



Case Study

Major East Asian Customs Service Leverages Hillstone Twin-Mode to Ensure Business Availability

Hillstone delivers unique capabilities: high reliability, scalability and performance.



Customer Profile

Customer

Customs Agency

Sector

Government

Location

Eastern Asia

Scope

Responsible for customs clearance via air, sea, rail and land; maritime safety; and protection of intellectual property

Size

14 office locations with several hundred employees

Challenges

Modernizing cybersecurity infrastructure in the data center, as well as maintaining quality of service in network traffic and cross-datacenter reliability.

Requirements

- Upgrade from traditional L2 routing to VxLAN network
- Add asymmetric routing for performance and reliability
- Assure reliability and scalability across the data center even for asymmetric traffic
- Provide advanced threat detection, visibility and forensics with centralized management

Result

For this data-centric department, Hillstone Twin-Mode solves the problem of asymmetric L3 traffic and helps assure continuous uptime even during maintenance and application migration.



The Challenges

Assuring Continuous Access to Critical Data

The Customs Agency for a major tourist destination and port city in southeast Asia processes millions of passengers and cargo transits via land, air, rail and sea each year, as well as safeguarding the intellectual property, patents and trademarks of enterprises within and outside of its borders.

Its operations generate an enormous amount of data, which can then be used for correlation, reporting and other purposes; staff also relies on the databases to efficiently and effectively perform their respective job duties.

As a result of the massive volume of data that must be managed, the agency had deployed three distributed data centers: two in active-active high-availability configuration and a third as a disaster recovery resource. However, high availability for the active-active pair was running over a traditional Layer 2 configuration, leading to issues with asymmetric traffic at Layer 3. This in turn caused dropped connections when requests were routed to the incorrect data center for processing.

In addition, the department sought to bolster its cybersecurity defenses through sophisticated next-gen firewalls, and to gain deep visibility across the data center network, improved threat detection, and forensics to protect against breaches. Furthermore, centralized management was a key consideration in order to ease management and maintenance in this fast-paced environment.

The Solutions

Unique Twin-Mode Capability, Breach Prevention and Consolidated Management

After careful research and consideration, the department's IT team selected Hillstone Networks' state-of-the-art A-Series Next Generation Firewalls (NGFWs) with their exclusive Twin-Mode option for the main active-active data centers. In addition, the agency deployed Hillstone's Breach Detection System (BDS) for advanced cybersecurity defenses, forensics and visibility. The solution is rounded out with the virtualized central security and monitoring system (Hillstone vHSM) for ease of configuration and monitoring.

The A-Series NGFWs offer strong performance at the application layer – a crucial need for highly active organizations such as this. In addition, it provides a broad spectrum of defense mechanisms to detect and protect against network attacks and malware. Further, the A-Series features a unified threat and analytics engine that spans all of the NGFW's cybersecurity mechanisms to significantly improve efficiency while subsequently reducing network latency.

Hillstone's A-Series also address one of the most difficult problems of redundant data centers (DCs). While other network devices like routers and load balancers support redundant DC failover, most NGFWs are stateful and therefore utilize session state information to enforce security policies. For example, if a given session that originated on DC A tries to traverse DC B to retrieve data, DC B is unaware of the session and will therefore drop the session – thereby ending it.

This phenomenon is called an asymmetric traffic flow and can occur in multiple scenarios. Hillstone's unique Firewall Twin-Mode solves this challenge by synchronizing firewalls through dedicated data control links. In essence, this creates a single, logical firewall that remains aware of sessions no matter where they may have



originated.

For this bustling customs agency, Hillstone Twin-Mode has made a big improvement in data accessibility. “We’ve noted a dramatic reduction in the number of complaints we receive about data availability,” noted the department’s IT manager. “In addition, we no longer need to apply for a maintenance window for service on the data centers, or for application migration.”

The new NGFWs with Twin-Mode, in active-active high-availability configuration, help assure business continuity and 24/7/365 high reliability across the data centers. In addition, the Hillstone BDS system has added intelligent threat detection and response, as well as comprehensive network breach prevention. Full visibility into real-time threats allow cybersecurity personnel to act promptly to head off potential malicious actors. BDS integrates smoothly with the Hillstone NGFWs, which allows automatic configuration to block future attacks, for example.

And finally, the vHSM consolidates and centralizes management of all Hillstone products into a single, convenient management portal. This in turn helps the agency’s IT team accelerate deployment,

Conclusion

Rock-Solid Availability with Robust Cybersecurity

For this customs department, the Hillstone NGFWs with Twin-Mode, BDS and vHSM have proved to be an unbeatable combination. The challenges of the prior environment, such as asymmetric traffic and the resulting dropped sessions, have been resolved. Further, Twin-Mode and the high-availability (HA) configuration help assure business continuity.

The agency has gained strong cybersecurity defenses both at the perimeter and within and amongst the data centers, as well as streamlined, centralized management for increased efficiency and reduced complexity – all of which combine to support the vital efforts of this customs agency.



We’ve noted a dramatic reduction in the number of complaints we receive about data availability. In addition, we no longer need to apply for a maintenance window for service on the data centers, or for application migration.

IT Manager





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 Breach Detection System \(BDS\) ⇒](#)

[Hillstone Security Management \(HSM\) ⇒](#)



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 \(NDR\) ⇒](#)