



# REVIEW: Crossbeam X-Series Platform Consolidates Security Functions

By: Matthew Sarrel

Every enterprise network is built on a switched Ethernet foundation. It's difficult to estimate just how many Ethernet switches are out there, but, according to Infonetics Research, devices worth \$3.4 billion were shipped in Q2 2009.

If any piece of network gear might be as widely deployed as the Ethernet switch it would be the firewall. And, as network usage evolves, enterprises must add more and more security devices and/or software solutions. Not only do these solutions need to be individually configured, managed and patched, but they take up space, use energy and generate heat in the data center.

The Crossbeam X-Series Platform is a modular Ethernet switch targeted at the enterprise and carrier market. The versatile, scalable and high-performance architecture can be thought of as a fully customizable combination of a UTM (unified threat management) device running on top of an Ethernet switch.

However, unlike most UTM devices, the Crossbeam X-Series Platform allows you to select best-of-breed security applications to deploy. Partners—currently including Checkpoint, IBM, Imperva, Sourcefire, Trend Micro and Websense—provide software ranging from firewall to anti-malware to URL filtering to IPS (intrusion prevention system). Such versatility contributes to data center consolidation by removing the need to rack, connect, power and manage a multitude of point solutions.

The X-Series consists of the seven-slot, 8U X45 chassis or the 14-slot, 14U X80 chassis. The backplane of the chassis itself is a 160G-bps nonblocking switch fabric.

Both the X45 and X80 models can be populated with a mix of APMs (Application Processor Modules), NPMs (Network Processor Modules) and CPMs (Control Processor Modules).

Each NPM has a 10G-bps full-duplex point-to-point con-

nection to each APM, CPM and the other NPMs. Each APM can receive up to 12G bps of network traffic, while all signaling and management information travels through a dedicated 1G-bps control path to the CPM.

Units can be configured for “single-box high availability” using redundant modules or “dual-box high availability” using redundant chassis.

NPMs are available in a variety of configurations (1G-bps Ethernet, 10G-bps Ethernet, copper and fiber), and include an integrated 16-core MIPS64 security processor, a high-speed NPU and a Crossbeam-designed switch fabric FPGA.

APMs, also available in a variety of configurations, are essentially a PC on a card complete with multiple dual-core Xeon processors, up to 4GB of RAM and up to two hard drives, plus an FPGA. The FPGA on the NPM and the FPGA on the APM build a virtual meshed network through which network traffic flows.

APMs run security applications—in my case, Checkpoint R70—on a hardened version of Red Hat. APMs can be load-balanced for performance and failover, and are hot-swappable. During testing, I yanked an APM out of the chassis and the box didn't miss a beat.

Finally, the CPMs then manage all components of the solution. If, for some reason, an APM crashes, it will reboot and the CPM will redeploy the security application automatically.

## Not for the Faint of Heart

I tested the Crossbeam X80 equipped with eight APMs, four NPMs (Model 8650) and one CPM—a configuration that lists for roughly \$500,000.

One thing that must be mentioned is that this is a serious piece of enterprise security equipment. Installation, configuration and management are not for the faint of heart; no one is going to simply sit down and wing it. The CLI is about as user-friendly as any CLI can be, with auto-complete and the

ability to enter multiple commands at once. The system also offers a browser-based GUI, but at the current time it is little more than a reporting tool.

Crossbeam gave me a sneak peek at the next generation of the GUI, and while I can't say much about it, I can say that it will be much more powerful and easier to use than the GUI that's currently available. Crossbeam does provide excellent best-practices guides on its technical support Website, but, frankly, this is such a sophisticated and powerful piece of security equipment that anyone who isn't comfortable with a CLI probably shouldn't deploy it to begin with.

Installation begins by connecting to the X80 using a serial cable, then logging in and launching the CLI-based wizard. Configurations can be saved as text files and then uploaded via SSH, which accelerates deployments involving multiple units.

First, VAP (virtual application) groups get set up, then applications (in my case, Checkpoint R70) get deployed to the VAPs. From that point forward, the security applications can be managed with their own GUIs, while hardware components are managed via the CLI.

Alerting capabilities are very good and include support for SNMP versions 1, 2 and 3, with automatically defined thresholds for parameters such as CPU, hard drive and memory utilization, as well as NPM and APM status. The CPM monitors the X80 chassis and all components with a breath-of-life heartbeat, and can issue alerts based on that status.

There is also full support for system logging via syslog and RMON. Hardware alerts are indicated by lights on the front of the chassis and are color-coded for critical, major and minor incidents. Minimal reporting is available through the GUI.

Performance is where the X80 really stood out. We used

Spirent TestCenter to generate stateless UDP traffic with a 64-byte payload. With two NPMs and four APMs, I pushed 19.4G bps of traffic through the X80; with four NPMs and one APM, I saturated our equipment with a full 40G bps. Interestingly, as we added APMs, UDP packet pushing performance declined. This makes sense because the NPMs can handle stateless traffic by themselves, and, in this case, the overhead of packet inspection using the APMs was unnecessary.

I then used a BreakingPoint Elite to generate both stateful HTTP and attack traffic against the X80 with four NPMs and four APMs running the Checkpoint R70 firewall and IPS. Attack traffic consisted of roughly 1 percent to 2 percent of all traffic during each test, while the average HTTP packet carried a 900-byte payload and the average attack packet carried a 684-byte payload.

The BreakingPoint Elite is capable of generating up to 40G bps of a realistic blend of application traffic and more than 4,200 different security attacks in a single three-slot chassis. Running only Checkpoint R70 firewall we processed 20G bps; with Checkpoint R70's firewall and the "default" IPS policy we processed 20G bps while only using three APMs. Using Checkpoint R70's "recommended" firewall policy, which more closely resembles real-world conditions than the default, and eight APMs we processed 18G bps.

Failover response was likewise excellent. Using four NPMs and eight APMs, we had the X80 processing 200,000 HTTP connections per second. We shut down one NPM, and traffic dropped to 180,000 connections per second for a little over a second and then quickly bounced back to the original 200,000. After enabling that NPM, we shut down an APM, and there was no detectable performance degradation.

*Matthew D. Sarrel is executive director of Sarrel Group, an IT test lab, editorial services and consulting company in New York.*



80 Central Street  
Boxborough, MA. 01719  
1-978-318-7500  
www.crossbeam.com