Network Security Testing Solution

Enterprise Solution

Enterprise customers include:

- AOL
- Bank of America
- Bank One
- BEA
- Costco.com
- DaimlerChrysler
- EBay
- EDS
- Forbes.com
- HSCC
- MSNBC
- National City Bank
- Reuters
- Wells Fargo

Spirent testing tightens network security at National City Bank.

Online banking customers expect quick access and tight security, and have no patience for delays or downtime. To deliver a secure and satisfying user experience, National City Bank needed solutions that could handle the testing challenges posed by a mixture of SSL-encrypted traffic and regular Web traffic.

The market-leading Avalanche and Reflector testing appliances provided visibility into every aspect of their network. After testing revealed that certain components did not perform at vendor-advertised thresholds, the equipment was replaced at no cost. The result? Optimized network performance and a superior customer experience.

Why test network security equipment?

Critical threats to network security emerge with alarming frequency. With today's increased threat levels, the need for realistic assessment of security devices and systems is greater than ever. As viruses, worms, Distributed Denial of Service (DDoS) attacks, and other threats become ever-more sophisticated, how can you ensure that your security infrastructure will protect your network from malicious attacks? Simply trusting vendors' performance claims isn't enough. To better assess your security needs, you need to ask yourself the following questions:

- Will my deep-packet inspection, intrusion detection systems (IDS), and intrusion protection systems (IPS) systems defend the network against new threats as soon as they emerge?
- Does my security infrastructure provide acceptable performance for valid user traffic during an attack?
- Do my "best-of-breed" devices work well together—are the policies on each device synergistic or conflicting?
- Can my network handle virus detection and spam filtering even under heavy loads?
- Can my firewalls enforce policies and resist hackers with traditional and application-level inspections?
- Can my devices resist DDoS attacks such as LAND, TearDrop, Ping of Death, SMURF attacks, SYN, or Wonk floods?
- How can I measure the tunnel capacity and performance of my Virtual Private Network (VPN)?
- Can my devices handle extreme loads, and if not, do they fail "open," letting all traffic through unchecked, or "closed," where no traffic gets through?

Finding the answers to these questions is simple: you test. By testing your network security infrastructure, including deep-packet inspection products, IDS/IPS devices, next-generation firewalls, IPSec VPN concentrators, and SSL accelerators, you can verify capacity and performance before you deploy or make major purchasing decisions—saving time, allocating resources wisely, and ensuring peace of mind in a malicious computing environment.

Why is realistic testing so important to ensure security?

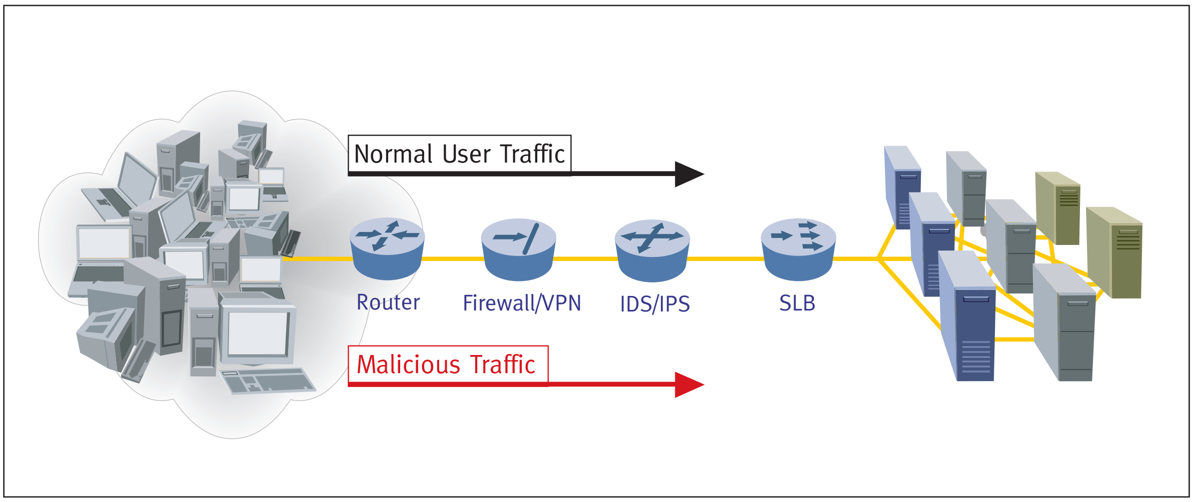
Legacy testing products aren't capable of realistically emulating user behavior or the characteristics of the network traffic and equipment in your operating environment. Each infrastructure is unique, making it impossible for generalized testing to assess the security of your network.

To ensure that your security infrastructure is solid, your testing solution needs to evaluate overall performance, supply a high degree user and network realism, and the deliver the ability to test with both normal and malicious traffic. In addition to providing comprehensive testing, it should also be easy to set up and use. Fortunately, there is such a solution: the Spirent Communications family of security testing products.

Spirent Communications
26750 Agoura Road
Calabasas Hills, CA
91302 USA
enterprise@spirentcom.com
www.spirentcom.com/enterprise

SPIRENT™ Communications

Analyze | Assure | Accelerate™



Security Testing Before: many testing solutions require racks of workstations and PCs to simulate client requests, as well as numerous servers to emulate Web server clusters.

Security Testing Solutions.

Spirent Communications offers a comprehensive line of products for testing the performance and capacity of security devices, including solutions for testing IDS/IPS devices, firewalls, VPN concentrators, and SSL accelerators. The Spirent Communications security testing solutions include:

- **Avalanche and Reflector:** Avalanche™ and Reflector™ load testing appliances offer stress-testing solutions for security devices such as firewalls, IPSec VPN concentrators, SSL accelerators, and other devices across the network.
- **ThreatEx:** Exposes devices and networks to actual threats in a controlled test lab environment to assess their defensive capabilities.

Spirent security testing appliances are compact, rack-mountable systems that combine hardware and software to replace racks of traditional PCs and servers. Network emulation testing saves money and space, and frees your IT staff from time-consuming hardware and software management tasks.

Spirent security solutions deliver a proactive testing approach that's designed to detect potential problems before new devices or software upgrades are deployed. This helps streamline deployments and prevent downtime, and also helps maintain optimum performance after the systems are online.

Testing security equipment and devices with the Spirent security solutions enable enterprises to:

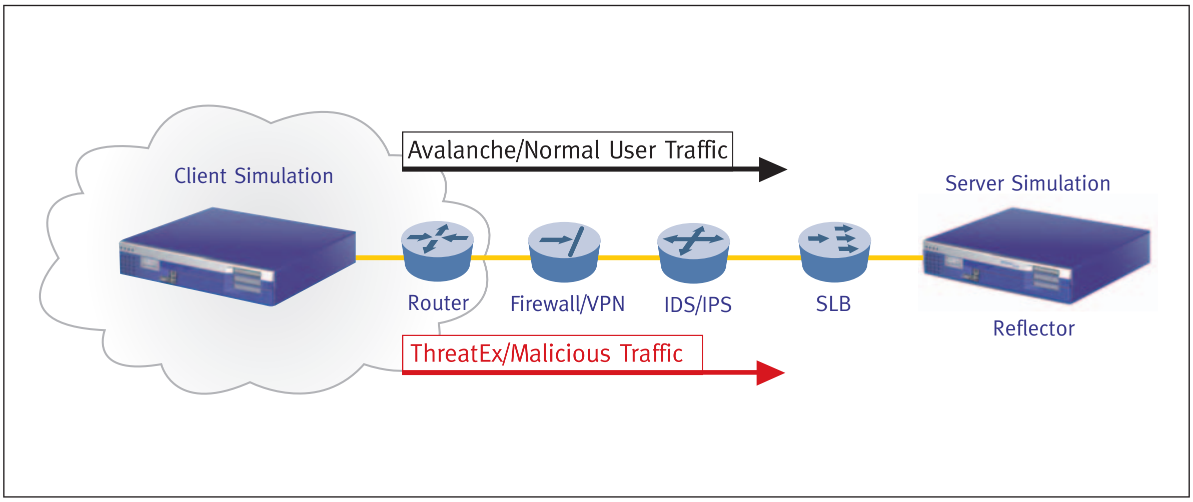
- **Reduce risk:** Significantly reduces the risk of performance hits and security breaches due to the failure of new security devices and software upgrades.
- **Increase security:** Identify vulnerabilities that are only visible under heavy loads, and ensure that your IDS/IPS systems are capable of defending the network infrastructure against the latest attacks.
- **Save money:** Determine how much infrastructure you really need to withstand real-world loads and ensure your enterprise's security, and avoid oversizing your infrastructure by purchasing too much equipment.

Avalanche and Reflector.

Avalanche and Reflector offer a comprehensive solution for stress-testing security devices such as firewalls, intrusion detection systems and SSL accelerators. Avalanche is capable of simulating an almost unlimited number of users, while Reflector emulates the behavior of large Web, application, and data server environments.

By using Avalanche to accurately simulate Web traffic and Reflector to simulate different server-side behaviors, you can quickly and easily test to capacity any security equipment you connect between the two systems. This proactive testing approach ensures that network devices will excel under real-world conditions when they are installed in your network.

The powerful combination of Avalanche and Reflector enables you to emulate realistic and diverse environments within the confines of your lab. This highly realistic testing approach enables you to find and fix security problems proactively, instead of after the network has been deployed, disrupted, or compromised.



Security testing with malicious traffic: Avalanche and ThreatEx provide a mixture of normal and malicious traffic, realistically emulating the input traffic of a network under attack. This allows you to replace racks of workstations and servers with rack-mountable, easy-to-manage appliances.

Next-Generation VPN Security.

Ensuring confidentiality, authentication, and data integrity when extending communications across public infrastructures — such as the Internet — is a difficult task. As organizations deploy VPNs that use IP Security (IPSec) and SSL VPNs to create secure tunnels across the public Internet, a very real performance burden is placed on the network.

Avalanche delivers a next-generation IPSec-based solution that offers highly-realistic emulated user activity and application simulation. This approach supports a complete range of intranet, extranet and remote access VPN configurations for both IPv4- and IPv6-based networks.

Designed to meet the complex requirements of today's security testing, the Avalanche IPSec implementation offers the broadest possible set of features. These include full Layer 4-7 stateful application protocol support, multi-vendor VPN client emulation, digital certificates, and the latest encryption algorithms. SSL VPN-encrypted sessions, including the generation and receipt of validated certificates, can also be simulated.

Application Realism.

Broad-based protocol support enables you to accurately test performance-sensitive network activities such as e-commerce, mail, streaming media, video-on-demand, file transfer, and next-generation IP. Avalanche generates highly-realistic Web traffic, emulating almost any user activity, and delivers a wide range of testing capabilities to any IP environment.

- **Capture-Replay:** Enables industry-standard packet capture (PCAP) files to be used as the source of TCP or UDP traffic that will be used to stress-test your devices and applications to maximum performance.
- **Network latency, packet loss and fragmentation:** Emulates latencies that are typical of asymmetric broadband connections. Packet loss and fragmentation can also be simulated.
- **TCP/IP stack characteristics:** Enables devices or networks to be fine-tuned by emulating different types of TCP behavior.
- **Protocol support:** Avalanche supports all major protocols, including HTTP 1.0/1.1, HTTPS, FTP, streaming media, IPv6, VoIP (SIP), mail (SMTP/POP3), DNS, Telnet, 802.1Q VLAN tagging, IPSec, and PPPoE.

Triple Play/IP Telephony (SIP) Testing.

Avalanche and Reflector are currently the only testing devices on the market that can generate voice, video, and data traffic from a single port using a single GUI. The *de facto* standard for Layer 4-7 triple-play testing, Avalanche features fully-integrated traffic testing and state-of-the-art reporting capabilities. In addition, Avalanche Analyzer is the only reporting tool available that delivers a single, integrated reporting view of triple-play traffic behavior.

Simulate a Virtually Unlimited Number of Users.

Avalanche can simulate up to 2 million concurrent connections, each appearing to come from a different IP address, at rates that can exceed 2 Gbps. Avalanche can also generate in excess of 45,000 HTTP requests per second and 30,000 streaming media requests. This allows realistic and accurate capacity assessment of security devices under heavy load, helping you expose hidden vulnerabilities.

ThreatEx.

A complementary solution to the Avalanche load-testing appliance, ThreatEx is a next-generation vulnerability testing solution. ThreatEx enables IT personnel to assess network defenses by directing threat-based traffic at devices and networks under controlled lab conditions.

In today's malicious computing environment, it's not enough to simply determine capacity thresholds for benign traffic. To protect the network against DDoS attacks, worms, and other malware, the effect of corrupt traffic and other network impairments must be measured and analyzed.

With new threats appearing almost every day, it's important to have a defensive partner helping you to protect your network. In addition to the ThreatEx device itself, there are three key components to the ThreatEx security solution:

- **ThreatEx Knowledge Base** offers a library of threat definitions that can be run on the ThreatEx platform for vulnerability testing. This subscription service provides zero-day access to the latest threats, ensuring that security testing can take place as soon as new threats are detected.
- **ThreatEx ThreatWalker** streamlines and automates the testing process by delivering a complete TCL scripting environment. Devices or networks can be tested using either a subset of, or all available, exploits. Test plans can be easily developed for Windows, Linux, or Sun environments.
- **ThreatEx Designer** enables in-house QA or IT staff to create or reproduce threats without hours of tedious programming. The intuitive user interface enables threats and exploits to be developed by simply describing them. The process of creating variations of a threat is streamlined, and threat files can either be executed by the appliance or stored in a database.

Automated Testing Solutions.

An integral component of the Avalanche solution, WorkSuite Manager (WSM) is an automated testing suite featuring an intuitive user interface. WSM can be used to execute a series of tests in a user-specified order while applying validation rules to each test. Alternatively, WSM can run a single test until a specific performance threshold has been defined. In addition, TCL-based scripting enables users to bypass the graphical user interface to develop, store, and reuse test bench configurations.

Spirent Global Services.

Spirent Communications understands that internal resources for managing testing programs may not always be available. Spirent Global Services supplement internal capabilities with test methodology expertise so that you can focus on your core business objectives. Our experienced engineers enable your business to quickly implement field-proven solutions, instead of expending the time and resources to develop them in-house.

Whether you are facing challenges in deploying mission-critical technologies, solving integration issues among devices from multiple vendors, or assessing network performance, Spirent can help. Currently assisting a wide range of enterprise companies, equipment manufacturers, government entities, and service providers, Spirent Global Services is focused on deploying testing solutions that lead to success.

To assist with the deployment of the new ThreatEx technology, Global Services provides turnkey support for deploying the Spirent ThreatEx solution. The comprehensive program manages all facets of installing and integrating the ThreatEx appliance into your test bed. Our experts ensure that your solution is properly configured, and can also provide training on an as-needed basis for your lab staff.

About Spirent Communications.

Spirent Communications is a worldwide provider of integrated performance analysis and service assurance systems for next-generation network technologies. The Spirent solutions accelerate the profitable development and deployment of network equipment and services by emulating real-world conditions in the lab and assuring end-to-end performance of large-scale networks.

Spirent Communications
26750 Agoura Road
Calabasas Hills, CA
91302 USA
e: enterprise@spirentcom.com

Sales Contacts
North America:
+1-800-927-2660
Europe,
Middle East, Africa:
+33-1-6137-2250
Asia Pacific:
+852-2166-8382
All Other Regions:
+1-818-676-2683

Spirent Federal:
714-692-6565
www.spirentfederal.com

www.spirentcom.com/enterprise

SPIRENT Communications

06/05