

# 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](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[步驟1.在DHCP伺服器中配置DHCP作用域](#)

[步驟2.配置Anyconnect](#)

[步驟2.1.配置連線配置檔案](#)

[步驟2.2.配置組策略](#)

[步驟2.3.配置地址分配策略](#)

[IP協助程式案例](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 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。

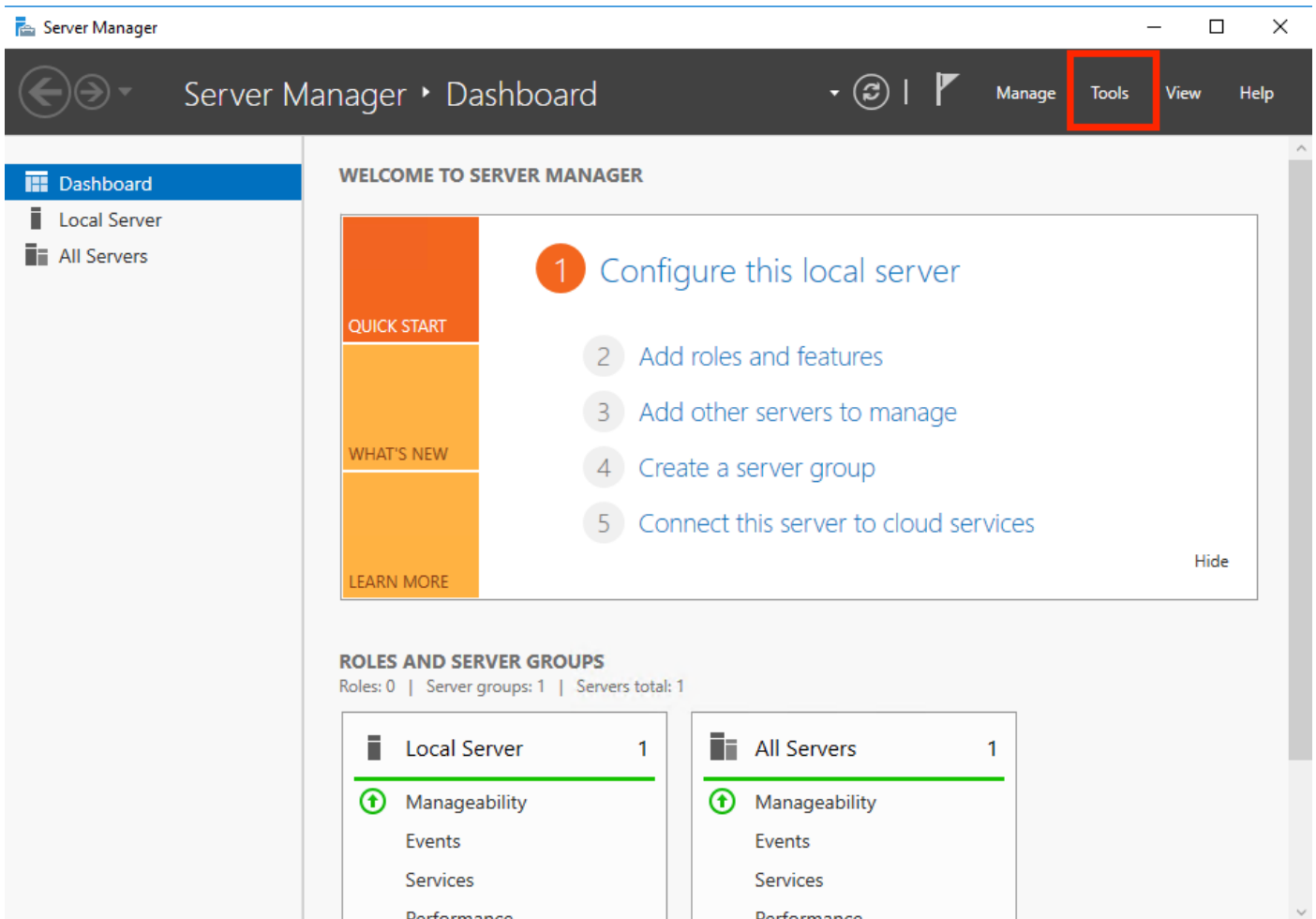
如果您正在查詢Anyconnect配置示例文檔，請參閱「在FTD上配置AnyConnect VPN客戶端：髮型和NAT免除」文檔。

## 設定

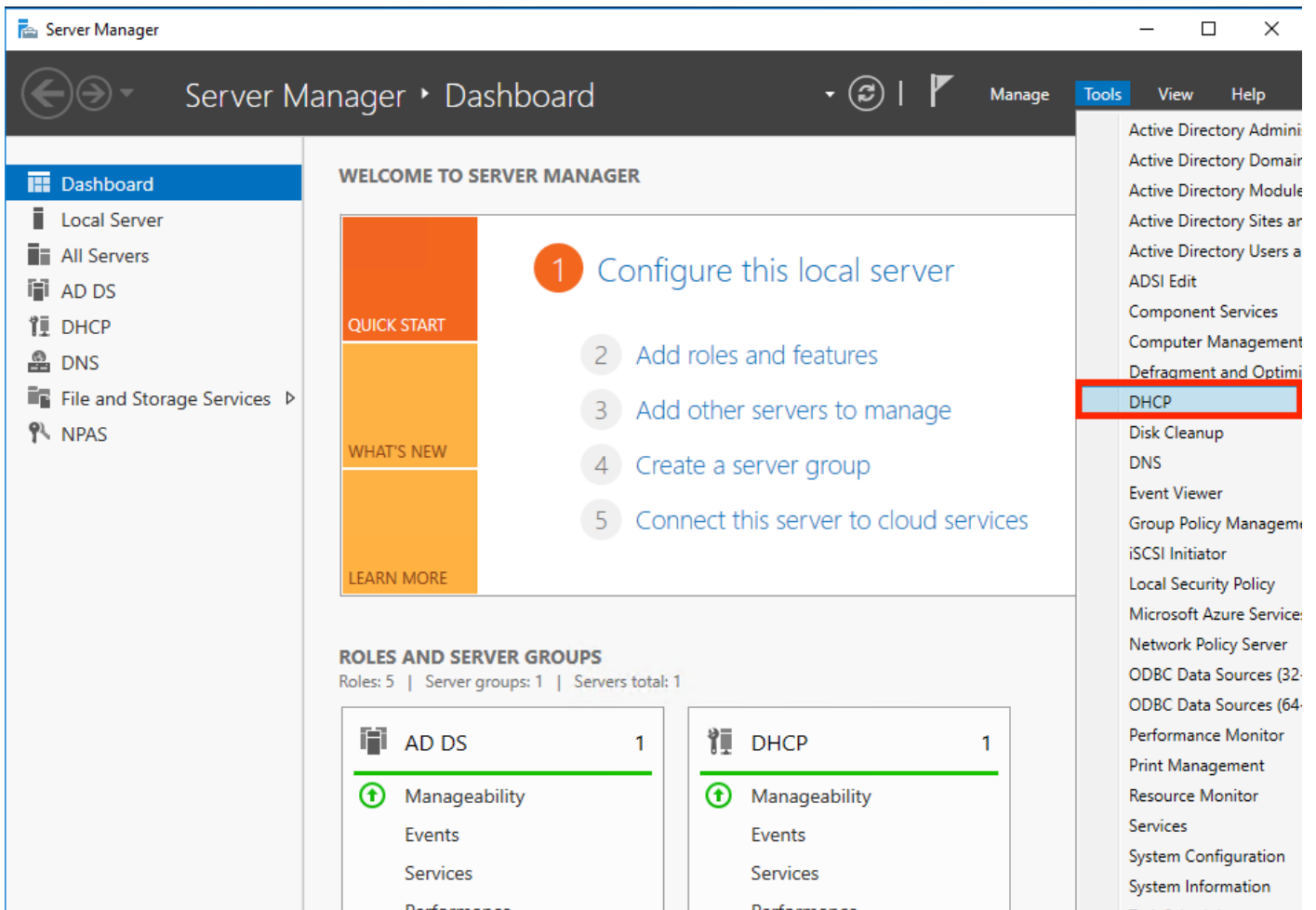
### 步驟1.在DHCP伺服器中配置DHCP作用域

在此案例中，DHCP伺服器位於FTD的內部介面後面。

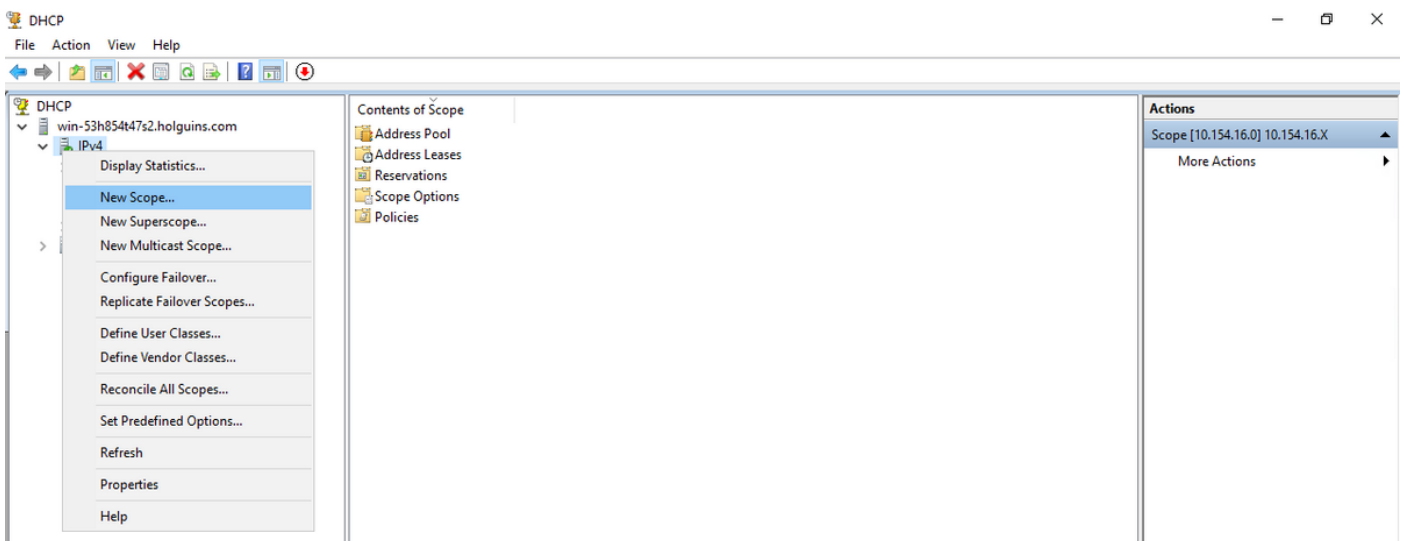
1.在Windows伺服器中開啟「伺服器管理器」，然後選擇「工具」，如下圖所示。



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。

## 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. 為作用域指定一個名稱，如下圖所示。

## 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.設定位址範圍，如下圖所示。

## 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. ( 可選 ) 設定排除，如下圖所示。

## 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. 配置租用期限，如下圖所示。

## 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. ( 可選 ) 配置DHCP作用域選項 :



## 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:選擇完成，如下圖所示。

## 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.

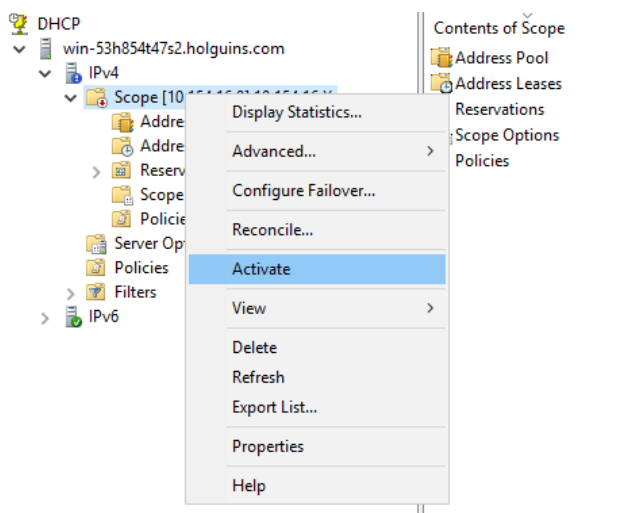
To close this wizard, click Finish.

< Back

Finish

Cancel


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



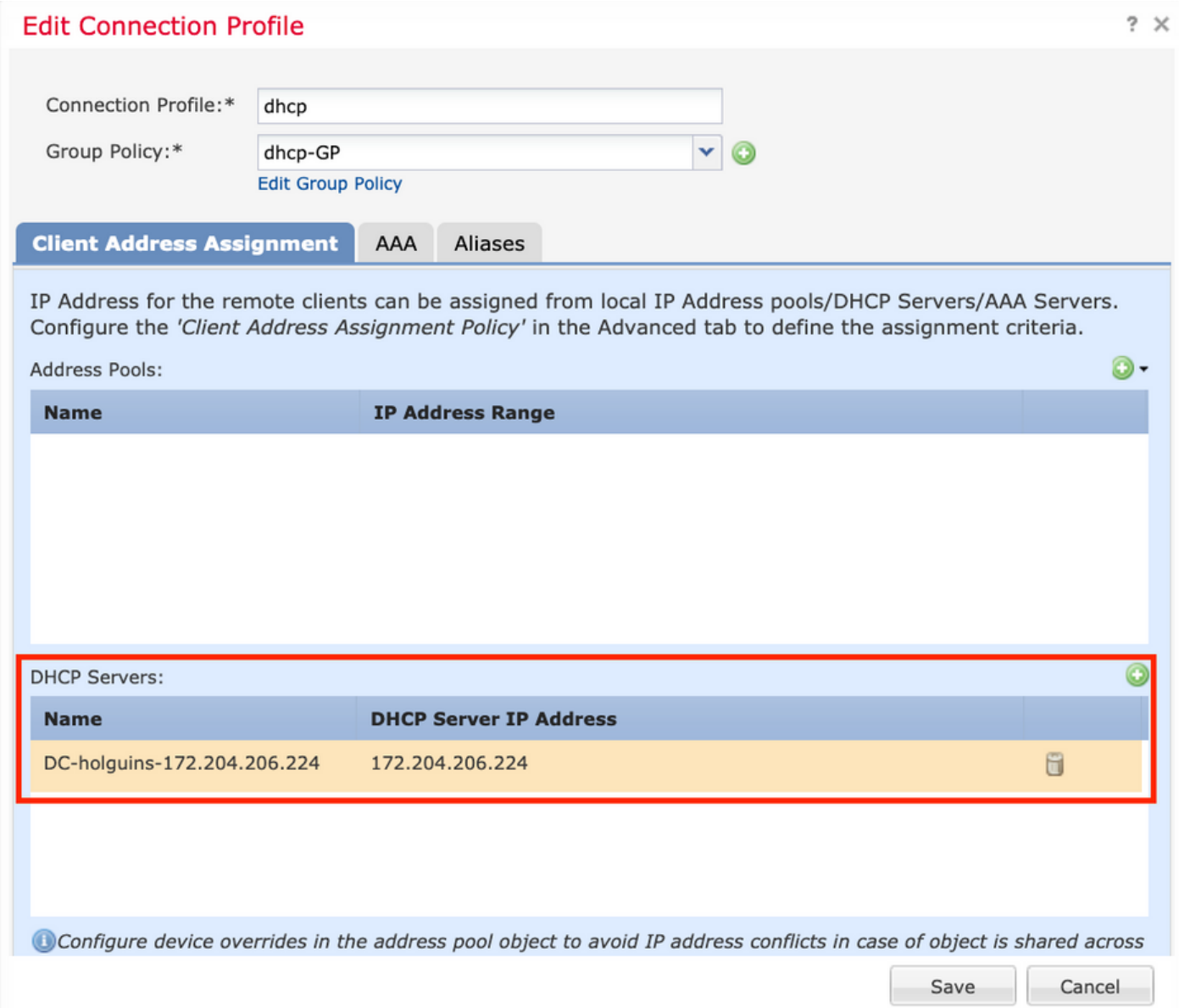
## 步驟2.配置Anyconnect

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。




**Edit Connection Profile** ? X

Connection Profile:\* dhcp


Group Policy:\* dhcp-GP  [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*

Save Cancel

## 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。

## 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:

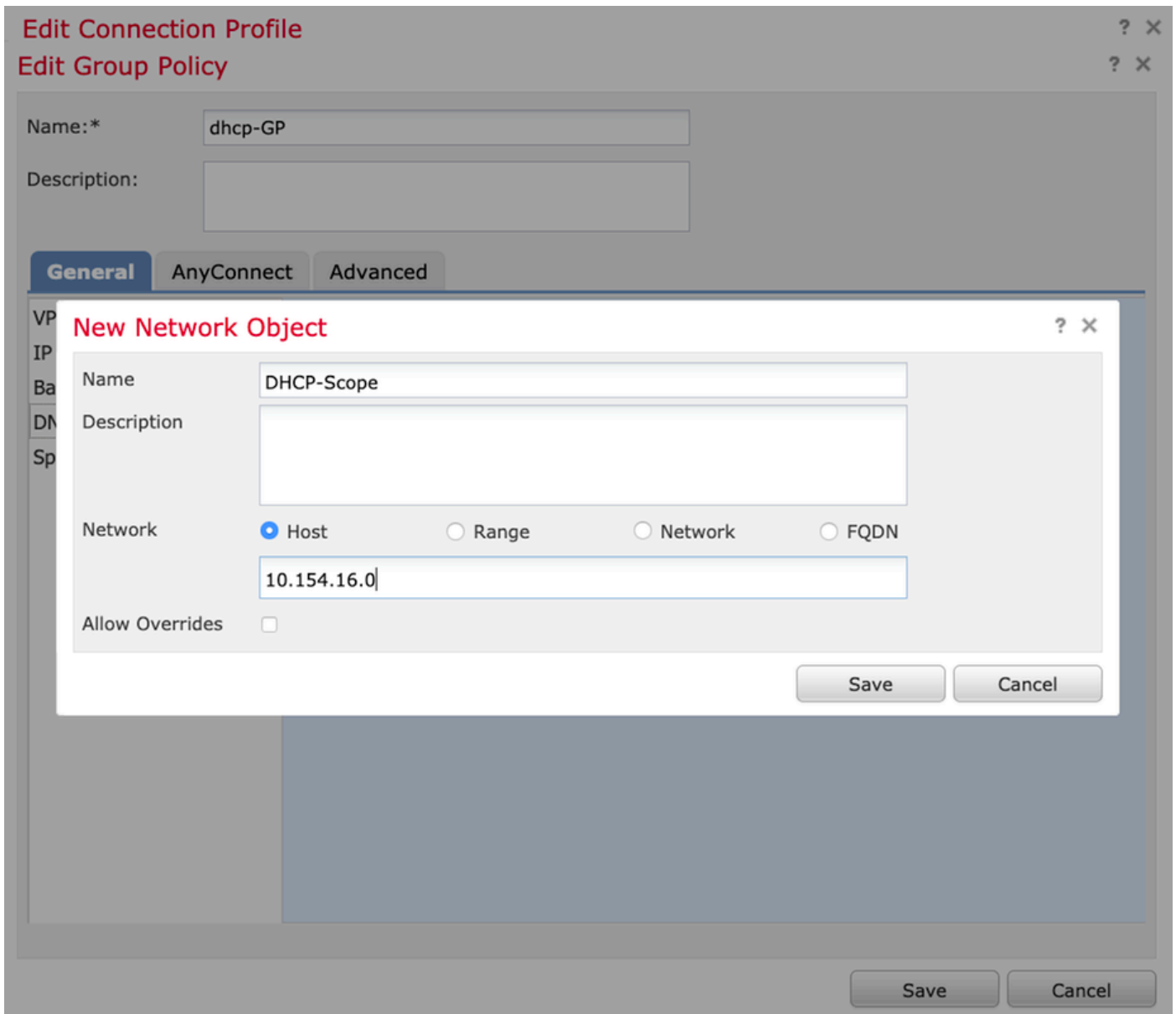
**DHCP Network Scope:**    
*Only network object with ipv4 address is allowed (Ex: 10.72.3.5)*

Default Domain:

Save Cancel

2. 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。

## 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

### 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。

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**

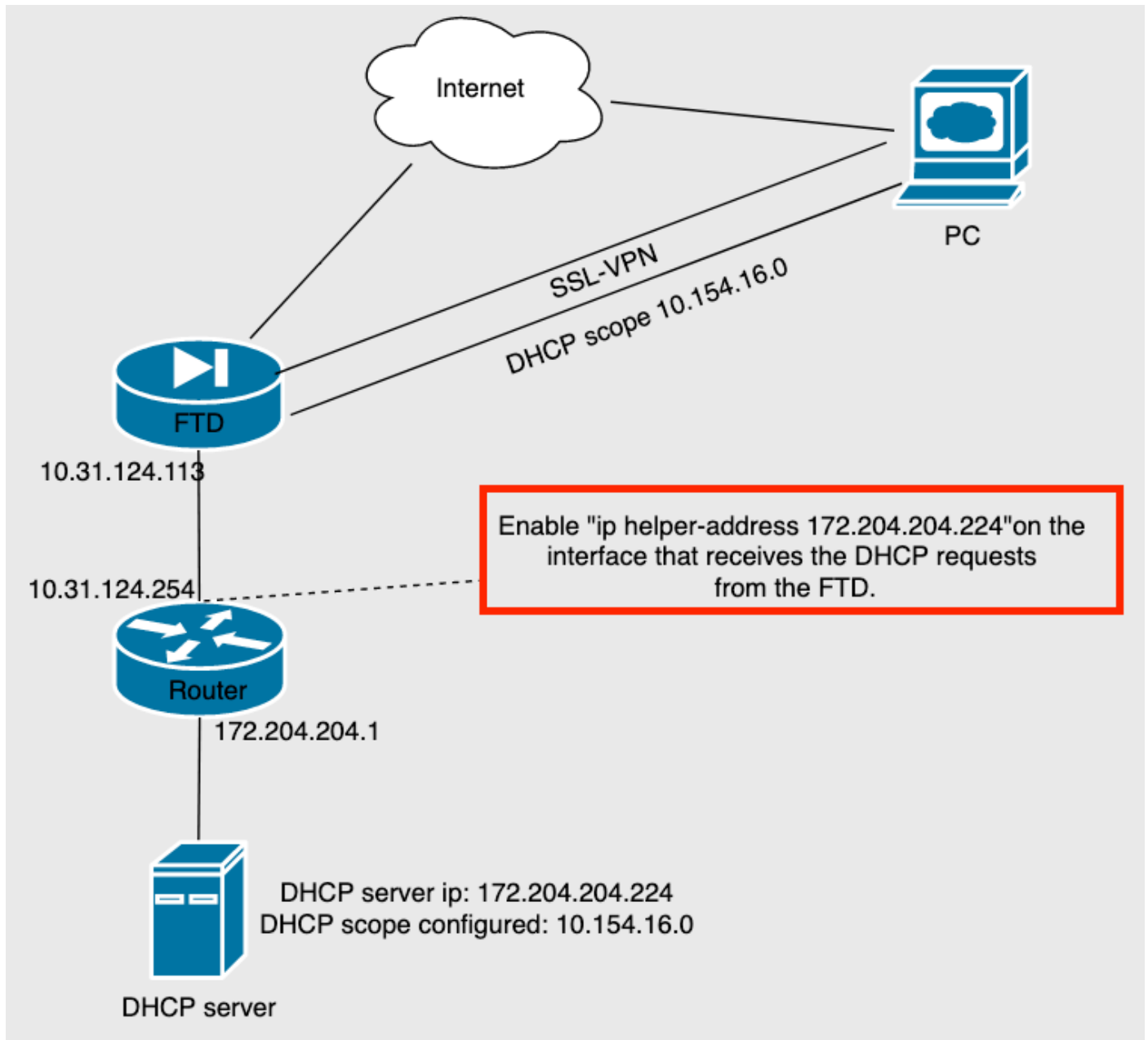
- Use authorization server (RADIUS Only)
- Use internal address pools

2.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。

```
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
```

- 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。



No.	Time	Source	Destination	Protocol	Length	Info
						Number



步驟3.登入到Anyconnect , DHCP協商應該如下圖所示。

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

```

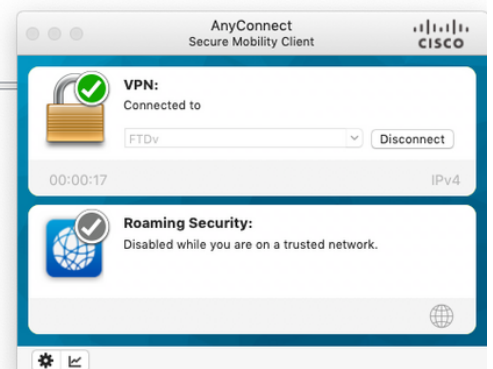
> Frame 4125: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{B27A96D9-4596-4DC3-A4C6-58020274134D}, id 0
> Ethernet II, Src: Cisco_d1:2d:30 (28:6f:7f:d1:2d:30), Dst: Vmware_96:23:b6 (00:50:56:96:23:b6)
> Internet Protocol Version 4, Src: 10.31.124.113, Dst: 172.204.204.224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

```



## 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](#)