

cPacket Networks
2061 Landings Drive
Mountain View, CA 94043
www.cpacket.com

For more press information contact:
Abigail Johnson/Paul Michelson
Roeder-Johnson Corporation
(650) 802-1850
<http://email.roeder-johnson.com>

For more customer information contact:
cPacket Networks
Mountain View, CA
+1 (650) 969-9500 FAX: +1 (650) 969-4900
info@cpacket.com

CPACKET'S 10 GIGABIT CFLOW APPLIANCE BENEFITS HIGH-PERFORMANCE NETWORK INTRUSION DETECTION SYSTEM AT LAWRENCE BERKELEY NATIONAL LABS

1U Box Frontends First Scalable, Stateful NIDS on Commodity PC Cluster

MOUNTAIN VIEW, CA - OCTOBER 15, 2008 - cPacket Networks revealed today that their previously-unannounced cFlow appliance is serving as the load-balancing frontend to a powerful, high-speed network intrusion detection system (NIDS) implemented at Lawrence Berkeley National Laboratory (Berkeley Lab), that uses clusters of commodity hardware for analysis. The cFlow splits a heterogeneous packet stream of 10 gigabits per second into multiple, load-balanced subsets that meet specific criteria - for example, all the interrelated packets of specific HTTP sessions - and redirects each such subset to a different destination in the cluster.

In the Lawrence Berkeley National Laboratory intrusion detection system, each such subset is redirected to one of the inexpensive commodity PCs in a cluster, which performs security analysis using an open-source analysis engine. The PCs communicate with a management PC to provide the fine-grained correlation necessary for high-quality operational security. The system is inherently scalable, easy to maintain, and can be made extremely fault tolerant with simple hot backups.

"The processing required to provide effective network intrusion detection for even a single gigabit traffic stream is far beyond the reach of single workstations, and it's only getting worse," said Berkeley Lab spokesperson Robin Sommer, one of the co-architects of the system. "We realized that just as large clusters of ordinary personal computers are routinely applied to solve computationally profound problems, a similar approach would work extremely well for intrusion detection. A key challenge, however, was to figure out how to balance the workload across the workstations in the cluster."

Berkeley Lab spokesperson Anne Hutton added that the Lab's team experimented with several approaches for distributing the traffic, including pure software, and specialized hardware.

"The software - a Linux application - worked, but didn't have the desired performance," said Hutton. "A second approach, using a custom-programmed hardware appliance, allowed the team to validate the concept and publish the research findings [see endnotes for reference]. Ultimately, however, we collaborated with the cPacket team to develop the cFlow solution, which delivers a load balancing frontend at full 10G line rate and is more versatile and easier to use for flow load balancing than other approaches."

"The cFlow hardware can be passively inserted like a "bump in the wire" into 10G links" said Rony Kay, president of cPacket. "We partition the traffic workload to multiple target machines in the cluster, such that each machine can process a subset of the traffic independently." According to Kay, the cFlow features two 10G fiber ports for "data in" and "data out", and an additional out-of-band management port.

"Provisioning is easy," Kay added. "The user can specify from a Web browser what traffic or protocols go to which target machines. It's that simple. And, if any machine in the cluster suddenly goes off

line, it is easy to redirect the traffic to a designated hot standby, or to rebalance the traffic over the remaining active resources."

The cFlow is packaged in a 1U rack-mount enclosure. Its internal processing engine is based on a unique cPacket "complete packet inspection" chip that can deliver 100% header and payload inspection at line speeds of 20 gigabits per second.

In addition to applications like the network intrusion detection system described above, Kay reports that the cFlow easily supports a number of other use cases. "For example," said Kay, "users can implement high speed NetFlow probes for 10Gbps traffic by leveraging several commodity PCs - without the need for specialized and expensive custom appliances. It can also be used in server farms for workload balancing over multiple server instances."

Similar to its other announced network hardware, cPacket conceives of the cFlow as a "production reference design". For certain landmark customers such as Berkeley Labs' high-profile NIDS project, the company will sell the box as a turnkey product. However, the bulk of the cFlow sales will be through cPacket's OEM partners who will private label the product.

The network at the Lawrence Berkeley National Laboratory consists of several thousand users and hosts connected to the Internet via a 10 gigabit per second link. The cFlow acts as the front end to the NIDS, classifying the packets into related flows and forwarding them to a cluster of approximately ten 3.6GHz dual-CPU Intel Pentium D commodity PCs for analysis.

"What the NIDS project team has achieved is extraordinary," concluded Kay. "They have added a layer of flexible, scalable, and easily-maintained flow balancing to support the operational security of an extremely sensitive, but highly trafficked network - with a minimum of complexity and cost. We are proud to play a key role."

The NIDS project team included researchers from Berkeley Lab, the International Computer Science Institute, and the Technical University Munich.

About cPacket

cPacket Networks is an emerging leader in chips and technologies that offers breakthrough, "complete" packet inspection at 10 gigabits per second or better, at a fraction of the complexity, power, or cost of preexisting approaches. It provides manufacturers of routers, switches and other network appliances a low-impact means to easily drop game-changing, wire-speed active network traffic analysis and response directly into their existing or planned designs - whether targeted at the service providers, the enterprise, or the small office. cPacket supports both these manufacturers and the market with production-class reference designs such as the cTap and cFlow that can be deployed as is, licensed for private-label distribution, or provide OEMs with a complete proof of concept for their own industry-leading designs based upon cPacket chips.

The exploding use of networks for media-centric applications makes the availability of truly pervasive deep packet inspection timely and crucial.

cPacket was founded in 2003 and is located in Mountain View, CA. For more information, visit www.cpacket.com.

Editors, note: All trademarks and registered trademarks are those of their respective companies.

Additional background information is available at www.roeder-johnson.com.

See also: [*"The NIDS Cluster: Scalable, Stateful Network Intrusion Detection on Commodity Hardware"*](#), M. Vallentin, R. Sommer, J. Lee, C. Leres, V. Paxson, and B. Tierney, *Proceedings of RAID 2007*.