THE TOLLY GROUP

No. 201111 July 2001

NetScreen Technologies Inc.

NetScreen-500 vs. Cisco Systems Inc. PIX 535

Competitive Evaluation of Enterprise-Class Internet Security Devices

Test Summary

Premise: *IT managers concerned with implementing network security infrastructure for E-businesses, enterprises, and service providers must consider a system capable of scalability. Information security professionals implementing security for enterprise customers and service providers need to ensure that network performance will not suffer degradation when implementing a firewall device providing both security and cryptography of sensitive information.*

NetScreen Technologies commissioned The Tolly Group to benchmark the NetScreen-500, a purpose-built Internet security system outfitted with Gigabit Ethernet interfaces, and to compare the results with those of a similarly outfitted Cisco PIX 535 firewall outfitted with an optional VPN Accelerator Card. For both 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. Both devices under test were subjected to a range of session loads, escalating from 1,000 sessions to 25,000 sessions.

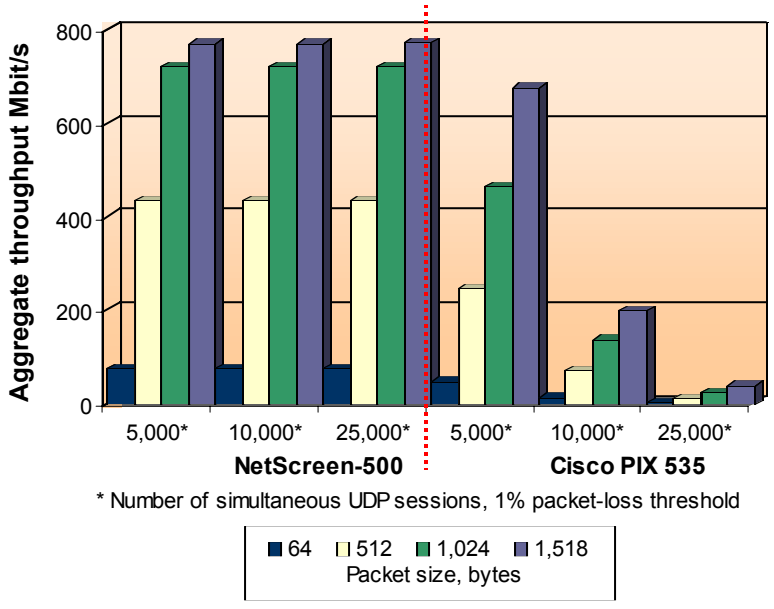
For zero-loss performance tests, The Tolly Group measured the steady-state throughput where loss was less than 0.001%, the same stringent metric that The Tolly Group employs to test Layer 2 and Layer 3 devices. While the NetScreen-500 exhibited no difference in throughput characteristics with a 0.001% packet-loss threshold, the Cisco PIX 535 was unable to perform at the same packet-loss threshold, which is easily achieved by workgroup-class Layer 2

Test Highlights

- Delivers 750 Mbit/s of bidirectional firewall throughput, even with 25,000 active sessions and a 0.001% packet-loss threshold versus just 2 Mbit/s for a Cisco PIX 535 with 1,000 sessions
- Achieves 110% more bidirectional throughput than Cisco PIX 535 with 1,400-byte packets and pumps 59% more data with 512-byte frames over a VPN tunnel with 3DES and SHA-1
- Processes more than 126 Mbit/s of zero-loss bidirectional throughput with 1,518-byte frames over a VPN tunnel employing 3DES and SHA-1, while Cisco PIX 535 discards large frames due to lack of fragmentation support
- Delivers up to 49% lower firewall latency and up to 54% lower latency over VPN tunnels than the Cisco PIX 535

Zero-Loss Throughput Across a "Single-Rule" Firewall with UDP Packets

Bidirectional Traffic, Full-Duplex Gigabit Ethernet



Source: The Tolly Group, July 2001

Figure 1

and Layer 3 switches. In fact, during initial zero-loss throughput tests, the Cisco PIX 535 achieved less than 2 Mbit/s of aggregate throughput over a full-duplex Gigabit Ethernet connection. Engineers consequently were forced to employ a 1% packet-loss threshold to obtain useable performance results for comparison with the NetScreen-500.

Test results show that the NetScreen-500 consistently offers superior performance to the Cisco device, even under heavy session loads. Testing was performed in April 2001.

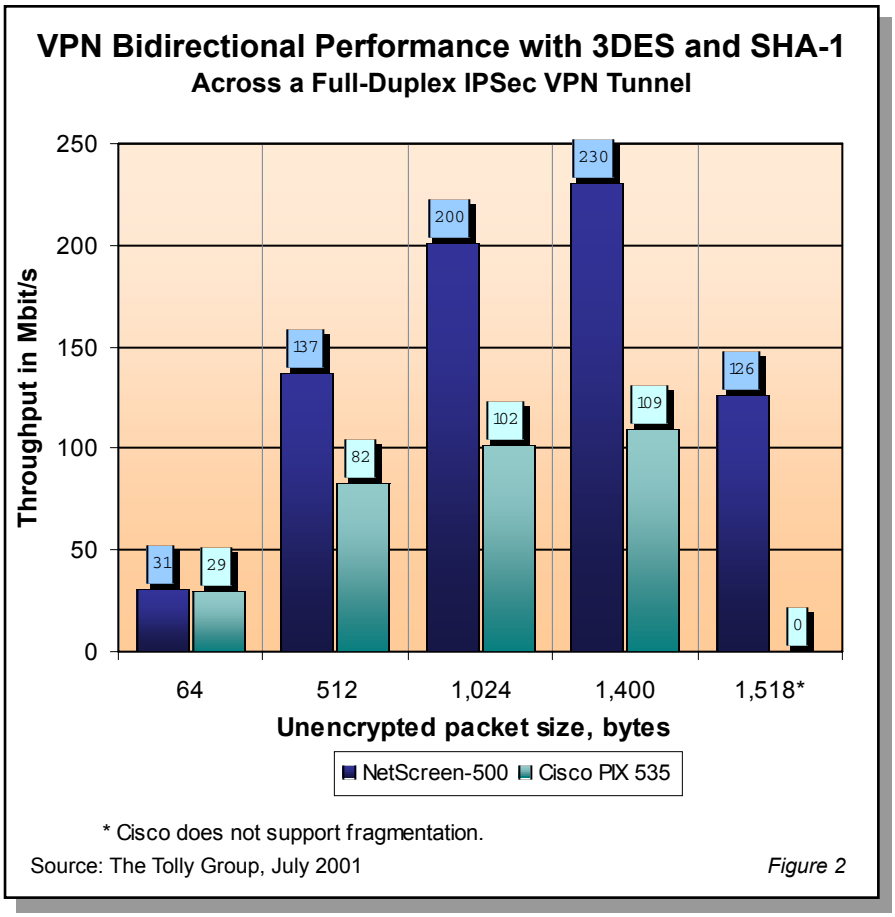
Results

Single-Rule Firewall Bidirectional Performance

Prototype testing demonstrated that a packet-loss tolerance of 0.001% was too demanding for the Cisco PIX 535. When engineers tested the Cisco device in a scenario with 1,518-byte frames and 1,000 sessions, the PIX 535 achieved just 2 Mbit/s of bidirectional throughput compared to the NetScreen-500, which delivered 757.4 Mbit/s of bidirectional throughput in a scenario supporting 25,000 simultaneous UDP sessions. UDP is a connectionless protocol, however state is maintained on the firewall for all "sessions" of the source-destination IP port pair.

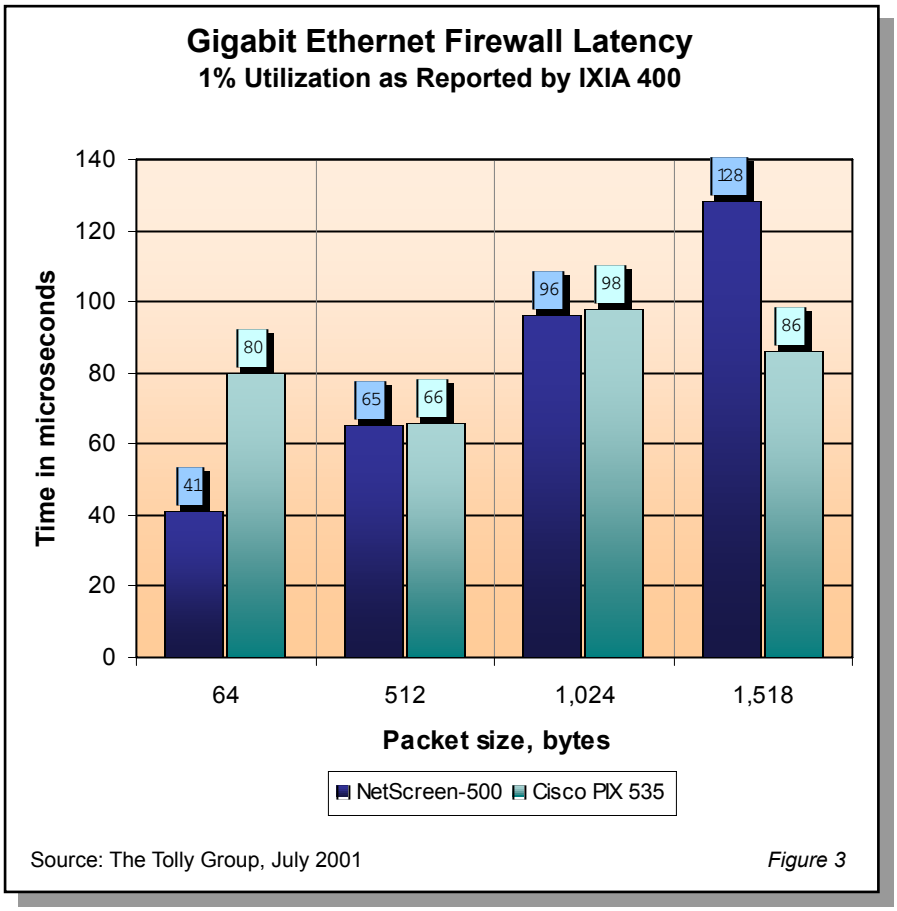
Upon reviewing the results, the testing team decided to use a 1% packet-loss tolerance for production testing to accommodate the high loss rates of the Cisco PIX 535. While such a loss-rate threshold likely would not be tolerated in production networks, it was required in order to get the Cisco device to complete the test and produce significant throughput.

As expected, testing at a 1% packet-loss tolerance, the NetScreen-500 exhibited similar performance across all four packet sizes tested, regardless of the session load. Additionally, the throughput figures obtained for the 1% packet-loss tolerance when compared to those of the more strin-



* Cisco does not support fragmentation.

Source: The Tolly Group, July 2001 *Figure 2*



Source: The Tolly Group, July 2001 *Figure 3*

gent packet-loss tolerance of 0.001%, showed no difference in throughput characteristics.

At 5,000 sessions, the NetScreen-500 demonstrated results that were between 13% and 76% higher than those of the Cisco PIX 535. At 10,000 sessions, the NetScreen-500 results ranged between 285% and 516% greater than the Cisco PIX 535 results – 769 Mbit/s for the NetScreen-500 when handling 1,518-byte frames and 10,000 sessions versus 199 Mbit/s for the Cisco PIX 535 under the same loading conditions (see figure 1). Finally at 25,000 sessions, the NetScreen-500 had between 18 and 25 times greater throughput than the Cisco PIX 535 – 770 Mbit/s for the NetScreen-500 when handling 1,518-byte frames and 25,000 sessions versus 39 Mbit/s for the Cisco PIX 535 under the same loading conditions.

Subsequent investigations into the performance disparities across tests run with 1,000, 5,000, 10,000 and 25,000 sessions, revealed a bug known to Cisco. Identified by Cisco as ID CSCdt86736, the Cisco bug report states that at 30-second intervals when 2,000 to 4,000 sessions are present the PIX will stop forwarding traffic for about four seconds.

This means that in the 60-second test duration – approximately four seconds, or almost 7% of the time, is spent pausing and passing no traffic.

Bidirectional throughput across a full-duplex performance VPN tunnel using 3DES and SHA-1

Testing demonstrated that with a single Security Association and a 1% packet-loss tolerance, the NetScreen-500 achieved a zero-loss throughput of 30.92 Mbit/s with an unencrypted input stream of 64-byte packets — 5% greater than Cisco's 29.36 Mbit/s (see figure 2). As the packet size increased, the performance gap widened between the two products.

With 512-byte packets of unencrypted traffic entering the device under test, the NetScreen-500 passed 136.71 Mbit/s compared to the Cisco PIX 535, which handled 41% less traffic, or 80.06 Mbit/s.

At 1,024-byte packets, the NetScreen-500 passed 200.5 Mbit/s while Cisco's PIX 535 passed 101.58 Mbit/s bidirectionally. With 1,400-byte packets, the NetScreen-500 exhibited a 110% increase over the Cisco PIX 535 with 230.3 Mbit/s vs. 109.1 Mbit/s.

Finally, the most significant difference between the products occurred when we conducted a zero-loss test of 1,518-byte packets. When using a VPN configuration with 3DES, SHA-1, the encapsulation of the packet adds additional header information and increases the size of the packet. With 1,518-byte packets, the encapsulated packet size is larger than maximum Ethernet allowable frame size and requires packet fragmentation, which the Cisco PIX 535 does not support. Therefore, the PIX 535 achieved zero throughput with 1,518-byte packets, compared to the NetScreen-500's 126.4 Mbit/s zero-loss throughput.

Single Rule Firewall Latency Performance

Latency testing revealed that the NetScreen-500 exhibited lower latency for 64-, 512- and 1,024-byte frames than the Cisco PIX 535. Latency results for 64-byte frames show the NetScreen-500 with an average latency of 40.8µs (microseconds), 49% lower than the PIX 535 at 80.2µs (see figure 3). Results of both the 512- and 1,024-byte frames showed the NetScreen-500 having only a slight (2% lower) advantage in reported latency times with 64.9µs and 95.8µs respectively. Cisco reported latency of 65.3µs and 98µs for the same. Testing of the 1,518-byte frames showed Cisco obtaining a 33% lower average latency with an 85.5µs than NetScreen's 128.5µs.

NetScreen Technologies, Inc.

NetScreen-500

Internet Security Device Competitive Performance Evaluation

NetScreen-500
Product Specifications*

Performance
- 250,000 concurrent sessions
- 22,000 new sessions/second
- 700 Mbit/s firewall throughput
- 250 Mbit/s 3DES (168-bit) throughput
- 20,000 policies
- 256 schedules

Virtual systems
- Up to 25 Virtual Systems
- 100 VLANs

Mode of operation
- Transparent mode support
- Route mode supported
- NAT (Network Address Translation) supported
- PAT (Port Address Translation) supported
- Unrestricted number of users per port

VPN
- 10,000 dedicated tunnels
- Manual key, IKE, and PKI (X.509)
- 56-bit DES & 168-bit 3DES (IPSec)
- SHA-1 and MD5
- Star (hub and spoke) VPN network topology
- L2TP

High availability
- Session protection for firewall and VPN
- Device failure detection
- Link failure detection
- Network notification on fail-over

Firewall & VPN user authentication
- Built-in internal database (15,000 user limit)
- RADIUS, RSA SecureID, or LDAP (external) databases

Traffic management
- Guaranteed and maximum bandwidth
- Priority-bandwidth utilization
- DiffServ stamp

For more information, contact:
NetScreen Technologies, Inc.
350 Oakmead Parkway
Sunnyvale, CA 94085
(800) 638-8296
(408) 730-6000
URL: http://www.netscreen.com

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

VPN Latency Performance

Tests of firewall latency in a VPN configuration demonstrated that the NetScreen-500 has consistently lower latency than the rival Cisco PIX 535. At 64-byte frames, the NetScreen-500 demonstrated latency of 164.3µs — or 64% lower than Cisco's PIX 535 latency of 467.4µs. (See figure 4.)

When testing frame sizes of 512-bytes and 1,024-bytes, the NetScreen-500 demonstrated 41% and 49% lower latency than the Cisco product, respectively.

Tests of 1,518-byte packets were impossible to execute in the current configuration due to the PIX 535's inability to fragment frames greater than the maximum Ethernet frame size. Due to this limitation, testing in the VPN configuration also was performed using 1,400-byte frames. With 1,400-byte frames, the NetScreen-500 again obtained 50% lower latency scores reporting 371µs compared to the Cisco PIX 525's 749µs of latency.

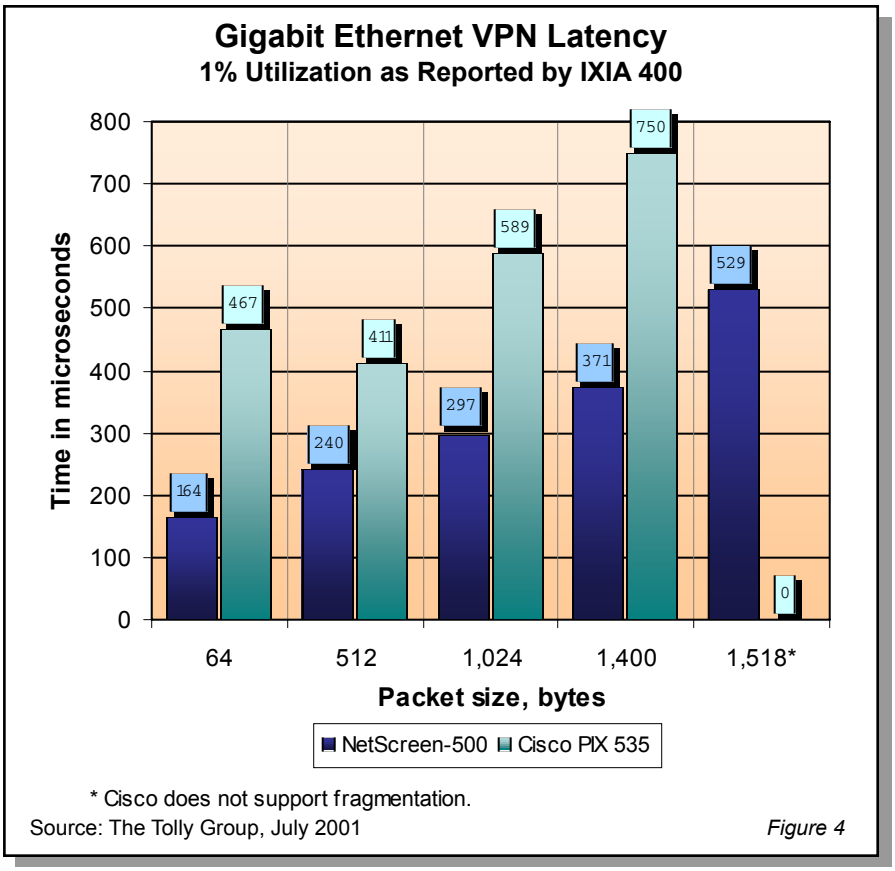


Figure 4

Analysis

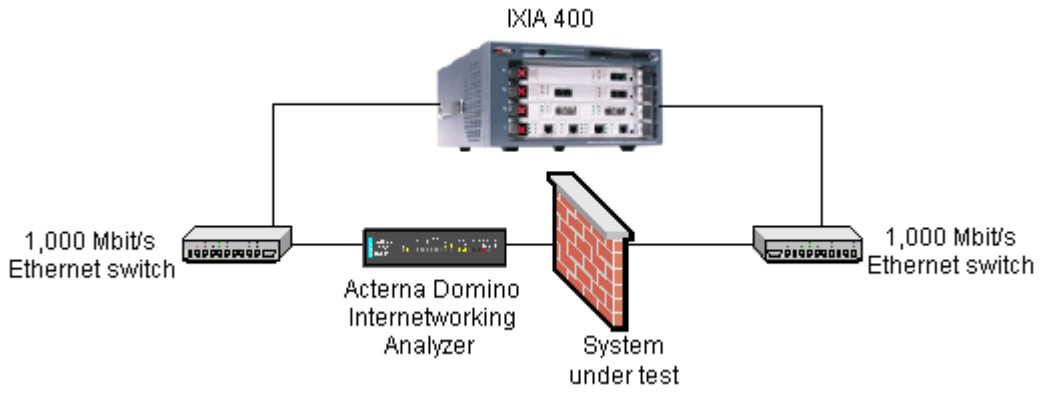
The NetScreen-500 in a firewall configuration demonstrates consistent throughput characteristics regardless of session loading and packet-loss tolerances. Cisco's PIX 535 firewall performs adequately in the baseline testing of 1,000 sessions, but when additional sessions are added, attempting to simulate session loads found on an enterprise firewall with Gigabit Ethernet interfaces, throughput plummets. Cisco has identified a related 'bug' in its knowledgebase. In its own bug report, Cisco admits, "At 30 second intervals the pix [sic] will stop forwarding for about 4 seconds." We observed this when session loads grew greater than 2,000 sessions, however Cisco had not released a patch or fix for the problem as of July 2001. Such a phenomenon may, in extreme cases, lead to session timeouts.

More troubling, is the inability of the Cisco device to perform at packet-loss thresholds easily achieved by even workgroup-class Layer 2 and Layer 3 switches. Customers who secure their networks with such devices likely will experience degradation to end-user session performance in times of heavy loading caused in part by the session resynchronization that will be required when packets are discarded.

Moreover, the Cisco PIX 535 exhibited performance limitations when tested over a secure VPN tunnel. Adding to the Cisco PIX 535's woes, the device does not support large-frame segmentation. When we attempted to test device throughput at 1,518-byte frames with additional 3DES and SHA-1 frame overhead, the Cisco 535 simply discarded packets instead of supporting fragmentation. When the overhead attributable to 3DES and SHA-1 processing exceeds the largest Ethernet frame size of 1,518 bytes, segmentation chops the frame into two separate frames for transmission. The PIX 535's lack of segmentation support poses a serious downside to users who wish to support large file transfers across a firewall. Moreover, the lack of segmentation support could lead to serious problems maintaining VPN tunnels. Discarding Ethernet's largest frame size means that the network devices will be forced to retransmit where necessary, which could result in elevated levels of network congestion. Moreover, such a condition would lengthen the time required for user downloads, which stresses applications and user limits, and in extreme cases may result in session timeouts. In some cases, the actual impact may be even worse. If, for some reason, an application is set to use 1,518-byte packets, it simply will not be able to communicate across the Cisco device since retransmissions of 1,518-byte packets are just discarded.

From a pure throughput perspective, the NetScreen-500 repeatedly outclassed the Cisco PIX 535 despite changes to frame size and session loading. VPN testing revealed similar throughput results for both products at the smallest packet size of 64

Firewall Throughput Test Bed



Source: The Tolly Group, July 2001

Figure 5

bytes. However, testing of the larger packet sizes is where we observed the NetScreen-500 excel with throughput that is up to 70% greater for 512-byte packets, jumps to nearly double for 1,024-byte packets, and more than doubles for 1,400-byte packets. The addition of the 1,400-byte packets was required to have some larger packet size latency figures since the PIX 535 does not fragment Ethernet frames when the encapsulated 1,518-byte packet is larger than the largest maximum Ethernet frame size.

The NetScreen-500 firewall delivered latency figures that were comparable or better than those of the Cisco for packet sizes up to and including 1,024-bytes. When tested with the 1,518-byte packets, the Cisco PIX 535demonstrated slightly lower latency then that of NetScreen. However, testing of the VPN configuration displayed the NetScreen-500 to exhibit latency times of almost half those collected for Cisco with 512-, 1,024- and 1,400-byte packets and only one quarter of the time for 64-byte packets.

Related Tests

In January 2001, The Tolly Group published a competitive evaluation of the NetScreen-100 versus a trio of rival products from Check Point Software Technologies, Cisco Systems, Inc. and Nokia Corp. The report, document 200225, is available on The Tolly Group Web site.

Test Configuration and Methodology

For performance tests, The Tolly Group tested a NetScreen-500, enterprise-class Internet security device equipped with Gigabit Ethernet interfaces and running firmware version 2.6.0 Beta 3 configured as a single rule, allow-all firewall with Network Address Translation (NAT) in idle mode. Engineers also tested a Cisco Systems Inc. PIX 535, a similarly outfitted and configured device running IOS version 5.3 (see figure 5). VPN testing required a second unit of each of the two devices under tests in order to create the VPN tunnel.

Each of the firewalls was connected to an IXIA 400 traffic generator with two Gigabit Ethernet connections. One connection simulated the internal or trusted domain, while the other simulated an external or untrusted domain. Engineers tested the devices in a VPN configuration by connecting a single Gigabit Ethernet interface on each of the two devices to the IXIA 400 and the second interface on the devices under test were connected to each other (see figure 6). During prototype testing, an Acterna DA-380 DominoGigabit InterNetwork Analyzer was placed in line to validate the encrypted traffic flow between VPN devices.

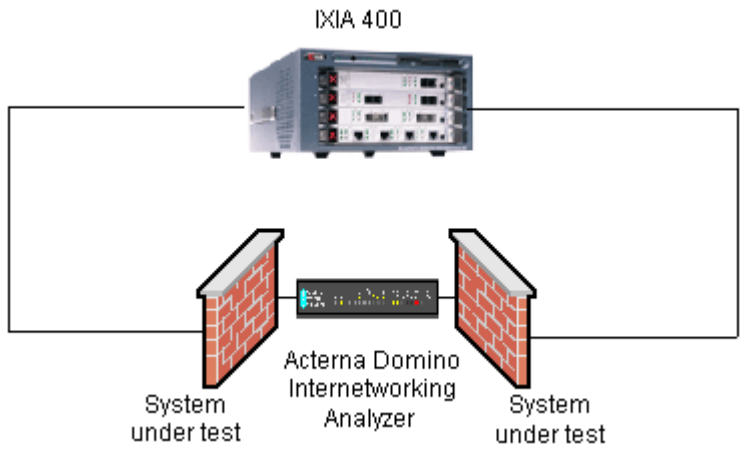
Using the IXIA 400 and a throughput test defined in the RFC2544 test suite, engineers generated UDP traffic of a specific frame size from the untrusted domain to the trusted domain and conversely at various session loads for test durations of 60 seconds. Upon completion of each test run, engineers compared 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 used a binary search algorithm to determine the next offered load and the test sequence repeated. This continued until the 'zero loss' was obtained. Testing for VPN throughput was accomplished using the same approach, only the test bed layout was modified in order to create the secure tunnel.

Latency testing was completed using the IXIA 400 and the latency test also defined in the RFC2544 test suite. While generating traffic at 1% of the theoretical maximum, latency calculations of the various frame sizes were obtained and reported. This was completed in both the firewall and VPN configurations.

Equipment Acquisition and Support

The Tolly Group obtained the Cisco PIX 535 through normal distribution

Firewall Latency Test Bed



Source: The Tolly Group, July 2001 *Figure 6*

channels. The Tolly Group contacted executives at Cisco Systems and invited them to provide a higher level of support than available through normal channels. The Tolly Group did not receive a response from Cisco and proceeded using standard support channels where appropriate.

Upon completion of the testing, The Tolly Group provided the results to Cisco's VPN and Security product line press relations contact for review. Cisco responded to the test results with some question regarding software versions used. Upon supplying the information to Cisco they corroborated that the level of code used for testing was appropriate. For further details regarding the interactions The Tolly Group had with Cisco, check out the Technical Support Diary for Competitive Products Tested posted on The Tolly Group's World Wide Web site at http://www.tolly.com. See document 201111.

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

Vendor	Product	Web address
Acterna Corp.	Domino DA-380	http://www.acterna.com
IXIA	IXIA 400	http://www.ixiacom.com

Since its inception, The Tolly Group has produced high-quality tests that meet three overarching criteria: All tests are objective, fully documented and repeatable.

We endeavor to provide complete disclosure of information concerning individual product tests, and multiparty competitive product evaluations.

As an independent organization, The Tolly Group does not accept retainer contracts from vendors, nor does it endorse products or suppliers. This open and honest environment assures vendors they are treated fairly, and with the necessary care to guarantee all parties that the results of these tests are accurate and valid. The Tolly Group has codified this into the Fair Testing Charter, which may be viewed at http://www.tolly.com.

Project Profile

Sponsor: NetScreen Technologies, Inc.
Document number: 201111
Product Class: Enterprise-class Internet security device
Products under test:
- NetScreen-500
- Cisco PIX 535

Testing window: April 2001
Software versions tested:
- NetScreen: Version 2.6.0 beta 3
- Cisco: IOS v.5.3

Software status:
- Generally available

Additional information available:
- Technical Support Diary - Yes
- Configuration Files
- Data Files

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. 201111 rev. clk 03 July 01