QUICK REFERENCE

PROTECTING AGAINST DENIAL OF SERVICE (DoS) ATTACKS

Objective

Protect the company against denial of service (DoS) attacks.

The number of DoS attacks has increased in the last few years. These attacks happen frequently and can be made against any entity with a network infrastructure connected to the Internet. That’s why you need to anticipate this threat and take some technical and organizational measures to deal with it.

This document presents distributed denial of service attacks and a list of elements to take into account to protect against them. The document reviews some best practices to implement to avoid participating inadvertently in DoS attacks.

Document recipient: Network administrators

Last update: 2017-06

What is a DoS attack?

A DoS attack aims is to render one or more services unavailable. A DoS attack may, for example, involve exploiting a hardware and software vulnerability. The service interruption may also deny access to the service, for example, by flooding the network bandwidth, which are referred to as volumetric attacks. An attack may solicit one or more resources of a service until depleted.

These attacks are referred to as Distributed Denial of Service (DDoS) attacks when a network of often compromised machines are used to interrupt the services in question.

How to protect against DoS attacks

Different protection solutions can be implemented to prevent DoS attacks. Deploying filtering equipment at the external limits of a company's computer system protects against attacks whose volume does not exceed the capacity of the network connections.

When a company's network connections are flooded, the transit operator or internet service provider often needs to be asked to filter the traffic upstream. Service providers also offer cloud-based protection solutions.

Using dedicated equipment at the external limits of a company's computer system can be combined with cloud-based filtering. This type of hybrid protection can be used to protect the company against volumetric attacks while giving it the ability to fight against low-volume attacks.

Here's a non-exhaustive list of possible protection solutions:

Network border filtering

- Firewall type equipment
- Use of specific equipment

Outsourced protection

- Protection provided by hosting companies
- Filtering by transit operator
- Use of a content delivery network
- Dedicated protection service (e.g., DNS redirection, traffic diversion)
- Other technical measures (e.g., network segmentation, network border filtering)

What to do in the event of an attack

DoS attacks are often highly effective against companies that are not prepared. Therefore, the threat must be anticipated by implementing appropriate measures and planning your response to this type of incident.

DETECT	• Put in place monitoring and alert methods to detect an incident in terms of the network and the services performed. • Determine the causes of the incident (e.g., failure, malfunction) by analyzing equipment and server logs.
REACT	• Identify the defective item, protocols used, sources of the attack and one or more identifiers in order to distinguish legitimate traffic from the traffic generated by the attack. • Block the IP addresses at the source of the attack. • Block the type of traffic used in the attack. • Limit the number of simultaneous connections by the source IP address at the firewall. • Reduce TCP connection hold times. • Block traffic at destination targets, depending on the impact of the attack on the rest of the network infrastructure.

How to avoid taking part in a DoS attack

Reduce the attack surface.

- Disable unnecessary services on the servers.
- Fortify operating systems.
- Beef up services settings.
- Keep up to date the frameworks and Content Management Systems (CMS) used for web applications and follow web development best practices.

Filter traffic.

- Make sure that there is limited access to the company's services so that only internal networks are authorized.
- Implement rate-limiting rules.
- Filter outgoing traffic to block the sending of traffic whose IP addresses have been compromised.

Reminder

- Each type of protection has its advantages and limitations, so take precautions before implementing any protection against DoS attacks.
- It's important to make sure that the service providers your company depends on are prepared for DoS attacks.
- Make sure you have appropriate contacts in the company, at transit operators and at protection service providers to react effectively in case of an attack.

For more information

- Guide de l'Agence Nationale de la sécurité des systèmes d'information https://www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DDoS.pdf (in French only)