Executive Summary

Network Security is a large and growing area of concern for corporations. CERT Coordination Center records show 294,037 incidents reported between 2000 and 2003, with 137,529 incidents reported in 2003 alone. Respondents to the 2003 CSI/FBI survey reported financial losses of $202 million associated with security incidents. In order to maintain an acceptable level of security in this environment, network administrators deploy a variety of perimeter and host-based tools, including firewalls, intrusion detection systems, patch and version managers, and anti-virus tools in order to deal with the constant threat. Working together, these tools form an integrated line of defense against network attacks.

For all perimeter tools, including intrusion detection systems, access to live network data is critical to effective monitoring performance. For an intrusion detection system (IDS) to be fully functional, its access to the network must be full-bandwidth, full-duplex, encompass all network traffic (not simply all well-formed, correctly-addressed packets), and provide minimal impact on network performance while still enhancing overall security. Passive Taps provide complete visibility to full-duplex traffic at multi-gigabit speeds while allowing monitoring and security systems to remain transparent to the network. As a result of these features, Taps address key concerns of IDS and security infrastructure deployments.

An Introduction to Intrusion Detection

Network managers and administrators must be on guard against all forms of unauthorized network use. An IDS monitors network traffic for activity that falls within the definition of banned activity for the network. When found, the IDS will alert administrators and allow them to take corrective action, blocking access to vulnerable ports, denying access to specific IP addresses, or shutting down services used to allow attacks. This fast-alert capability makes an IDS the front-line weapon in the network administrators’ war against hackers.

IDS software looks for patterns of activity outside the expected range of network traffic. In some cases, the patterns will be matched against known-attack signature files. In other cases, the IDS will look for certain packet types received or requested at a rate far above that seen in normal traffic. An IDS will also search for packets that have anomalies, especially those anomalies that are known to be part of attempted vulnerability exploits. Because many anomalies involve unexpected results to “standard” requests, in order to be successful at its task, the IDS must see both sides of transactions, and must have access to all traffic that flows through the network.

Keys to Successful IDS Deployment

Multiple factors are key to successfully deploying an IDS in an enterprise environment. Complete access to all network traffic, minimal impact on network operations, secure installation, and customization to specific network requirements are all critical for a successful IDS installation. Each of these factors deserves a closer look.

Access to Network Traffic

*IDS access to all network traffic* seems like an obvious requirement, but span ports may filter traffic—particularly layer 1 and select layer 2 errors—before allowing it to reach the IDS. In order to be effective, the IDS must see both correctly-formed and malformed packets, those with both proper and improper addressing, and all instances of identical packets.

*Access to traffic in both directions is critical* because some newer network and server exploits are difficult to recognize based solely on in-bound packet characteristics; not until a server responds in an unexpected
way—by opening a connection with a port usually reserved for inside-the-firewall communications, for example—will there be activity that can be recognized by the IDS.

*Monitoring device utilization should not be limited by access to traffic.* This problem occurs when attempting to monitor central backbone circuits through ports that have capacity of a fraction of the total backbone. An example might be a gigabit backbone that is monitored through a spanned 100BaseT port. While the IDS might take advantage of the full 100 megabit flow of the spanned port, it cannot possibly see the full gigabit backbone.

**Minimal Operational Impact**

*Monitoring devices should monitor, not modify, their target.* If devices are deployed “in-line,” such that all traffic must flow through and span across the fabric of the device, there is the possibility of injecting excessive latency because of internal processing. In addition, there is the possibility of blocking legitimate traffic. Span ports offer an alternative to in-line monitoring—but also may introduce latency, as the resources required to span data may detract from overall switch performance. This additional latency is not acceptable and will lead to both user and administrative dissatisfaction with the deployment.

**Secure Installation**

*A hidden deployment is a more secure deployment.* One of the most insidious threats to networks comes from attacks on the very systems used to protect networks. Depending on their base operating system, IDSs may very well prove vulnerable to attacks from the individuals it is intended to defend against. One of the most effective ways to protect an IDS against such attacks is to deploy it in such a way that its existence is hidden from the rest of the network, and from the outside world.

Hiding an IDS system makes certain requirements of the connection methods used by the system. One absolute requirement is that the connection method allow the IDS to connect to the network without requiring an IP address. Network Taps provide this capability.

**Customization to Specific Network Requirements**

*Topology.* Modern networks have come to depend on increasingly complex topologies to control security and function. A high degree of network segmentation, coupled with appliances such as load balancers and route optimizers can make finding the proper monitoring location a difficult task. The task can become more difficult if the IDS connection method is limited to a span port on a network infrastructure device. Network administrators must match IDS logical location to the concerns and vulnerabilities of the network and its stored data.

*Traffic patterns.* Traffic across an enterprise network comes from within the organization, from partners, customers and suppliers, and from the world-at-large through the Internet. Network administrators must determine which traffic poses the greatest risk and which the richest opportunity for hackers in determining where to place an IDS for optimum results. The location and the traffic it allows access to become especially important if there are any limitations on the portion of the total network flow which is accessible to the IDS software.

**An Introduction to Network Taps**

Network Taps are used to create permanent access ports for passive monitoring. A Tap, or Test Access Port, can be set up between any two network devices, such as switches, routers and firewalls. It can function as an access port for any monitoring device used to collect in-line data, including intrusion detection systems, intrusion prevention systems deployed in passive mode, protocol analyzers, and remote monitoring tools.
White Paper: Deploying Network Taps with Intrusion Detection Systems

The monitoring device connected to the Tap receives the same traffic as if it were also in-line, including all errors. Available for all major network topologies, Network Taps fall into two major categories: fiber optic and copper. Fiber Taps split the network signal into two streams, enabling both the network and monitoring device to receive the signal. Selecting the correct split ratio ensures that the network and monitoring device signals are of adequate strength. Instead of splitting the signal, Copper Taps regenerate the signal, increasing its strength so it can be received by the monitoring device as well as the network. Neither splitting nor regeneration introduce delay, or change the content or structure of information packets.

Both kinds of Taps are passive devices, enabling enabling the network to operate at a continuous flow regardless if power is available to the Tap. In the case of Fiber Taps, the key internal components do not require power, eliminating vulnerability to a power outage. If power is not available to a typical Copper Tap, the bypass circuit in the unit closes, so the transmitted signal passes directly to the receiving network device. The bypass circuit requires no external input, so Copper Taps remain passive.

Deploying an IDS Using Taps

Taps have key inherent characteristics that provide significant advantages for intrusion detection scenarios. These benefits include access to all full-duplex traffic on a link, no performance or functional overhead on the network, stealth deployment, and availability for all major network topologies.

The combination of characteristics discussed thus far make Taps an ideal network connection method for IDS deployment. Unlike network span ports, the second primary access method used for IDSs, Taps provide full network access for the IDS while imposing no filtering or performance penalty. In addition, Taps allow the IDS to easily be hidden from the rest of the network as a non-addressed device, reducing vulnerability to subversion or attack. These benefits are discussed in depth, below.

Provides Access to All Traffic

Some IDS connection methods, such as a span port on a switch, subject the network traffic to the inherent filtering mechanisms of the switch, such as the removal of layer 1 and select layer 2 errors, and under or over-sized packets, before forwarding them to the IDS. Post-filtered packets may not allow the IDS to protect the network from attacks and exploits that depend on specific badly-formed packets for success. Network Taps do not filter or otherwise interfere with network traffic, and so pass all traffic as it appears on the wire.

Access to full-duplex traffic. The issue of duplex—network traffic streams that represent either one direction, or both directions in and out of the corporate network—can be significant in any IDS implementation. To fully understand a network attack, the IDS must see both sides of the network conversation. Because Taps pass the entire physical traffic stream to the monitor port, packets in both directions can be delivered to the IDS, network sniffer, or network forensics system. Whether the monitored link is half- or full-duplex, the flow will be passed through the Tap.

Doesn’t throttle total traffic to the speed of a single port. Many network infrastructure components have interfaces of varying capacities—multiple 10/100 megabit ports and a single gigabit port, for example, or multiple gigabit ports and a single 10 gigabit port. In these instances, it is rare to dedicate the highest-speed interface as a span port for diagnostics or security. A span port based on one of the lower-speed ports will, however be able to monitor only a portion of the total device network traffic capacity. A Tap deployed on the highest-speed interface does not interfere with the capacity of the device, and provides monitoring capabilities at the full network capacity of the device.
Taps impose no speed or bandwidth limitations on the data they pass through to the monitored port—if an enterprise network has a gigabit backbone, a GigaBit Network Tap, whether fiber or copper, will pass the full bandwidth through to the network monitoring device.

Ensures Minimal Operational Impact and Secure Installation

When deployed in passive mode with a Network Tap, the IDS remains “outside” the network traffic stream. A Network Tap is not a network-addressable device, and does not impose a requirement for network addressability on any IDS connected to its monitoring port. Network traffic need not flow through the Tap-attached device to be forwarded to network destinations, and the IDS itself, when deployed in passive mode, generates no network traffic. The result is a deployment that approaches the ideal of a device that monitors the network while having no effect on normal network operations.

Because the Tap doesn’t depend on network addressing for access to network traffic, its deployment does not impose either physical or logical overhead on the network, and does not, therefore, have an impact on fragmentation, packet loss, or latency. Unlike devices that require network traffic to be processed before being forwarded, Taps allow network traffic to flow without interruption while providing a portion of the signal for use by connected analysis devices.

The same characteristics that allow Taps to provide access to traffic without impacting the network’s performance provide anonymity for any devices attached to the Tap’s monitoring port. The Tap does not require that any packets be addressed to the port or its connected device in order to monitor network traffic, and without a network address potential snoop or hackers have no way of sending potentially damaging packets to the monitoring device.

A network address is required for transmission over the network, and IDS will, in many cases, work with other network administration systems to shut off access to particular servers, applications, or services in the case of an attack. These communications may take place “out-of-band,” or outside the normal production enterprise network on a special-purpose administration network. The network interface used by the IDS for sending management messages will be visible to the management network, which is typically kept entirely separate from the production network, and safe from attacks and exploits.

Variety Allows Customization to Specific Network Requirements

One issue seldom discussed in the deployment of IDS appliances is that, if they are connected to span port interface or in-line, they are consuming valuable and limited corporate and network resources. The nature of Taps allows multiple Taps to be deployed at various locations around the enterprise, with IDS, network administration, sniffer, diagnostic, or other security and management devices connected as needed. Regeneration Taps, which amplify and distribute the network signal, allow multiple devices to be deployed at the same network point, so that assigning an IDS to a particular location, say, at the enterprise core, doesn’t prevent other devices from being deployed at the same location. This can be invaluable in building a rational, coordinated approach to network security and management.

Inside the Firewall

Deployment at the enterprise firewall allows the IDS to focus on those attacks and exploits that manage to traverse the firewall and begin to work inside the protected network. This is one of the most common locations for IDS deployment, since it brings the IDS to bear on the most important (and, in theory, most protected) portions of the total network infrastructure. As a result, most Tap deployments are within the corporate firewall. Depending on the precise location of the Tap, traffic monitored may be the entire protected stream or any portion of it. Taps may either be deployed in-line with network traffic, in which all
White Paper: Deploying Network Taps with Intrusion Detection Systems

network traffic flows directly through the Tap to the monitoring device, or in a one-armed configuration. Examples of one-armed configurations might be Taps attached to ports on routers or load-balancing devices.

Network Tap Implementation Inside the Firewall

The passive Tap creates a permanent, in-line access port to monitor all full-duplex traffic without data stream interference.

Depending on whether the Tap is fiber or copper, the network signal is split or regenerated so that the monitoring device has full access to the signal.

The monitoring device sees all traffic that has traversed the firewall, including all errors, providing critical support for network security.

In the DMZ

The DMZ is logical area of the enterprise network that is under the control of the organization but outside the protection of the corporate firewall. Devices located in the DMZ are typically those that must remain accessible to the public at large—web servers, web application servers, anonymous FTP servers, and the like. While sensitive corporate data tends not to be stored on DMZ servers, the public reputation of the company frequently rides on their availability and performance. An IDS monitoring the DMZ is not as useful for looking at total network attacks, since it will generate many false-positives that will be stopped at the corporate firewall. Instead, it can provide valuable information on and protection from those exploits and attacks aimed at bringing down corporate web servers and public browser-based applications. A Tap attached to a port in the DMZ will allow monitoring of traffic that might be filtered by the firewall or simply not passed by the enterprise boundary router—traffic that might well contain exploits and attacks that can have a significant impact on server and application performance.
In the LAN

Security and performance considerations lead most enterprises to build many subnets into their total network, and to deploy Virtual Private Networks (VPNs) to encrypt traffic flowing between clients and corporate servers. In order to keep overall network traffic manageable, packets that have both their origination and destination on the same subnet will not traverse other subnets. Because Taps don’t depend on the facilities built into any particular piece of network infrastructure, they can be deployed so that a given Tap provides a monitoring window either into a specific subnet or into as many subnets as possible. Since Taps are physical-layer devices, they will provide complete access to every bit flowing across the network, regardless of the network addresses or other characteristics attached to the traffic. Transactions on multiple logical subnets, with varying protocols, or different header characteristics will all be available to the IDS for analysis.

While Taps do not offer VPN decryption capabilities, they will allow network administrators to monitor traffic containing VPN tunnels, to be decrypted or not as security circumstances demand. Taps allow full access to all traffic flowing across the network to which they’re attached. This is especially important when the traffic is encapsulated within VPN tunnels. Many security systems use matching pairs of tunnels, one inbound and one outbound, for each complete VPN, and a half-duplex access solution will allow an IDS to receive only one side of a VPN transaction. When a growing number of security exploits take place at the application layer, riding within well-formed packets that might transit a VPN, it is critical that an IDS be deployed using Taps which allow complete access to both VPN tunnel pairs commonly used in enterprise deployment.
Increasing network use has led many enterprise network administrators to adopt route optimization and load balancing solutions to make best use of existing network connectivity. Both systems work by sending traffic originating within a network to the Internet over two or more WAN interfaces. Because the routing decisions are made on a packet-by-packet basis, it can be difficult to establish infrastructure span port locations at which complete transaction can be monitored. Taps can be put in place just outside core enterprise routers, or in other full-traffic locations as dictated by the particular enterprise network architecture, so that all network traffic, in both directions, may be inspected.

Taps can also be critical when the IDS interfaces are the point of load balancing. When an IDS with 100 Mbps sensor interfaces is deployed across a Gigabit network link, for example, a Tap will provide non-intrusive full-bandwidth access to all network traffic—traffic which is then balanced across an array of various 100 Mbps sensors. As enterprises begin to consider the move to 10 Gigabit backbones, Taps, especially in multiple-tap configurations, will continue to increase in importance, allowing current-generation IDS devices to function in higher-bandwidth networks without the risk of becoming a single point-of-failure bottleneck.
Tap Futures
Historically, passive and active modes were the two key means of IDS deployment. In passive mode, the IDS monitors all traffic for potential attacks, but is not deployed in-line. In active mode the IDS—now known as an intrusion prevention system—is deployed in-line to be able to both monitor and block attacks. Because of the legitimate worry of false positives causing an intrusion prevention system to block valid network traffic, passive mode is still the most common mode of deployment—but security administrators and IDS vendors have been working on ways to add active responses, such as the ability to drop packets and end sessions, to an otherwise passive deployment. As Network Taps are the ideal network connection methods for a passive deployment, it follows that the natural evolution of Network Taps is to support this Active Response capability. As the leader in the Network Tap space, Net Optics is first to market with Taps supporting advanced Active Response capability. Their new Active Response Regeneration Taps enable passive analysis of data, plus the optional utilization of an active port to inject responses such as TCP resets to network events.

Taps and IDS—An Ideal Partnership
The inherent qualities of Taps are an excellent match to the needs of an IDS for optimal detection and maximum security. The key benefits of deploying Taps with an IDS include:

- Taps allow access to all traffic on a network, providing an IDS with errors, malformed packets, streams to and from all network addresses, packets encapsulated within VPN tunnels, complete transactions (including traffic originating both within and without the network), and more. This complete, full-duplex network traffic access is perhaps the single most critical ingredient in allowing an IDS to succeed in its mission of protecting the network.

- Taps eliminate the IDS as a point of failure within the network—because the traffic flow does not pass through the IDS as a requirement for moving towards its destination, an IDS failure or compromise will not result in network failure. The passive nature of Taps also means that the Tap itself is not a point of failure within the network; in a worst-case failure, network traffic still flows through the Tap.

- Taps do not compromise the strength or integrity of network traffic that passes through them. In terms of network data integrity, Taps are a “zero-cost” network component. With Fiber Taps, the signal diverted for Tap attachment purposes does not meaningfully degrade the signal strength down-line. With Copper Taps, the signal is regenerated accurately, meaning that the network flow downstream is at least as strong as the network flow entering the Tap.

- Taps do not represent an increased overhead or security risk within the network, because the Taps are not processing the packets, and neither the Tap itself nor any IDS attached to the Tap require an IP address to function. Although there are exploits that can still operate against an IDS attached to a Tap (exploits designed, for example, to attack any device that receives the payload, regardless of its address), overall vulnerability is reduced when the IDS isn’t advertising its existence on the network. The Tap itself has no vulnerability to packet-borne exploits, making it a network infrastructure component impervious to these attacks.

- And finally, Taps provide multiple connection interfaces at key network locations, supporting multiple-device security systems and providing IDS availability within load-balanced networks.

The permanent, passive Tap solution eliminates the risks associated with monitoring with a span port or in-line connection. Taps are perfect demarcation points between the production network monitored by an IDS.
White Paper: Deploying Network Taps with Intrusion Detection Systems

and the secure “out-of-band,” management-only network behind the enterprise network itself. Since Taps are not themselves candidates for external exploit, there is no security cost to leaving Taps in place as permanent pieces of the network infrastructure. Multiple-tap configurations can provide full-time IDS interfaces while allowing for the occasional attachment of other network testing, diagnostic, or security components.

The nature of Taps makes them an ideal complement to enterprise IDS deployment—the combination allows the IDS to be used to its full capabilities while exposing both the IDS and the production network to minimum risk. Maximizing security and minimizing risk are the goals of a complete network security program which will include an IDS—deploying the IDS with Taps ensures that the IDS deployment itself meets the goals of the security program.

For further information, please contact:

Net Optics, Inc.
1130 Mountain View-Alviso Road
Sunnyvale, CA 94089
(408) 737-7777
info@netoptics.com
www.netoptics.com