RACKSPACE DDoS MITIGATION SERVICES

General Overview

Summary

RackSpace DDoS Mitigation Services is a unique DDoS hardware-based program that ensures customer uptime in the event of a DDoS attack. No other hosting provider has combined three such disparate technologies to create such an all-encompassing protection system for their network. From network-wide packet scanning through granular traffic analysis right down to server-level anomaly detection, three layers of detection identify and filter hostile traffic 24x7x365. In effect, all DDoS processing is offloaded from your configuration to a Rackspace infrastructure allowing you to continue to do business. Our DDoS Mitigation Services allow you to choose the level of service you need at the price you want to pay.

Two Different Levels of Service to Fit Your Budget Needs

- Subscription Service: Proactive Protection for Potential Attacks
- On-Demand Service: Protection Activated After the Onset of a Security Event

How It Works

TIER 1: Network-Level Traffic Monitoring & Analysis
The service starts by monitoring all traffic entering Rackspace network. Sophisticated Intrusion Detection technology, capable of handling over 30 million packets per second, examines each and every incoming packet for signs of malicious activity. Meanwhile, Cisco NetFlow statistics perform granular traffic analysis of source and destination IP addresses, protocol information, flow information, and traffic volume. Rackspace DDoS Mitigation Services report this information to Rackspace Network Operations Center (NOC) experts, who use it to make routing decisions for best performance and to provide information on the attack type, source, protocol, and duration to any affected customers.

TIER 2: Server-level Anomaly Detection
The service also searches for anomalies on a per-server basis. It does this two ways. The offering analyzes your server’s traffic patterns to learn about “normal” network behavior and combining the results with port usage information to create a profile of your server’s usual traffic. The service then monitors the traffic on your server, constantly comparing it to this profile and looking for unusual behavior. If it detects an anomaly, the malicious traffic is immediately filtered and blocked. The other Rackspace DDoS Mitigation Services offerings use a standard profile to determine any anomalies.

TIER 3: Traffic Filtering & Re-Routing
Finally, if malicious activity is detected, the service acts quickly, routing suspicious traffic through a “sanitation engine”, which uses multiple DDoS detection methods to filter out and divert malicious traffic. All legitimate traffic is then forwarded to the intended destination servers, which are able to serve clients entirely unaffected by the ongoing DDoS attack.

Features Include:

- Robust intrusion detection system
- Granular traffic analysis
- Real-time alerts
- Anomaly detection
- Non-intrusive – no upgrades or re-architecting required
- Default install - allows up to 4 IPs