

An abstract background graphic consisting of numerous horizontal, slightly blurred blue lines of varying lengths and opacities, creating a sense of motion and data flow. These lines are set against a dark, almost black, background.

WHITE PAPER

ARCHITECTING FOR SECURITY RESILIENCE

FAILSAFE AVAILABILITY + INTELLIGENT CONTROL FOR INLINE SECURITY


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 Data¹, 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

YOU NEED
SECURITY TOOLS
TO PROTECT YOUR
NETWORK.

WHAT HAVE YOU
DONE TO PROTECT
YOUR TOOLS?

A decorative graphic consisting of a series of parallel, slanted lines in a light blue color, arranged in a row.

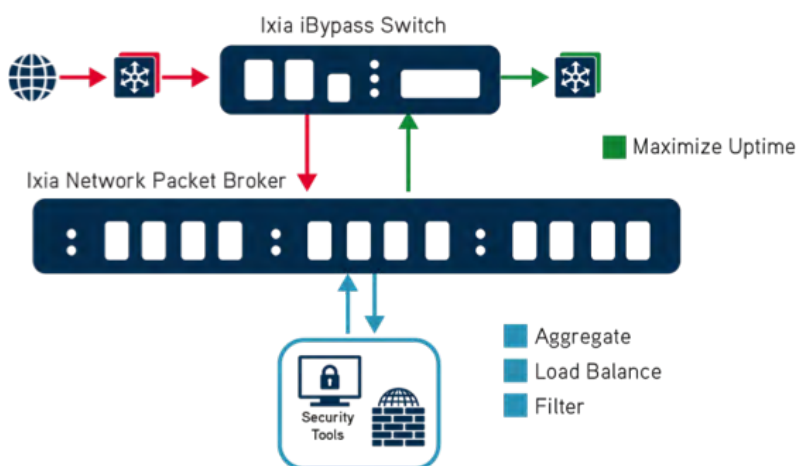
speeds without affecting traffic flow in the event of failure. But with different security tools requiring different data access, a simple bypass is typically not enough. Adding a network packet broker (NPB) or load balancer to that bypass intelligently routes traffic to different security tools for inspection. 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.

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.

Not all bypass switches are the same. Ixia 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. Ixia 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. The NPB is a critical part of a resilient, scalable security posture as it provides application-level filtering to ensure the right tools get the right data. But an NPB is only good if it actually delivers all the data accurately. Ixia provides the lowest-loss NPBs in the industry, ensuring the highest accuracy of delivered packets.

REDUCE NETWORK
DOWNTIME AND
UPGRADE
SECURITY TOOLS
WITH ZERO
NETWORK IMPACT



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.

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.

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.

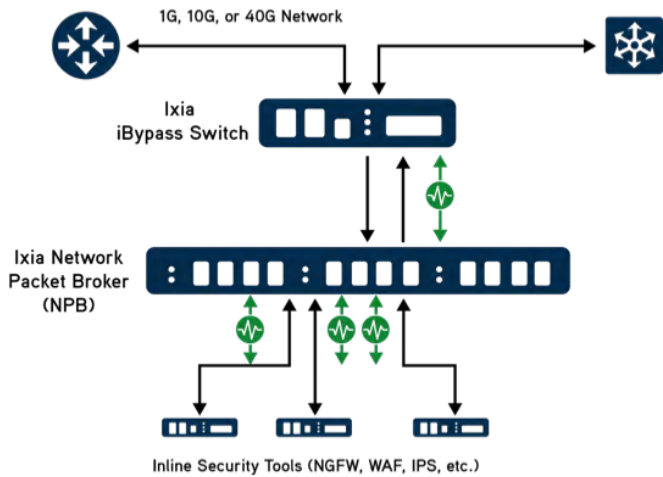
The NPB shapes and balances the traffic load across active tools while continuously verifying all are active. It also decouples network link speeds from security tool speeds, making it possible for a 1G tool protect a 10G network.

Ixia'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

OPTIMIZING LOAD
ACROSS YOUR
TOOLS: BETTER
PERFORMANCE AT
LOWER COST





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

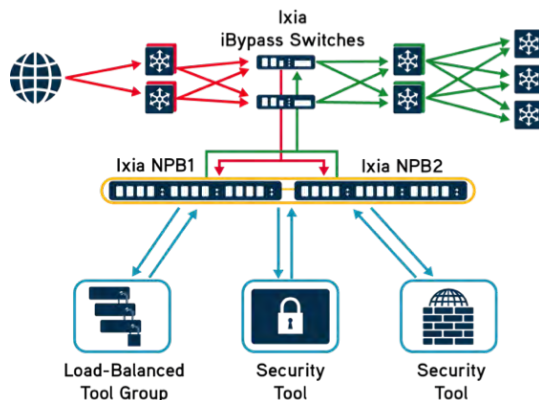
MAXIMUM NETWORK UPTIME AND AVAILABILITY

When high availability is a requirement, two Ixia 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. Ixia'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.

Ixia'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.

EXTENDING USEFUL LIFE OF SECURITY TOOLS

Since the HA architecture decouples the network links from the security tools, adding new links to the monitoring system is as easy as connecting them to the bypass switch. Once added, simply configure the new network link traffic into the filtering and load-balancing operations.

The NPB has both Layers 2-4 filtering capabilities and application intelligence, enabling it to extract traffic of interest for specific tools. For example, it can send all HTTP traffic to the web-application firewall (WAF). Once it isolates traffic of interest, you can configure it to pass the rest of the traffic directly back to the network link.

All of Ixia's security resilience designs provide:

- Scalability for your network by using a bypass switch to connect new network traffic to your existing security system
- Overload protection for your security tools by only sending them relevant traffic
- Delayed CAPEX spend by extending the useful life of your existing security tools that have unused capacity

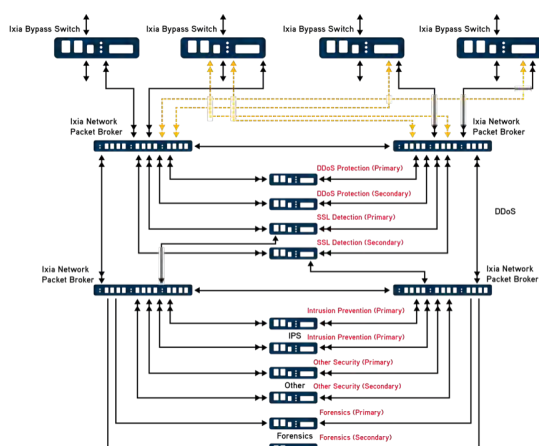
MANAGING COMPLEX SECURITY ARCHITECTURES

Very complex networks can include several purpose-built security tools. When configuring the bypass and NPBs as shown, a chaining of services cross-connects one security tool to another. For example, one NPB can distribute the output of a single SSL decryption tool to one or more other security tools.

Using Ixia products, complex architectures like the one below provide:

- Customizable traffic monitoring views using one NPB interface
- Ability to add logic to control and filter traffic amongst many security tools
- Scaling with failover paths should a primary device become unavailable

This architecture also adds minimal latency impact and eliminates tool contention by programmatically adapting to new security tools.



REDUCE CAPEX:
EXTEND THE
USEFUL LIFE OF
YOUR SECURITY
TOOLS



Remove risk and complexity even
for purpose-built security tools.



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. Ixia leads the industry in accurate, intelligent network packet brokers.

Extending the usefulness and life of your security tool investments is all about modularity, and Ixia 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.

Ixia supplies the industry's best foundation, enabling you to build more resilient, cost-effective, and secure networks. Contact Ixia today to learn how our intelligent security architectures can change your network experience.

Secure networks need inline security resilience. Secure networks need Ixia.

IXIA SUPPLIES
THE INDUSTRY'S
BEST FOUNDATION
FOR SECURITY
RESILIENCE



1. Dimension Data, Network Barometer Report 2015:

<http://www.dimensiondata.com/Global/Downloadable%20Documents/Network%20Barometer%20Report%202015.pdf#search=network%20barometer%20report%202015>

IXIA WORLDWIDE HEADQUARTERS

26601 AGOURA RD.
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942

(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 818.871.1805

WWW.IXIACOM.COM

IXIA EUROPEAN HEADQUARTERS

IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44 1628 408750
(FAX) +44 1628 639916

IXIA ASIA PACIFIC HEADQUARTERS

101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127