Business Services

PUBLICATION 1 SERVICE DESCRIPTION FOR FLEXIBLE SECURITY PLATFORM SERVICE

1.1 Definitions

All capitalized terms used but not defined herein will have the meanings given to such terms elsewhere in the Agreement. In the event of any conflict between the definitions provided in this Service Description and those provided elsewhere in the Agreement, the definitions in this Service Description will control for purposes of this Service Description.

"**Administrator**" means the individual assigned by the Customer to administer the Service (as notified to Orange).

"**Customer Security Policy**" means the security policies set by Customer that enforces the rules for transit traffic into its network at the application level, as well as at the port and protocol level.

"**Firewall**" means a system installed between Customer's internal network and external network, for controlling incoming and outgoing connections to keep information exchanges secure.

"**FSP**" means Flexible Security Platform.

"**FSP Portal**" means the security web portal (which Customer may access through MSS) that the Administrator may access using a secured token provided by Orange, where subscription of the features and configuration of the Service are managed, and where reports and logs regarding the Service can be retrieved.

"**GCSC**" means Orange's Global Customer Support Center.

"**Incident**" means a fault, failure, or malfunction in the Service.

"**Log**" means the automatically produced documentation of events to the FSP, where events are in reference to any identifiable occurrence that has significance for the FSP.

"**My Service Space**" or "**MSS**" means the Orange web portal which allows Customer to report and track Incidents, obtain information regarding the inventory of the Service, monitor and obtain reports for the Service, using a login name and password provided by Orange when the Service is implemented. MSS support is provided only in English.

"**NGFW**" means Fortinet Next Generation Firewall, which comprises a hardware or a software based network and application security system that is able to detect and block attacks according to the Customer Security Policy.

"**Service**" means the FSP service, as described in this Service Description.

"**Service Request Form**" or "**SRF**" means the form provided by Orange on which Customer details its specific needs for the Service.

1.2 Service Overview

The Service only provides the features and functionality set forth in this Service Description. FSP is a network and corporate Internet access security managed service based on ITIL V3 processes and is fully installed, supervised and maintained by Orange. It comprises (a) the NGFW to protect inbound and outbound network traffic ("**Core FSP Service**"), and (b) customizable features that can control bandwidth (only for FSP Cloud); authenticate users, applications and websites; clean up browsing and messaging traffic; and protect against intrusion attempts on network and server levels.

The FSP Portal allows Customer to subscribe to features of the Service, configure the security parameters, and view the reporting of the Service.

FSP Service is available either in the Orange cloud ("**Cloud FSP**"), or on Customer's premises ("**Local FSP**").

1.3 Platform Architecture and Features

1.3.1 Cloud FSP

Cloud FSP is a solution where the FSP is hosted in an Orange data center and is available only in the European countries identified by Orange.

Connection between the network of Customer and the FSP can be established via Orange Business VPN access (Galerie access required) or Orange Internet access (both of which are described in separate Service Descriptions and are subject to additional Charges), or any Internet access provided to Customer by a third party.

If Customer uses third party Internet access, then the connectivity between Customer's Location and the FSP will be done using an Internet Protocol Security (IPSec) Tunnel, which Customer will provide and for which Customer will be responsible (including all regulatory or other government approvals to use IPSec-enabled devices, etc.). Orange will not be responsible for any failure or delay in the Service caused by such IPSec Tunnel.

Customer will specify in the Order the Internet bandwidth it requires to use the Service made available by Orange within the Orange data center as part of the Service between the range of 5 Mb and 200 Mb. Any change to the Internet bandwidth within 20% of the originally stated range is done via the FSP Portal.

1.3.2 **Local FSP**

Local FSP is a solution where the dedicated FSP device (provided and owned by Orange) is hosted at the premises of Customer. The device capacity is dependent on the maximum Firewall throughput specified by Customer, as per the categorization below:

Category of Devices	Maximum Firewall-Only Mode Throughput	Maximum Throughput-including all optional features enabled, excluding SSL Inspection
Small	80 Mbps	25 Mbps
Medium	200 Mbps	60 Mbps
Large	600 Mbps	200 Mbps
Very large	1,000 Mbps	400 Mbps
X large	5,000 Mbps	1,000 Mbps
XX large	9,000 Mbps	3,000 Mbps

Internet access and bandwidth control is not included in the Service.

1.3.3 **Optional Features for Cloud FSP and Local FSP**

The following are optional features of the Service that Customer can subscribe to, subject to additional Charges. Unless otherwise specified, the optional features can be subscribed to and configured by Customer via the FSP Portal.

Optional Features:

(a) **Authentication:** The Authentication feature allows authentication to be performed by Customer applying the Internet browsing rights according to the settings determined by the Administrator.

Authentication can be either:

- internal, using the internal database of the Service to manage the User or User group, or
- external, using an external directory (e.g. Active Directory or Lightweight Directory Access Protocol) to manage the User or the User group.

(b) **Internet Protocol Security (IPsec) Tunnel:** The IPSec tunnel feature allows the establishment of a site-to-site IPsec tunnel between multiple Locations or third-party tunnel termination. In case of a third party tunnel termination, Customer is accountable for the configuration of the device.

(c) **Secure Sockets Layer (SSL) VPN Remote Access:** The SSL VPN Remote Access feature allows Users to access Customer's internal network resources via their mobile devices. This feature works through a **"Client Connection"** installed on the User's mobile device. The number of simultaneous connections is limited to a maximum of 30 concurrent User sessions. Customer must subscribe to the Authentication feature in order to activate SSL VPN Remote Access.

(d) **Web Filtering:** The Web Filtering (or Web Filter) feature controls access to Web services through a configurable URL filtering policy under the Customer Security Policy.

(e) **Application Control:** The Application Control feature allows the filtering of applications that pass through the Internet stream.

(f) **Anti-Virus**: The Anti-Virus option allows a systematic inspection of incoming traffic flows.

(g) **Intrusion Prevention System (IPS):** The IPS feature is used to detect and block malicious traffic or threat attacks, based on the Fortinet IPS databases of malicious behaviors and attacks.

(h) **Anti-Spam:** The Anti-Spam feature allows efficiency improvement of Customer's messaging system by applying spam management, which is based on the anti-spam database maintained by Fortinet.

(i) **Sandboxing:** The Sandboxing feature enables file content scanning and emulation to be conducted using Fortinet Sandboxing Cloud services. Suspicious files are sent securely via the Internet for further testing of the file(s). Customer may choose to send all files or only certain suspicious files for scanning, per the Customer Security Policy.

(j) **SSL Deep Inspection:** The SSL Deep Inspection feature allows Customer to decrypt packets and to analyze a potential threat. Any personal data processed in unlocking of the encryption is the sole responsibility of Customer.

(k) **Additional FSP Portal access:** The Additional FSP Portal Access feature allows Customer to obtain access to the FSP Portal for more than two Administrators. Subscription to this feature cannot be done through any Online Tools, including the FSP Portal. Instead, a physically signed Order from the Customer is required.

(l) **High Availability (HA):** The HA feature is available only for Local FSP. HA feature provides a secondary FSP device similar to the primary FSP device for redundancy, in the event Customer requires high availability of the Service.

In case of malfunction of the primary FSP device, the function will failover to the backup FSP device. This feature includes provision of network switches between the FSP device and the Customer network.

The HA feature comes in two architectures:

- Standard HA, with two Firewalls and two switches, one upstream and one downstream of the Firewalls;
- Premium HA, with one pair of switches located upstream of the Firewall, and another pair located downstream.

(m) **Demilitarized Zone (DMZ):** The DMZ feature is available only for Local FSP. It allows Customer to create secure areas which can be connected to Customer networks and resources, accessible according to Customer Security Policy.

1.4 Service Deployment

1.4.1 Initial Set-up

In order for Orange to configure the Service, Customer is required to complete the SRF. The SRF must be returned to Orange within two (2) weeks from the time it is provided to Customer. The initial set up of the Service will then be implemented by Orange based on the information provided by Customer in the SRF.

1.4.2 Device Installation for Local FSP

Unless otherwise agreed to by the Parties, installation required for Local FSP will be conducted during Business Hours. If Customer requests Orange to perform the installation outside of Business Hours, Orange will advise Customer of any increased charges prior to commencement of the installation.

Orange will not be responsible for any delay in the installation if such failure is due to any cause beyond its reasonable control, including Orange's inability to gain access to the Location as scheduled or Customer's failure to properly prepare the Location. If the Location is not ready for installation on the scheduled date, any rescheduling that requires Orange to either make more than one trip to the Location or remain at the Location and wait for the Location to be properly prepared will be billed at the Hourly Labor Rate, along with any Expenses incurred.

1.4.3 Acceptance Testing

Upon completion of the Service implementation, Orange will commence acceptance testing, during which all aspects of the FSP device and the Service are confirmed to be operational in accordance with the terms set forth in this Service Description and the parameters set forth in the SRF. Upon completion of the acceptance testing, Orange will provide to Customer a "**FSP Service Acceptance Form**" listing the Acceptance Tests performed by Orange. Customer will be deemed to have accepted the Service on the date on which Orange issues the FSP Service Acceptance Form, unless Customer notifies Orange in writing of a material fault in the Service within five (5) Business Days of receipt of the FSP Service Acceptance Form. In such event, the above acceptance process will be repeated.

1.5 Flexible Security Platform Service Management

During the operational phase, Orange will provide the following:

(a) **Incident management:** Orange will detect failures in the Service and restore its operation as quickly as possible.

(b) **Problem management:** Orange will strive to prevent the same Incidents from recurring, and to minimize the impact of Incidents that cannot be prevented.

(c) **Change management:** Orange will apply a standardized methods and procedures for change requests.

(d) **Configuration management:** this process tracks all of the individual configuration items useful for the Service

(e) **Release management:** this process guarantees the integrity of the live environment and ensures the correct components are released.

(f) **Service Level Management:** Orange will monitor the service level committed under the Service Level Agreement.

(g) **Availability management:** this process aims to define, analyze, plan, measure and improve all aspects of the availability of the Service.

(h) **Continuity management:** this process aims to manage risks that could seriously impact the Service.

(i) **24x7 Customer support service:** Administrator may report Incidents related to the Service to the GCSC at any time by telephone or email. Administrator will need to provide the GCSC with full details of the Incident and the contact details so that Orange may contact him or her in the event any follow-up is necessary. When registering an Incident, the GCSC will provide Administrator with an Incident number and will carry out a periodic follow-up until the Incident has been resolved.

(j) **Centralized management:** Customer can assign up to two (2) Administrators to access the FSP Portal in order to subscribe and configure all optional features, check and download reports and logs. Via the MSS Portal, Customer can also make and follow up changes requests; as well as report and track Incident(s).

(k) **Logs management:** Logs captured on how the Firewall handles various types of traffic are stored on Orange storage system for twelve (12) months from the date of its creation. The Logs are available in the FSP Portal for one month, after which Customer can request for the Logs to be downloaded using a change request.

(l) **Report access:** security reports are provided within the FSP Portal. Customer can access to daily, weekly, monthly security reports. The monthly reports are stored online for 6 months. All reports can be downloaded using the FSP Portal.

(m) **Change implementation:** Customer may request changes to its options configuration via the FSP Portal. However, if Customer wants to modify the Firewall rules, or if Customer wants Orange to modify the Security Policies, a request must be made via the MSS portal. Customer can detail its needs using the change catalog. All changes are charged referring to the change catalog.

(n) **Change in Customer Security Policies:** Customer may request a change in the configuration following a change in its Customer Security Policies. Orange may advise of any potential inadvertent reduction in the security effectiveness as a result of the change, but in no event shall Orange be held responsible for any security lapses.

1.6 Order Term and Service Termination

Notwithstanding anything to the contrary otherwise contained in the Agreement (including the General Conditions or applicable Specific Conditions), each Order shall be valid for a minimum Order Term of thirty-six (36) months commencing on the Date of Acceptance ("**Minimum Order Term**"), and termination by Customer prior to the expiry of the Minimum Order Term shall entitle Orange to invoice Customer the total sum of the Service for the remaining unexpired Minimum Order Term.

1.7 Pricing and Billing

One-time Charges apply for the implementation to the core FSP Service and to each optional feature.

Monthly recurring Charges apply to the Core FSP Service and to each optional feature. For Cloud FSP, the Charges are subject to the subscribed bandwidth. For Local FSP, the Charges are subject to the category of the FSP device (as described in Clause 1.3.2 (Local FSP) above) installed on the Customer's premises or Orange data center.

Any change requested by the Customer to Orange via the Change portal shall be subject to additional Charges.

END OF SERVICE DESCRIPTION FOR FLEXIBLE SECURITY PLATFORM SERVICE