



Contact:  
Kevin Gallagher  
Gallagher Group Communications  
925.831-1041  
[kevin@gg-comm.com](mailto:kevin@gg-comm.com)

## **MU HELPS ELIMINATE SERVICE, APPLICATION AND NETWORK DOWNTIME WITH ADDITION OF DENIAL OF SERVICE CAPABILITY**

New DoS Module Offers Strategic Enhancement to Mu's Existing Proactive Service Assurance Solution

**Sunnyvale, Calif. – May 19, 2008** – Mu Dynamics, a pioneer in helping network operators and their vendors eliminate downtime through proactive service assurance, today announced a breakthrough [Denial of Service \(DoS\) Module for the Mu-4000 appliance](#). This new Mu solution ensures service providers can proactively identify and eliminate service, application and network downtime caused by DoS and Distributed DoS attacks. Studies from Network Strategy Partners (NSP) and others put the cost of downtime for a large service provider network in excess of \$100,000 per hour. (See [The Business Case and Return on Investment for Deploying the Mu-4000 Security Analysis Platform.](#))

This latest enhancement enables Mu to deliver additional proactive service assurance options that result in a high return on investment for network operators and equipment vendors. The ability to minimize service/network downtime accelerates the rollout of new and more robust services, thereby increasing end-user satisfaction and reducing customer churn. (Editor's note: Please see separate announcement *Mu Dynamics (Formerly Mu Security) Receives \$10 Million Series C Financing Round to Expand Go To Market Efforts and Capitalize on Business Momentum.*)

"The proactive service assurance provided by Mu is cost-justified in a single release cycle," says Ir. Bilpen Nainggolan, senior manager research & development of network management at Telkom RDC Indonesia. "Our voice, video and data service customers count on Telkom RDC Indonesia to quickly roll out new and enhanced IP-based services that are always available and highly resilient. The inherent and growing complexity of VoIP

and IPTV services makes it increasingly important to ensure high availability and security. For Telkom RDC Indonesia, Mu's unique solution is essential for reliably provisioning new services more rapidly and with greater confidence to build customer satisfaction."

"Our customers require high-performance security products to be highly resistant to either inadvertent or malicious DoS weaknesses," said Michael Frendo, senior vice president, high-end security systems, Juniper Networks. "Mu helps our product development teams to ensure that customer's services using Juniper-based infrastructure are fast, reliable and secure—ultimately reducing costly application downtime."

### ***Denial of Service Module Enhances Prevention of Unexpected Service Weaknesses***

Mu's new DoS Module for the [Mu-4000 system](#) helps service providers, equipment vendors and enterprise IT departments assess their exposure to poorly "hardened" networked services and systems that could become unreachable or unusable under unintentional or malicious DoS attacks. The Module is pre-loaded with more than 40 customizable Extensible Mark-up Language (XML) templates including "Slammer Worm," "SIP Invite/Register," and "OSPF Hello" to model any networked application, product or service for known DoS and Distributed (DDoS) attacks. The Mu module also exposes the underlying software weaknesses or flaws that make networked applications subject to new forms of attack.

Unlike other solutions, users can customize Layer 2-4 protocols and application-level services being targeted, as well as the packet payloads, and the attack rate and patterns. The DoS Module also automatically alters certain fields, such as source and destination ports and addresses, and performs other randomizations to ensure tests are as rigorous as possible. The solution uniquely allows any service of interest to be independently monitored while the system is concurrently stressed with D/DoS attacks. For example, the impact on an independent service like HTTP can be monitored while a server on a network is being attacked with a SIP Invite/Register Flood. The automation elements throughout the Mu solution constantly monitors and records system behavior during the test to produce repeatable, actionable results that can be used to remediate any weaknesses discovered.

"The new DoS Module enhances Mu's ability to eliminate network and service downtime, and sets a new proactive standard for the industry," says Jessy Cavazos, industry manager, test & measurement at Frost & Sullivan. "The expanded breadth and depth of Mu's service assurance solution helps service providers and their vendors deliver a more comprehensive and systematic way to eliminate very costly service downtime. IP services like VoIP and

IPTV are inherently more fragile due to the complex interdependencies among the software and product. The Mu solution enables customers to identify potential weaknesses within these interdependencies and address them before the service goes live.”

The platform for the DoS Module, the Mu-4000 appliance, already leads the industry as the premiere choice for proactive service assurance with [more than 100 deployments worldwide](#). The majority of these deployments are with global service providers and their strategic vendors.

“Helping network operators reduce their costly downtime problem, maximize service revenue and ultimately bolstering their customer satisfaction is Mu’s number one priority,” says Dave Kresse, CEO of Mu Dynamics. “The addition of the new DoS Module helps improve customer satisfaction by enabling network operators to proactively understand where their services can be negatively impacted by DoS and DDoS attacks. We expect that many of our existing 100-plus deployments globally will add the DoS Module to their current configurations, and that many new customers will purchase Mu’s proactive service assurance solution based solely on its breakthrough capabilities.

### **About Mu Dynamics**

Mu Dynamics proactively eliminates the high cost of service, application and network downtime. Mu’s solution automates a systematic and repeatable process that identifies hard-to-detect sources of potential downtime within IP services, applications, and underlying networks. The award-winning Mu solution is deployed at more than 100 locations, primarily at leading global service providers, cable operators and network product vendors. Headquartered in Sunnyvale, California, Mu is backed by leading venture capital firms that include Accel Partners, Benchmark Capital, DAG Ventures and Focus Ventures.

###

### **Trademark Information:**

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.