EIR MANAGED DDOS SERVICE SCHEDULE

The supply of Goods/Services under this Schedule is subject to the provisions of the eircom Limited Master Terms and Conditions for the Supply of Goods and Services and all definitions not defined in this Schedule shall have the meaning ascribed to them in the eircom Limited Master Terms and Conditions for the Supply of Goods and Services at www.eir.ie/business/masterterms

1. SERVICE DESCRIPTION

The eir distributed denial-of-service (DDoS) service "the Service" enables customers of eir's Next Generation Network (NGN) Internet Access service to protect their networks against (DDoS) attacks launched by malicious users - on the Internet. A "DDoS Attack" is one in which a multitude of compromised systems attack a single target, thereby causing a degraded or complete loss of Internet access for users of the targeted system. This is achieved by a flood of incoming messages to the target system, usually from a network of compromised hosts also known as 'botnets', which essentially forces it to shut down, either by overloading the web server(s), firewall(s) or saturating the communications link, thereby denying service to the system to legitimate users.

The Service monitors traffic traversing the eir ISP network peering points and works by monitoring either a Customer provided single IP address, range of IP Addresses or Autonomous Systems Number, "Managed Objects"

In the event of a DDoS Attack alarm being triggered on a Customer's Managed Object eir will inform the Customer of such an attack by phone using the Customer provided technical contact details as supplied in the Order Form.

eir will confirm the Customer's identity by asking for their unique DDoS Service ID (provided by eir at the time of order) and seek the Customer's permission to activate the filtering out and rerouting of malicious DDoS traffic attacking a Customer's Managed Object(s) "Mitigation".

The Customer may also initiate a Mitigation by phoning the support desk and specifying the Managed Object they wish to apply Mitigation to by supplying their unique DDoS Service ID. The Customer must request all Mitigations by phone as other contact methods are not monitored 24x7 and may have been compromised by a DDoS Attack.

The Service is provided on a 24x7 basis.

The service is available to new and existing eir NGN Internet Access customers.

Traffic reports, Alert reports, and Mitigation reports are can be provided by email on a monthly basis.

1.1 Anomaly Detection

eir uses a network wide anomaly detection system which also includes a Threat Management System (TMS) collectively known as the "DDoS Detection System"

An "Anomaly" is,

- an event/condition on the Customers Managed Object that is identified as a statistical abnormality when compared to typical traffic patterns gleaned from previously collected profiles and baselines;

and/or;

- an event/condition that does not adhere to normal Internet use practices for a particular Managed Object.

The Service monitors traffic for Misuse and Profile anomalies, and can be used to filter out malicious traffic transmitted during a DDoS Attack on a Managed Object. The Service does not monitor for application attacks on a Managed Object.

1.2 Anomaly and attack types that indicate DDoS Attacks are occurring

Detection of the following Anomalies are strong indicators of the occurrence of a DDoS Attack.

1.2.1 Misuse Anomalies

Misuse anomaly alarms are generated for ICMP, TCP NULL, TCP SYN, TCP RST, IP NULL, IP Fragment, IP Private Address Space and DNS flood attacks. Misuse anomalies can also be used to generate alerts if a Managed Object receives more than a pre-defined amount of traffic, measured in packets per second or bits per second. A comparison between real time traffic and stored Customer supplied Misuse threshold levels is made and when threshold levels are breached an alarm is triggered whereby eir will contact the Customer to confirm if a Mitigation initiation is required.

1.2.2 Profile Anomalies

Profile Anomalies are anomalies that occur when the DDoS Detection System detects a difference between the current traffic levels on a Managed Object compared to baseline traffic levels captured for that Managed Object over a period of time defined by the eir network administrator. When the DDoS Detection System detects a profile anomaly, it gathers details about the anomalous traffic on the affected Managed Object. A comparison between real time traffic and stored baseline traffic is made and when thresholds are broken an alarm is triggered and eir will contact the Customer to confirm if a Mitigation initiation is required

The type of attacks that profiled detection captures is of generic traffic floods that resemble normal traffic patterns, shifting attacks and non TCP/UPD/ICMP attacks. These types of attacks would not be picked up by Misuse detection.

1.2.3 Application Layer Attacks

Application layer attacks are supported reactively. If the Customer suspects their managed Object is subject to an Application layer attack they must phone eir to report such an attack. eir will investigate the attack and initiate a Mitigation by rerouting the customer traffic through the DDoS Detection System. As soon as eir reasonably believes the attack has subsided it will phone the Customer to request permission to reroute the Customer traffic to its original path.

1.3 Mitigation Initiation

A request to initiate Mitigation must be provided by the Customer prior to eir engaging in any corrective action. This applies to all types of DDoS Attacks covered by the service i.e. Misuse, Profile anomaly, and Application Level attacks.

1.4 Restoration

Permission to restore Internet access to its original routing path must be provided by the Customer in each applicable instance. Once permission is given by the customer the Internet traffic diverted through the DDoS Detection System is restored to its original routing path within the eir network core. A restore request will be activated once the customer is satisfied that the attack is over and has requested the Mitigation process to stop.

1.5 Service Summary Table

Attack types	Detection	Mitigation	Data traffic types and attack summary
Misuse	Yes	Yes	Internet Control Message Protocol (ICMP), Transmission Core Protocol (TCP) NUL, TCP SYN, TCP RST, IP NULL, IP Fragment, IP private address space and Domain Name System (DNS) flood attacks.
Profile	Yes	Yes	Generic traffic floods that resemble normal traffic patterns, shifting attacks and non TCP/UPD/ICMP attacks.
Application Layer	No	Yes	Up to application layer 7

2. SERVICE RESTRICTIONS

The Service is available to eir NGN Internet access Customer's only.

The Service does not guarantee 100% throughput and availability of a Customer's Internet service.

The Service is designed for DDoS Attacks only, it does not provide firewall functionality and does not provide protection for all the Customer's network security requirements.

The Service monitors for attacks from traffic that is traversing the eir ISP external network peering points, as such it would not identify an attack in the unlikely event that it orginates within the internal eir network.The Service is operated on a shared platform that offers simultaneous protection for multiple customers. The platform capacity to filter out malicious traffic for any given Customer is dependent upon a number of factors, including but not limited to, the following:

- The availability of platform capacity which may be in concurrent capacity use filtering out malicious traffic for other customers on the shared DDoS Detection System.
- Method of attack used.
- The Service will only deal with DDoS Attacks to the Customer's network that come from the Internet via the eir IPS network peering points on aneir NGN Internet connection.

3. CUSTOMER OBLIGATIONS

- The Customer must ensure that any of its NGN Internet access circuits associated to any of its Managed Object(s) must have a 24x7 SLA.
- The Customer must notify eir if they are making any changes to their network that could trigger an alarm and result in a false positive alarm event.
- In the event of a DDoS Attack the Customer must Phone eir to start the Mitigation process.
- If the Customer is satisfied a DDoS Attack is no longer active the Customer may phone eir to stop the Mitigation process.
- The Customer must inform their account manager in writing regarding any changes to their designated contact information.
- Designated Customer contacts must be available on a 24x7 basis.
- It is the Customer's responsibility to ensure all Customer contact information is up to date at all times and in the event of the designated and alternate Customer contacts not being contactable eir will not initiate a Mitigation.

4. MITIGATION IMPACTS

- Some legitimate Customer traffic may be rerouted through the DDoS Detection System during a Mitigation of a DDoS Attack.
- Latency may increase during a Mitigation causing data throughput to reduce.
- The eir Service may become overwhelmed if the attack is greater than eir resources can process as it is a finite resource.
- A previously unknown type of attack may evolve that the Service is not designed to mitigate against resulting in failure to Mitigate the attack.
- eir cannot be held responsible for security weaknesses that arise through the implementation of customer requested changes.
- eir cannot be held responsible for non-DDoS security breaches on other parts of the customer's network infrastructure.