BT Managed Cloud Connect
Annex to the IP Connect UK Service Schedule

Contents

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the IP Connect UK Service Schedule, 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 IP Connect UK Service Schedule, Managed Service Schedule and the General Terms.

Part A – The Managed Cloud Connect Service

1 SERVICE SUMMARY

1.1 BT will provide you the Service Options set out in Paragraph 2 and as set out in the Order, up to the point of the Service Management Boundary as set out in Paragraph 3 ("**Services**").

1.2 The Services must be purchased with and as part of the IP Connect UK Service, and only where the IP Connect UK Service is purchased with the Managed Service and is subject to the terms set out in the IP Connect UK Service Schedule to the General Terms and Managed Service Schedule to the General Terms.

1.3 For the purposes of the Managed Service Schedule the Services are Associated Services.

1.4 You may purchase the Services with any of the Managed Service Packages, but Services will only be provided at Managed Service Package 1 level.

2 SERVICE OPTIONS

BT will provide you with the following Service Options in accordance with the details as set out in any applicable Order:

2.1 **Internet Gateway Regional and Cloud Firewall**

2.1.1 BT will provide you with access to Internet based applications from a single VPN(s). All Internet traffic from Sites in that VPN follows a default route to the Internet, in general using the nearest Internet Gateway (selected based upon BT Network topology) to take this traffic to the Internet via the IP Connect UK Service (**"Internet Gateway Regional"**).

2.1.2 For resiliency purposes, BT advises that you order at least two or more gateways per VPN. When you select more than one Internet Gateway, all of them are available. All Internet traffic from that VPN is dynamically routed via the alternate Internet Gateway(s) in the event of network outage.

2.1.3 You will have the ability to select a fixed capacity for the Internet Gateway Regional. All Sites on that VPN for accessing the Internet share that Internet Gateway bandwidth.

2.1.4 BT will provide the Internet Gateway Regional in the locations set out in the Order. If you allow Users, or otherwise configure or permit the configuration of the IP Connect Service in other locations which are not set out in the Order, then you will ensure that you operate within appropriate laws and regulations in each location from where you are using the Internet Gateway Regional. Any use of the IP Connect Service outside the locations set out in the Order is solely at your own risk and BT cannot accept any legal or regulatory responsibility for such use.

2.1.5 The IP Connect UK Service cannot be used for Internet browsing in the countries advised by BT as Blocked Countries, due to the laws and regulations that operate in these countries.

2.1.6 As part of the Internet Gateway Regional, BT will provide you with a network security service that controls inbound and outbound connectivity to the Internet from the IP Connect UK Service ("**Cloud Firewall**"):

(a) BT will provide a virtual Cloud Firewall using BT preferred technology hardware and software partner(s). Cloud Firewall is virtualised and hosted at BT locations.

(b) As part of the Cloud Firewall, BT will implement the initial Customer Security Policy ("**Initial Setup**"). You will specify the CSP prior to Order submission, using the CSP requirements template that BT will provide you with.

(c) BT does not guarantee that Cloud Firewall will detect or block all malicious threats.

2.1.7 Where you ordered multiple Internet Gateways, the Cloud Firewall will be resilient to failure of any single element, to the extent that traffic will be re-routed around a failed service element via an alternative service element, until BT restores the failed service element.

(a) In such cases there would be temporary interruption of the Cloud Firewall and active sessions will need to be re-established; and

(b) your re-routed traffic will egress to the Internet in other geographic locations if there is no alternate Internet Gateway in the same region.

2.1.8 **Cloud Firewall Components**: As part of your Cloud Firewall Service, BT will provide you with all of the following components:

(a) **Firewall Intrusion Prevention Service:**

(i) BT will monitor traffic passing through your Cloud Firewall for attacks, in accordance with the applicable intrusion signature files ("Firewall Intrusion Prevention Service").

(ii) BT:

i. will implement the Firewall Intrusion Prevention Service with a default configuration setting, including a standard signature list;

ii. will maintain a subscription to the necessary signature updates, and arrange for these to be applied following issue by the Supplier; and

iii. will not be responsible for evaluating these signatures beforehand.

(iii) BT will block high impact or high confidence attacks, as defined by the Supplier of the Software BT uses to deliver the Firewall Intrusion Prevention Service.

(iv) The Firewall Intrusion Prevention Service does 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.

(v) 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.

(b) **Firewall URL Filtering:**

BT will:

(i) block access to Internet sites 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 alert message to a User attempting to access a blocked or restricted site;

(iii) implement any requested alterations via the standard SSR process in the event of any change to your CSP.

("Firewall URL Filtering").

(c) **Firewall Anti-Virus:**

(i) BT will provide you with a service that will:

i. check web browser traffic for known malware;

ii. inspect requests from Users for an executable file from a site on the Internet, against the current anti-virus 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 anti-virus definition files up to date by regular downloads direct from the anti-virus service.

("Firewall Anti-Virus").

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

2.2 **Cloud Connect Direct**

2.2.1 BT will provide you with direct private access, through a VPN, to the Cloud Services in one or more interconnection points on the BT Network, as set out in the Order ("**Cloud Connect Direct**").

2.3 BT cannot guarantee that the Services will operate without Incident or interruption or to intercept or disarm all malware.

3 SERVICE MANAGEMENT BOUNDARY

3.1 BT will provide the Services in accordance with the IP Connect UK Service Schedule, Parts B and C of this Annex and as set out in any applicable Order ("Service Management Boundary") up to:

(a) for the Internet Gateway Regional: the port on the BT Equipment that provides connectivity to the Internet;

(b) for Cloud Connect Direct: the connection point between the third party service provider router and the BT Equipment.

3.2 BT is not responsible for the availability, applications or any other element or functionality of any associated third party services or any Enabling Services.

3.3 You are solely responsible for obtaining and maintaining all necessary software licences or other authorisations and consents required by the third party services or any Enabling Services.

3.4 BT will have no responsibility for the Services outside the Service Management Boundary.

3.5 BT does not make any representations, whether express or implied, about whether the Services will operate in combination with any Customer Equipment or other equipment and software.

4 SPECIFIC TERMS

4.1 **EULA**

4.1.1 BT will only provide the Cloud Firewall Service if you have entered into the end user licence agreement with the Supplier in the form set out at https://www.checkpoint.com/support-services/software-license-agreement-limited-hardware-warranty/("**EULA**").

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

4.1.3 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 Cloud Firewall Service upon reasonable Notice, and:

(a) you will continue to pay the Charges for the Cloud Firewall Service until the end of the Minimum period of Service; and

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

4.1.4 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.

4.1.5 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.

4.2 **Changes to the Customer Security Policy**

4.2.1 You may request additions, deletions, or modifications to your CSP and BT will provide you with the means to request SSR to the CSP through the Managed Services Portal.

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

4.2.3 BT may charge you for changes to the CSP in accordance with the SSR process set out in the Managed Services Schedule.

4.2.4 BT will only make configuration changes as set out in Paragraph 4.2.1. 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 will:

(a) offer you Professional Services as set out in the Managed Services Schedule; and

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

4.2.5 Access to the Managed Service Portal is controlled and you will ensure your Users will not share access. All User ID tokens/passwords are to be uniquely assigned to named individuals. These individuals will not:

(a) allow anyone else to use their token/ID or share passwords;

(b) leave their User account logged in while their computer is unlocked and unattended;

(c) submit any unauthorised changes; or

(d) 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 to their own organisation and to BT immediately.

4.2.6 BT will implement any reasonable changes to the CSP you requested, as set out in Paragraph 4.2.

4.2.7 Service Credits do not apply to CSP change requests.

4.3 **Invoicing**

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:

4.3.1 Charges for the refresh or upgrade of connections, hardware or software if required by you, unless the refresh or upgrade is operationally necessary to enable BT to continue to provide the Services, or any

part of the Services. This does not apply to changes to the CSP which will be charged in accordance with the Managed Service Schedule to the General Terms;

4.3.2 Charges for 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; and

4.3.3 Charges incurred due to inaccuracies or incomplete information you provided to BT.

4.4 **Changes to the Managed Service Schedule**

4.4.1 Paragraph 2.6.1 of the Managed Service Schedule to the General Terms will not apply to the Services, and as part of your Managed Service Package 1 BT will:

(a) carry out remote diagnosis if an Incident affecting the Services is found and in such case:

(i) log the Incident;
(ii) attempt to resolve the Incident;
(iii) contact you within one hour of detecting an Incident; and (iv) inform you what action has been taken or is required to resolve the Incident; and

collectively called "**Enhanced Proactive Monitoring Core**".

.

Part B – Service Delivery and Management

5 BT'S OBLIGATIONS

5.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the Services, BT will:

5.1.1 where applicable, configure the Cloud Firewall Service remotely in accordance with the Initial Setup as set out in Paragraph 2.1.6(b);

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

5.1.3 conduct a series of standard tests on the Services to ensure that they are configured correctly; and

5.1.4 on the date that BT has completed the activities in this Paragraph 5.1, confirm to you that the Services are available for performance of any Acceptance Tests as set out in Paragraph 6.2.

5.2 **During Operation**

On and from the Service Start Date, BT:

5.2.1 for Cloud Firewall service only, will, for a period of five Business Days after the Service Start Date, implement any minor corrections to the Customer Security Policy that may be necessary for the operation. BT will implement such changes as soon as reasonably practicable. Any substantial changes to the CSP will need to be requested through the Changes to CSP process as set out in Paragraph 4.2.3 and the Managed Service Schedule, and will be scheduled for implementation following this five Business Day period;

5.2.2 will maintain any relevant Managed Services Portal to provide you with online access to a range of functions and capability to submit Simple Service Requests as set out in Managed Service schedule, including placing CSP change requests in accordance with Paragraph 4.2 of this Annex;

5.2.3 will manage the ongoing maintenance, monitoring and configuration of BT Equipment for the duration of the Services;

5.2.4 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 Clause 17.2.2 of the General Terms, BT will extend the software licences and any required support contracts for a further 12 months;

5.2.5 will use secure protocols or provide a secure management link to connect to the Services via the Internet or other agreed network connection, in order to monitor the Services proactively and to assist in Incident diagnosis; and

5.2.6 will, from time to time, undertake work on the Services, which may interrupt the Services. In such cases, BT will endeavour to inform you in advance of any work being undertaken, and will endeavour to minimise the impact of such work.

5.3 **The End of the Service**

On termination of the Services by either one of us, or expiry, BT will:

5.3.1 terminate any relevant Software and stop providing the Services;

5.3.2 where requested in writing prior to the termination of this Contract, provide, where reasonably practical, configuration information relating to the Services or their part 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; and

5.3.3 not have any responsibility for securing your Internet connections and will not be liable for the increased risk you expose yourself to.

6 YOUR OBLIGATIONS

6.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the Services, you will:

6.1.1 in relation to Cloud Firewall:

(a) ensure that the standard CSP specified by you as part of the Initial Setup as set out in Paragraph 2.1.6 meets your requirements, including specifications that cover your legacy networks, application services, third party services and other Enabling Services;

(b) be responsible for defining your ongoing CSP beyond that Initial setup that you confirmed after Service Start Date of the Cloud Firewall;

(c) be responsible for the CSP;

6.1.2 ensure that your Enabling Services bandwidth is sufficient to meet your requirements;

6.1.3 manage, and where applicable provide BT with accurate details of your internal IP address design;

6.1.4 obtain and provide in-life support for any Software running on your end user devices;

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

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

6.1.7 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 miss-use the Services 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 Services and BT may refuse to restore the Services until BT receives an acceptable assurance from you that there will be no further contravention; or

(b) terminate the Services upon Notice in accordance with Clause 25 of the General Terms.

6.2 **Acceptance Tests**

6.2.1 After receiving Notice from BT under Paragraph 5.1.4, you will promptly carry out the Acceptance Tests for the Services. The Services will be deemed to have been accepted if you have not:

(a) carried out the Acceptance Tests and confirmed acceptance in writing; or

(b) notified BT in writing that the Services has not passed the Acceptance Tests,

within five Business Days following notification under Paragraph 5.1.4.

6.2.2 Subject to Paragraph 6.2.3, the Service Start Date will be the earlier of the following:

(a) the date that you confirm acceptance of the Services in writing under Paragraph 6.2.1(a); or

(b) the date of notification under Paragraph 5.1.4.

6.2.3 In the event that the Acceptance Tests are not passed, BT will remedy the non-conformance without undue delay and notify you 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 Services, or due to delays or inaccuracies in information provided by you to BT, including minor corrections of the Customer Security Policy as set out in Paragraph 5.2.1, BT may apply additional Charges to remedy the non-conformances.

6.3 **During Operation**

On and from the Service Start Date, you will:

6.3.1 ensure that all Software provided is used solely for operation of the Services;

6.3.2 in the event of a failure of a Cloud Firewall, permit BT or BT's agents at BT's discretion to remove and replace faulty components or to remove the faulty Cloud Firewall 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;

6.3.3 request, if applicable, access for additional authorized Users to a Managed Service Portal for use by you or your agents, as set out in Managed Service Schedule. You are responsible for your agents' use of these IDs; and

6.3.4 agree that:

(a) BT may share Customer information (including Personal Data) with the supplier of BT Equipment or Customer Equipment or Cloud Services as may be necessary for the provision and management of the Services. Depending on the Service(s) provided, Customer information may be automatically sent from Services hardware or Software to cloud-based infrastructure operated by the supplier;

(b) Processing of Customer information (including Personal Data) will be subject to the relevant supplier's EULA (where applicable) and privacy policy as may be amended or supplemented from time to time by the supplier. You agree that BT will not be liable for any claim arising out of or in connection with any failure by the supplier to comply with the supplier's EULA (where applicable) and privacy policy and any claims will be made directly by you against the supplier;

(c) BT will not be liable for failure to or delay in supplying the Services or their part if another supplier delays or refuses the supply of an electronic communications service to BT and no alternative service is available at reasonable cost;

(d) BT will provide the Services to you on an "**as is**" and "**as available**" basis. BT does not guarantee that the Services, or any part of the Services:

(i) will be performed error-free or uninterrupted or that BT will correct all errors in the Services;
(ii) will operate in combination with your content or applications or with any other software, hardware, systems or data; and
(iii) including any products, information or other material you obtain under or in connection with this Contract, will meet your requirements;

(e) 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;

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

(g) customer information may be transferred or stored outside the European Economic Area or the country where you and your Users are located in order to carry out the Services and BT's other obligations under this Contract; and

6.3.5 you will be responsible for results obtained from the use of the Services, 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 Services, or any actions taken by BT at your direction.

6.4 **The End of the Service**

6.4.1 On termination of the Services by either one of us, or expiry you will be responsible for securing your Internet connections and will be liable for the increased risk you expose yourself to.

Part C – Service Levels

There are no Service Levels for the Services.

Part D – Defined Terms

7 DEFINED TERMS

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

"**Acceptance Tests**" means those objective tests conducted by you, which, when passed confirm that you accept the Services and that the Services are ready for use save for any minor non-conformities, which will be resolved as an Incident as set out in Paragraph 6.2.

"**Blocked Countries**" means China, India, Russia and Columbia, however this list is subject to changes in laws and regulations. For the avoidance of doubt, countries may be added or removed from this list.

"**BT Network**" means the communications network owned or leased by BT and used to provide the Services.

"**Services**" have the meaning given in Paragraph 1.1.

"**Cloud Connect Direct**" has the meaning given in Paragraph 2.2.

"**Cloud Firewall**" has the meaning given in Paragraph 2.1.6.

"**Cloud Services**" means the cloud based computing infrastructure platforms known as Amazon Web Services and Microsoft Azure provided by Amazon Inc. and Microsoft Inc. respectively or any other cloud based computing infrastructure platform that BT confirms is compatible with the Services.

"**CSP**" or "**Customer Security Policy**" means your security policy containing the security rules set and owned by you, that are applied to the Cloud Firewall and determine the operation of the Cloud Firewall Service.

"**EULA**" has the meaning given in Paragraph 4.1.1.

"**Enhanced Proactive Monitoring Core**" has the meaning given in Paragraph 4.4.1.

"**Firewall Anti-Virus**" is a Service Option and is defined as set out in Paragraph 2.1.8(c).

"**Firewall Intrusion Prevention Service**" is a Service Option and is defined as set out in Paragraph 2.1.8(a).

"**Firewall URL Filtering**" is a Service Option and is defined as set out in Paragraph 2.1.8(b).

"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the Services or particular element of the Services.

"**Initial Setup**" means the facilitation of the setup and delivery of the Cloud Firewall as set out in Paragraph 2.1.6(b).

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

"**Internet Gateway**" means a network point allowing access to the Internet.

"**Internet Gateway Regional**" has the meaning given in Paragraph 2.1.1.

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

"**Schedule**" means IP Connect UK Schedule to the General Terms.

"**Service Desk**" means the helpdesk that you are able to contact to submit service requests, report Incidents and ask questions about the Service.

"**Uniform Resource Locator**" or "**URL**" means a character string that points to a resource on an intranet or the Internet.

"**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.