

Denial of Service (DoS) Analysis Module

Helping Network Operators to Prevent Service Outage

EXECUTIVE SUMMARY

With rising diversity and complexity, next-generation services including VoIP, IPTV and IMS-based applications, are getting more fragile and thus vulnerable to attack from entities on the Internet. One type of attack, Denial of Service (DoS), is of particular concern to many network operators due to its extremely disruptive and fast-propagating nature.

To prevent costly service outage, the most effective way to survive DoS attacks is to proactively and continuously harden networked products and services against the attacks by planning for the unexpected. Mu's DoS module, as part of Mu's Proactive Service Assurance solution, helps network operators and their suppliers identify and address underlying weaknesses in the network before damage is done.

What is DoS Analysis?

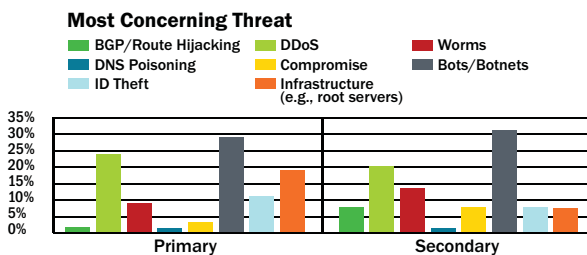
Historically, network operators lacked effective tools to help them methodically avoid DoS attacks against their networks, or understand service-level scaling limits within their network infrastructures. Mu's DoS module allows any network owner or developer to proactively discover service-level DoS weaknesses by modeling real-world traffic targeted both at the network products and application services, and observing the impacts on the rest of the system.

DoS Analysis provides insights into the reliability, availability, and security of the service in the face of either malicious DoS attacks or extreme amounts of valid service-level traffic. This analysis module arms network operators with actionable information to prevent the damaging effects of these attacks. The DoS module is one of Mu's four analysis software "blades" or modules tightly integrated with the award-winning Mu-4000 Service Assurance Platform.

How Does DoS Analysis Benefit me?

Even within time-tested VoIP applications and other successful real-time product deployments, e.g., routing, there are still active attacks emerging against newly discovered or exploited weaknesses in the protocols on which these services depend. In contrast, next-generation triple-play and quad-play IP network services, such as IPTV and IMS-based applications, often lack the benefit of years of punishing real-world exposure. Additionally, these latency-sensitive services are highly interconnected and consist of many interdependent subsystems involving multiple technologies sourced from multiple vendors. Software weaknesses in any component may result in a domino effect, affecting the reliability, availability and security of the entire system, and leading up to costly service downtime.

To ensure uninterrupted revenue streams, it is in the network operator's best interest to find and eliminate weaknesses before outage or customer service impairment is experienced. Mu's solution takes a distinct approach of proactively discovering and documenting application issues including buffer overflows, resource exhaustion, DoS exposures, CPU spikes, etc. By quickly removing these problems, Mu helps maximize network uptime, and minimize costly service disruptions and customer churn.



Source: Arbor Worldwide Infrastructure Security Report

WHY DoS?

DoS attacks have been very damaging historically:

- The economic cost of the downtime from the original Code Red worm and its more malicious cousin, Code Red II, exceeds US\$2 billion
- The Slammer worm infected about 75,000 hosts in the first 10 minutes and knocked several ISPs around the world offline for extended periods of time, causing major congestion of Internet traffic worldwide

And they continue to wreak havoc:

- New DoS attacks appear constantly, many are derivatives of existing attacks
- There are even detailed step-by-step instructions for manually constructing distributed DoS (DDoS), making it easy for people/organizations with malicious intents to launch attacks

How Does DoS Analysis Work?

Network operators and vendors lack effective tools to ensure the reliability of networked systems when subjected to unexpected quantities of valid or invalid network traffic. Mu's DoS module takes the guess work out of the process by using a systematic and repeatable testing methodology. Mu enables users to realistically model DoS situations, automatically monitors and measures the target system, correlating undesirable impacts with input traffic levels, and presents actionable data for DoS prevention and capacity planning.

An example below, where TCP SYN Flood is run against the HTTP Management Interface, illustrates how Mu's DoS module works.

DoS Testing Made Easy

Step 1. Model DoS Conditions

Users can now easily emulate and apply the effects of worms, botnets, amplification attacks, etc., in a controlled environment:

- Realistically model DoS traffic, targeted both at the infrastructure and at the application
- Randomize certain fields (e.g., the source address and/or source port) to emulate traffic coming from multiple senders (e.g., a botnet)
- Share new DoS templates as a best practice



Figure-1. Intuitive GUI helps users customize the type, pattern, rate and duration of a simulated DoS attack via simple XML templates.

Step 2. Measure Impact on Services

Mu helps users to:

- Monitor and visualize in real time the effect of DoS attacks on critical business services
- Gather detailed metrics on outages as well as recovery time
- Correlate application "health check" with DoS attacks. For example, users can measure the impact on DHCP services while attacking the Management Interface with an HTTP SYN Flood



Figure-2. In this simulated DoS attack, DHCP is initially unaffected at lower pps rate. At higher rates, the DHCP server becomes unavailable. At the highest rates, the DHCP server is effectively DOWN.

Step 3. Analyze Data

Mu helps users to:

- Gain actionable insights for resource and capacity planning
- Build a Product Deployment or Software Development Lifecycle (SDLC) plan to minimize DoS exposure
- Work with the vendors and developers on mitigation strategy



Figure-3. Interactive charts and reports enable users to visualize the negative impact on system response time and service availability under a DoS attack.

CUSTOMER USE CASE

A Tier 1 network operator pilots High Def TV service via IPTV to consumers in several cities in the US. The operator understands first-hand that losing even a SINGLE packet of IP-encapsulated high-def video results in visibly degraded video quality, impacting customer satisfaction. Denial-of-service or DoS is of particular concern for this provider. The requirement for the highest real-time content delivery makes the HD video delivery infrastructure more susceptible to both unintentional and malicious DoS.

The network operator now uses Mu's service assurance solution including DoS and Service Level Traffic Variations for proactive IPTV pre-deployment analysis. Mu's DoS module helps operations teams simulate a wide variety of both known and customized distributed denial of service attacks, worms, botnets, and amplification attacks in a controlled environment. Configuration of DoS simulation is made

easy and intuitive via simple XML templates. The result is realistic DoS simulations for this network operator to proactively build the reliability of IPTV or any other IP based application or service.

The Mu solution automatically gathers detailed data during the DoS simulation, and provides metrics on expected outages as well as recovery time. This information is critical for operations, network and security administrators during resource and capacity planning of their IPTV networks.

With Mu, the provider now has actionable information to ensure that content delivery network modifications, the additions of new systems and vendor updates meet the required level of availability for IPTV service.



web: www.mudynamics.com | email: info@mudynamics.com
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317