

FTDでAnyconnect VPN Clientを設定します。アドレス割り当てのDHCPサーバ

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ1:DHCPサーバでのDHCPスコープの設定](#)

[手順 2 : AnyConnect の設定](#)

[ステップ2.1 : 接続プロファイルの設定](#)

[ステップ2.2 : グループポリシーの設定](#)

[ステップ2.3 : アドレス割り当てポリシーの設定](#)

[IPヘルパーシナリオ](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、バージョン6.4のFirepower Threat Defense(FTD)の設定例を紹介します。この設定例を使用すると、リモートアクセスVPNセッションでサードパーティのDynamic Host Configuration Protocol(DHCP)サーバによって割り当てられたIPアドレスを取得できます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- FMC 6.5
- FTD 6.5
- Windows Server 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

このドキュメントでは、リモートアクセス設定全体については説明しません。ローカルアドレスプールからDHCPアドレス割り当てに変更するためにFTDに必要な設定だけです。

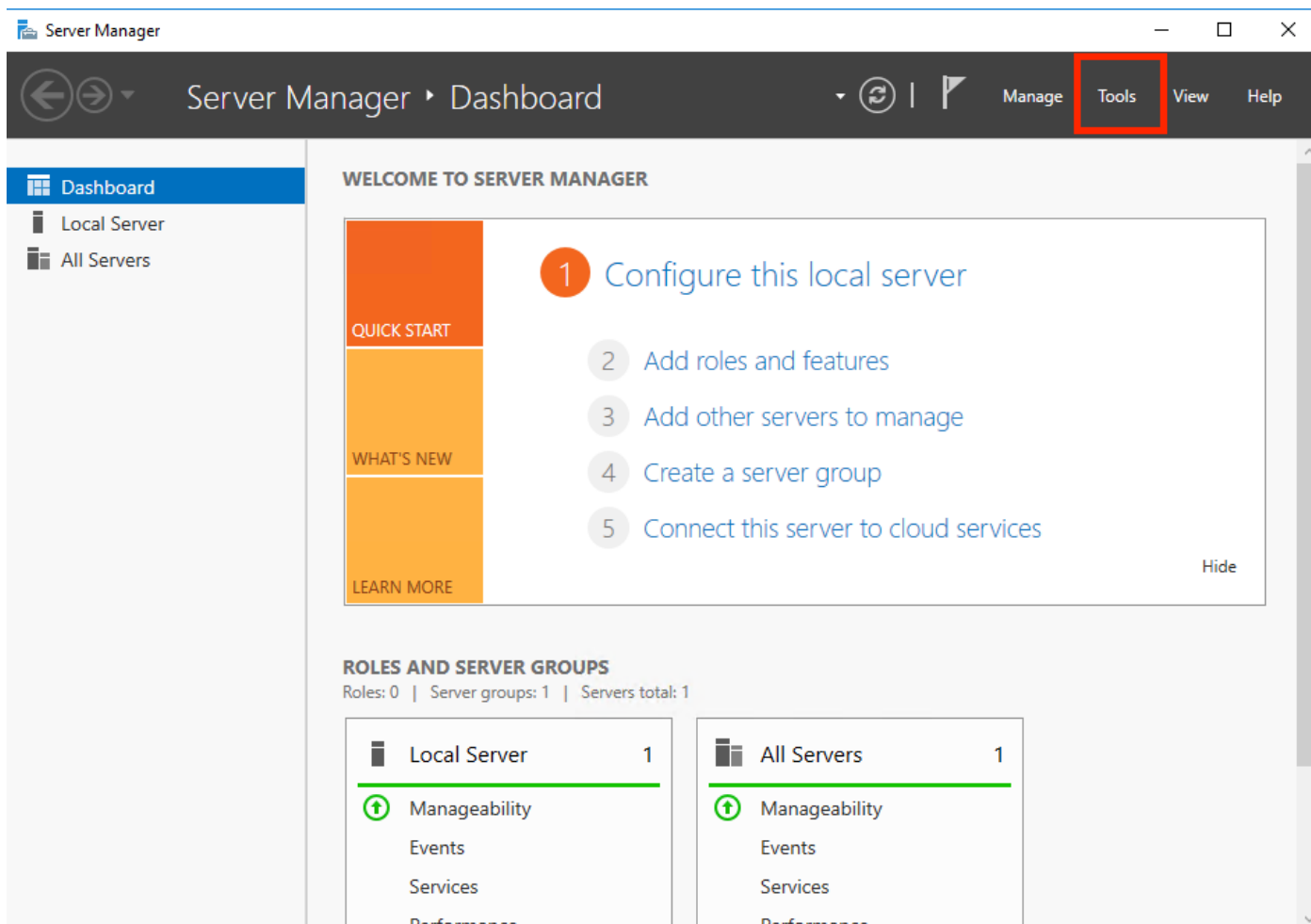
Anyconnectの設定例ドキュメントを探している場合は、「FTDでのAnyConnect VPN Clientの設定：Hairpinning and NAT Exemption」を参照してください。

設定

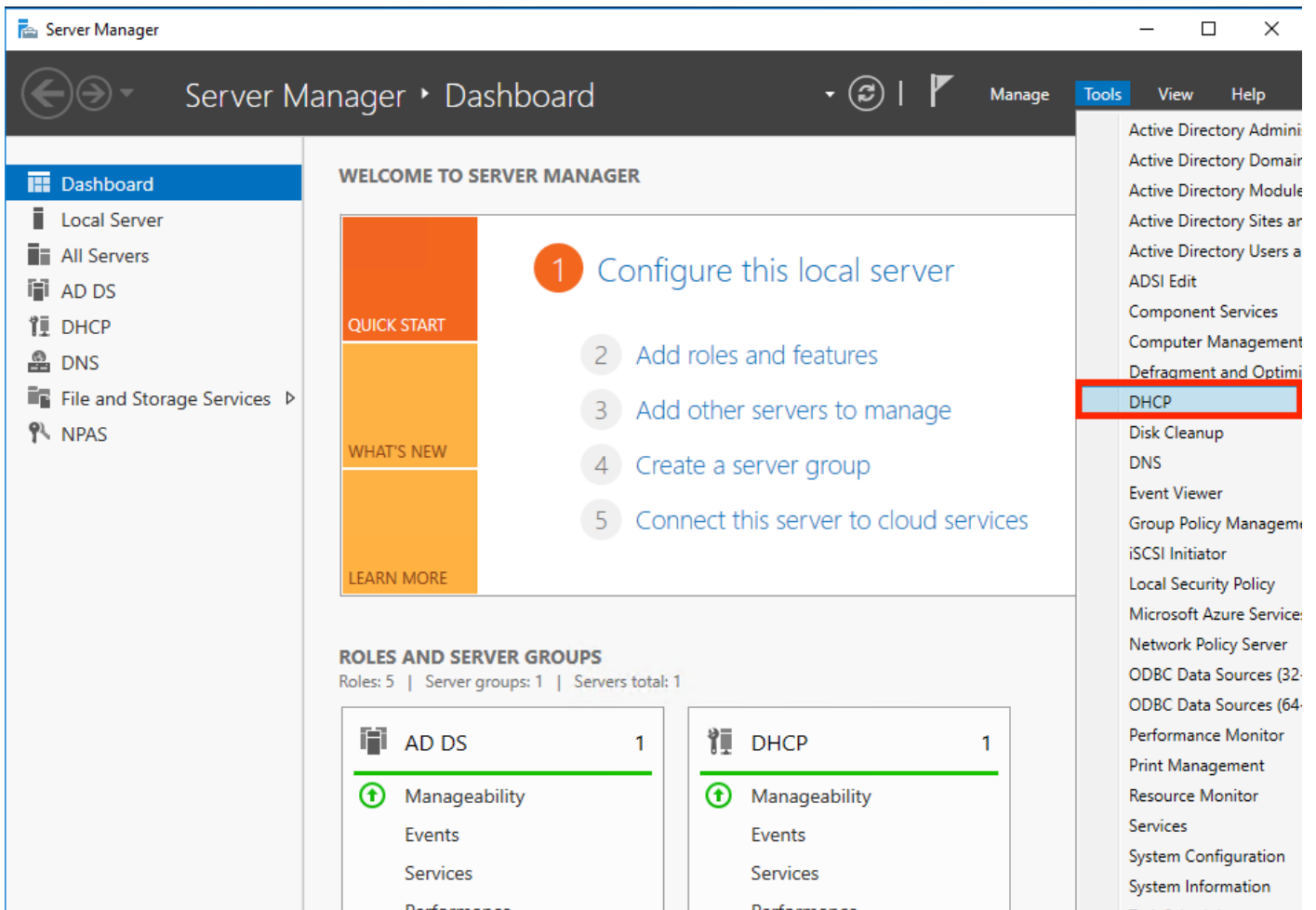
ステップ1:DHCPサーバでのDHCPスコープの設定

このシナリオでは、DHCPサーバはFTDの内部インターフェイスの背後にあります。

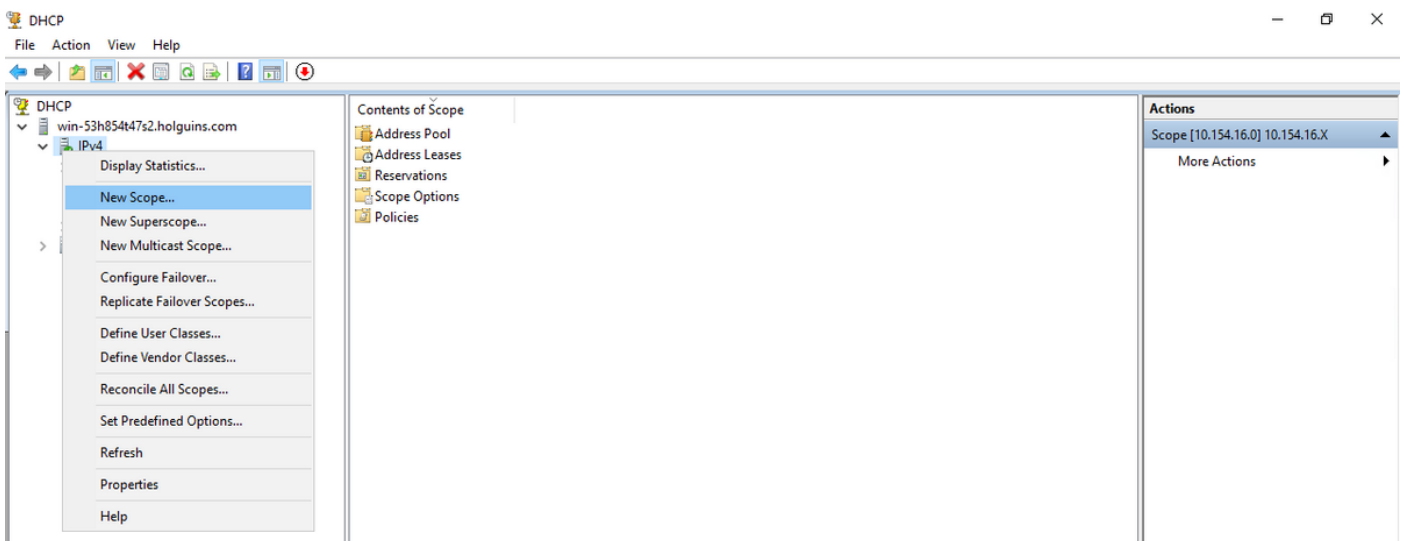
1. Windows ServerでServer Managerを開き、図に示すようにToolsを選択します。



2. DHCPの選択：



3. IPv4を選択して右クリックし、図に示すように**New Scope**を選択します。



4. 図に示すようにウィザードに従ってください。

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.図に示すように、スコープに名前を割り当てます。

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.図に示すように、アドレスの範囲を設定します。

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. (オプション) 図に示すように、除外を設定します。

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.図に示すようにリース期間を設定します。

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. (オプション) DHCPスコープオプションを設定します。

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:図に示すように[完了]を選択します。

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.

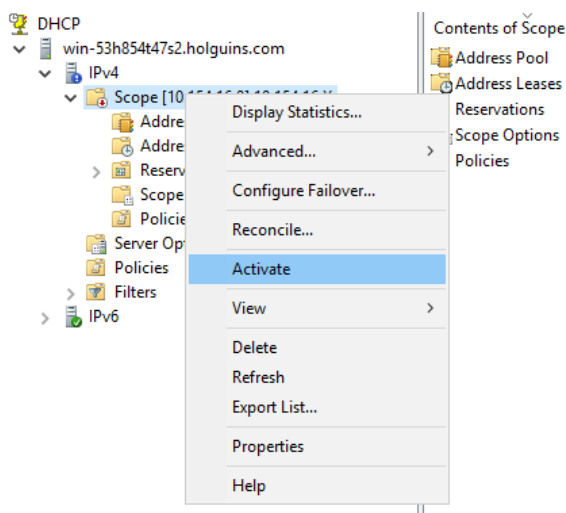
To close this wizard, click Finish.

< Back

Finish

Cancel

11 : 作成したスコープ内で右クリックし、図に示すように**Activate**を選択します。




手順 2 : AnyConnect の設定

DHCPスコープを設定してアクティブにすると、次の手順がFMCで実行されます。

ステップ2.1 : 接続プロファイルの設定


1. [DHCP Servers]セクションで、 DHCPサーバのIPアドレスを使用してオブジェクトを作成します。

2. 図に示すように、オブジェクトをDHCPサーバとして選択し、からIPアドレスを要求します。




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

ステップ2.2 : グループポリシーの設定

1. [Group Policy]メニュー内で、[General] > [DNS/WINS]に移動します。図に示すように、[DHCP Network Scope]セクションがあります。

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:

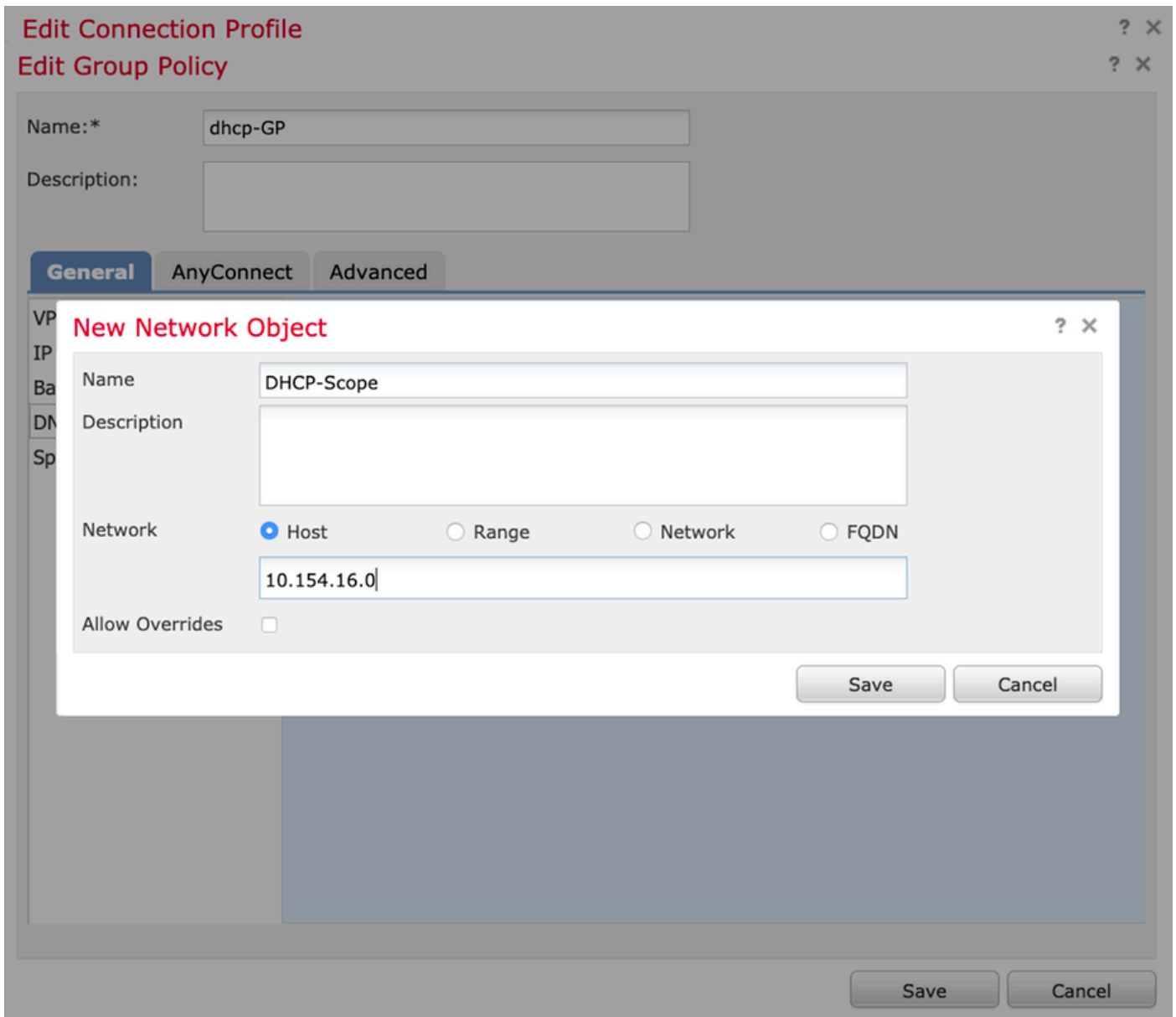
Secondary WINS Server:

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

Default Domain:

2.新しいオブジェクトを作成します。これは、DHCPサーバと同じネットワークスコープを持っている必要があります。

注：



3. DHCPスコープオブジェクトを選択し、図に示すように[保存]を選択します。

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

ステップ2.3 : アドレス割り当てポリシーの設定

1. [Advanced] > [Address Assignment Policy] に移動し、[Use DHCP] オプションが図のように切り替わっていることを確認します。

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

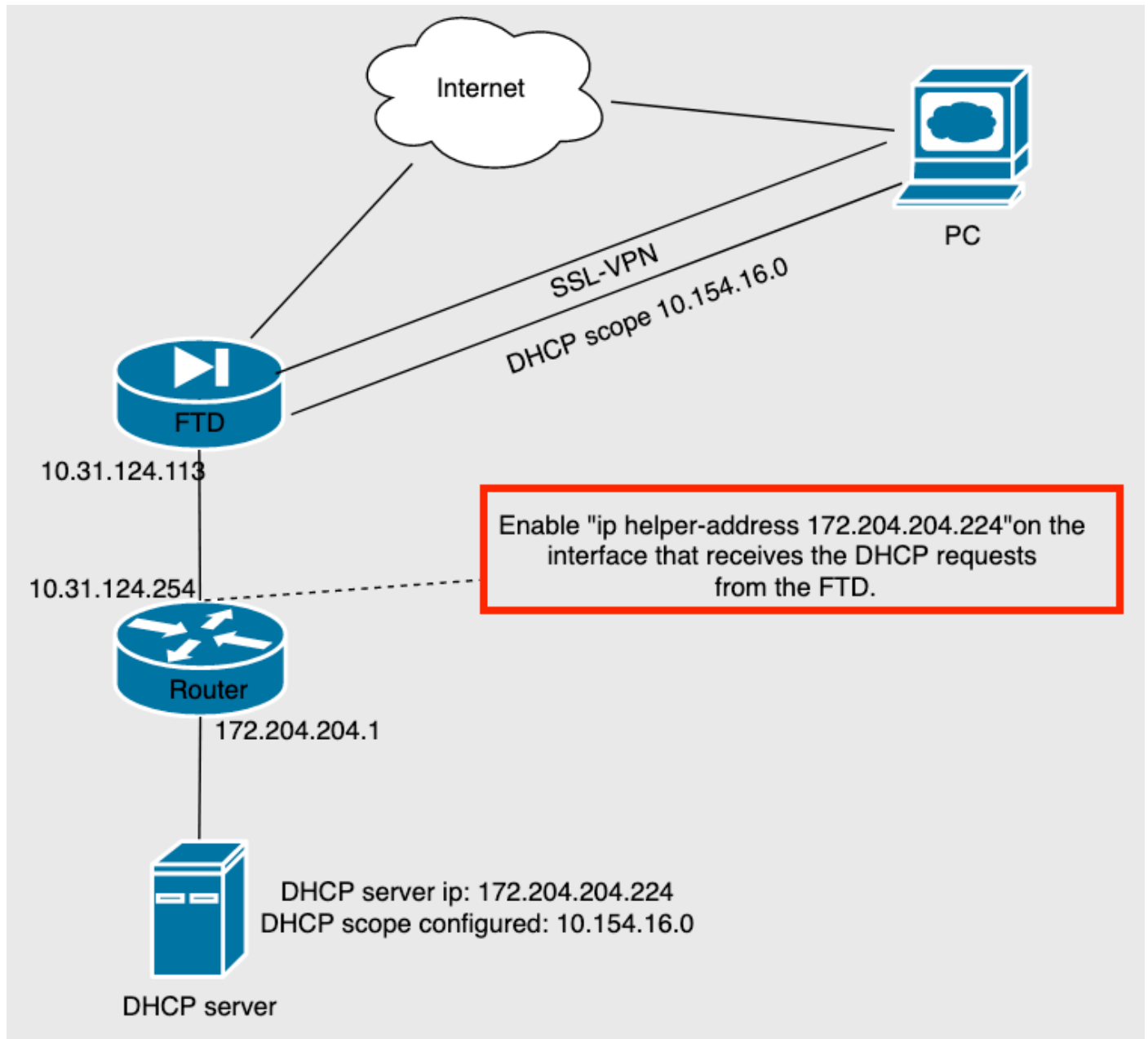
- Use authorization server (RADIUS Only)
- Use internal address pools

2.変更を保存し、構成を展開します。

IPヘルパーシナリオ

DHCPサーバがローカルエリアネットワーク(LAN)の別のルータの背後にある場合、DHCPサーバに要求を転送するには「IPヘルパー」が必要です。

図に示すように、トポロジはシナリオとネットワークで必要な変更を示しています。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

このセクションでは、FTDとDHCPサーバ間で交換されるDHCPパケットについて説明します。

- ディスカバリ:これは、FTDの内部インターフェイスからDHCPサーバに送信されるユニキャストパケットです。図に示すように、ペイロードでは、リレーエージェントのIPアドレスに

よってDHCPサーバの範囲が指定されます。

```
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
```

- オファー：このパケットはDHCPサーバからの応答で、FTDのDHCP範囲の送信元と宛先に付属しています。
- 要求：これは、FTDの内部インターフェイスからDHCPサーバに送信されるユニキャストパケットです。
- ACK:このパケットはDHCPサーバからの応答で、FTDのDHCP範囲の送信元と宛先に付属しています。

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ステップ1:DHCPサーバでwiresharkをダウンロードして有効にします。

ステップ2：図に示すように、キャプチャフィルタとしてDHCPを適用します。

No.	Time	Source	Destination	Protocol	Length	Info
						Number

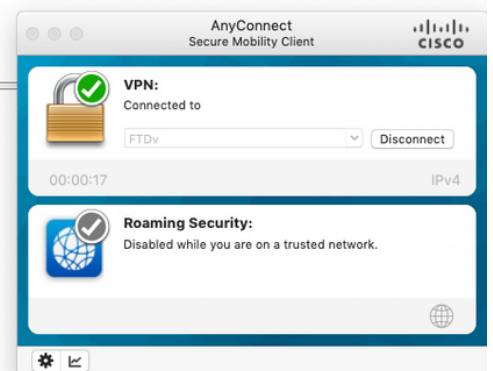


ステップ3: Anyconnectにログインすると、図のようにDHCPネゴシエーションが表示されます。

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  .....
```



関連情報

- このビデオでは、リモートアクセスVPNセッションがサードパーティのDHCPサーバによって割り当てられたIPアドレスを取得できるようにするFTDの設定例を示します。
- [テクニカル サポートとドキュメント - Cisco Systems](#)