NON-INTRUSIVE DDoS ATTACK DETECTION AND MITIGATION

The joint FlowTraq and Radware solution is an integrated DDoS detection and mitigation solution that enhances out-of-path detection and mitigation coverage against DDoS attacks for enterprises and service provider networks.

The Challenge
As the severity of denial-of-service and distributed denial-of-service (DoS/DDoS) attacks continue to rise each year, so does the business risk for online businesses, financial services, government agencies, public utilities and service providers.

The Solution
FlowTraq and Radware’s out-of-path DDoS detection and mitigation solution protects enterprise applications and data centers against DDoS attacks, Botnets, APT, misbehaving users and zero-day attacks.

Benefits
The joint solution maintains business continuity by detecting and mitigating all type of DDoS attacks in real-time and without blocking legitimate user’s traffic.

Solution Diagram: How It Works
The FlowTraq system collects and analyzes flow data (such as NetFlow, sFlow, IPFIX) produced by the network infrastructure and creates normal traffic baselines. Within seconds of the start of a DDoS attack, FlowTraq sends details of the attack to Radware DefenseFlow, the attack lifecycle management software. DefenseFlow redirects the suspicious traffic using BGP to the DefensePro mitigation device, which starts mitigating the attack in seconds. DefensePro forwards the clean traffic to its designated destination.

In today’s info-security threat landscape, denial-of-service and distributed denial-of-service (DoS/DDoS) attacks are a major cause of network downtime. Whether executed by hacktivists to draw attention to a cause, fraudsters trying to illegally obtain data or funds, or a result of geopolitical events, DDoS attacks are a destructive cyber weapon. Governments, utilities, financial services and commercial institutions face daily attacks. Attacks are becoming more sophisticated and increasing in severity as they bypass traditional cloud and CDN protection services to target an organization’s IT infrastructure and critical applications. The simplicity of launching cyber-attacks and variety of attack tools are reasons why organizations suffer from increased attacks, including DDoS. It is no longer about preventing attacks, but rather how to detect and mitigate them.
Once the attack is over, FlowTraq notifies DefenseFlow, which terminates the traffic rerouting and DefensePro returns to idle mode.

**Solution Benefits**
- Maintain business continuity of operations when under attack. The joint solution offers the widest coverage against all types of availability-based threats that target enterprise applications and data centers.
- Gain unprecedented visibility into network traffic, including a wide range of non-DDoS threats on your network.
- Reduced operational costs – fully automated DDoS attack detection and mitigation solution; system kicks-in only when under attack.
- Best price point for out-of-path DDoS protection.

**The Radware-FlowTraq Solution Differentiator**
- Accurate attack detection: the FlowTraq system uses flow-based behavioral analysis to detect DDoS attacks and evaluate the impact the attack has on all network resources along the path to the target.
- Most accurate and scalable attack mitigation solution in the industry with Radware DefensePro – uses behavioral real-time signatures with challenge mechanism to identify and block only attack traffic within seconds.

**About FlowTraq**
FlowTraq® provides software and services for high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors, including distributed denial of service (DDoS), brute force attacks, worms, network scans, botnets and other network traffic anomalies. For more information, please visit www.flowtraq.com. FlowTraq encourages you to join our community and follow us on Twitter and LinkedIn.

**About Radware**
Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware’s solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.