No. 205112 May 2005

Radware, Inc.

DefensePro 3000

Throughput Benchmark and Attack Mitigation Evaluation

Test Summary

Premise: *Intrusion prevention products need to detect and block a wide array of common network and application attack types while under extensive network load to make their usage effective for enterprise and carrier-class clients. Such products also must offer protection to multiple network segments to limit worm propagation, and offer protection from common evasion techniques. And they must do all this while also delivering legitimate traffic.*

Radware, Inc. commissioned The Tolly Group to evaluate its DefensePro 3000, an intrusion prevention switch with Denial of Service (DoS) protection that combines bandwidth management for attack isolation and traffic shaping to offer enterprise and carrier networks protection against a diverse range of network- and application-level attacks.

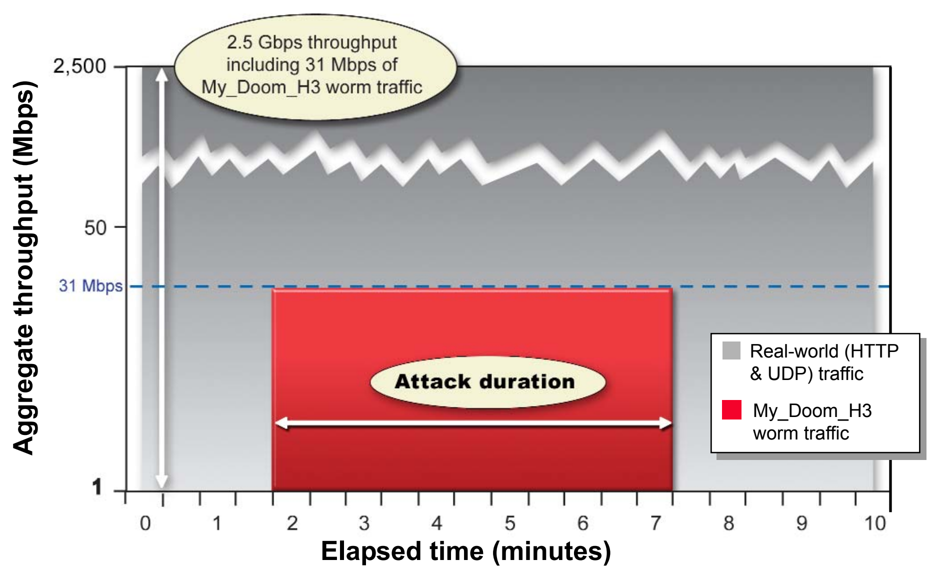
Tolly Group engineers examined the performance of the DefensePro 3000 in various scenarios to understand the maximum throughput offered by the switch while it actively handled various attacks and processed signature loads. Engineers also evaluated the manner in which the DefensePro 3000 was able to detect and block attacks that utilized common evasion techniques and engineers examined a facility that restricts bandwidth to background applications that other-

Test Highlights

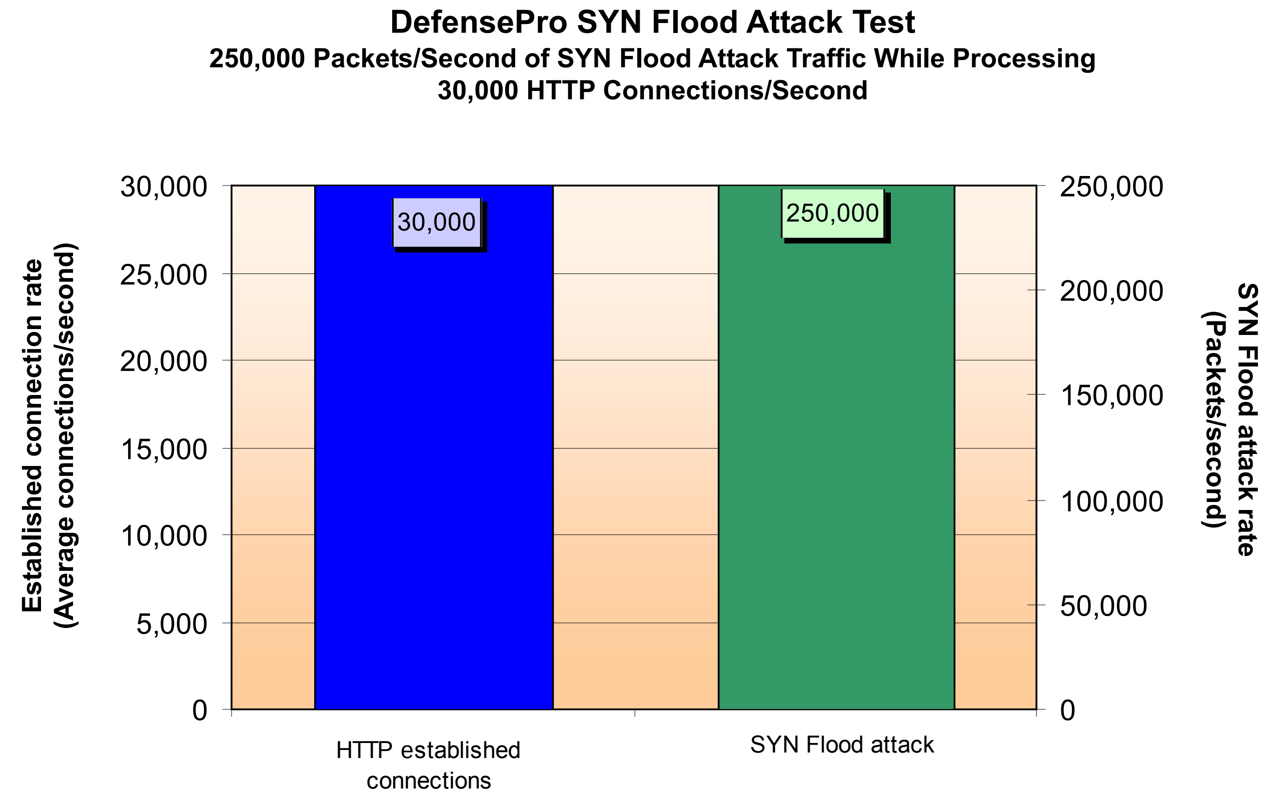
- Blocks inbound Juno2 DoS attacks inbound at 120 Mbps while allowing more than 2 Gbps of legitimate "real-world" traffic (HTTP and UDP) to be forwarded across the network
- Sustains total throughput of 2.5 Gbps while completely stopping a stream of 40,000 "My_Doom" attacks per second with 811 signatures scanned
- Blocks SYN Flood attacks when it sustained processing of 30,000 HTTP connections per second (without failures) while fending off 250,000 pps of SYN Flood traffic
- Detects and blocks a number of common attacks in their normal state even with evasion techniques such as SSL and IP fragmentation attempting to bypass IPS device
- Delivers the ability to use a single device to protect multiple segments of a network, each with a different IPS protection profile

DefensePro Real-World (HTTP & UDP) Traffic Performance

2.5 Gbps of Real-World (HTTP & UDP) Traffic with 811 Signatures Enabled and 40,000 pps (31 Mbps) of My_Doom_H3 worm



Source: The Tolly Group, April 2005 *Figure 1*



Source: The Tolly Group, April 2005

Figure 2

wise could interfere with mission-critical application traffic. Finally, The Tolly Group examined a capability of the DefensePro 3000 to implement protection options for different segments of supported networks, a capability that would prove invaluable to service providers and enterprise LAN implementations. Tests were conducted in April 2005 at Radware facilities in Israel.

Tests show that the DefensePro 3000 is adept at identifying and blocking attacks with zero instances of false positives, while simultaneously handling multi-Gigabit traffic loads. From a performance standpoint, the DefensePro 3000 was able to handle 2.5 Gbps of "real-world" throughput while simultaneously handling either a 40,000-packet per second (pps) worm attack, a 200-Mbps SYN Flood attack or a 100-Mbps DoS attack. Tests also show the DefensePro 3000[1] is capable of protecting Secure Sockets Layer (SSL) data and can isolate attacks to protect mass mailings and control P2P traffic.

Results and Analysis

High Performance Test: Real-World (HTTP & UDP Only) Traffic, High Attack Rate and High Signature Load

Network managers need to understand the capabilities of a network security appliance to process non-threatening HTTP (TCP) and UDP traffic while scanning a large signature base and fending off attacks coming at a high rate.

In this test scenario, engineers ran some 2.47 Gbps of "real-world" (HTTP & UDP) traffic through the DefensePro 3000 while it was filtering 40,000 worm instances per second while scanning over 800 signatures to demonstrate maximum performance as a corporate gateway IPS while showing zero false positive and false negative results. Engineers configured the traffic as 70% HTTP and 30% UDP. HTTP sessions were generated by an Avalanche/Reflector test tool using a 20-Kbyte file size.

The DefensePro 3000 sustained total throughput of 2.5 Gbps

[1] Using 64-byte packet size.

while completely blocking a stream of 40,000 "My_Doom" attacks per second. (See Figure 1.) Furthermore, engineers verified that the DefensePro 3000 was configured with a policy containing 811 signatures. This test illustrates the "carrier-class" strength of the device. That is, it can deliver multi-Gigabit throughput while scanning a large set of attack signatures while fending off a high rate of attacks.

DoS Test: SYN Flood Attack (HTTP-only)

Network managers need to understand the ability of an IPS device to support high HTTP connection rates while simultaneously fending off SYN Flood attacks. With Web-based applications, users need to differentiate between the real clients and the SYN Flood attack and be able to serve many HTTP connections while simultaneously blocking a large SYN attack.

In this test scenario, engineers generated HTTP-only background traffic at a rate of 30,000 HTTP connections per second using the Avalanche/Reflector test tool. Once the "steady-state" was reached, they waited for one to two minutes and then injected SYN Flood traffic using the SmartBits test tool and let the test run for about five additional minutes (300 seconds) in "steady-state" to ensure no unsuccessful transactions were recorded.

Tests show that the DefensePro 3000 was successful in blocking SYN Flood attacks when it sustained processing of 30,000 HTTP connections per second (without failures) while fending off 250,000 pps of SYN Flood traffic. (See Figure 2.) This test shows the "carrier-class" nature of the device in that it can continue to handle 2 Gbps+ of throughput while stopping a high-rate DoS attack that might occur on a high-speed ISP link.

DoS Test: SYN Flood Attack (Mixed Protocol Traffic)

Network managers need to understand the ability of a network security device to support a high-rate mix of HTTP, FTP, POP3, SMTP and DNS connections while simultaneously fending off SYN Flood attacks. This ensures the device under test can serve actual users while blocking a SYN Flood attack.

In this test scenario, engineers demonstrated the ability of the DefensePro 3000 to block SYN Flood attacks inbound at 280,000 pps while allowing 9,500 connections per second (cps) of legitimate "real-world" traffic (HTTP, SMTP, POP3, DNS, and FTP) to be forwarded to the network. An Avalanche/Reflector test tool generated a real-world traffic flow comprised of 85% HTTP traffic, 10% FTP traffic, 2% POP3 traffic, 2% SMTP traffic, and 1% DNS traffic.

Tests show that the DefensePro 3000 was successful in sustaining mixed protocol traffic (Web, E-mail, etc) of 9,500 cps (without failures) while fending off 280,000 pps of SYN Flood traffic. As with the previous tests, this test shows the "carrier-class" nature of the device in that it can continue to handle 2 Gbps+ of throughput while stopping a high-rate DoS attack

Radware, Inc.

DefensePro 3000

Performance and Attack Mitigation Effectiveness

TOLLY Up to Spec CERTIFIED

Radware, Inc.
DefensePro 3000
Product Specifications*

High Port Density
- Up to 11 network segments of protection in a single box
- Enables high capacity scanning across multiple network segments with a single device

Complete Application Security
- Performs bidirectional, stateful, deep packet inspection and accelerated signature matching to immediately block hidden worms, viruses, Trojans and intrusions
- Provides multi-Gigabit speed protection for over 1,500 attack signatures with 24x7 security updates

Stateful Inspection
- Includes access list for application control, and stateful protocol inspection
- Includes RFC compliance verification for protocol misuse protection
- IP defragmentation and TCP reassembly are also performed to overcome evasion techniques

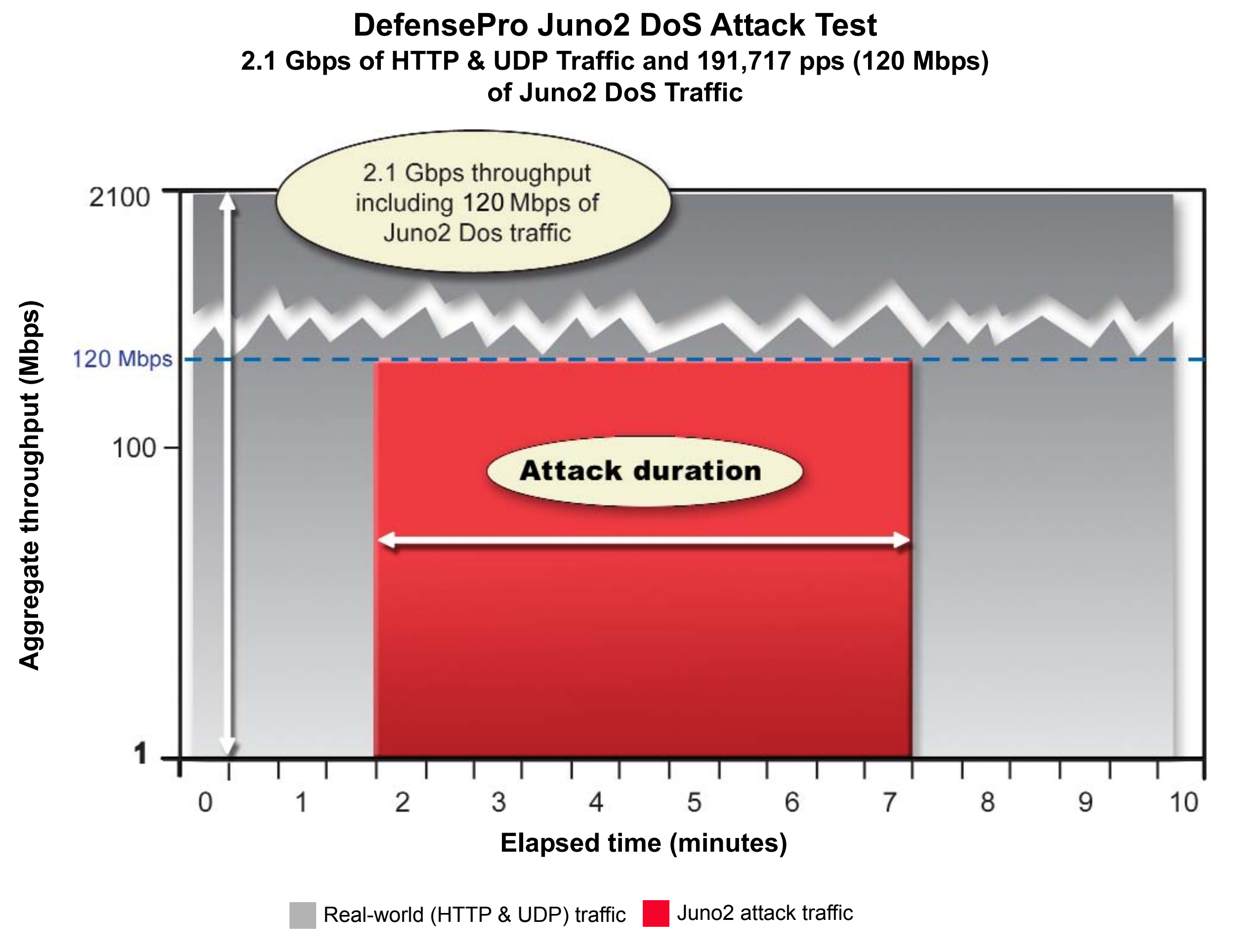
Real-time DoS/DDoS and SYN Flood Attack Protection
- Offers multi-Gigabit Denial of Service/DDoS protection
- Delivers advanced SYN flood protection for known and unknown SYN floods
- Thwarts up to 700,000 SYNs per second

End-to-end Traffic Shaping and Optimization
- Ensures the continuity of mission-critical applications by controlling end-to-end bandwidth to guarantee service levels
- Proactively isolates attack impact, preventing spread to users and applications

P2P Traffic Control
- Controls the bandwidth usage of P2P applications
- Reduces the propagation of worms and viruses via P2P applications

For more information contact:
Radware
575 Corporate Drive, Lobby 1
Mahwah, NJ 07430
Tel: (201) 512-9771
Toll Free: (888) 234-5763
Fax: (201) 512-9774
E-mail: info@radware.com
URL: *www.radware.com*

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



Source: The Tolly Group, April 2005

Figure 3

that might occur on a high-speed ISP link.

DoS Test: Juno Attack

Network managers need to understand the ability of a network security device to detect and prevent various kinds of DoS attacks such as a Juno attack, while serving legitimate users without compromising performance.

In this test scenario, engineers demonstrated the ability of the DefensePro 3000 to block Juno2 DoS attacks inbound at 120 Mbps while allowing more than 2 Gbps of legitimate "real-world" traffic (HTTP and UDP) to be forwarded to the network.

Engineers used the same traffic pattern from the HTTP/UDP SYN Flood test (see related section). Engineers configured the SmartBits to inject Juno2 worm packets at a rate of 120 Mbps. They generated protocol mix (HTTP and UDP) background traffic at a rate of 2.1 Gbps (1.8 Gbps for HTTP and 372 Mbps for UDP) connections per second using the Avalanche/Reflector test tool.

Tests show that the DefensePro 3000 was successful in sustaining total throughput of 2.1 Gbps (varied slightly over time) of HTTP and UDP traffic while completely stopping a stream of 120 Mbps of Juno2 DoS attacks per second. (See Figure 3.) As with the previous tests, this test shows the "carrier-class" nature of the device in that it can continue to handle 2.1 Gbps of throughput while stopping a high-rate DoS attack that might occur on a high-speed ISP link.

Accurate Attack Detection and Protection

When the IPS device protects applications at fast speeds, it is imperative that the security device can still accurately protect your network from various kinds

DefensePro 3000 Attack Evasion Test Results

Type of Attack	Event Description	Detected & Blocked
IP Fragmentation	IP reassembly of fragmented packets	✓
SSL Embedded Attack	Worm NIMDA embedded on SSL (HTTPS) traffic	✓

Source: The Tolly Group, April 2005

Figure 4

of network- and application-level attacks while forwarding all legitimate traffic without compromising performance.

Engineers demonstrated that the DefensePro is capable of detecting and isolating worms, viruses and application-level exploits. DefensePro blocked all attacks, while legitimate traffic (HTTP only) was forwarded to the network with zero false positives.

Tests confirm that the DefensePro 3000 sustained total throughput of 1 Gbps (varied slightly over time) of HTTP traffic while completely stopping a stream of 40,000 "My_Doom" attacks per second. Such results demonstrate the "carrier-class" nature of the device in that it can continue to handle 1 Gbps of Web throughput while stopping a high-rate attack that might occur on a high-speed ISP link.

Evasion Test: Attack Packaged in Encrypted SSL Packet

When the security device inspects traffic at high speeds, it is imperative that the security device can still protect your network from various kinds of network attacks even when the attacker tries to bypass the security device through different evasion techniques such as using encrypted SSL tunnels.

Engineers set out to demonstrate the ability of the DefensePro to mitigate SSL-based attacks and enforce security policies on encrypted traffic that uses different evasion techniques. Because SSL transactions are encrypted, the test requires the use of an adjunct device, the Radware CertainT-100 (Ver 3.03.16) to receive and decrypt SSL traffic mirrored from the main processing path.

(*Note: The SSL appliance was run in parallel with the mainline processing to avoid degrading performance. The SSL appliance decrypts the packet and returns it to the DefensePro for scanning. If the DefensePro detects an attack it immediately terminates the SSL session between end systems.*)

Engineers configured an HTTPS/ HTTP client and server to send/receive a traffic mix of HTTP and HTTPS through the DefensePro 3000 over one segment. HTTPS attacks were injected. The DefensePro 3000 then was tested for 100% attack detection and reporting of SSL or regular attacks. Engineers checked that the HTTPS attacks were reported with SSL context and they checked for zero-rate false positives and zero-rate false negatives.

This test showed that the DefensePro 3000 was able to process a stream of good HTTP and HTTPS traffic and detect/ reset attacks hidden in an encrypted SSL packet. (See Figure 4.) The test demonstrated the beneficial coupling of Radware's SSL appliance with the DefensePro 3000. It illustrates that the solution can overcome the SSL encryption evasion technique used by some hackers.

Evasion Test Using IP Fragmentation

When the security device is processing 1 Gbps of traffic or more it is imperative that the security device can still protect your network from various kinds of network attacks even when the attacker tries to bypass the security device using IP fragmentation to "cloak" the attack.

Engineers demonstrated the ability of the DefensePro 3000 to detect and block a number of common attacks in their normal state, with no evasion technique applied and with evasion techniques. The "FragRoute" public domain program was used to "cloak" the attack using a number of fragmentation techniques. The test was conducted with 1 Gbps of valid background traffic.

Engineers utilized a client PC and a server, representing the attacker and the victim devices, respectively. They next made the appropriate connections between devices using a single-segment configuration in the DefensePro 3000 and client/ server PCs – one segment for attacker (PC) and victim (PC). Engineers first ran a baseline test attack in normal state (no evasion techniques applied). Then, they ran the same number of IP fragmentation attacks using different evasion techniques. Engineers applied a sample of six to eight permutations.

The DefensePro 3000 successfully detected and blocked heavily fragmented attacks that employed variations of fragroute parameters (random, duplicates, etc.) to cloak the attack. (See Figure 4.) This test illustrates that the DefensePro 3000 can successfully reconstruct IP fragments and detect attacks cloaked within.

Bandwidth Management: Peer-to-Peer Traffic Limit Test

Availability of network resources is critical in today's corporate network environments. There are some traffic types, like P2P, that should be allowed through the IPS but should not be allowed to consume all system resources.

Engineers demonstrated the ability of the DefensePro 3000 to differentiate between mission-critical applications and non-critical applications (such as P2P) and limit the bandwidth consumed by the non-critical applications.

Engineers made the necessary connections between DefensePro 3000, Avalanche/Reflector and the SmartBits test tools in a dual-segment configuration (one segment for the P2P traffic from SmartBits and the other for HTTP traffic).

P2P traffic was created by copying a real P2P frame capture to the SmartBits frame creation buffer. (P2P used was a capture of eDonkey traffic.) From the DefensePro 3000, engineers set the P2P traffic limit along with security policies and created a policy to limit P2P traffic to 50 Mbps. Then they generated 200 Mbps of traffic (100 Mbps P2P traffic, and 100 Mbps HTTP traffic) using Avalanche/ Reflector and SmartBits test tools respectively.

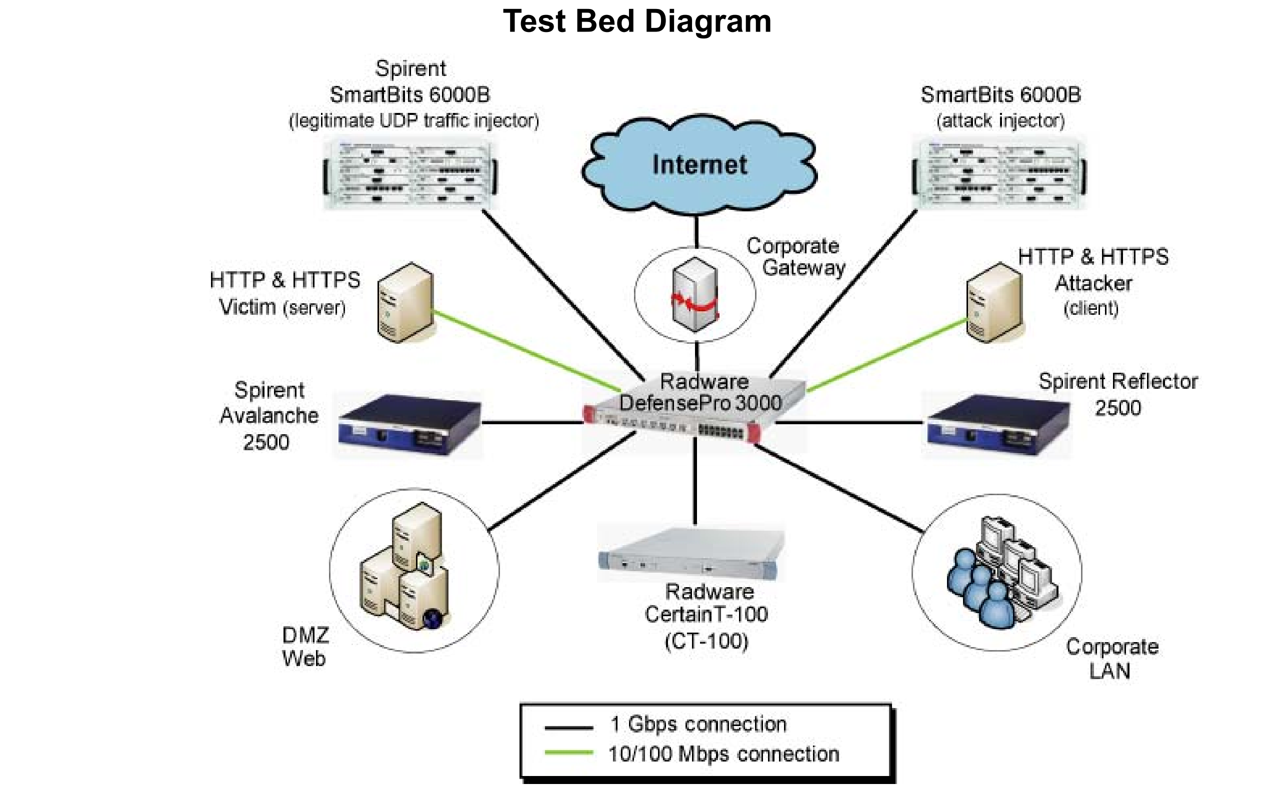
Engineers observed input P2P of 100 Mbps and output of 50 Mbps. Simultaneously, 100 Mbps of HTTP was passing through the system. Bandwidth management typically is not a feature of IPS devices. Normally, such devices take a "black or white" approach. That is, traffic is either "disallowed" and dropped or "allowed" and forwarded. More and more, we see a "gray" area like P2P where traffic should pass so long as it does not consume excessive bandwidth resources. This feature provides a powerful element of control for "gray" traffic and is highly desirable for Second Pass through the DefensePro 3000 and university environments whose links can get inundated with P2P traffic.

Attack Isolation Mass-Mailing Protection Test

The availability of network resources is a given in today's corporate networks. There are some traffic types, like SMTP, that should be allowed through the IPS but should not be allowed to consume all system resources. Furthermore, since SMTP can also be a vehicle for various attacks, it is essential that an IPS can isolate SMTP attacks – while processing background traffic to ensure critical application performance even under attack.

Engineers demonstrated that the DefensePro 3000 differentiates between mission-critical applications ensuring that if one of them is under attack the other critical applications will operate normally. At the same time, the test illustrated the DefensePro 3000 can both detect and stop SMTP "mass mailing" attacks and process 1 Gbps of background traffic.

Engineers set the mail traffic limit of the DefensePro 3000 to 45 Mbps along with security policies. They then generated 1 Gbps of



Source: The Tolly Group, April 2005

Figure 5

background traffic (HTTP) traffic using Avalanche/Reflector. Next they generated 20,000 pps of SMTP "mass mailing" attacks via SmartBits and generated 200 Mbps of "good" SMTP traffic (which subsequently was managed by the DefensePro 3000).

With SMTP bandwidth configured to a 45 Mbps ceiling, engineers observed input SMTP of 200 Mbps and output of 45 Mbps. Simultaneously, 100 Mbps of HTTP was passing through the system. Furthermore, all SMTP "mass mailer" attacks were blocked and 1 Gbps of background traffic successfully passed through the DefensePro 3000.

Multi-Segment Capabilities Test

Service providers and large enterprises may need the flexibility to implement different protection options for different segments of their networks.

Engineers demonstrated the ability of the DefensePro 3000 to use a single device to protect multiple segments of a network, each with a different protection profile. Three segments were created with different profiles and labeled as: Corporate Gateway, DMZ Web and Corporate LAN. The test illustrated that different protection profiles were assigned to each and that they functioned properly.

Logs from the DefensePro 3000 show three logically separate IPS "systems" running on a single multi-port switch. This functionality can provide economical scalability for large enterprises and service providers since they can avoid the need to purchase a separate device for each logical network.

Related Tests

Two of the tests conducted for this report are similar to tests previously conducted on other products. The Real-World (HTTP & UDP Only) Traffic, High Attack Rate and High Signature Load test related to test results in Tolly Group Test Summary # 203101, a February 2003 report focusing on Tipping Point Technologies, Inc.'s UnityOne Intrusion Prevention Appliance. The DoS Test: SYN Flood Attack (HTTP-only) test in this report relates to results found in Tolly Group Test Summary # 204146, a December 2004 competitive evaluation of Top Layer Networks Attack Mitigator IPS 5500 IPS versus a TippingPoint UnityOne-2400. Both free reports are available at *http://www.tolly.com*.

Test Configuration and Methodology

For performance tests, The Tolly Group tested a Radware DefensePro 3000 running software version 2.40.02, with AttackDB Build Ver. 4.00. The IPS/IDS device was outfitted with seven Gigabit Ethernet and 16 Fast Ethernet ports (Only six of the Fast Ethernet ports were used in testing).

A brief description for each of the test methodologies is incorporated into each of the results sections above. Given the number of tests conducted, there was not ample room in this report for a complete methodology description.

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

Vendor	Product	Web address
Open Source	Fragroute v.1.2	http://www.monkey.org/~dugsong/fragroute/
Spirent Communications	Avalanche/Reflector 2500 v.6.24.32276	http://www.spirentcom.com
Spirent Communications	SmartWindow v.8.50.120	http://www.spirentcom.com
Spirent Communications	SmartBits 6000B	http://www.spirentcom.com

Project Profile

Sponsor: Radware, Inc.
Document number: 205112
Product class: Intrusion detection/prevention security appliance
Products under test: DefensePro 3000
Testing window: April 2005
Software versions tested:

- Software Ver. 2.40.02, AttackDB Build Ver. 4.00.

Software status: Currently 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.