



Accès Mobile Sécurisé à L'aide de VPN SSL

Septembre 2005

**Un livre blanc préparé par Peter Rysavy
<http://www.rysavy.com>
+1-541-386-7475**

Rapport de synthèse

L'accès à distance gagne sans cesse en complexité. Il ne concerne plus seulement les cadres souhaitant accéder à leur courrier électronique ou à des données pendant leurs déplacements mais aussi des employés, des partenaires et des clients désireux de se connecter à partir d'environnements et de périphériques Internet très variés. De plus en plus, les employés nomades veulent accéder aux ressources de l'entreprise à partir de dispositifs mobiles comme des téléphones hybrides et des assistants numériques personnels sans fil. Ces appareils sont de puissants ordinateurs portables capables d'accéder à des informations très variées sur votre réseau, par l'intermédiaire d'applications Web et client/serveur. Les entreprises doivent à la fois sécuriser efficacement et fournir l'accès mobile aux seules ressources appropriées pour des utilisateurs et des dispositifs particuliers. Aventail relève le défi en proposant un réseau virtuel privé SSL (VPN SSL) aux fonctions spécialement conçues pour les dispositifs mobiles. Le VPN Smart SSL d'Aventail[®], qui incorpore la solution d'accès Aventail Secure Mobile Access, présente les caractéristiques suivantes :

- il utilise des méthodes éprouvées d'authentification des utilisateurs et de chiffrement des données ;
- il prend en charge l'accès mobile pour les dispositifs portatifs et les ordinateurs portables sur une seule plate-forme de sécurité, à la différence d'approches concurrentes qui nécessitent deux architectures d'accès mobile indépendantes ;
- il répond aux besoins spécifiques des utilisateurs de dispositifs mobiles en fournissant une interface utilisateur conçue pour les dispositifs de petit format ;
- il personnalise l'accès à l'information pour adapter cette dernière au dispositif utilisé ;
- il propose deux formes d'accès dont l'une autorise tout dispositif pourvu d'un navigateur Web à accéder à l'information et l'autre fournit un petit client téléchargeable via une session Web pour une interaction client/serveur totale ;
- il contient un outil de gestion et d'administration très complet pour un contrôle granulaire de l'accès.

Avec le VPN SSL d'Aventail, une architecture de sécurité protège toutes les formes d'accès à distance, y compris à partir de dispositifs portatifs et d'ordinateurs portables. Si vous utilisez déjà des terminaux mobiles pourvus de leur propre architecture de communication, notamment pour les applications de type « push e-mail », vous pouvez utiliser les solutions Aventail Mobile afin d'accroître la variété des applications et des données disponibles.

Introduction

Les modes d'accès aux ressources de l'entreprise par les employés nomades et les télétravailleurs continuent à se développer. L'accès à distance s'effectue essentiellement via des connexions par ligne commutée. Il couvre une large gamme d'options de réseau, notamment domestiques, Wi-Fi publics et cellulaires 3G. Le nombre d'options de connectivité réseau augmente, ainsi que celui des dispositifs mobiles utilisés pour l'accès.

Les ordinateurs portables fournis par l'entreprise ont été un temps le principal moyen d'accès à distance mais aujourd'hui les employés veulent aussi accéder aux ressources de

l'entreprise à partir d'ordinateurs personnels, de terminaux publics et de divers dispositifs mobiles comme les assistants numériques personnels sans fil et les téléphones hybrides. Bien que les entreprises fournissent nombre de ces appareils à leurs employés, il est fréquent que des utilisateurs s'équipent eux-mêmes en vue d'un usage professionnel et personnel.

Aujourd'hui, presque tous les téléphones mobiles sont équipés d'un micronavigateur potentiellement capable d'accéder aux ressources de l'entreprise. Par ailleurs, les téléphones hybrides et les assistants numériques personnels, plus puissants, sont pourvus de véritables systèmes d'exploitation multitâches, de navigateurs très performants, de clients de messagerie électronique aux fonctions très complètes ; capable de prendre en charge des transactions client/serveur sophistiquées. Ces terminaux mobiles fonctionnent principalement sous Linux, Windows Mobile, Palm OS, RIM Blackberry et Symbian.

Il incombe aux entreprises d'optimiser la sécurisation des communications à partir de ces dispositifs, de gérer la multiplicité des réseaux utilisés et de personnaliser l'accès aux ressources en fonction de l'identité de l'utilisateur et du niveau de sécurité du dispositif utilisé comme de l'environnement d'accès. Une solution de sécurité doit aussi inclure des méthodes d'authentification rigoureuses, utiliser des algorithmes de chiffrement éprouvés, limiter l'accès aux ressources de l'entreprise en fonction des dispositifs utilisés et fournir un moyen efficace et immédiat pour désactiver l'accès si un utilisateur perd son terminal mobile.

En tant qu'entreprise, vous avez le choix entre de nombreuses options d'accès mobile dont chacune a ses avantages et ses inconvénients. Ce livre blanc présente quelques-unes des méthodes d'accès à distance les plus courantes et montre que, pour de nombreuses sociétés, une architecture VPN SSL avancée peut prendre en charge une gamme très large de dispositifs d'accès au réseau. Gérer n'importe quel type de dispositif mobile nécessite d'intégrer des dispositions spécifiques au niveau du VPN SSL pour permettre l'accès à partir de dispositifs portatifs. Actuellement, seul le VPN Smart SSL d'Aventail, intégrant la technologie Aventail Mobile, répond à cette exigence.

Fonctionnalités des terminaux mobiles

Pour comprendre quand appliquer une méthode d'accès à distance particulière, il est utile de passer en revue les types de dispositifs mobiles les plus courants et de comprendre leurs fonctionnalités. Contrairement à l'ordinateur portable qui est devenu un produit grand public, les dispositifs de plus petit format forment encore une catégorie hétéroclite qui recouvre une large gamme de fonctionnalités, de multiples systèmes d'exploitation, des variations de formats considérables et des interfaces utilisateur très différentes.

La convergence des types de dispositifs est peu vraisemblable puisque les dispositifs correspondent à des modèles d'utilisation spécifiques très variés. Certaines personnes souhaitent des dispositifs servant principalement de téléphone mais capables occasionnellement de transmettre des données, éventuellement de surveiller les e-mails entrants mais rarement de composer ou d'envoyer des e-mails.

Ces utilisateurs opteront pour un appareil similaire à celui d'un téléphone standard mais pourvu d'un micronavigateur. D'autres auront de plus gros besoins d'accès aux données et préféreront un dispositif de type assistant personnel doté d'un clavier et capable d'exécuter des applications client/serveur.

Le tableau suivant recense les principales fonctionnalités des dispositifs mobiles actuels.

Tableau 1 : Fonctionnalités des terminaux mobiles actuels

Appareils les plus répandus	Téléphone mobile à grand écran Téléphone mobile à double coque avec grand écran et clavier Assistant numérique personnel sans clavier Assistant numérique personnel avec clavier miniature
Capacités d'affichage types	160 x 240 pixels 200 x 640 pixels 240 x 320 pixels 320 x 320 pixels
Systèmes d'exploitation	Linux Palm OS RIM Blackberry Symbian Windows Mobile Systèmes propriétaires
Options de l'environnement d'exécution d'applications	BREW (Binary Runtime Environment for Wireless) Basées sur un navigateur Java Applications natives (C++)
Fonctionnalités de messagerie électronique	Basées sur un navigateur Client prenant en charge Microsoft ActiveSync Client prenant en charge les protocoles Internet (POP3, IMAP) Client prenant en charge les protocoles RIM Blackberry
Fonctionnalités du navigateur	Wireless Markup Language HTML xHTML JavaScript SSL

Que peut-on conclure de ce tableau ? Les dispositifs mobiles actuels sont puissants mais très différents les uns des autres. Toutefois, tous ont deux choses en commun : la gestion des réseaux de données TCP/IP et la fourniture d'un accès aux informations de l'entreprise. L'accès mobile fut d'abord axé sur le courrier électronique et la synchronisation des agendas à distance mais de nombreuses sociétés commencent à voir les avantages liés à la fourniture d'autres informations aux employés nomades équipés de dispositifs portatifs. Les offres récentes proposent des applications pour le contrôle des stocks, une base de données client, la gestion de la relation client, la gestion de projet, l'automatisation de la force de vente et l'immobilier.

Toutefois, pour être utile et efficace, tout système d'accès mobile doit répondre aux besoins d'utilisateurs spécifiques et aux impératifs de dispositifs mobiles particuliers.

Accès à distance à l'aide d'un terminal mobile : les besoins

Il existe actuellement plusieurs approches destinées à fournir un accès mobile. Avant de comparer leurs avantages, il est important de comprendre les besoins décrits ci-après auxquels chacune doit impérativement répondre :

- **Sécurité.** Le système d'accès à distance doit utiliser des méthodes éprouvées d'authentification des utilisateurs et de chiffrement des données. Les premières doivent être suffisamment performantes pour gérer les conséquences de la perte d'un dispositif mobile par son utilisateur. Les secondes doivent empêcher les écoutes clandestines sur la liaison radio, en particulier sur une connexion Wi-Fi. Le chiffrement doit aussi protéger les communications sur Internet.
- **Un système commun pour tous les terminaux mobiles.** Il est très utile que le système d'accès mobile prenne en charge à la fois les ordinateurs portables et une grande variété de dispositifs portatifs, notamment des téléphones et assistants numériques personnels.
- **Réponse aux besoins spécifiques des utilisateurs de dispositifs mobiles.** Le système doit fournir une interface utilisateur adaptée aux petits écrans des dispositifs mobiles et autoriser l'accès au seul sous-ensemble d'informations de l'entreprise pertinentes pour un dispositif mobile particulier.
- **Granularité et facilité de gestion.** Les administrateurs doivent pouvoir définir facilement des règles de contrôle d'accès granulaire aux ressources, basées sur les règles de sécurité. Cela améliore le confort de l'utilisateur, qui ne voit que les informations pertinentes pour lui, et limite les risques en cas de perte d'un dispositif mobile. Des outils de gestion doivent aussi permettre de désactiver facilement l'accès si nécessaire.
- **Prise en charge des exigences propres aux réseaux sans fil.** Les connexions sans fil ne sont pas aussi stables que celles des réseaux câblés. Le système d'accès mobile devra supporter des difficultés de connectivité de courte durée.

Architectures pour l'accès mobile

Les fournisseurs adoptent des approches différentes pour l'accès mobile. Certaines solutions sont conçues spécifiquement pour les assistants personnels numériques et les téléphones hybrides, à l'exemple d'Extended Systems (Sybase), Good Technology, Intellisync, JP Mobile, RIM et Seven Networks. Leurs finalités premières sont l'envoi automatique des nouveaux messages électroniques au dispositif (« push e-mail ») et la synchronisation des agendas et des bases de données de contacts. Leurs fournisseurs travaillent aussi à rendre toutes autres informations de l'entreprise accessibles aux utilisateurs. Ces dispositifs mobiles recourent pour cela à des méthodes propriétaires nécessitant des applications tierces ou une programmation personnalisée. Bon nombre de ces architectures spécifiques aux terminaux mobiles possèdent des outils de gestion centralisée et la plupart proposent des passerelles derrière le pare-feu pour mettre en œuvre leurs systèmes. Certaines proposent aussi leurs solutions aux opérateurs de téléphones cellulaires qui implémentent les passerelles sur leurs réseaux et vendent l'accès moyennant un abonnement mensuel.

Si ces solutions peuvent s'avérer intéressantes, en particulier pour les entreprises qui déploient un très grand nombre de dispositifs portatifs où l'aspect gestion devient essentiel, elles nécessitent de recourir à des administrateurs de réseaux pour gérer un

système d'accès mobile complètement distinct du système distant utilisé par les télétravailleurs et les utilisateurs d'ordinateurs portables.

Une autre approche consiste à utiliser un VPN IPSec pour l'accès à partir des dispositifs portatifs. Ce type de solution présente plusieurs inconvénients : les clients VPN ne sont disponibles que pour un nombre limité de dispositifs mobiles. Il nécessite l'installation d'un logiciel client pour l'accès et assurer une gestion et un support permanents.

Dans l'architecture d'un VPN SSL, vous tirez parti du protocole de sécurité SSL d'un navigateur Web standard autorisant un accès sécurisé à partir de n'importe quel dispositif. Tous téléphones hybrides et assistants numériques personnels sans fil sont dotés de navigateurs capables de communiquer avec une passerelle de sécurité VPN SSL installée sur votre réseau. Cette architecture peut prendre en charge n'importe quel dispositif portatif. Et il n'y a qu'un seul système d'accès à gérer. Ajoutons qu'il est inutile d'installer un logiciel client sur les terminaux mobiles pour accéder au réseau.

Présentation d'Aventail Mobile

La solution d'accès Aventail Secure Mobile Access est un VPN SSL se distinguant des solutions IPSec et autres solutions VPN SSL classiques car il prend en charge l'accès à distance à partir de n'importe quel dispositif. Il gère également l'accès interne à partir de nœuds non sécurisés dans l'entreprise comme un ordinateur portable se connectant au réseau via une connexion Wi-Fi. Le VPN SSL offre l'avantage de fournir un accès avec un seul URL qualifiant l'interface de portail suivant que l'utilisateur accède à la passerelle via un ordinateur portable, un terminal public, un ordinateur domestique, un assistant numérique personnel ou un téléphone hybride. L'administrateur utilise également le même modèle centralisé de règles de sécurité pour gérer tous les dispositifs utilisés pour l'accès. En cela il se démarque très nettement de nombreuses architectures d'accès mobiles complètement distinctes des solutions d'accès à distance à partir d'un ordinateur portable.

L'utilisation du VPN SSL d'Aventail n'empêche aucune autre utilisation d'architectures d'accès mobile comme RIM Blackberry. Dans certains scénarios, utiliser deux architectures est tout à fait légitime, le VPN SSL fournissant l'accès aux données et aux applications générales, et l'autre solution fournissant des fonctionnalités de type « push e-mail ».

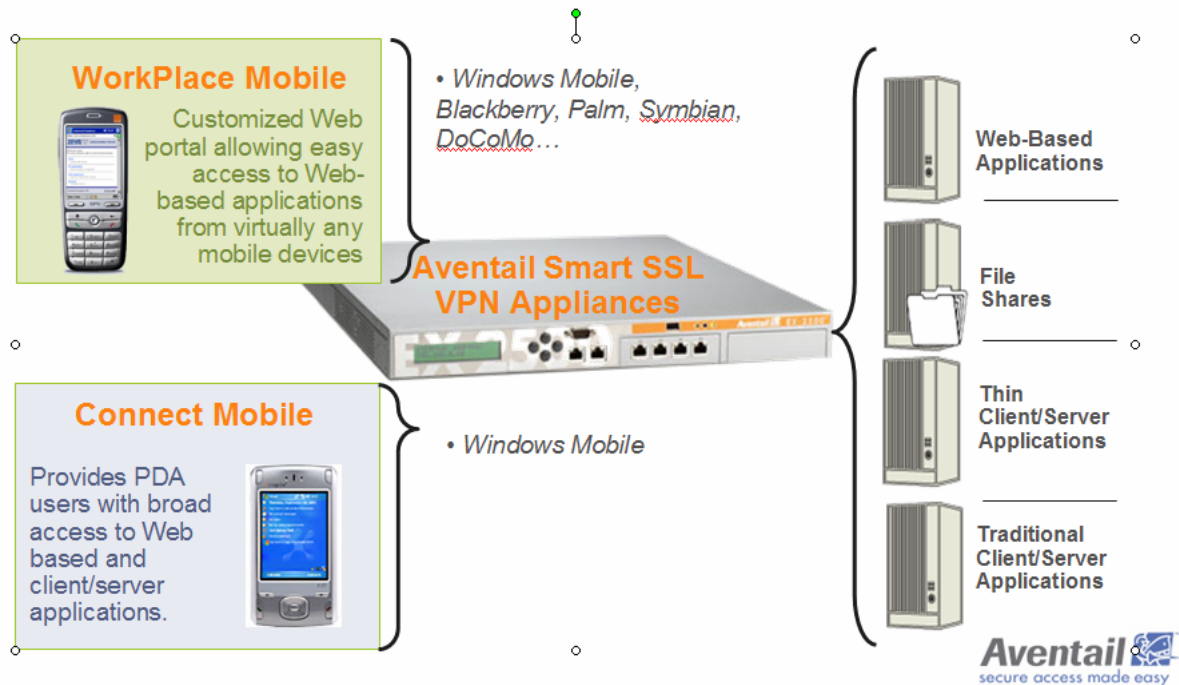
Le VPN SSL d'Aventail propose le chiffrement basé sur le protocole SSL, le contrôle d'accès de niveau utilisateur et une authentification des utilisateurs très stricte avec, notamment, les jetons RSA SecurID et les certifications numériques. L'accès des utilisateurs de terminaux mobiles est autorisé en fonction de l'identité de l'utilisateur et de la sécurité du dispositif utilisé. En outre, l'accès est limité aux ressources nommées et il n'y a pas de connexion directe avec le réseau de l'entreprise.

Capable de reconnaître les fonctionnalités de chaque dispositif mobile, le VPN SSL d'Aventail est conçu spécifiquement pour l'accès mobile. Il propose deux options d'accès : Aventail® WorkPlace Mobile™ et Aventail® Connect Mobile™. WorkPlace Mobile est un portail optimisé pour l'accès mobile conçu pour les dispositifs non gérés fournissant l'accès aux applications Web à partir de tout dispositif mobile. Il présente un contenu personnalisé basé sur les autorisations utilisateur et sur le type de méthode utilisée. Il prend en charge les dispositifs fonctionnant sous Palm OS, RIM Blackberry, Symbian, WAP browser et Windows Mobile.

Connect Mobile utilise un petit client déployé sur le Web fournissant aux utilisateurs d'assistants numériques personnels Windows Mobile un large accès aux applications Web et client/serveur par l'intermédiaire d'une connexion avec proxy pour éviter l'accès direct à votre réseau. Un contrôle hautement granulaire garantit aux utilisateurs un accès uniquement au contenu pertinent. Les utilisateurs n'ayant pas téléchargé le client Aventail Connect au préalable peuvent le faire depuis le portail WorkPlace Mobile.

La figure suivante illustre les deux approches précédemment décrites.

Figure 1 : Aventail WorkPlace Mobile et Aventail Connect Mobile



Les éléments clés de toute solution d'accès à distance sont des règles de sécurité et un contrôle d'accès centralisés. La technologie Aventail Mobile, totalement intégrée au modèle Aventail® Unified Policy™, facilite la définition par les administrateurs de règles de contrôle d'accès granulaire et de contrôle des terminaux mobiles servant à accéder aux ressources du réseau. L'administrateur peut spécifier précisément les ressources disponibles pour les utilisateurs de dispositifs mobiles.

Ces éléments constituent un système d'accès à distance capable de gérer tous les types de dispositifs mobiles. Le coût total de cette solution est inférieur à celui des solutions concurrentes, puisque sa gestion prend moins de temps.

Ainsi, le VPN SSL d'Aventail peut fournir un large accès réseau à partir de n'importe quel dispositif mobile ou presque, simplifiant la tâche des utilisateurs et du service informatique. Avec l'accès à distance Aventail, vos utilisateurs restent productifs où que leur travail les conduise.

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'informations, consultez le site www.aventail.com.