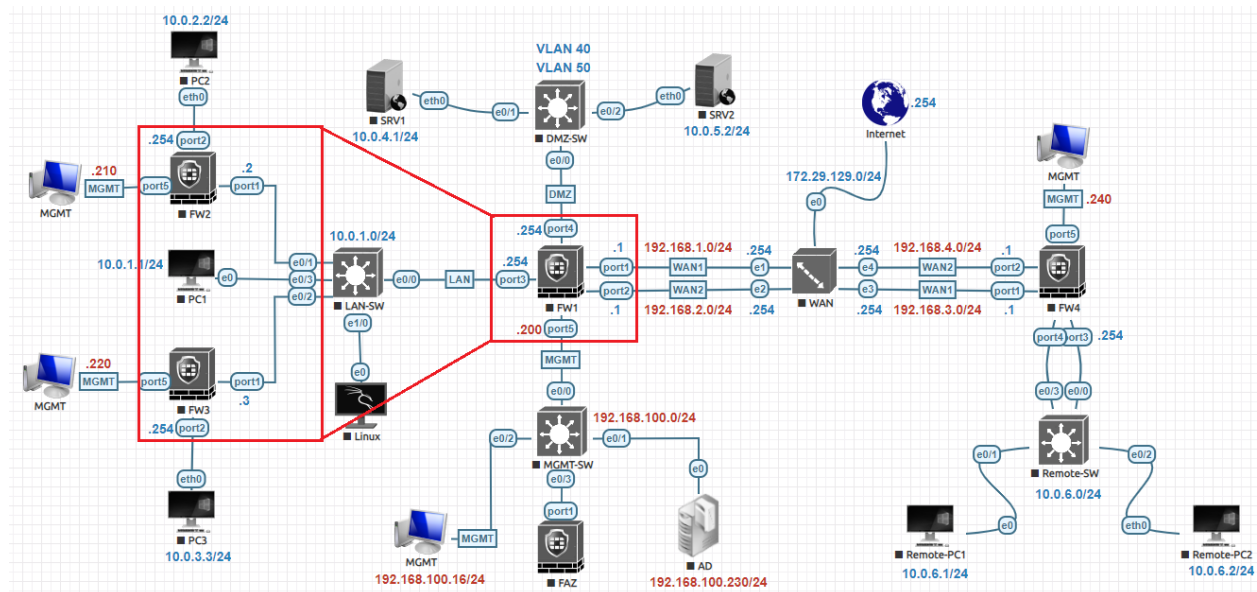


## Dynamic Protocol RIP Lab:



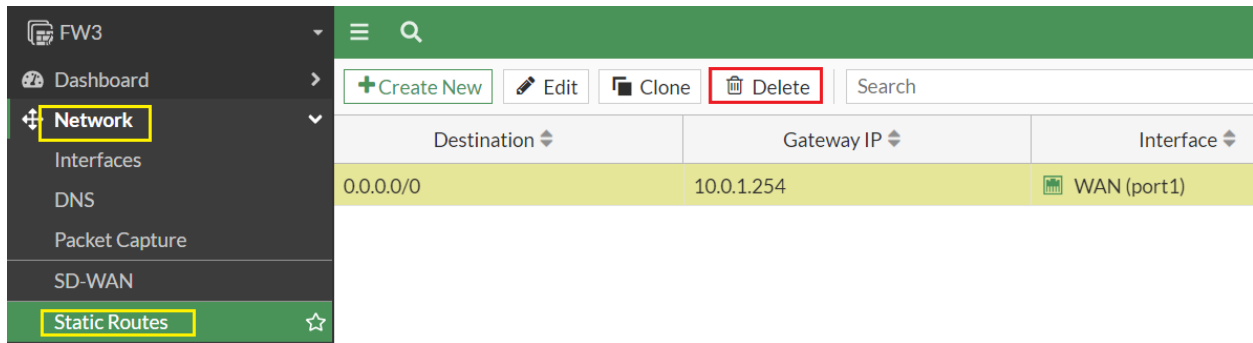
Two Core Firewall, FW2 and FW3, connect to the ISP Firewall FW1 for the internet access. Both FW2 and FW3 have different Local Networks. The ISP Firewall FW1 is using RIP for its connections to the core Firewalls, and redistributes its default route to the network - that is, default route injection is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

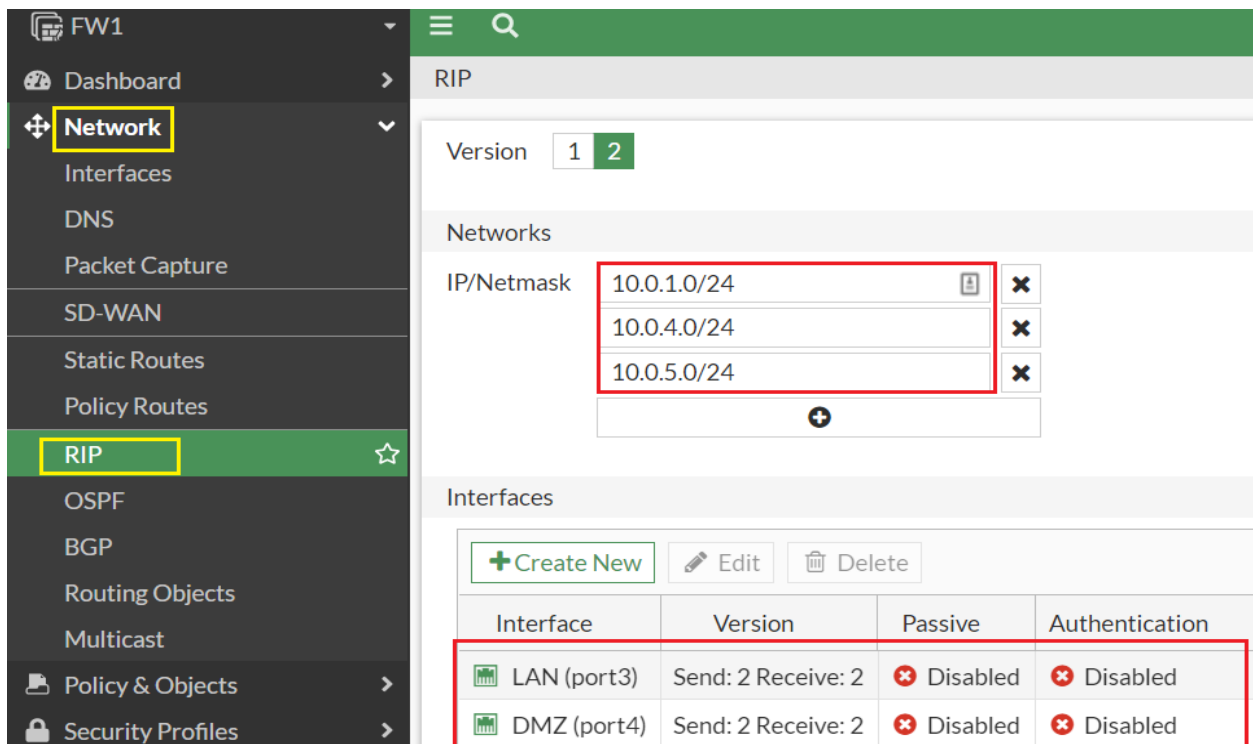
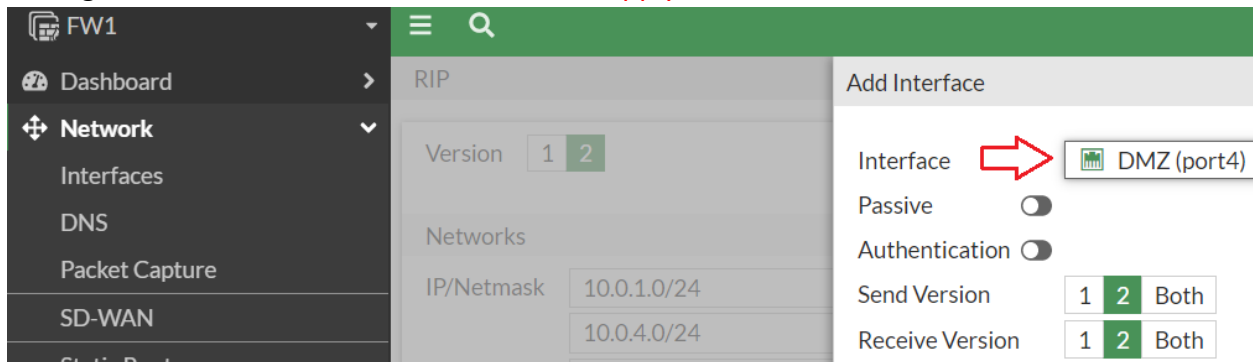
Destination	Gateway IP	Interface
0.0.0.0/0	192.168.1.254	WAN-1 (port1)
10.0.2.0/24	10.0.1.2	LAN (port3)
10.0.3.0/24	10.0.1.3	LAN (port3)
0.0.0.0/0	192.168.2.254	WAN-2 (port2)

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



### FW1 RIP Configuration:

Go to **Network > RIP** Set the Version to **2**. Under Networks, add three networks. In the Interfaces table, click Create New. Set Interface to port3 and port4. Leave the remaining settings as their default values. Click **OK**. Click **Apply**.



### FW2 RIP Configuration:

Go to **Network > RIP** Set the Version to **2**. Under Networks, add two networks. In the Interfaces table, click Create New. Set Interface to port1 and port2. Leave the remaining settings as their default values. Click **OK**. Click **Apply**.

The screenshot displays the configuration page for RIP on a firewall. The left-hand navigation pane is open to the 'RIP' section. The main content area shows the configuration for RIP version 2. The 'Version' is set to 2. Under the 'Networks' section, two networks are configured: 10.0.1.0/255.255.255.0 and 10.0.2.0/255.255.255.0. Below this, the 'Interfaces' section contains a table with the following data:

Interface	Version	Passive	Authentication
WAN (port1)	Send: 2 Receive: 2	Disabled	Disabled
LAN (port2)	Send: 2 Receive: 2	Disabled	Disabled

### FW3 RIP Configuration:

Go to **Network > RIP** Set the Version to **2**. Under Networks, add two networks. In the Interfaces table, click Create New. Set Interface to port1 and port2. Leave the remaining settings as their default values. Click **OK**. Click **Apply**.

FW3

Dashboard

**Network**

- Interfaces
- DNS
- Packet Capture
- SD-WAN
- Static Routes
- Policy Routes
- RIP**
- OSPF
- BGP
- Routing Objects
- Multicast
- Policy & Objects

RIP

Version 1 2

Networks

IP/Netmask 10.0.1.0 255.255.255.0

10.0.3.0 255.255.255.0

+

Interfaces

+ Create New Edit Delete

Interface	Version	Passive	Authentication
WAN (port1)	Send: 2 Receive: 2	✘ Disabled	✘ Disabled
LAN (port2)	Send: 2 Receive: 2	✘ Disabled	✘ Disabled

## 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 area 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
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 area 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
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 RIP in FW1.

```
FW1 #  
FW1 # get router info routing-table rip  
Routing table for VRF=0  
R    10.0.2.0/24 [120/2] via 10.0.1.2, port3, 00:21:59  
R    10.0.3.0/24 [120/2] via 10.0.1.3, port3, 00:21:39
```

The screenshot shows the FortiView interface for device FW1. The left sidebar has 'Network' selected. The main area displays the 'Routing' section with two donut charts showing 10 routes. The first chart shows 3 Connected (green), 2 Static (orange), and 5 RIP (purple) routes. The second chart shows 3 Connected (green), 2 Static (orange), 2 RIP (purple), 1 Static (red), and 2 Connected (blue) routes. Below the charts is a table of routes with columns: Network, Gateway IP, Interfaces, Distance, and Type. The first two rows are highlighted with a red box.

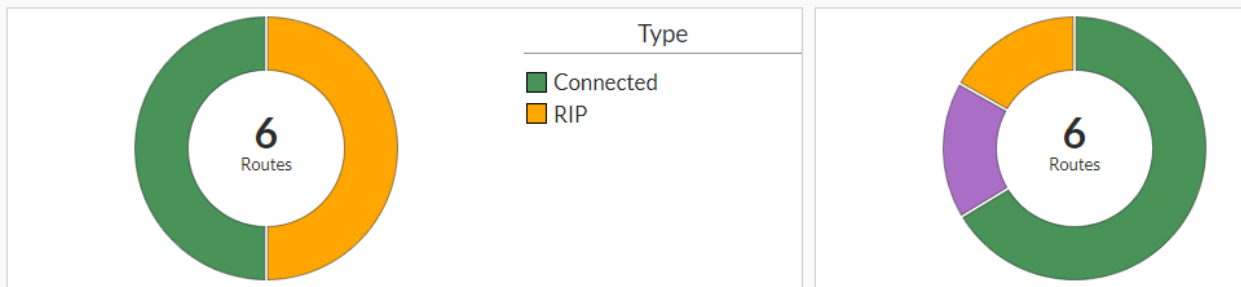
Network	Gateway IP	Interfaces	Distance	Type
10.0.2.0/24	10.0.1.2	LAN (port3)	120	RIP
10.0.3.0/24	10.0.1.3	LAN (port3)	120	RIP
0.0.0.0/0	192.168.1.254	WAN-1 (port1)	5	Static
0.0.0.0/0	192.168.2.254	WAN-2 (port2)	5	Static
10.0.1.0/24	0.0.0.0	LAN (port3)	0	Connected
10.0.4.0/24	0.0.0.0	SRV1 (VLAN40)	0	Connected
10.0.5.0/24	0.0.0.0	SRV2 (VLAN50)	0	Connected
192.168.1.0/24	0.0.0.0	WAN-1 (port1)	0	Connected
192.168.2.0/24	0.0.0.0	WAN-2 (port2)	0	Connected

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

```

FW2 #
FW2 # get router info routing-table rip
Routing table for VRF=0
R    10.0.3.0/24 [120/2] via 10.0.1.3, port1, 00:27:40
R    10.0.4.0/24 [120/2] via 10.0.1.254, port1, 00:28:00
R    10.0.5.0/24 [120/2] via 10.0.1.254, port1, 00:28:00
  
```

← Routing



🔍 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)	120	RIP
10.0.4.0/24	10.0.1.254	WAN (port1)	120	RIP
10.0.5.0/24	10.0.1.254	WAN (port1)	120	RIP
192.168.100.0/24	0.0.0.0	MGMT (port5)	0	Connected

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

```
FW3 #
FW3 # get router info routing-table rip
Routing table for VRF=0
R   10.0.2.0/24 [120/2] via 10.0.1.2, port1, 00:28:30
R   10.0.4.0/24 [120/2] via 10.0.1.254, port1, 00:28:30
R   10.0.5.0/24 [120/2] via 10.0.1.254, port1, 00:28:30
```

← Routing

6 Routes

6 Routes

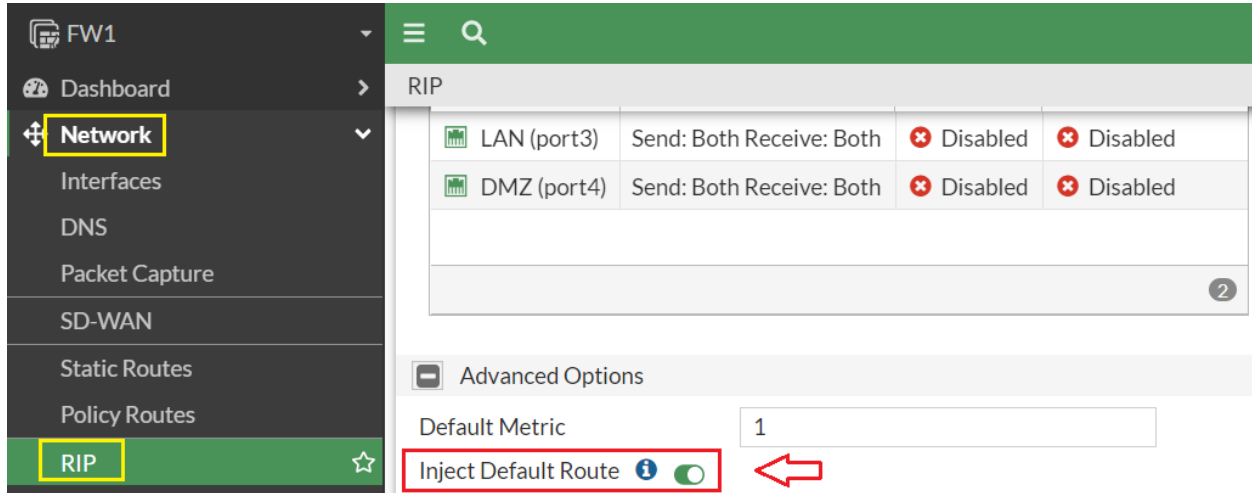
Network	Gateway IP	Interfaces	Distance	Type
10.0.1.0/24	0.0.0.0	WAN (port1)	0	Connected
10.0.2.0/24	10.0.1.2	WAN (port1)	120	RIP
10.0.3.0/24	0.0.0.0	LAN (port2)	0	Connected
10.0.4.0/24	10.0.1.254	WAN (port1)	120	RIP
10.0.5.0/24	10.0.1.254	WAN (port1)	120	RIP
192.168.100.0/24	0.0.0.0	MGMT (port5)	0	Connected

```
get router info routing-table all
get router info rip database
get router info rip interface
```

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 RIP 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 Advanced Options, 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 Mikrotik WinBox interface for configuring RIP on FW1. The left sidebar has 'RIP' selected. The main panel shows the RIP configuration for 'RIP'. The 'Advanced Options' section is expanded, showing 'Default Metric' set to 1 and 'Inject Default Route' enabled (indicated by a green toggle switch). A red box highlights the 'Inject Default Route' option, and a red arrow points to it.

Interface	Send	Receive	Both	Send	Receive	Both
LAN (port3)	Send: Both	Receive: Both	Both	✘ Disabled	✘ Disabled	✘ Disabled
DMZ (port4)	Send: Both	Receive: Both	Both	✘ Disabled	✘ Disabled	✘ 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 RIP Default Route.