BT Managed Next Generation Firewall
Appendix to the Managed Cisco SD-WAN Annex

Contents

A note on 'you' 2
Part A – BT Managed Next Generation Firewall Service 2
1 BT Managed Next Generation Firewall Service Summary 2
2 Standard BT Managed Next Generation Firewall Service Components 2
3 BT Managed Next Generation Firewall Service Options 3
4 BT Managed Next Generation Firewall Service Management Boundary 6
5 Associated Services and Third Parties 6
6 Specific Terms and Conditions 6
Part B – BT Managed Next Generation Firewall Service Delivery and Management 8
7 BT's Obligations 8
8 Your Obligations 10
9 Incidents 12
10 Invoicing 13
11 Charges at the end of the Contract 13
12 CSP Change Request Delivery Time Targets 14
Part D – Defined Terms 15
13 Defined Terms 15

BT Managed Next Generation Firewall Service Appendix

A note on 'you'

'You' and 'your' mean the Customer.

Phrases that refer to 'either', 'neither', 'each of us', 'both of us', 'we each' or 'we both' mean one or both of BT and the Customer, whichever makes sense in the context of the sentence.

Part A – BT Managed Next Generation Firewall Service

1 BT Managed Next Generation Firewall 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 Next Generation Firewall Service**").

1.2 BT Managed Next Generation Firewall Service will be provided as additional service to BT Managed Cisco SD-WAN Service to secure the Internet.

1.3 BT Managed Next Generation Firewall Service will only be available with Managed Service Package 2.

1.4 The terms set out in this Appendix are in addition to:

1.4.1 The General Terms;

1.4.2 The Managed Service Schedule; and

1.4.3 The BT Managed Cisco SD-WAN Annex,

which shall apply to the provision of the BT Managed Next Generation Firewall Service.

1.5 Paragraphs 4.7.3, 6.3, 6.4 and 6.5 of the Managed Service Schedule will not apply to BT Managed Next Generation Firewall Service.

2 Standard BT Managed Next Generation Firewall Service Components

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

2.1 In addition to the Proactive Monitoring capability set out in Paragraph 2.1 of the Managed Service Schedule BT will monitor the performance of the Associated Services against parameters that BT deems appropriate depending on the nature of the relevant Associated Service. BT will check the following Associated Services are operating correctly:

2.1.1 Appliance reachability: Polling the Security Appliance to check it is powered on and has network connectivity. If the Security Appliance is not powered on or does not have network connectivity, BT will investigate and either take appropriate action or recommend action that is required to be taken;

2.1.2 Security Appliance status: BT will test at regular intervals, at BT's discretion, as follows:

(a) resource status, such as CPU and RAM;

(b) physical status, such as temperature, where applicable to the Security Appliance;

(c) compare test results against standard vendor thresholds. BT will investigate and either take appropriate action or recommend action that is required to be taken.

2.1.3 Associated Services access monitoring: generate alerts in near real time for unauthorised access attempts;

2.1.4 Application update status: on UTM/URLF and other applications selected as part of the Associated Services;

2.1.5 monitoring applications under the relevant Associated Services against parameters set by BT;

2.1.6 Associated Service usage and capacity management reporting.

2.2 **Change Management – Simple Service Requests**

BT will only allocate you five SSRs per annum per device.

2.3 **Commercial Changes**

Commercial changes are available for adding or removing Sites, adding new firewalls or changing other commercial terms within the Contract. Commercial changes are requested via your BT Account Manager.

2.4 **Initial Setup**

BT will facilitate the setup and delivery of the BT Managed Next Generation Firewall Service.

2.5 **Security Optimisation Manager**

2.5.1 A desk-based Security Optimisation Manager will join your Service Management service review calls on a quarterly basis. As part of this review they will carry out:

(a) a review focussing on the performance of the BT Managed Next Generation Firewall Service; and

(b) a review of your CSP(s) focussing on the effectiveness of the rules applied to the CSP(s) and the need to fine tune or amend the rules of your CSP(s).

2.5.2 If BT has agreed to participate in a conference call, you will ensure that any report the Security Optimisation Manager provides you with will be reviewed by your suitably qualified personnel who are participating in the conference call prior to the conference call taking place.

2.5.3 You will be responsible for taking appropriate action to address issues as recommended by the Security Optimisation Manager including implementing security improvements as agreed with the Security Optimisation Manager or as advised by the Security Optimisation Manager.

2.5.4 In addition to your responsibilities set out in Paragraph 2.5.3, you will be responsible for initiating the appropriate change requests in accordance with the SSR process set out in the Managed Services Schedule to address any issues in respect of fine tuning or amending your CSP(s) as recommended by the Security Optimisation Manager.

2.6 **Security Appliances**

2.6.1 BT will provide you with the following Security Appliance delivery model:

BT will provide, install, commission and keep up to date 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 ("**BT Owned**").

2.6.2 The table below sets out the responsibilities of both of us 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), including Out of Band Access and switches	BT
Installation	BT
Commissioning	BT
Support agreements, software and licensing	BT

2.7 **Project Managed Installation**

BT's project manager will coordinate the BT Managed Next Generation Firewall Service 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.

2.8 **Service Performance Reports**

BT will provide near real-time or historic reports for key BT Managed Next Generation Firewall Service performance metrics, and for security-related events.

2.9 The following capabilities from the Managed Service Package 2 set out in the Managed Service Schedule to the General Terms will not apply to BT Managed Next Generation Firewall Service:

2.9.1 Maintenance Care Levels;

2.9.2 Configuration Management;

2.9.3 Service Reporting, Network Reporting, IPSLA Reporting and Vendor Network and Application Reporting, as part of the Performance Reporting Capability; and

2.9.4 PDS Project Coordination, PDS Hybrid Project Management, PDS Face to Face Project Management, On Site WLAN Survey, Remote WLAN Survey, Network Assessment Physical Detail Collection Package and Network Assessment Physical Detail Collection Day Rate, Infrastructure Cabling, as part of the Packaged Deployment Services Capability.

3 BT Managed Next Generation Firewall 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 **IPSec VPN:**

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

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

(ii) remote access 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; and

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

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:**

(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, including a standard signature list. BT will also maintain a subscription to the necessary signature updates, and arrange for these to be applied following issue by the supplier;

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

(iv) where "**bronze level services**" are selected in the Order, block high impact or high confidence attacks, as defined by the supplier of the Software used to deliver the Firewall Intrusion Detection and Prevention Service. Bronze level services do not include monitoring, alerting or service specific reporting and it will not be possible to make changes to this standard signature list. However, BT will disable the appropriate signature (or signature group if necessary) if you advise BT of a conflict with any of your legitimate business traffic; and

(v) where "**platinum level services**" are selected in the Order, apply additional signatures in "**detect**" mode. BT will provide 24x7x365 monitoring alerts relating to suspected intrusion incidents and categorise the alarm according to its severity. In the event that a high priority threat is discovered, BT will use reasonable endeavours to notify you as soon as practical and ask you if you wish to block the traffic causing the alert. BT will not proactively initiate this block in the absence of your instructions. BT will provide incident reports as part of this Service Option via the relevant Customer Portal.

(b) 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.

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; and

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

(b) This Service Option does not include reporting as standard. Reporting may be available in accordance with Paragraph 3.1.9.

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) This Service Option does not include reporting as standard. Reporting may be available in accordance with Paragraph 3.1.9.

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) 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 **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 e.g. some websites may not permit decryption.

3.1.8 **UTM Licence Renewals:**

BT will identify, test and implement signature updates for Unified Threat Management (UTM) functions on Associated Services that are explicitly managed by BT. Signature updates are classified as vendor specific updates that address the known countermeasure to threats.

3.1.9 **Security Event Reporting:**

(a) BT will:

(i) provide reporting facilities, which allows analysis of security-related events; and
(ii) not pro-actively view your reports and events for security incidents.

(b) 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.

3.1.10 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.

(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.

3.1.11 **Ad Hoc Professional Service:**

(a) BT may provide, at an additional Charge, Professional Services with each Order, to support your initial configuration of the BT Managed Next Generation Firewall Service and the ongoing operation of the BT Managed Next Generation Firewall Service.

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

3.1.12 **CSP production:**

If you require assistance in the production and implementation of your CSP(s), BT may provide you with Professional Services as a optional, chargeable service.

3.1.13 **Vulnerability Notification and Patching:**

(a) BT will identify, and dependent on Service Level, will apply a single secure coordinated process for implementing patches to reduce risk of known vulnerabilities on your Security Appliances. BT will rank all patch updates in accordance with the CVSS score.

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

3.2 The BT Managed Next Generation Firewall Service may not be available in all locations.

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

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

4 BT Managed Next Generation Firewall Service Management Boundary

4.1 BT will provide and manage the BT Managed Next Generation Firewall Service as set out in Parts A, B and C of this Appendix and as set out in the 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

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

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

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

4.2.1 issues on 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); or

4.2.3 identity source management.

4.3 BT does not make any representations, whether express or implied, about whether the BT Managed Next Generation Firewall 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 Next Generation Firewall 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 PSTN direct exchange line to enable Out of Band Access management;

5.1.4 LAN/DMZ connectivity and associated infrastructure;

5.1.5 PSTN connectivity; and

5.1.6 broader IT environment, including the Security Appliances where they are your responsibility as set out in Paragraph 2.6.2, including authentication services, additional switches where required as set out in Paragraph 3.1.10(c), 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 Next Generation Firewall Service (including any Enabling Service) this Schedule will not apply to those services and those services will be governed by their separate terms and conditions.

6 Specific Terms and Conditions

6.1 **EULA**

6.1.1 BT will only provide the BT Managed Next Generation Firewall Service if you have entered into an end user licence agreement with the supplier of BT Equipment or 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 Next Generation Firewall Service upon reasonable Notice, and:

(a) you will continue to pay the Charges for the BT Managed Next Generation Firewall 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 Next Generation Firewall 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 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 separately any changes to the BT Managed Next Generation Firewall Service that are required that involve physical changes to the BT Managed Next Generation Firewall 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 Next Generation Firewall 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 charge you for changes to the CSP within its Annual Service Management Fee. BT will invoice you for additional Charges where the changes are outside the scope of the Annual Service Management Fee.

6.2.5 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). Where the solution needs to be re-defined, BT:

(a) will offer you Professional Services in accordance with Paragraph 3.1.11; or

(b) agree a change to the Contract that will only be effective if in writing and signed by both of us.

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

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

(i) two per month per small Security Appliance;

(ii) four per month per medium Security Appliance; or

(iii) eight per month per large Security Appliance.

(b) Where BT's measurements show that change requests are being raised more frequently than the "**reasonable use**" restrictions set out in Paragraph 6.2.6(a), 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 "**reasonable use**" restrictions set out in Paragraph 6.2.6(a).

(c) BT reserves the right to charge you for Emergency or Urgent Changes you issued in error or in excess of the "**reasonable use**" restrictions.

Part B – BT Managed Next Generation Firewall 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 Next Generation Firewall Service BT:

7.1.1 will, once the requirements of the BT Managed Next Generation Firewall Service have been confirmed and agreed, and, where applicable, provide you with a date on which delivery of the BT Managed Next Generation Firewall Service is due to start ("**Customer Committed Date**") and will use reasonable endeavours to meet any Customer Committed Date;

7.1.2 where applicable, arrange for any surveys to be conducted to confirm the availability of a suitable environment for provision of the BT Managed Next Generation Firewall 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 Next Generation Firewall 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;

(iii) 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 Next Generation Firewall Service to the affected Site(s) and BT will have no obligation to provide the BT Managed Next Generation Firewall 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 configure the BT Managed Next Generation Firewall Service and policies;

7.1.4 will co-ordinate the delivery and installation of the BT Managed Next Generation Firewall Service;

7.1.5 will 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;

7.1.6 will co-ordinate delivery of the physical Security Appliances and keep you informed throughout the journey;

7.1.7 will provide you with the Site Planning Guide;

7.1.8 will appoint a named representative to be your single point of contact for BT's project management Service Option, as set out in Paragraph 2.7; and

7.1.9 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 Next Generation Firewall Service and subsequently terminate the BT Managed Next Generation Firewall 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. Once installed, BT will configure the BT Managed Next Generation Firewall Service remotely in accordance with your CSP;

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

7.2.4 on the date that BT has completed the activities in this Paragraph 7.2, subject to Paragraph 10.3, confirm to you that the BT Managed Next Generation Firewall 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 30 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 Next Generation Firewall 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 6.2.4 and may be scheduled for implementation following this 30 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 Next Generation Firewall Service, require you to change any or all of your passwords. BT does not guarantee the security of the BT Managed Next Generation Firewall Service against unauthorised or unlawful access or use;

7.3.4 will manage the ongoing maintenance, monitoring and configuration of BT Equipment or Customer Equipment for the duration of the BT Managed Next Generation Firewall 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 Next Generation Firewall Service;

7.3.5 will be responsible for ensuring software licences and any required support contracts are renewed for the term of this Contract. Unless you give BT Notice of an intention to terminate in accordance with Paragraph 4.2.2. of the Managed Service Schedule to the General Terms, BT will extend the software licences and any required support contracts for a further 12 months;

7.3.6 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 Next Generation Firewall Service proactively and to assist in Incident diagnosis;

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

7.3.8 will, if you select the CSP production Service Option as set out in Paragraph 3.1.12, capture the necessary information in consultation with your Customer Contact and produce the CSP;

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

7.3.10 will for any of the BT Owned, Customer Owned and BT Takeover delivery models provide 24x7x365 on-Site maintenance response where this is available locally. Where this level of cover is not available, on-Site support will be provided between 0800 to 1700 Monday to Friday in the relevant country;

7.3.11 will send you a report securely via email 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 will 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 use reasonable efforts to obtain a Patch for the Vulnerability from the Security Appliance vendor and will then test the Patch for installation and BT`s ability to roll-back the Software to the level prior to installing the Patch. Once testing is complete, BT will advise you that the Patch is available for installation and provide additional information, where available, to support you in deciding whether to install the Patch or not;

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

7.3.14 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.

7.4 **The End of the Service**

On termination of the BT Managed Next Generation Firewall 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 Next Generation Firewall Service;

7.4.2 will, where requested in writing prior to the termination of this Contract, provide, where reasonably practical, configuration information relating to the BT Managed Next Generation Firewall 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 Next Generation Firewall Service by BT, you will:

8.1.1 if you have not paid for the CSP production Service Option as set out in Paragraph 3.1.12, 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;

8.1.2 retain responsibility for the CSP;

8.1.3 if an Out of Band Access modem is not included as part of the BT Managed Next Generation Firewall 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;

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

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

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

8.1.7 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 Next Generation Firewall Service only provide direct physical connectivity between Security Appliances and are not intended to support any network routing functionality;

8.1.8 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;

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

8.1.10 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;

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

8.1.12 prepare and maintain the Site(s) for the installation of BT Equipment and supply of the BT Managed Next Generation Firewall Service, including:

(a) complying with the Site Planning Guide.

8.1.13 in relation to BT Equipment:

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

(b) 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;

(c) 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;

(d) 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;

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

(f) 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;

(g) 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);
(h) obtain appropriate insurance against any damage to or theft or loss of the BT Equipment;
(i) 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.;
(j) ensure that the BT Equipment appears in BT's name in your accounting books;
(k) 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
(l) notify interested third parties that BT owns the BT Equipment;

8.1.14 identify and provide the name and contact details for a Nominated Representative responsible for liaising with BT regarding the Vulnerability Notification and Patching Service Option; and

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

8.1.16 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 Next Generation Firewall 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 Next Generation Firewall Service is accepted by you if you confirm acceptance in writing during the Acceptance Test Period or is treated as being accepted by you if you do not provide BT with Notice to the contrary by the end of the Acceptance Test Period.

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

(a) the date that you confirm or BT deems acceptance of the BT Managed Next Generation Firewall 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 Next Generation Firewall 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 Users report Incidents to the Service Desk and not to the BT's project manager;

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

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

(a)
(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 Next Generation Firewall Service;

8.3.4 will distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the BT Managed Next Generation Firewall Service, including the Customer Portal;

8.3.5 will maintain a list of current Users and immediately terminate access for any person who ceases to be an authorised User;

8.3.6 will ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the BT Managed Next Generation Firewall Service and:

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

(b) take all reasonable steps to prevent unauthorised access to the BT Managed Next Generation Firewall Service; and

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

8.3.7 will, if BT requests you to do so and in order to ensure the security or integrity of the BT Managed Next Generation Firewall Service, change any or all passwords or other systems administration information used in connection with the BT Managed Next Generation Firewall Service;

8.3.8 will 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;

8.3.9 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;

8.3.10 agree that:

(a) BT will not be liable for failure to supply or delay in supplying the BT Managed Next Generation Firewall 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 Next Generation Firewall Service to you on an "**as is**" and "**as available**" basis. BT does not guarantee that the BT Managed Next Generation Firewall Service:

(i) will be performed error-free or uninterrupted or that BT will correct all errors in the BT Managed Next Generation Firewall 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; and

(iv) will detect or block all 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 Next Generation Firewall 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 Next Generation Firewall Service, or any actions taken by BT at your direction.

9 Incidents

9.1 Where you become aware of an Incident:

9.1.1 BT will give you a Ticket and assess the Incident in accordance with the criteria set out in the table below:

Priority	Description
P1	Serious impact and Incident cannot be circumvented, typically where the Associated Service is completely down / unavailable; for example: your Site is isolated or there is a complete loss of service to a Site or critical business functions are prevented from operating.
P2	Large impact on a portion of the Associated Service and cannot be circumvented, causes significant loss of the Associated Service, but the impacted business function is not halted; for example: there is a complete loss of primary link and the BT backup link (if provided) is invoked or business functions are disrupted but not prevented from operating.

Priority	Description
P3	Small impact on the Associated Service or where a single User or component is affected, and it causes some impact to your business; for example: there is an intermittent or occasional disturbance which does not have a major impact on the Associated Service or where a temporary work around has been provided.
P4	Incident minor or intermittent impact to a non-operational element of the Associated Service; for example: a temporary failure of reporting or billing.
P5	Incident has no direct impact on the Associated Service. Records normally kept for Incidents are used for information purposes. Example: to track upgrades, to obtain a reason for outage report (RFO), for planned outages or for enquiries as well as customer provoked Incidents.

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

(a) you confirm that the Incident is cleared within five hours of being informed; or

(b) 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 five hours of BT's attempt to contact you.

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

9.1.3 BT will keep you informed throughout the course of the Incident resolution at regular intervals. Updates may be provided by telephone, email or through your BT My Account.

10 Invoicing

10.1 In addition to the invoicing provisions set out elsewhere in this Contract and an Order, BT may invoice you for any of the following Charges:

10.1.1 Installation Charges, on the Service Start Date or monthly in arrears prior to the Service Start Date for any work carried out where the planned installation period is longer than one month;

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

10.1.3 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 Next Generation Firewall 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;

10.1.4 Charges incurred due to inaccuracies in information provided by you to BT, including the requirements of the CSP; and

10.2 Subject to Paragraph 10.1.1, the invoicing start date for the BT Managed Next Generation Firewall Service is the Service Start Date.

10.3 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 may commence invoicing for the BT Managed Next Generation Firewall Service.

11 Charges at the end of the Contract

11.1 In addition to the Charges set out elsewhere in this Contract, if you terminate during the Minimum Period of Service you will pay BT:

11.1.1 for any parts of the BT Managed Next Generation Firewall Service that were terminated during the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to:

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

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

(c) any waived Installation Charges.

11.1.2 for any parts of the BT Managed Next Generation Firewall Service that were terminated after the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to 35 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service.

Part C – Target CSP Change Request Times

12 CSP Change Request Delivery Time Targets

12.1 Targets apply to Urgent Changes and Standard Changes.

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

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

12.4 The response time for the changes is listed below:

Request	Target Implementation
Urgent Change and Emergency Change	4 Hours
Standard Change	8 Hours

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

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 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 Schedule):

"**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 Next Generation Firewall Service and that the BT Managed Next Generation Firewall 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.
"**Active Active**" has the meaning give in Paragraph 3.1.10(d).
"**Active Passive**" has the meaning given in Paragraph 3.1.10(d).
"**Availability**" means the period of time when the BT Managed Next Generation Firewall Service is functioning.
"**BT Managed Next Generation Firewall Service**" has the meaning given in Paragraph 1.1.
"**BT Owned**" has the meaning given to in Paragraph 2.6.1.
"**Circuit**" means any line, conductor, or other conduit between two terminals by which information is transmitted.
"**Critical CVSS score**" means a CVSS score range from 9.0 to 10.0.
"**Customer Committed Date**" has the meaning given in Paragraph 7.1.1.
"**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 Next Generation Firewall 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 Next Generation Firewall Service.
"**CVSS**" means Common Vulnerability Scoring System v3.0.
"**DMZ**" means de-militarised zone.
"**Domain Name**" means a readable name on an Internet page that is linked to a numeric IP Address.
"**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.
"**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.
"**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.
"**Minimum Period of Service**" means a period of 12 months beginning on the Service Start Date, unless otherwise set out in an Order.
"**Multi-Protocol Label Switching**" or "**MPLS**" means Multi-Protocol Label Switching, a private, global IP-based VPN service based on industry standards that provides the Customer with any-to-any connectivity and differentiated performance levels, prioritisation of delay and non-delay sensitive traffic as well as voice and multi-media applications, all on a single network.
"**BT MyAccount**" means an online portal you will have access to. That online portal provides instant access to your service, and allows you to:

(a) raise Incidents and check the progress of any 'live' Incidents BT is managing;
(b) request SSRs to your service; and
(c) obtain copies of your bills.

"**Nominated Representative**" means a person from your organisation nominated to be the point of contact for Vulnerability notifications.
"**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.
"**Professional Services**" means those services provided by BT which are labour related services.
"**PSTN**" means Public Switched Telephone Network, which is the concentration of the world's public circuit switched telephone networks.
"**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.
fails the BT Managed Next Generation Firewall 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 Optimisation Manager**" means the security manager appointed by BT who will work with you in respect of the activities as set out in Paragraph 2.5.
"**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 Next Generation Firewall Service.
"**SOC**" means Security Operations Centre.
"**Standard Change**" means upgrades and modifications resulting from planned developments and security improvements.
"**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.
"**Vulnerability**" means a Software susceptibility that may be exploitable by an attacker.