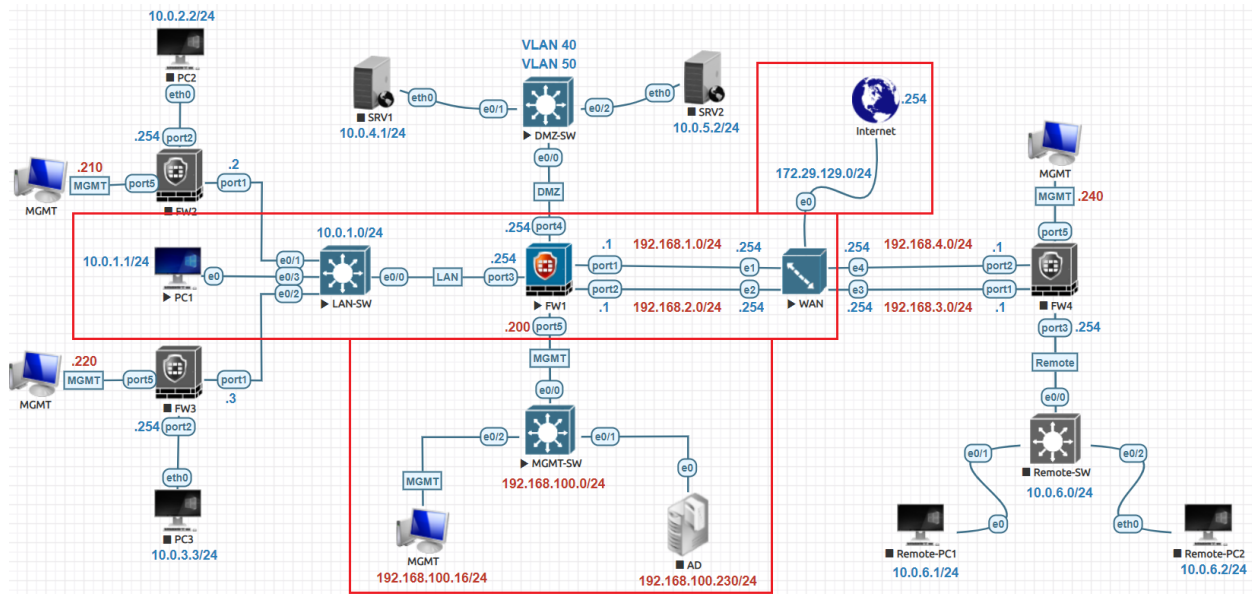


Initial Working Lab:



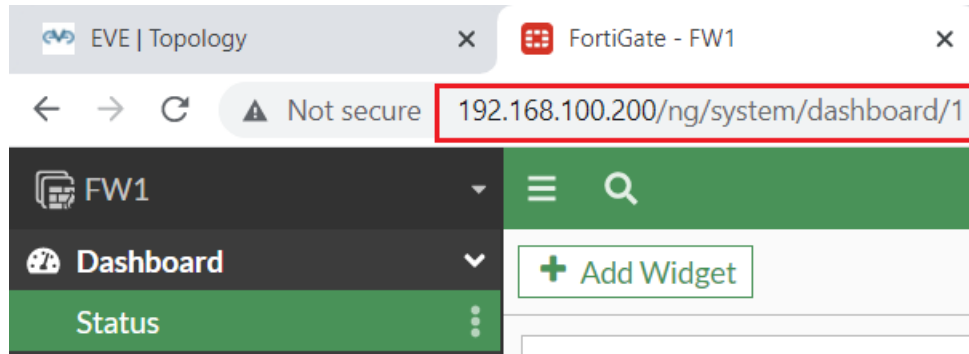
Change Hostname

```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FW1
FortiGate-VM64-KVM (global) # end
```

Configure Management Interface

```
FW1 # config system interface
FW1 (interface) # edit port5
FW1 (port4) # set mode static
FW1 (port4) # set ip 192.168.100.200/24
FW1 (port4) # set allowaccess https http ssh telnet ping
FW1 (port4) # end
```

Login to FortiGate Firewall type <http://192.168.100.200> in any browser.



Configure Interfaces:

Go to **Network>Interfaces** select **port1** Click **Edit**

The screenshot shows the FortiGate VM64-KVM configuration interface. The left sidebar is expanded to 'Network > Interfaces'. The main area displays a list of interfaces. The 'port1' interface is highlighted with a red box. The interface is a Physical Interface with IP/Netmask 192.168.1.102/255.255.255.0.

Name	Type	Members	IP/Netmask
802.3ad Aggregate 1			
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch
Physical Interface 6			
port1	Physical Interface		192.168.1.102/255.255.255.0

In **Alias** type **WAN**, change the Address Mode to **Manual** type **IP/Netmask 192.168.1.102/24**, in **Administrative access** uncheck everything only checked **PING** leave all the rest of configuration default and press **OK** button.

The screenshot shows the 'Edit Interface' configuration page for 'port1'. The 'Alias' is set to 'WAN', 'Addressing mode' is 'Manual', and 'IP/Netmask' is '192.168.1.102/255.255.255.0'. Under 'Administrative Access', 'PING' is checked. The 'OK' button is highlighted with a red arrow.

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: 192.168.1.102/255.255.255.0
Secondary IP address:
Administrative Access:
IPv4: HTTPS, HTTP, PING, SNMP, Security Fabric Connection
 FMG-Access, SSH
 FTM, RADIUS Accounting
 Speed Test
Receive LLDP: Use VDOM Setting Enable Disable
Transmit LLDP: Use VDOM Setting Enable Disable

Go to **Network>Interfaces** select **port3** Click **Edit**

Physical Interface 6			
port2	Physical Interface	0.0.0.0/0.0.0.0	
port3	Physical Interface	0.0.0.0/0.0.0.0	
port4	Physical Interface	0.0.0.0/0.0.0.0	PING HTTPS SSH HTTP TELNET
port5	Physical Interface	192.168.100.200/255.255.255.0	PING HTTPS SSH HTTP TELNET
port6	Physical Interface	0.0.0.0/0.0.0.0	

In **Alias** type **LAN**, change the Address Mode to **Manual** type **IP/Netmask 10.0.1.254/24**, in **Administrative access** only checked **PING** leave all the rest of configuration default & press **OK**.

The screenshot shows the 'Edit Interface' configuration for 'port3'. The 'Alias' is set to 'LAN'. The 'Addressing mode' is set to 'Manual' with an IP/Netmask of '10.0.1.254/24'. Under 'Administrative Access', the 'PING' checkbox is checked. The 'OK' button is highlighted with a red arrow.

Go to **Network>Interfaces** select **port5** Click **Edit**

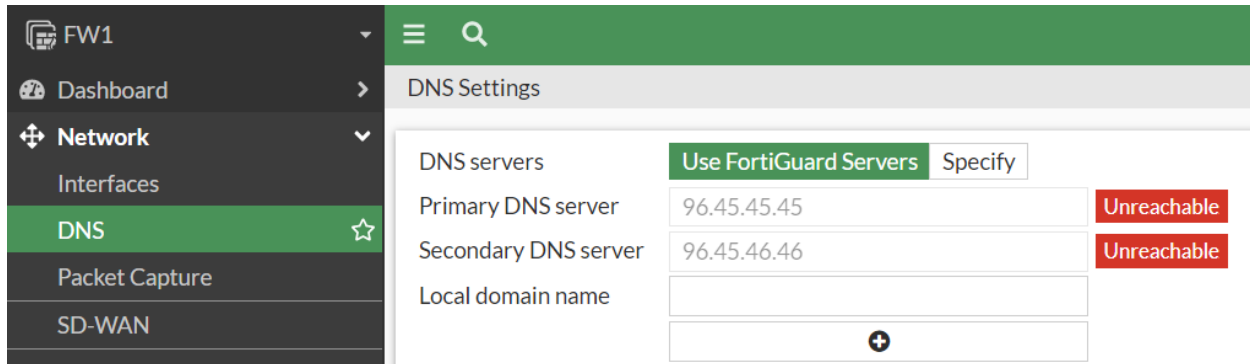
Physical Interface 6				
LAN (port3)	Physical Interface	10.0.1.254/255.255.255.0	PING	
port2	Physical Interface	0.0.0.0/0.0.0.0		
port4	Physical Interface	0.0.0.0/0.0.0.0	PING HTTPS SSH HTTP TELNET	
port5	Physical Interface	192.168.100.200/255.255.255.0	PING HTTPS SSH HTTP TELNET	

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 'Alias' field is set to 'MGMT'. The 'Type' is 'Physical Interface'. The 'VRF ID' is '0' and the 'Role' is 'Undefined'. The 'Dedicated Management Port' option is selected. The 'Addressing mode' is 'Manual' with the IP/Netmask '192.168.100.200/255.255.255.0'. The 'Administrative Access' section shows the following checked options: IPv4, HTTPS, HTTP, PING, TELNET, and Security Fabric Connection. The 'Receive LLDP' and 'Transmit LLDP' options are set to 'Use VDOM Setting'. The 'DHCP Server' option is not selected. The 'OK' button is highlighted with a red arrow.

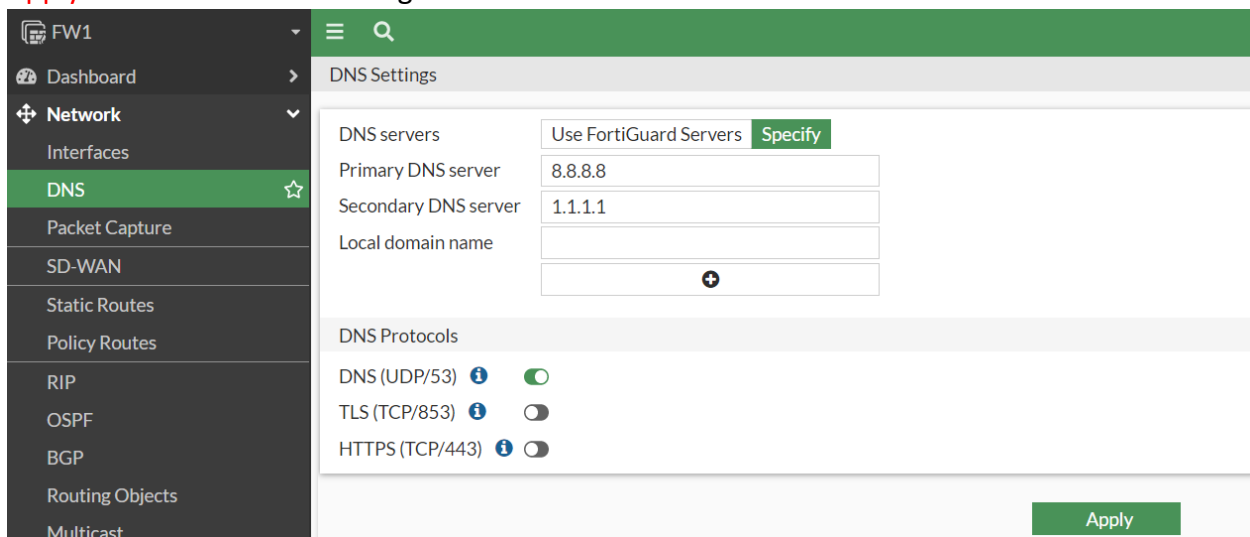
DNS Configuration:

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



The screenshot shows the FortiGate web interface for DNS Settings. The left sidebar is expanded to 'DNS'. The main panel shows 'DNS servers' set to 'Use FortiGuard Servers'. Below this, the 'Primary DNS server' is '96.45.45.45' and the 'Secondary DNS server' is '96.45.46.46', both with red 'Unreachable' status indicators. The 'Local domain name' field is empty. A '+ Add' button is visible at the bottom of the DNS servers list.

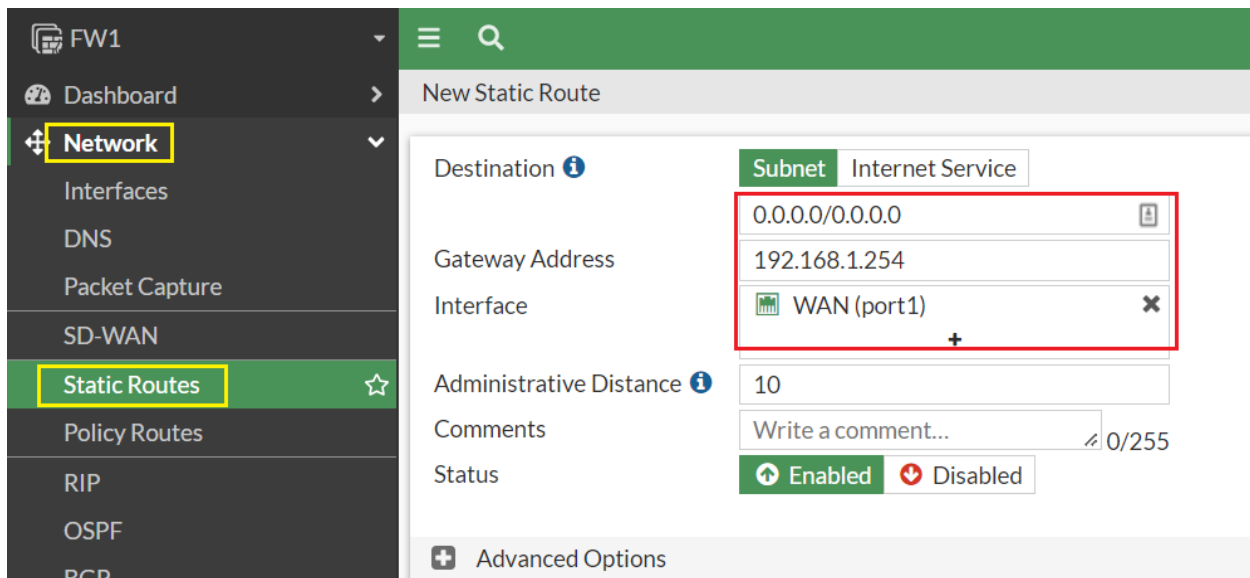
It is possible to specify using different DNS server, click on **Specify** and enter in primary / secondary DNS servers. In Primary DNS Server, type the IP address of the **primary DNS server 8.8.8.8**. In Secondary DNS Server, type the IP address of the **secondary DNS server 1.1.1.1**. Click **Apply**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



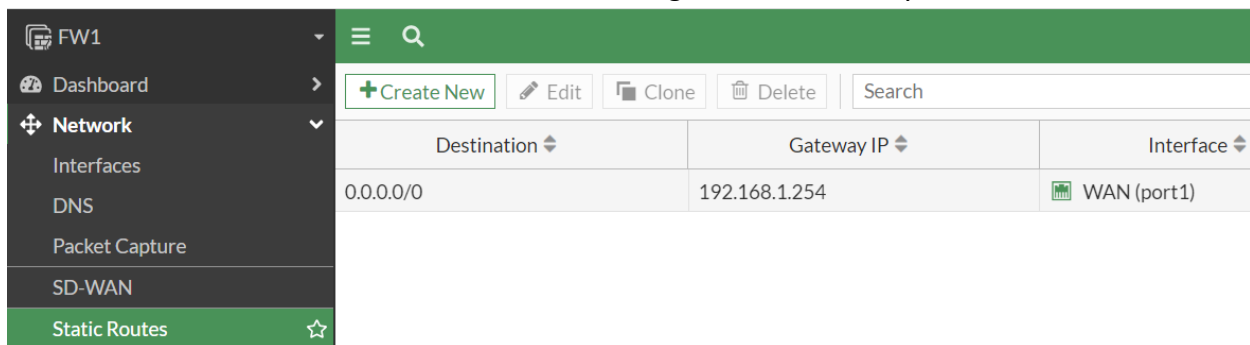
The screenshot shows the FortiGate web interface for DNS Settings after manual configuration. The 'DNS servers' section now shows 'Primary DNS server' as '8.8.8.8' and 'Secondary DNS server' as '1.1.1.1'. The 'Local domain name' field is empty. Below this, the 'DNS Protocols' section is visible with three options: 'DNS (UDP/53)' (checked), 'TLS (TCP/853)' (unchecked), and 'HTTPS (TCP/443)' (unchecked). An 'Apply' button is located at the bottom right of the settings panel.

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 **192.168.1.254** which the Gateway. Set the Interface to the **WAN** interface. Press **OK** to Save the changes.

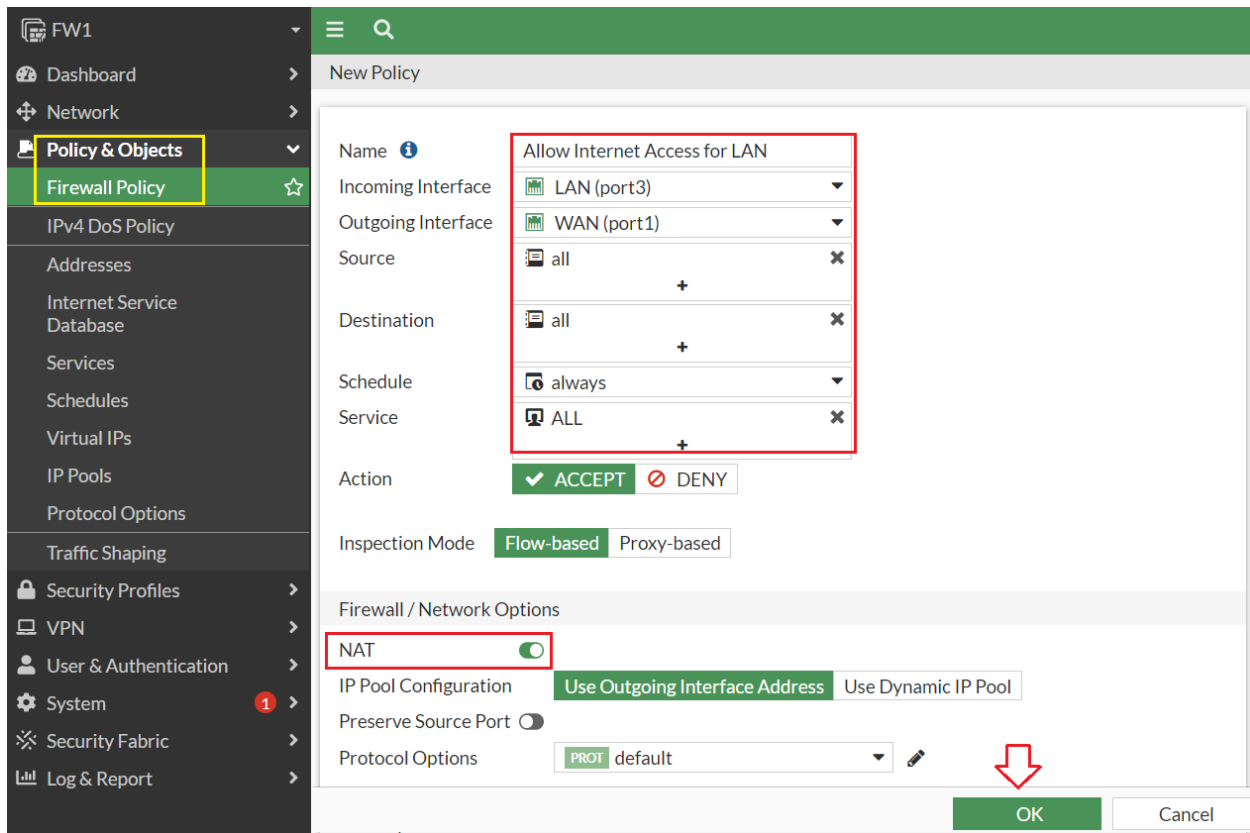


Go back to **Network > Static Routes** to see the configure routes, Finally, look like below.

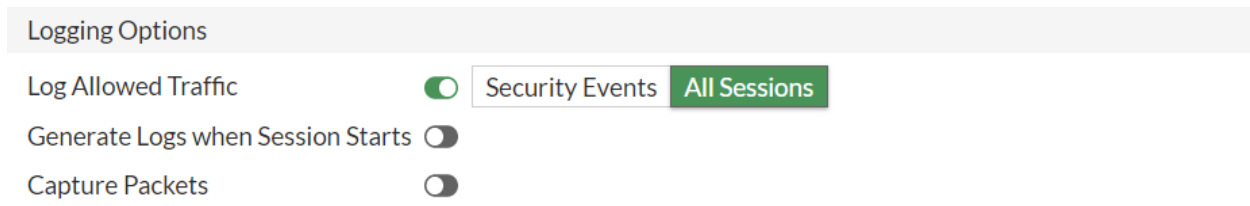


Creating a Policy:

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**.



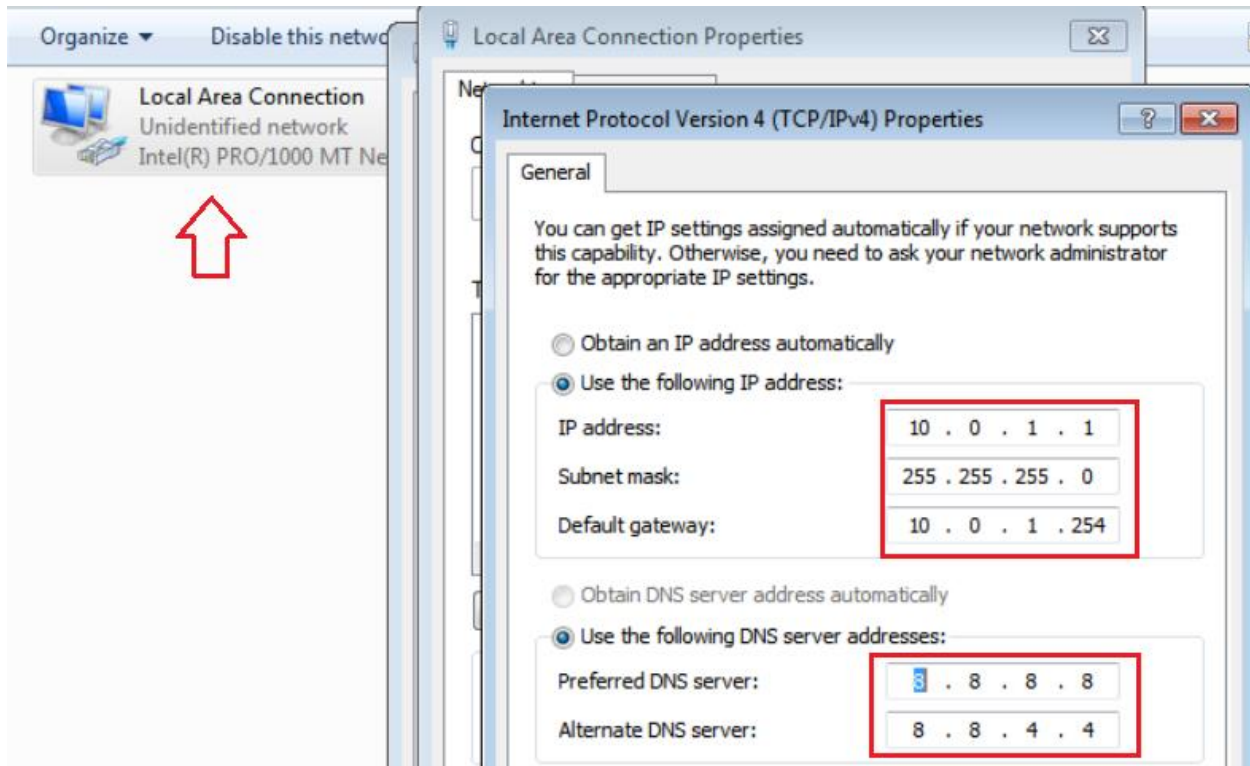
Scroll down to view the Logging Options. To view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



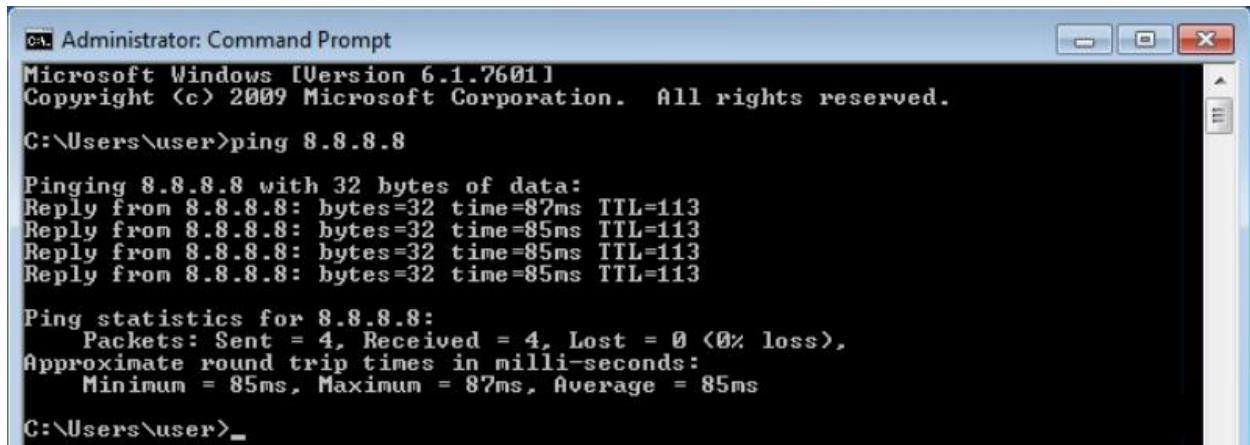
Go back to **Policy & Objects > Firewall Policy** to see the configure Policy, Finally, look like below.

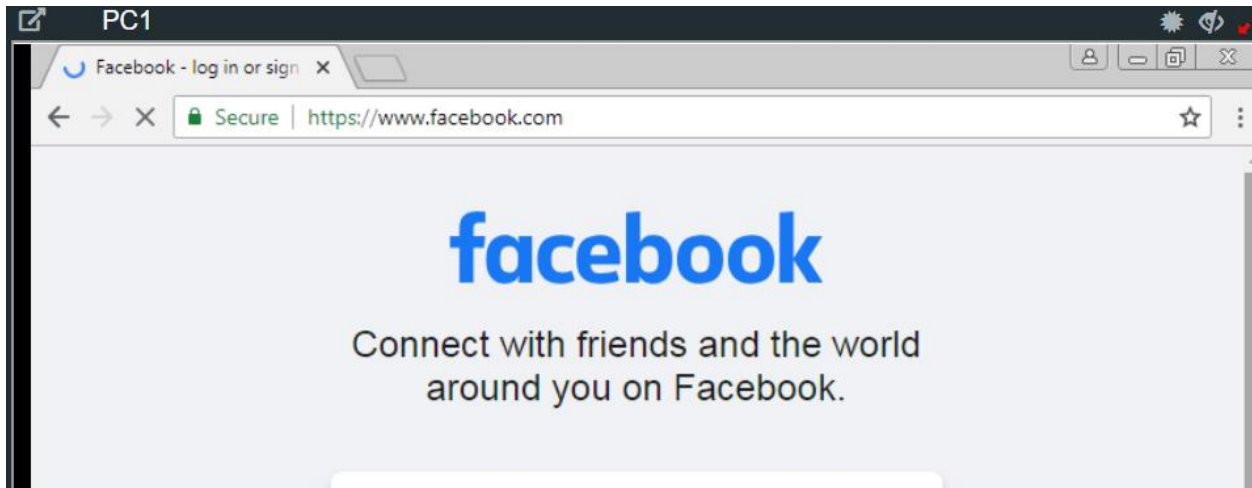
Name	Source	Destination	Schedule	Service	Action	NAT
LAN (port3) → WAN (port1) 1						
Allow Internet Access for LAN	all	all	always	ALL	ACCEPT	Enabled
Implicit 1						

Configure LAN PC:
assign static IP and details.



Browse the Internet using the PC on the internal network.





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

Source	Device	Bytes	Sessions	Bandwidth
10.0.1.1	USER-PC	2.66 MB	48	276.65 kbps

To view information about FortiGate traffic, go to **Dashboard > FortiView Destinations**. The appears on the list of Destinations.

Destination	Application	Bytes
www.google.com (142.250.200.196)	TCP/443	1.12 MB
clients2.googleusercontent.com (142.250.203.225)	TCP/443	1.07 MB
www.gstatic.com (216.58.212.99)	TCP/443	346.85 kB
edgedl.me.gvt1.com (34.104.35.123)		261.74 kB
ssl.gstatic.com (142.251.37.163)	TCP/443	237.39 kB

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

FortiView Sessions

+ Add Filter

Source	Device	Destination	Application	Protocol	Source Port
10.0.1.1	USER-PC	142.251.37.205	TCP/443	TCP	49171
10.0.1.1	USER-PC	142.251.37.174	TCP/443	TCP	49164
10.0.1.1	USER-PC	142.251.37.163	TCP/443	TCP	49174
10.0.1.1	USER-PC	142.251.37.163	TCP/443	TCP	49173
10.0.1.1	USER-PC	172.217.19.42	TCP/443	TCP	49172
10.0.1.1	USER-PC	172.217.19.35	TCP/443	TCP	49198
10.0.1.1	USER-PC	172.217.19.35	TCP/443	TCP	49197
10.0.1.1	USER-PC	172.217.21.14	TCP/443	TCP	49183

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

FortiView Policies by Bytes

+ Add Filter

Policy	Policy Type	Source Interface	Destination Interface
Allow Internet Access for LAN (1)	Firewall	LAN (port3)	WAN (port1)

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

Log & Report

Forward Traffic

+ Add Filter

Date/Time	Source	Device	Destination
24 seconds ago	10.0.1.1	USER-PC	142.250.203.225 (clients2.googleusercontent.com)
24 seconds ago	10.0.1.1	USER-PC	216.58.212.110 (clients2.google.com)
57 seconds ago	10.0.1.1	USER-PC	157.240.195.35 (www.facebook.com)