UQSchoolsNet

DDOS (DISTRIBUTED DENIAL OF SERVICE) PROTECTION

This service monitors the inbound consumer Internet traffic via edge routers and automatically mitigates DDoS attacks when detected.

A DDoS attack is a malicious attempt to make an online service unavailable by overwhelming it with traffic. DDoS usually uses a network of compromised systems to flood sites with connection requests, causing the website or server to slow down or crash entirely. DDos attacks increased globally by 80% in Q1 2020 compared to Q1 2019, and they continue to rise.

The DDos Protection Service focuses on Layer-4 characteristics of UDP, ICMP & TCP (SYN, RST, PSH/ACK, SYN/ACK):

- Service protection - flood of packets with the same destination port.
- Server protection - flood of packets with the same destination IP address.
- Reflections - flood of packets with the same source port.

And common DDoS attack methods (including payload inspection):

- DNS query response reflection.
- NTP Monlist response.
- SSDP reflection.
- Empty UDP data.
- Memcache attack.
- ICMP rules look for a flood of packets with ICMP error messages.

There is no set-up required on customer networks and no disruption to legitimate traffic.

As part of our internet services, the DDos Protection Service will safeguard your internet links from the increasing cyberattacks portrayed.

The University Of Queensland
AUSTRALIA

CREATE CHANGE