



Performance Measurements

May 2002



SECURE
COMPUTING

**Secure Computing Corporation
Corporate Headquarters**

4810 Harwood Road
San Jose, CA 95124

tel +1.800.379.4944

tel +1.408.979.6100

fax +1.408.979.6501

International Headquarters

tel +44.1753.410900

fax +44.1753.410901

www.securecomputing.com

T A B L E O F C O N T E N T S

Sidewinder performance measurements

Abstract3
Summary of results3
Hybrid security4
Performance measurements with gigabit traffic levels4
Measuring raw traffic speed4
Results: raw traffic speed6
Measuring Sidewinder connection rates with HTTP traffic6
Results: HTTP connection rates8
Performance measurements for 10 Mbit/sec environments8
Results: 10 Mbit/sec environments8
Conclusion9



Abstract

This paper describes the results of performance measurement tests performed with a Sidewinder™ firewall. The tests measure the traffic capabilities of a single stand-alone firewall in several network environments: an environment with gigabit traffic levels, and in an older environment with 10baseT traffic levels. These results are intended to help sites assess their requirements when installing Sidewinder.

To support high traffic levels, large-scale sites typically choose to deploy *multiple* Sidewinders in a *rack cluster*. Such configurations easily support unlimited multi-gigabit traffic levels while taking advantage of the unmatched effectiveness of application-level security filters. Clusters also provide high availability by allowing the site to hot swap hardware components in-and-out for maintenance upgrades.

Again, the tests described in this paper measure the traffic capabilities of a single stand-alone Sidewinder firewall on fairly typical, commercially available hardware platforms.

Summary of results

- Hardware limitations are the principal inhibitors to increased performance of the firewall, not the Sidewinder software.

The key point is that the faster the hardware, the better the firewall performs. In particular, firewall performance is dominated by bus speed. For Sidewinder, bus speed is clearly the biggest bottleneck impacting its throughput. After the bus speed factor, other hardware elements also come into play. In a rough priority order, the critical elements are processor speed, memory speed and quality (i.e., is the memory self correcting or not), and disk performance. The fact that hardware is the primary inhibitor to Sidewinder firewall performance is consistent with the performance measurements reported by the other major firewall vendors. Comparable security mechanisms on comparable hardware provide similar performance results.

- Recent tests examine performance in a gigabit-networking environment. These tests examined Sidewinder’s performance when handling gigabit-level traffic. They measured performance using Sidewinder’s stateful packet filtering features and its higher-security proxy features.

security filtering	Throughput	Connections/sec accepted
Packet filtering	635.2 Mb/sec	Unlimited
Network proxy	361.6 Mb/sec	2010.8

Table 1: Test results for gigabit traffic levels

- Earlier tests provide results based on 10 Mbit/second traffic levels. These tests examined Sidewinder’s performance when faced with traffic levels on the order of 11.5 Mb/sec, which slightly exceeds classic Ethernet performance. Specifically, the tests measured both the packet filter and generic proxy as having a negligible effect on throughput. The application proxy reduces the throughput to approximately 48% of its original value. If we add Secure Computing’s SmartFilter™ to filter URLs according to content, there is only a 2.7% further reduction in throughput.



Sidewinder performance measurements

Security filtering	Average throughput
Packet filtering, net proxy, or no Sidewinder	11.5 Mb/sec
Application proxy: without SmartFilter	5.54 Mb/sec
Application proxy: with SmartFilter	5.39 Mb/sec

Table 2: Test results for 10 megabit/second traffic levels

Hybrid security

Not all sites are 100 percent paranoid, nor are all sites 100 percent indifferent to network-borne security threats. Often sites are willing to take risks with some types of traffic that they won't take with others. This reflects the richness of today's Internet environment.

Today's Sidewinder provides the tunability needed in this environment because it is a *hybrid* firewall: it supports a whole range of techniques for filtering your Internet traffic. This allows a site to quickly and easily balance its traffic handling requirements with its security requirements. If some types of Internet traffic require high throughput and pose little or no intrusion threat, administrators can configure Sidewinder to pass that traffic through Sidewinder's stateful packet filtering mechanism to achieve the highest possible speeds. TCP traffic that receives moderate restrictions can pass through the somewhat more CPU-intensive generic proxy services. Services that pose a serious or critical security threat, like certain proprietary e-business Web traffic or FTP file transfers, can pass through Sidewinder's application level proxies, thus trading off some throughput performance for the highest level of security filtering attained by any product in the world. Sidewinder's secure embedded servers for e-mail and DNS provide the highest degree of protection attainable for those critical Internet services.

To make effective use of a hybrid firewall, administrators need to understand how the different security levels affect traffic levels. This paper provides an initial set of estimates to help understand these trade offs.

Performance measurements with gigabit traffic levels

The gigabit traffic experiments sought to produce repeatable measurements of Sidewinder performance when subjected to traffic that saturates a gigabit network. The tests focused on measuring maximum readings, partly to ensure that the results were comparable to those produced by other manufacturers, and partly to make it easier to make the process repeatable. Earlier measurements based on more realistic firewall traffic loads proved to be difficult to repeat reliably since they involved varying traffic loads.

In particular the gigabit tests focused on three metrics: throughput, connection rate, and concurrent connections. Only the first two results are described here in detail. The throughput metric indicates sustained data transfer rate through the firewall. Throughput is measured in megabits per second (Mbps). The connection rate metric indicates the rate at which the Sidewinder can accept new connections and is measured in connections per second (cps). The measurement of concurrent connections indicates the number of connections the firewall is capable of supporting at any given time.

Measuring raw traffic speed

These tests measured the Sidewinder's capacity to transfer large amounts of data over many concurrent connections. Figure 1 illustrates the test configuration. There were five hosts connected to a gigabit switch on the "internal" side of the Sidewinder, four hosts connected to a gigabit switch on the "external" side, and one host



Sidewinder performance measurements

connected to a third “DMZ” connection. Network links were a combination of gigabit copper, gigabit fiber, and lower speed copper, though the links arriving at the Sidewinder were all rated at gigabit speeds.

The throughput benchmark program generated data and collected the statistics. Different mixes of traffic between client/server pairs were tested in order to achieve maximum throughput. Each test host ran only one client and one server, since preliminary testing showed that performance was not improved by running multiple clients or servers on a single host.

To run a test, each participating client would connect to a particular server and then loop endlessly, sending 1,460-byte messages. Each server would listen to a single port and accept a single connection. All traffic flowed from clients to servers. In order to send traffic through the Sidewinder in different directions, the tests would start servers on the Sidewinder’s internal, external, and DMZ connections.

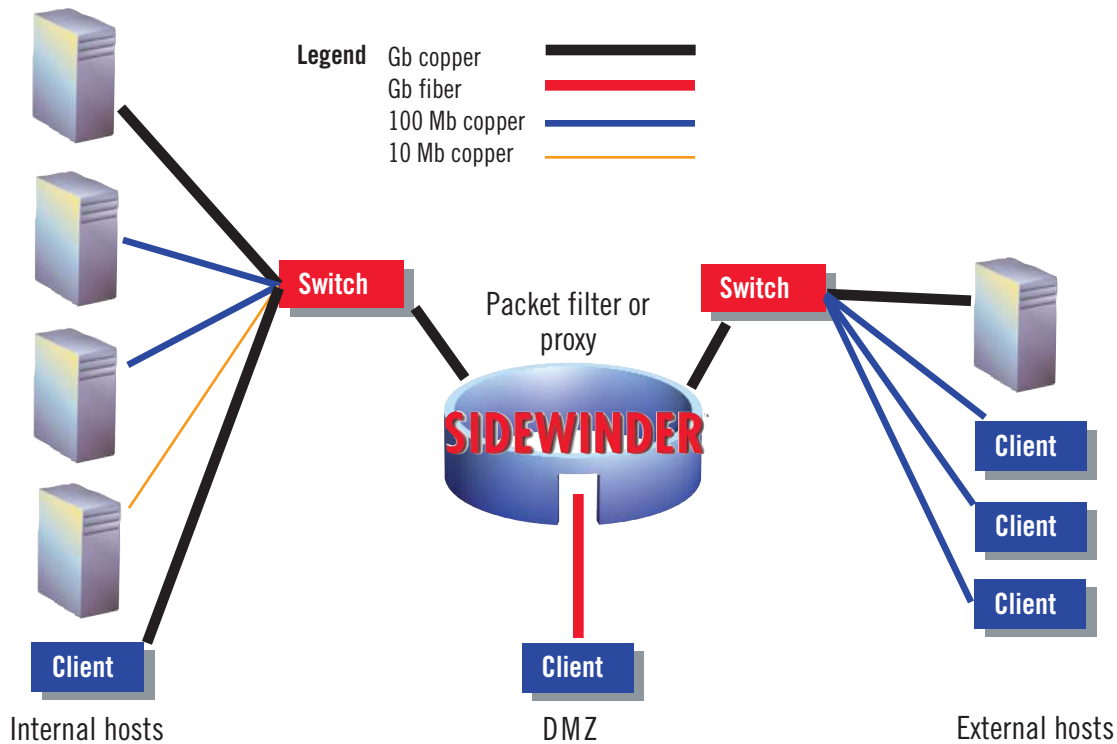


Figure 1: Throughput tests

The server would receive data on the connection, verify and count the data received, and keep track of the test time. Once the test run was completed, each server would calculate the rate at which it received data and print test metrics on the server’s console. The final throughput value was the aggregate of all the data transfer reported within the test interval.



Role	System	CPU	Memory
Firewall	Sidewinder 5.2	2GHz dual Xeon processors	512 MB
Internal server	FreeBSD 4.4-STABLE	1.8 GHz Pentium 4	256 MB
Internal server	Bsdi 4.2	800 MHz Pentium III	256 MB
Internal server	SecureOS	700 MHz Celeron	256 MB
Internal server	Bsdi 4.2	933 MHz Pentium III	256 MB
Internal client	FreeBSD 4.4-STABLE	900 MHz Pentium III Celeron	512 MB
DMZ client	Bsdi 4.3	863 MHz Pentium III	512 MB
External server	FreeBSD 4.4-STABLE	933 MHz Pentium III Celeron	256 MB
External client	Bsdi 4.2	933 MHz Pentium III	256 MB
External client	SecureOS	933 MHz Pentium III	512 MB
External client	SecureOS	933 MHz Pentium II	256 MB
Gigabit switch	D-Link DGS-1008T		

Table 3: Equipment used for throughput testing

Table 3 describes the equipment used for throughput testing. Servers and clients were all PC-based Unix platforms. SecureOS™ is Secure Computing’s proprietary, Unix-based operating system that incorporates Type Enforcement™ technology. SecureOS is the basis for Sidewinder’s unmatched resistance to sophisticated attacks.

Results: raw traffic speed

Here is a summary of the throughput measurements, in megabits per second (Mbps):

- Throughput of 635.2 Mbps, using stateful packet filtering via the IPfilter Mechanism.
- Throughput of 361.6 Mbps, using the generic TCP proxy with the fast path proxy option.

The engineers performing the tests found that CPU utilization never reached 100% while running the tests, which leads to the conclusion that higher performance can be achieved with higher performance hardware.

Measuring Sidewinder connection rates with HTTP traffic

This test measured the Sidewinder’s ability to respond to large numbers of closely spaced connection attempts via the HTTP proxy, which processes the standard TCP handshake and performs basic HTTP header validation. Figure 2 illustrates the test configuration, and Table 3 describes the equipment used. Two web servers were connected to one side of the Sidewinder via a D-Link DGS-1008T gigabit switch. Clients resided on a host connected to the other side of the Sidewinder via a pass-through fiber optic connection and a pair of Intel Pro1000 gigabit NICs.



Sidewinder performance measurements

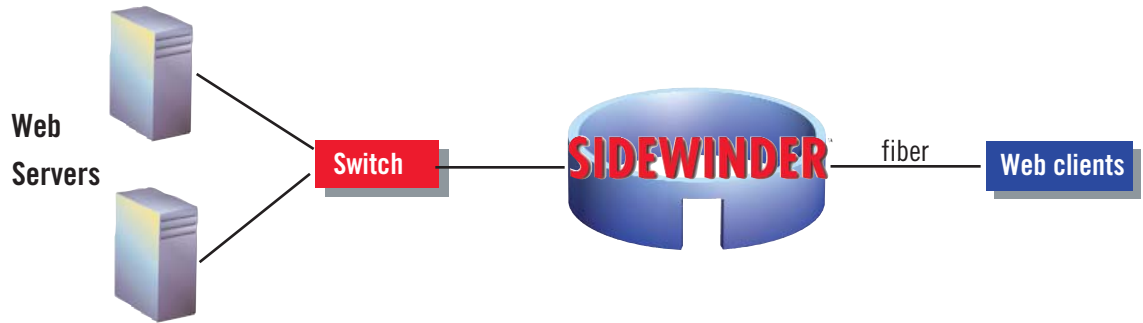


Figure 2: Connection rate benchmark

Role	System	CPU	Memory
Firewall	Sidewinder 5.2	2GHz dual Xeon processors	512 MB
Web server	FreeBSD 4.4-STABLE	930 MHz Pentium III Celeron	256 MB
Web server	Bsdi 4.2	1.8 GHz Pentium IV	256 MB
Web server	Bsdi 4.3	863 MHz Pentium III	256 MB
Gigabit switch	D-Link DGS-1008T		

Table 4: Connection rate machines

This test was performed by running a set of small, fast, Web clients on the client host. Each client would continuously request Web pages from one of the two servers. The servers used Turbo HTTP, a very small and fast Web server capable of handling very high traffic loads. Connections through the Sidewinder used the HTTP application level proxy.

Each client executed the following steps to establish a connection:

- Connect to the server via the Sidewinder
- Invoke an HTTP GET method for the URL
- Receive the HTTP response and Web page
- Tabulate the response
- Close the connection

These steps continued for the duration of the timed test. When the test interval ended, each client recorded its result in terms of the number of end-to-end transactions completed during that test. The total number of connections was calculated based on the results of the individual clients.

Here are some observations about the test environment:

- Running clients and servers on both sides of the Sidewinder did not increase the connection rate.
- FreeBSD 4.4-STABLE had a much slower server connection rate than did BSD/OS 4.2. The Sidewinder was not included in the preliminary test that identified this condition. FreeBSD could not produce an adequate connection rate to be used for this test.



Sidewinder performance measurements

- Both the BSD/OS and the FreeBSD kernel were configured to decrease the maximum segment lifetime (MSL) to 2 seconds. This configuration change was necessary to prevent the BSD machines from being the bottleneck in the test, so that the benchmark was not measuring performance of the server instead of the firewall. This configuration change decreased the length of time a connection was in TIME_WAIT state, freeing sockets for reuse more quickly. Otherwise the server would block once saturated with connections that had been closed, but had not yet been released by the operating system.
- Client and server processes needed to be run at high priorities in order to be adequately serviced by the operating system.

Results: HTTP connection rates

The Sidewinder achieved a maximum connection set-up rate of **2,010.8 connections per second** during a 30 second test in which 10 clients continuously requested pages of approximately 170 bytes (including HTTP headers). Six client processes requested the same set of pages from one server, and the other four clients requested pages from the other server. This connection set-up rate satisfies the majority of environments with comfortable room to spare.

Performance measurements for 10 Mbit/sec environments

Earlier tests were performed on Sidewinder using a variety of types of traffic and of security settings. The tests were intended to reflect “real world” firewall behavior and were based on measurements of actual firewall traffic. As such, the tests measured a number of different types of traffic being passed through different security configurations, including generic and application proxies as well as secure servers for e-mail. Unlike the gigabit tests, these tests did not attempt to measure maximum performance and did not use the fastest available host and networking hardware. This makes the results difficult to compare to the gigabit results except in relative terms.

The basic test organization follows that shown in Figures 1 and 2. The server and client equipment consisted on Sun Ultra-1, Ultra-5, and Ultra-10 computers. Hosts connected to the Sidewinder through Cisco Catalyst 3524XL switches that were configured to support gigahertz traffic between the switches and the Sidewinder. Unlike the 5.2 tests, however, there were not enough server and client hosts available to generate gigabit traffic levels.

Results: 10Mbit/sec environments

These results provide a rough guide to the impact of various security mechanisms on a Sidewinder’s network throughput.

- The test hosts generated a throughput rate of 11.52 megabits/second, on average. They were able to generate traffic at about this rate when connected via a bare wire. In fact, the test hosts maintained this rate even when running through Sidewinder’s packet filtering or generic proxy (within 0.8%).
- The application level Web proxy achieved a throughput of 5.54 Mb/sec, on average, in this environment. This indicates that the proxy achieved 48.1% of the rate achieved by Sidewinder’s lower security settings, or the rate of a bare wire.
- Using the application level Web proxy in conjunction with SmartFilter™ Web content filtering product yielded a relative throughput of 5.39 Mb/sec. This represents a 2.7% reduction in throughput relative to the rate supported by the application proxy itself.



Conclusion

Sidewinder is a tunable security system

Sidewinder is in an elite class of firewalls that are often called hybrid firewalls. These hybrid firewalls are capable of selectively securing traffic at all levels in the network protocol stack, from the wire up to and including layer 7, the application layer.

Today's Sidewinder provides the tunable flexibility needed in modern networking environments by supporting a mix and match security model, which allows a site to quickly and easily balance its traffic handling requirements with its security requirements. If some types of Internet traffic require high throughput and pose little or no intrusion threat, administrators can configure Sidewinder to pass that traffic through Sidewinder's low-level packet filtering mechanisms. For services that pose a serious or critical security threat, we would recommend the use of Sidewinder's application level proxies to achieve highest attainable level of security filtering possible from any product in the world.

Hardware limitations are the principal inhibitors to increased performance, not Sidewinder software.

The faster the hardware, the better the firewall performs. Hardware bus speed dominates firewall performance. This observation and the related measurements are consistent with the performance measurements reported by the other major firewall vendors. Comparable firewall security mechanisms on comparable hardware provide similar performance results.

Cluster Sidewinders in a rack for unlimited scalability and throughput

To support high traffic levels, large-scale sites typically choose to deploy multiple Sidewinders in a rack cluster. Such configurations easily support unlimited multi-gigabit traffic levels while taking advantage of the unmatched effectiveness of application-level security filters. Clusters also provide high availability by allowing the site to hot swap hardware components in-and-out for maintenance upgrades.

