RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

DÉNIS DE SERVICE DISTRIBUÉS (DDOS *)

1/ LES ATTAQUES DDOS, UNE MENACE PROTÉIFORME

➔ Les attaques DDoS peuvent être de plusieurs types :

> **volumétrique** visant à épuiser la bande passante réseau disponible (ex. : attaque consistant à envoyer des paquets depuis de multiples sources vers une cible – UDP *flood* ou ICMP *flood*) ;

> **protocolaire** visant à épuiser les ressources (CPU, RAM) d'une cible en détournant le fonctionnement d'un protocole (ex. : inondation SYN ou TCP, Smurf) ;

> **applicative** visant à épuiser les ressources (CPU, RAM) d'une cible en détournant le fonctionnement d'un service (ex. : attaque DNS *water torture* consistant à requêter massivement des serveurs pour des entrées DNS existantes).

➔ **Ces types d'attaque en disponibilité ne sont pas exclusifs** et les attaquants peuvent très facilement et rapidement adapter voire combiner leurs techniques au cours du temps. Par exemple, un attaquant pourra commencer par une attaque volumétrique puis, voyant que sa cible prend des mesures d'atténuation spécifiques, s'adaptera en déclenchant une attaque protocolaire ou autre.

➔ Des **mesures préventives et réactives** existent pour en limiter les conséquences. Dans le cas d'une attaque ciblée et très probablement évolutive, l'implication complémentaire d'experts est fortement recommandée pour **une réponse appropriée et spécifique**.

(*) L'acronyme anglais DDoS pour *Distributed Denial of Service* est le plus couramment utilisé.

2/ CONSTRUIRE ET PROTÉGER

➔ **Restreindre au strict besoin opérationnel les services exposés à Internet.**

➔ **Acquérir et mettre en œuvre un service de protection anti-DDoS dédié à cette seule fonction, et adapté au SI à protéger** :

> auprès de votre prestataire en cas d'hébergement externe, celui-ci pouvant déjà intégrer une prestation anti-DDoS, en fonction de l'offre d'hébergement souscrite ;

> et/ou auprès de vos fournisseurs d'accès à Internet (trou noir, dépollution des flux **) ;

> et/ou auprès d'un fournisseur de service professionnel (déroutement BGP, dépollution des flux **).

Le service mis en œuvre doit **protéger contre les attaques de niveaux 3, 4, 5 et 7 du modèle OSI**, par exemple en permettant un contrôle de débit, une limitation du nombre de requêtes, une protection anti-robot et une reconnaissance d'adresses IP réputées malveillantes.

Dans tous les cas, sa **mise en œuvre collaborative entre client et prestataire** nécessite une prise en main, un paramétrage adapté au trafic de l'entité et aux applications exposées (ex. : seuils de déclenchement d'alerte) et **des tests réguliers** pour s'assurer du bon fonctionnement et de l'absence d'effets de bord. Des procédures doivent être définies.

(**) Par exemple, la dépollution des flux peut faire intervenir des critères de géolocalisation, de conformité protocolaire, d'inspection de paquets et de volumétrie par protocole susceptible d'être utilisé dans les DDoS (ex. : DNS en UDP, NTP, CHARGEN).

V2.0 (04/24)

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

→ **Concevoir une architecture des services qui permet de répartir la charge et le trafic sur plusieurs sous-systèmes** (centre de données, mécanismes de bascule réseau, répartiteurs de charge, serveurs distribués, etc.).

→ **Dimensionner une architecture des services en prenant en compte les besoins métiers** qui peuvent fluctuer : bandes passantes, puissances de calcul et mémoire, capacités de stockage.

→ **Concevoir les architectures de telle sorte qu'un service exposé à Internet qui subit une attaque DDoS puisse continuer à être administré malgré cette attaque** (réseau d'administration physiquement dédié, cloisonnement réseau des flux de supervision, etc.).

→ **Concevoir les services exposés à Internet de façon à ce qu'une attaque DDoS sur un service n'ait pas d'impact sur la disponibilité des autres services** (chaînes d'accès Internet distinctes, segmentation des plans d'adressage réseau, hébergeurs distincts, etc.).

→ **Configurer les pare-feux en coupure d'Internet** :

> activer uniquement un filtrage au niveau réseau et transport (niveaux 3 et 4 du modèle OSI) et désactiver les fonctions de filtrage applicatif (niveaux 5 et plus) ;

> réduire les flux UDP entrants au strict nécessaire;

> anticiper la capacité à retirer temporairement le suivi de connexions.

→ **Configurer en aval des pare-feux applicatifs pour protéger les sites Web** en ajustant des limites de session et en appliquant des blocages de requêtes malveillantes.

→ **Protéger les sites Web avec un CDN (*Content Delivery Network*) pour la répartition de charge.** Les CDN permettent la répartition de ressources sur un grand nombre de serveurs, ce qui peut contribuer à améliorer la résistance aux attaques DDoS. **Une attention doit être portée au fait qu'une partie de ces ressources peut être hébergée à l'étranger (impact potentiel en confidentialité).**

3/ ANTICIPER ET RÉAGIR

→ **Mettre en place un dispositif de supervision et détection des attaques DDoS**, afin de détecter au plus tôt une attaque :

> utiliser un dispositif de centralisation des journaux afin de faciliter le diagnostic d'un incident DDoS *a posteriori* ;

> rédiger et tester régulièrement une procédure définissant la marche à suivre en cas d'attaque, en étroite collaboration avec les prestataires de services anti-DDoS. .

→ **Prévoir un mode dégradé pour les activités critiques en cas d'attaque DDoS**, le temps de la remédiation. Intégrer le fait que votre fournisseur d'accès à Internet peut aussi imposer un mode dégradé en cas d'attaque DDoS sur sa propre infrastructure, même si cette attaque ne cible pas directement votre entité.

→ **Faire régulièrement l'inventaire des services ouverts sur Internet** afin d'adapter la procédure de réponse à des attaques DDoS.

→ **Mettre en place un dispositif de gestion des crises**, en lien avec vos prestataires de protection DDoS d'une part et vos responsables communication d'autre part.

→ **Contrôler *a posteriori* les autres alertes de sécurité** générées pendant une attaque DDoS « bruyante », potentiels signes d'une attaque plus discrète et plus grave.

Pour aller plus loin : https://cyber.gouv.fr/guide-ddos

V2.0 (04/24)

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