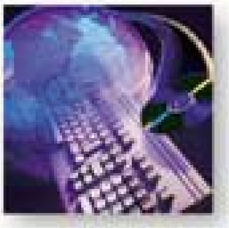

Firewall Module

WebSuite™

Product Overview

Network security devices such as firewalls and intrusion detection systems can be set up to keep distrusted users out of networks, counteract DDoS (Distributed Denial of Service) attacks, and detect reconnaissance tools used by hackers. However, these security devices are often a bottleneck in a network because of the burden placed on them to actively monitor all incoming and outgoing traffic along network boundaries. Qualifying the performance of these devices requires exposure to a high volume of traffic to model peak network conditions. Such conditions can be difficult to generate when using standard PCs. In addition, stateful security devices that may be configured with many application-specific rules, require mixtures of real L4-L7 traffic to forward or block traffic properly.

WebSuite Firewall is designed to test network security devices by simulating real-world web traffic loads. The software can generate millions of user transactions to assess total capacity, isolate potential throughput bottlenecks, and determine performance degradation in complex network security infrastructures.

Security equipment manufacturers can use WebSuite Firewall to validate and tune the algorithms within security devices that are used to detect and take various actions on attacks. Service providers and corporations can use WebSuite Firewall to determine how performance is impacted when these algorithms are active in security devices. Application throughput, connection capacity, session processing, latency, and loss can be measured to allow network planners to provision according to unique end-user requirements.

Websuite Firewall Applications

WebSuite Firewall is specifically designed to:

- Determine performance as multiple packet filtering rules are set up in a firewall.
- Gauge the performance of a firewall performing NAT (Network Address Translation) in both directions.
- Determine maximum application session capacity and processing power.
- Measure HTTP application throughput (goodput).
- Evaluate a firewall's ability to deal with DDoS (Distributed Denial of Service) attacks.
- Evaluate the ability for intrusion detection systems to detect common port-scans including stealth scans (TCP-RST, TCP-FIN) that are more difficult to detect.

Key Features

- Generate thousands of HTTP transactions per second, per port.
- Set up millions of concurrent TCP connections.
- Scale the test bed to hundreds of ports, without affecting system-level performance.
- Use real TCP sessions to gauge application throughput.
- Use traffic wizard to quickly set up TCP/HTTP sessions.
- Simulate various DDoS attacks and port-scans.
- Configure HTTP headers such as URL (Uniform Resource Locator) and cookie.
- Use VLAN tags on a per client and server basis for L4-L7 traffic and for L3 UDP traffic.
- Set up UDP background traffic and retrieve SmartMetrics™ test results.
- View measurements per session, per port, or for the whole system.
- View detailed IP, TCP, and HTTP counters and results.
- View measurements under user-controllable variable conditions, showing the full spectrum of performance characteristics of the device under varying loads.
- Validate concurrent connection capacities using verification options.
- Supports SAI (Scripting Automation Interface) on Windows®, Linux™, and UNIX™ platforms using Tcl, C/C++, and Visual Basic interfaces.

Test Descriptions

Concurrent Connection Capacity

This test sets up a configurable amount of connections at a fixed rate. By varying the number of connections used in multiple iterations, the test measures the maximum number of concurrent connections that the device or system under test can sustain. A full user session can be configured, including an HTTP transfer and TCP close.

Maximum Session Rate

This test performs TCP connection setups, followed by teardowns, for a configurable amount of connections at a specified rate. The test measures the peak rate at which a DUT can handle the setup and teardown of TCP connections over time.

Maximum Connection Rate

This test measures peak connection rates that can be sustained by the device or system under test over time. After each connection is established, an HTTP transaction takes place between client and server.

The average number of connections established in configurable time intervals is reported. All of the tests described above also provide the average time to establish and tear down TCP sessions.

Spirent Communications
27349 Agoura Road
Calabasas Hills, CA
91301 USA
E-mail: productinfo
@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

www.spirentcom.com

SPIRENT™ Communications

Analyze | Assure | Accelerate™

Denial of Service Handling

This test allows you to set up different ratios of attack traffic to be generated in parallel with other application traffic. This permits benchmarking of legal traffic performance while attack traffic is being directed at the device under test, consuming its resources.

Goodput

Packet loss in a DUT/SUT causes retransmissions at the TCP level and affects the transfer time that an end-user observes. This test measures goodput by dividing the object size transferred between two hosts by the amount of time it takes to receive all of the data. This is a TCP throughput test, so retransmissions are not counted as additional transferred data and will negatively impact the measurement since additional time will be needed to transfer the data.

Extended Duration

This test is designed to measure the performance and stability of the DUT/SUT over a long period of time by sending L4-L7 traffic continuously for up to a week. Results are retrieved after a specified duration.

Mixed Traffic

This test combines many traffic types, enabling you to perform capacity assessment and to analyze session-based metrics in the same test. Full TCP sessions and TCP Connection/HTTP traffic can run as L4-L7 traffic in the same test. UDP and attack traffic can be included as background in the test. By combining the HTTP traffic type with either attack traffic or UDP traffic, you can determine the effect that the presence of attack traffic and UDP traffic load have on the DUT/SUT's performance.

Traffic Types

TCP Connection/HTTP

This traffic uses a partial TCP engine to set up connections at a high rate and to simulate short, bursty HTTP 1.0 transactions.

HTTP Goodput

The HTTP traffic is passed down to a real TCP test stack with the ability to send large data objects across the sessions to determine the application throughput (goodput). The acknowledgement/retransmission architecture of TCP, as well as algorithms like slow start/congestion avoidance, are fully implemented and allow for an end-user perspective of data flow.

UDP

UDP flows can be set up to determine the performance characteristics of a DUT/SUT when exposed to various frame sizes, or to establish a level of background traffic. Available SmartMetrics results include Frame Loss, Latency Distribution, Latency over Time, and Jumbo.

DDoS Attacks and Port-Scans

DDoS Attacks: Simulate malicious Internet attacks and evaluate the DUT/SUT's ability to filter this traffic. Supported attacks include:

- SYN Flood
- Ping of Death, Ping Sweep, Ping Flood
- Smurf
- Teardrop
- Land-Based
- ARP Attack
- Jolt2 Attack
- UDP Flood

Port-Scans: Port-scans are popular reconnaissance tools used by hackers to discover active services that can be used to gain access into a network or device. Supported port-scans include:

- UDP Scan
- TCP-SYN Scan
- TCP-ACK Scan
- TCP SYN-ACK Scan
- TCP-FIN Scan
- X-mas Tree Scan
- TCP-RST Scan

Supported Modules

Module	Description
LAN-3101A/B	10/100Base-TX Ethernet, 6-port, SmartMetrics module
LAN-3102A	10/100Base-TX Ethernet, 2-port, SmartMetrics module
LAN-3111A	100Base-FX Ethernet, 6-port, multi-mode, 1300nm, SmartMetrics module
LAN-3111As	100Base-FX Ethernet, 6-port, single mode, 1310nm, SmartMetrics module
LAN-3300A	10/100/1000Base-T Ethernet Copper, 2-port, SmartMetrics module
LAN-3301A	10/100/1000Base-T Ethernet Copper, 2-port, TeraMetrics™ module
LAN-3302A	10/100Base-T Ethernet Copper, 2-port, TeraMetrics module
LAN-3310A	1000Base Ethernet, GBIC, 2-port, SmartMetrics module
LAN-3311A	1000Base Ethernet, GBIC, 2-port, TeraMetrics module

Requirements

- An SMB-600 or SMB-6000B chassis with the appropriate modules.
- An IBM or compatible Pentium PC running Windows 2000/NT, with mouse and color monitor.
- Microsoft Excel 97/2000 application for Windows (optional, but highly recommended).

Ordering Information

SWF-1219A

WebSuite Firewall Software Module

SMB-SUS

12-month Software Update Support Service

Spirent Communications
27349 Agoura Road
Calabasas Hills, CA
91301 USA
E-mail: productinfo
@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

www.spirentcom.com