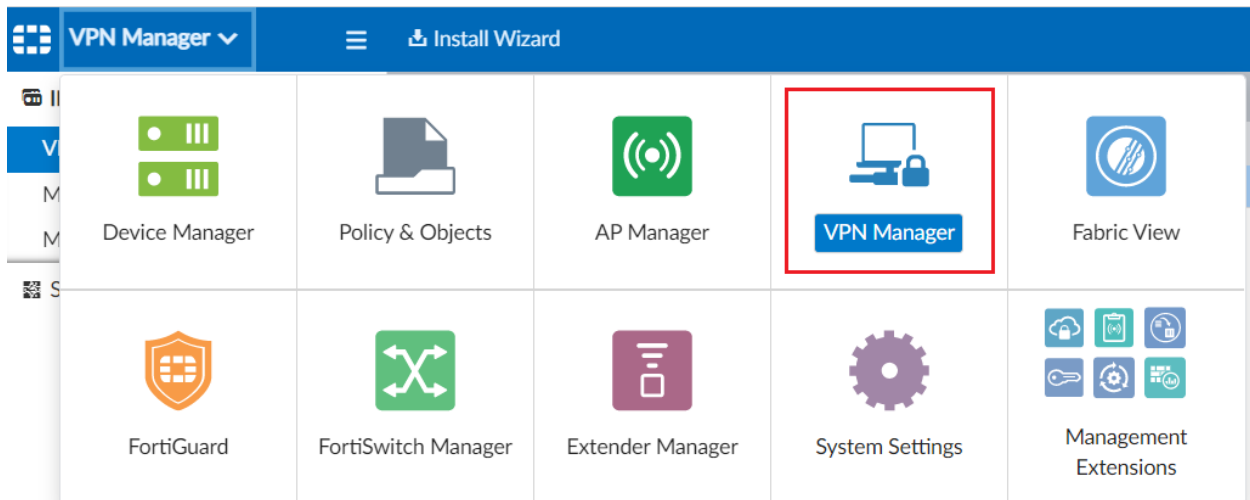


VPN Setup:

Create VPN Community:

You may create Full-Meshed, Star, and Dial-Up IPsec VPN Communities. IPsec VPN Communities are also sometimes called VPN topologies. We create a **Star Topology** with a hub and a spoke:

Go to **VPN Manager > IPsec VPN**.



In the toolbar, click **Create New**. The VPN Topology Setup Wizard dialog appears. Enter a name for the topology, In the Choose VPN topology field, Select **Star** Click **Next**.

← → ↻ ⚠ Not secure | https://192.168.114.210/p/app/#!/adom/vpn/ipsec/list

VPN Manager ▾ ☰ Install Wizard

IPsec VPN ▾

- VPN Communities (1)
- Map View
- Monitor

+ Create New ✎ Edit 🗑 Delete ⋮ More ⚙ Column Settings ▾

<input type="checkbox"/>	Name	Gateways
<input type="checkbox"/>	IPSec	> 0 Gateways

VPN Topology Setup Wizard

Choose VPN Topology

☐ Full Meshed

☒ Star

☐ Dial up

Next > < Back Cancel

Configure Phase 1 and Phase 2 according to your requirements.

VPN Topology Setup Wizard

Authentication & Encryption Settings:

Authentication

☒ Pre-shared Key ☐ Certificates

☐ Generate (random)

☒ Specify

Encryption

IKE Security (Phase 1) Properties

IKE Version ☒ 1 ☐ 2

#	Encryption	Authentication
1	<input type="text" value="DES"/>	<input type="text" value="MD5"/>

IPsec Security (Phase 2) Properties

#	Encryption	Authentication
1	<input type="text" value="DES"/>	<input type="text" value="MD5"/>

< Back **Next >** Cancel

VPN Topology Setup Wizard

☒ VPN Zone

IKE Security Phase 1 Advanced Properties

Diffie-Hellman Group(s) ☐ 1 ☒ 2 ☐ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32

Exchange Mode ☐ Aggressive ☒ Main(ID Protection)

Key Life (120-172800 seconds)

Dead Peer Detection ☐ Disable ☐ On Idle ☒ On Demand

IPsec Security Phase 2 Advanced Properties

Diffie-Hellman Group(s) ☐ 1 ☒ 2 ☐ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32

Replay Detection ☒

Perfect Forward Secrecy(PFS) ☒

Key Life ☒ Seconds ☐ KB ☐ Both seconds KB

☒ Auto-Negotiate

< Back **Next >** Cancel

Finally, **Phase 1** and **Phase 2** details are configured click **OK**.

VPN Topology Setup Wizard

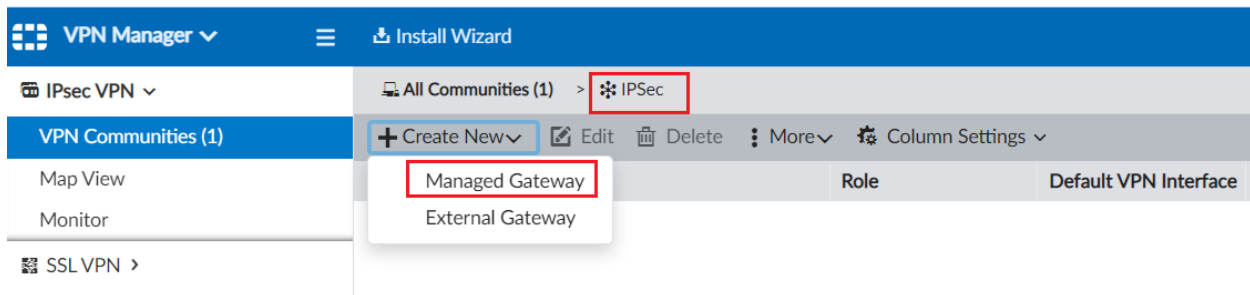
Summary

Name	IPSec
Topology	Star
Authentication	Pre-shared Key (Specify)
Encryption	IKE Security (Phase 1) Properties
	<input checked="" type="checkbox"/> 1: des-md5
	<input checked="" type="checkbox"/> Diffie-Hellman Group(s) : 2
	<input checked="" type="checkbox"/> Key Life : 28800 (seconds)
	<input checked="" type="checkbox"/> Dead Peer Detection : On Demand
	IPsec Security (Phase 2) Properties
	<input checked="" type="checkbox"/> 1: des-md5
	<input checked="" type="checkbox"/> Diffie-Hellman Group(s) : 2
	<input checked="" type="checkbox"/> Replay Detection
	<input checked="" type="checkbox"/> Perfect Forward Secrecy(PFS)
	<input checked="" type="checkbox"/> Key Life : 1800(seconds)
	<input checked="" type="checkbox"/> Auto Key Keep Alive
	<input checked="" type="checkbox"/> Auto-Negotiate
	<input checked="" type="checkbox"/> NAT-traversal : Keep Alive Frequency 10 (seconds)

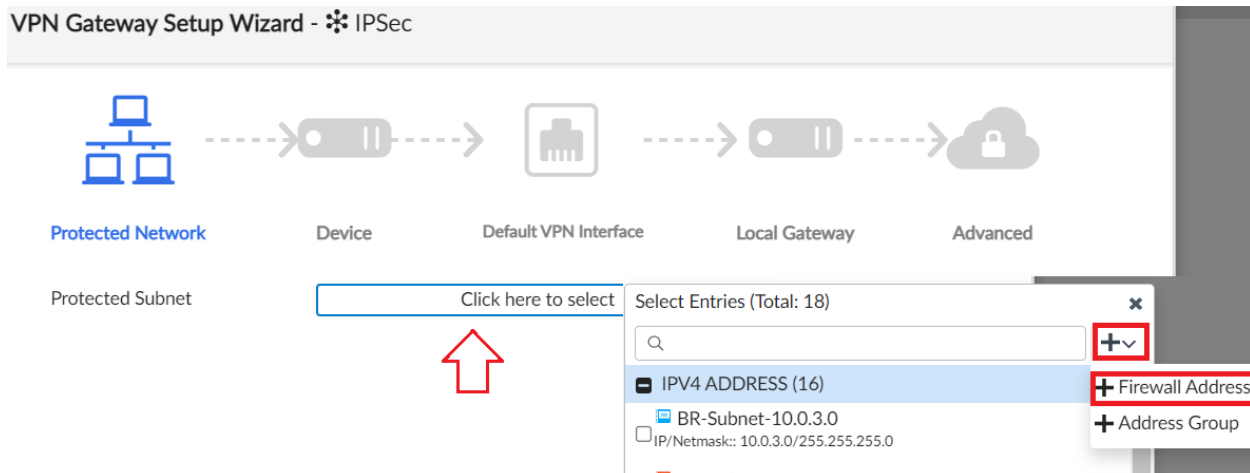
< Back **OK** Cancel

Create IPSEC VPN Gateways:

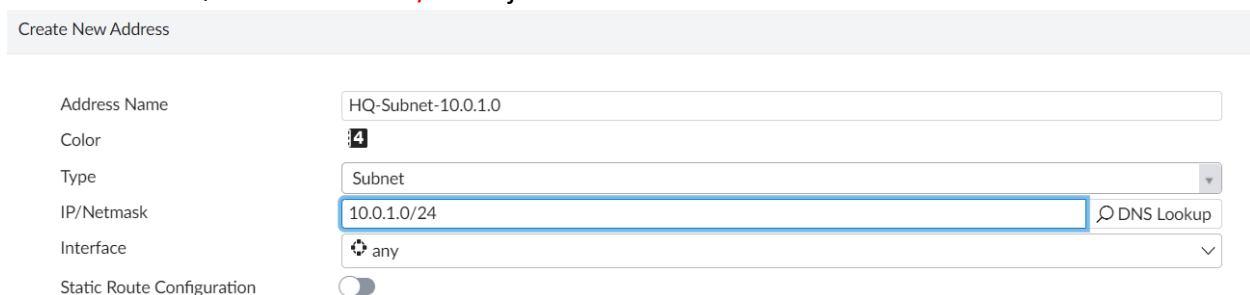
A VPN gateway functions as one end of a VPN tunnel. It receives incoming IPsec packets, decrypts the encapsulated data packets, then passes the data packets to the local network. It also encrypts, encapsulates, and sends the IPsec data packets to the gateway at the other end of the VPN tunnel. The IP address of a VPN gateway is usually the IP address of the network interface that connects to the Internet. Go to **VPN Manager > IPsec VPN**. In the tree menu, IPsec, In the toolbar, click **Create New > Managed Gateway**.



The VPN Gateway Setup Wizard – IPsec dialog appears. Select a Protected Subnet, and click **OK**. If you don't have object already created click on **plus** icon to create.



Let's create HQ Subnet **10.0.1.0/24** Object.



Let's create DC Subnet 10.0.2.0/24 Object.

Address Name	<input type="text" value="DC-Subnet-10.0.2.0"/>		
Color	<input type="text" value="4"/>		
Type	<input type="text" value="Subnet"/>		
IP/Netmask	<input type="text" value="10.0.2.0/255.255.255.0"/>	<input type="button" value="DNS Lookup"/>	
Interface	<input type="text" value="any"/>		
Static Route Configuration	<input type="checkbox"/>		
Comments	<div><div></div><div>0/255</div></div>		
Add To Groups	<input type="button" value="Click here to select"/>		
Advanced Options >			
Per-Device Mapping	<input type="checkbox"/>		
Revision			
Change Note *	<div></div>		

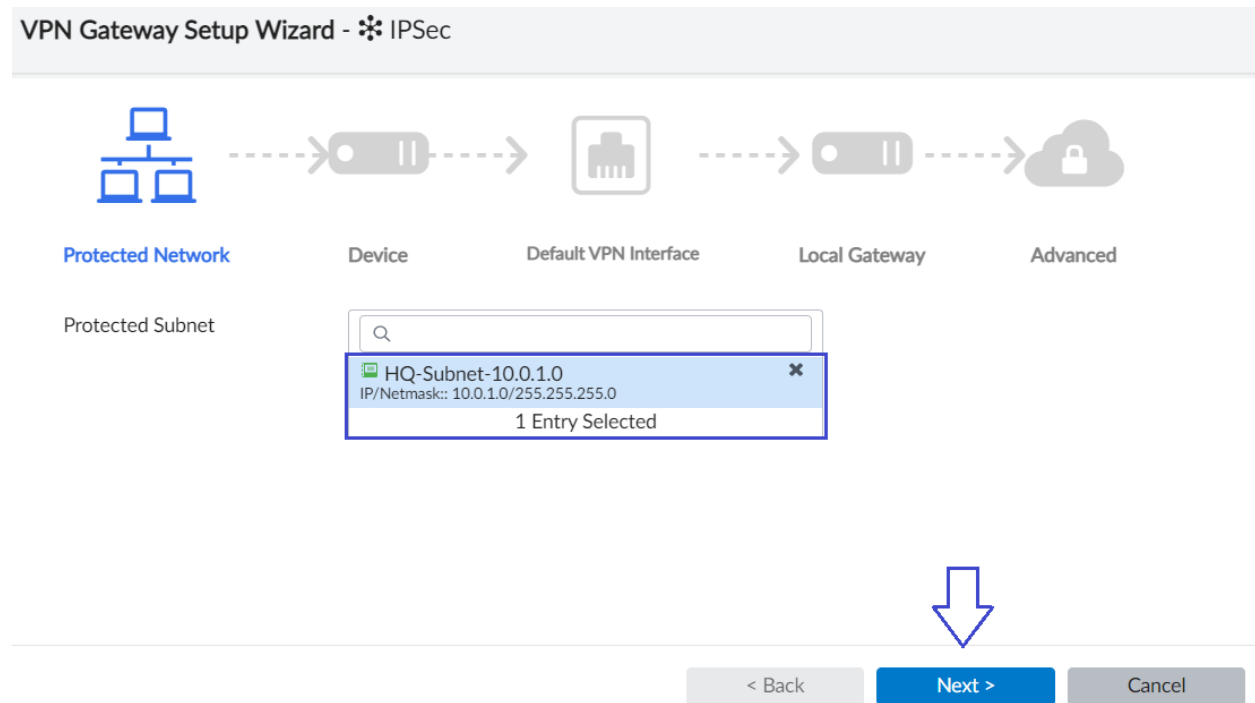
Let's create BR Subnet 10.0.3.0/24 Object.

Edit Address

Address Name	<input type="text" value="BR-Subnet-10.0.3.0"/>		
Color	<input type="text" value="4"/>		
Type	<input type="text" value="Subnet"/>		
IP/Netmask	<input type="text" value="10.0.3.0/255.255.255.0"/>	<input type="button" value="DNS Lookup"/>	
Interface	<input type="text" value="any"/>		
Static Route Configuration	<input type="checkbox"/>		
Comments	<div><div></div><div>0/255</div></div>		
Add To Groups	<input type="button" value="Click here to select"/>		
Advanced Options >			
Per-Device Mapping	<input type="checkbox"/>		

Select a **Protected Subnet**, and click **OK**.

VPN Gateway Setup Wizard - ❄️ IPSec



The diagram shows a sequence of steps: Protected Network (represented by a server icon), Device (represented by a router icon), Default VPN Interface (represented by a server icon), Local Gateway (represented by a router icon), and Advanced (represented by a cloud icon). The 'Protected Network' step is currently active.

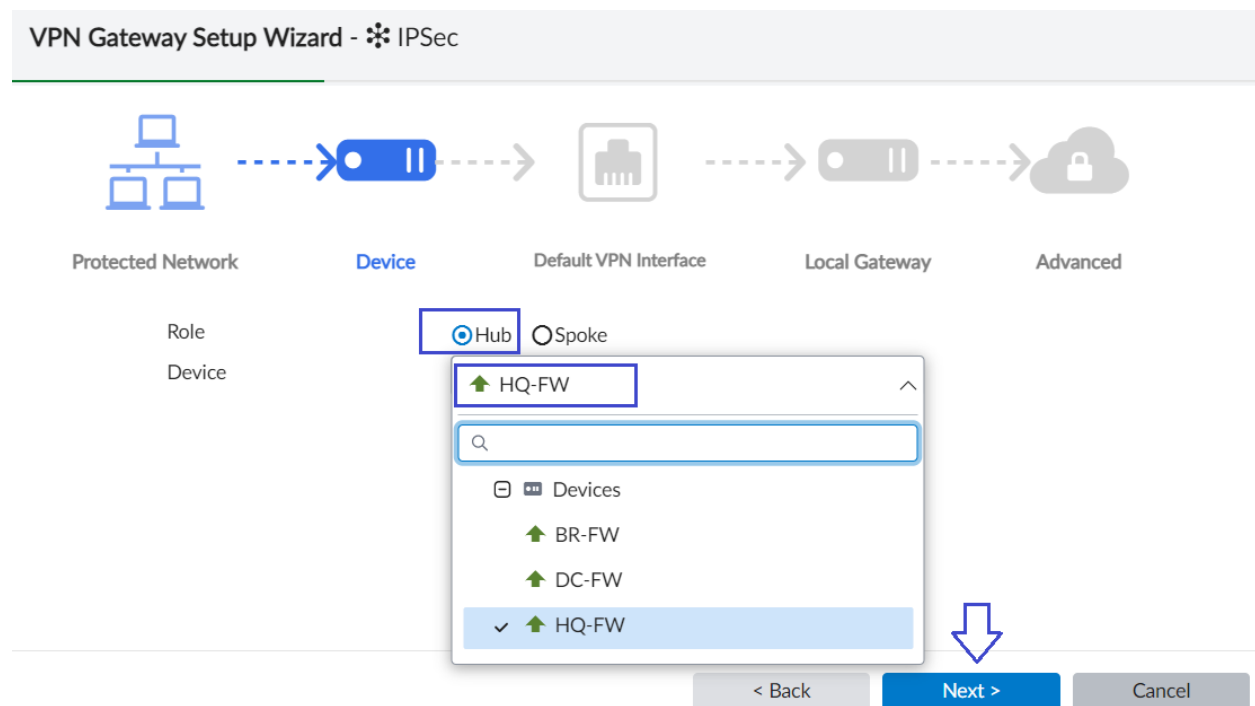
Protected Subnet

HQ-Subnet-10.0.1.0
IP/Netmask:: 10.0.1.0/255.255.255.0
1 Entry Selected

< Back Next > Cancel

Set the Role field to **Hub** and click **Next**.

VPN Gateway Setup Wizard - ❄️ IPSec



The diagram shows a sequence of steps: Protected Network (represented by a server icon), Device (represented by a router icon), Default VPN Interface (represented by a server icon), Local Gateway (represented by a router icon), and Advanced (represented by a cloud icon). The 'Device' step is currently active.

Role
Device

Hub Spoke

HQ-FW

Devices

BR-FW


DC-FW

✓ HQ-FW

< Back Next > Cancel

Default VPN interface usually the internet-facing interface in this case **port1** click **Next**.

VPN Gateway Setup Wizard - ❄️ IPSec



Protected Network

Device

Default VPN Interface

Local Gateway

Advanced

Default VPN Interface

port1

▼

Hub-to-Hub Interface

Click to select

▼

(Required for multiple Hubs)


< Back

Next >

Cancel

Set the local Gateway the public IP Address of Internet facing Interface **192.168.1.1**.

VPN Gateway Setup Wizard - ❄️ IPSec



Protected Network

Device

Default VPN Interface

Local Gateway

Advanced

Local Gateway

192.168.1.1

< Back

Next >

Cancel


In **Routing** choose the Automatic Option and Click **OK**.

VPN Gateway Setup Wizard - ❄️ IPsec

Local ID

Routing ☐ Manual (via Device Manager) ☒ Automatic

Summary Network(s)

Seq#	Network	Priority
Click here to add a new entry. 		

Advanced Options >

< Back **OK** Cancel

Create SPOKE-1 DC-FW:

The VPN Gateway Setup Wizard – **IPsec** dialog appears. Select a **Protected Subnet**, and click **OK**.

VPN Gateway Setup Wizard - ❄️ IPsec

Protected Network Device Default VPN Interface Local Gateway Advanced

Protected Subnet

DC-Subnet-10.0.2.0
IP/Netmask:: 10.0.2.0/255.255.255.0
1 Entry Selected

< Back **Next >** Cancel

Set the Role field to **Spoke** this time and from dropdown choose DC-FW click **Next**.

VPN Gateway Setup Wizard - ❄️ IPSec

Protected Network **Device** Default VPN Interface Local Gateway Advanced

Role
Device

☐ Hub ☒ Spoke

↑ DC-FW

< Back **Next >** Cancel

Default VPN interface usually the internet-facing interface in this case **port1** click **Next**.

VPN Gateway Setup Wizard - ❄️ IPSec

Protected Network Device **Default VPN Interface** Local Gateway Advanced






Default VPN Interface

port1

< Back **Next >** Cancel


Set the **Local Gateway** the public IP Address of Internet facing Interface **192.168.3.1**.

VPN Gateway Setup Wizard - ❄️ IPSec



Protected Network Device Default VPN Interface **Local Gateway** Advanced

Local Gateway



In **Routing** choose the Automatic Option and Click **OK**.

VPN Gateway Setup Wizard - ❄️ IPSec

Local ID

Routing ☐ Manual (via Device Manager) ☒ Automatic

Advanced Options >

Create SPOKE-2 BR-FW:

The VPN Gateway Setup Wizard – IPsec dialog appears. Select a **Protected Subnet**, and click **OK**.

VPN Gateway Setup Wizard - ❄ IPsec

The diagram shows a sequence of five steps: Protected Network, Device, Default VPN Interface, Local Gateway, and Advanced. The 'Protected Network' step is currently active, indicated by a blue icon and text. Below the step names, the 'Protected Subnet' field is highlighted with a red box. It contains a search bar and a list of results. The first result, 'BR-Subnet-10.0.3.0' with IP/Netmask '10.0.3.0/255.255.255.0', is selected. Below the list, it says '1 Entry Selected'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A red arrow points down to the 'Next >' button.

Protected Network Device Default VPN Interface Local Gateway Advanced

Protected Subnet

BR-Subnet-10.0.3.0
IP/Netmask:: 10.0.3.0/255.255.255.0
1 Entry Selected

< Back Next > Cancel

Set the Role field to **Spoke** this time and from dropdown choose BR-FW click **Next**.

VPN Gateway Setup Wizard - ❄ IPsec

The diagram shows the same sequence of five steps. The 'Device' step is now active, indicated by a blue icon and text. Below the step names, the 'Role' and 'Device' fields are highlighted with a red box. The 'Role' field has two radio buttons: 'Hub' and 'Spoke', with 'Spoke' selected. The 'Device' field is a dropdown menu showing 'BR-FW' with an upward arrow icon. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A red arrow points down to the 'Next >' button.

Protected Network Device Default VPN Interface Local Gateway Advanced

Role
Device

Hub Spoke
BR-FW

< Back Next > Cancel

Default VPN interface usually the internet-facing interface in this case **port1** click **Next**.

VPN Gateway Setup Wizard - ❄️ IPSec



The diagram shows a sequence of steps: Protected Network (represented by a network icon), Device (represented by a router icon), Default VPN Interface (represented by a router icon with a blue border), Local Gateway (represented by a router icon), and Advanced (represented by a cloud with a lock icon). Below the diagram, the 'Default VPN Interface' dropdown menu is highlighted with a red box and contains the selection 'port1'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A red arrow points down to the 'Next >' button.

Protected Network Device **Default VPN Interface** Local Gateway Advanced

Default VPN Interface:

< Back **Next >** Cancel

Set the **Local Gateway** the public IP Address of Internet facing Interface **192.168.5.1**.

VPN Gateway Setup Wizard - ❄️ IPSec



The diagram shows the same sequence of steps as the previous screen, but now 'Local Gateway' is highlighted with a blue border. Below the diagram, the 'Local Gateway' text box is highlighted with a red box and contains the value '192.168.5.1'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A red arrow points down to the 'Next >' button.

Protected Network Device Default VPN Interface **Local Gateway** Advanced

Local Gateway:

< Back **Next >** Cancel

In **Routing** choose the **Automatic** Option and Click **OK**.

VPN Gateway Setup Wizard - ❄️ IPsec

Local ID

Routing ☐ Manual (via Device Manager) ☒ Automatic

Advanced Options >

< Back OK Cancel

Finally, one Hub and two Spokes are created.

VPN Manager		Install Wizard			
IPsec VPN		All Communities (1) > ❄️ IPsec			
VPN Communities (1)		+ Create New Edit Delete More Column Settings			
Map View		<input type="checkbox"/>	Name	Role	Default VPN Interface Protected Subnet
Monitor		<input type="checkbox"/>	↑ HQ-FW[root]	Hub	port1 HQ-Subnet-10.0.1.0
SSL VPN >		<input type="checkbox"/>	↑ DC-FW[root]	Spoke	port1 DC-Subnet-10.0.2.0
		<input type="checkbox"/>	↑ DC-FW[root]	Spoke	port1 BR-Subnet-10.0.3.0

Install Wizard - Policy Package (HQ-FW)

✓ Policy package (HQ-FW) is installed successfully.

100%

Total: 1/1, ✓ Success: 1, ⚠ Warning: 0, ✗ Error: 0

View Installation Log

View Progress Report

Column Settings

Search...

#	Name	Time Used	Status
1	HQ-FW	40s	install and save finished status=OK

Similarly, install Wizard on Spoke-1 DC-FW and Spoke-2 BR-FW

Install Wizard

Install Policy Package & Device Settings

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package

DC-FW

Comment

0/127

☐ Create ADOM Revision

☐ Schedule Install

☐ Install Device Settings (only)



Next >

Cancel

Install Wizard - Policy Package and Device Setting (DC-FW)

Please select one or more devices to install (ⓘ Use checkbox or Ctrl or Shift key for multiple selections)

<input type="checkbox"/>	Device Name	IP Address	Platform
<input checked="" type="checkbox"/>	DC-FW	192.168.3.1	FortiGate-VM64-KVM

< Back

Next >

Cancel