A Solution to Network Security That Actually Works

Implementing Optimal Network Security with Ixia Solutions

Table of Contents

Executive Summary

Ixia understands the unique security challenges faced by modern enterprises. Potential threats can come from all directions, and no one can be trusted. The only way you'll be able to overcome these challenges is to use a comprehensive, multi-dimensional approach to network security. At the same time, security-focused IT personnel need to adopt the attitude that security isn't something you purchase, it's something you actively do – everyday.

Continually-evolving and new attacks seek to find yet-undiscovered holes in your network defense. Traditional network security testing using penetration methods or canned attacks is outdated and impractical. You need a resilient architecture that can withstand the onslaught of dynamic attack vectors to limit as many successful attacks as possible, and then recover quickly if a breach does occur.

To help our customers protect all of the different facets of their network, Ixia promotes a five-pronged security approach that is based upon customer feedback and many years of security expertise:

1. Understand your network better and how it works
2. Characterize your security architecture – both strengths and weaknesses
3. Strengthen the skills of your security professionals
4. Enhance your network monitoring capabilities for both virtual and physical networks
5. Improve your operational readiness for countering security attacks

Although the implementation of each of the five areas is dependent upon your specific network and your business goals, this paper provides a planning framework and how Ixia can help at each step. Implement the following proven approach to strengthen and protect your network and ensure ongoing security resiliency.

Ixia understands the need to secure the enterprise, the ramifications of what happens when a breach occurs, and the realities of IT budgets in a fast-changing world. We've put this document together to show our customers how they can take advantage of proven knowledge and expertise to strengthen their security defenses within the context of these three guiding requirements.

Understanding All Facets of Your Network

While the concept that you need to understand all facets of your network might sound simple, it's actually quite complicated. How many IT engineers can truly say they understand their network from the basic equipment, to the security architecture, to the visibility (monitoring) architecture, to storage, to applications, etc.? These different areas often end up as segregated silos within IT. Unfortunately, hackers know this and use this knowledge to probe for exploitable issues with equipment, software, and policies.

To implement a resilient security architecture, IT architects and managers will need to come to grips with the need to change their security model, understanding that network security isn't something they can purchase, but rather it's something that they need to work at every day.

The paradigm shift is to take a comprehensive, multi-dimensional approach to securing your network. While this sounds like a lot of work, and it is, there are simple steps you can take that will show solid improvements. There is no perfect security product that can stop intruders in their tracks. It needs to be a concerted process of best practices that are put into place and maintained.

A Visibility Architecture is Key to Effective Network Security

A visibility architecture is the first step to understanding all facets of your network and improving your security effectiveness. If you don't have a visibility architecture, then you need one. Just like it indicates, a visibility architecture is what will give you "visibility" into what is happening on your network. If there's a problem, would you rather guess at it and perform iterative trial-and-error approaches to fix it, or simply know right from the outset what the problem is? A visibility architecture gives you the capability to see and characterize anomalies on your network either in real-time or post-event, depending upon how you implement your architecture.

The only way to achieve scalable, reliable, and sustained visibility is with a holistic and strategic approach to visibility. IT operators must be able to, at a glance, get insight into the totality of the network traffic and security picture. What is happening, where is it happening, is it secure, and – most importantly – why is it happening?

Building this type of insight requires not just single solutions at various points in the network, but an end-to-end architecture for monitoring and security that scales along with network growth that can adapt to new types of applications and evolves to meet new demands. An easy-to-use and easily-adaptable intelligent visibility architecture is needed to make sure that you have a new perspective on the blind spots in the network.

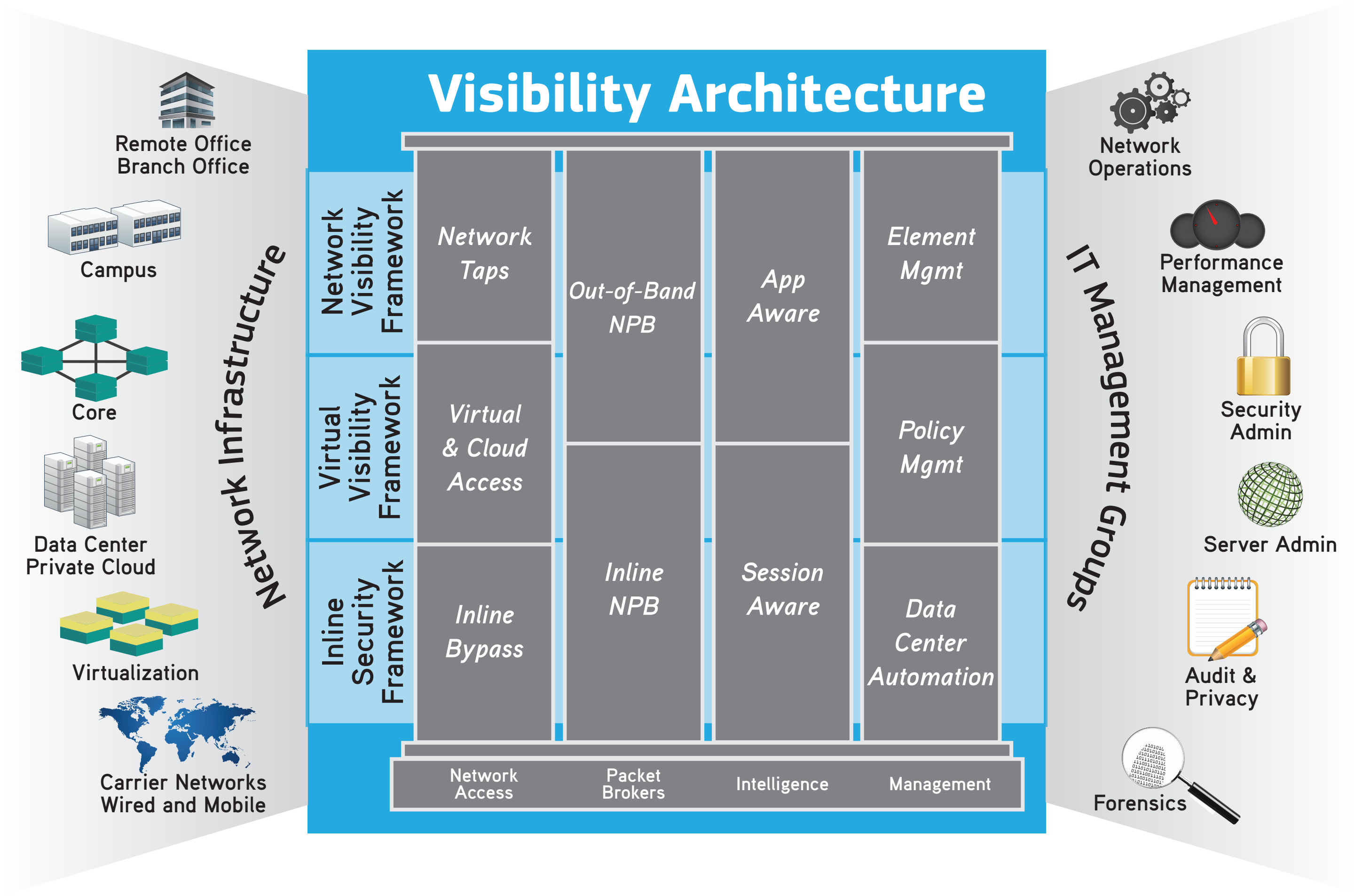
A visibility architecture, like the following one proposed by Ixia, is essentially a cost-effective design that provides access to network traffic, intelligently filters data, sends the groomed data to analysis tools, and then delivers information as output from the monitoring tools so that IT can make informed decisions about problem resolution and network improvements.

With the proper visibility architecture in place, you'll be able to see what is (and what is not) happening on your network. Simply put, you can't monitor what you can't measure and you can't make accurate corrections without accurate monitoring data.

Integrating Visibility and Security

To correctly secure your network, you'll need to integrate your visibility and security architectures. Some organizations look at these as silos, but the integration of the two systems is what will provide not only better insight into what is happening as your security architecture protects the network, but also allow you to answer important security questions, such as:

- Where are your blind spots? You need to know because bad things happen in blind spots.
- Is your security architecture stance going to be proactive or reactive?
- Do you need in-line security capabilities or out-of-band?
- Are the security policies you have put into place (BYOD, role-based access, malware analysis of email attachments, the control of customer data, etc.) effective?
- Do you have the same visibility into your virtual network as you do your physical network?
- Do you need Layer 7 deep packet inspection (DPI) information?



How you tie the visibility architecture and security architecture together depends upon your threat vulnerability assessment, your budget, and your ability to react to threats in real-time. Whatever the implementation of your joint security and visibility architecture, it should provide three valuable attributes to mitigate your security threats:

- Better data to analyze security threats
- Better operational response capabilities to attacks
- The ability to apply a set of consistent policies across your network

These three capabilities are the "golden key" to help you secure your network. Implementation of one or two capabilities may help, but it's the whole trifecta that will deliver the benefits that can safeguard your intellectual property and prevent exfiltration of critical company data.

In the end, it's not about buying more security products and services, but buying the right amount of them for *your* network.

For more information on creating an effective visibility architecture, see Ixia's white paper *Creating a Visibility Architecture* (http://info.ixiacom.com/creating_a_visibility_architecture.html)

Ixia Solutions Allow You to Characterize your Security Architecture

The second prong of the approach is to test and characterize your security architecture. To protect your network, you need to understand both your network security strengths and weaknesses. The only way to do this is to test it and analyze how it responds. You'll want to capture and understand the information necessary to:

- Evaluate security devices – how well do your firewall, intrusion prevention system (IPS), and intrusion detection system (IDS) perform
- Optimize configuration – are these devices configured properly within your network
- Benchmark/baseline architecture performance – what is the "golden configuration"

Security Device Evaluation

The first step here is to evaluate your architecture components and compare (or validate) the vendor's stated specifications before you purchase. Ixia's BreakingPoint® application and security test solution is uniquely capable to perform the analysis. Using this vendor-agnostic test solution, you can perform proof of concept (PoC) validations on individual components to see how they respond when faced with line-rate application traffic and security threats.

The only way to properly evaluate the device performance is to test it under the specific conditions that are found in your network. Any other measurement makes no sense. For instance, does the performance under real-world conditions measure up to the specifications as advertised by the seller? Oftentimes, the advertised abilities of a security device or solution are what are possible under "ideal" conditions. This has no relationship to a full production network. You need to validate the security device effectiveness under the different types and mixes of traffic – both good and bad – that your network will experience, all at line rate.

If vendor devices don't measure up, you can use this knowledge to buy something that does—or negotiate a discounted price for the product you've tested. If the product only delivers 70% of the performance stated on the product data sheet, why should you pay full price? You ought to receive a 30 percent discount off your negotiated sales price since you're going to probably need to deploy more equipment to overcome the device's lack of performance. Use the objective data results from the Ixia BreakingPoint product to prove to your prospective vendor that their product's performance doesn't measure up and negotiate that additional discount. Otherwise, look at a different vendor and determine how their solution will perform. Decisions are easier when you are empowered with accurate and objective information.

Adopting the right solution is a key weapon in a solid network defense against incursions.

Security Device Configuration Optimization

Organizations are making huge investments in IT systems (i.e., cloud, application performance, and mobile) to meet business needs, without nearly enough guarantee in the performance or resiliency of network security. Complex system interactions make it difficult for you to optimize security performance and network resiliency. Once the technology is chosen, you need to test to determine the configuration that best suits your needs. This may require repeated testing and tweaking cycles until the right settings have been found.

Ixia BreakingPoint enables you to simulate real-world user traffic, at line rate, to determine how a device will perform when it goes live into production. It acts both as a client and a server, sending good, clean traffic along with security strikes to the target, and performing critical measurements for round trip time, latency, and throughput. You can methodically run a test on individual devices or the entire network, optimize configurations, and then rerun the exact same tests to ensure optimally-performing network security.

Ixia BreakingPoint solutions help security strategists fine-tune defenses from product selection and infrastructure design to assessing upgrades and modeling potential threats to assess readiness. Evaluating DDoS responses and preparedness as security environments evolve minimizes risk over time and keeps organizations up to date and able to launch powerful, real-time responses to today's ever more complex and powerful attacks.

Pre-deployment testing to optimize components as they relate to the network as a whole should be a high priority. Principal among the security tests are:

- **Interoperability –** both positive and negative cases that help close security holes and ensure inter-operation between network components purchased from multiple vendors

- **Fuzzing –** perform targeted randomization on protocol packets to explore protocol implementation flaws and possible exploits in great detail
- **Known vulnerability testing –** potentially large number of tests that ensure that services and applications have been updated and improved to resist historical attacks
- **Performance –** determine the maximum real-world performance of devices, applications, and the overall network and how they perform under overload (i.e., rejecting new users, slowing down sessions, failing)

Benchmark/Baseline Your Architecture Performance

The third part of characterizing your network is the most crucial step: you need to benchmark your chosen tool, technology, and configuration as it sits in the network BEFORE you go live. If you don't test the setup, you will be under a false impression of security—the consequences of which may be a serious security breach.

Testing before you deploy prevents you from exposing your network with holes that missed your attention. It also allows you to determine how your security solution works as a whole, in the network, as opposed to just as its individual components.

Pre-deployment testing also provides a solid baseline performance metric that you can measure against once the system is live in the production network. When you inevitably upgrade, change, or modify the security configuration, you can see if the performance differs significantly against the original, pre-launch metrics. A new software update might fix one problem but cause another.

As the system moves forward, and additional devices or technologies are added, you need to continue pre-deployment testing as a crucial step. When testing, always compare the data against the most recent network benchmark. This comparison allows you to make the best decisions about the performance of your network and security infrastructure, based on empirical data rather than vendor specifications.

For more information on how BreakingPoint can help you evaluate devices, see Ixia's white paper *How to Maximize IT Investments with Data-Driven Proof of Concept* (http://info.ixiacom.com/Enterprise_IT_6_Steps_Data_Driven_Proof_of_Concept.html)

Ixia Solutions to Help Characterize your Security Architecture

Ixia Solution	Image	Description
Ixia BreakingPoint		Validate next-gen firewall, IPS, and other security devices with this industry-leading application and security test platform. It simulates an authentic, customized blend of stateful application traffic combined with live security attacks and massive-scale user load. You can easily create the actual behavior of millions of wired and wireless users, hundreds of applications, and tens of thousands of security attacks to validate, optimize, and benchmark the latest security gear.
Ixia BreakingPoint Application and Threat Intelligence (ATI) subscription service		Test and simulation conditions must reflect the latest security threats and applications so that you can ensure your equipment and systems will perform reliably and protect networks from the most advanced and malicious traffic. Empowering BreakingPoint test solutions, the ATI program delivers the industry's most up to date application and threat intelligence, including 260+ stateful application protocols and 36,000+ live malware strikes found in enterprise, core, and mobile networks.

Ixia Solutions Strengthen the Skills and Productivity of your Security Professionals

Many organizations and government agencies have answered the cyber defense challenge by arming their networks with firewalls, IPSs, and other defenses. Though this satisfies a rudimentary network security checklist, this approach alone has no hope of keeping pace with the rapid evolution and scale of cyber threats, and is destined to fail. Effective cyber security is the product of melding trained people, or cyber warriors, and automated systems into a unified defense.

The third prong in our recommended security approach is to implement solutions that allow security professionals the ability to work smarter, not harder. You often hear companies talk about this but Ixia actually delivers. Following are three areas to consider.

Use Ixia Cyber Range Solutions to Sharpen Personnel Skills

The cyber range discussion is really two-fold – set up a cyber range and train your cyber warriors. People are one of your most critical elements. You need to invest wisely in them. You must couple compact cyber ranges with standardized curriculum for the real-world exercises needed to build skills and hone cyber warrior instincts.

Traditional cyber ranges require significant, costly investments in hardware and personnel — and even then cannot scale effectively to address today's growing network traffic volume and ever-more complex attack vectors. But a cyber range is really nothing more than a realistic environment that is used for cyber technology development (i.e., device evaluations or PoCs) and cyber warfare training (including flag exercises, cyber competitions and red, blue, white team training exercises).

BreakingPoint can help you achieve cyber range testing and training without the need for the quickly-outdated and vast test beds of past cyber ranges. Ixia also offers excellent self-paced training and hands-on cyber-range exercises to transform your every-day personnel into cyber warriors. With Ixia, you can implement a scalable approach for training and certifying cyber warriors in critical information assurance (IA), information operations (IO), and mission assurance (MA) skills.

Use Pre-Built Test Suites to Make Testing Fast and Easy

Pre-built test suites significantly reduce test time, saving IT personnel hours of time and increasing their efficiency. BreakingPoint provides pre-configured application/language traffic mixes that leverage extensive automation and wizard-like labs to address many use-case scenarios, including validation of lawful intercept and data loss prevention (DLP) solutions, with a digital storm of content in multiple languages.

Users can quickly initiate a comprehensive and targeted test in about 30 seconds using 3,000+ pre-packaged ATI Super Flows, real-world mixes of applications and their behavior. An example of a Super Flow would be the behavior of a Gmail session, where a Gmail Client steps through all the required sequences of resolving DNS query, conducting TLS authentication session with a Gmail server, retrieving the mail and then closing the session.

Additionally, the ATI subscription ensures testing with real-world application traffic mixes and native application protocol support that includes a configurable weight per protocol and dynamic application content to more-easily simulate reality, where application data changes exactly as a real application would.

Use Automation Capabilities to Minimize Manual Intervention

Network packet broker (NPB) automation also makes your workforce more productive, efficient, and responsive. You can't be everywhere at one time, and neither can your monitoring tools. By leveraging automation capabilities of Ixia solutions, you set rules in place that allow components like an NPB to respond automatically to common scenarios. This lets you virtually move the monitoring switch wherever it needs to be, controlling capital expenditures while capturing the network information you need.

When automation is combined with a network packet broker, you can achieve near real-time responses to minimize security threats and dramatically decrease the mean time to repair (MTTR) for your network, since faster responses to problems results in a shorter mean time to diagnosis and a corresponding faster MTTR.

NPB automation, like the capability implemented within the Ixia Net Tool Optimizer® (NTO), has been identified as a key feature for data centers to optimize productivity. This includes network monitoring, where automation is critical to enabling adaptive monitoring capabilities and tactics to solve your visibility blind spots.

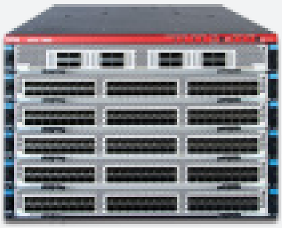
Once automation is configured, you can dramatically increase your network visibility – decreasing your OPEX, your provisioning cost, and the MTTR for your network. These benefits are due to the near real-time capabilities that you can now enable within the data network. For example, you can provision network monitoring functions for the NTO at the same time new services are set up and customers are added to the network. Another example is that adaptive network monitoring creates a proactive real-time solution to help you mitigate and/or eliminate problems and security threats as they occur, instead of at some point down the road.

If automation is implemented correctly within a network packet broker, the device will let you maximize the capabilities of your monitoring tools without specialization or changing your processes. Basically, a proper implementation of automation makes the monitoring switch conform to how you need to use it, not the other way round.

For more information on cyber range solutions and training, see *Cyber Range: Improving Network Defense and Security Readiness* (http://info.ixiacom.com/CyberRange_Improving_Network_Defense_and_Security_Readiness_White_Paper.html).

For more information on automation, see *Automation: The Future of Network Visibility* (http://www.ixiacom.com/sites/default/files/resources/whitepaper/visibility-switc-automation.pdf)

Ixia Solutions to Help Strengthen the Skills and Productivity of your Security Professionals

Ixia Solution	Image	Description
Ixia BreakingPoint		Validate next-gen firewall, IPS, and other security devices with this industry-leading application and security test platform. It simulates an authentic, customized blend of stateful application traffic combined with live security attacks and massive-scale user load. You can easily create the actual behavior of millions of wired and wireless users, hundreds of applications, and tens of thousands of security attacks to validate, optimize, and benchmark the latest security gear.
Ixia Cyber Range and Cyber Warrior Training Solutions		Enable you to quickly, compactly, and cost-effectively recreate Internet-scale cyber warfare scenarios in a controlled environment. Employing the same conditions as the world's largest cyber ranges, BreakingPoint cyber range solutions help you harden your defenses and train and certify your IT professionals as cyber warriors. Only Ixia BreakingPoint couples a compact cyber range with standardized curriculum for the real-world exercises needed to build skills and hone cyber warrior instincts. Using self-paced training and hands-on cyber range exercises, you'll transform IT personnel into cyber warriors.
Network Tool Optimizer (NTO)		Revolutionize the way you monitor your network with Ixia's NTO portfolio of network visibility solutions. These network monitoring switches, also known as network packet brokers, provide complete visibility into physical and virtual networks, improve network security, and optimize monitoring tool performance. Ixia NTO solutions provide complete visibility by intelligently connecting your data center with monitoring tools to aggregate, filter, load balance, and de-duplicate network traffic. Unlike other NPBs, Ixia's patented filtering and de-duplication technology ensures each monitoring tool gets exactly the right data needed for analysis. Ixia NTO solutions are powered by the easiest to use, drag-and-drop management interface in the industry. This improves the way you manage delivery of application services to your end users, saves valuable IT time, and maximizes ROI.

Ixia Solutions Enhance your Network Monitoring Capabilities

The next prong of the approach is to optimize your visibility architecture to meet your monitoring needs. What kind of data do you need? How will your systems process and consume the data? How does the visibility architecture help you optimize the security architecture? Once you know the answer to these questions, you can implement the following steps.

Build the Proper Monitoring Architecture to Support Your Security Needs

Today's networks are growing in both size and complexity, presenting new challenges for IT and network administrators. More mobile devices are now connecting to more data from more sources—and much of that is due to virtualization. IT challenges are further complicated by increasingly high customer expectations for always-on access and immediate application response. This complexity creates network "blind spots" where latent errors germinate, and pre-attack activity lurks.

Blind spots are commonly caused by the following issues: lack of SPAN and tap ports, which limit tool access to data; dropped and duplicated packets, which suppress or delay actionable information; and monitoring plans that are behind migration cycles. Stressed-out monitoring systems make it hard, if not impossible, to keep up with traffic and filter data "noise" at a rate that they were not designed to handle.

Network blind spots have become a costly and risk-filled challenge for network operators. Further, unseen inter-VM and cross-blade data center traffic leaves the network vulnerable to threats, noncompliance, loss of availability, and impaired performance. Today, up to 80 percent of data center traffic can travel between servers, making end-to-end visibility a real challenge.

The answer to these challenges is a highly scalable visibility architecture that helps eliminate blind spots, while providing resilience and control without complexity. Ixia's Visibility Architecture delivers a new, flexible perspective on network visibility. This architecture is detailed in other Ixia documentation but it basically consists of four layers:

- **Network Access –** This can be accomplished through SPANs or taps. Taps are suggested as they limit duplicate packets, don't summarize data, and don't affect timestamps – but you can use either access method.
- **Data Control –** This is accomplished through NPBs that can perform various functions like: filter out unnecessary data packets, de-duplicate packets, conduct packet slicing, load-balance data to monitoring tools, and aggregate data streams.
- **Application Intelligence –** This capability allows you to harness higher-level capability from your monitoring data such as: deep packet inspection (DPI) and specialized capabilities for verticalized markets (GTP session filtering, financial data monitoring, etc.).
- **Management –** Graphical user interfaces that simplify the ability to manage components, set up filter rules, and understand how your monitoring components interconnect make the management of the monitoring ease, which keeps costs low.

The Ixia Visibility Architecture enables you to combine different components to create the right solution for your needs.

Gauge Your Realistic Level of Commitment/Execution to Create In-Line Monitoring or Out-of-Band Monitoring Architectures

One of the most important elements for the design of the combined visibility and security architecture is to gauge your realistic level of commitment and execution. While everyone wants to say that they would be totally proactive in stopping every security attack exactly as it happens, to enable this philosophy can become quite expensive – both in terms of capital expenditures and also in personnel costs. This is where you'll want to decide on your ability to realistically execute a philosophy and whether you want to create in-line monitoring, out-of-band monitoring, high availability solutions, or all of them.

The first question to resolve is: will your monitoring solution be based on in-line or out-of-band monitoring? These solutions have different goals. In-line monitoring is designed for those that want to be proactive in regards to security threats and know right away that an attack is happening and defend against it. Out-of-band is a more reactive approach that is designed for those that don't have resources or budget to be able to react in real-time to security threats, but still want to defend their network as quickly and thoroughly as possible.

In-line appliances sit in the flow of live network traffic, close to endpoints that access the network. Client-side traffic into and out-of the network passes through them. As such, they are able to directly provide both pre-connect and post-connect security services. Because they are analyzing and passing live network traffic, in-line devices act as the enforcement point rather than relying on another network system. This analysis and enforcement offers major performance advantages and are thus much more effective in thwarting the spread of malware or malicious attacks.

In regards, to security monitoring, in-line solutions allow you new possibilities. You can either stop the threat vector in real-time as you discover it or you can divert it to a honeypot so that you can study the attack to learn how to better defend against it.

Out-of-band refers to the fact that the equipment is located further into the network. You can still use the components to analyze what's happening on your network, but the location of the equipment prevents the ability to perform any real-time filtering or diversion of data before it enters the main network. Typical use-cases for this type of monitoring from a security perspective center around: data recording, forensic analysis, anomaly analysis, and interaction with SIEMs. Using an out-of-band architecture will still let you know that an attack happened so that you can limit the amount of damage and also learn about the threat vectors used to attack your network.

Both approaches have advantages and drawbacks, and some combination of the two maybe necessary – depending upon your security objectives and budget.

Determine if You Need Layer 7 DPI to Validate Security Policies

One of the biggest challenges facing network administrators is complete network visibility that extends past Layer 4 information. Many applications today run over HTTP within your network or cloud infrastructure, and thus can be obscured. Application intelligence within a monitoring context provides expanded visibility that gives you deep knowledge of your network, including application bandwidth and geo-location of application traffic.

The question to ask yourself here is do you need Layer 7 application information and DPI to validate security policies (i.e., BYOD, role-based access, malware analysis of email attachments, control of customer data, etc.)? If so, the Ixia ATI Processor appliance can collect information on the signatures of applications running on your network, the bandwidth being consumed, geo-location of traffic, device type in use, browser type in use, as well as other information. This information is accessed using a native interface or sent downstream using NetFlow to your monitoring tools for analysis.

The application-level information can help you determine the effectiveness of some of your security policies. For instance:

- What types of device are running on your network and does this conform to your BYOD policy?
- How and where is your network being accessed and does this conform to your role-based access?
- Are your policies on the downloading of attachments and the malware analysis of email attachments effective or are users bypassing this policy by using applications for email that circumvent this?

No matter how you design your monitoring solution, you can use Ixia solutions to apply consistent processes across the network. Once the access medium (e.g. physical, virtual, copper, fiber, etc.) is resolved, you can forward consistent sets of data to the packet brokers, which filter, de-duplicate, and segment data as needed before sending it on to your monitoring tools for analysis.

For more information on overcoming blind spots in the virtualized environment, see Ixia's white paper *Illuminating Data Center Blind Spots* (http://info.ixiacom.com/Illuminating_Data_Center_Blind_Spots_LP_A.html)

Ixia Solutions to Enhance your Network Monitoring Capabilities

Ixia Solution	Image	Description
Ixia Net Optics Taps		Provides 100 percent visibility and permanent passive access points into your network – from 10/100Mb to 100GbE. When a monitoring tool is needed, simply connect the device to the tap instead of taking down the link and interrupting traffic. Taps pass all network traffic – including Layer 1 and 2 errors – without introducing bottlenecks or points of failure. Taps include: • **Net Optics Flex Tap™ family –** delivers total traffic visibility for network monitoring and security tools • **Net Optics Fiber Tap HD8 –** optimized and tested for high-performance fiber networks, is available in single-mode and multimode fiber, and supports passive monitoring and 24x7 reliability • **Slim Tap –** all-optical design is optimized for high-performance fiber networks and is 100 percent passive and easily removable • **Phantom vTap™ –** software solution that supports all leading hypervisors (VMware vSphere, Microsoft Hyper-V, Citrix XenServer) to provide 100% visibility of virtual traffic • **iBypass –** inline solution that protects full duplex network links from unexpected outages
Ixia Packet Brokers		Compact, hardware-based, rack-mounted devices that offer a new approach for handling and manipulating network packets. NPBs optimize the access and visibility of traffic from one or many network links to monitoring, security, and acceleration tools, up to 100GbE connections. • **NTO –** The Ixia portfolio of NTO network monitoring switches, also known as network packet brokers, provides complete visibility into physical and virtual networks, improves network security, and optimizes monitoring tool performance • **xStream –** This integrated platform advances the performance and reliability edge for customer networks, plus eases management with smooth navigation, exporting, and configuration capabilities
Ixia Application and Threat Intelligence (ATI) Processor		Delivers real-time application data to monitoring tools, empowering users to make better decisions with better data. It provides rich data on behavior and location of users and applications, in any format needed – raw packets, filtered packets, or metadata. This allows IT teams to identify unknown network applications, mitigate network security threats from suspicious applications and locations, and spot trends in application usage to predict and forestall congestion.
Ixia NTO Packet Capture Module (PCM)		Provides built-in, single-UI packet capture and Wireshark decode monitoring capability for quick troubleshooting of performance, security, and availability problems. The combined packet capture and packet decoding capability results in an extremely fast MTTR.

Ixia Solutions Improve Your Operational Readiness While Controlling Costs

The last prong to protecting your network security is to optimize your operational readiness to counter attacks. As discussed, the extent of your security and visibility architecture is dependent upon your budget, so cost controls come into play here as well. The more you optimize and control costs, the more budget is left to implement your security strategy. Ixia solutions help you achieve the following in this endeavor.

Create Resilience within Your Blended Security and Visibility Architectures

Security is all about reducing the risks posed by endpoint clients (PCs, laptops, remote systems, and mobile devices) connecting to the internal enterprise network. Security enforcement is becoming a critical business initiative as the network perimeter dissolves and as organizations open up their internal LANs to guests, contractors, and business partners.

A crucial component to network security is operational readiness to prevent or mitigate damage before, during, and after an attack. Per a previous discussion, Ixia in-line and out-of-band monitoring solutions will be key components to recognizing an attack. These solutions will enable your security tools like a FireEye device to recognize threats and let you know that something is happening.

Another product like the Ixia ATI Processor can help you form a sort of early warning system, especially when the product is combined with a Splunk dashboard. For instance, the ATI Processor has real-time geo-location capabilities that can let you know that a user in a foreign country is using one of your FTP servers in Dallas, TX to transfer files. With geo-location information that includes a network map, you can easily see that you have no legitimate users in that foreign country. While this doesn't tell you that a security breach is in progress, it does give you advance information that something is happening so that you can investigate further while the incident is happening. Again, it's about giving you access to information, when you need it so that you can make proper decisions.

Other Ixia solutions enable troubleshooting and triage. One example is the Ixia NTO Packet Capture Module (PCM). IT engineers need the ability to capture the packets associated with a network anomaly and/or problem, and then quickly analyze the packets to come up with a fast solution. When time to resolution is of the essence, this can be a powerful product in solving problems.

The Ixia PCM lets you create PCAPs so that you can quickly analyze point problems and anomalies. Not only can the target packets be captured, but a circular buffer window within the PCM provides the ability to automatically retain packets preceding the trigger point (i.e., captures what's still in the buffer) and then the desired packets after that point. This pre-event information is often a life saver in reducing the time to diagnosis. Using the built-in packet decoder, you can quickly see and understand network problems and events without ever leaving the user interface.

Finally, when testing to identify the source of a problem or current incursion, you need the ability to iteratively test against the current security configuration to methodically rule out options and hone in on the current problem. With Ixia's BreakingPoint application and security test solution you can perform iterative testing to help determine the root cause of security problems.

Effectively Control Costs with the Right Visibility and Security Solution

Using a holistic process that combines the right visibility and security solution allows you to effectively control costs. This is particularly due to the use of network packet brokers, which have been shown to reduce MTTR, increase ROI, and decrease the total cost of ownership (TCO). In fact, Ixia has an ROI calculator that can demonstrate the ROI for NPB-based solutions. For instance, MTTR times can be reduced from days to hours. Filtering rules are also implemented visually, which also saves lots of time, aggravation, and money, especially when compared to command line interfaces.

The Ixia BreakingPoint solution can help decrease your operational costs as well. It not only tests your architecture components but your security architecture as well to see how your network will react to DDoS attacks, malware, and high loads. By testing your network and its components ahead of time, you'll get data to help you reduce configuration time and costs.

In addition, BreakingPoint is powered with automatic updates from the ATI subscription service, ensuring that your security validation system is updated with the latest defenses while eliminating the need for IT staff to keep abreast of each new virus or malware.

Use Your Architecture to Better-Enable Business Objectives

Lastly, you can use your Ixia-based architecture to better-enable business objectives. For instance, vendor consolidation reduces overhead costs to your organization. Ixia has a plethora of products and solutions to help you not only optimize your technical requirements for your security architecture but your financial requirements as well.

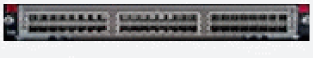
Ixia solutions can also help you to more-effectively demonstrate regulatory compliance. For instance, documenting regulatory compliance in a virtual environment can be a difficult task. The Ixia Phantom vTap gives you the access you need to your virtualized data traffic so that it can be sent to a monitoring tool for analysis to determine if there might be compliance issues. NPBs are also a key element to capturing and filtering proper regulatory compliance data and then forwarding that data on to the appropriate tools, like LogRhythm for example.

NPBs and taps also enable proper lawful intercept. Lawfully intercept within the enterprise is becoming more common. If your organization is asked to support lawful intercept captures, you need a solution that can faithfully deliver that information. At the same time, you don't want to have to spend additional money to modify your architecture just for this request. You want a solution that can handle this requirement along with all of your other requirements as an integrated, cost-effective solution.

For more information on In-line and out-of-band security tool placement and improving operational response capabilities, see Ixia's white paper *The Real Secret to Securing Your Network* (http://info.ixiacom.com/The_Real_Secret_to_Securing_Your_Network_White_Paper.html)

Ixia Solutions to Improve Your Operational Readiness While Controlling Costs

Ixia Solution	Image	Description
Ixia Net Optics Taps		Provides 100 percent visibility and permanent passive access points into your network – from 10/100Mb to 100GbE. When a monitoring tool is needed, simply connect the device to the tap instead of taking down the link and interrupting traffic. Taps pass all network traffic – including Layer 1 and 2 errors – without introducing bottlenecks or points of failure. Taps include: • **Net Optics Flex Tap™ family –** delivers total traffic visibility for network monitoring and security tools • **Net Optics Fiber Tap HD8 –** optimized and tested for high-performance fiber networks, is available in single-mode and multimode fiber, and supports passive monitoring and 24x7 reliability • **Slim Tap –** all-optical design is optimized for high-performance fiber networks and is 100 percent passive and easily removable • **Phantom vTap™ –** software solution that supports all leading hypervisors (VMware vSphere, Microsoft Hyper-V, Citrix XenServer) to provide 100% visibility of virtual traffic • **iBypass –** inline solution that protects full duplex network links from unexpected outages

Ixia Solution	Image	Description
Ixia Packet Brokers		Compact, hardware-based, rack-mounted devices that offer a new approach for handling and manipulating network packets. NPBs optimize the access and visibility of traffic from one or many network links to monitoring, security, and acceleration tools, up to 100GbE connections. • **NTO –** The Ixia portfolio of NTO network monitoring switches, also known as network packet brokers, provides complete visibility into physical and virtual networks, improves network security, and optimizes monitoring tool performance • **xStream –** This integrated platform advances the performance and reliability edge for customer networks, plus eases management with smooth navigation, exporting, and configuration capabilities
Ixia Application and Threat Intelligence (ATI) Processor		Delivers real-time application data to monitoring tools, empowering users to make better decisions with better data. It provides rich data on behavior and location of users and applications, in any format needed – raw packets, filtered packets, or metadata. This allows IT teams to identify unknown network applications, mitigate network security threats from suspicious applications and locations, and spot trends in application usage to predict and forestall congestion.
Ixia NTO Packet Capture Module (PCM)		Provides built-in, single-UI packet capture and Wireshark decode monitoring capability for quick troubleshooting of performance, security, and availability problems. The combined packet capture and packet decoding capability results in an extremely fast MTTR.
Ixia BreakingPoint		Validate next-gen firewall, IPS, and other security devices with this industry-leading application and security test platform. It simulates an authentic, customized blend of stateful application traffic combined with live security attacks and massive-scale user load. You can easily create the actual behavior of millions of wired and wireless users, hundreds of applications, and tens of thousands of security attacks to validate, optimize, and benchmark the latest security gear.

Summary

As your network continues to face the dangers of cyber attacks, internal breaches, and even careless employees, you'll want to use a comprehensive, multi-dimensional approach to network security. But due to the complexity and fast-evolving nature of network security, you need to adopt the attitude that security isn't something you purchase, but something you actively do – everyday. Ixia is the company that can enable you at every point along this migration path.

We are prepared with the technology solutions, expertise, and training you need to strengthen and protect your network and ensure ongoing security resiliency. With Ixia solutions you will:

- Better understand our network and how it works
- Discover the weaknesses of your security solutions and strengthen them
- Measure and improve the ability of your personnel to fend-off and recover from an attack
- Get the right network data to the right tools at the right time
- Gain visibility into network blind spots
- Improve operational readiness for countering attacks
- Optimize devices and processes to cut costs and improve performance

Ixia understands the need to secure the enterprise, the ramifications of what happens when a breach occurs, and the realities of IT budgets in a fast-changing world. Contact us today to see how we can help.

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
21 Serangoon North Avenue 5
#04-01
Singapore 554864

Sales +65.6332.0125
Fax +65.6332.0127