WLC 레이어 2 및 레이어 3 보안 호환성 매트릭스

목차

소개

이 문서에서는 WLC(Wireless LAN Controller)에서 지원되는 레이어 2 및 레이어 3 보안 메커니즘에 대한 호환성 매트릭스를 제공합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 경량형 AP 및 Cisco WLC 컨피그레이션에 대한 기본 지식
- LWAPP(Lightweight AP Protocol)에 대한 기본 지식
- 무선 보안 솔루션에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 펌웨어 버전 7.0.116.0을 실행하는 Cisco 4400/2100 Series WLC를 기반으로 합니다

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

Cisco Unified Wireless Network 보안 솔루션

Cisco Unified Wireless Network는 레이어 2 및 레이어 3 보안 방법을 지원합니다.

- 레이어 2 보안
- 레이어 3 보안(WLAN용) 또는 레이어 3 보안(게스트 LAN용)

게스트 LAN에서는 레이어 2 보안이 지원되지 않습니다.

이 표에는 Wireless LAN Controller에서 지원되는 다양한 레이어 2 및 레이어 3 보안 방법이 나열되어 있습니다. 이러한 보안 방법은 WLANs(WLAN) > **Edit(편집) WLAN**의 **Security(보안) 탭**에서 활성화할 수 있습니다.

레이어 2 보안 메커니즘		
매개변수		**설명**
레이어 2 보안	없음	선택된 레이어 2 보안이 없습니다.
	WPA+WPA2	Wi-Fi Protected Access를 활성화하려면 이 설정을 사용합니다.
	802.1X	802.1x 인증을 활성화하려면 이 설정을 사용합니다.
	고정 WEP	고정 WEP 암호화를 활성화하려면 이 설정을 사용합니다.
	고정 WEP + 802.1x	고정 WEP 및 802.1x 매개변수를 모두 활성화하려면 이 설정을 사용합니다.
	CKIP	Cisco CKIP(Key Integrity Protocol)를 사용하도록 설정하려면 이 설정을 사용합니다. AP 모델 1100, 1130 및 1200에서 작동하지만 AP 1000에서는 작동하지 않습니다. 이 기능이 작동하려면 Aironet IE를 활성화해야 합니다. CKIP는 암호화 키를 16바이트로 확장합니다.
MAC 필터링	MAC 주소로 클라이언트를 필터링하려면 선택합니다. MAC Filters(MAC 필터) > New(새) 페이지에서 MAC 주소별로 클라이언트를 로컬로 구성합니다. 그렇지 않으면 RADIUS 서버에서 클라이언트를 구성합니다.	
레이어 3 보안 메커니즘(WLAN용)		
매개변수		**설명**
레이어 3 보안	없음	선택된 레이어 3 보안이 없습니다.
	IPSec	IPSec을 활성화하려면 이 설정을 사용합니다. IPSec을 구현하기 전에 소프트웨어 가용성 및 클라이언트 하드웨어 호환성을 확인해야 합니다. **참고:** IPSec을 사용하려면

		VPN/Enhanced Security Module(암호화 프로세서 카드) 옵션을 설치해야 합니다. Inventory(인벤토리) 페이지의 컨트롤러에 설치되어 있는지 확인합니다.
	VPN 패스스루	VPN Pass-Through를 활성화하려면 이 설정을 사용합니다. **참고:** 이 옵션은 Cisco 5500 Series Controller 및 Cisco 2100 Series Controller에서는 사용할 수 없습니다. 그러나 ACL을 사용하여 개방형 WLAN을 생성하면 Cisco 5500 Series Controller 또는 Cisco 2100 Series Controller에서 이 기능을 복제할 수 있습니다.
웹 정책	웹 정책을 활성화하려면 이 확인란을 선택합니다. 컨트롤러는 인증 전에 무선 클라이언트에 DNS 트래픽을 전달합니다. **참고:** 웹 정책은 IPsec 또는 VPN Pass-Through 옵션과 함께 사용할 수 없습니다. 다음 매개변수가 표시됩니다. • Authentication(인증) - 이 옵션을 선택하면 클라이언트를 무선 네트워크에 연결하는 동안 사용자에게 사용자 이름 및 비밀번호를 묻는 메시지가 표시됩니다. • Passthrough(통과) - 이 옵션을 선택하면 사용자가 사용자 이름 및 비밀번호 인증 없이 네트워크에 직접 액세스할 수 있습니다. • Conditional Web Redirect(조건부 웹 리디렉션) - 이 옵션을 선택하면 802.1X 인증이 성공적으로 완료된 후 사용자가 특정 웹 페이지로 조건부 리디렉션될 수 있습니다. RADIUS 서버에서 리디렉션이 발생하는 조건 및 리디렉션 페이지를 지정할 수 있습니다. • Splash Page Web Redirect(스플래시 페이지 웹 리디렉션) - 이 옵션을 선택하면 802.1X 인증이 완료된 후 사용자가 특정 웹 페이지로 리디렉션됩니다. 리디렉션 후에는 사용자가 네트워크에 대한 전체 액세스 권한을 갖습니다. RADIUS 서버에서 스플래시 웹 페이지를 지정할 수 있습니다. • On MAC Filter failure(MAC 필터 실패 시) - 웹 인증 MAC 필터 실패를 활성화합니다.	
사전 인증 ACL	클라이언트와 컨트롤러 간의 트래픽에 사용할 ACL을 선택합니다.	
Over-	Authentication(인증)을 선택하는 경우 표시됩니다	

ride 글로벌 컨피그레이션	. 웹 로그인 페이지에서 전역 인증 구성 설정을 재정의하려면 이 확인란을 선택합니다.
웹 인증 유형	Web Policy(웹 정책) 및 Over-ride Global Config(전역 컨피그레이션 초과)를 선택한 경우 표시됩니다. 웹 인증 유형 선택: • 내부 • 사용자 지정(다운로드) Login Page(로그인 페이지) - 드롭다운 목록에서 로그인 페이지를 선택합니다.Login Failure page(로그인 실패 페이지) - 웹 인증이 실패할 경우 클라이언트에 표시되는 로그인 페이지를 선택합니다 .Logout page(로그아웃 페이지) - 사용자가 시스템에서 로그아웃할 때 클라이언트에 표시되는 로그인 페이지를 선택합니다. • 외부(외부 서버로 리디렉션) URL - 외부 서버의 URL을 입력합니다.
이메일 입력	패스스루를 선택하면 표시됩니다. 이 옵션을 선택하면 네트워크에 연결하는 동안 이메일 주소를 입력하라는 메시지가 표시됩니다.

레이어 3 보안 메커니즘(게스트 LAN용)		
매개변수		**설명**
레이어 3 보안	없음	선택된 레이어 3 보안이 없습니다.
	웹 인증	이 옵션을 선택하면 클라이언트를 네트워크에 연결하는 동안 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.
	웹 통과	이 옵션을 선택하면 사용자 이름 및 비밀번호 인증 없이 네트워크에 직접 액세스할 수 있습니다.
사전 인증 ACL		클라이언트와 컨트롤러 간의 트래픽에 사용할 ACL을 선택합니다.
Over-ride 글로벌 컨피그레이션		웹 로그인 페이지에서 전역 인증 구성 설정을 재정의하려면 이 확인란을 선택합니다.
웹 인증 유형		Over-ride Global Config를 선택한 경우 표시됩니다. 웹 인증 유형 선택: • 내부 • 사용자 지정(다운로드) Login Page(로그인 페이지) - 드롭다운 목록에서 로그인 페이지를 선택합니다.Login Failure page(로

	그인 실패 페이지) - 웹 인증이 실패할 경우 클라이언트에 표시되는 로그인 페이지를 선택합니다 .Logout page(로그아웃 페이지) - 사용자가 시스템에서 로그아웃할 때 클라이언트에 표시되는 로그인 페이지를 선택합니다. • 외부(외부 서버로 리디렉션) URL - 외부 서버의 URL을 입력합니다.
이메일 입력	Web Passthrough를 선택하면 표시됩니다. 이 옵션을 선택하면 네트워크에 연결하는 동안 이메일 주소를 입력하라는 메시지가 표시됩니다.

참고: 컨트롤러 소프트웨어 릴리스 4.1.185.0 이상에서는 CKIP가 고정 WEP에서만 사용하도록 지원됩니다. 동적 WEP와 함께 사용할 수 없습니다. 따라서 동적 WEP와 함께 CKIP를 사용하도록 구성된 무선 클라이언트는 CKIP용으로 구성된 무선 LAN에 연결할 수 없습니다. CKIP가 없는 동적 WEP(보안 수준이 낮음) 또는 TKIP 또는 AES가 있는 WPA/WPA2(보안 수준이 높음)를 사용하는 것이 좋습니다.

무선 LAN 컨트롤러 레이어 2 - 레이어 3 보안 호환성 매트릭스

무선 LAN에서 보안을 구성할 때 레이어 2 및 레이어 3 보안 방법을 모두 함께 사용할 수 있습니다. 그러나 모든 레이어 2 보안 방법을 모든 레이어 3 보안 방법과 함께 사용할 수는 없습니다. 이 표에서는 Wireless LAN Controller에서 지원되는 레이어 2 및 레이어 3 보안 방법에 대한 호환성 매트릭스를 보여줍니다.

레이어 2 보안 메커니즘	레이어 3 보안 메커니즘	호환성
없음	없음	Valid
WPA+WPA2	없음	Valid
WPA+WPA2	웹 인증	Invalid
WPA-PSK/WPA2-PSK	웹 인증	Valid
WPA+WPA2	웹 통과	Invalid
WPA-PSK/WPA2-PSK	웹 통과	Valid
WPA+WPA2	조건부 웹 리디렉션	Valid
WPA+WPA2	스플래시 페이지 웹 리디렉션	Valid
WPA+WPA2	VPN 패스스루	Valid
802.1x	없음	Valid

802.1x	웹 인증	Invalid
802.1x	웹 통과	Invalid
802.1x	조건부 웹 리디렉션	Valid
802.1x	스플래시 페이지 웹 리디렉션	Valid
802.1x	VPN 패스스루	Valid
고정 WEP	없음	Valid
고정 WEP	웹 인증	Valid
고정 WEP	웹 통과	Valid
고정 WEP	조건부 웹 리디렉션	Invalid
고정 WEP	스플래시 페이지 웹 리디렉션	Invalid
고정 WEP	VPN 패스스루	Valid
고정 WEP+ 802.1x	없음	Valid
고정 WEP+ 802.1x	웹 인증	Invalid
고정 WEP+ 802.1x	웹 통과	Invalid
고정 WEP+ 802.1x	조건부 웹 리디렉션	Invalid
고정 WEP+ 802.1x	스플래시 페이지 웹 리디렉션	Invalid
고정 WEP+ 802.1x	VPN 패스스루	Invalid
CKIP	없음	Valid
CKIP	웹 인증	Valid
CKIP	웹 통과	Valid
CKIP	조건부 웹 리디렉션	Invalid
CKIP	스플래시 페이지 웹 리디렉션	Invalid
CKIP	VPN 패스스루	Valid

관련 정보

- Wireless LAN Controller 및 Lightweight Access Point 기본 구성 예
- WLC(Wireless LAN Controller)에 LAP(Lightweight AP) 등록
- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 7.0.116.0
- 무선 LAN 컨트롤러(WLC)에 대한 FAQ

- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.