# Bâtir une architecture de protection contre les attaques par déni de service distribué (DDoS)

Les attaques par déni de service distribué (DDoS) sont en constante évolution. Si leur objectif reste de perturber les activités des entreprises, les attaques et les agresseurs sont toujours plus sophistiqués, les motivations de plus en plus financières ou politiques, et les conséquences toujours plus graves pour les victimes.

Par le passé, les attaques DDoS se concentraient sur les couches 3 et 4, et les pare-feu réseau étaient capables de déployer une première ligne de défense. Pour contourner cette protection, les attaquants ont monté d'un cran dans la pile et privilégient à présent les attaques SSL et la couche applicative pour inonder les ressources.

Incapables de suivre l'évolution, le volume et l'intelligence de ces attaques, les pare-feu réseau classiques ne sont pas en mesure de gérer le trafic de façon contextuelle, d'où leur impuissance face à des attaques multicouches.

Les services de nettoyage (scrubbing) sur le cloud se sont imposés comme un outil performant face aux attaques volumétriques de grande envergure, mais ils ne peuvent assurer une protection complète contre toutes les formes d'attaques DDoS. Une sécurité renforcée sur site est nécessaire pour repousser les attaques visant les serveurs d'applications (la logique métier, par exemple) et les serveurs DNS, ainsi que les attaques cachées dans les communications cryptées SSL.

## Architecture F5 multiniveaux : pour protéger toutes les couches

Face à la perspective d'attaques DDoS handicapantes, les institutions financières et les grandes entreprises refondent leurs réseaux en les dotant d'une fonction de lutte contre les attaques DDoS. En collaboration avec ces clients, F5 a développé une architecture de protection DDoS qui déploie des produits de sécurité F5 sur deux niveaux. Le niveau 1 (Tier 1) assure la protection du système DNS et des couches 3 et 4. À l'abri des attaques réseau, le niveau 2 peut utiliser ses ressources de calcul (CPU) pour protéger les protocoles d'application aux couches supérieures. Les avantages de cette stratégie sont déjà tangibles dans les datacenters de plusieurs clients de F5.

Cette architecture multiniveaux permet à la couche applicative au niveau 2 de monter en charge indépendamment du niveau 1, ainsi que de faire cohabiter sur les deux niveaux différentes versions du code, des plateformes et des règles de sécurité. Par exemple, une nouvelle règle mise en œuvre dans le pare-feu d'applications Web de F5 pourra être appliquée dans une unité autonome unique au niveau 2. Le niveau 1 pourra ainsi lui envoyer 1 % du trafic jusqu'à ce que la nouvelle règle soit validée.

À l'autre extrémité du spectre, les petites entreprises cherchent à maximiser la valeur de investissements consacrés à leur infrastructure informatique et utilisent à cet effet une unique plateforme de sécurité intégrée. F5 leur propose une solution à un seul niveau au coût optimisé qui comprend une protection complète contre les attaques DDoS des couches 3 à 7, DNS et SSL comprises.

## Principales caractéristiques

- **Montée en charge et performances** — jusqu'à 576 millions de connexions simultanées, 640 Gbits/s de débit et 8 millions de connexions par seconde.
- **Intelligence et gestion contextuelle** — surveiller les connexions entrantes et les temps de latence anormaux pour distinguer les agresseurs des utilisateurs légitimes.
- **Protection de toutes les couches** — sécurité DDoS sur toutes les couches : réseau, DNS, SSL et applications. Protège les protocoles (UDP, TCP, SIP, DNS, HTTP et SSL), ainsi que les applications.
- **Lutte dynamique contre les menaces** — utilisation de la solution F5 iRules pour créer un contexte de sécurité dynamique contre les attaques Jour zéro.

## Principaux avantages

- **Protégez l'infrastructure réseau** — contrez les attaques avant qu'elles ne touchent votre réseau avec un matériel dédié et une architecture full-proxy spécifique.
- **Protégez votre image de marque** — Vérifiez que vos clients peuvent continuer à mener des activités professionnelles en utilisant vos applications Web.
- **Défendez-vous contre les attaques ciblées** — protégez-vous contre un large éventail de vecteurs d'attaque DDoS et repoussez les attaques personnalisées (crafted).
- **Économisez de l'argent** — Consolidez les services de protection DDoS dans votre actuelle plateforme F5 et réduisez les coûts d'exploitation.

## La solution

Les composants de la solution de protection DDoS de F5 assurent une sécurité intrinsèque car ils sont associés et inspectent séparément chaque connexion utilisateur au lieu d'échantillonner ou d'observer le trafic sur un port en miroir. C'est ce qui permet aux clients de F5 à travers le monde de repousser les attaques DDoS jour après jour depuis plus de 10 ans. F5 est souvent la seule solution capable de contrer les attaques par déni de service distribué et de garantir la disponibilité des services et applications.

La protection assurée par F5 contre les attaques DDoS découle de la sécurité intrinsèque intégrée dans chacun des composants intelligents et évolutifs développés par F5 :

- Un pare-feu réseau haute performance contre les attaques DDoS sur la couche réseau (SYN Floods et ICMP Floods).
- Un pare-feu d'applications Web à la pointe de l'industrie, qui utilise la gestion contextuelle des applications (application fluency) pour détecter et contrer les attaques visant le protocole HTTP.
- **L'architecture DNS full-proxy, qui minimise les attaques DDoS contre le DNS tout en validant chaque requête DNS et en fournissant toutes les réponses DNS.**
- The F5 **application delivery controller** protects SSL resources by absorbing SSL DDoS attacks with high-performance, high-capacity cryptographic offload hardware.
- Le contrôleur de trafic applicatif (ADC) de F5, qui protège les ressources SSL en absorbant les attaques DDoS au moyen d'une solution de chiffrement matérielle de haute performance et de grande capacité.
- F5 s'est imposé depuis longtemps comme un spécialiste des attaques Jour zéro avec une capacité de programmation du data plane intégrée au langage de script iRules®.

## Pour en savoir plus

Pour toute information complémentaire concernant les solutions de protection DDoS de F5, consultez les ressources suivantes ou utilisez le moteur de recherche sur www.f5.com.

### Solution

Protection DDoS F5

### Produits

BIG-IP Advanced Firewall Manager

BIG-IP Application Security Manager

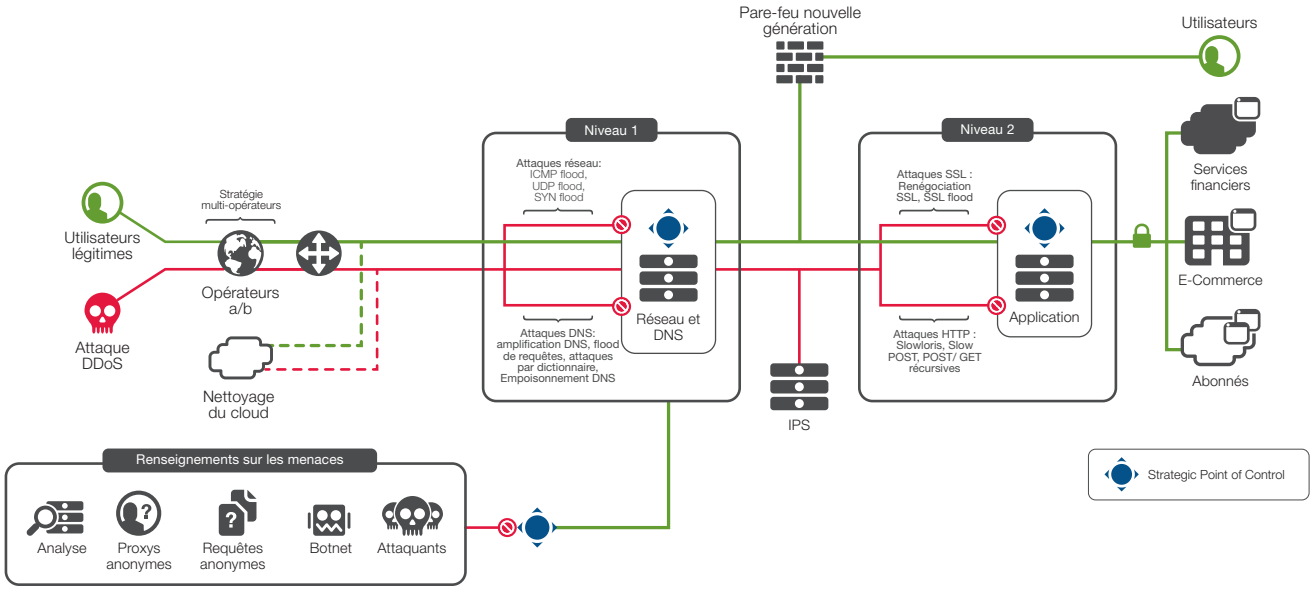
BIG-IP Global Traffic Manager

BIG-IP Local Traffic Manager

### Livres blancs

The DDoS Threat Spectrum

Mitigating DDoS Attacks with F5 Technology




Une architecture de protection DDoS à deux niveaux assure une efficacité et une flexibilité pour adapter les composants de sécurité.components.

**F5 Networks, Inc.** 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

Solutions for an application world


SOLP-SEC-11851-ddos-protection 1013