Infrastructuurbeheer Frame Protection (MFP) met WLC en LAP-configuratievoorbeeld

Inhoud

Inleiding

Dit document introduceert een nieuwe beveiligingsfunctie in de draadloze controller Management Frame Protection (MFP). Dit document beschrijft ook hoe u MFP kunt configureren in infrastructurele apparaten, zoals lichtgewicht access points (LAP's) en draadloze LAN-controllers (WLC's).

Voorwaarden

Vereisten

- Kennis van de manier waarop u de WLC en LAP voor een eenvoudige bediening kunt configureren
- Basiskennis van de beheerframes IEEE 802.11

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 2000 Series WLC-software met release 4.1
- Cisco 1131AG LAP
- Cisco Aironet 802.11a/b/g clientadapter voor firmware release 3.6
- Cisco Aironet desktophulpprogramma versie 3.6

Opmerking: MFP wordt ondersteund door WLC versie 4.0.15.5 en hoger, hoewel versie 4.0.206.0 de optimale prestaties met MFP biedt. ClientMFP wordt ondersteund op versie 4.1.17.1.0 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

In 802.11 zijn beheerframes zoals (de)authenticatie, (dis)associatie, bakens en sondes altijd niet echt bevonden en niet gecodeerd. Met andere woorden, 802.11 beheerframes worden altijd verzonden op een onbeveiligde manier, in tegenstelling tot het gegevensverkeer, dat versleuteld is met protocollen als WAP, WAP2 of, op zijn minst, EVN, enzovoort.

Dit staat een aanvaller toe om van een beheerkader van AP een cliënt aan te vallen die aan AP verbonden is. Met de gespoofde beheerframes kan een aanvaller deze acties uitvoeren:

- Start een Denial of Service (DOS) op WLAN
- Probeer een man in het midden aan te vallen op de cliënt wanneer hij opnieuw aansluit
- Een offline woordenboekaanval uitvoeren

MFP overtreft deze valkuilen wanneer het 802.11 beheerframes authentificeert die in de draadloze netwerkinfrastructuur worden uitgewisseld.

Opmerking: Dit document is gericht op **infrastructuur en client-MFP**.

Opmerking: Er zijn bepaalde beperkingen voor bepaalde draadloze klanten om te communiceren met MFP-enabled-infrastructuurelementen. MFP voegt een lange reeks informatie elementen toe aan elk sonde verzoek of SSID baken. Sommige draadloze klanten zoals PDA's, smartphones, barcodes scanners, enzovoort hebben een beperkt geheugen en een centrale verwerkingseenheid. Dus je kunt deze verzoeken of bakens niet verwerken. Als resultaat hiervan, ziet u SSID niet volledig of kunt u niet met deze infrastructuren associëren, door misverstanden van de mogelijkheden van SSID. Deze kwestie is niet specifiek voor MFP. Dit gebeurt ook met elke SSID die meerdere informatie-elementen (IE's) heeft. Het is altijd raadzaam om MFP *enabled* SSIDs op de omgeving te testen met al uw beschikbare clienttypen voordat u deze in real time implementeert.

Opmerking:

Dit zijn de onderdelen van MFP-infrastructuur:

- **Beheerskader bescherming**-Wanneer de bescherming van het beheerkader is ingeschakeld, voegt AP bericht integriteit controle informatie element (MIC IE) aan elk beheerkader toe dat het overdraagt. Elke poging om het kader te kopiëren, wijzigen of opnieuw af te spelen maakt de MIC ongeldig. AP, dat wordt gevormd om MFP frames te valideren ontvangt een kader met ongeldige MIC, meldt het aan WLC.
- **Validering van het beheerframe**-wanneer de validatie van het beheerframe is ingeschakeld, bevestigt AP elk beheerkader dat het van andere APs in het netwerk ontvangt. Dit waarborgt dat de MIC IE aanwezig is (wanneer de originator is ingesteld om MFP-frames door te geven) en de inhoud van het beheerkader aanpast. Als het een kader ontvangt dat geen geldig MIC IE van een BSSID bevat dat tot een AP behoort, dat wordt geconfigureerd om MFP-frames door te geven, rapporteert het de discrepantie aan het netwerkbeheersysteem.**Opmerking:** Om de tijdstempels goed te laten werken, moeten alle WLCs gesynchroniseerd zijn in Network Time Protocol (NTP).
- **Rapportage van gebeurtenis**—Het toegangspunt waarschuwt de WLC wanneer het een anomalie detecteert. WLC aggregeert de anomalische gebeurtenissen en rapporteert het door SNMP vallen aan de netwerkmanager.

MFP-functies voor infrastructuur

Met MFP worden alle beheerframes cryptografisch opgeslagen om een Berichtintegriteitscontrole (MIC) te maken. Het MIC wordt toegevoegd aan het einde van het frame (vóór de Frame Control Sequence (FCS)).

- In een gecentraliseerde draadloze architectuur wordt de infrastructuur MFP op de WLC in/uit gezet (globale configuratie). Bescherming kan selectief worden uitgeschakeld per WLAN, en validatie kan selectief worden uitgeschakeld per AP.
- Bescherming kan worden uitgeschakeld aan de WLAN's die worden gebruikt door apparaten die niet met extra IE's kunnen worden geconfronteerd.
- De validatie moet worden uitgeschakeld op AP's die overbelast of overbelast zijn.

Wanneer MFP is ingeschakeld op een of meer WLAN's die in de WLC zijn geconfigureerd, stuurt de WLC-applicatie een unieke sleutel naar elke geregistreerde AP. Beheerframes worden door AP via de MFP-enabled WLAN's verzonden. Deze AP's worden geëtiketteerd met een kader bescherming MIC IE. Elke poging om het frame te wijzigen maakt het bericht ongeldig, waardoor de ontvangende AP die is ingesteld om MFP-frames te detecteren, dit naar de WLAN-controller gaat.

Dit is een stapsgewijs MFP-proces, maar wordt uitgevoerd in een roamingomgeving:

1. Als MFP mondiaal ingeschakeld is, genereert het WLC een unieke sleutel voor elke AP/WLAN die is ingesteld voor MFP. WLC's communiceren binnen zichzelf zodat alle WLC's de sleutels van alle AP's/BSS's in een mobiliteitsdomein kennen.**Opmerking:** Alle controllers in een mobiliteit/RF-groep moeten op identieke wijze zijn geconfigureerd.
2. Wanneer een AP een MFP beschermd kader voor een BSS ontvangt dat zij niet over weet, buffert het een exemplaar van het kader en vraagt WLC om de sleutel te krijgen.
3. Als BSSID niet op WLC bekend is, keert het het bericht "Onbekende BSSID" terug aan AP,

en AP daalt de beheerkaders die van die BSSID worden ontvangen.
4. Als BSSID op WLC bekend is maar MFP op die BSSID wordt uitgeschakeld, keert WLC een "Gehandicapte BSSID" terug. Het AP veronderstelt dan dat alle beheerframes die van BSSID worden ontvangen geen MFP MIC hebben.
5. Als de BSSID bekend is en MFP is ingeschakeld, retourneert de WLC de MFP-toets naar de verzoekende AP (via de AES-gecodeerde LWAPP beheertunnel).
6. Op deze manier ontvangen AP-caches. Deze toets wordt gebruikt om MIC IE te valideren of toe te voegen.

ClientMFP-functies

Client MFP beschermt voor beveiligde clients van gespoofde frames, die de effectiviteit van veel gemeenschappelijke aanvallen tegen draadloze LAN's verhinderen. De meeste aanvallen, zoals de aanvallen van de authenticatie, keren terug naar de eenvoudigweg aangetaste prestaties wanneer ze botsen met geldige klanten.

Met name versleutelt client-MFP beheerframes die tussen toegangspunten en CCXv5-klanten worden verstuurd, zodat zowel toegangspunten als klanten preventieve actie kunnen ondernemen en gespoofde klasse 3 beheerframes (d.w.z. beheerframes die tussen een toegangspunt en een cliënt worden doorgegeven en die voor authentiek en geassocieerd is) kunnen laten vallen. ClientMFP maakt gebruik van de beveiligingsmechanismen die door IEEE 802.11i zijn gedefinieerd om deze typen beheerframes van klasse 3 te beschermen: disassociatie, decodering en QoS-actie (WMM). Client MFP kan een client-access point sessie beschermen tegen het meest gebruikelijke type 'denial-of-service'-aanval. Het beschermt class 3 beheerframes met dezelfde coderingsmethode die gebruikt wordt voor de gegevensframes van de sessie. Als een kader dat door het toegangspunt of de client wordt ontvangen, niet decryptie heeft, wordt het ingetrokken en wordt de gebeurtenis aan de controller gemeld.

Om MFP van een client te gebruiken moeten klanten CCXv5 MFP ondersteunen en moeten zij met WAP2 onderhandelen met TKIP of AES-CCMP. EAP of PSK kan worden gebruikt om de PMK te verkrijgen. CCKM en het mobiliteitsbeheer van controllers worden gebruikt om de sessies tussen toegangspunten of Layer 2 en Layer 3 snelle roaming te verdelen.

Om aanvallen tegen uitgezonden frames te voorkomen, zenden toegangspunten die CCXv5 ondersteunen geen uitzending uit van uitzending class 3 beheerframes (zoals disassociatie, deverificatie of actie). CCXv5-clients en toegangspunten moeten kabeltelevisieklasse 3-beheerframes weggooien.

ClientMFP vult infrastructuur MFP aan in plaats van deze te vervangen, omdat infrastructuren MFP ongeschikte eenastframes blijft detecteren en rapporteren die naar klanten worden gestuurd die niet geschikt zijn voor client-MFP, evenals ongeldige beheersframes van klasse 1 en 2. Infrastructuur MFP wordt alleen toegepast op beheerframes die niet door client MFP worden beschermd.

ClientMFP-componenten

ClientMFP bestaat uit deze componenten:

- Belangrijkste productie en distributie
- Bescherming en validatie van beheerframes

- Foutrapporten

Belangrijkste generatie en distributie

ClientMFP maakt geen gebruik van de sleutelgeneratie- en distributiesystemen die voor infrastructuur MFP zijn afgeleid. In plaats daarvan maakt client-MFP gebruik van de beveiligingsmechanismen die door IEEE 802.11i zijn gedefinieerd om ook klasse 3-beheerframes te beschermen. Stations moeten CCXv5 ondersteunen en moeten onderhandelen over TKIP of AES-CCMP om gebruik te maken van actieve MFP. EAP of PSK kan worden gebruikt om de PMK te verkrijgen.

Bescherming van beheerframes

Niet-geordende beheersframes van klasse 3 worden met de toepassing van ofwel AES-CCMP ofwel TKIP op een zelfde manier beschermd als die al gebruikt werd voor gegevensframes. De delen van de kop van het frame worden gekopieerd naar de gecodeerde payload-component van elk frame voor extra bescherming, zoals besproken in de volgende secties.

Deze frame-typen zijn beveiligd:

- disassociatie
- Verificatie
- QoS-actiekaders (WM)

Met AES-CCMP- en TKIP-beschermde gegevensframes bevatten een sequentieteller in de IV-velden, die wordt gebruikt om herhalingsdetectie te voorkomen. De huidige zendteller wordt gebruikt voor zowel gegevens als beheerframes, maar een nieuwe ontvangt teller wordt gebruikt voor beheerframes. De ontvangt tellers worden getest om te verzekeren dat elk kader een hoger aantal heeft dan het laatst ontvangen frame (om ervoor te zorgen dat de frames uniek zijn en niet zijn weergegeven), dus het geeft niet uit dat dit schema ervoor zorgt dat de ontvangen waarden niet sequentieel zijn.

Foutenmeldingen

MFP-1 rapportagemechanismen worden gebruikt om door toegangspunten gedetecteerde fouten in beheerframe-de-insluitingsfouten te melden. Dat wil zeggen, de WLC verzamelt MFI - valideringsfoutstatistieken en stuurt periodiek verzamelde informatie naar de WCS door.

MFP-overschrijdingsfouten die door clientstations zijn gedetecteerd, worden verwerkt door de optie CCXv5-roaming en realtime-diagnostiek en zijn niet in het toepassingsgebied van dit document opgenomen.

Bescherming voor breedbandbeheer

Om aanvallen te voorkomen die uitzendframes gebruiken, verzenden AP's die CCXv5 ondersteunen geen kabelbeheerframes 3 (d.w.z. disassoc-, deauth- of action) uit, behalve voor valse isolatie-/disassociatieframes. CCXv5-kabelstations moeten kabelstations van omroepklasse 3-beheerframes afwijzen. MFP-sessies worden verondersteld in een goed beveiligd netwerk te zijn (sterke authenticatie plus TKIP of CCMP), zodat het niet in acht nemen van aanvallen op uitzendingen van rotatiebeheersing geen probleem is.

Op dezelfde manier ontdoen APs inkomende uitzending beheerframes. Er worden momenteel geen inkomende uitzendbeheerframes ondersteund, dus er zijn hiervoor geen codewijzigingen vereist.

Ondersteunde platforms

Deze platforms worden ondersteund:

- WLAN-controllers200621064400WiSM3750 met ingesloten 40x-controller26/28/37/38xx routers
- LWAPP access pointsAP 1000AP 1100, 1130AP 1200, 1240, 1250AP 1310
- ClientsoftwareADU 3.6.4 en hoger
- NetwerkbeheersystemenWCS

AP met 1500 mesh LWAPP wordt niet ondersteund in deze release.

Ondersteunde modellen

Op LWAPP gebaseerde access points die op deze modi werken ondersteunen clientadaptertools voor MFP:

Ondersteunde access point modules	
Modus	**Ondersteuning van client-MFP**
Lokaal	Ja
monitor	Nee
Sniffer	Nee
schoordetectie	Nee
Hybride REAP	Ja
REAP	Nee
Bridge Root	Ja
WGB	Nee

Ondersteuning van gemengde cellen

Clientstations die niet geschikt zijn voor CCXv5 kunnen zich associëren met een MFP-2 WLAN. De toegangspunten houden bij welke cliënten MFP-2 kunnen worden gebruikt en welke niet kunnen bepalen of MFP-2 beveiligingsmaatregelen worden toegepast op uitgaande beheersframes voor het beheer van het net en worden verwacht op inkomende beheerframes voor het beheer van het net.

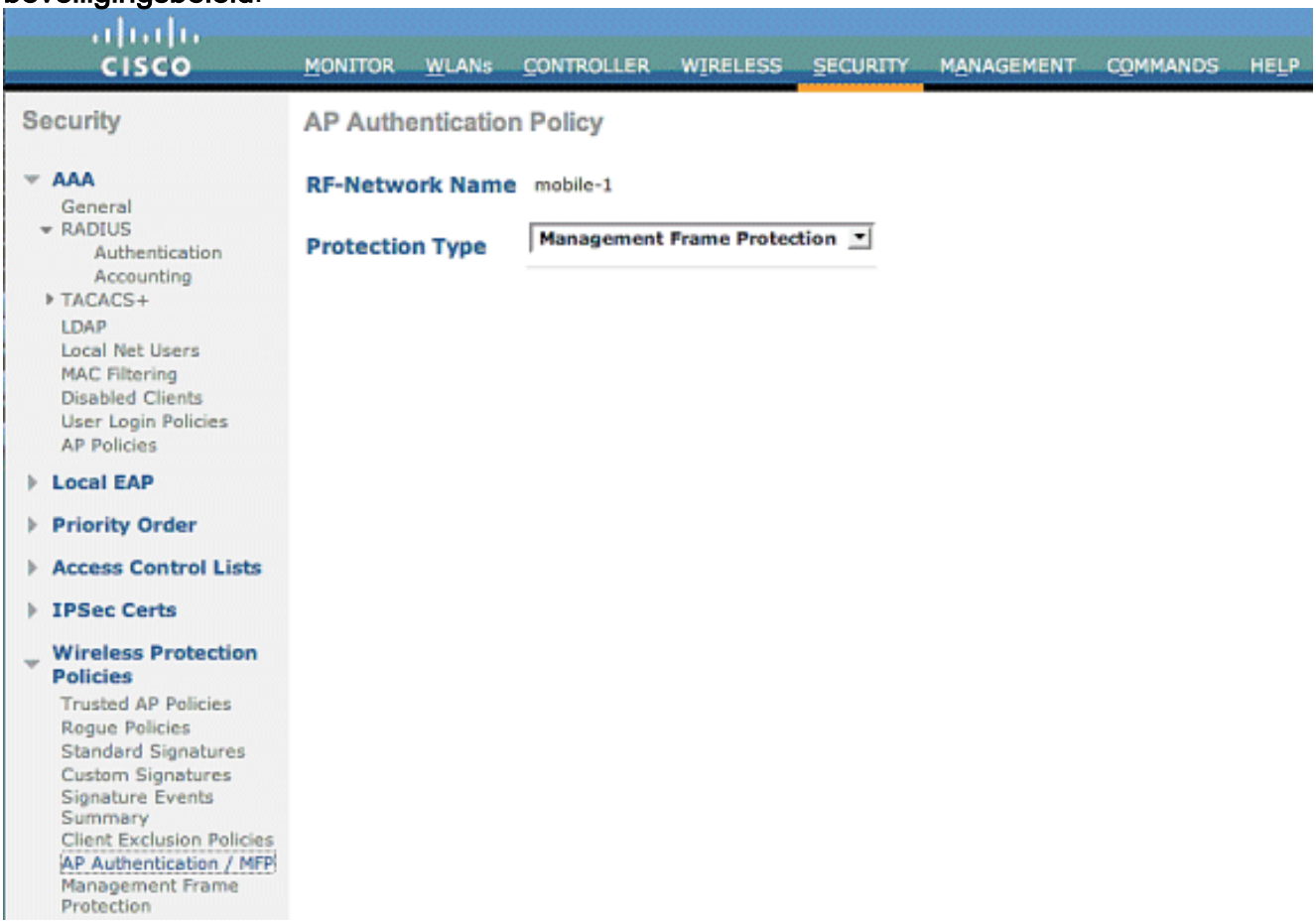
Configureren

MFP op een controller configureren

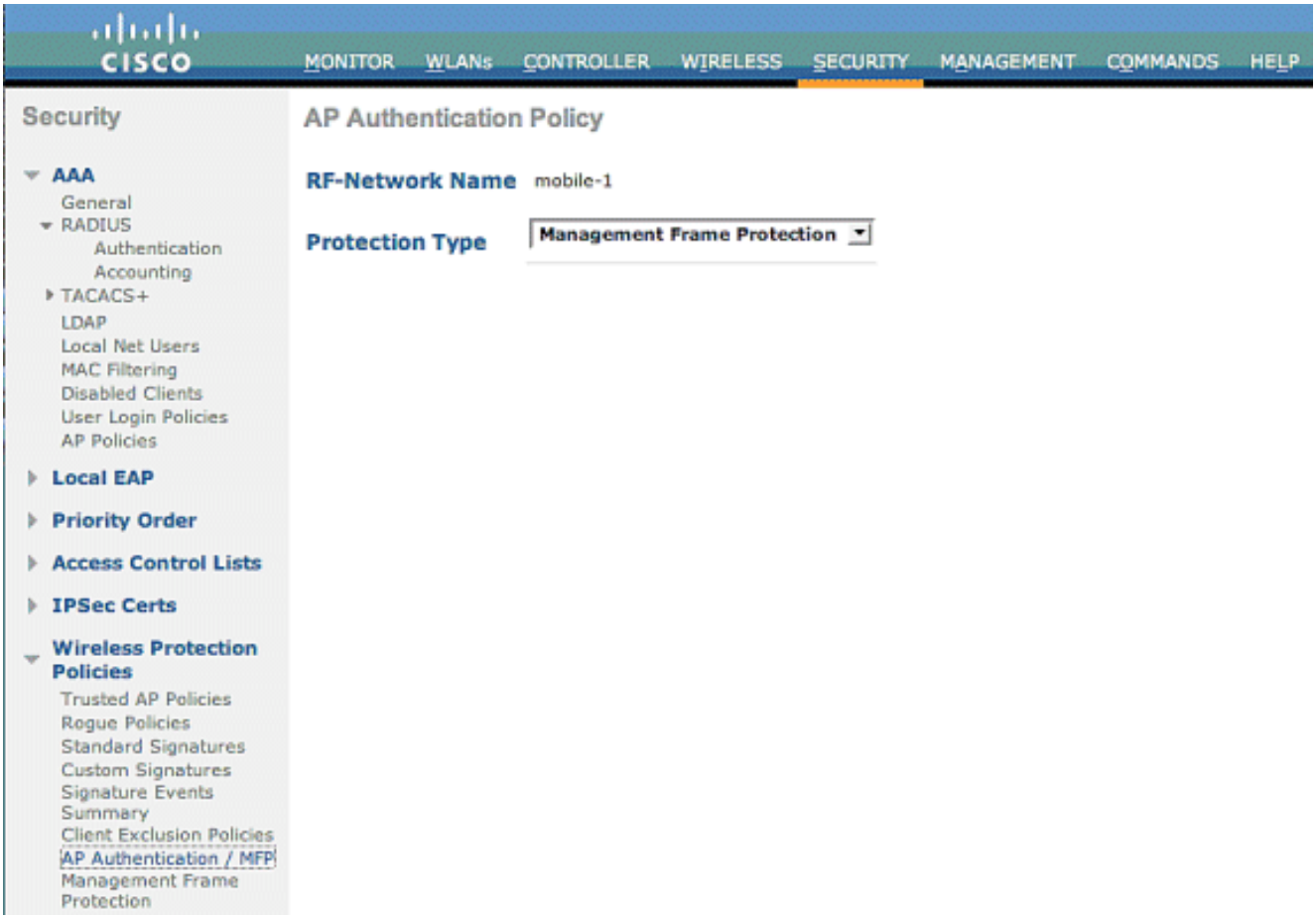
U kunt MFP over de hele wereld op een controller configureren. Wanneer u dit doet, **wordt de bescherming en validatie van het beheerframe standaard ingeschakeld voor elk aangesloten toegangspunt**, en de authenticatie van het toegangspunt wordt automatisch uitgeschakeld.

Voer deze stappen uit om MFP mondiaal aan te passen op een controller.

1. Klik vanuit de controller GUI op **Security**. Klik in het resulterende scherm op **AP-verificatie/MFP** onder **Draadloos beveiligingsbeleid**.



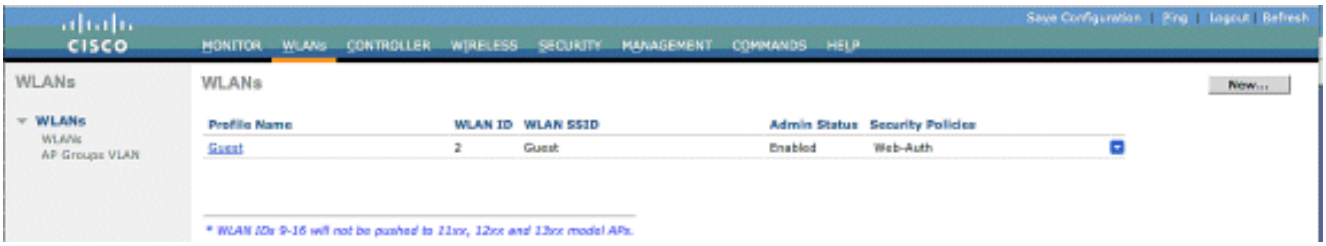
2. Kies in het vervolgkeuzemenu AP Verificatiebeleid de optie **Frame Protection Protection** (**Type** bescherming) en klik op **Toepassen**.



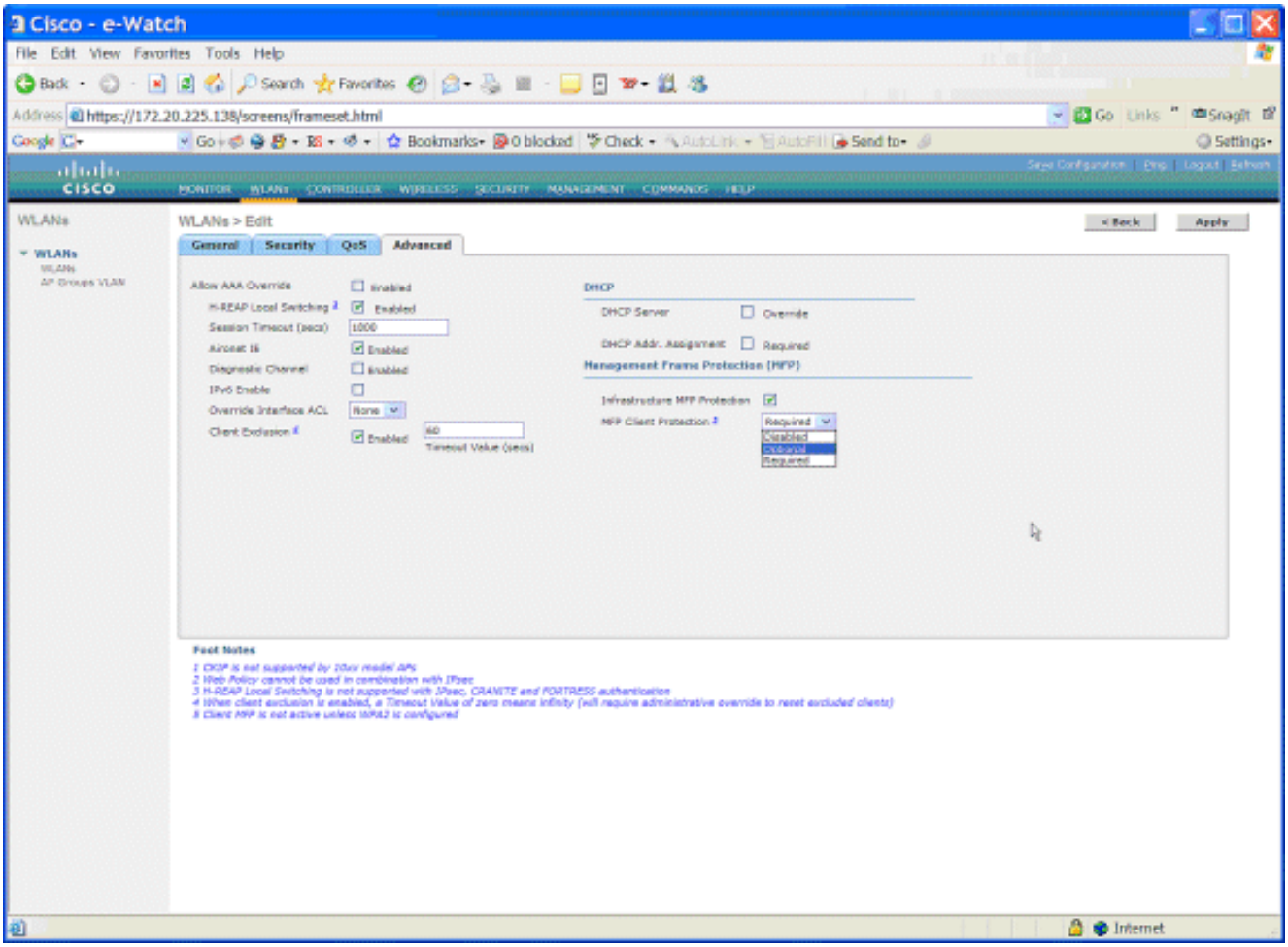
MFP configureren op WLAN

U kunt ook MFP-bescherming van de infrastructuur en MFP van de client en MFP inschakelen/uitschakelen bij elke WLAN die op de WLC zijn geconfigureerd. Beide worden standaard ingeschakeld door middel van MFP-bescherming van de infrastructuur, die alleen actief is als deze globaal ingeschakeld is, en MFP van de client alleen actief is als WLAN is geconfigureerd met WAP-beveiliging. Volg deze stappen om MFP op een WLAN:

1. Klik vanuit de WLC GUI op **WLAN's** en klik op **New** om een nieuwe WLAN-functie te creëren.

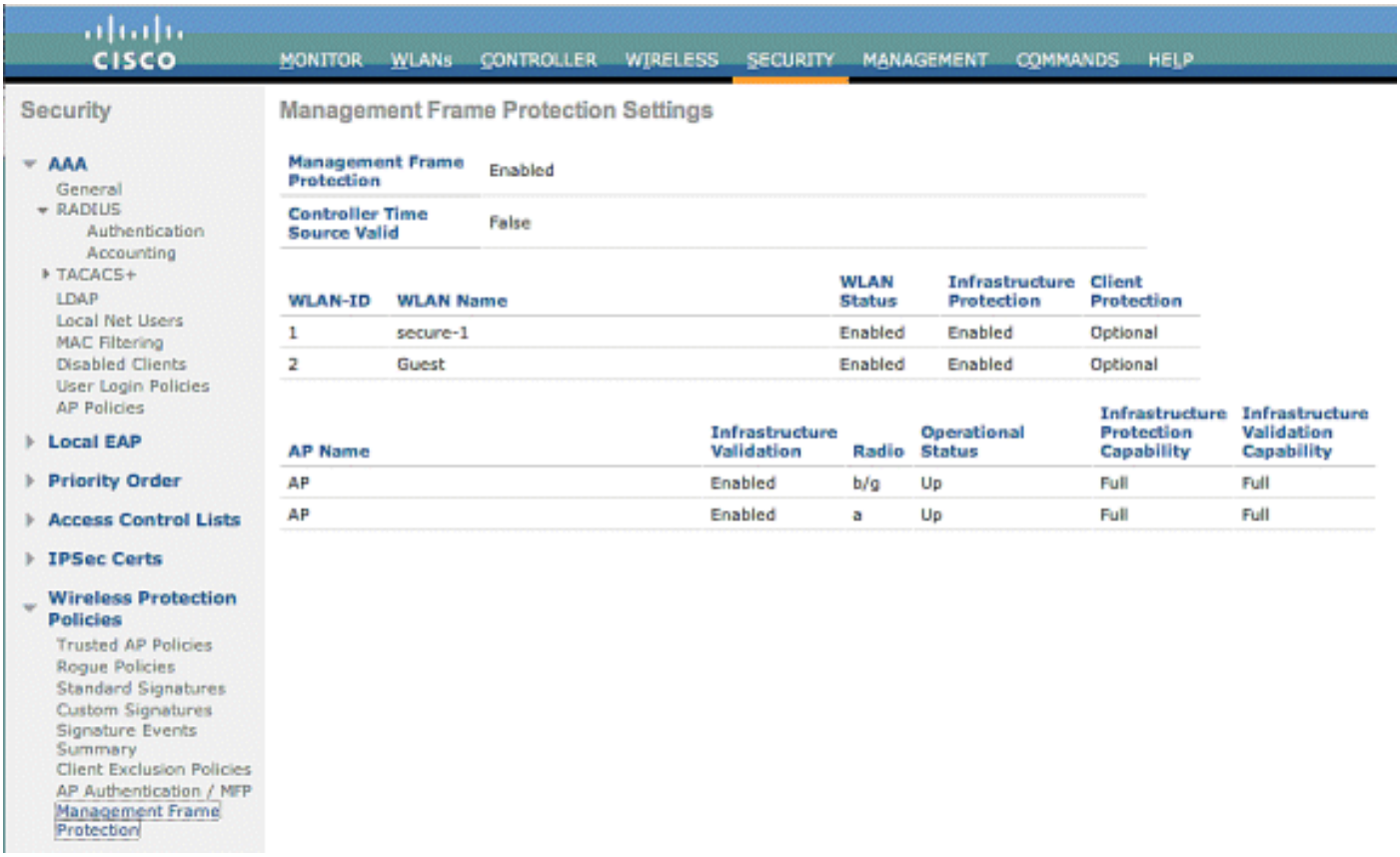


2. Ga in de WLAN's bewerkpagina naar het *tabblad Geavanceerd* en controleer het dialoogvenster **Infrastructuur MFP bescherming** om de infrastructuur MFP op dit WLAN in te schakelen. Schakel dit aankruisvakje uit om infrastructuur MFP-beveiliging voor dit WLAN uit te schakelen. Selecteer de gewenste of optionele optie in het vervolgkeuzemenu om Client MFP in te schakelen. Als u client MFP= verplicht kiest, zorg er dan voor dat al uw klanten ondersteuning hebben voor MFP-2 of dat ze geen verbinding kunnen maken. Als u optioneel kiest, kunnen zowel MFP- als niet-MFP-enabled-clients op dezelfde WLAN worden aangesloten.



Verifiëren

Om de MFP-configuraties vanuit de GUI te controleren, klikt u op **Beheersframe-bescherming** onder Draadloos beveiligingsbeleid op de beveiligingspagina. Dit brengt u naar de pagina MFP-instellingen.



In de pagina MFP-instellingen kunt u de MFP-configuratie zien op het WLC, LAP en WLAN. Dit is een voorbeeld.

- Het veld Beheersframe Protection toont aan of MFP mondiaal is ingeschakeld voor de WLC.
- Het veld Tijdbron van de controller geeft aan of de WLC-tijd lokaal is ingesteld (door handmatige invoer van de tijd) of via een externe bron (zoals een NTP-server). Als de tijd door een externe bron is ingesteld, is de waarde van dit veld "True". Als de tijd lokaal is ingesteld, is de waarde "False". De tijdbron wordt gebruikt om beheerframes tussen toegangspunten van verschillende WLC's te valideren die ook mobiliteit hebben ingesteld.**Opmerking:** Als MFP is ingeschakeld voor alle WLC's in een mobiliteits-/RF-groep, wordt altijd aanbevolen om een NTP-server te gebruiken om de WLC-tijd in een mobiliteitsgroep in te stellen.
- Het veld **MFP-bescherming** toont of MFP is ingeschakeld voor afzonderlijke WLAN's.
- Het veld **MFP-validatie** laat zien of MFP is ingeschakeld voor afzonderlijke toegangspunten.

Deze tonen opdrachten kunnen behulpzaam zijn:

- **toon samenvatting** - gebruik deze opdracht om een samenvatting van het huidige beleid voor draadloze beveiliging (met inbegrip van MFP) van de WLC te zien.
- **Laat de samenvatting van Wps-mfp zien** - om de huidige globale MFP instelling van de WLC te zien, voer deze opdracht in.
- **Toon ap web*AP_name*** —Om de huidige MFP staat voor een bepaald toegangspunt te zien, voer deze opdracht in.

Dit is een voorbeeld van de output van de **show ap opdracht *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
```

Dit is een voorbeeld van de output van de **summiere** opdracht van **show wps mfp**:

```
(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
```

Deze debug-opdrachten kunnen behulpzaam zijn.

- **debug wps mfp lwapp** - toont debug informatie voor MFP-berichten.
- **debug Wps mfp-detail**: toont gedetailleerde debug-informatie voor MFP-berichten.
- **debug-rapport van wps** - toont debug-informatie voor MFP-rapportage.
- **debug WP mm**-toont debug informatie voor MFP-mobiliteit (inter-controller) berichten.

Opmerking: Er zijn ook verschillende gratis draadloze Packet sluipschutters beschikbaar via het internet, die kunnen worden gebruikt om de 802.11 beheerframes op te nemen en te analyseren. Sommige voorbeelden van pakketsluipschutters zijn Omnipeek en Wireshark.

Gerelateerde informatie

- Beveiligingsoplossingen configureren: WLC-configuratiegids
- Beveiligingsoplossingen in WCS configureren
- PPP-verificatie met WLAN-controllers (WLC) - configuratievoorbeeld
- Configuratievoorbeeld van ACL's op draadloze LAN-controllers
- Configuratievoorbeeld voor externe webverificatie met draadloze LAN-controllers
- Configuratievoorbeeld van dynamische VLAN-toewijzing met RADIUS-server en draadloze LAN-controllers
- Cisco Secure Services-client met EAP-FAST-verificatie
- WLC FAQ
- Draadloze ondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems