WHITE PAPER

Best Practices for Network Monitoring

Monitoring Challenges In Today's Business Environment

The rapid evolution of business applications and systems is making information technology (IT) a strategic part of the world's most successful companies. The recent shift toward virtualization and cloud computing comes at a time of increasing threats of attack on these strategic assets by malicious entities. At the same time, increasingly-stringent government and industry regulations require stricter data center controls to ensure compliance. IT organizations are working hard to address these challenges while also working to improve the responsiveness and reliability of network and computer systems to help increase their company's competitive edge.

To get out in front of these data center challenges, IT teams use a number of technologies to proactively monitor their network and applications. Application performance monitors, network performance monitors, intrusion detection or prevention systems, VoIP monitors, data recorders, and traditional network analyzers are examples of monitoring tools that give an IT team better insight into the performance and problems in their network. These valuable tools all require access to network data to perform their analysis. Mirror ports (also known as SPAN ports) on network equipment and network taps create data access points that provide network data for tools to analyze. However, because the number of data access points on security and monitoring tools is limited, connecting a large number of monitoring tools to the network is impossible. A relatively new technology, the network packet broker (NPB), was created to solve this problem.

Because the number of data access points on security and monitoring tools is limited, connecting a large number of monitoring tools to the network is impossible. A relatively new technology, the network packet broker (NPB), was created to solve this problem.

KEYSIGHT TECHNOLOGIES

A NPB sits between network SPANs/taps and the monitoring tools. This technology allows network engineers to collect network traffic from SPAN and tap ports and provide monitoring tools with a copy of network data. Figure 1 shows where a NPB fits in a typical network. However, NPBs do far more than replicate data. They solve security, compliance, and visibility issues facing network engineers in today's data center.

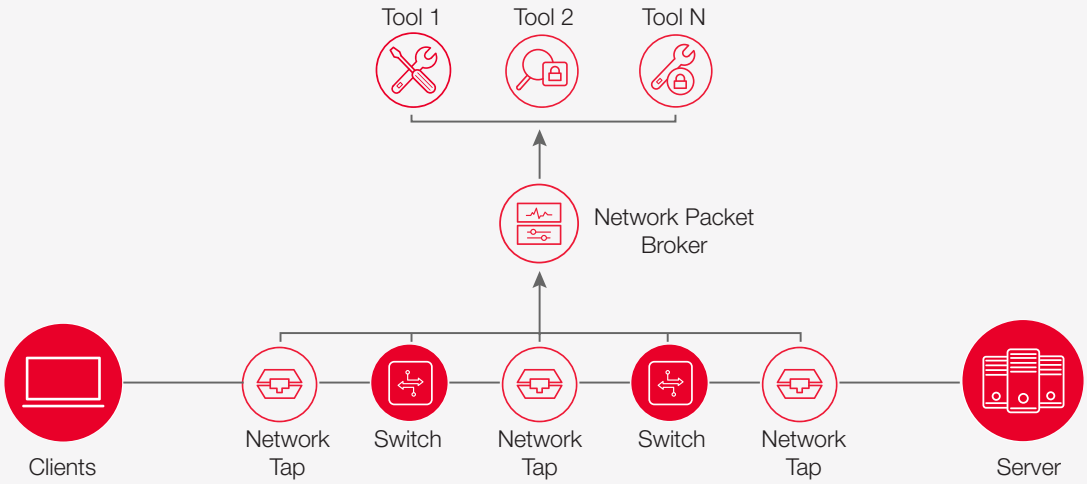

Figure 1. A network monitoring switch sits between network SPANs and taps and the monitoring tools.

Giving Monitoring Tools Full Visibility to the Network

Connecting monitoring tools directly to tap and SPAN ports in a network is the simplest way to get data for analysis, but this approach has several pitfalls. The most immediate problem is that there are just not enough tap and SPAN ports for all of the tools used by the typical IT team. According to research and analysis firm Enterprise Management Associates, Inc., 35% of organizations cited a shortage of SPAN and taps to be the primary reason they are unable to monitor 100% of network segments.

Modern network architectures provide multiple paths through the network, which helps increase network reliability, but also creates another problem for effective monitoring. This redundant network architecture ensures that data can still reach its destination when one or more links fail. However, the redundancy also means that data between two devices in the network may not travel the exact same path through the network and some data may be missed by the monitoring tool.

Because many monitoring tools require all of the data from a session to perform an accurate analysis, it is likely that missing data will lead to inaccurate reporting. Imagine trying to analyze traffic within a city by only counting the number of cars passing through a single street. The amount of traffic on that street is probably not representative of

NPBs do far more than replicate data. They solve security, compliance, and visibility issues facing network engineers in today's data center.

traffic elsewhere and a statistical analysis of the frequency of car models is likely to be distorted. This lack of visibility severely limits the effectiveness of monitoring tools.

The NPB solves this visibility problem. A NPB allows IT teams to quickly and easily connect taps and SPANs to monitoring tools and configure these connections through an easy to use control panel. In this way, monitoring tools can have access to all of the data from multiple network segments and get a complete view of the network traffic. In addition, monitoring tools can each get a copy of the data from one or more network segments, allowing more tools to have access to the same network data.

The NPB “downshifts” the speed of network data to match the speed of the available monitoring tool.

Upgrading a network is expensive, and becomes even more costly when network monitoring tools must be upgraded at the same time. Traditionally, network engineers did not have a choice. When they upgraded their network they also had to upgrade monitoring tools. With the advent of the NPB, network engineers now have a better choice because these new devices also allow lower-speed monitoring tools to receive data from high-speed core network segments. Network engineers now have the ability to monitor higher-speed backbone networks with their lower-speed tools, protecting their original monitoring tool investment.

So how does a monitoring switch work in the upgraded network? The NPB “downshifts” the speed of network data to match the speed of the available monitoring tool. Because of the potential speed mismatch between the network monitoring tool and of the upgraded network, the monitoring tool may be overwhelmed with data resulting in the loss of packets. The NPB provides a way to filter the network data to reduce the amount of data to match what the tool can handle.

This capability not only resolves the speed difference, but also can remove other unnecessary packets from the data stream, providing only the data required for analysis to the monitoring tool. As a result, the monitoring tool does not have to waste CPU and memory resources wading through irrelevant data. This not only extends monitoring tool investment as IT organizations transition to new, higher speed network technologies, it also allows IT teams to get improved performance from the monitoring tools they already own.

Making Monitoring Tools Work Better

IT organizations make large investments in monitoring tools. As a result, it is essential that IT teams get the most out of their monitoring tools by taking full advantage of their core capabilities. To help IT teams realize the full benefit of their monitoring tools, advanced NPBs provide a number of features that off-load compute intensive processing from their tools. Such features include packet filtering, load balancing, packet de-duplication, packet trimming and MPLS stripping.

Filtering

Using a monitoring tool to find the required packets and discard the remaining packets is a wasteful use of an expensive resource. It is also processor intensive. By filtering data in the NPB, the monitoring tool is freed to perform the work that it was purchased to do, resulting in more useful work being done by the monitoring tool.

Filtering is usually performed in three stages. The first stage is performed at the port where the network is attached (network port). The second stage is a highly capable, port-independent filter that is located between the network port and the port to which the monitoring tool is attached (tool port). The third stage of filtering is performed at the tool port. Three-stage filtering is important because filtering at the network port completely eliminates the excluded traffic from being available to ALL tool ports. Once this traffic is removed it is no longer available for analysis.

An alternative to this approach is filtering at the tool port, but this causes two problems. First, the tool port can be overrun by the volume of traffic coming from the network ports. Second, the interaction between the network filters and the tool filter is complex and not obvious unless you are well versed in set theory. The port-independent filter, also called a dynamic filter engine, is the ideal place to perform the bulk of the filtering as it is possible to understand exactly what is happening by looking at this single filter definition. When considering a NPB it is important to understand its filtering capabilities.

Load balancing

When the amount of data increases in an enterprise network, IT teams often find that the network data flow is increasing faster than the capabilities of their monitoring tools. A single monitoring tool that previously performed well is now out of capacity. Through “load balancing” some NPBs have the ability to send data across multiple tools and do it in a way that consistently sends all the data from a particular session to the single monitoring tool. The load balancing feature keeps session data together for better analysis, yet balances the total network load across multiple monitoring tools. This function is used extensively with network data recorders. Since session data is kept together, only one data recorder needs to be accessed to analyze any given session at a later time.

The load balancing feature keeps session data together for better analysis, yet balances the total network load across multiple monitoring tools.

Packet de-duplication

Another form of off-loading is the ability of NPBs to remove duplicate packets from network data streams. Duplicate packets are most commonly caused by the use of SPAN/mirror ports. While some monitoring tools are capable of removing duplicate packets, many tools do not have this capability. However, even if a monitoring tool has the ability to remove duplicate packets, doing so is an extremely resource intensive task. Off-loading duplicate packet removal to the NPB can cut the CPU load of a monitoring tool in half.

Another key benefit of removing duplicate packets is that the bandwidth at the Ethernet port of the tool is conserved, allowing more data to be provided to the monitoring tool. In extreme cases, the improvement in bandwidth efficiency can more than double the amount of "good" packets delivered, greatly improving the performance of the monitoring tool.

Network monitoring switches have the ability to integrate into network security systems, such as TACACS+ and allow administrators to specify which users and groups have access to network data.

Packet trimming

Packet trimming removes payload data from the packet, leaving the header information, prior to sending the packet to monitoring tools. Some monitoring tools do not require packet payload information, in which case, removing payload data allows more data to be sent across the link from the NPB to the monitoring tool. As a result, the monitoring tool can receive a far greater amount of network data. Additionally, for compliance reasons, it may be desirable to "trim" or remove sensitive payload data from packets before they are sent to a monitoring tool.

MPLS stripping

Removing MPLS labels is a form of off-loading that actually increases the capability of monitoring tools. Most monitoring tools are not capable of understanding MPLS-tagged packets, making them unable to monitor MPLS networks. A NPB can remove the MPLS headers and forward the original packet contained within the MPLS tagged packet. Standard network monitoring tools can then be used to monitor activities with the MPLS network.

Keeping Network Data Secure

Security is always a critical concern for IT organizations because they are responsible for ensuring that the wrong data does not end up in the wrong hands. Conversely, they must ensure that the right data gets into the right hands. NPBs have the ability to integrate into network security systems, such as TACACS+ and allow administrators to specify which users and groups have access to network data. Fine-grained access control makes it possible to specify which group or user has access and exactly what they are entitled to do—such as the right to modify port settings, data flow connections, and filter definitions.

Once control of the access to the NPB has been established, best security practices require that any changes are logged to a SYSLOG server. In this way it is possible to know when a change was made and by whom.

Improving productivity in IT

With IT departments strapped for time and resources, improvements in productivity can make a big difference. Because managing the network monitoring configuration, connections and filters definitions can be a complex task, how these configurations are managed with a monitoring tool is key. Managing configurations with a network

monitoring switch is performed in different ways, depending on the brand of monitoring switch chosen.

Some require CLI code exclusively to configure network traffic, some require a combination of GUI interface and CLI code, and some are managed completely through a drag-and-drop interface. Tools managed through a drag-and-drop control panel are easier to deploy than other versions as IT teams do not have to be experts in command language specific to that tool. An intuitive interface also allows IT teams to focus on the task of operating the monitoring tool rather than getting the data to the tool.

Filter libraries

Another time-saving feature of a NPB is the import and export of configuration information with granular control over what gets saved or loaded. Libraries of filter definitions can also be saved, allowing IT teams to create common filter definitions and disseminate these libraries for use among the teams.

Automation

Automation is a productivity enhancement available with some NPBs. Monitoring tools, network management systems and IT automation systems can dynamically control a NPB. Using RESTful, software-based systems can control any aspect of the NPB. IT teams can now create extremely powerful systems using multiple network devices that work cooperatively and automatically.

Imagine an intrusion detection system (IDS) system that detects an intrusion as it occurs. Using the automation capabilities of the NPB, the IDS sends a command that sets up a connection between the network port being monitored by the IDS and a network data recorder, immediately capturing the intrusion event 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.

Summary

IT teams are under ever-increasing pressure to improve the performance and security of corporate networks. To meet these challenges, IT teams rely on monitoring tools.

Monitoring for security, compliance, as well as application and network performance requires access to an increasing amount of network data, optimally-performing monitoring tools and full visibility into the network. Unfortunately, the limited number of data access points prevents effective monitoring. The NPB is a necessary tool in addressing these challenges. Not only does a NPB solve the problems of tap and SPAN shortages, it also optimizes the traffic to all monitoring tools, improving overall monitoring tool performance and protecting the IT team's monitoring tool investment.

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

This information is subject to change without notice. © Keysight Technologies, 2016 - 2020, Published in USA, May 27, 2020, 3120-1092.EN