THE TOLLY GROUP

No. 205136 November 2005

Reflex Security, Inc.

IPS100 Intrusion Prevention Appliance

Performance, Security and Usability Evaluation

Test Summary

***Premise:** Intrusion prevention systems (IPS) provide a proactive defense that detects and blocks attacks concealed in network traffic streams. An effective IPS solution needs to 1) provide wire-speed inspection performance that doesn't impede the flow of legitimate traffic; 2) protect against a wide range of security threats; 3) be highly reliable and support an appropriate response in the event of failure, and; 4) make it easy for users to safeguard their networks and appropriately respond to security events.*

Reflex Security, Inc. commissioned The Tolly Group to test the Reflex IPS100 network intrusion prevention appliance. The Reflex IPS blocks a comprehensive range of malicious traffic, including HTTP attacks, Denial-of-Service attempts, scans, backdoor exploits, floods, viruses, and worms. The Tolly Group validated the performance of the Reflex IPS, as well as the appliance's effectiveness at detecting and preventing a variety of attacks. The Tolly Group also evaluated the system's reliability, reporting and ease of use.

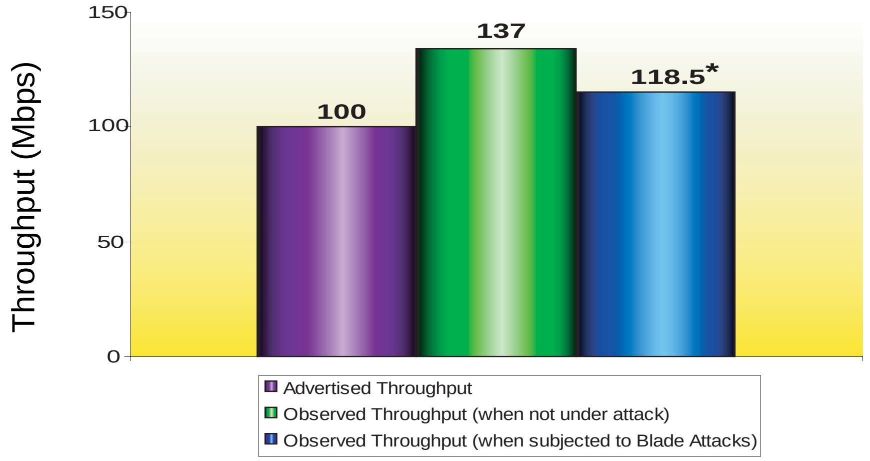
Tolly Group engineers conducted a battery of performance tests, focusing on HTTP throughput across the Reflex IPS appliance under normal conditions, and when subjected to attack traffic generated by Blade Software IDS Informer. They also performed a security test to measure the number of IDS Informer attacks blocked by the Reflex IPS100 while handling HTTP traffic in the background, and tests were also conducted to verify that the Reflex IPS100 appliance could block E-mails infected with worms and viruses.

Test Highlights

- Average bidirectional HTTP throughput well in excess of 100 Mbps using mixed object size traffic, both under normal traffic conditions, and while detecting and blocking 580 different attacks generated by Blade Software IDS Informer
- Detects and blocks 580 out of 580 attacks from the Blade Software IDS Informer (Attack Pack 4) in the presence of a background HTTP traffic of 118.5 Mbps
- Monitors SMTP traffic to block E-mails with attachments infected with various viruses and worms
- Supports high-availability using failover (fail-open and fail-close) mechanisms in the event of hardware and/or software failures
- Offers powerful, fully customizable reporting capability with real-time event aggregation/correlation, easy installation and configuration, centralized management capability and automated attack signature updates

Reflex Security IPS100 Intrusion Prevention Appliance Average Steady-State Bidirectional HTTP Throughput

across two Gigabit Ethernet ports as reported by Spirent Avalanche and Blade Software IDS Informer (Attack Pack 4)

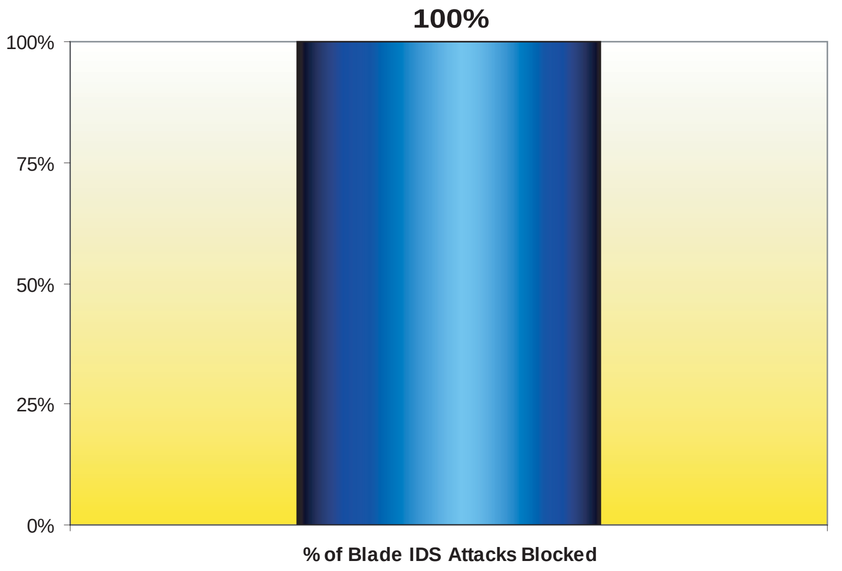


The Reflex IPS100 appliance was loaded with 1,288 attack signatures (including default signature set and the Blade attack signatures). Blade Software IDS Informer generated 580 different attacks. Spirent Avalanche and Reflector simulated bidirectional HTTP traffic across two Gigabit Ethernet ports on the IPS100 sensor.

*Ignoring the bandwidth corresponding to the attack traffic.

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

Reflex Security IPS100 Intrusion Prevention Appliance
Percentage of Attack Detection and Prevention
as reported by Blade Software IDS Informer* (Attack Pack 4)



Note:The Reflex IPS100 appliance blocked 580 out of 580 attacks generated by Blade IDS Informer Attack Pack 4, while processing 118.5 Mbps of bidirectional HTTP traffic generated by the Spirent Avalanche and Reflector.

Source: The Tolly Group, October 2005 *Figure 2*

Testing was conducted in September-October 2005, at Reflex Security's labs in Atlanta, GA and The Tolly Group's labs in Boca Raton, FL.

Results & Analysis

HTTP Performance Evaluation Test

Tolly Group engineers measured the Layer 4 HTTP performance of the Reflex IPS100 appliance in terms of bidirectional steady-state throughput and the number of connections established per second. The IPS100 appliance was tested under a normal traffic scenario, and while being subjected to more than 500 attacks generated by Blade Software IDS Informer.

HTTP traffic was generated using Spirent Avalanche and Reflector to simulate real-world HTTP transactions (TCP open – HTTP data transfer – TCP close). HTTP 1.1 was used with persistence mode enabled. Spirent Avalanche emulates Web clients generating requests for the chosen object sizes, and the Spirent Reflector emulates Web server responding to those requests.

Mixed-Object HTTP Throughput

Tolly Group engineers measured the steady-state bidirectional HTTP throughput of the IPS100 appliance under normal traffic conditions. The Web clients emulated by Spirent Avalanche requested 15 different objects ranging in size from 43 bytes to 64Kbytes, and the Web server emulated by Spirent Reflector responded to those requests. In this scenario, the HTTP traffic was passed through the Reflex IPS100 appliance and it achieved an average steady-state bidirectional HTTP throughput of 137 Mbps. This throughput is well beyond the device's advertised throughput of 100 Mbps. (See Figure 1.) This shows that under normal traffic conditions, the Reflex IPS100 delivers a performance beyond the advertised throughput of the device – thus delivering the promised value to the customer.

Mixed-Object HTTP Throughput Under Attack

Tolly Group engineers also evaluated the performance of the Reflex IPS100 appliance in terms of HTTP throughput while being subjected to 580 Blade IDS Informer attacks. This test provides valuable data to network managers regarding the impact of attack traffic on network performance, and the impact of the network traffic on the attack blocking performance of the appliance.

In this test, engineers passed HTTP traffic generated by Spirent Avalanche and Reflector, along with the attack traffic generated by IDS Informer through the Reflex IPS100 appliance. Once the HTTP traffic reached a steady-state, Blade Software's Attack Pack 4 was used with IDS Informer to generate HTTP attacks, Denial-of-Service attempts, scans, backdoor exploits, floods, viruses, and worms.

In this scenario, engineers found that the Reflex IPS100 demonstrated an average bidirectional HTTP throughput of 118.5 Mbps (not counting the attack traffic bandwidth) while it blocked 100% (580 out of 580) of the attacks generated by Blade Software IDS Informer. This shows that the Reflex IPS100 exceeds its advertised performance of 100 Mbps bidirectional throughput even while blocking 580 different attacks and that the attack blocking performance of the appliance is not compromised even when operating beyond its rated performance limit.

Reflex Security, Inc.

IPS100 Intrusion Prevention Appliance

Performance, Security and Usability Evaluation

TOLLY Up to Spec CERTIFIED

Maximum Connection Rate

Tolly Group engineers also tested the Reflex IPS100 appliance to measure the number of TCP connections that the appliance is capable of creating and closing per second in an ideal scenario. When using a security device in a network environment, network managers want to verify the TCP traffic handling capacity such as the maximum concurrent TCP connections and the maximum TCP connection rate (connections/sec). No failed transaction is allowed for this test.

The HTTP traffic was generated using Spirent Avalanche and Spirent Reflector. The clients emulated by the Spirent Avalanche request an 8-byte object repeatedly from the Web server emulated by Spirent Avalanche using HTTP 1.1, and the number of HTTP connections successfully created and torn down per second was measured. Under these circumstances, the Reflex IPS100 appliance established an average of 2,408 connections per second.

Security Evaluation Test

Blade Software IDS Informer Attack Prevention

Tolly Group engineers tested the security capability of the Reflex IPS100 appliance in terms of blocking different types of intrusion attacks generated by Blade Software IDS Informer. This test provides valuable information to network managers to understand the capabilities of the Reflex IPS100 appliance to detect and prevent network-based attacks prior to deployment in a network infrastructure.

This test used Blade Software's Attack Pack 4 with the IDS Informer to generate HTTP attacks, Denial-of-Service attempts, scans, backdoor exploits, floods, viruses, and worms. In this test, the Reflex IPS100 appliance successfully blocked 100% (580 out of 580) of the attacks generated by IDS Informer. (See Figure 2.) The Reflex Command Center monitoring the Reflex IPS100 appliance correctly generated alerts and reports on the various attacks detected and prevented. (See Figure 3.) This shows that the Reflex IPS100 has the ability to block various malicious attacks and provide powerful defense against well known network-based attacks.

Virus/Worm Attack Prevention

Tolly Group engineers also tested the ability of the Reflex IPS100 appliance to block SMTP traffic containing a selection of common viruses and worms. Spirent Avalanche was used to emulate SMTP clients and Spirent Reflector test tool emulated SMTP server. The SMTP clients emulated by the Spirent Avalanche

Reflex Security, Inc.
IPS100 Intrusion Prevention Appliance
Product Specifications*

Attack Prevention

- Protocol anomaly detection
- Distributed Denial-of-Service detection
- Packet flood detection
- Signature detection
- Port-scanning detection
- Network level user and server permission validation
- SYN packet flood detection

Precision

- 100% detection
- 100% denial
- Anti-virus gateway
- Mitigation by packet stream filtering, resource blocking or alerting

Performance

- Exceeds 100 Mbps throughput
- Sentrium™ solid state, driveless architecture
- Three network interfaces
- Over 2,400 new sessions per second

Easy to Setup and Manage

- Quick setup and out-of-box protection
- Centralized management through Reflex Command Center

Reflex Command Center

- User friendly GUI
- Aggregated and correlated alerts
- IPS and IDS capability
- Flexible reporting engine
- Auto signature updates
- Custom signature interface
- Secure SSH/SSL communication

For more information contact:
Reflex Security, Inc.
5730 Glenridge Drive - Suite 104
Atlanta, GA 30328
Phone: 770-408-2034
Fax: 770-408-2035
URL: ***http://www.reflexsecurity.com***

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

Reflex Security IPS100
Attack and Suspicious Event Types Blocked
(Introduced by IDS Informer, Attack Pack 4)

Attack events:	**Detected & blocked (580/580)**	**Attack events:**	**Detected & blocked**
HTTP	✓	Backdoor	✓
NetBIOS	✓	Covert channel	✓
Buffer overflow	✓	Vulnerability probing	✓
Trojans	✓	Port scanning	✓
Bots	✓	Stealthy port scanning	✓
Remote control mechanisms	✓	Network-based worms	✓
Malcode	✓	Encoding failures	✓
Viruses (85,000 signatures)	✓	Cross-site scripting	✓
Worms	✓	**Suspicious events:**	**Detected & blocked**
Denial of Service	✓	Probe	✓
Distributed DoS	✓	Protocol anomaly	✓
Flood	✓	Protocol violation	✓

Source: The Tolly Group, October 2005

Figure 3

generated E-mail messages containing attachments infected with selected viruses and worms. The Reflex IPS100 appliance monitored the traffic destined to the SMTP servers emulated by the Spirent Reflector. It was verified that the Reflex IPS100 successfully detected and blocked all the infected messages.

This test shows that the Reflex IPS100 appliance with available Antivirus module can monitor SMTP traffic successfully to detect and block viruses and worms.

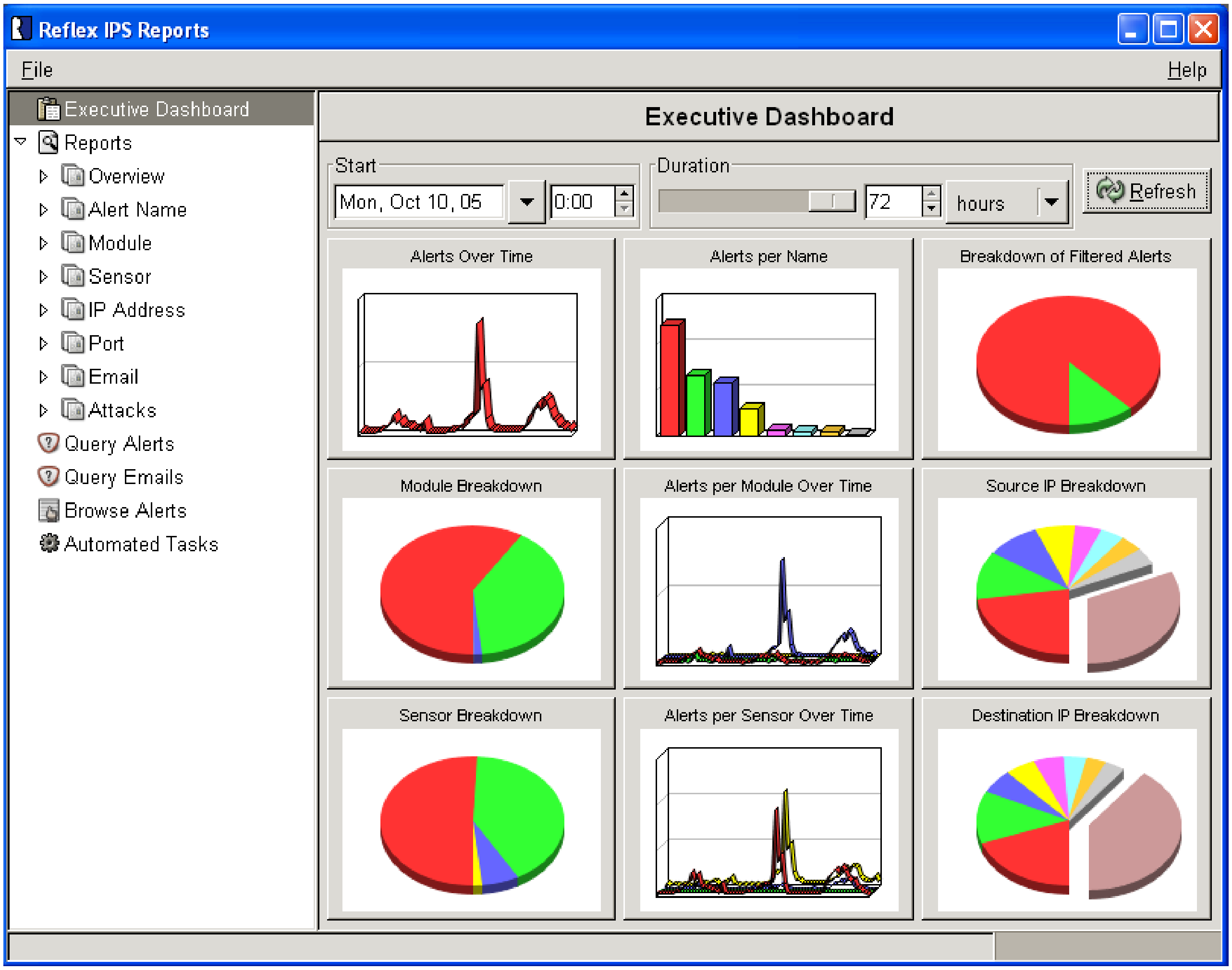
Reliability Test

High availability of network resources is critical in today's corporate network environments. Mission-critical applications on the network have become vital to the success and productivity of organizations and the unavailability of these resources for any length of time would result in critical damage. Network managers realize that devices at the core of their networks should include features that allow for high availability.

Engineers tested the Reflex IPS100 to verify its reliability features like fail-over in the event of a hardware failure, and Reflex Security's patent-pending Sentrium™ disk-on-chip architecture.

The Reflex IPS100 appliance sup-

The Reflex IPS Executive Dashboard



Start: Mon, Oct 10, 05 0:00

Duration: 72 hours

The Reflex IPS Executive Dashboard provides a cohesive, ongoing view of security events and can forward critical notifications to E-mail, SNMP or syslog recipients. Detailed reports can also be created ad-hoc or automatically distributed on a user defined schedule.

Source: The Tolly Group, October 2005

Figure 4

ports fail-over (fail-open or fail-close) in the event of software or hardware failures. The Fail-open allows all the traffic to pass in the event of failure and the Fail-close blocks all the traffic. The engineers tested the fail-open feature in the event of power failure to the appliance. Tolly Group tests confirmed the appliance's ability to consistently fail-open or fail-closed as configured. As a result, administrators can set policy to allow traffic to pass or be denied in the event of a device malfunction.

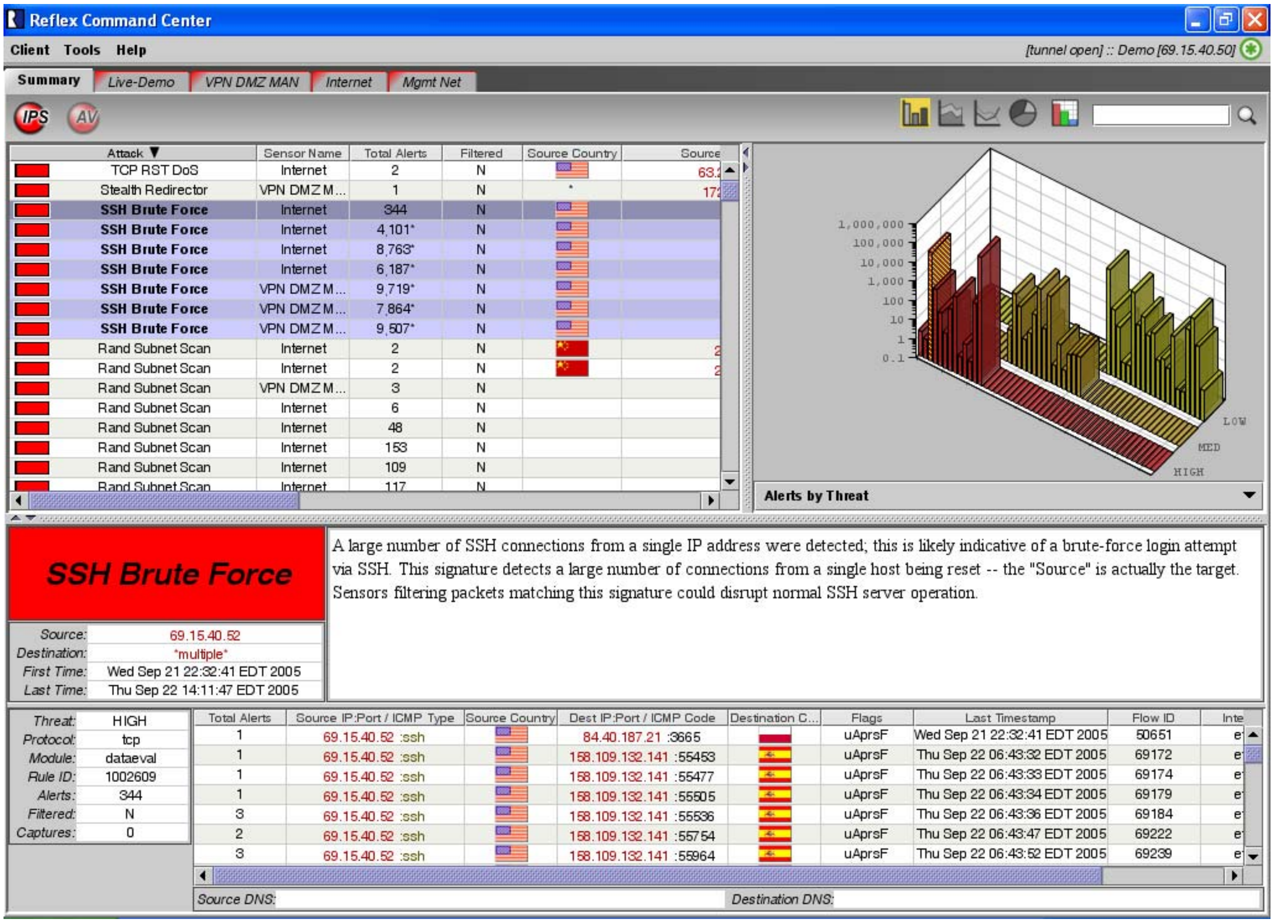
The Tolly Group tested the Reflex IPS100 appliance, which leverages the unique solid state Sentrium™ architecture. As tested, the Reflex IPS100 was configured with a 64MB flash chip. Reflex Security claims the company's Sentrium architecture offers adaptability and performance without the typical failure point of a hard drive in the appliance.

Management and Ease-of-Use Test

Deploying and managing any IPS device should be straightforward and user-friendly in order to fulfill the network security requirements quickly and completely. Network administrators need to understand what features are most important to them.

Tolly Group engineers tested the "Ease-of-Use" and management aspects provided by the Reflex IPS100 and recorded their experience and opinion. Tolly Group engineers noted that the Reflex IPS100 offers a powerful, fully customizable reporting capability with real-time event aggregation/correlation that helps administrators easily analyze security incidents and respond appropriately. Engineers

The Reflex Command Center



	Attack ▼	Sensor Name	Total Alerts	Filtered	Source Country	Source
🟥	TCP RST DoS	Internet	2	N	🇺🇸	63.2
🟥	Stealth Redirector	VPN DMZ M...	1	N	*	172
🟥	**SSH Brute Force**	Internet	344	N	🇺🇸	
🟥	**SSH Brute Force**	Internet	4,101*	N	🇺🇸	
🟥	**SSH Brute Force**	Internet	8,763*	N	🇺🇸	
🟥	**SSH Brute Force**	Internet	6,187*	N	🇺🇸	
🟥	**SSH Brute Force**	VPN DMZ M...	9,719*	N	🇺🇸	
🟥	**SSH Brute Force**	VPN DMZ M...	7,864*	N	🇺🇸	
🟥	**SSH Brute Force**	VPN DMZ M...	9,507*	N	🇺🇸	
🟥	Rand Subnet Scan	Internet	2	N	🇨🇳	2
🟥	Rand Subnet Scan	Internet	2	N	🇨🇳	2
🟥	Rand Subnet Scan	VPN DMZ M...	3	N		
🟥	Rand Subnet Scan	Internet	6	N		
🟥	Rand Subnet Scan	Internet	48	N		
🟥	Rand Subnet Scan	Internet	153	N		
🟥	Rand Subnet Scan	Internet	109	N		
🟥	Rand Subnet Scan	Internet	117	N		

SSH Brute Force

A large number of SSH connections from a single IP address were detected; this is likely indicative of a brute-force login attempt via SSH. This signature detects a large number of connections from a single host being reset -- the "Source" is actually the target. Sensors filtering packets matching this signature could disrupt normal SSH server operation.

Source:	69.15.40.52
Destination:	*multiple*
First Time:	Wed Sep 21 22:32:41 EDT 2005
Last Time:	Thu Sep 22 14:11:47 EDT 2005

Threat:	HIGH
Protocol:	tcp
Module:	dataeval
Rule ID:	1002609
Alerts:	344
Filtered:	N
Captures:	0

Total Alerts	Source IP:Port / ICMP Type	Source Country	Dest IP:Port / ICMP Code	Destination C...	Flags	Last Timestamp	Flow ID	Inte
1	69.15.40.52 :ssh	🇺🇸	84.40.187.21 :3665		uAprsF	Wed Sep 21 22:32:41 EDT 2005	50651	e
1	69.15.40.52 :ssh	🇺🇸	158.109.132.141 :55453	🇪🇸	uAprsF	Thu Sep 22 06:43:32 EDT 2005	69172	e
1	69.15.40.52 :ssh	🇺🇸	158.109.132.141 :55477	🇪🇸	uAprsF	Thu Sep 22 06:43:33 EDT 2005	69174	e
1	69.15.40.52 :ssh	🇺🇸	158.109.132.141 :55505	🇪🇸	uAprsF	Thu Sep 22 06:43:34 EDT 2005	69179	e
3	69.15.40.52 :ssh	🇺🇸	158.109.132.141 :55536	🇪🇸	uAprsF	Thu Sep 22 06:43:36 EDT 2005	69184	e
2	69.15.40.52 :ssh	🇺🇸	158.109.132.141 :55754	🇪🇸	uAprsF	Thu Sep 22 06:43:47 EDT 2005	69222	e
3	69.15.40.52 :ssh	🇺🇸	158.109.132.141 :55964	🇪🇸	uAprsF	Thu Sep 22 06:43:52 EDT 2005	69239	e

Source DNS:

Destination DNS:

The Reflex Command Center central management console provides real-time event aggregation, correlation and visualization that helps administrators quickly identify and react to urgent security incidents. The Command Center provides detailed attack information and facilitates an immediate response with simple right-click access to policy definition and Reflex configuration tools.

Source: The Tolly Group, October 2005

Figure 5

also noted other compelling features of the Reflex IPS100:

- Easy installation and configuration. The Reflex IPS 100 was installed and operational in less than 30 minutes.

- Centralized management capability. Reflex IPS appliances can be controlled from a single console, making it easy and cost-effective to manage security in larger deployments on distributed enterprise networks.

- Automated attack signature updates. This will help ensure effective protection against emerging threats and reduce security management effort.

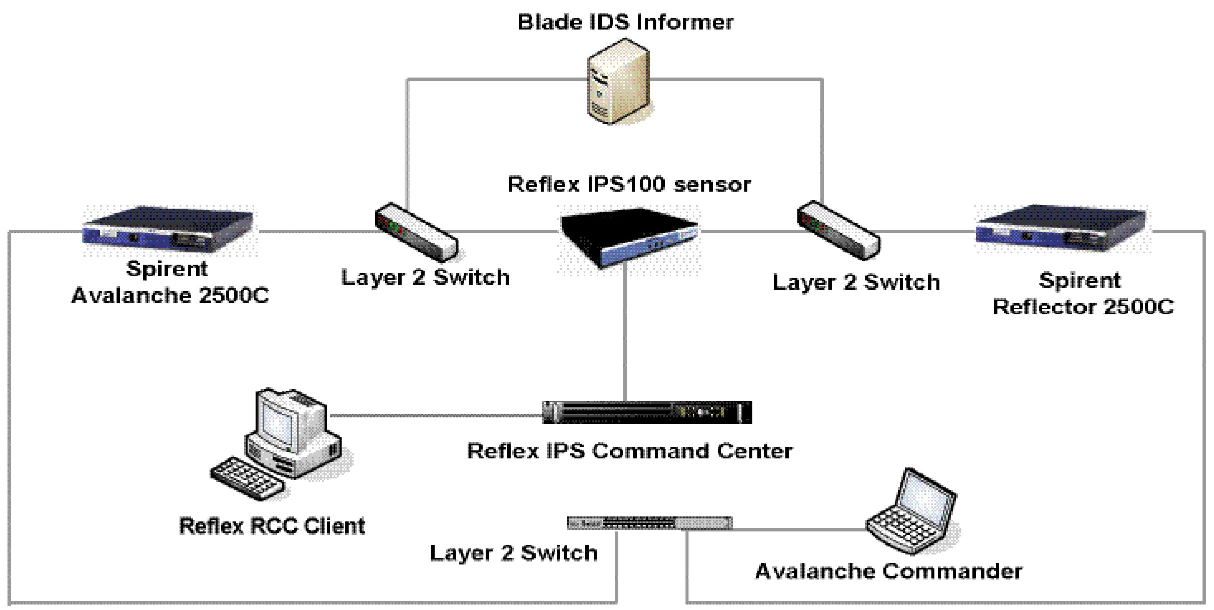
As shown in Figure 4, the user interface of the Reflex IPS100 provides a cohesive, ongoing view of security events and can forward critical notifications to E-mail, SMNP or syslog recipients. Detailed reports can also be created ad-hoc or automatically distributed on a user-defined schedule.

The Reflex Command Center shown in Figure 5 is a central management console that provides real-time event aggregation, correlation and visualization that helps administrators quickly identify and react to urgent security incidents. The Reflex Command Center works with a Reflex IPS core which can in turn monitor multiple Reflex IPS sensors deployed across the network. The Command Center provides detailed attack information and facilitates an immediate response with simple right-click access to policy definition and Reflex configuration tools.

Test Configuration and Methodology

The Tolly Group tested Reflex Security's IPS100 Intrusion Prevention Appliance (ver 4.4) with Reflex

Test Bed Diagram for Performance and Security Tests



Source: The Tolly Group, October 2005

Figure 6

Security Core (ver 4.4.3.4) along with the Reflex Command Center (ver 4.4.3.4). According to Reflex, this is production code and available to the general public. The testing focused on HTTP performance, security capability, reliability and ease of use of the IPS100 appliance.

The Reflex IPS100 sensor was configured with the DataEval, PermEval, ProtoEval, FloodEval, ScanEval, SynEval and VirusEval modules, along with 1,288 signatures (including the default signature set of IPS100, and signatures corresponding to Blade IDS attacks).

The Reflex IPS100 Command Center (RCC) appliance was configured with an Intel Pentium 4 processor operating at 2.8 GHz, containing 1GB of RAM, two Intel 82540EB Gigabit Ethernet cards, two Broadcom NetXtreme BCM5704 Gigabit Ethernet cards, and running Debian-based Linux with kernel version 2.4.311-P4-UP. The RCC was configured with an Intel Pentium 4 processor operating at 2.4 GHz, containing 1GB of RAM, two Intel 82546EB Gigabit Ethernet controller cards, and running SuSE Linux version 9.1 kernel 2.6.5-7.201-default.

The Blade IDS Informer test tool was running on a PC with an Intel Pentium 4 processor operating at 2.4 GHz, containing 512MB RAM, three Intel 82546EB Gigabit Ethernet cards, and running Microsoft Windows XP. Blade Software's Attack Pack 4 was used with 580 different attacks.

For the HTTP Performance tests, the test bed was connected as shown in Figure 6. The Spirent Avalanche emulates Web clients generating HTTP requests for specific object sizes. The Spirent Reflector emulated a Web server that responded to the client requests. For the performance tests under normal traffic conditions, average throughput and connection rate was measured during the steady state with no unsuccessful transactions. To measure the performance of the IPS100 appliance when it was under attack, the HTTP traffic from Avalanche was mixed with attack traffic generated by the Blade Software IDS Informer. The Avalanche traffic was allowed to reach a steady-state before introducing the Blade attack traffic. The load profile on the Avalanche was adjusted so that there were no unsuccessful transactions during the steady-state (of at least five-minute duration). The average throughput was measured, and the number of Blade IDS Informer attacks blocked by the Reflex IPS100 appliance was obtained from the reports generated by the IDS Informer and the Blade Command Center.

For the security tests, the test bed is as shown in Figure 6. The ability of the Reflex IPS100 to detect and block malicious network traffic was tested with HTTP background traffic. The Blade IDS Informer Attack Pack 4 was used and the Reflex IPS100 was configured with the latest signature set to detect the IPS attacks. The attack traffic generated by the Blade IDS Informer was passed through the IPS100 sensor, and the number of attacks detected and blocked by the IPS100 sensor was noted from the reports generated by the IDS Informer and the Reflex Command Center. The IPS100 also was tested to determine its ability to monitor SMTP traffic and block E-mails with attachments infected with viruses and worms. For this test, the Avalanche and Reflector were connected to the Reflex IPS100 sensor. The Avalanche emulated SMTP clients sending E-mails with virus and worm infected attachments to the Reflector emulating an SMTP server. The viruses and worms used in the attachments of the E-mails were generated by the Avalanche are shown in Figure 3.

To evaluate the reliability of the Reflex IPS100, the engineers tested the fail-open feature of the appliance in the event of a hardware or software failure. Two PCs were connected to the IPS100 sensor, and a continuous train of PING commands were run between the two PCs. With the PINGs running, the IPS100 sensor was powered off. It was observed that a few PINGs were dropped before the traffic started flowing again—indicating the fail-open feature of the IPS100 sensor.

TESTED with SPIRENT

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

Vendor	Product	Web address
Spirent Communications	Avalanche ver. 7.0	***http://www.spirentcom.com***
Spirent Communications	Avalanche 2500C Network Edition	***http://www.spirentcom.com***
Blade Software	IDS Informer ver 1.0.467	***http://www.bladesoftware.net***

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: Reflex Security, Inc.

Document number: 205136

Product class: Intrusion Prevention Appliance

Products under test:

- Reflex Security IPS100 Intrusion Prevention Appliance (sensor and core)
- Reflex Command Center

Testing window: September-October 2005

Software versions tested:

- IPS100 Version 4.4
- Reflex Command Center Version 4.4.3.4

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.

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. 205136 rev. dmk 17 Nov 05