

September 2008

# Deep Security

## DISA beefs up network security with deep packet inspection of IP transmissions.

BY CHERYL GERBER, MIT CORRESPONDENT

For the largest military network stretching across the globe, carrying diverse types and levels of traffic, security is a constant challenge that cannot be resolved with superficial or piecemeal technology. Enter deep packet inspection (DPI), which provides scrutiny of actual content in Internet Protocol transmissions.

“Deep packet inspection and analysis have always been the most sought-after capabilities by network defense analysts that monitor our networks, as they provide the ability to drill further into

In contrast to shallow or plain packet inspection, which only checks the metadata (data about data) or the header of a packet as it passes through a network inspection point, DPI significantly deepens and strengthens network security by examining the payload, the actual data beneath the header, for hidden viruses, intrusions, spam or noncompliance with security policy. As recently adopted by DISA, it represents a significant security enhancement for the Defense Information Systems Network (DISN).

transmit voice data in dedicated, point-to-point connections with entire messages following the same path.

In packet-switched networks, the data is broken up into formatted chunks or packets, each of which contains the IP address of the source and destination in a header and each taking a different path, reassembling at its destination. Circuit switching has been more reliable and expensive, while packet-switching has been more flexible.

A chief concern of global wide area networks using packet-switched networks, such as the DISN and worldwide telecommunications carriers, is achieving balance between reliability, security, flexibility and scalability. Relative to other networks, it has been the extreme requirement of the widest area global networks that has been hard to fulfill.

“Many solutions don’t always scale well given the extremes of DoD. They often have difficulty providing either physical interface diversity or allowing the integration of multiple software capabilities. And all these factors must fit within an environment that places reliability of service at the top of the list,” said McAllister.

---

**“Bivio Networks has a unique ability to share the same network stream of data with multiple processors that can be leveraged to run multiple applications.”**

**– Sean McAllister, DISA**

---

the packet data,” said Sean McAllister, chief of the Sensor Grid Branch, Information Assurance, Network Operations Program Executive Office at the Defense Information Systems Agency (DISA).

While most high-capacity networks today are packet-switched, rather than circuit-switched, the difference between the two lies in how data is sent. The legacy public switched telephone network uses circuit switching to

## Sensor Platform

DPI technology developments have come closer to meeting these requirements. A number of companies have released DPI products that illustrate the advancements, including Bivio Networks, IBM Cloudshield and Allot Communications. DISA chose to deploy the Bivio Networks' 2000 network appliance as its multi-functional sensor platform, on which DISA is leveraging Bivio's execution of the Linux operating system and aggregating several network defense efforts on one appliance.

"Bivio Networks has a unique ability to share the same network stream of data with multiple processors that can be leveraged to run multiple applications. They also supply a familiar and flexible Linux operating environment, which provides our analysts and developers the ability to extend the sensing framework," McAllister said. In addition to achieving deeper security by using DPI, DISA has utilized the Bivio solution to resolve other DPI platform concerns. "Basically Bivio addresses all three aspects of a DPI platform. We can do more than one thing with the same stream of network traffic, which address scalability. We can port all our current tools and applications within a familiar Linux environment, lending itself to flexibility, and it is being used as the DPI engine within several currently successful commercial solutions today, which hits the reliability factor," he said.

Captain Jeff Jaime was on the ground floor in 2006 when DISA was deciding how to implement DPI. He was the program manager/technical director for engineering and deployment of the Centaur program at the Joint Task Force-Global Network Operations (JTFGNO), working with DISA on network security.

"We collected massive amounts of flow records for the Centaur program. It was an average of 10 billion flow records per day in 2006 when I was running the program before I retired," said Jaime, who is now a network security consultant with Bivio Networks.

The solution in use at the time was not keeping up with changes in the network traffic rate. "We had a homegrown solution that we had pieced together, a sensor we deployed on different circuits on the networks. As traffic rates grew, we were starting to drop network traffic we did not want to drop. We wanted to process more than one software application on that platform, but whenever we added software, it would degrade the traffic performance on the sensing platform," said Jaime.

Interim quick fixes to the problem turned into piecemeal solutions that added unwanted complexity. "One sensor per application is the traditional way people do network security. Anti-virus, intrusion detection and intrusion prevention were all required, different pieces of software and hardware and each required its own sensor," he said.

JTF-GNO and DISA then questioned whether to build or buy a solution, and during that process decided to use the Bivio technology. "The Bivio 2000 appliance aggregates multiple Linux servers into one platform on one piece of hardware with separate servers inside of it. When you install software on one of the CPUs in the platform, it has no knowledge of another. The way it is physically organized, it's flexible so you can also load-balance the processing and run multiple applications across one processor or multiple processors. That flexibility is a key factor in why we chose to use Bivio," he said.

An often overlooked problem is the assumption that there is sufficient power available. "The world is not created equal with respect to power and space, so when you can get this computing power at lower voltage rates, then it can apply worldwide regardless of the availability of power," he added.

Tim Waters, vice president of marketing for Bivio Networks, noted the applicability of next generation DPI platforms throughout the federal government as well as other commercial market segments. "We have found that DISA's networking challenges are consistent with those across several other federal agencies. This includes the need for high speed networking coupled with high performance computing capabilities for information assurance and security purposes. That's why next generation DPI network appliance platforms will become commonplace throughout intelligence, DoD and civilian agencies."

## Functional Consolidation

Other companies also have seen the advantage of running DPI in single system consolidating multiple functions. IBM's BladeCenter family integrates servers, networking and storage in a single chassis, sharing processors, memory and I/O. The company teamed up with Cloudshield Technologies earlier this year to implement Cloudshield's DPI architecture as a telecommunications carrier-class blade in the IBM BladeCenter that will secure and manage IP networks.

The IBM BladeCenter and Cloudshield infrastructure currently under development aims to address the growing convergence of telecommunications and information technology and of voice, data and video on networks that are

also increasingly carrying voice over IP or IPTV services.

The Cloudshield blade is being programmed in a rapid application development environment using Blade Server-based specifications for building compatible blades, network and storage switches, as well as blade adaptor cards. IBM BladeCenter servers run on Intel, AMD and IBM processors. Themis Computer is also building a Sun Microsystems UltraSPARC processor blade to run in BladeCenter.

IBM BladeCenter comprises five chassis options with two targeted specifically for global telecommunications carriers, as they meet the Network Equipment-Building System standards. "The blades and switches are interchangeable among all five," said Paul Nordlund, business development manager, IBM Next Generation Networking.

"IBM will resell the Cloudshield blade as the IBM PN41. We are doing a purchase complete of the assembly from Cloudshield, and will sell it as a full-fledged IBM BladeCenter product. People have built specialized applications on the Cloudshield platform and tested them on the PN41, and it works in IBM beta so there's forward compatibility for Cloudshield customers," said Nordlund. IBM and Cloudshield also point to a small footprint, with BladeCenter measuring at 50 percent less floor space and 35 percent less energy usage than other solutions. "The military is faced with the same dynamics as large commercial concerns. They are running out of physical space as the demand is growing for more users on the network," noted Bruce Gilley, vice president of federal operations for Cloudshield.

### Bandwidth Needs

Allot Communications also has a single chassis solution consolidating multiple functions in order to save on power, space and operating costs. The company's two DPI product lines are based on how much bandwidth users

DPI allows network administrators to understand the applications that drive the need for network capacity upgrade and control, such as peak usage. The technology provides an ability to classify the growing complexity of applications on the network. As applications began

---

## DPI significantly deepens and strengthens network security... As recently adopted by DISA, it represents a significant security enhancement for the Defense Information Systems Network (DISN).

---

need. The higher end product is called the Service Gateway, running from 5 to 25 Gigabits, with technology in development that will eventually scale up to 250 Gigabits. Allot distinguishes its telecommunications-oriented market position by using the standard Advanced Telecommunications Chassis Architecture developed by Motorola, Intel and others.

"Other vendors' blades can run inside the same Service Gateway chassis, so it is not just an Allot-only chassis," said Cam Cullen, Allot director of product development for the Americas. Allot views DPI as an enabling technology from several perspectives. One of the chief justifications is cost savings. Because DPI provides a deeper look at a packet, it is not necessary to lose efficiency by having to look twice at a suspected packet. "You only want to look at a packet once in a network if possible. DPI looks at the details of a packet, so you only need to look once," said Cullen.

using common transport systems, they became more difficult to distinguish. Without DPI, all traffic on the network could look like Web traffic with no way to tell it apart. "The rise in the use of video and peer-to-peer technology has caused a subsequent rise in the use of DPI. For example, Juiced is a video application that uses peer-to-peer technology rather than a streaming Web application like YouTube," said Cullen. "It requires DPI to distinguish between the two."

The rising need for user management has also caused the growth of DPI. "Controlling cost and bandwidth use on networks is a main driver behind the rise of DPI. You might want to do quota management and limit users to 100 Gigabytes of download per month, for instance," Cullen said.

"By giving deeper visibility into application and bandwidth usage, network administrators can guarantee bandwidth for mission critical applications and postpone network

upgrades. You don't need to upgrade bandwidth capacity as quickly by guaranteeing bandwidth for mission critical applications," he continued. One common mistake is to add bandwidth continuously to fix jams. "When they see network congestion, network administrators just keep buying more bandwidth and as they do, users will keep using it," he said.

DPI is sometimes confused with network monitoring technology, but it is not the same. "DPI provides more application visibility than most network monitoring products. DPI tells you what application constitutes the high usage, not just when and where the high usage occurred," Cullen pointed out.

"A lot of security products do just packet inspection but do not do deep packet inspection. For example, they would not be able to tell when Skype was present. Skype is an international instant messaging application with voice, chat and video that uses Web protocols to connect to another user. If a product can tell whether Skype was present rather than just Web protocols, then it has some level of DPI," he said.

#### **Privacy Issue**

Privacy is one potential sticking point with DPI that has yet to be resolved. With its ability to read the actual content inside a packet, DPI could cause a loss of privacy and network neutrality. "Applications that take advantage of DPI can potentially reveal private information. Typically, the organization that deploys the DPI application would also have some sort of cryptographic function in place—like Secure Sockets—to protect against privacy concerns. Protecting privacy will be handled by policy, which is enforced by the organization," said Jaime.

Most network professionals believe the privacy matter ought to be handled individually. "How to preserve or not preserve privacy is something that needs to be handled on a case-by-case basis. I'm not of the opinion that there should be one general rule of thumb that says that in all cases preservation of privacy is relevant or not. I believe that privacy tradeoffs should be made in the context of a comprehensive risk assessment that evaluates all security parameters in play and provides the guidance necessary for answering the privacy question," said Mauricio Sanchez, chief architect of Hewlett Packard ProCurve. Most networking professionals want to see DPI installed within the network and regarded as standard. "Unquestionably it makes the most sense to deploy DPI as a native feature of intelligent networking equipment," said Sanchez.

DISA concurs. "As DPI technology evolves, there will come a time when a network security/monitoring device is inserted with the network to provide the network defense community the data and information required for their analysts, and be as commonplace as our routers and switches are today," said McAllister.