Bieten Sie Unabhängigkeit und Mobilität, ohne auf Sicherheit zu verzichten.

Sicherheit im Wireless LAN mit Cisco Aironet

Die Cisco Aironet Serie – drahtlose Unabhängigkeit mit Sicherheit

Die wichtigsten Daten Ihres Unternehmens nehmen den Weg über Ihr Netzwerk. Deshalb ist es extrem wichtig, auch für die Sicherheit dieser Daten zu sorgen. Wegen Sicherheitsbedenken verzichten manche Netzwerkmanager darauf, drahtlose Netzwerke (WLANs) zu installieren – ungeachtet ihrer zahlreichen Vorzüge.

Die Welt der drahtlosen Sicherheit hat sich aber verändert und IT-Manager können ohne Bedenken WLANs installieren. Heute gibt es für Unternehmen die Cisco® Wireless Security Suite – eine Standard-basierende WLAN-Sicherheitslösung für Produkte der Cisco Aironet® Serie und Cisco Compatible WLAN-Client-Geräte.

Folgende Leistungsmerkmale bietet die Cisco Wireless Security Suite:

- Wirksame, gegenseitige Authentifizierung sowie dynamische Schlüsselverwaltung durch Unterstützung von IEEE 802.1X
- Datenverschlüsselung mithilfe von Temporal Key Integrity Protocol (TKIP) und Wired Equivalent Privacy (WEP) des Advanced Encryption Standards (AES)
- Leistungsfähige Erweiterungen der TKIP-Verschlüsselung wie Message Integrity Check (MIC), Paket-spezifische Schlüssel über Initialization Vector Hashing sowie Broadcast Key Rotation
- Unterstützung für eine überaus breite Palette von Authentifizierungsarten nach 802.1X sowie marktüblichen Client-Geräten und Betriebssystemen
- Entschärfung von Netzwerkangriffen
- Volle Unterstützung des 2003 eingeführten Sicherheitsstandards Wi-Fi Protected Access (WPA) und WPA Version 2 der Wi-Fi Alliance

Als führender Netzwerk-Hersteller und treibende Kraft hinter dem Einsatz drahtloser Netze eröffnet Cisco Netzwerkmanagern die Möglichkeit, Anwendern die gewünschte Unabhängigkeit zu verschaffen, ohne auf die geforderte Netzwerksicherheit zu verzichten.

Sicherheit gegen Angreifer von außen

Netzwerkmanager müssen Anwendern zu Unabhängigkeit und Mobilität verhelfen, ohne dass Angreifer Zugang zum WLAN und den übermittelten Informationen erhalten sowie Informationen, die über das Netzwerk verfügbar sind. Bei einem WLAN werden die übertragenen Daten mittels Radiowellen durch die Luft gesendet. Damit kann jedes beliebige WLAN-Client-Gerät im Einzugsbereich des Access Points Daten empfangen, die zum oder vom Access Point übermittelt werden.

Da Radiowellen Decken, Fußböden und Wände durchdringen, können übertragene Daten unbeabsichtigt Empfänger auf einem anderen Stockwerk und sogar außerhalb des Gebäudes erreichen. Durch ein WLAN verlagert sich die Grenze des Netzwerks. Ohne strenge Sicherheitsvorkehrungen kann die Einrichtung eines WLANs die gleiche Wirkung haben, als würde man überall Ethernet-Anschlüsse verteilen, selbst auf dem Parkplatz.

Network Computing 2003 WELL-CONNECTED AWARDS WINNER

Nach gründlichen Tests über zwölf Monate in einer wirklichkeitsnahen Laborumgebung verliehen die Redakteure der Zeitschrift „Network Computing“ der Cisco Aironet-Serie 1200 die Auszeichnung „Well-Connected“ für 2003 in der Kategorie „Enterprise WLAN System“. Nach dem Urteil der Netzwerk-Spezialisten ist die Cisco Aironet-Serie 1200 eine wirklich innovative Lösung, die reale Anforderungen von Unternehmen an den Netzwerkbetrieb erfüllt.

Zudem haben mehrere Forschungsberichte und Artikel die Schwachstellen von WEP-Schlüsseln deutlich gemacht, die zum Ver- und Entschlüsseln der übertragenen Daten dienen. Angreifer haben leichten Zugang zu Tools, die zum Knacken von WEP-Schlüsseln dienen, wie etwa AirSnort. Damit kann ein Hacker Datenpakete passiv überwachen, analysieren und mit den so gewonnenen Informationen den WEP-Schlüssel brechen, mit dem die Pakete verschlüsselt sind.

Netzwerkmanager sind auf Lösungen angewiesen, die ihre Netzwerke vor solchen Schwachstellen schützen, und dass WLANs das gleiche Maß an Sicherheit, Verwaltbarkeit und Skalierbarkeit bieten wie drahtgebundene LANs.

Produkt: Aironet AP1100
Ausgabe: Network Computing 12/13 2004

Warum WLAN-Sicherheit wichtig ist

Ebenso wie in drahtgebundenen Netzwerken kann niemand eine vollständig sichere Netzwerkumgebung garantieren. Deshalb müssen Schutzvorkehrungen laufend auf dem neuesten Stand sein. Netzwerkmanager und WLAN-Hersteller müssen Hackern stets einen Schritt voraus sein.

Häufig müssen Netzwerkmanager die Sicherheitsfunktionen ihres WLANs einfach nur aktivieren. Im Jahr 2001 berichtete das „Wall Street Journal“ in einem Artikel von zwei Hackern, die im Silicon Valley mit einem Laptop und einer Antenne herumfuhren und nach verstreuten WLAN-Signalen „schnüffelten“. Die Hacker konnten Signale von zahlreichen Unternehmen auffangen, die sich einfach nicht die Mühe gemacht hatten, vorhandene WLAN-Sicherheitsfunktionen zu aktivieren.

Sicherheitsexperten empfehlen Unternehmen, mehrere Abwehrschichten über das Netzwerk zu legen, um Bedrohungen zu entschärfen. Als weitere Sicherheitskomponenten kommen Firewalls, Intrusion-Detection-Systeme (IDSs) und virtuelle LANs (VLANs) in Frage. Netzwerkmanager können das Risiko dadurch reduzieren, dass sie ihre drahtlosen Netzwerke umsichtig entwerfen und installieren, bewährte Sicherheitsvorkehrungen

Mehrere nach UL 2043 brandsichere Cisco Aironet Access Points sind Mittelpunkte eines wireless-only Netzwerks oder stellen die Verbindung zwischen einem drahtgebundenen und einem drahtlosen Netz her. Sie lassen sich überall in einem Gebäude oder auf einem Firmengelände anbringen.

Durch die Cisco Aironet Access Points können sich die Anwender im vom Funk abgedeckten Standortbereich frei bewegen.

Die Cisco Wireless Security Suite sorgt für voll gesicherten, unterbrechungsfreien Zugang zu allen Netzwerk-Ressourcen. Das Cisco Structured Wireless-Aware Network unterstützt die Installation, den Betrieb und die Verwaltung von Hunderten bis Tausenden von Cisco Aironet Access Points.

einsetzen sowie Geräte und Software verwenden, die Experten auf dem Gebiet der Netzwerksicherheit entwickelt haben. Als Branchenführer im Bereich Netzwerksicherheit ist Cisco eine hervorragende Wahl für die WLAN-Implementierung. Mit den preisgekrönten Sicherheitsfeatures der Cisco Wireless Security Suite können Netzwerkmanager die Risiken für ihr Netzwerk senken und die Sicherheit im WLAN erhöhen.

Die Sicherheitslösung für Wireless LANs

Ebenso wie bei anderen Netzwerken stehen bei der WLAN-Sicherheit Zugangskontrolle und Verschlüsselung im Mittelpunkt. Eine strenge Zugangskontrolle für WLANs, auch Authentifizierung genannt, hindert nicht autorisierte Anwender daran, über die Access Points zu kommunizieren. Durch eine stabile WLAN-Zugangskontrolle kann man sicherstellen, dass berechtigte Client-Stationen nur mit vertrauenswürdigen Access Points Verbindung aufnehmen und nicht mit unberechtigten oder nicht autorisierten Access Points.

Mit Verschlüsselung im WLAN sorgt man dafür, dass nur der vorgesehene Empfängerkreis die übertragenen Daten versteht. Die Vertraulichkeit von Daten im WLAN gilt als gewahrt, wenn diese Daten mit einem Schlüssel chiffriert werden, den nur der vorgesehene Empfänger der Daten kennt. Die Verschlüsselung von Daten sorgt auch dafür, dass die Daten während des Sende- und Empfangsprozesses nicht manipuliert werden können.

Gegenwärtig setzen Unternehmen, die mit WLANs arbeiten, vier verschiedene Sicherheitsstufen für Zugangskontrolle und Datenschutz ein: Open Access, Basic Security, Enhanced Security und Remote Access Security. Wie bei allen Sicherheitsvorkehrungen empfiehlt Cisco Unternehmen, eine Risikoanalyse für das Netzwerk durchzuführen, ehe sie eine bestimmte WLAN-Sicherheitslösung auswählen und implementieren.

Open Access

Wie alle von der Wi-Fi Alliance zertifizierten Produkte werden auch die Cisco Aironet-Produkte im „Open Access“-Modus geliefert, das heißt, mit abgeschalteten Sicherheitsfunktionen. Für öffentliche Hotspots – etwa in Cafés, auf Universitätsgelände, in Flughäfen oder an anderen öffentlichen Plätzen – mag Open Access oder keine Sicherheit angemessen und akzeptabel sein. Für eine Firmenorganisation ist dies jedoch nicht geeignet. Bei der Installation von drahtlosen Geräten in Unternehmensumgebungen müssen Sicherheitsfunktionen aktiviert werden. Wie schon erwähnt schalten manche Firmen ihre WLAN-Sicherheitsfunktionen nicht an. Diese Firmen setzen ihre Netze hohen Risiken aus.

Basic Security: SSIDs, WEP und MAC-Adressen-Authentifikation

Zur Basic Security zählen der Einsatz von Service Set Identifiern (SSIDs), Open- oder Shared-Key-Authentifizierung, statische WEP-Schlüssel sowie wahlweise Media Access Control (MAC-) Authentifizierung. Diese Kombination liefert ein rudimentäres Maß an Zugangskontrolle und Datenschutz, allerdings lässt sich jede dieser Komponenten überwinden.

Eine „SSID“ ist ein gemeinsamer Netzwerkname für die Geräte in einem WLAN-Teilsystem. Eine SSID versperrt jedem Client-Gerät den Zugang, das nicht die betreffende SSID hat. Allerdings kann ein Access Point seinen SSID in seinem Beacon (Suchsignal)

verbreiten. Auch wenn das Aussenden der SSID abgeschaltet ist, kann ein Angreifer oder Hacker den SSID durch so genanntes „Sniffing“ – unbemerktes Abhören des Netzwerks – ermitteln.

Der Standard 802.11, eine vom IEEE erarbeitete Gruppe von WLAN-Normen, unterstützt zwei Methoden zur Client-Authentifizierung: Open- und Shared-Key-Authentifikation. Open-Authentifizierung erfordert wenig mehr als die Angabe der korrekten SSID. Bei der Shared-Key-Authentifizierung sendet der Access Point dem Client-Gerät ein Datenpaket mit einem Test-Text („challenge text“). Diesen Text muss der Client mit dem korrekten WEP-Schlüssel chiffrieren und zum Access Point zurücksenden. Ohne den richtigen Schlüssel schlägt die Authentifizierung fehl und der Client erhält nicht die Erlaubnis, mit dem Access Point Verbindung aufzunehmen. Die Shared-Key-Authentifizierung gilt als unsicher, weil ein Angreifer den WEP-Schlüssel dechiffrieren kann, wenn er den Test-Text sowohl als Klartext als auch den mit dem WEP-Schlüssel chiffrierten Text auffängt.

Bei der Open-Authentifizierung hindert der Einsatz von WEP einen Client daran, Daten ohne korrekten WEP-Key zum Access Point zu senden und von dort zu empfangen. Dies gilt auch, wenn der Client sich vollständig authentifizieren und mit dem Access Point Verbindung aufnehmen kann. Ein WEP-Schlüssel umfasst entweder 40 oder 128 Bit. Normalerweise wird er vom Netzwerk-Administrator am Access Point und an allen Clients, die mit ihm kommunizieren, fest vorgegeben. Wenn statische WEP-Schlüssel verwendet werden, muss ein Netzwerk-Administrator die zeitraubende Aufgabe übernehmen, an jedem Gerät im WLAN denselben Schlüssel einzugeben.

Wenn ein Gerät, das statische WEP-Schlüssel verwendet, verloren geht oder gestohlen wird, kann der Dieb oder Finder des gestohlenen Geräts auf das Netzwerk zugreifen. Solange der Diebstahl nicht gemeldet wird, kann auch kein Administrator erkennen, dass sich ein unautorisierter Anwender in das WLAN eingeschlichen hat. Anschließend muss der Administrator den WEP-Schlüssel auf jedem Gerät ändern, das denselben statischen WEP-Schlüssel verwendet wie das fehlende Gerät. In einem großen Unternehmens-WLAN mit Hunderten oder sogar Tausenden von Anwendern kann sich das zu einer gewaltigen Aufgabe auswachsen. Noch schlimmer: Wird ein statischer WEP-Schlüssel durch ein Tool wie AirSnort dechiffriert, dann hat der Administrator keine Möglichkeit zu erfahren, dass der Schlüssel durch einen Angreifer entwertet worden ist.

Manche WLAN-Anbieter unterstützen Authentifizierung auf der Basis der physikalischen Adresse der Netzwerkkarte des Clients, der so genannten MAC-Adresse. Ein Access Point gestattet nur dann den Verbindungsaufbau durch einen Client, wenn sich dessen MAC-Adresse in einer Authentifikationstabelle des Access Points wieder findet. Doch ist MAC-Authentifizierung eine unzureichende Sicherheitsvorkehrung, denn MAC-Adressen lassen sich fälschen und Netzwerkkarten können verloren gehen oder gestohlen werden.

Basic Security mit einem WPA Pre-Shared Key

Als weitere Form von Basic Security ist jetzt der WPA Pre-Shared Key (PSK) verfügbar. Dieser Mechanismus verifiziert Anwender sowohl an der Client-Station als auch am Access Point über ein Passwort, beziehungsweise einen Identifizierungscode. Ein Client erhält nur dann Zugriff auf das Netzwerk, wenn sich die Passwörter des Clients und

des Access Points gleichen. Das Passwort liefert auch das Schlüsselmaterial, mit dem TKIP einen Chiffrierschlüssel für jedes übertragene Datenpaket erzeugt. WPA PSK ist zwar sicherer als WEP, ähnelt aber insofern dem statischen WEP, als der PSK auf der Client-Station gespeichert wird und seinen Wert verlieren kann, wenn dieses Gerät verloren geht oder gestohlen wird. Empfohlen wird eine starke PSK-Codesequenz mit einer Mischung aus Buchstaben, Ziffern und Sonderzeichen. Verbreitet ist diese Security-Maßnahme überwiegend im Home-Bereich und bei sehr kleinen Unternehmen.

Basic Security – Zusammenfassung

Basic WLAN Security, das sich auf eine Kombination von SSIDs, Open-Authentifizierung und statischen WEP-Schlüsseln stützt sowie WPA PSK reichen nur für sehr kleine Firmen sowie Unternehmen aus, die ihren WLAN-Netzwerken keine unternehmenskritischen Daten anvertrauen. Alle anderen Organisationen müssen in eine robuste WLAN-Sicherheitslösung der Enterprise-Klasse investieren.

Enhanced Security – die Vorteile der Cisco Wireless Security Suite

Enhanced Security wird für alle Kunden empfohlen, die wirkliche Sicherheit benötigen. Die Cisco Wireless Security Suite ist eine leistungsfähige Sicherheitslösung und bietet volle Unterstützung für WPA und seine Bausteine 802.1X mit TKIP. Die Cisco Wireless Security Suite umfasst folgende Leistungsmerkmale:

- Starke gegenseitige Authentifizierung und dynamische Benutzer- und Sitzungsspezifische Chiffrierschlüssel durch 802.1X
- Erweiterungen zur RC4-Verschlüsselung wie Key-Hashing (Paket-spezifische Verschlüsselung), Message Integrity Check (MIC), Wechsel des Initialisierungsvektors (IV) sowie Broadcast Key Rotation durch TKIP – der Advanced Encryption Standard (AES) für WPAv2 erlaubt die Verschlüsselung auf Basis eines weithin akzeptierten Standards auf höchstem Niveau. AES wurde im VPN-Bereich eingesetzt und zeichnet sich durch höchste Sicherheit aus.

Bei der Cisco Wireless Security Suite handelt es sich um eine Enhanced-Security-Lösung. Mit ihr können Netzwerk-Administratoren darauf vertrauen, dass sie WLANs mit hoher Datensicherheit und bestem Angriffsschutz einrichten.

VPN und Wireless LAN Security

In manchen Fällen benötigen Firmen übergreifende Sicherheit für den Schutz ihrer Unternehmensanwendungen. Mit Remote Access VPNs richten Administratoren ein virtuelles privates Netzwerk (VPN) ein. Damit können mobile Anwender an öffentlichen Hotspots – etwa in Flughäfen, Hotels oder Kongresszentren – eine Tunnelverbindung ins Firmennetz aufbauen.

Manche Unternehmen, etwa Geldinstitute, benötigen weiter reichende Sicherheitsvorkehrungen und implementieren eventuell auch innerhalb ihres internen Netzes VPN für WLANs. Normalerweise erfüllt die Cisco Aironet-Lösung die Anforderungen hinsichtlich der Wireless Security für die meisten Firmennetze. Ein zusätzlich überlagertes VPN mit seinem Extra-Aufwand, seinen Einschränkungen und seinen Kosten erübrigt sich.

Weitere Informationen über den Einsatz von VPNs in WLANs und die Installation einer Enhanced-WLAN-Security-Lösung finden Sie in dem Whitepaper „Cisco SAFE:

Wireless LAN Security in Depth“. Mit „SAFE Blueprints“ verfolgt Cisco einen modularen Ansatz zur Sicherung von WLANs. Darin werden Design, Implementierung und Managementprozesse im Bereich der Sicherheit dargestellt.

Zuverlässige Sicherheit mit der Cisco Wireless Security Suite

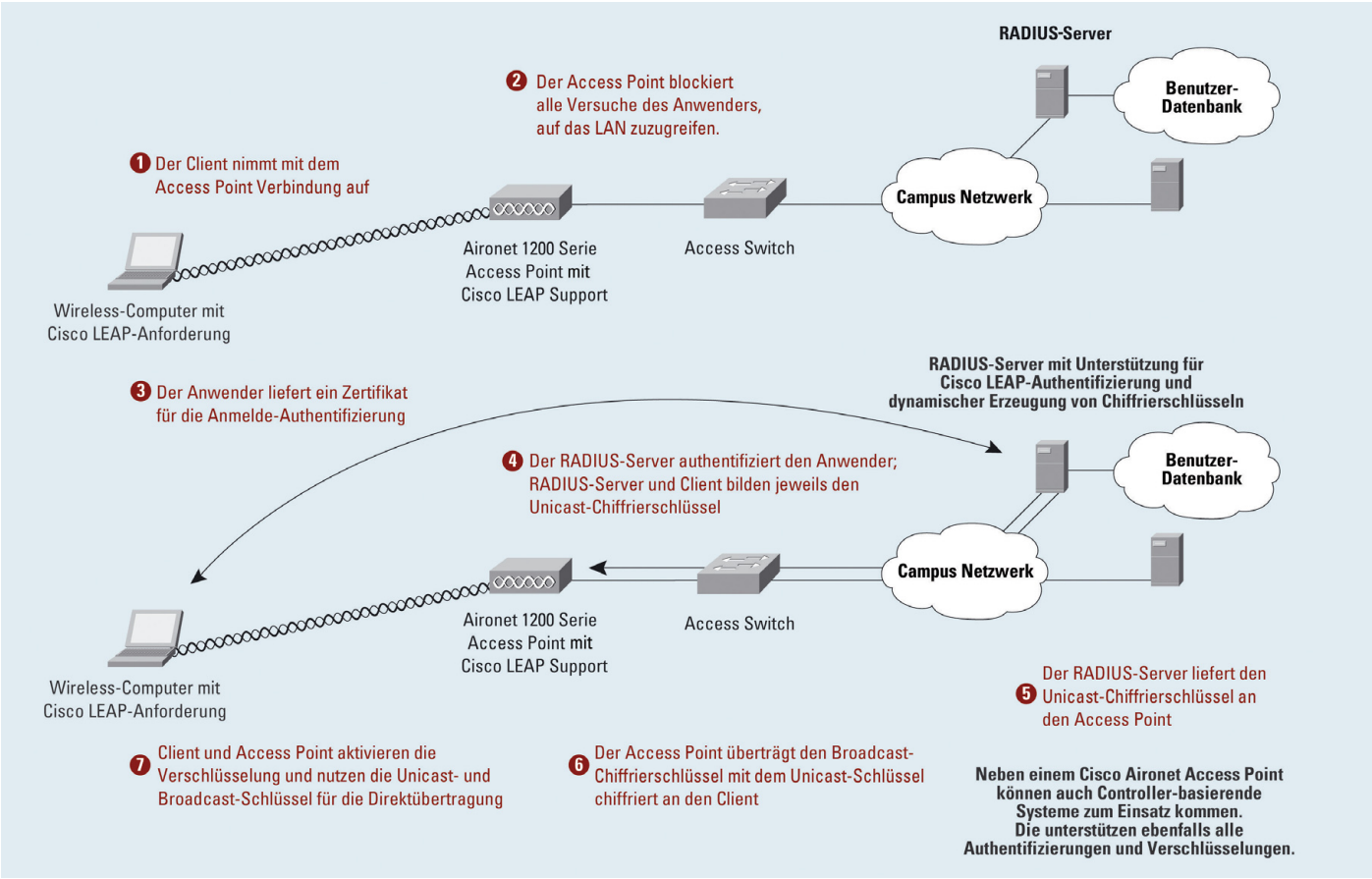
Für die Einrichtung umfangreicher, unternehmensweiter WLANs benötigen Netzwerk-Administratoren eine skalierbare, problemlose Sicherheitsverwaltung, die dem IT-Personal keine Mehrbelastung bringt. Bei der Cisco Wireless Security Suite brauchen Administratoren keine statischen Chiffrierschlüssel zu verwalten.

Die Cisco Wireless Security Suite für die Cisco Aironet-Serie liefert wichtige Wireless-Sicherheitsdienste, die der in drahtgebundenen LANs verfügbaren Sicherheit entspricht. Die Cisco Wireless Security Suite liefert Netzwerkmanagern eine erstklassige Sicherheitslösung, die Anwendern Freiheit und Mobilität bietet und zugleich für eine sichere Netzwerkumgebung sorgt.

Die Cisco Aironet-Lösung verhindert passive und aktive WLAN-Angriffe und bietet zuverlässiges, skalierbares, zentrales Sicherheitsmanagement. Sie unterstützt

- Wi-Fi Protected Access (WPA) und WPAv2
- Cisco Structured Wireless-Aware Network (SWAN)
- Cisco Aironet Access Points und Client-Adapter für Wireless-LANs und Controller-basierende Systeme
- Cisco Compatible WLAN-Client-Geräte

Erstklassige Sicherheit mit der Cisco Wireless Security Suite



Authentifizierung nach 802.1X und das Extensible Authentication Protocol

Das IEEE hat 802.1X als Standard für die Authentifizierung in drahtgebundenen und drahtlosen Netzwerken angenommen. Dieser Standard liefert in WLANs starke, gegenseitige Authentifizierung zwischen einem Client und einem Authentication-Server. Darüber hinaus sorgt 802.1X für dynamische Anwender- und Sitzungs-spezifische Chiffrierschlüssel und beseitigt damit den administrativen Aufwand und die Sicherheitsprobleme, die statische Chiffrierschlüssel mitbringen. Bei 802.1X werden die Zertifikate, die zur Authentifizierung dienen – etwa Kennwörter für die Anmeldung – niemals im Klartext, das heißt unverschlüsselt, über das drahtlose Medium übermittelt.

Es gibt mehrere 802.1X-Authentifikationsarten. Jede liefert einen anderen Ansatz für die Authentifizierung, stützt sich dabei aber auf dasselbe Funktionsschema und das Extensible Authentication Protocol (EAP) für die Kommunikation zwischen einem Client und einem Access Point. Die Cisco Aironet-Produkte unterstützen mehr 802.1X EAP Authentifikationsarten als alle anderen WLAN-Fabrikate. Zu den unterstützten Typen zählen: Cisco LEAP, EAP-Transport Layer Security (EAP-TLS) sowie Varianten, die über EAP-TLS arbeiten, wie Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-TTLS) sowie EAP-Subscriber Identity Module (EAP-SIM).

Cisco empfiehlt Kunden, ihre Netzwerke und die Sicherheitsumgebung zu analysieren und danach die beste EAP-Authentifikationsart für ihre 802.1X-Installation auszuwählen. Zu den für die Auswahl des EAP-Typs zu beurteilenden Punkten zählen: der für die Sicherheitszertifikate verwendete Sicherheitsmechanismus, die Datenbank für die Benutzer-Authentifizierung, die verwendeten Client-Betriebssysteme, welche Clients zu authentifizieren sind, die Art der benötigten Anwender-Anmeldung sowie die Server für Remote Authentication Dial-In User Service (RADIUS) oder Authentication, Authorization and Accounting (AAA).

Jedes EAP-Verfahren hat seine Vor- und Nachteile. Dabei sind Abstriche zu machen entweder bei der verfügbaren Sicherheit, der Verwaltbarkeit des EAP-Typs, den unterstützten Betriebssystemen und Client-Geräten, dem Aufwand bei Client-Software und Datenaustausch für die Authentifizierung, den Zertifikat-Erfordernissen, der Anwenderfreundlichkeit oder den unterstützten Geräten für die WLAN-Infrastruktur. Um spezielle Anforderungen der Authentifizierung von Client-Geräten oder von Anwendern zu erfüllen, kann man auch mehrere EAP-Arten innerhalb eines Netzes verwenden.

Für die 802.1X-Authentifizierung lässt sich eine breite Auswahl an RADIUS-Servern einsetzen, etwa der Cisco Secure Access Control Server (ACS) und der Cisco CNS Access Registrar® sowie AAA-RADIUS-Server anderer Hersteller wie Funk-Software (Steel-Belted RADIUS) oder Interlink Networks (AAA RADIUS).

Die Authentifizierung nach 802.1X authentifiziert eine Client-Station durch Zertifikat des Anwenders und nicht anhand eines physikalischen Attributs des Client-Geräts. Dies minimiert die mit dem Verlust des Geräts oder seiner WLAN-Interfacekarte verbundenen Risiken. Dazu bietet 802.1X weitere Vorteile, darunter die Entschärfung von Authentifizierungsangriffen wie „Man-in-the-Middle“-Attacken, zentrales Schlüsselmanagement mit Regel-basierter Schlüsselrotation und Schutz vor so genannten „Brute-Force“-Angriffen.

Zentrales Richtlinien(Policy)-Management für WLAN-Anwender

Ein weiterer Vorteil der 802.1X-Authentifikation ist die zentrale Verwaltung von WLAN-Anwendergruppen, mit regelorientierter Schlüsselrotation, dynamischer Schlüsselzuweisung, dynamischer VLAN-Zuweisung und SSID-Beschränkung. Diese Funktionen lassen die Chiffrierschlüssel rotieren, sie weisen die Anwender spezifischen VLANs zu und stellen dadurch sicher, dass Anwender nur zu bestimmten Ressourcen Zugang haben.

Nach erfolgreichem Abschluss der gegenseitigen Authentifizierung bilden der Client und RADIUS denselben Chiffrierschlüssel, mit dem sämtliche ausgetauschte Daten verschlüsselt werden. Über einen sicheren Kanal im drahtgebundenen Netzwerk sendet der RADIUS-Server den Schlüssel zum Access Point, der speichert ihn für diesen Client. Das Ergebnis sind Anwender- und Sitzungs-spezifische Chiffrierschlüssel. Dabei bestimmt eine auf dem RADIUS-Server festgelegte Richtlinie die Dauer der Sitzung. Wenn eine Sitzung endet oder der Client von einem Access Point zum nächsten wandert, findet eine neue Authentifizierung statt, die auch einen neuen Sitzungsschlüssel erzeugt. Diese erneute Authentifizierung erfolgt transparent für den Anwender.

In Verbindung mit den Chiffrierschlüsseln und der Zeitangabe für die Neu-Authentifizierung werden auch Angaben zur VLAN ID und SSID-Beschränkung an den Access Point übergeben. Wenn der Access Point eine entsprechende VLAN-ID-Zuweisung erhält ordnet er den Anwender der betreffenden VLAN ID zu. Wenn auch die Liste erlaubter SSIDs an den Access Point übergeben wird, stellt er auch mit sicher, dass der Anwender eine gültige SSID für den Zugang zum WLAN liefert. Wenn der Anwender eine SSID angibt, die in der Liste zulässiger SSIDs nicht enthalten ist, trennt der Access Point diesen Anwender vom WLAN.

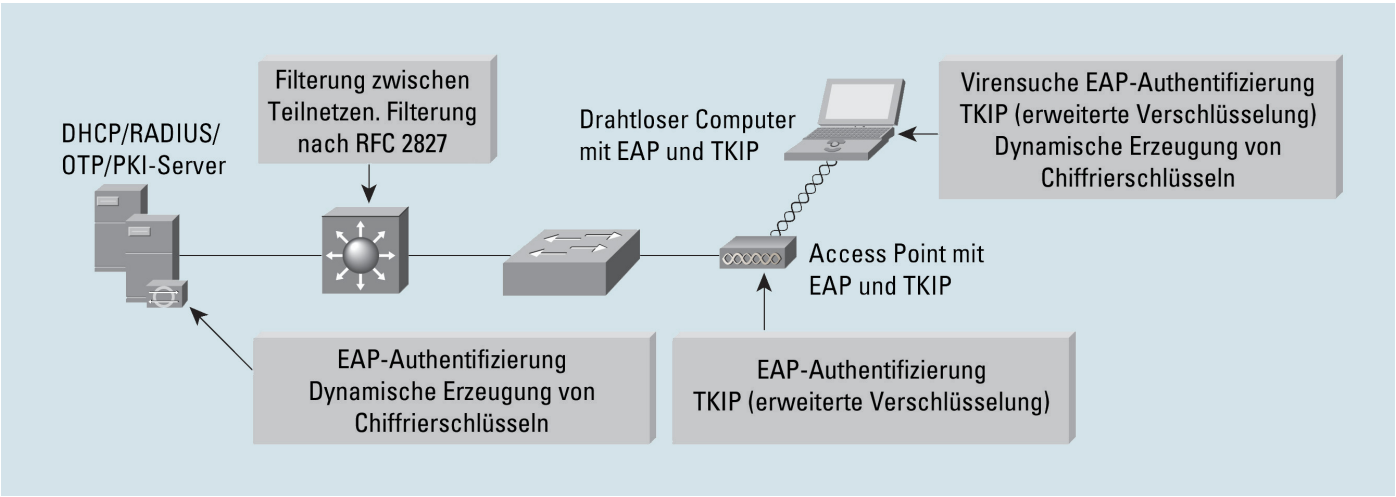
Brute-Force-Angriffe entschärft

Herkömmliche WLAN-Implementierungen auf der Basis statischer Chiffrierschlüssel sind sehr anfällig für so genannte „Brute-Force"-Netzwerkangriffe. Bei einem solchen Angriff versucht ein Angreifer einen Chiffrierschlüssel zu ermitteln, indem er einen Wert nach dem anderen ausprobiert. Beim standardmäßigen 128-Bit-WEP erfordert dies die Prüfung von maximal 2104 verschiedenen Schlüsseln. Bei dem Einsatz von dynamischen Anwender- und Sitzungs-spezifischen Chiffrierschlüsseln nach 802.1X bleibt ein Brute-Force-Angriff zwar theoretisch noch möglich. Er ist aber äußerst schwierig durchzuführen und so gut wie aussichtslos.

Das Temporal Key Integrity Protocol

Zwar bringen die Authentifizierungsarten nach 802.1X WLANs starke Authentifizierung, die Standard-WEP-Verschlüsselung nach 802.11 ist aber weiterhin anfällig für Netzwerkangriffe. Die Cisco Wireless Security Suite unterstützt TKIP mit sowohl statischen als auch dynamischen Chiffrierschlüsseln. Wie auch WEP verwendet TKIP eine von Ron Rivest entwickelte Verschlüsselungsmethode, bekannt als „Ron's Code 4 Encryption" (RC4). Allerdings sind bei TKIP zusätzliche Vorkehrungen wie Paket-spezifisches Key-Hashing, MIC und Broadcast Key Rotation vorgesehen, die bekannte Schwachstellen von WEP berücksichtigen.

Mit der Cisco Wireless Security Suite stehen auf Cisco Aironet Access Points sowie Cisco und Cisco Compatible WLAN Client-Geräten TKIP-Algorithmen sowohl von Cisco als auch nach WPA zur Verfügung. Zwar arbeiten Cisco TKIP und WPA TKIP



Funktionen bei der Abwehr von Angriffen im Standard-EAP-WLAN-Design

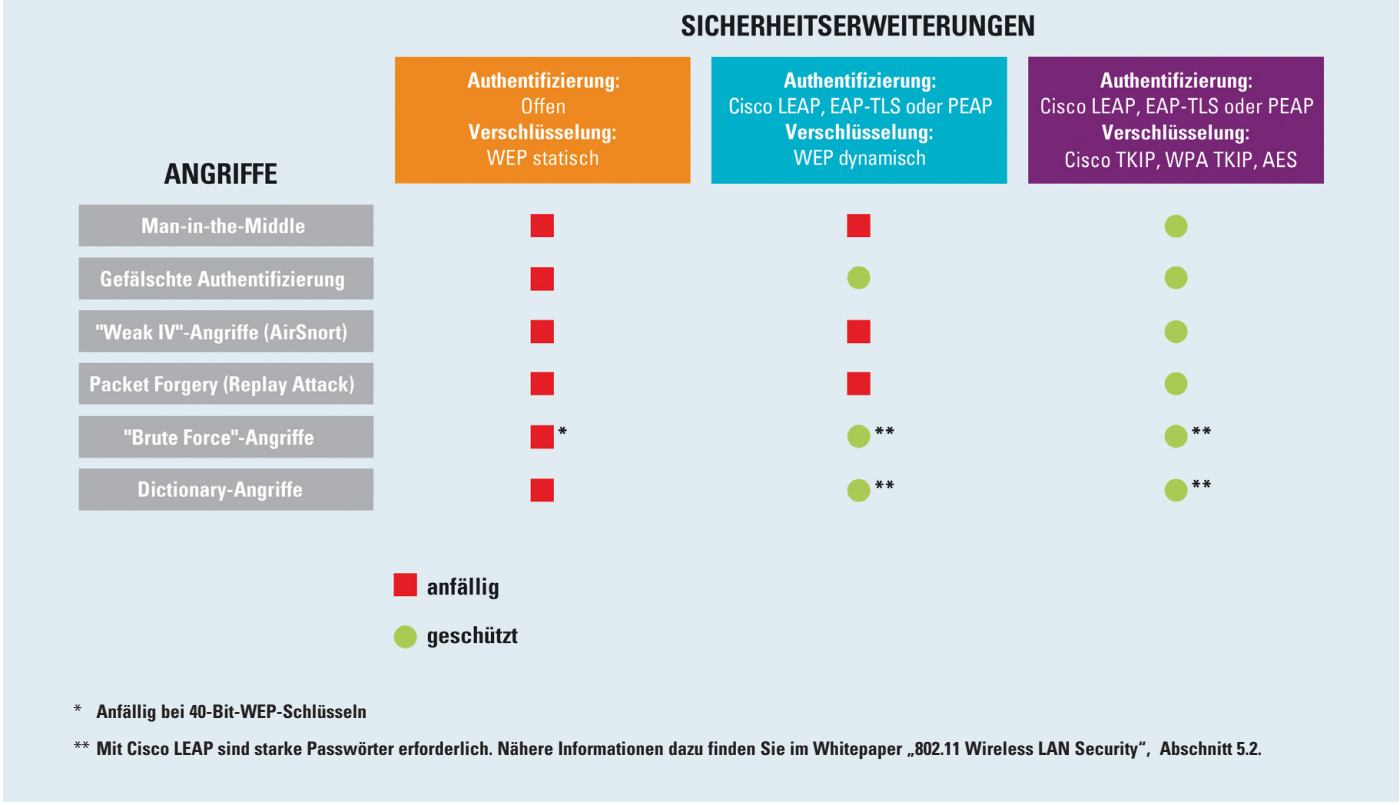
nicht zusammen, doch können die Access Points Cisco TKIP und WPA TKIP gleichzeitig auf unterschiedlichen VLANs verwenden. System-Administratoren müssen dann eine Gruppe von TKIP-Algorithmen auf den Client-Geräten auswählen, denn auch die Clients können nicht beide TKIP-Algorithmen gleichzeitig unterstützen.

Bei Installationen, die ausschließlich mit Client-Geräten von Cisco arbeiten, wird Cisco TKIP sowohl für die Access Points als auch für die Clients empfohlen. In gemischten Umgebungen empfiehlt Cisco für die Access Points sowohl Cisco TKIP als auch WPA TKIP Algorithmen. Damit können vorhandene Cisco und Cisco Compatible Client-Geräte Cisco TKIP verwenden; für alle anderen Client-Geräte wird WPA TKIP empfohlen.

Paket-spezifisches Key Hashing entschärft „Weak IV"-Angriffe

Wenn übertragene Daten mit einem WEP-Schlüssel chiffriert und dechiffriert werden, enthält jedes Paket einen Initialisierungsvektor (IV). Es handelt sich dabei um ein 24 Bit langes Feld, das sich mit jedem Paket ändert. Der Key-Scheduling-Algorithmus von RC4 bildet den IV-Vektor aus dem WEP-Basisschlüssel. Dabei erlaubt jedoch ein Fehler in der WEP-Implementierung von RC4 die Bildung „schwacher" IV-Vektoren, die auf den Basisschlüssel zurückschließen lassen. Mit einem Tool wie AirSnort kann ein Angreifer diesen Fehler ausnutzen, indem er mit ein und demselben Schlüssel chiffrierte Pakete sammelt und mithilfe des schwachen IV-Vektors den Basisschlüssel ermittelt.

Cisco TKIP und WPA TKIP bieten Key-Hashing, das heißt Paket-spezifische Verschlüsselung, um Weak-IV-Angriffe abzuwehren. Wenn die Unterstützung für Key-Hashing am Access Point sowie auf allen verbundenen Client-Geräten eingerichtet ist, rechnet der Datensender den Basisschlüssel per Hash-Funktion mit dem IV-Vektor um und erzeugt so für jedes Datenpaket einen neuen Schlüssel. So sorgt Key-Hashing dafür, dass jedes Paket mit einem anderen Schlüssel chiffriert wird, und beseitigt damit die Vorhersagbarkeit, auf die sich ein Angreifer stützt, um durch Ausnutzen der IV-Vektoren den WEP-Schlüssel zu ermitteln.



* Anfällig bei 40-Bit-WEP-Schlüsseln

** Mit Cisco LEAP sind starke Passwörter erforderlich. Nähere Informationen dazu finden Sie im Whitepaper „802.11 Wireless LAN Security", Abschnitt 5.2.

Neue Sicherheitserweiterungen entschärfen Netzwerk-Angriffe

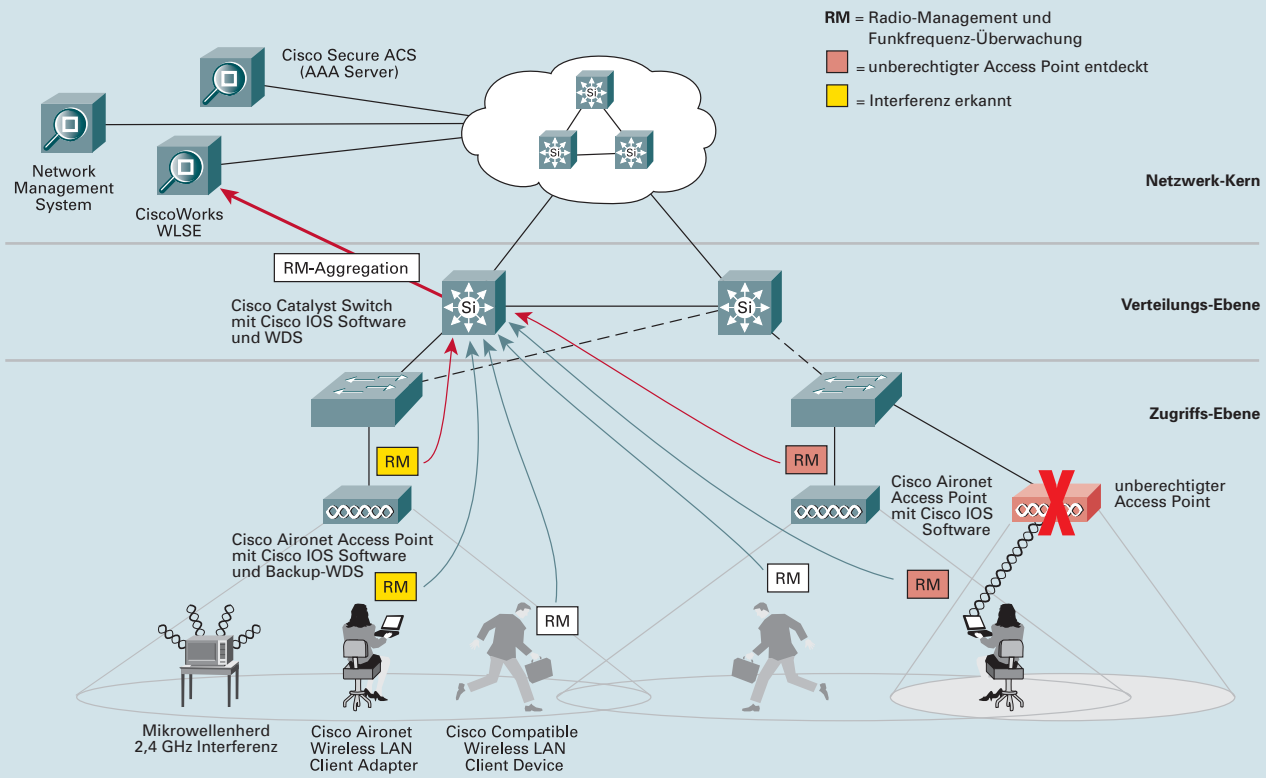
Message Integrity Check Protection schützt vor Active-Network-Angriffen

Mit einem MIC lässt sich der Active-Network-Angriff durchkreuzen, der dazu dient, den Schlüssel zu ermitteln, mit dem abgefangene Pakete chiffriert sind. Es handelt sich hierbei um eine Kombination des Bit-Flipping- mit dem Replay-Angriff. Wenn MIC-Unterstützung am Access Point sowie auf allen verbundenen Client-Geräten eingerichtet ist, fügt der Sender eines Datenpakets diesem Paket einige Bytes (MIC) hinzu, ehe er es verschlüsselt und versendet. Der Empfänger entschlüsselt das Paket nach dem Eintreffen und prüft den MIC-Wert. Wenn der MIC in dem Frame dem (mit der MIC-Funktion) berechneten Wert entspricht, akzeptiert der Empfänger das Paket, andernfalls verwirft er es.

Mithilfe des MIC werden Pakete eliminiert, die unterwegs in böswilliger Weise geändert wurden. Cisco Aironet-Produkte sind MIC-fähig. Sie erkennen geänderte Pakete und weisen sie ab. Daher können Angreifer das Netzwerk nicht mit Bit-Flipping- oder Active-Replay-Angriffen dazu verleiten, sie zu authentifizieren.

Broadcast-Key Rotation

Mit der Cisco Wireless Security Suite können Netzwerkmanager sowohl die Unicast- als auch die Broadcast-Schlüssel rotieren, die zur Chiffrierung von Broadcast- und Multicast-Sendungen dienen. Die Netzwerkmanager konfigurieren die Regeln für die Broadcast-Key-Rotation an den Access Points. Da ein statischer Broadcast-Schlüssel gegenüber denselben Angriffen anfällig ist wie Unicast-Schlüssel oder statische WEP-Schlüssel, wird ein Rotationswert für die Broadcast-Schlüssel geliefert, die diese Schwachstelle beseitigt.



1. **Clients und Access Points senden ihre Radio-Management(RM)-Daten für die Funkfrequenzverwaltung zum Access Point, Switch oder Router von Cisco, der mit wireless-fähiger IOS-Software arbeitet und Wireless Domain Services (WDS) bietet.**
2. **Mithilfe von RM-Aggregation verdichtet der mit wireless-fähiger IOS-Software arbeitende Access Point, Switch oder Router die RM-Daten, setzt sie in ein System kurzer Meldungen um und sendet diese Nachrichten an das CiscoWorks WLSE.**

IEEE 802.11i, WPA2 und der Advanced Encryption Standard

Seit November 2004 unterstützt die Cisco Wireless Security Suite auch IEEE 802.11i und WPA2. IEEE 802.11i ist der vorgeschlagene IEEE-Standard für WLAN-Sicherheit, und bei WPA2 handelt es sich um den Nachfolger von WPA. Sowohl 802.11i als auch WPA2 enthalten AES als Alternative zum TKIP.

Das Cisco Structured Wireless-Aware Network

Netzwerkmanager benötigen WLANs, die Sicherheit, Skalierbarkeit, Zuverlässigkeit, Installationsfreundlichkeit und Verwaltung auf demselben Niveau bieten wie von drahtgebundenen LANs gewohnt. Das Cisco Structured Wireless-Aware Network (SWAN) ist eine sichere, integrierte Wireless-LAN(WLAN)-Lösung aus wireless-fähigen („wireless aware“) Infrastrukturprodukten. Sie minimiert die WLAN-Gesamtkosten durch optimierte Installation und Verwaltung von Cisco Aironet Access Points, die sich im Markt bewährt haben und hohe Leistung sowie eine reiche Funktionsvielfalt bieten. Cisco SWAN bringt drahtlosen LANs dasselbe Niveau an Sicherheit, Skalierbarkeit, Zuverlässigkeit, Installationsfreundlichkeit und Verwaltung, wie es Kunden von ihren drahtgebundenen LANs gewohnt sind.

Cisco SWAN besteht aus vier Hauptkomponenten. Sein Funktionsumfang lässt sich durch Cisco und Cisco Compatible Client-Geräte erweitern. Künftig wird dies auch durch wireless-aware Infrastrukturprodukte für LANs von Cisco möglich sein, die integrierte Funktionen für drahtgebundene und drahtlose LANs bieten.

Die Kernkomponenten

- Mit Cisco IOS®-Software arbeitende Access Points der Cisco Aironet-Serie
- Die CiscoWorks Wireless LAN Solution Engine (WLSE) – als Alternative dazu Cisco Wireless LAN Controller und WCS als Management
- Ein IEEE 802.1X Authentication-Server, etwa der Cisco Secure Access Control Server (ACS)
- Wi-Fi-zertifizierte WLAN-Client-Adapter – Cisco Wireless Router 18xx oder 8xx

Optionale Komponenten

Mit folgenden Optionen erhalten Sie eine breite Palette von zusätzlichen Sicherheitsoptionen einschließlich sämtlicher Authentifizierungsarten nach 802.1X und erweiterten Funktionen zur Funkfrequenz-Verwaltung (Radio Management):

- Cisco Aironet Wireless LAN Client-Adapter
- Cisco Compatible Wireless LAN Client-Geräte

Vorteile: Kostenminimierung, Verfügbarkeit, Sicherheit

Cisco SWAN optimiert folgende Bereiche und sorgt damit für minimale Gesamtkosten sowie höchste Verfügbarkeit und Sicherheit von Netzwerken:

Einrichtung

- Unterstützung bei der Ausleuchtung (assisted site surveys)
- Funkfrequenz-Scannen und Überwachung „live“
- Interferenz-Erkennung
- Selbstkonfiguration neuer Access Points

Verwaltung

- Vereinfachter, automatisierter Funkbetrieb von vielen Access Points von einer einzigen Management-Konsole
- Erweiterte Fehlersuch- und Diagnosetools sowie Client- und Nutzungsberichte
- Hohe Verfügbarkeit durch selbst heilende so genannte „selfhealing“ Wireless-LANs
- Massen-Konfiguration und Firmware-Aktualisierung
- XML-API für Datenexport

Sicherheit

- Erkennung und Ortung unberechtigter Access Points
- WLAN-Betrieb auch bei unterbrochener WAN-Leitung
- Überwachung von Sicherheitsrichtlinien (mit Alarmen)
- Zentrale Sicherheitseinstellungen von Parametern wie 802.1X EAP und WPA
- Volle Zugangskontrolle und Datensicherheit mit Fast Secure Layer-2- und Layer-3-Roaming

Flexibilität

- Integrierte Dienste für drahtgebundene und drahtlose LANs mit der Cisco-Infrastruktur und Cisco IOS-Software
- Erweiterungen für Cisco Switches und Router

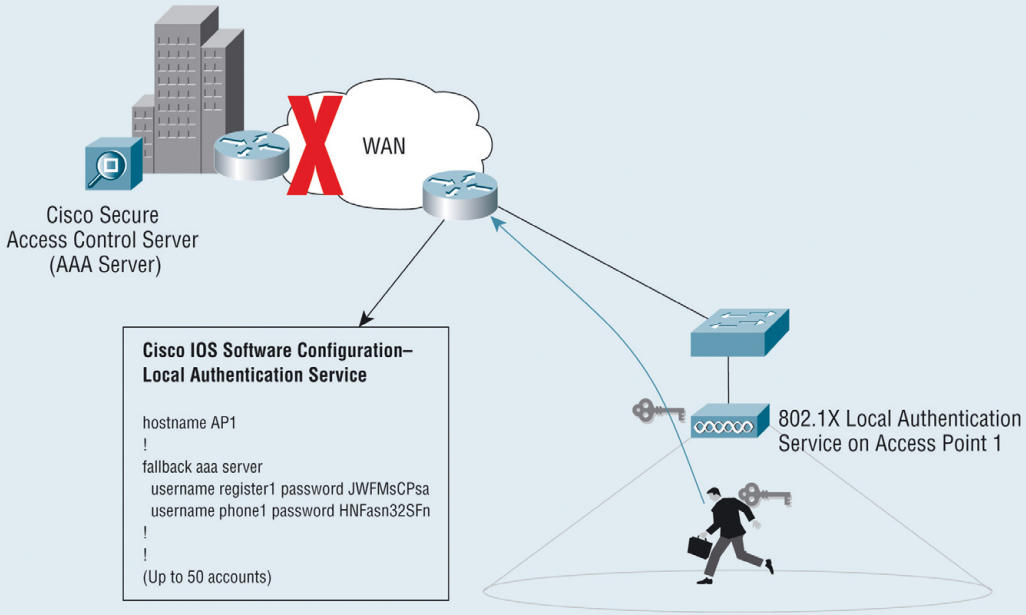
Support

- Gewährleistung und Support-Dienste von Cisco und Partnern sowie Partnerschaften mit anderen Herstellern über das Cisco-Compatible-Extensions-Programm

Erkennung von unberechtigten Access Points

Für die Sicherheit im WLAN ist es unverzichtbar, unberechtigte Access Points erkennen zu können. Von Angreifern oder nicht autorisierten Mitarbeitern installierte Access Points gefährden die Sicherheit des gesamten Netzwerks. Mit Cisco SWAN wird der Prozess zur Erkennung unberechtigter Access Points automatisiert. Sowohl Access Points als auch Client-Geräte beteiligen sich aktiv an der kontinuierlichen Überwachung der Funk-Umgebung. Daher können IT-Manager die unberechtigten Access Points einfach und automatisch erkennen, orten und deaktivieren, ebenso die Switch-Ports, mit denen sie verbunden sind.

WAN Link Remote Site Survivability mit lokalem 802.1X-Authentifizierungsdienst



WAN Link Remote Site Survivability

Durch den lokalen IEEE 802.1X-Authentifizierungsdienst der Access Points können entfernte Standorte bei Verbindungsstörungen weiterarbeiten. Mit diesem Dienst sind Cisco Aironet Access Points dafür eingerichtet, als lokale Authentication-Server zu wirken und Wireless-Clients zu authentifizieren, wenn der AAA-Server nicht verfügbar ist. Dies sorgt in WLANs in entfernten Standorten für sichere Authentifizierungsdienste ohne RADIUS-Server, wenn eine Weitverkehrsverbindung oder der Server ausfällt. Dadurch bleiben lokale Ressourcen wie Dateiserver oder Drucker weiterhin nutzbar.

Zusammenfassung

Mit den korrekt konfigurierten und aktivierten Sicherheitsfeatures der Cisco Wireless Security Suite können Netzwerk-Administratoren darauf vertrauen, dass ihre Firmendaten vertraulich und sicher bleiben. Die Netzwerkmanager können ihren Anwendern Unabhängigkeit und Mobilität bieten, ohne die Sicherheit des Netzes aufs Spiel zu setzen.

Die Cisco Aironet-Produktlinie lässt sich leicht in ein vorhandenes Netzwerk integrieren. Durch seine Mobilität und Flexibilität stellt es die beste Lösung für sicheren drahtlosen Netzbetrieb dar und ist zusätzlich leicht zu installieren. Die Cisco-Partner und Cisco Total Implementation Solutions (TIS) unterstützen Sie bei der Implementierung. Technische Betriebsunterstützung bietet der Cisco SMARTnet® Support.

Überzeugen Sie sich selbst davon, wie leicht es ist, ein sicheres Cisco Aironet Wireless-Netzwerk in Ihrem Betrieb zu installieren. Unter www.cisco.com/go/swan finden Sie mehr über Cisco SWAN. Zusätzliche Einzelheiten über WLAN-Sicherheit steht Ihnen auf der Website Cisco Wireless LAN Security unter www.cisco.com/go/aironet/security zur Verfügung. Auch können Sie sich für weitere Informationen an Ihren zuständigen Kundenberater bei Cisco oder Ihren Vertriebspartner wenden.

Cisco Systems GmbH
Kurfürstendamm 22
10719 Berlin
Fax: 030/97 89-2110

Cisco Systems GmbH
Neuer Wall 77
20354 Hamburg
Fax: 040/3767-4444

Cisco Systems GmbH
Hansaallee 249
40549 Düsseldorf
Fax: 02 11/52 02-9010

Cisco Systems GmbH
Friedrich-Ebert-Allee 67
53113 Bonn
Fax: 02 28/3 29-5199

Cisco Systems GmbH
Industriestraße 3
65760 Eschborn
Fax: 0 61 96/7 73-9700

Cisco Systems GmbH
Herold Center
Am Wilhelmsplatz 11
70182 Stuttgart
Fax: 07 11/2 39-1111

Cisco Systems GmbH
Am Söldnermoos 17
85399 Hallbergmoos
Fax: 08 11/5 59-5453

Tel.: 00800-9999-0522
info-center@cisco.com
www.cisco.de

Cisco Systems Austria
Millennium Tower
Handelskai 94-96
A-1200 Wien
Tel.: 00800-9999-0522
Fax: +43/1/2 40 30-63 00
www.cisco.at

Cisco (Switzerland) GmbH
Glatt-Com
8301 Glattzentrum
Schweiz
Tel.: 0800 878 1000
Fax: +41/1/8 78 92 92
www.cisco.ch