Anexo de Servicio BT Managed DDoS Security – On BT's Network
Parte B - Descripción del Servicio

Sección A - El Servicio

1. COMPONENTES ESTÁNDAR DEL SERVICIO

1.1 BT prestará al Cliente los siguientes Servicios de acuerdo con los detalles establecidos en el Pedido:

1.1.1 Supervisión de Internet y Notificación de Alertas

(a) supervisión de las conexiones a Internet del Cliente y suministro de notificaciones de Alertas por parte del Centro de Operaciones de Seguridad ("**SOC")** de BT para lo establecido en el Pedido. El Cliente podrá seleccionar en el Pedido:

(i) protección granular con 1 entidad de supervisión por Emplazamiento; o

(ii) Protección multi-Emplazamiento;

(b) supervisión del tráfico de Internet en los Objetos Gestionados por la plataforma DDoS de BT;

(c) investigación de cualquier patrón de tráfico anómalo en Internet;

(d) en función del nivel de Servicio seleccionado, las exclusiones de detección suprimen las alertas a direcciones IP específicas; y

(e) en caso de que se detecte un Ataque Malicioso o se informe de ello a BT, BT:

(i) proporcionará Alertas automáticas o asesoramiento por correo electrónico o teléfono (en función de lo que el Cliente haya seleccionado en el Pedido), incluido el asesoramiento, según proceda, sobre las pruebas y comprobaciones que debe realizar el Cliente;

(ii) realizará comprobaciones de diagnóstico desde las instalaciones de BT; y

(iii) mitigará el Ataque Malicioso mediante la aplicación de:

A. mitigación preaprobada; o

B. mitigación manual apoyada por el SOC de BT;

Las Partes evaluarán periódicamente si siguen siendo necesarias nuevas medidas de mitigación.

1.1.2 Service Desk - un Service Desk 24 horas al día, 7 días a la semana, para que el cliente informe de Incidencias y problemas de seguridad;

1.1.3 Revisión del Servicio - dependiendo del Nivel de Servicio seleccionado, revisiones del Servicio (remotamente) con un especialista en DDoS para incluir pruebas de desvío;

1.1.4 Portal – mantenimiento de un Portal para proporcionar al Cliente acceso en línea a los informes de rendimiento. Los informes de rendimiento estarán disponibles semanalmente y serán automatizados;

1.2 El Cliente seleccionará en el Pedido uno de los 3 Niveles de Servicio de la siguiente tabla:

Niveles de Aervicio	**Bronce**	**Plata**	**Oro**
Mitigación DDoS a	Nube ilimitada	Nube ilimitada	Nube ilimitada
Tiempo de respuesta a un taque DDoS	Mitigación automatizada durante 24 horas al día, 7 días a la semana - Normalmente la mitigación se activará en los 9 minutos siguientes al Ataque DDoS.	Mitigación automatizada durante 24 horas al día, 7 días a la semana - Normalmente la mitifación se activará en los 9 minutos siguientes al ataque DDoS.	Mitigación automatizada durante 24 horas al día, 7 días a la semana - Normalmente la mitigación se activará en los 9 minutos siguientes al ataque DdoS.

Objeto gestionado / Plantilla de mitigación	1 x Objeto Gestionado / se aplicará una Plantilla de Mitigación estándar	3 x Objeto Gestionado / se adaptará una Plantilla de Mitigación al Cliente.	5 x Objeto Gestionado / se adaptará una Plantilla de Mitigación al Cliente.
Servicio de Alerta	Alerta Alta: se enviará automáticamente un correo electrónico al Cliente y a los contactos comerciales de BT.	Alerta Alta: se enviará automáticamente un correo electrónico al Cliente y a los contactos comerciales de BT.	Alerta Alta: se enviará automáticamente un correo electrónico al cliente y a los contactos comerciales de BT.
Informes de tráfico y opciones de alerta disponibles a través del Portal	Sí	Sí	Sí
Reach-In / Reach-Out al Interlocutor del Cliente.	Reach-In limitado a la instalación inicial de lunes a viernes entre las 09:00 y las 17:00 GMT, excepto festivos en el Reino Unido. No Reach-Out.	Reach-In durante 24 horas al día, 7 días a la semana proporcionando apoyo reactivo bajo ataque / sospecha de ataque. No Reach-Out	Reach-In durante 24 horas al día, 7 días a la semana. Reach-Out - Alertas Altas proactivas.
Solicitudes de servicio sencillas (enmiendas a configuraciones DDoS y acciones)	Solicitudes de servicio ilimitadas de lunes a viernes de 09:00 a 17:00 GMT, excepto festivos en el Reino Unido.	Solicitudes de servicio ilimitadas de lunes a viernes de 09:00 a 17:00 GMT, excepto festivos en el Reino Unido.	Solicitudes de servicio ilimitadas de lunes a viernes entre las 09:00 y las 17:00 GMT, excepto festivos en el Reino Unido.
Fast Flood (detección más rápida y mitigación)	No	Sí. tiempo de mitigación < 1min.	Sí. tiempo de mitigación < 1min.
Supervisión de las operaciones de seguridad	No	Vigilancia durante 24 horas al día, 7 días a la semana	Vigilancia proactiva durante 24 horas al día, 7 días a la semana
Gestión de Incidencias Mitigación	Mitigación automática ilimitada	Mitigación automática ilimitada más mitigación manual.	Mitigación automática ilimitada más mitigación manual.
Revisión del servicio – en remoto	Anual	Trimestral	Mensual
Detección y exclusión	No	Incluidas	Incluidas

1.3 Los detalles de los aspectos de la gestión durante la vida útil se establecen en la sección C, incluido el proceso para los cambios simples y complejos de las solicitudes de servicio.

2. OPCIONES DE SERVICIO

BT proporcionará al Cliente cualquiera de las siguientes opciones según lo establecido en cualquier Pedido aplicable y de acuerdo con los detalles establecidos en dicho Pedido:

2.1 Managed DDoS Edge Defence.

2.1.1 Managed DDoS Edge Defence proporciona:

(a) protección contra los Ataques a la Capa de Aplicación; e

(b) informes más detallados sobre ataques en tiempo real, hosts bloqueados, países donde se originó el ataque y tendencias históricas a través del Portal.

2.1.2 Managed DDoS Edge Defence está disponible con los Niveles de Servicio Bronce, Plata y Oro.

2.1.3 Managed DDoS Edge Defence requiere que el Cliente:

(a) adquiera a BT los dispositivos de seguridad, incluido el software necesario (sujeto a un pedido por separado), y BT proporcionará e instalará los dispositivos de seguridad con el software necesario en cada Emplazamiento; o bien

(b) adquiera únicamente el Software necesario de BT, que se instalará en los Dispositivos de seguridad proporcionados por el Cliente, siempre que BT confirme que dichos equipos son adecuados para este Servicio. En el Pedido, el Cliente podrá elegir entre:

(i) que BT instale el Software; o

(ii) que el Cliente instale el Software.

3. LÍMITE DE GESTIÓN DEL SERVICIO

3.1 La responsabilidad de BT de prestar y gestionar el Servicio se limita física y lógicamente al siguiente límite de gestión del servicio:

3.1.1 Cuando el Cliente no haya solicitado Managed DDoS Edge Defence, BT prestará y gestionará el Servicio hasta la unidad de terminación de red de la conexión a Internet; o bien

3.1.2 Cuando el Cliente haya solicitado Managed DDoS Edge Defence, BT proporcionará y gestionará el Servicio de la siguiente manera:

(a) cuando no haya un cortafuegos entre el Managed DDoS Edge Defence y el router del cliente, el puerto Ethernet conectará el Managed DDoS Edge Defence con el router del cliente; o bien

(b) cuando haya un cortafuegos entre el Managed DDoS Edge Defence y el router del cliente, el puerto Ethernet conectará el Managed DDoS Edge Defence al cortafuegos del cliente.

3.2 El apartado 3.1 constituye el "**Límite de Gestión del Servicio**".

3.3 BT no será responsable del Servicio fuera del Límite de Gestión del Servicio.

3.4 BT no hace ninguna declaración, ya sea expresa o implícita, sobre si el Servicio funcionará en combinación con cualquier Equipo del Cliente u otro equipo y software.

4. SERVICIOS DE HABILITACIÓN

4.1 El Cliente dispondrá de los siguientes servicios necesarios para el funcionamiento del Servicio:

(a) Una conexión a Internet de BT como método de acceso (el "**Servicio de Habilitación**")

5. PUESTA EN MARCHA DEL SERVICIO

Antes de la Fecha de Servicio Operativo, BT:

5.1 entregará y configurará el Servicio realizando las acciones que se indican a continuación:

5.1.1 conectar el Servicio a cada Servicio de Habilitación;

5.1.2 si se ha solicitado Managed DDoS Edge Defense a BT, instalar y configurar los Dispositivos de seguridad para Managed DDoS Edge Defense en los Emplazamientos del Cliente;

5.1.3 configurar el Servicio de acuerdo con las especificaciones establecidas en el Pedido;

5.1.4 realizar una serie de pruebas estándar en el Servicio para garantizar que está configurado correctamente; y

5.1.5 en la fecha en que BT haya completado las actividades de este apartado 0, confirmar al Cliente que el Servicio está disponible para la realización de las Pruebas de Aceptación.

6. PRUEBAS DE ACEPTACIÓN

6.1 El Cliente llevará a cabo las Pruebas de Aceptación del Servicio en un plazo de cinco (5) Días Laborables tras recibir la notificación de BT ("**Periodo de Pruebas de Aceptación**").

6.2 El Servicio será aceptado por el Cliente si éste confirma su aceptación por escrito durante el Periodo de Prueba de Aceptación o se considerará aceptado por el Cliente si éste no notifica lo contrario a BT antes de que finalice el Periodo de Prueba de Aceptación.

6.3 Sin perjuicio de lo dispuesto en el apartado 6.4, la Fecha de Servicio Operativo será la primera de las siguientes:

6.3.1 la fecha en que el Cliente confirme por escrito, o BT considere que acepta el Servicio de conformidad con el apartado 6.2;

6.3.2 la fecha del primer día siguiente al Período de Pruebas de Aceptación; o

6.3.3 la fecha en que el Cliente comience a utilizar el Servicio.

6.4 Si, durante el Periodo de Pruebas de Aceptación, el Cliente notifica a BT que no se han superado las Pruebas de Aceptación, BT subsanará la no conformidad sin demoras indebidas y notificará al Cliente que BT ha subsanado la no conformidad e informará al Cliente de la Fecha de Servicio Operativo .

Sección B - Condiciones del Proveedor

7. CLUF

7.1 El CLUF aplicable será: https://www.netscout.com/sites/default/files/2019-01/NetScout-Systems-End-User-Product-License-Agreement.pdf

Sección C - Gestión del Servicio

8. GESTIÓN DEL SERVICIO

8.1 A este Servicio se le aplicará el Anexo de Gestión del Servicio contemplado en el Pedido para cualquier Incidencia técnica en vida.

8.2 Además del Anexo de Gestión del Servicio, se aplicarán las siguientes disposiciones a cualquier problema y cambio de seguridad durante la vida útil:

8.2.1 Supervisión

(a) BT supervisará el rendimiento del Servicio, de cualquier Servicio de Habilitación y de los Objetos Gestionados mediante la supervisión del rendimiento y de las aplicaciones a intervalos y parámetros establecidos por BT .

(b) En caso de problemas de seguridad durante el ciclo de vida, BT informará al Cliente y éste enviará un ticket al SOC, que investigará y tomará las medidas oportunas o recomendará las medidas que el Cliente debe tomar.

8.2.2 Informes

BT proporcionará;

(a) informes sobre el uso y la gestión de la capacidad

(b) recomendaciones al Cliente mediante informes en el Portal o por correo electrónico, según lo acordado por el Cliente, basándose en los umbrales históricos y actuales capturados a través de la supervisión de BT para prever problemas que puedan afectar al rendimiento de la red del Cliente.

8.2.3 Proceso de gestión de cambios del CSP

(a) BT aplicará los cambios en los CSP en respuesta a la solicitud del Cliente de la siguiente manera:

(i) **Cambios Simples** - E**stándar**; un cambio simple relacionado con actualizaciones y modificaciones necesarias debido a desarrollos planificados y mejoras de seguridad. BT implementará los Cambios estándar según los plazos acordados en el CSP, previa aprobación del Cliente.

(ii) **Cambios Simples - Urgentes**; un cambio simple relacionado con actualizaciones y modificaciones necesarias debido a actividades no planificadas o imprevistas, pero que no son críticas para mantener la seguridad de la red del Cliente. BT aplicará los Cambios Urgentes tan pronto como sea razonablemente posible, previa aprobación del Cliente.

(iii) **Cambios Simples - Emergencia**; un cambio sencillo de emergencia que debe implementarse lo antes posible específicamente para abordar un problema que tenga un impacto adverso en las operaciones comerciales del Cliente, o para prevenir o resolver un problema de Prioridad 1. BT implementará un Cambio Simple de Emergencia tan pronto como sea razonablemente posible, pero sin la aprobación previa del Cliente, siempre que, posteriormente, BT demuestre por qué era necesario dicho Cambio Simple de Emergencia.

9. (en conjunto, el "**Proceso de Gestión de Cambios del CSP**").

(i) **Cambios Complejos**; cualquier otro cambio no establecido anteriormente y por lo tanto requerirá una Orden adicional para acordar los detalles específicos sobre dicho cambio y los Cargos adicionales aplicables.

(b) BT sólo aceptará los cambios solicitados por el interlocutor autorizado del cliente por correo electrónico.

(c) BT comprobará la complejidad de cada solicitud y evaluará si considera que el cambio es (i) un Cambio Simple que puede realizarse a través del Proceso de Gestión de Cambios del CSP o (ii) un Cambio Complejo.

(d) Los siguientes cambios se califican como Cambios Simples:

(i) actualizaciones del grupo de notificación,

(ii) modificaciones del umbral, y

(iii) reinicio del Portal

(e) Cuando el Cliente plantee más de dieciséis (16) Cambios Simples Estándar y/o Urgentes en un periodo de doce (12) meses, las Partes se acordarán una de las siguientes situaciones:

(i) agrupar las solicitudes de los Clientes durante un periodo de tiempo para que puedan ejecutarse con mayor eficacia. En este caso puede haber algunos retrasos en la ejecución; o

(ii) revisar los requisitos del Cliente y acordar con el Cliente un proceso de aplicación alternativo adecuado y los Cargos asociados a través de un nuevo Pedido; o bien

(iii) cobrar dicha solicitud de cambio adicional según la tarifa establecida en el Pedido**.**