G Cloud 15
BT Service Definition for BT Managed Security DDoS

Contents Page

1 Services Overview

A distributed denial-of-service (DDoS or DoS) attack is one in which multiple compromised systems connected to the internet are used to attack another, thereby denying legitimate users service to the required system.

The BT Managed Security DDoS service guards against the three main types of DDoS attack:

- Volumetric attacks - The following are examples and are not exhaustive; Internet Control Message Protocol (ICMP), DNS Reflective attacks and volumetric attacks that target port 1900/SSDP to name a few.
- State exhaustion – including TCP (Transmission Control Protocol): For example a TCP flood can generate a high volume of Spoofed TCP requests designed to fill a system or firewalls state table and ensures that any of those systems resources are completely exhausted.
- Application layer attacks – including repeated Hypertext Transfer Protocol (HTTP) GET website commands, this demonstrates an alternate way of exhausting a systems resources at the upper layers and requires a slightly different approach to mitigation.

The BT Managed Security DDoS service will attempt to mitigate the high-volume attacks and state exhaustion attacks where botnets are trying to flood a customer's internet link or intentionally try to overwhelm a system or firewall TCP state table.

Over the past few years, the size and frequency of DDoS attacks have grown dramatically as attackers take advantage of botnets and other high-speed Internet access technologies to overwhelm their target's network infrastructure.

Not only are DDoS attacks getting larger and more frequent, but they are also becoming more sophisticated as they pinpoint specific applications (e.g., NTP, DNS, ICMP and TCP State) with smaller, more concealed and targeted attacks. Over a quarter of DDoS attacks are now application based.

Nation States, organisations and individuals carry out DDoS attacks for a variety of reasons; espionage, political and financial reasons, hacktivism or sometimes just pure vandalism. Botnets provide the opportunity to considerably damage brand credibility.

2 Types of DDoS Attack

Attack vectors generally fall into one of 3 categories:

2.1 Volumetric Attacks

Volumetric attacks consume the bandwidth either within the Buyer's network or between the Buyer's network and the rest of the Internet in an attempt to saturate the provider's internet links to the Buyer's network. These attacks revolve around causing congestion. Below are lists of volumetric attacks that can be utilised to target a client network:

N.B.: This is not an exhaustive list, and many scenarios are now well documented on the internet.

UDP Flood: UDP is a connectionless protocol that uses datagrams embedded in IP packets for communication without needing to create a session between two devices (in other words, it requires no handshake process). A UDP Flood attack does not exploit a specific vulnerability. Instead, it simply abuses normal behaviour at a high enough level to cause congestion for a targeted network. It consists of sending a large number of UDP datagrams from potentially spoofed IP addresses to random ports on a target server. The server receiving this traffic is unable to process every request, and consumes processing power and bandwidth attempting to send ICMP "destination unreachable" packet replies to confirm that no application was listening on the targeted ports. As a volumetric attack, a UDP flood is measured in BPS (bits per second) and PPS (packets per second).

ICMP Flood: This is another connectionless protocol used for IP operations, diagnostics, and errors. Just as with a UDP flood, an ICMP flood (or Ping Flood) is a non-vulnerability based attack; it does not rely on any specific vulnerability to achieve denial-of-service. An ICMP Flood can involve any type of ICMP message, such as a ping request (echo request and echo reply). Once enough ICMP traffic is sent to a target server, the server becomes overwhelmed attempting to process every request, resulting in a denial-of-service condition. Like a UDP Flood, an ICMP Flood is also a volumetric attack, measured in BPS (bits per second) and PPS (packets per second).

IGMP Flood: Internet Group Management Protocol (IGMP) is another connectionless protocol. It is used by IP hosts (computers and routers) to report, join, or leave multicast group memberships. An IGMP Flood is non-vulnerability based, as IGMP is designed to allow multicast. Such floods involve a large number of IGMP message reports being sent to a network or router, significantly slowing and eventually preventing legitimate traffic from being transmitted across the target network.

DNS Reflective: This attack requires the attacker to send thousands of spoofed DNS requests where the spoofed IP addresses are that of systems in the attacked client network. This results in thousands of large DNS responses packets originating from many different legitimate DNS sources flooding into the client network. This rapidly fills the client bandwidth whilst making the DNS and other servers hosted on the client network inaccessible. It is also possible that the DNS servers of the client Network are used as the reflection agent, which can have the effect of overwhelming those DNS servers and filling the client networks outbound capacity.

Volumetric attacks are generally designed to take out client infrastructure such as routers, switches, servers and links.

2.2 TCP State-Exhaustion Attacks

TCP State exhaustion attacks attempt to consume the connection state tables which are present in many infrastructure components such as load-balancers, firewalls and the application servers themselves. Even high capacity devices capable of maintaining state on millions of connections can be taken down by these attacks.

TCP State exhaustion: This attack vector exploits the stateful nature of the TCP protocol by flooding SYN, FIN and RST type packets to the recipient. All of these are intended to tie up the underlying system resources of the targeted system or server, rendering it unavailable and unable to respond to legitimate requests.

TCP Open Connection: these are evolving attack vectors that can quickly overwhelm a firewall's state table by opening sockets to fill the connection table. This essentially fills the firewalls state table so it is unable to open ports to legitimate users. The firewall can take some time to restore service and often will not recover without manual intervention.

2.3 Application Layer Attacks

These target some aspect of an application or service at Layer-7. These are the most dangerous kind of attacks as they can be very effective with as few as one attacking machine generating a low traffic rate (making this attack category very difficult to pro-actively detect and mitigate). These attacks have come to prevalence over recent years and application layer flood attacks (e.g. HTTP GET flood) are amongst the most common DDoS attacks.

Application layer attacks: exploit the limitations and functionality of specific applications; they generally take advantage of those applications that contain design flaws.

Application layer attacks are difficult to detect because the attacks themselves can be generated from a single device and at low packet volumes, meaning traditional monitoring and alert thresholds that monitor malicious traffic will never be breached and hence, go undetected.

Slow Loris: this attack vector works by opening multiple connections to the targeted server and attempts to keep them open as long as possible. This is achieved by

repeatedly sending partial HTTP requests which are never completed. Slow Loris then periodically sends HTTP headers for each request until the receiving web server's connection pool reaches its upper limit, stopping any legitimate HTTP requests from completing.

Because these are partial as opposed to malformed packets they generally go undetected by traditional IDS's.

2.4 DDoS Attacks are evolving

The Supplier has seen attacks in each of the above attack vectors continuously evolve, with many clients experiencing multi-vector attacks from spoofed addresses sourced from around the internet. The Supplier has seen a dramatic acceleration of innovation on the part of the hacking community. Attack tools are easier to find and download while public awareness of DDoS attacks and their implications for service have increased.

Multi-layered DDoS defence is required to keep up with increased attack sophistication along with good intelligence, continuous updating of known threats and responses. The Supplier and its suppliers provide constant updates containing the latest intelligence (i.e. compromised IP/Botnet addresses) as experience and up to date intelligence are vital in successfully combating DDoS attacks.

3 Service Overview

The BT Managed Security DDoS service can be broken down into four elements:-

- Monitoring
- Detection
- Mitigation
- Reporting.

3.1 Monitoring

The Supplier has developed a multifaceted and multi- layered DDoS security solution using network and cloud capabilities (and are therefore not reliant on a single technology or system) to defend its customers and its assets. The Supplier has deployed a layered security solution throughout the core, peering and transit part of our networks to ensure traffic entering the Supplier's autonomous system from the internet goes through a series of checks.

The Supplier has deployed large-scale traffic shaping and rate limiting features against known UDP flood attack vectors. This ensures that the maximum cleaning capacity at the next stage is never reached.

The Supplier analyses sampled "Netflow" data of all Internet traffic entering the Supplier's autonomous system.

The Netflow data is analysed for anomalies. When the Supplier deploys a DDoS solution for individual customers or the Supplier's critical assets, a review is completed to understand how severity thresholds should be configured. This enables the Supplier to trigger alerts when anomalous traffic has been detected. Utilising attack mitigation experience within the Cyber SOC (Security Operations Centre), the Supplier has designed and deployed an extended DDoS solution using intelligence-based architecture.

When the DDoS platform detects anomalous behaviour it determines whether the traffic should be diverted through one or all of the BT Threat Mitigation Systems (TMS), strategically placed within the BT network (excludes Bronze Lite). Once a decision has been made to divert anomalous network traffic, the mitigation process is initiated.

The Supplier is able to divert prefixes as small as a /32 (individual IP address).

The Supplier's Security Sales Specialist are there to help determine the appropriate level of service and can be contacted via the BT Account Manager.

The Buyer is provided with a web portal providing different access and views depending on the service variant they have chosen. (Excluding Bronze Lite).

There is no requirement to change or alter current IP addressing as part of this service.

Typical latency through the mitigation device is less than 2ms.

3.2 Detection

BT Managed Security DDoS service uses sampled Netflow Meta data from internet platform routers to detect attacks. Measured against previously agreed threshold values the system is looking for thresholds being exceeded. At this point it is unable to detect application attacks unless the behaviour results in an increase in traffic above the set thresholds.

The Supplier create Managed Objects (MOs) within our management platform which represent a particular type of internet service or services with certain characteristics. The MO collects all the configuration elements that control a customer's service, the key element being the IP address ranges used by the Buyer to access the Internet. The Netflow Meta data from the Internet platform is analysed and recorded based on matching the IP addresses in the Meta data with the IP addresses configured within the MO. A baseline is recorded for each MO so that the system understands normal traffic patterns for each specific customer; allowing the system to detect and differentiate between normal and abnormal unwanted traffic.

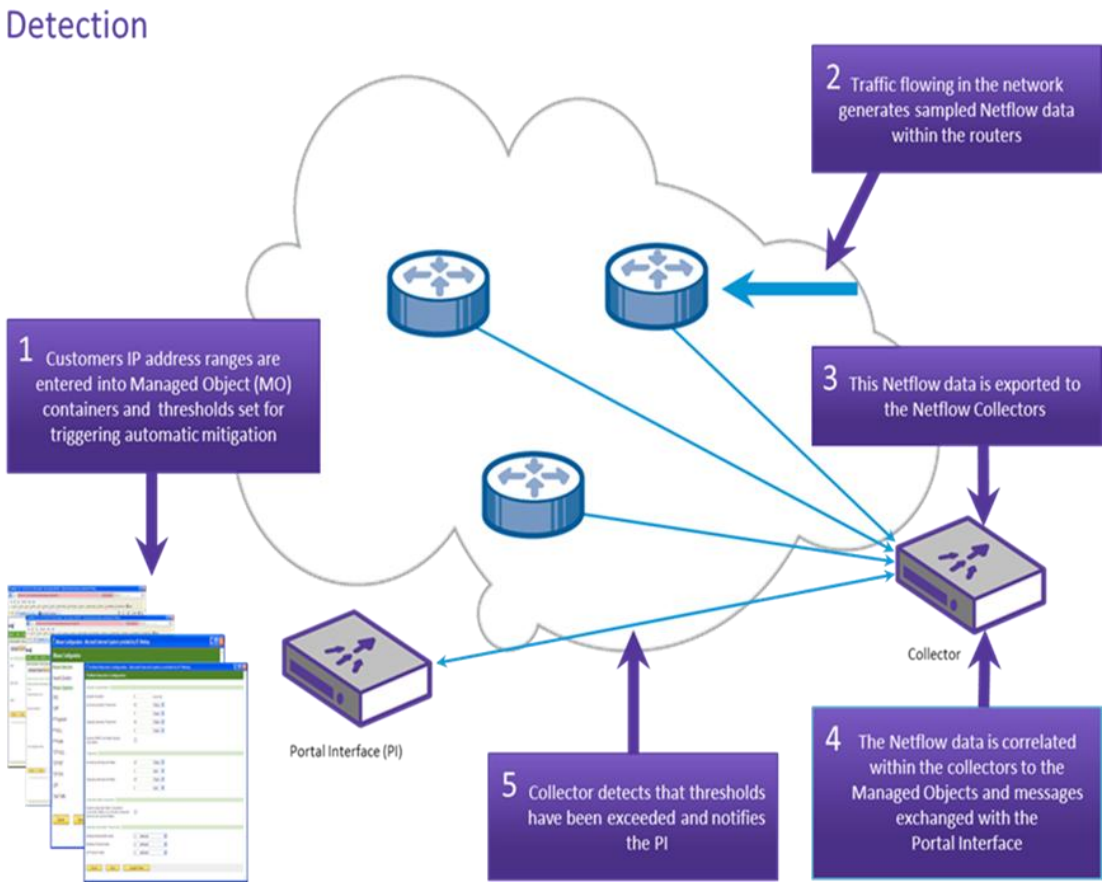

Figure 1: Detection

The management platform is designed to detect the symptoms of DDoS activity alerting according to configurable thresholds. During the commissioning process the Supplier determine the thresholds and values to use to maximise our ability to detect events while minimising false positives. Increasing service levels allow more MOs to be created; this allows individual MO and their associated countermeasures to be more focused on specific aspects of the services they protect. E.g. A web server can be treated differently to an Email relay.

Bronze Lite service uses a total traffic threshold to detect DDoS activity.

3.3 Mitigation

3.3.1 The Trigger

During the commissioning process the Supplier will work with the Buyer to prepare the DDoS platform to protect specific elements of the Buyer services. The Supplier works with the Buyer to determine what should be protected, what normal looks like and the countermeasures that can be safely used to maintain service during an attack. The Supplier configures tunnel interfaces between the TMS and Internet routers in the Buyer's network (excluding Bronze Lite). These tunnels provide a path to return cleaned traffic to the Buyer's network when running in mitigation mode.

During normal operation traffic to the Buyer's network follows the normal path, entering the Supplier's network at multiple points; where the Supplier connects to the wider Internet, content providers and other customers. This ingress traffic follows the normal IP routing determined path to the destination IP address, our DDoS management system continues to monitor this for signs of an attack, and updates MO baselines accordingly.

The BT Managed Security DDoS service detects a wide range of undesirable traffic and reduces the load on the web servers through the blocking of attack traffic while allowing valid traffic to pass. Inbound traffic is filtered by TMS using a combination of the following:

3.3.1.1 IP Filtering

- Drop Malformed IP
- Drop IP (Black Listing)
- Pass IP (Whitelisting) N.B. no further countermeasures are applied if this command is used
- Drop any combination of Protocol/port, source/destination (Black/White Listing)
- Pass any combination of Protocol/port, source/destination (Black/White Listing).

N.B. no further countermeasure is applied if this command is used.

3.3.1.2 Behavioural/Protocol Misuse

- HTTP authentication.
- Number of HTTP requests for single objects from a single source.
- Number of HTTP requests from a single source to multiple objects.
- HTTP malformed.
- Per connection Flood Protection.
- TCP Connection limiting.
- Time for TCP idle session timeout - (Preventing sessions being maintained if there is no traffic inbound).
- Slow request Detection and mitigation (E.G. Preventing clients trickling in headers to WEB servers and hence impacting server resources).
- TCP SYN authentication - (An anti-spoofing measure that requires a reset packet to be sent on the first connection of a successful TCP handshake. The connecting device must be able to deal with this initial reset packet and request the connection again. Most browser clients will do this).
- DNS Authentication Timeout.
- DNS Malformed.
- VOIP SIP Malformed.
- VOIP SIP source Limiting.
- Zombie Detection BPS - (rate limits the number of bits an individual source can send).
- Zombie Detection PPS - (rate limits the number of packets an individual source can send).
- SSL Negotiation.

3.3.2 Deep Packet Inspection

The Supplier's DDoS platform is capable of performing deep packet inspection on non-encrypted payloads.

Features within this are:

- HTTP Header Inspection.
- Packet level inspection.
- AIF = Arbor Intelligence Feed of botnet header contents.

3.3.3 Mitigation Implementation

When a DDoS attack begins, the attack traffic and normal traffic flow towards the attacked destination IP address/addresses. This can overwhelm the Buyer's network bandwidth, cause state and processing exhaustion in firewalls, load balancers, IDS/IPS systems, reverse proxies, and web servers. The Supplier's DDoS management platform starts to detect this traffic, identifying one or more signatures of an attack and shifts in the traffic distribution when compared to the MO baseline, gauging against configured thresholds. Where the service variant supports auto-mitigation after 5 minutes of consistently exceeding the high threshold, the DDoS Mitigation System instigates diversion of traffic. For critical services fast flood can be enabled to reduce auto mitigation latency.

BT's Threat Mitigation System (TMS) announces a preferred route to the attacked destination (excluding Bronze Lite). The Internet platform routers accept this route announcement and forward all traffic destined for the attacked destination to the TMS. The TMS applies a series of countermeasures recorded in the specific Buyer's Mitigation Template that is associated with the MO. The countermeasures engaged are those that were tested and configured during the commissioning process.

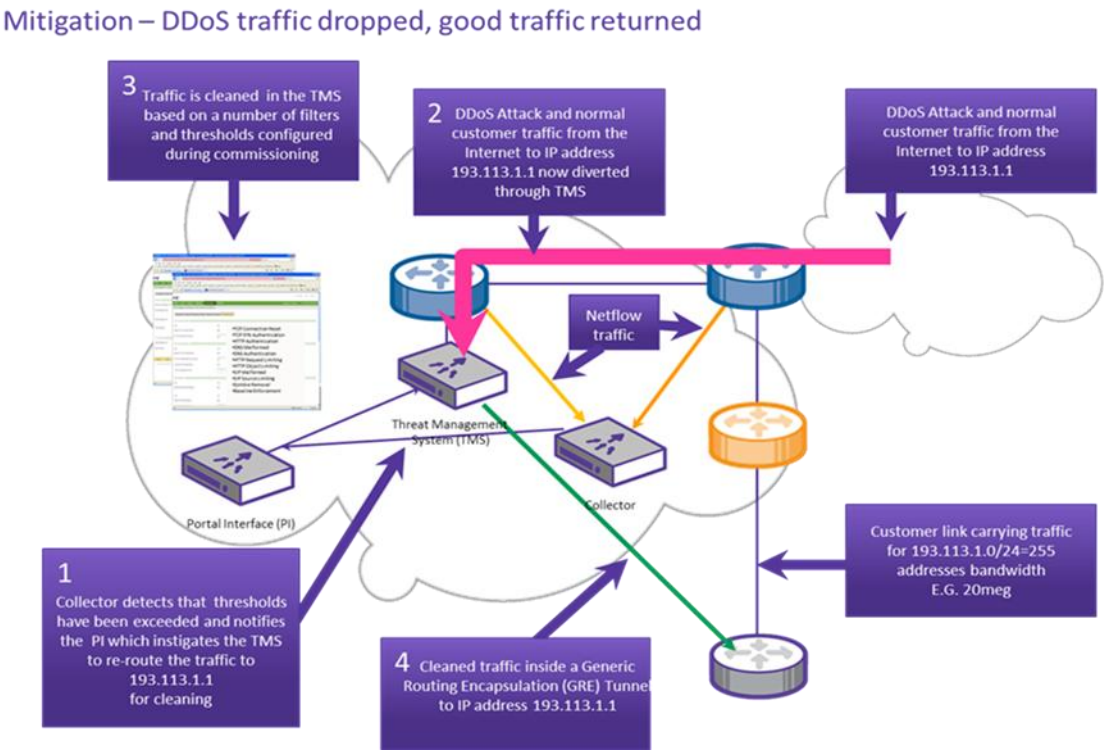

Figure 2: Mitigation - DDoS traffic dropped, good traffic returned

The Supplier's network design allows diverted traffic to flow through any one of the Supplier's TMS which are strategically placed within the core network. Where multiple TMS are used ingress traffic will flow via the logically closest TMS. The mitigation service continues to block traffic until the anomaly that triggered the mitigation has fallen below the configured thresholds for detection of a low level anomaly for a

latency period of 10 minutes. The DDoS service then withdraws the mitigation and traffic returns to normal path.

Mitigation Outcomes

Where a DDoS event is automatically mitigated (excluding Bronze Lite) there are four potential outcomes;

1. The mitigation service successfully blocks all 'illegitimate' traffic, protecting service
2. The BT Managed Security DDoS service has triggered the mitigation inappropriately (false positive) and the mitigation countermeasures are not impacting service. The Buyer may contact Cyber SOC and ask for the DDoS trigger threshold to be adjusted
3. The BT Managed Security DDoS service has triggered the mitigation inappropriately (false positive) and the mitigation countermeasures are adversely impacting service. The Buyer may contact Cyber SOC and ask for the Mitigation to be stopped, and may request a review of the countermeasures
4. The BT Managed Security DDoS service has triggered the mitigation from a valid anomaly but fails to provide successful mitigation due to some specific of the attack mechanism. The mitigation may require manual intervention by Cyber SOC. See individual service levels for information about the support provided.

3.3.4 Low level slow attacks

Certain DDoS attacks have been developed to specifically exploit weaknesses in operating systems and protocols that when exploited render the victim system inoperable without sending larger traffic volumes.

3.4 Reporting

3.4.1 Buyer Reports

The BT Managed Security DDoS service provides reports via the DDoS Portal on anomalies detected. The Buyer can drill down into this information on attack traffic pattern and the source and destination of the attack (excluding Bronze Lite).

Alert retention policy: Low = 1 month; Medium = 3 months; High = 12 months

PDF's can be downloaded from the system using the download option at the top of the alert display.

3.4.2 DDoS Portal

3.4.2.1 Bronze Lite View

The DDoS Portal access is not available for Bronze Lite Buyers.

3.4.2.2 Bronze View

Logged in view Bronze Service shows:

The general traffic seen over the past 24 hours.

The number of alerts active within retention policy.

A list of any on-going alerts.

Figure 3: Bronze view

3.4.3 Recent Mitigations

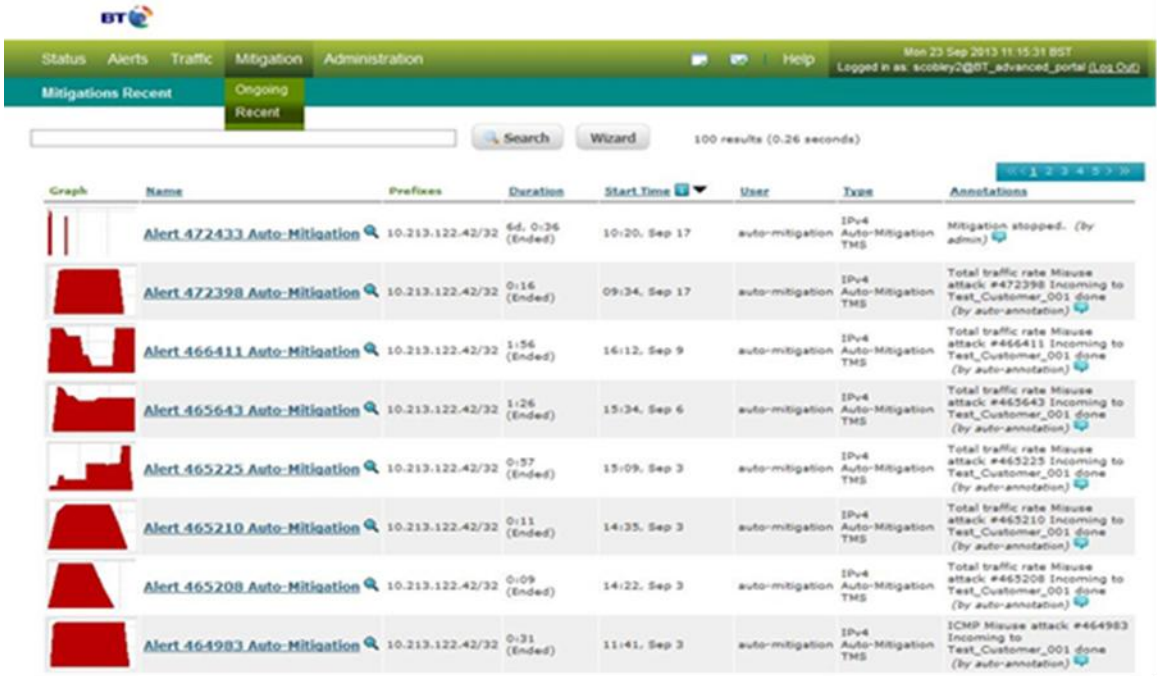

Figure 4: Recent mitigations

3.4.4 Mitigation Detail

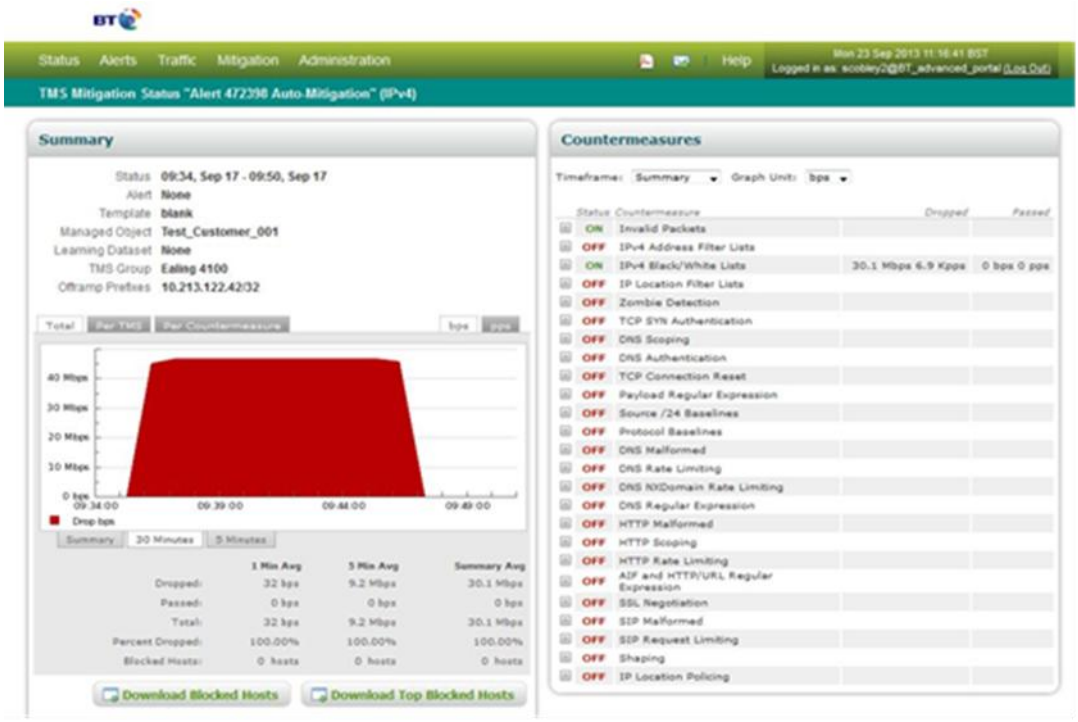

Figure 5: Mitigation detail

3.5 Service constraints

- This service is only available to BTnet / BT Internet Connect UK customers.
- In line with the Conditions of Service for BTnet / BT Internet connect circuits in the event of an attack that threatens BT's network or has significant impact on the Supplier's other customers, The Supplier reserve the right to suspend the service without notice. the Supplier will make all reasonable efforts to keep Buyers informed and to resume service as soon as possible.
- Should the Supplier feel that the BT DDoS Platform is under jeopardy, the Supplier may suspend the mitigation service, the Buyer will have the right to terminate services via written notice to the Supplier for up to thirty (30) days following suspension, in which case any prepaid fees shall be refunded and there will be no requirement for payment of Monthly Service Fees or any other fees (including Early Termination Charges) following the date of notification of suspension.

4 Service Variants

4.1 Service Options

The service is modular in design as indicated below i.e. the entry level service is Bronze Lite and this is built out to Bronze as follows:

4.1.1 Bronze Lite:

- Supports 1 Internet Connect UK circuit (generic for all applications/IP addresses).
- High alert e-mail automated notification service (24x7x365).
- 1 on-demand flowspec mitigation per contract term triggered by the Buyer's request (e-mail to ddos.bronze.lite@bt.com)
- The Supplier aims to respond within 1 hour within normal UK business hours (Monday – Friday 09:00 to 17:00 excluding bank holidays).
- No auto-mitigations.
- On demand mitigation to last for a single continuous period of up to 72 hours maximum facilitating time to upgrade to Bronze to continue protection.

4.1.2 Bronze:

- 1 Managed Object (generic for all applications/IP addresses).
- 1 Mitigation Template (best practice for all applications/IP addresses).
- High alert e-mail automated notification service (24x7x365).
- Self-service reporting via the portal.
- Unlimited automated mitigation service.
- Cyber SOC are available via e-mail during UK business hours (Monday-Friday 09:00 until 17:00 excluding bank holidays).

4.1.3 Service level feature table

The table below shows the differences between the Bronze Lite and Bronze service.

Table 1: The differences between the Bronze Lite and Bronze service

	Bronze Lite	Bronze
Managed Object	Generic based on port speed	1 tailored to the Buyer
Mitigation Template	None – reactive response to DDoS attack	1
Alerting Service	Yes	Yes
Reporting – via Portal	No	Yes

Permanent Mitigation [limited period up to 48 hours]	No	No
Mitigation supported	Single On demand at ingress (72 hours maximum).	Unlimited auto-mitigation.
Portal Accounts	None	1
Incident Support	Only to request single mitigation (per contract term).	No
Service Requests (DDoS Operational Team)	None	1 x annual check up
Cyber SOC Reach In	No	No
Cyber SOC Reach out	No	No
Onsite DDoS CPE option	No	No
FastFlood – Faster detection & mitigation of attacks	No	No

**Excluding Bank Holidays*

Bronze Lite is an entry level service to provide information to Buyers on the threat they face and to provide a once only on demand mitigation service against a volumetric attack for a maximum period of 72 hours. Further support beyond this can be implemented by the Buyer upgrading to the Bronze service.

5 Service Implementation

5.1 Successful implementation is dependent upon the following:

To implement a DDoS solution successfully the BT DDoS team will work with the Buyer to determine how to protect the Buyer's service. BT DDoS team will work with the Buyer to cover the following points:

- The correct thresholds to configure during implementation. A Data Capture Document will be provided to gather critical information about the services that require protection. This must be completed to allow for a robust defence strategy.
- The countermeasures to be used during a DDoS attack; these can be managed object specific.
- The operational model and contacts needed to operate DDoS services must be established.

For the Bronze service to deliver cleaned traffic back to the Buyer, the Supplier terminates a GRE tunnel on a router within the Buyer's infrastructure. An Internet Connect UK router can fulfil this requirement or a Buyer's owned router capable of terminating GRE tunnel can be used.

5.2 Service Delivery

Following Contract signature the implementation process can begin.

Standard Delivery timescales are:

- Bronze Lite – 10 working days.
- Bronze – 10 working days.

** Delivery timescales are based on the Buyer change window availability and the Buyer dependencies having already being completed. These delivery timescales do not account for the Buyer's induced delays.*

Pre-delivery checks are made to ensure all elements of the Buyer's end-to-end service are completed and operational prior to hand-over. Pre-delivery checks follow the test plans that are agreed with the Buyer and are required to be completed before the service can be handed over as live. Upon completion of service delivery, the Buyer is provided with contact details, escalation paths and additional information.

The BT DDoS team will send a welcome e-mail to the Buyer outlining the next steps and the timescales for delivery.

Once the Buyer's DDoS service has been implemented, the Buyer will receive another e-mail confirming the service set up and billing has started.

Upgrades from any service to any higher level of service are available and will build on the Buyer's existing service. Separate processes are in place to cover upgrades. The BT Account Manager and Security teams will work with the Buyer to capture all of the requirements necessary in providing a quote to deliver the new service.

5.3 Additions, Modifications & Cessation

All modifications can be broken down into two basic categories:

- Minor modification – an in-life modification that does not require a contract resign.
- Major modification – a modification that does requires a contract resign.

The request for additions, modifications and cessation can be made by the Buyer directly to the BT Account Manager who will also advise which category the modification requests fall under. All activities will be co-ordinated in a similar way as previously described for new service delivery.

Modifications for Bronze Lite will be facilitated by the Supplier professional services in 0.5-day increments charged at £225.00 per half day.

6 Customer Service

BT Managed Security DDoS service is available 24/7 for the automated service. The automated service is not available for Bronze Lite.

6.1 Service Hours

Contacting the Supplier:

All Buyers are given a single point of contact for fault reporting. The Supplier aims for calls to be answered within the first 30 seconds.

Bronze Lite:

Incident: The Buyer must report, by email, to ddos.bronze.lite@bt.com. The Supplier will aim to respond within an hour within normal business hours (Mon – Fri 09:00 to 17:00 excluding public holidays).

Non-incident: N/A.

Bronze:

Incident: Support is available within normal business hours (Mon – Fri 09:00 to 17:00 excluding public holidays).

Non-incident: Support is available within normal business hours (Mon – Fri 09:00 to 17:00 excluding public holidays).

6.2 Service Definitions – DDoS Platform

The BT DDoS platform is monitored and maintained 24/7/365.

Table 2: Service Definitions – DDoS Platform

Severity*	Response/Restoration
Sev 1 (Critical)	15M resp / 2hr restoration
Sev 2 (High)	15M resp / 4hr restoration
Sev 3 (Medium)	1hr resp / 8hr restoration
Sev 4 (Low)	1hr resp / 16hr restoration

** Definitions of severity below*

Restoration of the DDoS Platform is defined as invocation of manual mitigation strategy or service recovery actions that restore mitigation strategy capabilities.

N.B. – These times are NOT restoration times for individual Buyer's DDoS attacks. This is for the DDoS Platform.

Severity 1 (Critical) = an outage that the Supplier considers has a serious impact on the Service which cannot be circumvented.

Severity 2 (High) = an outage that the Supplier considers has a large impact on a portion of the Service which cannot be circumvented.

Severity 3 (Medium) = A service to the Buyer has been degraded and the Supplier has been able to provide an alternative to the Buyer such that they may continue to conduct their business.

Severity 4 (Low) = means that a minor issue (e.g. such as data cleanse) has occurred but needs to addressed by the relevant team.

Platform service availability is set at 99.95% based on the automated mitigation and the standard contract calculation and a denominator based on number of internet circuits and will be reported via the portal. The Bronze Lite service will not have a target for availability.

6.3 Service Level

For auto-mitigation to be engaged, anomalous traffic needs to be above a configured high severity threshold for a continuous 5-minute period. Where this criteria is fulfilled, auto-mitigation is engaged within 9 minutes.

During an intermittent DDoS campaign, manual mitigation can be implemented for a further 72 hours.

The Supplier reserves the right to charge for leaving Buyers in manual mitigation if requested.

6.4 Personal Data

Please note that given the standard nature of the product/service described in this catalogue entry, the Supplier and our suppliers may from time to time use back-office support and system functions which are located or can be accessed by users from outside of the UK and/or the European Economic Area.

7 Pricing

Pricing for this service is available on the G Cloud 15 website. For a full explanation of BT DDoS Mitigation Service prices, including provision, rental and added service charges, the Buyer should contact their BT Account Manager.

8 Billing

Buyers receive a bill per contractual commitments. All Buyer bills include a contact number for billing inquiries, available during local business hours.

9 Security Requirements

Due to the nature of the service within scope of this service offer, optional Call-Off Schedules 9A (Security: Short Form), 9B (Security: Consultancy), 9C (Security: Development), 9D (Security: Supplier-led Assurance) and 9E (Security: Buyer-led Assurance) are excluded and the **Suppliers standard Security Management Plan applies only**.

Additionally, BUYER'S SECURITY REQUIREMENTS AND ICT POLICY SECURITY REQUIREMENTS within the Call-Off Order Form will be marked with the option **There are no Security Requirements for the purposes of this Call-Off Contract** and SECURITY ASPECTS LETTER will be marked as **not applicable**.

9.1 The Security Management Plan

The Security Management Plan (SMP) defines the security measures that are implemented, and maintained, by BT. BT will maintain the adherence to the contracted security measures.

The plan supports the provision of the services in scope of this service offer and covers the following:

- Our approach to security
- Our information security policy
- External parties
- Human resource security
- Physical and environment security
- Asset management
- Operation of the plan
- The security lifecycle

9.2 Security Accreditation and Governance Standards

Security accreditation and governance standards will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

9.3 Operational Security

Operational security will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

9.4 Asset Protection

Operational security will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

9.5 Cyber Essentials Certification

Cyber essentials certification was a mandatory requirement to secure a place on the framework as a Supplier and to maintain our place on the agreement, all Suppliers must present evidence to Crown Commercial Service (CCS) of their continued certification.

Therefor the option under CYBER ESSENTIALS CERTIFICATION within the Call-Off Order Form under is marked as not applicable and for the purposes of Call-Off Schedule 27 (Cyber Essentials Scheme), clauses 2.1 to 2.4 are not used.

9.6 Staff Vetting Requirements and Background Checks

Staff vetting requirements will be in line with the details defined within the Suppliers Digital Marketplace submission and this Service Definition document and STAFF VETTING REQUIREMENTS within the Call-Off Order Form will be marked accordingly.

Our recruitment process includes pre-employment screening and vetting prior to placement to ensure adequate levels of confidentiality are maintained, screening includes:

- Application for a criminal record check
- Giving us contact details for reference checks
- Health declaration
- CIFAS- Staff Fraud Database check.

Additional checks are made when dealing with particularly sensitive positions (such those involved with sensitive contracts). The normal undertakings signed by individuals at recruitment include non-disclosure provisions and it is a disciplinary offence to misuse any information obtained from Supplier systems. Offenders are subject to disciplinary action up to and including dismissal and may be subject to prosecution, while ensuring compliance with local legislation.

Due to the nature of the service within scope of this service offer, optional Call-Off Schedule 18 (Background Checks) is excluded and in the event that Supplier Staff do not have the necessary clearance required, the Parties will agree an acceptable alternative such as escorted access.

10 Personal Data

Personal data in relation to services in scope of this service offer is divided into 2 areas:

- Managing the contract
- Managing the services

Personal data, where required to be managed, complies with the requirements of clause 17 Data protection and security, within the Framework Core Terms including new Clause 17.7 included via Framework Special Term 13

10.1 Managing the Contract

Joint Schedule 10 (Processing Data) will be completed to define what types of personal date in relation to managing the contract may be held, the nature and purposes of the processing and will confirm The Parties are Independent Controllers of Personal Data.

10.2 Managing the Service

Where personal data is held as part of delivering the service, how this will be managed will be defined, where applicable, within the Suppliers product specific Terms and Conditions that are attached to the Suppliers Digital Marketplace entry for this service offer. The Suppliers Digital Marketplace entry also confirms details of data storage and processing locations specific to this service.

The Supplier, including any Sub-processors of the Supplier, may from time to time use back-office support and system functions which are located or can be accessed by Users from outside of the UK and/or the European Economic Area. Any such processing will be in accordance with Joint Schedule 10 Paragraph 5.5.2, and for the purpose of clause 5.5.2 (a), the Buyer consents to the disclosure and transfer of Data, including Personal Data, as required in order to provide the Service.

10.3 Sub-processing

The Buyer consents to the Supplier's use of Sub-processors in accordance with the Framework Agreement. The Supplier will ensure that data protection obligations in respect of Processing Buyer Personal Data that are broadly comparable to those set out in the Framework Agreement and will be agreed with any Sub-processors.

The Supplier will inform the Buyer of intended changes to its Sub-processors from time to time, either by providing the Buyer with online access to intended changes or by such other means as the Supplier may determine. If the Buyer does not object to the proposed change within 30 days of this notice, the Buyer will be deemed to have authorised the use of the new Sub-processors.

11 Other Considerations

The service described in this Service Definition is based on the Supplier's standard offering for this cloud service and the contract is not defined as a Critical Service Contract. It should be noted that the G Cloud 15 Call-Off Order Form has a number of mandatory schedules, optional schedules and Call-Off Order Form options, and this section clarifies the position of these options for this service as provided by the Supplier. The service will additionally be delivered in line with the Supplier Terms and Conditions included within the Suppliers Digital Marketplace submission.

11.1 Modern Slavery, Environmental Requirements and Sustainability

To comply with the reporting requirements to the Buyer as defined within Joint Schedule 5 (Sustainability) the Buyers can access the Suppliers annual Modern Slavery Report, and where required (for lots 1a and 1b only) its Carbon Reduction Plan here Our reports & policies - Responsible business | BT Plc

Optional Call-Off Schedule 25 (Additional Sustainability Requirements) is excluded. The Suppliers approach to sustainability, managing our environment, and our modern slavery policies can be found here Our reports & policies - Responsible business | BT Plc

Optional Call-Off Schedule 26 (Carbon Reduction) is excluded. The Suppliers approach to carbon reduction and our carbon reduction plans can be found here Our reports & policies - Responsible business | BT Plc

11.2 Financial Difficulties

For the purpose of Joint Schedule 7 (Financial Difficulties), the Ratings Agencies listed within Annex 1 (Rating Agencies and their standard Rating System) will be Standard & Poor and Moody's and for Annex 2 (Credit Rating Thresholds) these will be BB+ for Standard and Poor and Ba1 for Moody's.

BT's published ratings are available here

11.3 Guarantee

For the purpose of Joint Schedule 8 (Guarantee), the Buyer does not require a Guarantee from the Supplier to award the contract.

11.4 IPR

For the purpose of Call-Off Schedule 1 (Intellectual Property Rights) **Part A Option A3: Supplier ownership of all New IPR with Buyer rights for the current contract only**; applies and is not further amended on the Call-Off Order Form under INTELLECTUAL PROPERTY RIGHTS.

11.5 Staff Transfer

No staff transfer is required and for the purposes of Call-Off Schedule 2 (Staff Transfer) **Part C: No Staff Transfer on the Start Date** only applies.

11.6 ICT Services

ICT services, where applicable, will be managed in line with the details defined within the Suppliers Digital Marketplace submission and supporting Supplier Terms, and where applicable within this Service Definition document and optional Call-Off Schedule 6 (ICT Services) is excluded, and the option under ICT POLICY within the order form will be marked as not applicable. Any maintenance of the ICT environment, where applicable, will be defined within this Service Definition document and the option under MAINTENANCE OF THE ICT ENVIRONMENT within the Call-Off Order Form will be marked as not applicable.

11.7 Business Continuity and Disaster Recovery

As noted by CCS guidance provided within Framework Schedule 6 (Order Form Template), optional Call-Off Schedule 8 (Business Continuity and Disaster Recovery) is not applicable for services under lots 2a and 2b and is excluded.

11.8 Corporate resolution planning

Due to the nature of the services within scope of this service offer, , which is available only when the Call-Off Contract is not a Critical Service Contract, optional Call-Off Schedule 24 (Corporate Resolution Planning) is excluded.

11.9 Exit Management

Optional Call-Off Schedule 10 (Exit Management) is excluded and at the end of the Call Off Contract Period, the offboarding process will be managed in line with the details defined within the Suppliers Digital Marketplace submission and where applicable within this Service Definition document. The Call-Off Order Form SPECIFIC EXIT MANAGEMENT ASSISTANCE (LOT 1A AND LOT 1B ONLY) and VIRTUAL LIBRARY will both also marked as not applicable.

11.10 Clustering and Leasing

Services will be contracted and invoiced to the Buyers detailed within Framework Schedule 6 (Order Form Template) and as such optional Call-Off Schedule 12 (Clustering) is excluded.

Due to the nature of the services within scope of this service offer, leasing of services is not applicable and as such, optional Call-Off Schedule 22 (Lease Terms) is also excluded.

11.11 Implementation Plan and testing

Due to the nature of the services within scope of this service offer, optional Call-Off Schedule 13 (Implementation Plan and Testing) is excluded and the services in scope will be implemented and tested in line with the details defined within the Suppliers Digital Marketplace submission and this Service Definition document.

11.12 Performance Levels

Due to the nature of the service within scope of this service offer, optional Call-Off Schedule 14 (Performance Levels) is excluded and the service levels provided are as defined within the Suppliers Digital Marketplace submission and this Service Definition document.

11.13 Service Credits

Any service credits for the services within scope of this service offer will be as detailed, where applicable, within this Service Definition document and SERVICE CREDITS within the Call-Off Order Form will be marked accordingly.

11.14 Call Off Schedule 17 (MOD Terms)

Where optional Call-Off Schedule 17 (MOD Terms) is required, this will be based on no additional DEFCONS or DEFFORMS being added within Annex 1 which incurs additional costs to the Supplier.

11.15 Call Off Specification and Deliverables

The services will be delivered in line with the Suppliers Digital Marketplace submission and this Service Definition document and as such, optional Call-Off Schedule 20 (Call-Off Specification) is excluded.

11.16 Call Off Special Terms

Due to the nature of the services within scope of this service offer based on the Supplier's standard offering for this cloud service, no additional call off special terms are introduced into the Call-Off Order Form under CALL OFF SPECIAL TERMS

11.17 Service Request Process

The service request process with be as defined within the Suppliers Digital Marketplace submission and this Service Definition document and SERVICE REQUEST PROCESS within the Call-Off Order Form will be marked accordingly.

11.18 Minimum Commitments

Any MINIMUM COMMITMENT(S) where applicable noted within Call-Off Order Form will be aligned to those as defined within the Suppliers Digital Marketplace submission and Suppliers Price Card where applicable and MINIMUM COMMITMENT(S) within the Call-Off Order Form will be marked accordingly.

11.19 Maximum Liability

The limitation of liability for this Call-Off Contract remains as stated in Clause 14.2 of the General Terms (as that Clause 14.2 has been amended pursuant to Framework Special Term 12 as set out in the Framework Award Form) and is not further amended on the Call-Off Order Form under MAXIMUM LIABILITY.

11.20 Additional Insurances

There is no requirement for additional insurances which will remain as defined within Joint Schedule 3 (Insurance Requirements) and ADDITIONAL INSURANCES on the Call-Off Order Form will be marked as not applicable.

11.21 Product Roadmaps

Any defined product roadmaps, where applicable, will be defined within this Service Definition document and PRODUCT ROADMAP (IF APPLICABLE) within the Call-Off Order Form will be marked as not used.

11.22 Quality Plans

Any defined quality maps, where applicable, will be defined within this Service Definition document and the option under QUALITY PLANS within the Call-Off Order Form will be marked as not applicable.

11.23 Social Value Commitment

Social value is at the heart of our purpose, driving impactful initiatives that address the needs of diverse communities across the UK. Our dedicated Social Value team have a focus on sustainability, community, sponsorship, charity, and the environment.

We're increasing digital inclusion and giving back to local communities through on-the-ground initiatives that make real-world positive changes.

The five pillars of social value at BT are:

- Outreach: no one is forgotten in our social value delivery.
- Improvement: continuous improvement in our delivery.
- Sustainability: our incentives are built to last.
- Engagement: user voice at the forefront and not an afterthought.
- Equity: leveraging our power to mobilise individuals, institutions, and communities

Details and reporting on what we are doing around social value can be found here Social Value At BT | About Us and SOCIAL VALUE COMMITMENT within the Call-Off Order Form will be marked accordingly and no additional bespoke commitments or reporting will be included.

12 Glossary

Various acronyms are used throughout this document. The meanings of which are:

AIF - ATLAS Intelligence Feed

CPE – Customer Premises Equipment

DDOS – Distributed Denial of Service

DNS - Domain Name System

Gbps – Gigabits

GUI – Graphical User Interface

HSM – Hardware Security Module

HTTP - Hypertext Transfer Protocol

IP – Internet Protocol

IPSEC - Internet Protocol Security

ICMP - Internet Control Message Protocol

ISP - Internet Service Providers

LLD – Low Level Design

MO - Managed Object.

MPLS - Multi-Protocol Label Switching

NIC - Network Interface Cards

NTP - Network Time Protocol

PPS – Packets per Second

RST - Reset

SNMP - Simple Network Management Protocol

SOC - Security Operating Centre

SSDP - Simple Service Discovery Protocol

SSL - Secure Socket Layer

SYN - Synchronization

TCP - Transmission Control Protocol

TMS – Threat Mitigation System.

UDP - User Datagram Protocol

VOIP – Voice over Internet Protocol

VPN – Virtual Private Network

WAN – Wide Area Network

Company information

Parent Company: BT Group plc

Company Legal Entity Name: British Telecommunications plc

Company Trading Name: BT

Address: One Braham, Braham Street, London, E1 8EE

Web Address: https://business.bt.com/