Feature Brief

NetFlow and Metadata Generation

Challenges of NetFlow Generation

As enterprise networks continue to grow and network speeds continue to increase, the ability for business-critical appliances to consume and analyze the additional data is, by contrast, diminishing at an equal proportion. Threat complexity, for instance, is requiring security devices to take on more complex analytics; but is also straining already scarce compute on appliances that could barely match 10Gb speed—let alone 40Gb and 100Gb.

In short, the problem is too much data, too little compute. And the answer? Metadata.

NetFlow is one form of metadata. This Layer 4 flow-generated data can increase visibility into traffic across systems and be used to build relationships and usage patterns between nodes on the network—but only if produced the right way. While routers and switches are capable of generating NetFlow metadata, they were not designed to do so for every packet. This creates challenges and limitations. Not only is router- or switch-generated NetFlow sampled, but it is also inconsistent in format and requires processing overhead that can introduce service degradation, latency, and packet drops.

What's more, even if processing issues were able to be resolved, NetFlow is only Layer 4. Organizations also need Layer 7 application-level metadata to achieve pervasive, actionable visibility and successful analysis.

The Gigamon® Solution

From incoming traffic streams, Gigamon can generate both Layer 4 and Layer 7 metadata. And the key differentiator and benefits? This NetFlow is unsampled; it supports a range of NetFlow formats, including versions 5 and 9 IPIX and CEF for seamless integration with an unlimited number of standards-based collectors, storage devices, and SIEMs; and it is done without causing any processing overload or performance degradation.

Additionally, Gigamon has extended IPFIX to include not only standard information about traffic—like source and destination IP addresses and ports—but also application-specific extensions, such as DNS, URL, and HTTP response codes, to name a few. To eliminate the risk of expending expensive production network resources in generating this data, Gigamon has enabled operators to offload metadata generation to an out-of-band solution like the Gigamon Visibility Fabric™. Gigamon's patented Flow Mapping® technology can also be used to pick and choose from flows to generate NetFlow and metadata statistics while, at the same time, sending the original packets to other monitoring tools. Operators can also export NetFlow records plus other network metadata to multiple collectors concurrently, creating a single flow source for business-critical management applications such as security, billing, capacity planning, and more. And finally, they can filter exported flows so that collectors only receive the specific records relevant to them.

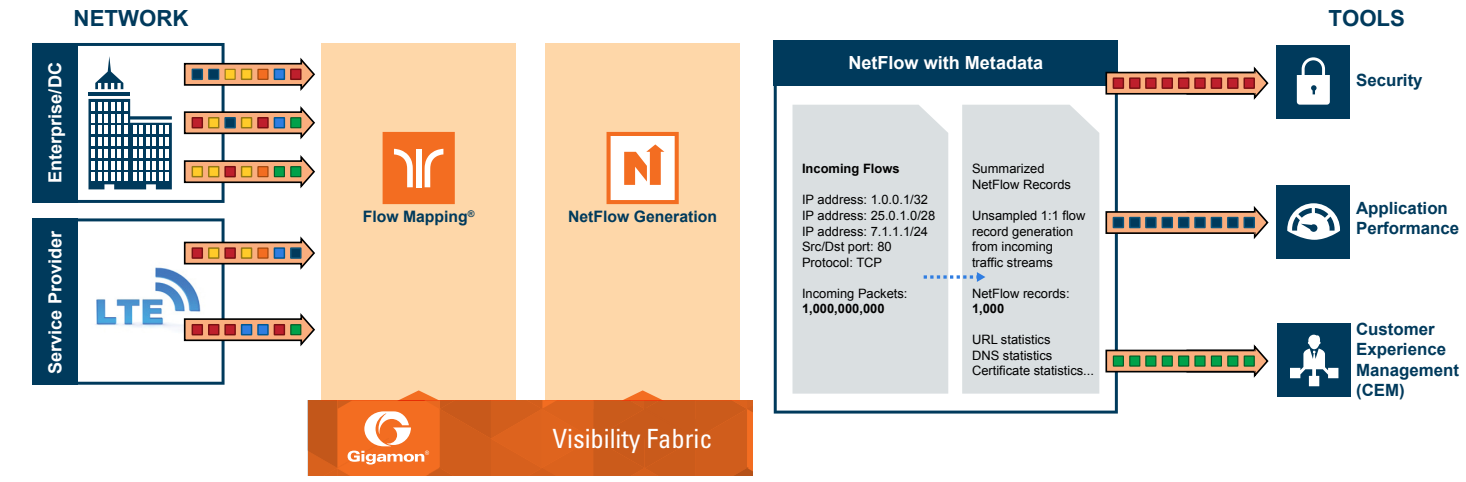

Figure 1: NetFlow generation

The Gigamon Visibility Fabric establishes a scalable framework to deliver pervasive, flow-level visibility across enterprises, data centers, and service provider environments to help users accurately design, engineer, optimize, and manage their network infrastructure.

Key Features and Benefits of NetFlow

Features	Benefits
Pervasive visibility with NetFlow generation across the entire network	Security and performance monitoring tools get complete view of the network versus isolated views of individual network segments generated by a specific router or switch
High-throughput out-of-band NetFlow solution	No performance impact of NetFlow generation from production routers and switches
Unsampled 1:1 NetFlow generation on every packet	Complete and precise picture of network activity for security monitoring without loss of fidelity incurred from sampled NetFlow generation
Support for a wide range of NetFlow export formats – v5, v9, IPFIX and CEF	Compatibility with legacy and next-generation NetFlow collectors
Ingress filtering on Layer 2, Layer 3 and Layer 4 headers using Gigamon Flow Mapping	Generate flow statistics for specific networks and applications
Support for up to six collectors with customizable templates and filters	Leveraging multiple vendors for security and application monitoring

Key Metadata Extensions

Extension	Fields Extracted	Benefit
DNS	• dnsIdentifier • dnsOpCode • dnsResponseCode • dnsQueryName • dnsResponseName • dnsResponseTTL • dnsResponseIPv4Addr • dnsResponseIPv6Addr	• Uncover domain lookups for malicious command and control (C&C) servers • Identify endpoints potentially infected with bots • Identify suspicious DNS servers that have low time-to-live (TTL) values • Identify rogue DNS servers in the network
URL	URL from method types • HTTP GET • POST • PUT • DELETE • HEAD	• Identify malicious communications to C&C servers • Identify potential SQL and other OWASP vulnerabilities from URLs • Identify productivity and compliance violations using URL metadata
HTTP Response Codes	HTTP Response Codes: • 100-199 (informational) • 200-299 (success related) • 300-399 (redirection) • 400-499 (client requests) • 500-599 (server related)	• Baseline of HTTP codes to uncover anomalous behavior patterns • Identify excessive redirections (3XX codes) that could point to compromise of internal servers • Identify excessive 4XX codes that could signal potential denial of service attacks and communications to C&C servers from infected hosts

Key Metadata Extensions continued

Extension	Fields Extracted	Benefit
Certificates	• sslCertificateSubject • sslCertificateValidNotBefore • sslCertificateValidNotAfter • sslCetificateSerialNumber • sslCertificateSignatureAlgorithm • sslCertificateSubjectPubAlgorithm • sslCertificateSubjectPubKeySize • sslCertificateSubjectAltName • sslServerNameIndication • sslServerVersion	• Identify expired certificates in the network • Identify self-signed certificates in the network • Identify certificates using weak cipher algorithms • Identify mismatches in certificate subject fields (if subject field does not match website domain name)
CDP	• Device ID • Port ID • TTL • Platform • SW Version • Native VLAN ID • Capabilities • Network Prefix Address • Network Prefix Mask • Interface Address • Management Address	• Identify source or destination machine type instead of IP address (e.g., Catalyst 6K switch) • Reduce time to resolution by identifying physical location of traffic within the network
LLDP	• Chassis IP • Port ID • TTL • Port Description • System Name • System Description • Management Address • Capabilities Available • Capabilities Enabled • VLAN Name • Port VLAN ID • Management VLAN ID • Link Aggregation ID • Link Aggregation Status • MTU	• Identify source or destination machine type instead of IP address • Reduce time to resolution by identifying physical location of traffic within the network
SIP	Sender and Receiver Information from • INVITE • ACK • BYE • REGISTER • OPTIONS • CANCEL request types	• Get source and destination caller information in addition to IP addresses for a SIP call

About Gigamon

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon's Visibility Fabric™ and GigaSECURE®, the industry's first Security Delivery Platform, deliver advanced intelligence so that security, network, and application performance management solutions in enterprise, government, and service provider networks operate more efficiently. As data volumes and network speeds grow and threats become more sophisticated, tools are increasingly overburdened. One hundred percent visibility is imperative. Gigamon is installed in more than three-quarters of the Fortune 100, more than half of the Fortune 500, and seven of the 10 largest service providers.

For more information about the Gigamon Unified Visibility Fabric visit: **www.gigamon.com**

3099-10 07/18

Gigamon®

3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com