SPAIN MANAGED SERVICES
MANAGED FIREWALL POLICY

8 November 2019

This Spain Managed Services – Managed Firewall Policy ("Policy") supplements and sets forth additional terms and conditions governing the provision of Managed Firewall Service, as specified in the applicable Order. This Policy shall form part of the terms and conditions of the Order and the Master Country Agreement or other similar agreement between the Parties ("Agreement").

1. Service Description

1.1 Definitions

Capitalized words used in this Policy will have the meaning ascribed to them herein, but if not defined in this Policy, shall have the meaning ascribed to them in the Agreement.

"Managed Firewall Platform" means the shared infrastructure at an IBX Center on which Equinix provides the Managed Firewall Service.

1.2 Set Up

Within the implementation of the Managed Firewall Service, Equinix will perform:

i. Configuration of routing and virtual local networks (VLANs) in the Managed Firewall Platform for the Customer.

ii. Configuration of the different rules for filtering and Network Access Translation requested by the Customer. If these rules are not defined by the Customer, traffic will be blocked by default.

iii. Configuration of remote access policies requested by the Customer.

iv. Configuration of load balancing requested by the Customer (only in the Advanced Managed Firewall Service).

v. (Configuration of the Intrusion Prevention System signatures for the profile definition chosen by the Customer (only in the Advanced Managed Firewall Service). If no such profile is selected, the Intrusion Prevention System will not apply a firewall policy.

1.3 Managed Firewall Service

The Managed Firewall Service is available in Basic and Advanced modes, with the features described and as indicated below:

FEATURES	BASIC MANAGED FIREWALL SERVICE	ADVANCED MANAGED FIREWALL SERVICE
Performance		
Firewall service capacity, IPv4/IPv6	20 Mbps	1 Gbps
Maximum number of firewall rules	25	150
Maximum number of Monthly Configuration Changes	5	15
Network coverage and protection		
Maximum number of Customer networks connected to the Managed Firewall Platform	1	16
Perimeter protection	Included	Included
Internal protection	Not available	Included
Integration of external communications line	Not available	Included
Additional Features (each as further described below)		
C2L	Optional	Included
L2L	Not available	Included
SLB	Not available	Included
IPS	Not available	Included

Monthly Configuration Changes

- In Basic mode, Monthly Configuration Changes means the total aggregate number of configuration changes made in a month to the firewall rules and, where purchased, C2L.
- In Advanced mode, Monthly Configuration Changes means the total aggregate number of configuration changes made in a month to the firewall rules, C2L, L2L, SLB and IPS.

Perimeter protection

- Is the protection that the Managed Firewall Platform provides by preventing traffic passing between the internet and the Customer's network(s), except as permitted by the firewall rules.

Internal protection

- Is the protection that the Managed Firewall Platform provides by preventing traffic passing between the different Customer's networks connected to the Managed Firewall Platform, except as permitted by the firewall rules.

Integration of external communications line

- Is the ability to include an external network, which is provided by a third party network provider (for example, a point to point line contracted by the Customer and that connects the Customer's headquarters with Customer's Equipment in the IBX Center), as one of the networks protected by the Managed Firewall Platform. The communications line must be physically connected to the Customer's Equipment and the Customer will have to route it to the Managed Firewall Platform, in order to include it into the networks protected.

VPN C2L

- **"C2L"** means a virtual private network that provides an authorised remote user with the ability to connect to the Customer's protected network via a secure encrypted tunnel built from the remote user's personal computer to the Managed Firewall Platform.
- Includes up to 8 profiles (tunnels) for remote VPN access, of the IPSEC type for connection of workstations to the Customer's protected network. Each profile will serve to establish independent access privileges in accordance with the user.
- The service requires a public IP address for termination of the VPN service.
- Up to a maximum of 25 local users in the definition of the VPN service.
- Includes availability for one (1) external authentication server (Windows Active Directory, RADIUS or LDAP), administered and provided by the Customer, with a limit of 100 users, allowing the authentication process to be performed against this server.
- Supports the use of VPN IPsec client for Windows (7 or higher) and Mac OSX (10.8 or higher) platforms.

VPN L2L

- **"L2L"** means a virtual private network that provides equipment in multiple fixed locations with the ability to connect to each other through a secure encrypted tunnel over a public network such as the internet via the Managed Firewall Platform.
- Includes up to 16 "Network to Network" IPSEC tunnels for the connection of complete networks or environments.
- The service requires a public IP address for the termination of the VPNs. This IP may be the same as that used in the C2L.

Service Load Balancing (SLB)

- **"SLB"** is a data centre architecture that distributes network traffic evenly across a group of servers.
- Includes up to 25 virtual balanced services.
- Load balancing service at the network level (OSI Layer4).
- Up to 8 monitors or health checks can be configured (Application Health Check) by means of PING surveys, TCP connection and HTTP request.
- Up to a maximum of 8 real servers per balanced service.
- Balancing algorithms supported: Round Robin, Least Session.
- Persistence methods supported: Source IP, Cookie HTTP.

Intrusion Prevention System (IPS)

- **"IPS"** is the system on the Managed Firewall Platform that monitors a network for malicious activities such as security threats or policy violations and blocks the associated traffic once detected.
- Up to 4 profiles to protect against intrusions.
- Protection of protocols (HTTP, HTTPS, FTP, SMTP, IMAP, SIP, SQL, others).
- Protection against malicious software (malware, botnets and exploits).

2. Customer Responsibilities

The provision of Managed Firewall is dependent on the following Customer responsibilities and others set out in this Policy. If the Customer fails to perform or fulfil the Customer responsibilities, Equinix will not be obliged to provide Managed Firewall Services and may charge additional non-recurring Fees that are caused by or arise from such failure to perform or fulfil the Customer responsibilities:

A. Customer must place an Order for Equinix Connect, which is a mandatory requirement to use the Managed Firewall Service.

B. Customer must provide all necessary information to enable Equinix to set up any required connections between Customer's Equipment and the Managed Firewall Platform, and to perform the implementation and setup tasks described in this Policy.

C. Customer must: (i) ensure Customer's Equipment remains functional and compatible with the original settings agreed during set up, and (ii) maintain and not amend Customer's Equipment settings or configuration, except with Equinix's prior consultation.

D. Customer will be responsible for the configuration of its networks elements so as to guarantee high availability of the service.

E. Customer must not perform stress tests or denial of service tests on the Managed Firewall Platform, which could (if performed) interfere with Equinix's operation of the Managed Firewall Platform and Equinix's other customers' use of it.

F. Customer must select the Intrusion Prevention System signatures for the profile definition (only in the Advanced Managed Firewall Service).

3. Charging Methodology

Where a defined term in this Charging Methodology is not defined in this Policy, its meaning shall be as described in the Support Services Policy.

The Unit of Measure (UoM) for Managed Firewall Service is the mode chosen, Basic or Advanced. In addition, and optionally within the Basic mode, the different Fees payable by Customer will also depend on the type of C2L deployed.

The Fees for the Managed Firewall Service will accrue from the Effective Date.

4. Service Level Agreement

The purpose of this Service Level Agreement (**"SLA"**) is to define the measurable performance levels for the Managed Firewall Service and specify remedies available to Customer if Equinix fails to achieve these levels. The service credits listed in the tables below are the sole and exclusive remedy for any failure to meet the service level thresholds stated herein.

Managed Firewall at 99.5+% availability. This is met by achieving less than two hundred and nineteen (219) minutes of Unavailability of the Managed Firewall Service over a calendar month period (**"Managed Firewall SLA Threshold"**). For the purposes of this paragraph and subject to the last paragraph of this section, the Managed Firewall Service is considered **"Unavailable"** when a failure in the Managed Firewall Platform means that the Customer is unable to pass traffic across the Managed Firewall Platform. The period of Unavailability is measured from Customer's notification to Equinix of the incident to the time the Unavailability has been remedied as confirmed by Equinix. Subject to the last paragraph of this section, if Unavailability exceeds the Managed Firewall SLA Threshold, Customer will be entitled to a credit equal to 1/30th of the Fees payable for the applicable calendar month for the affected Managed Firewall Service (**"MF Fees"**). Further, Customer will be entitled to an additional credit equal to 1/30th of the MF Fees for every full hour of Unavailability beyond the Managed Firewall SLA Threshold.

General. In any calendar month, the maximum credit to which Customer will be entitled will not exceed the MF Fees payable for the affected Managed Firewall Service in such calendar month. Customer must request a credit within thirty (30) days of the date of its occurrence by contacting the Equinix Service Desk, so Equinix may investigate and isolate the cause of the failure. All periods of Unavailability must be verified by Equinix. Approved credits will be applied by Equinix to the invoice for the month following the month in which the credit was approved. Notwithstanding anything to the contrary, the SLAs will not apply and Equinix will have no liability if the Unavailability: (a) is caused by circumstances beyond Equinix's reasonable control; (b) is caused by Customer's act or omission, including any denial of service test or stress test performed by Customer or on its behalf by a third party on the Managed Firewall Platform; (c) is caused by Customer's Equipment, software or connectivity on or between Customer's Equipment and the Managed Firewall Platform not provided by Equinix; or (d) that occurs during a scheduled maintenance window. Equinix will use reasonable efforts to notify Customer at least fourteen (14) days prior to any regularly scheduled maintenance and as soon as practicable before any emergency maintenance. Equinix will use commercially reasonable efforts to minimize disruption to Customer's Services when performing scheduled maintenance.

5. Miscellaneous

Equinix's customer support for the Services described in this Policy are outlined in the Managed Services – Support Services Policy for Spain – Managed Services available www.equinix.com/resources/product-documents/. This Policy and the Order, together with the Agreement, represents the complete agreement and understanding of the Parties with respect to the subject matter herein and in the Order, and supersedes any other agreement or understanding, written or oral.