![Hillstone Networks logo]

Case Study

Large Water Utility Services Provider Modernizes and Upgrades Security Infrastructure with Hillstone Networks

Hillstone's solutions provide comprehensive security, centralized management, improved performance and visibility for data center, remote sites and web applications

Customer Profile

Customer

Sistema Intermunicipal de Agua Potable y Alcantarillado (SIAPA) (Intermunicipal System of Sewerage Services)

Sector

Government Utility

Location

Guadalajara, Jalisco, Mexico

Size

Serves the majority of the Guadalajara metro area, the 3rd-largest in Mexico

Scope

Provides sewerage systems and sanitation services

Challenges

Previous security technology had become obsolete, requiring an upgrade to the latest generation technology to assure the security of data center and remote sites and gain centralized management and system-wide visibility.

Requirements

- Update the aging security infrastructure to meet a challenging threat environment
- Expanded security service for both data center and remote sites
- Centralization of management, maintenance and monitoring on a single platform
- Broad visibility across the infrastructure to improve detection and mitigation of threats

Result

Hillstone's broad product set provides in-depth protection, efficient centralized management and deep visibility with scalability and the ability to easily add features in the future.

The Challenge

Upgrading Security Infrastructure for a Water Utility

Founded in 1978, the Sistema Intermunicipal de los Servicios de Agua Potable y Alcantarillado (SIAPA) delivers water, sewerage and sanitation services for Guadalajara and four surrounding cities. Facilities include the data center, 17 remote sites and about 3,000 employees, serving more than four million residents.

As a public utility, SIAPA faces unique challenges, threats and regulatory requirements. Outages can severely impact users of the system, and monitoring quantity, quality and availability of service offerings is essential. In addition, subscribers' personal data must be kept safe from misuse or theft.

Public services and entities have globally come under increasing attacks by ransomware, malware and other cyberthreats. For example, in one recent incident in North America, hackers breached computers at multiple water utilities, targeting the industrial software used to control and monitor machinery.

A Careful Evaluation

Over time, the utility's aging cybersecurity infrastructure had become outmoded and obsolete. The SIAPA IT team began searching for a replacement solution that would bring the latest security technologies and expand upon the protections spanning the central and distributed facilities and the web-based user interfaces.

In addition to the technical criteria, the team focused heavily on the total cost of ownership (TCO) and cost/benefit ratio. As a public utility, SIAPA has a fiduciary responsibility to ratepayers to manage their resources conscientiously.

The team also took into consideration the changing threat landscape for utilities and the need for future expansion – both in numbers and scale of the security infrastructure, as well as in the ability to add new capabilities as needed down the road. Ultimately, SIAPA reviewed solutions from three different vendors. Through testing and evaluation, the choice became clear.

The Solution

Comprehensive Security, Central Management and a Future-Ready Platform

SIAPA chose Hillstone's A-Series next-generation firewalls (NGFWs) for their robust functionality, scalability, and integration of specific capabilities at no additional cost. In addition, the NGFWs can easily and affordably support other features such as ZTNA and SD-WAN capabilities.

The team also implemented the Hillstone Security Management platform (HSM) for centralized management and the Hillstone Security Audit platform (HSA) for security intelligence. Rounding out the solution are Hillstone's web application firewall (WAF) and application delivery controller (ADC).

Hillstone A-Series NGFWs provide intelligent threat detection and prevention, high performance and easy-to-use policy definition and operation. The A-Series is Hillstone's flagship NGFW and features outstanding application-layer performance to address threats, attacks and other malicious activities.

Two NGFWs are deployed at the data center in a high-availability pair, and other Hillstone NGFWs protect remote

facilities. All Hillstone firewalls have the ability to intercommunicate, resulting in a far stronger security posture across the entire architecture.

Centralized Management with Improved Forensics

With operations spanning multiple branches, the management and operations of the security infrastructure were also a high priority. SIAPA chose Hillstone's HSM to manage the distributed devices, reducing management overhead and accelerating deployment and configuration. HSM also serves as the central security manager for the SD-WAN solution for policy management and one-click set-up of SD-WAN networking.

Hillstone's HSA provides advanced forensics by aggregating and correlating logs across multiple security devices. This data can then be easily queried to analyze trends, potential threats and other security and operational concerns. Together, HSM and HSA provide visibility and security intelligence to help the SIAPA team move from a reactive to a proactive stance.

Noted Jose Luis Alvarez, Head of Infrastructure and Security Section for SIAPA and his team, "Previously we had almost no visibility into attacks. Now we have 100% visibility and are able to quickly work to mitigate them."

Protecting Web Apps, Improving Services

Service to subscribers is also an important mission for SIAPA, and it maintains an extensive web presence and web applications for payments, service orders and other functions. In addition, SIAPA staff rely upon multiple applications to perform their duties and serve the public.

To support these vital operations, SIAPA selected Hillstone's WAF and ADC. The WAF provides comprehensive security for web servers, applications and APIs, and protects against DDoS attacks, the OWASP Top 10 threats, bots, and other risks. Hillstone's ADC provides health checks for applications while ensuring application availability and performance.

The NGFWs, WAF and ADC interwork with the HSM and HSA for streamlined, coordinated management and operation. This consolidated approach also enables deep inspection of internet traffic to detect threats, malware and anomalies, all without impacting network performance.

> "We were able to cover more than we expected in the initial project and were able to include more security solutions within the same budget.

Jose Luis Alvarez
Head of Infrastructure and Security Section for SIAPA

Conclusion

A Revitalized, Robust Security Framework

The SIAPA team has seen near-instant results from the new security infrastructure. In addition to gaining new cross-network visibility, Alvarez noted that the IT team has changed from working reactively to proactively. In addition, he said, "We were able to cover more than we expected in the initial project, and were able to include more security solutions within the same budget with Hillstone Networks' solutions."

The impact on the vital web services for billing, ordering and other functions was particularly striking, Alvarez said. "We improved the performance and increased response times by 200 percent," which improved customer satisfaction and reduced staff time requirements for direct customer interaction.

SIAPA is now well-positioned to meet a changing threat environment through a modernized, robust security posture, centralized management, and improved visibility across its sprawling network.

About Hillstone Networks

Hillstone Networks is a leader in cybersecurity, delivering both depth and breadth of protection to companies of all sizes, from edge to cloud, and across any workload. Hillstone Networks' Integrative Cyber Security approach brings coverage, control, and consolidation to more than 26,000 enterprises worldwide.

Hillstone Networks is uniquely positioned with a platform that's future-proof to enable digital transformation and business continuity. For more information and to find your Integrative Cybersecurity solution, please visit www.hillstonenet.com

Learn more about Hillstone products mentioned in this case study

Hillstone Next Generation Firewall (NGFW) ⇨

Hillstone Security Management (HSM) ⇨

Hillstone Web Application Firewall (WAF) ⇨

Hillstone Application Delivery Controller (ADC) ⇨

Read about Hillstone solutions

Cloud Workload Protection (CWPP) ⇨

Extended Detection & Response (XDR) ⇨

Zero-Trust Network Access (ZTNA) ⇨

Secure SD-WAN ⇨

Micro-segmentation ⇨

Network Detection & Response (NDR) ⇨

Gartner Peer Insights Customers' Choice 2023

Hillstone
NETWORKS