



## GUIDE D'ÉVALUATION DES PRODUITS

### Fournisseurs

#### – sécurité sans fil

L'équipe Insight Technology Assessment Services (TAS) a évalué les produits de sécurité sans fil provenant des fournisseurs suivants :

- Bluefire
- Bluesocket
- CREDANT Technologies
- Good Technology
- NetMotion Wireless
- Symantec
- Trend Micro
- Trust Digital
- Vernier Networks

### SÉCURISATION DE LA MOBILITÉ AU SEIN DE L'ENTREPRISE

Après un début incertain, la technologie LAN sans fil est en train de gagner un accueil plus favorable qu'auparavant au milieu du travail. Au début, les entreprises ont agi avec beaucoup de lenteur pour adopter des initiatives sans fil à cause des problèmes de sécurité en raison des failles WEP (Wired Equivalency Protocol) qui fournissaient une protection inadéquate. Dans le but de surmonter cette hésitation, plusieurs fournisseurs offrent présentement des produits qui peuvent sécuriser votre réseau sans fil tout en fournissant un réseau privé virtuel de bout en bout à partir d'un portable à distance jusqu'au réseau. Ces commutateurs peuvent loger au front de votre réseau ou être centralisés dans vos armoires de répartition, tout en s'assurant de fournir un point de raccordement aux télétravailleurs.

Les nouvelles solutions liées à la sécurité mobile répondent aux points faibles WEP directement, tout en fournissant l'authentification sécurisée, l'autorisation et le chiffrement. C'est un moyen facile de centraliser la gestion d'un grand nombre de points d'accès, ce qui simplifiera votre WLAN par l'élimination de plusieurs points de raccordement, afin que vous puissiez contrôler l'usage de bande passante et surveiller la performance de votre réseau. L'itinérance et la persistance de session permettent aux utilisateurs de circuler librement de réseau en réseau sans perdre la connectivité de session.

### CONSIDÉRATIONS CLÉ

#### Infrastructure

Le développement d'une politique sensée touchant la sécurité est l'une des plus importantes étapes. Les points d'accès sauvages existent déjà, et si votre entreprise n'a pas encore mis en place un plan adéquat à cet effet, il est fort probable que vous risquez de perdre le contrôle de votre réseau. Et lorsque vous songez à sélectionner une solution liée à la sécurité mobile, prenez note de quelques éléments importants :

- **Sélection des points d'accès** - Choisissez les points d'accès 802.11 (catégorie d'entreprise) qui sauront soutenir vos standards et protocoles.
  - Si vous utilisez le protocole d'authentification 802.1x, il faudra s'assurer que les points d'accès le soutiennent.
  - Le soutien d'alimentation par câble Ethernet (POE – Power over Ethernet) élimine le besoin d'installation électrique à chaque emplacement de point d'accès, et cela peut se traduire par des économies. Renseignez-vous si le point d'accès sélectionné peut soutenir l'alimentation par câble Ethernet (POE).
  - Les points d'accès avec antenne haut de gamme fourniront des signaux puissants et cela vous aidera à empêcher des fuites en dehors de la zone de couverture désirée.
- **Compatibilité de base des données** - Cherchez une solution qui saura utiliser votre base de données d'authentification actuelle (par exemple, RADIUS, LDAP, etc.), car cela signifie que vous n'aurez pas besoin de créer et de maintenir des bases de données séparées.
- **Politiques qui s'appliquent aux utilisateurs** - Déterminer les personnes qui auront besoin de l'accès sans fil et le degré d'accès relatif (spécifier l'endroit d'accès). Traitez votre WLAN comme un réseau non sécurisé, et semblable à un réseau « accès distant »
- **Chiffrement des données** - Si les utilisateurs ont besoin de l'accès LAN à partir des emplacements sensibles (cafés, restaurants) il faudra utiliser une solution VPN pour chiffrer les données de bout en bout.

Insight®



- **Authentification** - Si vous utilisez l'authentification 802.1x, il faudra établir laquelle des méthodes d'authentification s'adapte à votre situation. Si vous disposez d'une infrastructure PKI à l'heure actuelle, peut être que la meilleure solution serait d'opter pour EAP-TLS. Autrement, il faut considérer PEAP ou EAP-TTLS, qui sont toujours sécuritaires.
- **Variabilité dimensionnelle** - Il faut s'assurer que votre solution puisse être extensible vers un réseau plus étendu, au besoin.

## FONCTIONNALITÉS CLÉ

Afin de s'assurer que vous connaissez la fonctionnalité dont vous avez besoin, il faudra effectuer une analyse complète de votre infrastructure. Les fonctionnalités inutiles pourront générer des frais de licences indésirables, ou des coûts indirects liés à votre réseau, tandis qu'une solution qui manque les fonctionnalités critiques ne saura pas limiter les risques auxquels s'expose votre organisation.

- **Gestion centralisée aux points d'accès** - Gestion et application des politiques à distance vers des points d'accès répartis.
- **Itinérance et persistance de session** - Transfert d'un client sans fil à partir d'un réseau à un autre, sans arrêter la connectivité.
- **Classe de service** - Réduire l'usage de bande passante et éviter qu'un seul utilisateur utilise la bande disponible en entier
- **Soutien – basculement de passerelle** - La garantie que votre réseau sans fil peut fournir du temps utilisable à 100% par l'entremise d'un commutateur de secours, selon le cas.
- **Soutien 802.1x** - Assure l'authentification mutuelle et sécurisée entre le client et un point d'accès.
- **Réseau privé virtuel** - Sessions chiffrées et sécurisées de bout en bout par rapport à des réseaux non sécurisés.
- **Équilibrage de charge** - Distribution des charges de session à travers plusieurs serveurs tout en s'assurant d'une performance parfaite pendant les sessions.
- **Basculement** - S'assurer que les sessions puissent continuer à fonctionner à partir d'un autre serveur, même s'il s'agit d'une panne.
- **Regroupement (mise en commun) de serveurs** - Gestion de plusieurs contrôleurs sans fil à partir d'un seul serveur logique.

## CONCLUSION

Les commutateurs à accès sans fil fournissent la sécurité essentielle du déploiement sans fil LAN et en même temps, sauront résoudre les problématiques antérieures relatives. Ces produits sauront prouver qu'avec une politique de sécurité sans fil solide, une sélection soignée et la détermination des emplacements de vos points accès, une solution appropriée en matière de sécurité pour les systèmes sans fil et la mise en œuvre d'un réseau 802.11, tous ces éléments pourront faire partie d'une initiative réussie pour faire bénéficier votre département TI, ou en d'autres mots, pour leur tranquillité d'esprit.

Nos directeurs de comptes spécialisés pourront s'entretenir à propos de vos besoins en matière de sécurité mobile, et notre soutien à la clientèle saura fournir les ressources techniques selon vos besoins. Et lorsque vous faites face à un éventail de problèmes qui peuvent survenir en raison de vos efforts pour sécuriser le réseau sans fil de votre organisation, Insight peut être d'une valeur inestimable.

**Pour de plus amples renseignements veuillez contacter votre directeur de comptes ou l'équipe du Service d'évaluation technologique d'Insight au [tas@insight.com](mailto:tas@insight.com)**

Insight et le logo d'Insight sont des marques déposées d'Insight Direct USA, Inc. Toute autre marque déposée, marque enregistrée, photos, logos et illustrations demeurent la propriété de leurs propriétaires respectifs. ©2007 Insight® Direct USA, Inc. Tous droits réservés.