RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

DISTRIBUTED DENIALS OF SERVICE (DDOS)

1/ DDoS ATTACKS, A PROTEAN THREAT

➔ There exist several types of DDoS attacks :

> **Volume-based**, aimed at exhausting available network bandwidth (ex. : an attack which consists in sending packets from multiple sources, in order to overwhelm a target – UDP flood ou ICMP flood);

> **Protocol-based**, aimed at exhausting a target's resources (CPU, RAM) by hijacking the operation of a protocol (ex. : TCP or SYN flood, smurf);

> **Application layer-based**, aimed at exhausting a target's resources (CPU, RAM) by hijacking the operation of a service (e.g. DNS water torture attack, in which servers are massively queried for existing DNS records).

➔ **These categories of attacks on availability are not exclusive**. Malicious actors can very easily and quickly adapt or combine their techniques over time. For example, an attacker might start with a volume-based attack but, later on, adjust their approach to the target's specific mitigation measures by switching to a protocol-based attack.

➔ **Preventive and reactive measures** can be implemented to limit the consequences of DDoS attacks. In the case of a targeted and very likely evolving attack, it is strongly recommended to call in experts for an **appropriate and specific response**.

(*) For example, DDoS scrubbing can involve criteria such as geolocation, protocol conformity, as well as packet and volume inspection for each protocol likely to be used in DDoS (e.g. DNS in UDP, NTP, CHARGEN).

2/ BUILD AND PROTECT

➔ **Restrict services exposed to the Internet to strict operational requirements.**

➔ **Acquire and implement an anti-DDoS protection service, dedicated to this function alone and specifically tailored to the IS which is to be protected :**

> from your service provider in the case of external hosting, which may already include an anti-DDoS service depending on the hosting package you have chosen;

> and/or from your Internet service providers (blackholing, DDoS scrubbing*);

> and/or from a professional service provider (BGP rerouting, DDoS scrubbing *).

The service selected **must offer protection against attacks at levels 3, 4, 5 and 7 of the OSI model**, for example by controlling bandwidth, limiting the number of requests, as well as implementing anti-bot protection and recognition of IP addresses deemed to be malicious.

In any case, **its collaborative implementation between customer and service provider** involves getting started with the solution, a parameterization suited to the entity's traffic and exposed applications (e.g. alert trigger thresholds), and **regular testing** to ensure smooth operation and the absence of side-effects. Procedures must be defined.

V2.0 (04/24)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

→ **Design a service architecture that distributes load and traffic over several subsystems** (data center, network failover mechanisms, load balancers, distributed servers, etc.).

→ **Scale a service architecture that takes into account fluctuating business needs**, such as bandwidth, memory and computing power, and storage capacity.

→ **Conceive architectures which make it possible to continue to administer a service exposed to the internet even after it has suffered a DDoS attack** (physically dedicated administration network, network partitioning of supervision flows, etc.).

→ **Design services exposed to the Internet in such a way that a DDoS attack on one service has no impact on the availability of other services** (separate Internet access chains, segmentation of network addressing plans, separate hosting providers, etc.).

→ **Configure perimeter firewalls :**

> enable only network and transport-level filtering (layers 3 and 4 of the OSI model) and disable application filtering functions (layers 5 and above);

> reduce incoming UDP flows to the bare minimum;

> anticipate the ability to temporarily remove connection tracking.

→ **Configure downstream application firewalls to protect websites** by setting session limits and applying malicious request blocking.

→ **Protect websites with a CDN (Content Delivery Network) for load balancing**. CDNs enable resources to be distributed across a large number of servers, which can help improve resistance to DDoS attacks. **Please note that some of these resources may be hosted abroad (potential impact on confidentiality).**

3/ ANTICIPATE AND REACT

→ **Set up a system for monitoring and detecting DDoS attacks**, in order to detect them as early as possible:

> use a log centralization system to facilitate downstream diagnosis of a DDoS incident;

> draw up and regularly test a procedure mapping out the course of action in the event of an attack, in close collaboration with anti-DDoS service providers .

→ **Plan a downgraded mode for critical activities in the event of a DDoS attack,** all the way throughout the remediation process. Bear in mind that your ISP may also impose a downgraded mode on its own infrastructure when suffering a DDoS attack, even if this attack does not directly target your entity.

→ **Make a regular inventory of services open on the Internet** in order to adapt the procedure for responding to DDoS attacks.

→ **Implement a crisis management system**, in liaison with your DDoS protection providers on the one hand, and your public relations managers on the other.

→ **Monitor, subsequently, other security alerts** generated during a "noisy" DDoS attack, which may be indicative of a more discreet, more serious attack.