



Firewall Performance Evaluation Secure Computing Sidewinder vs. Check Point NGX

June 1, 2007
Trusted Strategies LLC

Author: Bill Bosen



Firewall Performance Evaluation

Secure Computing Sidewinder 7 vs. Check Point NGX R62

June 1, 2007

In view of the fact that firewall performance is becoming more and more critical, particularly in light of the need to scrutinize data packets at a more sophisticated level than ever before, we decided to put two industry leaders to the test.

Check Point has consistently been thought of as a high performance firewall provider, and in recent years they've been expanding into a deeper level of analysis and security. Another great firewall, Secure Computing Corporation's *Sidewinder*, has traditionally been viewed as the most secure firewall, and is now gaining recognition as a fast performer as well. So we decided to see how these two hot competitors would perform head to head. From Check Point, we tested their NGX R62, and from Secure Computing, we tested Sidewinder version 7.

Over the course of about two weeks, we performed multiple exhaustive performance tests. We conducted tests at the network layer (stateful inspection mode) and tests at the application layer (protocol inspection mode). We tested how fast raw UDP data could be pumped through the firewalls as well as TCP performance using a variety of test configurations.

Key Findings and Conclusions

In UDP performance testing, Secure Computing Sidewinder performed over 50% faster than Check Point NGX. In TCP performance testing, Sidewinder's performance exceeded Check Point NGX by anywhere from 50% to 300%. TCP results showed:

- When operating in the minimal security mode of *stateful inspection* (network layer protection), Secure Computing Sidewinder and Check Point NGX were essentially identical in performance.
- When operating in the more secure *protocol inspection mode* (application layer protection), Secure Computing Sidewinder performed more than 300% faster than Check Point NGX.
- When both products were configured to provide a high level of protection including intrusion prevention (IPS) for web servers protected by the firewall, Secure Computing Sidewinder performed over 50% faster than Check Point NGX.

What was tested

Check Point NGX

Version: NGX R62 Build 031
OS: SecurePlatform Pro
SmartDefense Version: Date - 02 May 2007
SmartDefense Updates: 602051213

Secure Computing Sidewinder

Version: Sidewinder 7.0.001H01
OS: SecureOS
IPS Update: Date - 05 May 2007
IPS Signature Updates: 200705071415.113

Testing Approach and Configuration

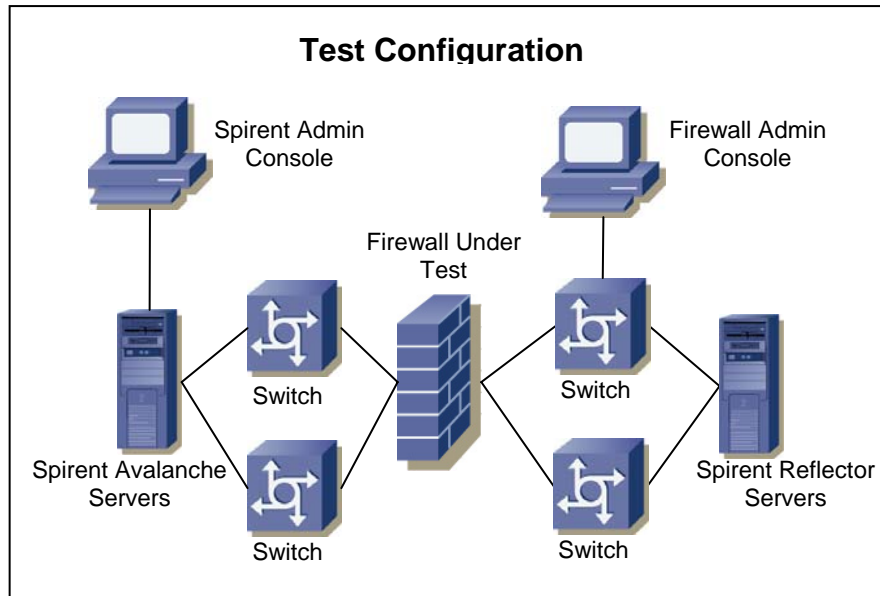
Identical test-bed conditions were used for all tests. Both firewalls ran on an identical Enterprise 2U platform hosting the latest and greatest hardware technology used by many security vendors. The platform included dual 2.66 GHz Dual Core Intel Xeon processors with 2 GB of ECC RAM with fully buffered DIMMS (FBD). Each had four 36 GB, 15K RPM hard drives, and utilized RAID 5 technology.

Hardware Form Factor	2U Platform
Processors (CPUs)	Two - 2.66 GHz Dual Core Xeon
Front-side Bus Speed	1333 MHz
Memory (RAM)	2 GB ECC Fully Buffered DIMMs (FBD)
Hard Drive(s)	4 - 36 GB 15K RPM
RAID	Yes, RAID 5
Power Supply	Dual
Number of Copper Interfaces Used in Testing	4 - 10/100/1000

Firewall Hardware Configuration

The Check Point NGX R62 system was Build 031, with Smart Defense version dated May 2, 2007, and Smart Defense update 602051213. The Secure Computing Sidewinder was version 7.0.001H01 with IPS Update dated May 5, 2007, and signature update 200705071415.113.

All TCP traffic for our performance tests was generated with a pair of Spirent Avalanche/Reflector model 2700 appliances. Two gigabit interfaces were used on each Spirent appliance. The UDP traffic was generated by SmartFlow software running on SmartBits. All traffic simulated as nearly as possible real-world network conditions.



For each of our four tests, we executed five test runs to ensure we were getting consistent results. For each TCP test run, the Avalanche/Reflector systems were set to automatically generate high rates of TCP traffic, which were directed to the particular firewall being tested (one at a time, in turn). Thousands of TCP connections were set up and terminated during each test run. Each test run, lasting from four to six minutes, consisted of *ramp-up*, *steady-state*, and *ramp-down* phases. The load on each system under test was increased until connections started dropping (as reported by the Avalanche/Reflector system). At this point the *maximum* throughput was recorded for the test run. Our UDP testing was done in the same manner, although we used SmartBits to generate the traffic.

For all tests, we performed each test run five times, recording the maximum throughput of each run. We then averaged the maximum throughput of all five test runs to arrive at the maximum throughput value we used.

Stateful Inspection Performance Tests

UDP Performance Tests

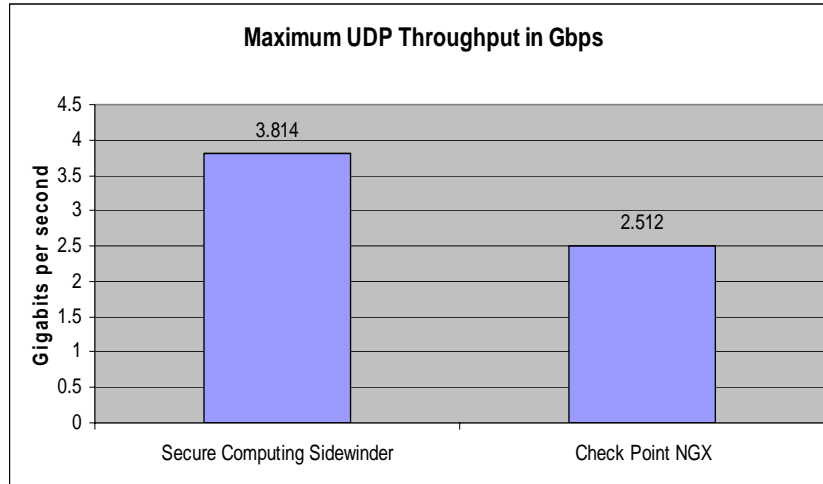
While it can, and should be argued that a UDP performance test does not adequately exercise a firewall, for various reasons many firewall performance tests have nonetheless been based on UDP. This can be attributed to the different vendors' desire to show the highest amount of throughput possible. Since UDP does not exercise connection setup and teardown, nor does it have the overhead required by TCP, testing how fast UDP packets can be passed through a firewall can show some mighty impressive numbers. So in spite of the fact that the overwhelming percentage of network traffic these days is TCP, and that filtering UDP packets does not adequately reflect what a firewall actually needs to do, a lot of performance testing has been based on UDP.

This has caused a lot of confusion among those reading the performance benchmarks in the marketing literature from the various vendors. Consumers often don't realize that some benchmarks are based on TCP while others are based on UDP. Many prospective buyers have been duped by what appeared to be a faster product, not knowing that the vendors were attempting to compare apples to oranges. So, to avoid any confusion, and at the same time give performance data that reflects what actually happens in the network, we decided to execute tests using both UDP and TCP.

For all exercises, including the UDP tests, we configured both Sidewinder and NGX identically. Both products were set up with one UDP stateful inspection filter rule on UDP port 80 from any source to any destination. **Protocol inspection** (application layer protection) was turned off, so both products were operating at the network layer doing *stateful inspection* only.

Our UDP tests consisted of sending thousands of UDP packets. Each packet had 1,518 bytes of information, including a payload of 1,472 bytes. As in all tests, we executed five test runs with each product to verify consistency, capturing the maximum throughput speed of each test run. The maximum speed of the five test runs was then averaged.

For this UDP test, we expected the Check Point NGX to outperform Secure Computing Sidewinder, but that wasn't the case. Sidewinder was essentially running at wire speed with an average maximum throughput of 3.814 Gbps whereas Check Point had an average maximum throughput of 2.512 Gbps. Both were impressive numbers, but Sidewinder was significantly faster, over 50% faster.



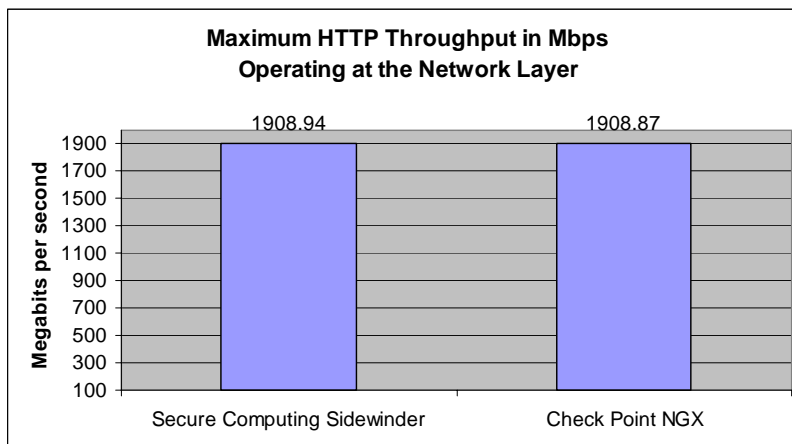
Since both products were running on the same hardware (including the network interface card), we attribute the speed advantage Secure Computing Sidewinder showed to better integration with the hardware platform and a more efficient, specifically tailored operating system.

TCP Performance Tests

For our next round of tests, we switched to TCP packets of varying lengths in order to determine the maximum throughput of HTTP data in stateful inspection mode. As in the prior tests, both firewalls were configured identically. *Protocol inspection* (application layer protection) was turned off, so both firewalls were operating at the network layer doing *stateful inspection only*. While this mode of operation is only fractionally as secure as protocol inspection or application layer protection, we felt it was important to establish a base line which could be used to compare against the more secure modes of operation.

For this test, as in the other tests, our Spirent Avalanche/Reflector load generators gradually increased the number of connections and HTTP packets transmitted until errors were received. Then the load was backed off to find the maximum level of data that could be pushed through each firewall in a stable matter. Once this was determined, we executed five test runs for each product, capturing the maximum speed of each test run. The maximum speeds of the five test runs were then averaged to arrive at the maximum throughput number we used for comparison purposes.

The result of this test was essentially a tie. The numbers were so close it seemed a bit spooky, at least at first. Secure Computing Sidewinder processed HTTP traffic at a maximum rate of 1,908.94 Megabits per second, and Check Point NGX handled the same HTTP traffic at a maximum rate of 1,908.87 Megabits per second. These numbers are amazingly close. However, since both firewalls were running on identical hardware with an identical test bed, and because stateful inspection requires so little processing and data scrutiny to be performed, we concluded that the near photo finish shouldn't be so surprising after all.



Protocol Inspection (Application Layer) Tests

Our performance testing encompassed a number of configurations; however we were most interested in testing the performance at the application layer as opposed to the network layer. Our reason for this is simple. It has become quite clear that the biggest threats a firewall must protect against are those that are buried within the application layer of the data packets.

This fact was underscored by Gartner Inc. when in a recent study they estimated that 75% of today's successful attacks occur at the application layer. Gartner made an even more frightening prediction, stating that by the year 2009, 80% of enterprises will be the victim of an application-layer attack.

Since firewalls purely inspecting at the *network layer* do not examine the actual payload of data packets, network layer firewalls have no way of checking for application layer attacks. Only firewalls inspecting traffic at the *application layer* can guard against today's threats.

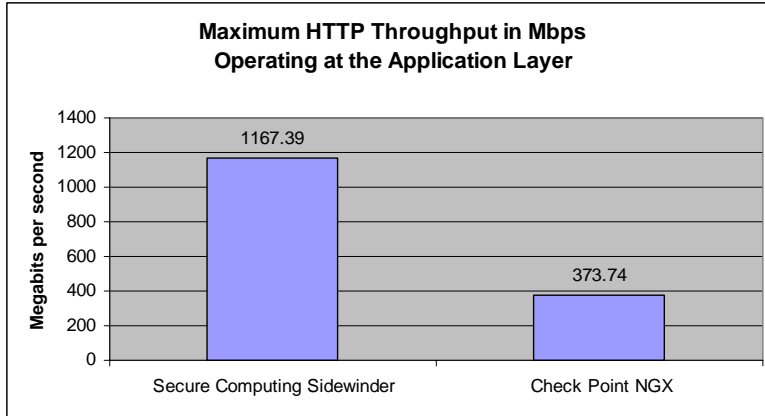
Providing protection at the application layer requires a great deal more processing and data handling, therefore questions about throughput and performance naturally surface. Which firewall will give the best performance while providing the application layer protection that's needed today? This was one of the key questions we set out to answer. So, for the remaining tests we configured both firewalls so that instead of inspecting at the network layer where they can not effectively examine application level data, they were examining at the application layer where the traffic could be fully scrutinized.

HTTP Protocol Inspection Mode (Proxy)

Our next round of tests focused on scrutinizing HTTP data in application layer mode. To accomplish this, Secure Computing Sidewinder was configured to use its *HTTP proxy* with full application defenses. Check Point NGX was likewise configured to utilize HTTP service with *HTTP protocol inspection*.

It's interesting to note that configuring Secure Computing Sidewinder in this manner was extremely straightforward and can be easily accomplished in a few clicks. Check Point, on the other hand, required configuring numerous individual settings. We did however love the information Check Point provided about the various threats and countermeasures. We would like to see Sidewinder do more in this area.

As in the other tests, we gradually increased the traffic until we found the maximum amount of data that could be processed successfully through each firewall. We then executed five test runs, capturing the maximum throughput of each run. Our test results showed Secure Computing Sidewinder's maximum throughput was more than 3 times faster than the Check Point NGX. Sidewinder's performance was 1,167.39 Mbps whereas the NGX's performance was 373.74 Mbps.

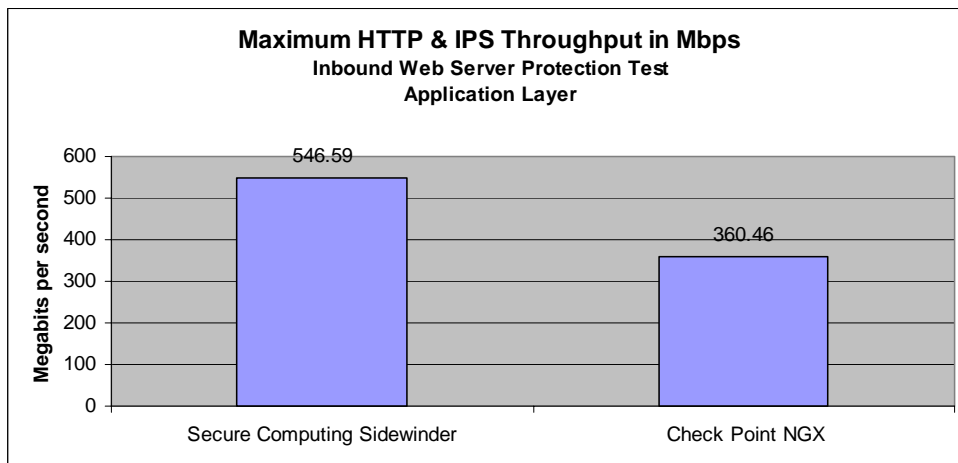


We expected Sidewinder to do well in this test, since Secure Computing has been perfecting this level of scrutiny for many years, but we were a bit surprised to see this much difference in performance versus Check Point.

Inbound Web Server Protection using Intrusion Prevention Signatures (IPS)

For our final test, we wanted to provide a high level of protection for web servers sitting behind the firewalls. In order to provide this protection, we configured both products to both inspect HTTP traffic at the application layer and inspect the traffic using intrusion prevention signatures (IPS). To accomplish the latter Secure Computing Sidewinder was configured specifically with IPS relating to Web services and Check Point NGX was configured with the Check Point SmartDefense matching services.

This test result showed Secure Computing Sidewinder to be over 50% faster than Check Point NGX. Sidewinder's maximum throughput was 546.59 Mbps while Check Point NGX's maximum throughput was 360.46 Mbps.



Summary Conclusions

As network speeds continue to increase, firewall performance is more critical than ever. At the same time, the sophistication and numbers of network security attacks are increasing at an alarming rate. These factors have made it imperative for an organization's firewalls to not only perform extremely well, but to process more security checks, and do so at a deeper level than ever before.

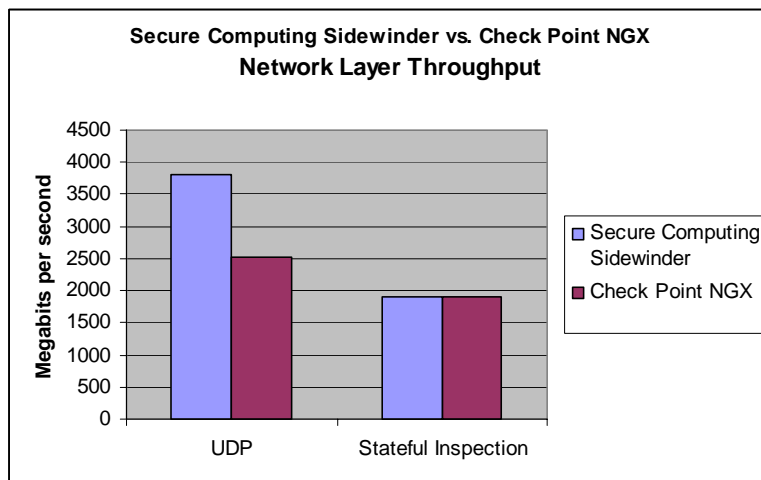
Putting Secure Computing Sidewinder and Check Point NGX through our rigorous tests and performance evaluations has shown that both products have improved in recent years. However, Secure Computing Sidewinder is the clear performance winner. Sidewinder was at least as fast as Check Point NGX in every test we conducted, and much faster in most tests, particularly in the medium to highest security configurations that the majority of organizations now seek.

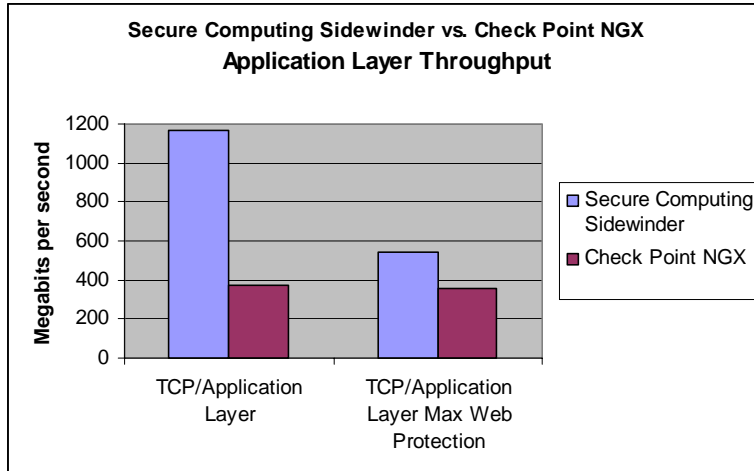
When operating in stateful inspection mode where firewall protection happens at the network layer only, Secure Computing Sidewinder and Check Point NGX perform equally well. So in those situations where minimal security is needed either product will provide more than adequate performance.

However, since 75% of today's successful attacks occur at the application layer as estimated by Gartner, network layer firewall inspection is insufficient. The only way to guard against application layer attacks is to actually inspect the packet's payload at the application layer, and this is where Sidewinder is the obvious choice.

Secure Computing Sidewinder was anywhere from 50% to 300% faster than Check Point NGX when providing application layer protection. When testing HTTP throughput at the application layer, Secure Computing Sidewinder clocked an impressive 1167.39 Mbps vs. 373.74 Mbps for Check Point NGX. When IPS for web servers was added, Sidewinder ran at 546.59 Mbps vs. NGX's 360.46 Mbps. Even protecting through the network layer only, Sidewinder's throughput was essentially equal to Check Point's at 1908.94 Mbps and 1908.87 Mbps, respectively.

Conclusion: Secure Computing Sidewinder performed as well or better than Check Point NGX in all our tests, and significantly better in the most secure configurations that today's networks demand.





Vendor Information

Check Point Software Technologies Ltd.

3A Jabotinsky St., Diamond Tower
 Ramat Gan, 52520
 Israel
 Tel: +972-3-753-4555
 Fax: +972-3-575-9256
www.checkpoint.com

Secure Computing Corporation

4810 Harwood Road
 San Jose, CA 95124-5206
 USA
 Toll Free: +1.800.692.5625
 Tel: +1.408.979.6100
 Fax: +1.408.979.6501
www.securecomputing.com

For additional information regarding this study, contact:

Bill Bosen, Founding Partner
Bill_Bosen@trustedstrategies.com
www.trustedstrategies.com



About Trusted Strategies

Trusted Strategies is a research and advisory firm focused exclusively on IT security. Our clients are product vendors who we help with market validation, positioning, competitive analysis, go-to-market strategies, business development, product and performance testing, and the creation of marketing and sales tools for their IT security related products. We also assist companies who are buying, selling, or otherwise acquiring IT security technology or firms.

With over 20 years of experience in the field, and as successful IT security entrepreneurs ourselves, Trusted Strategies understands the information security industry and how to provide just what our clients need.