# BT Managed Firewall Security
# Annex to the Managed Service Schedule

## Contents



© British Telecommunications plc 2023

# BT Managed Firewall Security Annex to the Managed Service Schedule

### A note on 'you'

'You' and 'your' mean the Customer.

### Words defined in the Managed Service Schedule and General Terms

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

## Part A – The BT Managed Firewall Security Service

### 1 Service Summary

1.1 BT will provide you with a service that controls inbound Internet traffic according to controlled exceptions, manages Users' outbound Internet access according to pre-defined policy and scans Internet traffic to block malware comprising:

1.1.1 the Standard Service Components; and

1.1.2 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 (the "**BT Managed Firewall Security Service**").

1.1.3 The BT Managed Firewall Security Service must be purchased under Managed Service and is subject to the Managed Service Schedule to the General Terms.

1.1.4 For the purposes of the Managed Service Schedule the BT Managed Firewall Security Service is an Associated Service.

1.1.5 The BT Managed Firewall Security Service must be taken with the Business Premium Care Level set out in Paragraph 2.5 of the Managed Service Schedule.

### 2 Standard Service Components

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

2.1 **Security Appliances**

2.1.1 You may choose from a range of Security Appliances or BT may recommend a Security Appliance as part of the overall design of the BT Managed Firewall Security Service.

2.1.2 You may request to use Customer Equipment for the BT Managed Firewall Security Service and BT may agree to such a request, subject to an assessment by BT that the Customer Equipment is suitable for use with the BT Managed Firewall Security Service. This assessment will be carried out once you have provided the following information and BT will provide written confirmation that BT is able to support the Customer Equipment:

(a) make and model of the Customer Equipment, and any hardware or software optional components;
(b) location of the Customer Equipment;
(c) serial numbers;
(d) software versions and licence information;
(e) network diagrams;
(f) Customer Equipment name and IP Addressing;
(g) details of any third party contracts, service level agreements and equipment; and
(h) details of your existing CSP(s).

2.1.3 BT will provide, install and commission any BT Equipment for the BT Managed Firewall Security Service, including any hardware and Software, licensing and support agreements for the Security Appliance and will arrange for any on-Site support and remote service management ("**BT Owned Delivery Model**" or "**BT Owned**");

2.1.4 If, following the process set out at Paragraph 2.1.2, BT agrees to your request to use Customer Equipment for the BT Managed Firewall Security Service, you will provide the Customer Equipment to BT's specification. BT will provide the BT Equipment and arrange applicable licensing and support agreements as set out in the table at Paragraph 2.1.5 and will renew those agreements when required. BT will install and commission that BT Equipment and Customer Equipment and will provide on-Site support and remote service management. If there is a fault in the Customer Equipment, BT will raise the necessary support requests on your behalf. You will retain ownership of all Customer Equipment;

2.1.5 The table below sets out the responsibilities of both of us with respect to the BT Owned Delivery Model for the supply and management of Security Appliances, unless otherwise specified in the Order:

| Description | BT Owned |
|---|---|
| **Security Appliance** | BT |
| **Other equipment (including BT Equipment or Customer Equipment), including Out of Band Access and switches** | BT / Customer |
| **Installation** | BT |
| **Commissioning** | BT |
| **Support agreements, software and licensing** | BT |

2.2 **Project Managed Installation**

BT's project manager for the BT Managed Firewall Security Service will coordinate installation and commissioning, in accordance with the BT Owned Delivery Model liaising with you, installers and equipment suppliers as appropriate, depending on whether BT Equipment or Customer Equipment is being used. All project management activity will be administered remotely and the named representative will not visit your Site.

2.3 **Service Performance Reports**

BT will provide near real-time or historic reports for key BT Managed Firewall Security Service performance metrics, and for security-related events. This may be either via a Customer Portal, or a reporting application provided by BT and installed on a server owned by you.

## 3 Service Options

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

3.1.1 **VPNs:**

(a) BT will set up and configure the following types of VPN in accordance with BT's prevailing technical standards:

(i) remote access IP Sec/SSL VPNs, for remote Users to gain secure access to your internal network. BT will implement your rules to authenticate against your authentication server. You are responsible for providing and managing your own end-user VPN software;

(ii) Site to Site IP Sec VPNs between two Security Appliances which are both owned by you and managed by BT; and

(iii) third party (extranet) IP Sec VPNs, for creating a site-to-site VPN between your Security Appliance managed by BT, and a Security Appliance owned or managed by you or a third party. BT will only deliver VPNs to Security Appliances managed by a third party after the Service Start Date.

(b) Where a digital certificate is required for remote VPN set up, either BT will provide, or you will provide to BT, as set out in the Order, an up-to-date digital certificate that will be installed on the Security Appliance.

(c) Where you provide the digital certificate, BT will install it within seven days of receipt from you.

(d) BT will notify you of the date of expiry of the digital certificate three months prior to the date of expiry. You will advise BT, in writing, within one month of the date of BT's notification whether or not you want to renew your digital certificate.

(e) If you want to renew your digital certificate and it is your responsibility as set out in the Order to provide BT with the digital certificate, you will provide the new digital certificate to BT at least seven days prior to the expiry of the original digital certificate.

(f) BT will not be liable for issues caused by expired digital certificates if:

(i) you do not confirm to BT that you want to renew your digital certificate in accordance with Paragraph 3.1.1(d); or

(ii) you do not provide BT with an up-to-date digital certificate in accordance with Paragraph 3.1.1(e).

3.1.2 **De Militarized Zones (DMZs):**

(a) BT will provide additional LAN segment interfaces on the Security Appliance, or on an adjacent network switch, according to your requirements.

(b) This is subject to there being sufficient physical ports available and additional Charges will apply if additional hardware is required to provide the interface.

3.1.3 **Firewall Intrusion Detection and Prevention Service ("IPS"):**

(a) BT will:

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

(ii) implement this Service Option with a default configuration setting, as defined by the supplier of the Software used to deliver the IPS. BT will also maintain a subscription to the necessary signature updates, and arrange for these to be applied following issue by the supplier; and

(iii) not be responsible for evaluating these signatures beforehand.

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

(c) If BT agrees 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 accept responsibility for the increased risk of false positives (blocks to legitimate traffic) or the increased risk of Attacks being missed.

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

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

(a) BT will:

(i) block access to those Internet sites that you ask BT to, in accordance with your CSP. Internet sites are arranged into groups which are regularly updated. You may choose to block or restrict access to any or all groups;

(ii) send an appropriate message to a User attempting to access a blocked or restricted 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;

(iii) implement the necessary alterations via the standard configuration management process in the event of any change in your CSP; and

(iv) if the SSL/TLS Inspection Service Option is selected, be able to scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided your CSP permits such scanning.

(b) This Service Option does not include reporting as standard. Reporting may be available in accordance with Paragraph 3.1.8.

3.1.5 **Firewall Anti-Virus:**

(a) BT will:

(i) check web browser (http) traffic for known malware;

(ii) inspect requests from Users for an executable file from a site on the Internet, against the current antivirus definition file. 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

(iii) keep antivirus definition files up to date by regular downloads direct from the antivirus service.

(b) Provision of this Service Option is subject to a maximum file size and compressed archive limits, depending on the Security Appliance selected.

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

(d) This Service Option does not include reporting as standard. Reporting may be available in accordance with Paragraph 3.1.8.

3.1.6 **Firewall Anti-Bot Service:**

(a) BT will check and block outbound traffic for communication with known "**command and control**" servers used by owners of malicious software.

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

(c) This Service Option does not include reporting as standard. Reporting may be available as an option depending on the Security Appliance being used.

3.1.7 **Threat Emulation Service:**

(a) BT will encrypt suspected malicious files and send them to the vendor's cloud-based infrastructure where they will be decrypted and analysed for malware by reviewing its behaviour in a virtual environment (sandbox).

(b) Depending on the Security Appliance you select, you may be able to choose whether to hold the file whilst it is being analysed (to provide increased security) or to release it and analyse it in the background (for improved User response). Background processing may lead to malicious files being permitted until signature updates are subsequently generated and applied to your Security Appliances.

(c) If a file has been deemed malicious, its characteristics will be added to the vendor's anti-virus signature list.

(d) BT will determine the country in which this inspection and analysis occurs.

(e) If you require the BT Managed Firewall Security Service to protect against malware contained within SMTP (email) attachments, you will arrange for your DNS mail exchange records to be re-directed to the Security Appliance so that email is delivered to that Security Appliance. BT will configure the Security Appliance to deliver email to your email server.

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

(g) Submission and processing of your data via the Threat Emulation Service will be at your sole discretion and at your own risk. Other than BT's obligations in Clause 14 of the General Terms, BT assumes no responsibility or liability for the receipt and processing of such data.

3.1.8 **Security Event Reporting:**

(a) BT will:

(i) provide reporting facilities, either on-line or on a server hosted on your Site, which allows analysis of security-related events; and

(ii) not pro-actively view your reports and events for Security Incidents.

(b) 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.

(c) The period over which data can be analysed is dependent on the capacity of the Security Appliances or the space allocated on the reporting platform.

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

3.1.9 **SSL/TLS Inspection**

(a) 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).

(b) BT will not intercept and decrypt SSL Encrypted Traffic for every category of web content due to a high possibility of issues with associated applications with certain websites. For example, some websites may not permit decryption.

3.1.10 **Identity Awareness / User groups:**

(a) BT will configure the features of the Security Appliance that support the Identity Awareness/User groups Service Option to apply certain rules of the CSP according to the authenticated identity of the User rather than just their IP Address.

(b) This may require client Software to be installed within your network or on end-user devices, or ensuring BT has remote, read-only, access to your active directory authentication server.

(c) You will maintain the authentication database of Users, groups and any access credentials that you require.

3.1.11 **High Availability (dual appliance) solutions:**

(a) BT will configure a pair of Security Appliances on a single Site to give increased resilience against failure.

(b) Each Security Appliance may be connected to a separate Internet circuit to provide further resilience as set out in the Order.

(c) This Service Option will require additional switches to be included as part of the solution which will be provided by BT or you as set out in Paragraph 2.1.5.

(d) Depending on the Security Appliances used and your CSP, BT may configure the Security Appliances as "**Active Active**" (both Security Appliances share the load under normal conditions) or "**Active Passive**" (one Security Appliance handles the load under normal conditions, with failover to a secondary Security Appliance in the event of the primary Security Appliance failing).

(e) For "**Active Active**" configurations, throughput performance may reduce under failure conditions unless each Security Appliance has capacity to handle the full load independently.

3.1.12 **Ad Hoc Professional Service:**

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

(b) Professional Services are delivered remotely unless otherwise set out in the Order.

3.1.13 **CSP production:**

BT will provide Professional Services to assist you in the production and implementation of your CSP for a period of three Business Days. If additional time is required for the creation of the CSP, this will be charged for as set out in Paragraph 9.1.1.

3.1.14 **Vulnerability Notification and Patching:**

(a) BT will identify, test and implement Patches for High and Critical CVSS scores in accordance with your authorisation;

(b) the Vulnerability Notification and Patching Service Option will only be available while the Security Appliance is supported by the vendor.

3.1.15 **Threat Defence Enhanced Firewall Service**

BT will provide you with the Threat Defence Enhanced Firewall Service, subject to the requirements set out below and as set out in the applicable Order.

(a) Existing Blocklist Enhancement

(i) Subject to BT confirming that your Security Appliance is suitable for use with the Threat Defence Enhanced Firewall Service, BT will use its Threat Defence 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 will 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 Threat Defence Enhanced Firewall service is specified, subject to the requirements of technical feasibility (as outlined above at Paragraph 3.1.15(b)(i)), BT will implement Automated IOC Blocking. By specifying the Threat Defence Enhanced Firewall Service, you hereby consent to BT implementing Automated IOC Blocking in respect of your Security Appliance.

(iii) BT will 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.

3.1.16 **Zero Touch Provision**

(a) BT will provide you with an optional physical firewall that can be set up by a self-installation process ("**Zero Touch Provision**"). As part of the Zero Touch Provision Service Option, BT will provide you with an Installation Guide to assist you with the installation of the physical firewall.

(b) Where you chose the Zero Touch Provision and are unable to complete the self-installation, BT may, at an additional Charge, provide support of BT engineer to perform the physical installation on your Site.

(c) Zero Touch Provision may not be available for installation on every model of physical firewall devices.

3.2 The BT Managed Firewall Security Service may not be available in all locations and Service Levels may vary depending on Site location.

3.3 Not all BT Managed Firewall Security Service Options may be available across all suppliers.

3.4 Service Options may not be available on all Security Appliances. BT is not responsible if BT is unable to deliver the BT Managed Firewall Security Service because of a lack of capacity on your selected Security Appliances.

3.5 BT cannot guarantee that the Service Options will operate without Incident or interruption or to intercept or disarm all malware.

## 4 Service Management Boundary

4.1 BT will provide and manage the BT Managed Firewall Security Service as set out in Parts A, B and C of this Annex and as set out in any applicable Order up to:

4.1.1 the Internet/WAN side: the cable connecting the firewall to your Router;

4.1.2 the LAN side: the Ethernet port(s) on the firewall or the switch provided by BT; and/or

4.1.3 the analogue exchange line: the cable connecting BT's provided modem to the Access Line socket,

("**Service Management Boundary**").

4.2 BT will have no responsibility for the BT Managed Firewall Security Service outside the Service Management Boundary, including:

4.2.1 issues on Users' machines, downloadable vendor software not provided by BT, or your servers (including operating system, coding languages and security settings);

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

4.2.3 identity source management.

4.3 BT does not make any representations, whether express or implied, about whether the BT Managed Firewall Security Service will operate in combination with any Customer Equipment or other equipment and software.

## 5 Associated Services and Third Parties

5.1 You will have the following services in place prior to the BT Managed Firewall Security Service being delivered. You will ensure that these services meet the minimum technical requirements that BT may specify:

5.1.1 Internet connectivity;

5.1.2 WAN connectivity;

5.1.3 Access Line, to enable Out of Band Access management;

5.1.4 LAN/DMZ connectivity and associated infrastructure;

5.1.5 Access Line connectivity; and

5.1.6 broader IT environment, including authentication services, server/client platforms, Security Incident and event management (SIEM) solutions,

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

5.2 If BT provides you with any services other than the BT Managed Firewall Security Service (including any Enabling Service) this Annex will not apply to those services and those services will be governed by their separate terms and conditions.

## 6 Specific Terms and Conditions

6.1 **EULA**

6.1.1 BT will only provide the BT Managed Firewall Security Service if you have entered into an end user licence agreement with the supplier of BT Equipment or any Customer Equipment as may be amended or supplemented from time to time by the supplier ("**EULA**").

6.1.2 You will observe and comply with the EULA for all or any use of the applicable Software.

6.1.3 In addition to what it says in Clause 15 of the General Terms, if you do not comply with the EULA, BT may restrict or suspend the BT Managed Firewall Security Service upon reasonable Notice, and:

(a) you will continue to pay the Charges for the BT Managed Firewall Security Service until the end of the Minimum Period of Service; and

(b) BT may charge a re-installation fee to re-start the BT Managed Firewall Security Service.

6.1.4 You will enter into the EULA for your own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the EULA are between you and the supplier and you will deal with the supplier with respect to any loss or damage suffered by either of you as such loss or damage will not be enforceable against BT.

6.1.5 Where the EULA is presented in a 'click to accept' function and you require BT to configure or install Software on your behalf, BT will do so as your agent and bind you to the EULA.

6.2 **Changes to the CSP**

6.2.1 Where you require a change to your CSP, for example as a result of changes to your application requirements or network environment, you may request additions, deletions, or modifications to your CSP and in accordance with Paragraphs 2.14 and 2.15 of the Managed Service Schedule, BT will provide you with the means to request Standard Changes or Urgent Changes to the CSP, either on the relevant Customer Portal or to the Service Desk.

6.2.2 You will order any changes to the BT Managed Firewall Security Service that are required that involve physical changes to the BT Managed Firewall Security Service, including Security Appliance upgrades and LAN re-arrangements. The CSP changes described in Paragraph 6.2.1 refer only to requests to change the rule-sets that define the BT Managed Firewall Security Service's operation.

6.2.3 BT will use reasonable endeavours to identify errors or potential unforeseen consequences of your requested CSP changes and advise you appropriately and will not be liable for any consequence arising from:

(a) your misspecification of your security requirements in the CSP; or
(b) unforeseen consequences of a correctly specified and correctly implemented CSP.

6.2.4 BT will only make configuration changes as set out in Paragraph 6.2.1. For changes that require additional hardware, licences or changes to Charges (including changes to ongoing Recurring Charges); or where the solution needs to be re-defined, BT:

(a) will offer you Professional Services in accordance with Paragraph 3.1.12; or
(b) agree a change to the Contract that will only be effective if in writing and signed by both of us.

6.2.5

(a) Where BT's measurements show that change requests are being raised more frequently than as set out in Paragraphs 2.14.10 and 2.14.11 of the Managed Service Schedule, 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;
(ii) review your requirements and agree with you an appropriate alternative implementation process and any associated charges; or
(iii) charge you for any changes above the permitted number of SSRs set out in Paragraphs 2.14.10 and 2.14.11 of the Managed Service Schedule.

(b) BT reserves the right to charge you for Emergency or Urgent Changes you issued in error.
(c) access to the Customer Portal is controlled and will not be shared by your employees. All User ID tokens/passwords are to be uniquely assigned to named individuals. These individuals will not:

(i) allow anyone else to use their token/ID or share passwords;
(ii) leave their User account logged in while the computer unattended and unlocked;
(iii) submit any unauthorised changes; or
(iv) attempt to access data that they are not authorised to access.

Customer Contacts are required to report the loss of any tokens or compromised passwords within your own organisation as per your standard security processes and to BT immediately.

## 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 Managed Firewall Security Service BT:

7.1.1 will, once the requirements of the BT Managed Firewall Security Service have been confirmed and agreed, provide you with a Customer Committed Date and will use reasonable endeavours to meet any Customer Committed Date;

7.1.2 where applicable, will arrange for any surveys to be conducted to confirm the availability of a suitable environment for provision of the BT Managed Firewall Security Service (including confirming the presence of Enabling Services). Where the surveys identify that additional work is required to be undertaken by you in order to provide a suitable environment, you will complete these works prior to installation of the BT Managed Firewall Security Service. Failure to do so may result in a change to the Customer Committed Date, Charges for an aborted Site visit, or BT may provide a new quote to you, detailing the additional Charges you will need to pay for the additional work to be completed and:

(a) where you accept the new quote, BT will either:

(i) cancel the existing Order to the affected Site(s) and generate a new Order for the affected Site(s), with a new Customer Committed Date; or

(ii) modify the existing Order to reflect the new requirements and provide a new Customer Committed Date; or

(b) where you do not accept the new quote or you do not instruct BT to proceed with the existing Order, BT will cancel your existing Order for the provision of BT Managed Firewall Security Service to the affected Site(s) and BT will have no obligation to provide the BT Managed Firewall Security Service to that Site. You will pay BT for any equipment that BT orders to fulfil BT's obligations where you subsequently cancel or amend such Order and BT is unable to return the equipment to the supplier;

7.1.3 will,

(a) in accordance with the BT Owned Delivery Model, provide, install and commission any BT Equipment, including any hardware and Software, licensing and support agreements for the Security Appliance and will arrange for any on-Site support and remote service management; and

(b) will, if BT accepts your request to use Customer Equipment for the BT Managed Firewall Security Service in accordance with Paragraph 2.1.2, install and commission that Customer Equipment, including hardware and software, licensing and support agreements for the Security Appliance to BT's specification and will provide on-Site support and remote service management;

7.1.4 will provide you with the Site Planning Guide;

7.1.5 will appoint a representative to be your single point of contact for BT's project management Service Option, as set out in Paragraph 2.2; and

7.1.6 will validate that you have ordered the correct number of licenses to serve your requirements, in accordance with vendor commercial terms and according to information provided by you and:

(a) if BT determines that you have not ordered sufficient licences, BT will notify you and you will seek to rectify the situation within 30 days of the date of notification;

(b) if the situation is not resolved within this time BT may suspend the BT Managed Firewall Security Service and subsequently terminate the BT Managed Firewall Security Service in accordance with Clause 18 of the General Terms; and

(c) in any event, BT is not liable for unknown breaches of vendor commercial terms, where BT is acting on information provided by you.

7.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

7.2.1 contact you and agree installation date(s), including access for third party installers;

7.2.2 install the BT Equipment or Customer Equipment (as applicable, where BT has agreed for Customer Equipment to be used in accordance with Paragraph 2.1.2). Once installed, BT will configure the BT Managed Firewall Security Service remotely in accordance with your CSP;

7.2.3 deploy and configure the Service Option(s) selected by you; and

7.2.4 on the date that BT has completed the activities in this Paragraph 7.2, subject to Paragraph 9.5, confirm to you that the BT Managed Firewall Security Service is available for performance of any Acceptance Tests in accordance with Paragraph 8.2.

7.3 **During Operation**

On and from the Service Start Date, BT:

7.3.1 will, for a period of five Business Days after the Service Start Date, implement any simple changes or corrections to the CSP that may be necessary for the operation of the BT Managed Firewall Security Service. BT will implement such changes as soon as reasonably practicable and they will typically involve individual lines of port/protocol, routing or network address translation changes. Any substantial changes to the CSP will incur additional Charges as set out in Paragraph 9.2 and may be scheduled for implementation following this five Business Day period;

7.3.2 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 6.2;

7.3.3 may, in the event of a security breach affecting the BT Managed Firewall Security Service, require you to change any or all of your passwords. BT does not guarantee the security of the BT Managed Firewall Security Service against unauthorised or unlawful access or use;

7.3.4 will in accordance with the BT Owned Delivery Model, or where BT has agreed that Customer Equipment may be used in accordance with Paragraph 2.1.2, manage the ongoing maintenance, monitoring and

configuration of BT Equipment or Customer Equipment, as applicable, for the duration of the BT Managed Firewall Security Service. In addition, unless specifically agreed otherwise, BT may install additional BT Equipment on your Site, for the purpose of monitoring and management of the BT Managed Firewall Security Service;

7.3.5 will be responsible for ensuring any required software licences and support contracts are renewed for the term of this Contract. Unless you give BT Notice of an intention to terminate in accordance with Paragraph 4.3.1 of the Managed Service Schedule, BT will extend the software licences and any required support contracts for a further 12 months;

7.3.6 will notify you if BT anticipates that your hardware or software will become End of Life and will no longer be supported by the BT Managed Firewall Security Service. BT will recommend to you to replace or upgrade the applicable hardware or software at an appropriate time. BT will notify you of any changes to the Charges if the relevant hardware or software is BT Owned and will discuss with you the costs of upgrade if the relevant hardware or Software is Customer Equipment;

7.3.7 will use secure protocols or provide a secure management link to connect to the Security Appliance via the Internet or other agreed network connection, in order to monitor the BT Managed Firewall Security Service proactively and to assist in Incident diagnosis;

7.3.8 will provide an Out of Band Access link that connects directly to the Security Appliance(s), via a modem provided by BT and an Access Line provided by you to allow further remote management and diagnostics capability;

7.3.9 will, if you select the CSP production Service Option as set out in Paragraph 3.1.13, capture the necessary information in consultation with your Customer Contact and produce the CSP;

7.3.10 will continuously monitor your Security Appliances at regular intervals over the Internet or other agreed network connection;

7.3.11 will provide you with a report in a secure manner if Vulnerabilities reported as having a CVSS score of 7.0 or above are identified. In the report, BT will advise your Nominated Representative of potential High and Critical CVSS scores. BT may not assess the configuration of a Security Appliance (a security policy or internal settings) or contextual exposure of any Security Appliances to the Vulnerability;

7.3.12 will, following your request to implement a Patch, agree an installation window with you and confirm to you when the Patch has been installed;

7.3.13 will roll the Patch back upon your request in the event that you detect undesirable side-effects. Any activity by BT required to resolve issues resulting from the implementation of a Patch is not covered by the Vulnerability Notification and Patching Service Option and BT will invoice you for additional reasonable Charges; and

7.3.14 where the Threat Defence 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 Managed Firewall Security Service by either of us, BT:

7.4.1 will terminate any rights of access to the relevant Customer Portal and relevant Software and stop providing all other elements of the BT Managed Firewall Security Service;

7.4.2 will, where requested in writing prior to the termination of this Service, provide, where reasonably practical, configuration information relating to the BT Managed Firewall Security Service provided at the Site(s) 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 Managed Firewall Security Service by BT, you will:

8.1.1 complete any preparation activities that BT may request to enable you to receive the BT Managed Firewall Security Service promptly and in accordance with any reasonable timescales, including, any account names and passwords necessary to install and commission the BT Managed Firewall Security Service on BT Equipment or Customer Equipment;

8.1.2 if you have not selected the CSP production Service Option as set out in Paragraph 3.1.13, submit a CSP that meets the requirements and specifications advised by BT at least 28 Business Days before the Customer Committed Date, including specifications that cover your legacy network, application services and other Enabling Services, using the CSP requirements template. BT will respond with a security

policy document, which will in turn be authorised by you at least 10 Business Days before the Customer Committed Date;

8.1.3 retain responsibility for the CSP;

8.1.4 if an Out of Band Access modem is not included as part of the BT Managed Firewall Security Service, agree an appropriate alternative with BT to allow for fault diagnosis and base configuration, allowing BT to establish in-band control of the Security Appliance, at the time of installation and following a failure of the Security Appliance;

8.1.5 ensure that your Internet access circuit bandwidth is sufficient to meet your requirements and the requirement for in-band management access from BT;

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

8.1.7 register any required Internet domain names using legitimate addresses which are public, registered and routed to your Site;

8.1.8 modify your network routing to ensure appropriate traffic is directed to the Security Appliance. You acknowledge that switches provided as part of the BT Managed Firewall Security Service only provide direct physical connectivity between Security Appliances and are not intended to support any network routing functionality;

8.1.9 ensure that Security Appliances are able to receive updates, such as Vulnerability signatures, directly over the Internet, or over an alternative path agreed with BT for that purpose;

8.1.10 obtain and provide in-life support for any Software running on your Security Appliances;

8.1.11 where necessary, provide and manage physical or virtual servers on your Site to a specification that BT agrees to run any Software that BT provides;

8.1.12 if BT has agreed to provide all or part of the BT Managed Firewall Security Service using Customer Equipment, ensure that the Customer Equipment is working correctly. If it is discovered to be faulty before the Service Start Date:

(a) you will be responsible for resolving any faults;
(b) BT will raise Charges to cover any additional Site visits; and
(c) agreed Customer Committed Date may no longer apply, in such case BT will notify you;

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

8.1.14 be responsible for ensuring compliance with Applicable Law, including obtaining (if required) local import and User licenses and the written authority from all respective authorities, particularly for countries where the use and import of encryption Software and devices may be restricted by Applicable Law, or the export and re-export of the encryption Software or devices may be subject to the United States of America export control law, not act to misuse the BT Managed Firewall Security Service as provided by BT to contravene or circumvent these laws. BT may treat any contravention of these laws as a material breach and:

(a) suspend the BT Managed Firewall Security Service and BT may refuse to restore BT Managed Firewall Security Service until BT receives an acceptable assurance from you that there will be no further contravention; or
(b) terminate the BT Managed Firewall Security Service upon Notice in accordance with Clause 25 of the General Terms;

8.1.15 prepare and maintain the Site(s) for the installation of BT Equipment and Customer Equipment and supply of the BT Managed Firewall Security Service, including:

(a) providing a suitable and safe operational environment for any BT Equipment or Customer Equipment including all necessary trunking, conduits, cable trays, and telecommunications connection points in accordance with BT's reasonable instructions and applicable installation standards;
(b) taking up or removing any fitted or fixed floor coverings, ceiling tiles and partition covers or providing any openings in buildings required to connect BT Equipment or Customer Equipment to appropriate telecommunications facilities in time to allow BT to undertake any necessary installation or maintenance services;
(c) carrying out any work that may be required after installation to make good any cosmetic damage caused during the installation or maintenance;
(d) providing a secure, continuous power supply at the Site(s) for the operation and maintenance of the BT Managed Firewall Security Service and BT Equipment or Customer Equipment at such points and with such connections as BT specifies, and, in order to mitigate any interruption to the BT Managed Firewall Security Service resulting from failure in the principal power supply, providing

back-up power with sufficient capacity to conform to the standby requirements of the applicable British standards; and

(e) complying with the Site Planning Guide.

8.1.16 in relation to BT Equipment:

(a) BT Equipment will remain BT's property at all times and risk in BT Equipment will pass to you upon delivery, whether or not the BT Equipment has been installed;

(b) keep the BT Equipment safe and without risk to health;

(c) only use the BT Equipment, or allow it to be used, in accordance with any instructions or authorisation BT may give and for the purpose for which it is designed;

(d) not move the BT Equipment or any part of it from the Site(s) without BT's prior written consent and you will pay BT's costs and expenses reasonably incurred as a result of such move or relocation;

(e) not make any alterations or attachments to, or otherwise interfere with the BT Equipment, nor permit any person (other than a person authorised by BT) to do so, without BT's prior written consent and if BT gives BT's consent agree that any alterations or attachments are part of the BT Equipment;

(f) not sell, charge, assign, transfer or dispose of or part with possession of the BT Equipment or any part of it;

(g) not allow any lien, encumbrance or security interest over the BT Equipment, nor pledge the credit of BT for the repair of the BT Equipment or otherwise;

(h) not claim to be owner of the BT Equipment and ensure that the owner of the Site(s) will not claim ownership of the BT Equipment, even where the BT Equipment is fixed to the Site(s);

(i) obtain appropriate insurance against any damage to or theft or loss of the BT Equipment;

(j) in addition to any other rights that BT may have, reimburse BT for any losses, costs or liabilities arising from your use or misuse of the BT Equipment or where the BT Equipment is damaged, stolen or lost, except where the loss or damage to BT Equipment is a result of fair wear and tear or caused by BT;

(k) ensure that the BT Equipment appears in BT's name in your accounting books;

(l) where there is a threatened seizure of the BT Equipment, or an Insolvency Event applies to you, immediately provide BT with Notice so that BT may take action to repossess the BT Equipment; and

(m) notify interested third parties that BT owns the BT Equipment;

8.1.17 identify and provide the name and contact details for a primary and secondary Nominated Representative who may both be responsible for liaising with BT regarding the Vulnerability Notification and Patching Service Option; and

8.1.18 advise BT if the Nominated Representative changes and ensure that BT has the current details of the Nominated Representative;

8.1.19 ensure that the Nominated Representative will:

(a) request implementation of Patches for each affected Security Appliance for the Vulnerability Notification and Patching Service Option;

(b) agree a time slot with BT for the implementation of such Patches;

(c) assess the suitability for deployment of the Patches that BT advises are available to address notified Vulnerabilities within your specific environments and for any post-implementation testing; and

(d) request and authorise that the Patch is reversed out in the event that the Patch introduces issues.

8.2 **Acceptance Tests**

8.2.1 You will carry out the Acceptance Tests for the BT Managed Firewall Security Service within five Business Days after receiving Notice from BT in accordance with Paragraph 7.2.4 ("**Acceptance Test Period**").

8.2.2 The BT Managed Firewall Security 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 BT Managed Firewall Security 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. Where the non-conformance is outside the scope of the BT Managed Firewall Security Service, or due to delays or inaccuracies in

information provided by you to BT, including the requirements of the CSP, BT may apply additional Charges to remedy the non-conformances.

8.3 **Service Operation**

On and from the Service Start Date, you:

8.3.1 will ensure that all Software provided is used solely for operation of the BT Managed Firewall Security Service;

8.3.2 will 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 Managed Firewall Security Service;

8.3.3 will distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the BT Managed Firewall Security Service, including the Customer Portal.

8.3.4 will agree to upgrade or replace your hardware or software if it becomes End of Life in accordance with BT's recommendation set out in Paragraph 7.3.6. If you do not replace or upgrade in accordance with BT's recommendation, BT will not be liable for any faults or errors when your hardware or software becomes out of support, and BT will only be able to provide you with a limited BT Managed Firewall Security Service;

8.3.5 will in relation to the BT Owned Delivery Model and in the event of a failure of a Security Appliance, permit BT or BT's agents at BT's discretion to remove and replace faulty components or to remove the faulty Security Appliance in its entirety and exchange it with a functioning replacement. BT will use reasonable endeavours to ensure any data on the recovered appliance or components is rendered unreadable prior to disposal or recycling;

8.3.6 will ensure the appropriate amount of capacity on your selected Security Appliances in order for BT to deliver the BT Managed Firewall Security Service.

8.3.7 will 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; and

8.3.8 agree that:

(a) BT will not be liable for failure to supply or delay in supplying the BT Managed Firewall Security Service if another supplier delays or refuses the supply of an electronic communications service to BT and no alternative service is available at reasonable cost;

(b) BT will provide the BT Managed Firewall Security Service to you on an "as is" and "as available" basis. BT does not guarantee that the BT Managed Firewall Security Service:

(i) will be performed error-free, without Incident or interruption or that BT will correct all errors in the BT Managed Firewall Security Service;

(ii) will operate in combination with your content or applications or with any other software, hardware, systems or data;

(iii) including any products, information or other material you obtain under or in connection with this Contract, will meet your requirements;

(iv) will ensure any particular outcome of Automated IOC Blocking undertaken as part of the Threat Defence 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; and

(v) will detect, intercept or block all malware or malicious threats;

(c) BT will not be liable in the event that Software updates from the supplier used to identify and control your network traffic (including malware signatures, URL categories or application definitions) contain errors or omissions, beyond making appropriate corrections (where reasonably possible) as soon as reasonably practical;

(d) you will own all right, title and interest in and to all of your information and will have sole responsibility for the legality, reliability, integrity, accuracy and quality of any of your information; and

(e) you will be responsible for results obtained from the use of the BT Managed Firewall Security Service, and for conclusions drawn from such use. BT will have no liability for any damage caused

by errors or omissions in any information, instructions or scripts provided to BT by you in connection with the BT Managed Firewall Security Service, or any actions taken by BT at your direction.

## 9 Invoicing

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

9.1.1 the following components, depending on the options selected in the Order:

| Pricing Component | One-time Charge | Recurring Charge | Notes |
|---|---|---|---|
| **Security Appliances** | Charges relating to the supply and installation of Security Appliances provided on an outright sale basis will be invoiced under the separate contract for the purchase of the Security Appliance. | Charges relating to the supply and installation of Security Appliances provided on a rental basis. | Different charges apply according to location and to different Security Appliances, depending on vendor and model. |
| **Security Licenses** | Charges relating to the supply of one-off or perpetual licences. | Charges relating to recurring licenses and supplier support contracts. | Charges vary, usually according to the number of your IP Addresses or Users. |
| **Service Provision** | Charges relating to project management and commissioning of the BT Managed Firewall Security Service. | N/A | Also applies to in-life changes to the BT Managed Firewall Security Service. |
| **Service Management Fee** | Set-up | Monthly Management | Covers provision and ongoing delivery of Service Options, including Out of Band management capability, Incident management and proactive monitoring of the BT Managed Firewall Security Service.<br><br>Covers implementation of CSP change requests in accordance with Paragraph 6.2.1. |
| **Professional Services** | Consultancy | N/A | Initial (optional) capture of CSP. Ad hoc consultancy as requested (charged on a per day basis). |
| **Service De-Installation** | De-Commissioning of the BT Managed Firewall Security Service. | N/A | Covers disconnection and removal of BT Equipment from your Site at end of Contract. |

9.1.2 any Termination Charges incurred are payable in accordance with Paragraph 4.7 of the Managed Service Schedule and Paragraph 10 of this Annex upon termination of the relevant BT Managed Firewall Security Service.

9.2 BT will charge you for changes to the CSP within its Service Management Fee. BT will invoice you for additional Charges where the changes are outside the scope of the Service Management Fee.

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

9.3.1 Charges for investigating Incidents that you report to BT where BT finds no Incident or that the Incident is outside the Service Management Boundary or where the cause of the Incident was found to be as a result of faulty Customer Equipment;

9.3.2 Charges for expediting provision of the BT Managed Firewall Security Service at your request after you have been informed of the Customer Committed Date;

9.3.3 Charges for the refresh or upgrade of appliances or applications if required by you, unless the refresh or upgrade is operationally necessary to enable BT to continue to provide the BT Managed Firewall Security Service. This does not apply to patching of applications or changes to the CSP. Any refresh or 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;

9.3.4 Charges incurred due to inaccuracies in information provided by you to BT, including the requirements of the CSP.

9.4 Subject to Paragraph 4.5.1(a) of the Managed Service Schedule, the invoicing start date for the BT Managed Firewall Security Service is the Service Start Date.

9.5 BT will usually install and configure BT Equipment or Customer Equipment (where relevant) on the same day. If you require BT to delay configuration once the BT Equipment or Customer Equipment has been installed, BT may commence invoicing for the BT Equipment or Customer Equipment from the date of installation. If configuration is delayed for more than 30 days at your request, BT will commence invoicing for the BT Managed Firewall Security Service.

## 10 Charges at the end of the Contract

10.1 In addition to the Charges set out at Paragraph 4.7 of the Managed Service Schedule, if you terminate the BT Managed Firewall Security Service for convenience in accordance with Clause 17 of the General Terms during the Minimum Period of Service you will pay BT:

10.1.1 for any parts of the BT Managed Firewall Security 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, with the exception of the Recurring Charges for the Security Appliances provided on a rental basis which will be 100 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service.

## 11 IP Addresses and Domain Names

11.1 Except for IP Addresses expressly registered in your name, all IP Addresses and Domain Names made available with the BT Managed Firewall Security Service will at all times remain BT's property or the property of BT's suppliers and are non-transferable.

11.2 All of your rights to use such IP Addresses or Domain Names will cease on termination or expiration of the BT Managed Firewall Security Service.

11.3 BT cannot ensure that any requested Domain Name is available from or approved for use by the applicable Regional Internet Registry and BT has no liability for any failure in the Domain Name registration, transfer or renewal process.

11.4 You will not use IP Addresses that you do not own or that are incorrectly specified and you will be responsible for the use of IP Addresses within your network. BT may apply additional Charges for dealing with changes or Incidents that occur as a result of incorrect / illegal IP Addressing schemes.

11.5 You warrant that you are the owner of, or are authorised by the owner of, the trade mark or name that you wish to use as a Domain Name, and that such Domain Name will not infringe the rights of any person in a corresponding trade mark or name.

11.6 You will pay all fees associated with registration and maintenance of your Domain Name, and will reimburse BT for any and all fees that BT pays to any applicable Regional Internet Registry, and thereafter pay such fees directly to the applicable Regional Internet Registry.

## 12 WEEE Directive

12.1 You will comply with Article 13 of the Waste Electrical and Electronic Equipment Directive 2012 ("**WEEE Directive**") for the costs of collection, treatment, recovery, recycling and environmentally sound disposal of any equipment supplied under the Contract that has become waste electrical and electronic equipment ("**WEEE**").

12.2 For the purposes of Article 13 of the WEEE Directive this Paragraph 12 is an alternative agreement to finance the collection, treatment, recovery, recycling and environmentally sound disposal of WEEE.

12.3 You will comply with any information recording or reporting obligations imposed by the WEEE Directive.

## Part C – Service Levels

### 13 On Time Delivery

13.1 **On Time Delivery Service Level**

13.1.1 BT will deliver the BT Managed Firewall Security Service on or before the Customer Committed Date (the "**On Time Delivery Service Level**").

13.2 **Exceptions**

13.2.1 If you request a change to the BT Managed Firewall Security Service or any part of the BT Managed Firewall Security Service, including any BT Equipment or Customer Equipment or any IP Address location, or delay the completion of your obligations as set out in Paragraph 8, then BT may change the Customer Committed Date to accommodate that change or delay.

13.2.2 The On-Time Delivery Service Level does not apply to upgrades or changes to the BT Managed Firewall Security 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.

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

### 14 Service Availability

14.1 **Availability Service Level**

14.1.1 From the Service Start Date, BT will provide the BT Managed Firewall Security Service with a target availability corresponding to the agreed SLA Category for the BT Managed Firewall Security Service as set out in the table in Paragraph 14.2.2 below (the "**Availability Service Level**").

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

(a) the Standard Availability Service Credit Rate, as set out in Paragraph 14.3.5; or
(b) as applicable, the Elevated Availability Service Credit Rate, as set out in Paragraph 14.3.6.

14.2 **SLA Categories**

14.2.1 The SLA Categories depend on a number of factors, including:

(a) any applications you deploy and any CSP you implement;
(b) the broader network and server environment including any resilient elements; and
(c) the physical location of the Security Appliances and availability of on-Site field support.

14.2.2 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 |

14.3 **Availability Service Credits**

14.3.1 If a Qualifying Incident occurs, BT will measure and record the Availability Downtime for the Site 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 7.1.3 of the Managed Service Schedule.

14.3.2 BT will measure the Availability Downtime in units of full minutes during the Local Contracted Business Hours for Access Line Incidents, and during the Contracted Maintenance Hours for BT Equipment Incidents. Where the BT Managed Firewall Service is connected to a third party network, the Availability Service Level will not apply.

14.3.3 Following the measurement taken in accordance with Paragraph 14.3.1 and Paragraph 14.3.2, BT will calculate the cumulative Availability Downtime for the calendar month(s) in which the Qualifying Incident occurred (the "**Cumulative Monthly Availability Downtime**") and for the previous 12 consecutive calendar months (the "**Cumulative Annual Availability Downtime**").

14.3.4 In the event a Site 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 Site or Circuit using the Availability Downtime data recorded to date.

14.3.5 If the Cumulative Monthly Availability Downtime of the Site 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.

14.3.6 If the Cumulative Annual Availability Downtime of the Site or Circuit 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 by BT Managed Firewall Security Service is less than the Maximum Annual Availability Downtime.

14.3.7 Availability Service Credits are available up to a maximum amount equal to 100 per cent of the monthly Recurring Charges.

## 15 Resiliency Restoration

15.1 **Resiliency Restoration Service Level**

Where you have purchased a Resilient Service (as set out in the applicable Order) and experience loss of BT Managed Firewall Security Service on any Resilient Component (which does not amount to a Severity Level 1 Incident), BT aims to restore the BT Managed Firewall Security Service to the affected Resilient Components within one Business Day of you reporting the Incident, or BT detecting the Incident, ("**Resiliency Restoration Service Level**"). The Resiliency Restoration Service Level will not apply where there is a Qualifying Incident (in which case, the Availability Service Level will apply, in accordance with Paragraph 14.

15.2 **Resiliency Restoration Service Credits**

15.2.1 If the affected Resilient Components are not restored within one Business Day, you may request a Resilience Restoration Service Credit for each commenced hour in excess of the Resiliency Restoration Service Level.

15.2.2 This Service Credit only applies where the Resilient Component is covered by an on-Site maintenance agreement of next Business Day or shorter.

## 16 Requests for Service Credits

16.1 You may request applicable Service Credits within 28 days of the end of the calendar month in which an Incident occurred by providing details of the reason for the claim. Any failure by you to submit a request in accordance with this Paragraph 16.1 will constitute a waiver of any claim for Service Credits for that calendar month.

16.2 Upon receipt of a valid request for Service Credits in accordance with Paragraph 16.1;

16.2.1 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

16.2.2 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.

16.3 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 BT Managed Firewall Security Service (before any discount has been applied).

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

16.5 The Service Levels under this Annex will not apply:

16.5.1 in the event that Clause 8 of the General Terms applies;

16.5.2 during any trial period of the BT Managed Firewall Security Service;

16.5.3 to failures due to any Force Majeure Event;

16.5.4 if you cause a delay or do not provide any requested information in accordance with any reasonable timescales BT tells you about;

16.5.5 if your hardware or software becomes End of Life and BT has notified you of this in accordance with Paragraph 7.3.6 and you choose not to replace or upgrade the applicable hardware or software; or

16.5.6 to any Incident not reported in accordance with Paragraph 7 of the Managed Service Schedule.

## 17 CSP Change Request Delivery Time Targets

17.1.1 Targets apply to Urgent Changes and Standard Changes.

17.1.2 If you submit a change with more than five lines of changes, the target times below will not apply.

17.1.3 The completion time for the change will be notified to you by BT.

17.1.4 The response time for the changes is listed below:

| Request | Target implementation from submission on Customer Portal |
|---|---|
| **Urgent Change and Emergency Change** | 4 Hours |
| **Standard Change** | 8 Hours |

17.1.5 Service Credits do not apply to CSP change requests and to the Vulnerability Notification and Patching Service Option.

## Part D – Defined Terms

### 18 Defined Terms

In addition to the defined terms in the General Terms, capitalised terms in this Annex will have the following 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 Annex):

"**Acceptance Test Period**" has the meaning given in Paragraph 8.2.1.
"**Acceptance Tests**" means those objective tests conducted by you, which, when passed confirm that you accept the BT Managed Firewall Security Service and that the BT Managed Firewall Security Service is ready for use save for any minor non-conformities, which will be resolved as an Incident as set out in Paragraph 7 of the Managed Service Schedule.
"**Access Line**" means a Circuit connecting the Site(s) to the BT Network.
"**Active Active**" has the meaning give in Paragraph 3.1.11(d).
"**Active Passive**" has the meaning given in Paragraph 3.1.11(d).
"**Attack**" means an attempted security incident with malicious intent.
"**Automated IOC Blocking**" has the meaning given in Paragraph 3.1.15(b)(i)
"**Availability**" means the period of time when the BT Managed Firewall Security Service is functioning.
"**Availability Downtime**" means the period of time during which a Qualifying Incident exists as measured by BT in accordance with Paragraph 14.3.1.
"**Availability Service Credit**" means the Service Credit 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 14.1.1.
"**BT Blocklist**" means any IOCs which BT has identified using its Threat Defence Platform.
"**BT Managed Firewall Security Service**" has the meaning given in Paragraph 1.1.
"**BT Owned**" or "**BT Owned Delivery Model**" has the meaning given to in Paragraph 2.1.3.
"**Circuit**" means any line, conductor, or other conduit between two terminals by which information is transmitted.
"**Contracted Maintenance Hours**" means the times during which BT will provide Maintenance for BT Equipment, which will be Business Hours unless specified otherwise in the Order.
"**Critical CVSS score**" means a CVSS score range from 9.0 to 10.0.
"**Cumulative Annual Availability Downtime**" has the meaning given in Paragraph 14.3.3.
"**Cumulative Monthly Availability Downtime**" has the meaning given in Paragraph 14.3.3.
"**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 Managed Firewall Security Service.
"**CSP**" means your customer security policy containing the security rules, set and owned by you, that are applied to the BT Equipment or Customer Equipment and determine the operation of the BT Managed Firewall Security Service.
"**CVSS**" means Common Vulnerability Scoring System v3.0.
"**DMZ**" means de-militarised zone.
"**DNS**" means the domain name system which is the hierarchical and decentralized naming system used to identify computers, services, and other resources reachable through the Internet or other Internet Protocol networks.
"**Domain Name**" means a readable name on an Internet page that is linked to a numeric IP Address.
"**Threat Defence Enhanced Firewall Service**" means the Service Option specified at Paragraph 3.1.15.
"**Threat Defence Platform**" means the solution through which BT will identify IOCs.
"**Elevated Availability Service Credit Rate**" means the applicable rate as set out in the table at Paragraph 14.2.2 for the relevant SLA Category.
"**Emergency Change**" means a change that requires immediate attention from SOC to address a live, service impacting issue that you are experiencing. Emergency Change should be used only as a last resort.
"**Enabling Service**" has the meaning given in Paragraph 5.1.
"**End of Life**" means any hardware or software that is no longer supported by the manufacturer, vendor or supplier and is incapable of cost-effective upgrade or update to a supported version. BT can only provide limited support if your hardware or software reaches this stage.
"**Existing Blocklist Enhancement**" has the meaning given in Paragraph 3.1.15(a)(ii).
"**Ethernet**" means a family of computer networking technologies for LANs.
"**EULA**" has the meaning given in Paragraph 6.1.
"**Firewall Intrusion Detection and Prevention Service**" means the Service Option as set out in Paragraph 3.1.3.
"**High CVSS score**" means a CVSS score range from 7.0 to 8.9.
"**Installation Guide**" means a PDF instructional document which provides steps for the Customer to provision the device.
"**IOCs**" or "**Indicators of Compromise**" has the meaning given in Paragraph 3.1.15(a)(i).

"**IPSec**" means IP security; it is a standards-based framework that provides layer 3 services for confidentiality, privacy, data integrity, authentication and replay prevention.
"**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.
"**Local Contracted Business Hours**" means the times during which Maintenance of any Access Line is provided, which will be Business Hours unless specified otherwise in the Order.
"**Managed Service Schedule**" means the Schedule to the General Terms that this Annex is appended to which details the management services that can apply to the BT Managed Firewall Security Service and that can be found at www.bt.com/terms.
"**Maximum Annual Availability Downtime**" has the meaning given in the table at Paragraph 14.2.2 for the relevant SLA Category.
"**Maximum Monthly Availability Downtime**" has the meaning given in the table at Paragraph 14.2.2 for the relevant SLA Category.
"**Nominated Representative**" means a person from your organisation nominated to be the point of contact for Vulnerability notifications.
"**On Time Delivery Service Credits**" means four per cent of the Recurring Charges for the applicable Site, per day.
"**On Time Delivery Service Level**" has the meaning given in Paragraph 13.1.
"**Out of Band Access**" means access used for initial configuration and for in-life management where the primary means of access to the Security Appliance has failed or to help resolve failure of the Security Appliance.
"**Patch**" means vendor provided Software intended to address a specific Vulnerability.
"**Qualifying Incident**" means a Severity 1 Level Incident, except where any of the following events have occurred:

(a) the BT Managed Firewall Security 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;
(d) an Incident has been reported and BT cannot confirm that an Incident exists after performing tests;
(e) you requested BT to test the BT Managed Firewall Security 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.

"**Regional Internet Registry**" means an organization that manages the allocation and registration of Internet number resources within a particular region of the world. Internet number resources include IP Addresses and autonomous system (AS) numbers.
"**Resiliency Restoration Service Credit**" means one per cent of the total monthly Recurring Charges for the Resilient Service up to a maximum amount equal to 100 per cent of the monthly Recurring Charges.
"**Resiliency Restoration Service Level**" has the meaning given in Paragraph 15.1.
"**Resilient Component**" means, with respect to a Resilient Service, any of the Access Lines, BT Equipment or Customer Equipment.
"**Resilient Service**" means a BT Managed Firewall Security Service or part of a BT Managed Firewall Security Service, as set out in the Order that is designed to have high availability and without single points of failure, such that if one component fails the BT Managed Firewall Security Service is still available.
"**Router**" means a device that forwards data packets between computer networks, creating an overlay internetwork.
"**Security Appliance**" means the BT Equipment used to apply the CSP.
"**Security Incident**" means an Attack which permeates your IT environment, infecting it with threatening material including malware.
"**Service Credit**" means each of the Availability Service Credit, the On Time Service Delivery Service Credit and the Resiliency Restoration Service Credit.
"**Service Credit Interval**" means as set out in the table at Paragraph 14.2.2 for the relevant SLA Category.
"**Service Management Boundary**" has the meaning given in Paragraph 4.1.
"**Service Management Fee**" means the fee that will cover inlife management and simple changes submitted via BT's change management system subject to Paragraph 6.2.1.
"**Service Options**" has the meaning given in Paragraph 3.1.
"**Severity Level 1 Incident**" means an Incident that cannot be circumvented and that constitutes a complete loss of service at the Site or Circuit and in respect of a Resilient Service, excluding any loss of service of a Resilient Component where you still have access to the BT Managed Firewall Security Service through the other back-up Resilient Component.

"**Site Planning Guide**" means a guide provided by BT to you detailing the hardware specification, including environmental, physical and electrical details of any BT Equipment provided to you with the BT Managed Firewall Security Service.

"**SLA Category**" means the category, as set out in the Order which, in accordance with the table set out at Paragraph 14.2.2, specifies the following in relation to the BT Managed Firewall Security Service, Site or Circuit:

(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.

"**SOC**" means Security Operations Centre.

"**SSL**" means secure sockets layer.

"**SSL Encrypted Traffic**" 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**" means the Service Option as set out in Paragraph 3.1.9.

"**Standard Availability Service Credit Rate**" means the applicable rate as set out in the table at Paragraph 14.2.2 for the relevant SLA Category.

"**Standard Change**" means upgrades and modifications resulting from planned developments and security improvements.

"**Standard Service Components**" has the meaning given in Paragraph 2.

"**Threat Emulation Service**" means the Service Option as set out in Paragraph 3.1.7.

"**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, but which are not critical to maintaining the security of the organisation.

"**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.

"**Vulnerability**" means a Software susceptibility that may be exploitable by an attacker.

"**WEEE**" has the meaning given in Paragraph 12.1.

"**WEEE Directive**" has the meaning given in Paragraph 12.1.

"**Zero Touch Provision**" has the meaning given in Paragraph 3.1.16.