

Simple UDP Flood

Protecting legitimate customers

Simple UDP floods are one of the simplest attacks.

An attacker can take a single web server offline that resides within a network, on a 100Mb link, and typically sees around 30 Mbps of TCP web traffic. To do this, the attacker can instruct as few as 5-10 bots to send a total of 300 Mbps of large UDP packets to the web server's IP address. This will cause 2/3 of packets to be dropped by the switch directly upstream of the server. With this degree of packet loss no TCP connections can be completed and the attack is successful.

Any anomaly-based DDoS Protection System deployed near the front of the network would be sure to detect such a significant increase in traffic. It would either:

- notice a significant portion of UDP traffic if there was usually very little. It could then block all the UDP traffic, which would block the attack but could deny legitimate customers access.
- notice that a small number of IP addresses are sending far too much traffic and black-list those addresses, but could at the same time inadvertently also block some legitimate customers.

IntelliGuard's DPS achieves the same goal differently. In less than 1 second it will detect traffic exceeding a 100 Mb limit set for the webserver. It will then give preference to legitimate customers causing the attacking IP addresses' traffic to be dropped.

