Assure
Advanced Performance Management

Barbarians at the Gates

DDoS Attacks are Still a Problem

Whatever sector your business operates in, you still have to consider the threat that DDoS poses to your online assets. Distributed Denial of Service (DDoS) attacks is based on the premise that any service has limited resources, whether network bandwidth, memory or TCP state tables if those resources are exhausted, your service will go down. DDoS attacks typically fall into one of three categories:

- Volumetric: based on an attempt to overwhelm the target's inbound network bandwidth with junk traffic, a volumetric attack often leverages amplification vulnerabilities within the Internet infrastructure, such as DNS.
- TCP state exhaustion: all hosts maintain a TCP state table that tracks the status of TCP connections. A TCP state exhaustion seeks to prevent the target from accepting new connections by filling the state table with junk or "half-open" connections.
- Application layer: also known as "low and slow" attacks, since the volume of attack traffic is small, application layer attacks rely on a vulnerability within the application stack to crash service components.

Whilst DDoS attacks have been a problem for some time, the wide availability of DDoS tools and the proliferation of botnets and amplification vulnerabilities in core Internet infrastructure has made a massive scale DDoS attack well within the capabilities of even the most non-technical user. Everyone is a potential target.

A Layered Defence Strategy

Each of the attack types, described above, demands a different strategy for mitigating or preventing them, meaning that a layered approach to DDoS prevention is the best policy. Anti-DDoS technology is either cloud-based or appliance-based.

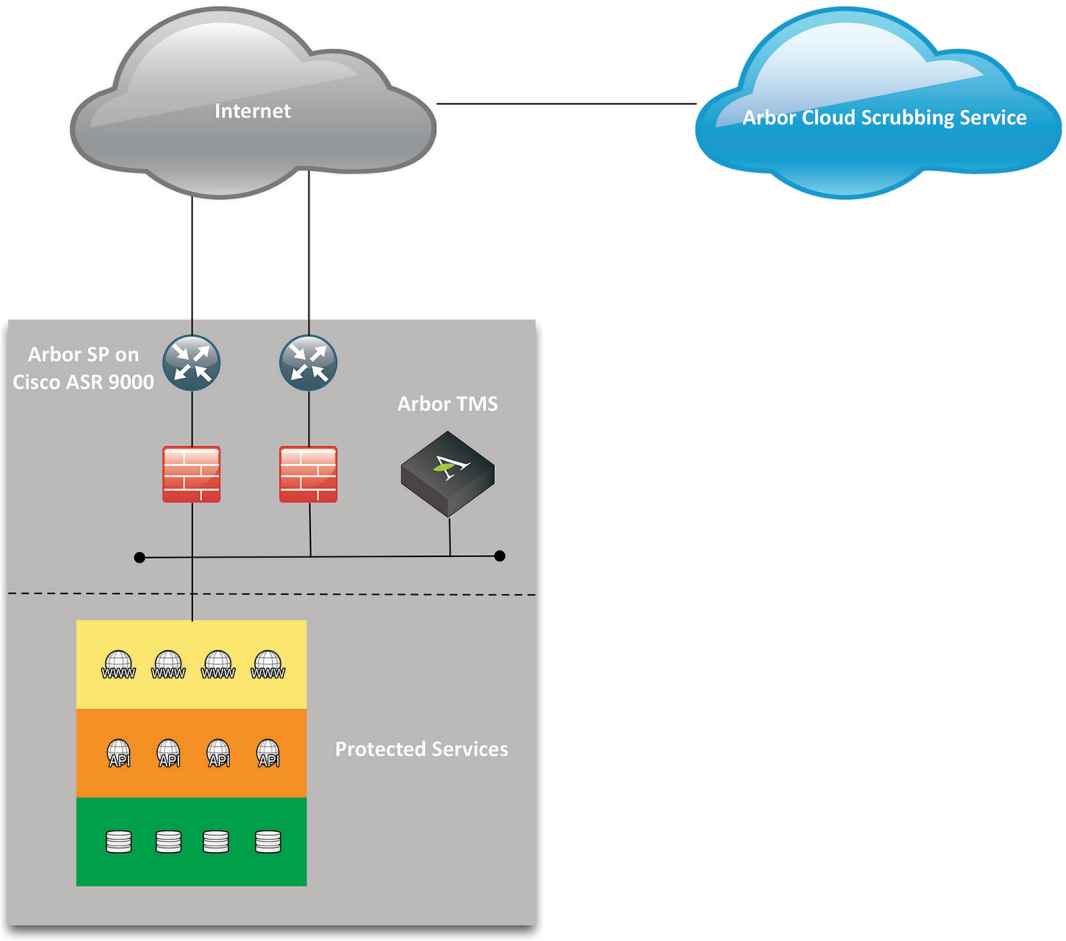

Figure 1 A Model Architecture for DDoS Defence

Cloud-based solutions are best placed to prevent and mitigate volumetric attacks. Implementing a cloud-based DDoS prevention service requires you to redirect your inbound Internet traffic via a vendor's data centre, which then carries out "scrubbing" on transit traffic to detect and drop DDoS traffic, before forwarding legitimate traffic on to your infrastructure.

Local anti-DDoS appliances are best for detecting and preventing TCP state exhaustion and application layer attacks. Appliances can be deployed inline, embedded within your perimeter routers, or out of band with traffic telemetry being forwarded via NetFlow, SNMP and BGP to detect attacks. Once an attack has been detected, attack traffic is forwarded to a scrubbing appliance, which drops malicious traffic before it hits your service infrastructure.

The Assure Service

Leveraging our unique insight into your application traffic through our Application Performance management and Micro-segmentation services, Assure can help to protect your infrastructure from DDoS attacks through our partnership with Arbor Networks. By integrating Arbor's market-leading portfolio of DDoS mitigation products with our unique application-centric solutions, Assure can provide comprehensive protection and visibility for your critical systems and services.

EDINBURH
Exchange Place 2
5 Semple Street
Edinburgh
EH3 8BL

LONDON
1st Floor
99 Bishopgate
London
EC2M 3XD

0131 677 8968
contact@assureapm.com
www.assureapm.com
@assureapm