

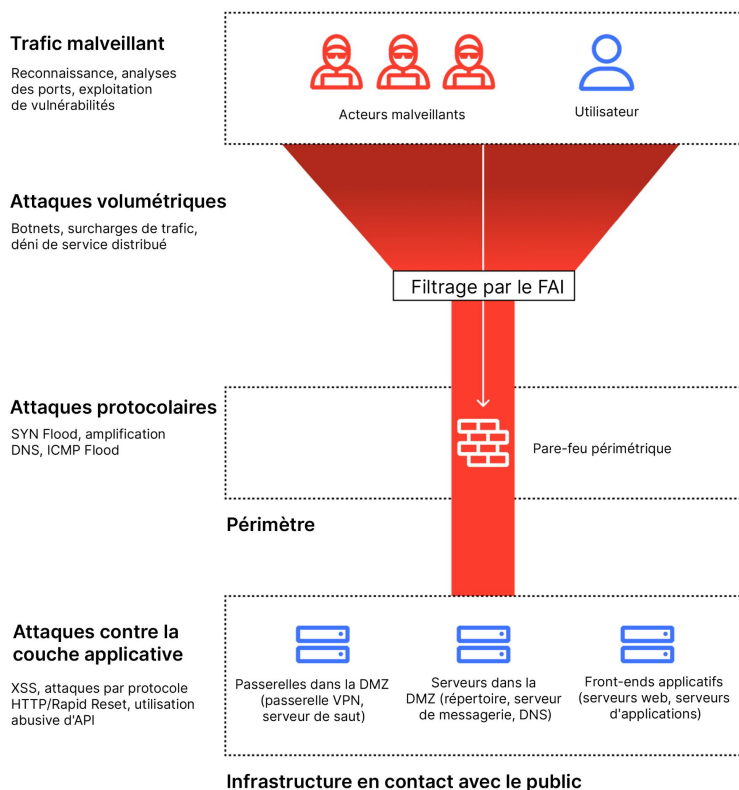
Protection réseau

Protéger les infrastructures en contact avec le public grâce au cloud de connectivité Cloudflare

Problème : compromis entre sécurité et performances

Les infrastructures en contact avec le public sont confrontées à des vulnérabilités en matière de sécurité, car le fait qu'elles soient accessibles depuis Internet en fait une cible toute trouvée pour divers types d'attaques. Les acteurs malveillants peuvent analyser le système à la recherche de services identifiables, exploiter des vulnérabilités non corrigées et lancer des attaques DDoS dévastatrices, qui causeront des dégâts financiers avant que les équipes de sécurité ne puissent réagir.

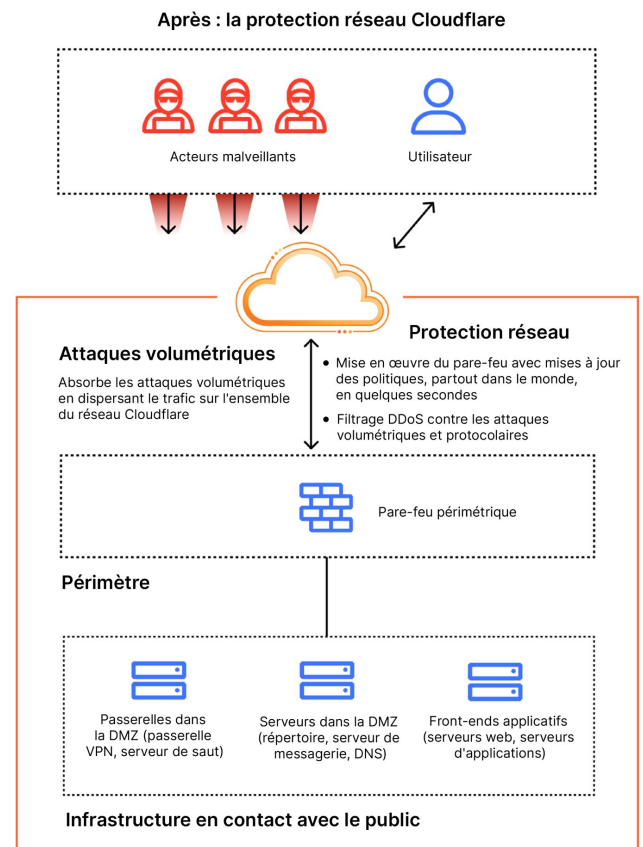
Les entreprises ont déployé de nombreux outils auxiliaires pour pare-feu et équipements réseau, mais ceux-ci engendrent souvent des inefficacités, tout en ne parvenant pas à protéger les systèmes contre les menaces sophistiquées.



Solution : la protection réseau

Simplifiez votre architecture et sécurisez-la davantage en étendant votre réseau grâce au [cloud de connectivité Cloudflare](#). Ajoutez facilement des fonctionnalités en activant des services mis en œuvre dans le cloud (plutôt que par le biais d'équipements) et soutenez le parcours de modernisation de votre réseau à l'aide d'une plateforme répondant à la fois aux besoins actuels et aux scénarios d'utilisation futurs.

Cloudflare assure une couverture mondiale avec un déploiement en une seule passe comprenant une protection multicouche contre les attaques volumétriques, protocolaires ou sur la couche applicative, ainsi qu'une visibilité sur l'état, le comportement et les performances du réseau.



Fonctionnement

1. Définissez un chemin vers le réseau Anycast de Cloudflare pour votre trafic par l'intermédiaire de tunnels IPsec, de tunnels GRE ou de l'interconnexion réseau Cloudflare (Cloudflare Network Interconnect, CNI).
2. Bénéficiez d'une protection automatique grâce à [Magic Transit](#) et [Magic Firewall](#), le tout au prix d'une configuration minimale.
3. Déployez des politiques à l'échelle mondiale en quelques secondes.

[Apprenez-en davantage](#) sur l'architecture Cloudflare afin de protéger votre infrastructure réseau existante.

Avantages

- **Ressources élastiques** : évitez les dépenses d'investissement en passant à l'échelle mondiale dès le premier jour.
- **Gestion simplifiée** : interface de contrôle unifiée pour l'ensemble des services, sans gestion d'équipements physiques ni refonte du réseau nécessaire.
- **Performances améliorées** : routage optimisé du trafic afin d'éviter les encombrements.
- **Réponse mondiale aux menaces** : le réseau Cloudflare protège près de 20 % d'Internet, bloque 227 milliards de cybermenaces chaque jour et s'appuie sur l'IA pour analyser les schémas de trafic mondial afin d'adapter la défense en temps réel.

Présence réseau mondiale

Vos ressources se situent à environ 50 ms de 95 % de la population mondiale connectée à Internet.

Un historique éprouvé

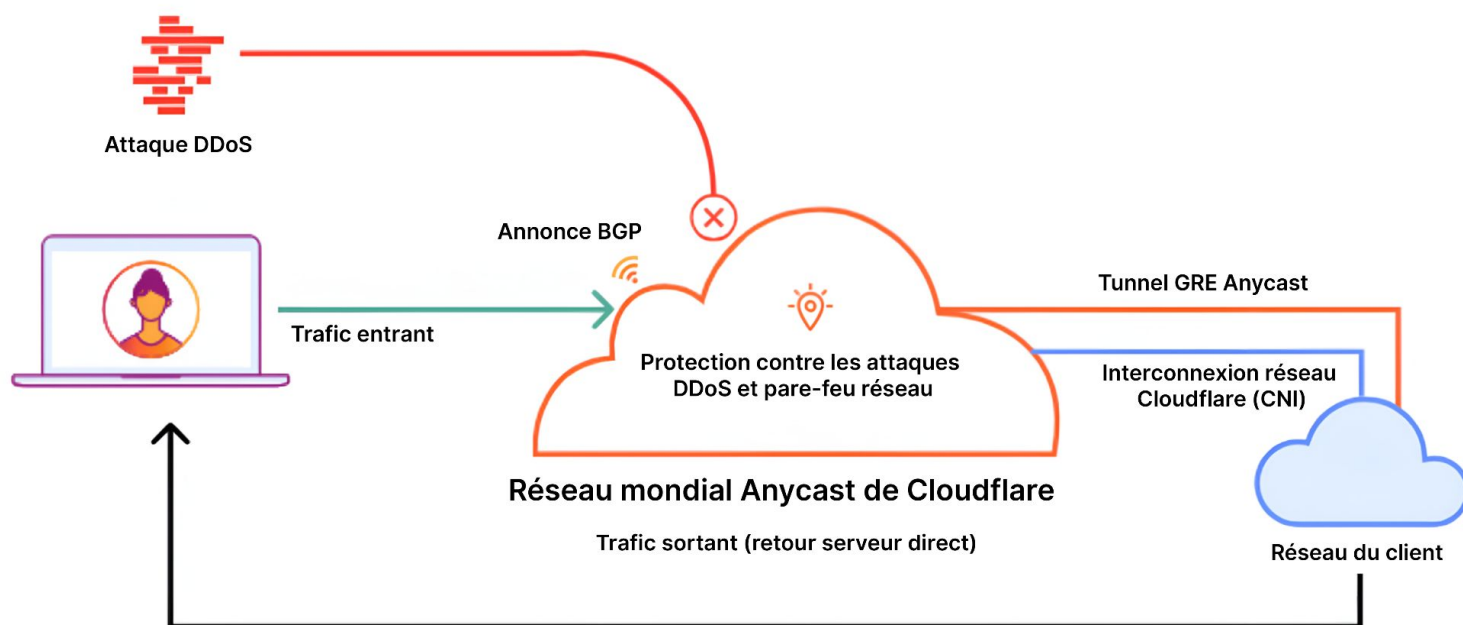
Nous protégeons des millions de propriétés Internet, ainsi que 35 % des entreprises figurant au Fortune 500.

Innovation continue

Les services réseau Cloudflare proposent une disponibilité de 100 % dans le cadre du SLA.

Consolidation économique

Remplacez plusieurs solutions dédiées par une plateforme unique et intégrée.



Pourquoi choisir Cloudflare ?



Chaque datacenter, chaque service

Traitez le trafic aussi près que possible de la source afin de réduire la charge de travail de vos pare-feu.



Protection multicouche, en une seule passe

Évitez la latence indésirable et favorisez la résilience grâce au réseau mondial Anycast de Cloudflare.



Connexion directe au réseau Cloudflare

Contournez l'Internet public et connectez-vous directement grâce à notre interconnexion réseau.

Demandez une démo

Découvrez la protection réseau Cloudflare en action grâce à une démo guidée en direct.

[Demander une démo](#)

Téléchargez le livre blanc sur la protection réseau

Découvrez les défis liés à la sécurisation de l'infrastructure réseau en contact avec le public et les limites des outils auxiliaires pour pare-feu.

[Télécharger](#)

Ressources complémentaires

- Webinaire : [« Dire adieu aux outils pour pare-feu traditionnels : obtenir la protection que votre réseau mérite »](#)
- Architecture de référence : <https://developers.cloudflare.com/reference-architecture/architectures/magic-transit/>

