THE TOLLY GROUP

No. 205102 February 2005

SECUi.COM Ltd.
NXG 2000
Non-Competitive Evaluation of Gigabit Ethernet Firewall & VPN Performance

TOLLY 16 YEARS 1989-2005

Test Summary

Premise: *Firewalls can provide a single point of defense between networks. Together with a firewall, VPNs can also provide security over a public shared network. VPNs provide a virtual secure connectivity by looking as if a public shared network is a private network. Today, more and more organizations are deploying firewalls and VPNs on internal networks operating at relatively high speeds, while most firewall and VPN implementations remain optimized for use over relatively low-speed wide-area connections. As a result, customers are often unsure whether the products they buy will stand up to high traffic loads.*

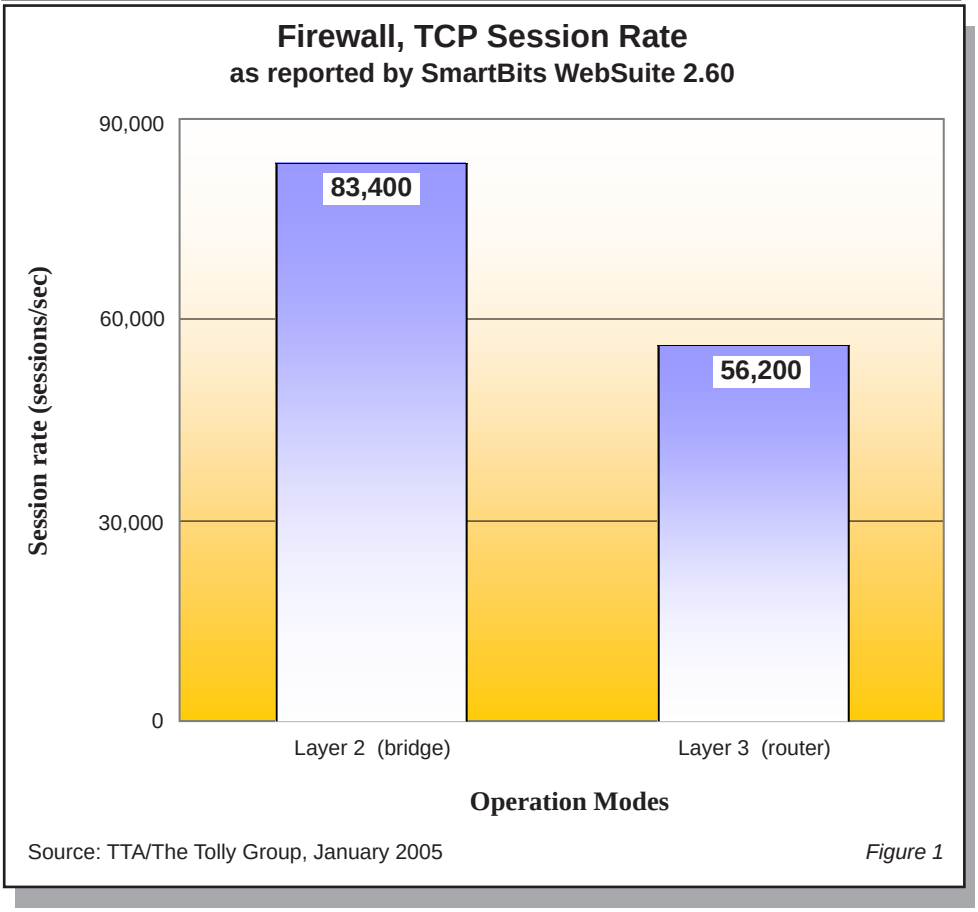
Test Highlights

- Processes up to 83,400 TCP sessions/sec in Layer 2 firewall mode, up to 56,200 TCP sessions/sec in Layer 3 firewall mode
- Forwards up to 1,923 Mbps and 1,907 Mbps of bi-directional, zero-loss throughput for a single VPN tunnel and 5,000 VPN tunnels respectively when tested with 1,400-byte frames
- Delivers up to 850,751 frames/sec and 858,397 frames/sec for a single-rule firewall and 2,000 rules respectively when tested with 64-byte frames in Layer 3 mode

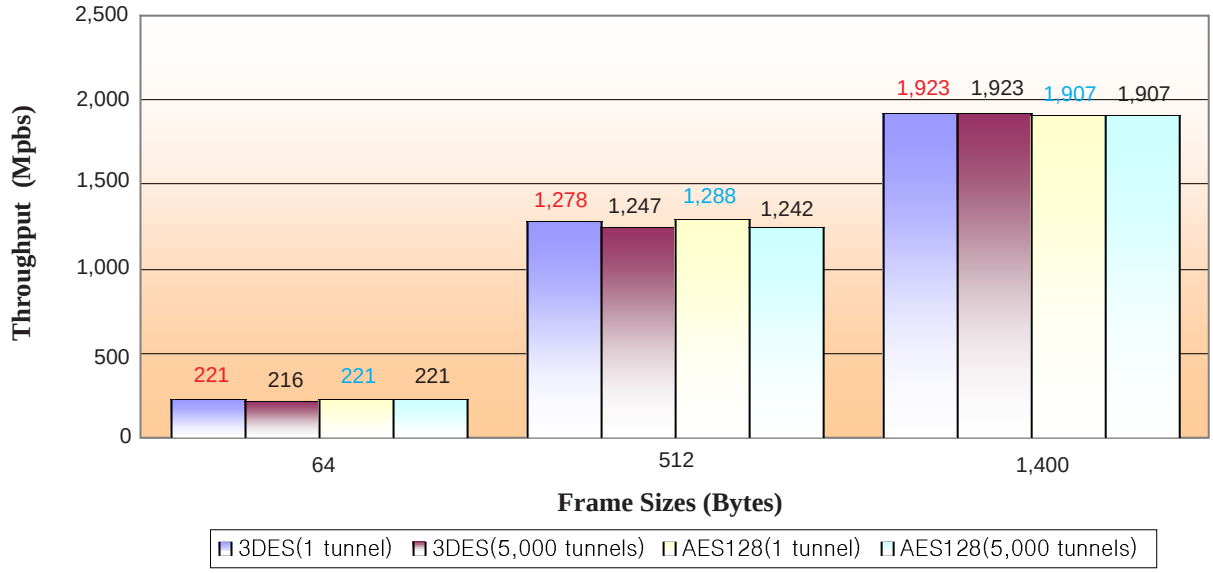
SECUi.COM Ltd. commissioned The Tolly Group/TTA (Telecommunications Technology Association) to test its NXG 2000, a Gigabit Ethernet firewall and VPN appliance.

TTA/TTG benchmarked the maximum TCP session rate when the NXG 2000 is operated in firewall mode only. The Spirent Communications SmartBits SMB-6000 (Testing S/W: WebSuite/ Firewall) was used to establish the TCP connections and to measure the maximum session rate.

TTA/TTG also benchmarked the bi-directional steady-state zero-loss (≤ 0.1%) UDP throughput under multiple rules and UDP sessions when the NXG 2000 was operated in firewall or VPN mode respectively. For VPN throughput testing, engineers utilized a variety of frame sizes (64, 128, 256, 512, 1,024, and 1,400 bytes) generated using the SmartBits SMB-6000 (Testing S/W: SmartFlow) equipped with two Gigabit Ethernet interfaces. The VPN test was run three times and the final result was an average of the three test iter-



Source: TTA/The Tolly Group, January 2005 *Figure 1*



Source: TTA/The Tolly Group, January 2005 *Figure 2*

ations. For the firewall throughput testing, engineers utilized frame sizes of 64, 128, 256 bytes; all frames were generated using the same Spirent Communications SmartBits SMB-6000 that was utilized in the VPN throughput test. This test also was run three times and the final result was derived from an average of the three test iterations.

Results

Firewall: Layer 2 / Layer 3 TCP Session Rate

Session rate is an important element of any firewall and security device located on the point of defense between networks because a variety of worms and peer-to-peer programs that can create the overwhelming sessions are prevalent over the Internet.

Engineers configured the NXG 2000 to serve as a Layer 2 (bridge mode) or Layer 3 (router mode) firewall configured with a single rule ("allow all"). Engineers configured the SmartBits to open and close up to 1 million requested TCP connections for each iteration and measured the maximum TCP session rate.

A TCP session consists of a three-way handshaking connection process using the sequence of SYN, SYN-ACK and ACK frames and a four-way handshaking close process immediately following with the sequence of FIN, ACK, FIN and ACK frames. That is, any other frames (e.g. HTTP or UDP as background traffic) are not used.

When handling 1 million requested TCP connections, the NXG 2000 processed up to 83,400 TCP sessions per second in Layer 2 mode, while processing up to 56,200 TCP sessions per second in Layer 3 mode. (*See Figure 1.*)

VPN:
3DES / SHA -1
AES128 / SHA-1
Bi-directional Zero-Loss Throughput

There is no sign of performance degration when the NXG 2000 supports up to 5,000 IPSec VPN tunnels. (For this round of testing, the number of tunnels has been established up to 5,000 tunnels and a single tunnel was used for the test traffic.)

Engineers configured two NXG 2000s to serve as an IPSec VPN gateway that supports 3DES and SHA-1 or AES128 and SHA-1 as the primary encryption and authentication method. One of two NXG 2000s was operated as the IPSec tunneling initiator and the other served as the IPSec tunneling responder. Engineers measured the bi-directional zero-loss (≤ 0.1%) throughput across a single tunnel between two NXG 2000s, connected with Gigabit Ethernet interfaces configured in full-duplex mode.

In both single-tunnel and 5,000-tunnels tests, engineers applied to the NXG 2000s a single UDP stream which consisted of a set of six frame sizes from 64 bytes to 1,400 bytes. For the 5,000 tunnels test, 5,000 tunnels were established by IKE (Internet Key Exchange) before running

the test and engineers used a single tunnel of established 5,000 tunnels for the throughput test.

In the 3DES/SHA-1 configuration, the NXG 2000 forwarded up to 1,923 Mbps regardless of the number of established tunnels when handling 1,400-byte frames. The NXG 2000 also achieved 221 Mbps for 64-byte, 711 Mbps for 256-byte, and 1,892 Mbps for 1024-byte frames when handling data across a single tunnel. (*See Figure 2.*)

In the AES128/SHA-1 configuration, the NXG 2000 forwarded up to 1,907 Mbps regardless of the number of established tunnels when handling 1,400-byte frames. The NXG 2000 also achieved 221 Mbps for 64-byte, 706 Mbps for 256-byte, and 1,876 Mbps for 1024-byte frames when handling data across a single tunnel. (*See Figure 2.*)

Firewall: Layer 2 / Layer 3 Bi-directional Zero-Loss Throughput

Engineers demonstrated that the NXG 2000 consistently achived the high performance when tested up to 2,000 rules and 10,000 UDP sessions. (*See Figure 3.*)

Engineers configured the NXG 2000 to serve as a Layer 2 (bridge mode) or a Layer 3 (router mode) firewall with single rule or 2,000 rules according to test cases. Engineers measured the bi-directional zero-loss ($\leq$ 0.1%) throughput across a firewall with Gigabit Ethernet interfaces configured in full-duplex mode.

Engineers set up the SmartBits to generate test traffic consisting of 10, 5,000, 10,000 UDP sessions according to test cases for the frame sizes of 64 bytes, 128 bytes and 256 bytes. Because the NXG 2000 is a firewall and most of viruses and worms are under 256-bytes, engineers had put only those frames into the test.

When handling 64-byte frames with a single rule in Layer 2 mode, the NXG 2000 delivered up to 827,596, 796,873 and 743,348 frames per second (fps) for each 10, 5,000 and 10,000 UDP sessions, while the NXG 2000 delivered up to 835,425, 796,943 and 735,677 fps for each number of sessions as 2,000 rules were set up.

When handling 128-byte frames with a single rule in Layer 2 mode, the NXG 2000 delivered up to 822,448, 783,353 and 722,392 fps for each UDP session, while the NXG 2000 delivered up to 826,909, 787,640 and 722,389 fps for each number of sessions as 2,000 rules were set up.

When handling 256-byte frames with single rule in Layer 2 mode, the NXG 2000 delivered up to 788,981, 765,665 and 711,784 fps for each UDP session, while the NXG 2000 delivered up to 798,042, 765,680 and 711,900 fps for each number of sessions as 2,000 rules were set up.

When handling 64-byte frames with a single rule in Layer 3 mode, the NXG 2000 delivered up to 850,751, 835,426 and 751,023 fps for each 10, 5,000 and 10,000 UDP sessions, while the NXG 2000 delivered up to 858,397, 835,426 and 766,270 fps for each number of sessions as 2,000 rules were set up.

When handling 128-byte frames with a single rule in Layer 3 mode the NXG 2000 delivered up to 839,969, 822,428 and 739,638 fps for each UDP session, while the NXG 2000 delivered up to 852,728, 826,540 and 744,164 fps for each number of sessions as 2,000 rules were set up.

When handling 256-byte frames with a single rule in Layer 3 mode, the NXG 2000 delivered up to 807,395, 788,966 and 721,167 fps for each UDP session, while the NXG 2000 delivered up to 807,570, 793,318 and 725,980 fps for each number of sessions as 2,000 rules

SECUi.COM Ltd.

NXG 2000

Gigabit Ethernet Firewall & VPN Performance Evaluation

SECUi.COM Ltd.
NXG 2000
Product Specifications*

Performance Feature
- 1,500,000 concurrent sessions
- 20,000 concurrent VPN tunnels
- Up to 2 Gbps firewall throughput(bi-directional)
- 2 Gbps 3DES-SHA-1/AES-SHA-1 VPN throughput (bi-directional)
- Multi-layer classification table that applies ultimate policies to packets with only 13-step checks

Mode of operation
- Transparent mode supported on all interfaces
- Router mode supported on all interfaces
- NAT supported per policy and per interface on all interfaces

Load balancing and High Availability
- Active-Active high availability with load balancing
  - Distributed stateful inspection technology supports
    - Kernel level session synchronization
    - Distributed session management
    - Seamless transition and session maintenance during fail over
  - Load balancing without external Layer 4 switch supports

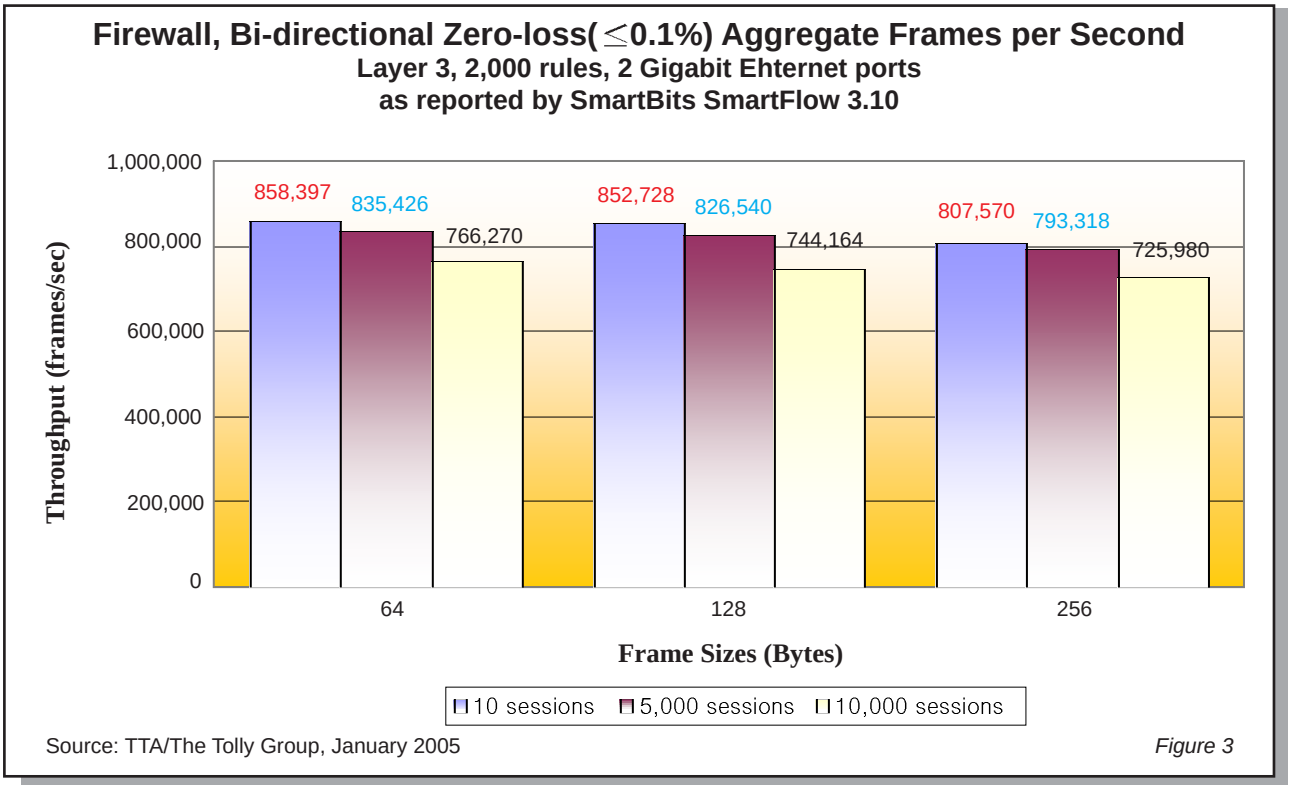
Intrusion Detection and Prevention
- Scan attack & DDoS detection and prevention
- Web vulnerability prevention
- Session shaping
- Content filtering
- Anti-virus & Anti-SPAM
- Signature/Traffic/Protocol anomaly analysis
- Vulnerability analysis & client quarantine

Management and Monitoring
- Integrated remote management of multiple NXG systems
- Multiple language support and diverse report generation

For more information contact:

SECUi.COM Corp.
18th FL., Ace Tower,
1-170, Soonhwa-dong, Jung-gu,
Seoul, Korea 100-712
Phone: 82-2-3783-6477,
Fax: 82-2-3783-6499
URL: http://www.secui.com

* Vendor-supplied information not verified by TTA /The Tolly Group



Source: TTA/The Tolly Group, January 2005 *Figure 3*

were set up.

Analysis

The NXG 2000 firewall provides packet-filtering function based on firewall rules configured by an administrator. Because of this processing intensive work, it is not surprising that it delivers the reduced throughput to a range associated with Gigabit Ethernet, but using a purpose-built hardware-based firewall may be the proper choice to maintain the consistent throughput levels for protected networks.

In the firewall TCP session rate test with the single ("allow all") rule, the NXG 2000 succeeded in establishing 83,400 TCP sessions per second in Layer 2 mode and established 56,200 TCP sessions per second in Layer 3 mode. The 56,200 TCP session rate in Layer 3 mode is good enough to handle almost all the connection requests occurring in the typical enterprise networks.

In the VPN throughput test, the NXG 2000 forwarded up to 1,923 Mbps and 1,907 Mbps for 3DES/SHA-1 and AES128/SHA-1 configurations respectively when tested with 1,400-byte frames and achieved the same performance for both a single tunnel and 5,000 tunnels. This is due to the crypto-accelerator being able to handle multiple packets concurrently and the unique "SPD-Search" algorithm with high efficiency. The NXG 2000 showed similar throughput results in both configurations.

In the firewall throughput test in the Layer 2 mode with a single rule and 10 sessions, the NXG 2000 forwarded up to 827,596 fps for 64-byte, 822,448 fps for 128-byte and 788,981 fps for 256-byte frames. Then, when tested in the Layer 2 mode with 2,000 rules and 10 sessions, the NXG 2000 forwarded up to 835,425 fps for 64-byte, 826,909 fps for 128-byte and 798,042 fps for 256-byte frames, respectively.

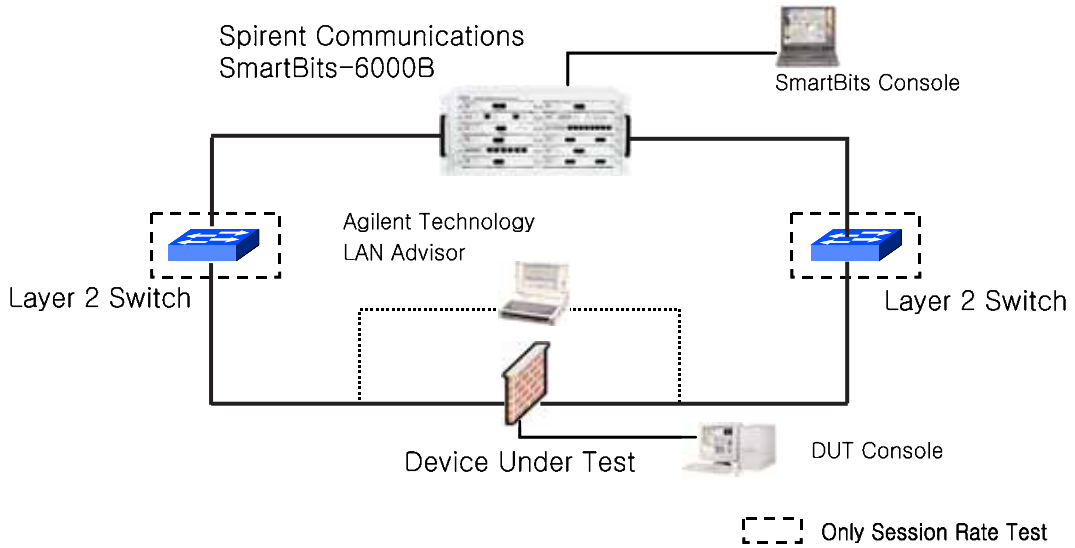
In the firewall throughput test in the Layer 3 mode with a single rule and 10 sessions, the NXG 2000 forwarded up to 850,751 fps for 64-byte, 839,969 fps for 128-byte and 807,395 fps for 256-byte frames. Then, when tested in the Layer 3 with 2,000 rules and 10 sessions, the NXG 2000 forwarded up to 858,397 fps for 64-byte, 852,728 fps for 128-byte and 807,570 fps for 256-byte frames, respectively.

The firewall throughput test shows that the number of rules configured on the firewall and the number of traffic flows did not have a large effect on the throughput performance in both Layer 2 and Layer 3 operation modes, when tested up to 2,000 rules and 10,000 UDP flows. This fact resulted from the patented traffic classification algorithm.

Test Configuration And Methodology

The Tolly Group/TTA tested the NXG 2000 running SecuiOS v1.1 (build 1.2.3R). The NXG 2000 was equipped with Gigabit Ethernet interfaces. The NXG 2000 was configured with various firewall rules and operation modes when operating

Firewall TCP Session Rate & UDP Throughput Test Bed



Source: TTA/The Tolly Group, January 2005

Figure 4

as a firewall. Also, the NXG 2000 was configured with various encryption and authentication methods when operated in VPN mode.

Engineers configured the NXG 2000 to provide only firewall function during the firewall UDP throughput and TCP session rate tests, while the NXG 2000 was configured to provide only VPN function when VPN UDP throughput was measured.

In the firewall TCP session rate test, engineers configured the NXG 2000 to operate in Layer 2 (bridge) mode or Layer 3 (router) mode with a single ("allow all") rule.

A SmartBits WebSuite/Firewall opened and closed 1 million requested TCP connections for each iteration across the NXG 2000. Engineers configured WebSuite/Firewall to increase the connection rate gradually by step-by-step mode. Engineers recorded the last "Connections Requested Per Second" reported by the test tool before the failure as the maximum session rate. Three test iterations were done and the results were averaged to obtain a final result.

In the firewall throughput test, engineers separately configured the NXG 2000 to operate in Layer 2 (bridge) mode or Layer 3 (router) mode with a single rule and 2,000 firewall rules. A SmartBits traffic generator was configured to generate 10, 5,000 and 10,000 UDP traffic flows.

A single firewall rule was activated for all traffic to be allowed to cross over the firewall without any denying, while 2,000 firewall rules consisted of 1,999 rules that deny the traffic matched up to IP address and service port and last rule that allow all traffic to cross over the firewall. Then engineers verified 2,000 rules activated on the NXG 2000 by CLI (Command Line Interface) commands. The CLI commands showed the lists of activated 2,000 rules and applied rules after finishing the test.

In the VPN throughput test, most of test configurations were similar to the set up of the firewall throughput test except that engineers configured two NXG 2000s to be operated as VPN gateways for VPN tunneling. Two NXG 2000s were connected with Gigabit Ethernet optic interfaces set up for full-duplex and auto-negotiation.

In the 5,000 tunnels test, all tunnels were established by IKE operations. For the test, engineers used a script to update the NXG 2000s configuration with 5,000 phase 2 tunnel entries before running the test. To verify the establishment of 5,000 tunnels,

Telecommunications Technology Association

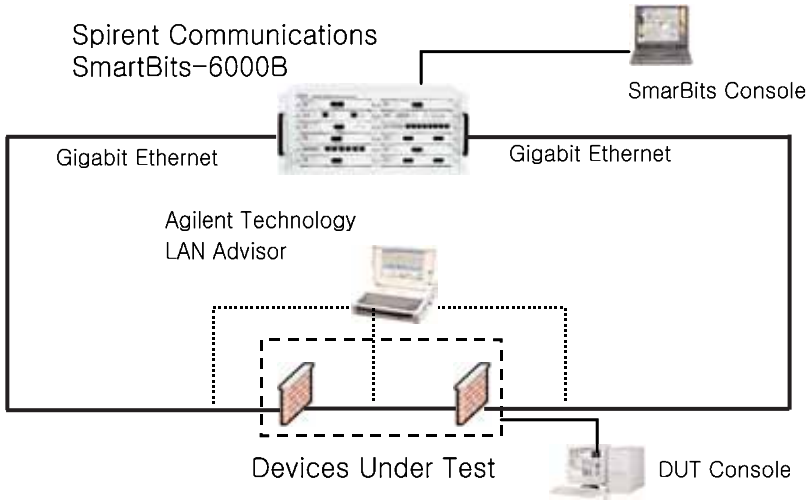
About TTA

The Telecommunications Technology Association (TTA) is a technology testing and standards organization established and sponsored by the Korean government. TTA provides third-party independent testing and certification services for IT products marketed in Korea to ensure IT products meet user needs, conform to standards, and provide interoperability.

TTA is licensed to use The Tolly Group's standard testing methodologies and Fair Testing Charter practices employed in the company's Up-to-Spec product evaluations.

Testing for this project was conducted by TTA, in conjunction with The Tolly Group, under the licensing agreement between the two companies. TTA followed standard procedures established by The Tolly Group. The Tolly Group reviewed all materials prior to publication.

VPN UDP Throughput Test Bed



Source: TTA/The Tolly Group, January 2005

Figure 5

engineers applied to the NXG 2000s test traffic that was designed to go through each of 5,000 tunnels using the "SmartWi-ndow" test tool and monitored the intermediate traffic between the NXG 2000 and SmartBits using monitoring device.

The Tolly Group gratefully acknowledges the providers of test equipment used in this project.

Vendor	Product	Web address
Spirent Communications	SmartBits-6000B	http://www.spirentcom.com
Agilent Technology	Agilent Advisor	http://www.agilent.com

Tolly Group Services

With more than a decade of testing experience of leading-edge network technologies, The Tolly Group employs time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy. Plus, unlike narrowly focused testing shops, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure. The company offers an unparalleled array of reports and services including: Test Summaries, Tolly Verifieds, performance certification programs, educational Webcasts, white paper production, proof-of-concept testing, network planning, industry studies, end-user services, strategic consulting and integrated marketing services. Learn more about The Tolly Group services by calling (732) 528-3300, or send E-mail to info@tolly.com.

For info on the Fair Testing Charter, visit:
http://www.tolly.com/Corporate/FTC.aspx

Project Profile

Sponsor: SECUi.COM Ltd.

Document number: 205102

Product class: Gigabit Ethernet Firewall and VPN

Products under test: NXG 2000

Testing window: September through November 2004

Software versions tested:
- OS: SecuiOS v 1.1 (build 1.2.3R)

Software status:
- Generally available

For more information on this document, or other services offered by The Tolly Group, visit our World Wide Web site at http://www.tolly.com, send E-mail to info@tolly.com, call (800) 933-1699 or (732) 528-3300.

The Tolly Group doc. 205102 rev. dat 23 February 05