

Top Layer Networks, Inc. Attack Mitigator IPS™ 5500-1000 Competitive Intrusion Prevention System Evaluation versus TippingPoint UnityOne-2400



Test Summary

Premise: Most Intrusion Prevention Systems (IPS) can detect and block worms and other security threats in the face of little or no background traffic. IPS vendors generally promote their IPS capabilities based on tests that don't simulate real-world network and traffic conditions. But embed the attacks in real traffic, with typical user load on real networks, and the true effectiveness of the IPS offerings rises to the surface.

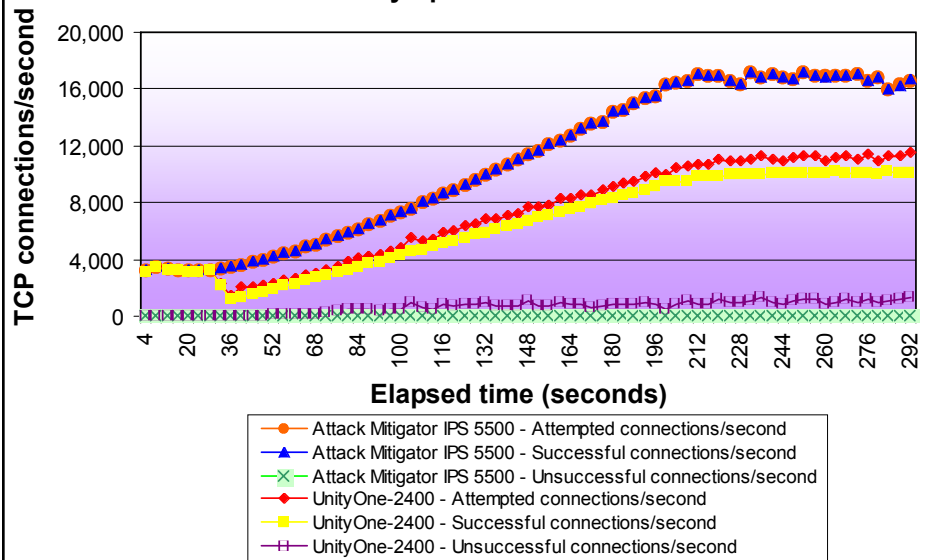
Top Layer Networks, Inc. commissioned The Tolly Group to evaluate its Attack Mitigator IPS 5500™, an intrusion prevention system designed to stop network-based threats while allowing legitimate transactions to complete.

The Tolly Group evaluated the effectiveness of the Attack Mitigator IPS 5500 at handling transactions in the face of Distributed Denial-of-Service (DDoS) SYN flood attacks. Moreover, engineers examined the capability of the Attack Mitigator IPS 5500 to handle real-time identification and blocking of embedded worms when mixed in otherwise normal traffic. (*Worms are programs or algorithms that replicate over a computer network and usually perform malicious actions.*) Tests focused on the capability to filter such traffic while monitoring

Test Highlights

- Up to 43% more effective than the UnityOne-2400 at processing legitimate connections while blocking embedded worm attacks
- Allows legitimate connections to complete with response times significantly lower than those allowed by the UnityOne-2400 when both are under SYN flood attack
- Completes 46% more HTTP connections/sec than the UnityOne-2400 and delivers 100% success rate
- Completes 65% more mixed protocol connections/sec than the UnityOne-2400 and delivers 100% success rate
- Achieves 100% of zero-loss throughput when tested at frame sizes of 128-bytes or higher at 2 Gbps traffic rates

"Real-World" SYN Flood Attack (HTTP Traffic) Comparison Attack Mitigator IPS 5500 and UnityOne-2400 as Measured by Spirent Avalanche/Reflector



¹Spirent Avalanche was configured to gradually ramp up its connection rate to a maximum of 20,000 connections per second. Actual rates generated during the tests varied due to the response characteristics of the Spirent Reflector and the IPS device under test.

Source: The Tolly Group, October 2004

Figure 1

SYN Flood Attack – HTTP Traffic Test Detailed Results											
Intrusion Prevention Solution		Response time (ms)					DDoS attack packets sent	SYN sent on client	SYN received on server	SYN/ACK sent from server	SYN/ACK received on client
		Page response	URL response	To TCP SYN/ACK	To first data byte	Est. server response					
Attack Mitigator IPS 5500	Minimum	0	0	0.05	0.21	0	35,855,550	3,824,440	3,824,366	3,824,375	3,824,360
	Average	0	0	0.09	0.22	0.04					
UnityOne-2400	Minimum	0	0	0.08	0.29	0	35,845,565	1,721,685	18,455,872	26,551,020	528,475
	Average	737	737	636.65	1374.56	453.85					

Source: The Tolly Group, October 2004 Figure 2

what, if any, degradation affected the IPS' connection rate.

Engineers conducted these tests on the Attack Mitigator IPS 5500 and compared the results to a TippingPoint Technologies Inc. UnityOne-2400 IPS. Tests were conducted in October 2004.

RESULTS

REAL-WORLD SYN FLOOD ATTACKS (HTTP FOREGROUND TRAFFIC ONLY)

In this test, engineers attempted to understand how a SYN flood attack to the same server(s) affects legitimate HTTP traffic passing through the IPS devices tested.

During the test, Spirent Avalanche was configured to gradually ramp up its connection rate to a maximum of 20,000 connections per second. Actual rates generated during the tests varied due to response characteristics of the Spirent Reflector and the IPS device under test.

Tests show that the Attack Mitigator IPS 5500 processed 11,978 out of 11,978 attempted legitimate HTTP connections per second while under the SYN flood attack. That is, the Attack Mitigator IPS 5500 was able to filter out all of the attacks without degrading the performance of the legitimate traffic. By contrast, the UnityOne-2400 was able to successfully complete only 7,309 out of 8,028 attempted legitimate HTTP connections per second while under the same SYN flood attack. (See Figure 1.)

Beyond the number of successful connections served, the Attack Mitigator IPS 5500 also held a distinct advantage in the area of response times. The Attack Mitigator IPS 5500 offered an average time-to-first-byte of 0.22 milliseconds (ms.) versus 1.37 seconds for the UnityOne-2400. (See Figure 2.) And the Spirent test tool reported an estimated server response time of 0.04 ms. for the Attack Mitigator IPS 5500 versus 453.9 ms. for the UnityOne-2400. These results indicate that the Attack Mitigator IPS 5500 processes the data

stream more quickly than the competing product.

REAL-WORLD SYN FLOOD ATTACKS (MIXED PROTOCOLS)

In this test, built on the previous test, engineers attempted to understand how a SYN flood attack to the same server(s) affects legitimate mixed protocol (HTTP, SMTP, POP3, and FTP) traffic passing through the IPS devices tested. During the test, 2,000 cps of legitimate "good" mixed traffic was sent by the Spirent Avalanche test tool, while 100,000 SYN flood attack packets per second were sent by a Spirent Avalanche/ Reflector.

Tests show that the Attack Mitigator IPS 5500 processed legitimate traffic at an average rate of 1,246 out of 1,246 attempted cps for the sum of all protocol traffic: POP3, HTTP, SMTP, FTP, while under SYN flood attack. (See Figures 3 & 4.) By contrast, the UnityOne-2400 was able to

process only 757 out of 1,207 attempted legitimate mixed protocol connections while under the SYN flood attack.

Therefore, the IPS 5500 handled 64.6% more cps than the UnityOne-2400.

MIXED WORM TRAFFIC ATTACK

The purpose of this test was to inject certain percentages of worms into legitimate HTTP connections. During the test, the Spirent test tool was set to 20,000 cps with different percentages of “good” HTTP traffic and “bad” (worm) HTTP traffic. At various test intervals, engineers injected worms into 5%, 10% and 25% of the test traffic. However, the actual connections generated by the Spirent Avalanche were less than 20,000 if the server and the device under test responded more slowly than the Avalanche could generate new connections.

(Note: In these scenarios, the UnityOne-2400 was offered smaller loads due a combination of the Spirent test tool and the processing on the device under test. Spirent's Avalanche ramps up load as quickly as the server (Spirent Reflector) responds to requests. In the test scenarios, the UnityOne-2400 exhibited longer latencies and slower overall response times, so the load offered by Avalanche wasn't as fast — or as quickly offered.)

In the 5% worm scenario, the IPS 5500 was sent a mix of legitimate and worm-infected HTTP traffic at a combined rate of

11,345 cps, and successfully processed 11,127 out of 11,127 attempted legitimate connections, while blocking all 218 worm-based connections per second. By contrast the UnityOne-2400 was offered a mix of “good” and “bad” HTTP traffic at an average rate of 9,454 connections per second, but successfully processed only 9,362 out of 9,362 attempted legitimate connections per second while blocking 91 out of 92 worm-infected connections per second. The IPS 5500 was 19% more effective than the UnityOne-2400 at allowing legitimate connections while blocking light worm traffic. (See Figures 5 & 6.)

In the 10% worm scenario, the IPS 5500 was sent a mix of legitimate and worm-infected HTTP connections at a combined average rate of 11,457 HTTP cps, and it successfully processed 11,094 out of 11,094 attempted legitimate connections per second, while blocking all of the 363 worm-based connections per second. By contrast, the UnityOne-2400 was offered a mix of “good” and “bad” HTTP traffic at an average rate of 8,893 connections per second, but successfully processed only 8,758 out of 8,758 attempted legitimate connections per second while blocking all 135 worm-infected connections per second. The IPS 5500 was 27% more effective than the UnityOne-2400 at allowing legitimate connections while blocking moderate worm traffic.

In the 25% worm scenario, the IPS 5500 was sent a mix of

Top Layer Networks, Inc.

Attack Mitigator IPS 5500

Intrusion Prevention System Performance



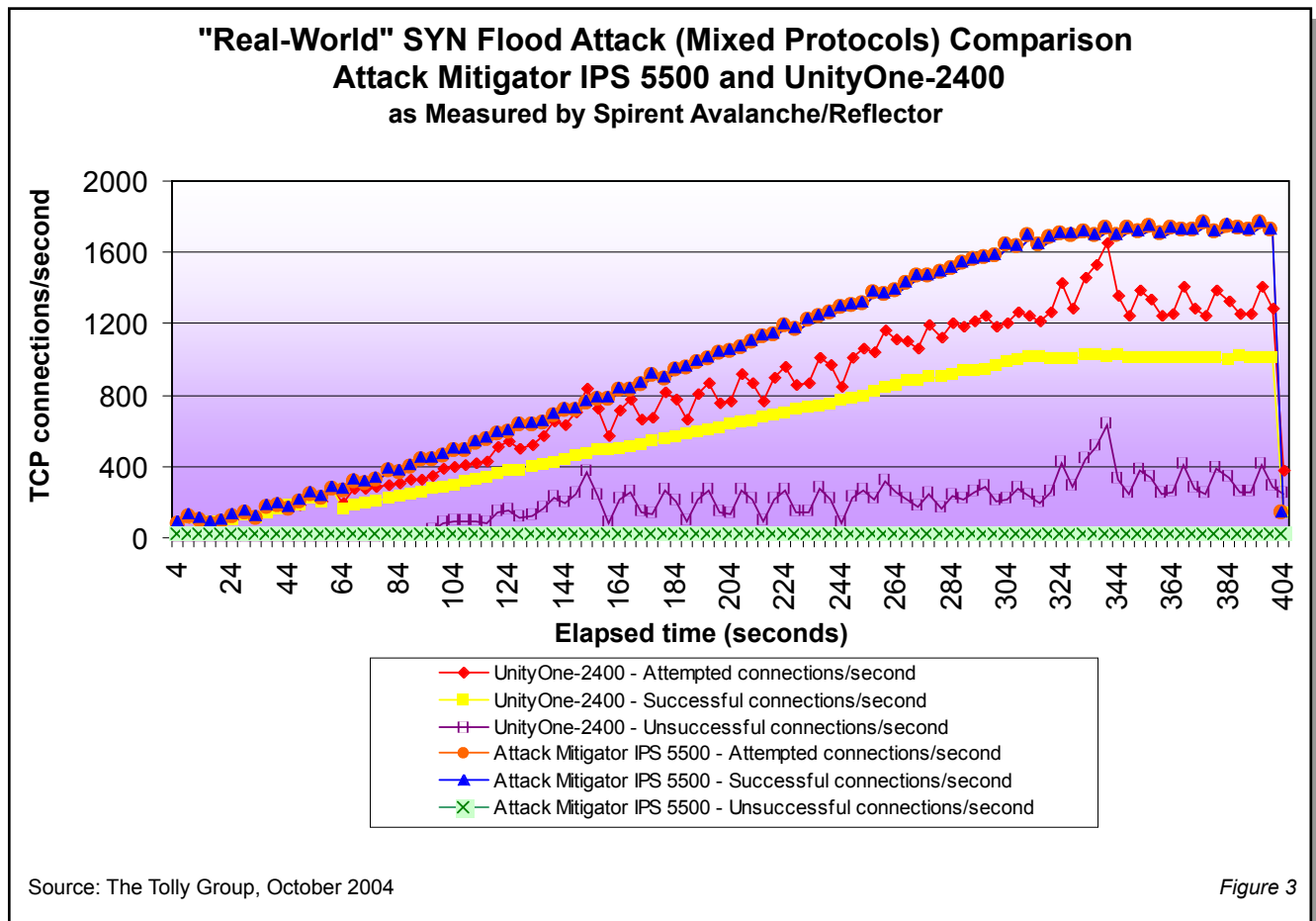
**Top Layer Networks, Inc.
Attack Mitigator IPS 5500
Product Specifications***

- Comprehensive Infrastructure Security
 - In-depth protection against network and application based threats including zero-day exploits
- Performance
 - Industry-leading inline inspection and real-time blockage of attacks with zero loss and microsecond latency
- Stateful Analysis
 - Active stateful inspection and custom signature capability
- Application Usage Enforcement and Protocol Validation
 - Protection through Deep-packet inspection combined with in-depth protocol and application usage analysis
- DDOS Protection
 - Most powerful protection from debilitating high-rate attacks such as SYN floods and other network and application-based DDOS attacks
- Reliability
 - True Active-Active load shared protection, hardened custom-OS, flexible port-bypass capabilities
- Easy to Deploy
 - IPS can be deployed seamlessly and start protecting critical resources in less than 30 minutes
- Easy to Manage
 - Powerful device management coupled with alerts, logging, reporting and integration with top third-party event management tools

For more information contact:

Top Layer Networks, Inc.
2400 Computer Drive, Westboro, MA 01581
Phone: (508) 870-1300
Fax: (508) 870-9797
URL: <http://www.TopLayer.com>
E-mail: info@TopLayer.com

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



legitimate and worm-filled HTTP connections at a combined average rate of 12,376 connections per second, and successfully processed 11,694 out of 11,694 attempted legitimate connections, while blocking all of the 682 worm-based connections per second. By contrast the UnityOne-2400 was offered a mix of "good" and "bad" HTTP traffic at an average rate of 8,365 connections per second, but successfully processed only 8,172 out of 8,172 attempted legitimate connections per second while blocking all 192 worm-infected connections per second. The IPS 5500 was 43% more effective at allowing legitimate connections while blocking higher levels of worm traffic.

VALIDATION OF 8 GBPS THROUGHPUT (ATTACK MITIGATOR IPS 5500 AND ATTACK MITIGATOR IPS 5500 PROTECTIONCLUSTER)

The purpose of this test was to benchmark the throughput of the IPS 5500-1000 and IPS 5500 ProtectionCluster™ when tested at various frame sizes and across different link types.

Tests show that the Attack Mitigator IPS 5500 achieved 100% of Gigabit Ethernet throughput with no frame loss when tested at frame sizes of 128 bytes to 1,518 bytes and handling an offered load of bidirectional 1 Gbps (or 2 Gbps

aggregate). When the offered load was 4.4 Gbps, the Attack Mitigator IPS 5500 achieved 100% of zero-loss throughput when tested with frame sizes of 512 bytes to 1,518 bytes. The IPS 5500 ProtectionCluster HA Solution achieved 8.8 Gbps with 100% of zero-loss throughput when tested with frame sizes of 512 bytes to 1,518 bytes.

ANALYSIS

When it comes to protection against brute force DoS and embedded worm attacks, users need equipment that can keep pace with the flow of real-time traffic and still separate the good traffic from the bad. The type of deep packet inspection

SYN Flood Attack - Mixed Protocol Test Individual Protocol Results									
Intrusion Prevention Solution	HTTP attempted connections	HTTP successful connections	SMTP attempted connections	SMTP successful connections	POP3 attempted connections	POP3 successful connections	FTP attempted connections	FTP successful connections	Test time (sec)
Attack Mitigator IPS 5500	451,716	451,716	31,482	31,482	17,982	17,982	4,500	4,500	406
UnityOne-2400	479,878	335,435	35,631	2,942	20,376	643	5,103	172	448

Source: The Tolly Group, October 2004

Figure 4

employed by IPS products often results in some element of overhead and delay introduced in packet processing.

Tests show that the Attack Mitigator IPS 5500 has algorithms and the processing power to keep pace with real-world user traffic and network environments, detect embedded security threats and eliminate them where other products are not as fast or as efficient.

By contrast, tests show that the UnityOne-2400 experienced difficulty enabling legitimate connections and protecting servers when under SYN flood attack. As shown in Figure 2, when faced with a combination of almost 36 million DDoS attack SYN packets and 1.72 million legitimate SYN packets, the UnityOne-2400 allowed over 18.4 million SYN packets to reach the protected server, the vast majority of which were the SYN flood attack packets. The Attack Mitigator IPS 5500, by contrast was able to process all 3.82 million legitimate SYN requests offered by the client and also disallowed all SYN

flood traffic. Therefore, the UnityOne was unable to process as many legitimate SYN requests from the client and worse yet, allowed a large percentage of SYN flood traffic to flood the server.

In the embedded worm attacks, the Attack Mitigator IPS 5500 successfully detected and blocked all worms in each of three traffic scenarios. The UnityOne-2400 was up to 30% less effective than the Attack Mitigator IPS 5500 at allowing good connections to complete while blocking worm traffic.

TEST CONFIGURATION AND METHODOLOGY

For performance tests, The Tolly Group tested a Top Layer Networks Attack Mitigator IPS 5500-1000 and Attack Mitigator IPS 5500 ProtectionCluster™, running software version 3.2. The Attack Mitigator IPS 5500-1000 came configured with four Gigabit Fiber and four 10BASE-T/100BASE-TX ports. The Attack Mitigator IPS

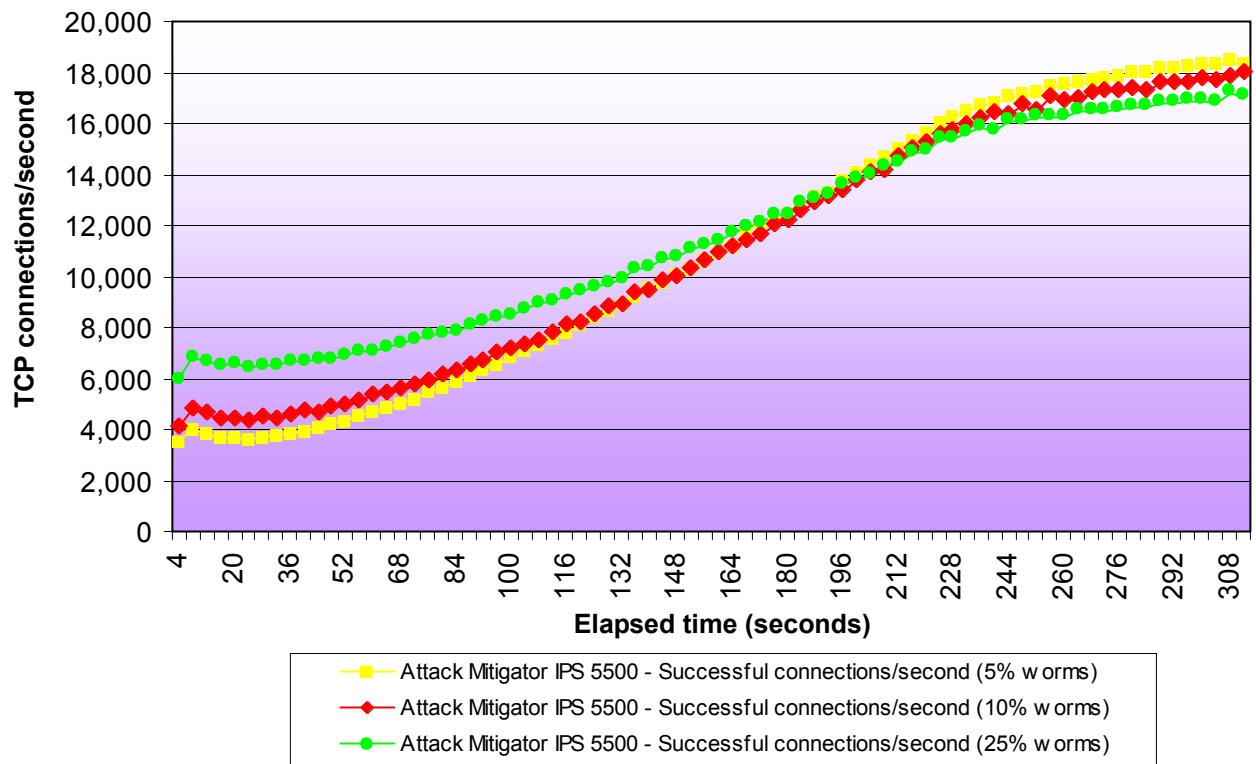
5500 ProtectionCluster™ was configured with two IPS 5500-1000 devices in a high performance, high-availability cluster. The Tolly Group also tested a TippingPoint Technologies, Inc. UnityOne-2400, running software version 1.4.2.6007 and configured with eight 10/100/1000 Ethernet ports (fiber). On the test date, engineers verified that this was the latest software available from the TippingPoint Web site.

For the real-world SYN flood and the embedded worm attack tests, each IPS was connected to a Spirent Communication Avalanche 2200 (running SW ver. 6.2 code) on one side, and a Spirent Communication Reflector (also running SW ver. 6.2 code) on the other side. (See Figure 7.)

For the SYN flood tests, engineers set up the Spirent Avalanche to send 20,000 cps of “good” traffic and flood 100,000 64-byte SYN packets onto the network.

Modifications were required on the Spirent Avalanche since it

Attack Mitigator IPS 5500 Embedded Worm Traffic Attack Various Percentages of Worm Injection as Introduced by Spirent Avalanche/Reflector



Source: The Tolly Group, October 2004

Figure 5

was not truly sending a DDoS attack. These modifications included fixing the source MAC address and varying the source TCP ports, and adding a new field for sequence numbering. The sequence number was used to reflect how the majority of the SYN flood tools available from the Internet run on top of actual TCP stacks. This was added to make the packet as close as possible to a routed SYN request. The addition of the sequence number field did not affect the outcome of any test. For assistance with these modifications, a Spirent

Engineer was hired to make these changes.

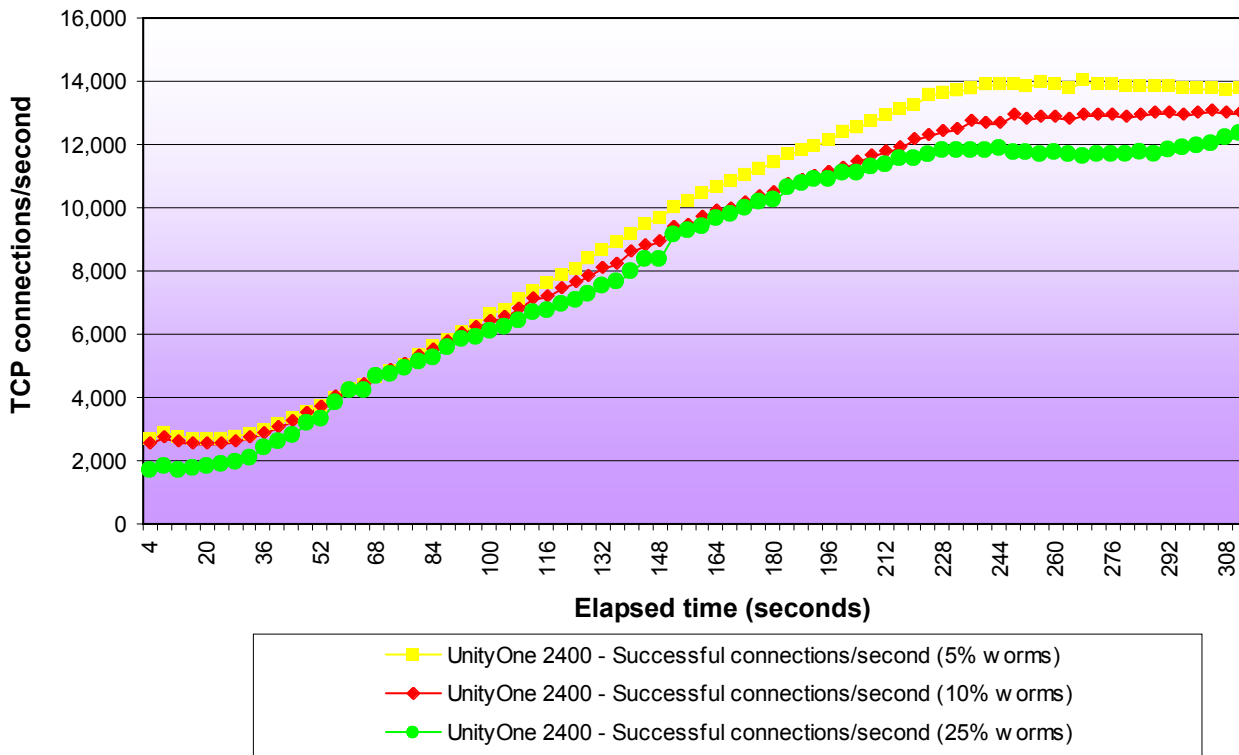
Two port pairs were used on the Spirent gear. Both pairs were configured using virtual routing to simulate a true customer deployment. On one of the port pairs, only good HTTP traffic was configured. On the other port pair, both good HTTP traffic, along with malicious traffic, was sent. The test ran for approximately six minutes and engineers used a 30-second offset from the time good traffic ramped up to the time DDoS attack was sent. This

was a provision to allow the UnityOne-2400 to learn about the Web server and not immediately start to block all legitimate traffic.

The mixed protocol SYN flood test was conducted similarly, though it employed a traffic profile as follows: HTTP – 70% (1K GETs); SMTP – 18% (300-bytes data); POP3 – 10% (256 to 312-bytes data); FTP – 2% (1K – 10K-bytes data).

In the embedded worm test, Avalanche was set up to send 20,000 connections/sec

**UnityOne-2400 Embedded Worm Traffic Attack
Various Percentages of Worm Injection
as Introduced by Spirent Avalanche/Reflector**



Source: The Tolly Group, October 2004

Figure 6

with different percentages of “good” HTTP traffic and “bad” (worm) HTTP traffic.

For the throughput test, engineers measure throughput with frame sizes of 64, 128, 256, 512, 1,028, and 1,518 bytes with a variable offered load ranging from 1 Gbps to 4.4 Gbps for the IPS 5500 and 8.8 Gbps for the IPS 5500 Protection-Cluster. For the IPS 5500 ProtectionCluster, throughput was measured across a pair of Attack Mitigator IPS 5500s, each with an Ixia 400T traffic generator attached to it and

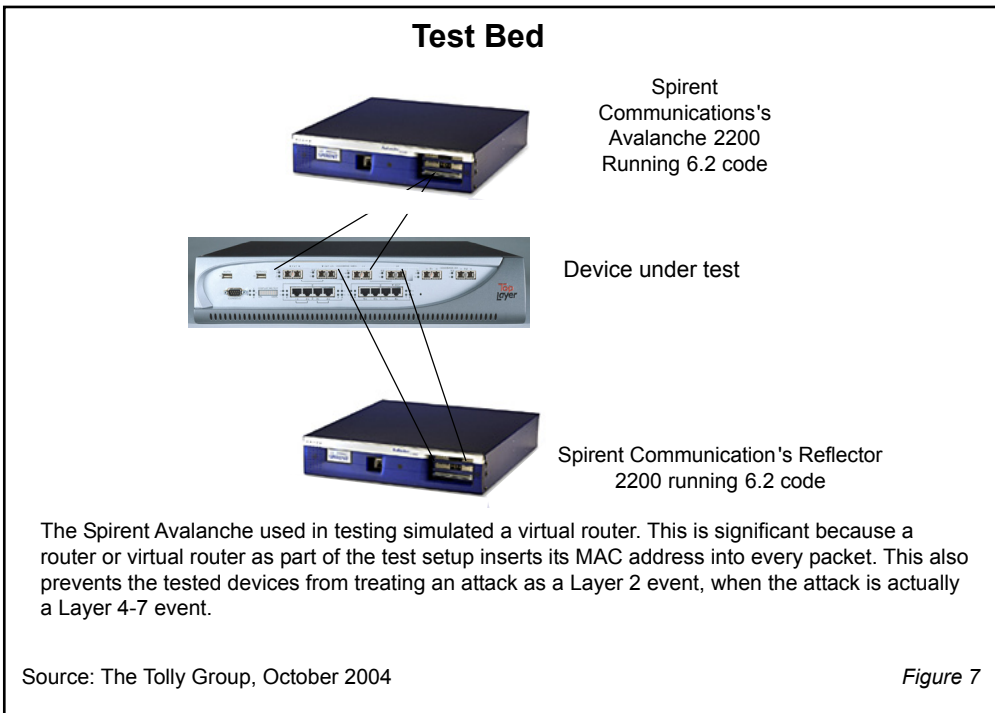
creating offered load to pass across the system.

EQUIPMENT ACQUISITION AND SUPPORT

TippingPoint’s UnityOne-2400 was acquired through normal product distribution channels by Top Layer Networks. The Tolly Group contacted executives at TippingPoint and invited them to provide a higher level of support than available through normal channels. The vendor declined to participate in the project.

The software level as supplied was 1.4.2.6007 for Tipping-Point’s UnityOne-2400 product. TippingPoint’s phone technical support was used to configure/tune the device for the test suites executed by The Tolly Group.

The Tolly Group verified product release levels and shared test configurations with the vendor in order to give them an opportunity to optimize their devices for the tests. Tipping-Point chose not to comment on the results.

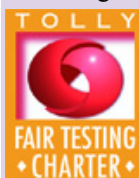


The Tolly Group gratefully acknowledges the providers of test equipment used in this project.

Vendor	Product	Web address
Ixia	IxScriptmate v.4.0.3.3	www.ixiacom.com
Ixia	Ixia 400T /w Gigabit interfaces	www.ixiacom.com
Spirent Communications	Avalanche 2200/Reflector 2200 v.6.2	www.spirentcom.com

TOLLY GROUP SERVICES

With more than 15 years 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 (561) 391-5610, or send E-mail to sales@tolly.com.



For info on the Fair Testing Charter, visit: <http://www.tolly.com/Corporate/FTC.aspx>

PROJECT PROFILE

Sponsor: Top Layer Networks, Inc.

Document number: 204146

Product class: Intrusion Prevention System

Products under test:

- Top Layer Networks Attack Mitigator IPS SW ver. 3.2.16
- TippingPoint Technologies, Inc. UnityOne-2400 SW ver. 1.4.2.6007

Testing window: October 2004

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.

Information 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. 204146 rev. clk 30 Nov 2004