1 SERVICE DESCRIPTION FOR UNIFIED DEFENSE 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.

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

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

"**Fault**" means a fault, failure, or malfunction in the Unified Defense Service.

"**Fault Call**" means the notification made by Customer to the GCSC to report a Fault.

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

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

"**Incident**" means a security event, alert, or problem regarding the Unified Defense Service detected by Orange.

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

"**Security Rules Base**" means the ordered set of rules against which each connection is checked, which may include up to 16 protection profiles, and which is configured on the Unified Defense Server. The Security Rules Base will be determined by Customer's security policy, as set forth in the SRF.

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

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

"**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 Unified Defense Service that controls Users' access to certain locations on the Internet.

"**Unified Defense Server**" means the server that supports the multiple security features of, and that is provided by Orange as CPE for, the Unified Defense Service.

1.2 Description of Service

The Unified Defense Service is a fully-managed Orange Security Service that provides Customer with a Firewall and Anti-Virus Software on the Unified Defense Server. Customer also may elect to receive the optional Network Intrusion and Detection Service (IDS/IPS), URL Filtering, High Availability, or User Authentication Services.

1.3 Service Request Form

1.3.1 Customer Requirements

Prior to commencement of the Unified Defense Service, 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. Customer will ensure that all information contained in the completed SRFs is accurate.

1.3.2 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 will be reported to the listed contacts, and Orange will respond only to Unified Defense Service requests and Fault Calls issued by such contacts.

For Severity Level 1 and Severity Level 2 Incidents, Orange will notify Customer's security contacts of the Incident using all contact details provided in the SRF. For Severity Level 3 Incidents, 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:

- All security contact information is maintained and current;
- Orange is notified before and after any planned outages or configuration changes to Customer's network or network services; and
- All 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.

1.4 Service Deployment

1.4.1 Site Survey

Promptly upon completion of the SRF, Customer will perform a survey of the physical premises where the Unified Defense 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 Unified Defense Service and to identify the specific tasks, if any, that Customer must complete to provide the Location with the proper infrastructure to support the Unified Defense 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.

1.4.2 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 Unified Defense Server. If Customer fails to complete all such required preparations, Orange will be relieved of its responsibilities to provide the Unified Defense Service at that Location until such time as the Location has been adequately prepared.

Customer must provide appropriate space, conditioned power, environmental controls, and a direct access PSTN line (with international call capability) for remote access into the Unified Defense Server at the Location. Customer will be responsible for all charges associated with the remote access communications using the PSTN line. The hardware components of the Unified Defense 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 secure location in which to install the Unified Defense Server, accessible on a 24x7 basis.
- Appropriate space within a standard 19" rack.
- Appropriate environmental controls.
- 6 power outlets per single Unified Defense Server, which are 110V/60Hz conditioned power outlets (or 220V/50Hz as appropriate for the applicable country) and installed within 3 feet of the Unified Defense Server.
- An Ethernet connection to Customer's internal IP-based Local Area Network (LAN).

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

1.4.3 Lead Time Requirements

The Unified Defense 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.

1.4.4 Configuration

Orange will configure each Unified Defense Server 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 Expenses.

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

Following installation and acceptance testing, Orange will accept requests for changes to the configuration of the Unified Defense Server only from the security contacts identified in the SRF, and Customer may submit up to 5 change folders to Orange per month. Except as otherwise identified by Orange, a change folder is composed of a maximum of:

- 30 objects (networks, hosts, services).
- 10 Firewall rules (add, modify, delete).
- 10 items related to protection profiles.

- 10 items related to Anti-Virus Software global configuration.
- 10 items related to URL Filtering global configuration.
- 10 items related to IDS/IPS global configuration.
- 10 items related to User Authentication (add, remove, and modify Users); substantial changes for several Users (e.g. 100) can be done using a single CSV file.

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 Unified Defense Service.

1.4.5 **Installation**

Before Orange will install the Unified Defense Server, Customer must provide written confirmation that the following tasks have been completed:

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

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

(c) The Location has been properly prepared in accordance with the terms of this Service Description.

Orange will install the Unified Defense Server upon its receipt of Customer's confirmation. Unless otherwise agreed to by the Parties, Unified Defense Server installation will be conducted during Business Hours. If Customer requests Orange to install the Unified Defense 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 Unified Defense 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 the terms of this Service Description.

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. If Orange determines that the Location has not been appropriately prepared, and that Orange cannot install the Unified Defense 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 escalation procedures provided in the General Conditions. Customer will advise Orange when the Location has been properly prepared, and the installation will be rescheduled depending 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 Unified Defense 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.

1.4.6 **Acceptance Testing**

Upon completion of the installation of each Unified Defense Server, Orange will commence acceptance testing, which will confirm that all aspects of the Unified Defense 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 "**Unified Defense 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 Unified Defense Service on the date on which Orange issues the Unified Defense Service Acceptance Form, unless Customer notifies Orange in writing of a material fault in the Service within 5 Business Days of receipt of the Unified Defense Service Acceptance Form. In such event, the above acceptance process will be repeated.

1.4.7 **Security Policy Changes Procedure**

Following installation and acceptance testing, Orange will accept requests for changes 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 Unified Defense 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:

- Completed change control form on the Unified Defense Service Customer Care Service web portal ("**Portal**");
- 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;
- Supporting details relevant to the specific change action; and
- Contingency plans and contact details of Customer personnel performing acceptance testing for the changes to the Security Rules Base.

1.4.8 Unified Defense Server Upgrades

Orange will provide version management of the operating system and various elements of the Unified Defense Server Software. Notwithstanding anything to the contrary contained herein, Orange has no obligation to provide all new releases of Software from the Unified Defense Server hardware vendors and Software licensors, and Orange, in its sole discretion, will decide when upgrades take place.

If Orange needs to take a Unified Defense 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 Unified Defense 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 Expenses.

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

1.5 Service Features

For the Unified Defense Service, Orange will provide the Unified Defense Server with a Firewall and Anti-Virus Software.

1.5.1 Unified Defense Server

The Unified Defense Server supports only static routing, cannot be used as a DNS proxy, and will not support content archive or IM/P2P user filter. Also, all information available on and regarding the Unified Defense Server will be provided in English. Real-time access to the Unified Server's statistics is not supported.

1.5.1.1 Monitoring

Orange monitors the Unified Defense Server installations 24 hours a day, 7 days a week for availability. Unified Defense Server availability does not cover operational problems relating to Internet service, web browsers, or Customer's line to the Internet.

The Unified Defense Server is monitored for 2 types of 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. In the case of a suspected security attack through the Unified Defense Server, Orange will have the right to shut down the Unified Defense Server.

1.5.1.2 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 Unified Defense Server.

1.5.1.3 Connections

All physical connections to the Unified Defense Server must be Ethernet, and the number of Ethernet connections available will depend on the model number of the Unified Defense Server hardware.

1.5.1.4 Logs

The Unified Defense Server is connected to a centralized administration system, which is located on the Orange premises and which may store the logs available on the Unified Defense Server for up to 10 days. The logs stored on the central administration system are subject to the following thresholds, based on the model/configuration of the Unified Defense Server:

Model/Configuration	Log Size Threshold (per Unified Defense Server)
Branch Office (up to 50 potential users)	800 MB
Small Site (up to 750 potential users)	6 GB
Corporate Site (up to 2,000 potential users)	10 GB
Data Center (up to 3,000 potential users)	15 GB

Orange will store the log for up to 1 year unless otherwise required by law. If Orange is so required to store the logs for more than 1 year, Orange will charge Customer for such additional storage time.

1.5.2 Firewall

Orange will implement the Security Rules Base on the Firewall, and the Firewall will examine the header, but not the content, of each packet it receives to match it against the Security Rules Base.

The Firewall 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. Also, a DMZ will be provided to contain potential external and internal threats and attacks.

Customer may access information about the hosts, networks and services declared on the Firewall, as well as the current Security Base Rules implemented on the Firewall, directly on the Unified Defense Server. Orange also will provide Customer with real-time access to the then-current Firewall logs directly on the Unified Defense Server.

1.5.3 Anti-Virus Software

Orange will provide the Anti-Virus Software as a companion service to the Firewall at the Locations identified in the applicable SRFs; the Anti-Virus Software cannot be provided as a stand-alone offer. The Anti-Virus Software allows the Unified Defense Server to be configured to meet Customer's requirements regarding the following actions:

- **File and Email blocking:** The Anti-Virus Software will block files of specified file types (e.g. .exe, .bat, etc.) from passing through the Unified Defense Server or block files or emails that exceed a specified size limit.
- **Virus Protection:** The Unified Defense Server will delete files infected with a virus from the content stream and, when possible, replace them with a standard alert message in English. The Unified Defense Server also will block files that are associated with known categories of unsolicited commercial software programs.

The Anti-Virus Software can be applied to various protocols, as may be specified by Orange from time to time (e.g. HTTP, FTP, POP3, IMAP, SMTP, Instant Messaging, etc.). However, the Unified Defense Server is unable to scan certain file formats (e.g. cdimage, .ace, .bzip2, etc.).

New pattern files for the Anti-Virus Software made available by the Software licensor are automatically downloaded onto the Unified Defense Server.

Customer may access information about the file patterns, categories of filtered files, and a list of blocked viruses directly on the Unified Defense Server. Orange also will provide Customer with real-time access to the then-current Anti-Virus Software logs directly on the Unified Defense Server.

1.6 Optional Features

As optional features of the Unified Defense Service, Customer may order the IDS/IPS, URL Filtering, High Availability, or User Authentication Services; these optional features may be subject to additional charges and are not provided as stand-alone offers.

1.6.1 IDS/IPS

With the IDS/IPS feature, the Unified Defense Server will detect and block malicious or unauthorized behaviors based on known attacks in conjunction with the Security Rules Base. The IDS/IPS feature can label actions associated with a suspicious packet or session as "pass" and "log", and the Unified Defense Server can drop, reset, or clear suspicious packets or sessions and send a log. New pattern files for the IDS/IPS Software made available by the Software licensor are automatically downloaded onto the Unified Defense Server; however, the Unified Defense Server will not support customized signature configuration. Customer will notify Orange of any change on its network architecture and ask for IPS configuration changes if the IPS configuration is to be tuned according to Customer's internal infrastructure.

Customer may access information about the list of signatures and associated actions directly on the Unified Defense Server. Orange also will provide Customer with real-time access to the then-current IDS/IPS logs directly on the Unified Defense Server.

1.6.2 URL Filtering

The URL Filtering Service allows Customer to scan a connection based on, or that supports HTTP protocol only. The URL Filtering Service is a category-based service that examines the content of visited web pages and filters them. The filtering process applies to the URLs, the page contents, and potential activated scripts when users read a web page.

The URL Filtering Service relies on 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 URL Filtering Software provided by the Software licensor are automatically downloaded onto the Unified Defense Server.

Customer can set a total of 3 actions to take when Users access web pages: allow, monitor, or reject. The URL Filtering Service does not provide the ability to partially filter scripts, but blocks all scripts of a denied type. When the URL Filtering Service blocks a web page, the Unified Defense Server will send a standard replacement message, including a short explanation, in English to the User. The URL

Filtering Service logs user activity, and Customer is responsible for declaring such activity to the appropriate authorities, where and when applicable.

Customer may access information about the list of blocked URLs and the categories of blocked URLs directly on the Unified Defense Server. Orange also will provide Customer with real-time access to the then-current URL Filtering Software logs directly on the Unified Defense Server.

Customer may configure parameters of the category-based filter, and for each parameter Customer may:

(a) add up to 100 block/exempt patterns into the content lists;

(b) add up to 100 block/exempt URLs into the URLs list;

(c) create up to 5 local categories and add up to 100 URLs in them; and

(d) modify up to 100 URLs default category.

1.6.3 **High Availability (HA)**

The High Availability Service option provides Customer with 2 Unified Defense Servers, one in active mode (i.e. the master unit) and one in passive mode (i.e. the slave or back-up unit) that continuously share state and configuration data. If the Unified Defense Server in active mode fails, fail-over to the Unified Defense Server in passive mode will occur automatically and all established Firewall connections will be maintained, although some delay-sensitive applications may lose their session and request a new one because of the time required to establish the backup connection (from a few to several dozen seconds). High Availability requires an additional switch to connect the Unified Defense Servers to the Internet access, and both Unified Defense Servers must be exactly in the same configuration.

1.6.4 **User Authentication**

(a) **Internal User Authentication.** Orange will implement a User database on the Unified Defense Server, and Users will be authenticated with a login and password that are not dynamic. Different security profiles can be applied to the different User groups.

(b) **External User Authentication.** To receive External User Authentication, Customer must also receive the Orange Strong Authentication Service, which will be described in a separate Service Description attached to this Agreement and which will be subject to additional Charges. Orange will implement a User database on a server other than the Unified Defense Server. Users will be authenticated with dynamic passwords produced by Tokens, as defined in the Service Description for the Strong Authentication Services. Only one User group can be supported.

1.7 Unified Defense Service Reporting

Through the Portal, Customer's security contacts may access information and daily or weekly reports regarding each of the Unified Defense Service features. 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.

1.8 Maintenance of the Unified Defense Server

1.8.1 **Remedial Maintenance**

Orange will maintain the hardware portion of the Unified Defense Server in Proper Operational Condition. If a Fault is caused by a failure in the Unified Defense Server hardware, Orange will repair the Fault following receipt of a Fault Call or detection of the Fault by Orange, whichever occurs first. If Orange is unable to restore the Unified Defense Server hardware to Proper Operational Condition remotely, an Orange field engineer will be dispatched to the Location.

The GCSC will classify all Fault Calls and 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.

1.8.2 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 Unified Defense Service or the Unified Defense Server caused by any of the following (collectively "**Limitations**"):

(a) Damage to the Unified Defense 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 Orange own representatives, its Subcontractors, or personnel approved in writing by Orange; or

(c) Any instabilities in the operation of the Unified Defense 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 Unified Defense Server and software, even if such combination is specified on a duly accepted SRF, or by any hardware connected to the Unified Defense Server.

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

Remedial Maintenance Services do not include:

- Electrical work external to the Unified Defense 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 Unified Defense Server.

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

END OF SERVICE DESCRIPTION FOR UNIFIED DEFENSE SERVICE