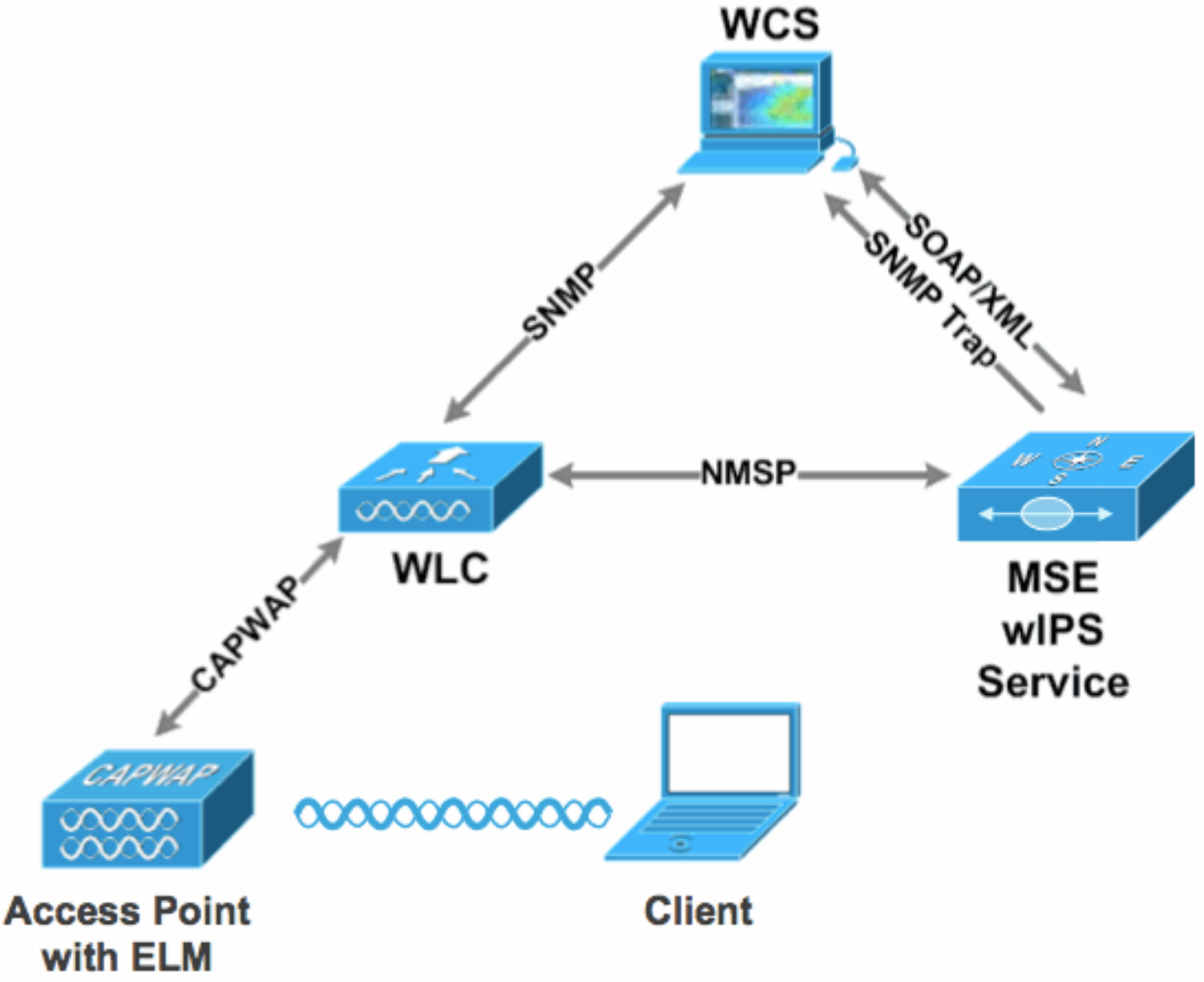
دليل تهيئة ونشر نظام منع التسلل (ELM) لمعيار wIPS المتكيف وفقا

المحتويات

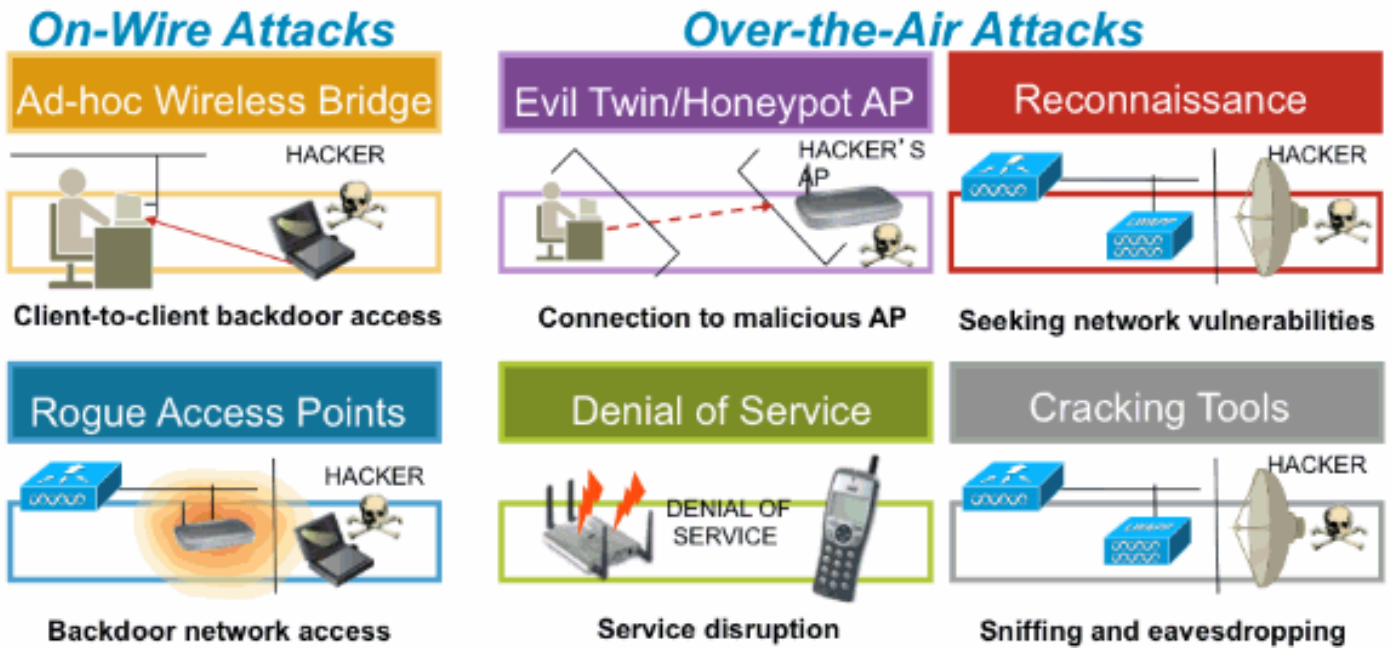
المقدمة

يضيف حل نظام منع التسلل اللاسلكي القابل للتكيف (IPS) من Cisco ميزة "الوضع المحلي المحسن" (ELM)، مما يتيح للمسؤولين إستخدام نقاط الوصول التي تم نشرها (AP) كمستشعرات مخصصة (شكل 1). قبل الخاصة بهم لتوفير حماية شاملة دون الحاجة إلى شبكة فرعية منفصلة Adaptive WIPS، يلزم وجود نقاط إدارة بيئة المؤسسة وفي النشر التقليدي لتقنية PCI أو الحماية وصول مخصصة لوضع المراقبة (MM) لتوفير إحتياجات التوافق مع بطاقات من الوصول غير المصرح به إلى الأمان واختراقه والهجمات عليه (الشكل 2). توفر تقنية ELM بشكل فعال عرض مماثل يعمل على تسهيل تنفيذ الأمان اللاسلكي مع خفض OpEx و CapEx في نفس الوقت. يركز هذا المستند فقط على ELM والي يوفر التكاليف بتعديل أية ميزات نشر موجودة لـ WIPS باستخدام نقاط الوصول من النوع MM.

الشكل 1 - نشر نقطة الوصول في الوضع المحلي المحسن



الشكل 2 - أهم تهديدات الأمان اللاسلكي



المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

مكونات ELM المطلوبة وإصدارات الحد الأدنى للكود

- وحدة التحكم في شبكة LAN اللاسلكية (WLC) - الإصدار 7.0.116.xx أو إصدار أحدث
- APs - الإصدار 7.0.116.xx أو أحدث
- نظام التحكم اللاسلكي (WCS) - الإصدار 7.0.172.xx أو إصدار أحدث
- Mobility Services Engine - الإصدار 7.0.201.xx أو إصدار أحدث

دعم منصات WLC

يتم دعم التحكم في الوصول عن بعد (ELM) على الأنظمة الأساسية WLC5508 و WLC4400 و WiSM-2WLC. و WiSM-1 و WLC2504 و WLC 2106.

دعم نقاط الوصول (AP)

يتم دعم ELM على نقاط الوصول عبر شبكة 11n بما في ذلك 3500 و 1250 و 1260 و 1040 و 1140.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. تم بدأ 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.

تدفق تنبيه ELM WIPS

تكون الهجمات ذات صلة فقط عندما تحدث على نقاط الوصول (APs) للبنية الأساسية طرق وحدة التحكم وتتصل بوحدة التحكم والوصول إلى ELM وستكشف نقاط الوصول. الموثوقة. مع MSE للإبلاغ عن إدارة WCS. يوفر الشكل 3 تدفق التنبيه من وجهة نظر المسؤول:

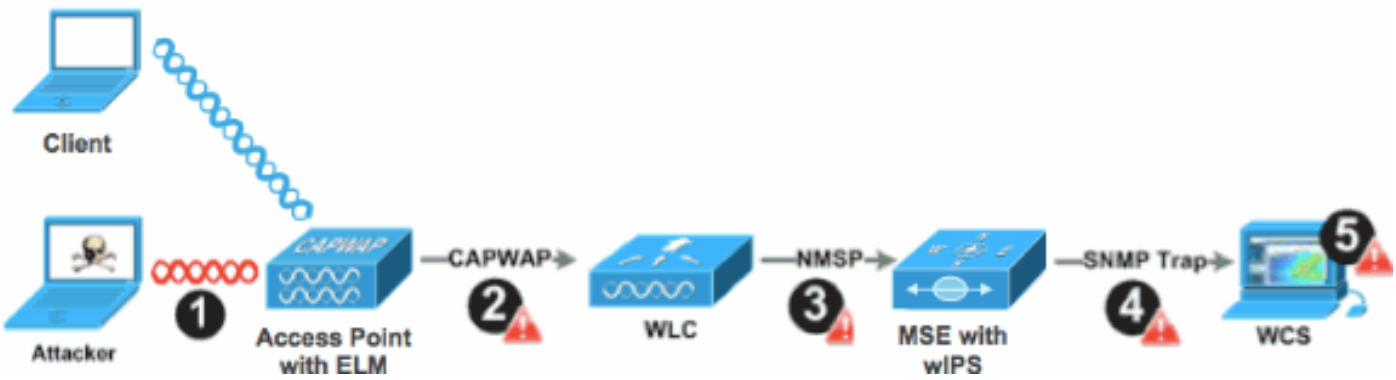
1. الهجوم الذي تم شنه على جهاز بنية أساسية ("Trusted" AP)
2. تم الكشف عنها على نقطة الوصول ELM التي تم الاتصال بها من خلال CAPWAP إلى WLC

3. مررت بشفافية إلى MSE عبر NMSP.

4. تم تسجيل الدخول إلى قاعدة بيانات wIPS على MSE الذي تم إرساله إلى WCS عبر مالئمة SNMP

5. معروض في WCS.

الشكل 3 - اكتشاف التهديدات وتدفق الإنذار



اعتبارات النشر الخاصة بالإدارة الإلكترونية

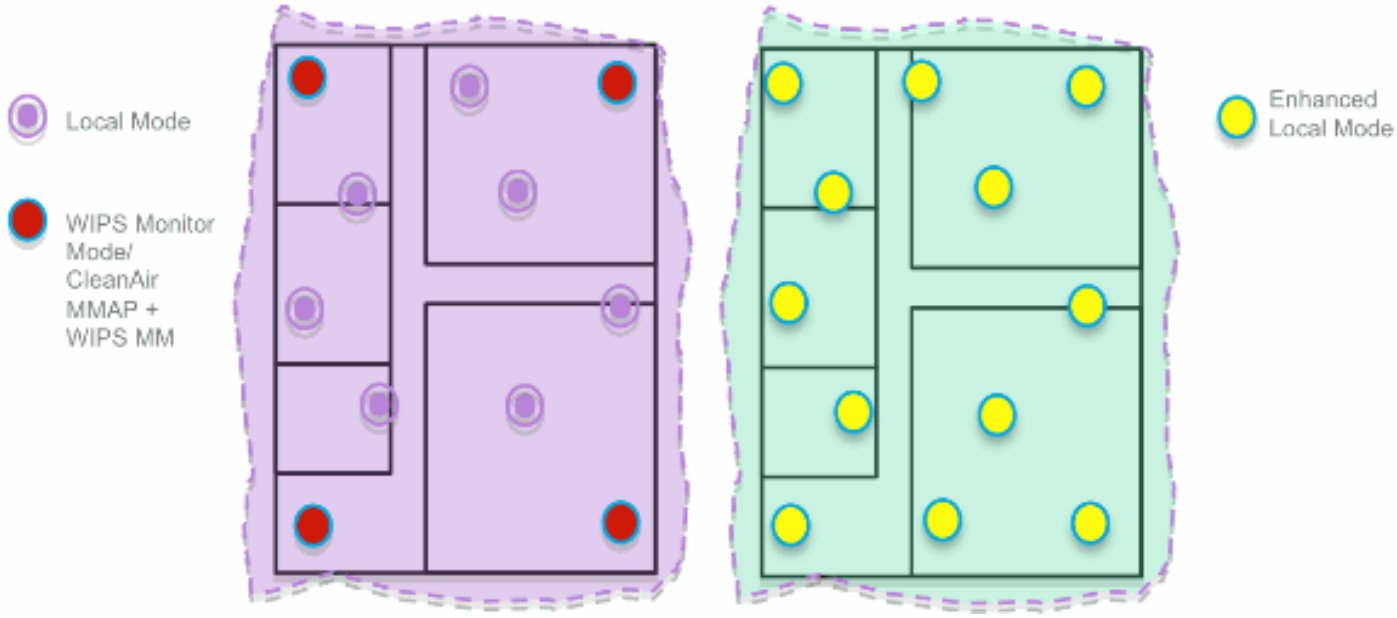
توصي Cisco بأن يتم تمكين ELM على كل نقطة وصول على الشبكة لتلبية معظم إحتياجات أمان العمالء عندما يكون تغشية الشبكة و/أو التكاليف جزءا من الاعتبار. تعمل ميزة ELM الأساسية بفعالية مع الهجمات التي يتم إجراؤها على القنوات، دون أي تضحية باألداء على عمالء البيانات والصوت والفيديو والخدمات.

ELM مقابل MM المخصص

يوفر الشكل 4 تباينا عاما بين عمليات النشر القياسية لنقاط الوصول من الفئة wIPS الشكل 4 تباينا عاما بين عمليات النشر القياسية لنقاط الوصول من الفئة wIPS ونقطة الوصول إلى شبكة Elm. وعند المراجعة، يشير نطاق التغطية النموذجي لكل MM الوضعين إلى ما يلي:

- تغطي نقطة الوصول المخصصة من الفئة wIPS MM عادة مساحة تتراوح من 15000 إلى 35000 قدم مربع
- تغطي نقطة الوصول التي تخدم العميل بشكل نموذجي مساحة تتراوح من 3000 إلى 5000 قدم مربع

الشكل 4 - تباين MM مقابل جميع نقاط الوصول ELM



في النشر التقليدي لنظام منع الاختراقات (IPS) القابل للتكيف، توصي Cisco بوجود نسبة نقطة وصول مقاس 1 ملم إلى كل خمس نقاط وصول (AP) في الوضع المحلي، والتي قد تختلف أيضا استنادا إلى تصميم الشبكة وإرشادات الخبراء للحصول على أفضل تغطية. ومن خلال وضع إدارة الأجهزة الافتراضية (ELM) في الاعتبار، يعمل المسؤول بسهولة على تمكين ميزة برنامج إدارة الأجهزة الافتراضية (ELM) لجميع نقاط الوصول (AP) الموجودة بالفعل، مما يعمل على إضافة عمليات نظام منع التسلل (IPS) إلى نقطة الوصول (AP) في وضع خدمة البيانات المحلية بشكل فعال مع الحفاظ على الأداء في نفس الوقت.

أداء خارج القناة والقناة

تستخدم نقطة الوصول من نوع MM 100٪ من وقت الراديو لمسح جميع القنوات، حيث أنها لا تخدم أي عملاء لشبكة WLAN. وتعمل الميزة الأساسية لإدارة المحتوى الافتراضي بفعالية لمواجهة الهجمات التي يتم تنفيذها عبر القنوات، دون أي تضحية بالأداء على عملاء وخدمات البيانات والصوت والفيديو. الفرق الأساسي في الوضع المحلي في حالة المسح الضوئي المتنوع خارج القناة، اعتمادا على النشاط، يوفر الفحص خارج القناة الحد الأدنى من الوقت المستغرق لجمع ما يكفي من المعلومات المتوفرة لتصنيف وتحديد الهجوم. قد يكون هناك مثال على عملاء الصوت المقترنين والذين يتم فيه تأجيل مسح AP RRM حتى يتم إلغاء اقتران العميل الصوتي للتأكد من عدم تأثر الخدمة. ومن أجل هذا الاعتبار، يعتبر الكشف عن ELM خارج القناة أفضل جهد. وتزيد نقاط الوصول المجاورة إلى شبكة ELM التي تعمل على جميع قنوات البلد أو DCA من فعاليتها، ومن ثم، فإن التوصية بتمكين إدارة التعلم الذاتي على كل نقطة وصول في الوضع المحلي من أجل تغطية الحماية القصوى. إذا كان المتطلب هو إجراء مسح ضوئي مخصص على جميع القنوات بدوام كامل، فستكون التوصية بنشر نقاط وصول من طراز MM.

تقوم هذه النقاط بمراجعة الفروق في الوضع المحلي ونقاط الوصول MM:

- نقطة الوصول في الوضع المحلي - توفر الخدمة لعملاء شبكة WLAN باستخدام ميزة تقسيم الوقت للمسح الضوئي خارج القناة، وتستمع لـ 50 مللي ثانية على كل قناة، كما تتميز بميزة المسح الضوئي القابل للتكوين لقنوات all/country/DCA.

- نقطة الوصول في وضع المراقبة - الـ WLAN، مخصصة للمسح الضوئي فقط، وتستمع إلى 1.2s على كل قناة، وتمسح كل القنوات.

ELM عبر إرتباطات WAN

بذلت Cisco جهودا كبيرة من أجل تحسين المميزات في السيناريوهات المليئة بالتحديات، مثل نشر نقاط الوصول إلى ELM عبر إرتباطات WAN ذات النطاق الترددي المنخفض. تتضمن ميزة ELM المعالجة المسبقة في تحديد توقيعات الهجوم في نقطة الوصول ويتم تحسينها للعمل على الروابط البطيئة. أفضل الممارسات، يوصى باختبار وقياس خط الأساس للتحقق من الأداء باستخدام إدارة مستوى الإدارة (ELM) عبر شبكة WAN.

تكامل الهواء النظيف

تعمل ميزة إدارة التخلص من المشكلات (ELM) على استكمال عمليات تقنية CleanAir بأداء وفوائد مماثلين لنشر نقاط الوصول من الفئة MM مع المميزات الحالية القائمة على مراعاة طيف CleanAir:

- ذكاء مخصص للترددات اللاسلكي على مستوى السليكون
- طرائز يتميز بوعي تام بالطيف، فضلا عن إمكانية حل المشكلات ذاتيا، فضلا عن إمكانية التحسين الذاتي
- تخفيف وتحديد القنوات غير المعيارية واكتشاف التداخل
- اكتشاف الشبكة غير اللاسلكية (Wi-Fi) مثل تقنية Bluetooth والموجات الدقيقة والهواتف التي لا سلكية وما إلى ذلك.
- اكتشاف هجمات رفض الخدمة (DOs) على طبقة الترددات اللاسلكي مثل أجهزة تشويش الترددات اللاسلكي وتحديد مواقعها

مزايا وفوائد إدارة الهيكل التنظيمي

- نقاط الوصول (AP) المحلية و H-REAP مسح ضوئي متكيف لنظام منع الاختراقات (IPS) في البيانات التي تخدم
- الحماية دون الحاجة إلى شبكة تغشية منفصلة
- متوفر كتنزيل مجاني لبرنامج SW لعملاء نظام منع التسلل (IPS) الحاليين
- يدعم التوافق مع بطاقة PCI للشبكات المحلية اللاسلكية
- 802.11 وغير 802.11 هجمات الكشف الكامل عن
- إضافة الطب الشرعي وإمكانات إعداد التقارير
- يمكن دمجه مع الإدارة الحالية لشبكة CUWM وشبكة WLAN
- مخصصة أو مدمجة MM لوصول نقاط تعيين في المرونة

- تعمل المعالجة المسبقة عند نقاط الوصول على تقليل نقل البيانات (أي العمل عبر إرتباطات النطاق الترددي المنخفض للغاية)
- تأثير منخفض على بيانات الخدمة

ترخيص ELM

ELM WIPS يضيف ترخيصا جديدا لطلب الشراء:

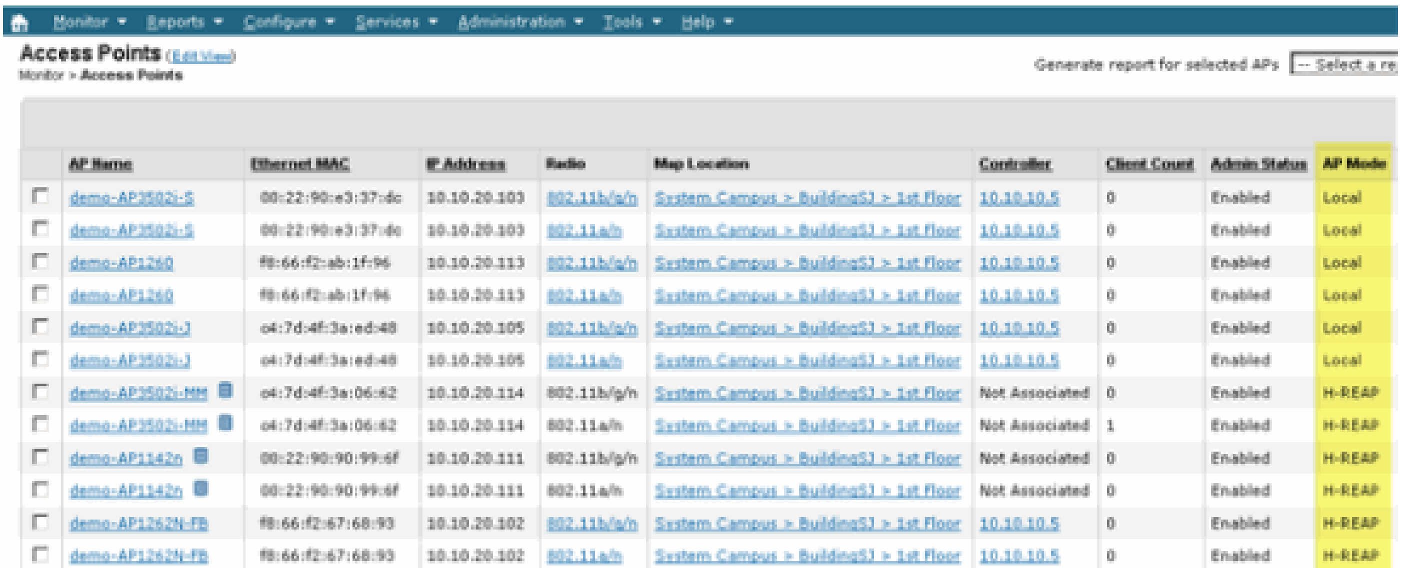
- ترخيص AIR-LM-WIPS-xx - Cisco ELM wIPS
- ترخيص AIR-WIPS-AP-xx - Cisco Wireless wIPS

ملاحظات ترخيص ELM الإضافية:

- إذا تم بالفعل تثبيت وحدة (وحدات) SKU الخاصة بترخيص نقطة الوصول طراز WIPS MM، يمكن إستخدام هذه التراخيص لنقاط الوصول الخاصة بالمتبرعين (ELM).
- تعد تراخيص نظام منع التسلل (IPS) وتراخيص نظام إدارة التعلم (ELM) دعما لحدود ترخيص النظام الأساسي لمحرك نظام منع التسلل (IPS)، و 2000 نقطة وصول في 3310 و 3000 نقطة وصول في 335x على التوالي.
- وسيشمل ترخيص التقييم 10 نقاط وصول من أجل نظام منع الاختراق و 10 لنقاط الوصول من أجل نظام إدارة التعلم لفترة تصل إلى 60 يوما. وقبل إدارة التعلم من بعد (ELM)، كان ترخيص التقييم يسمح بما يصل إلى 20 نقطة وصول من وحدات ذاكرة AP (AP) IPS MM. يجب تلبية الحد الأدنى من متطلبات إصدارات البرامج التي تدعم ELM.

تكوين ELM باستخدام WCS

الشكل 5 - إستخدام WCS لتكوين ELM

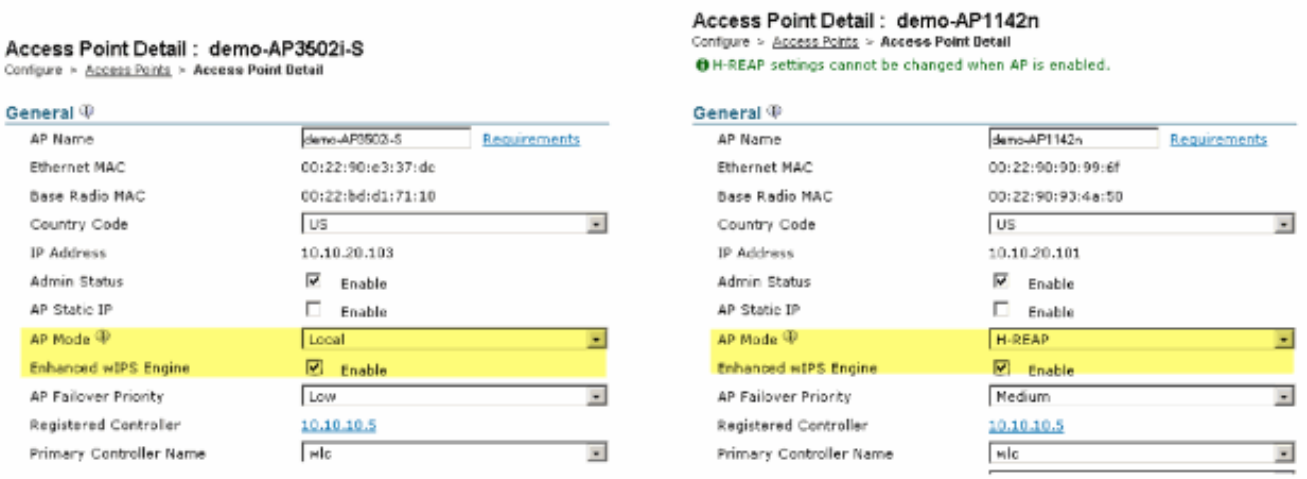


1. من WCS، قم بتعطيل كل من أجهزة الراديو 802.11b/g و 802.11a لنقطة الوصول قبل تمكين "محرك Enhanced wIPS".

ملاحظة: سيتم قطع اتصال جميع العملاء المرتبطين ولن ينضموا حتى يتم تمكين أجهزة الراديو.

2. قم بتكوين نقطة وصول واحدة، أو أستخدم قالب تكوين WCS للعديد من نقاط الوصول في الوضع Lightweight. راجع الشكل 6.

شكل 6 - تمكين الوضع الفرعي لمحرك IPS المحسن (ELM)



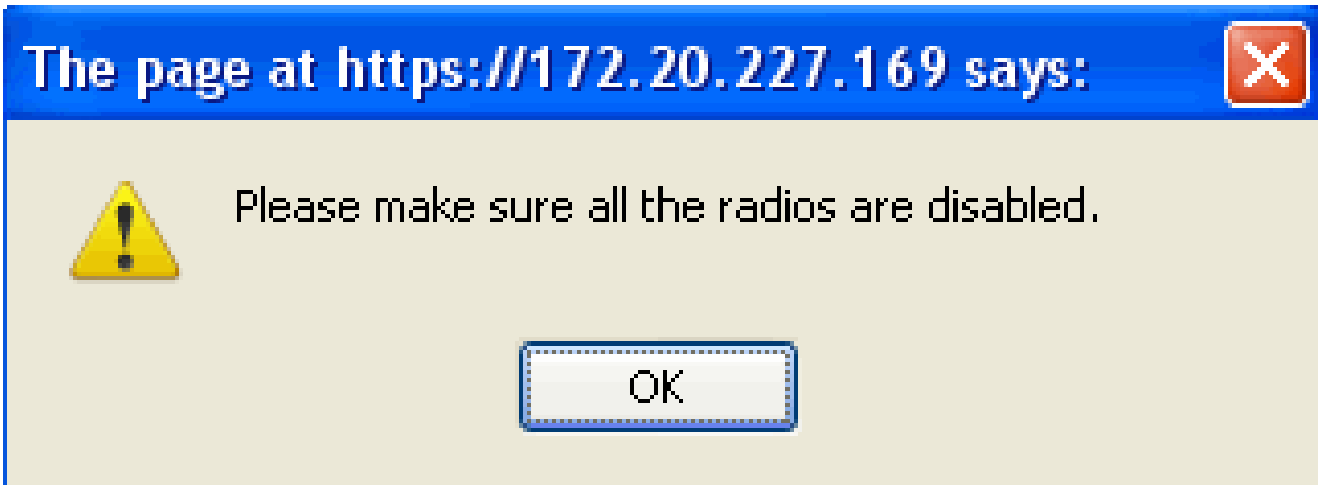
3. أختر Enhanced WIPS Engine، وانقر فوق حفظ.

a. لن يؤدي تمكين محرك wIPS المحسن إلى إعادة تمهيد نقطة الوصول

b. يتم دعم ميزة H-REAP، فهي تعمل بنفس الطريقة التي تعمل بها نقاط الوصول في الوضع المحلي.

ملاحظة: في حالة تمكين أي من أجهزة الإرسال اللاسلكية لنقطة الوصول هذه، سيقوم WCS بتجاهل التكوين وإلقاء الخطأ في الشكل 7.

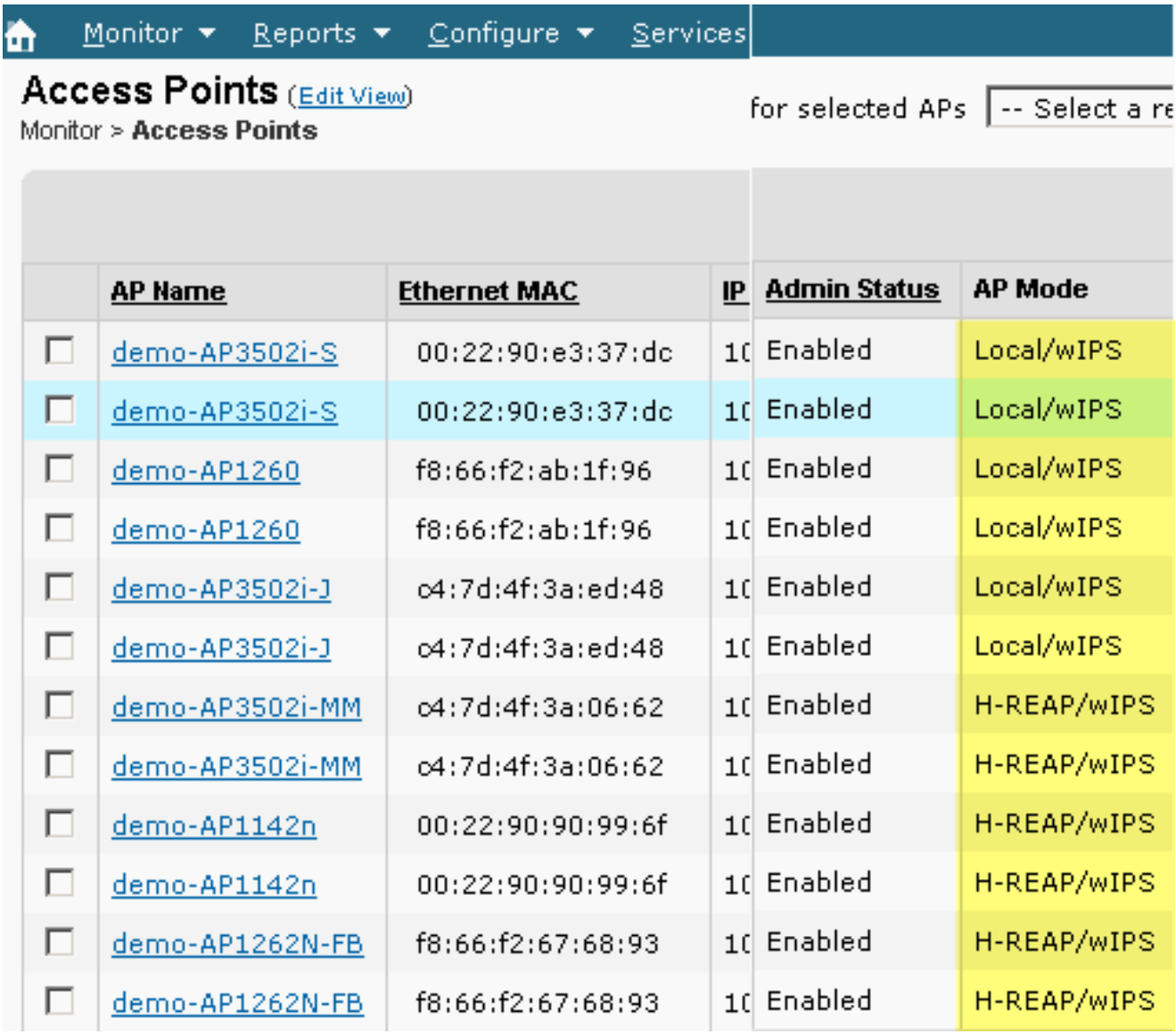
شكل 7 - تذكير WCS بتعطيل أجهزة الراديو AP قبل تمكين ELM



4. يمكن التحقق من نجاح التكوين من خلال مراقبة التغييرات في وضع نقطة الوصول من H-REAP/wIPS أو محلي/wIPS إلى "محلي أو H-REAP". راجع الشكل 8.

الشكل 8 - WCS الذي يعرض وضع نقطة الوصول لدمج بروتوكول الإنترنت (wIPS) مع

النات المحلي و/أو النات المحلي الإجمالي



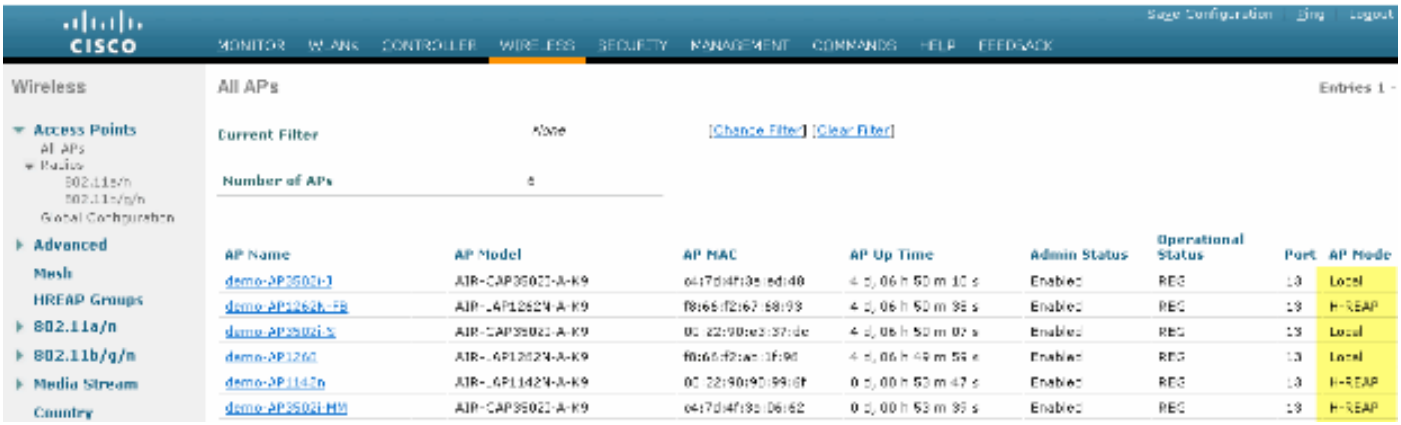
1.5. قم بتمكين أجهزة الراديو التي تم تعطيلها في الخطوة 1.

6. قم بإنشاء ملف تعريف wIPS ودفعه إلى وحدة التحكم حتى يكتمل التكوين.

ملاحظة: للحصول على معلومات التكوين الكاملة حول بروتوكول الإنترنت (IPS)، ارجع إلى دليل نشر Cisco Adaptive WIPS.

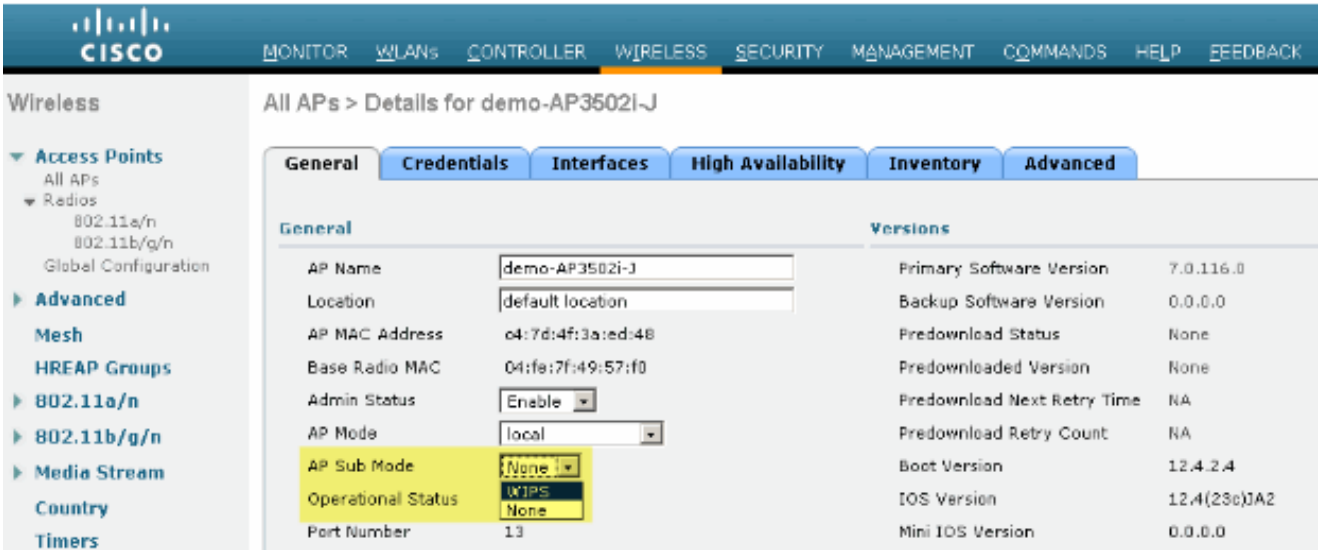
التكوين من WLC

الشكل 9 - تكوين ELM باستخدام WLC



1. أختر نقطة وصول من علامة تبويب اللاسلكي.

شكل 10 - تغيير الوضع الفرعي لنقطة الوصول (AP) من WLC لتضمين وضع WIPS ELM



2. أختر wIPS (شكل 10)، من القائمة المنسدلة الوضع الفرعي لنقطة الوصول (AP).

3. قم بحفظ ثم قم بتطبيق التكوين.

ملاحظة: لكي تعمل وظائف الإدارة المحلية الافتراضية (ELM)، يلزم توفر خدمات الإدارة (WCS) مع ترخيص نظام السلامة بيئيا (MSE) ونظام التحكم في الشبكة اللاسلكية (IPS). لن يؤدي تغيير الوضع الفرعي لنقطة الوصول من WLC وحده إلى منع الاختراق. تمكين ELM.

الهجمات التي تم الكشف عنها في ELM

الجدول 1 - مصفوفة دعم توقيعات نظام منع التسلل (IPS)

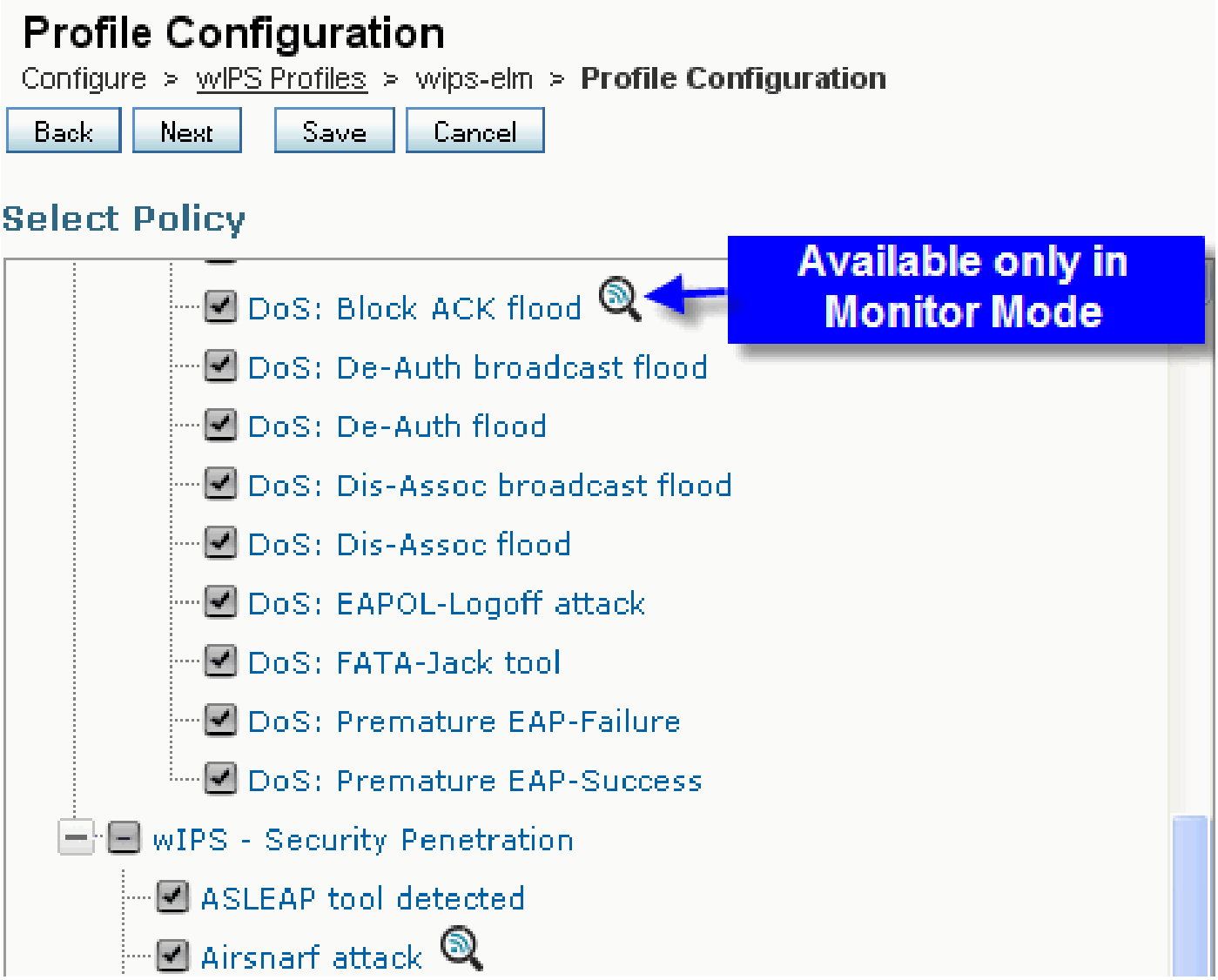
تم الكشف عن هجمات	إيلم	مم
هجوم رفض الخدمة (DoS) ضد AP		
فيضان الاقتران	Y	Y

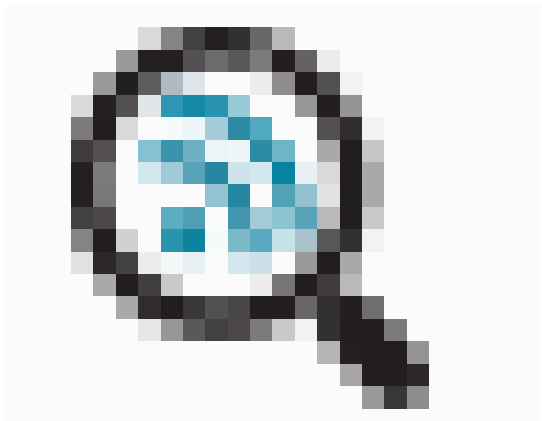
تجاوز جدول الاقتران	Y	Y
فيض المصادقة	Y	Y
هجوم Eapol-Start	Y	Y
فيضان PS-Poll	Y	Y
فيض طلب المسار	N	Y
اقتران غير مصدق	Y	Y
هجوم رفض الخدمة (DoS) على البنية الأساسية		
سيلز	N	Y
جامعة كوينزلاند للاستغلال التكنولوجي	N	Y
تشويش الترددات اللاسلكية	Y	Y
فيضان آر تي اس	N	Y
هجوم شركة الشحن الظاهرية	N	Y
هجوم رفض الخدمة على المحطة		
هجوم فشل المصادقة	Y	Y
غروب الماء	N	Y
بث دي أوث فيضان	Y	Y
طوفان دي أوث	Y	Y
إذاعة ديسي-آسوك	Y	Y
فيضان ديس-أسوك	Y	Y
هجوم ايبول-لوجوف	Y	Y
أداة قابس فاتا	Y	Y
فشل EAP السابق لأوانه	Y	Y
نجاح EAP سابق لأوانه	Y	Y
هجمات الاختراق الأمني		
تم الكشف عن أداة ASLEAP	Y	Y
هجوم إيرسنارف	N	Y
هجوم الشوب	Y	Y
هجوم يوم-صفر من قبل شاذ أمان WLAN	N	Y
هجوم يوم-صفر بسبب شذوذ أمان الجهاز	N	Y
حجب الجهاز عن نقاط الوصول (APs)	Y	Y
هجوم القاموس على أساليب EAP	Y	Y
هجوم EAP مقابل مصادقة 802.1x	Y	Y
تم اكتشاف نقاط وصول مزيفة	Y	Y

Y	N	فيزم DHCP مداخ نع فشكلا مت
Y	Y	ةعيرسلا WEP ققشتلا ةادأ نع فشكلا
Y	Y	ةئزجتلا موجه
Y	Y	ةدوزم (AP) لوصو ةطقن فاشتكا مت لسعلا حابصمب
Y	N	ةرارحلا بقارم ةادأ نع فشكلا مت
Y	N	ةحيحص ريغ ثب تاراطإ
Y	Y	لكشب ةلكشم 802.11 مزح نع فشكلا مت حيحص ريغ
Y	Y	طسوتملا موجهلا يف لجر
Y	Y	Netstumbler فاشتكا مت
Y	Y	Netstumbler ةيحض فاشتكا مت
Y	Y	PSPF كاهتنا نع فشكلا مت
Y	Y	وأ ةمعان (AP) لوصو ةطقن فاشتكا مت ةفيضم لوصو ةطقن
Y	Y	ةلحتنملا MAC ناونع نع فشكلا مت
Y	Y	دعب ةهوبشم رورم ةكرح نع فشكلا مت لمعلا تاعاس
Y	N	نيدروملا ةمئاق بسح هب حرصم ريغ نارتقا
Y	Y	هب حرصم ريغ نارتقا نع فشكلا مت
Y	Y	Wellenreiter فاشتكا مت

ملاحظة: إضافة CleanAir ةفاضإ نكمتس اضيأ نم فاشتكا تامجهلا يتلا ال يمتنت ىلإ ةئفلا 802.11.

WCS wIPS فيرعت فلم ضرع - 11 لكش





في الشكل 11، قم بتكوين ملف تعريف wIPS من WCS، تشير الأيقونة إلى أنه لن يتم اكتشاف الهجوم إلا عندما تكون نقطة الوصول بالمmm، بينما يتم اكتشاف أفضل جهد فقط عندما تكون في ELM.

أستكشاف أخطاء ELM وإصلاحها

تحقّق من العناصر التالية:

- تأكد من تكوين بروتوكول NTP.

- تأكد من أن إعداد الوقت MSE في UTC.
- ديهمت دعأ .يأ عم ةيشغشتلاب صاخلا SSID مدختسأ ،ةزهجألا ةعومجم لمع مدع ةلاح يف لوصولا ةطقن.
- تأكد من تكوين الترخيص (تستخدم نقاط الوصول من ELM حاليا ترخيص KAM)
- دكأت .ىرخأ ةرم MSE يف مكحتلا ةدحو ةنمازمب مق ،ادج اريثك wIPS تافيصوت رييغت اذإ من أن التوصيف نشط على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
- تأكد من أن WLC هو جزء من MSE باستخدام MSE CLIs:

1. SSH أو telnet إلى MSE الخاص بك.

2. إلى الوصول لهذه مكحتلا ةدحو مادختسإ نكمي - /opt/mse/wips/bin/wips_cli ذيفنتلا wIPS المتكيف. ظام الجاحلة المتعلقة بالمعلومات جمع التالية الأوامر.

3. وحدات من للتحقق الأمر هذا استخدام يتم .wIPS تحكم وحدة داخل إصدار - show wlc all التحكم التي تتصل بشكل نشط بخدمة wIPS على MSE. انظر الشكل 12.

الشكل 12 - MSE CLI التحقق من WLC نشط مع خدمات MSE WIPS

<#root>

```
wIPS>

show wlc all


WLC MAC              Profile              Profile
                      Status                   IP
                                  Onx Status Status
-------------------------------------------------
-------------------------------------------------
                                             ----
 00:21:55:06:F2:80    WCS-Default          Policy
         active on controller     172.20.226.197
                                           Active
```

- تأكد من اكتشاف أجهزة التنبيه على MSE باستخدام MSE CLIs.
  - show alarm list - مكحت ةدحو لخاد ةلكشملا wIPS. يتم إستخدام هذا الأمر لسرد الإنذارات التي تحتوي عليها حاليا قاعدة بيانات خدمة wIPS. حقل المفتاح هو معرف التجزئة الفريد الذي تم تعيينه للتحذير المحدد. حقل النوع هو نوع التنبيه. يوضح هذا المخطط في الشكل 13 قائمة بمعرفات التنبيه والأوصاف:

شكل 13 - أمر قائمة تنبيه MSE CLI

<#root>

```
wIPS>
```

```
show alarm list

                          Key           Type   Src MAC
 LastTime               Active           First Time
 ------------------------------------------------
      -------------------------------------------
89         89     00:00:00:00:00:00       2008/09/04
                18:19:26  2008/09/07 02:16:58    1
65631      95     00:00:00:00:00:00       2008/09/04
                17:18:31  2008/09/04 17:18:31    0
1989183    99     00:1A:1E:80:5C:40       2008/09/04
                18:19:44  2008/09/04 18:19:44    0
```

يشير الحقلان أول مرة وآخر مرة إلى الطوابع الزمنية عند اكتشاف التنبيه، ويتم تخزين هذه الطوابع في وقت UTC. يبرز الحقل النشط إذا كان التنبيه قد تم اكتشافه حاليا.

- مسح قاعدة بيانات MSE.
  - إذا واجهت حالة تكون فيها قاعدة بيانات MSE تالفة، أو لن تعمل أي أساليب أخرى لاستكشاف الأخطاء وإصلاحها، فقد يكون من الأفضل مسح قاعدة البيانات والبدء من جديد.

شكل 14 - أمر خدمات MSE

```
1. /etc/init.d/msed stop
2. Remove the database using the command 'rm
/opt/mse/locserver/db/linux/server-eng.db'
3. /etc/init.d/msed start
```

معلومات ذات صلة

- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 7.0.116.0
- دليل تكوين نظام التحكم اللاسلكي من Cisco، الإصدار 7.0.172.0
- 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).