Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Optimized Network Monitoring for Real-World Threats

Copyright SANS Institute
Author Retains Full Rights
Introduction

As the threat landscape evolves in today’s networks, information security teams are scrambling to keep up. Attackers are using new and stealthy methods to infiltrate organizations and steal data, while the complexity of most networks makes it easier than ever for attackers to send malicious traffic in and out of the network without being noticed. Attackers are also going after a wider variety of attack surfaces that are typically hard to monitor. For example, criminals are taking advantage of social media used by today’s workforce to infiltrate a variety of devices being used to access e-mail and other work applications. They’re also commonly using website vulnerabilities as a way into the organization by means of SQL injection, cross-site scripting and other common attack methods. In addition, web, VoIP (Voice Over Internet Protocol), video and other applications offer more pathways to hide malicious traffic in, while encryption is also increasingly deployed to conceal malicious content within this traffic.

Many network and security teams can’t even keep pace with the growing size of their networks, let alone keep up with all these new attack surface areas to monitor and protect. As a result, current deployments and operations of security monitoring infrastructures today leave significant gaps in coverage: Are we seeing all the traffic? What threats are passing by? Do we have remote segments that we’re completely missing? How do we get more information out of our network traffic monitoring to use for correlation? How do we see into encrypted traffic to make sure it isn’t carrying in a malicious payload or carrying out sensitive information or following remote commands?

As importantly, the operations team would also like to know that advanced monitoring functions, if implemented, won’t impede the flow of business by adding even small latencies to network operations. They’d even like these visibility tools to help improve performance and performance management of their networks.

The use of switch port analyzers (often called SPAN ports) and taps to help monitor traffic at the switches and elsewhere on the network have helped network administrators address some of these problems. However, more improvement and optimization of the taps is needed to meet the needs of security and operations teams in today’s diverse, threat-prone networking environments. This paper explores current threats today’s networks face that impact monitoring capabilities, the types of gaps that exist in many current monitoring architectures, and ways that network and security monitoring can be improved through advances in traffic capture and delivery technologies such as intelligent distributed taps.
Threat Overview

The threats organizations monitor for today are significantly more stealthy and advanced than those in the years leading up to 2006. Back then, the majority of the threats included fast-spreading malware, server-side vulnerabilities (particularly in Microsoft operating systems) that could be remotely exploited on easily identifiable ports, and the introduction of botnets that primarily communicated using Internet Relay Chat (IRC). Now organizations must monitor a variety of traffic types traversing their networks and the web that can more stealthily hide and insert malicious code into authorized end points, web, VoIP and other application traffic to spread, recruit and steal data from other devices and applications connected to the network.

Take, for example, sensitive data breaches, which are announced frequently at sites like PrivacyRights.org and DataLossDB.org, as well as through other media. In recent months, Citibank lost more than 360,000 credit card account holders’ data, and Sony experienced multiple sophisticated attacks that exposed more than 100 million compromised records. The RSA breach earlier this year is another example of a more complex attack that led to the probable exposure of RSA SecurID tokens held by millions of RSA customers.

Many of these breaches incorporate sophisticated methods of social engineering and client-side software manipulation that resulted in very stealthy data exfiltration. The attackers often use spear-phishing to get employees to give up access information to further their attacks; or they use password crackers against compromised applications to gain further access rights into the network. They also set up command and control communications channels with the compromised systems, particularly in the case of bot infections.

Many of the newest and most malicious bot variants affecting organizations today are emulating the most common traffic types to hide the command and control (C&C) channels used to communicate with the bots. To avoid detection, most of the attackers’ outbound traffic uses standard ports like 80 and 443, which typically cannot be inspected deeply due to the high volume of web traffic constantly traversing the network and the time latency such inspection would cause to daily operations. This traffic can even be encrypted, which most network sensors are programmed to simply allow through without inspection.

Figure 1 is an example of how two HTTP-based strings that include bot command and control traffic can bypass both Intrusion Prevention Systems (IPSs) and firewalls.

The ability to match patterns of usage and behavior to detect malicious activity is critical in an age of sophisticated threats, where signature pattern matching has become less useful than it has been in the past. In addition to looking for known threats, organizations need to decipher what traffic (at the packet layer) is entering and, perhaps more importantly, leaving the organization—and it must be able to do so with little or no latency. This is the cornerstone of advanced monitoring and threat management.
Drivers, Deployments and Gaps

Today’s security and compliance frameworks are increasingly recommending enhanced monitoring to achieve visibility on their networks and monitor for abuses.

Numerous controls within the SANS 20 Critical Security Controls version 3.0 call for the use of network monitoring and access control systems for network visibility and threat detection. For example, Critical Control 5, “Boundary Defense,” contains a number of “Quick Wins” that rely on IDS/IPS, as well as effective firewall implementation and segmentation to deeply inspect traffic for malicious behaviors and content. Other controls deal with controlling and limiting network ports and protocols, managing vulnerabilities and network device configurations, and security-oriented network design.¹ In other words, network traffic considerations are important to network design, and monitoring for vulnerabilities is the means for alerting for when devices, their applications, and their configurations fall out of compliance.

Monitoring for threats is equally important. The latest FISMA reporting requirements released in June 2011, for example, call for more in-depth continuous monitoring metrics, including IDS/IPS, large quantities of outbound traffic, and network access control lists and firewall rules.²

Unfortunately, with the volume and types of traffic to be gathered on today’s busy networks, achieving deep and continuous monitoring goals can be difficult, if not impossible. For some organizations, compliance requirements such as HIPAA, PCI DSS, FISMA, and others may drive the use of tools like full packet capture systems for network forensics. However, most environments are not using full packet capture and analysis tools and copy only specific traffic to their monitoring and analysis tools, such as their IDSs and network monitoring consoles.

To be effective without causing network performance issues, traffic capture tools need a very sound strategy for accurately copying all traffic in a particular segment to the appropriate monitoring devices. Taps can do this today by quickly sending traffic to the right devices. But what they can’t do is scale. In today’s large complex networks, this lack of scalability can leave multiple gaps in the monitoring coverage.

**Deployment Options**

Network monitoring may take many forms. Some techniques are more operationally focused, and others are clearly in place for security and compliance reasons. For example, security teams need to monitor traffic for evidence of attacks and sensitive data compromise to satisfy PCI DSS and other compliance mandates. Network teams want to monitor the same traffic to ensure throughput is adequate, services are communicating normally, and traffic-shaping rules continue to meet performance needs.

¹ [www.sans.org/critical-security-controls/](http://www.sans.org/critical-security-controls/)
There are many types of systems and controls typically included in a network operations and security monitoring architecture. The following are some of the most commonly seen implementations:

- **Software-based monitoring:** In most cases, software-based network monitoring relies on protocols such as Simple Network Management Protocol (SNMP) to coordinate periodic polling of network devices and other systems to gather configuration and statistical data about status and performance. Well-known tools include HP OpenView, SolarWinds Orion and LANSurveyor tools, and Spiceworks.

- **Network monitoring and capture hardware:** Network operations teams may implement hardware-based traffic analysis tools that are focused on high-speed packet capture and analysis or some aspect of network monitoring or control, such as DHCP address allocation or DNS server management. Examples of network monitoring appliances include those from KACE, Infrascape, and Infoblox.

- **Security monitoring hardware:** Security teams often implement and manage a variety of network monitoring hardware, usually in the form of an IDS or network forensics capture device. In addition, many organizations are now sending network traffic and events to aggregation and correlation systems such as log management platforms and Security Information and Event Management (SIEM) products.

### SPAN Port Monitoring

Most environments that are monitoring traffic are doing so by enabling SPAN/mirror ports on switches or implementing inline network taps. The use of SPAN ports creates a number of potential operational challenges.

1. Most switches cannot feasibly support more than one or two SPAN ports, which in many cases may not be adequate to gather all the required subnet traffic in a large environment. Trying to scan more than two SPAN ports makes these systems unreasonably slow and negatively impacts, or even shuts down, the traffic flow.

2. SPAN ports can additionally create performance issues, either by dropping packets arbitrarily or overloading the switch backplane and reducing overall throughput.

3. SPAN ports create changes in the architecture that also introduce performance and potential security gaps. Well-known technologist and blogger, Tim O’Neill describes some of the major changes brought about by SPAN port implementation:
   - SPAN ports change the timing of Ethernet frame interaction.
   - SPAN is not the switch’s primary function, and may be de-prioritized during frame replication.
   - SPAN ports may drop some frames that are corrupt or below minimum size.

---

O’Neill also points out the obvious: When 10Gb/second speeds are required, most enterprise switches have no hope of handling primary functions like switching and routing while mirroring traffic to one or more additional ports. In addition, remote SPAN (typically configured as RSPAN or ERSPAN ports) may not support the capture and copy of critical data types such as Cisco Discovery Protocol traffic, as well as VLAN trunking and Dynamic trunking.

Does this mean that SPAN ports do not have a place in network and security monitoring? SPAN ports absolutely do have an important position on the network; however, they are grossly inadequate in demanding environments with high speeds and traffic volumes, as well as numerous segments that require monitoring.

**Inline Taps for Monitoring**

The second primary means to gather network data for security and performance monitoring involves the use of inline taps to send traffic to separate interfaces where monitoring devices can be established.

Although many organizations have successfully used taps for enhanced network monitoring and traffic capture, taps have several potential limitations as network speeds and volume increase, including:

- **Many taps do not have the port density necessary for advanced deployments.** For example, both the network and security teams may have separate needs to gather traffic in a certain location, but available taps may provide only a low number of intercept ports.

- **Multiple management requirements increase operational overhead.** In the case of using multiple taps to gather traffic, each tap may require a separate and different management interface, thus increasing operational overhead, decreasing visibility, and also increasing the risk of losing monitoring capabilities if one tap fails.

- **Lack of granularity.** Taps often don’t have granular capabilities like load balancing and filtering rules for traffic capture, making them less useful as network traffic grows increasingly complex.

Regardless of what monitoring tools and methods organizations are using, many are experiencing problems related to scalability because most environments have too many distinct (and indistinct) subnets, ingress and egress points, and remote locations to monitor them all adequately. Many organizations simply cannot afford to purchase network security and monitoring devices for each possible subnet location.

These market needs, along with growing requirements for enhanced and continuous monitoring for compliance and security, are necessitating a more converged monitoring approach. At a nuts and bolts level, this requires the correlation and aggregation of traffic from SPAN ports and taps to assist monitoring devices in the collection, normalization and analysis of packets and data.
How, then, should organizations look to improve their network monitoring architecture and design for more robust compliance, security and operations? They need to look for ways to improve network monitoring to add better visibility through deep packet inspection, correlation, and decryption with nominal (if any) impact to performance. The following framework should help organizations identify their monitoring assets, needs and direction going forward.

- **Start with what you have.** As in every IT endeavor, monitoring programs need to start with policy. Today’s monitoring programs, however, have grown up organically around old and new threats, user conditions and trends in network traffic. Organizations need to start with policy they may already have around monitoring and assess the technical controls already in use to support those policies. For example, an organization may already be monitoring subnets that need to be accounted for using standalone taps or SPAN ports. It may also have specific traffic types that should be allowed, other traffic types that should be denied, and logical enforcement points that can also be used to serve network operations.

- **Determine what is still needed.** Now the question becomes, “Are the methods inventoried and in use appropriate and cost effective at accomplishing the monitoring policy goals?” For example, can the organization get access to all the traffic needed for proper correlation and analysis to meet compliance goals? Do the taps in place now support the speeds and port density needed to properly capture traffic and send it to monitoring devices located elsewhere in the network? If current technologies are not able to meet the policy and compliance requirements, then additional tools and processes are likely needed.

- **Develop an intelligent monitoring landscape.** This may start with how to draw more from the taps and SPAN ports in use and unify the data collected under a single management GUI. This may be done through virtualization or the use of third-party consolidation tools that emphasize network performance. This involves adding more intelligence into the taps and SPAN ports (through the use of third-party tools, agents and specially developed hardware) that will, in turn, enhance management and granularity of monitoring controls at these locations.

- **Plan for diversity.** Monitoring diverse environments relies on flexibility in both the hardware of the taps themselves, as well as the aforementioned filtering options. Hardware options for taps should be plentiful, ranging from copper and fiber connection types at different speeds to port density for monitoring. Taps that have redundancy capabilities for failover are also key, especially for networks with very little tolerance for downtime or latency in the case of a failure or spike in network traffic. In terms of filtering, a variety of options should be available for performing filtering at different layers of the OSI stack.
For example, simple MAC address filtering, or IP address filtering, should be enabled to specify all traffic from one or more devices. All traffic on particular TCP and UDP ports may be identifiable, and the ability to direct this traffic to specific monitoring or aggregation tools would greatly facilitate more rational data analysis for certain application and service types. The ability to filter traffic based on application layer components, such as URLs or HTTP header values, would also greatly augment the network and security teams’ ability to differentiate between specific web applications and other services using HTTP as a transport mechanism.

✔ **Include encrypted traffic.** To adequately monitor encrypted traffic, traffic capture devices such as taps must be able to identify the encrypted packets, then forward this traffic to devices specifically slated for rapid decryption and inspection of the traffic. This is not easily accomplished in high-speed networks. Several steps are involved in the process.

To do this, taps direct encrypted traffic (such as HTTPS) to a separate physical port for monitoring. From there it is sent to an accelerated decryption platform that can rapidly decrypt the traffic using a stored certificate or other key. Once decrypted, the traffic must then be assessed by any additional security or network monitoring tools like an IDS or flow analyzer. Finally, the traffic is sent on to its destination, usually after re-encryption.

If the architecture is not planned correctly, decrypting traffic for inspection can take too big of a toll on performance, which may be unacceptable in environments requiring very low latency levels. In addition, SSL offloading platforms and other high-speed decryption devices can be very expensive and difficult to configure and maintain, so setting up several of these in various locations is likely not an attractive option for most enterprises.

Intelligent taps that are capable of directing traffic elsewhere in the network at high speeds are an important component of a monitoring strategy that requires inspection of encrypted traffic. These intelligent taps should also be able to be deployed and managed at more than one network segment without requiring separate administration for each tap-enabled segment.

✔ **Distribute monitoring.** Distributed traffic monitoring is a new paradigm that relies heavily on the concept of a system of interconnected intelligent taps. Each tap is considered a node within the capturing framework, which is designed as a separate layer on top of the existing network infrastructure. Then these interconnected nodes can aggregate specific types of network data and send only actionable data to designated monitoring and management consoles.

The key to this type of distributed monitoring system is selective traffic forwarding to designated security and monitoring tools, such as IDS/IPS, firewalls, forensics analyzers and SIEMs. With an intelligent, distributed system, however, each node with an interconnected intelligent tap can send traffic to different parts of the network, where intrusion detection systems, performance monitoring tools, network forensic recording devices, and other network and security tools are waiting for actionable input. This significantly enhances the value of a capture and monitoring framework by allowing existing technology to be enhanced and augmented solely with the addition of improved intelligent taps and management tools for tap activities.
✓ **Optimize network traffic.** Because these intelligent taps need to monitor high volumes of diverse types of traffic, load balancing and filters that gather only specific types of traffic have a more positive impact on network performance overall—something operations teams are supportive of. In order to do this, intelligent taps need to be specially developed hardware that can support packet capture and optimized delivery at extremely high speeds. They must also support aggregation based on requirements of network operations and the security, forensics and analysis tools to which the packets are being sent.

To support these functions, time stamping of packets and inclusion by correlation engines such as a SIEM is helpful. Specifically for load-balancing, an example would be the ability for organizations that use VoIP to leverage intelligent taps to split VoIP traffic from other data traffic and send it to a separate network analyzer toolkit for analysis.

✓ **Centralize management.** Taps and SPAN ports have to communicate as a layer in order to simplify remote administration and correlation/aggregation between the devices themselves. This layer-level communication allows for simpler aggregation of traffic, as well as more operational efficiency for managing the devices and, where necessary, applying unified policies to the devices. SPAN ports are usually managed by network device management tools from their respective switch vendors or other vendors, and modern taps are usually managed from a simple intuitive centralized console, CLI or API.

Figure 2 illustrates a simple distributed tap layer that communicates and selectively sends traffic to SIEM or network management tools, along with a management console for control and customization. Intelligent taps and the tap management console are in red.

![Figure 2: Distributed Intelligent Tap Architecture](image-url)
Savings Calculations with Enhanced Monitoring

There are clearly big savings when the monitoring and traffic capture infrastructure aggregates and relays the data more efficiently into existing sensors and analysis tools rather than simply providing interfaces for only one or two network segments at a time. Features like segmentation and acceleration also enhance current network operations and reduce operational costs.

However, as is true of any IT development under consideration, organizations need to assess the initial and longer-term capital expenditures (CAPEX) and operational expenditures (OPEX) that relate to purchase or upgrade of current monitoring processes at their switches and elsewhere in the network. These costs should be compared to the cost of running things as they are against predicted savings of the new or upgraded deployment such as streamlined operations, reduced man-hours and improved incident response.

Potential cost savings is then compared to new product and system expenses PLUS the amount of time and effort required to install, maintain and monitor the new enhanced system. In the case of network monitoring components such as taps and management software, organizations will need to weigh the scalability of the solution and whether or not it will require additional costs related to purchasing more network or security monitoring devices and tools.

When determining costs versus savings in upgrading a network capture and monitoring infrastructure, there are three key questions to consider, including:

1. **Will the solution improve operational effectiveness and efficiency?** Operational efficiency for network and security monitoring usually comes down to two major factors: time spent monitoring the actual traffic for performance or security issues and time spent configuring, managing, and troubleshooting the infrastructure. Any network monitoring and capture toolkit should minimize time spent on the mundane elements of monitoring, such as configuring taps, managing outages, and directing traffic to actual monitoring devices already in place.

2. **Will the solution improve visibility?** With a more intelligent distributed monitoring system, the answer should be, “Yes.” In other words, the taps and other customized hardware associated with this kind of monitoring should handle fast speeds, provide additional ports for monitoring and data aggregation, and also allow network and security teams to gain a more complete view of the network at any given time, with both performance and traffic statistical data available.

3. **Will the solution cost less over time?** When evaluating the overall cost of network traffic capture and aggregation, organizations should consider the capital costs of purchasing an enhanced capture infrastructure and weigh those costs against the costs required to adequately cover their network segments with additional network monitoring tools, such as IDS/IPS sensors and performance monitoring systems. With an initial outlay of OPEX for tuning and installation, a well-designed distributed network traffic capture system should ostensibly reduce monitoring time spent on numerous distinct, distributed systems that are maintained by different groups.
So given all these factors, calculating costs versus savings looks something like this:

Calculate the cost of new system + maintenance + future costs related to new system/future monitoring efforts.

Subtract the value of operational improvements introduced with new system (reduced manpower, reduced contracts for managing load with one vendor and security with another, improved visibility, segmentation, network traffic management, and so on).

Compare this to the cost of doing it the old way, including the man-hours, system maintenance and repair + coverage gaps and potential cost of those exposures.
Network monitoring will continually be called on to provide enhanced visibility into today’s busy, multi-faceted networks. With demand for higher speeds, more complex traffic patterns, and highly distributed network segments, this is no simple feat. Monitoring hardware needs to be incredibly precise, while also increasing intelligence of traffic analysis and filtering and providing more adequate distribution of traffic to monitoring tools that may not be located close by.

In order to support today’s diverse network security and analysis needs, distributed intelligent taps need to improve the overall operational efficiency within the environment. This calls for more collaboration between existing network and security tools and vendors to ensure captured traffic is quickly segmented and forwarded to the right monitoring infrastructure tools. Such collaboration provides an environment in which network and security teams can more easily maintain and manage their distributed taps and capture tools. Redundancy and failover options need to be robust and simple to configure, as well.

Finally, intelligent taps need to make sense economically, with a clear picture of both OPEX and CAPEX savings that enable network and security teams to demonstrate significant savings and efficiency improvements. They should also be centrally managed. By reducing the need for multiple tools that perform one function well, the next generation monitoring infrastructure using intelligent taps should simplify the implementation and ongoing maintenance of network monitoring. It should also provide ample functionality for various IT teams to leverage for improved efficiencies and operations.
Dave Shackleford, founder and principal consultant with Voodoo Security, is a SANS analyst, instructor, and course author, as well as a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the co-author of “Hands-On Information Security” from Course Technology as well as the “Managing Incident Response” chapter in the Course Technology book “Readings and Cases in the Management of Information Security.” Recently, Dave co-authored the first published course on virtualization security for the SANS Institute. He currently serves on the board of directors at the Technology Association of Georgia’s Information Security Society and the SANS Technology Institute.
SANS would like to thank its sponsor:

![VSS Monitoring Logo]

*Network Intelligence. Optimized.*
## Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>OnlineTXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>