



- **Expérience familière de type « au bureau », de n'importe où**
- **Facilité de déploiement, de gestion et de contrôle**
- **SonicWALL Aventail Unified Policy**
- **Accès sécurisé à toutes les applications**
- **Contrôle de séparation des flux (split tunneling)**

### **Expérience familière de type « au bureau »**

Dans les entreprises modernes, les affaires se font de plus en plus souvent à distance. Télétravailleurs, cadres en déplacement travaillant sur leur portable géré, partenaires extranet... autant d'acteurs stratégiques qui doivent disposer d'un accès complet aux applications métier vitales, y compris les applications « back-connect » telles que les softphones VoIP et l'assistance technique à distance – comme s'ils se trouvaient au bureau. Pour les équipes informatiques, le défi consiste à offrir cet accès complet tout en garantissant une sécurité optimale au niveau des bureaux, notamment avec le contrôle de séparation des flux (split tunneling) et la détection des pare-feu personnels.

SonicWALL® Aventail® Connect Tunnel™ crée un environnement de type « au bureau », simple et sécurisé, pour les utilisateurs de VPN SSL E-Class SonicWALL Aventail. Ce client Web permet aux utilisateurs d'ordinateurs distants et portables autorisés d'accéder en toute sécurité, où qu'ils soient, à l'ensemble du réseau de leur entreprise. Connect Tunnel constitue la méthode d'accès distant sécurisé la plus simple et la plus complète actuellement disponible sur le marché, et protège idéalement les utilisateurs de réseaux sans fil (WLAN) et les employés nomades pour qui l'accès total au réseau est indispensable même en dehors du bureau.

### **Caractéristiques et avantages**

**Expérience familière de type « au bureau », de n'importe où.** Les utilisateurs à distance de terminaux gérés (ordinateurs de bureau ou portables autorisés, par exemple) bénéficient d'un accès aux ressources réseau aussi complet que lorsqu'ils sont sur le LAN de leur bureau. Connect Tunnel offre le plus haut niveau de transparence et une convivialité inégalée, grâce notamment à l'authentification unique, la reconnaissance automatique de réseau et l'intégration de numéroteurs de fournisseurs tiers. Les utilisateurs n'ont pas à se demander comment accéder au mieux à leurs ressources. Il leur suffit de cliquer sur une icône placée sur le bureau du terminal géré pour s'authentifier automatiquement sur le réseau via Internet. La technologie SonicWALL Aventail Smart Access™ détermine et active automatiquement la méthode d'accès à distance appropriée aux ressources réseau nécessaires, en tenant compte des règles administratives définies.

**Facilité de déploiement, de gestion et de contrôle.** Connect Tunnel s'installe sans difficulté sur les terminaux gérés et permet aux administrateurs d'activer l'installation automatique des nouvelles versions et de modifier la configuration sans plus d'intervention. Le client léger Aventail Connect Tunnel peut être préinstallé sur un terminal géré ou téléchargé à partir d'un portail Web. Il représente ainsi une alternative idéale et facile à installer aux clients VPN IPSec « lourds ».

**SonicWALL Aventail Unified Policy™.** Centralise le contrôle de l'ensemble des utilisateurs, groupes, ressources et appareils, permettant aux administrateurs de définir rapidement des règles uniques valables pour tous les objets. SonicWALL Aventail End Point Control™ permet d'identifier tous les terminaux Windows®, Macintosh® et Linux®, et d'appliquer les règles de

sécurité appropriées, grâce à la détection automatique de différents critères : logiciel antivirus, pare-feu personnels, applications, annuaires, noms et tailles de fichiers, horodatages, versions de Windows, domaines, entrées de registre...

**Accès sécurisé à toutes les applications** (y compris VoIP et assistance technique à distance). La technologie SonicWALL Aventail Smart Tunneling™ associe le contrôle de couche applicative du SSL à la portée d'un tunnel de couche 3. Cette architecture unique offre un accès aux applications sans équivalent sur le marché, qui prend en charge les protocoles UDP, TCP et IP, ainsi que le contrôle d'accès granulaire et bidirectionnel pour toutes les applications, y compris les applications « back-connect » comme VoIP et l'assistance technique à distance. Un terminal VoIP peut être interrogé et l'utilisateur authentifié avant autorisation de la connexion, afin de prévenir toute attaque de programme malveillant.

### **Contrôle de séparation des flux (split tunneling).**

Permet aux services informatiques de contrôler la capacité d'un utilisateur à se connecter à plusieurs réseaux au cours d'une session VPN. Le mode NAT traversal, la détection de proxy, le « traversal » et l'adaptation dynamique pour réduire les conflits d'adresses garantissent un accès universel aux applications. Connect Tunnel s'intègre facilement aux numéroteurs Internet et autres logiciels de bureau. Enfin, l'accès total des utilisateurs aux applications dont ils ont besoin, le contrôle granulaire des règles et la sécurité offerts par Connect Tunnel en font une alternative simple et efficace à la lourdeur des VPN IPSec.

**Connect Mobile**

E-Class EX-750

01-SSC-7704

Complément

E-Class EX-1600

Inclus

E-Class EX-2500

Inclus

**Fonctionnement de SonicWALL Aventail Connect Tunnel**

Le client léger SonicWALL Aventail Connect Tunnel peut être préinstallé sur un terminal géré par le service informatique ou téléchargé à partir d'un portail Web. Une fois Connect Tunnel installé, l'utilisateur n'a plus besoin de se rendre sur un site ou portail Web pour accéder aux ressources autorisées du réseau, et bénéficie pleinement d'une expérience de type « au bureau ». Il lui suffit de cliquer sur l'icône SonicWALL Aventail Connect de son bureau pour s'authentifier automatiquement et accéder au réseau via Internet, à partir du terminal géré.

Spécifications	Navigateur	Remarques
<b>Système d'exploitation</b> <b>Windows Vista®</b> <b>Windows XP Pro, SP2</b> <b>Windows 2000 Pro, SP4</b> <b>Windows XP Home, SP2</b>	ND	L'installation requiert des droits d'administrateur Windows
<b>Plate-forme de serveur Windows :</b> <b>Windows 2003 Server</b> <b>Windows 3000 Server, SP4</b>	ND	L'installation requiert des droits d'administrateur Windows
<b>Macintosh OS X v 10.5</b>	ND	L'installation requiert des droits d'administrateur End Point Control non pris en charge Macintosh OS X v 10.5 testé uniquement sur des ordinateurs Intel
<b>Linux kernel 2.4.20 ou version ultérieure</b>	Mozilla Firefox 2.0 (Mozilla Firefox 1.5)	L'installation requiert des droits d'administrateur Navigateur nécessaire uniquement pour la détection de proxy End Point Control non pris en charge

Pour plus d'informations sur les solutions VPN SSL E-Class de SonicWALL Aventail, rendez-vous sur [www.sonicwall.com](http://www.sonicwall.com)

**Support France**

Appel gratuit : 0800.970.019

Tél. : +31 (0) 411.617.812

E-mail : [sales\\_support-europe@sonicwall.com](mailto:sales_support-europe@sonicwall.com)**Bureau France**

Tél. : +33.0.1.49.33.73.09

Inside sales : +32 (0)15.293.001

E-mail : [france@sonicwall.com](mailto:france@sonicwall.com)

PROTECTION AT THE SPEED OF BUSINESS™