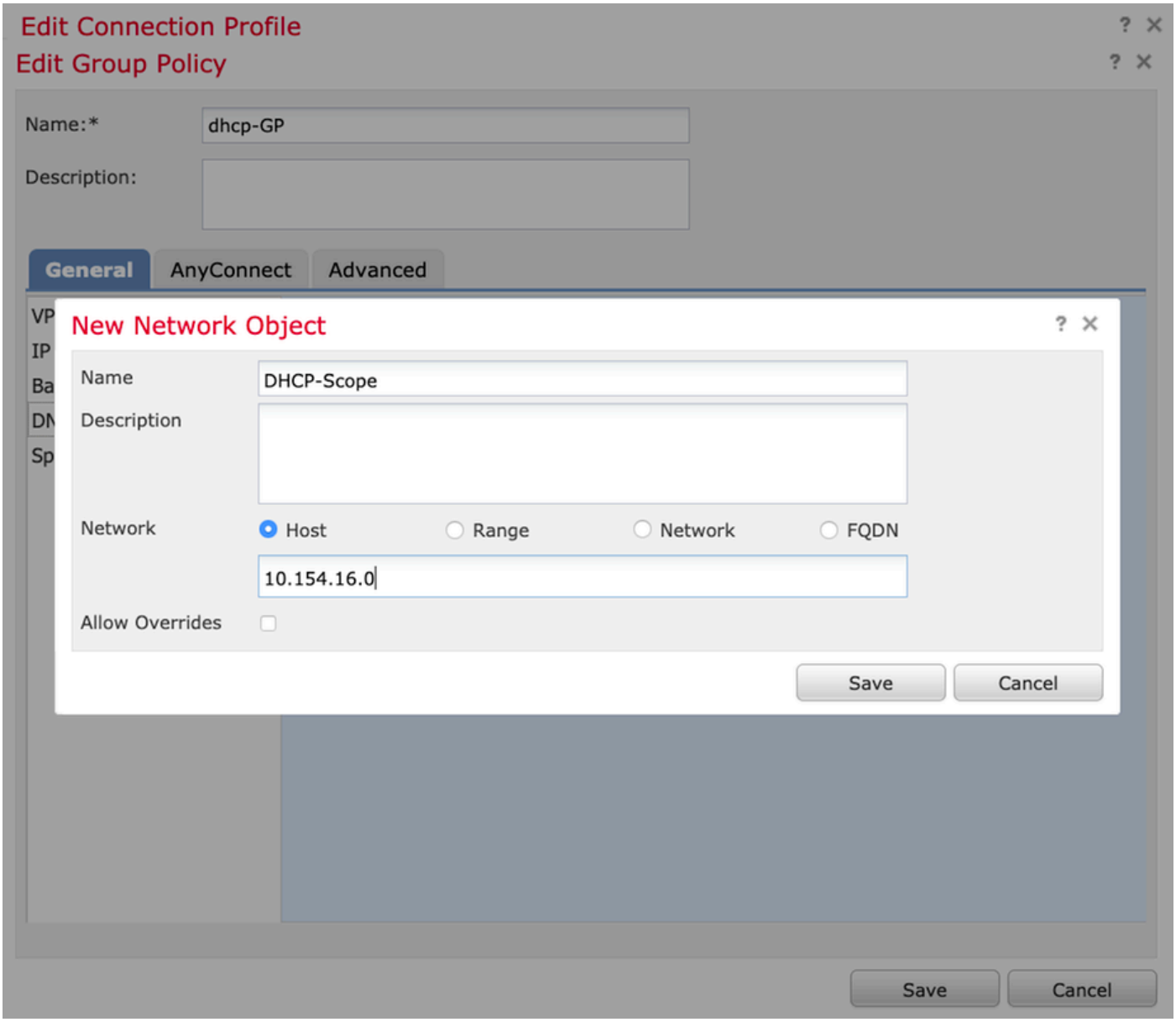
步驟2.2.配置組策略

1.在Group Policy選單中，導航到**General > DNS/WINS**，有一個**DHCP Network Scope**部分，如下圖所示。

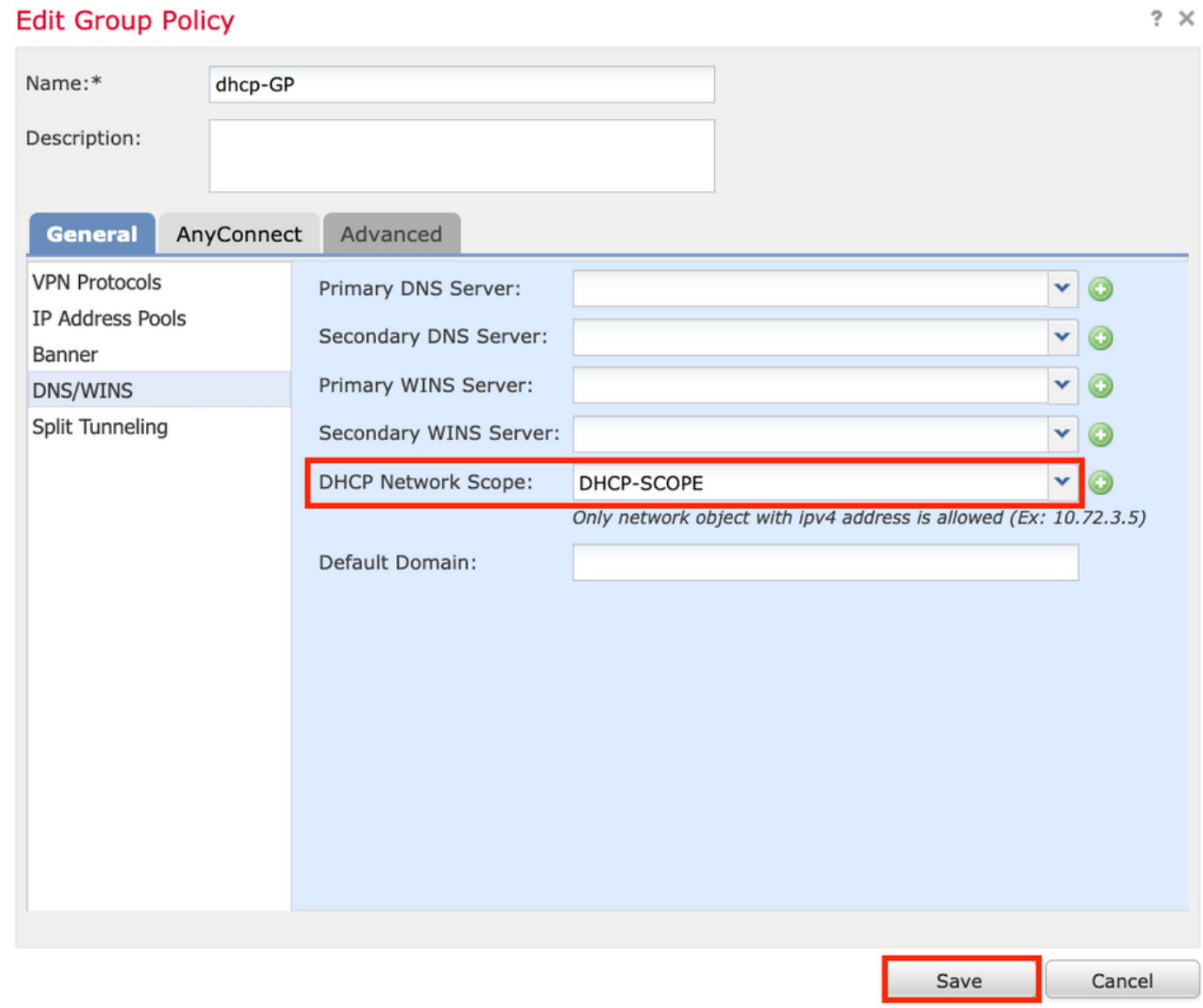


2.建立新對象，該對象必須與DHCP伺服器具有相同的網路範圍。

附註：

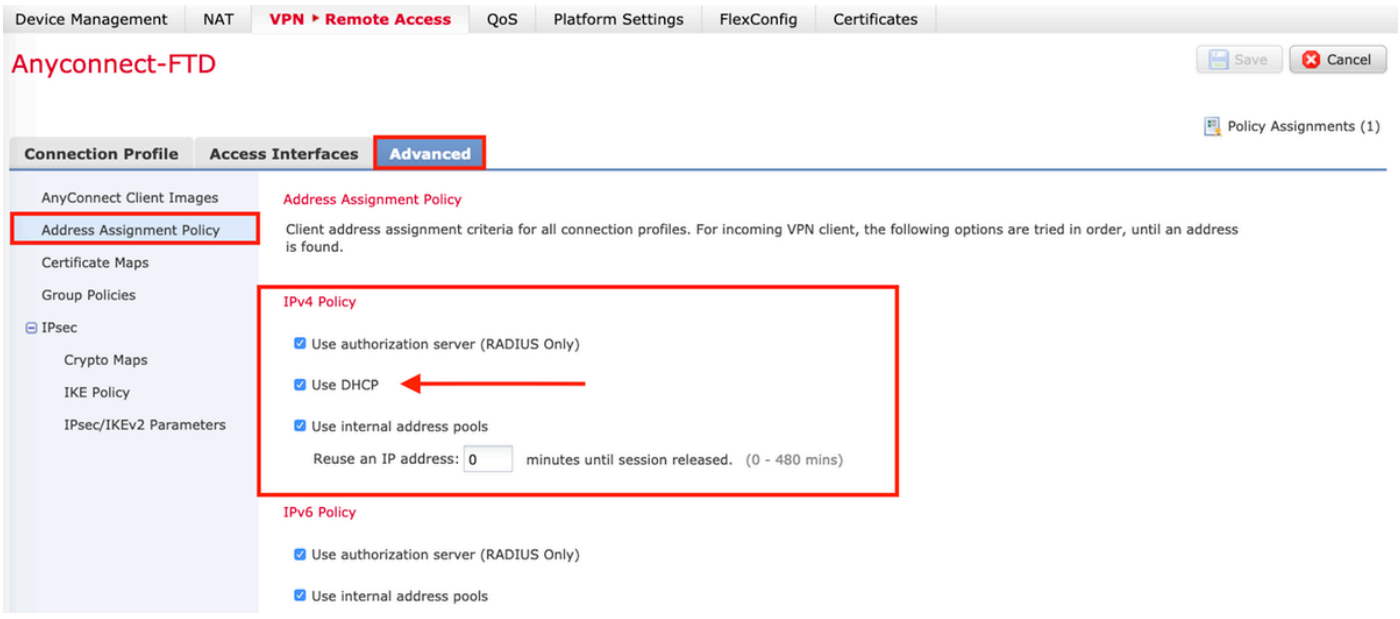


3.選擇DHCP作用域對象，然後選擇**Save**，如下圖所示。



步驟2.3.配置地址分配策略

1.導覽至Advanced > Address Assignment Policy，確保Use DHCP選項已切換，如下圖所示。

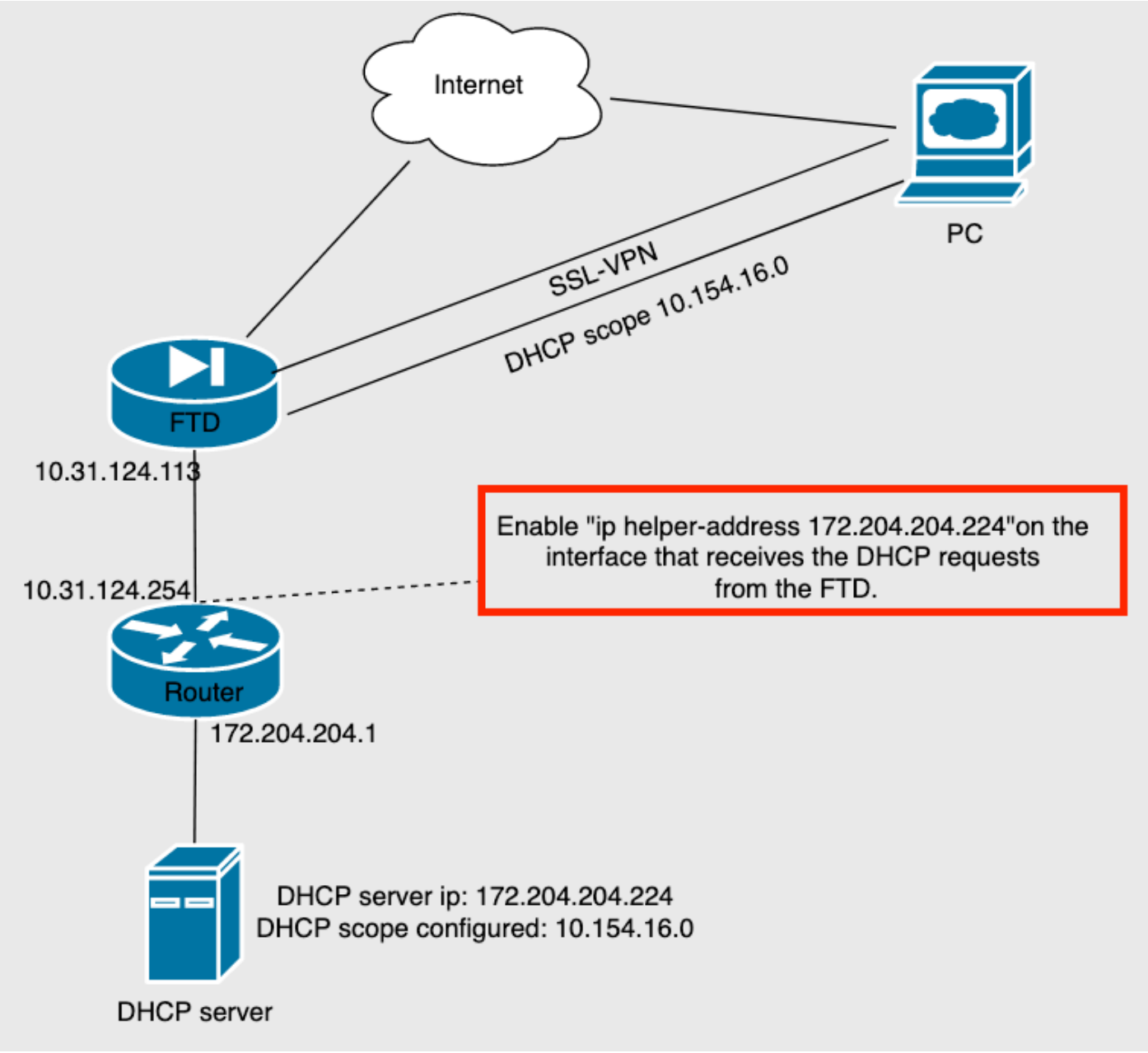


2.儲存更改並部署配置。

IP協助程式案例

當DHCP伺服器位於區域網路(LAN)中的另一個路由器後面時，需要「IP協助程式」將要求轉送到DHCP伺服器。

如圖所示，拓撲圖說明了場景以及網路中的必要更改。

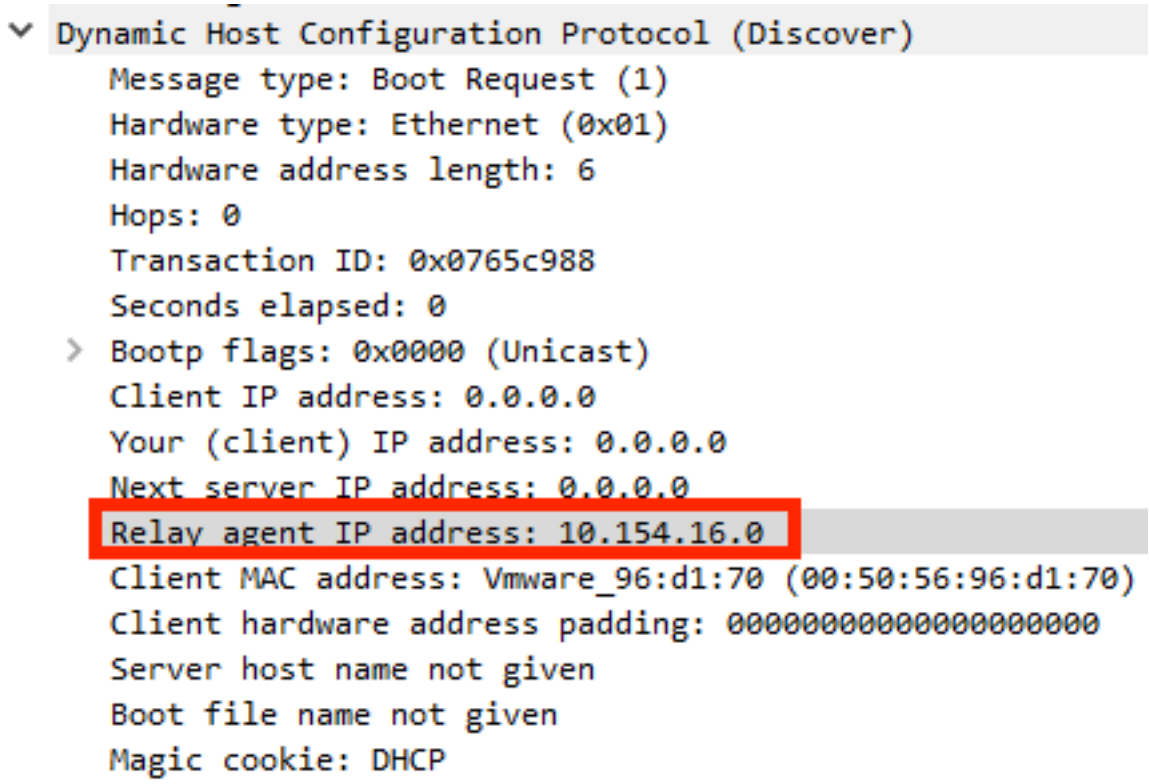


驗證

使用本節內容，確認您的組態是否正常運作。

本節介紹FTD和DHCP伺服器之間交換的DHCP封包。

- 發現：這是從FTD的內部介面傳送到DHCP伺服器的單點傳播封包。 在負載中，**中繼代理IP地址**指定DHCP伺服器的範圍，如下圖所示。



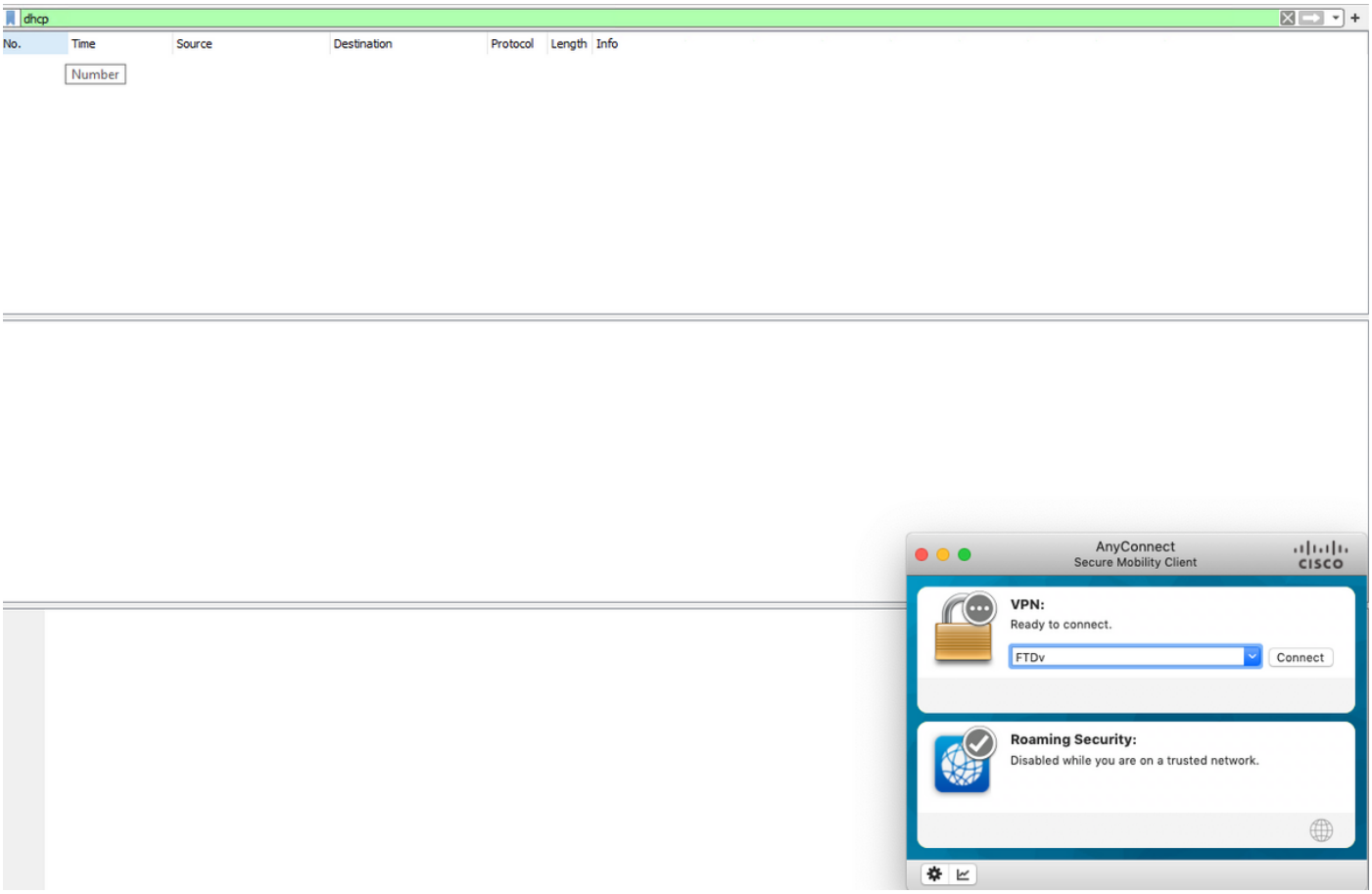
- 產品：此封包是來自DHCP伺服器的回應，並隨DHCP伺服器來源和FTD中DHCP作用域的目的地一起提供。
- 請求：這是從FTD的內部介面傳送到DHCP伺服器的單點傳播封包。
- ACK:此封包是來自DHCP伺服器的回應，並隨DHCP伺服器來源和FTD中DHCP作用域的目的地一起提供。

疑難排解

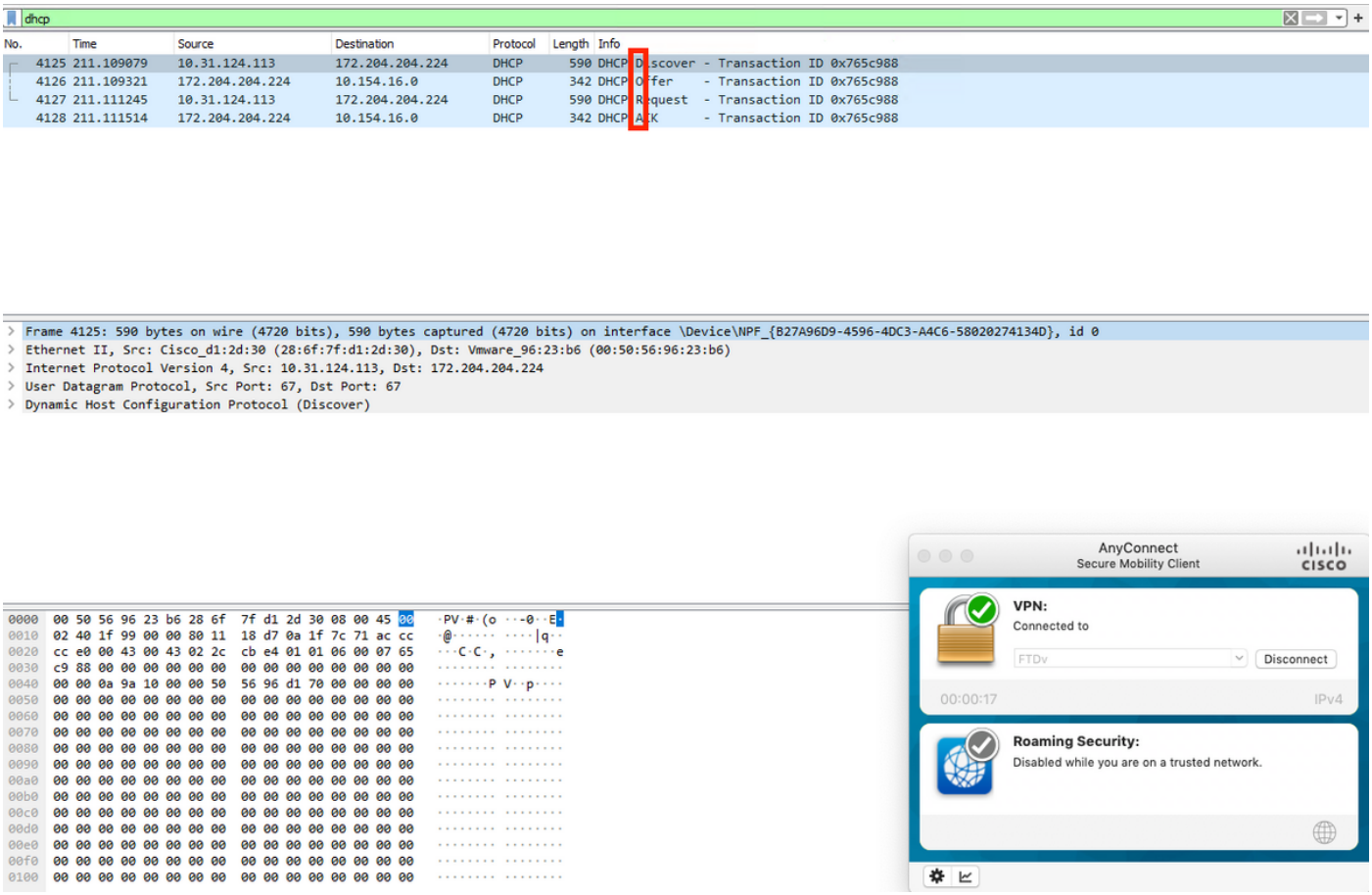
本節提供的資訊可用於對組態進行疑難排解。

步驟1.在DHCP伺服器中下載並啟用wireshark。

步驟2.應用DHCP作為捕獲過濾器，如下圖所示。



步驟3.登入到Anyconnect，DHCP協商應該如下圖所示。



相關資訊

- 此影片提供了FTD的配置示例，允許遠端訪問VPN會話獲取由第三方DHCP伺服器分配的IP地址。
- 技術支援與文件 - Cisco Systems