NEOHAPSIS

INDEPENDENT CLAIM VALIDATION

Juniper Networks SA6500 SSL VPN Appliance

May 2009

NEOHAPSIS LABS™

Cambridge, MA • San Jose, CA • Chicago, IL • Alexandria, VA • Edmonton, Canada • London, UK • Chennai, India

www.neohapsis.com

TABLE OF CONTENTS

Executive Summary

VENDOR PRODUCT OVERVIEW

Juniper Networks SA Series SSL VPN Appliances lead the SSL VPN market with a complete range of remote-access appliances. These products include the new, next-generation Juniper Networks SA2500 SSL VPN Appliance, the Juniper Networks SA4500 SSL VPN Appliance, and the Juniper Networks SA6500 SSL VPN Appliance. The SA Series combines the security of SSL with standards-based access controls, granular policy creation, and unparalleled flexibility. The result is ubiquitous security for all enterprise tasks with options for increasingly stringent levels of access control to protect the most sensitive applications and data. Juniper Networks SA Series SSL VPN Appliances deliver lower total cost of ownership over traditional IPsec client solutions and offer unique end-to-end security features.

This report focuses on the SA6500 SSL VPN Appliance. Its features include best-in-class performance, scalability, and redundancy for organizations with high volume secure access and authorization requirements. Additionally, the SA6500 offers high availability with seamless user failover. It also includes built-in compression for Web traffic and files and a state-of-the-art SSL acceleration chipset to speed CPU-intensive encrypt/decrypt processes.

The SA6500's high scalability and redundancy capabilities were designed specifically for large enterprises and service providers.

INDEPENDENT CLAIM VALIDATION

Neohapsis Labs™ was contracted by Juniper Networks to independently validate specific capabilities of its SA6500 SSL VPN Appliance. Testing was conducted at Neohapsis Labs™ from February through March 2009.

The following claim of Juniper Networks was subject to open and independent testing verification:

- The SA6500 SSL VPN Appliance can sustain 10,000 concurrent user tunnels.

RESULTS SUMMARY

To validate the proposed claim of the SA6500 SSL VPN Appliance, Neohapsis Labs™ created a topology using the IXIA 1600T chassis with seven cards running IXVPN version 2.20 and a custom Juniper VPN module.

The IXVPN was configured to perform an RFC 2544 soak test using 512-byte frames. A series of requested tunnels (7,112, 8,890, and 10,668) was configured on the IXIA 1600T chassis. Each value of the series was run three times for a total of nine rounds of testing. Soak tests were configured to run for two hours.

Testing results showed that the SA6500 was able to maintain over 10,000 VPN tunnels with less than 1 percent frame loss within the constraints of the test environment.

Test Methodology

Neohapsis Labs™ tested the Juniper Networks SA6500 SSL VPN Appliance in an isolated test environment within our lab. The network consisted of the following elements:

- SA6500 SSL VPN Appliance running SA software version 6.4 release 1
- IXIA 1600T chassis running IXOS firmware version 4.10.250 service pack 7 with seven cards running IXVPN version 2.20 and a custom Juniper VPN module
- IXIA external client workstation running Windows XP Professional and IXVPN version 2.20
- Microsoft Windows Server 2003 Active Directory for authentication
- HP ProCurve 3400 CL internal switch
- Juniper EX 3200 external switch
- Microsoft Windows XP external client
- Linux client workstation for traffic monitoring

The following test phases were completed:

1. Tunnel values were selected to provide a range inclusive of 10,000. This selection allowed trending on the results to determine performance. Tunnel values were selected by finding multiples of 254 that were cleanly divisible by the number of cards in the IXIA 1600T chassis. This equation is summarized as (254x)mod7, and it resulted in tunnel values of 7,112, 8,890, and 10,668.[1]
2. For each tunnel value, a routing table was created for the internal and external interfaces of the SA6500. Once the routing table was in place, the configuration was saved to the IXIA client workstation.
3. A configuration was created for the IXVPN using the selected number of tunnels and the RFC 2544 soak test with a frame size of 512 bytes and a duration of two hours. In addition, this test was configured to use bi-directional traffic with a limit of 150Mbps for an aggregate of 300Mbps.
4. Once both the SA6500 and the IXVPN configurations were in place, the test was executed. Results were recorded into a spreadsheet and exported to the IXIA client workstation.
5. A series of nine rounds of tests were run. One round consisted of one test of one tunnel value. Each of the three tunnel values (7,112, 8,890, and 10,668) was used for three non-consecutive rounds of tests.
6. The entire environment was reset after each round of testing. This reset included terminating all tunnels to the SA6500, restarting the IXIA 1600T chassis, and reloading the IXVPN software. The SA6500 was also restarted after each routing configuration change.

Traffic was monitored with tcpdump on the Linux client workstation and mirrored ports on the switches. The SA6500, the IXIA 1600T chassis, and the IXIA client workstation were all monitored throughout the testing. Monitoring provided a means of verifying the establishment of tunnels, the numbers of tunnels, and traffic.

WHY THESE TESTS MATTER

A number of critical areas need to be assessed when evaluating VPN technology. These areas include, but are not limited to, the number of authenticating clients, the number of sustainable tunnels, throughput during intensive tasks such as encrypting and packet inspection, and policy enforcement. Testing for this report focused on authentication and sustainable tunnels. The results of the tests performed at Neohapsis Labs™ demonstrate that the SA6500 was able to authenticate clients and to establish and sustain tunnels with traffic for two hours with over 10,000 tunnels requested by the IXIA 1600T chassis and the IXIA client workstation.

[1] The validation goal was the performance of the SA6500 at 10,000 simultaneous tunnels. Ideally, testing would have been performed using only that specified number of tunnels. Unfortunately, the IXIA 1600T chassis was designed to distribute IPs for the requested number of tunnels evenly across its interfaces without regard to subnetting.

Test Environment

The test environment consisted of the IXIA 1600T chassis connected to two dedicated switches, one external (the Juniper EX 3200) and one internal (the HP ProCurve 3400 CL). The Juniper Networks SA6500 SSL VPN Appliance was placed between the switches, emulating a border gateway device. Mirror ports were created on the switches to provide traffic monitoring and evaluation from the standalone Linux client workstation. A Windows XP client was placed on the external switch to allow manual SSL VPN connections to the SA6500. This placement allowed validation and testing of the environment during build out. Windows Server 2003 running Active Directory as a domain controller provided an authentication realm for the SA6500.

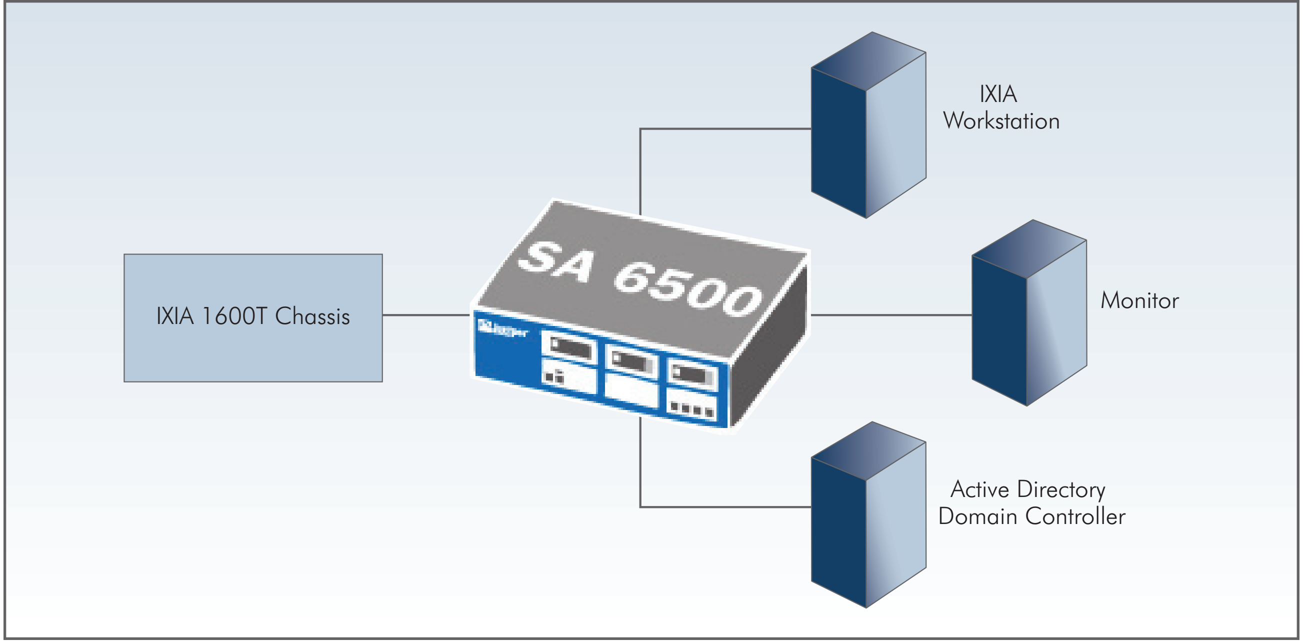
Management of the network was accomplished by dual homing the external workstation, Active Directory, and the Linux workstation with the network at Neohapsis Labs™. This setup allowed remote access to all systems while segmenting the test environment. (See Figure 1, "Physical Environment Diagram.")

The IXIA 1600T chassis was configured with seven cards, each of which had dual gigabit Ethernet ports, for a total of seven external and seven internal interfaces. Each of these interfaces was configured as a virtual router in the environment. The external interface of the SA6500 IP address was set to 5.0.0.10, which allowed the external virtual routers of the IXIA 1600T chassis to be configured as 5.0.0.[11-17]. The internal interface of the SA6500 mirrored the external configuration, with the IP address set to 4.0.0.10 and virtual routers set to 4.0.0.[11-17].

The IXIA client workstation was a Windows XP Professional system running the IXVPN 2.20 client. (This system was also capable of creating an independent SSL VPN connection to the device under test.) Configurations for the tests and the SA6500 were stored on this workstation over the course of the engagement.

Active Directory on a Windows Server 2003 machine provided only an authentication domain for the SA6500. A script was used to create 25,000 users within Active Directory.

FIGURE 1 - PHYSICAL ENVIRONMENT DIAGRAM

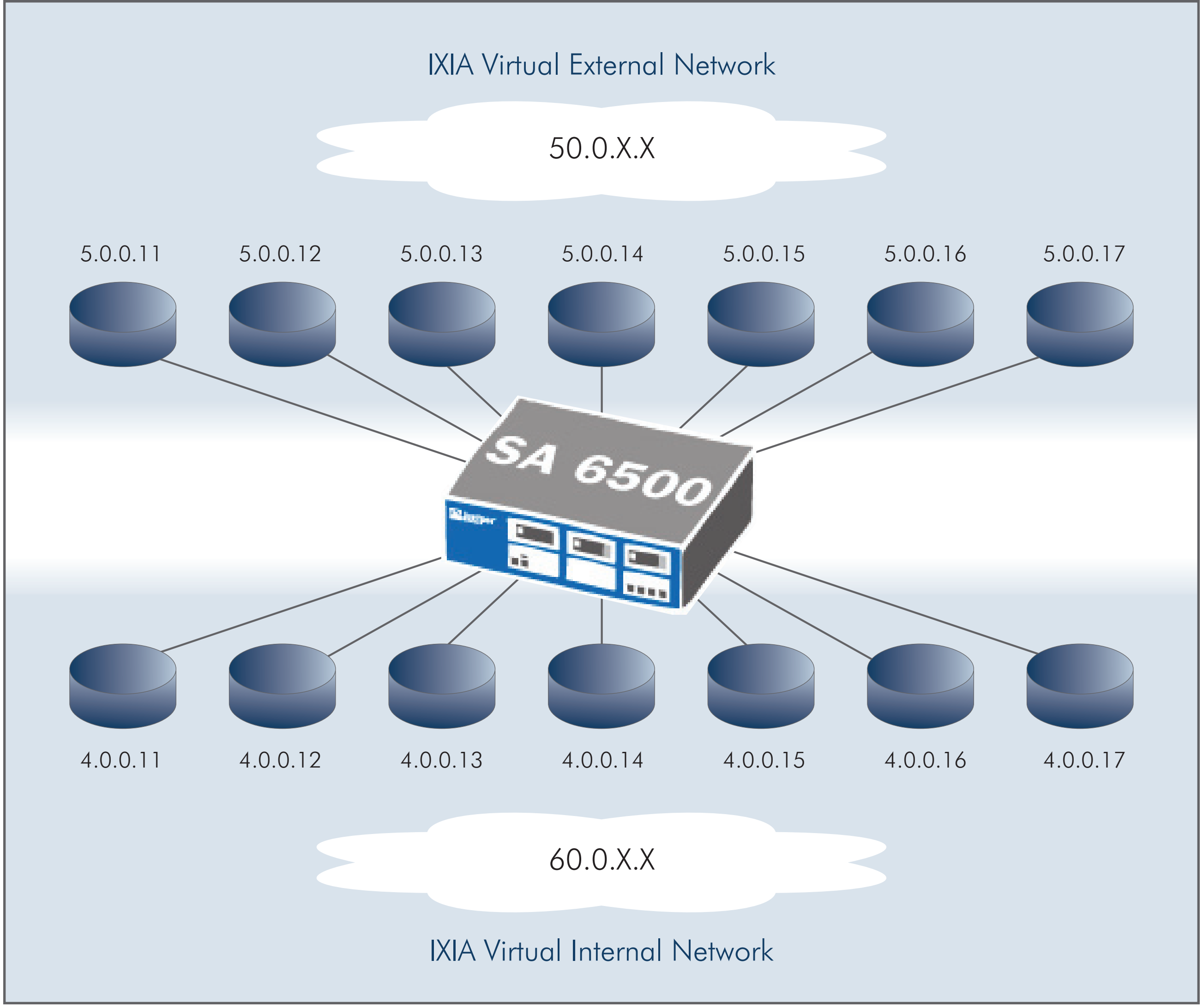


Test Environment

The monitoring system was configured with Ubuntu 8.10 and used tcpdump to monitor and verify network traffic. Captures of traffic were created and stored to analyze traffic and identify possible issues.

The IXIA 1600T chassis created a pool of virtual hosts within the external and internal cloud, using the IP spaces 50.0.0.0 and 60.0.0.0, respectively. In addition, the IXIA chassis dynamically assigned these hosts to specific virtual gateways based on the number of tunnels requested. To compensate for this assignment, routing tables were manually created and loaded on the SA6500 for each set of the selected tunnel settings. (See Figure 2, "Logical Environment Diagram.")

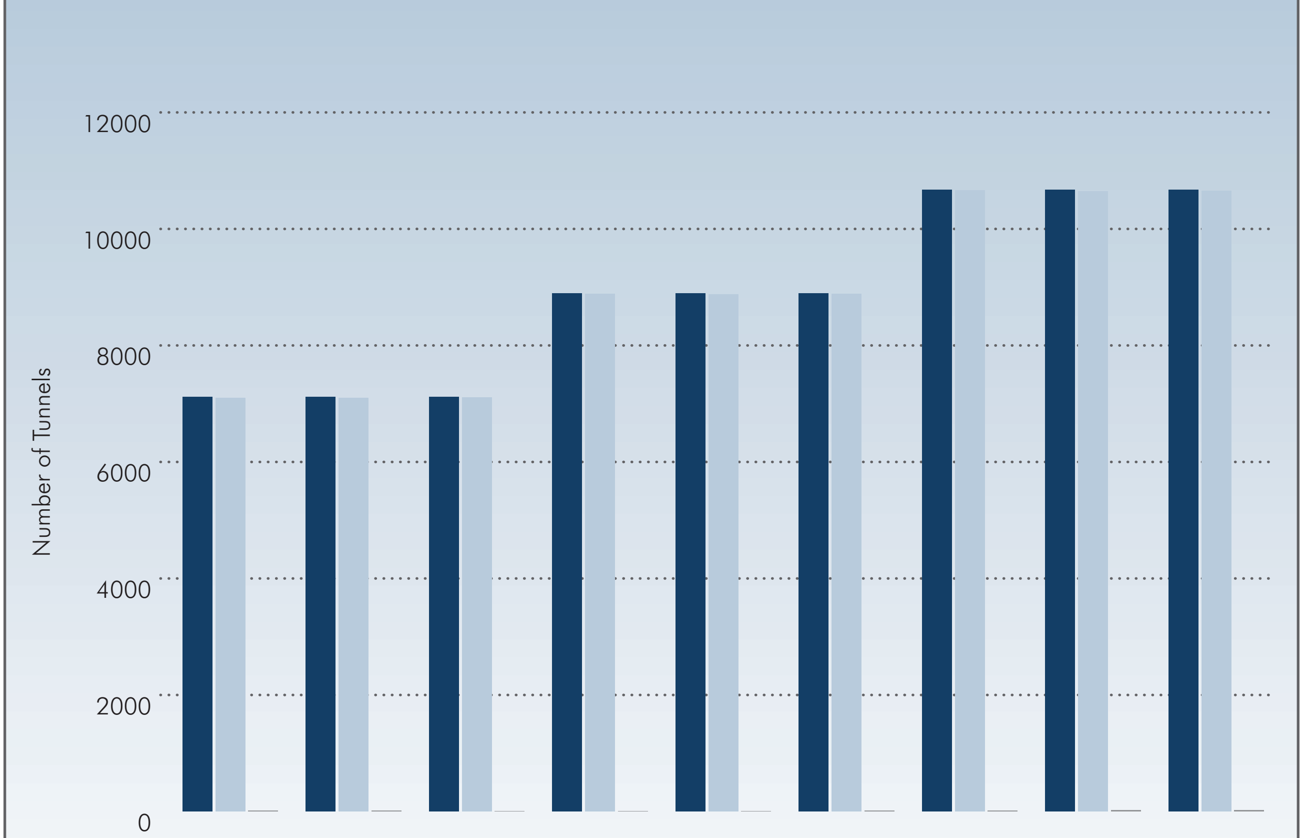
FIGURE 2 - LOGICAL ENVIRONMENT DIAGRAM



Results Summary

The Juniper Networks SA6500 SSL VPN Appliance successfully provided a less than 1 percent failure rate across all the tests in the series. It had a 99.87 percent success rate for sustaining from 7,112 to 10,668 tunnels for a period of two-plus hours. (Figure 3, "Sustained Tunnels," and Table 1, "Packet Loss," illustrate the data.)

FIGURE 3 - SUSTAINED TUNNELS



	1	2	3	4	5	6	7	8	9
Attempted ■	7112	7112	7112	8890	8890	8890	10668	10668	10668
Established □	7097	7102	7105	8883	8878	8882	10665	10643	10650
Failures ▨	15	10	7	7	8	12	13	25	18

Results Summary

Packet loss numbers were recorded for the decryption and encryption functions of the SA6500. The results indicated that decryption introduced a typical packet loss for tunnel values equal or less than 0.10 percent, with a single anomaly at 0.52 percent. Packet loss due to encryption was constant for all tunnel values at 0.03 percent. (Table 1, "Packet Loss," and Figure 4, "Packet Loss Less Than 1%," illustrate these results.)

TABLE 1 - PACKET LOSS

Decryption (packets)

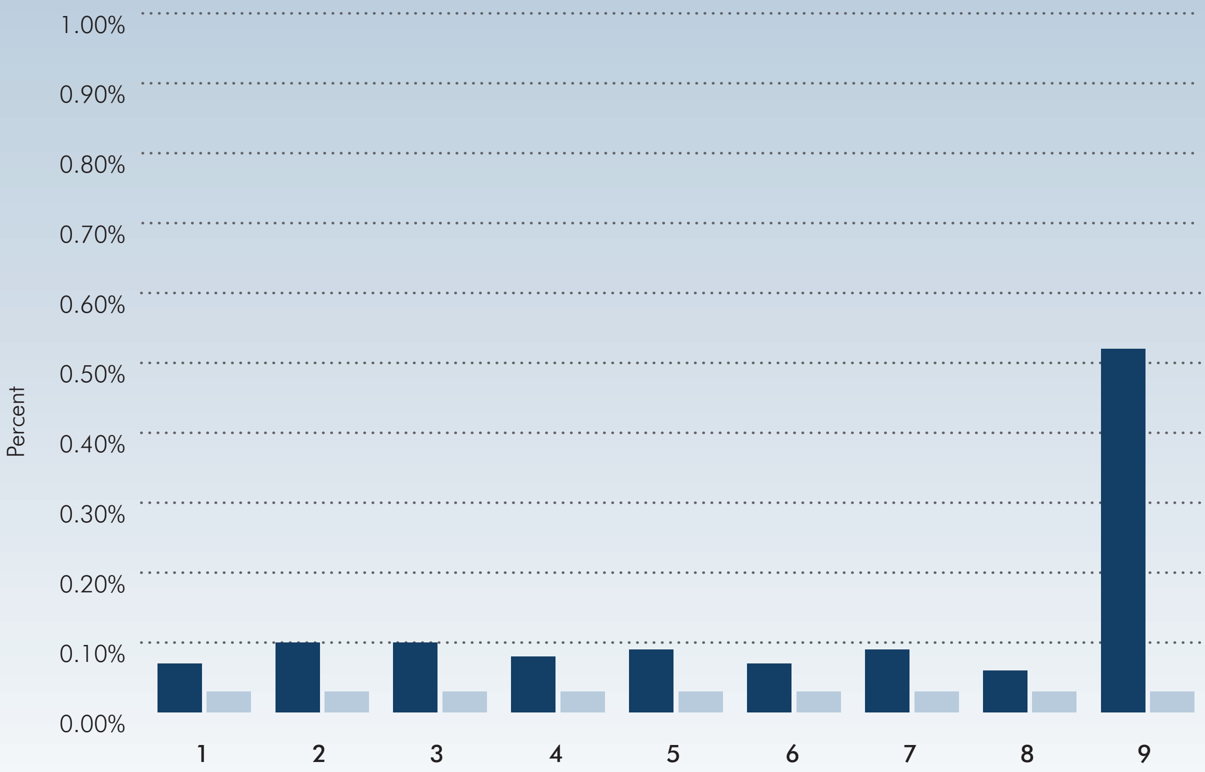
Round	Tunnels	Sent	Received	Loss	% Success	% Loss
1	7,097	263,753,934	263,575,671	178,263	99.93%	0.07%
2	7,102	263,769,075	263,513,463	255,612	99.90%	0.10%
3	7,105	263,750,849	263,496,304	254,545	99.90%	0.10%
4	8,883	263,759,783	263,561,870	197,913	99.92%	0.08%
5	8,878	263,783,438	263,554,271	229,167	99.91%	0.09%
6	8,882	263,781,582	263,586,666	194,916	99.93%	0.07%
7	10,665	263,768,332	263,539,926	228,406	99.91%	0.09%
8	10,643	263,777,271	263,630,776	146,495	99.94%	0.06%
9	10,650	263,765,971	262,395,809	1,370,162	99.48%	0.52%

Encryption (packets)

Round	Tunnels	Sent	Received	Loss	% Success	% Loss
1	7,097	263,753,812	263,674,363	79,449	99.97%	0.03%
2	7,102	263,769,254	263,689,923	79,331	99.97%	0.03%
3	7,105	263,751,066	263,671,202	79,864	99.97%	0.03%
4	8,883	263,760,081	263,677,564	82,517	99.97%	0.03%
5	8,878	263,767,782	263,686,677	81,105	99.97%	0.03%
6	8,882	263,781,850	263,700,452	81,398	99.97%	0.03%
7	10,665	263,768,368	263,682,658	85,710	99.97%	0.03%
8	10,643	263,777,671	263,692,108	85,563	99.97%	0.03%
9	10,650	263,766,192	263,680,281	85,911	99.97%	0.03%

Results Summary

FIGURE 4 - PACKET LOSS LESS THAN 1%



	1	2	3	4	5	6	7	8	9
Tunnels	7097	7102	7105	8883	8878	8882	10665	10643	10650
% Decrypt Loss ■	0.07%	0.10%	0.10%	0.08%	0.09%	0.07%	0.09%	0.06%	0.52%
% Encrypt Loss □	0.03%	0.03%	0.03%	0.03%	0.03%	0.03%	0.03%	0.03%	0.03%

CONCLUSIONS

After completing nine rounds of testing at Neohapsis Labs™ with the IXIA 1600T chassis and the IXIA client workstation, we determined that the Juniper Networks SA6500 SSL VPN Appliance was able to successfully maintain up to 10,650 tunnels with a maximum decryption packet loss of 0.52 percent and a maximum encryption packet loss of 0.03 percent.

Headquarters

215 First Street
Suite 005
Cambridge, MA 02142
Tel: +1 773 269 6300
Fax: +1 617 577 7922

Neohapsis Labs™

217 North Jefferson Street
Suite 200
Chicago, IL 60661
Tel: +1 773 269 6300
Fax: +1 773 394 8314

Regional Offices

San Jose, CA
Chicago, IL
Alexandria, VA
Edmonton, Canada
London, UK
Chennai, India

www.neohapsis.com