Case Study

Cutting-Edge Cyber-Defenses for a State-of-the-Art Medical Facility

Hillstone's NGFWs protect vital hospital and practice resources and data, help achieve compliance and assure high availability of critical services.

The Challenge

Rejuvenating and Enhancing Security Defenses

Based in Guayaquil, Ecuador, Interhospital is a physician-owned and -operated facility that features a hospital with multiple operating rooms as well as a state-of-the-art imaging and diagnostics center. More than 300 doctors practice 42 specialties at the center serving a broad area of the country's coast. Founded in 1996 as International Laboratories Services (Interlab) S.A., which focuses on clinical laboratory results, the Interhospital complex opened in early 2021.

Despite the relative newness of the medical center, the facility's firewalls had reached the end of service life and needed to be renewed. Interhospital's systems manager, Jenny Rezabala, began the search for replacements. The primary goal was to protect the network perimeter for both buildings while supporting all traffic to and from the network. Advanced cybersecurity was required to protect business operations as well as critical patient data while complying with the country's version of HIPAA regulations.

Special Considerations

In addition, the facilities utilize multiple Internet Service Providers (ISP) links to help ensure continuous availability and low congestion. These links would need to be load balanced to ensure efficient operation, and QoS rules applied for services like VoIP and others.

After considering multiple vendors' offerings, Interhospital's team selected Hillstone's E-Series next-gen firewalls for deployment.

Customer Profile

Customer

Interhospital

Sector

Healthcare

Location

Ecuador

Scope

Provides high-quality medical care for country's second-largest city

Size

Hospital and medical diagnostics center with 42 specialties, 300 doctors

Challenges

Refresh existing NGFWs within budget while gaining leading cybersecurity capabilities

Requirements

- Protect critical patient and other data against breach and attack
- Provide enhanced visibility and forensics into attack sources
- Support multiple ISP links for continuous uptime
- Deliver Quality of Service (QoS) for voice, data and other services

Result

Cutting-edge cybersecurity through NGFWs that offer intuitive management of security policies and processes while protecting critical data.

> In just one 24-hour span, they detected 270 medium-grade attacks which we were able to then quickly mitigate through the accurate identification of the source IPs.
>
> **Ms. Jenny Rezabala**
> Interhospital's systems manager

The Solution

Comprehensive Network Security, Advanced Features

Hillstone's Next Generation Firewalls (NGFWs) incorporate wide-ranging network security and advanced firewall features with comprehensive threat prevention capabilities and superior energy efficiency. It provides both in-depth and granular visibility and control of applications, users and user-groups.

Policies can be specified to guarantee bandwidth to mission-critical services while also blocking or restricting malicious or unauthorized applications. Said Ms. Rezabala, "Hillstone's security policies and processes are well established and intuitive," making set-up and management much easier.

She also noted that Hillstone's sales and support teams are highly responsive and provided assistance as needed throughout the evaluation and deployment process.

Meeting the Specialized Needs of Healthcare

Like many countries, Ecuador has instituted regulations similar to HIPAA – the U.S. Health Insurance Portability and Accountability Act. Therefore, protecting patients' confidential health information is of the utmost importance for Interhospital. The Hillstone NGFWs provide comprehensive security with advanced firewall features to detect and prevent threats such as viruses, spyware, SQL injections, ARP spoofing and many other threats. It includes a unified threat detection that can share packet details with other security engines as well.

In addition, the healthcare industry worldwide is among the most targeted by cyberattacks, according to multiple sources. Regarding the Hillstone NGFWs, Ms. Rezabala remarked, "In just one 24-hour span, they detected 270 medium-grade attacks which we were able to then quickly mitigate through the accurate identification of the source IPs."

Link Load Balancing for Multiple ISP Connections

Another advantage of the new NGFWs for Interhospital is the ability to load balance multiple ISP links for efficient operation and redundancy. Interhospital maintains three separate ISP connections for data, internet and voice services. The Interhospital IT team has established network traffic policies and QoS rules in the Hillstone NGFWs to improve overall network traffic both to and from the network perimeter. Outbound policies can be based upon multiple criteria, and inbound link load balancing supports SmartDNS and dynamic detection.

Conclusion

Leading Cyber-Defense Technologies for a Prominent Medical Facility

Interhospital's goal is to provide the ultimate in imaging and other diagnostic testing, as well as medical and surgical care, for its patients. Through the Hillstone Next-Gen Firewalls, Interhospital gains comprehensive network security, protections for sensitive patient health information, enhanced visibility and forensics, and more-efficient network services spanning multiple ISP links.

Learn more about Hillstone products mentioned in this case study

Hillstone Next Generation Firewalls (NGFW) ⇨

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 2022™

Hillstone
NETWORKS