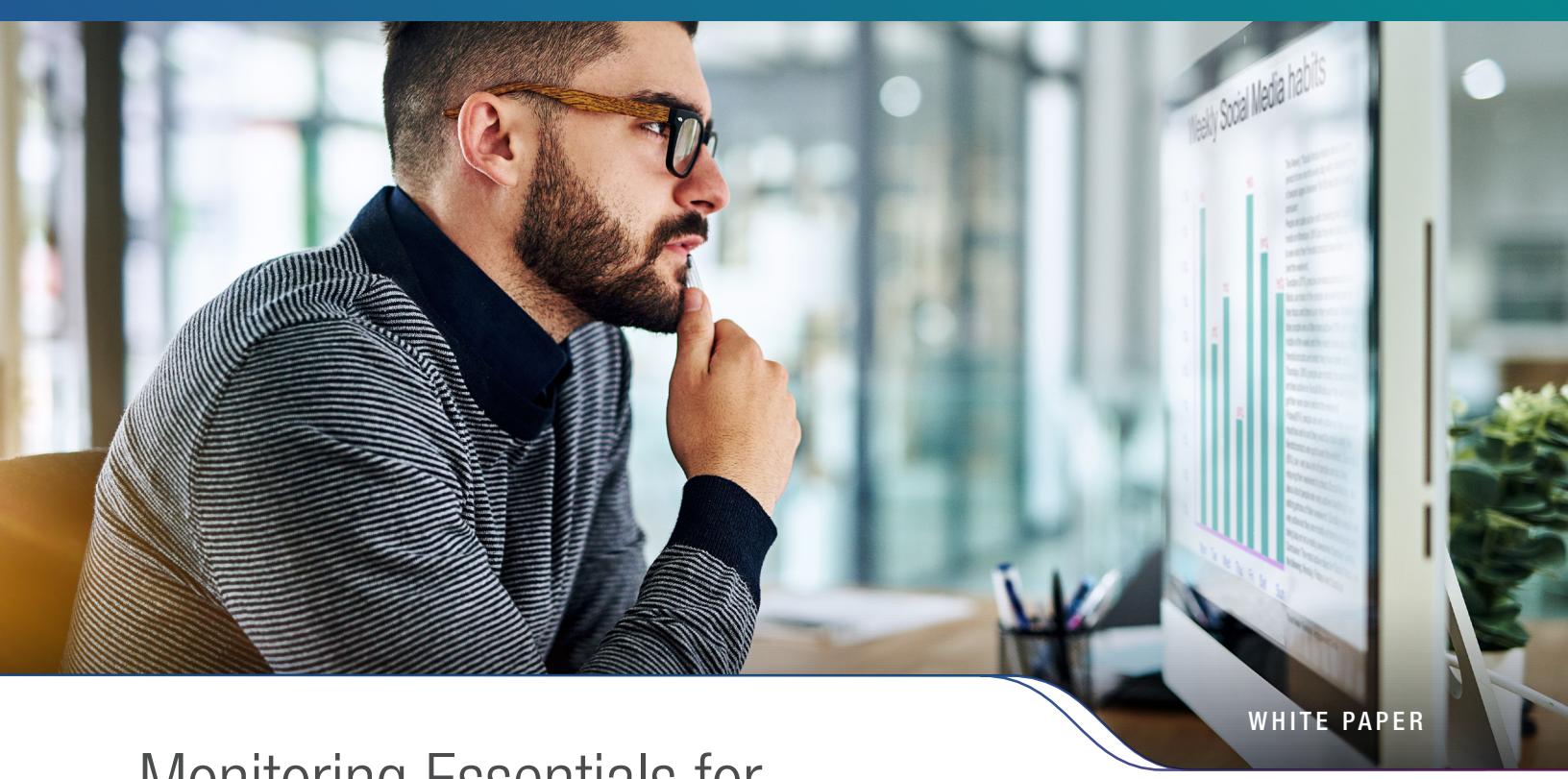

WHITE PAPER

Monitoring Essentials for Hybrid IT Networks

Introduction

The increasing use of virtualized infrastructure, cloud platforms, and agile software development has transformed IT into a strategic asset in the 21st century. At the same time, traffic volume is exploding, cyberattacks continue unabated, and internal stakeholders demand maximum availability and responsiveness. IT teams deploy a variety of solutions to monitor networks and applications to get ahead of these critical challenges.

This paper presents key practices for effective monitoring in today's hybrid IT environments, including how to:

- Enable monitoring in a distributed environment
- Ensure complete visibility to the hybrid IT infrastructure
- Give monitoring tools the right data to process
- Increase the efficiency of monitoring tools to control costs
- Improve productivity of operations staff

Because the number of direct connect access points is limited, you can use a network packet broker (NPB) to connect more tools to your network.

KEYSIGHT TECHNOLOGIES

Enable Monitoring in a Distributed Environment

Network and security teams use a growing number of special-purpose monitoring tools such as application performance monitors, network performance monitors, intrusion detection or prevention systems, forensics, voice over internet protocol (VoIP) monitors, data recorders, and traditional network analyzers. A recent study of network management practices found that one-third of network managers use 11 or more active tools.[1] These tools analyze traffic packets to provide insight into the performance and potential vulnerabilities of a network.

An NPB lets you connect all the monitoring tools you need to maintain the highest levels of security and performance monitoring.

Traditionally, monitoring tools were physically connected to the network. That approach works well until the number of tools exceeds the number of available network access points. At some point, direct connections are insufficient to support all the monitoring tools necessary.

If you solve the problem by leaving some network segments unmonitored, you expose your organization to unnecessary risk. Partial monitoring can result in a security threat remaining hidden in the network or an unresolved performance problem affecting application availability.

The NPB simplifies monitoring by receiving traffic from any number of network segments and sending a consolidated stream of traffic to any number of monitoring tools. Without an NPB, you can end up with a significant number of expensive tools and results in unused tool capacity on some segments. An NPB makes monitoring your system more effective and cost-efficient as the number of network segments and monitoring tools grows. Figure 1 shows how an NPB fits into a typical network.

[1] Enterprise Management Associates: "Network Management Megatrends 2018," April 2018, available to subscribers.

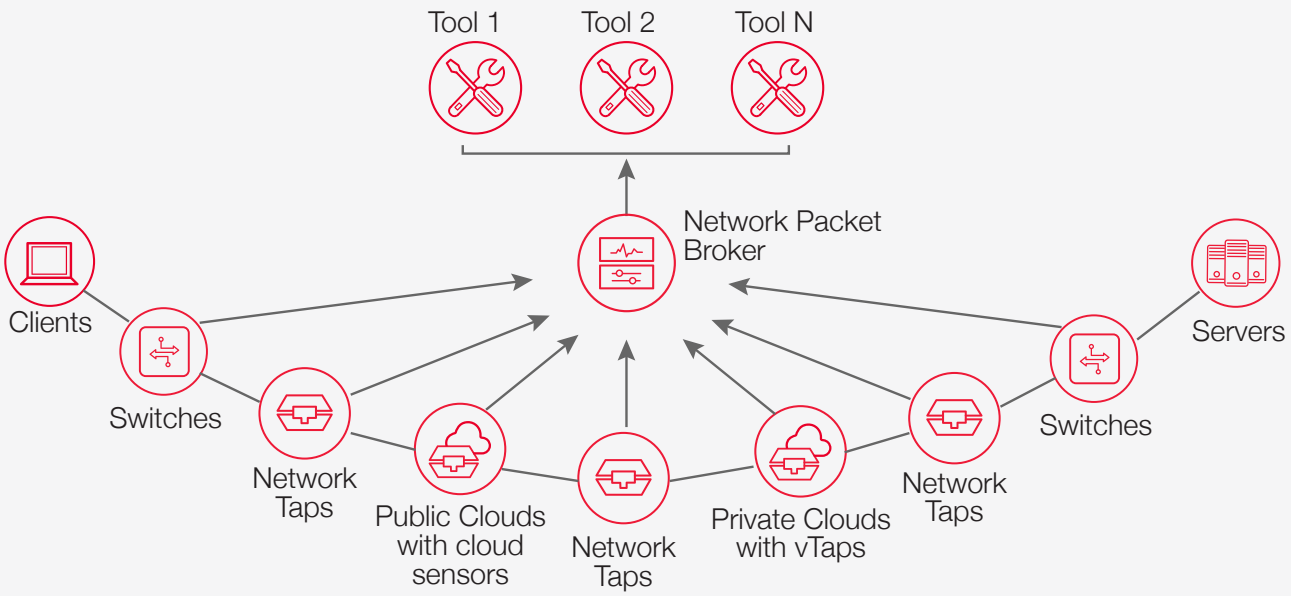

Figure 1. Network taps and sensors feed packet data to a packet broker.

Ensure Complete Visibility to Hybrid IT Infrastructure

In addition to being more distributed, enterprise networks today are also increasingly virtualized. Network managers need innovative solutions to access traffic packets that are essential for security and performance monitoring.

In virtual environments and private clouds, traffic moving between virtual resources (referred to as east-west traffic) does not pass a through a physical switch. It is invisible to traditional network taps and switched port analyzer (SPAN) ports. These areas are blind spots to your network monitoring solutions unless you use dedicated technology to access those packets and provide them to your monitoring tools. Virtual taps give you full access to network packets passing between virtual machines (VMs) running on major hypervisor platforms — even as VMs migrate to new physical locations. This approach is critical for the management of service level agreements (SLAs) and to satisfy compliance requirements.

In public cloud environments, eliminating blind spots is more complex. These workloads are highly dynamic, and IT managers do not have access to either the physical infrastructure or the hypervisor layer. To access network packets in public cloud environments, you need cloud-specific access technology. One approach embeds a container-based packet sensor into each cloud instance you spin-up. The sensor gives you copies of all the packets that move through that cloud and ensures no packets

are missing. With this type of solution, you achieve complete visibility to your clouds, without having to invest in any additional infrastructure.

Give Monitoring Tools the Right Traffic to Process

An NPB eliminates constraints on the ability to connect monitoring tools to help you maintain the highest levels of security and performance monitoring.

Once you eliminate the blind spots and establish 100% total visibility to your network, you must determine how to provide each of your security and performance monitoring tools with the relevant traffic to process. Frequently there are not enough tap and SPAN ports to directly connect all the tools used by the typical IT team.

Also, architects design modern network architectures with multiple paths through the network to increase network reliability. Redundant paths ensure data reaches its destination when one or more links fail. However, this may also mean that packets from a single session may not follow the same path. Because many monitoring tools require all the data from a communication session to perform an accurate analysis, missing data can lead to inaccurate reporting.

Role of the NPB

Aggregating network traffic from physical, virtual, and cloud-based sources and keeping session packets together is the role of the NPB. An NPB makes traffic monitoring more efficient in a distributed hybrid environment. Also, an NPB allows you to deploy as many monitoring tools as you want. With blind spots eliminated, your security tools can identify threats in any corner of your network. With visibility to virtual and cloud resources, your performance monitoring tools have an easier time to resolve issues.

An NPB is easily configured and managed through a graphical, drag-and-drop interface. As a result, IT teams can quickly setup traffic collection in a hybrid environment, filter traffic packets as needed, and deliver condensed data simultaneously to numerous monitoring tools. Also, with an NPB, you can send copies of network traffic to multiple monitoring tools for different types of analysis.

Decryption is another valuable NPB feature. Research indicates three-quarters of internet traffic is now encrypted, and the percentage continues to grow.[2] It is important to decrypt and inspect secure packets since hackers often use encryption to hide their attacks and avoid detection. Unfortunately, advanced security tools cannot understand encrypted traffic and require plain text. Some tools have onboard decryption capabilities, but decoding is compute intensive and can use a lot of the capacity of expensive security tools. It is also inefficient for more than one tool to perform decryption. It makes more economic sense to decode encrypted packets centrally at the NPB first, and then send the resulting plain text to all security tools.

[2] Fortinet "Quarterly Threat Landscape Report: Q3 2018," accessed online.

This process enables security tools to save processing cycles and to work more efficiently.

Another advantage of an NPB is the ability to use traffic monitoring tools that operate at a speed different from the core network. Upgrading a network is expensive and becomes even more costly if you must upgrade direct connect monitoring tools at the same time. An NPB deployed between the network and the tools can "downshift" the speed of the data to match each tool. This gives engineers an opportunity to separate the decision of when to upgrade the network from when to upgrade the tools. An NPB gives network engineers the ability to monitor a higher-speed network backbone with existing, lower-speed tools, protecting their original investment in monitoring tools.

It is more efficient to decrypt secure packets centrally at the NPB first, and then send the resulting plain text to all security tools at the same time.

Deploying an NPB between data sources and data monitoring solutions not only resolves the speed difference but can also remove unnecessary packets from the data stream to deliver only the necessary data for analysis by each monitoring tool. As a result, the monitoring tool does not have to waste CPU and memory resources wading through irrelevant data. Reducing the workload allows the tool to operate more efficiently, reduces the risk of traffic congestion, and helps extend the useful life of monitoring tools.

Increase Efficiency of Monitoring Tools to Control Costs

IT organizations make substantial investments in their monitoring solutions. As a result, it is essential that they get the most out of their monitoring tools and take full advantage of their core capabilities. Advanced NPBs provide several features that offload compute-intensive processing tasks from monitoring tools to free up capacity. These features include packet filtering, load balancing, packet de-duplication, packet trimming, and multiprotocol label switching (MPLS) stripping.

Filtering

Using a monitoring tool to sort through all the aggregated packets is a wasteful use of an expensive resource. Instead, if you use a less-costly NPB to filter the packets, the capacity of your tools is devoted entirely to the monitoring it was purchased to do. Using an NPB results in more cost-efficient monitoring.

High-performance NPBs use application intelligence to develop context awareness about individual data packets. With context awareness, the NPB can sort traffic by application type, operating platform, user device type, geographic location of users, and other characteristics. A visibility platform with application intelligence also shows you what applications are present on your network — to help you uncover unknown or suspicious activity. A dashboard displays statistics so you can see what applications

generate traffic, the amount of traffic, and the number of sessions that contribute to the traffic volume. Information like this is incredibly useful to isolate and resolve security or performance issues.

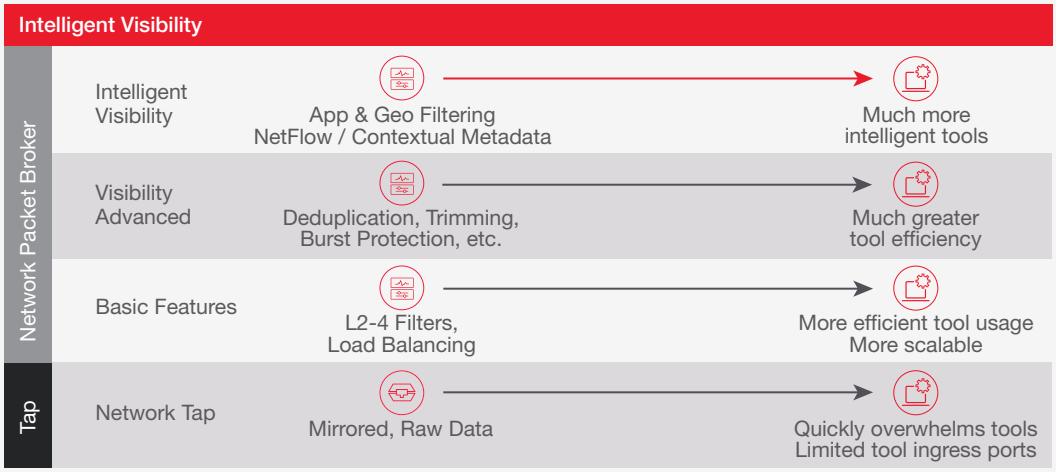

Figure 2. Basic illustration of the benefit of data filtration.

What makes context awareness even more useful is that an NPB can also tailor its behavior and forward traffic to specific tools based on context. Whether you want to continually monitor a particular type of application, or analyze application traffic that exhibits anomalies, your NPB can automatically and quickly send targeted traffic to a specific monitoring tool.

Problem discovery, forensics, and remediation may also require correlation of analysis from multiple tools that perform distinct functions. Using an NPB to enhance traffic with context helps to monitor tools work more efficiently and produce more accurate results.

Load balancing

When the amount of data increases in an enterprise network, IT teams often find the flow of network data increases faster than the capabilities of their monitoring tools. A single monitoring tool that previously performed well can quickly run out of capacity. Through load balancing, NPBs can allocate data across similar tools and send all the data from a single session to one tool. The load balancing feature ensures the tools have the data they need for accurate analysis and spreads the total workload across all the available monitoring tools.

Packet de-duplication

The most important way to keep monitoring tools working efficiently is to avoid traffic congestion, which can cause tools to drop packets and reduce monitoring accuracy. A typical network consists of redundant network paths that improve network reliability and response time. A side effect of redundancy is that network taps end up collecting many duplicate packets. An NPB can remove duplicate packets and reduce overall traffic volume to avoid tool congestion. While some monitoring tools can remove duplicate packets themselves, performing this function multiple times, at each tool, is an inefficient use of tool capacity. An NPB that performs de-duplication up-front is a more efficient solution and reduces the workload of a monitoring tool by up to fifty percent.

NPBs can remove sensitive payload or unnecessary header information before sending packets to your monitoring tools.

Packet trimming

You can also use an NPB to remove payload data from packets and send only metadata and header information to monitoring tools. Many monitoring tools do not need payload information to work effectively. You may also want to remove a sensitive payload for compliance purposes. Combining packet de-duplication with packet trimming reduces the workload for your monitoring tools so you can avoid tool upgrades as traffic volume increases.

MPLS stripping

Removing MPLS labels is another practice that increases the efficiency of monitoring tools. Most standard monitoring tools are not capable of understanding MPLS-tagged packets and therefore are unable to monitor MPLS network segments. An NPB removes the MPLS headers so you can forward the original packets to your tools and expand monitoring of your environment.

Improve Productivity of Operations Staff

With IT departments strapped for time and resources, improvements in staff productivity can make a significant difference. Managing the monitoring solution configurations, connections, and filter definitions is a complex task. A management interface that uses drag-and-drop icons to setup data transfer is faster to use, less prone to error, and easy for new employees to learn without formal training.

Filter libraries

Another time-saving feature of an NPB is the import and export of configuration information with granular control over what gets saved or loaded. Archived libraries of filter definitions allow IT teams to standardize filter definitions and share the configurations among the teams. This practice not only eliminates the manual effort of setting up new segments but reduces errors. A high-performance NPB keeps track of

all the filters you create for your monitoring tools and dynamically manages overlaps as your network expands and evolves. Filter management saves your staff from another time-intensive maintenance task.

Automation

Another type of automation is available with NPBs that include RESTful APIs — interfaces based on representational state transfer (REST) technology. Your staff can program an NPB with RESTful APIs to work cooperatively and automatically with other monitoring solutions to create more powerful monitoring systems.

For example, imagine an intrusion detection system (IDS) that flags an intrusion as it occurs. Using RESTful API integration, the IDS can alert the NPB to initiate traffic recording and capture the intrusion and subsequent events for later analysis. Similarly, network management systems can react to changes in the network and change filters or add/change/drop connections inside the NPB.

High-performance NPBs can dynamically and automatically update your configuration filters whenever you introduce a new segment to your network.

Summary

Incorporating these five key practices will enable more effective monitoring of your hybrid IT environment. A network visibility platform will give you access to traffic from all your physical, virtual, and cloud resources. A high-performance packet broker will let you decrypt secure traffic to enable deep packet inspection and filter traffic based on application-layer details. A visibility platform solves the problem of access point shortages and makes monitoring faster and more cost-efficient. Moreover, these key practices have the ability to improve overall return on your network monitoring investments.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES