Hillstone NETWORKS

A Third-party Testing Laboratory Secures its Remote Workforce with Hillstone Networks

The Customer

Founded in 2002, the customer is an U.S. based third-party laboratory that provides high quality testing, research, training and consulting services. It specializes in products sampling for the food, environmental, water, supplement and nutraceutical industries. The customer strives to help its clients obtain accurate, fast and reliable analytical data, and provides total solutions to help its clients ensure food safety, water quality and environmental health. The company's lab is ISO 17025 accredited, and testing is performed per industry-standard methods or through tests developed and validated in-house. Each test or test series is presented to clients in meticulously detailed reports.

The Challenge

The third-party testing laboratory serves a wide range of industries to meet their various regulatory requirements. All tests are conducted in the state-of-the-art lab. Oftentimes tests and reports must be completed in a short timeframe to meet customer needs. Like many technology companies, the customer offers a number of its employees flexible schedules and the option to telecommute at times to allow more flexibility in meeting customers' tight turnaround times. This trend towards remote work is common throughout the technology industry, especially during natural disasters, pandemics and other business disrupting events.

In order to facilitate teleworking, however, employees not only need remote access to the corporate network but also cloud-based services, that access needs to be ultra-secure. Remote work introduces new attack surfaces that can endanger critical corporate data and resources. Unsecured remote devices can be compromised by tactics such as spearfishing, Trojans and malware, and data in transit can be subject to Man-in-the-Middle (MITM) attacks or other intrusion attempts. These exploits can then traverse into the corporate network, compromising vital business data and other assets.

To defend against malicious attacks, the testing laboratory sought a secure remote access solution to protect its network and data within the corporate network as well as in its Amazon Web Services virtual private cloud (VPC). Specifically, the lab's IT team was looking for a solution that addressed four key requirements:

1. Secure remote access to the corporate network and the cloud environment for employees, anytime, anywhere, and on any device – desktop, laptop or mobile.
2. In-depth security through accurate identification, authentication and authorization.

A Third-party Testing Laboratory Secures its Remote Workforce with Hillstone Networks

3. Access control policies down to the application layer, as well as intelligent detection of potential threats to assure the highest levels of security.
4. Monitoring, logging and reporting for security administrators, with granular visibility and threat analysis to detect potential attacks and misuse.

In addition, the solution would need to provide comprehensive security for the corporate network as well as the data and applications running in the AWS environment, and provide consistency and ease of management across both platforms.

The Solution

After exploring several security offerings, the customer chose the solution from Hillstone Networks consisting of an E-Series next generation firewall (NGFW) to defend the corporate network perimeter and a Hillstone CloudEdge virtual NGFW to protect the AWS cloud services. The team at the lab deployed the physical E-Series NGFW as the office gateway, and CloudEdge as the VPC gateway within their AWS cloud environment.

"The setup is pretty straightforward. With CloudEdge, we can connect our corporate network to our AWS VPC instance, and share the same set of security features as provided on the physical NGFW platform. Aside from accessing corporate resources, we also enable its additional security features including Anti-Virus, Intrusion Prevention and Quality of Service (QoS) to secure our remote access. What's more, we can now see real-time threat attacks captured and displayed on the dashboard," said IT Manager of the lab.

In order to secure data-in-transit for its remote workforce, the customer enabled SSL VPN services on the E-Series NGFW and CloudEdge, and installed Hillstone's VPN client (called Secure Connect VPN) on all employees' home devices for secure access to the corporate network. Hillstone provides a variety of Secure Connect VPN clients that support Windows, Mac, and Linux OSs, as well as Android and iOS for mobile devices, allowing almost any remote device to connect securely and without issue.

"After passing user identity and device authentication, our remote workforce now has secure access to the company's internal network anytime, anywhere, and from virtually any device. We rarely have any downtime and productivity has increased," said the IT manager.

Addressing one of their critical requirements, role-based authentication is one of the most important security features of this solution. The Hillstone solution can interface with a wide variety of authentication servers, such as Active Directory, LDAP, RADIUS and others, to ensure only authorized users and devices can access network assets. In addition, Hillstone Solution includes an option for multifactor authentication via SMS or RSA token.

"We found that a key strength of CloudEdge is its fine-grained control at the user, user-group or role level. We can control which IP addresses or subnets a given user can access, for example," said the IT manager. "This control extends beyond just users, however, to both applications and user behaviors."

Addressing another key requirement for compliance and management, CloudEdge provides the customer a complete monitoring, logging and reporting package for executive briefs and audit purposes. Fine-grained monitoring and alarms – down to the application, device and behavior level – can help pinpoint problem areas. The data is provided in a rich user interface that gives an at-a-glance overview with the ability to drill down for more information and analysis.

The Conclusion

The customer had four key requirements when looking for a security solution to protect its remote workforce, and ultimately, its business. Hillstone delivered on all four and more with a secure remote connection to the corporate network anytime, anywhere with any device. Identity and device authentication and authorization help ensure appropriate access and protect against hacking attempts. The solution delivers in-depth security, especially application-layer access control. Meanwhile, monitoring, logging and reporting have helped the security team with deep visibility and actionable recommendations.

Hillstone NETWORKS

Visit **www.hillstonenet.com** to learn more
or contact Hillstone at **inquiry@hillstonenet.com**