THE TOLLY GROUP

No. 205120 June 2005

NETASQ

NETASQ F2000 IPS-Firewall

Multiservice Security Appliance Performance Evaluation

TOLLY 16 YEARS 1989-2005 Test Summary

Premise: *It is essential that today's firewall and other security devices all provide a multi-layered approach that stops network- and content-based threats at the edge of the network without compromising performance or requiring additional hardware. IPS and firewall appliances must offer optimum throughput and low latency to ensure that security processing does not become a network bottleneck.*

NETASQ commissioned The Tolly Group to evaluate its NETASQ F2000 IPS-Firewall, a purpose-built network security appliance that combines real-time intrusion prevention, firewall service, IPSec virtual private networking (VPN), clientless SSL VPNs, advanced content filtering, anti-spam, antivirus and other integrated security services.

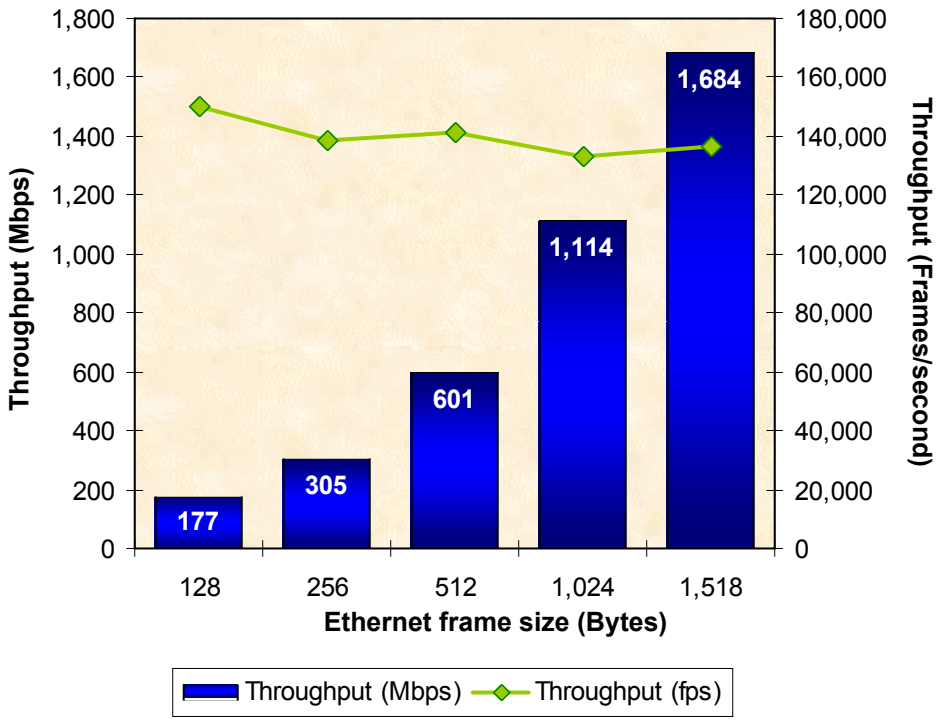
Tolly Group engineers focused testing on the performance of the NETASQ F2000 using a mostly default configuration, measuring the device's zero-loss throughput (while IPS services were active), benchmarking latency introduced by the device under varying traffic loads and conditions. (In its default state, the NETASQ F2000 enables protocol analysis and signature and port-scan detection, among other IPS capabilities.) Tests were conducted at The Tolly Group's Boca Raton, FL. facilities in May 2005.

Test results show that the NETASQ F2000 delivers Gigabit-class zero-loss Layer 2 throughput performance when tested at large frame sizes and an average of 777 Mbps of throughput across all frame sizes tested. The NETASQ F2000 generally introduced extremely low latency.

Test Highlights

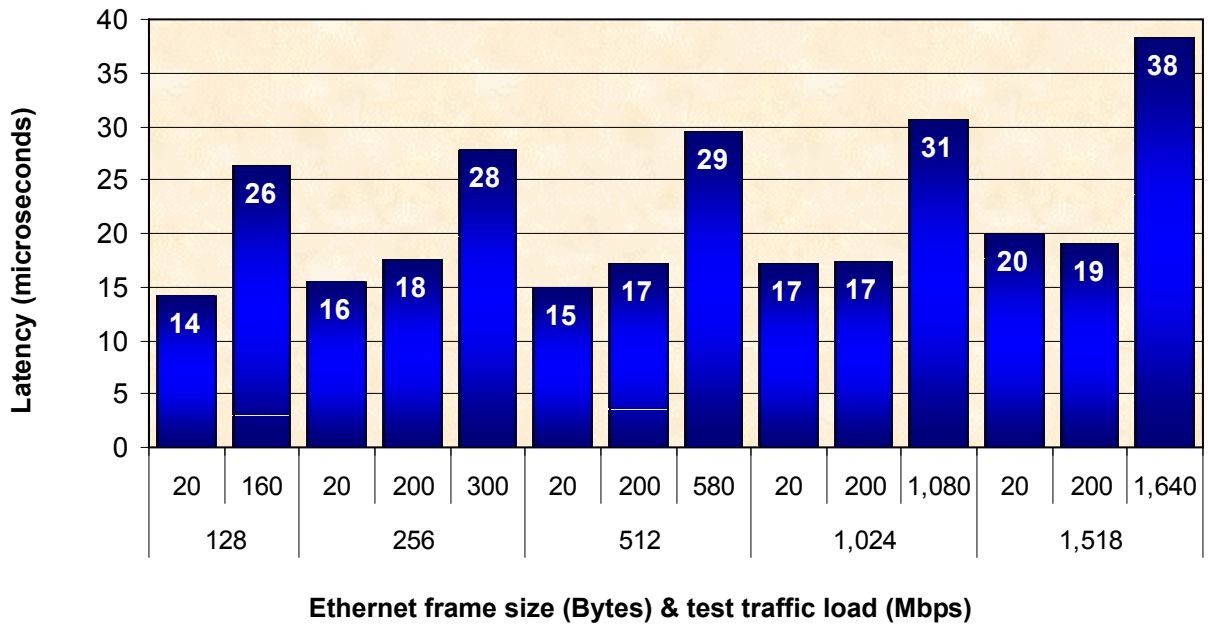
- Delivers aggregate zero-loss bidirectional throughput of 1.7 Gbps when handling 1,518-byte frames and 178 Mbps when handling the more taxing 128-byte frame size
- Introduces extremely low latency for IPS, ranging from 14 microseconds with 128-byte frames to 38 microseconds with 1,518-byte frames even at the maximum zero-loss traffic load

Zero-loss (≤0.001) Aggregate Ethernet Throughput
Across NETASQ F2000 in a Dual Gigabit Ethernet Interface Configuration as Reported by SmartBits SmartFlow



Source: The Tolly Group, May 2005

Figure 1



Source: The Tolly Group, May 2005

Figure 2

Results

Layer 2 Zero-Loss Throughput

Engineers measured the zero-loss (≤ 0.001%) bidirectional aggregate Layer 2 throughput using Ethernet frame sizes ranging from 128 bytes up to 1,518 bytes in a single-segment or dual Gigabit Ethernet (GbE) interface configuration. Throughput was measured while the NETASQ F2000 IPS engine was active, meaning it was constantly deep inspecting for the malicious traffic. During the test, bidirectional stateless traffic from a SmartBits packet generator flowed across the NETASQ F2000 IPS-Firewall. The NETASQ F2000 delivered bidirectional throughput of 1.64 Gbps when handling 136,832 frames per second (fps). When tested with a 128-byte frame size, the NETASQ F2000 delivered 178 Mbps of aggregate zero-loss throughput, when handling 149,914 fps. (See Figure 1.)

Average Latency

Engineers measured the average latency of the NETASQ F2000 across a variety of frame sizes and varying offered loads. Tests show that the NETASQ F2000 introduces extremely low latency ranging from 14 microseconds to 38 microseconds for different offered loads and different frame sizes.

Under relatively light traffic loads of 20 Mbps, the NETASQ F2000 introduced from 14 microseconds to 20 microseconds of latency. When the traffic load was increased to 200 Mbps, latency ranged from 17 to 19 microseconds. (See Figure 2.)

Finally, when the traffic load was ramped up to maximum traffic loads without frame loss, which was determined from the above throughput test, the NETASQ F2000 introduced latency ranging from 28 to 38 microseconds.

Analysis

The NETASQ F2000 is designed for service provider and enterprise-class networks. As such, it must activate most of the security functionalities provided by the device by default and still deliver high performance coupled with low latency.

Throughput alone, though, is not a true arbiter of the overall device performance. Latency must be accounted for in the equation, too. Here, again, the NETASQ F2000 introduced very low latency. Tests, in fact, show that latency is relatively uniform even as traffic loads are increased and frame sizes vary. This is extremely low latency considering that the NETASQ F2000 monitors every incoming packet all the way up to the application level. This is important when supporting real-time applications, such as voice over IP (VoIP) and multimedia, over secure connections.

The 1.7 Gbps zero-loss throughput achieved by the NETASQ F2000 is in large measure is due to NETASQ's IPS design – Active Security Qualification (ASQ). ASQ provides context-based intrusion prevention by analyzing traffic from network up to application layer, while applying multiple methods to identify and block malicious traffic. ASQ does not employ proxies or pattern databases, but uses classes of attacks to guarantee accuracy in identifying and blocking attacks. Its kernel-mode approach allows ASQ to screen traffic at wire speed without noticeable latency or performance drop. This unique concept takes maximum advantage of any hardware it's embedded in, providing real-time application layer intrusion prevention without degrading system performance.

Test Configuration and Methodology

For performance tests, The Tolly Group tested a NETASQ F2000 IPS-Firewall running firmware version: 6.0.5.

The F2000 was tested in in-line protection and bridge mode with mostly default out-of-the-box configurations for all tests. Engineers changed the rule set to "Pass All" and disabled the implicit rule. This configuration enables most IPS functionalities such as a stateful filtering, protocol analysis that blocks about 100 different classes of attacks (equivalent to more than 2,000 classical signatures), contextual signatures (~600), port-scan detection, according to NETASQ.

In the test bed, the F2000 was connected to a Spirent Communications SmartBits 6000B, which, in turn, was connected a SmartBits console running SmartFlow. The Blade Software IDS Informer was temporarily connected to the F2000 and configured to generate some of the attack traffic for the fact-check. This simple fact-check was to verify if the IPS module in the F2000 was up and running properly. (See Figure 4.)

In the stateless throughput test, SmartBits/SmartFlow was connected to the F2000 and configured to execute the test at the appropriate load, ranging from frame sizes of 128, 256, 512, 1,024 and 1,518 for a 60-second test duration at each iteration. Engineers configured the SmartBits to send and receive the test traffic (UDP packets) through the F2000 in a single-segment configuration in which two gigabit Ethernet interfaces on the tested device were utilized. Engineers used the binary search algorithm of SmartFlow to determine the maximum zero-loss (≤ 0.001%) throughput. They recorded the throughput as the Layer 2 received bps reported by SmartFlow. The test was repeated three times and the results were averaged.

Latency was measured in much the same manner as the stateless throughput, although engineers used three different offered loads for each frame size (20 Mbps aggregate, 200 Mbps aggregate and the maximum aggregate load without frame loss for each frame size except for 128-byte frame size). Engineers used a "store and forward latency" method for measuring latency.

NetASQ

NETASQ F2000 IPS-Firewall

Functionality and Performance

NETASQ
NETASQ F2000 IPS-Firewall
Product Specifications*

Hardware
- Up to 24 physical network segments
- Supports Gigabit interfaces
- Supports RAID1 hard disks
- Redundant power supplies

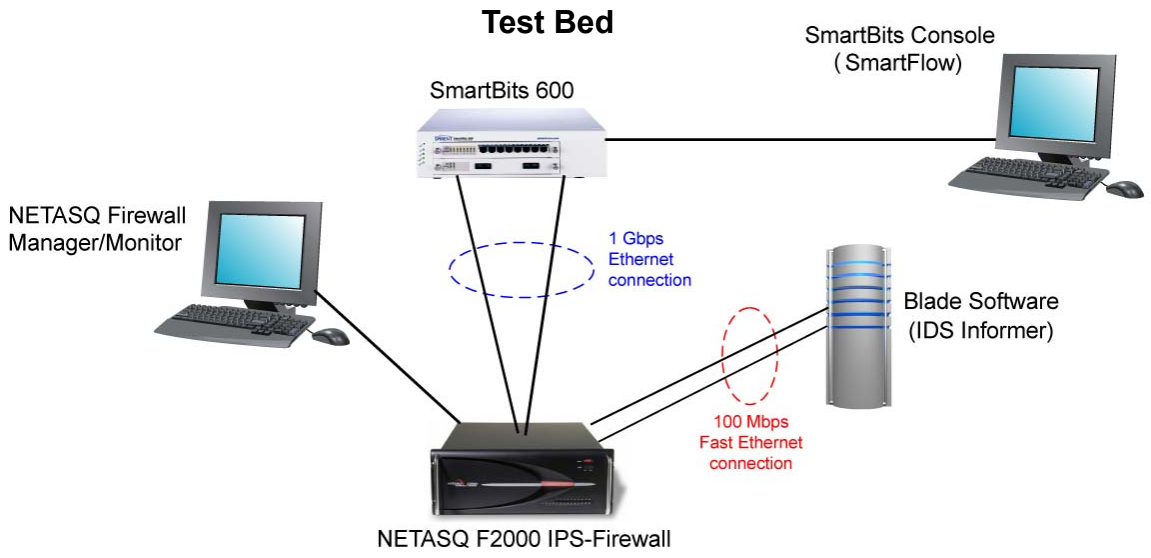
Intrusion Prevention
- Multi-layer and multi-method intrusion prevention system
- Protocol anomaly prevention (blocking more than 100 classes of attacks)
- Heuristic analysis for backdoors, port scans and flooding prevention
- Contextual signatures at the application level including spyware prevention, P2P and IM filtering, multimedia traffic filters, cross-scripting prevention…
- Application-layer intrusion prevention in VPN tunnels

Complete Security Appliance
- Anti-virus
- Anti-spam
- Dynamic URL filtering
- IPSEC VPN gateway
- Clientless SSL VPN gateway

System Interoperability
- Compatible with LDAP, RADIUS, ACTIVE DIRECTORY authentication databases
- Compatible with content filtering solutions through ICAP

For more information contact :
NETASQ
3, rue Archimède 59650 Villeneuve d'Ascq - France
Phone : +33 3 20 61 96 30
Fax : +33 3 20 61 96 39
URL : http://www.netasq.com

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



Source: The Tolly Group, May 2005

Figure 3

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

Vendor	Product	Web address
Blade Software	IDS Informer ver 1.0.467	http://www.bladesoftware.net
Spirent Communications	SmartBits 600 ver 2.6	http://www.spirentcom.com
Spirent Communications	SmartFlow ver 4.6	http://www.spirentcom.com
Spirent Communications	TeraMetric XD LAN-3327A ver 5.00.070	http://www.spirentcom.com

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.

This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.

The Tolly Group provides a fee-based service to assist users in understanding the applicability of a given test scenario to their specific needs. Contact us for information.

When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

Project Profile

Sponsor: NETASQ

Document number: 205120

Product class: Enterprise-class firewall

Products under test:

- NETASQ F2000 IPS-Firewall Ver 6.0.5

Testing window: May 2005

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 sales@tolly.com, call (561) 391-5610.

The Tolly Group doc. 205120 rev. clk 17 Jun 05