

NetScreen Technologies, Inc.

NetScreen-5200 versus Nokia IP740 and Cisco Systems PIX 535

Test Summary

Competitive Evaluation of Multi-gigabit Firewall/VPN Multifunction Devices

Premise: Two trends today are redefining security needs in large enterprise and service provider networks: The move to enforce security policies in the core of large enterprise networks and service provider networks, along with the need to support emerging multimedia applications that often use small packet sizes, which translates to heavier traffic loads and demand for low latency and no packet loss. That means service providers and enterprise-class architects alike must deploy multipurpose security devices that exhibit consistently high performance even in the presence of small packet sizes, while also delivering low latency.

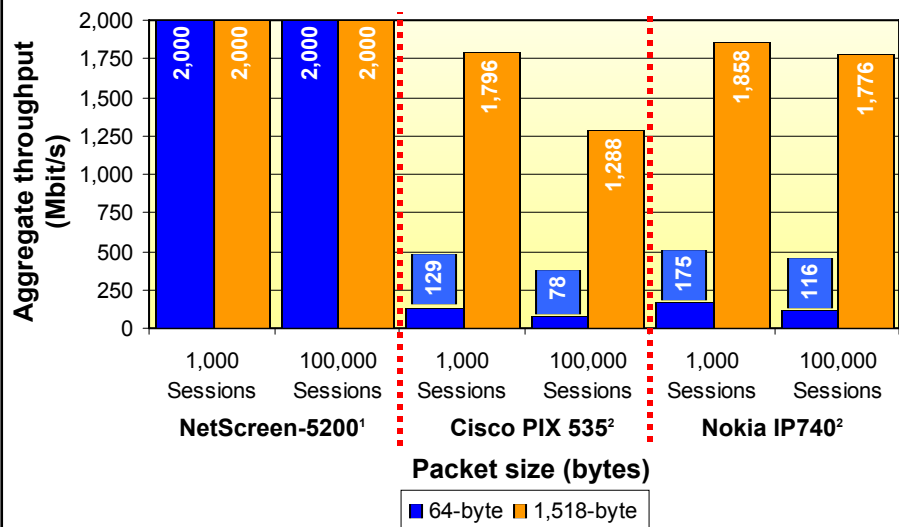
NetScreen Technologies commissioned The Tolly Group to benchmark the NetScreen-5200, a purpose-built high-performance Internet security system outfitted with Gigabit Ethernet interfaces, and compared the results with those of a similarly outfitted Cisco PIX 535 firewall/VPN and Nokia IP740 firewall device. For each of the devices under test, The Tolly Group conducted application throughput and zero-loss throughput tests, as well as standard latency tests for both firewall and VPN tunnel configurations, the latter incurring the extra processing factored in with support for 3DES and SHA-1. Each of the devices under test was subjected to a range of session loads, escalating from 1,000 sessions to as many as 500,000 sessions in our firewall tests.

For zero-loss performance tests, The Tolly Group measured the steady-state throughput where loss was less than 0.001%, the same stringent metric that The Tolly Group employs to test Layer 2 and

Test Highlights

- Delivers 4 Gbit/s of bidirectional firewall throughput and 2 Gbit/s of 3DES/SHA-1 VPN throughput
- Achieves full 2 Gbit/s wire-speed firewall throughput with 64-byte packets at 100,000 sessions, or 26X the Cisco PIX 535 performance and 17X the Nokia IP740 performance
- Achieves up to 100% of 2 Gbit/s theoretical maximum throughput across an IPSec tunnel with 3DES and SHA-1 versus a maximum of 6% for the Cisco PIX 535
- Scales easily to 500,000 sessions while delivering 100% of wire-speed throughput on 512-, 1,024- and 1,518-byte packets

Zero-Loss Throughput Across a "Single-Rule" Firewall with UDP Packets Bidirectional Traffic, Full-Duplex Gigabit Ethernet



¹ Number of simultaneous UDP sessions, <0.001% packet-loss threshold

² Number of simultaneous UDP sessions, 1% packet-loss threshold

Source: The Tolly Group, March 2002

Figure 1

Layer 3 devices. By contrast, The Tolly Group opted to test the Cisco PIX 535 and Nokia IP740 with a less stringent 1% packet-loss threshold to provide an apples-to-apples comparison with previous head-to-head tests conducted between the NetScreen and Cisco gear (Refer to Test Summary Document 201111).

Test results show that the NetScreen-5200 consistently offers superior performance to the Cisco and Nokia devices, even under heavy session loads. Testing was performed in March 2002.

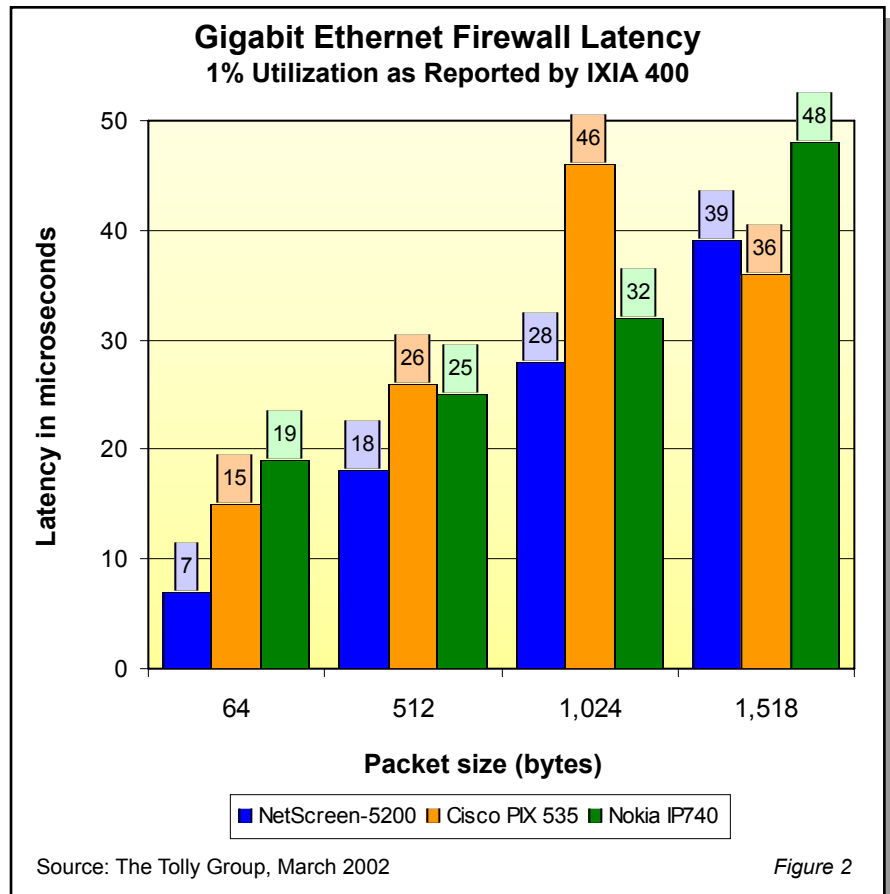
RESULTS

SINGLE-RULE FIREWALL BIDIRECTIONAL THROUGHPUT

In a single-rule “allow all” firewall configuration with Network Address Translation (NAT) disabled and 1,000 sessions supported, the NetScreen-5200 achieved 2 Gbit/s wire-speed throughput when handling 64-byte packets. By contrast, the Cisco PIX 535 achieved an average aggregate throughput of 129 Mbit/s and the Nokia IP740 achieved aggregate throughput of 175 Mbit/s – meaning the NetScreen-5200 throughput amounts to an 11X improvement over the Nokia IP740 and a 15X improvement over the Cisco PIX 535. (See figure 1.)

In subsequent tests of 1,000 sessions with larger packet sizes (512, 1,024 and 1,518 bytes), the NetScreen-5200 reported results that were between 8% and 129% higher than the Nokia IP740 and between 11% and 150% higher than the performance of the Cisco PIX 535.

Engineers next stepped the session configuration up to 50,000 sessions and ran the tests with frame sizes of 64, 512, 1,024, and 1,518 bytes. With 50,000 sessions and 64-byte packets, the NetScreen-5200 achieved aggregate throughput of 2 Gbit/s, versus 139 Mbit/s for the Nokia IP740 and 99 Mbit/s for the Cisco PIX 535. That equates to a 14X performance advan-



tage over the Nokia IP740 and 20X performance lead over the Cisco PIX 535. In subsequent tests of 50,000 sessions with larger packet sizes (512, 1,024 and 1,518 bytes), the NetScreen-5200 performed between 8% and 154% better than the Nokia IP740 and 26% to 232% better than the Cisco PIX 535.

At 100,000 sessions, the NetScreen-5200 increased the performance gap over the competitive products tested. While the NetScreen-5200 achieved wire-speed 2 Gbit/s aggregate throughput when handling 64-byte packets, the Nokia IP740 handled 116 Mbit/s of firewall performance and the Cisco PIX 535 managed 78 Mbit/s. When compared at larger packet sizes, the NetScreen-5200 provided from 15% to 174% more throughput than the Nokia device and from 55% to 318% greater throughput than the Cisco PIX 535.

Lastly, engineers tested the devices at 500,000 sessions to demonstrate their scalability for large-scale enter-

prise and service provider environments. Only the NetScreen-5200 successfully passed this test, delivering wire-speed zero-loss throughput for most packet sizes tested, and 1.4 Gbit/s or 70% of wire-speed throughput for taxing 64-byte packets.

The Nokia IP740 has a known session ceiling that is less than the 500,000 and hence was not tested in this scenario. Testing of the Cisco PIX 535 revealed that it could not successfully establish 500,000 sessions. Instead, when 500,000 sessions were attempted, the Cisco PIX 535 established only about 300,000 sessions; when engineers attempted to establish 300,000 sessions on the Cisco device, it only delivered 200,000 sessions. When the load was reduced to 200,000 sessions, engineers were only able to establish 98,000 sessions successfully, which was deemed an unnecessary run since we had previously tested successfully at 100,000 sessions.

MAXIMUM DEVICE FIREWALL BIDIRECTIONAL THROUGHPUT

Engineers determined the NetScreen-5200's maximum device throughput rate in a single-session test that pushed 64-byte, 512-byte and 1,518-byte packets through the device which was configured with four of the eight gigabit interfaces.

At 1,518-byte packets, the NetScreen-5200 delivered 100% zero-loss throughput of 4 Gbit/s when handling bidirectional, full-duplex Gigabit Ethernet traffic. The NetScreen-5200 achieved 95% and 59% of wire-speed throughput when handling 512-byte and 64-byte packets, respectively.

SINGLE-RULE FIREWALL LATENCY

Latency testing revealed that the NetScreen-5200 exhibited lower latency for the majority of frame sizes tested (64, 512, 1,024 and 1,518 bytes) when compared to the Nokia IP740 and the Cisco PIX 535.

Latency tests run with 64-byte packets revealed that the NetScreen-5200 exhibits an average latency of 6.5 microseconds, which is 57% lower than the latency reported for the Cisco PIX 535 (14.9 μ s) and 65% lower than the Nokia IP740 (18.6 μ s). (See figure 2.) Even in 512-byte packet tests, the NetScreen-5200 enjoyed 31% less latency than the Cisco PIX 535 and 29% less than the Nokia IP740. At 1,518-byte packets, the largest tested packet size, results show latency of 39 μ s for the NetScreen-5200, versus 36 μ s for the Cisco PIX 535 and 48 μ s for the Nokia IP740.

BIDIRECTIONAL THROUGHPUT ACROSS A FULL-DUPLEX VPN TUNNEL USING 3DES AND SHA-1

Testing demonstrated that with a single tunnel (Security Association) and <0.001% packet loss, the NetScreen-5200 obtained a zero-loss throughput

of 700 Mbit/s (or 35% of the 2 Gbit/s theoretical maximum with 64-byte packets), which was a 24X improvement over the Cisco PIX 535 aggregate throughput of 29.5 Mbit/s when measured in a test scenario with 64-byte packets and 1% packet loss¹. (See figure 3.) As the packet size increased, so did the delta between the two products. At 512-byte packets, the NetScreen-5200 passed 83% of the theoretical maximum, or 1.65 Gbit/s, compared to 4.1% of the theoretical maximum with the Cisco PIX 535, which passed just 82.4 Mbit/s of traffic across the single tunnel in the 512-byte packet test.

(The Nokia IP740 firewall did not participate in the VPN testing due to a lack of equipment.)

At 1,024-byte packets, the NetScreen-5200 attained zero-loss throughput at 94% of the theoretical maximum, or 1.88 Gbit/s, whereas the Cisco PIX 535 reached only 5% of the theoretical max, or 102 Mbit/s.

In the 1400-byte packet test, the NetScreen-5200 achieved an aggregate throughput across a single VPN tunnel of 1.93 Gbit/s, or 96.6% of the theoretical maximum throughput. The Cisco PIX 535, by contrast, delivered just 110 Mbit/s of aggregate throughput equal to 5.5% of the theoretical maximum throughput across a single tunnel with 3DES and SHA-1.

When the IPSec overhead of 50 bytes per packet is taken into account, the NetScreen-5200 obtained a zero-loss throughput of 56% of the theoretical maximum with 64-byte packets versus just 2% of theoretical maximum for the Cisco PIX 535. At 512-byte packets, the NetScreen-5200 passed 90% of the theoretical maximum, compared to just 5% for the Cisco PIX 535. At 1,024-byte packets, the NetScreen-5200 achieved zero-loss VPN throughput at 99% of theoretical maximum versus

¹ Tolly Group engineers used a 1% packet-loss tolerance for the Cisco PIX 535 and the Nokia IP740 to maintain an apples-to-apples performance comparison with results from a previous NetScreen-Cisco head-to-head evaluation. The NetScreen-5200 was tested at the <0.001% packet-loss level.

**NetScreen
Technologies, Inc.**

NetScreen-5200

**Competitive
Evaluation of
Internet Security
Devices**



**NetScreen Technologies, Inc.
NetScreen-5200
Product Specifications***

Performance Features

- 1,000,000 concurrent sessions
- 25,000 new sessions/second
- Up to 4 Gbit/s firewall throughput, 2 Gbit/s 64-byte packets
- Up to 2 Gbit/s 3DES (168-bit) throughput, 1 Gbit/s 64-byte packets (3DES, MD5)
- 40,000 policies

Virtual Systems

- Up to 500 Virtual Systems
- Up to 500 Virtual Routers
- 4,000 VLANs

Mode of operation

- Transparent mode support on all interfaces
- Route mode supported on all interfaces
- NAT supported per policy and per interface on all interfaces
- Unrestricted number of users per port

VPN

- 25,000 dedicated concurrent tunnels
- Manual key, IKE, and PKI (X.509)
- AES, 3DES, DES
- SHA-1, MD5
- Star (hub and spoke) and full-mesh VPN network topology
- IPSec NAT Traversal
- L2TP within IPSec

High Availability

- Firewall session and VPN synchronization
- Device failure detection
- Link failure detection
- Network notification on fail-over
- Encrypted HA traffic and dedicated HA ports

Firewall and VPN user authentication

- Built-in internal database (25,000 user limit)
- RADIUS, RSA SecurID or LDAP external databases

Traffic Management

- Maximum bandwidth per interface
- DiffServ stamp

For more information contact:

NetScreen Technologies, Inc.
350 Oakmead Parkway
Sunnyvale, CA 94085
(800) 638-8296
URL: <http://www.netscreen.com>

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

5% for the Cisco PIX 535. In the 1,400-byte packet test, the NetScreen-5200 achieved zero-loss VPN throughput at 100% of theoretical maximum versus 6% for the Cisco PIX 535.

VPN LATENCY

Engineers tested the latency incurred by each of the devices as they pass traffic across a single VPN tunnel with 3DES and SHA-1. The NetScreen-5200 demonstrated consistently lower latency results than the Cisco PIX 535.

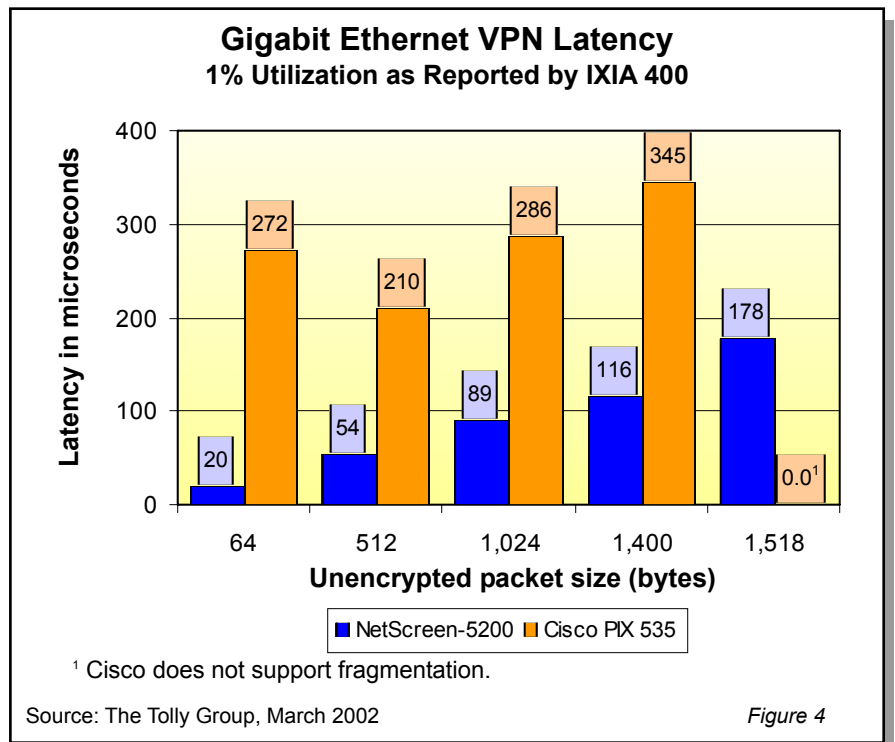
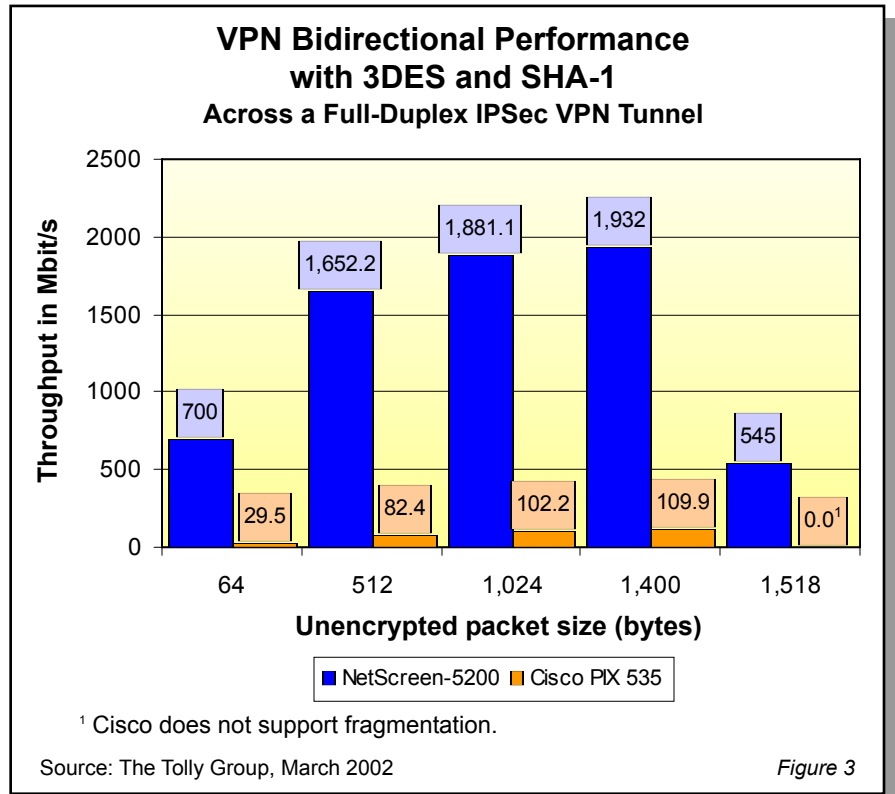
At 64-byte packets, the NetScreen-5200 demonstrated latency of 20 μ s, 93% lower than the 272 μ s of latency reported for the Cisco PIX 535. When testing 512-byte and 1,024-byte packets, the NetScreen-5200 exhibited 74% and 69% lower latency than the Cisco PIX 535. (See figure 4.)

At 1,400-byte packets, the NetScreen-5200 reported 116 μ s of latency, 66% lower than the 345 μ s of latency reported by the Cisco PIX 535. Testing of 1,518-byte packets was impossible due to the Cisco PIX 535's inability to fragment packets greater than the maximum Ethernet frame size, plus the overhead introduced by IPSec processing.

ANALYSIS

Enterprises and service providers looking to centralize their security deployments or intending to support multimedia, voice over IP and other latency-sensitive applications in a secure environment, realize that they must deploy multipurpose security devices that provide a consistently high-level of performance balanced against the backdrop of low latency.

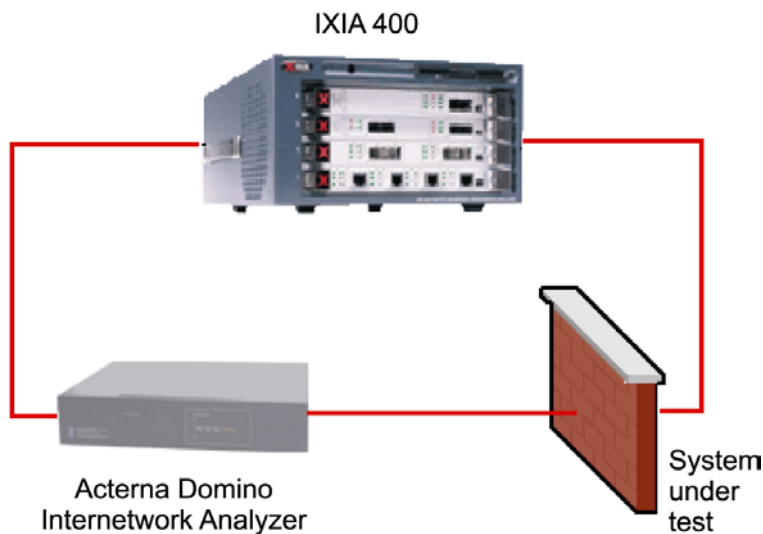
The NetScreen-5200 demonstrated repeatedly that it is capable of high throughput regardless of frame size, even as session loads scale to carrier-class proportions. Test after test proved that the NetScreen-5200 can handle high firewall and VPN tunnel loads, while competitive products from Cisco and Nokia sagged under the extra processing weight.



From a firewall perspective, even at a relatively low 1,000-session threshold, the NetScreen-5200 provided 16X the performance of the Cisco PIX 535 and 11X the performance of the Nokia IP 740 when tested at 64-byte packets. The performance gap

widened as engineers scaled up session load to 100,000 sessions; the NetScreen-5200 delivered 26X greater performance than the Cisco PIX 535 and 17X better performance than the Nokia IP740 when tested at 64-byte packets.

Firewall Throughput/Latency Test Bed



Source: The Tolly Group, March 2002

Figure 5

Clearly, as the session loads scaled up to 100,000 sessions, the performance of the NetScreen-5200 did not waver from the 2 Gbit/s wire-speed while the Cisco and Nokia devices achieved just 78 Mbit/s and 116 Mbit/s. From a firewall latency viewpoint, the NetScreen-5200 delivers up to 65% less latency than the rival products, proving it can offer consistent throughput **and** low latency.

On the VPN gateway side, the NetScreen-5200 delivered 700 Mbit/s across a single tunnel (SA) while handling the taxing 64-byte packets – that’s a 24X improvement over the Cisco PIX 535 at 29.5 Mbit/s. And as packet sizes across the VPN tunnel increase, so does the NetScreen-5200’s throughput on up to 1.93 Gbit/s at 1400-byte packets versus just 110 Mbit/s for the Cisco PIX 535.

On the VPN side, latency too is in favor of the NetScreen-5200. With 64-byte packets, the NetScreen-5200 reached a latency of 20 μ s, or 93% less than the Cisco device. Even at 1,400-byte packets the NetScreen-5200 offers 66% less than the Cisco PIX 535. Again, NetScreen demon-

strates it can deliver the tandem of consistent high-throughput along with low latency. That is a tandem that is worth consideration from enterprise network users and service providers, especially since tests show that the throughput results track consistently as session counts rise up to 500,000 sessions.

TEST CONFIGURATION AND METHODOLOGY

The Tolly Group tested a NetScreen Technologies, Inc. NetScreen-5200 enterprise-class Internet security device equipped with eight (8) Gigabit Ethernet interfaces and running firmware version 3.1.0b3.1 configured as a single rule, allow-all firewall with NAT in idle mode. Engineers also tested a Cisco Systems, Inc. PIX 535, PIX Version 6.1(3), and a Nokia IP740, Version release 87712.15.2001-064400, running Check Point Software FireWall-1, Version 5.0 SP1, each similarly outfitted. VPN testing required a second unit of each device under test in order to create the VPN tunnel; engineers tested only the NetScreen-5200 and the Cisco PIX 535 in the VPN

tunnel configuration since only one Nokia IP740 was available.

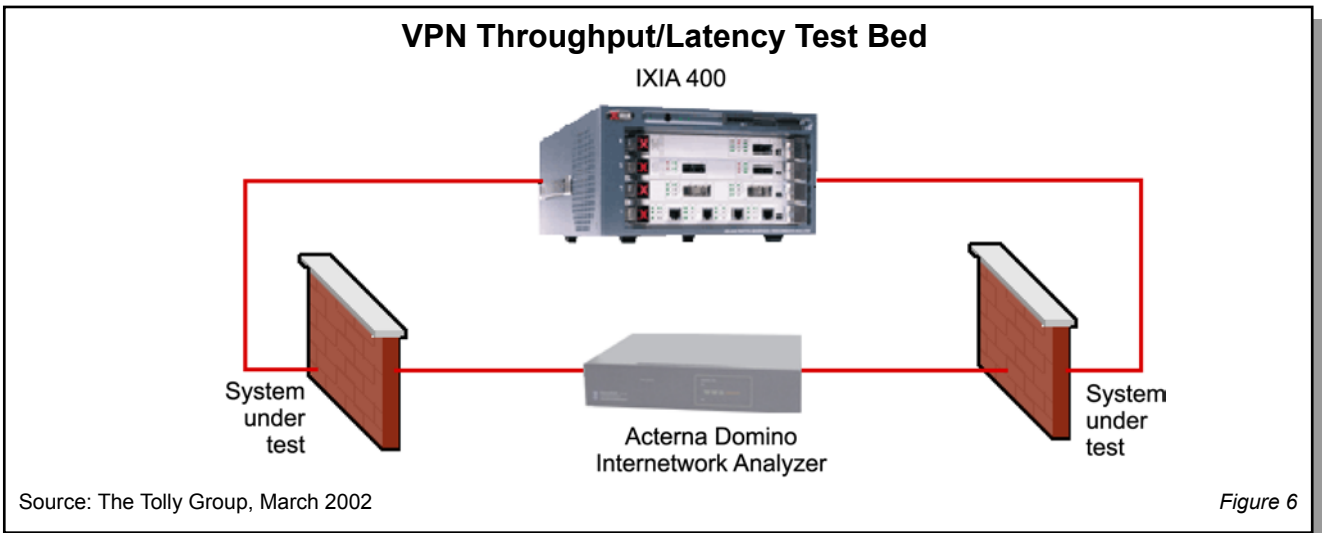
Each of the firewalls connected to an IXIA 400 traffic generator with Gigabit fiber connections. One connection simulated the internal or trusted domain, while the other simulated an external or untrusted domain. (See figure 5.) Engineers tested the NetScreen-5200 and the Cisco PIX 535 devices in a VPN configuration by connecting a single Gigabit Ethernet interface on the devices under test (DUTs) to the Ixia and the second interface on the DUTs connected to each other. (See figure 6.) During prototype testing, an Acterna DA-380 Domino Internetwork analyzer sat in line to validate the encrypted traffic flow between devices.

Using the Ixia, engineers generated UDP traffic of a specific frame size from the untrusted domain to the trusted domain and conversely at various session loads for a test duration of 60 seconds. Upon completion of each test run, engineers compared the total transmitted packets to those received and packet loss was calculated. If the packet loss was greater than the tolerance set for the test run, engineers adjusted the offered load in 1% decrements until zero loss was achieved. Testing for VPN throughput was accomplished using the same approach, except that the test bed layout was modified in order to create the secure tunnel.

Engineers conducted latency tests as defined in the RFC2544 test suite. Traffic was generated at 1% of the theoretical maximum for the various frame sizes tested in both firewall and VPN configurations.

EQUIPMENT ACQUISITION AND SUPPORT

The Cisco PIX 535 and the Nokia IP740 were acquired through normal product distribution channels. The



Tolly Group contacted executives at the vendor companies and invited them to provide a higher level of support than available through normal channels. While Nokia executives

inquired about test details, neither Nokia nor Cisco participated in providing technical support, which in fact was not needed to configure/tune the devices for the test suites executed by

The Tolly Group. Results were shared with the competitive vendors who neither acknowledged nor disputed the results.

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

| Vendor | Product | Web address |
|--------------|---------------------------------|---|
| Acterna Corp | Domino Internetworking Analyzer | http://www.acterna.com |
| Ixia | IXIA 400 | http://www.ixiacom.com |
| Ixia | IXIA ScriptMate | http://www.ixiacom.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: www.tolly.com/About/ftc.asp

PROJECT PROFILE

Sponsor: NetScreen Technologies, Inc.

Document number: 202121

Product class: Enterprise-class Internet security system

Products under test:

- NetScreen-5200, ScreenOS version 3.1.0b3.1
- Cisco PIX 535UR, PIX Version 6.1(3)
- Nokia IP740, Version releng 87712.15.2001-064400, Check Point Software FireWall-1, Version 5.0 SP1

Testing window: March 2002

Software status:

- Generally available

Additional information available:

- Technical Support Diary

For more information on this document, visit our Web site at <http://www.tolly.com>, send E-mail to info@tolly.com, or call (732) 528-3300.

Internetworking technology is an area of rapid growth and constant change. The Tolly Group conducts engineering-caliber testing in an effort to provide the internetworking industry with valuable information on current products and technology. While great care is taken to assure utmost accuracy, mistakes can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental, and consequential damages which may result from the use of information contained in this document. All trademarks are the property of their respective owners.

The Tolly Group doc. 202121 rev. clk 03 May 02