Services Réseaux

une marque éditée par SERVERD

# Protection contre les attaques DDoS
## Présentation Produit

SERVERD SAS – 10 rue de Penthièvre – 75008 Paris
Téléphone : 01 89 16 05 65 – Email : hello@netrix.fr

## Introduction

Netrix intègre un service de protection contre les attaques DDoS dans toutes ses offres de transit IP sans surcoût via le niveau de service **Anti-DDoS Standard**, offrant une protection complète contre les attaques courantes.

Pour les clients ayant besoin de personnalisation accrue, le niveau de service **Anti-DDoS Intense** permet un contrôle plus granulaire des seuils de protection, et offre des fonctionnalités avancées comme des rapports détaillés et un suivi en temps réel par notre SOC (Security Operations Center) lors d'attaques.

| **Caractéristiques** | **Standard** | **Intense** |
|---|---|---|
| Nombre d'attaques par mois | Illimitées | Illimitées |
| Volumétrie d'attaque maximale | Illimitée | Illimitée |
| Détection et mitigation automatiques | ☑ | ☑ |
| Vitesse de détection et mitigation | < 5 secondes | < 5 secondes |
| Protection L4 | ☑ | ☑ |
| Protection TCP avancée | ☑ | ☑ |
| Supervision SOC Netrix | ☑ | ☑ |
| Suivi des attaques par email | ☑ | ☑ |
| Interface web de suivi des attaques | ✗ | ☑ |
| Intervention proactive du SOC en cours d'attaque | ✗ | ☑ |
| Automatisations en cas d'attaque (webhook) | ✗ | ☑ |
| Règles de mitigation personnalisées | ✗ | ☑ |
| Seuils de déclenchement personnalisés | ✗ | ☑ |

L'Anti-DDoS Standard et l'Anti-DDoS Intense utilisent la même infrastructure ainsi que les mêmes mécanismes de protection contre les attaques DDoS et offrent ainsi les mêmes capacités de mitigation. L'offre Anti-DDoS Intense se distingue par ses fonctionnalités additionnelles ainsi que son plus haut niveau de personnalisation.

Notre solution Anti-DDoS est **entièrement développée en interne** et évolue en continu pour s'adapter aux nouvelles menaces DDoS.

Nous effectuons des **mises à jour fréquentes**, jusqu'à plusieurs fois par semaine, afin de garantir une efficacité maximale face aux menaces émergentes.

## Points clés du service de protection DDoS

**Détection et mitigation ultra-rapides** :

- **Détection des attaques** en temps réel (moins d'une seconde) offrant l'une des meilleures réactivités disponibles sur le marché.

- Objectif de mitigation (TTM) en **moins de 5 secondes** : Les règles de mitigation sont calculées et déployées de façon entièrement automatique et sont efficace en **2 à 3 secondes en moyenne**.

**Livraison du trafic propre :**

Le trafic propre (nettoyé de toute éventuelle attaque DDoS) est livré directement sur le port de transit IP du client, sans aucune configuration requise de la part du client (pas de tunnel GRE requis).

**Analyse en temps réel du trafic réseau** :

La totalité de nos interconnexions, y compris celles en peering direct, sont analysées en temps réel pour détecter la moindre attaque DDoS. Cette analyse précise nous permet de détecter les attaques DDoS dès les premiers instants, même lorsqu'elles sont hautement distribuées et proviennent de plusieurs interconnexions différentes.

**Évolution automatique de la mitigation pendant les attaques** :

Les filtres de mitigation sont ajustés **automatiquement** et **en temps réel** pendant l'attaque. Ces mécanismes assurent une réponse sur-mesure pour chaque attaque DDoS, en ciblant précisément chaque vecteur d'attaque identifié, même lorsqu'ils évoluent en cours d'attaque.

**Couverture complète des attaques L4/L5 UDP et TCP** :

Notre protection est régulièrement testée et maintenue à jour pour offrir la couverture de :

- **Toutes les attaques L4** : Tels que les flood aléatoires TCP, UDP, GRE (et autres protocoles), ainsi que les attaques par réflexion ou amplification (telles que DNS, NTP, SNMP, etc).

- **Toutes les attaques de sessions TCP (L5)** : Type SYN/ACK Flood. Ces attaques sont traitées automatiquement via un mécanisme **d'authentification TCP transparent** et asymétrique, sans **aucune déconnexion** (ou reset) de la session pour les utilisateurs légitimes.

**Trois mécanismes de mitigation complémentaires** :

Nous exploitons trois stratégies de mitigation différentes, qui s'activent de façon automatique en fonction des vecteurs d'attaques identifiés et de leur volumétrie :

- **Inline Mitigation** : Active sur tous les edges de notre réseau en tout temps, cette stratégie nous permet de déployer des règles de mitigation très ciblées, sans nécessité de re-router le trafic, offrant alors une vitesse de mitigation très élevée pour les attaques les plus communes.

- **Out-of-line Mitigation** : Certaines attaques TCP complexes nécessitent de l'authentification TCP. La stratégie Out-of-line nous permet, en quelques instants, de re-router une partie du trafic TCP dans une infrastructure de mitigation interne spécialisée (on-premise) et d'effectuer de l'authentification TCP transparente et asymétrique.

- **Scrubbing centers spécialisés** : Plus lente d'activation en raison de la convergence BGP, les scrubbing-centers n'offrent pas la même réactivité que nos outils de mitigations interne. Ils proposent cependant une capacité de mitigation très élevée (plusieurs Tbps) et sont exploités dans notre mitigation de façon automatique en cas de volumes d'attaques extraordinaires ou de scénarios d'attaques répétées.

**Mitigation de haute capacité :**

- **Mitigation interne** : Le réseau Netrix dispose de plusieurs centaines de Gbps de capacité native. Cette capacité est suffisante pour mitiger 99% des attaques **sans re-routage externe**, évitant ainsi les délais liés à la reconvergence BGP, ainsi que d'éventuelles baisse de qualité sur les routes en peering.

- **Scrubbing centers** : Nous disposons de plus de **5 Tbps** de capacité au travers de scrubbing-centers spécialisés, nous permettant de gérer des attaques d'envergure exceptionnelle, nous permettant de garantir une protection même contre les plus grandes attaques volumétriques jamais observées.

**Détection immédiate des attaques carpet-bombing** :

Nos mécanismes de détection et de mitigation sont conçus pour identifier précisément la cible d'une attaque DDoS, qu'il s'agisse d'une seule IP (/32) ou d'un bloc réseau (/24 par exemple). Ainsi nous sommes en mesure de détecter avec **la même précision les attaques de type carpet-bombing**, même de faible intensité, et de déployer des règles de mitigation adaptées à ces attaques, toujours avec un objectif de **moins de 5 secondes**.

**Double algorithme de détection** :

La détection d'attaque est réalisée entièrement en interne, via deux principales technologies différentes :

- **Analyse de signature** : Le trafic entrant est comparé à une base de données de signatures d'attaques connues, maintenue régulièrement à jour par l'équipe de notre SOC. Cette méthode offre le plus haut niveau de précision pour la détection des attaques les plus connues (amplification UDP, SYN Flood, etc).

- **Analyse heuristique** : Cette méthode analyse le trafic entrant et compare son niveau de déviation contre le trafic propre attendu. Elle permet de détecter des modèles d'attaques encore inconnus ou qui ne peuvent pas être identifiés via des signatures, offrant ainsi une protection même pour les nouvelles formes d'attaques DDoS.

**Aucune limite de taille d'attaque** :

Il n'y a **aucune limite** quant à la taille des attaques pouvant être traitées par notre système. Les infrastructures de Netrix sont dimensionnées pour filtrer la quasi-totalité des attaques en interne. Seules les attaques les plus inhabituelles sont redirigées vers les scrubbing centers pour un traitement externe.

**Mitigation entièrement gérée, sans intervention client**

La totalité des opérations de détection, de mitigation, ou d'ajustement en cours d'attaques, sont réalisés de façon **automatique**, en **quelques instants**, sans qu'aucune intervention ne soit nécessaire de la part du client. Notre équipe SOC supervise le bon fonctionnement de la mitigation et le blocage effectif des attaques. Les éventuels réglages nécessaires pour optimiser les stratégies de mitigation sont effectués par Netrix. **Aucune configuration n'est requise par le client**.

# Détails techniques des différents points d'analyse et de mitigation des attaques

## Mitigation inline

Tous les routeurs d'extrémités (Edges) de notre infrastructure participent à notre réseau **Inline Mitigation.**

Chaque paquet traversant nos routeurs d'extrémités, sur la totalité de nos interconnections (y compris peering) y est analysé et peut y être bloqué s'il correspond à du trafic identifié à une attaque DDoS en cours.

Ce mécanisme étant actif en permanence, tout le trafic réseau passe à tout instant dans la mitigation inline, **éliminent tout besoin de re-routage ou d'augmentation de latence** lors de la mitigation d'une attaque.

C'est une **protection continue**, sans point d'étranglement ni interruption.

Dans ce contexte, **l'Inline Mitigation** est idéale pour bloquer la majorité des attaques fréquentes, notamment les floods UDP et TCP de faible ou de haute intensité.

Comme ce mécanisme est entièrement intégré au réseau, il garantit une **protection systématique**, quel que soit le volume de l'attaque, sans redirection du trafic vers des infrastructures externes.

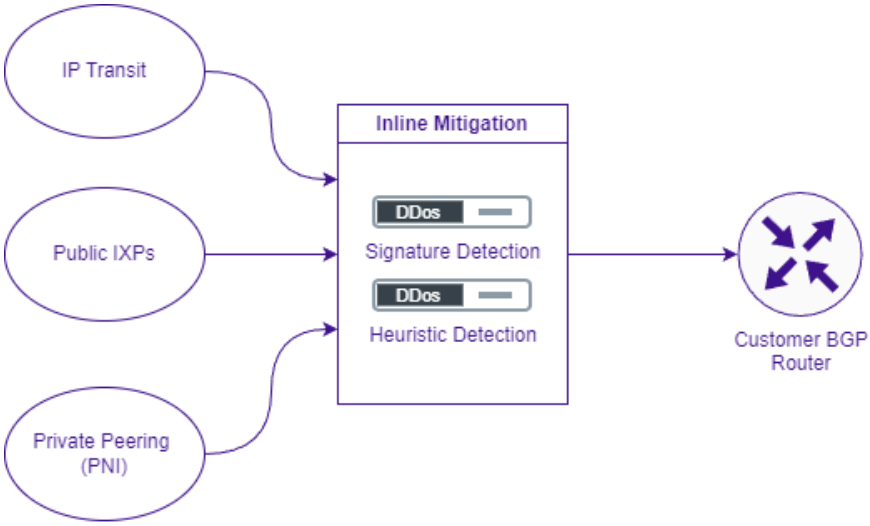


*Schéma de fonctionnement, Inline Mitigation*

## Out-of-Line Mitigation (authentification TCP)

Certaines attaques TCP complexes (notamment les attaques SYN qui visent à épuiser les ressources liées au sessions) peuvent nécessiter de **l'authentification TCP.**

Pour ce type d'attaque, le trafic TCP entrant est **redirigé automatiquement**, en quelques instants, dans une infrastructure spécialisée (hébergée on-premise, au sein de notre réseau).

Le trafic y est alors finement analysé, et une authentification TCP transparente y est réalisée si nécessaire.

Cette phase exploite le fonctionnement du handshake TCP pour challenger les connexions entrantes et ainsi vérifier qu'il s'agit d'utilisateurs réels et non pas de bots ou de requêtes spoofés.

Cette opération est entièrement transparente, il **n'interrompt pas les connexions légitimes** et ne cause pas de reset ou de déconnexion des sessions légitimes déjà établies. Ce mécanisme est également totalement asymétrique (le trafic TCP sortant n'est pas analysé ni redirigé) et est donc pleinement compatible avec un schéma multi-transit/multi-homé.

Cela permet une protection contre des attaques TCP complexes sans impact sur l'expérience utilisateur.

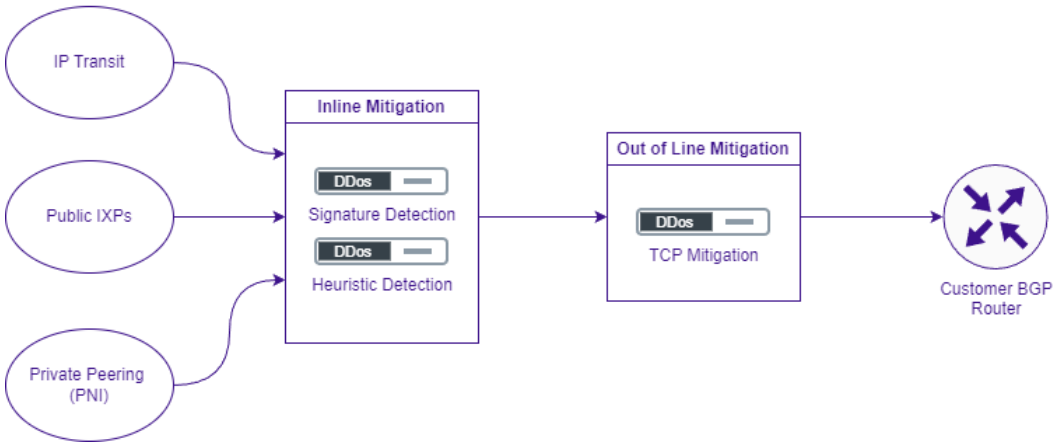


*Schéma de fonctionnement, mitigation Out Of Line (TCP)*

## Scrubbing Centers spécialisés

Lorsqu'une attaque atteint un volume exceptionnel ou lorsque nous détectons des campagnes d'**attaques persistantes et massives**, le trafic peut être redirigé vers des **centres de scrubbing** spécialisés.

Cette méthode concerne principalement les attaques qui dépassent la capacité de traitement interne, représentant moins de 1% des attaques observées.

Les **scrubbing centers** sont conçus pour gérer des attaques d'une ampleur exceptionnelle, capables de déployer plus de **5 Tbps de capacité** pour absorber et filtrer les attaques les plus violentes.

Ces centres sont également activés en cas de **harcèlement ciblé**, où les attaques répétées sur des périodes prolongées nécessitent une gestion plus approfondie du trafic pour éviter une saturation des ressources.

Bien que la majorité des peering soient désactivés lors de l'activation de scrubbing-center, certains peering spécialisés de confiance peuvent rester actifs (notamment les peering avec les FAI nationaux).

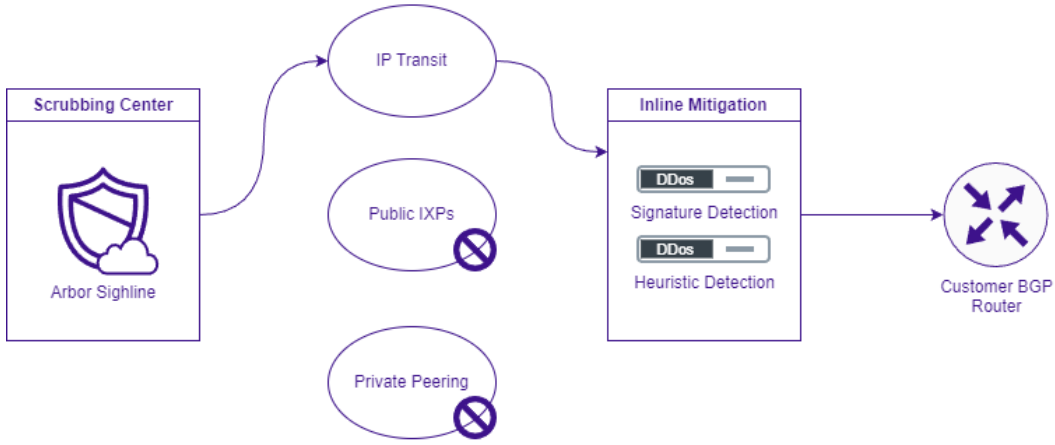


*Schéma de fonctionnement, mitigation via Scrubbing Center*

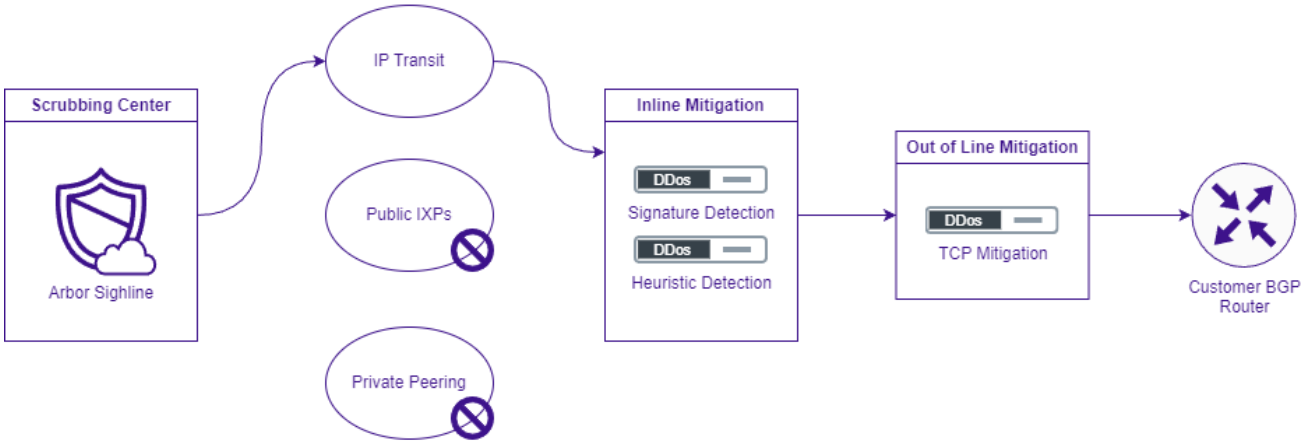


*Schéma de fonctionnement, mitigation via Scrubbing Center avec Mitigation Out Of Line (TCP)*

## Détection algorithmique

La totalité des paquets traversant notre infrastructure est analysé en temps réel par deux algorithmes différents :

### Analyse par signatures

Ce mécanisme permet de détecter avec une très haute précision les attaques déjà connues en comparant les paquets réseau transitant dans notre réseau avec une base de données de signature d'attaque connues (par exemple les amplifications UDP, les flood de protocoles, les attaques TCP SYN, etc). Chaque signature est liée à un ensemble de règle de mitigation testée et adaptée pour cette attaque.

Chaque nouvelle attaque rencontrée est ajoutée à cette base directement par notre équipe, améliorant ainsi la vitesse et fiabilité de détection de cette attaque lors de sa prochaine occurrence sur notre réseau.

Notre SOC effectue également une surveillance et une veille technologique accrue pour suivre les nouvelles menaces émergentes dans l'écosystème DDoS. Chaque fois qu'une nouvelle méthode d'attaque est identifiée, elle est rapidement transformée en signature, puis ajoutée à cette base.

Cela assure une protection contre les attaques connues, qui peuvent être facilement répliquées à grande échelle.

### Analyse heuristique

En complément de l'analyse par signatures, un algorithme d'analyse heuristique est déployé pour détecter les attaques non conventionnelles, c'est-à-dire des schémas d'attaques qui n'ont pas encore été observés ou qui ne suivent pas un modèle standard.

Ce mécanisme fonctionne en analysant les différentes courbes de trafic (pour chaque protocole) et en les comparant avec les courbes de trafic attendues sur le réseau. En cas de déviation importante, une analyse fine des paquets est effectuée pour déterminer le trafic responsable de la variation, et des contre-mesures ciblées sur ce trafic sont appliquées.

Ce mécanisme peut déployer un ensemble de règles de mitigation de façon très fine, pour bloquer ou rate-limiter uniquement le trafic responsable de la déviation, sans impacter le reste du trafic à destination de l'IP.

L'analyse heuristique permet au système de détecter des variations d'attaques ou des tentatives d'exploitation qui ne sont pas encore connues dans la base de signatures. Cela

comprend des attaques aux modèles aléatoires ou des schémas sophistiqués visant à contourner les systèmes de sécurité traditionnels.

Grâce à cette approche, Netrix est capable de réagir de manière proactive à des attaques en constante évolution et à des techniques émergentes.

**Double Algorithme**

Le système de Netrix combine ces deux algorithmes — signatures et heuristiques — dans une approche double. Ce modèle garantit :

- Réactivité pour bloquer les attaques identifiées instantanément avec les signatures.
- Adaptabilité pour anticiper et mitiger les nouvelles attaques ou les variantes grâce à l'analyse heuristique.

En conjuguant ces deux approches, Netrix maximise sa capacité à protéger son réseau contre un large éventail d'attaques, des plus courantes aux plus innovantes.

Ce double système assure une couverture à la fois préventive et réactive, garantissant ainsi une détection ultra-rapide et une mitigation efficace des menaces, même lorsqu'elles évoluent rapidement.

# Les différents niveaux de service anti-DDoS

## Niveau Anti-DDoS Standard – Incluse

Le niveau de service Anti-DDoS Standard offre les services suivants :

- Mitigations illimitées : Aucune limite sur le nombre d'attaques traitées, quel que soit le volume.
- Volumétrie illimitée : Protection contre les attaques, sans restriction sur leur ampleur.
- Détection et mitigation automatiques : En moins de 5 secondes avec une moyenne de 2 à 3 secondes.
- Protection L4 et TCP : Couverture complète des attaques UDP et TCP (ACK, SYN, RST, etc) avec authentification TCP transparente.
- Supervision SOC Netrix : Surveillance active de tout le trafic réseau et du bon fonctionnement de la mitigation, et analyse régulière de l'historique des mitigations
- Suivi des attaques par email : Notifications automatiques dès la détection d'une attaque, avec des rapports envoyés par mail.

## Niveau Anti-DDoS Intense – Sur option

Le niveau de service Anti-DDoS Intense offre les services du niveau Anti-DDoS Standard ainsi que :

- Interface web en temps réel : Accès à une plateforme de suivi détaillé des attaques en temps réel. Cela permet au client de visualiser l'ampleur, la durée, et l'état d'une attaque en cours directement depuis un tableau de bord personnalisé.
- Intervention proactive du SOC : Les équipes de sécurité de Netrix interviennent activement en cours d'attaque, ajustant manuellement si nécessaire les stratégies de mitigation pour s'assurer que la défense reste optimale face à des attaques évolutives ou complexes.
- Automatisation via webhook : En cas d'attaque, des webhooks peuvent être déclenchés et envoyées au client, pour que le client puisse automatiser certaines actions (comme des notifications internes ou l'exécution de scripts) permettant ainsi au client d'adapter son infrastructure de manière réactive.

- Personnalisation accrue de la mitigation : Bien que cela ne soit habituellement pas nécessaire, certains environnements très spécifiques pourraient nécessiter de créer des profils de mitigation ou de détection sur-mesure pour votre cas d'usage. Notre équipe pourra étudier et adapter la mitigation à votre besoin précis.

Notre niveau **Standard** offre une protection entièrement automatisée, sans compromis et sans aucune limite en termes de taille d'attaque ou de nombre d'attaque. Elle est parfaite pour protéger les usages courants ou si vous n'êtes pas régulièrement ciblé par les attaques.

Le niveau **Intense** est destiné aux clients ayant besoin d'une vigilance encore plus renforcé contre les attaques DDoS, où chaque instant compte (par exemple, les services bancaires, les services temps réel tels que les jeux vidéo, les fournisseurs de contenu, etc). Ce niveau de protection offre des outils de suivi et d'automatisation en temps réel ainsi qu'une intervention directe et proactive de notre SOC en cours d'attaque lorsque cela s'avère nécessaire.

netrix

**Service Commercial**
**Email : hello@netrix.fr**
**Téléphone : 01 89 16 05 65**