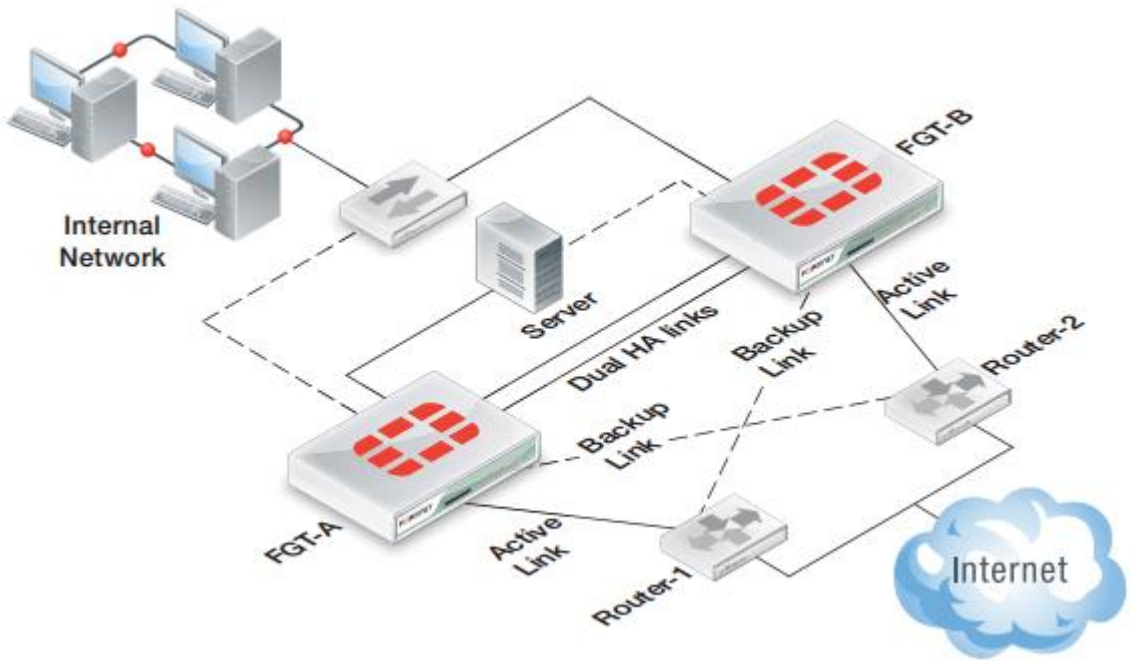
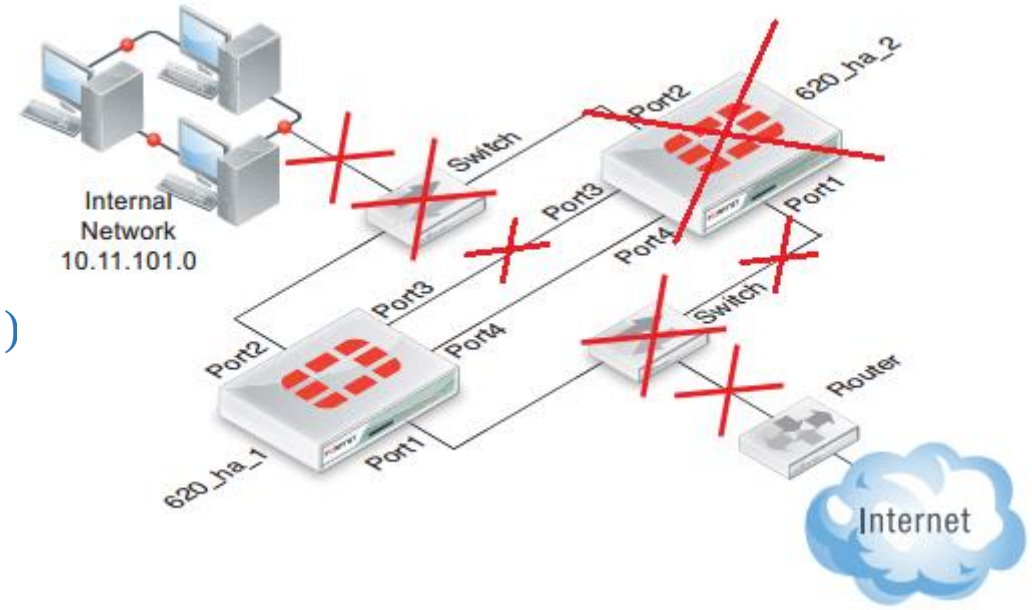
FortiGate High Availability (HA)



High Availability (HA) Requirements

- Device failover protection
- Link failover protection
- Remote link failover protection
- Session failover protection (ideally!)



First Hop Redundancy Protocols (FHRP)

- *Cisco - Hot-Standby Routing Protocol (HSRP) - 1994 - RFC 2281*
- *Cisco - Gateway Load Balancing Protocol (GLBP) - 2005*
- *Juniper - NetScreen Redundancy Protocol (NSRP)*
- *FortiGate - FortiGate Cluster Protocol (FGCP)*
- *FortiGate - FortiGate Session Life Support Protocol (FGSP)*
- *FortiGate - Fortinet Redundant UTM protocol (FRUP) (FortiGate 100D or higher)*
- *Virtual Router Redundancy Protocol (VRRP) – Open standard HSRP clone. Created by IETF in 1999*

Overview of HA

- "Two is one, one is none"
- STP is about Layer 2, First Hop Redundancy Protocols (FHRP) is about Layer 3
- Historically, one HA device is Active and the other(s) is/are Standby
- Some sort of 'Hello' protocol is used to see if the Active gateway is up.

Overview of HA

- *Question:* How do you get clients to choose a default gateway when the default fails?

  Answer: Assign the same gateway IP address to both devices

- *Question:* What about ARP caches? ARP caches last for 2-10 minutes on Windows boxes.

  Answer: Duplicate the Virtual MAC addresses (FGCP, HSRP, VRRP)

- Client never has to do anything, it is just a different device that answers the gateway IP address

Fun Fact!

The MAC address of the gateway device can tell you what redundant protocol is being used:

Protocol	MAC Address	Notes
VRRP	0000.5E00.01xx	where: xx=VRRP Group
HSRPv1	0000.0C07.ACxx	where: xx=HSRP Group
HSRPv2	0000.0C9F.Fxxx	where: xxx=HSRP Group
HSRP IPv6	0005.73A0.0xxx	where: xxx=000-FFF
GLBP	0007.B400.xxyy	where: xx=GLBP Group yy=AVF Number
NSRP	0010.DBFF.xxyy	where: xx=Cluster ID yy=VSD Group
FGCP	0009.0F09.xxyz	where: xx=Group ID y=VCluster Integer z=Index #

M'kay

FortiGate Cluster Protocol (FGCP)

- Device Failover Protection
- Link Failover Protection
- Remote Link Failover Protection
- Active-Active HA Load Balancing

FortiGate HA Cluster Management

- Automatic continuous configuration synchronization
- Synchronized Firmware upgrades/downgrades
- Individual cluster unit management
- Remove and add cluster units as needed
- Logging and reporting from each unit for each unit

FortiGate HA Cluster Characteristics

- FortiGates operate as an HA cluster of 2-4 units
- Cluster contains one Primary/Master unit and one or more Subordinate/slave/backup units
- Cluster can operate in Active-Passive (AP) or Active-Active (AA) mode
- All cluster units must also have the same hardware configuration
- All cluster units must be running in the same Operating mode (NAT/Route mode or Transparent mode)
- On startup, FGCP looks for other FortiGate units and negotiates to create a cluster

FGCP Cluster Heartbeat Overview

- Cluster units communicate with each other through heartbeat interfaces
- FGCP shares communication and synchronization over the heartbeat interface link
- Hello packets are sent at regular intervals by the heartbeat interface of each cluster unit
- Hello packets describe the state of the cluster unit and keep all units synchronized

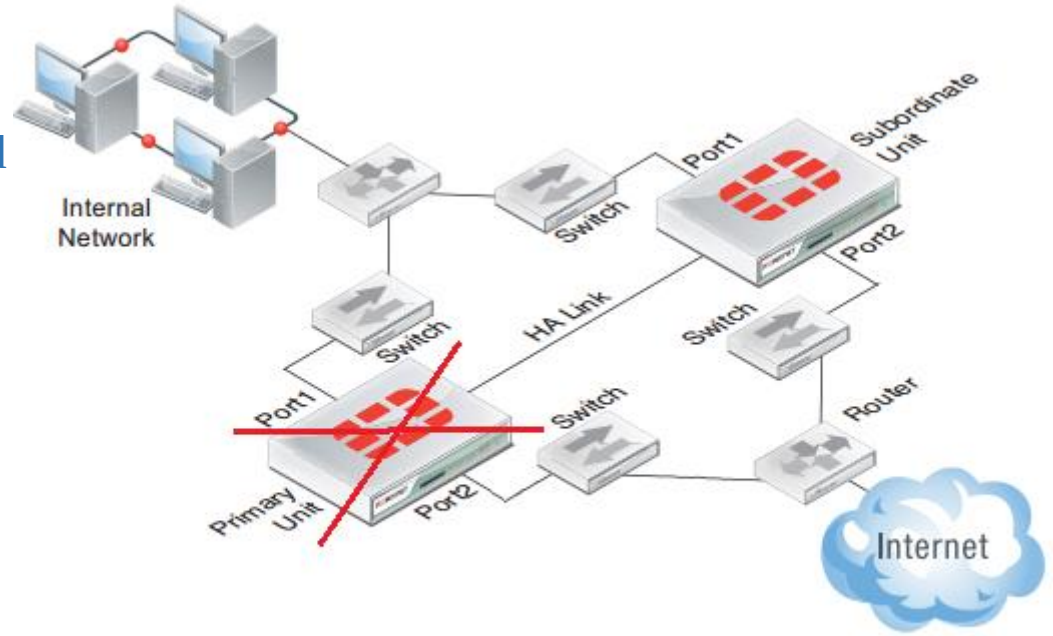
FGCP Cluster Heartbeat Details

- Cannot use a cluster unit *switch* port for the HA heartbeat traffic, have to use an *interface* port
- FGCP uses link-local IP4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses
- At least one heartbeat interface on each unit must be connected for the cluster to operate
- If heartbeat communication fails, all cluster members will think they are the Primary unit resulting in multiple devices on the network with the same IP addresses and MAC addresses, a condition referred to as Split Brain

Innocent and carefree, Stuart's left hand didn't know what the right was doing.

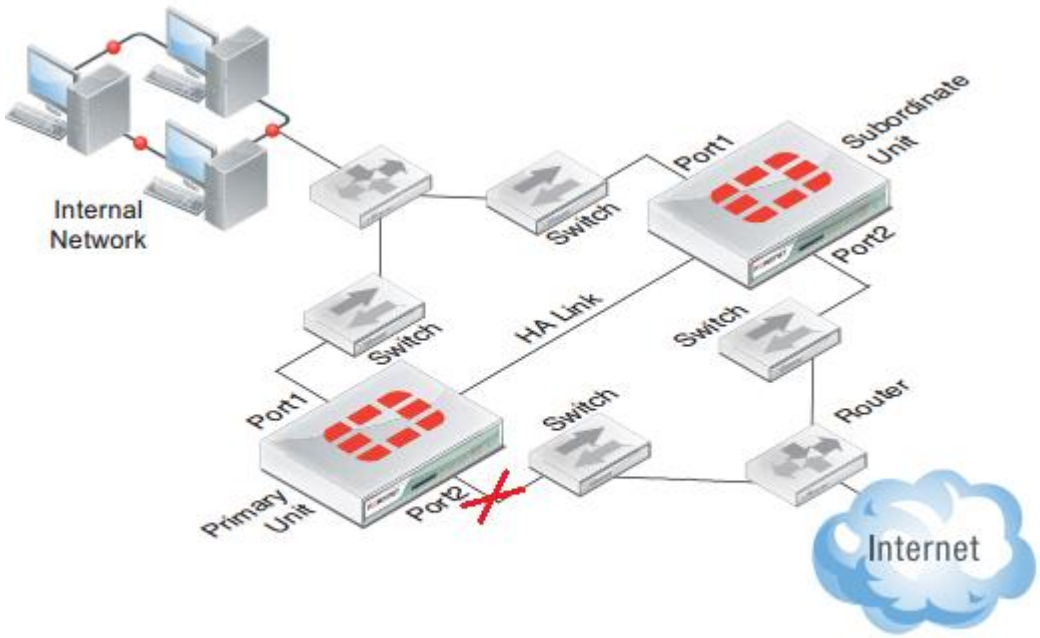
Device Failover Protection

- If the Primary unit fails to respond to HA heartbeat packets the Subordinate units assume the Primary unit has failed and negotiate to select a new Primary unit
- FGCP causes the interfaces on the new Primary unit interfaces to acquire the same virtual MAC addresses as the failed Primary unit
- FGCP then sends gratuitous ARP packets from the (new) Primary unit interfaces to reprogram the network



Link Failover (Port/Interface Monitoring)

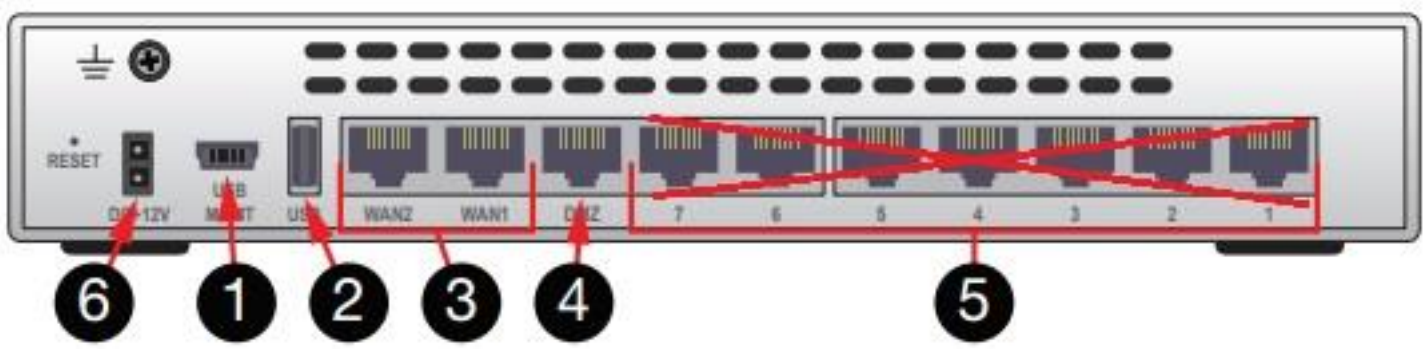
- If a monitored interface fails, the cluster reorganizes to reestablish a link to the network
- You manually configure monitored interfaces
- The interfaces that you can monitor appear on the port monitor list
- Port monitor configuration changes are synchronized to all cluster units



Link Failover (Port/Interface Monitoring)

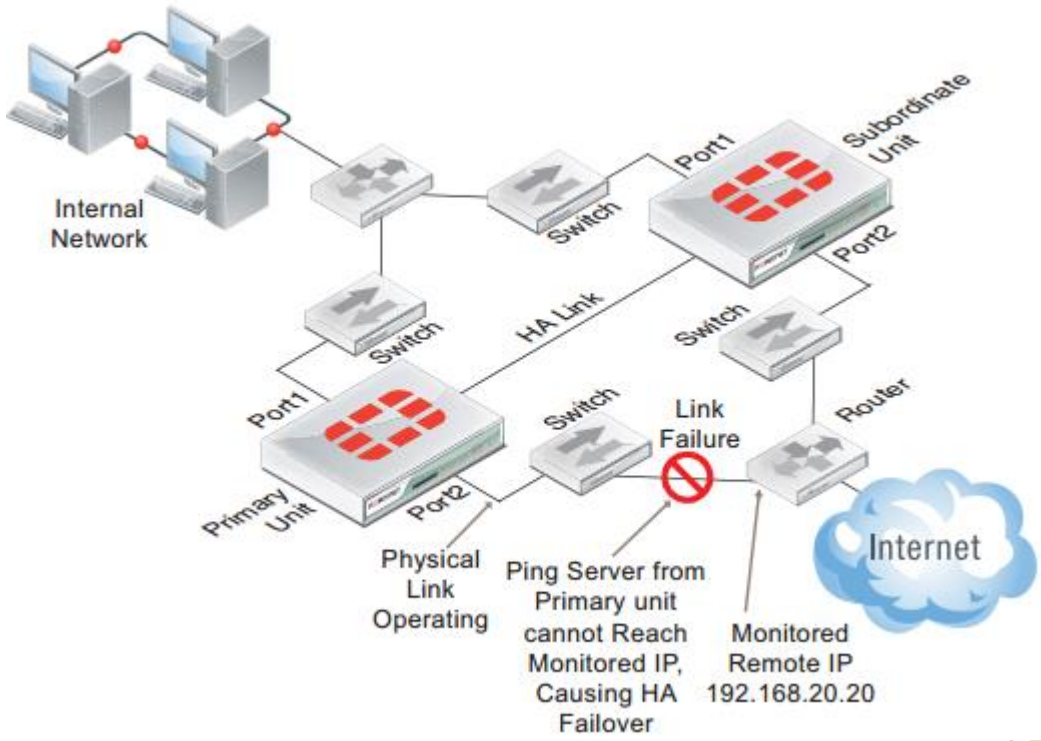
You can monitor all FortiGate interfaces including redundant interfaces and 802.3ad aggregate interfaces... except:

- FortiGate ports that are configured as part of an internal *switch*
- VLAN subinterfaces.
- IPsec VPN interfaces.
- Individual physical interfaces that have been added to a redundant or 802.3ad aggregate interface

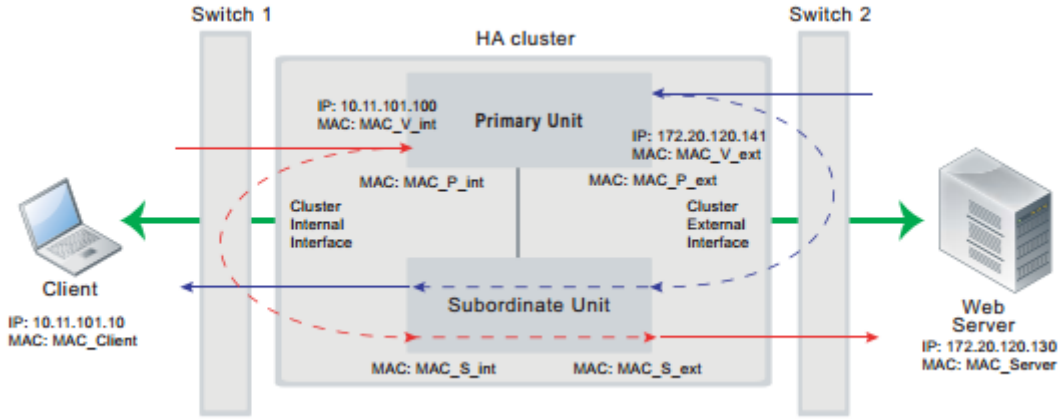


Remote Link Failover (Remote IP Monitoring)

- Remote IP Monitoring uses ping servers to test connectivity with IP addresses of network devices.
- Remote IP Monitoring causes a failover if one or more of these remote IP addresses does not respond to a ping server.
- You can enable HA Remote IP Monitoring on multiple interfaces



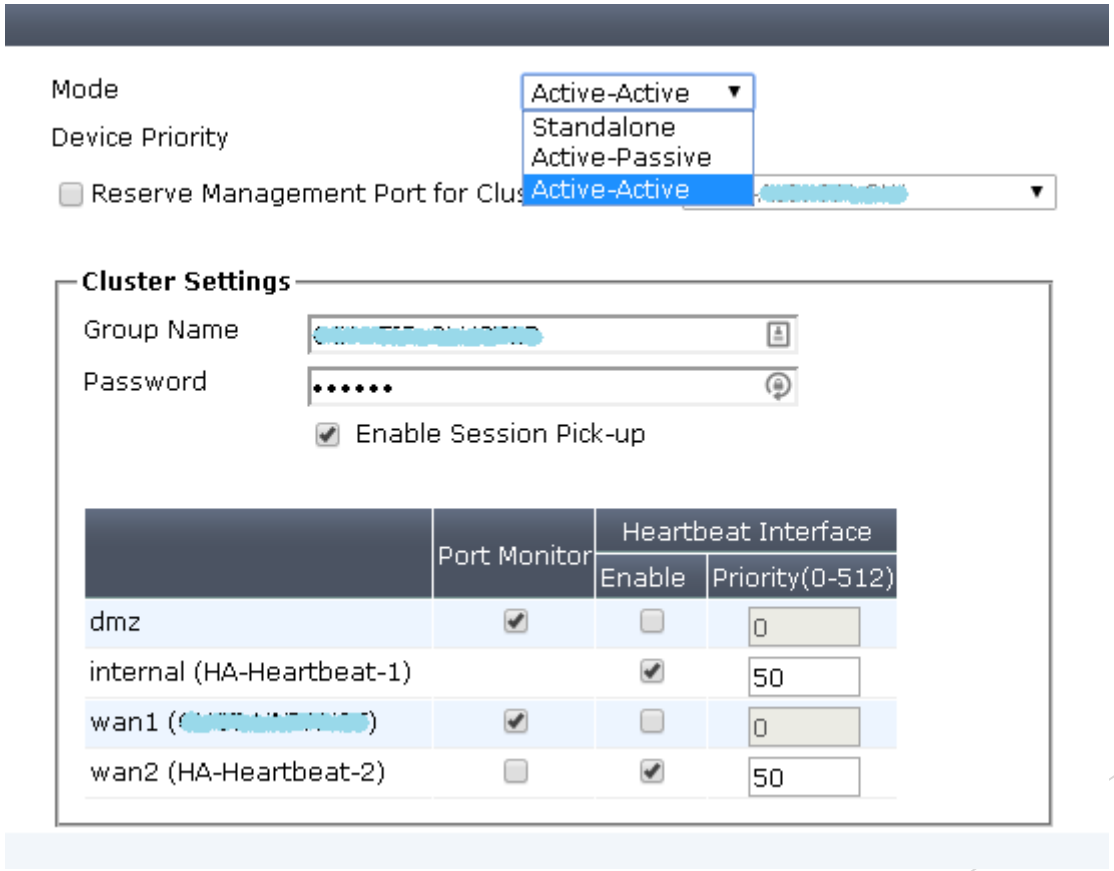
Session Failover Protection



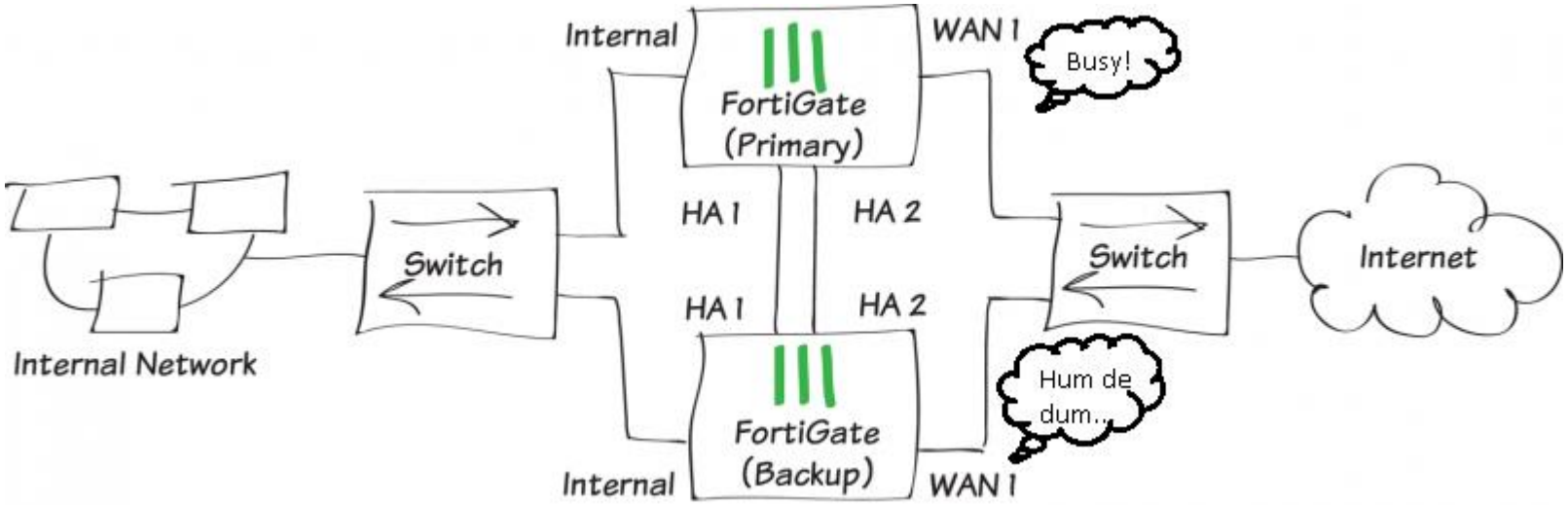
- FGCP session failover maintains TCP, SIP and *IPsec VPN* sessions after a failure
- FGCP session failover can also be configured to maintain UDP and ICMP sessions
- Session failover does ***not*** failover multicast, or *SSL VPN* sessions
- Session failover adds extra overhead to cluster operations and can be disabled to improve cluster performance if it is not required.

Active-Passive and Active-Active HA

- Choose Active-Passive or Active-Active HA mode
- All cluster units must be set to the same mode
- You can change the mode after the cluster is up and running

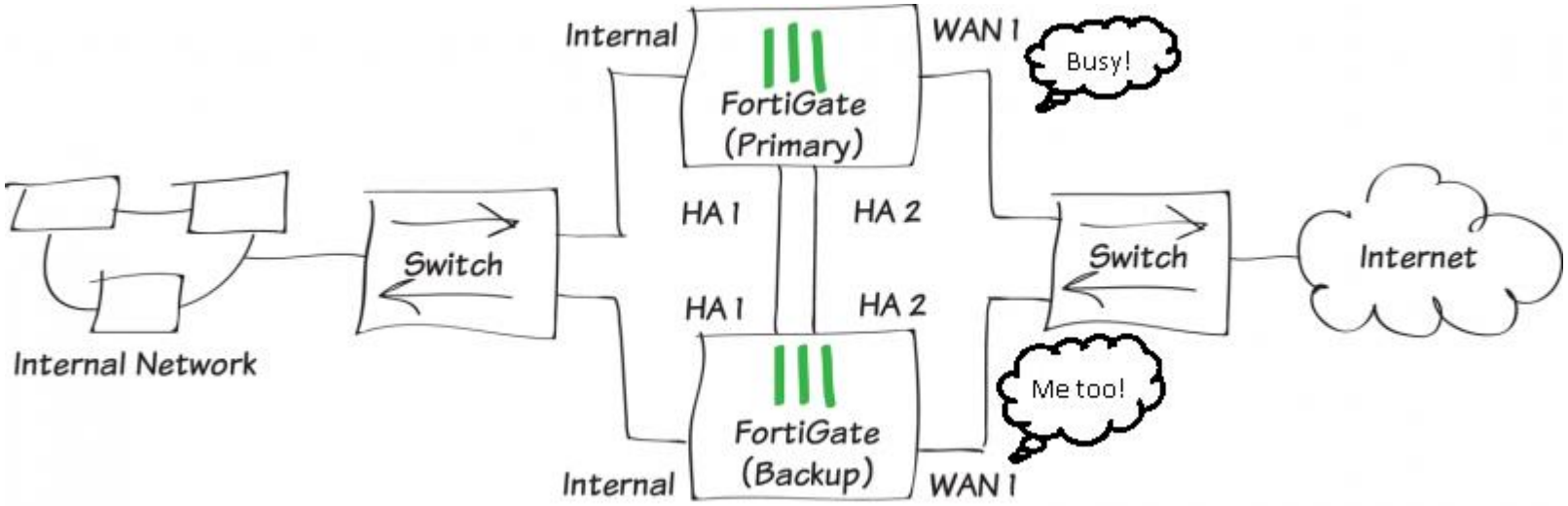


Active-Passive HA (Failover Protection)



- Active-Passive (A-P) cluster has a Primary unit and one or more Subordinate units.
- A-P Subordinate units run in a standby state and do not process communication sessions
- A-P HA provides transparent device and link failover
- A-P can also enable TCP, SIP and *IPsec VPN* session failover (aka 'session pickup')

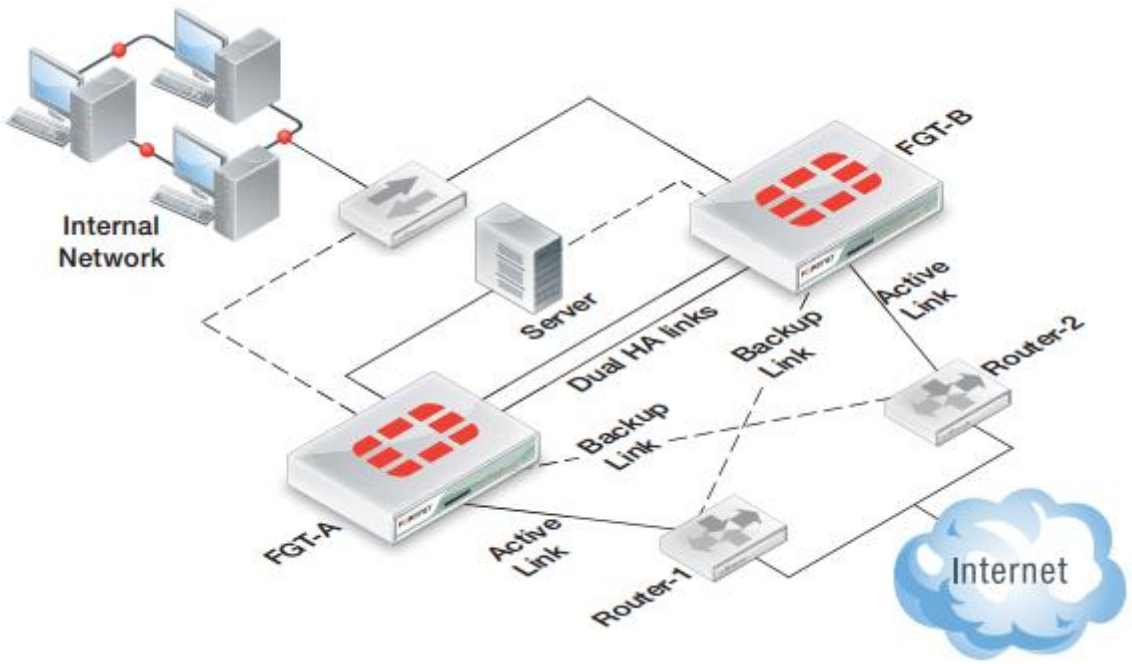
Active-Active HA (load balance and failover)



- Active-Active (A-A) cluster has a Primary unit and one or more Subordinate units
- A-A Primary unit receives all communication sessions and load balances those that require content inspection across Subordinate units
- Content inspection processing applies protocol recognition, virus scanning, IPS, web filtering, email filtering, data leak prevention (DLP), application control, and VoIP content scanning and protection to sessions accepted by security policies.

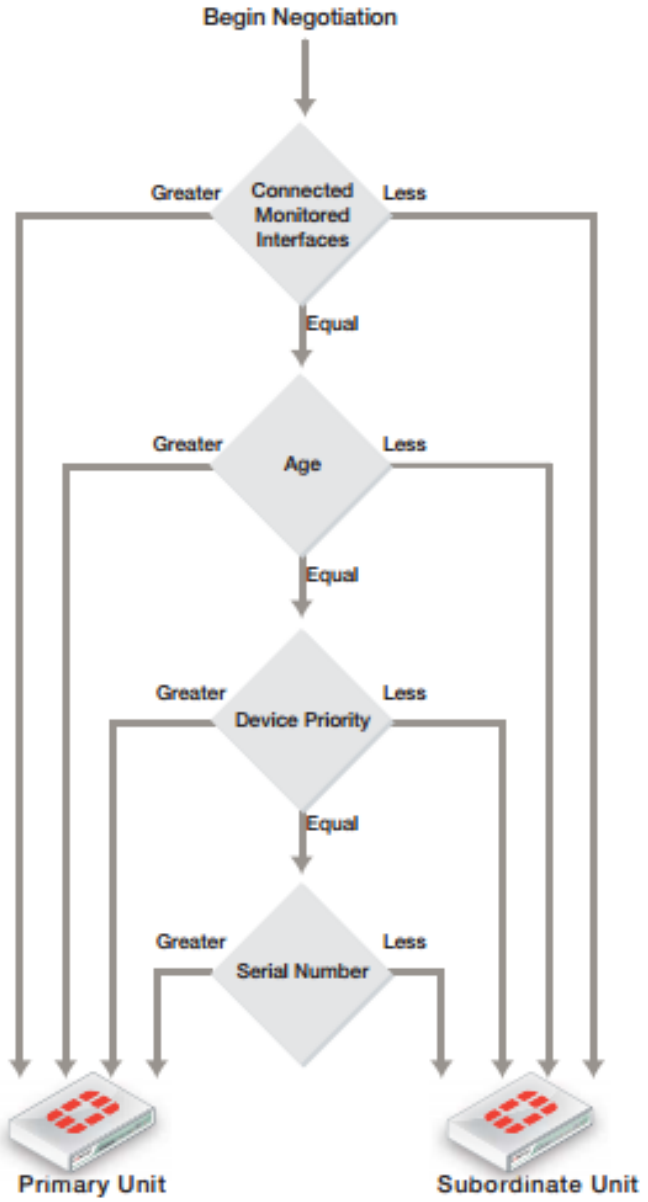
End

FortiGate High Availability (HA) Extended Edition



Primary Unit Selection

- Left alone, FGCP will choose a Primary unit based on the following factors in the following order:
  - 1st - Greater Number of Connected and Monitored Interfaces
  - 2nd - Greater Age(Stability)
  - 3rd - Greater Priority (Default=128, you can change this)
  - 4th - Greater Serial Number
- If all factors are left at default, or are equal, the unit with the highest serial number (the newest) becomes the Primary



1st - Primary Unit Selection and Monitored Interfaces

- The cluster unit with the highest number of connected monitored interfaces becomes the Primary unit
- A cluster always renegotiates when a Primary unit monitored interface fails, or is disconnected (link failover), *and* when it is restored
- If a Subordinate unit monitored interface fails or is disconnected, the cluster also renegotiates but will not necessarily select a new Primary unit
- Each time a monitored interface is disconnected or fails, the cluster renegotiates

2nd - Primary Unit Selection and Age

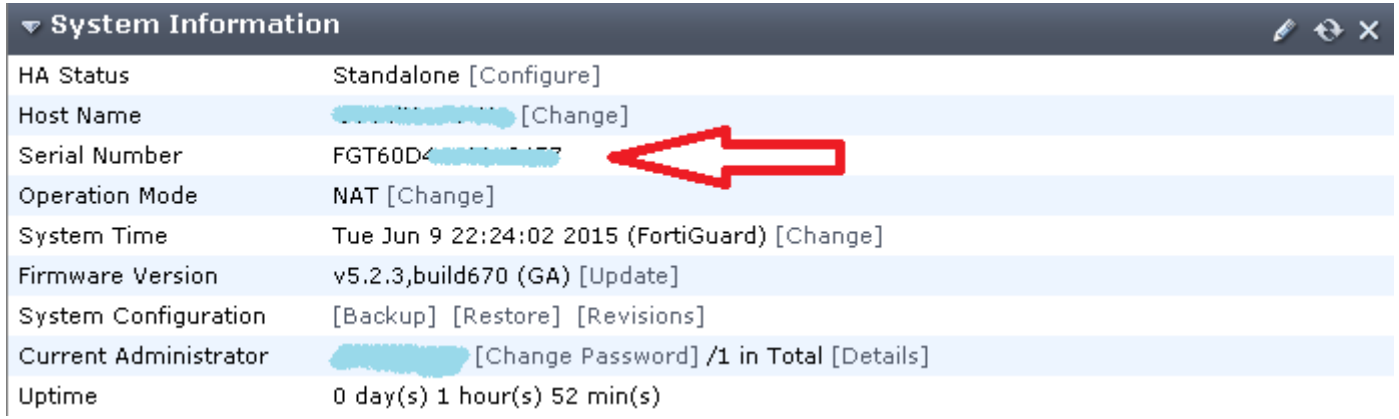
- The unit with the highest age value becomes the Primary unit
- The age of a cluster unit is the amount of time since a monitored interface failed or is disconnected
- Age does not affect Primary unit selection when all cluster units start up at the same time
- If a link failure of a monitored interface occurs, the age value for the unit is reset. Age is also reset when a cluster unit starts (boots up). That's why I call this the "Age before boot-ey" rule.

3rd - Primary Unit Selection and Device Priority

- A cluster unit with the highest device priority becomes the Primary unit when the cluster starts up or renegotiates
- You can change the device priority to control which FortiGate unit becomes the Primary unit
- Default device priority is 128. Range is 0-255.
- Can change Device Priority through GUI or CLI

4th – The Greater Serial Number Wins

- If all factors are left at default, or are equal, the unit with the highest serial number (the newest) becomes the Primary.
- Why? The highest serial number will have the most recent hardware and perform better.
- Opposite of the switching world!



HA Override

- HA Override is configured by setting the Device Priority (default=128, range=0-255)
- Primary unit selection considers device priority before age and serial number.
- If interface monitoring is enabled, unit with the most connected monitored interfaces still becomes Primary

HA Override

- Primary Unit Selection **without** HA Override:
  - 1st - Greater Number of Connected and Monitored Interfaces
  - 2nd - Greater Age (Stability)
  - 3rd - Greater Priority (Default=128, you can change this)
  - 4th - Greater Serial Number
- Primary Unit Selection **with** HA Override:
  - 1st - Greater Number of Connected and Monitored Interfaces
  - 2nd - Greater Priority (Default=128, you can change this)
  - 3rd - Greater Age (Stability)
  - 4th - Greater Serial Number

Why I Don't Like HA Override

- Configuration changes can be lost if override is enabled
- Changes and configuration **always** flow from Primary to Subordinate and Override occurs before syncronization
- So, if Primary (with highest priority) goes down, you make configuration changes, then Primary comes up and takes over again your changes are lost

FortiGate HA compatibility with PPPoE

- Not compatible with PPP protocols such as PPPoE.
- You cannot switch to operate in HA mode if one or more interfaces is configured by DHCP or PPPoE.
- You cannot switch to operate in HA mode if one or more interfaces is configured as a PPTP or L2TP client.

FortiGate HA compatibility with DHCP

- Not compatible with DHCP client on any interface
- You cannot switch to operate in HA mode if one or more interfaces is configured by DHCP or PPPoE
- You *can* configure a cluster to act as a DHCP server or a DHCP relay agent
- Primary unit responds to all DHCP requests (including relay) and maintains the DHCP server address lease database
- DHCP server address lease database is synced to the Subordinate units

FGCP HA Best Practices

- Use Active-Active HA to distribute TCP and UTM sessions among multiple cluster units.
- Use a different host name on each FortiGate unit
- Add an Alias to the interfaces used for the HA heartbeat
- Isolate heartbeat interfaces on a separate VLAN, or connect the heartbeat interfaces directly using a crossover cable
- Configure and connect redundant heartbeat interfaces
- Do not monitor dedicated heartbeat interfaces

More Information

- More Information, 295 pages worth, can be found at:

  http://docs.fortinet.com/uploaded/files/1088/fortigate-ha-50.pdf