Company:

Financial Services Company
One of the largest personal lines insurer in the United States with insurance operations in Canada as well.

Key Issues:
- A major security event in 2014 created a sense of urgency to improve overall security through network visibility
- NPBs (network packet brokers) were needed to support several new security tools

Solution:
- Ixia NTO 7300 base systems
- Ixia NTO 7300 ATIP (application and threat intelligence processor)
- Ixia NTO 6212 ATIP
- Ixia NTO 7300 Carrier Line Modules
- Ixia NTO 7300 AFM (advance feature module)
- Ixia NTO 7300 interface modules
- Ixia vTAP, Phantom 1 subscription
- Ixia Indigo Pro Manager Virtual
- Upgrade to Gold Maintenance Support

Results:

The Ixia Solution:
- Enhanced company security posture
- Provided critical security information to security tools
- More effectively protect infrastructure and reduce exposure to damaging security breaches
- In a POC (proof of concept) comparison to the competition, Ixia addressed the customer needs better and more reliably
- Improved productivity with single pane of glass management for central monitoring and alarming for all Ixia gear

SAFEGUARDING AGAINST CYBERATTACKS

FIRM ELIMINATES SECURITY BLIND SPOTS

As a personal lines insurer, there is much to protect. How many times have we all shuddered, hearing about personal information being breached, including identity, financial accounts, and even health records? Cyberattacks are top-of-mind for companies who must maintain a level of trust and integrity with their customers, clients, and partners.

Having a security event in 2014 created an even stronger sense of urgency to strengthen overall security through improved network visibility. Awareness of this effort was reported to the CIO, the CISO and even the CEO. Executives undoubtedly do not want to appear in articles on the biggest security breaches, like the one from Network World[1] entailing, for example, how data was stolen on 22 million current and former federal employees from the federal Office of Personnel Management.

A well-publicized security breach in 2015 resulted in the theft of personal data for 22 million current and former employees of the federal government.[1]
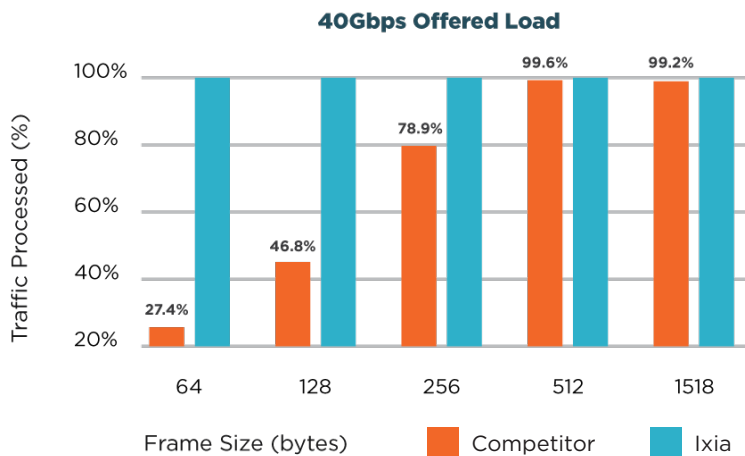
WHY NETWORK VISIBILITY?

This firm already had NPBs (network packet brokers) implemented by their network tools group. But now, the security group required NPBs to support several new security tools being deployed, including security analytics, firewalls, etc.

The Ixia solution allowed them to enhance their security posture by providing critical security information to those new security tools, more effectively protecting their infrastructure and reducing their exposure to damaging security breaches.

MORE RELIABILITY AND ZERO LOSS

Considering multiple vendors, the organization had to ensure resiliency of the solutions while implementing de-duplication, under load. The neutral, third-party partner working with this firm performed an "apples-to-apples" POC (proof of concept) comparison with Ixia solutions and another well-recognized network packet broker in the market. This neutral partner was able to confirm that, contrary to the competitive system reporting, their solution was indeed dropping packets, as revealed by an internal counter. Dropped packets create blind spots, compromise reliability and security. Learn more from the Tolly Report[2] how Ixia provides zero-loss advanced packet process while other competing systems, lost packets (e.g. 72.6% frame loss for 64-byte frames), creating security blind spots.

The conclusion: The company decided that Ixia could address their needs not only better than the competition, but more reliably as well.

40Gbps Offered Load

Traffic Processed (%)

Frame Size (bytes)	Competitor	Ixia
64	27.4%	100%
128	46.8%	100%
256	78.9%	100%
512	99.6%	100%
1518	99.2%	100%

IMPROVED IT TEAM PRODUCTIVITY

Finally, this company also chose to implement Ixia Indigo Pro Manager, providing a single pane of glass for management, central monitoring, and alarming of all Ixia gear. Why? The standard interfaces allow for easy configuration, statistics collection, and health monitoring. By automating processes such as software upgrades and configuration backups, Ixia Indigo Pro simplifies IT administrative tasks that would otherwise take days or weeks to complete, improving IT team productivity.

Single pane of glass management and automated processes vastly improve IT team productivity.

Source: [1] Network World; "Biggest data breaches of 2015"; 12/2/2015

[2] Tolly; Tolly Test Report #216100; Jan. 2016

ABOUT IXIA

Ixia provides testing, visibility, and security solutions, strengthening applications across physical and virtual networks for enterprises, governments, service providers, and network equipment manufacturers.

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) 1.818.871.1805
www.ixiacom.com

IXIA EUROPEAN HEADQUARTERS
IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL64FL
UNITED KINGDOM

SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC HEADQUARTERS
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 30 7591

SALES +65.6332.0125
(FAX) +65.6332.0127