# 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 enforce 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 that the Administrator may access through MSS 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 (a) report and track Incidents, (b) obtain information regarding the inventory of the Service, and (c) 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 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.

"**SDN**" means Software Defined Networking.

"**Business VPN Galerie**" means Orange Business VPN Galerie service, which is described in a separate Service Description.

## 1.2 Service Overview

The Specific Conditions for Security Services apply to the Service. 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, as defined below); 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. The FSP Portal may be used by up to two (2) Administrators unless Customer subscribes to the Additional FSP Portal access optional feature.

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

## 1.3 Core FSP Service Platform Architecture & Standard Features

### 1.3.1 FSP Cloud

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

Connection to the FSP can be established via VPN access provided by Orange (Business VPN Galerie access required) as described in the Service Description for Business VPN Galerie or Orange Internet access (as described in the separate Service Description for Internet Direct or Vendor Managed Service Internet (as applicable), or any Internet access provided to Customer by a third party. Business VPN Galerie access or any Internet access provided by Orange will be subject to additional Charges.

If Customer provides Internet access for use with the Service using a third party Internet access provider, 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). Orange will not be responsible for any failure or delay in the Service caused by such Internet Protocol Security (IPSec) tunnel.

Customer will specify in the Order the Internet bandwidth it requires to use the Service made available by Orange within the Orange datacenter as part of the Service between the range of 10Mb and 400Mb (or such other range as may be identified by Orange from time to time). Customer may change the Internet bandwidth within 20% of the originally stated range via the FSP Portal.

### 1.3.2 FSP Local

FSP Local 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 throughput with all optional features enabled, excluding SSL Inspection | Maximum throughput with all optional features enabled, including SSL Inspection |
|---|---|---|
| Small | 40 Mbps | 10 Mbps |
| Medium | 60 Mbps | 20 Mbps |
| Large | 300 Mbps | 120 Mbps |
| Very large | 600 Mbps | 250 Mbps |
| X Large | 1,000 Mbps | 400 Mbps |
| XX Large | 4,000 Mbps | 1,500 Mbps |

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

### 1.3.3 FSP for Galerie

For FSP for Galerie, Customer must order the Orange Business VPN Galerie service separately. FSP for Galerie is a solution where the FSP is hosted in a SDN point of presence located in an Orange datacenter and is available only in the countries identified by Orange. It protects Business VPN Galerie traffic to cloud service providers selected by Orange for its Business VPN Galerie Service. For redundancy reasons, two virtual Firewalls are implemented by Orange on two different SDN POPs. Different levels of service are available, depending on the Business VPN Galerie bandwidth to be protected.

| Service Category | Maximum Galerie throughput with all optional features enabled, excluding SSL Inspection | Maximum Galerie throughput with all optional features enabled, including SSL Inspection |
|---|---|---|
| Small | 50 Mbps | 15 Mbps |
| Medium | 200 Mbps | 60 Mbps |
| Large | 450 Mbps | 125 Mbps |
| Very Large | 900 Mbps (or higher upon prior study) | 250 Mbps |

### 1.3.4 Optional Features for FSP Cloud, FSP Local & FSP for Galerie

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.

(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:

- 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 an IPSec tunnel between FSP and another site (Orange's or third party's). The optional IPSec Tunnel feature is distinct from the Internet Protocol Security (IPSec) tunnel described in Clause 1.3.1, if applicable.

In case of a third-party tunnel termination, Customer is responsible for the configuration of the FSP device.

For FSP Cloud, a cap of 20 tunnels applies. The IPSec Tunnel optional feature is not available for FSP for Galerie.

(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.

| Service Range | | Maximum Simultaneous Connections |
|---|---|---|
| FSP Cloud | | 200 |
| FSP Local | Small | 70 |
| | Medium | 100 |
| | Large | 150 |
| | Very Large | 200 |

| Service Range | | Maximum Simultaneous Connections |
|---|---|---|
| | X Large | 250 |
| | XX Large | 300 |

Customer must subscribe to the Authentication optional feature in order to activate SSL VPN Remote Access.

SSL VPN Remote Access is not available for FSP for Galerie.

(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.

Sandboxing is not available for FSP for Galerie.

(j) **SSL Deep Inspection:** The SSL Deep Inspection feature allows Customer to decrypt packets and to analyze a potential threat. Customer will be responsible and liable for any processing of personal data in connection with unlocking the encryption, notwithstanding anything to the contrary otherwise contained in the Agreement, and Customer will indemnify Orange from and against any and all Losses arising out of or relating thereto.

(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 FSP Local. 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 Orange's 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; or
- 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 FSP Local. It allows Customer to create secure areas which can be connected to Customer networks and resources, accessible according to Customer Security Policy.

(n) **Additional Public IP Address:** The Additional Public IP address feature is available only for FSP Cloud. It allows Customer to order additional public IP addresses in increments of either two or sixteen in addition to the four public IP addresses included in FSP Cloud.

## 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 FSP Local

Unless otherwise agreed to by the Parties, installation required for FSP Local 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, and Customer agrees to pay such increased charges if Customer approves Orange performing the installation outside of Business Hours.

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.

### 1.5 Flexible Security Platform Service Management

During the Service Term, Orange will provide Service Management subject to the separate Service Description for Service Management. In addition, Orange will provide 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 (1) month, after which Customer can request for the Logs to be downloaded using a change request.

### 1.6 Order Term & 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 & Billing

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

Monthly recurring Charges apply to the core FSP Service and to each optional feature. For FSP Cloud, the Charges are subject to the subscribed bandwidth. For FSP Local, the Charges are subject to the category of the FSP device (as described in Clause 1.3.2 (FSP Local) above) installed on the Customer’s premises or Orange datacenter. For FSP for Galerie, the Charges are subject to the category of service (as described in Clause 1.3.3 (FSP for Galerie)). Any change requested by the Customer to Orange via the FSP Portal shall be subject to additional charges.

**END OF SERVICE DESCRIPTION FOR FLEXIBLE SECURITY PLATFORM SERVICE**