ThreatEx Network Attack Testing Solutions

In today's hostile computing environment, companies are justifiably concerned about suffering attacks from malicious entities. Denial of Service (DDoS), CodeRed II worm, Nimda, SQL Slammer and their endless variants — IT professionals understand that defending against these attacks is a difficult proposition, and that the price of failure is higher than most companies are willing to admit.

Now there's a way to control this dangerous exposure — by using the ThreatEx network attack testing solution from Spirent Communications to conduct realistic attacks on individual devices or whole networks. By running sequences of controlled attacks using exploits from our continuously-updated Knowledge Base, network security can be dramatically increased.

It's not enough to find capacity thresholds for benign traffic. To fully protect the network, the effect of corrupt traffic and other network impairments must be measured and analyzed. A complementary solution to the Spirent Communications Avalanche load testing appliance, ThreatEx is a next-generation solution that provides visibility into essential areas of network security.

Don't face the threat alone.

ThreatEx provides a powerful ally in the ongoing battle to defend your network against malicious traffic. In addition to facilitating vulnerability testing, Spirent offers zero-day response to new threats, and provides updated threat signatures and exploits on our Web site. The ThreatEx solution provides a range of key benefits:

- Provides a proactive threat containment strategy, reducing the risk of suffering costly network downtime
- Closes the window of vulnerability and reduces the need for in-house research by providing threat updates as soon as new outbreaks occur
- Enhances lab-based vulnerability testing by injecting hostile traffic into a highly controlled environment
- Enables IT personnel to confirm vendor claims by assessing network defenses by using negative testing
- Features diagnostic, assessment, and reporting capabilities highlighted by real-time displays

ThreatEx Knowledge Base and Update Service.

To ensure that you are fully protected against the latest threats, Spirent offers a subscription-based threat definition update service for the ThreatEx appliance. Subscribers are able to access the ThreatEx Knowledge Base, a Web-based repository of threat signatures used by the ThreatEx appliance for negative testing.

Spirent threat analysts constantly monitor listservs, service provider Web sites, news groups, and other resources to detect the latest malware outbreaks as soon as they occur. Once a threat has been identified, it is quickly duplicated using ThreatEx Designer and posted to the Knowledge Base. Subscription to this database ensures that your QA and IT staff will have immediate access to the latest threat signatures, delivering zero-day testing capabilities.

Companies are able to close the window of vulnerability by keeping their threat definitions current. Updates are easily accomplished — the ThreatEx appliance synchronizes with the Knowledge Base and automatically downloads all threat signatures added since the last check. ThreatEx Knowledge Base updates can be downloaded at the end of each business day, or pulled down on an as-needed basis.

ThreatEx Designer

ThreatEx Designer enables IT and QA staff to create threats within minutes, without time-intensive programming. The intuitive point-and-click graphical user interface enables threats and exploits to be developed in minutes by simply describing them. The software then generates a small XML-based file for each exploit in our patented TDL (Threat Definition Language) format. Creating multiple variations of basic threats is simplified, with variables such as test attributes and behaviors quickly modified through the ThreatEx GUI. Intermediate XML threat files can be executed directly by the ThreatEx Appliance or stored in a central database.

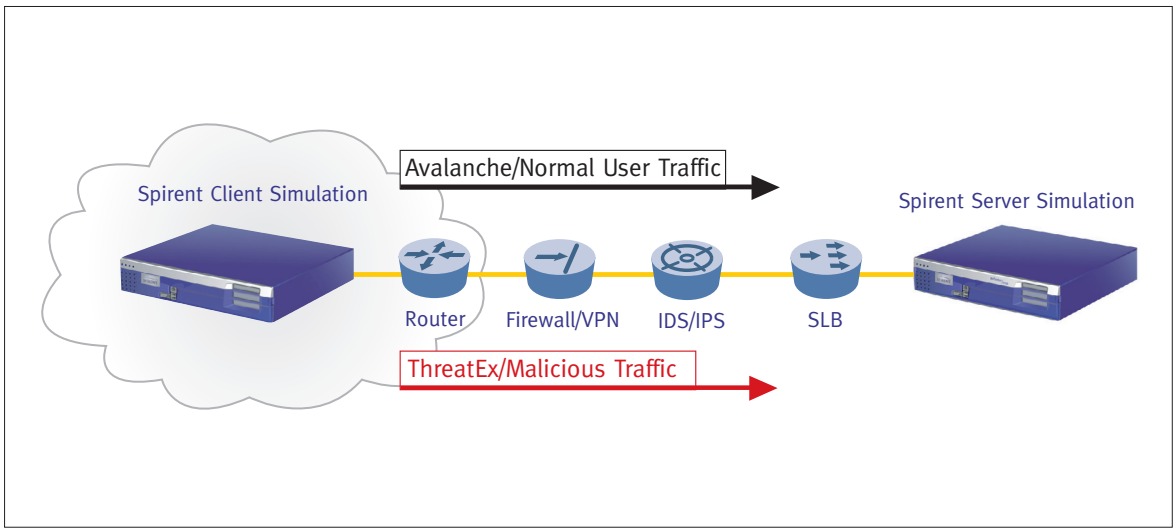
Spirent Communications
26750 Agoura Road
Calabasas Hills, CA
91302 USA
e: enterprise@spirentcom.com

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 *Analyze | Assure | Accelerate™*



Testing with Avalanche and ThreatEx: Enables IT and QA staff to use mixtures of both positive and negative traffic to test the security infrastructure.

Automation

To streamline and automate the testing process, the ThreatEx platform includes ThreatWalker, a complete TCL scripting environment for automating and developing test plans in Windows, Linux, or Sun environments. QA staff can either select an existing test plan, or develop an entire test through the API. This automated approach simplifies the process of re-testing the network each time a new threat is detected.

ThreatWalker enables suites of exploits to be executed sequentially, and can generate TCL scripts based on either pre-defined or user-defined templates. This approach delivers complete vulnerability assessment by testing devices or networks using either a subset of, or all available, exploits. A flexible and upgradeable solution, ThreatWalker can be easily updated with new exploits at the click of a mouse.

Script developers will benefit from ThreatWalker's streamlined approach to creating regression tests for executing exploits sequentially. Developers can configure test parameters, threat parameters, and statistical monitoring techniques through an intuitive GUI, and automatically generate TCL scripts that can be quickly customized using the TCL templates. ThreatWalker includes templates, integrated exploits, test plan attributes, and ready-to-execute threats, and is supported on Linux, Sun, and Windows platforms.

Spirent Global Services

Spirent Communications understands that internal resources for managing complex testing programs may not always be available. Our Global Services engineers enable your business to quickly implement field-proven solutions, instead of expending the time and resources to develop them in-house.

- **ThreatEx Implementation Service.** Spirent can help you manage all facets of installing the ThreatEx solution into your test bed — from site readiness analysis to physical installation and systems configuration. Knowledge transfer services are also available to help your staff perform critical testing tasks without delay.
- **Network Security Assessment.** Experienced engineers from Spirent Global services are available to assist in network vulnerability and performance assessment. Regulatory compliance can be established, and costs can be controlled by right-sizing your network security infrastructure.
- **Engineering Services.** In-house access to ThreatEx product experts can reduce your company's overall risk, and accelerate the delivery of custom functionality. Additional resources translates into quick ramp-up, development, testing, and deployment of customized attacks and protocols.

A Complete Solution.

The ThreatEx appliance delivers a complete vulnerability testing assessment solution that is designed to protect your network from hostile attacks. By selecting ThreatEx your company gains more than access to the market-leading testing platform for malicious attack — you also get a full and active partner that is constantly on the alert for new threats. Don't go it alone – deflect hostile network threats by using the ThreatEx solution.

ThreatEx Designer

Powerful Function Language

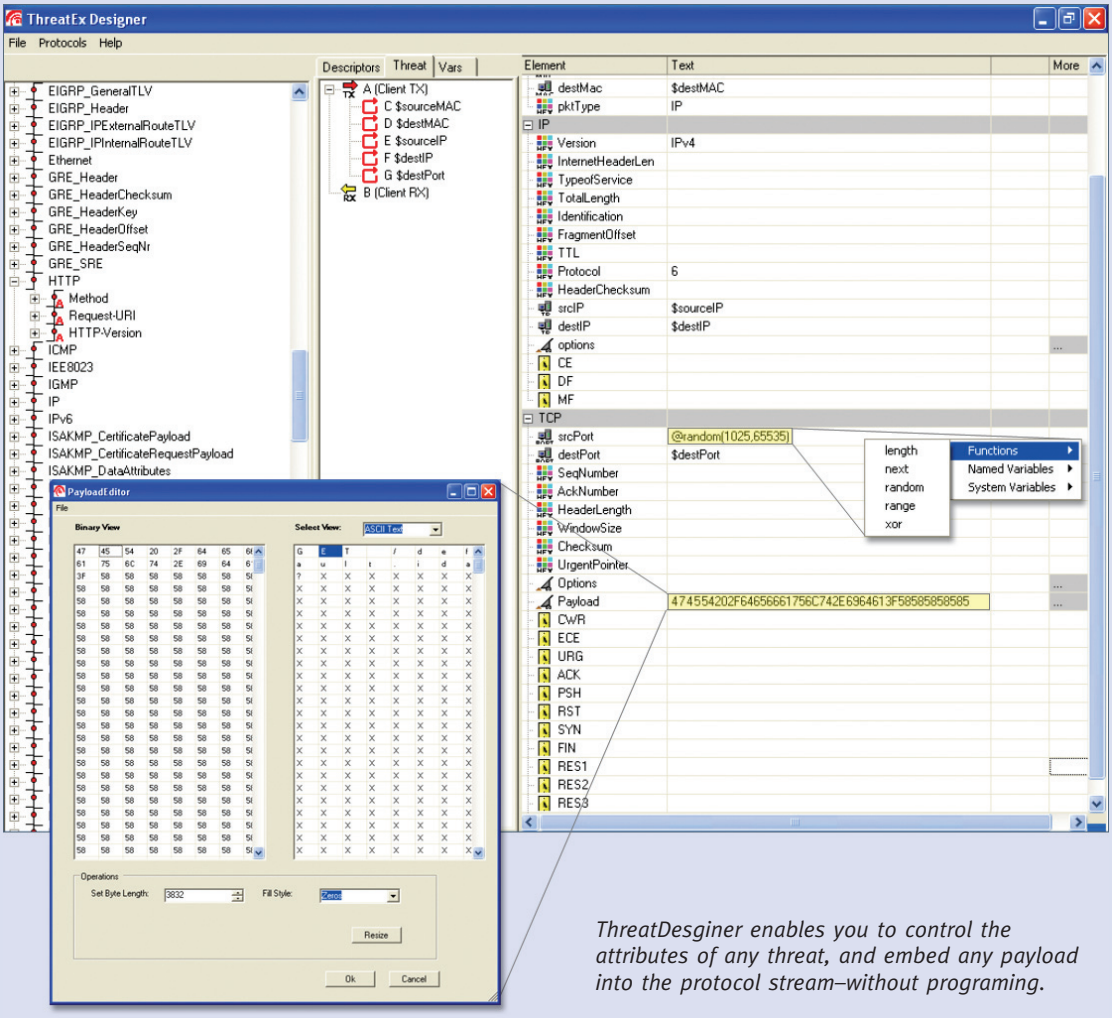
ThreatEx Designer features an extensive function vocabulary that enables users to spoof attribute values, modify payloads, vary threat behaviors, or change other aspects of a threat. By combining network objects with functions and test behaviors such as ramping, throughput, throttling, and diagnostics, an infinite variety of threats can be created — all without programming. QA engineers are able to change specific test variables during the testing process. This approach allows the test environment to be modified in real time, and facilitates the quick, efficient creation of test corner-cases.

File Capture and Replay

ThreatEx Designer enables QA personnel to import a PCAP file and use it to create a new network object (protocol, threat, etc.) The fields and attributes can be modified as needed, creating dynamic traffic from a static capture, and the new object loaded into ThreatEx for testing. Any payload can be associated with the created TCP objects, including DNS, DHCP, or SMTP. Automating the process of creating specific network traffic offers a huge leap in productivity.

Payload Editor

Payloads can be described independently for network objects using XML, enabling a single network object to have multiple payload definitions. Simply define the packet stream using the GUI, and ThreatEx Designer creates the protocol (network object) for you to use and test. A payload value can be provided and discrete portions of it modified through literals, variables, or functions. This approach delivers complete flexibility for protocol definition.



ThreatDesginer enables you to control the attributes of any threat, and embed any payload into the protocol stream–without programing.

	ThreatEx 2500
Physical Specifications	
Integrated Hardware and Software	2U, 19-inch rack-mountable infrastructure stressing appliance
Dimensions	3.485" H x 15.53" W x 19.75" D 8.852 cm H x 39.45 cm W x 50.17 cm D
Weight	22 lbs. (10 kg)
Operating Environment	5^0C-40^0C
Non-Operating Environment	0^0C-50^0C
Relative Humidity	10-90%, non-condensing
Power Requirements	115-230 V, 50/60 Hz
Maximum Power Consumption	460 W
Interfaces	Spirent ThreatEx is available in two configurations: Configuration 1: ▪ Three 10/100/1000 test ports (copper) with RJ-45 connectors ▪ One 10/100 management port (copper) with RJ-45 connector Configuration 2: ▪ Three 1 Gbps multimode fiber ports test ports with SC connectors ▪ One 10/100 management port (copper) with RJ-45 connector
Regulatory Approvals	FCC Class A, CE, UL-1950, GS Mark

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