



Enhanced Visibility, Improved ROI

Abstract

The IT Security/Network Infrastructure Management departments within an organization have access to some of the richest and most useful enterprise data. Because of this, it is uniquely positioned to capture, analyze and report on a variety of operational aspects within the enterprise, enhancing the investment made in tools, as well as elevating its own value within the organization. By increasing its significance through quality “traffic analyses,” the IT and information security staffers are better positioned to garner buy-in from key executives for important initiatives that best protect a company’s infrastructure and reputation.

This unprecedented level of visibility requires the right tools to accurately measure enterprise activity and to establish internal benchmarks to mark progress.

The first step in this process is ensuring access to data, and that such accessibility remains consistently available. Gaining access to critical infrastructure and application data is dependent not just on having the right technology, but also in managing the relationships between various IT functions to ensure that the data is available. Once access has been established, the tools and means to capture relevant enterprise activity needs to be evaluated and deployed.

Many such instruments already exist in your portfolio, and some may reside within other IT functions. Creating a manageable inventory of tools and getting all of them to work harmoniously is key to maximizing these investments.

Once the foundation has been laid, and data is being consistently captured and stored, the focus can shift to extracting value from the mountain of information. Proper analysis, through correlation, validation, or prioritization is where the human element has the opportunity to really enhance the technology. By providing total enterprise awareness and operational visibility, the security organization can return value by highlighting areas of poor performance, compliance shortcomings, or opportunities for improvement.



Introduction

Information technology staffers are often an organization's unsung heroes, particularly when it comes to security functions. IT management and staff do their jobs well when no one notices them doing their jobs at all. Only when a company suffers a data breach or downtime does the IT security team become a bigger blip on everyone's radar.

That is not the way to get noticed.

Instead, progressive security departments are learning how best to leverage the vast amounts of data captured from monitoring network traffic. By accurately accessing and analyzing this traffic, these IT departments show not just the value of the company's technology investments but the value of the security and IT staffers who deploy, maintain and enhance the tools that keep networks safe from invasion. And to do this, they must employ network monitoring tools that do not disrupt traffic, nor drop packets as traffic moves through access points.

By using the proper monitoring device, the security department will not only better "see" and interpret network traffic but, in turn, sharing reports with others in the organization will help bring more visibility to IT's role within the enterprise. Together, everyone will see a quicker return on investment by fully understanding how these security tools save the company time and money (and brand reputation) by minimizing downtime and protecting data assets from attacks. Ultimately, the decision-makers will not only realize the return on investment but continue to support security initiatives and software/hardware purchases that stay ahead of the next generation of cybercriminals.

The Three Pillars of Visibility

There are three ways in which security departments can create greater visibility within an organization: accessing network traffic; accurately monitoring activity; and analyzing the data. We'll examine some ways to excel in all three of these areas in order for security to stand out within any enterprise.

Unobtrusive Access Is Key

A properly architected enterprise network includes the capability to monitor and analyze network activity. Included within a company's technological configuration is the consolidation of monitoring and analysis tools that centralize data storage and can scale as the network expands.



Proper analysis of network data requires access to traffic flowing in, out and within the network without causing disruptions, is done typically one of two ways: using a SPAN session (sometimes called port mirroring) or through a network TAP (Test Access Port).

SPAN vs. TAP

Using a SPAN (Switched Port Analyzer) to gain access to network traffic can be challenging. Such technology tends to be inexpensive, but that savings comes at a cost when SPAN ports are over-subscribed and packets are dropped before data reaches the monitoring tool. Additionally, lost error packets make it impossible to troubleshoot since data never reaches the monitoring tool. The network administrator essentially is being asked to find a solution without fully knowing what the problem entails.

Risks with a SPAN session happen when:

- a switch filters out physical layer errors, hampering some types of analysis
- an extra burden is placed on a switch's CPU to copy all data passing through the ports results in time-stamping inaccuracies
- a SPAN port hides jitter from the monitoring device, critical to real-time applications such as VoIP that rely on very precise packet timing analysis

SPAN sessions' unreliability arises when there's increased internal traffic; SPAN traffic is the lowest priority traffic in the switch. Therefore, during periods of peak traffic levels and/or bursts, the switch will drop SPAN packets. This process compromises the accuracy of the data flow being presented to the monitoring tool. As such, the monitoring tool cannot provide 100% accurate analysis if it does not receive 100% accurate data.

Conversely, a network TAP – a hardware device inserted at a specific point in the network to capture data for testing purposes – ensures continuous network visibility and zero packet loss or latency. A TAP typically consists of four ports, two to collect traffic from the network and two to provide a copy of the traffic to an attached monitoring device. A network TAP usually is placed between two points on the network so traffic passively is routed through the TAP without the network's knowledge. This passive traffic monitoring occurs seamlessly without a compromise of network speed or loss of packets.



TAPs serve multiple purposes since they can enable many technologies to help secure and manage the network such as Intrusion Detection, Network Probes and Packet sniffers without interfering with network data flows.

Breakout TAPs consist of four ports to collect and monitor traffic from a single network segment, allowing examination and analysis without disturbing the network.

Aggregating TAPs allow monitoring from multiple segments and aggregate all of the information to a single monitoring port.

Regenerating TAPs pull data from one network segment and send it to multiple monitoring tools, so the network is tapped only once while the data is used for multiple, different purposes.

V-Line TAPs, also known as Inline or Bypass TAPs, connect monitoring devices to the TAP, rather than place the monitoring tools directly in line, reducing the chance of a point of failure along the network.

Full-duplex TAPs, which work with two-way communications traffic, are ideal for ensuring visibility because they:

- never drop packets, regardless of speed or utilization
- do not filter out physical layer errors from the monitoring device
- are completely passive; they do not interfere with networks

The 1/10G Aggregating Filtering System (AFS) is an 8, 16, 24, or 48 port fixed 1U chassis. The 1/10 Gigabit Ethernet ports support copper and fiber SFP, and SFP+ modules, including multi-mode, single mode and extended mode fiber.

Political and Organizational Hurdles

Access to network data often is hampered by the friction inherent in the IT and information security functions. Deploying monitoring tools may temporarily disrupt network service – or at least hold up implementation because of a fear of such interruptions. Such concerns not only delays necessary steps to access network traffic but it prevents IT managers and executives from being seen as transformational leaders able to reduce tensions.



As such, IT management must be armed with accurate information to allay alarmists and gain allies for strategic and tactical initiatives, including IT investments that lead to enhanced network protections. In the case of network monitoring devices, there are numerous options. Two dominant technologies include SPANs and TAPs.

The use of SPAN ports to monitor network activity requires engineering resources be diverted to configure the switch to replicate traffic to the SPAN port for capture. Conversely, a TAP allows traffic to be captured in-line and, once cabled to the infrastructure, does not cause any IT resources or disruption during configurations.

When asked about the immediate benefits of using Critical TAPs, Ken Mann, network security manager for PITO, said, “By integrating TAPs into the network’s perimeter points at an early stage, we have gained maximum flexibility in connecting security devices without disrupting the smooth running of the services we provide to our users. Using them is simplicity itself.”

Capturing and Analyzing Network Traffic

Capturing traffic without causing disruptions or dropped packets is critical to monitoring large networks. Without complete and accurate data, network and systems cannot fully be aware of, let alone understand normal network activity and analyze anomalies. Such data collection can quickly overwhelm IT staff and storage unless the data is in a centralized location and is easily shared across IT functions. This level of visibility has the added benefit of fostering cross-functional communications.

Everything from traditional monitoring tools to data leakage prevention technologies must compete for out-of-band data access. By laying the foundation of access and capture, these tools can now work in harmony by sharing the same data feeds, reducing the political burdens of hunting across the enterprise for the data. This allows more time and effort to be spent on analysis of the relevant data streams, adding value to the monitoring tool investments.

Having aggregated the data from across the enterprise, and created a centralized storage location, the correlation of the data across IT silos is greatly improved. Correlation value can be achieved with not just tools, but also through the collaboration fostered by a shared view of the enterprise.



By sharing a common source of data, regardless of the analytics in use above, the need for cross-silo validation drops dramatically. This improves working relations across IT and also saves valuable time in reaching a common ground from which to determine troubleshooting or incident handling follow-up activities.

Finally, by capturing all of the relevant traffic across the enterprise, the various stakeholders can have a total operational picture from which to prioritize performance and security issues. This common context is critical to making the best use of limited IT resources.

Benefits of Enhanced Visibility

Cost Savings

Statistics gleaned from network monitoring such as utilization levels, error counts, protocol/application distribution, hosts by protocol and byte/packet counts for the users of those applications can be extremely valuable. This information is vital when trying to understand which hosts and protocols are using critical bandwidth. Malicious software, P2P applications, and other misuse can be uncovered and quickly shut down, leading to more network resources for true business users.

Return on Investment

Network Critical makes the investment in monitoring tools yield higher returns. Most network monitoring has been focused on the application layer. As monitoring tools have become more capable and specialized, the ability to identify more event types and correlate diverse data sets has also grown more sophisticated. Unfortunately, the tools do not provide visibility into all parts of the network from a central location, leaving some segments of the network unmonitored and the monitoring tools either underutilized or oversubscribed.

Chris Bihary, Managing Director for the Americas at Network Critical, adds, “With this specialization comes the challenge of connecting multiple appliances to links and having them work in concert without impacting link uptime or network reliability. The SmartNA family of network access devices provides the flexibility to achieve maximum benefit from multiple appliances while maintaining 100% link availability.”



Aggregation allows the user to present multiple links to a single tool. Depending on bandwidth utilization of the links, the network manager can apply an 8:1 link to tool ratio in a 1U system. Assuming each monitoring appliance unit costs \$50,000, the investment of \$13,000 in an aggregating TAP will yield savings of \$350,000 per each set of eight 1G links.

Regeneration allows multiple tools to access a single link providing increased security and better performance management. The ROI calculation here is done by asking the question, “What does one minute of network downtime cost my company?” Then compare that number to the cost of applying multiple specialty appliances through a fail-safe TAP providing better uptime, security and availability to network users.

Enhancing Visibility with Network Critical

Complex performance, security, and compliance requirements are driving enterprises to deploy a variety of monitoring tools. However, there are only a limited number of available SPANs and TAPs for attaching these tools. As a result, operations and security teams are often at odds over which tool is attached to which access point.

Effective monitoring means being able to scale across multiple analytics systems, consuming data from a growing number of capture points. Network Critical’s traffic access devices allow deployment as a system for total monitoring and security coverage, while at the same time reducing deployment costs and achieving a higher ROI for the monitoring and analytics tools of choice.

Conclusion

Companies today scrutinize every decision and dollar like never before. This has created keen competition for limited financial dollars in downsized budgets and now requires every investment be justified with a strong return on investment. Selecting the correct technology, including network monitoring tools, is critical to not just to current security but future buy-in for software and hardware investments.

One way to determine ROI is through the use of tools that unobtrusively access network traffic and accurately analyze the packets flowing through it. These analytics can then be used to show the validity of current security policies and procedures and, perhaps, the need for upgraded equipment when the threats posed exceed security’s current means to fight them.



Quantifying the costs and savings associated with safeguarding network data from intrusions, infestations and the insider threat can be difficult. But tools like network test access ports are one proven way for IT security teams to both improve traffic monitoring and improve visibility – and value -- within the company. And that is just how you want to be both noticed ... and noted.

[For more information regarding Network Critical's TAP technology:](#)

Network Critical
37 Franklin Street, Suite 100
Buffalo, NY 14202
(716) 558-7280
info@networkcritical.com
www.networkcritical.com