Gigamon®

WHITE PAPER

Leveraging NetFlow Generation for Maximum Security Value

Overview

Cisco introduced NetFlow in 1996 as a way to monitor packets as they enter and exit networking device interfaces. The aim is to gain insight and resolve congestion. Typical information in a NetFlow record reveals traffic source and destination, as well as protocol or application, time stamps, and number of packets. Although NetFlow was initially not on a standards track, it has been superseded by the Internet Protocol Flow Information eXport (IPFIX), which is based on the NetFlow Version 9 implementation, and is on the IETF standards track with RFC 5101, RFC 5102.

As organizations refocus network security efforts on insider threats and detection of compromise, NetFlow provides rich and important contextual information about the traffic, augmenting analysis in order to determine where compromise has occurred. This takes NetFlow out of the traditional realm of use for optimizing network and application performance and into the security arena. Given that, if NetFlow is to be relied on as a required and continuous information source, the architecture to generate and analyze it has to be optimized for the use case. Here we'll review the NetFlow generation framework needed for security and how to leverage it for various related uses cases.

For Security, Sampled Data Doesn't Cut It

Most routers and switches from leading vendors now support the generation of NetFlow, IPFIX or similar (some vendors have their own versions). This is touted as a low-cost way to gain broad insight into network traffic. But NetFlow generation can be extremely taxing on this hardware, especially with exploding traffic volumes, with the majority of traffic now flowing east-west among users, applications, servers and databases. To ensure that latency and packet loss is not introduced into high-performance networks, networking devices are often configured for sampled NetFlow rather than one-for-one record to packet generation. This reduces the burden on networking devices: is somewhat reduced: Instead of 1:1 record to packet generation, records are generated for 1 of every *n* packets where *n* can vary from 100 to 1,000 or more. This is also true of technologies such as sFlow that operate only on a sampled basis.

This kind of sparse traffic record is enough to establish trends for network and application performance, but it's a non-starter for security analytics. Advanced persistent threats (APTs) can operate low and slow on the network, moving laterally and communicating with command and control sites over long periods of time (days, months or longer). The key to spotting anomalous traffic is looking for hard-to-spot patterns over the complete network activity picture. Naturally, looking at a fraction of packet records severely hampers the breadth and accuracy of the analysis.

Here are the drawbacks of generating NetFlow records using networking gear:

1. NetFlow generation can degrade router and switch performance
2. To manage the impact on performance, networking devices may give sampled NetFlow or just drop packets
3. Some vendors have their own version of NetFlow (sFlow, for example) which may not be supported by security devices
4. Networking devices can be limited in how many collectors they can support (such as two maximum)
5. Lack of policy-based forwarding limits how NetFlow is generated for traffic of interest

A Better Way: Centralize NetFlow Generation with a Security Delivery Platform

To avoid these issues and maximize the benefit of NetFlow data to network security, NetFlow generation is best performed by a security delivery platform (SDP). The Gigamon Visibility and Analytics Fabric gives you the complete picture of the network at line rate, including all packets and their NetFlow records without loss. This means that security analytics based on Gigamon NetFlow data will be much more accurate and better at spotting bad actors on the network.

Not only does this offload precious cycles from networking devices and raise security effectiveness, it also adds the powerful benefit of policy-based filtering and forwarding of the NetFlow data, delivering traffic of interest to the right security applications and tools at the right time.

Choose Your Use Case(s)

Chances are some or all of these use cases apply to your organization's network. Here's how centralized NetFlow generation improves security and efficiency.

1. Enforce egress filtering policies
NetFlow records include rich data about application use on the network and the resources involved in the communication. Such information can help administrators spot risky or unsanctioned applications and cloud-based services in use on their networks. Visibility into these traffic statistics allows security stakeholders to limit risky behavior and ensure only business use of those applications by defining egress policies at access control points or next generation firewalls (NGFWs) that can.

2. Detecting zero-day threats
Zero-day threats often use a new combination of steps and may evade signature-based defenses until discovered and security devices can be updated. To discover them in the interim, some NetFlow analytics tools look for anomalous patterns such as frequency and source of DNS queries or traffic on unique port/protocol combinations, which may indicate that a zero-day attack is underway. Since NetFlow information can be parsed for bandwidth consumption, application type and source, it can help shorten the time to discovery of a zero-day attack.

3. Find compromised endpoints and botnets
By correlating threat information from intrusion prevention systems (IPSs) with MAC and IP addresses from NetFlow and logon information from LDAP stores, security teams can more quickly identify the users and/or devices associated with unwanted or anomalous network traffic. Further queries of NetFlow can reveal all IP connections made from the compromised device, letting security administrators establish which connections are legitimate and which may be part a botnet's command and control communications. Using NetFlow reduces the time to discovery and remediation thereby limiting the window of exposure to risk.

4. Chaining security services
Deep packet inspection taxes compute resources and can reduce throughput dramatically on the devices that support it, such as next-generation firewalls (NGFWs) and UTMs. Security applications that support DPI such as IPSs, NGFWs and content inspection gateways, as well as advance threat detection and sandboxing devices, are often deployed on the side or in an out-of-band mode in order not to impede mission-critical traffic. Centralized NetFlow generation provided by an SDP offers brings these advanced protection mechanisms together. If a NetFlow analytics device detects anomalous traffic, it can trigger the same SDP to forward all subsequent packets associated with the NetFlow records to DPI-capable devices as well as advanced threat detection tools to inspect more deeply for the presence of malware. In fact, it can forward multiple copies of the traffic to multiple tools. All of this can be accomplished without disruption to the network.

5. Reducing cost of security monitoring
NetFlow generation for security can be costly. Many security applications require their own dedicated stream, and gathering NetFlow from remote locations can add to link congestion, especially if the network is under attack (when NetFlow analysis is particularly valuable). Centralizing NetFlow collection can reduce the number of collectors required and free up precious link bandwidth. This is particularly useful in monitoring remote sites connected via low-bandwidth connections. Gathering NetFlow records from a remote site provides an efficient way to gain visibility into remote infrastructure while still centralizing the tools in a single location.

In networks without pervasive security monitoring, NetFlow offers a cost-effective way to extend analytics and protection into areas network blindspots. Use of NetFlow allows first-pass analysis of vast amounts of internal traffic. When something suspicious is flagged, the packet stream can be forwarded to centralized security tools for more in-depth analysis. This offers security in depth and breadth without the cost and latency of deploying deeppacket inspection on every network segment.

6. Enabling forensics
When your network is compromised, you need to be able to look back in time and understand how exactly the attacker got in, which systems were compromised and how the bad actors progressed inside the network. NetFlow data is a compact and cost-effective alternative to the space and expense of storing security logs and full packet capture. NetFlow records show not only flows among the compromised endpoints, but also the flows that were associated with the breach in general and the movement of bad actors inside the network, giving a more complete view of the network's risk posture.

The Gigamon Solution: The Visibility and Analytics Fabric

The Gigamon Visibility and Analytics Fabric goes beyond unsampled NetFlow generation with value-added features like Flow Mapping® and Application Filtering Intelligence, which couples traffic flow metadata with intelligent traffic forwarding. Additionally, APIs allow for security automation by bridging NetFlow-based analytics to deep packet inspection and even enforcement. This type of automated response can shorten the time it takes to discover and respond to a threat.

Gigamon has also extended the IPFIX format by adding a private extension to capture the URL information embedded in HTTP and SIP connections. With this enhancement, big data-capable security applications can use the URL information to uncover unwanted and unwarranted web traffic. For example, you could run web traffic reports to identify the most visited sites in your organization, which may reveal they are attack targets. Security applications can also compare the URL against lists of known malicious sites such as a command and control servers to look for matches.

Finally, Gigamon has extended the IPFIX format to include the interface names as part of the NetFlow records. By supporting protocols like the Cisco Delivery Protocol (CDP), the Gigamon Visibility and Analytics Fabric provides the information needed to correlate traffic flows to the actual traffic sources. This data is vital to understanding attack movement on the network for forensics and risk mitigation.

Key NetFlow/IPFIX Generation Features of Visibility and Analytics Fabric

- Combined traffic and flow data visibility in one solution
  - Exports up to six NetFlow collectors
  - Combines traffic from multiple sources into summary statistics
  - Filters output for specific collectors and/or replicates
- Out-of-band NetFlow generation
  - Transforms packet data across multiple devices into summarized NetFlow statistics
- Supported NetFlow export formats
  - v5
  - v9
  - IPFIX
- Ingress filtering
  - Gigamon patented Flow Mapping technology enables selective NetFlow generation based on Layer 2, Layer 3 or Layer 4 header parameters
- Export filters
  - Advanced filters for custom exports to one or multiple NetFlow collectors, performance and security monitors
- URL collection (IPFIX only)
  - HTTP: GET, POST, PUT, DELETE and HEAD method types
  - HTTP response codes (2XX, 3XX, 4XX and so on) to help uncover suspicious behavior such as redirects and DOS attacks
  - SIP: INVITE, ACK, BYE, REGISTER, OPTIONS and CANCEL request types

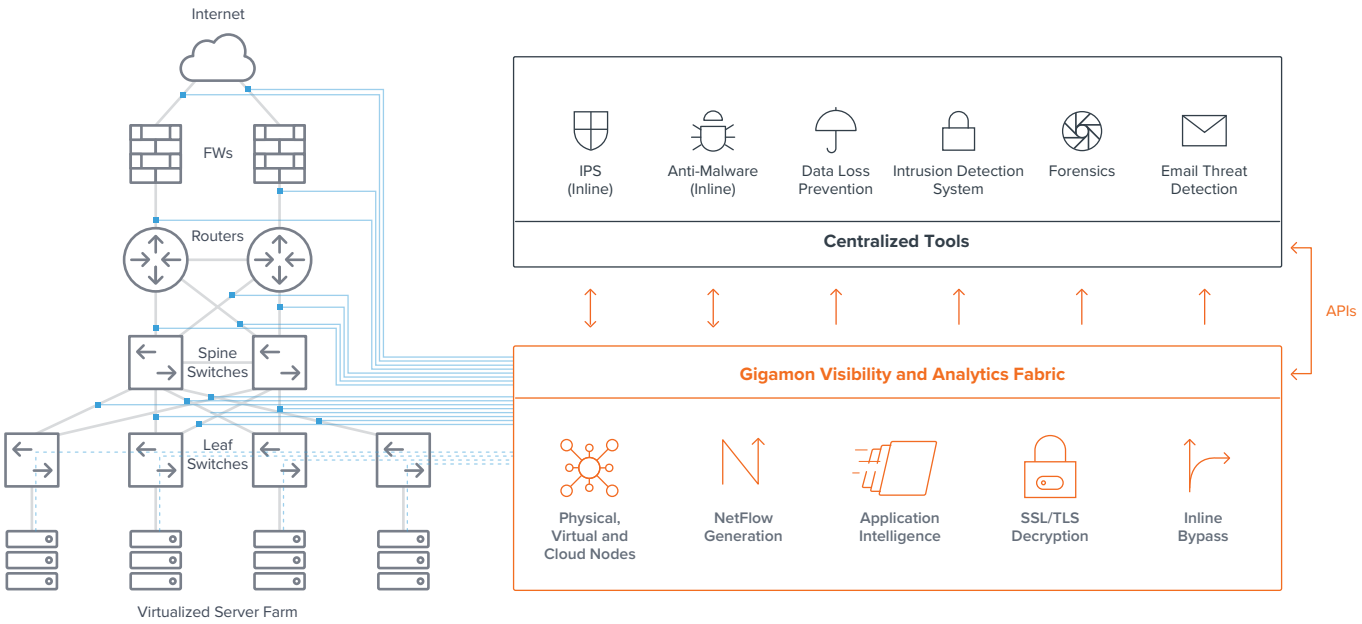

Figure 1: Gigamon Visibility and Analytics Fabric

Summary: NetFlow Is Vital to Security

NetFlow/IPFIX has become indispensible for security policy enforcement, analytics, breach discovery, mitigation and forensics in best-of-breed networks. For security monitoring, administrators need unsampled NetFlow to get precise visibility into all network activity happening in the infrastructure. Such a vital function shouldn't rely on ad hoc systems and resource-constrained networking gear. By centralizing NetFlow generation using the Gigamon Visibility and Analytics Fabric, you can combine unsampled data with the intelligence and scale of policy based traffic manipulation.

About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate. Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including 80 percent of the Fortune 100. Headquartered in Silicon Valley, Gigamon operates globally. For the full story on how Gigamon can help you, please visit www.gigamon.com.

Gigamon®

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