

Case Study – Taiwan online gaming provider

The Customer

The anonymous customer is an online gaming provider with a large number of subscribers.

Network Configuration

100Mb link -> Layer 3 switch -> firewall -> IPS

Attack History

At least weekly the company's gaming servers were being hit with 30-60 minute bursts of SYN floods of up to 800 Mbit/s.

The IntelliGuard Visualization & Management Tool screenshot at right of screen was captured during one such attack. The charts depict aggregate bandwidth and packets seen by the IntelliGuard DPS, the bulk of which consisted of attack traffic (red) targeting a single server.

IntelliGuard DPS Deployment

An IntelliGuard DPS 2200 was installed in-line in between the Layer 3 switch and the firewall. The DPS automatically discovered all the gaming servers. Limits, guarantees, and connection protection settings were then applied to each gaming server.

Successful Defense

The DPS 2200 recognized and passed traffic from trusted sources while enforcing the configured traffic limits for each server, thereby keeping gaming services fully accessible to subscribers during attacks.

