Hillstone NETWORKS

Guarantee Business Continuity

with Hillstone Application Delivery Controller (ADC)

Introduction

In IT, Networking is evolving quickly to meet the demands of organizations as they become increasingly reliant upon data to drive business growth and plan for the future. As reliance upon data and the insights gleaned from it increases, it becomes more imperative to ensure the availability, accessibility and security of the applications and servers, that process and consume that data in mission critical workloads.

Simply adding more memory or additional servers is no longer adequate in addressing the problems that impact user productivity and slow down business responsiveness. The networks of today are highly complex, and often encompass cloud computing, mobile and web-based applications, big data and many other elements.

What is needed is a solution that can:

- Constantly monitor server health and usage, as well as the health of internet access links, and then intelligently route traffic to optimize both accessibility and availability.
- Alert IT staff to potential issues before they ever impact the user experience.
- Navigate the complexity of IPv6 transition with ease and allow SSL-encrypted traffic to be fully inspected by security devices with only marginal impact to data throughput.

This solution is the Hillstone Application Delivery Controller (ADC), a full-featured ADC that offers server load balancing, link load balancing and global server load balancing, as well as a wide variety of other capabilities to address the high availability, accessibility and security needs of modern application delivery.

Hillstone ADC has been deployed in many industries throughout the world, including government, finance, enterprises, service providers, data centers and education, and can flexibly support a wide variety of deployment scenarios. It helps you guarantee business continuity while maintaining a positive and productive user experience.

The Challenges

An excellent user access experience is critical to employee (and thus, business) productivity. The key contributors to a poor user access experience are slow access and unstable services. Slow access can be characterized by slow page loading, slow submission of business inputs and data, and slow data queries. Unstable services are typically evidenced by the frequent inaccessibility of servers or applications, sudden interruptions of access, and accidental data loss.

These challenges are primarily caused by issues either on the server side, or on external links to the internet. Server-side issues could be caused by inadequate server performance, by slow detection of faults via the servers, or simply by bottlenecks in database access performance. External link issues can be comprised of slow cross-operator access, poor link stability and/or uneven distribution of traffic across multiple links from the same or different providers. It's important to note that these challenges can arise in local networks and servers as well as in geographically distributed servers and networks.

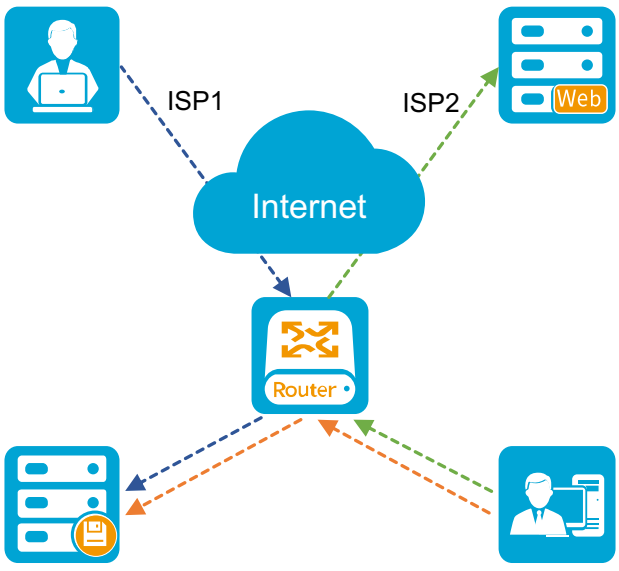

Figure 1: Typical server-side and external link challenges

Together, these issues can heavily impact the ability to scale as needed, and thus impede business growth.

However, there are other challenges associated with networking and data traffic in general that can affect the security and performance of servers and applications. For example, the majority of traffic traversing the internet is now encrypted via SSL, and, unfortunately, attackers have learned to conceal malicious payloads inside encrypted traffic. To fully inspect SSL traffic, it must therefore be decrypted – but decryption is extremely processor-intensive. Some security components may use software-only SSL processing, which is typically exceedingly slow and inefficient, while others lack the ability to process SSL traffic at all, and therefore bypass it. And, given the ever-changing nature of threats and attacks, a layered approach to data security can provide a multiplier effect that provides even stronger and more effective security.

It is also common for applications to indiscriminately download data to users' devices repeatedly, even though that same data was downloaded just minutes, hours or days prior. This adds unnecessary traffic to the network, potentially slowing response times and performance.

Another challenge that is becoming increasingly common is the use of IPv6 by service providers and web-based applications. IPv6 translation is needed to assure communications between IPv4 and IPv6-based resources. And finally, when multiple ISPs or links are in use, poor network utilization efficiency can affect the user experience, as well.

The Solution: The Hillstone Application Delivery Controller

Hillstone application delivery controllers are a new generation of enterprise-class solutions that optimize the delivery of applications and associated data. Available as physical or virtual appliances, and compatible with popular cloud platforms, the Hillstone ADC can deliver a marked improvement in the user access experience, contributing to overall operational efficiency and productivity.

The Hillstone ADC offers a full range of load balancing capabilities, including server load balancing (SLB), link load balancing (LLB) and global server load balancing (GSLB). In addition, the Hillstone ADC includes innovative features that complement the core load balancing functions and amplify their efficacy.

The Hillstone ADC also provides first-level security through access control, URL filtering, application bandwidth usage management and other techniques. Furthermore, identification of users, applications, content, location and other factors allows highly flexible and customizable management of security policies. The following sections provide a more in-depth discussion of these and other capabilities.

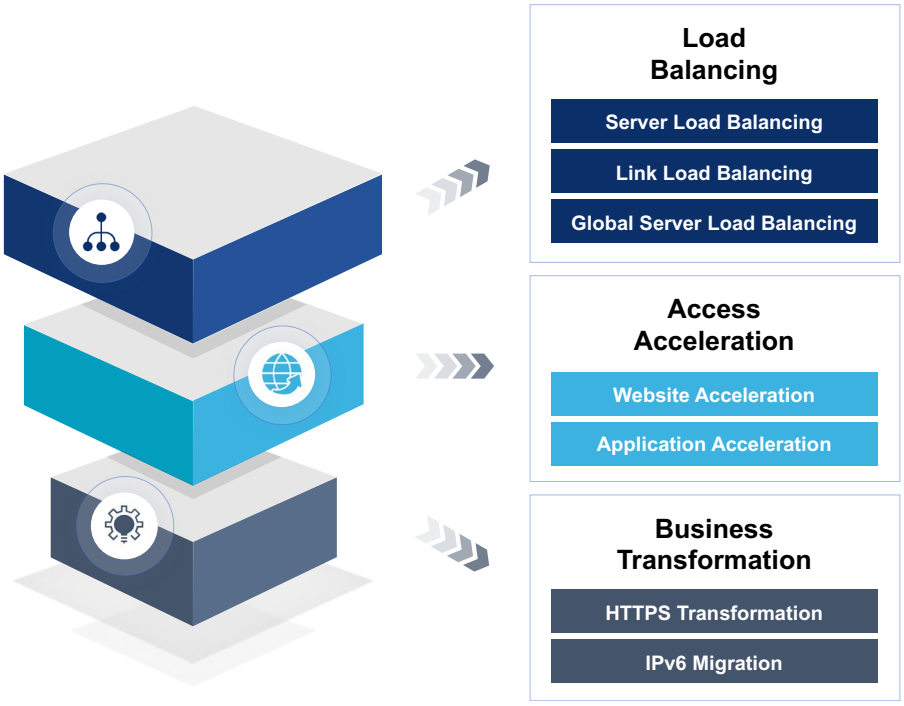

Figure 2: Hillstone ADC solves productivity and access challenges

Server Load Balancing (SLB)

Server load balancing is a key technology for improving the user access experience. At its essence, SLB simply distributes network traffic over multiple application and data servers to optimize their performance, assure availability and decrease response times. SLB thus optimizes the general processing capability of the target servers, which greatly improves the overall user access experience.

The Hillstone ADC goes beyond simple Layer 4 to layer 7 SLB capability, however, by offering more than 20 types of load balancing algorithms, such as persistent or non-persistent, SNMP-based, priority-based and others. Each of these algorithm types then contain multiple embedded algorithms like round robin, hash, least connections and others, as well as weighting values, all of which allow extremely fine-grained tuning of the SLB strategy to achieve optimum performance. In addition, maximum connection thresholds can be set for each server to avoid an overload situation.

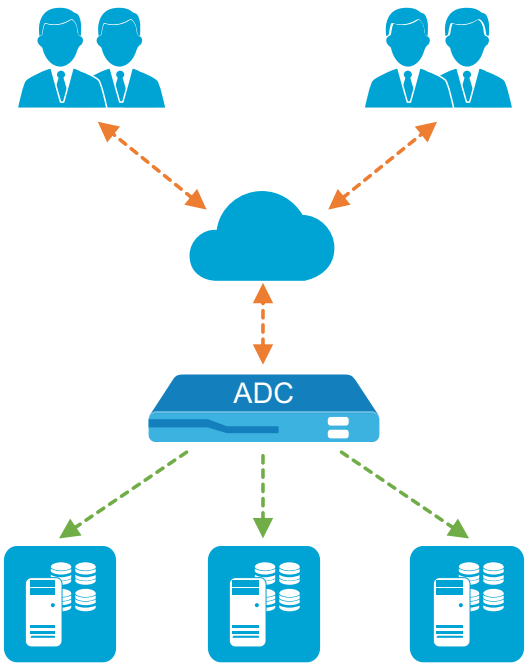

Figure 3: Server load balancing scenario

The Hillstone ADC also provides intelligent application identification based on behaviors, characteristics and related information, which allows IT staff to fine-tune performance and throughput to further improve the user access experience.

Session persistence is an important component of SLB, in that sessions are preserved even if a server fails. In addition, it allows any server to process requests for any number of sessions. The Hillstone ADC supports predefined and custom health checks like ICMP, TCP, UDP, HTTP/S, SMTP, POP3, third-party objects and others. Hillstone ADCs also support health checks for email exchange and RADIUS protocols. In addition, Hillstone ADC supports FastHTTP, HTTP2.0 and Websocket for optimum performance and compatibility.

Hillstone SLB can support business continuity both within the data center and by load balancing in GSLB mode to a dedicated disaster recovery data center, or to other geographically distributed data centers. It also supports high availability of servers, allowing servers to be taken offline for maintenance or for new servers to be added dynamically to the SLB pool with little or no impact to business operations.

Link Load Balancing (LLB)

An often-overlooked part of the performance equation, LLB helps assure the usage optimization of external links. Hillstone ADC supports a unique link selection control algorithm that detects connectivity, utilization, packet loss, jitter and delay in real time, then adapts on the fly to assure the highest quality performance across all links. In addition, it supports DNS diversion and link aggregation to further optimize link performance.

The Hillstone ADC utilizes an intelligent closed loop logic to determine the optimal route at a given time. This technique helps avoid slow cross-ISP access, unbalanced utilization of links, poor link stability and other problems. Multiple LLB options are available, including ECMP, application routing, dynamic link switching and ISP routing.

The two most common deployment scenarios for Hillstone LLB are dynamic link switching and application-based routing. In dynamic link switching, typically multiple links from multiple internet connectivity providers are in use for redundancy and business continuity. Hillstone LLB utilizes a patented passive detection technology to monitor the quality and bandwidth utilization of the links and adjust traffic flows to make use of the best quality links for improved performance and user experience. Thus, poorer-quality links are bypassed, while high-quality links are given preference.

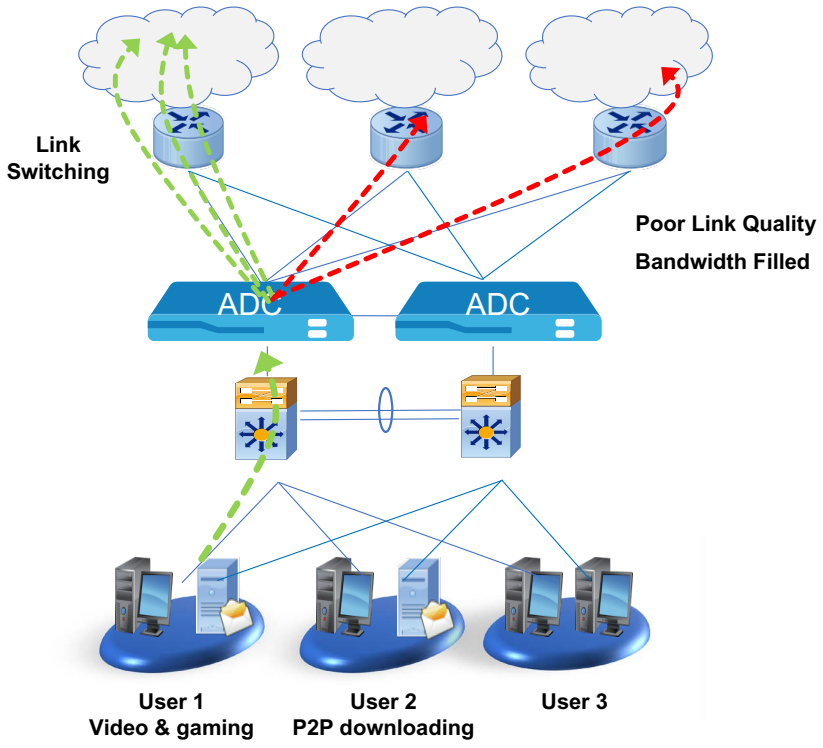

Figure 4: Link load balancing scenario – dynamic link switching

Application-based routing leverages the Hillstone ADC's ability to identify thousands of different applications based on their characteristics and other factors. This capability allows administrators to specify different applications (like video streaming, peer-to-peer downloading and others) to be routed to different internet links. For example, in a higher education deployment, students engaged in p2p downloading could be routed to lower-quality links while those who are using the internet for legitimate academic work are routed to higher quality links.

Hillstone link load balancing thus gives administrators a great degree of control in optimizing the use of internet links both for general traffic (through dynamic link switching) and for specific traffic (using application-based routing).

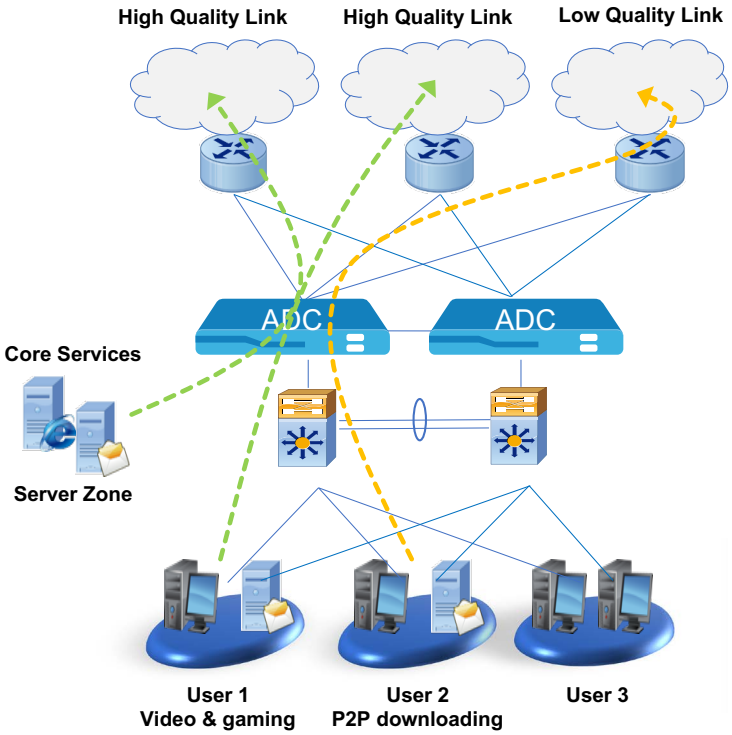

Figure 5: Link load balancing scenario – application-based routing

Global Server Load Balancing (GSLB)

Global Server Load Balancing is yet another strategy to improve productivity and user access for geographically distributed organizations. When applications are deployed across multiple data centers or clouds, GSLB allows users to be routed to the appropriate server no matter their location, thus providing a more stable and higher performance user access experience.

Hillstone ADC uses a comprehensive health check system to monitor all servers regardless of physical location, and route user traffic based on the status and overall health of the application servers as well as the data centers or clouds themselves. If, for example, a data center or application is experiencing an outage or is otherwise faulty, user access requests are then routed to healthy data centers, clouds, servers or backup data centers, and administrators will be notified of the issue. In addition, server traffic load and bandwidth utilization are also factored into the load balancing equation to further define and refine performance and throughput.

Hillstone ADC also includes the ability to act as an enterprise-class DNS server. Supporting A, AAAA, NS, CNAME and other DNS repositories, the Hillstone ADC provides seamless and efficient processing, for example adding an AAAA record to IPv6 traffic. Hillstone's SmartDNS technology can differentiate responses based on client location and other factors for fine-grained and customizable routing across geographically distributed data centers. GSLB can also assist in disaster recovery and business continuity by automatically and intelligently routing traffic to healthy servers and data centers. Further, it helps in maintaining the stability of user access while improving resource utilization across all data centers – thus helping servers run within their respective power bands.

Figure 6: Hillstone's GSLB with SmartDNS intelligently routes traffic among multiple data centers.

Website and Application Acceleration

Business applications can be inefficient in the transmission of data over the network, which results in excessive traffic that can impact the overall performance and throughput. For example, the same images, html and other data might be sent multiple times to the same end-user device even though it was downloaded just minutes or hours prior.

The Hillstone ADC utilizes multiple strategies to minimize and optimize transfer of application traffic. HTTP caching stores multiple file types (html, doc, xls, ppt, pdf and others) on the ADC so that it is instantly available without transiting the network. HTTP compression of Office and web files similarly improves efficiency. And TCP connection multiplexing combines multiple data streams into just one physical connection to improve link utilization and efficiency.

IPv6 Transformation

IPv6 is increasingly used not only in service-provider networks, but by other web and cloud-based resources as well and it is very often required by regulations. However, existing network technologies may not be capable of supporting IPv6 and upgrading the entire network stack would be both expensive and time-consuming.

The Hillstone ADC can help provide IPv6 services with no additional investment or changes required to the existing systems, and with easy deployment. It supports full IPv6 business transformation through a number of strategies and mechanisms. Intelligent link processing technology allows application-layer rewriting, which automatically replaces external IPv6 links and images with IPv4 equivalents.

Traceability and forensics are also important, and the Hillstone ADC provides application-layer log tracing with local database storage and export for security audits. An IPv6 homepage notice provides a perception of the transformation to end-users.

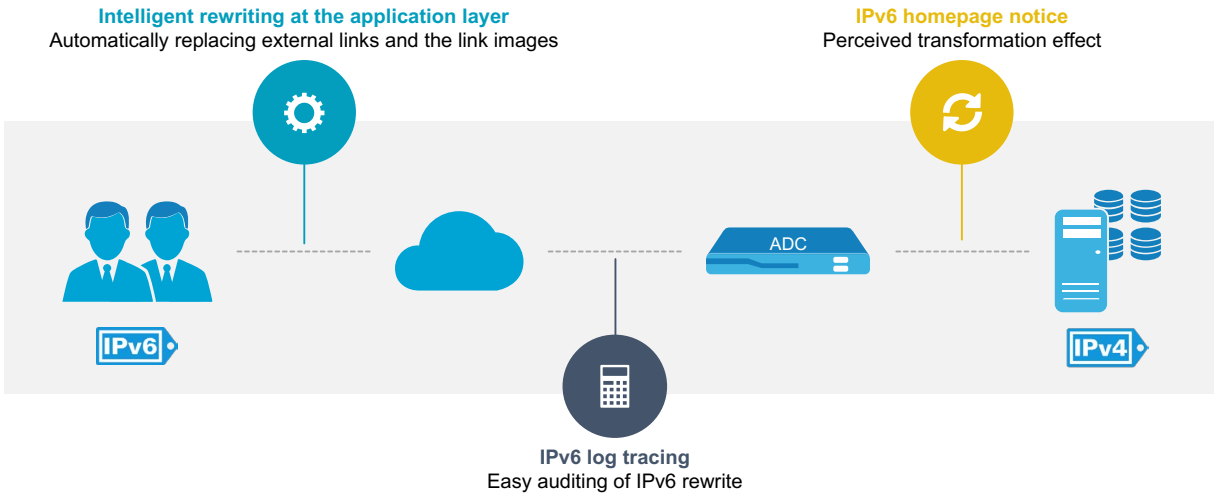

Figure 7: IPv6 Transformation

SSL Inspection

It is estimated that more than 90% of internet traffic is now encrypted via SSL/TLS. However as mentioned previously, many older security devices lack the ability to decrypt and fully inspect SSL traffic. Newer security solutions often use software-based SSL processing, which can be exceedingly slow and thus result in a significant amount of traffic being bypassed in order to maintain performance. In addition, the latest TLS ciphers are about 4X more compute-intensive that the previous 1024-bit ciphers.

Hillstone's hardware-based SSL processing resources offer significant performance advantages, up to 5X that of software-based processing. Hillstone's virtual ADCs utilize software-based SSL that leverages the Hillstone 64-bit parallel processing StoneOS security kernel. By offloading the processor-intensive SSL decryption and re-encryption, the Hillstone ADC significantly improves both performance of servers and other security devices and thoroughness of traffic inspection for improved overall security.

Both options utilize an SSL proxy that is completely transparent to users and to other devices to which traffic is mirrored in plaintext for inspection by sBDS, NIPS, etc. By utilizing Hillstone's SSL inspection capabilities, all traffic, both encrypted and unencrypted, can be fully visualized and inspected for in-depth security protection.

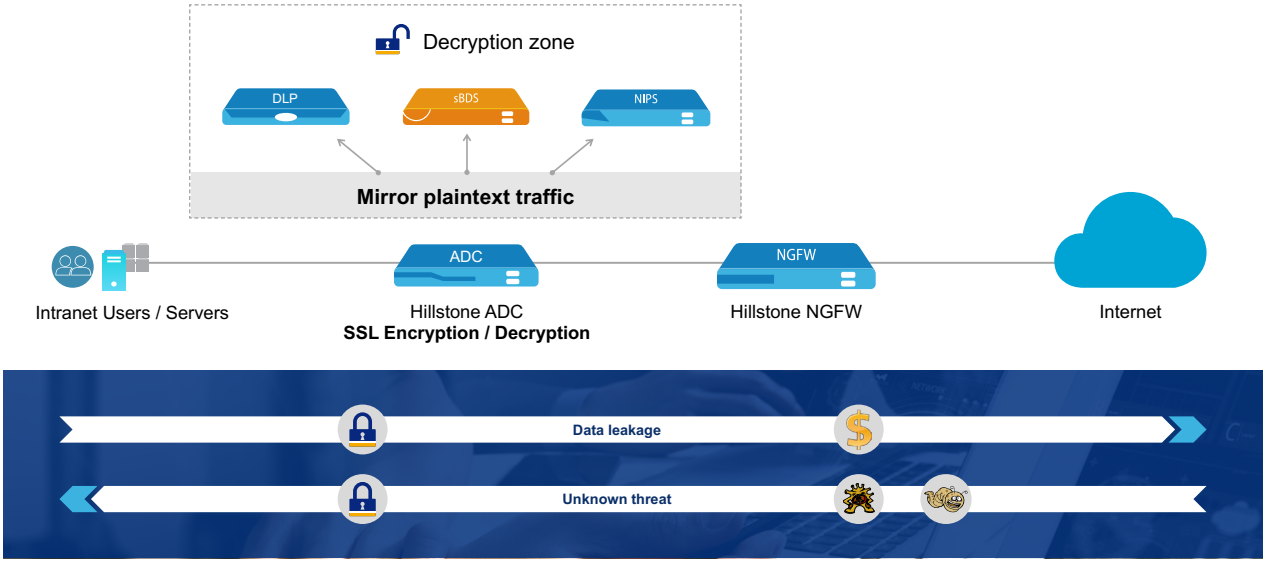

Figure 8: SSL Inspection

End-to-End Secure Application Delivery

In light of increasing cyberattacks and other threats, a strong security strategy is critical in protecting data and servers. In typical deployments, ADCs serve in a unique role at the network edge with visibility into all inbound and outbound traffic. The Hillstone ADC delivers deep detection and analysis of all network traffic for a comprehensive understanding of behaviors and patterns, as well as network visualization. For example, Hillstone ADC can identify applications, content, users, geography and other factors which in turn facilitates highly flexible security management and control. The Hillstone ADC offers other built-in security capabilities such as secure access control, application bandwidth management and URL filtering that add additional layers of security and control.

Hillstone Networks offers a wide variety of security products such as next-gen firewall, network intrusion prevention system and cloud micro-segmentation solution, among others, that can complement and interwork with the Hillstone ADC to provide end-to-end security from the network access to data centers to the cloud.

Hillstone NGFW has been recognized by Gartner six years in a row in its Magic Quadrant for Network Firewalls. This recognition is a testament to the innovation in technology and market penetration with Hillstone's solution portfolio. The Hillstone Networks Intrusion Prevention System, or NIPS, provides unparalleled threat protection without compromising performance. CloudHive is a micro-segmentation solution for virtualized data centers that stops lateral attacks between VMs. The Hillstone Server Breach Detection System (sBDS) is ideal for detecting unknown or zero-day attacks to protect against leaks and theft of data.

Rounding out the Hillstone portfolio are security management technologies including CloudView, a cloud-based security management and analytics platform (SaaS); Hillstone Security Management Platform (HSM), a centralized security management, configuration and monitoring solution; and the Hillstone Security Audit Platform, or HSA, which provides centralized log retention and high-speed retrieval.

By combining the built-in security and visibility capabilities of the Hillstone ADC with the robust security and management capabilities of other Hillstone products, IT managers can be assured of end-to-end secure application delivery that provides the highest quality, secured user experience.

Summary

In summary, the network environments of today are highly complex, and it is critical to address the productivity and access challenges that can impede day-to-day operations and business growth. Organizations are increasingly reliant on data and applications, and thus the high availability, accessibility and security of applications and servers are of critical importance. Organizations need a solution that can address these issues as well as the challenges of securing SSL-encrypted traffic and the complexity of IPv6 transformation.

The Hillstone Application Delivery Controller provides a comprehensive suite of load balancing and application acceleration features as well as important security capabilities, SSL decryption to allow full inspection of encrypted traffic, IPv6 and HTTPS transformation and much more.

The Hillstone Application Delivery Controller improves system availability through comprehensive load balancing and a variety of health checks. By thus improving server and bandwidth efficiency, as well as by optimizing web and application performance, the Hillstone ADC delivers the best user access experience to support user productivity and business growth.

In addition, the Hillstone ADC offers effortless IPv6 migration. High-performance SSL offloading allows full inspection of SSL-encrypted traffic by other security devices in the network. And importantly, the Hillstone ADC provides end-to-end secure application delivery to protect against ever-increasing attacks and threats.

Hillstone NETWORKS