DDoS Protection Service

Monitoring, detection and fast mitigation to ensure business continuity

Distributed Denial of Service (DDoS) attacks on Australia's research and education sector have become more prevalent in recent years. These attacks overload a target with a flood of internet traffic, disrupting critical online services, impacting productivity with potential financial and reputational implications.

AARNet's DDoS Protection solution helps customers manage DDoS attacks and the risk of business disruption. We've developed a system for the research and education sector that efficiently detects, filters and mitigates attacks well before they reach your campus network.

Using AARNet's extensive international and domestic network of border routers, real-time traffic analysis and automated application of firewall filters, mitigation of attacks can occur in seconds, significantly faster than most current commercial offerings. Legitimate traffic is unaffected, following its normal route, without limitation or disruption.

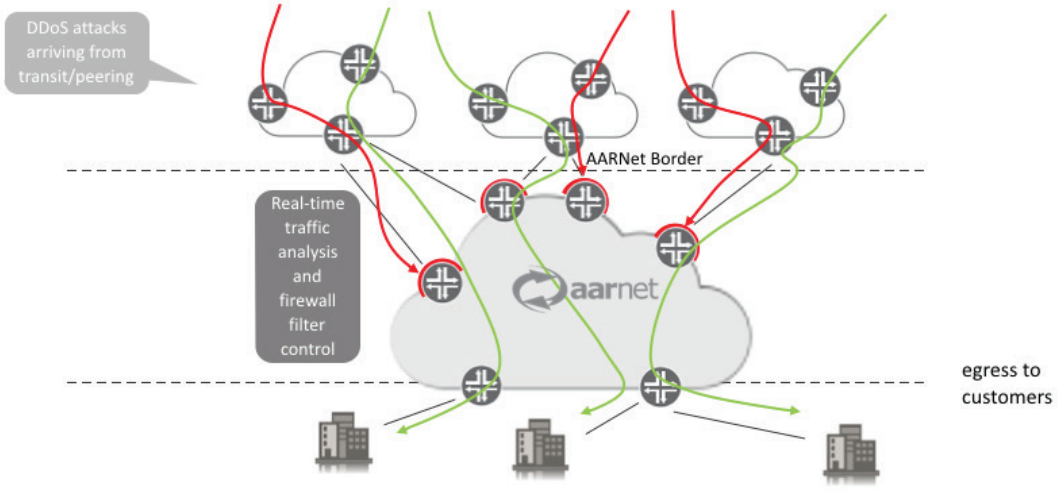
Benefits

- **Critical Asset Protection**
  Attacks are filtered fast to safeguard the availability of your internet connection, websites and online resources.
- **Managed Solution**
  Cost-effective protection from DDoS attacks without the need for specialist staff in-house.
- **Monitoring & Support**
  Proactive 24/7 monitoring and support from our Operations Centre network engineers.
- **Customer Portal**
  View your protected assets (named IP ranges), as well as traffic graphs and statistics for blocked and allowed traffic in one place.

How does it work?

AARNet border routers send sampled traffic and streaming telemetry back to our analytics and control systems. Firewall filters are applied to our border routers, blocking attack traffic, all within seconds. Legitimate traffic passes through untouched.

With our system, attacks are detected and responses automated according to an agreed policy and rule set. There is no need to re-route traffic to and from scrubbing centres. Our approach saves time and avoids disruptions to legitimate traffic.



Border routers are located globally in Asia, Europe and the US and domestically in most capital cities.

Pricing

- One-off onboarding charge.
- Fixed annual charge, based on the size of your organisation.
- There are no usage charges, bandwidth caps or other unexpected costs.

Manual interventions to mitigate DDoS attacks take precious time. Even the commercial DDoS scrubbing services take minutes to respond and can fail to avoid business disruption.

AARNet DDoS Protection	V	Traditional DDoS Scrubbing Services
Mitigates in seconds.		Slower to mitigate. Usually a manual re-routing to scrubbing.
No disruption to legitimate traffic.		Re-routing to scrubbing centres causes disruption to legitimate traffic.
No set-up required on campus network.		Detailed on-campus configuration required for re-routing and GRE tunnels. Multiple dependencies and high risk of disruption.
Samples live traffic, analysing packet header and payload characteristics, for accurate detection and filtering.		Typically analyses Netflow data (header only) to detect attacks. Less accurate and risk of overload during attack.
We own and operate our network and have full control over traffic throughout.		Can restrict traffic throughput due to commercial and technical constraints.
Automated filter clean-up with no business impact.		Manual resumption of normal traffic flows, risking further disruption.
Fixed cost for your whole network.		Variable cost subject to increases for more IP ranges and greater throughout.

More information:

Contact your AARNet Customer Relations representative
CustomerRelations@aarnet.edu.au

AARNet is an AHECS partner

AHECS AUSTRALASIAN HIGHER EDUCATION CYBERSECURITY SERVICE (AHECS)