Häufig gestellte Fragen zu Cisco Aironet Wireless Security

Inhalt

[Einführung](#)
[Häufig gestellte Fragen](#)
[Fehlerbehebung und Design FAQ](#)
[Zugehörige Informationen](#)

Einführung

Dieses Dokument enthält Informationen zu den am häufigsten gestellten Fragen (FAQs) zu Cisco Aironet Wireless Security.

Häufig gestellte Fragen

F. Was ist Wireless Security erforderlich?

Antwort: In einem kabelgebundenen Netzwerk verbleiben die Daten in den Kabeln, die die Endgeräte verbinden. Drahtlose Netzwerke übertragen und empfangen Daten durch eine Übertragung von RF-Signalen an die Luft. Da WLANs ihre Daten per Broadcast nutzen, besteht eine größere Gefahr für Hacker oder Eindringlinge, die auf die Daten zugreifen oder diese beschädigen können. Um dieses Problem zu beheben, benötigen alle WLANs zusätzlich:

1. Benutzerauthentifizierung, um nicht autorisierten Zugriff auf Netzwerkressourcen zu verhindern.
2. Datenschutz zum Schutz der Integrität und der Privatsphäre der übertragenen Daten (auch als Verschlüsselung bezeichnet).

F. Welche Authentifizierungsmethoden werden vom 802.11-Standard für Wireless LANs definiert?

Antwort: Der 802.11-Standard definiert zwei Mechanismen für die Authentifizierung von Wireless LAN-Clients:

1. Authentifizierung öffnen
2. Authentifizierung über gemeinsam genutzten Schlüssel

Es gibt zwei weitere häufig verwendete Mechanismen:

1. SSID-basierte Authentifizierung
2. MAC-Adressauthentifizierung

F. Was ist die offene Authentifizierung?

Antwort: Die offene Authentifizierung ist im Grunde ein Null-Authentifizierungsalgorithmus, d. h., dass der Benutzer oder das System nicht überprüft wird. Die offene Authentifizierung ermöglicht jedes Gerät, das eine Authentifizierungsanfrage an den Access Point (AP) stellt. Bei der Open Authentication wird eine Klartext-Übertragung verwendet, um einem Client die Zuordnung zu einem Access Point zu ermöglichen. Wenn keine Verschlüsselung aktiviert ist, kann jedes Gerät, das die SSID des WLAN kennt, Zugriff auf das Netzwerk erhalten. Wenn Wired Equivalent Privacy (WEP) auf dem AP aktiviert ist, wird der WEP-Schlüssel zu einem Mittel zur Zugriffskontrolle. Ein Gerät, das nicht über den richtigen WEP-Schlüssel verfügt, kann Daten nicht über den WAP übertragen, selbst wenn die Authentifizierung erfolgreich ist. Ebenso wenig kann ein solches Gerät Daten entschlüsseln, die der Access Point sendet.

F. Welche Schritte umfasst die offene Authentifizierung, damit ein Client dem Access Point zugeordnet werden kann?

1. Der Client sendet eine Anfrage an die APs.
2. Die APs senden Antworten auf Tests zurück.
3. Der Client bewertet die AP-Antworten und wählt den besten AP aus.
4. Der Client sendet eine Authentifizierungsanfrage an den AP.
5. Der Access Point bestätigt die Authentifizierung und registriert den Client.
6. Der Client sendet dann eine Zuordnungsanfrage an den Access Point.
7. Der Access Point bestätigt die Zuordnung und registriert den Client.

F. Welche Vor- und Nachteile hat die Open Authentication?

Antwort: Im Folgenden sind die Vor- und Nachteile der Open Authentication aufgeführt:

Vorteile: Die offene Authentifizierung ist ein grundlegender Authentifizierungsmechanismus, den Sie mit Wireless-Geräten verwenden können, die die komplexen Authentifizierungsalgorithmen nicht unterstützen. Die Authentifizierung in der 802.11-Spezifikation ist verbindungsorientiert. Die Anforderungen für die Authentifizierung ermöglichen es Geräten, schnell auf das Netzwerk zuzugreifen. In diesem Fall können Sie die Open Authentication verwenden.

Nachteile: Die offene Authentifizierung bietet keine Möglichkeit zu überprüfen, ob ein Client ein gültiger Client und kein Hacker-Client ist. Wenn Sie die WEP-Verschlüsselung nicht mit Open Authentication verwenden, kann jeder Benutzer, der die SSID des WLAN kennt, auf das Netzwerk zugreifen.

F. Was ist die Authentifizierung über gemeinsam genutzten Schlüssel?

Antwort: Die Authentifizierung mit gemeinsamem Schlüssel funktioniert ähnlich wie die Open Authentication mit einem großen Unterschied. Wenn Sie die Open Authentication mit dem WEP-Verschlüsselungsschlüssel verwenden, wird der WEP-Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet, jedoch nicht im Authentifizierungsschritt. Bei der Authentifizierung über den gemeinsamen Schlüssel wird die WEP-Verschlüsselung für die Authentifizierung verwendet. Wie bei der Open Authentication erfordert die Shared Key-Authentifizierung, dass der Client und der Access Point denselben WEP-Schlüssel haben. Der Access Point, der die Shared Key-Authentifizierung verwendet, sendet ein Challenge-Textpaket an den Client. Der Client verwendet den lokal konfigurierten WEP-Schlüssel, um den Anfragetext

zu verschlüsseln und mit einer nachfolgenden Authentifizierungsanfrage zu antworten. Wenn der Access Point die Authentifizierungsanforderung entschlüsseln und den ursprünglichen Challenge-Text abrufen kann, antwortet der Access Point mit einer Authentifizierungsantwort, die dem Client Zugriff gewährt.

F. Welche Schritte umfasst die Authentifizierung mit gemeinsam genutztem Schlüssel, damit ein Client dem Access Point zugeordnet werden kann?

1. Der Client sendet eine Anfrage an die APs.
2. Die APs senden Antworten auf Tests zurück.
3. Der Client bewertet die AP-Antworten und wählt den besten AP aus.
4. Der Client sendet eine Authentifizierungsanfrage an den AP.
5. Der WAP sendet eine Authentifizierungsantwort, die den unverschlüsselten Challenge-Text enthält.
6. Der Client verschlüsselt den Challenge-Text mit dem WEP-Schlüssel und sendet den Text an den AP.
7. Der AP vergleicht den unverschlüsselten Challenge-Text mit dem verschlüsselten Challenge-Text. Wenn die Authentifizierung den ursprünglichen Challenge-Text entschlüsseln und abrufen kann, ist die Authentifizierung erfolgreich.

Bei der Authentifizierung mit gemeinsam genutztem Schlüssel wird während des Clientzuordnungsprozesses die WEP-Verschlüsselung verwendet.

F. Welche Vor- und Nachteile hat die Shared Key Authentication?

Antwort: Bei der Shared Key-Authentifizierung tauschen der Client und der Access Point den Challenge-Text (Klartext) und die verschlüsselte Challenge aus. Daher ist diese Art der Authentifizierung anfällig für Man-in-the-Middle-Angriffe. Ein Hacker kann sich die unverschlüsselte Herausforderung und die verschlüsselte Herausforderung anhören und den WEP-Schlüssel (gemeinsamen Schlüssel) aus diesen Informationen extrahieren. Wenn ein Hacker den WEP-Schlüssel kennt, wird der gesamte Authentifizierungsmechanismus kompromittiert, und der Hacker kann auf das WLAN-Netzwerk zugreifen. Dies ist der größte Nachteil bei der Shared Key-Authentifizierung.

F. Was ist MAC-Adressauthentifizierung?

Antwort: Obwohl der 802.11-Standard keine MAC-Adressenauthentifizierung vorsieht, verwenden WLAN-Netzwerke in der Regel diese Authentifizierungstechnik. Daher unterstützen die meisten Anbieter von Wireless-Geräten, einschließlich Cisco, die MAC-Adressenauthentifizierung.

Bei der MAC-Adressenauthentifizierung werden die Clients anhand ihrer MAC-Adresse authentifiziert. Die MAC-Adressen der Clients werden anhand einer Liste von MAC-Adressen überprüft, die lokal auf dem Access Point oder einem externen Authentifizierungsserver gespeichert sind. Die MAC-Authentifizierung ist ein leistungsfähigerer Sicherheitsmechanismus als die Open und Shared Key Authentications-Funktionen, die 802.11 bereitstellt. Diese Form der Authentifizierung verringert die Wahrscheinlichkeit, dass nicht autorisierte Geräte auf das Netzwerk zugreifen können.

F. Warum funktioniert die MAC-Authentifizierung nicht mit Wi-Fi Protected Access (WPA) in Cisco IOS Software Release 12.3(8)JA2?

Antwort: Die einzige Sicherheitsstufe für die MAC-Authentifizierung besteht darin, die MAC-Adresse des Clients anhand einer Liste zulässiger MAC-Adressen zu überprüfen. Dies gilt als sehr schwach. In früheren Versionen der Cisco IOS-Software können Sie die MAC-Authentifizierung und WPA konfigurieren, um die Informationen zu verschlüsseln. Da die WPA selbst jedoch über eine MAC-Adresse verfügt, die überprüft wird, entschied sich Cisco, diese Art der Konfiguration in späteren Versionen der Cisco IOS-Software nicht zuzulassen, und beschloss, nur die Sicherheitsfunktionen zu verbessern.

F. Kann ich SSID als Methode zur Authentifizierung von Wireless-Geräten verwenden?

Antwort: Service Set Identifier (SSID) ist ein eindeutiger, alphanumerischer Wert, der von WLANs als Netzwerkname verwendet wird und zwischen Groß- und Kleinschreibung unterscheidet. Der SSID ist ein -Mechanismus, der die logische Trennung von Wireless-LANs ermöglicht. Die SSID stellt keine Funktionen zum Datenschutz bereit und authentifiziert den Client auch nicht durch die SSID-Daten beim Access Point. Der SSID-Wert wird in Beacons, Anfragen von Tests, Antworten von Tests und anderen Frames als Klartext übertragen. Mit einem 802.11 Wireless LAN Packet Analyzer, z. B. Sniffer Pro, kann ein Lauschkopf die SSID leicht ermitteln. Cisco empfiehlt nicht, die SSID als Methode zur Sicherung Ihres WLAN-Netzwerks zu verwenden.

F. Kann ich durch die Deaktivierung des SSID-Broadcast eine höhere Sicherheit in einem WLAN-Netzwerk erreichen?

Antwort: Wenn Sie den SSID-Broadcast deaktivieren, wird die SSID nicht in Beacon-Nachrichten gesendet. Andere Frames wie Anforderungs- und Anforderungsantworten verfügen jedoch noch immer über die SSID im Klartext. Wenn Sie die SSID deaktivieren, erzielen Sie daher keine erweiterte Wireless-Sicherheit. Die SSID ist nicht als Sicherheitsmechanismus konzipiert oder für den Einsatz vorgesehen. Wenn Sie die SSID-Broadcasts deaktivieren, können zudem Probleme mit der Wi-Fi-Interoperabilität bei Bereitstellungen mit unterschiedlichen Clients auftreten. Aus diesem Grund empfiehlt Cisco nicht, die SSID als Sicherheitsmodus zu verwenden.

F. Welche Sicherheitslücken wurden in der 802.11-Sicherheitslösung gefunden?

Antwort: Die wichtigsten Sicherheitslücken in 802.11-Systemen lassen sich wie folgt zusammenfassen:

- Schwache Authentifizierung nur für Geräte: Client-Geräte werden authentifiziert, nicht Benutzer.
- Schwache Datenverschlüsselung: Wired Equivalent Privacy (WEP) hat sich als unwirksam erwiesen, um Daten zu verschlüsseln.
- Keine Nachrichtenintegrität: Der Integritätsprüfwert (ICV) hat sich als unwirksam erwiesen, um die Integrität der Nachrichten zu gewährleisten.

F. Welche Rolle spielt die 802.1x-Authentifizierung im WLAN?

Antwort: Um die Mängel und Sicherheitsschwachstellen in den ursprünglichen Authentifizierungsverfahren zu beheben, die der 802.11-Standard definiert, ist das 802.1X-Authentifizierungs-Framework in den Entwurf für Sicherheitsverbesserungen auf der MAC-Schicht für 802.11 enthalten. Die IEEE 802.11 Task Group i (TGi) entwickelt diese Erweiterungen derzeit. Das 802.1X-Framework bietet eine erweiterbare Authentifizierung auf der Verbindungsebene, die

normalerweise nur in den höheren Ebenen sichtbar ist.

F. Welche drei Entitäten definiert das 802.1x-Framework?

Antwort: Für das 802.1x-Framework müssen diese drei logischen Einheiten die Geräte in einem WLAN-Netzwerk validieren.

1. **Supplicant** (Komponente): Die Komponente befindet sich auf dem Wireless LAN-Client und wird auch als EAP-Client bezeichnet.
2. **Authenticator**: Der Authentifizierer befindet sich auf dem Access Point.
3. **Authentication Server** (Authentifizierungsserver): Der Authentifizierungsserver befindet sich auf dem RADIUS-Server.

F. Wie erfolgt eine Wireless-Client-Authentifizierung, wenn ich das 802.1x-Authentifizierungs-Framework verwende?

Antwort: Wenn der Wireless-Client (EAP-Client) aktiv wird, authentifiziert sich der Wireless-Client entweder mit offener oder gemeinsam genutzter Authentifizierung. 802.1x arbeitet mit offener Authentifizierung und startet, nachdem der Client dem AP erfolgreich zugeordnet wurde. Die Client-Station kann Datenverkehr nur nach erfolgreicher 802.1x-Authentifizierung zuordnen, aber weiterleiten. Nachfolgend sind die Schritte zur 802.1x-Authentifizierung aufgeführt:

1. Der für 802.1x konfigurierte Access Point (Authentifizierer) fordert die Identität des Benutzers vom Client an.
2. Kunden antworten mit ihrer Identität innerhalb einer festgelegten Frist.
3. Der Server überprüft die Identität des Benutzers und beginnt mit der Authentifizierung beim Client, wenn die Identität des Benutzers in der Datenbank vorhanden ist.
4. Server sendet eine Erfolgsmeldung an den AP.
5. Sobald der Client authentifiziert wurde, leitet der Server den Verschlüsselungsschlüssel an den AP weiter, der zum Verschlüsseln/Entschlüsseln von Datenverkehr verwendet wird, der an den Client und vom Client gesendet wird.
6. Wenn in Schritt 4 die Identität des Benutzers nicht in der Datenbank vorhanden ist, verwirft der Server die Authentifizierung und sendet eine Fehlermeldung an den Access Point.
7. AP leitet diese Nachricht an den Client weiter, und der Client muss sich erneut mit den richtigen Anmeldeinformationen authentifizieren.

Hinweis: Während der 802.1x-Authentifizierung leitet AP die Authentifizierungsnachrichten einfach an den und vom Client weiter.

F. Welche EAP-Varianten kann ich mit dem 802.1x-Authentifizierungs-Framework verwenden?

Antwort: 802.1x definiert die Vorgehensweise zum Authentifizieren von Clients. Der im 802.1x-Framework verwendete EAP-Typ definiert den Typ der Anmeldeinformationen und die Authentifizierungsmethode für den 802.1x-Austausch. Das 802.1x-Framework kann eine der folgenden EAP-Varianten verwenden:

- EAP-TLS - Extensible Authentication Protocol Transport Layer Security
- EAP-FAST - Flexible EAP-Authentifizierung über gesicherten Tunnel
- EAP-SIM - EAP-Teilnehmeridentitätsmodul
- Cisco LEAP - Lightweight Extensible Authentication Protocol
- EAP-PEAP - EAP Protected Extensible Authentication Protocol
- EAP-MD5 - EAP-Message Digest Algorithm 5
- EAP-OTP - EAP-On-Time-Kennwort
- EAP-TTLS - EAP Tunneled Transport Layer Security

F. Wie wähle ich eine 802.1x EAP-Methode aus den verschiedenen verfügbaren Varianten aus?

Antwort: Der wichtigste Faktor, den Sie berücksichtigen müssen, ist, ob die EAP-Methode mit dem vorhandenen Netzwerk kompatibel ist oder nicht. Darüber hinaus empfiehlt Cisco, eine Methode auszuwählen, die die gegenseitige Authentifizierung unterstützt.

F. Was ist lokale EAP-Authentifizierung?

Antwort: Lokaler EAP ist ein Mechanismus, bei dem der WLC als Authentifizierungsserver fungiert. Benutzeranmeldeinformationen werden lokal im WLC gespeichert, um Wireless-Clients zu authentifizieren. Dies dient bei Serverausfällen als Backend-Prozess in Außenstellen. Benutzeranmeldeinformationen können entweder aus der lokalen Datenbank des WLC oder von einem externen LDAP-Server abgerufen werden. LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2 und PEAPv1/GTC sind verschiedene EAP-Authentifizierungen, die von lokalem EAP unterstützt werden.

F. Was ist Cisco LEAP?

Antwort: LEAP (Lightweight Extensible Authentication Protocol) ist eine proprietäre Authentifizierungsmethode von Cisco. Cisco LEAP ist ein 802.1X-Authentifizierungstyp für WLANs. Cisco LEAP unterstützt eine strikte gegenseitige Authentifizierung zwischen Client und RADIUS-Server durch ein Anmeldekennwort als gemeinsam genutzten geheimen Schlüssel. Cisco LEAP bietet dynamische Verschlüsselungsschlüssel pro Benutzer und Sitzung. LEAP ist die einfachste Methode zur Bereitstellung von 802.1x und erfordert nur einen RADIUS-Server. Weitere Informationen zu LEAP finden Sie unter Cisco LEAP.

F. Wie wirkt EAP-FAST?

Antwort: EAP-FAST verwendet symmetrische Schlüsselalgorithmen, um einen getunnelten Authentifizierungsprozess zu erreichen. Die Tunneleinrichtung basiert auf einer PAC (Protected Access Credential), die EAP-FAST über den AAA-Server (Authentication, Authorization, Accounting) (z. B. Cisco Secure Access Control Server [ACS] v. 3.2.3) dynamisch von EAP-FAST bereitgestellt und verwaltet werden kann. EAP-FAST bietet mit einem gegenseitig authentifizierten Tunnel Schutz vor Wörterbuchangriffen und Man-in-the-Middle-Schwachstellen. EAP-FAST umfasst folgende Phasen:

EAP-FAST verringert nicht nur die Risiken passiver Wörterbuchangriffe und Man-in-the-Middle-Angriffe, sondern ermöglicht auch eine sichere Authentifizierung auf Basis der aktuell bereitgestellten Infrastruktur.

- Phase 1: Einrichtung eines gegenseitig authentifizierten Tunnels - Client- und AAA-Server verwenden PAC zur gegenseitigen Authentifizierung und zur Einrichtung eines sicheren Tunnels.
- Phase 2: Ausführen der Client-Authentifizierung im etablierten Tunnel - Der Client sendet Benutzernamen und Kennwort, um die Client-Autorisierungsrichtlinie zu authentifizieren und festzulegen.
- Optional wird diese Phase in Phase 0 - Die EAP-FAST-Authentifizierung selten verwendet, um die dynamische Bereitstellung des Clients mit einer PAC zu ermöglichen. In dieser Phase wird eine sichere Zugriffsberechtigung für jeden Benutzer zwischen Benutzer und Netzwerk erstellt. In Phase 1 der Authentifizierung werden diese Anmeldeinformationen pro Benutzer, die als PAC bezeichnet werden, verwendet.

Weitere Informationen finden Sie unter Cisco EAP-FAST.

F. Gibt es Dokumente auf cisco.com, in denen die Konfiguration von EAP in einem Cisco WLAN-Netzwerk erläutert wird?

Antwort: Informationen zur Konfiguration der EAP-Authentifizierung in einem WLAN-Netzwerk finden Sie unter EAP-Authentifizierung mit RADIUS-Server.

Informationen zur Konfiguration der PEAP-Authentifizierung finden Sie im Protected EAP Application Note (Anwendungshinweis für geschützte EAP-Anwendungen).

Informationen zur Konfiguration der LEAP-Authentifizierung finden Sie unter LEAP-Authentifizierung mit lokalem RADIUS-Server.

F. Welche Verschlüsselungsmechanismen werden am häufigsten in Wireless-Netzwerken eingesetzt?

Antwort: Im Folgenden finden Sie die gebräuchlichsten Verschlüsselungsschemata für Wireless-Netzwerke:

- WEP
- TKIP
- AES

AES ist eine Hardware-Verschlüsselungsmethode, während WEP- und TKIP-Verschlüsselung auf der Firmware verarbeitet werden. Mit einem Firmware-Upgrade können WEP-Geräte TKIP unterstützen, sodass sie interoperabel sind. AES ist die sicherste und schnellste Methode, WEP hingegen die am wenigsten sichere.

F. Was ist WEP Encryption?

Antwort: WEP steht für Wired Equivalent Privacy. WEP wird zum Verschlüsseln und Entschlüsseln von Datensignalen verwendet, die zwischen WLAN-Geräten übertragen werden. WEP ist eine optionale IEEE 802.11-Funktion, die die Offenlegung und Änderung von Paketen bei der Übertragung verhindert und außerdem Zugriffskontrollen für die Nutzung des Netzwerks

ermöglicht. WEP stellt eine WLAN-Verbindung so sicher wie eine kabelgebundene Verbindung. Wie der Standard festlegt, verwendet WEP den RC4-Algorithmus mit einem 40-Bit- oder 104-Bit-Schlüssel. RC4 ist ein symmetrischer Algorithmus, da RC4 denselben Schlüssel für die Verschlüsselung und Entschlüsselung von Daten verwendet. Wenn WEP aktiviert ist, hat jede Funkstation einen Schlüssel. Der Schlüssel wird verwendet, um die Daten vor der Übertragung der Daten durch die Funkwellen zu verwirren. Wenn eine Station ein Paket empfängt, das nicht mit dem entsprechenden Schlüssel verschlüsselt wird, verwirft sie das Paket und übergibt dieses nie an den Host.

Informationen zur Konfiguration von WEP finden Sie unter Konfigurieren von WEP (Wired Equivalent Privacy).

F. Was ist Broadcast Key Rotation? Wie oft wird Broadcast Key Rotation (TDM) gesendet?

Antwort: Durch die Rotation der Broadcast-Tasten kann der Access Point den bestmöglichen zufälligen Gruppenschlüssel generieren. Die Rotation der Broadcast-Tasten aktualisiert regelmäßig alle Clients, die für die Schlüsselverwaltung geeignet sind. Wenn Sie Broadcast WEP-Schlüsselrotation aktivieren, stellt der AP einen dynamischen Broadcast-WEP-Schlüssel bereit und ändert den Schlüssel in dem von Ihnen festgelegten Intervall. Die Rotation von Broadcast-Schlüsseln ist eine hervorragende Alternative zu TKIP, wenn Ihr WLAN Wireless-Client-Geräte von Drittanbietern oder Geräte unterstützt, die für Cisco Client-Geräte nicht auf die neueste Firmware aktualisiert werden können. Informationen zur Konfiguration der Funktion für die Umdrehung des Sendeschlüssels finden Sie unter Aktivieren und Deaktivieren der Rotation der Sendeschlüssel.

F. Was ist TKIP?

Antwort: TKIP steht für Temporal Key Integrity Protocol. TKIP wurde eingeführt, um die Mängel der WEP-Verschlüsselung zu beheben. TKIP wird auch als WEP-Schlüssel-Hashing bezeichnet und wurde ursprünglich als WEP2 bezeichnet. TKIP ist eine temporäre Lösung, die das WEP-Hauptproblem bei der Wiederverwendung behebt. TKIP verwendet zur Verschlüsselung den RC4-Algorithmus, der mit WEP identisch ist. Ein großer Unterschied zu WEP besteht darin, dass TKIP den temporalen Schlüssel jedes Pakets ändert. Der temporale Schlüssel ändert jedes Paket, da sich der Hashwert für jedes Paket ändert.

F. Können Geräte, die TKIP verwenden, mit Geräten zusammenarbeiten, die WEP-Verschlüsselung verwenden?

Antwort: Ein Vorteil von TKIP besteht darin, dass WLANs mit vorhandenen WEP-basierten APs und Funkmodulen durch einfache Firmware-Patches ein Upgrade auf TKIP durchführen können. Auch WEP-Geräte, die nur WEP verwenden, sind weiterhin mit TKIP-fähigen Geräten kompatibel, die WEP verwenden.

F. Was ist Message Integrity Check (MIC)?

Antwort: MIC ist eine weitere Verbesserung zur Behebung von Schwachstellen in der WEP-Verschlüsselung. Die MIC verhindert Bit-Flip-Angriffe auf verschlüsselte Pakete. Bei einem Bit-Flip-Angriff fängt ein Eindringling eine verschlüsselte Nachricht ab, ändert die Nachricht und überträgt die geänderte Nachricht erneut. Der Empfänger weiß nicht, dass die Nachricht beschädigt und nicht legitim ist. Um dieses Problem zu beheben, fügt die MIC-Funktion dem

Wireless-Frame ein MIC-Feld hinzu. Das MIC-Feld bietet eine Überprüfung der Frame-Integrität, die nicht durch dieselben mathematischen Mängel wie der ICV gefährdet ist. Das MIC fügt dem Wireless-Frame auch ein Sequenznummer-Feld hinzu. Der Access Point verwirft außer Betrieb genommene Frames.

F. Was ist WPA? Worin unterscheidet sich WPA 2 von WPA?

Antwort: WPA ist eine standardbasierte Sicherheitslösung der Wi-Fi Alliance, die die Schwachstellen in nativen WLANs behebt. WPA bietet verbesserten Datenschutz und erweiterte Zugriffskontrolle für WLAN-Systeme. WPA behebt alle bekannten Wired Equivalent Privacy (WEP)-Schwachstellen in der ursprünglichen IEEE 802.11-Sicherheitsimplementierung und bietet eine sofortige Sicherheitslösung für WLAN-Netzwerke in Enterprise- und Small Office-Umgebungen (SOHO).

WPA2 ist die nächste Generation der Wi-Fi-Sicherheit. WPA2 ist die von der Wi-Fi Alliance kompatible Implementierung des ratifizierten IEEE 802.11i-Standards. WPA2 implementiert den vom National Institute of Standards and Technology (NIST) empfohlenen AES-Verschlüsselungsalgorithmus (Advanced Encryption Standard) unter Verwendung des Counter-Modus mit dem Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES Counter Mode ist eine Blockchiffre, die 128-Bit-Datenblöcke gleichzeitig mit einem 128-Bit-Verschlüsselungsschlüssel verschlüsselt. WPA2 bietet ein höheres Maß an Sicherheit als WPA. WPA2 erstellt bei jeder Zuordnung neue Sitzungsschlüssel. Die Verschlüsselungsschlüssel, die WPA2 für jeden Client im Netzwerk verwendet, sind eindeutig und spezifisch für diesen Client. Letztlich wird jedes Paket, das über die Luft gesendet wird, mit einem eindeutigen Schlüssel verschlüsselt.

WPA1 und WPA2 können entweder TKIP- oder CCMP-Verschlüsselung verwenden. (Es stimmt, dass einige Access Points und einige Clients die Kombinationen einschränken, aber es gibt vier mögliche Kombinationen). Der Unterschied zwischen WPA1 und WPA2 besteht in den Informationselementen, die in die Beacons, Zuordnungsrahmen und 4-Wege-Handshake-Frames eingegeben werden. Die Daten in diesen Informationselementen sind im Prinzip dieselben, aber der verwendete Bezeichner ist anders. Der Hauptunterschied beim Schlüsselhandshake besteht darin, dass WPA2 den anfänglichen Gruppenschlüssel im 4-Wege-Handshake enthält und der erste Gruppenschlüssel-Handshake übersprungen wird, während WPA diesen zusätzlichen Handshake durchführen muss, um die anfänglichen Gruppenschlüssel bereitzustellen. Die Neukennzeichnung des Gruppenschlüssels erfolgt auf dieselbe Weise. Der Handshake erfolgt vor der Auswahl und Verwendung der Verschlüsselungs-Suite (TKIP oder AES) für die Übertragung von Benutzerdatagrammen. Während des WPA1- oder WPA2-Handshake wird die zu verwendende Verschlüsselungssuite bestimmt. Nach der Auswahl wird die Verschlüsselungssuite für den gesamten Benutzerdatenverkehr verwendet. Daher ist WPA1 plus AES nicht WPA2. WPA1 ermöglicht (ist jedoch häufig Client-seitig eingeschränkt) entweder die TKIP- oder die AES-Verschlüsselung.

F. Was ist AES?

Antwort: AES steht für Advanced Encryption Standard. AES bietet eine deutlich stärkere Verschlüsselung. AES verwendet den Rijndael-Algorithmus, der eine Blockchiffre mit 128-, 192- und 256-Bit-Schlüsselunterstützung ist und viel stärker ist als RC4. Damit WLAN-Geräte AES unterstützen, muss die Hardware AES anstelle von WEP unterstützen.

F. Welche Authentifizierungsmethoden werden von einem Microsoft Internet

Authentication Service (IAS)-Server unterstützt?

Antwort: IAS unterstützt diese Authentifizierungsprotokolle:

- Password Authentication Protocol (PAP)
- Shiva Password Authentication Protocol (SPAP)
- CHAP (Challenge Handshake Authentication Protocol)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP v2)
- Extensible Authentication Protocol-Message Digest 5 CHAP (EAP-MD5 CHAP)
- EAP-Transport Layer Security (EAP-TLS)
- Geschützte EAP-MS-CHAP v2 (PEAP-MS-CHAP v2) (auch bekannt als PEAPv0/EAP-MSCHAPv2)

PEAP-TLS IAS im Windows 2000-Server unterstützt PEAP-MS-CHAP v2 und PEAP-TLS, wenn Windows 2000 Server Service Pack 4 installiert ist. Weitere Informationen finden Sie unter Authentifizierungsmethoden zur Verwendung mit IAS .

F. Wie wird VPN in einer Wireless-Umgebung implementiert?

Antwort: VPN ist ein Layer-3-Sicherheitsmechanismus. Wireless-Verschlüsselungsmechanismen werden auf Layer 2 implementiert. VPN wird über 802.1x, EAP, WEP, TKIP und AES implementiert. Wenn ein Layer-2-Mechanismus vorhanden ist, erhöht das VPN die Implementierungskosten. In Orten wie öffentlichen Hotspots und Hotels, in denen keine Sicherheitsmaßnahmen implementiert werden, wäre VPN eine nützliche Lösung zur Implementierung.

Fehlerbehebung und Design FAQ

F. Gibt es Best Practices für die Bereitstellung von Wireless-Sicherheit in einem Wireless LAN für Außenbereiche?

Antwort: Weitere Informationen finden Sie in den Best Practices für die Wireless-Sicherheit im Außenbereich. Dieses Dokument enthält Informationen zu Best Practices für die Sicherheit bei der Bereitstellung eines Wireless LAN für Außenbereiche.

F. Kann ich einen Windows 2000- oder 2003-Server mit Active Directory für einen RADIUS-Server verwenden, um Wireless-Clients zu authentifizieren?

Antwort: Der Windows 2000- oder 2003-Server mit einem aktiven Verzeichnis kann als RADIUS-Server arbeiten. Informationen zur Konfiguration dieses RADIUS-Servers erhalten Sie, wenn Sie sich an Microsoft wenden möchten, da Cisco die Windows-Serverkonfiguration nicht unterstützt.

F. Meine Website ist im Begriff, von einem offenen Wireless-Netzwerk (APs der Serien 350 und 1200) zu einem PEAP-Netzwerk zu migrieren. Ich möchte, dass sowohl die OPEN SSID (eine SSID, die für die offene Authentifizierung konfiguriert ist) als auch die PEAP-SSID (eine für die PEAP-Authentifizierung konfigurierte SSID) auf demselben Access Point gleichzeitig funktionieren. Dadurch haben wir Zeit, die Clients auf die PEAP-SSID zu migrieren. Gibt es eine Möglichkeit, eine

offene SSID und eine PEAP-SSID gleichzeitig auf demselben AP zu hosten?

Antwort: Die Cisco APs unterstützen VLANs (nur Layer 2). Nur so können Sie das erreichen, was Sie tun möchten. Sie müssen zwei VLANs erstellen (nativ und das andere VLAN). Dann können Sie einen WEP-Schlüssel für einen und keinen WEP-Schlüssel für einen anderen haben. Auf diese Weise können Sie eines der VLANs für die offene Authentifizierung und das andere VLAN für die PEAP-Authentifizierung konfigurieren. Informationen zur Konfiguration von VLANs finden Sie unter Verwenden von VLANs mit Cisco Aironet Wireless Equipment.

Beachten Sie, dass Sie Ihre Switches für dot1Q und für Inter-VLAN-Routing, Ihren L3-Switch oder Ihren Router konfigurieren müssen.

F. Ich möchte meinen Cisco AP 1200 VxWorks einrichten, damit sich die Wireless-Benutzer bei einem Cisco 3005 VPN-Konzentrator authentifizieren können. Welche Konfiguration muss auf dem Access Point und den Clients vorhanden sein, um dies zu erreichen?

Antwort: Für dieses Szenario ist keine spezifische Konfiguration des Access Points oder der Clients erforderlich. Sie müssen alle Konfigurationen auf dem VPN-Konzentrator vornehmen.

F. Ich stelle einen Cisco AP der Serie 1232 AG bereit. Ich würde gerne wissen, welche Methode ich mit diesem Access Point am sichersten einsetzen kann. Ich habe keinen AAA-Server, und meine einzigen Ressourcen sind der Access Point und eine Windows 2003-Domäne. Ich weiß, wie statische 128-Bit-WEP-Schlüssel, SSID-Non-Broadcast-SSID und MAC-Adressbeschränkungen verwendet werden. Benutzer arbeiten hauptsächlich mit Windows XP-Workstations und einigen PDAs. Was ist die sicherste Implementierung für diese Einrichtung?

Antwort: Wenn Sie keinen RADIUS-Server wie den Cisco ACS haben, können Sie Ihren AP als lokalen RADIUS-Server für die LEAP-, EAP-FAST- oder MAC-Authentifizierung konfigurieren.

Hinweis: Ein sehr wichtiger Punkt, den Sie berücksichtigen müssen, ist, ob Sie Ihre Clients mit LEAP oder EAP-FAST verwenden möchten. Wenn dies der Fall ist, müssen Ihre Clients über ein Dienstprogramm zur Unterstützung von LEAP oder EAP-FAST verfügen. Das Windows XP-Dienstprogramm unterstützt nur PEAP oder EAP-TLS.

F. Die PEAP-Authentifizierung schlägt mit dem Fehler "EAP-TLS oder PEAP-Authentifizierung ist während des SSL-Handshake fehlgeschlagen" fehl. Warum?

Antwort: Dieser Fehler kann aufgrund der Cisco Bug-ID CSCee06008 auftreten **(nur registrierte Kunden)**. PEAP schlägt mit ADU 1.2.0.4 fehl. Die Lösung für dieses Problem besteht darin, die neueste Version der ADU zu verwenden.

F. Kann ich WPA und lokale MAC-Authentifizierung auf derselben SSID haben?

Antwort: Der Cisco AP unterstützt keine lokale MAC-Authentifizierung und keinen Wi-Fi Protected Access Pre-Share Key (WPA-PSK) im gleichen Service Set Identifier (SSID). Wenn Sie die lokale MAC-Authentifizierung mit WPA-PSK aktivieren, funktioniert WPA-PSK nicht. Dieses Problem tritt auf, weil bei der lokalen MAC-Authentifizierung die Kennwortzeile für WPA-PSK ASCII aus der

Konfiguration entfernt wird.

F. Wir verfügen derzeit über drei Cisco 1231 Wireless APs mit 128-Bit-WEP-Verschlüsselung für unser Daten-VLAN. Die SSID wird nicht übertragen. In unserer Umgebung gibt es keinen separaten RADIUS-Server. Jemand konnte den WEP-Schlüssel mithilfe eines Scan-Tools ermitteln und einige Wochen lang unser Wireless-Datenverkehr mit diesem Tool überwachen. Wie können wir dies verhindern und das Netzwerk sicher machen?

Antwort: Static WEP ist für dieses Problem anfällig und kann abgeleitet werden, wenn ein Hacker genügend Pakete erfasst und zwei oder mehr Pakete mit demselben Initialisierungsvektor (IV) abrufen kann.

Es gibt mehrere Möglichkeiten, das Auftreten dieses Problems zu verhindern:

1. Verwenden Sie dynamische WEP-Schlüssel.
2. WPA verwenden.
3. Wenn Sie nur Cisco Adapter haben, aktivieren Sie Per Packet Key und MIC.

F. Wenn ich zwei verschiedene WLANs habe, die beide für Wi-Fi Protected Access (WPA)-Pre-Shared Key (PSK) konfiguriert sind, können dann die Pre-Shared Keys pro WLAN anders sein? Wenn es sich um andere WLANs handelt, betrifft dies das andere WLAN, das mit einem anderen vorinstallierten Schlüssel konfiguriert wurde?

Antwort: Die Einstellung des WPA-PSK muss pro WLAN erfolgen. Wenn Sie einen WPA-PSK ändern, sollte sich dies nicht auf das andere konfigurierte WLAN auswirken.

F. In meiner Umgebung verwende ich hauptsächlich Intel Pro/Wireless, Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) und Cisco Secure Access Control Server (ACS) 3.3, die mit Windows Active Directory (AD)-Konten verknüpft sind. Das Problem besteht darin, dass Windows den Benutzer nicht auffordert, das Kennwort zu ändern, wenn das Benutzerkennwort bald abläuft. Schließlich läuft das Konto ab. Gibt es eine Lösung, mit der Windows den Benutzer dazu auffordert, das Kennwort zu ändern?

Antwort: Mit der Funktion zur Kennwortalterung von Cisco Secure ACS können Sie Benutzer zwingen, ihre Kennwörter unter einer oder mehreren der folgenden Bedingungen zu ändern:

- Nach einer festgelegten Anzahl von Tagen (Regeln für das jeweilige Alter)
- Nach einer bestimmten Anzahl von Anmeldungen (Alters-by-Use-Regeln)
- Bei der ersten Anmeldung eines neuen Benutzers (Kennwortänderungsregel)

Weitere Informationen zum Konfigurieren von Cisco Secure ACS für diese Funktion finden Sie unter Aktivieren der Kennwortalterung für die CiscoSecure-Benutzerdatenbank.

F. Wenn sich ein Benutzer über LEAP drahtlos anmeldet, erhält er sein Anmeldeskript, um Netzwerklaufwerke zuzuordnen. Bei Verwendung von Wi-Fi Protected Access (WPA) oder WPA2 mit PEAP-Authentifizierung werden die

Anmeldeskripts jedoch nicht ausgeführt. Sowohl der Client als auch der Access Point sind Cisco und auch der RADIUS (ACS). Warum wird das Anmeldeskript nicht auf dem RADIUS (ACS) ausgeführt?

Antwort: Die maschinelle Authentifizierung ist erforderlich, damit Anmeldeskripts funktionieren. So können die Wireless-Benutzer vor der Anmeldung des Benutzers auf das Netzwerk zugreifen und Skripts laden.

Informationen zum Konfigurieren der Computerauthentifizierung mit PEAP-MS-CHAPv2 finden Sie unter Konfigurieren von Cisco Secure ACS für Windows v3.2 mit PEAP-MS-CHAPv2-Computerauthentifizierung.

F. Wenn ein Benutzer die Computerauthentifizierung für Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) mit dem Cisco Aironet Desktop Utility (ADU) Version 3.0 konfiguriert, kann der Benutzer mit ADU kein Profil erstellen. Warum?

Antwort: Grund hierfür ist die Cisco Bug ID CSCsg32032 (nur registrierte Kunden) . Dies kann auftreten, wenn auf dem Client-PC das Computerzertifikat installiert ist und kein Benutzerzertifikat vorhanden ist.

Die Problemumgehung besteht darin, das Computerzertifikat in den Benutzerspeicher zu kopieren, ein EAP-TLS-Profil zu erstellen und anschließend das Zertifikat aus dem Benutzerspeicher zu entfernen, um die Konfiguration der reinen Computerauthentifizierung zu ermöglichen.

F. Gibt es eine Möglichkeit, VLANs auf Grundlage der MAC-Adresse des Clients im Wireless LAN zuzuweisen?

Antwort: Nein. Das ist nicht möglich. Die VLAN-Zuordnung vom RADIUS-Server funktioniert nur mit 802.1x, nicht mit der MAC-Authentifizierung. Sie können RADIUS verwenden, um VSAs mit MAC-Authentifizierung zu übertragen, wenn die MAC-Adressen auf dem RADIUS-Server authentifiziert werden (in LEAP/PEAP als Benutzer/Kennwort definiert).

Zugehörige Informationen

- Wireless-Netzwerksicherheit
- Whitepaper zur Wireless LAN-Sicherheit
- Übersicht über die Sicherheit von Wireless LAN
- EAP-TLS-Implementierungsleitfaden für Wireless LAN-Netzwerke
- Cisco LEAP
- Konfigurieren von Wired Equivalent Privacy (WEP)
- Wireless-Produktunterstützung
- Technischer Support und Dokumentation für Cisco Systeme