

Conditions particulières – HG-Proxy et protection anti-DDoS

HG-HOSTING — Hébergement & infrastructure

Version 2026-10-24-1 · 24 octobre 2026

Relais de trafic pour serveurs de jeux et protection associée.

Identité du prestataire

HG-HOSTING, SAS au capital de 100 euros — RCS Nantes 991 163 932.

2 Allée du Verger, 44170 Nozay, France.

SIRET 991 163 932 00015 — TVA intracommunautaire FR70 991 163 932.

hg-hosting.fr · client.hg-hosting.fr

contact@hg-hosting.fr · 07 43 75 91 66

Données personnelles : privacy@hg-hosting.fr

Version du document

La version communiquée lors de votre commande s'applique à celle-ci. La publication de cette édition ne modifie pas rétroactivement les contrats déjà conclus.

SOMMAIRE

Accès direct aux articles

Cliquez sur un intitulé pour accéder à la section correspondante.

1. Service
2. Serveur de destination
3. Filtrage et limites
4. Adresses et sortie

1. Service

La commande définit les protocoles, ports, adresses, destination, débit, trafic et niveau de protection du proxy. HG-Proxy relaie le trafic vers le serveur de destination configuré ; il n'héberge pas automatiquement les fichiers ou bases de ce serveur.

Les offres HG-Proxy concernent le relais TCP/UDP de serveurs de jeux, notamment FiveM et Minecraft, avec la capacité de joueurs choisie à la commande. Le service associe le filtrage réseau annoncé pour l'offre et la mitigation Netrix en amont. Le transit utilisé par HG-Hosting pour acheminer ce trafic relève de son infrastructure ; il ne constitue pas une offre de transit IP vendue séparément au client.

2. Serveur de destination

Le client dispose de l'autorisation d'utiliser la destination et maintient le serveur, ses règles réseau et applications. Si l'objectif est de protéger la destination contre un accès direct, ses règles d'accès doivent être adaptées ; le simple changement d'adresse publique communiquée aux joueurs ne ferme pas l'ancienne adresse.

Certains logiciels peuvent voir l'adresse du proxy comme source de plusieurs utilisateurs. Les limites de connexions et mécanismes de confiance côté application doivent être adaptés sans ouvrir de contournement de sécurité. Une assistance spécifique n'est incluse que dans le périmètre annoncé.

3. Filtrage et limites

Le filtrage peut rejeter un trafic suspect et nécessite parfois un ajustement pour une application. HG-Hosting examine les faux positifs signalés avec des éléments techniques utiles. Une capacité globale de mitigation annoncée pour un réseau n'est pas une capacité dédiée à chaque contrat.

Une attaque exceptionnelle peut nécessiter une restriction temporaire de trafic ou de destination. La mesure doit rester nécessaire et proportionnée ; elle n'efface pas les engagements contractuels ni les recours applicables. La latence dépend également des réseaux d'accès et du chemin vers le backend.

4. Adresses et sortie

Les IP et ports sont attribués pour la durée du service et peuvent relever d'un opérateur tiers. Les conditions de changement, d'annonce BGP ou de portabilité sont celles expressément convenues ; aucune propriété ou portabilité universelle d'une adresse n'est promise.

À la fin du service, le client organise le changement de DNS ou d'adresse diffusée et retire les règles devenues inutiles. Les données de configuration exportables et la coopération de transition suivent les droits applicables.