AT&T Distributed Denial of Service (DDoS) Defense

DDoS Attacks Proliferate

Distributed Denial of Service (DDoS) attacks are among one of the most disruptive and vicious activities passing over the Internet. DDoS attacks can overwhelm web servers and saturate a company's connections to the Internet resulting in the inability to maintain efficient communications and connectivity and can ultimately impact business operations. By integrating the predictive and early warning capabilities of AT&T DDoS Defense Service, AT&T is delivering one of the most potent tools against denial of service attacks, which have crippled entire networks and brought businesses to a halt.

Proactively Help to Protect Your Networks

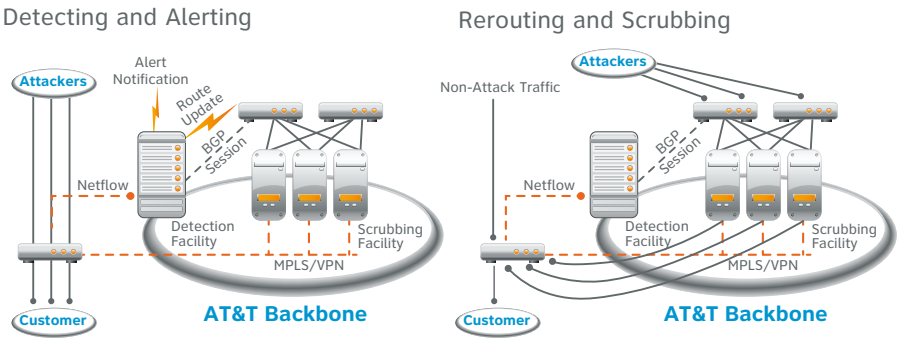
AT&T DDoS Defense detects and mitigates DDoS attacks. Organizations who want to better protect their network can obtain AT&T DDoS Defense Service no matter who their service provider or carrier is. Customers don't need to purchase their network connectivity from AT&T to purchase AT&T DDoS Defense.

DDoS identification and mitigation takes place within the AT&T IP backbone providing you with increased protection from identified malicious traffic before it reaches your network. DDoS Defense consists of a detection device that examines your net flow data. If a denial of service attack is detected, the traffic will be routed to a network mitigation farm, where the malicious DDoS attack packets are identified and dropped while the valid traffic is allowed to pass to you.

Detecting an Attack

DDoS Defense consists of a network detection facility that monitors your network traffic for a specified set of IP addresses to be protected. A set of network mitigation devices are available to scrub your traffic if a Distributed Denial of Service attack is detected. When the detector identifies a DDoS attack, an alarm is sent to both an AT&T operations center and to you notifying you of the detected attack. Concurrently, AT&T will notify you of the attack. AT&T will reroute traffic directed at the server under attack to the network scrubbing facility

AT&T DDoS Defense architecture overview



Potential Benefits

- Detects the presence of an identified DDoS attack
- Blocks malicious packets in real-time while allowing the flow of legitimate business traffic
- Stops denial of service traffic floods within the AT&T network before they choke your private network
- Allows you to be proactive vs. reactive when helping protect your network against malicious intruders and unauthorized activities

Features

- Provides a robust, all inclusive information security portal
- Notifies via e-mail and/or Pager on critical alerts, advisories and attacks
- Provides anomaly detection, packet scrubbing, traffic analysis and e-mail trap alerts
- Includes equipment, monitoring and management
- Monitors a specified IP address range
- Includes web portal access for service and status reporting information, including anomaly reporting, historical archival, dark address analysis and status page

To learn more about AT&T Managed Security Services, visit www.att.com/network-security or have us contact you.

Share this with your peers

within the AT&T IP Backbone. This traffic will then be scrubbed dropping the DDoS attack traffic and passing the valid traffic to your access router, while traffic destined to servers not under attack continues to flow directly to your network. Don't allow DDoS attacks to cripple your business operations. Rather, let AT&T DDoS Defense help you filter out malicious traffic before it impacts your network and servers keeping your business running smoothly.

AT&T Secure Network Gateway

AT&T Secure Network Gateway service delivers state-of-the-art security features with proactive monitoring and management. We have conveniently packaged and simplified the purchasing, contracting and billing of AT&T DDoS Defense Service, AT&T Network-Based Firewall Service, AT&T Secure E-mail Gateway Service and AT&T Web Security Service under one contract and one invoice providing an efficient and cost-effective way to help meet your business security needs.

Top Readiness Tips to Help Keep You Prepared

Ready Yourself for a DDoS Attack

- Have a reaction plan ready to implement
- Document the key technical players to help remediate an attack. Use small focused groups to make good decisions quickly
- Test your DDoS service annually and ensure all notifications are received as expected
- Engineer resources to accommodate attack scenarios above and beyond normal, anticipated loads
- Keep mitigation settings current with gateway architecture (i.e. circuits, IP addresses, servers, services, etc.)
- Be sure your DDoS Service Provider is experienced and well versed in current attack vectors
- Understand your ISP's capabilities for dealing with attacks
- You may need an alternate form of communication during an attack in the event that other IP based services are impacted i.e. VoIP, e-mail
- Understand and document your gateway architecture as it evolves, and know how to implement routing changes quickly

During a DDoS Attack

- Refer to your documented plan
- Document all mitigation/corrective steps taken
- Save logs and packet captures for post mortem reviews

Threat Landscape

- Attacker's motives include political, financial, and bragging rights - every corporation is susceptible to an attack
- A DDoS attack is often a diversionary tactic to enable other illicit activities such as data theft, fraud, etc.
- All attacks are different – some attack volumetrically, while others exploit Transmission Control Protocol (TCP) Layer 7 vulnerabilities. Some attacks exploit both
- Attacks tend to change and adapt to defensive measures put into place

For more information about AT&T DDoS Protection, visit us at www.att.com/ddos-protection or call us at 877 542-8666.

Share this with your peers

To learn more about AT&T Managed Security Services, visit www.att.com/network-security or have us contact you.

Scan this code to learn more.

02/20/14 AB-0292-14