



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!



JAYSBRICKBLOG.COM



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.



- 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



- 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



A LEGO Stormtrooper figure stands next to a LEGO toilet. The toilet has a white bowl and a brown base with several colored bricks (brown, green, pink) underneath. The Stormtrooper is white with black details and a black visor. The background is a soft, out-of-focus indoor setting.

Live Demo



What Has Changed with 8.0?



A LEGO Stormtrooper figure stands next to a LEGO toilet. The toilet has a white bowl and a brown base with several colored bricks (brown, green, pink) underneath. The Stormtrooper is white with black details and a black visor. The background is a soft, out-of-focus indoor setting.

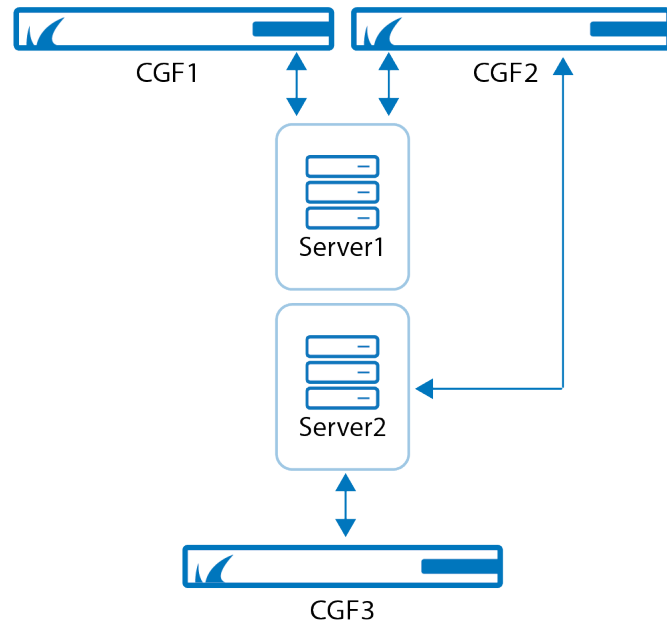
Live Demo



Virtual Server - Pros



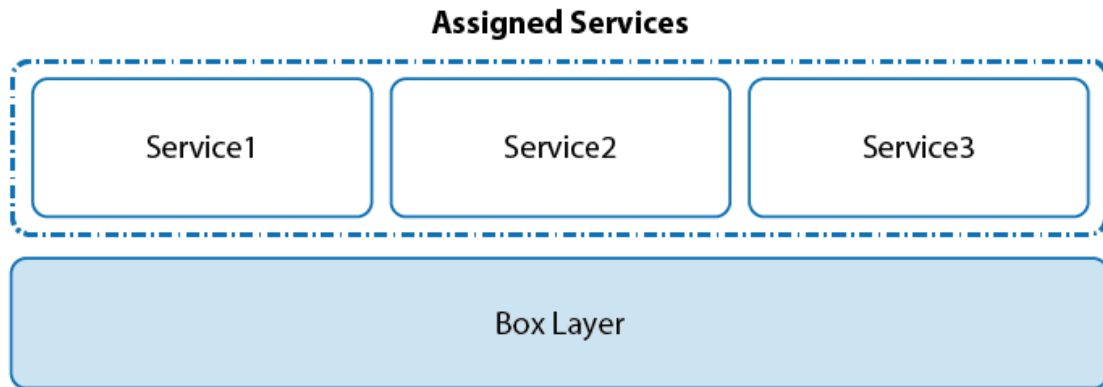
- The base concept for managing HA
 - Two different concepts (single vs managed box)
- Contains information for both partners
 - IP address, monitoring settings, probing information
- Very flexible
 - Multiple servers on one box
 - Move servers from one box to another
 - Lets you create complex HA scenarios



- 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



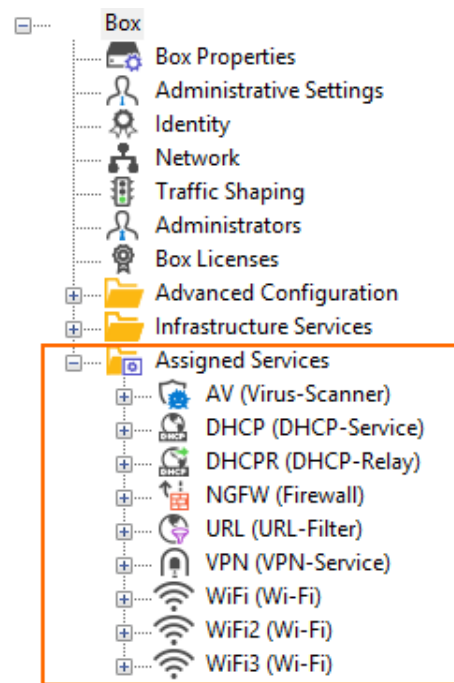
- **Box layer**
 - Runs infrastructure services and responsible for logging, event, configuration, and control
- **Assigned service**
 - Selected services can be activated by user if required.



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



A LEGO Stormtrooper figure stands next to a LEGO toilet. The toilet has a white bowl and a brown base with several colored bricks (brown, green, pink) underneath. The Stormtrooper is white with black details and a black visor. The background is a soft, out-of-focus indoor setting.

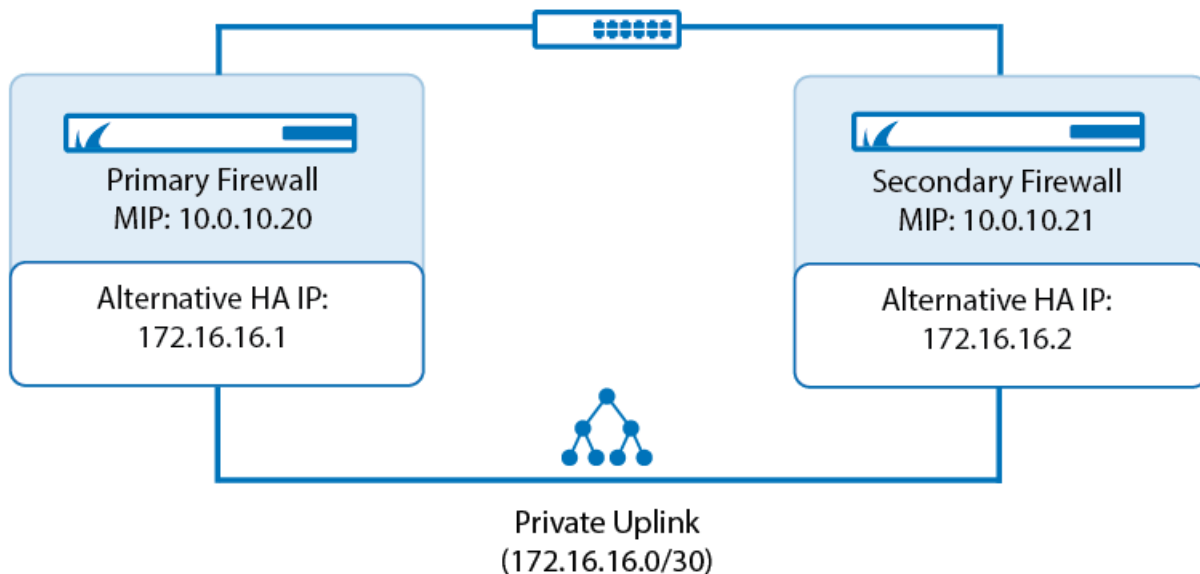
Live Demo



Under the Hood



A safeguard against failure of the switch connecting the HA units



- **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



- 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

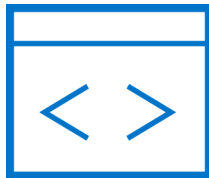


- Can help detect IP conflicts
 - When a machine receives an ARP request containing a source IP that matches its own, it knows there is an IP conflict.
- Assist in updating other machines' ARP tables
 - Clustering solutions utilize this when they move an IP from one NIC to another, or from one machine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



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



arp.isgratuitous == 1						
No.	Time	Source	Destination	Protocol	Length	Info
24	20.724561	Vmware_85:f0:7f	Broadcast	ARP	64	Gratuitous ARP for 192.0.2.43 (Request)
27	20.768955	Vmware_85:f0:7f	Broadcast	ARP	64	Gratuitous ARP for 192.0.2.43 (Request)
30	25.976857	Vmware_85:f0:7f	Broadcast	ARP	64	Gratuitous ARP for 192.0.2.43 (Request)
33	26.031636	Vmware_85:f0:7f	Broadcast	ARP	64	Gratuitous ARP for 192.0.2.43 (Request)
36	31.232926	Vmware_85:f0:7f	Broadcast	ARP	64	Gratuitous ARP for 192.0.2.43 (Request)
39	31.270793	Vmware_85:f0:7f	Broadcast	ARP	64	Gratuitous ARP for 192.0.2.43 (Request)
42	36.471654	Vmware_85:f0:7f	Broadcast	ARP	64	Gratuitous ARP for 192.0.2.43 (Request)
46	41.567543	Vmware_85:f0:7f	Broadcast	ARP	64	Gratuitous ARP for 192.0.2.43 (Request)

> Frame 36: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0

▼ Ethernet II, Src: Vmware_85:f0:7f (00:0c:29:85:f0:7f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- > Source: Vmware_85:f0:7f (00:0c:29:85:f0:7f)
 - Type: ARP (0x0806)
 - Padding: 00000000000000000000000000000000
 - Frame check sequence: 0x00000000 [unverified]
 - [FCS Status: Unverified]

▼ Address Resolution Protocol (request/gratuitous ARP)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- [Is gratuitous: True]
- Sender MAC address: Vmware_85:f0:7f (00:0c:29:85:f0:7f)
- Sender IP address: 192.0.2.43
- Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
- Target IP address: 192.0.2.43



An underwater photograph showing the lower legs and fins of a diver. The diver is positioned vertically, with their legs and fins pointing upwards towards the surface. The water is a clear, deep blue, and there are some small bubbles visible around the diver's legs. A white rope or line is visible on the left side of the frame, extending from the top towards the bottom. The text "Dive Deeper" is overlaid in the center of the image.

Dive Deeper



Monitoring Parameters

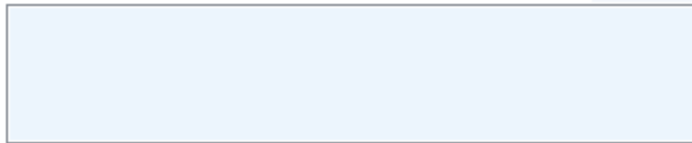
Startup Poll Interval [s]



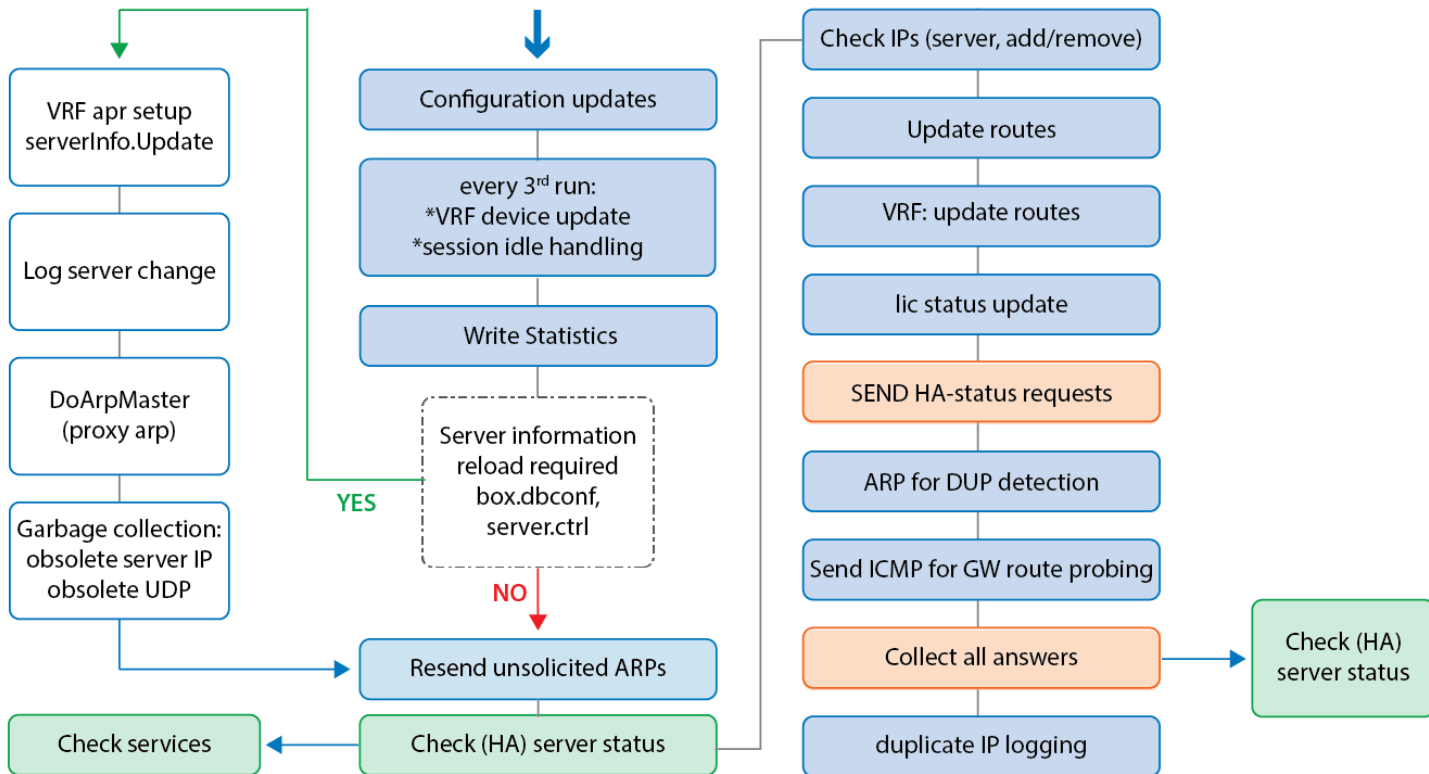
Regular Poll Interval [s]



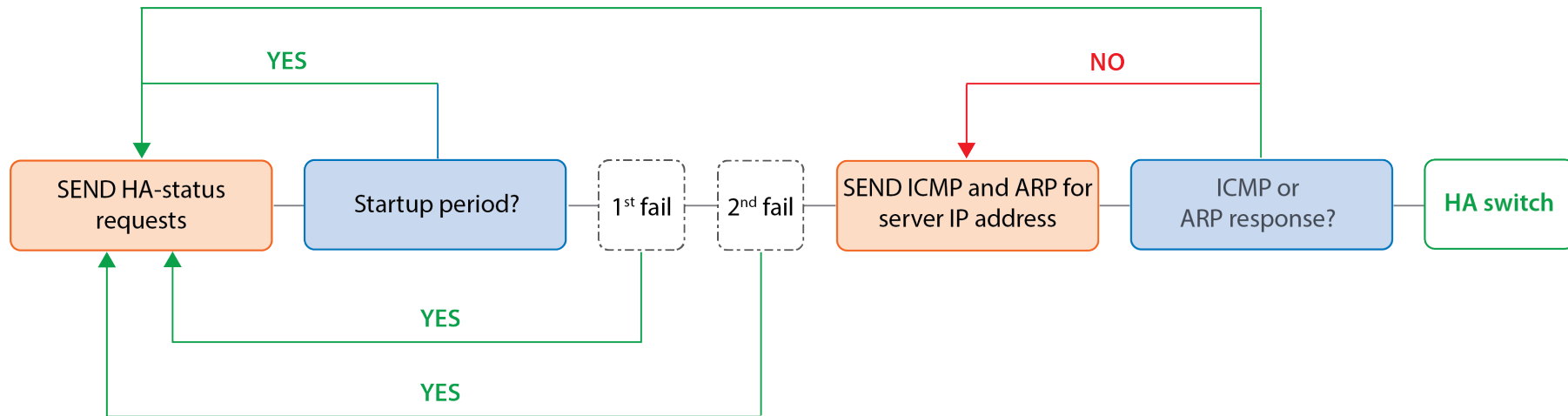
Deactivate Service



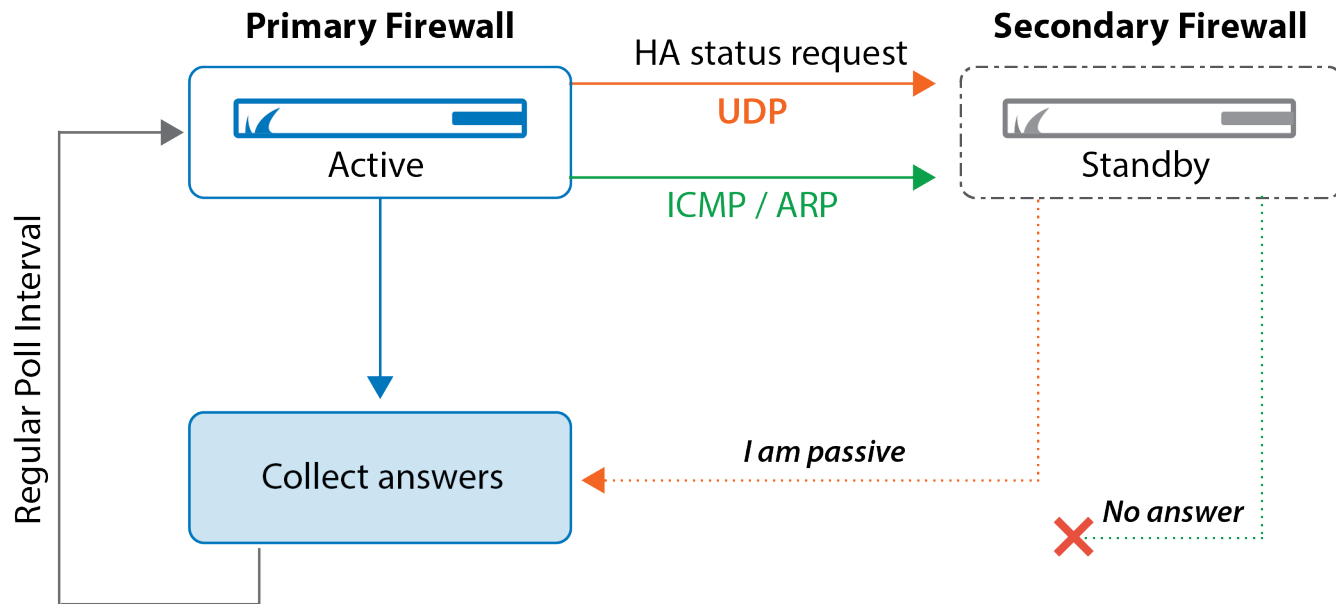
Regular Poll Workflow



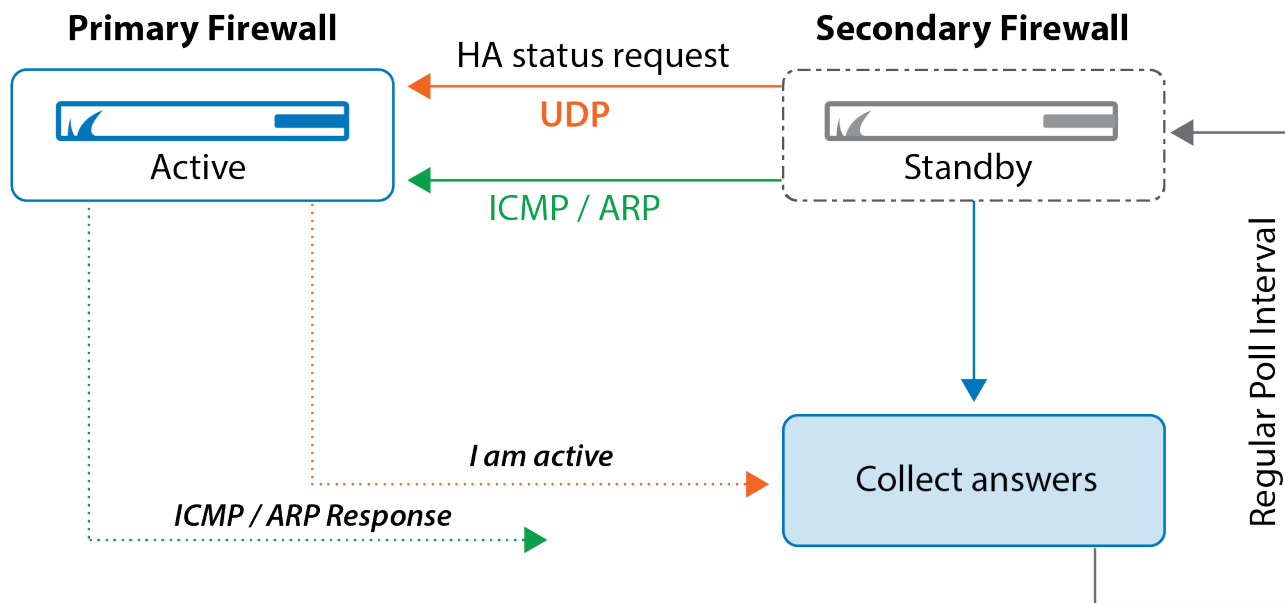
High Availability Decision Flow



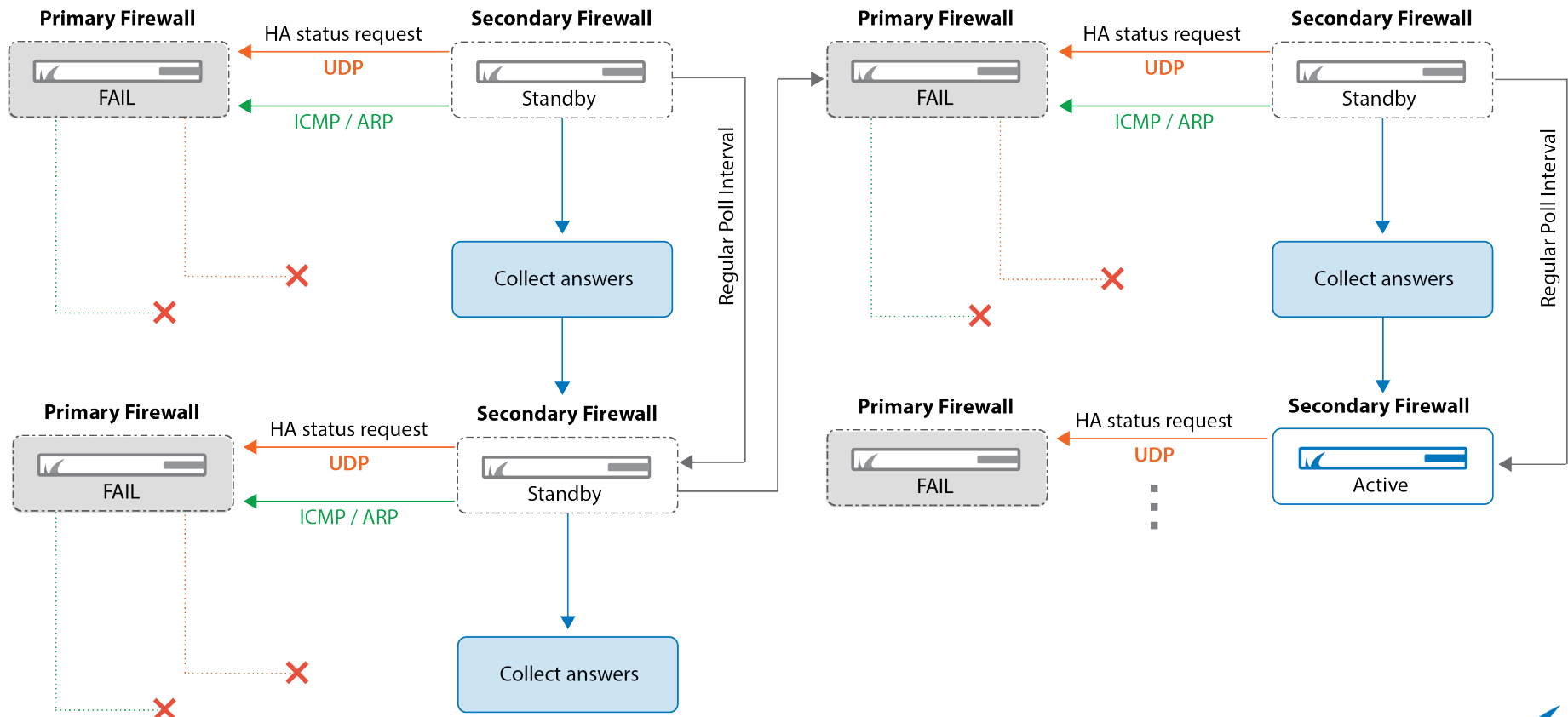
Normal Behavior – Active Site



Normal Behavior – Passive Site



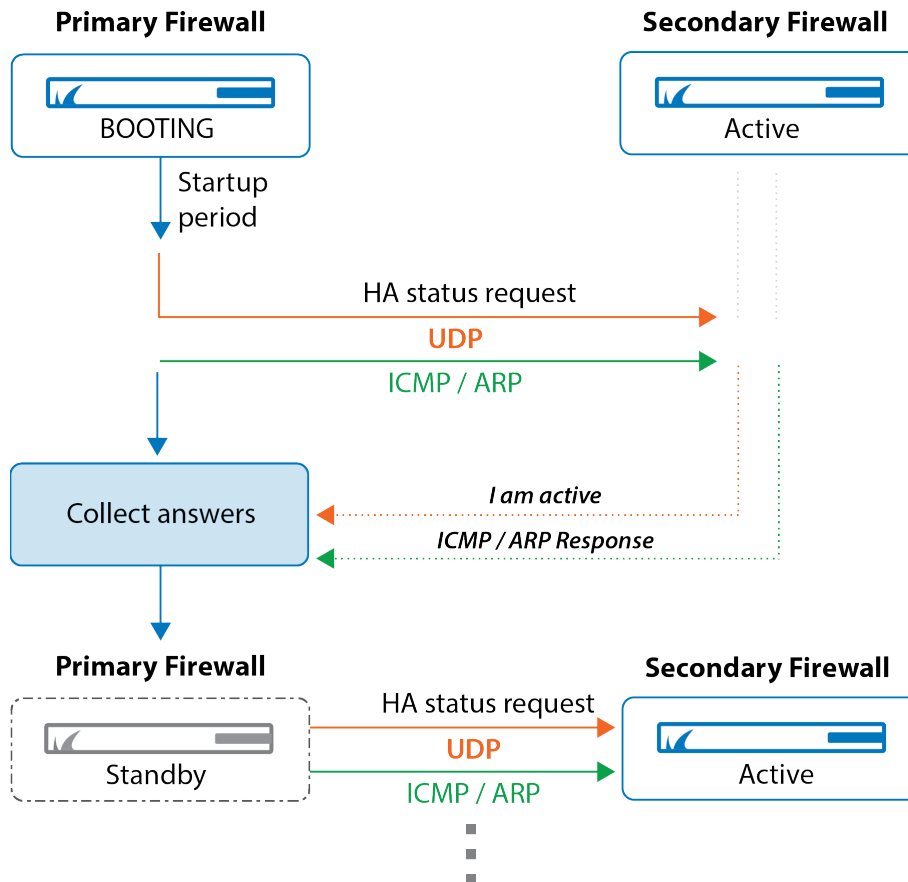
Primary Firewall Unreachable



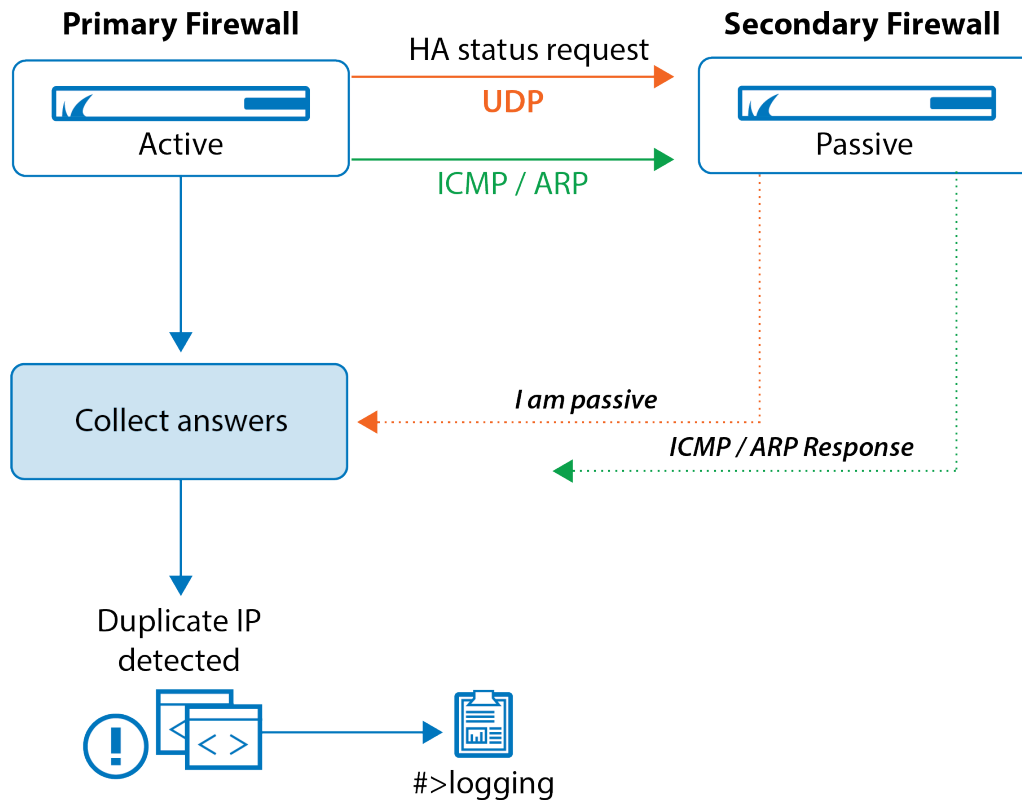
11



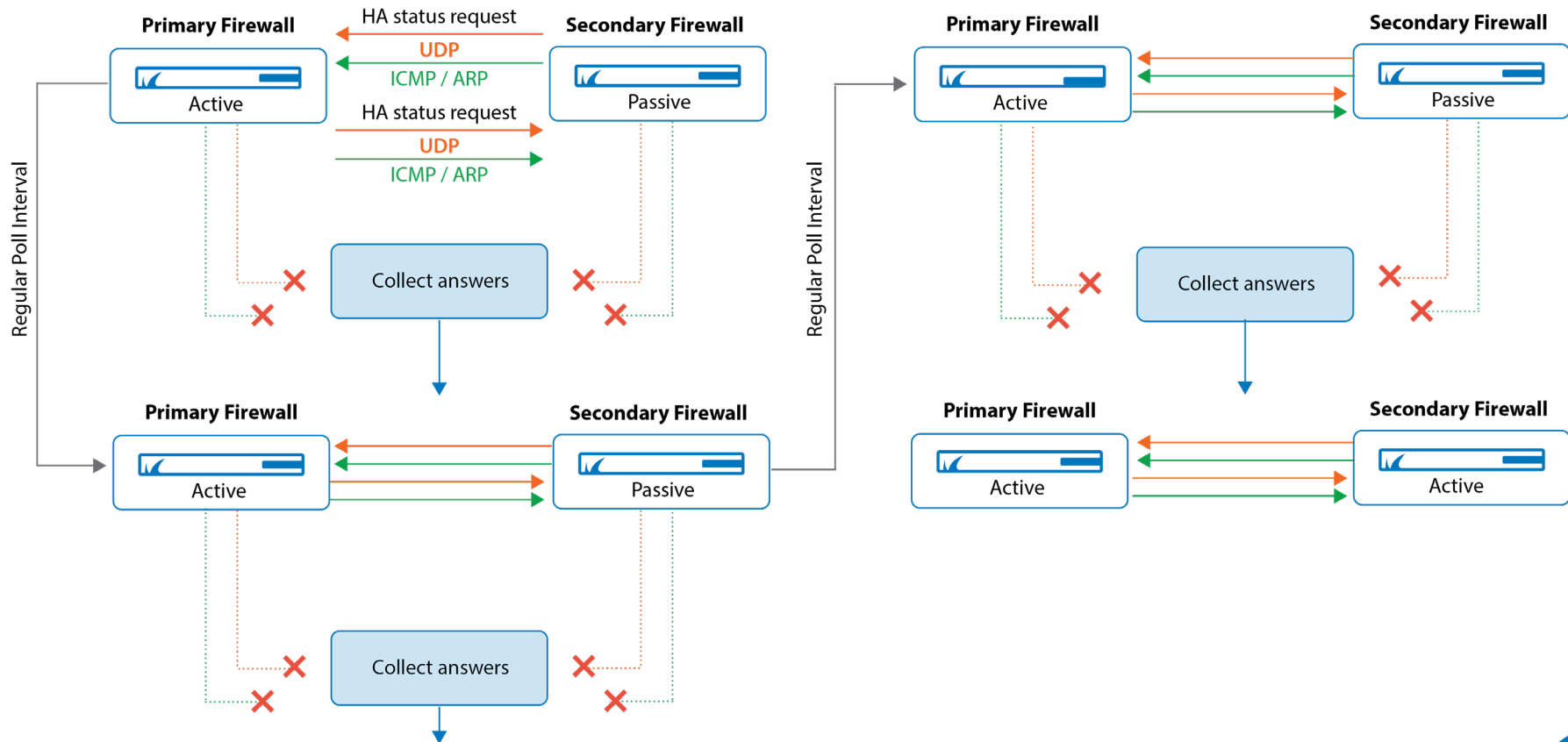
Primary Booting



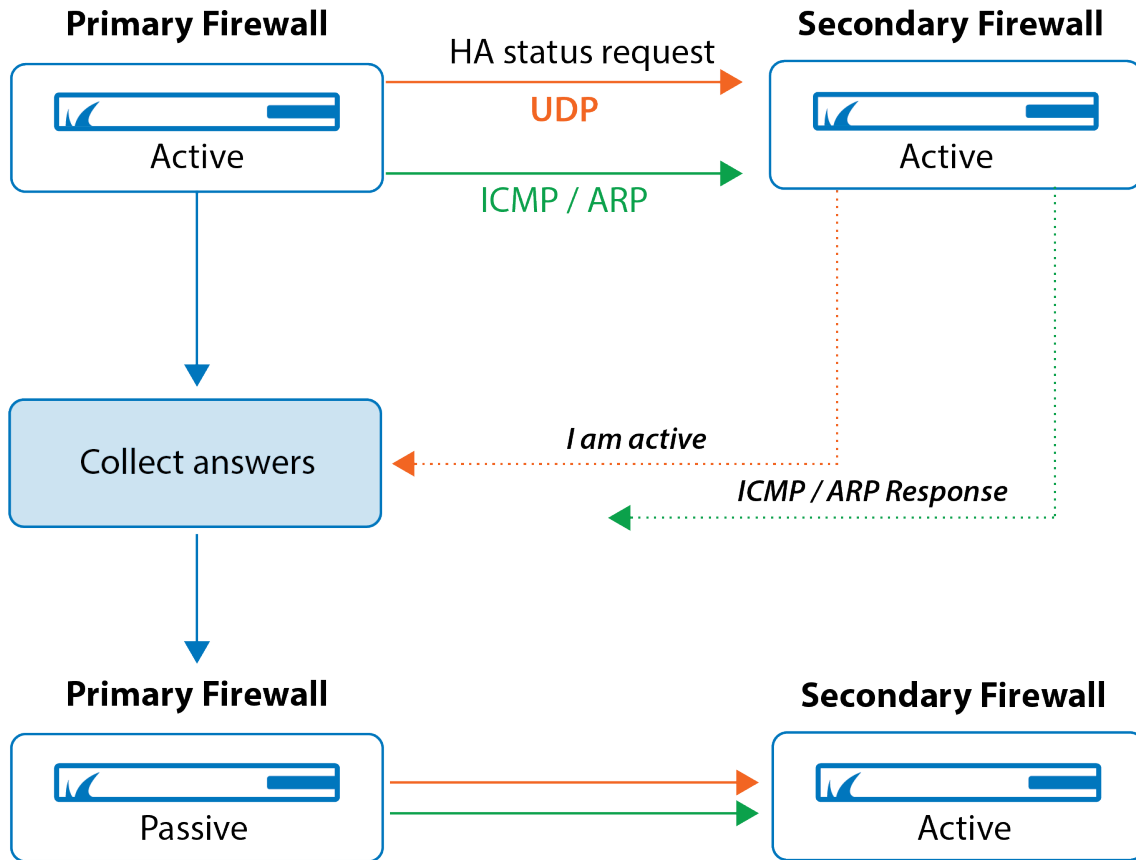
Duplicate IP Detected



Split Brain



Split Brain Resolved





Thank you

 Barracuda®
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT