

Konfigurieren des AnyConnect VPN-Clients auf FTD: DHCP-Server für die Adresszuweisung

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Konfigurieren des DHCP-Bereichs auf dem DHCP-Server](#)

[Schritt 2: Konfigurieren von AnyConnect](#)

[Schritt 2.1: Konfigurieren des Verbindungsprofils](#)

[Schritt 2.2: Konfigurieren der Gruppenrichtlinie](#)

[Schritt 2.3: Konfigurieren der Adresszuweisungsrichtlinie](#)

[IP-Helper-Szenario](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument enthält ein Konfigurationsbeispiel für Firepower Threat Defense (FTD) in Version 6.4, das Remotezugriff-VPN-Sitzungen den Erhalt einer IP-Adresse ermöglicht, die von einem Dynamic Host Configuration Protocol (DHCP)-Server eines Drittanbieters zugewiesen wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FTD
- FirePOWER Management Center (FMC)
- DHCP

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- FMC 6.5
- FTD 6.5

- Windows Server 2016

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

In diesem Dokument wird nicht die gesamte Remote-Zugriffskonfiguration beschrieben, sondern nur die erforderliche Konfiguration im FTD, um vom lokalen Adresspool zur DHCP-Adresszuweisung zu wechseln.

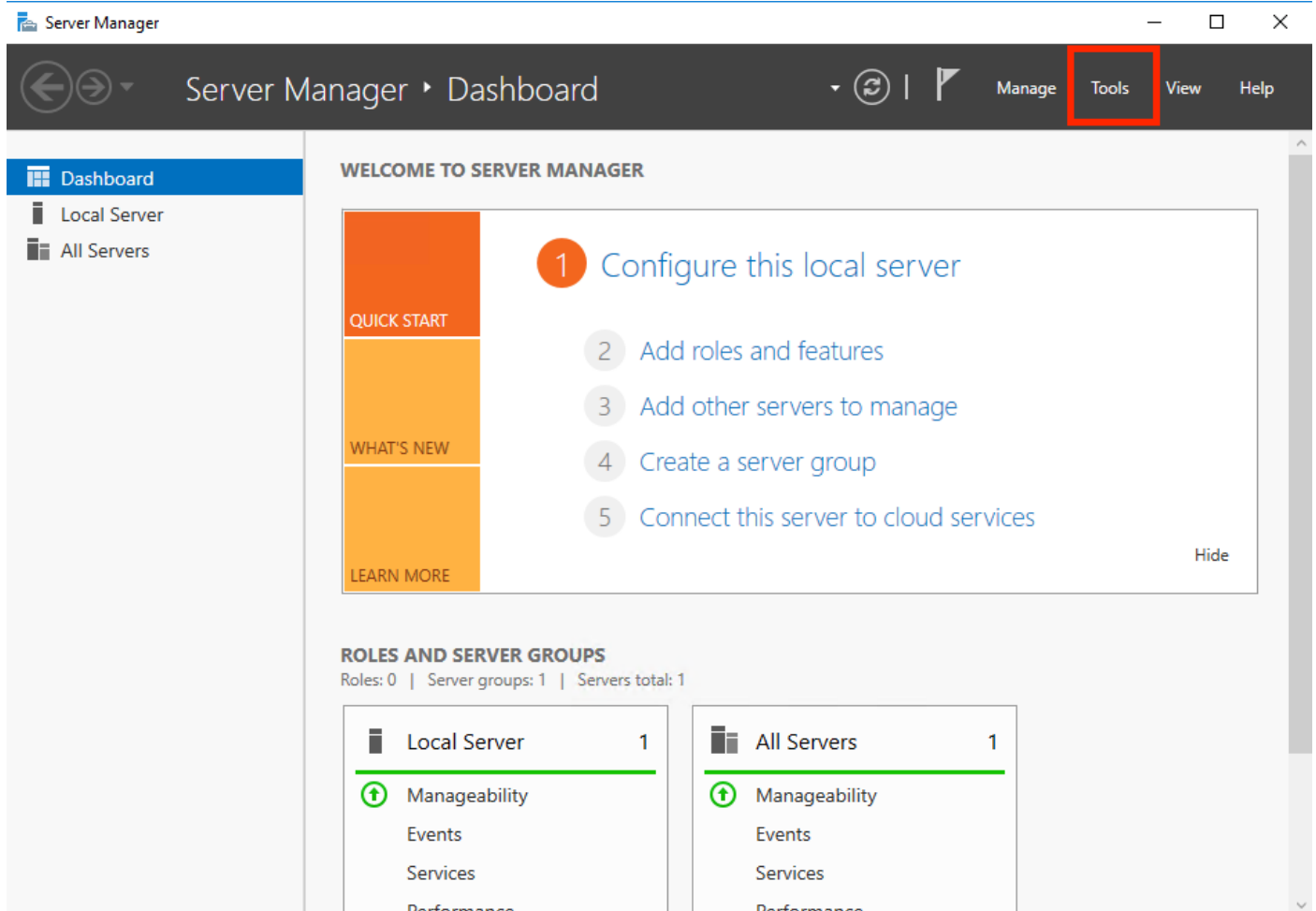
Wenn Sie nach dem AnyConnect-Konfigurationsbeispieldokument suchen, lesen Sie "Konfigurieren Sie den AnyConnect VPN Client auf FTD: Hairpinning and NAT Exemption".

Konfigurieren

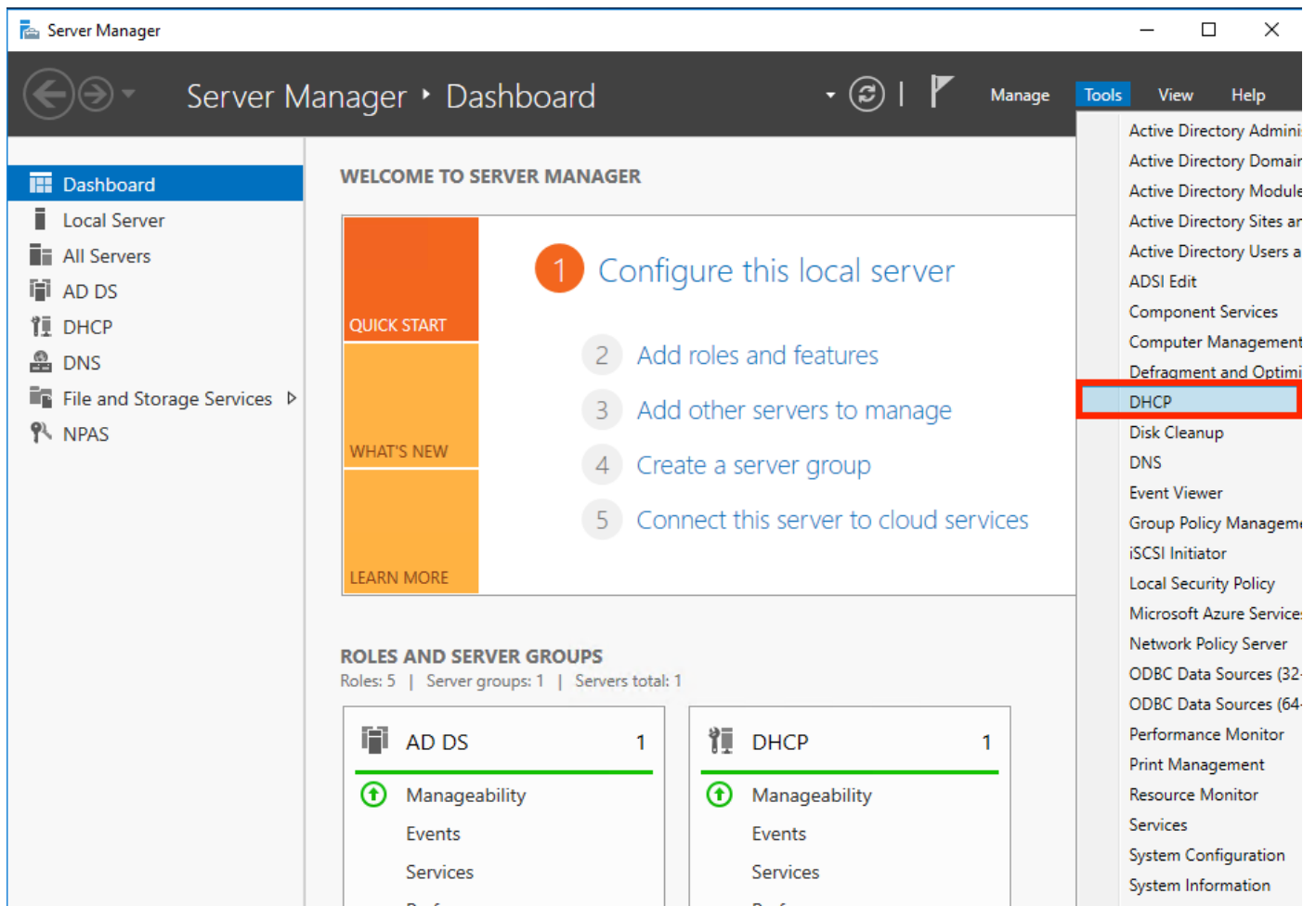
Schritt 1: Konfigurieren des DHCP-Bereichs auf dem DHCP-Server

In diesem Szenario befindet sich der DHCP-Server hinter der internen Schnittstelle der FTD.

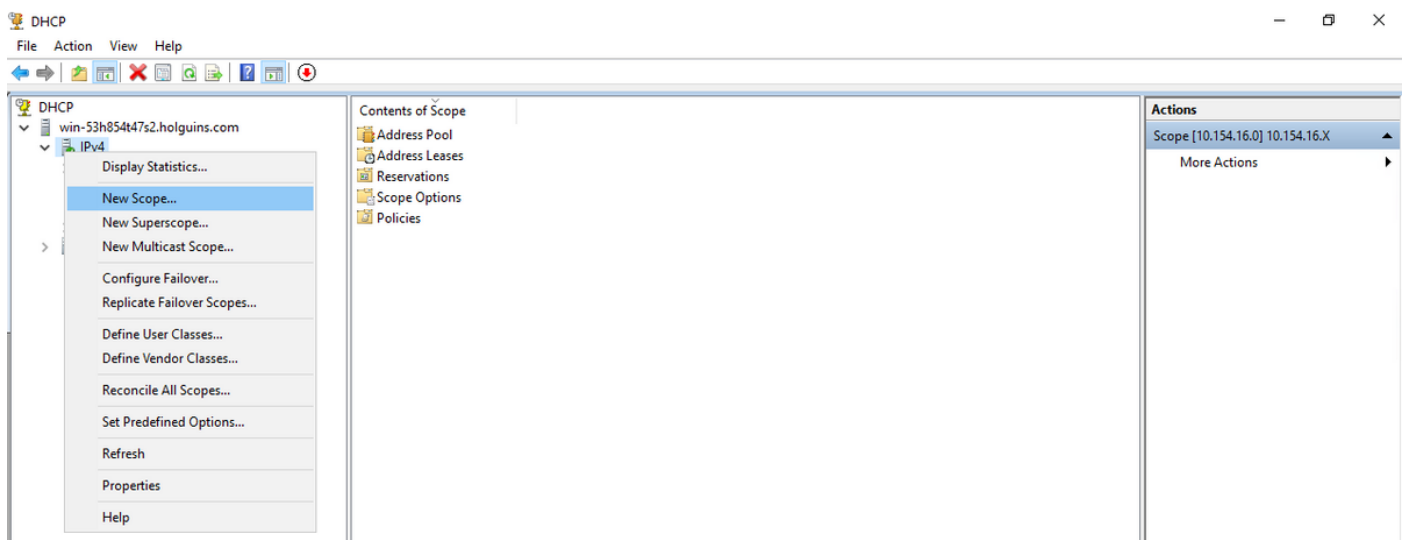
1. Öffnen Sie den Server Manager in Windows Server, und wählen Sie Tools wie im Bild dargestellt aus.



2. Wählen Sie DHCP:

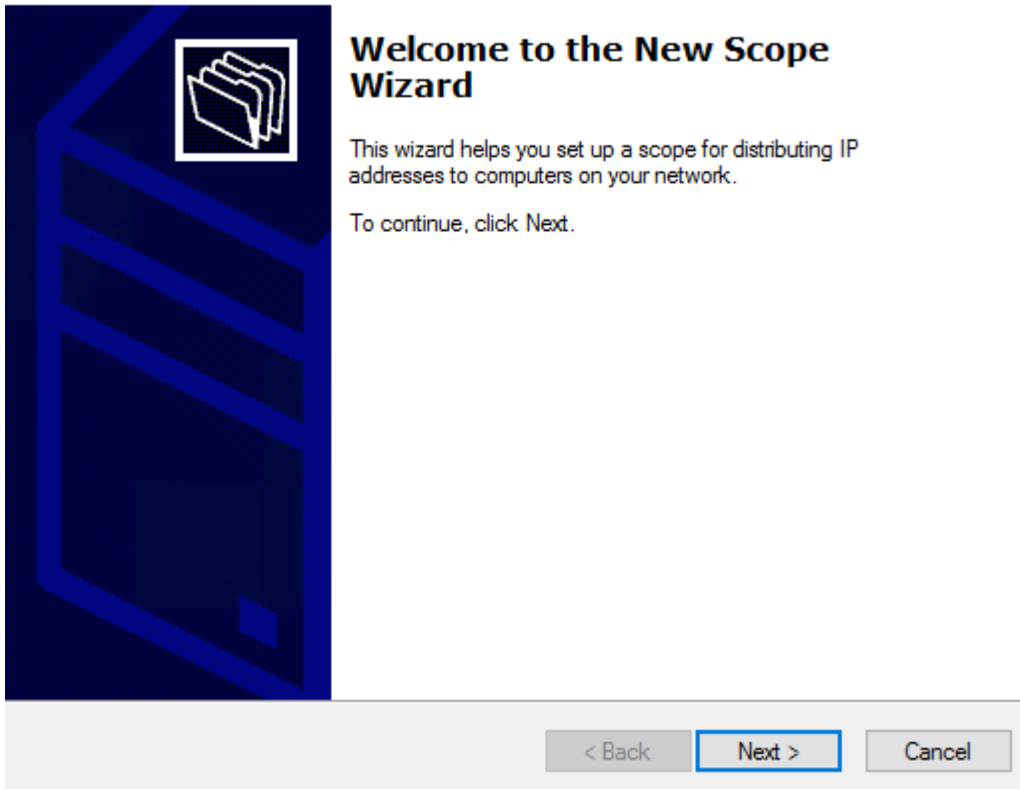


3. Wählen Sie IPv4 aus, klicken Sie mit der rechten Maustaste darauf, und wählen Sie Neuer Umfang aus, wie im Bild dargestellt.



4. Folgen Sie dem Assistenten, wie in der Abbildung dargestellt.

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. Weisen Sie dem Bereich einen Namen zu, wie im Bild dargestellt.

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. Konfigurieren Sie den Adressbereich wie im Bild dargestellt.

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. (Optional) Konfigurieren Sie die Ausschlüsse wie im Bild dargestellt.

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:

Excluded address range:

Subnet delay in milli second:

< Back Next > Cancel

8. Konfigurieren Sie die Leasingdauer wie im Bild dargestellt.

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. (Optional) Konfigurieren Sie DHCP-Bereichsoptionen:

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

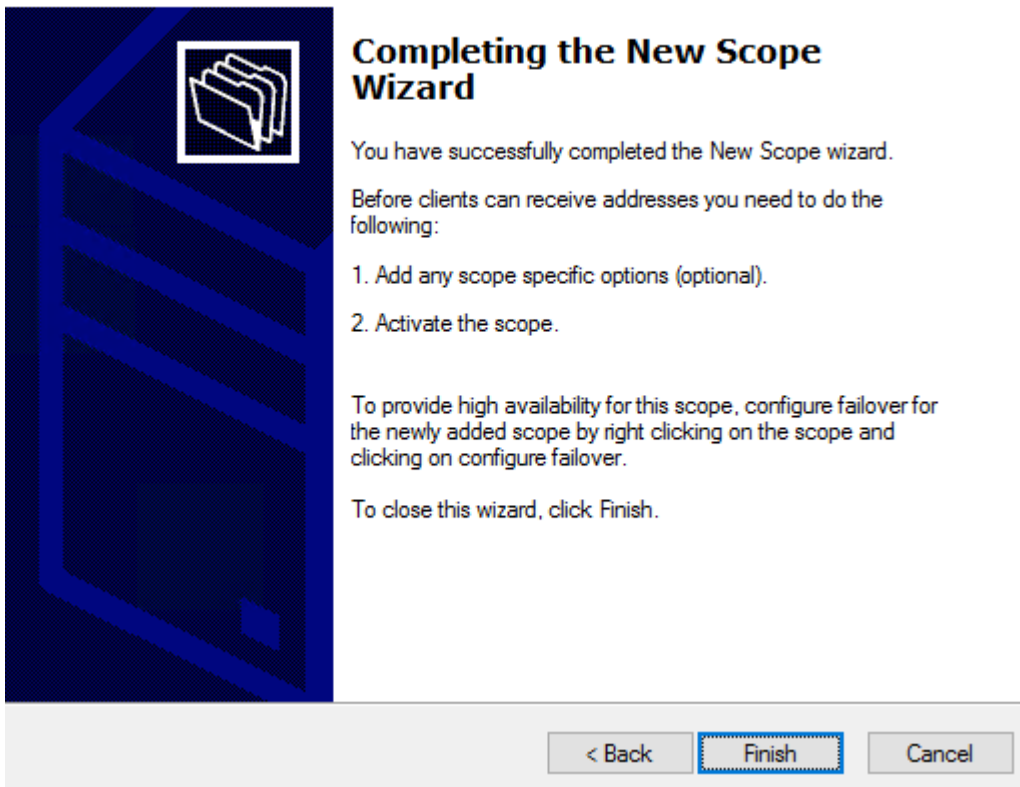
< Back

Next >

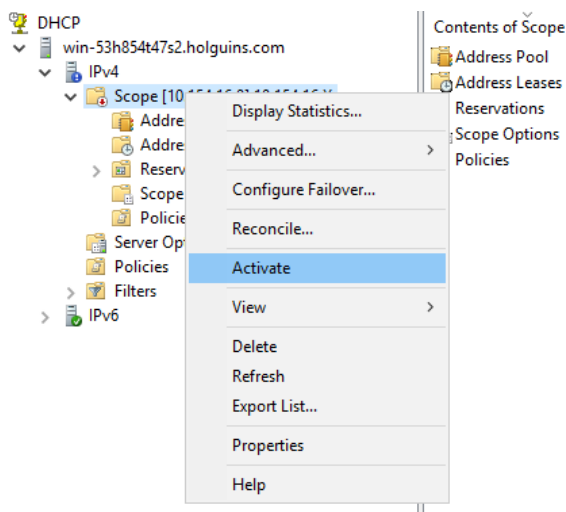
Cancel

10: Wählen Sie Beenden wie im Bild dargestellt aus.

New Scope Wizard



11: Klicken Sie mit der rechten Maustaste in den soeben erstellten Bereich, und wählen Sie Aktivieren aus, wie im Bild dargestellt.



Schritt 2: Konfigurieren von AnyConnect

Sobald der DHCP-Bereich konfiguriert und aktiviert ist, erfolgt das nächste Verfahren im FMC.

Schritt 2.1: Konfigurieren des Verbindungsprofils

1. Wählen Sie im Abschnitt "DHCP-Server"  und ein Objekt mit der IP-Adresse des DHCP-Servers erstellen.

2. Wählen Sie das Objekt als DHCP-Server aus, um eine IP-Adresse von anzufordern, wie im Bild gezeigt.

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

Schritt 2.2: Konfigurieren der Gruppenrichtlinie

1. Navigieren Sie im Menü Gruppenrichtlinie zu Allgemein > DNS/WINS. Es gibt einen Abschnitt DHCP-Netzwerkbereich, wie im Bild dargestellt.

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. Erstellen Sie ein neues Objekt, dieses muss den gleichen Netzwerkbereich wie der DHCP-Server haben.



Anmerkung: Dabei muss es sich um ein Hostobjekt und nicht um ein Subnetz handeln.

Edit Connection Profile ? X
Edit Group Policy ? X

Name:* dhcp-GP
Description:

General AnyConnect Advanced

VP
IP
Ba
DN
Sp

New Network Object ? X

Name DHCP-Scope
Description
Network ☒ Host ☐ Range ☐ Network ☐ FQDN
10.154.16.0
Allow Overrides ☐

Save Cancel

Save Cancel

3. Wählen Sie das DHCP-Bereichsobjekt und anschließend Speichern wie im Bild dargestellt.

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

Schritt 2.3: Konfigurieren der Adresszuweisungsrichtlinie

1. Navigieren Sie zu Erweitert > Adresszuweisungsrichtlinie, und stellen Sie sicher, dass die Option DHCP verwenden wie im Bild dargestellt umgeschaltet ist.

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Anyconnect-FTD Save Cancel

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

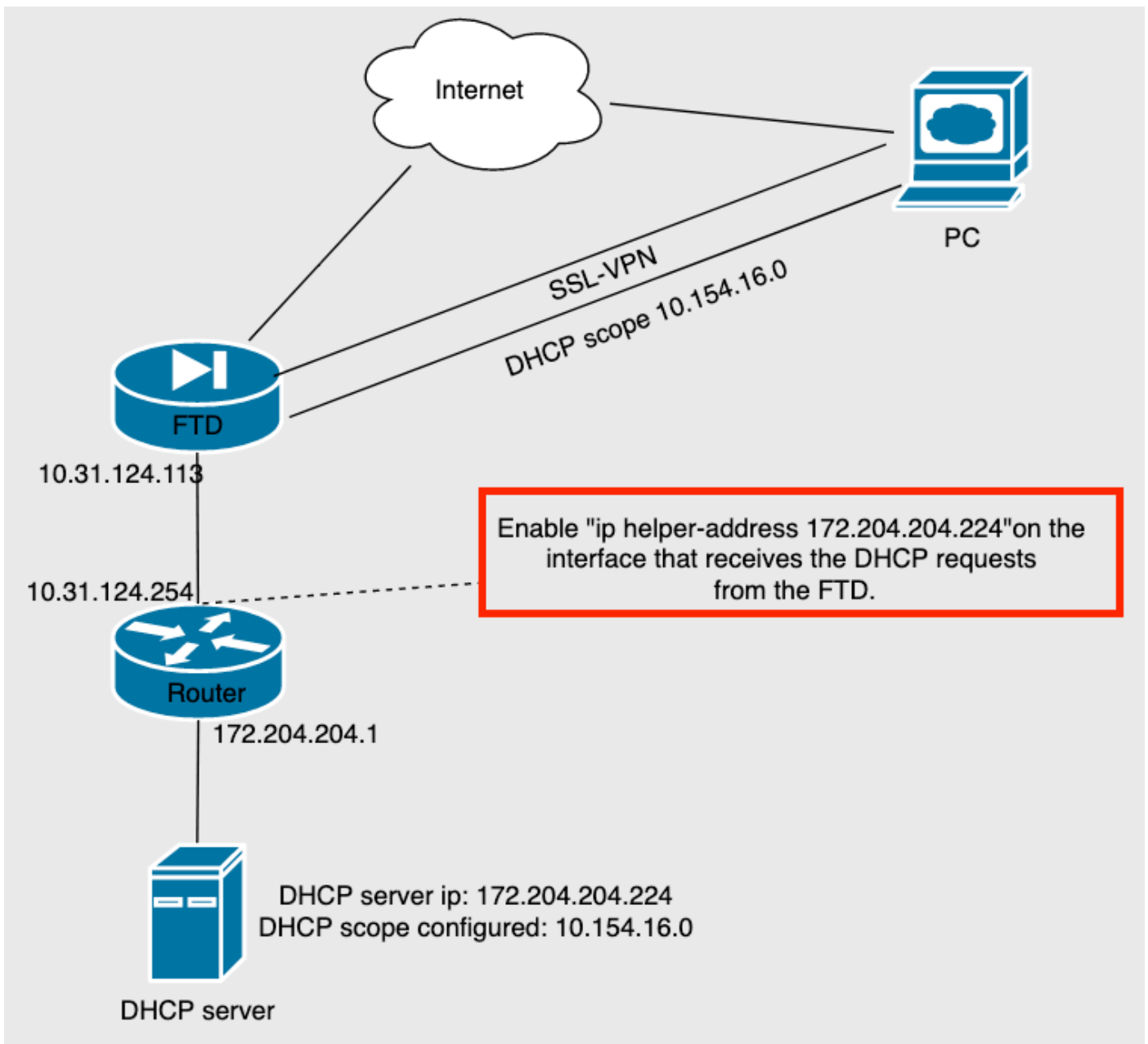
- ☒ Use authorization server (RADIUS Only)
- ☒ Use internal address pools

2. Speichern Sie die Änderungen, und stellen Sie die Konfiguration bereit.

IP-Helper-Szenario

Wenn sich der DHCP-Server hinter einem anderen Router im LAN befindet, ist ein "IP-Helper" erforderlich, um die Anfragen an den DHCP-Server weiterzuleiten.

Wie in der Abbildung dargestellt, veranschaulicht eine Topologie das Szenario und die erforderlichen Änderungen im Netzwerk.



Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

In diesem Abschnitt werden die DHCP-Pakete beschrieben, die zwischen dem FTD und dem DHCP-Server ausgetauscht werden.

- Erkennung: Dies ist ein Unicast-Paket, das von der internen FTD-Schnittstelle an den DHCP-Server gesendet wird.
 - In der Nutzlast gibt eine Relay-Agent-IP-Adresse den Bereich des DHCP-Servers an, wie im Abbild dargestellt.

```
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
```

- Angebot: Dieses Paket ist eine Antwort vom DHCP-Server. Es enthält die DHCP-Serverquelle und das Ziel des DHCP-Bereichs im FTD.
- Anforderung: Dies ist ein Unicast-Paket, das von der internen FTD-Schnittstelle an den DHCP-Server gesendet wird.
- ZURÜCK: Dieses Paket ist eine Antwort vom DHCP-Server. Es enthält die DHCP-Serverquelle und das Ziel des DHCP-Bereichs im FTD.

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Schritt 1: Laden Sie Wireshark auf den DHCP-Server herunter, und aktivieren Sie es.

Schritt 2: Wenden Sie DHCP wie im Bild gezeigt als Erfassungsfilter an.

dhcp

No.

Time

Source

Destination

Protocol

Length

Info

Number

AnyConnect Secure Mobility Client

CISCO

VPN:

Ready to connect.

FTDv

Connect

Roaming Security:

Disabled while you are on a trusted network.

Schritt 3: Melden Sie sich bei AnyConnect an. Die DHCP-Aushandlung sollte wie im Bild dargestellt angezeigt werden.

dhcp

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 P V--p--

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P V--p--

AnyConnect Secure Mobility Client

CISCO

VPN:

Connected to

FTDv

Disconnect

00:00:17

IPv4

Roaming Security:

Disabled while you are on a trusted network.

Zugehörige Informationen

- In diesem Video sehen Sie ein Konfigurationsbeispiel für FTD, das Remotezugriff-VPN-Sitzungen den Erhalt einer IP-Adresse ermöglicht, die von einem DHCP-Server eines Drittanbieters zugewiesen wurde.
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.