Managed Virtual Firewall Security Fortinet with Agile Connect Service

Annex to the BT Managed Security Schedule to the General Terms

Contents

Application of this Annex

This Annex sets out the additional terms that will apply where BT provides you with the Managed Virtual Firewall Security Fortinet with Agile Connect Service. The terms of this Annex apply in addition to the terms set out in:

(a) the Schedule; and
(b) the General Terms.

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the General Terms

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

Part A – The Managed Virtual Firewall Security Fortinet with Agile Connect Service

1 Service Summary

BT will provide you with a virtual managed firewall service, comprising:

1.1 the Standard Service Components; and

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 ("**Managed Virtual Firewall Security Fortinet with Agile Connect Service**" or "**Service**").

2 Standard Service Components

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

2.1 BT will:

2.1.1 as part of the Initial Setup:

(a) deploy an Image remotely within your Agile Connect Service infrastructure;
(b) commission the Virtual Firewall and establish remote service management of the Virtual Firewall using an IP Address provided by BT; and

2.1.2 monitor and manage the Virtual Firewall in accordance with the Schedule.

3 Service Options

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

3.1 **Firewall URL Filtering and Application Control**

3.1.1 BT will:

(a) block access to the Internet sites that you ask BT to, in accordance with your CSP;
(b) send an appropriate message to a User attempting to access a blocked or restricted Internet site to advise either:

(i) that the User request has been blocked;
(ii) that the User will first confirm acceptance of your acceptable use policy (or similar warning) and upon acceptance by the User, the page will be delivered; or
(iii) implement any alterations, via the standard configuration management process, in the event of any change in your CSP.

3.2 **Firewall Anti-Virus**

3.2.1 BT will:

(a) check web browser (http) traffic for known malware;
(b) inspect requests from Users for an executable file from a site on the Internet, against the current antivirus definition file set out in the applicable intrusion signature files. If no virus is detected, the file will be passed to the User. If a virus is detected the file will be blocked and deleted; and
(c) keep antivirus definition files up to date by regular downloads direct from the firewall supplier.

3.3 **Firewall Anti-Bot**

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

3.4 **Ad Hoc Professional Services**

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

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

3.5 **Eagle-I Enhanced Firewall Service**

BT shall provide you with the Eagle-I Enhanced Firewall Service, subject to the requirements set out below.

(a) Existing Blocklist Enhancement

(i) Subject to BT confirming that your Security Appliance is suitable for use with the Eagle-I Enhanced Firewall Service, BT will use its Eagle-I Platform to identify any unique malicious IPs and/or URLs to supplement your Security Appliance's existing blocklist of malicious IPs and/or URLs ("**Indicators of Compromise**" or "**IOCs**".)

(ii) Upon confirming the suitability of your Security Appliance, BT will add new IOCs to the BT Blocklist for consumption by your Security Appliance ("**Existing Blocklist Enhancement**".)

(b) Automated IOC Blocking

(i) Subject to BT confirming the technical feasibility of applying Automated IOC Blocking to your Security Appliance, as part of its remote service management of your Security Appliance, BT shall automatically implement changes to your Security Appliance so that it will block IOCs propagated from the BT Blocklist ("**Automated IOC Blocking**").

(ii) For the avoidance of doubt, when the Eagle-I Enhanced Firewall service is specified, subject to the requirements of technical feasibility (as outlined above at Paragraph 3.1.15(b)(i)), BT shall implement Automated IOC Blocking. By specifying the Eagle-I Enhanced Firewall Service, you hereby consent to BT implementing Automated IOC Blocking in respect of your Security Appliance.

(iii) BT shall not be responsible for any wider impact of any Automated IOC Blocking, including but not limited to any impact from the Automated IOC Blocking on Customer Equipment, or on your wider Network.

4 Service Management Boundary

4.1 BT will provide and manage the Service as set out in Parts A, B and C of this Annex and the Schedule ("**Service Management Boundary**").

4.2 BT will have no responsibility for the Service outside the Service Management Boundary including:

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

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

4.2.3 managing identities of Users.

4.3 BT does not make any representations or warranties, whether express or implied, as to any outcomes of Automated IOC Blocking undertaken as part of the Eagle-I Enhanced Firewall Service Option, including but not limited to any reduction in security incidents or to the threat impact on any Customer Equipment or your wider Network.

5 Enabling Services

5.1 You will ensure the Agile Connect Service ("**Enabling Service**") is in place as this is a requirement for the provision of the Service.

5.2 The Enabling Service is subject to separate terms and conditions and this Schedule will not apply to the Enabling Service.

6 Specific Terms

6.1 **Service Constraints**

6.1.1 BT does not warrant that:

(a) the Service is error free;

(b) the Service will detect all security or malicious code threats; or

(c) that use of the Service will keep your network or computer systems free from all viruses or other malicious or unwanted content or safe from intrusions or other security breaches.

6.1.2 You will be responsible for results obtained from the use of the Service, and for conclusions drawn from such use.

6.1.3 BT will not be liable for any damage or Claims caused by errors or omissions in any information, instructions or scripts provided to BT by you in connection with the Service, or any actions taken by BT at your direction.

6.1.4 In respect of the Firewall Anti-Virus Service Option, the executable file that is being inspected is subject to a maximum file size of 10 per cent of the available RAM allocated to the Virtual Firewall and up to a maximum limit of 1.6GB.

6.1.5 The Service may not be available in all locations.

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

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

6.1.8 The period over which data can be analysed is dependent on the number of events occurring on the Virtual Firewall and logged by the Virtual Firewall.

6.2 Termination of the Agile Connect Service

6.2.1 Where the Agile Connect Service is terminated for any reason:

(a) the Service will terminate automatically; and

(b) where termination is by you in accordance with Clause 17 of the General Terms, you will pay the Termination Charges as set out in Paragraph 9.5 of the Schedule.

6.2.2 You will notify BT immediately if the Agile Connect Service is terminated and if you do not do so, BT may continue to charge you in accordance with Paragraph 9.5 of the Schedule.

6.3 Amendments to the BT Managed Security Service Schedule

6.3.1 The wording in Paragraph 9.5.2 of the Schedule is deleted and replaced with the following:

9.5.2 In addition to the Charges set out at Paragraph 9.5.1 above, if you terminate the Service during the Minimum Period of Service or any Renewal Period, you will pay BT:

(a) three months applicable Recurring Charges; and

(b) any fees, charges, or costs paid by BT to a supplier than cannot be recovered from the supplier.

Part B – Service Delivery and Management

10 BT's Obligations

10.1 **During Operation**

10.1.1 On and from the Service Start Date, BT will use secure protocols or a secure management link to connect to the Virtual Firewall via the Internet or other agreed network connection, in order to monitor the Service proactively and to assist in Incident diagnosis.

10.1.2 where the Eagle-I Enhanced Firewall Service Option is specified, BT will implement any changes as part of Automated IOC Blocking as quickly as is technically practicable.

10.2 **The End of the Service**

On termination of the Service by either of us, BT will:

10.2.1 terminate any rights of access to the Security Portal and stop providing all other elements of the Service; and

10.2.2 where requested in writing prior to the termination of this Contract, provide, where reasonably practical, information relating to the Service in a format that BT reasonably specifies.

11 Your Obligations

11.1 **Service Delivery**

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

11.1.1 provide BT with the WAN/LAN IPI Address to enable BT to manage the Virtual Firewall;

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

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

11.1.4 ensure that Virtual Firewalls are able, in accordance with BT's instructions provided to you by BT, to receive updates, such as vulnerability signatures, directly over the Internet, or over an alternative path agreed with BT for that purpose; and

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

11.2 **During Operation**

On and from the Service Start Date, you will:

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

11.3 **The End of the Service**

On termination of the Service by either of us, you will promptly return or delete any confidential information that you have received from BT during the term of the Contract.

Part C – Service Levels

12 On Time Delivery

12.1 The On-Time Delivery Service Level set out in the Schedule does not apply to access to the reports made available via the Security Portal or the ability to request CSP changes via the Security Portal.

Part D – Defined Terms

13 Defined Terms

In addition to the defined terms in the General Terms and the Schedule, 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 and the Schedule, 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 and the Schedule. This is to make it easier for you to find the definitions when reading this Annex.

"**Ad Hoc Professional Services**" has the meaning given in Paragraph 3.4.

"Agile Connect Service" means the BT service that provides an overlay network solution service that will allow customers to remotely manage their own virtual, global network, enabling customers to automatically route and optimise network traffic and gain visibility of the performance of certain applications using a portal.

"**Automated IOC Blocking**" has the meaning given in Paragraph 3.5(b)(i)

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

"**BT Managed Security Service Schedule**" means a range of graded security management services which can be used in association with, and as an overlay to the Service.

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

"**Eagle-I Enhanced Firewall Service**" means the Service Option specified at Paragraph 3.5.

"**Eagle-I Platform**" means the solution through which BT shall identify IOCs.

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

"**Existing Blocklist Enhancement**" has the meaning given in Paragraph 3.5(a)(ii).

"**Firewall Anti-Bot**" has the meaning given in Paragraph 3.3.

"**Firewall Anti-Virus**" has the meaning given in Paragraph 3.2.

"**Firewall URL Filtering and Application Control**" has the meaning given in Paragraph 3.1.

"**General Terms**" means the general terms to which the Schedule and this Annex are attached or can be found at www.bt.com/terms, and that form part of the Contract.

"**Image**" means a valid KVM qcow2 software image of the Virtual Firewall.

"**IOCs**" or "**Indicators of Compromise**" has the meaning given in Paragraph 3.5(a)(i).

"**Managed Virtual Firewall Security Fortinet with Agile Connect Service**" or "**Service**" has the meaning given in Paragraph 1.

"**RAM**" means random access memory.

"**Schedule**" means the BT Managed Security Service Schedule to the General Terms.

"**Service Management Boundary**" has the meaning given in Paragraph 4.

"**Service Options**" has the meaning given in Paragraph 3.

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

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

"**Virtual Firewall**" means a software based network security system that uses rules to control incoming and outgoing network traffic.

"**WAN**" means wide area network.