Next-Generation Network Packet Broker (NG-NPB)
Kompletní viditelnost síťového provozu

Dejan Laketić  Sr. Sales Engineer, Gigamon, EMEA Central
“What you can’t see, can’t be monitored. What you can’t monitor, can’t be managed & secured”

“IT’S WHAT YOU CAN’T SEE THAT WILL SINK YOU”

- Introduction to Next Generation Network Packet Broker (NG-NPB)
- Benefits and Use Cases
Network & Security Visibility Challenges

- Full Visibility / Asymmetric Traffic?
- Network Upgrades?
- Data Volume Increase?
- Tool Load & Performance?
- New Tools?
- Compliance?
- Encryption / Decryption?
- CAPEX / OPEX?
Solution for better visibility – NG NPB

NEXT GENERATION NETWORK PACKET BROKER

GIGAMON
Complete Visibility into Data-in-Motion
Network Monitoring & Security Tools

**Out-of-Band Tool**
- SPAN
- Packets

**NetFlow Collector**
- NetFlow / IPFIX / CEF records & metadata

**Inline Tool**
- Inline (Active)

---

**DETECTION**

**PREVENTION**
Agnostic Visibility Solution

Working with any tool and any network
Network & Security Visibility Implementation Use Cases
Use Case:
1. First Step to Visibility: Get Reliable Data Access for Tools
Use Case:
1. First Step to Visibility: Get Reliable Data Access for Tools
Use Case:
1. First Step to Visibility: Get Reliable Data Access for Tools
Use Case:
1. First Step to Visibility: Get Reliable Data Access for Tools

**Eliminate SPAN Port Contention**
Few SPAN ports, many operational and security tools

**Without Gigamon**
- Switch with two SPAN session limitation
- Intrusion Detection System (IDS)
- Application Performance Management
- VoIP Analyzer
- Packet Capture

Customer is unable to use all tools!

**With Gigamon**

Customer has complete visibility for all tools!
Use Case:
1. First Step to Visibility: Get Reliable Data Access for Tools

Run Multiple Proof of Concept in Parallel
Accelerate Certification of New Tools

<table>
<thead>
<tr>
<th>Without Gigamon</th>
<th>With Gigamon</th>
</tr>
</thead>
<tbody>
<tr>
<td>POC #1 – Vendor X Tool</td>
<td>POC #1 Vendor X Tool</td>
</tr>
<tr>
<td>Tool tested w/ NW Segment – 4 weeks</td>
<td>1 month</td>
</tr>
<tr>
<td>POC #2 – Vendor Y Tool</td>
<td>POC #2 Vendor Y Tool</td>
</tr>
<tr>
<td>Tool tested w/ NW Segment – 4 weeks</td>
<td>2 months</td>
</tr>
<tr>
<td>POC #3 – Vendor Z Tool</td>
<td>POC #3 Vendor Z Tool</td>
</tr>
<tr>
<td>Tool tested w/ NW Segment – 4 weeks</td>
<td>3 months</td>
</tr>
<tr>
<td>Customer performs each proof of concept serially at different times using different data</td>
<td>Customer is able to run multiple POCs concurrently using the same data</td>
</tr>
</tbody>
</table>
Use Case: 2. Visibility During Network Upgrades/Expanding Network Coverage

Change Media and Speed
10Gb, 40Gb or 100Gb Traffic to 1/10Gb Tools

Without Gigamon

Customer migrates to a 100Gb network and 1Gb/10Gb monitoring tools become useless

With Gigamon

GigaVUE® Matches Your Network to Your Tools

Customer is able to extend the life of their 1Gb/10Gb network and security tools using GigaStream® load balancing and GigaSMART® intelligence
Use Case:
3. Improve Threat Prevention Efficacy with Inline Bypass
Use Case: 3. Improve Threat Prevention Efficacy with Inline Bypass

Maximize availability & resiliency (for network teams)
- Maximize tool efficacy
- Increase scale of security monitoring
- Bypass protection with advanced health checks to maximize availability

Maximize operational agility (for security teams)
- Add, remove, upgrade tools seamlessly: reduce risk and security effort
- Migrate tools from detection to prevention modes (and vice versa)
- Integrate inline, out-of-band, flow-based tools and metadata to a common platform

Example:
- Generic Web Traffic: IPS + WAF
- Specific Web Traffic: IPS + WAF + ATP
- Non-Web Traffic to/from Specific Subnets: IPS + ATP
- Backup traffic: No inspection
- All other traffic: IPS

IPS = Intrusion Prevention System
WAF = Web Application Firewall
ATP = Advanced Threat Prevention
Use Case:
3. Improve Threat Prevention Efficacy with Inline Bypass
Use Case:
4. Encrypted Traffic Management (TLS Decryption)

Need for Efficient SSL/TLS Inspection

- **80%** of enterprise traffic will be encrypted through 2019¹
- **50%** of malware will use encryption by 2019¹
- **100%** need for visibility into SSL traffic entering or leaving an organization
- **80%** performance degradation of security appliances due to SSL²

¹ Source: Gartner “Predicts 2017: Network and Gateway Security”
² Source: SSL Performance Problems, NSS Labs
Use Case:
4. Encrypted Traffic Management (TLS Decryption)

SSL Decryption Options:

Do nothing?
- Not the right answer

Enable SSL decryption on each tool?
- Serious performance hit on tools (>50% up to 80% capacity lost)
- Multiple decrypt/encrypt latency, troubleshooting difficulties

Insert standalone SSL decryption appliance?
- Another vendor/component added to mix, point of failure/problems
- Very limited tool chaining

Use Gigamon Next-Gen Packet Broker
- Single SSL decryption instance feeds all tools
- Decrypt once, feed any number of inline and out-of-band tools
- No physical wiring/changes required with existing NGPB
Use Case:
4. Encrypted Traffic Management (TLS Decryption)

Highlights
- Servers and clients located internally or externally
- Private keys not needed
- RSA, DH, PFS can be used
- Supports inline and out-of-band tools
Use Case: 4. Encrypted Traffic Management (TLS Decryption)

Key Capabilities

- **Automatic SSL/TLS detection** on any port or application: inbound and outbound
- **Scalable interface support** (1Gb to 100Gb)
- **Decrypt once, feed many tools**
- **Strong crypto support**: PFS, DHE, Elliptic Curve ciphers
- **Certificate validation and revocation lists**: strengthens organizations’ security posture
- **Strong privacy compliance**: categorize URL before decryption

[Diagram showing network components, including Internet, Clients, Corporate Servers, Internet Servers, Gateway, Active, Inline Appliance(s), Passive, Out-of-Band Appliance(s), APT Prevention, IPS, Network Forensics, Anti-malware, and Decrypt once, feed many tools, SSL, Certificate validation and revocation lists, Strong crypto support, Strong privacy compliance.]
Use Case: 5. Centralized NetFlow/IPFIX Generation

The Power of the Platform: NetFlow/IPFIX Generation

Without Gigamon

- Production Network
- Tools and Analytics
  - Security
  - Application Performance
  - Network Performance

NetFlow Records

Challenges:
- High impact on switches that generate flow records
- Switches generate sampled NetFlow inadequate for security
- Different formats across different switch manufacturers
- Lack of ubiquitous NetFlow generation capabilities across infrastructure
- Vanilla NetFlow records do not contain metadata beyond basic flow info

With Gigamon

- Production Network
- Tools and Analytics
  - Security
  - Application Performance
  - Network Performance
  - Gigamon NetFlow Generation
  - Visibility Platform

Benefits of the Gigamon approach:
- Pervasive visibility w/ centralized, high-fidelity, unsampled NetFlow generation
- Export in all standard formats (NetFlow v5, NetFlow v9, IPFIX, CEF)
- Combine Flow Mapping® with IPFIX generation for high-fidelity output
- Optional enhanced metadata added to flow records
- Combine with full packet analysis to create an effective monitoring strategy
Use Case:
6. Extract Network Metadata to Optimize SIEMs

Network
- DNS, SSL, HTTP, RDP, Powershell

Network Metadata

Metadata Engine

SIEM/COLLECTOR
- Extract and send only the critical metadata to the SIEM
- Reduce the quantity of data by several orders of magnitude
- Make it easier for the SIEM to find the proverbial needle in a haystack
Use Case:
7. Leverage Application Intelligence to Optimize Tool Stack
### Use Case: 7. Leverage Application Intelligence to Optimize Tool Stack

<table>
<thead>
<tr>
<th>Network Ingress</th>
<th>10 Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unanalyzed Email</td>
<td>- 1.5 Gbps</td>
</tr>
<tr>
<td>SMTP, IMAP</td>
<td></td>
</tr>
<tr>
<td>Streaming Video</td>
<td>- 3.0 Gbps</td>
</tr>
<tr>
<td>Youtube, Netflix, Hulu</td>
<td></td>
</tr>
<tr>
<td>Backups and Updates</td>
<td>- 1.2 Gbps</td>
</tr>
<tr>
<td>Windows, iOS, Android</td>
<td></td>
</tr>
<tr>
<td>Filtered from ATD tool</td>
<td>5.7 Gbps</td>
</tr>
<tr>
<td>Delivered to ATD tool</td>
<td>4.3 Gbps</td>
</tr>
</tbody>
</table>

Internal Network

- Email
- Streaming
- Backups
Use Case:
8. Visibility into Private Clouds (VMware ESX and NSX)

5 REASONS WHY YOU SHOULD CARE

1. Scope of security must cover virtualized workloads
2. Increasing VM density
3. Visibility into VM-VM traffic
4. Creating new virtual tool instances eats into compute capacity
5. Automated visibility after VM migration
Use Case:
8. Visibility into Private Clouds (VMware ESX and NSX)

- vCenter integration
- Bulk GigaVUE-VM onboarding
- Virtual traffic policy creation
- Automatic migration of monitoring policies

Internet

Tunneling

Private Cloud

SERVER I  SERVER II

Virtual Traffic Policies

Production Network

GigaVUE-FM

vCenter

Tools and Analytics

Application Performance
Network Performance
Security

Gigamon® Visibility Platform
Use Case:
9. Visibility into Hybrid Clouds (AWS, Azure, OpenStack, VMware ESX and NSX)
Use Case: 10. Visibility into Remote Sites

- Centralized tools
- Metadata generated from remote sites
- Flexibility to extract full traffic flows when needed
- Cost optimized: Reduce WAN costs with de-dup or slicing or IPFIX at remote site before backhaul
Use Case: 11. Lawful Intercept

Without Gigamon

Exchange 1
Legal Intercept Recorder

Exchange 2
Legal Intercept Recorder

Exchange 3
Legal Intercept Recorder

Challenges:
- Expensive, ad hoc approach
- Deploy equipment and staff as needed to each exchange/CO
- Requires staff and equipment to be immediately ready to deploy in order to satisfy the legal dates/terms on the government warrant

With Gigamon

Exchange 1
H SERIES

Exchange 1
H SERIES

Exchange 1
H SERIES

Central Data Center
H SERIES

Benefits of the Gigamon approach:
- Higher ROI: GigaVUE® nodes at each exchange tunnel traffic to a centralized Legal Intercept Recorder
- Flow Mapping® policies select only traffic that needs interception
- Ability to filter application flows to narrow traffic of interest
Corporate Overview

**THE ESSENTIAL ELEMENT OF YOUR SECURITY**

Gigamon is leading the convergence of networking and security. Our next generation network packet broker helps make threats more visible, deploy resources faster and maximize performance.

**Gigamon**

*HQ*
Santa Clara
California, USA

*FOUNDED*
2004

*EMPLOYING*
707 employees

*SERVING*
Over 2,800 customers

*NAMED*
Market leader

*GLOBAL OFFICES*
20 Countries

*CEO*
Paul Hooper

*PATENTS*
51 Global patents issued

*VERTICALS*
Public Sector | Financial Services | Healthcare | Retail Technology | Service Providers

*Feb 2018: Offices, employee and patent information
**Q1 2018: Customer count
Trusted by the World’s Leading Organizations

Gigamon Customers

- 7 of the top ten Global Banks
- 8 of the top ten Healthcare Providers
- 10 of the top ten U.S. Federal Agencies
- 8 of the top ten largest Tech Companies
- 83 of the Fortune 100
- 8 of the top ten Mobile Phone Network Operators

Customer data from April 2018. List sources available upon request.
Gigamon Portfolio

NG Network Packet Broker

Traffic Intelligence Capacity

HC1

Mid-Sized Enterprise

HC2

Large Enterprise

HC3

Service Provider

Throughput (Gbps)

Traffic aggregator

GigaVUE-TA10

GigaVUE-TA40

GigaVUE-TA100

GigaVUE-TA200

TAP

Serie A

Serie M

Serie G

BiDi 40G Fiber TAP
Thank you

Dejan Laketić
Dejan.Laketic@gigamon.com
M +420 774 419 960