TalkTalk Business

TalkTalk Business DDOS (Distributed Denial of Service Mitigation)

Service Definition

Contents

1. DDoS (Distributed Denial of Service) Mitigation

A denial-of-service attack (DoS attack) is a cyber-attack in which the attacker seeks to make a network resource, such as a website, paywall, or cloud server unavailable to users. Denial of service is typically achieved by flooding the targeted resource with superfluous requests to overload systems and thereby prevent legitimate requests from being fulfilled. The result is a user unable to gain access, like a group of people crowding a shop doorway, making it impossible for genuine customers to gain access.

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from multiple sources achieved using a network of previously infected machines (BotNets). Such networks can run into the hundreds of thousands of machines. Therefore, blocking the source of the request traffic is almost impossible.

In recent years the sophistication of attacks has grown from brute force, volumetric flood attacks to using combinations of small packets at high rates and large packets at lower rates. These DDoS attacks often behave in similar ways to normal traffic and are therefore capable of bypassing standard DDoS defences.

Increasing numbers of internet connected things means more devices to infect, potentially increasing the prevalence of BotNets. Attackers can also hire BotNets by the hour, significantly lowering barriers to entry for a DDoS attacker, offering users the option to anonymously attack any target, for as little as £20. They are advertised legitimately as “stressers”, with the stated use case being that they are tools to test the resilience of your own infrastructure. However, with no steps taken to verify your identity and your ownership of the target infrastructure, such tools can be pointed at anyone, enabling cybercrime, cyber-vandalism, and many other types of DDoS-related activities.

The targets of DDoS attacks used to be large e-retailers, financial services, gaming business and others that offer chargeable services accessed via public facing internet. By flooding the gateways that provide these services and effectively making them unavailable, the targeted organisation, facing significant revenue losses sometimes chose to pay the attacker to cease the DDoS attack.

With more of us working remotely and even when office based, using cloud ‘software as a service’ platforms for everything from CRM to telephony, the target for DDoS attacks has broadened. By flooding an organisation’s internet gateway with large volumes of traffic, an attacker can block user access to these software services, leaving them unable to take phone calls, process card payments and access customer records for example. By attacking an organisation’s VPN gateways, remote workers are cut off from resources they need. For even medium-sized organisations, losing access to such vital platforms can have a very real impact on productivity.

If you rely heavily on internet-based service revenues, use internet-based ‘software as a service’, rely on remote workers or use internet-connected industrial process systems, you are a target for a DDoS attack. The attackers are often opportunists and we’ve even seen (and prevented) a huge DDoS attack launched against a small restaurant.

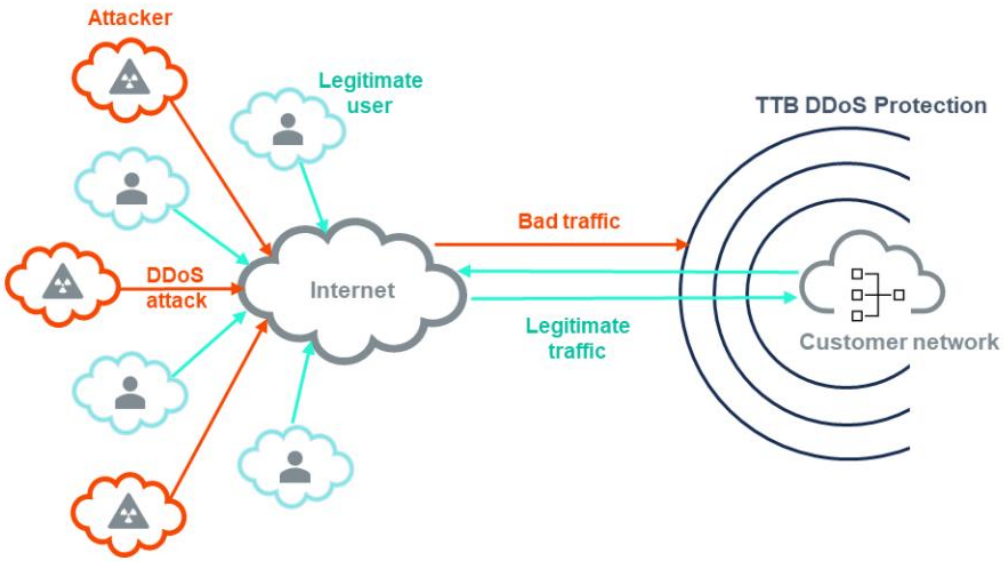
DDoS attacks continue to rise in size, frequency and complexity. High volume flood attacks that target internet connectivity must be mitigated further upstream, away from the intended target before they overwhelm any local protection. Just as important, the solution must have an intelligent up-to-date threat intelligence to stop dynamic, multi-vector DDoS attacks.

After extensive market analysis and testing, TalkTalk Business (TTB) has chosen to partner with NETSCOUT® Arbor. For the past 20+ years, Arbor has been the undisputed leader in DDoS attack protection solutions. Arbor's solutions are trusted by the majority of the world's Internet Service Providers and many of the world's largest Enterprises. Our solution is fully managed and intelligently automated, continuously backed by global threat intelligence. We've invested millions of pounds in integrating a NETSCOUT Arbor DDoS attack mitigation platform into our network.

As a result of this investment TTB can offer a sophisticated DDoS mitigation service at a significantly lower cost than our customers would face if they were to invest in their own platforms. Also, as the provider of business internet services it means you can take advantage of this protection built into our network.

The result is a reactive service that constantly monitors customer traffic for anomalous patterns and can take automatic action to redirect customer traffic through our NETSCOUT Arbor platform in the event of pre-agreed thresholds being breached. Redirection can also be initiated at your request if an attack is suspected or undertaken as a test as part of a compliance certification requirement.

A really simple way of thinking about our automated DDoS Mitigation service is that it keeps 'bad' traffic away from your network and allows 'good' traffic through as depicted in the following diagram.



A typical mitigation process can be broadly defined by these four stages:

Detection - the identification of traffic flow deviations that may signal the buildup of a DDoS assault. Detection effectiveness is measured by our ability to recognise an attack as early as possible, with instantaneous detection being the goal.

Diversion - traffic is automatically rerouted away from its target via DNS (Domain Name System). If the threshold trigger levels are reached, a decision is made whether to filter the traffic or discard it altogether. DNS routing is always-on.

Filtering - DDoS traffic is filtered out, usually by identifying patterns that instantly distinguish between legitimate traffic (i.e. humans, API calls and search engine bots) and malicious visitors.

Restoration – once traffic falls below the threshold trigger levels the DNS routing returns to normal.

The service is based on Managed Objects. A Managed Object is a sub-division of the equipment or services monitored by the DDoS Attack Mitigation Service which contains IP addresses for a group of protected servers and equipment. The DDoS Attack Mitigation Service provides protection for those IP Addresses only and is therefore sold on a per Managed Object basis.

TalkTalk's security platform will automatically start Mitigation based on traffic exceeding pre-defined Volumetric Thresholds. Mitigation will automatically end when the traffic drops below the Volumetric Thresholds.

What's included with TTB's DDoS Mitigation service:

- Reactive, automatic DDoS mitigation with one managed object pre-built
- Protection based on the bandwidth of a customer's TalkTalk Business DIA service
- Customer traffic is re-routed through our NETSCOUT Arbor platform for the duration of a DDoS attack
- Automated service reports – sent to customers weekly or monthly via email
- Two service changes per month (if required)
- Up to two mitigation service tests per annum (if required)
- 24/7 support
- Simple pricing structure per 'managed object' / IP block.

The service is fully automatic. Traffic diversion will occur within three minutes of a traffic trigger level being breached.

The service includes monthly report generation in standard form. Monthly reports will be sent to a nominated customer contact and are available on request by agreement.

1.1 Data backup and restore

The DDoS mitigation service does not include data backup and restore services.

Disaster recovery

At TTB we undertake best ITIL practices throughout the business and technology teams. The Service Desk team has a problem management and change process to ensure that root cause and preventative actions are managed effectively, in line with service levels. In addition, root cause investigations are completed as part of our problem management process, where change and incident information is analysed and collected to suggest preventative actions. Reason for Outage (RFO) for network incidents are distributed to impacted customers within 10 working days from root cause following a Priority 1(P1) or Major Service Outage (MSO).

Where the priority of a TTB Network Incident is MSO or P1, a Major Incident Manager is assigned to document and communicate the progress of an incident. A multi-disciplinary team will work collaboratively to resolve the incident as quickly as possible and with minimal impact on the business. The IT Service Management (ITSM) team record of the incident is updated throughout and resolved using defined metrics to drive post-incident analysis activities.

Major Incident notifications are distributed during the life of the incident via a dedicated Incidents Team. If the customer has any questions related to an RFO notification, or requires additional detail, these can be referred to the ITSM team via your Account Manager.

Business Continuity, Crisis Management and Disaster Recovery Plans are in place for all sites. Network resilience is assessed and monitored through testing on an annual basis. Continuous monitoring of network availability through the Technical Support Centre team will ensure any issues are identified in a timely manner.

Where an incident does occur, a robust incident response process is in place and is exercised to ensure an effective response, followed by a problem management review linked to service improvement. TTB recognises that network resilience is also reliant on Openreach for the last mile. If an outage was to occur on the Openreach infrastructure, we have agreed competitive SLAs with Openreach to mitigate risk. Other prioritised critical processes, systems and third parties are identified, and business owners are assigned accountability for assessing resilience and implementing business continuity plans to enable continuity of operations in the event of an incident.

TTB also continues to invest in supporting appropriate resilience of critical systems. Relationship owners are assigned accountability for requiring critical third parties to have adequate business continuity plans in place and obtaining third party assurance, where appropriate, that their plans have been reviewed and tested annually.

With usage consistently on the rise, we constantly monitor the network, forecasting and responding to the ongoing demand to maintain stability and minimise any congestion. Despite download usage increasing 40% year-on-year, our network has remained resilient. Additionally, due to Covid-19, further measures have been implemented to ensure the health and safety of our workforce and customers whilst

we successfully continue our provision of critical services, which involves enabling the remote working of both our workforce and third parties.

1.2 Onboarding

TTB has an onboarding model for all new customers, from SMEs through to major customers, undertaking the following process:

1. The customer order is received by the salesperson, along with a copy of the terms and conditions (signed using DocuSign)

2. All customer orders are verified, and credit checked and, once approved, put into the provisioning work in progress queue (WIP)

3. All orders are built within our Inventory System's billing system by the Delivery team

4. All updates and communication on installation dates will be provided to the customer via email by the Delivery Team

When onboarding a customer to our DDoS platform, a DDoS Protection Provisioning Form is sent to the Customer to complete. This is a short form which gives us sufficient information to provide the DDoS Mitigation Service. It includes contact details for provisioning and authorised customer contacts for in-life service amendments, along with the IP Address CIDR blocks and traffic types which need protecting e.g. DNS, email, VOIP, VPN etc.

The service is based on Managed Objects. A Managed Object is a sub-division of the equipment or services monitored by the DDoS Attack Mitigation Service which contains IP addresses for a group of protected servers and equipment. The DDoS Attack Mitigation Service provides protection for those IP Addresses only and is therefore sold on a per Managed Object basis.

TalkTalk's security platform will automatically start Mitigation based on traffic exceeding pre-defined Volumetric Thresholds. Mitigation will automatically end when the traffic drops below the Volumetric Thresholds.

<u>Service Tuning</u>

Traffic rate policing mechanisms (policers) are one of the most useful tools inside our platform to mitigate DDoS attacks. The parameters of the policer configuration are vital to the correct operation of the DDoS Mitigation Service. During the first week of service a tuning exercise is undertaken. This is because we recognise that anomalous traffic

patterns for one customer can be within tolerance for another customer. Following the tuning week, traffic parameters are put in place and thresholds are agreed. This means that during service operation, traffic diversion will only happen in the event of a real attack and service reports will offer more insight and value.

For all DDoS Mitigation Services, the following detection rates are configured by default. In most scenarios the default detection settings should be appropriate. If the Customer is expecting to exceed these thresholds with legitimate traffic, these should be noted in the DDoS Mitigation Provisioning Form.

Traffic Misuse Type	Trigger Rate	High Severity Rate
DNS	10Kpps	30Kpps
ICMP	5Kpps	10Kpps
IP Fragment	5Kpps	10Kpps
L2TP (bytes)	25Mbps	50Mbps
L2TP (packets)	25Kpps	50Kpps
TCP RST	1.5Kpps	20Kpps
TCP SYN	1.5Kpps	20Kpps
UDP	30Kpps	400Kpps

- 'Trigger Rate' is the traffic rate that must be exceeded before our system generates an alert
- The 'High Severity Rate' is the traffic rate that must be exceeded for a three-minute period after which our systems begin automatic DDoS mitigation
- The above thresholds apply per-protected host
- Only 'Traffic Misuse Types' in likely use are noted above. Other thresholds apply.

1.3 Off boarding

If a customer chooses to cease their TTB service, clear timescales will be mutually agreed between TTB and the end customer. Any managed CPE provided as part of the managed service remains the property of TTB and must be returned to TTB unless otherwise agreed.

1.4 Service constraints

For all planned notices and maintenance, the customer will be notified 10 business days in advance to allow them to make suitable arrangements. Emergency maintenance is rarely required and is typically not customer-affecting, as it is usually confined to one part of a resilient system. In the event emergency maintenance is required that is likely to be customer affecting, the planning and risk assessment we undertake will include making provision to minimise the impact in terms of scope and duration. Where it is possible, advanced notice will be given.

The DDoS mitigation service can be customised for each customer in terms of the volumetric thresholds in place which dictate when an automatic mitigation starts.

1.5 Service Levels

We successfully mitigate against 50+ DDoS attacks per week, to the extent that our end users don't realise an attack has taken place.

In the event of customer agreed traffic thresholds being breached, our security platform will respond by routing customer internet access through the DDoS Mitigation Service. This will allow the customer to keep services provided by the managed object available to their consumers / end users.

Our default configuration for automated response to a DDoS attack is three minutes. This is to ensure that the response initiates quickly enough to protect against disruption, without being too sensitive to fluctuations in traffic. However, this is configurable to a customer's individual needs.

Our standard reporting provides weekly and monthly reports summarising the traffic that has passed through the Customer's connection and details of any incidents requiring mitigation to be enabled. These reports are useful to understand incidents and how the Customer connection is being used day-to-day. Default reports summarise traffic by IP protocol, TCP port, AS number, country, and application. We are happy to make changes to reporting should you require it.

Customers are entitled to two service changes per month. A service change being a change that can be completed within 30 minutes during working hours. If a service amendment will take longer than 30 minutes or is required to be undertaken out of hours, then additional charges may be levied.

Support queries will be handled through the following channels and service level agreements. Our Service Assurance and Security Operations teams both work on a 24x7 basis.

Request Type	Contact	SLA
Configuration change	Security Operations – web form	Two working days
Ad-hoc reporting	Security Operations – web form	Two working days
Incident support	Service Assurance	One hour
Service outage	Service Assurance	In line with existing contracted SLAs
General queries	Service Assurance	In line with existing contracted SLAs

1.6 After Sales Support

Incident reporting and support requests should be raised by telephone on 0333 003 4333 or via email ttbenterpriseassurance@talktalk.business. Our team aims to diagnose faults within 30 minutes. Support requests which are less time sensitive should be raised by email.

1.7 Technical Requirements

The service is based on Managed Objects. A Managed Object is a sub-division of the equipment or services monitored by the DDoS Attack Mitigation Service which contains IP addresses for a group of protected servers and equipment. The DDoS Attack Mitigation Service provides protection for those IP Addresses only and is therefore sold on a per Managed Object basis.

The DDoS mitigation service coverage purchased must cover the whole of committed data rate / bandwidth ordered over the physical circuit or internet transit port. It is not possible to protect a portion of the committed data rate.

TalkTalk's security platform will automatically start Mitigation based on traffic exceeding pre-defined Volumetric Thresholds. Mitigation will automatically end when the traffic drops below the Volumetric Thresholds.

TTB's DDoS mitigation service can be applied to any TTB provided DIA (Dedicated Internet Access) product.

1.8 Outage and Maintenance

For all planned notices and maintenance, the customer will be notified 10 business days in advance. Regarding unplanned disruption or major failures, all TTB staff will receive email notification internally, informing them of the exact nature of the disruption and the details of the known failure. At this stage it will be the responsibility of the Assurance Desk to inform all affected customers via email and/or text message. Updates will be provided on a regular basis (every four hours) until fault restoration. For all Major Service Outages (MSOs) a full RFO report will be provided as part of the communication.

Reverting to a normal service in the event of a failure or MSO will follow a procedure whereby all necessary testing is completed within the Assurance and Technical Engineering teams. These teams will initially follow up through direct contact with named representatives within the customer's organisation. All relevant checks will be completed by both parties to ensure all services and deliverables are working correctly prior to any buyer sign-off.

This service does not offer hosting.

1.9 Access to data (upon exit)

Data is stored in a secure and resilient N+1 environment and, where applicable, is subject to near real time replication/mirroring across diverse geographic locations. In the event of an incident, including loss or degradation of resilience, the incident will be managed in line with an established procedure to ensure customer SLAs can continue to be supported. Should the customer require access to data upon exit, a plan will be put into place for requesting the data via the customer's Account Manager.

1.10 Security

Should intelligence or alerting indicate any potentially malicious activity, TTB operates a robust security incident management programme, and has deployed industry-leading endpoint protection technology (security solutions designed to protect endpoints—devices like laptops, desktops, servers, and mobile devices) to defend against advanced threats as part of our incident response program.

TTB has implemented an Information Security Management System based on industry good practice (NIST CSF, PCI DSS) and is externally certified to ISO 27001. This covers a range of policies and procedures (e.g., IP/TLS) to ensure the confidentiality, integrity and availability of information. Standard security protocols are followed for private network connectivity. The DDOS service has no additional security requirements as the security elements lie within the private network. The TTB Security Operations Centre (SOC) facilities are manned 24x7x365, providing a near real-time response to security events with an escalation process to senior management as required. Our 24/7 SOC performs extensive monitoring of internal and external security controls, coupled with curated threat intelligence feeds, and real-time alerts are activated if suspicious activity is detected. Incidents are triaged based on risk and impact and playbooks have been developed to focus on containment, eradication and recovery activities in-line with NIST best practices. TTB conducts security scanning of all its infrastructure on a bi-weekly basis. We also conduct weekly threat and vulnerability scanning of all our network assets via InsightVM. Critical/high risk vulnerabilities patches are applied within 14 days. All other updates are applied as soon as possible using a monthly patching cycle. Security updates are assessed and prioritised based on threat level, likelihood of compromise, consequences of compromise, environmental characteristics and regulatory or accreditation-based requirements. TTB gets its information about potential threats from InsightVM for scanning, Altiris Patch Management.

Version Control

Document Amendment History Log						
Document Owner	Andrew Stokes					
Created Date	28-01-26					
Author	Paul Ducklin					
Next Review Date	28-01-27					
Version Number	**Modified date**	**Amendment history**	**Reviewed by**	**Approved by**	**Approval date**	**Approval evidence**