Managed Private Firewall (MPF) – Service Description

Version 1.2, March 2025

TABLE OF CONTENTS

Managed Private Firewall (MPF) – Service Description 1
Managed Private Firewall 2
Standard Service 3
Virtual Appliance 3
Administrator Console 4
Log Analyzer Console 4
Service Options 5
Security Subscription 5
Type 5
Log Storage Quota 6
Service Demarcation & Enabling Services 7
Service Items 8
Roles & Responsibilities 9
Onboarding 9
Acceptance Into Service 9
Operational 9
Incident Management 10
Service Requests 11
Reporting 13
Reporting & Analyzing 13
Security Events 13
Service Levels 14
Support 14
Availability 14
Other documentations 15
Where to find more documentation? 15
Where to find EMS policy? 15
Where to find official Fortinet documentation? 15
How to ask for help 15

Managed Private Firewall

With Managed Private Firewall, organizations and resellers can entrust the procurement, installation, configuration, and day-to-day management of the firewall and infrastructure to a team of specialized experts.

It's about focusing on what truly matters, business objectives, while maintaining a secure, impenetrable network environment.

Managed Private Firewall diligently monitors and manages incoming and outgoing network traffic, following customer-controlled firewall rule set. Our global team of technical experts provide guaranteed uptime, self-serve administration, and turnkey access to market leading technology.

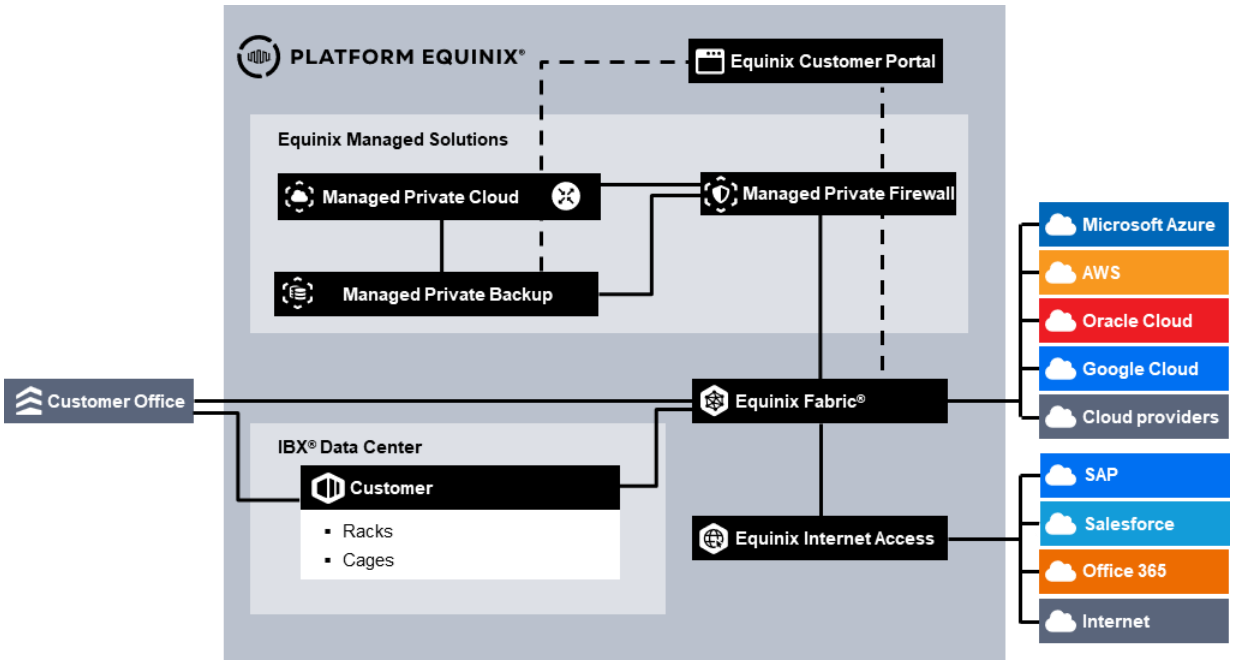
Managed Private Firewall is a virtual appliance built in a redundant configuration on High Availability digital infrastructure, ensuring accelerated time to market, eliminate logistical risk, and predictable expense management.

The benefits of the service include the following:

- Access to Market Leading technology.
- No major investments upfront
- Easy and quick upscaling of the required capacity
- Choice of additional functionality on top of the Next-Generation Firewall, such as Intrusion Prevention and Threat Protection.
- Self-service portal for policy configuration and access to reporting.
- High availability through an active-passive firewall pair setup.
- Managed by an experienced and certified Equinix Security Team.

Availability of the Managed Private Firewall service is subject to geographical availability. Further described in the “Geographic Availability” paragraph.

The figure below shows how applications hosted on Managed Private Cloud are protected with the Managed Private Firewall and how users on Equinix Fabric can securely access the applications and systems. It also shows the access for self-service and logging.



The Managed Firewall, which is by default a high availability pair, has two virtual domains (VDOMs):

- Customer domain
- Monitors and controls the traffic between the different trusted and untrusted network segments. This is the actual Customer Firewall.
- Management domain
- Used for management, only connected to the Equinix management environment. There is no connection between customer traffic and Equinix Management traffic.

In above example your applications are hosted on the Managed Private Cloud. The Firewall (customer domain) controls access to and from the Internet, the wide area network (WAN) and the network segments in Managed Private Cloud, based on a rule set which is configured via the self-service portal and/or a change request.

The Central Management System, which includes a self-service management portal and Analyzer Portal uses a Management ADOM to manage the customer's Firewall (Customer VDOM).

The Analyzer system collects logging and events information to provide online and real-time visibility via the portal.

Optionally logging information from the Customer domain can be send to an external SIEM system, so you can combine the information with the security logging and events from your other systems for wholistic security monitoring.

Standard Service

The standard service includes the following:

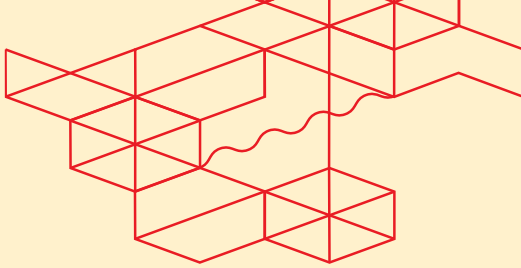
- The firewalls are deployed in an active-failover high availability pair in a single IBX offering at least 99.95% availability.
- Standard Logging is included
- Configuration of two usable network interfaces; dual-Homed Internet Access/WAN connectivity requires more interfaces.
- Routing is done with the default routing protocol BGP or static routing.
- Setup of the Self-Service and Analyzer Portal
- Regular patching and updating of the firewall(s).
- 24x7 monitoring of the firewall(s) uptime.
- Incident Management & Support
- Priority 1 Incidents: 24x7
- Priority 2 and 3 Incidents: Business Hours
- Service Requests: Business Hours
- The Firewall functionality is included in all subscriptions. It offers standard firewall service which are described in more detail (see Service Options).

Virtual Appliance

MPF is based on a high available active-passive virtual appliance pair, which is installed on top of the Managed Private Cloud platform in an Equinix IBX. We offer different performance options to accommodate different throughput requirements.

This variant includes:

- The needed vCPU, vRAM and storage resources required for the ordered performance option.
- Configuration of the resources.
- Installation and configuration of the HA Virtual Firewall pair in an IBX as set out in the order.
- Access to the Self-Service Portal and Analyzer Portal.



Administrator Console

The standard service uses a central self-service portal, technically defined as an administrative domain (ADOM). The ADOM enables the customer's Firewall administrator to create, delete and change firewall rules and policies as well as administer Virtual Private Networks specific to their Virtual Appliances

Log Analyzer Console

The standard service uses a central log-analyzer that customers access via ADOM. This console enables the customer's Firewall administrator to control log management, analytics, and reporting. The Log Analyzer Console, which is separate from Network Console, ensures the Customer's administrators can automate, orchestrate, and respond to logged events.

Service Options

The following Service Options can be ordered.

Security Subscription

The standard service is based on the Firewall license (see Standard Service). As a chargeable option also the IPS license or ATP/UTP bundle can be selected. See below table for the different features which are unlocked by these licenses.

LICENSE	DESCRIPTION	FEATURES
FW	Standard Service	Firewall
IPS	Intrusion Prevention Services	Firewall Intrusion Prevention Services
ATP	Advanced Threat Protection	Firewall Intrusion Prevention Services Advanced Malware Protection Service App Control
UTP	Unified Threat Protection	Firewall Intrusion Prevention Services Advanced Malware Protection Service App Control Web Security

Firewall

The Firewall functionality is included in all subscriptions. It offers the following functions and features.

- Network Interfaces
- Policy/Rules (Firewall Rules)
- Security Profiles (default “out-of-the-box” profiles)
- VPN IPsec
- VPN SSL (Web & Tunnel)
- NLB (Network Load Balancing)
- DoS Policy (L3/4 Anomalies)
- Logging (Analyzer)

IPS

Intrusion Prevention Services (IPS) protects against new and existing vulnerabilities and detects, and blocks known and zero-day threats. It also helps with Network-based virtual patching and detects hidden malware, ransomware, and other HTTPS-borne attacks.

Advanced Malware Protection Service

Antivirus, Botnet IP/Domain Security, Mobile Security, Sandbox Cloud, Virus Outbreak Protection, and Content Disarm & Reconstruction.

App Control

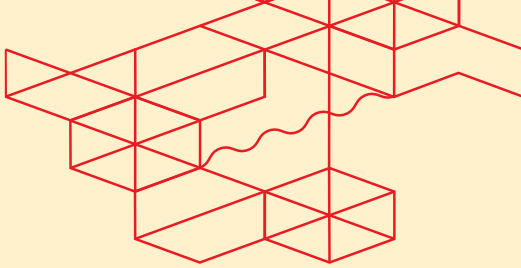
Application Control allows quick creation of policies to allow, deny, or restrict access to applications or entire categories of applications.

Web Security

Web Content Filtering controls access to web content by blocking web pages containing specific words or patterns. This helps to prevent access to pages with questionable material. Words, phrases, patterns, wildcards, and Perl regular expressions can be specified to match content on web pages.

Type

You can select from a range of Virtual Machine resource options conducive to the required throughput.



Performance options

The performance of the firewall in terms of Gbps throughput depends on the license selected, the vRAM and vCPU resources assigned to the virtual appliances and the features enabled on the firewall. The performance options range from Small (S) to Extra Large (XL). Below table gives an indication of the performance and the resources required.

	VM Resources[1]		Maximum Throughput in Gbps[2]		
Size	vCPU	vRAM	FW[3]	IPS[4]	ATP/UTP[5]
S (small)	2	4	7	1.7	0.9
M (medium)	4	8	10.8	3.3	1.8
L (large)	8	12	14	5.9	3.4
XL (extra-large)	16	16	15.5	10.1	6.3

[1] VM Resources are included in the service.

[2] Maximum throughput is the total incoming and outgoing amount of traffic ("throughput") that the firewall can handle. The displayed values are based on test data from the supplier. Depending on the set of rule sets, the functionalities used and the specific traffic of the customer, the maximum capacity achieved may differ. It is an estimation.

[3] Firewall throughput has been measured with UDP (512 byte) packets.

[4] IPS performance was measured with Enterprise Traffic Mix.

[5] Threat protection performance has been measured with IPS and Application Control and Malware protection, based on Enterprise Traffic Mix.

Log Storage Quota

Retained for 60 days, up to 1GB log data per day to a total of 10GB log data storage is included in the “Standard Logging” service per Managed Private Firewall Service pair. This log data can be used for security analyses and/or retention purposes. If a customer wishes to store more log data, this can be ordered as “Extended Logging”.

Service Demarcation & Enabling Services

The border between customer & Equinix environment.

Equinix is solely responsible for the Standard Service and combination of Service Options as set out in the Order(s) and subsequent Service Requests.

Equinix is not responsible for any client software or Internet connectivity to either manage or use the Service.

For the Virtual Firewalls the following service boundaries apply:

- Logical network interfaces on the Firewalls for production traffic
- UI and API for the Network and Analyzer Consoles

More details about demarcations can be found in the Roles and Responsibilities section of this document and in the Product Policies.

The Managed Private Firewall can only be ordered in combination with MPC (Managed Private Cloud) and as such act as a security component in a solution.

Service Items

When ordering the Managed Private Firewall service, choose the variant that best suits the requirements. The MPF Service is charged based on Baseline values. Refer to section 2 for an explanation of each variant.

Charge types

Baseline – the specific volume of Unit of Measure of the Service as defined in the Order.

Catalog of billing items

CATEGORY	PURCHASE UNIT	UOM	INSTALL FEE	BILLING METHOD	OVERAGE
MPF SERVICE	[FW-TYPE] [FW-LICENSE] [LOG STORAGE QUOTA]	Each	Yes	Baseline	No

Roles & Responsibilities

Onboarding

Installation

ACTIVITIES	EQUINIX	CUSTOMER
Schedule / execute project kickoff meeting	RA	CI
Schedule / execute customer onboarding	RA	CI
Virtual Machine resources (compute, storage, and networking) for the virtual firewall on MPC	RA	I
Virtual Firewall appliance software, licenses, and support	RA	I
Equinix management environment for firewall management including Network Console and Analyzer Console	RA	I

Configuration

ACTIVITIES	EQUINIX	CUSTOMER
Firewall-appliance basic configuration, Network interfaces, network settings and hardening	RA	I
Set up firewall monitoring and logging to Analyzer Console	RA	I
Setup customer accounts on portal for access to logging, reporting and self-service	RA	CI
Defining initial firewall ruleset	CI	RA
Loading initial firewall ruleset through Network consoles	CI	RA
Loading initial firewall rule-set trough Service Request	RA	CI

Acceptance Into Service

ACTIVITIES	EQUINIX	CUSTOMER
Test access to MPF Product page on Managed Solutions Portal	CI	RA
Test access to MPF documentation on docs.equinix.com	CI	RA
Test access to MPF operational console	CI	RA
Testing the configuration and failover as part of operational management	RA	CI
Functional testing	CI	RA

Operational

ACTIVITIES	EQUINIX	CUSTOMER
Technical management of the service (overall)	RAC	I
Functional management of the customer environment within the service (overall)	I	RAC
Service desk	RA	CI
Maintenance of the firewall-appliance (infrastructure break / fix, software updates, security patches)	RA	I
24x7 uptime monitoring of the virtual firewall including health checks	RA	I

Back-up and management of log files and rule base	RA	I
Submitting Service Request via the Portal	CI	RA
Implementation of Changes in accordance with change process based on Service Requests	RA	CI
Interpretation of security events		RA

For the avoidance of doubt the customer is responsible for the firewall rulesets and policies, optional VPN-connection configuration, and server load balancing configurations, Equinix will implement changes only based on Customer instructions.

Note: RACI stands for Responsible, Accountable, Consulted and Informed.

Incident Management

Incident management is included in service support. All incidents are handled based on priority. Priority is determined after the failure has been reported and assessed by Equinix based on the provided information.

PRIORITY	IMPACT/URGENCY	DESCRIPTION
P1 High	Unforeseen unavailability of a service / environment delivered and managed by Equinix, in accordance with service description due to a disruption. The user cannot fulfill its obligations towards its users. The user suffers direct demonstrable damage due to the unavailability of this functionality.	The service must be restored immediately; the production environment(s) is/ are unavailable, with platform-wide disruptions.
P2 Medium	The service does not offer full functionality or has partial functionality or a reduced performance, because of which the users are impacted. The user suffers direct demonstrable damage due to unavailability of the functionality. The service may be impacted due to limited availability of this functionality.	The service must be repaired the same working day; the management environment is not available.
P3 Low	The service functions with limited availability for one or more users and there is a workaround in place.	The moment of repair of the service is determined in consultation with the reporting person.

Note: This classification does not apply to disruptions that are, for example, caused by user-specific applications, actions by the user, or dependent on third parties.

The incidents can be submitted in the ECP in the Managed Solutions section.

P1 incidents need to be submitted by phone.

Service Requests

Service Requests are used to report an issue with the service or when there is a need to implement or assist with the implementation of a change.

Customers can raise a Service Request for configuration changes that cannot be implemented through Self Service in the Operational Console, or if they require assistance with implementation of changes via the Operational Console.

There is 24x7x365 support for the Managed Private Firewall Service.

There are two types of service requests available:

- **INCLUDED**: Service Requests which are in scope of the Service, and as such, no additional charges apply.
- **ADDITIONAL**: Service Requests which are out of scope of the Service, and therefore additional charges apply.

Guidance is available to be provided for all Service Requests that can be executed through self-serve, meaning we will provide procedural instruction and oversee the customer's execution of the task.
In addition to the standard service and if the appropriate service option(s) have been selected the following functionality / configuration can be requested either at installation or via Service Request as a chargeable option.

- **Add/Remove Additional Network** As standard the Firewall is configured with up to two subnets, with this option additional subnets can be added, for instance to provide an additional DMZ, firewalling between different tiers or an additional WAN connection.
- **Guided assistance to Add/Remove/Change Policy/Rule(s)** in rule base and/or include Security Profile (Maximum 5 rules per service request).
- **Guided assistance to Add/Remove/Change Security Profile (Additional/Custom)** Creating customer security profiles; (IPS, Web filtering etc.); A valid Subscription is needed.
- **Guided assistance to Add/Remove/Change VPN (Site to site)** connections to realize a secure (encrypted) connection over the Internet between two locations or sites via Gateway-to-Gateway IP-SEC VPN.
- **Guided assistance to Add/Remove/Change VPN (SSL) connections** Secure user access over the Internet to the firewall protected systems using an SSL VPN. User authentication needs to be provided by a customer administered system or a supporting service.
- **Guided assistance to Add/Remove/Change Add SSL Certificate** Creation of a Certificate Signing Request (CSR) and implement the certificate.
- **Guided assistance to Add/Remove/Change Server Load Balancing** supports basic traffic load balancing across multiple backend servers, based on multiple load balancing schedules including Static (failover), Round robin, Weighted. Supports L3 (IP), L4 (TCP/UDP), L7 (HTTP, HTTPS, SSL/TLS, IMAPS, POP3S, SMTPS). SLB offloads most SSL/TLS versions up to TLS 1.3.
- **Guided assistance to Add/Remove/Change DoS Policy** A Denial of Service (DoS) policy can be enabled to examine network traffic arriving at a Firewall for anomalous patterns at layer 3 and layer 4, which usually indicates an attack. When selecting this option, the Default Thresholds will be configured.

Some changes can be implemented via self-service as indicated in the table below or can be requested to be implemented by Equinix through the service portal as a Service Request.

TYPE OF CHANGE	SELF SERVICE	INCLUDED/ ADDITIONAL
Add/Remove Additional Network (Interface)	No	Additional
Guided assistance to Add/Remove/Change Policy/Rule(s) (Maximum 5 rules per service request)	Yes	Additional
Guided assistance to Add/Remove/Change Security Profile (Additional/Custom) (Subscription needed)	Yes	Additional
Guided assistance to Add/Remove/Change VPN (IPsec/S2S) (Maximum 3 VPN Tunnels per service request)	Yes	Additional

Guided assistance to Add/Remove/Change VPN (SSL) (Creation of certificate excluded). One change per Service Request	Yes	Additional
Guided assistance to Add/Remove/Change SSL Certificate	No	Additional
Guided assistance to Add/Remove/Change Server Load Balancing (Maximum 3 rules per service request)	Yes	Additional
Guided assistance to Add/Remove/Change DoS Policy	Yes	Additional

Customers can select changes which are not listed in the table above by selecting “change” at the service request module in the Managed Solutions Portal. Equinix will perform an impact analysis to determine whether the change can be implemented, to determine associated costs and lead time.

Any charges related to Service Requests will be deducted from the Premier Support Plan Balance (See the Service Description for Premier Support for more details), or in case of insufficient balance invoiced in arrears based on the prevailing rate.

Changes in the baseline capacity, amount ordered or any other change that will have an impact on the monthly service fee should be requested via the Sales team.

Reporting

Reporting & Analyzing

The customer can view and save reports on network traffic and security events via the console. The console offers a customizable, interactive dashboard which helps to quickly identify problems with intuitive graphs (see example in figure) of network traffic, threats, applications and more. It is a comprehensive monitoring system that integrates real-time and historical data into one overview.

Figure 2: Example of online reporting

Custom data reports can be generated using more than 70 built-in templates and more than 2000+ combined ready-to-use datasets, charts, and macros for analysis of anomaly detection, threat assessments, etc. These can be run directly (on-demand) or scheduled with optional automatic e-mail notifications. The format of the reports is flexible with a choice of PDF, HTML, CSV and XML and JSON.

Security Events

The customer's security teams can monitor and manage alerts and event logs from the firewall, with events processed and correlated in a format that analysts can easily understand.

Service Levels

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

Support

The SLA on support applies to the incident registration and resolution (see section 4.4 of this document).

PRIORITY	RESPONSE TIME[1]	RESOLUTION TIME[2]	EXECUTION OF WORK	SLA[3]
P1	< 30 min	< 4 hours	24 x 7	95 %
P2	< 60 min	< 24 hours	24 x 7	95 %
P3	< 120 min	< 5 days	24 x 7	95 %

Note:

Response time is from submitting the Trouble tickets and an Equinix Managed Solutions specialist sending a formal response.

Resolution time of a case is from registering to closing or cancelling the Trouble Ticket in the ITSM Tool or the hand over to IBX Support.

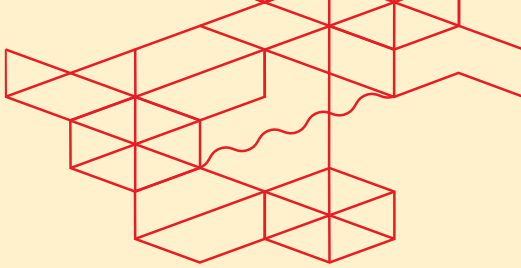
SLA applies to the response time, details on the SLA can be found in the Product Policy.

Availability

The MPF service is deemed "**Unavailable**" when customer firewall policies and/or rules are not applied to the traffic passing through the firewall for more than 5 minutes.

AVAILABILITY SERVICE LEVEL	DESCRIPTION
99.95%+	This is met by achieving less than twenty-two (22) minutes of Unavailability of the Firewall Service over a calendar month period.

A Service credit regime on the availability SLA is described in the Product Policy, as well as how to calculate SLA's and what exclusions are applicable.



Other documentations

Where to find more documentation?

You will find the most up to date documentation on docs.equinix.com website.

Where to find EMS policy?

You will find it on our website.

Where to find official Fortinet documentation?

You will find it on https://docs.fortinet.com

How to ask for help

Please make sure to open a ticket every time you need help. This is your guarantee that the right team has received your request and will work on that under the expected SLAs.

