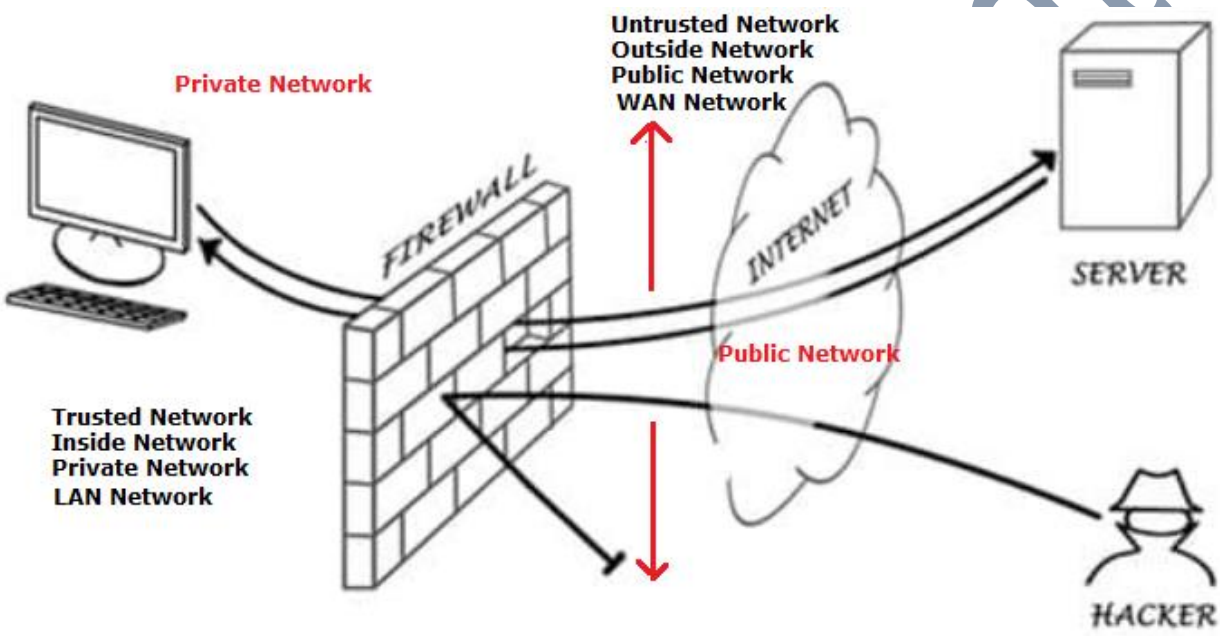
Firewall –

1. A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
2. A firewall is a one kind of device which replaced between trusted & untrusted network.
3. A firewall can be established between LAN network and WAN network, its depends on your requirement.
4. Using firewall we can prevents unauthorized users to access the network.
5. A firewall makes connection table but router doesn't make connection table.
6. We can replace to firewall in the place of router.



What can firewall do-

A firewall can do many things –

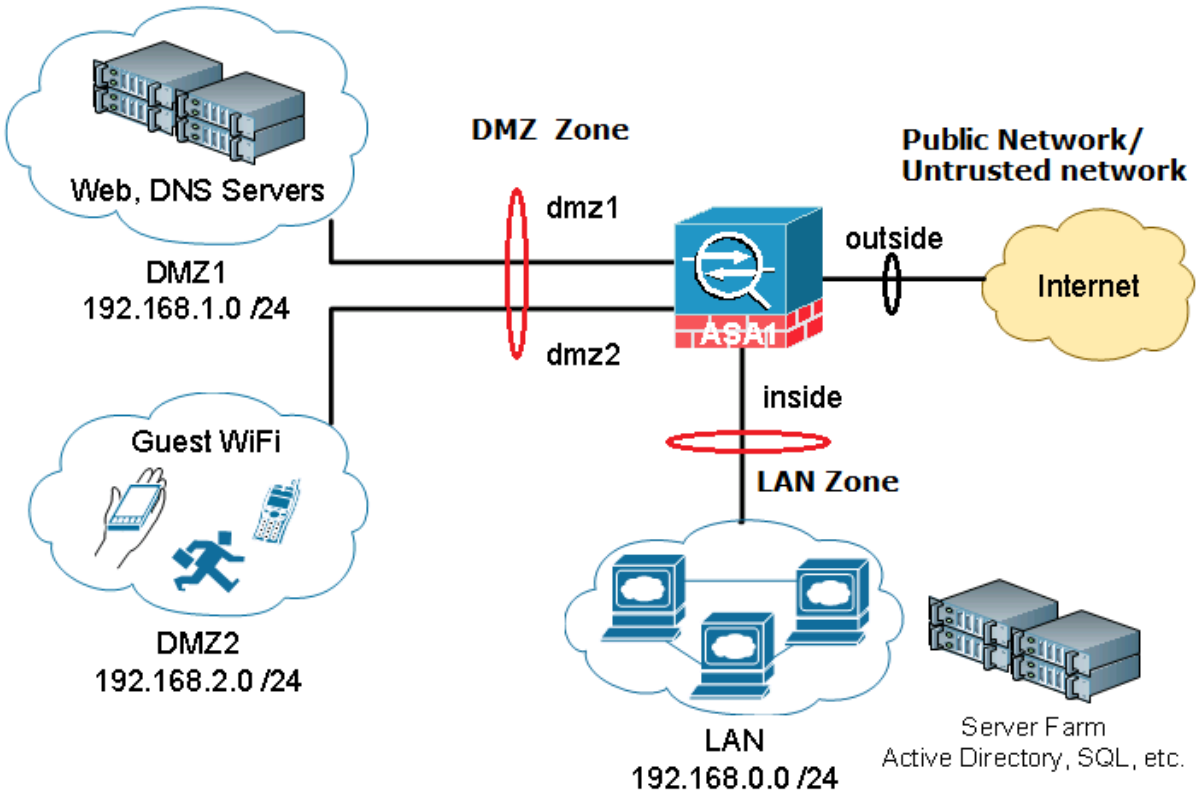
1. Make connection table
2. Filter incoming & outgoing traffic based on your requirements.
3. URL filtering / Web filtering
4. Provide IDS & IPS features.
5. VPN features
6. Filter packet up to 7 layers.
7. Antivirus & anti-spam features.
8. Application control

9. Data leak prevention
10. WAN optimization
11. Proxy based feature
12. DDOS Features
13. Deep level inspection features.

Many more features can have a next generation firewall.

DMZ- (Demilitarized zone)

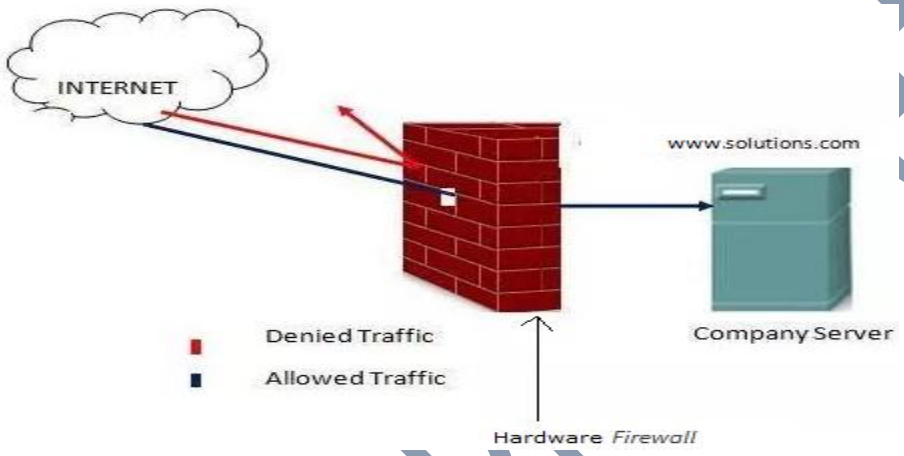
If any person or user is sitting outside world and he needs to access the database server or web server several times in a day of our organization and that server are available for 24 hours, then we make a zone behind the firewall that zone is called DMZ.



Firewall types – Firewall can be Hardware & Software base.

Hardware Firewall –

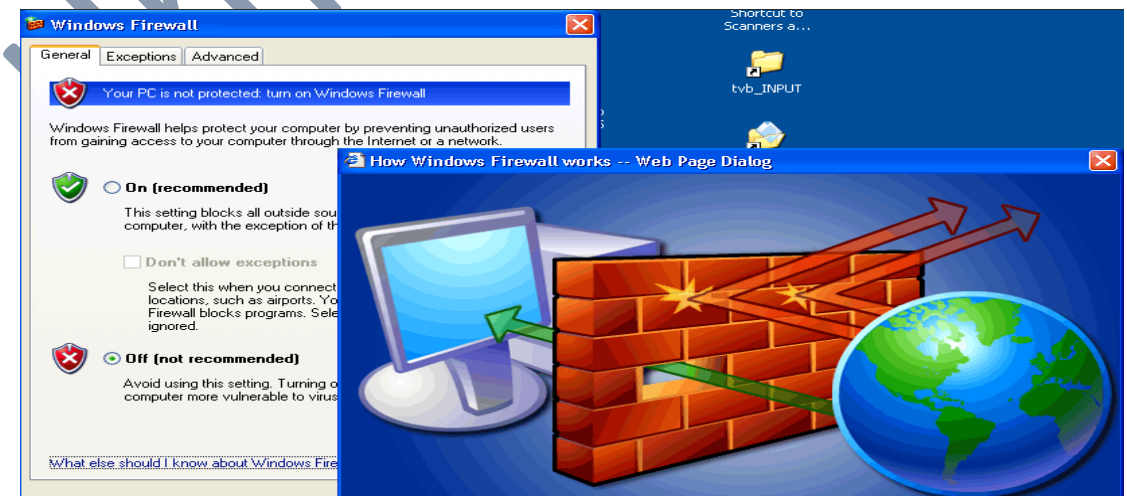
1. It is a physical device.
2. A hardware firewall acts as a gatekeeper/Gateway.
3. It sits directly behind the router/switch and can be configured to analyze incoming and outgoing traffic, filtering out specific threats as they come across the device.
4. Hardware firewall can be deployed as per your requirements. Such as – traffic's allowed or deny.



Software Firewall –

1. Firewall software is a tool that you can install on your device, the main use of a firewall software on your local computer is to monitor network traffic, using firewall software you can filter what traffic can get into your device and also what traffic can get out from your device, this process is accomplished by blocking the option for software to get out to the internet.

   Such as your windows PC firewall –



Stateless firewall & State full Firewall.

Stateless firewall -

1. Stateless firewall filters/inspect packet based on the source & destination IP and port no only.
2. Filter packet based on layer 3 & layer 4.
3. Router is a stateless firewall.
4. Easy to implement.
5. Performance delivery is very fast.
6. We can use firewall instead of router as firewall can do anything but router can't do.
7. Stateless firewall will not inspect that what is the source & destination IP, port number.
8. Does not inspect packet filtering based on – Antivirus, Application control. IDS & IPS, web filtering,
9. Doesn't make any connection table & session table that traffic goes through the firewall.

State full firewall –

1. State full firewall filters packet based on source & destination IP, port no, services such as – TCP/UDP packet.
2. Maintain session table.
3. Inspect packet up to layer 7 to layer 7.
4. If any suspicious traffic find during packet inspection firewall will block the traffic.
5. State full firewall provides features such as – Antivirus, Application control. Data leak prevention. IDS/IPS & web filtering.

Pointes –

1. IDS/IPS
2. WAF
3. SSL

IDS –

1. IDS stands for Intrusion Detection System.

2. An IDS is a system that monitors network traffic for suspicious activity and generates alerts or notification messages when such activity is discovered in the network.
3. Or you can say that it is one kind of tool or software application that scans a network or system activities or policy breaching which are harmful for our organization and inform to the administrator.
4. An intrusion detection system (IDS) is a tool or software that works with your network to keep it secure and flag when somebody is trying to break into your system.
5. If any suspicious traffic get detects in the network, IDS will just raise an alarm (to the administrator) but it will not be able to block the traffic.
6. IDS can be Hardware or software base.
7. An ID also detects malicious traffic.

Detection Method of IDS -

1. Signature-based Method
2. Anomaly-based Method
3. Reputation-based detection

IPS –

1. IPS stands for Intrusion Prevention system.
2. The major function of IPS is to identify the suspicious or malicious traffic and block to that traffic immediately when somebody is trying to break your network as it has capability to block the violated traffic based on predefined signature and generate a warning message to the administrator.
3. IPS can be Hardware or software application.
4. It has also ability to monitor the network traffic up to the layer 2 to layer 7.

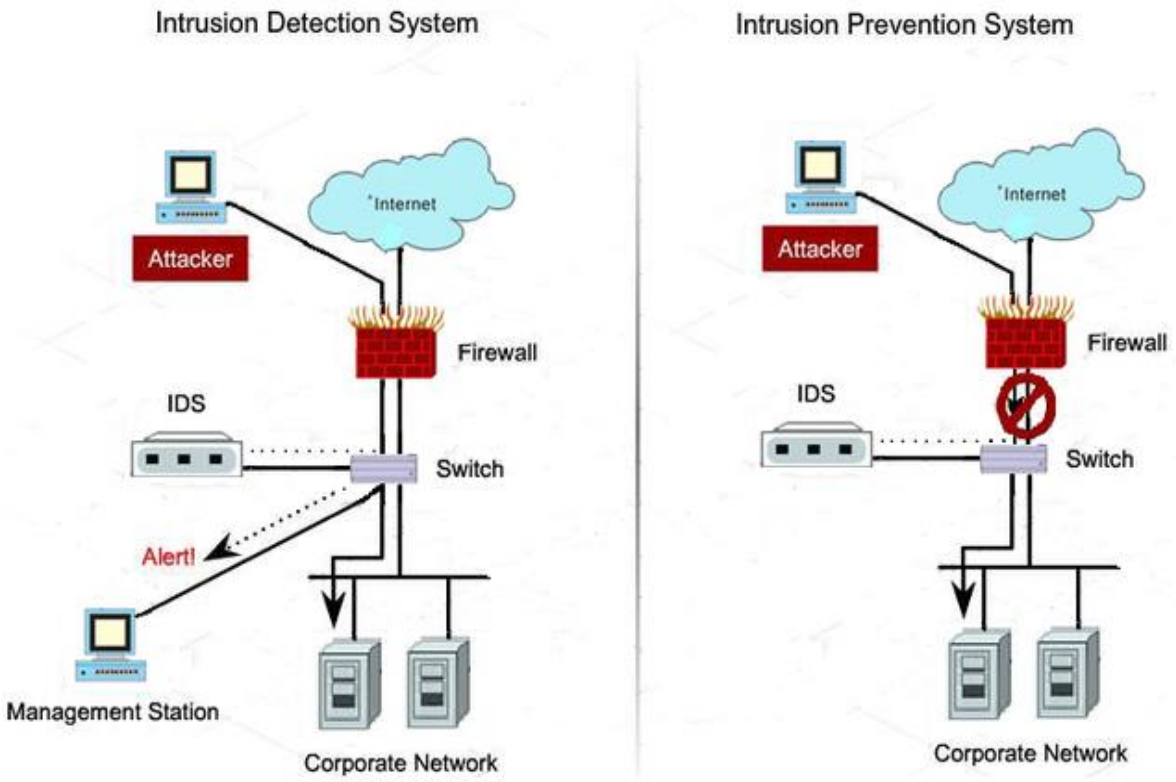
Detection Method of Intrusion Prevention System (IPS): -

1. Signature-based detection
2. Statistical anomaly-based detection
3. Stateful protocol analysis detection

What is signature in IDS and IPS –

- A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity, such as DDOS attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with predefined actions.

As here has been demonstrated a diagram to a little bit understand -



Firewall –

1. Firewall plays an essential role in Network Security.
2. A firewall is hardware or software based method that controls incoming and outgoing data traffic based on a set of guidelines that either permit or deny traffic on a network or host.
3. Firewalls should be used in every network as they monitor threats.

What is SSL -

Sorry this notes is the demo of Fortigate Firewall

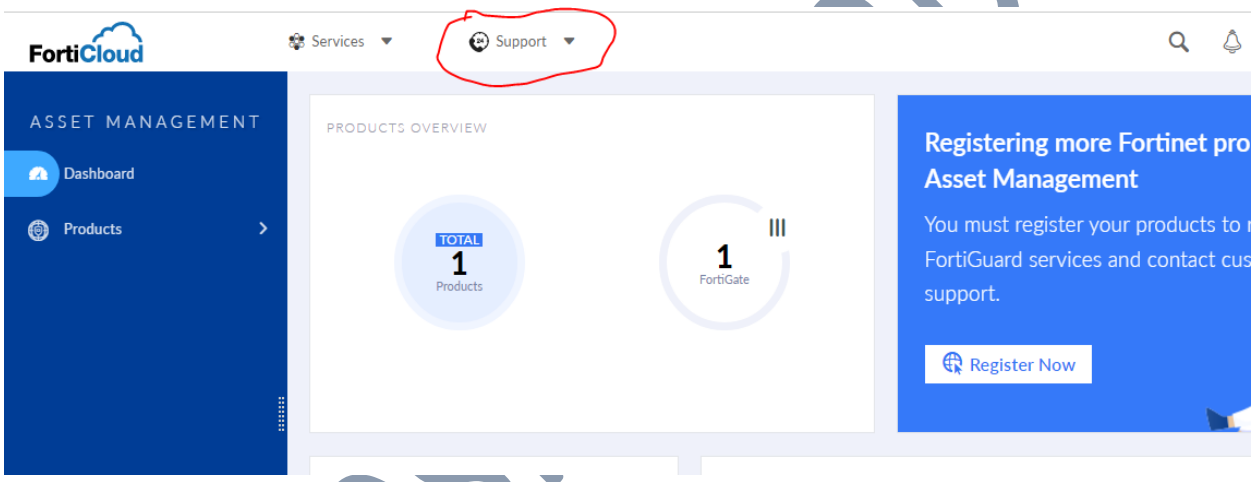
Fortigate Firewall 7.2.1 version installation Procedure in Gns3

Hello my dear friends in this article I am going to demonstrate you how to install Fortigate Firewall in Gns3, if you are fresher then it will be more useful for you all.

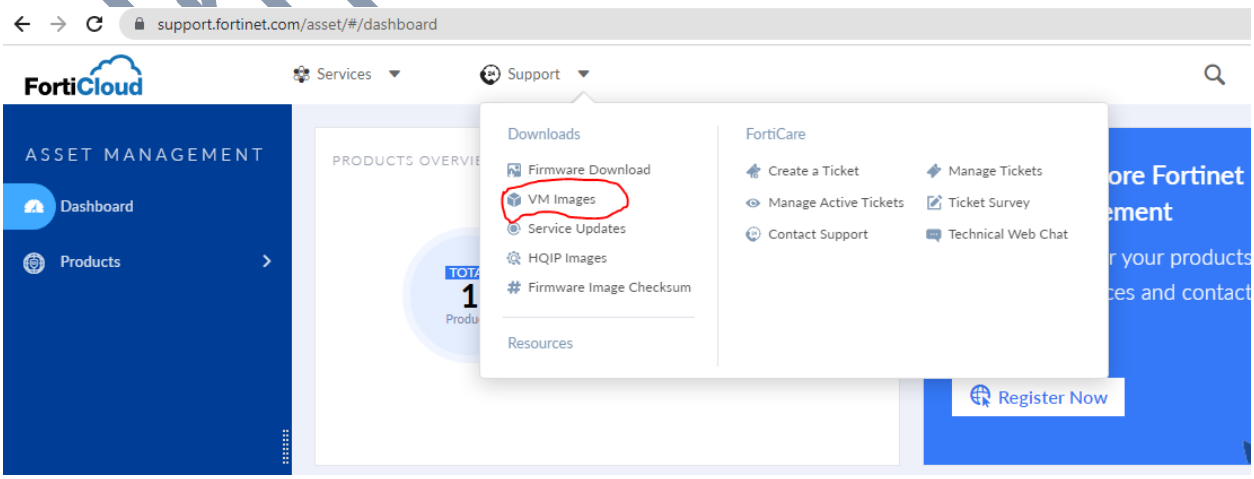
In order to install Fortigate OS in Gns3 make sure you should have an account in Fortigate portal. If you don't have account please go the below link and create an account first. https://support.fortinet.com/asset/#/

Once you create an account please follow the below procedure to download the Fortigate OS-

Step – 1

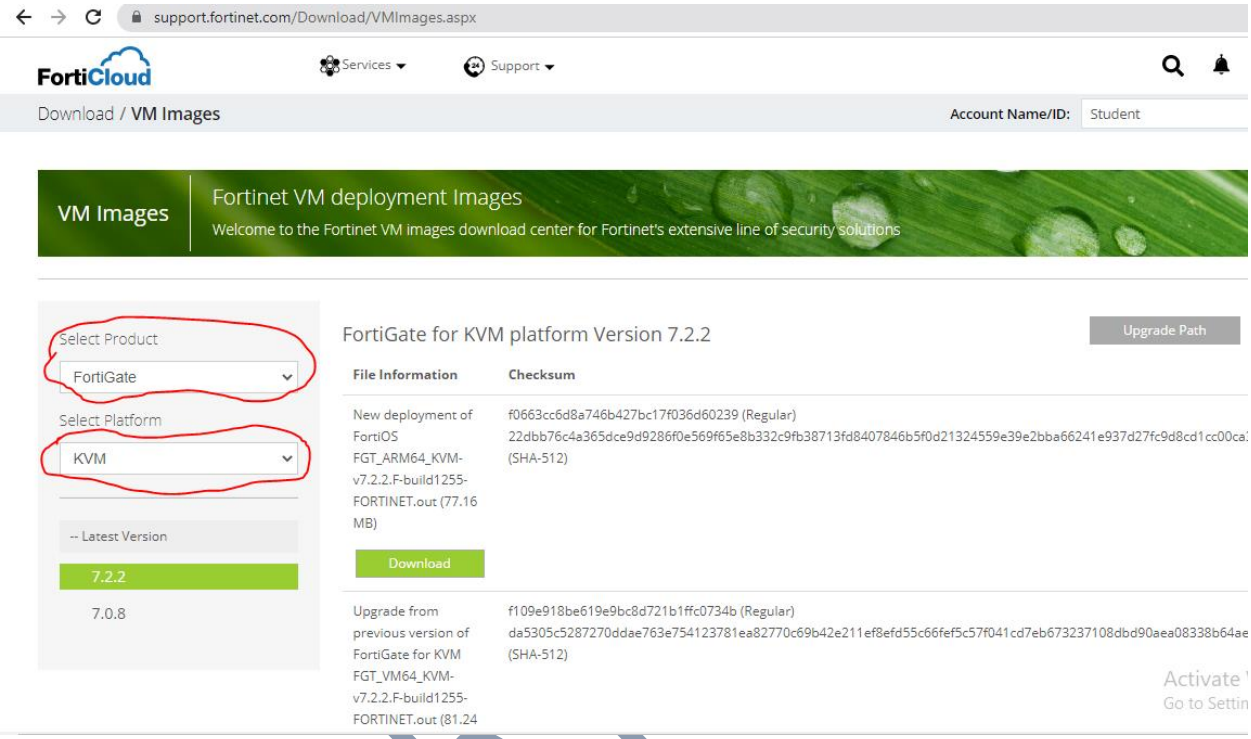


Step -2 Clicks on Vm image



Step -3 once you click on VM image page will redirect on Download/VM Images.

- Select Product Fortigate (By default will be selected Fortigate Product)
- Choose select platform KVM

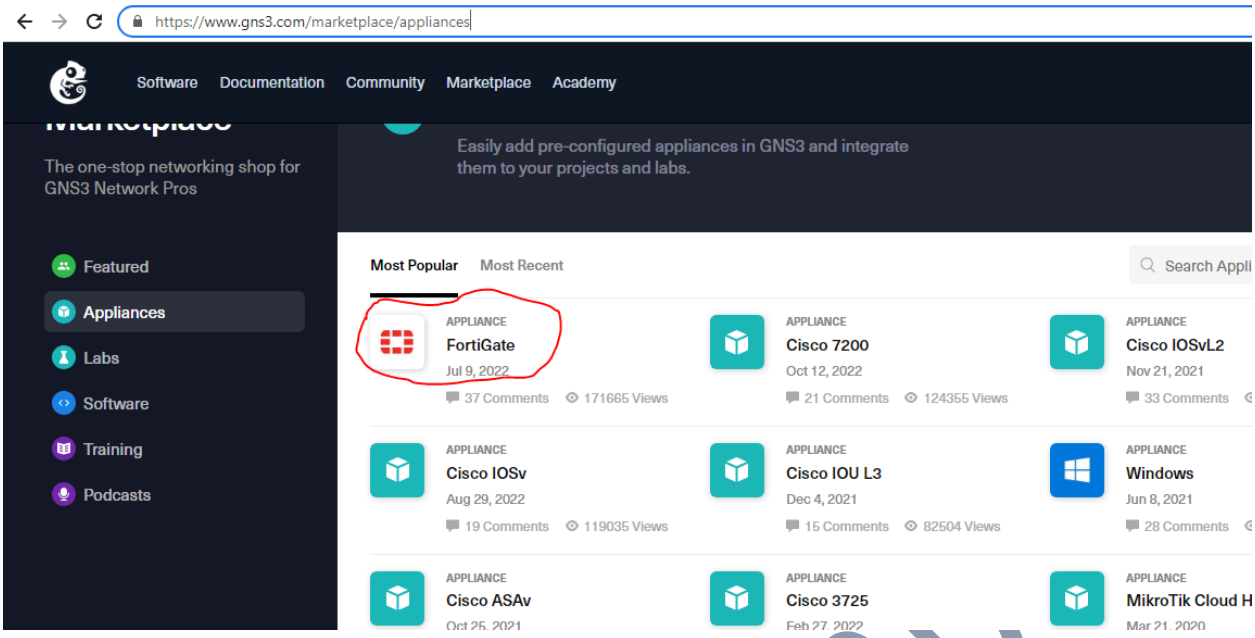


Here you can download any of the images as per your requirements; I mean any of the versions of the Fortigate Firewall.

Once you download it then go to Gns3 Fortigate official website to download one more image of Fortigate.

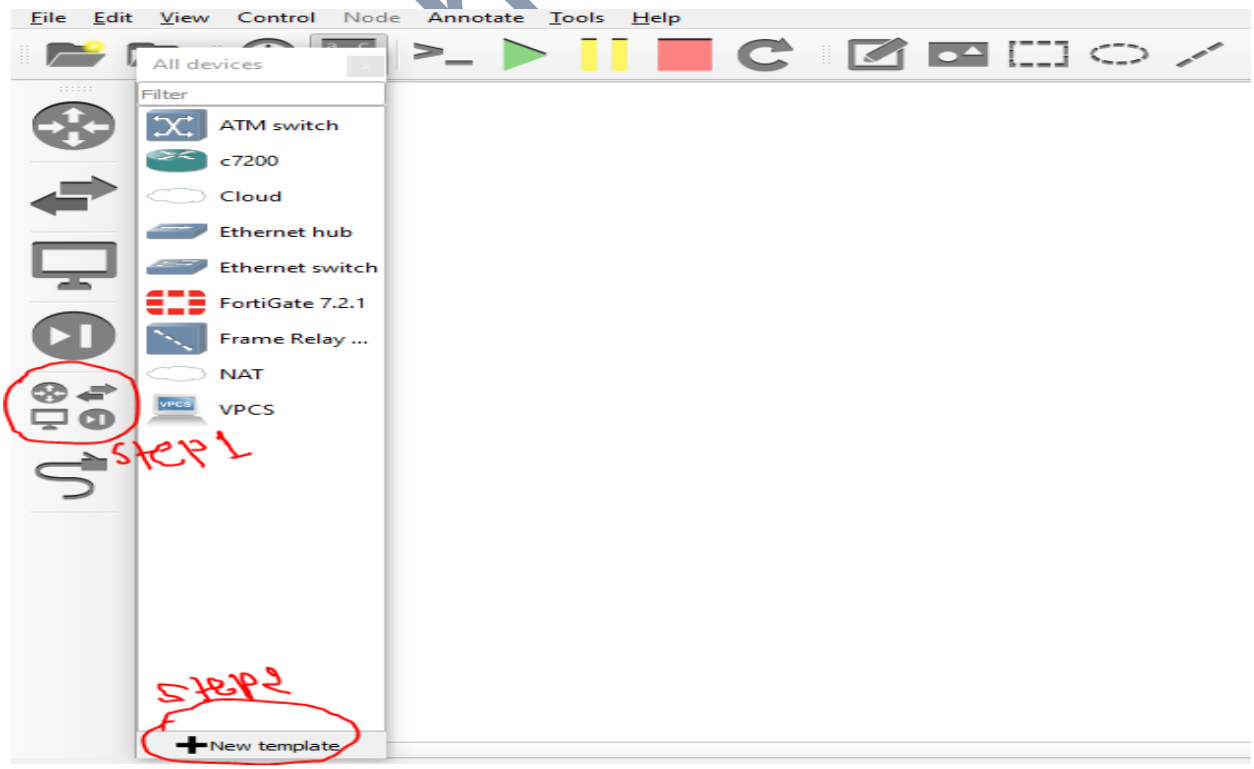
https://www.gns3.com/marketplace/featured (Gns3 portal)

1. Go to appliances.
2. Download Fortigate appliance

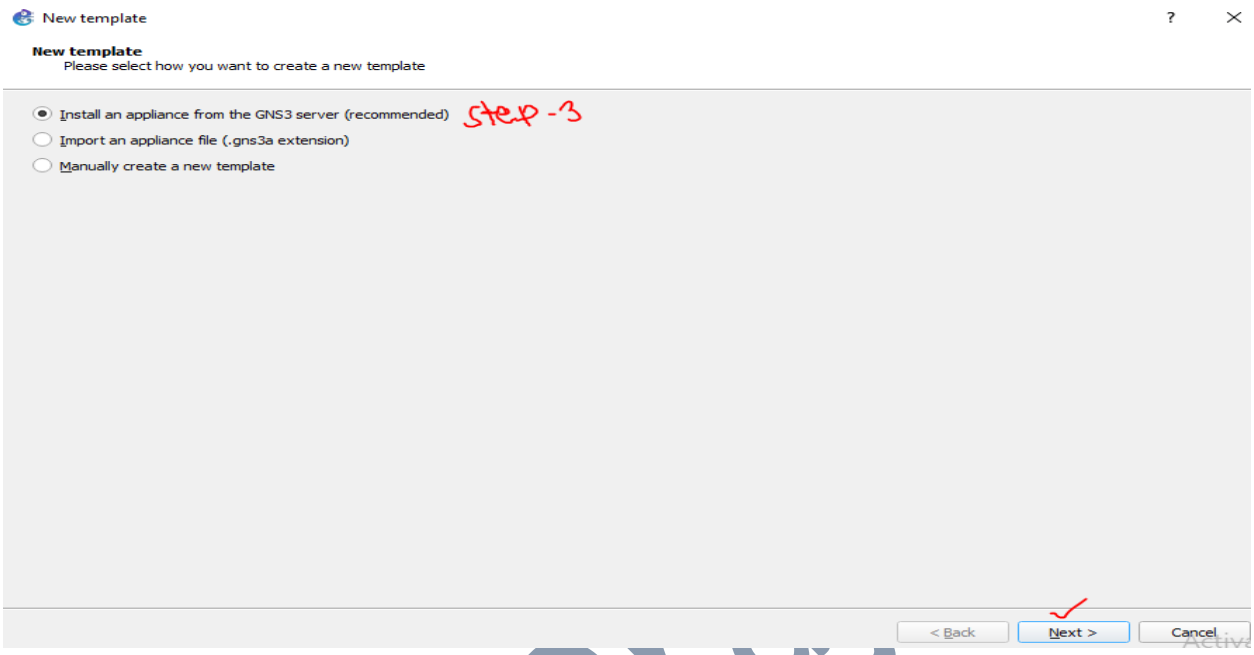


Now Fortigate Firewall installation process is getting started, therefore, please follow the below steps in Gns3.

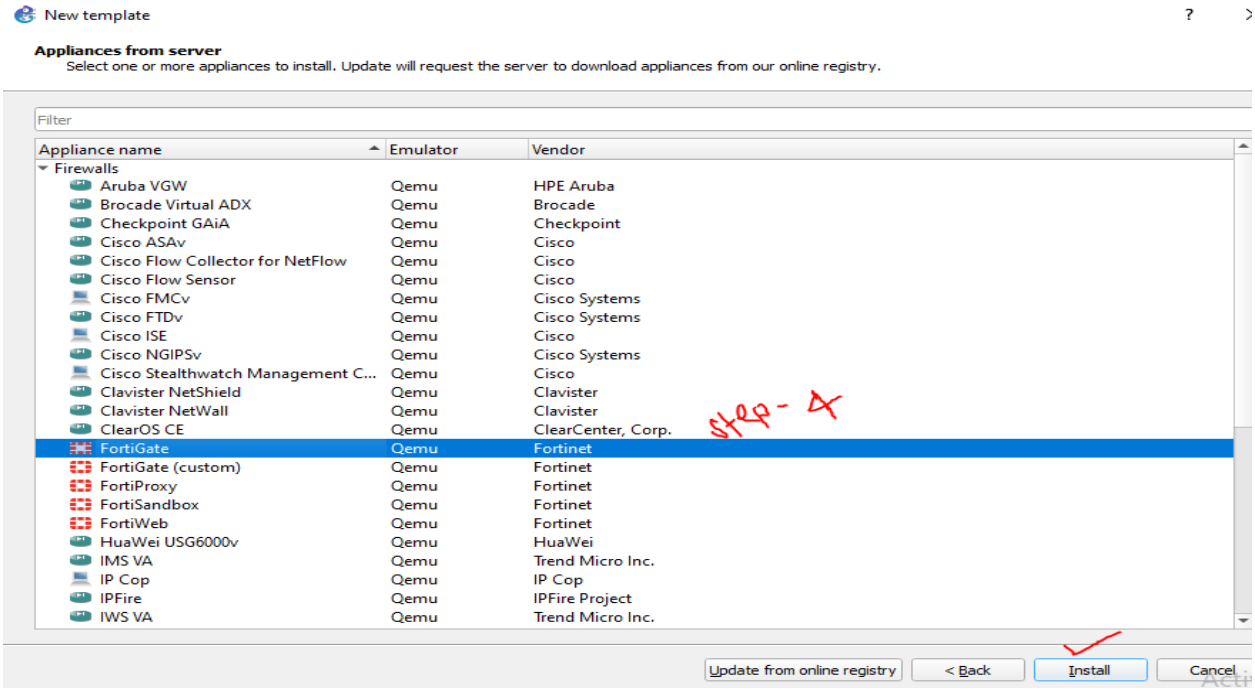
1. Open the Gns3 application
2. Go to browse all devices as per the below snapshots



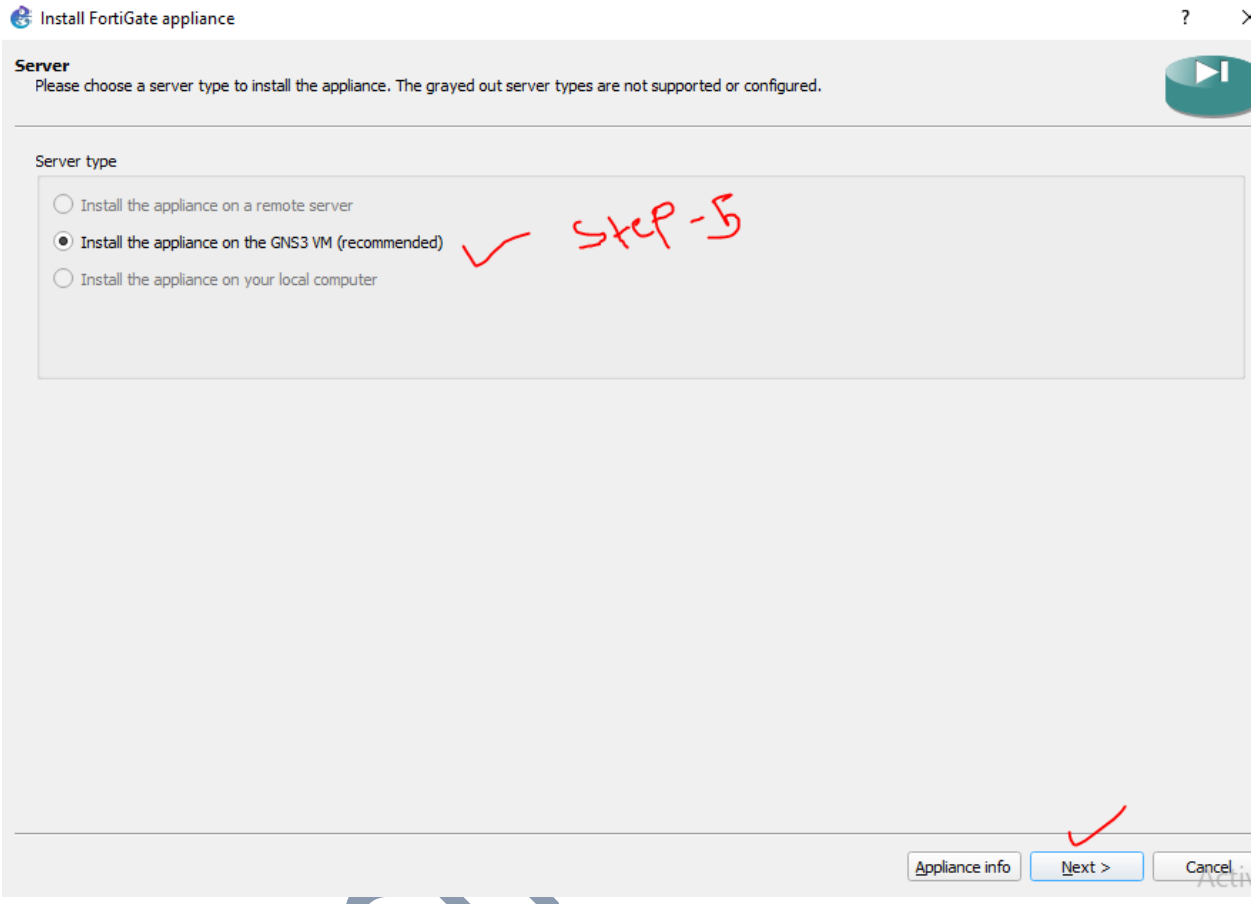
3. Click on new template then select install an appliance from the gns3 server.



4. Now select Firewall devices under the Firewall devices you have to choose Fortigate qemu, then install it.

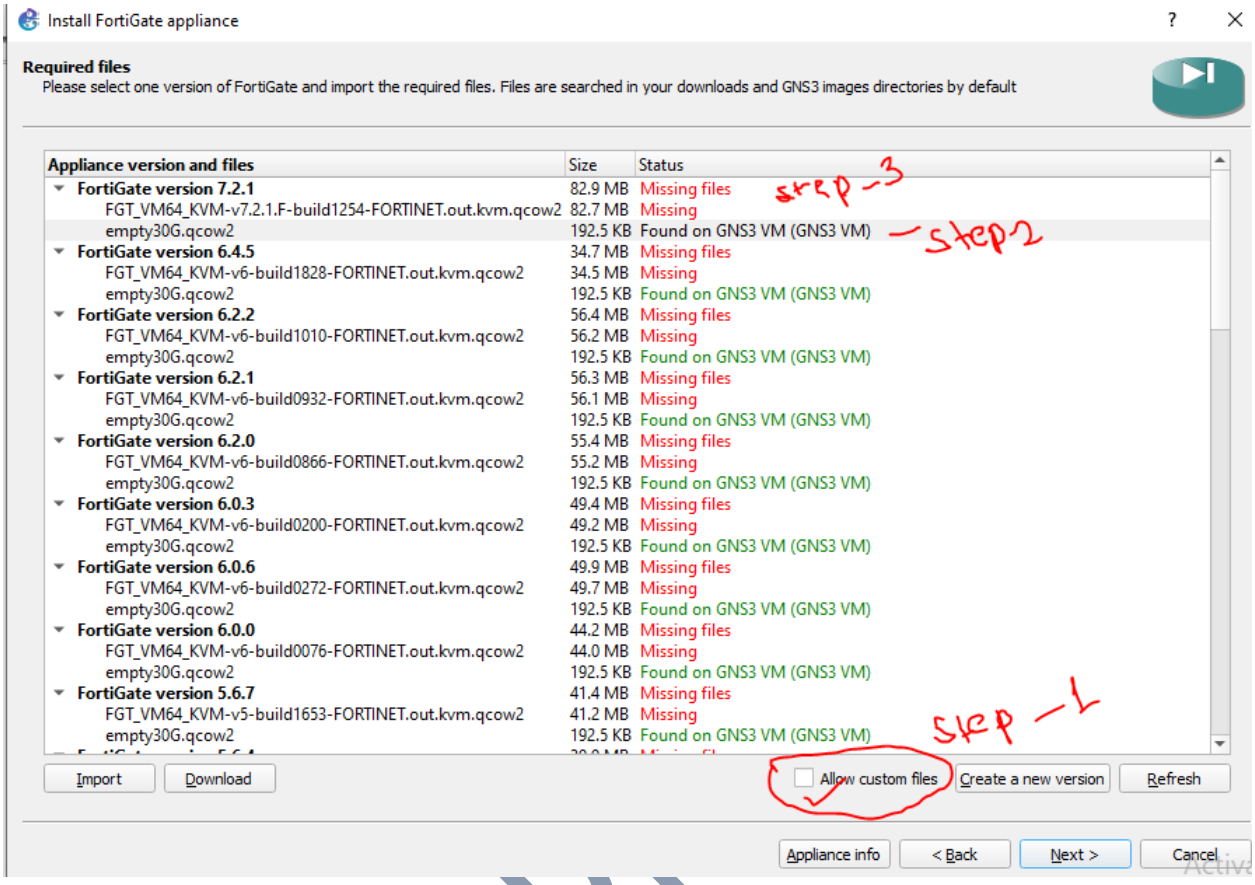


5. Choose Install the appliance on the Gns3 Vm (recommended) and the click next and next.

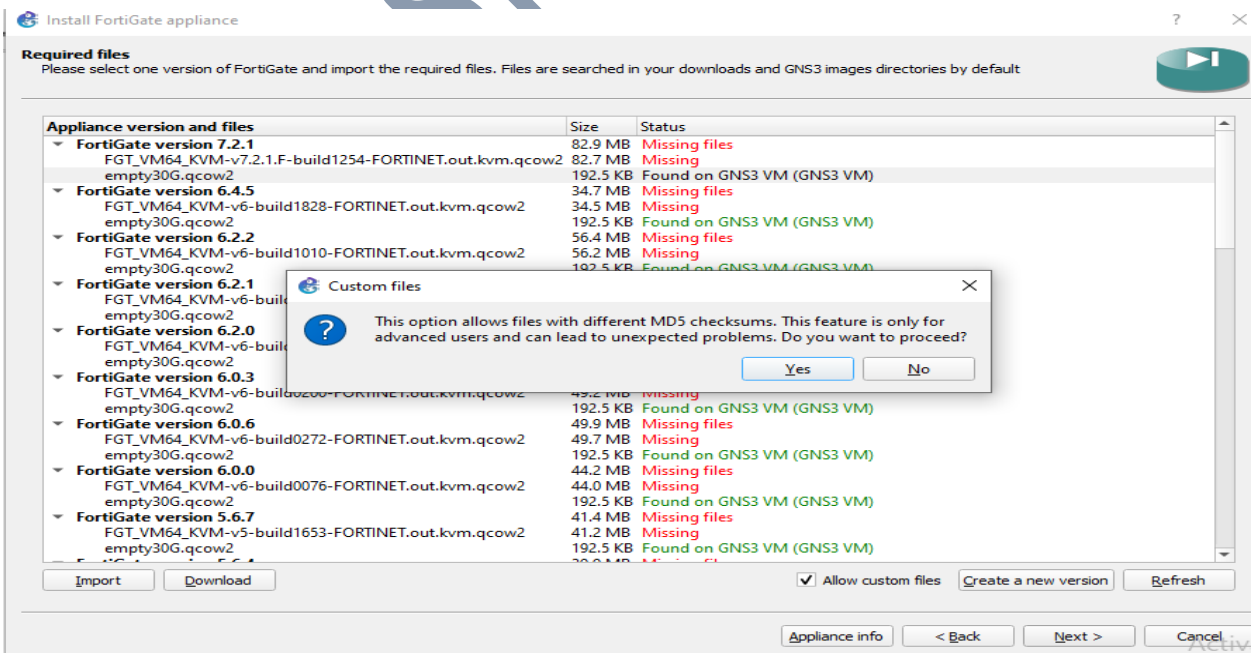


Now here you have to keep attention while selecting the images of gns3 and Fortigate which we have downloaded.

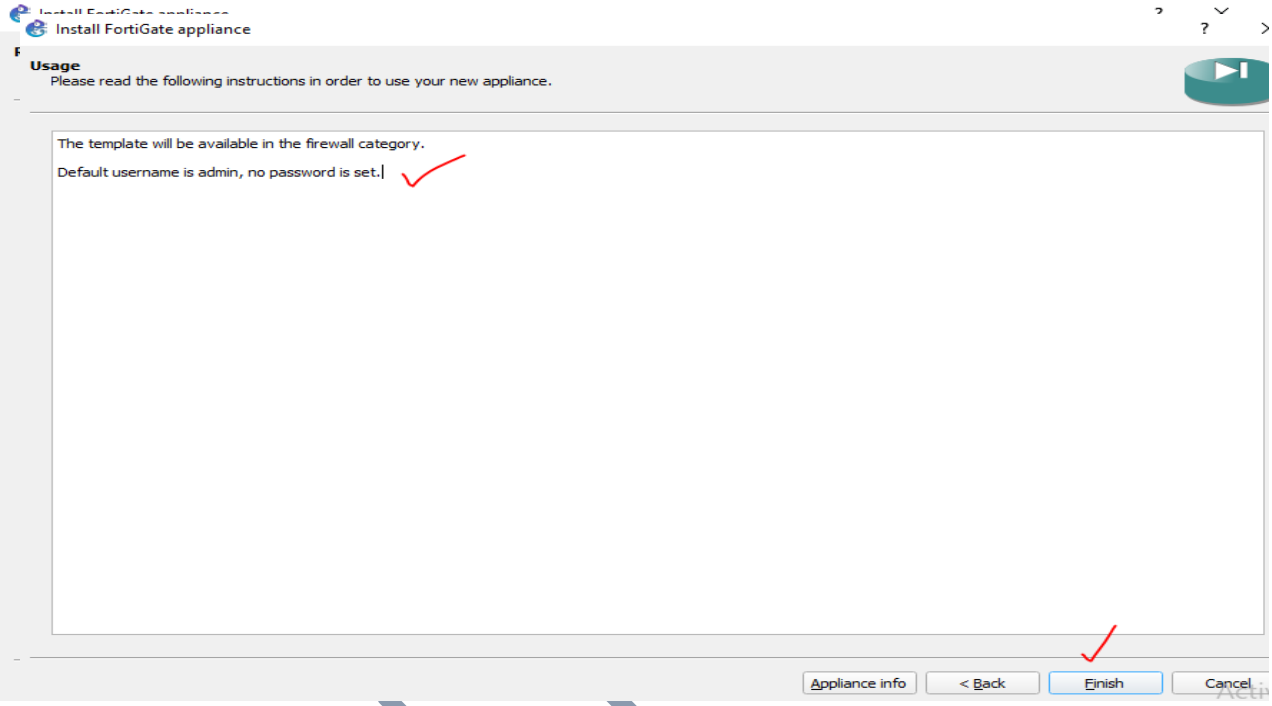
- Choose allow custom files first.
- Select Gns3 image
- Then select Fortigate image



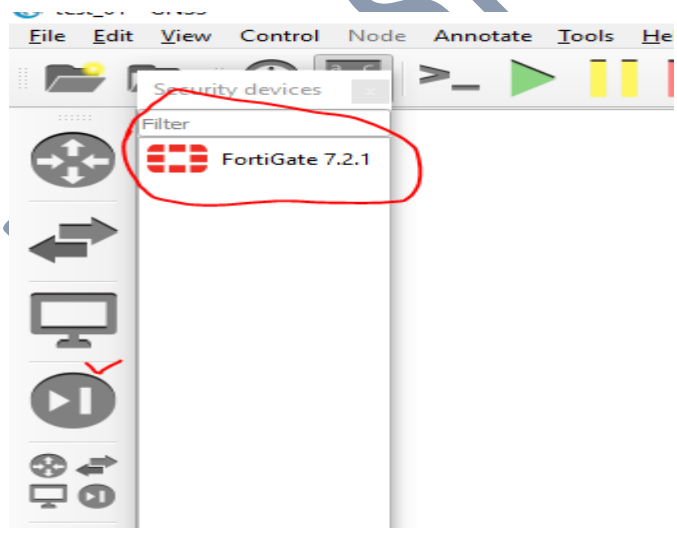
Once you click on – Allow custom files then it will show you a message the click yes.



6. Now you have to import gns3 appliance of Fortigate Firewall.
7. Then select Fortigate Firewall image which you have downloaded from the Fortigate official website. Now Fortigate Firewall has been successfully install in Gns3 then click next and Ok.



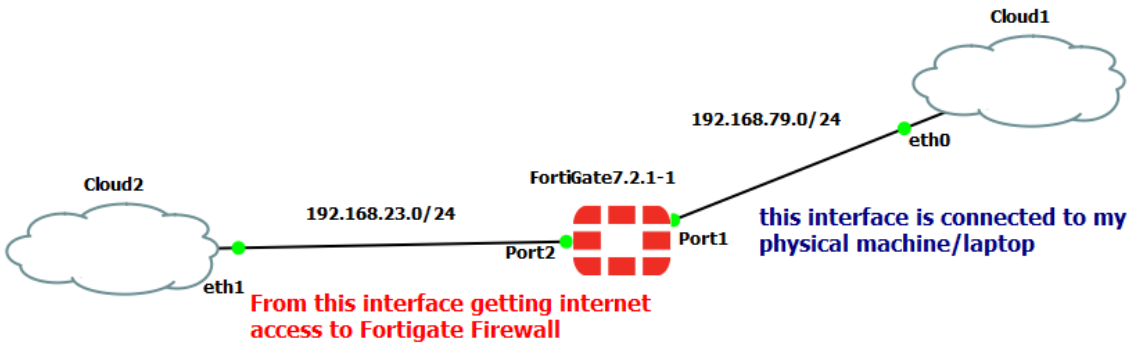
8. By default Fortigate has no password and username will be admin then click finish, then go to Gns3 Firewall option. Nice it has been installed.

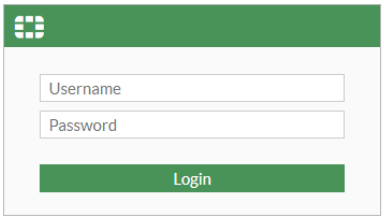


Note – Once Fortigate Firewall is installed in Gns3 then it will ask you evaluation license. (Fortigate provides free trials for 15 days only).

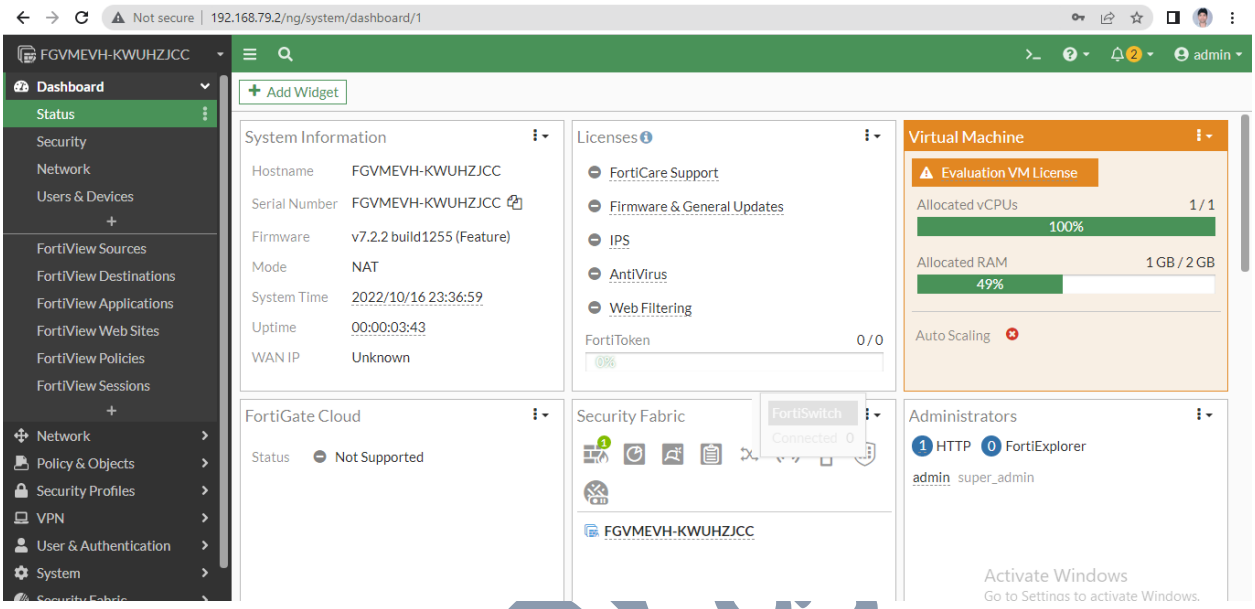
In order to access Fortigate in gns3 you have to connect one interface through your physical machine from where you can access the GUI and one interface should be connected through internet so that evaluation license can installed in Fortigate Firewall.

It will ask you registered email id and password – you may use your Fortigate account too. See the topology how I have designed in Gns3.





Note – First you have to configure management interface then you can access the GUI access of the Fortigate Firewall. Management interface can be configured using CLI.

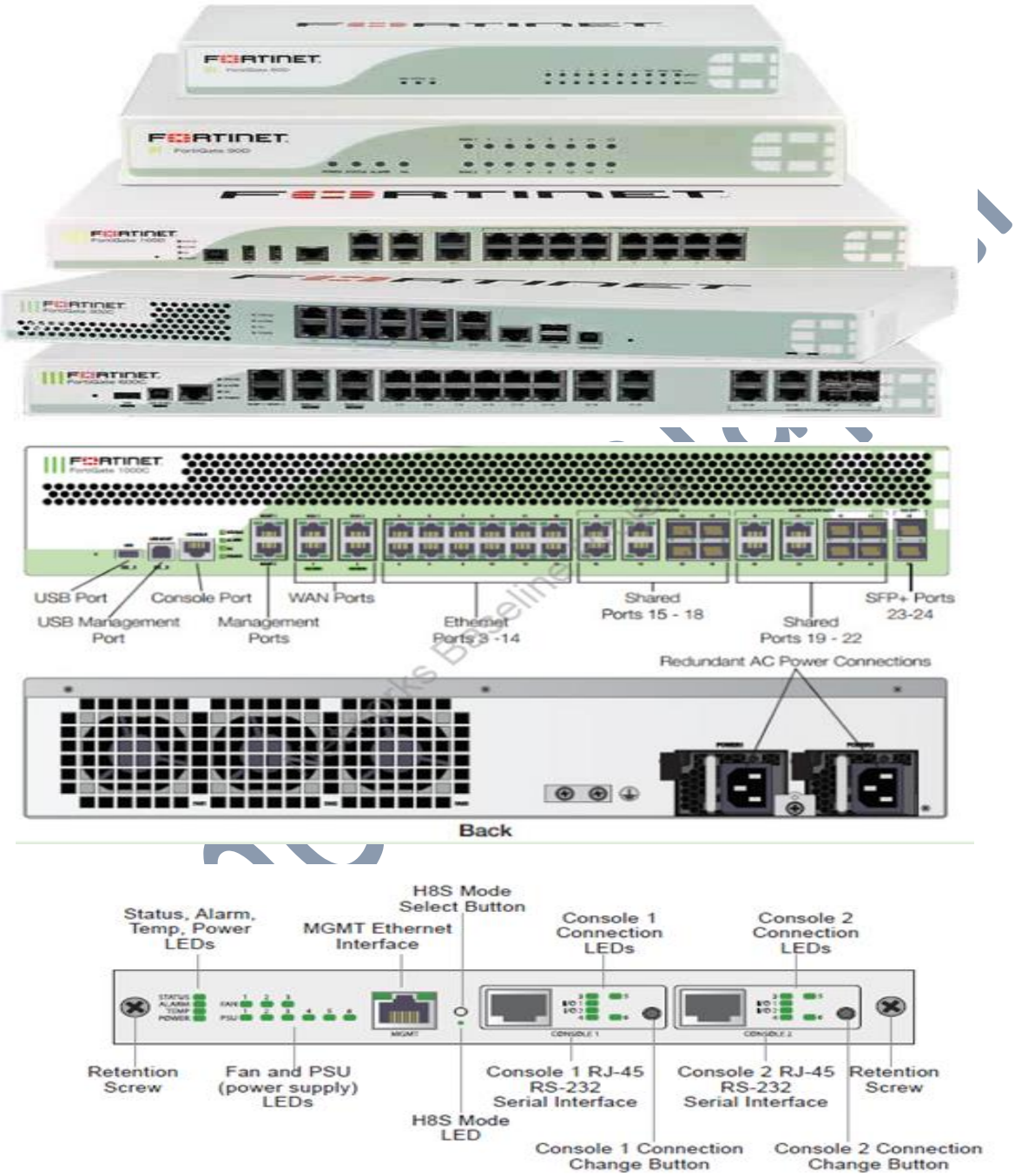


Thank you Fortigate Firewall installation process has been done you can see that in this image.

Thank you so much for reading this article – How to install Fortigate Firewall in Gns3.

Getting started Fortigate NGFW-

Let’s put one glimpse on fortigate firewall how it looks like.



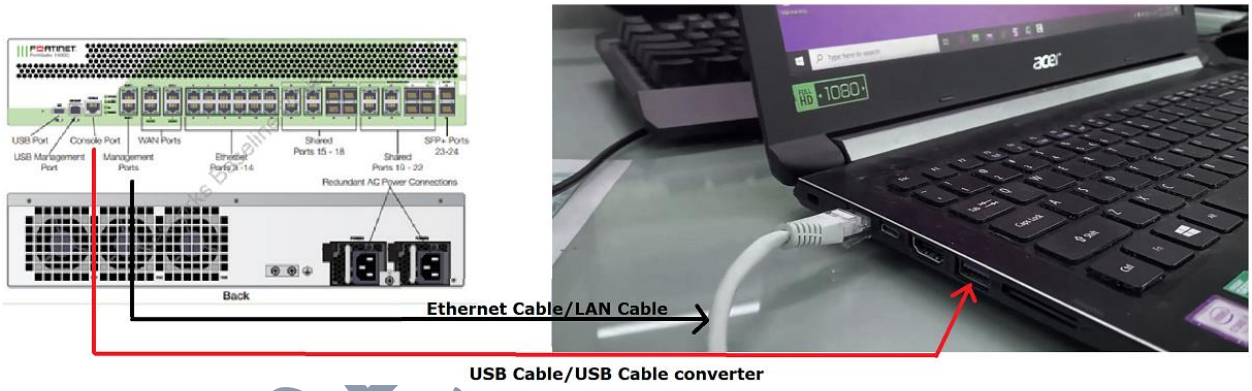
This article describes how to configure management port of the Fortigate firewall using console cable.

In order to configure management interface of Fortigate firewall you need to cables one the USB convert and other one is the Ethernet cable/LAN cable on which you will configure management ip.

Let me show you both cables right –

LAN/Ethernet Cable

USB Cable



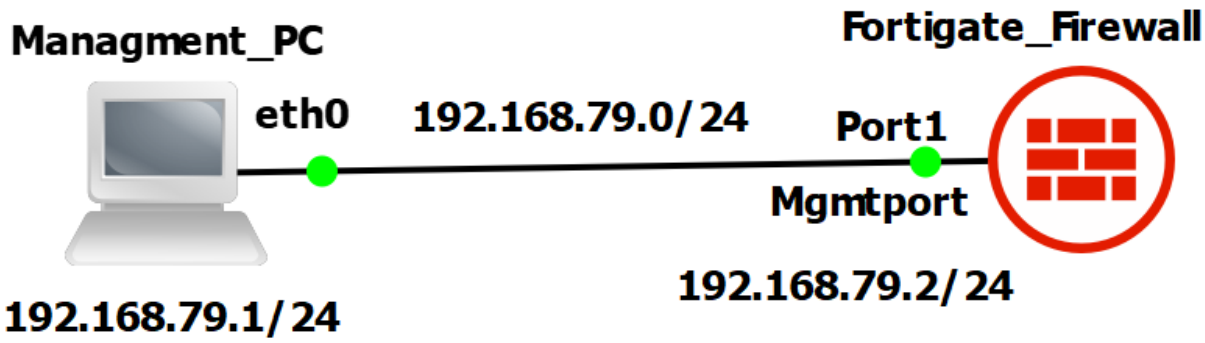
That's how you can connect Fortigate firewall to configure management interface using console cable along with LAN cable.

I would like to tell you that I don't have any hardware of Fortigate Firewall I will do the entire practical in simulator tool and that tool is GNS3.

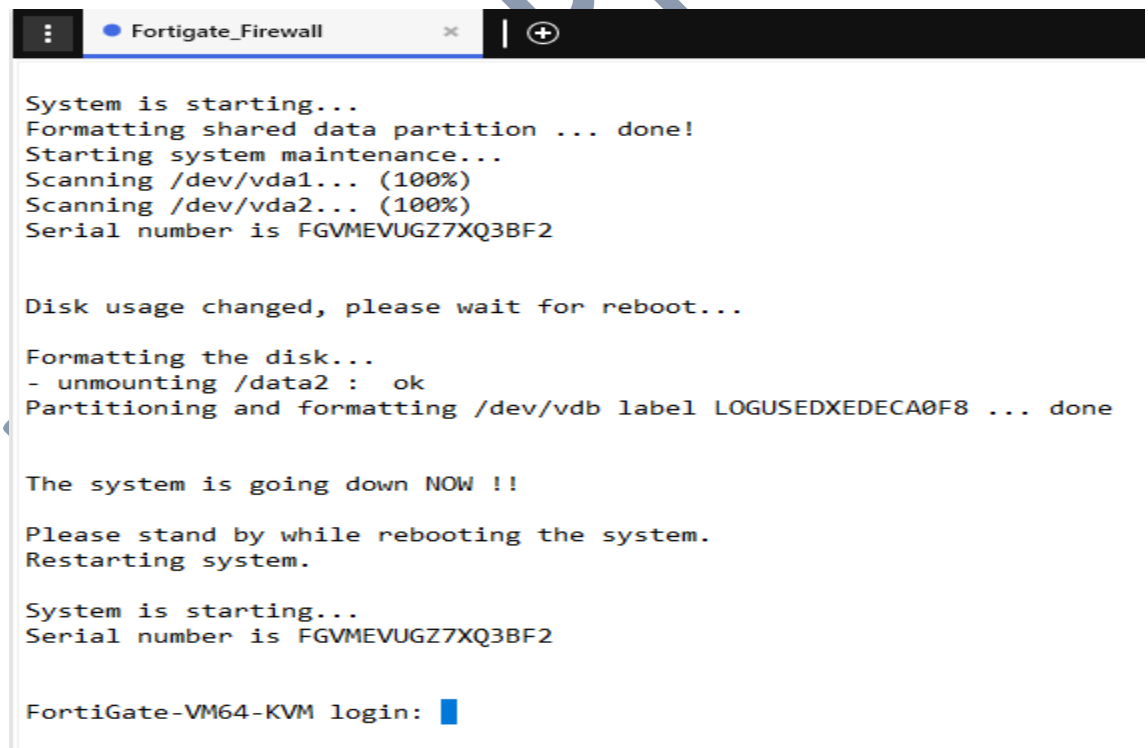
Let's move towards management interface configuration in GNS3.

I want to describe a little bit about this topology –

1. Port 1 is the management interface
2. Subnet/network must be same both side of the management interface to access the firewall.
3. From management PC will configure management IP.



As soon as you open putty you will see below out –



Then it will ask you username and password-

By default username – admin, there is no password you just need to press enter button of the keyboard after that you will have to enter password.

```
FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password, please input a new password.
New Password:***
Confirm Password:***
Welcome !

FortiGate-VM64-KVM #
```

Now in my case password has been set-

Username – admin

Password – 123 (password must be strong)

Change host name –

FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname Fortigate
Fortigate #

```
Fortigate # config system global

Fortigate (global) # set hostname Fortigate

Fortigate (global) # end

Fortigate #
```

Management IP address configuration-

Fortigate # config system interface
Fortigate (interface) # edit port1
Fortigate (port1) # set mode static
Fortigate (port1) # set ip 192.168.79.2/24
Fortigate (port1) # set allowaccess ping http https ssh snmp radius-ac
Fortigate (port1) # set description mgmtint

Fortigate (port1) # end
Fortigate #

```
Fortigate # config system interface

Fortigate (interface) # edit port1

Fortigate (port1) # set mode static

Fortigate (port1) # set ip 192.168.79.2/24

Fortigate (port1) # set allowaccess ping http https ssh snmp radius-ac

Fortigate (port1) # set description mgmtint

Fortigate (port1) # end
```

To verity the IP address whether it has been configured or not-

```
Fortigate # config system interface

Fortigate (interface) # show
config system interface
    edit "port1" ✓
        set vdom "root"
        set ip 192.168.79.2 255.255.255.0 ✓
        set allowaccess ping https ssh snmp http radius-acct ✓
        set type physical ✓
        set description "mgmtint" ✓
        set snmp-index 1
    next
```

Now we need to check management IP is pingable from the Firewall Firewall or not-

```
Fortigate # execute ping 192.168.79.1
PING 192.168.79.1 (192.168.79.1): 56 data bytes
64 bytes from 192.168.79.1: icmp_seq=0 ttl=128 time=3.2 ms
64 bytes from 192.168.79.1: icmp_seq=1 ttl=128 time=5.2 ms
64 bytes from 192.168.79.1: icmp_seq=2 ttl=128 time=6.5 ms
64 bytes from 192.168.79.1: icmp_seq=3 ttl=128 time=4.1 ms
64 bytes from 192.168.79.1: icmp_seq=4 ttl=128 time=48.0 ms

--- 192.168.79.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.2/13.4/48.0 ms

Fortigate #
```

Yes, I am able to ping from the Fortigate Firewall, now it should be also ping from the management PC.

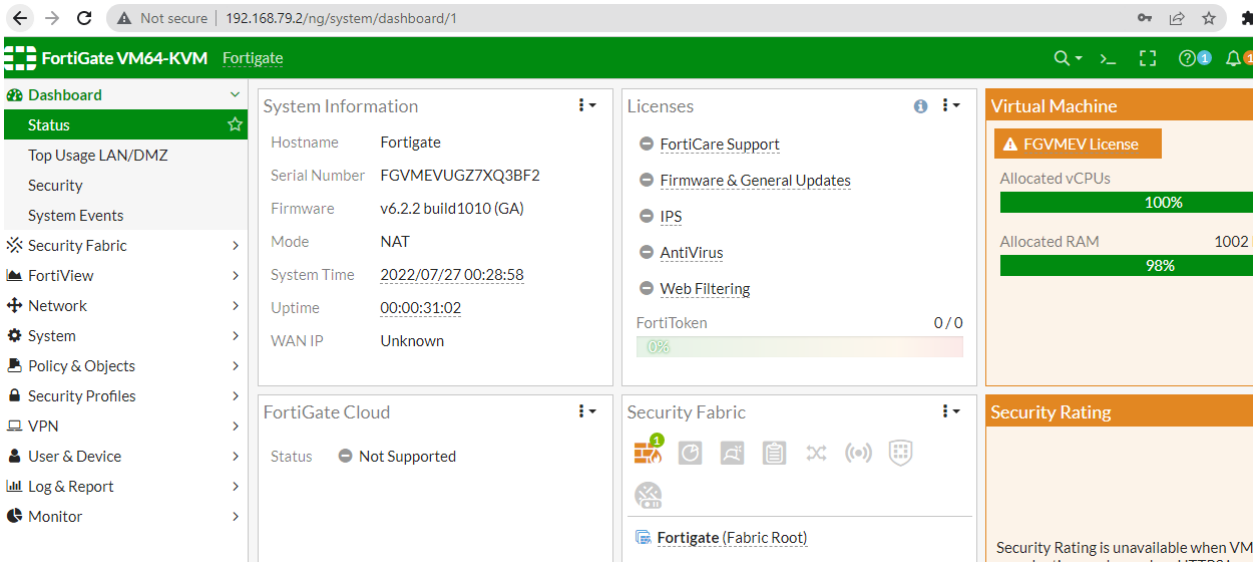
Now let’s access SSH & GUI from the management PC.

If you want access SSH through your PC’s CMD then you need to enter the below command –

:\Users\Dell.DESKTOP-G5EF6DM>**ssh -l admin 192.168.79.2**

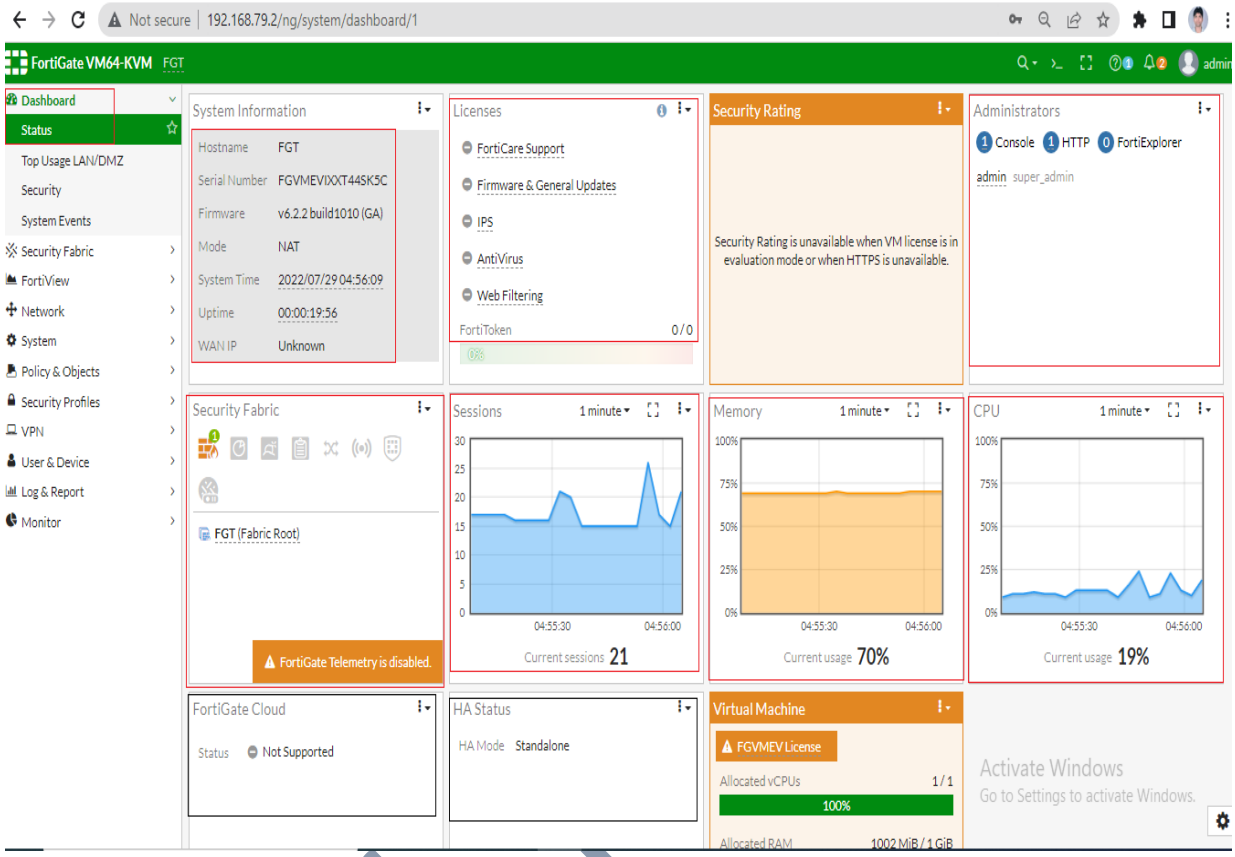
```
C:\Users\Dell.DESKTOP-G5EF6DM>ssh -l admin 192.168.79.2
The authenticity of host '192.168.79.2 (192.168.79.2)' can't be established.
ED25519 key fingerprint is SHA256:IgfeGTR6/FeZAy/j8HSEoIO+RFzC5WkMRAjDKh2Cepk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.79.2' (ED25519) to the list of known hosts.
admin@192.168.79.2's password:
Fortigate #
Fortigate #
Fortigate # config system int

Fortigate (interface) # show
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.79.2 255.255.255.0
        set allowaccess ping https ssh snmp http radius-acct
        set type physical
        set description "mgmtint"
        set snmp-index 1
    next
```

Successfully got the SSH access from the Management PC.



After configuring management IP we have seen that we are able to access SSH and GUI of the Fortigate.

Fortigate Dashboard explanation –



1. **System information –**
   Hostname of Fortigate
   Serial number – Serial number of the Fortigate
   Firmware – which version currently is going on Fortigate firewall
   NAT – (Modes of Firewall – NAT or Transparent)
   System uptime
   Uptime
   WAN IP – (WAN IP will be Public IP of ISP)
2. **License –**

This part will indicate that license is valid or expired =

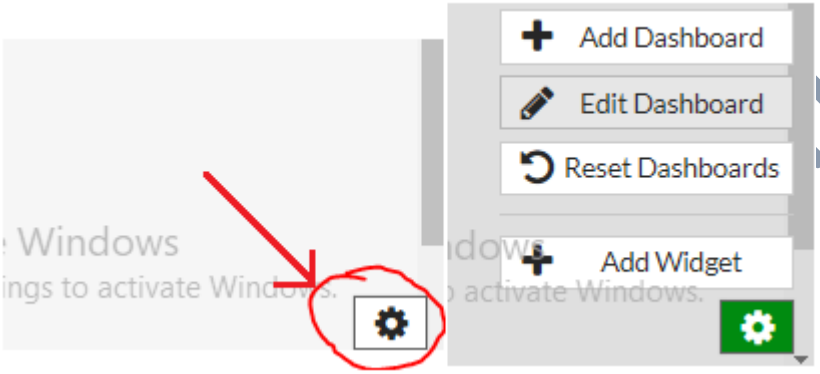
FortiCare Support
Firmware & General Updates
IPS (Intrusion prevention system)
AntiVirus
Web Filtering
FortiToken

3. **Security Rating-**
4. **Administrators –**

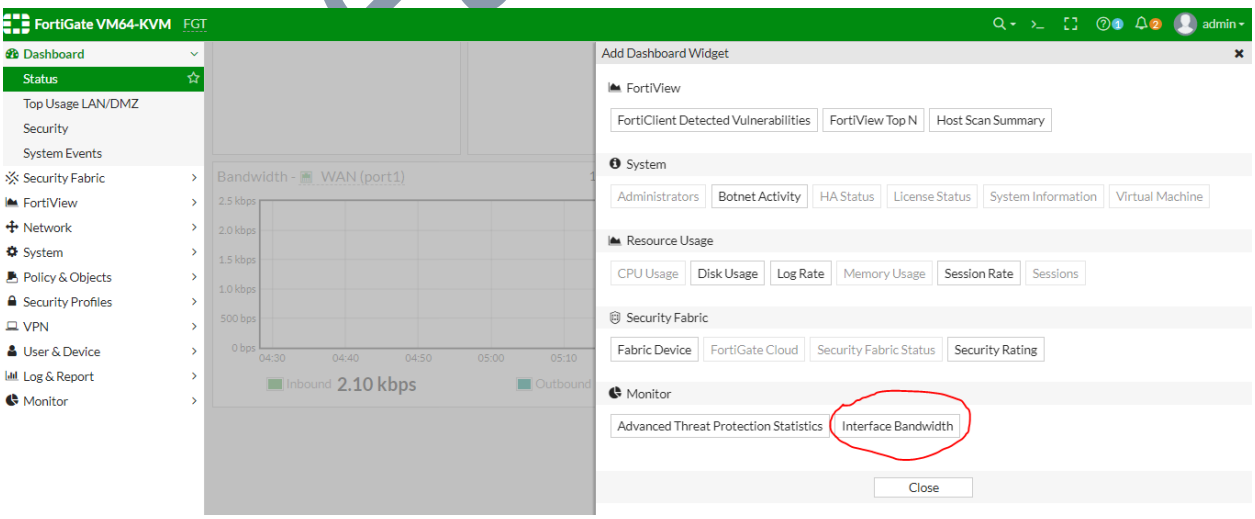
Right now who has taken access of Firewall using SSH or Webui, means who else is currently login.

5. **Security Fabric**
6. **Current Session**
7. **Memory of Forigate**
8. **CPU of Fortigate**
9. **Forticloud** - For logs
10. HA status - which is master or slave

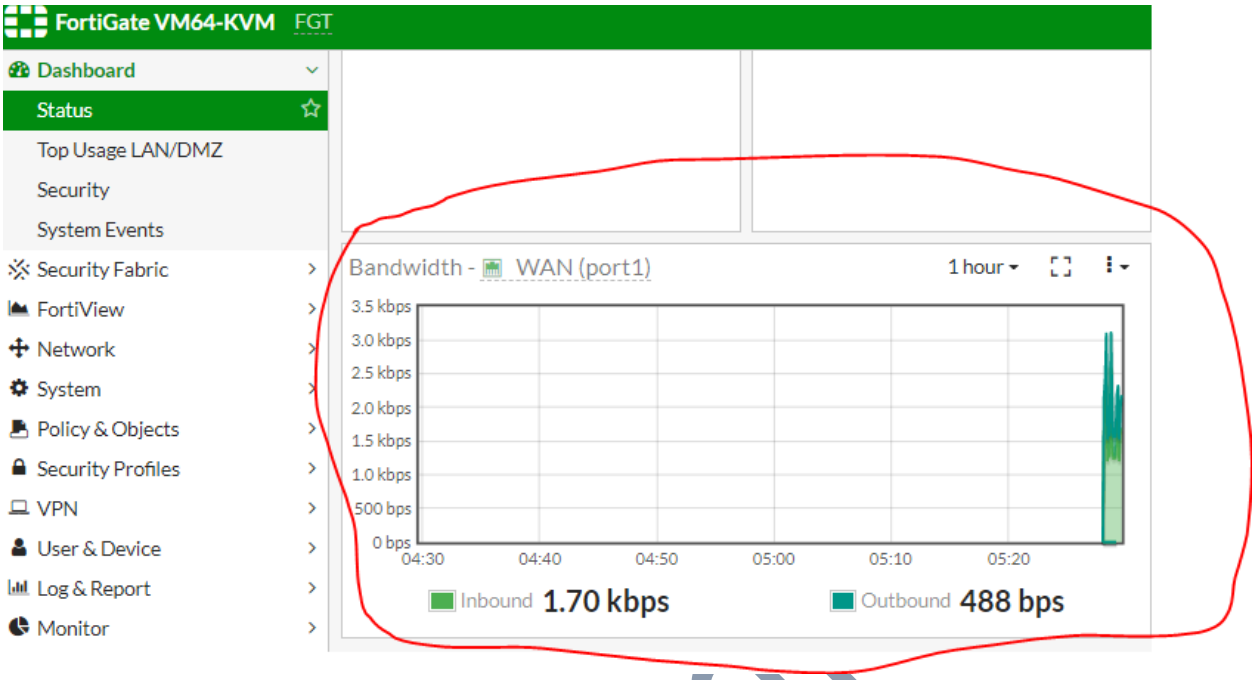
Note – you can manage Fortinet's dashboard youself by dragging, editing & modifying, If You want to add something in dashboard you can do that – Go down of dashboard let me show you that will be easy for us –



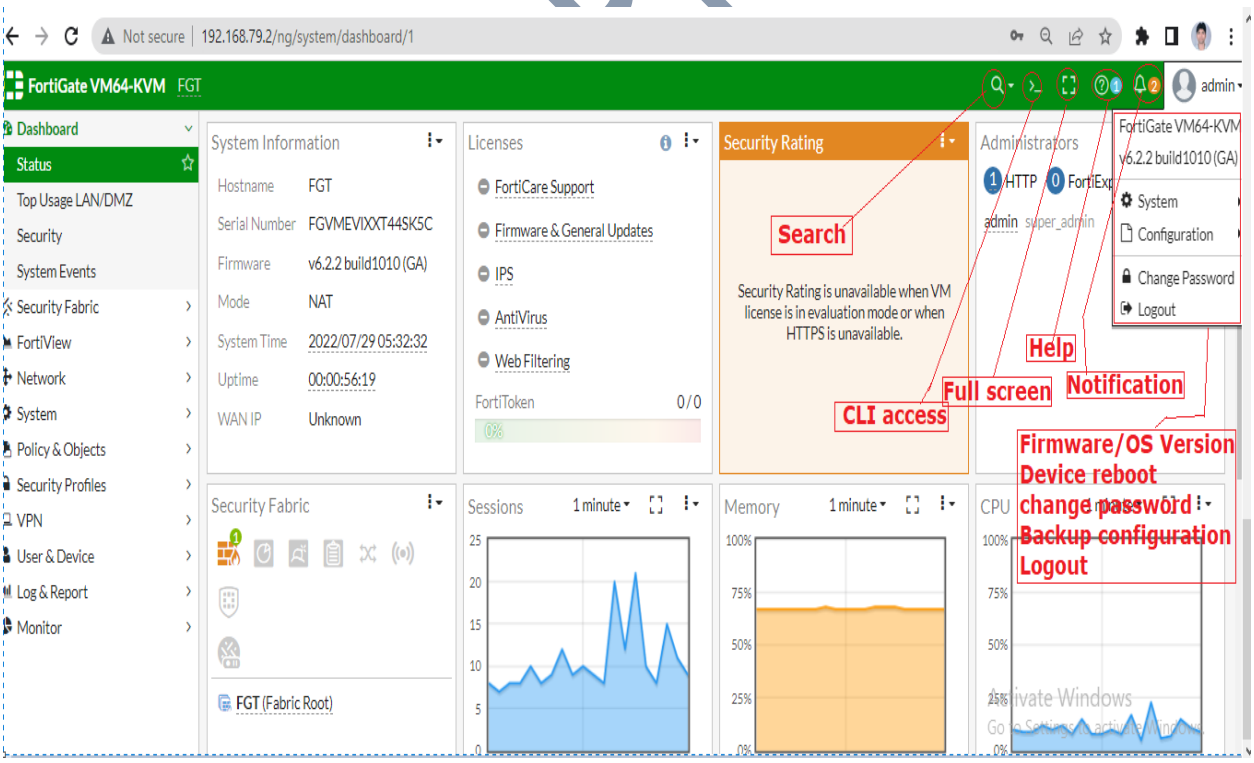
Let support I want to monitor bandwidth of ISP link –



Interface bandwidth has been added on Dashboard –



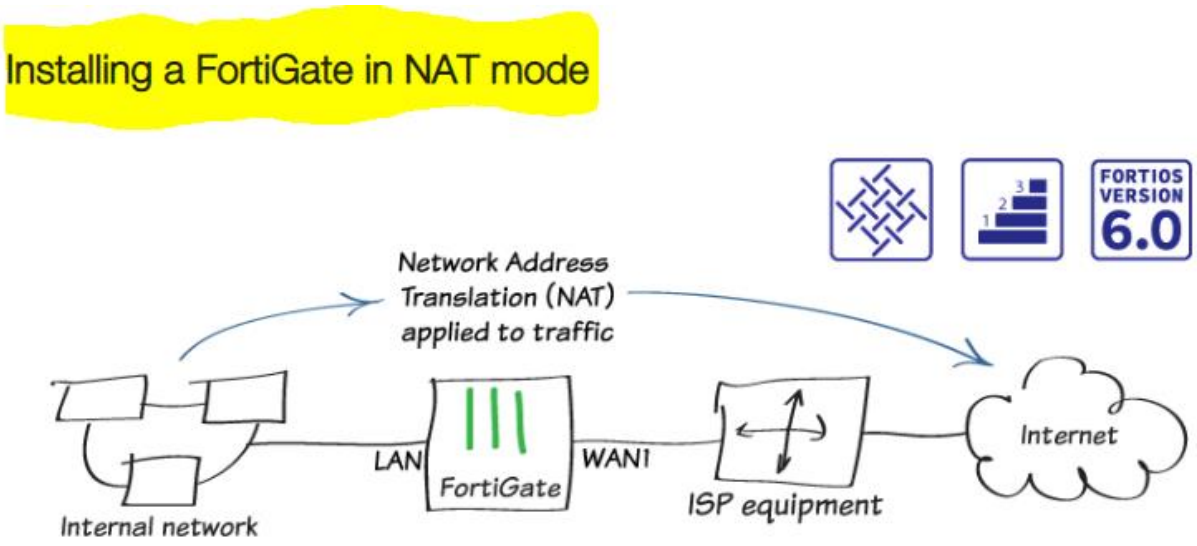
CLI access from the GUI –



Fortigate Installation mode –

Fortigate Firewall can be installed either NAT/Router or transparent mode.

NAT/Router mode –



In NAT mode Fortigate Firewall is installed as a gateway between the private network and public network FortiGate Firewall performs network address translation before IP packets are sent to the destination network.

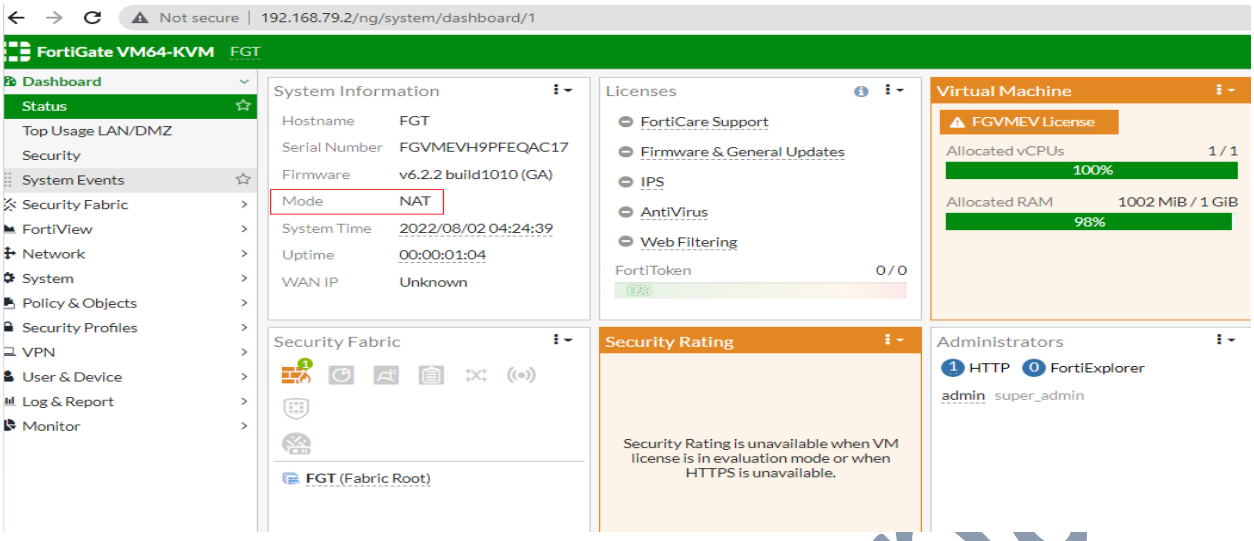
Or you can say that in this mode Fortigate Firewall is installed between the private network and public network to hide the private IP addresses.

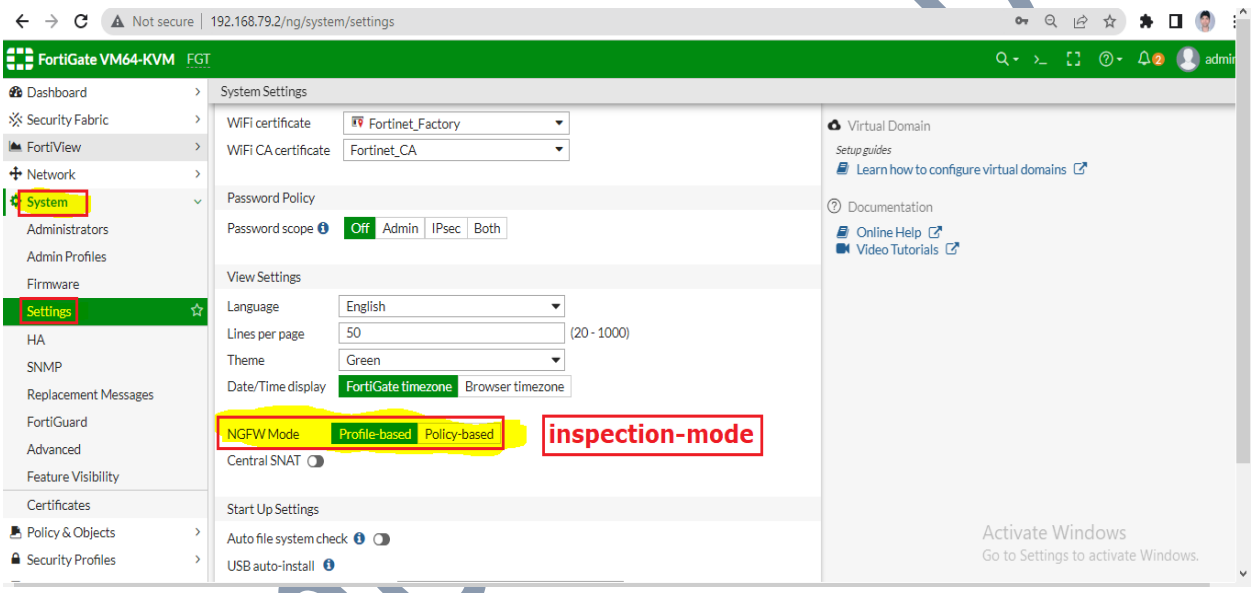
Typically Fortigate Firewall is installed /deployed between a private network and the Internet, which allows the FortiGate to hide the IP addresses of the private network using NAT.

These are some of the characteristics of NAT mode:

1. Typically used when the FortiGate unit is a gateway between private and public networks.
2. Can act as a router between multiple networks within a network infrastructure.
3. When used, the FortiGate unit is visible to the networks that are connected to.
4. Each logical interface is on a distinct subnet.
5. Each Interface needs to be assigned a valid IP address for the subnet that it is connected to it.

Fortigate NAT mode is the default mode – We can see the below image.





Fortigate works in two inspection modes –

1. Profile based (NAT mode default)
2. Policy based (Transparent mode)

This model is divided into two working modes — profile-based and policy based. Profile-based NGFW is the traditional mode where a user needs to create an AV/web/IPS profile which is applied to the policy.

Policy-based mode is new. In this mode, users can add applications and web filtering categories directly to a policy without having to first create and configure Application Control or Web Filtering profiles. If a URL category is set, the applications that are added to the policy must be within the browser-based

technology category. NGFW is per VDOM setting. This means users can operate their FortiGate or individual VDOMs on their FortiGate in NGFW policy-based mode when they select flow-based inspection.

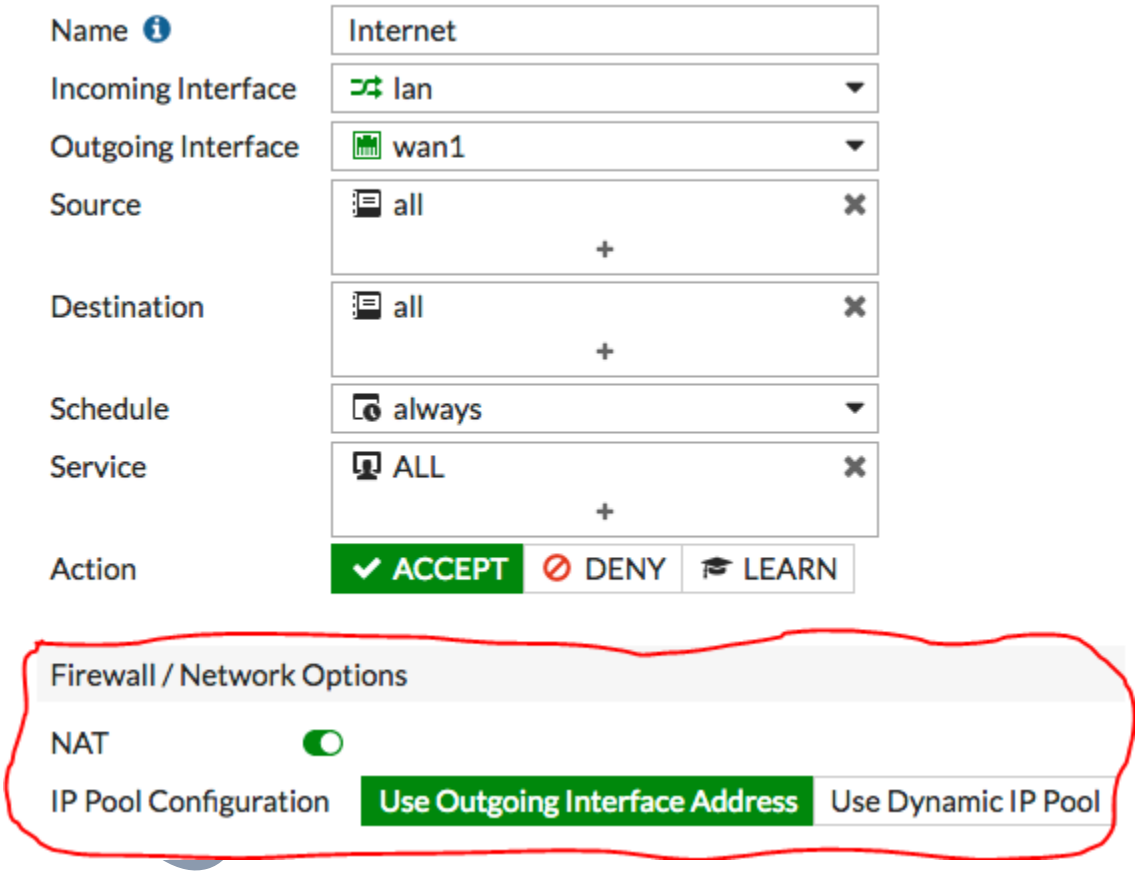
To enable policy-based NGFW mode using the GUI:-

Go to System > Settings.
In NGFW Mode, select profile-based/Policy-based

To enable policy-based NGFW mode using the CLI:

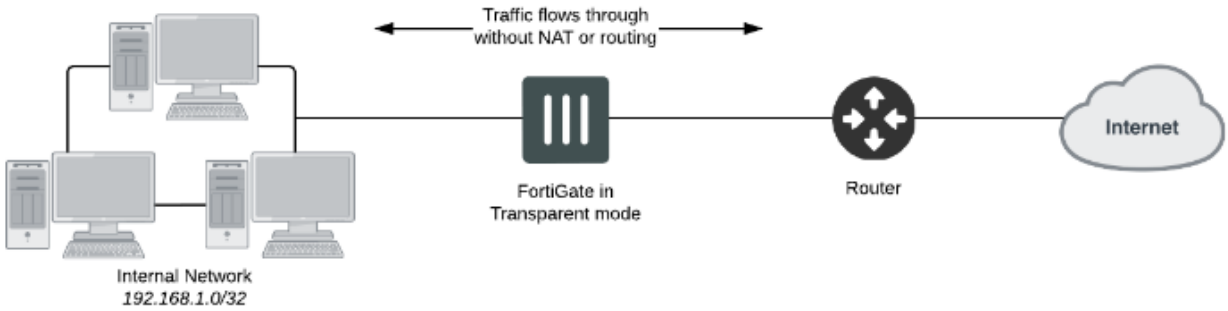
config system settings set ngfw-mode {profile-based | policy-based} end

Note – When your firewall is working NAT/Router, while policy configuring you see NAT option –



Transparent mode –

In Transparent mode, the FortiGate is installed between the internal network and the router. In this mode, the FortiGate does not make any changes to IP addresses and only applies security scanning to traffic.



In order to change mode from NAT mode to transparent mode –

- config system settings
- set opmode transparent
- set manageip <address and netmask>
- set gateway <address>
  end

For example -

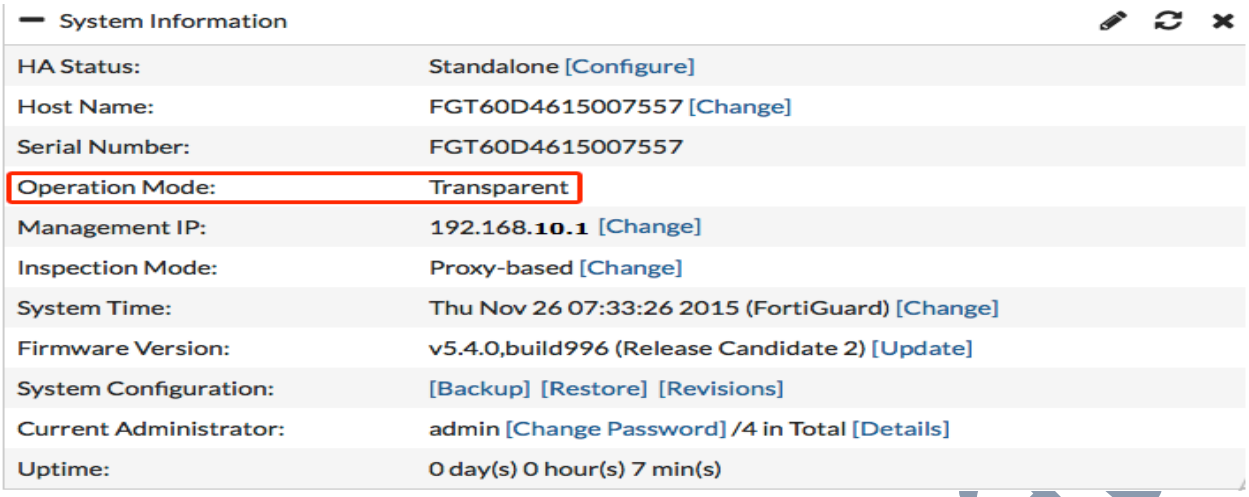
- `config system settings`
- `  set opmode transparent`
- `  set manageip 192.168.10.1 255.255.255.0`
- `  set gateway 192.168.10.10`
  `  end`

In order to access having changed the transparent mode of the firewall to access the GUI-

https://192.168.10.10

Attention – Before changing the mode from NAT to Transparent mode of the Firewall you must take the backup of the Firewall otherwise configuration will get lost.

Having changed the Fortigate mode you can see it at the Dashboard –



System Information

HA Status:	Standalone [Configure]
Host Name:	FGT60D4615007557 [Change]
Serial Number:	FGT60D4615007557
Operation Mode:	Transparent
Management IP:	192.168.10.1 [Change]
Inspection Mode:	Proxy-based [Change]
System Time:	Thu Nov 26 07:33:26 2015 (FortiGuard) [Change]
Firmware Version:	v5.4.0,build996 (Release Candidate 2) [Update]
System Configuration:	[Backup] [Restore] [Revisions]
Current Administrator:	admin [Change Password] /4 in Total [Details]
Uptime:	0 day(s) 0 hour(s) 7 min(s)

In sort transparent mode –

In layman term, transparent mode FortiGate is like a Layer 2 device. Hence, majority of the layer 3 features would not be available in transparent mode. In L3(NAT) deployment, the outside interface and internal interface IP subnet would need to be assigned with different subnet. However, in transparent mode, the upstream device (ISP Router/Switch and etc) would have the same IP range with the internal hosts. Hence, if you do not want to modify the IP subnet design on the network, that would be when you should use transparent mode FortiGate as it would require you to make no changes on the upstream and downstream devices.

I will discuss in depth later about transparent mode such as how does it work and what are the features of transparent mode ….etc.

Static Default routing configuration –

FGT # config router static
FGT (static) # edit 1
FGT (1) # set gateway 192.168.23.1
FGT (1) # set device port1
FGT (1) # set status enable
FGT (1) # set dst 0.0.0.0/0.0.0.0
FGT (1) # set comment WAN_INT

FGT (1) # show (To verify the command)

```
config router static
   edit 1
      set gateway 192.168.23.1
      set device "port1"
      set comment "WAN_INT"
   next
end
```

Configurations are available in static route-

```
FGT (1) # set
status                  Enable/disable this static route.
*dst                     Destination IP and mask for this route.
gateway                 Gateway IP for this route.
distance                Administrative distance (1 - 255).
weight                  Administrative weight (0 - 255).
priority                Administrative priority (0 - 4294967295).
*device                  Gateway out interface or tunnel.
comment                 Optional comments.
blackhole               Enable/disable black hole.
dynamic-gateway         Enable use of dynamic gateway retrieved from a DHCP or PPP server.
virtual-wan-link        Enable/disable egress through the virtual-wan-link.
dstaddr                 Name of firewall address or address group.
internet-service        Application ID in the Internet service database.
internet-service-custom Application name in the Internet service custom database.
link-monitor-exempt     Enable/disable withdrawal of this static route when link monitor or health check is down.
bfd                     Enable/disable Bidirectional Forwarding Detection (BFD).

FGT (1) # set
```

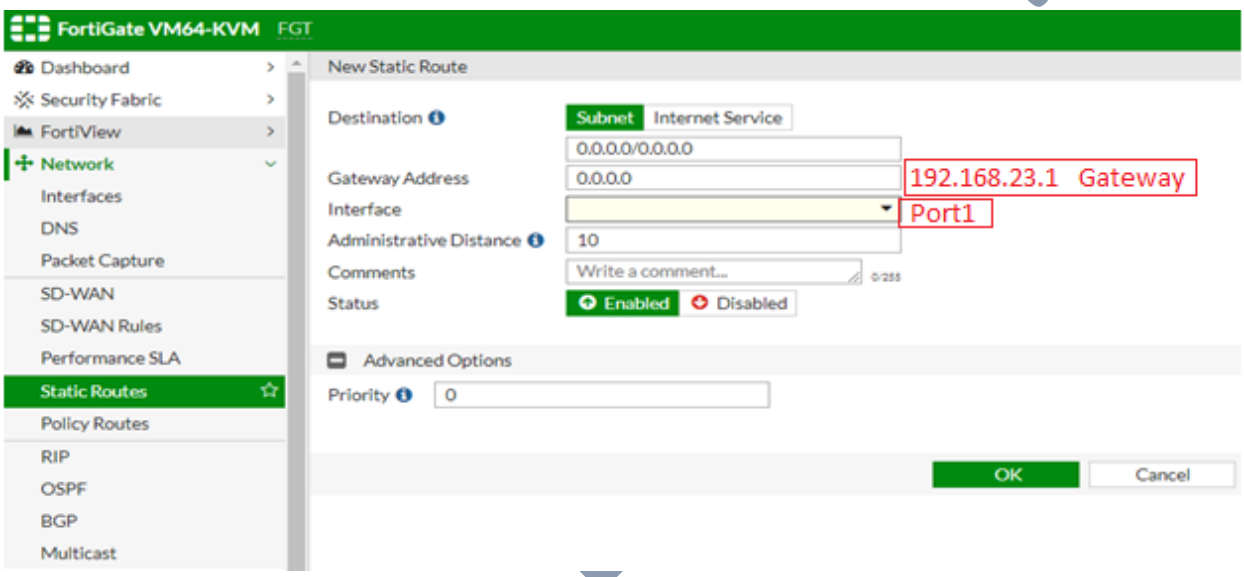
In order to configure static default route using GUI –

Step1. Go to network

Step2. Select static route

Step3. Create New

Step4. Administrative distance is optional.



To view routing table –

FGT # get router info routing-table all

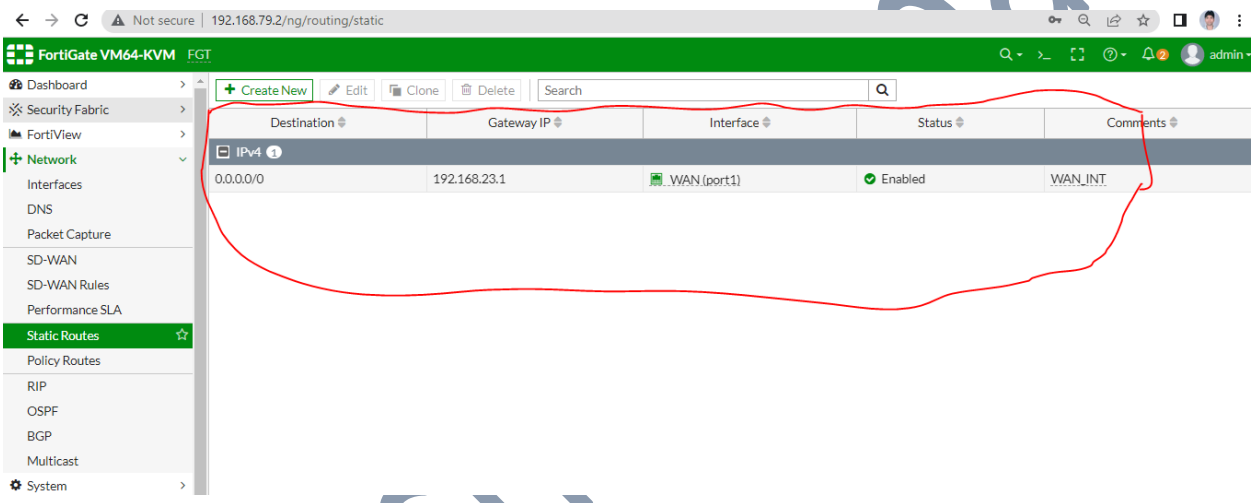
FGT # get router info routing-table database

```
FGT # get router info routing-table all

Routing table for VRF=0
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

S*      0.0.0.0/0 [10/0] via 192.168.23.1, port1
C       1.1.1.0/24 is directly connected, port1
C       192.168.79.0/24 is directly connected, port10


FGT #
```

For more information about routing table you can use below commands –

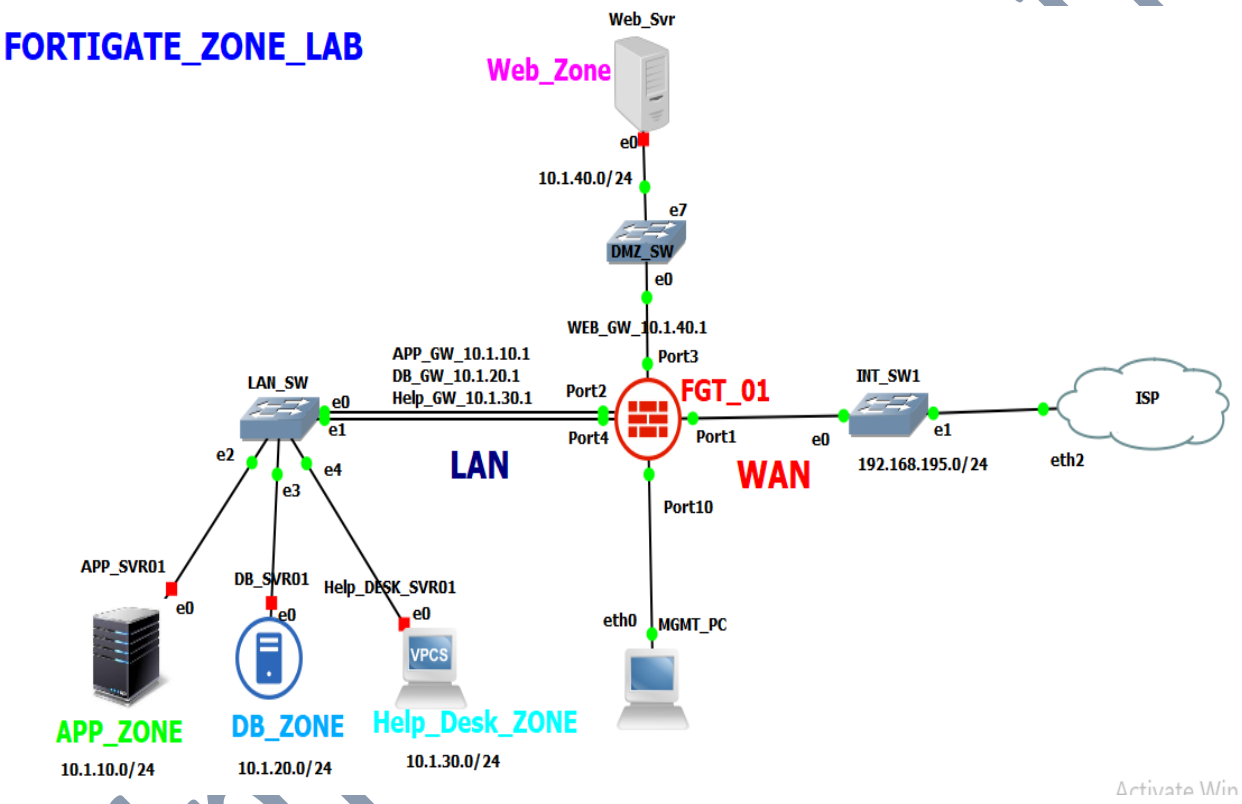
```
FGT # get router info routing-table
details       show routing table details information
all           show all routing table entries
rip           show rip routing table
ospf          show ospf routing table
bgp           show bgp routing table
isis          show isis routing table
static        show static routing table
connected     show connected routing table
database      show routing information base
```

In order to check static routing in GUI –

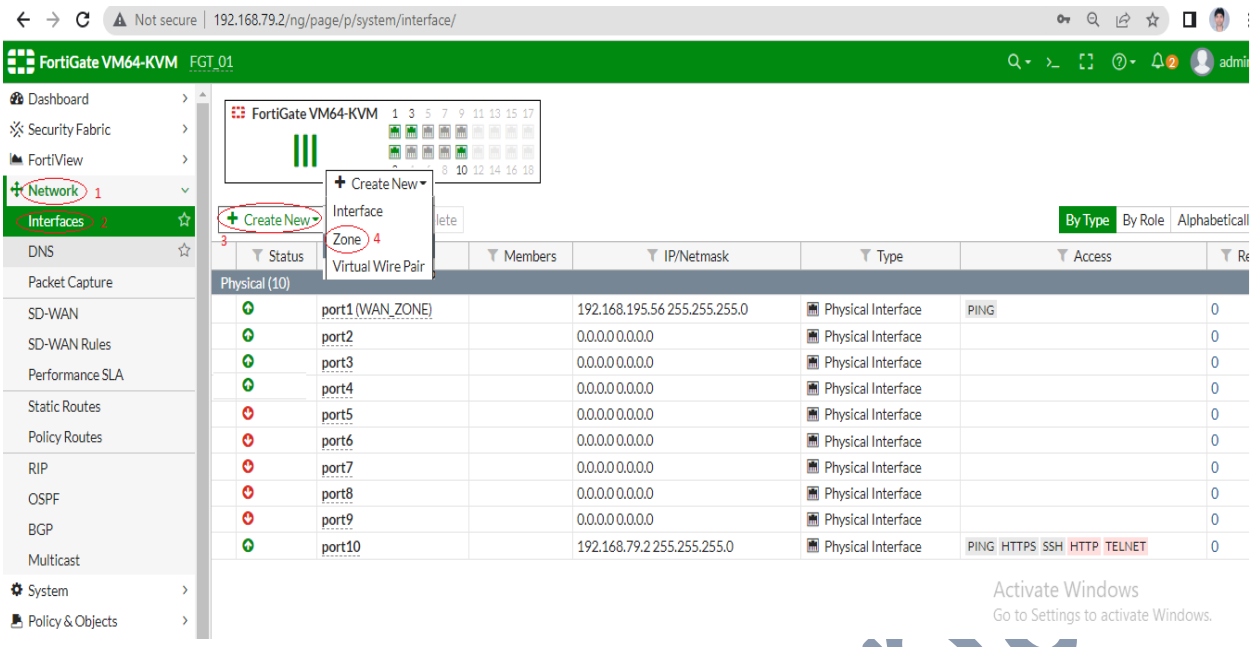


Fortigate Zone –

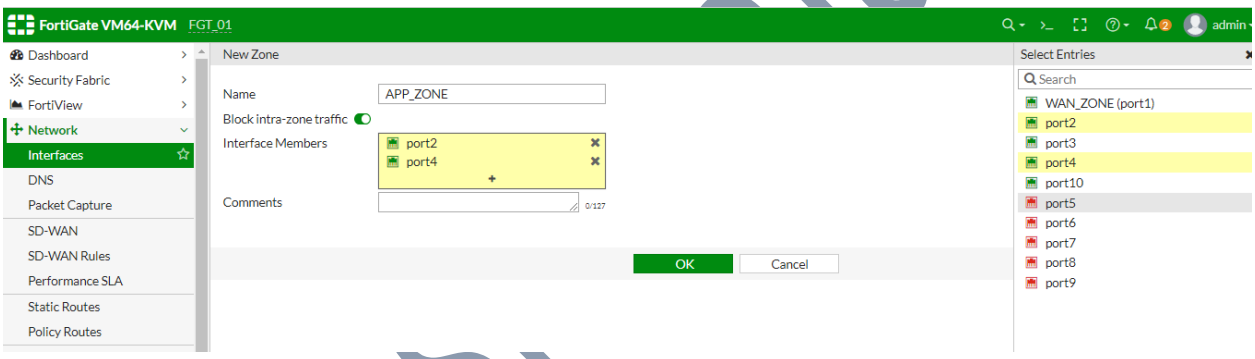
- Zones are a group of one or more physical or virtual FortiGate interfaces that you can apply security policies to control inbound and outbound traffic and you can use security policies to control the flow of intra-zone traffic.
- When you create a zone, either you select the names of the interfaces or VLAN subinterfaces to add to the zone.
- In Zone could be one or multiple physical interfaces or virtual interfaces.
- In order to create Zones please go through the below diagram.



Method -01 –using physical interfaces



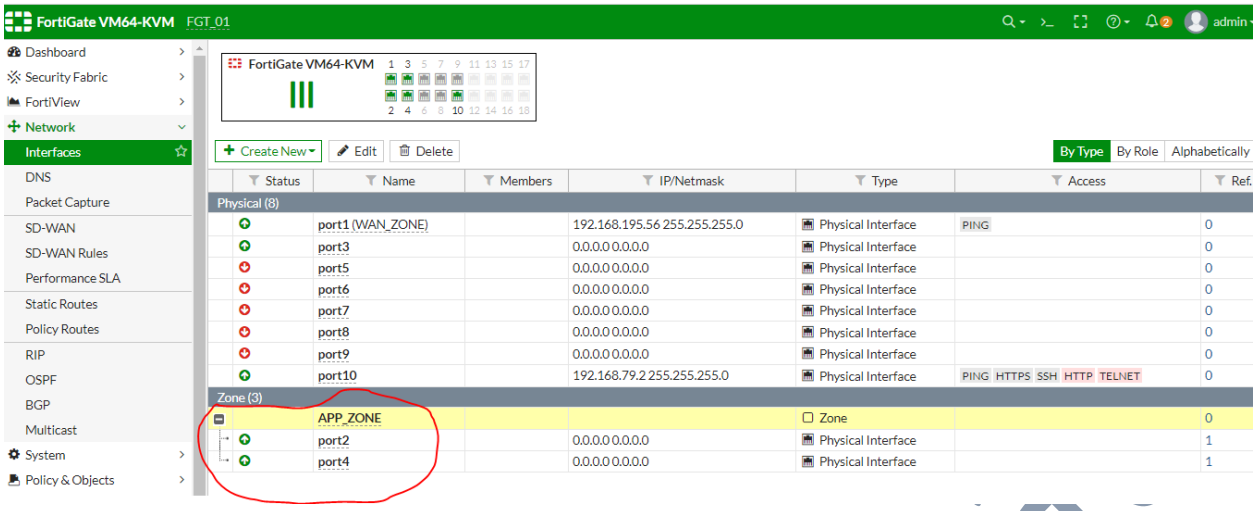
Now click on the zone tab after that it will redirect on the Fortinet Zone page where you will be able to create Zone with using Single physical interface or multiple interfaces. For example –



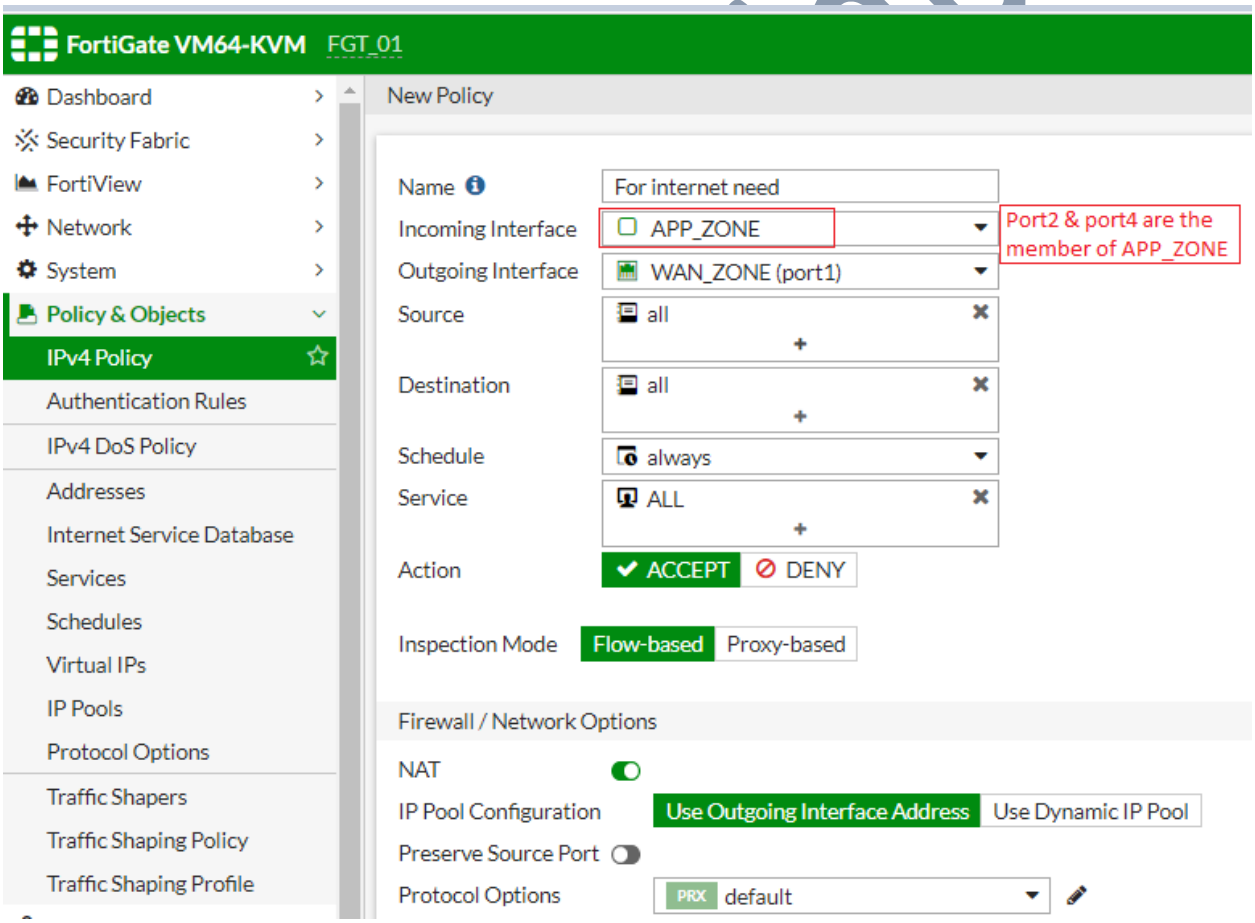
You can add one or two physical interfaces in the interface member option, and then click okay.

Note – Block intra-traffic means – Intra communication will not be happen you can off this button as per you need.

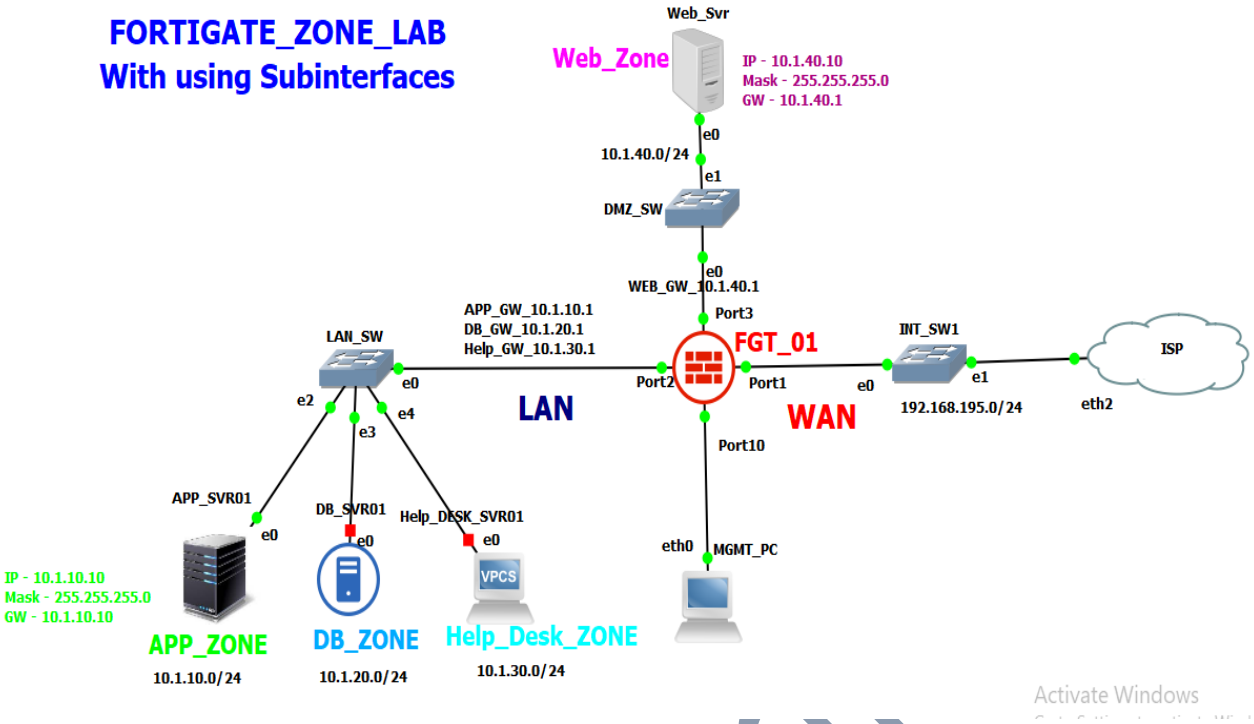
As you can see that both port (port2 & port4) are the member of APP_Zone.



Now you can create policy as per need-



Method 2 – In order to create Zones with using Subinterfaces



Steps to create Zone with using Sub interface –

1. Create subinterfaces according to VLANs
2. Add these Sub interface in Zone.

In this lab we have 4 VLANs so, have to create 4 Zones like –

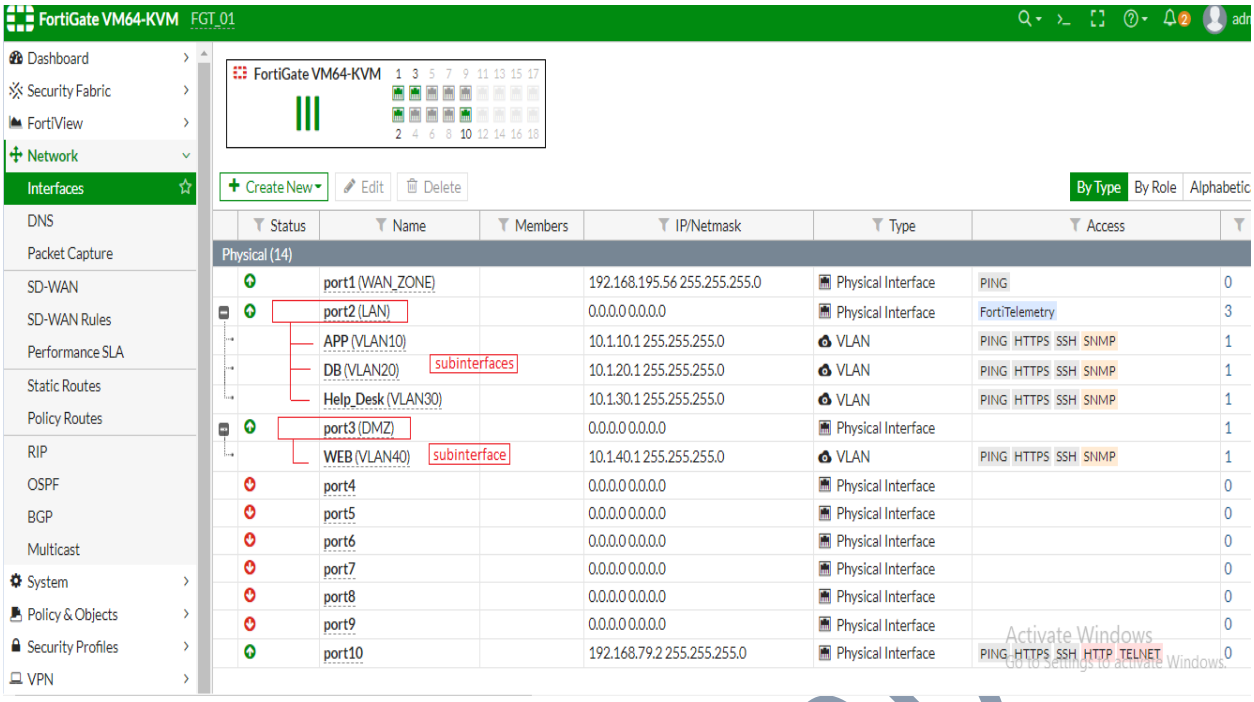
1. APP_ZONE - 10.1.10.0/24
2. DB_ZONE - 10.1.20.0/24
3. Helpdesk_ZONE – 10.1.30.0/24
4. WEB_ZONE - 10.1.40.0/24

Now Firstly I am going to create subinterfaces then I add these subinterfaces in different-2 ZONEs as per LAB.

Note – Here I am not going to show you how to create Subinterfaces, Will show you next page.

If you see the below image there are 4 subinterfaces as per the topology

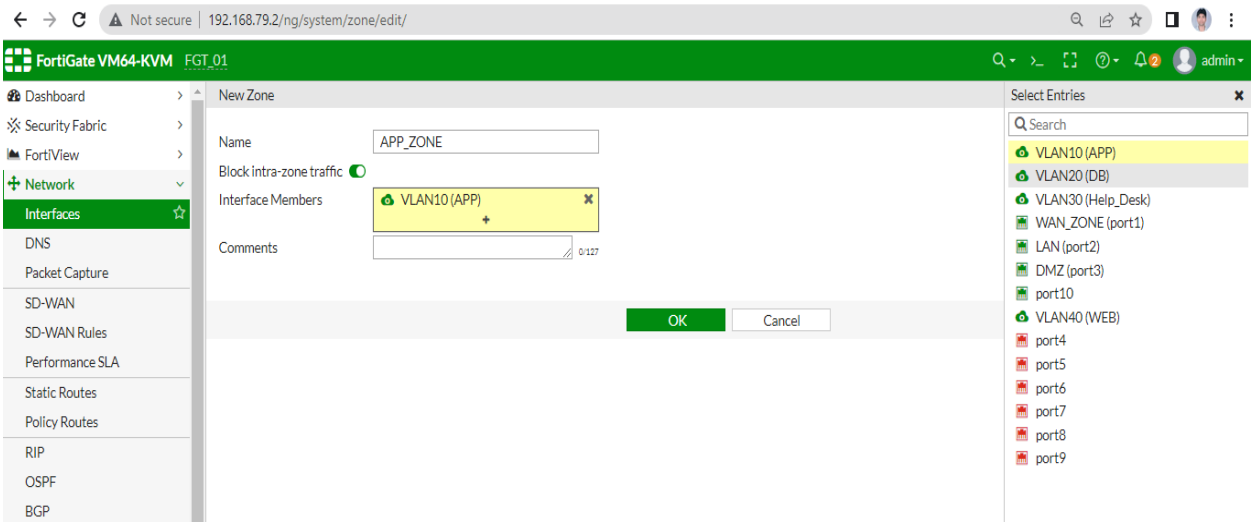
1. APP_VLAN10
2. DB_VLAN20
3. Helpdesk_VLAN30
4. WEB_VLAN40



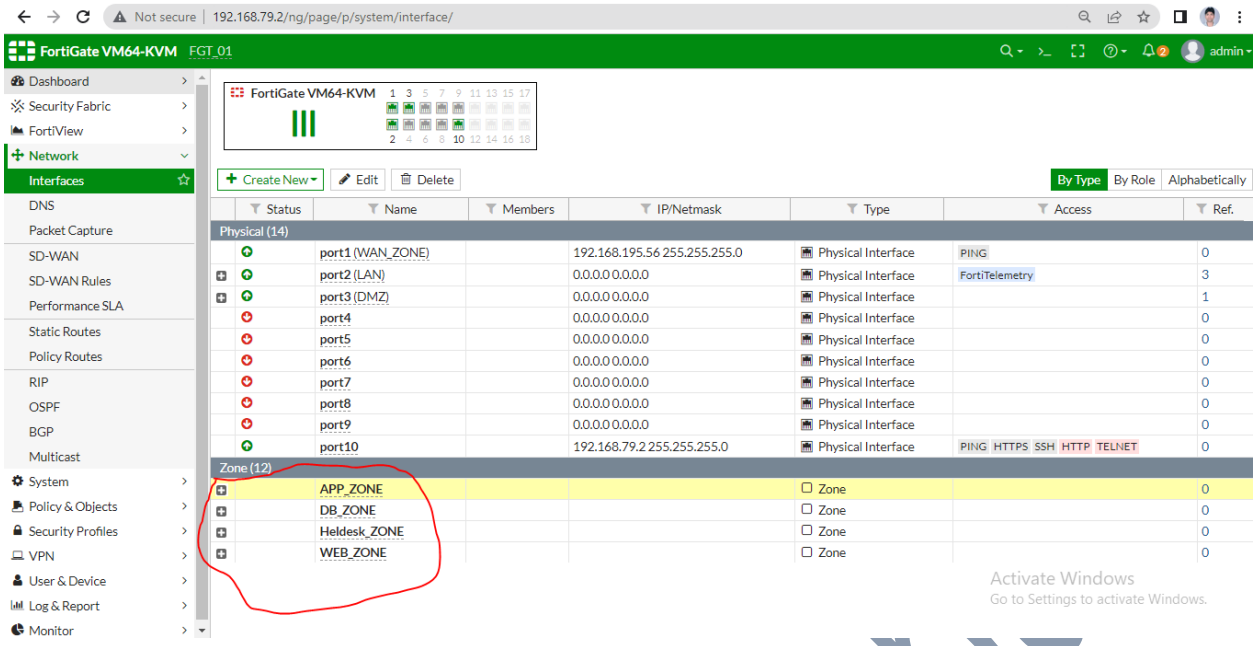
Now I am going to create 4 Zones

- APP_ZONE
- DB_ZONE
- Helpdesk_ZONE
- WEB_ZONE

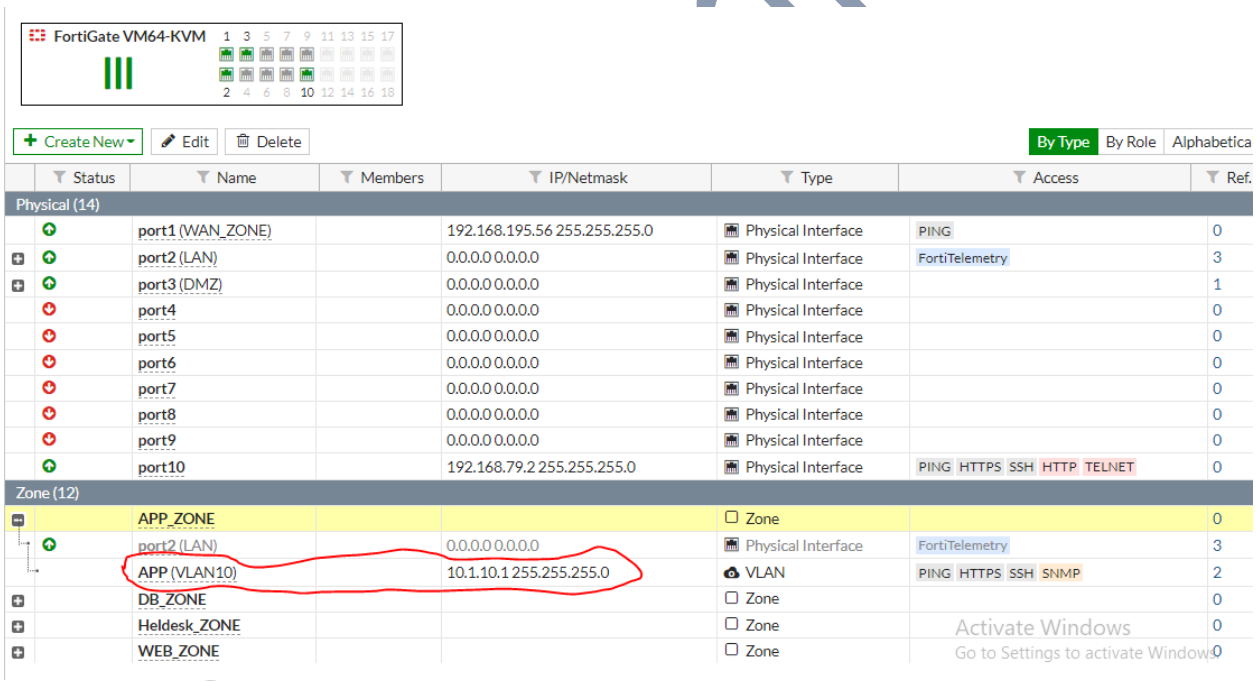
For example – APP_ZONE



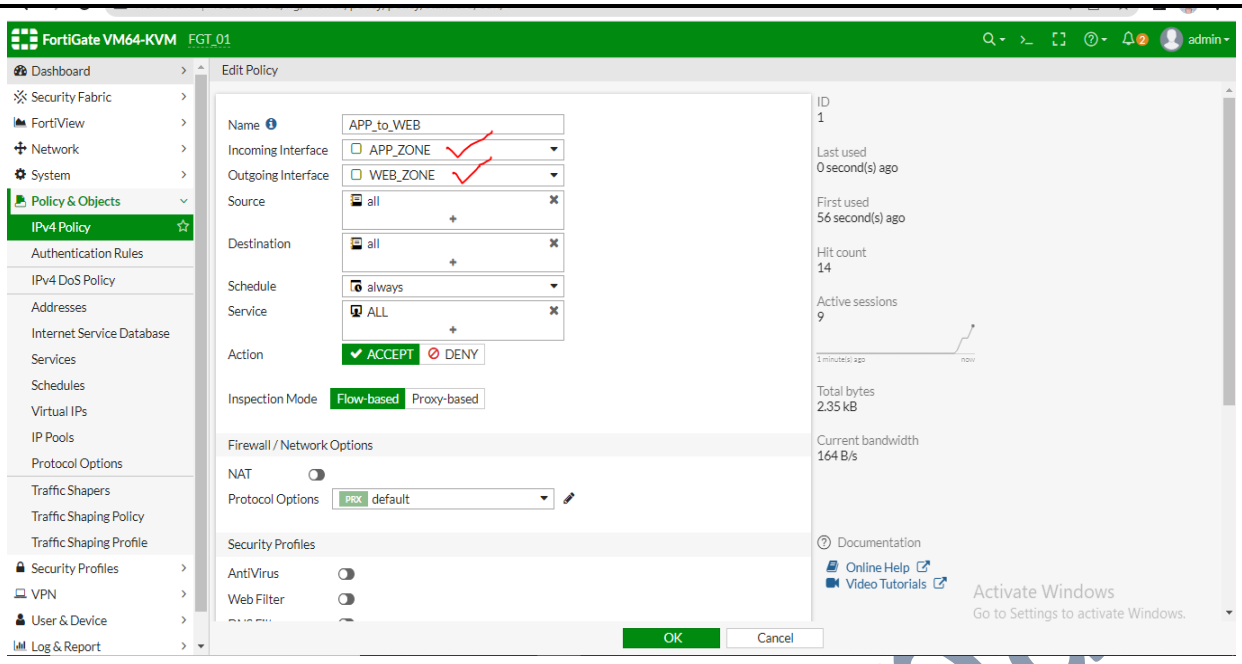
Zones have been created –



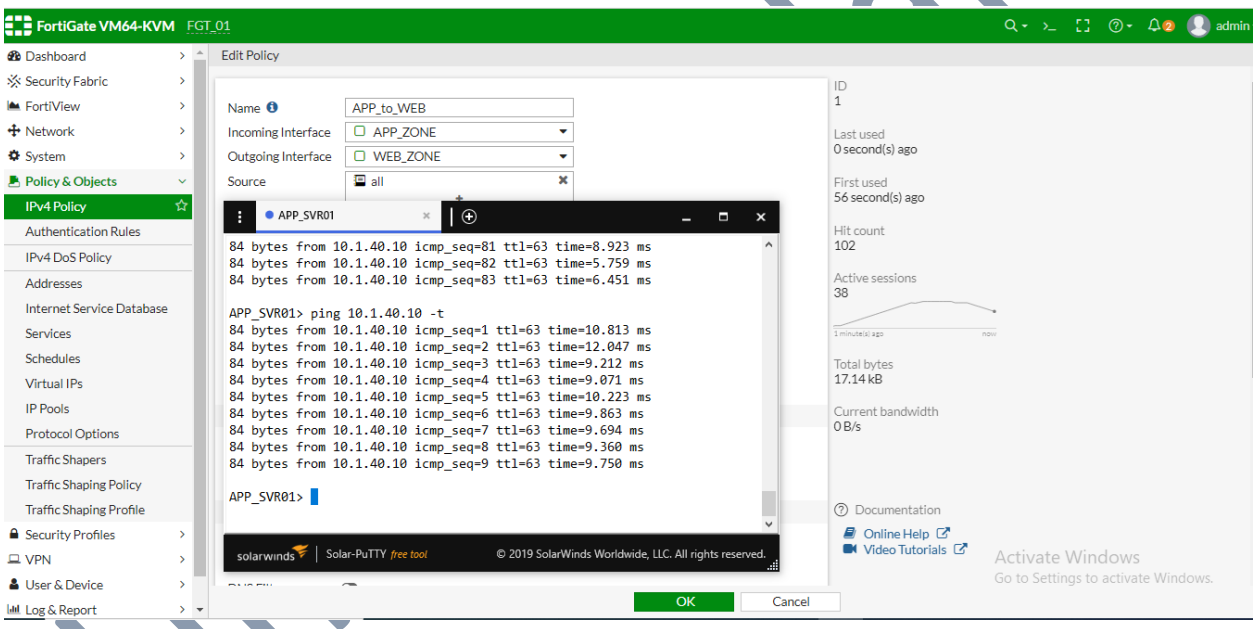
If you expand to zones you will see that under the ZONEs subinterfaces are added.



In order to verify the zones now let's create policy –



Testing policy – from APP_ZONE to WEB ZONE

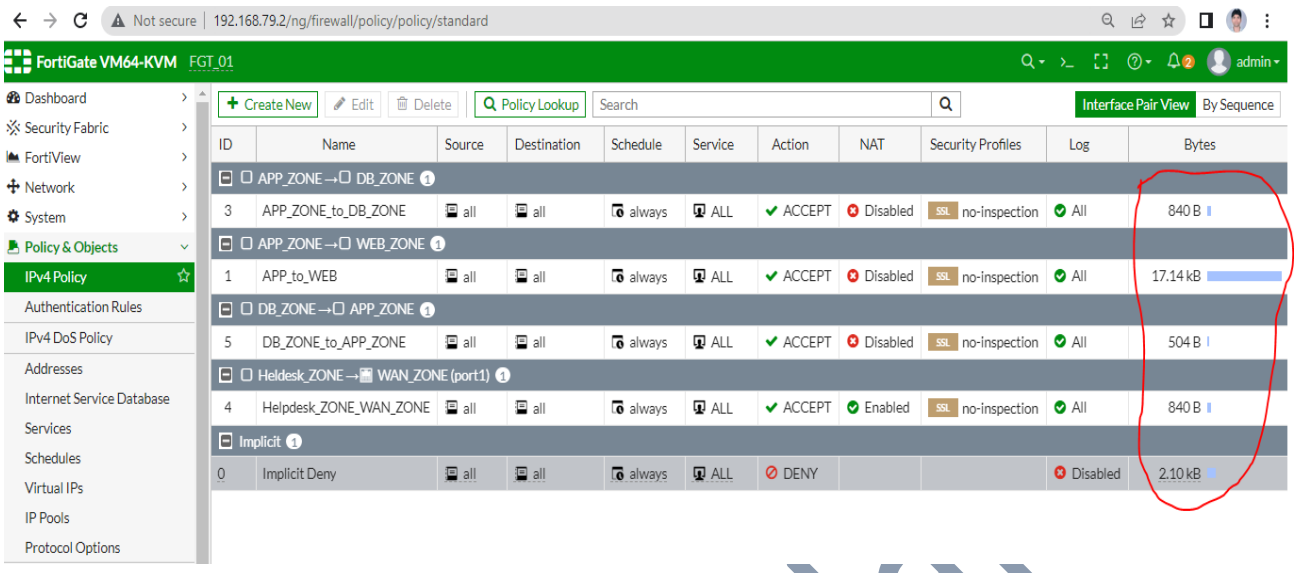


Point to be noted – Intra-zone communication will be denied because Intra-Zone is not allowed.

Below is the following policy what I am going to create according to my requirements.

1. APP_ZONE_to_WEB_ZONE (Webserver ZONE is in DMZ ZONE)
2. APP_ZONE_to_DB_ZONE

3. DB_ZONE_to_APP_ZONE
4. Helpdesk_ZONE_to _WAN_ZONE




```
APP_SVR01> ping 10.1.40.10 -t
84 bytes from 10.1.40.10 icmp_seq=1 ttl=63 time=10.813 ms
84 bytes from 10.1.40.10 icmp_seq=2 ttl=63 time=12.047 ms
84 bytes from 10.1.40.10 icmp_seq=3 ttl=63 time=9.212 ms
84 bytes from 10.1.40.10 icmp_seq=4 ttl=63 time=9.071 ms
84 bytes from 10.1.40.10 icmp_seq=5 ttl=63 time=10.223 ms
84 bytes from 10.1.40.10 icmp_seq=6 ttl=63 time=9.863 ms
84 bytes from 10.1.40.10 icmp_seq=7 ttl=63 time=9.694 ms
84 bytes from 10.1.40.10 icmp_seq=8 ttl=63 time=9.360 ms
84 bytes from 10.1.40.10 icmp_seq=9 ttl=63 time=9.750 ms

APP_SVR01> ping 10.1.20.10
84 bytes from 10.1.20.10 icmp_seq=1 ttl=63 time=12.794 ms
84 bytes from 10.1.20.10 icmp_seq=2 ttl=63 time=10.237 ms
84 bytes from 10.1.20.10 icmp_seq=3 ttl=63 time=10.507 ms
84 bytes from 10.1.20.10 icmp_seq=4 ttl=63 time=4.846 ms
84 bytes from 10.1.20.10 icmp_seq=5 ttl=63 time=14.012 ms

APP_SVR01> ping 8.8.8.8
8.8.8.8 icmp_seq=1 timeout
8.8.8.8 icmp_seq=2 timeout
8.8.8.8 icmp_seq=3 timeout
8.8.8.8 icmp_seq=4 timeout
8.8.8.8 icmp_seq=5 timeout

APP_SVR01>
```

APP_Server_ZONE

```
DB_SVR01> ping 10.1.10.10
84 bytes from 10.1.10.10 icmp_seq=1 ttl=63 time=16.773 ms
84 bytes from 10.1.10.10 icmp_seq=2 ttl=63 time=10.294 ms
84 bytes from 10.1.10.10 icmp_seq=3 ttl=63 time=10.540 ms

DB_SVR01>
```

DB_SERVER_ZONE

```
VPCS> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=112 time=91.491 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=112 time=56.720 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=112 time=55.966 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=112 time=57.298 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=112 time=58.782 ms

VPCS> ping 10.1.10.10
10.1.10.10 icmp_seq=1 timeout
10.1.10.10 icmp_seq=2 timeout
10.1.10.10 icmp_seq=3 timeout
10.1.10.10 icmp_seq=4 timeout

VPCS> ping 10.20.10.20
10.20.10.20 icmp_seq=1 timeout
10.20.10.20 icmp_seq=2 timeout
10.20.10.20 icmp_seq=3 timeout
10.20.10.20 icmp_seq=4 timeout
10.20.10.20 icmp_seq=5 timeout

VPCS>
```

Helpdesk_ZONE

WE have successfully configured Zones configure and seen intra zone communication is no allowed.

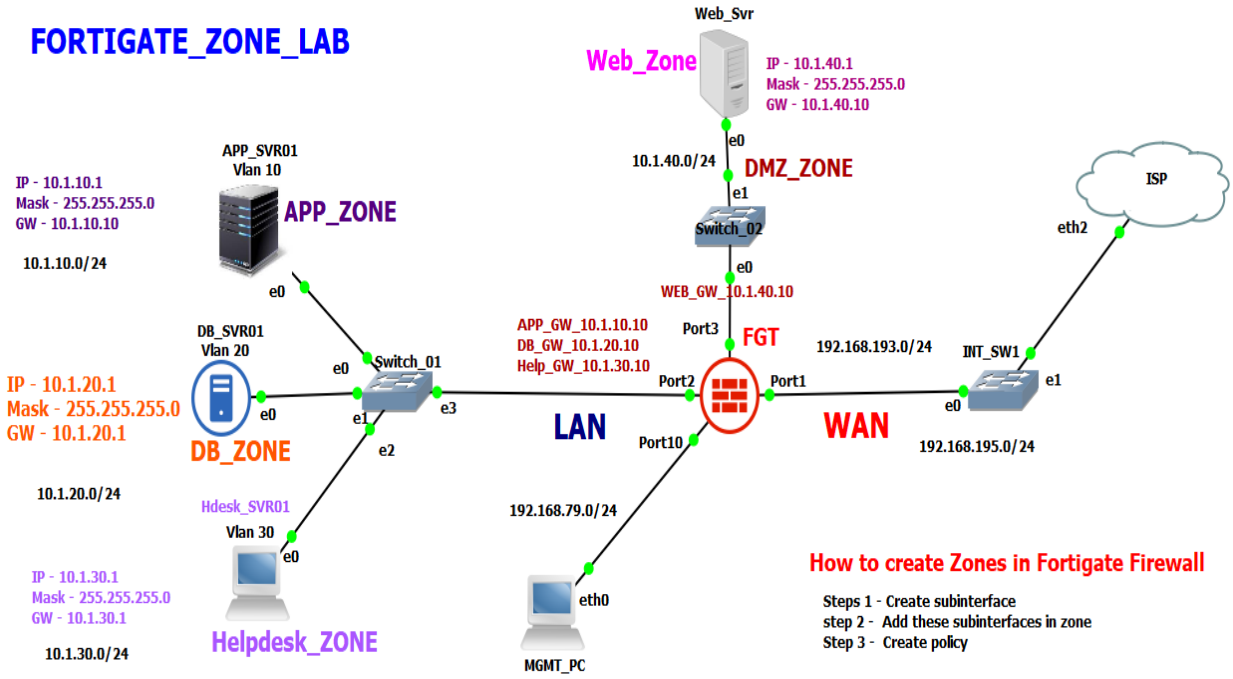
Let see or understand ZONE configuration from other topology –

Fortigate Firewall Zone –

In order to understand zones we have to go through few things.

- Zones are a group of one or more physical or virtual FortiGate interfaces that you can apply security policies to control inbound and outbound traffic. Or you can say -
- It helps while creating the security policy if we have multiple subnets / Networks.
- When you create a zone, either you select the names of the interfaces or VLAN sub interfaces to add to the zone.
- In Zone could be one or multiple physical interfaces or virtual interfaces.

In this document we would learn zones configuration with the help of SVI using below diagram.



Steps to create Zone with using Sub interface –

3. Create sub interfaces according to VLANs
4. Add these Sub interface in Zone.

In this lab we have 4 VLANs so, have to create 4 Zones like –

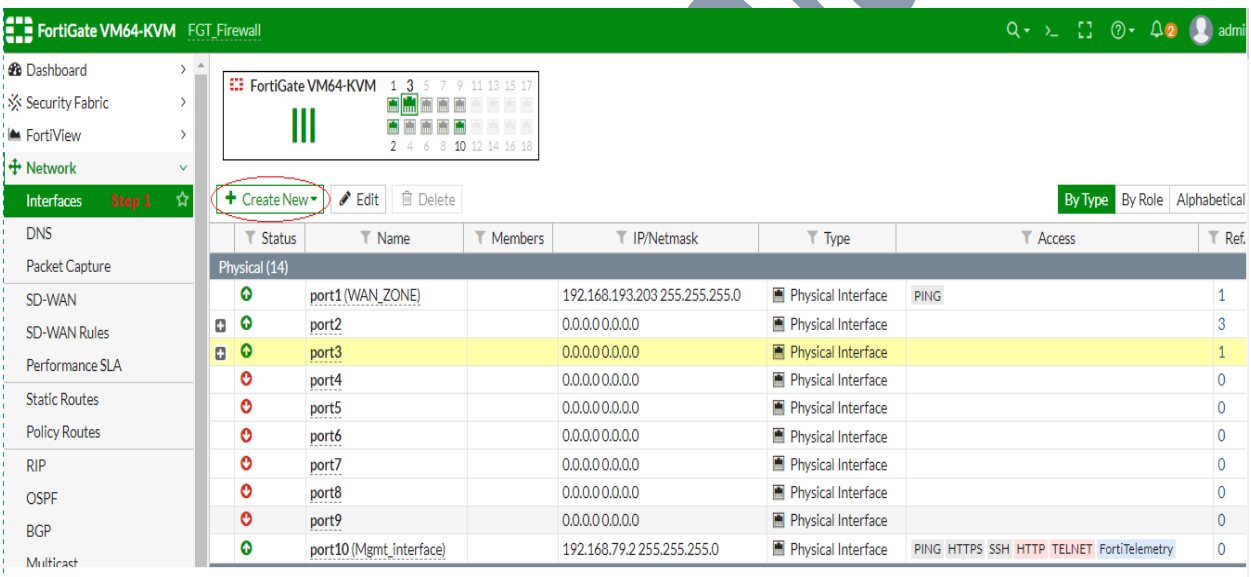
5. APP_ZONE - 10.1.10.0/24
6. DB_ZONE - 10.1.20.0/24
7. Helpdesk_ZONE – 10.1.30.0/24
8. WEB_ZONE - 10.1.40.0/24

Now Firstly I am going to create sub interfaces then I add these sub interfaces in different-2 ZONEs as per LAB.

Note – Here I am not going to show you how to create Sub interfaces as here I am explaining Zone configuration.

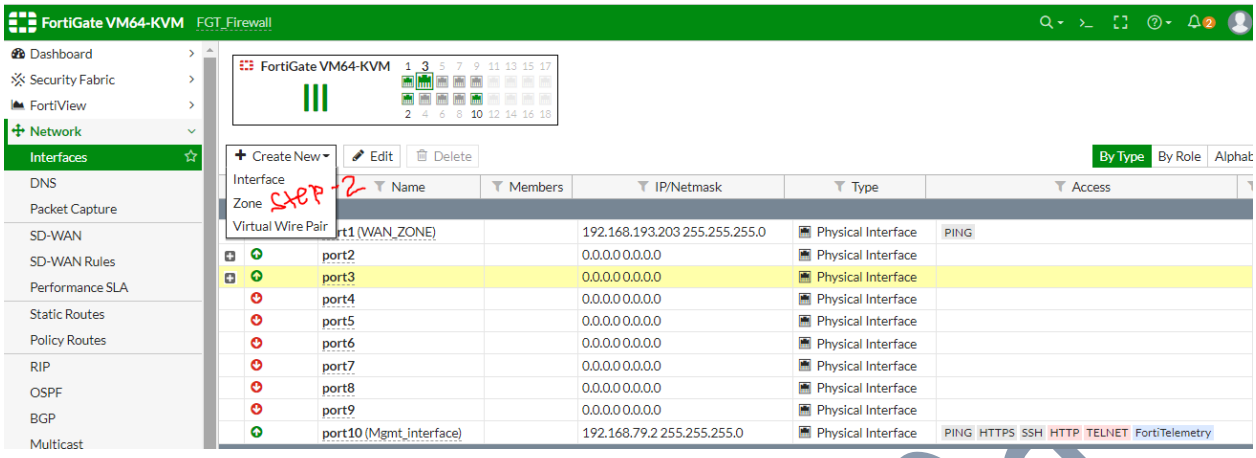
Once you create SVI on Fortigate Firewall please follow the below steps one by one –

Step-01



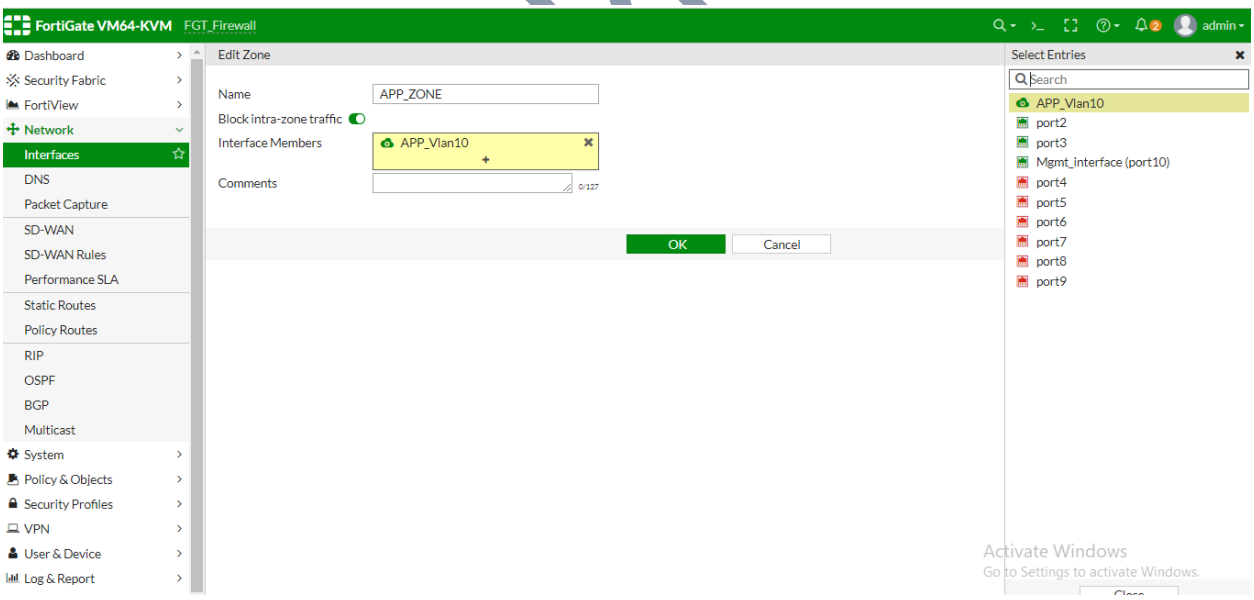
Step – 02

Click on create option here you will find Zone option for creation.



Step – 03

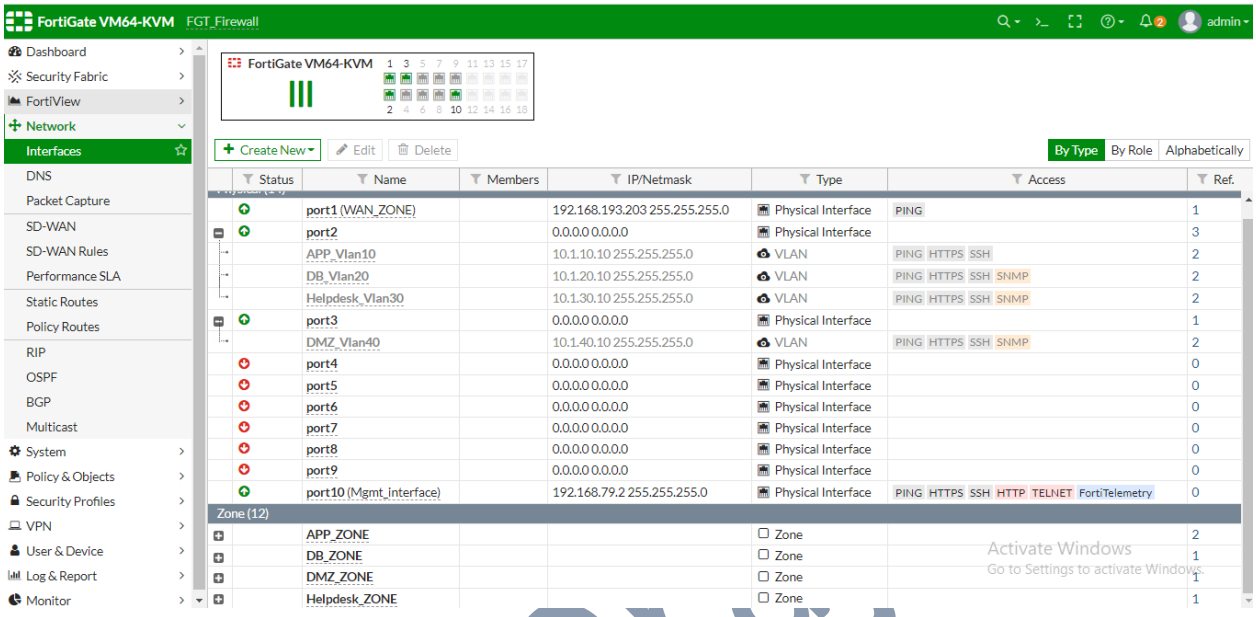
As you can see in step 3 I have added what SVI I had configured that has been added in member of APP_ZONE (this is the name of Zone you can have according to your requirement).



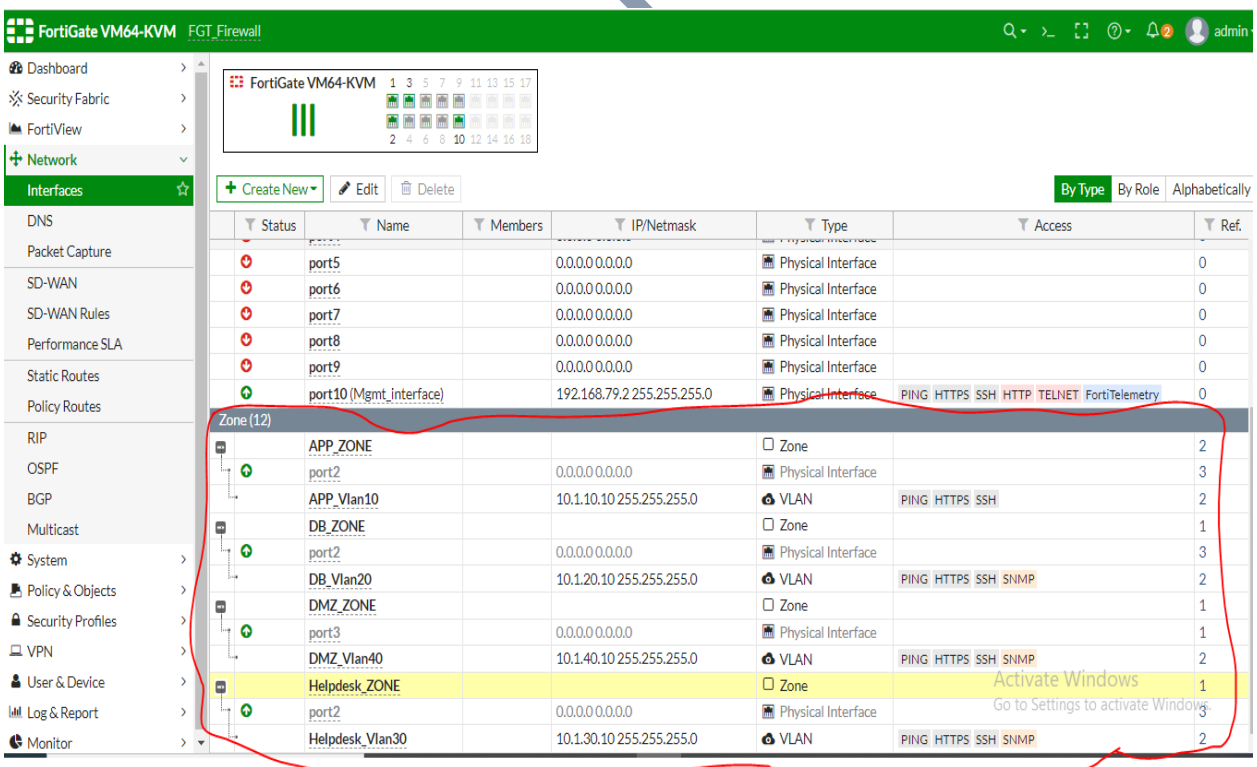
Note – Similarly you can create rest of the Zone. See the below snapshot where I have created all the ZONE.

If you see the below image there are 4 sub interfaces as per the topology

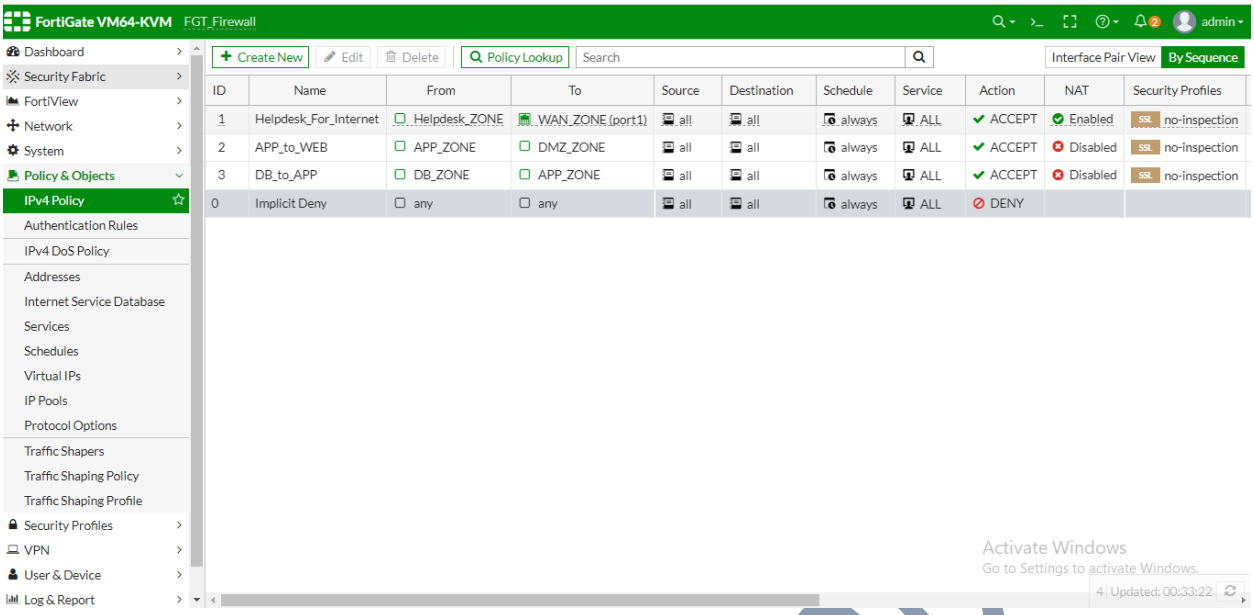
5. APP_VLAN10
6. DB_VLAN20
7. Helpdesk_VLAN30
8. WEB_VLAN40



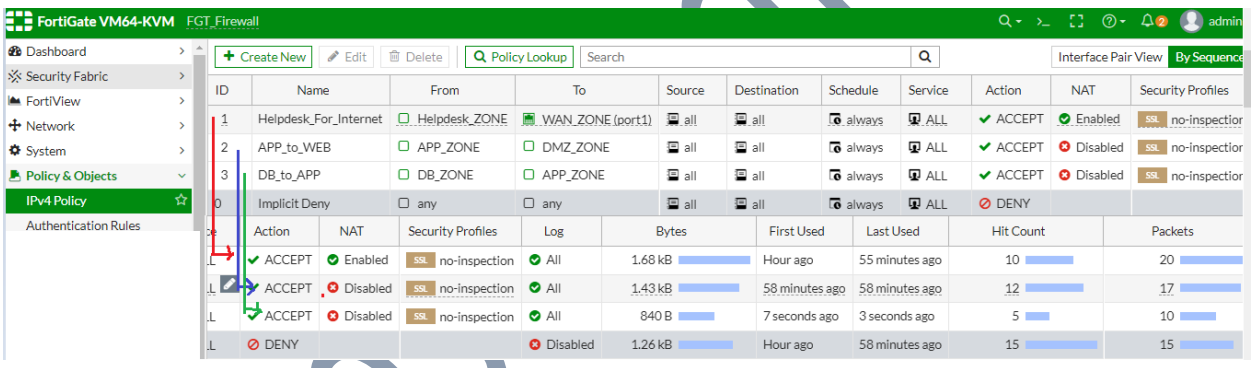
By Expending Zone configuration you can see the SVI have added which is the member of ZONE.



Now we can configure policy you would see that it has been as simple as we wanted it.



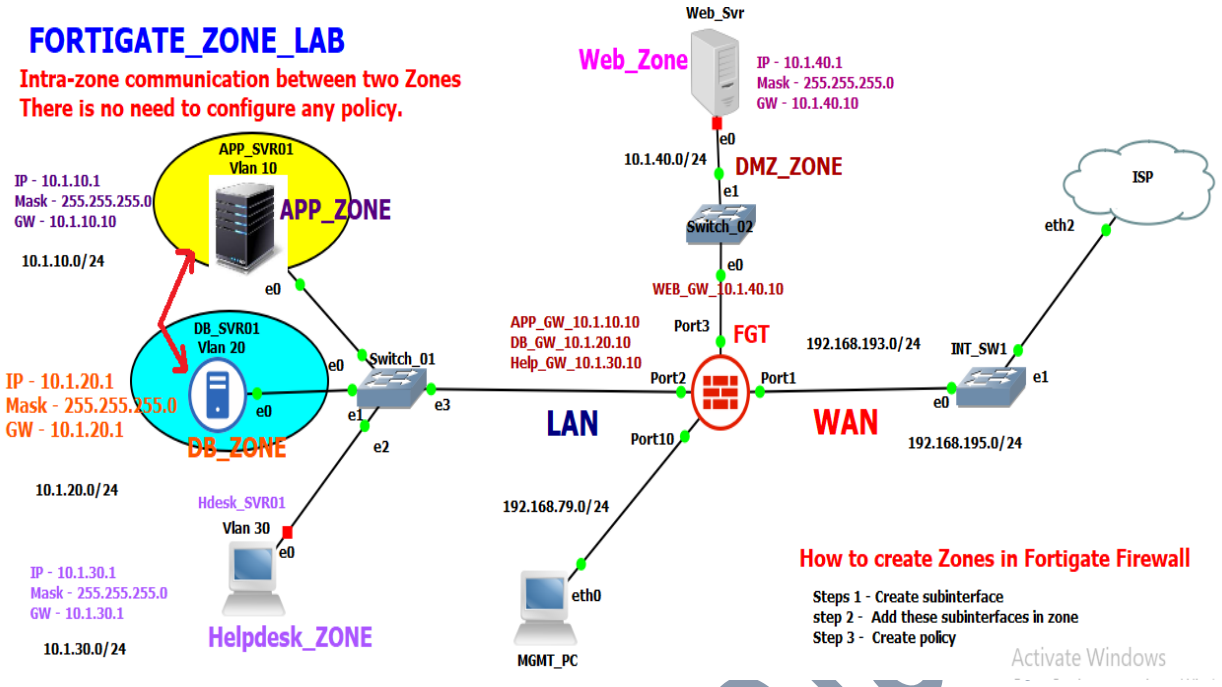
Now we can verify whether whatever we have configured or correct or not by hit count.



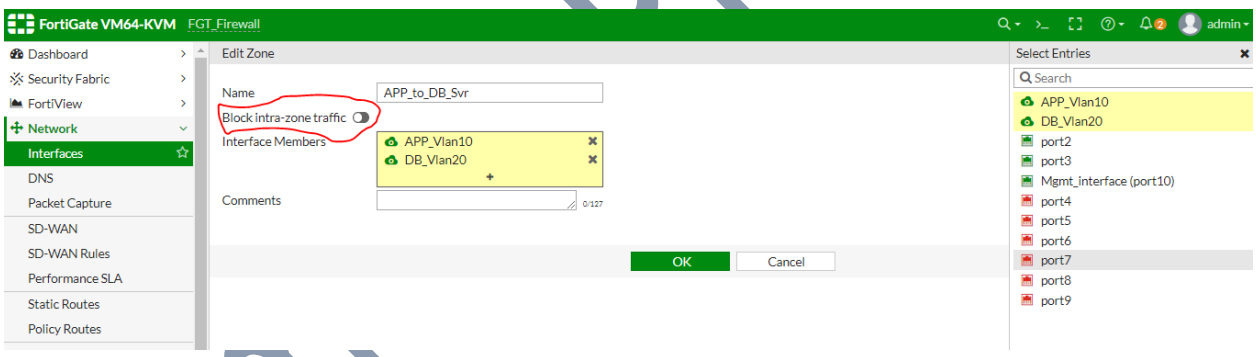
Fortigate Intra Zone communication configuration –

If you have created two Zone (APP, DB) and you want to ensure that communication should be between both server then you don't have to configure any policy between both Zones.

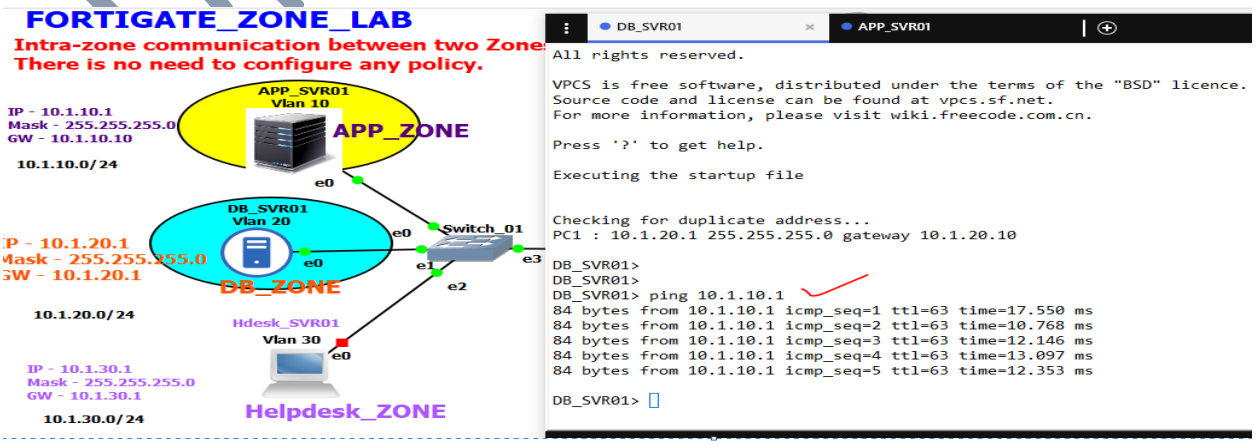
Note – In my case I have shown you only communication between two Zones but in your it could be multiple Zones.

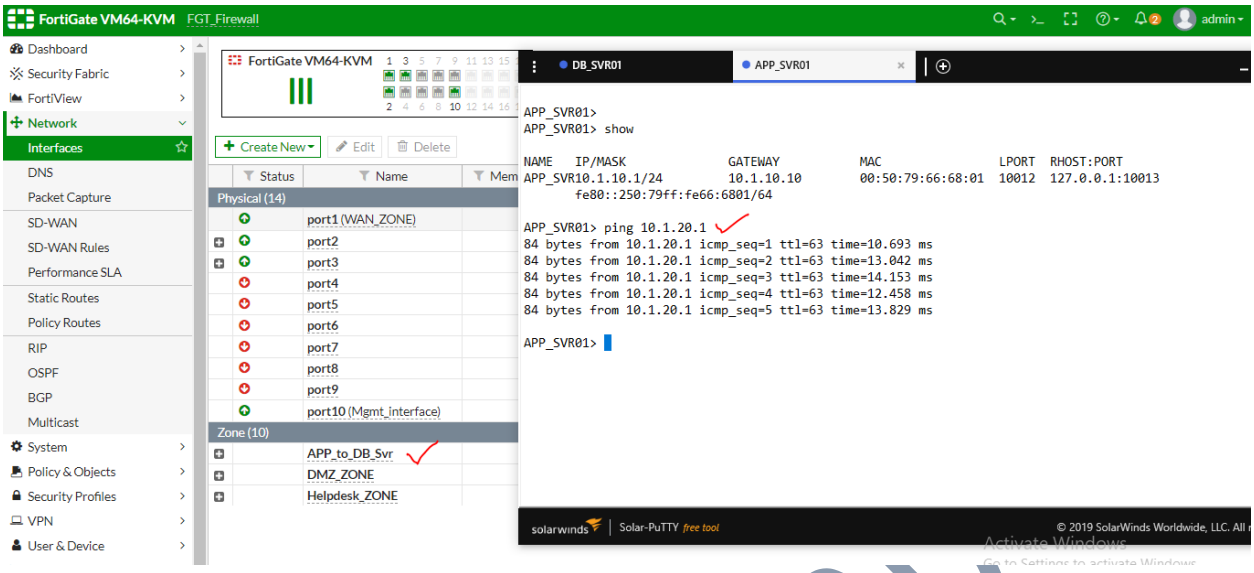


Between two zones ensure that Block intra-zone traffic should be off otherwise communication will not be happen between the zones.



Now lets check it out once turned off this option - Block intra-zone





Keep in mind – There is no policy required when you tuned off this option block intra zone traffic while creating the zones between two different Zones.

Object – Fortigate HA configuration – Active – passive mode.

Before to start the HA configuration I would like to discuss few things that we need to understand fortinet HA terminology and their modes. There are three modes that fortigate supports for HA.

1. Standalone mode (Default mode)
2. Active – Passive mode (A-P)
3. Active – Active mode (A-A)

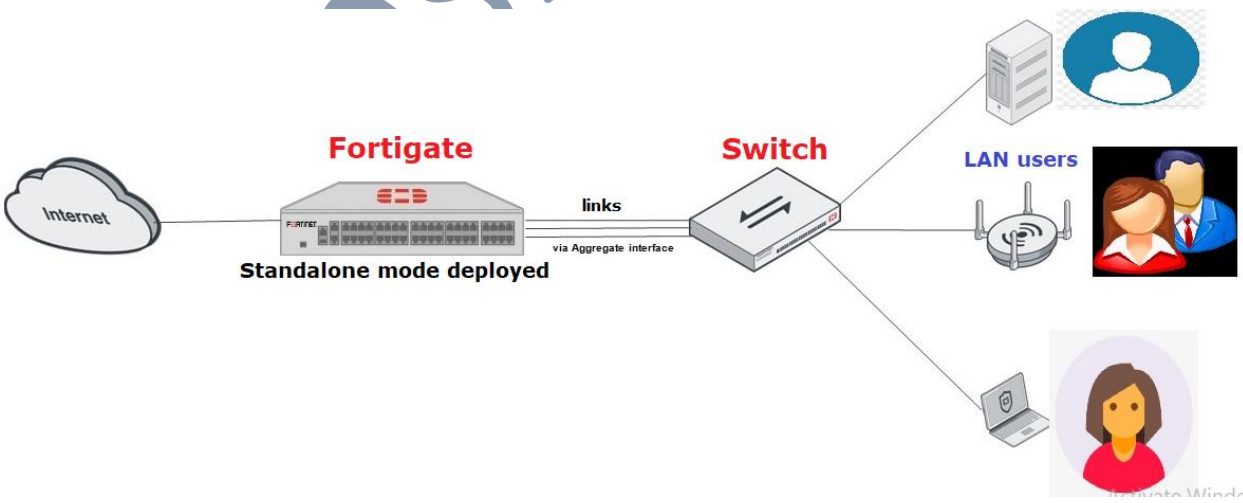
Now let's talk about what is HA and why it is required for our organization.

HA – High availability

1. High availability is one kind of mechanism that fortigate supports If in case of primary device goes down then secondary device will come up without any delay or interruptions. Or you can say that it provides redundancy in the Network.
2. HA functions similar to VRRP, but one of the main differences is that you absolutely must have two same FortiGate models to achieve HA.
3. Fortigate uses FGCP (Fortigate Clustering protocol) When fortigate sync their configurations with the clusters.
4. HA failover must be deployed in our organization if we want redundancy.
5. If there is single fortigate firewall deployed in your network so mode will be always – Standalone. For verification you check by – get system status.

Now let's put on one glimpse on standalone mode by below the topology.

What will happen If this standalone fortigate firewall get down, all the traffic will come to firewall and simply will be dropped.

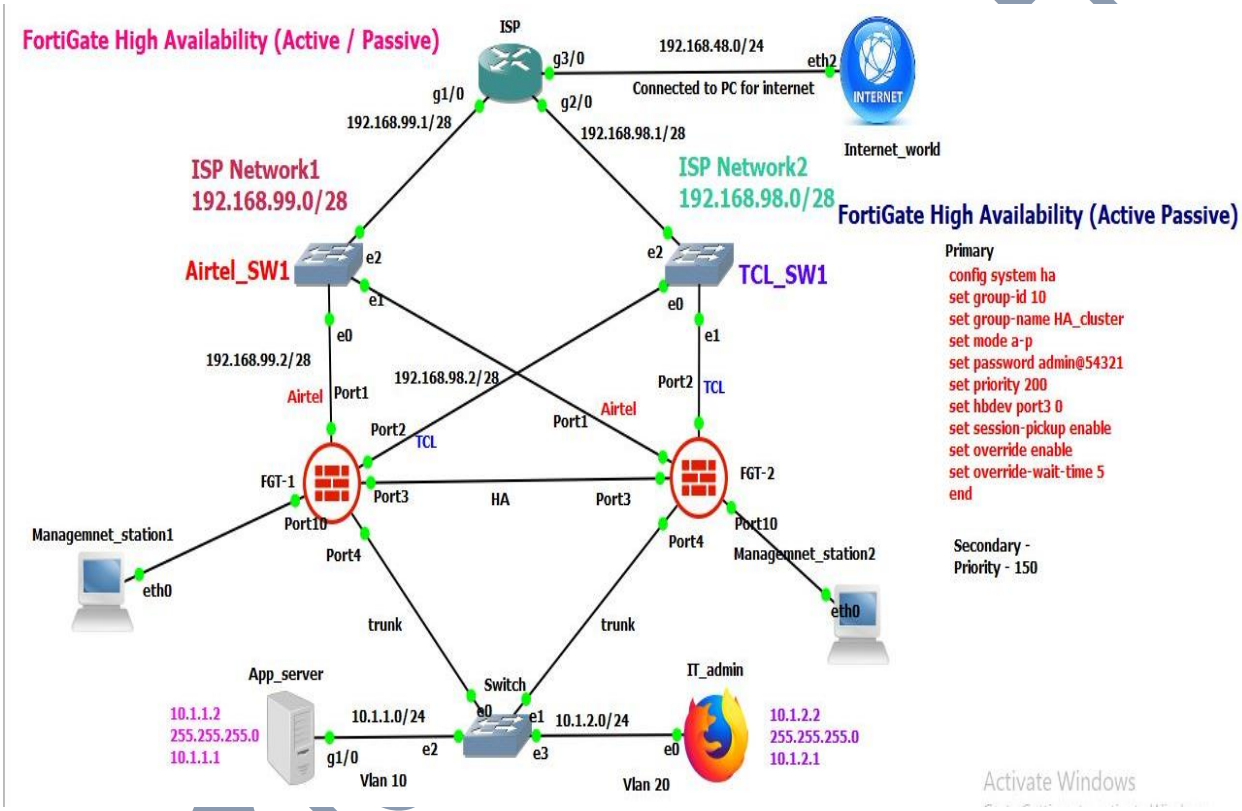


To achieve redundancy we deploy either A-P mode or A-A mode. Now in this article I am going to discuss only A-P mode. Will discuss for A-P next article.

Before to begin A-P mode configuration there are few prerequisites that fortigate recommends us to follow.

1. Make sure your FortiGate interfaces are configured with static IP addresses. If any interface gets its address using DHCP or PPPoE you should temporarily switch it to a static address and enable DHCP or PPPoE after the cluster has been established.
2. Make sure the FortiGates are running the same FortiOS firmware version.
3. All the FortiGates in a cluster must have the same level of licensing.

Now I am about to show you Fortigate HA (A-P) mode using the below topology.



Let me show you what I have done in this topology to achieve redundancy.

Configuration road map – At Switch

There are two vlans one is Vlan 10 and another one is Vlan 20 which belongs to App and IT respectively.

- Switch(config)#interface e 0/2

Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10

- Switch(config)#interface e 0/3
  Switch(config-if)#switchport mode access
  Switch(config-if)#switchport access vlan 20

- Switch(config)#interface range e 0/0 – e0/1
  Switch(config-if)#switchport trunk encapsulation dot1q
  Switch(config-if)#switchport mode trunk

Configuration road map – ISP Router (For example)

ISP(config)#interface G 3/0 is connected to public network/ Internet (This port is connected to my physical machine to get the internet).

- ISP(config)#interface G 3/0
  ISP (config-if)#ip address 192.168.50.1 255.255.255.0
  ISP (config-if)#no shutdown

- ISP(config)#interface G 1/0
  ISP (config-if)#ip address 192.168.99.1 255.255.255.248
  ISP (config-if)#no shutdown
- ISP(config)#interface G 2/0
  ISP (config-if)#ip address 192.168.98.1 255.255.255.248
  ISP (config-if)#no shutdown

Now here we have to configure interesting traffic that is called ACL and NAT needs to be configured.

- ISP (config)#access-list 10 permit any
  ISP(config)#ip nat inside source list 10 interface G 0/0 overload
  ISP(config)#interface G1/0
  ISP(config-if)#ip nat inside
  ISP(config)#interface G2/0
  ISP(config-if)#ip nat inside
  ISP(config)#interface G3/0
  ISP(config-if)#ip nat outside

Now I am going to assign IP address on the WAN interfaces.

- FGT_Primary (interface) # show
  Config system interface
  edit "port1"
  set ip 192.168.99.2 255.255.255.0

set allowaccess ping
set alias "Airtel_Port1"
set role wan
next
end

edit "port2"
set ip 192.168.98.2 255.255.255.0
set allowaccess ping
set type physical
set alias "TCL_Port2"
set role wan
next
end

For Management Interface –

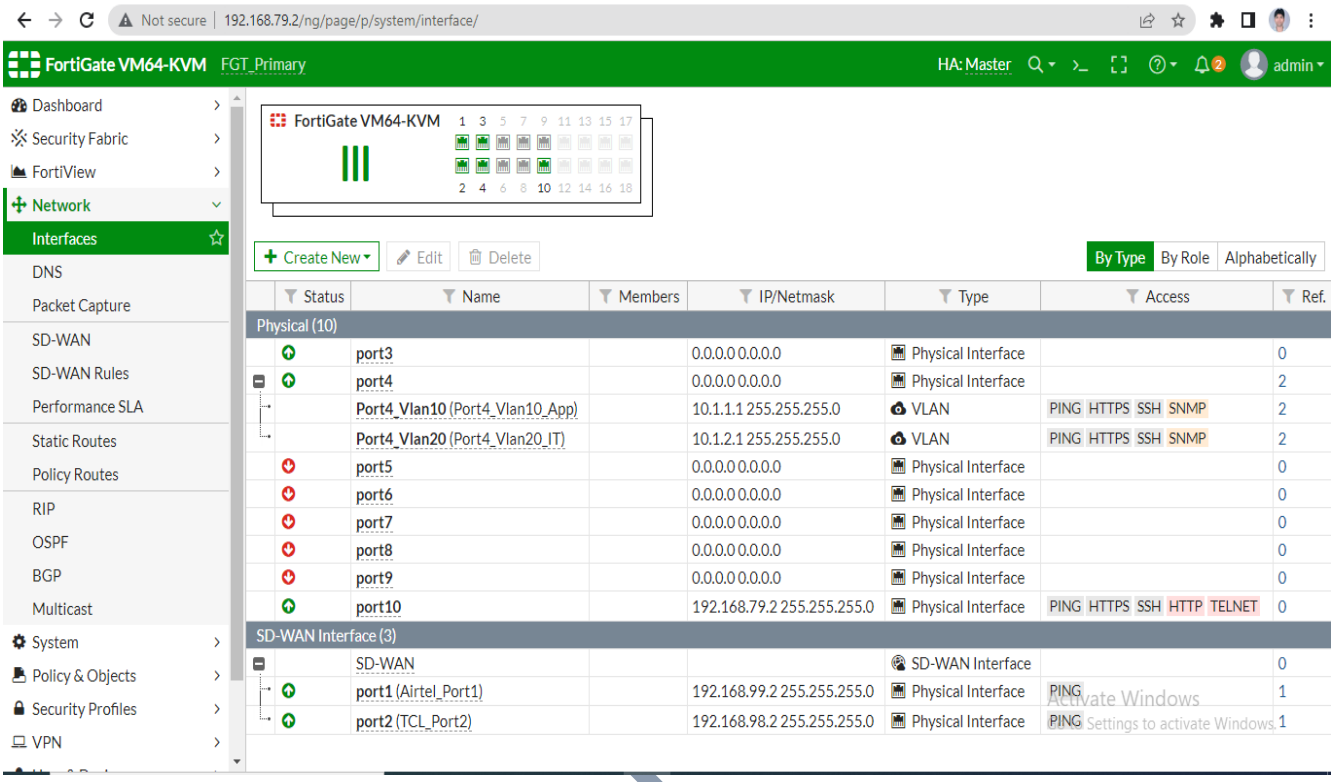
- FGT_Primary (interface) # show
  Config system interface
  edit "port10"
  set ip 192.168.79.2 255.255.255.0
  set allowaccess ping https ssh http telnet
  next
  end

Sub interfaces creation on fortigate firewall –

- edit "Port4_Vlan10"
  set ip 10.1.1.1 255.255.255.0
  set allowaccess ping https ssh snmp
  set alias "Port4_Vlan10_App"
  set role lan
  set interface "port4"
  set vlanid 10
  next
- edit "Port4_Vlan20"
  set ip 10.1.2.1 255.255.255.0
  set allowaccess ping https ssh snmp
  set alias "Port4_Vlan20_IT"
  set role lan
  set interface "port4"
  set vlanid 20
  next

end

What I have configured in CLI it will see in fortigate GUI page –



Note – I have configured SDWAN as well in this topology but at this time I will show you only for HA (A-P mode) in this article.

Now lets move towards HA configuration on primary firewall.

Please follow below simple configuration if you want to do lab right.

For this topology I have taken only single HA links but you can choose as per your requirements but I will recommend you choose two heartbeat interfaces.

At Primary HA Firewall -

- config system ha
  set group-id 10
  set group-name HA_cluster
  set mode a-p
  set password admin@54321

set priority 200
set hbdev port3 0
set session-pickup enable
set override enable
set override-wait-time 5
end

At Secondary HA Firewall –

Make sure we only have to configure host name & HA configuration along with change priority of slave device that's it.

- config system ha
  set group-id 10
  set group-name HA_cluster
  set mode a-p
  set password admin@54321
  set priority 150
  set hbdev port3 0
  set session-pickup enable
  set override enable
  set override-wait-time 5
  end

let's verified ha configuration using # get system ha status command.

FGT_Primary # get system ha status

HA Health Status: OK

Model: FortiGate-VM64-KVM

Mode: HA A-P

Group: 10

Debug: 0

Cluster Uptime: 0 days 0:25:21

Cluster state change time: 2022-05-23 00:06:51

Master selected using:

<2022/05/23 00:06:51> FGVMEVTIWWWKMM48 is selected as the master because it has the largest value of override priority.

<2022/05/22 23:42:29> FGVMEVTIWWWKMM48 is selected as the master because it's the only member in the cluster.

ses_pickup: enable, ses_pickup_delay=disable

override: enable

Configuration Status:

FGVMEVTIWWWKMM48(updated 2 seconds ago): in-sync

FGVMEVNIHXPQ_Y59(updated 2 seconds ago): in-sync

System Usage stats:

FGVMEVTIWWWKMM48(updated 2 seconds ago):

sessions=127, average-cpu-user/nice/system/idle=2%/0%/1%/87%, memory=83%

FGVMEVNIHXPQ_Y59(updated 2 seconds ago):

sessions=0, average-cpu-user/nice/system/idle=0%/0%/1%/90%, memory=77%

HBDEV stats:

FGVMEVTIWWWKMM48(updated 2 seconds ago):

port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=170522/593/0/0, tx=2901934/7868/0/0

FGVMEVNIHXPQ_Y59(updated 2 seconds ago):

port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=267505/767/0/0, tx=169429/590/0/0

Master: FGT_Primary , FGVMEVTIWWWKMM48, HA cluster index = 0

Slave : FGT_Secondary , FGVMEVNIHXPQ_Y59, HA cluster index = 1

number of vcluster: 1

vcluster 1: work 169.254.0.1

Master: FGVMEVTIWWWKMM48, HA operating index = 0

Slave : FGVMEVNIHXPQ_Y59, HA operating index = 1

FGT_Primary #

get system ha

FGT_Primary # get system ha

group-id : 10

group-name : HA_cluster

mode : a-p

sync-packet-balance : disable

password : *

hbdev : "port3" 0

session-sync-dev :

route-ttl : 10

route-wait : 0

route-hold : 10

multicast-ttl : 600

sync-config : enable

encryption : disable

authentication : disable

hb-interval : 2

hb-lost-threshold : 20

hello-holddown : 20

gratuitous-arps : enable

arps : 5

arps-interval : 8

session-pickup : enable

session-pickup-connectionless: disable

session-pickup-expectation: disable

session-pickup-delay: disable

link-failed-signal : disable

uninterruptible-upgrade: enable

ha-mgmt-status   : disable

ha-eth-type   : 8890

hc-eth-type   : 8891

l2ep-eth-type   : 8893

ha-uptime-diff-margin: 300

vcluster2   : disable

vcluster-id   : 1

override   : enable

priority   : 200

override-wait-time : 5

monitor   :

pingserver-monitor-interface:

vdom   : "root"

ssd-failover   : disable

memory-compatible-mode: disable

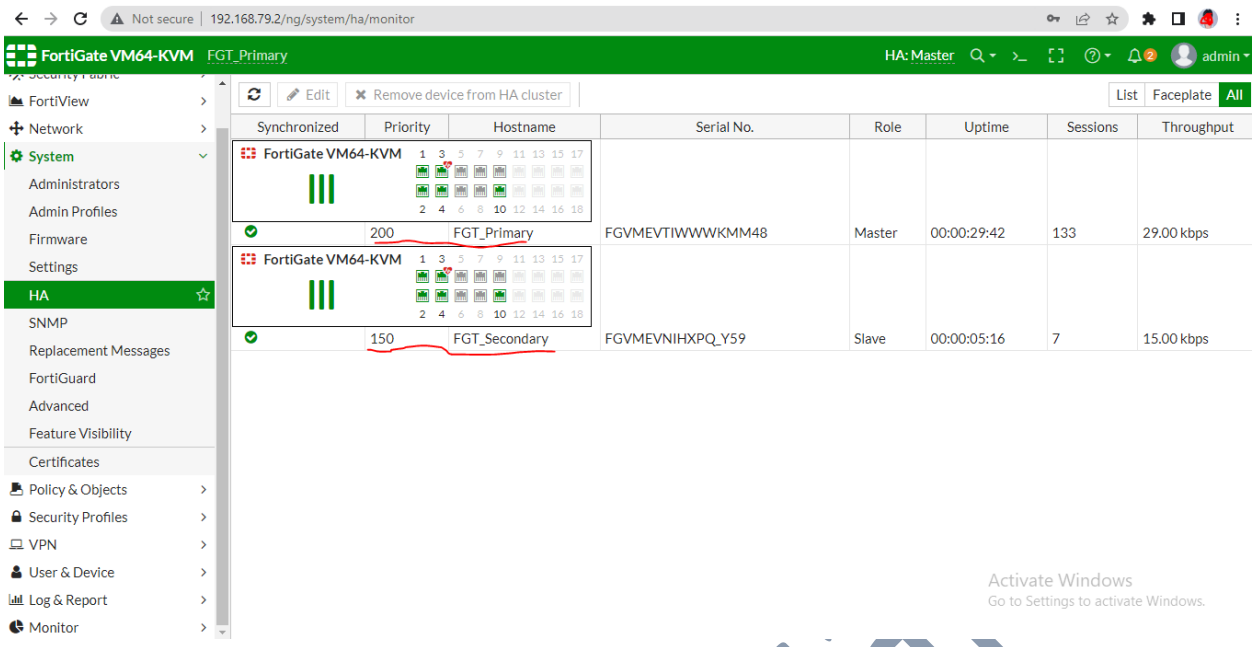
inter-cluster-session-sync: disable

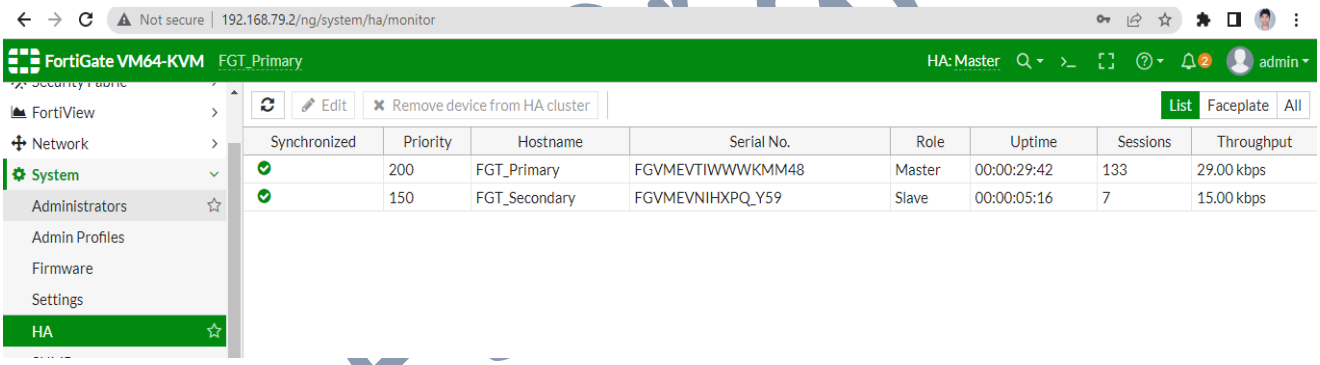
unicast-hb   : disable

logical-sn   : disable

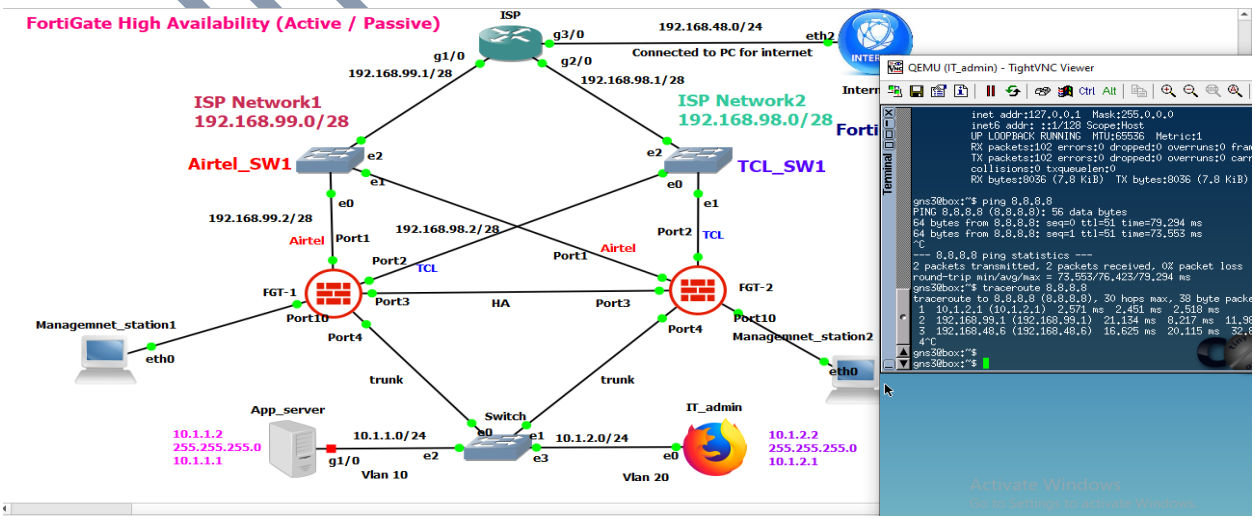
FGT_Primary #

For GUI verification - Go to system and click on HA

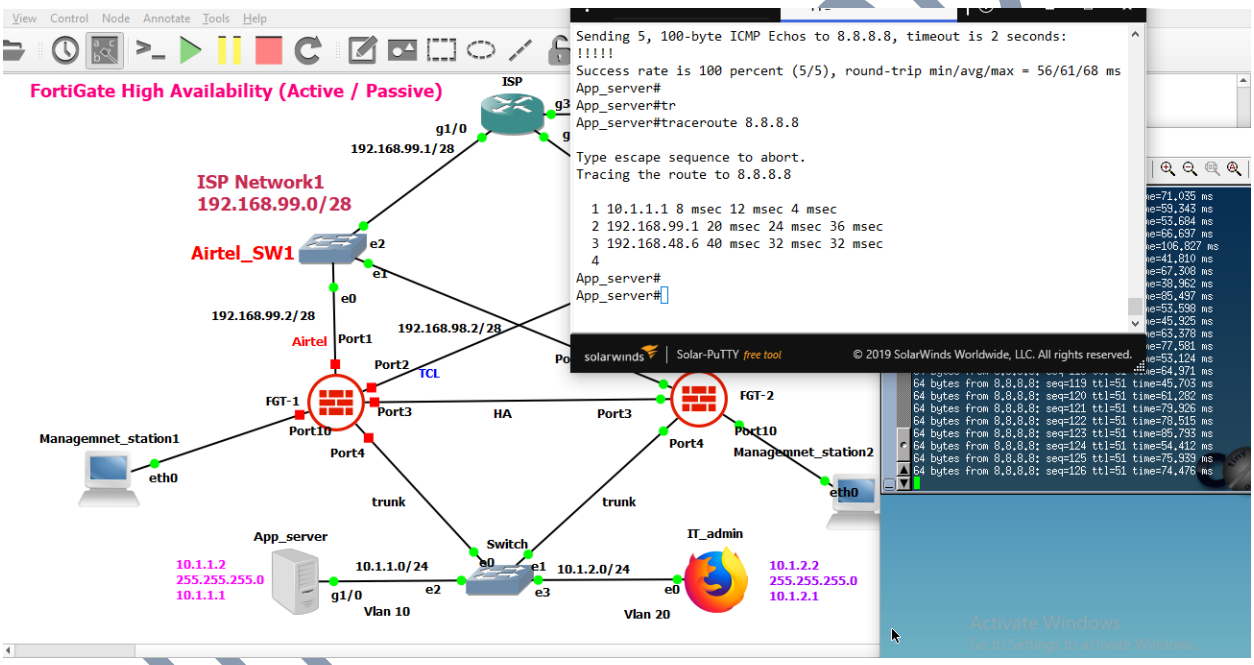




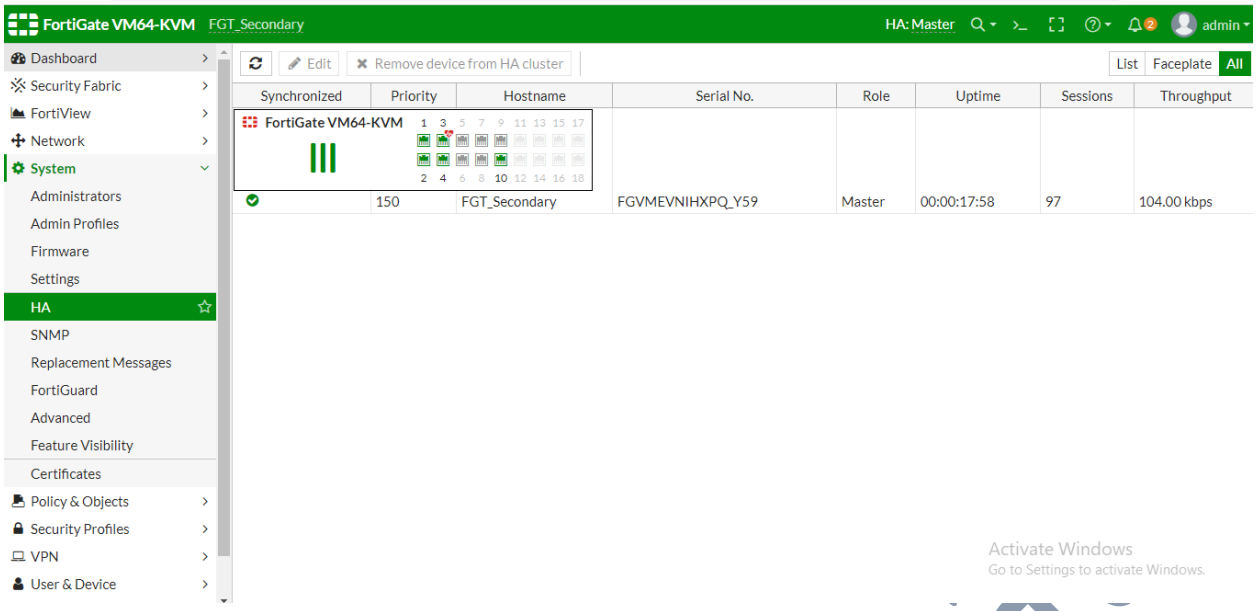
In order to verify I am going to check from the IT admin which belongs into Vlan 20.



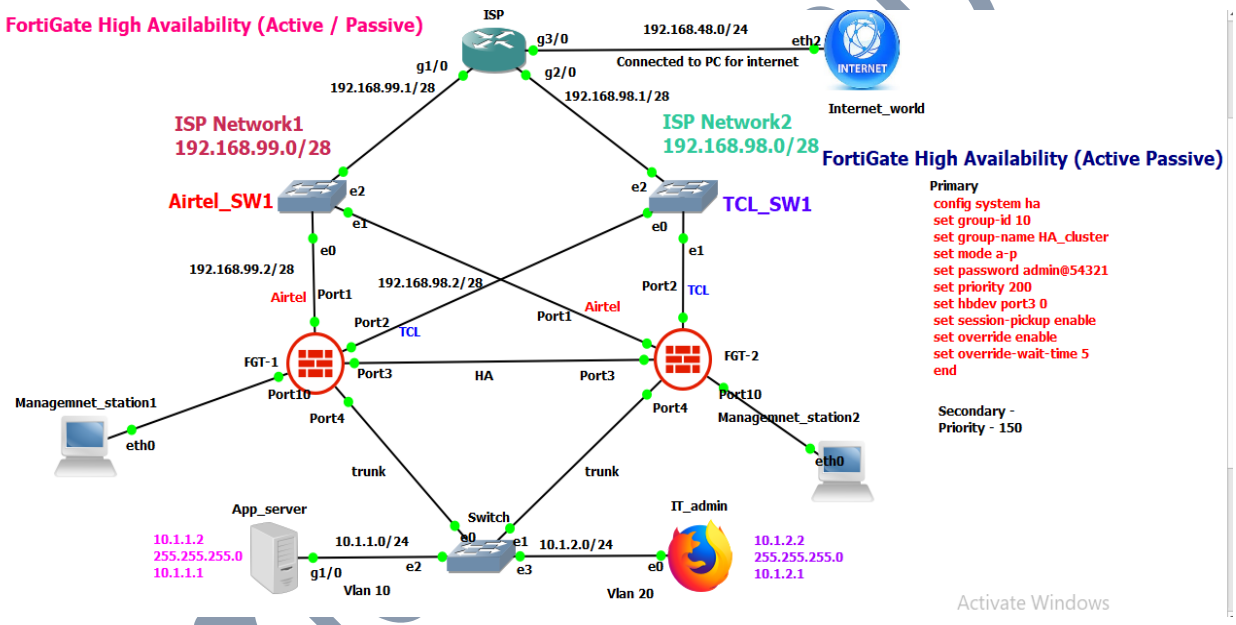
As you can see that traffic is going through primary foritgate firewall. Now I am going to down primary fortigate firewall



We can also verify from the GUI also that secondary Firewall is up & working fine once primary firewall goes down right.



Final Fortigate HA topology –



Point to be remembered – whenever you are going to deploy HA in your topology you must terminate your WAN/LAN links through switch.

Note – I will discuss all the HA configuration in details with wire shark in upcoming notes It was just for demonstration purpose only.

In order to configure HA A-A mode we must follow the following criteria according to fortinet.

- All the fortigates in the cluster must be the same model and have the same firmware installed. Or you can say that Appliances must have the same hardware model and same firmware version
- Cluster members must also have the same hardware configuration such as the same number of hard disks.
- Make sure the WAN / LAN interfaces are not getting their IP addresses from DHCP, or PPPoE otherwise there could be delay while getting IP addresses from DHCP or PPPOE. We must configure their IP addresses static. However we can do it but don't think.
- Ensure that WAN or LAN interface must be connected via switch.
- Must be use at least two heartbeat interfaces to avoid single point of network failure.

Active-active HA (load balancing and failover protection)-

- An active-active HA cluster consists of a primary unit that receives all communication sessions and load balances them among the primary unit and all of the subordinate units. In an active-active cluster the subordinate units are also considered active since they also process content processing sessions. In all other ways active-active HA operates the same as active-passive HA.
- With help of A-A mode fortinet can provide load balance between both clusters. Or you can say that to utilize both clusters we deploy in A-A mode.

I want to add those configuration which I will configuration in this lab. Getting started fortinet HA A-A mode configuration.

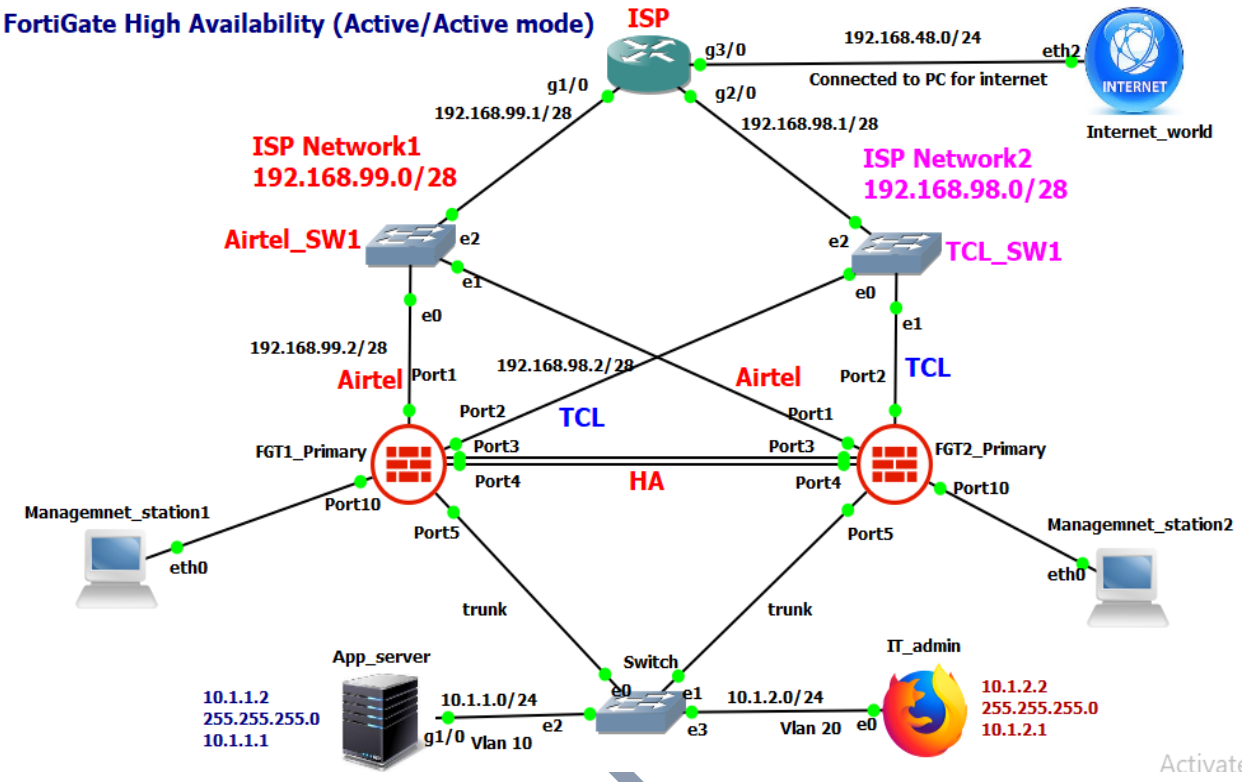
HA configuration road map -

- config system ha
- set group-id 10
- set group-name HA_cluster
- set mode a-a
- set password admin@54321
- set priority 200
- set hbdev port3 0 port4 1
- set session-pickup enable
- set override enable
- set override-wait-time 5
- set monitor port1 port2 port3 port4
- end

Point to be remember –

1. HA configuration must be configured same on every cluster otherwise HA will not be form.
2. You don't have to configure the entire configuration on every cluster except HA and their hostname.

3. Port must be connected the same for both clusters.



In this topology we will show you how to configure HA A-A mode but before that I would like to tell what I have configured on other device such as ISP router in order to ISP router can communicate outside world – Google) for example. At LAN switch I have configured vlans & trunking that's it.

- Interesting traffic configured - ISP (config)#access-list 10 permit any
- ISP(config)#ip nat inside source list 10 interface G 0/0 overload
  ISP(config)#interface range G1/0 -2
  ISP(config-if)#ip nat inside
  ISP(config)#interface G3/0
  ISP(config-if)#ip nat outside

Now I am going to describe a little bit about fortinet ha configuration commands–

- config system ha

- set group-id 10
- set group-name HA_cluster
- set mode a-a
- set password admin@54321
- set priority 200
- set hbdev port3 0 port4 1
- set session-pickup enable
- set override enable
- set override-wait-time 5
- set monitor port1 port2 port3 port4
- end

If you want to configure ha configuration then you will have to enter below command.

- config system ha

The following below commands are used for cluster identification-

- Group ID - set group-id 10
- Group name - set group-name
- Password - set password XXXXX

Priority decides which device will become primary or secondary

- Priority - set priority 200

For ha configuration you will have to decide which modes do we need to choose whether - stand alone, Active-Active or Active-Passive it's up to you.

- Set mode – stand alone , A-A, A-P

hbdev commands decides which port will use for heartbeat interface.(Set the network interface to be used for heartbeat packets. You can configure one or two heartbeat ports.) to configure heartbeat interface use the below command -

- set hbdev port3 0 port4 1 (as per the my topology)

If session pickup is not enabled, the FGCP does not synchronize the primary unit session table to other cluster units and sessions do not resume after a failover. After a device or link failover all sessions are briefly interrupted and must be re-established at the application level after the cluster renegotiates. If you want to enable it you can enable it by using the below command-

- set session-pickup enable

If you want to make sure that the same cluster unit always operates as the primary unit once come back up then you should enable below command- To enable override.

- set override enable (The HA override CLI command is disabled by default)

Note - Fortigate HA selection process -Priority, age, serial no of the device.

For links monitoring you should use below commands -

- set monitor port1 port2 port3 port4

Point to be remembered –

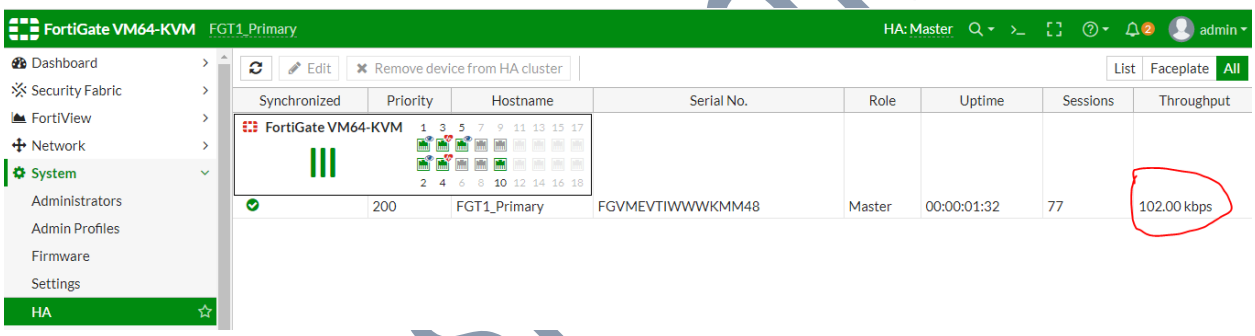
We have to configure only HA configuration and needs to be changed host name of secondary device that's it. Priority should be less than the primary device it depends up to you in my case it is – 150 at secondary device for primary it is 200.

Now let's check the fortinet HA active-active mode configuration on the primary device. Once configuration are done then you see the below output in the CLI & GUI of primary device.

```
FGT1_Primary # get system ha
group-id              : 10
group-name            : HA_cluster
mode                  : a-a
sync-packet-balance : disable
password              : *
hbdev                 : "port3" 0 "port4" 1
session-sync-dev      :
route-ttl             : 10
route-wait            : 0
route-hold            : 10
multicast-ttl         : 600
sync-config           : enable
encryption            : disable
authentication        : disable
hb-interval           : 2
hb-lost-threshold     : 20
hello-holddown        : 20
gratuitous-arps       : enable
arps                  : 5
arps-interval         : 8
session-pickup        : enable
session-pickup-connectionless: disable
session-pickup-expectation: disable
session-pickup-delay: disable
link-failed-signal  : disable
uninterruptible-upgrade: enable
ha-mgmt-status      : disable
ha-eth-type         : 8890
hc-eth-type         : 8891
l2ep-eth-type       : 8893
ha-uptime-diff-margin: 300
vcluster2           : disable
vcluster-id         : 1
override            : enable
priority            : 200
override-wait-time  : 5
schedule            : round-robin
monitor             : "port1" "port2" "port3" "port4" "port5"
pingserver-monitor-interface:
vdom                : "root"
ssd-failover        : disable
memory-compatible-mode: disable
inter-cluster-session-sync: disable
load-balance-all    : disable

FGT1_Primary #
```

```
FGT1_Primary # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-A
Group: 10
Debug: 0
Cluster Uptime: 0 days 0:2:25
Cluster state change time: 2022-05-27 00:03:19
Master selected using:
    <2022/05/27 00:03:19> FGVMEVTIWWWKMM48 is selected as the master because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
load_balance: disable
load_balance_udp: disable
schedule: Round robin.
upgrade_mode: unset

System Usage stats:
    FGVMEVTIWWWKMM48(updated 4 seconds ago):
        sessions=104, average-cpu-user/nice/system/idle=1%/0%/0%/92%, memory=80%
```

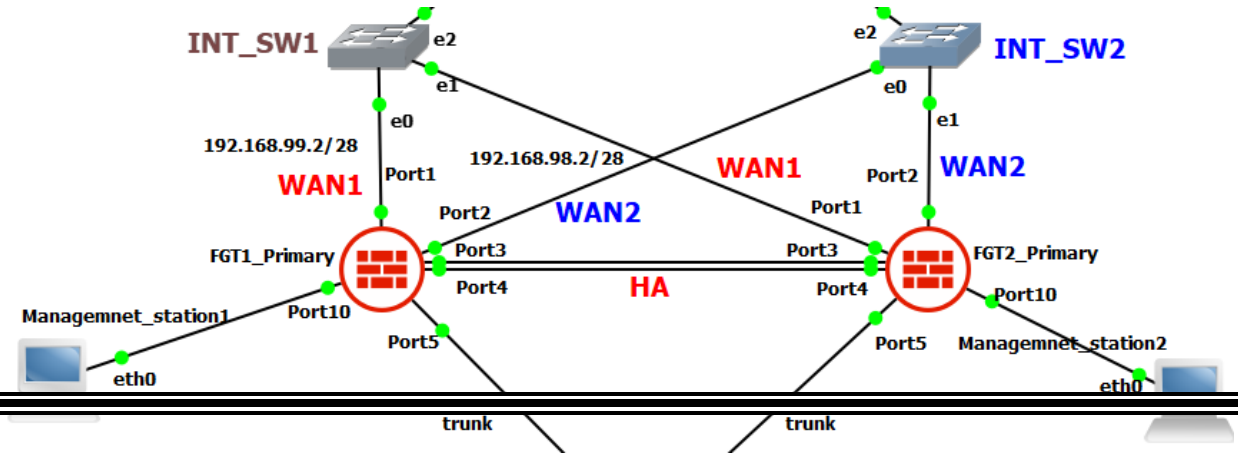
GUI view -



As you can see that there are two heartbeat interfaces which is showing heart symbol.

Now I am going to configure ha active-active configuration at secondary device. Once configuration will be configured at secondary device then you will see that both devices will work as a active –active.

Same HA configuration will be done and you have change priority and hostname that's it.



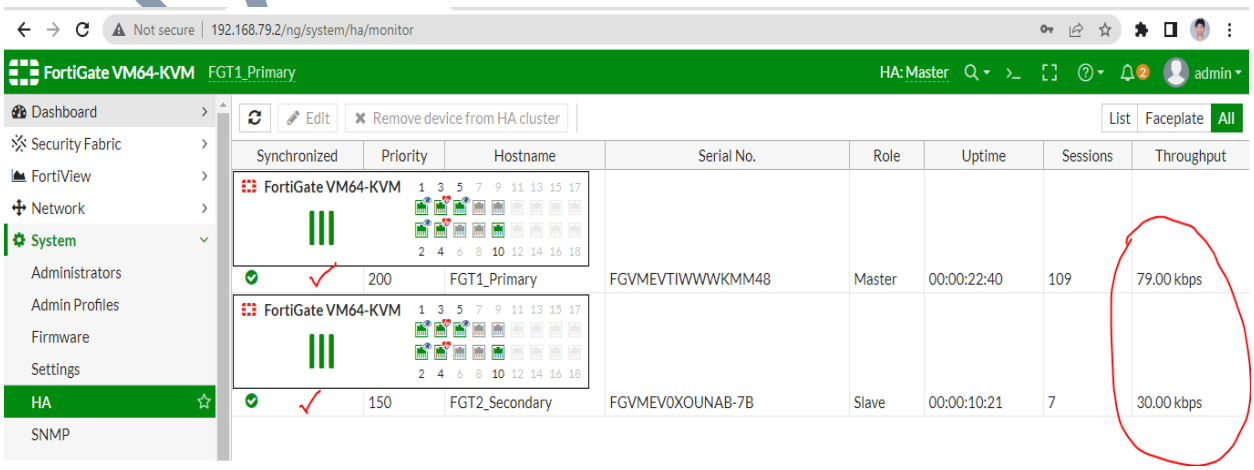
After configuring ha at secondary device –

```
FGT2_Secondary # get system ha
group-id              : 10
group-name            : HA_cluster
mode                  : a-a
sync-packet-balance : disable
password              : *
hbdev                 : "port3" 0 "port4" 1
session-sync-dev      :
route-ttl             : 10
route-wait            : 0
route-hold            : 10
multicast-ttl         : 600
sync-config           : enable
encryption            : disable
authentication        : disable
hb-interval           : 2
hb-lost-threshold     : 20
hello-holddown        : 20
gratuitous-arps       : enable
arps                  : 5
arps-interval         : 8
session-pickup        : enable
session-pickup-connectionless: disable
session-pickup-expectation: disable
session-pickup-delay: disable
uninterruptible-upgrade: enable
ha-mgmt-status        : disable
ha-eth-type           : 8890
hc-eth-type           : 8891
l2ep-eth-type         : 8893
ha-uptime-diff-margin: 300
vcluster2             : disable
vcluster-id           : 1
override              : enable
priority              : 150
override-wait-time    : 5
schedule              : round-robin
monitor               : "port1" "port2" "port3" "port4" "port5"
pingserver-monitor-interface:
vdom                  : "root"
ssd-failover          : disable
memory-compatible-mode: disable
inter-cluster-session-sync: disable
load-balance-all      : disable

FGT2_Secondary #
```

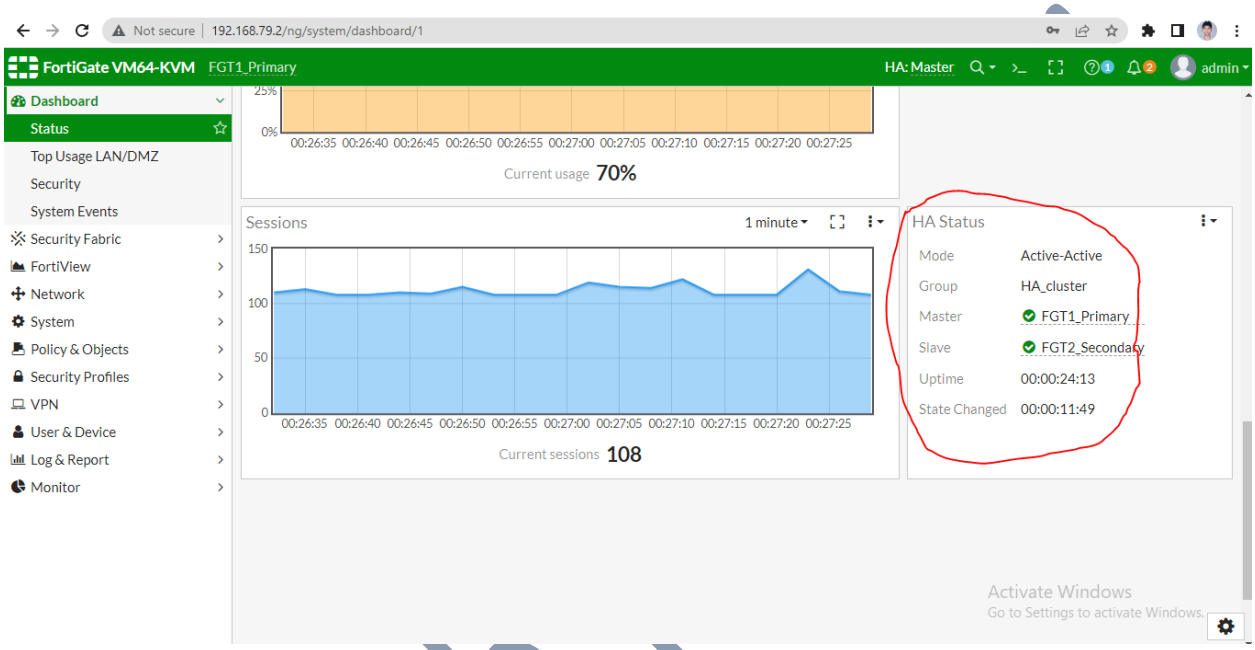


```
FGT2_Secondary # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-A
Group: 10
Debug: 0
Cluster Uptime: 0 days 0:19:47
Cluster state change time: 2022-05-27 00:15:44
Master selected using:
    <2022/05/27 00:15:44> FGVMEVTIWWWKMM48 is selected as the master because it has the largest value of override priority.
ses_pickup: enable, ses_pickup_delay=disable
load_balance: disable
load_balance_udp: disable
schedule: Round robin.
upgrade_mode: unset
override: enable
Configuration Status:
    FGVMEV0XOUNAB-7B(updated 1 seconds ago): in-sync
    FGVMEVTIWWWKMM48(updated 2 seconds ago): in-sync
System Usage stats:
    FGVMEV0XOUNAB-7B(updated 1 seconds ago):
    FGVMEVTIWWWKMM48(updated 2 seconds ago):
        sessions=100, average-cpu-user/nice/system/idle=0%/0%/0%/87%, memory=82%
```

```
HBDEV stats:
    FGVMEV0XOUNAB-7B(updated 1 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=897820/2420/0/0, tx=808134/2202/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=1394376/3185/0/0, tx=1010266/3172/0/0
    FGVMEVTIWWWKMM48(updated 2 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=807767/2201/0/0, tx=2200772/5932/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=1010148/3171/0/0, tx=2695926/6693/0/0
MONDEV stats:
    FGVMEV0XOUNAB-7B(updated 1 seconds ago):
        port1: physical/1000auto, up, rx-bytes/packets/dropped/errors=29100/485/0/0, tx=0/0/0/0
        port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=29100/485/0/0, tx=0/0/0/0
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=897820/2420/0/0, tx=808134/2202/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=1394376/3185/0/0, tx=1010266/3172/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=640/10/0/0, tx=0/0/0/0
    FGVMEVTIWWWKMM48(updated 2 seconds ago):
        port1: physical/1000auto, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=50220/1191/0/0
        port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=50178/1190/0/0
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=807767/2201/0/0, tx=2200772/5932/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=1010148/3171/0/0, tx=2695926/6693/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=1408/22/0/0
Slave : FGT2_Secondary  , FGVMEV0XOUNAB-7B, HA cluster index = 1
Master: FGT1_Primary    , FGVMEVTIWWWKMM48, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.1
Slave : FGVMEV0XOUNAB-7B, HA operating index = 1
Master: FGVMEVTIWWWKMM48, HA operating index = 0

FGT2_Secondary #
```



You can also verify it using Fortinet Dashboard –



Output of both HA clusters when they are in active –active mode.

Primary Device -

```
group-id              : 10
group-name            : HA_cluster
mode                  : a-a
sync-packet-balance   : disable
password              : *
hbdev                 : "port3" 0 "port4" 1
session-sync-dev      :
route-ttl             : 10
route-wait            : 0
route-hold            : 10
multicast-ttl         : 600
sync-config           : enable
encryption            : disable
authentication        : disable
hb-interval           : 2
hb-lost-threshold     : 20
hello-holddown        : 20
gratuitous-arps       : enable
arps                  : 5
arps-interval         : 8
session-pickup        : enable
session-pickup-connectionless: disable
session-pickup-expectation: disable
session-pickup-delay: disable
link-failed-signal    : disable
uninterruptible-upgrade: enable
ha-mgmt-status        : disable
ha-eth-type           : 8890
hc-eth-type           : 8891
l2ep-eth-type         : 8893
ha-uptime-diff-margin: 300
vcluster-id           : 1
override              : enable
priority              : 200
override-wait-time    : 5
schedule              : round-robin
monitor               : "port1" "port2" "port3" "port4" "port5"
pingserver-monitor-interface:
vdom                  : "root"
ssd-failover          : disable
memory-compatible-mode: disable
inter-cluster-session-sync: disable
load-balance-all      : disable

FGT1_Primary #
```

```
FGT1_Primary # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-A
Group: 10
Debug: 0
Cluster Uptime: 0 days 0:6:38
Cluster state change time: 2022-05-27 01:53:17
Master selected using:
    <2022/05/27 01:53:17> FGVMEVTIWWWKMM48 is selected as the master because it has the largest value of override priority.
    <2022/05/27 01:51:39> FGVMEVTIWWWKMM48 is selected as the master because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
load_balance: disable
load_balance_udp: disable
schedule: Round robin.
upgrade_mode: unset
override: enable
Configuration Status:
    FGVMEVTIWWWKMM48(updated 2 seconds ago): in-sync
    FGVMEV0XOUNAB-7B(updated 3 seconds ago): in-sync
System Usage stats:
    FGVMEVTIWWWKMM48(updated 2 seconds ago):
        sessions=101, average-cpu-user/nice/system/idle=0%/0%/1%/86%, memory=82%
    FGVMEV0XOUNAB-7B(updated 3 seconds ago):
        sessions=0, average-cpu-user/nice/system/idle=0%/0%/1%/89%, memory=77%
HBDEV stats:
    FGVMEVTIWWWKMM48(updated 2 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=543160/1480/0/0, tx=733467/1977/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=925630/2547/0/0, tx=1115677/2910/0/0
    FGVMEV0XOUNAB-7B(updated 3 seconds ago):
```

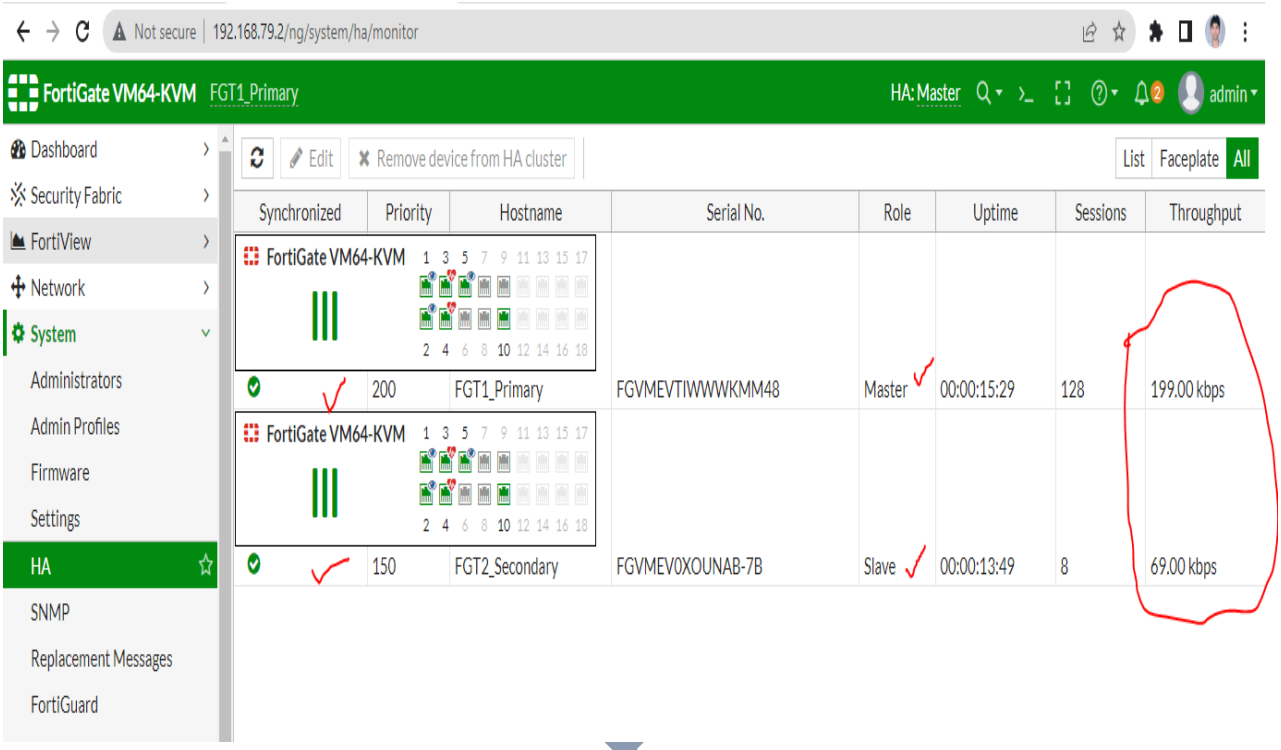
```
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=627732/1692/0/0, tx=542059/1477/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=1009519/2623/0/0, tx=923516/2543/0/0
MONDEV stats:
    FGVMEVTIWWWKMM48(updated 2 seconds ago):
        port1: physical/1000auto, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=17082/402/0/0
        port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=17040/401/0/0
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=543160/1480/0/0, tx=733467/1977/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=925630/2547/0/0, tx=1115677/2910/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=2022/13/0/0, tx=2230/29/0/0
    FGVMEV0XOUNAB-7B(updated 3 seconds ago):
        port1: physical/1000auto, up, rx-bytes/packets/dropped/errors=20880/348/0/0, tx=0/0/0/0
        port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=20820/347/0/0, tx=0/0/0/0
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=627732/1692/0/0, tx=542059/1477/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=1009519/2623/0/0, tx=923516/2543/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=832/13/0/0, tx=0/0/0/0
Master: FGT1_Primary    , FGVMEVTIWWWKMM48, HA cluster index = 0
Slave : FGT2_Secondary  , FGVMEV0XOUNAB-7B, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master: FGVMEVTIWWWKMM48, HA operating index = 0
Slave : FGVMEV0XOUNAB-7B, HA operating index = 1

FGT1_Primary #
```

```
FGT2_Secondary # get system ha
group-id              : 10
group-name            : HA_cluster
mode                  : a-a
sync-packet-balance : disable
password              : *
hbdev                 : "port3" 0 "port4" 1
session-sync-dev      :
route-ttl             : 10
route-wait            : 0
route-hold            : 10
multicast-ttl         : 600
sync-config           : enable
encryption            : disable
authentication        : disable
hb-interval           : 2
hb-lost-threshold     : 20
hello-holddown        : 20
gratuitous-arps       : enable
arps                  : 5
arps-interval         : 8
session-pickup        : enable
session-pickup-connectionless: disable
session-pickup-expectation: disable
session-pickup-delay: disable
link-failed-signal    : disable
uninterruptible-upgrade: enable
ha-mgmt-status        : disable
ha-eth-type           : 8890
hc-eth-type           : 8891
l2ep-eth-type         : 8893
ha-uptime-diff-margin: 300
vcluster2             : disable
vcluster-id           : 1
override              : enable
priority              : 150
override-wait-time    : 5
schedule              : round-robin
monitor               : "port1" "port2" "port3" "port4" "port5"
pingserver-monitor-interface:
vdom                  : "root"
ssd-failover          : disable
memory-compatible-mode: disable
inter-cluster-session-sync: disable
load-balance-all      : disable

FGT2_Secondary #
```

Secondary device –

```
FGT2_Secondary # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-A
Group: 10
Debug: 0
Cluster Uptime: 0 days 0:13:7
Cluster state change time: 2022-05-27 01:53:17
Master selected using:
    <2022/05/27 01:53:17> FGVMEVTIWWWKMM48 is selected as the master because it has the largest value of override priority.
ses_pickup: enable, ses_pickup_delay=disable
load_balance: disable
load_balance_udp: disable
schedule: Round robin.
upgrade_mode: unset
override: enable
Configuration Status:
    FGVMEV0XOUNAB-7B(updated 3 seconds ago): in-sync
    FGVMEVTIWWWKMM48(updated 2 seconds ago): in-sync
System Usage stats:
    FGVMEV0XOUNAB-7B(updated 3 seconds ago):
        sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/87%, memory=78%
    FGVMEVTIWWWKMM48(updated 2 seconds ago):
        sessions=100, average-cpu-user/nice/system/idle=0%/0%/0%/88%, memory=81%
HBDEV stats:
    FGVMEV0XOUNAB-7B(updated 3 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=1351553/3643/0/0, tx=1257709/3427/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=2104672/5211/0/0, tx=1890408/5354/0/0
    FGVMEVTIWWWKMM48(updated 2 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=1258810/3430/0/0, tx=1456917/3927/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=1892706/5358/0/0, tx=2210347/5497/0/0
MONDEV stats:
    FGVMEV0XOUNAB-7B(updated 3 seconds ago):
        port1: physical/1000auto, up, rx-bytes/packets/dropped/errors=44100/735/0/0, tx=0/0/0/0
        port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=44040/734/0/0, tx=0/0/0/0
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=1351553/3643/0/0, tx=1257709/3427/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=2104672/5211/0/0, tx=1890408/5354/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=832/13/0/0, tx=0/0/0/0
    FGVMEVTIWWWKMM48(updated 2 seconds ago):
        port1: physical/1000auto, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=33336/789/0/0
        port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=33294/788/0/0
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=1258810/3430/0/0, tx=1456917/3927/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=1892706/5358/0/0, tx=2210347/5497/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=2022/13/0/0, tx=2230/29/0/0
Slave : FGT2_Secondary  , FGVMEV0XOUNAB-7B, HA cluster index = 1
Master: FGT1_Primary    , FGVMEVTIWWWKMM48, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.1
Slave : FGVMEV0XOUNAB-7B, HA operating index = 1
Master: FGVMEVTIWWWKMM48, HA operating index = 0

FGT2_Secondary #
```

Output of HA status from the GUI –



You can verify ha status using the following commands –

#get system ha

#get system ha status

Point to be remembered if you want move from the primary device to secondary device then you will have to run below command –

execute ha manage Id (of the cluster) such as 0 , 1

If you want to check Id you can check it using the below command –

get system ha status

```
Master: FGT1_Primary    , FGVMEVTIWWWKMM48, HA cluster index = 0
Slave : FGT2_Secondary  , FGVMEV0XOUNAB-7B, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master: FGVMEVTIWWWKMM48, HA operating index = 0
Slave : FGVMEV0XOUNAB-7B, HA operating index = 1
```

execute ha manage ----→ output

```
FGT1_Primary # execute ha manage
<id>    please input peer box index.
<1>     Subsidary unit FGVMEV0XOUNAB-7B


FGT1_Primary # execute ha manage 1
Incomplete command!
Command fail. Return code -56

FGT1_Primary # execute ha manage 1
<string>    Login admin name.

FGT1_Primary # execute ha manage 1 admin
Warning: Permanently added '169.254.0.2' (ED25519) to the list of known hosts.
admin@169.254.0.2's password:
WARNING: File System Check Recommended! Unsafe reboot may have caused inconsistency in disk drive.
It is strongly recommended that you check file system consistency before proceeding.
Please run the 'execute disk list' and then 'execute disk scan <ref#>'.
Note: The device will reboot and scan during startup. This may take up to an hour
FGT2_Secondary #
FGT2_Secondary #
```

Example -

execute ha manage 0 admin-EXAMPLE < ----- 0 is the ID of secondary unit and EXAMPLE is the admin username.

execute ha manage 0 admin-EXAMPLE < ----- 1 is the ID of secondary unit and EXAMPLE is the admin username.

If you want to go back into primary device then type exit command in cli.

There are so many commands for ha configuration you can use it as per your requirement –

- config system ha
- set arps <integer>
- set arps-interval <integer>
- set datadev <datasource>
- set group-id <integer>
- set group-name <string>

- set hb-interval <integer>
- set hb-lost-threshold <integer>
- set hbdev <datasource>
- set http-persistence-pickup {enable|disable}
- set local-node-id <integer>
- set l4-persistence-pickup {enable|disable}
- set l4-session-pickup {enable|disable}
- set mode {active-active | active-passive | standalone}
- set monitor <datasource>
- set node-list {0 1 2 3 4 5 6 7}
- set override {enable|disable}
- set priority <integer>
- set remote-ip-monitor {enable|disable}
- set remote-ip-failover-hold-time <integer>
- set remote-ip-failover-threshold <integer>
- config remote-ip-monitor-list
- edit <name>
- set health-check-interval <integer>
- set health-check-retry <integer>
- set health-check-timeout <integer>
- set interface <datasource>
- set remote-address <class_ip>
- end

Keep attention –

I have configured these things as per my understanding if there are any kind of error please let me know as soon as possible and all the topics has been described in the layman term. I hope this note will be also helpful for you all.

I want your support to share, like and comment.

Your one comment, share and like will encourage to me make more notes as you know that I am posting daily basis notes here , I will highly appreciate your comment, like, share as well.

Remaining notes is paid if you wish you can contact me on the given email Id-

Umesh1123@gmail.com

Don’t Forget like, share and comment

Thank you so much for reading this note–

Umesh Prajapati

For more notes you can reach out to me via email – umesh11238@gmail.com