

October 30, 2008



## Another View: Leveraging Deep Packet Inspection

BY TIMOTHY WATERS, VICE PRESIDENT, BIVIO NETWORKS

Deep packet inspection applications offer agency IT managers improved tools to monitor and secure agency networks.

For years, government information technology managers have chased a holy grail: a truly policy-centric network that enables near-total oversight of who is on the network, what users are doing and the resources to which they have access.

In the past, traffic analysis solutions were largely passive and designed only to warn government IT managers of suspicious behavior or malicious content on their network. However, today's government network managers face an ever-increasing number of complex challenges — from the usual suspects such as worm and viruses, of course, but also from a net-centric environment that requires real-time security without impeding information sharing within and between agencies.

To meet these challenges, agencies are now deploying deep packet inspection (DPI)-based applications throughout their networks. DPI technology is widely embraced in some form in many government agencies, including the National Labs, intelligence agencies and the Defense Information Systems Agency. The

technology promises a wide range of further innovative capabilities that, when fully employed, can help government IT managers take networking monitoring, analysis and security to the next level.

### Policy-centric security

DPI technology enables the full examination of a data packet as it passes an inspection point, searching for viruses, spam, network intrusions, and malicious content, as well as any and all predefined policy criteria, and filters the packet accordingly.

Data packets deemed unsafe or inconsistent with established network policies can be routed to a different destination, while data packets that pass inspection can continue to their destination in real time. In other words, deep packet inspection uses customized security policies to inspect any and all data packets, regardless of type, and then direct them to the appropriate network resource at maximum throughput -- creating a truly policy-centric network environment for top-notch information assurance.

By allowing for the examination of a data packet's entire payload, DPI-based applications give agency IT managers unprecedented visibility into deeper levels of network traffic to identify and remedy security vulnerabilities. This enhanced ability to monitor, analyze and act on network traffic represents a significant improvement over the limited visibility and control government IT managers previously had over their networks.

The most popular use of DPI technology deployed by agencies today is for intrusion detection. DPI can combine the functionality of an intrusion detection system (IDS) and an intrusion prevention system (IPS) with a traditional stateful firewall. This combination makes it possible to detect attacks that neither the IDS/IPS nor the stateful firewall can catch on their own.

As DPI technology becomes widespread, agencies are in the process of extending its capabilities for stronger network protection.

### Beyond the basics

For example, the Defense Department implements Computer Network Defense activities to detect, analyze and respond to unauthorized activity in DOD information systems and computer networks. DPI technologies can play a key role in

strengthening the ability of CND efforts to detect and act on security threats. A great example is the Access Control Lists that the DOD establishes and maintains at the borders and gateways of its networks.

When a data packet requests to perform an operation, the system first checks the ACL list to decide whether to proceed with the operation. This method is satisfactory when the ACL is designed to

network may be highly encrypted, heuristic statistical (i.e., speculative) flow analysis uses data signatures to look for specific attributes and characteristics for detecting viruses and other forms of malware. This means IT managers are able to enforce security policies based on heuristic details that point to suspicious or likely malicious data, even though they are unable to access the exact information contained in the data packet. This ability, in combination with

---

## DPI technology is widely embraced in some form in many government agencies, including the National Labs, intelligence agencies and the Defense Information Systems Agency.

---

block a recognized, constant and standard security practice, such as blocking traffic that traverses port 139, which supports connection-oriented file sharing activities. This strategy fails, however, when “undesirable” traffic traverses ports that can never be blocked, such as port 80, the primary port for the Web. In this case, only deep inspection of a packet’s contents can provide sufficient detail on the true protocol that may be disguised as traditional port 80-traffic to take appropriate post-analysis action.

In addition, DPI can play a large role in identifying potential internal security risks through extrusion detection and data leak prevention, and can also be used in conjunction with heuristic statistical flow analysis to help agencies adapt their toolsets to monitor and analyze highly encrypted links.

For example, while data traversing the

DPI, presents a highly effective method of identifying and combating network vulnerabilities.

Beyond these current capabilities, DPI technology will evolve along with government practices, providing further opportunities for its use. In particular, one can envision DPI playing a role in supporting the area of Military Deception (MILDEC). MILDEC includes actions executed deliberately to mislead adversary decision makers as to friendly U.S. military capabilities, intentions and operations, causing the adversary to take specific action (or inaction) that will contribute to the accomplishment of the United States’ mission. DPI makes techniques that involve manipulation of data packets possible and, therefore, could be part of a MILDEC strategy to obscure secure government data to opponents attempting to tap into protected information.

### DPI myths dispelled

Although the benefits of DPI technology for the security of government IT networks are clear, the technology has raised privacy concerns. Yet, a deeper understanding of DPI functionality will go a long way toward allaying some of these concerns. In reality, rather than compromising privacy or security, DPI solutions actually serve to improve the safety of the network for its users.

DPI technologies are at times associated with the ability to pick private data such as credit card information or social security numbers out of a packet stream. In fact, the opposite is true. Legitimate Web sites use strong encryption techniques to conceal private data. Users are at significantly greater risk of losing their data by opening an infected e-mail attachment or visiting an untrustworthy Web page. DPI technologies are often deployed to identify and quarantine these types of attacks.

Moreover, and perhaps most importantly, it is not the goal of government agencies to go on fishing expeditions to “steal” private data. Rather, DPI enables users to take a narrowly focused, policy-centric approach to identifying specific malicious data traversing the network.

Government IT managers are getting ahead of the curve by creating policy-centric networks that effectively identify and neutralize potentially malicious threats before they have the chance to inflict harm. The challenge has been — and continues to be — how best to reconcile effective network policy and the goal of a secure common communications platform that supports secure data streaming to multiple locations. With DPI, Government IT managers can better protect the sensitive and critical data traversing their networks in today’s ever evolving IT environment.