

Configurare Anyconnect VPN Client su FTD: Server DHCP per assegnazione indirizzi

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Passaggio 1. Configurare l'ambito DHCP nel server DHCP](#)

[Passaggio 2. Configurare Anyconnect](#)

[Passaggio 2.1. Configurazione del profilo di connessione](#)

[Passaggio 2.2. Configurare Criteri di gruppo](#)

[Passaggio 2.3. Configurazione dei criteri di assegnazione degli indirizzi](#)

[Scenario helper IP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento offre un esempio di configurazione per Firepower Threat Defense (FTD) sulla versione 6.4, che consente alle sessioni VPN ad accesso remoto di ottenere un indirizzo IP assegnato da un server DHCP (Dynamic Host Configuration Protocol) di terze parti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- CCP 6.5
- FTD 6,5
- Windows Server 2016

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento non viene descritta l'intera configurazione di Accesso remoto, ma solo la configurazione richiesta nell'FTD per passare dal pool di indirizzi locale all'assegnazione degli indirizzi DHCP.

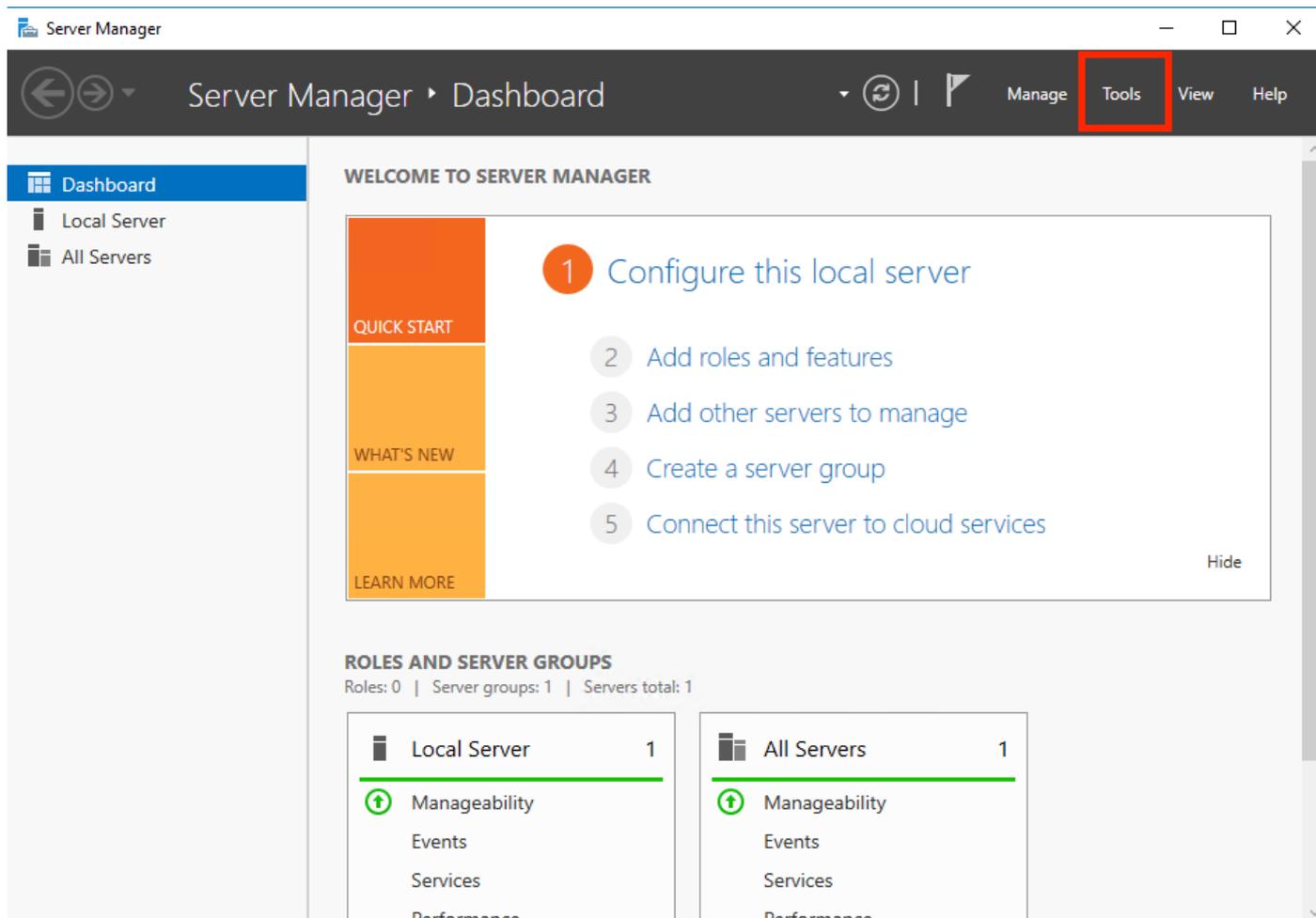
Se si sta cercando il documento di esempio della configurazione Anyconnect, consultare il documento "Configure AnyConnect VPN Client on FTD: Hairpinning and NAT Exemption".

Configurazione

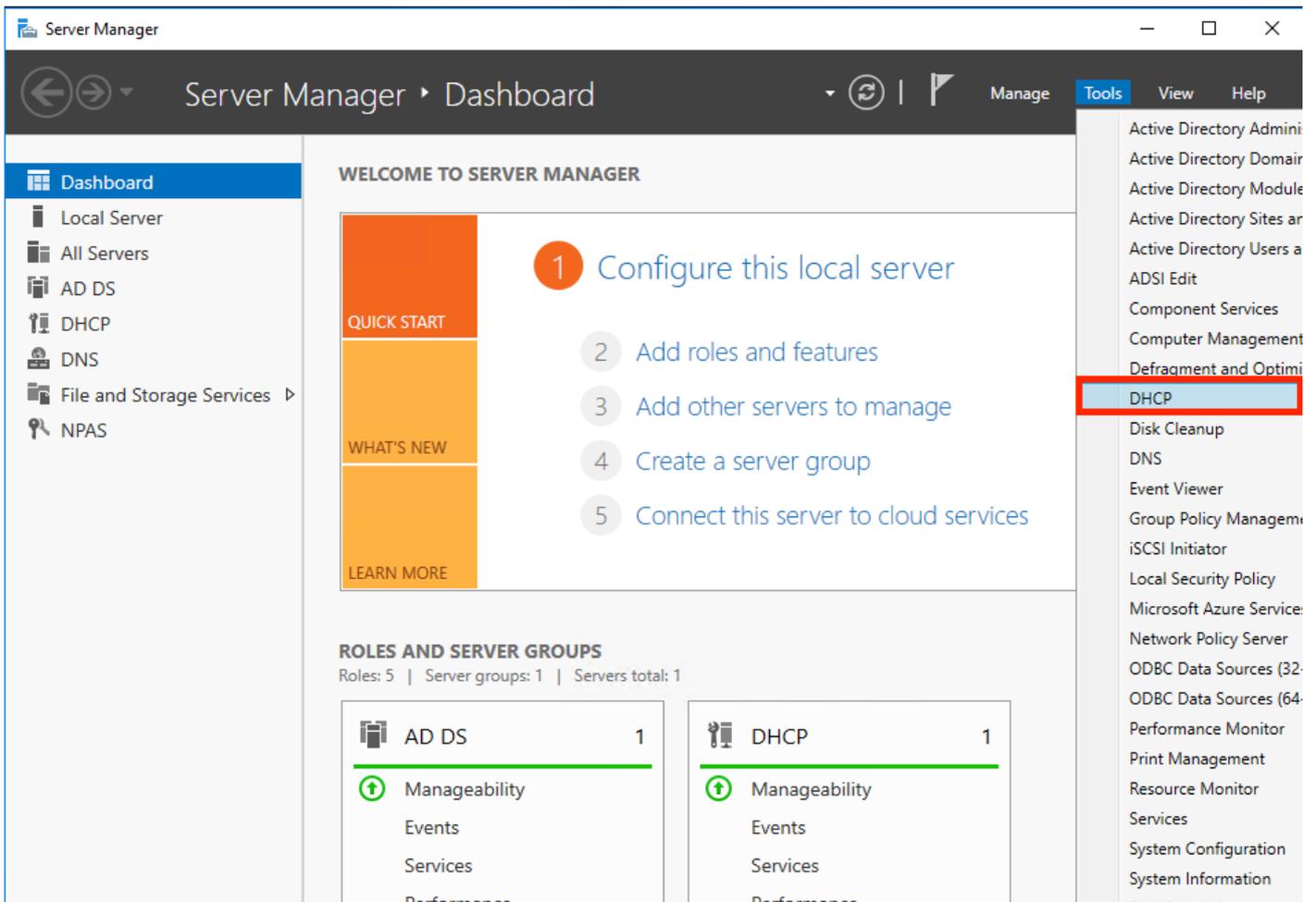
Passaggio 1. Configurare l'ambito DHCP nel server DHCP

In questo scenario, il server DHCP si trova dietro l'interfaccia interna dell'FTD.

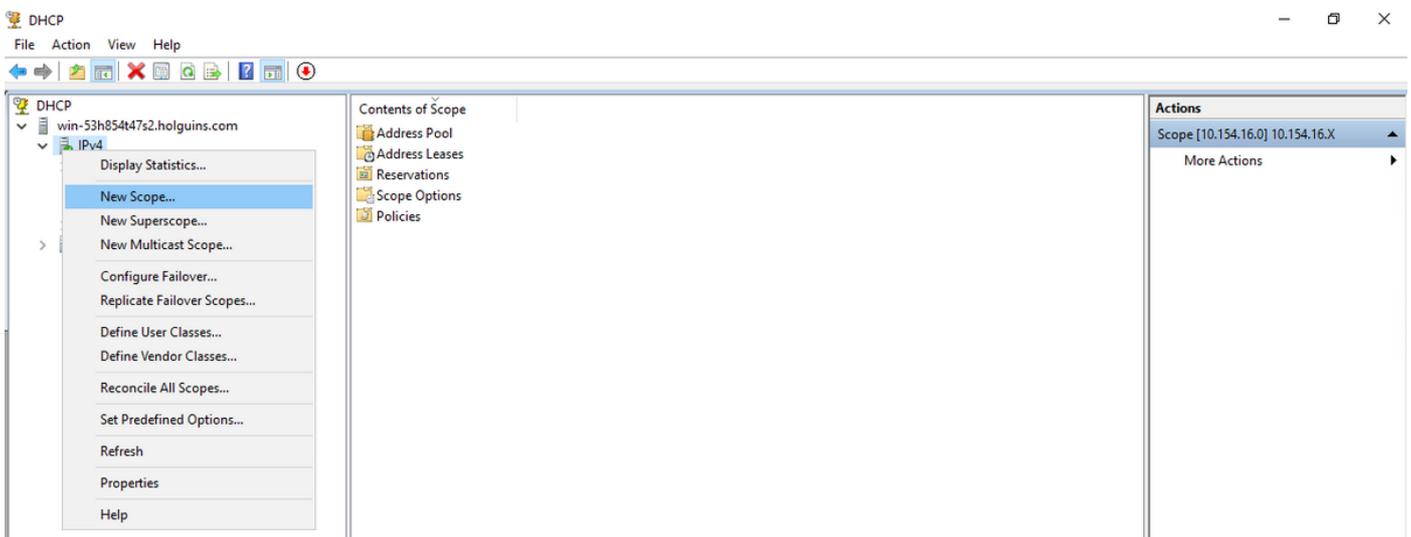
1. Aprire Server Manager in Windows Server e selezionare **Tools** (Strumenti) come mostrato nell'immagine.



2. Selezionare DHCP:



3. Selezionare IPv4, fare clic con il pulsante destro del mouse su di esso e selezionare **New Scope** (Nuovo ambito), come mostrato nell'immagine.



4. Seguire la **procedura guidata** come illustrato nell'immagine.

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. Assegnare un nome all'ambito come mostrato nell'immagine.

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. Configurare l'intervallo di indirizzi come mostrato nell'immagine.

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. (Facoltativo) Configurare le esclusioni come illustrato nell'immagine.

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. Configurare la **durata del lease** come mostrato nell'immagine.

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. (Facoltativo) Configurare le opzioni dell'ambito 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

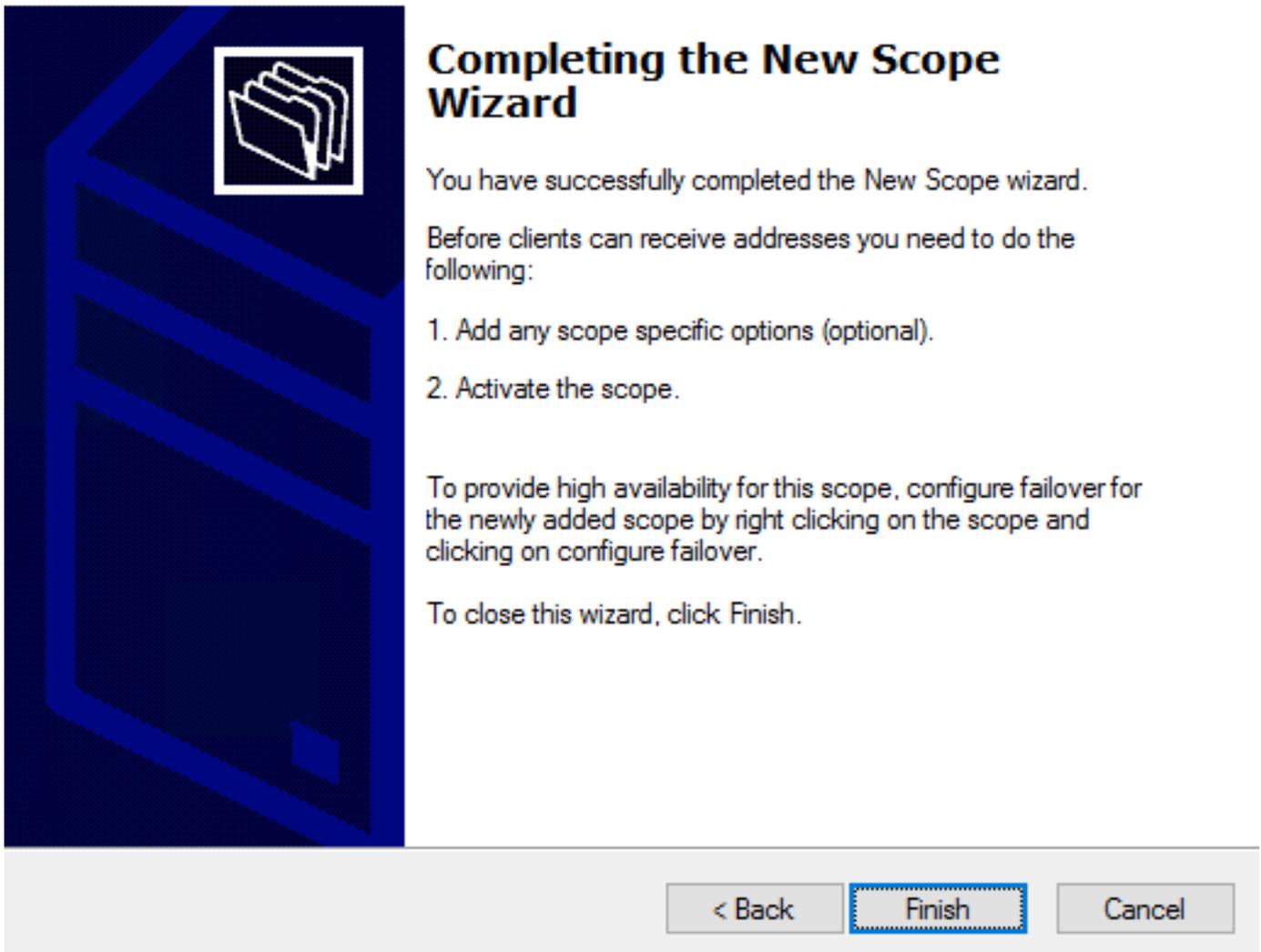
< Back

Next >

Cancel

10: Selezionare **Finish** (Fine) come mostrato nell'immagine.

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:

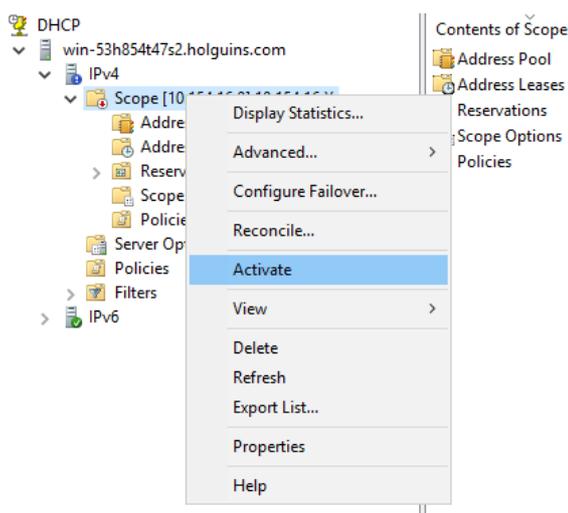
1. Add any scope specific options (optional).
2. Activate the scope.

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: Fare clic con il pulsante destro del mouse nell'ambito appena creato e selezionare **Attiva**, come mostrato nell'immagine.



Passaggio 2. Configurare Anyconnect

Dopo aver configurato e attivato l'ambito DHCP, la procedura successiva viene eseguita nel CCP.

Passaggio 2.1. Configurazione del profilo di connessione



1. Nella sezione Server DHCP, selezionare la scheda  e creare un oggetto con l'indirizzo IP del server DHCP.

2. Selezionare l'oggetto come server DHCP per richiedere un indirizzo IP, come mostrato nell'immagine.

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

Passaggio 2.2. Configurare Criteri di gruppo

1. All'interno del menu Criteri di gruppo, passare a **Generale > DNS/WINS**, c'è una sezione **DHCP Network Scope** (Ambito di rete DHCP) come mostrato nell'immagine.

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:

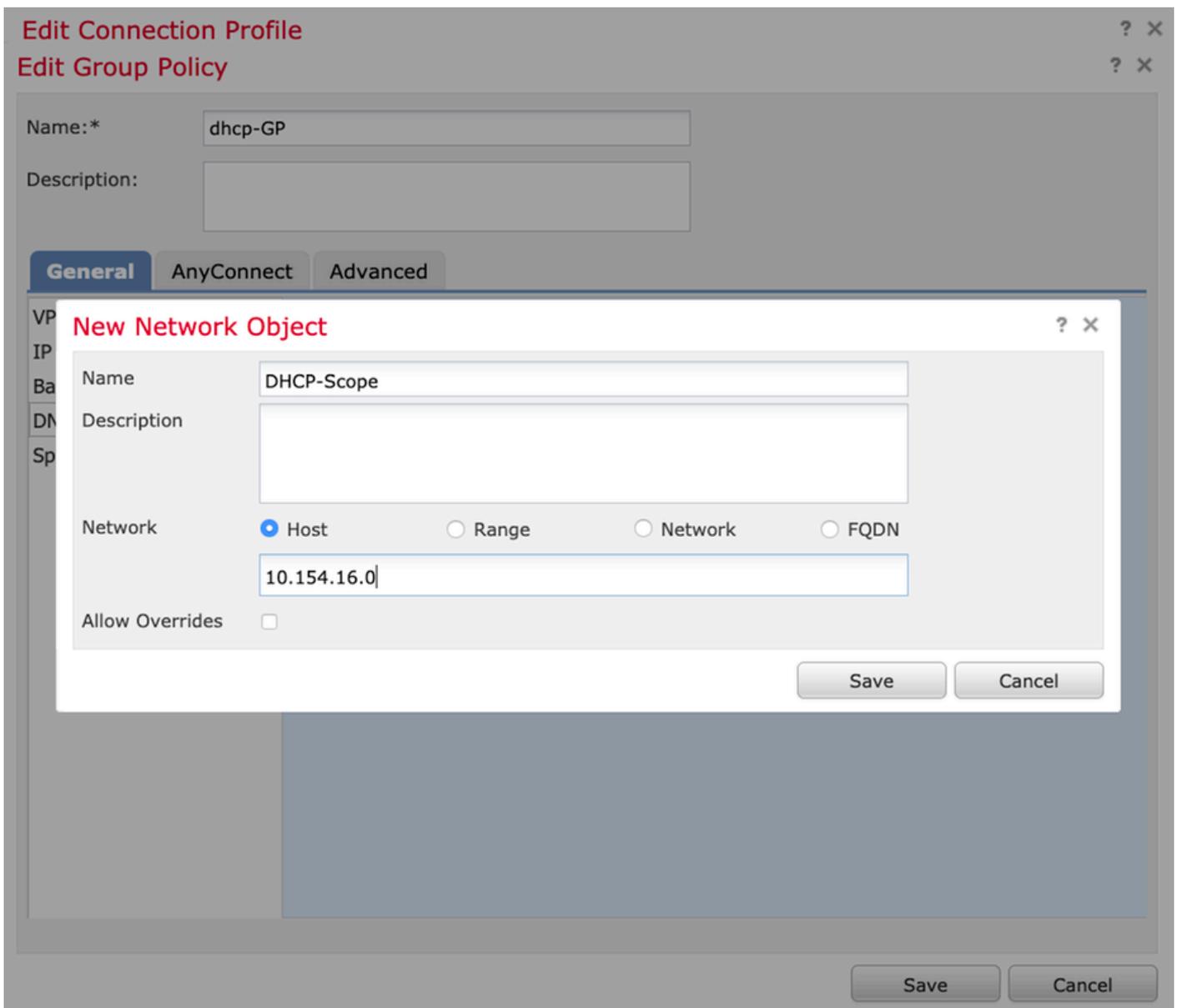
DHCP Network Scope:
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Save Cancel

2. Creare un nuovo oggetto con lo stesso ambito di rete del server DHCP.

Nota: Deve essere un oggetto host, non una subnet.



3. Selezionare l'oggetto ambito DHCP e selezionare **Save** (Salva) come mostrato nell'immagine.

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

Passaggio 2.3. Configurazione dei criteri di assegnazione degli indirizzi

1. Passare a **Advanced > Address Assignment Policy** e assicurarsi che l'opzione **Use DHCP** sia attivata e disattivata come mostrato nell'immagine.

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

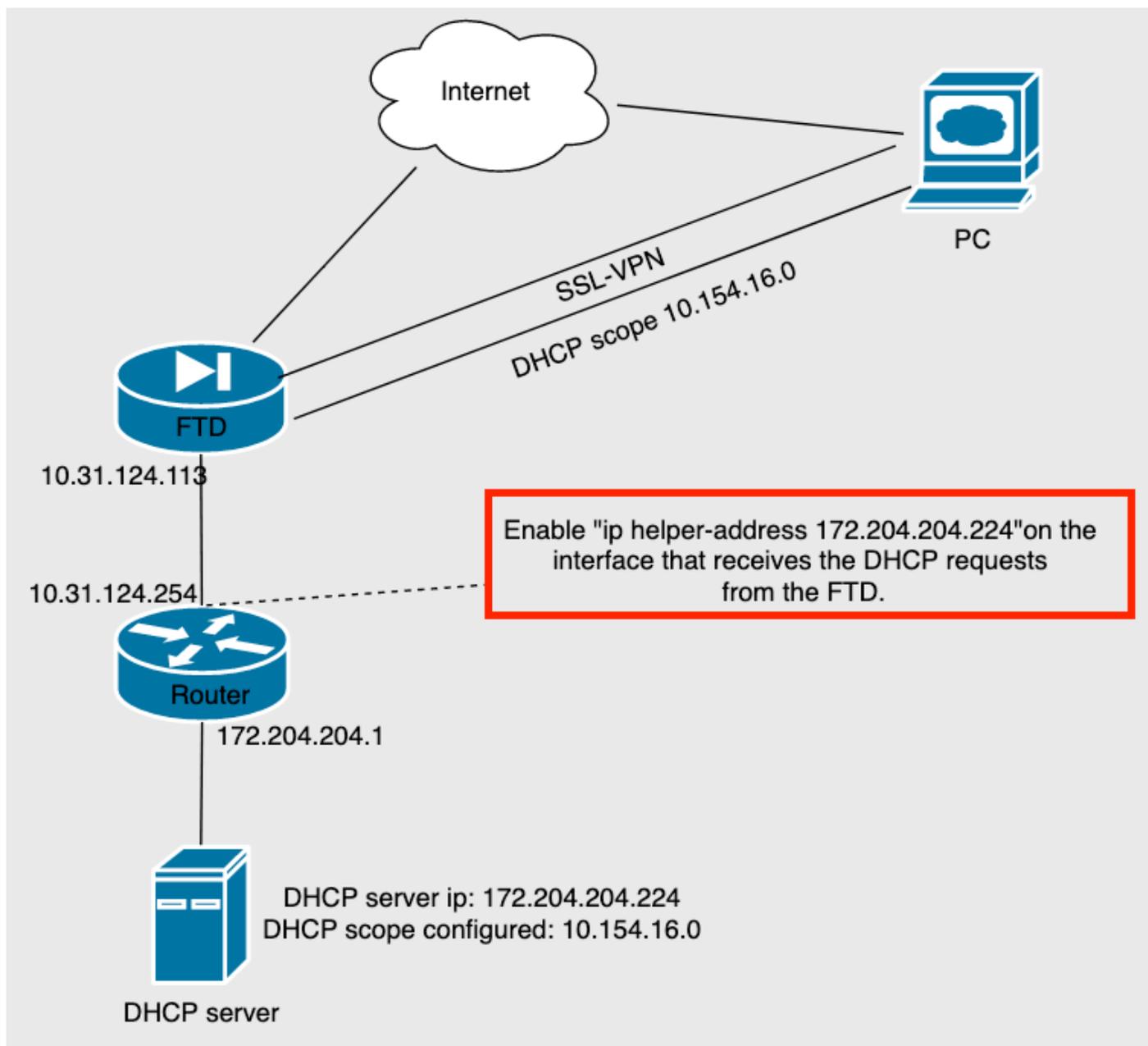
- Use authorization server (RADIUS Only)
- Use internal address pools

2. Salvare le modifiche e distribuire la configurazione.

Scenario helper IP

Quando il server DHCP si trova dietro un altro router nella LAN (Local Area Network), è necessario un "helper IP" per inoltrare le richieste al server DHCP.

Come mostrato nell'immagine, una topologia mostra lo scenario e le modifiche necessarie nella rete.



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

In questa sezione vengono descritti i pacchetti DHCP scambiati tra l'FTD e il server DHCP.

- Individuazione: Questo è un pacchetto unicast inviato dall'interfaccia interna del FTD al server

DHCP. Nel payload, un **indirizzo IP dell'agente di inoltra** specifica l'ambito del server DHCP come mostrato nell'immagine.

```
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
```

- Offerta: Questo pacchetto è una risposta del server DHCP, fornito con l'origine del server DHCP e la destinazione dell'ambito DHCP nell'FTD.
- Richiesta: Questo è un pacchetto unicast inviato dall'interfaccia interna del FTD al server DHCP.
- ACK: Questo pacchetto è una risposta del server DHCP, fornito con l'origine del server DHCP e la destinazione dell'ambito DHCP nell'FTD.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Passaggio 1. Scaricare e abilitare wireshark nel server DHCP.

Passaggio 2. Applicare DHCP come filtro di acquisizione come mostrato nell'immagine.

No.	Time	Source	Destination	Protocol	Length	Info

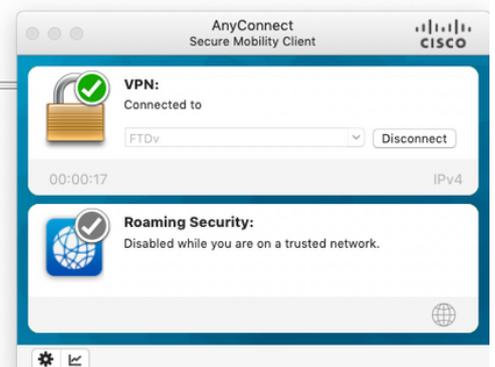


Passaggio 3. Accedere a Anyconnect e la negoziazione DHCP deve essere visualizzata come mostrato nell'immagine.

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  ..C.C,.....e
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  .....
```



Informazioni correlate

- In questo video viene illustrato l'esempio di configurazione di FTD, che consente alle sessioni VPN ad accesso remoto di ottenere un indirizzo IP assegnato da un server DHCP di terze parti.
- [Documentazione e supporto tecnico – Cisco Systems](#)