Security Annex for Firewalls

Additional Terms for Firewall Service

CONTENTS

1 GLOSSARY OF TERMS & DEFINITIONS

"**DMZ**" means demilitarised zone, i.e. a separate security zone configured on Firewall Device;

"**End Users**" means the actual end user of the Service;

"Event" means when any monitored component of the Service is not operating pursuant to its standard functionality, as indicated by alerts on Interoute's monitoring systems;

"Firewall Device" means the equipment, Virtual Machines (where applicable), systems, cabling and facilities provided by Interoute in order to make the Firewall Service available to the Customer;

"Firewall Policy" means the set of rules required by the Customer to be implemented on the firewall;

"**Firewall Service**" or "**Service**" means the optional feature of an Interoute Service for the supply and operation of the Firewall Device and service and any corresponding Licensed Software and implementation of the Firewall Policy within an Interoute Site;

"HA Pair" means Two (2) Firewall Devices working together in active-active or active-passive mode;

"**Incident**" means an unplanned interruption to a Service or deterioration in the normal quality of a Service;

"**Incident Management**" means the Incident management Service provided by Interoute pursuant to this Annex to investigate an Event or Incident;

"Next Generation Firewall Service" means the optional feature of the Firewall Service as described in paragraph 2.1.2;

"SLO" means Service Level Objective, which is a specific target within the Service Level Agreement;

"**SOW"** means a statement of works, or a data capture form ("DCF") used to capture the details of the Firewall Service, including the Firewall Policy;

"**Virtual Machine**" means a licensed software implementation of a physical server or machine.

Any other terms in capital letters shall have the meaning set forth in Schedule 1.

2 SERVICE DESCRIPTION

Interoute provides three types of Firewall Service that may be combined or purchased separately:

a. The Firewall Service provides the Customer with a Firewall Device maintained by Interoute.

b. The Roaming SSL Access Service allows the Customer's mobile workforce to securely maintain connectivity.

c. The DMZ Service provides a separate security zone configured on a Firewall Device.

2.1 FIREWALL SERVICE AND NEXT GENERATION FIREWALL SERVICE

2.1.1 Interoute shall provision a Firewall Device within an Interoute Site to control and mediate the Customer's network traffic.

2.1.2 The Next Generation Firewall Service provides additional visibility of the firewall devices and access to a reporting management interface, separate to My Services, with customer log in. This is read only access that also allows Next Generation Firewall Service customers to be able to construct reports based upon their parameters.

2.2 ROAMING SSL ACCESS SERVICES

2.2.1 Roaming SSL Access Service may only be purchased in conjunction with the Firewall Service.

2.2.2 Interoute may provide the remote access feature using access based on SSL (Secure Socket Layer) or TLS (Transport Layer Security).

2.3 DMZ SERVICES

2.3.1 The DMZ Service may only be purchased in conjunction with the Firewall Service, and must be directly connected to, or related to, said Firewall Service.

2.3.2 Single or multiple instances of the DMZ Service can be related to one (1) Firewall Service.

2.4 PROVISIONING

2.4.1 As a part of the Service, Interoute shall implement a default firewall configuration aligned to security industry good practices.

2.4.2 Where the Customer has an existing firewall, the Customer may request that Interoute implements the Firewall Policy associated with said firewall onto the Interoute Firewall Service, and Interoute will proceed, subject to the following conditions being met:

a. The implementation shall be performed under a separate SOW, and shall incur Professional Service Charges where thresholds in letter c and d below are exceeded. Assessment of work involved shall be decided at Interoute's sole discretion;

b. The implementation will be carried out at the Customer's own risk and sole cost;

c. The implementation shall require no more than one (1) Working Day of effort from Interoute;

d. The implementation will be carried out during a Working Day;

e. The Customer shall supply all information required to complete the SOW to Interoute within five (5) Working Days of Interoute's request.

3 VENDOR CHANGE

Interoute may from time to time change its third party supplier of these Services. Such change will not require the Customer's consent except where such change is likely to have a material adverse effect on the Service Levels following its implementation.

4 CHARGES

4.1 CHARGES PAYABLE BY THE CUSTOMER

Charges for the Service comprise of an initial on-boarding Installation Charge, a Fixed Rate Charge and any additional Charges set out within the Purchase Order.

4.2 ADDITIONAL CHARGES

Interoute reserves the right to apply the following additional charges in conjunction with those applicable for the Services:

a. Implementation of changes invoiced in accordance with a Change Order.

b. Any additional work agreed to be performed outside of a Working Day, will incur Professional Service Charges.

4.3 CHARGES FOR SERVICE CHANGES

4.3.1 Minor changes are non-chargeable for up to 3 change requests per calendar month then Professional Service Charges apply.

4.3.2 Major changes will incur Professional Service Charges.

5 SERVICE LEVELS

Further to the Service Levels set out within the Schedule 2 to which this Annex is appended, Service Levels are defined for the following Service performance measurements:

a. Firewall Service Availability

5.1 AVAILABILITY

Service	Availability SLO
Firewall Service	99.95%

Interoute uses the following formula to calculate monthly Availability:

$$Availability\ in\ \% = \frac{(Minutes\ in\ Monthly\ Review\ Period - Service\ Unavailability)}{Minutes\ in\ Monthly\ Review\ Period}$$

For the purpose of Availability measurement, Service Unavailability excludes any Planned Outage.

5.2 SERVICE UNAVAILABILITY

The Firewall Service is considered to be Unavailable where the Firewall Device is not operational and processing Customer network traffic.

6 SERVICE CREDITS

6.1 CLAIMING SERVICE CREDITS

6.1.1 Failure to meet a Service Level Objective (SLO) for a Service entitles the Customer to claim Service Credits (subject to the exceptions set out herein and in Schedule 1). The Customer must provide to Interoute all reasonable details regarding the relevant Service Credits claim, including but not limited to, detailed descriptions of the Incident, its duration and any attempts made by Customer to resolve it. Interoute will use all information reasonably available to it to validate claims and make a good faith judgment on whether the Service Levels apply to the claim.

6.1.2 Unavailability of the Service cannot be used to claim failure of another Interoute service. Interoute shall not be responsible for any cross default.

6.2 CALCULATION OF SERVICE CREDITS

Where Availability falls below target during any Monthly Review Period, the Customer will be entitled to Service Credits as follows:

Availability for each applicable firewall during Monthly Review Period falling below target by:	Service Credits as % of the applicable Firewall Fixed Rate Charge
Up to 1%	5%
1% ≤ 2%	10%
2% ≤ 3%	15%
More than 3%	20%

6.2.1 Exclusions to Service Credits for Next Generation Firewall Service

Any software supplied to enable the reporting management services for the Next Generation Firewall Service is supplied as is by third parties (e.g. distributors and or vendors of the equipment in use). Interoute will endeavour to ensure that these services are maintained and available to Next Generation Firewall Service customers. However, any failure of the reporting service will not constitute Unavailability of the Service and therefore will not accrue any Service Credits.

7 CUSTOMER RESPONSIBILITIES

The responsibilities set out in this paragraph 7 shall apply both during provisioning (paragraph 2.4) and during the Term.

7.1 TECHNICAL REPRESENTATIVES

The Customer must designate one or more qualified persons as their technical representatives and support points of contact with Interoute. These technical contacts can be updated online, by phone, or email and must be provided for both pre and post installation, and during Incident Management.

7.2 OTHER RESPONSIBILITIES

Customer undertakes that it shall:

a. Own the Firewall Policy and undertakes to keep Interoute fully informed of the Firewall Policy and to notify Interoute of any changes to it as soon as reasonably practical. Where requested by Interoute, the Customer shall provide a copy of the said Firewall Policy to Interoute.

   i. The Customer acknowledges and accepts that Interoute shall not be responsible for or liable for any security breach or failure resulting from the Firewall Policy and Interoute shall not be obliged to supply or advise on the Firewall Policy.

   ii. Where a Customer has purchased the DMZ Service, it is the Customer's responsibility to ensure that the Firewall Policy takes into account the presence of a DMZ Service and that the same conditions of implementation, record keeping and security control incumbent on the Customer apply when a DMZ Service is present within the Firewall Policy.

   iii. Further to this, Interoute reserves the right not to implement the Firewall Policy where such implementation may result in an Incident on the Service, or impair the integrity of the Interoute Network or impact any Interoute customer.

b. Perform an assessment to determine whether the Firewall Service is suitable for its requirements. Interoute does not warrant that the Firewall Service or the Next Generation Firewall Service will meet such requirements or that the Firewall Service or the Next Generation Firewall Service will operate in the particular circumstances in which it is used by the Customer or that any use will be uninterrupted or error free.

c. report any Incidents or problems with the Services to the Customer Contact Centre as soon as such problems have been identified;

d. provide feedback on any Interoute maintenance approval requests passed to the Customer within the reasonable times specified within such requests;

e. do such other things and provide such information as Interoute may reasonably request in order for Interoute to provide the Service;

f. not initiate a penetration test without agreeing and complying to the current Interoute Penetration Test Agreement. In case a penetration test is undertaken and no respective Interoute Penetration Test Agreement was signed, Customer herby agrees that the Interoute Penetration Test Agreement is deemed to have been signed and that its stipulations bindingly apply.

8 SERVICE OPERATION

8.1 SERVICE CHANGES

8.1.1 Firewall Service

The following changes are minor changes:

a. Loading of critical and security patches onto one (1) Firewall Device or HA Pair

b. Modification to the existing firewall rules

c. Addition of three (3) or fewer rules to the Firewall Policy

Any other change is a major change.

8.1.2 Changes specific to the Roaming SSL Service

For avoidance of doubt, for the Roaming SSL Service, the following changes are major changes:

a. Firewall Policy changes due to a request for user authentication;

b. Add / change SSL configuration.

8.2 INCIDENT MANAGEMENT

8.2.1 Depending on the impact an Event or Incident has on the Service, each Event or Incident is categorized pursuant to paragraph 8.2.2 into one of three priority levels: priority level 1 (Critical), priority level 2 (Major) or priority level 3 (Standard).

8.2.2 Any Events or Incidents relating to a security incident which requires post-restoration investigation are considered out of scope for the Incident Management Service and will incur Professional Service Charges.

Priority	Description	Hours of Operation	Response Time	Update Frequency
Critical (1)	• When the Service is Unavailable.	24/7	30 minutes	2 hours
Major (2)	• The performance of the Service is degraded, but it is still Available • A system or component of the Service is not available and a temporary fix may be available.	Working Day	2 hours	
Standard (3)	• Where there is not a critical need and no impact to the delivery or use of the Service.		4 hours	N/A

If Interoute responds to and works on a reported Incident and it is subsequently found not to be an Incident with the Service then Professional Service Charges will apply.

8.3 EXCLUSIONS

Interoute does not provide any analysis of Incidents and Events on the Service, including analysis or support of information generated by the Next Generation Firewall reporting management interface.

Log files are stored for 90 days, and can be made available on request.

Interoute will not provide technical support to End Users.