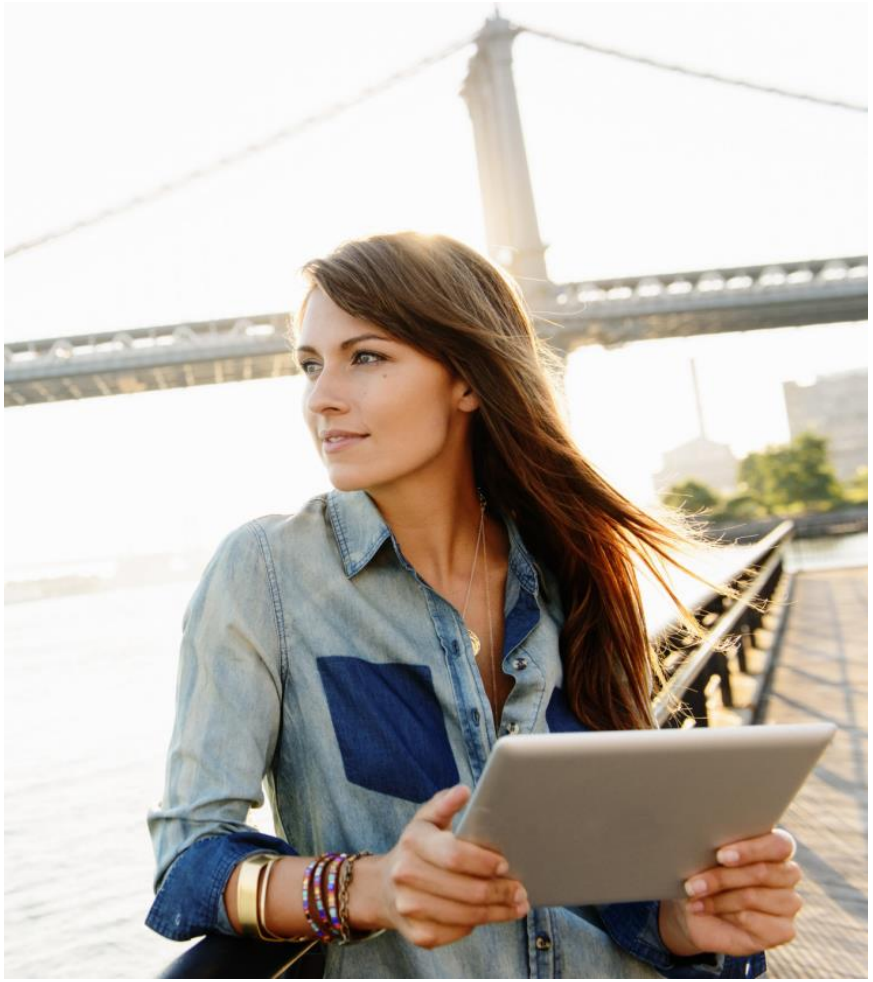
AT&T Distributed Denial of Service (DDoS) Defense

April 2016

How you can benefit from AT&T DDoS service

- DDoS attacks have increased over 60% in the past 2 years
- AT&T DDoS Defense service updates provide you with increased flexibility in the face of an evolving security landscape
- AT&T DDoS Defense service is capable of mitigating attacks of all sizes, both large and small
- AT&T has upgraded pricing tiers for you to select the appropriate plan based on your security profile and level of DDoS activity
- Additional higher support levels are also available to help meet your specific level of DDoS security needs



The AT&T advantage

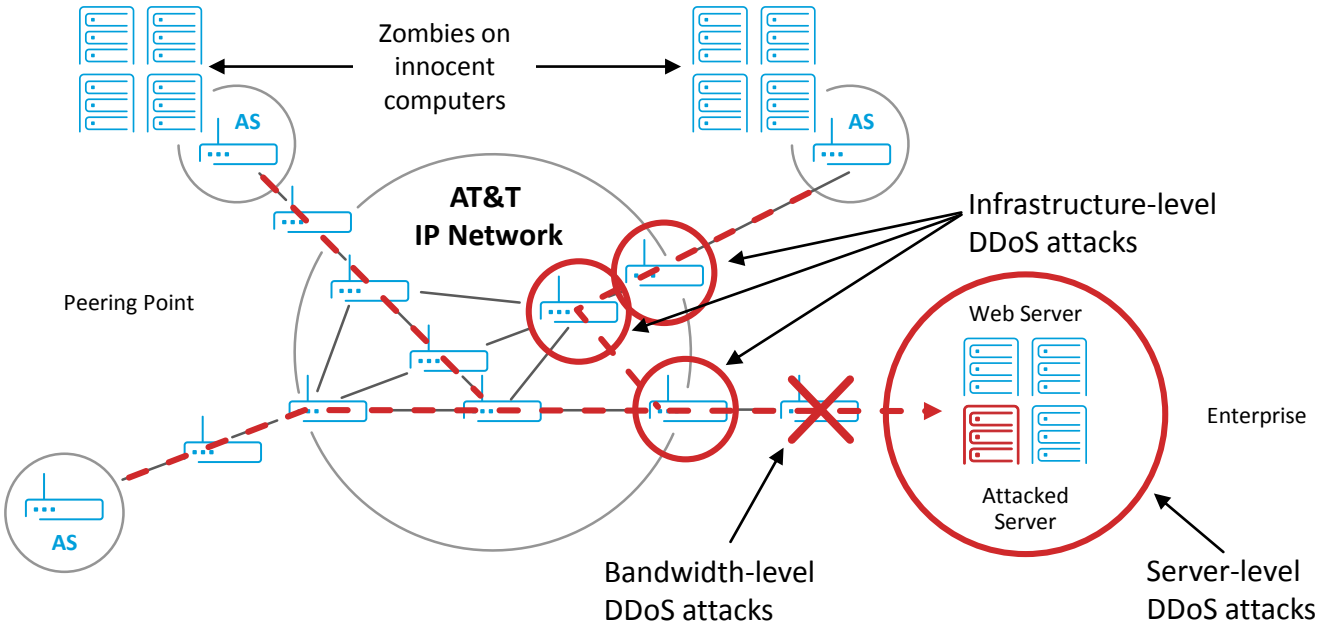
- **Unique Global View of Threats** – AT&T provides a proactive, early warning system of threats impacting the AT&T Network. As one of the world's largest Internet Providers, we have a unique, global view of the threat landscape and use this intelligence to help identify, predict, and thwart attacks.
- **Proactive** – Our DDoS Defense solution can proactively mitigate volumetric DDoS attacks before they reach your network and disrupt your business. We perform detailed traffic analysis and are able to identify anomalies in seconds. Then the malicious traffic can be sent to scrubbing facilities in the AT&T backbone and blocked.
- **Help remediate large and small attacks** – AT&T Threat Management and Network Operations teams work closely together to provide you with best-of-class capabilities including the ability to drop attack packets at the AT&T network edge.
- **Investment** – AT&T continually invests in expanding and upgrading its security and network infrastructure to keep up with the ever-growing threat landscape.
- **Global Footprint** – with scrubbing facilities around the world to prevent service disruption.

AT&T DDoS Defense Overview

	DDoS Defense
Scope	• Security alerting and mitigation of volumetric DDoS attacks impacting customers network
Features	• Monitors Customer Public network IP addresses • Detects profile and misuse anomalies
Benefits	• Designed to proactively eliminate DDoS attacks before they penetrate private network • Requires no additional hardware or software • Manual, Auto, or Platform initiated mitigation
Reports	• Traffic Summary • TCP Application Summary • UDP Application Summary • Dashboard view and widgets
Requirements	• AT&T Managed Internet Service (MIS)/MIS+/Global MIS Customers and/or AT&T Internet Data Center (IDC) Hosting customers

AT&T DDoS Defense

Multiple Points of Customer Network Vulnerability



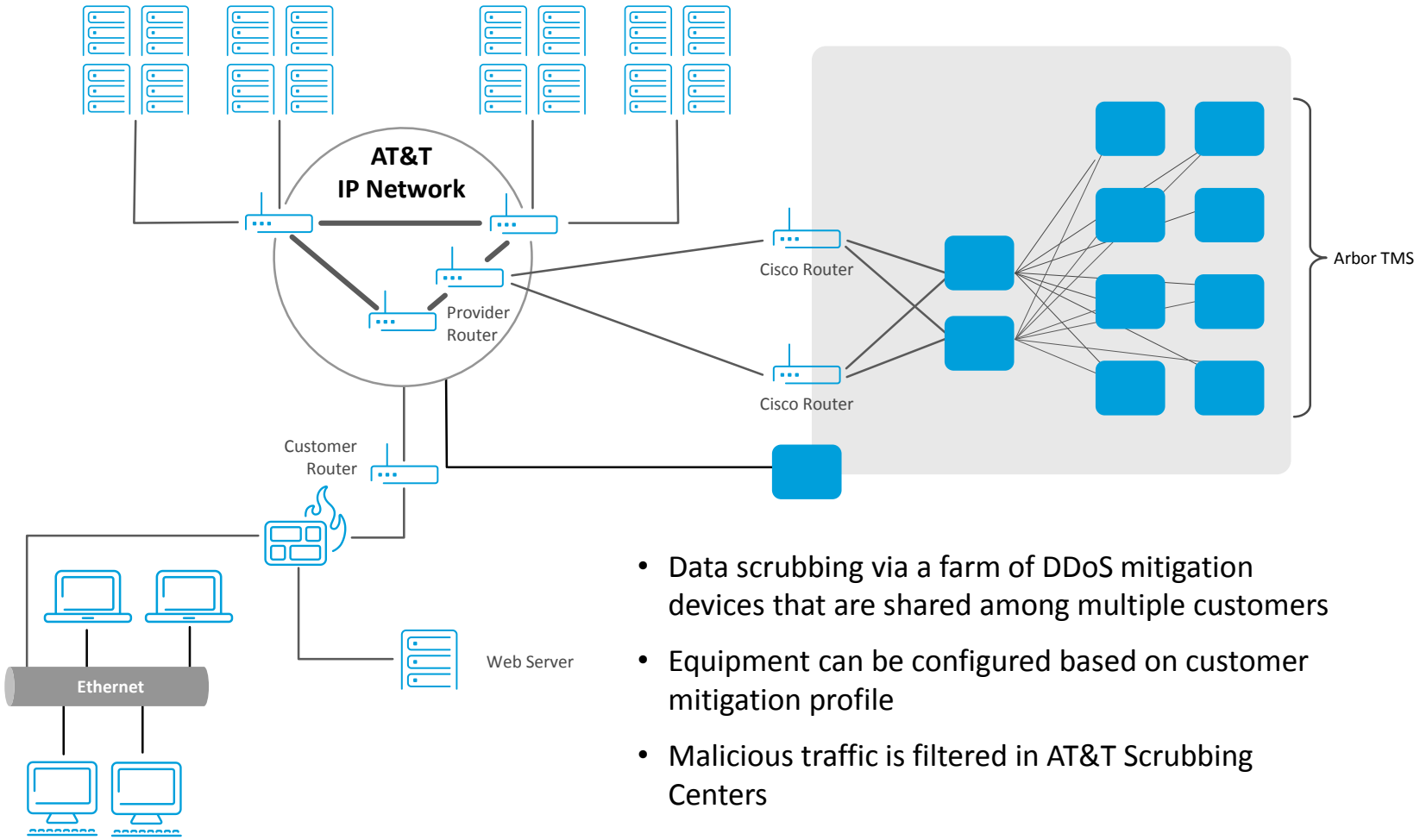
Features

- Capable of identifying attacks in seconds
- Can provide Immediate mitigation of a broad range of DDoS attacks

Benefits

- Defense against volumetric attacks designed specifically to disable infrastructure resources, applications and businesses
- Helps protect availability and ensures business continuity

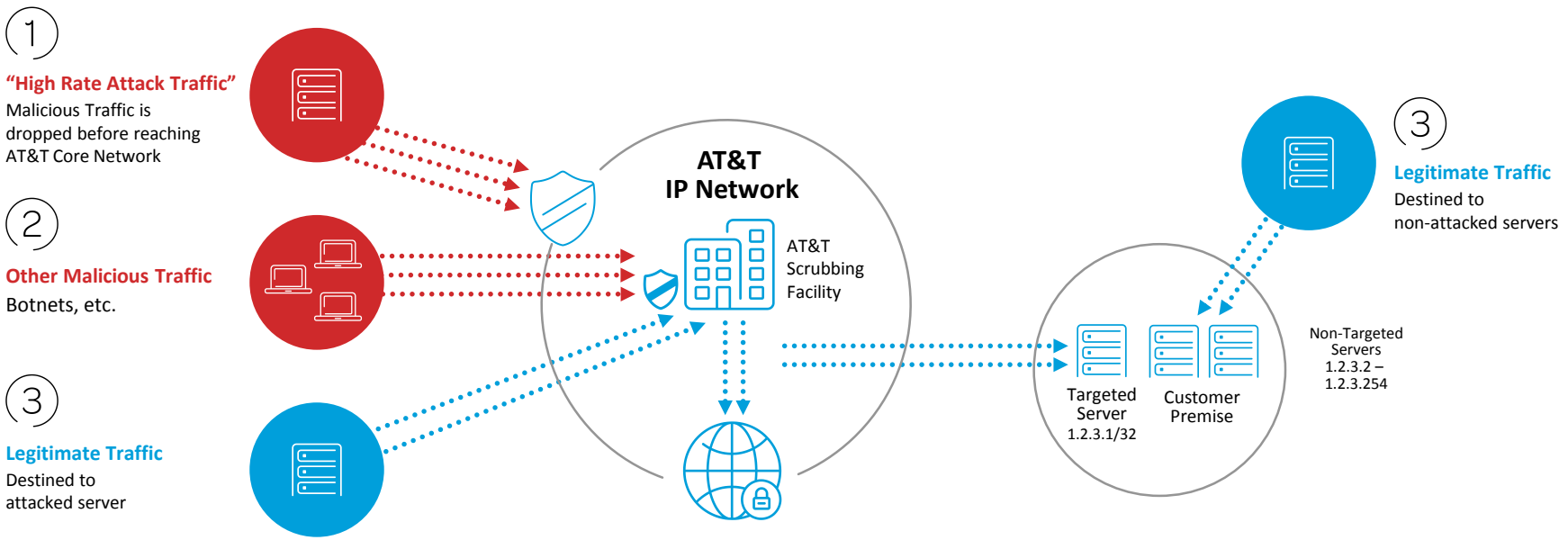
Shared Mitigation



- Data scrubbing via a farm of DDoS mitigation devices that are shared among multiple customers
- Equipment can be configured based on customer mitigation profile
- Malicious traffic is filtered in AT&T Scrubbing Centers

AT&T Distributed Denial of Service (DDoS) Defense

How AT&T helps protect you from DDoS attacks



Routing traffic through the AT&T Virtual Private Network (VPN) delivers clean traffic to the AT&T edge providing protection from other Internet-facing exposures

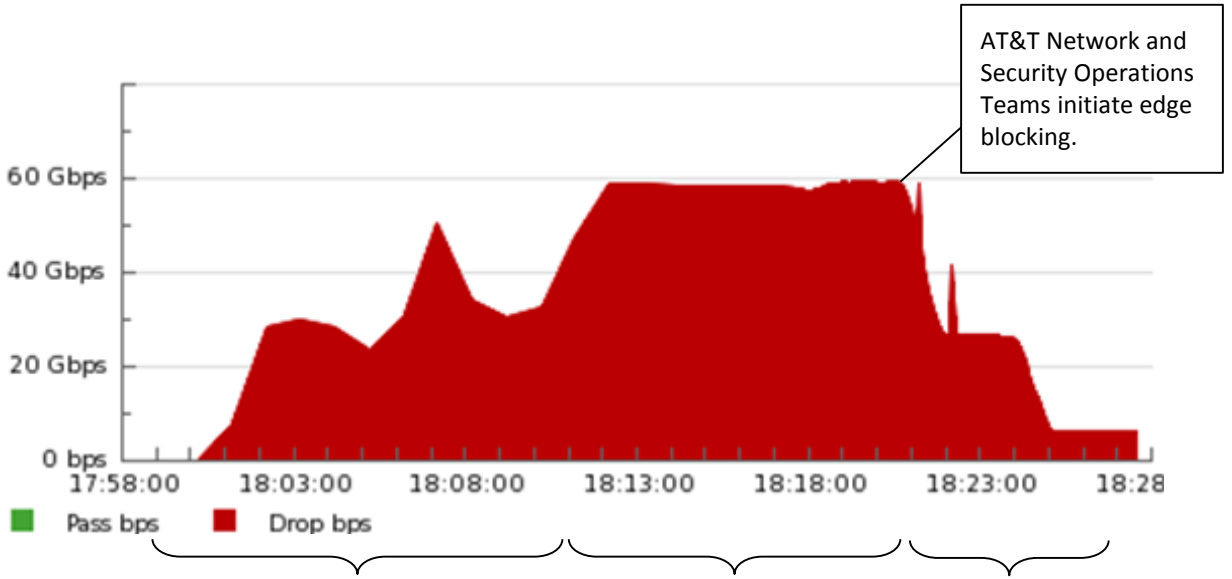
1. Black holes* help stop bad traffic at the Network Edge
2. Malicious traffic (Botnets, etc.) is identified and scrubbed in AT&T Cloud before reaching customers
3. Legitimate traffic flows to Customers

***Black holes** refer to places in the network where incoming traffic is silently discarded without informing the source that the data did not reach its intended recipient. The black holes are invisible and can only be detected by monitoring the lost traffic.

AT&T DDoS Defense Service

Anatomy of an Attack – Edge Blocking

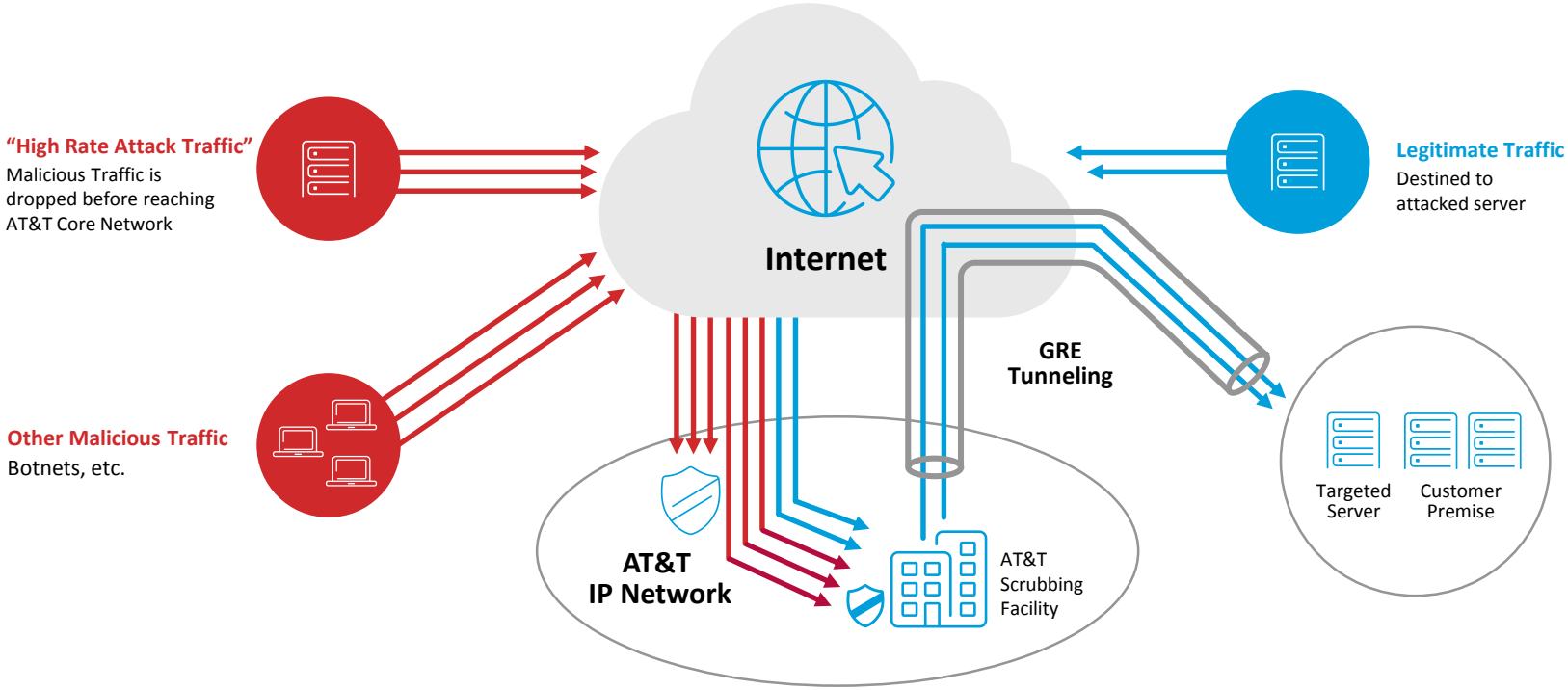
- At approximately 17:53 AT&T and Customer receive a high DDoS alert
- Customer site is inaccessible to legitimate users
- AT&T Managed Security Services Threat Team investigates the alert and subsequently contacts customer
- Decision made to mitigate attack at 17:58



The graph shows the amount of traffic the AT&T DDoS Scrubbing Center is dropping for the customer. The brackets denote actions taken during the noted time periods.

AT&T Distributed Denial of Service (DDoS) Defense

Carrier Agnostic Option of DDoS Defense



Domain Name System (DNS) A-record change
– Customer can change DNS A-record to an IP address provided by AT&T

Border Gateway Protocol (BGP) Direct Route Advertisement
– AT&T can advertise Customer's IP block to redirect traffic to AT&T's network

GRE (Generic Routing Encapsulation)
Tunnel is used to direct scrubbed traffic back to the Customer Premises

DDoS Defense

Carrier Agnostic Option

BGP Direct Advertisement

1. Monitoring provided by collecting Customer Flow Data sent to AT&T through GRE tunnels
2. If attack is detected:
   a) Customer de-preferences or withdraws the Class “C” route advertisement
   b) AT&T advertises Class “C” instead
   c) Traffic flows to AT&T scrubbing facility
   d) Scrubbed traffic is returned to Customer through GRE tunnels
   e) Customer’s return traffic takes the shortest path back to the source

DNS A-record Change

1. Monitoring provided by collecting Customer Flow Data sent to AT&T through GRE tunnels
2. If attack is detected:
   a) Customer changes DNS A-records for attacked hosts and withdraws the route advertisement from its ISP
   b) Traffic flows to AT&T scrubbing facility
   c) AT&T uses Network Address Translation (NAT) to the original destination IP
   d) Scrubbed traffic is returned to Customer through GRE tunnels
   e) Customer return traffic is sent back through GRE tunnels

Customer Benefits

- Combines customer specific Distributed Denial of Service (DDoS) detection with mitigation
- Supports trouble-free operation of your business critical applications – Not implementing can cause catastrophic results in the event of an attack
- Designed to block malicious packets in real time while allowing the flow of legitimate business traffic
- Removes malicious packets before reaching your last mile
- Scrubbing takes place on the AT&T OC-192 backbone
- Always monitored data flows enable greater visibility into your traffic characteristics
- Simple activation – no additional CPU or traffic load on your routers
- Scalable
- Fast attack identification
- Peacetime Learning for increased attack protection

Be Prepared for a DDoS Attack!

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, email.
- 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

AT&T Secure Network Gateway Service

Delivers multiple security capabilities embedded in the network, detecting and preventing threats in the cloud before they reach your premises

Security services include:

- AT&T DDoS Defense Service
- AT&T Network-Based Firewall Service
- AT&T Secure E-Mail Gateway Service
- AT&T Web Security Service

Security Bundles are an efficient and cost effective way to meet your security needs:

- Carrier-grade security services
- Single contract
- One bill
- Discounted pricing across multiple services

Secure Network Gateway is embedded in the AT&T Network

- Provides defense-in-depth with proactive 24X7 monitoring and management around the globe
- Delivers security at every layer from network to applications