Konfigurationsbeispiel für Infrastructure Management Frame Protection (MFP) mit WLC und LAP

Inhalt

Einleitung

In diesem Dokument wird eine neue Sicherheitsfunktion in Wireless eingeführt, die als Management Frame Protection (MFP) bezeichnet wird. In diesem Dokument wird auch beschrieben, wie MFP in Infrastrukturgeräten wie Lightweight Access Points (LAPs) und Wireless LAN Controller (WLCs) konfiguriert wird.

Voraussetzungen

Anforderungen

- Kenntnisse der Konfiguration von WLC und LAP für den Basisbetrieb

- Grundkenntnisse der Management-Frames nach IEEE 802.11

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco WLC der Serie 2000 mit Firmware-Version 4.1
- Cisco 1131AG LAP
- Cisco Aironet 802.11a/b/g Client-Adapter mit Firmware-Version 3.6
- Cisco Aironet Desktop Utility Version 3.6

Hinweis: MFP wird von WLC Version 4.0.155.5 und höher unterstützt, obwohl Version 4.0.206.0 die optimale Leistung mit MFP bietet. Client MFP wird ab Version 4.1.171.0 unterstützt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

In 802.11 sind Management-Frames wie (de)authentifizierung, (dis)zuordnung, Beacons und Sonden immer nicht authentifiziert und unverschlüsselt. Anders ausgedrückt: 802.11-Management-Frames werden immer ungesichert gesendet, anders als der Datenverkehr, der mit Protokollen wie WPA, WPA2 oder zumindest WEP verschlüsselt wird.

Dies ermöglicht es einem Angreifer, einen Verwaltungsrahmen vom Access Point zu verfälschen, um einen Client anzugreifen, der einem Access Point zugeordnet ist. Mit gefälschten Management-Frames kann ein Angreifer folgende Aktionen durchführen:

- Führen Sie einen Denial of Service (DOS) im WLAN aus.
- Versuchen Sie, einen Mann in der Mitte des Angriffs auf den Client, wenn er erneut eine Verbindung herstellt.
- Ausführen eines Offline-Wörterbuchangriffs

Das MFP überwindet diese Fehler, wenn es 802.11-Management-Frames authentifiziert, die in der Wireless-Netzwerkinfrastruktur ausgetauscht werden.

Hinweis: Der Schwerpunkt dieses Dokuments liegt auf **Infrastruktur- und Client-MFP**.

Hinweis: Einige Wireless-Clients können nur mit MFP-fähigen Infrastrukturgeräten kommunizieren. MFP fügt jeder Anfrage oder jedem SSID-Beacon eine Reihe von Informationselementen hinzu. Einige Wireless-Clients wie PDAs, Smartphones, Barcode-Scanner usw. verfügen über eingeschränkten Arbeitsspeicher und eine begrenzte CPU. Sie können diese Anfragen oder Beacons also nicht verarbeiten. Infolgedessen wird die SSID nicht vollständig angezeigt, oder Sie können aufgrund eines Missverständnisses der SSID-Funktionen keine Verbindung zu diesen

Infrastrukturgeräten herstellen. Dieses Problem betrifft nicht nur den MFP. Dies gilt auch für alle SSIDs mit mehreren Informationselementen (IEs). Es ist immer ratsam, MFP-*fähige* SSIDs in der Umgebung mit allen verfügbaren Clienttypen zu testen, bevor Sie sie in Echtzeit bereitstellen.

Anmerkung:

Dies sind die Komponenten des Infrastruktur-MFP:

- **Management Frame Protection** - Wenn der Management Frame Protection aktiviert ist, fügt AP jedem Management-Frame, den er überträgt, das Message Integrity Check Information Element (MIC IE) hinzu. Bei jedem Versuch, den Frame zu kopieren, zu verändern oder erneut abzuspielen, wird die MIC ungültig. Ein WAP, der so konfiguriert ist, dass er MFP-Frames validiert, empfängt einen Frame mit ungültiger MIC und meldet diesen an den WLC.
- **Validierung von Management-Frames** - Wenn die Management Frame-Validierung aktiviert ist, validiert der Access Point jeden Management-Frame, den er von anderen APs im Netzwerk empfängt. Es stellt sicher, dass der MIC IE vorhanden ist (wenn der Ausgangspunkt für die Übertragung von MFP-Frames konfiguriert ist) und den Inhalt des Management-Frames abstimmt. Wenn ein Frame empfangen wird, der keinen gültigen MIC IE von einer BSSID enthält, die zu einem AP gehört und für die Übertragung von MFP-Frames konfiguriert ist, meldet er die Diskrepanz zum Netzwerkmanagementsystem.**Hinweis:** Damit die Zeitstempel ordnungsgemäß funktionieren, müssen alle WLCs über das Network Time Protocol (NTP) synchronisiert sein.
- **Ereignisberichte**: Der Access Point benachrichtigt den WLC, wenn er eine Anomalie erkennt. WLC aggregiert die ungewöhnlichen Ereignisse und meldet diese über SNMP-Traps an den Netzwerkmanager.

Infrastruktur-MFP-Funktionalität

Mit MFP werden alle Management-Frames kryptografisch gehasht, um eine Message Integrity Check (MIC) zu erstellen. Das MIC wird am Ende des Frames (vor der Frame Check Sequence (FCS)) hinzugefügt.

- In einer zentralisierten Wireless-Architektur ist Infrastruktur-MFP auf dem WLC aktiviert/deaktiviert (globale Konfiguration). Der Schutz kann selektiv pro WLAN deaktiviert werden, und die Validierung kann pro WAP selektiv deaktiviert werden.
- Der Schutz kann in WLANs deaktiviert werden, die von Geräten verwendet werden, die keine zusätzlichen IEs bewältigen können.
- Die Validierung muss bei APs deaktiviert werden, die überlastet oder überlastet sind.

Wenn MFP auf einem oder mehreren im WLC konfigurierten WLANs aktiviert ist, sendet der WLC jedem Funkmodul eines registrierten WAP einen eindeutigen Schlüssel. Verwaltungs-Frames werden vom AP über die MFP-fähigen WLANs gesendet. Diese APs sind mit einem Frame Protection MIC IE gekennzeichnet. Bei jedem Versuch, den Frame zu ändern, wird die Nachricht ungültig. Dies bewirkt, dass der empfangende Access Point, der so konfiguriert ist, dass er MFP-Frames erkennt, die Diskrepanz dem WLAN-Controller meldet.

Hierbei handelt es sich um einen schrittweisen MFP-Prozess, der in einer Roaming-Umgebung implementiert wird:

1. Wenn MFP global aktiviert ist, generiert der WLC einen eindeutigen Schlüssel für jeden

AP/WLAN, der für MFP konfiguriert ist. WLCs kommunizieren untereinander, sodass alle WLCs die Schlüssel für alle APs/BSSs in einer Mobilitätsdomäne kennen.**Hinweis:** Für alle Controller in einer Mobility-/RF-Gruppe muss MFP identisch konfiguriert sein.

2. Wenn ein AP einen MFP-geschützten Frame für ein BSS empfängt, über das er nicht Bescheid weiß, puffert er eine Kopie des Frames und fragt den WLC ab, um den Schlüssel abzurufen.
3. Wenn die BSSID auf dem WLC nicht bekannt ist, wird die Meldung "Unknown BSSID" (Unbekannter BSSID) an den AP zurückgegeben, und der Access Point verwirft die von diesem BSSID empfangenen Management-Frames.
4. Wenn die BSSID auf dem WLC bekannt ist, MFP jedoch auf dieser BSSID deaktiviert ist, gibt der WLC die Option "Disabled BSSID" (Deaktivierte BSSID) zurück. Der Access Point geht dann davon aus, dass alle Management-Frames, die von dieser BSSID empfangen werden, über kein MFP-MIC verfügen.
5. Wenn die BSSID bekannt ist und MFP aktiviert ist, gibt der WLC den MFP-Schlüssel an den anfordernden AP zurück (über den AES-verschlüsselten LWAPP-Managementtunnel).
6. Der AP zwischenspeichert die Schlüssel, die auf diese Weise empfangen wurden. Dieser Schlüssel wird zum Validieren oder Hinzufügen von MIC IE verwendet.

Client-MFP-Funktionalität

Client MFP schützt authentifizierte Clients vor Spoofing-Frames, was die Effektivität vieler häufiger Angriffe auf WLANs verhindert. Die meisten Angriffe, wie z. B. Deauthentifizierungs-Angriffe, kehren zu schlicht herabgesetzter Leistung zurück, wenn sie mit gültigen Clients konkurrieren.

Client-MFP verschlüsselt Verwaltungs-Frames, die zwischen Access Points und CCXv5-Clients gesendet werden, sodass sowohl Access Points als auch Clients vorbeugende Maßnahmen ergreifen und gefälschte Management-Frames der Klasse 3 (d. h. Management-Frames, die zwischen einem Access Point und einem authentifizierten und zugeordneten Client übergeben werden) verwerfen können. Client MFP nutzt die von IEEE 802.11i definierten Sicherheitsmechanismen, um diese Typen von Unicast-Management-Frames der Klasse 3 zu schützen: Trennung, Entauthentifizierung und QoS (WMM)-Aktion. Client MFP kann eine Client-Access Point-Sitzung vor den häufigsten Denial-of-Service-Angriffen schützen. Sie schützt Management-Frames der Klasse 3 mit derselben Verschlüsselungsmethode, die auch für die Datenframes der Sitzung verwendet wird. Wenn ein vom Access Point oder Client empfangener Frame nicht entschlüsselt werden kann, wird er verworfen, und das Ereignis wird an den Controller gemeldet.

Um Client-MFP verwenden zu können, müssen Clients CCXv5 MFP unterstützen und WPA2 entweder mit TKIP oder AES-CCMP aushandeln. EAP oder PSK kann zum Erhalt des PMK verwendet werden. Das CCKM- und das Controller-Mobilitätsmanagement dienen zur Verteilung von Sitzungsschlüsseln zwischen Access Points oder dem schnellen Layer-2- und Layer-3-Roaming.

Um Angriffe auf Broadcast-Frames zu verhindern, geben Access Points, die CCXv5 unterstützen, keine Broadcast Class 3-Management-Frames aus (z. B. Trennung, Dekonauthentifizierung oder Aktion). CCXv5-Clients und Access Points müssen Management-Frames der Broadcast-Klasse 3 verwerfen.

Client MFP ergänzt die Infrastruktur-MFP, anstatt sie zu ersetzen, da Infrastruktur-MFP weiterhin ungültige Unicast-Frames erkennt und an Clients meldet, die nicht Client-MFP-fähig sind, sowie

ungültige Management-Frames der Klassen 1 und 2. Infrastruktur-MFP wird nur auf Management-Frames angewendet, die nicht durch Client-MFP geschützt sind.

Client-MFP-Komponenten

Client MFP besteht aus den folgenden Komponenten:

- Schlüsselgenerierung und -verteilung
- Schutz und Validierung von Management-Frames
- Fehlerberichte

Schlüsselgenerierung und -verteilung

Client MFP verwendet nicht die wichtigsten Erzeugungs- und Verteilungsmechanismen, die für Infrastruktur-MFP abgeleitet wurden. Stattdessen nutzt der Client-MFP die durch IEEE 802.11i definierten Sicherheitsmechanismen, um auch Unicast-Management-Frames der Klasse 3 zu schützen. Stationen müssen CCXv5 unterstützen und entweder TKIP oder AES-CCMP aushandeln, um MFP für Clients verwenden zu können. EAP oder PSK kann zum Erhalt des PMK verwendet werden.

Schutz von Management-Frames

Management-Frames der Unicast-Klasse 3 werden mit der Anwendung von AES-CCMP oder TKIP auf ähnliche Weise geschützt wie bereits für Daten-Frames verwendet. Teile des Frame-Headers werden zur zusätzlichen Absicherung in die verschlüsselte Payload-Komponente jedes Frames kopiert, wie in den nächsten Abschnitten beschrieben.

Diese Frame-Typen sind geschützt:

- Zerfall
- Deauthentifizierung
- QoS (WMM) Action-Frames

AES-CCMP- und TKIP-geschützte Datenrahmen enthalten einen Sequenzzähler in den IV-Feldern, der verwendet wird, um die Erkennung von Wiederholungen zu verhindern. Der aktuelle Transmit-Zähler wird sowohl für Daten- als auch für Management-Frames verwendet, für Management-Frames wird jedoch ein neuer Empfangszähler verwendet. Die Empfangs-Zähler werden getestet, um sicherzustellen, dass jeder Frame eine höhere Zahl als der zuletzt empfangene Frame hat (um sicherzustellen, dass die Frames eindeutig sind und nicht wiedergegeben wurden), sodass es nicht darauf ankommt, dass dieses Schema die empfangenen Werte als nicht sequenziell angibt.

Fehlerberichte

Die MFP-1-Reporting-Mechanismen werden verwendet, um von Access Points erkannte Fehler bei der Entkapselung von Verwaltungsrahmen zu melden. Das heißt, der WLC sammelt Statistiken zu Fehlern bei der MFP-Validierung und leitet die erfassten Informationen regelmäßig an das WCS weiter.

Die von Client-Stationen erkannten MFP-Verletzungsfehler werden von der CCXv5-Funktion für Roaming und Echtzeit-Diagnose behandelt und sind nicht in diesem Dokument enthalten.

Broadcast Management Frame-Schutz

Um Angriffe zu verhindern, die Broadcast-Frames verwenden, übertragen Access Points, die CCXv5 unterstützen, keine Broadcast Class 3 (d. h. disassoc, defekt oder action)-Management-Frames, außer bei Frames zur Deauthentifizierung und Trennung von nicht autorisierten Containments. CCXv5-fähige Client-Stationen müssen Management-Frames der Broadcast-Klasse 3 verwerfen. MFP-Sitzungen werden als in einem ordnungsgemäß gesicherten Netzwerk (starke Authentifizierung plus TKIP oder CCMP) angesehen, sodass die Nichtbeachtung von nicht autorisierten Containment-Broadcasts kein Problem darstellt.

Ebenso verwerfen APs eingehende Broadcast-Management-Frames. Derzeit werden keine eingehenden Broadcast-Management-Frames unterstützt, daher sind hierfür keine Codeänderungen erforderlich.

Unterstützte Plattformen

Diese Plattformen werden unterstützt:

- WLAN-Controller200621064400WiSM3750 mit integriertem 440x-ControllerRouter 26/28/37/38xx
- LWAPP Access PointsAP 1000AP 1100, 1130AP 1200, 1240, 1250AP 1310
- Client-SoftwareADU 3.6.4 und höher
- NetzwerkmanagementsystemeWCS

Der 1500 Mesh LWAPP AP wird in dieser Version nicht unterstützt.

Unterstützte Modi

LWAPP-basierte Access Points, die in diesen Modi betrieben werden, unterstützen Client MFP:

Unterstützte Access Point-Modi	
Modus	**Client-MFP-Unterstützung**
Lokal	Ja
Überwachung	Nein
Sniffer	Nein
Rogue-Erkennung	Nein
Hybrid-REAP	Ja
REAP	Nein
Bridge-Root	Ja
WGB	Nein

Unterstützung für gemischte Zellen

Client-Stationen, die nicht CCXv5-fähig sind, können einem MFP-2-WLAN zugeordnet werden. Die Access Points verfolgen, welche Clients MFP-2-fähig sind und welche nicht, um zu bestimmen, ob MFP-2-Sicherheitsmaßnahmen auf ausgehende Unicast-Management-Frames angewendet und bei eingehenden Unicast-Management-Frames erwartet werden.

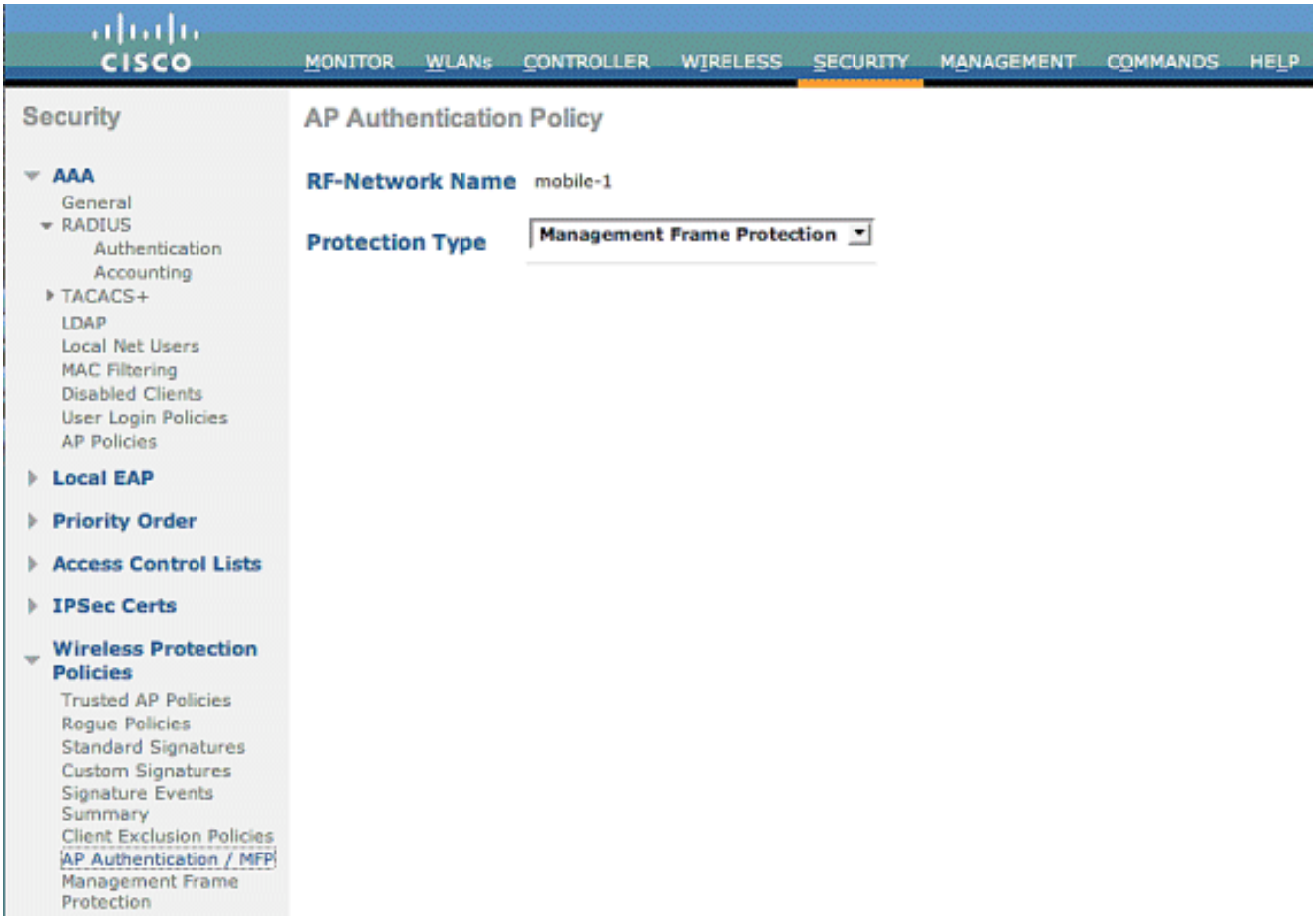
Konfigurieren

Konfigurieren von MFP auf einem Controller

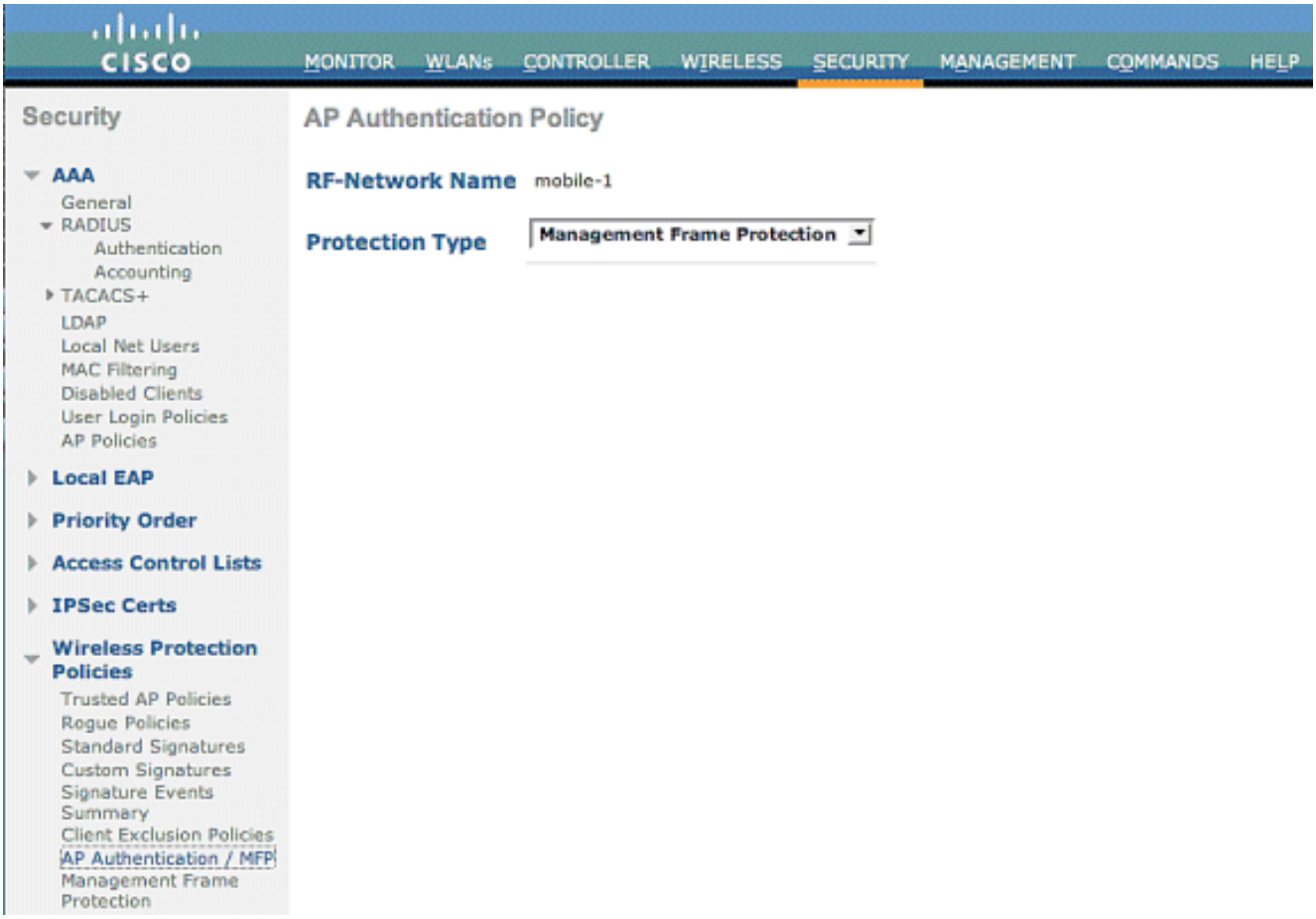
Sie können MFP auf einem Controller global konfigurieren. In diesem Fall **sind** der **Schutz und die Validierung von Management-Frames standardmäßig für jeden verbundenen Access Point aktiviert**, und die Authentifizierung von Access Points wird automatisch deaktiviert.

Führen Sie diese Schritte aus, um MFP global auf einem Controller zu konfigurieren.

1. Klicken Sie in der Controller-GUI auf **Sicherheit**. Klicken Sie im sich daraus ergebenden Bildschirm unter **Wireless Protection Policies (Wireless-Schutzrichtlinien)** auf **AP Authentication/MFP**.



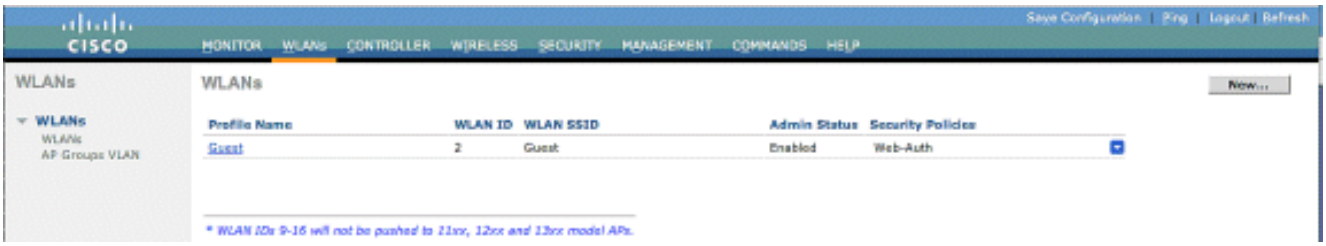
2. Wählen Sie im Dropdown-Menü **Protection Type** (**Schutztyp**) der Option AP Authentication Policy (AP-Authentifizierungsrichtlinie) die Option **Management Frame Protection (Management-Frame-Schutz**) aus, und klicken Sie auf **Apply**.



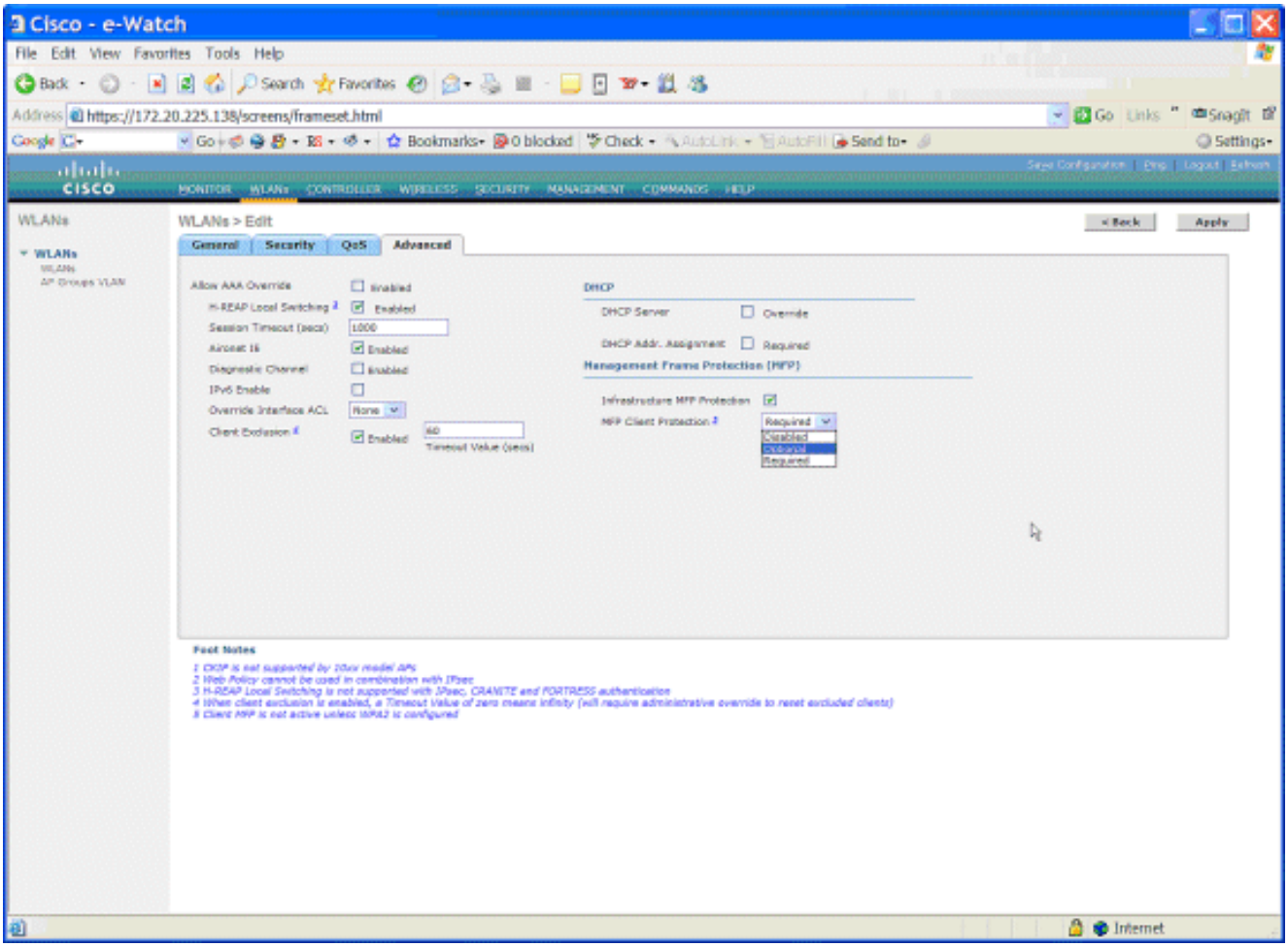
Konfigurieren von MFP für WLAN

Sie können auch den Infrastruktur-MFP-Schutz und Client-MFP für jedes WLAN aktivieren/deaktivieren, das auf dem WLC konfiguriert ist. Beide sind standardmäßig über den Infrastruktur-MFP-Schutz aktiviert, der nur aktiviert ist, wenn er global aktiviert ist, und der Client-MFP ist nur aktiv, wenn das WLAN mit WPA2-Sicherheit konfiguriert ist. Führen Sie die folgenden Schritte aus, um MFP in einem WLAN zu aktivieren:

1. Klicken Sie in der WLC-GUI auf **WLANs** und dann auf **Neu**, um ein neues WLAN zu erstellen.

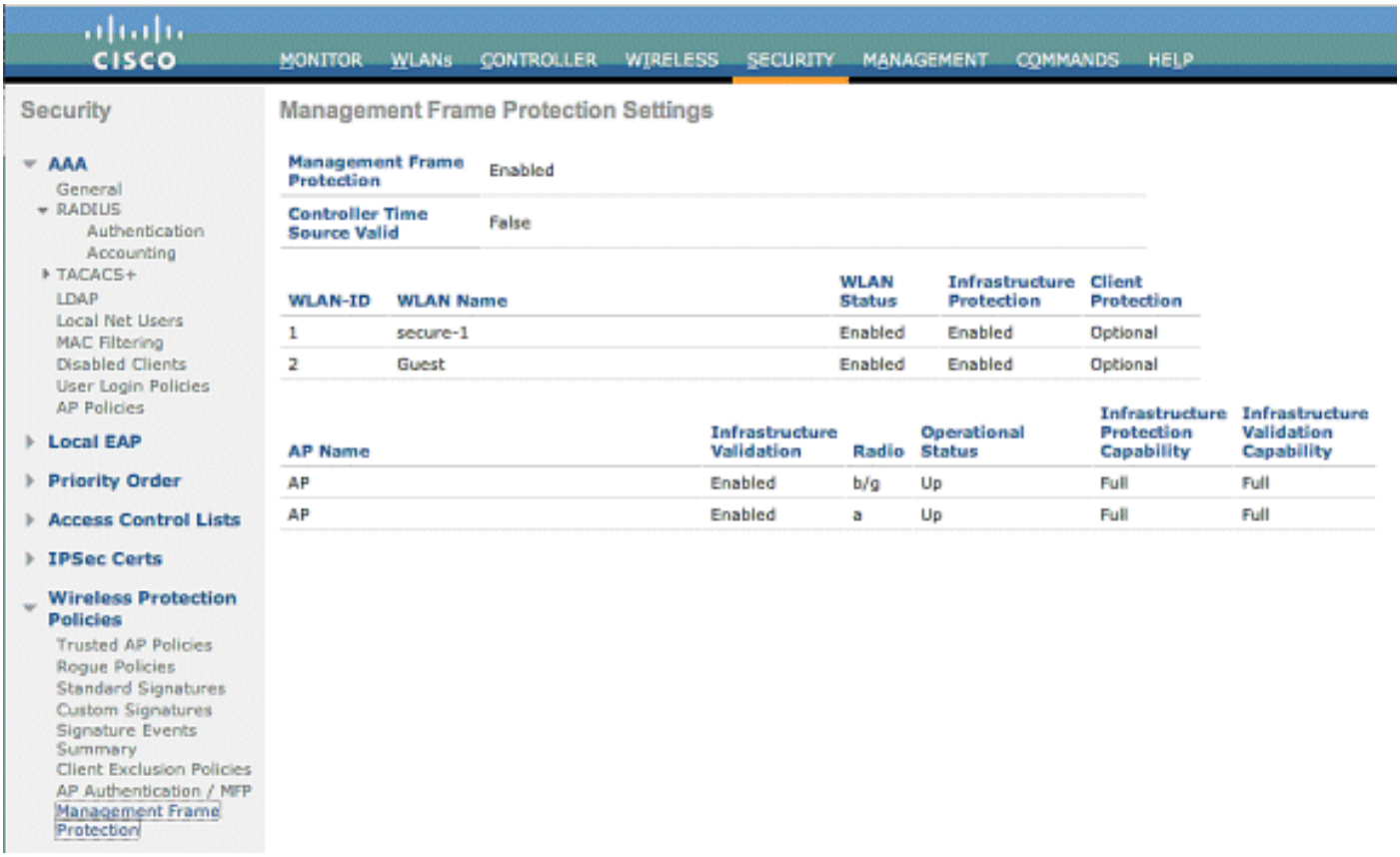


2. Wechseln Sie auf der Bearbeitungsseite für WLANs zur Registerkarte *Erweitert*, und aktivieren Sie das Kontrollkästchen **Infrastruktur-MFP-Schutz**, um den Infrastruktur-MFP für dieses WLAN zu aktivieren. Um den Infrastruktur-MFP-Schutz für dieses WLAN zu deaktivieren, deaktivieren Sie dieses Kontrollkästchen. Um Client MFP zu aktivieren, wählen Sie im Dropdown-Menü die gewünschte oder optionale Option aus. Wenn Sie Client MFP= Required auswählen, stellen Sie sicher, dass alle Ihre Clients MFP-2 unterstützen oder keine Verbindung herstellen können. Wenn Sie optional auswählen, können sowohl MFP- als auch Nicht-MFP-fähige Clients über dasselbe WLAN verbunden
werden.



Überprüfung

Um die MFP-Konfigurationen über die Benutzeroberfläche zu überprüfen, klicken Sie auf der Seite Sicherheit unter Wireless Protection Policies (Wireless-Schutzrichtlinien) auf **Management Frame Protection (Management-Frame-Schutz**). Dadurch gelangen Sie zur Seite "MFP Settings" (MFP-Einstellungen).



Auf der Seite "MFP Settings" (MFP-Einstellungen) wird die MFP-Konfiguration auf dem WLC, der LAP und dem WLAN angezeigt. Dies ist ein Beispiel.

- Das Feld Management Frame Protection (Management-Frame-Schutz) zeigt an, ob MFP global für den WLC aktiviert ist.
- Das Feld Controller Time Source Valid (Controller-Zeitquelle gültig) gibt an, ob die WLC-Zeit lokal (durch manuelle Eingabe der Zeit) oder über eine externe Quelle (z. B. einen NTP-Server) festgelegt wird. Wenn die Uhrzeit von einer externen Quelle festgelegt wird, lautet der Wert dieses Felds "True". Wenn die Uhrzeit lokal festgelegt wird, ist der Wert "False". Die Zeitquelle wird zur Validierung von Management-Frames zwischen Access Points verschiedener WLCs verwendet, für die ebenfalls Mobilität konfiguriert ist.**Hinweis:** Wenn MFP auf allen WLCs in einer Mobility-/RF-Gruppe aktiviert ist, wird immer empfohlen, zur Einstellung der WLC-Zeit in einer Mobilitätsgruppe einen NTP-Server zu verwenden.
- Das Feld **MFP-Schutz** zeigt an, ob MFP für einzelne WLANs aktiviert ist.
- Das Feld **MFP-Validierung** zeigt an, ob MFP für einzelne Access Points aktiviert ist.

Diese Befehle können hilfreich sein:

- **show wps summary** - Verwenden Sie diesen Befehl, um eine Zusammenfassung der aktuellen Wireless-Schutzrichtlinien (einschließlich MFP) des WLC anzuzeigen.
- **show wps mfp summary** - Geben Sie diesen Befehl ein, um die aktuelle globale MFP-Einstellung des WLC anzuzeigen.
- **show ap config general *AP_name*** - Geben Sie diesen Befehl ein, um den aktuellen MFP-Status für einen bestimmten Access Point anzuzeigen.

Dies ist ein Beispiel für die Ausgabe des Befehls **show ap config general *AP_name***:

```
(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
```

Dies ist ein Beispiel für die Ausgabe des Befehls **show wps mfp summary**:

```
(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
```

Diese Debug-Befehle können hilfreich sein.

- **debug wps mfp lwapp**: Zeigt Debuginformationen für MFP-Nachrichten an.
- **debug wps mfp detail**: Zeigt detaillierte Debuginformationen für MFP-Nachrichten an.
- **debug wps mfp report**: Zeigt Debuginformationen für MFP-Reporting.
- **debug wps mfp mm**: Zeigt Debuginformationen für MFP-Mobilitätsnachrichten (zwischen Controllern).

Hinweis: Im Internet stehen außerdem mehrere kostenlose Wireless-Paket-Sniffer zur Verfügung, mit denen die 802.11-Management-Frames erfasst und analysiert werden können. Einige Beispiele für Paket-Sniffer sind Omnipeek und Wireshark.

Zugehörige Informationen

- Konfigurieren von Sicherheitslösungen: WLC-Konfigurationsleitfaden
- Konfigurieren von Sicherheitslösungen in WCS
- Konfigurationsbeispiel für EAP-Authentifizierung mit WLAN-Controllern (WLC)
- Konfigurationsbeispiel für ACLs in Wireless LAN-Controllern
- Konfigurationsbeispiel für die externe Webauthentifizierung mit Wireless LAN-Controllern
- Konfigurationsbeispiel für dynamische VLAN-Zuweisung mit RADIUS-Server und Wireless LAN-Controller
- Cisco Secure Services Client mit EAP-FAST-Authentifizierung
- WLC FAQ
- Wireless-Support-Seite
- Technischer Support und Dokumentation für Cisco Systeme