



September 2008



Into the Deep: Exploring Deep Packet Inspection

BY TIMOTHY WATERS, VICE PRESIDENT, BIVIO NETWORKS

According to a report issued by the Office of Management and Budget, thousands of cyber-related attacks on government agency networks were reported last year, ranging from network intrusions to viruses to malicious worms. These attacks have monumentally increased over the years – by 56 percent since 2006 and by 80 percent since 2005.

Now more than ever, agencies need to scrutinize network traffic to understand who is using their networks and in what capacity. To that end, the need for budget-conscious, real-time programmable applications that enable information assurance and network-wide policy enforcement is critical. To help agencies transfer and monitor large amounts of data at wire speed, federal IT managers should look to a technology that enables unprecedented visibility into network traffic: Deep Packet Inspection (DPI).

Complex Traffic Brings Complex Security Concerns

In the past, perimeter-based network monitoring technologies were sufficient to guard against security threats. Now agencies are faced with new types of security threats originating from within and outside their networks. Internal threats arise from employees unknowingly downloading unsafe content, for instance. Hackers are now

more sophisticated and can easily mask malicious content to make it undetectable by firewalls.

In turn, government is becoming increasingly dependent on a growing pool of next-generation converged applications, like VoIP and streaming multimedia, to enhance communication and collaboration. At the same time, this diverse traffic presents unique challenges amidst the current push

The ABC's of DPI

Network monitoring technology must be sophisticated enough to allow federal IT managers to define their own network policies, identify security threats and take action to protect against threats once they are detected.

Federal IT managers need programmable, policy-centric technologies that allow more advanced knowledge and control over the data crossing their networks.

By enabling the examination of a data packet's entire payload, DPI gives unprecedented "visibility" into deeper levels of network traffic to identify and remedy vulnerabilities like viruses, data leakage and unauthorized access.

towards collaboration and information sharing.

Agencies need to manage this dynamic traffic and new security threats within and across multiple agency networks while ensuring that their networks can maintain the critical division between classified and unclassified data.

With DPI technology, shared data can be rapidly and efficiently processed and distributed across multiple government agency locations, increasing the ability to respond to security threats and manage the massive traffic processing and monitoring requirements of the modern collaborative agency environment.

By enabling the examination of a data packet's entire payload, DPI gives unprecedented "visibility" into deeper levels of network traffic to identify and remedy vulnerabilities like viruses, data leakage and unauthorized access. Plus when implemented on high performance network appliances, DPI permits the secure transfer of extremely large amounts of data at wire speed to support the demands of a collaborative, net-centric environment.

To better understand DPI, compare the data sent across a network to an envelope sent through the mail. Current network monitoring technology allows the recipient to scan only the address on the envelope. While the address may come from a trustworthy source, the data recipient is unable to view any of the content within the envelope which could

technology, a network is equipped to identify malicious content regardless of origin, ultimately preventing network infiltration.

DPI is not limited to improving the protection of internal networks, but ultimately enhances the overall capabilities of government networks. Lawful intercept is a good example.

Lawful intercept, used to gather intelligence for national security purposes, refers to the legal capture of communications information by law enforcement agencies in accordance with local and national laws. Integrated communications technologies – VoIP phones, e-mail and instant messaging – force lawful intercept to focus on monitoring traffic regardless of its origin.

Law enforcement agencies cannot easily

Agencies must depend on solutions that are tailored to their specific need to run scalable, DPI and information assurance applications at wire speed. To satisfy agency requirements, these platforms must be:

- **Programmable:** Agencies must be able to rapidly develop, deploy and manage mission-critical operations, new services and applications;
- **Customizable:** Every agency has different network users and uses, resulting in a varied set of ever-changing network solutions requirements;
- **Policy-centric:** Government agencies must have the ability to define their own policies for network traffic;
- **Linux-based:** A majority of forward-leaning security and network monitoring applications are open source and Linux-based;
- **Cost-efficient:** Physical space, facilities and power costs force agencies to make budget-conscious, high-performance decisions.

Government must arm its networks with technology that is as dynamic as the threats it is guarding against.

be malicious. DPI technology enables the network to examine the entire contents of the envelope along with the address for all types of malicious content to protect against a broad array of security threats.

DPI: The New Cyber Guard on Duty

Consider the large number of federal employees with external Web mail accounts through Yahoo! or Google mail. Federal employees can download unsafe content from their Web mail accounts while logged in to an agency network and unknowingly compromise it. Current network monitoring devices can protect against viruses or malware transferred within agency networks, but they cannot effectively monitor materials transferred or downloaded from external networks. With DPI

sift through the massive amounts of call record data from individual network entities, making lawful intercept more difficult. But a single DPI packet processor can intelligently identify calls, examine and extract specific call data and content from a call record, and help assess illegal activity and potential security threats.

Individual Threats Require Customized Solutions

The trend in federal agencies is to deploy security, traffic management and network monitoring and analysis solutions on one common operational platform leveraging both internally developed government off the shelf (GOTS) applications and best in class open source applications.

Thinking for the Future

Evolving network technologies, expanding network traffic and an increasing number of network users will continue to bedevil government agencies with mounting security threats. These threats and challenges continue to grow in number, sophistication and frequency.

Government must arm its networks with technology that is as dynamic as the threats they are guarding against. Supported by a flexible, programmable operational platform, DPI can help agencies manage, secure and control network traffic at wire speed, ultimately providing a long term solution for a long term problem.