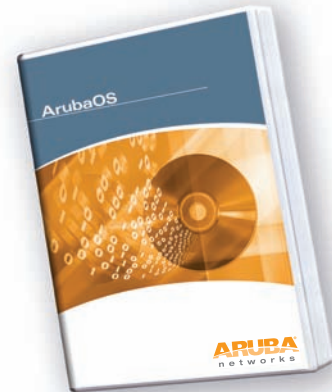




ARUBAOS WIRELESS INTRUSION PROTECTION MODULE

Das Wireless Intrusion Protection (WIP)-Modul von Aruba schützt Ihr Netzwerk vor drahtlosen Bedrohungen, indem es den Schutz vor Eindringlingen in die Netzwerkinfrastruktur integriert und so ein zusätzliches System von Funksensoren und Sicherheitsanwendungen überflüssig macht.

Das WIP-Modul ermöglicht Administratoren einen unübertroffenen transparenten Überblick des kabellosen Netzwerks, vereitelt und unterbindet Angriffe, betrügerische Imitationen von Access Points sowie nicht autorisierte Zugriffe, die kabellos durchgeführt werden.



SCHUTZ VOR NICHT AUTORISIERTEN ACCESS POINTS

- Erkennung, Klassifizierung, Lokalisierung und automatische Eindämmung nicht autorisierter Access Points

ERKENNUNG VON DENIAL OF SERVICE (DOS)-ANGRIFFEN

- Management-Frame-Flooding
- Deauthentication-Angriffe
- Authentication-Flooding
- Probe-Request-Flooding
- Fake-AP-Flooding
- Null-Probe-Responses
- EAP-Handshake-Flooding

PROBING UND NETWORK DISCOVERY

- Erkennung von NetStumbler und Broadcast Probes

CLIENT INTRUSION PREVENTION

- Schutz vor Honeypot-Access Points
- Schutz gültiger Stationen

NETWORK INTRUSION DETECTION

- Wireless Bridges
- ASLEAP-Angriffe

ÜBERWACHUNG

- Erkennung von schwacher Verschlüsselung bereits im Moment der Implementierung

ERKENNUNG VON UND SCHUTZ VOR IMPERSONATION

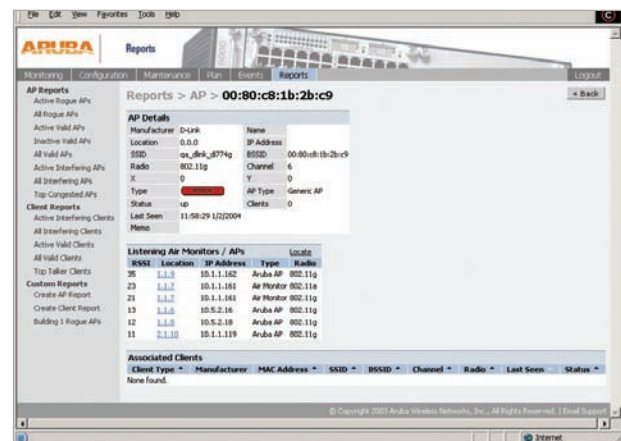
- Spoofing von MAC-Adressen
- Betrügerische Imitationen von Access Points
- Man-in-the-Middle-Angriffe
- Erkennung von Anomalien in der Sequenznummer

Erkennung ist nur ein Schritt bei der Absicherung der Umgebung vor unerwünschtem drahtlosem Zugriff. Angemessene Maßnahmen zur schnellen Beendigung nicht autorisierter Zugriffe sind von enormer Bedeutung beim Schutz sensibler Daten und Netzwerkressourcen. Um dies zu erreichen, benötigen Sie entsprechende Methoden zur Klassifizierung von Access Points und Stationen (z. B. gültig, nicht autorisiert, benachbart) sowie zur Bereitstellung automatisierter Reaktionen auf mögliche nicht autorisierte Zugriffsversuche.

Die Access Points von Aruba scannen kontinuierlich sämtliche Kanäle des Funkspektrums, überwachen den 802.11-Datenverkehr und untersuchen vor Ort die erfassten Daten. An den Aruba Mobility Controller werden dann nur tatsächliche Verletzungen der Richtlinien gesendet, damit die Aus-

wirkungen auf die Leistung des kabelgebundenen Netzwerks so weit wie möglich minimiert werden. Während des Scanvorgangs trägt das System Informationen sämtlicher drahtloser Access Points und Stationen zusammen und klassifiziert diese Geräte auf Basis des kabelgebundenen wie drahtlosen Datenverkehrs. Informationen über den Datenverkehr werden gesammelt und auf dem Mobility Controller miteinander in Verbindung gebracht.

Das WIP-Modul von Aruba verfügt sowohl über Erkennungs- als auch über Schutzfunktionen, damit Systemadministratoren auf versehentlichen wie auch auf böswärtigen Zugriff auf das Drahtlosnetzwerk angemessen reagieren können.



Nicht autorisierte Access Points genau erkennen und deaktivieren

ERKENNUNG UND DEAKTIVIERUNG NICHT AUTORISierter ACCESS POINTS

Die adaptive drahtlose Infrastruktur von Aruba erlaubt Access Points, die den WLAN-Clients zur Verfügung stehen, während diese die Umgebung nach nicht autorisierten Zugriffsversuchen scannen. Optional kann sie auch so konfiguriert werden, dass sie nur eine einzige Funktion erfüllt. Air Monitoring erkennt nicht autorisierte Access Points und Geräte, auch solche auf MIMO-Band und Bändern vor 802.11n. Erkannte Geräte werden als nicht autorisiert klassifiziert und können automatisch deaktiviert werden. Administratoren werden darüber hinaus auch über das Vorhandensein dieser Geräte informiert, wobei hier zur einfacheren Lösung des Problems auch deren exakte Position auf einem Grundriss angezeigt wird.

ARUBAOS WIRELESS INTRUSION PROTECTION MODULE

EINZIGARTIGE KLASSIFIKATION VON STANDORTEN UND BENUTZERN

Das patentierte System von Aruba identifiziert und klassifiziert automatisch sämtliche mit dem Netzwerk verbundenen Access Points und Stationen, um so die Anzahl möglicher Fehlalarme zu minimieren. Das System setzt auf eine innovative Logik, zu der unter anderem die Analyse der Datenverkehrsmuster, der Vergleich des kabelgebundenen und drahtlosen Datenverkehrs sowie Informationen zum Standort der Geräte gehören. Mit Hilfe dieser Logik können entdeckte Geräte und Access Points entsprechend klassifiziert werden: entweder als echte Bedrohungen und nicht autorisiert oder als Geräte, die zu benachbarten Netzwerken gehören.

SCHUTZ VOR DENIAL OF SERVICE-ANGRIFFEN UND IMPERSONATION

Aufgrund der offenen Beschaffenheit des Mediums sind Drahtlosnetzwerke attraktive Ziele für Denial of Service-Angriffe. Zu diesen gehören z. B. Software, die das Netzwerk mit Assoziierungs-Anfragen überflutet, Angriffe, die einen einzigen Laptop wie Tausende von Access Points erscheinen lassen oder Deauthentication-Flooding, bei dem gefälschte Deauthentifizierungs-Pakete gesendet werden. Mit dem ArubaOS WIP-Modul ausgestattete Aruba Mobility Controller kennen diese Signaturen vieler verschiedener drahtloser Angriffe und können diese abwehren, damit die Dienstverfügbarkeit nicht beeinträchtigt wird.

Ein erweiterter Schutz vor Denial of Service (DoS)-Angriffen bewahrt Unternehmen vor einer Vielzahl von drahtlosen Angriffen, darunter Association- und Deauthentication-Flooding, Honeyspots sowie gefälschten Access Points und Stationen. Basierend auf Standortsignaturen und Client-Klassifizierungen verwerfen die Access Points von Aruba illegale Anfragen und informieren Administratoren mit einem automatischen Alarm über den Angriff.

SCHUTZ VOR MAN-IN-THE-MIDDLE-ANGRIFFEN

Einer der häufigsten Angriffe auf ein Drahtlosnetzwerk ist der Man-in-the-Middle-Angriff. Während eines solchen Angriffs gibt sich ein Hacker als berechtigter Access Point aus, fungiert als Relaisknoten und bringt Benutzer und andere Access Points so dazu, Daten über dieses nicht autorisierte Gerät zu senden. Der Angreifer kann diese Daten dann verändern und korrumpieren oder auch Routinen zur Entschlüsselung von Kennwörtern laufen lassen.

Access Points von Aruba überwachen die Netzwerkumgebung, um drahtlose Stationen zu entdecken, die sich als gültige Access Points tarnen. Sobald ein solcher Täuschungsversuch entdeckt wird, werden angemessene Gegenmaßnahmen eingeleitet. Mobility Controller von Aruba können auch die einzigartigen „Signaturen“ jedes drahtlosen Clients im Netzwerk verfolgen. Wird nun eine neue Station aufgespürt, die sich zwar als ein bestimmter Client ausgibt, aber nicht über dessen passende Signatur verfügt, wird vor einem Angriff in Form einer bössartigen Imitation einer Station gewarnt.

DEFINITION UND DURCHSETZUNG VON RICHTLINIEN

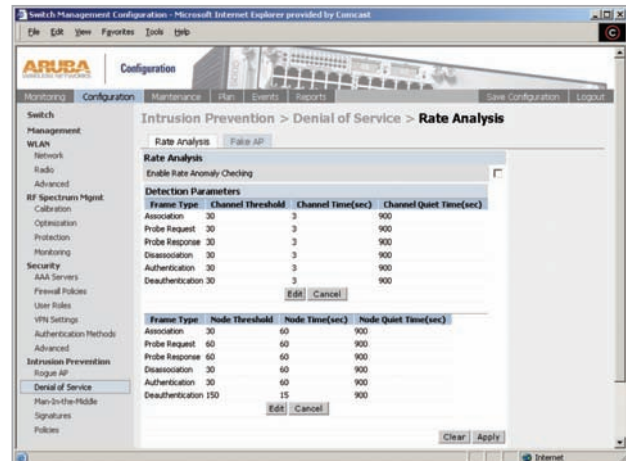
Das ArubaOS WIP-Modul verfügt über eine Reihe von Richtlinien, die so konfiguriert werden können, dass sie bei einem Verstoß automatisch reagieren. Zu den Richtlinien für den Drahtlosbetrieb gehören z. B. die Erkennung schwacher WEP-Schutzmaßnahmen bereits im Moment der Implementierung, der Schutz vor fehlerhafter Konfiguration von Access Points, die Erkennung von und der Schutz vor Ad-hoc-Netzwerken, die Erkennung nicht autorisierter NIC-Typen sowie die Erkennung von Wireless Bridges.

EINSATZ DRAHTLOSER TECHNIKEN ZUM SCHUTZ DES KABELGEBUNDENEN NETZWERKS

Auch wenn gar kein Drahtlosnetzwerk eingesetzt wird, stoppt WIP von Aruba drahtlosen Datenverkehr, bevor dieser über nicht autorisierte Access Points, die unbewusst mit einem Netzwerkport verbunden wurden, ins kabelgebundene Netzwerk gelangen kann. So wird das Netzwerk noch besser vor Sicherheitslücken in der drahtlosen Umgebung und den daraus resultierenden Angriffen geschützt. Sobald das Unternehmen soweit ist, Drahtlosnetzwerke einzusetzen, kann das System von Aruba problemlos neu konfiguriert werden, um dafür eine skalierbare und sichere Infrastruktur zu bieten.

EINSATZ DRAHTLOSER TECHNIKEN ZUM SCHUTZ DES BESTEHENDEN DRAHTLOSNETZWERKS

ArubaOS WIP vervollständigt und ergänzt jedes bestehende WLAN-Deployment (auch von Cisco) durch erweiterte Funksicherheit und -kontrollfunktionen, die in der ersten Generation drahtloser Produkte noch nicht möglich waren.



Wireless Intrusion Protection erkennt alle möglichen Bedrohungen aus der Funkumgebung



WWW.ARUBANETWORKS.COM

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