



## Services de sécurité gérés – Entreprise

### DESCRIPTION DU SERVICE

Le groupe Services de sécurité gérés – Entreprise d'*Allstream* a pour mandat de mettre en place et d'effectuer la maintenance d'une solution de sécurité qui protège les ressources réseau d'importance critique du *client*. Dans le cadre de ces activités, *Allstream* fournit un service constant, fiable et de qualité élevée, qui met efficacement à profit l'expertise de représentants en service à la clientèle et d'ingénieurs en sécurité agréés.

### CARACTÉRISTIQUES

**Soutien.** *Allstream* effectue la surveillance des systèmes et fournit le soutien technique 24 heures sur 24, 7 jours sur 7. La société garantit à cet égard un temps de réponse de 30 minutes ou moins. Cela signifie que dans les 30 minutes suivant un appel au centre d'assistance d'*Allstream*, le représentant désigné du *client* recevra un appel d'un spécialiste en sécurité certifié d'*Allstream*.

**Surveillance.** *Allstream* surveille le fonctionnement de la solution de sécurité afin de s'assurer que tous les dispositifs de sécurité sont en état de marche et qu'ils fonctionnent normalement, que tous les logiciels de sécurité (les « *logiciels* ») et tout le matériel de sécurité (le « *matériel* ») (collectivement désignés sous l'appellation « *système de sécurité* ») fonctionnent; et pour confirmer l'état de la connexion Internet. Si *Allstream* est informée d'un problème lié au *système de sécurité*, un technicien des Services de sécurité gérés est alerté, fait enquête et résout le problème.

#### Rapports mensuels.

*Allstream* fournit au *client* :

- i) un rapport mensuel reflétant l'infrastructure de réseau du *client* et l'ensemble des règles en matière de filtrage des adresses URL (si le *client* est abonné au service de filtrage des adresses URL géré);
- ii) un rapport mensuel reflétant le trafic d'arrivée accepté et refusé, le trafic de départ accepté et refusé, la vérification liée au pare-feu, les rapports d'utilisation liés à l'unité CPU du pare-feu, les rapports liés aux fiches de dérangement et un rapport d'utilisation du RPV (si le client est abonné au service de RPV géré d'*Allstream*);
- iii) un rapport trimestriel sur la détection de faiblesses par balayage des dispositifs de sécurité gérés en vertu des services de sécurité gérés complets d'*Allstream*. \*\*

Le *client* peut disposer d'un accès sans écriture pour consulter les règles chargées dans le système de gestion du pare-feu. De la même manière, le *client* abonné aux services de filtrage antivirus gérés d'*Allstream* peut disposer d'un accès sans écriture au serveur de filtrage de la passerelle afin de passer en revue l'activité antivirale.

\*\* L'interprétation des rapports sur la détection de faiblesses par balayage est offerte en fonction des tarifs applicables aux services professionnels d'*Allstream*.

### DESCRIPTION DE L'INFRASTRUCTURE DE RÉSEAU

Dans le cadre de la mise en place des services de sécurité gérés, *Allstream* travaille de concert avec le représentant désigné du *client* à préparer une description de l'infrastructure de réseau de ce dernier. L'information requise pour la description du réseau aux fins du service de pare-feu géré comprend : les adresses IP de tout dispositif situé à l'intérieur de la zone d'accueil (DMZ) mais hors de la zone du service de pare-feu géré, un diagramme de réseau indiquant où le pare-feu géré est situé, et le domaine des adresses IP tel que fourni par le FSI ou tel qu'enregistré auprès de l'ICCAN. Les renseignements devant être fournis pour le service de filtrage des adresses URL géré sont les suivants : identification des sous-réseaux configurés au sein du réseau, de même qu'un diagramme de réseau indiquant où est situé le serveur de filtrage des adresses URL géré. Enfin, le *client* doit fournir un diagramme de réseau indiquant où se trouve le serveur de filtrage antivirus géré si le *client* se prévaut du service de filtrage antivirus géré.

## **GESTION ET MAINTENANCE DU SYSTÈME DE SÉCURITÉ**

En plus de la gestion et de la maintenance du *système de sécurité* du *client* selon les dispositions de la Politique relative à l'utilisation d'Internet d'*Allstream*, la société protège le *client* des nouveaux risques en fonction des modalités suivantes.

- ❑ Mises à jour et corrections provisoires. *Allstream* s'assure, d'une manière continue, que le *système de sécurité* du *client* reste à jour en installant les mises à jour et les corrections provisoires requises. *Allstream* classe ces modifications en quatre catégories.
- ❑ Modification d'importance critique. – Il existe un danger réel et imminent d'intrusion pouvant causer de sérieux dommages si les *logiciels* ne sont pas mis à jour. La mise à jour sera installée sur les dispositifs appropriés du *système de sécurité* dans les 24 heures après réception de l'avis de mise à jour par le fabricant de logiciel. Si le *client* ne s'est pas abonné au service de disponibilité élevée offert par *Allstream* pour le dispositif en question, il est possible qu'une interruption du service survienne durant la mise à jour des *logiciels*. Une interruption de service découlant d'une telle mise à jour sera exclue de tout calcul de disponibilité du service aux fins de la garantie de disponibilité. *Allstream* communiquera avec le représentant désigné dans les 12 heures suivant la réception de l'avis de mise à jour du fabricant. Les mises à jour seront effectuées après avoir été approuvées par le vice-président, Service à la clientèle d'*Allstream*.
- ❑ Modification importante. – Sans cette modification, le *client* s'expose à une intrusion qui peut causer des dommages sérieux. La mise à jour sera installée sur le dispositif approprié du *système de sécurité* durant la prochaine période de maintenance permettant ce genre de travaux. *Allstream* fournira un préavis d'au moins deux semaines avant de procéder à la mise à jour.
- ❑ Modification non importante. – Sans cette modification, le *client* s'expose à des intrusions qui peuvent causer certains désagréments mais aucun dommage sérieux. La mise à jour sera effectuée sur les dispositifs appropriés du *système de sécurité* dans le cadre d'une mise à jour générale visant à préserver la conformité de l'image logicielle du *système de sécurité* géré. *Allstream* fournira un préavis d'au moins deux semaines avant de procéder à la mise à jour, qui sera effectuée durant une période de maintenance standard.
- ❑ Modification non pertinente. – La mise à niveau ou la correction ne concerne pas l'environnement de réseau du *client*. Toutefois, *Allstream* peut, à sa seule discrétion, décider d'installer la mise à jour sur les dispositifs appropriés du *système de sécurité* afin de préserver la conformité de l'image logicielle. *Allstream* fournira un préavis d'au moins deux semaines avant de procéder à la mise à jour, qui sera effectuée durant une période de maintenance standard.
- ❑ Modifications aux règles. *Allstream* effectuera les modifications aux règles demandées par le *client* ou suggérées par les ingénieurs en sécurité d'*Allstream*. Dans le cadre des services de sécurité gérés, *Allstream* admet 20 modifications par mois et par dispositif du *système de sécurité* (ce qui comprend les ajouts et les suppressions).

Le *client* qui accepte de réduire le nombre de modifications mensuelles aux règles peut bénéficier de tarifs plus bas, en fonction des seuils donnés ci-dessous.

<b>Licence Check Point pour micro-entreprises (SOHO)</b>	Maximum de 5 modifications mensuelles.
<b>Licence Check Point pour grandes entreprises (Enterprise)</b>	Maximum de 20 modifications mensuelles au cours des 3 premiers mois de la durée du <i>contrat</i> ; puis, de 5 modifications mensuelles par la suite.

Lorsque le *client* demande une modification en particulier, il lui revient de s'assurer que cette modification n'entraînera pas une vulnérabilité de son réseau. Les modifications aux règles seront effectuées en fonction d'un délai ne dépassant pas quatre heures par règle à compter du moment où la demande de la modification à la règle est présentée à *Allstream*. Un ingénieur en sécurité d'*Allstream* communiquera avec le représentant désigné du *client* dans les 30 minutes de la réception de la demande de modification aux règles par *Allstream*. Lorsque le *client* demande une modification aux règles, il lui revient de s'assurer que cette modification n'entraînera pas une vulnérabilité de son réseau. Toute requête d'installation d'une nouvelle page Web sera traitée comme une demande de modification aux règles.

- ❑ Abonnements aux logiciels. *Allstream* effectue le suivi des abonnements pour ce qui est des *logiciels* auxquels le *client* est abonné. *Allstream* en effectue également le renouvellement.
- ❑ Sauvegardes de l'information du client. *Allstream* conserve les journaux des sauvegardes, les politiques et les configurations afin de s'assurer que la configuration la plus récente demeure toujours disponible. *Allstream* conserve cinq versions antérieures des politiques et des configurations. Ces dernières feront l'objet d'une sauvegarde dans les 24 heures précédant une modification des politiques ou des configurations. Les journaux seront fournis par courriel ou livrés sur CD-ROM par messenger dans les deux jours ouvrables suivant la demande. Le *client* peut soumettre un maximum de 12 demandes similaires par année.

- ❑ Journaux archivés. Les journaux archivés sont conservés pendant un an. L'archivage s'effectue une fois toutes les 24 heures. Voici la liste des journaux qui font l'objet d'un archivage.
  - Service de pare-feu géré / service de RPV : journaux système et journaux d'activités de l'utilisateur.
  - Service de filtrage antivirus géré : journaux système et journaux de détection des virus.
  - Service de filtrage des adresses URL géré : journaux système et journaux de filtrage des adresses URL.
- ❑ Panne de matériel. Si une panne de *matériel* installé au Canada survient et qu'*Allstream* se trouve dans l'impossibilité de résoudre le problème à distance, *Allstream* s'assurera d'expédier le *matériel* de remplacement par messenger le prochain jour ouvrable pour livraison le jour ouvrable suivant.
- ❑ Gestion des clés. À tous les trimestres, *Allstream* renouvelle la clé de chiffrement sur les passerelles RPV pour les RPV inter-emplacements lorsque les deux extrémités du tunnel RPV sont gérées par *Allstream*. À tous les trimestres, *Allstream* renouvelle la clé de chiffrement entre la passerelle RPV et le serveur RADIUS, qui sont tous deux gérés par *Allstream*.
- ❑ Tunnels RPV entre les passerelles RPV gérées ou non gérées par Allstream. *Allstream* fournit à la personne qui gère la passerelle RPV et qui établit un tunnel RPV vers une passerelle RPV gérée par *Allstream*, les paramètres IPSec qui permettront une connexion adéquate à la passerelle RPV gérée par *Allstream*. *Allstream* veille à ce que les paramètres IPSec correspondants soient configurés sur la passerelle RPV gérée par *Allstream*. *Allstream* veille également à ce que la configuration fournie respecte les normes IPSec approuvée par le groupe Internet Engineering Task Force. *Allstream* ne peut garantir le succès d'une connexion RPV si la passerelle RPV à laquelle *Allstream* se raccorde ne respecte pas entièrement les normes IPSec.
- ❑ Soutien aux logiciels clients RPV. *Allstream* offre un soutien téléphonique 24 heures sur 24, 7 jours sur 7 à l'égard des *logiciels*. Un soutien de deuxième niveau est offert. Le soutien de deuxième niveau signifie que seuls les administrateurs du centre de dépannage du *client* peuvent communiquer avec le centre de dépannage d'*Allstream* pour obtenir du soutien. Les frais applicables aux services professionnels d'*Allstream* peuvent s'appliquer à l'intégration du serveur RADIUS du *client* au service d'accès à distance par RVP Internet offert dans le cadre des services de sécurité gérés d'*Allstream*.
- ❑ Distribution des logiciels clients RPV. Le *client* est responsable de la distribution et de l'installation des *logiciels*. *Allstream* assure le soutien de deuxième niveau. Des recommandations sur les stratégies de distribution des *logiciels* peuvent être comprises dans les services professionnels d'*Allstream* et celles-ci seront offertes en fonction des tarifs applicables aux services professionnels d'*Allstream*.
- ❑ Guide d'administration. *Allstream* fournit au *client* un exemplaire du *Guide de l'administrateur* des services de sécurité gérés. Ce guide comprend ce qui suit : un guide d'installation et d'utilisation des *logiciels* qui se rapportent aux services de sécurité gérés d'*Allstream* ; les lignes directrices sur les politiques de sécurité ; et un guide de soutien de premier niveau pour le dépannage des *logiciels*. Le *client* peut obtenir une politique de sécurité personnalisée, offerte en fonction des tarifs applicables aux services professionnels d'*Allstream*.