PUBLICATION 1 SERVICE DESCRIPTION FOR SECURE GATEWAY SERVICES

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.

"**Anti-Virus Software**" means the Software provided by Orange as part of the Managed Anti-Virus Service that screens incoming data for potentially malicious software codes.

"**Appliance**" means the CPE (hardware and Software) provided by Orange for, and as part of, the Managed Web Security Service.

"**Cache**" means the proxy or cache Server provided by Orange for, and as part of, the Cache Management Forward or Reverse Proxy Service.

"**DMZ**" means "**De-Militarized Zone**", which is a sub-network, typically between the protected internal network protected by Firewalls and an "untrusted" external network, such as the Internet.

"**Firewall**" means a method of to enhance a network security.

"**GCSC**" means the Orange Global Customer Support Centers.

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

"**Origin Server**" means the server from which a Cache retrieves and replicates data.

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

"**Proper Operational Condition**" means that the Server is functioning in accordance with the parameters of the Secure Gateway Service, as set forth in this Service Description and in the applicable SRFs.

"**Security Rules Base**" means the ordered set of rules against which each connection is checked, which is configured in the Server Software. The Security Rules Base will be determined by Customer's security policy, as set forth in the SRF.

"**Server**" means the CPE (including any Cache or Appliance) provided by Orange as part of the Secure Gateway Service, including both hardware and Software.

"**Service Request Form**" or "**SRF**" means the form that details Customer's specific Secure Gateway Service requirements.

"**Severity Level**" means the category assigned by the GCSC for Incidents.

"**URL**" means Uniform Resource Locator, which is the address that defines the route to a file on the World Wide Web or any other Internet facility.

"**URL Filtering Software**" means the Software provided as part of the Managed Web Security Service that controls Users' access to certain locations on the Internet.

1.2 Service Obligations

1.2.1 **Customer Requirements.** Prior to commencement of the Secure Gateway Services, the Parties will complete the applicable SRFs.

Customer will provide all relevant technical specifications and documentation regarding its existing network and Orange will reasonably assist Customer in completion of the SRFs; however, Customer will ensure that all information contained in the completed SRFs is accurate.

1.2.2 **Customer Security Contacts.** Customer will identify a primary security contact and between 2 and 4 secondary security contacts in each SRF. Customer will ensure that all primary and secondary contacts are available and can be contacted by Orange 24 hours a day, 7 days a week. All Incidents detected by Orange will be reported to the listed contacts, and Orange will respond only to Secure Gateway Service requests and Incidents reported by such contacts.

For Severity Level-1 and Severity Level-2 Incidents detected by Orange, Orange will notify Customer's security contacts of the Incident using all contact details provided in the SRF. For Severity Level-3 Incidents detected by Orange, Orange will send a message to the email addresses set forth in the SRF. All contacts by Orange will be made in English, unless otherwise agreed to by the Parties.

The primary security contact identified in the SRF will ensure that:

(a) All security contact information is maintained and current;

(b) Orange is notified before and after any planned outages or configuration changes to Customer's network or network services; and

(c) Configuration changes are scheduled at least 5 Business Days in advance.

All changes to Customer's primary security contact must be made in writing, on Customer's letterhead, and signed by a senior manager in Customer's organization.

1.3 Scope of Services

1.3.1 Service Deployment

1.3.1.1 **Site Survey.** Promptly upon completion of the SRF, Customer will perform a survey of the physical premises where the Server will be installed (a "**Site Survey**"). Customer must gather the information requested in the Site Survey form provided by Orange for Orange to determine if the Location meets the necessary requirements for the proper installation and functioning of the Service and to identify the specific tasks, if any, that Customer must complete to provide the Location with the proper infrastructure to support the Server. Upon Customer's request and for an additional charge, Orange will perform the Site Survey. If Orange performs the Site Survey, a Customer representative must provide Orange access to the Location and accompany the Orange personnel at all times during the Site Survey.

1.3.1.2 **Physical Environment Requirements.** Upon completion of the Site Survey, Orange will advise Customer of all Location preparation requirements that Customer must complete prior to the scheduled date for commencing installation of the Server. If Customer fails to complete all such required preparations, Orange is relieved of its Secure Gateway Service responsibilities at that Location until such time as it has been adequately prepared.

The Location must provide appropriate space, conditioned power, environmental controls, and a direct access PSTN line for remote access into the Server. The PSTN line must be able to accept and make calls and, for security reasons, must not be advertised in any telephone directories. Callback and international calling must be enabled on the PSTN line. The hardware components of the Server have been designed to operate as a single unit and must be located within 3 feet of each other. Customer also must provide:

(a) A secure location in which to install the Server, accessible on a 24 x 7 basis.

(b) Appropriate space within a standard 19" rack.

(c) Appropriate environmental controls.

(d) Appropriate number of power outlets for the required configuration, as directed by Orange. All power outlets supplied must be 110V/60Hz. conditioned power outlets or 220V/50Hz, as appropriate for the applicable country, and installed within 3 feet/1 meter of the Server.

(e) An Ethernet connection to Customer's internal IP-based Local Area Network (LAN).

Alternatively, the Server can be housed in an Orange facility, where the requirements set forth above can be provided for additional charges.

1.3.1.3 **Lead Time Requirements.** The Server will be deployed 10 weeks from the date on which the completed SRF is received and signed by Orange, and such deployment will be delayed if Customer requires changes to the specifications listed in the completed and accepted SRF.

1.3.1.4 **Configuration.** Orange will configure the Server, and will apply sizing rules, wholly based upon specifications contained in the applicable SRF. Any configuration changes required due to inaccurate or revised specifications will be charged to and paid by Customer at the Hourly Labor Rate for such services, plus the cost of materials.

Upon completion of the configuration, the Server will be delivered to the Location specified in the SRF. Customer will visibly inspect the exterior condition of the Server packaging prior to accepting delivery. After accepting delivery, Customer will store the Server in a secure location until Orange commences installation. Customer will bear the risk of loss while the Server remains at the Location.

Following installation and acceptance testing, Orange will accept requests for changes to the configuration of the Server only from the security contacts identified in the SRF. All such changes will be subject to verification by Orange in accordance with mutually established procedures agreed to in writing by the Parties prior to commencement of the Secure Gateway Service.

1.3.1.5 **Installation of Server.** Before Orange will install the Server, Customer must provide written confirmation that the following tasks have been completed:

(a) Satisfactory delivery of the Server to the Location;

(b) All data circuits are installed and operational; and

(c) The Location has been properly prepared in accordance with Clause 1.3.1.2 and the Orange direction pursuant to the Site Survey.

Orange will install the Server upon its receipt of Customer's confirmation. Unless otherwise agreed to by the Parties, Server installation will be conducted during Business Hours. If Customer requests Orange to install the Server 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 of the Server if such failure is due to any cause beyond its reasonable control, including the inability by Orange to gain access as scheduled to the Location, failure by the local TO to complete installation of the circuits, or Customer's failure to prepare the Location in accordance with Clause 1.3.1.2 and direction from Orange.

Orange will contact Customer at least one day prior to the scheduled installation date to confirm the installation appointment and will confirm with Customer that the Location has been properly prepared, as directed by Orange. If Orange determines that the Location has not been appropriately prepared, and that Orange cannot install the Server, then Orange will notify Customer promptly, and Orange will have no responsibility to continue the installation. However, if the designated Customer contact disagrees with the assessment by Orange that the Location has not

been properly prepared, the Parties will escalate the issue promptly in accordance with the Parties' escalation procedures, as may be provided in the General Conditions. Customer will advise Orange when the Location has been properly prepared, and the installation will be rescheduled dependent upon the preparation activities required. If, as a result of rescheduling, Orange must make more than one trip to the Location or remain at the Location and wait for the Location to be adequately prepared, then the additional time required will be billed at the Hourly Labor Rate.

As part of the installation, Orange will interconnect the Server to the Demarcation and Customer's network and will notify Customer promptly if any problems occur during installation that adversely affect the installation process.

1.3.1.6 **Acceptance Testing.** Upon completion of the installation of each Server, Orange will commence acceptance testing, which will confirm that all aspects of the Server and the Service are 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 "**Secure Gateway Service Acceptance Form**" for Customer's execution, which form will identify the acceptance tests performed by Orange. Customer will be deemed to have accepted the Service on the date on which Orange issues the Secure Gateway Service Acceptance Form, unless Customer notifies Orange in writing of a material fault in the Service within 5 Business Days of receipt of the Secure Gateway Service Acceptance Form. In such event, the above acceptance process will be repeated.

1.3.1.7 **Security Policy Changes Procedure.** Following installation and acceptance testing, Orange will accept up to two requests for changes per month to the Security Rules Base only from the security contacts identified in the SRF. All such changes will be subject to verification by Orange in accordance with mutually established procedures agreed to in writing by the Parties prior to the commencement of the Secure Gateway Service.

Orange will contact the primary security contact to agree to the appropriate actions, timeframes, and charges, if applicable. Any potential conflict in the Security Rules Base or any inadvertent reduction in the security effectiveness perceived by Orange will be brought to Customer's attention, and Orange will recommend alternative strategies.

Orange will require the following information for any changes to the Security Rules Base:

(a) Completed change control form on the Portal;

(b) Date by which Customer requests the change to be completed, which will be no earlier than 5 Business Days after Orange receives the change request (provided that Orange may assess, and Customer will pay, an additional charge for any changes Orange agrees to provide sooner);

(c) Supporting details relevant to the specific change action; and

(d) Contingency plans and contact details of Customer personnel performing acceptance testing for the changes to the Security Rules Base.

1.3.2 **Server Upgrades.** Orange will provide version management of the operating system and various elements of the Secure Gateway Service Software. Server upgrades may include the addition of patches to the operating system that are of a security nature and those that would affect the operation of the Software. The upgrade to a new operating system level also will be made if Orange deems it necessary for security reasons or for support of the Software. Notwithstanding anything to the contrary contained herein, Orange has no obligation to provide all new releases of Software from the Server hardware vendors and Software licensors, and Orange, in its sole discretion, will decide when upgrades take place.

If Orange needs to take a Server off-line to implement Software updates or network enhancements, Orange will provide at least 7 days prior written notice of such events. When possible, Orange will work with Customer to minimize any impact this could have. When possible, Orange will implement Server upgrades remotely during Business Hours. If Orange is required to install an upgrade at the Location or outside of Business Hours, Customer will be charged at the Hourly Labor Rates for such services, plus the cost of materials.

If Customer has requested a customized Server and Orange cannot update the Software remotely, Software upgrades will be charged at the Hourly Labor Rates for such services, plus the cost of materials.

1.4 Description of Services

The Secure Gateway Service includes the Managed Firewall Service, and Customer may elect to receive the optional Managed Web Security Service, Managed Anti-Virus Services, Cache Management Forward Reverse Proxy Service, or Cache Management Reverse Proxy Service. Separate Charges will apply to each of the foregoing Services. Customer will receive two SSL certificates for access to the Portal as part of the Secure Gateway Service; any additional SSL certificates provided will be subject to additional charges.

1.4.1 **Managed Firewall Service.** The elements of the Orange Managed Firewall Service are set forth in Exhibit A, which is attached hereto and is incorporated herein by reference. In addition, Orange will provide the following:

1.4.1.1 **Firewall Monitoring.** Orange monitors all Firewall installations 24 hours a day, 7 days a week, for Server and Firewall presence.

Firewall monitoring and Server availability do not cover operational problems relating to Internet service, web browsers, or Customer's line to the Internet.

1.4.1.2 **Real Time Alerting.** Real-Time altering consists of the detection of Incidents. The Server is monitored for two types of real-time alerts:

(a) Operating system alerts from the hardware; and;

(b) Application alerts from the Software.

Orange will respond to Incidents based on the applicable Severity Level. An escalation process involving Customer's security contacts will be agreed to with Customer for the various Severity Levels. In the case of a suspected security attack through the Firewall, Orange will have the right to shut down the Firewall.

1.4.1.3 **Vulnerability Scanning.** Through an independent third party, Orange will provide on a regular basis a vulnerability scan of the IP address of the installed, Internet-facing Firewalls.

1.4.1.4 **Monthly Service Reporting.** Through the Portal, Customer's security contacts may access information and reports regarding the Secure Gateway Service, as described below. This access is protected through a personal digital certificate. All communications through the Portal are encrypted using SSL v3 or such other encryption method selected by Orange.

- **Firewall Configuration.** Information about the hosts, networks, and services declared on the Firewall(s), as well as the current Security Base Rules implemented on the Firewall.
- **Firewall Logs Analysis.** Customer may request queries on demand from daily and monthly consolidated Firewall logs. Several queries are available (e.g. usage, sources, destinations, Users). The consolidated logs give an analysis of Customer's traffic, not of filtering or attacks (except the number of rejected connections). Some information on consolidated logs is not available, since queries are often limited to a maximum of 100 (top 100).

Customer may request reports on the accepted/dropped connections, activity per IP source and per IP destination, and User activity.

Firewall logs analysis is limited to restrict the impact of DDoS attacks. If the traffic logging exceeds the threshold defined by Orange, no log will be reported. In addition, the IP address resolution has a threshold, as defined by Orange, and if the number of IP addresses to resolve exceeds such threshold, then no resolution will be performed.

- **Firewall Availability**. This monthly report captures the amount of time (as a percentage of the report duration) that the Server and Software runs.
- **Firewall Vulnerability Scan.** This is a copy of a report provided monthly by the third party that tests the Orange managed Firewalls by performing a vulnerability scan of the Firewall IP address; this report is available only for Internet facing Firewalls.

1.4.2 **Managed Web Security Service.** If ordered by Customer, Orange will provide the Managed Web Security Service, which provides Customer with web filtering or anti-malware functionality, as selected by Customer, using the dedicated Appliance. For web filtering, the Managed Web Security Service will analyze and filter HTTP web requests passing through the Appliance using URL Filtering and Web Reputation Filters. For antimalware, the Managed Web Security Service will analyze web traffic through the Appliance to detect infected files or other malicious codes. Managed Web Security does not monitor outgoing traffic.

Managed Web Security is a companion service of the Managed Firewall Service and cannot be installed as a stand-alone offer. The Appliance is placed in a DMZ, and all connections involving access to the Internet must go through the Firewall.

1.4.2.1 **Service Reporting.** Through the Portal, Customer's security contacts will have access to Customer's Managed Web Security Service configuration as well as certain reports for the Service (e.g. overview, User statistics, malware statistics, or web filtering statistics). Customer's security contacts also may access reports directly from the Appliance (e.g. overview, web activity, malware risk, URL categories, and web reputation filters).

1.4.2.2 **URL Filtering Lists and Web Reputation Filters**

(a) **URL Filtering Lists.** There are two types of URL lists that the Appliance uses: (1) predefined URL lists and (2) Customer URL lists.

(i) **Predefined URL Lists.** The URL Filtering Software has a standard database of non-business URLs classified per category, and neither Customer nor Orange can modify these lists. They can only be updated by downloading new "non-business" URLs and new categories made available by the Software licensor.

(ii) **Custom URL Lists.** Customer's administrator can create local filter lists to filter additional URLs. When a request for Internet access is made, the URL Filtering Software will check the Customer local filter lists before the predefined filter lists. When checking a URL, the URL Filtering Software looks for the most exact match, enabling the Appliance to block access to individual pages, entire directories, machines, or domains.

Customer's URL list can cover one or several individual Users, a group of Users, or the entire Appliance. The Appliance's default filtering policy will apply to Users or groups of Users for which no custom filter policy is defined by Customer.

(b) **Web Reputation Filters.** Web Reputation Filters use security modeling algorithms to assess a URL using defined parameters, converting the overall probability of a URL presenting a threat into a web reputation rating. Based on the web reputation rating, when a User attempts to access the URL, the Managed Web Security Service will allow the User to access the URL, prevent the User from accessing the URL, or apply additional controls to which Customer has subscribed based on the reputation rating.

(c) **Updating URL Filtering Lists and Web Reputation Filters.** The URL Filtering and Web Reputation Filter Software licensors continually update the URL Filtering Software's predefined content category lists and the Web Reputation Filter's algorithms, agents and parameters. The Appliance polls the Software licensors

periodically to determine whether updated versions have been provided. If new versions are available, the URL Filtering Software or Web Reputation Filter Software automatically initiates a download. Update times are scheduled within the applicable Software and cannot be modified by Orange or Customer.

1.4.2.3 **Anti-Malware.** Anti-Malware analyzes web traffic (HTTP) and FTP traffic passing through the Appliance to detect infected files or other malicious code. Web objects are analyzed in streaming mode in an effort to minimize latency times; accordingly, the scanning begins when the download of the object begins, and the download is stopped immediately if malicious code is identified.

1.4.2.4 **Access Policy Management.** The Parties will jointly manage the Managed Web Security Access Policy, which determines the Users who may access the Internet and what information may be accessed. Orange will create one privileged account for Customer on the Appliance and will provide Customer's administrator with the information needed to use this account (login / password and documentation). Using the Portal, Customer may access to the web filtering or anti-malware functions (as applicable), through which Customer may make changes to the Access Policy.

1.4.2.5 **Logs.** Logs generated by the Managed Web Security Service are retained locally on the Appliance and are exported to a backup server daily.

1.4.2.6 **Optional Service Feature.** For an additional charge, Customer may purchase the following option:

- **High Availability.** Orange will provide an additional Orange-managed Appliance at a single Location to reduce the probability that any single Appliance failure interrupts service.

1.4.3 **Managed Anti-Virus Service.** If ordered by Customer, Orange will provide the Managed Anti-Virus Service, which is a companion service of the Orange Managed Firewall Service and which cannot be provided as a stand-alone offer.

Orange will provide Managed Anti-Virus Service to Customer at the Location(s) identified in the applicable SRFs. The Managed Anti-Virus Service allows the Server to be configured to meet Customer's requirements regarding the following actions:

- Analyze file types, compression formats and MIME encoding formats.
- Scan document contents by file extension and DOS/Windows system header.
- Ignore (not scan) some selected MIME content (embedded on an HTML page), such as text or image contents to improve service efficiency.
- Protect against Java applets or any executable files, preventing mobile codes from being executed on the User workstation.
- Enable (not scan) or disable (scan and delete if infected) Microsoft macro codes.
- Ensure that the Server processes mail for internal delivery only.
- Reject files above a certain size without further scanning or processing.
- Apply a variety of actions upon virus detection such as delete, pass, auto-clean or delete, and auto-clean or pass.
- Send notifications, warning, or disclaimer messages to administrators, senders, and receivers.

1.4.3.1 **Anti-Virus Software Updates.** New pattern files made available by the Software licensor are automatically downloaded onto an Orange central server. The pattern file integrity is checked and then automatically downloaded to the Managed Anti-Virus Server.

1.4.3.2 **Monthly Service Reporting.** Through the Portal, Customer's security contacts may access the following information and reports regarding the Orange Managed Anti-Virus service:

- **Configuration.** Information regarding the parameters for each scanned protocol, as per the current Security Base Rules implemented.
- **Version.** Information about the version of Managed Anti-Virus Software implemented.
- **Statistics.** Information regarding the actions taken on viruses detected by the Managed Anti-Virus service.
- **Logs.** Customer may request queries on demand from daily and monthly consolidated Managed Anti-virus service logs.
- **Availability.** This monthly report captures the amount of time (as a percentage of the report duration) that the Managed Anti-Virus server and Software is operational.

1.4.4 **Cache Management Forward Proxy Service.** If ordered by Customer, Orange will provide the Cache Management Forward Proxy Service, which includes the following standard features:

(a) Acceleration of Users' access to web data stored on the Cache at the Location;

(b) Basic Authentication, using usernames and passwords;

(c) Filtering Users' data requests using access control lists and security policies provided by Customer; and

(d) Notifying Users of Customer's policies regarding access to web data and blocking or allowing Users access to such data, based on the information provided by Customer for use with the Forward Proxy Service.

Orange will monitor the Caches, and Orange will identify and may modify from time to time the protocols supported by the Forward Proxy Service. The Forward Proxy Service does not include the provision of sock clients or authentication servers, although the Forward Proxy Service may be configured to support Customer's authentication service in accordance with the SRF. The Forward Proxy Service will support the Domain Name Service proxy feature, which allows translation of a fully qualified Domain Name into an IP address.

1.4.4.1 **Optional Service Features.** For an additional charge, Customer may purchase the following options:

(a) **Service Management:**

(i) CSM. Customer will receive support from a designated English-speaking Customer Service Manager ("**CSM**"), who will be available during Business Hours. The CSM will proactively manage operational performance within Orange on Customer's behalf and work with the Orange internal operations groups to maintain or improve performance of the Forward Proxy Service as needed. The CSM will be Customer's single point of contact for all inquiries regarding performance, procedural or other technical aspects of the Forward Proxy Service, and the CSM will accept Customer's requests and inquiries only from Customer's authorized designated contacts. The CSM will respond to Customer's inquiries promptly.

(ii) Security TechPro. Customer may elect to receive support from a designated English-speaking Security TechPro, who will be available during Business Hours; provided that Customer may only receive support from the Security TechPro if Customer also receives support from a CSM. The Security TechPro will provide security management for the Forward Proxy Service, communicate, and coordinate with Customer regarding new threat or major market security crises, and retrieve data from the Caches to provide risk assessments and vulnerability surveys to Customer.

(b) **Reporting.** Orange will generate reports on daily cache log files (up to 250 Mbytes uncompressed) providing information to Customer on how the Caches are used. Customer may access such reports via the Orange My Service Space Service (as described in a separate Service Description attached to this Agreement). Customer also may access reports regarding the Forward Proxy Service via portals made available by Orange.

(c) **High Availability.** Orange will provide an additional Orange-managed Cache at a single Location to reduce the probability that any single Cache failure interrupts service.

(d) **Streaming.** Orange will provide and active streaming licenses on the Cache to allow the support and caching of streaming media; provided that Customer will provide all other equipment and service necessary to support such streaming media.

(e) **URL/IP Filtering.** Orange will provide Software allowing Customer to restrict access to data based on Customer's security policy and a standard database of URLs classified in various categories (i.e. groups of potentially dangerous or harmful topics such as drugs, weapons, etc.), which is updated when new versions of the Software provided by the Software licensor are automatically downloaded onto the Cache.

(f) **Peer to Peer Controlling and Instant Messaging Filtering.** Orange will implement controlling methods to block connections to any supernode and create deny lists, and will implement filtering policies for Instant Messaging, as agreed upon with Customer.

1.4.5 **Cache Management Reverse Proxy Service.** If ordered by Customer, Orange will provide the Cache Management Reverse Proxy Service, which includes the following standard features:

(a) Acceleration of Users' access to web data stored on the Cache at the Location, thereby offloading the back-end servers; and

(b) Basic Authentication, using usernames and passwords.

The Reverse Proxy Service enhances the performance and security of Customer's web applications by offloading content delivery from Customer's Web servers to the Caches. When a request for data is made, the request is routed to a Cache rather than directly to Customer's Web servers, thereby preventing direct visibility into the IP address of the Customer's web server. The Reverse Proxy Service does not include the provision of sock clients or authentication servers, although the Reverse Proxy Service may be configured to support Customer's authentication service in accordance with the SRF.

1.4.5.1 **Physical Environment Requirements.** Orange will provide the following environmental conditions for the Caches located in its data centers:

- A secure site in which to install the Cache.
- Appropriate space within a standard 19" rack
- Appropriate environmental controls.
- Appropriate number of power outlets for the required configuration, as directed by Orange.

All power outlets must be supplied on 110V/60Hz or 220V/50Hz conditioned power outlets, as appropriate for the applicable country, and installed within 3 feet/1 meter from the Cache.

Customer is solely responsible for, and Orange will not be liable for, the installation of circuits for use with the Reverse Proxy Service, except as otherwise provided in this Agreement. In addition, Customer is solely responsible for assessing its own computer, transmission, and security network needs; and the results to be obtained therefrom.

Customer is not granted, and specifically disclaims, any possessory, leasehold, or other real property interest in the Orange data center housing the Cache, or any other portion of the building or project in which such data center is located. Without limiting the foregoing, Customer has no rights whatsoever under the Orange lease for the data center.

1.4.5.2 **Installation.** Orange will not be responsible for any delay in the installation of the Cache if such delay is due to any cause beyond its reasonable control. As part of the installation, Orange will interconnect the Cache immediately in front of Customer's Web servers at the Orange data center and will notify Customer promptly if any problems occur during installation, which adversely affect the installation process.

1.4.5.3 **Monitoring.** Orange will monitor all Caches. Caches in the Orange data centers via the internal monitoring solution deployed in such data centers.

1.4.5.4 **Service Options.** For an additional charge, Customer may purchase the following service options:

(a) **Service Management.**

(i) **CSM.** Customer will receive support from a designated English-speaking Customer Service Manager ("**CSM**"), who will be available during Business Hours. The CSM will proactively manage operational performance within Orange on Customer's behalf and work with the Orange internal operations groups to maintain or improve performance of the Reverse Proxy Service as needed. The CSM will be Customer's single point of contact for all inquiries regarding performance, procedural or other technical aspects of the Reverse Proxy Service, and the CSM will accept Customer's requests and inquiries only from Customer's authorized designated contacts. The CSM will respond to Customer's inquiries promptly.

(ii) **Security TechPro.** Customer may elect to receive support from a designated English-speaking Security TechPro, who will be available during Business Hours; provided that Customer may only receive support from the Security TechPro if Customer also receives support from a CSM. The Security TechPro will provide security management for the Reverse Proxy Service, communicate, and coordinate with Customer regarding new threat or major market security crises, and retrieve data from the Caches to provide risk assessments and vulnerability surveys to Customer.

(b) **Reporting.** Orange will generate reports based on daily Cache log files providing information to Customer on how the Caches are used; provided that Customer will be not be required to pay an additional charge for this service if the daily log volume for each Cache does not exceed 500 Mbps. Customer may access such reports via the Orange My Service Space Service (as described in a separate Service Description attached to this Agreement) or via portals made available by Orange.

(c) **SSL Card.** Orange will install an SSL acceleration card in the Cache, which will expand the SSL processing capacity and increasing throughput.

(d) **High Availability.** Orange will provide an additional Orange-managed Cache at a single Location to reduce the probability that any single Cache failure interrupts service.

(e) **Load Balancing.** Orange will provide load balancing by distributing between Caches the requests for data to Customer's Web servers.

1.5 Maintenance of the Server and Cache

1.5.1 **Remedial Maintenance.** Orange will maintain the hardware portion of the Server in Proper Operational Condition. If an Incident is caused by a failure in the Server hardware, Orange will repair the Server following receipt of a call from Customer regarding, or the Orange detection of, the Incident, whichever occurs first. If Orange is unable to restore the Server hardware to Proper Operational Condition remotely, an Orange field engineer will be dispatched to the Location.

The GCSC will classify all Incidents as follows:

Severity 1	Problems causing critical impact to the business function(s) or customer(s). Justifies immediate management attention and dedicated resources applying continuous efforts to resolve as soon as possible.
Severity 2	Problems causing degradation of service resulting in impact to business function of customer. Impact justifies priority attention and application of resources to resolve in a timely manner
Severity 3	Problems causing low impact to the business function(s) and customer(s). Requires timely resolution to minimize future impacts. Resources should be allocated in accordance with normal managerial planning prioritization

1.5.2 **Remedial Maintenance Exclusions.** Orange will have no obligation to furnish Remedial Maintenance Services for, nor will Orange be liable to Customer for damages for loss of Secure Gateway Services or the Server caused by any of the following (collectively "**Limitations**"):

(a) Damage to the Server caused by temperature or electrical current fluctuation, or any Force Majeure Event, or any other casualty or loss;

(b) Damage caused by adjustments and repairs made by persons other than the Orange own representatives, its Subcontractors, or personnel approved in writing by Orange; or

(c) Any instabilities in the operation of the Server that are caused by or related to the use of certain software, or by any other software provided by Customer or its designees, or by combinations of the Server and software, even if such combination is specified on a duly accepted SRF, or by any hardware connected to the Server.

Remedial Maintenance Services rendered necessary by the above causes may be performed by Orange at the Customer's request, and will be charged to and paid by Customer at the Hourly Labor Rate, plus the cost of materials.

Remedial Maintenance Services do not include:

- Electrical work external to the Server, except as otherwise set forth in this Service Description;
- Maintenance of attachments or other devices not specified in the SRFs;

- Correction of software databases and/or programming errors or any errors or damages caused by or arising out of input or error, except as otherwise set forth in this Service Description; or
- Failure by Customer to meet the physical and environmental specifications for the Server.

Any visits to a Location or repairs to the Server made necessary by the preceding causes will be charged to and paid by Customer at the Hourly Labor Rate, plus the cost of materials.

1.6 Data Processing

Exhibit B 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 MANAGED FIREWALL SERVICE FEATURES

ExA.1 Resilient/High Availability Configuration

The standard solution for the High Availability ("**HA**") of the Secure Gateway Service is based on two firewalls (one active, also called the primary or master, and one passive, also called the secondary or slave or fail over) that run Virtual Router Redundancy Protocol ("**VRRP**"). The VRRP monitors circuits instead of individual interfaces and provides for the automatic backup of both IP address and MAC address of the master router. These addresses are virtual and can be assigned to one or more slave routers. The virtual addresses are used as the default router for hosts in the network.

The master router forwards all packets sent to the virtual address. The VRRP election process provides for dynamic fail-over (within 2-5 seconds) to a hot standby, should the master router become unreachable.

The Orange resilient/HA solution does not require host or server reconfiguration and provides a fully integrated router Firewall platform. Synchronized Firewall-1 modules update each other with their state information every 50 milliseconds. In the case of a failure of the primary, the only state information (and therefore logical network connections) that may be lost would be those that were initiated by the primary Firewall-1 module in the 50 millisecond before the failure.

ExA.2 LAN Interface Support

All physical connections to the Server must be Ethernet; the number of Ethernet connections available will depend on the model number of the Server hardware. The Server may support additional LAN connections to provide multiple network connections, such as a DMZ.

ExA.3 Network Address Translation

The Managed Firewall Service supports the use of network address translation, which provides the ability for all internal addresses to appear externally as one external address. Addresses also can be mapped on a ‘one-to-one’ basis.

ExA.4 Security Policy Rules

Customer’s security policy, as set forth in the SRFs, is converted into a rule base, which is implemented on the Firewall. A rule base is an ordered set of rules against which each connection is checked. Each rule specifies the source, destination, service, time limitation, action to take for each connection (i.e. permit or deny), and applicable logging level.

ExA.5 Authentication on the Firewall

As a chargeable option of the Managed Firewall Service, authentication on the Firewall is possible for a limited number of Users. The types of authentication available for the Managed Firewall Service are as follows:

- User Authentication allows Users to be granted access privileges on connection basis, without regard to the User’s IP address. This type of authentication is limited to the Telnet, HTTP, and FTP protocols or such other protocols as may be identified by Orange.
- Client Authentication permits Users to use any service from the IP address on which the authentication takes place. Client authentication is not restricted to some services as in User Authentication mode. User information (login and password) is stored in the Firewall proprietary internal User database.

ExA.6 Internet services

The Managed Firewall Service provides control of Internet services by applying the Customer’s security policy, as set forth in the SRF.

ExA.7 Encryption

Orange offers AES-256 encryption for use with VPNs, except as otherwise notified by Orange. Subject to export/import restrictions in certain countries, DES (56 bits), 3DES, or AES-128 encryption can be provided on request, provided that Orange may change the encryption methods made available at any time.

EXHIBIT B DESCRIPTION OF PROCESSING OF PERSONAL DATA BY ORANGE BUSINESS SERVICES AS PROCESSOR FOR CUSTOMER - ARTICLE 28 OF GDPR

Name of the Service: Secure Gateway

ExB.1 Processing Activities

Collection (receiving personal data of employees and users of customer who are natural persons, etc.).	Yes
Recording (capturing personal data in a file or software program, including the generation of metadata like Call Details Records, etc.).	Yes
Organization (organizing personal data in a software program, etc.).	Yes
Storage (keeping the personal data in a software program for a determined period, including for archiving purposes, etc.).	Yes
Modification (modifying the content or the way the personal data are structured, etc.).	No
Consultation (looking at personal data that we have stored in our files or software programs, etc.).	Yes
Disclosure or otherwise making available (communicating personal data to another recipient by any means, etc.). Except for disclosure mentioned in the service description or required by law, or otherwise specifically directed by the customer, the categories of potential recipients are only those subcontractors referenced herein or otherwise approved by the customer.	No
Combination (merging two or more databases with personal data, etc.).	Yes
Restriction (implementing security measures in order to restrict the access to the personal data, etc.).	Yes
Deletion or destruction (deleting or anonymizing the personal data or destroying the hard copies, etc.).	Yes
Other use (if "YES" to be detailed).	No

ExB.2 Categories of Personal Data Processed (Type of Personal Data)

Categories of Personal Data Identifiable by Orange	
Identification data (ID document / number, phone number, email, etc.).	Yes
Traffic / Connection data (IP address, Mac address, CDRs, access and usage data, online tracking and monitoring of services).	Yes
Location Data (geographic location, device location).	No
Customer Relationship Management data (billing information, customer service data, ticketing info, telephone recordings, etc.).	Yes
Financial data (bank account details, payment information).	No
Sensitive Data (racial/ethnic background, religion, political or philosophical beliefs, trade union membership, biometric data, genetic data, health data, sexual life, and/or orientation).	No
Categories of Personal Data Not Identifiable by Orange	
Any categories of personal data that may be recorded or stored (voicemail, call recording, files) by Customer and which recording is hosted on Orange infrastructure.	No

ExB.3 Subject-Matter and Duration of the Processing

Subject-Matter of Processing		**Duration of Processing**
Service activation.	Yes	For the period necessary to provide the service to the customer plus 6 months.
User authentication.	Yes	
Incident Management.	Yes	
Quality of Service.	Yes	
Invoice, contract, order (if they show the name and details of the contact person of Customer).	Yes	For the period required by applicable law.
Itemized billing (including traffic / connection data of end-users who are natural persons).	No	
Customer reporting.	Yes	For the duration requested by Customer.
Hosting.	Yes	For the duration of the service ordered by Customer.
Other. [if yes please describe]	No	

ExB.4 Purposes of Processing

Provision of the service to Customer.

ExB.5 Categories of Data Subject

Customer's employees/self-employed contractors using or managing the service or the contract who are natural persons.	Yes
Customer's other end-users of the service who are natural persons (client of the Customer, etc.); usable by users other than internal users.	No

ExB.6 Sub-Processors

Sub-Processors Approved by Customer	Safety Measures
Orange Business Services entities that are processing information for this Service and that are within the EU/EEA are communicated separately to the Customer.	NA
Orange Business Services entities that are processing information for This Service and that are outside of the EU/EEA are communicated separately to the customer.	Intra-group agreements with standard model clauses, Binding Corporate Rules approval request filed with CNIL.
Orange Business Services suppliers which are performing one or more processing activities described above in connection with this Service and that are within the EU/EEA are communicated separately to the Customer.	NA
Orange Business Services suppliers that are processing information for this Service and that are outside of the EU/EEA are communicated separately to the Customer.	Standard Model Clauses in contract with supplier.

END OF SERVICE DESCRIPTION FOR SECURE GATEWAY SERVICES