IBM Proventia Network Intrusion Prevention System With Crossbeam® X80 Platform

September 2008

OPUS ONE

Executive Summary

The objective of this report is to provide performance guidance for IBM's Proventia Network Intrusion Prevention System 2.0 (IPS) for Crossbeam running on the Crossbeam X-Series Next Generation Security Platform with XOS 8.1 software. Opus One conducted performance tests with and without attack traffic as part of the overall traffic mix. The goal of these tests was to determine the performance of the IBM Proventia for Crossbeam solution under conditions simulating real world traffic mixes.

In unburdened tests with UDP traffic, a fully populated Crossbeam X80 platform returned performance of nearly 40 Gbit/sec with no traffic lost and full inspection capability.

The same Crossbeam X80 configuration exhibited near-linear scalability in IPS performance using a typical Internet mix of traffic, including a substantial level of attack traffic. Our tests indicate that a Crossbeam X80 platform would handle "real-world" traffic of approximately 15.2 Gbit/sec while maintaining full "N+1" redundancy. A fully populated platform without internal redundancy could support a load of up to 18.9 Gbit/second with zero traffic loss and no reduction in protection.

Based on this validated performance, the IBM Proventia for Crossbeam IPS solution has proven itself to be capable of handling very high traffic and attack loads not just at an Internet boundary but deep in the core of both enterprise and service provider networks.

Testing "Real World" Performance

We tested the IBM Proventia for Crossbeam IPS solution using equipment from Spirent, including their L4-7 test application (commonly called Avalanche/Reflector) and Spirent Test Center test application, and from Mu Dynamics, including their Mu-4000 test tool. Opus One was solely responsible for building and evaluating the test configuration, test plans, and for performing the tests and recording results.

Crossbeam and IBM staff members were available during the test process and were responsible for installation and configuration of all hardware and software. Opus One validated the configuration of both the IBM Proventia Network IPS software and Crossbeam X80 platform.

The overall goal of our IPS testing was to determine the worst case (highly stressed) performance of the IBM Proventia Network IPS software on Crossbeam hardware when "real world" network traffic supplemented with a high level of attack traffic was passing through the IPS. The performance tests were designed to determine how an IBM Proventia for Crossbeam IPS would operate in a real-world network and provide a safe lower performance bound for network engineers sizing systems.

Our first test focused on a traffic mix that would simulate typical Internet traffic. In earlier testing by Opus One for Network World, we had determined that the most stressful (highest CPU load) traffic to present to an IBM Proventia IPS is HTTP traffic. This is true of most all Intrusion Prevention Systems (IPS). Because of the high level of HTTP-based attacks, an IPS has to perform more analysis on HTTP traffic than any other protocol. HTTP also causes additional stress because of the relatively free-form nature of the protocol. To give a worst-case performance number, we used only HTTP traffic in our testing. Depending on where the IPS is located and in which type of network, the load we presented could represent normal traffic flow (such as at the edge of a service provider network) or could be more stressful than is normal (such as at the core of an enterprise network).

The HTTP traffic profile was based on measurements Opus One has taken at several enterprises and service providers of actual HTTP traffic. We loaded 10 different web objects (ranging in size from 1 Kbyte to 1.5 Mbyte) into the Spirent test equipment, including HTML (with embedded JavaScript), GIF and JPEG images, PDF files, ZIP archives, and Windows executable files. No viruses or spyware were in the objects. The test equipment was configured to deliver this actual content from web servers to web clients in a mix of sizes and object types to approximate the Internet HTTP traffic of an enterprise or service provider environment.

To provide additional stress on the IBM Proventia for Crossbeam IPS, and to more closely simulate real-world outside-the-firewall traffic, we added a mix of attack traffic to our HTTP traffic. To do this, we turned to the Mu Dynamics Mu-4000, an appliance-based security testing tool. We used the Mu-4000 to generate approximately 1200 attacks across a wide variety of protocols, and captured the attacks. Then, using the open source TCPReplay tool, we fed the attacks back at a high rate of speed to the IBM Proventia for Crossbeam IPS to create stress. In a typical configuration, the IPS

would be protected by a firewall and see only attacks on traffic let through into the enterprise. We were unable to find any research to uncover what percentage of traffic "inside the firewall" was attack traffic. However, several security researchers have proposed traffic loads from 1% to 3% as being typical levels of attack traffic seen on the open Internet. To provide an aggressive real world test, we supplemented the benign HTTP traffic with an additional 3% of attack traffic.

Finally, to complete the "real world" test, we established a subset of the 1200 attacks that we manually verified the Proventia Network IPS software would catch at a zero load. By transmitting those attacks using the Mu-4000 test tool, we could determine whether or not the IBM Proventia Network IPS software was missing attacks and letting malicious traffic through.[1]

Most network engineers have a goal of "zero loss" for their networks, so we defined a successful run as a steady state where three results were true:

- IBM Proventia Network IPS correctly processes all HTTP sessions without abnormally terminating any session
- IBM Proventia Network IPS continued to block the same set of attacks
- TCP latency introduced by the IPS was limited to 5 ms (round trip) or less

Using an iterative testing process, we determined an offered load that would meet this zero loss goal, and then verified the load and performance by running three separate tests of five minutes each. For each test run, we selected a constant area of three minutes within the test (after ramp-up and before ramp-down) and averaged throughput and latency values across all three tests to give our final results.

Overall, we feel that these test scenarios provide aggressive numbers for the performance of the IBM Proventia Network IPS solution on the Crossbeam X80 platform. We believe that security and network architects can use the results of these tests to size IPS solutions for real-world networks when deploying the IBM Proventia for Crossbeam IPS solution.

"Real World" Performance Test Results

Our testing provides two important results:

- the IBM Proventia Network IPS software loaded on Crossbeam X80 platform APMs has near linear scalability as the number of APMs is increased
- each Crossbeam APM running the IBM Proventia Network IPS software is capable of providing approximately 2 Gbit/second IPS protection on real world traffic, including attack traffic, without any loss or missed attacks**.**

[1] We defined a "miss" as an attack that was let through by the IPS software. We did not validate whether attacks at high rates were all logged by the SiteProtector management system.

Test Description	Number of APMs	Total HTTP Goodput[2]	Added Latency
Typical Internet HTTP traffic mix; attack traffic at 3% of total load; zero missed attacks; zero disrupted TCP sessions	1	2.01 Gbit/sec	0.64 msec
	2	3.75 Gbit/sec	0.79 msec
	3	5.78 Gbit/sec	2.56 msec

Table 1: Results of "Real World" testing

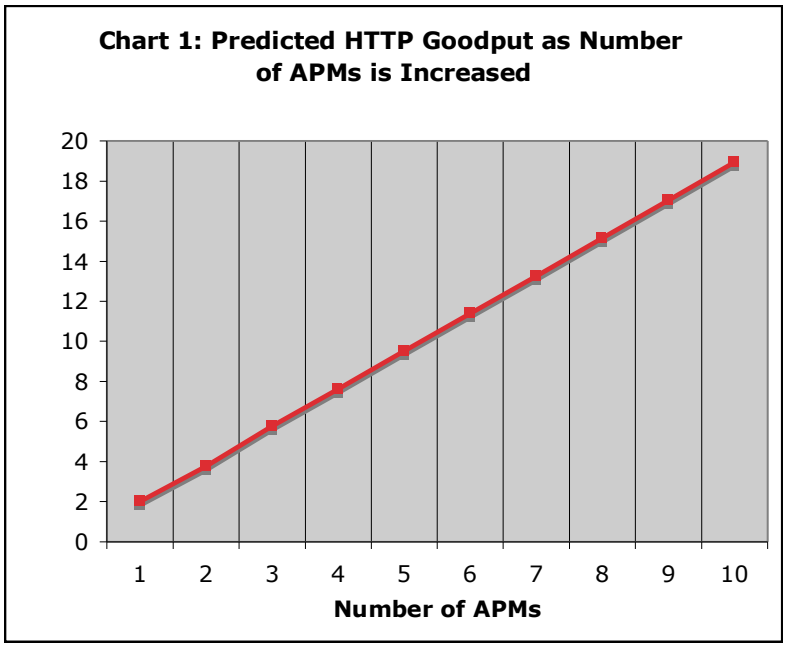
Due to the limitations in the Spirent test equipment we had available, we were unable to offer a load to the X80 platform above approximately 7.5 Gbit/second. This let us drive the Crossbeam X80 platform and IBM Proventia Network IPS software to the loss point only with 3 APMs or fewer. Table 1 shows the results of our real world testing.

In Chart 1, we used a least squares curve fitting to attempt to predict the HTTP goodput of the Crossbeam X80 platform for larger numbers of APMs than we were able to test.

We did discover a limitation in the integration of the Crossbeam XOS and IBM Proventia Network IPS worth mentioning. Under extreme volume of traffic used in this test, the IBM Proventia for Crossbeam IPS was unable to consistently send TCP RESET packets to tear down connections after an attack was blocked. However, as long as the attack traffic itself was blocked, we considered this a successful block by the IPS.[3]

[2] goodput is a term defined in RFC2647 and is used in measuring firewall performance. Defined as "The number of bits per unit of time forwarded to the correct destination interface of the DUT/SUT, minus any bits lost or retransmitted," it is the most appropriate term to use for a device such as an IPS (or firewall) sitting in the middle of an active TCP session.

[3] As a way to protect against certain attacks, the IPS included TCP session tear downs in addition to blocking the actual attack traffic. This is a common IPS strategy that helps to minimize the impact of attack traffic on servers. In our testing, we discovered that during periods of very high stress, the IBM Proventia IPS was unable to send TCP RESET packets (to tear down the session) because the buffer used to insert these packets into the data was overflowing due to the high rate of traffic load offered. Because the attack was still blocked, we did not consider this a significant security issue.



Testing Maximum Throughput Performance

A common measure of intrusion prevention systems is their raw performance when passing UDP traffic. This type of test can validate overall system performance by showing how the IPS will behave when passing traffic that does not stress the attack detection part of the IPS engine. In very high-speed IPS systems where a significant percentage of the traffic may be un-scanned or lightly scanned (such as file transfers between servers, database backups, encrypted traffic, voice traffic, or other "white listed" traffic), this test helps to validate the best case performance of an IPS. Our second suite of tests focused on throughput performance

We tested the Crossbeam X80 platform and IBM Proventia Network IPS by sending streams of UDP packets across multiple 10 Gigabit Ethernet interfaces. In our test, we used a single X80 chassis configuration with four NPMs (rated to a maximum throughput of 10 Gbps per NPM) and eight APMs running the IBM Proventia Network IPS software.

We ran four separate tests using the Spirent Test Center to generate the UDP packets with data from many source and destination IP addresses and a single destination port, UDP port 1025. In the first two tests, we sent UDP traffic using two different frame size profiles (see Table 2). We ran the tests until we saw data loss, or we reached maximum interface speed of 40 Gbps, whichever occurred first. The performance results reported for these tests are true zero-loss values.

Datagram Size	"Maximum Size" profile	"JMIX" profile
60 octets	0%	23%
120 octets	0%	31%
576 octets	0%	8%
1500 octets	100%	38%

Table 2: Composition, by Datagram Size, of UDP Traffic

In the second set of two tests focused on maximizing throughput, we combined the UDP traffic with 3% attack traffic, as in the "Real World" performance tests, to see how the IBM Proventia for Crossbeam IPS solution would perform when under a higher level of stress. In this case, we reported performance here with a loss rate of less than 1 frame in 10,000 transmitted frames.

Results of Maximum Throughput Performance Testing

In testing the Crossbeam X80 platform with the IBM Proventia Network IPS software, we were able to achieve a steady-state transfer rate at 99% of line speed (39.6 Gbit/second) across four 10 Gigabit Ethernet interfaces using four NPMs and eight APMs and a maximum size profile.

This very high level of IPS performance—essentially 40 Gbit/second—shows that the Crossbeam X80 platform combined with IBM's Proventia Network IPS is capable of handling very high traffic loads not just at an Internet boundary but deep in the core of both enterprise and service provider networks.

The full results of our testing appear in Table 3.

Traffic Profile	Throughput and Loss	Throughput and Loss (3% attack traffic)
Maximum Size UDP	39.6 Gbit/second; zero loss	30.0 Gbit/second; < 0.01% loss
JMIX UDP profile	32.4 Gbit/second; zero loss	27.6 Gbit/second; < 0.01% loss

Table 3: Results of Maximum Throughput Performance Testing

Summary of Results

Opus One's testing demonstrates three critical facts relevant to engineers and security architects incorporating IBM Proventia Network IPS for Crossbeam in enterprise and service provider networks:

- Real-world traffic, including attacks, can be inspected with zero loss, full IPS protection, and minimal additional latency at speeds of up to 1.9 Gbit/second per APM, or 18.9 Gbit/second for a fully populated Crossbeam X80 platform with 10 APMs.

- UDP traffic of various sizes and including attacks can be passed with very low loss and no drop in security at speeds between 27.6 Gbit/second and 30.0 Gbit/second for a Crossbeam X80 platform with four NPMs and eight APMs.

- UDP traffic at maximum size with no attacks, which might be typical of internal or core network traffic, can be passed with zero loss at 39.6 Gbit/second on a Crossbeam X80 platform with four NPMs and eight APMs.

These three facts validate that the IBM Proventia Network IPS for Crossbeam solution is fully capable of sitting in-line within enterprise and service provider networks under very heavy load and attack conditions.

About the IBM Proventia Network Intrusion Prevention System

IBM Proventia Network Intrusion Prevention System is an IPS designed for enterprise networks. When combined with IBM's Site Protector management system, Proventia intrusion prevention sensors can be linked together for centralized management and reporting, while maintaining a very high level of performance. The Proventia IPS detection engine and management system is available as a software-based solution, in dedicated appliances, and in conjunction with partners.

This test was conducted using IBM Proventia IPS for Crossbeam v2.0.

About Crossbeam Systems and the Crossbeam Next Generation Security Platform

Crossbeam Systems builds network security platforms. The flagship line is the **Crossbeam X-Series™** Security Services Platform, the largest of which is the Crossbeam X80™ platform, a 14-slot platform running the Crossbeam XOS™ network operating system with high availability, load balancing, dynamic routing, and package management built-in to the platform. The Crossbeam X80 platform can support up to 10 application processing modules (APMs), each of which can be dedicated to a particular security application, such as intrusion prevention or firewalling, or grouped together to run one application. In our IPS testing, all APMs were dedicated to the IBM intrusion prevention application.

Crossbeam, with their partner IBM, offers a platform-based solution for intrusion prevention that integrates IBM Proventia IPS technology with Crossbeam XOS™ software, load balancing, and application management tool. The end goal is a very high performance security appliance that can include multiple threat management functions, such as firewall, IPS, and other security applications, while maintaining very high levels of performance and reliability.

This test was conducted using Crossbeam XOS v8.1 software on a Crossbeam X80-AC-3 chassis using APM-8600, CPM-8600, and NPM-8600 modules.

About Opus One

Opus One is an information technology consultancy based in Tucson, Arizona. For more than 25 years, Opus One has worked with enterprise and service provider clients to help design and deploy of large scale secure networks and email. Opus One provides unbiased and expert product evaluation services to clients on five continents.