RESEARCH
Influence and insight
through social media

July 2018

How to Strengthen Security While Optimizing

NETWORK PERFORMANCE

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: UNDERSTANDING THE ROLE OF THE NETWORK PACKET BROKER

In the digital era, companies will compete based on their ability to see trends in the market and transform faster than the competition. Therefore, they need a highly agile IT foundation to move with speed. Every business is now dependent on its infrastructure technology to make the pivot to becoming a digital company.

However, legacy infrastructure was never designed with business agility in mind. To adapt, businesses have brought in several new technologies, such as the Internet of Things (IoT), virtualization, mobility and cloud computing. And while these technologies have enabled businesses to become more dynamic and distributed, they have made the environment increasingly more complex as more endpoints get connected (Exhibit 1).

This poses some significant challenges for managing the user experience and securing the environment. Managing IT infrastructure and inferring the user experience have historically been done through the monitoring of various IT elements such as servers and storage. However, this is no longer ideal, as businesses have shifted resources to the cloud. To truly understand how IT is performing and to maximize security, it's critical to shift the management strategy to the network—as the network is the one pervasive resource that reaches everywhere.

The network generates massive amounts of data. With the right tools and processes, the following questions can be answered to help improve manageability and security:

- Who is on the network?
- What resources are they accessing?
- Where are they connecting to the network from?
- When did these activities take place?

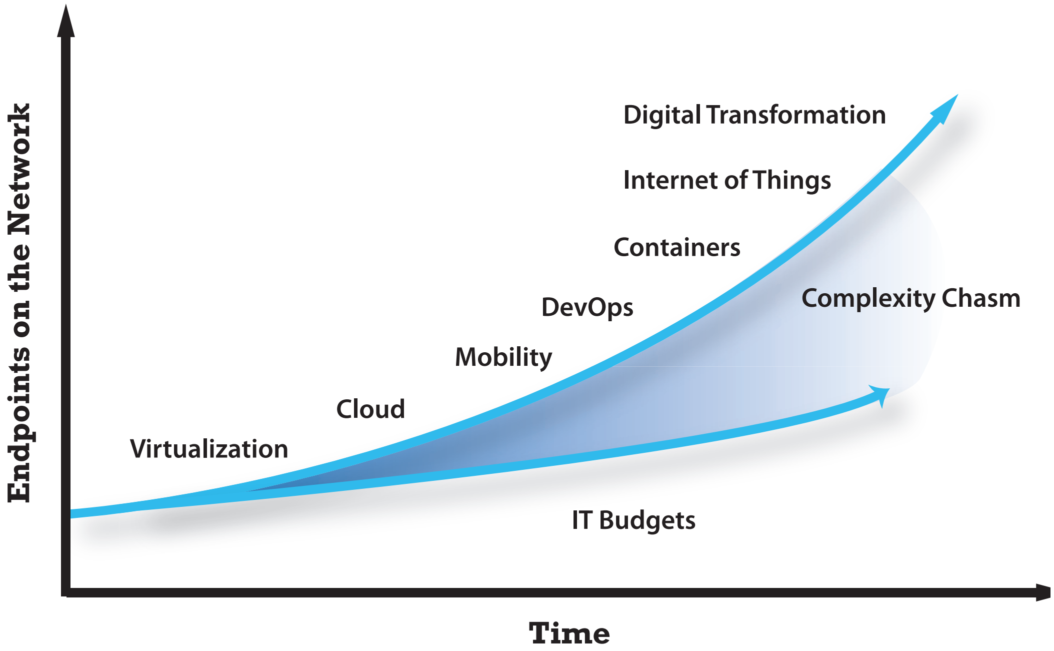
The challenge is that finding the answer to each of these questions—or even a partial answer—requires a separate tool for security, network performance, forensics and other functions. Organizations that set forth to gain the required data and insights have deployed a wide range of discrete tools that each provided a partial picture. These tools were limited in value to the type of information and traffic fed into the system. If the traffic was limited to a specific LAN segment or branch, the tool's visibility was limited to that part of the network, so IT professionals had to try to manually correlate the information.

This type of approach was fine in a static environment, as network managers could connect the tool in the area where value would be maximized. However, in today's networked computing environment where resources are always on the move, the best location for the tool can change almost minute by minute. With IT now shifting to the cloud and outside the physical confines of the corporate walls, the problem becomes exacerbated. Understanding the who, what, where, when problem becomes almost an impossible task, as the combination of tools and infrastructure creates

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

Exhibit 1: The Dynamic Nature of IT Increases Complexity



ZK Research, 2018

a complex, chaotic system (Exhibit 2). Every tool must be plugged into each infrastructure component to have a complete view of the environment.

Moving forward, the problem will only get worse because the number of specialty tools has risen. Businesses must find a better way to distribute information from the infrastructure to the tools before “tool sprawl” overwhelms the IT organization. A network packet broker (NPB) is ideally suited to meet this challenge.

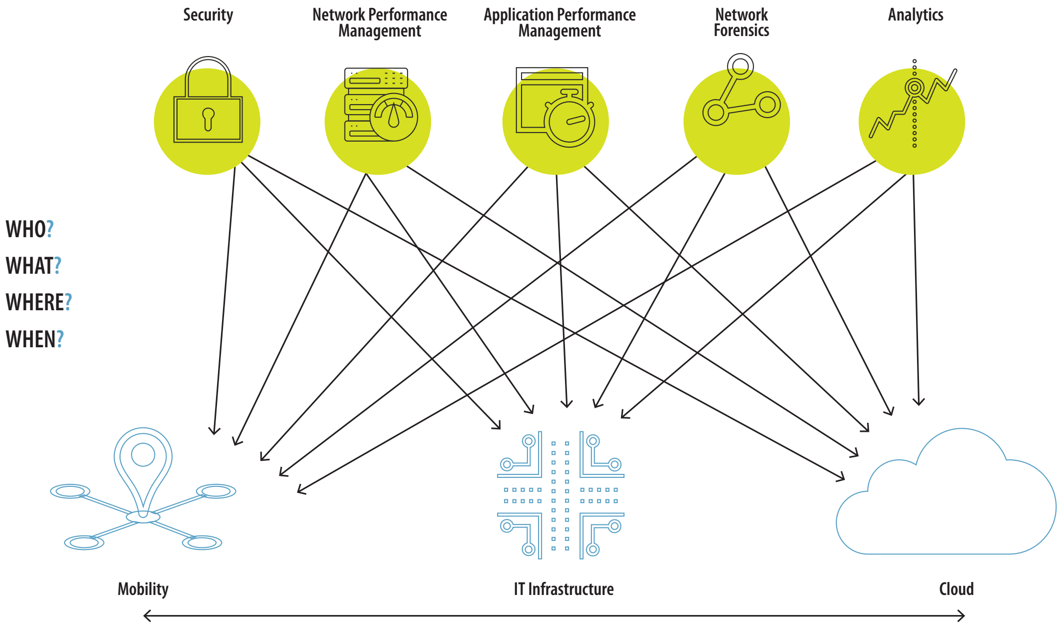
SECTION II: THE EVOLUTION OF THE NETWORK PACKET BROKER

Network packet brokers sit between the tools and infrastructure layers. Each infrastructure component is plugged into the NPB once, as are the tools. This is significantly simpler than having every tool plugged into each IT device (Exhibit 3).

Over time, NPBs have evolved in both their capabilities and their strategic value. The following are the different evolutionary phases for NPBs:

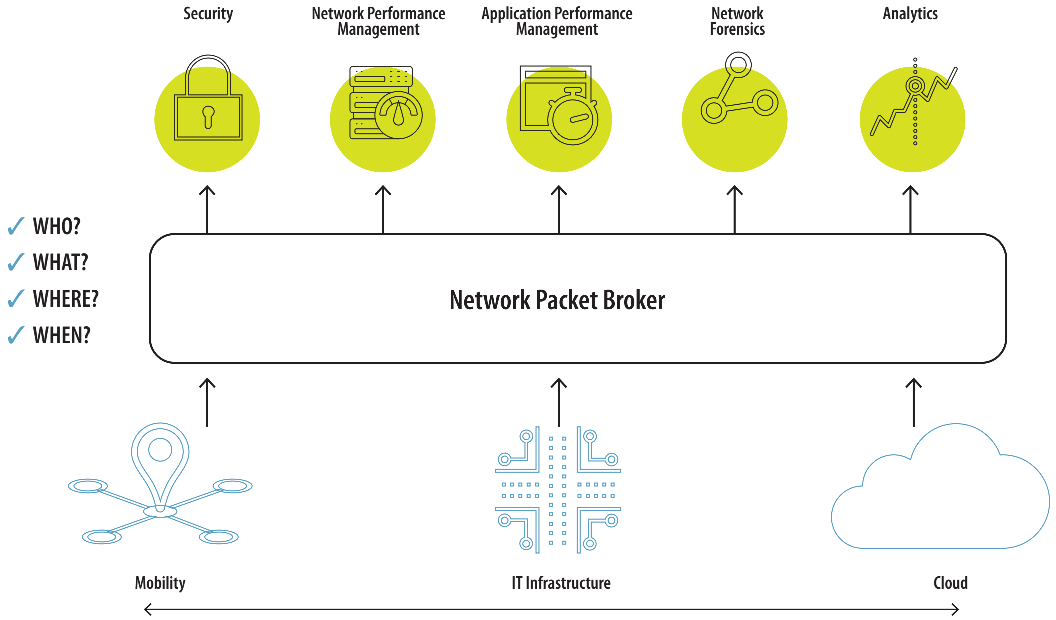
Terminal access point (TAP) aggregation: This is the most basic function for an NPB. Initially, NPBs were designed to receive information from network and other devices, sort the data and pass it along to each tool plugged into the NPB. The value of the NPB was to ensure that each tool received all the data from all the tools to avoid potential blind spots.

Exhibit 2: Tool Sprawl Increases Management and Security Challenges



ZK Research, 2018

Exhibit 3: Network Packet Broker Simplifies Management and Security



ZK Research, 2018

Next-generation packet brokers are designed to meet the needs of businesses that are becoming increasingly digitized.

Intelligent TAP aggregation: In this phase, NPBs became smarter and would apply some filtering capabilities to the data before sending it to the tools. Features like de-duplication, intelligent filtering and packet splicing were brought to NPBs. Also, an NPB had the intelligence to understand what data was coming in and what tool it was sending the information to. For example, email security tools only need to receive email. Without an intelligent NPB, all data would be sent to it, and it would need to filter the data and drop what it does not need. The value of intelligent TAP aggregation is that each tool only receives what data it needs to perform its function, which greatly reduces the amount of processing the tools have to do.

Security packet broker: As cybersecurity threats have evolved, so has the number of security tools. As this happened, NPBs developed security-specific capabilities to optimize the effectiveness of the security tools. One example is the pre-filtering capabilities brought into intelligent TAP aggregation. Another capability of security packet brokers is the ability to operate out of band so the security tools can perform their task at line rate but not impact the performance of applications.

Today's network packet brokers play a key role in enabling businesses to perform several functions such as moving to a virtual network, upgrading the network and cost effectively adding new tools (Exhibit 4). However, infrastructure evolution continues to march on, and now it's time for the network packet broker to evolve once again.

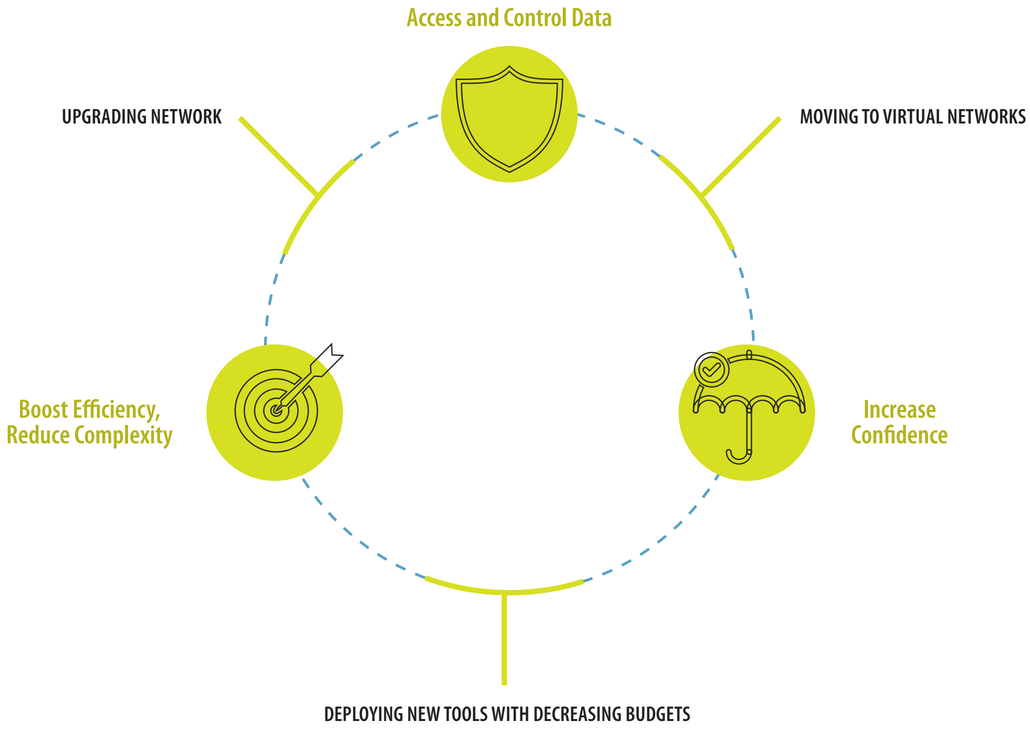
SECTION III: INTRODUCING NEXT-GENERATION PACKET BROKERS

As their name suggests, next-generation packet brokers (NG-NPBs) are designed to meet the needs of businesses that are becoming increasingly digitized. A good analogy to consider is the evolution of application delivery controllers (ADCs). Those devices started as simple load balancers and then added advanced load balancing capabilities to become ADCs. After several years, security and cloud capabilities were introduced, and the product category shifted to advanced ADCs. The same trend is happening with NPBs.

Many basic NPBs are available today, and their capabilities include the following:

- Data aggregation
- De-duplication
- Intelligent filtering
- Packet slicing
- Decapsulation
- Masking
- Intelligent redistribution

Exhibit 4: Today's Network Packet Broker Value Proposition


Access and Control Data
UPGRADING NETWORK
MOVING TO VIRTUAL NETWORKS
Boost Efficiency, Reduce Complexity
Increase Confidence
DEPLOYING NEW TOOLS WITH DECREASING BUDGETS

ZK Research, 2018

The capabilities of NPBs made it significantly easier to deploy and upgrade tools, manage the end-to-end environment, understand user behavior and help businesses protect themselves. Their dynamic and distributed nature has introduced a new set of requirements, including the following:

- Metadata engine
- SSL decryption
- Application session filtering
- Inline bypass

Additionally, the form factor of NPBs needs to change. A traditional NPB is a hardware-centric appliance that still has tremendous value when guaranteed performance is a requirement. However, this form factor must now be augmented by others that bring the functionality to cloud and virtual environments. This augmentation will enable organizations to extend the NPB layer to public, private and hybrid cloud environments, giving businesses true end-to-end visibility.

Also, as the number of NPBs expands, the ability to manage them individually becomes increasingly more difficult. Centralizing management capabilities will give IT professionals the ability to make a single change and then propagate it across every NG-NPB at once. Lastly, automation and orchestration capabilities would allow changes to be made to the NG-NPB when a business policy dictates without having to involve IT operations. Over time, automation, orchestration and a closed-loop data exchange will give rise to the vision of intent-based operations for NG-NPBs, where business policies will dictate configuration changes. Exhibit 5 shows the evolution of NPBs to NG-NPBs.

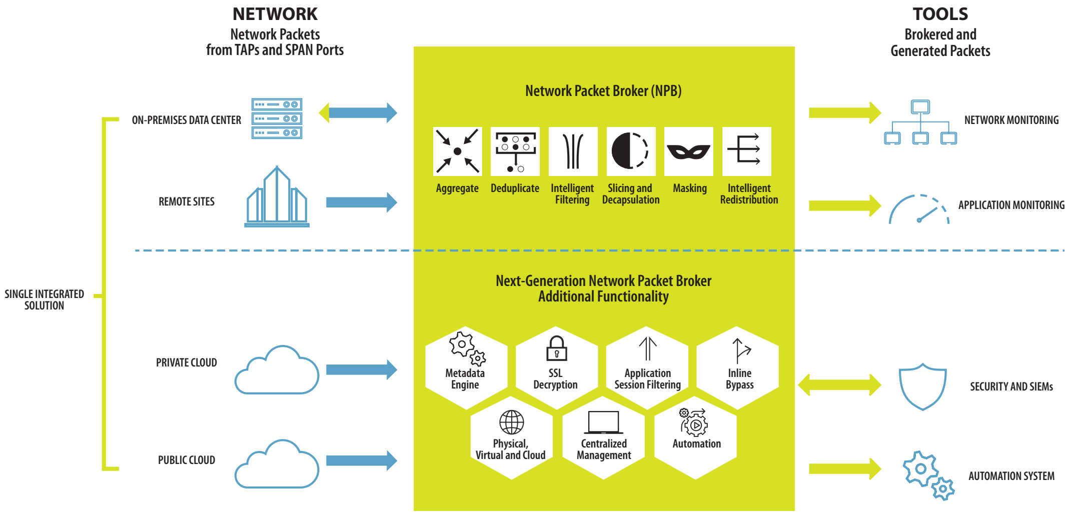
These advanced capabilities are required in digital organizations, as business success is determined by speed and agility. If an organization wants to capitalize on a market transition, the limited feature set and manual nature of operations in traditional NPBs will hold the business back. NG-NPBs modernize the packet broker and align it with current trends.

NG-NPBs play an important role in better aligning the network and security teams. Historically, these groups have operated in independent silos. As businesses have become more dependent on their network, it's critical that security and network operations work in lockstep with one another to ensure the business is protected but productivity is not impaired. Aligning the security and networking teams has been difficult, if not impossible, as they were operating with different data sets. NG-NPBs create a single view of the infrastructure and data to be the bridge that can bring network and security teams into alignment.

SECTION IV: CONCLUSION AND RECOMMENDATIONS

The rise of digital transformation is the most significant change in business to date. Digital initiatives are being fueled by several IT trends such as mobility, cloud computing and virtualization. Companies can now accomplish so much more than they ever have before and are moving ever

Exhibit 5: NG-NPBs Are Critical to Success in the Digital Era



ZK Research, 2018

closer to the ultimate goal of becoming an agile business capable of turning on a dime to capture market opportunities faster than their competition.

However, all of the new technology that has been ushered into organizations has come at a price. The complexity chasm that IT is facing is growing wider at an accelerated pace. As the IT complexity chasm widens, IT pros will deploy more tools to help add visibility and security to the network. As this happens, next-generation packet brokers become a strategic digital enabler because they can increase visibility, improve security and enable companies to maximize the value from their tools investment. An NG-NPB deployment must be at the top of every IT leader's priority list. With this understanding, ZK Research makes the following recommendations:

Shift your IT management strategy away from discrete tools and deploy NG-NPBs. More tools don't necessarily make management or security easier. In fact, tool sprawl can add to complexity and have the reverse effect. NG-NPBs should be deployed in advance of any more tools to ensure companies are maximizing their investments.

Automate as much as possible. Manual operations continue to plague IT. This has never been ideal but did not impair business operations a decade ago, as companies could afford long change-management cycles. Today, IT must work at an accelerated pace, and automation is mandatory to keep up.

Choose your NPB vendor based on NG-NPB features. When making an NPB decision, it may be easiest to choose a low-cost vendor, thinking the NG capabilities aren't necessary. But even if those features are not necessary at this moment, they will be in the very near future as the organization becomes more connected and extended to the cloud. After evaluating several leading NPB vendors, ZK Research believes Gigamon most closely meets the definition of NG-NPBs.

CONTACT

zeus@zkresearch.com
Cell: 301-775-7447
Office: 978-252-5314