



Mobilité sécurisée pour les réseaux locaux sans fil propriétaires

Solution de mobilité sécurisée d'Aruba pour les réseaux locaux sans fil propriétaires

Un grand nombre d'organisations visionnaires ont reconnu les avantages des réseaux locaux sans fil depuis longtemps et les ont déployée pour augmenter la productivité de leurs employés, activer de nouvelles applications et permettre la mobilité du réseau. Autrefois, les réseaux locaux sans fil s'appuyaient sur des points d'accès lourds et utilisaient le protocole de chiffrement WEP. Aujourd'hui, ces technologies sont considérées comme encombrantes, voire même dangereuses. Néanmoins, de nombreuses organisations ont largement investi dans ces technologies et n'ont pas les moyens d'effectuer une mise à niveau à grande échelle. Aruba Networks permet à ces organisations d'étendre leurs points d'accès au réseau local sans fil existant pour fournir un réseau orienté sur l'utilisateur.

Obstacles à l'extension des réseaux locaux sans fil propriétaires

MANQUE DE MOBILITÉ

Les points d'accès propriétaires sont ancrés aux réseaux locaux sans fil et aux sous-réseaux IP, ce qui signifie que les clients sans fil sont également ancrés à ces réseaux locaux sans fil. Lorsqu'un client se déplace sur un point d'accès connecté à un réseau local sans fil différent, la transition n'est pas transparente. Les clients sont forcés d'obtenir une nouvelle adresse IP et les sessions existantes doivent être redémarrées.

FAILLES DE SÉCURITÉ DES RÉSEAUX LOCAUX SANS FIL

De nombreux points d'accès plus anciens prennent uniquement en charge WEP et ne peuvent être mis à niveau pour prendre en charge WPA2, la norme de sécurité sans fil actuelle. Ceci expose l'organisation concernée à un risque plus important. Les réseaux locaux sans fil propriétaires fournissent également un accès aux utilisateurs qui une fois connectés ont accès à l'ensemble des ressources. Ce système ne permet pas l'accès sécurisé des invités et ouvre des brèches dans le réseau dans lesquelles

des dispositifs simples, tels que des scanners de codes à barres sans fil, disposent de droits d'accès excessifs.

MANQUE DE VISIBILITÉ DES RÉSEAUX LOCAUX SANS FIL

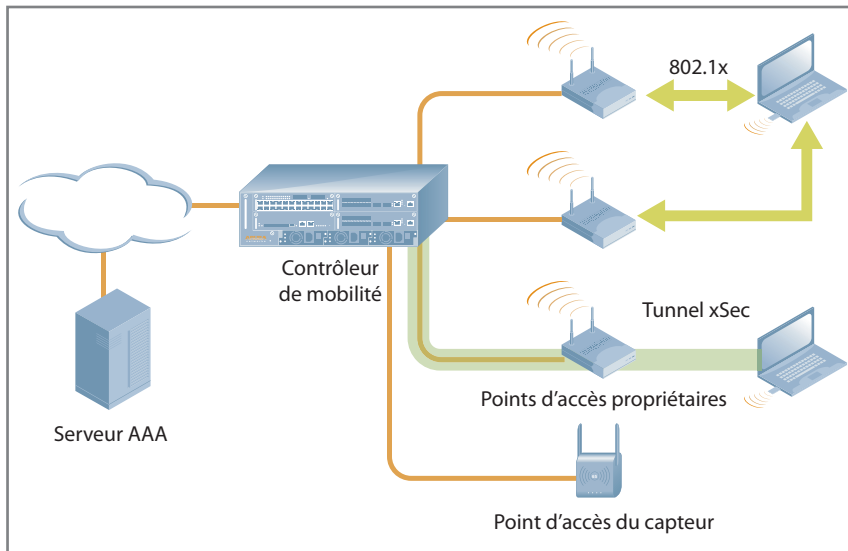
Les réseaux locaux sans fil propriétaires fournissent une visibilité limitée voire nulle dans le domaine des radiofréquences. Le dépannage, la détection et la localisation des points d'accès indésirables ainsi que la détection des attaques sont des processus manuels qui nécessitent une connaissance approfondie des réseaux locaux sans fil.

DÉPANNAGE ENCOMBRANT

Lorsqu'un point d'accès propriétaire n'est plus accessible à partir du réseau, les administrateurs doivent effectuer un dépannage manuel du point d'accès. Ceci est à la fois fastidieux et coûteux.

Avantages :

- Mise à niveau instantanée des fonctions de sécurité des réseaux locaux sans fil sans remplacer les points d'accès
- Élimination des échecs d'itinérance entre les réseaux locaux
- Renforcement de la sécurité globale avec la protection contre les intrusions sur le réseau sans fil
- Meilleure application des règles de sécurité avec le pare-feu dynamique d'Aruba
- Chemin de migration simple des réseaux locaux sans fil propriétaires aux réseaux locaux sans fil modernes et centralisés

**Mobilité sécurisée pour
les réseaux locaux
sans fil propriétaires****Comment Aruba sécurise et rend mobiles les
réseaux locaux sans fil propriétaires**

En installant un contrôleur de mobilité Aruba sur le réseau et en connectant des points d'accès propriétaires via le contrôleur, physiquement ou logiquement, les points d'accès propriétaires peuvent bénéficier de nombreux avantages découlant de l'utilisation d'un réseau local sans fil moderne et centralisé.

ITINÉRANCE TRANSPARENTE

Le serveur DHCP proxy d'Aruba permet d'obtenir une itinérance transparente, quel que soit le réseau local auquel le point d'accès est physiquement connecté. Lorsqu'un client accède au réseau pour la première fois, une adresse IP lui est attribuée selon les règles habituelles (le réseau local sur lequel le point d'accès réside). Lorsque le client se déplace, une demande de renouvellement DHCP est émise chaque fois qu'un nouveau point d'accès lui est associé. Le contrôleur de mobilité capture la demande DHCP et y répond, indiquant au client de garder la même adresse IP. De cette façon, un client peut se déplacer au sein des réseaux locaux, sans le redémarrage des sessions en cours.

**AUTHENTIFICATION 802.1X
DYNAMIQUE**

L'authentification 802.1x dynamique permet au contrôleur de mobilité

de connaître l'identité et le rôle d'un utilisateur connecté à un point d'accès tiers. Lorsqu'un point d'accès 802.1x envoie une requête RADIUS au serveur AAA, le contrôleur de mobilité inspecte la requête et la réponse associée pour connaître l'état d'authentification de l'utilisateur. Il applique ensuite des fonctions et règles de sécurité basées sur l'identité via le pare-feu d'application.

**PARE-FEU D'APPLICATION DES
RÈGLES DE SÉCURITÉ**

Avec le pare-feu d'application des règles de sécurité certifié ICASA d'Aruba, le contrôleur de mobilité peut appliquer un contrôle d'accès basé sur l'identité des utilisateurs. Les utilisateurs sont associés à des rôles basés sur l'appartenance à un groupe, avec des droits d'accès différents pour chaque rôle. Avec le pare-feu d'application des règles de sécurité, un accès ouvert peut être accordé aux employés travaillant sur des ordinateurs portables tandis qu'un accès très limité est accordé aux utilisateurs de dispositifs tels que les scanners de codes à barres – même si les deux dispositifs ont le même identifiant de réseau. Par ailleurs, il est possible de limiter l'accès des invités à Internet tout en accordant aux sous-traitants des droits d'accès limités au réseau interne.

Mobilité sécurisée pour les réseaux locaux sans fil propriétaires

SERIAL-OVER-ETHERNET ET POWER-OVER-ETHERNET

Lorsque des points d'accès tiers sont connectés directement à un contrôleur de mobilité, les technologies POE (Power-over-Ethernet) et SOE (Serial-over-Ethernet) sont fournies par le contrôleur de mobilité. En utilisant SOE avec le séparateur approprié, le point d'accès peut être connecté via le serveur de terminal intégré du contrôleur de mobilité en reliant les connexions série RS-232 via les fils inutilisés des câbles à paires torsadées standard. Les administrateurs n'ont plus besoin d'escalader des échelles pour connecter les ports de console aux points d'accès lorsque des opérations de dépannage doivent être réalisées. Il leur suffit de se connecter au contrôleur de mobilité via Telnet ou SSH, ce qui leur permet d'accéder immédiatement au point d'accès tiers.

VPN XSEC DE COUCHE 2

Certains points d'accès propriétaires ne peuvent pas être mis à niveau pour prendre en charge les normes de sécurité modernes telles que WPA ou WPA2. Pour ces points d'accès, le protocole xSec d'Aruba fournit un moyen de contourner entièrement la sécurité du point d'accès tout en offrant tous les avantages de WPA2 avec chiffrement AES. En utilisant le logiciel client xSec, un tunnel sécurisé est créé sur la liaison sans fil au contrôleur de mobilité Aruba. Alors que le point d'accès peut fonctionner en mode « ouvert », tout trafic transitant par le point d'accès est authentifié et chiffré comme avec WPA2. Le logiciel est disponible avec un certain nombre de systèmes d'exploitation courants.

VISIBILITÉ DES RADIOFRÉQUENCES

En ajoutant un petit nombre de points d'accès Aruba pour qu'ils agissent comme des dispositifs de contrôle, le spectre radiofréquence est fourni à l'administrateur réseau pour qu'il puisse visualiser les activités, les interférences et les conditions d'erreur. Pour le dépannage des sessions, des captures de paquets distants en temps réel peuvent être transférées vers l'outil d'analyse Enterprise Analyzer d'Aruba.

PRÉVENTION DES INTRUSIONS SUR UN RÉSEAU SANS FIL

Afin d'améliorer la sécurité des réseaux sans fil, Aruba fournit un module de prévention des intrusions sans fil intégré à chaque contrôleur de mobilité. Ce système contrôle à la fois les points d'accès d'Aruba et les points d'accès tiers et peut identifier un certain nombre de vulnérabilités et d'attaques contre les réseaux locaux sans fil, y compris les points d'accès indésirables, le chevauchement de dispositifs clients et les dénis de service. Pour des fonctions plus poussées incluant la corrélation et la visualisation avancée des événements, Aruba offre également l'application logicielle indépendante RFprotect™ qui s'intègre aux points d'accès sans fil d'Aruba agissant comme des capteurs.



WWW.ARUBANETWORKS.COM

1322 Crossman Avenue. Sunnyvale, CA 94089 | Tél. +1 408.227.4500 | Fax. +1 408.227.4550