

SECURITE radio 802.11b

Installation par défaut d'un réseau 802.11b

Les points d'accès CISCO AP1100 et AP1200, par défaut, sont configurés sans aucune protection. Ce type de configuration est le même sur n'importe quel autre point d'accès vendu par un autre fabricant. Cela permet à un utilisateur de mettre en place rapidement un réseau sans fil.

Mise à niveau de la sécurité par JAM

JAM distribue et met en place des systèmes RF (802.11b). En matière de sécurité radio, JAM propose le paramétrage de tous les différents matériels qu'il vend. Le paramétrage de base est d'un niveau de sécurité peu élevé : il permet de limiter, mais pas d'empêcher les intrusions sur le réseau du client via la radiofréquence.

Ce paramétrage consiste à paramétrer les lecteurs et les points d'accès pour qu'ils utilisent tous, et sans problème, un cryptage **WEP** + **TKIP** 128 bits (pour matériel CISCO) et une authentification par adresse MAC.

WEP (*Wired Equivalent Privacy*) : Système de cryptage qui permet d'authentifier les clients RF qui peuvent se connecter à une Access Point. Si un client désire se connecter à un Access Point et n'a pas la clé WEP définie, il ne pourra pas se connecter. Cette clé peut être de longueur 40 bits ou 104 bits.

TKIP (*Temporary Key Integrity Protocol*) : le cryptage WEP étant peu fiable (il est possible de trouver une clé WEP en quelques heures en sniffant un réseau RF et en utilisant certains outils disponibles librement), CISCO a essayé de combler ces faiblesses en mettant en place le protocole TKIP. TKIP est un ensemble de fonctions ajoutées au WEP standard qui permet de rendre plus long le temps de craquage d'une clé WEP. On a ainsi une clé de cryptage sur 128 bits = 104 bits de la clé WEP standard + 24 bits ajoutés automatiquement par TKIP.

Ce TKIP est un système CISCO, nous n'avons pas encore validé si cela fonctionnait avec des cartes 802.11b autres que CISCO.

L'authentification par adresse MAC permet de bloquer les lecteurs qui ne font pas partie d'une liste d'adresses MAC stockée dans les antennes. L'inconvénient de cette authentification est qu'il faut ajouter à la main toutes les adresses MAC des nouveaux appareils qui vont se connecter au réseau sans-fil (pas très pratique si beaucoup de matériel 802.11b). De plus, ce système n'est pas totalement sûr, car il est toujours possible de trouver une adresse MAC valide et de l'utiliser pour pouvoir se connecter au réseau sans-fil.

Améliorer la sécurité

Pour améliorer la sécurité, il est possible de mettre en place un système d'authentification et de cryptage dynamique avec le protocole **LEAP** et un serveur **RADIUS**.

JAM peut fournir les différents drivers CISCO nécessaires pour pouvoir utiliser LEAP mais JAM ne réalise pas le paramétrage et l'administration de serveurs RADIUS.

De la même façon, il est possible d'utiliser d'autres méthodes de sécurité (EAP-TLS, PEAP, VPN + Isec, etc.), qui sont plus ou moins simples à mettre en œuvre suivant le matériel utilisé, et surtout de la politique d'administration réseau du client.

Dans ce cas, nous vous conseillons de consulter JAM afin de valider la faisabilité sur le type de matériel et de logiciel choisis.

Lexique

LEAP = Lightweight Extensible Authentication protocol

VPN = Virtual Private Network

EAP-TLS = EAP Transport Layer Security

PEAP = Protected EAP

Pour plus d'informations

1. Documentation détaillée sur le site web de CISCO : <http://www.cisco.com/go/safe/>

Le document qui s'appelle « Wireless LAN security in depth » explique comment mettre en place un réseau sans-fil sécurisé suivant les besoins de l'entreprise.

2. Autres documents (plus techniques) disponibles à l'adresse suivante: <http://www.cisco.com/go/aironet/security>