

Schedule 2s

Additional terms for Security Services

1. Security Service Description

This Schedule describes the additional terms and conditions applicable to the following Interoute Services:

3. DDoS Protection Service.....	3
4. Email and Web Content Filtering (non-hardware based) Services.....	6
5. Roaming iPASS.....	6
6. Roaming IPsec/SSL Access	6
7. Firewall Service and Managed CPE Firewall Service	7
8. DMZ Service	8
9. Managed Authentication Service	9
10. Web Content Filtering Service (hardware based).....	9

These Services can be acquired by the Customer as supplemental to other Services. The Charges for Security Services will be set out in the applicable Purchase Order.

2. Definitions

In this Schedule, capitalised terms shall have the meaning ascribed to them below:

“**Administrator**” means any person the Customer designates to use MAP to provision and support the End Users and Devices purchased by the Customer;

“**A-PoP or Authentication Point of Presence**” means the designated part of the Interoute Network that communicates with the Customer's Authentication Node;

“**Authentication Node**” means any item of Customer Equipment that is configured to receive access requests from End Users and to forward same along with the End Users' credentials to MAS for verification;

“**Authentication Service**” means an internet based service that validates the credentials of End Users passed to it by the Authentication Node;

“**Black Holing**” means discarding all data destined for a particular IP Address so that it does not disrupt the flow of data to other IP Addresses;

“**Critical Incident**” is a Incident without which there will be a serious business impact to the Customer's online operation;

“**Customer Token Pool**” means the inventory of Devices allocated to Customer and which the Administrator can assign to End Users to be used by End Users for authentication;

“**Deliverable**” means Hardware Devices and Software;

“**Device(s)**” means Hardware Devices and Software Devices;

“**DDoS or Distributed Denial of Service**” means a form of electronic attack involving multiple computers, which send repeated requests to a server (web site) generating false traffic and rendering it inaccessible to valid users;

“**End User**” means anyone who uses an Interoute Service using the Customer's access details;

Schedule 2s

Additional terms for Security Services

“Event Log” means a log file which stores information about several events for future analysis;

“Fault” means an incident that would prevent the use (full or partial) of the Service;

“Firewall Policy” means the document provided to Interoute which states the Customer required rules for Interoute to implement in the Firewall Service;

“Firewall Service” means an optional feature of the IP VPN, Internet or Hosting Service ordered on the applicable Purchase Order comprising Internet Access and a Managed Firewall co-located within one of the Interoute Core IP Nodes;

“Hardware Device(s)” means hardware tokens which may incorporate firmware (such as a key-fob token);

“IP Address” means the identifying number of a computer attached to the Internet. Every computer must have a unique IP Address. IP Addresses are written as four sets of numbers separated by full stops: for example 123.345.63.2;

“IP Customers” means Customers who purchase Internet, VPN, Hosting, Managed or Unmanaged CPE or any other Service type that relies upon the IP Protocol suite as its transport mechanism;

“Managed CPE Firewall” means an optional feature of the Internet Access Service ordered on the applicable Purchase Order comprising Internet Access and a Managed Firewall Service;

“Managed Firewall Equipment” means the Equipment, systems, cabling and facilities provided by Interoute in order to make the Managed Firewall Service available to the Customer;

“MAE” means Metropolitan Area Exchange;

“Managed Firewall Service” means the optional feature of the Internet Service for the supply and operation of Managed Firewall Equipment and Service and any corresponding Licensed Software and implementation of Customer’s Firewall Policy within an Interoute Co-Location facility or a Site;

“Managed Object” means a Customer specific profile configured on Interoute’s DDoS Protection Service detailing the IP addresses or autonomous system number to be protected by the Service.

“MAS or Managed Authentication Service” means the Deliverables and Services;

“MAP” or MAS Administration Portal” means an Internet portal that allows the Administrator, through a web browser, to perform administrative functions including, but not limited to, assigning and de-assigning Devices to End Users;

“NAP” means Network Access Point;

“Non-Critical Request” is a request such as a request for information which has no immediate or significant impact on the running of the Customer online operation;

“Secrets” means passwords, personal identification numbers, question and answer combinations or other information that must be kept confidential and may be used by either Party to identify End Users or to prevent anyone other than the End User from using MAS;

“Secure Items” means Devices and Secrets;

“Software” means (i) Software Devices; and/or (ii) all other software provided by Interoute to Customer;

Schedule 2s

Additional terms for Security Services

“**Software Devices**” means software tokens installed on generic hardware such as a PC, mobile phone or personal digital assistant; and

“**Working Hours**” means 9.00 am-5.00 pm GMT on a Working Day in London;

Any other capitalised terms have the meanings set out in Schedule 1 or the applicable Additional Terms.

3. DDoS Protection Service

a. The following terms and conditions apply where the Customer has indicated on an applicable Purchase Order that they require DDoS Protection or where Interoute has advised the Customer that DDoS Protection is required for the Service(s) they are purchasing. The Interoute DDoS Protection Service offers Customers the ability to protect against DDoS attacks.

b. Provision Of Service

The DDoS Protection Service comprises of the cleaning of the traffic directed towards the Customer's website – and includes:

- I. installation and maintenance of the Service on the relevant Equipment;
- II. configuration of a set of pre-defined monitoring parameters as specified by Interoute;
- III. monitoring of agreed parameters and status information via the Event Log.

c. **Monitoring and Detection** – It is the Customer's responsibility to monitor and detect abnormal or unusual traffic. If any such behaviour is detected, Customer must inform Interoute immediately and request that the DDoS Protection Service is enabled. Following this request, Interoute will work with the Customer to identify when a DDoS attack is occurring.

d. **Cleaning and Mitigation** - When Interoute is notified of an attack, traffic destined for the targeted IP address or autonomous system number will be redirected by Interoute to its DDoS protection infrastructure, for inspection. Diverted traffic will be subjected to multiple layers of statistical analysis, active verification and anomaly recognition to identify malicious sources, reveal abnormal behaviour and discard packets that do not conform to the normal traffic pattern. Whilst traffic cleaning is underway it is envisaged that an increase in latency will occur and during such periods Interoute's standard service performance levels (Service Levels) will not apply.

e. Interoute will use reasonable endeavours to ensure that legitimate traffic is received as normally as possible during an attack, and that the website user experience is affected as little as possible. In an attack, countermeasures will be deployed by Interoute to ensure disruptions to operations are minimised, and measures such as “Black Holing” will only be used by Interoute if all other measures have been deemed by Interoute to have failed or will be likely to fail.

f. Where Customer reports a Non-Critical Request to reconfigure the DDoS parameters, Interoute will use reasonable endeavours to re-configure the Service parameters to achieve maximum DDoS protection with minimum processing overhead and traffic disruption.

g. Interoute will monitor the Devices used by Interoute to provide this Service (via ICMP and SNMP) and Interoute will configure them via secure connections.

h. During the first full calendar month following the Ready For Service Date, the Customer shall be entitled to request certain reasonable changes (to be determined by Interoute) which will be covered by a non-recurring Charge. Thereafter, Interoute will perform a maximum of one (1) Critical Incident

Schedule 2s

Additional terms for Security Services

and five (5) Non-Critical Requests to the Service in any calendar month at no additional Charge, thereafter Interoute reserves the right to levy Charges.

i. The DDoS Protection Service neither offers nor provides:

- I. Load balancing of traffic or of the functionality of any Service, including Security Services described herein
- II. Direct access to Interoute's network security or engineering staff. All initial contact between the Customer and Interoute must be directed to Interoute's Customer Service Centre.
- III. Archival and storage of log files beyond thirty (30) days
- IV. Incident response, forensics and investigations
- V. Legal case preparation, PR incident support
- VI. Security consulting services (e.g. security policy design, security auditing, penetration testing, contingency/disaster recovery planning, etc)
- VII. Security reporting and analysis
- VIII. Permanent filtering or cleaning of traffic

j. **Service Provision requirements**

In order to provide the Service, the following requirements apply:

- I. The Customer will not have access to any Equipment or Software required for the Service;
- II. The Customer must specify the IP Addresses, IP Address ranges or the autonomous system number for which the Customer desires the DDoS Protection Service to be activated, by completing a form which Interoute will provide to the Customer
- III. The Customer must provide Interoute with contact details for the departments and/or people Interoute are to contact during a DDoS attack.

k. **No Warranty**

This Service is designed to protect the Customer and the Customer's End Users from DDoS attacks. However, Interoute does not warrant that it shall withstand these attacks on all occasions. Interoute reserve the right to "Black Hole" any of the Customer traffic as required to protect the Interoute Network or its or its other customers' traffic.

Interoute's DDoS Protection supports a maximum throughput of 20Gbps ("Maximum Throughput"). If the Maximum Throughput is exceeded, the level traffic will be indiscriminately discarded by Interoute's DDoS Protection Service.

l. **Service Levels**

Availability

Interoute will use reasonable efforts to ensure that the DDoS Protection Service is available to the Customer 99% of any Monthly Review Period ("Service Availability").

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

Schedule 2s

Additional terms for Security Services

Unavailability below target	Duration	Service Credits as % of Monthly Recurring Charge:
≤ 0.25% below target		5%
≤ 0.75% below target		10%
≤ 1.5% below target		15%
≤ 2.5% below target		20%
≤ 3.5% below target		25%
> 3.5% below target		30%

Interoute will use reasonable endeavours to reach the following Service Levels:

Response Times:

Non-Critical Request	Response: Within 4 Working Hours Resolution: Within 8 Working Hours
Critical Incident Request (Excludes enabling DDoS Protection)	Response: Within 1 hour Resolution: Within 4 hours
Enabling of DDoS Protection	Within 1 hour of Customer raising a trouble ticket with Interoute

- I. If the Customer requires any work for the provision of service to be undertaken outside of normal Working Hours, or the Customer requests Non-Critical Request support beyond the allocated number per calendar month, Interoute reserve the right to make a charge based on the applicable professional services rate.

II.

Fault Support for DDoS Protection Service

Fault Support	Via NOC, 24 hours per day, 7 days per week
Fault Response	Within 1 hour of receipt of Fault report
Clear	Resumption of service within 8 hours where replacement hardware is not required

- III. Where Interoute can not resolve a Fault at the time the Customer reported the Fault to the Customer's satisfaction then Interoute will ask the Customer to provide a contact telephone number to enable reports on progress with the Fault clearance to be made.
- IV. Interoute will:
 1. provide advice by telephone;
 2. carry out tests and diagnostics on the Service;
 3. work to resolve the Fault within the agreed time period as stated in the table set out above.
- V. If Interoute responds to and works on a reported Fault and it is subsequently found not to be a Fault with the Service then a charge will be made based on the applicable rate.

m. Exclusions

Interoute shall not be liable to the Customer for:

- I. The performance of third party networks including Third Party Local Access circuits, traffic exchange points including Internet networks, transit and peering connections

Schedule 2s

Additional terms for Security Services

provided and controlled by other companies, and public and private exchange points such as NAPs and MAEs;

4. Email and Web Content Filtering (non-hardware based) Services

- a. The following terms and conditions apply where the Customer has indicated on a Purchase Order that they require the Interoute Email Services and/or Web Content Filtering Services. These Services are provided to Customers through Interoute's third party supplier. Email Services include Email Anti Virus, Anti Spam, Email Image control, Email Content control and Boundary encryption Services. Web Content Filtering Services include Web Anti Virus, Web Anti Spyware and Web URL filtering (as defined in the terms and conditions referenced below).
- b. The terms and conditions for the Email Service and the Web Content Filtering Service are available at www.interoute.com/legal. In addition to these terms and conditions, Interoute will provide a first line support service to the Customer's IT department which shall include: call logging and basic technical trouble shooting. Interoute shall, at its sole discretion determine what is classed as first line support. All other support shall be provided by Interoute's third party supplier. Except as set out in this Agreement, Interoute shall have no further liability in relation to these Services.
- c. Provided that it does not materially diminish the quality and functionality of the Service, Interoute reserves the right to change its third party supplier of these Services with 30 Days notice to the Customer.

5. Roaming iPASS

- a. The following terms and conditions apply where IP Customers have indicated on a Purchase Order that they require the Interoute Roaming iPASS Service. This Service is provided to Customers who have End Users that require Internet access from non-fixed locations.
- b. The terms and conditions for the Roaming iPASS Service are available at www.interoute.com/legal. In addition to these terms and conditions, Interoute will provide a first line support service to the Customer's IT department which shall include; call logging and basic technical trouble shooting. Interoute shall, at its sole discretion determine what is classed as first line support. All other support shall be provided by the third party supplier identifiable through the URL above. Except as set out in this Agreement, Interoute shall have no further liability in relation to these Services.
- c. Provided that it does not materially diminish the quality and functionality of the Service, Interoute reserves the right to change its third party supplier of these Services without notice to the Customer.

6. Roaming IPsec/SSL Access

- a. The following terms and conditions apply where IP Customers (who have also purchased the Firewall Service) have indicated on a Purchase Order that they require the Roaming IPsec/SSL Access Service to use with their IPVPN Service. This Service is provided to Customers who have End Users that require access to corporate resources on the IPVPN Service from non-fixed locations. Interoute can provide the Remote Access feature using an IPsec client on mobile devices such as laptops or provide access based on SSL (Secure Socket Layer).
- b. The terms and conditions for the Roaming IPsec/SSL Access Service are available at www.interoute.com/legal. In addition to these terms and conditions, Interoute will provide a support service to the Customer's IT department. Except as set out in this Agreement, Interoute shall have no further liability in relation to these Services.

Schedule 2s

Additional terms for Security Services

- c. Provided that it does not materially diminish the quality and functionality of the Service, Interoute reserves the right to change its third party supplier of these Services without notice to the Customer.

7. Firewall Service

- a. The following terms and conditions apply where IP Customers have indicated on a Purchase Order that they require the Firewall Service.
- b. The Firewall Service is provided to IP Customers who require public Internet access delivered through one central point. The Service offers controlled and mediated public Internet Access through a central interconnect between the Customer VPN and the public Internet. This feature is known as Firewall. Firewall is delivered as a central 100Mb/s or 1 Gb/s connection provided in one of Interoute's facilities. Interoute shall provision a centrally managed firewall device and security policy for this purpose.
- c. Where the Firewall Service is purchased the Customer agrees and warrants to own, maintain and keep a Firewall Policy and undertakes to keep Interoute fully informed of the Firewall Policy and to notify Interoute of any changes to it immediately. Where requested by Interoute, the Customer shall provide a copy of the said Firewall Policy to Interoute.
- d. The Customer acknowledges and accepts that Interoute shall not be responsible for or liable for any security breach or failure resulting from the Customer's Firewall Policy and Interoute shall not be obliged to supply, advise or comply with the Customer's Firewall Policy.
- e. Where the Customer has purchased the Firewall Service, the Customer agrees that it has assessed for itself the suitability of the Firewall Service for its requirements based on the Firewall Policy. Interoute does not warrant that the Firewall Service will meet such requirements or that the 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.
- f. The Parties acknowledge that it is technically impracticable to provide the Firewall Policy Service free of faults. However, without prejudice to the generality of the foregoing, Interoute shall endeavour to provide the Services in accordance with the relevant Service Levels detailed below. Interoute endeavours to carry out maintenance work, updating, remedy, repair or reconnection of Customer Equipment, and the Services in accordance with the provisions contained within this Agreement.

g. Service Availability for the Firewall Service

Service type used when connecting to the Interoute IP Network	Target Site Availability
Firewall Service	99.95%

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

Service Availability for each applicable Site during Monthly Review Period falling below target Availability by:	Service Credits as % of the applicable Site Monthly Charge:
---	--

Schedule 2s

Additional terms for Security Services

Up to 1%	5%
Up to 2%	10%
Up to 3%	15%
More than 3%	20%

Service Credits are the sole and exclusive remedy for any cause of action arising out of the failure of the Firewall Service.

8. DMZ Service

- a. The DMZ Service provides a separate security zone configured on a Firewall device where Interoute provides a Firewall Service.
- b. The following terms and conditions apply where IP Customers have indicated on a Purchase Order that they require the DMZ Service.
- c. The DMZ Service is provided only in conjunction with a new or existing Firewall Service. The DMZ Service(s) is directly connected, or related to its Firewall Service.
- d. Single or multiple incidents of the DMZ Service can be related to one (1) Firewall Service.

e. Service Availability for the DMZ Service:

Service type used when connecting to the Interoute IP Network	Target Service Availability
DMZ Service	99.95%

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

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

- f. Service Credits are the sole and exclusive remedy for any cause of action arising out of the failure of the DMZ Service.
- g. Where an Internet Access 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.
- h. Where the DMZ Service is purchased the Customer agrees and warrants to own, maintain and keep a Firewall Policy and undertakes to keep Interoute fully informed of the Firewall Policy and to notify Interoute of any changes to it immediately. Where requested by Interoute, the Customer shall provide a copy of the 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 Customer's Firewall Policy in relation to the DMZ Service and Interoute shall not be obliged to supply, advise or comply with the Customer's Firewall Policy.

Schedule 2s

Additional terms for Security Services

- j. The Parties acknowledge that it is technically impracticable to provide the DMZ Service free of faults. However, without prejudice to the generality of the foregoing, Interoute shall endeavour to provide the Services in accordance with the relevant Service Levels detailed within this Schedule 2S.

9. Managed Authentication Service

- a. The following terms and conditions apply where IP Customers who have purchase the Roaming IPsec/SSL Service have indicated on a Purchase Order that they require additional security to access their network. This additional fully Managed Authentication Service uses two factor authentication (2FA) Secure Tokens to access the Customer's network. In order to permit access to the Customer's network the End User must have their username, password and (if applicable) the token in their possession.
- b. The end user schedules applicable to the Managed Authentication Service which supplement the terms and conditions contained within this Schedule 2S are available at www.interoute.com/legal . In addition to the terms and conditions set out in the end user schedules, Interoute will provide a first line support service to the Customer's IT department which shall include; call logging and basic technical trouble shooting. Interoute shall, at its sole discretion determine what is classed as first line support. Interoute provide the first line support service between the hours of 08:00 and 18:00, Monday to Friday Central European Time (CET). All other support shall be provided by the third party supplier identifiable through the URL above. Except as set out in this Agreement, Interoute shall have no further liability in relation to these Services.
- c. Provided that it does not materially diminish the quality and functionality of the Service, Interoute reserves the right to change its third party supplier of these Services without notice to the Customer.

d. Optional Managed Authentication Services

- I. **Provisioning Service:** Interoute will 'initialise' all tokens for use on the Managed Authentication Service and will deliver Devices to the Customer at the single token delivery address outlined on the relevant Purchase Order. It shall be the Customer's responsibility to distribute tokens to End Users.
- II. **Initial Set-up:** Interoute will provide reasonable assistance to Customer in the set up of its Authentication Node, including adding the Authentication Node details into MAP.
- III. **Technical Support:** Interoute will provide technical support relating to any aspect of the Managed Authentication Service to the Administrator for the Term of this Agreement. Interoute will not provide technical support to End Users.
- IV. For the avoidance of doubt, the Administrator is solely responsible for the following:
 - 1. Managing profiles, permissions and other aspects in respect of setting up and maintaining End Users within the system;
 - 2. Providing information and instructions to End Users to enable authentication using the Managed Authentication Service;
 - 3. Unlocking, resetting and re-synchronising Devices;
 - 4. Diagnosing and replacing faulty and broken or lost Devices;
 - 5. Managing the operation of the Authentication Node(s).

10. Web Content Filtering Service (hardware based)

- a. The following terms and conditions apply where IP Customers (who have also purchased the Firewall Service) have indicated on a Purchase Order that they require a hardware based web filtering service. The Interoute Web Content Filtering Service is an appliance based Service that provides corporate Customers with a solution to manage their own corporate Internet access policy.

Schedule 2s

Additional terms for Security Services

- b. It is the Customer's responsibility to set its policies, allowing them to decide what content corporate Internet access End Users are allowed to see.
- c. The hardware associated with the Interoute Content Filtering Service is specific to each Customer and allows the Customer to have their own specific policy on the appliance according to corporate guidelines and individual requirements.
- d. The Interoute Web Content Filtering Service must be provisioned in conjunction with the Firewall Service, and can only be sold in the same Interoute co-location facility that is used for the Firewall Service.
- e. This managed Service includes daily updates of the URL categorisation database, which are uploaded onto the appliance daily.
- f. In the event of hardware failure, Interoute will use reasonable endeavours to ensure hardware replacements are delivered to the Customer by the next Working Day. Although the appliance will block all traffic in the event of a hardware failure, Interoute will as soon as reasonably practicable and upon Customer request implement a change to allow the Customer to have unfiltered Internet access directly via the Firewall Service.
- g. Interoute is not responsible for the Customers rules and/or policies. Further, Interoute accepts no liability in relation to such rules and/or policies or their content.
- h. The Customer is responsible for advising Interoute of any websites it requires to be blocked.
- i. Interoute will use reasonable endeavours to provision Customer requests as soon as reasonably possible.
- j. **Service Availability**
 - l. Interoute shall use reasonable endeavours to ensure the Web Content Filtering Service is available 99.5% during any Monthly Review Period. Interoute shall have no liability to the Customer in relation to the Interoute Web Content Filtering Service. Service Credits are not applicable to this Service.

Liability

- l. The provision of Service Credits (where applicable) shall be the sole and exclusive remedy for the failure to meet targets for any Security Service. Interoute shall have no additional liability to the Customer.