



Fiche application sur la conformité PCI

Le vendredi 04 mai 2007, le pire cauchemar de tout revendeur est devenu réalité lorsque le Wall Street Journal a publié à sa une un article décrivant une intrusion dans un réseau local sans fil ayant entraîné le plus grand vol de cartes de crédit de l'histoire. Le Conseil des normes de sécurité PCI, qui regroupe les cinq premières marques de paiement (American Express, Visa, Mastercard, Discover et JCB), a publié la norme PCI DSS (Payment Card Industry Data Security Standard) pour empêcher précisément ce type d'intrusion. Le Conseil des normes de sécurité PCI oblige les revendeurs du monde entier à traiter les réseaux locaux sans fil comme des réseaux publics, à appliquer des contrôles de sécurité renforcés en tout point des réseaux locaux sans fil et à empêcher toute entrée non autorisée via le réseau local sans fil.

Le respect des règles de conformité PCI strictes s'avère toutefois coûteux et complexe. Les réseaux avec et sans fil existants doivent être réarchitecturés et réactualisés en vue d'assurer la sécurité nécessaire. Des services de sécurité complémentaires doivent être installés. La réarchitecture et la réactualisation des réseaux deviennent vite très coûteuses et déconcertantes, en particulier lorsque des modifications doivent être apportées à des centaines, voire à des milliers de magasins. Les réseaux centrés sur l'utilisateur d'Aruba proposent la seule solution de sécurité intégrée pour l'accès à distance et les réseaux locaux sans fil assurant une mise en conformité PCI facile et efficace au niveau des coûts. Aruba propose une solution de sécurité à gestion centralisée qui se superpose aux réseaux existants et qui rend tout changement d'architecture et toute réactualisation inutiles. La plate-forme d'Aruba présente par ailleurs l'avantage d'être une plate-forme d'activation d'applications. La solution utilisée pour la sécurité peut de ce fait également être utilisée pour assurer la prise en charge sécurisée des applications sans fil existantes et pour activer de nouvelles applications.

Règles PCI visant à sécuriser les réseaux locaux sans fil

Le Conseil des normes de sécurité PCI a publié une norme DSS (Data Security Standard) en mai 2006 avec entrée en vigueur au 1er janvier 2007. Il y prescrit la mise en œuvre de contrôles de sécurité spécifiques qui diffèrent selon le niveau d'utilisation des réseaux locaux sans fil.

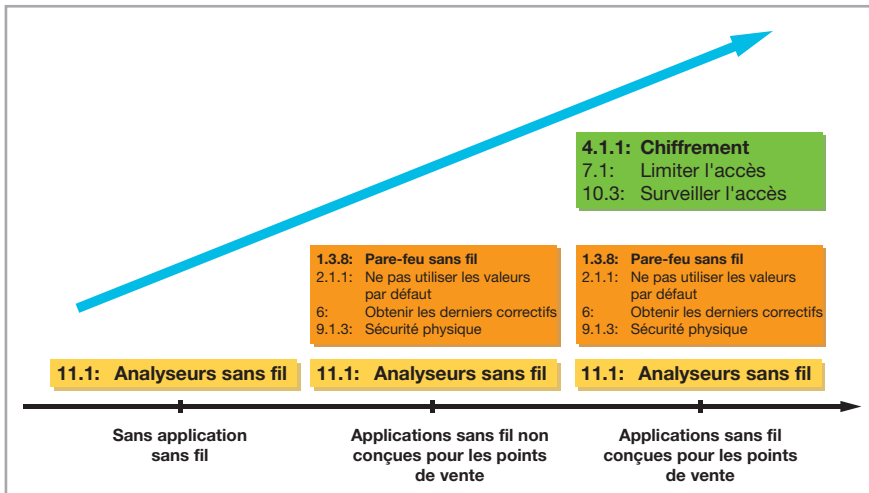
Comme indiqué dans le schéma, même si aucun réseau local sans fil n'est utilisé, les revendeurs sont tenus de mettre en œuvre des « analyseurs sans fil » pour éviter la mise en place de réseaux sans fil non autorisés ou accidentels. A l'autre extrémité du spectre, si des réseaux locaux sans fil sont utilisés pour des applications de points de vente de manière à transmettre des informations sur les cartes de crédit par les ondes, les revendeurs doivent alors mettre en œuvre un chiffrement robuste (ne répondant pas au protocole WEP), utiliser un pare-feu certifié ICASA entre les réseaux locaux sans fil et le réseau des points de vente et surveiller régulièrement les réseaux locaux sans fil.

La conformité PCI est une nécessité urgente. En premier lieu, la conformité PCI permet de sécuriser les réseaux contre les intrusions, protégeant ainsi votre marque et vos consommateurs. En second lieu, les marques de paiement ont mis en place des mesures d'incitation visant à développer et à accélérer la conformité PCI de telle sorte que vous puissiez :

- éviter des amendes pour non-conformité à hauteur de 25 000 \$ par magasin et par mois ;
- remplir les conditions requises pour pouvoir bénéficier de taux de transaction préférentiels ;
- être protégé dans le cadre de la déclaration de « règle refuge » selon laquelle les revendeurs ayant rempli leur obligation de conformité PCI ne sont pas tenus pour responsables ou n'ont pas à payer une indemnité par déclaration de vol de carte de crédit en cas d'intrusion.

Avantages:

- Permet un coût total de possession peu élevé grâce à une sécurité intégrée assurant la conformité PCI.
- Protège les réseaux avec et sans fil traditionnels grâce à une architecture hiérarchique.
- Empêche les mises à niveau des périphériques exclusivement WEP grâce à la sécurité basée sur l'identité.
- Facilite la migration vers la nouvelle génération de réseaux locaux sans fil grâce à une plate-forme multifonctionnelle.
- Est conçu pour s'adapter à un nombre élevé de points de vente distants.

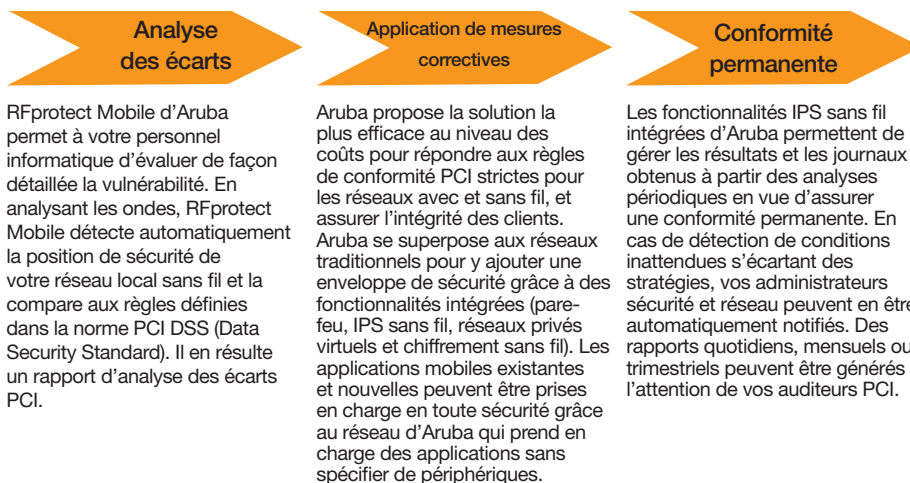


Conformité PCI proposée par Aruba

Aruba Networks est le premier à utiliser une méthode unique en son genre visant à répondre aux règles PCI avec facilité et efficacité au niveau des coûts. Grâce à une solution intégrant le contrôle de la sécurité, les réseaux avec et sans fil et l'accès à distance, les revendeurs peuvent activer le niveau de sécurité nécessaire à la conformité PCI tout en activant simultanément les applications de gestion, sans mettre à niveau les réseaux traditionnels. La solution de conformité PCI proposée par Aruba est décrite en détail à l'adresse suivante : http://www.arubanetworks.com/pdf/company/wp_PCI-Primer.pdf.

Grâce à la solution de bout en bout proposée par Aruba, votre réseau local sans fil respecte les règles de conformité PCI strictes et votre réseau est, par-dessus tout, protégé. De l'analyse des écarts visant à détecter d'éventuelles failles de sécurité à des solutions d'applications de mesures correctives en passant par la surveillance et l'audit de conformité permanent, Aruba vous protège entièrement.

SÉCURITÉ PCI SOUS FORME DE SUPERPOSITION:
 Les fonctionnalités IPS (Intrusion Protection Services) sans fil peuvent



être superposées aux réseaux sans fil existants. La solution proposée par Aruba est composée d'un surveilleur d'ondes (ou de plusieurs surveilleurs d'ondes) au niveau des magasins et d'un serveur de protection contre les intrusions sans fil au niveau du centre de données. Les contrôleurs d'ondes effectuent des analyses des réseaux avec et sans fil dans l'environnement de magasins. Des serveurs centralisés regroupent et étudient ensuite ces résultats en vue de générer des rapports d'analyse et d'assurer la conformité PCI. En cas d'événement non autorisé, les fonctionnalités IPS sans fil proposées par Aruba génèrent également des alertes et empêchent automatiquement les attaques. La solution proposée par Aruba est unique en son genre du fait que le matériel utilisé pour les fonctionnalités IPS sans fil peut également être configuré pour assurer un accès sans fil, tout en proposant une voie d'évolution facile et efficace au niveau des coûts vers la nouvelle génération de réseaux locaux sans fil.

INUTILITÉ DES MISES À NIVEAU ET DES RECONCEPTIONS DES RÉSEAUX LOCAUX CÂBLÉS:

Grâce aux fonctionnalités intégrées d'Aruba (pare-feu dynamique certifié ICASA, réseaux privés virtuels et authentification/chiffrement des réseaux locaux sans fil), les produits propres aux réseaux câblés existants (routeurs, pare-feu, etc.) n'ont pas besoin de faire l'objet d'une mise à niveau pour activer la segmentation des réseaux locaux virtuels, les fonctionnalités des réseaux privés virtuels ou les services AAA en vue d'assurer la sécurité du réseau sans fil.

SÉCURITÉ BASÉE SUR L'IDENTITÉ POUR PROTÉGER LES PÉRIPHÉRIQUES EXCLUSIVEMENT WEP:

Les rôles de sécurité basés sur l'identité d'Aruba empêchent les périphériques exclusivement WEP d'ouvrir une porte dérobée dans le centre de données. Même si le chiffrement WEP est remis en question, l'accès au réseau est limité grâce aux fonctionnalités intégrées d'Aruba (pare-feu avec état et inspection détaillée des paquets).

UNE PLATE-FORME, PLUSIEURS USAGES:

Outre ses fonctionnalités de sécurité renforcées, la solution proposée par Aruba assure une connectivité d'entreprise sécurisée aux réseaux locaux câblés, aux réseaux maillés et aux réseaux locaux sans fil pour diverses applications, notamment la prise en charge simultanée d'applications de données, de voix et de vidéo sur un même périphérique.

GESTION CENTRALISÉE: Aruba propose des options adaptées à la taille de différents magasins pouvant tous bénéficier d'une gestion centralisée en tant que réseau unique. La solution proposée par Aruba est conçue pour fonctionner en toute sécurité sur des réseaux privés et publics, jusqu'à des milliers de sites distants, l'ensemble des stratégies de sécurité étant définies et suivies de façon centralisée.



WWW.ARUBANETWORKS.COM

1322 Crossman Avenue. Sunnyvale, CA 94089, États-Unis | Tel. +1 408.227.4500 | Fax.

+1 408.227.4550