White Paper

ixia

Best Practices for Security Monitoring

...You Can't Monitor What You Can't See

26601 Agoura Road, Calabasas, CA 91302 | Tel: 818.871.1800 | Fax: 818.871.1805 | www.ixiacom.com | 915-6508-01 Rev. B, June 2013

Table of Contents

Executive Summary

Most security professionals focus on policy, training, tools, and technologies to address network security. Security tools and technologies, however, are only as good as the network data they receive for analysis. With mounting Governance, Risk Management and Compliance (GRC) requirements, the need for network monitoring is intensifying.

A new technology can help – the Network Monitoring Switch. It provides exactly the right data to each security tool and enables monitoring with dynamic adaptation. The Network Monitoring Switch resolves issues security teams have in getting visibility into the network and getting the right data for analysis. This whitepaper, targeted at security professionals, will address network visibility and will focus on:

- Monitoring inclusive of virtualized environments
- Monitoring 10GE/40GE networks using existing 1GE/10GE security tools
- Providing automated responses for adaptive monitoring
- Improving incident remediation
- Improving handling of sensitive data
- Providing granular access control so the entire monitoring process is tightly controlled

The Network Monitoring Switch resolves issues security teams have in getting visibility into the network and getting the right data for analysis.

The Challenges in Getting the Right Network Data for Analysis

Most companies have made significant investments in network security technologies and tools over the past decade. Given greatly-increased awareness of vulnerabilities, media coverage of attacks with financial impact, hacktivism, and the consumerization of IT, investments in security technology have become high priority for large enterprises. Add to these phenomenon GRC regulatory requirements, such as PCI-DSS, HIPAA, Federal Information Security Management Act (FISMA), Federal Financial Institutions Examination Council (FFIEC), Gramm-Leach-Bliley Act (GLBA), Fair and Accurate Credit Transactions Act (FACTA) and Sarbanes-Oxley, and most organizations have no choice but to invest heavily in security technologies.

However, security and compliance management tools may have limited visibility into the network due to limited TAPs and ports on networking equipment. The security professional is forced to prioritize which network segments to monitor with each tool, and as a result, may miss valuable information in other network segments.

For those unfamiliar with networking lingo, “TAP” originates in old telecommunication technology, where operators could monitor the voice line. Today, a TAP refers to a device, located on the network, which passes a copy of every packet to a monitoring/analysis technology. Another key networking term is “SPAN”, which is a Cisco term for Switched Port Analyzer. It is a bus-based way to access data packets by mirroring what comes into the port or out of the port for monitoring purposes. Other networking vendors may have

other terms for port mirroring, but the SPAN is most well-known.

Without a network monitoring switch, data is generally sent indiscriminately to tools from SPANs or TAPs, forcing the tools to perform the filtering operation and consume significant bandwidth in the process. For example, if you have SPAN ports feeding a VoIP analyzer, they may be dumping a huge amount of data on the tool, when the VoIP analyzer only needs VoIP flows.

Similarly, the IDS/IPS is sub-optimized. With limited network monitoring ports, only a subset of the network may be monitored. For example, if you have a limited number of TAPs, you may have to abandon the monitoring of one segment of the network in order to study a different network segment where suspicious behavior is detected.

In addition, you may need to get the approval of a Change Board to insert the TAP in the new segment, which can be a very time-consuming effort. The Network Data Recorder may be overloaded, and miss valuable information due to dropped packets. This can produce bad data and distorted views of the network situation, causing faulty decision-making and debugging.

The Network Analyzer (commonly known as a "Crash Cart") is physically transported to the network segments where malicious behavior and other network troubles are suspected. While it is focused on one network segment, it is entirely possible that the attack is misdirecting and damage is actually being done in another network segment.

Figure 1 depicts how a lack of network visibility leads to under-use of security and network monitoring tools

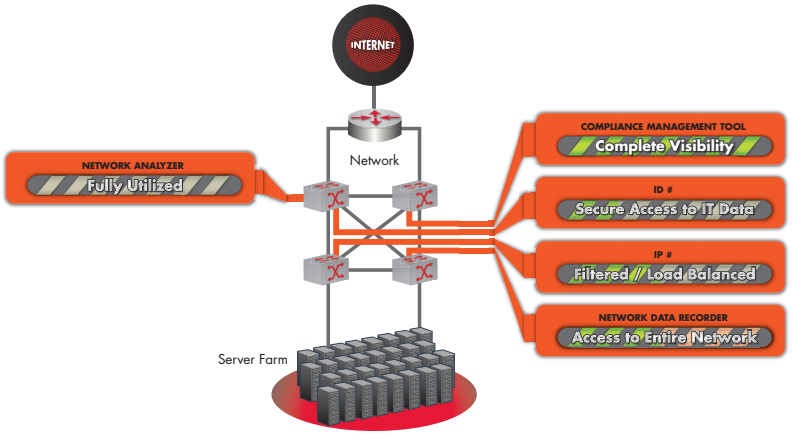

Figure 1. Your network before a network monitoring switch

In addition to under-use of tools, there are other monitoring challenges solved by a network monitoring switch:

- **Many organizations are moving from 1GE networks to 10GE or even 40GE.** Monitoring these networks can be nearly impossible with existing 1GE security tools. We will discuss the network monitoring switch as a way to address getting exactly the right data to the right security tool at the right time, and to load-balance network data so 1GE tools can remain effective.

- **Data from virtualized environments has traditionally been difficult to collect and**

Without a network monitoring switch, data is generally sent indiscriminately to tools from SPANs or TAPs, forcing the tools to perform the filtering operation and consume significant bandwidth in the process.

monitor for security purposes. We will discuss using the network monitoring switch working with VMware to allow for the aggregation of data from both physical and virtual environments for analysis with existing security tools and technologies.

- **Traditional monitoring is passive rather than dynamic.** While much of IT has made significant progress in automating tasks, network security has lagged behind in some respects. We will discuss the use of the network monitoring switch as a means to reduce human interaction by automating monitoring tasks and adaptations as required in response to the dynamic situation in the network. This improves incident remediation and reduces time to address security issues.

- **The analysis of sensitive data itself introduces potential vulnerabilities and the network monitoring switch can assist here as well.**

Granular access control is a key feature for the Network Monitoring Switch, as it is aggregating key information from the collective network.

What is a Network Monitoring Switch?

The network monitoring switch is an innovation in network management and monitoring that allows security technologies to get exactly the right data at the right time, and provides visibility to the entire network, rather than a myopic and potentially distorted view of a subset of the network.

The network monitoring switch is an innovation in network management and monitoring that allows security technologies to get exactly the right data at the right time, and provides visibility to the entire network, rather than a myopic and potentially distorted view of a subset of the network. They reside in data centers in between network SPANs or TAPs and monitoring and security tools. Network monitoring switches provide complete network visibility by aggregating, filtering, and replicating traffic so all tools get the data they need.

Network Monitoring Switch: Delivers the Right Data at the Right Time to Security Tools

With a network monitoring switch, security professionals and network engineers can aggregate information across scarce network ports and describe which security and monitoring tools need particular data. They can define and filter the data that is provided to each tool. Filtering allows the security professional to deliver just the data required for analysis to each security tool.

Figure 2 shows how a network monitoring switch improves the effectiveness of security tools and technologies to approach 100% use.

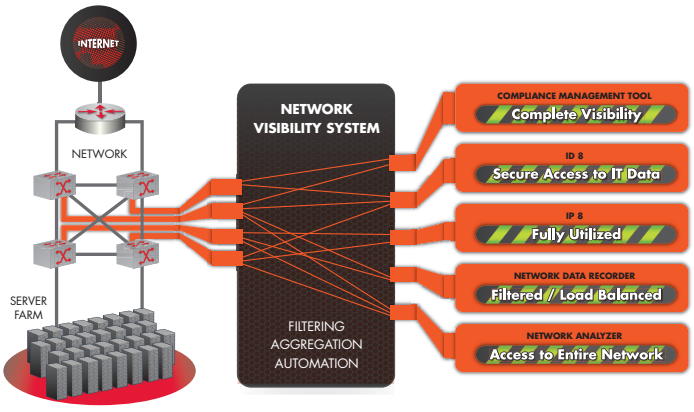

Figure 2. Your network after a network monitoring switch

Dealing with Higher Speed Ethernet (HSE)

In addition, organizations are increasingly upgrading their networks from 1GE to 10GE, and even 40GE in response to growing amounts of high-bandwidth data. Existing security tools and technologies may not be capable of accepting 10GE/40GE throughput – the hardware and/or software is not designed for that amount of data.

Using a network monitoring switch, you can filter and load-balance traffic so that existing 1GE tools can work, and investment in 1GE security tools is protected. Filtering reduces the overall amount of traffic by removing data that a tool does not need. Without the unnecessary data, a tool can do its job more effectively.

By load balancing, a network monitoring switch can divide traffic on a 10GE/40GE network across several existing 1GE tools, extending the tools' usefulness despite their native inability to handle higher bandwidth traffic.

The way a network monitoring switch performs load balancing is far more powerful than traditional load balancing. Traditional load balancing simply splits network traffic into equal loads across multiple tool ports. Tools that need to analyze data collectively, based on session, such as bi-directional traffic like VoIP calls and client-server communications have a problem with the inconsistent session-level data they receive from traditional load balancing. The network monitoring switch can load balance using layer 2, layer 3 and layer 4 packet header information, so you can perform very sophisticated load balancing.

In addition to filtering data, the network monitoring switch can solve the problem of multiple copies of the same data packet. A network monitoring configuration can cause multiple copies of the same data packet to be delivered to security tools – this is common when configuring SPANs and is accepted in network engineering circles where the priority is the production network rather than monitoring.

Sometimes, tools are capable of packet de-duplication. This is suboptimal, however, since the packets will have traversed the monitoring infrastructure prior to de-duplication. In addition, the process of de-duplicating packets consumes the processing power of the security tool, which would be better invested in providing accurate security analysis and response. The network monitoring switch performs packet de-duplication BEFORE delivery to security tools.

Using a network monitoring switch, you can filter and load-balance traffic so that existing 1GE tools can work, and investment in 1GE security tools is protected.

Security Monitoring for Virtualized Environments

Security in virtual environments is as important as security in the rest of IT. In the 2010 State of Virtualization Survey conducted by Prism Microsystems:

- **86.3% of all respondents felt that securing the virtual environment was as important as securing the rest of their IT architecture**
- **9% felt it was more important than securing the rest of their IT architecture**

Even though security is important for virtual environments, virtualized environments have traditionally been an area of frustration for security professionals due to lack of visibility. Data in the virtual environment has previously been difficult to acquire for analysis.

Even though security is important for virtual environments, virtualized environments have traditionally been an area of frustration for security professionals due to lack of visibility.

Rather than forming two separate network monitoring camps, security professionals should be included in the virtualization process, particularly if an external Cloud provider is involved. From the Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 published by the Cloud Security Alliance in December 2009:

- ***"A portion of the cost savings obtained by Cloud Computing services must be invested into increased scrutiny of the security capabilities of the provider, application of security controls, and ongoing detailed assessments and audits, to ensure requirements are continuously met."***

Regulatory requirements do not go away in the case of virtualized environments. According to the Information Supplement to the PCI DSS Virtualization Guidelines published June 2011:

- ***"Appropriate security controls should be identified and implemented in a virtualized environment that provide the same level and depth of security as can be achieved in a physical environment."***

Much of the requisite security technology is not in the virtualized environment. From the Prism study referenced above, only 20.2% of respondents were using virtual-environment-specific security solutions and strategies. In addition, security analysis done exclusively in the virtualized environment may not provide the holistic view you require to detect sophisticated attacks.

With vSphere 5.0, VMware greatly enhanced their vNetwork Distributed Switch (VDS) with NetFlow support and Port Mirroring – the ability to SPAN encrypted virtual traffic to the physical world and decrypt it. This technology allows monitoring in a virtual environment, both intra-host and inter-host. As a result, security professionals can now use existing security tools in virtualized environments.

For a description of how to configure the Ixia Net Tool Optimizer Network Monitoring Switch to perform this function, see this blog:

http://www.ixiacom.com/about-us/news-events/corporate-blog/monitoring-virtual-data-centers-its-business-usual-now

Automated Responses for Active, Adaptive, Proactive Monitoring

In a powerful way, the network monitoring switch can proactively send security tools "intel" that can be used to make other things in the network happen. Using a full tool command language (Tcl), the network monitoring switch allows security professionals and network engineers to define automation triggers based on dynamic changes in the network.

You can use Tcl automation triggers on the network monitoring switch to initiate triggers directly from statistics or filter criteria from the network monitoring tool. Tcl automation triggers can also be delivered by any network tool that can launch a third party script. Examples include Security Information and Event Management (SIEM), Network Management Systems and event correlation and logging systems. A monitoring appliance can also provide triggers via API.

These triggers make things happen with the network monitoring switch. A security policy can dictate that a particular stepped-up monitoring process must be used when there is suspicion of attack, and the network monitoring switch will make this happen. For example, a trigger from an IDS may prompt the network monitoring switch to divert data from a segment of the network where abnormal behavior is being observed to a secondary IDS for confirmation, or to a data recorder.

In a powerful way, the network monitoring switch can proactively send security tools "intel" that can be used to make other things in the network happen.

Speeding Incident Remediation

When used with SIEM, the network monitoring switch can provide dynamic incident remediation. It will automatically capture packets from security events identified by SIEM, speeding root cause analysis, eliminating time consuming manual steps, and simplifying compliance.

The network monitoring switch's automation capability complements SIEM's ability to detect, analyze, and respond to security threats. When SIEM detects an anomaly, the network monitoring switch can automatically, or via a mouse click, send the right traffic to a forensic recorder or other security probe. Incident remediation can begin the instant an anomaly occurs with the benefit of having all the required packet information.

Forensic recorders, malware protection systems, and data loss prevention appliances are only as useful as the data they receive. When you automate data center monitoring, the right traffic can be sent to the right monitoring tool at the right time. Threats can be resolved more effectively and quickly with the right packet information, leveraging fully-existing forensic recorder and security appliance investments.

Reducing the Security Risk of Sensitive Data

In some situations, a key concern for security professionals is the sensitivity of data being monitored, typically for GRC or privacy reasons. Handling sensitive personal information (SPI) is an emerging concern.

With copies of packets being generated and transported across the monitoring network in order for analysis to be performed, another potential for attack has been introduced,

even if the data never leaves the organization. Insider threats are very real and can be very expensive. According to the 2010 CyberSecurity Watch Survey, sponsored by CSO Magazine, the United States Secret Service (USSS), CERT, and Deloitte:

- **The mean monetary value of losses due to cybercrime was $394,700 among the organizations that experienced a security event. Note that this figure accounts for all types of security incidents, including both insiders and outsiders.**
- **67% of respondents stated that insider breaches are more costly than outsider breaches.**

Data may be sensitive due to compliance issues, privacy, and security implications. PCI-DSS, HIPAA, and SOX are among the compliance regulations. For example, privacy may relate to employee and customer personal information. Data being transported across the network for the purpose of security and network analysis can actually introduce a point of attack.

Very often, the security analysis tool doesn't require the data packet payload at all. It may require only the packet header, which is rich in information, such as the source of the packet, packet length and other data of analytical value. The network monitoring switch can selectively strip the data packet payload before sending the data stream to security and network performance monitoring tools. That way, your sensitive data will not traverse the network and tools that only analyze the packet header will not be exposed to sensitive data.

A network monitoring switch integrates into the existing network security management infrastructure and provides information to the network management system via SNMP.

Granular Access Control

This security whitepaper wouldn't be complete without addressing access control, because with a network monitoring switch, you are able to pull together valuable information from the collective network, which could amount to a "keys to the kingdom" scenario. Fortunately, a network monitoring switch provides an integrated approach to secure access to network data.

It can be configured to govern which users can access the control panel, and exactly which resources they can view or modify. Access to data can be controlled at multiple points, including access to network ports, tool ports, or data filters. Resources that are out of scope for an individual are locked within the control panel and are inaccessible to unauthorized users. It also provides group-level access control and integrates with TACACS+ users and groups.

A network monitoring switch integrates into the existing network security management infrastructure and provides information to the network management system via SNMP. It also provides auditable and verifiable compliance documentation.

Of critical importance is that with granular access control, security professionals will be able to access exactly the data they need for analysis without requiring excessive access. Likewise, network engineers' access is restricted to the data required for their job function.

The Network Change Board – Hindering Incident Response

Network engineers are typically under strict change control when modifying the production network. For example, they normally can't add a TAP in the network without permission from an enterprise change board. If you are investigating a potential security incident and want to modify the amount of monitoring you are doing in a certain part of the network, with a network monitoring switch, you don't need to go before a change board to modify what you monitor in the network. It is a simple matter of reconfiguring the network data flow, using a drag and drop control panel.

Conclusion

Monitoring technologies for security, compliance, and network performance are an IT responsibility that require an increasing amount of high-quality network data. Even with the best security technologies in the world, given bad or incomplete data, they will analyze the bad data and deliver incorrect and misleading analysis, thus compromising network security.

With a network monitoring switch, security professionals are empowered to get exactly the data they need to their security analysis tools to meet GRC and security requirements. The network monitoring switch provides network visibility — timely and accurate network data needed by each tool to perform analysis, along with a host of additional benefits. Key among these are: monitoring inclusive of virtualized environments, automated responses for adaptive monitoring, improved incident remediation, and improved handling of sensitive data, all while providing granular access control so the entire monitoring process is tightly managed.

Monitoring technologies for security, compliance, and network performance are an IT responsibility that require an increasing amount of high-quality network data.

ixia

For more information see http://www.ixiacom.com/