

Effective: July 1, 2018

## MANAGED SERVICES - MANAGED FIREWALL SERVICE DESCRIPTION

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(s) thereof (“the Agreement”).

### 1. Set-Up

In setting up the **Firewall Service** Equinix shall:

- 1.1 make available:
  - a) a dedicated firewall device which can be virtual or physical via a single device, or via a fully resilient pair, or in a multi-tiered format (any one of which being a “**Firewall Device**”); and
  - b) install or implement the Firewall Device into the Customer’s computer infrastructure (the “**Customer’s System**”) hosted at an Equinix data centre (IBX), in accordance with good industry practice.
- 1.2 Equinix shall configure (and manage) the Firewall Device in accordance with:
  - a) the Customer’s reasonable written instructions, rules or criteria which detail the traffic to be blocked or allowed through the Firewall Device (on the condition that the specific Firewall device is capable of implementing such instructions, rules or criteria) or in the absence of such instructions, in accordance with good industry practice; and/or
  - b) Equinix’s ‘build standard’.
- 1.3 install client-to-site or site-to-site VPN if agreed in an Order.

### 2. Service Operation

- 2.1 Equinix will ensure that the Firewall Device is configured with a view to it blocking unauthorized traffic to and from the Customer’s System while permitting authorized traffic.
- 2.2 Where the Customer has purchased a unified threat management (“**UTM**”) device, those additional UTM services will be specified in an Order.

### 3. Equinix Obligations

- 3.1 Equinix shall provide the following support services:
  - a) monitoring of the Firewall Device in accordance with the Monitoring & Maintenance Service;
  - b) responding to and implementing reasonable requested changes to the configuration, within 2 full Business Days of request, or such longer period as specified by the Customer;
  - c) upgrading and patching the software utilised by the Firewall Device(s) within a reasonable time after such upgrades and patches become available in accordance with the Patching Policy contained in the Managed Services Maintenance and Monitoring Policy; and

- d) fixing broken or malfunctioning Firewall Devices (or their applicable software) within a reasonable time (generally, assuming Equinix has successfully notified the relevant supplier on a Business Day during Business Hours, commencement of the fix will take place within 2 Business Days).

3.2 The provision of the Firewall Device monitoring service is dependent on Equinix being able to access the Firewall Devices via an internet connection or other suitable connectivity solution (and Equinix shall not be obliged to provide any relevant part of the Firewall Device monitoring service to the extent that such connection is not in place).

#### **4. Customer Obligations**

4.1 Where the Customer requires a Firewall Device to be installed and managed in a Customer's System, the Customer must provide Equinix with sufficient connectivity to ensure the solution functions as expected. A minimum of one copper 1GbE connection for internet connectivity, and one copper 1GbE connection for internal connectivity, will need to be provided by the Customer for the service to work as expected.

4.2 Where internet connectivity and or underlying hardware has not been provided by Equinix as part of a Service, it shall be the Customer's responsibility to ensure that it is in place and available and has sufficient hardware / software support contracts.

4.3 In the event that the Customer does not receive an internet connectivity service from Equinix directly, the Customer must allow Equinix to connect to relevant hardware via such third party internet connectivity service on request if Equinix wishes to do so in order to carry out its obligations.

4.4 Where the Customer provides its own hardware, it is the Customer's sole responsibility to ensure that the hardware has sufficient capability to cope with the expected usage of the firewall(s). Where the hardware cannot cope with the actual usage of the firewall, Equinix shall have no liability for any service level failure which may result.

4.5 The Customer acknowledges that the provision of a Firewall Device may affect the Customer's power draw within an IBX, and may use a small amount of bandwidth for management and monitoring purposes.

#### **5. Monitoring**

5.1 Equinix will monitor the Firewall Device(s) in accordance with the Monitoring & Maintenance Service.

#### **6. Service Level Objective**

6.1 For the purposes of this Service Level Objective the following words and phrases shall have the following meanings:

**"Application"** means an application or website used by Customer which is installed by or on behalf of Customer upon the Customer System.

**"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.

**“Highly Available Configuration”** means two or more devices which have been configured with more than one node and are resilient.

**“No-Liability Outage”** means an outage which is not considered a Service Outage and will not attract SLA 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.

**“Non-Highly Available Configuration”** means a single node device which is not configured as a resilient, highly available pair of devices.

**“Service Availability”** means the amount of time during a month, expressed as a percentage of the total time during the month, during which there is no Service Outage.

**“Service Outage”** means an outage for the duration that it causes the Firewall Device to fail or be materially adversely affected which renders the Service as unusable and in any event which is not responding to the Device Monitoring Service.

6.1 The following Service Availability percentages in a month shall give rise to the Service Credits specified in the following table, and Equinix shall account to Customer for such Service Credits only in relation to the Affected Components. For the avoidance of doubt Service Credits are payable only in relation to the Order containing the Services affected by the service level failure. Service Credits shall be the Customer’s sole and exclusive remedy for a service level failure.

Service Availability percentage for Highly Available Configuration	Service Credit
Less than 99.95%, but greater than or equal to 99.90%	Credit equivalent to 15% of one month’s fee payable for the Firewall Device in the Order
Less than 99.90%, but greater than or equal to 99.85%	Credit equivalent to 20% of one month’s fee payable for the Firewall Device in the Order
Less than 99.85%, but greater than or equal to 99.80%	Credit equivalent to 30% of one month’s fee payable for Firewall Device in the Order
Less than 99.80%	Credit equivalent to 100% of one month’s fee payable for the Firewall Device in the Order

Service Availability – Non Highly Available Configuration	Service Credit
Availability of systems configured in a non-highly available configuration will be provided on a "best-effort" basis. Equinix will use all reasonable effort to provide and maintain 99% availability, however there is no guarantee of such service, which may depend on 3 <sup>rd</sup> party hardware replacement.	N/A

- 6.4 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.
- 6.5 Equinix shall only be liable for service credits for the Affected Components.
- 6.6 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.