CONTRACTS

MANAGED FIREWALL POLICY

October 30, 2019

This Managed Firewall Policy ("Policy") complements and provides additional terms and conditions for the Customer's use of Managed Firewall, as described in the relevant Equinix Order. Any terms not defined in this document are defined in the Equinix Order, MCA, or other similar document.

1. Product Description

The term Firewall refers to a system whose main function is to filter the traffic of networks that consist of data packets in order to prevent or allow access over the network to particular equipment or Customer's service, based on information about IP addresses and the source and destination port of the packets transmitted.

Managed Firewall service consists of providing a customer's network protection system and its servers by monitoring and controlling inbound and outbound network traffic based on predetermined Firewall rules. Management can be done by the customer (self-service in the Managed Services Portal) or by qualified Equinix Management team (Equinix Management) .

Product Enablement

Equinix is responsible for initial product installation. The Customer will receive an email regarding Managed Firewall product availability and instructions for use of the services. From that point forward, the Customer will receive instructions for use of the services and thereafter the responsibility for the rules configuration, operation, Technical support and administration of any other development programs (software) or applications that may be installed on the service used is the customer's sole discretion.

Basic Support

Equinix offers 24x7 support for Managed Firewall product. The following services may be ordered by opening a ticket with the Equinix Service Desk, by phone or online, at no additional charge:

- Investigate and solve service failure
- Product information

Additional Support

Equinix offers Additional Support, it is not included in the Managed Firewall product. All services are listed in the Equinix Service Catalog. Requested through the Managed Services Portal and it will be charged additionaly with Technical Hours, with non-recurring information (NRC).

2. Customer Responsibilities

The Customer shall: (i) provide the email address and phone number for a primary and an operational contact and ensure information is up-to-date 24 hours a day; (ii) configuration of firewall rules; (iii) provide all materials, equipment or facilities required to use Managed Firewall product, and be responsible for all equipment, software, services, and Customer components not provided by Equinix, including selection, compatibility, monitoring and troubleshooting; (iv) provide all required information during product enablement; (v) allow Equinix, without any liability or notice to the Customer, to allow duly authorized employees, agents, or state or federal police authorities to install equipment, make changes to Managed Firewall product, or intercept any information to the extent permitted by law; (vi) the customer will have 48 (forty-eight) business hours, counted from when the message is sent by Equinix , to express themselves on any failure or defect in the service enablement. After such period, if the Customer has not expressed otherwise, the services shall be considered fully enabled with retroactive billing from the date the enablement communication enablement was sent.

The Customer may not: (i) conduct any activity that may interfere with or harm any other Customer's service; (ii) take any action in order to circumvent payment to Equinix for the use of the Managed Firewall product.

Equinix Brasil is not responsible for: (i) the intrinsic operating characteristics of third party Managed Firewall software or systems used to provide the service; (ii) improper access to systems connected to the network filtered by the Managed Firewall service in cases where client-based Managed Firewall rules permit such use. In both cases Equinix will not be responsible for any damages caused to the customer or related third parties.

3. Service Level Agreement (SLA) - 99,95%

The purpose of this Service Level Agreement ("SLA") is to set measurable performance levels for the Managed Firewall product and specify the discount available to the Customer if Equinix cannot achieve those levels.

For the purpose of this SLA, and subject to the final paragraph of this section, "Unavailability" is defined as the length of time that failure of any Managed Firewall product component results in failure to access Customer data, measured from when Equinix is notified of the incident by the Customer or the actual start of the incident as mutually agreed upon between the parties, until the time that the service is no longer unavailable as confirmed by Equinix .

The maximum credit that Equinix will issue for each billing period is

one (1) monthly MRC for each Managed Firewall directly impacted by outages. The Customer must report unavailability and request a credit by contacting the Equinix Service Desk. Equinix may investigate and isolate the cause of unavailability during parsing of the request.

COUNTRY	SERVICES	MAXIMUM TIME FOR CRASH RECOVERY (CONTRACT MONTH)	MRC CREDIT FOR EACH MANAGED FIREWALL
BRAZIL	**Firewall**	22 minutes	Discount equivalent to 1 (one) day of service. Discounts equivalent to 1 (one) hour of service for each outage period of 15 (fifteen) minutes following the maximum agreed time

The SLA shall not apply (and Equinix will have no responsibility) if Unavailability: (a) is caused by circumstances beyond Equinix's reasonable control; (b) occurs during a scheduled maintenance window. The Equinix will ideally notify the Customer at least 15 (fifteen) days prior to any maintenance window, and at least 48 hours prior to imminent situations, and will make reasonable operational efforts to minimize the duration and impact of maintenance windows.

In addition, Equinix shall take the necessary measures to diagnose and fix any Managed Firewall product-related emergencies in order to restore the environment, and will make reasonable operational efforts to notify the Customer if an emergency might cause an outage.

Equinix reserves the right to make the necessary adjustments to ensure the stability and quality of services to all Customers, avoiding improper use or misuse of the product.

4. Modes

Firewall Throughpu

In the Managed Firewall Throughput the Customer's network is filtered through a Firewall system configured in High Availability using redundant Hardware to increase failure tolerance shared with other customers. The Managed Firewall Throughput system filters the communication of the Customer's equipment hosted in an Equinix Data Center with: Internet public network, remote private networks owned by the customer and connected directly to Equinix's Brazil network - if there are any -, and with the other customers using the service.

This service is sold in relation to the Throughput capacity of the Internet Bandwidth used, and the contracted capacity shall be specified in the Equinix Order approved by the customer.

The application of security policies on the Customer's network is made according to pre-established rules, which determine the filtering criteria of incoming and outgoing traffic. These may be established by the customer unlimitedly and are administered via Managed Services Portal.

In addition to network filtering, Managed Firewall Throughput allows for contracting the additional Client-to-Site VPN (Virtual Private Network) functionality, which is sold separately.

The Client-to-Site VPN for Managed Firewall Throughput establishes a secure connection over the Internet by using tunneling and encryption technologies to keep data traffic safe. The Client-to-Site VPN product has the following features:

- Used by customers who have already contracted Managed Firewall, this product encrypts the traffic between certain origins and the network servers, filtered by the Managed Firewall.
- Access to Client-to-Site VPN shall be performed through a software that will be automatically installed on the user's computer when first connecting to the VPN tunnel. The settings and access release to end users is performed via Managed Services Portal.
- This product is configured according to the maximum capacity of VPN users, incremented from 1 up to a maximum of 50 users.
- This product shall be charged for the number of users.

Additional desired functionalities shall be informed by the customers upon contract.

The Managed Firewall Throughput service has the following restrictions:

- The capacity limit per customer for purchase is up to 100 Mbps (one hundred megabits per second) of traffic. For capacities larger than 100 Mbps (one hundred megabits per second), we provide Virtual Appliance - Firewall or Security Hardware - Firewall. products.
- This product can only be used to filter physical or virtual equipment networks hosted in an Equinix Brazil data center. The shared solution applies to any level of Colocation.
- VoIP traffic or online games are not permitted.
- Log functionalities of Managed Firewall Throughput access rules are not available.
- Restriction of up to 50 (fifty) users for Client-to-Site VPN capability.
- It is not possible to use NAT (Network Address Translation).
- The bandwidth contracted by the CUSTOMER shall be applied to all contracted network(s) and bandwidth divisions shall not be allowed (e.g., half the contracted bandwidth for web access and the other half for e-mailing).

- If the customer has two or more active networks in the same Firewall, the bandwidth contracted shall be shared between these networks.
- A Customer's network IP shall be allocated in the Managed Firewall for Equinix's use.

5. Miscellaneous Provisions

This Policy and the Service Order requested by the Customer represent the complete agreement and understanding of the parties with respect to the subject matter herein and in the agreement, and supersede any other agreement or understanding, written or oral.