THE TOLLY GROUP

No. 207219 July 2007

Reflex Security, Inc.

Reflex MG10 Network Security System

Performance Evaluation under Severe Attack Strain with No Transaction Loss and High Availability Examination

TOLLY Up to Spec CERTIFIED Test Summary

Premise: *Multi-gigabit networks are fast emerging as a standard for corporate networks as the demand for data-intensive applications grows. 10 Gigabit Ethernet (10GbE) is common now in data centers and at the network core where the aggregation of multiple gigabit networks occurs. Users are seeking secure switching solutions that can keep up with the performance demand created by these network types. It is essential then that strategic security products that include intrusion prevention systems (IPSs), network access control (NAC) and firewalls support 10GbE connectivity, 10 Gbps traffic inspection and high availability.*

Reflex Security Inc. commissioned The Tolly Group to measure the performance of the vendor's Reflex MG10, a network security system that employs a blade-based Distributed Security Architecture™ (DSA) that provides scalable throughput from 10 Mbps to 10 Gigabit per second (Gbps).

Engineers measured the multi-Gigabit performance of the MG10, both with and without exposing the device to a serious load of security threats. Engineers also measured the number of open TCP connections sustained across the MG10, and examined how the unit responds during an invoked failure.

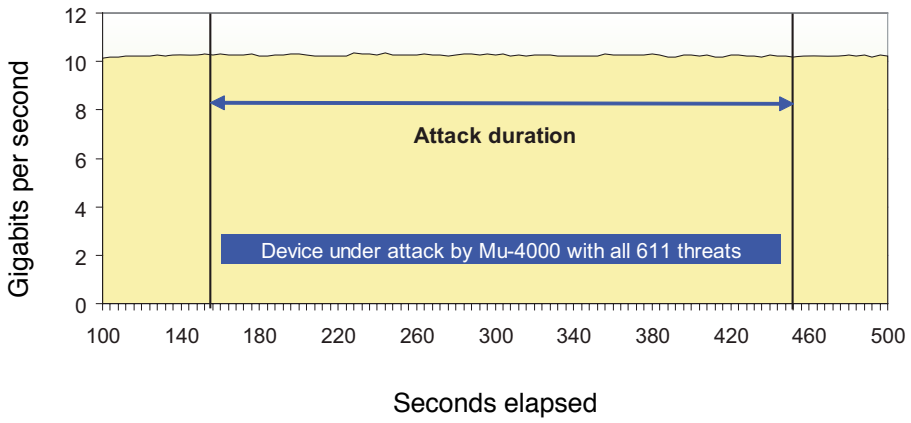
Testing was conducted in June 2007.

Test Highlights

- Maintains average maximum throughput of 10.25 Gbps even when device is processing 611 unique threats — the maximum attacks supported by the Mu-4000 Security Analyzer with Version 2.3.28 attack library
- Blocks 611 security threats out of 611 generated
- Sustains throughput, with zero failed transactions, during random blade failure
- Supports almost 5.8 million steady-state TCP connections over two 10GbE and eight GbE ports

Reflex MG10 Maximum Throughput Under Attack with 611 Unique Threats

(as Reported by Avalanche Commander 7.51 and Mu-4000)



Source: The Tolly Group, June 2007

Figure 1

Executive Summary

The Reflex MG10 averaged throughput of 10.25 Gbps while processing 611 unique threats and also sustained traffic rates during a simulated outage of a single blade and the rejoin of the blade into the system chassis.

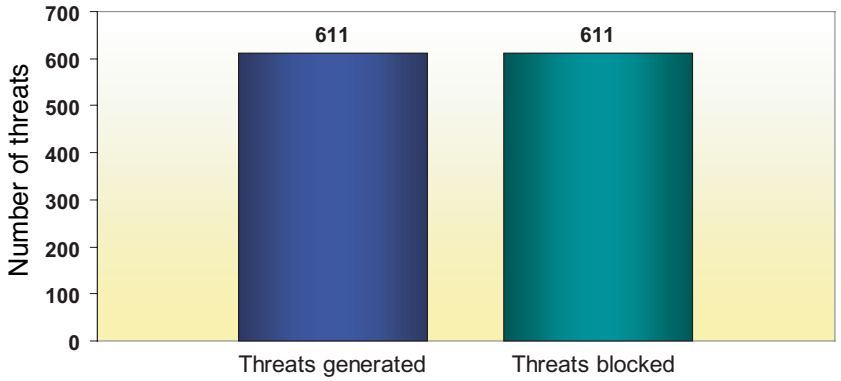
Tolly Group tests of the Reflex MG10 show that the device delivers the speed, the scalability and the high availability required to ensure that network security threats are stopped at the entrance to the enterprise network, without adversely affecting the performance of application traffic.

Throughput tests show that the MG10 delivers 10.25 Gbps of throughput under normal conditions and continues to deliver that same performance even when the system was being hammered by 611 unique security threats. In effect, the MG10 demonstrates that it is based on an architecture that can maintain performance even when subjected to heavy processing loads.

Moreover, tests of TCP connections shows that the security switch can sustain 5.8 million open TCP connections over the device backplane.

Finally, tests show that the MG10 can sustain traffic throughput even during the outage of a security blade — and without loss of transactions.

Reflex MG10 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, June 2007

Figure 2

Throughput Baseline

Engineers measured the amount of simulated real-world traffic with mixed protocols that could pass across the backplane of the MG10, without the presence of security threats.

Tests show that the MG10 was able to sustain an average of 10.25 Gbps of traffic across the device's backplane.

Maximum Throughput under Attack

Engineers measured the throughput delivered by the MG10 while it simultaneously was processing security threats and blocking them. While the MG10 handled its security processing, the measurement taken shows the amount of throughput the MG10 was able to sustain while under the load of security processing.

Sample of Security Threat Categories Tested

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

Figure 3

Engineers ramped up traffic to 10.25 Gbps, or the maximum traffic rate sustained by the MG10. At the time that the maximum throughput was attained, engineers then launched a multi-pronged attack using the Published Vulnerability Version: 2.3.28 attack library from an Mu Security Mu-4000 Security Analyzer.

Tests show that the MG10 sustained the maximum throughput of 10.25 Gbps without failed transactions even while it handled the extra burden of attack mitigation and 611 different attacks launched against it — the maximum number of attacks supported by the security analyzer's threat database. (See Figures 1 and 2.)

The attack lasted for five minutes, without any deleterious affect on throughput. Additionally, the tests demonstrates the accuracy of the MG10.

With the constant evolution of security threats on the Internet, it is crucial that a security device support up-to-date threat databases. During the maximum throughput test, the MG10 demonstrated accuracy of threat detection and blockage by correctly identifying and blocking all 611 available threats launched from the security analyzer. (See Figures 2 and 3.)

Open TCP Connections

Engineers set out to measure the total number of TCP connections sustained by the MG10. Engineers measured the ability of the MG10 to perform a SYN-SYN ACK process to open a connection with another device and then maintain that open TCP connection.

Tests show that the MG10 was able to handle almost 5.8 million TCP connections across the device. (See Figure 4.)

High Availability

Engineers set out to determine the impact that a blade failure would have on overall system performance.

For the test, engineers passed simulated, real-world traffic to the MG10 at a rate of 6.3 Gbps. The 6.3 Gbps rate was chosen on an arbitrary basis, and it represents the amount of traffic generated by two pairs of Avalanche/Reflector 2700 test tool generators.

Engineers passed traffic through the MG10, bringing it to its maximum performance level. Then, they simulated a failure by pulling a system blade for 60 seconds. This represents a serious hardware failure on the device. However, the MG10 continued to deliver 6.3 Gbps of throughput even with the loss of a single blade. (See Figure 5.)

Further, the insertion of a blade into a chassis often may cause a system to fail transactions or

Reflex Security, Inc.

Reflex MG10 Network Security System

Performance and High Availability

Product Specifications

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

Reflex Security, Inc.
Reflex MG10
Product Specifications*

Key Functionality:

- Scalable throughput
- High availability
- High port density
- High detection rate
- Flexible architecture (ATCA)
- Link aggregation (802.3AD)
- VLAN Tagging (802.1Q)
- VLAN based security policies
- 10 Gig interfaces
- Multi core architecture
- Firewall
- IPS
- Anti-spyware
- Anti-virus
- Network access control
- Identity management (IP2ID)
- DoS protection

For more info, contact:

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

act in an unstable manner. However, engineers noted that the reinsertion of the MG10 blade did not result in the loss of any transactions, and the offered traffic rate of 6.3 Gbps was maintained even during the outage.

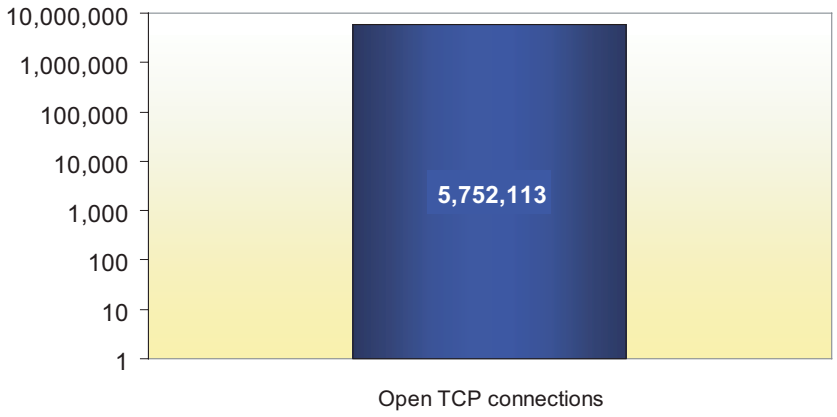
Test Setup & Methodology

The Tolly Group tested a Reflex MG10 appliance outfitted with 12 blades, four available 10GbE ports, and eight GbE ports. The system supported the Reflex MG V 6.0 threat signature and Reflex Command Center V 6.0 management software.

Engineers configured inline protection mode with the highest security protection on the MG10 and placed it between simulated internal and external data center networks. On the internal end, engineers used four units of Reflector (two units of 2700 and two units of 2500) with two Gigabit Ethernet switches. For the external network, engineers used four units of Avalanche (two units of 2700 and two units of 2500) with one GbE and one 10GbE switch. In addition, engineers used a Linux server with Tomahawk and one GbE port was connected to the internal network and another port to the external network.

Two trunks were created. At the internal network, four GbE ports from a switch and four GbE ports from the MG10's DSP (Distributed Security Processor) board were configured as link aggregation (802.3 AD) to create a trunk. The configuration from the internal network was applied to the eight GbE ports (four from a switch and four from the DSP) at the external network.

Steady-State Open TCP Connections Supported Across Two 10GbE and Eight GbE Ports
(as Reported by Avalanche Commander 7.51)



Source: The Tolly Group, June 2007

Figure 4

Attacks generated by the Mu-4000 Security Analyzer were directed onto networks via two GbE ports: one was connected to external networks and the other to internal networks. (See Figure 6.)

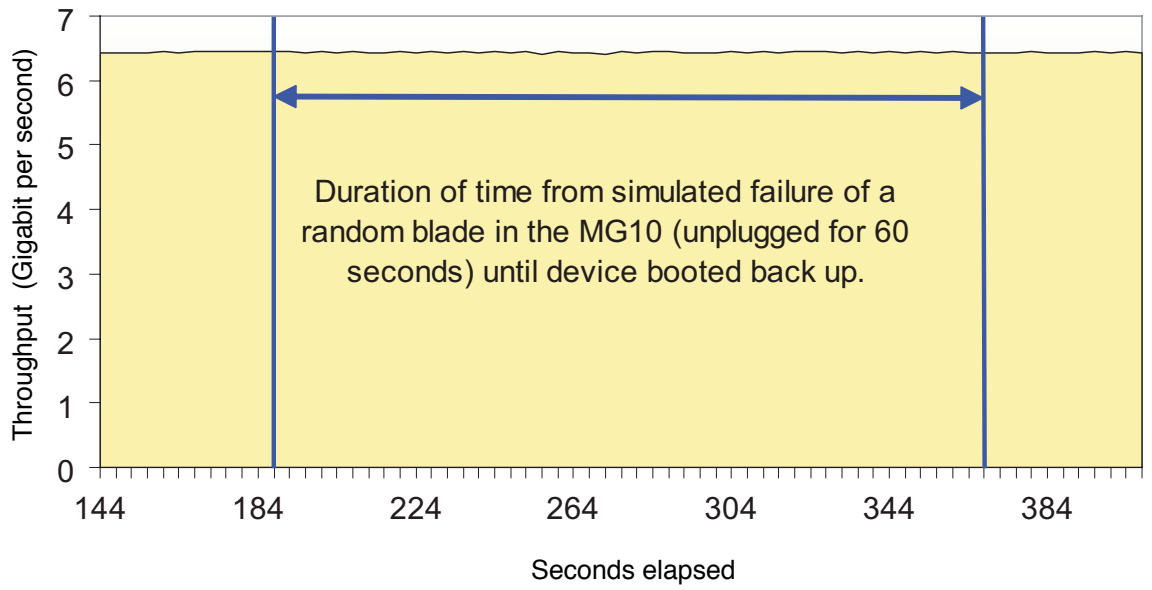
Baseline Throughput

Engineers used four pairs of Avalanche and Reflector test tools (two pairs of 2700 and two pairs of 2500) to generate real-world traffic with mixed protocols and ratios; HTTP (80%), FTP (10%), RTSP (5%), SMTP (2%), POP3 (2%) and DNS (1%). HTTP object sizes tested ranged from 43K to 64K bytes. For FTP, 1K and 1M-byte data sizes were used. For RTSP, 36K and 250K bytes of QuickTime files 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 baseline traffic in two sections through the MG10. Two pairs of Avalanche/Reflector 2700s generated 6.3 Gbps that traveled through the two 10GbE ports and two pairs of Avalanche/Reflector 2500s generated another 3 Gbps of traffic through the trunk.

In order to reach the maximum throughput of the MG10 and due to limited traffic generated by four pairs of Avalanche/Reflectors used in testing (9.3 Gbps), engineers utilized a Linux server with Tomahawk version 1.1 to generate 1 Gbps traffic. The traffic was a reply of packet trace (pcap) file, the captured traffic from one pair of Avalanche/Reflector (main-

Sustained Throughput with Zero Failed Transactions During Simulated Outage
(as Reported by Avalanche Commander 7.51)



Source: The Tolly Group, June 2007

Figure 5

tained same mix protocols and ratio).

Traffic was maintained at the peak without any failed transactions for 300 seconds and an average was calculated.

Maximum Throughput Under Attack

Engineers configured the Mu-4000 Security Analyzer and ran the Published Vulnerability Analysis with all the 611 threats over the same network used for the baseline throughput test.

The Mu-4000 created a report after the test was finished.

Maximum TCP Connections

Engineers used an available Avalanche/Reflector maximum open connections test. The HTTP 1.1 persistence protocol used on both client (Avalanche) and server (Reflector) sides. The test was run at the maximum concurrent connections and a steady state of 300 seconds was maintained. An average number of concurrent TCP connection was calculated at the steady state.

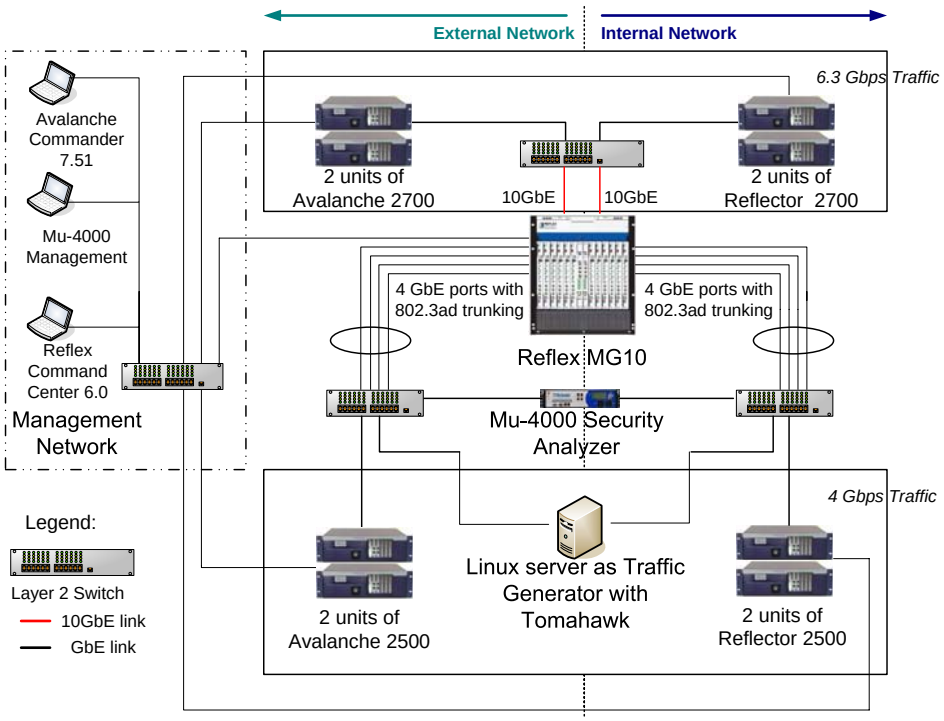
High Availability

In this test case, engineers shut down two pairs of Avalanche and Reflector 2500 and maintained the same configuration from the baseline test. With traffic running around 6.3 Gbps from two pairs of Avalanche and Reflector 2700s, engineers randomly picked a blade and pulled it out from its chassis. Engineers observed any failed transactions and waited 60 seconds to plug the blade back into its chassis.

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, June 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 2500 Avalanche/Reflector 2700	http://www.spirent.com
Technical Pursuit, Inc.	Tomahawk IPS 1.1	http://www.tomahawktesttool.org

207219-sphfst2-cdb-10July07