BT Managed DDoS Security
Service Schedule

Contents

Words defined in the General Terms and Conditions

Words that are capitalised but have not been defined in the Schedule have the meanings given to them in the General Terms and Conditions.

Part A – The BT Managed DDoS Security Service

1 Service Summary

1.1 BT will provide the Customer with a service that mitigates attacks by profiling normal Internet traffic behaviour and proactively monitoring the Internet traffic routing to the Customer's Internet connection. DDoS detects floods, worm and anomalous traffic behaviour and in these circumstances and appropriate to the Service Option, BT will instigate mitigation which will permit legitimate traffic to proceed. The BT Managed DDoS Security Service is comprised of:

1.1.1 the Standard Service Components; and

1.1.2 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 (the "**BT Managed DDoS Security Service**").

1.2 The BT Managed DDoS Security Service is not available in all countries.

1.3 Where the Customer selects the BT Managed DDoS Security Service under the BT Managed Security Service:

2 Standard Service Components

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

2.1 a service that monitors the Customer's BT Internet Service in the countries that the Customer has selected the BT Managed DDoS Security Service for as set out in the Order only and alerts against DDoS Attacks;

2.2 a Service Desk for the Customer to report Incidents to;

2.3 monitoring of traffic on Managed Object(s);

2.4 investigation of anomalous traffic patterns; and

2.5 Alerts.

3 Service Options

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

3.1 **Bronze, Silver and Gold Service Options**

The specifications of the Service Options are as set out in the table below. All Service Options provide automated detection of attacks. The different Service Option levels set out in the table below will dictate the types of attacks detected.

Service Option specification	Bronze	Silver	Gold
DDoS Mitigation	Unlimited Cloud.	Unlimited Cloud.	Unlimited Cloud.
Response Time to DDoS Attack	Automated mitigation 24x7x365 – typically mitigation will be triggered within 9 minutes of attack.	Automated mitigation 24x7x365 - typically mitigation will be triggered within 9 minutes of attack.	Automated mitigation 24x7x365 - typically mitigation will be triggered within 9 minutes of attack.
Managed Object / Mitigation Template	1 x Managed Object / a Mitigation Template tailored to the Customer.	3 x Managed Object / a Mitigation Template tailored to the Customer.	5 x Managed Object / a Mitigation Template tailored to the Customer.
Alerting Service	High Alert auto email to the Customer and BT sales contacts.	High Alert auto email to the Customer and BT sales contacts.	High Alert auto email to the Customer and BT sales contacts.
Traffic reports and Alert options available via the Portal.	Yes.	Yes.	Yes.
Ability to modify reports via the Portal.	Yes.	Yes.	Yes.

Service Option specification	Bronze	Silver	Gold
Reach In / Reach out to CCO	No. Reach In limited to initial set up (Monday – Friday 09:00 to 17:00 excluding public holidays).	No Reach Out. 24x7x365 Reach In – reactive support under attack / suspected attack.	24x7x365 Reach In / Reach Out – pro-active High Alerts.
Service Requests (amendments to DDoS configurations and actions)	No.	Up to 16 service requests per annum (Mon – Fri 09:00 to 17:00 excluding public holidays).	Unlimited service requests (Mon – Fri 09:00 to 17:00 excluding public holidays).
Fast Flood (Faster detection and mitigation)	No.	Yes – mitigation time < 1min.	Yes – mitigation time < 1min.
Security ops monitoring	No.	24x7x365 monitoring.	24x7x365 pro-active monitoring.
Incident Management	Unlimited auto-mitigations.	Unlimited auto-mitigations plus manual mitigation.	Unlimited auto-mitigations plus manual mitigation.

4 Service Management Boundary

4.1 BT will provide and manage the BT Managed DDoS Security Service as set out in Parts A, B and C of this Schedule and as set out in the Order up to demarcation points as set out in the remainder of this Paragraph 4 ("**Service Management Boundary**").

4.2 For BT Managed DDoS Security Service provided as a cloud service only (with no Additional CPE), the Service Management Boundary is up to the NTU of the Access Line.

4.3 BT will have no responsibility for the BT Managed DDoS Security Service outside the Service Management Boundary.

4.4 BT does not make any representations, whether express or implied, about the interoperability between the BT Managed DDoS Security Service and any Customer Equipment.

5 BT Internet Service

5.1 The Customer will ensure that the BT Internet Service is in place as this is a requirement for the provision of the BT Managed DDoS Security Service.

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

5.3 Upon termination of the BT Internet Service:

(a) the BT Managed DDoS Security Service will terminate automatically; and

(b) where the Customer terminates the BT Internet Service in accordance with Clause 17 of the General Terms and Conditions, BT will apply the Termination Charges for BT Managed DDoS Security Service as set out in Paragraph 6.66. These Termination Charges will apply in addition to any Termination Charges applicable to the BT Internet Service.

6 Specific Terms

6.1 **Minimum Period of Service**

6.1.1 At the end of the Minimum Period of Service, unless BT or the Customer has given Notice to the other Party of an intention to terminate the BT Managed DDoS Security Service in accordance with the Agreement, BT will continue to provide the BT Managed DDoS Security Service and BT and the Customer will continue to perform its obligations in accordance with the Agreement.

6.1.2 If BT or the Customer gives Notice to the other Party of an intention to terminate the BT Managed DDoS Security Service, BT will cease delivering the BT Managed DDoS Security Service at the time of 23:59 on the day that the Notice period expires.

6.2 **Service Option Upgrades and Downgrades**

At any time, the Customer may request a move from one of the Service Options set out in Paragraph 3.1 to another.

6.2.1 If the Customer decides to upgrade to a higher Service Option, the following terms will apply:

(a) no Termination Charges will be payable for the Service Option that the Customer is moving from;
(b) BT will re-calculate the Charges for the upgraded Service Option; and
(c) a new Minimum Period of Service will apply to the upgraded Service Option, which BT will advise the Customer of at the time of upgrading.

6.2.2 If the Customer decides to downgrade to a lower Service Option, the following terms will apply:

(a) the Customer will pay the Termination Charges for the Service Option that the Customer is moving from, as set out in Paragraph 6.66 below;
(b) BT will recalculate the Charges for the downgraded Service Option; and
(c) a new Minimum Period of Service will apply to the downgraded Service Option, which BT will advise the Customer of at the time of downgrading.

6.3 Suspension and Termination

6.3.1 Where BT believes that a Malicious Attack or frequent Malicious Attacks threaten the BT Network or are having a significant impact on BT's other customers:

(a) BT may (without Notice) prevent incoming traffic coming to the target of the Malicious Attack and deny traffic to that target to all areas of the BT Network, which may mean in some instances the target under attack may lose some or all Internet service; and
(b) BT will make all reasonable efforts to keep the Customer informed of reasons for suspension and anticipated timescale for resumption of Internet service and to resume Internet service as soon as possible.

6.3.2 Where the BT Internet Service is terminated for any reason:

(a) the BT Managed DDoS Security Service will automatically terminate; and
(b) where the termination is by the Customer in accordance with Clause 17 of the General Terms and Conditions, the Customer will pay the Termination Charges set out in Paragraph 6.6 of this Schedule.

6.4 Service Limitations

6.4.1 BT will not be able to detect and mitigate all Malicious Attacks.

6.4.2 In some circumstances the mitigation may also filter out legitimate traffic.

6.4.3 BT will not be liable for any failure to detect and/or mitigate any Malicious Attack or for filtering out legitimate traffic.

6.5 Invoicing

6.5.1 BT will invoice the Customer for the Charges for the BT Managed DDoS Security Service as set out in Paragraph 6.5.3 in the amounts specified in any Orders.

6.5.2 The Charges for the BT Managed DDoS Security Service will begin on the Operational Service Date and are fixed for the Minimum Period of Service. All Charges will be calculated in accordance with the charging information attached to the Order.

6.5.3 Unless stated otherwise in an applicable Order, BT will invoice the Customer for the following Charges in the amounts set out in any applicable Order:

(a) the Recurring Charges as set out in the Order, monthly in advance and for any period where the BT Managed DDoS Security Service is provided for less than one month, the Recurring Charges will be calculated on a daily basis;
(b) Installation Charges, where applicable, on the Operational Service Date;
(c) Charges for the Professional Services where applicable for this BT Managed DDoS Security Service, as set out in the Order, on the Operational Service Date, or agreed during the term of the Agreement; and
(d) any Termination Charges incurred in accordance with Paragraph 6.66 upon termination of the relevant BT Managed DDoS Security Service.

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

(a) Charges for investigating Incidents that the Customer reports to BT where BT finds no Incident or that the Incident is caused by something for which BT is not responsible under the Agreement;
(b) Charges for commissioning the BT Managed DDoS Security Service as set out in Paragraph 7.2 outside of Business Hours;
(c) Charges for expediting provision of the BT Managed DDoS Security Service at the Customer's request after BT has informed the Customer of the Customer Committed Date; and

(d) any other Charges set out in any applicable Order or otherwise agreed between BT and the Customer.

6.6 **Termination Charges**

6.6.1 If the Customer terminates the Agreement or the BT Managed DDoS Security Service for convenience in accordance with Clause 17 of the General Terms and Conditions, the Customer will pay BT:

(a) all outstanding Charges or payments due and payable under the Agreement;

(b) any other Charges as set out in any applicable Order;

(c) any Charges reasonably incurred by BT from a supplier as a result of early termination of the BT Managed DDoS Security Service; and

(d) any waived installation Charges.

6.6.2 In addition to the Charges set out at Paragraph 6.6.1, if the termination of the BT Managed DDoS Security Service occurs within the Minimum Period of Service, the Customer will pay BT:

(a) for any parts of the BT Managed DDoS Security Service terminated during the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to:

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

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

(b) for any parts of the BT Managed DDoS Security Service terminated after the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to 20 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service.

6.6.3 BT will refund to the Customer any money the Customer has paid in advance after deducting any Charges or other payments due to BT under the Agreement.

6.7 **Acceptable Use**

6.7.1 The Customer will comply with the Acceptable Use Policy and make sure that the Customer's Users do as well.

6.7.2 If the Customer does not comply with the Acceptable Use Policy, the Customer will be liable for any Claims, losses, costs or liabilities that BT incurs as a result.

6.7.3 BT may, where there is a serious breach of the Acceptable Use Policy, report the Customer and provide the Customer's personal information, including Personal Data, to the relevant law enforcement agency.

6.7.4 BT may restrict or suspend the BT Managed DDoS Security Service if the Customer does not follow the Acceptable Use Policy.

Part B – Service Delivery and Management

7 BT's Obligations

7.1 Service Delivery

Before the Operational Service Date and, where applicable, throughout the provision of the BT Managed DDoS Security Service, BT will:

7.1.1 provide the Customer with contact details for the Service Desk; and

7.1.2 comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at the Site(s) and that the Customer has notified to BT in writing, but BT will not be liable if, as a result of any such compliance, BT is in breach of any of its obligations under this Agreement.

7.2 Commissioning of the Service

Before the Operational Service Date, BT will:

7.2.1 configure the BT Managed DDoS Security Service;

7.2.2 conduct a series of standard tests on the BT Managed DDoS Security Service to ensure that it is configured correctly;

7.2.3 connect the BT Managed DDoS Security Service to the BT Internet Service; and

7.2.4 on the date that BT has completed the activities in this Paragraph 7.2 confirm to the Customer the Operational Service Date.

7.3 During Operation

On and from the Operational Service Date, BT:

7.3.1 in the event of a Malicious Attack being detected or advised to BT:

(a) will provide automatic Alerts or advice by telephone (depending on the Service Option chosen by the Customer), including advice as appropriate on tests and checks to be carried out by the Customer;

(b) carry out diagnostic checks from BT's premises; and

(c) will mitigate the Malicious Attack by:

(i) automated mitigation; or

(ii) manual mitigation (if agreed between BT and the Customer);

7.3.2 will maintain a web Portal to provide the Customer with online access to performance reports;

7.3.3 may, in the event of a security breach affecting the BT Managed DDoS Security Service, require the Customer to change any or all of the Customer's passwords to the Portal; and

7.3.4 upgrade software/enhance functionality.

8 The Customer's Obligations

8.1 Service Delivery

Before the Operational Service Date and, where applicable, throughout the provision of the BT Managed DDoS Security Service by BT, the Customer will:

8.1.1 provide BT with any information reasonably required without undue delay, including full details of the Managed Object(s);

8.1.2 advise BT immediately of any changes to the Managed Object(s), authorised traffic and/or the contact details of the Customer Contact;

8.1.3 provide BT with details of the Managed Object(s) via the Mitigation Templates;

8.1.4 complete and agree the Mitigation Template;

8.1.5 complete any preparation activities that BT may request to enable the Customer to receive the BT Managed DDoS Security Service promptly and in accordance with any reasonable timescales;

8.2 Service Operation

On and from the Operational Service Date, the Customer will:

8.2.1 take any steps that BT advises the Customer to take in the event of prolonged and frequent Malicious Attacks;

8.2.2 ensure that the Customer Contact reports Incidents and Malicious Attacks initially to the Service Desk using the reporting procedures agreed between BT and the Customer, and will be available for all subsequent Incident and Malicious Attack management communications;

8.2.3 immediately terminate access for any Customer Contact who ceases to be an authorised Customer Contact;

8.2.4 monitor and maintain any Customer Equipment connected to the BT Managed DDoS Security Service or used in connection with a BT Managed DDoS Security Service;

8.2.5 ensure that any Customer Equipment that is connected to the BT Managed DDoS Security Service or that the Customer uses, directly or indirectly, in relation to the BT Managed DDoS Security Service is:

(a) technically compatible with the BT Managed DDoS Security Service and will not harm or damage the BT Network, or any of BT's supplier's or subcontractor's network or equipment; and

(b) approved and used in accordance with relevant instructions, standards and Applicable Law and any safety and security procedures applicable to the use of that Customer Equipment;

8.2.6 immediately disconnect any Customer Equipment, or advise BT to do so at the Customer's expense, where Customer Equipment:

(a) does not meet any relevant instructions, standards or Applicable Law; or

(b) contains or creates material that is in breach of the Acceptable Use Policy and the Customer is contacted by BT about such material;

and resolve the issues with the Customer Equipment prior to reconnection to the BT Managed DDoS Security Service;

8.2.7 maintain a written list of current Users, provide a copy of such list to BT within five Business Days following BT's written request at any time and immediately terminate access for any person who ceases to be an authorised User; and

8.2.8 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the BT Managed DDoS Security Service and:

(a) immediately terminate access for any person who is no longer a User;

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

(c) take all reasonable steps to prevent unauthorised access to the BT Managed DDoS Security Service;

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

(e) change any or all passwords or other systems administration information used in connection with the BT Managed DDoS Security Service if BT requests the Customer to do so in order to ensure the security or integrity of the BT Managed DDoS Security Service.

8.3 The End of the Service

On termination of the BT Managed DDoS Security Service by BT or the Customer, the Customer will:

8.3.1 disconnect any Customer Equipment from the Service.

9 Notification of Incidents

9.1 Where the Customer becomes aware of an Incident:

9.1.1 the Customer Contact will report it to the Service Desk;

9.1.2 BT will:

(a) give the Customer a Ticket;

(b) provide advice by telephone, including where appropriate advice tests and checks to be carried out by the Customer; and

(c) where possible, carry out diagnostic checks from BT's premises and the Customer will co-operate in diagnosing Incidents by carrying out any diagnostic and test routines requested by BT or included in the manufacturer's instructions;

9.1.3 BT will inform the Customer when BT believes the Incident is cleared, and will close the Ticket when:

(a) the Customer confirms that the Incident is cleared within 24 hours of being informed; or

(b) BT has attempted unsuccessfully to contact the Customer, in the way agreed between BT and the Customer, in relation to the Incident and the Customer has not responded within 24 hours following BT's attempt to contact the Customer.

9.1.4 If the Customer confirms that the Incident is not cleared within 24 hours of being informed, the Ticket will remain open, and BT will continue to work to resolve the Incident.

9.1.5 Where BT becomes aware of an Incident, Paragraph 9.1.2, 9.1.3 and 9.1.4 will apply.

Part C – Service Targets

10 Service Availability

10.1 **Availability Service Targets**

From the Operational Service Date, BT will aim to provide the BT Managed DDoS Security Service with target availability as follows:

10.1.1 99.95% availability at all times, subject to the terms of this Agreement.

(the "**Availability Service Target**").

Part D – Defined Terms

11 Defined Terms

In addition to the defined terms in the General Terms and Conditions, capitalised terms in this Schedule will have the following meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms and Conditions, these defined terms will take precedence for the purposes of this Schedule):

"**Access Line**" means a Circuit connecting a Site to the BT Network.
"**Application Layer Attacks**" is a form of denial-of-service (DDoS Attack) where attackers target the application layer of the Open Systems Interconnection model. The attack over-exercises specific functions or features of a website with the intention to disable those functions or features. This application-layer attack is different from an entire network attack.
"**Alert**" means notification by BT to the Customer by email or any other means agreed between BT and the Customer of a Malicious Attack.
"**Availability Service Target**" has the meaning given in Paragraph 10.1.
"**Broadband Router**" means the BT Internet Service router.
"**BT Managed DDoS Security Service**" has the meaning given in Paragraph 1.
"**BT Managed Security Service**" means a range of graded security management services which can be used in "**BT Internet Service**" means BT's data services that allow the Customer to connect to the Internet using a range of access methods at a variety of speeds over the BT Network
"**BT Management Router**" means a Cisco 1941 combined Router/Terminal Server or equivalent router.
"**BT Network**" means the communications network owned or leased by BT and used to provide a BT Managed DDoS Security Service.
"**Business Hours**" means between the hours of 0800 and 1700 in a Business Day.
"**Circuit**" means any line, conductor, or other conduit between two terminals by which information is transmitted. **"Cyber Commercial Operations"** or **"CCO"** means the BT team supporting cyber security monitoring for customers.
"**Customer Equipment**" means any equipment including any Purchased Equipment and software, other than BT Equipment, used by the Customer in connection with the BT Managed DDoS Security Service.
"**Customer Router**" means the Internet access router owned by the Customer.
"**DDoS**" means Distributed Denial of Service.
"**DDoS Attack**" means an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. "**Ethernet**" means a family of computer networking technologies for LANs.
"**EU**" means European Union.
"Fast Flood" means a service by which a DDoS Attack can be detected quicker and mitigation therefore commenced with less delay and service impact.
"High Alert" means a high level of traffic for a significant period which indicates a likelihood that a customer may be under a DDoS Attack.
"**HSM Module**" means a hardware security module that is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. "**Incident**" means an unplanned interruption to, or a reduction in the quality of, the BT Managed DDoS Security Service or particular element of the BT Managed DDoS Security Service.
"**Installation Charges**" means those Charges set out in any applicable Order in relation to installation of the BT Managed DDoS Security Service or any Purchased Equipment, Customer Equipment or BT Equipment as applicable.
"**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.
"**IP Address**" means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.
"**Local Area Network**" or "**LAN**" means the infrastructure that enables the ability to transfer IP services within Sites (including data, voice and video conferencing services).
"Malicious Attack" means a DDoS Attack, DDoS flood, protocol misuse and behaviour anomaly based attack.
"**Managed Object**" means a range of IP Addresses that BT will monitor and thresholds that will be used to trigger an Alert and subsequently automated mitigation.
"**Minimum Period of Service**" means a period of 12, 36 or 60 consecutive months beginning on the Operational Service Date, as set out in an Order.

"**Mitigation Template**" means the form which sets out the section of countermeasures that will be applied when the system goes into automatic or manual mitigation, and will be agreed by the Customer and BT.
"**Network Terminating Unit**" or "**NTU**" means the socket where the Customer's wiring, equipment or existing qualifying data service is connected to the Access Line.
"**Portal**" means a secure shared website that enables the Customer to view service information, request changes and download service reports.
"**Professional Services**" means assistance with the implementation, configuration of the BT Managed DDoS Security Service and operational assistance.
"Purchased Equipment" means any equipment, including any Software, that BT sells or licenses to the Customer.
"Reach In" means that in addition to the automated mitigation (and Alerts) BT can be contacted to assist and support customers who are either under attack or fear they will be attacked.
"Reach Out" means that in addition to the automated mitigation (and Alerts), BT will actively monitor the traffic on the customer's network and pro-actively investigate any High Alerts and advise the customer of any action to take.
"**Recurring Charges**" means the monthly fees payable by the Customer for the BT Managed DDoS Security Service or applicable part of the BT Managed DDoS Security Service that are invoiced repeatedly in every payment period (e.g. monthly), as set in any applicable Order.
"**Service Desk**" means the helpdesk that the Customer is able to contact to submit service requests, report Incidents and ask questions about the BT Managed DDoS Security Service.
"**Service Management Boundary**" has the meaning given in Paragraph 4.1.
"**Service Options**" has the meaning given in Paragraph 3.
"**Site**" means a location at which the BT Managed DDoS Security Service is provided.
"**Standard Service Components**" has the meaning given in Paragraph 2.
"**Termination Charges**" means those Charges incurred in accordance with Paragraph 6.6
"**Territory**" means the country in which BT is registered as resident for corporate income tax purposes.
"**Ticket**" means the unique reference number provided by BT for an Incident and that may be known as a "**fault reference number**".
"Unlimited Cloud" means a service where BT provides the Customer with an unlimited number of mitigations, through its cloud based system.