



January 2009

Securing Carrier Networks

BY RICHARD "ZIPPY" GRIGONIS

In the Enterprise Network Management article elsewhere in this issue, Yours Truly comments on how businesses are trying to get a handle on what's happening in their network with centralized tools that can help them easily visualize, monitor and troubleshoot network phenomena, both mundane and mysterious. Similarly, carriers and service providers strive for the same utopian state of affairs, except that their networks are orders of magnitude larger and complex than those of other organizations.

One player that stands out is Arbor Networks, which supplies secure service control solutions to over 70 percent of the world's ISPs and many large enterprises. Network-wide visibility is their forte, and they're known for their highly regarded network security, traffic management, network monitoring, bandwidth management and broadband service optimization. Their solutions also help providers create differentiated services that can increase revenue and profitability. By employing flow-based and Deep Packet Inspection (DPI) technologies, Arbor solutions can manage and protect entire networks - from the network core to the broadband edge.

Deep, Deeper, Deepest...

Deep Packet Inspection (DPI) is an interesting technology that has skyrocketed in importance in recent years, primarily because it combines the functionality of an Intrusion Detection System (IDS) and

an Intrusion Prevention System (IPS) with a traditional stateful firewall. This amalgamation makes it possible to detect certain kinds of attacks that neither the IDS/IPS nor the stateful firewall can catch individually.

Radware, a leader in integrated application delivery and application security solutions for networks of all sizes, offers

and service floods to safeguard network resources and services in real time, without affecting legitimate traffic or impacting service performance.

Radware can supply DPI/DFI-based infrastructure DoS/DDoS protection at the carrier perimeter/peering edge. Their DefensePro product operates at multi-gigabit speeds as a remarkably trans-

DPI underlies services that span from security to subscriber management, information assurance [and] traffic management. It's a unifying capability.

DPI/DFI security based on their innovative network behavioral analysis technology capable of detecting ("zero-touch") and mitigating all types of known and unknown ("zero-minute") network IPS/DoS and DDoS floods. The network behavioral analysis module monitors network-wide behaviors, establishing the traffic and service baselines needed to immediately identify anomalies and potential service attacks. Utilizing advanced statistics, fuzzy logic and adaptive, self-learning feedback mechanisms, this behavioral network analysis module automatically and proactively blocks high-volume self-propagating worms

parent in-line device, in the process affording complete visibility, blocking and rate limiting of all ingress attack traffic, thus extending a first line of defense at the point of entry to the carrier core. By cleansing ("coarse grain granularity") carrier networks from all mass-volume attacks at the peering edge, DefensePro prevents attacks from ever impacting the carrier network or subscribers.

DefensePro's attack signature IPS protection, DoS prevention, worm propagation mitigation and anti-scanning, secure against known and unknown server exploits and application vulnerabilities.

As mentioned above, DefensePro's advanced behavioral IPS/DoS technologies detect and deliver zero-minute mitigation of service and resource abuses – including DNS query floods, spoofed Syn attacks, BOTs (HTTP and SIP) detection and mitigation, providing fine-grained detection capabilities.

To bolster their DPI, the previously-mentioned Arbor Networks has partnered with Bivio Networks, a specialist in the field.

plication and then engaging the markets. We have a broad sales model – we have OEM relationships with companies such as Sourcefire and Arbor Networks that use our products either in terms of intrusion detection as in the case of Sourcefire, or the DDoS threat mitigation system for carriers in the case of Arbor. We sell through the channel to the federal government a variety of information assurance applications. Some of our deals are visible and public such as our announcement with Defense Information

ments. That necessarily creates the demand for a different type of infrastructure, and that's the set of products that we offer. The boxes that we sell are in appliance form. We have a variety of different 'flavors', from 1 gigabit per second [Gbps] all the way up to 10 gigabits per second and beyond. We have scaling capabilities where you can scale both the compute dimension and throughput dimension. All-in-all it makes for a very interesting platform on which companies and customers can develop applications. On the one hand, we offer a high-speed networking device, on the other hand, it has a Linux development and execution environment that looks very much like a server and so it's the best of both worlds from a technical standpoint."

We see DPI as the fundamental networking technology of the future that underlies networking services, much in the same way that switching and routing evolved 15 or so years ago.

Bivio's CEO, Elan Amir, says, "We've been around since 2000. We've been on the product path of Deep Packet Inspection [DPI] since about 2004. Bivio has in effect built a DPI networking element. The reason for that is that we see DPI as perhaps the fundamental networking technology of the future that underlies networking services, much in the same way that switching and routing evolved 15 or so years ago. Now, DPI underlies many services that span everything from security to subscriber management on the carrier side to information assurance, to traffic management. It's a unifying capability. So, about five years ago Bivio felt the time was right to devise a new type of networking element that would focus on the requirements of DPI without actually perusing a specific ap-

plication and then engaging the markets. We have a broad sales model – we have OEM relationships with companies such as Sourcefire and Arbor Networks that use our products either in terms of intrusion detection as in the case of Sourcefire, or the DDoS threat mitigation system for carriers in the case of Arbor. We sell through the channel to the federal government a variety of information assurance applications. Some of our deals are visible and public such as our announcement with Defense Information

Systems Agency [DISA] that we are the security platform of the future for the Department of Defense [DoD], and some of our deals are classified."

"We also sell to service providers that use our products for the development of next-generation service delivery and next-gen gateways," says Amir. "Again, the unifying technology that underlies of these applications is deep packet inspection and the characteristics of those applications are very different than traditional networking applications that were either low-throughput and high compute in nature, or else high throughput and relatively low compute. As it happens, DPI applications are characterized by a combination of both high throughput and high compute require-

Bivio's top-of-the-line 7000 Series of Network Appliance Platforms is a family of compact, high-performance, fully programmable network appliances that combine Bivio's packet processing hardware architecture with a software platform that includes a standard Linux-based execution environment and a comprehensive set of networking features. Designed specifically to provide super-fast, wire speed deep packet processing, the Bivio 7000 Series architecture fuses Network Processing components with Application Processing CPUs in an effort to deliver both high performance and enhanced flexibility. The platform family includes two main product groups that provide performance optimized features to deliver true line rate packet processing from 3 Gbps through 10 Gbps throughput.

"As for carrier security, we tend to touch that area through our partnership with Arbor Networks, which is the leader in that area," says Amir. "Also, we encour-

The value to organizations is that, [from the] inside, you only see what's coming into your organization and you don't necessarily have the ability to cross-correlate that information with what's going on in the network in general. [With DPI], service providers can cross-correlate a lot of traffic that is traversing multiple organizations [to] complement internal security technologies.

ter it in some projects that we've done with service providers around the world. Many of these are not publicly known, but they do suggest some trends. First, in their ever-continuing quest for adding value on top of sheer connectivity, carriers look at security as an area for added value and the ability to increase their ARPU, increase customer stickiness and lower churn, and all of those great things that make their business model work. They have focused in the area that's collectively called 'clean pipes' – that's obviously the broad term for trying to remove everything that's bad on the service provider pipe. Our partnership with Arbor certainly does that. Some of our partnerships in Asia have used our boxes to try and determine appropriate access based on the billing conditions and/or security conditions in the network, with the ultimate objective being that everything that flows on the network should only be authorized and approved either on a subscriber level, at a traffic level, at a payload level, compared either against security databases or subscriber databases. At the end of the day,

it's all the same. The value ultimately is to the end user, because he or she is now guaranteed that the integrity of the pipe is maintained."

"In the federal space and in vertically-oriented service providers, you tend to see a lot of emphasis on 'sensing' and just trying to be aware of what exactly is running on the network – not for any nefarious reasons that make headlines, but for just for maintaining general network integrity," says Amir. "Networks are the backbone of many organizations and being able to know what's running on the network is important, because you can correlate that information with potential threats."

"Overall, the service providers have a role to play in all of this, because they have a unique vantage point where they can cross-correlate many activities across many organizations," says Amir. "The value to organizations is that, when you're sitting inside of an organization, you only see what's coming into your organization and you don't necessarily

have the ability to cross-correlate that information with what's going on in the network in general. The service providers can't really help you with what's going on inside your organization, but on the other hand, they can cross-correlate a lot of traffic that is traversing multiple organizations and therefore they can complement the internal security technologies. We tend to see movement in that direction quite a bit."