THE TOLLY GROUP

No. 207241 October 2007

Reflex Security, Inc.

Reflex Interceptor 1000

Performance Evaluation of Network Security Switch under Severe Attack Strain and Fail-Open Scenarios

TOLLY Up to Spec CERTIFIED Test Summary

Premise: *As security threats become more prevalent, gigabit network security technology needs to be incorporated within the network to protect critical assets. An effective gigabit network security solution needs to incorporate fully-featured, multi-vector protection, handle dynamic network threats and attacks automatically without slowing down the network, and guard against becoming a single point of failure by offering high reliability. Reflex Security provides the solution for high network security, performance and reliability with its Interceptor 1000 network security switch.*

Reflex Security, Inc. commissioned The Tolly Group to measure the performance of the vendor's Reflex Interceptor 1000, a network security switch with eight GbE ports (four in, four out) that provides 1 Gigabit (Gbps) throughput for medium to large enterprises.

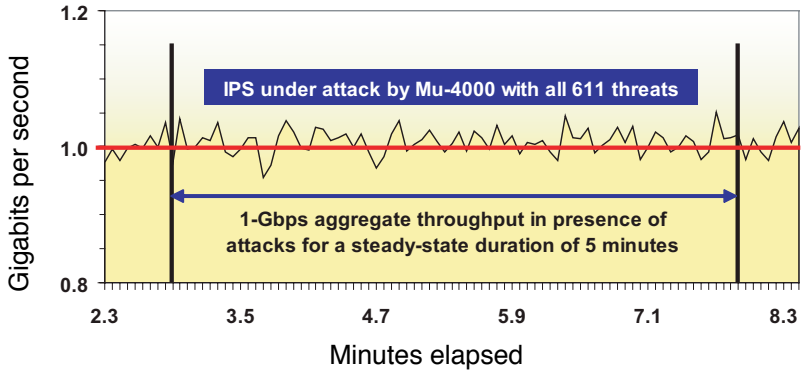
Engineers measured the performance of the Interceptor 1000 across four pairs of GbE interfaces, both with and without exposing the device to a taxing load of security threats. Engineers also measured the number of concurrent TCP connections sustained across the Interceptor 1000 and examined how the unit responds during an invoked power failure. Tests were conducted in August 2007.

Test Highlights

- Maintains aggregate throughput of 1 Gbps even when device is processing 611 unique threats
- Blocks 611 security threats out of 611 generated
- Maintains throughput levels, with zero failed transactions, during power failure
- Supports up to 1.5 million concurrent TCP connections over eight GbE ports

Reflex Interceptor 1000 Maximum Throughput Under Attack with 611 Unique Threats

(as Reported by Avalanche Commander 7.51 and Mu-4000 across four pairs of GbE ports)



Note: Protocol distribution of he traffic was HTTP (84.4%), FTP (10.9%), SMTP (2.4%), POP3 (1.3%) and DNS (1%).

Source: The Tolly Group, August 2007

Figure 1

Executive Summary

The Reflex Interceptor 1000 averaged throughput of 1 Gbps while blocking 611 unique threats and also sustained a traffic rate of 1 Gbps even during an induced power failure.

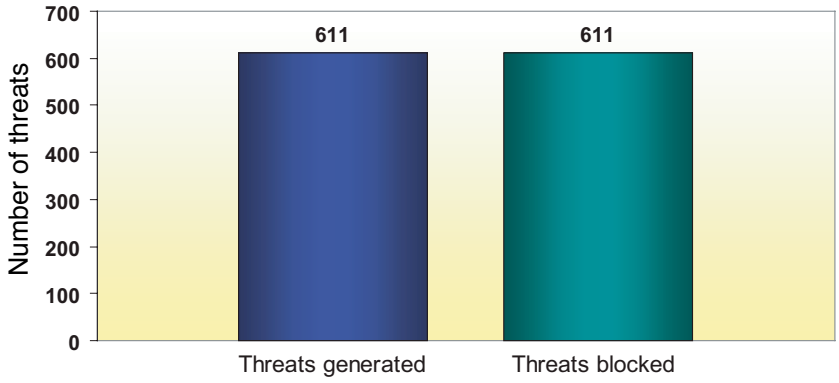
Tolly Group tests of the Reflex Interceptor 1000 show that the device delivers the speed, the scalability and the high availability required to ensure that network security threats are stopped at the entrance to the enterprise, without adversely affecting the performance of application traffic.

Throughput tests show that the Interceptor 1000 delivers 1 Gbps of aggregate throughput under normal conditions using four pairs (four in, four out) GbE ports, and continues to deliver that same performance even when the security device was blocking 611 unique security threats. The Interceptor 1000 demonstrates that it can maintain performance even when subjected to sustained, heavy traffic loads.

Tests of TCP connection scalability shows that the appliance can sustain 1.5 million TCP connections simultaneously.

Finally, tests show that the Interceptor 1000 can sustain 1 Gbps traffic throughput even during an outage of the security switch.

Reflex Interceptor 1000 Threat Mitigation Accuracy
(as Reported by Mu-4000 Security Analyzer with Published Vulnerability Ver. 2.3.28)



The 611 unique threats generated represents the maximum number of threats offered by the Mu-4000 Security Analyzer.

Source: The Tolly Group, August 2007

Figure 2

Throughput Baseline

Engineers measured the amount of simulated real-world traffic with mixed protocols that can pass across the Interceptor 1000 network security switch, without the presence of security threats.

Tests show that the Interceptor 1000 was able to sustain an average of 1 Gbps of traffic across the Interceptor 1000 appliance. (See Figure 5.)

Aggregate Throughput under Attack

Engineers measured the throughput delivered by the Interceptor 1000 while it simultaneously was detecting security threats and blocking

Sample of Security Threat Categories Tested

- HTTP
- SMTP
- imap2
- Microsoft DS
- NetBIOS-ssn
- LDAP
- POP3
- TCP
- mySQL

Figure 3

them. While the Interceptor 1000 handled its security processing, the measurement taken shows the amount of throughput the Interceptor 1000 was able to sustain while under the load of security processing.

Engineers ramped up traffic to 1 Gbps, or the maximum traffic rate sustained by the Interceptor 1000, over its four pairs of GbE ports. When the maximum throughput was attained, engineers launched a multi-pronged attack using the Published Vulnerability Version: 2.3.28 attack library from a Mu Security Mu-4000 Security Analyzer.

Tests show that the Interceptor 1000 sustained the maximum throughput of 1 Gbps without failed transactions even while it handled the extra burden of attack mitigation with 611 different attacks launched against it — the maximum number of attacks supported by the Mu-4000 Security Analyzer's threat database. (See Figures 1 and 2.)

The attack lasted for five minutes, without any deleterious affect on throughput. Additionally, the test demonstrates the security accuracy of the Interceptor 1000.

With the constant evolution of security threats on the Internet, it is critical for any security appliance to support up-to-date threat databases. During the maximum throughput test, the Interceptor 1000 demonstrated accuracy of threat detection and blockage by correctly identifying and blocking all 611 available threats launched from the analyzer. (See Figures 2 & 3.)

Concurrent TCP Connections

Engineers set out to measure the total number of TCP connections sustained by the Interceptor 1000. Engineers measured the ability of the Interceptor 1000 to perform a SYN-SYN ACK-ACK process to open a connection with another device and then maintain that open TCP connection.

Tests show that the Interceptor 1000 was able to handle almost 1.5 million simultaneous TCP connections across the device. (See Figure 4.)

Fail-Open Test

Tolly Group engineers set out to determine the impact that an interface failure or total power failure to the Reflex Interceptor 1000 would have on the network.

For the test, engineers passed the same simulated, real-world traffic used on the baseline throughput scenario to the Interceptor 1000 device. The traffic rate was 1 Gbps across four pairs of GbE interfaces.

Reflex Security, Inc.

Reflex Interceptor 1000

Performance and High Availability

TOLLY Up to Spec CERTIFIED

Product Specifications

Vendor-supplied information not necessarily verified by The Tolly Group

Reflex Security, Inc.
Reflex Interceptor 1000
Product Specifications*

Key Functionality:

- High port density
- High detection rate
- High accuracy
- Firewall
- IPS
- Multi-core architecture
- Anti-spyware
- Network access control
- Identity management (IP2ID)
- DoS protection
- High availability
- Support switching mode

For more info, contact:

Reflex Security, Inc.
53 Perimeter Center East
Atlanta, GA 30346
Phone: 1-888-872-7555
URL:
http://www.reflexsecurity.com

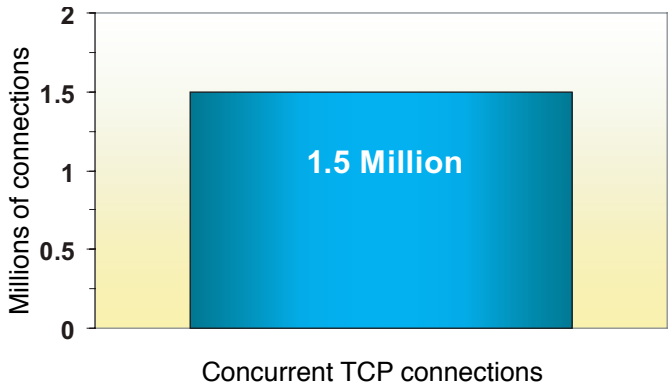
Next, engineers simulated an interface failure by disabling a 10/100/1000 Base-T interface via software for five minutes while the Avalanche/Reflector test ran to completion. This represents a serious hardware failure on the device. The Interceptor 1000 "failed open" and continued to transmit the traffic passively, without scanning, delivering 1 Gbps of throughput.

The Reflex Interceptor 1000 network security switch also supports fail-open (by-pass) in the event of total power failures. Tolly Group engineers induced total power failure on the Interceptor 1000 by disconnecting its power cord for five minutes while the Avalanche/Reflector test ran to completion. Tests confirmed the appliance still delivered 1 Gbps of throughput using four pairs of 10/100/1000 Base-T ports in "fail-open" mode.

Test Setup & Methodology

The Tolly Group tested a Reflex Interceptor 1000 with eight 10/100/1000 copper interfaces, four modular fiber interfaces and a dual processor, quad-core design. The system supported the Reflex MG V 6.1 threat signature and Reflex Command Center V 6.1 management software.

Concurrent TCP Connections Supported Across Four Pairs of GbE Ports
(as Reported by Avalanche Commander 7.51)



Source: The Tolly Group, August 2007

Figure 4

Engineers configured inline protection mode with the highest security protection on the Interceptor 1000 and placed it between simulated internal and external data center networks.

On the internal network side, engineers used one unit of Reflector 2700 and connected all four GbE interfaces to the Interceptor 1000. For the external network side, engineers used one unit of Avalanche 2007 and also, connected all four GbE ports to the Interceptor 1000 device.

Attacks generated by the Mu-4000 Security Analyzer were directed onto the appliance device via two GbE ports. The version used for the Mu-4000 Security Analyzer appliance was 2.3.3.r9336 with attack library version 2.3.28. (See Figure 6.)

Baseline Throughput

Engineers used a pair of Avalanche and Reflector 2700 test tools to generate real-world traffic with mixed protocols and ratios; HTTP (84.4%), FTP (10.9%), SMTP (2.4%), POP3 (1.3%) and DNS (1%). HTTP object sizes tested ranged from 43 bytes to 64K bytes. For FTP, 1K-byte and 1M-byte data sizes were used. For SMTP, 12K-byte and 24K-byte data sizes were used. For POP3, 1,280- to 1,518-byte message lengths were used.

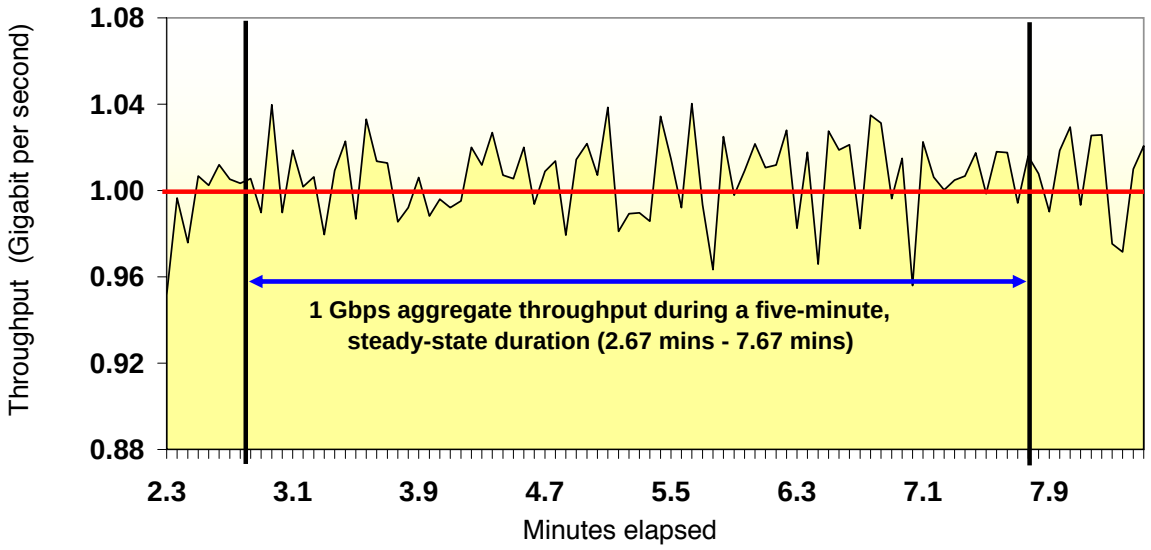
Engineers generated the 1 Gbps baseline traffic by using all four ports available on the pair of Avalanche and Reflector 2700 test tools. Traffic was maintained at the peak without any failed transactions for 300 seconds and an average throughput was calculated.

Maximum Throughput Under Attack

Engineers configured the Mu-4000 Security Analyzer and ran the Published Vulnerability Analysis with all the 611 threats available through the Interceptor

Interceptor 1000 Aggregate Baseline Throughput with Simulated Real-World Traffic Across Four Pairs of 10/100/1000 Base-T Ports

(as Reported by Spirent Avalanche 7.51)



Note: Traffic protocol distribution was HTTP (84.4%), FTP (10.9%), SMTP (2.4%), POP3 (1.3%) and DNS (1%).

Source: The Tolly Group, August 2007

Figure 5

1000 device. The Mu-4000 created a report after the test completed.

Concurrent TCP Connections

Engineers used an Avalanche and Reflector pair for the maximum open connections test. The HTTP 1.1 protocol (with persistence mode) was used on both client (Avalanche) and server (Reflector) sides.

The test was run at the maximum concurrent connections; a steady state of 300 seconds was maintained. An average number of concurrent TCP connections was calculated at the steady state.

Fail-Open Test

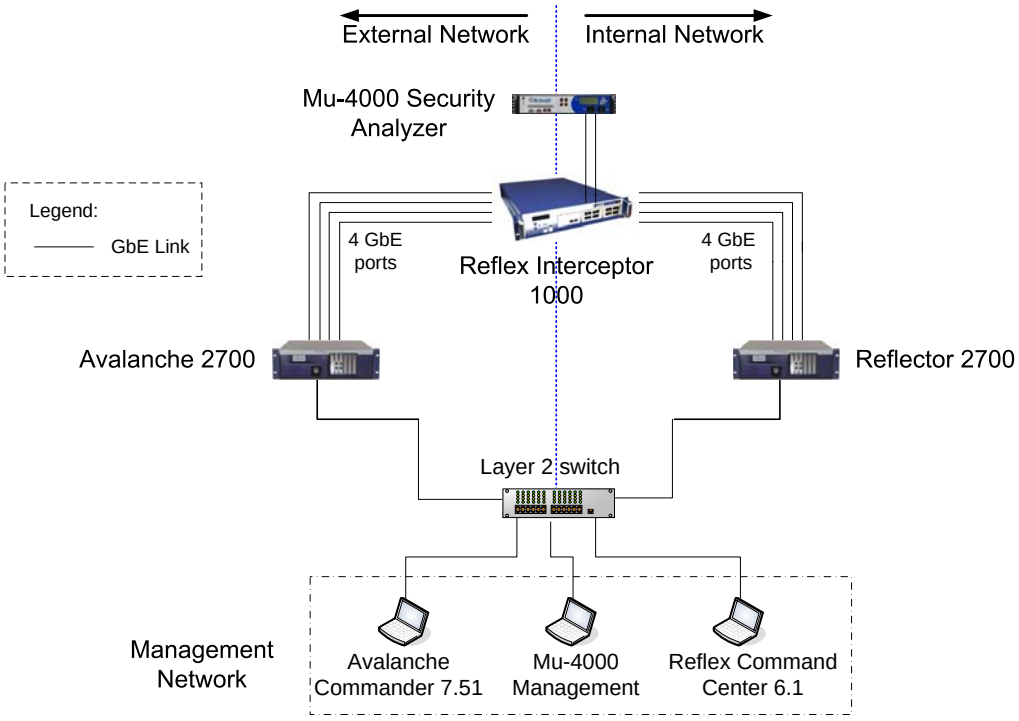
In this test case, engineers used one pair of Spirent Communications Avalanche and Reflector 2700 traffic generator test tool to transmit 1 Gbps of mixed protocol traffic. With traffic running around 1 Gbps from the pair of Avalanche and Reflector 2700, engineers disabled an interface in software and, separately, unplugged the power cord from the Interceptor 1000.

Engineers observed in both scenarios that the Reflex Interceptor 1000 supports a fail-open capability that allows all incoming traffic to pass through the appliance without being scanned, as if the data was passing across a physical wire.

The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services.

The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at http://www.tolly.com, sales@tolly.com

Test Bed Diagram



Source: The Tolly Group, August 2007

Figure 6

Test Equipment Summary

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

Vendor	Product	Web
Mu Security	Mu-4000 Security Analyzer	http://www.musecurity.com
Spirent Communications	Avalanche/Reflector 2700	http://www.spirentcom.com

207241-sphfst3-cdb-10Oct2007