CMP
United Business Media

Network Computing
Driving IT Decisions

August 5, 2002
www.networkcomputing.com

SNEAK PREVIEW

IMPROVEMENTS TIGHTEN LUCENT'S SECURITY MANAGEMENT SERVER

BY MIKE FRATTO

Last year NETWORK COMPUTING proclaimed Lucent Technologies' Lucent Brick 1000 and Lucent Security Management Server 6.0 "hotter than a Haitian sunset" (see *www.nwc.com/ 1219/1219sp1.html*). Now we're advising you to keep a look out for the September release of LSMS 7.0, which is replete with QoS support, DHCP Relay and Brick DHCP client support, HTTP application filtering, robust TCP protocol inspection, and other new features. Designed to bring tighter filtering and integration to a network, LSMS 7.0 also includes new software for Lucent's Brick firewalls. I tested a beta version in our Syracuse University Real-World Labs® and was impressed.

For my tests, I used a Brick Model 300 with seven 10/100 Fast Ethernet interfaces. I assigned three interfaces to the public and private zones and I configured the zones with IP addresses in separate subnets, which forced the Brick to route traffic. To generate HTTP traffic, I used Caw Networks' WebAvalanche 1800 (see *www.nwc.com/1309/1309sp1.html* for more on WebAvalanche) and WebReflector to simulate Web users and Web servers. I created a transaction



WITH LSMS 7.0, LUCENT HAS ADDRESSED MANY OF THE PROBLEMS WE FOUND IN PREVIOUS VERSIONS.

using an HTTP 1.1 connection to grab a 5,800-byte file. I ran each test for more than an hour to generate 20 million sessions, and, though I didn't run exhaustive performance testing, the system generated more than 8,000 transactions per second before overrunning the 300 Mbps offered by the three private Fast Ethernet interfaces.

PACKET HANDLING

Although I'm reluctant to use the cliché that Lucent eats its own dog food, I do have it on good authority that at least one Lucent SE does eat his own cat food. That said, Greg Shipley and the crew at security consultancy Neohapsis discovered a few problems with how the Bricks running 6.0 code handled TCP state inspection in our last firewall review (see *www.nwc.com/ 1223/1223f2.html*). Lucent has addressed those issues *and* has added other TCP-level features, including sequence-number randomization, which strengthens the servers with predictable initial sequence-number generation. LSMS 7.0 also brings support for T/TCP and allows experimental TCP options.

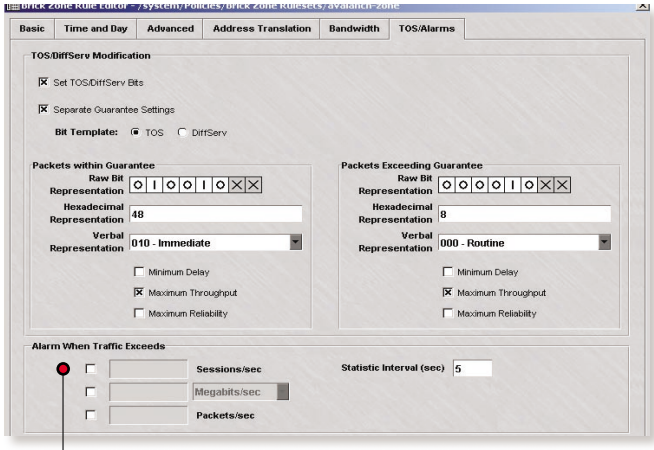
GOOD NEWS

- TCP STATE CHECKING AND TCP ISN RANDOMIZATION.
- HIGHLY CONFIGURABLE QOS AND BANDWIDTH MANAGEMENT.
- CLI ON BOTH LSMS 7.0 AND BRICK.

BAD NEWS

- NO WAY TO GET TO A CLI OTHER THAN THROUGH LSMS OR SERIAL/MODEM CONNECTIONS.
- APPLICATION-FILTERING CONFIGURATION IS LIMITED.
- HTTP APPLICATION FILTERING DOES NOT CHECK SYNTAX.

The advanced options, applied per rule in a security zone, let you tailor the level of inspection to your needs.



THE RULE EDITOR LETS YOU TAG TRAFFIC DEPENDING ON TRAFFIC LEVELS. IN ADDITION, ALARMS CAN BE SET IF TRAFFIC LEVELS EXCEED THRESHOLDS.

I tested the new features by placing a laptop running Wild Packets' EtherPeek NX protocol analyzer on a shared segment next to the Web servers and inspecting the TCP packets off the wire. I also used EtherPeek NX on the client side to capture and inject modified TCP packets into the stream. LSMS 7.0 passed the tests the earlier version had failed in the aforementioned firewall review. I also confirmed that LSMS 7.0 modified TCP initial-sequence numbers on the fly by comparing packets' ISNs on either side of the firewall with EtherPeek NX.

Although still rudimentary, the HTTP application filters set limits on the length of a URL—4,096 characters by default—performs pattern matching on URL strings and blocks directory traversal beyond the directory root via "../.."-style strings. Unfortunately the application filter doesn't check HTTP syntax. I tested the URL length matching by using eEye Digital Security's IISHack buffer overflow exploit against a protected Web server. The Brick successfully caught the long URL and killed the connection by sending TCP resets to both the client and the host. I also tested directory traversal, which on older or misconfigured Web servers lets attackers break out of the Web root and access any file to which the Web server has access rights, using ASCII "../.." and the UniCode string "..%C0%AF.." both of which were blocked. Although my tests weren't exhaustive, many canned attacks scripts can be blocked.

INTEGRATION SUPPORT

Bandwidth management is available at the interface and rule levels via traffic shaping and QoS tagging using DiffServ (Differentiated Services) and ToS (Type of Service). Rule-level bandwidth management takes precedence over interface level. Aggregate bandwidth minimum/maximum bandwidth guarantees a limit on the amount of data passing through an interface or zone, and limits can be placed on the number of simultaneous sessions into and out of the zone as well. Packets can be tagged with new DiffServ/ ToS settings as they pass through the Brick. Packets that exceed the maximum bandwidth are queued up and can be tagged with different DiffServ/ToS bits.

I tested bandwidth management by setting maximum bandwidth on each interface and then monitoring the traffic flowing through the Brick. Testing QoS tagging was simpler. I configured tagging on each zone and monitored the traffic passing through to verify the tags were set properly. In both cases, bandwidth management worked as advertised and did not hurt performance.

LSMS 7.0 also supports DHCP Relay and dynamic IP address assignment via DHCP. Both applications are welcome additions. The DHCP client works as expected. When the Brick boots up, it sends out a DHCP address request and configures its IP network according to the response it receives. Then the Brick contacts the LSMS with its new address.

Missing from the Brick in previous versions was a command-line interface. LSMS 7.0 brings a CLI to the Brick and makes it available through the LSMS GUI or via a console cable. The CLI has a full set of tools that, when all else fails, can get you on the road to troubleshooting. However, there aren't any configuration options on the Brick except to set up the serial port and a modem.

LSMS has a CLI as well with a subset of the configuration commands available. The LSMS CLI lets administrators restore archived Brick configurations and offers utilities to modify the LSMS configuration. In addition to utilities that list configurations for Bricks and rule sets, you can add zone rule sets to existing groups and apply zone rule sets to Bricks. Although there is little reason to use the LSMS CLI, it is handy if the management GUI is unavailable.

Lucent has responded to user needs with gusto, and at this price, LSMS 7.0 is an option for any business.

LUCENT HAS RESPONDED TO USER NEEDS WITH GUSTO, AND AT THIS PRICE, LSMS 7.0 IS AN OPTION FOR ANY BUSINESS.

Mike Fratto is a senior technology editor based in NETWORK COMPUTING's Syracuse University Real-World Labs®; he covers all security-related topics. Prior to joining this magazine, Mike worked as an independent consultant in central New York. Send your comments on this article to him at mfratto@nwc.com.

VENDOR INFORMATION

■ LUCENT SECURITY MANAGEMENT SERVER 7.0, starts at $6,000. Available: September. Lucent Technologies, (888) 4LUCENT, (908) 582-8500. *www.lucent.com/security*

Lucent Technologies
Bell Labs Innovations



Copyright© 2002 by **CMP Media LLC,** 600 Community Drive, Manhasset, NY 11030. Reprinted from NETWORK COMPUTING with permission.