

CONDITIONS PARTICULIÈRES

Prestations réseau

Tunnel IP protégé, adresses IP, sessions BGP avec ou sans protection anti-DDoS, et FiveBunker pour les serveurs FiveM hébergés ailleurs.

HelloServ et Flexicore sont des marques de FLEXICORE SAS, société par actions simplifiée immatriculée au RCS de Paris sous le numéro 989 715 958, dont le siège est situé Bureau 326, 78 avenue des Champs-Élysées, 75008 Paris, opérateur du système autonome AS215124.

Sommaire

Article 1 : Objet et documents applicables

Article 2 : Définitions

Article 3 : Tunnel IP protégé

Article 4 : Adresses IP et blocs

Article 5 : Sessions BGP

Article 6 : Session BGP avec protection

Article 7 : Protection d'un ASN du client : retrait de la protection

Article 8 : FiveBunker pour un serveur FiveM hébergé ailleurs

Article 9 : Usage du réseau, tests et abus

Article 10 : Données techniques du trafic

Article 11 : Durée, renouvellement et fin du service

Article 12 : Disponibilité, maintenance et responsabilité

Article 1: Objet et documents applicables

1.1. Les présentes conditions particulières s'appliquent aux prestations réseau suivantes, commandées auprès de HelloServ ou de Flexicore : tunnel IP protégé, adresses IP supplémentaires et blocs d'adresses, sessions BGP avec ou sans protection, transit IP associé à une colocation, et FiveBunker pour un serveur FiveM hébergé hors de HelloServ.

1.2. Elles complètent les Conditions générales de vente (CGV) et les Conditions générales d'utilisation (CGU) de HelloServ, publiées sur la page Mentions légales de helloserv.fr, ainsi que le devis accepté par le client lorsqu'il y en a un. Les renvois à un article des CGV ou des CGU visent la version en vigueur au jour de la commande ou du renouvellement.

1.3. En cas de contradiction, le devis accepté prévaut sur les présentes conditions particulières, qui prévalent elles-mêmes sur les CGV et les CGU. Pour tout ce qu'ils ne règlent pas, les CGV et les CGU s'appliquent.

1.4. Le client accepte les présentes conditions en validant sa commande, ou en signant le devis ou le contrat qui y renvoie. Elles restent consultables à tout moment sur la page Mentions légales de helloserv.fr et dans la page Documents de l'espace client. Une nouvelle version s'applique à partir du renouvellement qui suit sa publication.

Article 2: Définitions

2.1. Dans les présentes conditions :

- **Préfixe** : bloc d'adresses IP contiguës, par exemple un /24 en IPv4 (256 adresses).
- **ASN** : numéro de système autonome, qui identifie un réseau sur Internet. Celui de FLEXICORE SAS est AS215124.
- **Session BGP** : échange de routes entre le routeur du client et celui de HelloServ, par lequel HelloServ annonce sur Internet les préfixes du client.

- **LOA** : lettre par laquelle le titulaire d'un préfixe ou d'un ASN autorise son annonce par HelloServ.
- **IRR et RPKI** : registres publics qui déclarent quel ASN a le droit d'annoncer un préfixe (objets route dans l'IRR, enregistrements ROA dans la RPKI).
- **Débit garanti** : débit réservé au client et compris dans le prix de son offre.
- **95e percentile** : méthode de mesure du débit sur le mois. Le débit est relevé à intervalles réguliers, les 5 % de relevés les plus élevés sont écartés et le plus haut des relevés restants est retenu.
- **Blackhole** : mesure qui rend une adresse IP injoignable depuis Internet pour arrêter une attaque qui la vise.

Article 3 : Tunnel IP protégé

3.1. Le tunnel IP relie un serveur du client, hébergé hors de HelloServ, au réseau de HelloServ par un tunnel GRE ou WireGuard. Le trafic destiné aux adresses du tunnel est filtré par l'anti-DDoS de HelloServ, puis acheminé jusqu'au serveur du client.

3.2. Chaque tunnel comprend une adresse IPv4 et le débit garanti du palier choisi. Le tunnel accepte des pointes jusqu'à 1 Gbps. Le débit consommé au-delà du débit garanti est mesuré au 95e percentile et facturé au tarif en vigueur sur la facture du mois. Le trafic d'attaque filtré n'est jamais compté. Un courriel prévient le client lorsqu'il atteint 80 % de son débit garanti.

3.3. Lorsque le client choisit de limiter le tunnel à son débit garanti, aucun dépassement n'est facturé ; le débit au-delà est écrêté.

3.4. Le client installe et maintient la configuration du tunnel fournie par HelloServ sur son serveur ou son routeur. Le débit et la latence réellement obtenus dépendent aussi de la connexion du serveur chez son hébergeur, qui échappe à HelloServ.

3.5. Seul le trafic qui passe par le tunnel est protégé. Le trafic adressé directement à l'adresse du serveur chez son hébergeur ne l'est pas : il appartient au client de ne pas la publier et de la filtrer.

Article 4 : Adresses IP et blocs

4.1. Les adresses et blocs mis à disposition appartiennent aux ressources de FLEXICORE SAS (AS215124). Le client en a l'usage pendant la durée du service, pour ce seul service ; ils ne sont ni cessibles ni transférables, et reviennent à FLEXICORE SAS à la fin du service.

4.2. Le client qui attribue des adresses de ses blocs à ses propres clients répond de leur usage comme du sien et transmet à HelloServ, sur demande, les informations nécessaires au traitement d'un abus ou d'une réquisition.

4.3. Une adresse ou un bloc peut avoir été utilisé auparavant. HelloServ ne garantit pas qu'il soit absent de toute liste de blocage au moment de sa remise ; à la demande du client, elle l'aide à en obtenir le retrait.

Article 5 : Sessions BGP

5.1. Une session BGP permet au client de faire annoncer par HelloServ ses propres préfixes, à partir d'un /24 en IPv4, avec son propre ASN ou avec AS215124.

5.2. La commande d'une session BGP fait l'objet d'un contrat signé électroniquement et d'une vérification de l'identité du client : vérification d'identité (KYC) pour un particulier, extrait Kbis et pièce d'identité de son représentant légal pour un professionnel. La mise en service a lieu sur devis, après vérification par HelloServ des droits du client sur les préfixes et, le cas échéant, sur l'ASN : LOA, objets IRR et enregistrements RPKI cohérents avec l'annonce. Le client garantit être titulaire de ces droits ou autorisé à les exercer, et tient ces objets à jour pendant toute la durée du service.

5.3. Un préfixe qui n'a ni enregistrement RPKI valide ni objet IRR cohérent avec l'annonce n'est pas accepté. Une session BGP comprend au moins 100 Mbps de débit garanti, aux conditions de l'article 3.2.

5.4. Sans protection, une adresse visée par une attaque est mise en blackhole pendant la durée de l'attaque ; les autres adresses du client restent en service.

5.5. HelloServ peut refuser, suspendre ou retirer l'annonce d'un préfixe ou d'un ASN dont la légitimité n'est pas établie, qui figure sur une liste de réputation ou de blocage reconnue (Spamhaus DROP, EDROP ou ASN-DROP, par exemple), ou qui est associé à des activités illicites ou abusives.

Article 6 : Session BGP avec protection

6.1. Avec la protection, le trafic destiné aux préfixes du client est filtré par l'anti-DDoS de HelloServ et de ses fournisseurs de transit. La protection relève d'une obligation de moyens : lorsqu'une attaque, par son volume ou sa nature, dépasse les capacités du service ou menace l'infrastructure commune, l'adresse visée peut être mise en blackhole le temps nécessaire, même protégée.

6.2. Le client qui annonce ses préfixes avec son propre ASN s'engage, pendant toute la durée du service :

- à n'annoncer que les préfixes et ASN déclarés à HelloServ, et à ne pas faire bénéficier de la protection des préfixes ou ASN de tiers non déclarés, y compris en faisant passer leur trafic par ses adresses protégées (tunnel, traduction d'adresses ou proxy) ;
- à ne pas modifier ses objets IRR, ses AS-SET ou ses déclarations pour échapper aux contrôles ou à la facturation ;
- à ne pas proposer à des tiers une offre dont la protection anti-DDoS constitue l'activité principale ou fait l'objet d'une promotion, ni à revendre cette protection, sauf accord écrit préalable de HelloServ ;
- à ne présenter la protection que comme une caractéristique accessoire de ses propres services, sans la présenter comme développée ou détenue par lui, sans en exagérer les capacités et sans déclaration pouvant inciter à la tester ou à la contourner ;
- à ne pas émettre ni laisser émettre de trafic d'attaque depuis ses préfixes.

6.3. HelloServ peut exclure un ASN de la protection, notamment en cas de manquement à l'article 6.2, de déclaration inexacte, d'abus, d'atteinte à l'image de HelloServ ou de ses fournisseurs, d'inscription sur une liste de réputation, ou lorsque les préfixes hébergent des cibles qui attirent de manière récurrente des attaques disproportionnées mettant en péril l'infrastructure commune. L'ASN exclu continue d'être acheminé sans protection, aux conditions de l'article 5.4. HelloServ en informe le client sans délai.

Article 7 : Protection d'un ASN du client : retrait de la protection

7.1. Lorsque les préfixes du client sont annoncés avec son propre ASN et protégés, le client peut résilier le service à tout moment dans les conditions de l'article 11. La résiliation, qui met fin à l'annonce de ses préfixes par HelloServ, n'est soumise à aucune durée minimale.

7.2. Tant que ses préfixes restent annoncés par HelloServ, le client ne peut en revanche retirer la protection de son ASN (passage en session BGP sans protection) qu'à l'issue d'une durée minimale de six (6) mois à compter de son activation, moyennant un préavis de trois (3) mois notifié par écrit au support. Le préavis peut courir pendant la durée minimale. Le retrait prend effet à l'échéance mensuelle qui suit l'expiration du préavis, et au plus tôt à la fin de la durée minimale ; la protection et sa facturation sont maintenues jusqu'à cette date. Par exemple, pour une protection activée le 15 janvier, une demande de retrait notifiée le 2 mars prend effet le 15 juillet, une demande notifiée le 10 juin prend effet le 15 septembre.

7.3. Si les préfixes du client sont de nouveau annoncés par HelloServ moins de douze (12) mois après la fin de leur annonce, la protection reprend, et la durée minimale comme le préavis éventuellement en cours reprennent pour la durée qui restait à courir. Au-delà de douze mois, après un retrait de la protection ou après une exclusion, toute nouvelle activation de la protection ouvre une nouvelle durée minimale de six (6) mois.

7.4. À compter de son exclusion en application de l'article 6.3, l'ASN est facturé au tarif de la session BGP sans protection.

7.5. Lorsque les préfixes sont annoncés avec AS215124, la protection peut être retirée à tout moment : la session BGP, avec ou sans protection, suit l'article 11.

Article 8 : FiveBunker pour un serveur FiveM hébergé ailleurs

8.1. FiveBunker protège un serveur FiveM hébergé hors de HelloServ : les joueurs se connectent par une adresse protégée, et les points de contrôle de HelloServ vérifient chaque connexion avant de l'acheminer vers le serveur du client.

8.2. Le client choisit l'offre dont le nombre de joueurs est au moins égal au paramètre `sv_maxclients` de son serveur, et passe à l'offre supérieure lorsque ce paramètre augmente.

8.3. Le client applique dans son fichier `server.cfg` les lignes générées par HelloServ. Il est invité à n'ouvrir le port de son serveur qu'aux adresses des points de contrôle, selon la procédure fournie : le trafic adressé directement à l'adresse réelle du serveur n'est pas protégé.

8.4. Le client fournit sa propre clé de licence Cfx.re et respecte les conditions de la plateforme Cfx.re. Une adresse IP dédiée peut être commandée en option.

Article 9 : Usage du réseau, tests et abus

9.1. Outre les usages interdits par l'article 6 des CGU, le client s'interdit d'émettre du trafic avec une adresse source qui ne lui est pas attribuée, d'exploiter des services ouverts permettant d'amplifier une attaque, d'envoyer des courriels non sollicités et de mener des attaques ou des analyses non sollicitées contre des systèmes tiers.

9.2. Le client ne lance ni ne fait lancer de test de charge ou d'attaque simulée vers ses adresses ou vers l'infrastructure de HelloServ sans accord écrit préalable. Un tel test est traité comme une attaque.

9.3. Une adresse ou un préfixe qui émet une attaque ou du trafic malveillant, y compris à l'insu du client, peut être filtré ou isolé sans préavis, le temps de faire cesser ce trafic. HelloServ en informe le client.

9.4. Les signalements d'abus reçus par HelloServ (abuse@flexicore.fr) sont transmis au client, qui y donne suite dans les meilleurs délais. En cas d'abus avéré ou de risque pour l'infrastructure, HelloServ peut filtrer le trafic en cause, retirer une annonce ou suspendre le service, dans les conditions de l'article 8 des CGU.

Article 10 : Données techniques du trafic

10.1. Pour filtrer les attaques, mesurer le débit et traiter les abus, HelloServ et ses fournisseurs de transit traitent des données techniques du trafic (adresses IP, en-têtes des paquets, volumes, journaux des attaques), sans en lire le contenu. Ces données sont traitées pour leurs propres besoins de sécurité et de facturation, et conservées le temps nécessaire à ces fins.

10.2. Les données personnelles que le client traite sur ses propres serveurs restent sous sa seule responsabilité : HelloServ achemine le trafic sans héberger ces données.

Article 11 : Durée, renouvellement et fin du service

11.1. Les prestations réseau sont souscrites au mois, sans engagement au-delà de la période payée ; seul le retrait de la protection d'un ASN du client suit l'article 7.2. Le renouvellement, sa désactivation et les conséquences d'un défaut de paiement suivent l'article 9 des CGV (Durée, renouvellement et résiliation).

11.2. Le débit consommé au-delà du débit garanti au cours d'un mois reste dû, même si le service prend fin avant l'émission de la facture correspondante.

11.3. À la fin du service, HelloServ cesse d'acheminer le trafic et retire les annonces du client. Les adresses de FLEXICORE SAS reviennent à HelloServ.

11.4. Une suspension ou une résiliation prononcée pour manquement aux CGU, aux CGV ou aux présentes conditions ne donne lieu à aucun remboursement (article 10 des CGV).

Article 12 : Disponibilité, maintenance et responsabilité

12.1. HelloServ ne s'engage pas sur un taux de disponibilité chiffré. L'état de ses services est publié en temps réel sur status.helloserv.fr.

12.2. HelloServ ne répond ni de la connexion du serveur du client chez son hébergeur, ni des réseaux tiers empruntés par le trafic avant d'atteindre son réseau ou après l'avoir quitté.

12.3. Les opérations de maintenance de HelloServ et de ses fournisseurs de transit peuvent entraîner de courtes interruptions. Sauf urgence, elles sont annoncées à l'avance lorsque HelloServ en a connaissance.

12.4. Une interruption causée par une attaque venant d'un tiers, alors que la protection était en place, ne donne lieu à aucun remboursement.

12.5. Lorsque le client agit à titre professionnel, la responsabilité de HelloServ est limitée aux dommages directs et plafonnée aux sommes qu'il a payées pour le service en cause pendant les douze (12) mois précédant le fait générateur ; les dommages indirects (perte de chiffre d'affaires, de données, de clientèle ou d'image) ne sont pas indemnisés. Cette limite ne s'applique pas en cas de faute lourde ou intentionnelle. Le client consommateur conserve l'ensemble des droits que lui reconnaît la loi.