BTnet Security
Annex to the BTnet (Internet Connect UK) Schedule

Contents

A note on 'you'

'You' and 'your' mean the Customer and your Users, where applicable.

Words Defined in the General Terms and Schedule

Words that are capitalised but have not been defined in this Annex have the meanings given to them in the General Terms and the BTnet (Internet Connect UK) Schedule to the General Terms.

Application of this Annex

The terms in this Annex apply in addition to those in the BTnet (Internet Connect UK) Schedule and the General Terms.

Part A – The BTnet Security Service

1 Service Summary

This Annex to the BTnet (Internet Connect UK) Schedule will only apply where you have selected the compatible Cisco Meraki Managed CPE as part of the BTnet (Internet Connect UK) Service. The BTnet Security Service is for use with a single BTnet Internet connection from your Sites in the UK and does not provide any site to site VPN capability.

2 Standard Service Components

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

2.1 **Managed Installation**

BT will coordinate the BTnet Security Service installation and commissioning, liaising with you, installers and equipment suppliers as appropriate. BT will administer all activities remotely.

2.2 **Incident Fault and Change Management**

(a) BT will provide a 24x7x365 Service Centre to respond to Incidents.

(b) You may request configuration changes to the BTnet Security Service via the BTnet User Portal which will initiate a request to the BTnet (Internet Connect UK) Service team for action. BT will action the configuration changes during normal Business Hours and complete it by the end of next Business Day.

(c) BT may charge you for configuration changes if BT considers that the number or frequency of such changes are excessive. Both of us will agree on the pricing for any configuration changes before implementation.

2.3 **Service Performance Reports**

BT will grant you access to reporting functionality for key Service performance metrics and for some security-related events via the BTnet User Portal.

3 Service Options

BT will provide you with the following Service Options that are only available in the UK, as set out in any applicable Order and in accordance with the details as set out in that Order:

3.1 **Layer 3 Firewall**

3.1.1 BT will configure your firewall to allow outbound traffic. All inbound traffic will be blocked by default.

3.1.2 BT will carry out configuration changes to your Layer 3 Firewall on request, where necessary.

3.1.3 If BT agrees a request from you to alter your firewall policy, you accept responsibility for these changes.

3.1.4 BT will provide a standard security configuration template for your BTnet Security Service but you will own and will be responsible for this configuration, including any changes or additions that you ask BT to make to your configurations and policies.

3.2 **Layer 7 Firewall with Application Control**

3.2.1 Layer 7 Firewall enables to, upon your request, create firewall rules to block specific web-based services, websites, or types of websites without having to specify IP addresses or port ranges. BT will block certain categories by default when BT accepts your Order.

3.2.2 You may request BT to provide you with the list of blocked application categories and all additional available categories.

3.2.3 BT is not responsible for how the applications are categorised, the regularity of update or for evaluating which applications fall under each category.

3.2.4 You may request BT to add or remove available application categories.

3.2.5 You will accept responsibility for the configuration and any changes made to access applications and any increased risk of being exposed to malicious content.

3.3 **Content Filtering**

3.3.1 BT will block certain categories of websites by default when BT accepts your Order. You may request BT to provide you with the list of blocked categories and all additional available categories.

3.3.2 BT will provide you with Content Filtering in two modes: the full list mode or the top sites only mode.

3.3.3 BT will set your default configuration to the full list mode for better coverage. In this mode, your request for a URL that is not in the list of top sites only will cause the appliance to look the URL up in a cloud-hosted database. You acknowledge that this may have a noticeable impact on browsing speed and performance when visiting a Site for the first time. The result will then be cached locally. Over time, the full list performance should approach the speed of the top sites only mode.

3.3.4 Once your Service is up and running, you may choose to switch your setting to the top sites only. In this mode, the list of top sites in each of the blocked categories will be cached locally on the appliance. Your request for a URL that is not in the top sites only list will always be permitted (as long as they are not in the blocked categories list).

3.3.5 To block access to sites that employ https rather than http you must set the full list. You acknowledge that it is not possible to return an explanatory page to a user where the URL filtering element has blocked an https based website.

3.3.6 The websites and applications captured under these categories are dependent on the Webroot BrightCloud® URL categorisation database for CIPA and IWF compliant content-filtering. Website categories are regularly updated. BT does not take any responsibility for how the websites and applications are categorised or the regularity of updates.

3.3.7 You may request BT to add or remove available categories to restrict or allow your Users access to categories of websites.

3.3.8 For URL filtering, you may request BT to white list or block particular URL addresses within a category.

3.3.9 You will be responsible for the configuration and any changes made to access to websites and any increased risk of being exposed to malicious web content.

3.4 **Intrusion Detection and Prevention Service**

3.4.1 BT will:

(a) monitor traffic passing through your BTnet (Internet Connect UK) Managed CPE to identify traffic patterns that match known threats, in accordance with the applicable intrusion signature files using Cisco Sourcefire SNORT® Engine

(b) implement this Service Option with a default configuration setting, including a standard signature list which works using Cisco Sourcefire SNORT® Engine;

(c) not be responsible for evaluating the signatures beforehand;

(d) select the "**balanced**" ruleset as your default detection setting. "**Balanced**" ruleset contains rules that are from the current year and the previous two years, are for vulnerabilities with a CVSS (Common Vulnerability Scoring System) score of 9 or greater, and are in one of the following categories:

(i) **Malware-CNC (Command and Control)**: Rules for known malicious command and control activity for identified botnet traffic. This includes call home, downloading of dropped files, and ex-filtration of data.

(ii) **Blacklist**: Rules for URLs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.

(iii) **SQL (Structured Query Language) Injection**: Rules that are designed to detect SQL Injection attempts.

(iv) **Exploit-kit**: Rules that are designed to detect exploit kit activity.

(e) select "**prevention**" as the default configuration setting in the Order. Traffic will be automatically blocked if it is detected as malicious based on the detection ruleset set out in Paragraph 3.4.1(d);

(f) agree to alter the setting from "**prevention**" to "**detection**" or "**disabled**" upon your request. If "**detection**" mode is selected, the BTnet Security Service will no longer block traffic patterns which match

(g) known threats and only identify them, and if "**disabled**" mode is selected, no prevention or detection will take place; and

(h) not pro-actively or reactively investigate or act upon detected or prevented threats or attacks.

3.4.2 Use of Intrusion Prevention may result in false positives where certain applications and traffic flows may cause the feature to block legitimate traffic (e.g. applications not adhering to network communication standards). BT will not be liable if false positives occur and as a result, legitimate traffic is blocked.

3.4.3 If BT agrees a request from you to alter the parameters for applying new signatures to give a greater or lower sensitivity to attacks, you will be responsible for the outcome of these changes and accept the potential increased risk of false positives (blocks to legitimate traffic) or the increased risk of threats being missed. This includes whitelisting a specific intrusion detection signature or changing your ruleset from 'balanced' to a different mode.

3.5 **Advanced-Malware Protection (AMP)**

3.5.1 BT will:

(a) inspect HTTP file downloads and block or allow file downloads based on their disposition, by using a file reputation based protection engine powered by Cisco AMP; and

(b) determine the disposition of a file as "**clean**", "**malicious**" or "**unknown**" using the threat intelligence retrieved from Cisco AMP.

3.5.2 Files can change disposition based on new threat intelligence e.g. a downloaded file can go from having a "**clean**" to a "**malicious**" disposition. BT will not be responsible for taking any action or for informing you should a file change disposition. BT will only classify the file at the point of inspection.

3.5.3 When traffic is filtered, the URL or ID and the action taken are logged in the portal used by BT.

3.5.4 You may white list specific URL's and files upon request. You may also disable the AMP Service Option entirely upon request.

3.5.5 You will be responsible for the configuration and any changes made to the AMP Service Option and any increased risk of being exposed to malicious content.

3.5.6 Use of AMP may result in false positives where a file or URL that you deem safe is blocked. BT is not liable when false positives occur and result in legitimate files or URL's being blocked.

3.6 **Security Event Reporting**

3.6.1 BT will:

(a) provide reporting functionality for key Service performance metrics, and for some security-related events. This will be available via the BTnet User Portal; and

(b) not pro-actively view your reports and events for security incidents or threats. BT will not pro-actively send you any information regarding security event reporting.

3.6.2 The period over which BT can analyse data is dependent on the capacity of, or the space allocated on, the reporting platform.

3.7 **Security Settings and Configuration**

3.7.1 BT will configure your compatible BTnet Security Service with a templated set of security policies.

3.7.2 You will own and will be responsible for this templated configuration, including any changes or additions that you ask BT to make to your security configurations and policies.

3.7.3 BT will not vet or assess any changes to your security configuration that you ask to be made.

3.7.4 BT is not responsible for the total security of your network, User devices, connection or Internet traffic.

3.7.5 If you require configuration changes, BT will make these in life and upon your request via the BTnet User Portal.

3.7.6 The BTnet (Internet Connect UK) Service team will action the requested configuration changes during normal Business Hours and will complete them by the end of next Business Day.

3.7.7 BT may charge you for configuration changes if BT considers that the number or frequency of such changes are excessive. Both of us will agree on pricing for any configuration changes before implementation.

4 Service Management Boundary

BT will have no responsibility for the Service outside the Service Management Boundary as set out in Paragraph 4 of the BTnet (Internet Connect UK) Service Schedule.

5 Associated Services

You will have the following services in place that will connect to the Service being delivered and are necessary for the BTnet Security Service to function and will ensure that these services meet the minimum technical requirements that BT specifies:

5.1 BTnet (Internet Connect UK) Service (the "**Enabling Service**") that includes:

5.1.1 connectivity to the internet as defined within the BTnet (Internet Connect UK) Service Schedule; and

5.1.2 a supported Cisco Meraki Managed CPE provided as part of the BTnet (Internet Connect UK) Service. BT does not support the BTnet Security Service where you use a customer-provided CPE as part of Wires Only BTnet (Internet Connect UK) Service.

6 Installation and Acceptance

6.1 For Orders that you have placed at the same time as the Enabling Service, BT will aim to install the BTnet Security Service on the Customer Committed Date. BT will activate the BTnet Security Service on the Service Start Date.

6.2 Subject to Paragraph 5, for Orders that you have placed for existing BTnet (Internet Connect UK) Service, BT will activate the BTnet Security Service, during Business Hours, in three Business Days from acceptance of Order.

6.3 On the date that BT has completed the activities set out in this Paragraph 6, BT will confirm to you the BTnet Security Service Start Date or, if applicable, that the BTnet Security Service is available for performance of any Acceptance Tests as set out in Paragraph 12.2.

7 Security

7.1 You will ensure the proper use of any usernames, personal identification numbers and passwords used with the BTnet Security Service, and you will take all necessary steps to ensure that they are kept confidential, secure and not made available to unauthorised persons.

7.2 BT does not guarantee the security of the BTnet Security Service against unauthorised or unlawful access or use.

8 Minimum Period of Service

8.1 The BTnet Security Service will commence from the BTnet Security Service Start Date and will run co-terminus with the Committed Term for your BTnet (Internet Connect UK) Service.

8.2 On completion of the Committed Term, the BTnet Security Service will continue to be active and BT will bill you on a rolling basis, until such a time that you either the BTnet Security Service or the BTnet (Internet Connect UK) Service is terminated in accordance with Clause 17, 18 or 19 of the General Terms.

8.3 If you exercise your right under Clause 17 of the General Terms to terminate the BTnet Security Service, for convenience, during the Committed Term, you will pay BT, by way of compensation an amount equal to 50 per cent of the Recurring Charges for all other remaining months of the Committed Term.

8.4 If BT exercises BT's right under Clause 18 of the General Terms to terminate the BTnet Security Service you will pay BT the Termination Charges due, if any, as set out in Paragraph 8.3.

9 EULA

9.1 BT will only provide the BTnet Security Service if you have entered into the end user licence agreement with the Supplier in the form set out at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/meraki-seula.pdf as may be amended or supplemented from time to time by the Supplier ("**EULA**").

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

9.3 In addition to Clause 15 of the General Terms, if you do not comply with the EULA, BT may restrict or suspend the BTnet Security Service upon reasonable Notice, and:

9.4 you will continue to pay the Charges for the BTnet Security Service until the end of the Minimum period of Service; and

9.5 BT may charge a re-installation fee to re-start the BTnet Security Service.

9.6 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.

9.7 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.

10 Invoicing

10.1 BT will invoice you for the Charges for the BTnet Security Service as set out in Paragraphs 10.2 and 10.3 in the amounts and currency specified in any Orders.

10.2 Unless stated otherwise in an applicable Order, BT will invoice you for:

10.2.1 Recurring Charges quarterly in advance on the first day of the relevant quarter (for any period where the BTnet Security Service is provided for less than one quarter, the Recurring Charges will be calculated on a daily basis); and

10.2.2 any Termination Charges incurred in accordance with Paragraph 8 of the BTnet (Internet Connect UK) Service Schedule upon termination of the BTnet Security Service.

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

10.3.1 Charges for investigating Customer reported Incidents where BT finds no Incident or that the Incident is outside the Service Management Boundary;

10.3.2 Charges for restoring the BTnet Security Service if the BTnet Security Service has been suspended in accordance with Clause 10.1.2 of the General Terms;

10.3.3 Charges for cancelling the BTnet Security Service in accordance with Clause 16 of the General Terms;

10.3.4 any fees payable by you for deviations from the standard provision of the BTnet Security Service, as set out in the Contract; and

10.3.5 any other Charges set out in any applicable Order or otherwise agreed between both of us.

10.3.6 BT may charge you for configuration changes to the BTnet Security Service as set out in Paragraph 3.7.7, if BT considers that the number or frequency of such changes are excessive. Both of us will agree pricing for any configuration changes before implementation.

11 PCI DSS Compliance Obligations

11.1 The BTnet Security Service is not compliant with PCI DSS nor is it designed or intended to be and you will not use the BTnet Security Service for the processing, storage or transmission of any Cardholder Data or any data that is subject to PCI DSS.

11.2 You will indemnify BT for any Claims, losses, costs or liabilities that it incurs as a result of you storing, processing or transmitting data that is subject to PCI DSS.

Part B – Service Delivery and Management

12 BT's Obligations

12.1 **Service Delivery and Commissioning of the BTnet Security Service**

Before the BTnet Security Service Start Date and, where applicable, throughout the provision of the BTnet Security Service, BT:

12.1.1 will configure the BTnet Security Service remotely in accordance with the default security configuration ready for BTnet Security Service Start Date;

12.1.2 on the date that BT has completed the activities in this Paragraph 12.1, confirm to you that the BTnet Security Service is available for performance of any Acceptance Tests in accordance with Paragraph 13.2.

12.2 **During Operation**

On and from the BTnet Security Service Start Date, BT:

12.2.1 will work with the relevant supplier to restore the BTnet Security Service as soon as practicable if you report an Incident with the BTnet Security Service;

12.2.2 will maintain the BTnet User Portal to provide you with online access to service reports and placing security configuration change requests;

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

12.2.4 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.

12.2.5 will provide the BTnet Security Service to you on an "**as is**" and "**as available**" basis. BT does not guarantee that the BTnet Security Service will be performed error-free or uninterrupted or that BT will correct all errors in the BTnet Security Service.

12.3 **The End of the Service**

On notification of termination of the BTnet Security Service by either one of us, or notification of expiry of the BTnet Security Service, BT will:

12.3.1 terminate any rights of access to the relevant Software and stop the BTnet Security Service; and

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

13 Your obligations

13.1 **BTnet Security Service Delivery and Commissioning of the Service**

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

13.1.1 ensure that the LAN protocols and applications you use are compatible with the BTnet Security Service;

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

(a) inform your Users that as part of the BTnet Security Service being delivered by BT, BT may monitor and report to you the use of any targeted applications by them;

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

(c) agree that BT will not be liable for any failure by you to comply with this Paragraph 13.1.1, you will be liable to BT for any Claims, losses, costs or liabilities incurred or suffered by BT due to your failure to comply with this Paragraph 13.1.1.

13.1.3 be responsible for your security configuration, and for reviewing and requesting any changes to that configuration;

13.1.4 manage, and provide BT with accurate details of your internal IP address design;

13.1.5 obtain and provide in-life support for any software running on your Users' devices; the security and operation of Users' devices is your responsibility;

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

13.2 **Acceptance Tests**

13.2.1 After receiving Notice from BT under Paragraph 12.1.2, you will promptly carry out the Acceptance Tests for the BTnet Security Service. The BTnet Security Service will be deemed to have been accepted if you have not:

(a) carried out the Acceptance Tests and confirmed acceptance to the BT Commissioning Team; or

(b) notified to the BT Commissioning Team that the BTnet Security Service has not passed the Acceptance Tests,

within five Business Days following notification under Paragraph 12.1.2.

13.2.2 Subject to Paragraph 13.2.3, the BTnet Security Service Start Date will be the earlier of the following:

(a) the date that you confirm acceptance of the BTnet Security Service to the BT Commissioning Team under Paragraph 13.1.2(a); or

(b) the date following the fifth Business Day following notification under Paragraph 12.2.

13.2.3 In the event that the Acceptance Tests are not passed, BT will remedy the non-conformance without undue delay, notify you that BT has remedied the non-conformance and inform you of the BTnet Security Service Start Date.

13.2.4 Where the non-conformance is outside the scope of the BTnet Security Service, or due to delays or inaccuracies in information that you have provided BT, BT may apply Additional Charges to remedy the non-conformances.

13.3 **During Operation**

On and from the BTnet Security Service Start Date, you will:

13.3.1 distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the BTnet Security Service, including the BTnet User Portal;

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

13.3.3 permit BT or BT's agents at BT's discretion to remove and replace faulty components or to remove the faulty Managed CPE 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;

13.3.4 agree that the processing of customer information and Customer Personal Data will be subject to the relevant supplier's 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 privacy policy and you will make any claims directly against the supplier;

13.3.5 agree that the BTnet Security Service will operate in combination with your content or applications or with any other software, hardware, systems or data;

13.3.6 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;

13.3.7 be responsible for results that you have obtained from the use of the BTnet 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 that you have provided to BT in connection with the BTnet Security Service, or any actions that BT has taken at your direction.

13.4 **The End of the Service**

On notification of termination of the BTnet Security Service by either one of us, or notification of expiry of the BTnet, you will be responsible for securing your Internet connection and will be liable for the increased risk you expose yourself to.

14 Notification of Incidents

14.1 Notifications of incidents will be handled in accordance with Paragraph 10 of the BTnet (Internet Connect UK) Service Schedule. Part C (Service Levels) of the BTnet (Internet Connect UK) Service Schedule will not apply.

Part C – Defined Terms

15 Defined Terms

In addition to the defined terms in the General Terms and Schedule, 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 and the Schedule, these defined terms will take precedence for the purposes of this Annex):

"**BTnet Security Service**" has the meaning given in Paragraph 1.

"**BTnet Security Service Start Date**" means, for each BTnet Security Service, the date on which that BTnet Security Service is first made available to you.

"**BTnet User Portal**" means a web portal through which you access the monitoring pages to track aspects of the BTnet Security Service.

"**Cardholder Data**" means the unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. Cardholder data may also include any of the following: cardholder name, expiration date, service code or sensitive authentication data.

"**CIPA**" means Children's Internet Protection Act.

"**Cisco AMP**" means the Advanced Malware Protection system provided by Cisco, or similar technology from time to time, used as part of the BTnet Security Service.

"**Cisco Meraki Managed CPE**" means the Cisco Meraki brand Managed CPE provided by BT as part of the BTnet Security Service.

"**Cisco Sourcefire SNORT® Engine**" means an open source network intrusion prevention system and network intrusion detection system, or similar technology from time to time, used as part of the BTnet Security Service.

"**Content Filtering**" means web or URL filtering and does not include any email or file scanning.

"**DNS**" means Domain Name System.

"**EULA**" has the meaning given in Paragraph 9.1.

"**HTTP**" means hypertext transfer protocol.

"**IWF**" means Internet Watch Foundation.

"**Layer 3 Firewall**" has the meaning given in Paragraph 3.1.

"**Layer 7 Firewall**" has the meaning given in Paragraph 3.2.

"**PCI DSS**" means the Payment Card Industry Data Security Standards, a set of policies and procedures, issued by the PCI Security Standards Council LLC (as may be adopted by local regulators) and intended to optimise the security of credit and debit card transactions and protect cardholders against misuse of their personal information.

"**URL**" means Uniform Resource Locator (a website link).

"**VPN**" means Virtual Private Network.

"**Webroot BrightCloud®**" means a system that provides Content Filtering lists and databases, or similar technology from time to time, used as part of the BTnet Security Service.