



# **ETABLISSEMENT D'UN RESEAU SECURISE SANS FIL A L'AIDE D'UN VPN SSL**

**Rédigé par Peter Rysavy  
<http://www.rysavy.com>  
1-541-386-7475**

## TABLE DES MATIERES

<b>RAPPORT DE SYNTHÈSE</b> .....	<b>2</b>
<b>PREDOMINANCE DES RESEAUX SANS FIL</b> .....	<b>3</b>
<b>PROBLEMES DE SECURITE DES CONNEXIONS SANS FIL</b> .....	<b>3</b>
Problèmes posés par la technologie Wi-Fi .....	3
Problèmes posés par les réseaux cellulaires.....	4
Multiplicité des connexions et des plates-formes .....	4
<b>ARCHITECTURE SECURITAIRE RECOMMANDEE</b> .....	<b>5</b>
Modèle de sécurité inversée .....	6
VPN SSL et autres approches .....	6
<b>FONCTIONNALITES DES VPN SSL D'AVENTAIL</b> .....	<b>7</b>
Aventail Smart Access .....	8
Aventail Smart Tunneling.....	9
Aventail End Point Control .....	9
Intégration à l'infrastructure existante de gestion de la sécurité .....	9
<b>CONCLUSION</b> .....	<b>10</b>
<b>A PROPOS D'AVENTAIL</b> .....	<b>10</b>

## Rapport de synthèse

Les entreprises se tournent vers les technologies sans fil pour améliorer leur productivité, assouplir la manière de travailler de leurs employés tout en collaborant plus étroitement avec leurs partenaires commerciaux. Les technologies sans fil englobent les systèmes locaux et étendus. Toutefois, la multiplicité des options de réseau et des plates-formes informatiques pose d'importants problèmes de sécurité :

- Disparité des options de sécurité entre les réseaux locaux sans fil (WLAN) et les réseaux cellulaires.
- Evolutivité de la sécurité des réseaux locaux sans fil et problèmes d'interopérabilité entre fournisseurs.
- Equipements de WLAN obsolètes et non sécurisés.
- Points d'accès incontrôlables.
- Transit par Internet de nombreuses solutions d'accès à distance.
- Les employés utilisant des terminaux gérés ou non par le service informatique, par exemple des ordinateurs domestiques ou des terminaux publics.

Les réseaux privés virtuels (VPN) SSL - notamment ceux d'Aventail - constituent l'architecture sécuritaire capable de résoudre tous ces problèmes. Les VPN Smart SSL d'Aventail permettent de protéger chaque nœud interne ou externe de l'entreprise, ce qui correspond au principe de modèle de sécurité inversée non tributaire d'un périmètre protégé. En utilisant les navigateurs en place et la couche de sécurité SSL, les entreprises peuvent offrir un accès depuis des ordinateurs non dotés d'un client VPN mais également assouplir la communication des systèmes équipés de logiciels installés de façon dynamique. Le VPN Smart SSL d'Aventail® fournit aussi un accès hautement granulaire afin de limiter l'accès des utilisateurs à des applications spécifiques.

Afin d'être toujours plus performants, Aventail a mis au point les fonctionnalités suivantes pour renforcer la sécurité et réduire les coûts de déploiement et de gestion :

- 1. Aventail® Smart Tunneling™.** Ce composant crée un tunnel de réseau IP complet, basé sur la technologie SSL, destiné au fonctionnement de toutes les applications, même les plus exigeantes, comme celles utilisant la Voix sur IP (VoIP, Voice over Internet Protocol).
- 2. Aventail® End Point Control™.** Les zones de confiance d'Aventail correspondent à des scénarios d'accès très divers et incluent notamment l'inspection des ordinateurs afin de les protéger contre des antiprogrammes locaux et l'effacement des caches en fin de session.

3. **Intégration à l'infrastructure sécuritaire existante.** Aventail® Unified Policy™ permet l'intégration aux systèmes de sécurité existants tels RADIUS (Remote Authentication Dial-In User Service), LDAP (Lightweight Directory Access Protocol), Active Directory, et autres certificats numériques et authentification à deux facteurs.

## Prédominance des réseaux sans fil

Nombre d'entreprises adoptent les technologies de réseau sans fil pour accroître la productivité de leurs employés, améliorer le service à la clientèle, mais aussi pour fournir un accès Internet à leurs visiteurs. Lors de leurs déplacements professionnels, les employés ont recours aux points d'accès sans fil installés dans les lieux publics (aéroports, restaurants...) et utilisent volontiers une connexion Wi-Fi dans leur chambre d'hôtel ou chez eux. Ils se servent également des réseaux cellulaires pour communiquer de quasiment n'importe quel endroit.

Bien que la transmission sans fil de données repose essentiellement sur la technologie Wi-Fi (norme IEEE 802.11), les entreprises utilisent de plus en plus les services du réseau cellulaire, car ceux-ci offrent des transmissions semblables aux connexions à large bande, avec une large couverture. La connexion cellulaire s'établit à l'aide de téléphones hybrides, d'assistants numériques, d'ordinateurs portables dotés de cartes modem PC ou utilisant un téléphone comme modem au moyen d'une connexion câblée ou d'une carte Bluetooth. Les réseaux cellulaires recouvrent diverses technologies, les plus courantes étant notamment : EDGE (Enhanced Data Rates for GSM Evolution), WCDMA (Wideband CDMA) et le groupe CDMA2000. Malgré leurs appellations diverses, elles remplissent une même fonction : la transmission par paquets à l'aide du protocole IP, de pratiquement n'importe quel endroit.

Les technologies émergentes telles WiMAX promettent d'être encore plus performantes sur de grandes zones géographiques. Alors que les réseaux cellulaires assurent un débit proche de 1 Mbit/s, les fournisseurs de WiMAX espèrent faire mieux.

De nombreux professionnels utilisent à la fois la technologie Wi-Fi et les réseaux cellulaires. Les réseaux sans fil n'augmentent pas seulement la productivité, ils améliorent aussi le mode de vie des employés en leur permettant de travailler de chez eux, ou quelque soit l'endroit où ils se trouvent.

Toutefois, la multiplicité des modes de connexion soulève la question cruciale de la sécurité. Les entreprises doivent, en effet, sécuriser les connexions tout en étant compatibles avec divers types de plates-formes informatiques mobiles, en simplifiant la tâche des utilisateurs et en limitant l'accès à des ressources spécifiques, le tout dans un système facilement administrable.

## Problèmes de sécurité des connexions sans fil

En matière de réseau sans fil, la sécurité constitue la principale préoccupation des responsables de services informatiques. Cette inquiétude est compréhensible, car les radiosignaux sont particulièrement exposés aux indiscretions en raison de leur large propagation.

Fort heureusement, les modes de sécurisation des connexions Wi-Fi et cellulaires ne manquent pas. Pour en distinguer les avantages et les limites, un examen minutieux des problèmes de sécurité s'impose.

### ***Problèmes posés par la technologie Wi-Fi***

Première tentative de sécurisation des connexions Wi-Fi, le WEP (Wired Equivalency Protocol) a été totalement inadéquat, car une personne malveillante et déterminée pouvait facilement surveiller les connexions ou accéder au réseau. La norme de sécurité IEEE 802.11i a ensuite été mise au point pour pallier à ces inconvénients. Elle comporte deux versions :

- WPA (Wi-Fi Protected Access) corrige les défauts du WEP,
- WPA2 assure le chiffrement à l'aide de la norme AES (Advanced Encryption Standard).

La norme IEEE 802.11i repose sur IEEE 802.1X, une architecture sécuritaire basée sur les ports, dans laquelle l'authentification combine méthodes EAP (Extensible Authentication Protocol) et systèmes d'authentification de type RADIUS. La plupart des nouveaux équipements prennent en charge les normes WPA ou WPA2, considérées comme assez sûres.

Cependant, les organisations dont les réseaux Wi-Fi reposent sur la norme IEEE 802.11i sont confrontées à plusieurs problèmes : IEEE 802.11i ne gère pas les équipements déployés les moins récents, ensuite elle ne protège que les équipements d'accès contrôlés par l'organisation. Ajoutons que la complexité des solutions de sécurité basées sur IEEE 802.11i pose de nombreux problèmes des problèmes d'interopérabilité entre les divers fournisseurs d'équipements.

Pour combler les lacunes sécuritaires des réseaux Wi-Fi, nombre de fournisseurs ont doté leurs équipements de compléments, souvent sous forme de cartes ou de points d'accès en vente chez eux. Cette dépendance vis-à-vis des fournisseurs vaut également pour les architectures des nouveaux réseaux locaux sans fil (WLAN), qui utilisent des contrôleurs centralisés pour la coordination et la gestion des points d'accès. Ceux-ci comprennent généralement des fonctions de sécurité permettant, entre autres, la détection de points d'accès incontrôlables et la fourniture d'extrémités de tunnel VPN. Toutefois, les avantages sécuritaires de ces architectures ne profitent qu'aux nœuds de WLAN directement connectés, à l'exclusion des autres connexions, de type Ethernet ou WLAN, établies dans les lieux publics ou au domicile des employés.

### ***Problèmes posés par les réseaux cellulaires***

Les problèmes sécuritaires liés aux connexions cellulaires diffèrent quelque peu de ceux des réseaux Wi-Fi. Ainsi, alors que les attaques contre les réseaux Wi-Fi nécessitent un matériel Wi-Fi ordinaire, celles dirigées contre le réseau cellulaire ont lieu à l'aide d'un dispositif spécial de réception et de décodage des radiosignaux. Cependant, le prix de cet équipement n'est pas suffisamment dissuasif. Conséquence, certains réseaux cellulaires recourent au chiffrement de la liaison radio. Ils emploient généralement les technologies 3 G, dont la génération la plus récente offre un puissant cryptage à l'aide d'algorithmes comme Kasumi et AES. Néanmoins, si ces réseaux venaient à se multiplier, ils continueraient probablement à utiliser la technologie de génération antérieure pour la couverture des zones à faible densité démographique (où le cryptage n'est pas toujours de rigueur). En outre, même si votre propre opérateur a recours au chiffrement, il se peut que la liaison transite par le réseau non chiffré d'un autre opérateur. En résumé, la sécurité de la liaison radio n'est pas garantie.

Un même problème se pose pour les connexions cellulaires et les points d'accès Wi-Fi. Ceux-ci ont pour principale fonction d'offrir un accès à Internet mais, même si leurs radiosignaux sont chiffrés, le trafic IP n'est pas protégé sur Internet. Pour y remédier, certains opérateurs proposent des options de connexion arrière plus sécurisée, de leur réseau d'infrastructure au réseau du client, avec circuits de relayage de trames dédiés ou connexions VPN IPSec de réseau à réseau. Cependant, ces aménagements induisent des coûts supplémentaires, comprenant les frais de mise en place du réseau et une contribution mensuelle.

### ***Multiplicité des connexions et des plates-formes***

Bien qu'il soit possible de mettre en œuvre des solutions spécifiques de sécurisation des connexions Wi-Fi et cellulaires, chaque solution est unique et leur gestion conjointe n'est probablement pas réalisable.

Autre sujet de préoccupation : les employés peuvent utiliser divers dispositifs, dont des ordinateurs portables ou domestiques, des téléphones hybrides, des assistants numériques et des terminaux publics. Le service informatique n'en gèrera qu'une partie ; les autres terminaux, dont les systèmes domestiques et les stations de travail publiques, risquent de compromettre la sécurité du réseau.

# Architecture sécuritaire recommandée

L'informatique nomade et sans fil a manifestement besoin d'une solution sécuritaire unique, recouvrant tous les types de connexions disponibles, notamment Wi-Fi hors/sur les lieux, cellulaires, bornes publiques, accès domestiques, etc.

Néanmoins pour pouvoir définir une architecture sécuritaire efficace, d'autres fonctions importantes de la sécurité seront probablement nécessaires, notamment :

- Prise en charge des nœuds gérés ou non et d'une vaste gamme de terminaux : ordinateurs de bureau, portables, assistants personnels et téléphones hybrides.
- Contrôle granulaire de l'accès aux ressources au lieu de la simple fourniture d'un accès réseau.
- Contrôle du nœud d'extrémité afin de vérifier la configuration logicielle (par exemple la présence d'un antivirus), de rechercher des codes dangereux sur le système et d'effacer les caches.
- Possibilité de se conformer aux lois protégeant la confidentialité des informations financières et médicales.

Les VPN SSL remplissent toutes ces conditions car ils tirent parti des navigateurs et de la couche de sécurité SSL disponibles sur la quasi totalité des plates-formes : ordinateurs portatifs, assistants personnels, téléphones hybrides... La figure 1 représente un dispositif SSL offrant tous les types d'accès sans fil et l'acheminement du trafic IP via un tunnel SSL.

## [[Graph Page 5]]

**Un VPN SSL fournit des accès distants internes et externes.**

Cellular Data Network	Réseau cellulaire
Wireless Hotspot	Point d'accès sans fil
Home Network	Réseau domestique
Internet	Internet
Firewall	Pare-feu
Aventail Appliance	Boîtier Aventail
Enterprise Access Points	Points d'accès de l'entreprise
Enterprise Resources	Ressources de l'entreprise
Application	Application
NON SSL	Non SSL
SSL	SSL
TCP	TCP
IP	IP
Layers 1,2	Couches 1, 2
Redirection of IP traffic into SSL Tunnel	Réacheminement du trafic IP via un tunnel SSL

## Modèle de sécurité inversée

Les architectures sécuritaires traditionnelles reposent sur la notion de périmètre, au sein duquel des pare-feu s'interposent entre réseaux externes non sécurisés et réseaux internes sécurisés. Ce modèle ne fonctionne pas si un pourcentage important de vos employés utilise des réseaux publics ou si vous souhaitez offrir un accès limité à des entrepreneurs, à des partenaires commerciaux ou à des clients.

Dans le modèle de sécurité inversée, aucun nœud (externe ou interne) n'est supposé sûr, mais l'accent est mis sur l'identité granulaire et la gestion des accès. Les VPN SSL appliquent ce modèle en assurant un puissant contrôle des extrémités, une forte authentification de l'utilisateur, l'accès aux ressources prédéfinies, l'intégrité des données, la non-répudiation et un audit détaillé. En limitant l'accès au niveau de la couche application, les VPN SSL déplacent la gestion de la sécurité du réseau vers l'utilisateur.

## VPN SSL et autres approches

Selon Forrester Research<sup>1</sup>, les VPN SSL sont en passe de dominer le marché des solutions d'accès à distance : "En revigorant la mobilité et l'accès distant sécurisé, les VPN SSL vont connaître un essor significatif car les fournisseurs et opérateurs voudront améliorer leurs offres. Cette croissance va se poursuivre et selon les prévisions des analystes, les VPN SSL devraient dominer le marché en 2008." En attendant, la connexion sans fil devient le mode d'accès distant privilégié.

Les atouts des VPN SSL sont évidents : sécurité et confidentialité éprouvées de la transmission des données, multiples méthodes d'authentification des utilisateurs, contrôle des applications accessibles, souplesse accrue à l'égard des types de plates-formes utilisées, possibilité de sécuriser toutes les connexions, qu'elles soient internes ou externes, ce qui les met totalement à l'abri des risques inhérents aux réseaux sans fil.

Les VPN IPSec continueront d'être utilisés, mais ils conviennent davantage aux connexions de réseau à réseau. D'autres approches sécuritaires des réseaux sans fil prennent la forme de solutions diverses, spécifiques aux applications, comme RIM Blackberry. Elles sont hautement optimisées pour certaines applications, par exemple de type "push e-mail », synchronisation des agendas et d'autres solutions mobiles. Toutefois, ces solutions ne sont pas universelles comme les VPN SSL. Dans certains cas, votre VPN SSL rendra inutiles d'autres solutions de sécurité de plates-formes mobiles, pour d'autres, il sera possible de combiner les deux approches. Le tableau 1 résume les caractéristiques des diverses approches sécuritaires.

**Tableau 1 : Avantages et inconvénients des différentes approches sécuritaires**

Type de solution sécuritaire	Avantages	Inconvénients
<b>Norme IEEE 802.11i</b>	Standard sécuritaire complet des connexions Wi-Fi.	Disponible uniquement dans les configurations d'entreprises. Ne gère pas les autres connexions sans fil telles les connexions cellulaires. Ne prend pas en charge le matériel obsolète. Problèmes d'interopérabilité entre fournisseurs.

<sup>1</sup> Forrester Research, "SSL Is The Future Of Remote Access VPNs", juin 2004

Type de solution sécuritaire	Avantages	Inconvénients
<b>Mécanismes de sécurité des réseaux cellulaires</b>	Principalement conçus pour protéger l'opérateur contre un usage frauduleux. De nombreux réseaux - mais pas tous - chiffrent la liaison radio.	Solution partielle de sécurité, valable uniquement si l'opérateur assure le chiffrement des données.  Dans les configurations normales, les données sont transmises en clair sur Internet.  Ne gère pas les autres connexions sans fil telles les connexions Wi-Fi.
<b>VPN IPSec</b>	Une solution en pleine maturité, disponible chez de nombreux fournisseurs.	Nécessite un code client.  Elle n'est pas nécessairement disponible pour toutes les plates-formes mobiles.  Fonctionnement optimal avec l'accès réseau et non avec un accès au niveau de l'application.
<b>VPN pour communications sans fil</b>	Fonctionne avec les réseaux sans fil.	Spécifique au réseau sans fil, il ne constitue pas un cadre sécuritaire complet pour l'entreprise.
<b>Solutions spécifiques aux applications (ex. messagerie électronique sans fil)</b>	Fonctionne avec les réseaux sans fil.  Limite l'accès à certaines ressources.	Nécessite un code client.  Elle convient aux petites applications comme la messagerie électronique, la synchronisation d'agendas et les bases de contacts.  Il ne s'agit pas d'une solution universelle d'accès à distance.
<b>VPN SSL</b>	Fonctionne avec les réseaux sans fil.  Des fonctionnalités améliorées comme les sessions persistantes permettent de résoudre les problèmes inhérents aux connexions sans fil.  Sécurise toutes les formes de connexions : réseaux WLAN, cellulaires et autres.  Assure le plus haut degré de contrôle de l'accès aux ressources.  Flexibilité maximum : navigateur sans client, navigateur avec code d'agent et version complète avec client.	Il n'est pas aussi couramment employé que les VPN IPSec.  Le marché est en évolution.

## Fonctionnalités des VPN SSL d'Aventail

Leaders du marché, les solutions de VPN SSL d'Aventail offrent toute une gamme d'options d'accès. Les utilisateurs bénéficient d'un accès universel sécurisé aux applications en fonction du niveau de confiance attribué aux terminaux reliés à Internet : des postes de travail publics aux ordinateurs gérés par l'entreprise. En fournissant des méthodes d'accès à large bande, la prise en charge de diverses plates-formes, la gestion granulaire des règles, avec protection et correction avancée des données, Aventail permet aux entreprises d'étendre l'accès sécurisé à davantage d'applications et de ressources tout en utilisant un plus grand nombre de méthodes de réseautage (comme les réseaux sans fil), pour un coût d'acquisition réduit.

Les VPN SSL éprouvés d'Aventail ajoutent une couche de sécurité et de contrôle à l'architecture sans fil. Un boîtier VPN SSL Aventail crée une passerelle sécurisée entre votre réseau sans fil ou un autre réseau d'accès à distance et votre réseau interne. Il assure un robuste cryptage SSL, un contrôle de l'accès au niveau de l'utilisateur, ainsi qu'une authentification stricte de ce dernier, notamment par le biais de jetons RSA SecurID et de certificats numériques.

Les VPN SSL d'Aventail fonctionnent sur n'importe quel réseau IP, y compris sur les réseaux Wi-Fi et cellulaire. En créant une connexion SSL chiffrée et authentifiée au niveau de la couche application du protocole réseau, Aventail sécurise votre réseau indépendamment de la connexion sans fil établie au niveau de la couche liaison et même en cas de désactivation de toutes les fonctions de sécurité Wi-Fi intégrées au niveau des points d'accès. Ce cas de figure peut se présenter si la session est ouverte du domicile d'un employé ou d'un point d'accès sans fil public.

Les VPN SSL d'Aventail offrent un contrôle d'accès granulaire aux administrateurs et un accès transparent aux utilisateurs autorisés. Protéger votre système de noms de domaines (DNS) interne et la topologie du réseau vis-à-vis des utilisateurs sans fil réduit les risques d'accès non autorisé ou d'attaques contre vos ressources réseau. Le contrôle d'accès granulaire vous permet de limiter l'accès en fonction de paramètres comme la source (adresse IP ou nom d'hôte) et le port, la destination, l'identité de l'utilisateur et/ou l'affiliation à un groupe, l'heure et l'intervalle, le jour et/ou la date, l'application et/ou le service, la méthode d'authentification et/ou l'algorithme de chiffrement et l'accès au niveau de l'URL. C'est précisément cette protection supplémentaire de votre réseau câblé qui garantit la sécurité de l'accès distant au réseau d'entreprise.

Pour une protection plus complète, Aventail collabore avec plusieurs organisations d'évaluation des vulnérabilités afin de mener un contrôle proactif de la sécurité de votre réseau et de vos applications et, ainsi, améliorer la protection de vos informations sensibles.

Parmi les fonctionnalités et technologies supplémentaires intégrées aux VPN Smart SSL d'Aventail, mentionnons Aventail<sup>®</sup> Smart Access<sup>™</sup>, Smart Tunneling, End Point Control et l'intégration à l'infrastructure existante de gestion de la sécurité.

## **Aventail Smart Access**

Aventail Smart Access détermine et déploie automatiquement la méthode appropriée d'accès distant aux ressources, de sorte que vos utilisateurs n'auront pas à s'en préoccuper. Grâce au contrôle d'accès granulaire, à la fonction de séparation des flux, à l'option "NAT Traversal" et au franchissement de pare-feu, Aventail permet de gérer tous les cas de figures et offre un véritable accès universel sécurisé. De plus, en utilisant la technologie Smart Tunneling d'Aventail, les VPN Smart SSL d'Aventail étendent l'accessibilité des applications, car ils prennent également en charge les protocoles UDP, TCP et IP ainsi que les applications connectées en arrière-plan telles que les applications VoIP.

La flexibilité de l'accès repose notamment sur :

- Aventail<sup>®</sup> WorkPlace : à travers son portail sécurisé, basé sur des règles et personnalisable, Aventail fournit aux utilisateurs un accès sécurisé et sans client aux applications internes Web, client/serveur et de partage des fichiers. Aventail Smart Access détermine et déploie automatiquement la méthode d'accès la plus appropriée, de manière transparente pour l'utilisateur final. Si, un utilisateur souhaite accéder à des applications client léger telles Citrix ou à des applications client/serveur comme Microsoft Exchange, SAP ou Lotus Notes, Smart Access déploie automatiquement le client Aventail<sup>®</sup> OnDemand<sup>™</sup> sur le terminal utilisé, dispensant ainsi l'utilisateur de le télécharger manuellement ou de toute autre opération.
- Aventail<sup>®</sup> Connect<sup>™</sup> : téléchargeable, ce client Microsoft Windows offre aux utilisateurs autorisés un accès sécurisé à toutes les ressources du réseau local de l'entreprise (LAN). Bien qu'il nécessite un téléchargement initial, Aventail Connect n'est pas un client VPN traditionnel. Comme avec Aventail WorkPlace, les utilisateurs ont l'impression d'être au bureau, mais ils bénéficient d'un surcroît de transparence et de simplicité. Ils jouissent ainsi d'une mobilité illimitée et d'une intégration complète au bureau Windows.

Aventail Smart Access et Aventail Unified Policy fonctionnent de concert, d'où la gestion centralisée de l'ensemble des méthodes d'accès et ressources. Les sessions persistantes figurent parmi les autres fonctions d'Aventail Smart Access. Particulièrement utiles dans les

environnements mobiles et sans fil, elles permettent à l'utilisateur de passer d'une méthode d'accès à l'autre sans se déconnecter du réseau.

## ***Aventail Smart Tunneling***

Grâce à la technologie Aventail Smart Tunneling, des tunnels de réseau IP complets peuvent utiliser le protocole SSL. Les VPN SSL d'Aventail offrent ainsi davantage de possibilités et de performances par rapport à la plupart des VPN SSL présents sur le marché. En outre, Smart Tunneling permet à toutes les applications de fonctionner, ce qui constitue un progrès par rapport aux précédents VPN SSL.

Aventail Smart Tunneling assure un accès contrôlé direct aux applications, les règles d'accès (définies par le système de gestion des règles) déterminant l'ouverture du tunnel. Dans les autres modèles de sécurité, les tunnels restent ouverts en permanence, tandis qu'avec Aventail Smart Tunneling, ils demeurent fermés jusqu'à leur ouverture dynamique pour une application donnée, en fonction des règles d'accès et de la sécurité du terminal d'extrémité.

La technologie Aventail interroge l'extrémité pour recueillir des informations essentielles concernant l'adresse IP et les données de routage utilisées par le réseau d'accès concerné. Puis, elle détecte et résout les éventuels conflits et attribue les adresses IP en conséquence. Ensuite, Aventail Smart Tunneling achemine les paquets IP en toute transparence, sans interférences ni conflits d'adresse.

Contrairement à d'autres solutions VPN SSL, Aventail Smart Tunneling n'utilise pas le protocole PPP. Les tunnels PPP ne disposent pas d'un accès absolu au réseau et sont confrontés à des problèmes d'adressage IP. Avec d'autres approches, telles IPSec, les règles et contrôles de sécurité s'avèrent difficiles à définir et ne permettent pas une authentification rigoureuse.

Contrairement aux solutions IPSec, la technologie Aventail Smart Tunneling offre l'avantage du franchissement de pare-feu et de la solution NAT Traversal ainsi que celui de la gestion granulaire des règles.

Les clients Aventail OnDemand et Aventail Connect, décrits précédemment, sont également disponibles avec Smart Tunneling.

## ***Aventail End Point Control***

Les vulnérabilités de Windows et l'absence de sécurité des réseaux sans fil augmentent les risques de brèche sécuritaire, sauf si les paramètres de réseautage et de partage sont correctement configurés. Les bornes publiques connectées aux réseaux locaux sans fil (WLAN) sont particulièrement exposées.

Avec Aventail End Point Control (EPC), vous bénéficiez désormais de la meilleure application des règles disponibles sur les VPN SSL. L'EPC permet d'appliquer les règles en fonction du niveau de confiance attribué à l'environnement (câblé ou non) de l'utilisateur et à ce dernier. En recourant à la technologie Aventail pour gérer l'accès selon l'environnement et à celle des partenaires d'Aventail pour sécuriser ces environnements, vous pourrez fournir un accès universel véritablement sécurisé sur n'importe quel type de réseau.

Aventail EPC offre la possibilité de définir une règle de contrôle d'accès hautement granulaire, qui ne se résume pas uniquement à une autorisation ou à une interdiction, mais attribue divers niveaux d'accès en fonction de l'environnement de l'utilisateur. Le composant Policy Zones permet de créer jusqu'à 10 zones de confiance adaptées à une multitude de scénarios d'accès à distance. Les partenaires d'Aventail mettent en œuvre les règles de pare-feu, de détection des intrusions, d'antivirus et d'autres règles relatives à la sécurité côté client, tandis qu'Aventail code et autorise l'accès à toutes les ressources de l'entreprise par le biais de règles de contrôle d'accès dépendant de l'identité de l'utilisateur et de la sécurité de son environnement.

## ***Intégration à l'infrastructure existante de gestion de la sécurité***

Aventail Unified Policy centralise l'administration au moyen d'un jeu de règles uniques pour l'ensemble des ressources et des méthodes d'accès. Les VPN Smart SSL d'Aventail s'intègrent

facilement à l'infrastructure sécuritaire existante, notamment aux systèmes d'authentification et d'autorisation tels RADIUS, LDAP, Active Directory, aux certificats numériques, et à l'authentification à deux facteurs (ex. jetons RSA SecurID ou autres). En résumé, en exploitant les composants d'annuaire et de sécurité probablement utilisés par vos utilisateurs distants, vous ferez l'économie de la formation et de l'assistance des utilisateurs finaux, réduirez vos coûts d'administration et de gestion et éviterez bien des tracas au service informatique.

En déployant le VPN Smart SSL d'Aventail, vous pourrez immédiatement renforcer la sécurité de vos connexions sans fil et vous affranchir de votre fournisseur. Les solutions VPN SSL d'Aventail fonctionnent sur tous les réseaux sans fil car elles font appel à une seule infrastructure intégrée, qui sécurise vos connexions sans fil ainsi que tous les réseaux auxquels vos employés, partenaires commerciaux et clients seront susceptibles d'accéder. Avec Aventail, vous disposerez d'une solution sans client, adaptée à l'entreprise, offrant un accès universel aisé et sécurisé à des applications plus nombreuses, à partir d'un plus grand nombre d'endroits, dont des environnements vulnérables comme les points d'accès Wi-Fi.

## Conclusion

Malgré les avancées significatives des technologies Wi-Fi en matière de sécurité, quantité de fonctionnalités ne sont disponibles qu'à partir d'équipements récents et d'une infrastructure gérée par un service informatique. Les réseaux cellulaires, quant à eux, reposent sur une architecture sécuritaire totalement distincte, qui met l'accent sur la protection de la liaison radio et n'assure pas de chiffrement de bout en bout.

En utilisant un VPN SSL, vous serez en mesure de sécuriser toutes les formes de communications sans fil, aussi bien en interne qu'en externe. En outre, cette approche convient à une grande variété d'équipements d'utilisateurs. Les VPN SSL d'Aventail présentent des avantages significatifs : utilisation de la quasi totalité des applications de réseautage via Smart Tunneling, haut degré de contrôle de l'équipement de l'utilisateur grâce à End Point Control, et gestion et intégration efficaces aux infrastructures de gestion existante de la sécurité via Aventail Unified Policy.

Les VPN SSL d'Aventail ne présentent pas seulement un avantage indiscutable en terme de sécurité des connexions sans fil, ils jettent aussi les bases d'une entreprise étendue, reposant sur un modèle de sécurité inversée, dans laquelle l'architecture sécuritaire assure un contrôle central de l'accès des utilisateurs et fournit un accès granulaire aux ressources. Flexible, le réseau ainsi mis en place est accessible aux employés comme aux partenaires commerciaux et permet à l'entreprise d'atteindre une rentabilité et une compétitivité optimales.

## 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](http://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.