

Effective: July 1, 2018

## MANAGED SERVICES - DDOS MITIGATION POLICY

### 1 INTRODUCTION

- 1.1 This Service Description describes the Distributed Denial of Service attack mitigation service ("**DDoS Mitigation**") that Equinix will provide, upon signature by Equinix and the Customer of an Order for the provision of the DDoS Mitigation.
- 1.2 Except where such terms are defined in this Service Description, capitalised terms used in this Service Description that are not defined herein shall have the meaning given to them in the MCA, GTC, MSA or any equivalent thereof.
- 1.3 This Service Description shall form part of the Terms and Conditions of the Order which is governed by our MCA, GTC and or MSA or any equivalent thereof ("the Agreement").
- 1.4 For the purposes of the DDoS Mitigation service, the following terms shall have the meanings set out below.
- 1.5 The "**Relevant Connectivity Service**" means internet connectivity provided by Equinix to the Customer pursuant to an Equinix Connect Order which is in turn referred to expressly on the relevant Order for DDoS Mitigation.
- 1.6 The "**Protected IP Block(s)**" means the IP range or addresses which are agreed to be subject to DDoS Mitigation pursuant to paragraph 2.1(a) below. These will be listed in a provision form.
- 1.7 An "**Attack**" refers to a distributed denial of service and or a denial of service attack which is perceived by the DDoS Solution and which affects part or all of the Protected IP Block(s).
- 1.8 "**Attack Traffic Overage**" means the bandwidth of an Attack within Equinix's network which is in excess of the relevant bandwidth actually paid for (whether as a recurring fee or a variable fee overage) pursuant to the Relevant Connectivity Service order.

### 2 DDOS MITIGATION SERVICE

#### 2.1 Set-up

##### 2.2.1 in providing the DDoS Mitigation, Equinix shall:

- (a) consult with the Customer to (i) set up DDoS Mitigation for the Relevant Connectivity Service, for a specified Customer IP range or individual IP addresses; and (ii) identify those IP ranges or IP addresses for which no DDoS Mitigation service will be necessary;
- (b) configure the Relevant Connectivity Service to incorporate Equinix's DDoS mitigation solution (such solution essentially being hardware which performs DDoS attack mitigation) (the "**DDoS Solution**");

##### 2.2.2 Service Operation

- (c) the ongoing operation of the DDoS Solution is such that it is able to monitor the Protected IP Block(s), and where there is no Attack, permit the traffic to bypass or pass through the mitigation service and reach its end destination with no interruption from the mitigation service;

- (d) the DDoS Solution is configured to notify Equinix of Attacks, and Equinix shall inform the Customer promptly of any such notification which Equinix actually receives;
- (e) when the Attack ceases, procure that the Relevant Connectivity Service will again bypass or pass through the mitigation service and reach its end destination with no interruption from the mitigation service;
- (f) Equinix will be responsible for coordinating all testing and repair work relating to the DDoS Mitigation service and the equipment used to provide the DDoS Mitigation service.

### 2.2.3 Support

- (a) on Customer request (whether as a result of such notification or not) or automatically (depending on the chosen service), Equinix will route the Relevant Connectivity Service through a part of the DDoS Solution which performs such cleaning and attack mitigation to the Protected IP Block(s) as the DDoS Solution is able to perform;
- (b) upon request, Equinix can provide reports, detailing the type of traffic going to the Protected IP Block(s), whether or not there has been an Attack, and details of any such Attack; and
- (c) where Equinix is unable to mitigate the attack Equinix shall liaise between and work with the Customer and the relevant supplier of the DDoS Solution in the event that the Customer is experiencing, has experienced, and/or may experience an Attack or other similar event on which the DDoS Solution is not having, has not had and/or will not have the desired effect.
- (d) Due to the nature of Attacks, provision of DDoS Mitigation is intended to help weather an Attack only, and there may be some types of Attack against which DDoS Mitigation has no effect. DDoS Mitigation is less likely to be effective during the period of time immediately after the Service Commencement Date (a 'bedding-in' period).
- (e) Equinix may take any reasonable action in the event that, in Equinix's sole opinion, the volume of Attack traffic is either: i) putting Equinix's IP network (also known as the 'Equinix Connect') at risk; or ii) putting the ability for Equinix to provide internet connectivity to its other customers at risk. Depending on the circumstances, such action may include blocking or 'black-holing' specified IP addresses or ranges, or suspending or terminating all or any part of Equinix's provision of internet connectivity to the Customer.
- (f) Where Equinix blocks or "black holes" IP addresses, the Customer accepts and agrees that Equinix cannot provide the DDoS Mitigation for those IP addresses that are black holed and or blocked.



### 3 CUSTOMER DEPENDENCIES

- 3.1 The Customer shall act promptly, reasonably and reasonably consistently in responding to Equinix and working with Equinix in order to agree any aspect of any DDoS Mitigation that is not agreed and expressly specified within this service description and provisioning document.
- 3.2 The Customer shall notify Equinix of any problem with the DDoS Mitigation service of which it is aware, including where Equinix's obligations would not in themselves necessarily make Equinix aware of such problem.
- 3.3 In the event that Equinix representatives receive conflicting or different instructions from various representatives of the Customer, Equinix shall take any action that it in its sole discretion deems to be appropriate or practicable (which may include taking no action whatsoever).

### 4 SERVICE LEVELS

- 4.1 For the purposes of this clause 4, the following terms and phrases have the following meanings:

**"Affected Components"** means the Service(s) that have been affected by the failure to meet a Service Level Objective and includes the initial Service that failed plus any additional Service(s) which suffer a Service Outage as a result of the initial Service's failure.

**"No-Liability Outage"** means an outage which is not considered a Service Outage and will not attract service credits if it is caused by any one or more of the issues listed below:

- (a) An Application, or any part of an application layer hosted upon the Customer System, and / or any problem or issue with the Application or such application layer.
- (b) If the relevant Managed Services provided to Customer under an Order do not have appropriate capability or sufficient capacity to manage the volume or type of traffic flowing through the Service.
- (c) Any request, act or omission of Customer.
- (d) Any act or omission of any Third Parties other than direct Equinix suppliers (for example but without limitation, a hack, virus attack or presence of other malware, or a DDoS attack; or if a Customer supplier interferes with the Service etc).
- (e) A Suspension.
- (f) Downtime to the Service due to Maintenance being carried out. For the avoidance of doubt this applies to both Scheduled and Emergency Maintenance.
- (g) Any change requiring downtime to the Services that is agreed to by Customer.

**"No Performance"** is where an Attack causes a Protected Site to be unavailable despite the provision of DDoS Mitigation or any other mitigation service procured from Equinix by Customer. (Unavailability in this context shall be ascertained from the point of view of a (theoretical) appropriate independent third party monitoring the availability of the Protected Site from the internet. Neither Equinix nor the Customer is obliged to use such a third party for monitoring purposes, but there shall not be any No Performance unless the Customer can produce reasonable evidence of the same which Equinix cannot rebut with contrary evidence which is at least equally credible);

**"Protected Site"** is a particular part of the Customer's IT infrastructure that is set up to be protected by DDoS Mitigation, for example a certain website or IP address;



**“Slow Performance”** is where an Attack causes a Protected Site to perform more slowly than usual, despite the provision of the Service or any other mitigation service procured by the Customer.

- 4.2 Where an Attack causes the following durations of No Performance, the following Service Credits shall apply, subject to any other relevant provisions of this Service Description:

Duration of No Performance	Service Credit sum (calculated as a percentage of the Service Fee due to be paid by the Customer for the applicable month)
Up to 60 consecutive minutes	0%
More than 60 but less than 120 consecutive minutes.	25%
More than 120 but less than 180 consecutive minutes.	50%
More than 180 but less than 240 consecutive minutes.	75%
More than 240 consecutive minutes	100%

#### **GENERAL PROVISIONS REGARDING SERVICE CREDITS**

- 4.3 No Service Credits shall apply if there is Slow Performance.
- 4.4 For the avoidance of doubt, No Performance or Slow Performance is not of itself a breach of contract, or evidence of any other cause of action against Equinix.
- 4.5 To receive any Service Credit the customer must contact Equinix within 7 days after the end of the month in which the Service Level Objective is not met.
- 4.6 Equinix shall only be liable for service credits for the Affected Components.
- 4.7 The maximum credit Equinix will issue per billing period is one (1) month's MRC (or of prorated amount if applicable for the billing period during which the Service Outage was experienced) for each Affected Component directly impacted by the Service Outage. Service Credits shall be the Customer's sole and exclusive remedy for a service level failure.

