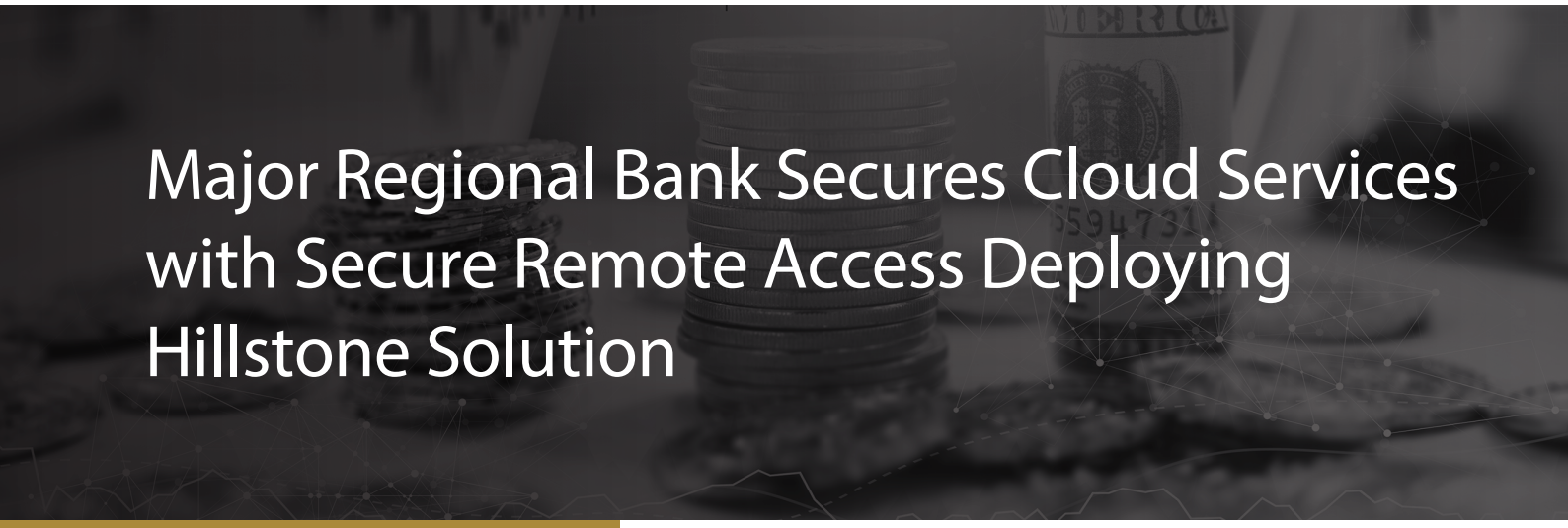
Hillstone NETWORKS



Major Regional Bank Secures Cloud Services with Secure Remote Access Deploying Hillstone Solution

The Customer

Established more than 10 years ago, a major regional bank in Asia Pacific serves both consumers and commercial accounts, with assets totaling more than $15B. It currently operates more than 70 branches with over 1,700 employees. The bank is ranked at the forefront of regional financial institutions.

The Challenge

The financial industry is under strict regulatory compliance requirements. Under these requirements, banks are mandated to build redundant data centers that can provide disaster recovery (DR) for financial and confidential data. This requires accurate data synchronization and communication between data centers, as well as protection against malware and other exploits.

To address DR and ensure business continuity, the bank's data centers, which were originally deployed as main and backup, needed to ensure synchronization of both session and configuration information to further improve reliability. For data integrity, different access rights need to be granted for different workloads; and all internal traffic (East-West) need to be monitored. To maintain data protection, DMZ and production zones have to be segmented in order for maximum protection.

The bank's service systems consist of multiple security zones. The existing data center firewall in their virtual VMware NSX environment no longer met the bank's service needs. Moreover, the backup data center was not secured with a firewall, rendering it non-compliant. It became evident that they urgently needed to do two critical things:

• Upgrade their firewall solutions to address compliance and data protection mandates.

• Purchase high-performance firewalls for perimeter protection and a firewall to protect critical servers in the virtualized data center.

For the 70 branch offices, they lacked a means of securely connecting to corporate network and intranet resources. Employees throughout the organization also needed secure remote access while working from home during the pandemic, as well as in other business-disrupting events.

Major Regional Bank Secures Cloud Services with Secure Remote Access Deploying Hillstone Solution

Given these requirements, the bank initiated a rigorous examination of multiple options to determine the best path forward to meet their needs from a regulatory, compliance, and business operation perspective.

The Solution

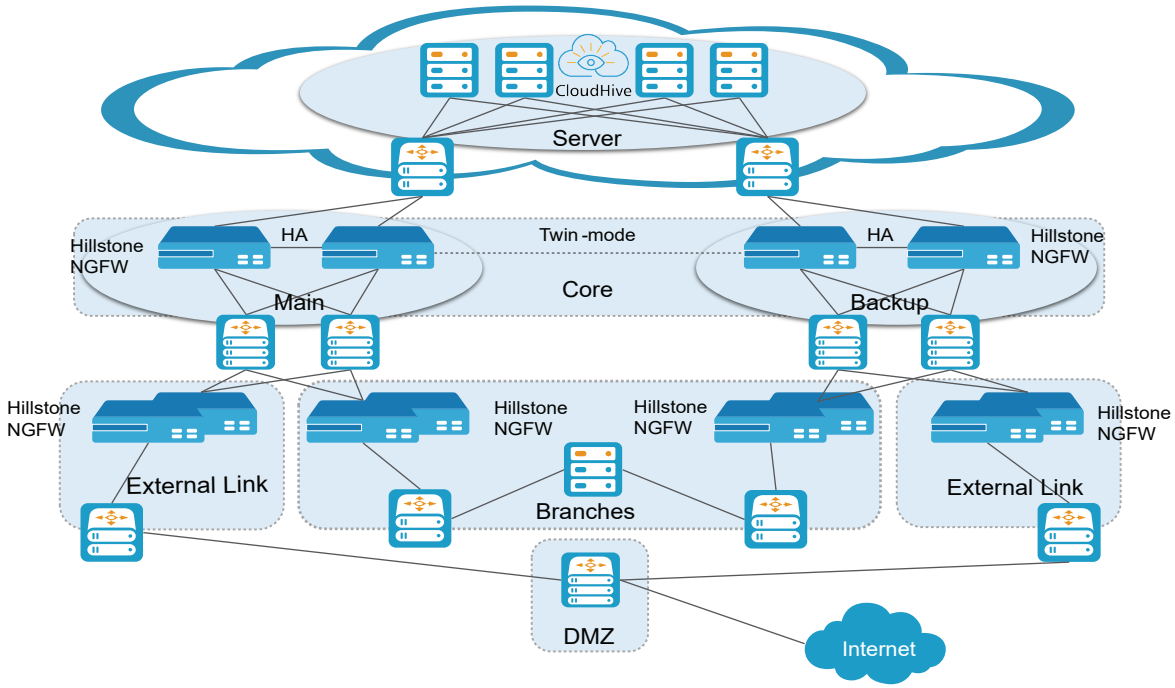
The bank selected Hillstone Networks as a solution for their multiple objectives. The key reasons for their decision include:

• Hillstone's strength in its patent-pending Twin-mode firewall synchronization capability, which delivers 24/7/365 business continuity and disaster recovery without any gaps in data center security.
• Hillstone's micro-segmentation technology, for securing cloud services and workloads
• Robust SSL VPN capabilities in Hillstone's firewall solution for securing remote access

In the first phase of their roll-out, the financial institution deployed more than 100 CPUs of Hillstone CloudHive, in their server zones, and 12 high-end Hillstone E-Series next-generation firewalls (NGFW) in the initial rollout.

The figure below illustrates how CloudHive is deployed in conjunction with five distinct VMware vCenter management domains across the server zones, while the E-Series NGFWs are deployed in the core zone and DMZ of the data centers, all in Twin-mode.

Hillstone's Twin-mode feature links redundant firewall pairs



across data centers to maintain full security for all redundant data center traffic flow. With Hillstone's unique Twin-mode firewall solution, the E-Series firewalls automatically synchronize configuration and session information among the high-availability pairs. For instance, in a virtual environment running VMware, this synchronization ensures uninterrupted service during vMotion between data centers and solves the problem of asymmetric traffic between redundant data centers. Together, the Twin-mode and micro-segmentation technologies can hierarchically protect services in different zones within a virtualized or cloud environment.

By deploying Hillstone CloudHive in their private cloud resource pools, the bank can enable micro-segmentation:

Major Regional Bank Secures Cloud Services with Secure Remote Access Deploying Hillstone Solution

Different business systems in data centers and different security zones within business systems can be segmented and have visibility and monitoring over their traffic. Application access control in different security zones is also ensured throughout the cloud environment. In addition, the high performance and high reliability benefits delivered by CloudHive in the NSX environment easily meets the customer's performance requirements.

For the customer, CloudHive provides comprehensive protection from L2 to L7, including multiple security functions such as antivirus, attack defense (AD), URL filtering and IPS. Deployment at L2 means that it eliminates the need for network configuration changes by the IT team. No root authority or plugin is required, which minimizes any impact on any VM and the VMware ESXi hypervisor.

The IT team at the bank can expand or scale services as needed through CloudHive's fully distributed processing architecture. The IU visualized dashboard monitors application status in the cloud and observes interactions and relationships of their assets in the cloud in real time.

"Hillstone's CloudHive solution solved our problems of poor reliability in our virtualized environment. After the deployment of the NGFWs with Twin-mode feature, the solution has been running stably, delivering excellent experience. The visualized monitoring capabilities give us a more intuitive and comprehensive understanding of east-west traffic and the threat posture of the VMs running in our intranet. Advanced security features such as antivirus and intrusion prevention capabilities inside the cloud are also a greatly benefit for our remote workers," said the bank's IT manager.

For their final requirement of securing their remote workers, the SSL VPN capabilities included in the E-Series NGFWs now allow remote branch workers to quickly, easily and securely connect to corporate resources, driving overall productivity.

The Conclusion

Hillstone CloudHive runs in the VMware NSX environment of the bank's redundant data centers. It perfectly solves the customer's requirements for visibility and control of traffic in a virtualized environment. At the same time, Hillstone CloudHive's Insight function gives the admins overall visibility of interaction and threat status of assets inside their cloud deployment. The L2-L7 protection satisfies the requirements for intrusion protection, antivirus, and application control, and SSL VPN included in the E-Series firewalls provides safe, secure remote access for branch employees and others.

As a bank that has strict regulatory requirements, Hillstone's solution (Twin-mode synchronization, CloudHive securing the virtual data center, and the E-Series' SSL VPN capability) help achieve compliance while improving the cloud operations' resiliency and performance. Since deployment, the solution has met all the client's criteria and kept their business running smoothly and securely.

Hillstone NETWORKS

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