SOLUTION BRIEF

Strengthen Security and Reduce Risk of Downtime

Fail-Safe Inspection of Live Network Traffic

Prevent outages of inline security appliances from escalating into costly downtime.

Solution

You can safely inspect live network traffic and strengthen your security defenses by:

- Installing an external bypass in front of security devices deployed inline
- Using a network packet broker (NPB) to aggregate the traffic you send to security appliances
- Using device redundancy and automatic failover to ensure maximum uptime

According to Ponemon Institute, cybercrime represents the fastest growing cause of data center outages, at 22 percent of all outages in the latest study[1].

1 Ponemon Institute, Cost of Data Center Outages, January 2016

Case In Point

An inline Security Fabric™ solution keeps network traffic moving, even during unexpected software or hardware failures

Network engineers and operations center staff can be justifiably concerned about the impact of security appliances on network and application performance and business processes. But, there are easy and cost-efficient ways to protect the network from disruptions due to traffic congestion, configuration errors, or the unexpected loss of power to a security device. Rather than placing security appliances directly inline on the live network, they can be deployed as part of a Security Fabric using an external bypass switch and a network packet broker to give you greater control over the process of live traffic inspection. A Security Fabric can move traffic around any appliance that stops responding to ensure network availability and maintain service levels, while your security appliances inspect both incoming and outgoing traffic for suspicious or irregular behavior.

Inline security monitoring involves three essential functions (see Figure 1): access to traffic moving across both physical and virtual network links; control and management of traffic to extract necessary data; and monitoring of traffic to maintain security and optimize performance. Once established, a Security Fabric serves both inline inspection of live network traffic, as well as out-of-band analysis used to identify multi-stage cyberattacks that are executed in phases to avoid detection by inline tools.

KEYSIGHT TECHNOLOGIES

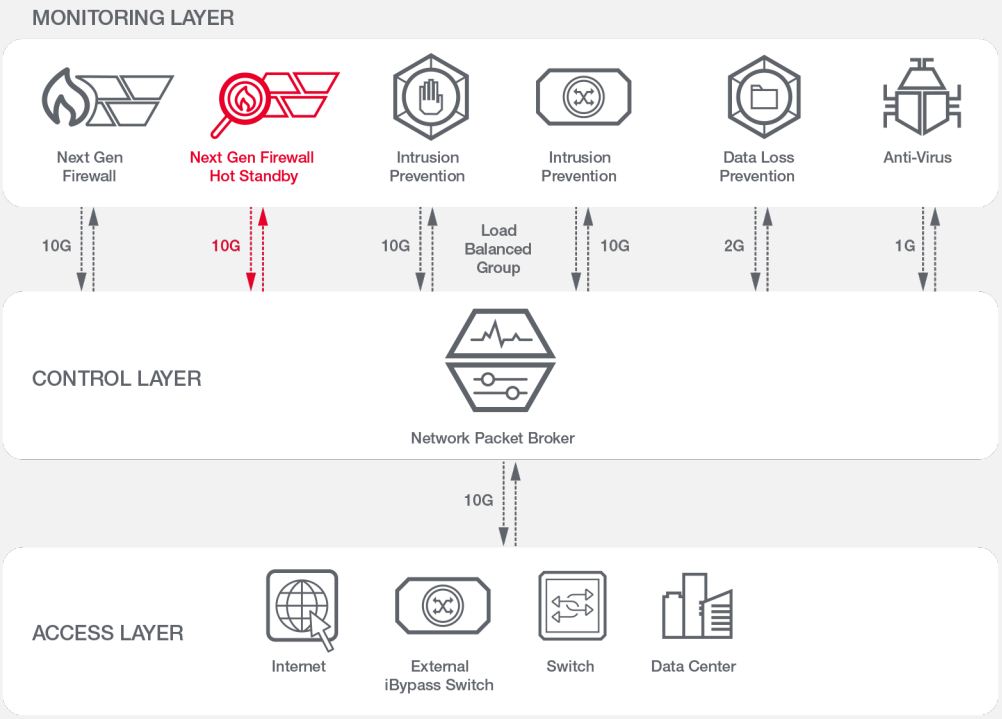

Figure 1. Inline Security Monitoring. The basic architecture for safe inline security establishes access directly on the live network link, passes traffic to a control layer for packet grooming and then delivers the appropriate data to the security appliances.

Bypass Technology. One key function of the Security Fabric is to automatically and quickly route live traffic around any security device that stops functioning to avoid impacting network availability. This is done by installing a bypass switch on the live network in front of each security device to continuously verify the device's ability to process network traffic. While many next generation firewalls (NGFWs) and intrusion prevention systems (IPSs) are shipped with an embedded bypass function, Keysight recommends using a high-performance external bypass switch with a micro-second response time to achieve more flexibility and control. With an external bypass, you can proactively and temporarily take any security device out of service for a software or hardware upgrade or for troubleshooting without impacting the network. Keysight external bypass switches also provide an alternative traffic path, so you can automatically send traffic to an alternate device if the first one stops responding. This additional feature gives you more options when planning a strategy to increase resiliency.

Bypass switches with a micro-second response time ensure traffic is immediately routed around any outage.

Packet Broker Control. A second benefit of a Security Fabric is the ability to let you choose the traffic each security device processes to make better use of its capacity. This is done using a high-performance NPB, which aggregates traffic from across multiple network links, and delivers the data appropriate for each device. For example, traffic that is not transactional in nature, like Netflix video

traffic, can be passed around an IPS focused on identifying vulnerability exploits. This can substantially reduce the capacity required and save an organization from having to upgrade its IPS before it is really needed. An NPB, therefore, increases efficiency by streamlining security inspection and lowering the risk of tool congestion, which can lead to tool failure. NPBs can also be used to load balance among multiple instances of the same tool to further reduce the risk of oversubscription, particularly in environments with quickly expanding network volume and bursts of seasonal activity.

Security Fabric Resiliency. If you do not already have a Security Fabric in place, you may be wondering how the addition of an external bypass and NPB will affect the overall resiliency of network security. Keysight's external bypass is a simple switch and the mean time between failures (MTBF) for this type of device is very high—generally four to five times the MTBF of security appliance or filtering device. This is much better than the MTBF when a bypass is embedded in a security appliance or a network visibility controller (another vendor's version of an NPB). Ixia bypasses offer a secondary path with automatic failover, so you do not have to worry about a failure creating a network outage.

Keysight NPBs are uniquely capable of being configured for high availability in active–active mode. This means both devices are actively sharing the workload in normal operations and maintain complete synchronization. In the event that one Keysight NPB experiences an outage or needs to be taken offline for maintenance, the other NPB immediately begins receiving all traffic, with no delay required to bring up the second device and verify it is ready to receive traffic.

Related Information. Find out more about building a high-availability security architecture with Keysight solutions by downloading the solution brief "Evaluating Inline Security Fabric: Key Considerations".

About Keysight

Keysight delivers a powerful combination of innovative solutions and trusted insight to support network and security infrastructures from concept to operation. Whether you are preparing a product for launch, deploying a service or application, or managing performance in operation, we offer an extensive array of solutions in testing, visibility, and security—all in one place.

Our solutions are used worldwide to validate network functions, test the integrity of security infrastructures, and deliver an end-to-end view of the network. The result: stronger applications, better performance, increased security resilience, happier customers, and maximum ROI.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES