

مداخ فTD: ىل ع AnyConnect VPN ليمع نيوكت نيوانعلا نييعتل DHCP

تايوتحمل

[عمدقمل](#)

[سياسال تابلطمل](#)

[تابلطمل](#)

[عمدختسمل تانوكمل](#)

[سياسال تامولعم](#)

[نيوكتل](#)

[DHCP مداخ في DHCP قاطن نيوكت 1. ةوطخل](#)

[AnyConnect نيوكت 2. ةوطخل](#)

[لاصلال فيرعت فلم نيوكت 2.1. ةوطخل](#)

[عمومحمل جهن نيوكت 2.2. ةوطخل](#)

[نيوانعلا نييعتل جهن نيوكت 2.3. ةوطخل](#)

[IP دعاسم ويرانس](#)

[حصلا نم ققحتل](#)

[احالصال واطخال افاشكتسا](#)

[قلص تاذا تامولعم](#)

عمدقمل

رادصلال ىل ع Firepower Threat Defense (FTD) ب صاخل نيوكتل الالم دنن سمل اذ عمدق
م IP ناوع ىل ع لوصلل دع ب نع لوصول VPN تاك بش لمع تاسل ل حمسي يذلاو، 6.4
فرطلاب صاخل (DHCP) فيضملل كي ماني دل نيوكتل لوكوت ورب مداخ ةطساوب هنييعت
ثلاثل.

سياسال تابلطمل

تابلطمل

ةيلاتل عيضاوملاب ةفرعم كي دل نوكت ناب Cisco ي صوت:

- Firepower Threat Defense (FTD) ماظن
- Firepower (FMC) ةرادا زكرم
- DHCP

عمدختسمل تانوكمل

ةيلاتل اماربال تارادصلال دنن سمل اذ في ةدراول تامولعملا دنن ست:

- FMC 6.5
- FTD 6.5

- Windows Server 2016 لي غشتال ماظن

ةصاخ ةيلم عم ةئيب ي ف ةدوجوملا ةزهجالا نم دنتسملا اذه ي ف ةدراولما تامولعملما عاشن ا م ت تناك اذا .(يضا رتفا) حوسمم نيوكت ب دنتسملا اذه ي ف ةمدختسملا ةزهجالا عي مج ت ادب رما يال لم تحملا ريثاتلل كمهف نم دكات ف ، ةرشابم كتك ب ش

ةيساسا تامولعم

ي ف طقف بولطملا نيوكتلا لب ، لمكلاب دع ب نع لوصولا نيوكت دنتسملا اذه فص ي نل DHCP ناو نع نيوعت يلى لىلحملا نيوانعلا عمجت نم ريغتلل FTD.

نيوكت " دنتسم يلى عوجرلا يجر ي ف AnyConnect نيوكت لاثم دنتسم نع شحتب تنك اذا " NAT ءافء او رصانعلا زرف : FTD يلى ع AnyConnect VPN لىم عم

نيوكتلا

DHCP مداخل ي ف DHCP قاطن نيوكت 1. ةوطخل

ةيلخادلا FTD ةهجاو فلخ DHCP مداخل عقي ، وي رانيسلا اذه ي ف

ةروصل ي ف حوضوم وه امك تاودال دحو Windows Server ي ف "مداخل ةرادا" حتفا 1.

The screenshot shows the Windows Server Manager interface. The 'Tools' menu item is highlighted with a red box. The main content area displays a 'QUICK START' section with a numbered list of tasks: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this, there is a 'ROLES AND SERVER GROUPS' section showing 'Local Server' and 'All Servers' groups, each with a 'Manageability' role.

2. DHCP دحو:

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. ةروصل لاي ف حضم وه امك قاطن لل مسا ني عتب مق.

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. ةروصلال ي ف حضوم وه امك نيوانعلا قاطن نيوك تب مق .

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. ةروصلال ي ف حضوم وه امك تاءانثتسالال نيوكتب مق (يرايخا).

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. ةروصولا في حضورم وه امك ريأأال ةدم نيوك ت.

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. DHCP قاطن تاراخ نيوكتب مق (يراي تخا):

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

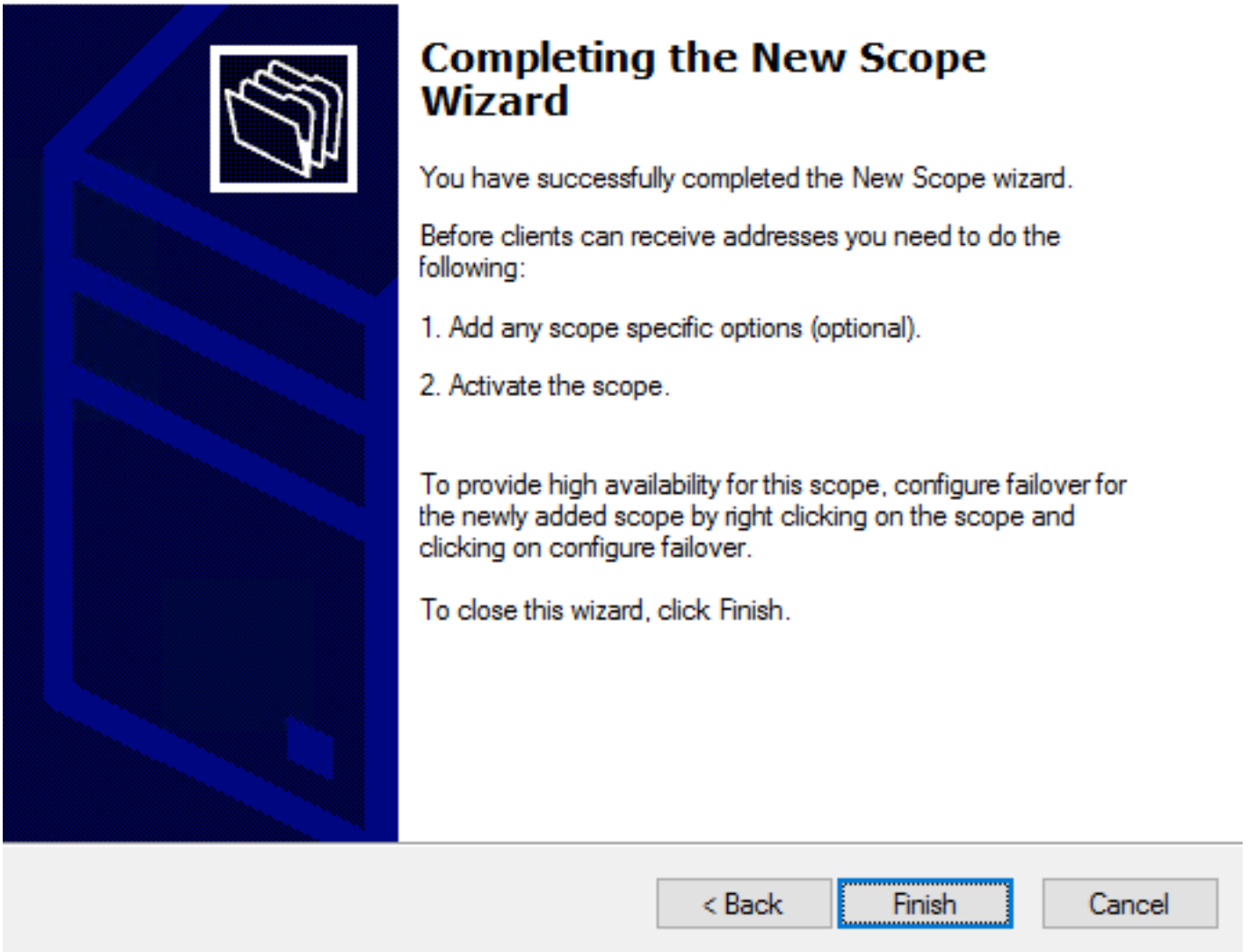
< Back

Next >

Cancel

10: ةروصل لاي ف حضوم وه امك ءاهن | ددح

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:

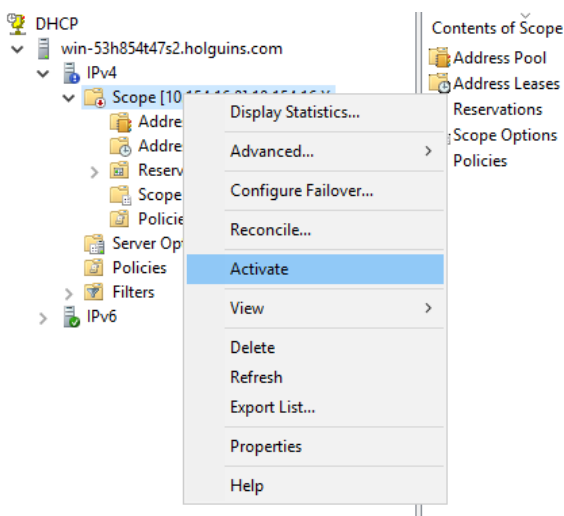
1. Add any scope specific options (optional).
2. Activate the scope.

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

حضوره امك طيشنت دحو وتلل هؤاشن| مت يذلا قاطنلا ي نميألا سواملا رزب رقنا 11: ةروصلا يف.



AnyConnect نيوكت 2. ةوطخلا

يف مكحتلا ةدحو يف يلاتلا ءارجالا ذيفنت متي، هطيشنتو DHCP قاطن نيوكت درجمب (FMC) ةساسألا ةرادإلا.


لاصتالال فيرعت فلم نيوكت 2.1 ةوطخلال

1. DHCP مداخل IP ناونع مادختساب نئاك عاشن اوزمر  ددح، DHCP مداوخ مسق في.

2. ةروصلال في حضورم وه امك نم IP ناونع بلطل DHCP مداخل نئالال ددح.


Edit Connection Profile

Connection Profile:*


Group Policy:*  [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

ةومجملال جهن نيوكت 2.2 ةوطخلال

1. DHCP ةكبش قاطن مسق كانه، DNS/WINS > ماع لى لقتنا، "ةومجملال جهن" ةمئاق لخاد. ةروصلال في حضورم وه امك.

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:

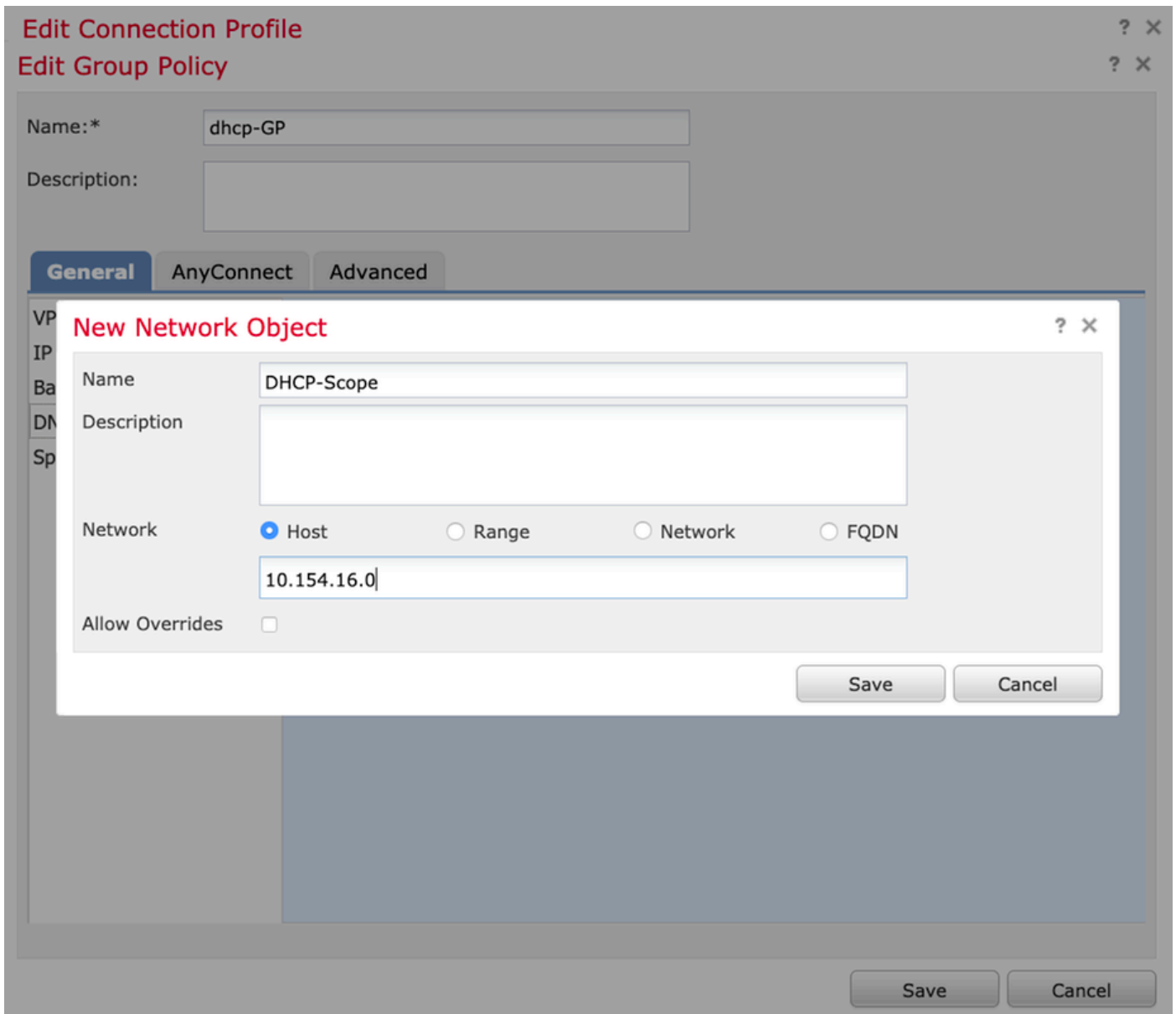
Secondary WINS Server:

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

Default Domain:

مداخ هك لتمي يذلا ةكبش لاقاطن سفن ىلع اذه يوتحي نأ بجي و، ديدج نئاك عاش ناب مق 2. DHCP.

ةي عرف تكبش سيلو، فيضم نئاك اذه نوكي نأ بجي: **ةطحالم**



3. ةروصل لآ يف ءضوم وه امك ظفء دءءو DHCP قاطن نئاك دءء.

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

نېوانع ل نېيغت جهن نېوكت 2.3. ةوطخل

رايخ رييغت مت هنا نم دكأت و ناو نعل ل نېيغت ةسايس > ةمدقتم تاراخي ل لقتنا 1.
ةروصل ل ي ف حضورم وه امك DHCP مادختسا

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

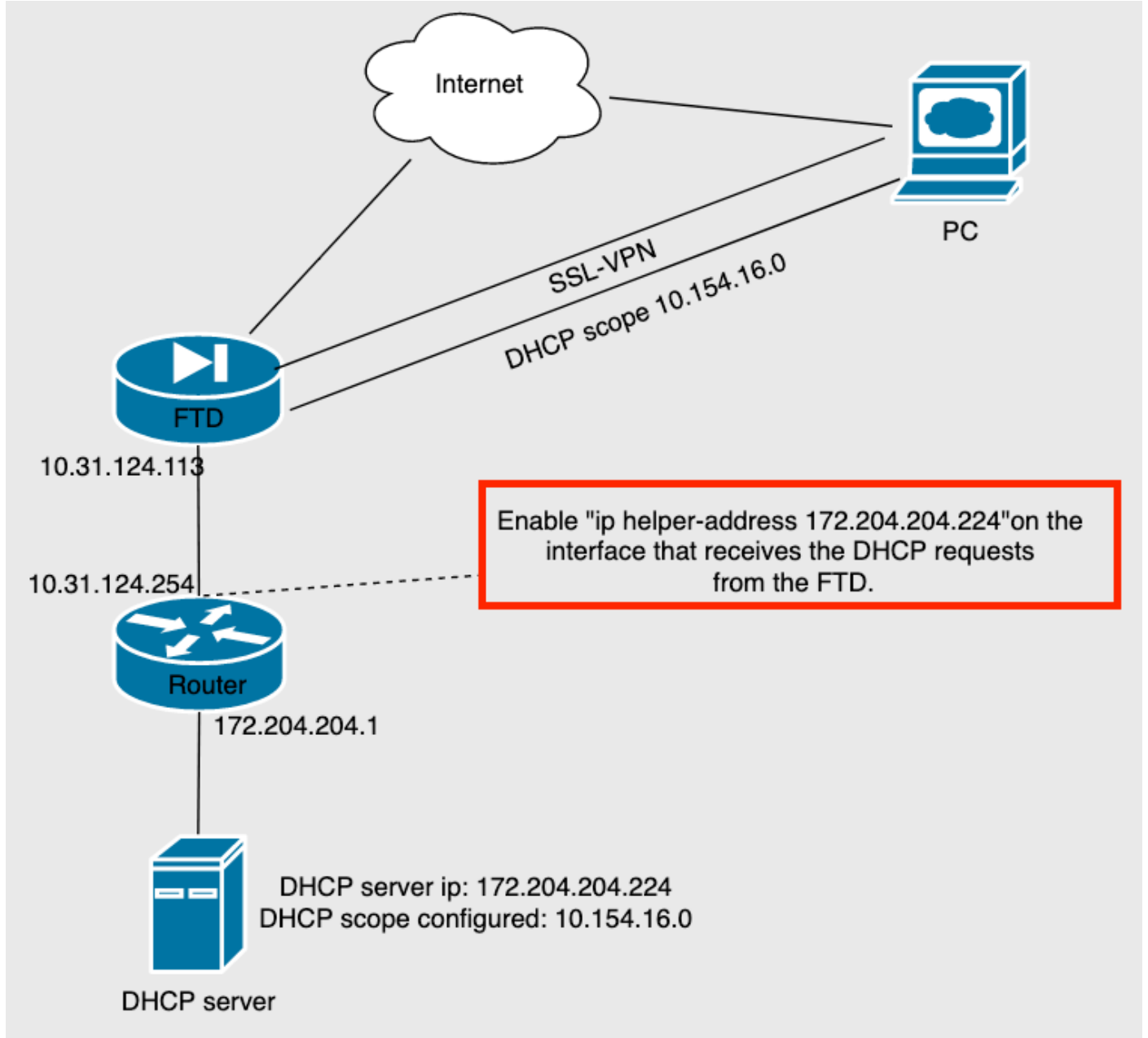
- Use authorization server (RADIUS Only)
- Use internal address pools

2. نيوكتالا رشنو تاريغيغتاللا ظفح.

IP دعاسم ويرانيس

دعاسم "دوجو مزلي، (LAN) ةيلحمللا قطنملا ةكبش ي ف رخآ هجوم فلخ DHCP مداخل نوكي ام دنع DHCP مداخل ىلا تابلللا هيجوت ةداعل IP".

ةكبشلا ي ف ةمزاللا تاريغيغتاللا ويرانيسلا ططخم حضوي، ةروصللا ي ف حضوم وه امك.



ةحصللا نم ققحتلا

ححص لكش ب نيوكتالا لمع ديكأتل مسقلا اذه مدختسا

DHCP مداخلو FTD نيب ةلدابتلم DHCP مزح مسقلا اذه فصبي

- ةلومحلا ي ف DHCP مداخل ىلا ةيلخادللا FTD ةهجاو نم ةلسرم unicast ةمزح هذه: فاشتكالا، ةروصللا ي ف حضوم وه امك DHCP مداخل قاطن ليحرت لماعل IP ناوع ددحي

```
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
```

- قاطن ةهجوو DHCP مداخل ردصم عم اذه يتأي، DHCP مداخل نم ةباجتسإ يه ةمزحل هذه: ضرعلا DHCP في FTD.
- لدان DHCP لى لى نراق لخد FTD نم لسري طبر unicast اذه: بطلال.
- قاطن ةهجوو DHCP مداخل ردصم عم اذه يتأي، DHCP مداخل نم ةباجتسإ يه ةمزحل هذه: ACK: DHCP في FTD.

اهحالصإو ءاطخال فاشكتسا

اهحالصإو نيوكتلا ءاطخال فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي

DHCP مداخل في هنيكمتو يكلساللا كلساللا ليزنتب مق 1. ةوطخال

ةروصلال في حضورم وه امك طاقتلالا حشرمك DHCP قيبتت 2. ةوطخال

No.	Time	Source	Destination	Protocol	Length	Info
						Number

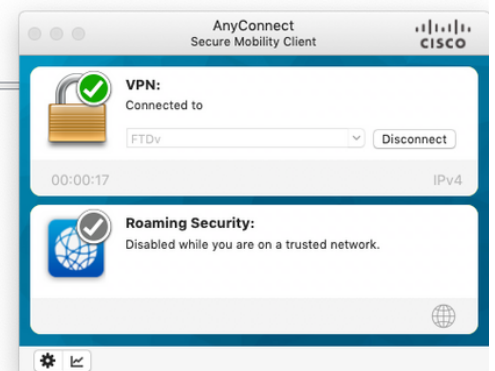


ةروصل ايف حضورم وه امك DHCP ضوافت رابتع| ب جي ، AnyConnect ىل لوخذلا ل جس .3 ةوطخل

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 ..
0050 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 ..
0070 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 ..
0090 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 ..
00b0 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 ..
00d0 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 ..
00f0 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 ..
```



ةلص تاذا تامولعم

- دع ب نع لوصولل VPN لمع تاسلجل حمسي يذلا ، FTD ل نيوكتللا لاثم ويديفلا اذم مدقي
ةجراخللا هجلل DHCP مداخ ةطساوب هنييعة مت IP ناوع لعل لوصحلل
- [Cisco Systems - تادنتس مل او ينقتلا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء مء دقء ةل ةل ةفارتحال ةمچرتل عم لالحل و
ىل إأمءءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل