Description de service : « Cisco Cloud Web Security Service » Service Cisco de sécurité de l'informatique en nuage sur le Web

Ce document définit les caractéristiques et les fonctionnalités du service Cisco de sécurité de l'informatique en nuage sur le Web (le « Service »). Selon que vous avez acheté la version Essentials ou la version Premium du Service, toutes les fonctionnalités décrites ci-après peuvent ne pas être disponibles (comme cela est indiqué dans la Section 3 ci-dessous).

Si vous avez souscrit à ce service auprès d'un partenaire Cisco agréé, ce document n'a qu'un caractère informatif. Par ailleurs, le contrat (s'il y a lieu) régissant la prestation du service est celui que vous avez conclu avec votre partenaire Cisco agréé. Votre partenaire Cisco agréé doit vous fournir ce document. Vous pouvez également en obtenir une copie à l'adresse suivante : www.cisco.com/web/CA/about/doing_business/legal/service_descriptions/index_fr.html.

Les termes en majuscules sont définis dans le Glossaire qui figure à la fin du présent document.

1. Présentation

1.1 Le service Cisco de sécurité de l'informatique en nuage sur le Web est fourni par le biais de matériel et de logiciels déployés dans des centres de données gérés par Cisco. Cisco conservera la propriété, le cas échéant, de tous les composants d'infrastructure matérielle utilisés dans ses centres de données dans le cadre du Service.

1.2 Le service n'inclut pas de connexion d'accès à Internet ni de matériel nécessaire pour établir une telle connexion, le client étant tenu de s'en charger.

1.3 Les services qui ne sont pas expressément exposés dans la présente description de service ne sont pas couverts. Cela comprend, sans toutefois s'y limiter, les éléments suivants :

a) Toute personnalisation de logiciel ou de matériel ou toute main-d'œuvre requise pour installer les Logiciels ou le Matériel.

b) Toute dépense engagée lors d'une visite chez le client, sauf si elle jugée nécessaire par Cisco en cas de renvoi d'un problème à un niveau supérieur d'assistance.

c) Les services ou logiciels permettant de résoudre des problèmes liés à des logiciels ou du matériel résultant d'un produit tiers, de causes échappant au contrôle de Cisco ou d'un manquement du client envers ses responsabilités telles qu'elles sont exposées dans la présente description de service.

d) Services relatifs à des produits ne provenant pas de Cisco mais utilisés dans le cadre du service.

1.4 Certaines options de déploiement peuvent obliger le client à télécharger et à installer un Logiciel Cisco (par ex. le Logiciel Connector ou AnyConnect, comme cela est décrit ci-après). L'utilisation dudit Logiciel est régie par des contrats de licence d'utilisateur final distincts, qui seront mis à disposition lors du téléchargement du Logiciel en question. Sauf indication contraire mentionnée dans lesdits contrats, les droits relatifs au Logiciel, notamment les médias, la documentation, le code binaire, le code source ou l'accès par voie électronique ou autre ne sont pas fournis.

2. Responsabilités de Cisco

2.1 Tant que le client s'acquitte de tous les frais applicables, Cisco :

a) Fournira le service conformément à la commande du client;

b) Fournira toutes les mises à jour et versions commercialisées par Cisco;

c) Fournira des efforts commercialement raisonnables pour résoudre les problèmes techniques inhérents au service. Cisco n'offre aucune assistance technique pour tout matériel ou logiciel tiers non acheté et/ou autorisé par Cisco.

3. Fonctionnalité

3.1 La version Essentials du Service comprend la Détection de logiciels malveillants sur le Web et le Filtrage Web. La version Premium du Service inclut également une Protection avancée contre les logiciels malveillants et l'outil d'analyse Cognitive Threat Analytics. Les fonctionnalités du Service sont décrites ci-dessous.

3.2 Les demandes HTTP, HTTPS et FTP sur HTTP externes du client (y compris les pièces jointes, macros et exécutables) sont acheminées par le biais du service. Les paramètres de configuration requis pour acheminer ce trafic externe via le service sont définis et gérés par le client (avec l'aide et l'assistance de Cisco, dans la limite du raisonnable) et dépendent de l'infrastructure technique de ce dernier. Le client doit

s'assurer que le trafic HTTP, HTTPS et FTP sur HTTP interne (par ex. le trafic du réseau intranet de l'entreprise) ne transite pas via le service.

Détection de logiciels malveillants sur le Web (« MS »)

3.3 Dès que les modifications appropriées de la configuration sont effectuées, les pages Web et pièces jointes non chiffrées seront analysées par la plateforme de sécurité privée Outbreak Intelligence™, qui détecte les menaces de programmes malveillants grâce à une association de diverses technologies de détection adaptées, notamment des moteurs anti-programmes malveillants de pointe.

3.4 L'APM analysera autant de pages Web et de pièces jointes que possible. Il se peut que certaines pages Web ou pièces jointes ne puissent faire l'objet d'une analyse (en raison d'une protection par mot de passe, par exemple). Les pièces jointes qui ne peuvent pas être analysées seront bloquées. Le trafic chiffré (HTTPS ou SSL par ex.) ne peut pas être analysé et sera transféré vers les éléments non analysés de l'APM (sauf si l'Inspection HTTPS est activée, comme cela est décrit dans le paragraphe 3 ci-après).

3.5 Si une page Web ou une pièce jointe demandée renferme un programme malveillant (ou si elle est jugée inanalysable conformément au paragraphe 3.4, sauf pour le trafic SSL), l'accès à cette page ou à la pièce jointe est refusé et une page Web d'alerte s'affiche automatiquement à l'écran. Une notification peut également être adressée par courriel à l'administrateur du client.

Filtrage Web (« FW »)

3.6 Dès que les modifications appropriées de la configuration sont effectuées, les pages Web et pièces jointes seront filtrées à l'aide d'un outil de catégorisation des adresses URL et d'analyse du contenu à la pointe de la technologie. Les adresses URL sont classées suivant un nombre de catégories prédéfinies, comme cela est indiqué au paragraphe consacré au Portail (voir ci-après).

3.7 Le client peut configurer le FW pour créer des stratégies de restriction d'accès (basées sur les catégories et les types de contenu) et les appliquer, à des moments précis, à des utilisateurs ou groupes en particulier. De nombreuses fonctionnalités supplémentaires (fonctionnalité de liste « bloquée » ou « autorisée ») sont également disponibles.

3.8 Le FW filtrera autant de pages Web et de pièces jointes que possible. Il se peut que certaines pages Web ou pièces jointes ne puissent faire l'objet d'un filtrage (en raison d'une protection par mot de passe, par exemple). Le client a également la possibilité de configurer des exceptions spécifiques pour les sites Web ne devant pas être filtrés. Le trafic chiffré (HTTPS ou SSL par ex.) ne peut pas être filtré et sera transféré vers les éléments non filtrés du FW, sauf si le client indique une autre action à entreprendre en lien avec les catégories spécifiques de contenu. Le FW filtrera uniquement les pages Web catégorisées par FW conformément à la catégorie que le client a choisi de filtrer.

3.9 Le client peut employer des fonctions d'administration d'utilisateurs individuels et/ou de groupes et d'élaboration de rapports, disponibles grâce au logiciel Connector décrit ci-après.

3.10 Si un utilisateur demande une page Web ou une pièce jointe pour laquelle une stratégie de restriction d'accès s'applique, l'accès à cette page Web ou pièce jointe est refusé et une page Web d'alerte s'affiche automatiquement à l'écran. Une notification peut également être adressée par courriel à l'administrateur du client.

Inspection HTTPS

3.11 Lorsqu'elle est activée, la fonction Inspection HTTPS permet à l'administrateur de définir une stratégie déterminant quels domaines et catégories de trafic HTTPS sont déchiffrés et inspectés par l'infrastructure d'analyse. Normalement, les données sont chiffrées depuis le serveur Web vers la tour d'analyse. Néanmoins, pour les sites que le client souhaite inspecter, la tour d'analyse met fin à la connexion SSL, inspecte les données de la même manière que pour le trafic HTTP, puis chiffre à nouveau le trafic depuis la tour d'analyse vers l'utilisateur final à l'aide d'un certificat différent. L'organisme de certification correspondant devra être déployé comme organisme de certification approuvé sur les navigateurs Web du client afin d'empêcher que des avertissements de discordance de domaine ne s'affichent à l'écran des utilisateurs finaux. L'Inspection HTTPS peut être utilisée pour détecter les programmes malveillants et mener des actions de filtrage Web, comme le Contrôle de contenu sortant.

Contrôle de contenu sortant

3.12 Le Contrôle de contenu sortant permet aux clients disposant du composant Filtrage Web de définir des règles basées sur la fonction POST du protocole HTTP. Ces filtres recherchent des fichiers en particulier jouissant de certaines caractéristiques (totaux de contrôle MD5 ou SHA1 par ex.), réalisent une analyse des mots-clés, des types de fichiers entrants, des identifiants préconfigurés (numéro de carte bancaire ou de sécurité sociale par ex.) et recherchent des expressions DFA récurrentes.

Pages d'alerte de blocage

3.13 Les pages d'alerte de blocage sont des pages HTML créées de manière dynamique et qui sont affichées aux utilisateurs finaux lorsque ces derniers sont privés d'accès à du contenu Web interdit. Le client a le choix entre une page d'alerte de blocage standard et son propre contenu personnalisé qu'il peut télécharger via le Portail (voir ci-après). Cisco se charge d'héberger les pages bloquées.

Logiciel Connector

3.14 Sur demande du client, Cisco fournira le logiciel Connector afin que le client l'installe dans son réseau conformément aux directives d'installation indiquées par Cisco. Le logiciel Connector n'est pas compatible avec l'ensemble des systèmes et dispositifs potentiels du client.

3.15 Le logiciel Connector permet aux utilisateurs de se connecter au service sans adresse IP statique grâce à une clé d'authentification. Si des utilisateurs bénéficient d'autres services nécessitant une adresse IP fixe pour fins d'identification, ils peuvent configurer des connexions directes pour des sites Web, des domaines, des hôtes ou des réseaux spécifiques.

3.16 Les administrateurs ont la possibilité de créer, révoquer, activer et désactiver les clés d'authentification du logiciel Connector par groupe ou par utilisateur individuel.

Cisco AnyConnect (mobilité sécurisée)

3.17 Si le client le commande, Cisco fournira le logiciel AnyConnect afin que le client l'installe sur les PC et ordinateurs portables de ses utilisateurs finaux conformément aux directives d'installation indiquées par Cisco. AnyConnect ne prend pas en charge les paramètres de configuration des clients potentiels.

3.18 AnyConnect permet au PC ou à l'ordinateur portable de l'utilisateur final de se connecter au service depuis un emplacement distant en dehors du réseau interne du client. Ce logiciel n'a pas besoin d'adresses IP fournies.

Protection avancée contre les logiciels malveillants (PALM)

3.19 La Protection avancée contre les logiciels malveillants (PALM) est incluse avec le Service Premium et peut être commandée séparément par les clients ayant souscrit la version Essentials du Service. En cas de commande par le client, Cisco fournira la technologie PALM au client en vue de réaliser des analyses des fichiers au niveau de la passerelle pour détecter toute menace de logiciel malveillant. Cette fonctionnalité renforce les fonctions de détection et de blocage des logiciels malveillants offertes par la Détection de logiciels malveillants sur le Web.

3.20 Des hachages cryptographiques de fichiers sont recueillis et transmis à un serveur infonuagique géré par Cisco, où une analyse est réalisée afin de déterminer si le fichier est malveillant, neutre ou inconnu.

3.21 Si aucune détermination ne peut être réalisée à l'issue de l'analyse du hachage d'un fichier, le client a la possibilité d'envoyer le fichier vers un autre bac à sable infonuagique géré par Cisco afin d'y être analysé plus en profondeur. Le client peut configurer la PALM de manière à limiter le type de fichiers envoyés vers le bac à sable.

3.22 À l'issue de l'analyse du fichier, un rapport sur la réputation, un rapport sur le comportement du fichier et des alertes rétrospectives de verdict sont mis à disposition via le Portail.

Cognitive Threat Analytics

3.23 L'outil d'analyse Cognitive Threat Analytics (CTA) est inclus avec le Service Premium et peut être commandé séparément par les clients, avec la technologie PALM, afin de passer à la version Essentials du Service. S'il est inclus dans le Service commandé par le client, l'outil CTA effectue une analyse comportementale des journaux Web générés par le Service et identifie le trafic anormal qui indique de possibles infections par des logiciels malveillants, une activité malveillante ou des violations de politiques sur le réseau du client (les « Incidents »). L'outil CTA génère alors un Rapport d'incidents, que le client pourra consulter via le Portail. Le Rapport d'incidents de l'outil CTA dresse la liste des Incidents qui indiquent des hôtes potentiellement infectés sur le réseau du client communiquant par l'intermédiaire du Service.

3.24 Cisco ne garantit pas la disponibilité des rapports du Portail ni l'identification ou le signalement précis des Incidents par l'outil CTA. La détection et le signalement des Incidents dépendent de l'environnement du réseau du client et de nombreux autres facteurs sur lesquels Cisco n'exerce aucun contrôle.

3.25 Il incombe au client d'examiner et/ou d'atténuer les Incidents signalés par l'outil CTA. Cisco n'est aucunement responsable de l'examen et/ou de l'atténuation des Incidents.

3.26 Pour que l'outil CTA fonctionne de manière optimale, il incombe au client de configurer son trafic réseau de manière à ce que chaque utilisateur final dispose d'une identité distincte et unique. Le client doit veiller à ce que plusieurs utilisateurs ne disposent pas de la même identification. Si des identités distinctes et uniques des utilisateurs ne sont pas fournies, les analyses comportementales de l'outil CTA se baseront sur l'adresse IP du client et risquent de ne pas générer des Rapports d'incidents précis.

Portail

3.27 Le client bénéficiera d'un accès à un portail Web, hébergé par Cisco, qui lui permettra de gérer et d'élaborer des rapports sur le service. L'accès au Portail, qui se fait via un site Web sécurisé (protocole HTTPS), est protégé par mot de passe.

3.28 Le client peut disposer de plusieurs administrateurs pour un seul et même compte. Le client peut octroyer à chaque administrateur un identifiant unique et offrir un accès complet ou des privilèges de lecture seule à chacun des utilisateurs. Cette fonctionnalité permet à un seul et unique compte de « super-utilisateur » de créer plusieurs comptes d'administrateurs.

3.29 Le Portail permet à l'administrateur du client :

a) d'analyser les statistiques des programmes malveillants et autre contenu Web bloqués;

b) de générer des rapports en lien avec les outils PALM et CTA du Service (le cas échéant);

c) de créer des restrictions d'accès et de les appliquer à des utilisateurs ou groupes en particulier (si le logiciel Connector a été installé);

d) de personnaliser les pages d'alerte s'affichant sur les navigateurs et visualisées par les utilisateurs lorsqu'ils accèdent à un site Web ou à un fichier en particulier dont l'accès est refusé;

e) de mettre à jour les détails d'administration pour les alertes électroniques en temps réel; et

f) de configurer et de programmer une création automatisée de contrôles et de rapports sur le système.

3.30 Les rapports automatisés sont axés sur le trafic global, la bande passante, les adresses URL bloquées, les fichiers malveillants et les programmes malveillants paralysés. Le Portail propose également une sélection complète de rapports supplémentaires, créés quotidiennement, qui fournissent une analyse approfondie sous la forme de graphiques, de tableaux et de fichiers de données exportables. Le client peut programmer des rapports réguliers pour différentes fonctions du service et spécifier des utilisateurs, des plages horaires, et les envoyer par courriel à certains utilisateurs ou groupes.

3.31 La fonction de Consignation des contrôles enregistre les modifications d'administration, de configuration, de filtrage et de stratégies apportées pour le service. Elle peut être configurée par les administrateurs jouissant d'un accès complet ou par le super-utilisateur. Les Contrôles indiquent l'auteur, la nature et la date de la modification. Les journaux de contrôle peuvent faire l'objet d'une recherche en fonction d'une plage horaire, d'une catégorie ou d'un type de journal et d'un type d'action entreprise.

3.32 Lorsqu'elle est activée, la fonction de Consignation confidentielle enregistre le moment auquel les pages Web sont bloquées selon la stratégie de filtrage Web, mais ne divulgue pas les détails privés comme le nom d'utilisateur source et l'adresse IP. Cette fonction est destinée aux clients devant se conformer à des politiques ou réglementations locales encadrant le respect de la vie privée.

4. Maintenance et mises à jour

4.1 Cisco exécute périodiquement des opérations d'entretien programmées visant à actualiser les serveurs et les logiciels utilisés pour la prestation du service. Cisco entreprendra des efforts raisonnables pour informer le client au moins cinq (5) jours ouvrables à l'avance de toute période d'arrêt prévue ou de toute maintenance programmée. Nonobstant ce qui est indiqué dans les présentes, le client accepte que Cisco puisse dans certaines situations être dans l'obligation d'exécuter sans préavis diverses opérations urgentes d'entretien.

4.2 Cisco se réserve le droit de modifier et de mettre à jour les fonctionnalités des Services, sans que cela n'engendre de coûts supplémentaires pour le client, dans le but de fournir au client des Services de qualité égale ou supérieure. Ces mises à jour doivent inclure toute version ultérieure des Services contenant des améliorations fonctionnelles, des extensions, des corrections d'erreurs ou des correctifs qui sont généralement mis à disposition gratuitement aux clients ayant souscrit le niveau approprié des Services. Les mises à jour n'incluent aucune version, aucune option ni aucun produit futur que Cisco concède sous licence séparément ou qui ne sont pas inclus au titre du niveau de soutien applicable.

4.3 Cisco transmettra au client un préavis écrit en cas de modification ou de mise à jour importante. Cisco emploiera des efforts raisonnables pour veiller à ce que de telles modifications ou mises à jour n'aient pas d'impact négatif majeur sur la performance des Services ou sur l'usage que fait le client des Services. Cisco veillera à ce que les modifications ou mises à jour ne contraignent pas le client à devoir s'acquitter d'un coût supplémentaire important pour continuer à utiliser les Services.

4.4 Cisco emploiera des efforts raisonnables pour mettre en œuvre les modifications ou mises à jour de manière à limiter au maximum tout impact sur l'utilisation que fait le client des Services. Cisco préviendra le client de toute maintenance programmée au moins sept (7) jours à l'avance. Le cas échéant, les opérations de maintenance programmée seront réalisées au cours des fins de semaine ou entre 20 h et 8 h (heure locale du client). Cisco peut se voir contraint de réaliser des opérations de maintenance d'urgence à d'autres moments en cas de problème urgent (sans préjudice des dispositions de la Section 10).

5. Conditions tarifaires

5.1 Le client doit informer Cisco dans les 14 jours si le nombre de licences nécessaires augmente de plus de 5 % par rapport au nombre de licences alors déclaré. Cisco se réserve le droit d'exiger du client qu'il achète des licences supplémentaires si le nombre réel d'utilisateurs distincts (indiqué par les journaux de trafic Web de Cisco) est supérieur au nombre de licences octroyées périodiquement.

5.2 La tarification est fonction de la bande passante maximale par Licence du client (trafic entrant ou sortant, le plus élevé étant retenu, mesuré sur la base du 95e centile), qui ne devra pas dépasser une moyenne de 15 Kbit/s au cours d'un mois civil donné. Les frais facturés seront augmentés proportionnellement si ce niveau est dépassé pendant au moins deux mois civils. Cisco informera le client en cas de dépassement de ce niveau au cours d'un mois donné. Une telle notification sera adressée dans les 10 jours ouvrables suivant la fin du mois en question.

5.3 Si le client a commandé le Service pour des points d'accès à Internet sans fil et que la tarification est ainsi basée sur le niveau de bande passante plutôt que sur le nombre de Licences, les dispositions suivantes s'appliquent :

a) Le niveau de bande passante utilisé par le client sera déterminé en employant la méthodologie suivante :

b) Cisco générera un rapport mensuel (à l'aide de l'outil d'élaboration de rapports WIRe) indiquant le volume moyen de données transmis par seconde au cours du mois en question par plages de 5 minutes, vers ou depuis les utilisateurs finaux du client pour chaque centre de données utilisé par le client (le ou les « Échantillon(s) de trafic »).

c) Cisco classera les Échantillons de trafic par taille pour chaque centre de données.

d) Cisco exclura les 5 % les plus élevés de tous les Échantillons de trafic pour chaque centre de données.

e) Le niveau de trafic pour chaque centre de données sera considéré comme équivalant au débit moyen de données transmises au cours du prochain Échantillon de trafic le plus élevé (c.-à-d. le 95^{e} centile), divisé par 300 (soit le nombre de secondes en 5 minutes).

f) Le niveau total de trafic sera considéré comme équivalant à la somme des chiffres du 95^{e} centile pour chaque centre de données.

g) Cisco fournira au client des détails relatifs aux rapports et calculs mentionnés ci-dessus et utilisés au cours d'un mois civil donné. Une telle notification sera adressée dans les 20 jours ouvrables suivant la fin du mois en question.

À la suite d'une telle notification de la part de Cisco, si au cours d'un mois civil donné la bande passante maximale du client dépasse le niveau de bande passante précédemment commandé, le client devra passer une nouvelle commande (au même tarif par Mbit/s) afin que le niveau total de bande passante commandé continue à être supérieur à la bande passante maximale du client (le nombre sera arrondi à la dizaine de Mbit/s la plus proche).

6. Responsabilités du client

6.1 Le client s'engage à fournir à Cisco toutes les données techniques et autres informations pouvant être exigées de manière raisonnable par Cisco de temps à autre afin de permettre à ce dernier d'assurer la prestation du service au client, ce qui comprend un questionnaire de déploiement rempli et une matrice du site.

6.2 Le client reconnaît que les renseignements qu'il communique et qui lui sont communiqués transiteront par les systèmes de Cisco et s'engage donc à se conformer à la législation en vigueur encadrant l'utilisation qu'il fait d'Internet.

6.3 Le client est tenu de créer et d'utiliser des mots de passe complexes pour accéder à l'infrastructure Cisco dédiée et au portail d'assistance y afférent.

Ci-après figurent des directives courantes s'appliquant à la création d'un mot de passe complexe. Ces directives visent à rendre les mots de passe moins faciles à deviner :

- *Le mot de passe doit comporter des chiffres, des symboles et des lettres en majuscules et en minuscules.*
- *Le mot de passe doit être composé de 12 à 14 caractères environ.*
- *Évitez de créer un mot de passe basé sur la répétition, des mots figurant dans le dictionnaire, des séquences de lettres ou de chiffres, des noms d'utilisateurs, des noms de proches ou d'animaux domestiques, ou encore des renseignements biographiques (date, numéro d'identification, noms d'ancêtres, etc.).*

6.4 Dans le cadre de la prestation du service, Cisco peut devoir demander au client de réaliser certaines tâches ou certaines vérifications en lien avec le réseau de ce dernier. Le client devra, à ses propres frais, effectuer ces tâches et vérifications. Le client fournira à Cisco (ou à son représentant agréé) un accès gratuit et raisonnable à son matériel de réseautage. Il ne sera jamais demandé au client de fournir du matériel spécialisé ou du savoir-faire. Le client paiera à Cisco, conformément à la grille tarifaire Cisco alors en vigueur et majoré de toutes menues dépenses raisonnables, tout travail supplémentaire découlant d'une modification du service demandée par le client (et acceptée par Cisco) ou toute action ou omission du client, notamment en cas de communication d'informations erronées à Cisco. Cisco s'engage à obtenir l'approbation du client avant d'engager ces coûts, s'il sait que ces dépenses seront engagées suite à une telle action ou omission de la part du client.

6.5 Le client est responsable d'obtenir toutes les autorisations requises par des tiers pour que Cisco puisse fournir le service. Cisco ne sera pas en défaut face à ses engagements s'il lui est impossible de fournir le service parce qu'une autorisation n'a pas été obtenue ou parce qu'un tiers empêche d'une quelconque manière Cisco de fournir ledit service.

6.6 Le client s'engage à ne pas revendre le service ni à créer ou proposer des œuvres dérivées du service, que ce soit directement ou par l'entremise d'un tiers.

6.7 Le client assume l'entière responsabilité en ce qui concerne le contrôle et l'utilisation des données figurant dans les rapports fournis par Cisco en vertu des présentes. Le client reconnaît la possibilité de problèmes de confidentialité ou autres en lien avec la collecte et l'utilisation de ces données.

6.8 Le client assume l'entière responsabilité de sauvegarder et/ou de protéger d'une autre manière les données contre toute perte, tout endommagement ou toute destruction. Le client reconnaît qu'il lui a été conseillé de sauvegarder et/ou de protéger d'une autre manière les données contre toute perte, tout endommagement ou toute destruction.

6.9 Le client doit se conformer aux lois et réglementations encadrant l'utilisation, l'exportation, la réexportation et le transfert de technologies Cisco et doit obtenir les autorisations, permis et licences requis aux États-Unis.

6.10 En cas de non-respect de la présente Section, le client sera reconnu coupable de violation substantielle.

7. Confidentialité des données

7.1 Sous réserve de la Déclaration de confidentialité de Cisco publiée à l'adresse URL http://www.cisco.com/web/siteassets/legal/privacy_full.html ou à une autre adresse du site, celle-ci pouvant être modifiée en tant que de besoin par Cisco, le client consent par la présente et accorde à Cisco une licence lui permettant de recueillir et d'utiliser les données du client, comme cela est décrit dans la Documentation, cette dernière pouvant être modifiée en tant que de besoin par Cisco (les « Données »). Dans la mesure où les rapports ou statistiques sont générés à partir des Données, ils seront divulgués à des tiers uniquement sous forme globale et anonymisée. Aucun renseignement permettant d'identifier un utilisateur final ne sera inclus dans les Données, en ce compris notamment les noms d'utilisateurs, les numéros de téléphone, les noms de fichiers non brouillés, les adresses électroniques, les adresses de voirie et le contenu des fichiers.

8. Licences et propriété

8.1 Sous réserve du respect par le client des dispositions de la présente description de service, Cisco concède au client une licence mondiale, non exclusive et incessible lui permettant d'utiliser, à des fins commerciales internes uniquement et pendant toute la durée spécifiée sur le bon de commande applicable : (i) le service; (ii) les autres éléments livrables indiqués dans un EDT applicable, s'il y a lieu; et (iii) les Outils de collecte de données, le cas échéant (désignés collectivement et individuellement par l'expression ***« Éléments sous licence »***). Ces octrois de licences n'incluent aucun droit de concession en sous-licence; étant entendu que le client peut autoriser ses fournisseurs, sous-traitants et autres tiers connexes à utiliser les Éléments sous licence uniquement au nom et pour le compte du client, sous réserve que ce dernier veille à ce que toute utilisation de la sorte soit sujette à des restrictions de licence et à des obligations de confidentialité au minimum autant protectrices des droits de Cisco que celles dont sont pourvus les Éléments sous licence et qui sont spécifiées dans la présente description de service.

8.2 Sauf mention contraire explicite dans la présente description de service, le client s'interdit (et s'interdit de permettre à un tiers) d'apporter des corrections d'erreurs ou de créer des œuvres dérivées de, ou de modifier, décompiler, déchiffrer, désosser, désassembler ou autrement transcrire en langage humain intelligible tout ou partie de tout Élément livrable, Outil de collecte de données ou service. Il s'interdit également de transférer, concéder en sous-licence, louer, céder à crédit-bail, distribuer ou vendre le Service, les Éléments livrables ou les Outils de collecte de données. Le client reconnaît qu'il ne reçoit aucune licence implicite en vertu de la présente description de service, et tous les droits non octroyés expressément aux présentes sont réservés à Cisco.

8.3 Chaque partie conservera la propriété exclusive de l'ensemble de sa Technologie préexistante.

8.4 Sauf disposition contraire expressément stipulée dans la présente description de service, Cisco est et restera propriétaire de tout droit, titre et participation inhérents au Matériel, au Service, aux Éléments livrables, aux Outils de collecte de données, aux Rapports, aux schémas, aux textes, au savoir-faire, aux démonstrations de faisabilité d'un produit, aux illustrations, aux logiciels, algorithmes, méthodes, processus, codes identificateurs ou autres technologies fournies ou développées par Cisco (ou par un tiers agissant pour le compte de Cisco), conformément à la présente description de service, y compris les modifications, enrichissements, améliorations ou œuvres dérivées de tout ce qui précède, indépendamment de qui est le premier à les concevoir ou à les mettre en pratique, et de toute la Propriété intellectuelle inhérente à tout ce qui précède (collectivement, la « ***Propriété intellectuelle de Cisco*** »).

8.5 Dans les relations entre le client et Cisco, le client conserve en tout temps tout droit, titre et participation sur sa Technologie préexistante et toute la Propriété intellectuelle qui est développée par le client ou par un tiers pour le compte de celui-ci, autre que la Propriété intellectuelle de Cisco. Les produits fournis au client par tout tiers resteront en tout temps la propriété du tiers en question, et seront soumis aux conditions de toute licence tierce applicable.

8.6 Par les présentes, le client concède à Cisco un droit et une licence perpétuels, irrévocables, exempts de redevances et internationaux envers toute la Propriété intellectuelle inhérente aux rétroactions du client (comme définies ci-dessous) afin d'utiliser et d'incorporer les rétroactions du client dans tout service, produit, élément livrable, Outil de collecte de données, Rapport ou Technologie préexistante de Cisco, et afin d'utiliser, concevoir, faire concevoir, proposer à la vente, vendre, copier, distribuer et créer des œuvres dérivées desdites rétroactions du client à toutes fins. En outre, le client reconnaît et accepte qu'il ne lui sera octroyé aucun droit envers les services, les produits, les éléments livrables, les Outils de collecte de données, les Rapports ou la Technologie préexistante de Cisco suite à l'utilisation par ce dernier de toute rétroaction du client. Aux fins de la présente description de service, les « rétroactions du client » correspondent à toutes les communications orales ou écrites au sujet des améliorations ou des changements relatifs à tout service, produit, élément livrable, Outil de collecte de données, Rapport ou Technologie préexistante de Cisco que le client fournit à Cisco.

9. Politique d'utilisation acceptable

9.1 Il incombe au client de veiller à ce que tous les utilisateurs du service connaissent la présente politique. Il doit également veiller à ce que ces réglementations soient respectées à chaque instant, et s'engage à tenir Cisco indemne et à couvert de toute responsabilité (civile ou pénale) en cas de violation par lesdits utilisateurs auxquels le client permet d'utiliser le service.

9.2 Les utilisateurs ne doivent en aucune circonstance commettre, tenter de commettre, faciliter ou encourager toute action susceptible de menacer le service, ce qui comprend notamment les activités suivantes :

- utiliser le service à des fins illégales, attentatoires, contrevenantes, diffamatoires ou frauduleuses;
- transmettre de manière intentionnelle tout virus, ver, cheval de Troie, pièce jointe ou code malveillant avec le service;
- interférer avec l'utilisation que font d'autres utilisateurs autorisés du service;
- modifier, falsifier ou contourner tout aspect du service;
- fomenter le plantage d'un hôte ou du réseau du service;
- perpétrer des attaques entraînant un refus de service ou des attaques dites d'inondation;
- revendre, transférer, louer, céder à crédit-bail, exploiter en temps partagé ou marquer le service ou fournir le service autrement à toute partie non autorisée par nos soins à recevoir le service en vertu d'un contrat;
- tester ou désosser le service afin de déceler les limitations, les vulnérabilités ou de contourner les capacités de filtrage;
- fournir des informations privées concernant le service, incluant notamment des captures d'écran, de la documentation sur les produits, des démonstrations, des descriptions de services, des annonces ou des feuilles de route de fonctionnalités à des tiers non autorisés;
- tenter de contourner l'authentification d'un utilisateur ou la sécurité d'un hôte ou du réseau du service;
- créer, transmettre, stocker ou publier tout type de virus, de programme de corruption ou de données corrompues;
- toute autre action pouvant nuire au service.

9.3 Cisco se réserve le droit de suspendre ou de résilier le service, ainsi que de prendre toute action défensive de la sorte qu'il juge nécessaire, à sa seule discrétion, en cas d'attaque perpétrée à l'encontre du service ou du réseau. En outre, Cisco a la possibilité d'engager des poursuites au civil et/ou au pénal selon le cas contre les auteurs d'une telle action interdite.

10. Contrats de niveau de service

Disponibilité du service

10.1 Cisco garantit que son réseau traitera et honorera les requêtes Web du client à hauteur d'au moins 99,999 % des heures totales au cours de chaque mois d'utilisation du service par le client (la « Disponibilité »). La Disponibilité sera déterminée de manière globale sur tous les sites du client. Cisco fournit des adresses proxy à la fois primaires et secondaires pour chaque site depuis lequel le trafic Web peut être acheminé. En conséquence, une indisponibilité survient uniquement lorsque du contenu Web envoyé d'un site vers les deux adresses proxy n'est pas reçu par ou transmis aux utilisateurs finaux sur le site concerné du client.

10.2 Si Cisco ne respecte pas la garantie de Disponibilité, Cisco s'engage à offrir des crédits de service sur les cotisations mensuelles acquittées par le client selon le schéma suivant :

Disponibilité mensuelle du service	% de remboursement des frais de service mensuels
99,999 à 99,5 %	10
99,49 à 99,0 %	20
98,99 à 98,5 %	30
98,49 à 98,0 %	40
97,99 à 97,5 %	50
97,49 à 97,0 %	60
96,99 à 96,5 %	70
96,49 à 96,0 %	80
95,99 à 95,5 %	90
Moins de 95,5 %	100

Latence de filtrage Web

10.3 La Latence de filtrage Web fait référence au temps de chargement supplémentaire des pages Web occasionné par le service. La Latence de filtrage Web est évaluée par référence à la moyenne de temps écoulé entre :

- une demande de page Web envoyée vers le centre de données de Cisco où sont localisées les tours d'analyse; et
- la réception des données de cette page Web par l'auteur de la demande.

10.4 La Latence de filtrage Web doit être évaluée exclusivement par référence au temps qui a été nécessaire pour télécharger une ressource discrète depuis une sélection de sites Web populaires. Afin de lever tout doute, le SLA pour la Latence de filtrage Web ne s'applique pas au service AnyConnect.

10.5 Pour calculer la Latence de filtrage Web moyenne, Cisco évalue la durée moyenne écoulée pour télécharger une ressource discrète depuis chacun des sites Web susmentionnés (le « Délai de réponse filtrée ») et compare cette durée à la durée moyenne écoulée pour des demandes de page Web identiques effectuées par le même auteur au cours de la même période de test et qui ne sont pas traitées par le biais du service (le « Délai de réponse non filtrée »). Chaque échantillon de la sorte de Délai de réponse filtrée et de Délai de réponse non filtrée est désigné par l'expression « Paire échantillonnée ». Ces échantillons seront prélevés toutes les 60 minutes.

10.6 Cisco garantit que le Délai de réponse filtrée (dont la moyenne a été calculée à partir de toutes les Paires échantillonnées) au cours d'un mois civil donné ne sera pas supérieur à :

- une seconde de plus que le Délai de réponse non filtrée; ou
- trois fois le Délai de réponse filtrée (la plus grande des deux valeurs étant retenue).

10.7 Si Cisco ne respecte pas la garantie susmentionnée, il s'engage à offrir des crédits de service d'un montant égal à 10 % des frais de service mensuels acquittés par le client pour le service fourni au cours de ce mois.

Taux de filtrage Web des faux positifs

10.8 Le niveau de service « Taux de filtrage Web des faux positifs » mesure le pourcentage d'adresses URL et de domaines ayant été bloqués par le service mais qui, sur la base des stratégies de catégorisation choisies par le client, n'auraient pas dû être bloquées (les « Blocages erronés »). Afin de lever tout doute, si une adresse URL figure dans la catégorie « Éléments non classés », elle devrait être bloquée si le client a choisi de bloquer toutes les URL non classées.

Taux de filtrage Web des faux positifs =

100

x le nombre total de Blocages erronés au cours d'un mois civil donné sur tous les sites

÷ le nombre total d'URL analysées par le service de Filtrage Web sur tous les sites au cours du même mois civil

où les Blocages erronés sont déterminés par Cisco de manière raisonnable.

10.9 Si le Taux de filtrage Web des faux positifs est supérieur ou égal à 0,0004 %, Cisco s'engage à offrir des crédits de service d'un montant égal à 10 % des frais de service mensuels acquittés par le client pour le service de Filtrage Web. Cisco s'engage à répondre dans les sept jours qui suivent la notification d'un client estimant qu'il a été confronté à un Blocage erroné, et doit motiver sa décision selon laquelle il juge ou non qu'il y a effectivement eu un Blocage erroné.

Taux de filtrage Web des faux négatifs

10.10 Le niveau de service « Taux de filtrage Web des faux négatifs » mesure le pourcentage d'adresses URL et de domaines n'ayant pas été bloqués par le service mais qui, sur la base des stratégies de catégorisation choisies par le client, auraient dû être bloquées (les « Blocages manqués »). Afin de lever tout doute, si une adresse URL figure dans la catégorie « Éléments non classés », elle devrait uniquement être bloquée si le client a choisi de bloquer toutes les URL non classées.

Taux de filtrage Web des faux négatifs =

100

x le nombre total de Blocages manqués au cours d'un mois civil donné sur tous les sites

÷ le nombre total d'URL analysées par le service de Filtrage Web sur tous les sites au cours du même mois civil

où les Blocages manqués sont déterminés par Cisco de manière raisonnable.

10.11 Si le Taux de filtrage Web des faux négatifs est supérieur ou égal à 0,0004 %, Cisco s'engage à offrir des crédits de service d'un montant égal à 10 % des frais de service mensuels acquittés par le client pour le service de Filtrage Web. Cisco s'engage à répondre dans les sept jours qui suivent la notification d'un client estimant qu'il a été confronté à un Blocage manqué, et doit motiver sa décision selon laquelle il juge ou non qu'il y a effectivement eu un Blocage manqué.

Généralités

10.12 S'il estime que Cisco n'a pas honoré l'une des garanties susmentionnées, le client doit contacter Cisco par écrit dans les 15 jours ouvrables à compter de la fin du mois au cours duquel le client estime que la garantie en question n'a pas été respectée.

10.13 Cisco mettra en œuvre, gérera et utilisera des processus, procédures et outils appropriés pour surveiller, calculer et élaborer des rapports sur les performances du service par rapport aux niveaux de service exposés dans la présente Section. En cas de différend découlant de la présente Section, Cisco procédera à une détermination de bonne foi en se basant sur ses journaux système, rapports de surveillance et archives de configuration.

10.14 Pour pouvoir se prévaloir de l'un des recours mentionnés dans la présente Section, le client doit s'être acquitté de tous les frais et avoir honoré toutes ses obligations au titre de la présente description de service.

10.15 Les recours exposés dans la présente Section ne s'appliquent pas aux sujets découlant de l'une des exceptions suivantes :

- Mises à niveau matérielles ou logicielles demandées par le client, déplacements, mises à niveau des installations, etc.
- Une période de maintenance prévue, annoncée au moins 24 heures à l'avance.
- Matériel, logiciels ou autre équipement de centre de données ou services échappant au contrôle de Cisco ou au mandat du service.
- Modifications de la configuration matérielle ou logicielle apportées par le client sans avoir obtenu au préalable l'accord écrit de Cisco.

- Attaques entraînant un refus de service sur l'infrastructure de sécurité des courriels installée ou les services connexes.
- Événements échappant au contrôle raisonnable de Cisco, y compris notamment les catastrophes naturelles, un séisme, des conflits sociaux, des pénuries de fournitures frappant l'ensemble du secteur, des émeutes, une guerre, des actes de terrorisme, un incendie, une épidémie ou encore des retards des transporteurs publics.

10.16 Les recours présentés dans cette Section constituent le seul et unique recours du client, que ce soit en vertu du contrat, d'un préjudice ou autrement en lien avec les événements en question. Une seule et unique catégorie de crédit peut faire l'objet d'une réclamation en lien avec tout problème.

10.17 Afin de lever toute ambiguïté, même si Cisco emploiera des efforts raisonnables pour détecter les logiciels malveillants, il ne garantit pas que le Service (outils PALM et CTA compris) sera à même de détecter ou de bloquer toute menace malveillante spécifique.

11. Assistance et procédure de signalisation à suivre

11.1 Cisco offre un service d'assistance disponible 24 heures sur 24, 7 jours sur 7. Si les ingénieurs sont incapables de résoudre le problème, ce problème sera envoyé au niveau interne supérieur.

11.2 Le client est tenu d'entreprendre des efforts raisonnables pour résoudre en interne toute question d'assistance avant de contacter Cisco. Il incombe au client de signaler par écrit (en langue anglaise) et sans délai toute erreur et de fournir des informations suffisantes à Cisco afin de permettre à Cisco d'analyser comme il se doit les circonstances indiquant un défaut ou une erreur de Logiciel. Le client est tenu de fournir les informations techniques requises par les ingénieurs systèmes ou analystes en sécurité de Cisco, incluant notamment les adresses IP afférentes à la solution existante du client.

11.3 Une demande d'assistance du CAT peut être ouverte de plusieurs manières : 1) via un outil de demande d'assistance en ligne, 2) par courriel ou 3) par téléphone.

a) L'outil de demande d'assistance en ligne, disponible sur « Cisco.com », permet au client de saisir des informations sur le problème.

b) Le client a la possibilité d'envoyer un courriel à tac@cisco.com en incluant une description du problème et en précisant ses coordonnées.

c) Le client peut également utiliser le téléphone. Lorsque le client appelle le numéro (+1) 800, l'appel est transféré vers un agent du Réseau d'interaction avec la clientèle (RIC) qui consigne les renseignements initiaux concernant la Demande d'assistance du client et transmet l'appel à l'ingénieur adéquat. L'équipe du RIC reçoit tous les appels téléphoniques et tous les courriels de demande d'assistance. L'agent du RIC exécute les tâches suivantes pour chaque demande d'assistance : a) ouverture de dossier, b) vérification des droits du client, c) évaluation et établissement de la priorité (selon la gravité définie par le client sur une échelle de 1 à 4) et d) transmission de la demande à l'équipe appropriée du CAT.

Numéros du Centre d'assistance

	Téléphone	Courriel	Web
EMOA	+44 (0) 20 7034 9400	tac@cisco.com	http://www.cisco.com/cisco/web/support/index.html
US	+1 800 553 2447	tac@cisco.com	http://www.cisco.com/cisco/web/support/index.html
Asie-Pacifique	+1 877 472 2680	supporttac@scansafecisco.com	http://www.cisco.com/cisco/web/support/index.html

Définitions en matière de gravité

11.4 Le Centre d'assistance Cisco doit attribuer un niveau de gravité à chaque problème signalé par le client.

- Gravité 1 : un réseau existant est arrêté ou il existe un impact critique sur les activités de l'entreprise du client. Cisco et le client mobilisent des ressources à plein temps pour trouver une solution.
- Gravité 2 : le fonctionnement d'un réseau existant est fortement dégradé, ou des aspects importants du fonctionnement de l'entreprise du client sont impactés négativement par des performances réseau inacceptables. Cisco et le client mobilisent des ressources à plein temps au cours des Heures ouvrables standard pour résoudre le problème.
- Gravité 3 : les performances opérationnelles du réseau sont affectées, mais les autres fonctions sont intactes. Cisco et le client sont disposés à mobiliser des ressources raisonnables au cours des Heures ouvrables standard afin de restaurer le service à des niveaux satisfaisants.

- Gravité 4 : des informations ou une assistance sont requises sur les capacités, l'installation ou la configuration du produit. Il y a clairement peu ou pas d'impact sur les activités de l'entreprise du client. Cisco et le client sont disposés à mobiliser des ressources au cours des Heures ouvrables standard pour fournir des informations ou une assistance.

11.5 Aux fins du présent document :

a) L'expression « jours ouvrables » désigne les jours de travail ouvrés généralement acceptés pour le travail hebdomadaire au sein de la région concernée où le service sera fourni, hormis les jours fériés.

b) L'expression « heure locale » signifie l'heure d'Europe centrale si le service est fourni dans la zone Europe, Moyen Orient et Afrique, l'heure normale de l'Est de l'Australie si le service est fourni en Australie, l'heure normale du Japon si le service est fourni au Japon et l'heure normale du Pacifique si le service est fourni dans une autre région.

c) L'expression « heures ouvrables standard » désigne la plage horaire allant de 8 h à 17 h (heure locale du pays) les jours ouvrables.

Processus de signalisation

11.6 Les clients feront appel aux contacts inscrits ci-dessous lorsqu'un problème doit faire l'objet d'une signalisation.

11.7 * Les durées de signalisation du niveau de gravité 1 sont mesurées en heures standard, 24 heures sur 24, 7 jours sur 7. Les durées de signalisation des niveaux de gravité 2, 3 et 4 correspondent aux heures ouvrables standard.

Temps écoulé	Gravité 1	Gravité 2	Gravité 3	Gravité 4
1 heure	Technicien supérieur en entretien et en réparation pour la clientèle			
4 heures	Responsable des niveaux de service	Technicien supérieur en entretien et en réparation pour la clientèle		
24 heures	Responsable de l'assistance technique	Responsable des niveaux de service		
48 heures	Directeur de l'assistance technique	Responsable de l'assistance technique		
72 heures		Directeur de l'assistance technique	Responsable des niveaux de service	
96 heures			Responsable de l'assistance technique	Responsable des niveaux de service

GLOSSAIRE

Cisco désigne Cisco Systems, Inc. et comprend dans les cas appropriés les entreprises de son groupe (Cisco International Limited, Cisco Systems International B.V., Cisco Systems G.K., Cisco Systems Australia Pty. Ltd., Cisco Systems Canada Co. et Cisco Systems (Italy) s.r.l.)

Documentation signifie les manuels de l'utilisateur, les supports de formation, les descriptions et spécifications de services, les manuels techniques, les contrats de licence, les documents connexes et toute autre information liée aux services proposés par Cisco, qu'ils soient distribués sur papier, par voie électronique, sur CD-ROM ou via vidéo.

Logiciel signifie les programmes logiciels fournis au client par Cisco, y compris toutes copies, mises à jour, mises à niveau, modifications, améliorations et œuvres dérivées.

Matériel signifie les équipements, appareils ou composants tangibles de Cisco mis à la disposition des clients.

Mise à jour signifie les versions de Cisco contenant la même configuration ou le même ensemble de fonctionnalités tels qu'acquis initialement, à moins que le client n'ait mis à niveau le service applicable vers une configuration ou un ensemble de fonctionnalités différents, ainsi que les frais de licence applicables acquittés par le client. Les mises à jour n'incluent pas les versions logicielles faisant l'objet d'un octroi de licence et d'une tarification distincts et qui renferment une configuration ou un ensemble de fonctionnalités amélioré.

Outils de collecte de données signifie le Matériel et/ou Logiciels permettant à Cisco de résoudre des problèmes, d'analyser des données et de créer des rapports.

Propriété intellectuelle signifie tous les éléments tangibles ou non tangibles suivants : (i) droits liés à des œuvres d'auteur à l'échelle mondiale, y compris mais sans s'y limiter, copyrights, droits d'auteur, droits voisins, droits moraux, droits de masquage et toutes les œuvres dérivées; (ii) marques de commerce, dénominations commerciales et droits similaires; (iii) droits relatifs aux secrets commerciaux; (iv) brevets, conceptions, algorithmes et autres droits de propriété industrielle; (v) tous les autres droits de propriété intellectuelle et industrielle (de toute nature à travers le monde et sous quelque forme que ce soit), qu'ils découlent ou non des effets de la loi, d'un contrat, d'une licence ou autre; et (vi) inscriptions, demandes initiales, renouvellements, prolongements, continuations, divisions ou rééditions de celles-ci ou ci-après en vigueur (y compris tous les droits concernant tout ce qui précède).

Rapports signifie les rapports, recommandations, diagrammes de configuration de réseau et autres prestations connexes fournies par IronPort au client.

Service signifie le service de sécurité de l'informatique en nuage sur le Web décrit dans ce document.

Technologie préexistante, appliquée à l'une ou l'autre partie, désigne l'ensemble de la Propriété intellectuelle préexistante de cette dernière, ses informations confidentielles et documents, y compris notamment les idées privées, schémas, textes, savoir-faire, démonstrations de faisabilité d'un produit, illustrations, logiciels, algorithmes, méthodes, processus, codes identificateurs ou autres technologies détenues par une partie avant que ne commencent les services décrits aux présentes, ou qui sont autrement développées par ou pour cette partie en dehors du champ d'application de la présente description de service.

Version signifie la version logicielle incrémentielle qui fournit des correctifs ainsi que d'éventuelles fonctionnalités supplémentaires.