Understanding the Value of Application-Aware Network Operations

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Gigamon®
Shamus McGillicuddy
June 2019

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

UNDERSTANDING THE VALUE OF APPLICATION-AWARE NETWORK OPERATIONS

MODERN NETOPS MUST BE APPLICATION-AWARE

Network operations teams can no longer ignore the application layer. Application experience can make or break a digital enterprise, and today most enterprises are digital. To deliver optimal performance, network operations tools must be application-aware. However, application-awareness in the network and security tool layer is expensive and difficult to scale. Enterprises can mitigate these challenges with a network visibility architecture that includes application-aware network packet brokers (NPBs).

EMA recommends that today's network operations teams modernize their approach with full application visibility. EMA research has found that network teams are increasingly focused on directly addressing security risk reduction, service quality, end-user experience, and application performance. All of these new network operations benchmarks will require deeper application-level visibility. For instance, a network team focused on service quality will want to take a top-down approach to performance management. They need to stop starting at the network layer and trying to correlate it with end-user complaints. Instead, they need to start at the application layer and dive into the network data for answers. Application insight should tell them were to look and what network data can reveal about real problems, threats, and risks to the business.

This awareness is also critical because applications are becoming more diverse and numerous. For instance, network managers say the classes of applications that are generating the most traffic on their networks today are cloud applications, secure web applications (HTTP), and collaboration. Many of these services will simply look like Port 80 or Port 443 traffic to old-school tools, with no ability to identify criticality. Layer 7 visibility allows network operations teams to know which applications need the best quality of service, which ones need to be tightly secured, and which ones they can safely ignore or deprioritize.

APPLICATION VISIBILITY IS NOT EASY

Application awareness is difficult to achieve for a variety of reasons. Network operations tools either lack this visibility, or the visibility requires resource-intensive deep packet inspection. Thus, IT organizations often apply it sparingly.

Some tools advertise application awareness, but it is limited. Older-generation packet monitoring tools can identify TCP ports, which offer some context for the application. However, the effectiveness of this approach has eroded with the rise of web-based services. Now, an enterprise might have hundreds of applications that access Port 80 (HTTP) or Port 443 (HTTPS). Without more context, everything looks the same.

URL filtering helps to some extent. By correlating the TCP port number with Facebook.com, for instance, the network team knows that certain traffic is associated with social media activity. However, Facebook has evolved into an platform of its own, running video, voice, gaming, and more, meaning Facebook traffic is too diverse to manage without true application awareness. Also, port spoofing is a significant weakness of this TCP port filtering approach. Malicious actors often hide their malignant traffic by spoofing legitimate port numbers. An advanced threat might appear as a harmless web session or email traffic. In reality, it's a penetration of your perimeter.

Another approach to application visibility is filtering traffic by protocol. For instance, network managers could forward SIP and Real-Time Transport Protocol (RTP) traffic to unified communications monitoring tools. FTP traffic could be forwarded to data loss prevention systems, and HTTP traffic could be forwarded to a next-generation firewall. However, malicious or frivolous traffic can hide in these protocols, too.

Ultimately, the best way to achieve application awareness is full Layer 7 inspection, with application and protocol decodes. This approach is effective, but it pushes tools to the limit. When an enterprise turns on Layer 7 visibility in a network performance management tool or a next-generation firewall, line rate performance of that tool can degrade. When traffic increases, many tools will fall down. Also, these individual deep packet inspection tools do not share their Layer 7 insights, because these capabilities are proprietary. Consequently, enterprises end up with pockets of visibility.

Enterprises should consider protecting Layer 7 tool performance with application-aware NPBs, which can reduce overhead on packet inspection tools and make a network team smarter about services overall. These NPBs can filter, deduplicate, decapsulate headers, decrypt, splice, and mask packets in order to deliver only relevant data to your tools. They can also load balance packet flows across multiple instances of a tool to facilitate scalability. What follows is a list of some of the many benefits enterprises can experience with application-aware NPBs.

KEY BENEFITS TO TARGET WITH APPLICATION-LEVEL VISIBILITY

Protect Your NetOps and SecOps Tools from Oversubscription

IT operations can set policies with Layer 7 filtering on an NPB so tools only receive relevant traffic. For instance, network operations can identify the most critical services to a business and configure NPBs to forward all traffic associated with these applications to network performance management and application performance management tools for improved service assurance. EMA research recently confirmed the importance of these capabilities. For instance, 38% of enterprises say Layer 7 outbound filtering is one of the most critical features on an NPB, and 37% said intelligent deduplication is critical.[1]

This Layer 7 filtering is also essential to security. The security team can set policies that flag certain types of traffic that require further inspection or less inspection. If the enterprise knows that it's impossible for a certain form of traffic to contain sensitive data, such as a Spotify session, that traffic doesn't need to be forwarded to a data loss prevention (DLP) tool. However, if an application-aware NPB detects traffic associated with DropBox, security operations will definitely want that traffic to go to the DLP system. EMA's research recently found that 38% of enterprises consider outbound Layer 7 filtering to be critical to security monitoring.[2]

Overall, an NPB with application awareness can extend the life of existing tool investments by lowering packet processing requirements, which in turn will speed up a tool's ability to detect problems.

Understand Digital Transformation

New digital enterprises are building highly distributed services that rely on a variety of software packages and technologies, including Internet of Things devices, location-based analytics, frontend applications in the public cloud, and backend ERP systems that tie it all together. Application-aware NPBs can tag traffic associated with each of these components as part of a new digital service. Then, it can forward all tagged traffic to a performance management tool, which will have the service-level context for its analysis.

IT operations can even build a service dashboard in the NPB or the performance management tools that reveals how all these components fit together and perform as a new service, with the option of diving into each service component for more insight.

Interrogate the Unknown

The universe of enterprise applications is constantly growing, and solutions can have a signature for everyone. That being said, application-aware NPBs can help here, too. IT operations teams can configure NPBs to flag services that they don't recognize for deeper scrutiny, if additional context suggests that it is necessary.

For example, IT operations might see an unknown software package, but the source, destination, behavior, and associated URLs all might suggest that the traffic is harmless, as long as it isn't consuming too much bandwidth. However, if there is something suspicious about the traffic, an enterprise can have policies in place to isolate the traffic and forward it for full packet capture and forensic analysis. Forty-seven percent of enterprises that have application-aware NPBs do this today.[3]

1 EMA, "Next-Generation Network Packet Brokers; Defining the Future of Network Visibility Fabrics," August 2018.
2 Ibid.
3 Ibid.

Protect Critical Applications from Bandwidth Hogs

Enterprises know which applications are important and which are frivolous, and they can use application-aware NPBs to build policies that protect their performance. This visibility can provide real-time and trend analysis opportunities for understanding how bandwidth-intensive, noncritical traffic affects the performance of strategic services.

With application-aware analysis, network operations can identify patterns that are hard to see otherwise. For instance, with the right insight, the network engineering team can adjust network use policies and quality of service settings to restrict Facetime chats and Instagram use to certain times of day, or block them altogether. Furthermore, the network team can identify ideal windows for moving massive amounts of data, such as storage backups or big data analysis.

Manage True User Experience

Application-aware NPBs can generate metadata that allows service assurance tools to analyze the end-user experience. For example, an NPB can tag packets associated with a WebEx session with metadata about when a user logged on and off the web meeting, the length of the meeting, frames per second from start to finish, and how it changes. It could also tag different components of the meeting, such as voice quality.

Service assurance tools can correlate traffic data with this metadata to understand better how network conditions impacted user experience. In fact, 38% of enterprises say metadata generation is a critical NPB feature for network operations.[4]

Identify Rogue Traffic and Shadow IT

Finally, application-aware NPBs can provide insight into unauthorized applications or services adopted by the business without the IT organization's involvement. For instance, a business might allow some employees to use certain services on Facebook for business purposes, such as messaging newsfeeds, while others would be banned, such as gaming or video chat. An NPB can filter for these banned or partially banned services and send them to appropriate tools.

These NPBs can also help detect shadow IT, such as a sales team's rogue decision to use DropBox to share purchase agreements with customers. Network operations can identify DropBox traffic in this context and send it to a DLP tool, and then the GRC group will be able to send a strongly-worded memo to the head of sales.

Not every NPB product offers application awareness, so enterprises should inquire about it during product evaluation. Gigamon, a leading NPB vendor, has a well-established track record in this area.

ABOUT GIGAMON

Gigamon is the recognized leader in network visibility and control solutions, providing the application intelligence required to optimize the security and performance of your digital enterprise. With Gigamon solutions, which deliver rich network data while ensuring complete visibility across physical, virtual, and cloud networks, our customers are empowered to solve the complex business challenges of digital transformation. Since 2004, our 800+ employees have earned 66 technology patents and cultivated a global customer base that now includes more than 80% of the Fortune 100, and 10 out of the top 10 government agencies. For the full story on how our network visibility and security solutions can help evolve your digital enterprise, visit our website, follow our blog, and connect with us on your favorite social media channels — Twitter, LinkedIn, and Facebook.

4 Ibid.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3821.040319