Independent Testing Services

Validation Testing Report

October 2004 | Test No. ITS 04002

Juniper® NETWORKS

Juniper Networks | **NetScreen-ISG 2000**

CMP
United Business Media

600 Community Drive, Manhasset, NY 11030
Tel: (516) 562-5000 • Fax: (516) 562-5500
Email: info@nwctests.com • URL: www.nwctests.com

POWERED BY Network Computing Labs

Table of Contents

Executive Summary

POWERED BY Network Computing Labs

Product Overview

Juniper Networks Integrated Security Gateway, the NetScreen-ISG 2000, is designed to deliver scalable network and application security for large enterprise, carrier and datacenter networks. The NetScreen-ISG 2000 is built on Juniper Networks' next-generation architecture, which includes a fourth-generation security ASIC, the GigaScreen3, high-speed microprocessors and add-on security modules, to provide the predictable multi-gigabit performance the most demanding network segments need.

Independent Validation Claims

From July through September 2004, Independent Testing Services powered by Network Computing Labs™ (ITS) was contracted by Juniper Networks to independently validate specific capabilities of the NetScreen-ISG 2000. The following claims of Juniper Networks NetScreen-ISG 2000 were subject to open and independent testing verification:

1. Functions as a 2-Gbps, low-latency stateful firewall under randomized traffic patterns with varying packet sizes and session loads up to 400,000
2. Minimally impacts a heavily utilized Web-centric environment
3. Capable of sustaining TCP connection rates beyond 20,000 per second
4. Provides 1-Gbps VPN throughput (3DES with SHA1) at varying traffic and packet sizes while establishing 80 tunnels per second

Test Objectives

ITS tested Juniper Networks NetScreen-ISG 2000 to validate performance claims of 2-Gbps firewall and 1-Gbps VPN performance at any packet size using traffic conditions and topologies that simulate real-world environments. Where applicable, tests were performed in both NAT mode and Routed mode. Testing was performed using an environment capable of initiating realistic traffic mixes at gigabit speeds. Testing consisted of the following scenarios:

- **Raw Throughput** – Low-level packet forwarding and latency performance at 64-, 512- and 1,518-byte packet sizes with single session and 400,000 session loads
- **HTTP Performance** – Impact on real-world Web traffic using 4-, 16- and 64-kilobyte (KB) response sizes
- **TCP Session Rates** – Rate for connection establishment in a real-world environment using external to internal connection methodology
- **IPSec VPN Performance** – Tunnel establishment rate and throughput for IPSec 3DES VPN using 64-, 512- and 1,518-byte packet sizes with one, 10 and 100 tunnels

Results Summary

Raw Throughput Validation of 2 Gbps:
The NetScreen-ISG 2000 sustained line rate (2-Gbps) performance for all tested traffic conditions except 64-byte packets, which resulted in minor performance degradation (see specific results for more details). Uni-directional latency remained under 45 microseconds (µSec) for all tested packet sizes up to 400,000 concurrent sessions.

Minimal Impact on Heavily Utilized Web-Centric Environment:
The results indicated that inserting the NetScreen-ISG 2000 into the test topology had little or no negative impact on HTTP performance.

TCP Session Performance Greater Than 20,000 Sessions Per Second:
The NetScreen-ISG 2000 sustained performance between 22,000 and 30,000 TCP connections per second under all conditions tested.

IPSec 3DES Throughput at Gigabit Speeds:
The NetScreen-ISG 2000 sustained 1-Gbps performance (including IPSec overhead) without exception for all packet sizes tested. Burst tunnel requests up to 200 tunnels per second were negotiated successfully on a first come, first serve basis at 80 tunnels per second.

Validation Test 1: Raw Throughput

Test Summary

Performance Claim Subject to Validation:
NetScreen-ISG 2000 successfully functions as a 2-Gbps stateful firewall for 64-, 512- and 1,518-byte packet sizes under single and 400,000 session loads.

Validation Test Methodology:
Raw packet forwarding performance was measured in both NAT and Routed modes with UDP streaming involving multiple packet sizes and up to 400,000 source destination pairs.

Results Conclusion:
The NetScreen-ISG 2000 sustained line rate (2-Gbps) performance for all tested traffic conditions except 64-byte packets in NAT mode. In NAT mode with 64-byte packet sizes, maximum performance partially degraded to just under 1.6 Gbps.

Test Design

The NetScreen-ISG 2000 is a stateful firewall that tracks session status information for any traffic flow, thus traffic flow composition can positively or negatively impact overall performance. To generate traffic flow types that would be more real-world in nature, the following test constraints were established:

- **50 Servers** – Addressed by incremental IP addresses representing a typical server farm
- **400,000 Clients** – Addressed by a combination of random and incremental IP addresses representing 500 subnets of client workstations with 800 clients per subnet
- **Client to Server** – Random UDP source port, fixed UDP destination—port 80
- **Server to Client** – Random UDP source port, random UDP destination port

Why These Tests Matter:
ITS believes that UDP testing for firewalls historically has been of limited value because of the heavier reliance on TCP by most real-world environments. However, with the recent rise in newer UDP-based applications such as VoIP, both latency and UDP session ramping are becoming more relevant concerns. These drivers ultimately led to the performance of both UDP- and TCP/HTTP-based tests.

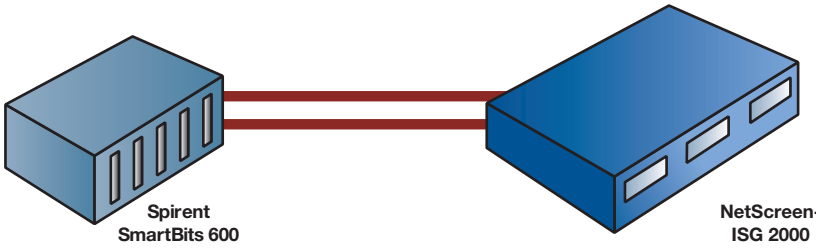
Validation Test 1: Raw Throughput

Test Environment

The testing environment consisted of the following:

- Spirent SmartBits SMB 600 with LAN-3301A interfaces
- Spirent SmartFlow 3.00.124.1
- NetScreen-ISG 2000 configured in both NAT and Routed modes

Testing was executed in both NAT and Routed modes with up to 400,000 clients and 50 servers for 60 seconds per test. Clients and servers were created with a pseudo-random distribution of traffic flows within SmartFlow, resulting in 200,000 unique traffic flows per direction, 400,000 clients and 50 servers. (A description of traffic flows is documented in the "Additional Test Details" section on page 6.)

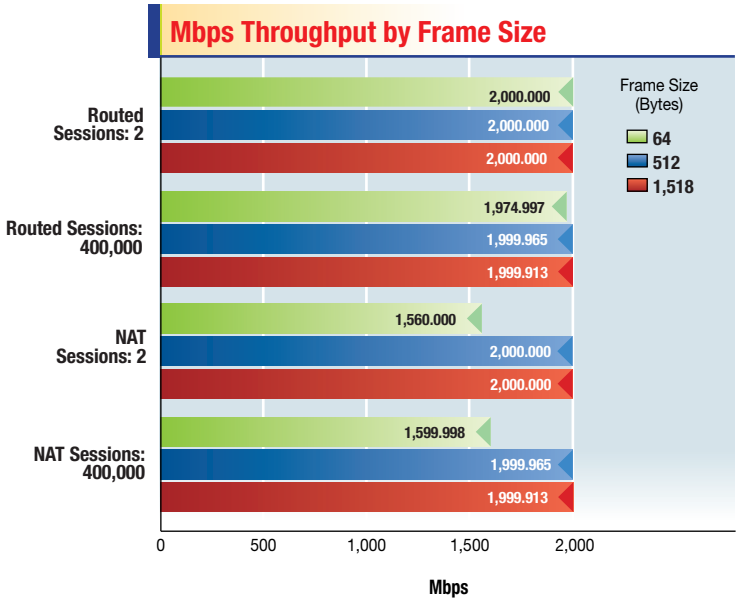


Slot 1 port 1 of the NetScreen-ISG 2000 was connected to slot 1 of the SmartBits 600. Slot 3 port 1 of the NetScreen-ISG 2000 was connected to slot 2 of the SmartBits 600. Both SmartBits interface slots were installed with LAN-3301A interfaces. All traffic traversed the NetScreen-ISG 2000 back plane.

Throughput Test Results

The NetScreen-ISG 2000 was capable of line rate performance in both 512- and 1,518-byte frames. With 64-byte frames, NAT performance was just under 1,600 Mbps, or approximately 80 percent utilization of full duplex Gigabit Ethernet.

In Routed mode, the NetScreen-ISG 2000 performed as a near line rate (2-Gbps) firewall for 512 and 1,518 frame sizes. There was a slight degradation (by 25 Mbps) in routed performance at 400,000 sessions for 64-byte frames.



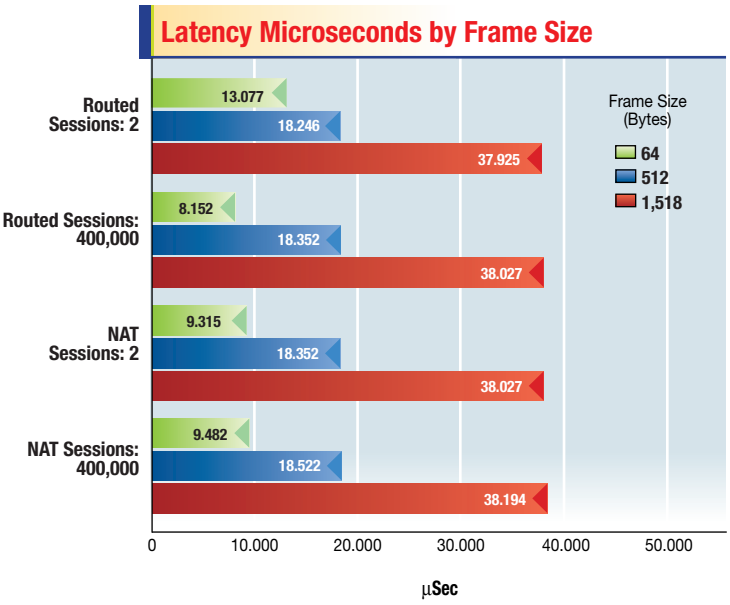
NOTE: During testing, it was discovered that multiple 60-second test runs were required per data point. The NetScreen-ISG 2000 changed in performance after what appeared to be a period of "learning" the traffic patterns. During initial learning for a new traffic flow, the NetScreen-ISG 2000 degraded in performance for a few seconds per flow.

Validation Test 1: Raw Throughput

Latency Under Maximum Load Test Results

While under the maximum load from the throughput testing, average uni-directional latency remained constant across both NAT and Routed modes in each respective frame size. Because of the insertion time of larger frames onto Gigabit Ethernet, the difference in latency between 64- and 1,518-byte frames was fully expected.

Why These Tests Matter:
Transaction response time, hence end-user response time, has a direct correlation to network latency. Any substantial increase in latency will negatively impact network application performance and responsiveness. Each device in a network adds to the total end-to-end latency, thus it remains critical that every component maintain a minimal forwarding delay.



NOTE: 1 millisecond (mSec) = 1,000 microseconds (µSec)

Additional Test Details

Using Spirent SmartFlow, the following topology was established:

- **Servers** – 50 servers with linear IP addressing (a Web server farm)
- **Clients** – 500 random client groups *times* 800 linear clients per group *equals* 400,000 clients
- **Client to Server** – 250 random flows of 800 clients per flow with a pseudo-random UDP source and a port 80 destination. Each client transmits to one server with a pseudo-random UDP source port and a UDP destination—port 80
- **Server to Client** – 250 random flows of 800 client destinations per flow with a pseudo-random UDP source port and a pseudo-random UDP destination port. Each of the 50 servers transmits to 800 linear clients per group *times* five random IP groups *equals* 200,000 sessions per server
- **Random Generation** – Random generation of base IP addresses and ports for all 500 flows

NOTE: Pseudo-Random Generation: UDP port values, incremented by 13 from base random generation, used on a per-flow basis across 800 clients per client group.

Validation Test 2: HTTP Performance

Test Summary

Performance Claim Subject to Validation:
The NetScreen-ISG 2000 minimally impacts a heavily utilized Web-centric environment.

Validation Test Methodology:
The goal was not to find the theoretical maximum throughput for Web traffic, but to measure the effects on Web traffic when the firewall was introduced into an existing high-utilization environment. The testing methodology consisted of establishing a baseline in the test topology and then inserting the NetScreen-ISG 2000 into this topology and measuring the change in performance metrics. The effects on the baseline were measured with the NetScreen-ISG 2000 in both NAT and Routed modes.

Results Conclusion:
The results indicated that inserting the NetScreen-ISG 2000 into the test topology had little or no negative impact on end-user HTTP performance for both latency and bandwidth effects.

Test Design

As TCP and HTTP traffic begin to approach a bandwidth limit, metrics like latency begin to spike and transactions begin to starve, thereby causing instabilities. For this reason, the environment was loaded incrementally without the NetScreen-ISG 2000 (using the Network Baseline Temporary Connection) to determine where a fully stable, sufficiently high utilization existed for each traffic type. To ensure consistency across traffic patterns and types, separate baselines were established for each combination. The traffic was composed under the following conditions:

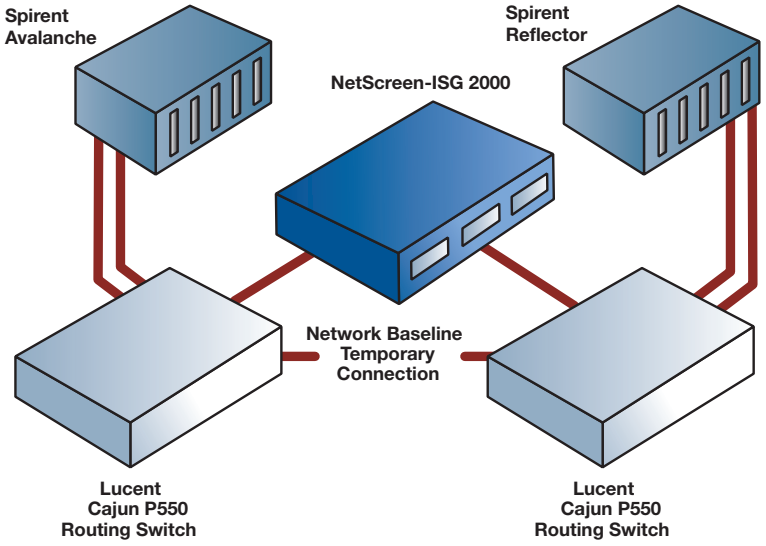
- **HTTP Transaction Size** – 4, 16 and 64 KB
- **Transactions** – Eight HTTP transactions per TCP connection
- **TCP Maximum Segment Size (MSS)** – 536 and 1,460 bytes
- **Individual Test Duration** – Two minutes sustained load, plus 30 seconds ramp up time
- **Number of Clients** – 2,032 Avalanche IP addresses
- **Number of Servers** – Four Reflector HTTP servers
- **Browser Emulation** – Internet Explorer

Why These Tests Matter:
TCP and HTTP session tests were included because they help validate performance concerns surrounding traffic types that often are more "bursty" and because TCP is the dominant session protocol used in many firewall deployments. In conjunction with the TCP session rate tests, using HTTP tests brings the test profile as close to a production traffic profile as possible and helps validate one of the more heavily used protocols in many transaction-centric environments.

Test Environment

The testing environment consisted of the following:

- Spirent Avalanche and Reflector
- Two Lucent P550 routing switches
- All connections are fiber Gigabit Ethernet
- NetScreen-ISG 2000 configured with a policy of "allow any HTTP" with Deep Inspection disabled



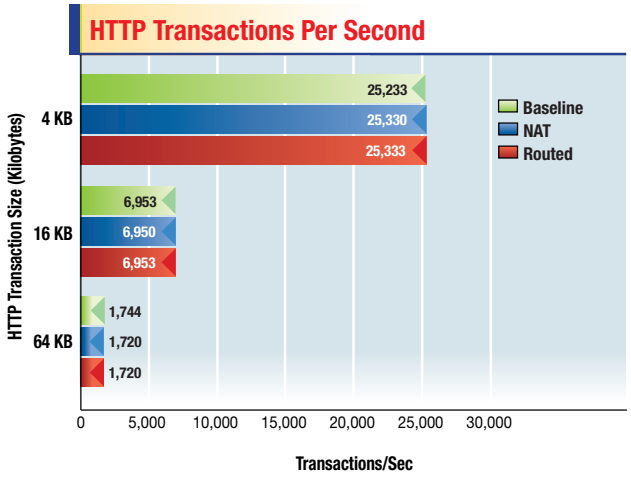
Each Cajun P550 switch was equipped with a route switch processor, thereby enabling the layer 3 routing capability. Each Spirent Avalanche and Reflector was connected to a corresponding Cajun P550 via dual gigabit fibers. The NetScreen-ISG 2000 was connected to the Cajun P550s through slot 1 port 1 and slot 3 port 1, respectively. All traffic traversed the NetScreen-ISG 2000 back plane. A temporary link between the Cajun P550 was used to baseline the traffic environment.

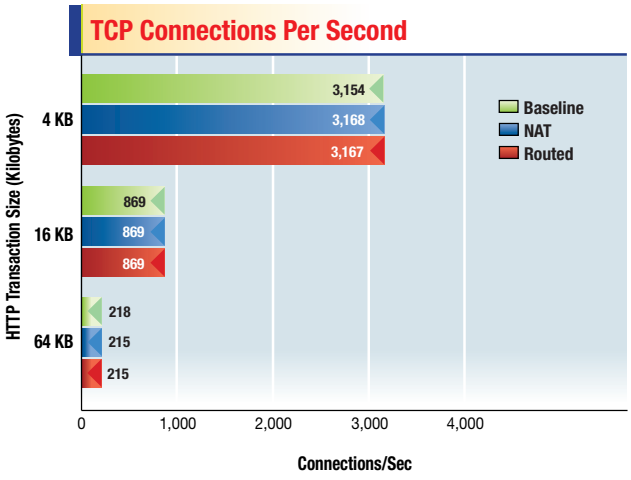
Validation Test 2: HTTP Performance

HTTP Test Results

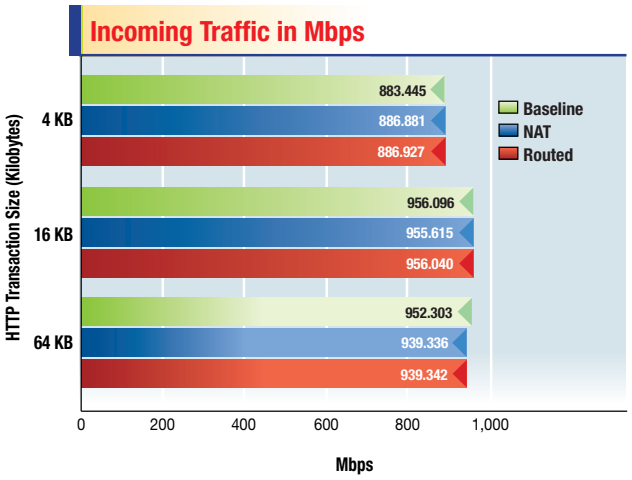
The results clearly indicated that inserting the NetScreen-ISG 2000 into the test topology had little or no negative impact on network performance. Each metric demonstrates the performance differences among the baseline with no firewall present, the NetScreen-ISG 2000 in NAT mode and the NetScreen-ISG 2000 in Routed mode. Across all metrics, the differences in performance among the baseline, Routed mode and NAT mode were negligible.

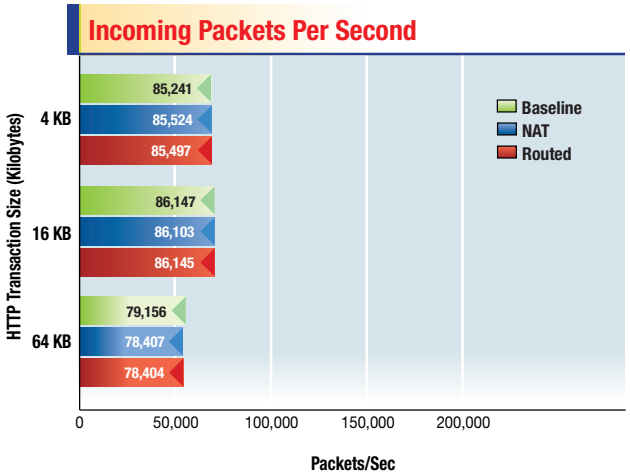
The following results used a TCP MSS of 1,460 bytes with varying HTTP transaction sizes in kilobytes. Results indicate the NetScreen-ISG 2000 sustained no substantial negative impact on throughput or latency performance.

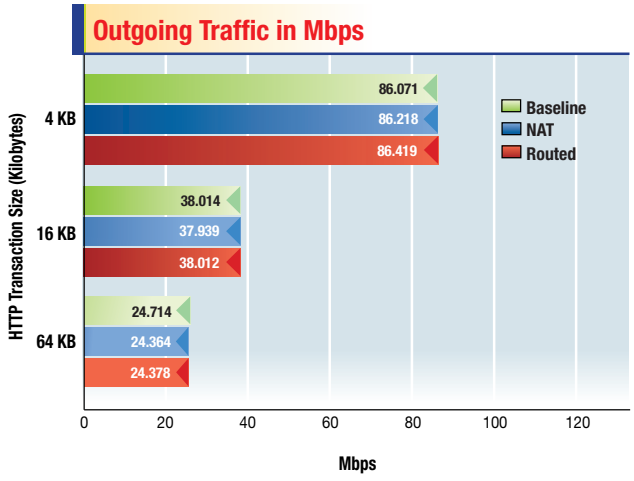


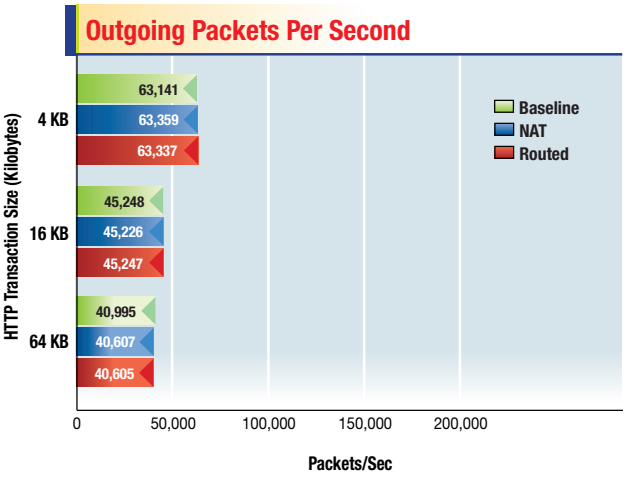


HTTP Test Results *continued*





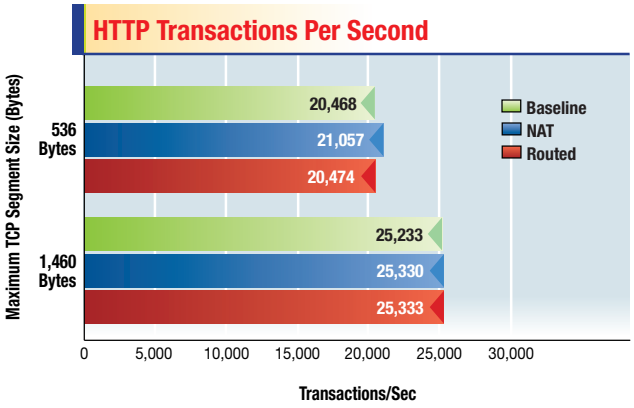


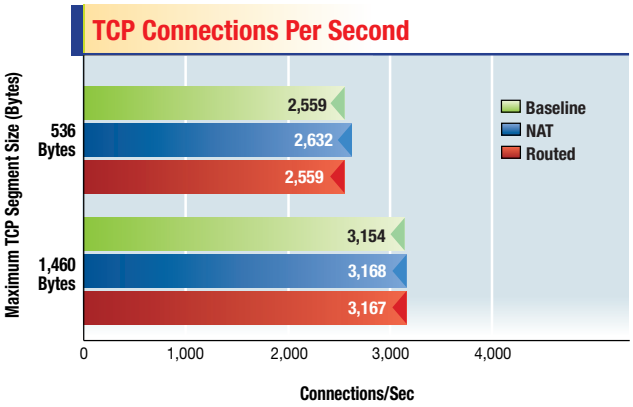


Validation Test 2: HTTP Performance

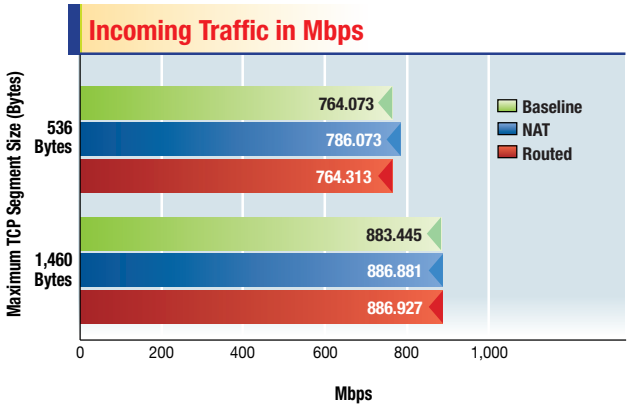
HTTP Test Results *continued*

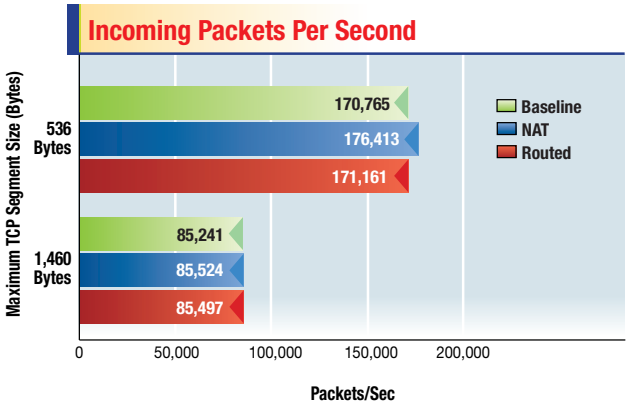
The following results used a fixed transaction size of four kilobytes with an MSS of both 536 and 1,460 bytes. Results indicate the NetScreen-ISG 2000 sustained no substantial negative impact on throughput or latency performance.

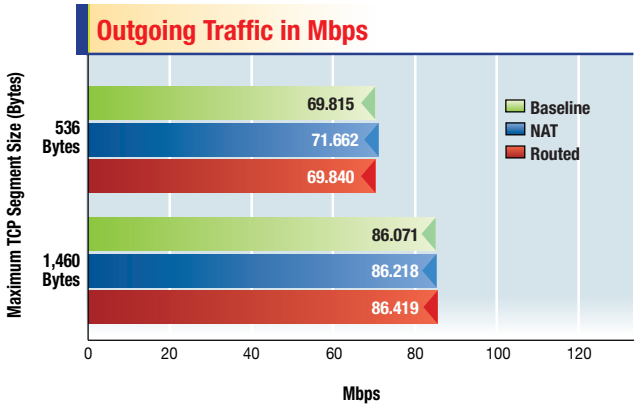


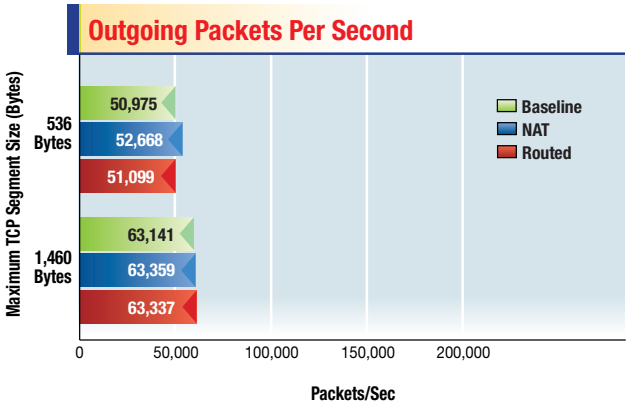


HTTP Test Results *continued*









Validation Test 3: TCP Session Rate

Test Summary

Performance Claim Subject to Validation:
The NetScreen-ISG 2000 is capable of sustaining TCP connection rates beyond 20,000 per second.

Validation Test Methodology:
TCP session rate is the number of new TCP connections per second that the firewall can negotiate successfully. The testing methodology consisted of ramping up TCP sessions to 400,000 sessions at varying rates using Spirent WebSuite. Each highest successfully sustained connection rate was plotted, resulting in a graph of connection rate against total number of connections established.

Results Conclusion:
Under all tested conditions, the NetScreen-ISG 2000 exhibited sustained performance between 22,000 and 30,000 TCP connections per second.

Test Design

The NetScreen-ISG 2000 was configured for Routed mode with a policy of "accept any all" between zones. One zone was assigned "External," representing the client network, and the other zone was assigned "Internal," representing the protected servers.

Connections were initiated from the client/External side, with a server/Internal network destination. The following variations in topology were verified to exhibit the same performance results:

- 100 hosts, 1,000 connections per host, four servers
- 1,000 hosts, 400 connections per host, one server

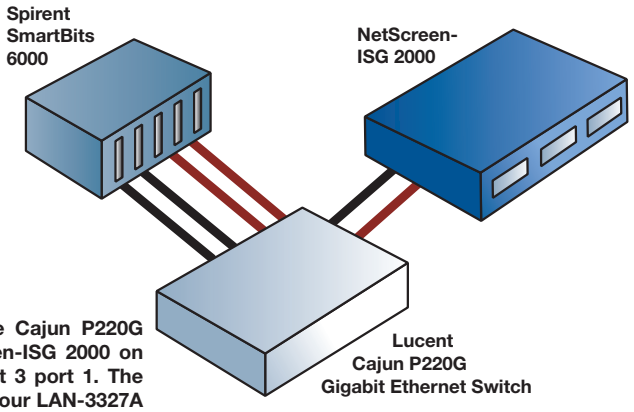
To ensure that the SmartBits 6000 was not the constraint (bottleneck) in the testing, testing was repeated with two and four SMB 6000 interfaces.

Why These Tests Matter:
TCP session rate and time to establish a connection directly impact end-user response time and ability to continue processing client requests. The vast majority of Web-based applications negotiate an independent TCP connection per response page. Multiple transactions are possible per connection; however, the performance for concurrent connections will limit the total number of users and the responsiveness of the application.

Test Environment

The testing environment consisted of the following:

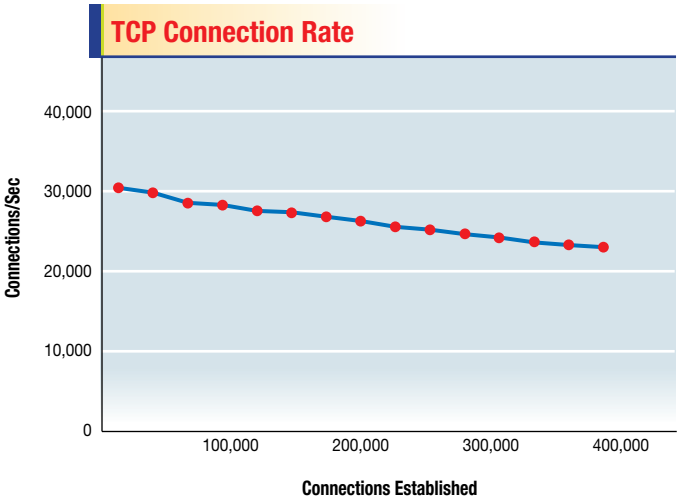
- Spirent SmartBits SMB 6000 with LAN-3327A interfaces
- Spirent WebSuite 2.60.001
- Lucent Cajun P220G Line Rate GE Switch partitioned with two VLANs
- NetScreen-ISG 2000 configured for Routed mode with a policy of "accept any all" between zones

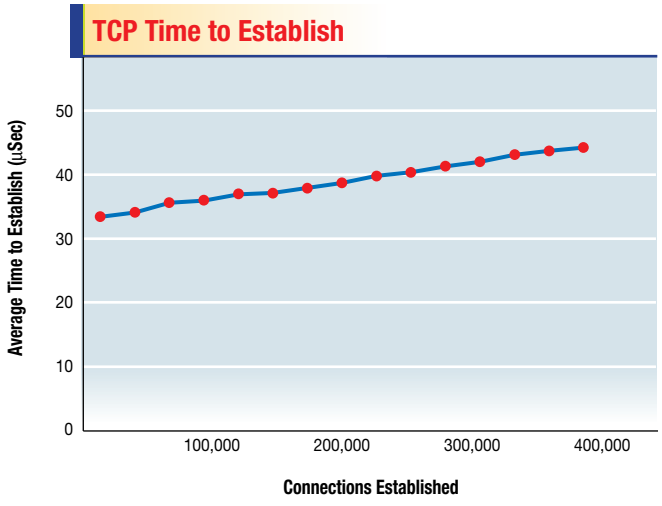


Two port-based VLANs were established in the Cajun P220G switch. VLAN 1 was connected to the NetScreen-ISG 2000 on slot 1 port 1 and VLAN 2 was connected to slot 3 port 1. The Spirent SmartBits SMB 6000 was equipped with four LAN-3327A interfaces, with two interfaces connected to each VLAN. All traffic traversed the NetScreen-ISG 2000 back plane.

TCP Test Results

Under all tested conditions, the NetScreen-ISG 2000 exhibited sustained performance between 22,000 and 30,000 TCP connections per second. Variable performance was exhibited based on the number of previously established connections. As the total concurrent connection count increased, there was a slight degradation in the rate at which new connections could be established. Overall, the NetScreen-ISG 2000 sustained well over 20,000 connections per second.





NOTE: 1 millisecond (MSec) = 1,000 microseconds (µSec)

The average time to establish a TCP connection is a measure of latency induced by the device under test. As with TCP connection rate, TCP time to establish correlates with the total number of previously established connections. Average time to establish a TCP connection varies from 33 microseconds to just under 45 microseconds. In real-world deployments, metrics are in multiples of milliseconds not microseconds, indicating that the latency performance of the NetScreen-ISG 2000 would be sufficiently low and would have little or no negative impact on end-user connections.

Validation Test 4: IPSec VPN

Test Summary

Performance Claim Subject to Validation:
NetScreen-ISG 2000 provides 1-Gbps throughput (3DES with SHA1, IPSec header + payload) using 64-, 512- and 1,518-byte frame sizes with one, 10 and 100 tunnels.

Validation Test Methodology:
Benchmarking IPSec has two common methods:

1. Use IPSec-specific performance measurement equipment such as Spirent TeraVPN
2. Connect two VPN concentrators to each other using IPSec encryption between them

To measure IPSec tunnel establishment rates (ramp rate) as well as raw throughput for all packet sizes, both testing methods were used.

Results Conclusion:
Iterative testing of IPSec ramp rate at incremental rates with TeraVPN found that the NetScreen-ISG 2000 could sustain negotiating 80 tunnels per second.

Taking into account all overhead, the NetScreen-ISG 2000 sustained 1-Gbps performance for both 512- and 1,518-byte frame sizes. The 1,518-byte frames required IPSec fragmentation when encapsulated in an IPSec payload, which also demonstrated 1-Gbps performance.

Test Design

Validation Test 1: Ramp Rate Testing
The NetScreen-ISG 2000 was configured with 1,200 individual IPSec 3DES SHA-1 tunnels corresponding to 1,200 TeraVPN tunnels. Each tunnel was assigned a unique source, destination and tunnel endpoint identifier, resulting in an independent IPSec Phase I and Phase II association per tunnel. To ensure that the SmartBits 6000 was not the constraint (bottleneck) in the VPN ramp rate, testing was repeated with two and four SMB 6000 interfaces.

Validation Test 2: Throughput Testing
Each NetScreen-ISG 2000 was configured with 100 policy-based IPSec 3DES SHA-1 tunnels. Each tunnel was assigned a unique source, destination and tunnel endpoint identifier, resulting in an independent IPSec Phase I and Phase II association per tunnel. The following variations in topology were tested:

- **Frame Size** – 64, 512, 1,518 bytes (1,518 required fragmentation across the IPSec tunnels)
- **Number of Tunnels** – one, 10, 100 (bi-directional UDP flows in SmartFlow mapped to individual tunnels)

Why These Tests Matter:
To understand a VPN device's overall performance profile, it is important to test both the device's session ramping and its throughput capabilities. IPSec session negotiations are important for morning rushes and tunnel turnaround times. Of particular concern is how the device performs if overloaded by new tunnel requests. Throughput tests are also important, but are often of less value if they aren't compared to session negotiation capabilities as well.

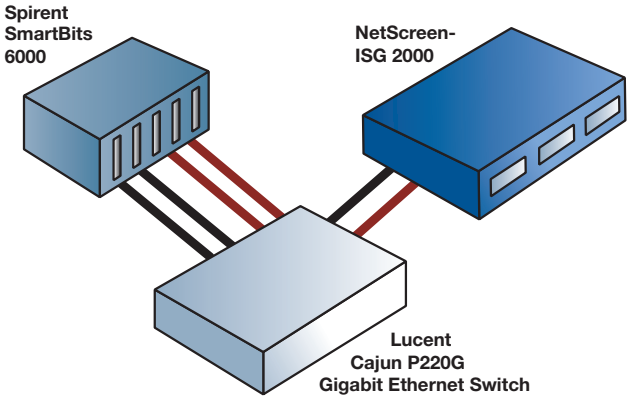
Validation Test 4: IPSec VPN

Test Environment

Test Topology 1: Ramp Rate Testing

The ramp rate test environment included:

- SmartBits 6000 supporting four LAN-3327A interfaces with VPN accelerators
- TeraVPN 4.00.060 configured with 1,200 independent tunnels
- Lucent Cajun P220G Line Rate GE Switch partitioned with two VLANs
- NetScreen-ISG 2000 configured with 1,200 independent 3DES SHA-1 tunnels

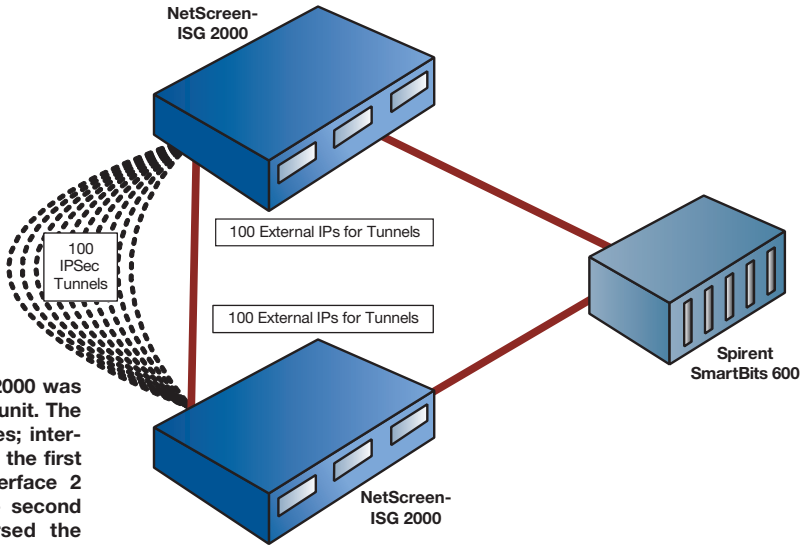


Two port-based VLANs were established in the Cajun P220G switch. VLAN 1 was connected to the NetScreen-ISG 2000 on slot 1 port 1 and VLAN 2 was connected to slot 3 port 1. The Spirent SmartBits SMB 6000 was equipped with four LAN-3327A interfaces, with two interfaces connected to each VLAN. All traffic traversed the NetScreen-ISG 2000 back plane.

Test Topology 2: Throughput Testing

The IPSec VPN throughput test environment included:

- Spirent SmartBits SMB 600 with LAN-3301A interfaces
- Spirent SmartFlow 3.00.124.1
- Two NetScreen-ISG 2000s configured with 100 IPSec tunnels



Slot 1 port 1 of the first NetScreen-ISG 2000 was connected to slot 1 port 1 of the second unit. The SmartBits used two LAN-3301A interfaces; interface 1 was connected to slot 3 port 1 on the first NetScreen-ISG 2000 and SmartBits interface 2 was connected to slot 1 port 3 on the second NetScreen-ISG 2000. All traffic traversed the NetScreen-ISG 2000 back plane.

IPSec Test Results

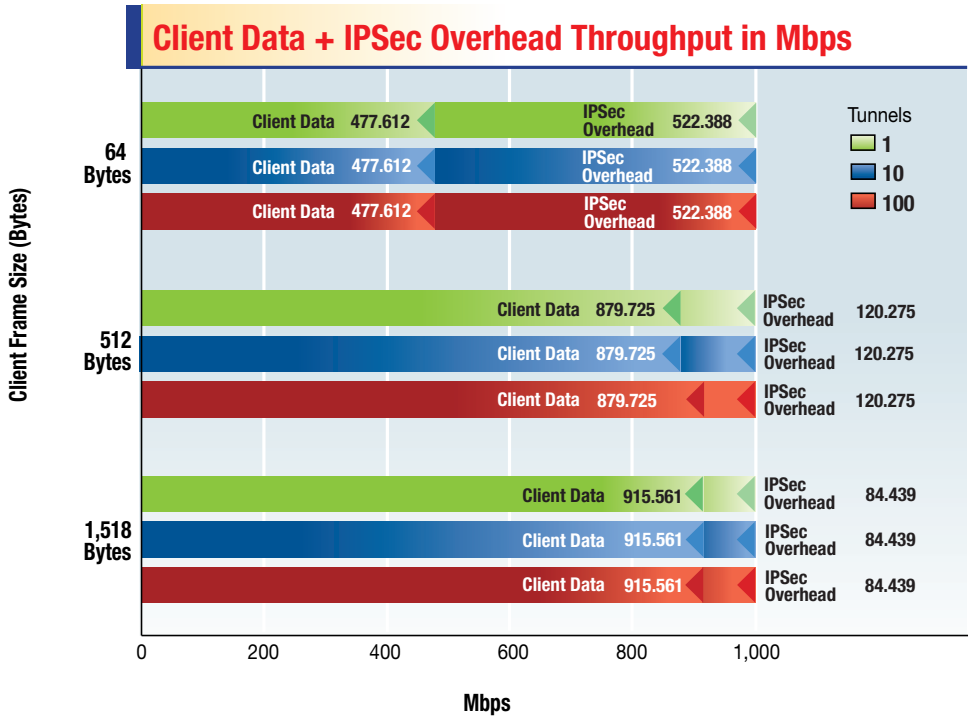
Test Topology 1: Ramp Rate Testing

Iterative testing of IPSec ramp rate at incremental rates with TeraVPN found that the NetScreen-ISG 2000 could sustain negotiating 80 tunnels per second.

When higher establishment rates were requested (tested up to 200 per second), the NetScreen-ISG 2000 buffered the requests and responded to the connection requests in a first come, first serve manor at approximately 80 tunnels per second. At no time during the testing were sessions dropped, and all requested sessions negotiated successfully.

Test Topology 2: Throughput Testing

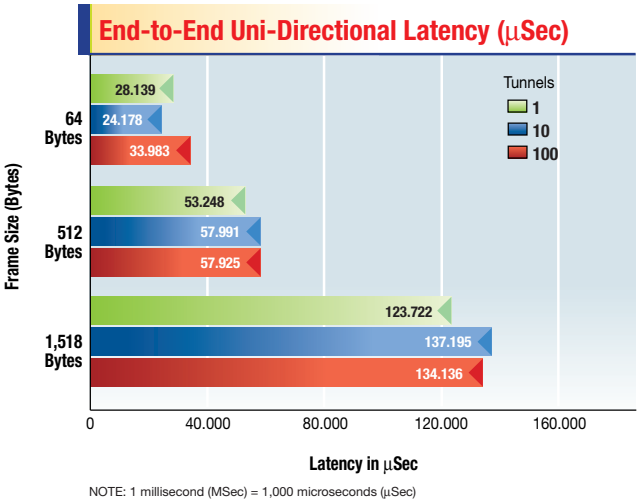
Bi-directional throughput in IPSec is reported both with and without the 50-byte IPSec overhead (in addition to the 20-byte packet gap and preamble) incurred on the basis common to all IPSec implementations. For 64-, 512- and 1,518-byte frame sizes, the NetScreen-ISG 2000 performed at 1 Gbps across one, 10 and 100 simultaneous tunnels.



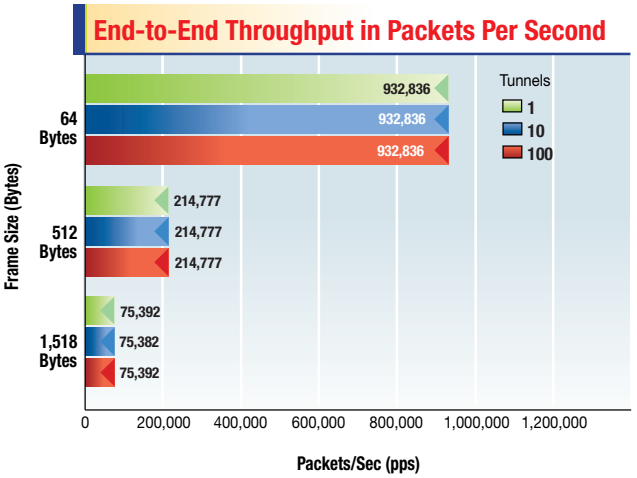
NOTE: 1,518-byte packets require fragmentation across two IPSec packets, thereby incurring twice the overhead. The NetScreen-ISG 2000 continued to process at 1 Gbps under these fragmented conditions.

IPSec Test Results *continued*

Configured with two NetScreen-ISG 2000s encrypting and decrypting bi-directionally, the test topology exhibited less than 150 microseconds for all packet sizes. Most VPN implementations exhibit several milliseconds of latency. With the NetScreen-ISG 2000 performing in the microsecond range, the induced latency was considerably lower than what Internet VPN consumers currently experience.



NOTE: 1 millisecond (MSec) = 1,000 microseconds (µSec)



Final Thoughts

POWERED BY Network Computing Labs

Test Profile

Vendor: Juniper Networks
Firmware Version: nsISG2000.5.0.0g1.2
Test Window: July 2004 – September 2004
Price: Starts at $34,995
Report Number: ITS04002
Report Date: October 19, 2004
Vendor Contact: www.juniper.net,
888-JUNIPER (888-586-4737), 408-745-2000

Test Infrastructure:

Products:

- Spirent SmartBits SMB 6000 with LAN-3327A interfaces
- Spirent SmartBits SMB 600 with LAN-3301A interfaces
- Spirent SmartFlow 3.00.124.1
- Spirent WebSuite 2.60.001
- Spirent Avalanche and Reflector
- Spirent TeraVPN 4.00.060
- **URL:** www.spirentcom.com

Other Infrastructure:

- Two Lucent P550 Routing Switches
- Cajun P220G GE Switch

Special thanks go to Spirent Communications for both support and equipment provisioning for this testing.

About Us

For well over a decade, ***Network Computing*** has set the standard for real-world analysis of enterprise-class products, technologies and services. Creating unbiased testing methodologies and defining what matters most have been the cornerstones of our Labs.

Independent Testing Services powered by Network Computing Labs™ (ITS) offers a credible and well-respected third-party validation of vendors' product feature claims. The expert practitioners at ITS draw upon their vast experience and expertise to craft test plans with the same care and attention to real-world relevance as found in the pages of ***Network Computing*** Magazine.

POWERED BY Network Computing Labs

For more information about our testing services, please visit us at ***www.nwctests.com***. If you're interested in testing validation services, please contact us at ***info@nwctests.com.***