Virtual Firewall Public Cloud Service
Schedule to the General Terms

Contents

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 Virtual Firewall Public Cloud Service

1 Service Summary

BT will provide you with a remotely managed service capability that will deliver, manage and orchestrate a variety of firewall services through a software platform hosted on your Public Cloud Infrastructure, comprising of:

1.1 the Standard Service Components; and

1.2 any of the Service Options as set out in any applicable Order,

up to the point of the Service Management Boundary as set out in Paragraph 4 ("**Virtual Firewall Public Cloud Service**").

2 Standard Service Components

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

2.1 **Virtual Firewall Application**

BT will:

2.1.1 provide the Virtual Firewall within your Public Cloud Infrastructure, which will be installed and base configured by you or whichever party manages your Public Cloud Infrastructure on your behalf. BT will then gain access once it is running to complete the configuration and ensure that traffic is passing through the Virtual Firewall from your Public Cloud Infrastructure;

2.1.2 provide management and support by:

(a) monitoring the Virtual Firewall;
(b) diagnosing and resolving failures on the Virtual Firewall; and

2.1.3 provide service performance reports via the BT Portal.

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:

(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 URL Filtering and Application Control**

3.2.1 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) and upon acceptance by the User, the page will be delivered; and

(c) implement any alterations, via the standard configuration management process, in the event of any change in your CSP.

3.2.2 This Service Option does not include reporting as standard. Reporting may be available in accordance with Paragraph 3.8.

3.3 **Firewall Anti-Virus**

3.3.1 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 firewall supplier.

3.3.2 This Service Option does not include reporting as standard. Reporting may be available in accordance with Paragraph 3.8.

3.4 **Firewall Anti-Bot**

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

3.5 **Firewall Intrusion Detection and Prevention Service**

3.5.1 BT will:

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

(b) implement this Service Option with a default configuration setting, as defined by the supplier of the Software used to deliver the IPS;

(c) maintain a subscription to the necessary signature updates, and arrange their application when issued by the Supplier. BT will not be responsible for evaluating these signatures beforehand **("IPS").**

3.5.2 BT will advise you how the IPS that you have selected operates with regard to alerting or IPS specific reporting.

3.5.3 If BT agrees to a request from you to alter the parameters for applying new signatures in "block" mode, to give a greater or lower sensitivity to attacks, you certify that you are aware of the increased risk of false positives (blocks to legitimate traffic) or the increased risk of attacks being missed.

3.5.4 If the SSL/TLS Inspection is selected, BT will scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided your CSP permits such scanning.

3.6 **SSL/TLS Inspection**

3.6.1 BT will intercept and decrypt SSL Encrypted Traffic in order to carry out inspection in accordance with the CSP. Once the traffic has been inspected, it will be re-encrypted and relayed to its original destination (if permitted by the CSP) (**"SSL/TLS Inspection"**).

3.6.2 BT will not intercept and decrypt SSL Encrypted Traffic for every category of web content due to a high possibility of issues between associated applications and certain websites.

3.7 **Ad Hoc Professional Services**

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

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

3.8 **Security Event Reporting**

3.8.1 BT will provide reporting facilities, either on-line or on a server hosted on your Site, which allows analysis of security-related events.

3.8.2 If this Service Option is delivered via a shared reporting platform, BT will configure the platform such that you are only provided with access to your reports. This may mean that some of the platform's functionality is restricted to preserve the confidentiality of all customers using that platform.

3.8.3 The period over which data can be analysed is dependent on the capacity of the reporting platform or the space allocated on the reporting platform.

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 3.9.1(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 Virtual Firewall Public Cloud Service as set out in Parts A, B and C of this Schedule ("**Service Management Boundary**").

4.2 BT will have no responsibility for the Virtual Firewall Public Cloud Service outside the Service Management Boundary, including:

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

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

4.2.3 managing identities of Users; and/or

4.2.4 your Public Cloud Infrastructure.

4.3 BT will not have access to, and will not manage, your Public Cloud Infrastructure as part of this Virtual Firewall Public Cloud Service.

4.4 BT does not make any representations, whether express or implied, about whether the Virtual Firewall Public Cloud Service will operate in combination with any Customer Equipment or other equipment and software.

4.5 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

5.1 You will have the following services in place that will connect to the Virtual Firewall Public Cloud Service and are necessary for the Virtual Firewall Public Cloud Service to function and will ensure that these services meet the minimum technical requirements that BT specifies:

5.1.1 Internet circuit with a static WAN IP Address; and

5.1.2 public cloud native load balancer (if a high availability pair of virtual firewalls are required),

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

5.2 If BT provides you with any services other than the Virtual Firewall Public Cloud 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.

6 Specific Terms

6.1 **Minimum Period of Service and Renewal Periods**

6.1.1 Unless one of us gives Notice to the other of an intention to terminate the Virtual Firewall Public Cloud Service at least 90 days before the end of the Minimum Period of Service or a Renewal Period, at the end of the Minimum Period of Service or Renewal Period the Virtual Firewall Public Cloud Service will automatically extend for a Renewal Period and:

(a) BT will continue to provide the Virtual Firewall Public Cloud Service;

(b) the Charges applicable during the Minimum Period of Service may cease to apply and BT may propose changes to the Charges in accordance with Paragraph 6.1.2. If BT proposes changes to the Charges, BT will invoice you the Charges agreed in accordance with Paragraph 6.1.3 from the beginning of the following Renewal Period; and

(c) both of us will continue to perform each of our obligations in accordance with the Contract.

6.1.2 BT may propose changes to this Schedule or the Charges (or both) by giving you Notice at least 90 days prior to the end of the Minimum Period of Service and each Renewal Period ("**Notice to Amend**").

6.1.3 Within 30 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 beginning of the following Renewal Period; or

(b) terminating the Contract at the end of the Minimum Period of Service or Renewal Period, as applicable.

6.1.4 If either of us gives Notice to the other of an intention to terminate the Virtual Firewall Public Cloud Service in accordance with Paragraph 6.1.1 or Paragraph 6.1.3, BT will cease delivering the Virtual Firewall Public Cloud Service at 23.59 on the last day of the Minimum Period of Service or subsequent Renewal Period as applicable.

6.2 **Termination for Convenience**

For the purposes of Clause 17 of the General Terms, either of us may, at any time after the end of the Minimum Period of Service and without cause, terminate the Virtual Firewall Public Cloud Service or any Order by giving 90 days' Notice to the other.

6.3 **Customer Committed Date**

6.3.1 If you request a change to the Virtual Firewall Public Cloud Service or any part of the Virtual Firewall Public Cloud Service, then BT may revise the Customer Committed Date to accommodate that change.

6.3.2 BT may expedite delivery of the Virtual Firewall Public Cloud Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

6.4 **Changes to your CSP**

6.4.1 BT will apply the following "reasonable use" restrictions ("Reasonable Use Policy") for changes to the CSP(s):

(a) you will not raise Standard Change requests more frequently than:

(i) six per month per Security Appliance in respect of Foundation;

(ii) eight per month per Security Appliance in respect of Foundation Plus; and

(iii) 10 per month per Security Appliance in respect of Premium;

(b) you will not raise Urgent Change requests more frequently than:

(i) one per month per Security Appliance in respect of Foundation;

(ii) two per month per Security Appliance in respect of Foundation Plus; and

(iii) three per month per Security Appliance in respect of Premium;

(c) where BT's measurements show that change requests are being raised more frequently than as set out in Paragraphs 6.4.1(a) and 6.4.1(b), 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.]

6.4.2 You may request changes to your CSP in relation to the rule-sets that define the Virtual Firewall Public Cloud Service operation, either via the BT Portal or the Service Desk.

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

6.4.4 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.

6.4.5 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.

6.5 **Invoicing**

6.5.1 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) Recurring Charges, monthly in advance on the first day of the relevant month and for any period where the Virtual Firewall Public Cloud Service is provided for less than one month, the Recurring Charges will be calculated on a daily basis; and

(b) Professional Services Charges.

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

(a) Charges for investigating 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 commissioning the Virtual Firewall Public Cloud Service in accordance with Paragraph 7.2 below, outside of Business Hours;

(c) Charges for expediting provision of the Virtual Firewall Public Cloud 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 below;

(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 Virtual Firewall Public Cloud 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;

(g) Charges for restoring Service if the Service has been suspended in accordance with Clause 10.1.2 of the General Terms;

(h) any Termination Charges incurred in accordance with Paragraph 6.6 below, upon termination of the relevant Virtual Firewall Public Cloud Service; and

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

6.6 **Termination Charges**

6.6.1 If you terminate the Contract or the Virtual Firewall Public Cloud 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 early termination.

6.6.2 In addition to the Charges set out at Paragraph 6.6.1 above, if you terminate during the Minimum Period of Service or any Renewal Period, you will pay BT:

(a) for any parts of the Virtual Firewall Public Cloud Service that were terminated during the Minimum Period of Service or Renewal Period, Termination Charges, as compensation, equal to:

(i) 100 per cent of the Recurring Charges for any remaining months of the first 12 months of the Minimum Period of Service or Renewal Period; and

(ii) 20 per cent of the Recurring Charges for the remaining months, other than the first 12 months of the Minimum Period of Service or Renewal Period; and

(b) for any parts of the Virtual Firewall Public Cloud Service that were terminated after the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to 20 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service.

6.6.3 If you terminate the Virtual Firewall Public Cloud Service the Termination Charges set out in Paragraph 6.6.2 will be calculated on the Recurring Charges after any discount has been applied.

6.6.4 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.

6.7 **Service Constraints**

6.7.1 BT does not warrant that:

(a) the Virtual Firewall Public Cloud Service is error free;

(b) the Virtual Firewall Public Cloud Service will detect all security or malicious code threats; or

(c) use of the Virtual Firewall Public Cloud 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.

6.7.2 You will be responsible for results obtained from the use of the Virtual Firewall Public Cloud Service, and for conclusions drawn from such use.

6.7.3 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 Virtual Firewall Public Cloud Service, or any actions taken by BT at your direction.

6.7.4 The Virtual Firewall Public Cloud Service may not be available in all locations.

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

6.7.6 BT will not be liable if BT is unable to deliver the Virtual Firewall Public Cloud Service because of a lack of network capacity on your selected Virtual Firewalls.

6.7.7 BT will not pro-actively view your reports and events for security vulnerabilities.

6.7.8 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 Virtual Firewall Public Cloud 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 Virtual Firewall Public Cloud Service;

7.2.2 conduct a series of standard tests on the Virtual Firewall Public Cloud 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 Virtual Firewall Public Cloud Service is available for performance of any Acceptance Tests in accordance with Paragraph 8.2 below.

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 and in accordance with the Service Levels in Part C of the Contract if BT detects or if you report an Incident;

7.3.2 will, for a period of five consecutive 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 Virtual Firewall Public Cloud Service. BT will implement such changes as soon as reasonably practicable;

7.3.3 will maintain the BT Portal to provide you with access to reports and to place CSP change requests in accordance with Paragraph 6.4 above;

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 Virtual Firewall Public Cloud 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 Virtual Firewall Public Cloud 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 Virtual Firewall Public Cloud Service proactively and to assist in Incident diagnosis;

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

7.3.8 will not be liable for any delay in rectifying an Incident with the Virtual Firewall Public Cloud Service, where the Virtual Firewall Public Cloud Service is connected to a non-BT provided Enabling Service and BT is unable to connect to the Virtual Firewall in order to rectify such Incident; and

7.3.9 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 Virtual Firewall Public Cloud Service by either of us, BT will:

7.4.1 terminate any rights of access to the BT Portal and stop providing all other elements of the Virtual Firewall Public Cloud Service; and

7.4.2 where requested in writing prior to the termination of this Contract, provide, where reasonably practical, information relating to the Virtual Firewall Public Cloud 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 Virtual Firewall Public Cloud Service, you will:

8.1.1 provide BT with the WAN IP of the newly installed Virtual Firewall so BT can access and manage the Virtual Firewall;

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

(a) inform your Users that as part of the Virtual Firewall Public Cloud 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, 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;

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

8.1.4 modify your network routing to ensure appropriate traffic is directed to the Virtual Firewall;

8.1.5 ensure that Virtual Firewalls are able, in accordance with BT's instructions 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;

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

8.1.7 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;

8.1.8 ensure, unless BT has agreed in writing to do so, that the LAN protocols and applications you use, are compatible with the Virtual Firewall Public Cloud Service;

8.1.9 provide your LAN details to BT when requested without undue delay;

8.1.10 not misuse the Virtual Firewall Public Cloud Service to contravene or circumvent local laws and regulations; such contravention will be treated as a material breach and BT may:

(a) suspend the Virtual Firewall Public Cloud Service and refuse to restore the Virtual Firewall Public Cloud Service until BT receives an acceptable assurance from you that there will be no further contravention or circumvention; or

(b) terminate the Virtual Firewall Public Cloud Service upon written Notice;

8.1.11 provide BT with any information that is reasonably requested by any regulatory body, legal authority or government entity in any country in connection with the encryption capabilities of the Virtual Firewall Public Cloud Service;

8.1.12 obtain any local import and User licenses and any necessary written authority from the relevant regulatory bodies to enable BT to provide you with the Virtual Firewall Public Cloud Service;

8.1.13 provide BT with any documentation reasonably required in order to deliver the Virtual Firewall Public Cloud Service, including documentation relating to the Enabling Services set out in Paragraph 5.1 above.

8.2 **Acceptance Tests**

8.2.1 You will carry out the Acceptance Tests for the Virtual Firewall Public Cloud Service within five Business Days after receiving Notice from BT in accordance with Paragraph 7.2.3 ("**Acceptance Test Period**").

8.2.2 The Virtual Firewall Public Cloud 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 or BT deems acceptance of the Virtual Firewall Public Cloud Service in writing 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 is available for all subsequent Incident management communications;

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

8.3.4 monitor and maintain any Customer Equipment connected to the Virtual Firewall Public Cloud Service or used in connection with a Virtual Firewall Public Cloud Service including your hardware and Virtual Machine managing software hosting the Virtual Firewall.

8.3.5 ensure that any Customer Equipment that is connected to the Virtual Firewall Public Cloud Service or that you use, directly or indirectly, in relation to the Virtual Firewall Public Cloud Service is:

(a) adequately protected against viruses and other breaches of security;
(b) technically compatible with the Virtual Firewall Public Cloud Service and will not harm or damage BT Equipment, the BT Network, or any of BT's suppliers' or subcontractors' network or equipment; and
(c) 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;

8.3.6 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 resolve the issue with the Customer Equipment prior to reconnection to the Virtual Firewall Public Cloud Service;

8.3.7 distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the BT Portal;

8.3.8 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the BT Portal and:

(a) immediately terminate access for any person who is no longer a User;
(b) inform BT immediately if a User's 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 Portal and your Public Cloud Infrastructure;
(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 Portal if BT requests you to do so in order to ensure the security or integrity of the Virtual Firewall Public Cloud Service.

8.3.9 request, if applicable, up to five login/password combinations for access to the BT Portal for use by you or your agents. You may assign one login combination to BT's service support personnel.

8.3.10 before reporting an Incident to BT, ensure that any Enabling Service is working correctly;

8.3.11 not disclose any information in relation to the performance of the Virtual Firewall Public Cloud Service to any third party without BT's prior written consent; and

8.3.12 duplicate and store Content you wish to keep on other devices not connected to the Virtual Firewall Public Cloud Service.

8.4 **The End of the Service**

On termination of the Virtual Firewall Public Cloud Service by either of us, you will promptly return or delete any Confidential Information that you have received from BT during the term of the Contract.

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 after having been 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 following BT's attempt to contact you.

9.4 If you confirm that the Incident is not cleared within 24 hours after having been 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 Service Availability

10.1 **Availability Service Level**

10.1.1 From the Service Start Date, BT will provide the Virtual Firewall Public Cloud Service with a target availability corresponding to the applicable SLA Category for the Virtual Firewall as set out in the applicable Order, as set out in the table in Paragraph 10.2.1 ("**Availability Service Level**")

10.1.2 You may request Availability Service Credits for Severity Level 1 Incidents at either:

(a) the Standard Availability Service Credit Rate, as set out in Paragraph 10.3.4; or

(b) as applicable, the Elevated Availability Service Credit Rate, as set out in Paragraph 10.3.5.

10.2 **SLA Categories**

10.2.1 The following table sets out the Availability Annual Targets, the Maximum Annual Availability Downtime, the Maximum Monthly Availability Downtime, the Standard Availability Service Credit Rate, the Elevated Availability Service Credit Rate and the Service Credit Interval for each SLA Category:

SLA Category	Availability Annual Target	Maximum Annual Availability Downtime	Maximum Monthly Availability Downtime	Standard Availability Service Credit Rate	Elevated Availability Service Credit Rate	Service Credit Interval
Cat A++	≥ 99.999%	5 minutes	0 minutes	4%	8%	5 min
Cat A+	≥ 99.99%	1 hour	0 minutes	4%	8%	15 min
Cat A1	≥ 99.97%	3 hours	0 minutes	4%	8%	1 hour
Cat A	≥ 99.95%	4 hours	0 minutes	4%	8%	1 hour
Cat B	≥ 99.90%	8 hours	1 hour	4%	8%	1 hour
Cat C	≥ 99.85%	13 hours	3 hours	4%	4%	1 hour
Cat D	≥ 99.80%	17 hours	5 hours	4%	4%	1 hour
Cat E	≥ 99.70%	26 hours	7 hours	4%	4%	1 hour
Cat F	≥ 99.50%	43 hours	9 hours	4%	4%	1 hour
Cat G	≥ 99.00%	87 hours	11 hours	4%	4%	1 hour
Cat H	≥ 98.00%	175 hours	13 hours	4%	4%	1 hour
Cat I	≥ 97.00%	262 hours	15 hours	4%	4%	1 hour

10.3 **Availability Service Credits**

10.3.1 If a Severity Level 1 Incident occurs, BT will measure the Availability Downtime for the Virtual Firewall(s) starting from when you report or BT gives you notice of a Severity Level 1 Incident, and ending when BT closes the Incident in accordance with Paragraph 9.3 above.

10.3.2 BT will measure the Availability Downtime in units of full minutes during the Contracted Maintenance Hours.

10.3.3 BT will then calculate the cumulative Availability Downtime for the calendar months in which the Severity Level 1 Incident occurred ("**Cumulative Monthly Availability Downtime**") and for the previous 12 consecutive calendar months (the "**Cumulative Annual Availability Downtime**"), but in the event that the 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 using the Availability Downtime data recorded to date.

10.3.4 If the Cumulative Monthly Availability Downtime of the Virtual Firewall Public Cloud Service exceeds the Maximum Monthly Availability Downtime, you may request Availability Service Credits at the Standard Availability Service Credit Rate for each Service Credit Interval above the Maximum Monthly Availability Downtime.

10.3.5 If the Cumulative Annual Availability Downtime of the Virtual Firewall Public Cloud Service exceeds the Maximum Annual Availability Downtime, you may request Availability Service Credits for all further Severity Level 1 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 by Service is less than the Maximum Annual Availability Downtime.

10.4 **Exceptions**

10.4.1 The Availability Service Level does not apply to Incidents caused by the unavailability of the Enabling Service.

11 Requests for Service Credits

11.1 You may request applicable Service Credits within 28 days of the end of the calendar month in which a Severity Level 1 Incident occurred by providing details of the reason for the claim. Any failure by you to submit a request in accordance with this Paragraph will constitute a waiver of any claim for Service Credits for that calendar month.

11.2 Upon receipt of a valid request for Service Credits in accordance with Paragraph 11.1 above:

11.2.1 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

11.2.2 following expiry or 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.

11.3 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.

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

11.5 The Service Levels under this Schedule will not apply:

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

11.5.2 during any trial period of the Virtual Firewall Public Cloud Service;

11.5.3 to Simple Service Requests; or

11.5.4 to any Incident not reported in accordance with Paragraph 9.

12 CSP Change Request Delivery Time Targets

12.1 BT will deliver Urgent and Standard Changes to your CSP in accordance with the table set out in Paragraph 12.2.

12.2 The target response times for any Urgent or Standard Changes to your CSP are as follows:

Request	Target Response
Urgent Change	4 Hours
Standard Change	8 Hours

12.3 Service Credits will not apply to any CSP change requests.

Part D – Defined Terms

13 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 Virtual Firewall Public Cloud Service and that the Virtual Firewall Public Cloud 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 the Virtual Firewall Public Cloud Service is functioning.

"**Availability Annual Target**" has the meaning given in the table at Paragraph 10.2.1 for the relevant SLA Category.

"**Availability Downtime**" means the period of time during which a Severity Level 1 Incident exists as measured by BT in accordance with Paragraph 10.3.1.

"**Availability Service Credit**" means the Service Credit available for a failure to meet the Availability Service Level, as set out in Paragraphs 10.3

"**Availability Service Level**" has the meaning given in in Paragraph 10.1.

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

"**BT Network**" means the communications network owned or leased by BT.

"**BT Portal**" means an online web page you can access to view the current status of your Virtual Firewall Public Cloud Service.

"**Business Hours**" means between the hours of 08.00 and 17.00 in a Business Day.

"**Content**" means applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material.

"**Contracted Maintenance Hours**" means the times during which BT will provide maintenance for the Virtual Firewall Public Cloud Service, which are Business Hours unless set out otherwise in any applicable Order.

"**Cumulative Annual Availability Downtime**" has the meaning given in Paragraph 10.3.3.

"**Cumulative Monthly Availability Downtime**" has the meaning given in Paragraph 10.3.3.

"**Customer Equipment**" means any equipment including any software, other than BT Equipment, used by you in connection with a Virtual Firewall Public Cloud Service.

"**Customer Security Policy**" or "**CSP**" means your security policy containing the security rules, set and owned by you, that are applied to the Virtual Firewall and determine the operation of the Virtual Firewall Public Cloud 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 the applicable rate as set out in the table at Paragraph 10.2.1 for the relevant SLA Category.

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

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

"**Firewall Intrusion Detection and Prevention Service**" means the Service Option as set out in Paragraph 3.5.

"**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 Virtual Firewall Public Cloud Service or particular element of the Virtual Firewall Public Cloud Service.

"**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.

"IPS" has the meaning given in Paragraph 3.5.1.

"**Local Area Network**" or "**LAN**" means the infrastructure that enables the ability to transfer IP services within Site(s) (including data, voice and video conferencing services).

"**Maximum Annual Availability Downtime**" has the meaning given in the table at Paragraph 10.2.1 for the relevant SLA Category.
"**Maximum Monthly Availability Downtime**" has the meaning given in the table at Paragraph 10.2.1 for the relevant SLA Category.
"**Minimum Period of Service**" means a period of 12 consecutive months beginning on the Service Start Date, unless set out otherwise in any applicable Order.
"**Notice to Amend**" has the meaning given in Paragraph 6.1.2.
"**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.
"**Public Cloud Infrastructure**" means a virtual infrastructure that is delivered or accessed via the Internet.
"**Qualifying Incident**" means an Incident, except where any of the following events have occurred:

(a) the Virtual Firewall Public Cloud Service has been modified or altered in any way by you, or by BT in accordance with your instructions;
(b) Maintenance;
(c) you have performed any network configurations 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;
(e) you requested BT to test the Virtual Firewall Public Cloud Service at a time when no Incident has been detected or reported; or
(f) the Incident has arisen as a result of you changing your CSP(s).

"**Recurring Charges**" means the Charges for the Virtual Firewall Public Cloud Service or applicable part of the Virtual Firewall Public Cloud Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.
"**Renewal Period**" means for each Virtual Firewall Public Cloud Service, the initial 12 month period following the Minimum Period of Service, and each subsequent 12 month period.
"**Security Appliance**" means the BT Equipment or Purchased Equipment that BT manages on your behalf as part of the Associated Services used to apply the CSP(s). The Security Appliance may be physical or virtual.
"**Service Credit Interval**" has the meaning given in the table at Paragraph 10.2.1 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 Virtual Firewall Public Cloud Service.
"**Service Level**" means the Availability Service Level.
"**Service Management Boundary**" has the meaning given in Paragraph 4.1.
"**Service Options**" has the meaning given in Paragraph 3.
"**Severity Level 1 Incident**" means a Qualifying Incident that cannot be circumvented and that constitutes a complete loss of service at the Site(s).
"**Simple Change**" means the Simple Changes set out in the document titled Simple and Complex Change which may be accessed on the BT Portal.
"**Simple Service Request**" means small requests, as set out on the BT Portal, for predefined simple configuration changes to the Virtual Firewall Public Cloud Service, which have no impact on your inventory.
"**Site**" means a location at which the Virtual Firewall Public Cloud Service is provided.
"**SLA Category**" means the category, as set out in any applicable Order, which, in accordance with the table set out at Paragraph 10.2.1, specifies the following in relation to the Virtual Firewall Public Cloud Service or Site:

(a) Availability Annual Target;
(b) Maximum Annual Availability Downtime;
(c) Maximum Monthly Availability Downtime;
(d) Standard Availability Service Credit Rate;
(e) Elevated Availability Service Credit Rate; and
(f) Service Credit Interval.

"SSL" means secure sockets layer.
"SSL Encrypted Traffic" means means encrypted traffic transferred via the following protocols that BT will support for SSL/TLS Inspection:

(a) HTTPS;
(b) SMTPS;
(c) POP3S;
(d) IMPAS; and
(e) FTPS.

"SSL/TLS Inspection" has the meaning given in Paragraph 3.6.1.

"**Standard Availability Service Credit Rate**" means the applicable rate as set out in the table at Paragraph 10.2.1 for the relevant SLA Category.
"**Standard Change**" means in respect of a Simple Change upgrades and modifications needed as a result of planned developments and security improvements.
"**Standard Service Components**" has the meaning given in Paragraph 2.
"**Supplier**" means Fortinet Inc., 899 Kifer Road, Sunnyvale, CA USA or Fortinet Singapore Pvt Ltd, Beach Road, #20-01, The Concourse, Singapore 199555, as applicable.
"**Ticket**" means the unique reference number provided by BT for an Incident and that may also be known as a "**fault reference number**".
"**Urgent Change**" means in respect of a Simple Change upgrades and modifications needed as a result of unplanned activities or unforeseen activities, but which are not critical to maintaining the security of the organisation. BT may charge you for an Urgent Change.
"**Virtual Firewall**" means a software based network security system that uses rules to control incoming and outgoing network traffic.
"**Virtual Firewall Public Cloud Service**" has the meaning given in Paragraph 1.
"**Virtual Machine**" means a self-contained operating system that functions as a separate server.
"**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 network infrastructure that is shared with other customers. Unless otherwise agreed in writing, your communications over your VPN are restricted to those Sites belonging to your VPN.
"**WAN**" means Wide Area Network, the infrastructure that enables the transmission of data between Sites.