1.1 Network Protect

1.1.1 **Overview.** Network Protect Service is an optional feature of the Business VPN Service. It allows Customer to enhance the security of its Business VPN branch Locations with Orange-managed Firewall and Intrusion Prevention, as described below.

(a) **Network Protect - Firewall.** For Firewall Service, Customer will define the traffic filtering rules corresponding to the CSPR. "**CSPR**" means the Customer Security Policy Request, which is the ordered set of rules against which Customer's data traffic is checked in respect to three zones of the network (i.e. LAN, demilitarized zone or "**DMZ**", and WAN) and which is configured in the CPE for the Firewall Service. The CSPR will be determined by Customer, as set forth in the Service Request Form ("**SRF**"). The CSPR can be set on a universal basis or on a per Location basis. As used herein, 'Firewall' means a method to enhance a network security.

(b) **Network Protect - Intrusion Prevention.** Intrusion Prevention compares the contents of the packet crossing the CPE router against a list of attack signatures (i.e. the signature file). If a packet matches one of the attack signatures, then the packet will be dropped. Orange maintains only one standard version of signature file for all Locations and for all of its customers.

1.1.2 **Availability.** The Network Protect option is available on Business VPN Small, Business VPN Small Off-Net, and Business VPN Corporate, and the availability of this optional feature will vary from country to country.

1.1.3 **Leveling Requirements and Customer Security Policy Request**

(a) To ensure the correct operation of the Network Protect services, software and hardware leveling towards the CPE may be required, and the Charges for such leveling will be in addition to the Charges for Business VPN Service and Network Protect services.

(b) The Firewall service requires Customer to provide Orange with a CSPR at the time it orders the Firewall service. Customer can provide Orange with either a CSPR per Location or a universal CSPR for all Locations.

1.1.4 **Configuration**

(a) **Network Protect – Firewall Service Configuration.** If Customer does not provide a CSPR at the time it orders Network Protect, then Orange will set up an 'Open' configuration, which corresponds to a security policy that does not filter any traffic. Customer will then request a change to the Open configuration once it completes the CSPR. If Customer provides a CSPR without specifying any traffic filtering rules, then the Firewall will be configured as a 'diode' (i.e. all the outgoing traffic from the LAN are authorized and all the incoming traffic are blocked).

(b) **Network Protect – Intrusion Prevention Service.** Orange has one standard version of signature file for all Locations and all customers. If Customer requires a customized signature file for its Locations, then Orange will need to review and approve Customer's requirement, and additional Charges may apply in addition to the Charges for the Intrusion Prevention service and the Business VPN Service.

1.1.5 **Change Management**

(a) **Network Protect – Firewall Service.** Following the installation of the Firewall Service, Orange will accept changes to the CSPR only in accordance with the Change Management services provided as part of the Service Select – Service Support Service, as described in a separate Service Description attached to the Agreement. All changes will be subject to verification by Orange, and Orange will require the following information in addition to any information otherwise required for Service Select – Service Support Service:

- Complete redefinition of the applicable CSPR for the affected Location(s);
- 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 traffic filtering rules for the affected Location(s).

(b) **Network Protect – Intrusion Prevention Service.** Since the signature file for the Intrusion Prevention service is common to all Locations and all Orange customers, Customer cannot modify the standard version of the signature file. Orange may periodically update the standard version of the signature file based on updates made available by the vendor or manufacturer. Customer will only use a change request if it requires a customized signature file to be created by Orange as described in the Clause 1.1.4(b) (Network Protect – Intrusion Prevention Service) above.

1.1.6 **Incident Management.** Incident (as defined in the Service Level Agreement for Business VPN Service) management for Network Protect Service will be provided through the Orange Service Select – Service Support, and will depend on which type of Service Select – Service Support feature (i.e. standard support or extended support) Customer has purchased for the Business VPN Service. If an update of CSPR is required in order to repair an Incident, then Customer must complete and submit a

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL

change request to Orange in accordance with the Change Management services provided as part of the Service Select – Service Support Service. If a 'false positive' Incident (i.e. the packets of a legitimate application match an attack signature, and are dropped) occurs, Customer will contact the GCSC. Once the attack signature that caused the 'false positive' Incident is identified, Customer may elect to deactivate such attack signature on certain Locations by notifying Orange in writing.

1.1.7 **Reporting.** Customers will be able to see via My Service Space its security policy, as implemented by Orange on the CPE router, and the creation date of the attack signatures activated on the CPE router.

1.1.8 **Geographical Coverage.** Unless prohibited by law or regulation, Network Protect services are available in countries where Orange provides Customer with Business VPN Service.

1.1.9 **Limitation of Service.** Network Protect Service does not include any supervision or reporting of security events. Log files are stored on the CPE router and won't be accessible by the Customer. There is also no URL or content filtering with standard Network Protect definition. Network Protect URL Filtering or Web Content Protection system are only available on special request Customer will be solely responsible for its own network security policy and security violation response procedures. While the Network Protect Service enhances Customer's ability to impede unauthorized access to Customer's network and data and assist Customer in detecting potential security breaches and network irregularities, Customer acknowledges that the Network Protect Service does not guarantee in any sense network security or prevent incidents of security breaches. It is Customer's responsibility to design a comprehensive security program in conjunction with any other service providers or professionals chosen by Customer.

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL