WHITE PAPER

Outdated Monitoring Processes Increase Costs and Reduce Responsivity

Outdated Processes and Monitoring Tool Overload

The rapid evolution of business applications and systems is making information technology (IT) a strategic part of mission critical operations for government agencies. This increase in dependence upon technology and data mining has caused government agencies to deploy more security and monitoring tools to analyze the requisite types of data. Assuming that government and civilian IT trends are similar, an Enterprise Management Associates (EMA) report (Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Computing) estimates 40% of enterprises are using somewhere between four to ten tools to monitor and troubleshoot their networks. An estimated 27% use eleven or more tools.

Unfortunately, the increased number of security and monitoring tools has made managing the network more difficult, not easier. For instance, one challenge is that all devices need simultaneous access to network data either in real time or near real time. Additionally, these different tools require different subsets of the available network data. An easy (but outdated) “firehose” approach of sending a complete copy of all network data will overload the CPU and memory caches of the tools, further reducing the efficiency of those devices. It also creates an unnecessary security risk for your critical infrastructure.

An Enterprise Management Associates (EMA) report (Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Computing) estimates 40% of enterprises are using somewhere between four to ten tools to monitor and troubleshoot their networks. An estimated 27% use eleven or more tools.

KEYSIGHT TECHNOLOGIES

Fortunately, there are some simple actions that can be implemented to increase efficiency, reduce costs, delay component obsolescence, and maximize uptime of critical infrastructure components:

- Optimize monitoring data connectivity and capture points within your network
- Implement data aggregation to reduce costs and simplify the infrastructure
- Create powerful data filtering that is also intuitive and easy to maintain

"Network visibility as a whole is probably one of the most important aspects of a cyber security shop."

Rob Lewis,
Enterprise Threat Manager for U.S. Department of the Interior

Proper Monitoring Starts with Data Connectivity Optimization

Network visibility is increasing in importance for all government agency monitoring strategies. According to Rob Lewis, Enterprise Threat Manager for the U.S. Department of the Interior, "Network visibility as a whole is probably one of the most important aspects of a cyber security shop."

When it comes to data collection and monitoring, ensuring proper access to network data is the most critical thing you can do. Everything else, data filtering and the conversion of data into actionable information, are all dependent on the initial data being correct and relevant. If this practice is ignored, you can experience "garbage in equals garbage out".

To get ahead 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 require access to different types of network data to perform their analysis.

Proper visibility starts with proper data access; however, this activity also happens to be one of the least thought about activities by IT engineers. When it comes to data monitoring, many IT professionals simply use SPAN (switched port analyzer) ports from their Layer 2 and Layer 3 network routing switches because "it was there" and "it was free". This is now considered an outdated process. Corporate enterprises have already been making the move to newer test access point (tap) technologies to modernize their infrastructure. This is for three very good reasons:

- Taps are simpler to operate than SPAN ports
- SPAN ports do not provide a complete copy of all network data
- Taps can be deployed anywhere in the network

Connecting monitoring equipment to taps is easy—you just connect to an open “data out” port on the tap and you get all the information you need. As for programming, there is none; a tap creates a complete copy of all data. Unlike SPAN ports, there is no command line interface (CLI) or any other type of programming needed. There are no reconfigurations; taps are as simple as “set and forget”.

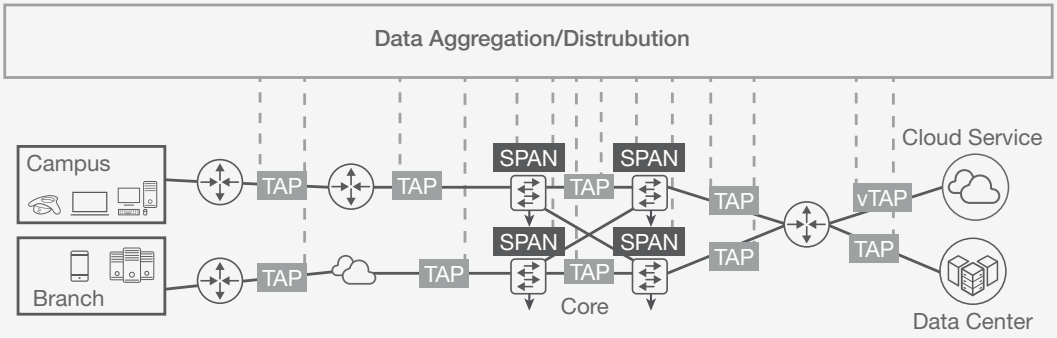

Figure 1. Data collection from multiple points across the network.

An all too common issue with SPAN ports are the direct and hidden costs. First and foremost, SPAN ports do not make a complete copy of all packets. Layers 1 and 2 data are often missing. This data is important for troubleshooting purposes. Instead of having a digital view of the network, where it is either working or not working, it is nice to have the data points in-between showing where and when things started to go wrong. This allows you to isolate problems faster. Malformed packets and other error packets are often dropped by SPAN ports, so you miss that hidden information. If the SPAN ports become overloaded with data, they will also drop potentially critical data. Since the SPAN port drops this data behind the scenes, you may never know that it existed in the first place.

A third advantage of the tap is that you can deploy it throughout the network. In contrast, SPAN ports are tied hand-in-hand to where the network switches are located. This means you cannot just place a SPAN at a trouble location to get data when you need to. In addition, you often don’t get network ingress and egress packet data, which can be very useful data.

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.

Data Aggregation Reduces Costs While Creating Simpicity

Another problem is the lack of input ports on the tools. Most monitoring and security tools need access to packet data from many locations within the network. Inserting

a direct connection to every device would be impractical and expensive. Basically, each of these devices has only a limited set of output (tap) or input (tool) ports. For instance, if you need to monitor six or more segments, you will find it difficult to directly connect them all to the monitoring tool.

Aggregation is a simple but powerful feature that eliminates this problem by consolidating a larger amount of data streams into a fewer amount of data streams. 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 also provide multiple paths through the network. This helps increase network reliability, but also creates another problem for effective monitoring. The redundant network architecture ensures that data can still reach its destination when one or more links fail. However, the redundancy also means the 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. Therefore, you may need access to double the amount of information for analysis purposes. This could be especially true if a Cisco ACI architecture with Bi-Di taps is deployed.

Because many monitoring tools require all 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 on a single street. The amount of traffic on that street is probably not representative of 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 network packet broker (NPB) solves this visibility problem. Aggregation is a simple but powerful feature of an NPB. IT engineers can use aggregation to remove port contention issues on SPAN ports, tap ports, and security and monitoring tool ports. If data from SPAN ports is still required, the 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. Data from multiple sources can be combined into a single output stream to specific or multiple tools, as needed. In this way, monitoring tools can have access to all the data from multiple network segments and to get a complete view of the network traffic. The desired data can then be replicated and distributed to one or more security and monitoring tools. This allows monitoring tools to each get a copy of the data from one or more network segments; allowing more tools to have access to the same network data.

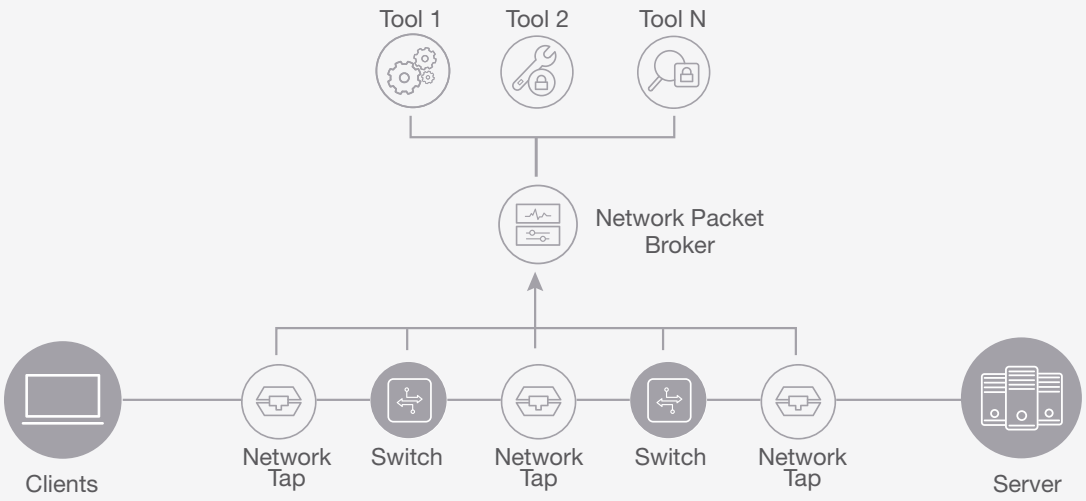

Figure 2. A network packet broker aggregates data from tap and SPAN ports.

Powerful Data Filtering Made Easy

Government IT teams are under ever-increasing pressure to improve the performance and security of corporate networks; monitoring for security, compliance, as well as application and network performance. This requires access to an increasing amount of network data, optimally performing monitoring tools, and full visibility into the network.

To meet these challenges, IT teams 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, an NPB can provide many features that off-load compute intensive processing from their tools. Such features include packet filtering, load balancing, packet deduplication, packet trimming and multiprotocol label switching (MPLS) stripping.

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 perform; resulting in more useful work being done by the monitoring tool.

In addition, most of the monitoring tools operate with a wide range of polling intervals. Some look at every packet, while others look every few seconds, and still others look only at specified intervals. This creates an inconsistent view of the network. IT often resorts to outdated and unnecessary manual processes to determine if there is an actual issue.

To modernize the infrastructure for 21st century security threats and monitoring targets, data needs to be grouped and filtered before it can be analyzed to yield actionable information. While all NPBs can perform filtering, not all NPBs achieve the same results.

However, to modernize the infrastructure for 21st century security threats and monitoring targets, data needs to be grouped and filtered before it can be analyzed to yield actionable information. While all NPBs can perform filtering, not all NPBs achieve the same results. The way the data is filtered will determine how well your agency meets its data information target.

When considering a NPB it is important to understand its filtering capabilities. Essentially, filtering can be performed in three stages.

- The first stage is performed at the port where the network is attached (network port) to the NPB.
- The second stage should be 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 downstream.

An alternative to this approach is to filter data 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 located within the NPB, 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. As an example, Keysight's solution has a patented dynamic filter engine that checks every filter that is created to eliminate potential misconfigurations and data clipping errors. While the engine checks every rule for error, it still allows overlapping filters so that multiple tools can get all the data they need.

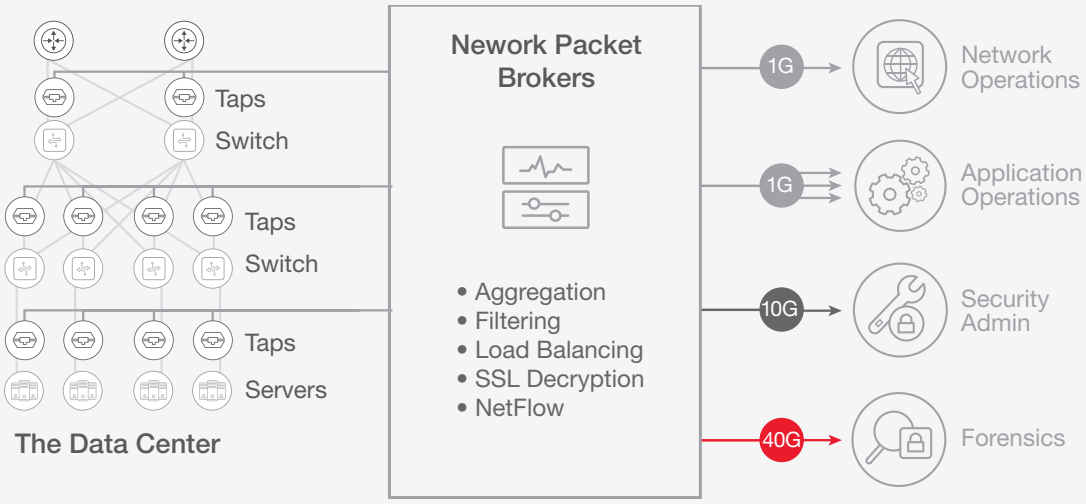

Figure 3. The network packet broker filters data before distribution to monitoring tools.

Another critical ingredient is the programming interface to the NPB. The older command line interface (CLI) is being replaced with graphical user interfaces (GUI). A GUI interface is quick and simple to both learn and use, essentially drag-and-drop with point-and-click functions. No extensive training is necessary, as the system is intuitively obvious to use. This all but eliminates filter errors due to the interface type. In contrast, ZK Research estimates that monitoring filters which have been created by a CLI interface have errors in them at least 20% of the time. This is due to the complexity of the interface that uses a series of programmatic lines and Boolean algebra to accomplish filter creation.

The GUI interface also delivers another benefit. Because of the intuitive interface, processing delays can be minimized, if not deleted. CLI-based configurations take four times longer than when using a GUI. This becomes significant because almost 50% of network managers spend more than half of their time configuring monitoring tools—leaving little time for innovation.

CLI-based configurations take four times longer than when using a GUI. This becomes significant because almost 50% of network managers spend more than half of their time configuring monitoring tools - leaving little time for innovation.

Another timesaving feature of an NPB is the ability to import and export 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 multiple IT teams (network monitoring, security, compliance, troubleshooting, etc.).

Conclusion

As government agencies attempt to comply with modernization mandates and static (if not shrinking) budgets, there are technological solutions available that can help. Network visibility is one such solution that is not only low cost but high value as well. The addition of a visibility architecture should be a strategic part of any mission critical operations. The visibility architecture's main purpose is to expose hidden network blind spots and enhance and remove any unnecessary obstacles to the agency's mission. The key point is to implement a visibility architecture that creates the fundamental capture and sharing of the valuable data needed.

There are three low cost activities that government IT personnel can implement to strengthen network security, improve overall data collection processes, and upgrade IT networks to 21st century technology:

- Implement taps for better, more flexible, data collection
- Install a network packet broker to provide data aggregation and eliminate security and monitoring tool port contention issues
- Purchase a packet broker with a dynamic filter engine and GUI interface that ensures accurate high-speed data filtering with a powerful but very easy to use interface

Keysight network visibility solutions are a powerful way to optimize your network monitoring architecture and strengthen your network security. For more information on network monitoring solutions, visit www.keysight.com/solutions/network-visibility

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