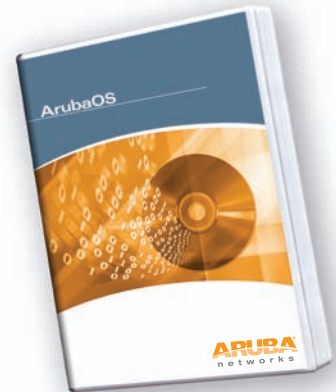




MODULE ARUBAOS XSEC

xSec est un protocole de couche de liaison de données (Layer 2) hautement sécurisé offrant une structure homogène pour sécuriser toutes les connexions de réseau connecté et sans fil à l'aide d'outils de chiffrement et d'authentification puissants. xSec est équipé d'une solution conforme à la norme FIPS visant à fournir une sécurité basée sur l'identité aux agences gouvernementales et aux entités commerciales qui doivent transmettre des données très confidentielles sur des réseaux sans fil. xSec offre une meilleure sécurité que les autres technologies de chiffrement Layer 2 en utilisant des clés plus longues, des algorithmes de chiffrement validés par le FIPS (AES-CBC-256 avec HMAC-SHA1) et le chiffrement des informations d'en-tête Layer 2, y compris les adresses MAC. Aruba Networks et Funk Software, une division de Juniper Networks, ont développé conjointement xSec.



STRUCTURE DE SÉCURITÉ HOMOGENÈME

- Authentification et chiffrement universels pour les utilisateurs des connexions filaires et sans fil, quelle que soit la méthode d'accès à ces réseaux

TECHNOLOGIE VALIDÉE PAR LE FIPS

- Certifiée et conforme à la norme FIPS 140-2

PROTECTION DU MATÉRIEL ANCIEN

- Une solution client basée sur un logiciel qui supporte la présence de points d'accès sans fil et de cartes réseau d'anciennes générations

TECHNOLOGIE CONÇUE À DES FINS DE COMPATIBILITÉ

- Basée sur la structure IEEE 802.1x avec prise en charge de toutes les méthodes EAP sécurisées

PRÉVENTION CONTRE LES POINTS D'ACCÈS MALVEILLANTS

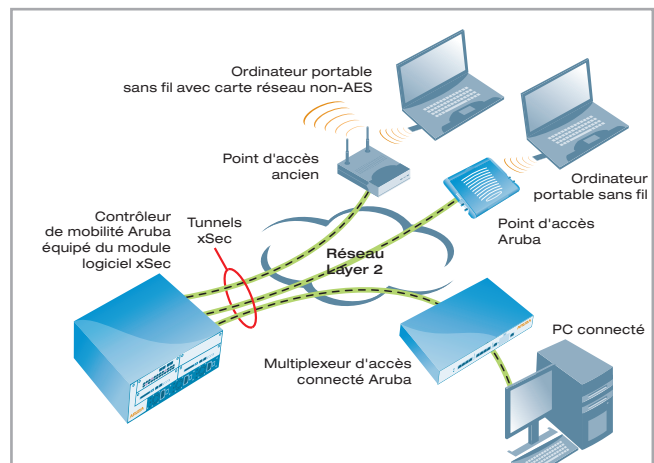
- Détection, classification, localisation et confinement automatique des points d'accès malveillants

CHIFFREMENT LAYER 2 NÉCESSAIRE

Le chiffrement est traditionnellement effectué au niveau de la couche Layer 3 (couche réseau) au même titre que la technologie IPsec. IPsec fait appel au chiffrement 3DES ou AES, et peut chiffrer le paquet IP, y compris les adresses IP source et de destination dans l'en-tête. IPsec fournit une méthode de communication sécurisée acceptée généralement sur les réseaux non sécurisés, car les seules informations non chiffrées représentent des en-têtes de paquet et un trafic Layer 2 authentique, tels que les paquets ARP et DHCP.

Lorsque la confidentialité des données chiffrées par IPsec n'est pas remise en question, il se peut qu'un attaquant accédant directement aux autres périphériques d'un réseau via la couche de liaison s'en prenne à ces périphériques. Par exemple, un réseau sans fil sécurisé avec WEP et IPsec peut exposer les périphériques client à d'éventuels risques si un attaquant obtient la clé WEP et accède au réseau via la couche Layer 2. En outre, l'utilisation d'informations d'en-tête de paquet affichées en vue d'une attaque constitue une réelle préoccupation pour de nombreux groupes de sécurité.

C'est pourquoi maintes agences gouvernementales et entités commerciales exigent le déploiement de technologies puissantes de chiffrement Layer 2 pour garantir la confidentialité absolue des données. Un grand nombre d'agences de protection exigent le chiffrement au niveau de la couche Layer 2 de toutes les données transmises via des périphériques sans fil commerciaux. Les moteurs cryptographiques utilisés pour toute communication confidentielle entre les agences gouvernementales doivent être validés comme conformes aux normes FIPS 140-2. C'est dans cette optique qu'a été conçue la technologie xSec, qui présente d'autres avantages.



Connexion de périphériques connectés et sans fil via xSec

STRUCTURE DE SÉCURITÉ HOMOGENÈME

xSec permet l'authentification et le chiffrement universels, quelle que soit la méthode d'accès. Chaque client connecté au réseau (connecté ou sans fil) peut s'authentifier auprès d'un contrôleur de mobilité Aruba à l'aide d'un client xSec. L'authentification à l'intérieur du protocole xSec s'effectue via la norme EAP 802.1x et un serveur RADIUS standard pour valider les informations de connexion. xSec prend en charge l'authentification en utilisant des mots de passe, des certificats, des cartes intelligentes, des cartes de jeton ou autres informations de connexion pris en charge par le type EAP sélectionné.

MODULE ARUBAOS XSEC

TECHNOLOGIE VALIDÉE PAR LE FIPS

En utilisant AES-CBC avec une clé 256 bits pour le chiffrement, xSec fournit le seul protocole Layer 2 pour produits commerciaux validé par le FIPS. Par conséquent, xSec représente la solution idéale pour les applications de sécurité utilisées dans les secteurs public, financier et médical. FIPS est une norme de sécurité plus contraignante que celles requises dans le secteur commercial. Par conséquent, elle répond mieux aux critères de conformité avec les dispositions commerciales en vigueur, telles que HIPAA et GLBA.

PROTECTION DU MATÉRIEL ANCIEN

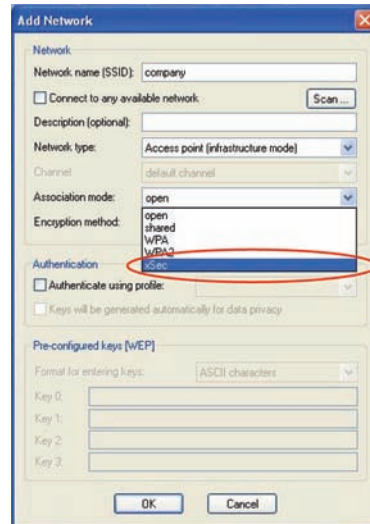
La plupart des équipements anciens ne peuvent pas être mis à niveau pour prendre en charge les dernières normes de sécurité, comme 802.11i et WPA2. Toutefois, le chiffrement est effectué au niveau matériel par le contrôleur de mobilité Aruba et dans le logiciel au niveau du client, ce qui implique la possibilité de mettre à niveau un réseau existant pour qu'il prenne en charge la dernière technologie de sécurité sans remplacer les points d'accès anciens ou les cartes réseau sans fil.

TECHNOLOGIE CONÇUE À DES FINS DE COMPATIBILITÉ

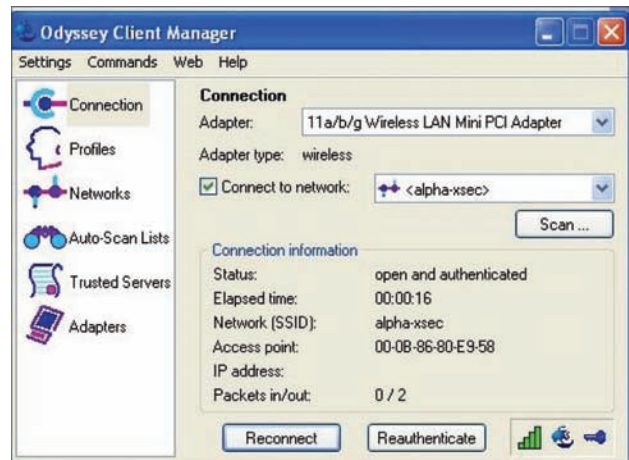
xSec repose sur la norme de sécurité IEEE 802.1x. Les méthodes EAP sécurisées (EAP-TLS, TTLS et PEAP) sont prises en charge, rendant ainsi xSec compatible avec les outils de sécurité existants, comme les jetons RSA et les certificats PKI. xSec se veut transparent pour l'infrastructure Layer 2 et fonctionne via un réseau Ethernet commuté, et ce sans aucun risque d'interception des trames EAP par des commutateurs Ethernet conformes 802.1x. La solution Odyssey Client de Juniper Networks, dotée de la technologie xSec, est disponible pour Windows 2000, Windows XP et Windows Mobile.

SCÉNARIOS DE DÉPLOIEMENT

xSec est déployé en activant la licence logicielle correspondante sur un contrôleur de mobilité Aruba, puis en installant la solution Odyssey Client de Juniper Networks sur un PC connecté ou sans fil. xSec permet de sécuriser le trafic entre un contrôleur de mobilité Aruba et un client sans fil, entre un contrôleur de mobilité Aruba et un client connecté ou entre deux contrôleurs de mobilité sur le même VLAN.



Configuration du client à des fins de chiffrement xSec pour le SSID « company »



Solution Odyssey Client connectée au SSID « alpha-xsec » via le protocole xSec



WWW.ARUBANETWORKS.COM

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