

Accès à distance et continuité d'activité

**Tim Clark, associé de
The Fact Point Group**

Juillet 2005

**300 Third Street, Suite 10
Los Altos, CA 94022
650-233-1748
tclark@factpoint.com**

Rapport de synthèse

Les récentes catastrophes naturelles, menaces de pandémies, grèves des transports, activités terroristes ou autres évènements ont poussé les entreprises à mettre en place des plans de reprise d'activité.

Les perturbations de l'activité normale d'une entreprise occasionnent plus que des désagréments ; elles sont souvent synonymes d'occasions manquées, de perte de revenus et nuisent à l'image de marque. L'objectif de toute entreprise est la continuité de son activité, c'est-à-dire le maintien de ses fonctions métier de base en toutes circonstances. Cet objectif devient toutefois de plus en plus difficile à atteindre car l'entreprise est la cible de menaces résultant de facteurs très divers, internes et externes, naturels et humains. Le délai d'intervention attendu suite à une perturbation de l'activité s'est lui aussi contracté : les employés, les partenaires, les clients et organismes de réglementation exigent une résolution immédiate.

La continuité d'activité couvre de nombreux secteurs d'une entreprise, physiques et numériques. La gestion de l'accès à l'information est l'un des aspects clés à prendre en compte pour préserver cette continuité : toutes les entités constituant une entreprise doivent pouvoir accéder à l'information rapidement et facilement en cas de sinistre ou de perturbation de l'activité. La dépendance à l'égard des ordinateurs et des réseaux d'entreprise impose que ces derniers fonctionnent sans interruption. Il faut également mettre en œuvre une solution d'accès à distance aux ressources du réseau rapide et simple.

L'accès à distance n'a pas pour seule finalité d'assurer la continuité de l'activité. Beaucoup d'organisations ont adopté des solutions d'accès à distance pour augmenter leur productivité et préserver leur sécurité en réponse au

développement du télétravail, à l'augmentation du nombre des utilisateurs nomades et des entreprises aux activités internationales. Ces facteurs rendent nécessaire une connectivité permanente à partir de n'importe quel lieu, n'importe quel réseau et n'importe quel dispositif. En cas de perturbation d'activité ou de sinistre, les besoins d'accès à distance propres aux scénarios quotidiens que nous venons d'évoquer deviennent ceux de tous les utilisateurs de réseaux.

La continuité d'activité et l'accès à distance vont de pair, les perturbations de l'activité éloignant les employés et les autres utilisateurs de leur bureau et du réseau local. Par exemple, pendant une grosse tempête en hiver, les conditions de circulation ou la fermeture des bureaux et des écoles peuvent contraindre des employés à rester chez eux. Dans les organisations qui ont mis en œuvre une solution d'accès à distance, les employés peuvent alors rester productifs et travailler depuis leur domicile comme s'ils étaient au bureau.

Continuité d'activité et accès distant : ce qu'un CIO doit savoir

- Une réponse bâclée à un sinistre peut avoir un impact négatif sur le chiffre d'affaires et l'image de l'entreprise.
- Les obligations réglementaires imposant l'audit des données sensibles restent applicables pendant un sinistre.
- L'accès distant sécurisé joue un rôle crucial dans les plans de continuité d'activité.
- Équiper le centre de données de secours d'un boîtier VPN SSL permet l'exécution des processus métier pendant un sinistre.
- Un VPN SSL à maintenance réduite limite la dépendance à l'égard du service informatique pour la reprise après sinistre.

La technologie des VPN SSL s'est imposée comme la solution de premier plan pour l'accès à distance. Ces réseaux privés virtuels qui utilisent des protocoles de sécurité SSL (Secure Socket Layer) sont bien adaptés à l'accès à distance sécurisé en cas d'urgence car ils permettent aux employés et aux partenaires de se connecter via Internet et en toute sécurité au réseau de l'entreprise pour accéder aux données et aux applications. Ce document détaille les meilleures pratiques pour planifier la continuité d'activité avec l'accès à distance et décrit le rôle des VPN SSL dans ce processus.

Facteurs déterminants pour planifier la continuité d'activité

Une entreprise doit prévoir les interruptions d'activité potentielles et s'y préparer. Il n'est pas possible de s'atteler au problème le jour où un sinistre survient. À ce stade, il est déjà trop tard. Quand l'activité est perturbée, l'incapacité à fonctionner normalement ou à fournir un accès aux ressources stratégiques peut affecter négativement le chiffre d'affaires, la réputation de la société ou de sa marque. C'est pourquoi l'élaboration de plans en prévision de catastrophes, autrefois anecdotique et dévolue aux cadres intermédiaires, incombe aujourd'hui aux hautes sphères de l'entreprise. Un plan de continuité d'activité efficace nécessite l'implication et l'adhésion des techniciens et des gestionnaires de l'entreprise.

Plusieurs facteurs sont déterminants pour la continuité d'activité :

- **Protection des sources de revenus :** une interruption d'activité peut entraîner une perte de revenus, de clients et d'opportunités commerciales. Elle touche virtuellement toutes les parties prenantes — investisseurs, clients, employés et partenaires.
- **Renforcement du positionnement face à la concurrence :** avec un plan de continuité d'activité efficace, vous pouvez vous positionner en tant que partenaire ou fournisseur fiable, en donnant à vos clients et partenaires l'assurance que vous continuerez à fonctionner, même pendant un sinistre.
- **Maintien de la productivité :** personne ne peut prévoir les détails d'une crise, mais parce que toutes les entreprises dépendent de l'information et du réseau, le maintien de l'accès, et donc de la productivité des employés, est crucial. Ces employés bien sûr, mais aussi les clients, les fournisseurs, les partenaires commerciaux et les autres tiers ont besoin d'un accès à distance aux ressources de l'entreprise en cas d'interruption de son activité.
- **Respect des réglementations :** un sinistre ne vous dispense pas de respecter des réglementations comme celles de la loi Sarbanes-Oxley, de l'HIPAA et de Bâle 2. L'entreprise doit donc garantir un accès sécurisé et auditable à certaines informations clés, même lorsque son activité est perturbée.

- **Réduction des risques et des menaces informatiques** : pendant une perturbation de son activité, l'entreprise est exposée aux hackers et autres menaces informatiques. Une solution d'accès à distance sécurisé protège votre propriété intellectuelle et vos ressources stratégiques. En autorisant l'accès aux seuls utilisateurs authentifiés et ressources autorisées, vous êtes assuré que ceux qui ont besoin de l'information l'obtiennent rapidement et que ceux qui ne disposent pas des droits idoines sont écartés.

Impératifs pour planifier la continuité d'activité

Si vous voulez atteindre les objectifs que nous venons de décrire, votre solution d'accès à distance doit respecter les impératifs suivants :

- **Autoriser l'accès** aux ressources et aux applications du réseau par les employés, les clients, les fournisseurs et les partenaires où qu'ils soient, à tout moment et via n'importe quel dispositif. Cela peut vouloir dire octroyer aux employés un accès ininterrompu à l'application de gestion de la relation client dont ils dépendent ou permettre aux utilisateurs externes de rester connectés via un extranet ou une application de la chaîne d'approvisionnement.
- **Préserver la sécurité et la confidentialité des données** en protégeant ces dernières des menaces internes et externes. Cela suppose un contrôle d'accès granulaire pour que les utilisateurs accèdent seulement aux données et applications appropriées. Il faut notamment définir une règle cohérente qui n'autorisera l'accès qu'aux utilisateurs disposant des informations d'identification et de connexion idoines pour les données et les applications spécifiées.
- **Simplifier la gestion de l'accès à distance** pour limiter le recours des utilisateurs au service d'assistance pour l'accès à distance et permettre au service informatique de se concentrer sur les problèmes directement liés au sinistre.
- **Autoriser la création en continu de pistes d'audit pour l'accès** aux informations sensibles et ce faisant se conformer aux diverses réglementations (Sarbanes-Oxley, HIPAA ou Gramm-Leach-Bliley). La directive de l'Union européenne sur la protection des données est très contraignante concernant la protection des données personnelles par les sociétés exerçant leurs activités en Europe, qu'elles y soient basées ou pas. Au début de cette année, le Japon a voté une loi pour la protection des informations personnelles qui impose des réglementations strictes aux entités publiques ou privées qui collectent, gèrent ou utilisent des informations personnelles.
- **Bloquer les connexions à distance** avec des systèmes non sécurisés qui pourraient infecter le réseau d'entreprise avec des virus ou d'autres logiciels malveillants.

- **Préserver la disponibilité des applications stratégiques** comme les applications de gestion de la relation client, de gestion d'entreprise et de messagerie électronique. Les technologies plus récentes comme le protocole VoIP (Voice over Internet protocol) et les conférences Web peuvent aussi jouer un rôle accru en cas de sinistre si les services téléphoniques sont indisponibles et qu'il est plus que jamais nécessaire de rester en contact avec les clients.
- **Prendre en charge une pointe de trafic réseau** résultant d'une situation d'urgence. De même que beaucoup de personnes contactent leurs amis ou leur famille pour prendre de leurs nouvelles quand elles les croient en danger, un sinistre peut inciter les clients, les partenaires et les fournisseurs à s'assurer que leur activité ne sera pas perturbée par un sinistre. Il faut donc prévoir une solution d'accès à distance évolutive qui pourra faire face à un pic de demande.

Entraves à la continuité d'activité

La continuité d'activité suppose d'anticiper les sinistres majeurs mais aussi des scénarios plus courants. Ne considérez pas que seuls des événements exceptionnels tels une inondation centennale ou une attaque terroriste nécessitent une intervention d'urgence. Vous devez aussi vous préparer à des situations plus ordinaires mais inattendues et perturbantes auxquelles des milliers d'entreprises sont confrontées chaque jour.

Divers événements peuvent entraver la continuité d'activité :

- **Risques naturels et catastrophes** : des perturbations bien moins sérieuses qu'un tsunami ou une tornade peuvent causer des ravages. Des incidents comme un incendie dans un centre de données, une forte pluie, une tempête de neige ou la foudre peuvent transformer une journée de travail en crise. Ils peuvent bloquer les employés chez eux, interrompre la chaîne d'approvisionnement ou la fourniture d'électricité, autant d'événements qui perturbent le fonctionnement normal de l'entreprise.
- **Défaillances technologiques** : le temps n'est pas la seule cause à l'origine de la suspension de la fourniture d'électricité ou d'autres services publics. Un accident de la route peut affecter un réseau électrique et un été caniculaire peut entraîner des baisses de tension. Même une défaillance des services téléphoniques ou des assistants personnels Blackberry peut être gênante. Les organisations dotées d'un plan de continuité d'activité bien conçu s'assurent que tous les utilisateurs du réseau peuvent être redirigés immédiatement vers un centre de données redondant où ils retrouveront toutes les ressources de l'entreprise.

- **Cyber-attaques** : une cyber-attaque visant votre réseau risque de ralentir ou d'interrompre la communication par e-mails. Un site de commerce électronique attaqué peut constater une baisse instantanée de son chiffre d'affaires. Pour un fabricant qui pratique le juste-à-temps, une interruption de la chaîne d'approvisionnement peut empêcher l'exécution d'une commande importante ou différer des rentrées d'argent et empêcher la réalisation des objectifs financiers. Un plan de continuité d'activité doit prendre en compte tous ces risques.
- **Crises de gouvernance** : il faut envisager le risque d'une crise de gouvernance où un partenaire perdrait les données personnelles de millions de clients. Le plan de continuité d'activité doit prévoir comment déterminer la cause de cet événement, comment informer les clients, quand rendre l'information publique, comment éviter que le problème se reproduise et comment restaurer l'image de l'entreprise après la crise.
- **Problèmes liés à l'externalisation** : l'externalisation expose l'entreprise à des brèches de sécurité, des retards et des problèmes de qualité imputables à un partenaire. La résilience de votre chaîne d'approvisionnement devient alors stratégique et vous devrez peut-être imposer à vos fournisseurs des plans de secours à appliquer en cas de sinistre. Vos clients ou partenaires pourront exiger la même chose de vous.
- **Ordinateurs perdus** : un cadre qui perd un ordinateur portable de son entreprise peut aussi lancer une intervention après un sinistre. Tout d'abord, il faut supposer que l'ordinateur est entre de mauvaises mains et bloquer son accès au réseau de l'entreprise. Il faut aussi prévoir que le cadre aura besoin d'accéder à des données sensibles sur ce réseau à partir d'un dispositif moins sécurisé ou non géré.

Rôle des VPN SSL dans la continuité d'activité

Dans notre monde très dépendant de l'information, il est essentiel de préserver l'accès aux ressources stratégiques pendant une interruption d'activité. Cela vaut pour tous les secteurs d'activité et les sociétés de toutes tailles, de la petite agence locale à la grosse multinationale. Les réseaux virtuels privés SSL (VPN SSL) s'imposent comme la technologie par excellence pour l'accès à distance sécurisé.

Les VPN SSL sans client fonctionnent avec tout navigateur Internet et facilitent l'accès à partir de dispositifs gérés et non gérés. Un utilisateur se connecte au boîtier VPN SSL et, après authentification, accède aux applications et aux ressources pour lesquelles il dispose de privilèges d'accès. Les VPN SSL fonctionnant au niveau de la couche application, il n'y a jamais de connexion directe avec le réseau et les utilisateurs se connectent seulement à la ressource. Ces réseaux virtuels supportent des contrôles d'accès granulaires et la totalité du flux des données est chiffrée avec SSL, le protocole de sécurité pour le trafic Internet.

Avec un VPN SSL, l'accès à distance pour la continuité d'activité offre divers avantages :

- **Des connexions sécurisées** pour l'accès par les employés aux données et aux applications de l'entreprise et surtout, aux seules ressources approuvées par les règles. Dans les VPN SSL, les contrôles d'accès acceptent les utilisateurs autorisés et rejettent les autres, ce qui est crucial pendant un sinistre.
- **La poursuite normale de l'activité** pour les clients, les fournisseurs et les partenaires, même si leurs propres opérations sont perturbées et qu'ils doivent se connecter à partir de sites distants.
- **Aucun logiciel spécial** ni configuration particulière n'est nécessaire ; les VPN SSL peuvent être utilisés à partir de dispositifs non gérés par votre service informatique, comme les bornes Internet d'aéroport et les PC domestiques, ce qui réduit la charge et les coûts liés au support.
- **La facilité de gestion**, pour que les services informatiques n'aient pas à gérer un afflux d'appels d'utilisateurs ni à dépanner un système d'accès à distance inefficace pendant une reprise sur sinistre et puissent se concentrer sur d'autres problèmes.
- **Le respect des réglementations**, les VPN SSL assurant en permanence la surveillance, l'audit et le respect de la vie privée dans le cadre d'un scénario de continuité d'activité.

Infrastructure de continuité d'activité : modèle basé sur la redondance

La redondance est le modèle à appliquer pour assurer la continuité d'activité et l'accès à distance : vous devez prévoir un centre de données de secours complètement redondant en plus du centre de données principal de votre entreprise. Une solution d'accès à distance comme un VPN SSL d'Aventail® doit se situer au périmètre de chacun de ces centres pour garantir que seules les personnes autorisées accèdent aux applications stratégiques (voir la figure 1).

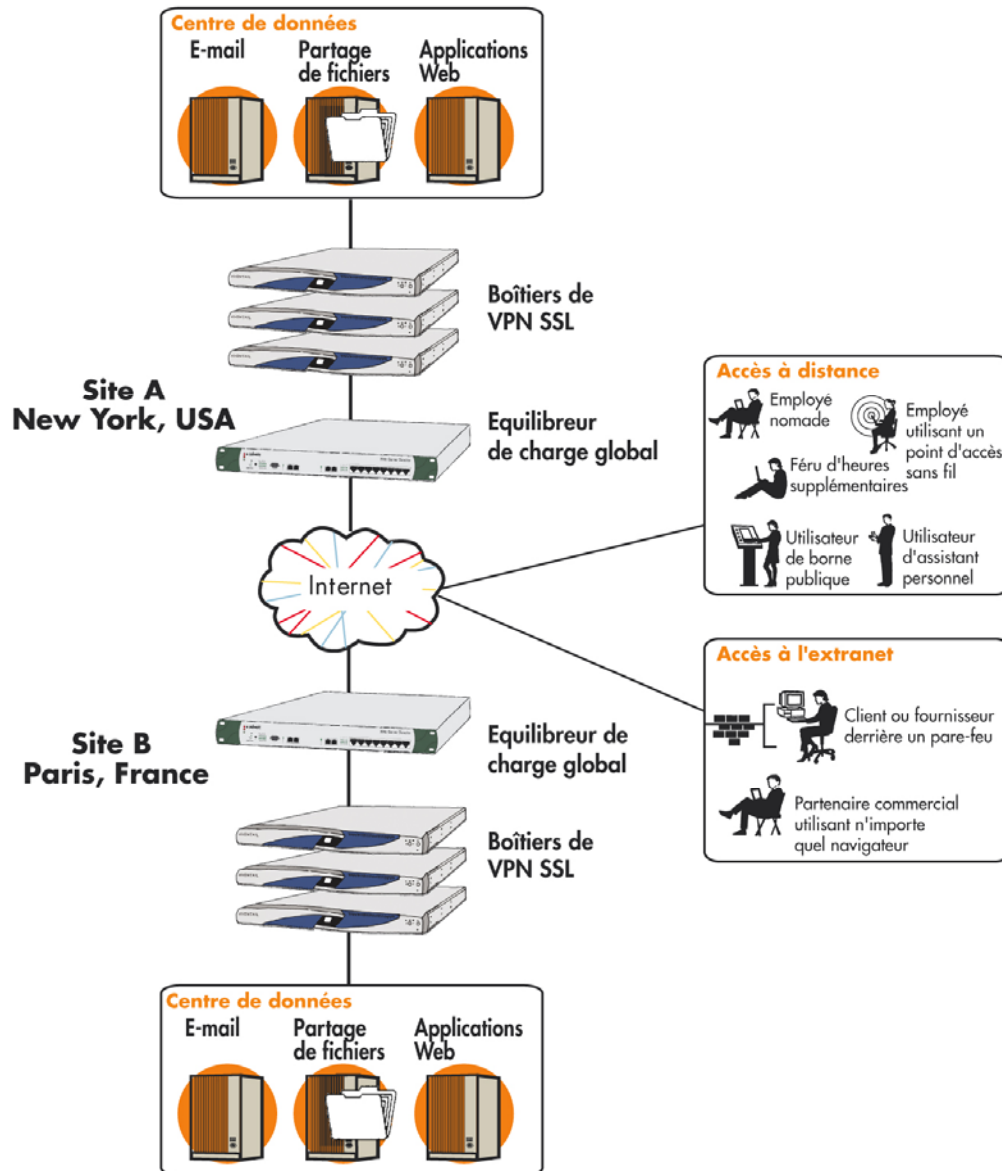


Figure 1. Un VPN SSL d'Aventail qui applique un modèle de redondance pour la continuité d'activité contribue à garantir que les utilisateurs ont accès à tout moment aux ressources dont ils ont besoin. En cas d'indisponibilité du centre de données suite à une interruption d'activité, tous les utilisateurs peuvent être dirigés sur le centre de données de secours via le portail Aventail® WorkPlace.

Solution d'accès à distance d'Aventail pour la continuité d'activité

Le VPN SSL d'Aventail garantit l'accès à distance au réseau d'entreprise pendant une interruption d'activité. Il doit s'adapter à des changements considérables concernant l'emplacement et les dispositifs pour l'accès au réseau d'entreprise. Les fonctionnalités clés suivantes du VPN Smart SSL d'Aventail® sont particulièrement pertinentes pour la continuité d'activité :

- **Accès à toutes les applications :** Aventail peut gérer l'accès à n'importe quelle ressource à partir d'un ordinateur portable de l'entreprise ou d'un dispositif non géré. Le VPN SSL d'Aventail combine l'accès Web et la technologie Aventail® Smart Tunneling™ (en instance de brevet) qui fournit une connexion réseau SSL de couche 3 pour l'accès à n'importe quelle ressource client/serveur.
- **Facilité d'utilisation :** Aventail® Smart Access™ rend l'accès plus simple, plus rapide et plus transparent pour les utilisateurs finaux car il détermine et lance automatiquement le mode d'accès le plus approprié. Les utilisateurs n'ont pas à se soucier de ce mode d'accès, du logiciel chargé sur leur PC ni du système d'exploitation utilisé. L'accès à l'application requise s'effectue en temps réel.
- **Facilité de gestion :** Aventail est le seul fournisseur de VPN SSL qui propose un modèle Unified Policy incorporant un seul jeu de règles pour tous les modes d'accès, ressources, utilisateurs et groupes. Cela facilite la configuration et réduit les coûts de gestion.
- **Cohérence :** En se servant du nom pour fournir les applications et les ressources, les règles s'adaptent aux changements dynamiques qui surviennent en cas d'indisponibilité du centre de données. Cela garantit que ces règles sont appliquées de façon cohérente dans tous les centres de données.

James Richardson International

James Richardson International (JRI) est un des principaux groupes agroalimentaires du Canada et la première entreprise céréalière privée du pays. Fonctionnant 24 heures sur 24 et 7 jours sur 7, il devait autoriser l'accès à plusieurs groupes d'utilisateurs depuis n'importe où.

JRI a conservé son VPN IPSec pour les connexions entre sites pour 85 filiales mais déployé un VPN SSL Aventail pour l'accès distant. Cette solution Aventail, sécurisée, évolutive et souple mais facile à utiliser et à gérer, répond parfaitement aux besoins de JRI.

De plus, le VPN SSL Aventail s'intégrera à la solution de reprise après un sinistre de JRI. En cas d'interruption de l'activité de JRI, les utilisateurs disposent d'un accès universel aux ressources dont ils ont besoin via le portail Aventail. JRI a acquis deux boîtiers d'Aventail afin d'assurer un basculement pour la reprise après sinistre.

- **Contrôles d'accès granulaires** : avec Aventail, les administrateurs peuvent ajuster les contrôles d'accès très précisément pour toutes les communautés d'utilisateurs. Le modèle orienté objet Aventail Unified Policy, très souple, permet aux organisations les plus complexes d'adapter leurs contrôles de règles et d'accès.
- **Évolutivité** : les solutions d'Aventail acceptent de 5 à plus de 5 000 utilisateurs avec un équilibreur de charge intégré ou externe qui permet de gérer tout aussi facilement plusieurs centaines d'utilisateurs ou quelques-uns seulement.
- **Sécurité maximum** : Aventail® End Point Control™ permet d'appliquer une règle en fonction du niveau de confiance attribué par le service informatique à l'utilisateur distant et à son environnement.

Conclusion

Les organisations qui préparent un plan de continuité d'activité doivent faire de l'accès à distance un composant essentiel de l'infrastructure mise en place. En cas de sinistre ou d'une autre interruption d'activité, il est plus important que jamais de pouvoir accéder à l'information stratégique de l'entreprise et de maintenir la productivité. Une solution d'accès à distance peut aussi contribuer à protéger les sources de revenus et la réputation de la société.

L'accès à distance sécurisé avec un VPN SSL d'Aventail permet aux employés, aux clients et aux partenaires d'accéder aux données et aux applications clés du réseau depuis l'extérieur de la société. Cet accès universel à partir de n'importe quel dispositif et n'importe quelle connexion Internet est totalement sécurisé.

En préservant les sources de revenus et le maintien de l'activité pendant une crise, le plan de continuité d'activité protège la réputation de l'entreprise. Cette dernière devient un fournisseur et un partenaire plus fort et plus fiable qui possède une longueur d'avance sur ses concurrents moins bien préparés. De plus, le plan de continuité d'activité est conforme aux réglementations qui imposent des pistes d'audit pour les informations sensibles ou protégées. Disposer d'un accès à distance sécurisé dans le cadre de ce plan allège la charge de travail du service informatique quand un problème survient.

Rappelons-le une dernière fois, bénéficier de ces avantages suppose toutefois de se préparer aux situations de crise en élaborant un plan.

À propos de l'auteur

Tim Clark est un associé du cabinet d'analyse et d'études de marché The FactPoint Group (www.factpoint.com) implanté dans la Silicon Valley. Depuis 1992, ce cabinet fournit des services de conseil et des études personnalisées et multiclients aux éditeurs de logiciels et aux entreprises. Récemment, Tim Clark a axé ses recherches sur la continuité d'activité, l'informatique à la demande, la sécurité réseau, les réseaux de capteurs, l'exploitation sous licence du code source ouvert et les services Web. Auparavant, il était analyste senior chez Jupiter Media Metrix et Net Market Makers. Avant cela, il fut journaliste et rédacteur pendant 24 ans, et notamment chroniqueur pour CNET News.com où il couvrait le commerce électronique et la sécurité sur Internet.

À propos de SonicWALL®

Leader mondialement reconnu de la sécurité et de la protection de données, SonicWALL® conçoit, développe et fabrique des solutions assurant une protection complète du réseau et des données dans les domaines de la sécurité réseau, de l'accès distant sécurisé, de la sécurité du courrier électronique et des accès Web, et de la sauvegarde/récupération de données. SonicWALL donne aux organisations de toutes tailles les moyens de protéger efficacement leur réseau et leurs informations sensibles. A travers son vaste portefeuille de solutions — déployées sous forme d'appliances ou de services à valeur ajoutée accessibles par abonnement —, SonicWALL propose un système complet de protection des accès Internet et des données d'entreprise, de façon à préserver le réseau et l'activité même de ses clients. Pour plus d'information, visitez www.sonicwall.com.

À propos d'Aventail

Aventail est une société leader de l'accès distant qui dès 1997, fournit la première solution de VPN SSL du marché. Aventail est actuellement le leader du marché grâce à sa solution facile à utiliser et au contrôle d'accès distant. Les appliances Smart VPN SSL d'Aventail fournissent aux utilisateurs une transparence, un accès sans client à un maximum d'applications depuis tout type d'environnement réseau. Pour les DSI, Aventail fournit un simple accès sécurisé pour tous les utilisateurs, interne et externe à l'ensemble des ressources réseau avec une sécurité complète. Avec plus de 2 millions d'utilisateurs dans le monde, Aventail est le VPN SSL de choix des moyennes et grandes entreprises mondiales notamment AT&T, l'Agence de Protection de l'Environnement (EPA), Chicago Housing Authority, DuPont, Radiology Ltd, James Richardson International, Organisation de Coopération et de Développement Economiques (OCDE), Overlake Hospital, IBM Global Services, etc. Pour plus d'information, visitez www.aventail.com