Architecting for Security Resilience

Failsafe Availability + Intelligent Control for Inline Security

You need security tools to protect your network.

What have you done to protect your tools?

Continuous investment is what drives today's network security. Threats evolve rapidly so enterprises must add, maintain, and upgrade their frontline security multiple times per year. What was once a firewall now also includes a next-gen firewall, web-application firewall (WAF), intrusion detection and prevention system, forensics tools and more. You purchase security tools to protect your network, but what have you done to protect your tools?

Vendors recommend that enterprises place security tools inline of the traffic flow to inspect live traffic. Every network architect knows that daisy-chaining a series of tools one after the other creates a mess should any of them freeze, reboot, or require maintenance. Serial inline deployment is dangerous. Network traffic would stop in the event that any single tool fails; and according to a report from Dimension Data[1], 42% of network incidents are due to hardware failure. A resilient Inline security framework ensures tool failures do not become network failures.

Network architects understand that resilience starts at the foundation. A proper network foundation begins with a stable bypass architecture where inline tools can operate at line speeds without affecting traffic flow in the event of failure. But with

[1] Dimension Data, Network Barometer Report 2015: http://www.dimensiondata.com/Global/Downloadable%20Documents/Network%20Barometer%20Report%202015.pdf#search=network%20barometer%20report%202015

different security tools requiring different data access, a simple bypass is typically not enough. A network packet broker (NPB) can decrypt data for security tools to inspect and load balance traffic across multiple tools is required. Without these two working together, packets could be lost, failures could bring your network down, and security holes could emerge. Security needs a resilient architecture to maximize network performance.

There are several ways to create an inline security architecture. Creating a resilient inline security architecture requires attention to details. This paper provides best-practice guidelines on how to deploy the most resilient inline security framework. The result will reduce network downtime, enable upgrading tools with zero network impact, and extend the useful life of your security investments.

Reduce network downtime and upgrade security tools with zero network impact.

The Nerve Center of Robust Security

A basic intelligent inline security architecture includes a high-speed bypass switch and a network packet broker. Rather than going directly to your security tools, the bypass switch acts as a failsafe mechanism between the security tools and the network traffic. Should a tool fail for any reason, the bypass switch is programmable to keep your network traffic flowing.

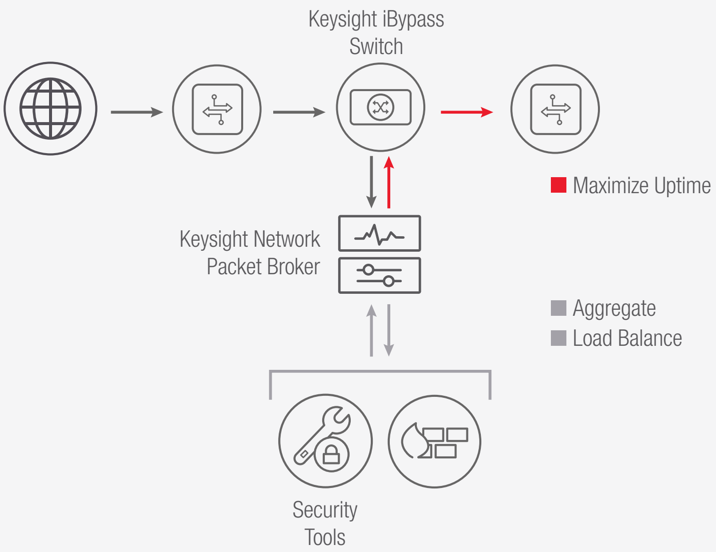


Figure 1. A proper network foundation begins with a stable bypass architecture where inline tools can operate at line speeds without affecting traffic flow in the event of failure.

Not all bypass switches are the same. Keysight bypass switches have the industry's fastest heartbeat, constantly monitoring any attached tools to make sure they are alive. They are also external rather than embedded inside the NPB appliance, so they can more-easily scale with your growing business needs. Keysight solutions offer flexibility, scalability, and the broadest array of bypass switch options in the industry.

From the bypass, network traffic flows to the NPB that load balances traffic and distributes data to the available tools. But an NPB is only good if it actually delivers all the data accurately. Keysight provides the lowest-loss NPBs in the industry, ensuring the highest accuracy of delivered packets.

The choices in architecture determine how many of the benefits in the following table you can achieve in your network. We review a few use cases to explain how to deploy intelligent inline security solutions to solve these challenges.

Optimizing load across your tools: Better performance at lower cost.

Security Tool Challenge	Intelligent Inline Security Architecture Solution	Benefit
Sometimes security tools fail.	Continually send a status check to each security tool and, if a tool is not functional, program that tool out of the traffic path.	Ensures high availability (HA) for network traffic.
Some security tools are overwhelmed while others are underutilized.	Load-balance traffic across security tools to optimize use of existing security tool capacity.	Reduces CAPEX by extending the useful life of existing tools.
Tools require maintenance and updates.	Reroute traffic to other tools to ensure uninterrupted network services during planned inline tool maintenance.	Ensures uninterrupted service and security.
Upgrading network speed requires new higher-speed tools.	Decouple network link speeds from security monitoring tool speeds. This extends security gear life as you move to higher-speed networks.	Reduces CAPEX by extending the useful life of lower-speed tools.
Not all traffic needs to go through every tool.	Send specific traffic directly to the most appropriate security tools or, for already trusted data, directly onto the network.	Provides better performance and reduced CAPEX.

Scaling and Extending Security Tool Life

When a bypass switch sits in front of a set of security tools, it uses a heartbeat function to determine if each of the security tools is alive and active. Without this, a tool might become non-responsive, impacting both security and service.

The NPB shapes and balances the traffic load across active tools while continuously verifying all are active. It also decouples network link speeds from security tool speeds, making it possible for a 1G tool protect a 10G network.

Keysight's baseline security resilience design recommendation below:

- Improves network reliability and availability with the industry's fastest heartbeat, making sure your tools are always active and available
- Easy scales with modular design, using external instead of an embedded bypass switch
- Extends the useful life of your network and security tool investments by decoupling speeds

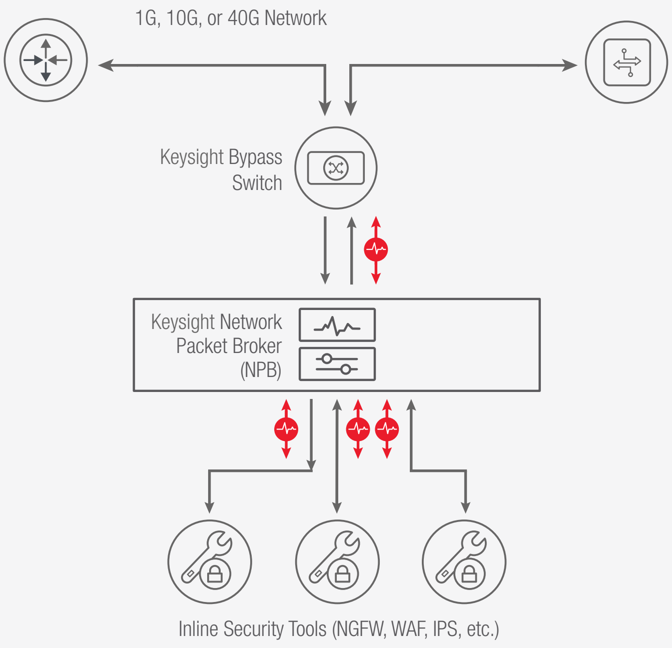

1G, 10G, or 40G Network
Keysight Bypass Switch
Keysight Network Packet Broker (NPB)
Inline Security Tools (NGFW, WAF, IPS, etc.)

Figure 2. Enable greater scalability and usability from security tools by optimizing load across them and decoupling network link speeds from security tool speeds.

Maximum Network Uptime and Availability

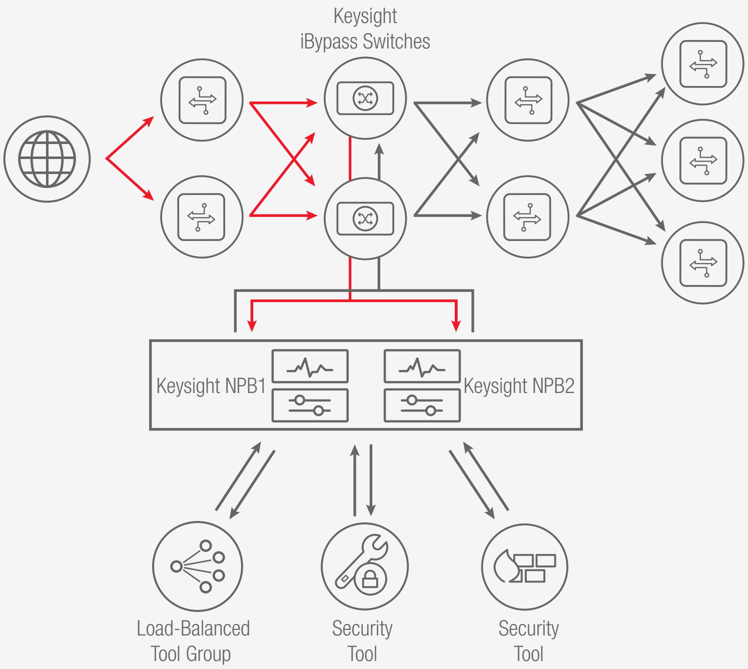
When high availability is a requirement, two Keysight NPBs in HA mode can synchronize their state for higher levels of redundancy. When the primary bypass switch NPB1 connects to NPB2, failover is automatic. The NPB1 bypass heartbeat verifies the tools on the primary path are active, continuously sharing that status with NPB2. If they are not active or slow to respond due to loading, it automatically reroutes traffic to NPB2 to handle the extra load. Keysight's unique technology does this so fast that it is transparent to the network.

When operating in HA mode, the NPBs work together to ensure each security tool receives a full set of TCP/IP traffic, even if transmitted on two different links. The HA design ensures traffic does not fragment and coordinates load balancing. Adding other tools requires configuring only one NPB because it shares the logic with its peers.

Keysight's HA security resilience design recommendation below provides:

- Redundant failover protection with dual monitoring paths
- Nonstop traffic inspection with auto load-rebalancing, even when removing a tool for servicing
- Session integrity, even in the case of asymmetric routing

High availability:
More load balancing, redundant paths, and failover options.



Security Architectures Built for Resilience and Scale

The stability and security of your network starts at the foundation. Building your foundation using fast, flexible, and modular components will keep you from spending countless hours rewiring every time you want to upgrade your network security. Not all bypass switches and network packet brokers are the same, so choosing the ones offering the best stability, best performance, and best extendibility makes sense.

Plan for growth. Speeds will increase, new tools will become available, and maintenance will be necessary. Scaling requires modular choices with programmable intelligence that, most importantly, does not drop packets. Keysight leads the industry in accurate, intelligent network packet brokers.

Extending the usefulness and life of your security tool investments is all about modularity, and Keysight leads there as well. Smart load balancing and programmable architectures can dramatically extend the life of your security tools, even after your network capacity has made them obsolete. If you build your network with these concepts in mind, you will decrease your CAPEX, your network management OPEX, and your network downtime all at once.

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