WHITE PAPER

Network Visibility: The Benefits of an Inline Solution

When we talk about network monitoring or network visibility, what we are really talking about is the network infrastructure that accesses and distributes traffic to IT appliances that handle security, analytics, compliance, and performance monitoring. A good visibility solution can take traffic from anywhere on the network, at any speed and with perfect accuracy, and send it to any of the appliances or tools you have. Ideally, it collects, aggregates, deduplicates, decrypts, and distributes your traffic without adding latency or dropping packets.

You can implement a visibility solution in one of two ways: inline, which supports real-time security and monitoring services, and out of band, which enables non-real-time monitoring, analytics, and data compliance services. Either way, you want the best possible infrastructure for your network. You also want a visibility architecture that provides the most flexibility, least downtime, and best upgrade options — not just for your visibility gear but also for the rest of your network appliances.

This paper discusses inline security and the benefits of this approach. Topics include load balancing, network availability, performance, and getting the best possible return on your network and security investments.

The use cases in this guide are a starting point to help you to plan and implement visibility solutions for immediate results. Each use case features typical network issues, visibility architecture solutions, and the benefits to you and your organization.

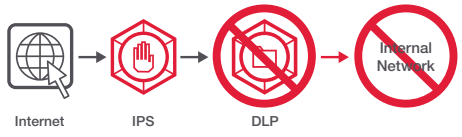
KEYSIGHT TECHNOLOGIES

Protecting Network Availability:
When an inline security system fails or requires maintenance

Situation

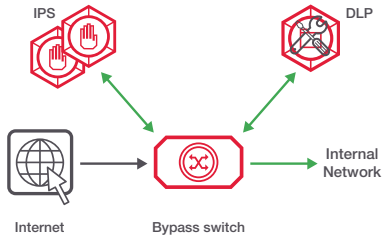
Security appliances deployed inline in a production network must operate at peak performance without fail. When deployed inline on a live network, each appliance is a single point of failure that can take hours to deploy and require downtime to upgrade, troubleshoot, or reconfigure. Waiting for an available maintenance window increases the risk of missing a threat or attack.

Without Keysight Visibility



Each inline tool is a single point of failure in the network

With Keysight Visibility



Keysight automatically protects network availability during tool failure or maintenance

Solution

Deploying external bypass switches in front of security appliances to operate in inline, tap, or bypass mode increases the reliability of network and security systems. Keysight iBypass switches are preconfigured to monitor security appliances using the industry's fastest heartbeat and are ready to install in minutes. Pilot solutions out of band and later move them inline without downtime. Keysight also provides automatic failover between two redundant appliances for better resiliency.

Result

Keysight iBypass switches reduce network downtime and increase solution resilience:

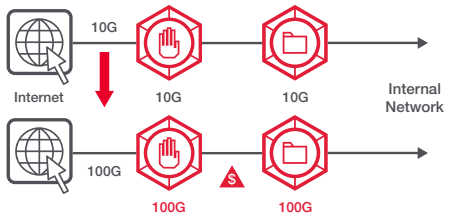
- Preconfigured bypass deploys in minutes and enables subsequent deployment of new security appliances with no network downtime.
- The switches protect your network from hardware, software, and port failure.
- You can update the solution without the need for a maintenance window.
- Support for automatic failover between two active appliances maintains solution uptimes.

Extending the Useful Life of Security Solutions:
When network upgrades cause interface mismatch

Situation

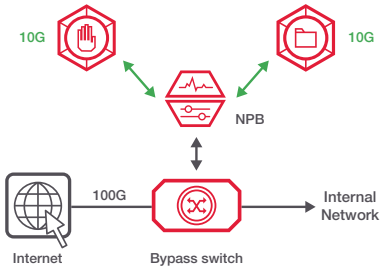
Upgrades to network devices often result in changes to network interface speed. This can prevent the continued use of existing inline security solutions and trigger the need for additional upgrades, even if existing devices still have useful capacity and functionality. Paying for upgrades might force some organizations to delay the purchase of more advanced solutions that address emerging cyberthreats and attacks.

Without Keysight Visibility



Upgrading network link requires simultaneous upgrade for inline security tools

With Keysight Visibility



An NPB delivers traffic at the tool's designated speed to extend useful life

Solution

Adding an NPB enables aggregation of data from diverse network interfaces. Security solutions can then receive traffic with different connection speeds, thereby extending their useful life. Keysight's NPBs are easy to deploy and centrally manage to ensure that the right data goes to the right tool. The Keysight Vision portfolio of NPBs features a user-friendly drag-and-drop interface that quickly connects monitoring tools to appropriate traffic sources with a mouse click.

Result

Extend the useful life of existing solutions and free up budget for advanced solutions:

- Maximize the lifetime value of investments in inline security solutions.
- Enable a diverse set of platforms to work together, regardless of interfaces or speeds.
- Free up budget for the purchase of more advanced solutions that strengthen your defenses against emerging threats and attacks.

Resilient Security Monitoring:
Failover and redundant devices

Situation

During failover of an inline security system, traffic may continue flowing without inspection to avoid business disruption. Visibility solutions that can only be configured in active-passive mode will need a minute or more to restore full processing and restart data delivery. But a lot can happen in 60 seconds, and the increased risk of cyberattacks, malware, or data exfiltration may be too great in some industries.

Solution

Redundant NPBs configured in active-active mode work with complete synchronicity to aggregate, process, and deliver data to all inline security solutions. This increases efficiency, helps with bursty traffic, and enables failover in less than 1 second, maintaining gapless security and inspection. Active-active deployments prevent downtime for tools, NPBs, or bypass switches. Keysight is the only provider with the ability to provide near-instant recovery of inline security monitoring, critical to industries such as financial services and healthcare.

Result

Visibility components in active-active mode enable continuous security monitoring:

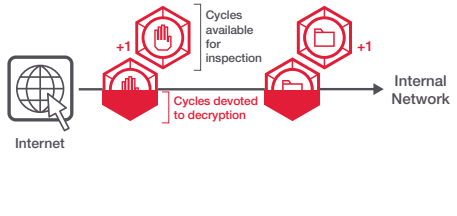
- Fast failover helps you maximize security resilience and minimize risk.
- Active-active configurations with load balancing can help you increase return on investment on redundant NPBs by using them to load balance during normal operations.
- Redundant architectures protect against NPB failure.

Offload SSL Decryption to Visibility Layer:
Don't let decryption impact overall performance

Situation

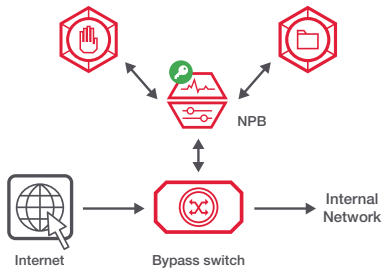
It is imperative to monitor encrypted traffic to maintain strong security, but security solutions are meant to process clear text. To overcome this limitation, some solutions now offer an optional decryption function. However, decryption is a compute-intensive operation that can significantly reduce solution performance. Furthermore, security solutions decrypt traffic for internal inspection only and don't share live traffic with other security solutions, reducing efficiency as multiple tools perform the same decryption function on traffic.

Without Keysight Visibility



Processing decryption on each inline tool uses up valuable processing cycles, forcing tool upgrades

With Keysight Visibility



Active SSL feature in the NPB decrypts / encrypts once to offload tools and make them more efficient

Solution

Adding an NPB with active Secure Sockets Layer (SSL) lets you decrypt, sending the resulting cleartext traffic to all of your security monitoring solutions simultaneously. This offloads your security appliances, which can then devote all of their processing cycles to their core function, increasing their efficiency. To ensure the best possible performance, Keysight NPBs use a cryptographic processor to perform active decryption with zero packet loss.

Result

Offloading SSL decryption lets security solutions focus on deep packet inspection, yielding the following benefits:

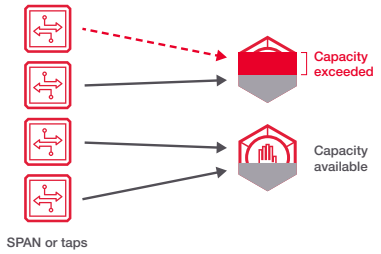
- Decrease overall security risk by inspecting encrypted traffic and re-encrypting securely.
- Increase the capacity and performance of security solutions.
- Cost-effectively share decrypted traffic with all desired security and performance monitoring tools.
- Cost-effectively scale up decryption capacity through an NPB.

Load Balancing for Better Performance:
When bursting or volume varies among network links

Situation

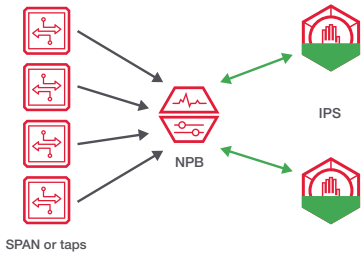
Data bursts or sudden increases in traffic on a particular interface can cause some security appliances to exceed capacity, while other appliances in the same network may be underutilized. Congestion on security appliances can cause device failure or dropped packets. Adding and configuring tool capacity can disrupt network operations and security monitoring, impacting business and creating downtime.

Without Keysight Visibility



Growth in volume or traffic bursts can overwhelm one appliance while others have unused capacity

With Keysight Visibility



The NPB automatically load balances data among available solutions without manual intervention

Solution

Adding an NPB allows aggregation of traffic on the network side and automatic load balancing among multiple monitoring tools on the inspection side. You can quickly deploy Keysight's NPBs and centrally manage them to ensure that the right data goes to the right tool. The Keysight Vision portfolio of NPBs features a user-friendly drag-and-drop interface that quickly connects monitoring tools to appropriate traffic sources with a mouse click.

Result

Load balancing with network packet brokers yields the following benefits:

- increased utilization of security and monitoring tools by load balancing data across multiple tools to prevent individual system overload
- cost-effective and risk-reducing n+1 survivability for monitoring solutions
- increased reliability of security monitoring and decreased risk associated with dropped packets

About Keysight

Edge computing, the cloud, security, compliance, and the ever-growing need for bandwidth are creating new challenges for IT. Keysight, long the source of truth for makers of routers, switches, firewalls, and other network gear, helps IT meet those challenges. Keysight delivers rich data about network traffic, applications, and users in any environment — cloud, virtual, or on-premises. This deep insight, what we call dynamic network intelligence, helps our customers — enterprises, governments, financial markets, service providers, and network equipment manufacturers — drive innovation, stay competitive, meet aggressive service-level agreements, and keep applications running smoothly and securely.

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