

# iPolicy Networks

## iPolicy-6420 Intrusion Prevention Firewall

### Competitive Performance Evaluation versus Fortinet FortiGate-3600 Anti-Virus Firewall



Test  
Summary

*Premise: Multifunction security appliances promise to offer two key advantages: (1) eliminate the risk of blended threats (multi-vector threats) and (2) save money by consolidating a number of security services into one box. But for such devices to be truly effective they must handle peak processing loads and deliver optimum connection set up rates even as security applications are active, adding processing overhead.*

iPolicy Networks commissioned The Tolly Group to evaluate and compare its iPolicy-6420 Intrusion Prevention Firewall (consisting of the iPolicy-6420 and iPolicy-SA-990; the latter only used for anti-virus security scanning) with Fortinet's FortiGate-3600 anti-virus firewall. Both devices are multifunction security appliances designed to protect data networks from a wide range of security threats with no compromise to network performance. Both products are marketed to service providers and large enterprises.

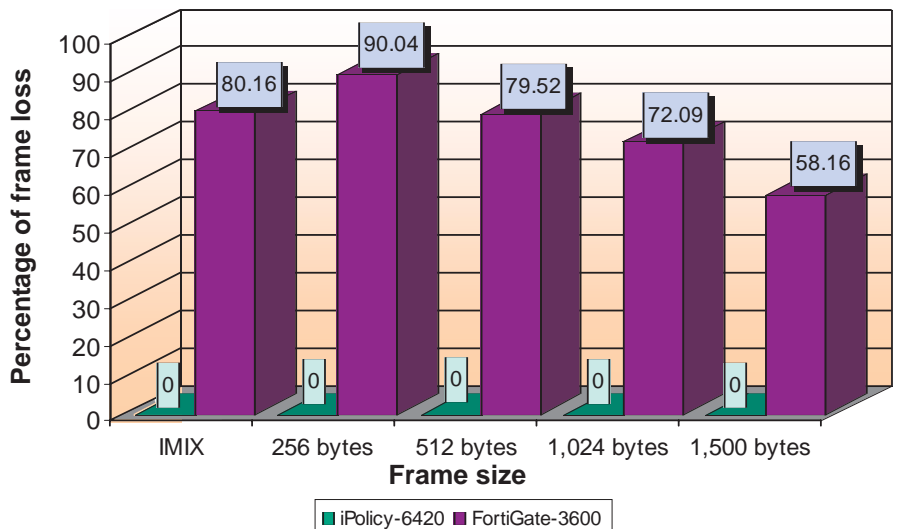
Tests focused on three main functional areas: UDP frame loss, TCP/UDP per-second connection rate, and the ability to establish new connections per second when the device already has a large number of connections active. Tests were conducted during August 2004.

Tests show that the iPolicy-6420 consistently delivers high performance in every test scenario, even with a range of security applications running. That was not the case with the FortiGate-3600; it demonstrated significantly low throughput, significantly lower TCP/UDP connection

### Test Highlights

- iPolicy-6420 experiences near 0% UDP frame loss even with firewall, IDS/IPS, URL filtering, and anti-virus enabled (while processing 4 Gbps of data). By contrast FortiGate-3600 suffers frame loss as high as 90% (for 256-byte test case)
- iPolicy-6420 maintains 200 times the TCP connections-per-second rate of the FortiGate-3600 when attempting 30,000 new TCP connection per second
- iPolicy-6420 demonstrates successfully completed transactions even at a high connections-per-second rate, unlike FortiGate-3600 which completes a very small percentage of transactions even at low connections-per-second rate
- iPolicy-6420 establishes new connections-per-second even when the platform is loaded with 930K active sessions (15,000 connections-per-second tested), unlike FortiGate-3600 that only achieves 29 connections-per-second with 930K active sessions

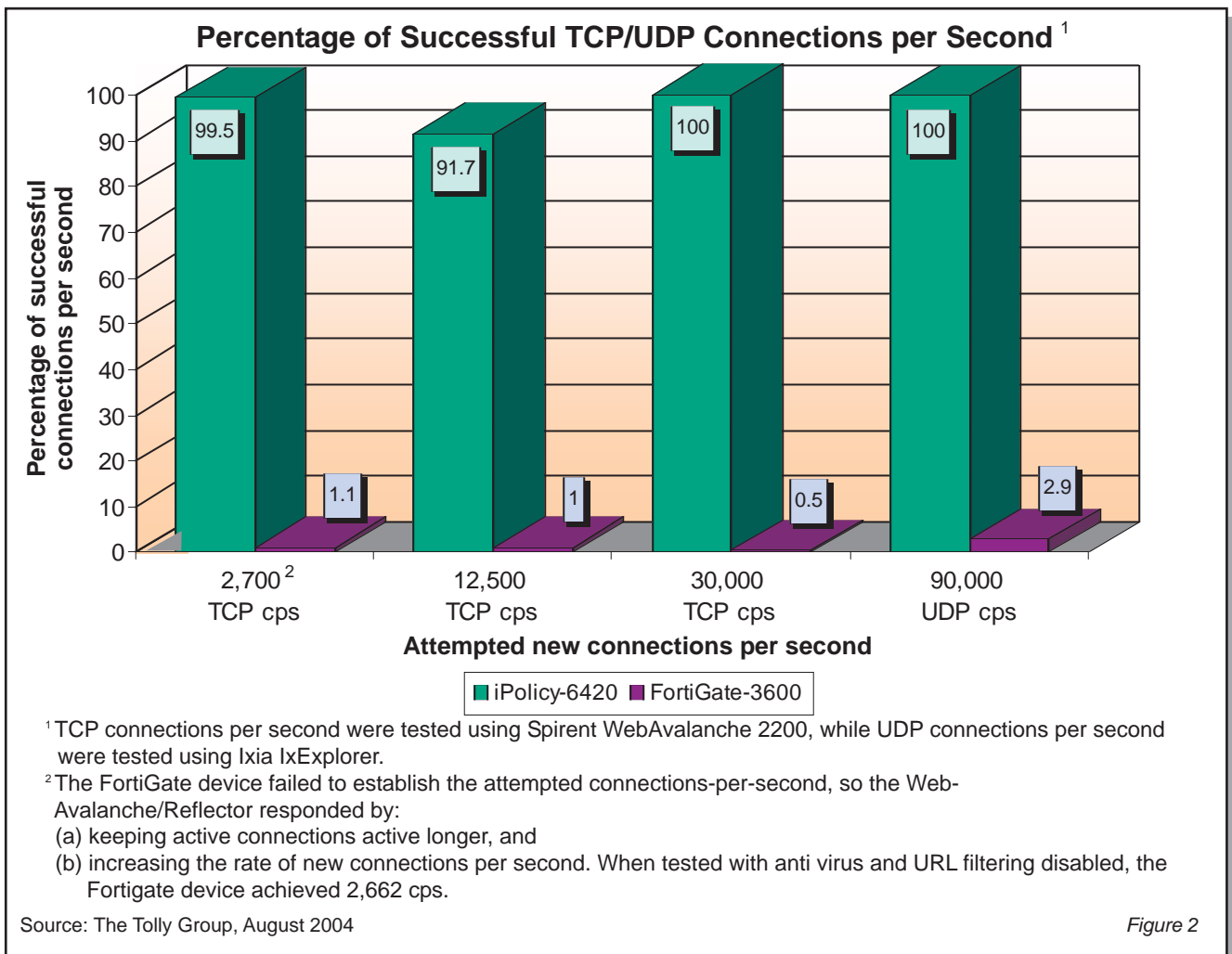
**% Frame Loss for Various UDP Frame Sizes @ 4 Gbps as Reported by Ixia IxExplorer**



Note: Internet Mix (IMIX) flows consist of 56% frames of 70 bytes, 6% frames of 78 bytes, 16% frames of 576 bytes and 22% frames of 1,500 bytes)

Source: The Tolly Group, August 2004

Figure 1



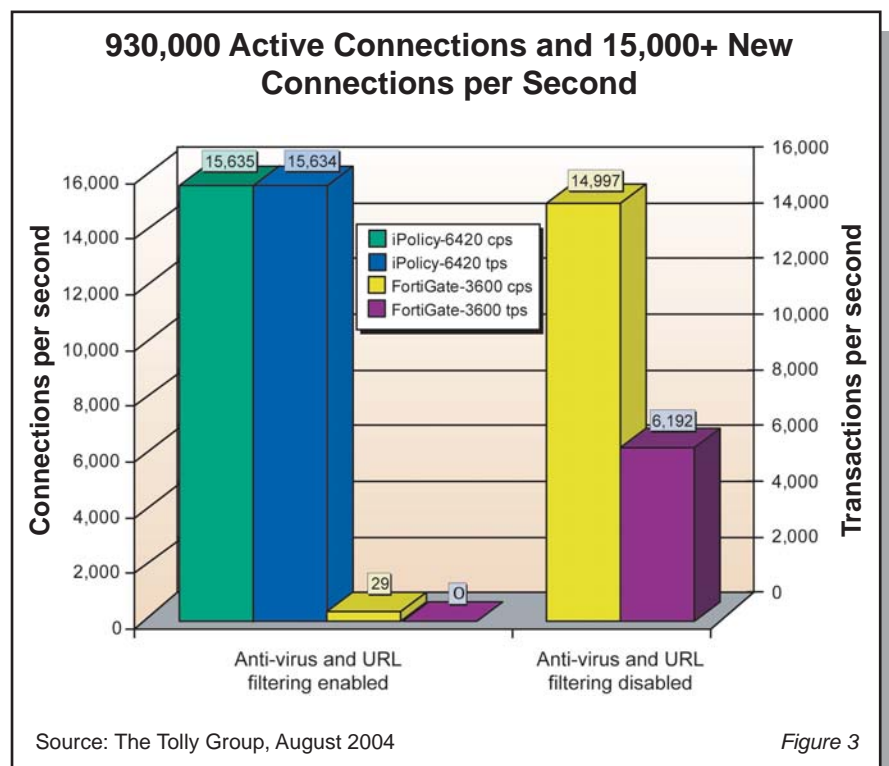
rates, and was barely able to complete any transactions successfully under such test scenarios.

## RESULTS

### UDP FRAME LOSS

Engineers measured the frame-loss percentage of both devices with firewall, IDS/IPS, URL filtering, and anti-virus applications enabled. Various UDP frame sizes (256, 512, 1,024, and 1,500 bytes and an Internet mix [IMIX consisted of 56% frames of 70-bytes, 6% frames of 78-bytes, 16% frames of 576-bytes and 22% frames of 1500-bytes]) were transmitted to the tested devices at the rates of 4, 2, and 1 Gbps, and the throughput of the device was measured.

In this scenario, the iPolicy-6420 experienced near 0% frame loss for



frame sizes of 1,500, 1024, 512, 256 bytes and an IMIX, all operating at frame rates of 1, 2 and 4 Gbps.

The Fortinet FortiGate-3600, by contrast, suffered frame loss in excess of 90% for 256-byte frames while operating at 4 Gbps. (See Figure 1.) For the IMIX test case, the frame loss while operating at 2 Gbps was 39%; Operating at 1 Gbps, the frame loss was 25%.

#### TCP/UDP CONNECTION RATE

This test identified the rate at which the tested device can set up new connections with firewall, IDS/IPS, URL filtering, and anti-virus applications enabled. The connection rate is noted by the number of successful connections per second (cps) recorded.

With all the applications enabled, the iPolicy-6420 consistently outperformed the FortiGate-3600,

delivering up to 200 times the number of connections per second than the FortiGate-3600. (At 30,000 cps, iPolicy-6420 did 100% and FortiGate-3600 did .5% or 1/200th of 100%.) (See Figure 2.)

Engineers also attempted to create 90,000 new UDP sessions per second using 1,500-byte UDP packets at 1-Gbps rate with firewall, anti-virus, IDS/IPS, URL filtering and content scanning enabled on the tested devices. The iPolicy-6420 established new UDP connections at the rate of 89,995 cps while the FortiGate-3600 only established 2,577 new UDP cps, even at the rate of 1 Gbps using 1,500-byte UDP frames.

This shows that even though the FortiGate-3600 claims to support 25,000 connections-per-second rate, with firewall, IDS/IPS, URL filtering, and anti-virus applications enabled, FortiGate-3600 fails to achieve more than 125 connections

#### iPolicy Networks

#### iPolicy-6420 Intrusion Prevention Firewall

#### TCP/UDP

#### Connection Rates and Frame Loss



per second (1/200th of its claimed connections-per-second capacity).

#### MAXIMUM CONCURRENT TCP CONNECTIONS

In this test, the iPolicy-6420 again outperformed the FortiGate-3600 by a wide margin. With 930,000 active connections maintained at any time on the tested devices, engineers attempted to nail up 15,000 new connections per second, all while firewall, IDS/IPS, URL filtering,

#### iPolicy Networks iPolicy-6420 Intrusion Prevention Firewall Product Specifications\*

##### Performance

- 4 Gbps throughput
- 1 million sessions
- 100,000 sessions/second
- 4,000 security domains
- 300,000 security policies

##### Firewall

- Layer 3-7 stateful inspection
- Bidirectional and inter-domain
- NAT, PAT
- Gateway, transparent mode
- User authentication
- H.323 NAT traversal
- Time-of-day policies
- Inline bidirectional IDS/IPS

##### Intrusion & Real-time Attack Prevention

- 1,700+ attack and worm signatures
- DoS/DDoS attack mitigation
- Protocol/traffic anomaly detection
- Malicious packet drop
- Attack connection reset/drop
- Dynamic firewall hardening
- Bandwidth control
- Connection rate control
- Traffic normalization

##### URL Screening

- 5.3M+ Web URLs
- 1.2B+ Web pages
- 44 predefined categories
- Black list/White list
- Keyword search blocking
- Java scripts, ActiveX, cookies

##### Management

- Command line interface
- Centralized management
- Secure Telnet

##### High Availability

- Full mesh active-active, master-slave
- State synchronization

##### Dimensions

- 17.5x23x3.5 (WxDxH inch)

##### For more information contact:

iPolicy Networks  
47467 Fremont Blvd.  
Fremont, CA 94538  
Phone: (510) 687-3000  
Fax: (510) 687-1767  
URL: [www.ipolicynetworks.com](http://www.ipolicynetworks.com)

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

and anti-virus applications were enabled.

The iPolicy-6420 achieved a successful connection rate of 15,634 cps with a peak bandwidth of 196.5 Mbps and 15,634 successful transactions per second. (See Figure 3.) By contrast, the FortiGate-3600 only established 29 successful cps with peak bandwidth of 83.3 Mbps, but the device could not complete any of the attempted transactions.

This shows that even though the FortiGate-3600 claims to support a maximum of 1 million simultaneous connections, when firewall, IDS/IPS, URL filtering, and anti-virus are enabled, it cannot accept many new connection requests; nor does it successfully complete any new transactions at the tested load of 930,000 concurrent connections.

**ANALYSIS**

Providing complete network security, for service providers and for large enterprises, typically requires the purchase and the installation of disparate, multi-vendor point products. These include

Configuration Details		
	iPolicy-6420	FortiGate-3600
Customers simulated	14	14
Firewall applications enabled	208	50
IPS/IDS signatures enabled	1,691	757
Anti-virus signatures enabled	92,885	4,350
URL database entries enabled	5.3M+	10 <sup>1</sup>

<sup>1</sup>FortiGate 3600 supports a maximum of 10 URL whitelist/blacklist entries

Source: The Tolly Group, August 2004 Figure 4

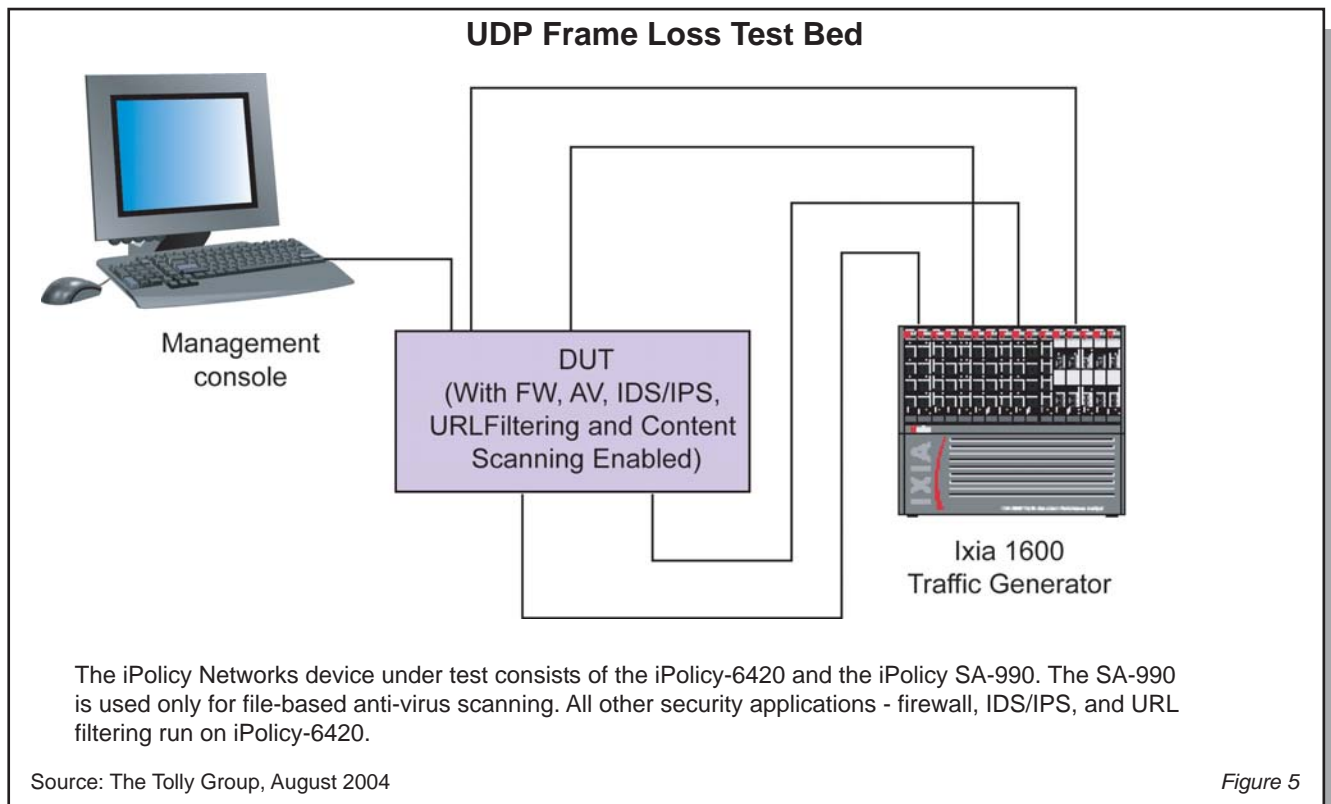
firewall, VPN, Intrusion Detection Systems, Intrusion Prevention Systems, anti-virus, and content filtering. The downside is that each security solution comes with its own set of policies and its own management interface.

Integrated all-in-one security appliances, like the iPolicy-6420 and the Fortinet FortiGate-3600, can provide a cohesive suite of security services, but must do so with minimal impact

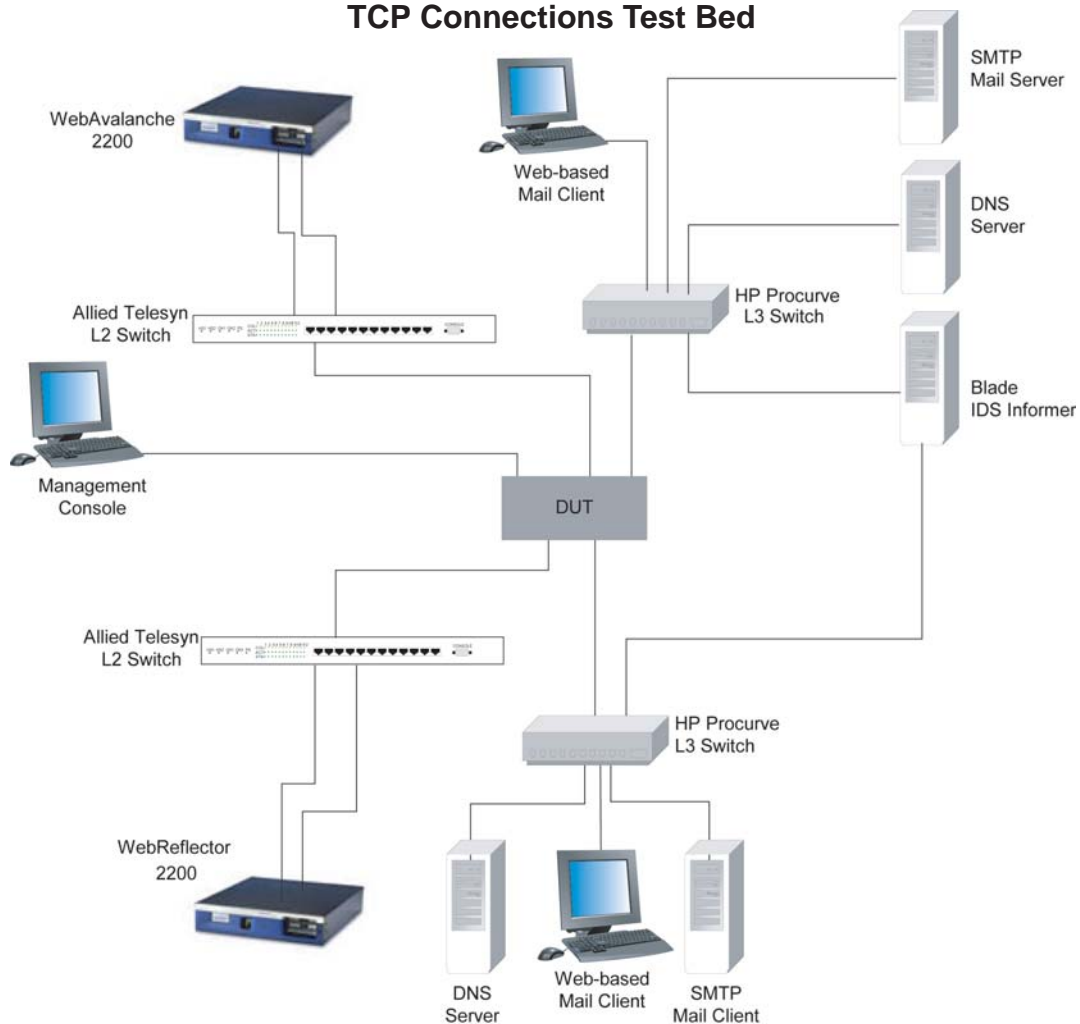
on performance. However, not all security appliances are created equal as testing shows.

The iPolicy Intrusion Prevention Firewall demonstrates that it delivers high performance even with all the security applications enabled and with a far more demanding configuration (See figure 4.)

- The UDP frame loss test uncovers compelling test data that has



## TCP Connections Test Bed



The iPolicy Networks device under test consists of the iPolicy-6420 and the iPolicy SA-990. The SA-990 is used only for file-based anti-virus scanning. All other security applications - firewall, IDS/IPS, and URL filtering run on iPolicy-6420.

Source: The Tolly Group, August 2004

Figure 6

implications for service providers and enterprises alike. Network administrators should note that the iPolicy-6420 delivered near 0% frame loss for frame sizes of 1,500, 1024, 512, 256 bytes and IMIX traffic, making iPolicy-6420 a reliable choice for their networks. By contrast, the FortiGate-3600 suffered frame loss as high as 90% for the frame sizes tested.

- For the TCP/UDP connection rate, the iPolicy-6420 exhibited scalability to 90,000 connections-per-second as claimed in its datasheet. By contrast, Fortinet FortiGate-3600 could

only scale to a maximum of 125 connections-per-second.

- With 930K connections active, testing showed that the iPolicy-6420 could still add new connections (max of 15K connections-per-second tested) and complete transactions. This is in-line with its datasheet that claims 1 million consecutive connections and 100,000 new connections per second. By contrast, the Fortinet FortiGate-3600 maxed out at 29 connections-per-second with 0 successful transactions under the same test case.

## TEST CONFIGURATION AND METHODOLOGY

For performance tests, The Tolly Group tested an iPolicy-6420 Intrusion Prevention Firewall SW Version 1.7.1.5716. Engineers also tested a Fortinet FortiGate-3600 SW Version 2.5 Rev 9.

For the UDP frame loss test, the iPolicy-6420 and the Fortinet FortiGate-3600 connected to an Ixia 1600T traffic generator and to a management console (See Figure 5). The test configuration for the TCP connection test was more involved, with the devices under test connected via gener-

ic Layer 2 switches to a Spirent Communications WebAvalanche 2200 and to a Web-Reflector 2200 (See Figure 6).

In the TCP connections tests, Blade IDS Informer test tool generated a pre-selected list of intrusion attacks at the rate of one attack per second directed at the DUT. Engineers made sure to select the subset of available Blade IDS Informer attacks that was detectable by both DUTs. The SMTP mail server generated messages containing virus attachments at the rate of 15 per second, addressed to the Web-based Mail Client on the protected side of the firewall. While the intrusion attacks and virus E-mails were active, the DUTs were put to the test to establish new connections at rates relevant to the specific test

iteration. The DUT and the Web-based E-mail client were connected to the Blade IDS Informer and the SMTP Mail Server using a Layer-3 switch, as shown in Figure 6.

## EQUIPMENT ACQUISITION AND SUPPORT

As per The Tolly Group's Fair Testing Charter, Fortinet was approached to participate in the tests. The company responded quickly and agreed to participate. A Fortinet engineer reviewed the test methodology and provided feedback during the testing cycle. Tolly Group engineers implemented Fortinet's technical suggestions when offered. For instance, with regard to the TCP connection rate test, Fortinet support engineers asked us to disable a TCP Options func-

tion to improve performance. Tolly Group engineers did so, but performance did not improve. The Tolly Group also upgraded the FortiGate-3600's firmware at the company's request, without any impact on performance results.

As per our policy, we shared the FortiGate-3600 test results with Fortinet. Fortinet representatives responded by claiming the test results were not accurate. Yet, when The Tolly Group requested further details, Fortinet would not elaborate. Moreover, at one stage a Tolly Group engineer requested methodology info on how Fortinet achieved performance claims stated in product data sheets. Fortinet would not share its methodology.

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

Vendor	Product	Web address
Blade Software	IDS Informer V. 1.0.241	<a href="http://www.blade-software.com">http://www.blade-software.com</a>
Ixia	IxExplorer V. 3.65 build 284	<a href="http://www.ixiacom.com">http://www.ixiacom.com</a>
Spirent Communications	WebAvalanche 2200 V.6.2.0.30909	<a href="http://www.spirentcom.com">http://www.spirentcom.com</a>
Spirent Communications	WebReflector 2200 V.6.2.0.30909	<a href="http://www.spirentcom.com">http://www.spirentcom.com</a>



## 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](mailto:sales@tolly.com).

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

## PROJECT PROFILE

**Sponsor:** iPolicy Networks

**Document number:** 204138

**Product class:** Multifunction security appliance

**Products under test:**

- iPolicy-6420 Intrusion Prevention Firewall SW Version 1.7.1.5716
- Fortinet FortiGate-3600 SW Version 2.5 Rev 9

**Testing window:** August 2004

**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](mailto: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. 204138 rev. 11 Oct 2004*