Cisco Aironet Wireless Security FAQ

목차

소개

이 문서에서는 Cisco Aironet Wireless Security에 대한 가장 자주 묻는 질문(FAQ)에 대한 정보를 제공합니다.

일반 FAQ

Q. Wireless Security의 필요성은 무엇입니까?

A. 유선 네트워크에서는 엔드 디바이스를 연결하는 케이블에 데이터가 남아 있습니다.그러나 무선 네트워크는 RF 신호를 브로드캐스트로 송수신합니다.WLAN에서 사용하는 브로드캐스트 특성 때문에 데이터에 액세스하거나 데이터를 손상시킬 수 있는 해커 또는 침입자의 위협이 더욱 커집니다.이 문제를 해결하기 위해 모든 WLAN에 다음을 추가해야 합니다.

1. 네트워크 리소스에 대한 무단 액세스를 방지하기 위한 사용자 인증
2. 데이터 프라이버시를 통해 전송된 데이터의 무결성 및 개인 정보 보호(암호화라고도 함)

Q. 무선 LAN에 대한 802.11 표준에서 정의하는 다른 인증 방법은 무엇입니까?

A. 802.11 표준은 무선 LAN 클라이언트 인증을 위한 두 가지 메커니즘을 정의합니다.

1. 인증 열기
2. 공유 키 인증

일반적으로 사용되는 두 가지 메커니즘이 있습니다.

1. SSID 기반 인증
2. MAC 주소 인증

Q. 개방형 인증이란 무엇입니까?

A. 개방형 인증은 기본적으로 null 인증 알고리즘이며, 사용자 또는 시스템에 대한 확인이 없음을 의미합니다.Open Authentication(개방 인증)은 인증 요청을 액세스 포인트(AP)에 배치하는 모든 디바이스를 허용합니다. Open Authentication은 클라이언트가 AP에 연결할 수 있도록 일반 텍스트 전송을 사용합니다.암호화를 활성화하지 않으면 WLAN의 SSID를 알고 있는 모든 디바이스에서 네트워

크에 액세스할 수 있습니다.AP에서 WEP(Wired Equivalent Privacy)가 활성화된 경우 WEP 키는 액세스 제어 수단이 됩니다.올바른 WEP 키가 없는 장치는 인증에 성공하더라도 AP를 통해 데이터를 전송할 수 없습니다.이러한 디바이스 모두 AP가 전송하는 데이터의 암호를 해독할 수 없습니다.

Q: 클라이언트가 AP와 연결할 때 열린 인증에는 어떤 단계가 포함됩니까?

1. 클라이언트가 AP에 프로브 요청을 보냅니다.
2. AP가 다시 프로브 응답을 보냅니다.
3. 클라이언트는 AP 응답을 평가하고 최상의 AP를 선택합니다.
4. 클라이언트가 AP에 인증 요청을 보냅니다.
5. AP는 인증을 확인하고 클라이언트를 등록합니다.
6. 그러면 클라이언트가 AP에 연결 요청을 보냅니다.
7. AP는 연결을 확인하고 클라이언트를 등록합니다.

Q. 개방형 인증의 장점과 단점은 무엇입니까?

A. 다음은 오픈 인증의 장점과 단점입니다.

장점: Open Authentication은 기본 인증 메커니즘으로, 복잡한 인증 알고리즘을 지원하지 않는 무선 디바이스에서 사용할 수 있습니다.802.11 사양의 인증은 연결 지향적입니다.인증을 위한 요구 사항을 설계하면 디바이스가 네트워크에 빠르게 액세스할 수 있습니다.이러한 경우 Open Authentication을 사용할 수 있습니다.

단점: Open Authentication은 클라이언트가 유효한 클라이언트이고 해커 클라이언트가 아닌지 확인할 수 있는 방법을 제공하지 않습니다.개방 인증과 함께 WEP 암호화를 사용하지 않을 경우 WLAN의 SSID를 알고 있는 모든 사용자가 네트워크에 액세스할 수 있습니다.

Q. 공유 키 인증이란 무엇입니까?

A. 공유 키 인증은 개방 인증과 유사하며 한 가지 중요한 차이점이 있습니다.WEP 암호화 키를 사용하여 개방 인증을 사용하는 경우 WEP 키를 사용하여 데이터를 암호화하고 해독하지만 인증 단계에서는 사용되지 않습니다.공유 키 인증에서 WEP 암호화가 인증에 사용됩니다.공개 인증과 마찬가지로 공유 키 인증에서는 클라이언트와 AP에 동일한 WEP 키가 있어야 합니다.공유 키 인증을 사용하는 AP는 클라이언트에 챌린지 텍스트 패킷을 전송합니다.클라이언트는 로컬로 구성된 WEP 키를 사용하여 챌린지 텍스트를 암호화하고 후속 인증 요청으로 응답합니다.AP가 인증 요청을 해독하고 원래 챌린지 텍스트를 검색할 수 있으면 AP는 클라이언트에 대한 액세스를 허용하는 인증 응답으로 응답합니다.

Q: 클라이언트가 AP와 연결하는 공유 키 인증에는 어떤 단계가 포함됩니까?

1. 클라이언트가 AP에 프로브 요청을 보냅니다.
2. AP가 다시 프로브 응답을 보냅니다.
3. 클라이언트는 AP 응답을 평가하고 최상의 AP를 선택합니다.
4. 클라이언트가 AP에 인증 요청을 보냅니다.
5. AP는 암호화되지 않은 챌린지 텍스트가 포함된 인증 응답을 전송합니다.
6. 클라이언트는 WEP 키로 챌린지 텍스트를 암호화하고 AP에 텍스트를 보냅니다.
7. AP는 암호화되지 않은 챌린지 텍스트를 암호화된 챌린지 텍스트와 비교합니다.인증에서 원래 챌린지 텍스트를 해독하고 검색할 수 있는 경우 인증에 성공합니다.

공유 키 인증은 클라이언트 연결 프로세스 중에 WEP 암호화를 사용합니다.

Q. 공유 키 인증의 장점과 단점은 무엇입니까?

A. 공유 키 인증에서 클라이언트와 AP는 챌린지 텍스트(일반 텍스트)와 암호화된 챌린지를 교환합니다.따라서 이러한 유형의 인증은 중간자 공격에 취약합니다.해커는 암호화되지 않은 도전과 암호화된 과제를 듣고 이 정보에서 WEP 키(공유 키)를 추출할 수 있습니다.해커가 WEP 키를 알면 전체 인증 메커니즘이 손상되고 해커가 WLAN 네트워크에 액세스할 수 있습니다.이는 공유 키 인증의 주요 단점입니다.

Q. MAC 주소 인증이란 무엇입니까?

A. 802.11 표준은 MAC 주소 인증을 지정하지 않지만 WLAN 네트워크는 일반적으로 이 인증 기술을 사용합니다.따라서 Cisco를 비롯한 대부분의 무선 장치 공급업체는 MAC 주소 인증을 지원합니다.

MAC Address Authentication(MAC 주소 인증)에서 클라이언트는 MAC 주소를 기반으로 인증됩니다. 클라이언트의 MAC 주소는 AP 또는 외부 인증 서버에 로컬로 저장된 MAC 주소 목록을 기준으로 확인됩니다.MAC 인증은 802.11에서 제공하는 공개 및 공유 키 인증보다 강력한 보안 메커니즘입니다.이러한 형태의 인증은 네트워크에 액세스할 수 있는 권한이 없는 디바이스의 가능성을 더욱 줄여줍니다.

Q. Cisco IOS Software Release 12.3(8)JA2의 WPA(Wi-Fi Protected Access)에서 MAC 인증이 작동하지 않는 이유는 무엇입니까?

A. MAC 인증을 위한 유일한 보안 레벨은 허용된 MAC 주소 목록과 비교하여 클라이언트의 MAC 주소를 확인하는 것입니다.이것은 매우 약하다고 여겨진다.이전 Cisco IOS Software 릴리스에서는 정보를 암호화하도록 MAC 인증 및 WPA를 구성할 수 있습니다.그러나 WPA 자체에는 확인 MAC 주소가 있기 때문에 Cisco는 나중에 Cisco IOS Software 릴리스에서는 이러한 유형의 구성을 허용하지 않기로 결정했으며 보안 기능만 개선하기로 결정했습니다.

Q. SSID를 무선 디바이스를 인증하는 방법으로 사용할 수 있습니까?

A. SSID(Service Set Identifier)는 WLAN이 네트워크 이름으로 사용하는 고유한 대/소문자 구분 영숫자 값입니다.SSID는 무선 LAN의 논리적 분리를 허용하는 메커니즘입니다.SSID는 데이터 프라이버시 기능을 제공하지 않으며 SSID가 AP에 클라이언트를 실제로 인증하지도 않습니다.SSID 값은 신호, 프로브 요청, 프로브 응답 및 기타 유형의 프레임에서 일반 텍스트로 브로드캐스트됩니다.엿보는 사람은 802.11 무선 LAN 패킷 분석기의 사용(예: Sniffer Pro)으로 SSID를 쉽게 확인할 수 있습니다.Cisco에서는 WLAN 네트워크 보안을 위한 방법으로 SSID를 사용하지 않는 것이 좋습니다.

Q. SSID 브로드캐스트를 비활성화하는 경우 WLAN 네트워크에서 향상된 보안을 실현할 수 있습니까?

A. SSID 브로드캐스트를 비활성화하면 비컨 메시지에서 SSID가 전송되지 않습니다.그러나 Probe Requests 및 Probe Responses와 같은 다른 프레임에는 여전히 일반 텍스트로 SSID가 있습니다.따라서 SSID를 비활성화하면 향상된 무선 보안을 실현할 수 없습니다.SSID는 보안 메커니즘으로 설계되거나 사용할 수 없습니다.또한 SSID 브로드캐스트를 비활성화하면 혼합 클라이언트 구축을 위한 Wi-Fi 상호운용성에 문제가 발생할 수 있습니다.따라서 보안 모드로 SSID를 사용하는 것은 권장하지 않습니다.

Q. 802.11 보안에서 발견되는 취약성은 무엇입니까?

A. 802.11 보안의 주요 취약성은 다음과 같이 요약할 수 있습니다.

- 약한 장치 전용 인증:클라이언트 장치는 사용자가 아니라 인증됩니다.
- 약한 데이터 암호화:WEP(Wired Equivalent Privacy)는 데이터를 암호화하는 수단으로서 효과가 없는 것으로 입증되었습니다.
- 메시지 무결성 없음:ICV(Integrity Check Value)는 메시지 무결성을 보장하기 위한 수단으로서 효과가 없는 것으로 입증되었습니다.

Q. WLAN에서 802.1x 인증의 역할은 무엇입니까?

A. 802.11 표준이 정의하는 원래 인증 방법의 단점 및 보안 취약성을 해결하기 위해 802.11 MAC 레이어 보안 개선 사항을 위한 초안에 802.1X 인증 프레임워크가 포함되어 있습니다.IEEE 802.11 TGi(Task Group i)는 현재 이러한 개선 사항을 개발하고 있습니다.802.1X 프레임워크는 일반적으로 상위 레이어에서만 볼 수 있는 확장 가능한 인증을 제공하는 링크 레이어를 제공합니다.

Q. 802.1x 프레임워크에서 정의하는 세 가지 엔티티는 무엇입니까?

A.802.1x 프레임워크는 WLAN 네트워크에서 디바이스를 검증하기 위해 이러한 3개의 논리적 엔티티가 필요합니다.

1. **서 플리 컨 트** - 서 플리 컨 트가 무선 LAN 클라이언트에 있으며 EAP 클라이언트라고도 합니다.
2. **Authenticator** - 인증자가 AP에 상주합니다.
3. **Authentication Server(인증 서버)** - 인증 서버가 RADIUS 서버에 상주합니다.

Q. 802.1x 인증 프레임워크를 사용할 때 무선 클라이언트 인증은 어떻게 발생합니까?

A. 무선 클라이언트(EAP 클라이언트)가 활성화되면 무선 클라이언트는 개방 또는 공유 인증을 사용하여 인증합니다.802.1x는 열린 인증과 함께 작동하며 클라이언트가 AP에 성공적으로 연결되면 시작됩니다.클라이언트 스테이션은 연결할 수 있지만, 802.1x 인증에 성공한 후에만 데이터 트래픽을 전달할 수 있습니다.802.1x 인증의 단계는 다음과 같습니다.

1. 802.1x에 대해 구성된 AP(Authenticator)가 클라이언트로부터 사용자 ID를 요청합니다.
2. 클라이언트는 지정된 기간 내에 ID로 응답합니다.
3. 서버는 사용자의 ID를 확인하고 사용자 ID가 데이터베이스에 있는 경우 클라이언트와의 인증을 시작합니다.
4. 서버가 AP에 성공 메시지를 전송합니다.
5. 클라이언트가 인증되면 서버는 암호화 키를 AP에 전달합니다. AP는 클라이언트에서 보내고 받는 트래픽을 암호화/해독하는 데 사용됩니다.
6. 4단계에서 사용자의 ID가 데이터베이스에 없는 경우 서버는 인증을 삭제하고 AP에 오류 메시

지를 보냅니다.
7. AP는 이 메시지를 클라이언트에 전달하며, 클라이언트는 올바른 자격 증명을 사용하여 다시 인증해야 합니다.

참고: 802.1x 인증 전반에 걸쳐 AP는 인증 메시지를 클라이언트로부터 수신합니다.

Q. 802.1x 인증 프레임워크와 함께 사용할 수 있는 다양한 EAP 변형은 무엇입니까?

A.802.1x는 클라이언트를 인증하는 절차를 정의합니다.802.1x 프레임워크에 사용되는 EAP 유형은 802.1x 교환에서 사용되는 자격 증명 유형 및 인증 방법을 정의합니다.802.1x 프레임워크는 다음 EAP 변형 중 하나를 사용할 수 있습니다.

- EAP-TLS - 확장 가능 한 인증 프로토콜 전송 계층 보안
- EAP-FAST - 보안 터널을 통한 EAP Flexible Authentication
- EAP-SIM - EAP 가입자 ID 모듈
- Cisco LEAP—경량 확장 인증 프로토콜
- EAP-PEAP - EAP 보호 확장 가능 인증 프로토콜
- EAP-MD5 - EAP 메시지 다이제스트 알고리즘 5
- EAP-OTP - EAP On-Time 비밀번호
- EAP-TTLS - EAP 터널링 전송 계층 보안

Q. 사용 가능한 다양한 변종에서 802.1x EAP 방법을 선택하려면 어떻게 해야 합니까?

A. 고려해야 하는 가장 중요한 요소는 EAP 방법이 기존 네트워크와 호환되는지 여부입니다.또한 상호 인증을 지원하는 방법을 선택할 것을 권장합니다.

Q. 로컬 EAP 인증이란 무엇입니까?

A. 로컬 EAP는 WLC가 인증 서버로 작동하는 메커니즘입니다.사용자 자격 증명은 무선 클라이언트를 인증하기 위해 WLC에 로컬로 저장되며, 이는 서버가 다운될 때 원격 사무실에서 백엔드 프로세스로 작동합니다.WLC의 로컬 데이터베이스 또는 외부 LDAP 서버에서 사용자 자격 증명을 검색할 수 있습니다.LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2 및 PEAPv1/GTC는 로컬 EAP에서 지원하는 서로 다른 EAP 인증입니다.

Q. Cisco LEAP란 무엇입니까?

A. LEAP(Lightweight Extensible Authentication Protocol)는 Cisco의 고유한 인증 방법입니다.Cisco LEAP는 WLAN(무선 LAN)용 802.1X 인증 유형입니다. Cisco LEAP는 로그온 암호를 공유 암호로 사용하여 클라이언트와 RADIUS 서버 간에 강력한 상호 인증을 지원합니다.Cisco LEAP는 사용자별, 세션별 동적 암호화 키를 제공합니다.LEAP는 802.1x를 구축하는 가장 복잡한 방법이며 RADIUS 서버만 필요합니다.LEAP에 대한 자세한 내용은 Cisco LEAP를 참조하십시오.

Q. EAP-FAST는 어떻게 작동합니까?

A. EAP-FAST는 대칭 키 알고리즘을 사용하여 터널링 인증 프로세스를 수행합니다.터널 설정은 EAP-FAST가 인증, 권한 부여 및 계정 관리(예: Cisco ACS(Secure Access Control Server) v. 3.2.3)을 통해 EAP-FAST에 의해 동적으로 프로비저닝 및 관리될 수 있는 PAC(Protected Access Credential)에 의존합니다. 상호 인증된 터널을 통해 EAP-FAST는 사전 공격 및 중간자 취약성으로부터 보호합니다.EAP-FAST의 단계는 다음과 같습니다.

EAP-FAST는 패시브 사전 공격 및 Man-in-the-Middle 공격으로부터 위험을 완화하는 것은 물론, 현재 구축된 인프라를 기반으로 보안 인증을 활성화합니다.

- 1단계:상호 인증 터널 설정 - 클라이언트와 AAA 서버는 PAC를 사용하여 서로를 인증하고 보안 터널을 설정합니다.
- 2단계:Perform client authentication in the established tunnel(설정된 터널에서 클라이언트 인증 수행) - 클라이언트가 사용자 이름과 비밀번호를 전송하여 클라이언트 권한 부여 정책을 인증하고 설정합니다.
- 선택적으로, Phase 0(단계 0) - EAP-FAST 인증은 이 단계를 자주 사용하여 클라이언트가 PAC로 동적으로 프로비저닝되도록 합니다.이 단계에서는 사용자와 네트워크 간에 사용자 단위 액세스 자격 증명을 안전하게 생성합니다.인증의 1단계에서는 PAC라고 하는 사용자별 자격 증명을 사용합니다.

자세한 내용은 Cisco EAP-FAST를 참조하십시오.

Q. cisco.com에서 Cisco WLAN 네트워크에서 EAP를 구성하는 방법을 설명하는 문서가 있습니까?

A. WLAN 네트워크에서 EAP 인증을 구성하는 방법에 대한 자세한 내용은 RADIUS 서버를 통한 EAP 인증을 참조하십시오.

PEAP 인증을 구성하는 방법에 대한 자세한 내용은 보호된 EAP 애플리케이션 노트를 참조하십시오.

LEAP 인증을 구성하는 방법에 대한 자세한 내용은 로컬 RADIUS 서버를 사용한 LEAP 인증을 참조하십시오.

Q. 무선 네트워크에서 가장 일반적으로 사용되는 암호화 메커니즘은 무엇입니까?

A. 다음은 무선 네트워크에서 사용되는 가장 일반적으로 사용되는 암호화 방법입니다.

- WEP
- TKIP
- AES

AES는 하드웨어 암호화 방법이지만 WEP 및 TKIP 암호화는 펌웨어에서 처리됩니다.펌웨어 업그레이드를 통해 WEP 장치는 TKIP를 지원하므로 상호 운용 가능합니다.AES는 가장 안전하고 빠른 방법이지만 WEP는 가장 안전하지 않은 방법입니다.

Q. WEP 암호화란 무엇입니까?

A. WEP는 Wired Equivalent Privacy를 의미합니다.WEP는 WLAN 장치 간에 전송되는 데이터 신호를 암호화하고 해독하는 데 사용됩니다.WEP는 전송 중인 패킷의 공개 및 수정을 방지하고 네트워크 사용을 위한 액세스 제어를 제공하는 선택적 IEEE 802.11 기능입니다.WEP는 WLAN 링크를 유선 링크처럼 안전하게 만듭니다.표준에서 지정한 대로 WEP는 40비트 또는 104비트 키와 함께 RC4 알고리즘을 사용합니다.RC4는 데이터의 암호화와 해독에 동일한 키를 사용하기 때문에 대칭 알고리즘입니다.WEP가 활성화되면 각 라디오 "스테이션"에 키가 있습니다.이 키는 전파를 통해 데이터를 전송하기 전에 데이터를 스크램블하는 데 사용된다.스테이션에서 적절한 키로 스크램블되지 않은 패킷을 수신하면 스테이션은 패킷을 폐기하고 그러한 패킷을 호스트에 전달하지 않습니다.

WEP 구성 방법에 대한 자세한 내용은 WEP(Wired Equivalent Privacy) 구성을 참조하십시오.

Q. 브로드캐스트 키 순환이란 무엇입니까?브로드캐스트 키 순환의 빈도는 얼마입니까?

A. 브로드캐스트 키 회전을 통해 AP는 가능한 최고의 임의 그룹 키를 생성할 수 있습니다.브로드캐스트 키 순환은 키 관리가 가능한 모든 클라이언트를 주기적으로 업데이트합니다.브로드캐스트 WEP 키 순환을 활성화하면 AP는 동적 브로드캐스트 WEP 키를 제공하고 사용자가 설정한 간격으로 키를 변경합니다.무선 LAN이 Cisco 클라이언트 장치에 대한 최신 펌웨어로 업그레이드할 수 없는 타사 무선 클라이언트 장치 또는 장치를 지원하는 경우 브로드캐스트 키 순환은 TKIP에 대한 훌륭한 대안입니다.브로드캐스트 키 순환 기능을 구성하는 방법에 대한 자세한 내용은 브로드캐스트 키 순환 활성화 및 비활성화를 참조하십시오.

Q. TKIP란 무엇입니까?

A. TKIP는 임시 키 무결성 프로토콜을 의미합니다.WEP 암호화의 단점을 해결하기 위해 TKIP가 도입되었습니다.TKIP는 WEP 키 해싱이라고도 하며 처음에는 WEP2라고 불렀습니다. TKIP는 WEP의 키 재사용 문제를 해결하는 임시 솔루션입니다.TKIP는 RC4 알고리즘을 사용하여 암호화를 수행합니다. 이는 WEP와 동일합니다.WEP와 큰 차이점은 TKIP가 모든 패킷의 임시 키를 변경한다는 것입니다.모든 패킷의 해시 값이 변경되므로 임시 키는 모든 패킷을 변경합니다.

Q. TKIP를 사용하는 장치는 WEP 암호화를 사용하는 장치와 상호 작용할 수 있습니까?

A. TKIP의 장점은 기존 WEP 기반 AP와 무선 장치가 있는 WLAN이 간단한 펌웨어 패치를 통해 TKIP로 업그레이드할 수 있다는 것입니다.또한 WEP 전용 장비는 WEP를 사용하는 TKIP 지원 장치와 계속 상호 운용됩니다.

Q. MIC(Message Integrity Check)란 무엇입니까?

A. MIC는 WEP 암호화의 취약성을 해결하기 위한 또 다른 개선 사항입니다.MIC는 암호화된 패킷에 대한 비트 플립 공격을 방지합니다.비트 플립 공격 중에 침입자가 암호화된 메시지를 인터셉트하고 메시지를 변경한 다음 변경된 메시지를 다시 전송합니다.수신자가 메시지가 손상되었으며 올바른 메시지가 아님을 알지 못합니다.이 문제를 해결하기 위해 MIC 기능은 무선 프레임에 MIC 필드를 추가합니다.MIC 필드는 ICV와 동일한 수학적 단점에 취약하지 않은 프레임 무결성 검사를 제공합니다.또한 MIC는 무선 프레임에 시퀀스 번호 필드를 추가합니다.AP가 잘못 수신한 프레임을 삭제합니다.

Q. WPA란 무엇입니까?WPA 2는 WPA와 어떻게 다릅니까?

A. WPA는 기본 WLAN의 취약성을 해결하는 Wi-Fi Alliance의 표준 기반 보안 솔루션입니다.WPA는 WLAN 시스템에 대해 향상된 데이터 보호 및 액세스 제어를 제공합니다.WPA는 원래 IEEE 802.11 보안 구현에서 알려진 모든 WEP(Wired Equivalent Privacy) 취약성을 해결하며 기업 및 소규모 사무실, 홈 오피스(SOHO) 환경 모두에서 WLAN 네트워크에 즉시 보안 솔루션을 제공합니다.

WPA2는 차세대 Wi-Fi 보안입니다.WPA2는 승인된 IEEE 802.11i 표준의 Wi-Fi Alliance 상호 운용 가능한 구현입니다.WPA2는 CCMP(Cipher Block Chaining Message Authentication Code Protocol)를 사용하여 카운터 모드를 사용하는 NIST(National Institute of Standards and Technology) 권장 AES(Advanced Encryption Standard) 암호화 알고리즘을 구현합니다.AES 카운터 모드는 128비트 암호화 키를 사용하여 한 번에 128비트 데이터 블록을 암호화하는 블록 암호입니다.WPA2는 WPA보다 높은 수준의 보안을 제공합니다.WPA2는 모든 연결에 새 세션 키를 만듭니다.WPA2가 네트워크의 각 클라이언트에 사용하는 암호화 키는 고유하며 해당 클라이언트에 특정

합니다.결국, 공기를 통해 전송되는 모든 패킷은 고유한 키로 암호화됩니다.

WPA1과 WPA2는 모두 TKIP 또는 CCMP 암호화를 사용할 수 있습니다.(일부 액세스 포인트와 일부 클라이언트는 조합을 제한하지만 가능한 4가지 조합이 있습니다.) WPA1과 WPA2의 차이점은 신호, 연결 프레임 및 4방향 핸드셰이크 프레임에 삽입되는 정보 요소에 있습니다.이러한 정보 요소의 데이터는 기본적으로 동일하지만 사용되는 식별자는 다릅니다.키 핸드셰이크의 주요 차이점은 WPA2에는 4방향 핸드셰이크에 초기 그룹 키가 포함되며 첫 번째 그룹 키 핸드셰이크는 건너뛰는 반면 WPA는 초기 그룹 키를 전달하려면 이 추가 핸드셰이크를 수행해야 합니다.그룹 키의 키 재지정도 같은 방식으로 수행됩니다.핸드셰이크는 사용자 데이터그램 전송을 위해 암호 그룹(TKIP 또는 AES)을 선택하고 사용하기 전에 발생합니다.WPA1 또는 WPA2 핸드셰이크 중에 사용할 암호 그룹이 결정됩니다.선택하면 암호 그룹이 모든 사용자 트래픽에 사용됩니다.따라서 WPA1과 AES는 WPA2가 아닙니다. WPA1은 TKIP 또는 AES 암호 중 하나를 허용합니다(그러나 클라이언트 측에서 제한되는 경우도 있음).

Q. AES란 무엇입니까?

A. AES는 Advanced Encryption Standard를 의미합니다.AES는 훨씬 강력한 암호화를 제공합니다.AES는 128, 192 및 256비트 키를 지원하는 블록 암호인 Rijndael 알고리즘을 사용하며 RC4보다 훨씬 강력합니다. WLAN 장치가 AES를 지원하려면 하드웨어가 WEP 대신 AES를 지원해야 합니다.

Q. Microsoft IAS(Internet Authentication Service) 서버에서 어떤 인증 방법을 지원합니까?

A. IAS는 다음 인증 프로토콜을 지원합니다.

- PAP(Password Authentication Protocol)
- SPAP(Shiva Password Authentication Protocol)
- 챌린지 핸드셰이크 인증 프로토콜(CHAP)
- Microsoft MS-CHAP(Challenge Handshake Authentication Protocol)
- Microsoft Challenge Handshake Authentication Protocol 버전 2(MS-CHAP v2)
- 확장 가능 한 인증 프로토콜 메시지 다이제스트 5 CHAP (EAP-MD5 CHAP)
- EAP-전송 계층 보안(EAP-TLS)
- 보호된 EAP-MS-CHAP v2(PEAP-MS-CHAP v2)(PEAPv0/EAP-MSCHAPv2라고도 함)

Windows 2000 Server의 PEAP-TLS IAS는 Windows 2000 Server 서비스 팩 4가 설치된 경우 PEAP-MS-CHAP v2 및 PEAP-TLS를 지원합니다.자세한 내용은 IAS와 함께 사용할 인증 방법을 참조하십시오 .

Q. 무선 환경에서 VPN은 어떻게 구현됩니까?

A. VPN은 레이어 3 보안 메커니즘입니다.무선 암호화 메커니즘은 레이어 2에서 구현됩니다. VPN은 802.1x, EAP, WEP, TKIP 및 AES를 통해 구현됩니다.레이어 2 메커니즘이 구축되면 VPN은 구현에 오버헤드를 추가합니다.공용 핫스팟과 보안이 구현되지 않은 호텔 같은 장소에서 VPN은 구현하기에 유용한 솔루션입니다.

문제 해결 및 설계 FAQ

Q. 실외 무선 LAN에 무선 보안을 구축하는 데 모범 사례가 있습니까?

A. 실외 무선 보안 모범 사례를 참조하십시오.이 문서에서는 실외 무선 LAN을 구축하기 위한 보안 모범 사례에 대한 정보를 제공합니다.

Q. RADIUS 서버를 위해 Active Directory가 있는 Windows 2000 또는 2003 서버를 사용하여 무선 클라이언트를 인증할 수 있습니까?

A. Active Directory가 있는 Windows 2000 또는 2003 서버는 RADIUS 서버로 작동할 수 있습니다.이 RADIUS 서버를 구성하는 방법에 대한 자세한 내용은 Cisco에서 Windows 서버 구성을 지원하지 않으므로 Microsoft에 문의해야 합니다.

Q. 내 사이트는 오픈 무선 네트워크(350 및 1200 시리즈 AP)에서 PEAP 네트워크로 마이그레이션하려고 합니다.OPEN SSID(Open Authentication에 대해 구성된 SSID)와 PEAP SSID(PEAP 인증을 위해 구성된 SSID)를 동시에 동일한 AP에서 작동하게 하고 싶습니다.이렇게 하면 클라이언트를 PEAP SSID로 마이그레이션할 수 있습니다.동일한 AP에서 Open SSID와 PEAP SSID를 동시에 호스팅할 수 있는 방법이 있습니까?

A. Cisco AP는 VLAN을 지원합니다(레이어 2에만 해당). 이것은 실제로 여러분이 하고 싶은 것을 성취하는 유일한 방법입니다.두 개의 VLAN(기본 및 기타 VLAN)을 생성해야 합니다. 그런 다음 한 WEP 키를 사용하고 다른 WEP 키를 사용할 수 없습니다.이렇게 하면 개방형 인증을 위한 VLAN 중 하나와 PEAP 인증을 위한 다른 VLAN을 구성할 수 있습니다.VLAN을 구성하는 방법을 알아보려면 Cisco Aironet Wireless Equipment에서 VLAN 사용을 참조하십시오.

dot1Q 및 VLAN 간 라우팅, L3 스위치 또는 라우터에 대한 스위치를 구성해야 합니다.

Q. 무선 사용자가 Cisco 3005 VPN Concentrator를 인증하도록 Cisco AP 1200 VxWorks를 설정하려고 합니다.이를 위해 AP 및 클라이언트에 어떤 컨피그레이션이 있어야 합니까?

A. 이 시나리오의 AP 또는 클라이언트에 필요한 특정 컨피그레이션이 없습니다.VPN Concentrator에서 모든 컨피그레이션을 수행해야 합니다.

Q. Cisco 1232 AG AP를 구축하고 있습니다.이 AP를 사용하여 구축할 수 있는 가장 안전한 방법을 알고 싶습니다.AAA 서버가 없으며 AP와 Windows 2003 도메인만 있습니다.고정 128비트 WEP 키, 비브로드캐스트 SSID 및 MAC 주소 제한을 사용하는 방법에 대해 잘 알고 있습니다.대부분의 사용자는 Windows XP 워크스테이션과 일부 PDA를 사용합니다.이 설정에 가장 안전한 구현은 무엇입니까?

A. Cisco ACS와 같은 RADIUS 서버가 없는 경우 AP를 LEAP, EAP-FAST 또는 MAC 인증을 위한 로컬 RADIUS 서버로 구성할 수 있습니다.

참고: LEAP 또는 EAP-FAST와 함께 클라이언트를 사용할 것인지 여부를 고려해야 하는 매우 중요한 사항입니다.이 경우, 클라이언트에는 LEAP 또는 EAP-FAST를 지원하는 유틸리티가 있어야 합니다.Windows XP 유틸리티는 PEAP 또는 EAP-TLS만 지원합니다.

Q. PEAP 인증은 "SSL 핸드셰이크 중에 EAP-TLS 또는 PEAP 인증 실패"라는 오류 메시지와 함께 실패합니다. 왜?

A. 이 오류는 Cisco 버그 ID **CSCee06008(등록된 고객만 해당)** 때문에 발생할 수 **있습니다**.ADU 1.2.0.4에서 PEAP가 실패합니다. 이 문제를 해결하려면 최신 버전의 ADU를 사용합니다.

Q. 동일한 SSID에서 WPA 및 로컬 MAC 인증을 사용할 수 있습니까?

A. Cisco AP는 동일한 SSID(Service Set Identifier)에서 로컬 MAC 인증 및 WPA-PSK(Wi-Fi Protected Access Pre-Share Key)를 지원하지 않습니다. WPA-PSK를 사용하여 로컬 MAC 인증을 활성화하면 WPA-PSK가 작동하지 않습니다.이 문제는 로컬 MAC 인증이 컨피그레이션에서 WPA-PSK ASCII 비밀번호 라인을 제거하므로 발생합니다.

Q. 현재 데이터 VLAN을 위한 Ciphers 128비트 WEP 암호화와 함께 3개의 Cisco 1231 무선 AP가 설정되어 있습니다.SSID는 브로드캐스트하지 않습니다.환경에 별도의 RADIUS 서버가 없습니다.누군가가 스캐닝 도구를 통해 WEP 키를 확인하고 이 도구를 사용하여 무선 트래픽을 모니터링했습니다.이를 방지하고 네트워크를 안전하게 만들려면 어떻게 해야 합니까?

A. 고정 WEP는 이 문제에 취약하며 해커가 충분한 패킷을 캡처하고 동일한 초기화 벡터(IV)를 사용하여 둘 이상의 패킷을 얻을 수 있는 경우 파생될 수 있습니다.

이 문제의 발생을 방지하는 방법은 여러 가지가 있습니다.

1. 동적 WEP 키를 사용합니다.
2. WPA를 사용합니다.
3. Cisco 어댑터만 있는 경우 Per Packet Key 및 MIC를 활성화합니다.

Q. 두 개의 서로 다른 WLAN이 있는 경우, 두 WLAN은 모두 WPA(Wi-Fi Protected Access)-PSK(Pre-Shared Key)에 대해 구성되어 있으면 사전 공유 키가 WLAN마다 다를 수 있습니까?다른 경우 다른 사전 공유 키로 구성된 다른 WLAN에 영향을 미칩니까?

A. WPA-PSK의 설정은 WLAN별로 설정해야 합니다.하나의 WPA-PSK를 변경할 경우 구성된 다른 WLAN에는 영향을 주지 않습니다.

Q. 내 환경에서 주로 Intel Pro/무선, EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) 및 Windows AD(Active Directory) 계정에 연결된 Cisco ACS(Secure Access Control Server) 3.3을 사용합니다.문제는 사용자 암호가 만료될 때 사용자에게 암호를 변경하라는 메시지를 표시하지 않습니다.결국 이 계정은 만료됩니다.Windows에서 사용자에게 암호를 변경하라는 메시지를 표시하도록 하는 솔루션이 있습니까?

A. Cisco Secure ACS 비밀번호 에이징 기능을 사용하면 다음 조건 중 하나 이상에서 사용자가 비밀번호를 변경하도록 강제할 수 있습니다.

- 지정된 일 수 이후(기간별 규칙)
- 지정된 로그인 수 이후(기간별 규칙)
- 새 사용자가 처음 로그인하는 경우(비밀번호 변경 규칙)

이 기능에 대해 Cisco Secure ACS를 구성하는 방법에 대한 자세한 내용은 CiscoSecure User Database에 대한 비밀번호 에이징 활성화를 참조하십시오.

Q. 사용자가 LEAP를 사용하여 무선으로 로그인하면 로그인 스크립트를 통해 네트워크 드라이브를 매핑합니다.그러나 PEAP 인증을 사용하여 WPA(Wi-Fi Protected Access) 또는 WPA2를 사용하면 로그인 스크립트가 실행되지 않습니다.클라이언트와 액세스 포인트 모두 RADIUS(ACS)와 마찬가지로 Cisco입니다. 로그인 스크립트가 RADIUS(ACS)에서 실행되지 않는 이유는 무엇입니까?

A. 로그인 스크립트가 작동하려면 머신 인증이 필수입니다.이렇게 하면 무선 사용자는 사용자가 로그온하기 전에 스크립트를 로드하기 위해 네트워크에 액세스할 수 있습니다.

PEAP-MS-CHAPv2로 머신 인증을 구성하는 방법에 대한 자세한 내용은 Windows v3.2용 Cisco Secure ACS With PEAP-MS-CHAPv2 Machine Authentication을 참조하십시오.

Q. Cisco ADU(Aironet Desktop Utility) 릴리스 3.0을 사용하는 경우 사용자가 EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)에 대해 머신 인증을 구성할 때 ADU는 사용자가 프로필을 생성할 수 없도록 합니다.왜?

A. 이는 Cisco 버그 ID CSCsg32032(등록된 고객만 해당) 때문입니다. 클라이언트 PC에 컴퓨터 인증서가 설치되어 있고 사용자 인증서가 없는 경우 이 문제가 발생할 수 있습니다.

해결 방법은 시스템 인증서를 사용자 저장소에 복사하고, EAP-TLS 프로파일을 생성한 다음, 머신 인증 전용 컨피그레이션에 대한 사용자 저장소에서 인증서를 제거하는 것입니다.

Q. 클라이언트의 MAC 주소를 기반으로 무선 LAN에 VLAN을 할당하는 방법이 있습니까?

A. 아니요. 이건 불가능합니다.RADIUS 서버의 VLAN 할당은 MAC 인증이 아닌 802.1x에서만 작동합니다.MAC 주소가 RADIUS 서버에서 인증된 경우(LEAP/PEAP에서 사용자 ID/비밀번호로 정의됨) RADIUS를 사용하여 MAC 인증으로 VSA를 푸시할 수 있습니다.

관련 정보

- 무선 네트워크 보안
- 무선 LAN 보안 백서
- 무선 LAN 보안 개요
- 무선 LAN 네트워크용 EAP-TLS 구축 설명서
- Cisco LEAP
- WEP(Wired Equivalent Privacy) 구성
- 무선 제품 지원
- 기술 지원 및 문서 – Cisco Systems