CONDITIONS SPECIFIQUES DE VENTE

Solution Anti DDoS

Applicables à compter du 1er Septembre

Les présentes Conditions Spécifiques s'appliquent à l'Offre dite de Solutions Anti DDoS lorsque celle-ci est incluse par Monaco Telecom ou souscrite par le Client en complément des Services éligibles tel que mentionné dans le Bon de Commande correspondant. Elles complètent selon la Commande du Client les Conditions Spécifiques de Vente Connectivity ou les CGV Solutions Entreprise correspondantes (« **CGV** »). En cas de contradiction entre les présentes Conditions Spécifiques et les CGV, les stipulations des premières prévaudront.

Ces conditions sont régulièrement portées à la connaissance du Client pour lui permettre de passer commande. Les tarifs et descriptions d'Offres applicables sont précisés au Bon de Commande.

1. Définitions

Les termes ci-après, utilisés au singulier ou au pluriel, ont dans le cadre des présentes la signification suivante :

- **Adresse IP** : désigne l'adresse affectée à chaque station connectée à internet (on parle alors d'adresse IP publique) et plus généralement à tout équipement physique qui utilise le protocole TCP/IP.
- **Solution(s) Anti-DDoS** : désignent la/les solution(s) applicative(s) permettant la détection automatique, la sécurisation et protection des flux de données transitant sur les liens inclus dans les Offres Monaco Telecom éligibles contre les Attaques DoS/DDoS visant à rendre indisponible un service et d'empêcher ainsi les utilisateurs légitimes de bénéficier de ce service.
- **Anti-DDoS Standard** : désigne le Service standard permettant une protection volumétrique applicable sur les flux des protocoles UDP, ICMP et TCP incluse dans le Backbone Internet, proposé par MT sur lequel reposent les Offres Connectivity ou Offres Cloud Serveurs.
- **Anti-DDoS Protector** : désigne l'Offre permettant une protection volumétrique et/ou applicative, applicable sur les flux du protocole UDP souscrite par le Client sur lequel reposent les Offres Connectivity ou Offres Cloud Serveurs pouvant aller jusqu'à une protection de niveau 7.
- **Anti DDoS Optimum** : désigne l'Offre permettant une protection intégrale, volumétrique et/ou applicative, applicable sur les flux des protocoles UDP, ICMP et TCP souscrite par le Client sur lequel reposent les Offres Connectivity ou Offres Cloud Serveurs pouvant aller jusqu'à une protection de niveau 7.
- **Attaque DoS/DDoS** : littéralement « Denial of Service » (déni de service) ou « Distributed Denial of Service » (ou déni de service distribué) désigne une attaque malveillante et potentiellement massive, à l'encontre des réseaux ou des services, visant à rendre ceux-ci inefficients.
- **Backbone** ou **Backbone Internet** : désigne le réseau de transmission multiservice central de MT faisant l'agrégation entre plateformes de service et plateformes d'accès.
- **Bande Passante Internet** : désigne la capacité de transmission (mesurée en Mbit/s) du raccordement à internet affectée à l'usage du Client.
- **Cibles IP** : désigne les adresses IP publiques, selon la définition de la RFC 1918, désignées pour la mise en place de l'option et susceptibles selon le Client et l'analyse des flux par MT, d'être visées par les Attaque DoS/DDoS.
- **Data Center** : désigne le centre de stockage (ou d'hébergement) des données, il est un site sécurisé MT pour l'hébergement de serveurs informatiques et d'applications du Client.
- **Données** : désignent sans que cela soit limitatif, les informations de toute nature (notamment applications informatiques et base de données) appartenant au "Client", générées, collectées et/ou stockées par lui.
- **Fibre Optique** : désigne le fil transparent ayant la capacité de conduire des signaux lumineux permettant ainsi de transporter un débit important de données et supportant un Réseau local à large Bande Passante.
- **Heures d'Ingénierie** : Désigne le quota d'heures disponible pour le Client auprès des équipes techniques MT en vue de procéder à des re-paramétrages de sa Solution Anti-DDoS postérieurement à la période de Simulation. Les Heures d'Ingénierie seront utilisables en une ou plusieurs fois, à la discrétion du Client.
  Les quotas octroyés sans surcoût à la souscription sont les suivants :
  - Anti DDoS Protector : 4 heures ;
  - Anti DDoS Optimum : 8 heures ;

  Toute demande supplémentaire du Client après utilisation du quota fera l'objet d'un BdC et sera facturé après évaluation et selon le barème établi par MT.
- **ICMP** ou **Internet Control Message Protocol** : Protocole de niveau 3 servant au signalement des problèmes, utilisé par le protocole IP
- **Infrastructure IT du Client** : désigne l'environnement informatique et réseau existant sur le Site Client, sous sa responsabilité tel que décrit par lui et objet de l'évaluation des flux pendant la phase préalable à l'implémentation.
- **Jours Ouvrés** : représente une journée de 10 heures ouvrées (actuellement de 8h à 18h) entre le lundi et le vendredi hors jours fériés monégasques tels que publiés au journal officiel monégasque.
- **Simulation** : période post-signature du BdC durant laquelle l'Equipement opérera l'ensemble de ses opérations de traitement et d'analyses de trafic mais n'appliquera pas effectivement la politique de filtrage, en ce sens que les flux et/ou paquets détectés comme malicieux ne seront pas rejetés, mais réinjectés vers les équipements du Client. Les alertes utiles à la restitution analytique seront notamment produites.
- **Sonde :** désigne l'équipement utilisé par MT pour assurer notamment le nettoyage des flux dans le cadre des Solutions Anti-DDoS
- **TCP** ou **Transmission Control Protocol** : Protocole connecté, de transport ISO de niveau 4
- **UDP** ou **User Datagram Protocol** : Protocole non connecté, de transport ISO de niveau 4

2. Objet

Les présentes Conditions Spécifiques ont pour objet de définir les conditions et modalités selon lesquelles MT fournit au Client, l'Anti-DDoS Standard et l'Anti DDoS Protector ou Optimum si le Client y souscrit.

Par la signature du Contrat, le Client reconnaît avoir vérifié l'adéquation à ses besoins, de l'Offre choisie, et accepte les présentes CSV sans réserve.

3. Description du Service

Les Solutions Anti-DDoS consistent en particulier à :

- analyser le trafic réseau à destination des services du Client, grâce aux Sondes
- intercepter, via ces Sondes, le trafic entrant dans ses serveurs
- minimiser ou bloquer l'Attaque DoS/DDoS, en agissant sur tout ou partie des paquets IP non légitimes reçus afin de laisser passer les paquets IP autorisés

Compte tenu des standards des métiers, la mise en œuvre d'une protection Anti-DDoS ne peut être constitutive d'une obligation de résultat quant à la capacité de bloquer les Attaques DoS/DDoS mais de mettre en œuvre les mesures de minimisation ou de blocage des flux malveillants identifiés. Dans le cas ultime où les mécanismes seraient insuffisants pour traiter une Attaque DoS/DDoS trop violente, MT se réserve le droit d'agir comme pour tout accès client (protégé ou non par les protections Anti-DDoS) en isolant l'accès client du réseau pendant la durée des effets constatés.

3.1 L' Anti-DDoS Standard permet d'assurer une mise en œuvre des mesures techniques agissant sur les protocoles UDP, ICMP et TCP dans le but d'améliorer le maintien des connexions légitimes entre internet et le Backbone Internet MT, alors qu'une Attaque DoS/DDoS vise tout ou partie du réseau MT.

3.2. L'Anti DDoS Protector permet d'assurer une mise en œuvre des mesures techniques agissant sur le protocole UDP dans le but d'améliorer le maintien des connexions légitimes entre internet et les infrastructures IT du Client alors qu'une Attaque DoS/DDoS vise à nuire à ses Infrastructures IT.

Lorsqu'elle est souscrite, la solution Anti-DDoS Protector s'ajoute de facto à la protection Anti-DDoS Standard.

3.3 L'Offre Anti-DDoS Optimum permet d'assurer une mise en œuvre des mesures techniques agissant sur les protocoles UDP, ICMP et TCP dans le but d'améliorer le maintien des connexions légitimes entre Internet et les infrastructures IT du Client alors qu'une Attaque DoS/DDoS vise à nuire à ses Infrastructures IT.

Le Client reçoit une notification l'informant de l'attaque en fonction de critères spécifiques définis lors de la souscription.

Lorsqu'elle est souscrite, l'Offre Anti-DDoS Optimum s'ajoute de facto à la protection Anti-DDoS Standard.

3.4. Périmètre de la protection :

L'Anti-DDoS Optimum et l'Anti-DDoS Protector s'appliquent sur le volume de bande passante de l'ensemble de liens portant les Adresses IP déclarées.

4. Mise en service

La mise en service peut être conditionnée par la conformité de l'environnement client à certains prérequis techniques. En tout état de cause, l'Anti DDoS Protector ou Optimum est ajustée en tenant compte du niveau de prévention souhaité, des éléments décrits dans le Bon de Commande et des dispositions techniques convenus lors de la période de Simulation.

A l'issue des opérations nécessaires à la mise en service, MT confirme par tout moyen jugé approprié par elle, le bon fonctionnement et l'activation de la protection Anti-DDoS Protector ou Optimum mise en œuvre.

Le Client reconnaît expressément être informé du fait que MT procèdera à une période de Simulation technique du Service basée sur les informations que le Client peut communiquer à MT. La période de Simulation technique durera cinq (5) jours ouvrés. Cette période sera suivie d'une permettra la restitution analytique par MT avec le Client.

Dans cette phase de Simulation, le Client participera activement et avec la transparence requise, avec les experts de MT, à l'identification et à la qualification précise de ses besoins dans le but d'adapter au mieux la protection à son besoin.

Toute demande de modification postérieurement à la phase de Simulation entraînera un décompte du quota d'Heures d'Ingénierie calculé par Monaco Telecom sur la base de son propre barème.

Le Client reconnaît et accepte que les modalités de calcul ainsi que l'évaluation des Heures d'Ingénierie nécessaires au paramétrage demandé ne pourront faire l'objet d'aucune contestation.

Toute demande formulée par le Client après utilisation de son quota d'Heures d'Ingénierie donnera lieu à établissement d'un BdC et à une facturation spécifique. Sous réserve du respect des conditions d'éligibilité de l'Offre définies par MT, la disponibilité du Service n'est assurée qu'à l'issue d'un délai de vingt-et-un (21) jours à compter de la signature de la Commande, et la désignation des Cibles IP et services à protéger.

Le Client est responsable de tous dommages causés de son fait ou par l'utilisation qu'il fait de sa protection anti-DDoS et des Services souscrits auxquels il l'associe, et leur impact sur les installations et/ou infrastructures Client et de MT, ses sous-traitants et/ou ses autres Clients.

Le Client reconnaît être informé que toute opération ou test ou changement de configuration menée par lui-même ou un tiers et susceptible d'impacter le fonctionnement de la protection Anti-DDoS ou de l'infrastructure MT et ne répondant pas aux critères d'utilisation devra faire l'objet d'une information adressée à MT qui précise tout élément pertinent pour l'ajustement éventuel de la configuration selon la faisabilité et l'éligibilité techniques ; à défaut d'information, MT ne pourra proposer les solutions adaptées aux besoins ;

5. Limites du Service :

MT est tenue à une obligation de moyens et non de résultat sur la fourniture et le niveau d'efficacité des solutions incluses ou souscrites au titre des présentes sans être tenue à un taux d'échec ou de succès particulier.

MT ne saurait garantir la bonne réception des notifications adressées au Client dans le cadre de l'Anti-DDoS Optimum, celles-ci ayant un caractère purement informatif.

Le service fonctionne de manière optimale par rapport à ses caractéristiques à condition que le Client ait dûment respecté ses obligations pendant la phase d'implémentation du service.

Le Client est seul et entièrement responsable des Données, de leur exploitation et de l'utilisation ainsi que de la sécurité globale de ses Infrastructures et ses choix techniques.

6. Entrée en vigueur et durée du Contrat - Durée du Bon de Commande

L'Offre entre en vigueur à compter de sa souscription sur le Bon de Commande. Elle coure jusqu'à son arrêt demandé par le Client moyennant un préavis de quinze (15) jours, et à défaut pour la durée restant à courir du Contrat portant les offres sur lesquelles l'Offre s'appuie, conformément aux CGV.

7. Conditions Financières

7.1 Le tarif mensuel de la solution Anti DDoS, des éventuelles options associées et les frais de mise en service associés, spécifiques au niveau de vigilance requise par le Client, sont précisés dans le BdC après analyse du besoin par MT. Le prix récurrent de l'Offre est fixé dans le Bon de Commande selon les tarifs applicables auprès de MT pour la configuration retenue. La date de début de la facturation de l'Offre Anti-DDoS concernée interviendra à la date de Mise en Service susvisée.

7.2. La tarification de l'Offre s'applique selon la règle suivante :
Une Offre Anti-DDoS peut être souscrite pour un ou plusieurs Service(s) éligible(s) par Client. Le choix de l'Offre Anti-DDoS devra alors correspondre au volume cumulé des bandes passantes souscrites pour chaque Service éligible à considérer dans le périmètre de protection comme souhaité par le Client. Toute demande de changement d'Offre fera l'objet d'une étude de faisabilité compte tenu des configurations techniques que le changement d'offre impliquera.