In These Transformative Times, Take These Practical Steps to Ease the Network Burden

14 HANDS-ON WAYS GIGAMON ENABLES STABLE, SECURE AND EFFICIENT OPERATIONS

If you're tasked with securing your network and ensuring its performance, you'll want to review these 14 customer-driven use cases to see the real-world ways the Gigamon Visibility and Analytics Fabric™ can make this happen. It's vital given the sudden flood of people working from home, which has replaced traditional intranet traffic with WAN-based internet traffic — with all of the operational and security challenges that come with that shift.

We call this the new tomorrow, and below you'll find practical, easy-to-deploy implementation examples that demonstrate how you can help assure network performance, eliminate vulnerabilities and maintain infrastructure uptime.

#1. OVERLOADED VPN CONCENTRATORS WITH DOUBLING OF INTERNET TRAFFIC

Certain organizations, particularly U.S. federal agencies, require remote employees to access on-premise IT infrastructure for internal resources and external internet use via VPN tunneling. This significantly increases the number of concurrent tunnels, forcing concentrators to be scaled up with more potential blind spots. Traffic must also go through the full security stack and be sent to network monitoring tools. With all traffic backhauled onsite and then boomeranged back to internet websites, traffic is potentially twice normal levels. There is no split tunneling support to separate internally versus externally destined traffic. This complication can also cause packet duplication. Lastly, a significant portion of internet traffic is irrelevant — traffic from Netflix or Microsoft Windows updates, for example — and can be safely ignored.

Solution: Federal agencies and a branch of the U.S. armed forces deployed GigaVUE® HC visibility appliances with three GigaSMART® capabilities: De-duplication, Application Filtering and Application Metadata. Working together, these Gigamon Visibility and Analytics Fabric™ solutions 1) mirrored all traffic, including traffic from added VPN appliances, 2) removed duplicate packets, 3) provided additional metadata for SIEM tools and 4) filtered out select applications to offload security and monitoring tools. Gigamon Professional Services optimized and expedited the deployment.

#2. IDENTIFICATION OF EXPIRED TLS CERTIFICATES, UNTRUSTED SOURCES OR SELF-SIGNED CERTS

Financial services, healthcare and many other types of organizations use these certificates to help facilitate encryption and authentication. They are also effectively mandatory for web servers. Without them visitors will quickly move on. With validity dates becoming shorter, sometimes only a few weeks, it is imperative to find the certs that are defunct. IT needs to detect non-trusted or self-signed certificates for TLS-decrypted traffic that could result in nefarious activity.

Solution: One of America's largest credit agencies, as well as major international banking institutions use GigaVUE HC Gigamon Visibility and Analytics Fabric solutions, combined with two GigaSMART applications: SSL/TLS Encryption and Application Metadata Intelligence (AMI). AMI provides certificate expiry dates, as well as any revoked or expired certificates along with the names of the application servers using these certs for compliance. Other relevant AMI attributes include Valid Not Before, Valid Not After, Serial Numbers and Signature Algorithm to help validate certificate use. Real-time alerts can be automatically generated to expediate remediation.

#3. MANAGING ENCRYPTED TRAFFIC BLIND SPOTS WITH REGULATORY COMPLIANCE CONFLICTS

Several industries, including financial services and healthcare, are subject to privacy standards. For instance, HIPAA mandates patient record confidentiality, with data in motion secured via encryption. Decryption solutions should not decrypt but bypass this traffic and send it directly to the server.

Solution: Gigamon proposed that one of the largest healthcare organizations in California, a major online brokerage services provider, as well as a global wealth management and investment bank use the visibility and analytics fabric in conjunction with Gigamon Inline Bypass and GigaSMART (with TLS Decryption) modules.

With TLS 1.2 and prior versions, the Subject Name Identifier (SNI) in the TLS handshake "client hello" enables bypass. For TLS 1.3, server certificates and Subject Alternate Name (SAN) in the "server hello" are no longer visible. The answer is to decrypt traffic inline, completely within the GigaVUE HC Series platform with its full-proxy mode and then re-encrypt before forwarding data to and from the server. In this case the SNI can be matched with the certificate SAN and server identity; self-signed certificates can be verified to provide other anomaly detection and threat hunting activities.

#4. TROUBLESHOOT AND QUICKLY REMEDIATE POOR PERFORMANCE

IT needs to determine if the underlying cause is from the network or application. To evaluate, metadata can assist IT. AMI allows NetOps teams to use application broadcast and multicast control packets. Applications send these packets at regular intervals, and by analyzing them over time, administrators can determine average intervals between them. A differential in packet interval time could indicate device malfunction, network congestion or network traffic storms. Attributes involving SNMP, SMTP, UPNP and other broadcast packets can also be useful in pinpointing root causes.

Solution: AMI can isolate the traffic for, and help tools debug, poor videoconferencing experience in apps like Zoom, GoToMeeting and WebEx, which is especially pertinent today. Usable attributes of video embedded in an application include:

+ Starting frames per second rate, and how it changes over time
+ Bitrate changes over time
+ Drop from HD to standard video quality
+ Length of video
+ When the user stopped the video

Application and network performance monitoring tools can use this information to determine the user's true video viewing experience and potential causes of service degradation.

To determine if application response times are the underlying cause, metadata related to HTTP, ICMP and IPMI can be exported to network monitoring tools to detect and report failures of devices or connections, network bandwidth utilization of links, round trip times and other aspects of network operations. You can pinpoint application servers with slower response times using average and top response times (such as DNS servers, which will cause latency and overall undesirable user experience).

#5. ENSURING PROPER VOICE QUALITY FOR REMOTE CALL CENTER OPERATIONS

Service providers with a sudden dispersed, mobile workforce must guarantee that conversations from distributed calls have the required audio clarity and that recorded conversations satisfy compliance mandates. At the same time, administrators look to minimize their expansion of voice recording and quality measurement tools.

Solution: A leading telco with millions of customers evaluated the GigaSMART SIP/RTP Correlation application that enables complex IP-based voice and video traffic to be easily sorted, filtered and/or sampled by identifiers, such as by phone numbers. Now the telco's IT team can accurately identify and

extract pertinent VoIP and other media streams, including full subscriber conversations. Subscriber-specific control and media sessions are intelligently forwarded to specific tools, such as voice quality analyzers, performance monitoring, analytics and security tools. Filtering can be implemented on a specific user ID or ID range. It also supports whitelisting for high-priority sessions.

This allows service providers to rapidly adapt to shifting network patterns created by a mobile workforce. With irrelevant conversations filtered out, less is spent on voice recording tools and ROI is increased. Compliance is improved by extracting only relevant streams of interest. With visibility into all potential VoIP streams and forwarding to tools, audio intelligibility and user-experience issues can be found and corrected.

#6. IDENTIFY CUSTOMER BANDWIDTH BY APPLICATION AND CATEGORY

Service providers and other organizations need granular visibility into network usage to discover what applications are running, how much throughput they are consuming and whether any of the applications should not be in use. With users nefariously using network resources to access Facebook, Instagram or other social networking sites or streaming media, increased bandwidth consumption can cause higher priority traffic to suffer performance loss.

Solution: Gigamon proposed that a large satellite-based service provider use Gigamon Application Filtering Intelligence (AFI). AFI provides the identification of more than 3,200 apps and their bandwidth utilization. Applications can also be grouped into categories such as social media and streaming media. IT may leverage this data to enforce bandwidth limits by application via rate-limiting or other methods.

AFI helps IT prioritize the most critical traffic based on apps. Modern networks typically incorporate quality of service (QoS) methods to give priority to select traffic, but this is based on L2–L4. With AFI, you can give traffic from specific apps precedence. Typically, these apps would involve things like e-commerce, outbound web-based servers or VoIP and would be elevated over things like CRM, email and internal streaming media users.

#7. IDENTIFY TLS VERSUS NON-TLS TRAFFIC

For a host of reasons, organizations need visibility into which traffic is encrypted. One of the principle needs is to identify encrypted apps running on nonstandard ports. Apps normally are assigned to specific ports, and IT can to some degree identify and filter them based on port. However, for many apps this is not the case, especially when SSL/TLS encrypted, running on nonstandard ports, and IT desires to filter out ports such as 443.

Another concern involves port spoofing. With traditional client-server traffic, hackers can use port spoofing techniques where they send SSH traffic over port 443, which is used for SSL, thus causing the traffic to be misidentified as SSL. A third aspect involves locating weak ciphers to help ensure security compliance. Ideally, clients and servers should employ only the strongest cipher suites available and negotiate to one of these during the TLS handshake, but this is not always the case.

Solution: A top internet infrastructure company based on the east coast of the U.S. has used AFI to identify and manage TLS traffic. AFI informs SecOps teams which ports are involved and then filters as needed. AFI can also see through port spoofing misdirection and properly classify traffic. With the addition of Gigamon Application Metadata Intelligence, IT can be alerted to the use of weak ciphers on all TLS connections, including 1.3, as well as the applications and systems hosting these apps, and take corrective action.

#8. ENSURE COMPLIANCE OF IOT DEVICES AND REMOVE THOSE THAT DON'T BELONG

The deployment of IoT in the network is expanding at a rapid rate. From medical provider infrastructures to the manufacturing floor to smart homes, these devices provide new sources of data that can overwhelm the network and potentially include unauthorized devices.

Solution: Gigamon proposed AFI to one of the largest healthcare organizations in California to help it get a handle on its medical and non-medical devices. The first step in finding IoT devices is to identify the applications they are running, and then block any apps used by rogue elements. As traffic from IoT devices is fed from wireless sensors to the corporate network, the Gigamon Visibility and Analytics Fabric sees it all. Then the end IoT clients are identified and administrators can validate compliance.

If unidentified apps are found, the sources of this traffic can be tracked down and the IoT device and nature of its app determined. Using deep packet inspection, AFI then identifies and filters custom applications by defining signatures and searching for these regular expressions in the header or payload.

Gigamon also suggested using Gigamon ThreatINSIGHT™ network detection and response SaaS solution. This platform quickly accesses real-time network data to accelerate threat investigations. With it users can:

+ Prioritize threat severity and remediate to reduce mean time to detection and response
+ Investigate in real-time and quickly triage alerts and gather intelligence to direct efficient responses
+ Gain broad situational awareness across physical, virtual and cloud networks
+ Focus SecOps on threats, not tools, and ensure rapid deployment with zero maintenance

#9. ELEPHANT FLOWS ARE SLOWING AND POSSIBLY CRASHING TOOLS

Elephant flows are large continuous TCP/UDP/QUIC-based flows through the network. With video and mobile applications being the predominate source of traffic today, networks and tools either need to scale up at great expense or alternatives must be found to offload them from the content deluge. Administrators also need to troubleshoot performance issues in minutes, not months.

Solution: A major government health agency turned to AFI to prevent overloaded tools. They focused on relevant flows by filtering out high-volume, low-risk traffic. Some content can be deemed safe by design, such as high-bandwidth Amazon Prime and Hulu streaming. This content does not have, for instance, hidden command-and-control code. The content is from a known, secure source.

NetOps teams leverage various methods to properly route traffic. With AFI, these teams are also able to identify missing or misclassified traffic and direct it to the right tools. Furthermore, AFI can help validate legacy routing methods to ensure accuracy and completeness.

Threat detection tools are primarily interested in suspicious traffic. If these tools spend their processing power inspecting all the traffic in the network, then most of the tools' resources are being spent without yielding any additional threat detection. Some network tools focus exclusively on certain applications and protocols, and therefore feeding them anything outside of a narrow protocol suite (HTTP or email, for example) is not necessary.

AFI helped enable network monitoring tools to expedite network analysis and diagnose performance issues within five minutes, not six months as before.

Elephant flow issues are also greatly helped by Gigamon Advanced Flow Slicing to ease the burden on tools. With this GigaSMART application, IT can granularly select and drop superfluous packet content and reduce traffic by over 60 percent.

#10. ACCELERATE CISCO APPLICATION CENTRIC INFRASTRUCTURE (ACI) UPGRADES

Cisco ACI is a leading SDN platform for application agility and data center operations with a single point of control. This policy-based networking solution combines hardware, such as the Nexus line of switches, with software components, including a data center policy engine. To function properly and provide required security, ACI needs a detailed understanding of the applications present and their co-dependences. Organizations combine ACI with application security-policy-management tools and intrusion prevention system (IPS) solutions. Yet, they need accurate granular application identification in real time.

Solution: A large multinational bank and investment services company is evaluating Gigamon AFI to help accelerate its ACI upgrade, which is significantly behind schedule. AFI uses deep packet inspection to identify applications and protocols from network packets and appropriately filter them. AFI classifies applications based on various attributes around traffic behavior, and uses flow-based matching, bi-directional flow correlation, heuristics and statistical analysis. This lets IT accurately identify and filter traffic from over 3,000 off-the-shelf software applications, as well as from custom apps. The company is evaluating AFI

in conjunction with vArmour to assist with defining app relationships, baselining their behavior and enforcing security policies.

#11. DETECT THREATS BY ANALYZING REMOTE EMPLOYEE VPN TRAFFIC FOR UNUSUAL EVENTS

Due to increased demand for employees working from home, organizations must expose new services and profiles for remote connectivity. This is a new challenge, since it's very sensitive information and therefore IT needs to analyze the traffic from remote workers. Third-party tools can be leveraged to spot anomalies.

Solution: A major technology company is evaluating Gigamon SSL and flexible inline solutions to decrypt SSL traffic and send it to security tools, both inline and out of band, including advanced threat protection solutions from FireEye and Trend Micro.

Other methods to consider in identifying questionable behavior include uncovering untrusted SSH, RDP and Telnet remote connections. This is accomplished by looking at leading indicators, such as bandwidth usage, longevity of these connections, IP reputation and Geo-location. This can help uncover the detection of unauthorized external remote connections used for data exfiltration.

Suspicious WAN activity can be detected by identifying command-and-control attacks using machine learning. Admins can determine whether a domain is legitimate or was generated using a botnet-controlled domain generating algorithm (DGA). SecOps teams can verify authenticity by leveraging external sources, such as VirusTotal. Dashboards of interest here include the total unique domains seen on the network and those predicted to be legitimate versus DGA generated.

#12. OVERLOADED VIDEO CONFERENCING SYSTEMS

With educational institutions from K–12 to graduate schools using remote broadcasting systems for instruction, organizations that service them must expand current solutions and find new, efficient management and packet acquisition methods to offset the resulting large increase in traffic volume.

Solution: An existing Gigamon customer that provides unified communications, contact center and other services needed to expand its existing footprint due to its educational customers' remote classrooms. It purchased additional GigaVUE-HC2 series visibility nodes, GigaVUE-FM Fabric Manager for centralized management, G-vTAP VMs and physical Gigamon TA TAPs.

#13. APPLICATION PERFORMANCE TOOLS ARE ENCUMBERED

A Gigamon customer observed that its remote traffic had increased by a factor of two to four times. The increase has continued to build, with no end in sight. With rules in place to require all content be sent to both security tools and the Riverbed Application Response product, the latter solution was getting overloaded. Existing deployed Gigamon solutions provided data de-duplication, but more was needed.

Solution: A major U.S. healthcare provider has expanded its Gigamon solutions to include GigaVUE HC3 Series visibility and analytic nodes, more Gigamon TA10 TAPs and the GigaSMART Packet Slicing application. While the security tools needed to see all traffic within each packet, the Riverbed APM tool needed to observe only the first 768 bytes. The security tool port was reconfigured as a hybrid port, and traffic sent from this security tool to the Riverbed APM tool was truncated so only the first 768 bytes were sent. This radically reduced the total traffic sent and eliminated the data overload problem.

#14. NEED TO FLEXIBLY SCALE TRAFFIC TO PREVENT OVERWHELMING SECURITY TOOLS

Service providers are observing a substantial increase in traffic, both from internal employees and external customers who are working from home. Internal traffic is sent through a smaller subset of security tools, but it must be identified by application to determine which tools to use. At the same time, provider networks need to scale traffic flexibly since the tools cannot be expanded quickly enough. With traffic flows varying throughout the day and transient spikes occurring, this data overload is amplified.

Solution: A major U.S. service provider deployed GigaVUE HC2 and GigaVUE HC3 Series visibility and analytics nodes, Inline Bypass and GigaSMART applications, including NetFlow, FlowVUE® and Application Filtering. FlowVUE allowed this provider to scale traffic up and down as needed. FlowVUE uses IP-based flow sampling to provide a representative view of traffic for diagnostic coverage and thus allows customers to connect high-speed pipes to the tools' lower speed pipes. Being able to parse subsets of traffic is critical in this new working-from-home environment, as is sending each set of traffic through the correct set of tools, and AFI provided those capabilities. Flex Inline minimized the impact on traffic.

It's Easy to Get Started

We choose these 14 examples because they can produce big results in a short amount of time — without undo heavy lifting. Some Gigamon customers, in fact, have implemented many of these solutions in a matter of weeks, if not faster. So, if you're looking for immediate ways to address the challenges of the new tomorrow today, contact Gigamon for a live demo.

Gigamon®

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