



White Paper

Testing High-Performance Mobile Firewalls for 4G-LTE Networks



Prepared by

Gabriel Brown
Senior Analyst, *Heavy Reading*
www.heavyreading.com

on behalf of



<http://www.Crossbeam.com>

January 2012

Introduction: Mobile Firewalls in LTE Networks

In December 2011, *Light Reading* commissioned the European Advanced Networking Test Center (EANTC) to complete a series of independent tests behalf of Crossbeam Systems and its new X80-S networking hardware platform running the XOS9.6 operating system and Check Point Security Gateway. The intent was to establish the scalability of Crossbeam's security products in mobile broadband networks with specific reference to Long Term Evolution (LTE).

Highlights & Key Findings

The Crossbeam X80-S product was shown to perform consistently in a bespoke test environment designed by EANTC to emulate real-world conditions. Using Spirent test equipment, the companies together set a new benchmark for high performance mobile firewall testing. Among the key findings:

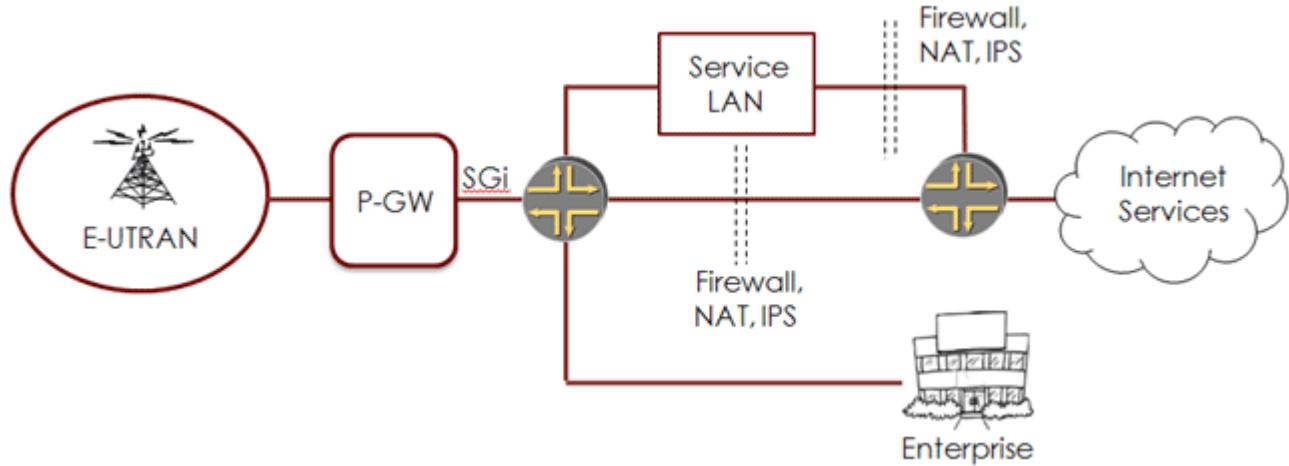
- **The Crossbeam X80-S Firewall was observed to support 106 Gbit/s of steady state throughput in a realistic load environment.** Using a stateful traffic model that emulates real-world usage this steady state performance was demonstrated over multiple test-runs and provides the first publicly available test data of a high-performance mobile firewall product from a trusted third-party.
- **106 Gbit/s of performance was maintained with NAT and IPS functions activated.** The Crossbeam/Check Point firewall was tested with the default Network Address Translation (NAT) and Intrusion Prevention System (IPS) switched-on and performance was not noticeably impacted. Although advanced NAT and IPS functions were not tested, this test provides a baseline against for any future tests by vendors and their test-houses.
- **Data-plane performance was demonstrated with a large number of active connections, high transaction rates and stable page load times.** During steady state the tests showed the X80-S supporting 1 million active users, 4 million active TCP connections and a setup rate of 250,000 new TCP connections per second. HTTP latency was between 30-50 milliseconds in the test environment inclusive of the handset- and server-induced latency.

Strategic Importance of SGi Interface

The Crossbeam firewall was tested at the SGi interface of an emulated mobile network. SGi is the interface that connects the LTE network to external networks, such as the Internet and corporate networks. It is similar to the Gi interface in 3G UMTS network and will ultimately replace Gi when operators move to a common core network based on the Evolved Packet Core (EPC).

The SGi "domain" is where operator networks connect to end-user services and is therefore critical. It is growing in importance as end-user performance expectations continue to increase, operator business models evolve and services become more sophisticated and interactive. The SGi interface provides connectivity into a complex environment. As shown in the diagram below, this includes the operator's Service LAN where its own services are hosted, a series of packet edge and border gateway routers (with various extra functions pre-integrated), virtual private network (VPN) connections to large enterprise customers, connections to the internet and to content delivery networks, and so on.

Figure 1: SGi Environment



Source: Heavy Reading

Because it exposes the internal network, security of the SGi interface is a primary concern to operators. Devices such as firewalls and intrusion prevention systems are critical. In the first instance, firewalls are used to protect the operator's own network elements and services, where the need is clear. Increasingly operators are also considering the role of firewall devices between their networks and the Internet to protect end-user traffic. This is more economically challenging due to high traffic volumes and will require higher-performance equipment with better cost per Gbit/s of processing capacity to continue to scale and meet demand.

The Rising Profile of Security in Mobile Networks

The mobile industry has a well-developed security framework that has evolved through generations of technology and has proven value. It is not coincidence that the world's first mass-market encryption device was the mobile phone. Industry bodies such as the 3GPP and the GSM Association maintain active programs to progress the industry as a whole in meeting changing security needs.

Operators themselves are keen to ensure they remain providers of secure communications services in the data era and to accrue the value that derives from this. In the *Light Reading* 2011 Security Benchmark Survey 85 percent of respondents said the proportion of their capital spending allocated to mobile network security would increase in 2011 and 2012 and 72 percent cited security as essential to their company's five-year network plan. The challenge, obviously, lies in the transition to data, both in the network hardware and in operational expertise.

A Real-World Test Scenario

In December 2011, EANTC carried out detailed testing of the Crossbeam X80-S at Crossbeam's lab facilities in Boxborough, MA. The tests were designed and managed by EANTC with support from test equipment supplier Spirent and from Crossbeam's own technical staff.

In discussion between Crossbeam, EANTC and *Heavy Reading* when defining the scope of the project, it was agreed the objective should be to create a test plan that would emulate real-world conditions as closely as possible within budget and time constraints. This is unusual for vendor-sponsored tests, which tend to focus on peak-rate performance across narrowly-defined criteria. It is a credit to Crossbeam that it was prepared to take the risk and have its new platform measured against an independently-created and executed test plan.

Performance Summary

The table below summarizes the measured forwarding performance of the Crossbeam X80-S product running at steady state for 15 minutes. Basic NAT and IPS functions were switched on, a large number of connections were created and closed-down during the test run, and a bespoke, stateful traffic model that emulated real users and usage patterns was used.

Figure 2: Measured Steady-State Performance of Crossbeam X80-S Firewall

METRIC	OBSERVED PERFORMANCE
Throughput	100 Gbit/s down; 5.5 G/bits up
Simultaneously active users	1 million
Active TCP connections	4 million
TCP connections / user	4:1 (average over steady state period)
New TCP connections / second	242,000
New users / second	42,000
CPU load	Network CPU 99%, Application CPU 60%
Duration of steady state	15 minutes
NAT	Switched on; 1:1 configuration
IPS	Switched on; Default configuration
Traffic Model	EANTC-developed profile for high-performance mobile firewall environment

Source: EANTC, Heavy Reading

In practice, the performance shown in the table above is the result of trial and error in attempting to determine the "sweet spot" for the X80-S. While the box can produce higher throughput and support more simultaneous users and connections per second, 106Gbit/s forwarding performance is the point where it can manage all the functions simultaneously without noticeable degradation in performance.

What This Means in Practice

Producing 106 Gbit/s of throughput is, by virtually any measure, very substantial and should be more than sufficient for a typical mobile installation. At 1 million active users, this allows 100 kbit/s of throughput per user – far greater than the average busy-hour throughput per user, which is rarely above 20 kbit/s in advanced networks, and often much lower. Of course, individual users will burst to higher rates, but they will also fall idle.

One million simultaneously active mobile data users would support an operator with 10 million data subscribers, assuming a 10 percent activity level at busy hour. Assuming 50 percent of an operator's subscribers are active data users, this would equate to an operator with something of the order of 20 million subscribers in total. In other words, in theory, this 106 Gbit/s of capacity should be enough to support virtually any European network or a major region of a North American network on a single chassis.

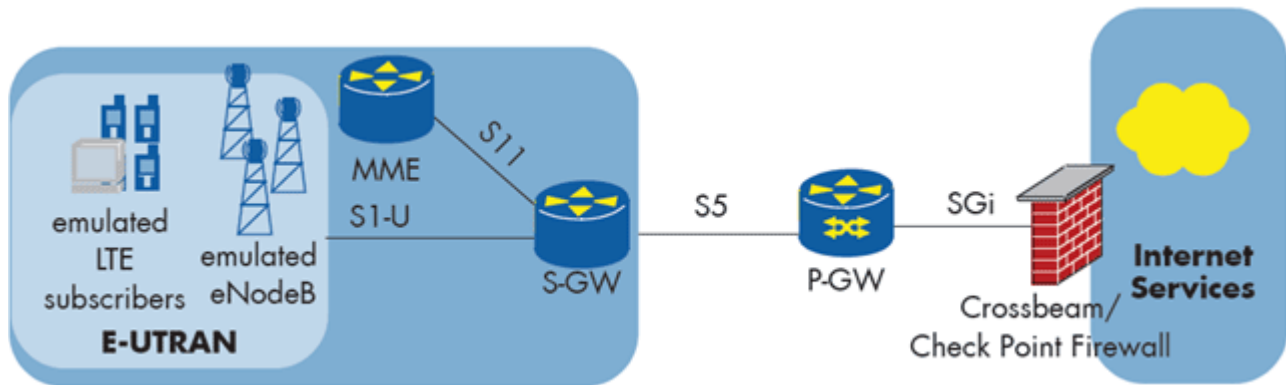
In reality, operators will not run equipment anything like this close to capacity, especially given the role firewalls play in protecting against attack. Typically 30 percent of capacity is an acceptable utilization level, so as to allow for failover and spikes in usage. Operators will also want to deploy multiple pieces of equipment in multiple locations for resiliency. This, of course, increases the number of chassis and firewall clusters that will be needed.

The conclusion, in *Heavy Reading's* view, is that the X80-S product provides more forwarding capacity per chassis than is needed for today's mobile broadband networks, as currently typically configured, and will be able to support ongoing growth in 3G and LTE traffic for the foreseeable future.

Discussion of Testing Criteria

The logical test setup is shown in the diagram below. Everything on either side of the firewall was emulated using Spirent Avalanche equipment.

Figure 3: Logical Network – Firewall Forwarding Performance



Source: EANTC

It is useful to briefly discuss some of the metrics highlighted in **Figure 3**, as this provides important context:

Simultaneously Active Users: This metric was set at 1 million during steady state. This number was selected partly on judgment and partly because it was within the known limits imposed by the total number of connections and the connection per second setup rate.

Active TCP Connections: The 4 million active connections were made up primarily of HTTP sessions (see below for more detail on traffic model).

TCP Connections Per User: The 4:1 ratio of connections per user represents an average figure for the duration of the test run. In reality, it fluctuated depending on the traffic type and the point in time that each connection was active. Each HTTP user, for example, had a peak of nine active TCP connections to represent a real-world Web browsing session.

New TCP Connections Per Second: This was the amount of new connections created per second during steady state (i.e., while the 4 million total connections were active). Existing sessions completed their tasks before being shut-down to allow new connections to be created.

New Users Per Second: This worked out at 42,000 per second which implies a 6:1 average ratio of new connections per new user at setup (242,000/42,000).

Duration of Steady State: Steady state was maintained for 15 minutes in each test run, which is long enough to establish confidence in the results. This represents industry best-practice versus the shorter test runs used by some other test houses. CPU load did not increase noticeably over time.

NAT Configuration: The firewall was configured to support a 1:1 mapping of IP addresses, but port configuration remained static. It would be interesting to see an N:1 mapping where both port and IP address are dynamic.

IPS Configuration: The IPS configuration used was the Check Point default. It is challenging to test against recommended IPS configurations because the testers look like rogue users when such a large volume of connection request are directed at a small number of servers (per the test environment).

Real-World Traffic Model

Tests that seek to emulate the real environment are far more useful to operators than those that seek to demonstrate maximum peak performance for a single metric. To execute this test, EANTC developed a traffic model that is closer to reality than the straightforward file transfer and HTTP traffic models that would typically be used in firewall testing. Spirent worked to implement this in the test equipment to create a bespoke test environment.

Of the 1 million active users, 95 percent were HTTP sessions with various small-sized URL files transferred; 1 percent were SMTP connections sending 64 kB objects, 2 percent were POP3 connections also sending 64 kB files; 1 percent were smart-phone OS over-the-air updates with 2 MB file sizes.

As would be expected, HTTP traffic dominated. Each of these user sessions simulated a user opening and browsing to a realistic mobile Web page using HTTP 1.1 with persistence. At the end of the page load, there were four open TCP connections and five completed transactions.

Detailed Discussion of Test Runs

There were four test runs in total, each covering different scenarios according to whether the IPS and NAT functions were enabled. In each test run the number of users, active TCP connections and TCP connections setups per second were kept more or less constant. The results of the four test runs are summarized in this table:

Figure 4: Summary of Firewall Forwarding Performance by Test Run

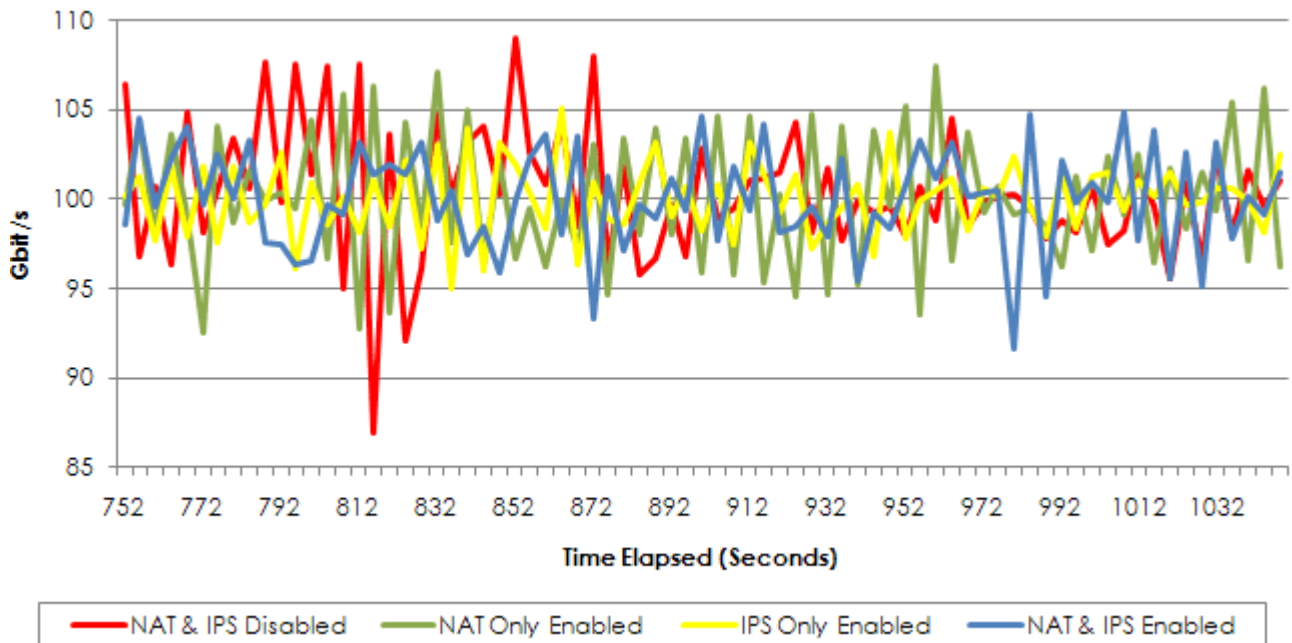
RUN	NAT	IPS	TCP CONNECTIONS*	AVERAGE THROUGHPUT (GBIT/S)*		TCP CONNECTION SET-UPS PER SECOND*
				DOWNSTREAM	UPSTREAM	
Run 1	On	Off	207,996,911	101.5	5.6	247,152
Run 2	On	On	210,830,122	100	5.5	241,595
Run 3	Off	Off	210,270,881	101.8	5.5	244,166
Run 4	Off	On	208,058,410	100.9	5.6	243,616

* During steady state

Source: EANTC, Heavy Reading

The primary point is that there is virtually no difference between the test runs. This is demonstrated by **Figure 5**, which shows downlink throughput for 320 seconds of steady state performance for each test run. Each run demonstrates the variability inherent in stateful traffic and each is clustered around the 100Gbit/s level.

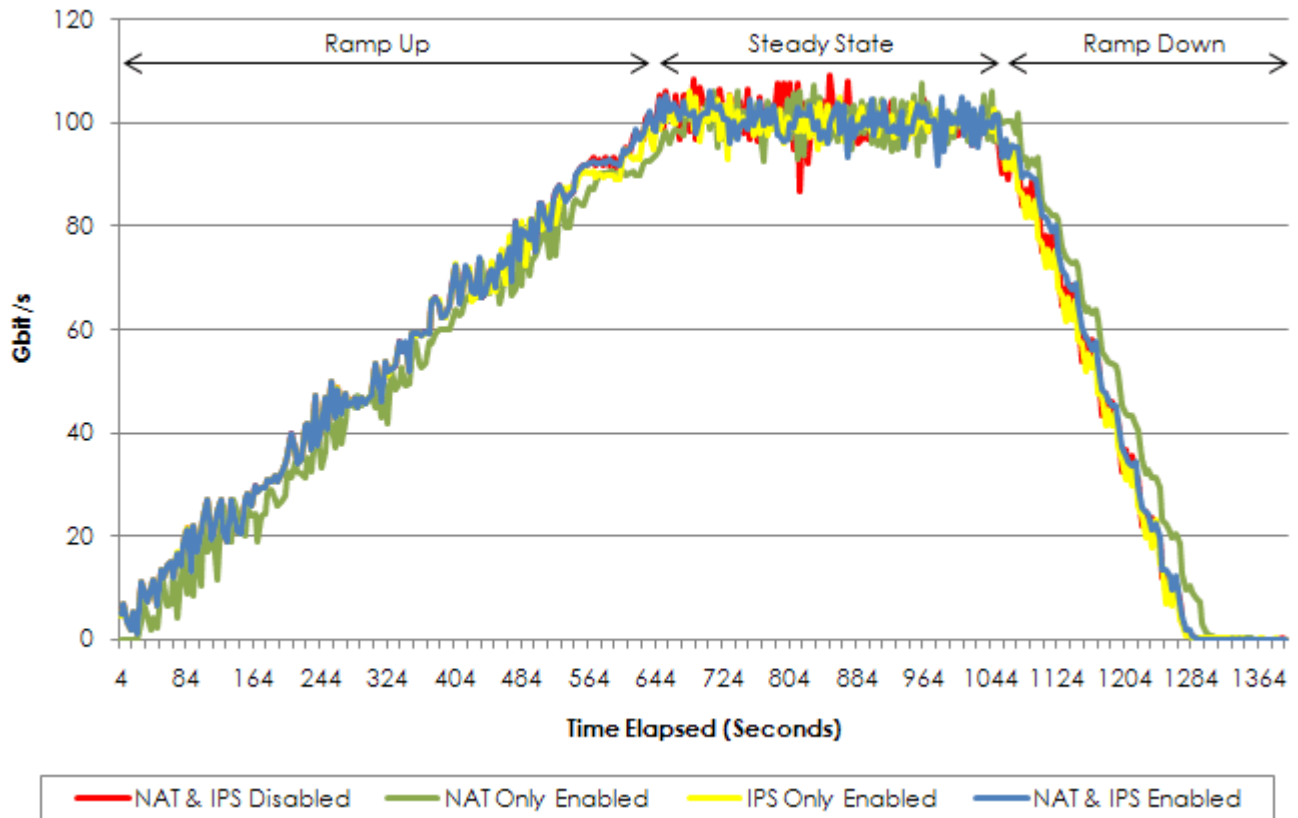
Figure 5: Downlink Forwarding Performance at Steady State



Source: EANTC

In **Figure 6** we show the downlink throughput data for the entirety of each test run. Steady state is clearly seen by the plateau at 100 Gbit/s. As before, there is no appreciable difference in the test runs. Essentially, this demonstrates a repeatable performance, which is critical.

Figure 6: Firewall Forwarding Performance by Test Run



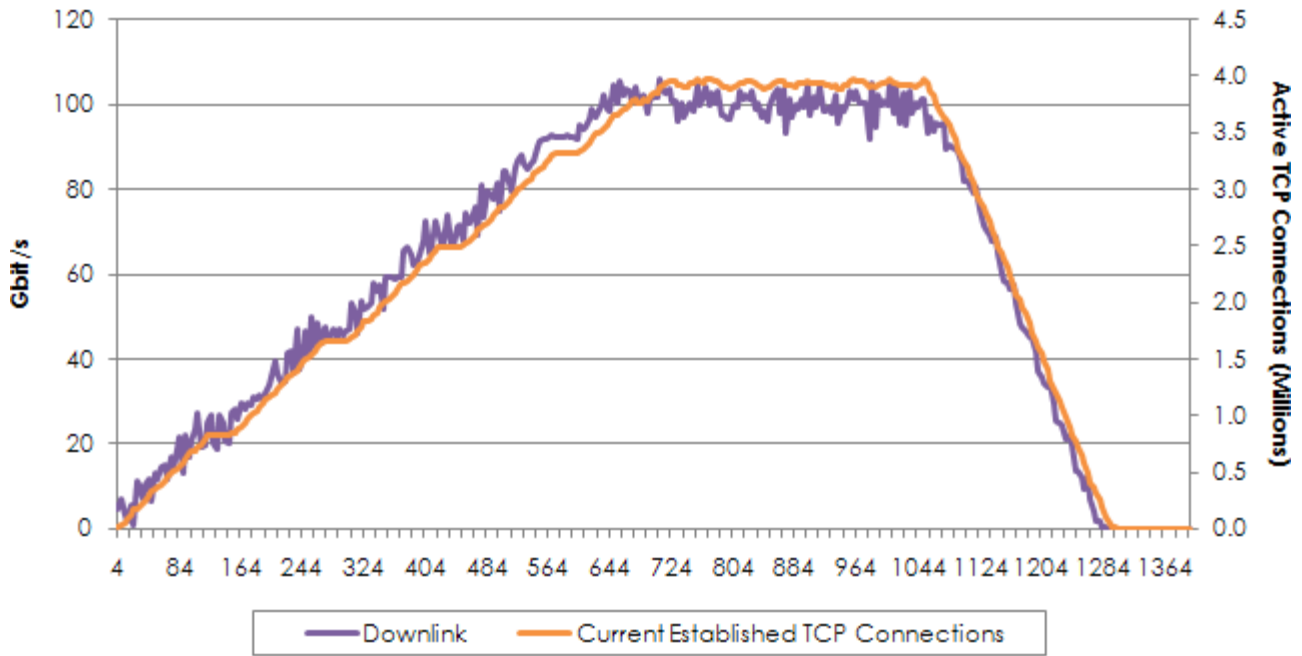
Source: EANTC

Test Run with IPS + NAT Enabled

To demonstrate how the X80-S scales, it is useful to examine a single test run in more detail. Given that it is the most challenging, Test Run 2 with NAT and IPS switched-on, is most interesting. The chart below shows downlink throughput for this test run in blue. As discussed previously, this was 100 Gbit/s during steady state. In orange, on the secondary vertical axis, the chart shows the total number of TCP connections active at each stage of the test run, which stabilizes at 4 million during steady state.

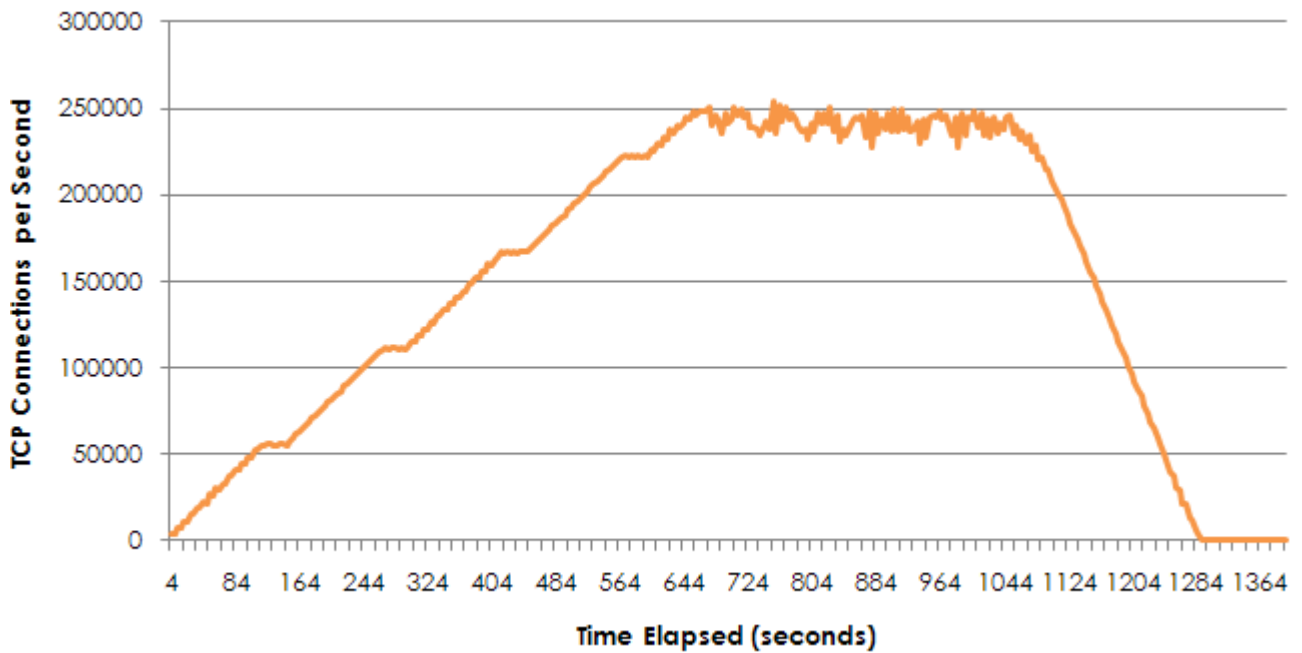
The second chart below shows the setup rate for new TCP connections. In steady state, this stabilizes at between 230,000 and 250,000 per second. This is effectively a measure of transaction rate performance. This was further examined in a separate test-run, which demonstrated a maximum of 8 million TCP connections and TCP setup rate of 274,000 per second are possible (versus 4 million and 250,000 during the full tests, respectively).

Figure 7: Firewall Forwarding & Active TCP Connections (NAT & IPS Enabled)



Source: EANTC

Figure 8: New TCP Connections per Second (NAT & IPS Enabled)



Source: EANTC

Conclusion

The EANTC test of Crossbeam's new X80-S networking hardware running Check Point firewall software has set an industry benchmark for high-performance mobile network firewall testing. Using a traffic model that emulates real users and testing against a broad set of criteria, the tests provide a useful guide to operators considering the selection and deployment of firewalls in mobile networks.

The mobile firewall product category will be increasingly important as operators move to LTE and the requirement for high-performance, low-latency, reliable data services becomes more critical. Security of the network and of end-user services is an established source of value for operators and their customers.

The SGi domain, where operator networks connect to end-user services and to external networks such as the Internet, is increasingly critical, complex and exposed to threats. To protect their networks and meet their objective of being secure communications providers, mobile operators are increasingly looking at advanced firewalls, denial-of-service protection and intrusion prevention systems.

According to the EANTC tests, the Crossbeam X80-S networking hardware is capable of 106 Gbit/s of throughput, while maintaining a realistic and useful number of subscribers and TCP connections. In *Heavy Reading's* view, this throughput is in excess of what is typically deployed in mobile networks today and should provide headroom for operators to securely scale mobile internet services in the LTE era.

Background to This Paper

Original Research

This *Heavy Reading* White Paper was commissioned by Crossbeam, but is based on independent research. The research and opinions expressed in the report are those of *Heavy Reading*.

About the Author

Gabriel Brown
Senior Analyst, *Heavy Reading*

Brown's coverage at *Heavy Reading* focuses on wireless data networking technologies, including WLAN, 3G/HSPA and LTE, with reference to how these technologies impact the wider mobile data services market. Brown has covered the wireless data industry since 1998. Before moving to *Heavy Reading*, Brown was Chief Analyst of the monthly *Insider Research Services*, published by *Heavy Reading's* parent company *Light Reading*.

Prior to joining the Light Reading Communications Group, Brown was the editor of *IP Wireline and Wireless Week* at London's Euromoney Institutional Investor. He often presents research findings at industry events and is regularly consulted by wireless networking technology leaders. Brown is based in the U.K. and can be reached at brown@heavyreading.com.

About Heavy Reading

Heavy Reading (www.heavyreading.com) is an independent research organization offering deep analysis of emerging telecom trends to network operators, technology suppliers and investors. Its product portfolio includes in-depth reports that address critical next-generation technology and service issues, market trackers that focus on the telecom industry's most critical technology sectors, exclusive worldwide surveys of network operator decision-makers that identify future purchasing and deployment plans, and a rich array of custom and consulting services that give clients the market intelligence needed to compete successfully in the \$4 trillion global telecom industry. As a telecom research arm of the Light Reading Communications Network (www.lrcn.com), *Heavy Reading* contributes to the only integrated business information platform serving the global communications industry.

Heavy Reading
240 West 35th Street, 8th Floor
New York, NY 10001
Phone: +1 212-600-3000