حماية إطار إدارة البنية الأساسية (MFP) مع عرض الوصول في نقاط الوصول في تكوين مثال WLC و Lightweight (LAP)

المحتويات

المقدمة

يقدم هذا المستند ميزة أمان جديدة في الشبكة اللاسلكية تسمى حماية إطار الإدارة (MFP). يصف هذا المستند أيضا كيفية تكوين MFP في أجهزة البنية الأساسية، مثل نقاط الوصول في الوضع Lightweight (LAPs) ووحدات التحكم في شبكة LAN اللاسلكية (WLCs).

المتطلبات الأساسية

المتطلبات

- معرفة كيفية تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ونقاط الوصول في الوضع Lightweight للتشغيل الأساسي

- معرفة أساسية بإطارات إدارة IEEE 802.11

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco 2000 Series WLC الذي يشغل البرنامج الثابت، الإصدار 4.1
- نقطة الوصول Cisco 1131AG LAP
- مهايئ عميل Cisco Aironet 802.11a/b/g الذي يشغل البرنامج الثابت، الإصدار 3.6
- Cisco Aironet Desktop Utility، الإصدار 3.6

ملاحظة: يتم دعم MFP من WLC الإصدار 4.0.155.5 والإصدارات الأحدث، رغم أن الإصدار 4.0.206.0 يوفر الأداء الأمثل مع MFP. يتم دعم MFP للعميل على الإصدار 4.1.171.0 والإصدارات الأعلى.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

في 802.11، تكون إطارات الإدارة مثل (de)المصادقة، (dis)الاقتران، المرشدات، والمستكشفات غير مصدق عليها وغير مشفرة دائما. بمعنى آخر، غالبا ما يتم إرسال إطارات الإدارة 802.11 بطريقة غير آمنة، بخلاف حركة مرور البيانات، والتي يتم تشفيرها ببروتوكولات مثل WPA2 ،WPA، أو على الأقل، WEP، وهكذا دواليك.

وهذا يسمح للمهاجم بانتحال إطار إدارة من نقطة الوصول لمهاجمة عميل مرتبط بنقطة وصول. باستخدام إطارات الإدارة المنتحلة، يمكن للمهاجم تنفيذ هذه الإجراءات:

- تشغيل حجب الخدمة (DoS) على شبكة WLAN
- حاول تنفيذ هجوم على العميل أثناء إعادة الاتصال
- تشغيل هجوم القاموس غير المتصل

تتغلب MFP على هذه المزالق عندما تصادق إطارات الإدارة 802.11 المتبادلة في البنية الأساسية للشبكة اللاسلكية.

ملاحظة: يركز هذا المستند على **Infrastructure و Client MFP**.

ملاحظة: هناك قيود معينة مفروضة على بعض الأجهزة العميلة اللاسلكية للاتصال بأجهزة البنية الأساسية التي تم تمكين MFP عليها. تضيف MFP مجموعة طويلة من عناصر المعلومات لكل طلب تحقيق أو منارة SSID. تتمتع بعض الأجهزة اللاسلكية مثل أجهزة المساعد الرقمي الشخصي (PDA) والهواتف الذكية والماسحات الضوئية للرمز الشريطي وما إلى ذلك بذاكرة محدودة ووحدة معالجة مركزية (CPU). لذلك لا يمكنك معالجة هذه الطلبات أو أجهزة الإرشاد. ونتيجة لذلك، تفشل في رؤية SSID بشكل كامل، أو يتعذر عليك الاقتران بأجهزة البنية الأساسية هذه، بسبب سوء فهم إمكانات SSID. هذا إصدار ليس خاص إلى MFP. ويحدث ذلك أيضا مع أي SSID يحتوي على عناصر معلومات متعددة (IEs). من المستحسن دائما إختبار SSIDs *التي تم تمكين* MFP عليها في البيئة باستخدام جميع أنواع العملاء المتاحة لديك قبل نشرها في الوقت الفعلي.

ملاحظة:

هذه هي مكونات MFP للبنية الأساسية:

- **حماية إطار الإدارة**- عند تمكين حماية إطار الإدارة، تضيف نقطة الوصول عنصر معلومات التحقق من سلامة الرسائل (MIC IE) إلى كل إطار إدارة تنقله. تؤدي أي محاولة لنسخ الإطار أو تعديله أو إعادة تشغيله إلى إبطال الميكروفون. نقطة الوصول، التي تم تكوينها للتحقق من صحة إطارات MFP، تتلقى إطارا بميكروفون غير صالح، وتقوم بإبلاغها إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
- **التحقق من إطار الإدارة**—عند تمكين التحقق من إطار الإدارة، يتحقق نقطة الوصول من صحة كل إطار إدارة تتلقاه من نقاط وصول أخرى في الشبكة. يضمن أن يكون MIC IE موجودا (عندما يتم تكوين المنشئ لإرسال إطارات MFP) ويطابق محتوى إطار الإدارة. إذا كان يستلم أي إطار لا يحتوي على MIC IE صالح من BSSID ينتمي إلى AP، والذي تم تكوينه لإرسال إطارات MFP، فإنه يبلغ عن الاختلاف إلى نظام إدارة الشبكة.**ملاحظة:** لكي تعمل الطوابع الزمنية بشكل صحيح، يجب أن تكون جميع مجموعات التحكم في الشبكة المحلية اللاسلكية (WLC) متزامنة مع بروتوكول وقت الشبكة (NTP).
- **الإبلاغ عن الأحداث** — تقوم نقطة الوصول بإعلام عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) عند اكتشافها لخطأ ما. تقوم WLC بتجميع الأحداث غير العادية والإبلاغ عنها من خلال إختبارات SNMP إلى مدير الشبكة.

وظائف MFP للبنية الأساسية

باستخدام MFP، يتم تجزئة جميع إطارات الإدارة بطريقة تشفير لإنشاء تحقق من سلامة الرسائل (MIC). تتم إضافة الميكروفون إلى نهاية الإطار (قبل تسلسل التحقق من الإطارات (FCS)).

- في بنية لاسلكية مركزية، يتم تمكين/تعطيل MFP للبنية الأساسية على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) (التكوين العام). يمكن تعطيل الحماية انتقائيا لكل شبكة محلية لاسلكية (WLAN)، كما يمكن تعطيل التحقق من الصحة انتقائيا لكل نقطة وصول.
- يمكن تعطيل الحماية على شبكات WLAN التي يتم إستخدامها من قبل الأجهزة التي لا يمكنها التعامل مع ملفات IE الإضافية.
- يجب تعطيل التحقق من الصحة على نقاط الوصول (APs) التي تم تحميلها بشكل زائد أو تجاوزها.

عندما يتم تمكين MFP على شبكة WLAN واحدة أو أكثر تم تكوينها في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، يرسل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مفتاحا فريدا إلى كل جهاز لاسلكي على كل نقطة وصول مسجلة. يتم إرسال إطارات الإدارة بواسطة نقطة الوصول عبر شبكات WLAN التي تم تمكين MFP بها. يتم تسمية نقاط الوصول هذه بملف IE لميكروفون لحماية الإطارات. تؤدي أي محاولة لتغيير الإطار إلى إبطال الرسالة، مما يتسبب في جعل نقطة الوصول المتلقية التي تم تكوينها للكشف عن إطارات MFP للإبلاغ عن الاختلاف إلى وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN).

هذه عملية تدريجية ل MFP أثناء تنفيذها في بيئة تجوال:

1. مع تمكين MFP بشكل عام، تولد WLC مفتاح فريد لكل نقطة وصول / WLAN يتم تكوينه ل MFP. تتصل وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs) ببعضها البعض حتى تعرف جميع وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs) مفاتيح جميع نقاط الوصول (APs)/وحدات التحكم في الشبكة المحلية اللاسلكية (BSSs) في مجال قابلية التنقل.**ملاحظة:** يجب أن تحتوي جميع وحدات التحكم في مجموعة قابلية التنقل/التردد اللاسلكي على MFP مكونة بشكل متماثل.
2. عندما يستلم ap إطار MFP محمي ل BSS لا يعرف عنه، هو يخزن نسخة من الإطار ويستعلم ال WLC أن يحصل المفتاح.
3. إذا لم يكن BSSID معروفا على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فإنه يرجع الرسالة "BSSID غير معروف" إلى نقطة الوصول، وتقوم نقطة الوصول بإسقاط إطارات الإدارة المتلقاة من معرف فئة المورد (BSSID) هذا.
4. إذا كان BSSID معروفا على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، ولكن MFP معطل على BSSID، ترجع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) "معرف فئة مورد (BSSID) معطل". يفترض نقطة الوصول بعد ذلك أن جميع إطارات الإدارة المتلقاة من تلك BSSID ليس بها MFP MIC.
5. إذا كان معرف فئة المورد (BSSID) معروفا وتم تمكين MFP به، فإن عنصر التحكم في الشبكة المحلية

اللاسلكية (WLC) يقوم بإرجاع مفتاح MFP إلى نقطة الوصول (عبر نفق إدارة AES المشفر LWAPP).
6. تقوم نقاط الوصول بتخزين المفاتيح التي تم تلقيها بهذه الطريقة. يستخدم هذا المفتاح للتحقق من صحة IE لميكروفون أو إضافته.

وظائف MFP للعميل

تقوم أجهزة MFP العميلة بحماية العملاء المصادق عليهم من الإطارات المنتحلة، مما يمنع فعالية العديد من الهجمات الشائعة ضد الشبكات المحلية اللاسلكية. معظم الهجمات، مثل هجمات إلغاء المصادقة، ترجع إلى الأداء المخفض ببساطة عندما تتعامل مع عملاء صالحين.

تحديدا، يقوم العميل MFP بتشفير إطارات الإدارة المرسلة بين نقاط الوصول وعملاء CCXv5 حتى يمكن لنقاط الوصول والعملاء إتخاذ إجراء وقائي وإسقاط إطارات الإدارة المنتحلة من الفئة 3 (أي إطارات الإدارة التي يتم تمريرها بين نقطة وصول وعميل تتم مصادقته والاقتران به). تستفيد أجهزة MFP العميلة من آليات الأمان التي يحددها IEEE 802.11i لحماية هذه الأنواع من إطارات إدارة البث الأحادي من الفئة 3: إجراءات إلغاء الاقتران وإلغاء المصادقة جودة الخدمة (WMM). يمكن لجهاز الإرسال/الاستقبال العميل حماية جلسة عمل نقطة وصول العميل من النوع الأكثر شيوعا لهجوم رفض الخدمة. إنه يحمي إطارات الإدارة من الفئة 3 بنفس طريقة التشفير المستخدمة لإطارات بيانات الجلسة. في حالة فشل فك تشفير إطار تم إستقباله بواسطة نقطة الوصول أو العميل، يتم إسقاطه ويتم إبلاغ الحدث إلى وحدة التحكم.

من أجل إستخدام MFP العميل، يجب على العملاء دعم CCXv5 MFP ويجب عليهم التفاوض WPA2 مع إما TKIP أو AES-CCMP. يمكن إستخدام EAP أو PSK للحصول على CCKM. PMK ووحدة تحكم حركية إدارة استعملت أن يوزع مفتاح جلسة بين نقاط الوصول أو طبقة 2 و 3 تجوال سريع.

لمنع الهجمات ضد إطارات البث، لا تصدر نقاط الوصول التي تدعم CCXv5 أي إطارات إدارة من الفئة 3 للبث (مثل إلغاء الاقتران أو إلغاء المصادقة أو الإجراء). يجب أن يتجاهل عملاء CCXv5 ونقاط الوصول إطارات إدارة فئة البث 3.

يكمل MFP العميل البنية الأساسية MFP بدلا من إستبدالها لأن MFP للبنية الأساسية تستمر في اكتشاف إطارات البث الأحادي غير الصالحة المرسلة إلى العملاء التي لا تدعم MFP-العميل بالإضافة إلى إطارات الإدارة غير الصالحة من الفئة 1 و 2 والإبلاغ عنها. يتم تطبيق MFP للبنية الأساسية فقط على إطارات الإدارة التي لا تكون محمية بواسطة MFP العميل.

مكونات MFP للعميل

يتكون MFP العميل من المكونات التالية:

- إنشاء المفتاح وتوزيعه
- حماية أطر الإدارة والتحقق منها
- تقارير الأخطاء

إنشاء المفتاح وتوزيعه

لا تستخدم MFP العميل آليات إنشاء وتوزيع المفاتيح التي تم اشتقاقها ل MFP للبنية الأساسية. وبدلا من ذلك، يعمل بروتوكول MFP الخاص بالعميل على زيادة فعالية آليات الأمان المعرفة بواسطة IEEE 802.11i لحماية إطارات إدارة البث الأحادي من الفئة 3 أيضا. يجب أن تدعم المحطات CCXv5 ويجب أن تتفاوض إما TKIP أو AES-CCMP لاستخدام MFP المحلي. يمكن إستخدام EAP أو PSK للحصول على PMK.

حماية إطارات الإدارة

تتم حماية إطارات إدارة فئة 3 للبث الأحادي باستخدام تطبيق إما AES-CCMP أو TKIP بطريقة مماثلة لتلك

المستخدمة بالفعل لإطارات البيانات. يتم نسخ أجزاء من رأس الإطار في مكون الحمولة المشفرة لكل إطار من أجل حماية إضافية، كما هو موضح في الأقسام التالية.

تكون أنواع الإطارات هذه محمية:

- إنفصال
- إلغاء المصادقة
- إطارات عمل جودة الخدمة (WMM)

تتضمن إطارات البيانات المحمية ب AES-CCMP و TKIP عداد تسلسل في حقول IV، والذي يستخدم لمنع اكتشاف إعادة التشغيل. يتم إستخدام عداد الإرسال الحالي لكل من إطارات البيانات والإدارة، ولكن يتم إستخدام عداد إستقبال جديد لإطارات الإدارة. يتم إختبار عدادات التلقي لضمان أن كل إطار له رقم أعلى من الإطار الأخير الذي تم تلقيه (لضمان أن الإطارات فريدة ولم تتم إعادة تشغيلها)، لذلك لا يهم أن هذا النظام يتسبب في أن تكون القيم المستلمة غير متسلسلة.

تقارير الأخطاء

يتم إستخدام آليات إعداد التقارير MFP-1 للإبلاغ عن أخطاء إزالة كبسلة إطار الإدارة التي تم الكشف عنها بواسطة نقاط الوصول. وهذا يعني أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يجمع إحصائيات أخطاء التحقق من صحة MFP ويرسل المعلومات المجمعة بشكل دوري إلى عنصر التحكم في الشبكة.

يتم التعامل مع أخطاء انتهاك MFP التي يتم اكتشافها بواسطة محطات العميل بواسطة ميزة "التشخيصات تجوال وال وال في الوقت الفعلي ل CCXv5" ولا تكون في نطاق هذا المستند.

حماية إطار إدارة البث

لمنع الهجمات التي تستخدم إطارات البث، لا ترسل نقاط الوصول التي تدعم CCXv5 أي إطارات إدارة من الفئة 3 للبث (أي، DEAUTH، DISASSOC، أو الإجراء) باستثناء إطارات إلغاء المصادقة/فك الارتباط احتوائية مخادعة. يجب أن تتجاهل محطات العملاء التي تدعم CCXv5 إطارات إدارة فئة البث 3. يفترض أن جلسات عمل MFP في شبكة مؤمنة بشكل صحيح (مصادقة قوية بالإضافة إلى TKIP أو CCMP) لذلك لا يعد تجاهل عمليات بث الاحتواء المخادعة مشكلة.

وبالمثل، تتجاهل نقاط الوصول (APs) إطارات إدارة البث الواردة. لا توجد إطارات إدارة بث واردة مدعومة حاليا، لذلك لا يلزم إجراء أي تغييرات على التعليمات البرمجية لهذا الأمر.

الأنظمة الأساسية المدعومة

هذه الأنظمة الأساسية مدعومة:

- وحدات التحكم في WLAN200621064400WiSM3750 مع وحدة التحكم 440x المضمنةالموجهات 38xx/37/28/26
- نقاط وصول LWAPPنقطة الوصول 1100 AP 1000AP و 1200 1130AP و 1240 و 1250نقطة الوصول 1310
- برنامج العميلADU 3.6.4 وأعلى
- أنظمة إدارة الشبكةWCS

نقطة الوصول Mesh LWAPP 1500 غير مدعومة في هذا الإصدار.

الأوضاع المدعومة

تدعم نقاط الوصول المستندة إلى LWAPP التي تعمل في هذه الأوضاع MFP العميل:

أوضاع نقاط الوصول المدعومة	
نمط	**دعم MFP للعميل**
محلي	نعم
جهاز العرض	لا
sniffer	لا
جهاز كشف المخادع	لا
الحصاد الهجين	نعم
تحصد	لا
جذر الجسر	نعم
WGB	لا

دعم الخلايا المختلطة

يمكن لمحطات العملاء التي ليست قادرة على CCXv5 الاقتران بشبكة WLAN MFP-2. تتعقب نقاط الوصول أي من العملاء قادرين على MFP-2 وأي من العملاء ليسوا من أجل تحديد ما إذا كانت تدابير أمان MFP-2 يتم تطبيقها على إطارات إدارة البث الأحادي الصادرة والمتوقعة على إطارات إدارة البث الأحادي الواردة.

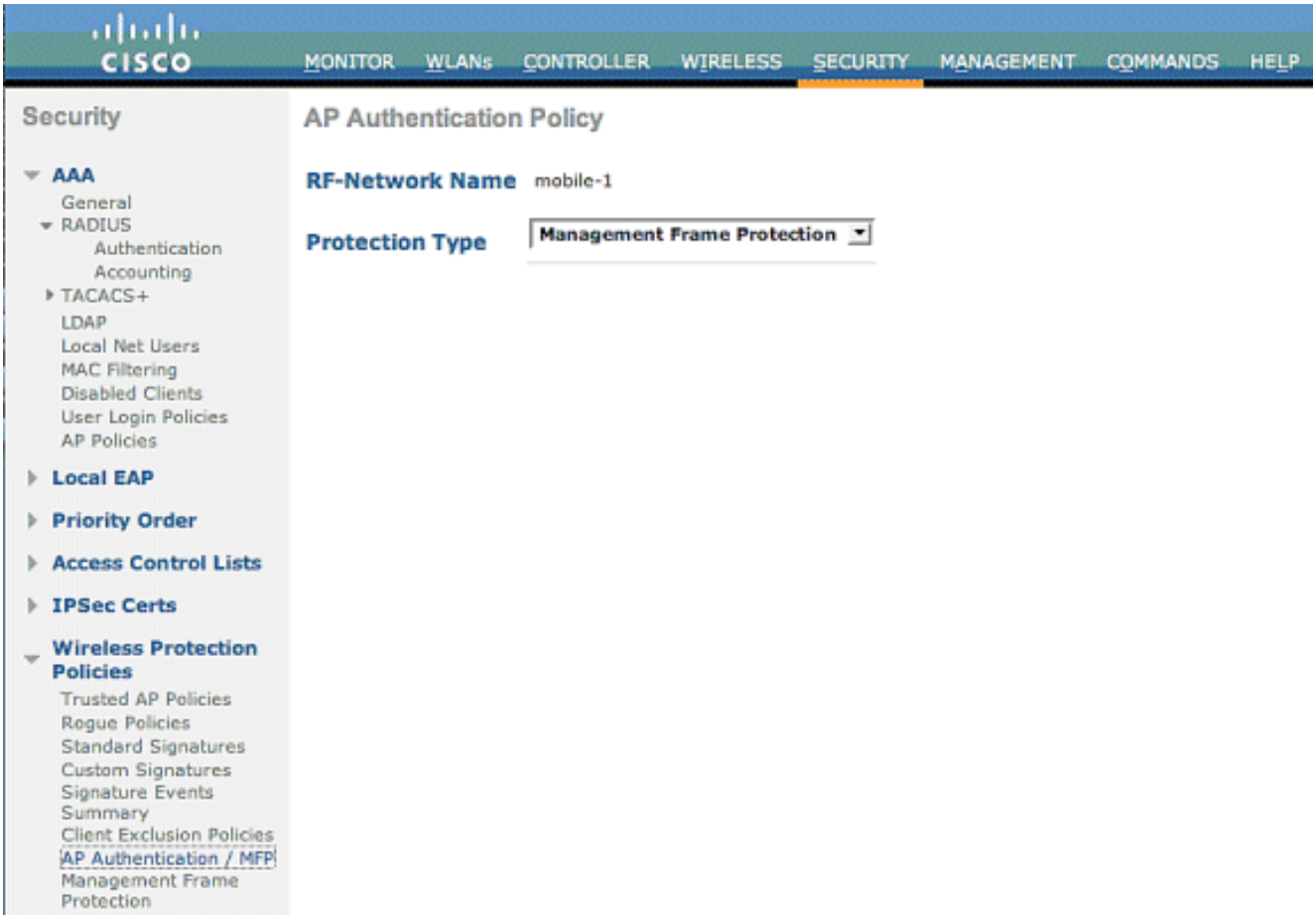
التكوين

تكوين MFP على وحدة تحكم

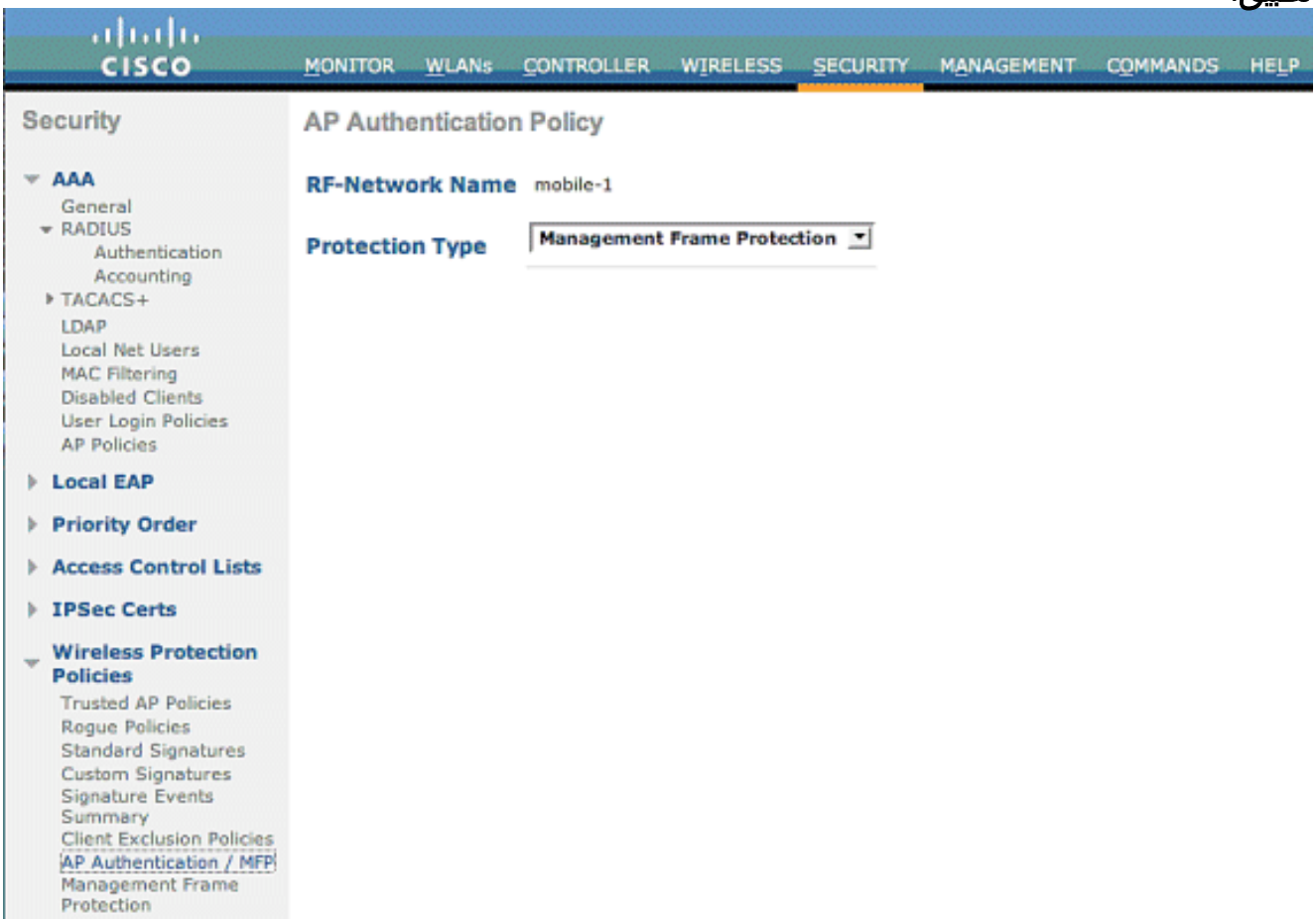
يمكنك تكوين MFP بشكل عام على وحدة تحكم. عندما تقوم بذلك، **يتم تمكين حماية إطار الإدارة والتحقق من صحته بشكل افتراضي لكل نقطة وصول مرتبطة**، ويتم تعطيل مصادقة نقطة الوصول تلقائيا.

قم بإجراء هذه الخطوات لتكوين MFP بشكل عام على وحدة تحكم.

1. من واجهة المستخدم الرسومية (GUI) لوحدة التحكم، انقر فوق **الأمان**. في الشاشة الناتجة، انقر على **مصادقة AP/MFP** ضمن **نهج الحماية اللاسلكية**.



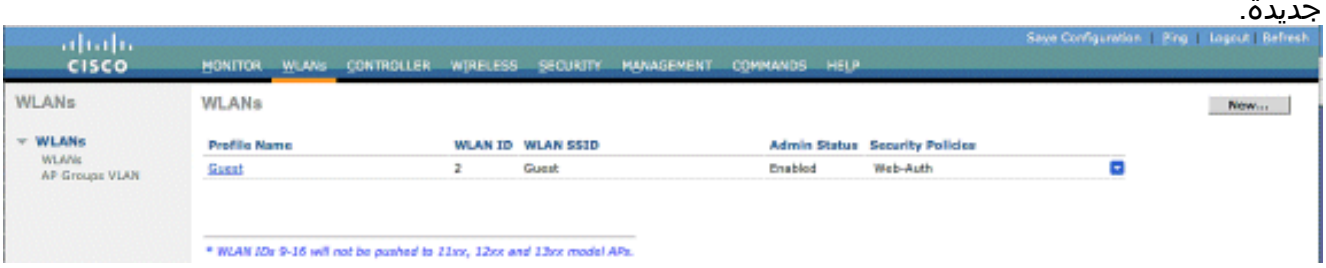
2. في سياسة مصادقة نقطة الوصول، أختر **حماية إطار الإدارة** من **القائمة المنسدلة نوع الحماية** وانقر فوق **تطبيق**.



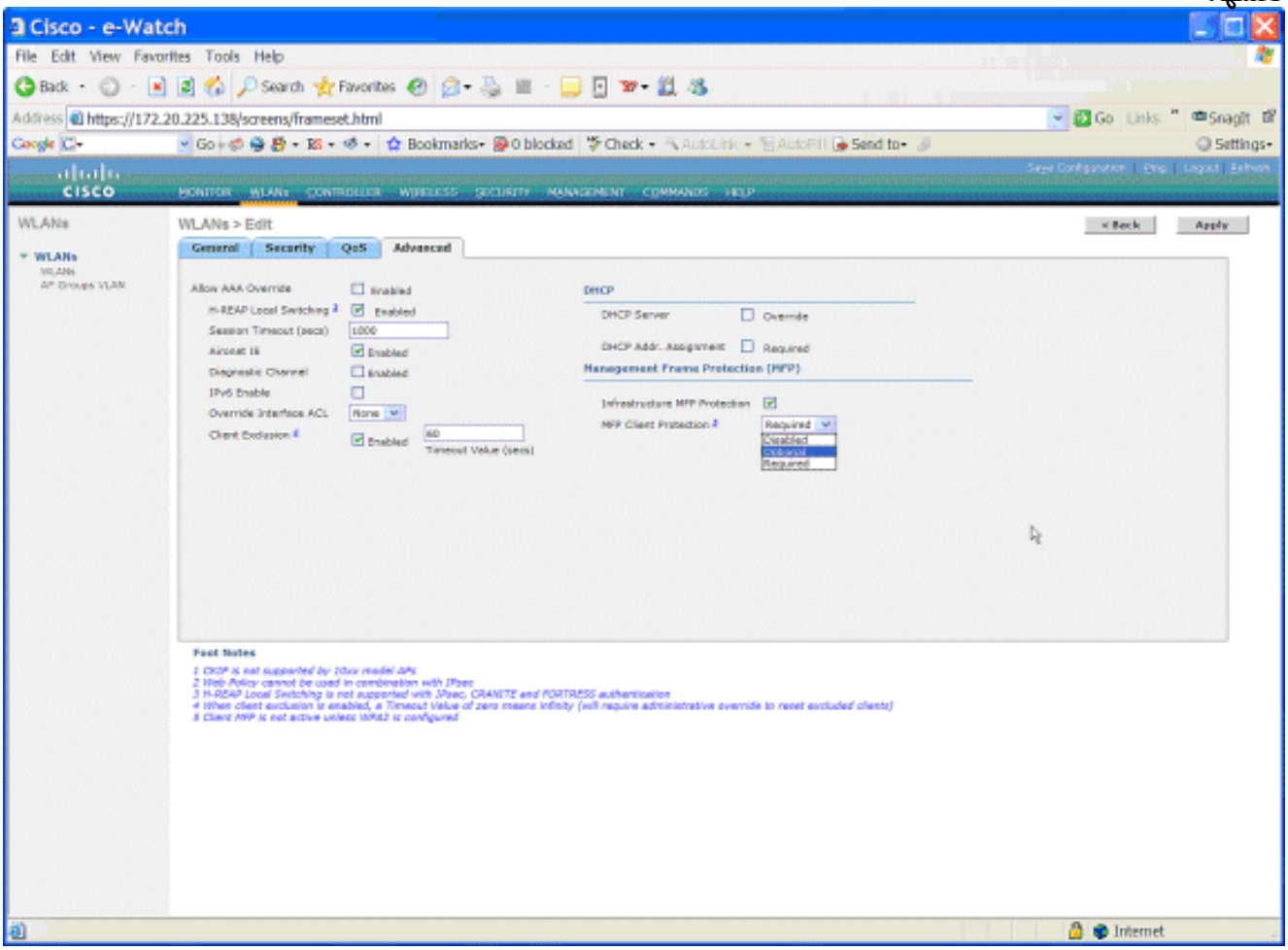
[تكوين MFP على WLAN](#)

أنت يستطيع أيضا مكنت/disable بنية MFP حماية وعميل MFP على كل WLAN يشكل على ال WLC. كلاهما مكنت افتراضيا من خلال بنية أساسية MFP حماية، أي يكون فقط نشط إن مكنت بشكل عام، والعميل MFP يكون نشط فقط إن ال WLAN شكلت مع WPA2 أمن. اتبع هذه الخطوات لتمكين MFP على شبكة WLAN:

1. من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق **شبكات WLAN** وانقر **جديد** لإنشاء شبكة WLAN جديدة.

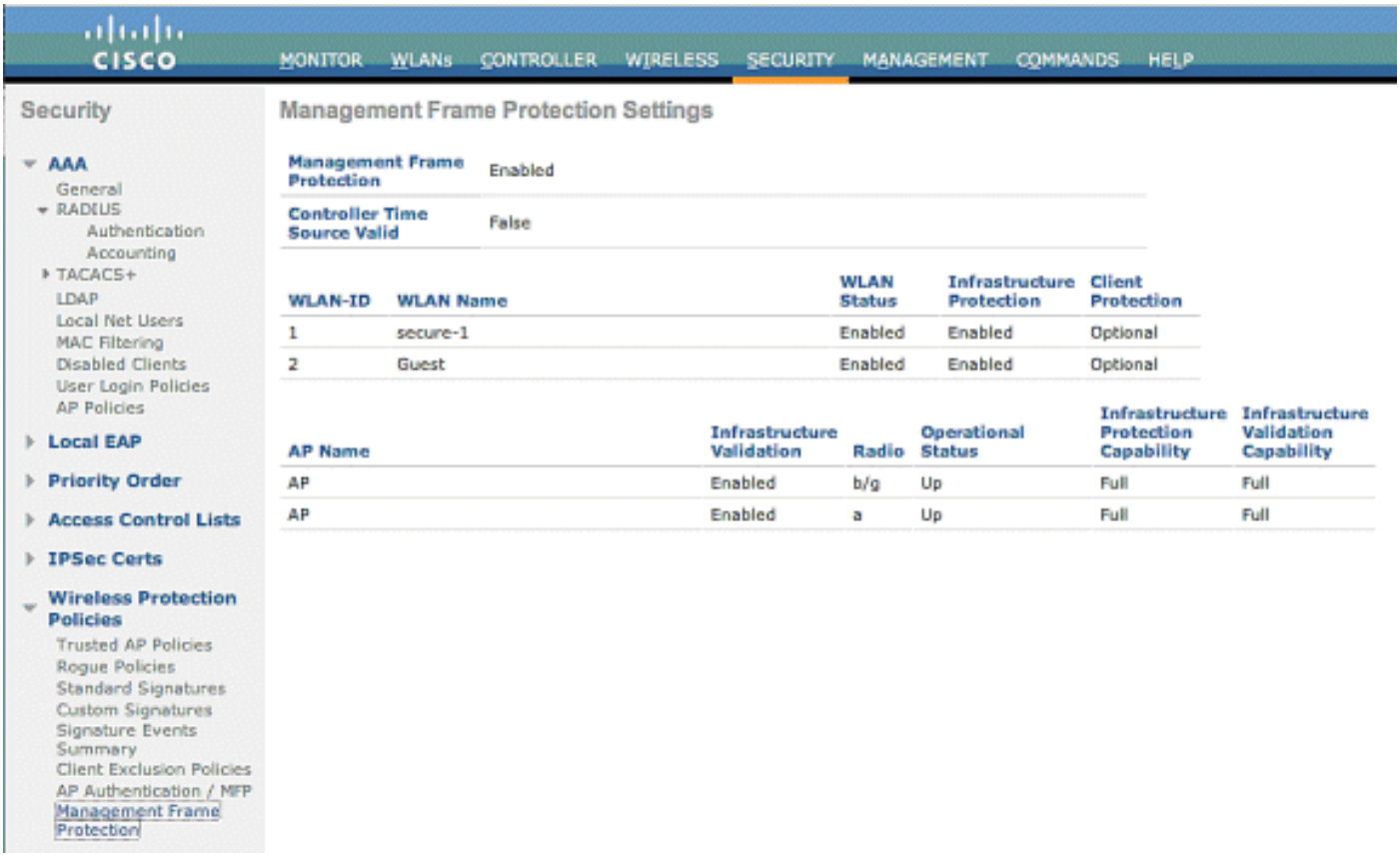


2. على صفحة تحرير شبكات WLAN، انتقل إلى علامة التبويب *خيارات متقدمة* وحدد خانة الاختيار **Infrastructure MFP Protection** لتمكين البنية الأساسية MFP على شبكة WLAN هذه. لتعطيل حماية MFP للبنية الأساسية لشبكة WLAN هذه، قم بإلغاء تحديد خانة الاختيار هذه. لتمكين MFP العميل، أختر الخيار المطلوب أو الاختياري من القائمة المنسدلة. إذا أخترت عميل MFP= مطلوب، فتأكد من أن كل عملائك لديهم دعم ل MFP- 2 أو أنهم غير قادرين على الاتصال. إذا أخترت إختياري، فإن كلا من العملاء الذين تم تمكينهم MFP وغير MFP يمكنهم الاتصال على شبكة WLAN نفسها.



التحقق من الصحة

للتحقق من تكوينات MFP من واجهة المستخدم الرسومية، انقر فوق **حماية إطار الإدارة** بموجب سياسات الحماية اللاسلكية من صفحة الأمان. ينقلك هذا إلى صفحة إعدادات MFP.



في صفحة إعدادات MFP، أنت يستطيع رأيت ال MFP تشكيل على ال LAP ،WLC، و WLAN. وفيما يلي مثال على هذا.

- يظهر حقل حماية إطار الإدارة ما إذا تم تمكين MFP بشكل عام ل WLC.
- يشير حقل مصدر وقت وحدة التحكم الصالح إلى ما إذا تم تعيين وقت عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) محليا (من خلال الإدخال اليدوي للوقت) أو من خلال مصدر خارجي (مثل خادم NTP). إذا تم تعيين الوقت بواسطة مصدر خارجي، فإن قيمة هذا الحقل هي "صواب". إذا تم تعيين الوقت محليا، تكون القيمة "false". يتم إستخدام مصدر الوقت للتحقق من إطارات الإدارة بين نقاط الوصول الخاصة بمجموعات محلية لاسلكية (WLCs) مختلفة والتي تم تكوين قابلية التنقل عليها أيضا.**ملاحظة:** إذا تم تمكين MFP على جميع قوائم التحكم في الشبكة المحلية اللاسلكية (WLCs) في مجموعة قابلية التنقل/RF، يوصى دائما باستخدام خادم NTP لتعيين وقت WLC في مجموعة قابلية التنقل.
- يظهر حقل **حماية MFP** ما إذا تم تمكين MFP لشبكات WLAN الفردية.
- يظهر حقل **التحقق من صحة MFP** ما إذا تم تمكين MFP لنقاط الوصول الفردية.

يمكن أن تكون أوامر show هذه مفيدة:

- **show wps summary** — أستخدم هذا الأمر لعرض ملخص لنهج الحماية اللاسلكية الحالية (والذي يتضمن MFP) الخاصة بعنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
- **أبديت wps mfp خلاصة**— in order to رأيت الحالي شامل MFP عملية إعداد من ال WLC، دخلت هذا أمر.
- أبديت ap config عام *ap_name* — ***in order to رأيت الحالي MFP دولة ل خاص منفذ نقطة، دخلت هذا أمر.***

هذا مثال من الإنتاج من **العرض** ap config **عام** ***ap_name*** أمر:

```
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
```

هذا مثال من الإنتاج من **العرض wps mfp** أمر ملخص:

```
                                    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
                                  ---------- ---------- --------- ------------------------- -------
                                    secure-1                  Enabled    Enabled     Optional        1
Guest                                   Enabled    Enabled     Optional but inactive (WPA2 not       2
                                                                                        (configured


                    --Infra.             Operational     --Infra. Capability
                   AP Name               Validation  Radio  State           Protection  Validation
                   ---------- ---------- ------------- ----- ---------- -------------------
                         AP                   Enabled     b/g    Up              Full        Full
```

يمكن أن تكون أوامر تصحيح الأخطاء هذه مفيدة؛

- **debug wps mfp lwapp**—يعرض معلومات تصحيح الأخطاء لرسائل MFP.
- **debug wps mfp detail**—يعرض معلومات تصحيح الأخطاء التفصيلية لرسائل MFP.
- **debug wps mfp report**— يعرض معلومات تصحيح الأخطاء لتقارير MFP.
- **debug wps mfp mm**— يعرض معلومات تصحيح الأخطاء لرسائل تنقل MFP (بين وحدات التحكم).

ملاحظة: هناك أيضا العديد من sniffer الحزمة اللاسلكية المجانية المتاحة من الإنترنت، والتي يمكن إستخدامها لالتقاط وتحليل إطارات إدارة 802.11. بعض مثال sniffer ربط هو omnipeek و Wireshark.

معلومات ذات صلة

- تكوين حلول الأمان: دليل تكوين WLC
- تكوين حلول الأمان في WCS
- مصادقة EAP باستخدام مثال تكوين وحدات التحكم في الشبكة المحلية اللاسلكية (WLC)
- مثال على تكوين ACL على وحدة تحكّم الشبكة المحلية اللاسلكية
- مثال تكوين المصادقة الخارجية للويب مع وحدات تحكم الشبكة المحلية (LAN) اللاسلكية
- تعيين شبكة VLAN الديناميكية مع مثال تكوين خادم RADIUS ووحدة تحكم شبكة LAN اللاسلكية
- Cisco Secure Services Client مع مصادقة EAP-FAST
- الأسئلة المتداولة حول WLC
- صفحة الدعم اللاسلكي
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).