WHITE PAPER

Deploying an Inline Security Architecture: Key Considerations

Introduction

The key to successful inline security monitoring is to enable traffic inspection and detection without impacting network and application availability. If one of your security tools becomes congested or fails, you need to keep traffic moving, continue monitoring, and prevent a network or application outage. Some organizations deploy their inline security appliances behind the firewall in a serial configuration. With this design, if an appliance becomes congested or fails, traffic stops. Redundant network paths can help avoid this, but they require twice the number of tools. Ensuring both paths can handle the full volume of traffic is expensive and leaves tools on the inactive path underutilized during normal operations.

To address these issues, many organizations are deploying an underlying security architecture that can ensure failsafe operation of key security appliances and solutions, and also help these solutions operate more efficiently. This paper describes key functions of a high-performing security architecture —one that protects network availability and ensures continued inspection of everything crossing your network.

Your security architecture should enable failsafe deployment and efficent operation of security tools.

KEYSIGHT TECHNOLOGIES

Deploying bypass switches and network packet brokers together in your security architecture enables untrusted traffic from the internet (in red) to be passed by the bypass switch to an NPB which aggregates, and load balances the traffic across the security tools and solutions you use to monitor for threats and attacks. After inspection is complete, the now trusted traffic (in green) passes into the enterprise and on to its intended destination.

The rest of this paper will describe the features and functions of a top-performing security architecture, to help you build the best foundation for protecting your enterprise.

Function of a High Performing Security Architecture

The goal of creating an inline security architecture is to enable adequate security inspection at maximum efficiency while adding only minimal latency to your network. This is achieved by creating an additional layer of control between live traffic and your monitoring tools. This control layer becomes an essential element of your overall security architecture with the ability to increase accuracy, efficiency, and cost-effectiveness in the following areas.

Maintain Network Availability

A well-designed security architecture strengthens security, but does not allow security monitoring to slow or disrupt network response times. The goal is to allow you to proactively take action before either of these events occurs.

Automatic Failover

Security vendors sometimes embed bypass functionality inside of a security tool and label it failsafe. The claim is true in the sense that, if the tool stops responding, the internal bypass will route traffic around the tool and protect network availability. A separate and external bypass device, however, can also protect the network if you need to temporarily take the tool out of service for software or hardware upgrades, or for troubleshooting. Using an external bypass in front of a security tool separates it completely from the flow of live traffic, so you can perform tool maintenance or any operational task, without having to wait for a scheduled maintenance window. The external bypass continues passing traffic along—even without a tool attached. This improves both network resilience and overall security monitoring, since tools can be maintained as quickly and frequently as needed.

An additional advantage is that the reliability of a simple external bypass switch is much greater than that of sophisticated security tools with embedded bypasses. The general rule is that the more complex the tool, the shorter the mean time between failure (MTBF), and the greater the risk of failure to the entire system. Using an external bypass switch enables you to maximize both network protection and traffic inspection.

Security Architecture: Key Components

External Bypass Switch

Protects network availability by routing traffic around any inline monitoring solution that is not responding.

Network Packet Broker

Aggregates traffic from multiple points across network and passes traffic to your security solutions.

Nanosecond heartbeat packets

Bypass switches send very small heartbeat packets on a regular cadence to your tools to confirm their ability to respond. If a response is not received, the bypass can be configured to fail “open,” and traffic will flow on to the next device. The key characteristic of the bypass is the speed at which it can detect an issue and redirect traffic. You want this to happen as fast as possible to maintain network responsiveness. While heartbeats are common in many devices, solutions where the heartbeat packets originate in the hardware, rather than in software, can be sent at very high frequency—one per nanosecond. This enables the bypass to detect the failure instantaneously and react accordingly.

Another feature to look for in bypass switches is whether they continue to send heartbeat packets even after a tool stops responding. Bypasses with this feature will know very quickly when the tool comes back online and can resume routing traffic through the tool. This self-healing feature enables fast and automatic recovery when tools recover and limits the impact of tool outages.

You want your bypass to function at the fastest speed possible, to maintain network responsiveness.

Traffic flow monitoring

The ability to collect data on traffic moving through the bypass is another distinguishing characteristic of top-performing solutions. Some bypass switches keep track of traffic patterns in both the uplink and downlink directions and use this information for reporting. The data, known as bi-directional utilization and peak traffic indicators, allows administrators to identify possible network or application anomalies before there is a network outage. Another feature to look for is the ability to integrate this data into your existing management tools to streamline network management.

Increase Monitoring Efficiency

Monitoring for security, compliance, and performance will be more efficient if you can provide each tool with all of the data it needs and nothing it doesn't. A security architecture can support this process by gathering traffic from across your network and eliminating any traffic that is irrelevant to each tool, thus reducing the volume of packets being processed and the risk of tool congestion leading to tool failure.

Traffic aggregation

Modern network architecture provides multiple paths through the network to increase network reliability. This creates a challenge for effective monitoring. Security tools require all data from a session to perform an accurate analysis. How can you ensure your tools get all the relevant data they need? A security architecture using a powerful packet processing engine can address this need by aggregating traffic from multiple links, essentially stitching it together, to provide a more complete view to your monitoring tools and improve inspection and detection (See Figure 1.) A network packet broker (NPB) serves this function and is also able to route to multiple tools for concurrent analysis. This ability eliminates tool contention, which can force organizations to choose between two different types of inspection or suffer slower response times to allow for sequential processing.

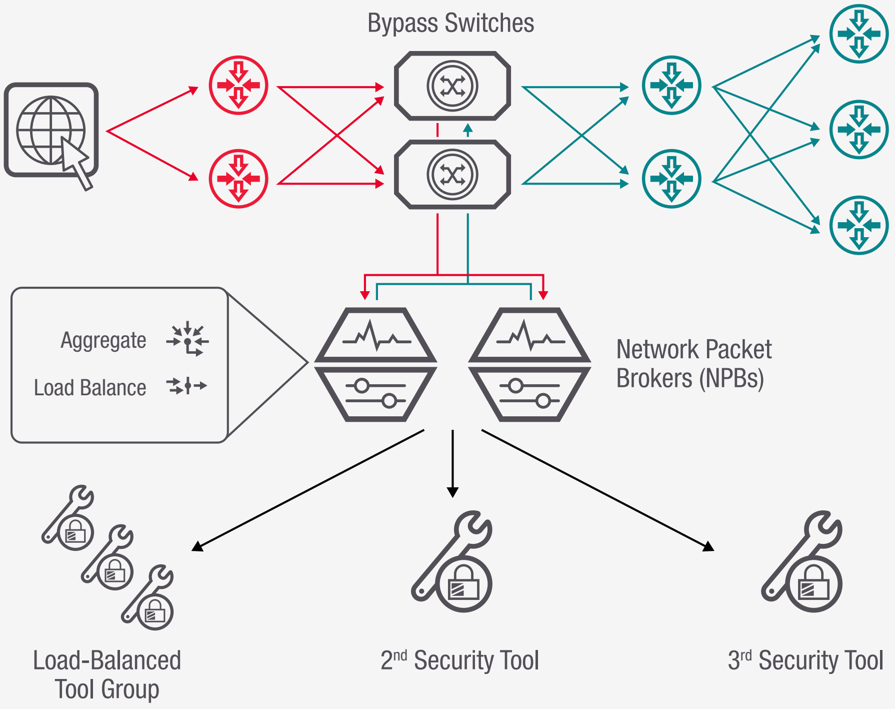

Figure 1. Components of an inline security architecture

Data conditioning

Using advanced security tools to sort through large volumes of traffic and find packets of interest is a waste of an expensive tool's processing power. Some tools are especially sensitive to being "oversubscribed" and will noticeably slow traffic or begin dropping packets randomly if flow exceeds their processing capability. A security architecture with application intelligence—the ability to see packet details—lets you filter packets based on different criteria and forward only those relevant to a particular tool's purpose.

When evaluating packet processors to function as the engine of your security architecture, look for data conditioning features such as removal of duplicate packets, trimming of packet headers, and stripping of unnecessary packet data. The ability to filter packets based on application layer details will be particularly useful, as well as the ability to easily create user-defined filters.

While some monitoring tools are capable of handling some of these tasks, many tools do not have these capabilities. And even when they do, these are resource-intensive functions. Offloading these tasks to a feature-rich NPB can cut the load on your monitoring tools by 50% or more. Reducing the workload on your tools enables more efficient processing and lengthens their service life. Some packet brokers allow the import and export of filtering definitions, increasing the speed of configuration in new network links or data centers.

Load balancing

Ideally, your tools should be operating at no more than 80% of their rated capacity, so intermittent data surges or microbursts do not overwhelm their ports and cause packet loss. This threshold can be difficult to maintain. Top-performing NPBs use load balancing to sense and relieve overloaded monitoring tools by distributing traffic across multiple devices. The ability to establish multiple load balancing groups with and traffic allocation rules is a powerful feature. Look for solutions with the ability to keep session data together for more accurate analysis.

Load balancing also enables upgrades and capacity scaling to be performed with no impact to either network availability or security monitoring. Assuming sufficient capacity is available, you can remove a device from active processing, and the load balancing feature will automatically allocate traffic to the remaining devices with no disruption in service. When a device is added or brought back online, the load balancer automatically spreads the traffic across all active devices to achieve maximum efficiency.

Use your packet processor to create load balancing rules that keep your solutions from becoming overloaded.

Speed of traffic processing

For inline monitoring, the speed at which your network packet broker can aggregate and pass packets through intrusion prevention, and other inline solutions is particularly important because overall processing time adds to application latency. The faster an NPB can operate, the less impact there will be on the user experience.

A hardware-based solution using field programmable gate arrays (FPGAs) will offer significant benefits over software-based solutions, and enable full line-rate processing with zero packet loss. This means you don't have to worry about the NPB dropping packets and providing incomplete data to your security solutions. With full visibility, your security solutions will have the data they need to keep your defenses strong.

Intuitive drag-and-drop controls

Because maintaining configurations, connections, and filter definitions can be complex, be sure to evaluate the management interface of the solution you select for packet processing. Well-designed interfaces provide a consolidated view and a single managerial access point across the entire architecture. A graphical drag-and-drop interface is the easiest to use and allows out-of-the-box deployment with no special training or preparation. Configurations for traffic filtering, flow management, and load balancing can be easily replicated across multiple network paths, or even between data centers, to get security up and running quickly. Software and hardware updates can be performed quickly and efficiently across all common devices. Being able to initiate tasks remotely from a web browser with drag-and-drop simplicity will greatly reduce the time you spend on security administration and configuration errors.

Security Resilience

Security infrastructure is under intense pressure as traffic volumes soar, applications proliferate, and users demand faster response times. New compliance regulations may require enhanced security measures. A security breach can have a devastating impact on an organization. As a result, many are demanding high availability for their security infrastructure, as they do for their core network infrastructure. Even with a limited budget, you have options for strengthening your overall security posture and increasing the amount of traffic being inspected. A security architecture built with modular external bypass switches and powerful NPBs lets you incrementally increase resiliency over time to achieve very high uptime for security monitoring.

Active-active configurability

With redundancy of the external bypass switches, NPBs, and security monitoring solutions, your security architecture can be configured with alternative monitoring paths that ensure traffic inspection will survive the outage of any device (See Figure 2.)

With NPBs that can be configured for concurrent processing with complete synchronicity, known as active-active configuration, failover is automatic. The NPBs work together to ensure each security tool receives a full set of traffic, even if transmitted on two different links, and coordinate load balancing. Adding other tools requires configuring only one NPB, because it shares logic with its peer. Designs of this type provide marked improvement in throughput during normal operations, since both NPBs are actively processing traffic. And if one NPB goes down, the synchronous configuration ensures the other NPB can take over seamlessly with no lost packets. With a fully redundant security architecture, you can maximize security monitoring while protecting the network for a well-balanced approach. Not all NPBs can be configured in active-active mode, so be sure to look for this feature if full failover is desired for your environment.

With active-active configuration, your security architecture can provide nearly instant failover, with no lost packets.

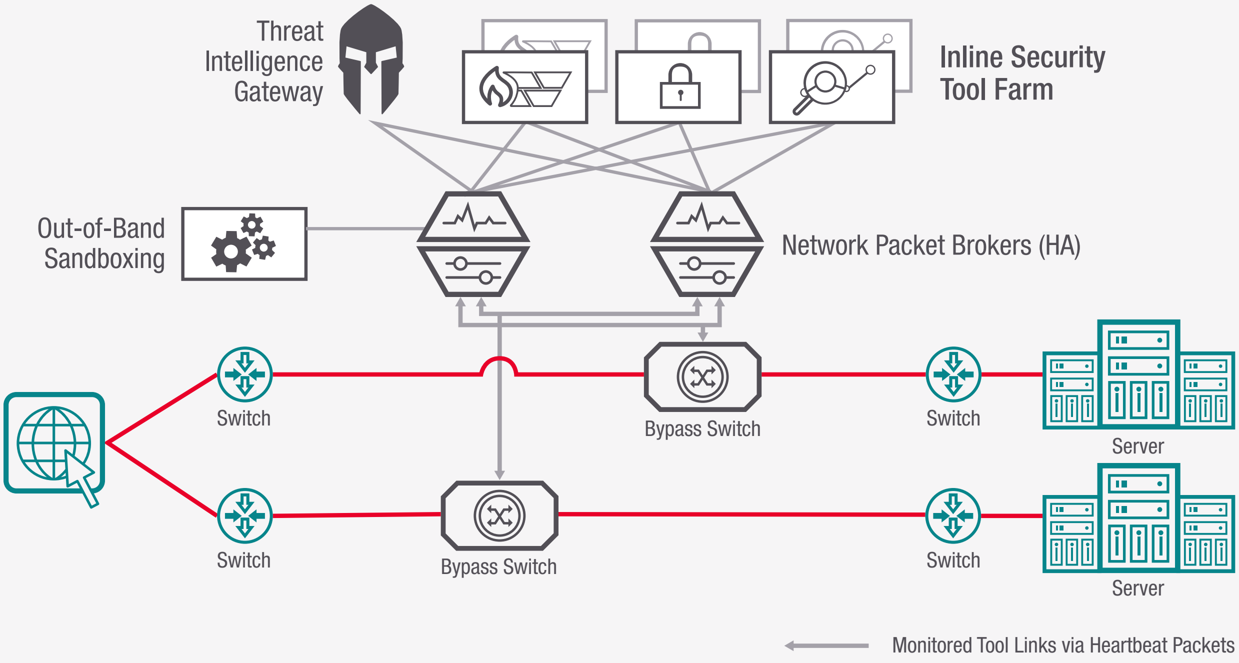
Threat Intelligence Gateway
Inline Security Tool Farm
Out-of-Band Sandboxing
Network Packet Brokers (HA)
Switch
Bypass Switch
Switch
Server
Switch
Bypass Switch
Switch
Server
Monitored Tool Links via Heartbeat Packets

Figure 2. High Availability through Active-Active Configuration

Resilience in complex architectures

Some organizations create customized inspection paths by deploying high availability security architecture in multiple tiers. In this approach, traffic with the highest risk can be routed through a series (or chain) of security tools to ensure thorough inspection, while less risky packets are moved through inspection more quickly or skip inspection all together. An example might be an encrypted packet that must pass through a decryption device before moving to other inspection tools and being delivered to its intended recipient. In contrast, Netflix video traffic can be safely routed to the trusted network without inspection, to save bandwidth and processing power for more risky traffic.

To perform serial chaining effectively, you need NPBs with extremely low latency, since a packet may pass through the NPB multiple times during the inspection process. You do not want the security infrastructure to cause noticeable delays in response. Moreover, you need your NPBs to have built-in fail-open or fail-close options, just like the bypass switches, so if tools in front of a service chain fail, traffic can continue on to be inspected by the remaining active tools.

Context-Aware Data Processing

The growing use of web applications and social media has widened the focus of security beyond just the network. Security attacks at the application layer are a challenge because malicious code can masquerade as a valid client request or normal application data. Popular applications like Twitter, Facebook, and YouTube can cause users to download viruses unintentionally. File sharing can easily cause malware to be downloaded into your network. In addition, applications that use a lot of bandwidth, like streaming media, can crowd out bandwidth that is needed for business applications.

Application intelligence lets you take action based on the context of a particular packet, increasing precision.

Traditional inline security appliances use information from the network and transport layers (Layers 2–4) to protect the internal network from undesirable traffic. They filter out packets based on source or destination Internet Protocol (IP) address, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers, or connection state. A security architecture featuring NPBs with application intelligence—the ability to identify packets based on their content—can go further. This feature uses deep packet inspection to examine information in the headers or content of the message to either block traffic or forward it to a monitoring device. This allows organizations to develop rich data on the behavior and location of users and applications, to identify hidden applications running on the network, mitigate security threats from rogue applications and users, and improve network performance based on application data.

Context-aware application filtering allows you to create granular security policies to block or manage use of applications for individuals or groups of individuals. With application filtering, you can identify, allow, or block thousands of applications and Internet sites to provide protection against threats and malware. You can control employee Internet access to inappropriate or illicit websites and manage bandwidth, to prevent unintentional or even malicious activity by insiders.

Another important function of application intelligence is its ability to produce detailed logs and reports, which can be examined out-of-band for warning signs of impending or actual attacks.

Security Intelligence

Your security posture can be strengthened even more through use of security-specific processing functions. One example is the masking sensitive or personally identifiable information (PII) such as credit card or social security numbers. A high performance NPB has the ability to recognize sensitive information and automatically mask before passing the data to your monitoring solutions. This is vital for compliance and to avoid penalties and fines.

Another key function is the ability to see inside and decode encrypted traffic, to ensure there are no blind spots in your network where malware or some other attack can hide. By decrypting SSL traffic in the NPB, you gain total visibility and offload the processing-intensive decryption work from your security tools.

Some NPBs also offer the option to integrate a threat intelligence feed, a continually-updated compilation of IP addresses known to be involved with malware and attacks, that is produced by security specialists. With threat intelligence, the NPB can automatically block all traffic from these addresses and reduce the number of security alerts your staff must investigate.

A security intelligence feed provided by a dedicated organization that continually tests and validates its database is critical so you do not end up blocking legitimate traffic. A solution that provides information on every address it blocks helps you understand the threat environment and learn from the risks to your network.

Maximize Return on Your Security Investments

Inline security appliances and solutions can be costly, and the need for new infrastructure can easily outpace your security budget. A next generation firewall can cost half a million dollars. Deploying a second firewall on a redundant path, when the first one is operating at less than half capacity, is hard to justify. Deploying a foundational security architecture can help you realize the full value of your existing investments and minimize new tool purchases.

Tool Sharing

The most significant operational improvement you can realize is the ability to share tool capacity across many network links. A centralized control panel allows you to quickly and easily aggregate the data from taps and Switched Port Analyzer (SPAN) ports across your network and prepare it for delivery to a single set of monitoring tools. In this way, your tools get visibility to all of the traffic entering and leaving your network, providing more comprehensive security inspection and detection. With the ability to share tool capacity, many organizations are able to adopt an "n+1" approach to high-availability load balancing, meaning they purchase only the number of devices required to handle the volume of traffic, plus one additional device that can take over in the event of a component failure. This approach can significantly reduce planned capital expenditure (CAPEX) and stretch your security budget much further.

Tool Upgrade Flexibility

Another budget challenge comes from having to match tool speed to the speed of the underlying network. Upgrading a network is expensive and becomes even more costly when monitoring tools must be upgraded at the same time. A security architecture separates the operation of your tools from the live network, which allows lower-speed monitoring tools to receive data from higher-speed core network links. You can make independent decisions about when to upgrade your network and tool infrastructure and extend the life of your 1G or 10G tools or even invest in newer, more powerful security tools without waiting for the network to be upgraded. Having more flexibility over the timing of tool upgrades helps you make better use of the security budget you have to work with.

Pay-As-You-Grow Options

Another way to stretch your security budget is to look for solutions that can be deployed with limited functionality now and expanded as your organization grows. So-called “pay as you grow” options minimize upfront expenditures and let you grow into more advanced features. Licensing costs can be based strictly on capacity, such as the number of ports, or possibly include the number of advanced features that are activated in the solution.

Summary

Security monitoring is critical to protecting your company’s data and resources from accidental exposure or theft. In addition to having powerful inspection and analysis capabilities, your security architecture must ensure you are seeing and monitoring all of the traffic that flows through your network. A top-performing security architecture will provide full data access, application intelligence, and security resilience, as well as help you increase monitoring efficiency and maximize your budget.

Monitoring requires processing an exploding amount of data. Your security infrastructure must be strong enough to protect your assets and data, and efficient enough to not impact network or application response time. Your solutions should have the features and options that let you get maximum value from your security budget.

Find out more about Keysight solutions for Inline Security Monitoring on our website.

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