HAPROXY

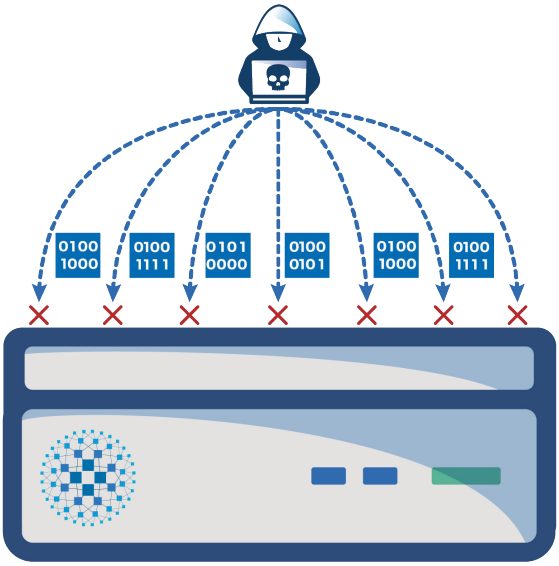
DATA SHEET

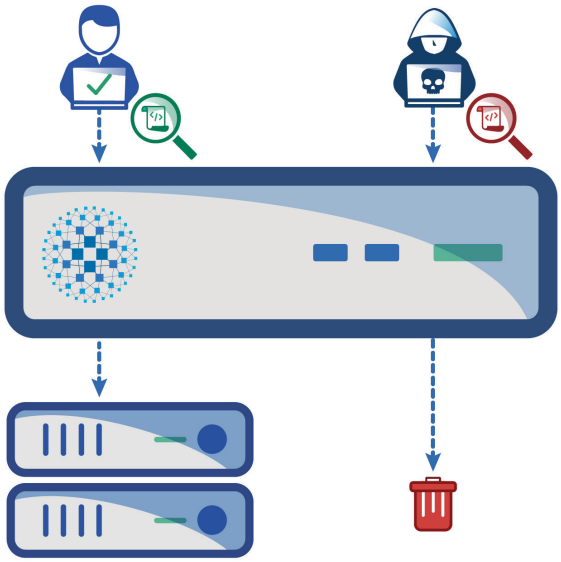
ALOHA PACKETSHIELD

The First Defense Against DDoS Attacks

Distributed denial of service attacks (DDoS) are designed to saturate network equipment and server resources (firewalls, load-balancers, etc.) in order to make a site or service unstable or unavailable to legitimate traffic.

More and more common, both in terms of scale and sophistication, these attacks have a real cost to companies in terms of loss of turnover, service interruption, impact on company image as well as financial blackmail all leading to a decrease in profit...





PROTECTION AGAINST DDOS

ALOHA PacketShield offers a simple, efficient and cost effective response to DDoS attacks :

- Wire-Speed packet analysis, in front of the firewalls, load-balancers and web-servers
- Real-time filtering and blocking of unwanted traffic, whilst maintaining access for legitimate traffic
- Patented solution guaranteeing zero false positives
- Traffic recognition via customizable access lists

TYPES OF PROTECTION

- Protocol verification: automatic blocking of badly formatted
- Protection against SYN Flood attacks: transmission of SYN cookie
- ACK/RST flood attack prevention, with stateful packet inspection
- Protection against ACK attacks from NAT equipment itself under attack
- Prevention of DNS amplification attacks using valid response recognitions

THE FIRST DEFENCE AGAINST NETWORK DDOS ATTACKS, PACKETSHIELD CAN BE :

- Deployed as a router, or load-balancer (L4 or 7),
- Combined with any other load-balancing solution, for example HAProxy or ALOHA Load Balancer, for multi-layer network and application protection.

	PacketShield 3200	PacketShield 5200	PacketShield 5200 - 10G
Bandwidth	1G	1G	10G
Max. Number of Connections	Unlimited		
Packets Processed / Sec.	1 000 000	1 000 000	14 000 000
Deployment Mode	Inline router, inline L4 load-balancer, inline L7 load-balancer		
High Availability	Active / Passive or Active / Active		