Solutions Guide

End-to-End Visibility and Security for Your Cisco Infrastructure

Table of Contents

Introduction

Across the globe, many companies choose a Cisco networking infrastructure to service their physical and virtual networking needs for enterprise and data center operations. When implementing a large-scale Cisco network, monitoring tools typically rely upon Cisco technologies, such as NetFlow, SPAN, RSPAN, ERSPAN, and VACL for traffic visibility. Traffic is extracted and sent to the tools. However, these technologies are often difficult to scale and can modify traffic (e.g. encapsulate traffic), making it difficult to support the diverse monitoring needs of network, security, application, and server groups as they strive to maintain maximized uptime, secure the network, realize operational efficiencies, and gain greater insight into business decision making.

In addition, gaining end-to-end visibility across physical, virtual, and emerging architectures such as Cisco's Application Centric Infrastructure (ACI) and Software Defined Networking (SDN) environments can be challenging, not only during the initial period of transition, but also after the rollout is completed. The interaction between multiple ACI components—APIC (Controller), Application Network Profiles and the underlying ACI fabric—means that the reliance on traffic to comprehensively determine real-time state of the infrastructure only increases. Moreover, the use of integrated overlay technologies, such as VXLAN inside the ACI fabric, means that operational tools that need visibility inside the platform need a translation layer that removes the VXLAN headers and extracts traffic from a particular Endpoint Group before sending traffic to that operational tool. Additionally, ACI is often implemented as part of a 40Gb transition and many customers choose Cisco 40Gb BiDi technology to simplify the transition from 10Gb to 40Gb. During this transition, it is important to be mindful of maintaining visibility through a system of BiDi-capable network TAPs. ACI uses application network profiles determined by application requirements to guide networking behavior and automate the provisioning of the network. However, as emerging technologies like ACI evolve, so does the need to efficiently monitor and manage it.

This guide reviews the various architecture and technologies that are typically deployed in Cisco networking infrastructure environments, identifies the key elements to building end-to-end visibility that can help maximize effectiveness of the Cisco infrastructure, and illustrates how it can be achieved using the Gigamon® Visibility Platform.

Overview of Cisco Technologies

Cisco provides a wide range of solutions and technologies to deliver a network optimized for performance. Network, security, application, and server teams are accountable to ensure the infrastructure is manageable, efficient, and secure. This section provides an overview of Cisco technologies, monitoring methods, and challenges affecting end-to-end visibility:

- Application Centric Infrastructure (ACI)
- Cisco 40Gb BiDi Links
- Cisco Fabric Extender (FEX) and VN-Tag
- Cisco FabricPath
- Cisco Virtual Infrastructure
- Cisco Monitoring Methodologies
  - NetFlow/IPFIX
  - SPAN
  - RSPAN
  - ERSPAN
  - VACL
- Inline Bypass Protection of Cisco FirePOWER Intrusion Prevention System (IPS)

Monitoring Cisco Application Centric Infrastructure (ACI)

Cisco's innovative ACI architecture is designed to address the new world of distributed applications in private cloud deployments and data centers. The ACI architecture uses two key concepts of SDN—integrated overlays and a centralized controller to deliver centralized automation and policy-driven application network profiles. The Application Policy Infrastructure Controller (APIC) is the unification point of policy enforcement and translates the application-centric policies to network policy configuration that are programmed into the underlying ACI fabric. Overlays provide more flexibility because they offer the power of separating device location from device identity. For a network administrator, it is important to have the necessary visibility into the communication between the APIC and the physical/virtual nodes to immediately determine if the APIC and the infrastructure state are ever out of sync. Further, being able to correlate network traffic activity to what the controller expects the switches to be doing is going to be a critical aspect of ensuring the success of SDN deployments.

In addition, the use of technologies like VXLAN introduces new visibility challenges. The wide range of operational tools used for network administration is often unaware of VXLAN and requires the VXLAN headers to be stripped before they are delivered to the tools. And, in a virtualized environment, the administrator needs to have visibility into both virtual as well as physical elements in the ACI fabric to ensure that there are no blind spots in this infrastructure.

Cisco 40Gb BiDi Links

One of the design elements of ACI is the move to leaf/spine infrastructures running over 40Gb links. Unfortunately, traditional 40Gb short-range links require multiple lanes of multi-mode fiber that requires using up to four such pairs of fiber. In many cases, fiber is deployed in groups of 12. Consequently, an upgrade from 10Gb to 40Gb could create a 6x increase in fiber cost.

To mitigate this issue, Cisco solves this challenge with an innovation in 40Gb called BiDi that allows 40Gb traffic to run over existing 10Gb cabling. This is done by multiplexing two lanes of 20Gb on a single pair of multi-mode fiber. While this eliminates the fiber cost issue, it raises a new challenge that standard TAPs cannot be used to monitor these links. Moreover, Cisco customers can also implement 40Gb BiDi independent of ACI, which means that this challenge can be significantly more impactful.

Cisco Fabric Extender (FEX) and VN-Tag

When Cisco introduced the Unified Fabric, the goal was to unify storage, data networking, and network services to deliver architectural flexibility across physical, virtual, and cloud environments.

One of the key components is the Cisco Fabric Extender Technology (FEX), which delivers fabric extensibility across the network and server hypervisor connectivity. The Cisco FEX Technology includes a parent switch and an extender switch. The parent switch can be a Cisco Nexus 5000 Series switch, Nexus 6000 Series switch, Nexus 7000 Series switch, or a Cisco UCS Fabric Interconnect. The fabric of the parent switch is extended to connect to the server either as a remote line card with Nexus 2000 Series Fabric Extenders or virtual adapter ports to connect to any type of servers—rack and/or blades, with Cisco Adapter FEX and VM-FEX technologies. Initially based on IEEE802.1Qbh, a VN-Tag is inserted into each frame exchanged between the extender switch and the Nexus parent switch.

While the goal of Cisco's Fabric Extender is to simplify data center connectivity, it introduces potential issues for the security and analytic tools that do not fully understand VN-Tag headers or require additional CPU processing to remove the VN-Tag headers. Therefore, the need for a centralized monitoring infrastructure with the ability to "normalize" traffic will help the tools regain visibility, while maintaining operational efficiency.

Cisco FabricPath

With Cisco FabricPath, highly scalable Layer 2 multipath networks can be built simply and provisioned easily without Spanning Tree Protocol. Such networks are particularly suitable for large virtualization deployments, private clouds, and high-performance computing (HPC) environments. However, much like Cisco Fabric Extender, Cisco FabricPath introduces potential blind spots for security and analytic tools that do not fully understand the FabricPath headers that are added to the traffic in this environment. In addition, even if the operational tool is able to remove such headers, additional CPU processing from the tool is required. Again, there is a need for a centralized monitoring infrastructure with the ability to "normalize" traffic so that the various operational tools can gain visibility while maintaining efficiency to focus on their specialized tasks.

Cisco Virtual Infrastructure

Cisco Nexus 1000V Series represents the first example of third-party distributed virtual switches that are fully integrated with VMware virtual infrastructure, including VMware vCenter for the virtualization administrator. When deployed, the Cisco Nexus 1000V Series not only maintains the virtualization administrator's regular workflow; it also offloads the vSwitch and port group configuration to the network administrator, reducing network configuration mistakes and helping ensure that consistent network policy is enforced throughout the data center.

In the Cisco Nexus 1000V Series, traffic between virtual machines on the same host is switched locally without ever hitting the physical switch or network, resulting in the increased potential for blind spots. Cisco technologies such as SPAN, RSPAN, ERSPAN, and VACL may be used on the Nexus 1000V, but there are limitations that will be discussed in the next section of this document—Cisco Monitoring Methodologies.

Cisco Monitoring Methodologies

NetFlow/IPFIX

The combination of Cisco's NetFlow and its standards-based constituent IPFIX is a feature that collects IP traffic statistics. By analyzing these statistics, known as NetFlow/IPFIX records, a network administrator can determine things such as the source and destination of the traffic, class of service, and the cause of congestion. This insight can help in optimizing resource usage, planning network capacity, and identifying the optimal application layer for Quality of Service (QoS). It can also play a critical role in network security by detecting Denial of Service (DoS) attacks and network-propagated worms.

When enabled natively in the Cisco switching infrastructure, NetFlow could consume precious compute resources that may burden the switch in times of high utilization potentially causing contention for resources which could affect the performance of the network switching, the ability to deliver accurate NetFlow statistics, or both. Often administrators correct for this by setting a low sampling rate. However, too low of a sample rate can result in important network events being missed. In addition, NetFlow on an individual switch offers a limited view of traffic that the switch sees. An out-of-band, centralized approach to NetFlow generation could offer visibility into NetFlow statistics across the network and not affect the performance of the production

network. The centralized approach is especially important in modern data centers that are highly virtualized and feature distributed applications. The ability to collect NetFlow records from a centralized point provides insight into the nature of traffic patterns across the network vs. a single node. Often, the Cisco infrastructure is also used with other equipment that may not be NetFlow capable; in this case, centralized NetFlow/IPFIX generation is a viable approach to gaining NetFlow visibility across such a multi-vendor network.

Cisco SPAN

The Switch Port Analyzer (SPAN) functionality is offered in all Cisco switching solutions. A SPAN port copies data from one or more source ports to a destination port. Figure 1 shows an example of how the SPAN function operates. With most Cisco switching products, users are limited to two SPAN sessions per switch. For large enterprises this is typically not adequate for monitoring purposes. In most large organizations between the network and security groups there can be up to four or more monitoring or analysis tools that all need to contend for the same data. Examples of some of the tools that are utilized by IT teams are Application Performance Monitoring (APM), Network Performance Monitoring (NPM), Intrusion Detection Systems (IDS), Data Recorders, Web monitoring tools, and many more.

There are also other limitations with this model that prevent users from sending data from one source port to both of the available SPAN sessions, as well as limitations that allow VLAN and non-VLAN traffic to be sent to the same port. In summary, SPAN sessions are good for spot analysis but are limited in terms of scaling to support enterprise-wide monitoring policies. SPAN ports are typically best for small to medium environments where monitoring needs are minimal.

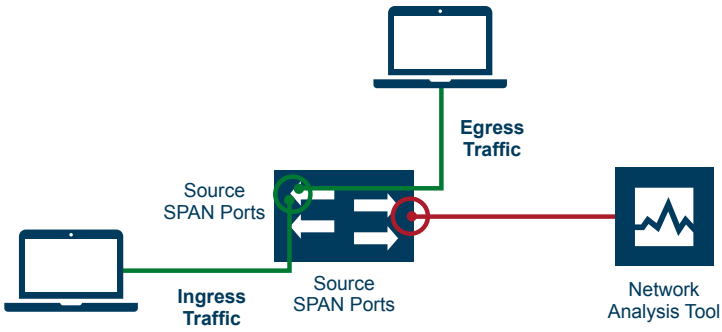

Figure 1: Cisco SPAN Example: Inside a Cisco switch data is copied from a network port to a SPAN port which has a monitoring tool connected

Cisco ERSPAN

Encapsulated Remote SPAN (ERSPAN) data from remote switches can be forwarded to a source monitoring tool over a routed network or Internet using a GRE Tunnel that is configured on the Cisco switches (Figure 2).

ERSPAN is a feature that is supported on Cisco switches beginning with the Supervisor Engine 720 with PFC3A. This means the feature has limited support beyond Cisco switch families such as the Catalyst 6500 and Nexus families. Packets of an ERSPAN session are encapsulated with a 50-byte header. Fragmented frames and jumbo frames can be problematic. ERSPAN does not support fragmented frames and all switches in the path have to be configured to support jumbo frames otherwise frames that increase past the 1500-byte MTU limit with the 50 bytes of ERSPAN encapsulation are dropped.

As with all other SPAN technologies, users can only create two ERSPAN destinations per switch. ERSPAN requires additional configuration complexity to ensure that the tunneling and frame sizes are correct for proper routing of data.

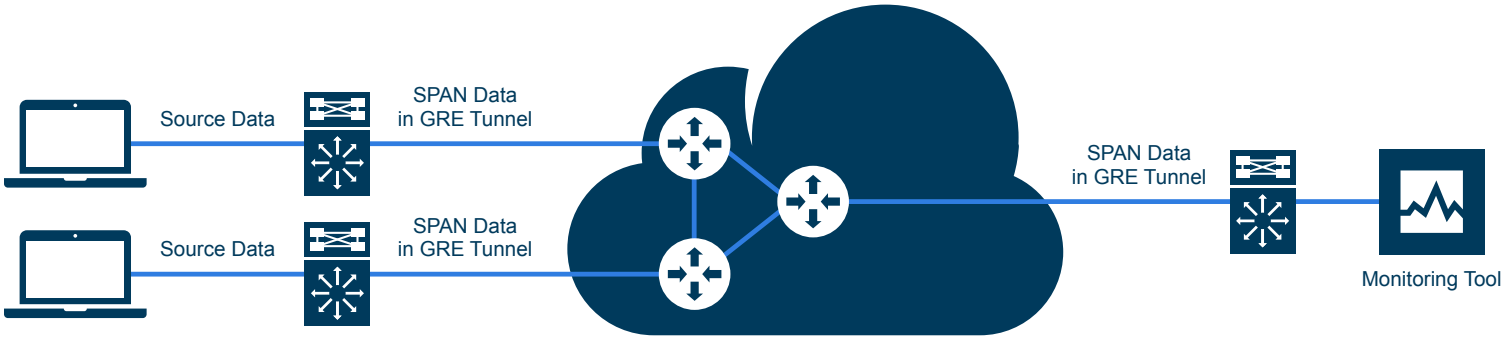

Figure 2: Cisco ERSPAN example

Cisco RSPAN

Cisco Remote Switch Port Analyzer (RSPAN) works very much like SPAN with the exception that data can be sent between remote monitoring ports in the switching architecture using the Cisco VLAN Trunking Protocol (VTP) and reflector ports (Figure 3).

Users are only allowed to send data to two RSPAN destinations. Similar to the SPAN function, data from the same source port or VLAN cannot be shared across the two sessions. RSPAN presents configuration complexity as users have to configure the correct VTP domains on each switch that RSPAN data traverses. In addition to the potential for duplicate packets in SPAN configuration, an RSPAN will not pass Layer 2 data.

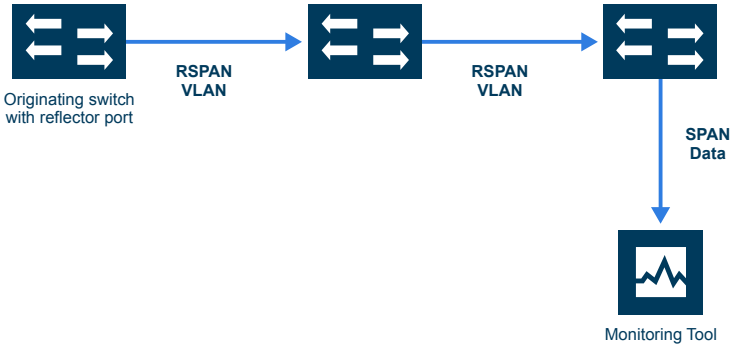

Figure 3: Cisco RSPAN Example: Data on the originating switch is sent over a RSPAN VLAN created using VTP and Reflector Ports

Cisco VACL

VLAN access lists (VACLs) overcome most SPAN limitations in addition to providing the ability to filter for certain types of traffic such as a TCP port or IP address. VACLs are ACLs that apply to all packets, whether bridged within a VLAN or routed to/from a VLAN (unlike ACLs that are typically configured on router interfaces and applied on router ports). See Figure 5. The maximum number of VACLs a switch can support is determined by the number of VLANs in a switch. For example, if a switch only has five configured VLANs, then five VACL capture ports can be created.

Users will mainly use VACLs to free up SPAN resources as a Band-Aid to a complete monitoring infrastructure. Configuring VACLs is usually reserved for more senior networking staff as VACLs require the most configuration attention of all the Cisco network visibility technologies. Many users can mistakenly block data from the VACL capture port if care is not taken when configuring the VACL. Like SPANs, source data cannot be sent to multiple VACLs limiting the benefit of having extra VACL ports as many times monitoring tools will have to see many VLANs at once leaving the user with one or two VACL capture ports that can be used.

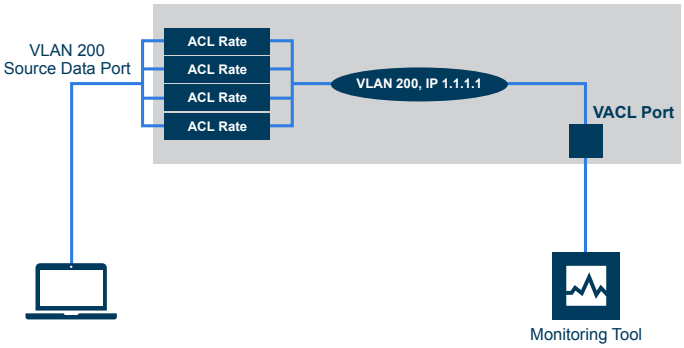

Figure 4: Cisco VACL example: Data from IP address 1.1.1.1 in VLAN 200 is forwarded to a VLAN capture port

Inline bypass protection of Cisco FirePOWER Intrusion Prevention Systems (IPS)

Given the attack continuum facing organizations before, during and after an attack, organizations today need continuous security monitoring to cope with the new security landscape. In the world of network security, visibility is everything. Limited access points to traffic in the infrastructure create blind spots. To cope with this broad range of challenges, organizations are keen on implementing effective inline security systems for effective protection. Cisco's FirePOWER IPS systems provide best-in-class protection to provide intelligent cybersecurity solutions. Implementing such solutions inline need the following considerations:

- **Ensure high availability and resiliency.** When implementing FirePOWER IPS inline, security operations often face concerns raised by network operations on high availability and resiliency.
- **Intelligent filtering of traffic to inline appliances.** Security operations personnel also have a need to get real-time network traffic of interest to avoid overloading the FirePOWER IPS
- **Upgrade, add/remove new IPS without waiting for network maintenance windows.** Security operations personnel need to maintain, upgrade, add/remove the FirePOWER IPS appliances without having to coordinate maintenance windows with network operations
- **Application-aware filtering to decouple performance of IPS from performance of the network:** This allows 1Gb FirePOWER appliances to be used in-line with a 10Gb network and 10Gb appliances with a 40Gb network, increasing overall utilization without compromising security.

Requirements for End-to-End Visibility

The challenges around gaining end-to-end visibility across Cisco infrastructure and technologies are driving IT departments to look more closely at an out-of-band monitoring infrastructure to provide the traffic visibility essential to manage, analyze, and secure their production networks. With today's complex infrastructure and technology transformation, traffic monitoring and network monitoring require an agile and dynamic approach built on a scalable and intelligent platform.

Agile and Dynamic: Monitoring tools may need to be added or removed, and traffic sent to the tools may need to be adjusted. Statically attaching tools to segments of the network is neither efficient, nor scalable. Additions of tools or the process to modify the traffic selection criteria of a NetFlow, SPAN, RSPAN, ERSPAN, and VACL port typically involves a reconfiguration of the production network, which can only occur during scheduled maintenance windows. With the drive to maintain 99.999% uptime, maintenance windows are normally short and infrequent (potentially monthly) which causes a notable delay before configuration change can be made.

Intelligent: Highly specialized monitoring tools are having difficulty keeping pace with today's high-speed networks. By receiving irrelevant or non-optimized traffic, the monitoring tools are susceptible to degradation in their efficiency and effectiveness which could lead to oversubscription, inaccurate analysis, and security risk. A monitoring infrastructure should intelligently provide only relevant traffic information reducing the unnecessary burden on the tools. In addition, features such as header stripping and decapsulation tunneling functions provide tools access to protocols and data they may otherwise be blind to.

Scalable and Pervasive: The number and variety of monitoring tools wanting to view traffic traversing the network infrastructure is increasing—whether it be application performance management or network performance management (APM/NPM), intrusion detection or prevention systems (IDS/IPS), forensics, NetFlow collectors, or customer experience management (CEM) tools. In addition, the network is growing at unprecedented speeds of 10Gb, 40Gb, and 100Gb. The network is also no longer physical, with the leaf of many data center networks now residing as a virtual element inside a server. Large enterprise networks can be dispersed geographically with remote locations that require monitoring by a centralized IT infrastructure staff. A scalable and pervasive approach to monitoring is needed across infrastructure and technologies.

Gigamon Visibility Platform

A New Approach to Monitoring

Gigamon's Visibility Platform provides a centralized out-of-band monitoring infrastructure for pervasive visibility across Cisco networks (physical or virtual) to centralized monitoring, data capture, and security tools. (See Figure 5).

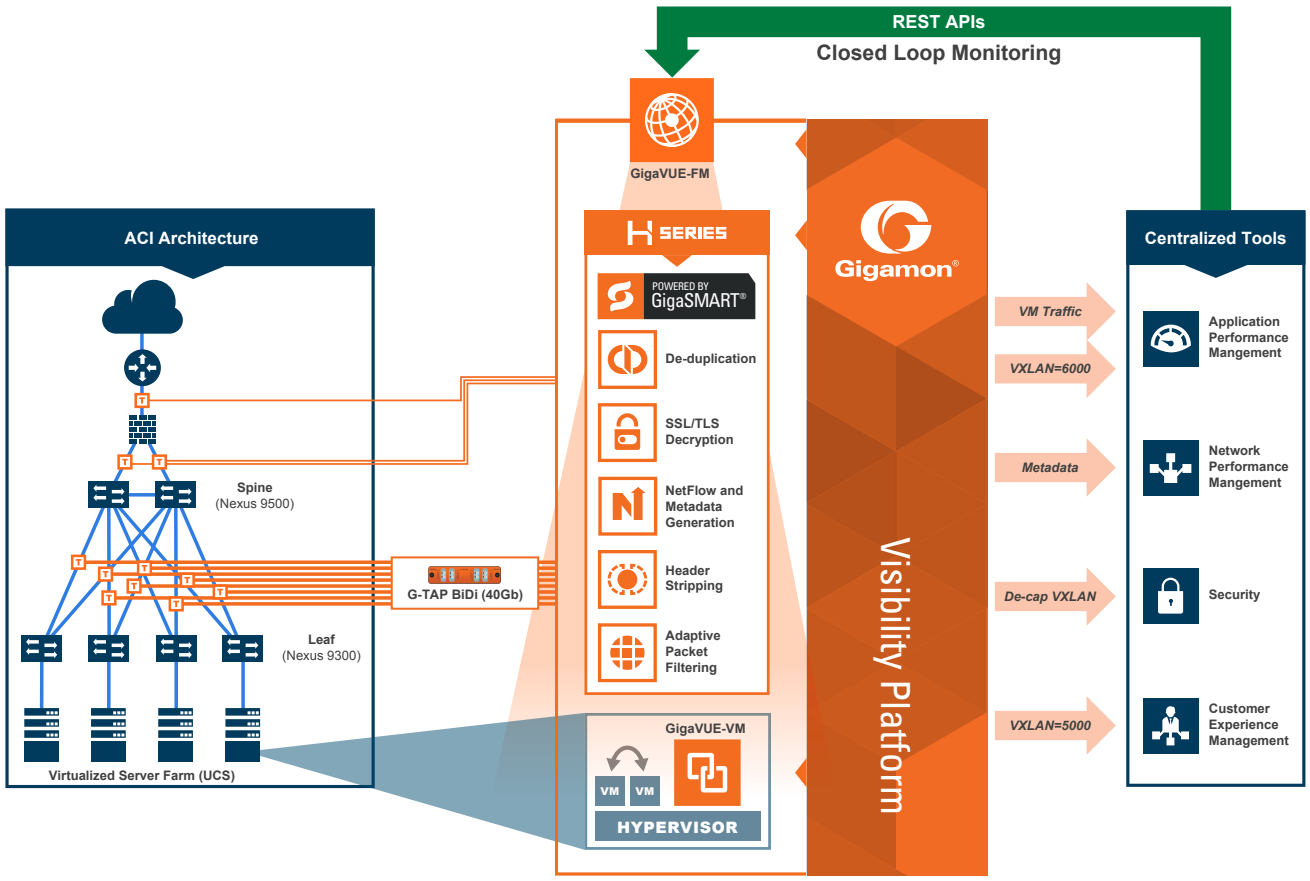

Figure 5: Gigamon Visibility Platform

Users can connect inputs in the form of SPAN or TAP ports, then aggregate, replicate, and intelligently filter and manipulate data at line-rate speeds to any number of tools. Users can connect SPANs, RSPANs, VACLs, ERSPAN, and TAP input ports to control the traffic flow from all network inputs to all monitoring inputs. One can think of the Gigamon Visibility Platform as the central hub of a monitoring infrastructure supporting 1Gb, 10Gb, 40Gb, and even 100Gb infrastructure links across physical and virtual environments. Gigamon 40Gb TAPs are available for both traditional and BiDi 40Gb links.

Visibility Platform Benefits for Cisco ACI Implementations

- The Visibility Platform helps in the transition from a classic data center network architecture to an ACI architecture
- De-duplication to relieve tool processing resources when packets are acquired from multiple collection points along a path by only forwarding a packet once
- Metadata Engine to generate high-fidelity, un-sampled NetFlow/IPFIX records from a centralized Visibility Platform; in addition to standard NetFlow and IPFIX records, other value-added metadata like HTTP URLs/Response Codes, DNS Request/Response sources and Certificate Anomalies can also be generated, so SIEM tools can detect and analyze nefarious activities in the network
- Use advanced filtering capabilities to non-intrusively TAP traffic inside the ACI fabric and filter based on parameters such as VNID (Virtual Network ID), Source VTEP (Virtual Tunnel End Point), Destination VTEP (Virtual Tunnel End Point), Source Endpoint Group (Source EPG) or other Endpoint Group parameters
- Leverage Adaptive Packet Filtering (content-based filtering) to correlate between logical and physical networks; monitor control/management plane exchanges between the APIC controller and the underlying ACI fabric or between network services connected to the ACI fabric. Allow SSL/TLS traffic flowing between application tiers through an ACI fabric to be decrypted for analysis by operational tools
- Enable the 40Gb links to be non-intrusively tapped using purpose-built 40Gb BiDi TAPs. 40Gb BiDi links use two lanes of 20Gb in each direction and regular TAPs inadequate
- GigaVUE-FM Fabric Manager for single-pane-of-glass management of the Visibility Platform, while also discovering and visualizing the topology of the connected Cisco network using Cisco Discovery Protocol (CDP) analysis

Benefits of Gigamon for Cisco Infrastructure

There are many benefits that users can gain by implementing the Gigamon Visibility Platform:

- Eliminate SPAN, RSPAN, and ERSPAN contention issues
- Share traffic across multiple monitoring tools and IT departments
- Make changes without affecting the production network while visualizing the network traffic interfaces
- Provide secure access to monitoring data
- Access 10Gb or higher network links with 1Gb monitoring tools
- Monitor asymmetric links and high availability standby links such as HSRP effortlessly
- Intelligently filter on Layer 2-4 fields within a packet, as well as "user- defined" filters that delve deeper into packet structures
- Load balance data from multiple 1Gb and 10Gb network links to multiple 1Gb and 10Gb network tool interfaces
- Leverage advanced features such as packet slicing, masking, source port labeling, tunneling, de-duplication, header stripping, time stamping, and L7 load balancing
- Strip VXLAN, VN-Tag and Cisco FabricPath headers before delivering them to the appropriate tools
- Filter FCoE (Fiber Channel over Ethernet) traffic IP VXLAN headers before delivering them to the appropriate tools

Agile and Dynamic Patented Flow Mapping® Technology

Gigamon's patented Flow Mapping technology allows the creation of traffic distribution maps that can direct monitored traffic to any number of monitoring tools at line rate. Flow Mapping is different from port filtering—network engineers create map rules that direct data to the desired monitoring port(s) (see Figure 6).

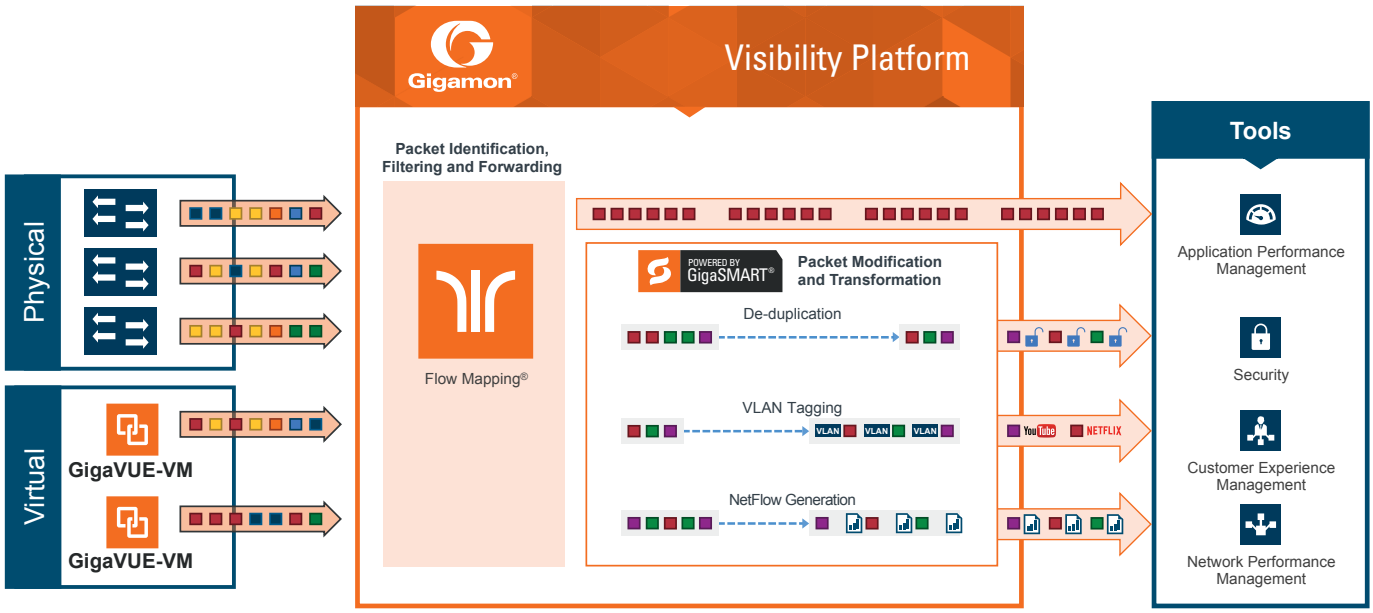

Figure 6: Example of Gigamon Flow Mapping technology with GigaSMART traffic intelligence

Once a map is created, input ports can be bound to the map. This allows for dynamic changes to data flows that would be impossible using port filters as network engineers would have to change the filtering on each port individually. Using other technology such as collectors and pass-alls, users can have access to unfiltered traffic while traffic is being filtered using the map. Gigamon users can augment the power of Flow Mapping technology by further reducing traffic loads on egress tool ports as well. All these features create a powerful and dynamic monitoring platform.

Intelligent Packet Transformation to Enable Tool Optimization with GigaSMART®

Gigamon GigaSMART technology can enhance the monitoring infrastructure with a range of applications and features to enable the modification, manipulation, transformation and transport of monitored traffic from the Cisco network (physical or virtual) to the monitoring tools.

GigaSMART provides capabilities to modify packets at line rate and adds valuable information through features including packet slicing, masking, source port labeling, tunneling, de-duplication, header stripping, time stamping, and Layer 7 load balancing.

De-duplication

- Relieve tool processing resources when packets are gathered from multiple collection points along a path by only forwarding a packet once
- Remove packet duplication caused by inter-VLAN communication or incorrect switch configuration

Header Stripping

- Eliminate the need for monitoring tools to decipher protocols
- Allow easy filtering, aggregation and load balancing of packets with headers removed
- Support for ISL header/trailer removal and VXLAN, VN-Tag, VLAN, MPLS, and GTP-U tunnel stripping

SSL/TLS Decryption

- Provide visibility into encrypted sessions
- Send decrypted packets to multiple inline or out-of-band tools: IDS, DLP, APM, CEM, etc.

Adaptive Packet Filtering

- Offers regular expression pattern matching anywhere within the packet
- Filter, at wire speed, any string in the packet stream on monitored network segments
- Decapsulate traffic in overlay networks including VXLAN, ERSPAN, VN-Tag, and several others
- Extends visibility into storage area networks and iSCSI network traffic

NetFlow and Metadata Generation

- Offload NetFlow and metadata generation from network elements and generate critical security-specific metadata such as URLs and HTTP response codes from any traffic
- Obtain high-fidelity, unsampled 1:1 packet to flow record statistics
- Export records to up to six (6) collectors supporting NetFlow v5/v9 and IPFIX as well as extensions for other metadata (ex. URL, HTTP response codes, SIP)

Application Session Filtering

- Forward traffic corresponding to application sessions to security appliances increasing their efficacy and performance
- Classify flows of interest using signatures to filter applications such as video streaming, email, web 2.0, and other business applications
- Provide complete visibility into traffic flows by forwarding all packets from session initiation to termination to security and monitoring tools

Packet Slicing

- Reduce packet size to increase processing and monitoring throughput
- Optimize the deployment of forensic recorder tools

Masking

- Conceal private data including financial and medical information
- Empower network monitoring tools to perform their task and maintain PCI and HIPAA compliance
- Enable more data storage in a recorder application

Source Port Labeling

- Add labels to the packets indicating the ingress port
- Easily identify where a packet is coming from
- Enhance the efficiency of network monitoring tools by eliminating the potential of duplicate data streams

Tunneling

- Encapsulate and forward packets to monitoring tools between networks on separate routed paths
- Enable routing of data from lights-out data centers to central monitoring facilities

Advanced Tunneling including ERSPAN Termination

- Provides tunnel termination of ERSPAN sessions enabling consolidation, filtering, and forwarding of relevant ERSPAN traffic
- Enable analysis tools to receive filtered traffic from remote networks

Time Stamping

- Add packet time stamps at line rate for subsequent analysis
- Troubleshoot and measure application response times jitter and latency

L7 Load Balancing

- Traffic distribution among multiple ports based on fixed or variable matching fields
- Filtering and traffic distribution capabilities applied to any field in the packet beyond Layer 2 – Layer 4 and into the application layer

Scalable Visibility into Cisco Virtual Infrastructure

As an integral part of the Gigamon Visibility Platform architecture, the GigaVUE-VM node addresses visibility requirements in virtual environments. With GigaVUE-VM visibility nodes deployed, virtual traffic can be intelligently detected, selected, filtered, and forwarded locally or remotely, without any changes to the operational procedure or adding any further complexity to the underlying infrastructure. Currently deployed monitoring and management tools can thus be utilized to analyze traffic flowing across the virtual infrastructure using best-of-breed virtual switching including vSphere Distributed Switch (VDS) and Cisco Nexus 1000V (Figure 7).

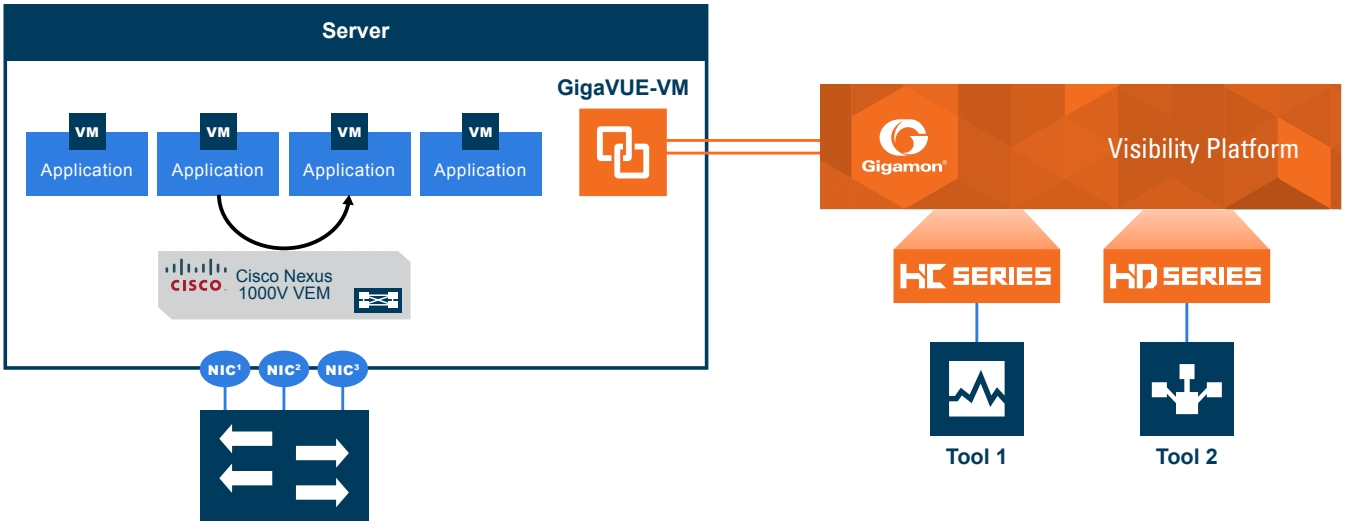

Figure 7: Visibility in Cisco Nexus 1000V deployments with GigaVUE-VM visibility nodes

Inline bypass protection of Cisco FirePOWER Intrusion Prevention Systems (IPS)

One of the services provided by the Gigamon Visibility Platform is "inline bypass". This capability allows multiple security tools to be placed inline with the network, while alleviating concerns on impact on network availability and increasing the agility, flexibility and utilization of both the security tools and the network. The use of Gigamon inline bypass with Cisco FirePOWER IPS provides the following joint benefits:

- **Enhanced security:** Close the gap in enterprise security by protecting high-value applications and data assets in a data center
- **Network Reliability:** Reduce risk of network outage with pass-through or failover contingencies
- **Scale:** Easily scale to monitor networks of any size or multiple network links with a single FirePOWER IPS.
- **Increased Efficiency:** Implementing the Gigamon bypass solution extends the life of 1Gb Cisco FirePOWER IPS using capabilities such as application-aware filtering and load balancing, since much of the traffic often does not need inspection (e.g. YouTube traffic or traffic that has already gone through one level of inspection)
- **Pervasive visibility:** Gain full network visibility from all parts of the network
- **Security Reliability:** Ensure availability of Intrusion Prevention Systems (IPS) using features such as heartbeat detection
- **Flexibility and Agility:** Simplify additions/removals of multiple security tools within your DMZ without compromising security or network availability

Achieving End-to-End Visibility

Figure 8 shows an example of a large Cisco network with a Gigamon Visibility Platform providing end-to-end visibility. In this diagram all major switch-to-switch connections are tapped using Gigamon G-TAP™ network TAPs or integrated TAPs with the GigaVUE® visibility node. By tapping at strategic locations, network engineers have increased visibility into traffic. For example, by tapping the interface between the Internet and the firewall or the firewall and router, engineers can view all traffic coming into and out of the network from the Internet. Because TAPs are used, all traffic at full line rate can be viewed without missing traffic or degrading the performance of the production switches and routers. SPAN port traffic is routed to the platform where it can be aggregated, replicated, and filtered to multiple monitoring tools. In most new 10Gb infrastructures SPAN traffic is usually limited to the access layer as an easy way to view end-user traffic. GigaVUE nodes can be stacked, cascaded, or clustered in order to be controlled from one central interface that can dynamically route specific traffic to specific tool ports. GigaVUE-VM provides visibility into the Cisco virtual environment. Traffic is tunneled back to a GigaVUE visibility node, decapsulated by GigaSMART technology, and sent to your physical centralized monitoring tools. By centralizing tools, CAPEX can be reduced and management is simplified helping to reduce OPEX.

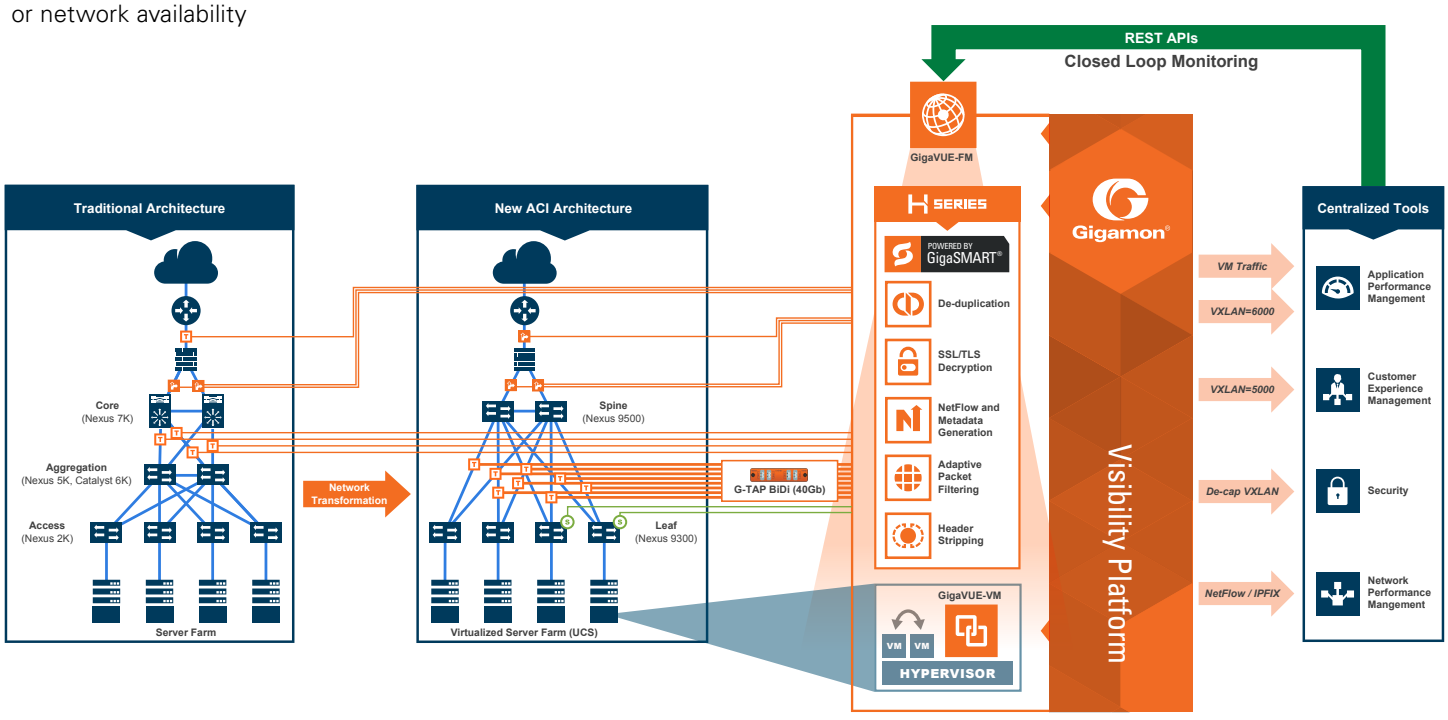

Figure 8: Example of end-to-end visibility for your Cisco infrastructure

End-to-End Security of Cisco Networks Using GigaSECURE

The GigaSECURE® Security Delivery Platform (SDP) connects into the network, both physical and virtual, and can be configured to deliver traffic to all of the applications that require it. Security appliances simply connect into the GigaSECURE platform—at whatever interface speeds they are capable of—to receive a high-fidelity stream of relevant traffic from across the network infrastructure. The GigaSECURE platform also extracts flow-based metadata from network traffic, which can be routed to various security tools for analysis. Additionally, it also serves as a platform for deployment of a diverse set of security solutions that need to sit inline with the network traffic. Inline security solutions typically provide the ability to take preventive measures in real-time on detection of threats, malware or anomalous behavior.

The Security Delivery Platform is comprised of GigaVUE visibility nodes, GigaVUE-OS™ software with patented Flow Mapping technology, traffic intelligence functions powered by GigaSMART, and a centralized fabric controller (GigaVUE-FM), which, when implemented together provide an ideal platform for security delivery.

The features and benefits of this platform include:

- **Network-wide Reach:** The GigaVUE TA Series of visibility nodes, along with the GigaVUE-OS in conjunction with whitebox Ethernet switches, provide a cost-effective way to provide scale-out traffic visibility. The combination of the GigaVUE-VM and the GigaVUE TA Series enables visibility into east-west traffic and visibility across the internal campus and data center networks.
- **NetFlow (IPFIX) and Metadata Generation:** The flow records can be served up to a variety of security solutions that analyze flow metadata. The flow metadata generation is done at very high throughput so as to generate high-fidelity records that are essential for good security analytics. The solution also enables custom templates to be defined so that the information that can be gleaned from the traffic can be highly tailored to the specific deployment environment.
- **Application Session Filtering:** This powerful capability allows precise control of what types of traffic data are sent to security tools based on L4 - L7 and more sophisticated content matching, thereby ensuring that security solutions are focused on working off network traffic that is most relevant to them, while simultaneously offloading those appliances from having to process large volumes of irrelevant data. The identification of what is relevant and what is not can be customized to each security appliance.
- **SSL/TLS Decryption:** Decrypting those encrypted channels of communication is best handled within the GigaSECURE Security Delivery Platform, so that this is done once, at very high performance, thereby eliminating this blind spot simultaneously for multiple security appliances that do not have the ability to deal with encrypted communications.
- **Inline Protection and Load Balancing:** Many security appliances work inline with the network traffic to block malware and malicious activities in real time. Other security devices inspect traffic and conduct analysis in an out-of-band mode for detection and alerting purposes. The GigaSECURE Security Delivery Platform provides a common platform to serve traffic feeds for both inline and out-of-band security deployments connected to the platform simultaneously.

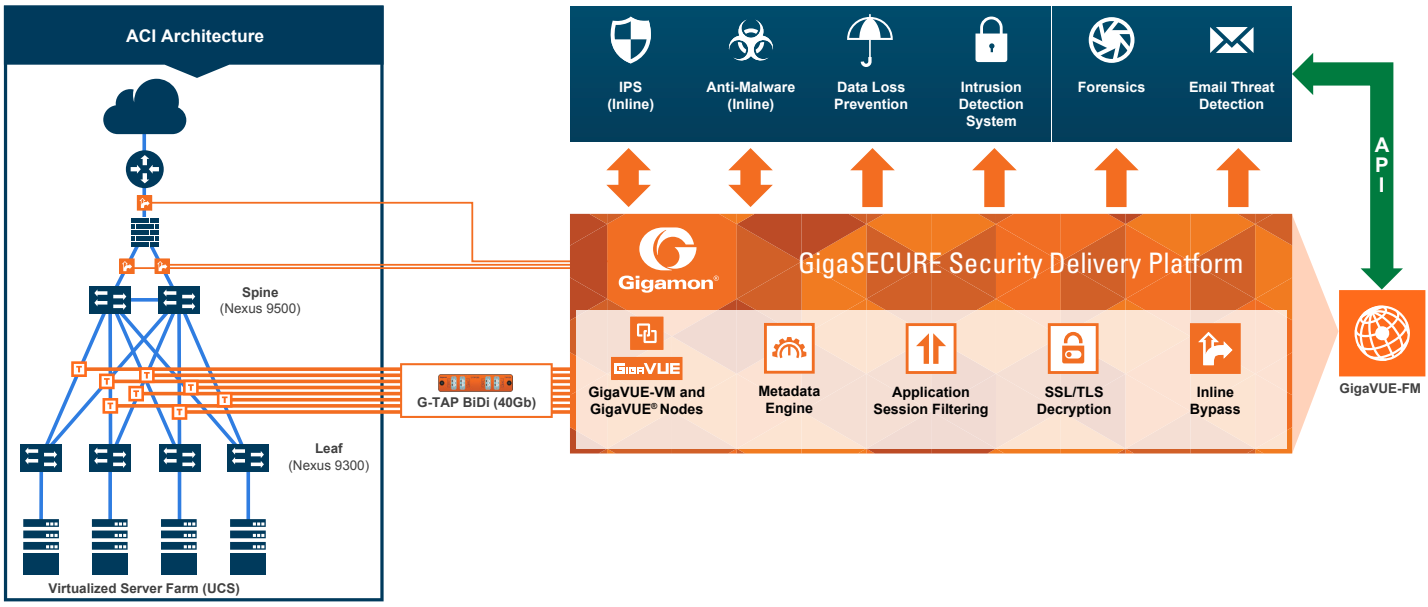

Figure 9: End-to-End Security for Cisco ACI with GigaSECURE Security Delivery Platform

Optimize and Secure Your Cisco Network with Metadata Generation

NetFlow is commonly used in Cisco networking environments as an effective way for traffic monitoring and collecting IP-level statistics. However, NetFlow in a production network can run the risk of spikes in processor/memory load and, in extreme situations, can lead to a drop in production traffic when contention is high. Often administrators correct for this by setting a low sampling rate— and too low a sample rate can result in important network events being missed. Even if the network elements can handle the load, data centers with distributed applications on a highly virtualized infrastructure pose a new problem—VM mobility. This raises the need for NetFlow traffic to be collected from a central point without impacting production traffic. Given that the Gigamon Visibility Platform has access to all the traffic that is flowing through the network, GigaVUE visibility nodes are in a unique position to not only generate NetFlow and IPFIXrecords, but also provide contextual metadata visibility into traffic that helps SecOps administrators analyze any nefarious activities like command-and-control takeover of servers or DDoS attacks by tracking HTTP URLs/Response Codes, DNS Queries/Responses and Certificate anomalies. Using this out-of-band approach also eliminates the risk of losing production traffic as a result of generating NetFlow and metadata (see Figure 10).

Conclusion

By leveraging the power of the Gigamon Visibility Platform and the GigaSECURE Security Delivery Platform, NetOps and SecOps teams can now achieve pervasive and dynamic visibility across their physical, virtual, and emerging Cisco architectures, such as ACI. Data can be intelligently delivered to various management, monitoring, and security tools supporting the diverse monitoring needs of network, security, application, and server groups as they strive to maintain maximize uptime, secure the network, realize operational efficiencies, and gain greater insight into business decision making. The Visibility Platform allows IT organizations to more efficiently manage and secure their Cisco networks, and provides a solution that can quickly evolve and scale as network needs change.

About Gigamon

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon's Visibility Platform 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 Visibility Platform visit:
www.gigamon.com

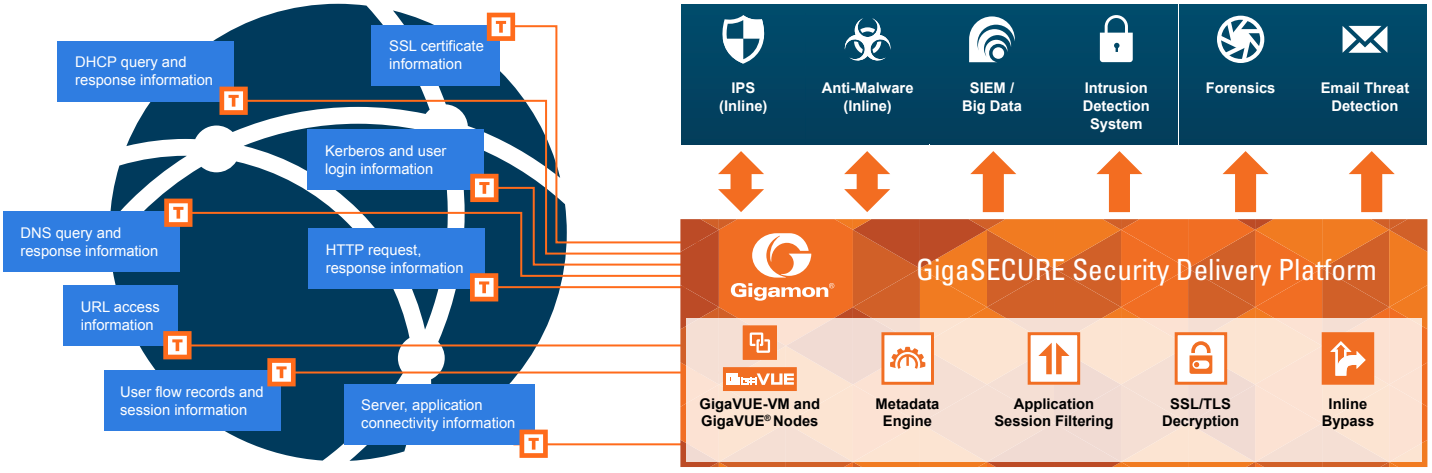

Figure 10: Example of Gigamon NetFlow and metadata generation

3041-08 03/17

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