AT&T Distributed Denial of Service (DDoS) Defense

DDoS Attacks Proliferate

More than ever, Distributed Denial of Service (DDoS) attacks are among 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, or offering the AT&T Reactive DDoS Defense service, AT&T is delivering one of the most potent tools against denial of service attacks.

Detecting and Mitigating an Attack

The AT&T DDoS Defense Service line includes the fully managed AT&T DDoS Defense Service and the Customer directed AT&T Reactive DDoS Defense Service. Customers who have subscribed to the AT&T Reactive DDoS Defense service may call the AT&T Threat Management Center to activate mitigation after recognizing they are under attack.

On the other hand, the full featured managed AT&T DDoS Defense Service consists of a network detection facility as well that monitors a specific set of IP addresses in the Customer's network sending alarms to AT&T operations center and the Customer notifying them when an attack is detected.

Next, network based mitigation devices are available to scrub the traffic if a Distributed Denial of Service attack is detected. This is where AT&T will reroute all traffic directed at the server under attack to filter out the DDoS attack traffic and pass on the valid traffic to the Customer's access router while traffic destined to servers not under attack continues to flow directly to the network. Don't allow DDoS attacks to cripple business operations.

Let AT&T DDoS Defense services help filter out malicious traffic before it impacts the network and servers so the business can continue to run smoothly.

Potential Benefits

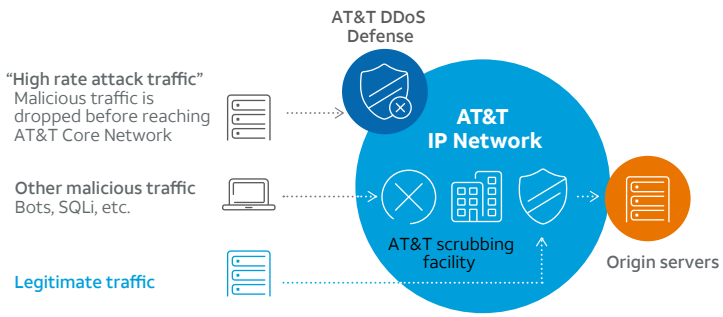
- Detect the presence of an identified DDoS attack (full managed AT&T DDoS Defense)
- Block malicious packets in real-time while allowing the flow of legitimate business traffic
- Stop denial of service traffic floods within the AT&T cloud before overwhelming the private network
- Offer the option to be proactive vs. reactive when starting mitigation
- Help protect the internal network against malicious intruders and unauthorized activities

Features

- The full managed service may notify via e-mail on critical alerts, advisories and attacks
- The full managed service may provide anomaly detection, packet scrubbing, traffic analysis and e-mail trap alerts
- The full managed service may monitor a specified IP address range
- Include equipment, monitoring and management
- Stop identified DDoS attack regardless of size
- Include web portal access for service and status reporting information, that may contain anomaly reporting, historical archival, dark address analysis

AT&T DDoS Defense architecture overview

How AT&T helps protect against DDoS attacks



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

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 or AT&T Reactive 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 the business' security needs.

Top Readiness Tips to Help Keep You Prepared

Getting Ready for a DDoS Attack

- Have a reaction plan ready to implement.
- Document the key technical players to help remediate an attack. Use small task forces to make good decisions quickly.
- Depending on the level of service chosen, allow for testing of the anti-DDoS service annually and see to it that all notifications are received as expected.
- Engineer network components and other 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).
- Be sure your anti-DDoS attack Service Provider is experienced and well versed in current attack vectors.
- Understand the ISP's capabilities for dealing with attacks.
- Prepare 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 the gateway architecture as it evolves and know how to implement routing changes quickly.

During a DDoS Attack

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

Threat Landscape

- Attackers' motives include political agendas, financial gains, and bragging rights. Every business is susceptible to an attack.
- A DDoS attack is often a diversionary tactic to enable other illicit activities such as data theft or fraud.
- All attacks are different – some are volumetric in nature while others exploit Transmission Control Protocol Layer 7 vulnerabilities. Yet some attacks exploit both.
- Attackers tend to change their tactics and adapt to defensive measures put into place.

Share this with your peers

For more information about AT&T DDoS Protection, visit us at www.att.com/ddos-protection or call us at 877.542.8666.

Scan this code to learn more.

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

12/07/16 AB-0292-15