DDoS Protection

Your Network, Protected

Global Secure Layer

Our solution

Distributed denial-of-service (DDoS) attacks are one of the most complex security challenges of the modern internet. At Global Secure Layer, we understand the magnitude of these attacks and the impact they can have on our customers if not mitigated quickly and efficiently.

Our protection as a service is provisioned at our global networks edge, using real-time technology to match and protect against even the most sophisticated attacks. Our industry-leading technical team inspects, detects and mitigates entirely inline across our worldwide Anycast network.

Our global protection currently stands at multi-terabits of mitigation capacity. We are continuing to expand our footprint across borders in order to analyse, detect and mitigate attacks closer to the originating source.

When it comes to protecting your network, seconds make all the difference.

DDoS key features

Inline and automated
Our DDoS mitigation clusters operate inline at the networks edge - detecting and mitigating attacks in real-time. Our inline protection exceeds offsite mitigation architectures as it ensures all packets that enter our secure network are analysed with precision, guaranteeing only legitimate traffic reaches its destination.

Time to mitigate
DDoS attack response times are critical for any organisation - being offline for just a few seconds can have significant financial implications. With our ‘time to mitigate’ being under one second, we provide precise, automated and surgical mitigation capabilities.

Global infrastructure
Our global Anycast network allows us to mitigate across all of our international PoP’s. This provides a distributed mitigation surface allowing GSL to absorb the growing number of sophisticated attacks.

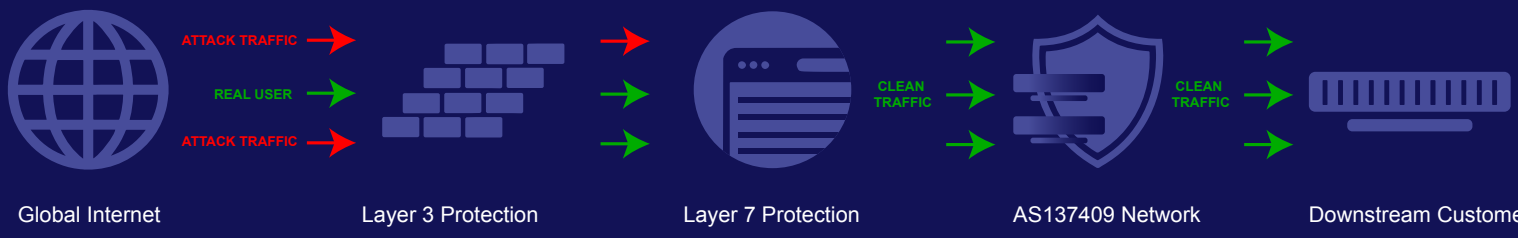
Mitigation engineers
Global Secure Layer has a dedicated NOC providing 24/7 assistance. Our team of industry-leading mitigation engineers are always available to assist you with specific attacks.

Included protection
All IP Transit services come with 20Gbit+ protection, with additional protection available to be purchased as a service.

DDoS portal
Our DDoS portal provides access to real-time reporting allowing you to instantly see when an attack is happening.

Protects all industries
Our DDoS protection can be tailored to meet the security needs of all industries.

Types of DDoS attacks



Volumetric

Volumetric attacks are designed to overwhelm network capacity. This type of attack sends a high volume of traffic or request packets to a specific target with a goal of saturating the bandwidth.

Usual request sizes are in the 10's of Gbps; however, recent attacks have scaled to over 1Tbps. Volumetric attacks can happen to organisations of any size and anywhere in the world. The techniques deployed often result in traffic originating from multiple sources. As a result these attacks are much more difficult to manually mitigate.

Reflective & Amplification

Reflective and amplification attacks use a small amount of traffic from a source that is then amplified via servers and targeted towards a victim's IP.

These requests start small and turn into large attacks - an example of this vector is 'Memcached' which targets port 11211 and has an amplification factor of up to 51,200 x the original request size. This is concerning for all industries, because even a small 10 byte request would be amplified into a 512Kb response targeted towards the victim.

Resource Exhaustion

This type of attack targets a specific application, with a sole purpose of overwhelming the individual applications computational resources. This involves the attacker sending traffic that appears to be legitimate traffic at a 'slow rate' so as to not be detected by traditional mitigation measures. This vector typically targets web servers using a form of 'slow injection' in the hopes to exploit the web servers code and cause legitimate users not to be able to access the website.

This form of attack is difficult to detect with traditional mitigation since it is extremely small and may only require a single computer to execute. Our protection is able to find, identify and surgically remove the attack traffic before it reaches the intended destination.

Gaming Specific

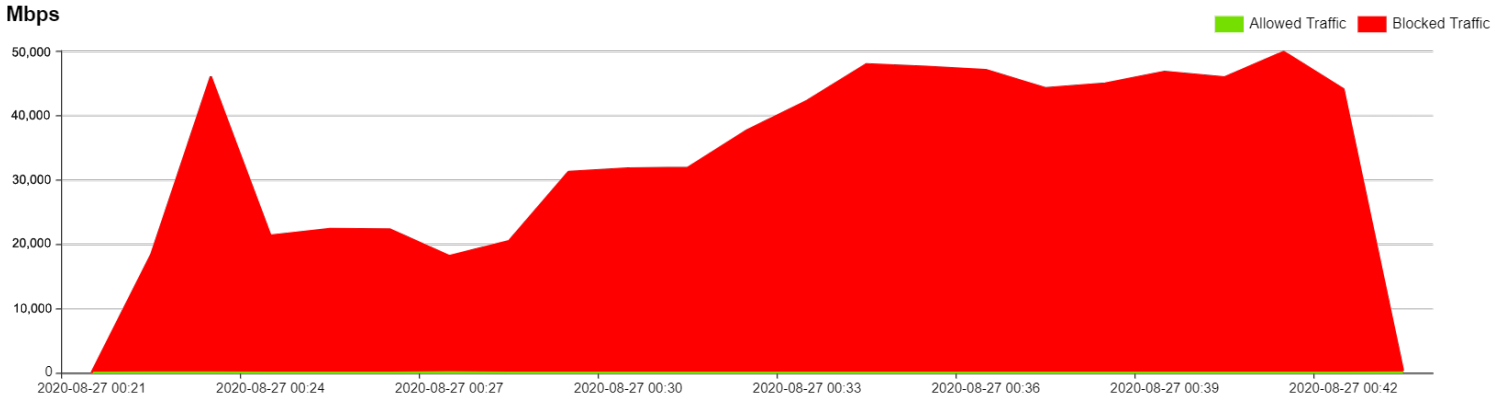
Similar to resource exhaustion, the aim of this attack is to prevent users from joining by overwhelming the host servers' resources by targeting an exploit in the code. This type of attack is specifically related to the gaming industry, which can also have a knock on effect to other industries. These attack types are becoming more common as the world shifts and brings gaming into the spotlight.

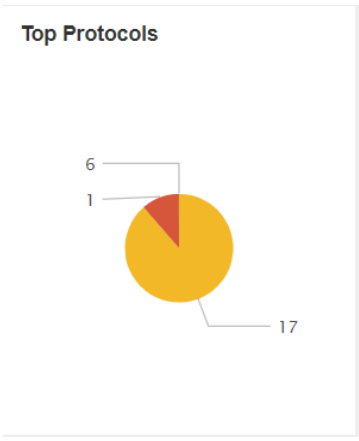
An example of this vector involves sending a specific 'spiked' payload to the target machine, with the hope that the game application unpacks the payload, loads it and executes it resulting in CPU/memory exhaustion causing the server to become unusable.

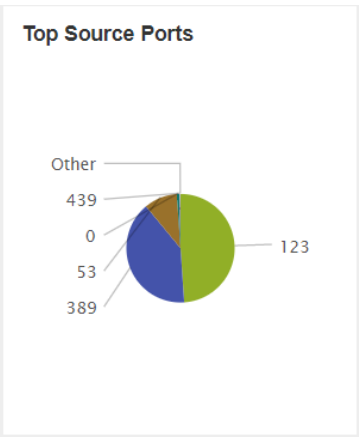
Security coverage

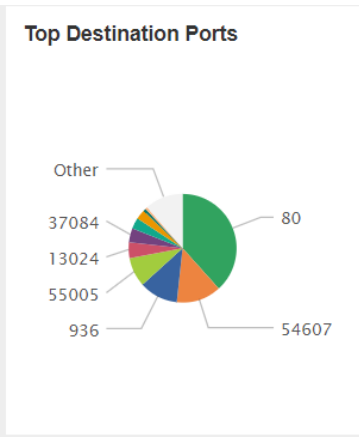
ATTACK COVERAGE			
Volumetric Coverage	**Reflective & Amplification**	**Resource Exhaustion**	**Gaming Specific**
• TCP Flood » ACK » PSH » SYN » RST • UDP Flood • UDP Fragmentation • ICMP Flood » Ping of Death » Failed Reflectors	• NTP Amplification • SSDP/UPnP • SNMP • Chargen • Smurf • Fraggle attack DNS • DNS Amplification • LDAP • RIP • TFTP • Memcached	• Malformed & truncated packets • IP fragmentation • Invalid TCP segment ID's • Bad Checksums • Illegal TCP/UDP flags • Invalid TCP/UDP ports • Reserved IP address	• A2S Source Flood • A2S GETSUM • FiveM Exhaustion • RTFM Request • TS3INIT • NetBIOS

Real-time protection in action









An example of our mitigation appliances surgically removing a Multivector Volumetric attack.

For more information on our DDoS Protection, please contact the team at GSL.