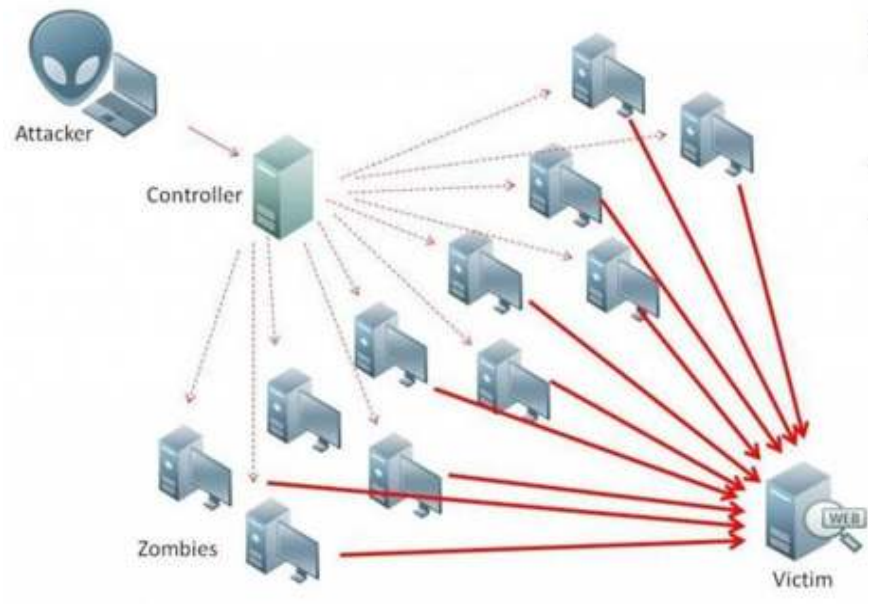
LIBERTY GLOBAL'S ANTI-DDoS

WHAT IS A DDOS ATTACK?

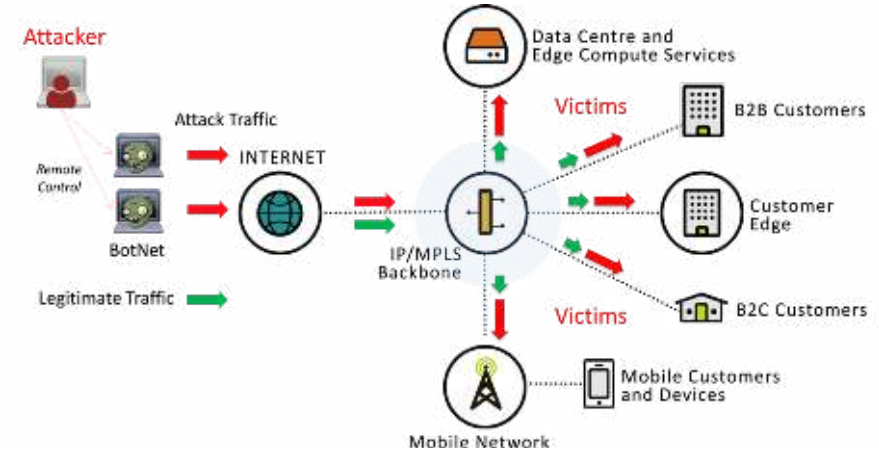
Distributed Denial of Service (DDoS) is a particularly malicious form of cyber-attack which occurs where multiple compromised computer systems are controlled and used to target a single system or end user. This overwhelms not just the end victim but also the associated network links, firewalls and web servers soaking up bandwidth and causing a severe denial of service.

The attacker gains control over a large network of online devices in order to carry out the attack. Home computers and other internet connected devices infected with malware turns each one into a 'bot'. The attacker has remote control of many bots (collectively called the 'botnet') which may consist of hundreds of thousands of devices. With remote control established, the bots can be instructed to send data (attack traffic) to the victim and overwhelm it. As a result, the victim becomes either slow to respond or unresponsive. This has a severe impact since it can completely paralyze your business for multiple days.



Types of DDoS attack

There are many types of DDoS attack techniques (called 'vectors') that can be used to overwhelm the victim. Examples are HTTP floods, TCP/SYN floods and UDP floods. The more complex attacks consist of a blend of different attacks referred to as 'multi-vector attacks'. DDoS attacks can have many motives - political, commercial, financial or personal, and may also be a smokescreen for other malicious activity such as data theft. Performing a DDoS attack is extremely easy since they simply can be ordered on the internet. An amateur can have the power to shut down a whole network if they pay enough money.



Liberty Global DDoS protection

Liberty Global is actively protecting its infrastructure, services and customers from DDoS attacks. Firstly, on our edge routers where we connect to the Internet and our customers, we manually apply filters according to industry best practice. Secondly, we have an Arbor anti-DDoS platform that looks for DDoS attacks by continuously analysing traffic that enters our network.

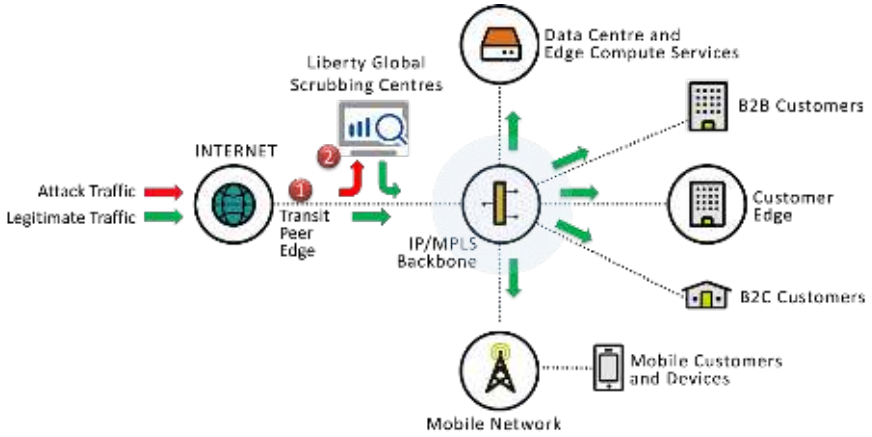
Arbor platform

Liberty Global uses a number of tools and methodologies to protect our network and customers from attacks, such as the Arbor Platform. Netscout is the market leader for anti-DDoS and protects 90% of the world ISPs.

- Arbor SP provides an analytical tool whereby internet traffic can be analysed to aid planning, management and identify potential attack traffic.
- Arbor TMS provides protection against DDoS by surgically removing the offending attack traffic, allowing the legitimate traffic to continue to its destination

When a DDoS attack is detected, the Arbor platform will automatically take one of two actions:

1. Instruct our edge routers to remove the attack traffic.
2. Instruct our edge routers to send the attack traffic to a network 'scrubbing centre' for removal.



The choice of action is relative to the complexity of the DDoS attack. If it detects likely DDoS attack traffic it signals the network using BGP - Border Gateway Protocol which is a standardised exterior gateway internet protocol designed to exchange routing information, to redirect the victims traffic to an appropriate Arbor TMS (Threat Mitigations System). The platform is fully resilient, so if one TMS fails, then another is chosen. The TMS will scrub the traffic to remove the attack element. The legitimate traffic is returned to the victim who will notice little or no impact to service.

Complex DDoS attacks are sent to the Arbor scrubbing centres. The scrubbing centres have the capability to process hundreds of gigabits of traffic in addition to the filtering capacity of our peering edge routers. During April 2020, our Arbor anti-DDoS platform detected and removed 14,380 attacks against our infrastructure and customers.

B2B DDOS PROTECTION SERVICES

Liberty Global's commercialized anti-DDoS solution is a premium service that is offered to our B2B customers in eight markets. B2B customers are given access to our own portal that protects our own infrastructure where they are able to fine-tune some parameters and view details and prevent DDoS attacks against them.

The B2B DDoS (Distributed Denial Of Service) Protection Service is an 'add-on' service to the Internet and IP Transit Services and is based upon the European backbone of Liberty Global. The DDoS Protection Service is permanently switched on and works automatically with the need of human input.

DDoS Protection Service Overview

The TMS (Threat Management System) appliances are located in 'scrubbing centers' within the Liberty Global backbone in the UK, Netherlands and Germany. The distribution of the mitigation function ensures the capability to encounter even large scale attacks.

The TMS selected to mitigate an attack is normally the closest to the attacker. So if an attack is coming from the USA for example, the traffic will be 'scrubbed' in the UK. However, traffic could also be forward to a specific TMS if needed.

DDoS attack detection

DDoS attacks are detected by obtaining netflow data from pre-defined provider edge routers (PEs). Attacks detected include generic flood attacks, fragmentation attacks, TCP stack flood attacks, connection attacks and application attacks.

DDoS attack mitigation countermeasures

The mitigation countermeasures taken can be grouped into per-packet countermeasures and application-specific countermeasures.

The DDoS Protection Service Description

Service SLA

The DDoS Protection Service Option of the Business Internet or IP Transit comes with a 7x24h support time SLA. It is 7x24 standby and will automatically kick in within 60 seconds.

Service implementation

IP ranges

The IP ranges included in the DDoS Protection Service reflect the IP ranges of the Business Internet or IP Transit services.

Implementation

The initial setup of the mitigation is done in close cooperation with the customer and will generally be finalized with 2 weeks. In the event that a beginning customer is being threatened with
an attack, LG will put in all effort to speed this process up.

Service pricing and billing

DDoS service pricing includes an initial setup fee (one time charge) and a fixed monthly recurring charge. The price will not be affected by the quantity of attacks.

Customer Portal

Part of the service is a customer portal. This portal provides the customer with detailed information about his Anti-DDoS service like detailed profile information and a history of DDoS attacks.