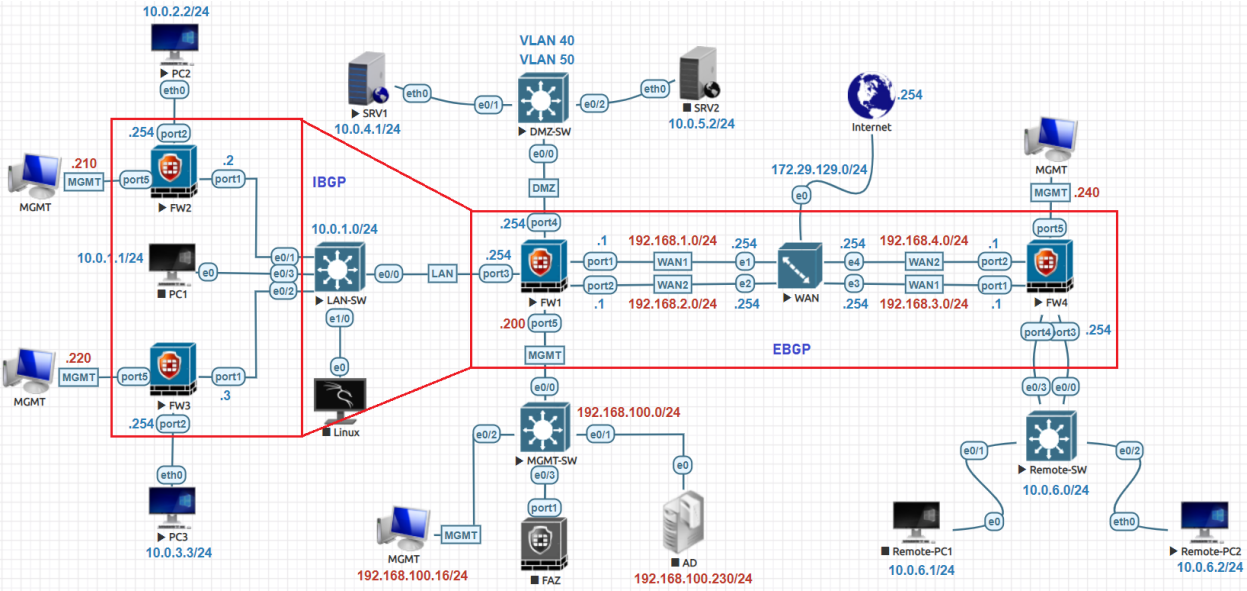
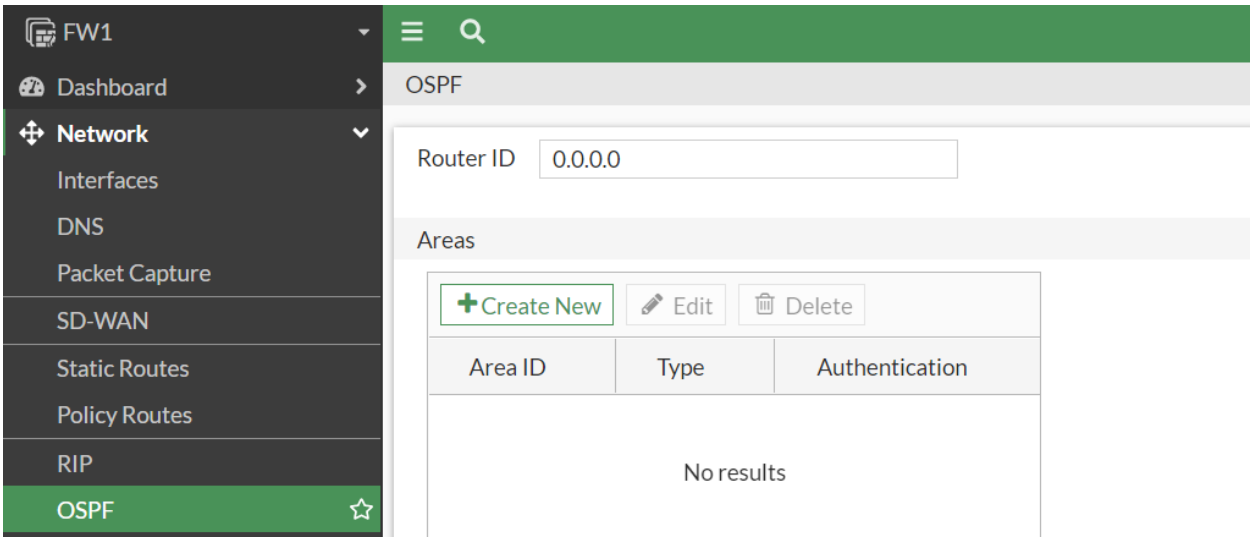
Dynamic Protocol BGP Lab:



Two Core Firewall, FW2 and FW3, connect to the ISP Firewall FW1 for the internet access. Both FW2 and FW3 have different Local Networks. The ISP Firewall FW1 is using IBGP for its connections to the core Firewalls, and redistributes its default route to the network - that is, default route injection is enabled. The ISP Firewall FW1 uses NAT and has a static route to the internet. None of the other Firewalls use NAT or static routes.

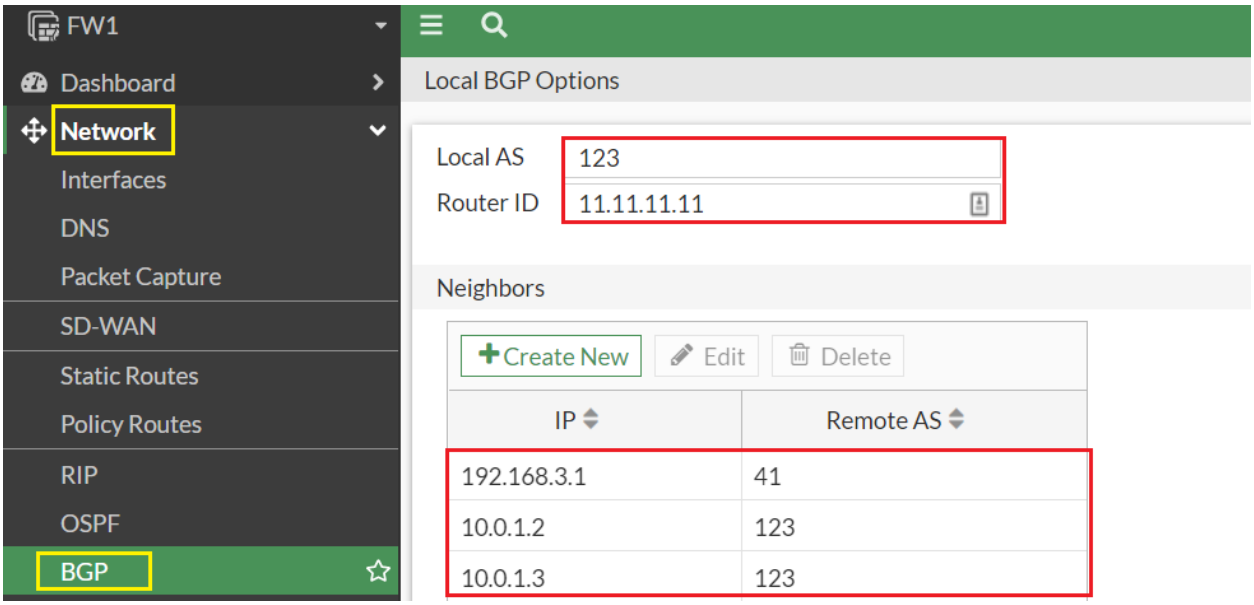
Deleted OSPF Routes:

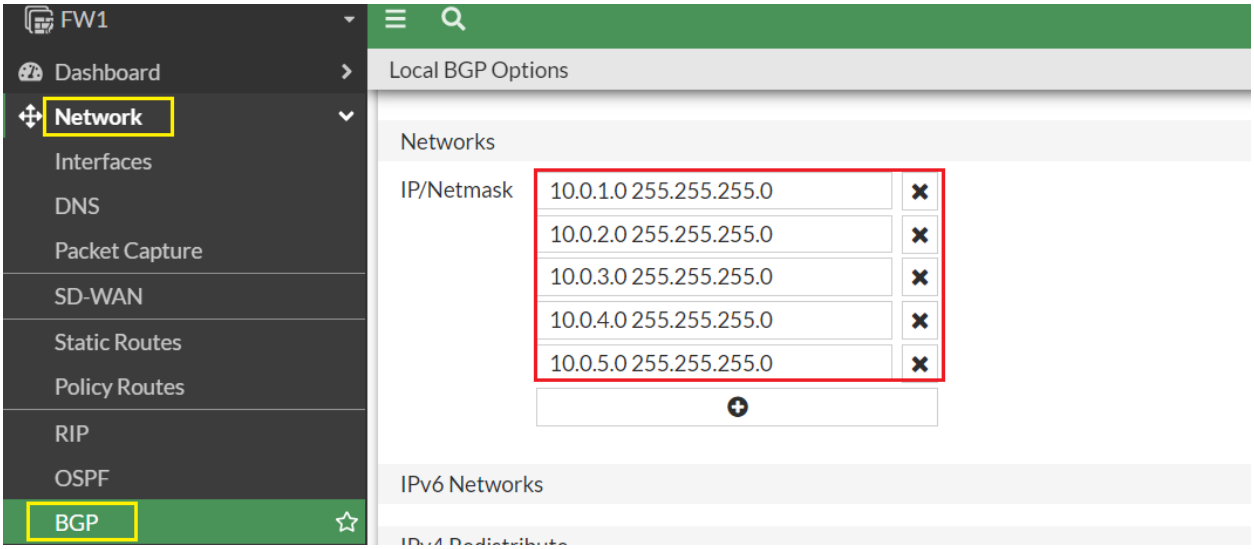
First we need to delete OSPF configured Routing protocol from previous lab.



FW1 BGP Configuration:

Go to Network > BGP Set the Local AS in this case 123. Set the Router ID 11.11.11.11. Configure the remote router's AS number, any other properties used for peering with the neighbor, under Networks, add five networks. Leave the remaining settings as their default values. Click OK. Click Apply.

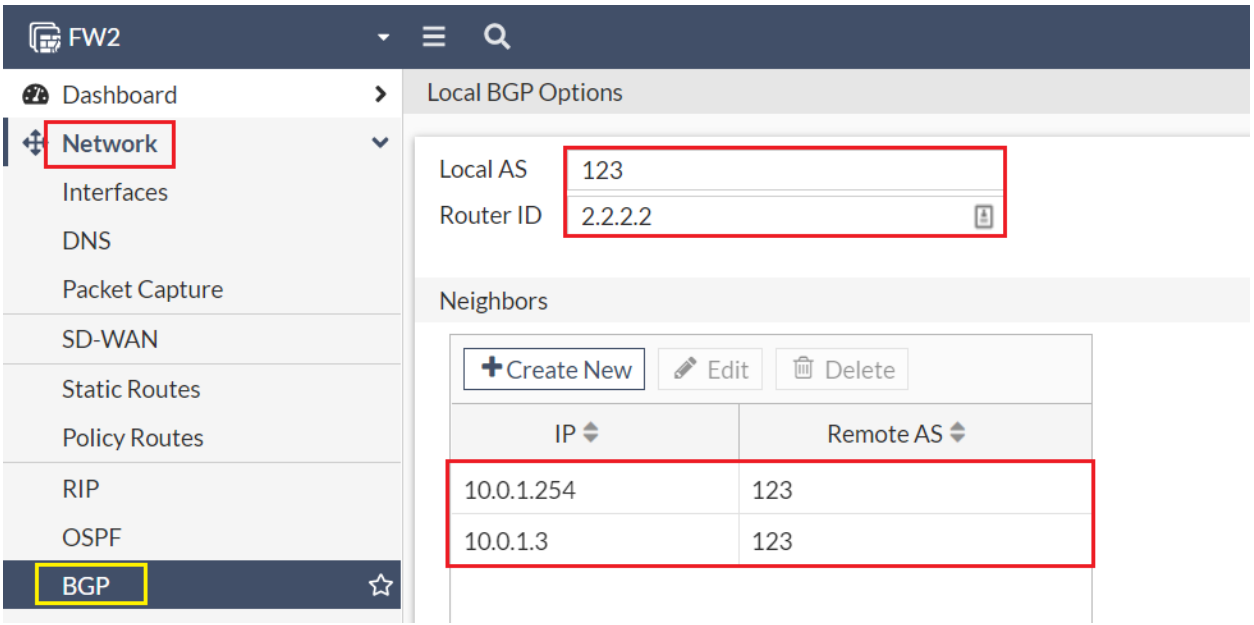


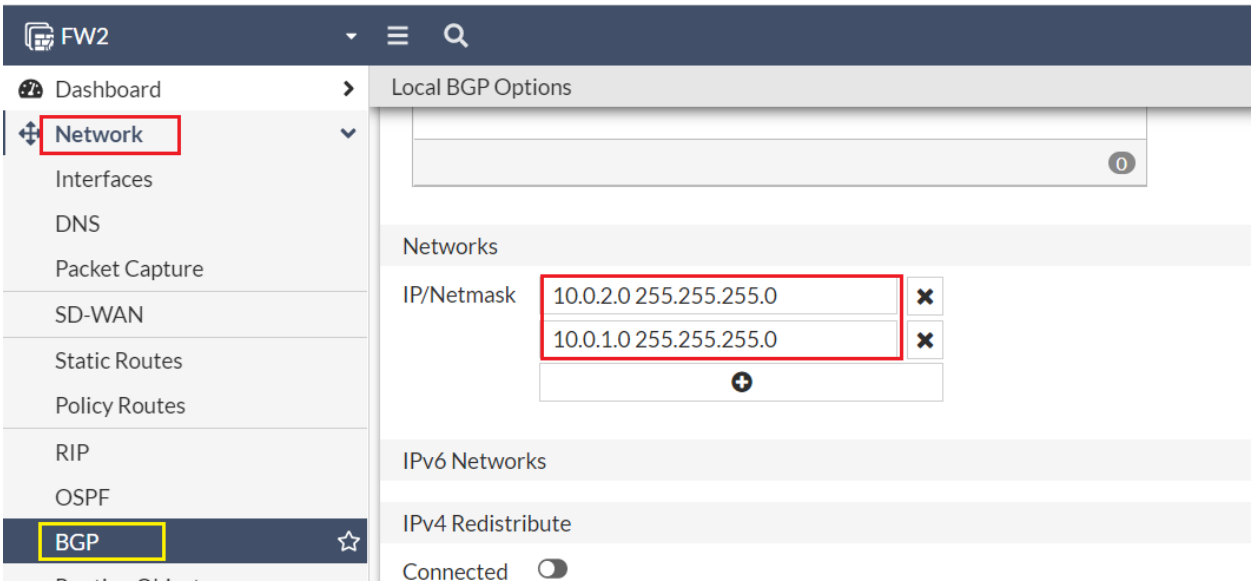


FW1 to FW4 change multihop for EBGP
config router bgp config neighbor edit "192.168.1.102" set ebgp-enforce-multihop enable set ebgp-multihop-ttl 255 end

FW2 BGP Configuration:

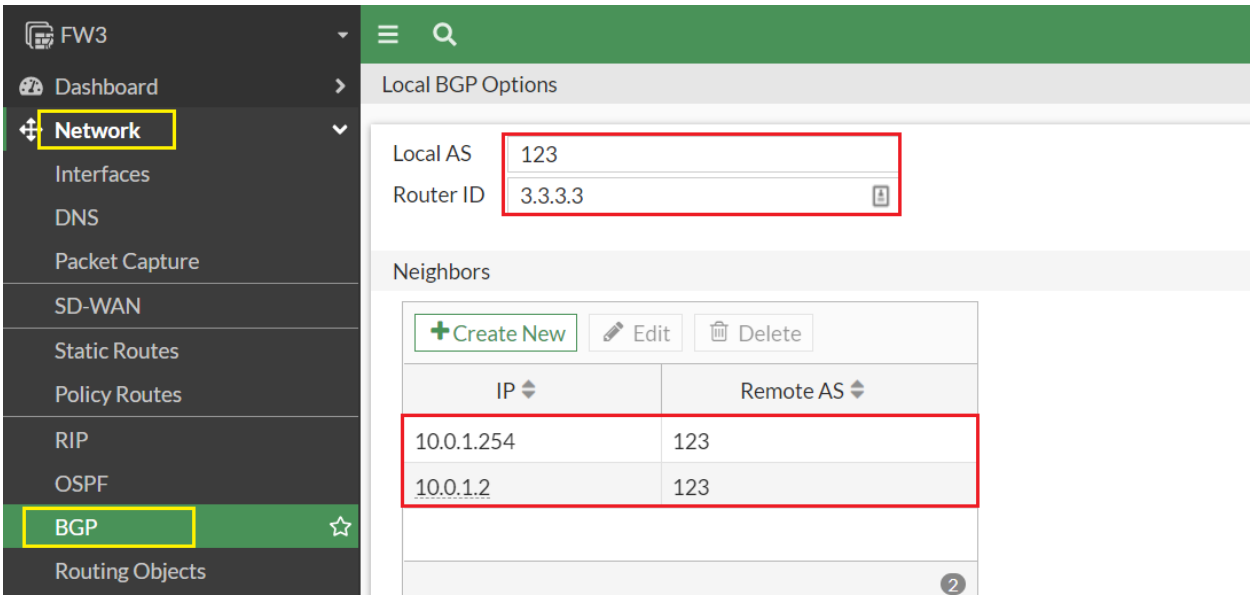
Go to Network > BGP Set the Local AS in this case 123. Set the Router ID 2.2.2.2. Configure the remote router's AS number, any other properties used for peering with the neighbor, under Networks, add two networks. Leave the remaining settings as their default values. Click OK. Click Apply.

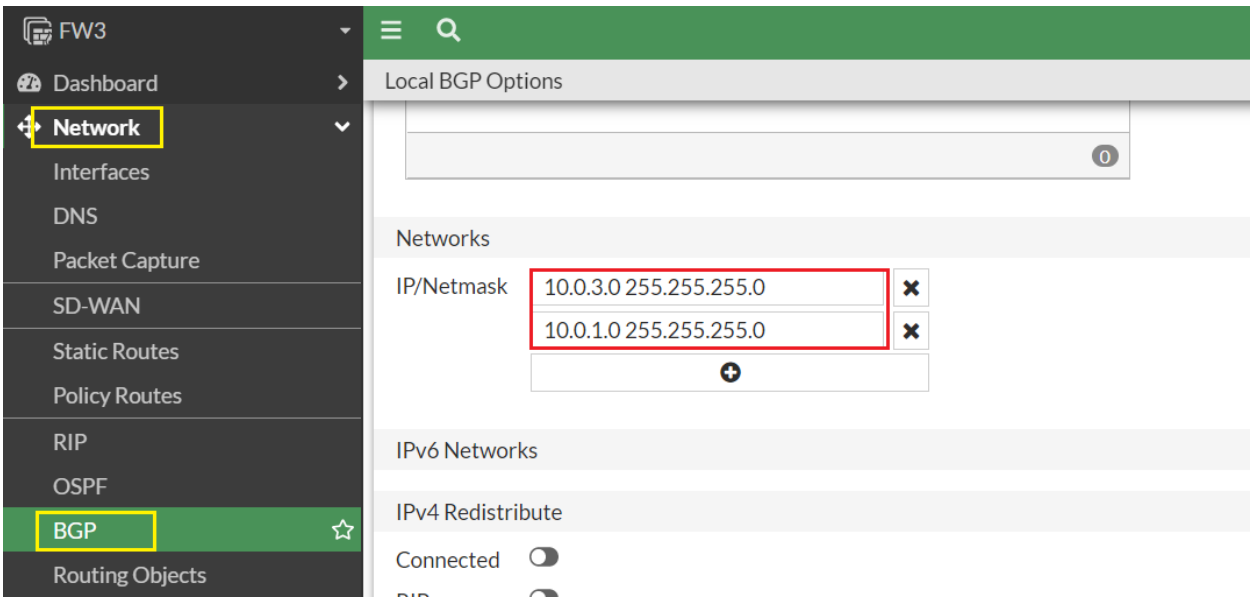




FW3 BGP Configuration:

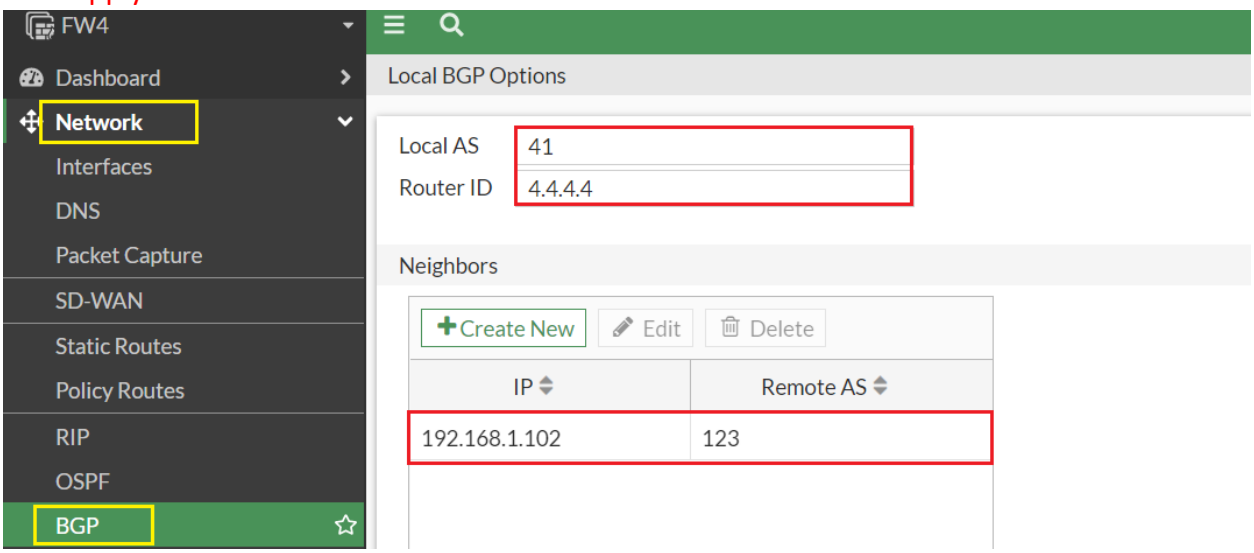
Go to Network > BGP Set the Local AS in this case 123. Set the Router ID 3.3.3.3. Configure the remote router's AS number, any other properties used for peering with the neighbor, under Networks, add two networks. Leave the remaining settings as their default values. Click OK. Click Apply.

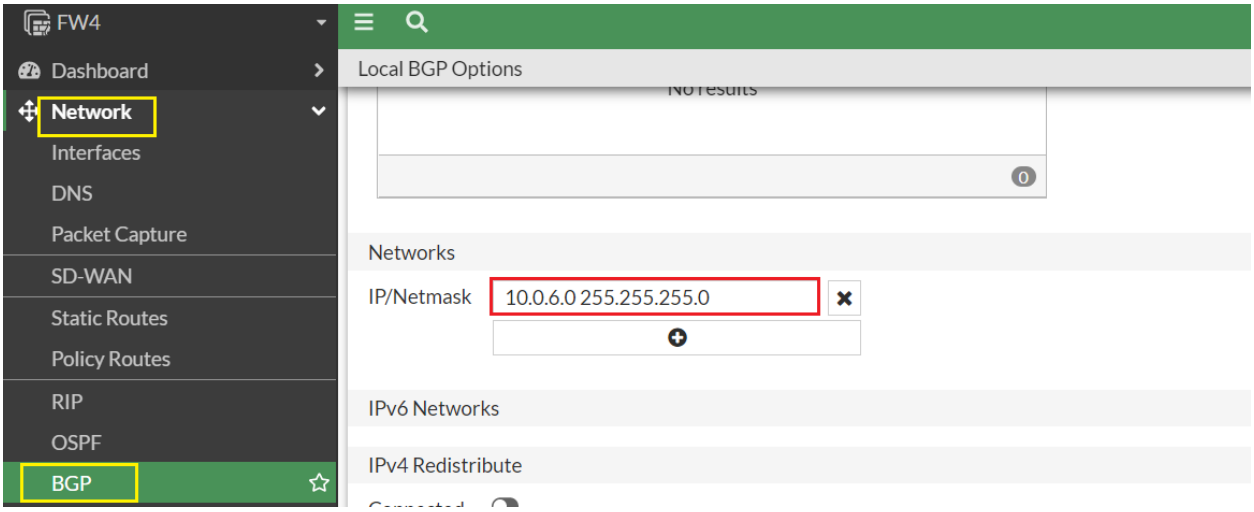




FW4 BGP Configuration:

Go to Network > BGP Set the Local AS in this case 41. Set the Router ID 4.4.4.4. Configure the remote router's AS number, any other properties used for peering with the neighbor, under Networks, add two networks. Leave the remaining settings as their default values. Click OK. Click Apply.

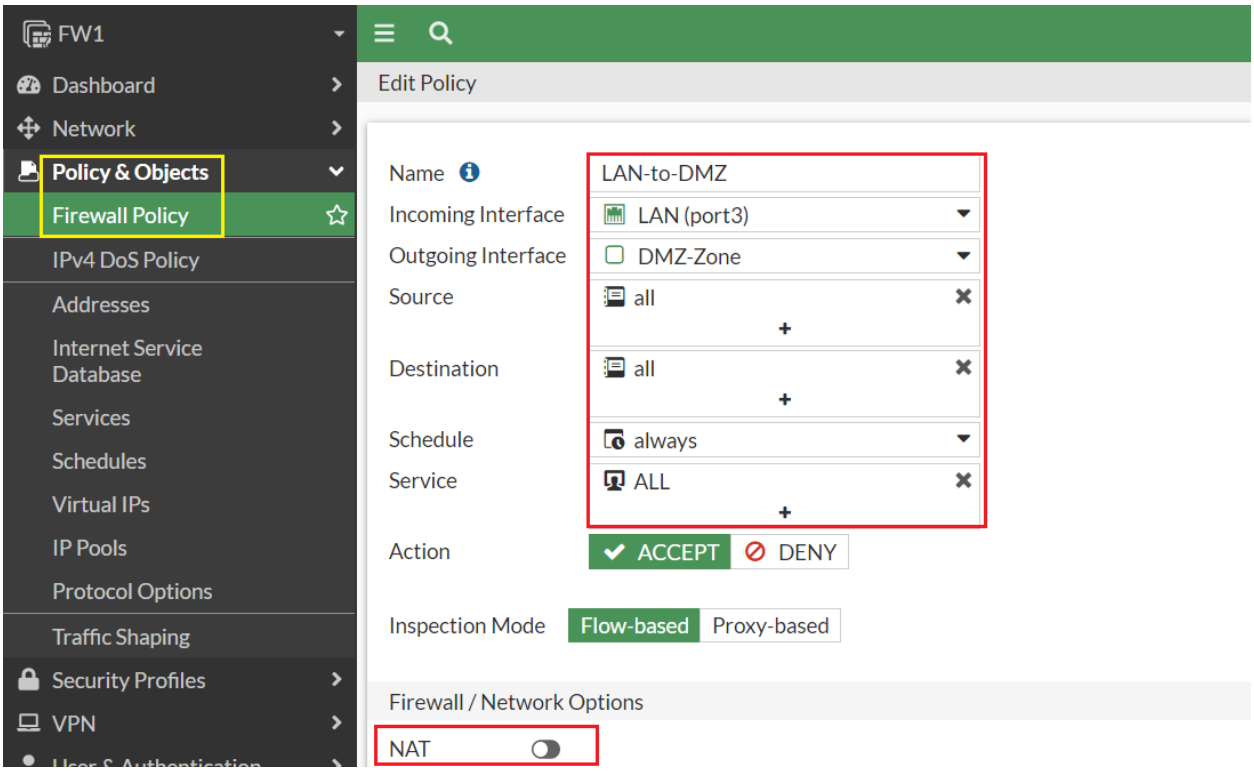


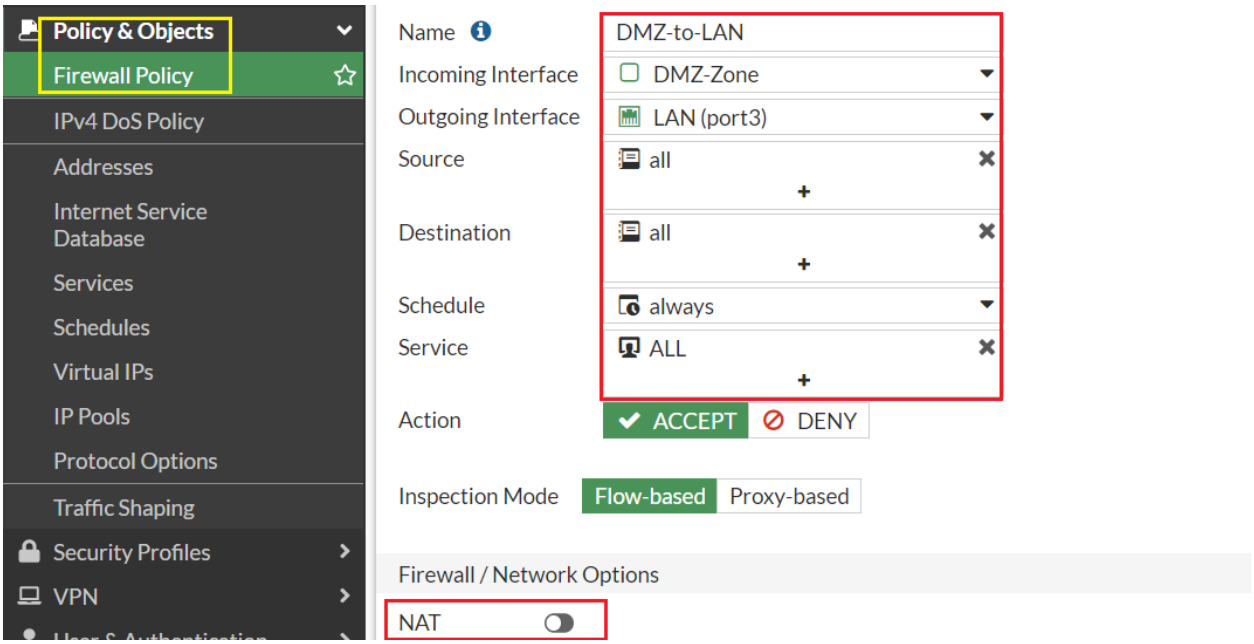


FW4 to FW1 change multihop for EBGP
config router bgp config neighbor edit "192.168.1.102" set ebgp-enforce-multihop enable set ebgp-multihop-ttl 255 end

FW1 Firewall Policy:

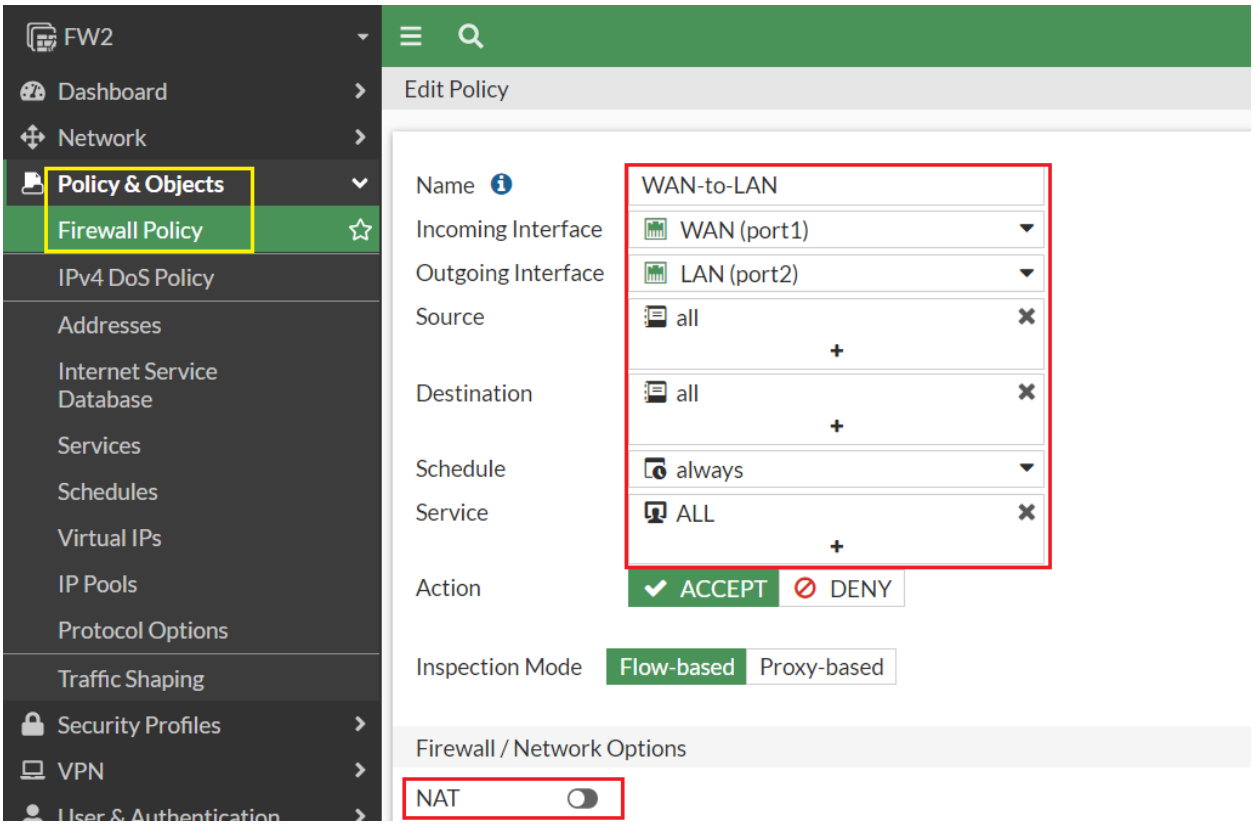
To create a new policy, go to Policy & Objects > Firewall Policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet in my case it is Allow-All. Set the Incoming Interface to LAN and the Outgoing Interface to DMZ-Zone. Set Source, Destination Address, Schedule, and Services, as required in this case All. Ensure the Action is set to ACCEPT. Turn off NAT and select Use Outgoing Interface Address.





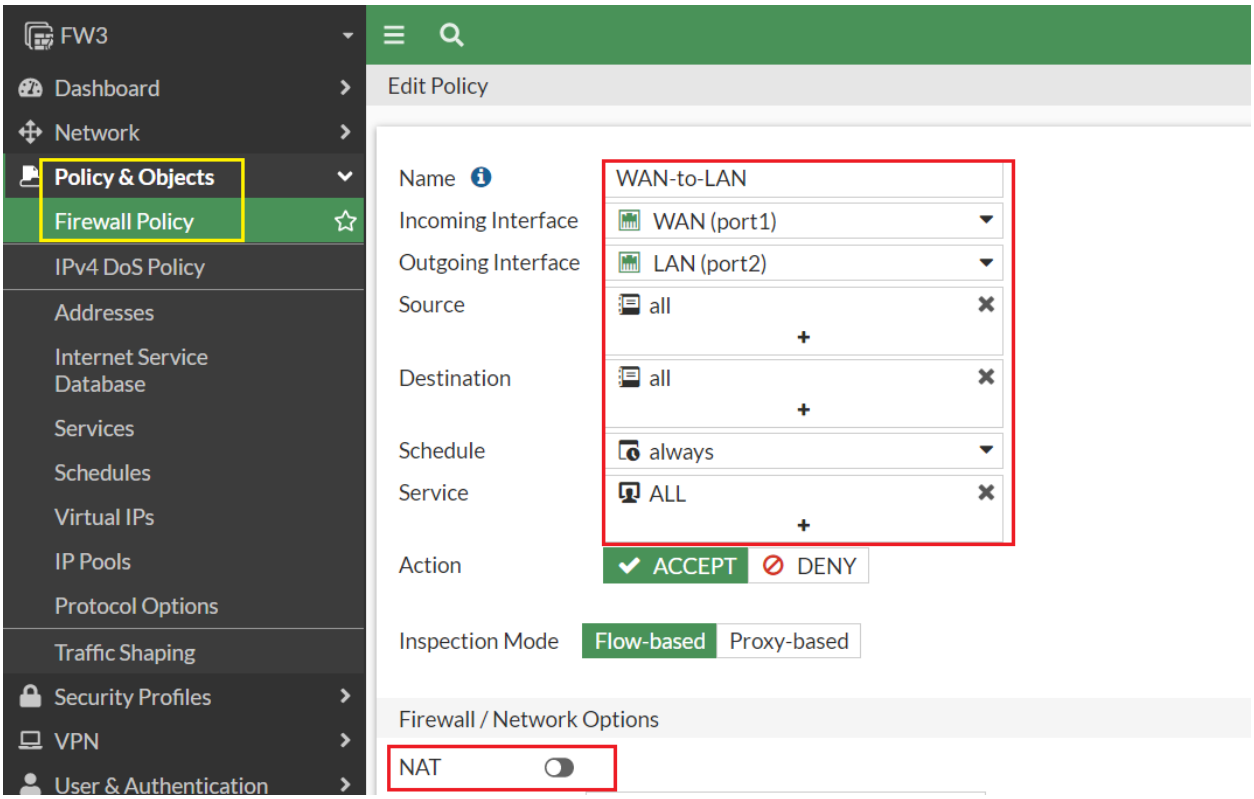
FW2 Firewall Policy:

To create a new policy, go to Policy & Objects > Firewall Policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet in my case it is Allow-All. Set the Incoming Interface to WAN and the Outgoing Interface to LAN. Set Source, Destination Address, Schedule, and Services, as required in this case All. Ensure the Action is set to ACCEPT.
Turn off NAT and select Use Outgoing Interface Address.



FW3 Firewall Policy:

To create a new policy, go to Policy & Objects > Firewall Policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet in my case it is Allow-All. Set the Incoming Interface to WAN and the Outgoing Interface to LAN. Set Source, Destination Address, Schedule, and Services, as required in this case All. Ensure the Action is set to ACCEPT.
Turn off NAT and select Use Outgoing Interface Address.



Testing and Verification:

Let's Check the routing table for BGP in FW1.

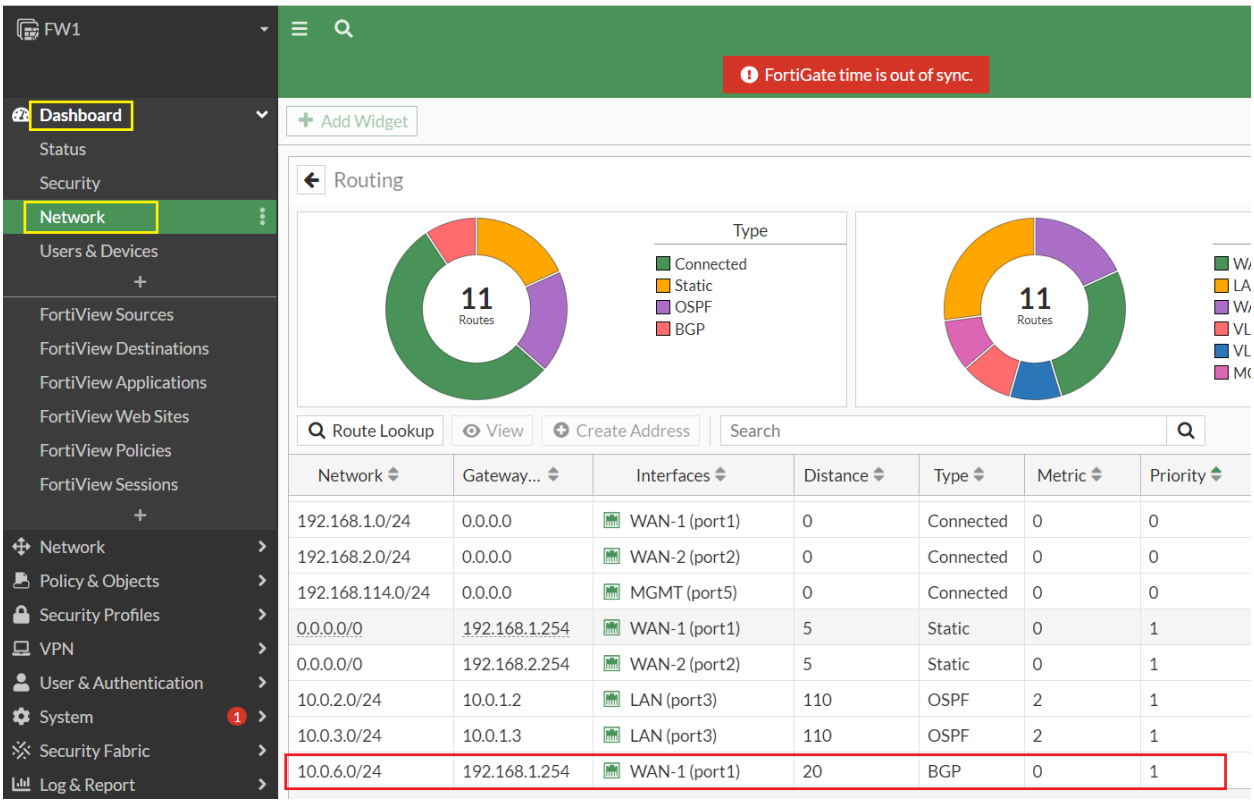
FW1

```
FW1 # get router info routing-table bgp
Routing table for VRF=0
B       10.0.6.0/24 [20/0] via 192.168.3.1 (recursive via 192.168.1.254, port1), 00:37:05
                                           (recursive via 192.168.2.254, port2), 00:37:05
```

FW1

```
FW1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 192.168.1.254, port1, [1/0]
                  [5/0] via 192.168.2.254, port2, [1/0]
C       10.0.1.0/24 is directly connected, port3
O       10.0.2.0/24 [110/2] via 10.0.1.2, port3, 01:34:06
O       10.0.3.0/24 [110/2] via 10.0.1.3, port3, 01:34:06
C       10.0.4.0/24 is directly connected, VLAN-40
C       10.0.5.0/24 is directly connected, VLAN-50
B       10.0.6.0/24 [20/0] via 192.168.3.1 (recursive via 192.168.1.254, port1), 00:37:29
                                           (recursive via 192.168.2.254, port2), 00:37:29
C       192.168.1.0/24 is directly connected, port1
C       192.168.2.0/24 is directly connected, port2
C       192.168.114.0/24 is directly connected, port5
```



Let’s Check the routing table for BGP in FW2.

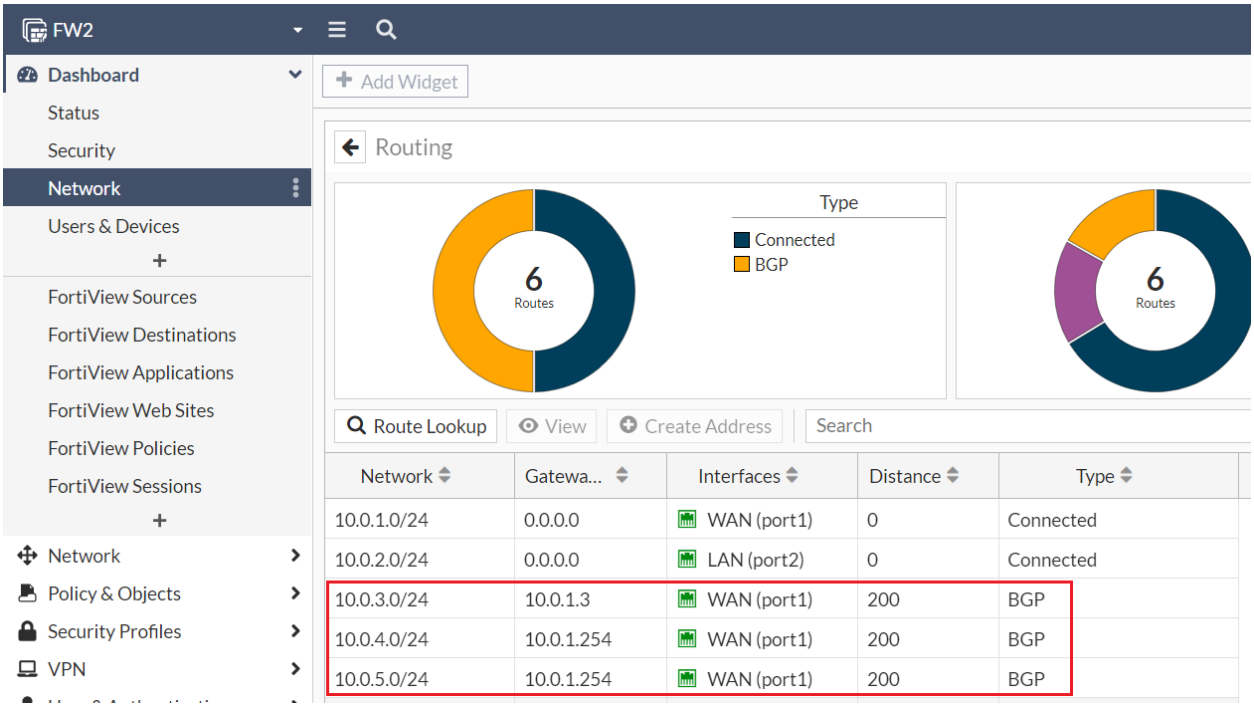
FW2

```
FW2 # get route info routing-table bgp
Routing table for VRF=0
B       10.0.3.0/24 [200/0] via 10.0.1.3 (recursive is directly connected, port1), 00:50:50
B       10.0.4.0/24 [200/0] via 10.0.1.254 (recursive is directly connected, port1), 00:52:42
B       10.0.5.0/24 [200/0] via 10.0.1.254 (recursive is directly connected, port1), 00:52:42
```

FW2

```
FW2 # get route info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
C       10.0.1.0/24 is directly connected, port1
C       10.0.2.0/24 is directly connected, port2
B       10.0.3.0/24 [200/0] via 10.0.1.3 (recursive is directly connected, port1), 00:52:03
B       10.0.4.0/24 [200/0] via 10.0.1.254 (recursive is directly connected, port1), 00:53:55
B       10.0.5.0/24 [200/0] via 10.0.1.254 (recursive is directly connected, port1), 00:53:55
C       192.168.114.0/24 is directly connected, port5
```



Let’s Check the routing table for OSPF in FW3.

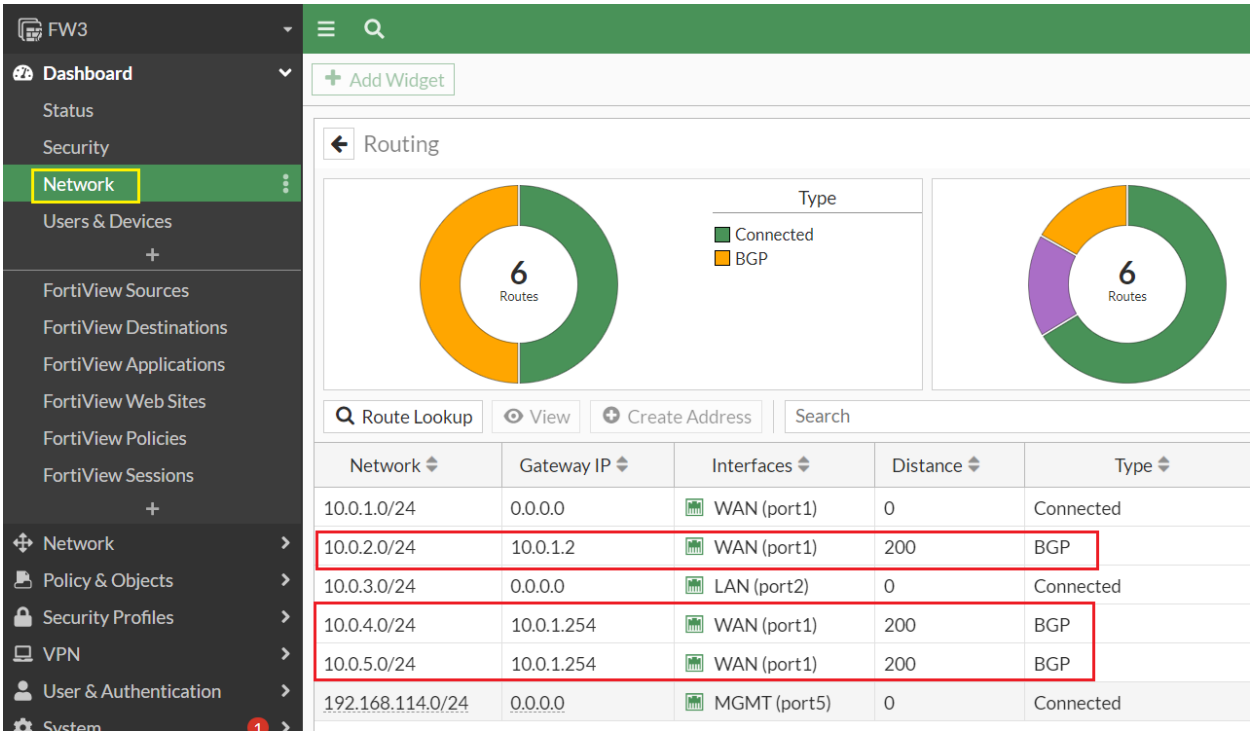
FW3

```
FW3 #
FW3 # get router info routing-table bgp
Routing table for VRF=0
B       10.0.2.0/24 [200/0] via 10.0.1.2 (recursive is directly connected, port1), 00:53:08
B       10.0.4.0/24 [200/0] via 10.0.1.254 (recursive is directly connected, port1), 00:53:09
B       10.0.5.0/24 [200/0] via 10.0.1.254 (recursive is directly connected, port1), 00:53:09
```

FW3

```
FW3 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
C       10.0.1.0/24 is directly connected, port1
B       10.0.2.0/24 [200/0] via 10.0.1.2 (recursive is directly connected, port1), 00:53:35
C       10.0.3.0/24 is directly connected, port2
B       10.0.4.0/24 [200/0] via 10.0.1.254 (recursive is directly connected, port1), 00:53:36
B       10.0.5.0/24 [200/0] via 10.0.1.254 (recursive is directly connected, port1), 00:53:36
C       192.168.114.0/24 is directly connected, port5
```



Let's Check the routing table for BGP in FW4.

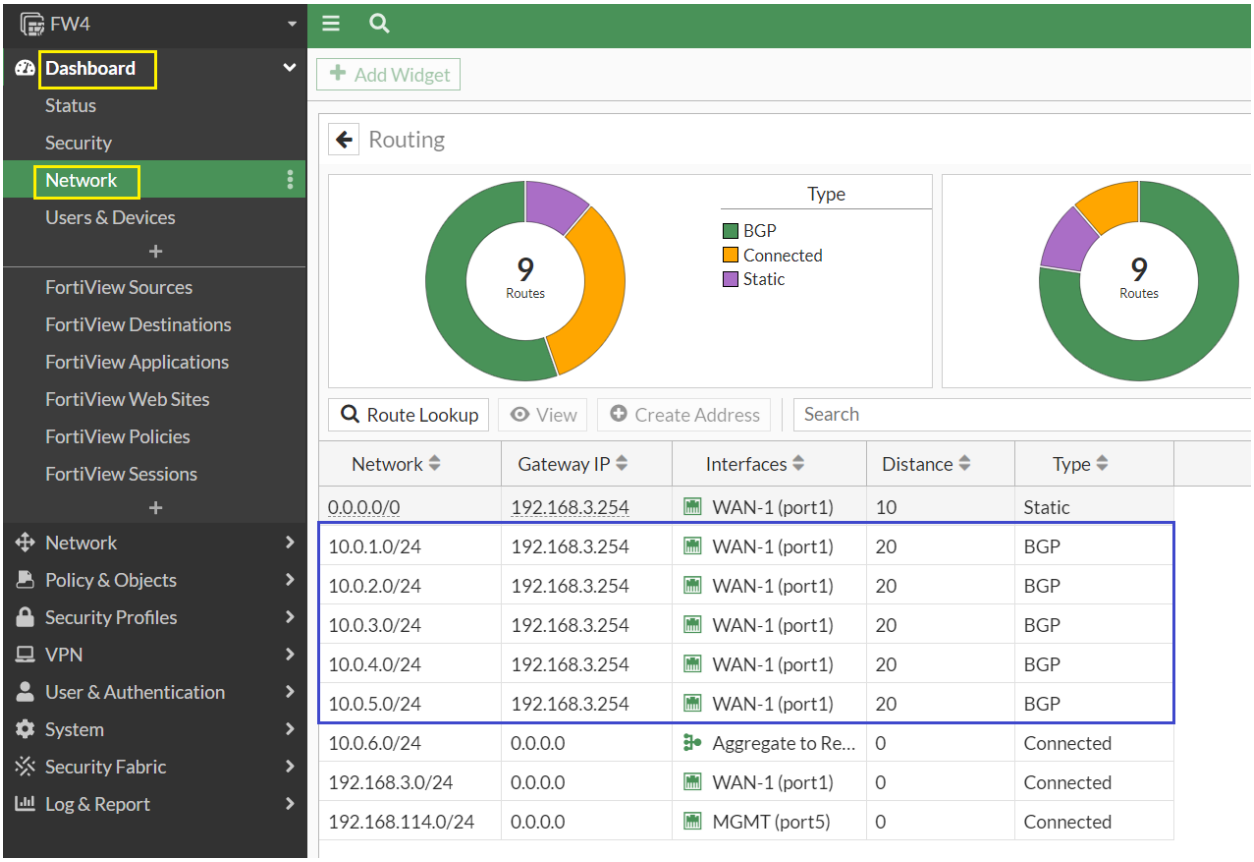
```
FW4

FW4 # get router info routing-table bgp
Routing table for VRF=0
B       10.0.1.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:28:28
B       10.0.2.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:28:28
B       10.0.3.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:28:28
B       10.0.4.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:28:28
B       10.0.5.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:28:28
```

```
FW4

FW4 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 192.168.3.254, port1, [1/0]
B       10.0.1.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:29:11
B       10.0.2.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:29:11
B       10.0.3.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:29:11
B       10.0.4.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:29:11
B       10.0.5.0/24 [20/0] via 192.168.1.102 (recursive via 192.168.3.254, port1), 00:29:11
C       10.0.6.0/24 is directly connected, AG-1
C       192.168.3.0/24 is directly connected, port1
C       192.168.114.0/24 is directly connected, port5
```



Commands
get router info routing-table all
show router bgp
get router info bgp summary
get router info bgp network
get router info routing-table bgp
get router info bgp neighbors
get router info bgp neighbors 192.168.3.1 advertised-routes
get router info bgp neighbors routes
get router info bgp neighbors 192.168.3.1 received-routes
diagnose sys tcpsock | grep 179
diagnose ip router bgp level info
diagnose ip router bgp all enable
exec router clear bgp all

Try to ping from PC1, PC2 and PC3 to each other even you can ping DMZ SRV1 and SRV2 if the firewall policy is properly configured it will work through BGP protocols.