Case Study

Defending the Critical Web Servers and Assets for a Government Agency

Hillstone Network Intrusion Prevention System (NIPS) defends against DDoS attacks, cyberthreats and exploits aimed at a government agency under the Malaysia's Ministry of Primary Industries.

The Challenge

A Data Center Under Constant Threats

The customer is a government agency under the country's Ministry of Primary Industries. The agency's data center hosts servers and systems that serve multiple of divisions under the umbrellas of research and services, as well as other government agencies. Due to its relatively high profile, the agency found itself under the attack radar of hackers and was the subject of frequent DDoS attacks and other cyberthreats and exploits.

Its existing intrusion prevention system (IPS) had reached end of life and would soon lose its eligibility for support. While other security technologies were in place for web application access, given the level of threat activity directed at its data center, the agency's IT team determined that it was critical to deploy a new IPS to help assure security and business continuity.

A New First Line of Perimeter Protection

Like the previous IPS, the new solution would need to provide a first line of perimeter protection for the critical data center infrastructure and balance the workload on the existing web application firewall (WAF) solution. Ideally, the new IPS would require minimal up-front costs and be easy to manage and maintain - all while providing superior visibility and intelligence into advanced threats.

The IT team zeroed in on two possible solutions - the latest model of the existing IPS system, and Hillstone Networks' Network Intrusion Prevention System (NIPS). Almost immediately the team recognized that the newest version of the competing solution would require not one but two separate devices (management and sensor), which added to cost, complexity, and management and maintenance overhead.

Agency's information technology officer said, "Our overall mission is to serve and foster the industry, and as such it is also our responsibility to ensure that our critical network assets are secured in the most efficient and cost-effective way".

Customer Profile

Customer

A government agency under the Malaysia's Ministry of Primary Industries.

Sector

Government

Location

Malaysia

Size

Multiple divisions as well as other government agencies

Challenge

Replace an obsolete product with a new, state-of-the-art IPS to protect critical DC infrastructure

Requirements

- Deliver first-line perimeter protection for the data center
- Provide superior visibility and threat intelligence
- Relieve load on existing WAF through SSL proxy offload
- Minimal up-front cost with easy management and maintenance

Result

An all-in-one IPS solution that delivers superior visibility into network elements as well as advanced threat intelligence to provide comprehensive protection for critical assets.

> “It was crucial for us to find a solution that would help reduce the workload on the WAF, especially in the event of DDoS attacks, and also provide detailed reporting on threat event details. In Hillstone, we believe we have found the best of all worlds – strong protections against threats and attacks with the extensive visibility we need.”
>
> **Agency's information technology officer.**

The Solution

A Managed IPS Solution for Advanced Protection

After a careful review and testing, the agency’s team selected Hillstone NIPS, an all-in-one solution that provides superior visibility and threat intelligence. The solution was deployed as a managed service by local Hillstone partner, Secure Sourced, running in transparent Layer 2 mode. NIPS provides comprehensive protection for agency’s business-critical assets by covering the gamut of potencial threats - including spam, botnet and virus filtering and IP reputation to defend against risky sites. Further, Hillstone’s NIPS adds DDoS prevention capabilities that are crucial to maintaining continous operations and finally, NIPS includes a cloud sandbox and an advanced threat engine to provide defenses beyond those of traditional IPS solutions.

Transparent mode, sometimes called passive network tap mode, provides thorough screening without disrupting normal traffic flows. If in the future the IT team deems it necessary, they can switch to active in-line mode which provides screening as well as immediate blocking of threats.

Importantly, Hillstone’s NIPS goes beyond traditional IPS solutions that understand only network-layer information – by contrast, NIPS is also application-aware. This allows highly accurate threat detection and precision blocking of threats, and results in far fewer false positives while providing enterpise-class protection of the network infrastructures. The agency’s team noted a roughly 10 percent increase in detection of threats that were either new or had never been seen before, indicating a major improvement in the threat detection rate versus the previous IPS.

Easy Visualization, Management & Forensics

NIPS also provides a dynamic, real-time dashboard for easy visualization of network status, with the ability to easily drill down across multiple aggregation that allows forensic investigation of potential threats and anomalies. In addition, the IT team noted that NIPS provides much more in-depth alert details and mechanisms, which greatly improved the speed and accuracy of the team’s alert verification and investigation processes.

The Conclusion

Assuring Resiliency Against Threats

The agency serves an important function for the country's industry by providing research into elements that affect production and profitability, as well as through services to help producers grow their respective businesses. With Hillstone NIPS, the agency helps assure business continuity and resiliency in the face of an ever-changing threat landscape.

Learn more about Hillstone products mentioned in this case study

Hillstone Network Intrusion Prevention System (NIPS) ⇨

Hillstone W-Series Web Application Firewall (WAF) ⇨

Read about Hillstone solutions

Cloud Workload Protection Platform (CWPP) ⇨

Extended Detection & Response (XDR) ⇨

Zero-Trust Network Access (ZTNA) ⇨

Secure SD-WAN ⇨

Micro-segmentation ⇨

Network Detection & Response (NDR) ⇨

Hillstone NETWORKS