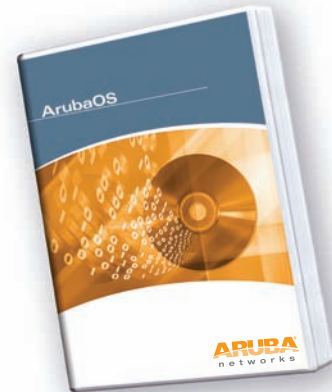




MÓDULO DE PROTECCIÓN CONTRA INTRUSIONES INALÁMBRICAS ARUBAOS

El módulo de protección contra intrusiones inalámbricas (o WIP, Wireless Intrusion Protection) Aruba protege a la red frente a las amenazas inalámbricas, ya que incorpora una protección inalámbrica contra intrusiones en la infraestructura de red y ya no se requiere un sistema separado de sensores RF y de equipos de seguridad. El módulo WIP dota a los administradores de una visibilidad extraordinaria de la red inalámbrica y frustra los ataques maliciosos inalámbricos, las suplantaciones y las intrusiones no autorizadas.



PROTECCIÓN CONTRA AP MALICIOSOS

- Detección, clasificación, localización y contención automática de AP maliciosos

DETECCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO

- Inundaciones de tramas de gestión
- Ataques de desautenticación
- Inundaciones de autenticación
- Inundaciones de probe requests
- Inundaciones de AP falsos
- Respuestas null probe
- Inundaciones de EAP handshake

SONDEO Y DESCUBRIMIENTO DE RED

- Detección de NetStumbler y de probes broadcast

PROTECCIÓN CONTRA INTRUSIONES EN CLIENTES

- Protección contra AP tarro de miel
- Protección de estación válida

DETECCIÓN DE INTRUSIONES EN LA RED

- Puentes inalámbricos
- Ataques ASLEAP

CONTROL

- Detección de implementaciones de cifrado débiles

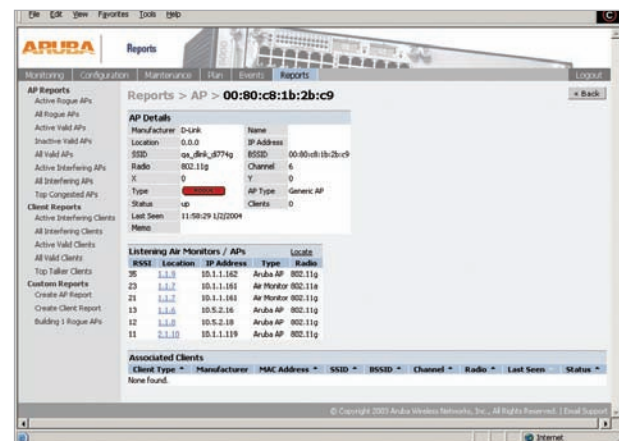
DETECCIÓN Y PREVENCIÓN CONTRA SUPLANTACIONES

- Suplantación de dirección MAC
- Suplantaciones de AP
- Ataques Man-in-the-middle
- Detección de anomalías en el número de secuencia

La detección sólo es un paso de todo el proceso de asegurar el entorno corporativo contra el acceso inalámbrico no deseado. Las medidas adecuadas para bloquear rápidamente las intrusiones son cruciales para proteger la información sensible y los recursos de red. Para conseguirlo se necesitan medios apropiados para clasificar los AP y las estaciones (p. ej., válidos, maliciosos o vecinos), así como para ofrecer una respuesta automatizada a los posibles intentos de intrusión.

Los puntos de acceso Aruba exploran de forma constante todos los canales del espectro RF, capturan todo el tráfico 802.11 y examinan localmente los datos capturados. Únicamente las infracciones de las políticas se envían al controlador de movilidad Aruba para minimizar el impacto en el rendimiento de la red conectada por cable. Durante la exploración, el sistema estudia todas las estaciones y los AP inalámbricos y clasifica dichos dispositivos basándose en los flujos del tráfico vistos por cable y por aire. Los datos del tráfico se reúnen y correlacionan en el controlador de movilidad.

El módulo WIP de Aruba ofrece funcionalidades de detección y prevención para que los administradores puedan reaccionar adecuadamente contra el acceso involuntario y malicioso a la WLAN.



Detección y anulación precisas de los puntos de acceso maliciosos

DETECCIÓN Y DESHABILITACIÓN DE LOS APS MALICIOSOS

La infraestructura WLAN adaptativa de Aruba permite que los APs presten servicio a los clientes WLAN mientras monitorizan el aire en busca de eventos de intrusión, aunque también es posible configurarlos para que sólo presten una función. La monitorización del aire detecta los APs y los dispositivos no autorizados, incluyendo los que disponen de radios MIMO o pre-802.11n. Los dispositivos detectados se clasifican como maliciosos y se pueden deshabilitar automáticamente. Los administradores reciben una notificación en la que se les avisa de la presencia de dispositivos maliciosos junto con su ubicación física exacta en los mapas de edificio para que procedan a la mitigación.

MÓDULO DE PROTECCIÓN CONTRA INTRUSIONES INALÁMBRICAS ARUBAOS

CLASIFICACIÓN ÚNICA DE ESTACIONES Y USUARIOS

De forma automática, el sistema patentado de Aruba identifica y clasifica todos los AP y las estaciones que están conectados a la red para minimizar los falsos positivos. El sistema funciona con una lógica innovadora que incluye el análisis de patrones de tráfico, la comparación entre el tráfico conectado por cable y el inalámbrico, así como la información sobre la ubicación de los dispositivos. Tras aplicar esta lógica, los dispositivos y los AP encontrados se clasifican con precisión como verdaderas amenazas o dispositivos maliciosos para distinguirlos de los dispositivos que pertenecen a redes vecinas.

PROTECCIÓN CONTRA LA DENEGACIÓN DE SERVICIO Y LAS SUPLANTACIONES

Debido a que funcionan en un medio abierto, las redes inalámbricas son un objetivo muy atractivo para los ataques de denegación de servicio. Este tipo de ataques incluye software que inunda la red con peticiones de asociación, ataques que hacen que un portátil parezca ser miles de APs e inundaciones de desautenticación. Los controladores de movilidad Aruba equipados con el módulo WIP ArubaOS mantienen firmas de abundantes ataques inalámbricos y son capaces de bloquearlos para que el servicio no se interrumpa. La protección avanzada contra la denegación de servicio mantiene segura a la empresa contra distintos ataques inalámbricos, que incluyen las inundaciones de asociación y de desautenticación, los tarros de miel y las suplantaciones de los AP y las estaciones. Basándose en las firmas de las ubicaciones y en la clasificación de los clientes, los puntos de acceso Aruba descartan las peticiones no válidas y generan alertas para notificar del ataque a los administradores.

PROTECCIÓN CONTRA HOMBRE-EN-MEDIO

Uno de los ataques más frecuentes contra las redes inalámbricas es el del hombre-en-medio (man-in-the-middle). En este tipo de ataques un pirata informático se hace pasar por un AP legítimo y, desde esta posición, actúa como un punto de distribución y engaña a los usuarios y a los otros AP para que envíen datos a través del dispositivo no autorizado. Posteriormente, el atacante puede modificar o corromper esos datos o bien ejecutar rutinas para averiguar contraseñas. Los puntos de acceso Aruba monitorizan el aire para detectar otras estaciones inalámbricas que se estén haciendo pasar por APs válidos. Una vez detectada la suplantación se ponen en marcha los mecanismos de defensa adecuados. Los controladores de movilidad Aruba también hacen un seguimiento de "firmas" únicas para cada uno de los clientes inalámbricos de la red. Así, si una estación nueva se presenta diciendo ser un cliente particular pero carece de una firma adecuada, se declara un ataque de suplantación de estación.

DEFINICIÓN Y APLICACIÓN DE POLÍTICAS

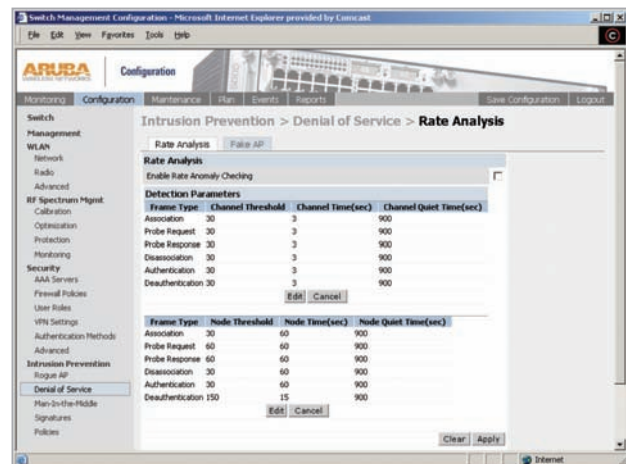
El módulo WIP ArubaOS utiliza numerosas políticas que se pueden configurar para que actúen automáticamente en caso de infracción de políticas. Algunos ejemplos de políticas inalámbricas son la detección de implementaciones WEP débiles, la protección contra errores de configuración de los AP, la detección y la protección redes ad-hoc, la detección del tipo de NIC no autorizado y la detección de puentes inalámbricos.

TECNOLOGÍA INALÁMBRICA PARA PROTEGER LA RED CONECTADA POR CABLE

Incluso si no se utilizan las LAN inalámbricas, el módulo WIP Aruba impide que el tráfico inalámbrico acceda a la red conectada por cable a través de AP maliciosos que no se sabía que estaban conectados a un puerto de red. Esta funcionalidad protege la red contra las brechas de seguridad inalámbricas. Cuando la empresa ya esté preparada para desplegar las LAN inalámbricas, el sistema Aruba se puede volver a configurar muy fácilmente para disponer de una infraestructura LAN inalámbrica segura y escalable.

TECNOLOGÍA INALÁMBRICA PARA PROTEGER LA RED INALÁMBRICA EXISTENTE

El módulo WIP ArubaOS complementa y amplía cualquier despliegue WLAN existente, incluyendo los despliegues Cisco, ya que proporciona funciones avanzadas de seguridad RF y de control que no se encuentran en los productos inalámbricos de primera generación.



La protección contra intrusiones inalámbricas detecta rangos completos de amenazas RF



[WWW.ARUBANETWORKS.COM](http://www.arubanetworks.com)

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