
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT
Barracuda CloudGen Firewall
High availability under the hood

Why Do We Need High Availability?

What Is Better than a Superhero?

A Superhero with a Sidekick!

Three Principles

- Eliminating single points of failure
  - Adding redundancy to the system so failure of a component does not lead to failure of the entire system.
- Reliable crossover
  - In redundant systems, the crossover point itself tends to become a single point of failure. Reliable systems must provide for reliable crossover.
- Detecting failures as they occur
  - If the two principles above are observed, a user may never see a failure – but the maintenance activity must.

Implementation

- IP addresses can be “moved” between primary and secondary firewall
  - Based on the state of the firewall
- Layer 2 and Layer 3 monitoring
  - Decision-based failover
- Additional private uplinks
  - Only real limitation RTT <80ms
- Active monitoring of all involved components
  - Involves more than just reachability of the other side

Implementation

- Multiple servers with…
  - …multiple services
  - …different set of IPs
  - …different L2/L3 monitoring options
- Some services cannot run multiple times on the same firewall
- Services must reside on the same server to interact
  - This got even worse with the introduction of Application Control

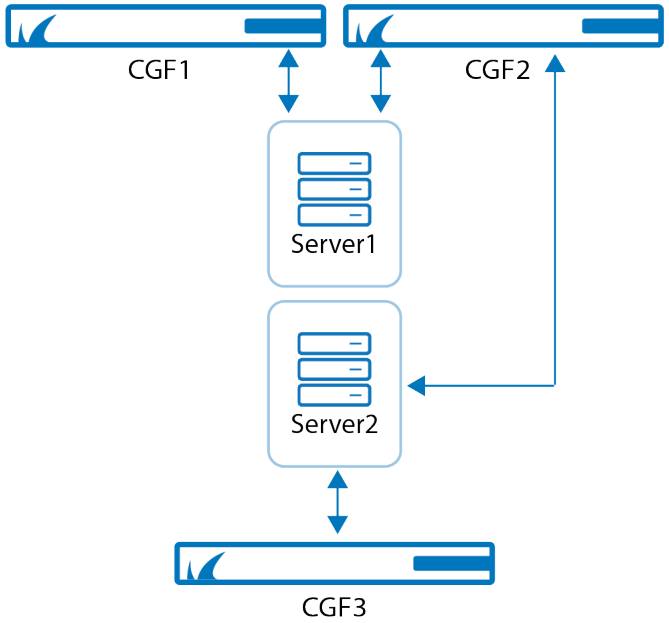

Live Demo

What Has Changed with 8.0?


Live Demo

Virtual Server - Pros

- The base concept for managing HA
  - Two different concepts (single vs managed box)
- Contains information for both partners
  - IP address, monitoring settings, probing information
- Very flexible
  - Multiple servers on one box
  - Move servers from one box to another
  - Lets you create complex HA scenarios

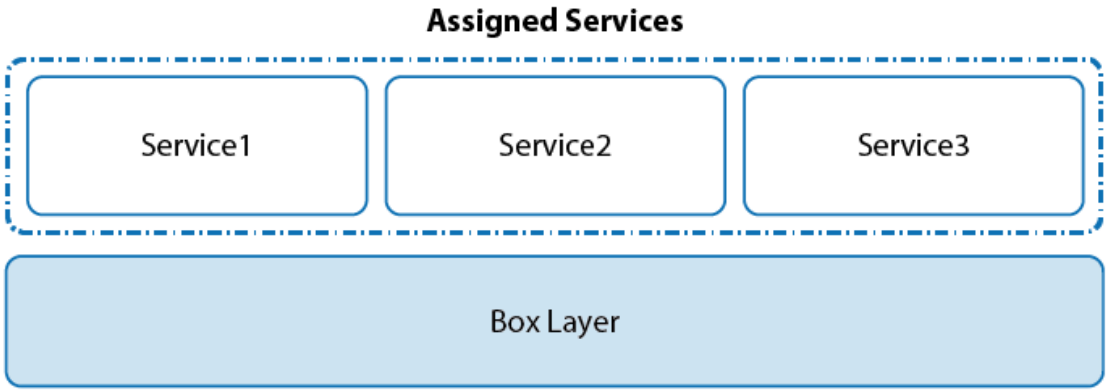


Virtual Server - Cons

- Configuration spread on different nodes
- Complex HA scenarios not used at all
- “Free floating” servers impose various drawbacks
- Previous solutions did not remove complexity
  - Simple configuration mode
  - Linking product type to virtual server

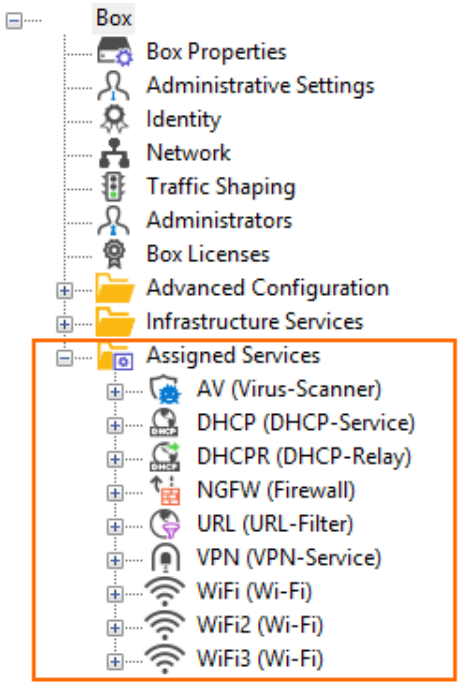
Assigned Services

- Box layer
  - Runs infrastructure services and responsible for logging, event, configuration, and control
- Assigned service
  - Selected services can be activated by user if required.



Assigned Services Changes Everything

- Server IPs moved to Network node
- HA Box Properties and Network node now merged
- Monitoring Policies moved to Control node
- CC-managed firewalls box layer is no longer separated
- Migrating stand-alone HA to CC-managed now simplified



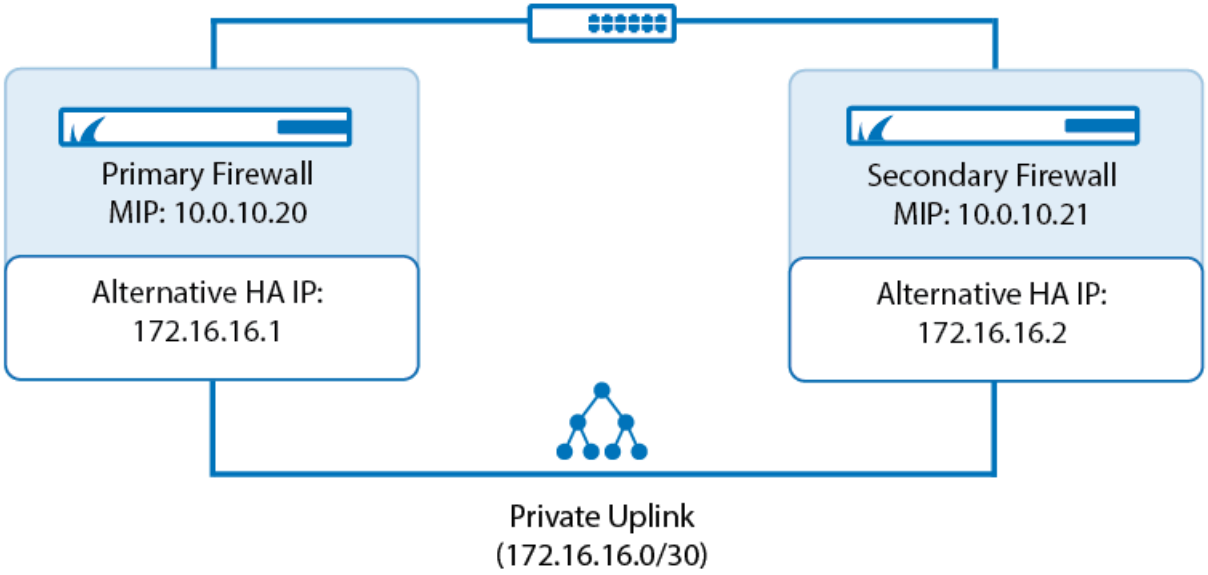

Live Demo

Under the Hood

JAYSBRICKBLOG.COM

Private Uplink

A safeguard against failure of the switch connecting the HA units



Virtual Server Monitoring

- Layer 3 monitoring policy
  - The IP addresses must be reachable for the virtual server to stay up
  - ICMP check on all IP addresses in 10-second intervals
  - If no answer is received, the IP addresses are probed every second for a 10-second period.
  - ARP responses are also monitored
- Layer 2 monitoring policy
  - Defines the interface monitoring
  - Link status of each interface is checked on a regular basis

Virtual Server Monitoring

- Extends the monitoring policy to both units
- Shared HA probing combines the IP address and interface information of both units
- Only local health check target resources are probed
  - Every HA partner performs its own monitoring procedure

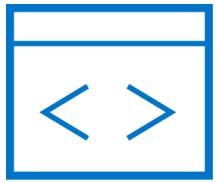
Gratuitous ARPs

- Can help detect IP conflicts
  - When a machine receives an ARP request containing a source IP that matches its own, it knows there is an IP conflict.
- Assist in updating other machines' ARP tables
  - Clustering solutions utilize this when they move an IP from one NIC to another, or from one machine to another.
- Inform switches of the MAC address of the machine on a given switch port

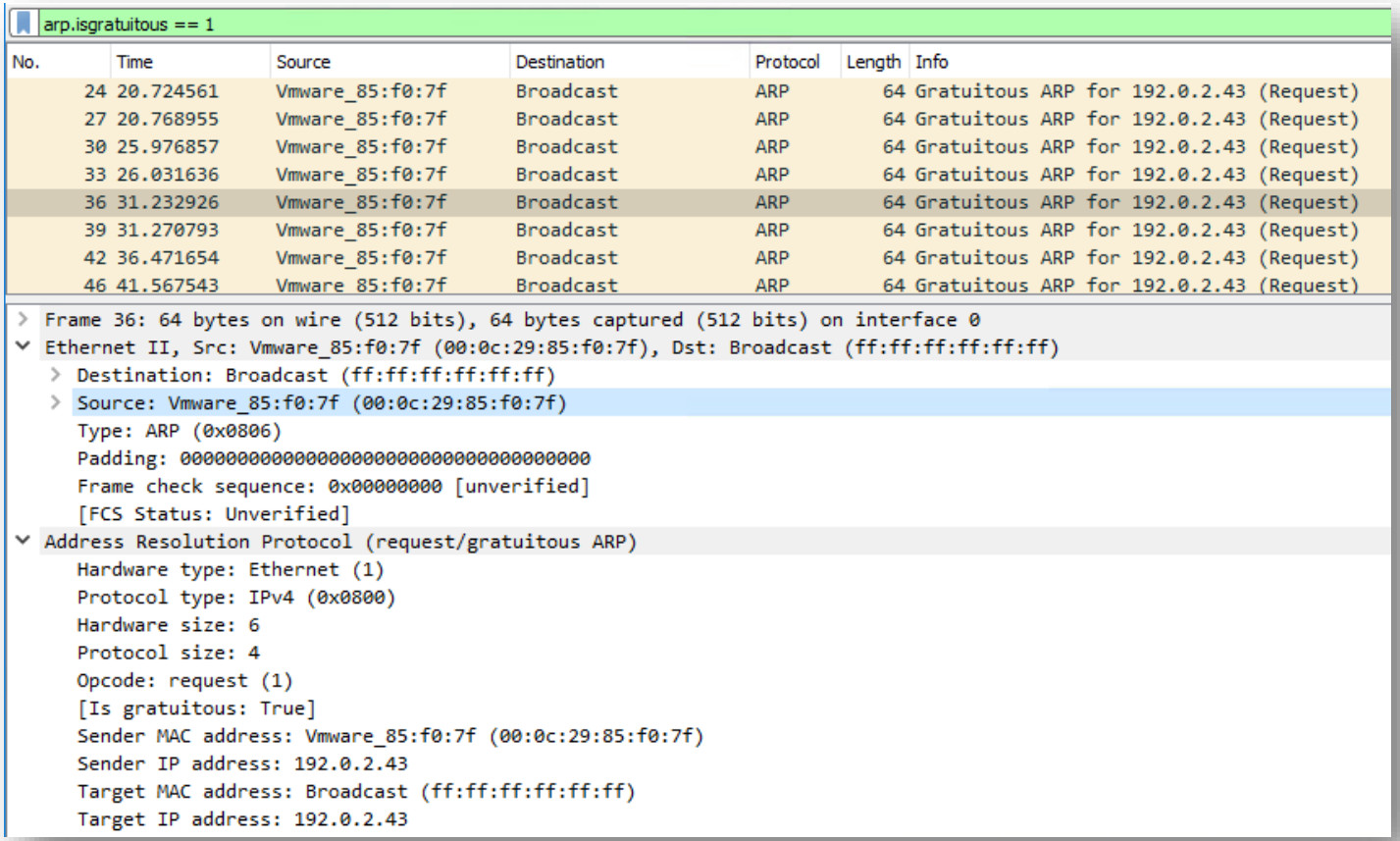
Gratuitous ARP

Every time an IP interface or link goes up, the driver for that interface typically sends a gratuitous ARP to preload the ARP tables of all other local hosts.

- If you frequently see multiple gratuitous ARPs from the same host, it can be an indication of bad Ethernet hardware/cabling resulting in frequent link bounces.

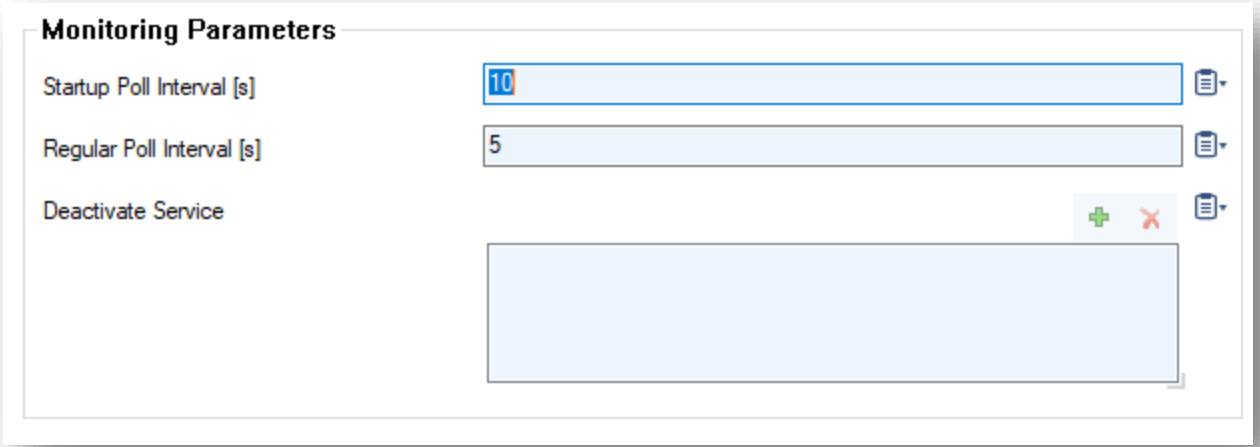


Gratuitous ARP

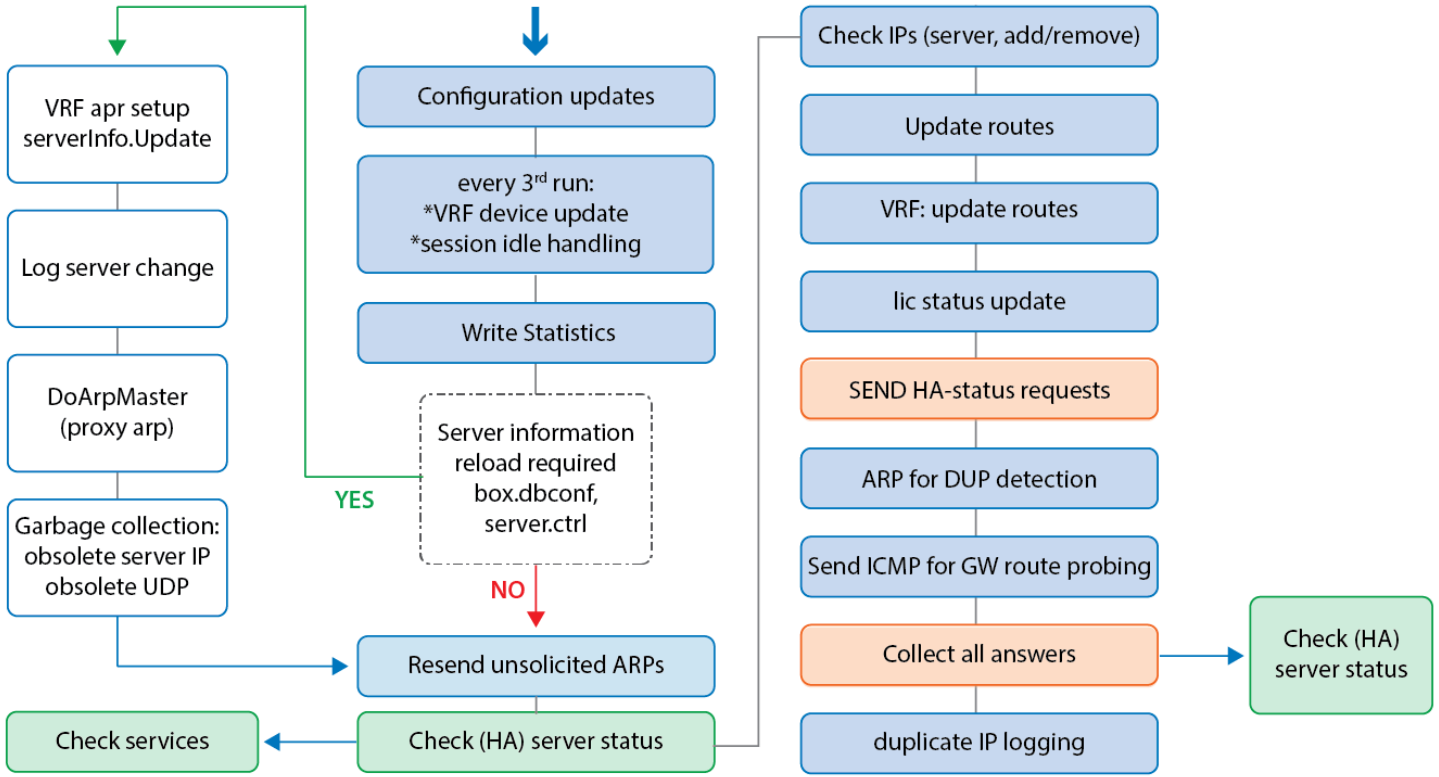


Dive Deeper

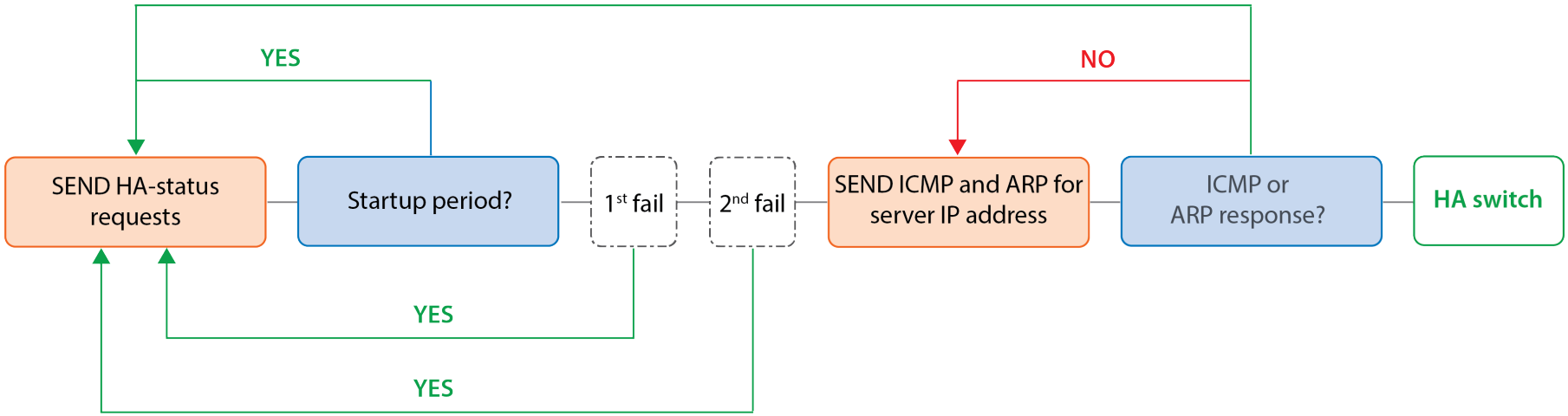
Poll Interval



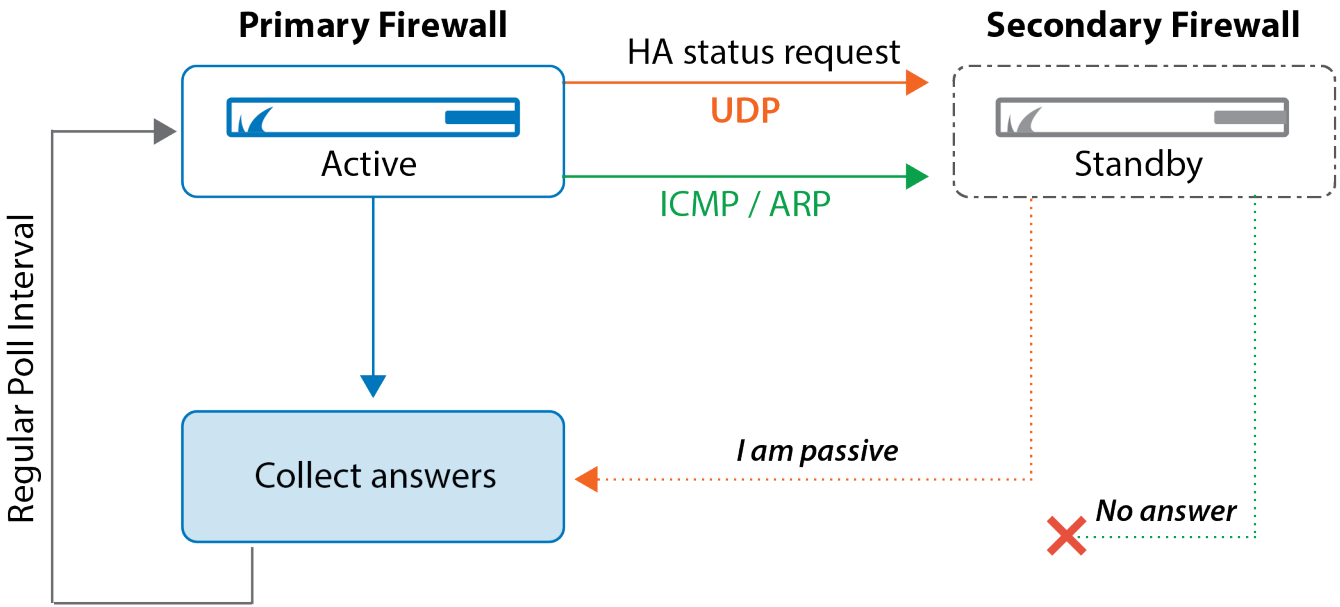
Regular Poll Workflow



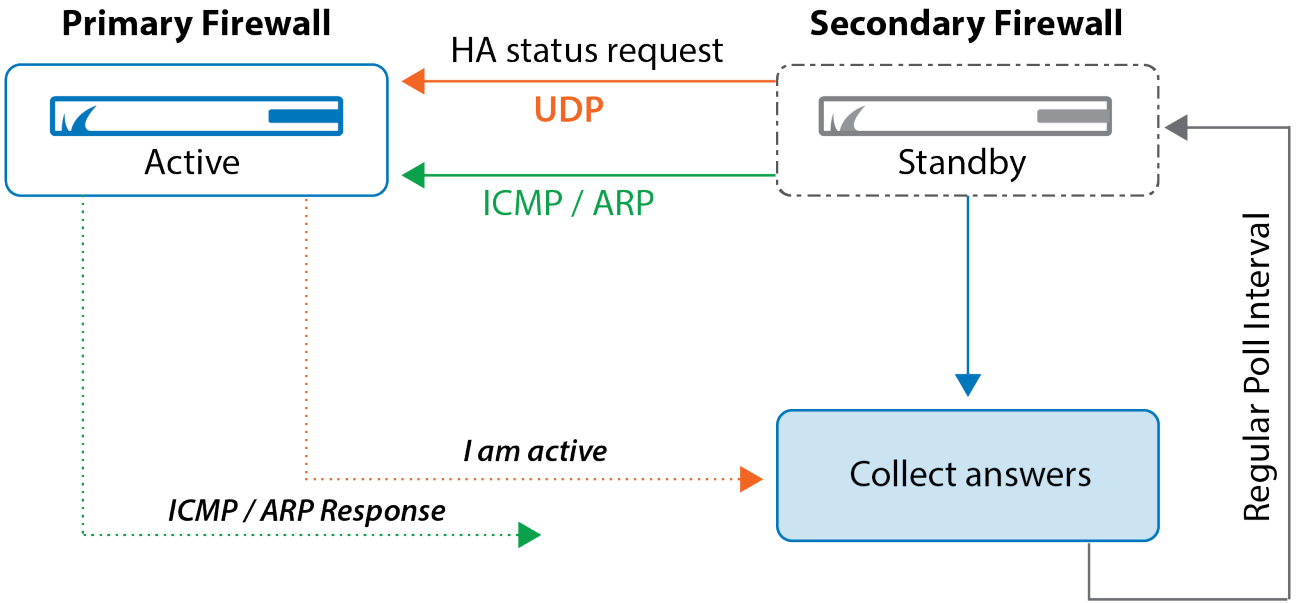
High Availability Decision Flow



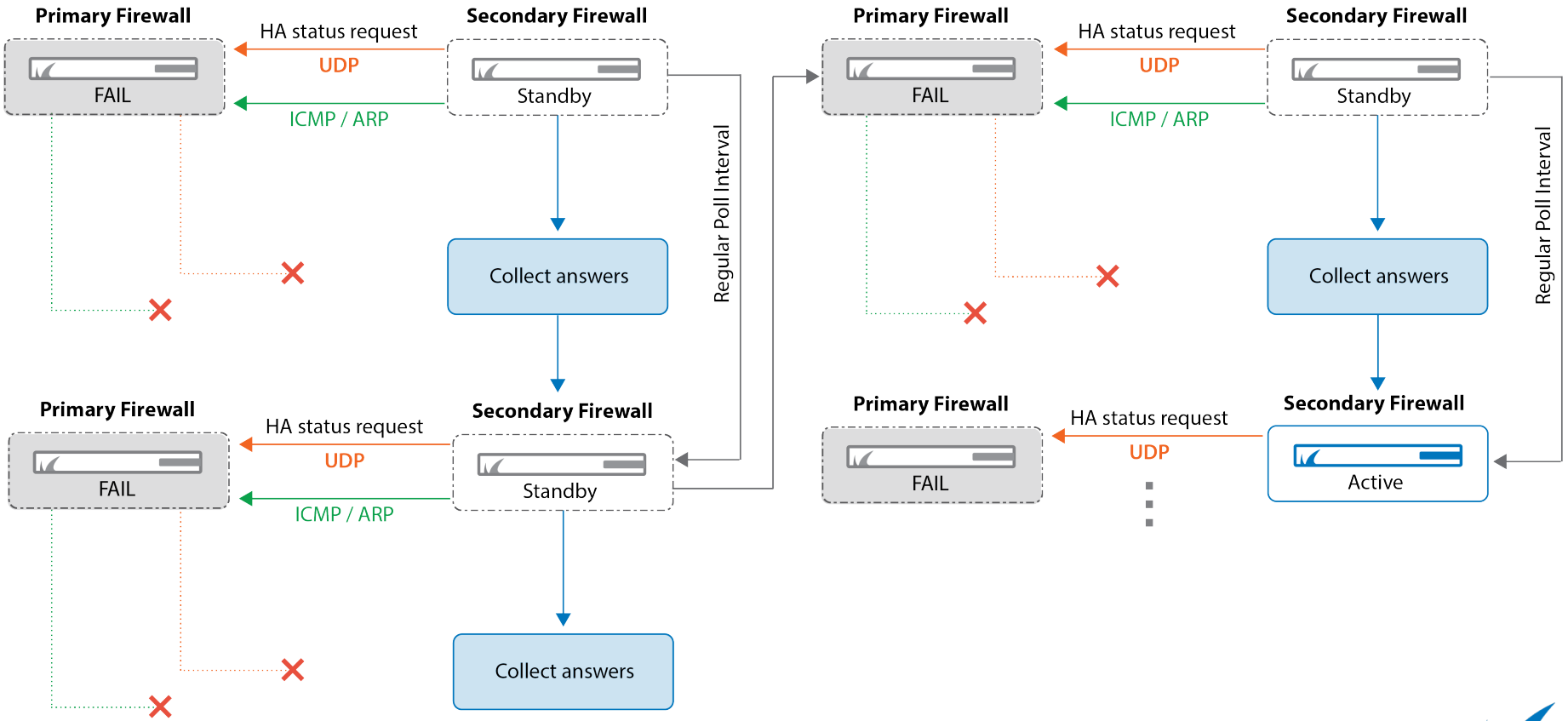
Normal Behavior – Active Site



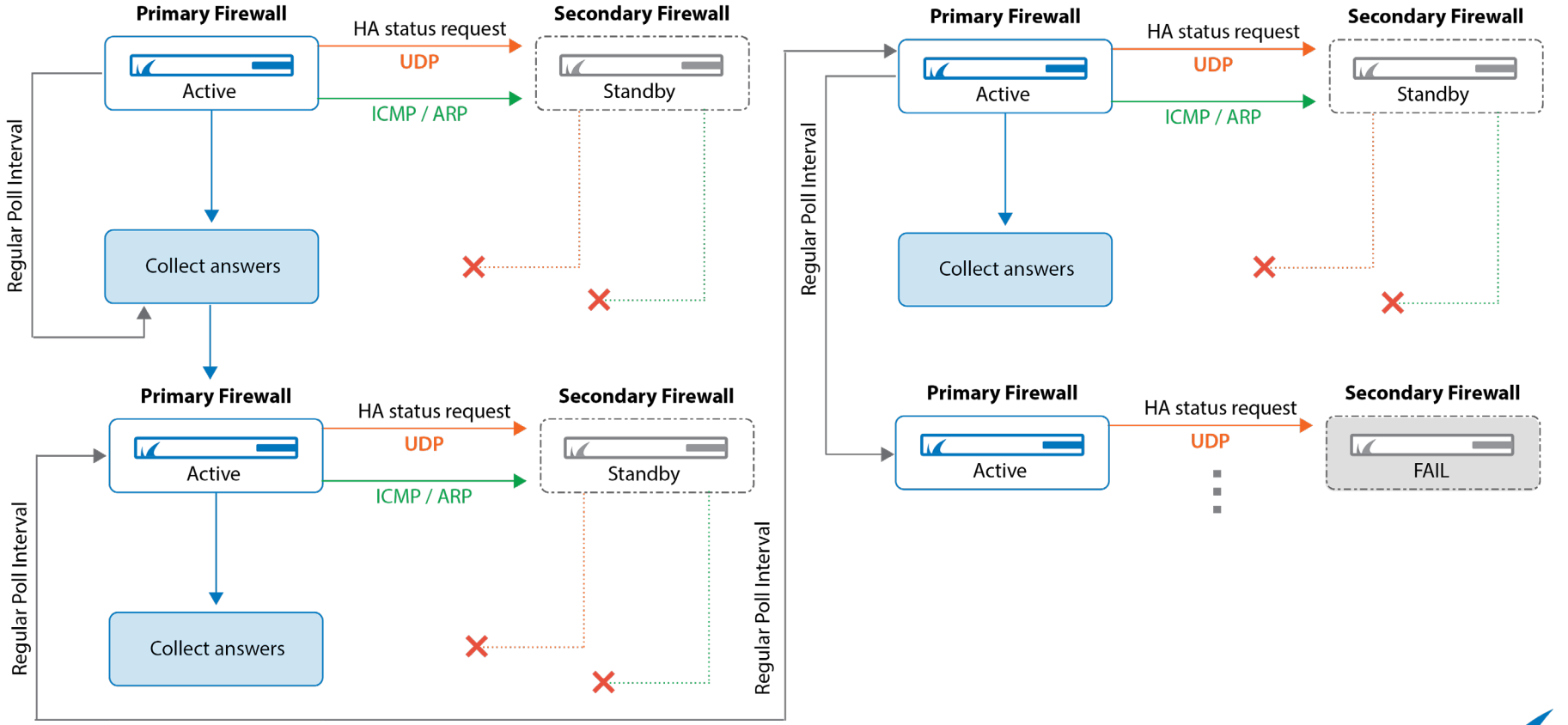
Normal Behavior – Passive Site



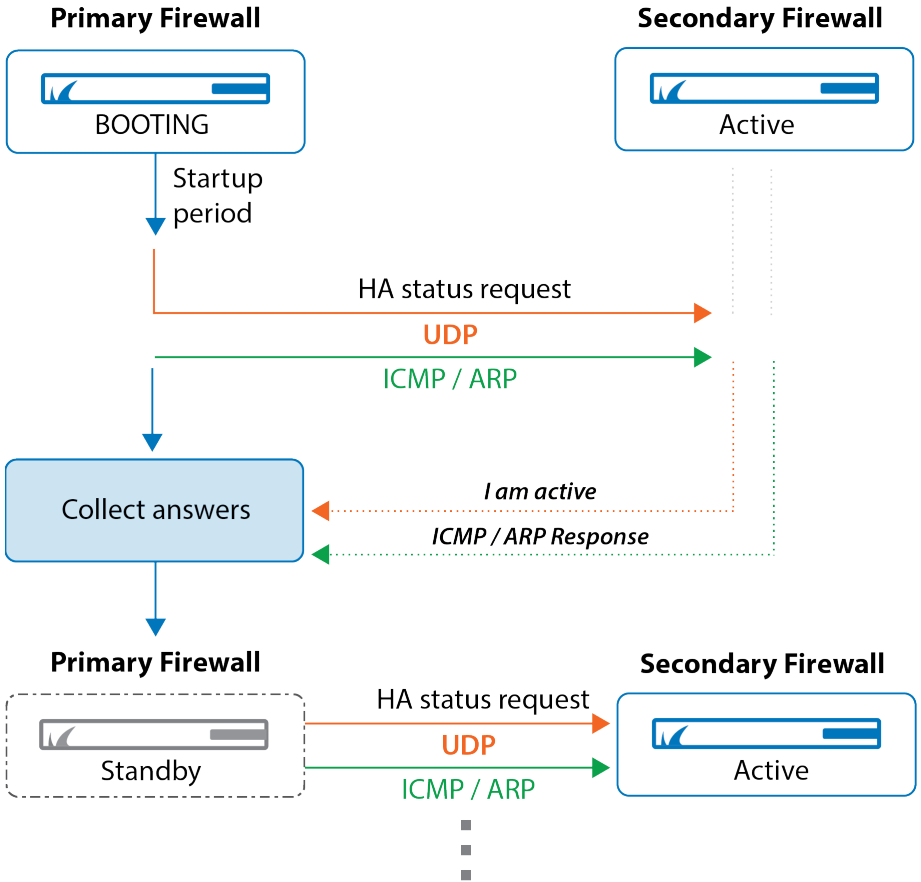
Primary Firewall Unreachable



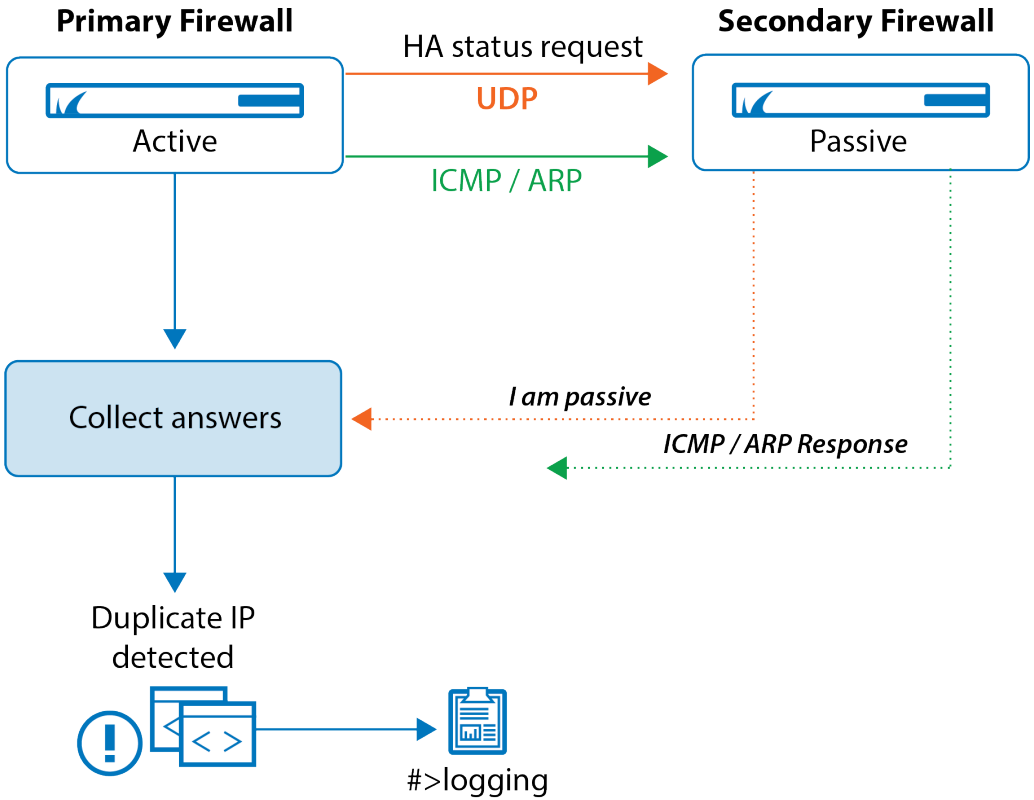
Secondary Firewall Unreachable



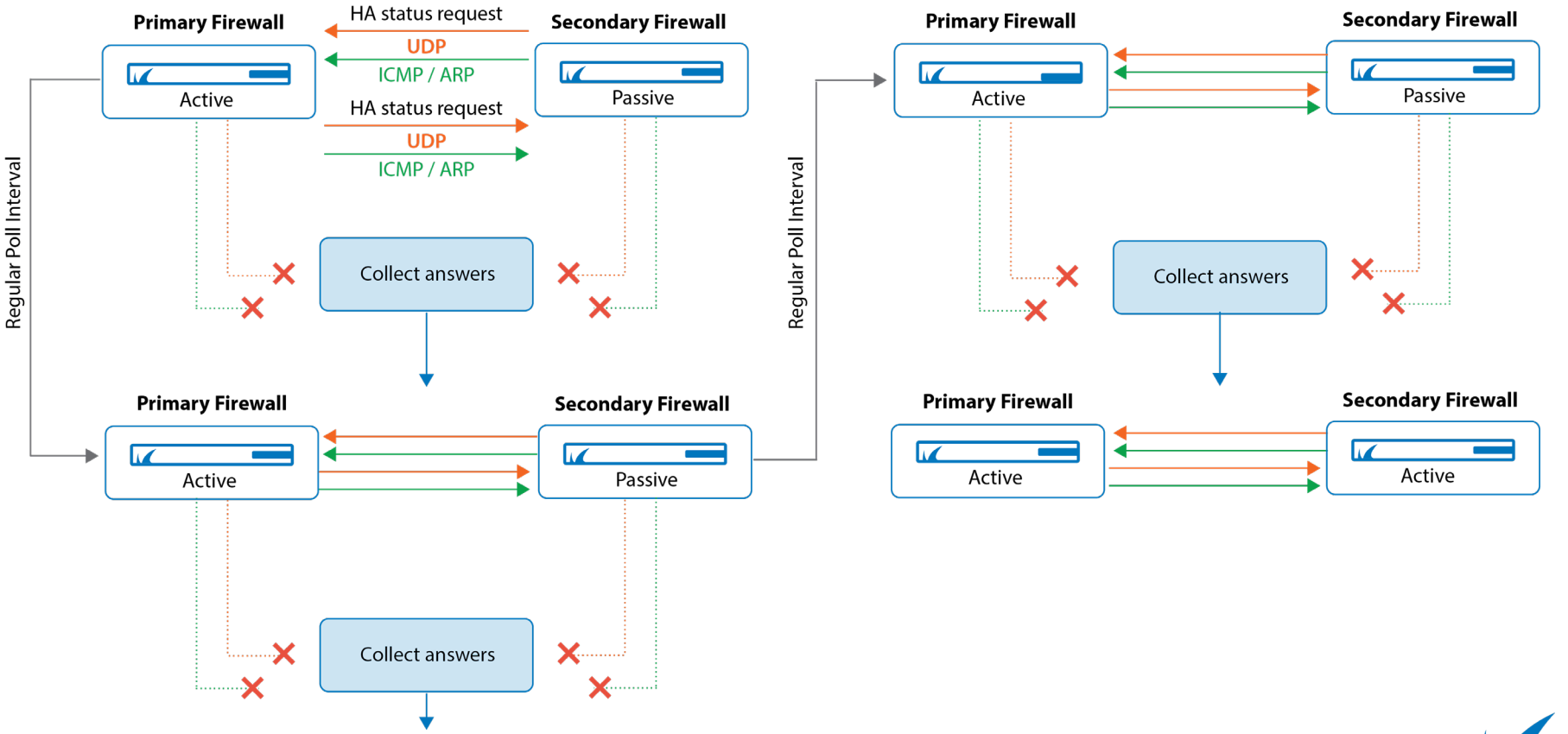
Primary Booting



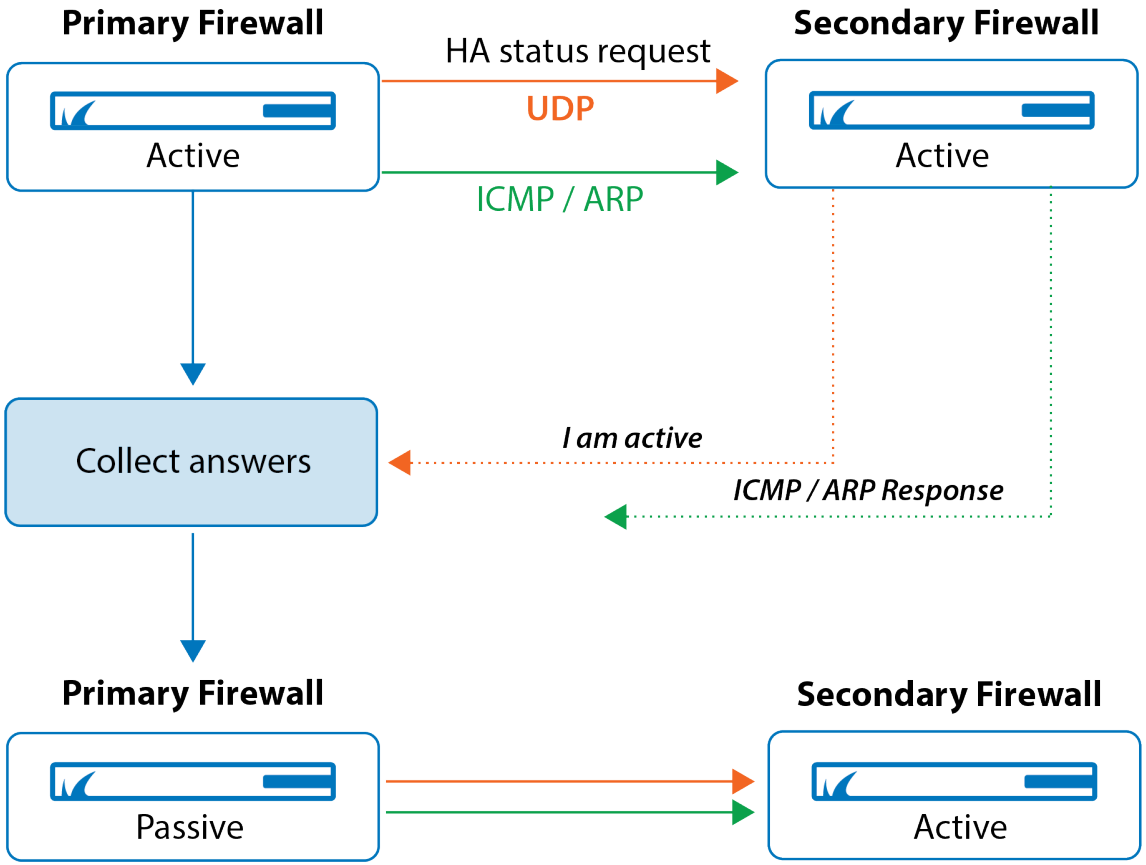
Duplicate IP Detected



Split Brain


Primary Firewall
Secondary Firewall
HA status request
UDP
ICMP / ARP
HA status request
UDP
ICMP / ARP
Active
Passive
Regular Poll Interval
Collect answers
Primary Firewall
Secondary Firewall
Active
Passive
Collect answers
Primary Firewall
Secondary Firewall
Active
Active
Regular Poll Interval
Primary Firewall
Secondary Firewall
Active
Passive
Collect answers
Primary Firewall
Secondary Firewall
Active
Active

Split Brain Resolved




Thank you
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT