What is a Network Packet Broker?

(AND WHY DO YOU NEED ONE)

Keeping networks safe, and users thriving amidst the relentless flux requires a host of sophisticated tools performing real-time analysis. Your monitoring infrastructure might feature network and application performance monitors (NPM/APM), data recorders, and traditional network analyzers, while your defenses leverage firewalls, intrusion prevention systems (IPS), data loss prevention (DLP), anti-malware, and other point solutions.

However specialized security and monitoring tools may be, they all have two things in common:

- They need to know exactly what's happening in the network
- Their output is only as good as the data they receive

30%
of survey respondents were not confident analysis tools are receiving all the data needed

35%
cited SPAN/tap shortages as the #1 reason they can't monitor 100% of segments[1]

A 2016 survey conducted by Enterprise Management Associates (EMA) found nearly 30 percent of respondents were not confident that their tools were receiving all the data they required. This equates to having blinds spots in the network and ultimately to wasted effort, redundant cost, and a higher risk of being hacked.

The visibility needed to avoid waste and blind spots starts with collecting data about what's taking place across your network. Network taps and mirror ports on network equipment—also known as switched port analyzer or SPAN ports—create access points for capturing traffic for analysis.

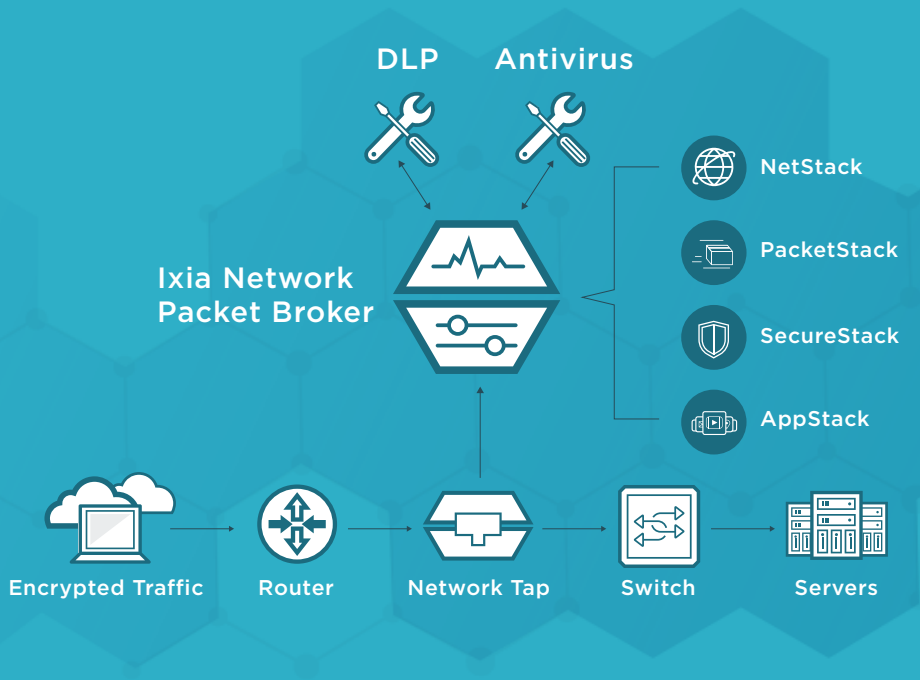
This can be considered the "easy part." The real challenge lies in efficiently funneling data from the network to each tool that needs it. If you only have a few network segments, and relatively few analysis tools, the two may be connected directly. More often, 1:1 connections may pose a management nightmare that becomes unwieldly, if not logistically impossible as the network grows.

EMA reported that 35 percent of organizations cited a shortage of SPAN ports and taps as the primary reason they were unable to monitor 100% of their network segments. Ports on high-end analysis tools, such as firewalls, may also be in even shorter supply, and it is critical not to overtax devices to the point of compromising performance.

" Packet loss in a network visibility tool should be unacceptable. Visibility is supposed to enable clear insight into network data, not degrade the data that the analytics tools require."

TOLLY

[1] Enterprise Management Associates, 2016



Why Do I Need NPBs?

NPBs are installed between taps and SPAN ports used to access network data and sophisticated security and monitoring tools that typically reside in data centers. Network packet brokers do just what their name says: they broker network packet data to ensure every analysis tool sees exactly the data it needs to perform at the highest possible level.

The NPB adds an increasingly critical layer of intelligence—one that reduces cost and complexity to help you achieve:

Better data for better decisions

A fabric of packet brokers with advanced filtering capabilities serves to organize and streamline data for your monitoring, performance, and security tools.

Tighter security

It is hard to stop threats when you do not see them coming. NPBs work to assure that your firewalls, IPSs, and other defenses see exactly the right data, all of the time.

Faster problem resolution

Zeus Kerravala, Principal Analyst at ZK Research observes, "Problem identification is IT's biggest challenge" with up to 85% of mean time to repair (MTTR) spent simply identifying that there is, in fact, an issue. Downtime is money, and starting down the wrong path can have devastating effects for your business.

Context-aware filtering provided by NPBs helps you detect and determine the root cause of issues faster by introducing advanced application intelligence. Ixia's robust Security Fabric™ leverages this intelligence to speed up troubleshooting by providing insight into the geographic location of outages and the vendors that may be causing disruptions.

5 WAYS TO IMPROVE ROI WITH PACKET BROKERS

- Speed troubleshooting
- Detect breaches faster
- Reduce burden on security tools
- Extend the life of monitoring tools during upgrades
- Streamline regulatory compliance

"Infrastructure leaders should reprioritize network visibility and invest in tools to aid such insight. If the network budget is a challenge, pull funding from security and application teams, as visibility provides direct benefits for them."

Gartner Research Note: "Avoid These 'Bottom Ten' Networking Worst Practices," December 2015, refreshed April 2017

Increased proactivity

The use of metadata, provided through NetFlow by intelligent NPBs, also aids in accessing the empirical data used to manage bandwidth usage, trending, and growth, and thus, prevent problems from occurring in the first place.

Better ROI

Intelligent NPBs do not merely aggregate traffic from monitoring points the way a switch might; instead, they filter and groom data to enhance the utilization and the productivity of security and monitoring tools. With only relevant traffic to process, tool performance improves, congestion is reduced, false positives are minimized, and better coverage is achieved using fewer devices.

What Exactly Does the NPB Do?

Conceptually, aggregating, filtering, and delivering data sounds simple. In practice, intelligent NPBs perform very sophisticated functions to produce exponentially higher efficiency and security gains.

One way they do this is by load balancing traffic. For example, if you upgrade your data center network from 1Gbps to 10Gbps, 40Gbps, or higher, NPBs can downshift speeds such that higher-speed traffic can be distributed across a pool of existing lower-speed 1G or 2G monitoring tools for analysis. This extends the value of your current monitoring investments and avoids costly rip-and-replace upgrades as you migrate.

Other powerful features and functions performed by the NPB include:

De-duplicating redundant packets

Analysis and security tools stand to receive a slew of duplicate packets as multiple taps forward traffic. NPBs can eliminate duplicates to keep tools from wasting processing capacity handling redundant data.

SSL Decryption

Secure Socket Layer (SSL) encryption is the standard technology used to safely send private information. However, hackers can also hide malicious cyber-threats within encrypted packets.

Decryption is necessary to inspect this data, but unraveling code takes valuable processing power. Leading packet brokers can offload decryption from security tools to ensure total visibility while easing the burden on high-cost resources.

Data masking

SSL decryption leaves data visible to anyone with access to security and monitoring tools. NPBs can mask sensitive personally identifiable information (PII) such as credit card or Social Security numbers, protected health information (PHI), or other sensitive data, before passing it on so it is not exposed to tools and their administrators.

Protocol header stripping

An NPB may strip out protocol headers such as VLAN, VXLAN, L3VPN, etc. so that tools that are unable to process these protocols can still receive and process packet data. Context-aware visibility helps in spotting rogue applications running on your network and footprints left by attackers as they work their way through your systems and networks.

WHAT TO LOOK FOR IN AN NPB

- Ease-of-use and management
- Intelligence capabilities that remove the burden from your teams
- No dropped packets – 100% reliability while running advanced features
- Architected for high performance

Application and threat intelligence

Early detection of breaches mitigates the loss of sensitive information and the ultimate cost of breaches. Context-aware visibility delivered by NPBs can be used to expose indicators of compromise (IoCs), identify the geolocation of attack vectors, and combat encrypted threats.

Application intelligence extends beyond Layer 2 through 4 (of the OSI model) to Layer 7 (the application layer) of the packet data. Rich data about the behavior and location of users and applications can be created and exported for use in thwarting application layer attacks featuring malicious code masquerading as normal data and valid client requests.

Context-aware visibility helps in spotting rogue applications running on your network and footprints left by attackers as they work their way through your systems and networks.

Application monitoring

Application-aware visibility also has profound implications for performance and management. Maybe you would like to know when employees are using cloud-based services such as Dropbox, or Web-based email to bypass security policies and transfer company files, or when former employees attempt to access files using personal, cloud-based storage services.

NETWORK MONITORING TOOLS FACE OFF

" Using [other vendor's] filters we spent the better part of four hours and some trial and error to get the map and its filters defined and applied. Ixia's smart filtering feature, on the other hand, took all of 10 minutes to perform the same task in our tests."

BRUCE BOARDMAN, NETWORK COMPUTING EDITOR

ixia

Top Four Considerations in Choosing the Right NPB

Assuming the benefits of using NPBs speak for themselves, it should be noted that not all solutions are created equal. Every network visibility solution is different, and the differences may directly impact the security, cost, and efficiency benefits you achieve. Replicating your unique network environment and conducting a head-to-head bake off is the best way to put competing solutions to the test, but before you do that, you can use four key selection criteria to thin the field:

Does it perform as advertised—at all times and at any speed?

According to the Cisco Visual Network Index, Forecast and Methodology: 2015–2020, global Internet Protocol (IP) traffic levels will triple from 72.5EB per month in 2015 to 194.4EB per month in 2020. Network visibility, and networks themselves, will be hard-pressed to keep up.

Since partial visibility may effectively be the equivalent of no visibility at all, you need to look for a zero-loss NPB solution that can perform advanced functions at the vendor's specified line rate. Ixia NPBs are built for performance, architected from the ground up to deliver 100% reliable data processing while performing intelligent filtering, de-duplication, SSL decryption, and other processing-intensive functions.

Make sure to assess performance at a load of 60% or higher. A test conducted by Tolly validated that Ixia NPBs processed 100% of the traffic at every speed while running the most advanced features. By contrast, a competing solution from Gigamon demonstrated packet loss ranging from 20% to nearly 75% at every data size. Worse still, the fact that data had been dropped went unreported.

How robust is the solution architecture?

Purpose-built to perform intensive processing at line rate, Ixia's network packet brokers are optimized with a field-programmable gate array (FPGA), a piece of hardware, that accelerates the packet processing engine of the NPB. This design offers significant architectural benefits and delivers full line-rate performance with a single module for better total cost of ownership (TCO) than the competition, which often requires regular investment in additional modules.

Does it enhance your security?

NPBs are the lynchpin of a robust Security Fabric™, delivering enhanced resilience along with better threat detection. In typical deployments of two redundant tools, one is generally active while the other exists in "standby" mode for ensured resilience. But, this can mean risking that the standby device has failed silently and will not be available to take over when the time comes.

Ixia NPBs can operate in active-active mode, so both nodes are actively working, and each is aware of the traffic being processed by the other. Should one fail, recovery is instantaneous.

REAL-WORLD CASE STUDY

The IT team at the University of Texas (UT) at Austin was using traditional network switches to replicate production traffic back to the monitoring tools. "But we had a problem," the university's chief information security officer reported. "As [traffic] volumes grew, these mirrored flows were exhausting resources on the switches, causing packet drops. Volume was really becoming an issue and dropping packets was simply unacceptable."

Using ixia visibility solutions, the school reduced its intrusion detection system (IDS) capacity demands by 20–30%.

READ THE FULL CASE STUDY

See for Yourself

Any gap in monitoring or security coverage compromises your ability to manage and defend your data centers, networks, and applications. Contact Ixia or your authorized Ixia reseller to conduct a demonstration tailored to your unique needs and challenges and start seeing better performance, security, and return on investment (ROI) today.

[Network Visibility - Performance Matters Video]

[Network Visibility - Resilience Matters Video]

[Network Visibility for Dummies Book]

[Vision ONE Video]

[Network Visibility - Ease of Use Matters Video]

[Network Visibility - Feature Compatibility Matters Video]

[Ixia's 2017 Security Report]

IXIA WORLDWIDE HEADQUARTERS
26601 W. 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 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