WHITE PAPER

The Model for Deploying and Integrating Network Security and Monitoring Tools

INTRODUCTION

Over the years, information technology (IT) departments have been implementing solutions that answer two questions:

- How do I make as many services available to stakeholders as possible?
- How do I protect and secure everything?

While some IT departments approach these questions as a dual mandate, others treat them as mutually exclusive. Many times, new technologies are so powerful or transformative to a business that they simply have to be used immediately. Sometimes, compromises around security have to be negotiated between the business and IT. Other times, the benefits of new technology simply overrule IT security.

Cloud, virtualization, and mobility brought a wave of vendors offering point solutions with benefits such as scalability and efficiency. At the same time, the number of security vendors offering different types of protection exploded. While new trends in IT have increased availability and access to services, it has also shattered the traditional network boundary—data and assets no longer sit in a single location behind a firewall. As a result, many enterprises have erred on the side of *there is no such thing as too much security*, especially with the increased frequency and sophistication of attacks. Today, the average large enterprise uses 32 security vendors in the fight to protect itself.[1]

> Today, the average large enterprise uses 32 security vendors in the fight to protect itself.
> — ZK Research, 2015

[1] 2015. ZK Research Security Survey.

With company data everywhere and a slew of security products and network monitoring tools already deployed, enterprises are now asking if there is a way to get more out of these investments. A way not only to get access to data no matter where it is, but also to provide security tools with needs-based access to all, some, or none of the data, in the format it can use. There is a way. It is called the Ixia Security Fabric and it turns network security and intelligence into a cohesive unit to fend off the threats facing enterprises.

The Digital Warfare Attackers Are Waging

Protecting data and IT assets is more challenging partly because attackers employ more sophisticated methods to get around enterprise security. Some of these attacks hide within encrypted communications and Gartner predicts this technique will represent more than half of network attacks in 2017.[*] Here are some common weapons in a hacker's arsenal and how they use them.

Malware - Malicious software that comes in many different forms. Many malware instances morph or are regenerated daily so they can avoid signature-based detection systems.

Phishing - an attack where seemingly valid emails are sent to unsuspecting users in an attempt to trick the user into clicking on an embedded link in the email. Phishing emails typically appear to be from valid senders, such as an employer or the user's bank. When the recipient follows a link, they are then prompted to enter sensitive information or malware is pushed down to their system.

Botnet - an orchestrated army of infected hosts that unknowingly participate in malicious campaigns under the control of a botnet herder or controller. The botnet controllers communicate with these infected hosts using "Command and Control (C2)" connections, which can be sent over many different common protocols such as IRC, HTTP, DNS, and others. They are typically encrypted to avoid detection. Botnet controllers send commands to infected hosts directing them to leak sensitive data, download additional malware, or attack other targets in a DDoS attack.

Exploit - Hackers often conduct large-scale reconnaissance, looking for hosts with exposed vulnerabilities. Many services have to be advertised to the Internet in order to conduct business such as HTTP/HTTPS, SSH, VoIP, RDP, VPN, and others. Vulnerabilities are discovered over time in the software packages which advertise these services and hackers are constantly scanning for sites which run vulnerable services.

Hijacked IP Ranges - are stolen from their legitimate owners, typically by corrupting the routing tables of Internet backbone routers. Once hijacked, they are used for malicious purposes such as phishing and malware distribution.

Distributed Denial of Service (DDoS) - an orchestrated attack from hundreds or thousands of sources that flood a target with so much needless traffic that it cannot process legitimate traffic. DDoS attacks aim to disrupt and overload a system to bring it down or to impair network security from properly protecting the network. Some DDoS attacks are used as a smoke screen for data theft.

Advanced Persistent Threat (APT) - a network attack where the goal is to get into a network and stay there, undetected, for a long time. The purpose is to steal data rather than do damage. It usually starts with an attacker gaining access and then establishing a back door so he can come and go easily. Once inside, the attacker attempts to gain access to other systems and networks and opens more back doors. Malware is spread inside the network to collect data and then it is exfiltrated through the numerous back doors.

[*] D'Hoinne, Jeremy, and Adam Hils. "Security Leaders Must Address Threats from Rising SSL Traffic." Gartner. December 9, 2013. https://www.gartner.com/doc/2635018/security-leaders-address-threats-rising

IT TRENDS

New trends in IT such as cloud and virtualization combined with workforce mobility and globalization means businesses must protect themselves from all angles. Data centers are now distributed and new technology trends are forcing companies to extend their network edge—often into places where they cannot easily gain visibility to the traffic they need to monitor. This causes blind spots, which rapidly become havens for security attacks.

- **The Mobile Employee** - Modern employees are no longer tethered to the office. They use an array of mobile devices for both personal and professional purposes, blurring the line between home and work. As a result, employees are downloading their own applications to their devices, beyond what was part of the corporate standard issue. In some cases, this means trusted and untrusted applications run side-by-side, dangerously close to sensitive data that might exist on the mobile device. While IT is trying valiantly to retain control, the reality is that risks become harder to identify. Gartner predicts that by 2018, 25% of corporate data traffic will bypass traditional security defenses and flow directly from mobile devices to the cloud.[2]
- **The Cloud** - As businesses migrate workloads from their private data center to public clouds, applications and data no longer have a permanent home. While the cloud offers unprecedented flexibility, it also expands the perimeter. Data, sensitive or not, are being sent to the cloud, worked on in the cloud, and stored in the cloud. In fact, according to Forbes, cloud applications will account for 90% of worldwide mobile data traffic by 2019.[3] And enterprises are not just using one cloud or one application in the cloud. More and more, enterprises are embracing software-as-a-service (SaaS) for functions like accounting, payroll, and human resources. More than 40% of businesses use five or more cloud providers[4] and the average company uses between 10 and 16 off-the-shelf cloud applications.[5]
- **The Internet of Things** - IoT is transforming off-line or manual functions into devices that are now connected to the network and share information. This happens often with little to no security oversight. Whether it is IoT devices like security cameras or production automation, IT security has more network connections to manage and more data in transit to monitor. In 2016, Gartner

[2] Gartner. 2013. "Gartner, Predicts 2014: CSPs' Opportunities and Challenges Will Arise from Cloud Computing and Mobility Trends." G00250687. November. https://www.gartner.com/doc/2630416/predicts--csps-opportunities-challenges

[3] Columbus, Louis. "Roundup of Cloud Computing Forecasts and Market Estimates Q3 Update, 2015," Forbes. September 27, 2015. Accessed September 21, 2016. http://www.forbes.com/sites/louiscolumbus/2015/09/27/roundup-of-cloud-computing-forecasts-and-market-estimates-q3-update-2015/#dc1e8ae6c7ad

[4] Verizon. 2016. "State of the Market: Enterprise Cloud 2016. http://www.verizonenterprise.com/resources/reports/rp_state-of-the-market-enterprise-cloud-2016_en_xg.pdf

[5] Business @ Work." Okta. March 2016. Accessed September 21, 2016. https://www.okta.com/Businesses-At-Work/2016-03/

expects 5.5 million new IoT devices will get connected every day.[6] By 2020, every person on the planet will create about 150GB of new data every day.[7]

THE CHALLENGES OF SECURING ENTERPRISE NETWORKS

Businesses are using a complex array of multi-vendor appliances and threat analysis tools to protect, secure, and analyze network traffic. Choosing between them, integrating them successfully, and monitoring them effectively has become a significant network visibility challenge. With traffic volumes and threats increasing, the number of security tools that need access to a reliable stream of data is also growing.

- **Inline Security** - The key to successful inline security monitoring is to enable active, real-time traffic inspection and detection without impacting network and application availability. This methodology is designed for proactive threat prevention. If one of your security tools becomes congested or fails, you need to keep traffic moving, continue monitoring, and prevent a network or application outage. Some organizations deploy their inline security appliances behind the firewall in a serial configuration. With this design, if an appliance becomes congested or fails, traffic stops. Redundant network paths can help avoid this, but they require twice the number of tools. Ensuring both paths can handle the full volume of traffic is expensive and leaves tools on the inactive path under-utilized during normal operations. Examples of typical inline security tools include the following:
    - Intrusion prevention systems (IPS)
    - Firewalls and next-generation firewalls (NGFWs)
    - Data loss prevention (DLP) systems
    - Unified threat management (UTM) systems
    - SSL decryption appliances
    - Web application firewalls (WAF)
- **Out-of-Band Security** - The key to successful out-of-band security monitoring is to enable passive traffic inspection, detection, and recording for routine analysis. This methodology is useful for delivering key information to your security tools for detailed threat analysis. Either a standard network tap, a virtual tap, or a network switch port is converted to a SPAN to gain access to network data from different points in the network. Some organizations directly connect out-of-band security appliances to a tap or SPAN port, but this greatly reduces scalability when there are more network segments that need monitoring than ports on a tool. Examples of typical out-of-band security tools include the following:

[6] Gartner. 2015. “Gartner Says 6.4 Billion Connected ‘Things’ Will Be in Use in 2016, Up 30 Percent from 2015.” Press Release. November. http://www.gartner.com/newsroom/id/3165317

[7] Marr, Bernard. 2015. “Big Data: 20 Mind-Boggling Facts Everyone Must Read.” Forbes. September 30, 2015. http://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#51506a916c1d

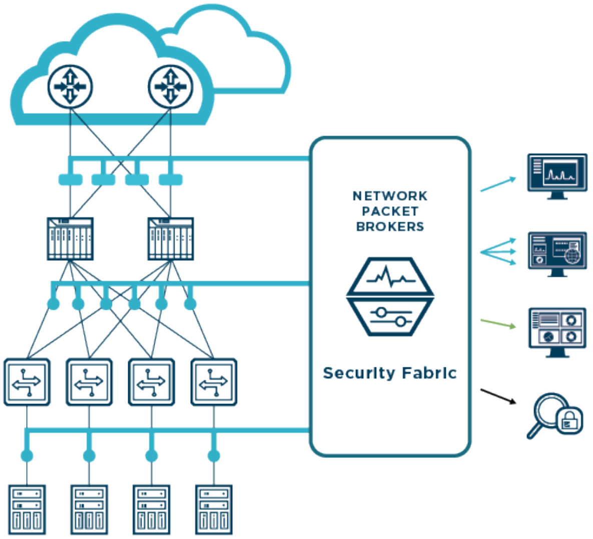
- Security Information and Event Management (SIEM) systems
- Intrusion Detection Systems (IDS)
- Behavior analysis systems
- Forensic tools
- Data recording
- Malware analysis tools
- Log management systems
- Packet capture tools

HOW TO PREPARE ENTERPRISE NETWORKS FOR STRONGER PROTECTION

Organizations today are moving away from connecting security tools directly to tap or SPAN ports. Instead, they are connecting a security delivery platform to taps, SPAN ports, and bypass switches and connecting security appliances and tools to the platform. This is a better solution because it enables both failsafe deployment and provides a stable foundation for any number of network and security tools. At Ixia, we call this platform a Security Fabric.

Modern network architecture provides multiple paths through the network to increase network reliability. Using virtualization and cloud resources to run workloads creates a high amount of east-west traffic that may never touch a touch a physical link. Both of these realities create a challenge for effective monitoring. Security tools need all data from a session to perform an accurate analysis. A Security Fabric addresses this need by aggregating traffic from multiple physical and virtual links, essentially stitching it together, to provide a more complete view to your security tools, which improves inspection, detection, and protection.

The goal of a Security Fabric is to provide your security tools with the specific type of traffic they are designed to monitor, no matter where that traffic is in your network. It is about protecting your network from both internal and external threats. A Security Fabric combines 100% data access, resilience, and intelligence to reduce the load for the enterprise security team by ensuring the right data gets to the right tools, every time, even at high speeds.



THE IXIA SECURITY FABRIC™

The Ixia Security Fabric delivers complete, end-to-end visibility for both inline and out-of-band security tools all in one solution. Some security tools need to see all data, while others only a subset. But they all need safeguards to ensure alternate paths exist in case of single tool outages. With the Ixia Security Fabric, you increase the effectiveness of analytics and security tools and optimize their data access.

Why graphical configuration is superior to command line

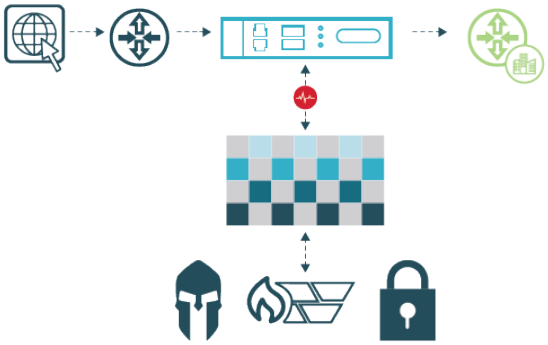
As you configure connections and define filters in any visibility platform, management and control can quickly become complex, especially when there are many traffic sources and many tools. You want to distribute only relevant data to your tools—not the traffic it does not need. For example, you may want to send a certain monitoring tool only VLAN 100, 200, 201, and 300 traffic in addition to HTTP traffic, HTTPS traffic, and email traffic. This is an overlapping filter. With CLI, filtering traffic to these dimensions might not be cumbersome—if you only have one tool and one data source. What if you have hundreds of data sources and many tools? CLI can quickly consume you during initial setup and overwhelm the team responsible for managing it going forward. It is also prone to mistakes and errors you may not uncover until you perform analysis. By then, it is too late. With the Ixia Security Fabric, you configure and manage data sources and tools using an intuitive and powerful drag-and-drop interface. You have complete, granular control of your data and the patented compiler automatically creates and updates simple filters, overlapping filters, and dynamic filters behind the scenes. This ensures every type of packet you want delivered to a security tool gets there. With the Ixia Security Fabric, you visually see the connections and the data no matter if you have one data source going to multiple tools or multiple data sources going to one tool—regardless of how you filter traffic.

The Ixia Security Fabric strengthens security, but does not allow security monitoring to slow or disrupt network response times. It comes down to security-aware, intelligent data handling in live operation. While 100% reliable data access is crucial, it is just the start. The Ixia Security Fabric's real strength comes from providing context-awareness and security intelligence to the data flows and distributing relevant traffic to your network security and monitoring tools. It is also a breeze to configure and manage.

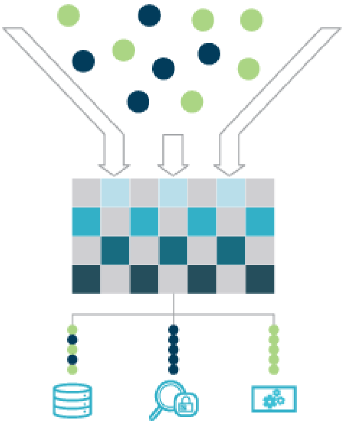
The Ixia Security Fabric has four layers, each adding a critical element to create a powerful visibility engine for your security appliances and network monitoring appliances and network monitoring tools.

Data Access Anywhere - To get security tools the data they need, data access is critical. This can be done with physical and virtual taps or by converting a switch port to a SPAN port on a network switch. While using SPAN ports can be effective, they do have limitations. SPAN ports can only mirror traffic that passes through a network switch. If the network switch gets busy, the switch will drop packets on SPAN ports in favor of processing live traffic on switch ports. On the other hand, taps are a passive splitting mechanism placed between two network devices. A tap does not introduce delay and is unaffected by bandwidth saturation. It duplicates all traffic on the link (including MAC and media errors) and forwards it to the Security Fabric's processing engines.

Security Resilience - To achieve security resilience for inline (or in-band) security tools, deployment requires maximizing availability and minimizing the impact from a failure. This is done with an external bypass switch that constantly monitors ports and paths and can automatically route around security tools at nanosecond speeds when traffic congestion, security tool failures, or security tool maintenance happens. To monitor every tool and path, Ixia Security Fabric uses regular and negative heartbeats. Regular heartbeats are injected into

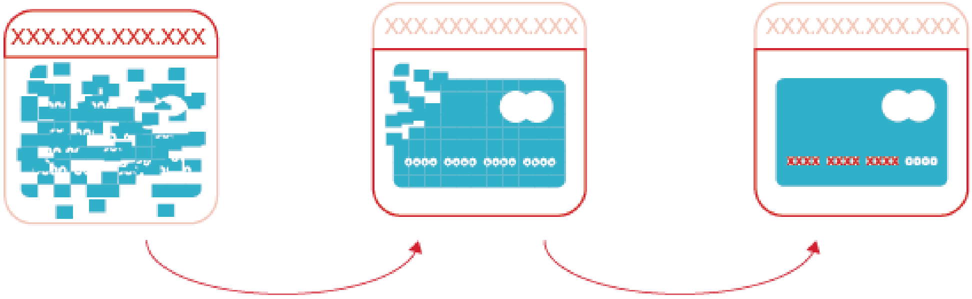


the normal data stream to see if a path or device is alive. Negative heartbeats are injected to see if the security device, like a firewall, is functioning properly and blocking bad traffic. Ixia bypass switches also have the ability to fail open to ensure continued network availability or fail closed and block access to the network. When high availability is a requirement, the Ixia Security Fabric supports serial or parallel high availability and uses synchronous configuration and load balancing to ensure fully redundant security with near instant failover.



Context-Aware Data Processing - To get the right data to the right security tools, the Ixia Security Fabric uses intelligent data processing to recognize rich metadata and deliver enhanced NetFlow information. This goes deeper than source and destination ports and IP addresses. Context-awareness requires a deep understanding of network traffic based on applications, devices, sessions, conversations, and geolocation and knowing which security tools need the data. And when multiple network segments are tapped, the Ixia Security Fabric automatically keeps track of duplicate packets and ensures security tools only get one copy. Context-Aware Data Processing uses both shallow and deep packet inspection to provide rich application awareness and allows you to create granular rules on the traffic forwarded to your security and monitoring tools. With Ixia Security Fabric, over 220 application signatures are already built-in—just point, click, and configure with no cookbooks or scripting necessary.

Security Intelligence Processing - Your security tools are already working hard enough. With Security Intelligence Processing, you can free your security tools to focus on suspicious traffic analysis. It starts with seeing all of the data, clear or encrypted. Decryption inside the Security Fabric allows data to be identified and intelligently distributed to security tools. It saves security tools from processor intensive decryption and helps avoid blind spots as some



security tools do not have decryption capabilities. Security intelligence also means supporting data compliance. Ixia's Security Fabric has the capability to strip off header data containing sensitive information or mask personally identifiable information such as credit cards or social security numbers before passing the data to network monitoring and security analysis tools. This is vital for compliance and to avoid penalties and fines. With an Ixia Security Fabric, security intelligence goes beyond other visibility solutions. Using a threat intelligence feed, you can remove known bad traffic from ever entering your network. The Ixia Security Fabric's threat intelligence gateway analyzes a packet's IP address and compares it to a database of IP addresses known to distribute malware, viruses, and other attacks. Removing this known bad traffic can help relieve security tools from inspecting and blocking this traffic by up to 35%[8] and reduce the SIEM alerts by up to 80%[9].

SUMMARY

Network security monitoring requires processing and examining data that is exploding within a perimeter that is expanding. Hackers and the tools they use to infiltrate enterprise networks and exfiltrate company secrets are more sophisticated than ever. As a result, many organizations are using more security and network monitoring tools to spot threats and protect their business. This requires a deployment and integration model for inline and out-of-band security tools to integrate them properly and get the most out of their capabilities.

The Ixia Security Fabric is a powerful network visibility engine that ensures resilient traffic delivery to enterprise security, compliance, and analytics tools. Ixia's Security Fabric is the foundation for stronger inline and out-of-band security deployments. With context-aware and security intelligence data processing engines, the Ixia Security Fabric delivers only relevant, de-duplicated traffic to your network security and monitoring tools.

Find out more about the Ixia Security Fabric at www.ixiacom.com/securityfabric.

[8] Based on the amount of traffic on a customer's network that is considered "low-risk," such as voice and video traffic, which an IPS typically does not need to screen. Ixia internal analysis. 2016.

[9] Ixia. 2016. Hyper Box Tackles Attack Traffic with Ixia ThreatARMOR. "The number of intrusions detected by the IDSs decreased from 1M to 200K cases." Case Study.

WORLDWIDE HEADQUARTERS

26601 W. Agoura Road
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

EUROPEAN HEADQUARTERS

Ixia Technologies Europe LTD
Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

ASIA PACIFIC HEADQUARTERS

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127