PUBLICATION 1 SERVICE DESCRIPTION FOR SECURE GATEWAY

1.1 Definitions

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

"**Anti-Spam**" means a Service feature for restricting or blocking the distribution of unwanted emails.

"**Application control**" means a Service feature displaying the applications, by category, that the Customer wishes to authorize or block for its users.

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

"**Incident**" means a fault, failure or malfunction in the Service which can be either a Security Incident or a Platform Incident.

"**Intrusion Detection System**" or "**IDS**" means a passive Service feature for tracking malicious activities at both network and application level.

"**Intrusion Prevention System**" or "**IPS**" means a Service feature incorporating an active function for blocking malicious actions.

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

"**Platform**" means the Service hardware or software which is the core of the Service.

"**Platform Incident**" means an alarm leading to a disruption (with or without an impact) of the Service. A Platform Incident has a predefined management process.

"**Portal**" means the Service web portal which Customer may use as described in this Service Description.

"**Proxy**" means the intermediary feature allowing to relay sessions between a workstation and a server.

"**Sandbox**" means a dedicated or cloud-type Service feature, which emulates the content of a file to check its integrity.

"**Security Incident**" means a security detection identified by the Platform triggering analysis, reporting, and response by Orange.

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

"**Service Management Service**" means the Service Management service, which is described in a separate Service Description.

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

"**Site-to-site Connectivity**" means a Service feature enabling an internet connection between a remote site and the Service via a secure IPSec (Internet Protocol Security) tunnel.

"**SSL inspection**" means a Service feature for decrypting communications from sites using the HTTPS protocol and based on certificates and a procedure for blocking sessions between sites and users by means of a firewall, which can read the decrypted content of a session for analysis purposes.

"**User Remote Access**" is a feature that allows Users to access Customer’s internal network resources via its mobile devices. This feature works through a client connection installed on the User's mobile device. This functionality can also be used as a stand-alone remote access solution.

"**Web filtering**" means a Service feature for managing the categories of websites or URLs that the Customer wishes to authorize or block for its users.

1.2 Service Overview

The Service is a managed network/corporate Internet access security service and comprises the basic and advanced features set forth in this Service Description.

The Service also comprises the NGFW, in the form of hardware (known as a "**Physical Firewall**") or virtual software license (known as a "**Virtual Firewall**") to protect inbound and outbound network traffic. Depending on the selected options, the hardware or software licenses may be either owned/purchased and managed by Orange (the "Opex" option) or owned/purchased by Customer but managed by Orange (the "Capex" option), with different Charges based on the selected option. There are further options for (i) Physical Firewalls in the context of a range of

equipment which allows the Customer to protect the traffic for various sizes of Sites and (ii) Virtual Firewalls in the context of third-party supplier technology/products. Such options will be set out in a SRF and confirmed in Order(s).

Further, as Virtual Firewalls are supported on both public and private clouds, Orange is only responsible for managing the Firewall but not for the backend infrastructure of such clouds.

Depending on the selected options, the Service is available either in an Orange datacenter or on the Customer's premises (physical datacenter or public cloud). Also, the Customer is responsible for providing the needed computing resources recommended by Orange for deploying the Firewall.

The Specific Conditions for Security Services apply to the Service.

1.2.1 **Physical Firewalls**

Depending on the Customer's choice of third-party supplier used by Orange, the hardware for the Physical Firewall is selected in a range of equipment which allows the Customer to protect the traffic for Sites of various sizes, as follows:

- Branch office
- Small office
- Corporate office
- Data center
- Large data center
- Very large data center

1.2.2 **Virtual Firewalls**

Virtual Firewalls will differ depending on the third-party supplier technology, the platform foundation, the level of service needed by the Customer, feature requirements and business needs. Virtual Firewalls are supported on both public and

private clouds. Orange is only responsible for managing the Firewall: Orange is not responsible for the backend infrastructure of the public cloud supplier.

Customer is responsible for providing the needed computing resources recommended by Orange for deploying the Firewall.

1.3 Levels of Service

There are two levels of Service ('Standard' and 'Premium') and the table below sets out the components which are available for each level:

Service Components	Standard	Premium
Basic Features	Included	Included
Advanced Features	Included	Included
Policy Review (as described below)	Included	Included
Application Policy Management (as described below)	Optional	Included
Threat Protection Policy Management (as described below)	Excluded	Included

1.4 Basic Features

- Dynamic inspection (stateful inspection).
- Network address translation (NAT).
- LAN interface management.
- Customer Security Policy Rules.
- Proxy service.
- Reporting via the Portal.
- Access to the configuration parameters via the Portal.
- Access to archived logs.
- Additional LAN interfaces.

1.5 Advanced Features ***

Subject to additional charges, Customer may order one or more of the following advanced features:

- High availability*.
- Internal authentication.
- External authentication.

- Site-to-site Connectivity.
- User Remote Access.
- SSL inspection.
- User management (assigning polices for users or user groups).
- Application control.
- Web filter.
- IPS/IDS **.
- Antivirus/Antibot **.
- Anti-SPAM **.
- Sandbox **.

* With physical appliances.

** Only delivered in Premium services.

*** Depending on the technology vendor.

1.6 Ancillary Services

The following are ancillary services to the Service that Customer can purchase, subject to additional charges.

1.6.1 **Application Policy Management**

Application Policy Management service provides an up-to-date application control policy matching Customer's business environment and rights allocated by user or group of users. The Application Policy is built following a period of observation of the Customer's traffic. It also considers the Customer's needs on applying policies on specific applications for their users as well as the recommendations from our own teams. Monthly application reviews will be held with the Customer to manage the application policy.

1.6.2 **Threat Protection Policy Management**

Threat Protection Policy Management service provides an up-to-date threat protection IPS or IDS policy matching Customer's business environment and protected assets. The Threat Protection is built following a period of observation of the Customer's traffic. It also considers the Customer's needs on applying policies on specific cyber threats as well as the recommendations from our own teams. Monthly threat management reviews will be held with the Customer to manage the threat protection policy.

1.6.3 **Policy Review**

Orange will perform a Firewall policy rule review every six (6) months to identify:

- Unused policy rules;
- Policy rules being hidden by other Firewall rules; and
- Rules usage statistics.

1.7 Service Implementation

(a) **Configuration Information Provided by Customer**

Customer shall provide all information reasonably requested by Orange to configure the Service (e.g. network subnets, server IP addresses, etc.) (collectively, the "**Configuration Information**")) using the electronic form of the SRF provided by Orange. Customer is responsible for ensuring that all Configuration Information provided is accurate and complete. In the event of delays due to Customer's failure to provide all or accurate Configuration Information, Orange may adjust any previously agreed target date accordingly.

(b) **Device Installation**

Unless otherwise agreed in writing by the Parties, installation of the Platform 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 (without limitation) 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.

1.8 Managed Service Features

In addition to the features set out in the service description for Service Management Service, the following service management features for the Service shall apply:

(a) **Hardware and Software Management (Physical or Virtual Firewalls)**

Unless the Customer transitions its existing hardware or virtual software license to Orange, Orange will supply the hardware and software from its third-party supplier (including the software subscription and/or license which manages the Service's security functions). Also, Orange will grant access to the Portal to enable the Customer to (i) manage the Firewall, (ii) access usage statistics, (iii) track and submit changes, and (iv) track and submit Incidents.

(b) **Release Management**

- **Customer Security Policy definition and configuration**

  In order to configure the Service, a Customer Security Policy must be defined by the Parties after a consulting phase with a contact appointed by Orange. The security policy requirements will contain technical information on the Customer's network and details of the Firewall rule configurations to be applied.

- **Installation**

  Unless the Customer transitions its existing hardware or virtual software license to Orange, Orange will order the relevant hardware and software, and configure and install the hardware at the Location.

  Once the hardware is installed, Orange will perform connection tests to check that the Service is operational, the IP addresses are correct, and the security policy is consistent with the Customer Security Policy.

- **Management of Hardware and Software Versions.**

  Orange is not obliged to deploy every new version of the hardware and software made available by its third-party suppliers. It is up to Orange to decide when to perform any upgrades. However, if the Service needs to be interrupted in order to perform an upgrade, Orange will schedule any upgrade in consultation with the Customer. Although there is no limit to the number of service interruptions that may occur in any given month, Orange will endeavor to minimize the number of service interruptions to reduce any material adverse impact to the Customer.

(c) **Continuity Management**

Continuity management manages availability risks that could materially impact the Service. Orange will plan a semi-annual business continuity test for the Service which will be (i) at a pre-arranged time mutually agreeable to Orange and Customer and (ii) subject to Customer having a high availability solution (i.e. two firewalls in a cluster).

(d) **Service Developments**

Orange may modify and update the features and functionality of the Service. Such modifications/updates may include (without limitation) any subsequent release or version of the Service containing functional enhancements, extensions, error corrections, or fixes. Updates will not automatically include new features (which may be subject to an additional charge). Orange will, in its sole discretion, determine whether a third-party supplier update is implemented for the Service.

(e) **Log Management**

Log management shall comprise system health logs, security logs, and Firewall logs that are stored by Orange for twelve (12) months from the date of their creation. Such logs are available in the Portal for one (1) month, after which the Customer can request for the logs to be downloaded using a change request.

1.9 Order Term for the Service

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**"). Termination of an Order 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.

1.10 Charges

One-time Charges apply to the implementation of the Standard/Premium level of Service and to each optional/advanced feature and ancillary service (as described above).

Monthly recurring Charges apply to the Service and to each optional/advanced feature and ancillary service (as described above). Charges are subject to the type of hardware installed at the Customer's Location or Orange

datacenter. Any change to an Order as described below, as requested by the Customer to Orange, shall be subject to additional charges:

- **Level of Service upgrade:** changing Customer's monthly recurring Charges following a request by Customer to change to a higher capacity level of Service. A level of Service upgrade can be implemented on one (1) month's written notice or as agreed in writing between the Parties.
- **Level of Service downgrade:** changing Customer's monthly recurring Charges following a request by Customer to change to a lower capacity level of Service. A level of Service downgrade can be implemented on three (3) months' written notice or as agreed in writing between the Parties.

1.11 Data Processing

Exhibit A sets out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and the categories of Data Subjects of the Processing of Personal Data carried out by Orange as part of this Service.

EXHIBIT A DESCRIPTION OF PROCESSING OF PERSONAL DATA BY ORANGE AS PROCESSOR FOR CUSTOMER

This Description of Processing applies to the Processing of Customer Personal Data for the provision of **Secure Gateway.**

Nature of the Processing Activities	Customer Personal Data are processed to provide the Service in accordance with the Service Description or as further instructed by Customer. Processing operations include collection, consultation, transfer, storage, and deletion of Customer Personal Data, as well as other Processing activities in accordance with the configuration and options of each Service, such as recording.

Subject Matter of the Processing Activities	**Duration**
Activating and implementing the Services and changes to the Services. Delivering, operating, and managing the Services (including intrusion detection and monitoring the Services if ordered by Customer). Incident management and support.	For the necessary period to provide the Service plus 6 months.
In accordance with the Service Description and the options selected:	
Reporting, i.e. reports on billing, usage, quality of service and other reports if and as required by the Customer.	As per Service Description or Customer instructions.
Portals, i.e. providing access and use of portals, on-line tools and other applications managed by Orange as part of the provision of its Services.	As long as necessary for the provision of the Services.

Types of Customer Personal Data to be Processed	**Contact Data:** first name, last name, email address. **Support Data:** Customer representative or end user service ticket information (including feedback, comments, or questions) and if applicable, Customer representative or end user telephone recordings for incident. **Identity Data:** first name, last name, username, or similar identifier. **Technical Data:** login data, browser type and version, time zone setting and location, browser plug-in types, and versions, operating system, and platform, as well as other technology on the devices natural persons use to access areas of Orange portals, or other technical data generated through the use of the Service. **Traffic/Connection Data:** IP address, and timestamp.
Categories of Data Subjects	Employees of Customer and of its Affiliates. If applicable, other individuals using the Service or whose Personal Data are collected via the Service.
Authorized Sub-Processors	Orange Affiliates in the EU and outside of the EU Processing Customer Personal Data for the purpose of this Agreement and communicated separately to Customer.
	Orange suppliers in the EU and outside of the EU Processing Customer Personal Data for the purpose of this Agreement and communicated separately to Customer.

END OF SERVICE DESCRIPTION FOR SECURE GATEWAY