WHITE PAPER

Get More From Your Performance Monitoring Tools

Strategies To Address Top Five Challenges

Learn how to increase the efficiency of your monitoring tools. This paper addresses five common situations faced by IT teams across sectors and geographies.

Introduction

Performance is key to the end-user experience, whether your users are customers, partners, or employees. There are hundreds of tools available for monitoring performance in organizations of every size. Your aggregate investment in these tools is not trivial. How can you make sure your tools deliver the highest return on your investment? This paper examines five areas that offer the potential to increase the value of your performance monitoring tools. Consider the following to get the most from your tools:

- **Expanding volume**: Traffic is multiplying, and your tools need to keep up.
- **More secure traffic**: Secure traffic is becoming the norm and your monitoring tools cannot process encrypted packets.
- **Cloud access**: Public cloud is the default in many enterprises. How can you get access to traffic in the cloud?
- **Edge monitoring**: More critical processing is taking place at remote sites. How can IT protect service quality at the network edge?
- **Cost control**: Monitoring tools are expensive. How can you control costs as your enterprise grows?

KEYSIGHT TECHNOLOGIES

1. Boost Efficiency To Handle More Volume

A visibility platform reduces the load on your monitoring tools by grooming and filtering traffic to eliminate unnecessary processing cycles.

Maintaining response time and service availability during periods of high traffic volume is a top priority. Traffic monitoring is key—enabling you to identify potential disruptions and take action before problems escalate. But what happens when the capacity of your monitoring tools is insufficient for the volume of traffic? Adding capacity is expensive. Do you cut back on the number of segments you monitor?

Some organizations do, but rationing the capacity of your monitoring tools creates blind spots in your network where problems can go unnoticed. And cutting back the segments you monitor increases the risk you will suffer a critical incident or outage.

What if you could operate your monitoring tools more efficiently so they process more volume with the same capacity? What if you could reduce the work your monitoring tools have to perform without impacting accuracy or speed? Consider the following proven ways to boost tool efficiency:

Deploy a high-performance visibility platform. A network visibility platform sits between the network and your monitoring tools. It grooms the data before delivering it to tools to increase monitoring efficiency. It functions like a personal assistant, offloading non-core tasks and making things run more smoothly. If you only used one or two monitoring tools you might not appreciate the value of a visibility platform. But research shows that nearly one-third of operations teams use 11 or more tools.[1] That level of complexity is not easy to manage. A visibility platform with fast internal processors can handle lower-level tasks and allow your monitoring tools to focus on what they do best.

Process only relevant data. Different tools process different types of data. Some monitoring tools use packet details while others use NetFlow data. Video data can completely overwhelm your security tools. The intelligent engine of the visibility platform—the network packet broker (NPB)— reduces tool workload by filtering network packets according to what the tools need. You program the NPB using a simple, graphical drag-and-drop interface. The NPB keeps track of the data each tool uses and forwards exactly what is needed and no more. The NPB ensures changes you make for one tool do not negatively impact another. The result is less work for your tools and better use of tool capacity.

Share tool capacity. A visibility platform also provides a way to share the capacity of similar tools deployed at different locations on the network. If one tool is under-utilized and another is oversubscribed, an NPB can collect the traffic from both locations and allocate it equally between both tools. The ability to share capacity helps you get good value from every tool you purchase.

1 EMA Research: "Network Management Megatrends 2018," June 2018, accessed on SlideShare.

Reduce congestion and improve accuracy. Some tools are especially sensitive to congestion. When traffic flow exceeds their available capacity they noticeably slow down processing or begin randomly dropping packets, which affects accuracy. Ideally, your tools should operate at no more than 80 percent of their rated capacity so intermittent data surges or microbursts do not overwhelm tool ports and cause packet loss. This threshold is difficult to maintain. An NPB uses automatic load balancing to sense and relieve overloaded tools by distributing traffic across multiple devices. Some NPBs let you create multiple load balancing groups with unique allocation rules. This gives you the flexibility to move traffic during maintenance or troubleshooting without reducing coverage.

2. Offload Traffic Decryption

Secure Sockets Layer (SSL) encryption standards are widely used by senders and receivers to protect the transmission of sensitive and private communications. Encryption makes it harder for hackers to eavesdrop and intercept information they can use to steal data or disrupt business. But encryption does not stop a motivated thief. Hackers routinely encrypt their requests to bypass security systems and gain access to your network. Once inside, they masquerade as authorized users to avoid detection and move to a location from which they can launch their attack. To defeat hackers, security experts advise companies to monitor secure traffic just as they do other communications.

Your monitoring tools need granular packet data to isolate the root cause of performance problems and identify security threats.

Faster, more efficient decryption. Security and performance monitoring solutions can only process plain text. This means you need to decrypt all secure packets before they can be recognized by your monitoring tools. Some security tools offer onboard decryption as an option to overcome this limitation. The downside of this approach is that decryption is very process-intensive and can quickly use up a tool's available capacity, requiring you to purchase an expensive upgrade. In addition, if you use more than one monitoring tool, you may end up decrypting packets more than one time. This is a waste of valuable processing cycles.

A faster, more efficient approach is to offload decryption from your tools completely and let the NPB in your visibility platform do it. An NPB with SSL decryption can decode (and recode) secure traffic one time and deliver the resulting plain text to multiple monitoring tools. With decryption offloaded you have more tool capacity for deeper analysis.

Active SSL. In March 2018 an updated encryption protocol was approved by the Internet Engineering Task Force (IETF), the consortium that evaluates and publishes network standards. Transport Layer Security (TLS) 1.3 will strengthen security against increasingly savvy hackers. TLS 1.3 requires the use of more advanced encryption algorithms that are harder for hackers to break. The new standards also require every client-server pair to negotiate encryption keys anew for every secure session, rather than reusing existing keys. To enter into a secure communication under TLS 1.3, both sides of the communication must be active participants in the encryption process. It will take some time for TLS 1.3 to be widely adopted. In the meantime, network operators should verify that their network visibility platform is able to support TLS 1.3 decryption and re-encryption.

3. Give Monitoring Tools Access To Cloud Traffic

By 2021, networking experts project that 94 percent of all workloads and compute instances will be processed by infrastructure in cloud-based data centers.[2] This means monitoring your cloud environments is no longer optional, but critical.

Cloud providers may supply summarized network data or policy violations for their clients to use for performance monitoring, but this information is insufficient for detailed analysis. Your monitoring tools need granular packet data to isolate the root cause of performance problems and identify security threats. Therefore, you need a cloud visibility solution that provides access to network packets.

Cloud computing depends on virtualization, in which functions once processed by dedicated hardware are transformed into software tasks that are processed by generic servers. Traditionally, network packets used for monitoring were collected by network taps as the packets moved through a physical switch. That technique does not work in the cloud and accessing packet data can be a challenge. A recent survey sponsored by Ixia, a Keysight business, found that 68 percent of IT professionals found it difficult to access network traffic in their hybrid and public cloud environments.[3]

Access virtual traffic. In virtual environments and private clouds, traffic moving between virtual servers—referred to as east-west traffic—cannot be accessed by traditional network taps. Unless you deploy a cloud visibility solution, east-west traffic is invisible to your tools and represents a giant blind spot in your monitoring.

2 Cisco Global Cloud Index: "Forecast and Methodology, 2016-20121 White Paper," Trend 2: Continued global data center virtualization, 11/19/2018.
3 Ixia: "The State of Cloud Monitoring," results of a survey conducted by Dimensional Research, March 2019.

To see network packets moving in a virtual environment, you need visibility into the virtualization layer or platform. This is the role of virtual network taps. In a private cloud environment, virtual taps also track workloads that migrate from one physical server to another, without causing downtime and without losing monitoring efficiency. This approach is critical for effective monitoring of virtual data centers and private clouds.

Access traffic in public clouds. Establishing network visibility in public clouds is a bit more involved because the infrastructure used by public cloud providers is inaccessible to customers. A public cloud visibility solution uses container-based sensors automatically deployed inside each cloud server to access traffic packets. Sensor-based technology is "cloud-native" and this approach gives you complete visibility to every packet, without the need to purchase additional infrastructure. With a cloud-native solution, your visibility scales right along with your cloud servers.

Filter at the data source. Once you access network traffic from your public cloud servers, you need to decide whether you will monitor that traffic in the cloud or backhaul the traffic to your data center and use monitoring tools deployed there. Some cloud visibility vendors provide a cloud-based version of the visibility engine which filters packets in the cloud and transfers them directly to cloud-based tools. This is faster and sometimes less expensive than backhauling traffic to the data center for monitoring.

4. Monitor At The Network Edge

Enterprises are shifting more of their operations to branch and remote locations to provide users with faster access to critical business applications and data. Researchers at Enterprise Management Associates have observed a steady uptick in the number of remote sites connecting to wide-area networks and the number of devices connecting to the network at those sites.[4] Ideally, the NetOps team should monitor the quality of experience at each of these sites.

Active monitoring lets network operators run simulations with realistic traffic to anticipate and resolve disruptions before they impact end-users.

Packet access at the edge. Unfortunately, many NetOps teams lack the tools to acquire deep visibility at the network edge. Some organizations use flow analysis to get information on network performance and device status at the edge. However, flow data does not provide the deeper insight needed to diagnose complex issues or unravel sophisticated security threats. The most valuable data for understanding user experience at the edge are network packets. An intelligent NPB is the best solution for edge monitoring.

4 Enterprise Management Associates: "Managing Service Quality at the Network Edge," report prepared for Ixia, a Keysight Business, April 2019.

Remote Site Monitoring

A visibility solution uses edge-oriented NPBs to collect packets at remote sites and deliver them securely to monitoring tools in the data center.

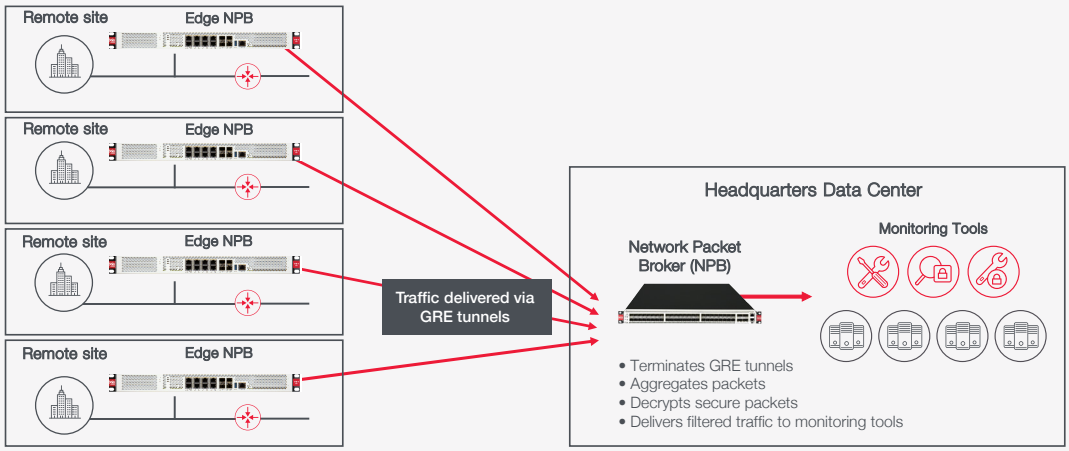

Figure 1. Distributed monitoring architecture.

An NPB will time-stamp and filter packet data and deliver filtered data to all your monitoring tools. Context awareness is the feature that lets an NPB identify useful details like the location of the requestor, the type of device the requestor is using, and the applications the requestor is asking for. With details like this your monitoring tools can zero in more quickly on the root cause of an issue so you can implement a solution that will prevent the issue from recurring.

Teams that operate a network visibility platform in their data center may wonder how they can afford to replicate this powerful solution at all their remote locations. What they need is a solution designed specifically for edge deployment—one that provides packet visibility and filtering but is right-sized for remote sites on the network edge. Recently vendors have introduced products like this to the market and now provide network visibility in an edge-sized package.

Active monitoring. A valuable feature of some edge visibility platforms is the addition of active monitoring (also known as proactive monitoring). This feature lets network operators identify potential performance problems before they impact end-users. The platform runs synthetic traffic that mimics the expected volume and mix of actual traffic through the network in test mode. The active monitoring feature measures key performance indicators, such as response times, error rates, and packet loss, to determine the quality of the user experience. Running the simulations give operators a heads-up on any performance degradation and gives them time to fix it before end-users experience the issue with live traffic.

5. Control The Cost Of Monitoring

Cost avoidance is a good strategy for controlling costs as your enterprise expands. If you can do more with the tools you already have, you can avoid or eliminate new tool purchases and boost the return on your existing investments.

Eliminate duplicate packets. Network paths in the modern organization are complex and not easily distinguishable. To ensure adequate monitoring and eliminate blind spots you install taps on nearly every network segment. In the process, you end up collecting multiple copies of many packets. (Academic researchers have estimated the volume of duplicate packets at 50 percent of total packets.[5]) These duplicate packets essentially double the workload for your monitoring tools and cause tool congestion.

When tools become congested and run out of capacity, they can drop packets and produce inaccurate results. Accurate monitoring is essential for ensuring performance and security, so you need to keep tools working efficiently. For this reason, many teams address packet congestion by adding more tool capacity at a significant cost to the organization.

Another strategy is to use an NPB to eliminate duplicate packets and condense the data you send to your monitoring tools. This one technique can substantially cut the workload for your tools and eliminate the need to add capacity.

Reduce capacity requirements. You can also make better use of your monitoring tools by offloading non-core processing tasks. High-performance NPBs not only deduplicate and decrypt packets, but also strip off unnecessary packet headers, obscure sensitive information with data masks, generate NetFlow for tools that need it, and perform packet filtering. With these “grooming” tasks handled by a less-expensive and centrally-located NPB, you need less capacity in your monitoring tools.

Extend tool life. Tools deployed directly on the network must operate at the same speed as the network. Over time, you may decide to upgrade your network to deliver faster response and a better end-user experience. Network upgrades are expensive, particularly when you must simultaneously replace all your monitoring tools.

A visibility platform can reduce the cost of a network upgrade by letting you extend the useful life of your existing, lower-speed monitoring tools. An NPB sits between the network and your monitoring tools and functions as a modulator. It accepts traffic from your higher-speed network, processes it,

5 Ucar, Morato, Magana, and Izal: “Duplicate detection methodology for IP network traffic analysis,” Department of Automatics and Computer Science, University of Navarre, Spain; Nov 2013.

and delivers groomed and filtered packets to monitoring tools at whatever speed they require. With an NPB you can delay the purchase of higher-speed monitoring tools. Using your existing tools longer helps you boost the overall return on your original investment.

Spend less time on analysis. Another way to reduce the total cost of network monitoring is to reduce the time it takes to identify and resolve a performance issue. Zeus Kerravala, Principal Analyst at ZK Research notes that, "Problem identification is IT's biggest challenge." His research found that 85% of the mean time to repair (MTTR) an issue is the time it takes the operations team to identify what is happening.[6] The longer it takes, the more risk there is that the business will suffer.

A network visibility platform can reduce MTTR by providing deeper insight into the problem. If operators implement a fix without first identifying the root cause of an issue, the fix will likely not hold up and the issue will recur.

An NPB with context-awareness can isolate the information needed for more effective troubleshooting. For example, monitoring tools can use geo-location awareness to quickly pinpoint the location of outages and focus troubleshooting efforts where they make the most sense. The ability to narrow down the scope of the analysis reduces the overall time and effort required to restore performance.

6 ZK Research: "Digitization Drives the Need for Application Strengthening," January 2016.

Conclusion

Monitoring network and application performance is important in a complex, modern network. Make sure you get the most from your monitoring tool investments by offloading non-core tasks, eliminating redundant or unnecessary processing, and keeping tools free from congestion. Give your tools the granular details they need to quickly identify the root cause of disruptions and help you deliver the right fix as fast as possible.

Control rising costs by preserving the processing power of your monitoring tools for sophisticated analysis and detection. Deploy a visibility solution with:

- Powerful packet grooming and filtering
- Centralized SSL decryption (both passive and active)
- Access to packets in all your cloud servers
- Cost-effective edge-sized options
- Active monitoring to anticipate performance disruptions

Learn more about Keysight's performance monitoring solutions at
https://www.keysight.com/us/en/products/network-test/performance-monitoring.html

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