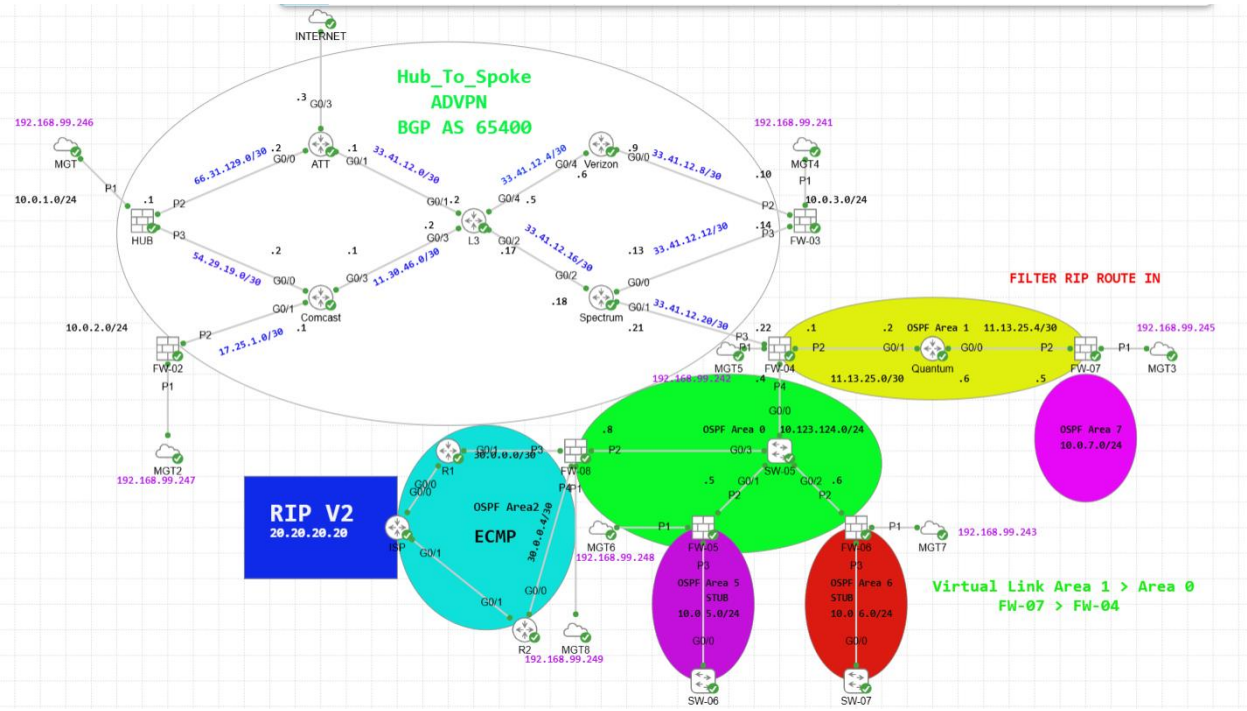
Topology



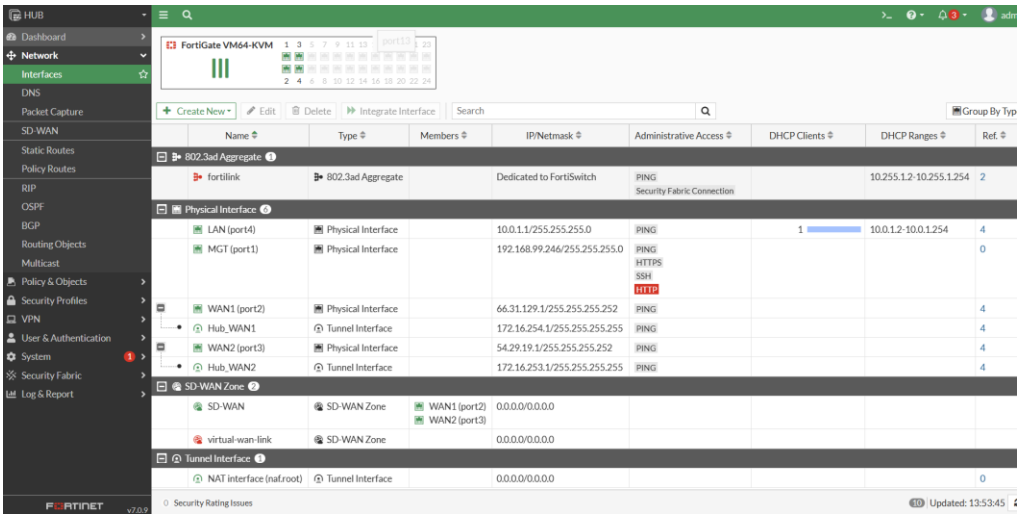
Before we start:

- All Routers are configured to route all routes back and forward, the configuration of such are outside the scope of this lesson.
- The purpose of this lab is to configure ADVPN with hub and spoke and spoke to spoke connection between firewalls.
- Internet connection is primarily coming out of ATT.
- Hub and Spoke Design with ADVPN configured, we are using iBGP for the Overlay routing protocol.
- The Overlay subnets are 172.16.254.0 for WAN1 and 172.16.253.0 for WAN2.
- The LAN IP Addresses are 10.0.1.0, 10.0.2.0, 10.0.3.0, 10.0.5.0, 10.0.6.0, 10.0.7.0
- We are to configure a Virtual Link on FW-07 for communication with FW-04.
- We are to configure ECMP for RIP route on FW-08
- We are to configure SD-WAN according to client needs at HUB and FW-03
- We are to configure BFD for fast convergence of BGP.

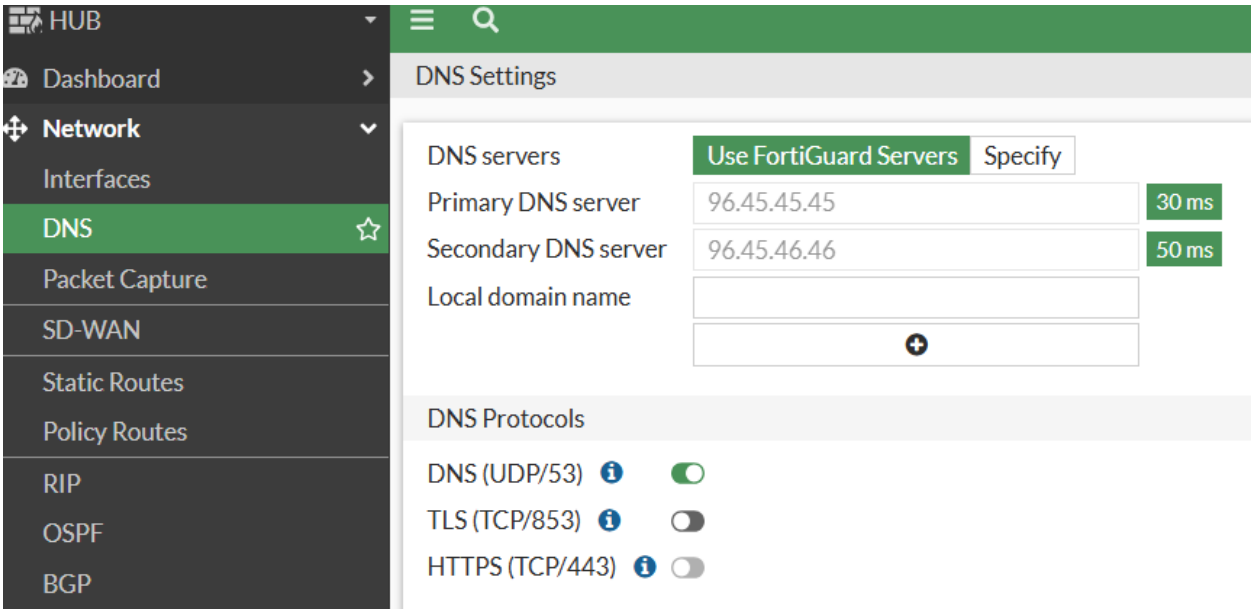
- We are to filter Routes from RIP at FW-07 to reach the Routing table using prefix list.
- Test connectivity between LANs
- Test Failover to WAN2 during live PING from one of the Spokes.

HUB Configuration

Interfaces:



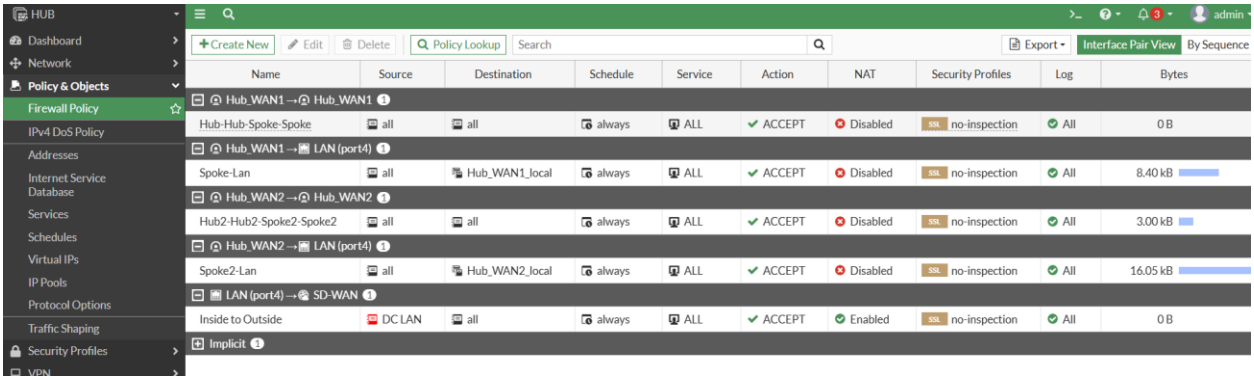
DNS:



Static Routes:

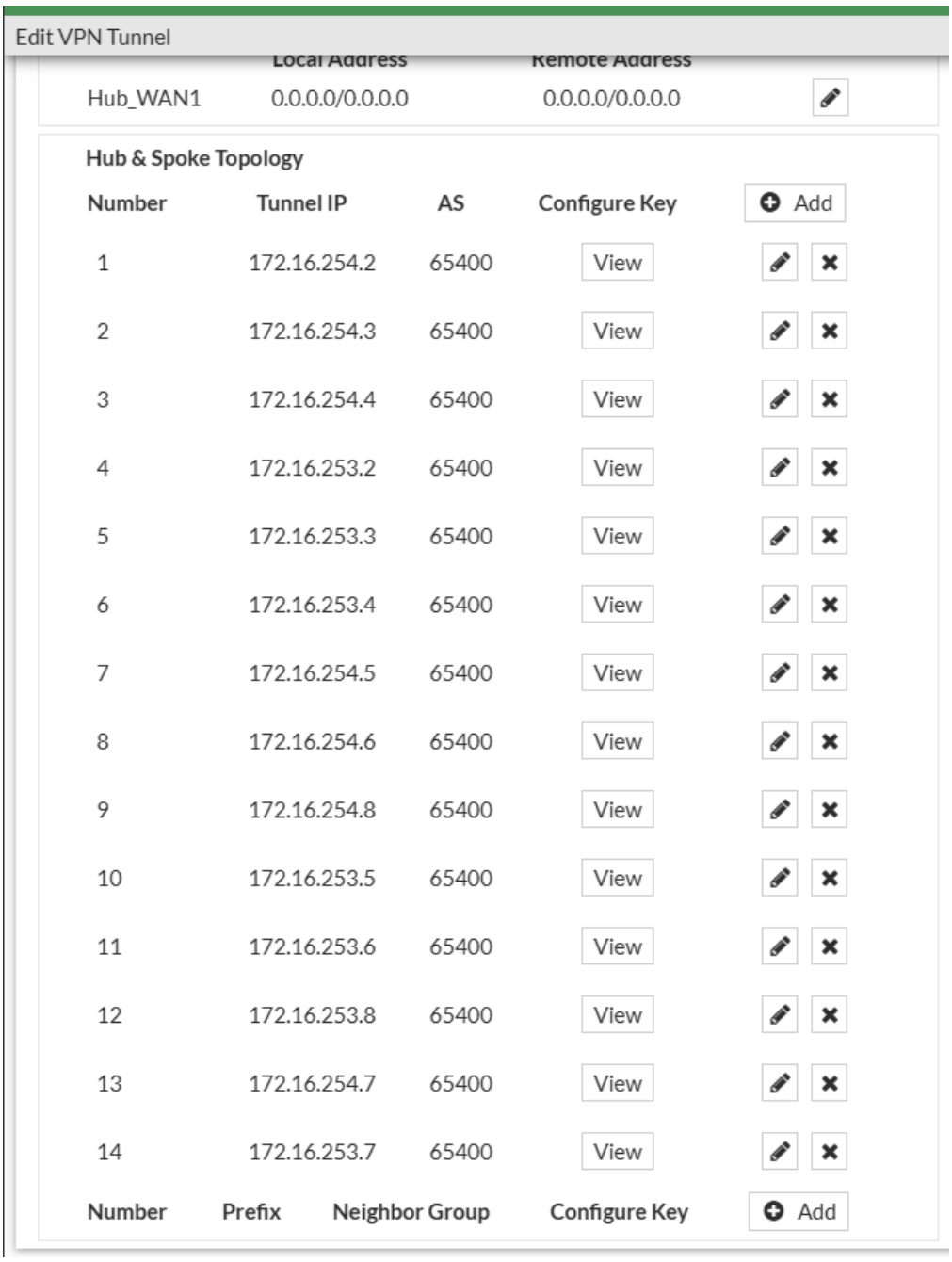


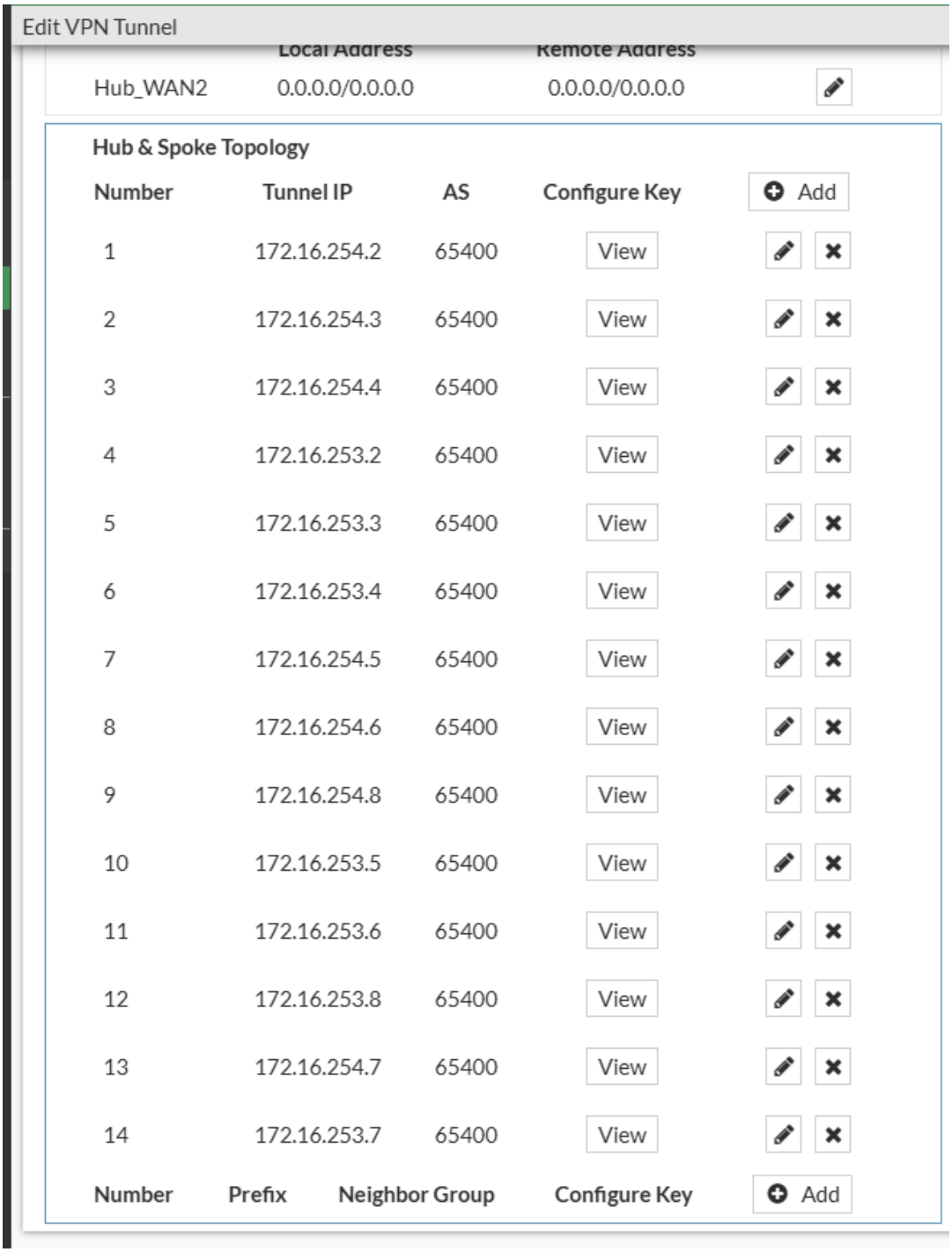
Firewall Policy:



ADVPN



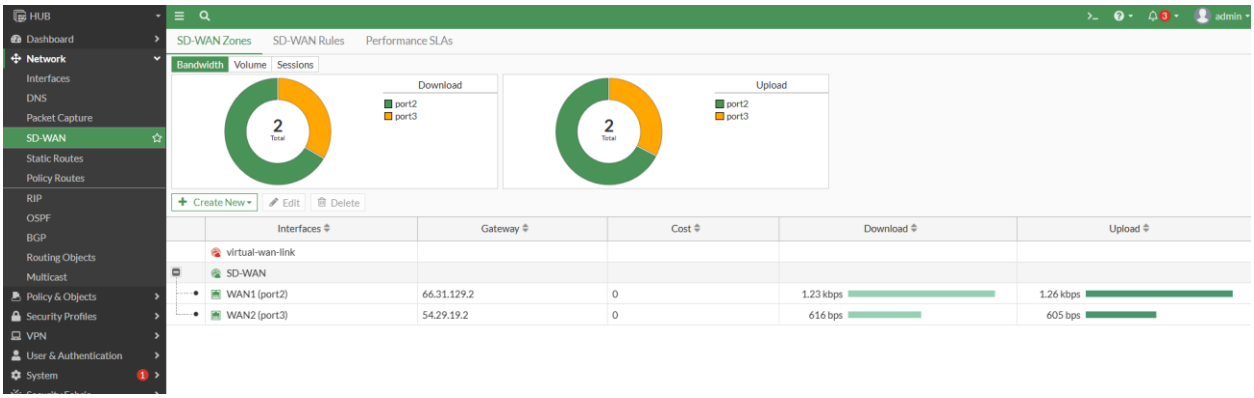

Edit VPN Tunnel
Local Address
Remote Address
Hub_WAN1
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0
Hub & Spoke Topology
Number
Tunnel IP
AS
Configure Key
Add
1 172.16.254.2 65400 View
2 172.16.254.3 65400 View
3 172.16.254.4 65400 View
4 172.16.253.2 65400 View
5 172.16.253.3 65400 View
6 172.16.253.4 65400 View
7 172.16.254.5 65400 View
8 172.16.254.6 65400 View
9 172.16.254.8 65400 View
10 172.16.253.5 65400 View
11 172.16.253.6 65400 View
12 172.16.253.8 65400 View
13 172.16.254.7 65400 View
14 172.16.253.7 65400 View
Number
Prefix
Neighbor Group
Configure Key
Add

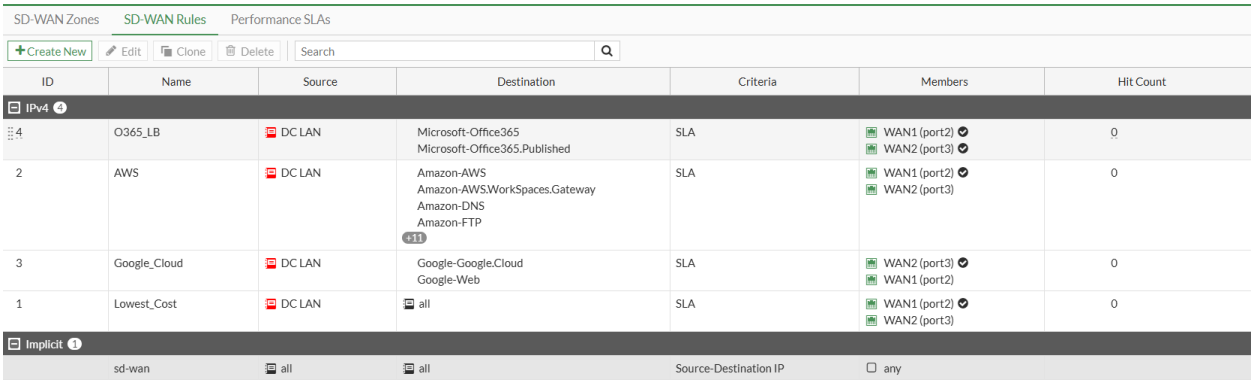


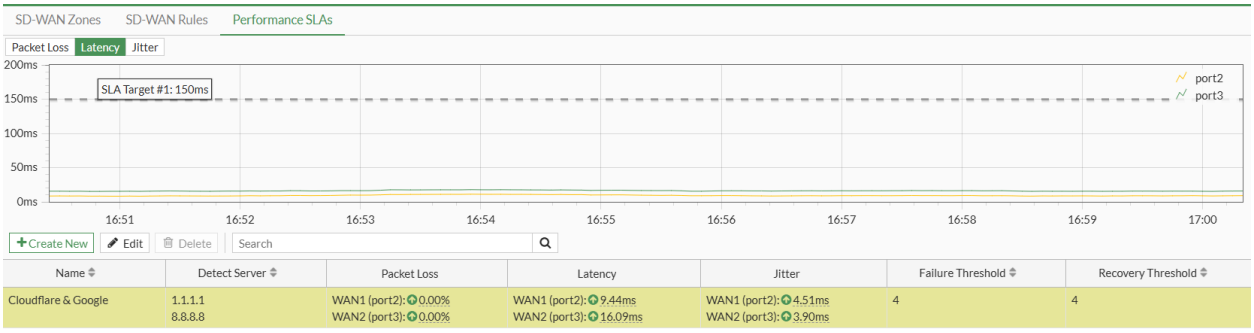
SD-WAN

- Our WAN1is the fastest circuit, most of the rules will choose WAN1.
- Client requested all O365 traffic to be load balanced across both connections.

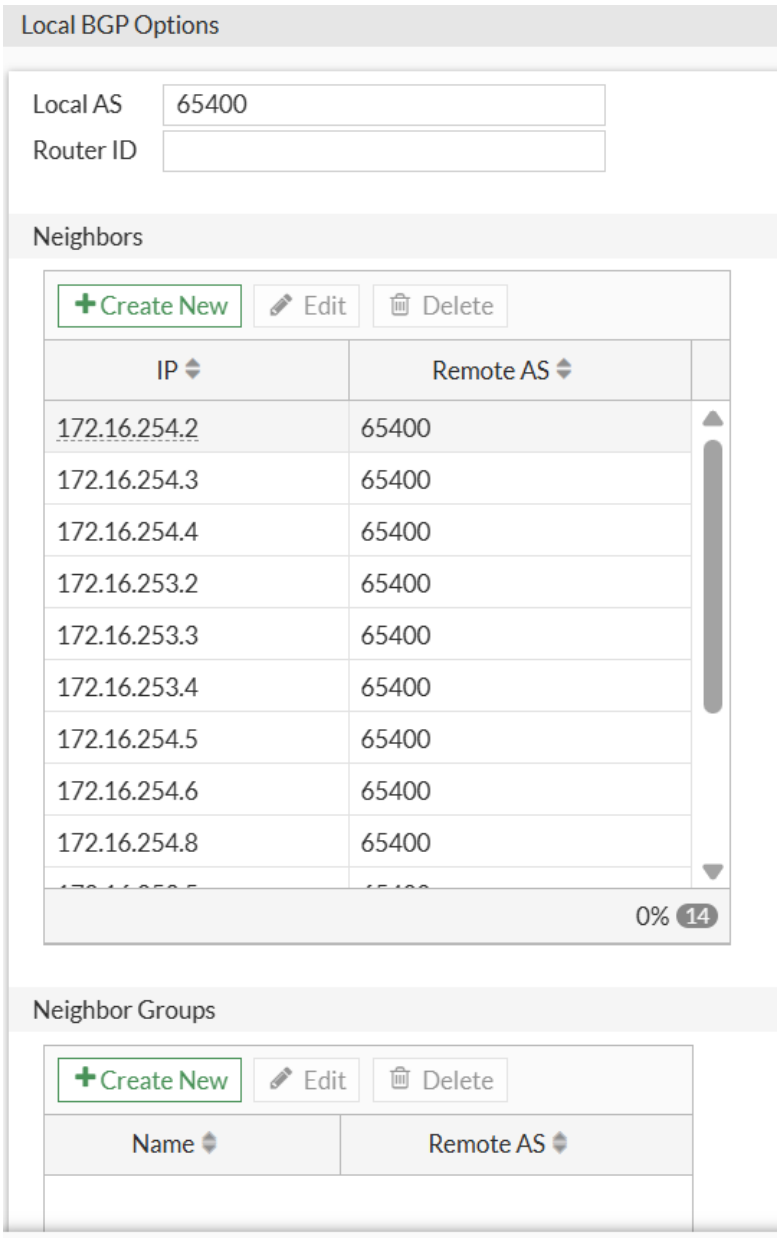
- Client requested AWS to be sent out primarily out of **WAN1** but if it does not meet SLA send it out of **WAN2**.
- Client requested all Google Cloud services to be sent out of **WAN2** but if it does not meed SLA send it out of WAN1.
- For all other traffic that is not specified send it out of **WAN1** the fastest circuit.

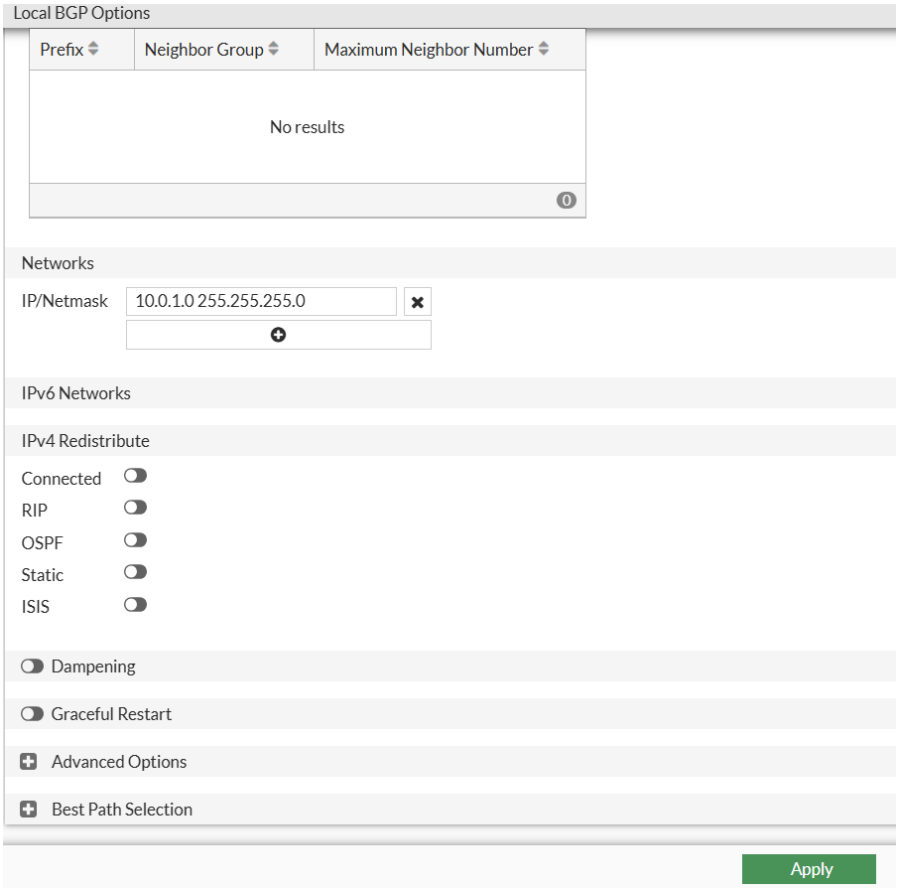




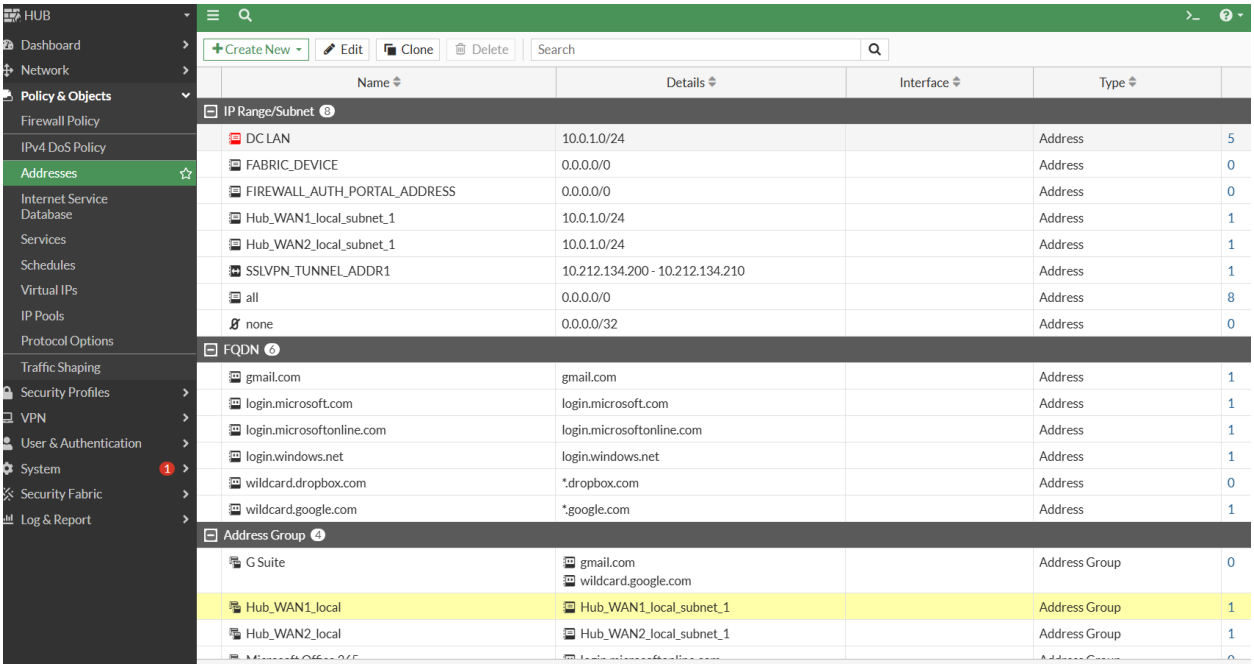


BGP


Local BGP Options
Local AS
65400
Router ID
Neighbors
Create New
Edit
Delete
IP
Remote AS
172.16.254.2
65400
172.16.254.3
65400
172.16.254.4
65400
172.16.253.2
65400
172.16.253.3
65400
172.16.253.4
65400
172.16.254.5
65400
172.16.254.6
65400
172.16.254.8
65400
0%
14
Neighbor Groups
Create New
Edit
Delete
Name
Remote AS

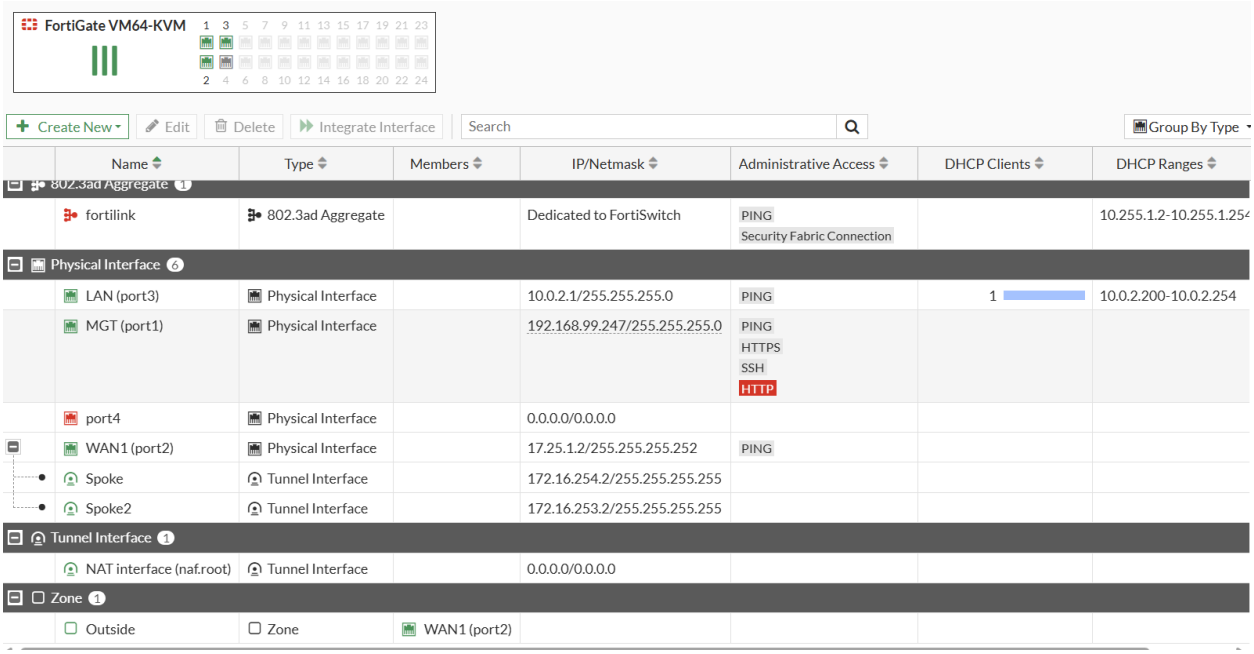

Local BGP Options
Prefix
Neighbor Group
Maximum Neighbor Number
No results
0
Networks
IP/Netmask
10.0.1.0 255.255.255.0
IPv6 Networks
IPv4 Redistribute
Connected
RIP
OSPF
Static
ISIS
Dampening
Graceful Restart
Advanced Options
Best Path Selection
Apply

Addresses:


HUB
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
Create New
Edit
Clone
Delete
Search
Name
Details
Interface
Type
IP Range/Subnet 8
DC LAN 10.0.1.0/24 Address 5
FABRIC_DEVICE 0.0.0.0/0 Address 0
FIREWALL_AUTH_PORTAL_ADDRESS 0.0.0.0/0 Address 0
Hub_WAN1_local_subnet_1 10.0.1.0/24 Address 1
Hub_WAN2_local_subnet_1 10.0.1.0/24 Address 1
SSLVPN_TUNNEL_ADDR1 10.212.134.200 - 10.212.134.210 Address 1
all 0.0.0.0/0 Address 8
none 0.0.0.0/32 Address 0
FQDN 6
gmail.com gmail.com Address 1
login.microsoft.com login.microsoft.com Address 1
login.microsoftonline.com login.microsoftonline.com Address 1
login.windows.net login.windows.net Address 1
wildcard.dropbox.com *.dropbox.com Address 0
wildcard.google.com *.google.com Address 1
Address Group 4
G Suite gmail.com wildcard.google.com Address Group 0
Hub_WAN1_local Hub_WAN1_local_subnet_1 Address Group 1
Hub_WAN2_local Hub_WAN2_local_subnet_1 Address Group 1

FW-02 Configuration

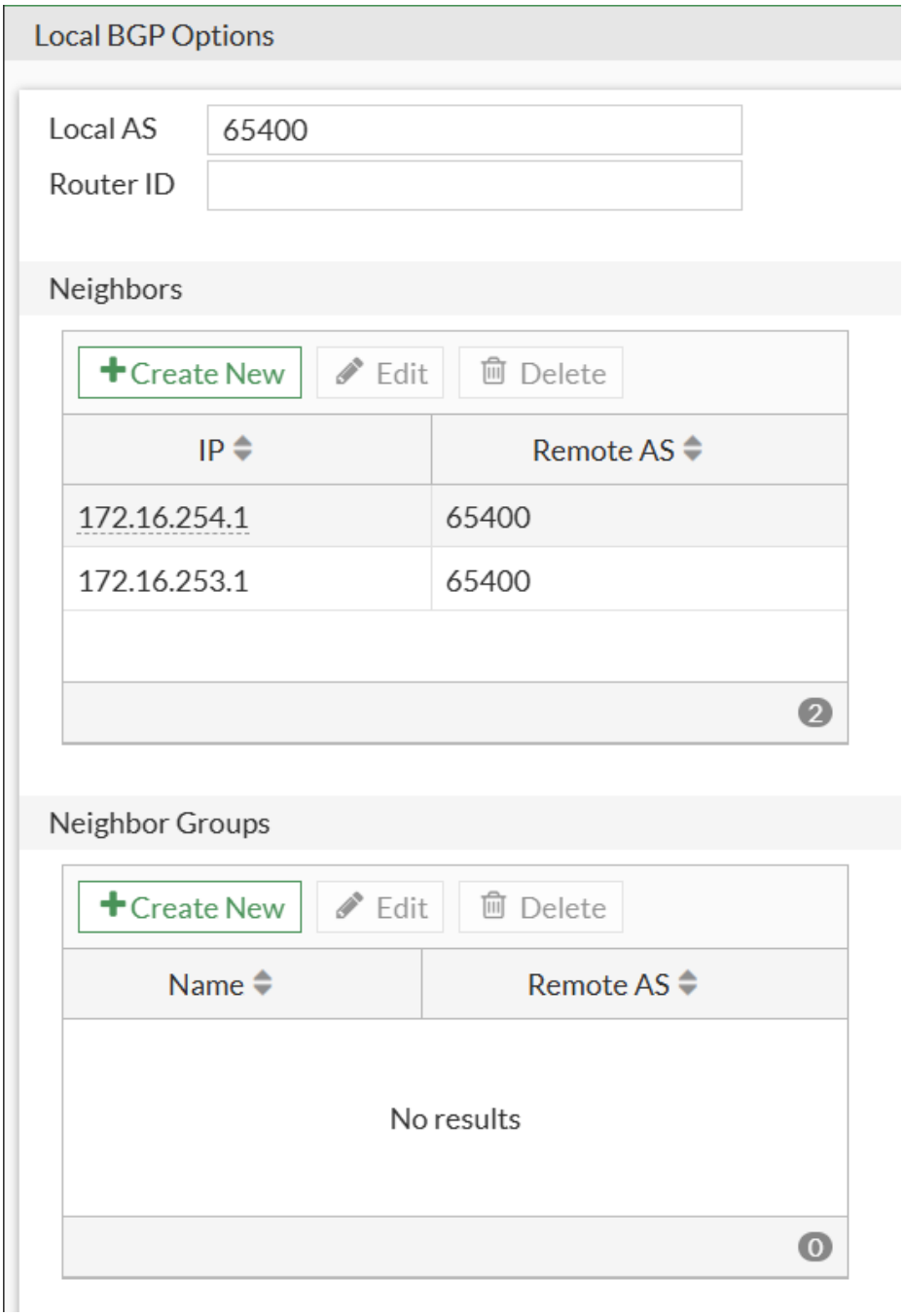
Interfaces:

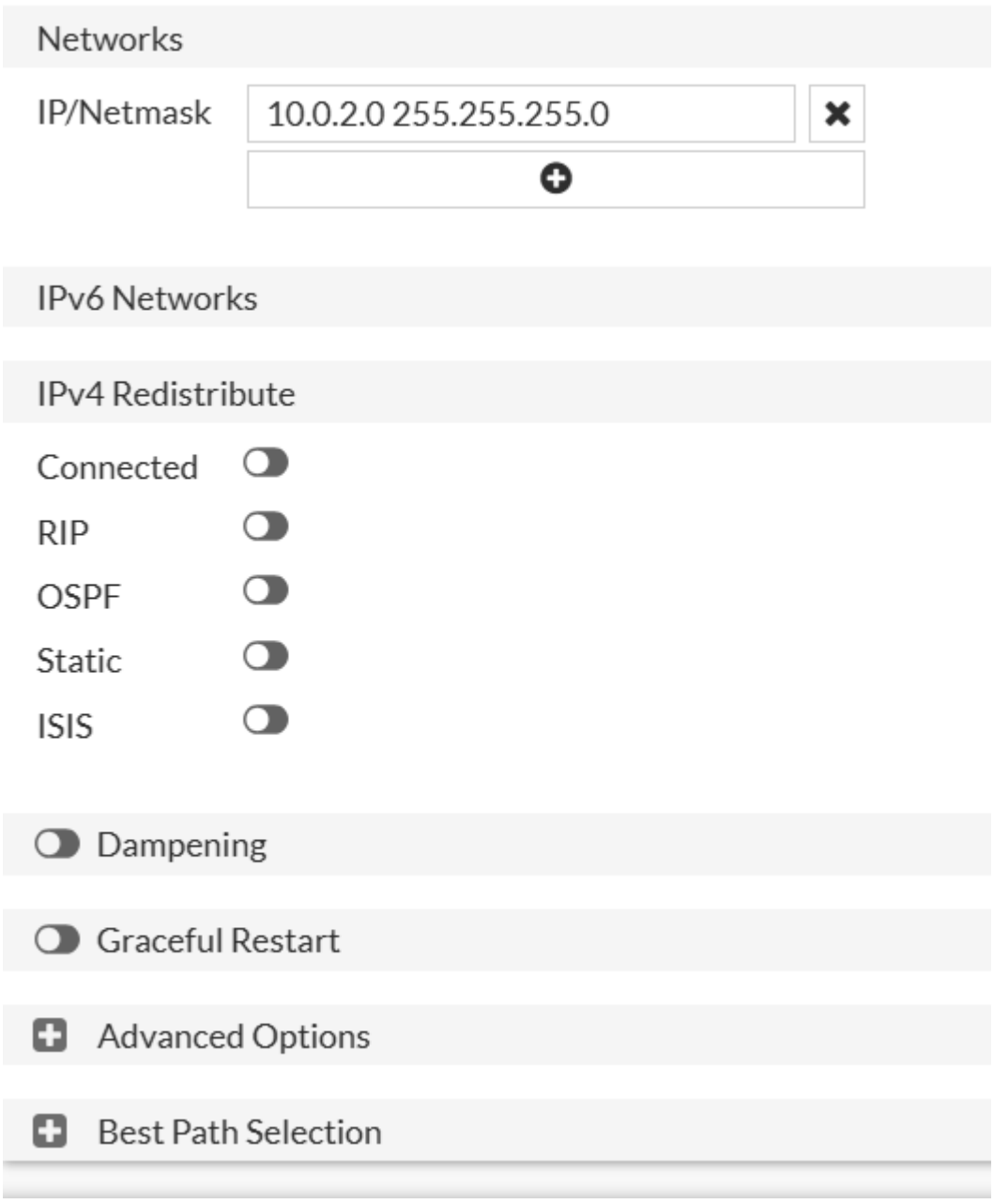


Static Route

Destination	Gateway IP	Interface	Status
0.0.0.0/0	17.25.1.1	WAN1 (port2)	Enabled

BGP


Local BGP Options
Local AS
65400
Router ID
Neighbors
Create New
Edit
Delete
IP
Remote AS
172.16.254.1
65400
172.16.253.1
65400
2
Neighbor Groups
Create New
Edit
Delete
Name
Remote AS
No results
0



Firewall Policies

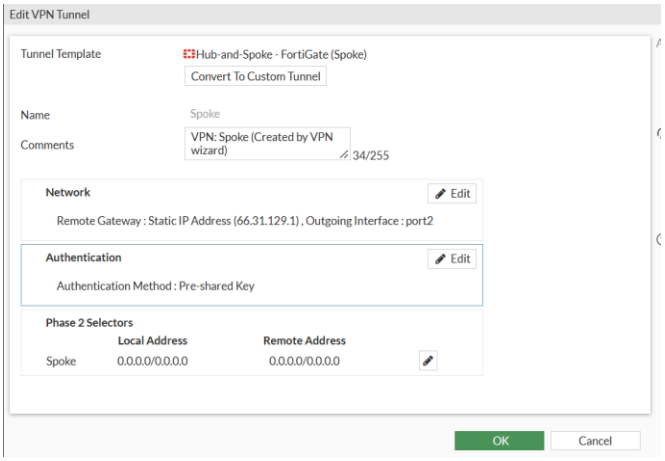
Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Inside to Outside	LAN (port3)	Outside	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	2.00 kB
vpn_Spoke_remote_0	Spoke	LAN (port3)	all	Spoke_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
vpn_Spoke_local_0	LAN (port3)	Spoke	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
vpn_Spoke2_remote_0	Spoke2	LAN (port3)	all	Spoke2_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	4.98 kB
vpn_Spoke2_local_0	LAN (port3)	Spoke2	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	0 B

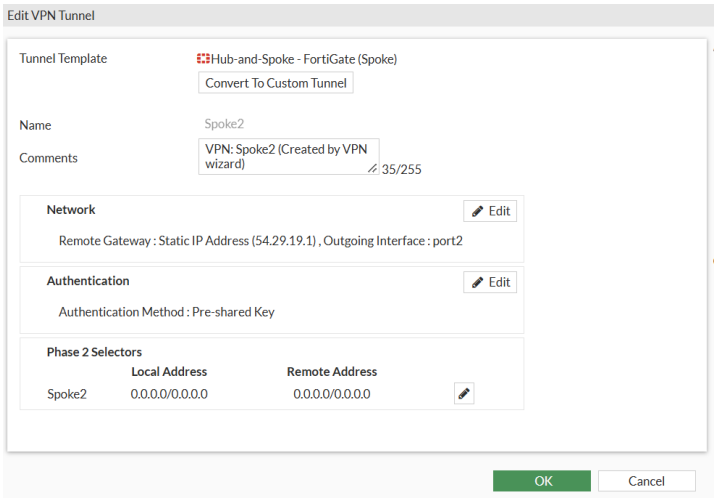
Addresses:

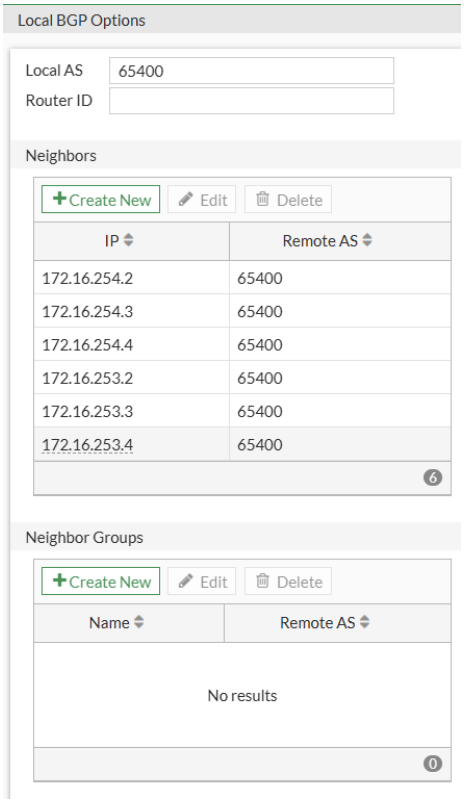
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	1
Spoke2_local_subnet_1	10.0.2.0/24		Address	1
Spoke_local_subnet_1	10.0.2.0/24		Address	1
all	0.0.0.0/0		Address	8
none	0.0.0.0/32		Address	0
FQDN 6				
gmail.com	gmail.com		Address	1
login.microsoft.com	login.microsoft.com		Address	1
login.microsoftonline.com	login.microsoftonline.com		Address	1
login.windows.net	login.windows.net		Address	1
wildcard.dropbox.com	*.dropbox.com		Address	0
wildcard.google.com	*.google.com		Address	1
Address Group 4				
G Suite	gmail.com wildcard.google.com		Address Group	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		Address Group	0
Spoke2_local	Spoke2_local_subnet_1		Address Group	1
Spoke_local	Spoke_local_subnet_1		Address Group	1

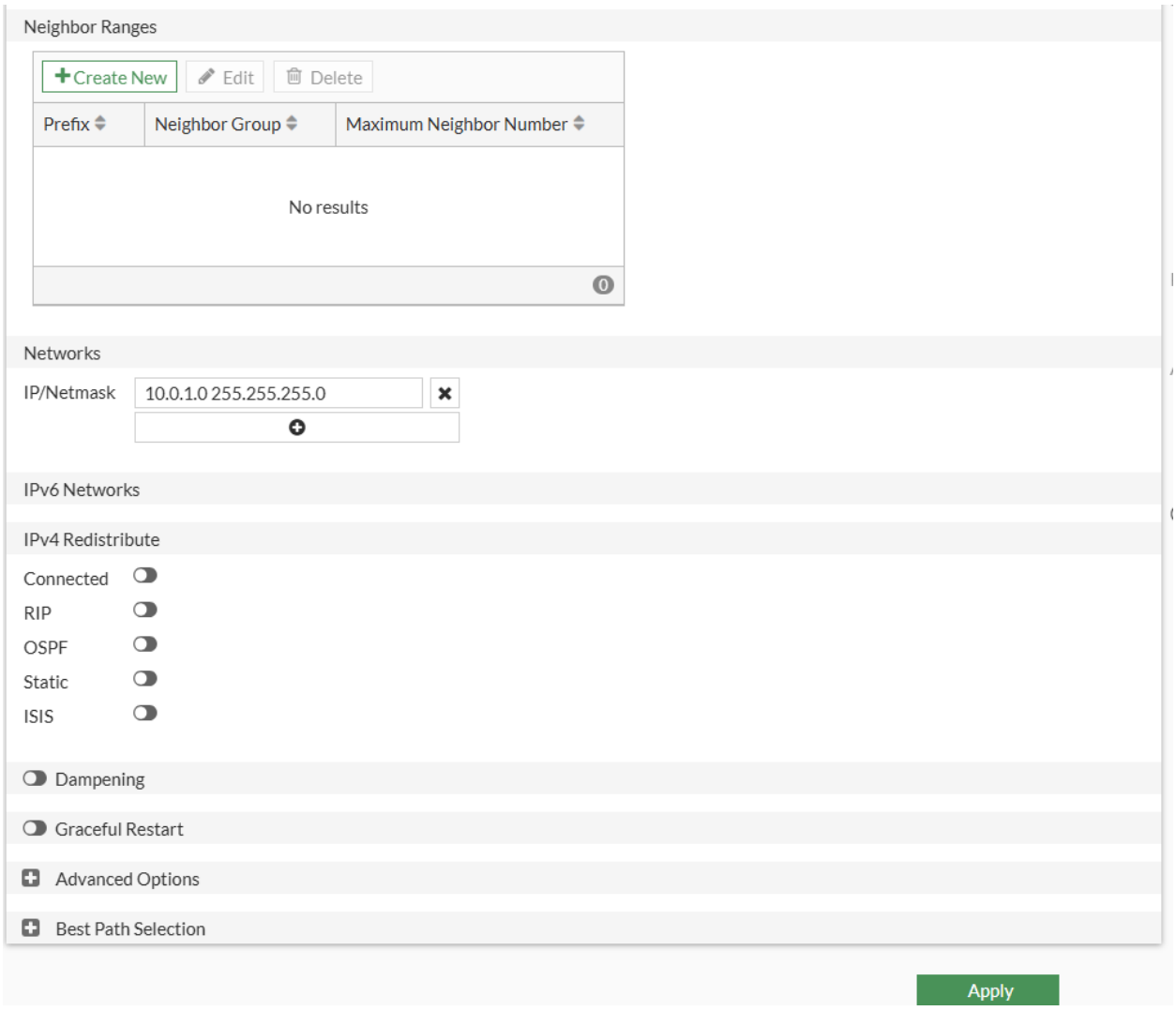
VPN

Hub-and-Spoke - FortiGate (Spoke) 2			
Spoke	WAN1 (port2)	Up	3
Spoke2	WAN1 (port2)	Up	3



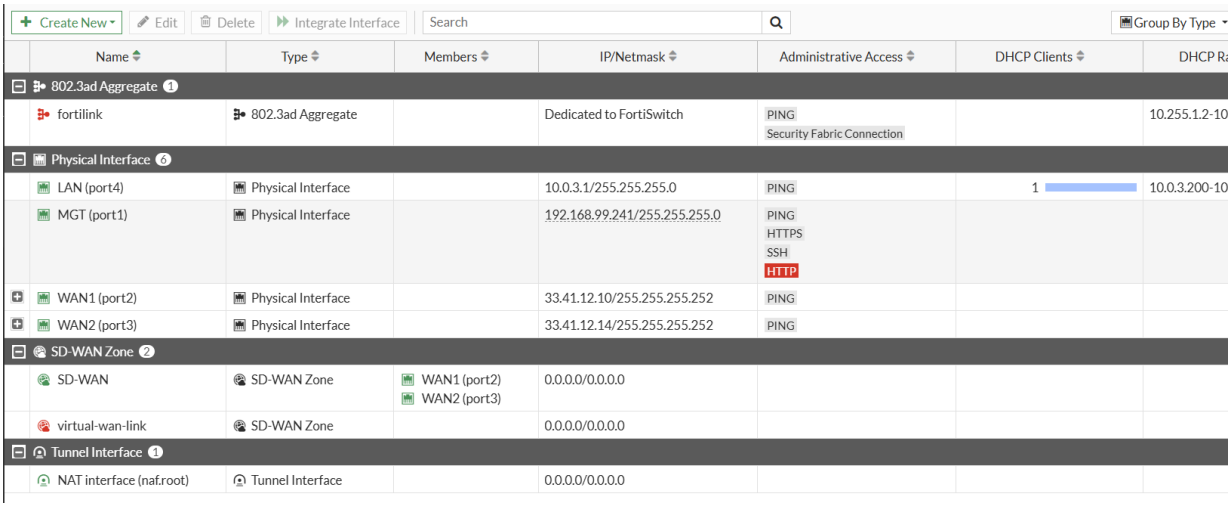

Edit VPN Tunnel
Tunnel Template
Hub-and-Spoke - FortiGate (Spoke)
Convert To Custom Tunnel
Name
Spoke2
Comments
VPN: Spoke2 (Created by VPN wizard)
35/255
Network
Edit
Remote Gateway : Static IP Address (54.29.19.1) , Outgoing Interface : port2
Authentication
Edit
Authentication Method : Pre-shared Key
Phase 2 Selectors
Local Address
Remote Address
Spoke2
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0
OK
Cancel


Local BGP Options
Local AS
65400
Router ID
Neighbors
Create New
Edit
Delete
IP
Remote AS
172.16.254.2
65400
172.16.254.3
65400
172.16.254.4
65400
172.16.253.2
65400
172.16.253.3
65400
172.16.253.4
65400
6
Neighbor Groups
Create New
Edit
Delete
Name
Remote AS
No results
0

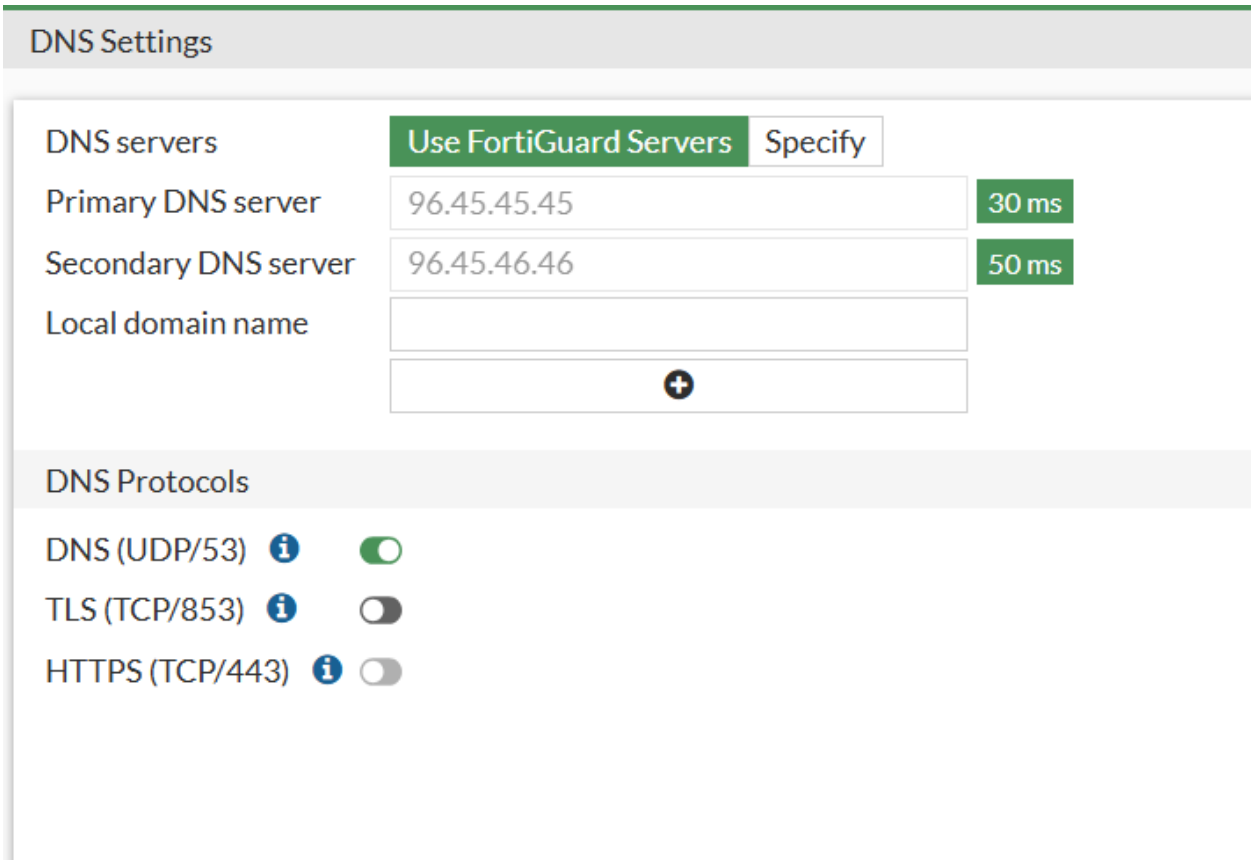

Neighbor Ranges
Create New
Edit
Delete
Prefix
Neighbor Group
Maximum Neighbor Number
No results
0
Networks
IP/Netmask
10.0.1.0 255.255.255.0
IPv6 Networks
IPv4 Redistribute
Connected
RIP
OSPF
Static
ISIS
Dampening
Graceful Restart
Advanced Options
Best Path Selection
Apply

FW-03 Configuration

Interfaces:

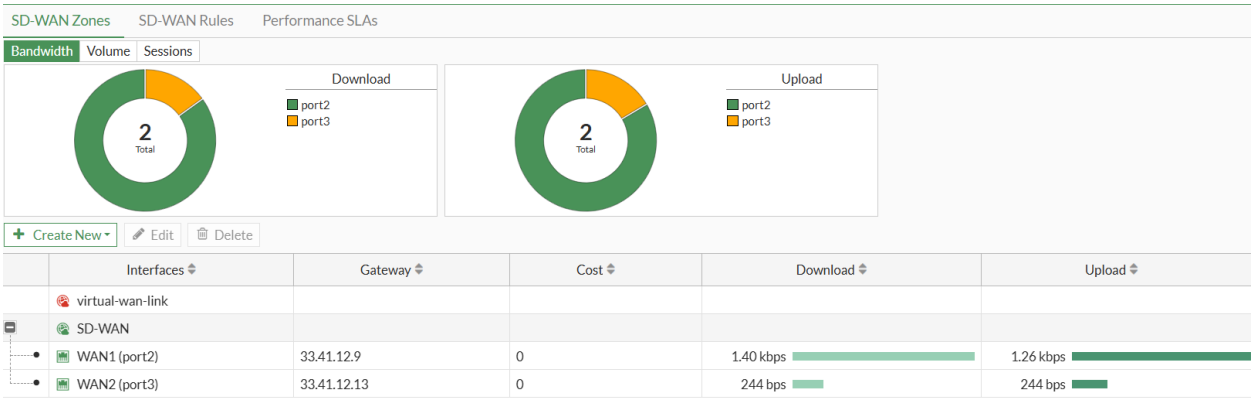


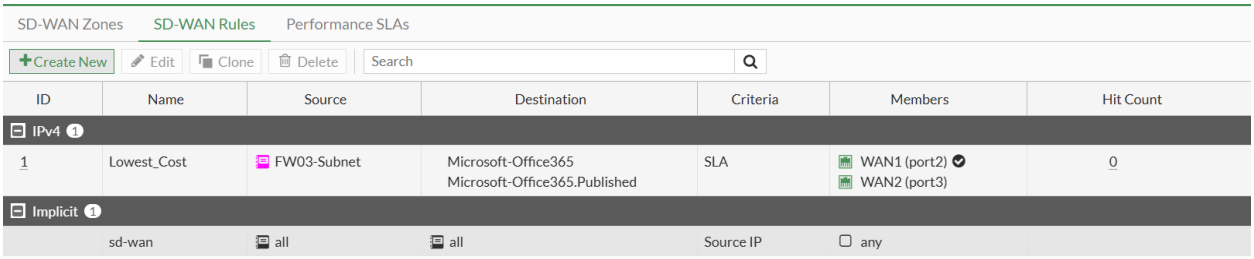
DNS

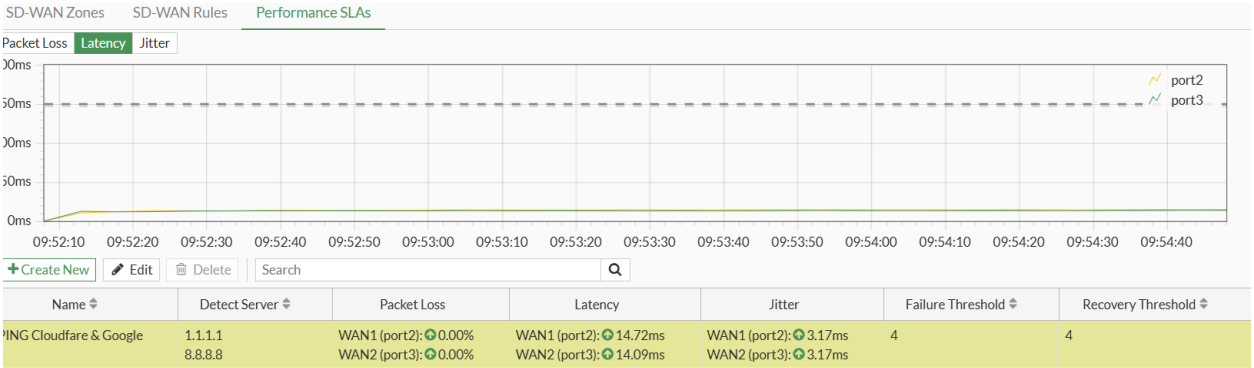


SD-WAN

- Because Verizon WAN2 only has 50 Mbps it is used as a backup in case WAN1 performance degrades.
- We are to configure WAN1 as the primary but monitor actively for Performance of Latency, Jitter and Packet loss, if it doesn't meet the SLA it will failover to WAN2 Verizon.



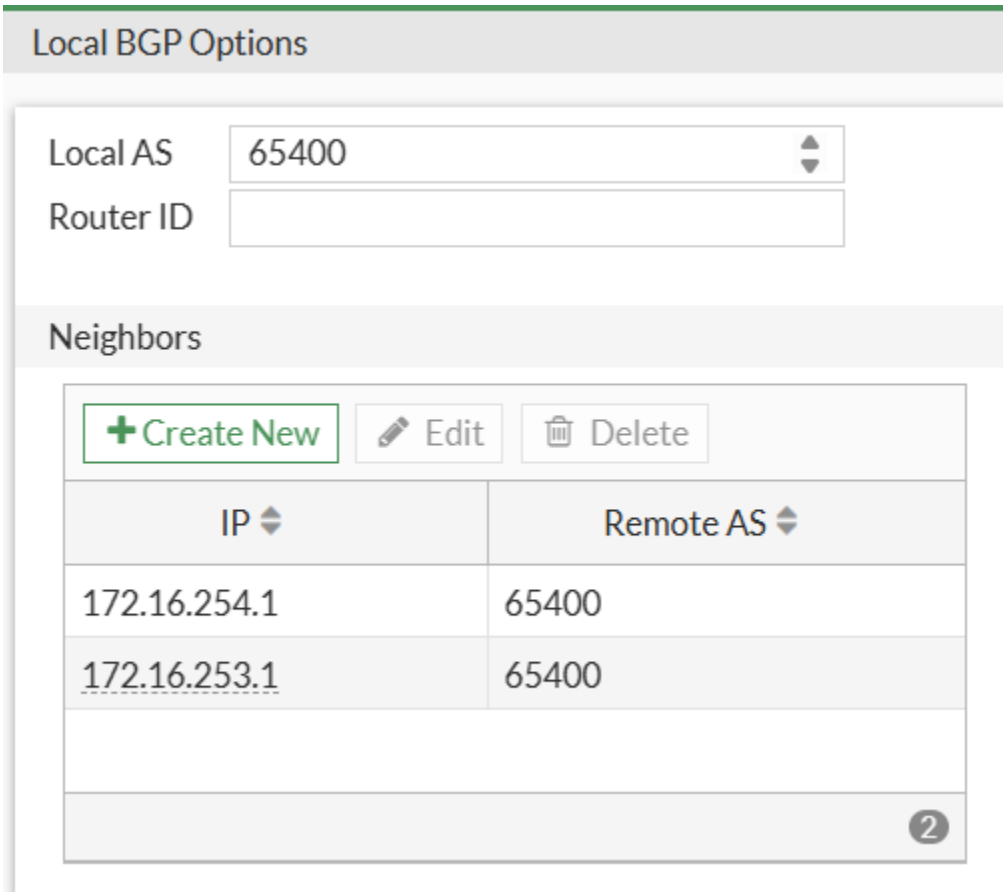




Static Routes

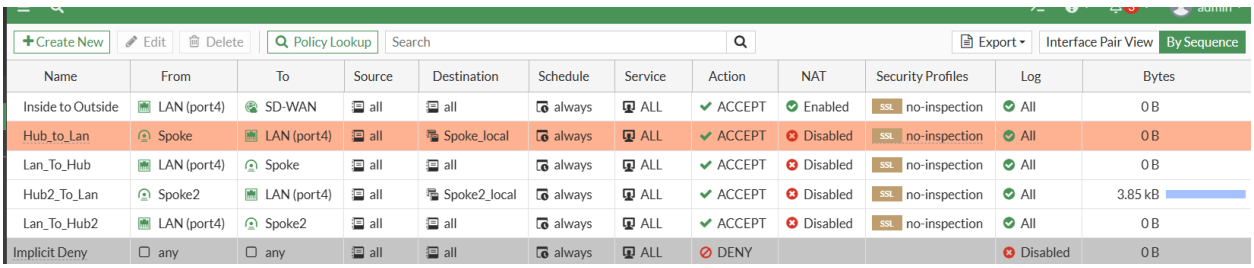


BGP





Firewall Policies:

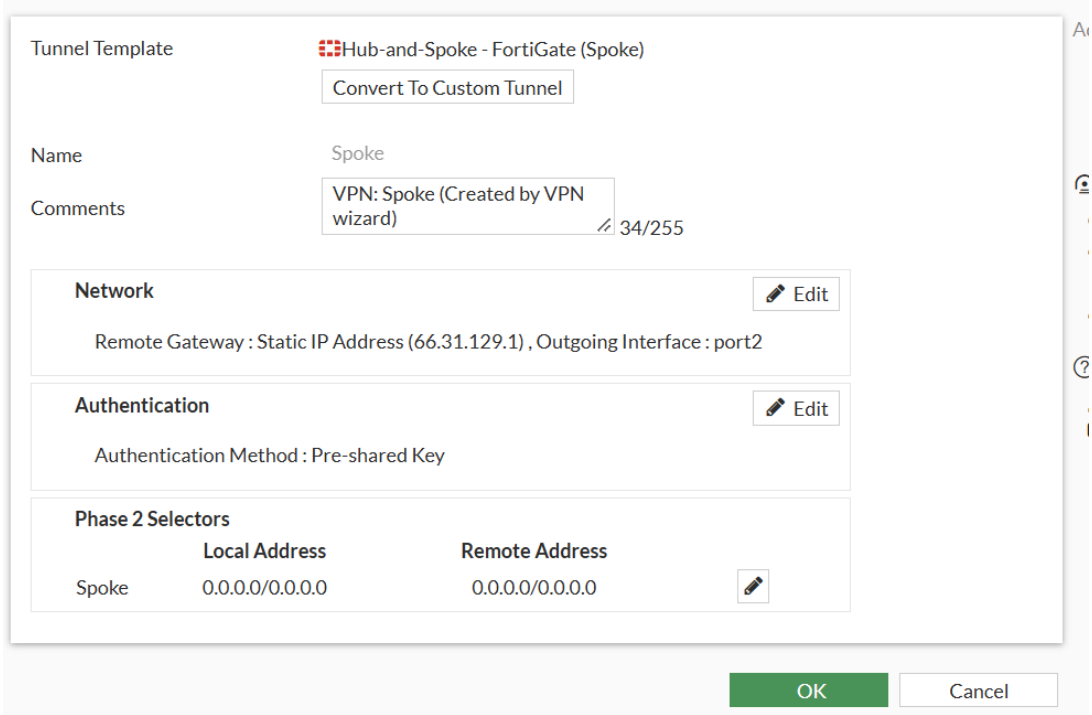


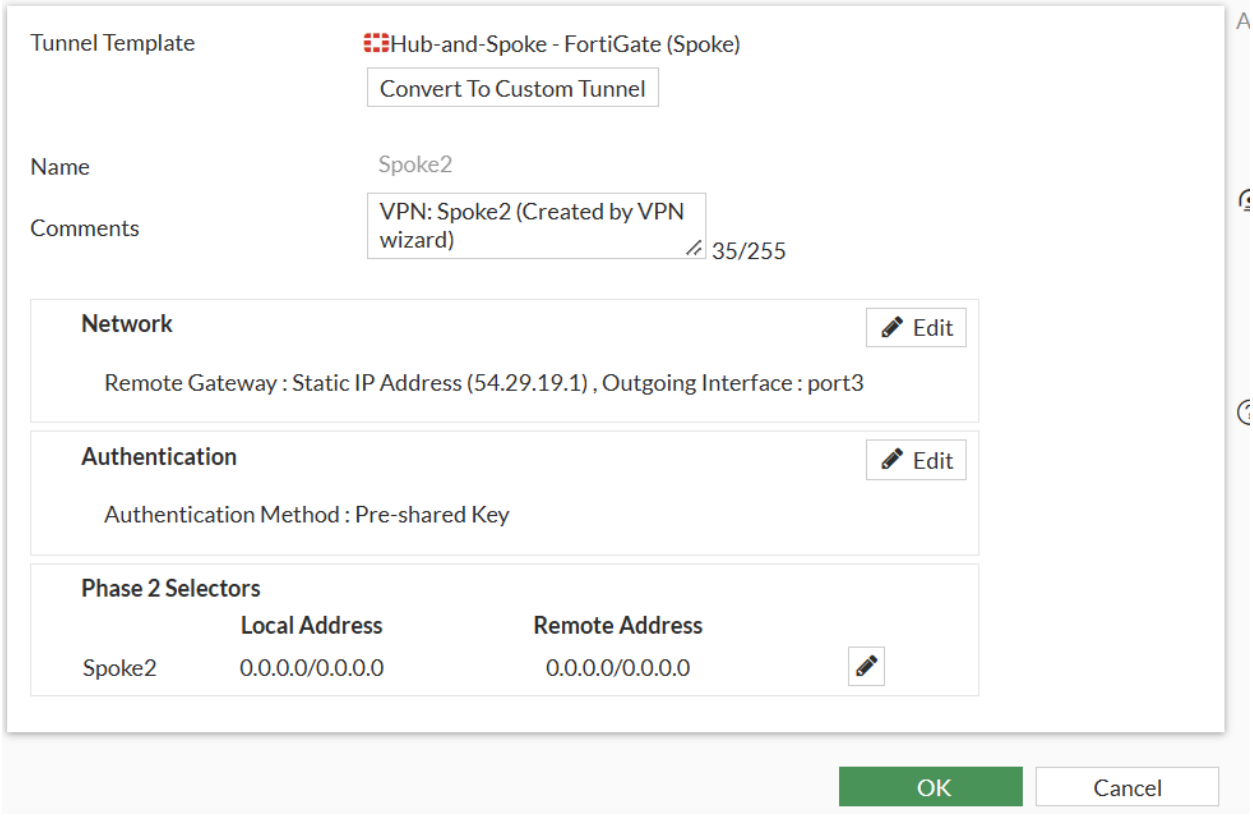
Addresses:

IP Range/Subnet 8				
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
FW03-Subnet	10.0.3.0/24		Address	1
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	1
Spoke2_local_subnet_1	10.0.3.0/24		Address	1
Spoke_local_subnet_1	10.0.3.0/24		Address	1
all	0.0.0.0/0		Address	8
none	0.0.0.0/32		Address	0
FQDN 6				
gmail.com	gmail.com		Address	1
login.microsoft.com	login.microsoft.com		Address	1
login.microsoftonline.com	login.microsoftonline.com		Address	1
login.windows.net	login.windows.net		Address	1
wildcard.dropbox.com	*.dropbox.com		Address	0
wildcard.google.com	*.google.com		Address	1
Address Group 4				
G Suite	gmail.com wildcard.google.com		Address Group	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		Address Group	0
Spoke2_local	Spoke2_local_subnet_1		Address Group	1
Spoke_local	Spoke_local_subnet_1		Address Group	1

VPN:

Hub-and-Spoke - FortiGate (Spoke) 2			
Spoke	WAN1 (port2)	Up	3
Spoke2	WAN2 (port3)	Up	3



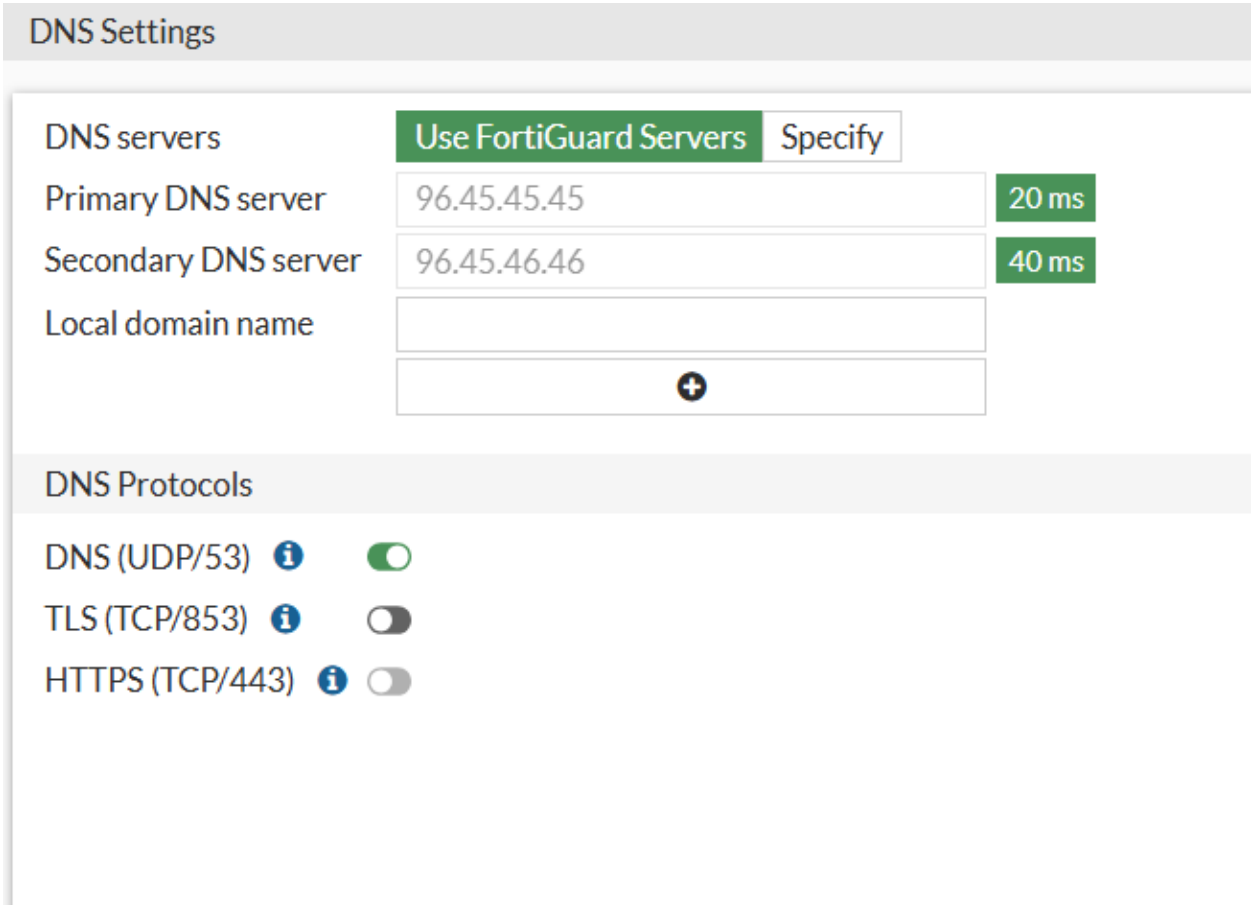


FW-04 Configuration

Interfaces:

802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Physical Interface 6							
Area 0 (port4)	Physical Interface		10.123.124.4/255.255.255.0	PING HTTPS SSH			1
Area 1 (port2)	Physical Interface		11.13.25.1/255.255.255.252	PING			1
MGT (port1)	Physical Interface		192.168.99.242/255.255.255.0	PING HTTPS SSH HTTP			0
WAN (port3)	Physical Interface		33.41.12.22/255.255.255.252	PING			6
Tunnel Interface 1							
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0
Zone 1							
OSPF	Zone	Area 1 (port2) Area 0 (port4)					5

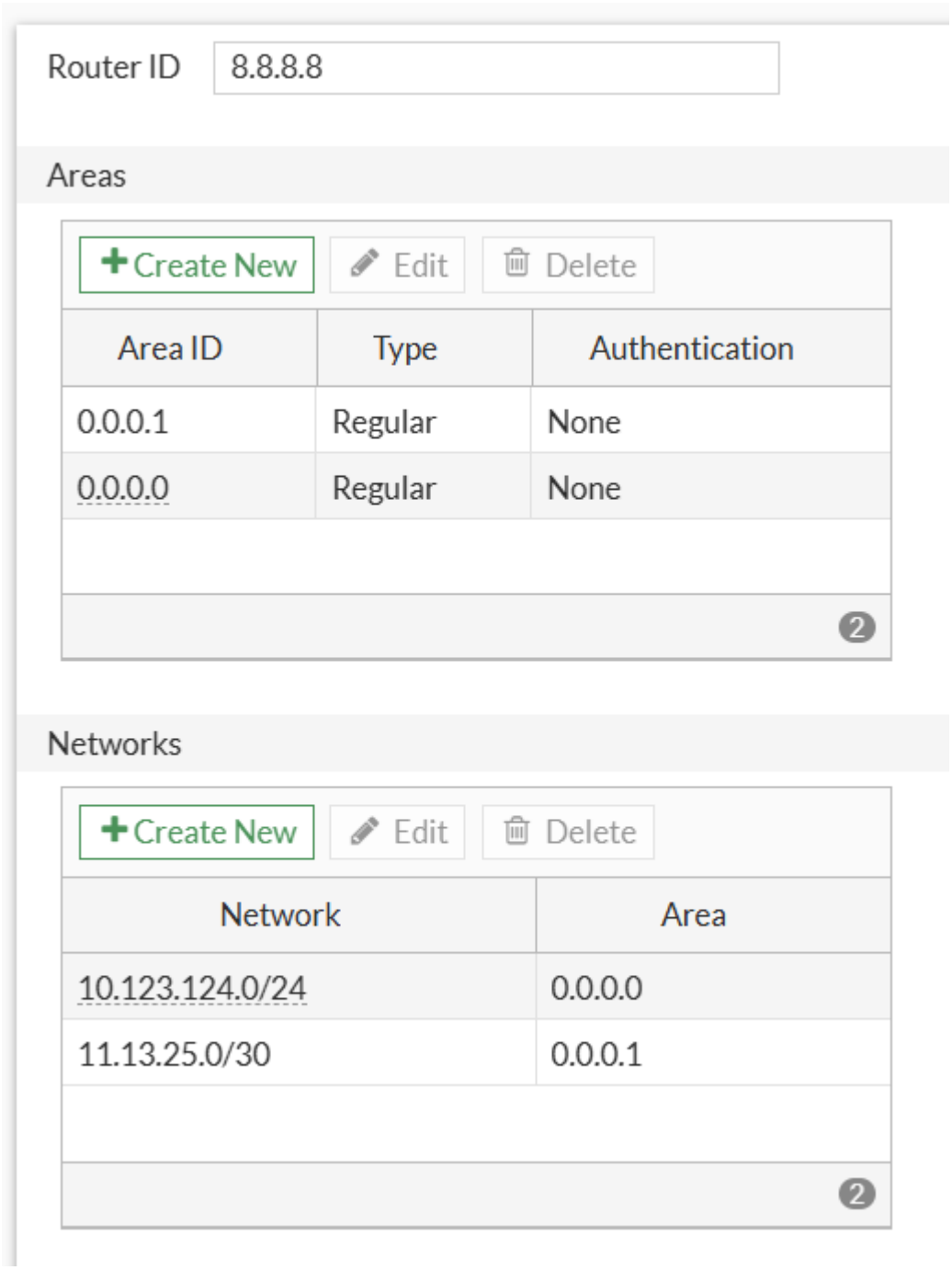
DNS



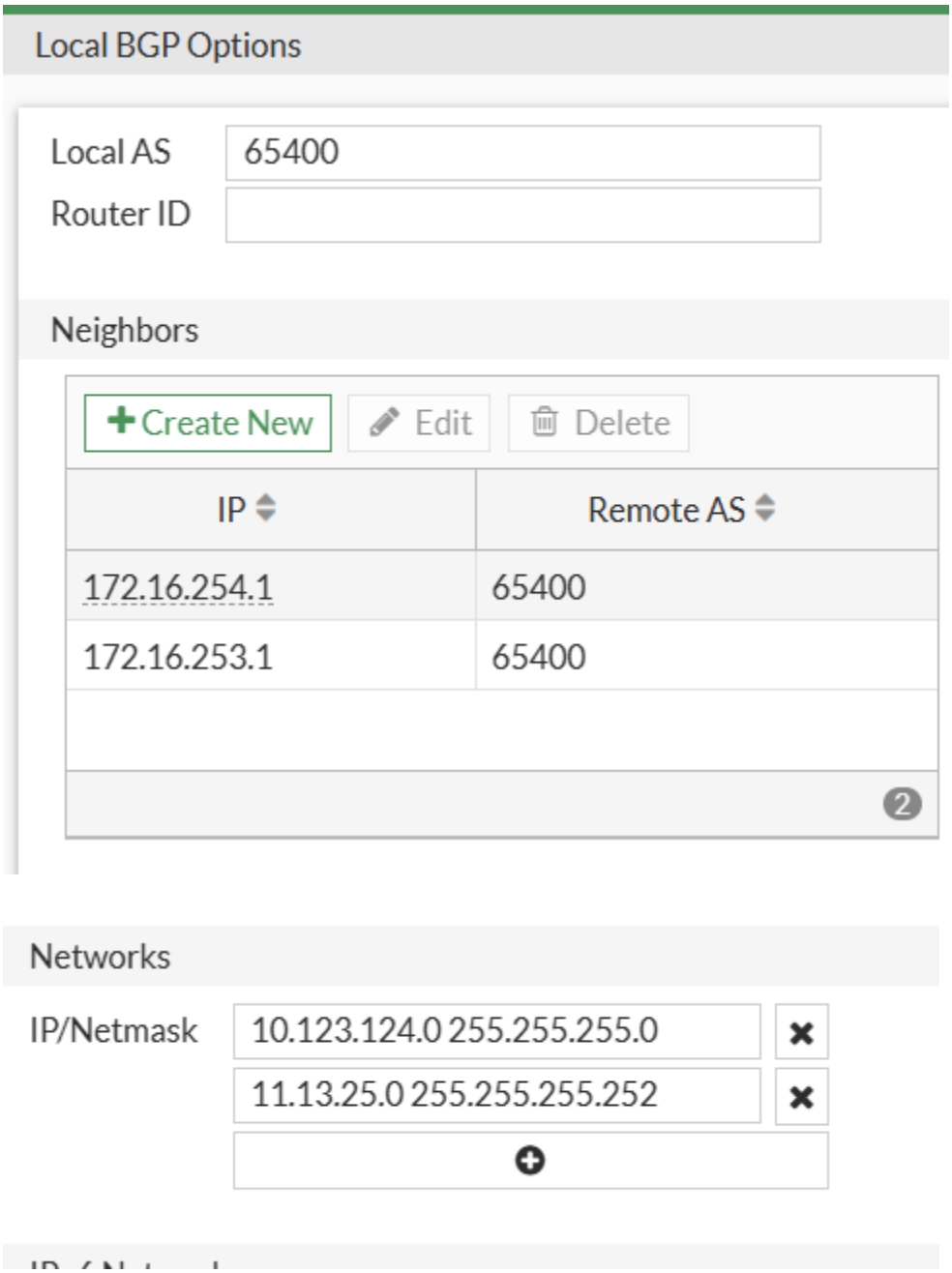
Static Route

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	33.41.12.21	WAN (port3)	Enabled	

OSPF


Router ID
8.8.8.8
Areas
Create New
Edit
Delete
Area ID
Type
Authentication
0.0.0.1
Regular
None
0.0.0.0
Regular
None
2
Networks
Create New
Edit
Delete
Network
Area
10.123.124.0/24
0.0.0.0
11.13.25.0/30
0.0.0.1
2

BGP


Local BGP Options
Local AS
65400
Router ID
Neighbors
Create New
Edit
Delete
IP
Remote AS
172.16.254.1
65400
172.16.253.1
65400
2
Networks
IP/Netmask
10.123.124.0 255.255.255.0
11.13.25.0 255.255.255.252

Firewall Policies

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
OSPF to BGP	OSPF	WAN (port3)	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All	209.51 MB
Hub to OSPF	Spoke	OSPF	all	Spoke_local	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
OSPF to Hub	OSPF	Spoke	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
Hub2 To OSPF	To_Hub_WAN2	OSPF	all	To_Hub_WAN2_local	always	ALL	ACCEPT	Disabled	no-inspection	UTM	2.52 kB
OSPF to Hub2	OSPF	To_Hub_WAN2	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	13.99 kB
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	2.37 kB

Addresses

IP Range/Subnet 9				
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	1
Spoke_local_subnet_1	10.123.124.0/24		Address	1
Spoke_local_subnet_2	11.13.25.0/30		Address	1
To_Hub_WAN2_local_subnet_1	10.123.124.0/24		Address	1
To_Hub_WAN2_local_subnet_2	11.13.25.0/30		Address	1
all	0.0.0.0/0		Address	8
none	0.0.0.0/32		Address	0
FQDN 6				
gmail.com	gmail.com		Address	1
login.microsoft.com	login.microsoft.com		Address	1
login.microsoftonline.com	login.microsoftonline.com		Address	1
login.windows.net	login.windows.net		Address	1
wildcard.dropbox.com	*.dropbox.com		Address	0
wildcard.google.com	*.google.com		Address	1
Address Group 4				
G Suite	gmail.com wildcard.google.com		Address Group	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		Address Group	0
Spoke_local	Spoke_local_subnet_1 Spoke_local_subnet_2		Address Group	1
To_Hub_WAN2_local	To_Hub_WAN2_local_subnet_1		Address Group	1

VPN

Hub-and-Spoke - FortiGate (Spoke) 2			
Spoke	WAN (port3)	Up	3
To_Hub_WAN2	WAN (port3)	Up	3

Tunnel Template: Hub-and-Spoke - FortiGate (Spoke)

Convert To Custom Tunnel

Name: Spoke

Comments: VPN: Spoke (Created by VPN wizard) 34/255

Network Edit

Remote Gateway : Static IP Address (66.31.129.1) , Outgoing Interface : port3

Authentication Edit

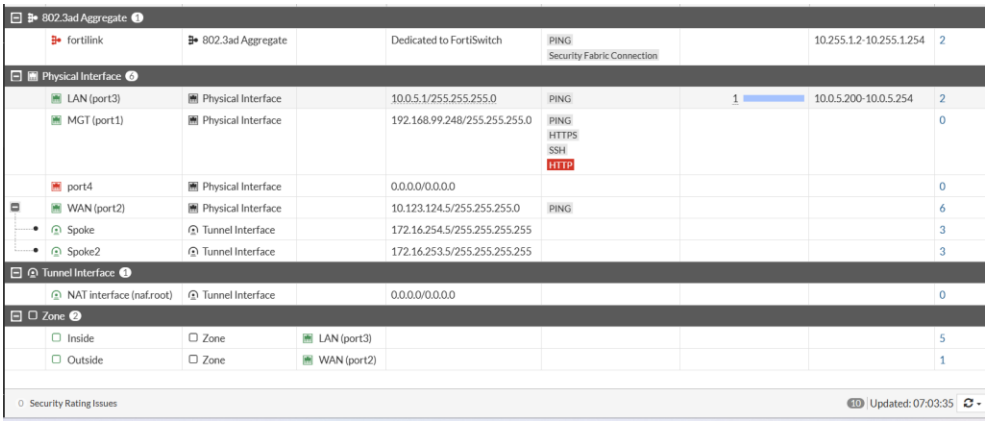
Authentication Method : Pre-shared Key

Phase 2 Selectors

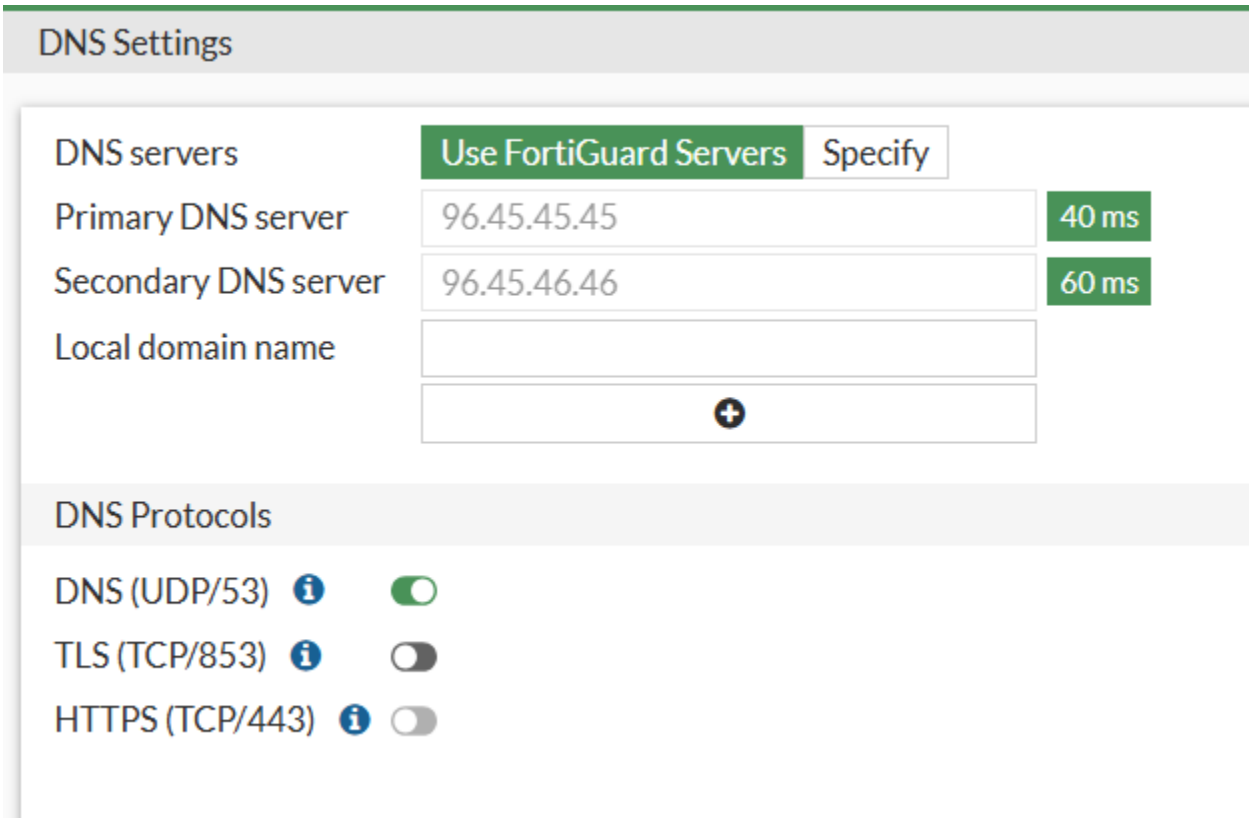
	Local Address	Remote Address
Spoke	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

FW-05 Configuration

Interfaces:



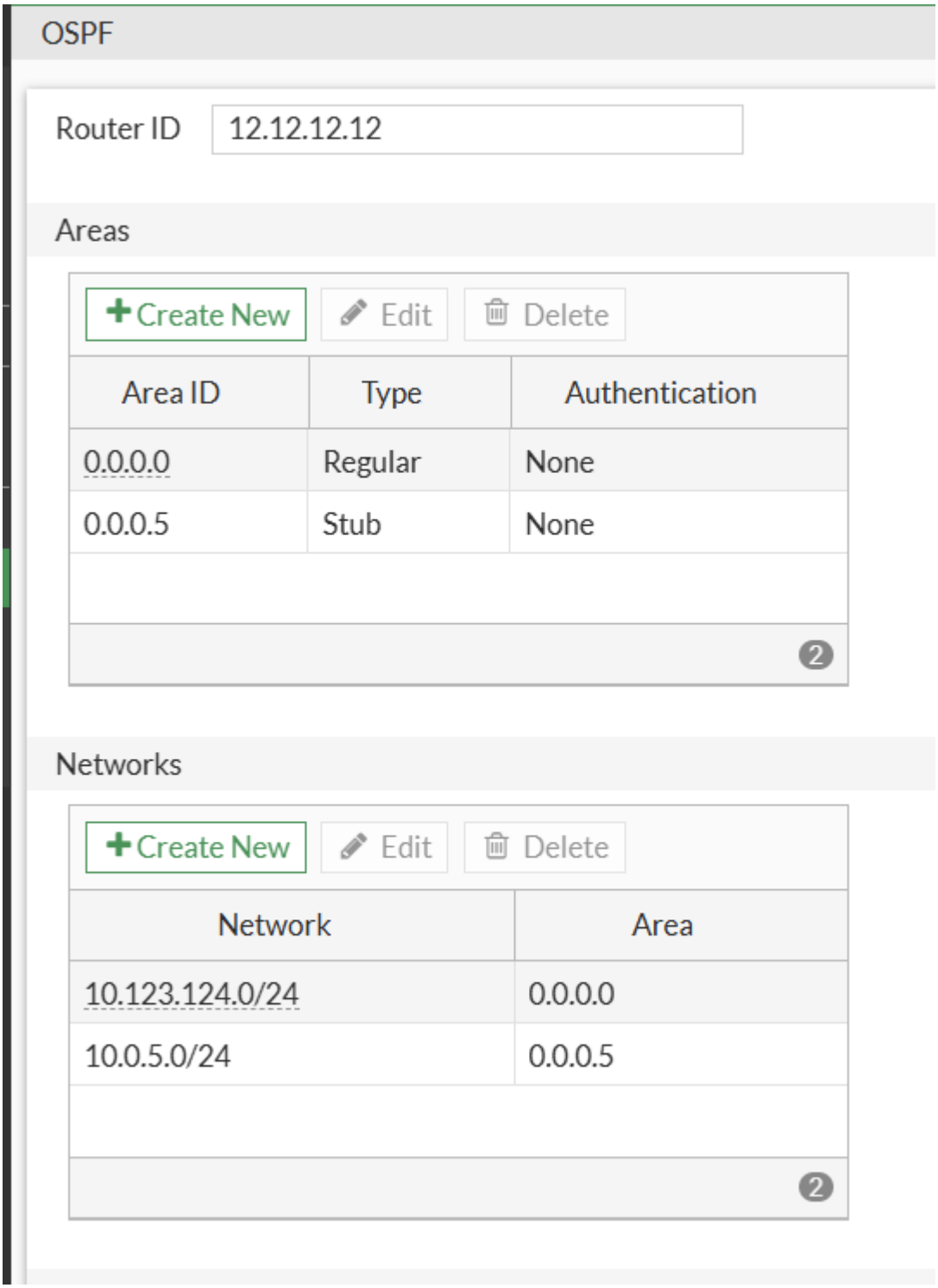
DNS



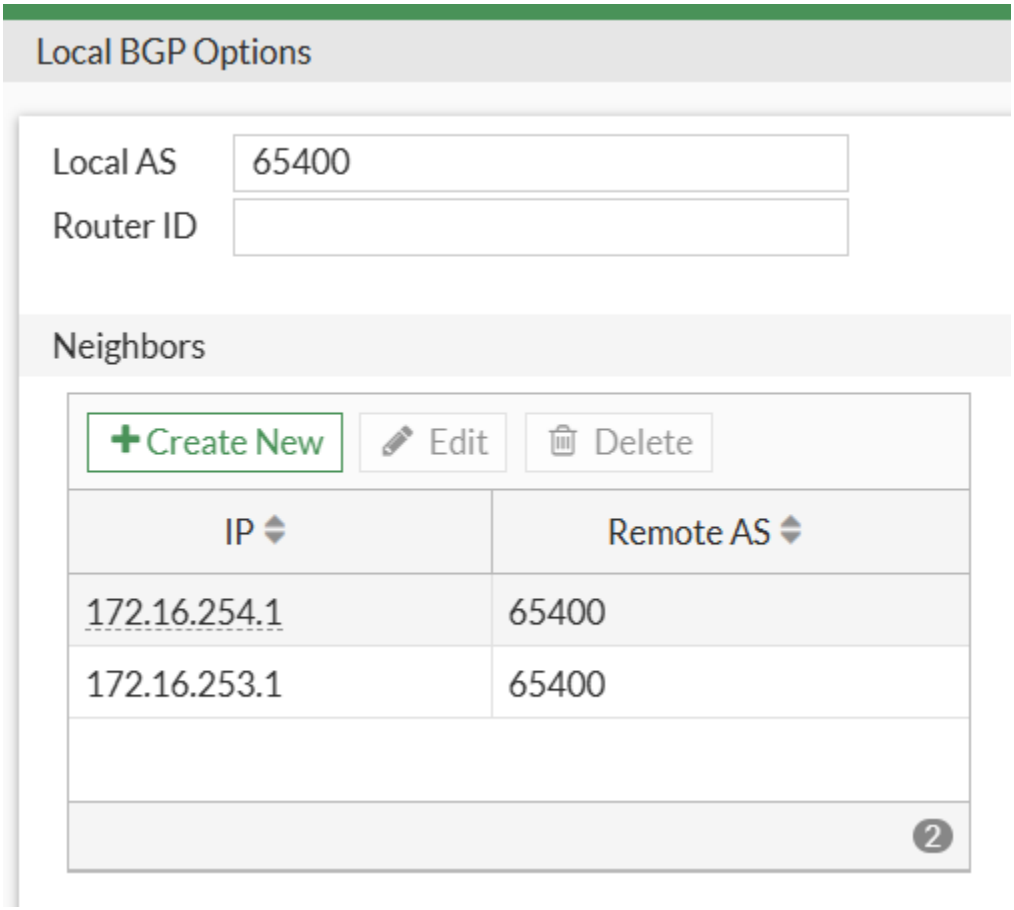
Static Route

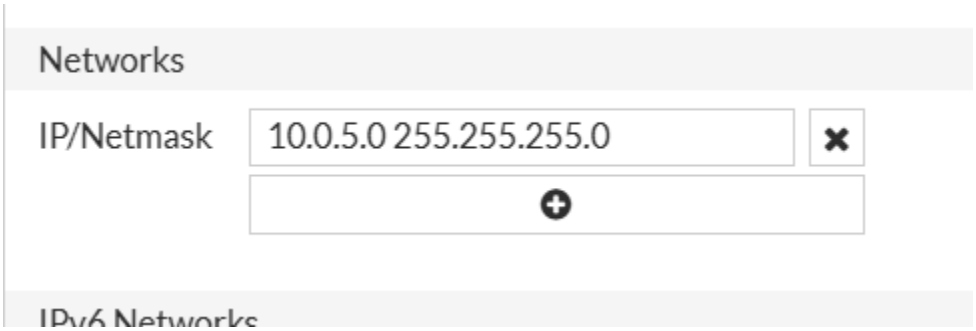
Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	10.123.124.4	WAN (port2)	Enabled	

OSPF


OSPF
Router ID
12.12.12.12
Areas
Create New
Edit
Delete
Area ID
Type
Authentication
0.0.0.0
Regular
None
0.0.0.5
Stub
None
2
Networks
Create New
Edit
Delete
Network
Area
10.123.124.0/24
0.0.0.0
10.0.5.0/24
0.0.0.5
2

BGP





Firewall Policies

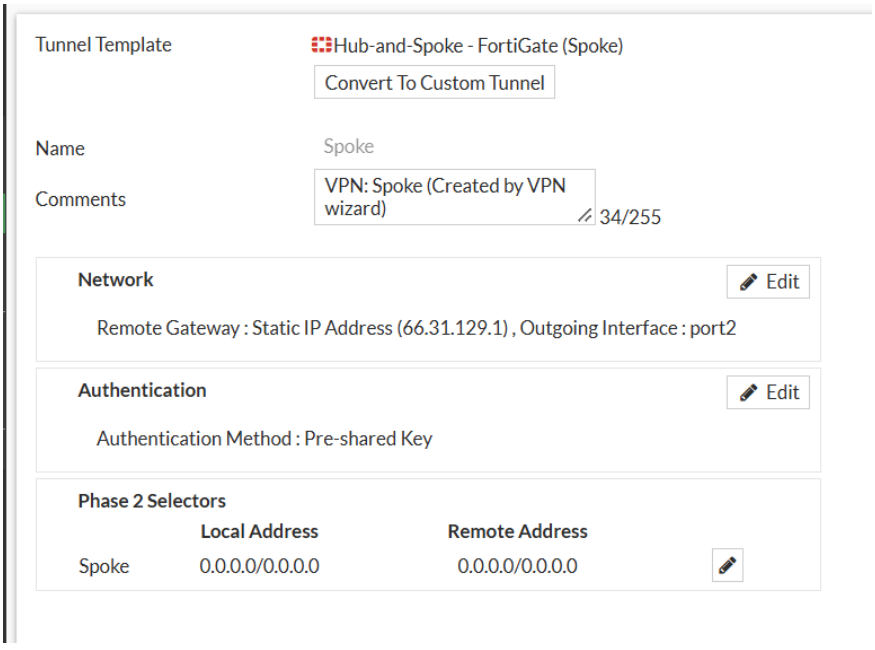
Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
In to Out	Inside	Outside	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	5.00 kB
vpn_Spoke_remote_0	Spoke	Inside	all	Spoke_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
vpn_Spoke_local_0	Inside	Spoke	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
vpn_Spoke2_remote_0	Spoke2	Inside	all	Spoke2_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	672 B
vpn_Spoke2_local_0	Inside	Spoke2	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	0 B

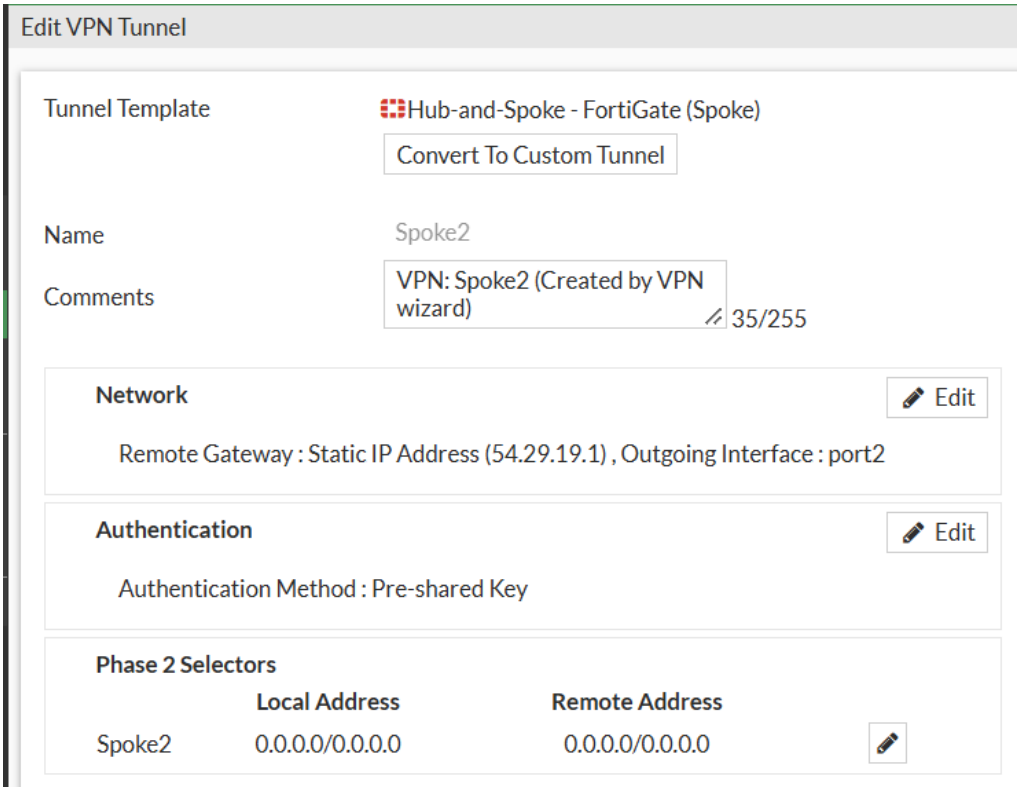
Addresses

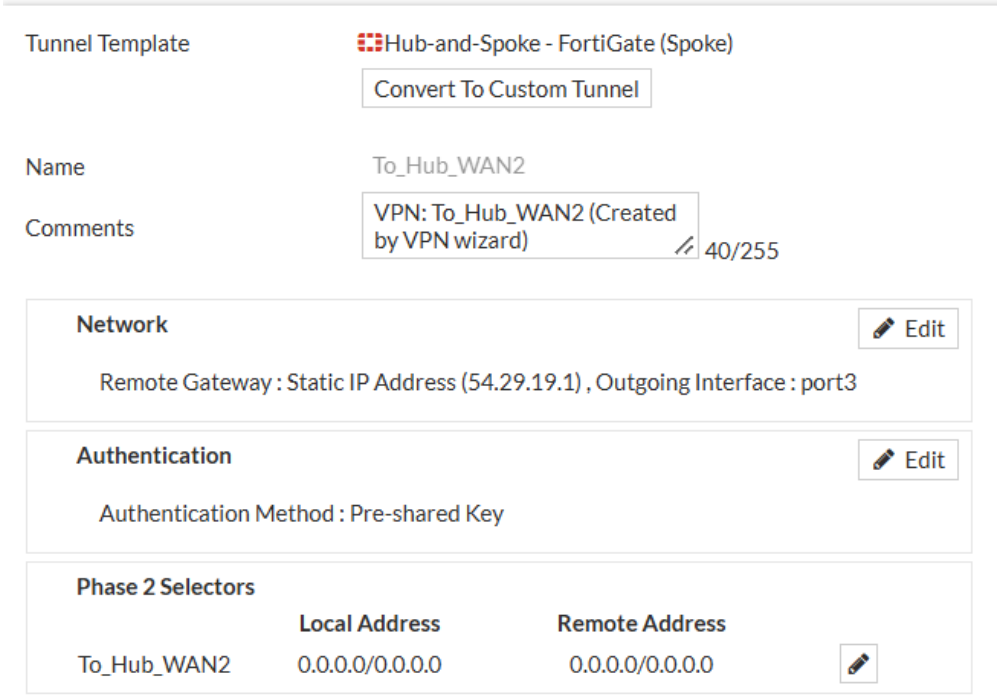
Name	Details	Interface	Type	Ref.
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	1
Spoke2_local_subnet_1	10.0.5.0/24		Address	1
Spoke_local_subnet_1	10.0.5.0/24		Address	1
all	0.0.0.0/0		Address	8
none	0.0.0.0/32		Address	0
FQDN 6				
gmail.com	gmail.com		Address	1
login.microsoft.com	login.microsoft.com		Address	1
login.microsoftonline.com	login.microsoftonline.com		Address	1
login.windows.net	login.windows.net		Address	1
wildcard.dropbox.com	*.dropbox.com		Address	0
wildcard.google.com	*.google.com		Address	1
Address Group 4				
G Suite	gmail.com wildcard.google.com		Address Group	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		Address Group	0
Spoke2_local	Spoke2_local_subnet_1		Address Group	1
Spoke_local	Spoke_local_subnet_1		Address Group	1

VPN

Hub-and-Spoke - FortiGate (Spoke) 2			
Spoke	WAN (port2)	Up	3
Spoke2	WAN (port2)	Up	3




Edit VPN Tunnel
Tunnel Template
Hub-and-Spoke - FortiGate (Spoke)
Convert To Custom Tunnel
Name
Spoke2
Comments
VPN: Spoke2 (Created by VPN wizard)
35/255
Network
Edit
Remote Gateway : Static IP Address (54.29.19.1) , Outgoing Interface : port2
Authentication
Edit
Authentication Method : Pre-shared Key
Phase 2 Selectors
Local Address
Remote Address
Spoke2
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0

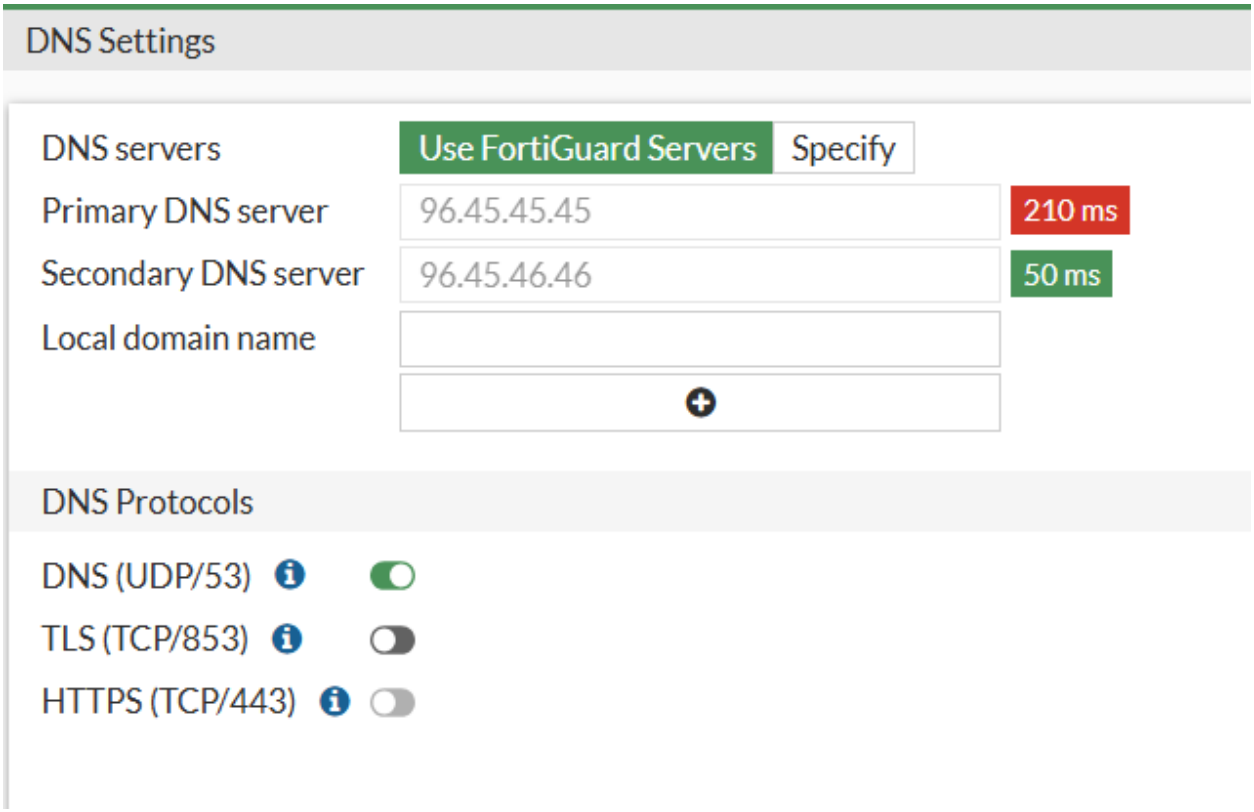

Tunnel Template
Hub-and-Spoke - FortiGate (Spoke)
Convert To Custom Tunnel
Name
To_Hub_WAN2
Comments
VPN: To_Hub_WAN2 (Created by VPN wizard)
40/255
Network
Edit
Remote Gateway : Static IP Address (54.29.19.1) , Outgoing Interface : port3
Authentication
Edit
Authentication Method : Pre-shared Key
Phase 2 Selectors
Local Address
Remote Address
To_Hub_WAN2
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0

FW-06 Configuration

Interfaces:

802.3ad Aggregate 1								
	fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Physical Interface 6								
	WAN (port2)	Physical Interface		10.123.124.6/255.255.255.0	PING			6
	To_Hub2	Tunnel Interface		172.16.253.6/255.255.255.255				3
	To_Hub	Tunnel Interface		172.16.254.6/255.255.255.255				3
	port4	Physical Interface		0.0.0.0/0.0.0.0				0
	MGT (port1)	Physical Interface		192.168.99.243/255.255.255.0	PING HTTPS SSH HTTP			0
	LAN (port3)	Physical Interface		10.0.6.1/255.255.255.0	PING	1	10.0.6.200-10.0.6.254	2
Tunnel Interface 1								
	NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0
Zone 2								
	Outside	Zone	WAN (port2)					1
	Inside	Zone	LAN (port3)					5

DNS



Static Routes

Destination	Gateway IP	Interface	Status
0.0.0.0/0	10.123.124.4	WAN (port2)	Enabled

OSPF

OSPF

Router ID 11.11.11.11

Areas

Create New | Edit | Delete

Area ID	Type	Authentication
0.0.0.0	Regular	None
0.0.0.6	Stub	None

2

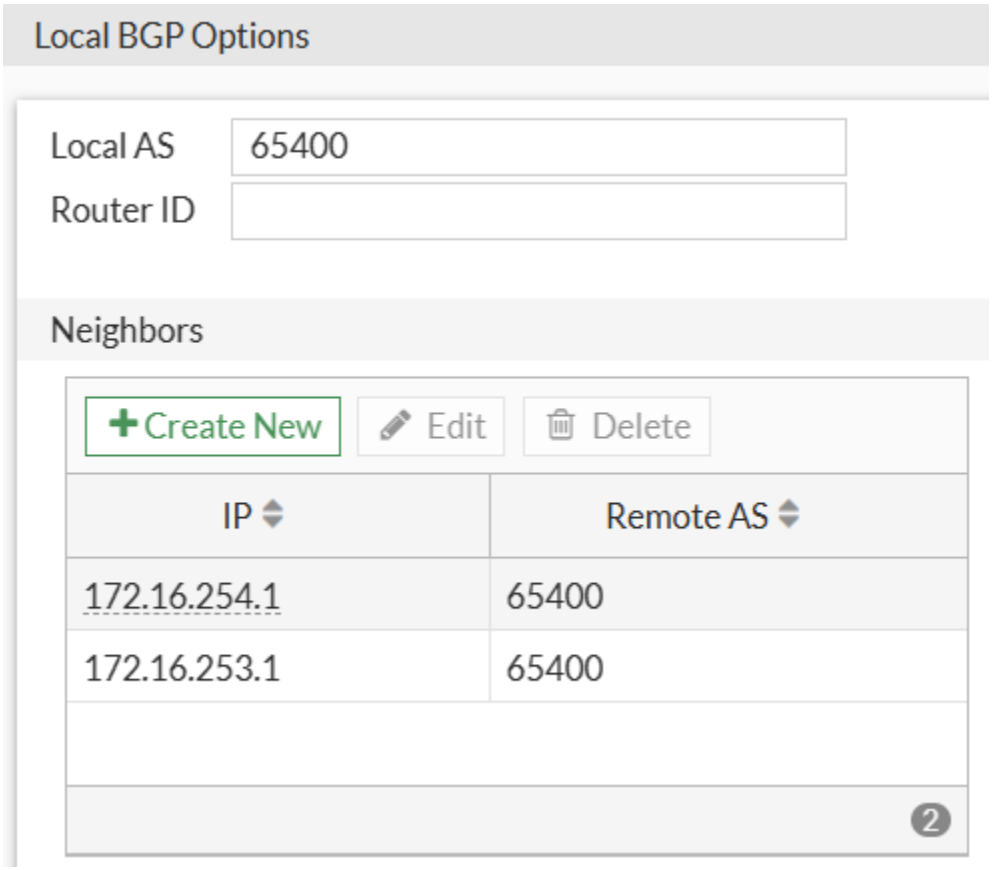
Networks

Create New | Edit | Delete

Network	Area
10.123.124.0/24	0.0.0.0
10.0.6.0/24	0.0.0.6

2

BGP





Firewall Policies



Addresses

Name	Details	Interface	Type	Ref.
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	1
To_Hub2_local_subnet_1	10.0.6.0/24		Address	1
To_Hub_local_subnet_1	10.0.6.0/24		Address	1
all	0.0.0.0/0		Address	8
none	0.0.0.0/32		Address	0
FQDN 6				
gmail.com	gmail.com		Address	1
login.microsoft.com	login.microsoft.com		Address	1
login.microsoftonline.com	login.microsoftonline.com		Address	1
login.windows.net	login.windows.net		Address	1
wildcard.dropbox.com	*.dropbox.com		Address	0
wildcard.google.com	*.google.com		Address	1
Address Group 4				
G Suite	gmail.com wildcard.google.com		Address Group	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		Address Group	0
To_Hub2_local	To_Hub2_local_subnet_1		Address Group	1
To_Hub_local	To_Hub_local_subnet_1		Address Group	1

VPN

Hub-and-Spoke - FortiGate (Spoke) 2			
To_Hub	WAN (port2)	Up	3
To_Hub2	WAN (port2)	Up	3

Edit VPN Tunnel

Tunnel Template: Hub-and-Spoke - FortiGate (Spoke)

Convert To Custom Tunnel

Name: To_Hub

Comments: VPN: To_Hub (Created by VPN wizard) 35/255

Network Edit

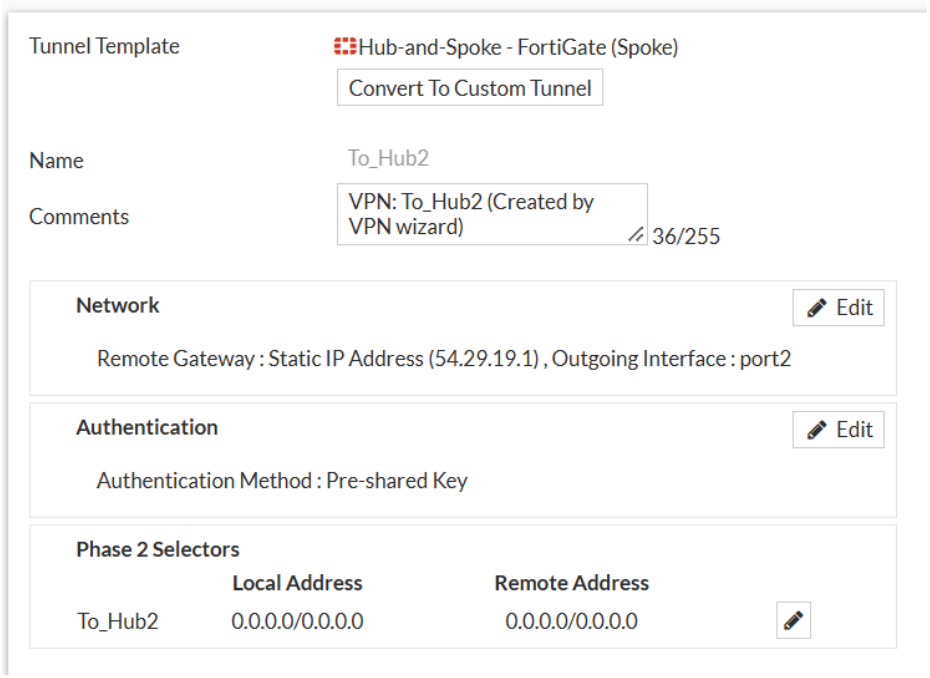
Remote Gateway : Static IP Address (66.31.129.1) , Outgoing Interface : port2

Authentication Edit

Authentication Method : Pre-shared Key

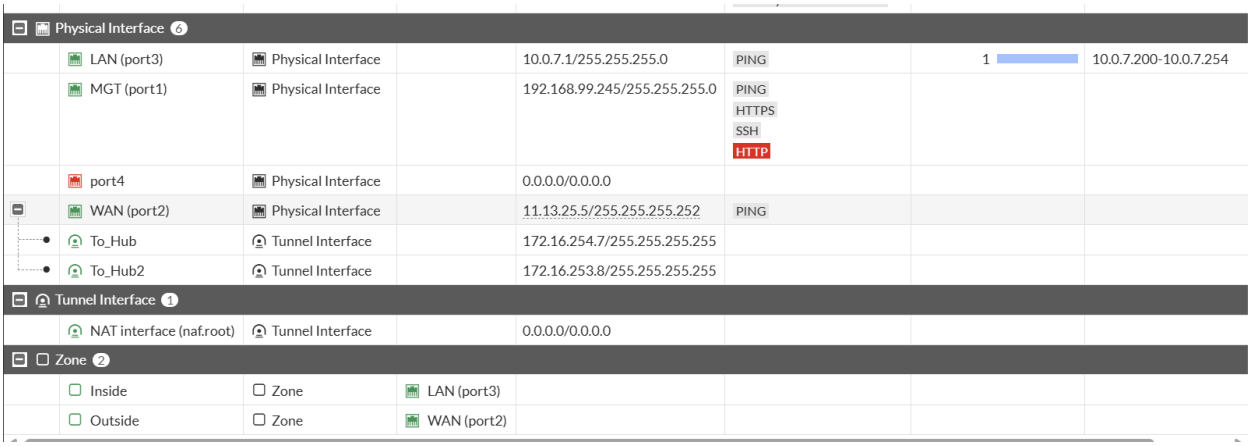
Phase 2 Selectors

	Local Address	Remote Address	
To_Hub	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	

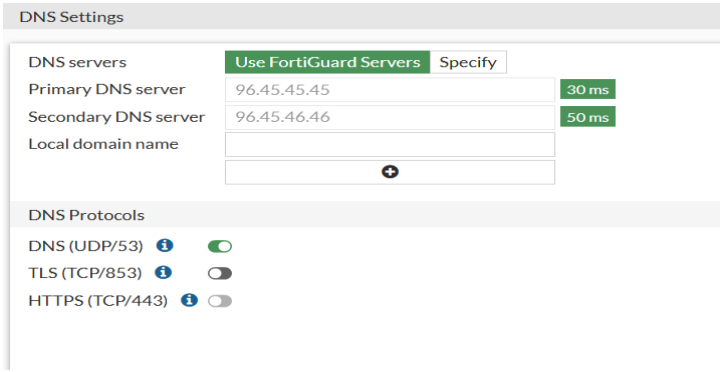


FW-07 Configuration

Interfaces:



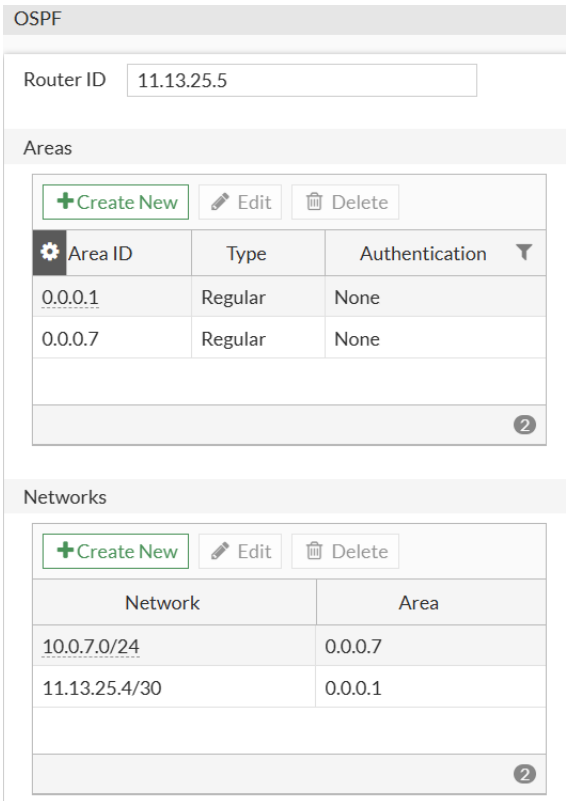
DNS



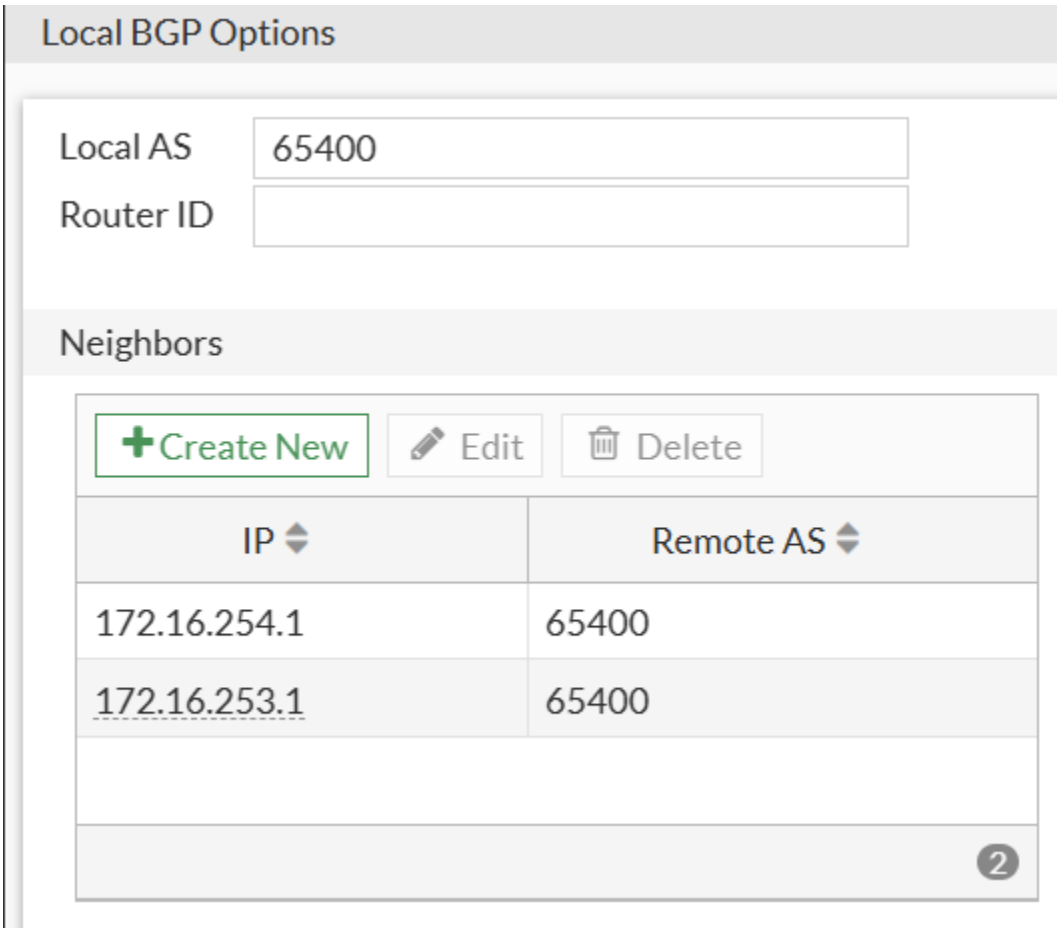
Static Routes

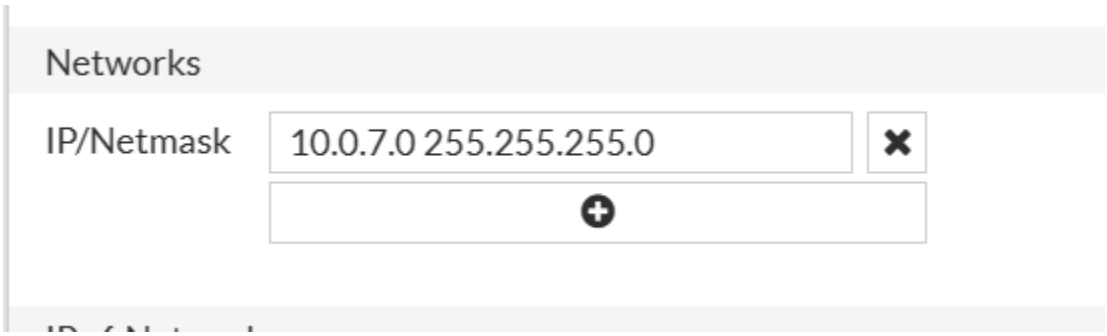
Destination	Gateway IP	Interface	Status
0.0.0.0/0	11.13.25.6	WAN (port2)	Enabled

OSPF



BGP





Firewall Policies

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Inside to Outside	Inside	Outside	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All	8.00 kB
vpn_To_Hub_remote_0	To_Hub	Inside	all	To_Hub_local	always	ALL	ACCEPT	Disabled	no-inspection	UTM	504 B
vpn_To_Hub_local_0	Inside	To_Hub	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
vpn_To_Hub2_remote_0	To_Hub2	Inside	all	To_Hub2_local	always	ALL	ACCEPT	Disabled	no-inspection	UTM	168 B
vpn_To_Hub2_local_0	Inside	To_Hub2	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	5.86 kB

VPN



Hub-and-Spoke - FortiGate (Spoke) 2			
To_Hub	WAN (port2)	Up	3
To_Hub2	WAN (port2)	Up	3

Virtual Link to FW-04

```
config area
    edit 0.0.0.1
        config virtual-link
            edit "VLINK"
                set peer 8.8.8.8
            next
        end
```

```
FW-07 # get router info ospf virtual-links
Virtual Link VLINK1 to router 8.8.8.8 is up
  Process ID 0, VRF 0, Router ID 11.13.25.5, Cost: 2
  Transit area 0.0.0.1 via interface port2
  Local address 11.13.25.5/32
  Remote address 11.13.25.1/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
    Adjacency state Full


FW-07 #
```

```
FW-07 # get router info ospf neighbor all

OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.10       1   Full/DR         00:00:36    11.13.25.6      port2
8.8.8.8           1   Full/ -         00:00:34    11.13.25.1      VLINK1


FW-07 #
```

Filtering RIP Route 20.20.20.20

```
FW-07 (prefix-list) # show
config router prefix-list
    edit "DenyRIP"
        config rule
            edit 1
                set action deny
                set prefix 20.20.20.20 255.255.255.255
                unset ge
                unset le
            next
            edit 2
                set prefix any
                unset ge
                unset le
            next
        end
    next
end
```

```
FW-07 (ospf) # show
config router ospf
    set router-id 11.13.25.5
    set distribute-list-in "DenyRIP"
```

```
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 11.13.25.6, port2, [1/0]
B       10.0.1.0/24 [200/0] via 172.16.254.1 (recursive via To_Hub tunnel 66.31.129.1), 01:24:48
B       10.0.2.0/24 [200/0] via 172.16.253.2 (recursive is directly connected, To_Hub2_0), 01:24:48
B       10.0.3.0/24 [200/0] via 172.16.253.3 (recursive via To_Hub2 tunnel 54.29.19.1), 01:24:48
O IA    10.0.5.0/24 [110/4] via 11.13.25.6, port2, 2d21h29m
O IA    10.0.6.0/24 [110/4] via 11.13.25.6, port2, 2d21h29m
C       10.0.7.0/24 is directly connected, port3
O       10.123.124.0/24 [110/3] via 11.13.25.6, port2, 2d21h29m
O       11.13.25.0/30 [110/2] via 11.13.25.6, port2, 2d21h29m
C       11.13.25.4/30 is directly connected, port2
O IA    30.0.0.0/30 [110/4] via 11.13.25.6, port2, 2d21h29m
O IA    30.0.0.4/30 [110/4] via 11.13.25.6, port2, 2d21h29m
O IA    30.0.0.8/30 [110/5] via 11.13.25.6, port2, 2d21h29m
O IA    30.0.0.12/30 [110/5] via 11.13.25.6, port2, 2d21h29m
S       172.16.253.0/24 [5/0] via To_Hub2 tunnel 54.29.19.1, [1/0]
S       172.16.253.1/32 [15/0] via To_Hub2 tunnel 54.29.19.1, [1/0]
C       172.16.253.2/32 is directly connected, To_Hub2_0
C       172.16.253.8/32 is directly connected, To_Hub2
                        is directly connected, To_Hub2_0
S       172.16.254.0/24 [5/0] via To_Hub tunnel 66.31.129.1, [1/0]
S       172.16.254.1/32 [15/0] via To_Hub tunnel 66.31.129.1, [1/0]
C       172.16.254.7/32 is directly connected, To_Hub
C       192.168.99.0/24 is directly connected, port1
```

FW-08 Configuration

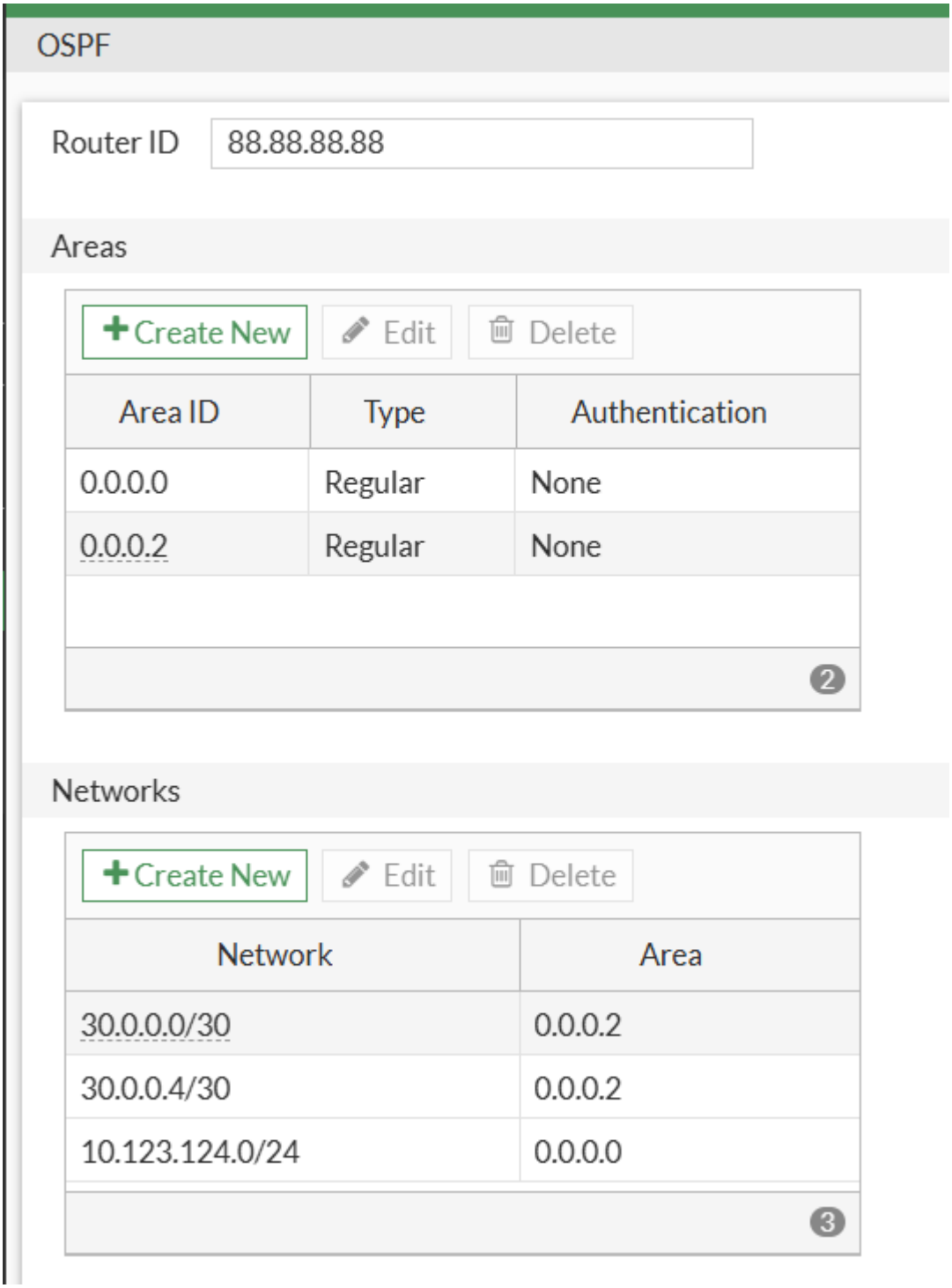
Interfaces:

802.3ad Aggregate 1								
	fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Physical Interface 6								
	Area 0 (port2)	Physical Interface		10.123.124.8/255.255.255.0	PING			7
	To_Hub	Tunnel Interface		172.16.254.8/255.255.255.255				3
	To_Hub2	Tunnel Interface		172.16.253.8/255.255.255.255				3
	port1	Physical Interface		192.168.99.249/255.255.255.0	PING HTTPS SSH HTTP			0
	WAN1 (port3)	Physical Interface		30.0.0.1/255.255.255.252	PING			1
	WAN2 (port4)	Physical Interface		30.0.0.5/255.255.255.252	PING			1
Tunnel Interface 1								
	NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0
Zone 1								
	Area2	Zone	WAN1 (port3) WAN2 (port4)					6

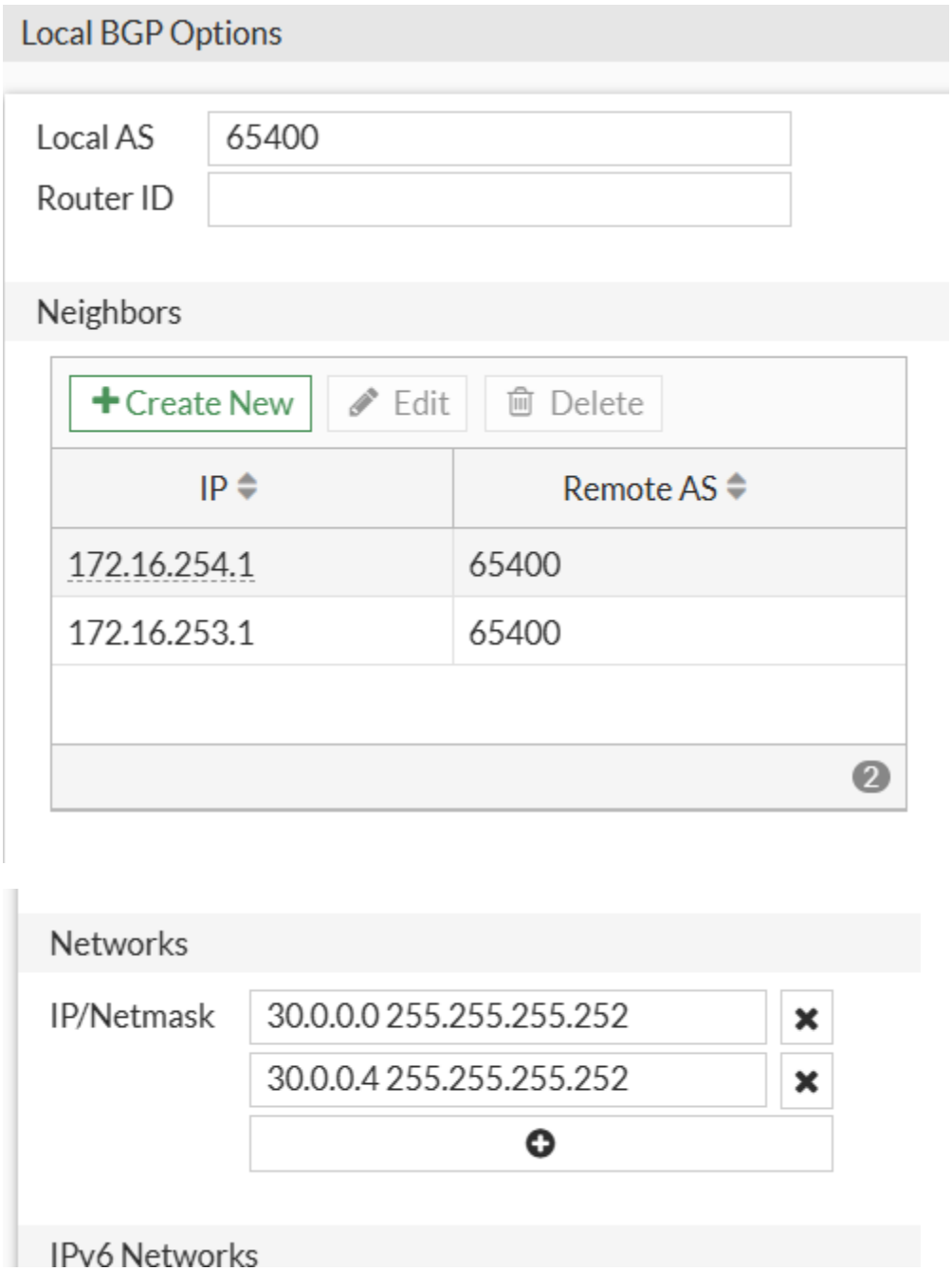
Static Routes

Destination	Gateway IP	Interface	Status
0.0.0.0/0	10.123.124.4	Area 0 (port2)	Enabled

OSPF


OSPF
Router ID
88.88.88.88
Areas
Create New
Edit
Delete
Area ID
Type
Authentication
0.0.0.0
Regular
None
0.0.0.2
Regular
None
2
Networks
Create New
Edit
Delete
Network
Area
30.0.0.0/30
0.0.0.2
30.0.0.4/30
0.0.0.2
10.123.124.0/24
0.0.0.0
3

BGP


Local BGP Options
Local AS
65400
Router ID
Neighbors
Create New
Edit
Delete
IP
Remote AS
172.16.254.1
65400
172.16.253.1
65400
2
Networks
IP/Netmask
30.0.0.0 255.255.255.252
30.0.0.4 255.255.255.252
IPv6 Networks

Firewall Policies

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Area2_To_Area0	Area2	Area 0 (port2)	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
Area0_To_Area2	Area 0 (port2)	Area2	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	504 B
vpn_To_Hub_remote_0	To_Hub	Area2	all	To_Hub_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
vpn_To_Hub_local_0	Area2	To_Hub	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
vpn_To_Hub2_remote	To_Hub2	Area2	all	To_Hub2_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
vpn_To_Hub2_local_0	Area2	To_Hub2	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	504 B

VPN

Hub-and-Spoke - FortiGate (Spoke) 2			
To_Hub	Area 0 (port2)	Up	3
To_Hub2	Area 0 (port2)	Up	3

ECMP Route to RIP

```
FW-08 # get router info routing-table ospf
Routing table for VRF=0
O IA     10.0.5.0/24 [110/2] via 10.123.124.5, port2, 2d22h54m
O IA     10.0.6.0/24 [110/2] via 10.123.124.6, port2, 2d22h54m
O IA     10.0.7.0/24 [110/4] via 10.123.124.4, port2, 2d21h28m
O IA     11.13.25.0/30 [110/2] via 10.123.124.4, port2, 2d21h53m
O IA     11.13.25.4/30 [110/3] via 10.123.124.4, port2, 2d21h53m
O E2     20.20.20.20/32 [110/20] via 30.0.0.2, port3, 2d23h07m
                        [110/20] via 30.0.0.6, port4, 2d23h07m
O        30.0.0.8/30 [110/2] via 30.0.0.2, port3, 2d23h33m
O        30.0.0.12/30 [110/2] via 30.0.0.6, port4, 2d23h33m
```

TESTING

Hub to Spokes LAN:

HUB # execute ping-options source 10.0.1.1

HUB # execute ping 10.0.2.1

PING 10.0.2.1 (10.0.2.1): 56 data bytes

64 bytes from 10.0.2.1: icmp_seq=0 ttl=255 time=7.3 ms

64 bytes from 10.0.2.1: icmp_seq=1 ttl=255 time=5.6 ms

64 bytes from 10.0.2.1: icmp_seq=2 ttl=255 time=6.0 ms

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 5.6/6.3/7.3 ms

HUB # execute ping 10.0.3.1

PING 10.0.3.1 (10.0.3.1): 56 data bytes

64 bytes from 10.0.3.1: icmp_seq=0 ttl=255 time=8.8 ms

64 bytes from 10.0.3.1: icmp_seq=1 ttl=255 time=12.0 ms

64 bytes from 10.0.3.1: icmp_seq=2 ttl=255 time=9.9 ms

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 8.8/10.2/12.0 ms

HUB # execute ping 10.0.5.1

PING 10.0.5.1 (10.0.5.1): 56 data bytes

64 bytes from 10.0.5.1: icmp_seq=0 ttl=255 time=21.0 ms

64 bytes from 10.0.5.1: icmp_seq=1 ttl=255 time=18.2 ms

64 bytes from 10.0.5.1: icmp_seq=2 ttl=255 time=17.1 ms

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 17.1/18.7/21.0 ms

HUB # execute ping 10.0.6.1

PING 10.0.6.1 (10.0.6.1): 56 data bytes

64 bytes from 10.0.6.1: icmp_seq=0 ttl=255 time=16.1 ms

64 bytes from 10.0.6.1: icmp_seq=1 ttl=255 time=18.2 ms

64 bytes from 10.0.6.1: icmp_seq=2 ttl=255 time=18.5 ms

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 16.1/17.6/18.5 ms

HUB # execute ping 10.0.7.1

PING 10.0.7.1 (10.0.7.1): 56 data bytes

64 bytes from 10.0.7.1: icmp_seq=0 ttl=255 time=18.2 ms

64 bytes from 10.0.7.1: icmp_seq=1 ttl=255 time=16.9 ms

64 bytes from 10.0.7.1: icmp_seq=2 ttl=255 time=18.8 ms

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 16.9/17.9/18.8 ms

HUB # execute ping 30.0.0.1

PING 30.0.0.1 (30.0.0.1): 56 data bytes

64 bytes from 30.0.0.1: icmp_seq=0 ttl=255 time=17.6 ms

64 bytes from 30.0.0.1: icmp_seq=1 ttl=255 time=17.8 ms

64 bytes from 30.0.0.1: icmp_seq=2 ttl=255 time=18.0 ms

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 17.6/17.8/18.0 ms

HUB # execute ping 30.0.0.5

PING 30.0.0.5 (30.0.0.5): 56 data bytes

64 bytes from 30.0.0.5: icmp_seq=0 ttl=255 time=16.3 ms

64 bytes from 30.0.0.5: icmp_seq=1 ttl=255 time=17.3 ms

64 bytes from 30.0.0.5: icmp_seq=2 ttl=255 time=17.3 ms

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 16.3/16.9/17.3 ms

Spokes to Spoke:

FW-02 # execute ping-options source 10.0.2.1

FW-02 # execute ping 10.0.1.1

PING 10.0.1.1 (10.0.1.1): 56 data bytes

64 bytes from 10.0.1.1: icmp_seq=0 ttl=255 time=6.5 ms

64 bytes from 10.0.1.1: icmp_seq=1 ttl=255 time=5.7 ms

64 bytes from 10.0.1.1: icmp_seq=2 ttl=255 time=5.0 ms

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 5.0/5.7/6.5 ms

FW-02 # execute ping 10.0.3.1

PING 10.0.3.1 (10.0.3.1): 56 data bytes

64 bytes from 10.0.3.1: icmp_seq=0 ttl=254 time=16.6 ms

64 bytes from 10.0.3.1: icmp_seq=2 ttl=255 time=10.9 ms

64 bytes from 10.0.3.1: icmp_seq=3 ttl=255 time=11.4 ms

4 packets transmitted, 3 packets received, 25% packet loss

round-trip min/avg/max = 10.9/12.9/16.6 ms

FW-02 # execute ping 10.0.5.1

PING 10.0.5.1 (10.0.5.1): 56 data bytes

64 bytes from 10.0.5.1: icmp_seq=0 ttl=254 time=21.1 ms

64 bytes from 10.0.5.1: icmp_seq=3 ttl=255 time=16.5 ms

64 bytes from 10.0.5.1: icmp_seq=4 ttl=255 time=16.6 ms

5 packets transmitted, 3 packets received, 40% packet loss

round-trip min/avg/max = 16.5/18.0/21.1 ms

FW-02 # execute ping 10.0.6.1

PING 10.0.6.1 (10.0.6.1): 56 data bytes

64 bytes from 10.0.6.1: icmp_seq=0 ttl=254 time=23.2 ms

64 bytes from 10.0.6.1: icmp_seq=2 ttl=255 time=16.8 ms

64 bytes from 10.0.6.1: icmp_seq=3 ttl=255 time=17.4 ms

4 packets transmitted, 3 packets received, 25% packet loss

round-trip min/avg/max = 16.8/19.1/23.2 ms

FW-02 # execute ping 10.0.7.1

PING 10.0.7.1 (10.0.7.1): 56 data bytes

64 bytes from 10.0.7.1: icmp_seq=0 ttl=254 time=21.3 ms

64 bytes from 10.0.7.1: icmp_seq=2 ttl=255 time=14.8 ms

64 bytes from 10.0.7.1: icmp_seq=3 ttl=255 time=16.8 ms

4 packets transmitted, 3 packets received, 25% packet loss

round-trip min/avg/max = 14.8/17.6/21.3 ms

Hub WAN1 Failing Over to WAN2 (BFD).

- Because BGP is very slow with convergence we are going to need to configure all Firewalls with BFD for faster convergence.
- Here's what we did on the HUB and FW02 as a Spoke example:

SPOKE

```
FW-02 (Spoke) # show
config system interface
    edit "Spoke"
        set vdom "root"
        set ip 172.16.254.2 255.255.255.255
        set allowaccess ping
        set bfd enable
        set type tunnel
        set remote-ip 172.16.254.1 255.255.255.0
        set snmp-index 9
        set interface "port2"
    next
end
```

```
FW-02 (bgp) # show
config router bgp
    set as 65400
    config neighbor
        edit "172.16.254.1"
            set bfd enable
            set remote-as 65400
        next
        edit "172.16.253.1"
            set bfd enable
            set remote-as 65400
        next
```

```
FW-02 (settings) # show
config system settings
    set bfd enable
    set bfd-desired-min-tx 300
    set bfd-required-min-rx 300
end
```

HUB:

```
FW-02 (settings) # show
config system settings
    set bfd enable
    set bfd-desired-min-tx 300
    set bfd-required-min-rx 300
end
```

```
edit "Hub_WAN1"
    set vdom "root"
    set ip 172.16.254.1 255.255.255.255
    set allowaccess ping
    set bfd enable
    set type tunnel
    set remote-ip 172.16.254.254 255.255.255.0
    set snmp-index 9
    set interface "port2"
next
edit "Hub_WAN2"
    set vdom "root"
    set ip 172.16.253.1 255.255.255.255
    set allowaccess ping
    set bfd enable
    set type tunnel
    set remote-ip 172.16.253.254 255.255.255.0
    set snmp-index 10
    set interface "port3"
next
```

```
config router bgp
    set as 65400
    config neighbor
        edit "172.16.254.2"
            set bfd enable
        next
        edit "172.16.254.3"
            set bfd enable
        next
        edit "172.16.254.4"
           set bfd enable
        next
        edit "172.16.253.2"
            set bfd enable
        next
        edit "172.16.253.3"
           set bfd enable
        next
        edit "172.16.253.4"
          set bfd enable
        edit "172.16.254.5"
         set bfd enable
        edit "172.16.254.6"
         set bfd enable
        next
        edit "172.16.254.8"
            set bfd enable
        next
        edit "172.16.253.5"
            set bfd enable
        next
        edit "172.16.253.6"
            set bfd enable
        next
        edit "172.16.253.8"
            set bfd enable
        next
        edit "172.16.254.7"
            set bfd enable
        next
        edit "172.16.253.7"
            set bfd enable
        next
    end
```

- We are going to ping from FW02 to 10.0.1.1 which is the LAN behind the HUB.
- We are going to shutdown WAN1 interface while pinging 10.0.1.1 from FW02 and capture the packet loss and how it would failover to Wan2 on the HUB live.
- This is the status of the BFD neighbors:

```
FW-02 # get router info bfd neighbor

OurAddress      NeighAddress    State       Interface       LDesc/RDesc
172.16.254.2    172.16.254.1    UP          Spoke           9/46
172.16.253.2    172.16.253.1    UP          Spoke2          8/40

FW-02 #
```

FW-02 # execute ping 10.0.1.1

PING 10.0.1.1 (10.0.1.1): 56 data bytes

64 bytes from 10.0.1.1: icmp_seq=0 ttl=255 time=4.9 ms

64 bytes from 10.0.1.1: icmp_seq=1 ttl=255 time=3.8 ms

64 bytes from 10.0.1.1: icmp_seq=2 ttl=255 time=8.4 ms

64 bytes from 10.0.1.1: icmp_seq=3 ttl=255 time=4.8 ms

64 bytes from 10.0.1.1: icmp_seq=4 ttl=255 time=5.3 ms

64 bytes from 10.0.1.1: icmp_seq=5 ttl=255 time=4.7 ms

64 bytes from 10.0.1.1: icmp_seq=6 ttl=255 time=3.9 ms

64 bytes from 10.0.1.1: icmp_seq=7 ttl=255 time=4.9 ms

64 bytes from 10.0.1.1: icmp_seq=8 ttl=255 time=4.1 ms

64 bytes from 10.0.1.1: icmp_seq=9 ttl=255 time=4.6 ms

64 bytes from 10.0.1.1: icmp_seq=10 ttl=255 time=4.7 ms

64 bytes from 10.0.1.1: icmp_seq=11 ttl=255 time=4.3 ms

64 bytes from 10.0.1.1: icmp_seq=12 ttl=255 time=3.9 ms

64 bytes from 10.0.1.1: icmp_seq=13 ttl=255 time=3.4 ms

64 bytes from 10.0.1.1: icmp_seq=14 ttl=255 time=5.7 ms

64 bytes from 10.0.1.1: icmp_seq=15 ttl=255 time=4.4 ms

64 bytes from 10.0.1.1: icmp_seq=16 ttl=255 time=5.9 ms

64 bytes from 10.0.1.1: icmp_seq=17 ttl=255 time=4.4 ms

64 bytes from 10.0.1.1: icmp_seq=18 ttl=255 time=3.8 ms

64 bytes from 10.0.1.1: icmp_seq=19 ttl=255 time=4.2 ms

64 bytes from 10.0.1.1: icmp_seq=20 ttl=255 time=7.0 ms

64 bytes from 10.0.1.1: icmp_seq=21 ttl=255 time=3.9 ms

64 bytes from 10.0.1.1: icmp_seq=22 ttl=255 time=4.5 ms

64 bytes from 10.0.1.1: icmp_seq=23 ttl=255 time=4.9 ms

64 bytes from 10.0.1.1: icmp_seq=24 ttl=255 time=4.1 ms

64 bytes from 10.0.1.1: icmp_seq=25 ttl=255 time=5.2 ms

26 packets transmitted, 26 packets received, 0% packet loss

round-trip min/avg/max = 3.4/4.7/8.4 ms

- There was 0 Packet loss after shutting down WAN1.