

netopia®

**La Sécurité Simplifiée
pour les Réseaux Sans Fil
des Petites Entreprises et
des Particuliers**

60 à 70 % des réseaux sans fil dans les petites entreprises et chez les particuliers ne sont pas sécurisés

La certification **WPS (Wi-Fi Protected Setup)** intègre les passerelles résidentielles et professionnelles de Netopia. Cette innovation permet de configurer un réseau Wi-Fi sécurisé chez un particulier ou dans une petite entreprise selon un processus aussi simple que de saisir un code confidentiel ou d'appuyer sur un bouton : la passerelle Netopia détecte tout nouveau périphérique Wi-Fi à portée et invite l'utilisateur à décider si ce périphérique peut ou non se connecter au réseau. Netopia commencera à déployer la certification WPS sur ses passerelles résidentielles et professionnelles début 2007.

QUELQUES MOTS SUR LA SÉCURITÉ DES RÉSEAUX SANS FIL

La sécurité des réseaux sans fil est aussi importante pour les particuliers et les petites sociétés que pour les grandes entreprises. Si votre réseau sans fil n'est pas sécurisé, n'importe qui se trouvant dans les parages peut épier votre activité en ligne. Selon la façon dont votre réseau est configuré, quelqu'un pourrait même obtenir l'accès complet au disque dur de votre ordinateur via un réseau sans fil non sécurisé.

Sans même parler d'espionnage ou d'actes malveillants à votre rencontre, vos voisins pourraient se servir de votre connexion internet. Une telle pratique vous priverait non seulement du débit que vous payez, mais si votre voisin s'adonne à des activités illégales en ligne, les autorités pourraient remonter jusqu'à votre réseau. On estime que 60 à 70 % des réseaux sans fil dans les petites entreprises et chez les particuliers ne sont pas sécurisés. Or, les études montrent que si vous avez une connexion sans fil non sécurisée, les probabilités que votre réseau soit exploité sont plutôt élevées.

POURQUOI Y A-T-IL TELLEMENT DE RÉSEAUX SANS FIL NON SÉCURISÉS ?

La technologie permettant de sécuriser les réseaux des petites entreprises et des particuliers existe depuis un certain temps. Les premières solutions sécurisaient le réseau mais pouvaient être facilement contournées à cause des limites des technologies de cryptage, comme dans le cas du WEP

(Wired Equivalent Privacy). Le cryptage WEP était censé offrir une confidentialité comparable à celle des réseaux filaires traditionnels. Toutefois, cette technologie posait quelques problèmes. L'installation, le paramétrage et la configuration étaient très compliqués pour la plupart des utilisateurs, ce qui signifiait que la majorité d'entre eux ne l'installaient pas du tout ou pas correctement. Pour les réseaux où le cryptage WEP était convenablement installé, une faille très sérieuse a été identifiée : n'importe quelle clé WEP peut être piratée en moins de deux minutes à l'aide de logiciels très faciles à se procurer. Un grave problème !

ACCÈS WI-FI PROTÉGÉ (WPA ET WPA2)

Une alternative au cryptage WEP a été proposée par le mécanisme WPA (Wi-Fi Protected Access) en 2003, puis par la norme IEE 802.11i (également connue sous le nom de WPA2) en 2004. Le Wi-Fi Protected Access (WPA et WPA2) est une catégorie de systèmes permettant de sécuriser les réseaux informatiques sans fil. Il a été créé suite à l'identification par les chercheurs de graves failles dans le système (WEP). Le Wi-Fi Protected Access est une spécification d'améliorations de la sécurité interopérables et basées sur des normes, ce qui augmente considérablement le niveau de protection des données (cryptage) et de contrôle d'accès (authentification) pour les réseaux locaux sans fil Wi-Fi existants et futurs. L'effort a également été motivé par la nécessité d'améliorer la sécurité Wi-Fi en rendant possible la mise à niveau logicielle des produits certifiés Wi-Fi qui existent aujourd'hui.

Le WPA est une version modifiée du cryptage WEP qui modifie la clé régulièrement. Il est beaucoup plus sécurisé que le cryptage WEP. Depuis sept. 2003, tous les nouveaux équipements 802.11b et g testés pour la certification Wi-Fi doivent implémenter le mécanisme WPA, ce qui explique pourquoi il est relativement répandu. Le WPA implémente la majeure partie de la norme IEE 802.11i et a été créé comme une mesure intermédiaire visant à prendre la place du cryptage WEP. Le WPA est censé fonctionner avec toutes les cartes d'interface sans fil, mais pas forcément avec les points d'accès sans fil de première génération.

43 % des utilisateurs sans fil trouvent que l'installation de mécanismes de sécurité sur un réseau Wi-Fi domestique est moyennement à très difficile

Le Wi-Fi Protected Access est un mécanisme de sécurité sans fil très puissant. Si aucune solution de sécurité ne peut se targuer d'être totalement sûre, la protection offerte par le WPA est relativement élevée. De nombreux cryptographes assurent que le WPA pare toutes les attaques connues contre le cryptage WEP. De plus, il ajoute l'authentification des utilisateurs, qui était absente du WEP.

Le WPA2 est une implémentation de seconde génération, basée sur une nouvelle technologie de cryptage. Le mécanisme WPA initial utilisait le cryptage WEP, amélioré par des changements de clé fréquents. Pour sa part, le WPA2 est basé sur une nouvelle technologie de cryptage : l'AES (Advanced Encryption Standard). La certification WPA2 est en vigueur depuis septembre 2004. Depuis le 13 mars 2006, tous les équipements utilisant la dénomination Wi-Fi doivent être certifiés WPA2. Cette protection implémente la norme IEEE 802.11i dans son intégralité.

Le WPA et le WPA2 comportent un mode spécial destiné aux petites entreprises et aux particuliers qui n'auront pas accès aux serveurs réseau. Dans ce mode, l'utilisateur saisit manuellement le mot de passe de démarrage pour activer le Wi-Fi Protected Access.

Dans le mode de fonctionnement dédié aux entreprises, l'authentification est réalisée via la norme 802.1X et le protocole EAP. Le mode "personnel" (pour les petites entreprises et les particuliers) ne nécessite qu'un point d'accès et un périphérique client, tandis que le mode "entreprise" requiert généralement un serveur RADIUS ou tout autre serveur d'authentification sur le réseau.

LA CONFIGURATION POUR LE WPA ET LE WPA2 RESTE TRÈS COMPLIQUÉE

De nombreux particuliers et professionnels en petites entreprises trouvent que l'installation, le paramétrage et la configuration d'un réseau sans fil sont très compliqués. Une étude récente montre que 43 % des utilisateurs de Wi-Fi trouvent que l'installation de mécanismes de sécurité sur un réseau Wi-Fi domestique est moyennement

à très difficile (Wi-Fi Alliance/Kelton Research, 2006).

Les produits Wi-Fi actuels ne facilitent pas toujours les choses, la configuration de leurs fonctionnalités de sécurité pouvant s'avérer lente et peu intuitive. Par exemple, pour utiliser la protection WPA Wi-Fi avec Windows XP, vous devez appliquer manuellement un correctif logiciel aux clients sans fil Windows XP, avant de vous assurer que vos points d'accès sans fil et adaptateurs réseau sont correctement configurés.

Suivez les instructions ci-après pour paramétrer le mécanisme WPA sur les réseaux Wi-Fi composés de clients Windows XP :

1. Lisez la Présentation de la mise à jour de sécurité sans fil WPA dans Windows XP (base de connaissances Microsoft, article Q815485).
2. Vérifiez que chaque client Windows XP exécute le Service Pack 1 (SP1) de Windows XP ou ultérieur.
3. Sur chaque client Windows XP, vérifiez que l'adaptateur réseau du client est compatible avec le service Wireless Zero Configuration (WZC). Consultez la documentation livrée avec l'adaptateur ou le site web du fabricant, ou contactez l'assistance téléphonique appropriée pour plus d'informations. Mettez à niveau le pilote de l'adaptateur réseau et le logiciel de configuration pour ajouter la prise en charge de WZC sur les clients qui en ont besoin.
4. Pour chaque client Windows XP, téléchargez et installez le correctif logiciel Windows XP pour WPA, en suivant les instructions fournies.
5. Apportez les modifications nécessaires aux points d'accès sans fil, comme indiqué dans l'article référencé à l'étape 1.
6. Apportez les modifications nécessaires aux adaptateurs réseau sans fil, comme indiqué dans l'article référencé à l'étape 1.

LA SOLUTION POUR SÉCURISER LES RÉSEAUX SANS FIL PLUS SIMPLE- MENT : WI-FI PROTECTED SETUP (WPS)

Le WPS sert à faciliter l'installation et l'activation des fonctionnalités de sécurité sur un réseau afin d'améliorer l'expérience des utilisateurs avec un réseau Wi-Fi domestique. Il possède toutes les fonctionnalités de sécurité évoluées offertes par les mécanismes WPA et WPA2 et est conçu pour accélérer et simplifier l'installation et l'activation des fonctionnalités de sécurité sur un réseau Wi-Fi.

"Comme la technologie Wi-Fi intègre un éventail de plus en plus large de produits électroniques grand public, la convivialité est plus importante que jamais", explique Frank Hanzlik, directeur de la Wi-Fi Alliance. "La Wi-Fi Alliance continuera de jouer un rôle central dans l'amélioration de l'expérience pour les utilisateurs".

La certification WPS rejoindra le portefeuille de certifications disponibles aux membres de la Wi-Fi Alliance qui fabriquent une grande variété d'appareils, allant des PC et imprimantes aux téléviseurs, appareils photo et consoles de jeu.

Le système WPS permettra aux consommateurs d'activer un cryptage WPA renforcé sur leurs réseaux en quelques clics seulement. Plus besoin d'inventer des phrases secrètes compliquées à retenir. Terminées les longues séquences de caractères hexadécimaux à saisir. Plus de "C'est trop compliqué".

Le WPS a été conçu pour faciliter la configuration des réseaux Wi-Fi protégés par des mécanismes de sécurité dans les environnements des particuliers et des petites entreprises. Il prend en charge des méthodes qui sont connues de la plupart des consommateurs pour configurer un réseau et activer la sécurité, comme appuyer sur un bouton ou saisir un code confidentiel. Le nouveau système, qui sera incorporé dans Windows Vista, fonctionnera avec les ordinateurs, les passerelles, les périphériques et les produits électroniques grand public. L'idée est d'initier un mode WPS sur une passerelle, puis de saisir une simple suite de chiffres (comme un code secret), d'appuyer sur un bouton ou d'utiliser une méthode tout aussi simple pour démarrer un échange de clés sécurisé afin d'extraire la clé WPA. Pour plus de sécurité, les appareils pourront également produire la clé WPA sous-jacente. Par le passé, on a souvent évoqué la possibilité de transférer cette clé sur un périphérique USB, par exemple, afin de permettre l'échange de clés via le matériel plutôt que sans fil.

Le WPS est une spécification non propriétaire qui s'intégrera parfaitement dans l'univers hétérogène du Wi-Fi et sera une technologie certifiée contrôlée par la Wi-Fi Alliance. Ainsi, n'importe quel périphérique utilisant l'appellation WPS devra avoir satisfait à des tests en laboratoire. ■

En plus d'offrir les fonctions de sécurité évoluées de WPA et WPA2, WPS est conçu pour accélérer et simplifier l'installation et l'activation des fonctions de sécurité sur un réseau Wi-Fi

netopia®

Pour plus d'informations, composez le 01 45 29 91 00 ou visitez le site www.netopia.com

Copyright © 2006, Netopia, Inc. Tous droits réservés. Netopia et le design Netopia sont des marques déposées, détenues par Netopia, Inc. et enregistrées auprès du bureau américain des brevets et des marques. "Broadband Without Boundaries" et "3-D Reach" sont des marques détenues par Netopia, Inc. Toutes les autres marques citées sont la propriété de leurs détenteurs respectifs.

Netopia Europe
Tel +33 (0) 1 45 29 91 00
info@netopia.fr