DDoS Mitigation

Following an increasing number of high-profile DDoS attacks, we have launched a new service giving protection against these increasing occurances. We are now able to provide protection against DDoS attacks up to 500 Gbps. Through our dedicated dashboards, our skilled engineers can see when an attack occurs and can inform you or take the relevant actions immediately.

What is a DDoS attack?

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

What kind of businesses get attacked?

Unfortuantely, the answer to this is: any business. Although, common targets are gambling or gaming targets. As an example, Custodian had a 25Gbps attack on a web site hosted by a client who sold 'plastic toy soliders'. DDoS attacks are now so easy to launch that any business is now a potential target.

How does DDoS Protection work?

As your network provider we will monitor trafic closely, for large scale DdoS attacks the mitigation service will be turned on as soon as we notice the attack, for small scale attacks notification from clients or confirmation will be needed.

There are 11 scrubbing centres in 11 global Data Centres (THN London is just one of them) and the service is delivered identically with an ISP upstream link.

Prefix's are advertised to our provider once we have seen an ack and will be un announced from other peers. For "sensitive" prefixes which are commonly under attack - we are able to offer a permanent announcement to our provider with the possibility to change mitigation status for each IP independently.

The anti-DDoS scrubbing cluster is based on a two-layer protection system: first there's an ACL layer on the border/edge routers capable of collecting attacks up to 500Gbps.

This layer is used for filtering attacks with known sources and/or de-amplify-ing an attack with spoofing components.

The second layer is based on a reverse proxy linux cluster which can (if-needed) decapsulate every packet up to layer 7 (including layer 7) in order to filter the traffic and pass towards the client only the legitimate component of the traffic.

To enquire about implementing our DDoS Mitigation service for your business, call a member of our team on

01622 230382 or email **Info@CustodianDC.com**

Common types of DDoS attacks that can be mitigated:

- IP non-existing protocol attack
- Attack with fragments
- ICMP attacks
- TCP attacks
- UDP attacks
- HTTP attacks
- Misused application attack
- Slow read attack

Forms of prevention our provider employs to keep your traffic free of DDoS attacks:

- Significant Network Edge Capacity (<Tbps)
- Special arrangements with some Asian Networks to stop attacks coming from China
- 11 scrubbing centres located in Amsterdam, Bucharest, Frankfurt, London, LA, Miami and Washington DC (Equinex LA 1, Terrermark NAP, Telehouse North, Telecity Meridian Gate, Equinex FR5, Interxion FRA3, Interxion FRA8, Telecity 2, NXDATA1 & NXDATA2, Voxility, IRD)
- Controllod mitigation process

Once an attack has been identified and DdoS mitigation is switched on, how does Filtering work?

Once a subnet is advertised to our provider – Custodian will use the following states to address each IP:

"sensor"	"always on"	"always off"
Detects and starts DDoS mitigation on the traffic only when a DDoS attack is detected	Traffic is always filtered against DDoS attacks, good for IPs that are very sensitive to abrupt load of traffic, but we do not recommend this status unless is necessary	Doesn't filter the traffic against DDoS attacks whatever happens. For first 2 states layer 7 filtering can be disabled. Layers 2, 3, 4 and 7 are inspected, anti-spoof is implemented for TCP (layer 3) to HTTP bots (layer 7)

If you are using our anti DDoS with layer 7 filtering (reverse proxy), when you receive an attack toward web server port 80, the content of your site is cached by DoS filter. Only non-cached filtered traffic will reach your server.

Reverse Proxy is an army of web servers that cache your content and multiplies the capacity of your server hundreds of times. As a side effect it accelerates web-content delivery. Content that cannot be cached is passed to your server after the user-initiated session is checked against possible malformations. All the IPs announced initially with a DDoS protected dedicated server are in status "sensor" mode by default after importation, but we can manually change the status if you send us an email once you start testing/using the service.

How "Sensor" mode works?

When there are no attacks detected, the traffic flows directly to your equipment as in normal mode of operation, Custodian has sensors to detect attacks everywhere in the network. When a suspicious pattern is detected, traffic toward that IP is redirected for mitigation in the same data centre Security Cloud. The network sensors detect instantly when an attack occurs and redirects traffic in seconds from the affected IP to the mitigation cloud. Redirection automatically stop within minutes after the attack ends.

How "Always on mode" works?

Instead of permitting traffic to flow directly toward your server, this protection mode permanently applies the anti-DDoS filters. Basically, the traffic flows permanently through our DDoS mitigation service providers Security Cloud.