FINLAND MANAGED SERVICES
MANAGED FIREWALL POLICY

20 November 2019

This Finland Managed Services – Managed Firewall Policy ("Policy") supplements and sets forth additional terms and conditions governing the provision of the Managed Firewall, 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

24x7	This means 24 hours a day and 7 days a week.
8x5	This term refers to Office hours.
Acceptance	On completion of the Managed Firewall, the Customer accepts it by signing an acceptance protocol in a format determined by Equinix, in accordance with the Acceptance paragraph mentioned in this document. This is the point at which the Managed Firewall formally becomes operational.
Availability	The percentage of the total time, measured over a complete contract month, in which no Fault(s) in the Managed Firewall are recorded.
Complaint	An expression of dissatisfaction by the Customer about the Managed Firewall that does not involve a Fault or a Hindrance.
Emergency Repairs	Occasional and/or unplanned emergency repairs to prevent a Fault, also known as "Emergency Maintenance". Equinix has conducted a risk analysis from which it is apparent that the non-performance of emergency repair work presents a major risk for the Managed Firewall.
Fault	A Fault occurs if there is an outage in the Managed Firewall of at least 5 consecutive minutes. A Fault does not include: 1. An interruption due to Maintenance/or Emergency Maintenance, 2. Situations that are caused by actions of the Customer.
Freeze	Period associated with a special event during which the performance of Maintenance is not permitted. The performance of Emergency Repair work as a result of Faults, if this is necessary, is in principle permitted but may be deferred in consultation with the Customer. An important aspect is that the decisions on Freezes by Equinix must be approved by the Equinix management.
HA	HA or "High Availability" is met if the Managed Firewall has a secondary device paired online, meaning that if the main device goes offline for whatever reason, a secondary device will continue to work independently.
Hindrance	All situations in which the Service Levels are not fulfilled without intervention of a Fault.
Network	The active and passive components of the network services provided by Equinix.
Office hours	Work days between 8.00 am and 4.00 pm. Saturdays, Sundays and generally recognized public holidays in Finland are not work days.
Maintenance	The performance of work on the Managed Firewall to maintain the quality of the service or to enable extensions. The non-availability as a result of maintenance does not impair availability.
Priority	Defines the impact on the Availability in the categories critical, high, normal and low.
Reaction Time	The time between fault notification by the Customer and the first contact between Equinix and the Customer regarding the progress of Fault clearance.
Redundancy	Duplicate and optionally separated implementation of devices and/or wiring in order to increase Availability. The provision of redundancy does not change Repair Times.
Remote hands	Work performed at Equinix on request by the customer by Equinix employees (or contractors), also referred to as "Smart Hands".

Repair Time	The time measured and logged by Equinix between the Fault notification(s) by the Customer to Equinix or its confirmation by Equinix and the Fault cleared message from Equinix to the Customer (or the point in time at which Equinix tries to pass on the Fault cleared message). The Repair Time is independent of Redundancy.
SAL	Secure Access List – List with all technical and commercial contacts of the Customer.
Service Window	The time frame in which the Managed Firewall in compliance with the SLA is available for use.
ServiceDesk	First point of contact for incidents, changes, requests and questions.
Managed Firewall Fees	The Fees payable for the applicable calendar month for the Managed Firewall.
Managed Firewall	Managed Firewall consist of one or two (physical and/or virtual) devices which are located in Equinix IBX Centers.
SLA	The Service Level Agreement setting out the rights and obligations relating to the agreed service levels (the levels of quality of the Managed Firewall as delivered to the Customer).
Support Window	The time in which the Managed Firewall in accordance with the SLA is available and in which Equinix can be accessed to report Faults and deal with these.
Working arrangements	Supplementary operational agreements agreed in writing by the Customer and Supplier

Except where such terms are defined in this Policy, capitalised terms used in this Policy have the meaning given to them in the Agreement.

1.2 Set Up

In setting up the Managed Firewall, Equinix will proceed installation according to the Order.

Equinix will confirm when the setup of the Managed Firewall pursuant to this section is complete, and the delivery of the Managed Firewall commences in accordance with the Acceptance regime mentioned in this document.

Where a description of this Managed Firewall refers to the provision of another managed service, such other managed service shall be provided as an integral part of this Managed Firewall.

2. Customer Responsibilities

The provision of the Managed Firewall is dependent on the following Customer responsibilities and if the Customer fails to perform or fulfil the Customer responsibilities, Equinix will not be obliged to provide the Managed Firewall and may – if and when applicable (e.g. not in case the set-up does not include any Customer devices) - charge additional non-recurring Fees that are caused by or arise from such failure to perform or fulfil the Customer responsibilities:

A. Customer must provide all necessary information to enable Equinix to set up any required connections between Customer's Equipment and the Managed Firewall.

B. 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.

Equinix shall not be obliged to carry out any part of any Managed Firewall to the extent that Equinix is unable to carry out the same as a result of the Customer having failed to carry out any Customer dependency or having delayed in carrying out any Customer dependency.

Some aspects of the Managed Firewall should or can only be performed where Equinix representatives have discussed and/or agreed that aspect with a Customer Representative.

a. In the event that:

i) a Customer Representative and his/her contact details have not been notified to Equinix either on the relevant Order or via the Customer portal, or

ii) the Customer Representative is either not contactable or is unable to provide the necessary information or assistance, or

iii) the Customer Representative provides inaccurate information to Equinix,

Equinix shall take any action in relation to the relevant aspects as it in its sole discretion deems appropriate or practicable (which may include taking no action whatsoever). Equinix shall not be liable for anything arising from such action or inaction (including any failure to provide all or part of the Managed Firewall).

b. In the event that Equinix representatives receive conflicting or different instructions from various representatives of the Customer:

   i) Equinix shall be entitled to act on the instructions of the Customer Representative as opposed to any conflicting or different instructions from the Customer; and

   ii) in the absence of instructions from the Customer Representative, without prejudice to the paragraph above, Equinix shall take any action that it in its sole discretion deems appropriate or practicable (which may include taking no action whatsoever).

c. The Customer shall act promptly, reasonably and consistently in responding to Equinix and working with Equinix in order to agree any aspect of any Managed Firewall that is not agreed and expressly specified within (or incorporated within) the Order.

Where applicable, the Customer shall ensure that any firewalls or connectivity operated by the Customer or third party (e.g. at its own office(s)/site(s)) are functional, and are configured such that the Customer is able to receive each applicable Managed Firewall element.

Where applicable, the Customer shall ensure that any application hosted on an applicable Managed Firewall above the operating system level will not adversely affect the smooth- running of the Managed Firewall.

The Customer shall notify Equinix of any problem with the Managed Firewall of which it is aware, including where Equinix's obligations would not in themselves necessarily make Equinix aware of such Managed Firewall problem.

In the event that the Customer does not receive an internet connectivity service from Equinix directly, 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 be able to carry out its obligations.

3. Charging Methodology

Fees for the Managed Firewall are further described in the Order.

4. Service Level Agreement and miscellaneous

4.1 Hardware

Where Equinix provides or makes available items of hardware specified in an Order, the provision and use of such hardware shall be subject to any terms and conditions provided to Equinix by the third party supplier or manufacturer of such hardware (the "Vendor"). However, in the event of any conflict between the provisions of this Policy and such terms and conditions, the provisions of this Policy and the Agreement shall prevail.

Equinix has no liability for any failure or delay or partial performance of the relevant Managed Firewall to the extent such liability arises from any failure or limitations of any hardware that is specified in an Order and which is obtained from a Vendor, and any related software, patches or other items provided by a Vendor unless that software is misfunctioning causing upgrade failures to hardware devices. In the latter case liability between Customer and Equinix is limited to the limitation of liability agreed upon with the Vendor by Equinix.

In relation to any hardware made available by Equinix under an Order, Equinix reserves the right to upgrade or replace such hardware with a different model with substantially the same or better functionality on any reasonable grounds. The content of the Order shall hereby be deemed to be varied in the event of such upgrades or replacements, in the absence of a formal contract variation or binding change control notification.

4.2 Relationship with Colocation Services and Network Services

Where hardware is specified to be provided by Equinix, it shall be racked in an Equinix Data Center (IBX) specified in the Order and the Colocation Service shall apply accordingly. The Customer acknowledges that the provision of hardware and a Managed Firewall may affect the Customer's power draw within a Data Center (IBX), and may use a small amount of Network Services bandwidth.

4.3 Maintenance

Equinix may carry out Maintenance (whether to physical and/or virtual devices, Equinix's IP network, the Data Center (IBX)Infrastructure or anything else) from time to time, if applicable. Maintenance work at the Customer end that may generate alarms may result in the Equinix Management Systems to be alarmed, must be reported in advance to the Equinix ServiceDesk. Any non-availability due to Maintenance shall not be included in the calculation of the Availability. The costs of work and associated travel costs for (planned/scheduled) Maintenance is included in the contract price, excluding Maintenance which might be caused by Customer actions.

Any specific agreements about Customer Freeze period must be set out in the Order.

Notifications of any Maintenance shall be made to the Customer Representative or any appropriate individual(s) notified to Equinix pursuant to the "Customer Contact Details" available. If the contact details provided by the Customer in relation to such individuals are missing or incorrect, Equinix shall not be obliged to make any notification pursuant from any Maintenance.

Customer must accept or can propose a new timeslot for Maintenance within 48 hours of the first notice thereto. If the Customer does not respond to the written notification within the aforementioned timeframe or if Equinix does not get any response, Parties agree that the proposed Maintenance timeslot is suitable for and accepted by the Customer.

Customer will be notified fourteen (14) days before Maintenance occurs. If Maintenance is performed sooner than the aforementioned fourteen (14) days, the timing of the Maintenance may be discussed with the Customer beforehand.

Equinix will send a Maintenance notice to the Customer which includes at least the following points:

- Type of Maintenance
- the starting time/date
- the duration of the activities
- the expected duration of non-availability
- the nature of the activities

4.3.1 Emergency Maintenance

Equinix may, if special circumstances in its opinion warrant this, carry out Emergency Maintenance.

Equinix will provide notification for the Customer as soon as reasonably possible, but any (repair or other required) work is allowed to start before the first notification is sent. Emergency repairs and the time required shall not be counted against Availability. Some internal criteria for the risk analysis to be performed by Equinix are: Service or devices have become “unmanaged”, there is a more than 75% chance that the service or equipment will cause a predicted incident within 72 hours.

The agreement between the Parties will be based on the risk assessment performed by Equinix that any delay of Emergency Maintenance does not further deteriorate or causes (additional) Faults in the provisioning of the Managed Firewall.

Equinix shall endeavor to give as much prior notice of Emergency Maintenance as reasonably practicable, if it is practicable to do so at all. Equinix shall use all reasonable endeavors to carry out any Maintenance described above without causing a Service Level Failure.

4.4 Incident resolution

Where an incident affects the provision of the Managed Firewall to the Customer in a manner where Equinix fails to comply with its obligations to provide the Managed Firewall, Equinix will use reasonable endeavors to resolve the issue as soon as practicable where it is within Equinix’s control to do so. Until resolution, Equinix shall escalate such issues internally according to its internal priority and escalation policy in place from time to time.

When Equinix is obliged to resolve service incidents, Equinix shall:

- notify the Customer of the incident as soon as reasonably practicable after Equinix is aware of it; and
- provide updates to the Customer on incident resolution progress.

Updates provided by Equinix shall be provided whenever reasonably practicable to do so or as soon as reasonable in all the circumstances after the initial notification or previous update. Updates shall include as much of the following information (without limitation) that is reasonable for Equinix to provide in all the circumstances:

- the Managed Firewall affected;
- the start time of the incident;
- the current status of the incident resolution; and
- a description of the incident.

4.5 Acceptance

The acceptance of the Managed Firewall shall be in consultation with the Customer. The delivery period starts after the Agreement signed by the Customer is received by Equinix. Equinix shall confirm the receipt in writing, including the day and/or week of delivery. Equinix shall promptly report any likelihood of the delivery date being exceeded. The delivery periods and conditions are stated in the Order.

If and when the Customer 1) does not respond within two (2) weeks after the Managed Firewall has been delivered and/or 2) the Customer uses the Managed Firewall, the Managed Firewall is considered to be Accepted by the Customer. Small deficiencies and/or defects that do not prevent the Customer from using the Managed Firewall will not withhold the Customer from Acceptance.

4.6 Availability

Equinix shall, after Acceptance, make the service specified in the Order available, in compliance with the Agreement and SLA. The Managed Firewall is defined as available if:

- the Managed Firewall is provided in accordance with the service levels under this Agreement and the SLA ;
- the Customer has identified a Fault but Equinix has not yet been notified thereof;
- the Customer has reported a Fault and it appears from an investigation that this was not the case. In this case, the Customer will be invoiced for investigation costs in compliance with section Expenses;
- the service is not functioning or incomplete due to the actions or omissions of the Customer. In this case, the Customer will be invoiced for investigation and repair costs in compliance with section Expenses;

The Managed Firewall is regarded as unavailable if the Customer reports a Fault. Equinix shall open a “incident ticket” in this regard. The Managed Firewall remains unavailable for use until Equinix confirms the Fault by telephone, on request by e-mail, as cleared to the Customer.

4.7 Fault management

Faults in the Managed Firewall can be reported by the Customer 24 hours a day, 7 days a week to the ServiceDesk. Faults that can be detected by the Customer shall only be reported by the authorised persons. The authorised persons should state the service name in which the Fault has allegedly occurred. Faults must be notified by telephone to the Equinix ServiceDesk, where fault clearance is coordinated. This notification marks the start of the Fault. After the Fault has been notified by telephone, the Customer will be informed about the nature of the Fault and its expected Repair Time. The Customer shall receive a ticket number on reporting of a Fault. The Customer must state this ticket number with all related contacts with Equinix. The Customer shall provide Equinix with any required assistance to expedite the Repair Time. This shall include the provision of clear and relevant information.

Immediately after the Fault has been cleared, Equinix shall notify the Customer thereof by telephone, and, on request, confirm by email. The Customer shall promptly, and no later than 30 minutes after notification of Fault clearance, notify Equinix by telephone if the Customer has not actually experienced Fault clearance. If the Customer indicates that the Fault has not been cleared within 30 minutes, this does not count as a new Fault .

If Equinix determines that the cause of the Fault is not in its own Managed Firewall, systems or network, the Customer will be notified of this by telephone with, on request, confirmation by email. The Customer will be required to take corrective action itself in those circumstances. Equinix will provide assistance for this purpose if and when requested against smart hand Fees.

For the avoidance of doubt, Equinix monitors the Managed Firewall and may receive alerts if a Fault occurs. In such case as described above, Equinix may inform Customer about the Fault.

Equinix is not liable if the Fault is due to:

- Acts or omissions by the Customer that cause Faults.
- Customer over allocates storage.
- Customer over allocates dedicated host resources when HA requirements are not met.
- Force majeure.

4.8 Accuracy of information

The Customer bears responsibility for providing correct and up-to-date information to Equinix for the Secure Access List.

4.9 Fault parameters

SERVICE & SUPPORT WINDOW

Service Window	24x7
Support Window	24x7

PRIORITISATION

Priority*	Impact on availability
Critical	The Managed Firewall (HA) is completely unavailable
High	The Managed Firewall (HA) is available with reduced functionality
Normal	The Managed Firewall (HA) is available but there is a risk of it becoming unavailable
Low	Work or change request

• Only applicable with HA setup. without HA set up Equinix will use reasonable endeavors to prioritize the impact and repair. However no credits apply and Equinix cannot be held liable for any damages.

FAULT REPAIR TIMES

PRIORITY*	PERFORMANCE OF WORK	REACTION TIME	REPAIR TIME
Critical	24x7	0,5 hr	4 hrs
High	24x7	1 hrs	8 hrs
Normal	Office hours	8 hrs	24 hrs
Low	Office hours	16 hrs	56 hrs

* Only applicable with HA setup. without HA set up Equinix will use reasonable endeavors to prioritize the impact and repair. However no credits apply and Equinix cannot be held liable for any damages.

MANAGED FIREWALL AVAILABILITY PERCENTAGE (ONLY APPLICABLE WITH HA SETUP)	SERVICE CREDIT
Less than 99,982%, but greater than or equal to 99,741%	Credit equivalent to 10% of one month´s fee for the Managed Firewall payable under the Order
Less than 99,741%, but greater than or equal to 98,70%	Credit equivalent to 20% of one month´s fee for the Managed Firewall payable under the Order
Less than 98,70%	Credit equivalent to 50% of one month´s fee for the Managed Firewall payable under the Order

If the Managed Firewall Availability percentage is less than 98,70% for two consecutive months, Customer is allowed to terminate the relevant Managed Firewall Order before the end of the term but within 30 Business days after the event occurred.

The aforementioned service credits are the sole & exclusive remedies for any Fault related to the Managed Firewall Availability

4.10 Escalation procedure

Equinix uses escalation procedures to ensure that complaints about requests/deliveries and complaints about the handling of Faults are given sufficient attention and priority. This is designed to ensure that Faults are cleared quickly and effectively and any specific arrangements about the situation can be made with the Customer.

Escalation requests concerning handling of Faults can be submitted by telephone to Equinix 24 hours a day, 7 days a week, by the responsible and authorized contact person designated by the Customer. The Customer must state the relevant ticket number for fault escalation requests.

Escalation requests concerning queries, supplies or other administrative matters can be submitted by telephone during Office hours to the Equinix Service Desk.

4.11 Service Desk

The Equinix Service Desk can be contacted 24x7. The Service Desk will create a ticket and/or directs calls to the designated person. The Service Desk contact details are made available to the Customer.

4.12 Managed Firewall Reports

Equinix will provide reports about Faults if these require escalation. The Customer may submit a request for such a report within 10 days of Fault clearance, citing the corresponding Fault ticket number. In this case, Equinix will issue an “escalation report” within 10 working days of the request.

4.13 Expenses

If Equinix incurs expenses in the investigation of a Fault as described in the section Fault Management, Equinix is entitled to invoice the (investigation) costs by means of a (supplementary) invoice against smart hand fees.

4.14 Entire Agreement

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.

ATTACHMENT A: ACCEPTABLE USE POLICY ("AUP")

1. This AUP is intended to protect Customer and the Internet community from the inappropriate use of Equinix's computing/ network services and the Internet.

2. Customer, and its end users or any third party that uses its services, must not:-

   a. use the Services to accept, transmit or distribute unsolicited bulk data (which includes, without limitation, e-mail, bulletin boards, newsgroups, software, files) or otherwise send, or facilitate the sending of unsolicited commercial email and mail bombs to any person or system in a way that could be expected to adversely impact Equinix's network or facilities, or may potentially encroach on a third party's intellectual property rights or any rights of publicity or privacy; The only circumstances in which the Services may be used to send unsolicited data of an advertising or promotional nature is where the unsolicited data is sent to persons with whom the sender has a pre-existing business, professional or personal relationship or to persons who have previously indicated their consent to receive data from the sender from time to time, for example by ticking a box to that effect on the sender's web site. Unless these requirements are met, users must not send unsolicited bulk data through the Services. If these requirements are met, the user must also provide an unsubscribe function on their web site (and make this function known to recipients in the relevant data) which allows those recipients to be removed from that mailing list;

   b. attempt to connect to any third party systems without prior permission or arrangement;

   c. use the Services in a manner which is intended to abuse or to violate the property rights of others, including, without limitation, activities which result in the distribution of viruses, worms, time bombs, Trojan horses, cancelbots, or other destructive activities like Denial of Services attacks, or scanning or any form of probing/ automated network status polls / information collection of a third party's network / system without prior permission, intentional or otherwise;

   d. use the Services to conduct any other activities, which in Equinix's discretion are considered detrimental to its customers and/or its own operations;

   e. Use the Services to:

      i) send data, or cause data to be sent, to or through Equinix Connect that hides or obscures the source of the data, that contains invalid or forged headers or domain names or deceptive addressing; and

      ii) relay data from a third party's mail server without permission or which employs similar techniques to hide or obscure the source of the data; and

   f. violate or attempt to violate the security of the Services, including without limitation, attempting to interfere with, disrupt or disable services to any user, host or network, including but not limited to via means of overloading, "flooding", "mail bombing" or "crashing".

3. Customer must immediately notify Equinix of any unauthorized access or attempted breach of security and may report violations of this AUP by notifying:

   EMEA: the Equinix European Network Support Engineering Team ("EU NSE") through the local IBX Center or by email at abuse@ap.equinix.com.

   Asia-Pacific: the Equinix Computer Security Incident Response Team ("CSIRT") through the local IBX Center or by email at abuse@equinix.com.

   North America: the Equinix Service Desk ("ESD") through the local IBX Center or by email at abuse@equinix.com.

4. Each Customer is responsible for ensuring that Customer's Equipment is configured in a secure manner. Customers should not, through action or inaction, allow others to use its network for illegal or inappropriate activities.

5. Equinix will not be obliged to intervene in the event a host or network address which is assigned to Customer is being blocked or blacklisted by other internet service providers or policing bodies.

6. Upon discovery of a security breach affecting a Customer, or upon the ESD, EU NSE or CSIRT (as applicable) being notified about a security complaint affecting Customer, Customer must take immediate steps to rectify the compromised systems. It is Customer's responsibility to ensure that all its computers and network equipment, as well as Customer's Equipment that utilizes an Equinix assigned network address is, in the opinion of Equinix, reasonably free from viruses, worms, trojan-horses, scanning codes and other malicious systems/software.

7. For event(s) that do not critically impact on the operations of Equinix's network or other customers' systems, Equinix will issue written notice to Customer regarding any violation of the AUP. Customer will make all necessary rectification to Customer's equipment within fourteen (14) days from the date of Equinix's notice.

8. For event(s) that critically impact on the operations of Equinix's network and/or other customers' systems, Equinix may, at its sole discretion, remove or disable Customer's network connections, block network addresses, or suspend all Services to Customer with or without prior notice to Customer. Service suspension under this paragraph will not prejudice any of Equinix's rights or remedies under the Agreement or otherwise.

9. Equinix will not be liable for any loss, expense, costs or damages of any nature suffered by Customer resulting in whole or in part from Equinix's exercise of its rights under this AUP. By using the Services, Customer agrees to waive and hold harmless Equinix from any claims relating to any action taken by Equinix under this AUP including conduct of investigation, issuing of warnings, refusal to post materials, removal of material, or suspension or termination of services, or other appropriate action.