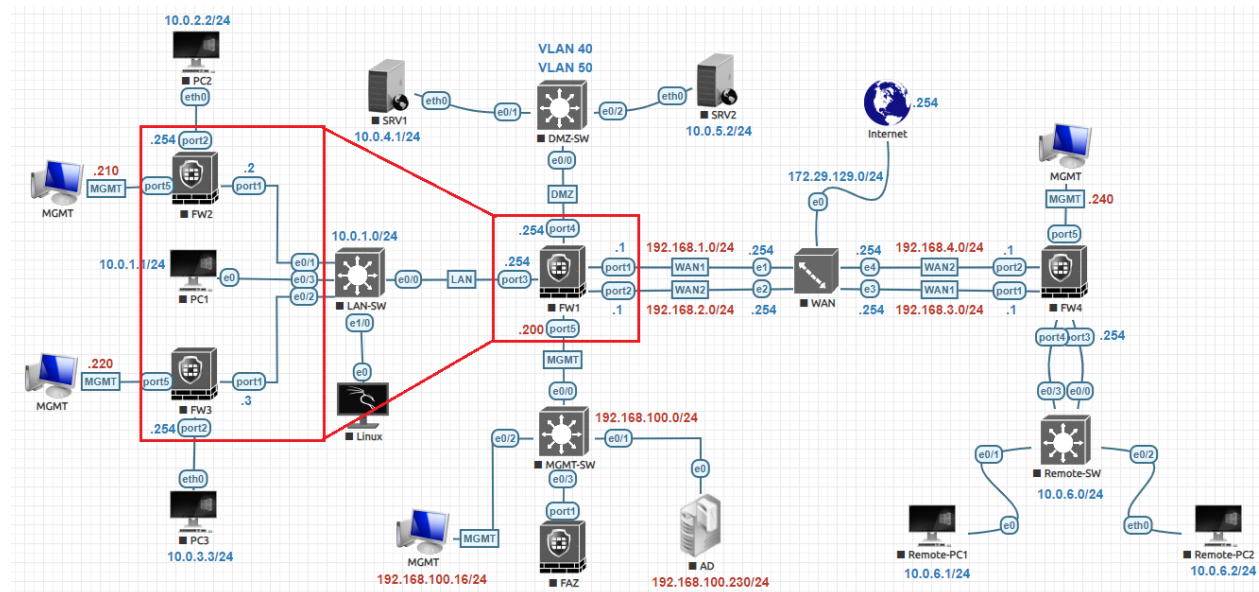


Static & Default Route Lab:



Change Hostname FW2

```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FW2
FortiGate-VM64-KVM (global) # end
```

Configure Management Interface FW2

```
FW2 # config system interface
FW2 (interface) # edit port5
FW2 (port4) # set mode static
FW2 (port4) # set ip 192.168.100.210/24
FW2 (port4) # set allowaccess https http ssh telnet ping
FW2 (port4) # end
```

Change Hostname FW3

```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FW3
FortiGate-VM64-KVM (global) # end
```

Configure Management Interface FW3

```
FW3 # config system interface
FW3 (interface) # edit port5
FW3 (port4) # set mode static
FW3 (port4) # set ip 192.168.100.220/24
FW3 (port4) # set allowaccess https http ssh telnet ping
FW3 (port4) # end
```

Login to FortiGate Firewall type <http://192.168.100.210> in any browser. Select **Optimal** and click **OK** to continue log in to Fortigate Firewall dashboard.

Setup Progress

- Specify Hostname ✓
- Change Your Password ✓
- **Dashboard Setup**
- Upgrade Firmware ✓

Dashboard Setup

Select one of the following options to decide what dashboards will be available by default. You can always change your selection or manually customize your own dashboards later.

Optimal
A set of popular default dashboards and FortiView monitors.

Comprehensive
A set of default dashboards as well as all monitors and FortiViews. This set will be familiar to users coming from previous FortiOS versions

OK Later

FW2 Configure Interfaces:

Go to **Network>Interfaces** select **port1** Click **Edit** in **Alias** type **WAN**, change the Address Mode to **Manual** type **IP/Netmask 10.0.1.2/24**, in **Administrative access** uncheck everything only checked **PING** leave all the rest of configuration default and press **OK** button.

Edit Interface

Name: port1

Alias: WAN

Type: Physical Interface

VRF ID: 0

Role: WAN

Estimated bandwidth: 0 kbps Upstream, 0 kbps Downstream

Dedicated Management Port

Address

Addressing mode: Manual, DHCP

IP/Netmask: 10.0.1.2/24

Secondary IP address:

Administrative Access

IPv4: HTTPS, HTTP, PING

Go to **Network>Interfaces** select **port2** Click **Edit** in **Alias** type **LAN**, change the Address Mode to **Manual** type **IP/Netmask** **10.0.2.254/24**, in **Administrative access** only checked **PING** leave all the rest of configuration default & press **OK**.

The screenshot shows the 'Edit Interface' configuration page for 'port2'. The left sidebar is expanded to 'Network > Interfaces'. The main configuration area is as follows:

- Name: port2
- Alias: LAN
- Type: Physical Interface
- VRF ID: 0
- Role: LAN
- Dedicated Management Port:
- Addressing mode: Manual (selected), DHCP, Auto-managed by IPAM, One-Arm Sniffer
- IP/Netmask: 10.0.2.254/24
- Create address object matching subnet:
- Secondary IP address:
- Administrative Access:
 - IPv4: HTTPS, PING, FMG-Access

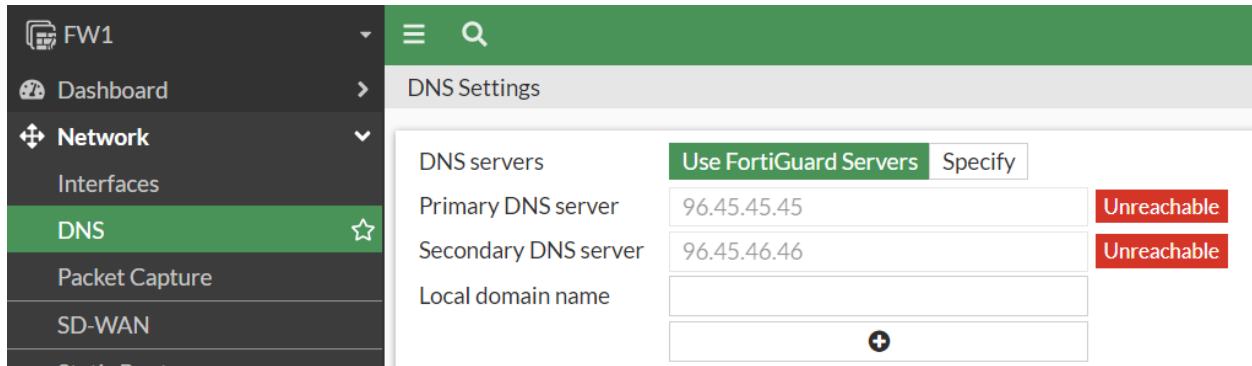
Go to **Network>Interfaces** select **port5** Click **Edit** in **Alias** type **MGMT**, leave all the rest of configuration default and press **OK** button.

The screenshot shows the 'Edit Interface' configuration page for 'port5'. The left sidebar is expanded to 'Network > Interfaces'. The main configuration area is as follows:

- Name: port5
- Alias: MGMT
- Type: Physical Interface
- VRF ID: 0
- Role: Undefined
- Dedicated Management Port:
- Addressing mode: Manual (selected), DHCP, Auto-managed by IPAM, One-Arm Sniffer
- IP/Netmask: 192.168.100.210/255.255.255.0
- Secondary IP address:
- Administrative Access:
 - IPv4: HTTPS, HTTP, PING, FMG-Access, SSH, SNMP

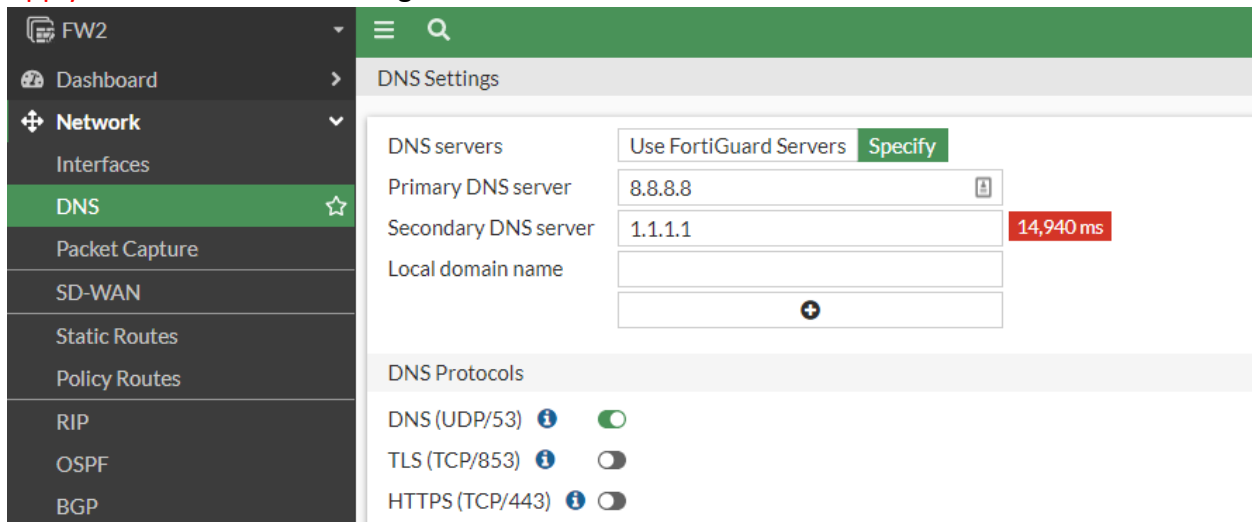
FW2 DNS Configuration:

Go to **Network > DNS** by default, using Fortinet's FortiGuard servers are select.



The screenshot shows the DNS Settings page for FW1. The 'DNS servers' dropdown is set to 'Use FortiGuard Servers'. The 'Primary DNS server' is 96.45.45.45 and the 'Secondary DNS server' is 96.45.46.46. Both are marked as 'Unreachable' in red boxes. The 'Local domain name' field is empty.

It is possible to specify using different DNS server, click on **Specify** and enter in primary / secondary DNS servers. In Primary DNS Server, type the IP address of the **primary DNS server 8.8.8.8**. In Secondary DNS Server, type the IP address of the **secondary DNS server 1.1.1.1**. Click **Apply** button to save the changes.



The screenshot shows the DNS Settings page for FW2. The 'DNS servers' dropdown is set to 'Specify'. The 'Primary DNS server' is 8.8.8.8 and the 'Secondary DNS server' is 1.1.1.1. The 'Secondary DNS server' is marked as '14,940 ms' in a red box. The 'Local domain name' field is empty. Below the settings, the 'DNS Protocols' section shows 'DNS (UDP/53)' is enabled, 'TLS (TCP/853)' is disabled, and 'HTTPS (TCP/443)' is disabled.

```
CLI Console (1)
FW2 # get system dns
primary       : 8.8.8.8
secondary    : 1.1.1.1
protocol      : cleartext
ssl-certificate : Fortinet_Factory
domain       :
```

Login to FortiGate Firewall type <http://192.168.100.220> in any browser. Select **Optimal** and click **OK** to continue log in to Fortigate Firewall dashboard.

Setup Progress

- Specify Hostname ✓
- Change Your Password ✓
- Dashboard Setup
- Upgrade Firmware ✓

Dashboard Setup

Select one of the following options to decide what dashboards will be available by default. You can always change your selection or manually customize your own dashboards later.

Optimal
A set of popular default dashboards and FortiView monitors.

Comprehensive
A set of default dashboards as well as all monitors and FortiViews. This set will be familiar to users coming from previous FortiOS versions

OK Later

FW3 Configure Interfaces:

Go to **Network>Interfaces** select **port1** Click **Edit** in **Alias** type **WAN**, change the Address Mode to **Manual** type **IP/Netmask 10.0.1.3/24**, in **Administrative access** uncheck everything only checked **PING** leave all the rest of configuration default and press **OK** button.

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

Edit Interface

Name: port1

Alias: WAN

Type: Physical Interface

VRF ID: 0

Role: WAN

Estimated bandwidth: 0 kbps Upstream, 0 kbps Downstream

Dedicated Management Port

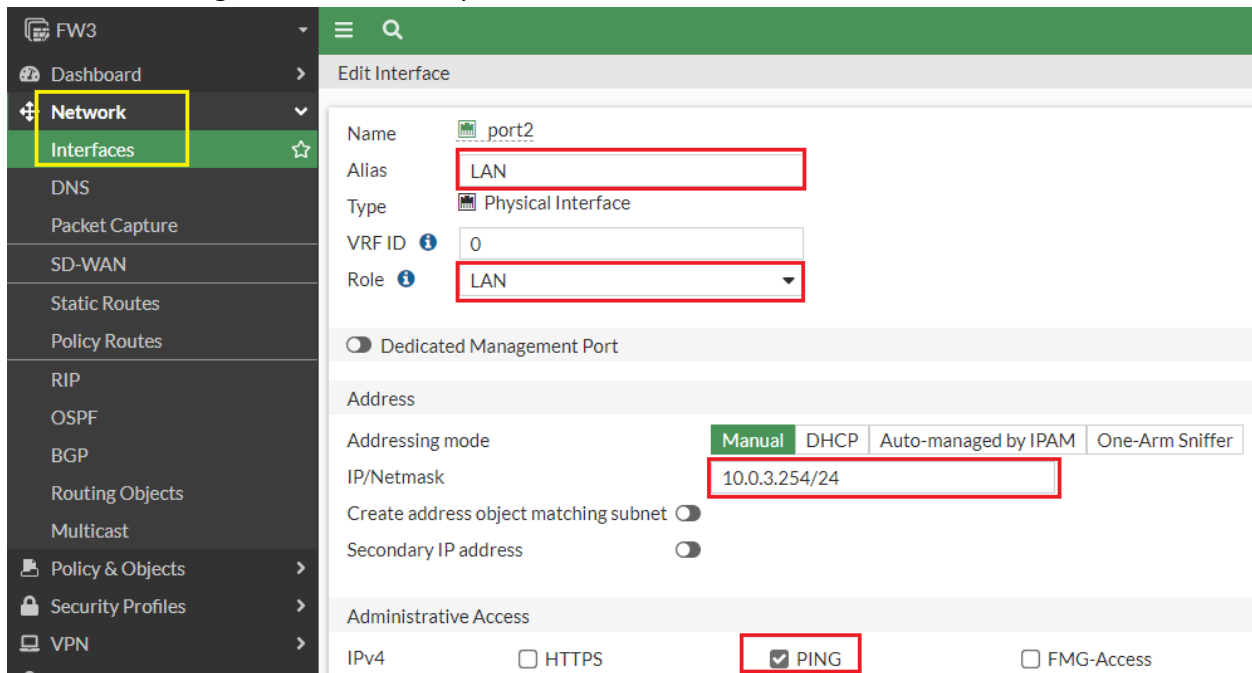
Addressing mode: Manual, DHCP

IP/Netmask: 10.0.1.3/24

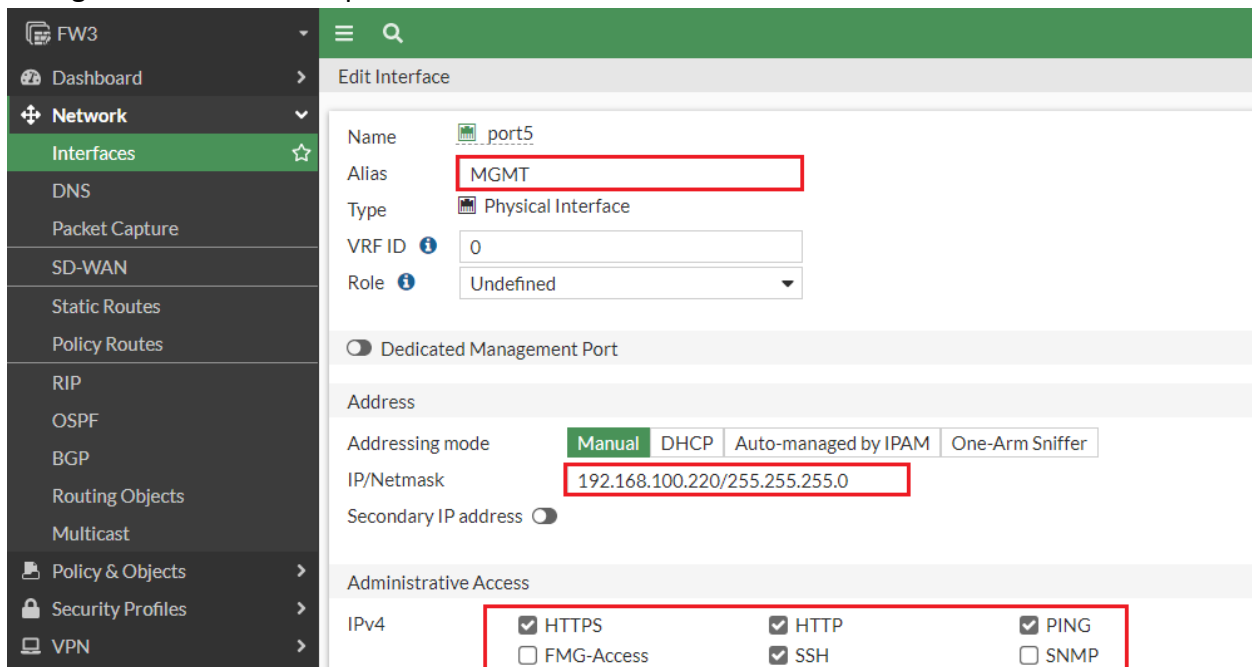
Secondary IP address:

Administrative Access: IPv4, HTTPS, HTTP, PING

Go to **Network>Interfaces** select **port2** Click **Edit** in **Alias** type **LAN**, change the Address Mode to **Manual** type **IP/Netmask** **10.0.3.254/24**, in **Administrative access** only checked **PING** leave all the rest of configuration default & press **OK**.

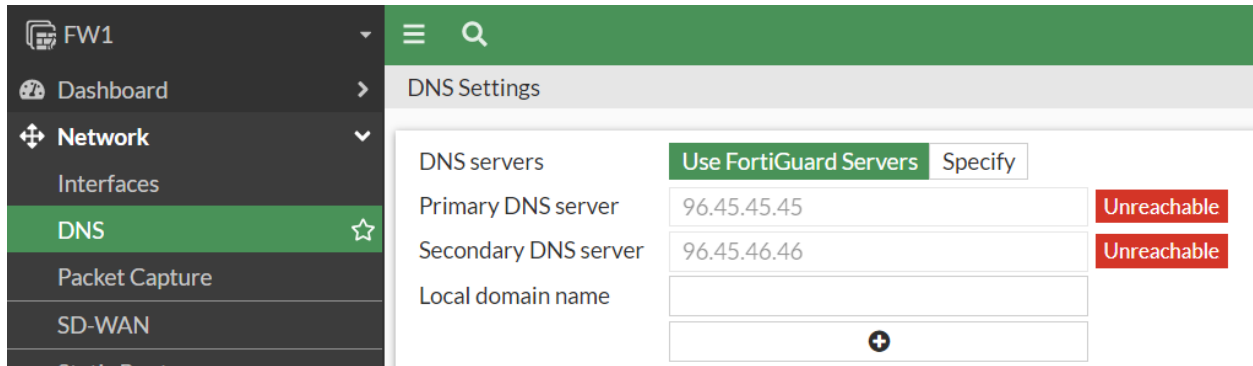


Go to **Network>Interfaces** select **port5** Click **Edit** in **Alias** type **MGMT**, leave all the rest of configuration default and press **OK** button.



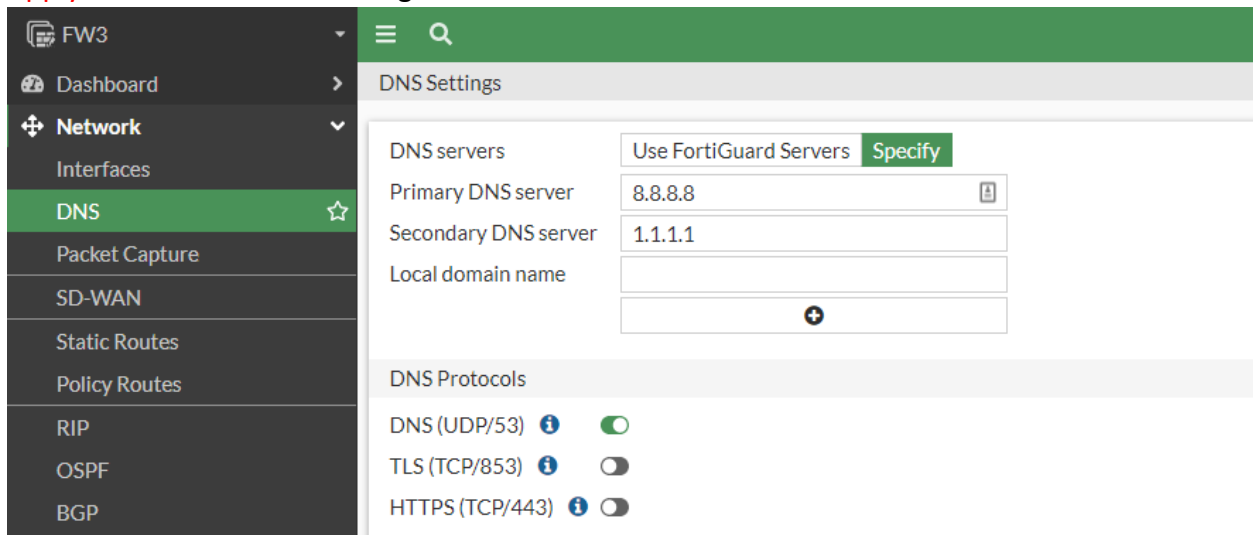
FW3 DNS Configuration:

Go to **Network > DNS** by default, using Fortinet's FortiGuard servers are select.



The screenshot shows the FortiGate FW1 web interface. The left sidebar is expanded to 'Network > DNS'. The main panel is titled 'DNS Settings'. Under 'DNS servers', the 'Use FortiGuard Servers' option is selected. Below this, the 'Primary DNS server' is set to 96.45.45.45 and the 'Secondary DNS server' is set to 96.45.46.46. Both server status indicators are red and labeled 'Unreachable'. The 'Local domain name' field is empty.

It is possible to specify using different DNS server, click on **Specify** and enter in primary / secondary DNS servers. In Primary DNS Server, type the IP address of the **primary DNS server 8.8.8.8**. In Secondary DNS Server, type the IP address of the **secondary DNS server 1.1.1.1**. Click **Apply** button to save the changes.

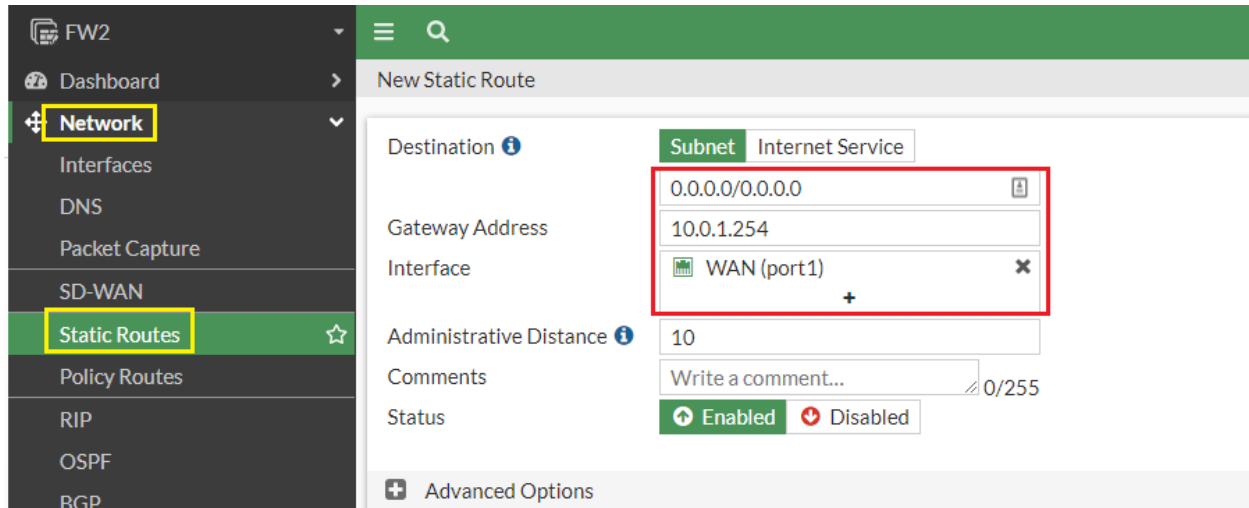


The screenshot shows the FortiGate FW3 web interface. The left sidebar is expanded to 'Network > DNS'. The main panel is titled 'DNS Settings'. Under 'DNS servers', the 'Specify' option is selected. Below this, the 'Primary DNS server' is set to 8.8.8.8 and the 'Secondary DNS server' is set to 1.1.1.1. The 'Local domain name' field is empty. Below the DNS servers section, the 'DNS Protocols' section is visible, with 'DNS (UDP/53)' checked and 'TLS (TCP/853)' and 'HTTPS (TCP/443)' unchecked.

```
CLI Console (1)
FW3 # get system dns
primary      : 8.8.8.8
secondary   : 1.1.1.1
protocol     : cleartext
ssl-certificate : Fortinet_Factory
domain      :
```

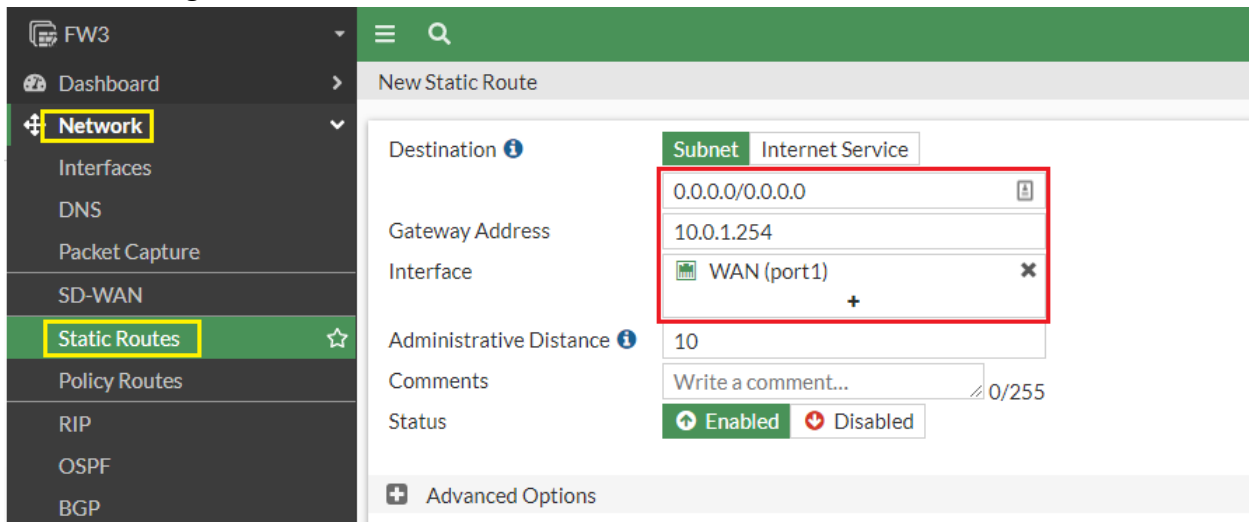
FW2 Default Route Configuration:

To create a new default route, go to **Network > Static Routes** and create a static route for ISP. Set Destination to **Subnet** and leave the destination IP address set to **0.0.0.0/0.0.0.0**. Set Gateway to the IP address provided by your ISP and Interface to the Internet-facing interface in my case **10.0.1.254** which the Gateway. Set the Interface to the **WAN** interface. Press **OK** to Save the changes.



FW3 Default Route Configuration:

To create a new default route, go to **Network > Static Routes** and create a static route for ISP. Set Destination to **Subnet** and leave the destination IP address set to **0.0.0.0/0.0.0.0**. Set Gateway to the IP address provided by your ISP and Interface to the Internet-facing interface in my case **10.0.1.254** which the Gateway. Set the Interface to the **WAN** interface. Press **OK** to Save the changes.



In FW1 we already configured Default route which gateway is **192.168.1.254**.

FW1 Static Route Configuration:

Let's create a static route for FW2 LAN Subnet while the gateway is FW2 IP address.

The screenshot shows the 'New Static Route' configuration form for FW1. The 'Destination' field is set to 'Subnet' with the value '10.0.2.2/24'. The 'Gateway Address' is '10.0.1.2' and the 'Interface' is 'LAN (port3)'. The 'Administrative Distance' is '10'. The status is 'Enabled'.

Let's create a static route for FW3 LAN Subnet while the gateway is FW3 IP address.

The screenshot shows the 'New Static Route' configuration form for FW1. The 'Destination' field is set to 'Subnet' with the value '10.0.3.0/24'. The 'Gateway Address' is '10.0.1.3' and the 'Interface' is 'LAN (port3)'. The 'Administrative Distance' is '10'. The status is 'Enabled'.

Finally, in FW1 we have three 3 routes one is default route going outside Internet while two 2 are static Routes for each firewall LAN Subnets.

Destination	Gateway IP	Interface
0.0.0.0/0	192.168.1.254	WAN (port1)
10.0.2.0/24	10.0.1.2	LAN (port3)
10.0.3.0/24	10.0.1.3	LAN (port3)

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 **WAN**. Set Source, Destination Address, Schedule, and Services, as required in this case All. Ensure the **Action** is set to **ACCEPT**. Turn on **NAT** and select **Use Outgoing Interface Address**.

The screenshot shows the 'New Policy' configuration window. The left sidebar has 'Policy & Objects' selected, with 'Firewall Policy' highlighted. The main configuration area is titled 'New Policy' and contains the following fields:

- Name: Allow Internet Access for LAN
- Incoming Interface: LAN (port3)
- Outgoing Interface: WAN (port1)
- Source: all
- Destination: all
- Schedule: always
- Service: ALL
- Action: ACCEPT (checked), DENY
- Inspection Mode: Flow-based (selected), Proxy-based
- Firewall / Network Options: NAT (checked)
- IP Pool Configuration: Use Outgoing Interface Address (selected), Use Dynamic IP Pool
- Preserve Source Port: OFF
- Protocol Options: default

A red box highlights the Name, Incoming Interface, Outgoing Interface, Source, Destination, and Service fields. Another red box highlights the NAT toggle and IP Pool Configuration options. A red arrow points to the 'OK' button.

Scroll down to view the Logging Options. To view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

Logging Options

The screenshot shows the 'Logging Options' section with the following settings:

- Log Allowed Traffic: Security Events **All Sessions**
- Generate Logs when Session Starts:
- Capture Packets:

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 **LAN** and the **Outgoing Interface** to **WAN**. 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 'New Policy' configuration page in a network management interface. The left sidebar has 'Policy & Objects' and 'Firewall Policy' highlighted. The main form is titled 'New Policy' and contains the following fields:

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

PC2 IP address configuration default gateway is FW2 IP Address.

The screenshot shows the configuration page for 'PC2'. On the left, there is a list of devices with their status (ON/OFF). 'PC2' is highlighted with a red box. On the right, there is a terminal window with the following commands:

```
ip addr add 10.0.2.2/24 dev eth0 ||true
ip route add default via 10.0.2.254||true
cat>/etc/resolv.conf<<EOF
nameserver 8.8.8.8
EOF
```

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 **LAN** and the **Outgoing Interface** to **WAN**. 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 'New Policy' configuration page in a network management interface. The left sidebar is dark grey with 'Policy & Objects' and 'Firewall Policy' highlighted. The main content area is white with a green header 'New Policy'. The configuration form includes the following fields:

- Name: Allow LAN Access
- Incoming Interface: LAN (port2)
- Outgoing Interface: WAN (port1)
- 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)

PC3 IP address configuration default gateway is FW3 IP Address.

The screenshot shows a network configuration interface. On the left, there is a list of devices with their status:

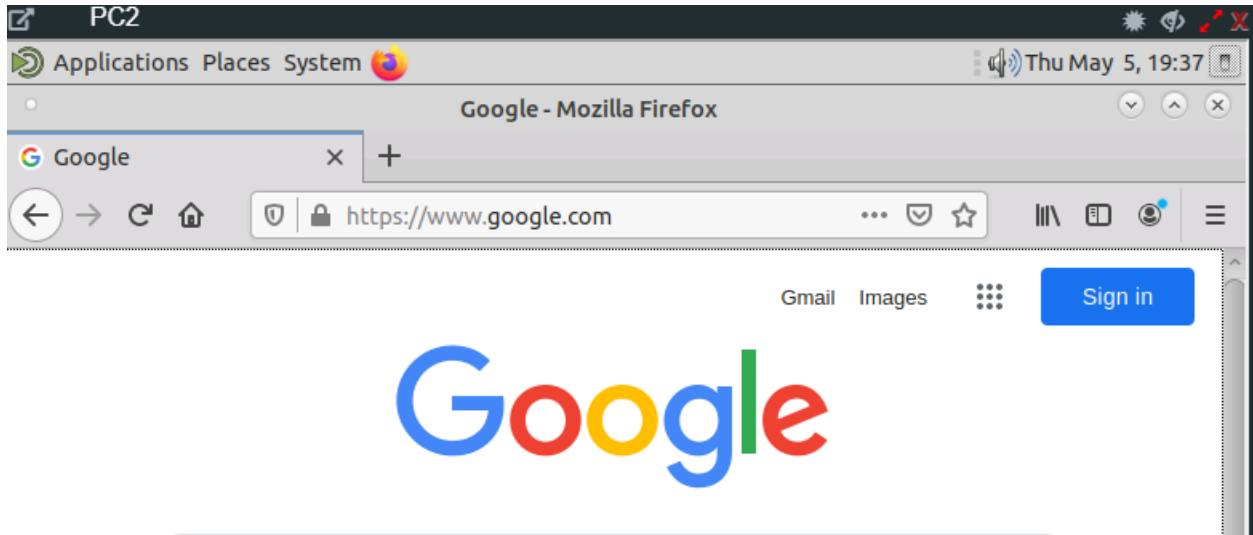
- LAN-SW: OFF
- DMZ-SW: OFF
- MGMT-SW: OFF
- Remote-SW: OFF
- SRV1: ON
- SRV2: ON
- PC2: ON
- PC3: ON

On the right, a terminal window shows the configuration commands for PC3:

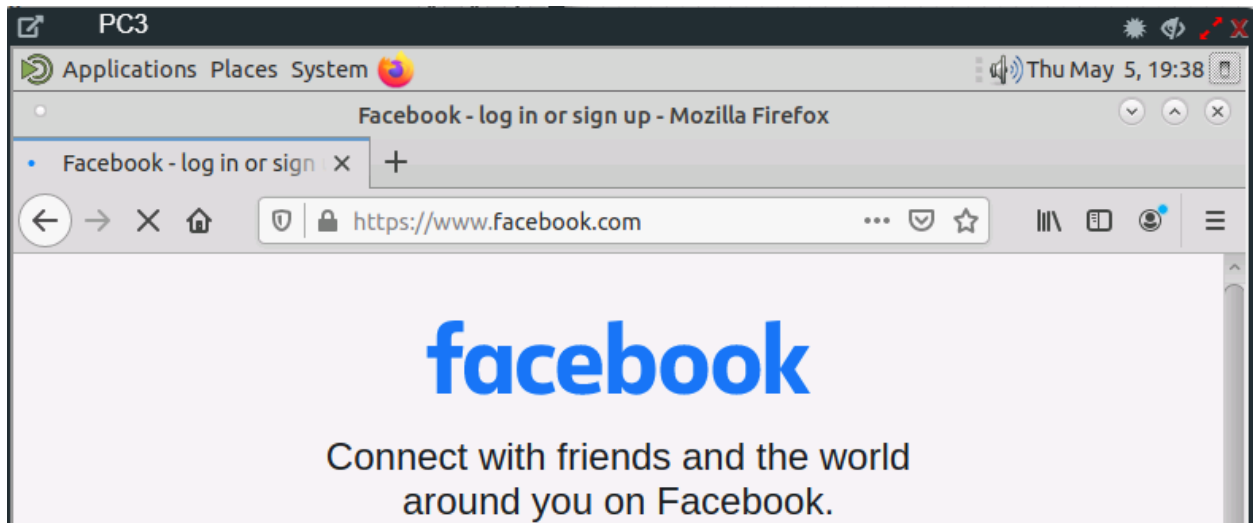
```
ip addr add 10.0.3.3/24 dev eth0 ||true
ip route add default via 10.0.3.254||true
cat>/etc/resolv.conf<<EOF
nameserver 8.8.8.8
EOF
```

Testing and Verification:

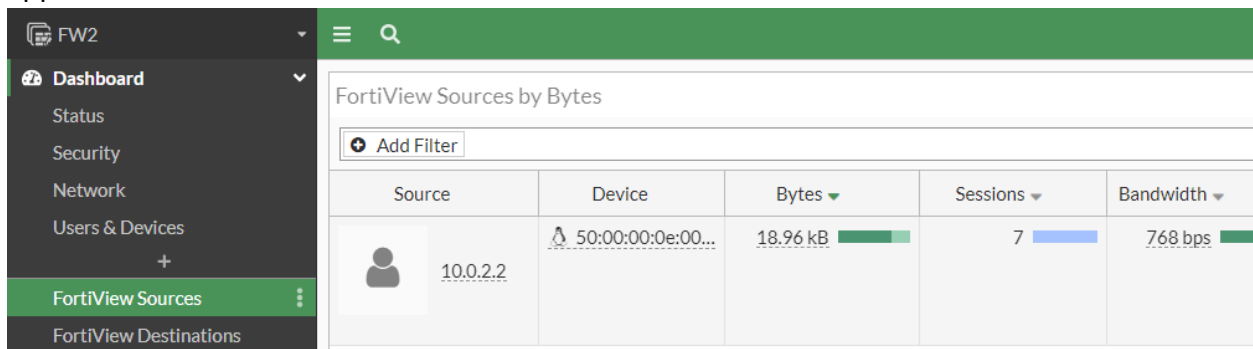
Browse the Internet using the PC2 on the internal LAN network of FW2.



Browse the Internet using the PC3 on the internal LAN network of FW3.



To view information about FortiGate traffic, go to **Dashboard > FortiView Sources**. The PC2 appears on the list of sources in FW2.



To view information about FortiGate traffic, go to **Dashboard > FortiView Sources**. The PC3 appears on the list of sources in FW3.

Source	Device	Bytes	Sessions	Bandwidth
10.0.3.3	50:00:00:0f:00:...	71.73 kB	17	2.96 kbps

To view information about traffic, Go to **Dashboard > FortiView Sessions**.

Source	Device	Destination	Application	Protocol	Source Port	Destination Port
10.0.2.2	50:00:00:0e:00:00	54.189.35.180	TCP/443	TCP	57068	443

To view information about which policy has been used Go to **Dashboard > FortiView Policies**

Policy	Policy Type	Source Interface	Destination Interface	Bytes
Allow LAN Access (1)	Firewall	LAN (port2)	WAN (port1)	7.84 kB

To view information about FortiGate traffic, go to **Log & Report > Forward Traffic**.

Date/Time	Source	Device	Destination
2 minutes ago	10.0.2.2	50:00:00:0e:00:00	8.8.8.8 (dns.google)
2 minutes ago	10.0.2.2	50:00:00:0e:00:00	8.8.8.8 (dns.google)
2 minutes ago	10.0.2.2	50:00:00:0e:00:00	8.8.8.8 (dns.google)
2 minutes ago	10.0.2.2	50:00:00:0e:00:00	8.8.8.8 (dns.google)
2 minutes ago	10.0.2.2	50:00:00:0e:00:00	54.189.35.180 (push.services.mozilla.com)
3 minutes ago	10.0.2.2	50:00:00:0e:00:00	34.120.208.123 (incoming.telemetry.mozilla.o...
3 minutes ago	10.0.2.2	50:00:00:0e:00:00	172.217.21.4 (www.google.com)

Let's Verify the routing table of Firewall FW1.

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	192.168.1.254	WAN (port1)	10	Static
10.0.1.0/24	0.0.0.0	LAN (port3)	0	Connected
10.0.2.0/24	10.0.1.2	LAN (port3)	10	Static
10.0.3.0/24	10.0.1.3	LAN (port3)	10	Static
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 (port1)	0	Connected
192.168.100.0/24	0.0.0.0	MGMT (port5)	0	Connected

```

CLI Console (1)
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 [10/0] via 192.168.1.254, port1, [1/0]
C 10.0.1.0/24 is directly connected, port3
S 10.0.2.0/24 [10/0] via 10.0.1.2, port3, [1/0]
S 10.0.3.0/24 [10/0] via 10.0.1.3, port3, [1/0]
C 10.0.4.0/24 is directly connected, VLAN40
C 10.0.5.0/24 is directly connected, VLAN50
C 192.168.1.0/24 is directly connected, port1
C 192.168.100.0/24 is directly connected, port5

```

```

FW1 # get router info routing-table details 10.0.2.0

Routing table for VRF=0
Routing entry for 10.0.2.0/24
Known via "static", distance 10, metric 0, best
* 10.0.1.2, via port3

FW1 # get router info routing-table details 10.0.3.0

Routing table for VRF=0
Routing entry for 10.0.3.0/24
Known via "static", distance 10, metric 0, best
* 10.0.1.3, via port3

```

Let's Verify the routing table of Firewall FW2.

The screenshot shows the FortiGate GUI for Firewall FW2. The left sidebar has 'Network' highlighted. The main area shows the 'Routing' page with two donut charts and a table of routes.

Routing Table:

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.0.1.254	WAN (port1)	10	Static
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
192.168.100.0/24	0.0.0.0	MGMT (port5)	0	Connected

```

CLI Console (1)
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
S* 0.0.0.0/0 [10/0] via 10.0.1.254, port1, [1/0]
C   10.0.1.0/24 is directly connected, port1
C   10.0.2.0/24 is directly connected, port2
C   192.168.100.0/24 is directly connected, port5

FW2 #
    
```

```

CLI Console (1)
FW2 # get router info routing-table details 8.8.8.8

Routing table for VRF=0
Routing entry for 0.0.0.0/0
  Known via "static", distance 10, metric 0, best
  * 10.0.1.254, via port1

FW2 #
    
```

Let's Verify the routing table of Firewall FW3.

The screenshot shows the FortiGate GUI for Firewall FW3. The left sidebar menu is expanded to 'Network'. The main content area displays the 'Routing' page for VRF=0. It features two donut charts showing the distribution of route types: 4 routes in total, with 3 Connected (green) and 1 Static (orange). Below the charts is a table of routes.

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.0.1.254	WAN (port1)	10	Static
10.0.1.0/24	0.0.0.0	WAN (port1)	0	Connected
10.0.3.0/24	0.0.0.0	LAN (port2)	0	Connected
192.168.100.0/24	0.0.0.0	MGMT (port5)	0	Connected

```

CLI Console (1)
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
S*   0.0.0.0/0 [10/0] via 10.0.1.254, port1, [1/0]
C    10.0.1.0/24 is directly connected, port1
C    10.0.3.0/24 is directly connected, port2
C    192.168.100.0/24 is directly connected, port5

FW3 #
    
```

```

CLI Console (1)
FW3 # get router info routing-table details 8.8.8.8

Routing table for VRF=0
Routing entry for 0.0.0.0/0
  Known via "static", distance 10, metric 0, best
  * 10.0.1.254, via port1

FW3 #
    
```

```
PC2
Applications Places System Thu May 5, 20:07
root@PC2: ~
File Edit View Search Terminal Help
root@PC2:~# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.0.2.254 (10.0.2.254)  4.750 ms  4.715 ms  4.701 ms
 2  10.0.1.254 (10.0.1.254)  9.570 ms  9.572 ms  9.562 ms
 3  192.168.1.254 (192.168.1.254)  9.812 ms  9.809 ms  9.801 ms
 4  172.29.129.254 (172.29.129.254)  9.961 ms  9.958 ms  9.950 ms
 5  192.168.100.1 (192.168.100.1)  11.122 ms  11.122 ms  11.114 ms
 6  84-235-86-35.saudi.net.sa (84.235.86.35)  16.899 ms  11.451 ms  14.235 ms
 7  10.188.193.68 (10.188.193.68)  14.234 ms  11.162 ms  13.207 ms
 8  10.188.193.43 (10.188.193.43)  32.668 ms  10.188.193.21 (10.188.193.21)  13.8
42 ms  10.188.193.43 (10.188.193.43)  13.842 ms
 9  10.188.195.73 (10.188.195.73)  30.723 ms  10.188.199.40 (10.188.199.40)  28.7
29 ms  10.188.199.44 (10.188.199.44)  28.684 ms
10  74.125.50.128 (74.125.50.128)  82.082 ms  82.036 ms  82.054 ms
11  108.170.252.241 (108.170.252.241)  82.047 ms * *
12  142.250.224.197 (142.250.224.197)  94.106 ms  172.253.67.155 (172.253.67.155)
73.768 ms dns.google (8.8.8.8)  83.309 ms
root@PC2:~#
```

```
PC3
Applications Places System Thu May 5, 20:08
root@PC3: ~
File Edit View Search Terminal Help
root@PC3:~# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.0.3.254 (10.0.3.254)  6.562 ms  6.514 ms  6.500 ms
 2  10.0.1.254 (10.0.1.254)  6.395 ms  6.414 ms  6.407 ms
 3  192.168.1.254 (192.168.1.254)  10.292 ms  10.520 ms  10.900 ms
 4  172.29.129.254 (172.29.129.254)  14.859 ms  15.301 ms  15.491 ms
 5  192.168.100.1 (192.168.100.1)  15.683 ms  15.851 ms  16.034 ms
 6  84-235-86-35.saudi.net.sa (84.235.86.35)  20.581 ms  11.412 ms  11.388 ms
 7  10.188.193.68 (10.188.193.68)  19.845 ms  20.045 ms  10.188.193.80 (10.188.19
3.80)  23.083 ms
 8  10.188.193.45 (10.188.193.45)  22.769 ms  10.188.193.43 (10.188.193.43)  12.0
11 ms  10.188.193.23 (10.188.193.23)  15.505 ms
 9  10.188.199.40 (10.188.199.40)  24.694 ms  30.501 ms  32.486 ms
10  72.14.197.0 (72.14.197.0)  83.701 ms  72.14.211.158 (72.14.211.158)  85.821 m
s  74.125.147.124 (74.125.147.124)  86.595 ms
11  74.125.244.225 (74.125.244.225)  83.664 ms * *
12  dns.google (8.8.8.8)  91.292 ms  91.315 ms  66.249.94.83 (66.249.94.83)  95.2
09 ms
root@PC3:~#
```