BT Compute Protect firewall service
Schedule to the General Terms

Contents

© British Telecommunications plc 2018

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the General Terms

Words that are capitalised but have not been defined in this Schedule have the meanings given to them in the General Terms.

Part A – The BT Compute Protect firewall service

1 Service Summary

BT will provide you with a virtual managed firewall service, comprising:

1.1 the Standard Service Components; and

1.2 any of the Service Options that are selected by you as set out in any applicable Order,

up to the point of the Service Management Boundary as set out in Paragraph 4 ("**BT Compute Protect firewall service**")

2 Standard Service Components

BT will provide you with all of the following standard service components ("**Standard Service Components**") in accordance with the details set out in any applicable Order:

2.1 **Virtual Firewall**

2.1.1 BT will provide a Virtual Firewall image to be deployed within your Cloud Infrastructure.

2.1.2 BT will commission the Virtual Firewall and will establish remote service management of the Virtual Firewall.

2.2 **Service Performance Reports**

2.2.1 BT will provide BT standard near real-time or historic reports for key performance metrics and for security-related events via a Customer Portal.

2.3 **Network Segments**

2.3.1 BT will support multiple (virtual) network segments.

3 Service Options

BT will provide you with any of the following options ("**Service Options**") that are set out in any applicable Order and in accordance with the details set out in that Order:

3.1 **VPN:**

3.1.1 BT will set up and configure the following types of VPN in accordance with BT's prevailing technical standards as set out in the user guide provided to you by BT:

(a) site-to-site VPNs between two Virtual Firewalls which are both managed by BT;

(b) remote access VPNs, for remote Users to gain secure access to your internal network. BT will implement your rules to authenticate the User's access against your authentication server; and

(c) third party (extranet) VPNs, for creating a site-to-site VPN between your Virtual Firewall managed by BT, and a Virtual Firewall owned or managed by you or a third party. BT will only deliver VPNs to firewalls managed by a third party after the Service Start Date.

3.2 **Firewall Intrusion Detection and Prevention Service:**

3.2.1 BT will:

(a) monitor traffic passing through your Virtual Firewall for attacks, in accordance with the applicable intrusion signature files;

(b) implement this Service Option with a default configuration setting, including a standard signature list;

(c) maintain a subscription, on your behalf with the supplier, to the signature updates;

(d) apply the signature updates following issue to BT by the supplier of the Software;

(e) block high impact or high confidence attacks, as defined by the supplier of the Software; and

(f) disable the appropriate signature (or signature group if necessary) if you advise BT of a conflict with any of your legitimate business traffic.

3.2.2 BT will not:

(a) make changes to the standard signature list;

(b) evaluate the signatures before applying them; and
(c) monitor, provide alerts or service specific reports outside of the generic monitoring, alerting or summary reporting.

3.2.3 Reporting for this Service Option will be available in accordance with Paragraph 2.2.

3.2.4 If BT alters the parameters for applying new signatures in "**block**" mode upon your request, you will accept responsibility for the increased risk of false positives (blocks to legitimate traffic) or the increased risk of attacks being missed.

3.3 **Firewall URL Filtering and Application Control:**

3.3.1 BT will:

(a) block access to the Internet sites that you ask BT to, in accordance with your CSP;
(b) send an appropriate message to a User attempting to access a blocked or restricted Internet site to advise either:
(i) that the User request has been blocked; or
(ii) that the User will first confirm acceptance of your acceptable use policy (or similar warning). Upon acceptance, the page will be delivered; and
(c) implement any alterations via the standard configuration management process, as set out in the user guide provided to you by BT, in the event of any change in your CSP.

3.3.2 Reporting for this Service Option will be available in accordance with Paragraph 2.2.

3.4 **Firewall Anti-Virus:**

3.4.1 BT will:

(a) check web browser (http) traffic for known malware;
(b) inspect requests from Users for an executable file from a site on the Internet, against the current antivirus definition file set out in the applicable intrusion signature files. If no virus is detected, the file will be passed to the User. If a virus is detected the file will be blocked and deleted; and
(c) keep antivirus definition files up to date by regular downloads direct from the supplier.

3.4.2 Reporting for this Service Option will be available in accordance with Paragraph 2.2.

3.5 **Firewall Anti-Bot Service:**

3.5.1 BT will check and block outbound traffic for communication with known command and control servers used by owners of malicious software.

3.5.2 Reporting for this Service Option will be available in accordance with Paragraph 2.2.

3.6 **Ad Hoc Professional Service:**

3.6.1 BT will provide ad hoc technical support, chargeable per day, as set out in the applicable Order.

3.6.2 Professional Services are delivered remotely unless otherwise set out in the applicable Order.

3.7 **CSP production:**

3.7.1 BT will provide Professional Services to assist you in the production and implementation of your CSP for a period of three Business Days.

3.7.2 If additional time is required for the creation of your CSP, BT will charge you for this in accordance with Paragraph 3.6.

3.8 **Log Streaming:**

3.8.1 BT will configure your Virtual Firewall to provide a log stream to your SIEM.

3.9 **Eagle-I Enhanced Firewall Service:**

3.9.1 BT shall provide you with the Eagle-I Enhanced Firewall Service, subject to the requirements set out below.

(a) Existing Blocklist Enhancement
(i) Subject to BT confirming that your Security Appliance is suitable for use with the Eagle-I Enhanced Firewall Service, BT will use its Eagle-I Platform to identify any unique malicious IPs and/or URLs to supplement your Security Appliance's existing blocklist of malicious IPs and/or URLs ("**Indicators of Compromise**" or "**IOCs**".)
(ii) Upon confirming the suitability of your Security Appliance, BT will add new IOCs to the BT Blocklist for consumption by your Security Appliance ("**Existing Blocklist Enhancement**".)

(b) Automated IOC Blocking
(i) Subject to BT confirming the technical feasibility of applying Automated IOC Blocking to your Security Appliance, as part of its remote service management of your Security

Appliance, BT shall automatically implement changes to your Security Appliance so that it will block IOCs propagated from the BT Blocklist ("**Automated IOC Blocking**").

(ii) For the avoidance of doubt, when the Eagle-I Enhanced Firewall service is specified, subject to the requirements of technical feasibility (as outlined above at Paragraph 3.1.15(b)(i)), BT shall implement Automated IOC Blocking. By specifying the Eagle-I Enhanced Firewall Service, you hereby consent to BT implementing Automated IOC Blocking in respect of your Security Appliance.

(iii) BT shall not be responsible for any wider impact of any Automated IOC Blocking, including but not limited to any impact from the Automated IOC Blocking on Customer Equipment, or on your wider Network.

4 Service Management Boundary

4.1 BT will provide and manage the BT Compute Protect firewall service as set out in Parts A, B and C of this Schedule, ("**Service Management Boundary**").

4.2 BT is responsible for monitoring and managing the Virtual Firewall.

4.3 BT will have no responsibility for the BT Compute Protect firewall service outside the Service Management Boundary, including:

4.3.1 issues on Users' machines or your servers (e.g. operating system, coding languages and security settings);

4.3.2 end to end network connectivity (e.g. your network or Internet connectivity); or

4.3.3 managing identities of Users.

4.4 BT does not make any representations or warranties, whether express or implied, as to any outcomes of Automated IOC Blocking undertaken as part of the Eagle-I Enhanced Firewall Service Option, including but not limited to any reduction in security incidents or to the threat impact on any Customer Equipment or your wider Network.

5 Associated Services and Third Parties

5.1 You will have the following services in place to be able to deploy the Virtual Firewall prior to the BT Compute Protect firewall service being delivered. You will ensure that these services meet the minimum technical requirements that BT may specify:

5.1.1 the BT Cloud Compute Service; and

5.1.2 SIEM, if you select the Log Streaming Service Option,

(each an "**Enabling Service**").

5.2 If BT provides you with any services other than the BT Compute Protect firewall service (including, but not limited to any Enabling Service) this Schedule will not apply to those services and those services will be governed by their separate terms and conditions.

6 Specific Terms

6.1 **Changes to the BT Compute Protect firewall service**

6.1.1 BT may amend the Charges at any time by either:

(a) publishing the amendment online via the Customer Portal; or

(b) by giving Notice to you.

6.1.2 BT may propose changes to this Schedule (unless those changes relate to the Charges where Paragraph 6.1.1 applies) by giving you Notice at least 30 days prior to the change taking effect ("**Notice to Amend**").

6.1.3 Within 21 days of any Notice to Amend, you will provide BT Notice:

(a) agreeing to the changes BT proposed, in which case those changes will apply from the date of our agreement; or

(b) terminating the Contract.

6.1.4 If we have not reached agreement in accordance with Paragraph 6.1.3(a) within 15 days, the terms of this Schedule will continue to apply unless you give Notice in accordance with Paragraph 6.1.3(b) or BT may give Notice of termination, in which case BT will immediately cease delivering the BT Compute Protect firewall service.

6.1.5 Except as set out above in Paragraphs 6.1.1 and 6.1.2, both of us will agree any other changes to the Contract in accordance with the provisions in Clause 31 of the General Terms.

6.2 **Minimum Period of Service**

6.2.1 At the end of the Minimum Period of Service, unless one of us has given at least 14 days' Notice to the other of an intention to terminate the BT Compute Protect firewall service in accordance with the Contract, BT will continue to provide the BT Compute Protect firewall service and each of us will continue to perform our obligations in accordance with the Contract.

6.2.2 If either of us gives Notice to the other of an intention to terminate the BT Compute Protect firewall service, BT will cease delivering the BT Compute Protect firewall service at 23.59 on the last day of the Minimum Period of Service.

6.3 **Termination for Convenience**

For the purposes of Clause 17 of the General Terms either of us may, at any time after the Service Start Date and without cause, terminate the BT Compute Protect firewall service or any Order by giving 14 days' Notice to the other.

6.4 **Customer Committed Date**

6.4.1 If you request a change to the BT Compute Protect firewall service or any part of the BT Compute Protect firewall service, then BT may revise the Customer Committed Date to accommodate that change.

6.4.2 BT may expedite delivery of the BT Compute Protect firewall service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

6.5 **Changes to your CSP**

6.5.1 You may request additions, deletions, or modifications to your CSP and BT will enable you to request Standard Changes or Urgent Changes to your CSP, either on the Customer Portal or via the Service Desk.

6.5.2 The CSP changes set out in Paragraph 6.5.1 refer only to requests to change the rule-sets that define the BT Compute Protect firewall service's operation.

6.5.3 BT will use reasonable endeavours to identify errors or potential unforeseen consequences of your requested CSP changes and advise you appropriately.

6.5.4 BT will not be liable for any consequences arising from:

(a) your misspecification of your security requirements in your CSP; or

(b) unforeseen consequences of a correctly specified and correctly implemented CSP.

6.5.5 BT will only make configuration changes as set out in Paragraph 6.5.1.

6.5.6 BT will apply the following "**reasonable use**" restrictions for changes to your CSP:

(a) you will not raise change requests more frequently than once a week. This will be measured by BT as an average over a rolling period of three months, per CSP. In the event that BT's measurements show that you are raising change requests more frequently than once per week, BT may, either:

(i) aggregate your requests over a period of time, so that they may be implemented more efficiently. In this event there may be some implementation delays; or

(ii) review your requirements and agree with you an appropriate alternative implementation process and any associated Charges.

6.6 **Invoicing**

6.6.1 Unless set out otherwise in any applicable Order, BT will invoice you for the following Charges in the amounts set out in any applicable Order:

(a) Installation Charges, on the Service Start Date;

(b) Recurring Charges, except Usage Charges, monthly in advance on the first day of the relevant month and for any period where the BT Compute Protect firewall service is provided for less than one month, the Recurring Charges will be calculated on a daily basis;

(c) Usage Charges, monthly in arrears, calculated at the then current rates;

(d) Professional Services Charges; and

(e) any Termination Charges incurred in accordance with Paragraph 6.7 upon termination of the relevant BT Compute Protect firewall service.

6.6.2 BT may invoice you for any of the following Charges in addition to those set out in any applicable Order:

(a) Charges for investigating and resolving Incidents that you report to BT where BT finds no Incident or that the Incident is caused by something for which BT is not responsible under the Contract;

(b) Charges for restoring BT Compute Protect firewall service if the BT Compute Protect firewall service has been suspended in accordance with Clause 10.1.2 of the General Terms;

(c) Charges for expediting provision of the BT Compute Protect firewall service at your request after BT has informed you of the Customer Committed Date;

(d) reasonable expenses incurred by BT in providing configuration information in accordance with Paragraph 7.4.2;

(e) Charges for the upgrade of the Virtual Firewall if required by you, unless the upgrade is operationally necessary to enable BT to continue to provide the BT Compute Protect firewall service. This does not apply to patching of applications or changes to your CSP. Any upgrade that is required as a result of capacity issues arising as a consequence of an increase in traffic or activation of new features will be charged to you;

(f) Charges incurred due to inaccuracies in information provided by you to BT, including the requirements of your CSP; and

(g) any other Charges set out in any applicable Order or the Customer Portal or otherwise agreed between both of us.

6.6.3 The invoicing start date for the BT Compute Protect firewall service is the Service Start Date.

6.7 **Termination Charges**

6.7.1 If you terminate the Contract or the BT Compute Protect firewall service for convenience in accordance with Clause 17 of the General Terms you will pay BT:

(a) all outstanding Charges or payments due and payable under the Contract;

(b) any other Charges as set out in any applicable Order; and

(c) any charges reasonably incurred by BT from a supplier as a result of the early termination.

6.7.2 In addition to the Charges set out at Paragraph 6.7.1 above, if you terminate during the Minimum Period of Service, you will pay BT Termination Charges, as compensation, equal to 100 per cent of the Recurring Charges for the remainder of the Minimum Period of Service.

6.7.3 BT will refund to you any remaining balance which you have paid in advance after deducting any Charges or other payments due to BT under the Contract. This refund will also be subject to adjustments for any discounts that have been received due to the advance payment.

6.8 **Service Constraints**

6.8.1 Given the nature and volume of malicious and unwanted electronic content, BT does not warrant that:

(a) the BT Compute Protect firewall service is error free;

(b) the BT Compute Protect firewall service will detect all security or malicious code threats; or

(c) that use of the BT Compute Protect firewall service will keep your network or computer systems free from all viruses or other malicious or unwanted content or safe from intrusions or other security breaches.

6.8.2 You will be responsible for results obtained from the use of the BT Compute Protect firewall service, and for conclusions drawn from such use.

6.8.3 BT will not be liable for any damage or Claims caused by errors or omissions in any information, instructions or scripts provided to BT by you in connection with the BT Compute Protect firewall service, or any actions taken by BT at your direction.

6.8.4 In respect of the Firewall Anti-Virus Service Option, the executable file that is being inspected is subject to a maximum file size of 10 per cent of the available RAM allocated to the Virtual Firewall and up to a maximum limit of 1.6GB.

6.8.5 The BT Compute Protect firewall service may not be available in all locations.

6.8.6 Some Service Options may not be available on all Virtual Firewalls.

6.8.7 BT will not be liable if BT is unable to deliver the BT Compute Protect firewall service because of a lack of capacity on your selected Virtual Firewalls.

6.8.8 BT will not pro-actively view your reports and events for security incidents.

6.8.9 The period over which data can be analysed is dependent on the number of events occurring on the Virtual Firewall and logged by the Virtual Firewall.

Part B – Service Delivery and Management

7 BT's Obligations

7.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the BT Compute Protect firewall service, BT will provide you with contact details for the Service Desk.

7.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

7.2.1 configure the Service Option(s) selected by you;

7.2.2 conduct a series of standard tests on the BT Compute Protect firewall service to ensure that it is configured correctly; and

7.2.3 on the date that BT has completed the activities in this Paragraph 7.2, confirm to you that the BT Compute Protect firewall service is available for performance of any Acceptance Tests as set out in Paragraph 8.2.

7.3 **During Operation**

On and from the Service Start Date, BT:

7.3.1 will respond and use reasonable endeavours to remedy an Incident without undue delay if BT detects or if you report an Incident with the BT Compute Protect firewall service;

7.3.2 will, for a period of five Business Days after the Service Start Date, implement any minor changes or corrections to your CSP that may be necessary for the operation of the BT Compute Protect firewall service. BT will implement such changes as soon as reasonably practicable. Any substantial changes to your CSP will incur additional Charges and may be scheduled for implementation following this initial five Business Day period in accordance with Paragraph 6.5;

7.3.3 will maintain any relevant Customer Portal and server to provide you with online access to a range of functions including performance reports and placing CSP change requests in accordance with Paragraph 6.5;

7.3.4 may carry out Maintenance from time to time and will use reasonable endeavours to inform you at least five Business Days before any Planned Maintenance on the BT Compute Protect firewall service. However, BT may inform you with less notice than normal where Maintenance is required in an emergency;

7.3.5 may, in the event of a security breach affecting the BT Compute Protect firewall service, require you to change any or all of your passwords;

7.3.6 will use secure protocols or a secure management link to connect to the Virtual Firewall via the Internet or other agreed network connection, in order to monitor the BT Compute Protect firewall service proactively and to assist in Incident diagnosis;

7.3.7 will, if you select the CSP production Service Option as set out in Paragraph 3.7, capture the necessary information in consultation with your Customer Contact and produce your CSP;

7.3.8 will continuously monitor your Virtual Firewall for security alerts and regularly poll the Virtual Firewall to check it is operational;

7.3.9 provide you with a user guide for the BT Compute Protect firewall service; and

7.3.10 where the Eagle-I Enhanced Firewall Service Option is specified, BT will implement any changes as part of Automated IOC Blocking as quickly as is technically practicable.

7.4 **The End of the Service**

On termination of the BT Compute Protect firewall service by either of us, BT will:

7.4.1 terminate any rights of access to the relevant Customer Portal and stop providing all other elements of the BT Compute Protect firewall service; and

7.4.2 where requested in writing prior to the termination of this Contract, provide, where reasonably practical, configuration information relating to the BT Compute Protect firewall service in a format that BT reasonably specifies, provided you have, at that time, paid all Charges outstanding at and resulting from termination (whether or not due at the date of termination). You will pay all reasonable expenses incurred by BT in providing this information.

8 Your Obligations

8.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the BT Compute Protect firewall service by BT, you will:

8.1.1 complete any preparation activities that BT may request to enable you to receive the BT Compute Protect firewall service promptly and in accordance with any reasonable timescales;

8.1.2 in jurisdictions where an employer is legally required to make such disclosure to its Users and other employees:

(a) inform your Users or other employees that as part of the BT Compute Protect firewall service being delivered by BT, BT may monitor and report to you the use of any targeted applications by them;

(b) ensure that your Users or other employees have consented or are deemed to have consented to such monitoring and reporting (if such consent is legally required); and

(c) agree that BT will not be liable for any failure by you to comply with this Paragraph 8.1.2, and you will be liable to BT for any Claims, losses, costs or liabilities incurred or suffered by BT due to your failure to comply with this Paragraph 8.1.2;

8.1.3 if you have not paid for the CSP production Service Option as set out in Paragraph 3.7, submit, at the time of placing an Order, a CSP that meets the requirements and specifications advised by BT to you, including specifications that cover your legacy network, application services and other Enabling Services, using the CSP requirements template provided by BT;

8.1.4 retain responsibility for your CSP;

8.1.5 manage, and provide BT with accurate details of your internal IP Address design;

8.1.6 modify your network routing to ensure appropriate traffic is directed to the Virtual Firewall.

8.1.7 ensure that Virtual Firewalls are able, in accordance with BT's instructions or any user guide provided to you by BT, to receive updates, such as vulnerability signatures, directly over the Internet, or over an alternative path agreed with BT for that purpose;

8.1.8 ensure that your network and all applications conform to relevant industry standards and provide written confirmation to BT upon reasonable request;

8.1.9 not act to misuse the BT Compute Protect firewall service to contravene or circumvent any Applicable Laws. BT may treat any contravention of the Applicable Laws as a material breach and:

(a) suspend the BT Compute Protect firewall service and BT may refuse to restore BT Compute Protect firewall service until BT receives an acceptable assurance from you that there will be no further contravention; or

(b) terminate the BT Compute Protect firewall service upon Notice in accordance with Clause 25 of the General Terms;

8.1.10 use the Virtual Firewall image to create a Virtual Firewall within your Cloud Infrastructure;

8.1.11 provide BT with the IP Address to enable BT to take over the management of the Virtual Firewall;

8.1.12 provide and manage your own end-user VPN software including authentication of Users if you select the VPN Service Option set out in Paragraph 3.1; and

8.1.13 be responsible for the availability of and the correct configuration of the Enabling Services in accordance with the user guide provided to you by BT.

8.2 **Acceptance Tests**

8.2.1 You will carry out the Acceptance Tests for the BT Compute Protect firewall service within five Business Days after receiving Notice from BT in accordance with Paragraph 7.2.3 ("**Acceptance Test Period**").

8.2.2 The BT Compute Protect firewall service is accepted by you if you confirm acceptance in writing during the Acceptance Test Period or is treated as being accepted by you if you do not provide BT with Notice to the contrary by the end of the Acceptance Test Period.

8.2.3 Subject to Paragraph 8.2.4, the Service Start Date will be the earlier of the following:

(a) the date that you confirm in writing acceptance of, or BT deems acceptance of, the BT Compute Protect firewall service in accordance with Paragraph 8.2.2; or

(b) the date of the first day following the Acceptance Test Period.

8.2.4 If, during the Acceptance Test Period, you provide BT Notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide you Notice that BT has remedied the non-conformance and inform you of the Service Start Date.

8.3 **During Operation**

On and from the Service Start Date, you will:

8.3.1 ensure that Users report Incidents to the Customer Contact and not to the Service Desk;

8.3.2 ensure that the Customer Contact will take Incident reports from Users and pass these to the Service Desk using the reporting procedures agreed between both of us, and will be available for all subsequent Incident management communications;

8.3.3 notify BT of any planned work that may cause an Incident;

8.3.4 ensure that any Customer Equipment that is connected to the BT Compute Protect firewall service or that you use, directly or indirectly, in relation to the BT Compute Protect firewall service is:

(a) technically compatible with the BT Compute Protect firewall service and will not harm or damage BT Equipment, the BT Network, or any of BT's supplier's or subcontractor's network or equipment;

(b) connected, approved and used in accordance with relevant instructions, standards and Applicable Law and any safety and security procedures applicable to the use of that Customer Equipment; and

(c) adequately protected against viruses and other breaches of security;

8.3.5 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment:

(a) does not meet any relevant instructions, standards or Applicable Law; or

(b) contains or creates material that is in breach of the Acceptable Use Policy and you are contacted by BT about such material,

and redress the issues with the Customer Equipment prior to reconnection to the BT Compute Protect firewall service;

8.3.6 distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the BT Compute Protect firewall service, including the Customer Portal;

8.3.7 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the BT Compute Protect firewall service and:

(a) immediately terminate access for any person who is no longer a User;

(b) inform BT immediately if a user ID or password has, or is likely to, become known to an unauthorised person, or is being or may be used in an unauthorised way;

(c) take all reasonable steps to prevent unauthorised access to the BT Compute Protect firewall service;

(d) satisfy BT's security checks if a password is lost or forgotten; and

(e) change any or all passwords or other systems administration information used in connection with the BT Compute Protect firewall service if BT requests you to do so in order to ensure the security or integrity of the BT Compute Protect firewall service;

8.3.8 request, if applicable, up to five login/password combinations for access to a Customer Portal for use by you or your agents. You may assign one login combination to BT's personnel. You are responsible for your agents' use of these IDs;

8.3.9 not stop, close down or delete the Virtual Machine on which the Virtual Firewall is hosted without the prior written consent of BT. BT shall not unreasonably withhold or delay its consent; and

8.3.10 take daily VM Snap Shots of the Virtual Firewall.

8.4 **The End of the Service**

On termination of the BT Compute Protect firewall service by either of us, you will destroy the Virtual Machine on which the Virtual Firewall is hosted.

9 Notification of Incidents

Where you become aware of an Incident:

9.1 the Customer Contact will report it to the Service Desk;

9.2 BT will give you a Ticket;

9.3 BT will inform you when it believes the Incident is cleared and will close the Ticket when:

9.3.1 you confirm that the Incident is cleared within 24 hours of being informed; or

9.3.2 BT has attempted unsuccessfully to contact you, in the way agreed between both of us in relation to the Incident, and you have not responded within 24 hours of BT's attempt to contact you.

9.4 If you confirm that the Incident is not cleared within 24 hours of being informed, the Ticket will remain open and BT will continue to work to resolve the Incident.

9.5 Where BT becomes aware of an Incident, Paragraphs 9.2, 9.3 and 9.4 will apply.

9.6 BT will keep you informed throughout the course of the Incident resolution at regular intervals. Updates may be provided by telephone or email.

Part C – Service Levels

10 On Time Delivery

10.1 **On Time Delivery Service Level**

10.1.1 BT will deliver the BT Compute Protect firewall service on or before the Customer Committed Date (the "**On Time Delivery Service Level**").

10.2 **On Time Delivery Service Credits**

10.2.1 If BT does not meet the On Time Delivery Service Level, you may claim On Time Delivery Service Credits for each day after the Customer Committed Date until the Service Start Date as set out in this Paragraph 10.

10.2.2 You may claim On Time Delivery Service Credits by reporting any failure to meet the On Time Delivery Service Level to the Service Desk in accordance with Paragraph 10.

10.2.3 If both of us have agreed a revised Customer Committed Date in writing, or if BT exercises BT's right to revise the Customer Committed Date as set out in Paragraph 6.4.1, the calculation of any On Time Delivery Service Credits will be made by reference to the revised Customer Committed Date.

10.3 **Exceptions**

10.3.1 The On-Time Delivery Service Level does not apply to upgrades or changes to the BT Compute Protect firewall services, unless these require the installation of new components and have an agreed delivery date, in which case the Customer Committed Date will be that agreed delivery date.

10.3.2 The On-Time Delivery Service Level does not apply to access to the Service Performance Reports via the Customer Portal or the ability to request CSP changes via the Customer Portal.

11 Service Availability

11.1 **Availability Service Level**

11.1.1 From the Service Start Date, BT will provide the BT Compute Protect firewall service with a target availability corresponding to the applicable SLA Category for the BT Compute Protect firewall service as set out in the table in Paragraph 11.2.1 below (the "**Availability Service Level**").

11.1.2 You may request Availability Service Credits for Qualifying Incidents at either:

(a) the Standard Availability Service Credit Rate, as set out in Paragraph 11.3.5; or

(b) as applicable, the Elevated Availability Service Credit Rate, as set out in Paragraph 11.3.6.

11.2 **SLA Categories**

11.2.1 The following table sets out the Availability Annual Target, the Maximum Annual Availability Downtime, the Maximum Monthly Availability Downtime, and the Service Credit Interval for each SLA Category:

SLA Category	Availability Annual Target	Maximum Annual Availability Downtime	Maximum Monthly Availability Downtime	Service Credit Interval
Cat B	≥ 99.9%	8 hours	1 hour	1 hour

11.3 **Availability Service Credits**

11.3.1 If a Qualifying Incident occurs, BT will measure the Availability Downtime for the Virtual Firewall starting from when you report or BT gives you notice of a Qualifying Incident, and ending when BT closes the Incident in accordance with Paragraph 9.3.

11.3.2 BT will measure the Availability Downtime in units of full minutes.

11.3.3 BT will then calculate the cumulative Availability Downtime per Virtual Firewall for the calendar month in which the Qualifying Incident occurred ("**Cumulative Monthly Availability Downtime**") and for the previous 12 consecutive calendar months (the "**Cumulative Annual Availability Downtime**").

11.3.4 In the event a Virtual Firewall has been installed for less than 12 consecutive months, BT will apply an assumed Cumulative Annual Availability Downtime for the previous 12 consecutive months for that Virtual Firewall using the Availability Downtime data recorded to date.

11.3.5 In the event that the Cumulative Monthly Availability Downtime of a Virtual Firewall exceeds the Maximum Monthly Availability Downtime, you may request Availability Service Credits at the Standard Availability Service Credit Rate for each stated Service Credit Interval above the Maximum Monthly Availability Downtime.

11.3.6 In the event that the Cumulative Annual Availability Downtime of a Virtual Firewall, measured in accordance with Paragraph 11.3.1 above, exceeds the Maximum Annual Availability Downtime, you

may request Availability Service Credits for all further Qualifying Incidents at the Elevated Availability Service Credit Rate for each started Service Credit Interval above the Maximum Annual Availability Downtime up to and until the Cumulative Annual Availability Downtime of a Virtual Firewall is less than the Maximum Annual Availability Downtime. The Elevated Availability Service Credits under this Paragraph 11.3.6 replace the Standard Availability Service Credits in Paragraph 11.3.5 and will be applicable irrespective of the Cumulative Monthly Availability Downtime of a Virtual Firewall exceeding the Maximum Monthly Availability Downtime in the respective month.

12 Requests for Service Credits

12.1 You may request applicable Service Credits within 28 days of the end of the calendar month in which a Qualifying Incident occurred by providing details of the reason for the claim. Any failure by you to submit a request in accordance with this Paragraph 12.1 will constitute a waiver of any claim for Service Credits for that calendar month.

12.2 Upon receipt of a valid request for Service Credits in accordance with Paragraph 12.1;

12.2.1 BT will issue you with the applicable Service Credits by deducting those Service Credits from your invoice within two billing cycles of the request being received; and

12.2.2 following termination of the Contract where no further invoices are due to be issued by BT, BT will pay you the Service Credits in a reasonable period of time.

12.3 Service Credits for all Service Levels will be aggregated and are available up to a maximum amount equal to 100 per cent of the Monthly Recurring Charge for the affected Virtual Firewall.

12.4 All Service Levels and Service Credits will be calculated in accordance with information recorded by, or on behalf of, BT.

12.5 The Service Levels under this Schedule will not apply:

12.5.1 in the event that Clause 8 or Clause 23 of the General Terms applies; or

12.5.2 during any trial period of the BT Compute Protect firewall service.

13 CSP Change Request Delivery Time Targets

13.1 Targets apply to Urgent and Standard Changes.

13.2 The response time for the changes is set out below:

Request	Target Response
Urgent Change	4 Hours
Standard Change	8 Hours

13.2.1 Service Credits do not apply to CSP change requests.

Part D – Defined Terms

14 Defined Terms

In addition to the defined terms in the General Terms, capitalised terms in this Schedule will have the below meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms, these defined terms will take precedence for the purposes of this Schedule). BT has repeated some definitions in this Schedule that are already defined in the General Terms. This is to make it easier for you to find the definitions when reading this Schedule.

"**Acceptance Test Period**" has the meaning given in Paragraph 8.2.1.

"**Acceptance Tests**" means those objective tests conducted by you that when passed confirm that you accept the BT Compute Protect firewall service and that the BT Compute Protect firewall service is ready for use save for any minor non-conformities that will be resolved as an Incident in accordance with Paragraph 7.3.1.

"**Automated IOC Blocking**" has the meaning given in Paragraph 3.9.1(b)(i).

"**Availability**" means the period of time when a Virtual Firewall is functioning.

"**Availability Annual Target**" has the meaning given in the table at Paragraph 11.2.1 for the relevant SLA Category.

"**Availability Downtime**" means the period of time during which a Qualifying Incident exists as measured by BT in accordance with Paragraph 11.3.1.

"**Availability Service Credit**" means the Service Credit available for a failure to meet the Availability Service Level and calculated at the Standard Availability Service Credit Rate or at the Elevated Availability Service Credit Rate as applicable.

"**Availability Service Level**" has the meaning given in Paragraph 11.1.1.

"**BT Blocklist**" means any IOCs which BT has identified using its Eagle-I Platform.

"**BT Cloud Compute Service**" means the BT cloud based service providing you with a self-service capability to browse, select, provision, and manage virtual infrastructure including a Virtual Machine, network, storage for recording and storing information and data, and security.

"**BT Compute Protect firewall service**" has the meaning given in Paragraph 1.

"**Cloud Infrastructure**" means your virtual infrastructure used to host the Virtual Firewall or which is protected by the Virtual Firewall.

"**CSP**" means your customer security policy containing the security rules, set and owned by you, that are applied to the Virtual Firewall and determine the operation of the BT Compute Protect firewall service.

"**Cumulative Annual Availability Downtime**" has the meaning given in Paragraph 11.3.3.

"**Cumulative Monthly Availability Downtime**" has the meaning given in Paragraph 11.3.3.

"**Customer Equipment**" means any equipment including any Purchased Equipment and any software, used by you in connection with the BT Compute Protect firewall service.

"**Customer Portal**" means one or more webpages made available to you by BT to provide for one or more specific functions in relation to the BT Compute Protect firewall service.

"**Eagle-I Enhanced Firewall Service**" means the Service Option specified at Paragraph 3.9.

"**Eagle-I Platform**" means the solution through which BT shall identify IOCs.

"**Elevated Availability Service Credit Rate**" means 8 per cent of the Monthly Recurring Charges for the applicable Virtual Firewall.

"**Enabling Service**" has the meaning given in Paragraph 5.1.

"**Existing Blocklist Enhancement**" has the meaning given in Paragraph 3.9.1(a)(ii).

"**General Terms**" means the general terms to which this Schedule is attached or can be found at www.bt.com/terms, and that form part of the Contract.

"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the BT Compute Protect firewall service or particular element of the BT Compute Protect firewall service.

"**Installation Charges**" means those Charges set out in any applicable Order in relation to installation of the BT Compute Protect firewall service or any Purchased Equipment, Customer Equipment or BT Equipment as applicable.

"**Internet**" means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.

"**Internet Protocol**" or "**IP**" means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.

"**IOCs**" or "**Indicators of Compromise**" has the meaning given in Paragraph 3.9.1(a)(i).

"**IP Address**" means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.

"**Maximum Annual Availability Downtime**" has the meaning given in the table at Paragraph 11.2.1 for the relevant SLA Category.

"**Maximum Monthly Availability Downtime**" has the meaning given in the table at Paragraph 11.2.1 for the relevant SLA Category.
"**Minimum Period of Service**" means a period of 30 consecutive days beginning on the Service Start Date.
"**Monthly Recurring Charges**" means the monthly Recurring Charges for the applicable Virtual Firewall and the sum of the Usage Charges for the three full previous months divided by three.
"**Notice to Amend**" has the meaning given in Paragraph 6.1.2.
"**On Time Delivery Service Credits**" means the Service Credit available for a failure to meet the On Time Delivery Service Level, which are equal to 4 per cent of the Recurring Charges for the applicable Virtual Firewall, per day.
"**On Time Delivery Service Level**" has the meaning given in Paragraph 10.1.
"**Planned Maintenance**" means any Maintenance BT has planned to do in advance.
"**Professional Services**" means those services provided by BT which are labour related services.
"**Qualifying Incident**" means a Severity Level 1 Incident, except where any of the following events have occurred:

(a) the BT Compute Protect firewall service has been modified or altered in any way by you, or by BT in accordance with your instructions;
(b) Planned Maintenance;
(c) you have performed any configurations on the Enabling Services that BT did not approve or you cease or disable the Enabling Services;
(d) an Incident has been reported and BT cannot confirm that an Incident exists after performing tests; or
(e) you requested BT to test the BT Compute Protect firewall service at a time when no Incident has been detected or reported.

"**RAM**" means random access memory.
"**Recurring Charges**" means the Charges for the BT Compute Protect firewall service or applicable part of the BT Compute Protect firewall service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.
"**Security Information and Event Management**" or "**SIEM**" means software operating centrally which collects, stores, and analyses logs from perimeter to end user. It monitors for security threats in real time for quick attack detection, containment, and response with holistic security reporting and compliance management.
"**Service Credit Interval**" has the meaning given in the table at Paragraph 11.2.1 for the relevant SLA Category.
"**Service Desk**" means the helpdesk that you are able to contact to submit service requests, report Incidents and ask questions about the BT Compute Protect firewall service.
"**Service Level**" means each of the On Time Delivery Service Level and the Availability Service Level.
"**Service Management Boundary**" has the meaning given in Paragraph 4.
"**Service Options**" has the meaning given in Paragraph 3.
"**Service Performance Reports**" means the Standard Service Component set out in Paragraph 2.2.
"**Service Start Date**" means the date BT first makes a BT Compute Protect firewall service available to you even if access to the Service Performance Reports via the Customer Portal or the ability to request CSP changes via the Customer Portal are not available.
"**Severity Level 1 Incident**" means an Incident that cannot be circumvented and that constitutes a complete loss of service at a Virtual Firewall.
"**SLA Category**" means the category, which, in accordance with the table set out at Paragraph 11.2.1, specifies the following in relation to the applicable Virtual Firewall:

(a) Availability Annual Target;
(b) Maximum Annual Availability Downtime;
(c) Maximum Monthly Availability Downtime; and
(d) Service Credit Interval.

"**Standard Availability Service Credit Rate**" means 4 per cent of the Monthly Recurring Charges for the applicable Virtual Firewall.
"**Standard Change**" means upgrades and modifications resulting from planned developments and security improvements.
"**Standard Service Components**" has the meaning given in Paragraph 2.
"**Ticket**" means the unique reference number provided by BT for an Incident and that may also be known as a "**fault reference number**".
"**Uniform Resource Locator**" or "**URL**" means a character string that points to a resource on an intranet or the Internet.
"**Urgent Change**" means upgrades and modifications needed as a result of unplanned activities or unforeseen activities which are critical to maintaining the security of your organisation. BT may charge you for an Urgent Change.

"**Usage Charges**" means the Charges for the BT Compute Protect firewall service or applicable part of the BT Compute Protect firewall service that are calculated by multiplying the volume of units that you used or incurred in a period (e.g. number of agents using the BT Compute Protect firewall service, or the number of minutes the BT Compute Protect firewall service was used for) with the relevant fee as set out in any applicable Order.
"**Virtual Firewall**" means a software based network security system that uses rules to control incoming and outgoing network traffic.
"**Virtual Machine**" or "**VM**" means a self-contained operating system that functions as a separate server.
"**VM Snap Shot**" means a recording of the state and data of a Virtual Machine at a particular point in time, so the same state can be returned to repeatedly if required. The VM Snap Shot is not a copy of the Virtual Machine's disk volume but a change log file from the moment in time when the VM Snap Shot was taken.
"**VPN**" means a virtual private network with the use of encryption to provide a communications network that appears private to your Users while being provided over the Internet.