



BT Managed Fortinet SD-WAN

Annex to the Managed Service Schedule

Contents

A note on 'you'	2
Words defined in the General Terms and the Schedule	2
Part A – The Fortinet Service	2
1 Service Summary.....	2
2 Standard Service Components	2
3 Service Options	4
4 Service Management Boundary	5
5 Associated Services and Third Parties	5
6 Equipment.....	6
7 Specific Terms.....	7
Part B – Service Delivery and Management	9
8 Your Obligations.....	9
9 Notification of Incidents.....	10
Part C – Service Levels	11
10 Service Levels.....	11
Part D – Defined Terms	12
11 Defined Terms	12



A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the General Terms and the 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 Schedule.

Part A – The Fortinet Service

1 Service Summary

BT will provide you with managed network solution that will allow you to manage your virtual network comprising:

- 1.1 the Standard Service Components; and
- 1.2 any of the Service Options as set out in any applicable Order, up to the point of the Service Management Boundary as set out in Paragraph 4 ("**Fortinet Service**").
- 1.3 The Fortinet Service must be purchased under Managed Service and is subject to the Schedule to the General Terms.
- 1.4 For the purposes of the Schedule the Fortinet Service is an Associated Service.

2 Standard Service Components

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

2.1 SD-WAN Devices

- 2.1.1 BT will provide you with SD-WAN Devices including requisite Software licences for the SD-WAN Device as detailed in the Order.
- 2.1.2 Where BT provides you with Physical SD-WAN CPE Devices, BT will install these at your Sites and they will connect into your network in order that BT can provide you with the Fortinet Service.
- 2.1.3 Where you have selected a Virtual SD-WAN Device BT will provide you with the Licence Subscription required to run the Fortinet Service and you will install the Software on your Virtual Environment.
- 2.1.4 You will purchase a Licence Subscription for each of your SD-WAN Devices as set out in Paragraph 2.6.
- 2.1.5 Any maintenance of the SD-WAN Device will be in line with the Maintenance Care Level you select in the Order.

2.2 Cloud Hosted Control Infrastructure

- 2.2.1 BT will provide a cloud hosted management infrastructure that will allow BT to:
 - (a) orchestrate the delivery of your Fortinet Service;
 - (b) monitor in real time your network and the performance of the SD-WAN Devices;
 - (c) identify issues, inefficiencies or delays with your network;
 - (d) troubleshoot issues with your network; and
 - (e) view data flows across your network and Sites,("Cloud Hosted Control Infrastructure").

2.3 Cloud Hosted Report Infrastructure

- 2.3.1 BT will provide you with access to the Managed Service Portal that will allow you to:
 - (a) view, in real time, the performance of your applications that run over your network;
 - (b) identify issues, inefficiencies or delays with your network;
 - (c) troubleshoot issues with your network; and
 - (d) view data flows across your network and Sites;("Cloud Hosted Report Infrastructure").
- 2.3.2 BT will not provide training on the Managed Service Portal as part of the Fortinet Service.

2.4 Transport Independent VPN

- 2.4.1 BT will provide you with a VPN and encryption service that will allow you to:
 - (a) build corporate VPNs across your Sites; and
 - (b) transfer information securely across your network and the Internet using encryption technology,("Transport Independent VPN").

2.5 Application Aware Routing



- 2.5.1 BT will provide you with a facility that manages your traffic and Applications in order to improve the efficiency of your network ("**Application Aware Routing**").
- 2.5.2 You will be able to categorise certain Applications as business critical through your own pre-defined categories, as agreed between us, and BT will implement these for you through the BT Hosted Control Infrastructure.
- 2.5.3 Any changes to the categories will be dealt with as a Simple Service Request.
- 2.5.4 Application Aware Routing will work optimally if there are two Enabling Services connected to your Sites.
- 2.6 **Licence Subscriptions**
 - 2.6.1 You will purchase at least one of the Licence Subscriptions below for each SD-WAN Device as set out in the applicable Order. Where there are multiple SD-WAN Devices on a Site, they will all have the same Licence Subscription, but Licence Subscriptions may vary across the network:
 - (a) Standard Licence Subscription
 - (i) The Standard Licence Subscription aligns with the technical features supported by the Supplier as detailed in the Order.
 - (b) Virtual Licence Subscription
 - (i) The Virtual Licence Subscription that is used in your Virtual Environment includes all features provided as part of the Standard Licence Subscription;
 - (ii) You may modify the number of virtual CPUs, in the set range, that you need for your virtual instance by raising a change request order to BT;
 - (iii) You may raise a change request and this will be effective only where reasonable lead-times apply after your acceptance;
 - (iv) BT will work with you to check and validate the request before it is effective;
 - (v) You may change the number of virtual CPUs at any time subject to not less than 30 days notice; and
 - (vi) The Virtual Licence Subscription monthly charge will vary by the number of virtual CPUs and the selected Security Licence Subscription.
- 2.7 **Security Licence Subscription**
 - 2.7.1 The Security Licence Subscription will be included with the Standard Licence Subscription if you order the Physical SD-WAN CPE Device; and
 - 2.7.2 If you order the Virtual Licence Subscription for your Virtual SD-WAN Device to be deployed in your own Virtual Environment, you have the option to opt-in or opt-out of BT's Security Licence Subscription.
- 2.8 **Customer Portal**
 - 2.8.1 BT will provide you with a customer portal accessible via the Managed Service Portal, that will allow you to monitor your network status and generate reports ("**Customer Portal**").
 - 2.8.2 BT will not provide training on the Customer Portal as part of the Fortinet Service.
- 2.9 **Co-Managed Service ('CMS') - Self-Service**
 - 2.9.1 BT will grant you right to access and use the Co-Managed Service ('CMS') - Self Service, where you can either:
 - (a) configure service settings into your Service; or
 - (b) raise a Simple Service Request (SSR) for BT to configure your service settings for you.
 - 2.9.2 BT will provide you a maximum of 5 User Accounts for the CMS Portal and Nominated Users will be able to configure service settings for your Service.
 - 2.9.3 You will be responsible for ensuring that the Nominated Users keep the User Login Credentials confidential and secure and not disclose or share these User Login Credentials.
 - 2.9.4 You shall notify BT immediately if a Nominated User ceases to be authorised by you, including where they leave your organisation, so that BT can revoke that User's access to the CMS Portal.
 - 2.9.5 BT will not be liable for any security breach arising out of your misconfiguration, misuse of User Login Credentials or amendment of the set profiles. Any configuration applied by your Nominated User(s) will be treated as your action. You will be responsible for the impact of implementing the changes and BT will not be liable for any losses or consequences arising from this action, including but not limited to any performance issues or outages to your Service.
 - 2.9.6 You shall not configure any service settings that impacts BT's ability to provide the Service, any such action will result in the revocation of the Nominated User(s) access without advance notice.
 - 2.9.7 The Service Levels described in Part C of the Schedule will not apply if an Incident was a result of you implementing changes to your configuration as part of the CMS – Self Service.
 - 2.9.8 Where an Incident has arisen as a result of you implementing a change on the CMS Portal and you need BT to provide assistance to resolve it, BT will use reasonable effort to resolve such Incident and reserves the right to apply additional charges for any corrective action and the resolution of the Incident.



- 2.9.9 In addition to other rights, BT reserves the right to remove access to the CMS at any time without liability, by giving you at least 30 days' notice.

3 Service Options

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 LAN CPE Devices

- 3.1.1 BT will provide you with LAN CPE Devices including LAN CPE Switches and LAN CPE Wi-Fi Access Points and the requisite Software licences for the LAN CPE Device as detailed in the Order, which BT will install at your Sites and that will connect into your network in order that BT can provide you with the ordered service.

3.2 Mobile Data Access

- 3.2.1 BT will provide you with Mobile Data Access, using one of the Service Options below, if set out in the Order:
- (a) Backup Mobile Data Access; or
 - (b) Backup Plus Mobile Data Access;
 - (c) Active-Active Mobile Data Access; or
 - (d) Prime Mobile Data Access.
- 3.2.2 The Mobile Data Access you select can be either BT Managed Mobile Data Access or Customer Managed Mobile Data Access.
- 3.2.3 Mobile Data Access can be purchased in one of the following variants:
- (a) BT Managed Mobile Data Access – External;
 - (b) BT Managed Mobile Data Access – Internal Hub;
 - (c) BT Managed Mobile Data Access – SIM Only (4G only – limited models);
 - (d) Your own SIM for use with Devices with embedded SIM Card (4G Only - Limited models).
- 3.2.4 Active-Active Mobile Data Access is only available over 5G where 5G is available to you.
- 3.2.5 Where you select BT Managed Mobile Data Access, BT will:
- (a) install, maintain and support the Mobile Data Equipment/SIM Card;
 - (b) hold and deploy additional Mobile Data Equipment when required; and
 - (c) remotely and proactively monitor the Mobile Data Equipment and report on any performance issues.
- 3.2.6 Where you select BT Managed Mobile Data Access – Internal Hub or BT Managed Mobile Data Access – SIM Only, in the unlikely event of the failure of the SIM Card, a replacement SIM Card will be ordered, which can take in excess of 3 Business Days.
- 3.2.7 Where you select Customer Managed Mobile Data Access you are responsible for:
- (a) provision of the Customer SIM Card;
 - (b) any charges or fees associated with or incurred by your use of the Customer SIM Card; and
 - (c) arranging for the SIM Card to be activated prior to the day of installation.
- 3.2.8 BT or one of its suppliers, will retain title in the Mobile Data Equipment which will be classified as BT Equipment under this Contract, except as set out in Paragraph 3.2.11
- 3.2.9 BT grants you a licence to use the Mobile Data Equipment and SIM Card solely for accessing the Mobile Network in accordance with this Contract during the Minimum Period of Service and any Renewal Periods.
- 3.2.10 Upon termination or expiry of this Contract for any reason, or where the Mobile Data Equipment is no longer required or is faulty, BT will, at its option, collect the Mobile Data Equipment or ask you to return it to BT at your expense, except as set out in Paragraph 3.2.11
- 3.2.11 Upon termination or expiry of this Contract, the title in Physical SD-WAN CPE Devices, including the Internal Hub, transfers to you and you are responsible for their disposal as set out in Paragraph 6.5
- 3.2.12 Mobile Data Access provides access across a public Mobile Network which can be subject to degradation, congestion and interference (including lack of access to 5G) which are beyond BT's control.
- 3.2.13 Where you have selected Customer Managed Mobile Data Access BT will not be responsible for any problems with the signal strength or quality or with any access to the Fortinet Service using Mobile Data Access.
- 3.2.14 In addition to any rights BT may have under Clause 18 of the General Terms, if you use the Mobile Data Access in breach of Paragraphs 8.2.7 or 8.2.8 of this Annex or Clauses 6.6 and 12.3 of the General Terms, BT may, without notice:
- (a) terminate the Mobile Data Access; or
 - (b) temporarily or permanently block the BT SIM Card used with the Mobile Data Access.
- 3.2.15 Issues identified with Mobile Network connectivity, between the Site and the local cell tower, may take in excess of 5 Business Days to resolve.



3.3 Cloud Deployment

Where you have selected Cloud Deployment, BT will enable you to activate the Virtual SD-WAN Device in your Virtual Environment as part of the Fortinet Service if set out in the Order.

3.4 Fortinet Security Options

3.4.1 BT will enable certain security features on your SD-WAN Device as part of your licence subscription as set out in Paragraph 2.6.

3.4.2 The Fortinet Security Options will be configured in accordance with the design agreed with you with applicable Licence Subscriptions and you can monitor the performance of them via the Customer Portal however, as standard, we do not proactively take any action on security alerts received.

3.4.3 A full list of available Fortinet Security Options will be set out in the service description.

3.5 Service Options may not be available in all countries.

3.6 Protective Monitoring Service

3.6.1 Where you have selected the Protective Monitoring Service option, BT will provide you with a Protective Monitoring Service ("PMS") that provides 24/7 monitoring of High and Critical Security Events.

3.6.2 To select PMS, you will need to opt into the Security Licence Subscription and enable logging functionality. To obtain the best quality, you will have to enable and configure secure socket layer inspection.

3.6.3 BT will notify you of any required remedial action and engage BT Service Management to action pre-defined playbooks (agreed with you) where applicable. You and/or BT Service Management may be responsible for carrying out remedial action.

4 Service Management Boundary

4.1 BT will provide and manage the Fortinet Service in accordance with Parts A, B and C of this Annex and as set out in any applicable Order:

4.1.1 in respect of the Physical SD-WAN CPE Devices, between the WAN and LAN ports of each Physical SD-WAN CPE Device and excluding any Customer SIM Card;

4.1.2 in respect of the Virtual SD-WAN Device, within the Virtual SD-WAN Device hosted on the Enabling Service but not any underlying virtual or physical infrastructure supporting this, including an Enabling Service;

4.1.3 in respect of the LAN CPE Switches between the WAN and LAN ports of each LAN CPE Device; and

4.1.4 in respect of the LAN CPE Wi-Fi Access Point, between the LAN port and the Wi-Fi antennae.

("Service Management Boundary").

4.2 BT will have no responsibility for the Fortinet Service outside the Service Management Boundary, including access using the Customer Managed Mobile Data Access.

4.3 BT does not make any representations, whether express or implied, about whether the Fortinet Service will operate in combination with any Customer Equipment, including the Customer SIM Card, or other equipment and software that is not provided by BT.

4.4 BT will have no responsibility under this Contract for any of the Enabling Services, including the Enabling Service that the Virtual SD-WAN Device is hosted on.

4.5 BT will provide the Fortinet Service in the locations set out in the Order. If you allow Users, or otherwise configure or permit the configuration of the Fortinet 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 Fortinet Service. Any use of the Fortinet 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.

5 Associated Services and Third Parties

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

5.1.1 You will have resilient internet routing connectivity from the SD-WAN CPE Devices to the BT Hosted Control Infrastructure which is necessary for the Fortinet Service to function, including any necessary configuration through your firewalls; and

5.1.2 one or more of the following connectivity services:

(a) a BT Internet service;

(b) a BT MPLS service;

(c) a BT Ethernet service;

(d) your own or third party provided WAN that BT has confirmed to you in writing is compatible with the Fortinet Service,



(each an “Enabling Service”)

- 5.2 If BT provides you with any services other than the Fortinet Service (including, but not limited to any Enabling Service) this Annex will not apply to those services and those services will be governed by their separate terms.
- 5.3 BT will not be liable for failure to or delay in supplying the Fortinet Service if another supplier delays or refuses the supply of an electronic communications service to us and no alternative service is available at reasonable cost.
- 5.4 Where the SD-WAN Device is directly deployed onto an Enabling Service set out in Paragraph 5.1.2 without a separate WAN router or NTE, any functionality of Enabling Service is determined only by the capability of the Fortinet Service and you acknowledge this may result in a decreased functionality of such Enabling Service.

6 Equipment

6.1 Use of BT Equipment

In relation to BT Equipment you will:

- 6.1.1 keep the BT Equipment safe and without risk to health;
- 6.1.2 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;
- 6.1.3 not move the BT Equipment or any part of it from the Site(s) without BT’s written consent and you will pay BT’s costs and expenses reasonably incurred as a result of such move or relocation;
- 6.1.4 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 its consent, agree that any alterations or attachments are part of the BT Equipment;
- 6.1.5 not sell, charge, assign, transfer or dispose of (except as set out in Paragraph 6.5) or part with possession of the BT Equipment or any part of it;
- 6.1.6 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;
- 6.1.7 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);
- 6.1.8 obtain appropriate insurance against any damage to or theft or loss of the BT Equipment;
- 6.1.9 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;
- 6.1.10 ensure that the BT Equipment appears in BT’s name in your accounting books;
- 6.1.11 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
- 6.1.12 notify any interested third parties that BT owns the BT Equipment.

6.2 Ownership and Risk of BT Equipment

BT Equipment will remain BT’s property at all times and risk in BT Equipment will pass to you upon delivery, whether or not the BT Equipment has been installed.

6.3 Security

- 6.3.1 You are responsible for the proper use of any user names, personal identification numbers and passwords used with the BT Equipment or the Fortinet Service, and you will take all necessary steps to ensure that they are kept confidential, secure and not made available to unauthorised persons.
- 6.3.2 BT does not guarantee the security of the BT Equipment against unauthorised or unlawful access or use.
- 6.3.3 You agree that you will promptly terminate access of any person who is no longer an authorized individual User, and you will promptly inform BT if an individual User’s 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. You further agree to change any or all passwords or other systems administration information used in connection with the Fortinet Service if BT asks you to do so in order to help safeguard ensure the security or integrity of the Fortinet Service.
- 6.3.4 You acknowledge and agree that deployment using Cloud Deployment will result in the creation of a number of default security components on your Enabling Service where applicable.

6.4 Software Licence

On and from the Service Start Date, you will comply with the provisions of any Software licences provided with or as part of any BT Equipment, including SD-WAN Devices.

6.5 WEEE Directive



- 6.5.1 Subject to Paragraph 6.5.4, you are responsible under Article 13 of the Waste Electrical and Electronic Equipment Directive 2012/19/EU ("WEEE Directive") for the costs of collection, treatment, recovery, recycling and environmentally sound disposal of any equipment supplied under the Contract, including BT Equipment, which has become waste electrical and electronic equipment ("WEEE").
- 6.5.2 For the purposes of Article 13 of the WEEE Directive this Paragraph 6.5 is an alternative arrangement to finance the collection, treatment, recovery, recycling and environmentally sound disposal of WEEE.
- 6.5.3 You will comply with any information recording or reporting obligations imposed by the WEEE Directive.
- 6.5.4 Mobile Data Equipment is excluded from the obligations set out in this Paragraph 6.5 and shall be returned to BT in accordance with Paragraph 3.2.10

7 Specific Terms

7.1 EULA and Supplier Terms

- 7.1.1 You hereby agree to the terms of the end user licence agreement with the Supplier in the form set out at: <http://www.fortinet.com/doc/legal/EULA.pdf> as may be amended or supplemented from time to time by the Supplier ("EULA").
- 7.1.2 You will ensure that your Users also comply with the terms of the EULA.
- 7.1.3 You will observe and comply with the EULA for all any use of the applicable Software.
- 7.1.4 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 Fortinet Service upon reasonable Notice, and:
 - (a) you will continue to pay the Charges for the Fortinet Service until the end of the Minimum Period of Service; and
 - (b) BT may charge a re-installation fee to re-start the Fortinet Service.
- 7.1.5 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.
- 7.1.6 Where the EULA are 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.

7.2 Use of Telemetry Data

- 7.2.1 BT or its Supplier may, for the purposes set out in Paragraph 7.2.2, collect Telemetry Data which includes such items as:
 - (a) system statistics (for example, CPU, memory);
 - (b) interface statistics;
 - (c) flow statistics including application and application family; and
 - (d) device configurations and usage per interface.
- 7.2.2 Notwithstanding anything to the contrary in this Contract, BT and its Supplier shall only use Telemetry Data as follows:
 - (a) to deliver and maintain the Fortinet Service;
 - (b) for the Supplier to provide support to BT (for example, by providing BT with recommendations for WAN configuration optimisation, licence expiration, renewal notices, licence or bandwidth enforcement); and
 - (c) the Supplier may use Statistical Data for the general purpose of improving its SD-WAN product and other product offerings, including customer experience and use of such product in the context of generally available software feature releases.

7.3 Export of Content using Cloud Services

- 7.3.1 The Fortinet Service comprises of a cloud service that utilises software and technology that may be subject to export control laws of various countries. You are solely responsible for any compliance related to the way you use the Fortinet Service and the location the Fortinet Service is used including access by Users to the Fortinet Service and for your Content transferred or processed using the Fortinet Service, including any publication of such Content.
- 7.3.2 You will indemnify BT against all Claims, losses, costs or liabilities brought against BT as a result of, or arising out of or in connection with, your non-compliance with any laws (including sanctions and export control laws) of any country you use, access or transfer Content to.

7.4 Charges on termination of the Fortinet Service

- 7.4.1 In addition to the Charges set out in the Managed Services Schedule, if you terminate the Fortinet Service before the end of the Minimum Period of Service or Renewal Period, you will pay BT Termination Charges for any parts of the Fortinet Service that were terminated during the Minimum Period of Service or Renewal Period, equal to:
 - (a) 100 per cent of the Recurring Charges applicable to the Fortinet Service, where any Licence Subscription has been ordered, including the Charges for the Managed Service, for any remaining months of the first 12 months of the Minimum Period of Service or Renewal Period (if terminated within the first 12 months of a Minimum Period of Service or Renewal Period);



- (b) in respect of the Recurring Charges for the Licence Subscriptions applicable or ordered as part of the Fortinet Service, 100 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service or Renewal Period after the first 12 months of such period; and
- (c) 100 per cent of the Recurring Charges in respect of the maintenance provided as part of the Fortinet Service, for any remaining months of the Minimum Period of Service or Renewal Period.

7.5 **Changes to the Fortinet Service as a result of changes to laws or regulations**

- 7.5.1 BT reserves the full right to change or withdraw the Fortinet Service or any applicable part of the Fortinet Service at any time as a result of either changes to applicable laws or regulations or changes to the interpretation of the applicable laws and regulation.

7.6 **Use of the Fortinet Service**

- 7.6.1 Unless agreed in writing with BT:
 - (a) the Customer will only use the Fortinet Service for the commercial and business purposes for which they have been designed; and
 - (b) the Customer will not modify, amend, change, reconfigure or otherwise repurpose all or any part of the Fortinet Service for uses other than those pursuant to paragraph 7.6.1(a) above.



Part B – Service Delivery and Management

8 Your Obligations

8.1 Service Delivery

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

- 8.1.1 not act to misuse the Fortinet Service to contravene or circumvent Applicable Law. BT will treat any such contravention as a material breach and as such BT may:
 - (a) suspend the Fortinet Service and BT can refuse to restore the Fortinet Service until BT receives an acceptable assurance from you that there will be no further contravention or circumvention; or
 - (b) terminate the Fortinet Service upon written notice;
- 8.1.2 prepare and maintain the Site(s) for the installation of BT Equipment and supply of the Fortinet Service, including:
 - (a) providing a suitable and safe operational environment for any BT Equipment including all necessary trunking, conduits, cable trays, and telecommunications connection points in accordance with BT's reasonable instructions and applicable installation standards;
 - (b) taking up or removing any fitted or fixed floor coverings, ceiling tiles and partition covers or provide any openings in buildings required to connect BT Equipment to appropriate network facilities in time to allow BT to undertake any necessary installation or maintenance of the Fortinet Service;
 - (c) carrying out any work that may be required after installation to make good any cosmetic damage caused during installation or maintenance;
 - (d) providing a secure, continuous power supply at the Site(s) for the operation and maintenance of the Fortinet Service and BT Equipment at such points and with such connections as BT specifies, and, in order to mitigate any interruption to the Fortinet Service resulting from failure in the principal power supply, provide back-up power with sufficient capacity to conform to the standby requirements of the applicable standards;
 - (e) providing internal cabling between the BT Equipment and any Customer Equipment, as appropriate; and
 - (f) where you have selected BT Managed Mobile Data Access – Internal Hub, - provide mains power for the power adapter.

8.2 During Operation

On and from the Service Start Date, you will:

- 8.2.1 ensure that Users do not raise as Incidents any general or training queries concerning the data made visible on the Managed Service Portal as the Service Desk will not provide such support or training;
- 8.2.2 ensure that any Customer Equipment that is connected to the Fortinet Service or that you use, directly or indirectly, in relation to the Fortinet Service is connected using the applicable BT Network termination point, unless you have BT's permission to connect by another means;
- 8.2.3 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment does not meet any relevant instructions, standards or Applicable Law;
- 8.2.4 not allow any User licence to be used by more than one individual User unless it has been reassigned in its entirety to another individual User, in which case you will ensure the prior User will no longer have any right to access or use the Fortinet Service;
- 8.2.5 comply with Paragraph 9 before reporting Incidents;
- 8.2.6 inform BT of any planned works on any third party provided Enabling Service;
- 8.2.7 where you have BT Managed Mobile Data Access, only use Backup Mobile Data Access if your Enabling Service fails and Backup Plus Mobile Data Access in the period before BT connects the Fortinet Service to the Enabling Service;
- 8.2.8 not remove the BT SIM Card from the Mobile Data Equipment;
- 8.2.9 be responsible for any charges incurred from use of the Customer SIM Card;
- 8.2.10 ensure that after deployment using Cloud Deployment you ensure the configuration remains compliant to your own security standards; and
- 8.2.11 you agree that:
 - (a) BT will not be liable for failure to supply or delay in supplying the Fortinet 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 Fortinet Service to you on an "as is" and "as available" basis. BT does not guarantee that the Fortinet Service:
 - (i) will be performed error-free, without Incident or interruption or that BT will correct all errors in the Fortinet 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 Annex, will meet your requirements;
 - (iv) will detect, intercept or block all malware or malicious threats
- (c) BT will not be liable in the event that software updates from the supplier used to identify and control your network traffic (including malware signatures, URL categories or application definitions) contain errors or omissions, beyond making appropriate corrections (where reasonably possible) as soon as reasonably practical;
- (d) you will own all right, title and interest in and to all of your information and will have sole responsibility for the legality, reliability, integrity, accuracy and quality of any of your information; and
- (e) you will be responsible for results obtained from the use of the Fortinet 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 Fortinet Service, or any actions taken by BT at your direction.

8.3 The End of the Service

On expiry or termination of the Fortinet Service by either of us, you will:

- 8.3.1 provide BT with all reasonable assistance necessary to remove Mobile Data Equipment from the Site(s);
- 8.3.2 disconnect any Customer Equipment from Mobile Data Equipment located at the Site(s);
- 8.3.3 not dispose of or use the Mobile Data Equipment other than in accordance with BT's written instructions or authorisation;
- 8.3.4 if required in accordance with Paragraph 3.2.10 arrange for any Mobile Data Equipment located at the Site(s) to be returned to BT;
- 8.3.5 be liable for any reasonable costs of recovery that BT incurs in recovering the Mobile Data Equipment;
- 8.3.6 promptly return or delete any confidential information that you have received from BT during the term of the Contract; and
- 8.3.7 comply with your obligations set out in Paragraph 6.5 in relation to disposal of equipment, including BT Equipment.

9 Notification of Incidents

- 9.1 You will report Incidents in accordance with the process set out in the Schedule.
- 9.2 Where you have selected Customer Managed Mobile Data Access:
 - 9.2.1 you will ensure and confirm to BT that the Incident is not the result of the Mobile Data Access failing before reporting Incidents to BT;
 - 9.2.2 BT will not be liable for any delay in rectifying an Incident where the Incident has been caused by the Mobile Data Access;
 - 9.2.3 and you have provided your own- or third-party WAN Enabling Service as set out in Paragraph 5.1.2(d), you will ensure and confirm to BT that the service is working correctly. Without such confirmation you cannot report Incidents to BT; and
 - 9.2.4 BT will not be liable for any delay in rectifying an Incident where BT has been unable to connect to the SD-WAN Device.



10 Service Levels

Service Levels and Service Credits do not apply to the Fortinet Service. Any service levels that apply to the Enabling Services will be set out in the terms associated with such Enabling Service.



Part D – Defined Terms

11 Defined Terms

In addition to the defined terms in the General Terms and in the 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 or the 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 and in the Schedule to the General Terms. This is to make it easier for you to find the definitions when reading this Annex, if there are any conflicts in these definitions the ones in the original documents will take precedence.

“Active-Active Mobile Data Access” is a Service Option that allows an additional connection via the 5G Mobile Network using either one of the Mobile Data Equipment or Customer SIM Card, as applicable, to allow use of the MM SD-WAN Service including for backup purposes or prior to installation and connection with an Enabling Service.

“Application” means a programme or software.

“Application Aware Routing” has the meaning given in Paragraph 2.5.1.

“AWS” means Amazon Web Services and is a subsidiary of Amazon that provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis.

“Azure” means Microsoft Azure, a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centres.

“Backup Mobile Data Access” is a Service Option and means a resilient service that in the event any element of your Enabling Service fails (other than Backup Mobile Data Access), will use the Mobile Data Equipment or Customer SIM Card (as applicable) to automatically connect to the Mobile Network to allow continued use of the Fortinet Service until the Enabling Service is restored.

“Backup Plus Mobile Data Access” is a Service Option and includes the service described in Backup Mobile Data Access and in addition allows you to use the Mobile Data Equipment or Customer SIM Card (as applicable) to connect to the Mobile Network to allow use of the MM SD-WAN Service prior to installation and connection with the Enabling Service.

“BT Managed Mobile Data Access” means the provision of Mobile Data Access using the Mobile Data Equipment.

“BT Managed Mobile Data Access – External” means a service consisting of an external antenna which is attached to the outside of your premises and cabled back to the comms room.

“BT Managed Mobile Data Access – Internal Hub” means a 4G/5G device supplied by BT with a SIM Card which enables connection to the Mobile Network to provide internet access. Internal Hub is connected to the SD-WAN controller WAN port via an Ethernet connection.

BT Managed Mobile Data – SIM Only” means a SIM card which can be inserted into supporting devices, and which will provide access via the 4G network.

“BT SIM Card” means a card, provided by BT, or one of its suppliers, that is inserted into the router of the Mobile Data Equipment and that is used to connect to the Mobile Network and is BT Equipment.

“Cloud Hosted Control Infrastructure” has the meaning given in Paragraph 2.2.11.

“Cloud Hosted Report Infrastructure” has the meaning given in Paragraph 2.3.1.

“Cloud Deployment” means a software for deploying the Virtual SD-WAN Device into the Virtual Environment as part of the Fortinet Service.

“Content” means applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material uploaded or used in connection with the Fortinet Service.

“Customer Equipment” means any equipment and any software, other than BT Equipment, used by you in connection with the Fortinet Service.

“Customer Managed Mobile Data Access” means the provision of Mobile Data Access using the Customer SIM Card.

“Customer Portal” has the meaning given in Paragraph 2.8.

“Customer SIM Card” means a card, provided by you, that is inserted into the Physical SD-WAN CPE Device and that is used to connect to the Mobile Network and is Customer Equipment.

“Device” means any mobile handset, laptop, tablet or other item of handheld equipment, including all peripherals, excluding SIM Cards and applications, which are in scope of the Fortinet Service, as set out in the Order.

“Fortinet Security Options” means a UTP that can be applied to your SD-WAN Device.

“Fortinet Service” has the meaning given in Paragraph 1.

“Google Cloud Platform” or **“GCP”**, offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products.

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

“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.

“Kernel-based Virtual Machine” or **“KVM”** is a virtualization module in the Linux kernel that allows the kernel to function as a hypervisor.

“LAN CPE Device” means either the LAN CPE Switch or the LAN CPE Wi-Fi Access Point and is for the purposes of the Schedule.

“LAN CPE Switch” means hardware that connects to the local cabling within your Site to create a local area network by cross connecting network devices.



"LAN CPE Wi-Fi Access Point" means a hardware device that connects to the LAN and broadcasts the network signal for wireless Devices to connect to.

"Licence Subscription" means either the Standard Licence Subscription or Virtual Licence Subscription or the Security Licence Subscription.

"Local Area Network" or **"LAN"** means the infrastructure that enables the ability to transfer IP services within Site(s) (including data, voice and video conferencing services).

"Maintenance Care Level" means the maintenance option you select in the Order as more fully described in the Schedule.

"Managed Service" has the meaning given to it in the Schedule.

"Managed Service Portal" has the meaning given to it in the Schedule.

"Microsoft Hyper-V" means a native hypervisor, that can create virtual machines on x86-64 systems running Windows.

"Mobile Data Access" means a UK only Service of one or a combination of Active-Active Mobile Data Access, Backup Mobile Data Access or Backup Plus Mobile Data Access.

"Mobile Data Equipment" means a business grade router, antenna, BT SIM Card, cabling and any other ancillary equipment if specified in the Order that is provided as part of the BT Managed Mobile Data Access and is BT Equipment for the purposes of this Schedule and MS Equipment for the purposes of the Schedule.

"Mobile Network" means a 5G or 4G communication network (4G where 5G is not available and 3G where 4G is not available) where the last link is wireless.

"Nominated User" means any User(s) that you notify BT of in writing as being authorised to implement configuration changes to the Service under the CMS Self-Service option.

"Oracle Cloud" is a cloud computing service offered by Oracle Corporation providing servers, storage, network, applications and services through a global network of Oracle Corporation managed data centers. The company allows these services to be provisioned on demand over the Internet.

"Physical SD-WAN CPE Device" means hardware, and associated software, that connects to your network and provides a secure overlay network over a mix of WAN transports and that is BT Equipment for the purposes of this Contract. "

"Prime Mobile Data Access" means a Service Option that allows connection to the Mobile Network using either the Mobile Data Equipment or Customer SIM Card, as applicable, to allow use of the Fortinet Service as a sole Enabling Service.

"Protective Monitoring Service" or **"PMS"** means the process of monitoring activity on a network, with a view to identifying potentially malicious behaviours.

"Schedule" means the Managed Service Schedule to the General Terms that this Annex is appended to which details the management services that can apply to the Fortinet Service.

"SD-WAN Device" means either a Physical SD-WAN CPE Device or a Virtual SD-WAN Device.

"Security Events" means the events described in the following link:
<https://docs.fortinet.com/document/fortianalyzer/7.4.0/administration-guide/778986/predefined-event-handlers>

"Service Desk" has the meaning given to it in the Schedule.

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

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

"SIM Card" means a card that is inserted into the router of the Mobile Data Equipment and that is used to connect to the Mobile Network.

"Simple Service Request" or **"SSR"** has the meaning given to it in the Schedule.

"Site" means a location at which the Fortinet Service is provided.

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

"Supplier" means Fortinet UK Limited, address: Gainsborough House 2 Manor Park, Manor Farm Road, Reading, Berkshire, RG2 0NA and any group or parent company of the Supplier.

"Security Licence Subscription" means the Supplier's UTP where set out in any applicable Order.

"Standard Licence Subscription" means a type of licence for the Physical SD-WAN CPE Device, purchased for a fixed term.

"Statistical Data" means any information or data that the Supplier derives from customer data or Telemetry Data, provided that such information or data is aggregated or de-identified such that it cannot reasonably be used to identify an individual or entity.

"Telemetry Data" means information generated by instrumentation and logging systems created through the use and operation of the Fortinet Service.

"Transport Independent VPN" has the meaning given to it in Paragraph 2.4.

"User Accounts" means the accounts for Users made available to you by BT in order to access the Cloud Hosted Report Infrastructure.

"User Login Credentials" means the username and password provided by BT for the Customer to access Co-Managed Service

"Virtual CPU" means a virtual CPU also known as a virtual processor (vCPU), is a physical central processing unit (CPU) that is assigned to a virtual machine (VM).

"Virtual SD-WAN Device" means software that connects to your network and provides a secure overlay network over a mix of WAN transports and that is BT Equipment for the purposes of this Contract.

"Virtual Environment" means a private or public virtual environment with network connectivity that is not owned or managed by BT. The Virtual Environment is limited to either KVM, VMware ESXi, Microsoft Hyper-V, AWS, Azure, GCP or Oracle Cloud virtual environments respectively where the Virtual SD-WAN Device will be deployed by you. The Virtual Environment allows the Virtual SD-WAN Device to communicate with our management device in order to provide our Managed Service to you, via internet connectivity.

"Virtual Licence Subscription" means the FortiGate-VM licence activated in the Virtual Environment.



“**VPN**” means a virtual private network.

“**Unified Threat Protection**” or “**UTP**” means a Supplier security feature (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service) provided and managed by the Supplier.

“**WAN**” means Wide Area Network, the infrastructure that enables the transmission of data between Sites.

“**WEEE**” has the meaning given in Paragraph 6.5.1.

“**WEEE Directive**” has the meaning given in Paragraph 6.5.1.

“**Wi-Fi**” means a facility allowing computers, smartphones, or other Devices to connect to the Internet or communicate with one another wirelessly within a particular area.