Global Secure Layer

DDoS Protection

Your Network, Accelerated

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 network 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 100Gbit 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.

Volumetric

Global Secure Layer is a tier 2 network operator with an international Anycast infrastructure providing IP Transit. Our solution is a blend of tier one providers, global content networks and major peering exchanges. We focus on establishing direct interconnects and bilateral peering with numerous providers allowing us to achieve route optimised connectivity and a high level of diversity.

GSL provides a large range of industries including all levels of government, enterprises and ISPs with worldwide carrier-grade internet that is secured end-to-end with industry leading DDoS protection. We build our infrastructure with a redundant fibre backbone to meet the needs of our 24/7 connected world.

Our global network solution has been built on a world-class fibre network with a focus on low latency, resilience and scalability ensuring our customers stay globally connected.

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.

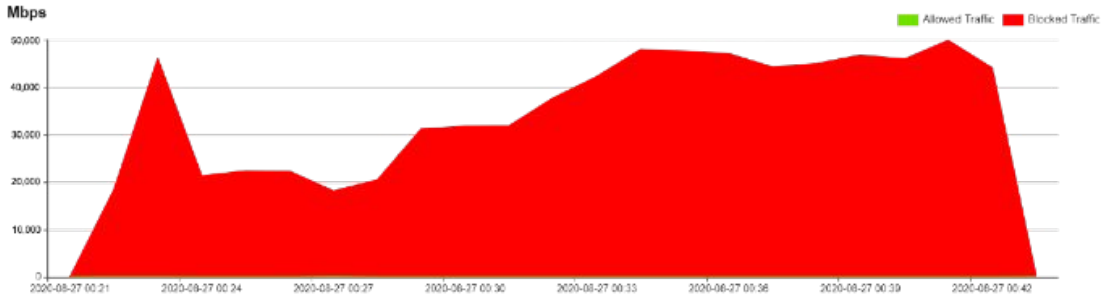
An example of this vector involves sending a specific 'spiked' payload to the target machine, with the hope that the game application unpacks the payload, loads it and executes it resulting in CPU/ memory exhaustion causing the server to become unusable.

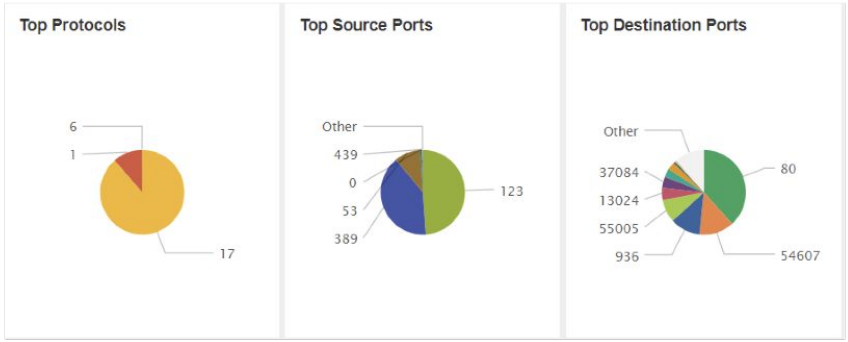
Security coverage

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 Reflections
	• 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
		• Baad 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

CONTACT INFORMATION

For more information about Global Secure Layer and our products, please contact:

Sean Aikins
Sales Director

Email: sean@globalsecurelayer.com
Phone: +61 459 469 489