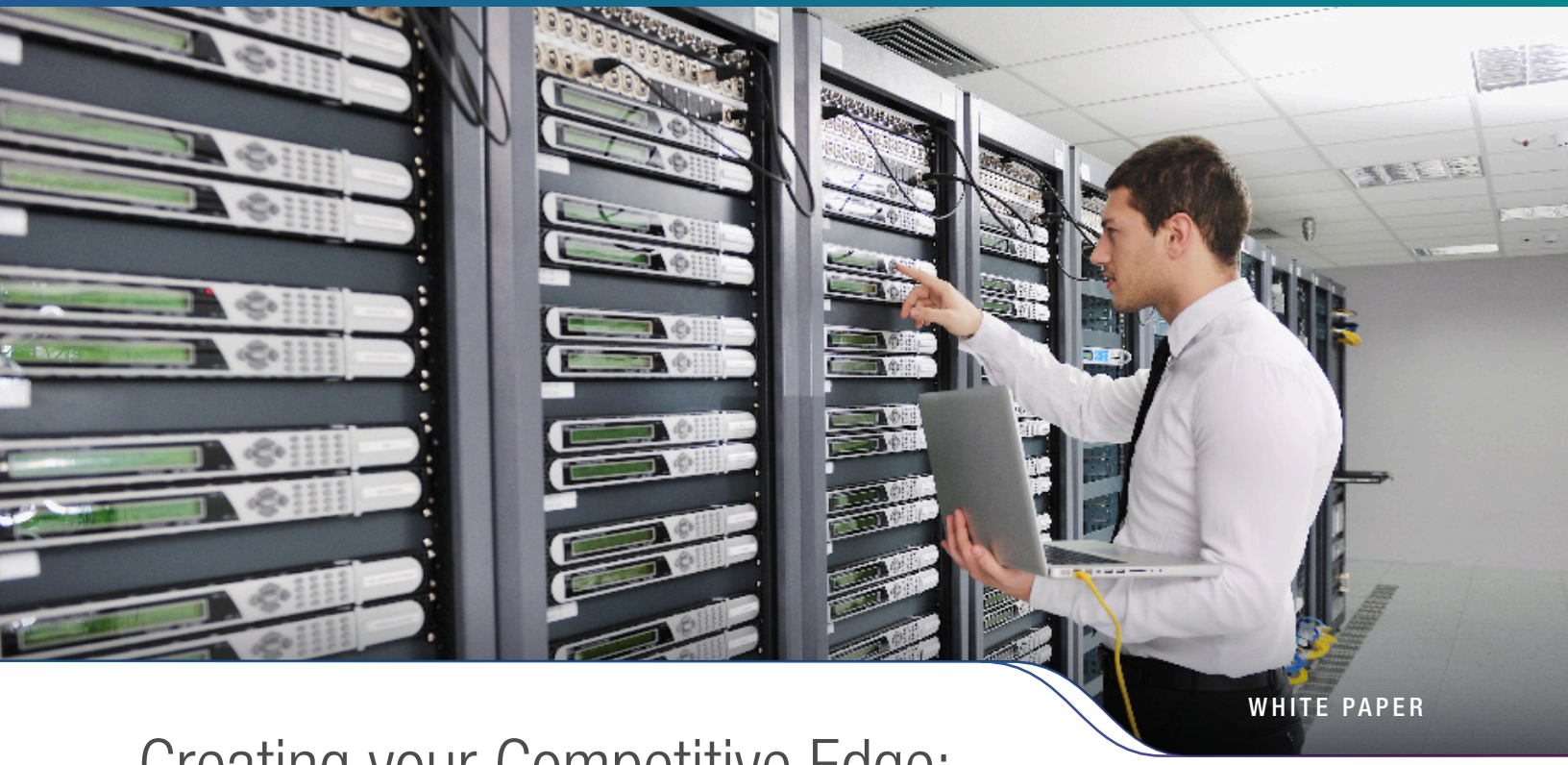


WHITE PAPER

Creating your Competitive Edge: Uncompromised Visibility and Security Performance

Seeking a Performance Advantage

As enterprises, government agencies, and service providers upgrade networks to 10G, 40G, and 100G, key concerns are the ability of security and monitoring tools to support accelerated speeds and throughput, and maximizing the business contribution and investment provided by these tools. Uncompromised visibility, where the organization has end-to-end views of each and every critical packet, becomes a business imperative, resulting in greater security and meeting essential performance thresholds.

Research from IT analyst firm Enterprise Management Associates (EMA) shows 47% of businesses are not properly utilizing the tools they have in place, and 25% of tools are often overloaded and dropping packets. Inserting a Network Packet Broker (NPB) into your security solution to filter, load balance and distribute monitoring data not only provides a welcome performance improvement, but invariably represents a leap forward in the solution value and return on investment. An NPB can extend the lifetime of slower monitoring tools and enable others to more effectively process traffic when duplicate packets and non-suspect data is filtered out.

Research shows 47% of businesses are not properly utilizing the tools they have in place, and 25% of tools are often overloaded and dropping packets.

KEYSIGHT TECHNOLOGIES

But not all NPBs are created equal. NPB technology continues to rapidly evolve with increasing customer requirements and solutions addressed.

Keysight offers customers patent-protected engines and functionality, resulting in NPB performance advantages and usability you can leverage to generate business benefits that provide a competitive edge, with proof points offered in this paper.[1]

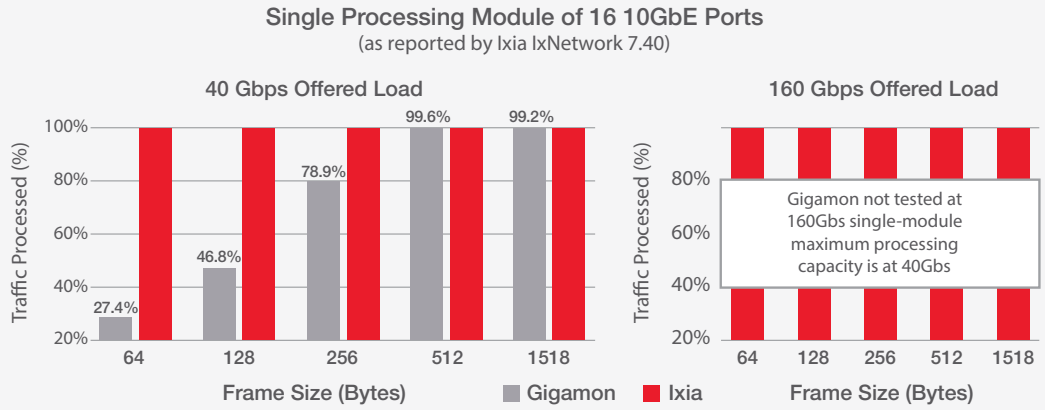
Superior NPB Performance, Verified by Third Party Testing

Unlike other major competitors, in dealing with advanced feature processing such as packet deduplication, protocol header stripping, packet trimming, data masking and timestamping, Keysight's field-programmable gate array (FPGA) based hardware technology enables all Keysight ports to operate at full line rate without restriction. Alternatively, the use of CPU and software-based units results in processing capability limited by the CPU's capability, where resources will be shared across all ports via the backplane. This shortcoming is further pronounced with oversubscription, where multiple standard ports share a single port's resources for advanced packet processing. Cost constraints typically lead to this limited configuration, since a NPB Advanced Feature Module typically costs much more than regular ports.

Multiple features enabled on most industry-standard NPBs result not only in reduced performance but (even worse) dropped packets. These network "blind spots" pose significant risk when tools are not provided all essential traffic to evaluate and measure. The loss of these packets going to security and performance tools increases the risk of security breaches and possible data loss with performance repercussions. Details of this approach have been evaluated and certified by an independent research organization, The Tolly Group. A summary of Tolly's research findings focused on a network running only a single advanced feature, packet deduplication, is documented here.

While the Keysight NPB was tested with 160Gbps, the Gigamon competitive module could not be tested above their stated capacity of 40Gbps.

1 Superior line rate and zero-loss packet processing confirmed in a third party report from The Tolly Group. Keysight sponsored The Tolly Group to perform independent testing on Keysight and like-type Gigamon NPBs. The findings are reported here.



Note: The Keysight NTO 5288 had one 16-port AFM SFP+ module to process data. The Gigamon GigaVUE-HC2 had one SMT-HCOVX16 16-port SFP+ GigaSMART front module to process the data. Unidirectional data was used. All ports on the processing module were egress ports. Each DUT has another 16-port SFP+ module as the input module. Source: Tolly, December 2015

Figure 1. 10Gbe packet processing performance, Keysight vs. Gigamon, with the packet deduplication feature single processing module of 16 10Gbe ports.

The risk of dropped packets, a performance issue most enterprises and organizations would be unwilling to take, rises with increased load and added NPB functionality, discussed in the next section. More findings, including a description of the differences between Gigamon and Keysight visibility architectures, can be found in The Tolly Group report.

While the Keysight NPB was tested by The Tolly Group with 16 10GbE ports, with zero loss of packets, the Gigamon competitive module could not be tested successfully above their stated capacity of 40Gbps.

Seamlessly Integrated Keysight NPB Architecture Offers Multi-Processing Functionality

An ideal NPB should have all the best features integrated and made available in a single platform. In our work with customers, key NPB advanced features typically include:

- Advanced packet processing, including packet header stripping, deduplication, slicing and masking
- Application identification or flexible data packet inspection
- Secure socket layer (SSL) decryption
- NetFlow generation
- Support of inline tool deployment with high availability

		Slicing	Masking	Source ID	Header/Trailer Remove	Dedup	Tunnel Encap	Tunnel Decap	Strip Header	Add Header	FlowVUE	Flow-Filter QTF	QTP Whitelist	QTP Flow Smp.	APF	ASF	1st Level Maps	2nd Level Maps	Load Balance	SSL Decryption
	Slicing																			
	Masking																			
	Source ID	X																		
	Header/Trailer Remove	X																		
	Dedup																			
	Tunnel Encap																			
	Tunnel Decap				X		X													
	Strip Header																			
	Add Header																			
Flow-Ops	FlowVUE						X	X												
Flow-Ops	Flow-Filter QTF		X	X	X	X	X	X	X	X	X									
Flow-Ops	QTP Whitelist		X	X	X	X	X	X	X	X	X									
Flow-Ops	QTP Flow Smp.		X	X	X	X	X	X	X	X	X									
	APF				X			X				X	X							
	ASF				X			X				X	X							
NetFlow	1st Level Maps	X	X	X	X		X	X	X	X	X	X	X	X	X	X				
NetFlow	2nd Level Maps	X	X	X	X		X	X	X	X	X	X	X	X		X				
	Load Balance																X	X		
	SSL Decryption	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	

Figure 2. The table summarizes the valid combinations of GigaSMART operations (an X in the table indicates an invalid combination).[2]

Multiple modules plugged into a single chassis for an "all-in-one" architecture sounds appealing, but actually running the modules simultaneously to offer features in parallel falls short. In contrast, Keysight's flagship NPB, Vision ONE, currently offers up to four advanced features in parallel; a capability not possible with other major competitive NPBs.

Figure 2 depicts the advertised list of invalid combinations from one major competitor. With a vast majority of enterprises encrypting traffic today, a good example of paired functions might be SSL decryption with NetFlow generation, which would negate any

Keysight's flagship NPB, Vision ONE, currently offers up to four advanced features in parallel; a capability not possible with other major competitive NPBs.

2 Reconstructed from GigaSMART Documentation.

advanced feature processing with this model. Not depicted in the table is another critical constraint around inline capability, which is limited to a specific module that can't be used for other purposes.

Inline High Availability Delivered Cost Effectively

An "active-active" protective configuration from Keysight enables customers to distribute inline traffic intelligently to all tools, yet provide a backup on failures.

Many enterprises, including financial services, retailers, hospitals and government agencies, choose to deploy tools inline to combat security threats in real time as they occur. One key inhibitor curtailing this action is the very real fear the visibility solution may introduce a single point of failure, and as a result, network service may experience disruption or even blackout.

With the introduction of Keysight's inline NPB with High Availability (HA), organizations can realize the benefits of a cost-effective inline security solution with protection for that single point of failure. An "active-active" protective configuration from Keysight enables customers to distribute traffic intelligently to all tools, yet provide a backup in case of failure. This design assumes both the primary unit and secondary unit will share the load via load balancing during normal operations. If one should go down, the other automatically takes over all traffic seamlessly with no or minimal interruption.

Keysight's inline solution offers exceptional performance with a reasonable, cost-effective configuration that considers the fact that failures, in general, are only a tiny percentage of total hours. Equally important, it addresses the need to maximize investments in expensive security tools, negating a requirement for organizations to invest in dedicated tools that sit idle during normal operations.

The Keysight active-active HA mode is depicted in Figure 3. It shows two inline NPBs working in active-active HA mode. One is primary and the other secondary. The bypass switch also offers HA mode, configured in active-standby mode. During normal operations traffic reaches both the primary and the secondary NPB via two routing paths. Both NPBs then distribute traffic via load balancing to several tools of a similar type. If one NPB dies, the bypass switch can detect the failure via HeartBeat™ packets and activate the standby segment so traffic can be routed to the secondary NPB, continuing uninterrupted processing.

This design allows maximum resiliency against all kinds of failures, such as: single tool failure, tool group failure, NPB failure and even bypass switch failure. An optimal design achieves high availability for inline tools deployments, and contrasts with competitive designs that require standby[3].

3 Based on a per rack throughput comparison with Gigamon and NetScout, as well as active-active and active-standby support for resiliency.

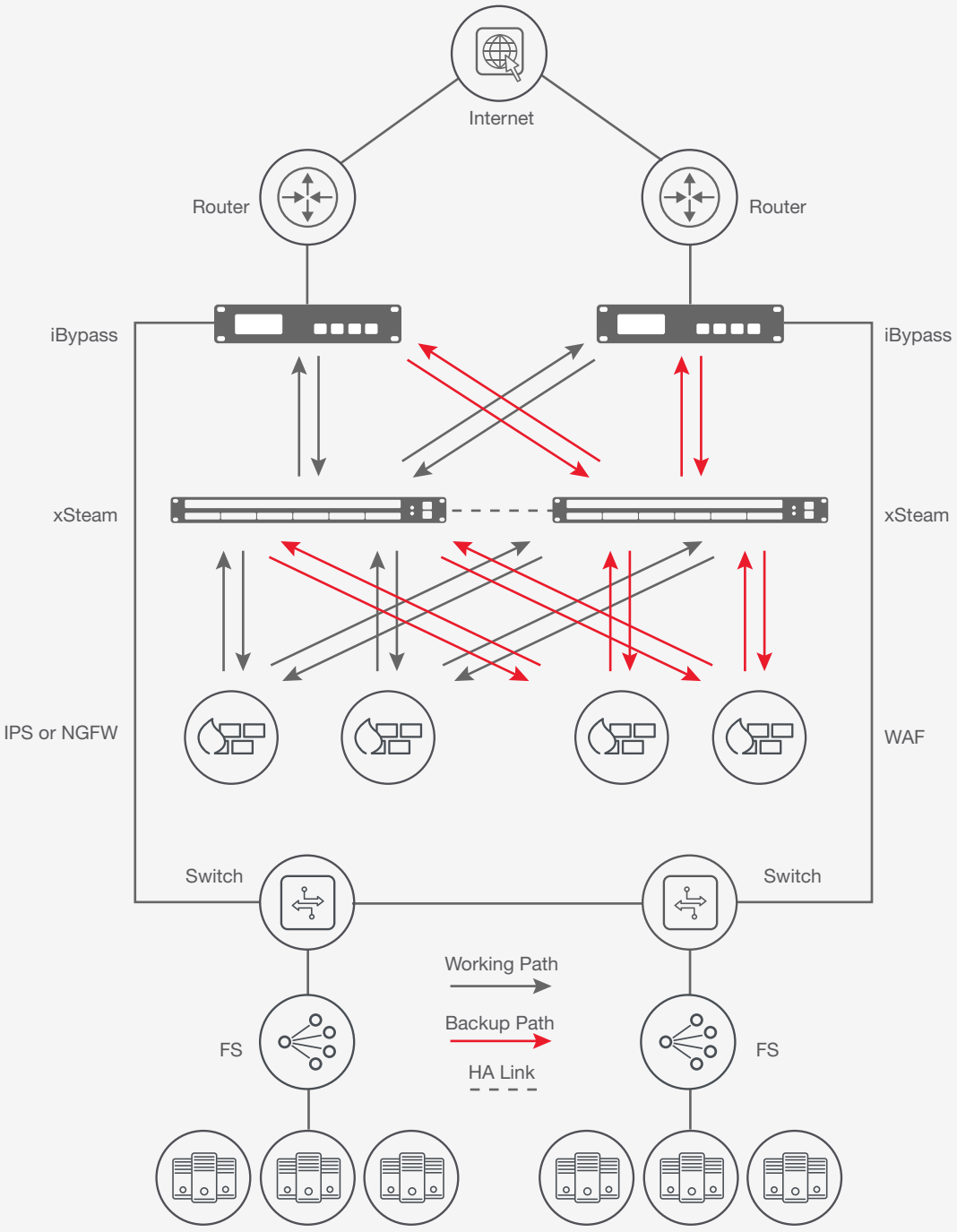


Figure 3. Keysight's active-active inline design for maximum resiliency and performance.

With other major competitors, inline tool deployment is achieved with a dedicated hardware module, which has integrated bypass switches. Two boxes are daisy chained in the traffic path via the integrated bypass switch. Should the primary NPB

fail, the cutover operation is achieved via bypass fail-open action so the first box is skipped all together.

The key limitation to this design is that it can only work in active-standby mode. During normal operation, the secondary box can NOT take traffic or else the tools will receive duplicated traffic. Therefore, the second box is totally idle for as long as the first NPB/integrated bypass switch is working, with the associated loss of resource productivity. And if there are multiple traffic paths you must deploy this dual box setup for each of the traffic paths, at even greater expense with little payback. That said, the chief impediment is the design only protects box level failure such as power loss. It cannot protect individual tool or tool group failures, the predominant cause of failures.

The key limitation to an integrated bypass switch is that it can only work in active-standby mode. During normal operation, the secondary box can NOT take traffic or else the tools will receive duplicated traffic.

Keysight: Offering a Performance Edge for Greater ROI and Value

In summary, Keysight's NPB portfolio offers customers a competitive advantage in the area of visibility performance, which translates to solid business benefits:

- A hardware-based FPGA packet processing engine offering significant architectural benefits, enabling full line-rate NPB function with a single module investment for better Total Cost of Ownership (TCO)
- Importantly, full line-rate packet processing is conducted with zero packet loss and no network "blind spots", protecting your business by ensuring all network data reaches the security and network analysis tools that manage and secure your critical applications
- Keysight's truly integrated packet brokers allow multiple advanced packet processing features operating in parallel, relieving tools from being overloaded and again providing lower TCO and necessary multi-processing
- Inline tool deployment with high availability processors that distribute traffic evenly, better protecting your network in the event of tool failure, and enabling you to maximize availability cost-effectively

Keysight's NPB portfolio is based on engineering innovation that deeply considers customer impact and business issues. The performance edge provided by these solutions can make a difference to your operation. Talk to an Keysight representative or channel partner today to begin your network packet broker Proof of Concept.

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

This information is subject to change without notice. © Keysight Technologies, 2016 - 2022, Published in USA, January 6, 2022, 3120-1132.EN