

Major National Bank Embraces Cyber-Resilience with Deployment of Hillstone NIPS and NGFW

The Customer

A large and well-known bank in Southeast Asia is responsible for the country's central credit fund and tasked with regulating capital across the entire system including accepting deposits, issuing loans, and assuring stability. Founded in 1995, the bank has grown from just 20 employees to an extensive organization with 32 branches and 66 transaction offices serving nearly all provinces and cities nationwide. The bank continuously strives to expand, improve operational efficiency, and develop new products and services to meet the needs of its members.

The Challenge

For financial institutions, security is of paramount importance. Some years ago, the bank had installed a next-gen firewall as a first line of perimeter defense; however, it was nearing end of life and lacked several capabilities that the IT staff deemed critical.

The team set out to assess options for replacement. At minimum, they sought a modern NGFW with robust security features and affordable pricing, as well as an IPS system to protect the increasingly segmented server farm. The new NGFW should equal or exceed the capabilities of the existing firewall and offer a user-friendly graphical user interface to ease management complexity and reduce IT staff workload.

The team also identified two key requirements: The NGFW would need to support both IPsec VPNs, to provide secure connectivity for branches and transaction offices, as well as SSL VPN to allow field staff and others to securely connect to the headquarters or remote networks. The latter would also help assure cyber-resilience in the event of a natural disaster, pandemic, or other business-disruptive event. And finally, to further ensure business continuity and uninterrupted accessibility, the NGFW needed to support an active-standby high-availability configuration.

From a more strategic viewpoint, the bank's IT team sought a solution that would offer improved protection at the perimeter and support for higher bandwidth than the current firewall. In addition, the IPS solution needed to not only protect servers, but also accommodate legacy operating systems or applications running on them.

The bank's IT director noted, "We needed better protection at the perimeter with a firewall that would accommodate much greater bandwidth than our current one. In addition, our IPS needs were complicated because of a mixed server environment supporting both new and older applications and operating systems."

Major National Bank Embraces Cyber-Resilience with Deployment of Hillstone NIPS and NGFW

The Solution

After a thorough review and proof-of-concept (POC) testing with multiple vendors' solutions, the bank chose Hillstone's next-generation firewalls (NGFWs) and network intrusion prevention system (NIPS). The Hillstone solutions easily met the routing and security requirements of the project.

Said the IT director, "In Hillstone's products, we found a solution that performed exceptionally well during our POC. The NGFW and NIPS clearly meet our needs today, and we have high confidence that they will support our continued growth in the future."

The Hillstone NGFW and IPS solutions stood out during the POC for meeting not only the routing and security requirements for the project, but also excelling at several specific technical needs. In addition, the NGFW offers extended features like load balancing, which the bank found highly attractive. The customer also gave high marks to Hillstone's technical support services, which they found to be extremely responsive and reliable.

Hillstone's NGFW includes comprehensive network security with advanced firewall features and provides a superior total cost of ownership (TCO), excellent energy efficiency, and

comprehensive threat prevention capability. It provides granular and comprehensive visibility and control of applications and can identify and prevent potential threats associated with high-risk applications. The NGFW provides policy-based control over applications, users, and user-groups for fine-grained security access. Policies can be defined to ensure bandwidth for mission-critical applications while restricting or blocking unauthorized or malicious applications.

The Hillstone NIPS delivers advanced network intrusion detection and prevention capabilities. Using a sophisticated threat engine and context/application awareness, it detects, analyzes, and blocks advanced threats from business-critical servers in real time. Hillstone NIPS also integrates seamlessly with other Hillstone security solutions; for example, it can sync up policies for Hillstone NGFWs to block future attacks.

Conclusion

For this prominent financial institution, Hillstone's NGFW and NIPS solutions are a winning combination. Together, they provide robust and extensible security, much easier management, and future-ready features, all of which combine to help achieve cyber-resilience. Further, the bank gains extended capabilities like IPsec and SSL VPN, load balancing and others that help meet its stated goal of improved operational efficiency.