TOLLY Benchmarks

Volume 5, Issue 1

2 **Nortel Ethernet Routing Switch 5000 Series "stacks" up well against rivals in performance tests**

Nortel solution forwards nearly 10X more frames than the Cisco solution and nearly twice the frames of the HP solution in an eight-switch stack configuration

3 **AirTight Networks' wireless intrusion prevention system significantly outperforms options from AirMagnet and Aruba Networks**

SpectraGuard Enterprise wireless IPS detects and stops 100% of threats launched and locates threats with a high degree of precision

4 **Nortel Secure Router 3120 demonstrates superior DS3/T1 throughput**

Secure Router 3120 demonstrates wire-speed performance while simultaneously supporting active QoS, ACL filters and NAT services

5 **Nortel Secure Routers dominate in branch office T1 connectivity tests**

Secure Routers 1002 and 1004 achieve wire-speed performance for most packet sizes tested while also supporting active QoS, IPSec VPN and stateful firewall services over T1 lines

7 **Symantec blocks attack barrage, struts security performance while Cisco and NetScreen devices lag behind**

Blocks 100% of attacks launched from two industry-standard test tools, while Cisco and Juniper Networks devices tested struggled with attack blockage

THE TOLLY GROUP

ABOUT

Tolly Benchmarks is a regular advertising supplement that highlights innovative and compelling technology research conducted by The Tolly Group, the industry's leading independent testing and strategic consulting organization based in Boca Raton, FL. **For more information** on any of the products or technologies covered here, visit The Tolly Group's Web site at **http://www.tolly.com**.

info@tolly.com	phone (561) 391-5610	fax (561) 391-5810

Nortel Ethernet Routing Switch 5000 Series "stacks" up well against rivals in performance tests

Sponsor: **Nortel**
Document number: **206106**
Product Class: **Stackable GbE switch**
Products under test:

- Nortel Ethernet Routing Switch 5510-48T (Running switch software version 4.2.0.004)
- Nortel Ethernet Routing Switch 5510-24T (Running switch software version 4.2.0.004)
- Nortel Ethernet Routing Switch 5520-48T-PWR (Running switch software version 4.2.0.004)
- Nortel Ethernet Routing Switch 5530-24TFD (Running switch software version 4.2.0.004)
- Nortel Ethernet Routing Switch 8600 (Running switch software version 4.0.1.0)
- Cisco Catalyst 3750G-48TS (running switch software version 12.2 (25) SEB1)
- Cisco Catalyst 3750G-48PS (running switch software version 12.2 (25) SEB1)
- Cisco Catalyst 3750G-24TS (running switch software version 12.2 (25) SEB1)
- Cisco Catalyst 3750G-16TD-S (running switch software version 12.2 (25) SEB1)
- Cisco Catalyst 6500 (running switch software version 12.2 (18) SXD5)
- HP ProCurve 3400cl-48G (running switch software version M.08.66)
- HP ProCurve 3400cl-24G (running switch software version M.08.66)
- HP ProCurve 9304M (running switch software version 07.8.00aT53)

Testing window: **September 2005**

A battery of performance tests commissioned by Nortel show that the company's Ethernet Routing Switch 5000 Series outperforms rival products from Cisco and HP to provide high-density Gigabit Ethernet desktop connectivity to enterprise customers' wiring closets.

Tolly Group engineers tested 24- and 48-port versions of the Nortel Ethernet Routing Switch 5510, 5520 and 5530 models – single rack-unit stackable Gigabit Ethernet (GbE) Layer 3 routing switches. Engineers measured the performance and resiliency characteristics of the Ethernet Routing Switch 5000 series switches against Cisco Systems, Inc. Catalyst 3750G switches and Hewlett-Packard Co. ProCurve 3400cl switches.

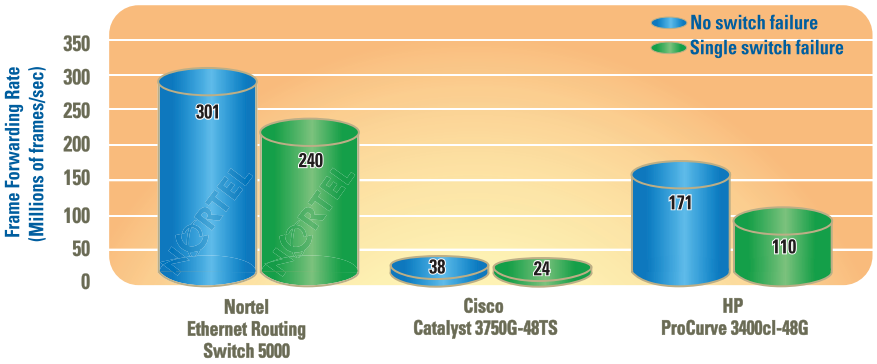
Tests show that the Nortel Switch 5510-48T in an eight-switch stack configuration with 320 GbE ports delivers 640 Gbps of switching capacity and 320 Gbps of throughput.

- Delivers superior stacking performance of up to 640 Gbps of switching capacity in an eight-unit stack of Nortel 5500 switches
- **Achieves line-rate performance of 202 Gbps frame-forwarding in an eight-unit stack, while Cisco and HP switches support only 25.7 Gbps and 114.7 Gbps respectively**
- Demonstrates 36% to 44% less average latency, when compared to Cisco and HP devices tested
- **Recovers from link and switch outages almost 10X faster using Nortel's SMLT implementation than the RSTP implementation in the Cisco Catalyst and HP ProCurve solutions tested**
- Offers the lowest cost per megabit of throughput among the switches tested at just below $90 versus almost $100 HP and over $300 for Cisco

Layer 2 Stack Resiliency Comparison

Impact of Stacked Switch Failures on Frame Forwarding Rate

202 GbE ports in an 8-Switch Stack with 64-byte Frames at 100% Line-rate Load
as Reported by Spirent SmartFlow 4.60



Note:
This test set-up with 202 GbE ports was chosen due to competitive equipment availability.

In competitive frame forwarding tests, the Nortel Ethernet Routing Switch 5000 solution forwarded nearly 10X more frames than the Cisco solution tested, and nearly twice the frames of the HP solution when tested across 202 GbE ports in an eight-switch stack configuration.

Engineers tested the failover times of the Rapid Spanning Tree Protocol (RSTP) and Nortel's Split Multi-Link Trunking (SMLT) technologies in the event of a link failure and a switch failure. Nortel switches demonstrated the fastest failover times during a link failure – Nortel's solution using SMLT failed over in 0.5 seconds while Cisco's solution took 1.7 seconds and HP's solution took 3.1 seconds. Nortel also held a distinct advantage in switch failover times.

Regarding ease of use, Nortel's SMLT implementation required fewer number of CLI commands to configure the test bed compared to HP's and Cisco's implementations of RSTP – a total of 60 commands to configure SMLT versus 102 for the HP ProCurve solution and 156 for the Cisco Catalyst solution.

This shows that Nortel's SMLT implementation requires fewer CLI commands to configure the test bed compared to HP's and Cisco's implementations of RSTP.

View the full report at:
http://www.tolly.com/DocDetail.aspx?DocNumber=206106

AirTight Networks' Wireless Intrusion Prevention System significantly outperforms options from AirMagnet and Aruba Networks

A recent white paper from The Tolly Group on wireless intrusion prevention systems shows that while many systems promise to detect and block wireless threats, only one solution tested from AirTight Networks delivered the type of performance and breadth of functionality that enterprises need.

The Tolly Group assessed the capability of SpectraGuard Enterprise to detect and block a range of wireless threats – from dealing with rogue APs, to detection and prevention of access point (AP) MAC address spoofing, to detection and prevention of Denial of Service (DoS) attacks, and several others.

Tolly Group engineers measured the effectiveness of SpectraGuard Enterprise against two other products: AirMagnet Inc.'s AirMagnet Enterprise and Aruba Networks Aruba Mobility Controller. AirTight Networks commissioned The Tolly Group to evaluate all three products; the results are documented in a comprehensive white paper titled: "Evaluating Wireless Intrusion Prevention Systems."

In the test, 24 different wireless threats (or groups of threats) were thrown at all three systems. The results show that AirTight's SpectraGuard Enterprise detected all 24 threat scenarios launched against the networks, blocked unauthorized traffic and prevented threats from inflicting network damage in all 24 scenarios. Competing devices were not nearly as effective, detecting about 30% fewer threats, and preventing only about half of the threats from operating in the network.

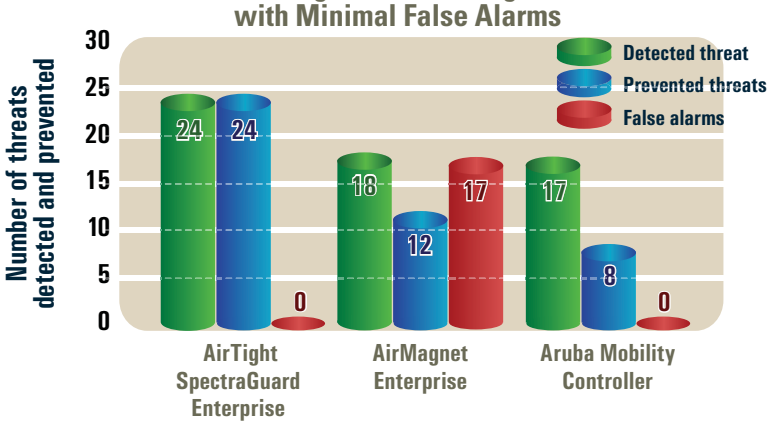
Some of the interesting data results include:

- Neither Aruba MobilityController nor AirMagnet Enterprise could stop a wireless DoS attack
- Aruba Mobility Controller could not prevent laptops from logging onto external networks

- **Detects 100% of the security threats launched against it, while AirMagnet Enterprise missed 25%, and Aruba Mobility Controller missed 30%**
- **Prevents 100% of the threats, while AirMagnet Enterprise prevented half of them, and Aruba prevented only one-third**
- **Effectively prevents multiple threats simultaneously from a single sensor, while the competitive devices did not**
- **Continues to scan for new wireless threats even while preventing active threats, while the other systems did not**
- **Creates zero false alarms, unlike AirMagnet Enterprise which threw off as many false alarms as threats detected**
- **Locates wireless threats with a high degree of accuracy – within 4 meters in test scenarios, while the Aruba Mobility Controller did not converge on a location, and AirMagnet Enterprise was 12 to 40 meters off**

View the full report at:
http://www.tolly.com/DocDetail.aspx?DocNumber=206103

Efficiency of Wireless Intrusion Prevention Systems at Detecting and Preventing Threats with Minimal False Alarms



- AirMagnet Enterprise could not stop two laptops from forming an ad-hoc network
- Only AirTight Networks' SpectraGuard Enterprise product allows an enterprise to define different WiFi security policies for different VLANs – enabling an enterprise to have guest WiFi access in one portion of a building, but a "no WiFi policy" in another section.

Tests prove that only SpectraGuard Enterprise delivered three basic sets of functionality:

- Detecting and automatically classifying wireless threats;
- Preventing multiple simultaneous wireless threats while continuing to scan for new threats; and,
- Accurately locating wireless threats on a floor map.

Lastly, SpectraGuard Enterprise's management reporting, WLAN troubleshooting and RF display/visualization capabilities provide a depth of functionality that is unmatched by the other products tested.

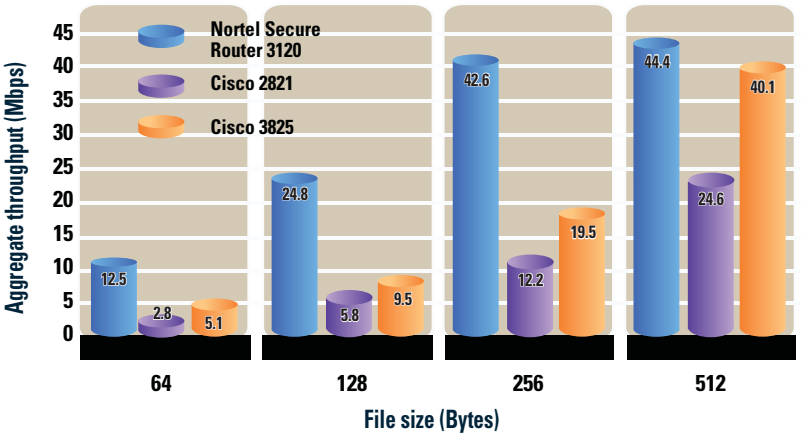
Sponsor: **AirTight Networks**
Document number: **206103**
Product class: **Wireless intrusion prevention system**
Products under test:

- **AirTight Networks SpectraGuard Enterprise Ver. 4.0**
- **AirMagnet, Inc. AirMagnet Enterprise Ver. 6.1.0**
- **Aruba Networks Aruba Mobility Controller Ver. 2.4.1.0**

Testing window: **December 2005**

Nortel Secure Router 3120 demonstrates superior DS3/T1 throughput

- **Secure Router 3120 demonstrates wire-speed performance while simultaneously supporting active Quality of Service (QoS), Access Control List (ACL) filters and Network Address Translation (NAT) services**
- **Delivers more than double the throughput of the Cisco 3825 and as much as four times the throughput of the Cisco 2821 when tested over a point-to-point DS3 link**
- **Outperforms Cisco 2821 routers, delivering more than 4X the throughput when tested across a group of eight point-to-point T1 connections**



Wide-area network routers that aggregate traffic from many remote sites, especially across DS3 or multiple T1/E1 links, must be able to deliver high throughput, even with Quality of Service (QoS), Network Address Translation (NAT), and security services active and vying for processor cycles.

In a series of tests commissioned by Nortel, Tolly Group engineers measured the multilink Point-to-Point Protocol (PPP) zero-loss throughput of the modular Nortel Secure Router 3120 with QoS, NAT and Access Control List (ACL) features enabled.

Tests show that the Nortel Secure Router 3120 delivers superior throughput for the majority of packet sizes tested, especially with regards to smaller packet sizes (64 bytes to 256 bytes), generally delivering from 2X to 4X greater throughput than the Cisco Systems 3825 Integrated Services Router and 2821 Integrated Services Router tested.

When tested with a group of eight T1s, the Nortel Secure Router 3120 outperformed the Cisco 2821 routers, delivering more than 4X the throughput - 11.3 Mbps aggregate throughput for the Secure Router 3120 versus just 2.4 Mbps for the Cisco devices when tested at 64-byte frames.

Testing demonstrates that the Nortel Secure Router 3120 possesses an enormous amount of processing headroom to accommodate network services while simultaneously offering wire-speed throughput.

In addition to delivering wire-speed packet processing, tests show that the Secure Router 3120 has the horsepower to simultaneously handle QoS, ACL and NAT processing. In head-to-head testing, the Secure Router 3120 demonstrates more than double the throughput of the Cisco 3825 and as much as four times the throughput of the Cisco 2821 over a DS3 link. In a multiple T1 scenario, the Secure Router 3120 achieves 4X more throughput than the Cisco 2821.

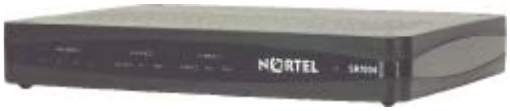
View the full test summary at:
http://www.tolly.com/DocDetail.aspx?DocNumber=205146

Sponsor: **Nortel**
Document number: **205146**
Product class: **WAN router**
Products under test:

- **Nortel Secure Router 3120 OS Ver 9.0/BootROM Ver. T1002 09120**
- **Cisco Systems 3825 Integrated Services Router OS Ver. 12.4.2T1/BootROM Ver. 12.3(11r)T**
- **Cisco Systems 2821 Integrated Services Router OS Ver. 12.4.2T1/BootROM Ver. 12.3(8r)T7**

Testing window: **September 2005**
For more info on this test, visit: **http://www.nortel.com**

Nortel Secure Routers dominate in branch office T1 connectivity tests



Nortel commissioned The Tolly Group to evaluate the Nortel Secure Router 1004 and Secure Router 1002 wide-area network routers with integrated network services such as Quality of Service (QoS), IPSec VPN with on-board hardware acceleration, stateful firewall, Network Address Translation (NAT) and Access Control Lists (ACLs) for enterprises and service providers.

Tolly Group engineers measured the multilink Point-to-Point Protocol (MLPPP) zero-loss throughput of the Secure Router 1004 against Cisco 2811 and Cisco 2821 routers, with QoS, NAT and ACL features enabled in a scenario with multilink PPP traffic riding over four T1s.

Tests show that the Secure Routers 1004/1002 can deliver wire-speed throughput at most packet sizes tested, while simultaneously processing a combination of QoS, NAT, ACL filters, IPSec VPN and firewall services.

By contrast, tests show that the performance of the Cisco 1841/2811/2821 routers sag under the processing load, especially when smaller, more taxing packet sizes come into play.

Test results show that the Secure Routers 1004 and 1002 deliver superior throughput for the majority of packet sizes tested, especially with regards to smaller packet sizes (64 bytes to 256 bytes), delivering up to 6.4X greater throughput than the Cisco devices tested.

In a scenario with the WAN routers supporting multilink PPP traffic across four T1s, the Nortel Secure Router 1004 delivered zero-loss aggregate throughput ranging from 3.9 Mbps at 64-byte frames to 6.2 Mbps when tested at 512-byte frames with QoS/VPN and firewall services enabled. By contrast, the Cisco 2811 achieved throughput ranging from 1.1 Mbps to 4.1 Mbps.

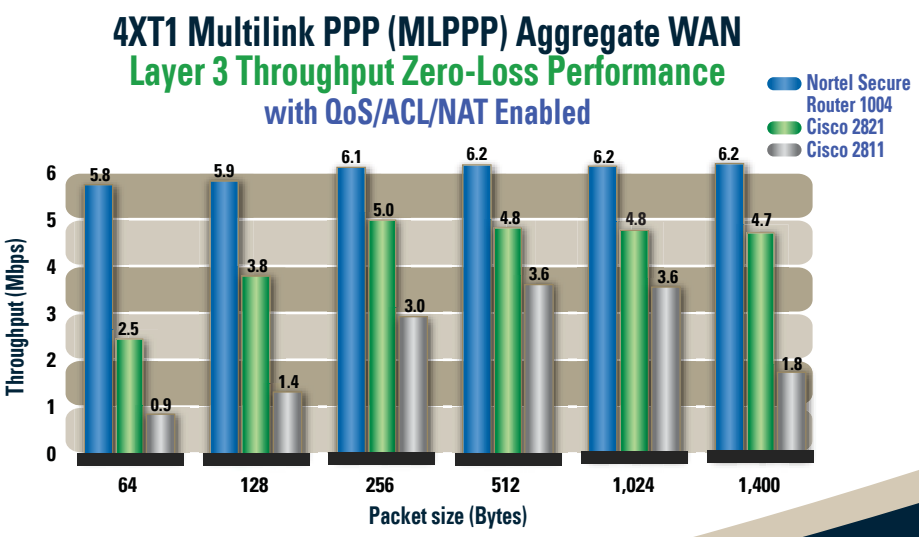
In a scenario with WAN routers supporting multilink PPP traffic across two T1s, the Nortel Secure Router 1004 delivered 3.1 Mbps across the range of packet sizes tested. By contrast, the Cisco 2811 and Cisco 1841 routers tested achieved an average of 2 Mbps and 1.25 Mbps, respectively.

- Secure Router 1004 operated at or near wire-speed throughput and outperformed Cisco 2811 and 2821 routers, delivering 6X and 2X more throughput respectively, while simultaneously supporting active QoS, ACL filters and NAT over four T1 lines
- Secure Routers 1002 and 1004 demonstrated wire-speed performance for most packet sizes tested while simultaneously supporting active QoS, IPSec VPN and stateful firewall services over two or four T1 lines
- Secure Router 1004 consistently outperformed the Cisco 2811 for all packet sizes tested, especially at smaller packet sizes, when tested across four T1s with QoS, IPSec VPN and stateful firewall services, delivering 3X more throughput than its counterpart
- Secure Router 1002 achieved wire-speed throughput at all packet sizes, while performance of Cisco 2811 and 1841 weaken when handling 64- 128- and 256-byte packets tested across two T1s with QoS, IPSec VPN and stateful firewall services

Sponsor: Nortel
Document number: **205143**
Product class: WAN router
Products under test:

- **Nortel Secure Router 1004 OS Ver 8.2.1/ BootROM Ver. T1k031605**
- **Nortel Secure Router 1002 OS Ver 8.2.1/ BootROM Ver. T1k031605**
- **Cisco 1841 Integrated Services Router OS Ver. 12.4.2T1/ BootROM Ver. 12.3(8r)T8**
- **Cisco 2811 Integrated Services Router OS Ver. 12.4.2T1/ BootROM Ver. 12.3(8r)T7**
- **Cisco 2821 Integrated Services Router OS Ver. 12.4.2T1/ BootROM Ver. 12.3(8r)T7**

Testing window: September 2005
For more info on this test, visit: **http://www.nortel.com/**



For more info on this test, visit:
http://www.tolly.com/DocDetail.aspx?DocNumber=205143

Introducing The Tolly Group's End-User Services Division…

Uncharted waters? Don't go IT alone.

The rapid evolution of network technology is challenging network managers to venture into uncharted waters at a time when money and resources are stretched tight.

Let The Tolly Group collaborate with your team to leverage existing and emerging technologies for maximum return on investment.

The Tolly Group is the industry's premiere performance testing and hands-on consulting services organization with 17+ years of experience with emerging technologies. Tolly Group executives maintain relationships with key executive management, CTOs, engineers, and system architects of many vendors.

Our knowledge of equipment, software and tools, will reduce your learning curve and speed deployment of new technology.

Tolly Group executives have originated from the user ranks, like you, and over the years gained the experience to understand your issues. The Tolly Group is 100% independent and guards its objectivity and neutrality carefully.

End-user services include:

- Wireless LAN performance/intrusion
- VoIP/Video/Data convergence
- Security – Intrusion
- Storage – Fibre Channel, iSCSI, etc
- Messaging
- LAN switching

Contact The Tolly Group TODAY. You've got everything to gain.

Visit *www.tolly.com*

TOLLY 17 YEARS 1989-2006

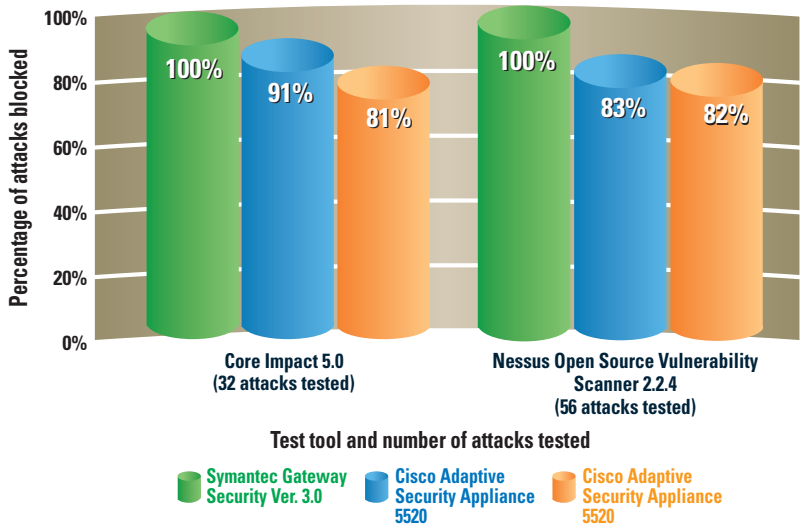
TOLLY FAIR TESTING CHARTER

Contact Joe Lombardo at:
Phone: **(561) 391-5610 ext. 196**
E-mail: **Joe.Lombardo@tolly.com**

THE TOLLY GROUP

Symantec blocks attack barrage, struts security performance while Cisco and NetScreen devices lag behind

Percentage of Attacks Blocked by Symantec Gateway Security Ver. 3.0 versus Cisco Adaptive Security Appliance 5520 and Juniper NetScreen-500



Sponsor: **Symantec Corp.**
Document number: **206108**
Product class:
Unified threat management appliance
Products under test:

- Symantec Gateway Security, Version 3.0, HW Model: 5660
- Cisco Systems, Inc. Adaptive Security Appliance 5520 ver 7.0(1), Device Manager Version 5.0(1)
- Juniper Networks, Inc. NetScreen-500 ver. 5.2.0 r2.0

Testing window:
September through November 2005
For more info on this test, visit: http://www.symantec.com

In today's market for multifunction security gateways, it is important to look beyond raw throughput capabilities to understand the broader device security provided by attack detection and blockage, anti-virus capabilities, intrusion prevention capabilities, connections per-second supported and other embedded security functions.

- **Blocks 100% of the attacks launched from two industry-standard test tools, while the Cisco and Juniper Networks devices tested struggled with attack blockage**
- **Delivers almost 3X the firewall throughput compared to the Juniper device tested, even while processing 50 rules**
- **Provides users with greater management information through the Security Gateway Management Interface (SGMI) than available to users from the Cisco or Juniper devices**

Symantec Corp.'s Symantec Gateway Security (SGS) Version 3.0 software blocked 100% of a battery of attacks launched, while competing devices from Cisco Systems and NetScreen blocked only a subset of the attacks in each scenario, in tests commissioned by Symantec.

Test results provided in this report identify over 200 single and blended threat attacks/vulnerabilities that the Symantec gateway blocked while Juniper and Cisco gateways faltered in fully protecting against all of the attacks.

From a firewall throughput perspective, the Symantec Gateway Security 5660 delivered about three times more throughput than other devices tested, even while processing 50 security rules. The Symantec Gateway Security 5660 achieved the highest throughput 2.1 Gbps for 1,518-byte packets versus 725 Mbps for the Juniper NetScreen-500 for 1,518-byte packets.

Tests also show the Symantec Gateway Security 5660 achieves three times the connection rate than the Juniper NetScreen-500 tested and delivers a more detailed graphical user interface.

Symantec's Security Gateway Management Interface (SGMI) presented all of the critical functionalities of the device in logical groups and was extremely informative. The SGMI offered explanations of each major subcategory with links to help pages with even more detailed information. This is in contrast to the user interfaces of the Cisco and Juniper devices tested, which do not provide as much readily accessible information about various configuration, monitoring and maintenance options available on each device.

View the full Test Summary at: http://www.tolly.com/DocDetail.aspx?DocNumber=206108

The Power of Proof™

GET PROOF

You deserve The Power of Proof.
It's the only way to separate fact from fiction.

For 17 years companies worldwide have come to
The Tolly Group to get that proof.

TOLLY Up to Spec CERTIFIED

Independent.
Authoritative.
Reliable.

Prove it to yourself at www. tolly.com

THE TOLLY GROUP

3701 FAU Blvd, Suite 100, Boca Raton, FL 33431
(561) 391-5610 Sales@tolly.com