

Fortigate HA configuration

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)

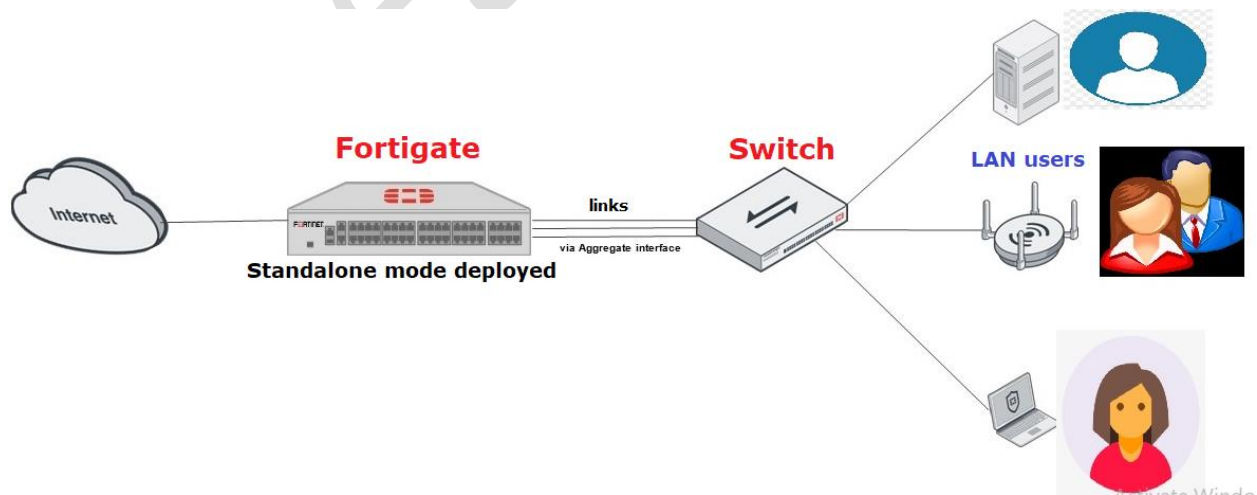
Now let's talk about what is HA and why it is required for our organization.

HA – High availability

1. High availability is one kind of mechanism that's provides redundancy in the network 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 using below the topology.

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



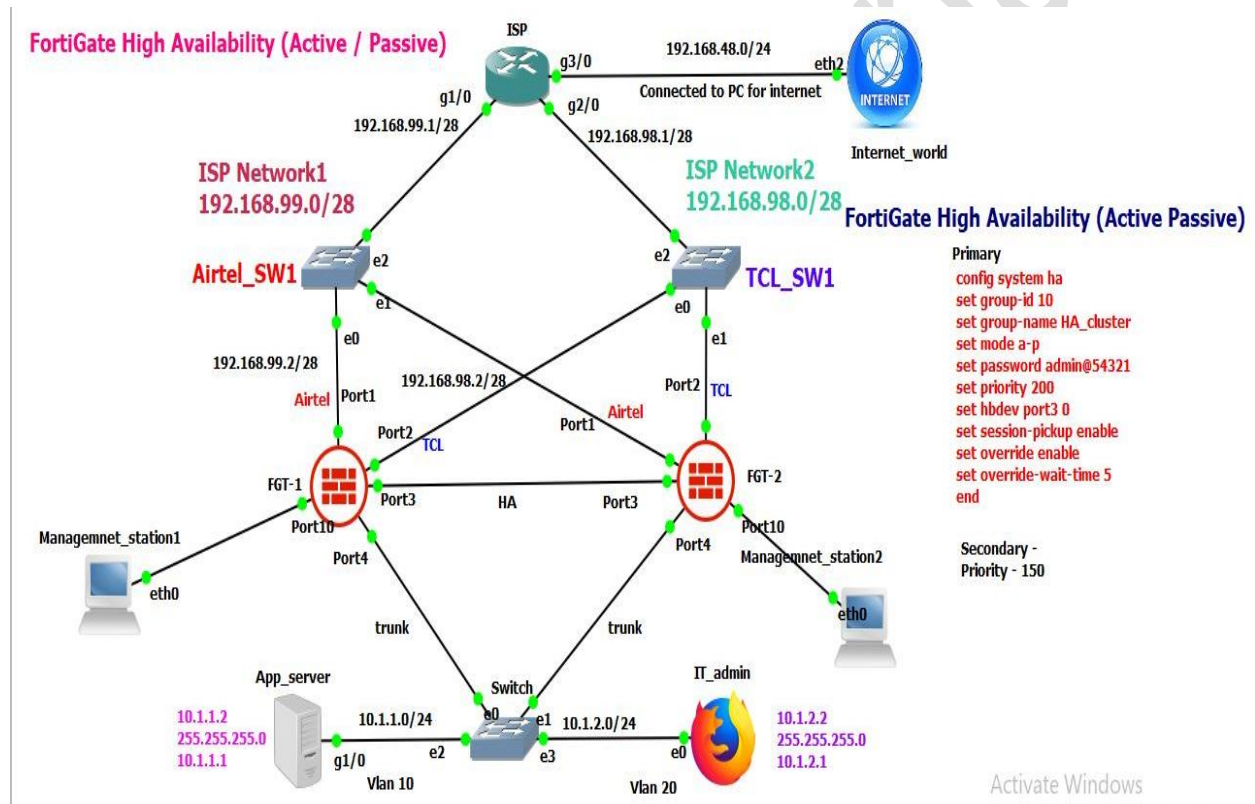
Fortigate HA configuration

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-A 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.

Fortigate HA configuration

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

Fortigate HA configuration

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

Fortigate HA configuration

- 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 –

The screenshot shows the FortiGate VM64-KVM GUI. The left sidebar has a menu with 'Network' selected, and 'Interfaces' is the active view. The main area displays a table of interfaces. A small window above the table shows a 4x4 grid of interface status icons, with the 10th icon in the second row highlighted. The table has columns for Status, Name, Members, IP/Netmask, Type, Access, and Ref. It lists 10 physical interfaces (port3 to port10) and 3 SD-WAN interfaces (SD-WAN, port1, port2). Port4 and Port4_Vlan20 are highlighted with green status icons.

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (10)						
🟢	port3		0.0.0.0 0.0.0.0	Physical Interface		0
🟢	port4		0.0.0.0 0.0.0.0	Physical Interface		2
🟢	Port4_Vlan10 (Port4_Vlan10_App)		10.1.1.1 255.255.255.0	VLAN	PING HTTPS SSH SNMP	2
🟢	Port4_Vlan20 (Port4_Vlan20_IT)		10.1.2.1 255.255.255.0	VLAN	PING HTTPS SSH SNMP	2
🔴	port5		0.0.0.0 0.0.0.0	Physical Interface		0
🔴	port6		0.0.0.0 0.0.0.0	Physical Interface		0
🔴	port7		0.0.0.0 0.0.0.0	Physical Interface		0
🔴	port8		0.0.0.0 0.0.0.0	Physical Interface		0
🔴	port9		0.0.0.0 0.0.0.0	Physical Interface		0
🟢	port10		192.168.79.2 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP TELNET	0
SD-WAN Interface (3)						
🟢	SD-WAN			SD-WAN Interface		0
🟢	port1 (Airtel_Port1)		192.168.99.2 255.255.255.0	Physical Interface	PING	1
🟢	port2 (TCL_Port2)		192.168.98.2 255.255.255.0	Physical Interface	PING	1

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.

Fortigate HA configuration

Now let's 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

Fortigate HA configuration

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> FGVMEVTIWWKMM48 is selected as the master because it has the largest value of override priority.

<2022/05/22 23:42:29> FGVMEVTIWWKMM48 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:

FGVMEVTIWWKMM48(updated 2 seconds ago): in-sync

FGVMEVNIHXPO_Y59(updated 2 seconds ago): in-sync

System Usage stats:

FGVMEVTIWWKMM48(updated 2 seconds ago):

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

FGVMEVNIHXPO_Y59(updated 2 seconds ago):

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

HBDEV stats:

Fortigate HA configuration

FGVMEVTIWWKMM48(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 , FGVMEVTIWWKMM48, 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: FGVMEVTIWWKMM48, 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

Fortigate HA configuration

multicast-ttl : 600

sync-config : enable

encryption : disable

authentication : disable

hb-interval : 2

hb-lost-threshold : 20

hello-holddown : 20

gratuitous-arp : enable

arp : 5

arp-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

Fortigate HA configuration

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

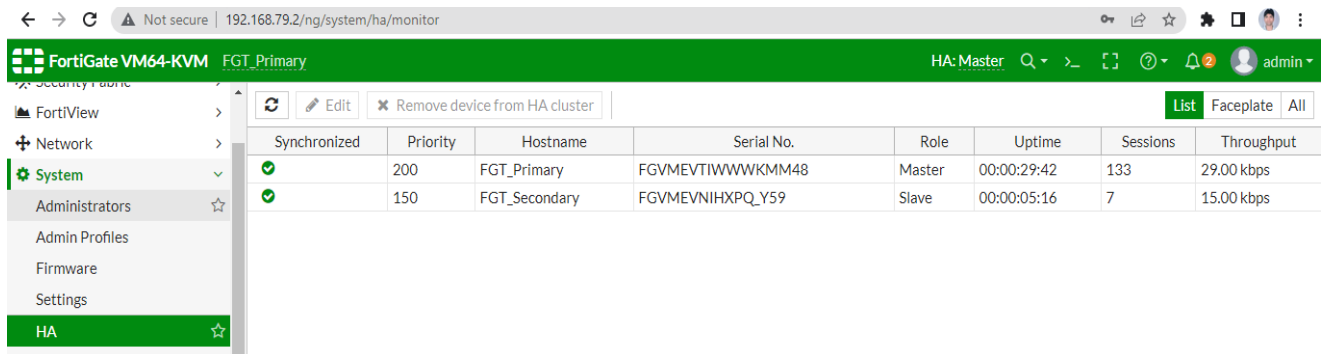
FGT_Primary #

For GUI verification - Go to system and click on HA

The screenshot shows the FortiGate VM64-KVM HA configuration page. The left sidebar contains a menu with options like FortiView, Network, System, HA, and others. The main content area displays a table of HA cluster members. The table has columns for Synchronized, Priority, Hostname, Serial No., Role, Uptime, Sessions, and Throughput. Two devices are listed: FGT_Primary (Priority 200, Master role) and FGT_Secondary (Priority 150, Slave role). The HA status is shown as 'HA: Master'.

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
1 3 5 7 9 11 13 15 17 2 4 6 8 10 12 14 16 18	200	FGT_Primary	FGVMEVTIWWKMM48	Master	00:00:29:42	133	29.00 kbps
1 3 5 7 9 11 13 15 17 2 4 6 8 10 12 14 16 18	150	FGT_Secondary	FGVMEVNIHPQ_Y59	Slave	00:00:05:16	7	15.00 kbps

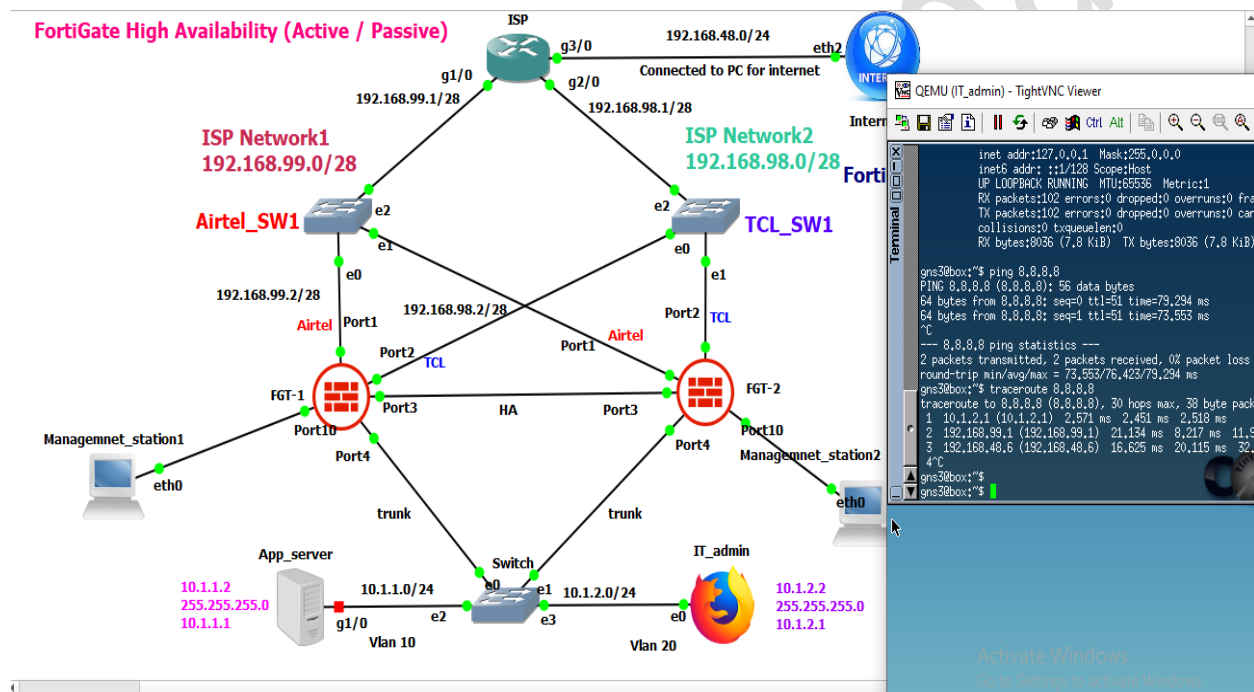
Fortigate HA configuration



FortiGate VM64-KVM FGT_Primary HA: Master

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
✓	200	FGT_Primary	FGVMEVTIWWKMM48	Master	00:00:29:42	133	29.00 kbps
✓	150	FGT_Secondary	FGVMEVNIHXPQ_Y59	Slave	00:00:05:16	7	15.00 kbps

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



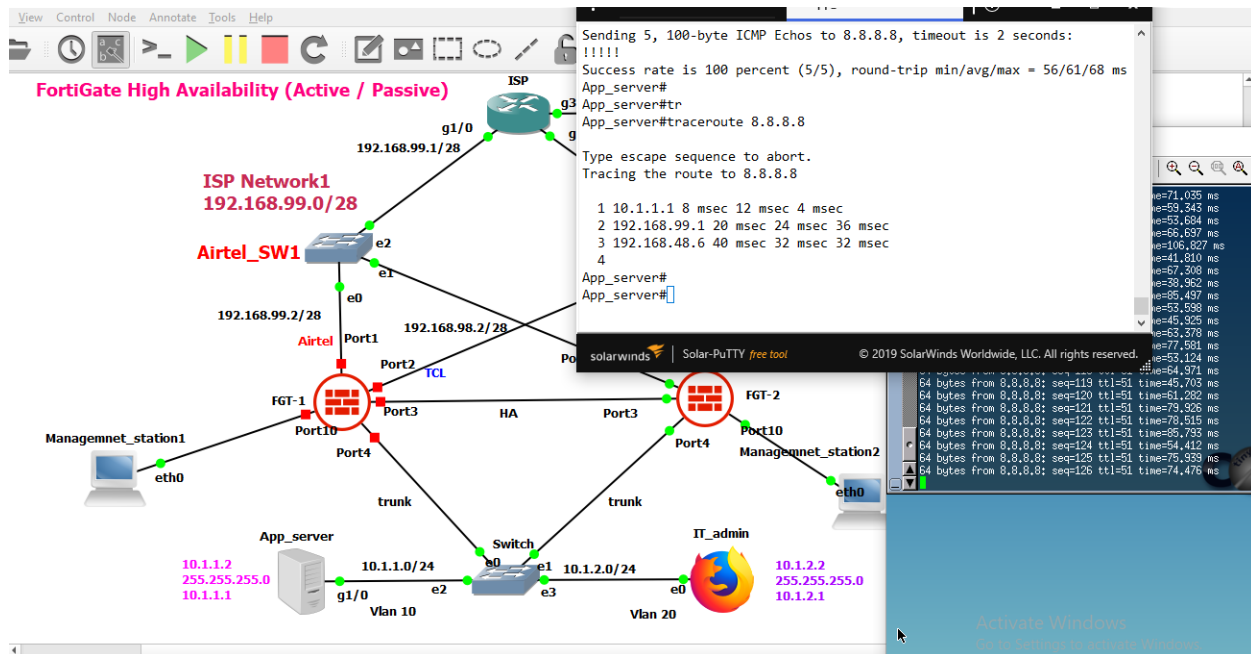
As you can see that traffic is going through primary fortigate firewall. Now I am going to down primary fortigate firewall

For HA verification you can use below command in CLI-

- #get system ha status
- #get system ha

For troubleshooting - #diagnose system ha status (Carefully)

Fortigate HA configuration



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

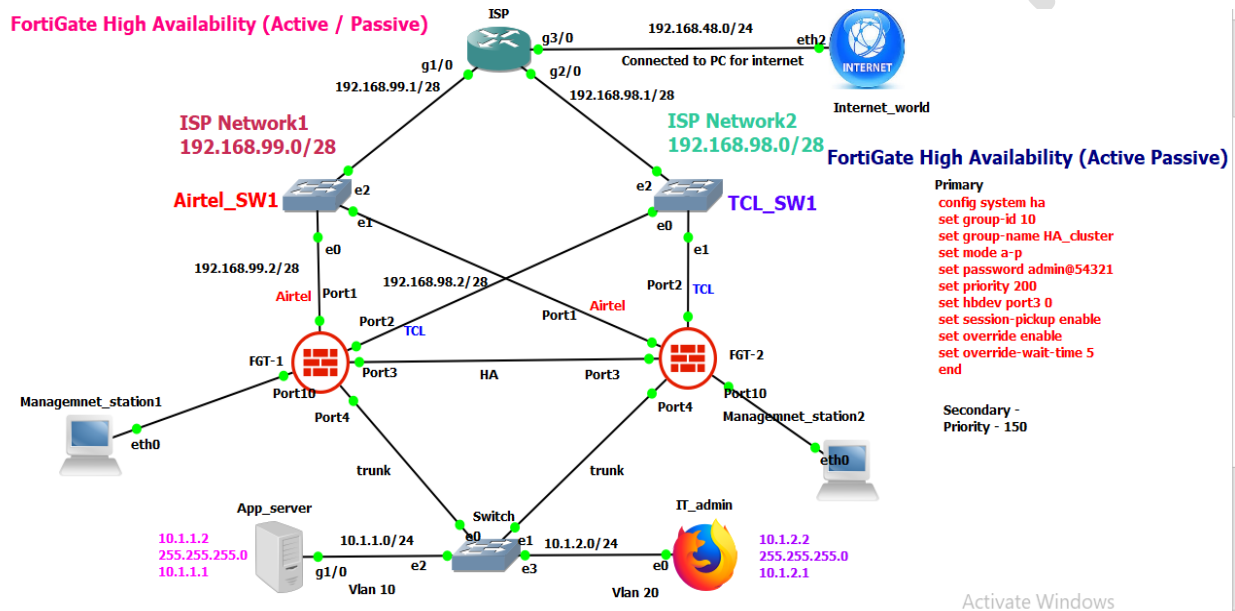
FortiGate VM64-KVM FGT_Secondary HA: Master

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
FortiGate VM64-KVM	150	FGT_Secondary	FGVMEVNIHXPQ_Y59	Master	00:00:17:58	97	104.00 kbps

Activate Windows
Go to Settings to activate Windows.

Fortigate HA configuration

Please see the below Final High availability cluster topology between two FortiGate units.



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.

I will request you all please do like, share & comment, If there are miner mistake please let me so that I can improve my tech skills.

- **Thank you.**

Umesh Prajapati

Email – umesh11238@gmail.com