WLC 및 LAP 구성을 사용하는 MFP(Infrastructure Management Frame Protection) 예

목차

소개

이 문서에서는 MFP(Management Frame Protection)라는 새로운 무선 보안 기능을 소개합니다. 이 문서에서는 LAP(Lightweight Access Point) 및 WLC(Wireless LAN Controller)와 같은 인프라 디바이스에서 MFP를 구성하는 방법에 대해서도 설명합니다.

사전 요구 사항

요구 사항

- 기본 작업을 위해 WLC 및 LAP를 구성하는 방법에 대한 지식
- IEEE 802.11 관리 프레임에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 4.1을 실행하는 Cisco 2000 Series WLC
- Cisco 1131AG LAP
- 펌웨어 릴리스 3.6을 실행하는 Cisco Aironet 802.11a/b/g Client Adapter
- Cisco Aironet Desktop Utility 버전 3.6

참고: MFP는 WLC 버전 4.0.155.5 이상에서 지원되지만 버전 4.0.206.0은 MFP를 통해 최적의 성능을 제공합니다.클라이언트 MFP는 버전 4.1.171.0 이상에서 지원됩니다.

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.

배경 정보

802.11에서는 (de) authentication, (dis) association, beacon 및 프로브와 같은 관리 프레임이 항상 인증되지 않고 암호화되지 않습니다.즉, 802.11 관리 프레임은 WPA, WPA2 또는 적어도 WEP 등과 같은 프로토콜로 암호화된 데이터 트래픽과는 달리 항상 보안되지 않은 방식으로 전송됩니다.

이렇게 하면 공격자가 AP에서 관리 프레임을 스푸핑하여 AP에 연결된 클라이언트를 공격할 수 있습니다.스푸핑된 관리 프레임을 사용하여 공격자는 다음 작업을 수행할 수 있습니다.

- WLAN에서 서비스 거부(DOS) 실행
- 클라이언트가 다시 연결될 때 중간자 공격 시도
- 오프라인 사전 공격 실행

MFP는 무선 네트워크 인프라에서 교환되는 802.11 관리 프레임을 인증하면 이러한 위험을 극복합니다.

참고: 이 문서는 **인프라 및 클라이언트 MFP에** 중점을 **둡니다**.

참고: 일부 무선 클라이언트가 MFP 지원 인프라 디바이스와 통신하는 데 특정한 제한이 있습니다.MFP는 각 프로브 요청 또는 SSID 신호에 긴 정보 요소 집합을 추가합니다.PDA, 스마트폰, 바코드 스캐너 등과 같은 일부 무선 클라이언트는 메모리와 CPU가 제한되어 있습니다.따라서 이러한 요청이나 신호를 처리할 수 없습니다.따라서 SSID를 완전히 볼 수 없거나 SSID 기능에 대한 오해로 인해 이러한 인프라 디바이스와 연결할 수 없습니다.이 문제는 MFP에만 국한되지 않습니다.이는 IE(정보 요소)가 여러 개인 SSID에서도 발생합니다. 실시간으로 배포하기 전에 사용 가능한 모든 클라이언트 유형을 사용하여 환경에서 MFP *사용 가능* SSID를 테스트하는 것이 좋습니다.

참고:

다음은 인프라 MFP의 구성 요소입니다.

- **관리 프레임 보호** - 관리 프레임 보호가 활성화되면 AP는 전송되는 각 관리 프레임에 MIC IE(메시지 무결성 검사 정보 요소)를 추가합니다.프레임을 복사, 변경 또는 재생하려는 모든 시도에

서 MIC가 무효화됩니다.MFP 프레임의 유효성을 검사하도록 구성된 AP가 유효하지 않은 MIC가 포함된 프레임을 수신하면 WLC에 이를 보고합니다.
- **관리 프레임 검증** - 관리 프레임 검증이 활성화되면 AP는 네트워크의 다른 AP에서 수신하는 모든 관리 프레임을 검증합니다.MIC IE가 있는지 확인하고(발신자가 MFP 프레임을 전송하도록 구성된 경우) 관리 프레임의 내용과 일치시킵니다.MFP 프레임을 전송하도록 구성된 AP에 속한 BSSID에서 유효한 MIC IE를 포함하지 않는 프레임을 수신하면 네트워크 관리 시스템에 불일치를 보고합니다.**참고:** 타임스탬프가 제대로 작동하려면 모든 WLC가 NTP(Network Time Protocol)가 동기화되어야 합니다.
- **이벤트 보고** - 액세스 포인트에서 이상 징후를 탐지하면 WLC에 알립니다.WLC는 비정상적인 이벤트를 집계하여 SNMP 트랩을 통해 네트워크 관리자에게 보고합니다.

인프라 MFP 기능

MFP를 사용하면 모든 관리 프레임이 암호화를 통해 MIC(Message Integrity Check)를 생성합니다. MIC가 프레임 끝(FCS(Frame Check Sequence) 앞에 추가됩니다.

- 중앙 집중식 무선 아키텍처에서 인프라 MFP는 WLC(글로벌 컨피그레이션)에서 활성화/비활성화됩니다. WLAN당 보호를 선택적으로 비활성화할 수 있으며, AP당 검증을 선택적으로 비활성화할 수 있습니다.
- 추가 IE를 처리할 수 없는 디바이스에서 사용하는 WLAN에서 보호를 비활성화할 수 있습니다.
- 오버로드 또는 오버파워 상태인 AP에서 검증을 비활성화해야 합니다.

WLC에 구성된 하나 이상의 WLAN에서 MFP가 활성화되면 WLC는 등록된 각 AP의 각 무선에 고유한 키를 전송합니다.관리 프레임은 MFP 지원 WLAN을 통해 AP에 의해 전송됩니다.이러한 AP에는 프레임 보호 MIC IE로 레이블이 지정됩니다.프레임을 변경하려고 시도하면 메시지가 무효화됩니다. 그러면 MFP 프레임을 탐지하도록 구성된 수신 AP가 WLAN 컨트롤러에 불일치를 보고하도록 됩니다.

이는 로밍 환경에서 구현되는 동안 MFP의 단계별 프로세스입니다.

1. MFP가 전역적으로 활성화되면 WLC는 MFP용으로 구성된 모든 AP/WLAN에 대해 고유한 키를 생성합니다.WLC는 모든 WLC가 모빌리티 도메인에 있는 모든 AP/BSS의 키를 알 수 있도록 자체 내에서 통신합니다.**참고:** 모빌리티/RF 그룹의 모든 컨트롤러는 동일하게 MFP를 구성해야 합니다.
2. AP는 모르는 BSS에 대해 MFP 보호 프레임을 수신하면 프레임 복사본을 버퍼링하고 WLC에 쿼리하여 키를 가져옵니다.
3. WLC에서 BSSID를 모르는 경우 AP에 "Unknown BSSID(알 수 없는 BSSID)" 메시지가 반환되고 AP가 해당 BSSID에서 수신한 관리 프레임을 삭제합니다.
4. WLC에서 BSSID를 알고 있지만 해당 BSSID에서 MFP가 비활성화된 경우 WLC는 "Disabled BSSID"를 반환합니다. 그러면 AP는 해당 BSSID에서 수신한 모든 관리 프레임에 MFP MIC가 없다고 가정합니다.
5. BSSID를 알고 있고 MFP가 활성화된 경우 WLC는 AES 암호화 LWAPP 관리 터널을 통해 요청 AP에 MFP 키를 반환합니다.
6. AP는 이 방법으로 받은 키를 캐시합니다.이 키는 MIC IE의 유효성을 검사하거나 추가하는 데 사용됩니다.

클라이언트 MFP 기능

클라이언트 MFP는 인증된 클라이언트를 스푸핑된 프레임으로부터 보호하므로 무선 LAN에 대한 많은 일반적인 공격의 효과를 방지합니다.디인증 공격과 같은 대부분의 공격은 유효한 클라이언트와 경쟁할 때 성능이 저하된 상태로 돌아갑니다.

특히 클라이언트 MFP는 액세스 포인트와 CCXv5 클라이언트 간에 전송되는 관리 프레임을 암호화하여 액세스 포인트와 클라이언트 모두 예방 조치를 취하고 스푸핑된 클래스 3 관리 프레임(즉, 액세스 포인트와 인증 및 연결된 클라이언트 간에 전달되는 관리 프레임)을 삭제할 수 있도록 합니다.클라이언트 MFP는 IEEE 802.11i에서 정의한 보안 메커니즘을 활용하여 다음과 같은 유형의 클래스 3 유니캐스트 관리 프레임을 보호합니다.disassociation, deauthentication 및 QoS(WMM) 작업클라이언트 MFP는 가장 일반적인 유형의 서비스 거부 공격으로부터 클라이언트 액세스 포인트 세션을 보호할 수 있습니다.세션의 데이터 프레임에 사용되는 것과 동일한 암호화 방법으로 클래스 3 관리 프레임을 보호합니다.액세스 포인트 또는 클라이언트에서 받은 프레임이 암호 해독에 실패하면 해당 프레임이 삭제되고 이벤트가 컨트롤러에 보고됩니다.

클라이언트 MFP를 사용하려면 클라이언트가 CCXv5 MFP를 지원해야 하며 TKIP 또는 AES-CCMP와 WPA2를 협상해야 합니다.EAP 또는 PSK를 사용하여 PMK를 얻을 수 있습니다.CCKM 및 컨트롤러 모빌리티 관리는 액세스 포인트 또는 레이어 2 및 레이어 3 빠른 로밍 간에 세션 키를 배포하는 데 사용됩니다.

브로드캐스트 프레임에 대한 공격을 방지하기 위해 CCXv5를 지원하는 액세스 포인트는 어떤 브로드캐스트 클래스 3 관리 프레임(예: 연결 해제, 인증 해제 또는 작업)도 내보내지 않습니다.CCXv5 클라이언트 및 액세스 포인트는 브로드캐스트 클래스 3 관리 프레임을 폐기해야 합니다.

인프라 MFP는 클라이언트-MFP를 지원하지 않는 클라이언트로 보내진 잘못된 유니캐스트 프레임뿐만 아니라 잘못된 클래스 1 및 2 관리 프레임도 탐지하고 보고하기 때문에 클라이언트 MFP는 인프라 MFP를 대체하지 않고 보완합니다.인프라 MFP는 클라이언트 MFP에 의해 보호되지 않는 관리 프레임에만 적용됩니다.

클라이언트 MFP 구성 요소

클라이언트 MFP는 다음 구성 요소로 구성됩니다.

- 키 생성 및 배포
- 관리 프레임 보호 및 검증
- 오류 보고서

키 생성 및 배포

클라이언트 MFP는 인프라 MFP에 대해 파생된 키 생성 및 배포 메커니즘을 사용하지 않습니다.대신 클라이언트 MFP는 IEEE 802.11i에서 정의한 보안 메커니즘을 활용하여 클래스 3 유니캐스트 관리 프레임도 보호합니다.스테이션은 CCXv5를 지원해야 하며 클라이언트 MFP를 사용하려면 TKIP 또는 AES-CCMP를 협상해야 합니다.EAP 또는 PSK를 사용하여 PMK를 얻을 수 있습니다.

관리 프레임 보호

유니캐스트 클래스 3 관리 프레임은 AES-CCMP 또는 TKIP를 사용하여 이미 데이터 프레임에 사용된 것과 비슷한 방식으로 보호됩니다.다음 섹션에서 설명한 대로 프레임 헤더의 일부는 보호를 강화하기 위해 각 프레임의 암호화된 페이로드 구성 요소에 복사됩니다.

이러한 프레임 유형은 보호됩니다.

- 연결 해제
- 인증 취소
- WMM(QoS) 작업 프레임

AES-CCMP 및 TKIP 보호 데이터 프레임에는 재생 탐지를 방지하는 데 사용되는 IV 필드에 시퀀스 카운터가 포함됩니다.현재 전송 카운터는 데이터 프레임과 관리 프레임 모두에 사용되지만 새 수신 카운터는 관리 프레임에 사용됩니다.수신 카운터는 마지막으로 받은 프레임보다 많은 수의 프레임을 갖도록 테스트되므로(프레임이 고유하고 재생되지 않았는지 확인), 이 구성표가 수신되는 값을 비순차적 값으로 만드는 것은 중요하지 않습니다.

오류 보고서

MFP-1 보고 메커니즘은 액세스 포인트에서 탐지된 관리 프레임 캡슐화 해제 오류를 보고하는 데 사용됩니다.즉, WLC는 MFP 검증 오류 통계를 수집하고 정기적으로 수집된 정보를 WCS에 전달합니다.

클라이언트 스테이션에서 탐지된 MFP 위반 오류는 CCXv5 로밍 및 실시간 진단 기능에 의해 처리되며 이 문서의 범위에 속하지 않습니다.

브로드캐스트 관리 프레임 보호

브로드캐스트 프레임을 사용하는 공격을 방지하기 위해 CCXv5를 지원하는 AP는 비인가 억제 디인증/연결 해제 프레임을 제외하고 브로드캐스트 클래스 3(즉, disassoc, 디인증 또는 작업) 관리 프레임을 전송하지 않습니다.CCXv5 지원 클라이언트 스테이션은 브로드캐스트 클래스 3 관리 프레임을 폐기해야 합니다.MFP 세션은 적절한 보안 네트워크(강력한 인증 + TKIP 또는 CCMP)에 있는 것으로 간주되므로 비인가 억제 브로드캐스트를 무시해도 문제가 되지 않습니다.

마찬가지로 AP는 인바운드 브로드캐스트 관리 프레임을 폐기합니다.현재 인바운드 브로드캐스트 관리 프레임이 지원되지 않으므로 이에 대해 코드를 변경할 필요가 없습니다.

지원되는 플랫폼

다음 플랫폼이 지원됩니다.

- WLAN 컨트롤러200621064400WiSM내장형 440x 컨트롤러 포함 375026/28/37/38xx 라우터
- LWAPP 액세스 포인트AP 1000AP 1100, 1130AP 1200, 1240, 1250AP 1310
- 클라이언트 소프트웨어ADU 3.6.4 이상
- 네트워크 관리 시스템WCS

1500 메시 LWAPP AP는 이 릴리스에서 지원되지 않습니다.

지원되는 모드

이러한 모드에서 작동하는 LWAPP 기반 액세스 포인트는 클라이언트 MFP를 지원합니다.

지원되는 액세스 포인트 모드	
모드	**클라이언트 MFP 지원**
로컬	예
모니터	아니요
스니퍼	아니요

비인가 탐지기	아니요
하이브리드 REAP	예
REAP	아니요
브리지 루트	예
WGB	아니요

혼합 셀 지원

CCXv5를 지원하지 않는 클라이언트 스테이션은 MFP-2 WLAN과 연결할 수 있습니다.액세스 포인트는 어떤 클라이언트가 MFP-2를 지원하는지 추적하며, 이는 MFP-2 보안 조치가 아웃바운드 유니캐스트 관리 프레임에 적용되는지 그리고 인바운드 유니캐스트 관리 프레임에서 예상되는지 결정하기 위한 것이 아닙니다.

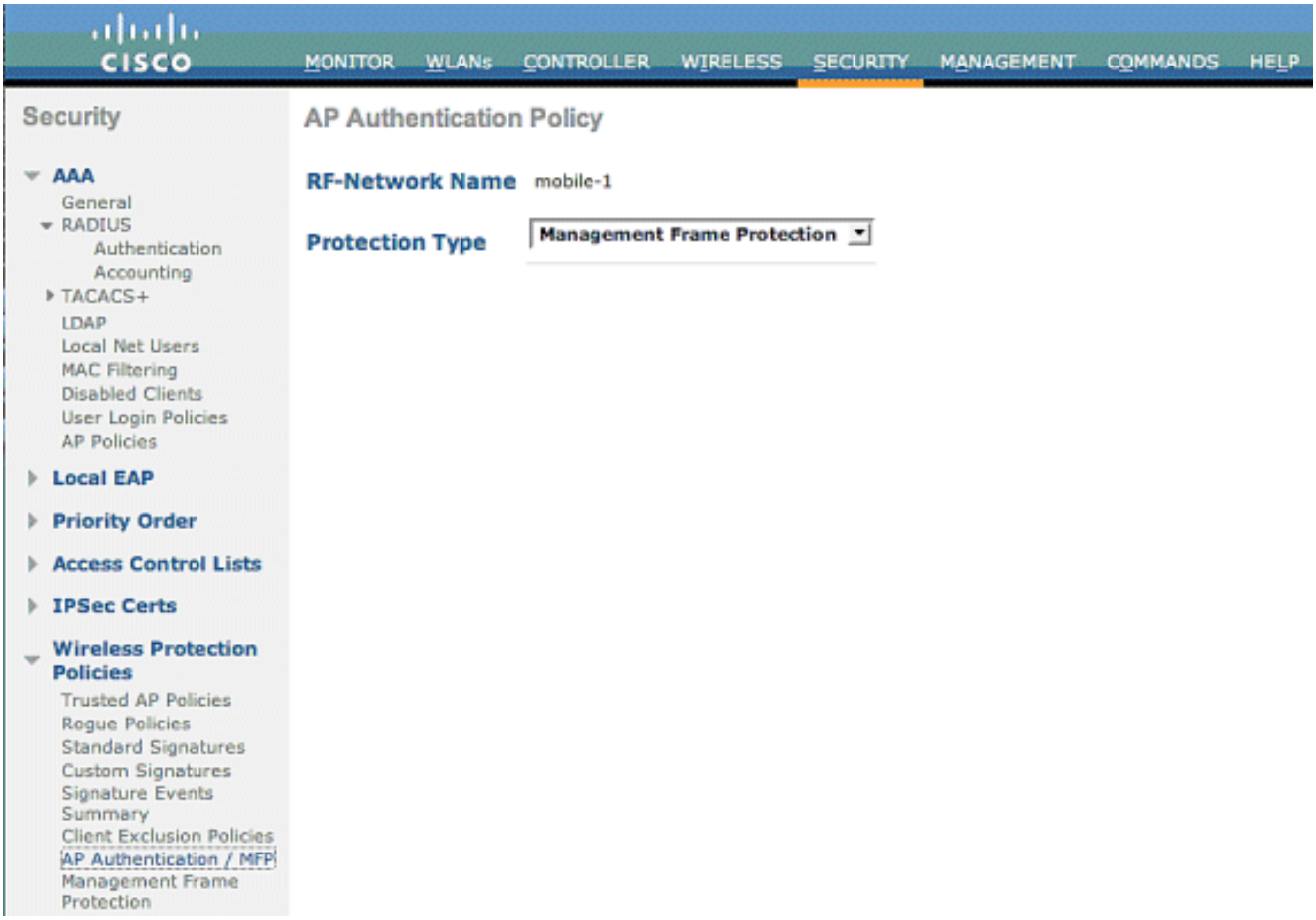
구성

컨트롤러에서 MFP 구성

컨트롤러에서 MFP를 전역적으로 구성할 수 있습니다.이렇게 하면 **조인된 각 액세스 포인트에 대해 기본적으로 관리 프레임 보호 및 유효성 검사가 활성화되며** 액세스 포인트 인증이 자동으로 비활성화됩니다.

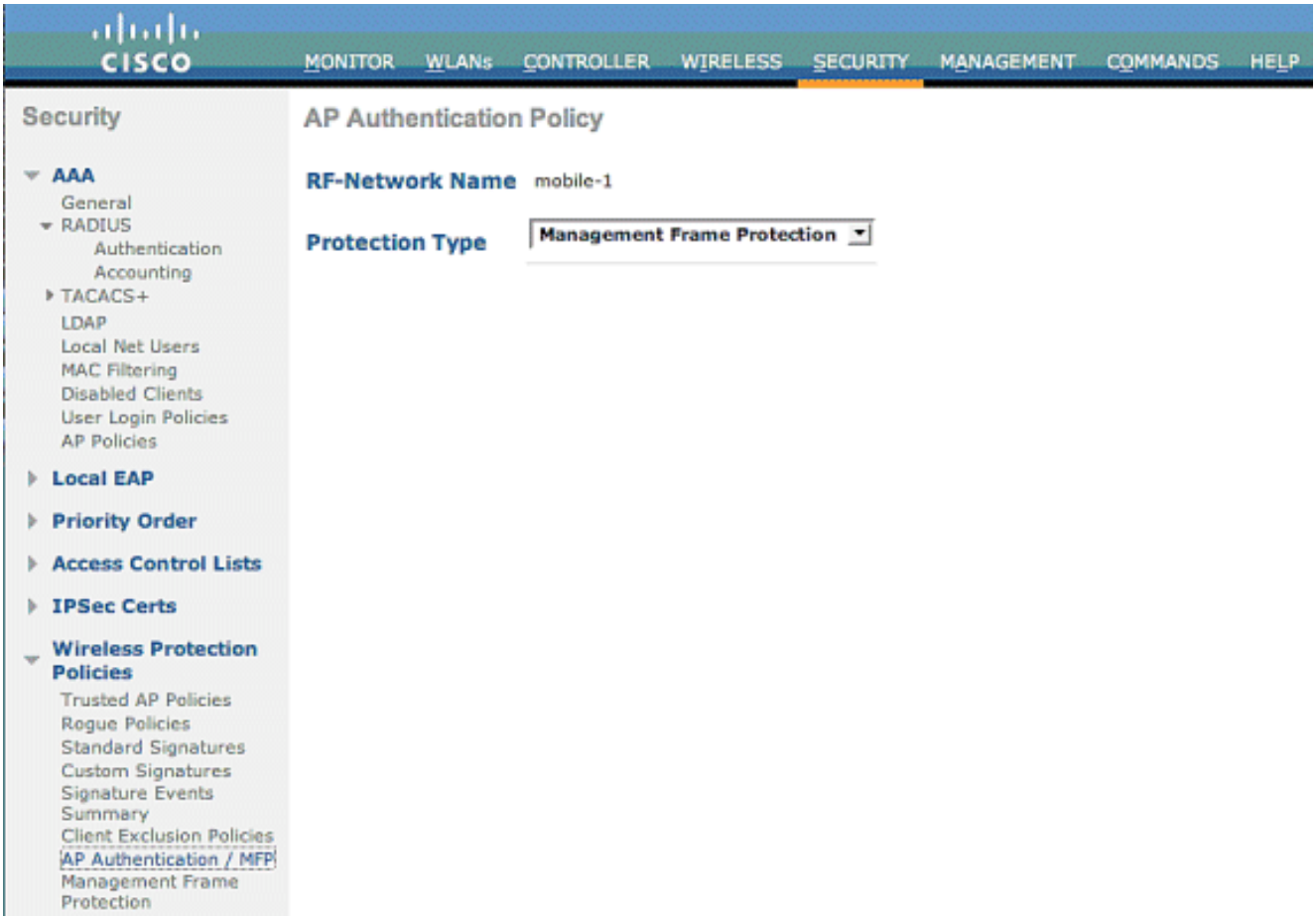
컨트롤러에서 MFP를 전역적으로 구성하려면 다음 단계를 수행합니다.

1. 컨트롤러 GUI에서 Security(**보안**)를 클릭합니다.결과 화면에서 Wireless Protection Policies(**무선 보호 정책**)에서 **AP Authentication/MFP(AP 인증/MFP)를** 클릭합니다
.



2. AP Authentication Policy(AP 인증 정책)의 Protection Type(**보호 유형**) 드롭다운 메뉴에서 **Management Frame Protection(관리 프레임 보호)을** 선택하고 **Apply(적용)를 클릭합니다**

.

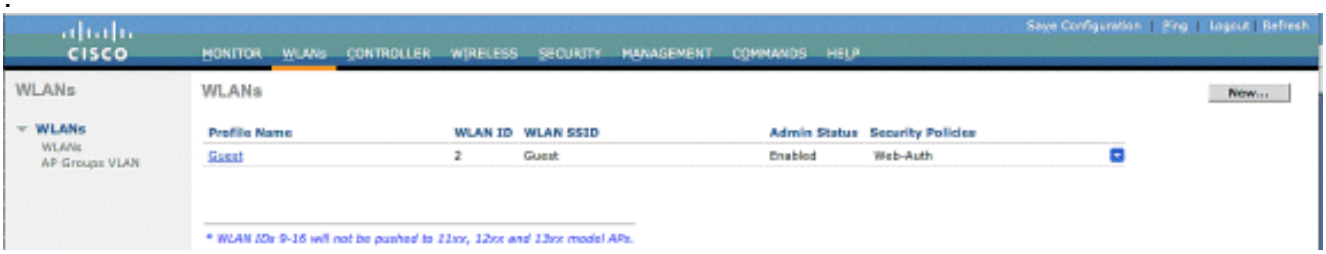


WLAN에서 MFP 구성

또한 WLC에 구성된 각 WLAN에서 인프라 MFP 보호 및 클라이언트 MFP를 활성화/비활성화할 수 있습니다.인프라 MFP 보호(전역적으로 활성화된 경우에만 활성화됨)와 WLAN이 WPA2 보안으로 구성된 경우에만 클라이언트 MFP가 활성화되어 있는 경우 두 가지 모두 기본적으로 활성화됩니다 .WLAN에서 MFP를 활성화하려면 다음 단계를 수행합니다.

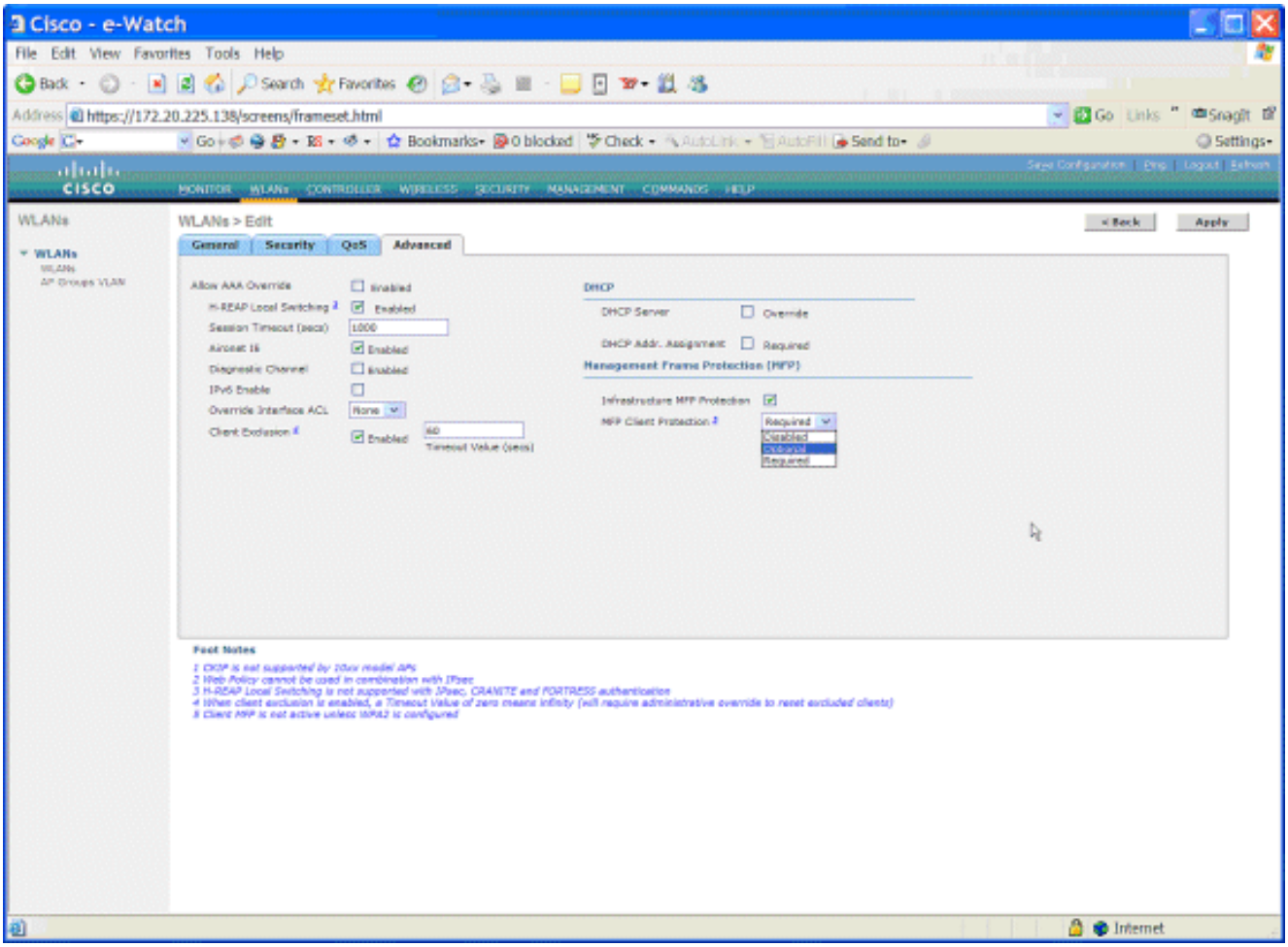
1. WLC GUI에서 **WLANs(WLAN)**를 클릭하고 **New(새로 만들기)**를 클릭하여 새 WLAN을 생성합니다

.



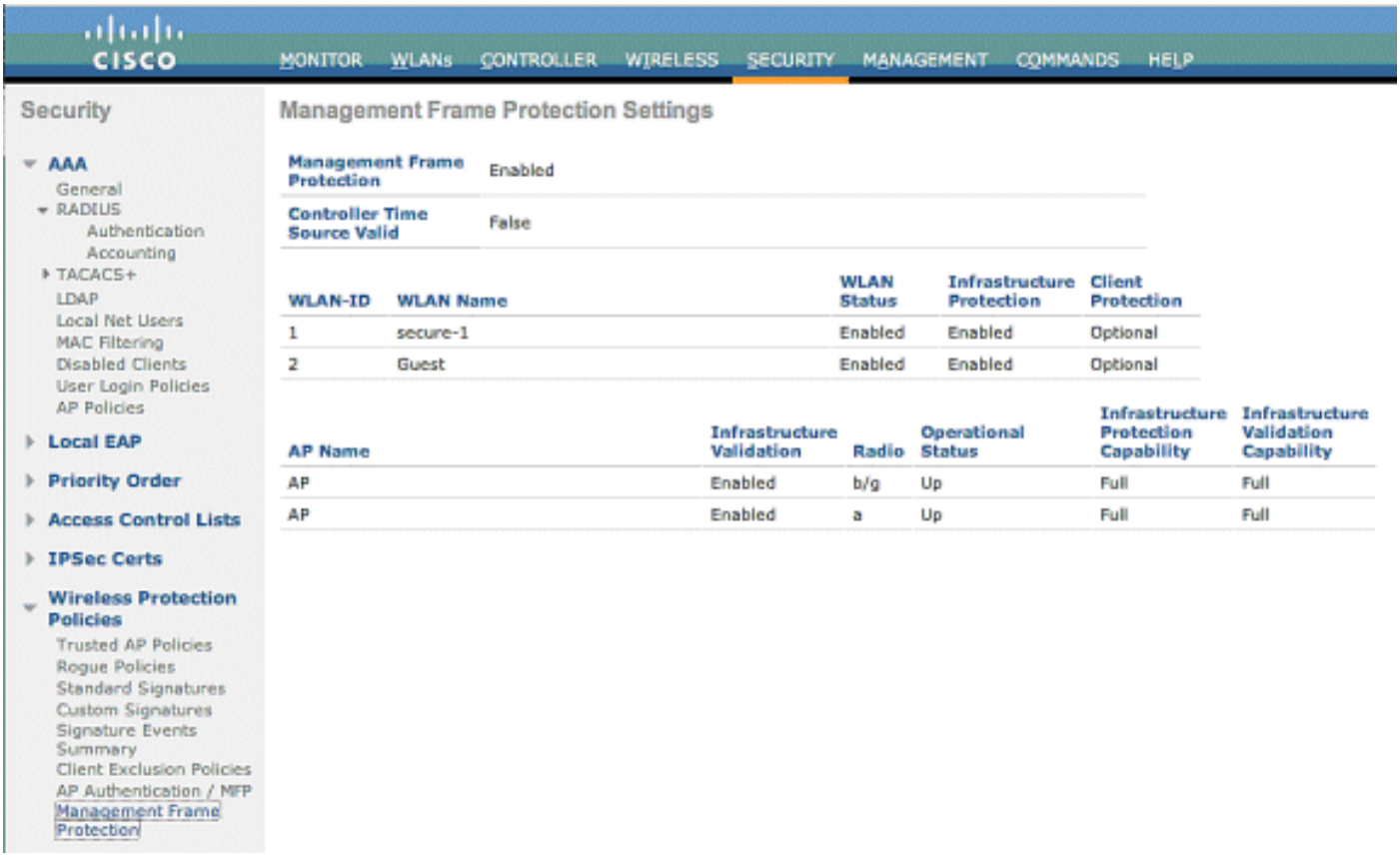
2. WLANs edit(WLAN 수정) 페이지에서 *Advanced(고급)* 탭으로 이동하여 **Infrastructure MFP Protection(인프라 MFP 보호)** 확인란을 선택하여 이 WLAN에서 인프라 MFP를 활성화합니다 .이 WLAN에 대한 인프라 MFP 보호를 비활성화하려면 이 확인란의 선택을 취소합니다.Client MFP를 활성화하려면 드롭다운 메뉴에서 필수 또는 옵션 옵션을 선택합니다.Client MFP= Required(클라이언트 MFP= 필수)를 선택하는 경우 모든 클라이언트가 MFP-2를 지원하는지 또는 연결할 수 없는지 확인합니다.선택 사항을 선택할 경우 MFP 및 비 MFP 지원 클라이언트는 모두 동일한 WLAN에 연결할 수 있습니다

.



다음을 확인합니다.

GUI에서 MFP 컨피그레이션을 확인하려면 Security(보안) 페이지의 Wireless Protection Policies(무선 보호 정책) 아래에서 **Management Frame Protection(관리 프레임 보호)**을 클릭합니다.그러면 MFP 설정 페이지로 이동합니다.



MFP Settings(MFP 설정) 페이지에서 WLC, LAP 및 WLAN의 MFP 컨피그레이션을 확인할 수 있습니다.이것은 예시이다.

- Management Frame Protection(관리 프레임 보호) 필드는 WLC에 대해 MFP가 전역적으로 활성화되었는지 여부를 표시합니다.
- Controller Time Source Valid(컨트롤러 시간 소스 유효) 필드는 WLC 시간이 로컬에서(수동 시간 입력) 설정되는지 아니면 외부 소스(예: NTP 서버)를 통해 설정되는지를 나타냅니다. 시간이 외부 소스에 의해 설정된 경우 이 필드의 값은 "True"입니다. 시간을 로컬로 설정하면 값이 "False"입니다. 시간 소스는 모빌리티가 구성된 서로 다른 WLC의 액세스 포인트 간 관리 프레임을 확인하는 데 사용됩니다.**참고:** 모빌리티/RF 그룹의 모든 WLC에서 MFP가 활성화된 경우 항상 NTP 서버를 사용하여 모빌리티 그룹에서 WLC 시간을 설정하는 것이 좋습니다.
- MFP **Protection(MFP 보호)** 필드에는 개별 WLAN에 대해 MFP가 활성화되어 있는지 여부가 표시됩니다.
- MFP **Validation(MFP 검증)** 필드에는 개별 액세스 포인트에 대해 MFP가 활성화되어 있는지 여부가 표시됩니다.

다음과 같은 show 명령이 도움이 될 수 있습니다.

- **show wps summary** - WLC의 현재 무선 보호 정책(MFP 포함)에 대한 요약을 보려면 이 명령을 사용합니다.
- **show wps mfp summary** - WLC의 현재 전역 MFP 설정을 보려면 이 명령을 입력합니다.
- **show ap config general *AP_name*—**특정 액세스 포인트의 현재 MFP 상태를 보려면 이 명령을 입력합니다.

다음은 **show ap config general *AP_name* 명령**의 출력 **예입니다**.

```
(Cisco Controller) >show ap config general AP

Cisco AP Identifier.............................. 4
```

```
Cisco AP Name..................................... AP
Country code...................................... US  - United States
Regulatory Domain allowed by Country.............. 802.11bg:-AB    802.11a:-AB
AP Country code................................... US  - United States
AP Regulatory Domain.............................. 802.11bg:-A    802.11a:-A
Switch Port Number ............................... 29
MAC Address....................................... 00:19:2f:7e:3a:30
IP Address Configuration.......................... DHCP
IP Address........................................ 172.20.225.142
IP NetMask........................................ 255.255.255.248
Gateway IP Addr................................... 172.20.225.137
Cisco AP Location................................. default location
Cisco AP Group Name............................... default-group
Primary Cisco Switch..............................
Secondary Cisco Switch............................
Tertiary Cisco Switch.............................
Administrative State ............................. ADMIN_ENABLED
Operation State .................................. REGISTERED
Mirroring Mode ................................... Disabled
AP Mode .......................................... H-Reap
Public Safety .................................... Global: Disabled, Local: Disabled
Remote AP Debug .................................. Disabled
S/W  Version ..................................... 4.1.169.24
Boot  Version .................................... 12.3.7.1
Mini IOS Version ................................. 3.0.51.0
Stats Reporting Period ........................... 180
LED State......................................... Enabled
PoE Pre-Standard Switch........................... Disabled
PoE Power Injector MAC Addr....................... Disabled
Number Of Slots................................... 2
AP Model.......................................... AIR-LAP1242AG-A-K9
IOS Version....................................... 12.4(20070414:021809)
Reset Button...................................... Enabled
AP Serial Number.................................. FTX1035B3QX
AP Certificate Type............................... Manufacture Installed
H-REAP Vlan mode :................................ Disabled
Management Frame Protection Validation............ Enabled
Console Login Name................................
Console Login State............................... Unknown
Ethernet Port Duplex.............................. Auto
Ethernet Port Speed............................... Auto
```

다음은 show wps mfp **summary** 명령의 출력의 예입니다.

```
(Cisco Controller) >show wps mfp summary

Global MFP state................................. enabled
Controller Time Source Valid..................... false


                                    WLAN        Infra.      Client
WLAN ID  WLAN Name                  Status      Protection  Protection
-------  -------------------------  ---------   ----------  ----------
1        secure-1                   Enabled     Enabled     Optional
2        Guest                      Enabled     Enabled     Optional but inactive (WPA2 not
configured)

                     Infra.             Operational     --Infra. Capability--
```

```
AP Name                Validation  Radio  State           Protection  Validation
---------------------  ----------  -----  --------------  ----------  ----------
AP                     Enabled     b/g    Up              Full        Full
```

이러한 debug 명령은 유용할 수 있습니다.

- **debug wps mfp lwapp** - MFP 메시지에 대한 디버그 정보를 표시합니다.
- **debug wps mfp detail** - MFP 메시지에 대한 자세한 디버그 정보를 표시합니다.
- **debug wps mfp report** - MFP 보고에 대한 디버그 정보를 표시합니다.
- **debug wps mfp mm**—MFP 모빌리티(컨트롤러 간) 메시지에 대한 디버그 정보를 표시합니다.

참고: 인터넷에서 사용 가능한 무선 패킷 스나이퍼는 여러 가지가 있으며, 이 스위치는 802.11 관리 프레임을 캡처하고 분석하는 데 사용할 수 있습니다.일부 패킷 스니퍼는 Omnpeek 및 Wireshark입니다.

관련 정보

- 보안 솔루션 구성:WLC 컨피그레이션 가이드
- WCS에서 보안 솔루션 구성
- WLAN 컨트롤러(WLC)를 사용한 EAP 인증 컨피그레이션 예
- 무선 LAN 컨트롤러 컨피그레이션의 ACL 예
- 무선 LAN 컨트롤러를 사용한 외부 웹 인증 컨피그레이션 예
- RADIUS 서버 및 무선 LAN 컨트롤러 구성을 통한 동적 VLAN 할당 예
- EAP-FAST 인증을 사용하는 Cisco Secure Services Client
- WLC FAQ
- 무선 지원 페이지
- 기술 지원 및 문서 – Cisco Systems