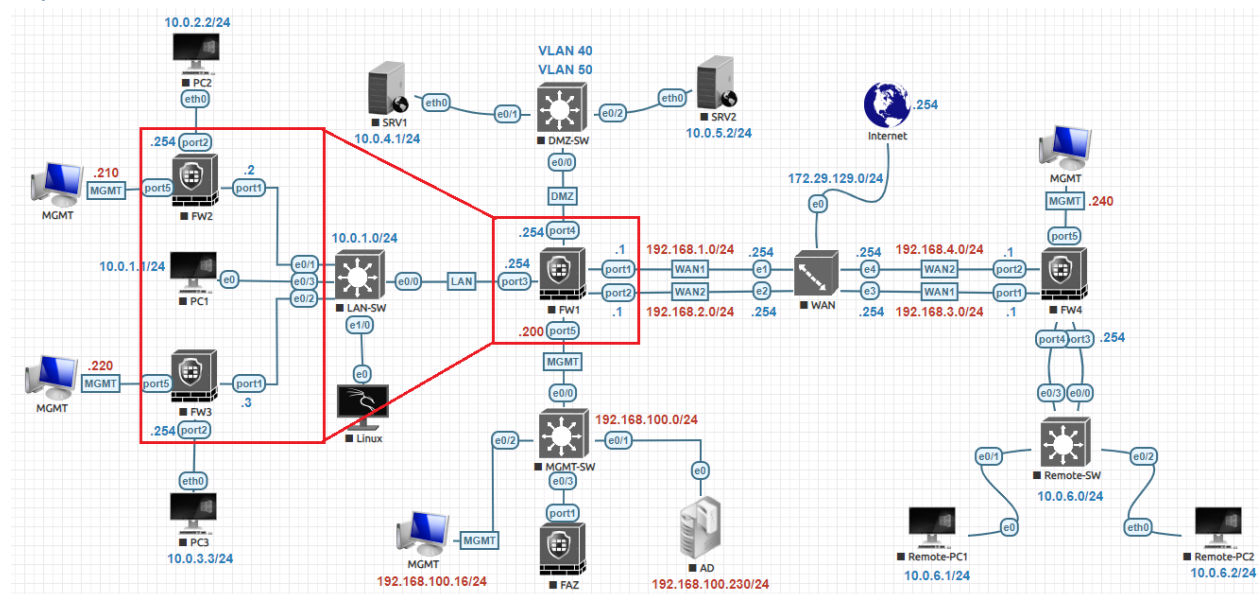


Dynamic Protocol OSPF Lab:



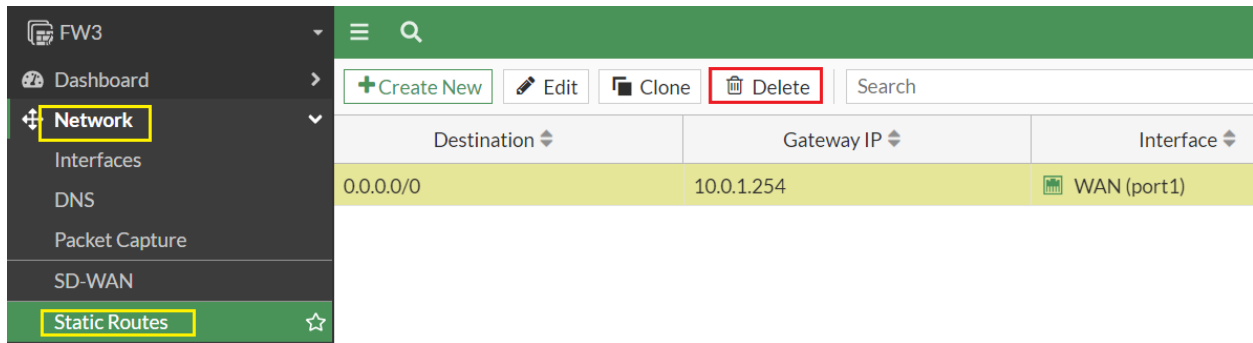
Two Core Firewall, FW2 and FW3, connect to the ISP Firewall FW1 for the internet access. Both FW2 and FW3 have different Local Networks. The ISP Firewall FW1 is using OSPF for its connections to the core Firewalls, and redistributes its default route to the network - that is, default route injection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

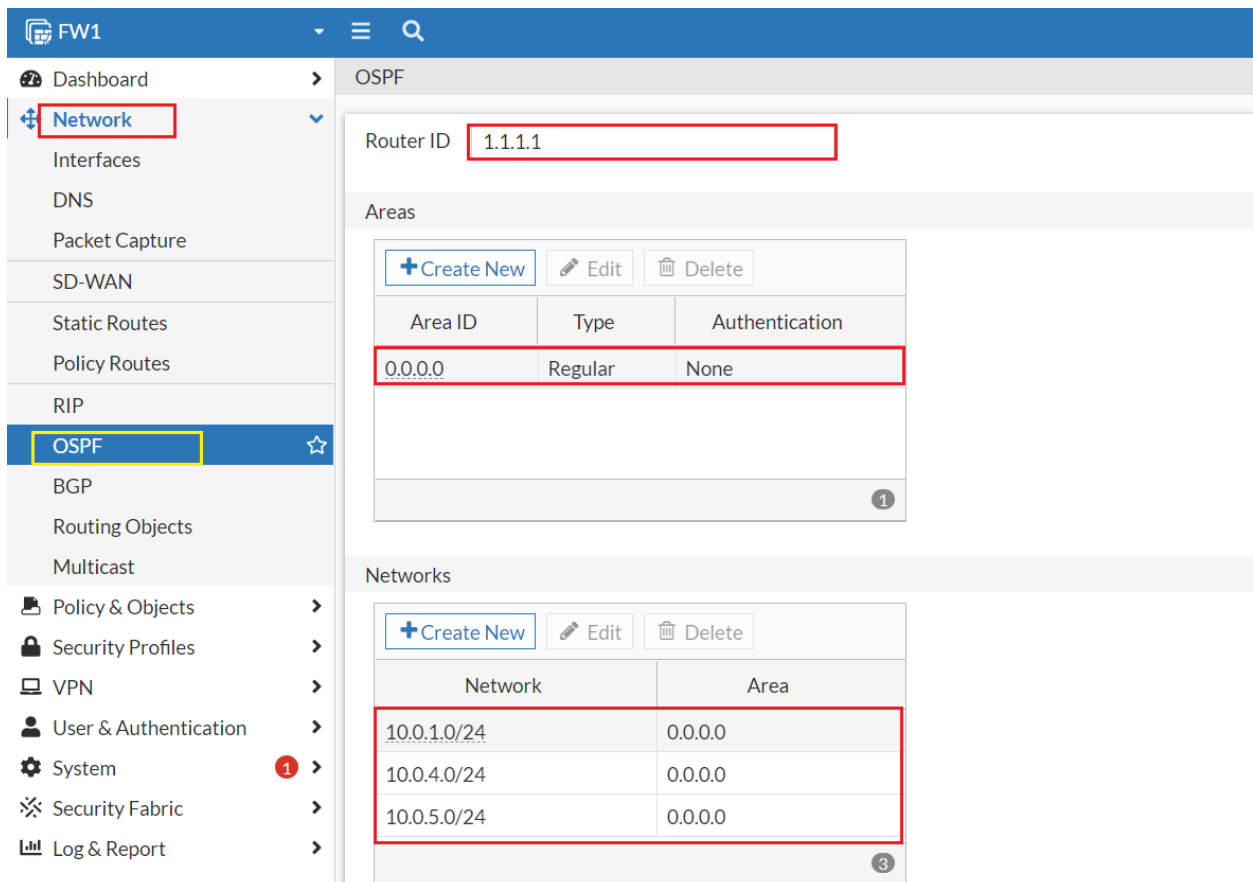
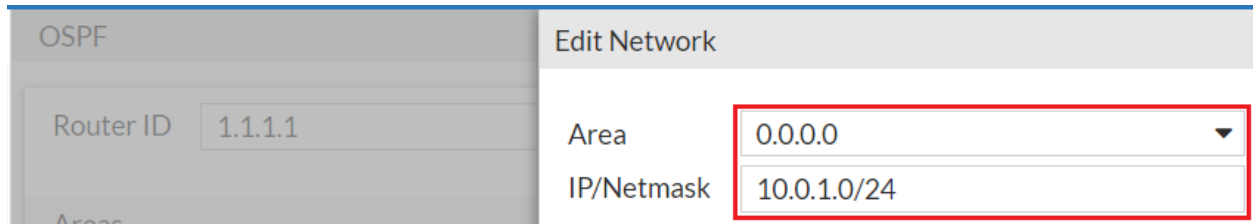
FW1	Destination	Gateway IP	Interface
	0.0.0.0/0	192.168.1.254	WAN-1 (port1)
	10.0.2.0/24	10.0.1.2	LAN (port3)
	10.0.3.0/24	10.0.1.3	LAN (port3)
	0.0.0.0/0	192.168.2.254	WAN-2 (port2)

FW2	Destination	Gateway IP	Interface
	0.0.0.0/0	10.0.1.254	WAN (port1)



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**.

OSPF

Router ID 1.1.1.1

Area

Area 0.0.0.0

IP/Netmask 10.0.1.0/24

FW2

Dashboard > OSPF

Network > Interfaces > DNS > Packet Capture > SD-WAN > Static Routes > Policy Routes > RIP > OSPF > BGP > Routing Objects > Multicast > Policy & Objects > Security Profiles > VPN > User & Authentication > System

Router ID 2.2.2.2

Areas

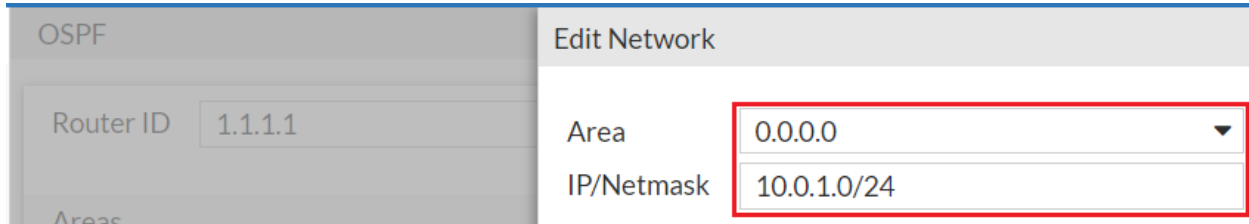
Area ID	Type	Authentication
0.0.0.0	Regular	None

Networks

Network	Area
10.0.1.0/24	0.0.0.0
10.0.2.0/24	0.0.0.0

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**.



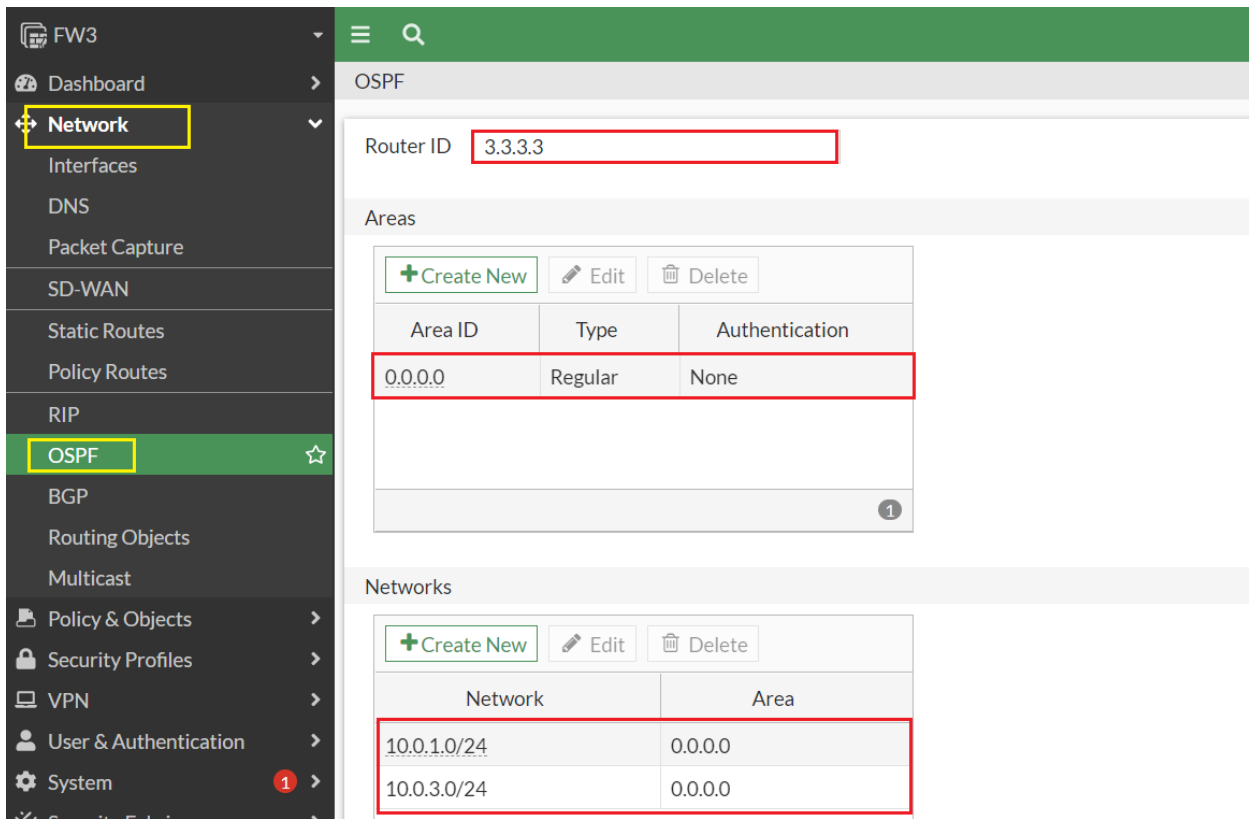
OSPF

Router ID 1.1.1.1

Area

Area 0.0.0.0

IP/Netmask 10.0.1.0/24



FW3

Dashboard

Network

Interfaces

DNS

Packet Capture

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Policy & Objects

Security Profiles

VPN

User & Authentication

System

OSPF

Router ID 3.3.3.3

Areas

+ Create New Edit Delete

Area ID	Type	Authentication
0.0.0.0	Regular	None

1

Networks

+ Create New Edit Delete

Network	Area
10.0.1.0/24	0.0.0.0
10.0.3.0/24	0.0.0.0

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**.

The screenshot shows the Mikrotik WinBox interface for editing a Firewall Policy. The left sidebar has 'Policy & Objects' and 'Firewall Policy' highlighted. The main panel is titled 'Edit Policy'. The configuration is as follows:

Name	LAN-to-DMZ
Incoming Interface	LAN (port3)
Outgoing Interface	DMZ-Zone
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based <input type="checkbox"/> Proxy-based <input type="checkbox"/>
Firewall / Network Options	
NAT	<input type="checkbox"/>

The screenshot shows the Mikrotik WinBox interface for editing a Firewall Policy. The left sidebar has 'Policy & Objects' and 'Firewall Policy' highlighted. The main panel is titled 'Edit Policy'. The configuration is as follows:

Name	DMZ-to-LAN
Incoming Interface	DMZ-Zone
Outgoing Interface	LAN (port3)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based <input type="checkbox"/> Proxy-based <input type="checkbox"/>
Firewall / Network Options	
NAT	<input type="checkbox"/>

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**.

The screenshot displays the configuration for a Firewall Policy named "WAN-to-LAN". The configuration is as follows:

Field	Value
Name	WAN-to-LAN
Incoming Interface	WAN (port1)
Outgoing Interface	LAN (port2)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT
Inspection Mode	Flow-based
NAT	Off

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**.

The screenshot shows the Mikrotik WinBox interface for editing a Firewall Policy. The left sidebar is dark grey with a yellow box around 'Policy & Objects' and a green box around 'Firewall Policy'. The main area is titled 'Edit Policy' and contains the following configuration:

- Name:** WAN-to-LAN
- Incoming Interface:** WAN (port1)
- Outgoing Interface:** LAN (port2)
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (selected), Proxy-based (unselected)
- Firewall / Network Options:** NAT (unchecked)

Testing and Verification:

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

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

Network	Gateway IP	Interfaces	Distance	Type	Metric	Priority
10.0.1.0/24	0.0.0.0	LAN (port3)	0	Connected	0	0
10.0.2.0/24	10.0.1.2	LAN (port3)	110	OSPF	2	1
10.0.3.0/24	10.0.1.3	LAN (port3)	110	OSPF	2	1
192.168.1.0/24	0.0.0.0	WAN-1 (port1)	0	Connected	0	0
192.168.2.0/24	0.0.0.0	WAN-2 (port2)	0	Connected	0	0
192.168.114.0/24	0.0.0.0	MGMT (port5)	0	Connected	0	0

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

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

```
FW2 #
FW2 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
0 - 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
0      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
```

FW2

Dashboard

Network

Routing

4 Routes

Type

- Connected
- OSPF

Route Lookup View Create Address Search

Network	Gateway IP	Interfaces	Distance	Type
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

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

```
FW3 # get router info routing-table ospf
Routing table for VRF=0
0      10.0.2.0/24 [110/2] via 10.0.1.2, port1, 00:07:41
```

Network	Gateway IP	Interfaces	Dist...	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**.

The screenshot shows the OSPF configuration page for FW1. In the 'Default Settings' section, the 'Inject default route' option is set to 'Always'. Other settings include 'Metric type' set to 'Type 2', 'Metric value' set to '10', and 'Route map' set to 'All'. The 'Redistribute Connected' and 'Redistribute Static' options are currently disabled.

Try to ping and browse from PC1, PC2, PC3, SRV1 and SRV2 to any internet 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