Security: Financial Banking

Ensuring Complete High Availability (HA) Redundancy for Critical Links

Major financial institutions experienced 80% more cyberattacks over the past 12 months, a 13% year-over-year increase, with a 238% surge in cyberattacks against banks during the coronavirus pandemic.[1] According to a new analysis by the Federal Reserve Bank of New York, a single cyberattack on one of the top U.S. banks would likely have a major effect on the global financial system.[2]

The banking industry faces a whole range of risks as they evolve in the interconnected edge enterprise landscape while battling a growing list of software attacks including denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, man-in-the-middle (MitM) attack, phishing, and spear-phishing attacks, credential stuffing, and ransomware.

While a majority of threats target software vulnerabilities, banks also risk hardware vulnerabilities that could put the organization's digital infrastructure at risk, from an employee device to a router connected to an unsecured network, through the Internet of Things (IoT) and cloud exploitation.

The core concept for the banking Cyber Security Strategy is to safeguard customer assets and their transactions. As breaches lead to damage banks' standing in the financial market, consequences, and penalties for FDIC non-compliance, monetary losses, and customer confidence.

Challenge: This was the environment when one of the United States' largest financial corporations, who specialize in Business and Commercial Banking and Financing came to Garland Technology looking to future proof their security deployment with a cost effective, scalable connectivity strategy that provides resilience and redundancy.

This organization's security strategy involved the use of Intrusion Prevention Systems (IPS) and DDoS protection for all critical links. IPS is a network security tool that examines network traffic flow to detect

©2020 Garland Technology LLC. All Rights Reserved

and prevent vulnerability exploits. A DDoS protection tool specifically blocks denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

Both security solutions are deployed inline, meaning the tool sits directly in the path of network traffic to actively protect and block potential threats. The company reached out to Garland Technology as a leader in inline security, whose CTO Jerry Dillard invented bypass technology, knowing they needed a scalable connectivity strategy that accounted for inline deployment sensitivities.

Architecting networks with High Availability (HA) or redundant designs, creates added challenges for security and networking teams, in not only effectively deploying and updating tools effectively, without creating a single point of failure for each device but how to adjust once an HA has been triggered.

Goal: Ensure all critical links are actively protected using IPS and DDoS technology, incorporating a strategy of resilience, reliability and redundancy so there is no business interruption or downtime, while protecting sensitive data.

Solution: Garland's engineering team worked with the IT team to design an HA architecture that solved all of their challenges, while providing additional value and functionality, leading them to expand this use case throughout their enterprise.

Our teams worked through questions like, do we have to buy two of everything? What happens if traffic switches from primary to secondary? How are we going to track that data? How do we correlate everything? While working through expectations, urgency, and availability of each device.

There are two options for incorporating High Availability (HA) solutions, Active/Standby, and Active/Active. Active-Standby (Or Active/Passive) deploys to a secondary tool, providing failover from a primary device to the backup appliance. Active/Active deploys to a redundant link, providing failover if either active device fails.

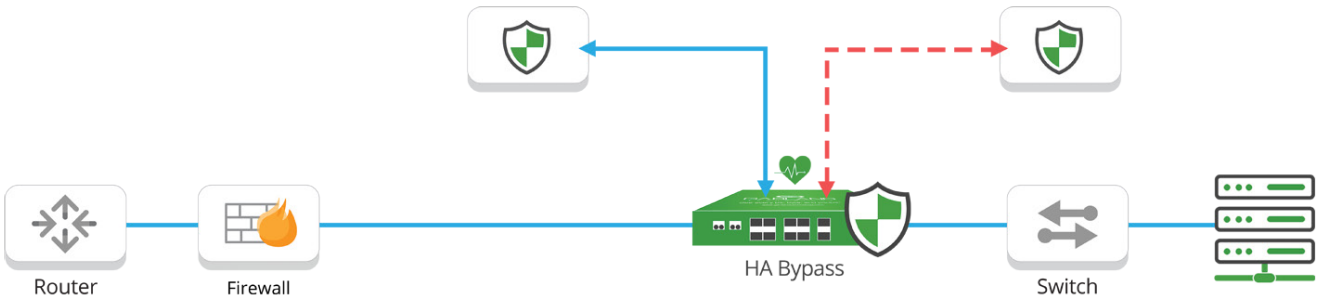

Diagram 1: High Availability (HA) solution for Active/Passive, provides failover from primary device to backup appliance

©2020 Garland Technology LLC. All Rights Reserved

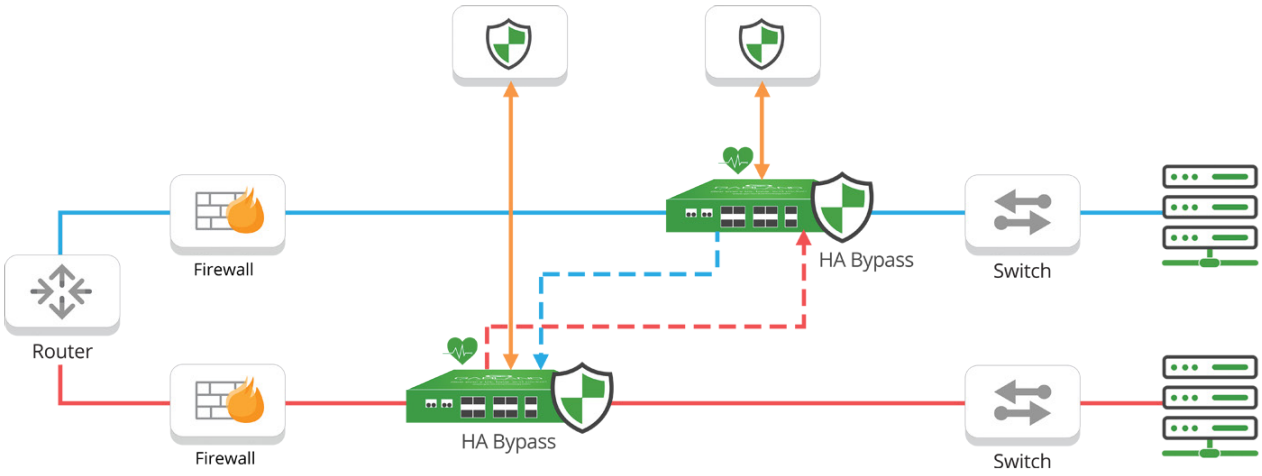

Diagram 2: High Availability (HA) Crossfire solution for Active/Active, provides failover if either active device fails.

The EdgeLens® Inline Security Packet Broker transformed their network security capabilities, instead of replying on a single bypass TAP for each device, they were able to not only provide the same reliability and management controls of a bypass, but also managing multiple inline and out-of-band tools from the same device with packet broker functionality, which easily complemented either HA architecture.

For each link deployment the IPS was deemed critical, so each EdgeLens deployed two redundant IPS etools in an active standby scenario, one IPS as the primary or “active” appliance brought inline through the EdgeLens and the secondary IPS or “passive” appliance, which still receive live traffic, but is not considered inline. This provides “Hot Standby” redundancy. In the event the primary appliance goes down and the heartbeats stop being received by the TAP, the secondary appliance will immediately and automatically take over as primary and be brought inline.

Each deployment also incorporated one DDoS protection tool, which was managed by the bypass functionality, providing heartbeat health checks and “inline lifecycle management” which allows you to easily take tools out-of-band for updates, installing patches, maintenance or troubleshooting to optimize and validate before pushing back inline.

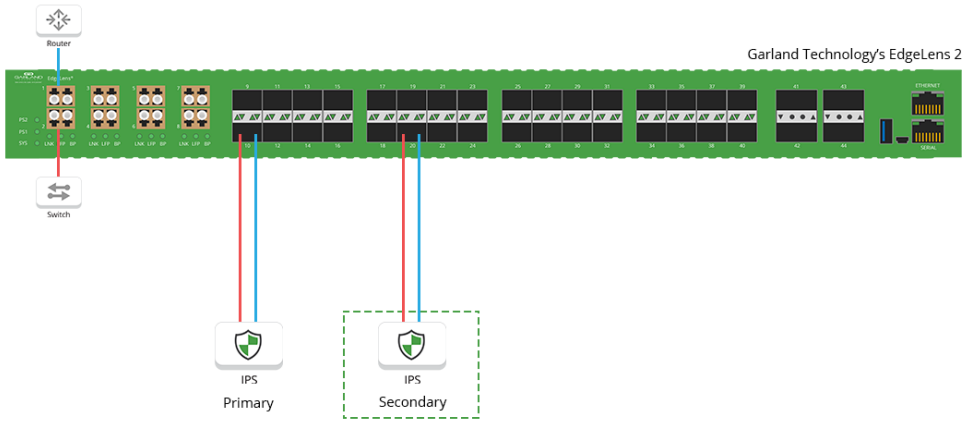

Diagram 3: High Availability (HA) Crossfire solution for Active/Active, provides failover if either active device fails.

©2020 Garland Technology LLC. All Rights Reserved

Simplified Security Stack

This solution provided an easy, hardware base chaining solution, that allows you to manage multiple inline and out-of-band tools individually, between multiple network segments from the same device, while also providing bypass resilience. If one of the tools in the chain can't keep up, load balance to the other tools 1:1 or 1:N (one to many) tools.

Benefits:

- Distribute traffic before and after an inline tool (WAF, NGFW, or IPS) to out-of-band tools
- Simplify security stack and reduced network complexity by managing multiple inline tools
- Provide filtering, aggregation, and load balancing to inline links
- Reduced risk of unplanned downtime
- Network resilience - flexibility to bypass the tool and keep the network up, or to failover to a High Availability [HA] solution

Looking to add visibility and reduce network complexity, but not sure where to start? Join us for a brief network Design-IT consultation or demo. No obligation - it's what we love to do.

1-VMware Carbon Black third edition Modern Bank Heists report https://www.carbonblack.com/resource/modern-bank-heists-3-0/
2-https://www.newyorkfed.org/research/staff_reports/sr909

©2020 Garland Technology LLC. All Rights Reserved