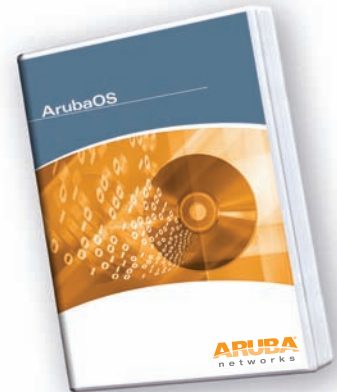




ARUBAOS WIRELESS INTRUSION PROTECTION (PROTECTION CONTRE LES INTRUSIONS SANS FIL ARUBAOS)

Le module Wireless Intrusion Protection (protection contre les intrusions sans fil) d'Aruba protège le réseau contre les menaces liées à la sécurité des réseaux sans fil en intégrant dans son infrastructure un système de prévention des intrusions sans fil. Plus besoin d'utiliser un système de capteurs RF et de dispositifs de sécurité à part ! Le module Wireless Intrusion Protection (protection contre les intrusions sans fil) donne aux administrateurs une visibilité unique sur les réseaux sans fil, déjoue les attaques sans fil malveillantes, l'usurpation d'identités et les intrusions non autorisées.



PRÉVENTION CONTRE LES POINTS D'ACCÈS MALVEILLANTS

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

DÉTECTION DES ATTAQUES PAR DÉNI DE SERVICE

- Saturation par émission de trames de gestion
- Attaques par désauthentification
- Saturation par authentifications multiples
- Saturation par « probe requests »
- Création de points d'accès fictifs
- Attaques de type « null probe response »
- Saturation de trames EAP

SURVEILLANCE ET DÉCOUVERTE DU RÉSEAU

- Détection des sondes NetStumbler et de diffusion

PRÉVENTION DES INTRUSIONS CLIENTS

- Protection des points d'accès par la technique « pot de miel »
- Protection des stations valides

NETWORK INTRUSION DETECTION

- Ponts sans fil
- Attaques ASLEAP

SURVEILLANCE

- Détection d'une mise en œuvre de chiffrement insuffisante

DÉTECTION ET PREVENTION DES USURPATIONS D'IDENTITÉS

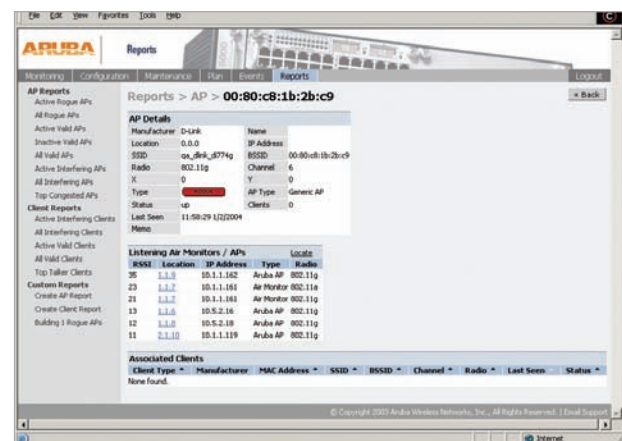
- Usurpation d'adresses MAC
- Usurpation d'identités de points d'accès
- Attaques « man in the middle »
- Détection des anomalies de numéro d'ordre

La détection ne constitue qu'une étape de la protection de l'environnement de l'entreprise contre les tentatives d'accès sans fil non autorisées. Les mesures appropriées appliquées pour mettre rapidement fin aux intrusions jouent un rôle crucial dans la protection des données confidentielles et des ressources réseau. Pour ce faire, vous devez disposer d'outils de classification précis pour les stations et les points d'accès (valides, malveillants ou voisins) et répondre automatiquement aux tentatives d'intrusion possibles.

Les points d'accès Aruba analysent en permanence tous les canaux du spectre RF, en capturant l'ensemble du trafic 802.11 et en examinant

localement les données capturées. Seules les violations de stratégie sont envoyées au contrôleur de mobilité Aruba afin de minimiser l'impact sur les performances du réseau connecté. Lors de l'analyse, le système prend connaissance de tous les points d'accès et stations sans fil, et classe ces périphériques en fonction des flux de trafic observés au niveau de la connexion et dans l'espace. Les données de trafic sont collectées et mises en corrélation sur le contrôleur de mobilité.

Le module Wireless Intrusion Protection (protection contre les intrusions sans fil) d'Aruba offre des fonctions de détection et de prévention. Par conséquent, les administrateurs peuvent répondre à toute tentative d'accès involontaire ou malveillante au réseau local sans fil.



Détection et interruption précises des points d'accès malveillants

DÉTECTION ET DÉSACTIVATION DES POINTS D'ACCÈS MALVEILLANTS

L'infrastructure de réseau local sans fil adaptatif d'Aruba permet aux points d'accès de prendre en charge les clients du réseau local sans fil et de repérer les tentatives d'intrusion au niveau radio. Vous pouvez également la configurer pour qu'elle ne prenne en charge qu'une seule fonction. Ce repérage consiste à détecter les points d'accès et périphériques non autorisés, y compris ceux équipés de systèmes radio MIMO ou antérieurs à 802.11n. Les périphériques détectés sont considérés comme malveillants et automatiquement désactivés. En outre, les administrateurs sont avisés de la présence de ces périphériques et de leur emplacement physique précis sur un plan d'étage pour réduire leur impact.

ARUBAOS WIRELESS INTRUSION PROTECTION (PROTECTION CONTRE LES INTRUSIONS SANS FIL ARUBAOS)

CLASSIFICATION UNIQUE DES STATIONS ET DES UTILISATEURS

Le système breveté d'Aruba identifie et classe automatiquement tous les points d'accès et stations connectés au réseau afin de réduire les fausses alertes. Ce système obéit à une logique innovante incluant l'analyse des tendances de trafic, la comparaison des trafics côté réseau connecté et côté réseau sans fil, ainsi que des informations sur l'emplacement des périphériques. Dans cette logique, les périphériques et points d'accès détectés sont précisément considérés comme malveillants ou constituant une menace réelle, par opposition aux périphériques des réseaux voisins.

PROTECTION CONTRE LES ATTAQUES PAR DÉNI DE SERVICE ET USURPATIONS D'IDENTITÉS

Les réseaux sans fil étant des réseaux ouverts, ils représentent des cibles de choix pour les attaques par déni de service. Ces attaques englobent les logiciels qui dirigent le réseau avec des requêtes d'association, les attaques donnant à un ordinateur portable l'apparence de milliers de points d'accès permettant la saturation par milliers de trames de de-authentication. Les contrôleurs de mobilité Aruba équipés du module ArubaOS Wireless Intrusion Protection (protection contre les intrusions sans fil) mettent à jour les signatures de diverses attaques sans fil et peuvent les empêcher d'interrompre le service.

En ce qui concerne les entreprises, la protection avancée contre les attaques par déni de service s'applique à diverses attaques sans fil, y compris les saturation d'associations et de de-authentication, les techniques de type « pots de miel », les usurpations d'identités pour les stations et points d'accès. Selon les signatures d'emplacement et la classification des clients, les points d'accès Aruba suppriment les requêtes non autorisées et génèrent des alertes pour aviser les administrateurs de l'attaque.

PROTECTION CONTRE LES ATTAQUES « MAN IN THE MIDDLE

Les attaques « man in the middle » font partie des types d'attaque de réseau sans fil courantes. Lors de ces attaques, un pirate se fait passer pour un point d'accès légitime et, en faisant office de point de relais, envoie des données via le périphérique non autorisé à l'insu des utilisateurs et des autres points d'accès. L'attaquant peut ensuite modifier ou endommager ces données, ou exécuter des sous-programmes d'altération de mot de passe.

Les points d'accès Aruba repèrent dans l'espace les autres stations sans fil se faisant passer pour des points d'accès valides. Lorsque cette tentative est détectée, les mesures de sécurité appropriées sont appliquées. En outre, les contrôleurs de mobilité Aruba suivent les « signatures » uniques pour chaque client sans fil sur le réseau. Si une nouvelle station est présentée comme un client particulier, mais qu'elle ne dispose pas d'une signature valide, une attaque par usurpation d'identité pour cette station est déclarée.

DÉFINITION ET APPLICATION DE STRATÉGIES

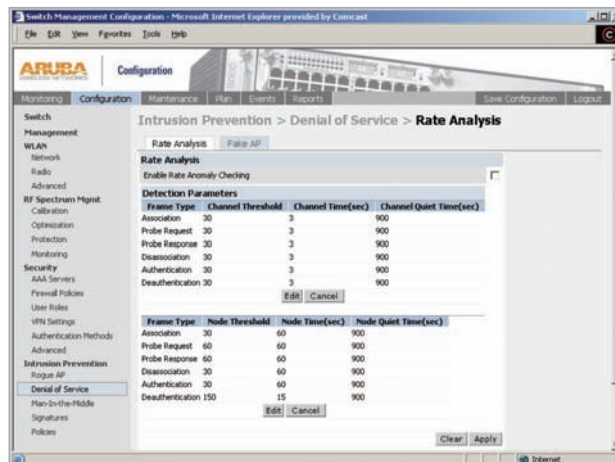
Le module ArubaOS Wireless Intrusion Protection (protection contre les intrusions sans fil ArubaOS) utilise plusieurs stratégies configurables à appliquer automatiquement en cas de violation. Voici quelques exemples de stratégies sans fil : la détection de mise en œuvre de chiffrement WEP insuffisant, la protection contre les configurations de point d'accès incorrectes, la détection et la protection de réseaux ad hoc, la détection de types de carte réseau non autorisés ou de ponts sans fil.

UTILISATION DE LA TECHNOLOGIE SANS FIL POUR PROTÉGER VOTRE RESEAU CONNECTE

Même en l'absence de LAN sans fil, le module Wireless Intrusion Protection (protection contre les intrusions sans fil) d'Aruba interrompt le flux de trafic sans fil sur le réseau connecté via les points d'accès malveillants connectés à son insu à un port réseau. Cette fonction protège le réseau contre les failles de sécurité sans fil. Une fois l'entreprise prête à déployer des réseaux LAN sans fil, le système Aruba peut aisément être reconfiguré de manière à offrir une infrastructure LAN sans fil sécurisée évolutive.

UTILISATION DE LA TECHNOLOGIE SANS FIL POUR PROTÉGER VOTRE RÉSEAU SANS FIL EXISTANT

ArubaOS Wireless Intrusion Protection (protection contre les intrusions sans fil ArubaOS) complète et améliore les déploiements de réseau local sans fil existants, y compris les déploiements Cisco, en fournissant des fonctions avancées de contrôle et de sécurité RF non disponibles dans les solutions sans fil de première génération.



Wireless Intrusion Protection (protection contre les intrusions sans fil) détecte tout un ensemble de menaces RF.



WWW.ARUBANETWORKS.COM

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