AIDE-MÉMOIRE

SE PROTÉGER CONTRE UNE ATTAQUE PAR DÉNI DE SERVICE (DDOS)

Objectif du document

Protéger l'entreprise contre les attaques par déni de service (DDOS).

Le nombre d'attaques par DDOS a augmenté au cours des dernières années. Ces attaques sont fréquentes et peuvent viser toute entité disposant d'une infrastructure réseau connectée à Internet. Pour cette raison, il est nécessaire d'anticiper cette menace et de prendre un certain nombre de mesures techniques et organisationnelles afin d'y faire face.

Ce document présente les attaques par déni de service distribué ainsi que la liste des éléments à prendre en compte afin de s'en protéger. Par ailleurs, le document rappelle les bonnes pratiques à mettre en place afin de ne pas participer involontairement à une attaque par DDOS.

Destinataire du document : Administrateur réseau

Date de la dernière modification : 2017-06

Qu'est-ce qu'une attaque par DDOS?

Une attaque par déni de service vise à rendre indisponibles un ou plusieurs services. Un déni de service peut consister à exploiter, par exemple, une vulnérabilité logicielle ou matérielle. L'interruption de service peut également s'effectuer en empêchant l'accès à ce service, par exemple en saturant la bande passante du réseau : on parle alors d'attaque volumétrique. Par ailleurs, une attaque peut solliciter, jusqu'à épuisement, une ou plusieurs ressources d'un service.

On parle de « déni de service distribué » (de l'anglais *Distributed Denial of Service* ou DDOS) lorsque l'attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés.

Comment se protéger contre les DDOS?

Il existe différentes solutions de protection qui peuvent être mises en place afin de lutter contre les attaques par DDOS. Le déploiement d'équipements de filtrage en bordure du système d'information d'une entité offre une protection pour les attaques dont le volume n'excède pas la capacité des liens réseau.

Lorsque les liens réseau d'une entité sont saturés, il est souvent nécessaire de solliciter l'opérateur de transit ou le fournisseur d'accès à Internet afin de filtrer le trafic en amont. Par ailleurs, des prestataires offrent des solutions de protection dédiées en infonuagique.

Il est possible de combiner l'usage d'équipements dédiés en bordure du réseau d'une entité à un filtrage effectué en infonuagique. Ce type de protection hybride permet notamment de protéger l'entité contre des

attaques volumétriques tout en lui donnant la capacité de lutter contre des attaques de débit plus faible.

Voici une liste non exhaustive de solutions de protection pouvant être envisagées :

Filtrage en bordure du réseau de l'entité

- Équipements de type pare-feu.
- Recours à des équipements spécifiques.

Protection externalisée

- Protection offerte par les hébergeurs.
- Filtrage par l'opérateur de transit.
- Recours à un réseau de diffusion de contenu (CDN).
- Services de protection dédiée (ex. : redirection DNS, détournement du trafic).
- Autres mesures techniques (ex. : segmentation du réseau, filtrage à la bordure du réseau de l'entité).

Comment réagir lors d'une attaque ?

Les attaques DDOS sont souvent très efficaces contre une entité non préparée. Il est donc nécessaire d'anticiper cette menace en mettant en place des moyens de protection appropriés, et de planifier la réponse à ce type d'incident.

DÉTECTER	• Disposer de moyens de supervision et d'alertes afin de détecter un incident, tant au niveau du réseau que des services. • Déterminer les causes de l'incident (ex. : panne, dysfonctionnement) en analysant les journaux des équipements et des serveurs.
RÉAGIR	• Identifier l'élément défaillant, les protocoles utilisés, les sources de l'attaque et un ou plusieurs discriminants permettant de distinguer le trafic légitime du trafic généré par l'attaque. • Bloquer les adresses IP sources identifiées comme étant à l'origine de l'attaque. • Bloquer le type de trafic impliqué dans l'attaque. • Limiter le nombre de connexions simultanées par adresse IP source au niveau du pare-feu. • Réduire les délais de garde des connexions TCP. • Bloquer le trafic à destination des cibles, en fonction de l'impact de l'attaque sur le reste de l'infrastructure réseau.

Comment éviter de participer à un DDOS?

Réduire la surface d'attaque

- Désactiver les services inutiles au niveau des serveurs.
- Endurcir les systèmes d'exploitation.
- Endurcir les configurations des services.
- Maintenir à jour les cadres d'applications (*frameworks)* et les systèmes de gestion de contenu (CMS) utilisés pour les applications Web et suivre les bonnes pratiques de développement Web.

Filtrer le trafic

- S'assurer que l'accès aux services d'une entité est restreint afin de n'autoriser que les réseaux internes.
- Mettre en place des règles de *rate limiting.*
- Filtrer le trafic sortant afin de bloquer l'envoi de trafic pour lequel les adresses IP sources sont usurpées.

Rappel

- Chaque type de protection a ses avantages et ses limites. Il est nécessaire de prendre des précautions avant la mise en place d'une protection contre les attaques par DDOS.
- Il est important de s'assurer que les fournisseurs de services dont dépend votre entreprise sont préparés aux attaques DDOS.
- Il est impératif de disposer de contacts appropriés à l'interne, chez les opérateurs de transit ainsi qu'auprès des fournisseurs d'un service de protection pour réagir efficacement en cas d'attaque.

Pour aller plus loin

- Guide de l'Agence nationale de la sécurité des systèmes d'information
  https://www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DDoS.pdf