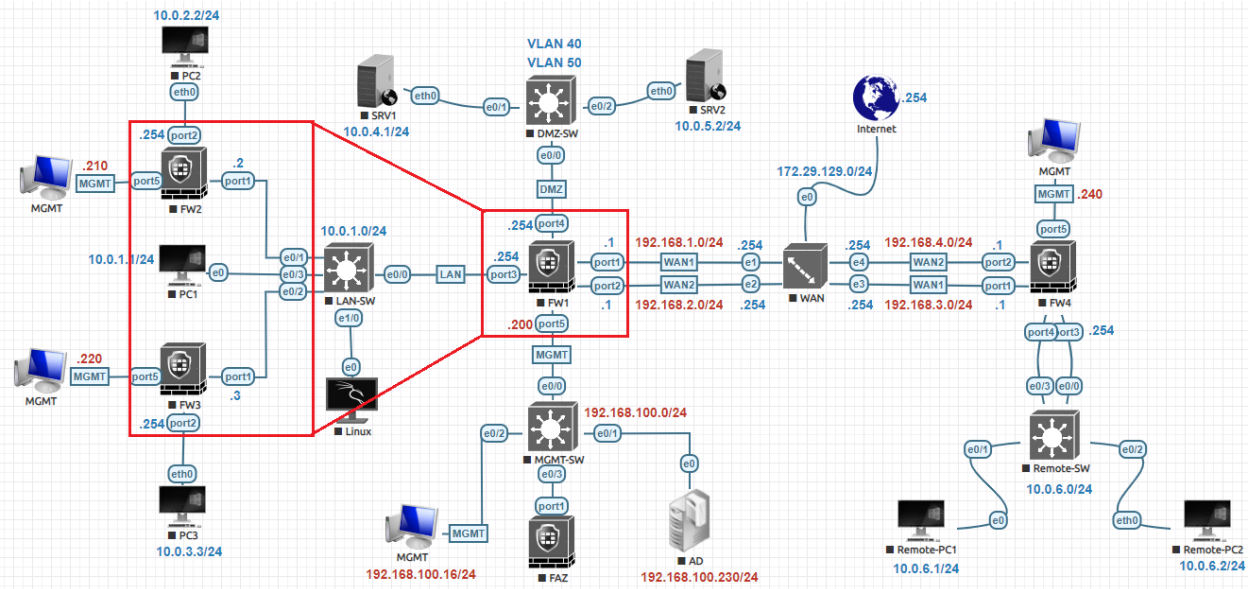
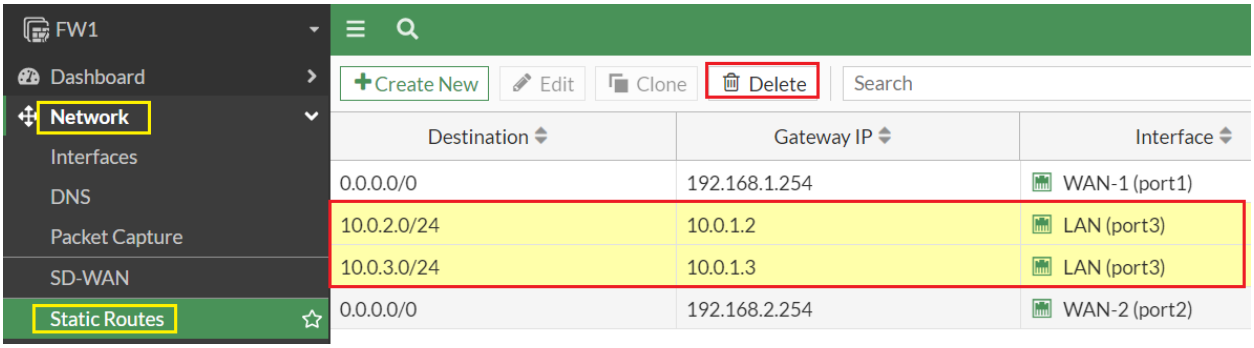
Dynamic Protocol OSPF Lab:

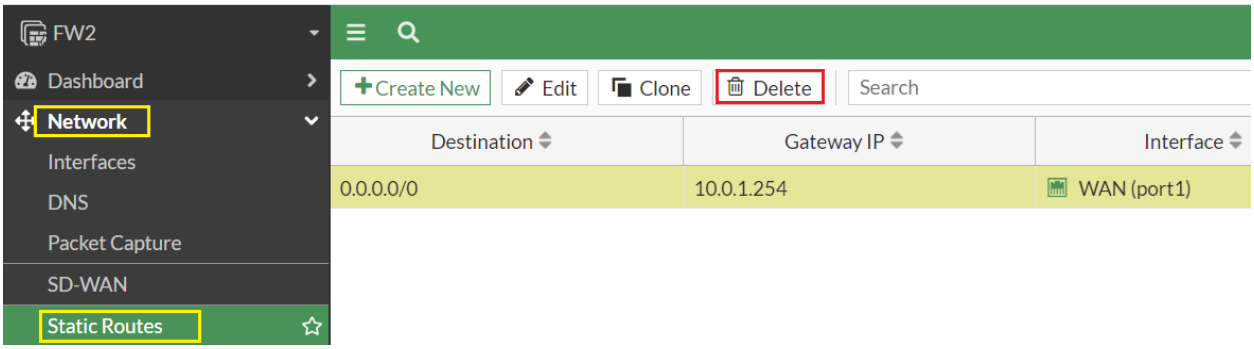


Two Core Firewall, FW2 and FW3, connect to the ISP Firewall FW1 for the internet access. Both FW2 and FW3 have different Local Networks. The ISP Firewall FW1 is using OSPF for its connections to the core Firewalls, and redistributes its default route to the network - that is, default route injection 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.

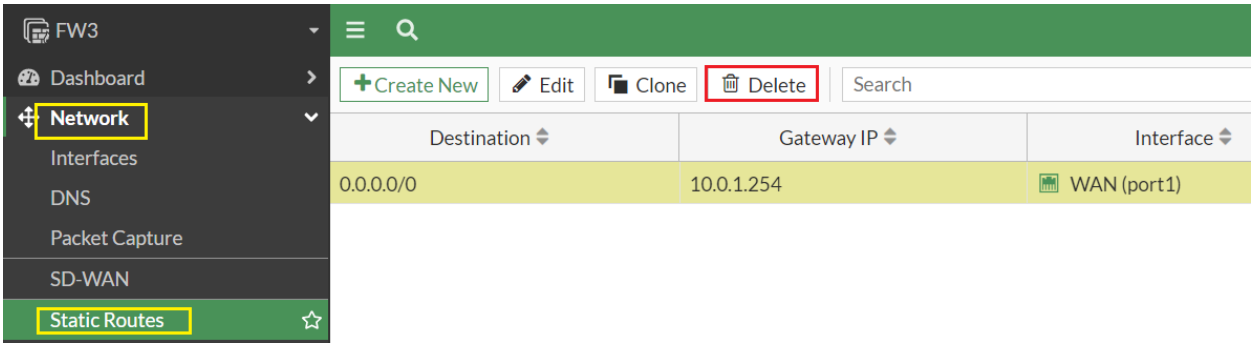
Disable or Deleted Default/Static Routes:

First we need to delete are disable default and static routes configured from previous lab.



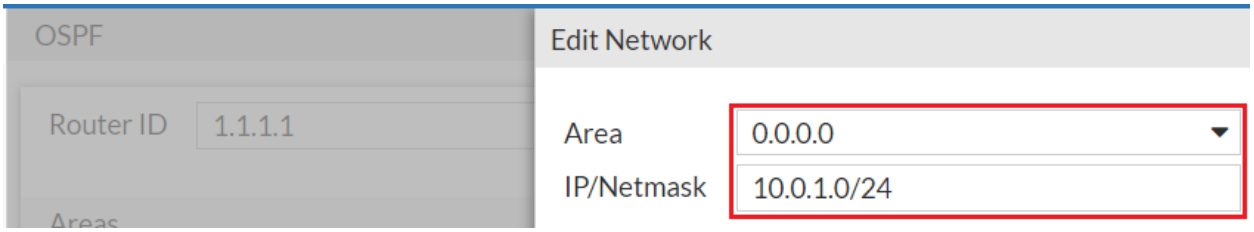


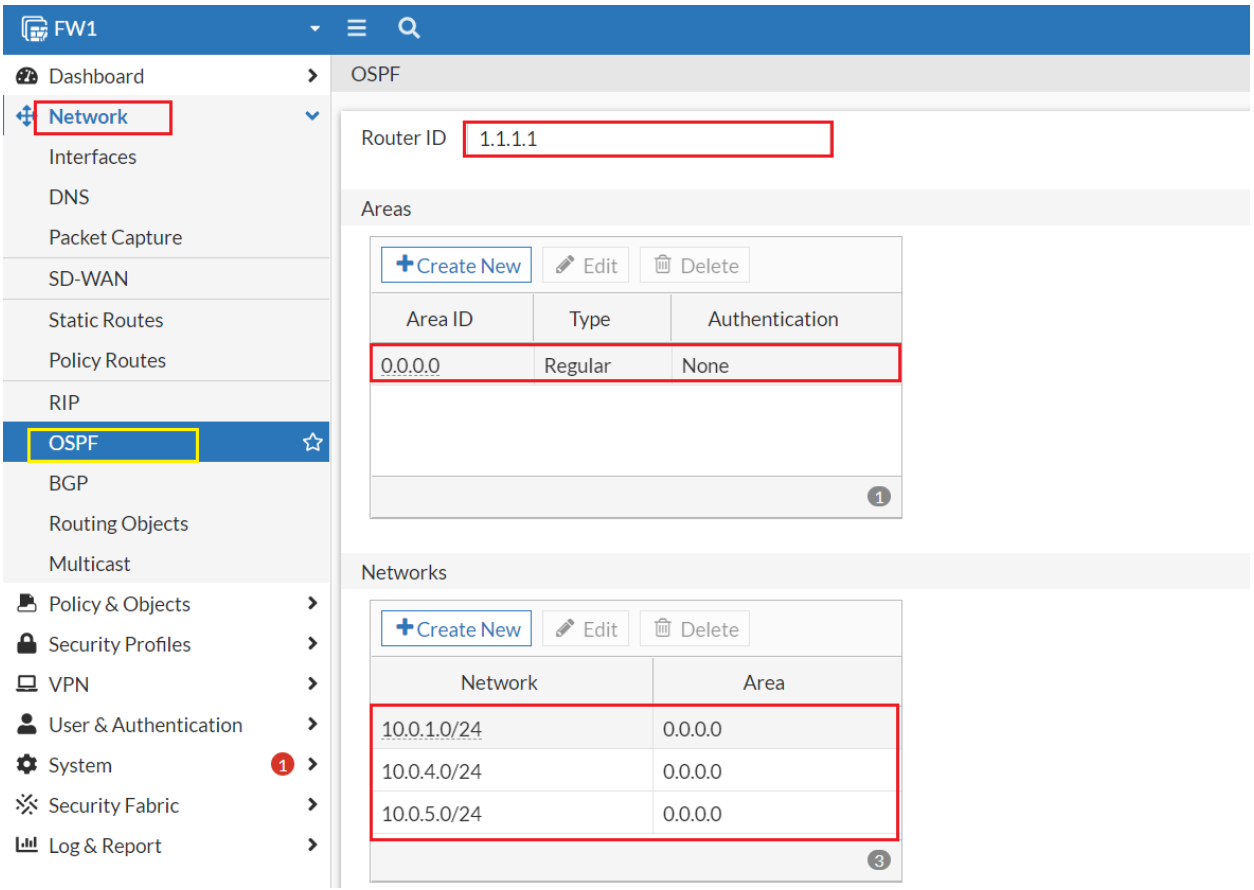
 Created by Ahmad Ali E-Mail: ahmadalimsc@gmail.com , WhatsApp: 00966564303717



FW1 OSPF Configuration:

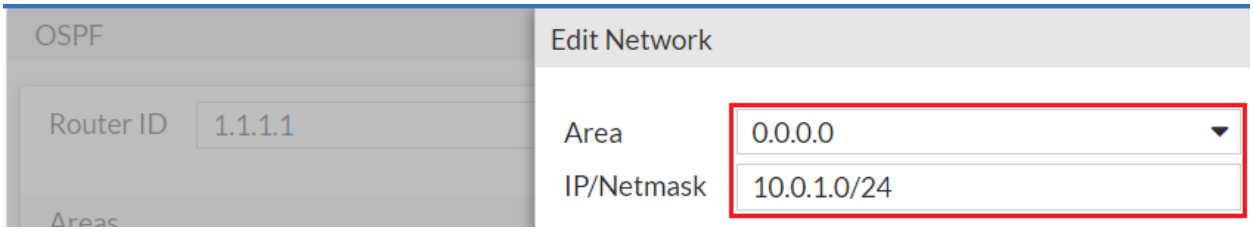
Go to Network > OSPF Set the Router ID 1.1.1.1. Set the Areas to 0.0.0.0. Under Networks, add three networks. In the Interfaces table, click Create New. Leave the remaining settings as their default values. Click OK. Click Apply.

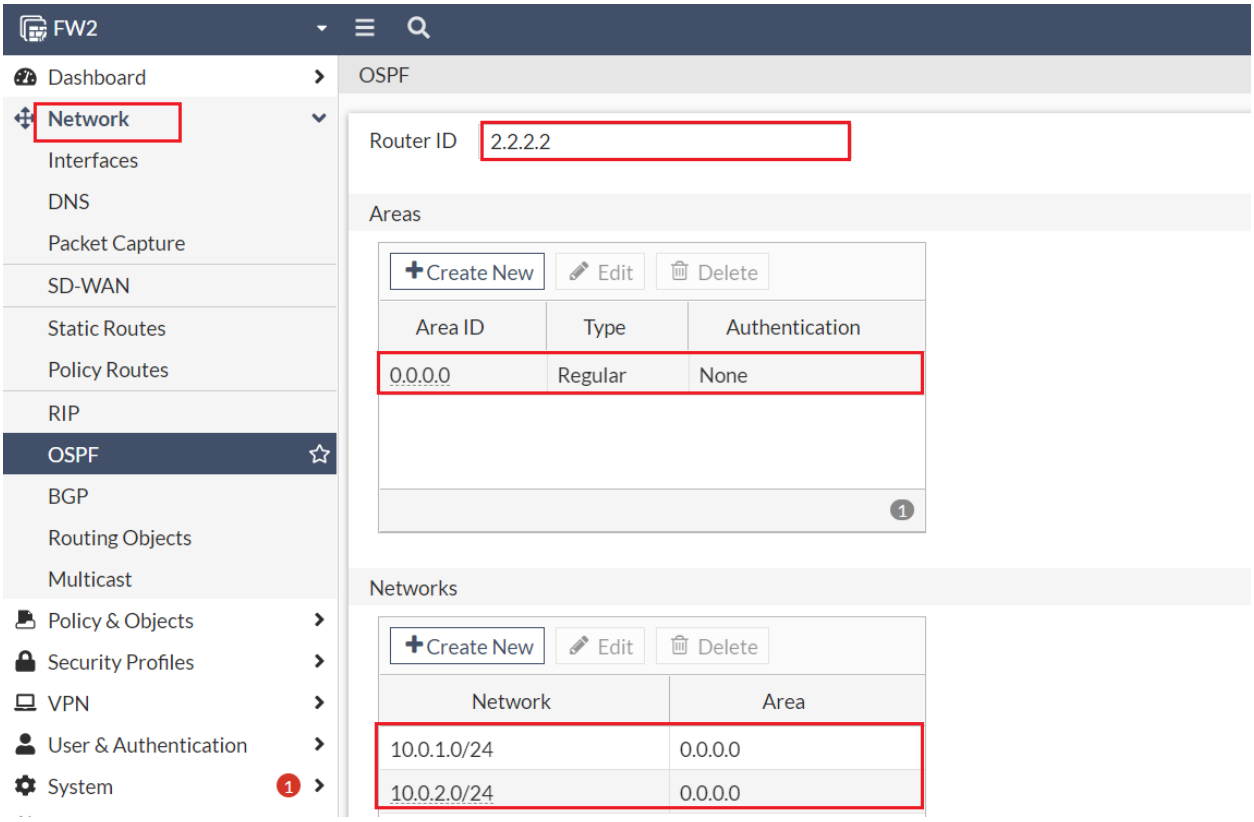




FW2 OSPF Configuration:

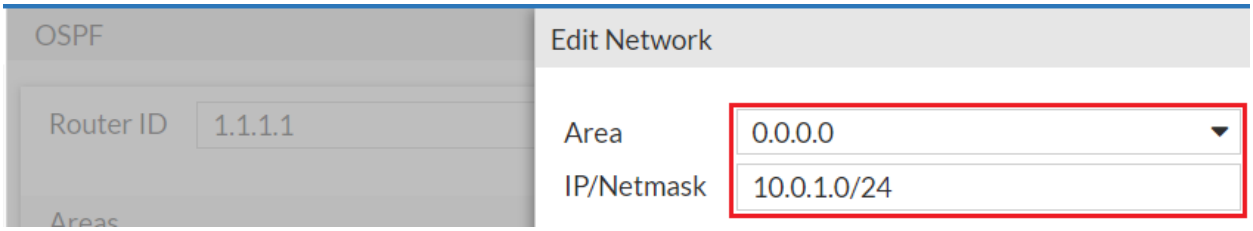
Go to Network > OSPF Set the Router ID to 2.2.2.2. Set the Areas to 0.0.0.0. Under Networks, add two networks. In the Interfaces table, click Create New. Leave the remaining settings as their default values. Click OK. Click Apply.

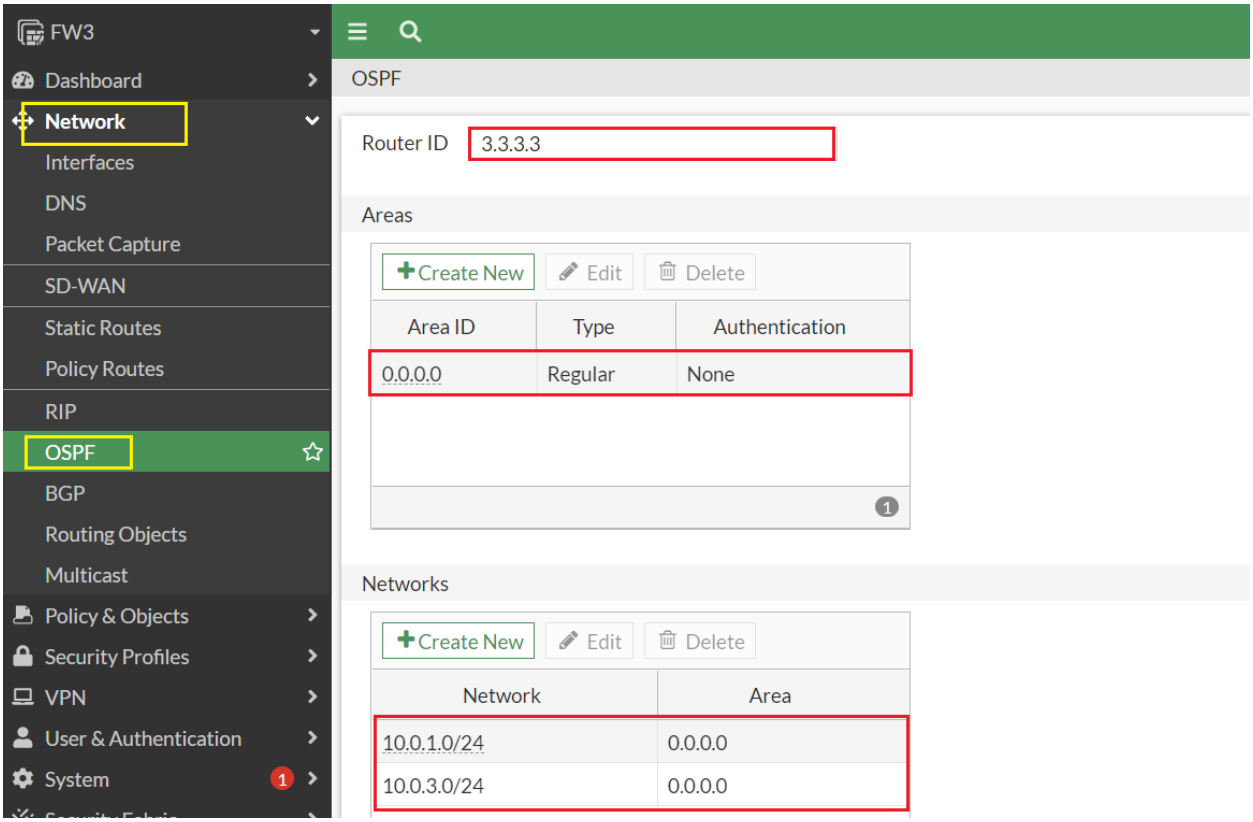




FW3 OSPF Configuration:

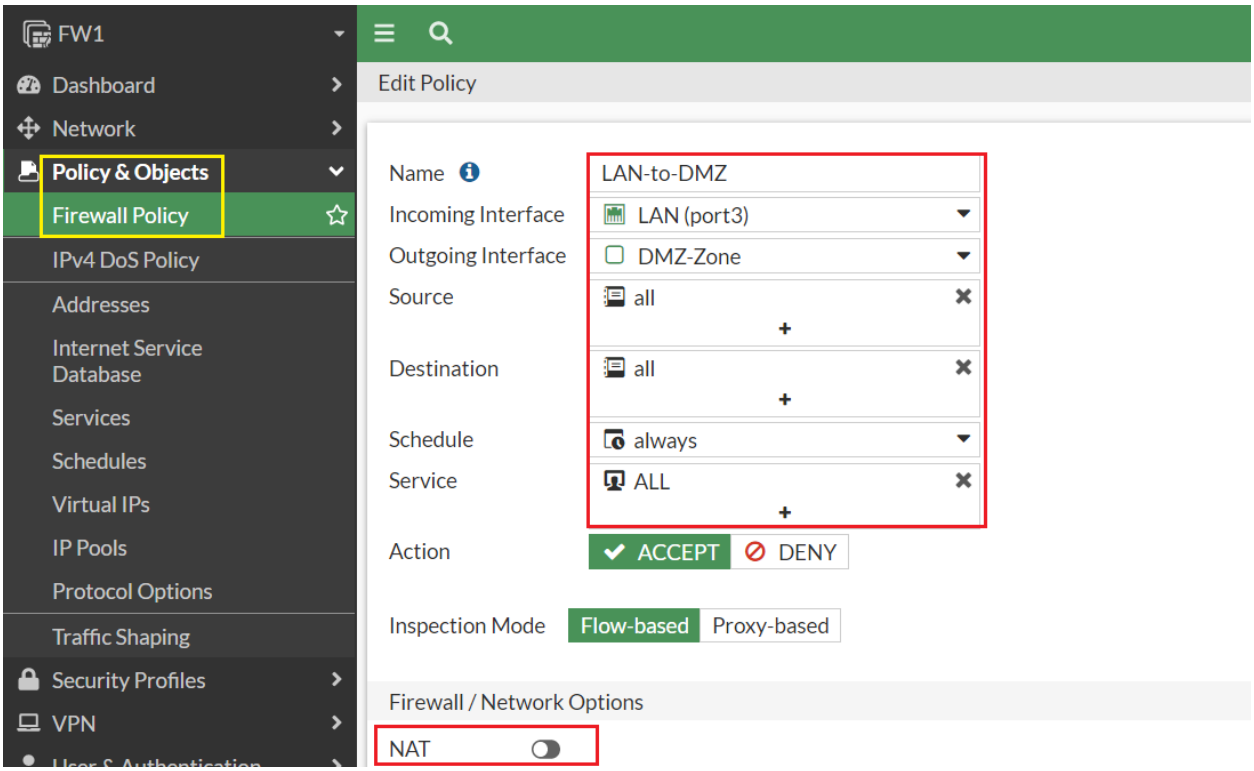
Go to Network > OSPF Set the Router ID 3.3.3.3. Set the Areas to 0.0.0.0. Under Networks, add two networks. In the Interfaces table, click Create New. Leave the remaining settings as their default values. Click OK. Click Apply.

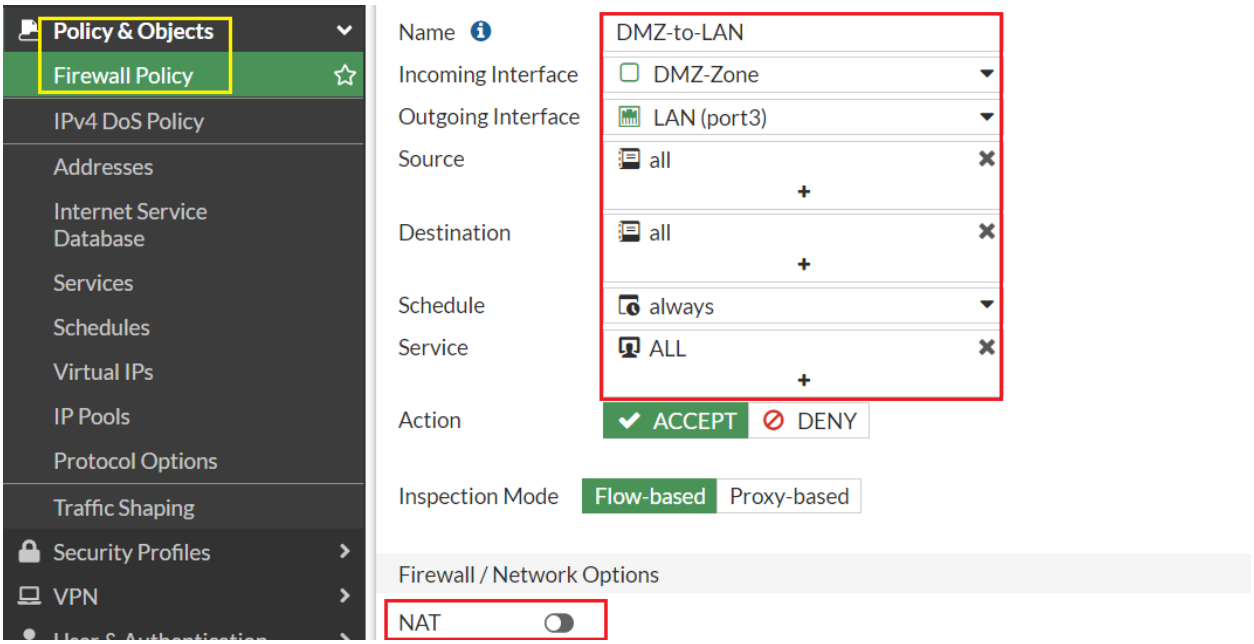




FW1 Firewall Policy:

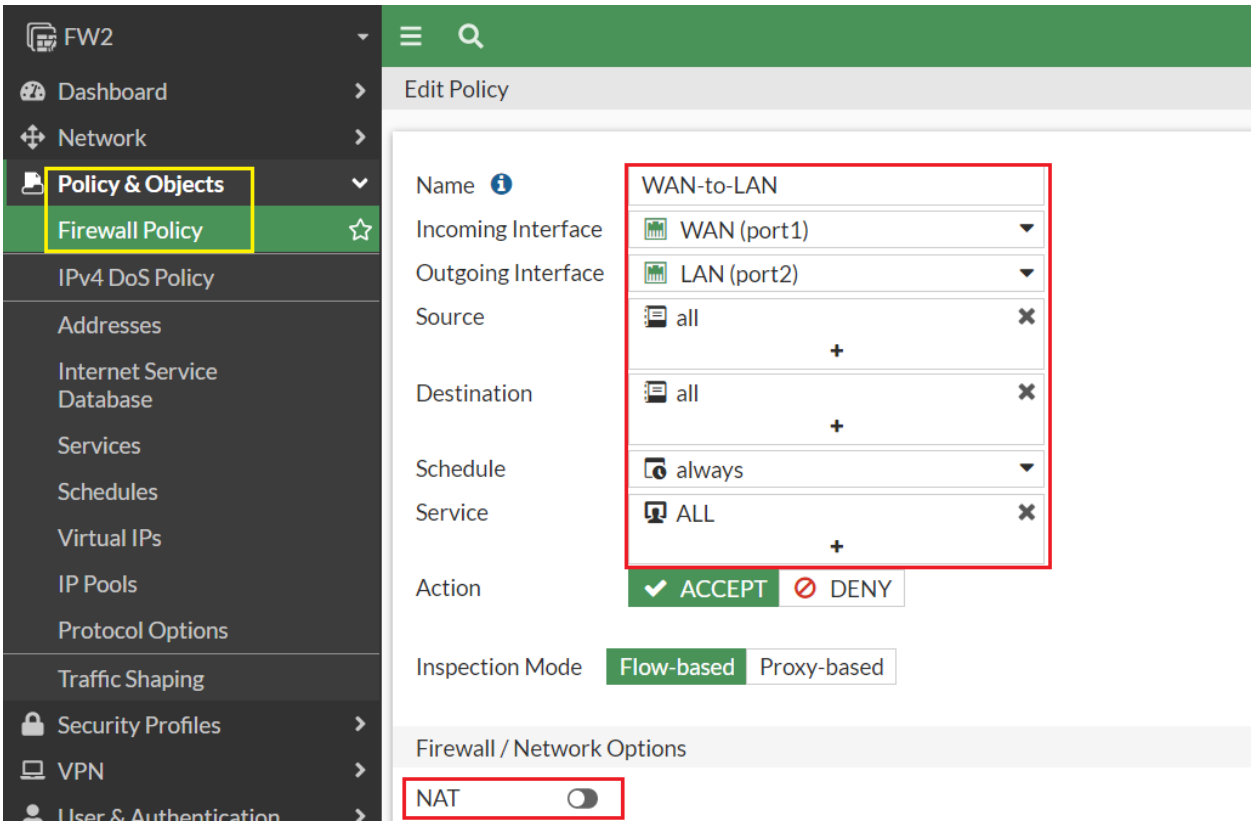
To create a new policy, go to Policy & Objects > Firewall Policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet in my case it is Allow-All. Set the Incoming Interface to LAN and the Outgoing Interface to DMZ-Zone. Set Source, Destination Address, Schedule,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





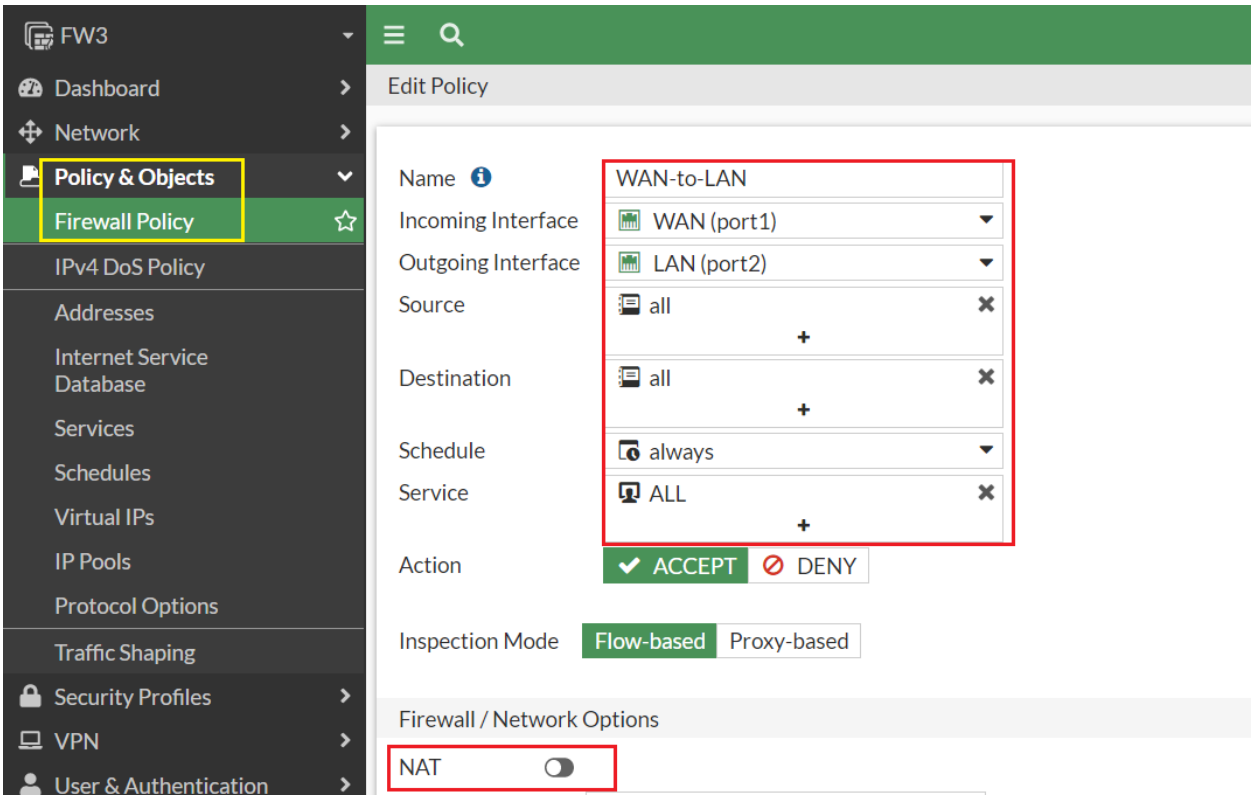
FW2 Firewall Policy:

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:

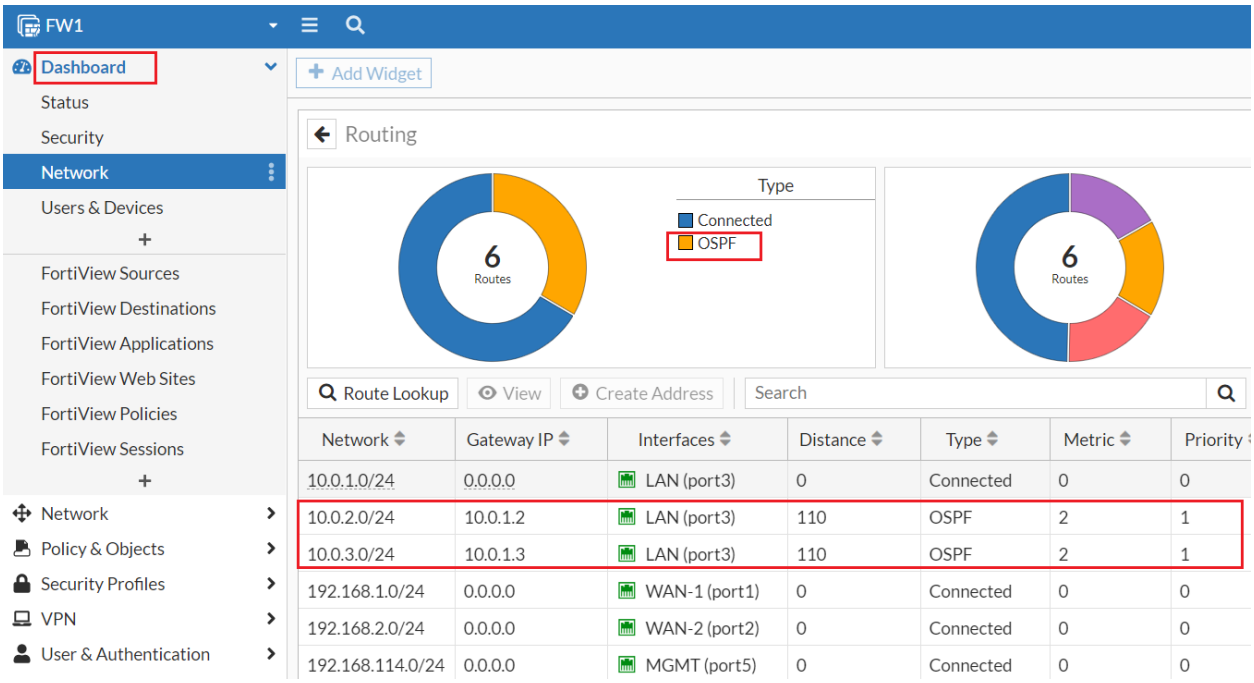
To create a new policy, go to Policy & Objects > Firewall Policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet in my case it is Allow-All. Set the Incoming Interface to WAN and the Outgoing Interface to LAN. Set Source, Destination Address, Schedule, and Services, 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 OSPF in FW1.

```
FW1
FW1 #
FW1 # get router info routing-table ospf
Routing table for VRF=0
O       10.0.2.0/24 [110/2] via 10.0.1.2, port3, 00:03:55
O       10.0.3.0/24 [110/2] via 10.0.1.3, port3, 00:01:39
```

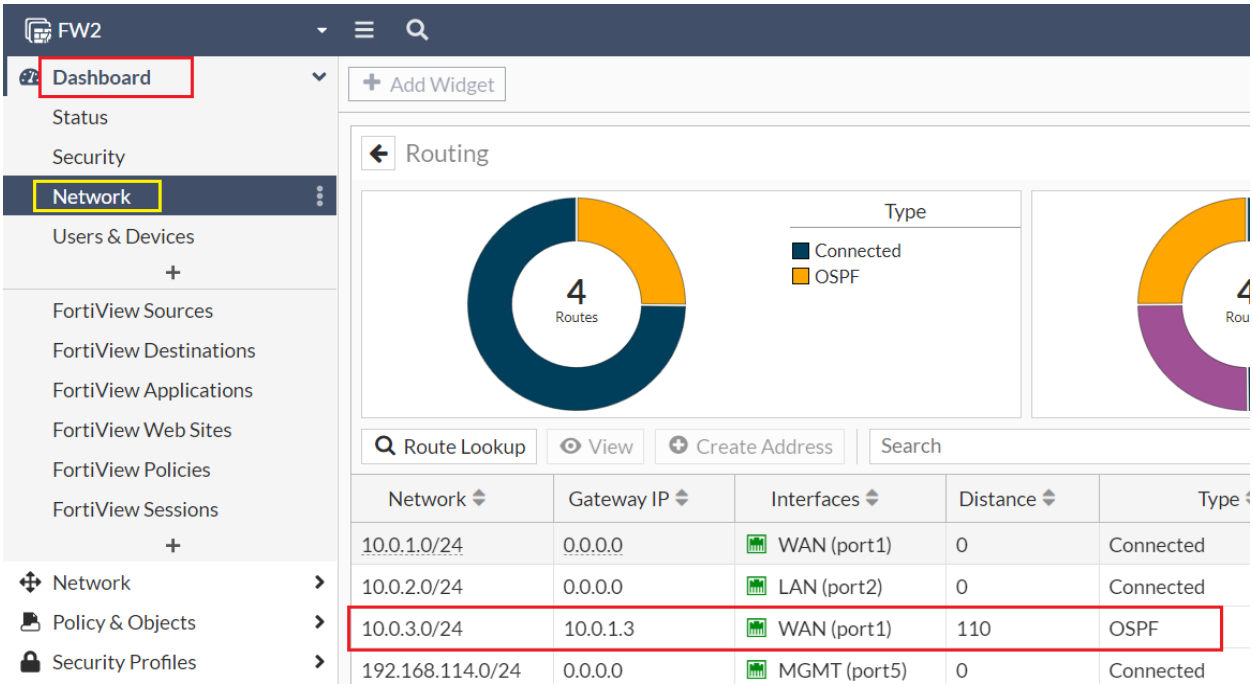


Let's Check the routing table for OSPF in FW2.

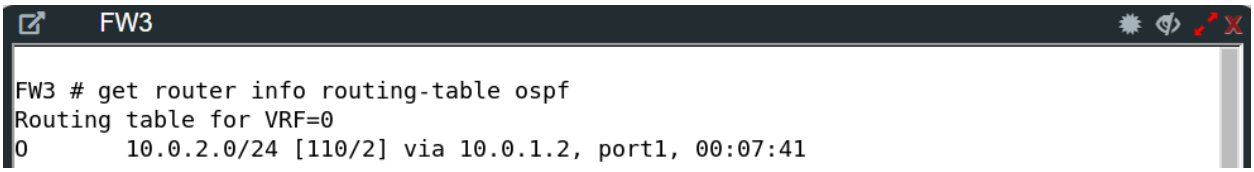
```
FW2
FW2 # get router  info routing-table ospf
Routing table for VRF=0
O       10.0.3.0/24 [110/2] via 10.0.1.3, port1, 00:04:22
```

```
FW2
FW2 #
FW2 # 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
C       10.0.2.0/24 is directly connected, port2
O       10.0.3.0/24 [110/2] via 10.0.1.3, port1, 00:04:52
C       192.168.114.0/24 is directly connected, port5
```



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



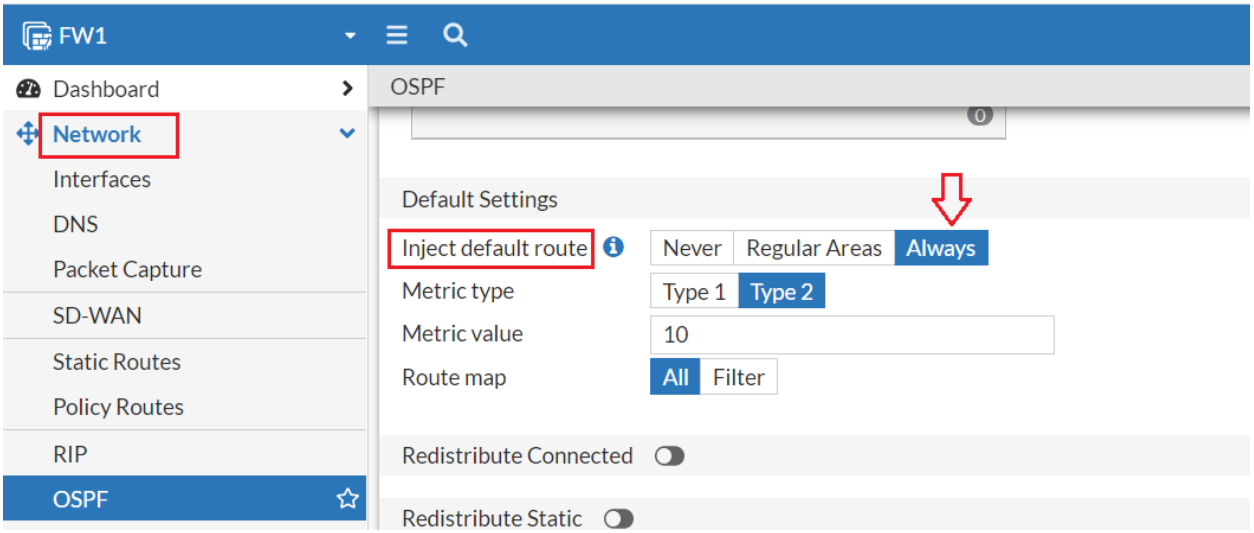
Network	Gateway IP	Interfaces	Dista...	Type
10.0.1.0/24	0.0.0.0	WAN (port1)	0	Connected
10.0.2.0/24	10.0.1.2	WAN (port1)	110	OSPF
10.0.3.0/24	0.0.0.0	LAN (port2)	0	Connected
192.168.114.0/24	0.0.0.0	MGMT (port5)	0	Connected

Commands
get router info routing-table all
get router info ospf interface
get router ospf

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 OSPF protocols.

Inject Default Route:

If you want that all the LAN Networks behinds FW2 and FW3 to reach to Internet, you need to enable Default Route injection in FW1. Under Default Settings, enable Inject Default Route. This setting allows the ISP FW1 to share its default 0.0.0.0 routes with other Firewalls FW2 and FW3 in the RIP network. Click Apply.



Try to ping and browse from PC1, PC2, PC3, SRV1 and SRV2 to any interment website if the firewall policy is properly configured it will work through OSPF Default Route.

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.0.1.254	WAN (port1)	110	OSPF (External type 2)
10.0.1.0/24	0.0.0.0	WAN (port1)	0	Connected
10.0.2.0/24	0.0.0.0	LAN (port2)	0	Connected
10.0.3.0/24	10.0.1.3	WAN (port1)	110	OSPF
192.168.114.0/24	0.0.0.0	MGMT (port5)	0	Connected

Network	Gateway ...	Interfaces	Distance	Type
0.0.0.0/0	10.0.1.254	WAN (port1)	110	OSPF (External type 2)
10.0.1.0/24	0.0.0.0	WAN (port1)	0	Connected
10.0.2.0/24	10.0.1.2	WAN (port1)	110	OSPF
10.0.3.0/24	0.0.0.0	LAN (port2)	0	Connected
192.168.114.0/24	0.0.0.0	MGMT (port5)	0	Connected