

**Note: The DDoS Defense Service Guide is updated frequently. Please see the following link for further updates.**

[http://serviceguidenew.att.com/sg\\_CustomPreviewer?attachmentId=00P1A00000na2luUAI](http://serviceguidenew.att.com/sg_CustomPreviewer?attachmentId=00P1A00000na2luUAI)

## **SD-10. AT&T Distributed Denial of Service (DDoS) Defense**

### **SD-10.1. Overview**

The AT&T DDoS Service (“DDoS Service” or the “Service”) can only be provided to AT&T MIS/MIS+/GMIS Customers and/or AT&T Internet Data Center (“IDC”) Hosting customers with connectivity to the AT&T IP Backbone.

The DDoS Service includes DDoS detection and mitigation that takes place within AT&T’s backbone and provides protection against volumetric attack traffic before reaching the Customer site. It consists of a network detection device, which examines samples of Customer traffic flow data from the AT&T network for each address identified by Customer. Upon detection, or Customer notification of a perceived DDoS Attack, AT&T can reroute traffic targeted at an attacked host through the AT&T IP Backbone to a shared Scrubbing device which then ‘scrubs’ the rerouted traffic by dropping the suspected DDoS attack traffic. The DDoS Service is designed to then pass valid traffic to the Customer access router. AT&T will resume the normal routing of Customer traffic once AT&T determines the DDoS attack has subsided. The Customer will have access to reports on the attack and mitigation activity through a Customer-specific portal (“DDoS Defense Portal”). In addition, AT&T shall:

- ☐ During the first two (2) weeks following the Service Activation Date, examine samples of Customer traffic flow data and analyze patterns within such data in order to baseline Customer traffic patterns to assist in determining when a DDoS attack is occurring;
- ☐ When AT&T believes that conditions so warrant; (a) issue Alert(s) to Customer about IP Threat(s) which shall direct Customer to the DDoS Defense Portal for further information; (b) provide information via the DDoS Service Portal to assist Customer in addressing and/or mitigating IP Threats;
- ☐ Notify Customer via email within fifteen (15) minutes, and where warranted, by telephone within twenty (20) minutes, when AT&T believes a DDoS attack is occurring;
- ☐ Provide Customer access to reports on specific attacks and mitigation activity through an AT&T specific website provided to Customer; and
- ☐ Make available to Customer the Traffic Anomaly Detection analysis and Traffic Anomaly Detection reports related to any DDoS Attacks on Customer during the period in which DDoS Service is provided to Customer. All reports are AT&T Proprietary Information and are subject to the terms and provisions of the Agreement.

#### **SD-10.1.1. Customer Responsibilities**

Customer shall:

- ☐ Cooperate with AT&T in all aspects of the Service, including, but not limited to providing AT&T with the names(s) of a point of contact for the Service;
- ☐ Assure that only it or its designated Users will access the Service and that Customer and all Users will not share User IDs or other methods for accessing the Service with individuals who are not the designated Users of the Service. Customer further agrees to notify AT&T of the

designated User of each User ID provided with the Service. Customer shall promptly notify AT&T of any changes to any of the designated Users assigned to the User ID, not disclose, copy, disseminate, redistribute or publish any portion of the Service to any other party. Reproduction of the Service in any form or by any means is forbidden without AT&T's written permission, including, but not limited to: (a) information storage and retrieval systems; (b) recordings and re-transmittals over any network (including any local area network); (c) use in timesharing, service bureau, bulleting board or similar arrangement or public display; (d) posting any portion of the Service to any other online service (including bulleting boards or the Internet); or (e) sublicensing, leasing, selling, offering for sale or assigning the Service(s) to another entity or User;

☐ Assure that its and User's use of the Service(s) will comply with written and electronic instructions for use of the DDoS Defense Portal;

☐ Be solely responsible for determining the configuration of and how and where to use the DDoS Defense Portal views and reporting features. The portal views and reporting features of the Services are intended to provide Customer with information that is helpful in optimizing and otherwise managing its network and the Service purchased from AT&T;

☐ Be the owner and controller of any data collected via these portal views and reporting features. AT&T shall be acting only as a data processor as to such information;

☐ Be responsible either for (a) taking all relevant procedural steps to ensure that viewing and using the portal views and reports is in compliance with applicable local laws and (b) ensuring that the portal views and reports are not used in countries where this is not permitted;

☐ Cooperate with AT&T in all aspects of the Service, including, but not limited to, providing AT&T information regarding any changes to the Customer network in order to assist AT&T in its analysis and examination of the Customer traffic flow data;

☐ Provide AT&T with a list of Customer IP addresses connected to the AT&T IP Backbone that Customer wishes to have subject to the DDoS Service, and immediately notify AT&T of any additions or deletions to such list while Customer is receiving DDoS Service;

☐ Provide AT&T with the names of three (3) Customer points of contact and related contact information;

☐ Immediately notify AT&T of events that Customer becomes aware of that would cause significant traffic pattern changes in the Customer network that is being monitored under the DDoS Service; and

☐ Immediately notify AT&T if Customer believes it is under a DDoS attack and the Customer believes that AT&T failed to detect or notify Customer of such attack.

Customer acknowledges and understand that if Customer does not fulfill its obligations or provide the necessary information as provided herein, then the DDoS Service may be degraded or AT&T may not be able to provide the DDoS Service to Customer.

When using multi ISP solution, Customer is responsible to:

☐ Ensure that the AT&T link is sized to support any additional traffic during the attack; and

☐ Withdraw the super block advertisement(s) from other ISPs.

### **SD-10.1.1.1. Additional Customer Responsibilities regarding DDOS Defense Service**

Customer shall:

- ☐ provide AT&T with a list of Customer IP addresses connected to the AT&T IP Backbone that Customer wishes to have subject to the DDoS Option, and immediately notify AT&T of any additions or deletions to such list throughout the term of the service agreement;
- ☐ provide AT&T with the names of three (3) Customer points of contact and related contact information;
- ☐ immediately notify AT&T of events that Customer becomes aware of that would cause significant traffic pattern changes in Customer's network that is being monitored under the DDoS Defense Option; and
- ☐ immediately notify AT&T if Customer believes it is under a DDoS attack and the Customer believes that AT&T failed to detect or notify Customer of such attack.

### **SD-10.2. Traffic Anomaly Detection**

AT&T uses sampled traffic flow data from access routers within the AT&T network. This data is directed to the AT&T Anomaly Traffic Detection devices.

Traffic Anomaly Detection has two algorithms that run on a single detection portal. The first algorithm looks for "Misuse Anomalies" while the second algorithm looks for "Profiled Anomalies". Traffic Anomaly Detection, using both algorithms, is designed to detect anomalous traffic patterns that are considered malicious and to alert Customer that mitigation may be warranted.

#### **SD-10.2.1. Methods of Detection**

AT&T uses the NetFlow traffic from the access router within the AT&T network. The NetFlow traffic is directed to the AT&T Anomaly traffic detection device.

### **SD-10.3. Detection Capabilities and Exclusions**

The DDoS Service is designed to detect and help protect against attacks that are volumetric in nature. For the purposes of this Service Guide, a volumetric attack is defined as an attack that sends high volumes of traffic designed to overutilize bandwidth and eventually deny access for legitimate users. Volumetric attacks include those attacks listed in the Volumetric Attack Types and Description table set forth below. Volumetric attacks do not include: (i) application layer attacks (those that primarily target applications); (ii) SSL attacks (those aimed at exploiting the CPU intensive nature of encrypting and decrypting packets); and (iii) "low and slow" attacks (those that consume a high number of connections and can exhaust server resources).

#### **Volumetric Attack Types and Descriptions**

| <b>Attack Type</b> | <b>Description</b>                                |
|--------------------|---------------------------------------------------|
| Spoofed            | Sending packets with a forged source address      |
| Malformed          | Sending packets with abnormal bits or flags set   |
| Floods             | Sending high rates of legitimately formed packets |

|             |                                                          |
|-------------|----------------------------------------------------------|
| Null        | Sending packets with no content or illegitimate protocol |
| Fragmented  | Sending packet fragments that will never be completed    |
| Brute Force | Sending packets that exceed defined flow rates threshold |

#### **SD-10.4. DDoS Anomalies**

Misuse Anomalies are traffic patterns that are of known DoS signatures including high rates of protocol fragments, ICMP, SYNs, RSTs and Nulls (No payload).

Profiled Anomalies are traffic patterns that have exceeded the learned baselines that have been generated by AT&T based on a sliding two week interval of Customer traffic flow. Profiled thresholds are set at certain levels of Packets Per Second ("PPS") or Bits Per Second ("BPS") in excess of the pre-determined baseline.

Both Misuse Anomalies and Profiled Anomalies have three severity levels: LOW, MEDIUM, and HIGH. Low level anomalies are generated when traffic exceeds a minimum threshold. Medium level anomalies occur when the traffic exceeds a higher threshold value. A High level anomaly occurs if the attack exceeds a higher threshold and is sustained for 300 seconds (5 minutes). An Alert is automatically generated in response to a High level anomaly. Low and Medium level anomalies can be viewed via the DDoS Defense Portal. Anomaly notifications will be deleted after thirty (30) days if Low level, sixty (60) days if Medium level and one year if High level.

#### **SD-10.5. Mitigation**

Network Packet Scrubbing facilities utilize centralized DDoS mitigation devices to mitigate known malicious packets destined to the Customer network. A predefined BGP speaker will instruct a facility to re-route Customer traffic to one or more Scrubbing facilities. The BGP speaker will advertise the specific /32 address that is being attacked. This will reroute only that traffic targeted for the specific IP address to one or more of the AT&T Scrubbing facilities. After the Scrubbing facilities mitigate the malicious content, traffic determined to be valid will be forwarded back to the Customer through path that includes an AT&T managed virtual private network ("VPN"). Customer is not required to purchase VPN services from AT&T for mitigation to take place.

### **SD-10.6. Methods of Triggering**

AT&T will activate the DDoS Service mitigation via BGP speaker within the AT&T network. During service enablement, Customer may choose between Automatic Mitigation and Manual Mitigation.

- ☐ Automatic Mitigation: When the AT&T detection device identifies a volumetric attack and provides an Alert to the S/NOC and the Customer, the work center will trigger the start of mitigation prior to notifying the Customer
- ☐ Manual Mitigation: When the AT&T detection device identifies a volumetric attack and provides an Alert, the S/NOC will consult with the Customer before any mitigation is activated.

In addition, in the event Customer identifies a volumetric attack, it can notify AT&T to request and activate mitigation.

### **SD-10.7. Annual Tests**

Customer can request up to two (2) tests of the DDoS Service within one calendar year. A test must be coordinated with the AT&T Operations team and will consist of AT&T generating a volume of data traffic that will exceed Customer-defined thresholds as measured on network detection devices. A test is designed to simulate attack and to assess the systems for alerting Customer. Additionally, a test can confirm successful traffic mitigation as well as validate that valid traffic can be returned to the Customer site.

### **SD-10.8. Service Activation**

AT&T provides Service Activation for the DDoS Service. Service Activation consists of the following elements:

- ☐ Provisioning AT&T equipment used for monitoring of Customer IP address blocks
- ☐ Identifying access routers on which Customer traffic is located
- ☐ Exporting Customer traffic flow data from access routers to a DDoS Defense Portal platform for analysis
- ☐ Activating Customer on the DDoS Defense Portal

The Service Activation will occur after the above steps are complete. Billing will begin upon Service Activation.

### **SD-10.9. DDoS Defense Portal**

Reports of the DDoS Service are available to the Customer via the DDoS Defense Portal. Access to the DDoS Defense Portal is provided through the AT&T Security Center, which can be accessed through AT&T BusinessDirect®. The Customer is responsible for maintaining

AT&T BusinessDirect® Login IDs and appropriate access for individual users requiring access to the DDoS Defense Portal.

#### **SD-10.10. Third Party ISP support**

Service mitigation is only provided on the AT&T Common Backbone ("CBB"). Detection and mitigation can only be supported with traffic that terminates on an AT&T-provided Internet circuit.

In order for AT&T to provide mitigation for traffic on a third party ISP network, the attack traffic will need to be rerouted to the AT&T CBB. Customer is responsible for understanding and coordinating the withdrawal of route advertisements from third party ISPs.

#### **SD-10.11. Changes**

If Customer is currently an AT&T Enterprise Hosting Customer and needs to make a change, either adding circuits or disconnecting circuits, Customer must advise its AT&T Sales Representative of such change so as not to negatively impact the DDoS Service that Customer receives. Service Level Agreements will not apply if Customer fails to notify AT&T of such change(s).

#### **SD-10.12. DDoS Defense Welcome Kit**

AT&T will provide Customer with an AT&T DDoS Defense Welcome Kit which includes an overview of the provisioning of the Service, FAQ's and other documentation.