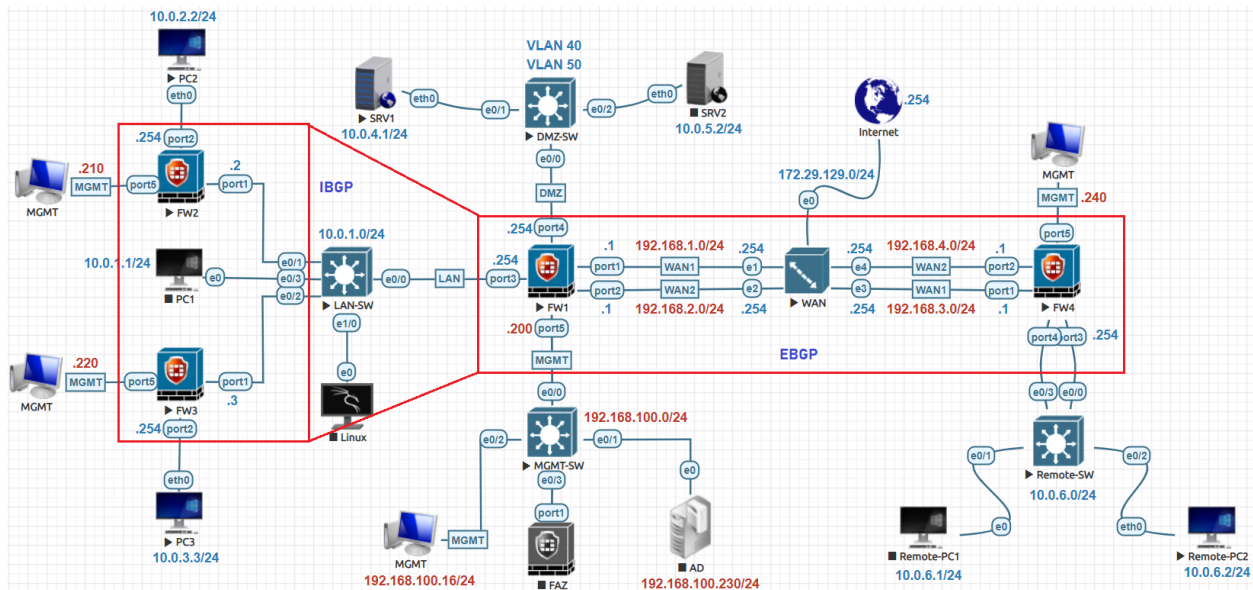


Dynamic Protocol BGP Lab:



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
- Dashboard
- Network**
- Interfaces
- DNS
- Packet Capture
- SD-WAN
- Static Routes
- Policy Routes
- RIP
- OSPF

OSPF
Router ID

Areas

+ Create New
Edit
Delete

Area ID	Type	Authentication
No results		

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**.

The screenshot shows the 'Local BGP Options' configuration page. The 'Local AS' is set to 123 and the 'Router ID' is set to 11.11.11.11. Under the 'Neighbors' section, there is a table with the following data:

IP	Remote AS
192.168.3.1	41
10.0.1.2	123
10.0.1.3	123

The screenshot shows the 'Networks' section of the BGP configuration. It contains a table with the following data:

IP/Netmask	
10.0.1.0 255.255.255.0	✘
10.0.2.0 255.255.255.0	✘
10.0.3.0 255.255.255.0	✘
10.0.4.0 255.255.255.0	✘
10.0.5.0 255.255.255.0	✘

FW1 to FW4 change multihop for EBG

```
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**.

The screenshot shows the 'Local BGP Options' configuration page. The 'Local AS' is set to 123 and the 'Router ID' is 2.2.2.2. Under the 'Neighbors' section, there are two entries:

IP	Remote AS
10.0.1.254	123
10.0.1.3	123

The screenshot shows the 'Networks' section of the BGP configuration. Two networks are listed:

IP/Netmask	Action
10.0.2.0 255.255.255.0	✕
10.0.1.0 255.255.255.0	✕

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**.

The screenshot shows the configuration page for BGP on FW3. The left sidebar has 'Network' and 'BGP' highlighted. The main content area is titled 'Local BGP Options'. Under 'Local BGP Options', the 'Local AS' is set to 123 and the 'Router ID' is set to 3.3.3.3. Below this is the 'Neighbors' section, which contains a table with two columns: 'IP' and 'Remote AS'. Two neighbors are listed: 10.0.1.254 with Remote AS 123, and 10.0.1.2 with Remote AS 123. There are also buttons for '+ Create New', 'Edit', and 'Delete'.

IP	Remote AS
10.0.1.254	123
10.0.1.2	123

The screenshot shows the configuration page for BGP on FW3, specifically the 'Networks' section. The left sidebar has 'Network' and 'BGP' highlighted. The main content area is titled 'Local BGP Options'. Under 'Networks', there are two entries: 10.0.3.0 255.255.255.0 and 10.0.1.0 255.255.255.0. There are also buttons for '+', 'x', and 'x'.

IP/Netmask	
10.0.3.0 255.255.255.0	x
10.0.1.0 255.255.255.0	x

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**.

The screenshot shows the 'Local BGP Options' configuration page in the FW4 interface. The 'Local AS' is set to 41 and the 'Router ID' is set to 4.4.4.4. Under the 'Neighbors' section, a table lists the neighbor configuration:

IP	Remote AS
192.168.1.102	123

The screenshot shows the 'Networks' section of the BGP configuration page. The 'IP/Netmask' field is set to 10.0.6.0 255.255.255.0. The 'IPv6 Networks' and 'IPv4 Redistribute' sections are also visible.

FW4 to FW1 change multihop for EGBP

```
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**.

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 contains a navigation menu with 'Policy & Objects' and 'Firewall Policy' highlighted. The main area is titled 'Edit Policy' and contains the following configuration fields:

- 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 BGP in 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 # 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
```

FortiGate time is out of sync.

Routing

11 Routes

Type

- Connected
- Static
- OSPF
- BGP

11 Routes

- W
- LA
- W
- VL
- VL
- MC

Route Lookup View Create Address Search

Network	Gateway...	Interfaces	Distance	Type	Metric	Priority
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
0.0.0.0/0	192.168.1.254	WAN-1 (port1)	5	Static	0	1
0.0.0.0/0	192.168.2.254	WAN-2 (port2)	5	Static	0	1
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
10.0.6.0/24	192.168.1.254	WAN-1 (port1)	20	BGP	0	1

Let's Check the routing table for BGP in 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 # get route 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
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
```

The screenshot shows the FortiGate FW2 GUI. On the left is a navigation menu with options like Dashboard, Status, Security, Network, Users & Devices, etc. The main area displays the 'Routing' page with two donut charts showing route counts (6 Connected, 1 BGP). Below the charts is a 'Route Lookup' table with columns for Network, Gateway, Interfaces, Distance, and Type. The BGP routes are highlighted with a red box.

Network	Gatewa...	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)	200	BGP
10.0.4.0/24	10.0.1.254	WAN (port1)	200	BGP
10.0.5.0/24	10.0.1.254	WAN (port1)	200	BGP

Let's Check the routing table for OSPF in 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 # 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
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
```

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)	200	BGP
10.0.3.0/24	0.0.0.0	LAN (port2)	0	Connected
10.0.4.0/24	10.0.1.254	WAN (port1)	200	BGP
10.0.5.0/24	10.0.1.254	WAN (port1)	200	BGP
192.168.114.0/24	0.0.0.0	MGMT (port5)	0	Connected

Let's Check the routing table for BGP in 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 # 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
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
```

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	192.168.3.254	WAN-1 (port1)	10	Static
10.0.1.0/24	192.168.3.254	WAN-1 (port1)	20	BGP
10.0.2.0/24	192.168.3.254	WAN-1 (port1)	20	BGP
10.0.3.0/24	192.168.3.254	WAN-1 (port1)	20	BGP
10.0.4.0/24	192.168.3.254	WAN-1 (port1)	20	BGP
10.0.5.0/24	192.168.3.254	WAN-1 (port1)	20	BGP
10.0.6.0/24	0.0.0.0	Aggregate to Re...	0	Connected
192.168.3.0/24	0.0.0.0	WAN-1 (port1)	0	Connected
192.168.114.0/24	0.0.0.0	MGMT (port5)	0	Connected

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.

```
root@PC2: ~  
File Edit View Search Terminal Help  
root@PC2:~# ping 10.0.3.3  
PING 10.0.3.3 (10.0.3.3) 56(84) bytes of data.  
64 bytes from 10.0.3.3: icmp_seq=1 ttl=62 time=3.31 ms  
64 bytes from 10.0.3.3: icmp_seq=2 ttl=62 time=11.0 ms  
^C  
--- 10.0.3.3 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 3.310/7.169/11.029/3.860 ms  
root@PC2:~#
```

```
root@PC2: ~  
File Edit View Search Terminal Help  
root@PC2:~# ping 10.0.4.1  
PING 10.0.4.1 (10.0.4.1) 56(84) bytes of data.  
64 bytes from 10.0.4.1: icmp_seq=1 ttl=62 time=3.10 ms  
64 bytes from 10.0.4.1: icmp_seq=2 ttl=62 time=3.06 ms  
^C  
--- 10.0.4.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 3.064/3.085/3.106/0.021 ms  
root@PC2:~#
```