sure. business

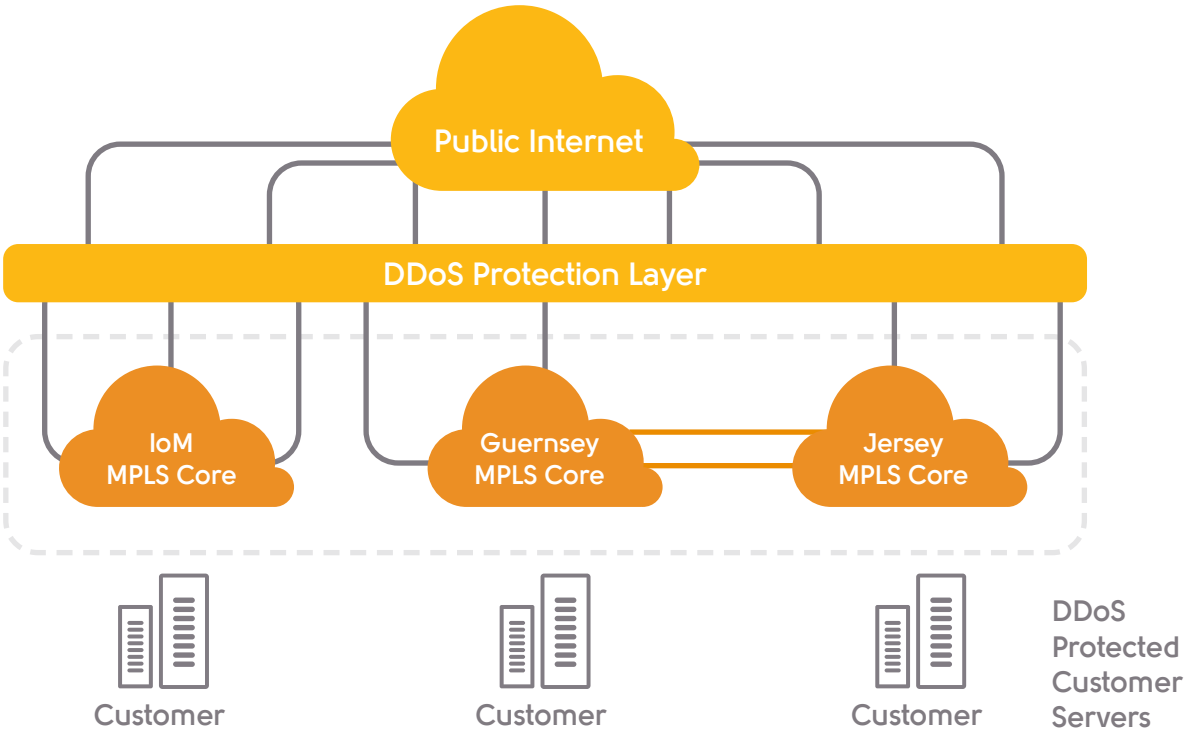
Cybersecurity Solutions
Distributed Denial of Service (DDoS) Protection

Denial of service attacks have plagued network and data centre operations since the early days of the Internet - and they are here to stay. They are no longer a problem solely for major online organisations or gaming and betting sites. A wide range of companies from retail to finance sectors increasingly depend on web-based transactions and might be affected. Additionally, the Internet grows more complex each year, and there is greater demand for highly available Internet connectivity as businesses access more cloud-based services.

To maximise the protection and security that our clients and networks need, Sure uses a combination of in-line and dedicated attack mitigation solutions.

The Sure Solution for DDoS Protection

The Sure solution integrates network-wide intelligence and anomaly detection with carrier-class threat management to help identify and stop volumetric, TCP state exhaustion, application layer and other DDoS attack vectors.



Our on-net dedicated network devices provide the vital, traffic-scrubbing component. This supports a mitigation architecture called "diversion/reinjection". In this mode, only the traffic stream carrying the DDoS attack is redirected to those dedicated devices through routing updates. These mitigation devices remove only the malicious traffic from that data stream and forwards the legitimate traffic to its intended destination.

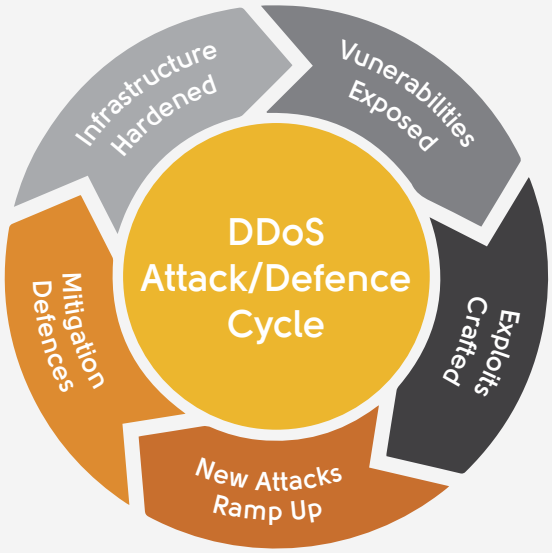
The Sure in-line core router based DDoS mitigation has the ability to remove malicious traffic in the same way as the dedicated on-net solution, but with much greater performance and capacity, scaling to multiple 100's of Gbps. This is highly advantageous for any public facing web presence as it enables a single, centrally located solution to protect multiple links and data centres. It results in much more efficient use of mitigation and fully non-intrusive security.

Comprehensive Threat Detection

Data centres and public networks present multiple targets for DDoS attacks. These targets include infrastructure devices (e.g. routers, switches and load balancers), Domain Name Systems (DNS), bandwidth capacity and key applications such as web, eCommerce, voice and video. Even security devices such as Firewalls and Intrusion Prevention Systems are targets of attack. The Sure DDoS mitigation solution provides the most comprehensive and adaptive suite of threat detection capabilities in the industry, designed to protect diverse resources from complex, blended attacks. These capabilities include statistical anomaly detection, protocol anomaly detection, fingerprint matching and profiled anomaly detection. Our solution continually learns and adapts in real-time, alerting operators to attacks, as well as to unusual changes in demand and service levels.

Management & Support

The entire Sure DDoS platform, both in-line and dedicated, is managed by a team year-round 24/7, comprising our dedicated Service Operations Centre (SOC) supported by Sure's own IP Engineers and backed by the solution vendors. The "Team" is available whenever they are needed, to support all our DDoS customers and to ensure that any DDoS mitigation, traffic profiling, DDoS platform and portal configurations are performed to the highest security standards.



Business Continuity
No service or business downtime due to DDoS

Ransom Resilience
Confidence to ignore DDoS ransom threats

Traceability
Know which traffic was/ wasn't blocked as DDoS and why

Mitigation in Seconds

Key to effective mitigation is the ability to identify and block attack traffic while allowing non-attack traffic to flow through to its intended destination. Large-scale DDoS attacks not only affect the intended victim, but also other unfortunate customers who may be using the same shared network. To reduce this collateral damage, Service Providers and Hosting Providers often shut down all traffic destined for the victim's site, thus completing the DDoS attack. Whether it is a high-volume flood attack designed to exhaust bandwidth capacity or a targeted attack looking to bring down a specific website, Sure's DDoS solution can usually isolate and remove the attack traffic, without affecting other users, in a matter of seconds. This rapid response is especially important as more than 85% of attacks last 10 minutes or less.

Methods include identifying and blacklisting malicious hosts, IP location-based mitigation, protocol anomaly-based filtering, OpenVPN reflection, malformed packet removal and rate limiting (to gracefully manage non-malicious demand spikes). Mitigations can be automated or operator-initiated and countermeasures can be combined to address blended attacks. Automated mitigation is beneficial as it allows attack vectors that have been "in the wild" for months but only just seen to be detected and mitigated.

Advisory & Design

At Sure we have a team of specialist consultants with expertise in designing and optimising customer networks including Internet, hosting & security solutions. Ask your account manager how Sure's Advisory & Design Services can help modernise your infrastructure.

Real-Time Response

Detection and mitigation in seconds, rather than the minutes or tens of minutes taken by legacy solutions, ensuring online business continuity.

Automatic Mitigation

Accurate automatic mitigation delivers lowest TCO and enables your IT and security teams to spend more time defending against other threats.

Clear Actionable Intelligence

Comprehensive visibility with reporting and alerting for clear, actionable intelligence on the DDoS attack activity across the network.

Sure's dedicated DDoS mitigation solution provides a "cleaning" capacity of up to 2x40Gbps of returned clean traffic. Sure's in-line DDoS mitigation solution provides a cleaning capacity of up to 500Gbps, and would normally be used for very large volumetric and high packet rate attacks. Overall mitigation capacity is important as there has been a 70% growth in attacks over 10Gbps. Note in both dedicated and in-line mitigation the attack is mitigated before the traffic reaches the Islands.