Veille Technologique

BTS SIO – Option SISR

Année scolaire 2024–2026

Thème :

Les attaques DDoS : un défi majeur pour la cybersécurité des infrastructures réseau

Nom : AMAVI Wesley

Classe : BTS SIO SISR 2eme année

Établissement : INSTA

Sommaire

- ➤ **Schéma 3 : Moyens de protection**

6. Analyse personnelle et conclusion

- 6.1. Bilan : maîtrise technique nécessaire face à l'essor de l'IoT et de l'IA.
- 6.2. Conclusion : l'importance vitale de la veille technologique et de la formation continue.

7. Sources et annexes

-

1. Introduction

Les attaques DDoS (Distributed Denial of Service) représentent aujourd'hui une menace majeure pour les infrastructures réseau. Leur objectif est simple : rendre un service, un site web ou une application indisponible en le saturant de requêtes malveillantes provenant de multiples sources.

Ces attaques deviennent de plus en plus fréquentes, complexes et puissantes, impactant fortement les entreprises et organisations. En tant qu'étudiant en BTS SIO option SISR, comprendre ces attaques et savoir comment les prévenir est essentiel, car c'est un enjeu central de la sécurité des systèmes et réseaux.

Problématique

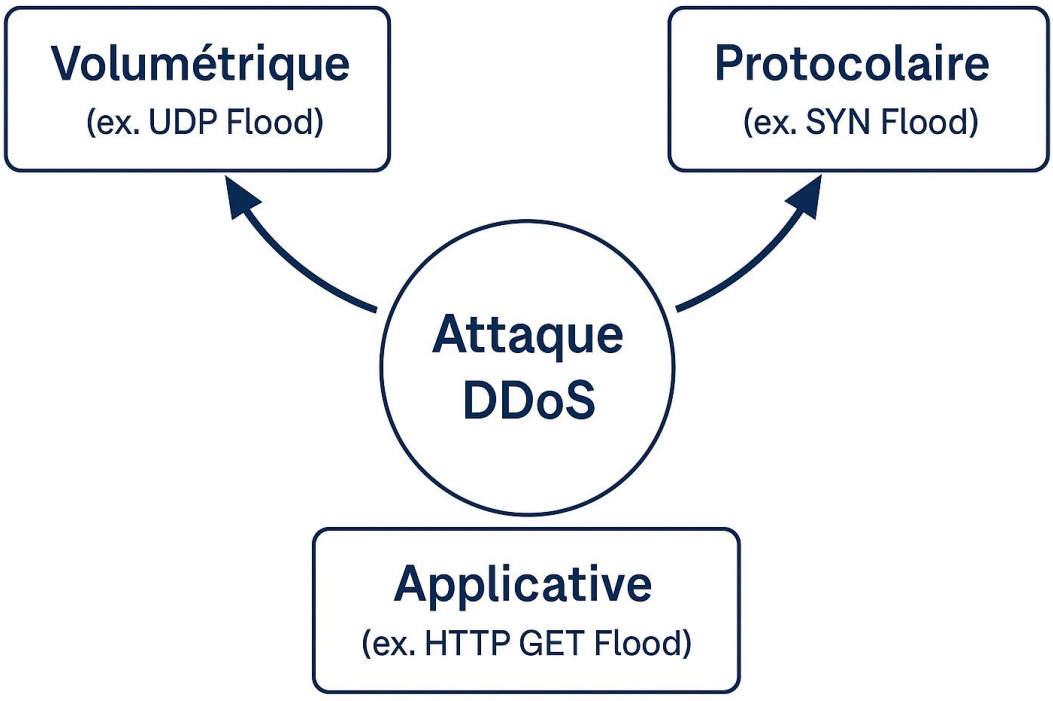
Comment les attaques DDoS évoluent-elles face aux nouvelles technologies, et quelles stratégies un technicien SISR peut-il mettre en œuvre pour protéger les infrastructures réseau ?

2. Fonctionnement des attaques DDoS

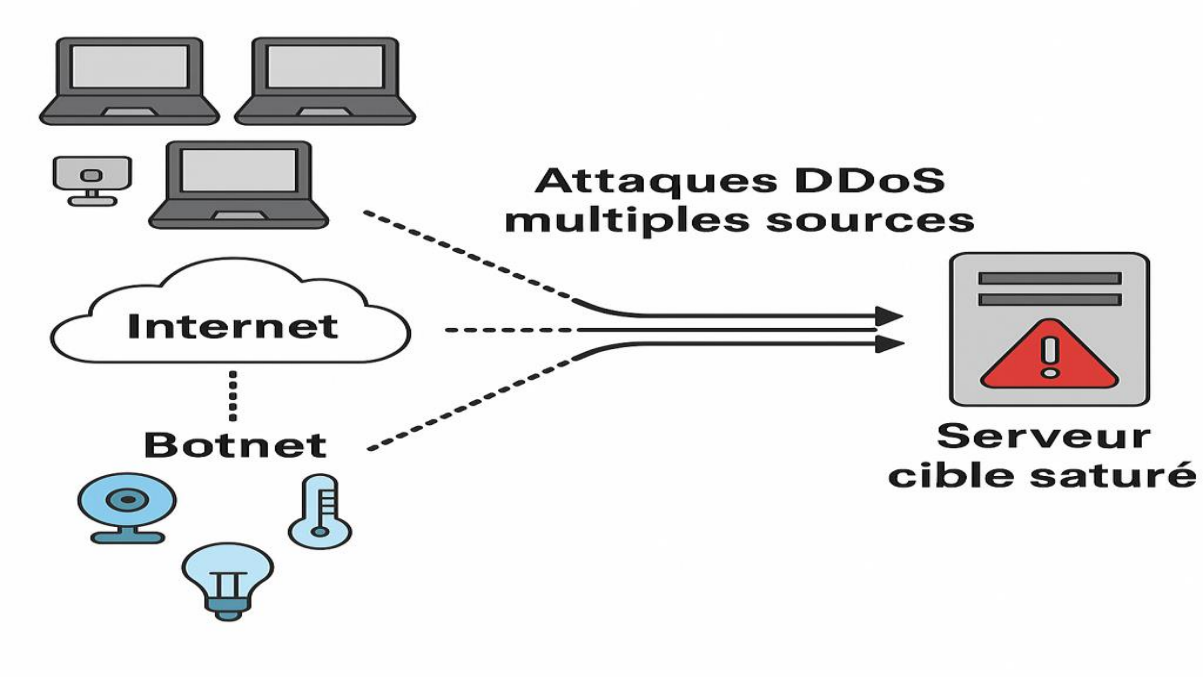
Une attaque DDoS utilise un réseau de machines compromises, appelées **botnets**, qui envoient simultanément un volume important de requêtes vers une cible. Le but est de saturer les ressources du serveur (CPU, mémoire, bande passante) pour provoquer son indisponibilité.

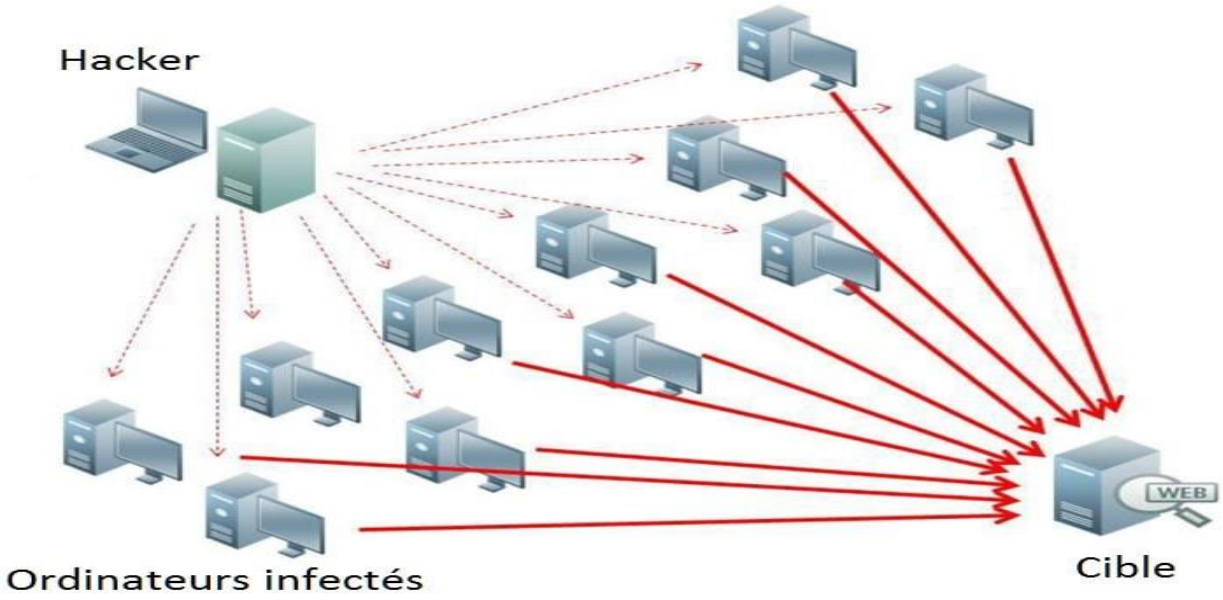
On distingue plusieurs types d'attaques DDoS :

- **Attaques volumétriques** : Elles visent la saturation de la bande passante. Par exemple, les attaques UDP Flood ou Amplification DNS génèrent un trafic massif.
- **Attaques protocolaires** : Elles exploitent des failles ou limites des protocoles réseau, comme le SYN Flood qui surcharge la table de connexions TCP.
- **Attaques applicatives** : Ciblent directement les services web (couche 7), en envoyant un grand nombre de requêtes HTTP spécifiques pour épuiser les ressources applicatives.



Ces attaques peuvent durer de quelques secondes à plusieurs jours et sont souvent masquées par des techniques de **spoofing** (usurpation d'adresses IP).





3. Exemples d’actions DDoS récentes

Ces derniers mois, les attaques DDoS ont atteint des niveaux record et une sophistication accrue :

- **Juin 2025** : Une attaque DDoS record a ciblé une grande entreprise de jeux vidéo, atteignant un pic de **46 millions de requêtes HTTPS par seconde**. Cette action ciblée sur la couche applicative a été neutralisée grâce à **Google Cloud Armor**, un service de protection cloud.
- **Mars 2025** : Le réseau social X (ex-Twitter) a été paralysé par une attaque revendiquée par le groupe hacktiviste **Dark Storm Team**. Cette attaque a duré plusieurs heures, provoquant une indisponibilité notable et soulignant l'utilisation des DDoS comme moyen de pression politique.
- Selon le rapport **Link11 Cybersecurity 2025**, les attaques DDoS en Europe ont augmenté de **137 %** sur l'année, avec des attaques souvent courtes, intenses et multi-vecteurs, combinant plusieurs types d'attaques simultanément.
- Par ailleurs, des actions DDoS coordonnées ont visé des sites d'e-commerce et de streaming lors de périodes commerciales stratégiques (exemple : Black Friday), afin de perturber les ventes et la visibilité en ligne.

Ces exemples montrent que les attaques DDoS sont désormais des outils stratégiques dans des contextes politiques, économiques et commerciaux, et qu'elles utilisent de plus en plus les réseaux d'objets connectés (IoT) pour augmenter leur puissance.

4. Impacts des attaques DDoS

Les conséquences d'une attaque DDoS sont souvent lourdes :

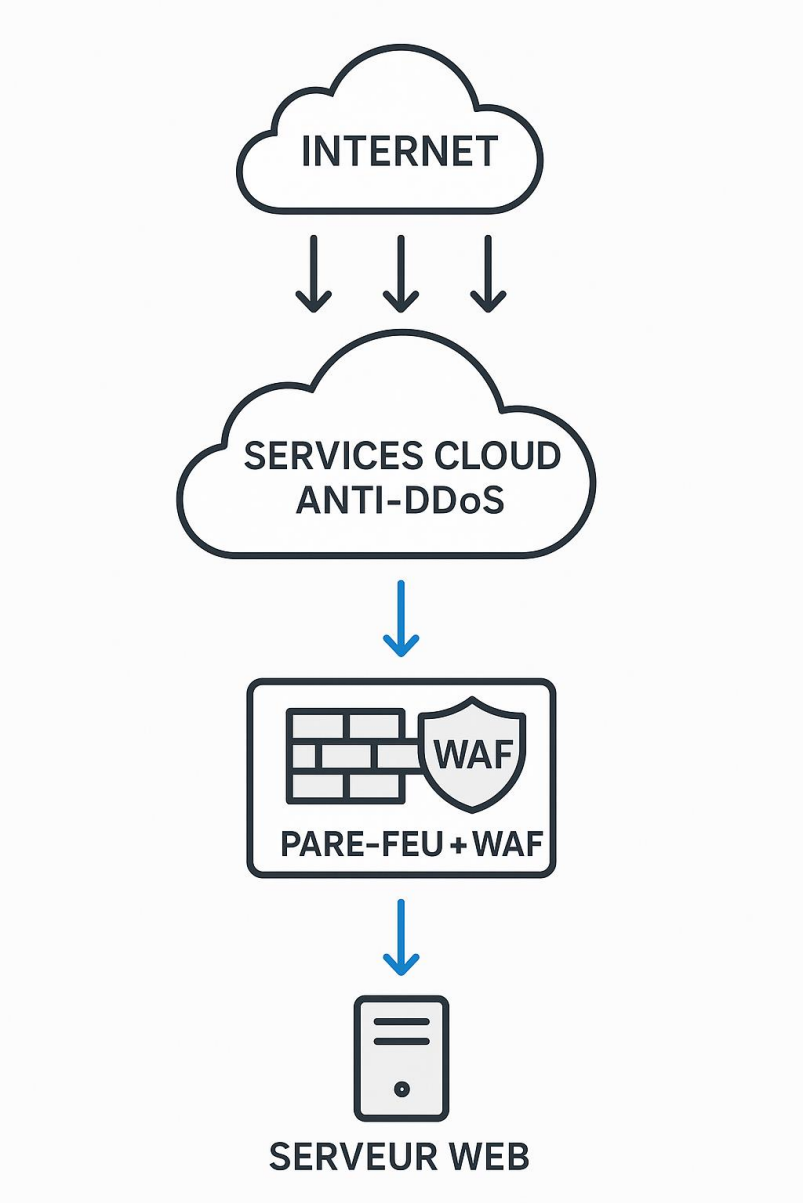
- **Pertes financières importantes**, par exemple plusieurs milliers d'euros perdus chaque minute en cas d'arrêt d'un site e-commerce ou d'un service en ligne.
- **Perte de confiance et d'image** : les clients et partenaires peuvent douter de la fiabilité d'une entreprise touchée.
- **Interruption de services critiques** : notamment dans la santé, la banque, les services publics, où la disponibilité est essentielle.
- **Diversion pour des attaques plus ciblées** : certaines attaques DDoS servent à détourner l'attention pendant qu'une autre intrusion est réalisée (vol de données, ransomware).

5. Moyens de protection contre les attaques DDoS

Pour limiter les risques, plusieurs solutions existent :

Protection technique

- **Pare-feu, systèmes IDS/IPS** (Snort, Suricata) qui détectent et bloquent les flux suspects.
- **WAF (Web Application Firewall)** protège les applications web en filtrant les requêtes malveillantes.
- **CDN et reverse proxy** (Cloudflare, Akamai) répartissent la charge et filtrent le trafic.
- **Services cloud anti-DDoS** (AWS Shield, Google Cloud Armor, Azure DDoS Protection) qui absorbent les attaques massives.
- **Load balancing** pour répartir la charge entre plusieurs serveurs.



Rôle du technicien SISR

- Configurer et superviser les équipements réseau.
- Mettre en place des outils de surveillance en temps réel (Zabbix, Centreon).
- Définir et appliquer des règles de filtrage adaptées.
- Maintenir à jour la sécurité des infrastructures.
- Préparer des plans de réponse aux incidents.

Bonnes pratiques

- Former les équipes à la détection et à la réaction rapide.
- Limiter la surface d'attaque en sécurisant les équipements IoT.
- Effectuer une veille technologique régulière.

6. Analyse personnelle et conclusion

Cette veille technologique m'a permis de mieux comprendre les menaces que représentent les attaques DDoS dans le monde actuel. En tant que futur technicien SISR, il est crucial de maîtriser à la fois la compréhension technique de ces attaques et les solutions pour les contrer.

Les attaques DDoS évoluent constamment avec l'essor des objets connectés, l'intelligence artificielle et la virtualisation des infrastructures. Ainsi, la veille continue et la formation sont indispensables pour anticiper ces menaces et protéger efficacement les systèmes d'information.

7. Sources et annexes

- https://radar.cloudflare.com
- https://blog.google/products/cloud/
- https://www.link11.com/en/resources/
- https://www.enisa.europa.eu/topics/csirt-cert-services/incident-management
- https://www.zataz.com
- https://www.lemondeinformatique.fr