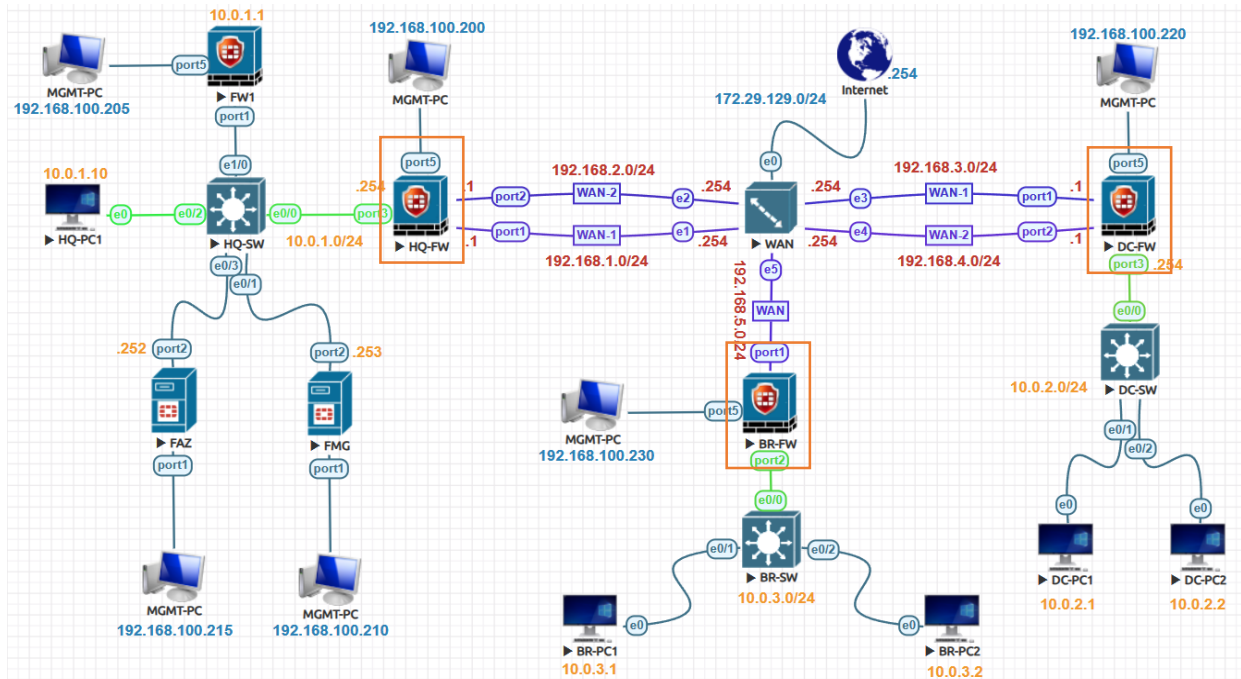


## ADVPN CLI Template Lab:



HUB Firewall	HQ-FW
Spoke-1 Firewall	DC-FW
Spoke-2 Firewall	BR-FW
HUB Tunnel Interface IP Address	172.16.1.1
Spoke-1 Tunnel Interface IP Address	172.16.1.2
Spoke-2 Tunnel Interface IP Address	172.16.1.3
HUB Public IP Address	192.168.1.1
IKE Version	Version 2
Pre-Shared Key	test123
Phase 1 and Phase 2 Name	advpn
VPN Proposal	DES and MD5
VPN Tunnel Interface Name	advpn
BGP AS	65000
BGP Flavor	IBGP
Topology	HUB and Spoke
Spoke Communication	Spoke to Spoke Shortcut

Hub:

`set exchange-interface-ip enable` Replace with `set auto-discovery-sender enable`

SPOKES:

`set exchange-interface-ip enable` Replace with `set auto-discovery-receiver enable`

### Hub HQ-FW Phase 1 Configuration

```
HQ-FW # config vpn ipsec phase1-interface
HQ-FW (phase1-interface) # edit advpn
HQ-FW (advpn) # set ike-version 2
HQ-FW (advpn) # set proposal des-md5
HQ-FW (advpn) # set dhgrp 5
HQ-FW (advpn) # set authmethod psk
HQ-FW (advpn) # set psksecret test123
HQ-FW (advpn) # set nattraversal disable
HQ-FW (advpn) # set keylife 86400
HQ-FW (advpn) # set dpd on-demand
HQ-FW (advpn) # set dpd-retrycount 3
HQ-FW (advpn) # set dpd-retryinterval 20
HQ-FW (advpn) # set interface port1
HQ-FW (advpn) # set type dynamic
HQ-FW (advpn) # set peertype any
HQ-FW (advpn) # set net-device disable
HQ-FW (advpn) # set add-route disable
HQ-FW (advpn) # set exchange-interface-ip disable
HQ-FW (advpn) # set auto-discovery-sender enable
HQ-FW (advpn) # next
HQ-FW (phase1-interface) # end
```

### Hub HQ-FW Phase 2 Configuration

```
HQ-FW # config vpn ipsec phase2-interface
HQ-FW (phase2-interface) # edit advpn
HQ-FW (advpn) # set encapsulation tunnel-mode
HQ-FW (advpn) # set proposal des-md5
HQ-FW (advpn) # set pfs disable
HQ-FW (advpn) # set keylife-type seconds
HQ-FW (advpn) # set keylifeseconds 43200
HQ-FW (advpn) # set keepalive disable
HQ-FW (advpn) # set phase1name advpn
HQ-FW (advpn) # next
HQ-FW (phase2-interface) # end
```

### Hub HQ-FW Tunnel Interface Configuration

```
HQ-FW # config system interface
HQ-FW (interface) # edit advpn
HQ-FW (advpn) # set ip 172.16.1.1/32
HQ-FW (advpn) # set remote-ip 172.16.1.254/24
HQ-FW (advpn) # set allowaccess ping
HQ-FW (advpn) # set type tunnel
HQ-FW (advpn) # set interface port1
HQ-FW (advpn) # next
HQ-FW (interface) # end
```

### Hub HQ-FW BGP Configuration

```
HQ-FW # config router bgp
HQ-FW (bgp) # set as 65000
HQ-FW (bgp) # set router-id 10.0.1.254
HQ-FW (bgp) # set ibgp-multipath enable
HQ-FW (bgp) # config neighbor-group
HQ-FW (neighbor-group) # edit advpn-peers
HQ-FW (advpn-peers) # set remote-as 65000
HQ-FW (advpn-peers) # set interface advpn
HQ-FW (advpn-peers) # set update-source advpn
HQ-FW (advpn-peers) # set route-reflector-client enable
HQ-FW (advpn-peers) # next
HQ-FW (neighbor-group) # end
HQ-FW (bgp) # config neighbor-range
HQ-FW (neighbor-range) # edit 1
HQ-FW (1) # set prefix 172.16.1.0 255.255.255.0
HQ-FW (1) # set neighbor-group advpn-peers
HQ-FW (1) # next
HQ-FW (neighbor-range) # end
HQ-FW (bgp) # config network
HQ-FW (network) # edit 1
HQ-FW (1) # set prefix 10.0.1.0 255.255.255.0
HQ-FW (1) # next
HQ-FW (network) # end
HQ-FW (bgp) # end
```

#### Hub HQ-FW LAN to VPN Policy

```
HQ-FW # config firewall policy
HQ-FW (policy) # edit 1
HQ-FW (1) # set name LAN-to-VPN
HQ-FW (1) # set srcintf port3
HQ-FW (1) # set dstintf advpn
HQ-FW (1) # set action accept
HQ-FW (1) # set srcaddr all
HQ-FW (1) # set dstaddr all
HQ-FW (1) # set schedule always
HQ-FW (1) # set service ALL
HQ-FW (1) # set logtraffic all
HQ-FW (1) # set status enable
HQ-FW (1) # end
```

#### Hub HQ-FW VPN to LAN Policy

```
HQ-FW # config firewall policy
HQ-FW (policy) # edit 2
HQ-FW (2) # set name VPN-to-LAN
HQ-FW (2) # set srcintf advpn
HQ-FW (2) # set dstintf port3
HQ-FW (2) # set action accept
HQ-FW (2) # set srcaddr all
HQ-FW (2) # set dstaddr all
HQ-FW (2) # set schedule always
HQ-FW (2) # set service ALL
HQ-FW (2) # set logtraffic all
HQ-FW (2) # set status enable
```

#### Hub HQ-FW Spoke to Spoke Policy

```
HQ-FW # config firewall policy
HQ-FW (policy) # edit 4
HQ-FW (4) # set name VPN-to-VPN
HQ-FW (4) # set srcintf advpn
HQ-FW (4) # set dstintf advpn
HQ-FW (4) # set action accept
HQ-FW (4) # set srcaddr all
HQ-FW (4) # set dstaddr all
HQ-FW (4) # set schedule always
HQ-FW (4) # set service ALL
HQ-FW (4) # set logtraffic all
HQ-FW (4) # set status enable
HQ-FW (4) # end
```

### Spoke-1 DC-FW Phase 1 Configuration

```
DC-FW # config vpn ipsec phase1-interface
DC-FW (phase1-interface) # edit advpn
DC-FW (advpn) # set ike-version 2
DC-FW (advpn) # set proposal des-md5
DC-FW (advpn) # set dhgrp 5
DC-FW (advpn) # set authmethod psk
DC-FW (advpn) # set psksecret test123
DC-FW (advpn) # set nattraversal disable
DC-FW (advpn) # set keylife 86400
DC-FW (advpn) # set dpd on-idle
DC-FW (advpn) # set dpd-retrycount 3
DC-FW (advpn) # set dpd-retryinterval 20
DC-FW (advpn) # set interface port1
DC-FW (advpn) # set type static
DC-FW (advpn) # set peertype any
DC-FW (advpn) # set remote-gw 192.168.1.1
DC-FW (advpn) # set net-device enable
DC-FW (advpn) # set add-route disable
DC-FW (advpn) # set exchange-interface-ip disable
DC-FW (advpn) # set auto-discovery-receiver enable
DC-FW (advpn) # next
DC-FW (phase1-interface) # end
```

### Spoke-1 DC-FW Phase 2 Configuration

```
DC-FW # config vpn ipsec phase2-interface
DC-FW (phase2-interface) # edit advpn
DC-FW (advpn) # set encapsulation tunnel-mode
DC-FW (advpn) # set proposal des-md5
DC-FW (advpn) # set pfs disable
DC-FW (advpn) # set keylife-type seconds
DC-FW (advpn) # set keylifeseconds 43200
DC-FW (advpn) # set phase1name advpn
DC-FW (advpn) # set auto-negotiate enable
DC-FW (advpn) # next
DC-FW (phase2-interface) # end
```

### Spoke-1 DC-FW Tunnel Interface Configuration

```
DC-FW # config system interface
DC-FW (interface) # edit advpn
DC-FW (advpn) # set ip 172.16.1.2/32
DC-FW (advpn) # set remote-ip 172.16.1.1/24
DC-FW (advpn) # set allowaccess ping
DC-FW (advpn) # set type tunnel
DC-FW (advpn) # set interface port1
DC-FW (advpn) # next
DC-FW (interface) # end
```

### Spoke-1 DC-FW BGP Configuration

```
DC-FW # config router bgp
DC-FW (bgp) # set as 65000
DC-FW (bgp) # set router-id 10.0.2.254
DC-FW (bgp) # set ibgp-multipath enable
DC-FW (bgp) # config neighbor
DC-FW (neighbor) # edit 172.16.1.1
DC-FW (172.16.1.1) # set remote-as 65000
DC-FW (172.16.1.1) # set interface advpn
DC-FW (172.16.1.1) # set update-source advpn
DC-FW (172.16.1.1) # next
DC-FW (neighbor) # end
DC-FW (bgp) # config network
DC-FW (network) # edit 1
DC-FW (1) # set prefix 10.0.2.0 255.255.255.0
DC-FW (1) # next
DC-FW (network) # end
```

### Spoke-1 DC-FW LAN to VPN Policy

```
DC-FW # config firewall policy
DC-FW (policy) # edit 2
DC-FW (2) # set name LAN-to-VPN
DC-FW (2) # set srcintf port3
DC-FW (2) # set dstintf advpn
DC-FW (2) # set action accept
DC-FW (2) # set srcaddr all
DC-FW (2) # set dstaddr all
DC-FW (2) # set schedule always
DC-FW (2) # set service ALL
DC-FW (2) # set logtraffic all
DC-FW (2) # set status enable
DC-FW (2) # end
```

### Spoke-1 DC-FW VPN to LAN Policy

```
DC-FW # config firewall policy
DC-FW (policy) # edit 3
DC-FW (3) # set name VPN-to-LAN
DC-FW (3) # set srcintf advpn
DC-FW (3) # set dstintf port3
DC-FW (3) # set action accept
DC-FW (3) # set srcaddr all
DC-FW (3) # set dstaddr all
DC-FW (3) # set schedule always
DC-FW (3) # set service ALL
DC-FW (3) # set logtraffic all
DC-FW (3) # set status enable
DC-FW (3) # end
```

### Spoke-2 BR-FW Phase 1 Configuration

```
BR-FW # config vpn ipsec phase1-interface
BR-FW (phase1-interface) # edit advpn
BR-FW (advpn) # set ike-version 2
BR-FW (advpn) # set proposal des-md5
BR-FW (advpn) # set dhgrp 5
BR-FW (advpn) # set authmethod psk
BR-FW (advpn) # set psksecret test123
BR-FW (advpn) # set nattraversal disable
BR-FW (advpn) # set keylife 86400
BR-FW (advpn) # set dpd on-idle
BR-FW (advpn) # set dpd-retrycount 3
BR-FW (advpn) # set dpd-retryinterval 20
BR-FW (advpn) # set interface port1
BR-FW (advpn) # set type static
BR-FW (advpn) # set peertype any
BR-FW (advpn) # set remote-gw 192.168.1.1
BR-FW (advpn) # set net-device enable
BR-FW (advpn) # set exchange-interface-ip disable
BR-FW (advpn) # set auto-discovery-receiver enable
BR-FW (advpn) # next
BR-FW (phase1-interface) # end
```

### Spoke-2 BR-FW Phase 2 Configuration

```
BR-FW # config vpn ipsec phase2-interface
BR-FW (phase2-interface) # edit advpn
BR-FW (advpn) # set encapsulation tunnel-mode
BR-FW (advpn) # set proposal des-md5
BR-FW (advpn) # set pfs disable
BR-FW (advpn) # set keylife-type seconds
BR-FW (advpn) # set keylifeseconds 43200
BR-FW (advpn) # set phase1name advpn
BR-FW (advpn) # set auto-negotiate enable
BR-FW (advpn) # next
BR-FW (phase2-interface) # end
```



### Spoke-2 BR-FW Tunnel Interface Configuration

```
BR-FW # config system interface
BR-FW (interface) # edit advpn
BR-FW (advpn) # set ip 172.16.1.3/32
BR-FW (advpn) # set remote-ip 172.16.1.1/24
BR-FW (advpn) # set allowaccess ping
BR-FW (advpn) # set type tunnel
BR-FW (advpn) # set interface port1
BR-FW (advpn) # next
BR-FW (interface) # end
```

### Spoke-2 BR-FW BGP Configuration

```
BR-FW # config router bgp
BR-FW (bgp) # set as 65000
BR-FW (bgp) # set router-id 10.0.3.254
BR-FW (bgp) # set ibgp-multipath enable
BR-FW (bgp) # config neighbor
BR-FW (neighbor) # edit 172.16.1.1
BR-FW (172.16.1.1) # set remote-as 65000
BR-FW (172.16.1.1) # set interface advpn
BR-FW (172.16.1.1) # set update-source advpn
BR-FW (172.16.1.1) # next
BR-FW (neighbor) # end
BR-FW (bgp) # config network
BR-FW (network) # edit 1
BR-FW (1) # set prefix 10.0.3.0 255.255.255.0
BR-FW (1) # next
BR-FW (network) # end
BR-FW (bgp) # end
```

#### Spoke-2 BR-FW LAN to VPN Policy

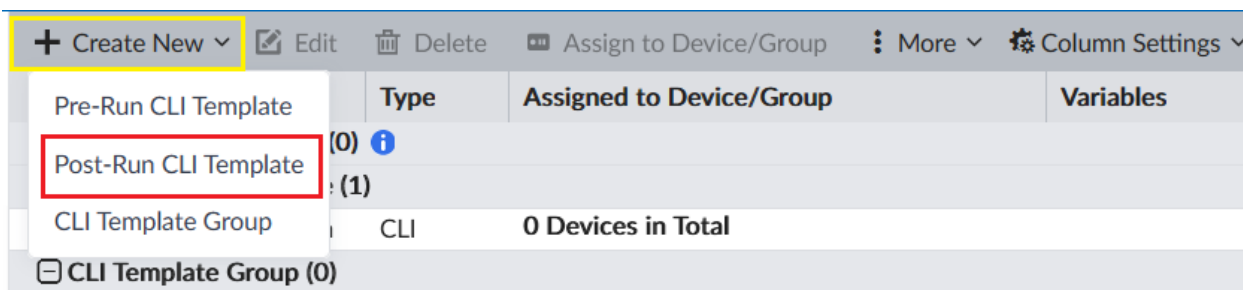
```
BR-FW # config firewall policy
BR-FW (policy) # edit 2
BR-FW (2) # set name LAN-to-VPN
BR-FW (2) # set srcintf port2
BR-FW (2) # set dstintf advpn
BR-FW (2) # set action accept
BR-FW (2) # set srcaddr all
BR-FW (2) # set dstaddr all
BR-FW (2) # set schedule always
BR-FW (2) # set service ALL
BR-FW (2) # set logtraffic all
BR-FW (2) # set status enable
BR-FW (2) # end
```

#### Spoke-2 BR-FW VPN to LAN Policy

```
BR-FW # config firewall policy
BR-FW (policy) # edit 3
BR-FW (3) # set name VPN-to-LAN
BR-FW (3) # set srcintf advpn
BR-FW (3) # set dstintf port2
BR-FW (3) # set action accept
BR-FW (3) # set srcaddr all
BR-FW (3) # set dstaddr all
BR-FW (3) # set schedule always
BR-FW (3) # set service ALL
BR-FW (3) # set logtraffic all
BR-FW (3) # set status enable
BR-FW (3) # end
```

## CLI Template:

Go to **Device Manager > Provisioning Templates > CLI Templates**. Click **Create New > Post-Run CLI Template**. The Create New CLI Template pane is displayed. Enter the required information Click **OK**.



Create New Post-Run CLI Template

Template Name: HQ-ADVPN

Type: CLI Script

Description: HQ ADVPN configuration

Script Details

```
91 end
92 config firewall policy
93 edit 4
94 set name VPN-to-VPN
95 set srcintf advpn
96 set dstintf advpn
97 set action accept
98 set srcaddr all
99 set dstaddr all
100 set schedule always
101 set service ALL
102 set logtraffic all
103 set status enable
104 end
```

Revert All Changes

OK Cancel

Create New

Edit

Delete

Assign to Device/Group

More

Column Settings

<div></div>	Name	Type	Assigned to Device/Group	Variables
<div><div></div><div>Pre-Run CLI Template (0)</div><div></div></div>				
<div><div></div><div>Post-Run CLI Template (1)</div><div></div></div>				
<div><div></div><div>HQ-ADVPN</div></div>	CLI	0 Devices in Total		
<div><div></div><div>CLI Template Group (0)</div><div></div></div>				

<span>+</span> Create New <span>✎</span> Edit <span>🗑</span> Delete <span>🗨</span> Assign to Device/Group <span>⋮</span> More <span>⚙</span> Column Settings				
<input type="checkbox"/>	Name	Type	Assigned to Device/Group	Variables
<input type="checkbox"/>	Pre-Run CLI Template (0) <span>ℹ</span>			
<input type="checkbox"/>	Post-Run CLI Template (1)			
<input checked="" type="checkbox"/>	HQ-ADVPN	CLI	0 Devices in Total	
<input type="checkbox"/>	CLI Template			

✎ Edit  
🗑 Clone  
🗑 Delete  
🗨 Assign to Device/Group

Right Click

## Assign to Devices/Groups

Post-Run CLI Template: HQ-ADVPN

**Available Entries (3)**

- ☐ ↑ BR-FW [root] (IP: 192.168.100.230, Platform: FortiGate-VN)
- ☐ ↑ DC-FW [root] (IP: 192.168.100.220, Platform: FortiGate-VI)
- ☐ ↑ FW1 [root] (IP: 192.168.100.205, Platform: FortiGate-VM6)

**Selected Entries (1)**

- ☐ ↑ HQ-FW [root] (IP: 192.168.100.200, Platform: FortiGate-V)

## 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 HQ-FW

Comment

☐ Create ADOM Revision

☐ Schedule Install

### ☐ Install Device Settings (only)

Next >

Cancel

## Test and Verification:

Let's traceroute from Spoke-2 BR-PC1 to Spoke-1 DC-PC1 first time the packet going to through HUB HQ-FW 172.16.1.1 next time directly spoke to spoke communication.

QEMU (BR-PC1)

192.

```
root@slax:~#
root@slax:~# traceroute 10.0.2.1 -d
traceroute to 10.0.2.1 (10.0.2.1), 30 hops max, 60 byte packets
 1  10.0.3.254 (10.0.3.254)  19.910 ms  18.146 ms  17.893 ms
 2  172.16.1.1 (172.16.1.1)  17.811 ms  20.928 ms  37.145 ms
 3  172.16.1.2 (172.16.1.2)  60.685 ms  60.560 ms  67.986 ms
 4  10.0.2.1 (10.0.2.1)  67.872 ms  67.853 ms  67.790 ms
root@slax:~# traceroute 10.0.2.1 -d
traceroute to 10.0.2.1 (10.0.2.1), 30 hops max, 60 byte packets
 1  10.0.3.254 (10.0.3.254)  5.993 ms  5.674 ms  5.383 ms
 2  172.16.1.2 (172.16.1.2)  24.199 ms  24.107 ms  24.916 ms
 3  10.0.2.1 (10.0.2.1)  37.921 ms  37.849 ms  37.293 ms
root@slax:~#
```

1st Time

2nd Time

Enter host <Alt+R>

✓ HQ-FW ✓ DC-FW × ✓ BR-FW

```
DC-FW #
DC-FW # diagnose ip address list | grep advpn
IP=172.16.1.2->172.16.1.2/255.255.255.255 index=17 devname=advpn
IP=172.16.1.2->172.16.1.3/255.255.255.255 index=18 devname=advpn_0
DC-FW #
```

✓ HQ-FW ✓ DC-FW ✓ BR-FW ×

```
BR-FW #
BR-FW # diagnose ip address list | grep advpn
IP=172.16.1.3->172.16.1.3/255.255.255.255 index=17 devname=advpn
IP=172.16.1.3->172.16.1.2/255.255.255.255 index=18 devname=advpn_0
BR-FW #
```

IPsec

Reset Statistics Bring Up Bring Down Locate on VPN Map

Name	Remote Gateway	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 2					
advpn	192.168.1.1	2.02 kB	2.20 kB	advpn	advpn
advpn_0	192.168.5.1	2.26 kB	2.37 kB	advpn_0	advpn

IPsec

Reset Statistics

Bring Up

Bring Down

Locate on VPN Map

	Name	Remote Gateway	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
<div><div></div><div>Custom</div><div>2</div></div>						
	<div><div></div>advpn</div>	192.168.1.1	2.53 kB <div></div>	2.26 kB <div></div>	<div><div></div>advpn</div>	<div><div></div>advpn</div>
	<div><div></div>advpn_0</div>	192.168.3.1	2.37 kB <div></div>	2.26 kB <div></div>	<div><div></div>advpn_0</div>	<div><div></div>advpn</div>

### Verification Commands

HQ-FW# diagnose vpn tunnel list

DC-FW# diagnose vpn tunnel list

BR-FW# diagnose vpn tunnel list

HQ-FW# get router info routing-table bgp

HQ-FW# diagnose ip address list | grep advpn

BR-FW# diagnose ip address list | grep advpn

DC-FW# diagnose ip address list | grep advpn

BR-FW# diagnose vpn ike gateway list

BR-FW# get router info bgp summary

BR-FW# get router info bgp network

DC-FW# get router info bgp network

HQ-FW# get router info bgp network

DC-FW # diagnose vpn tunnel flush advpn\_0