

Network Traffic Port Aggregation: Improved Visibility, Security, and Efficiency

White Paper

January 2007

The Challenge

The 2006 eCrime Watch Survey shows that 58% of security events were committed by intruders or people outside of the organization, whereas 27% of events were committed by people within the organization.

The Solution

Performance management architectures that combine the benefits of test access ports (Taps) with that of established monitoring devices.

Introduction

Enterprise entities rely on network systems for internal operations and external communications. Companies of all sizes require that these communication paths function at top speed and transfer data accurately, completely, and consistently. Network systems are also expected to keep the transfer of information exclusively between authorized users, both internal and external to the enterprise.

The 2006 eCrime Watch Survey shows that 58% of security events were committed by intruders or people outside of the organization, whereas 27% of events were committed by people within the organization. The number of organizations reporting at least one insider event has increased 16% over the previous year. Financial and operational losses combined with harm to an enterprise's reputation are significant results of these security events. (1)

The Ponemon Institute and ArcSight, Inc. surveyed 450 experienced IT security professionals. The results show that "more than 78% of respondents reported one or more unreported insider-related security breaches within their company." (2) Maintaining privacy and keeping proprietary information within the appropriate departments of an organization are critical goals for the business community.

Each day, enterprise managers require more statistics to achieve visibility, security, and efficiency in network systems. More hardware is required increasing cost and physical space as additional monitoring units are placed in the system. The value of intelligence within networks is becoming accepted as the norm in network operations.

"Because industries that rely on the network to drive competitive differentiation, like those in finance to transmit real-time market data, benefit the most from network-resident intelligence. We expect that the less bleeding-edge industries like manufacturing will seek smart networks in a few years' time as these capabilities become more commonplace," writes Robert Whiteley of Forrester Research, Inc. (3)

Differing Goals of Network Departments

In small organizations, visibility, security, and efficiency may be the goals of the same person, and the needs of the organization and the network may be more easily addressed. More often, separate departments within the organization having different priorities are responsible for achievement of security and performance in the network. Network engineers are responsible for the overall reliability of the network. These employees need to know baseline statistics, application responses, and the general health of the network at any one point in time. Meanwhile, network security staff tend to focus on the detection and prevention of unauthorized use of the network by hackers (external) or unauthorized use by company personnel (internal).

Providing Optimum Performance in the Network

In order to achieve optimum performance, network engineers want to know the following information:

- Is every link functioning?
- Is the data being transferred completely and accurately?
- Are there high and low use periods? When and where do they occur?
- How do these trends affect network service?
- What affect do new applications have on the network?

The answers to these questions assist network engineers with providing smooth uninterrupted service to the enterprise. In the finance industry, a breakdown in the network typically results in the loss of irreplaceable dollars by disrupting precisely timed transfers.

Established Monitoring Devices

Remote monitoring (RMON) probes, and protocol analyzers or sniffers, are monitoring devices that are deployed on networks and allow managers to observe network activity from remote locations. These devices assist network personnel to troubleshoot faulty links, monitor network usage, gather and report network statistics, and filter for suspicious content.

Network security managers use one or more devices to secure incoming and outgoing traffic. Security devices have differing capabilities and provide different purposes to an enterprise. Intrusion Detection Systems (IDS) provide information regarding viruses, threats, and denial of service on the network. IDS devices monitor network links enabling managers to view the activity. The managers then decide whether to act on the information. Intrusion Prevention Systems (IPS) are placed in-line where they serve to notify network security of suspicious activity and respond to the activity by blocking traffic.

Established Industry Methods—Using Span Ports with Monitoring Devices

Network engineers use switched port analyzers (span ports) to copy, or mirror, the transmission stream to their network monitoring devices. However, the monitoring devices connected to span ports do not always see the characteristics of the traffic on a link.

Network traffic consists of packets that can become damaged or corrupt, may fall below minimum size, or become too large. These errors in physical layers 1 and 2 are not visible through a span port. Although the span port makes a copy of all traffic, it cannot transmit errors to monitoring devices. As a result, network engineers can only view passed traffic and are unable to make an educated assessment without the full traffic.

Additionally, using span ports to monitor operations on a routine basis requires extensive set-up and reconfiguration time. Network monitoring through span ports also limits visibility to the data you have defined. Network security and network engineers must coordinate their schedules and hardware in order to access the network through the limited number of NICs and span ports.

Often, multiple monitoring devices are required to be connected to the network to meet the needs of the organization. Since each monitoring device requires an available NIC to receive the traffic, network engineers may need to connect and disconnect hardware to pinpoint network issues. If multiple devices are required by security demands of the enterprise, a shortage of NICs becomes a limiting factor that may result in reduced service and or increased costs for equipment and space.

In the past, additional NICs could be added to computer hardware through expansion slots; currently, computers normally have one integrated NIC.

Using Span Ports with Monitoring Devices Network engineers use switched port analyzers (span ports) to copy, or mirror, the transmission stream to their network monitoring devices. However, the monitoring devices connected to span ports do not always see the characteristics of the traffic on a link.

In-line Devices

Another fairly recent development in network monitoring is the placement of IDS and IPS devices directly in the networks path, allowing network managers to collect or manipulate traffic as it passes through the device. The critical drawback to placing devices in the traffic path is that if and when a device fails or requires servicing, the physical stream is blocked and network service is interrupted.

Network Test Access Ports (Taps)

Permanent access to the physical link between two devices was achieved by the development of test access ports, or Taps. Taps are placed between any two network devices and allow full-duplex traffic to pass through without affecting the data stream. Taps have two ports that connect directly to the monitoring device enabling the manager to passively view all traffic without affecting the traffic.

Taps are an improvement over span ports because taps send all traffic in the physical 1 and 2 layers to the monitoring device, including errors. By using taps, network engineers gain visibility into the network to look for packet errors and bandwidth anomalies that were not visible using span ports.

Although taps are placed in-line just as monitoring devices can be placed in-line, the passive design of the tap means that the device does not affect the physical stream if the tap fails. Industry-leading features include dual power supplies providing increased reliability.

Port Aggregation

Although having two ports on a tap was beneficial to network managers, the issue then became how to monitor data if the IDS had only one NIC. This recurring shortage of ports when using monitoring devices instigated the development of combined port functions.

In a port aggregator tap, the full-duplex stream is combined into one port on the tap and sent to one port on the monitoring device. Monitoring devices with multiple NICs can now monitor more than one segment at a time.

This Port Aggregator tap combines the two TX streams into a single output interface. This single-output device makes it easy to connect a device that has only a single monitoring interface. (4)

Equipment efficiency increases using port aggregation, since fewer NICs are required within the monitoring device, enabling more ports to be available at any one time.

In addition, the buffering functionality introduced by Net Optics help to better optimize the flow of traffic being forwarded to monitoring devices. If traffic flow exceeds the bandwidth capability of the link, the overflow is collected in the Tap's buffer until the load diminishes. The data is then sent on to the monitoring device without interruption or loss of information.

Expanding the Function of Taps

Today, network administrators are installing hardware and software that allow real-time views of the network. In a recent report from Forrester Research, Inc., Robert Whiteley describes a smart network as "one with embedded intel-

ligence like security, virtualization, and optimization technologies” whereas a dumb network has “simple ‘plumbing’ that just routes and switches” (5). The results of the Forrester research survey show that 71% of businesses prefer smart networks (6).

The increasing need expressed by customers for more detailed traffic information, easy access to those statistics, more control of the taps, and the shortage of ports for monitoring devices encouraged Net Optics, Inc. to develop iTap Port Aggregator technology. The intelligent technology in iTap helps network managers use their monitoring and security devices more effectively, reduce response time to anomalies, and observe network status on a continual basis from remote locations. The iTap Port Aggregator assists network engineers in achieving the overall security, efficiency, and reliability demanded by small companies and large enterprise organizations. “It’s not a replacement for probes and other network monitors, but it provides a heads-up on where and when those tools should be used”, wrote Bruce Boardman of Network Computing. (7)

Port Aggregation - iTap

The Port Aggregation functionality within iTap solves two important network operation issues—combining traffic and viewing network statistics. First, this device combines both directions of a full-duplex stream. Secondly, a display on the front panel of the unit allows network statistics to be viewed at any time.

Furthermore, the iTap Port Aggregator includes onboard memory for buffering excess data when traffic exceeds bandwidth capacity. When traffic volume drops below capacity, the buffer resumes sending the collected packets to the monitoring device in the order the packets were received. In March 2006, Richard Bejtlich commented, “With the iTap, you can see immediate and ongoing traffic statistics that ensure you’re observing and collecting what you expect.” (8)

Information Visible Through an iTap

A closer look at the information available from the iTap Port Aggregator reveals the percent of network utilization, physical layer statistics, links, and power status to the iTap. This network utilization detail is important for seamless, reliable transmission of data throughout organizations. The iTap Port Aggregator front panel shows the individual current bandwidth utilization for each side of the link as a percent of total capacity as well as the separate current peak levels for A and B. Knowing peak levels is critical since packets can be dropped during high-load periods resulting in incomplete information at the destination. A manual reset button on the front panel resets the unit to record the next peak event.

Unlike many taps, the iTap Port Aggregator displays detailed statistics about the physical stream through the tap on a continuous basis. The Net Optics iTap counts bytes, individual packets, under- and over-sized packets, and packet collisions. Packet loss, transmission latency, and errors identified by cyclic redundancy checks (CRC) are recorded as well. These facts assist network engineers and operators to identify trends and abnormalities, spot high traffic periods, and locate faulty hardware.

By watching the continuous statistics shown on the front panel of the iTap or by viewing from remote monitoring stations, network engineers can verify that

“With the iTap, you can see immediate and ongoing traffic statistics that ensure you’re observing and collecting what you expect.”

Richard Bejtlich

Tao Security Monitoring

March 2006

"But just deploying gear isn't enough", writes Robert Whiteley. "To handle a more complex, more intelligent network, firms must invest in the right network management tools."

links and connections are intact. Loss of power to the iTap does not interrupt the network traffic.

The LED lights on the front panel indicate power on or off. Network operators can see at-a-glance that the Tap is powered and thus can pinpoint or eliminate the Tap when troubleshooting on the network. The iTap is equipped with redundant power that keeps the tap operating when one electrical circuit fails, while the visible power indicator provides quick information when both fail or the unit is turned off.

Accessibility and Control

Network managers require control in the taps they deploy. The taps must offer functions that can be turned on and off independently, such as threshold alarms and management port visibility using IP addresses. Most importantly, network engineers demand accessibility to the statistics and functions at the site of deployment as well as the ability to retrieve statistics and control functions from remote locations.

Unlike previous taps, the iTap Port Aggregator incorporates threshold alarms that are both visible on the front panel via LEDs and alarms that are sent to management tools to alert network managers when traffic load is increasing. Network managers then have time to take measures to prevent packet loss and service interruption.

Another control function built into the iTap is the IP address assigned to the management port. Many network managers want to be able to communicate with the management port from remote locations—a task requiring an IP address to be seen on the Internet. For extra security measures, network managers can disable the remote access to the iTap management port.

Software Management Tools

"But just deploying gear isn't enough", writes Robert Whiteley. "To handle a more complex, more intelligent network, firms must invest in the right network management tools." [9]

The demand for accessible information and control of hardware from multiple locations encouraged Net Optics, Inc. to broaden the control functions of its intelligent Taps. The iTap provides managers with several tools to view and obtain statistics:

- Command Line Interface (CLI)
- Web Manager
- System Manager
- Management Information Base (MIB)
- Wireless Access

Command Line Interface—The CLI interface allows for local control of all management functions for a single device. Access is achieved via password-protected RS232 port.

Web Manager—Added iTap intelligence provides remote access manageability per single targeted device. All network statistics and functions previously only available via CLI are now accessible through the Internet. No specialized software is required.

System Manager—GUI based “System Manager” creates centralized management of all iTap devices in the network. All or select iTaps can now be grouped by department or function for optimum manageability and more efficient monitoring. You can view all status, configuration, and traffic information, as well as quickly make changes to any iTap in the system.

MIB—The System Manager software application is not required to organize and manage multiple iTap Port Aggregators. Enterprises with existing simple network management protocol (SNMP) tools in place or who wish to use another SNMP product can load the iTap Management Information Base (MIB) into their own software.

Wireless Access—The iTap Port Aggregator also offers an optional wireless control capability on most Taps. iTaps can be monitored and assessed using handheld wireless products; however, the products must be within close range. A network engineer passing an iTap could perform a spot check with a cell phone or PDA (personal digital assistant).

Accessibility to all iTaps from remote locations reduces time spent inspecting each tap for errors and manually resetting after an overload situation. Network managers can monitor and troubleshoot from a central location to keep the network up and running smoothly while the enterprise operates productively and efficiently. Robert Whiteley believes that “Network hardware is no longer the center of innovation—software is. The network’s value is in its embedded software, not hardware.” (10)

Conclusion

The “intelligence” in the iTap Port Aggregator assists enterprise entities to achieve optimal use of its security measures, to implement efficient, seamless network operation, and to provide uninterrupted network service to all departments in the organization. The iTap provides information, control, and access, allowing network engineers to more rapidly pinpoint and diagnose disruptions in service, to better monitor trends in use of the network, and to use the software they prefer to access the hardware and statistics.

As Robert Whiteley writes in his article *The Debate is Over: Businesses Prefer Smart Networks*, “Companies, regardless of size, region, or industry, overwhelmingly prefer to use smart networks in their architecture. Hardware advancements, more sophisticated network software, and better management tools mean that firms can reliably embed intelligent security, mobility, virtualization, and acceleration directly into the network.” (11)

Further iTap functionality will continue to be added to Net Optics products based upon market trends and customer feedback. This will further enable network managers to deploy the most current network equipment available to achieve optimum visibility, security, and efficiency in their networks.

For more information on this and other Net Optics solutions, visit our website or contact Net Optics customer service.

Endnotes

1. CERT® Coordination Center, "The 2006 eCrime Watch Survey", <http://www.cert.org/archive/pdf/ecrimesurvey06.pdf>, 9/29/06.
2. Ponemon Institute, "Latest Ponemon Institute Study Ties Lack of Awareness in Corner Office to Insider Threat Challenges", http://www.ponemon.org/press/Ponemon_ArcSight_Insider_Study_9.pdf, press release September 12, 2006.
3. Robert Whiteley, "The Debate Is Over: Businesses Prefer Smart Networks", Forrester Research, Inc., September 8, 2006.
4. Richard Bejtlich, *The Tao of Network Security Monitoring* (Addison-Wesley, 2005), 72.
5. See note 3.
6. See note 3.
7. Bruce Boardman, "Tap into Easy Network Management", *Network Computing*, December 8, 2005.
8. Richard Bejtlich, <http://taosecurity.blogspot.com/2006/03/net-optics-introduces-itap-this.html>, 9/22/06.
9. See note 3.
10. See note 3.
11. See note 3.



Customer First!

5303 Betsy Ross Drive
Santa Clara, CA 95054
www.netoptics.com