

# ةيلحم لاةكبش لاة ف مكحت لاة دحو IPS لم اكل لةل دوة لةل س لاة

## المحتويات

<a href="#">المقدمة</a>
<a href="#">المتطلبات الأساسية</a>
<a href="#">المتطلبات</a>
<a href="#">المكونات المستخدمة</a>
<a href="#">الاصطلاحات</a>
<a href="#">نظرة عامة على Cisco IDS</a>
<a href="#">Cisco IDS و WLC - نظرة عامة على التكامل</a>
<a href="#">تجنب IDS</a>
<a href="#">تصميم بنية الشبكة</a>
<a href="#">تكوين مستشعر Cisco IDS</a>
<a href="#">تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)</a>
<a href="#">تكوين عينة مستشعر Cisco IDS</a>
<a href="#">تكوين ASA للمعرفات</a>
<a href="#">شكلت AIP-SSM ل حركة مرور تفتيش</a>
<a href="#">تكوين WLC لاستطلاع AIP-SSM لكتل العميل</a>
<a href="#">إضافة توقيع حظر إلى AIP-SSM</a>
<a href="#">حظر المراقبة والأحداث باستخدام إدارة البيانات الرقمية</a>
<a href="#">مراقبة استثناء العميل في وحدة تحكم لاسلكية</a>
<a href="#">مراقبة الأحداث في WCS</a>
<a href="#">تكوين ASA العينة من Cisco</a>
<a href="#">تكوين عينة مستشعر نظام منع الاقتحام Cisco Intrusion Prevention System Sensor Sample</a>
<a href="#">التحقق من الصحة</a>
<a href="#">استكشاف الأخطاء وإصلاحها</a>
<a href="#">معلومات ذات صلة</a>

## المقدمة

يعد النظام الموحد لاكتشاف الاقتحام (IDS)/نظام منع الاقتحام (IPS) من Cisco جزءا من شبكة الدفاع الذاتي من Cisco، كما أنه أول حل أمان سلكي ولاسلكي مدمج في هذه الصناعة. تتبع تقنية معرفات IPS الموحدة من Cisco أسلوبا شاملا في الأمان - من الحافة اللاسلكية، والحافة السلكية، وطرف الشبكة واسعة النطاق (WAN)، ومن خلال مركز البيانات. عندما يرسل عميل مقترن حركة مرور ضارة من خلال الشبكة اللاسلكية الموحدة من Cisco، يكتشف جهاز Cisco IDS السلكي الهجوم ويرسل طلبات رفض إلى وحدات تحكم الشبكة المحلية اللاسلكية (WLCs) من Cisco، والتي تقوم بعد ذلك بحل جهاز العميل.

يعد نظام منع الاختراقات (IPS) من Cisco حلا مضمنا قائما على الشبكة، تم تصميمه خصيصا لتحديد حركة المرور الضارة وتصنيفها ووقفها بشكل صحيح، بما في ذلك الفيروسات المتنقلة وبرامج التجسس / البرامج الدعائية وفيروسات الشبكة وإساءة استخدام التطبيقات، قبل أن تؤثر على إستمرارية الأعمال.

باستخدام برنامج مستشعر Cisco IPS، الإصدار 5، يجمع حل Cisco IPS بين خدمات الحماية المضمنة والتقنيات المبتكرة لتحسين الدقة. والنتيجة هي الثقة التامة في الحماية التي يوفرها حل التبدل داخل الشاشة (IPS) لديك، دون التخلص من الخوف من حركة المرور الشرعية. كما يوفر حل Cisco IPS حماية شاملة لشبكتك من خلال قدرتها الفريدة على التعاون مع موارد أمان الشبكة الأخرى، كما يوفر نهجا استباقيا لحماية شبكتك.

يساعد حل Cisco IPS المستخدمين على إيقاف المزيد من التهديدات بثقة أكبر من خلال استخدام الميزات التالية:

- **تقنيات وقائية دقيقة ومتوفرة** — توفر ثقة لا مثيل لها لاتخاذ إجراء وقائي ضد نطاق أوسع من التهديدات دون خطر إسقاط حركة المرور الشرعية. توفر هذه التقنيات الفريدة تحليلا سياقيا ذكيا مؤتمتا لبياناتك، كما تساعد على ضمان حصولك على أقصى استفادة من حل منع التسلسل.
- **التعرف على التهديد متعدد النواقل** — يحمي شبكتك من انتهاك السياسة واستكشاف الثغرات الأمنية والأنشطة الشاذة من خلال الفحص التفصيلي لحركة مرور البيانات من الطبقات من 2 إلى 7.
- **تعاون الشبكة الفريد** — يحسن قابلية التطوير والمرونة من خلال تعاون الشبكة، بما في ذلك تقنيات التقاط حركة المرور الفعالة وإمكانات موازنة الأحمال وإمكانية الرؤية في حركة المرور المشفرة.
- **حلول النشر الشاملة** — توفر حولا لجميع البيئات، بدءا من الشركات صغيرة ومتوسطة الحجم (SMB) ومواقع المكاتب الفرعية وحتى عمليات تركيب المؤسسات الكبيرة ومزودي الخدمة.
- **الإدارة الفعالة، ربط الأحداث، وخدمات الدعم** — توفر حلا متكاملًا، بما في ذلك خدمات التكوين والإدارة وترابط البيانات وخدمات الدعم المتقدمة. يحدد نظام Cisco لمراقبة الأمان وتحليله والاستجابة (MARS) العناصر المخالفة ويعزلها ويوصي بإزالتها بدقة للوصول إلى حل لمنع الاقتحام على نطاق الشبكة. كما يمنع نظام Cisco للتحكم في الحوادث انتشار الفيروسات المتنقلة الجديدة من خلال تمكين الشبكة من التكيف بسرعة وتوفير إستجابة موزعة.

وعند الجمع بين هذه العناصر، فإنها توفر حلا شاملا للوقاية المضمنة وتمنحك الثقة للكشف عن أوسع نطاق من حركة المرور الضارة وإيقاف تشغيلها قبل أن تؤثر على إستمرارية الأعمال. تدعو مبادرة شبكة الدفاع الذاتي من Cisco إلى توفير أمان مدمج ومضمن لحلول الشبكات. لا تدعم أنظمة شبكة محلية لاسلكية (WLAN) الحالية القائمة على بروتوكول نقطة الوصول في الوضع (LWAPP) (Lightweight) سوى ميزات معرفات الهوية الأساسية نظرا لحقيقة أنه نظام من الطبقة 2 بشكل أساسي، كما أنه يتسم بقوة معالجة خطية محدودة. تطلق Cisco تعليمات برمجية جديدة في الوقت المناسب لتضمين الميزات المحسنة الجديدة في الرموز الجديدة. يحتوي الإصدار 4.0 على أحدث الميزات التي تتضمن دمج نظام شبكة محلية لاسلكية (WLAN) قائم على LWAPP مع خط منتجات Cisco IDS/IPS. في هذا الإصدار، يكون الهدف هو السماح لنظام Cisco IDS/IPS بإصدار تعليمات إلى قوائم التحكم في الشبكة المحلية اللاسلكية (WLCs) لحظر وصول عملاء معينين إلى الشبكات اللاسلكية عند اكتشاف هجوم في أي مكان من الطبقة 3 إلى الطبقة 7 التي تتضمن العميل المعنى.

## المتطلبات الأساسية

### المتطلبات

تأكد من استيفاء الحد الأدنى من المتطلبات التالية:

- الإصدار x.4 من البرنامج الثابت WLC والإصدارات الأحدث
- من المفضل معرفة كيفية تكوين Cisco IPS و Cisco WLC.

### المكونات المستخدمة

Cisco WLC

يتم تضمين وحدات التحكم هذه مع الإصدار 4.0 من البرنامج لتعديلات IDS:

- Cisco 2000 Series WLC
- Cisco 2100 Series WLC

- Cisco 4400 Series WLC
- Cisco Wireless Services Module (WiSM)
- المحول Cisco Catalyst 3750G Series Unified Access Switch
- وحدة التحكم في شبكة LAN اللاسلكية (WLCM) من Cisco

### نقاط الوصول

- نقاط الوصول خفيفة الوزن للسلسلة Cisco Aironet 1100 AG Series
- نقاط الوصول خفيفة الوزن للسلسلة Cisco Aironet 1200 AG Series
- نقاط الوصول خفيفة الوزن للسلسلة Cisco Aironet 1300 Series
- نقاط الوصول خفيفة الوزن للسلسلة Cisco Aironet 1000 Series

### الذاتية المحسنة

- نظام التحكم اللاسلكي (WCS) من Cisco
- مستشعر سلسلة Cisco 4200
- إدارة نظام اكتشاف الاقتحام من Cisco - مدير جهاز (IDS) من Cisco

### أنظمة Cisco Unified IDS/IPS الأساسية

- أجهزة استشعار Cisco IPS 4200 Series مع برنامج مستشعر Cisco IPS 5.x أو إصدار أحدث.
  - SSM10 و SSM20 لأجهزة الأمان المعدلة من السلسلة Cisco ASA 5500 Series مع برنامج مستشعر Cisco IPS 5.x
  - أجهزة الأمان المعدلة Cisco ASA 5500 Series مع برنامج مستشعر Cisco IPS 5.x
  - الوحدة النمطية لشبكة (IDS) من Cisco مع برنامج مستشعر Cisco IPS 5.x
  - الوحدة النمطية لنظام اكتشاف الاقتحام من Cisco Catalyst 6500 Series الطراز 2 (IDSM-2) مع برنامج مستشعر Cisco IPS الإصدار x.5
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

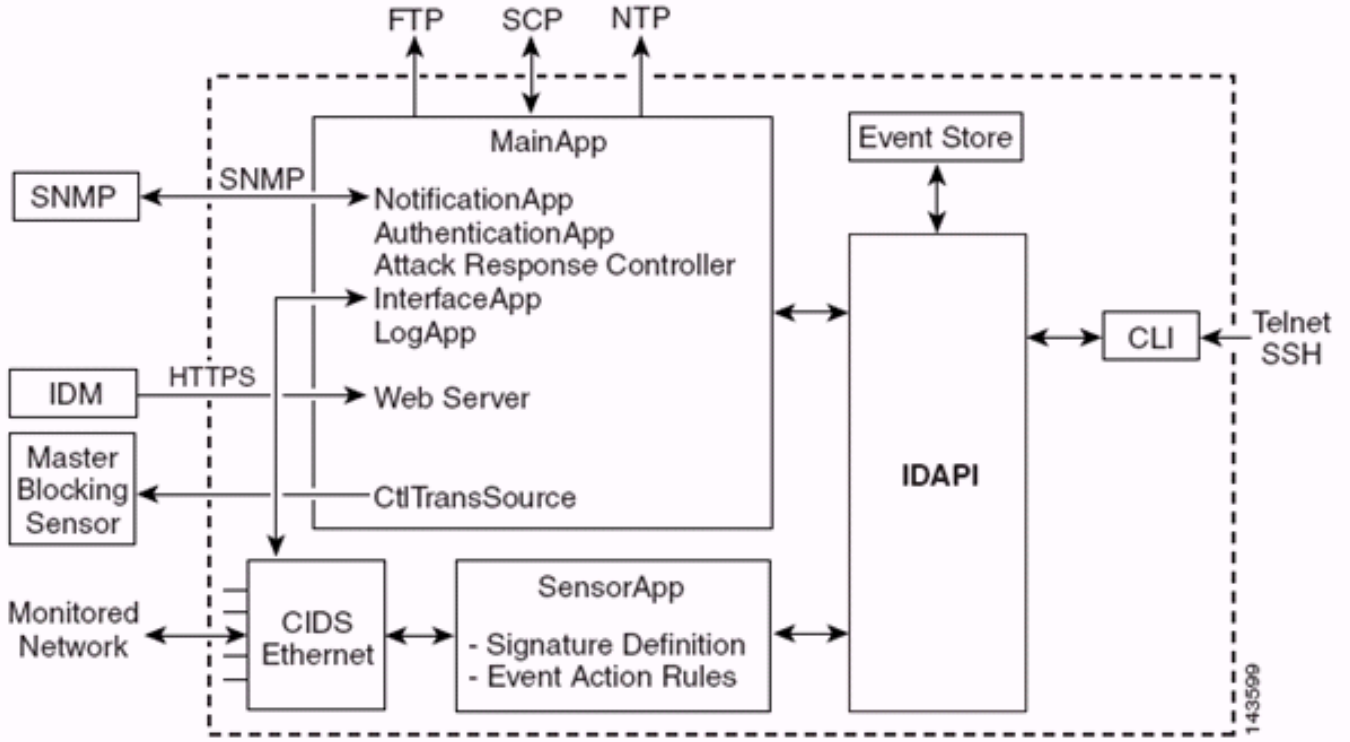
### الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## نظرة عامة على Cisco IDS

المكونات الرئيسية لمعرفة Cisco (الإصدار 5.0) هي:

- تطبيق المستشعر — يقوم بإجراء التقاط الحزمة وتحليلها.
- وحدة إدارة وإجراءات تخزين الأحداث - توفر إمكانية تخزين انتهاكات السياسة.
- Imaging, Install and Startup Module—تقوم بتحميل وتهيئة وتشغيل جميع برامج النظام.
- واجهات المستخدم ووحدة دعم واجهة المستخدم—توفر واجهة سطر أوامر (CLI) مضمنة وميزة IDM.
- نظام تشغيل المستشعر — نظام تشغيل المضيف (يعتمد على نظام التشغيل Linux).



يتكون تطبيق المستشعر (برنامج IPS) من:

- **التطبيق الرئيسي** — بدء النظام، وبدء تشغيل التطبيقات الأخرى وإيقافها، وتكوين نظام التشغيل، وهو مسؤول عن الترقية. يحتوي على المكونات التالية: **Control Transaction Server**—يسمح لأجهزة الاستشعار بإرسال حركات التحكم التي يتم استخدامها لتمكين قدرة مستشعر الحظر الرئيسي لوحدة تحكم إستجابة الهجمات (المعروفة سابقاً باسم وحدة تحكم الوصول إلى الشبكة). **مخزن الأحداث** — مخزن مفهرس يستخدم لتخزين أحداث IPS (الأخطاء والحالة ورسائل التنبيه) يمكن الوصول إليه من خلال CLI أو IDM أو مدير أجهزة الأمان المعدلة (ASDM) أو بروتوكول تبادل البيانات عن بعد (RDEP).
- **تطبيق الواجهة**—يعالج الإعدادات الالتفافية والمادية ويعرف الواجهات المزدوجة. تتألف الإعدادات المادية من السرعة والإرسال ثنائي الإتجاه والحالات الإدارية.
- **Log App**—يكتب رسائل السجل الخاصة بالتطبيق إلى ملف السجل ورسائل الخطأ إلى مخزن الأحداث.
- **تقوم وحدة التحكم في الاستجابة للهجوم (ARC) (المعروفة سابقاً باسم وحدة التحكم في الوصول إلى الشبكة)**— بإدارة أجهزة الشبكة البعيدة (جدران الحماية والموجهات والمحولات) لتوفير إمكانيات الحظر عند حدوث حدث تنبيه. يقوم ARC بإنشاء وتطبيق قوائم التحكم في الوصول (ACL) على جهاز الشبكة الذي يتم التحكم فيه أو يستخدم أمر **SHUN** (جدران الحماية).
- **تطبيق الإعلّامات**— يرسل إختبارات SNMP عند تشغيلها بواسطة أحداث التنبيه والحالة والخطأ. يستخدم "تطبيق الإعلّامات" وكيل SNMP للمجال العام من أجل تحقيق ذلك. توفر خدمات SNMP GETs معلومات حول حالة المستشعر. **خادم الويب (خادم HTTP RDEP2)**— يوفر واجهة مستخدم ويب. كما يوفر وسيلة للاتصال بأجهزة IPS الأخرى من خلال بروتوكول RDEP2 باستخدام عدة خوادم لتوفير خدمات بروتوكول الإنترنت (IPS). **تطبيق المصادقة**— يتحقق من أن المستخدمين مخولون لتنفيذ إجراءات CLI أو IDM أو ASDM أو RDEP.
- **تطبيق المستشعر (Analysis Engine)** — يقوم بإجراء التقاط الحزمة وتحليلها.
- **cli**— الواجهة التي يتم تشغيلها عندما يقوم المستخدمون بتسجيل الدخول إلى المستشعر بنجاح من خلال برنامج Telnet أو SSH. تستخدم جميع الحسابات التي تم إنشاؤها من خلال واجهة سطر الأوامر (CLI) واجهة سطر الأوامر (CLI) كطبقة خاصة بها (باستثناء حساب الخدمة - يتم السماح بحساب خدمة واحد فقط). تعتمد أوامر CLI المسموح بها على امتياز المستخدم.

تتصل جميع تطبيقات التبديل داخل الشاشة (IPS) ببعضها البعض من خلال واجهة برنامج تطبيق مشتركة (API) تسمى IDAPI. تتصل التطبيقات البعيدة (أجهزة الاستشعار الأخرى وتطبيقات الإدارة وبرامج الطرف الثالث) بأجهزة الاستشعار من خلال بروتوكولات تبادل أحداث أجهزة الأمان (SDEE) و RDEP2.

يجب ملاحظة أن "المستشعر" يحتوي على أقسام القرص هذه:

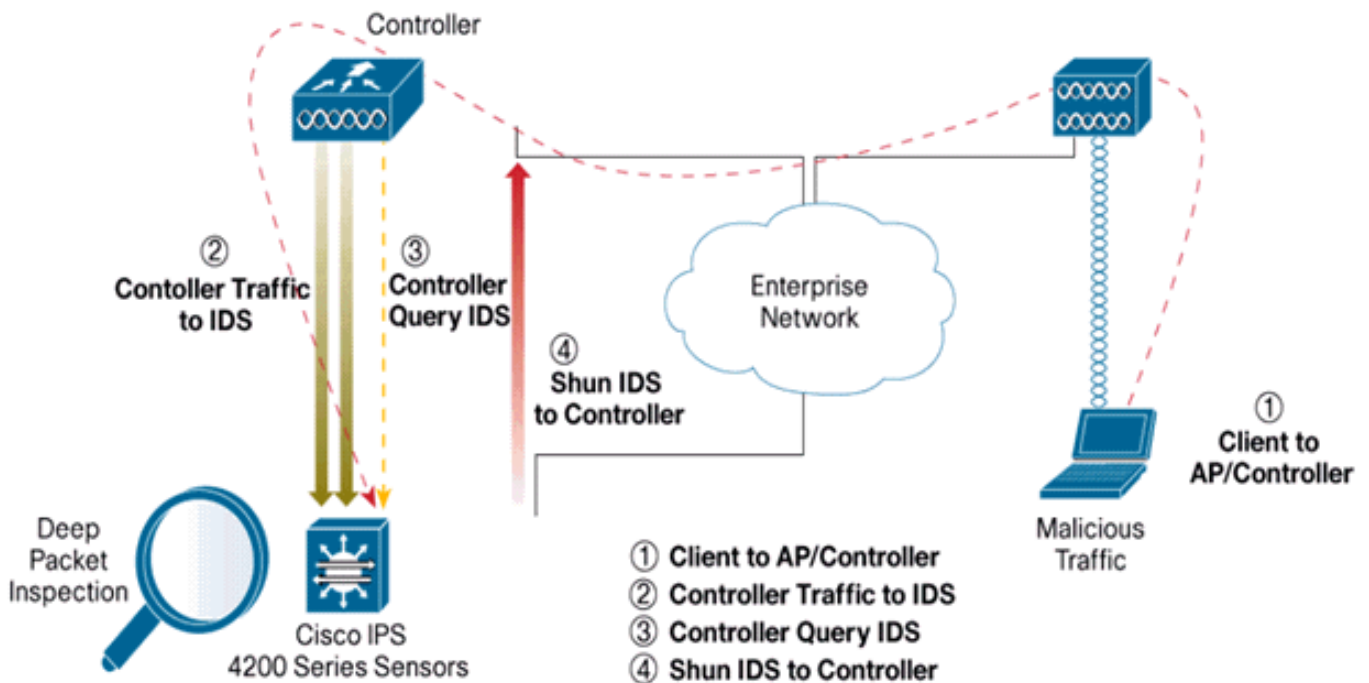
- قسم التطبيق—يحتوي على صورة نظام IPS بالكامل.
- قسم الصيانة — صورة IPS لأغراض خاصة يتم استخدامها لإعادة تكوين قسم التطبيق الخاص بـ IDS-2.
- قسم إعادة صورة لقسم الصيانة إعدادات تكوين مفقودة.
- قسم الاسترداد — صورة مخصصة الغرض تستخدم لاسترداد المستشعر. يؤدي التمهيد في قسم الاسترداد إلى تمكين المستخدمين من إعادة تكوين قسم التطبيق بالكامل. يتم الاحتفاظ بإعدادات الشبكة، ولكن يتم فقد جميع التكوينات الأخرى.

## WLC و Cisco IDS - نظرة عامة على التكامل

يقدم الإصدار 5.0 من Cisco IDS إمكانية تكوين إجراءات الرفض عند الكشف عن انتهاكات النهج (التوقعات). استنادا إلى تكوين المستخدم في نظام المعرفات/IPS، يمكن إرسال طلب يتجنب إلى جدار حماية أو موجه أو WLC لحظر الحزم من عنوان IP معين.

مع برنامج Cisco Unified Wireless Network الإصدار 4.0 لوحدة التحكم اللاسلكية من Cisco، يلزم إرسال طلب إلى وحدة تحكم في الشبكة المحلية اللاسلكية (WLC) لتشغيل سلوك العميل الذي يشير إلى الإدراج في القائمة السوداء أو الاستبعاد المتاح على وحدة التحكم. الواجهة التي تستخدمها وحدة التحكم للحصول على طلب الإحجام هي واجهة الأمر والتحكم على معرفات Cisco.

- تسمح وحدة التحكم بتكوين ما يصل إلى خمسة أجهزة استشعار IDS على وحدة تحكم معينة.
- يتم تعريف كل مستشعر IDS تم تكوينه بواسطة عنوان IP الخاص به أو اسم الشبكة المؤهلة وبيانات اعتماد التحويل.
- يمكن تكوين كل مستشعر IDS على وحدة تحكم بمعدل استعلام فريد في ثوان.



### تجنب IDS

تستعلم وحدة التحكم عن "المستشعر" بمعدل الاستعلام الذي تم تكوينه لاسترداد كافة أحداث الإحجام. يتم توزيع طلب تجنب معين عبر مجموعة التقليل بأكملها لوحدة التحكم التي تسترجع الطلب من مستشعر IDS. يتم تطبيق كل طلب لملء عنوان IP للعميل لقيمة ثواني المهلة المحددة. إذا كانت قيمة المهلة تشير إلى وقت لا نهائي، فإن حدث عدم الظهور ينتهي فقط إذا تم إزالة إدخال SHUN على المعرفات. يتم الاحتفاظ بحالة العميل المبعد على كل وحدة

تحكم في مجموعة التنقل حتى في حالة إعادة تعيين أي من وحدات التحكم أو كلها.

**ملاحظة:** يتخذ مستشعر IDS دائما قرار تجنب أحد العملاء. لا يكتشف جهاز التحكم هجمات الطبقة 3. وهي عملية أكثر تعقيدا إلى حد كبير لتحديد أن العميل يشن هجوما خبيثا على الطبقة 3. تتم مصادقة العميل في الطبقة 2 التي تعد جيدة بدرجة كافية لوحدة التحكم لمنع وصول الطبقة 2.

**ملاحظة:** على سبيل المثال، إذا حصل العميل على عنوان IP (مهمل) سابق تم تعيينه، فإن مهلة المستشعر هي إلغاء حظر وصول الطبقة 2 لهذا العميل الجديد. حتى إذا أعطت وحدة التحكم حق الوصول في الطبقة 2، فقد يتم حظر حركة مرور العميل في الموجهات في الطبقة 3 على أي حال، لأن المستشعر يقوم أيضا بإعلام الموجهات بحدث عدم الاتصال.

بافتراض أن العميل لديه عنوان IP A. الآن، عندما يقوم جهاز التحكم باستطلاع معرفات أحداث الإحجام، تقوم معرفات الهوية بإرسال طلب الإحجام إلى جهاز التحكم بعنوان IP A كعنوان IP الهدف. الآن، يسرد أسود وحدة التحكم هذا العميل A. على وحدة التحكم، يتم تعطيل العملاء استنادا إلى عنوان MAC.

الآن، لنفترض أن العميل يغير عنوان IP الخاص به من A إلى B. وخلال الاستطلاع التالي، يحصل جهاز التحكم على قائمة بالعملاء المتجنين استنادا إلى عنوان IP. هذه المرة أيضا، لا يزال عنوان IP A في القائمة المبعد. ولكن بما أن العميل قد قام بتغيير عنوان IP الخاص به من A إلى B (والذي لم يكن في قائمة عناوين IP التي تم تجاهلها)، يتم إطلاق هذا العميل بعنوان IP جديد من B بمجرد الوصول إلى مهلة العملاء السود المدرجين على وحدة التحكم. الآن، يبدأ جهاز التحكم في السماح لهذا العميل بعنوان IP جديد من B (ولكن يظل عنوان MAC الخاص بالعميل كما هو).

لذلك، على الرغم من أن العميل يبقى معاق لمدة وقت إستثناء وحدة التحكم ويتم إعادة إستبعاده إذا اكتسب عنوان DHCP السابق الخاص به، فإن ذلك العميل لم يعد معطلا إذا تغير عنوان IP الخاص بالعميل الذي يتم تجنبه. على سبيل المثال، إذا كان العميل يتصل بنفس الشبكة ولم تنتهي مهلة تأجير DHCP.

تدعم وحدات التحكم فقط الاتصال بمعرفات رفات العملاء لطلبات تجنب العملاء التي تستخدم منفذ الإدارة على وحدة التحكم. تتصل وحدة التحكم بمعرفات فحص الحزم من خلال واجهات VLAN القابلة للتطبيق التي تحمل حركة مرور العميل اللاسلكي.

في وحدة التحكم، تظهر صفحة تعطيل العملاء كل عميل تم تعطيله عبر طلب مستشعر IDS. يعرض الأمر CLI **show** أيضا قائمة بالعملاء المدرجة في القائمة السوداء.

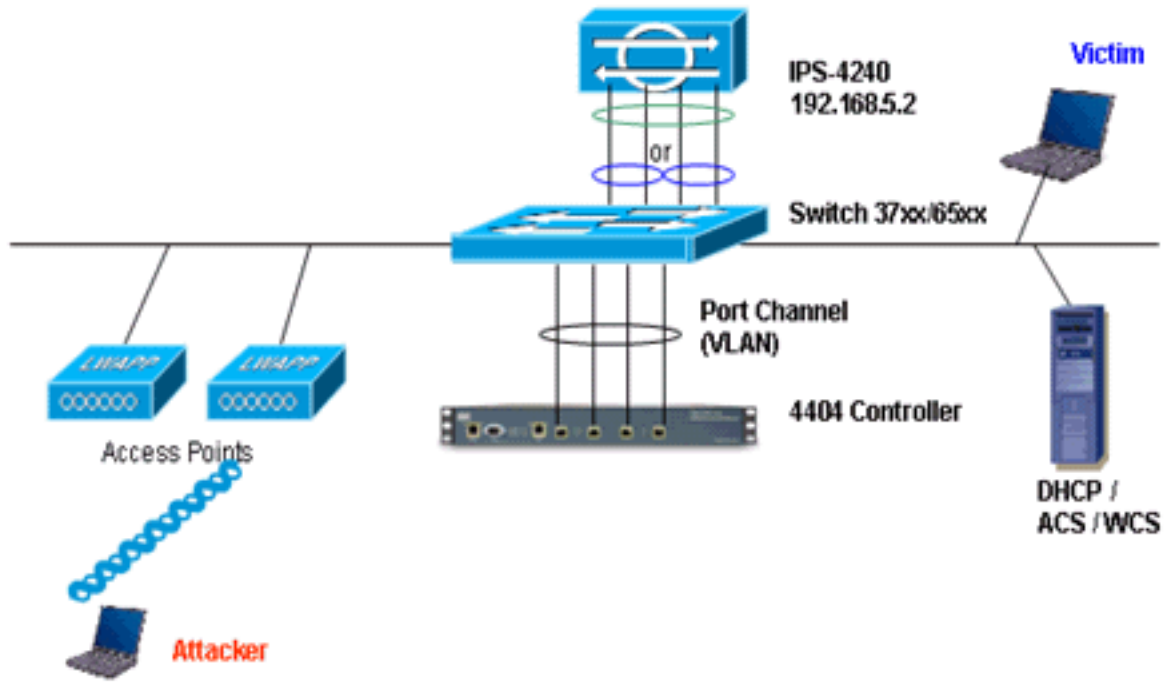
في WCS، يتم عرض العملاء المستبعدين تحت علامة التبوب الفرعي أمان.

فيما يلي الخطوات التي يجب اتباعها لاستكمال تكامل أجهزة إستشعار Cisco IPS و Cisco WLCs.

1. قم بتثبيت جهاز IDS وتوصيله على المحول نفسه حيث توجد وحدة التحكم اللاسلكية.
2. انسخ (فسحة بين دعامتين) منافذ WLC التي تحمل حركة مرور العميل اللاسلكي إلى جهاز IDS.
3. يستلم جهاز IDS نسخة من كل حزمة ويفحص حركة المرور في طبقة 3 حتى 7.
4. يوفر جهاز IDS ملف توقيع قابل للتنزيل، والذي يمكن تخصيصه أيضا.
5. يقوم جهاز IDS بإنشاء التنبيه باستخدام إجراء حدث تم تجنبه عند اكتشاف توقيع هجوم.
6. تستطلع لجنة الاتصال اللاسلكية WLC معرفات الإنذار.
7. عند اكتشاف تنبيه بعنوان IP لعميل لاسلكي، مقترن ب WLC، فإنه يضع العميل في قائمة الاستبعاد.
8. يتم إنشاء الملائمة بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ويتم إعلام WCS.
9. تتم إزالة المستخدم من قائمة الاستبعاد بعد الفترة الزمنية المحددة.

**تصميم بنية الشبكة**





ال Cisco WLC ربطت إلى ال gigabit قارن على المادة حفازة 6500. قم بإنشاء قناة منفذ لواجهات جيغابت وتمكين جميع الارتباطات (LAG) على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

Cisco Controller) >show interface summary)

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr
ap-manager	LAG	untagged	10.10.99.3	Static	Yes
management	LAG	untagged	10.10.99.2	Static	No
service-port	N/A	N/A	192.168.1.1	Static	No
virtual	N/A	N/A	1.1.1.1	Static	No
vlan101	LAG	101	10.10.101.5	Dynamic	No

ربطت الجهاز تحكم إلى قارن gigabit 5/1 و gigabit 5/2 على المادة حفازة 6500.

```
cat6506#show run interface gigabit 5/1
...Building configuration
```

```
Current configuration : 183 bytes
!
interface GigabitEthernet5/1
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport mode trunk
no ip address
channel-group 99 mode on
end
```

```
cat6506#show run interface gigabit 5/2
...Building configuration
```

```
Current configuration : 183 bytes
!
interface GigabitEthernet5/2
switchport
```

```
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport mode trunk
no ip address
channel-group 99 mode on
end
```

```
cat6506#show run interface port-channel 99
...Building configuration
```

```
Current configuration : 153 bytes
!
interface Port-channel99
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport mode trunk
no ip address
end
```

يمكن أن تعمل واجهات الاستشعار لمستشعر IPS بشكل فردي في الوضع المختلط أو يمكنك مزجها لإنشاء واجهات داخلية لوضع الاستشعار الداخلي.

في الوضع المختلطة، لا تدفق الحزم عبر المستشعر. يقوم المستشعر بتحليل نسخة من حركة المرور المراقبة بدلا من الحزمة الفعلية المعاد توجيهها. تتمثل ميزة التشغيل في الوضع المختلط في أن المستشعر لا يؤثر على تدفق الحزمة مع حركة المرور التي تمت إعادة توجيهها.

**ملاحظة: الرسم التخطيطي للبنية المعمارية** هو مجرد مثال لإعداد بنية WLC و IPS المدمجة. يشرح مثال التكوين الظاهر هنا واجهة استشعار IDS التي تعمل في الوضع المختلطة. [الرسم التخطيطي المعماري](#) يوضح واجهات الاستشعار التي يتم مزامنتها للعمل في وضع زوج الخطية. راجع [الوضع المضمن](#) للحصول على مزيد من المعلومات حول وضع الواجهة المضمنة.

وفي هذا التكوين، يفترض أن واجهة الاستشعار تعمل في الوضع المختلطة. ربطت ال monitorه قارن من ال cisco IDS مستشعر إلى ال gigabit قارن 3/5 على المادة حفازة 6500. خلقت مدرب جلسة على المادة حفازة 6500 حيث ال port-channel قارن المصدر من الربط والغاية يكون gigabit قارن حيث ال monitorه قارن من ال cisco ips مستشعر يكون ربطت. هذا يكرر كل مدخل ومخرج حركة مرور من الجهاز تحكم يربط قارن إلى المعرفات للطبقة 3 من خلال طبقة 7 تفتيش.

```
cat6506#show run | inc monitor
monitor session 5 source interface Po99
monitor session 5 destination interface Gi5/3
```

```
cat6506#show monitor session 5
Session 5
-----
Type                : Local Session
Source Ports        :
Both                : Po99
Destination Ports   : Gi5/3
cat6506#
```

## تكوين مستشعر Cisco IDS

يتم إجراء التكوين الأولي لمستشعر Cisco IDS من منفذ وحدة التحكم أو من خلال توصيل شاشة ولوحة مفاتيح بالمستشعر.

1. تسجيل الدخول إلى الجهاز: توصيل منفذ وحدة تحكم بالمستشعر. قم بتوصيل شاشة ولوحة مفاتيح بالمستشعر.
2. اكتب اسم المستخدم وكلمة المرور الخاصين بك في مطالبة تسجيل الدخول. **ملاحظة:** التقصير username



وكلمة كلا cisco. تتم مطالبتك بتغييرها أول مرة تقوم فيها بتسجيل الدخول إلى الجهاز. أنت ينبغي أولاً دخلت ال UNIX كلمة، أي يكون cisco. بعد ذلك يجب عليك إدخال كلمة المرور الجديدة مرتين.

```
login: cisco
:Password
***NOTICE***
```

This product contains cryptographic features and is subject to ,United States and local country laws governing import, export transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. importers, exporters, distributors and users are .responsible for compliance with U.S. and local country laws By using this product you agree to comply with applicable laws ,and regulations. If you are unable to comply with U.S. and local laws .return this product immediately

A summary of U.S. laws governing Cisco cryptographic products may :be found at

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending .email to [export@cisco.com](mailto:export@cisco.com)

\*\*\*LICENSE NOTICE\*\*\*

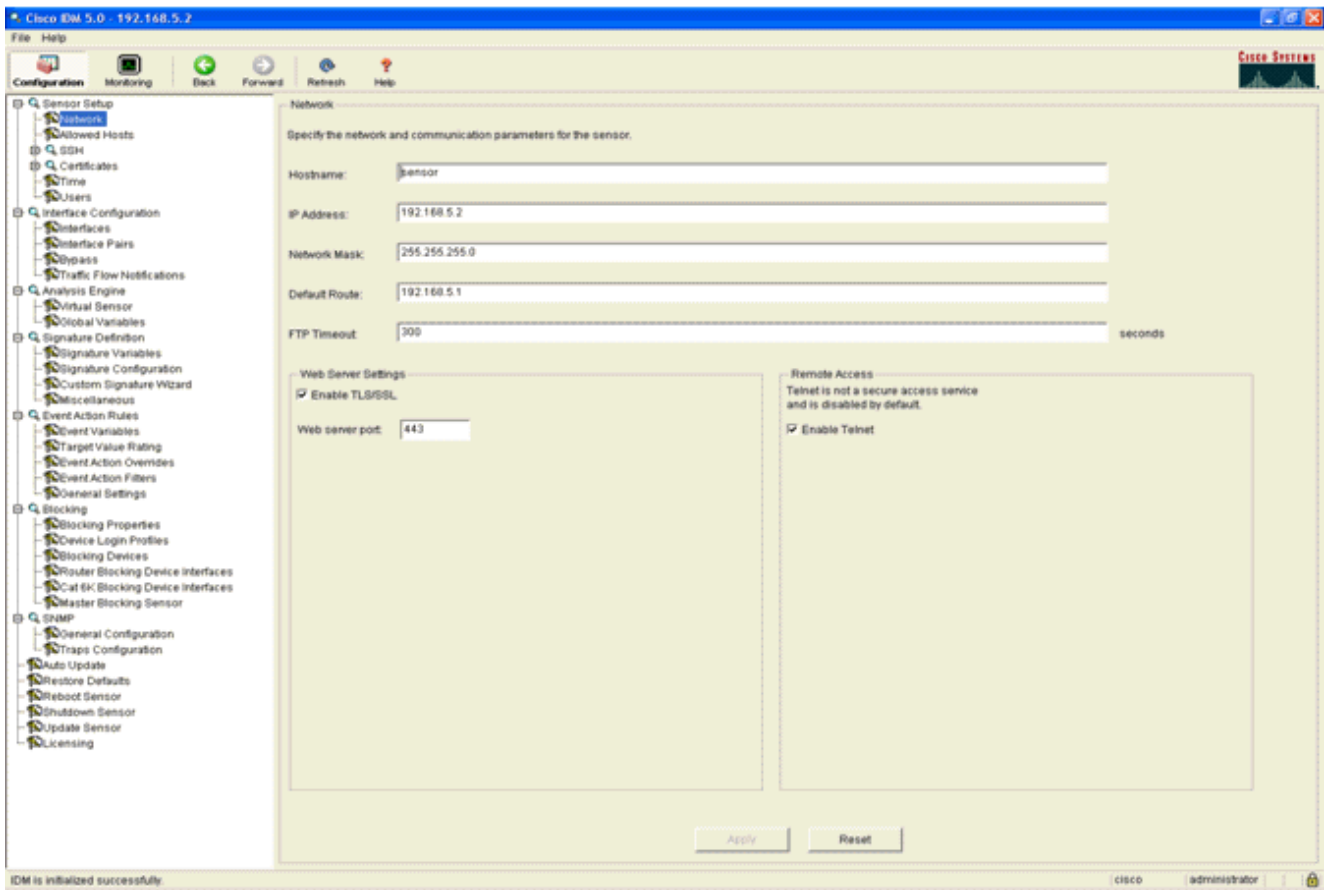
.There is no license key installed on the system

Please go to <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> (registered .customers only) to obtain a new license or install a license

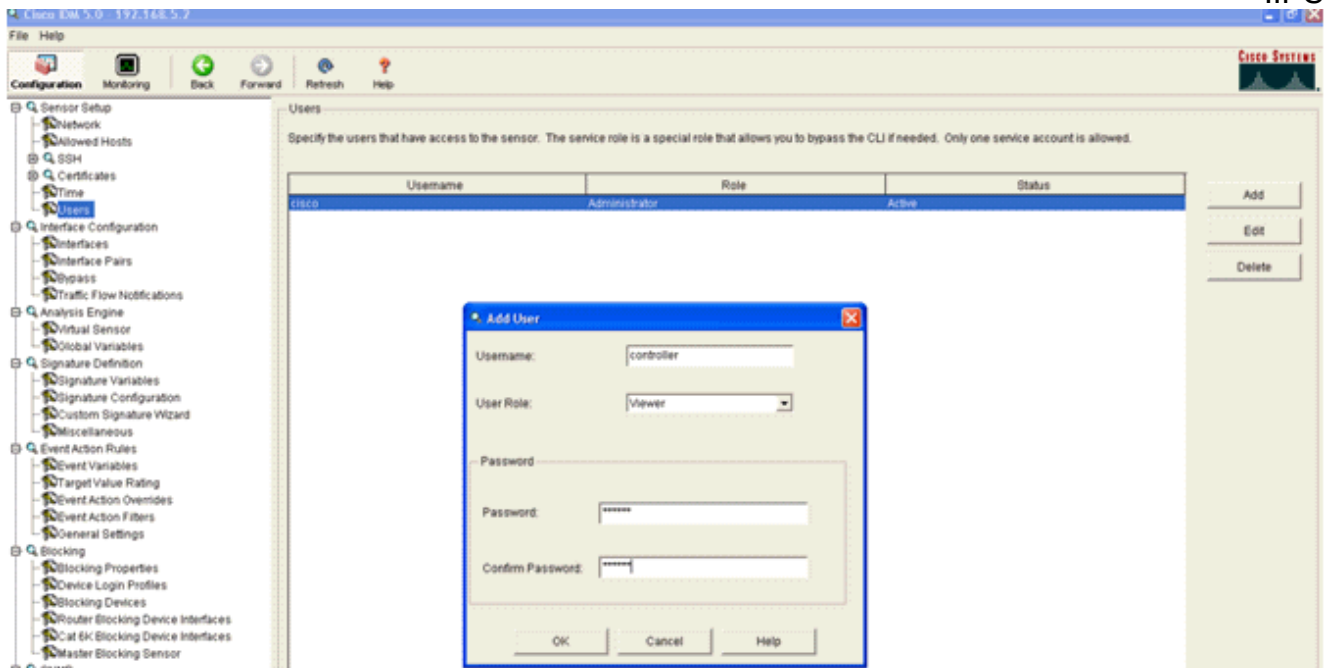
3. قم بتكوين عنوان IP وقناع الشبكة الفرعية وقائمة الوصول على المستشعر. ملاحظة: هذه هي واجهة الأمر والتحكم على المعرفات المستخدمة للاتصال بوحدة التحكم. يجب أن يكون هذا العنوان قابلاً للتوجيه إلى واجهة إدارة وحدة التحكم. ولا تتطلب واجهات الاستشعار معالجة. يجب أن تتضمن قائمة الوصول عنوان واجهة إدارة وحدة التحكم (وحدات التحكم)، بالإضافة إلى العناوين المسموح بها لإدارة المعرفات.

```
sensor#configure terminal
sensor(config)#service host
sensor(config-host)#network-settings
sensor(config-host-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-host-net)#access-list 10.0.0.0/8
sensor(config-host-net)#access-list 40.0.0.0/8
sensor(config-host-net)#telnet-option enabled
sensor(config-host-net)#exit
sensor(config-host)#exit
Apply Changes?[yes]: yes
sensor(config)#exit
#sensor
sensor#ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1): 56 data bytes
bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=0.3 ms 64
bytes from 192.168.5.1: icmp_seq=1 ttl=255 time=0.9 ms 64
bytes from 192.168.5.1: icmp_seq=2 ttl=255 time=0.3 ms 64
bytes from 192.168.5.1: icmp_seq=3 ttl=255 time=1.0 ms 64
--- ping statistics 192.168.5.1 ---
packets transmitted, 4 packets received, 0% packet loss 4
round-trip min/avg/max = 0.3/0.6/1.0 ms
#sensor
```

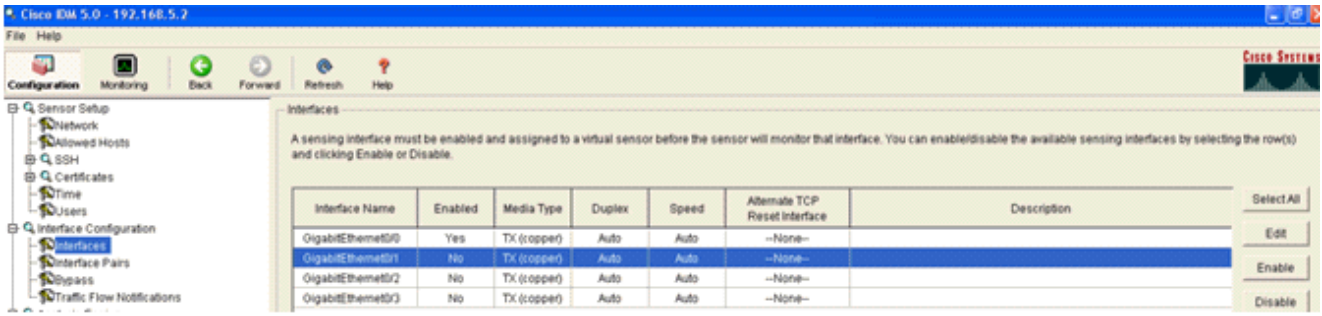
4. أنت يستطيع الآن شكلت ال IPS مستشعر من ال gui. قم بتوجيه المستعرض إلى عنوان IP الخاص بإدارة المستشعر. تعرض هذه الصورة عينة حيث يتم تكوين المستشعر باستخدام 192.168.5.2.



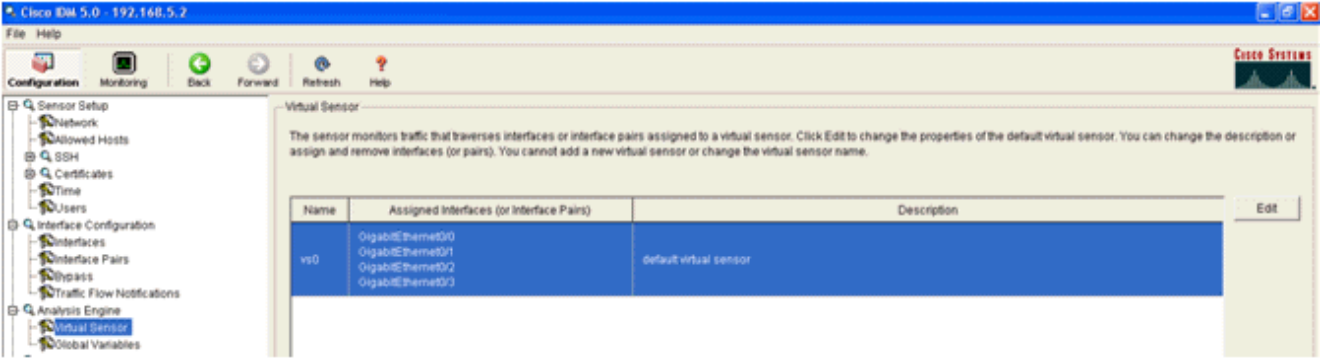
5. إضافة مستخدم يستخدم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للوصول إلى أحداث مستشعر IPS.



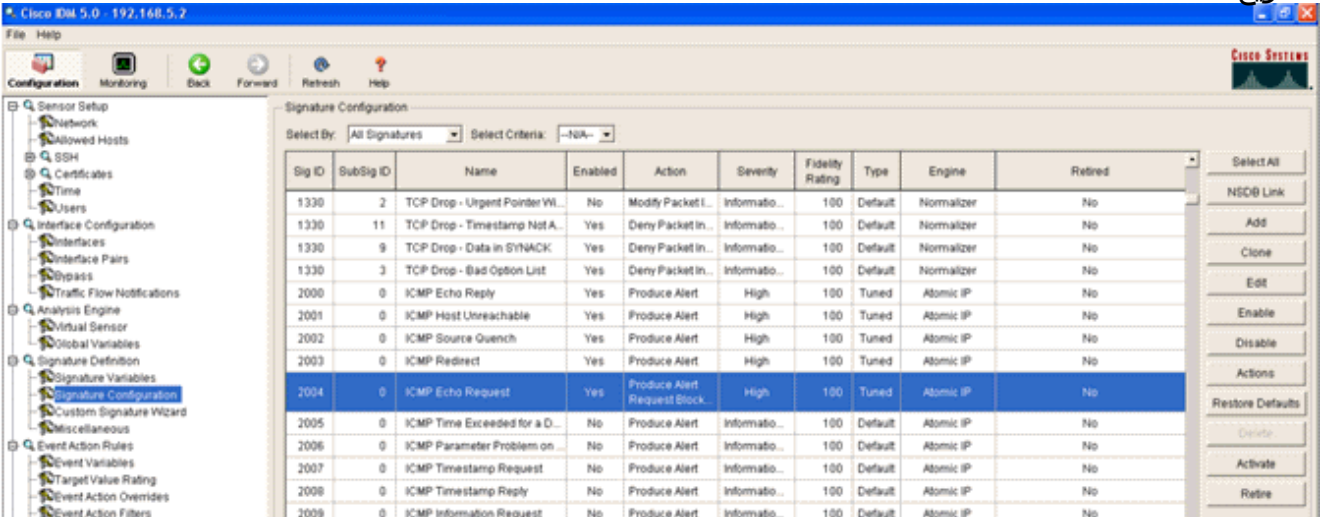
6. قم بتمكين واجهات المراقبة.



يجب إضافة واجهات المراقبة إلى "محرك التحليل"، كما توضح هذه النافذة:



7. حدد توقيع 2004 (طلب صدى ICMP) لإجراء التحقق من الإعداد السريع.



يجب تمكين التوقيع، وتعيين خطورة التنبيه على عالي وتعيين إجراء الحدث لإنتاج تنبيه ومضيف كتلة الطلب لإتمام خطوة التحقق هذه.

**Edit Signature**

Name	Value
Signature ID:	2004
SubSignature ID:	0
Alert Severity:	High
Sig Fidelity Rating:	100
Promiscuous Delta:	0
<b>Sig Description:</b>	
Signature Name:	ICMP Echo Request
Alert Notes:	
User Comments:	
Alert Traits:	0
Release:	S1
<b>Engine:</b> Atomic IP	
Event Action:	Produce Alert
Fragment Status:	Any
Specify Layer 4 Protocol:	Yes
<b>Layer 4 Protocol:</b> ICMP Protocol	
Specify ICMP Sequence:	No
Specify ICMP Type:	Yes
ICMP Type:	8
Specify ICMP Code:	No
Specify ICMP Identifier:	No
Specify ICMP Total Length:	No

Parameter uses the Default Value. Click the icon to edit the value.  
Parameter uses a User-Defined Value. Click the icon to restore the default value.

OK Cancel Help

## تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

أتمت هذا steps in order to شكلت ال WLC:

1. بمجرد تكوين جهاز IPS واستعداده لإضافة وحدة التحكم، اختر الأمان < أدوات CIDS < أجهزة الاستشعار < جديد.
2. قم بإضافة عنوان IP، ورقم منفذ TCP، واسم المستخدم وكلمة المرور التي أنشأتها مسبقاً. من أجل الحصول على بصمة الإصبع من مستشعر IPS، قم بتنفيذ هذا الأمر في مستشعر IPS وأضف بصمة SHA1 على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) (دون علامة القولون). يستخدم هذا لتأمين اتصال اقتراع وحدة التحكم إلى ID.

**sensor#show tls fingerprint**

MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19

SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42

Save Configuration Ping Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Security

CIDS Sensor Add < Back Apply

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

Network Access Control

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Signature Events
- Summary
- Client Exclusion Policies
- AP Authentication
- Management Frame Protection

Web Login Page

CIDS

- Sensors
- Shunned Clients

Index: 1

Server Address: 192.168.5.2

Port: 443

Username: controller

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Query Interval: 15 seconds

State:

Fingerprint (SHA1 hash): 1662E996362A9A1EF08899A7C1645F5CB56A8B42 40 hex chars

3. تحقق من حالة الاتصال بين مستشعر IPS و WLC.

Save Configuration Ping Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Security

CIDS Sensors List New...

Index	Server Address	Port	State	Query Interval	Last Query (count)	
1	192.168.5.2	443	Enabled	15	Success (6083)	<a href="#">Detail</a> <a href="#">Remove</a>

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

Network Access Control

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Signature Events
- Summary
- Client Exclusion Policies
- AP Authentication
- Management Frame Protection

Web Login Page

CIDS

- Sensors
- Shunned Clients

4. بمجرد إنشاء الاتصال باستخدام مستشعر Cisco IPS، تأكد من أن تكوين شبكة WLAN صحيح ومن تمكين إستثناء العميل. قيمة مهلة إستثناء العميل الافتراضية هي 60 ثانية. لاحظ أيضا أنه بغض النظر عن مؤقت إستثناء العميل، يستمر إستثناء العميل طالما ظل كتلة العميل التي تم استدعاؤها بواسطة المعرفات نشطا. وقت الحظر الافتراضي في المعرفات هو 30 دقيقة.

5. يمكنك تشغيل حدث في نظام Cisco IPS إما عند إجراء مسح NMAP لأجهزة معينة في الشبكة أو عند إجراء اختبار اتصال لبعض الأجهزة المضيغة التي تتم مراقبتها بواسطة مستشعر Cisco IPS. بمجرد تشغيل الإنذار في Cisco IPS، انتقل إلى المراقبة وحواجز المضيف النشطة للتحقق من تفاصيل حول المضيف.

Source IP	Destination IP	Destination Port	Protocol	Minutes Remaining	Timeout (minutes)	VLAN	Connection Block Enable
10.10.99.21	10.10.99.1	0	1	10	10	0	false

يتم الآن ملء قائمة العملاء المبعدين في وحدة التحكم بعنوان IP و MAC الخاص

Cisco Systems

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

Network Access Control

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Signature Events
- Summary
- Client Exclusion Policies
- AP Authentication
- Management Frame Protection

Web Login Page

CIDS

- Sensors
- Shunned Clients

CIDS Shun List

Re-sync

IP Address	Last MAC Address	Expire	Sensor IP / Index
10.10.99.21	00:40:96:ad:0d:1b	326979296	192.168.5.2 / 1

تم

بالمضيف.

إضافة المستخدم إلى قائمة "إستبعاد العميل".

Cisco Systems

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor

Summary

Statistics

- Controller
- Ports

Wireless

Excluded Clients

Search by MAC address  Search

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Exclusion Reason	Port
00:40:96:ad:0d:1b	AP1242-2	00:14:1b:59:3e:10	IPS	802.11b	UnknownEnum:5	29 <a href="#">Detail</a> <a href="#">Link</a> <a href="#">Test</a> <a href="#">Disable</a> <a href="#">Remove</a>

يتم إنشاء سجل ملائمة أثناء إضافة عميل إلى قائمة

Cisco Systems

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Management

Summary

SNMP

- General
- SNMP V3 Users
- Communities
- Trap Receivers
- Trap Controls
- Trap Logs

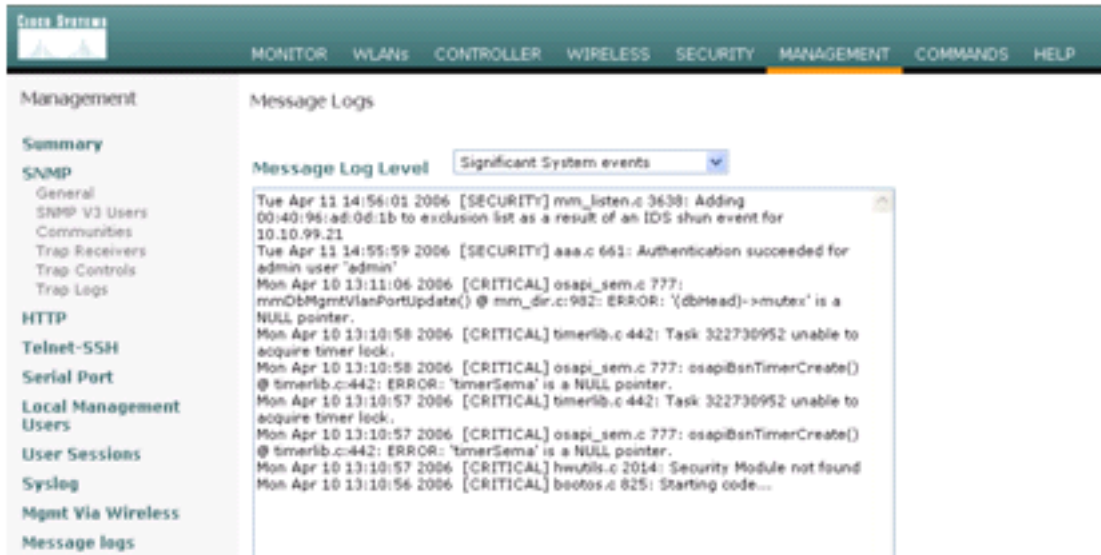
32	Tue Apr 11 14:41:00 2006	Rogue AP : 00:15:c7:82:83:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g) with RSSI: -83 and SNR: 6
33	Tue Apr 11 14:40:16 2006	New client at 10.10.99.21 requested to be shunned by Sensor at 192.168.5.2
34	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85:54:de:5d removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
35	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85:54:de:5e removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
36	Tue Apr 11 14:39:44	Rogue : 00:0b:85:54:de:5f removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)

يتم

التجاهل.

م أيضا إنشاء سجل رسائل

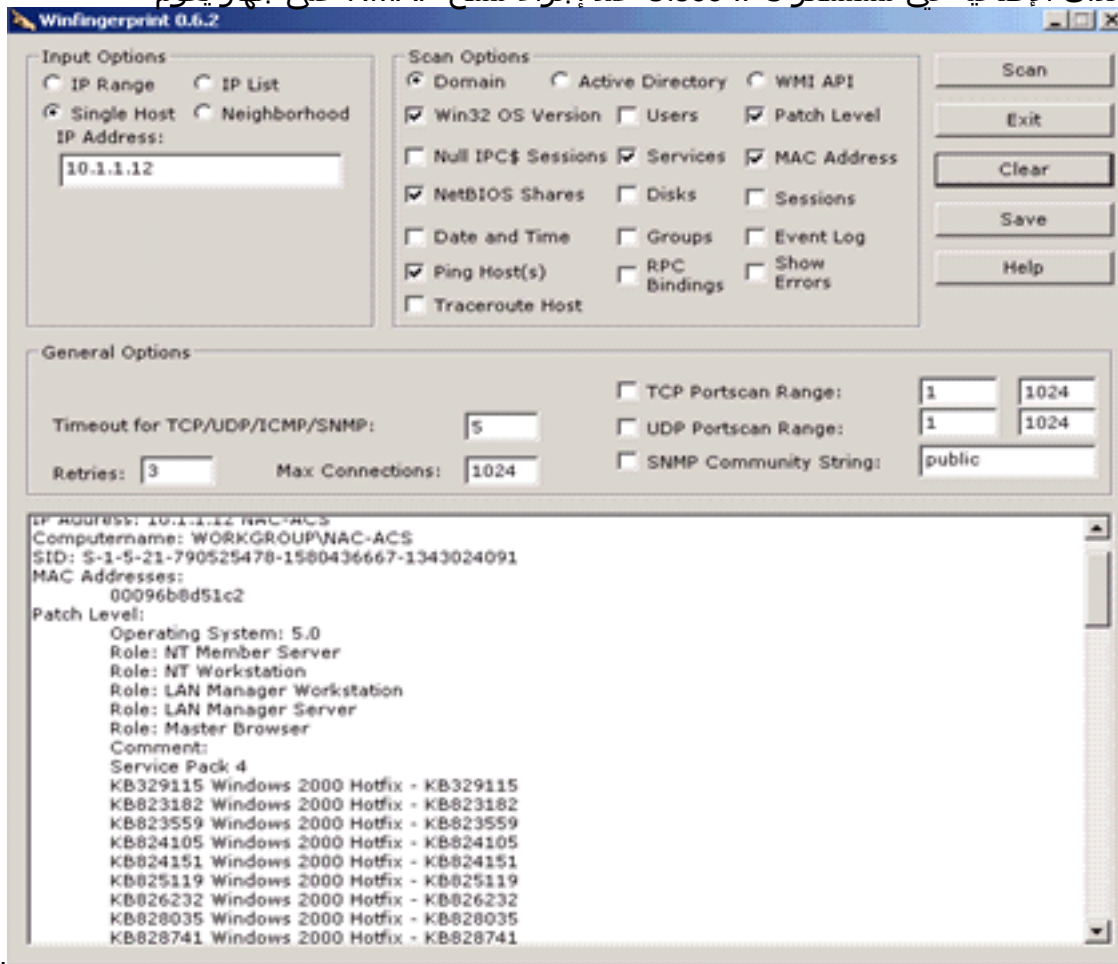




يتم إنشاء

للحدث.

بعض الأحداث الإضافية في مستشعر Cisco IPS عند إجراء مسح NMAP على جهاز يقوم

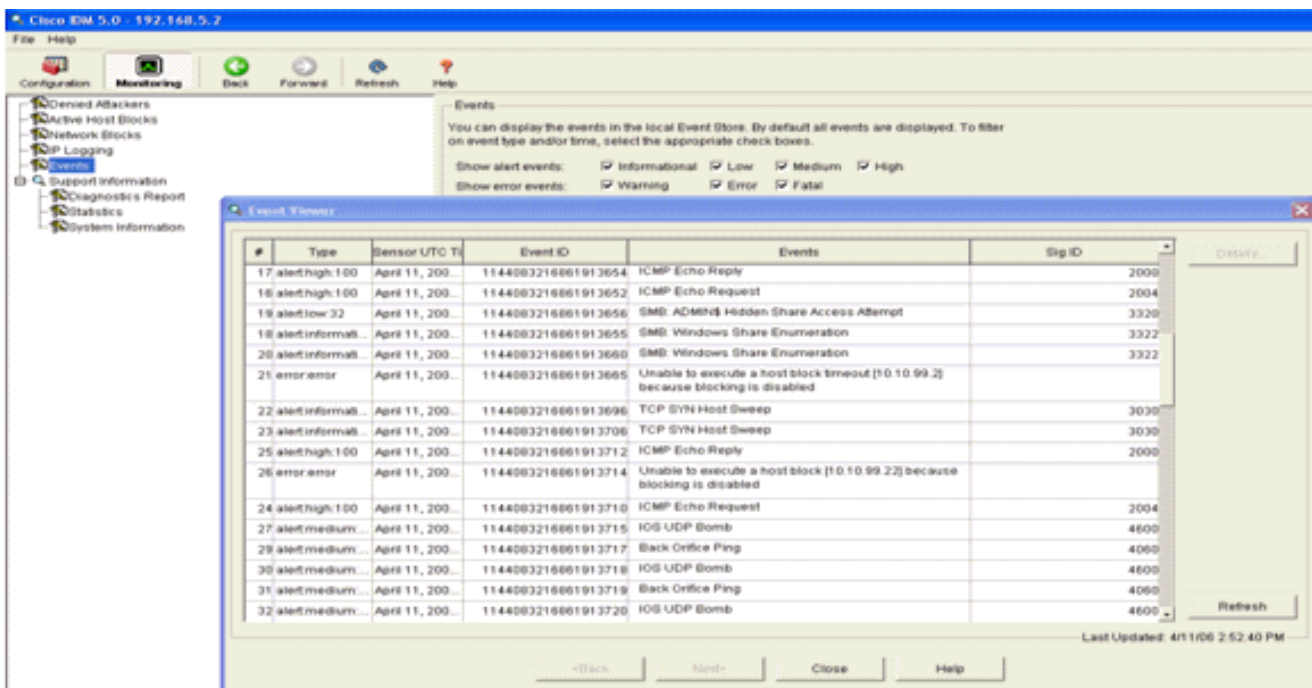


بيدي

بمراقبته.

هذا نافذة أحداث ولدت في ال Cisco IPS مستشعر.

مستشعر.



## Cisco IDS تكوين عينة مستشعر

هذا هو المخرج من البرنامج النصي للإعداد من الثبيت:

```

sensor#show config
----- !
              (Version 5.0(2)
Current configuration last modified Mon Apr 03 15:32:07 2006 !
----- !
              service host
              network-settings
host-ip 192.168.5.2/25,192.168.5.1
              host-name sensor
              telnet-option enabled
              access-list 10.0.0.0/8
              access-list 40.0.0.0/8
              exit
              time-zone-settings
              offset 0
              standard-time-zone-name UTC
              exit
              exit
----- !
              service notification
              exit
----- !
              service signature-definition sig0
              signatures 2000 0
              alert-severity high
              status
              enabled true
              exit
              exit
              signatures 2001 0
              alert-severity high
              status
              enabled true
              exit

```

```

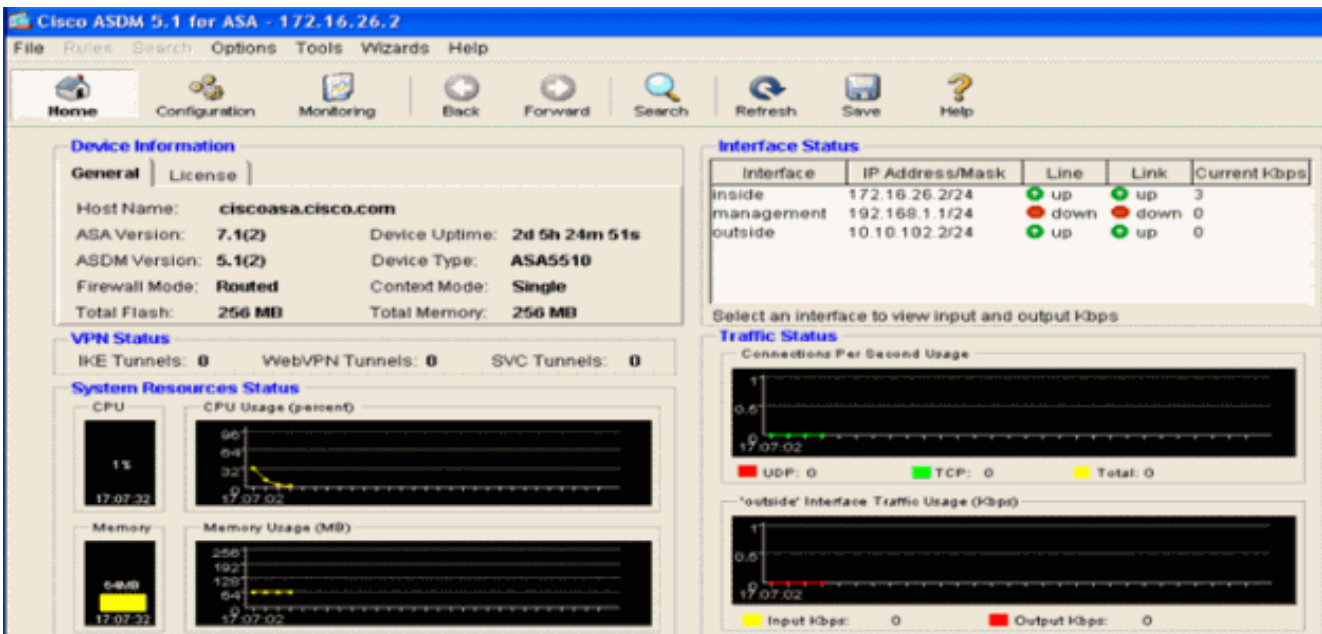
exit
signatures 2002 0
alert-severity high
status
enabled true
exit
exit
signatures 2003 0
alert-severity high
status
enabled true
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
----- !
service event-action-rules rules0
exit
----- !
service logger
exit
----- !
service network-access
exit
----- !
service authentication
exit
----- !
service web-server
exit
----- !
service ssh-known-hosts
exit
----- !
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/0
exit
exit
----- !
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
exit
----- !
service trusted-certificates
exit
#sensor

```

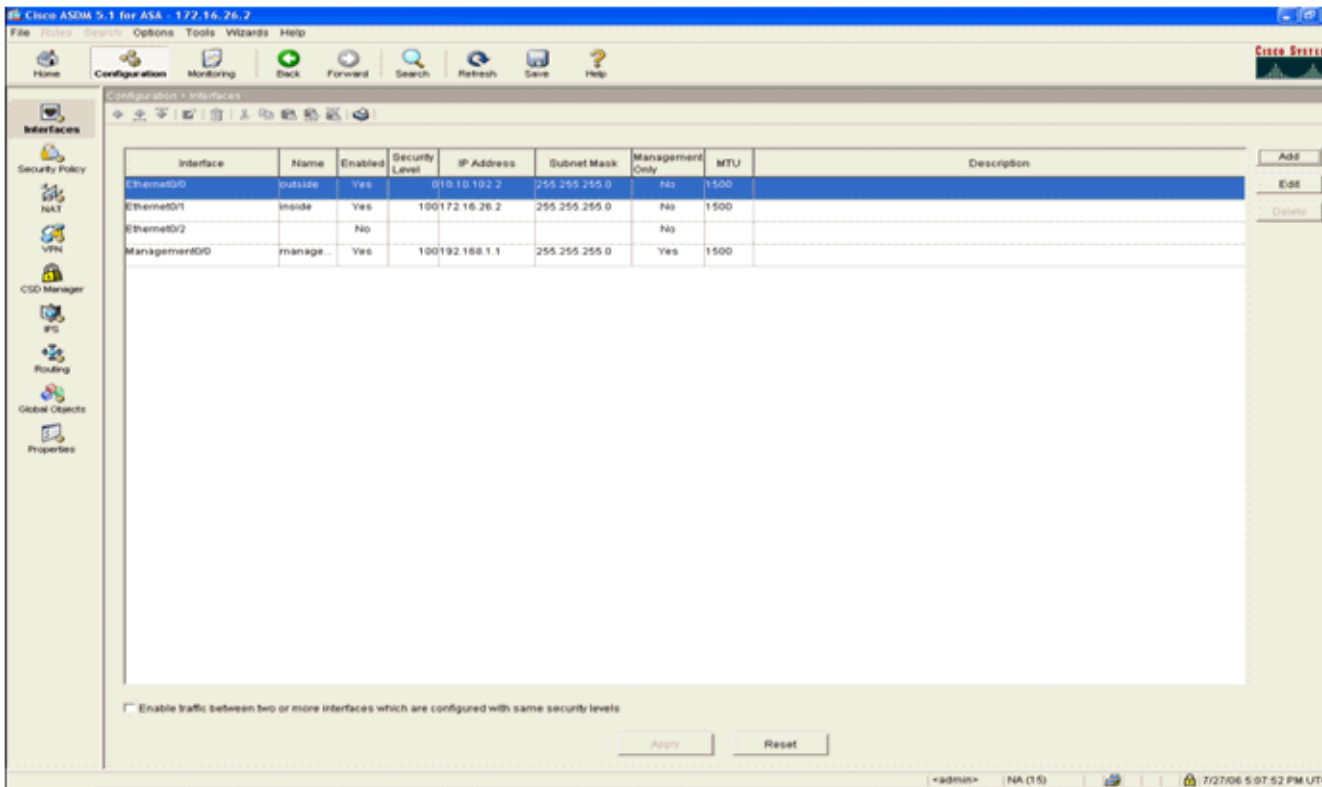
## تكوين ASA للمعرفات

وعلى عكس مستشعر اكتشاف الاقتحام التقليدي، يجب أن يكون ASA دائما في مسار البيانات. instead of يجسر حركة مرور من مفتاح ميناء إلى حامل ينشق ميناء على المستشعر، ال ASA ينبغي إستلمت in other words.

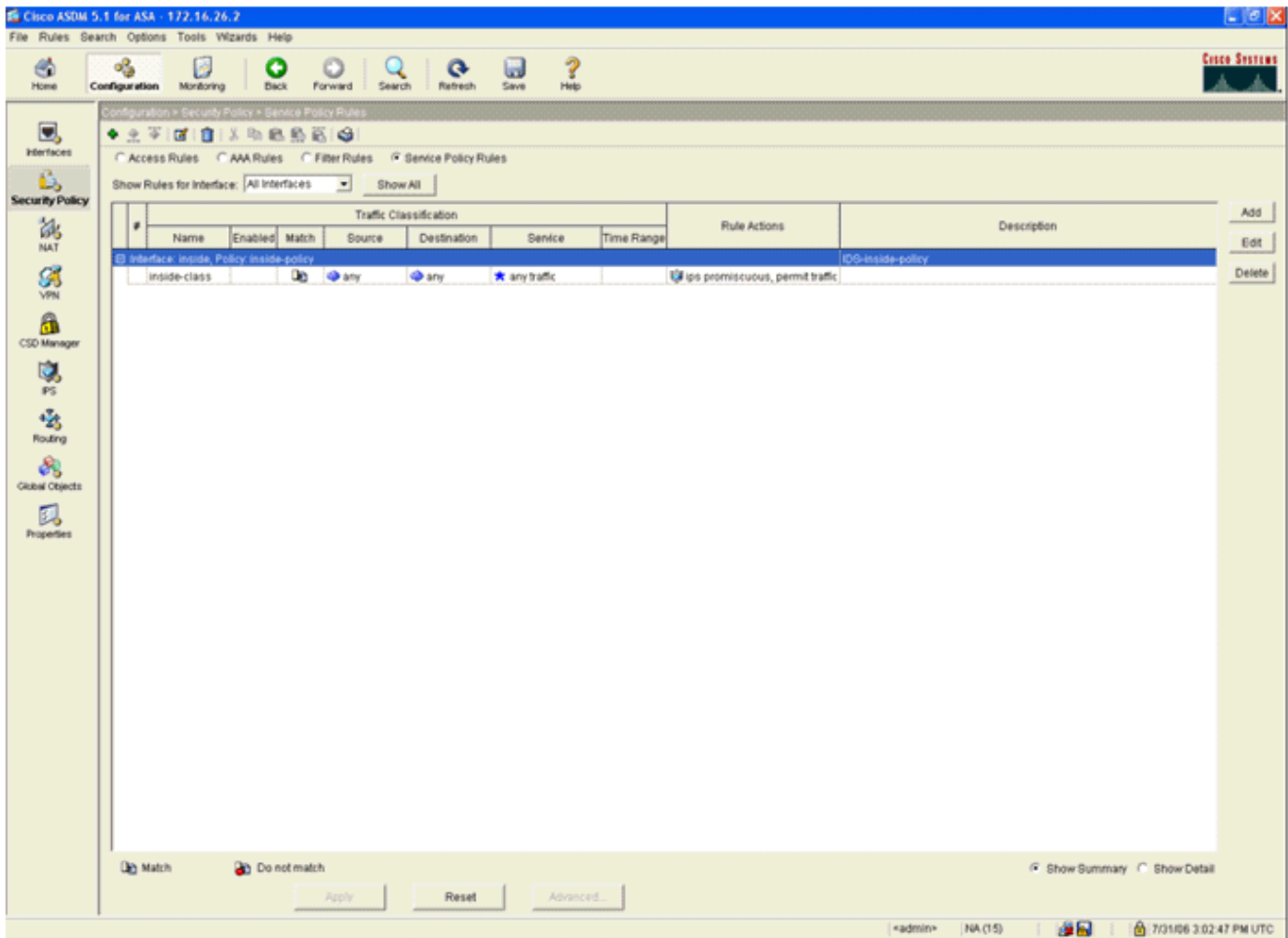




2. انقر فوق تكوين في أعلى الصفحة. تبديل النافذة إلى طريقة عرض واجهات ASA.



3. انقر فوق نهج الأمان في الجانب الأيسر من الإطار. في الإطار الناتج، أختار علامة التبويب قواعد سياسة الخدمة.



4. انقر فوق **إضافة** لإنشاء سياسة جديدة. يتم تشغيل "معالج إضافة قاعدة سياسة الخدمة" في نافذة جديدة. انقر فوق **الواجهة** ثم اختر الواجهة الصحيحة من القائمة المنسدلة لإنشاء سياسة جديدة مرتبطة بإحدى الواجهات التي تمرر حركة مرور البيانات. قم بتسمية النهج ووصف ما تقوم به السياسة باستخدام مربعي النص. طقطقت بعد ذلك in order to نقلت إلى الخطوة تالي.

**Add Service Policy Rule Wizard - Service Policy**

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a service policy and apply to:

Interface:

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

Description:

< Back   Next >   Cancel   Help

5. قم بإنشاء فئة حركة مرور جديدة لتطبيقها على السياسة. من المنطقي إنشاء فئات معينة للتحقق من أنواع بيانات معينة، ولكن في هذا المثال، يتم تحديد أي حركة مرور للتبسيط. طقطقت بعد ذلك in order to باشرت.



**Add Service Policy Rule Wizard - Traffic Classification Criteria**

Create a new traffic class:

Description (optional):

Traffic match criteria

Default Inspection Traffic

Source and Destination IP Address (uses ACL)

Tunnel Group

TCP or UDP Destination Port

RTP Range

IP DiffServ CodePoints (DSCP)

IP Precedence

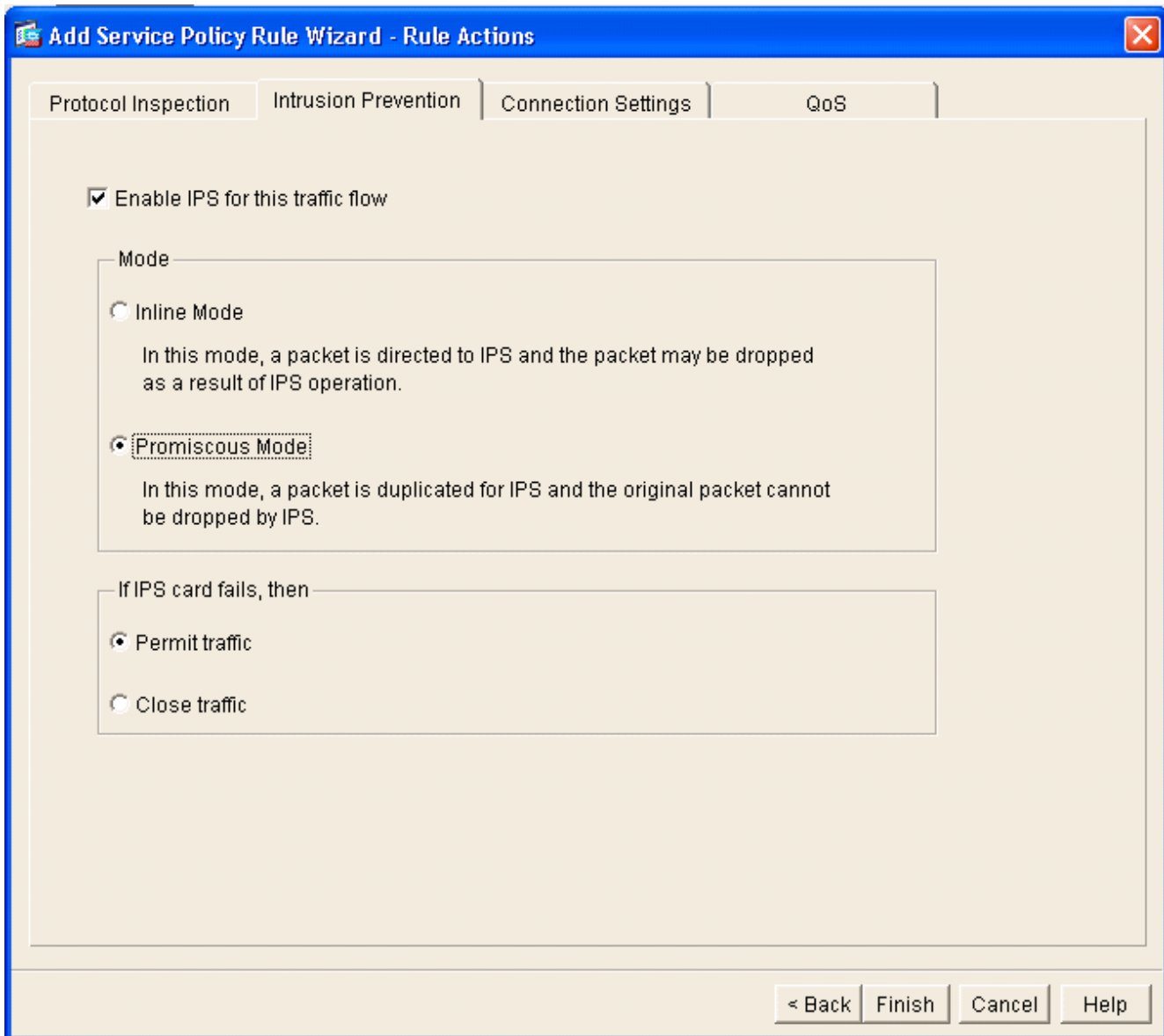
Any traffic

If traffic does not match a existing traffic class, then it will match the class-default traffic class.  
Class-default can be used in catch all situation.

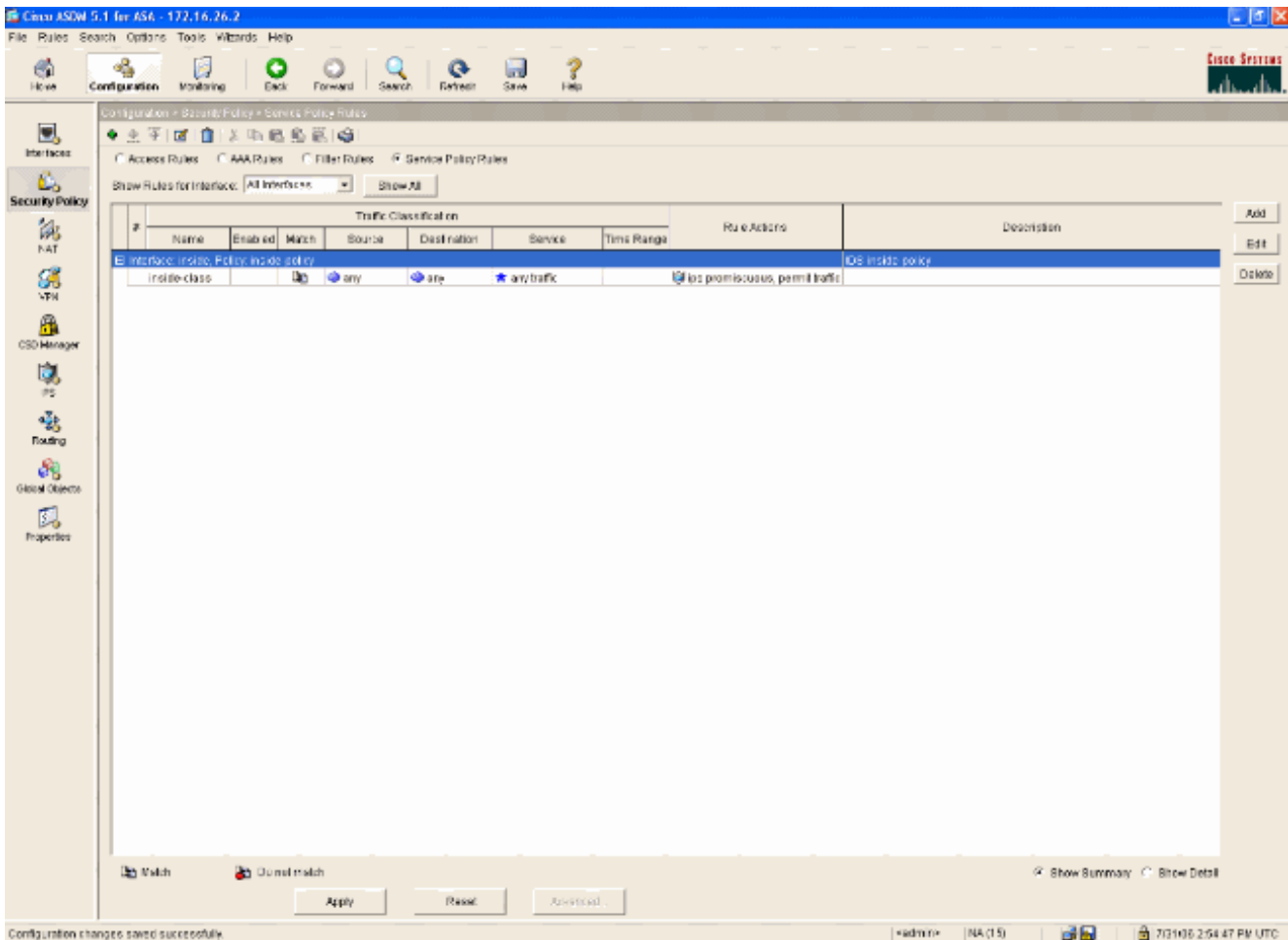
Use class-default as the traffic class.

< Back   Next >   Cancel   Help

6. أتمت هذا steps in order to توجيه ASA لتوجيه حركة المرور إلى AIP-SSM الخاص به. تحقق من تمكين IPS لتدفق حركة المرور هذا لتمكين اكتشاف التسلسل. قم بتعيين الوضع على المختلطة بحيث يتم إرسال نسخة من حركة المرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات. طقطقة يسمح حركة مرور in order to ضمنت أن ال ASA يحول إلى حالة فشل-مفتوح في حالة أن AIP-SSM يفشل. طقطقة إنجاز in order to أنجزت التغيير.



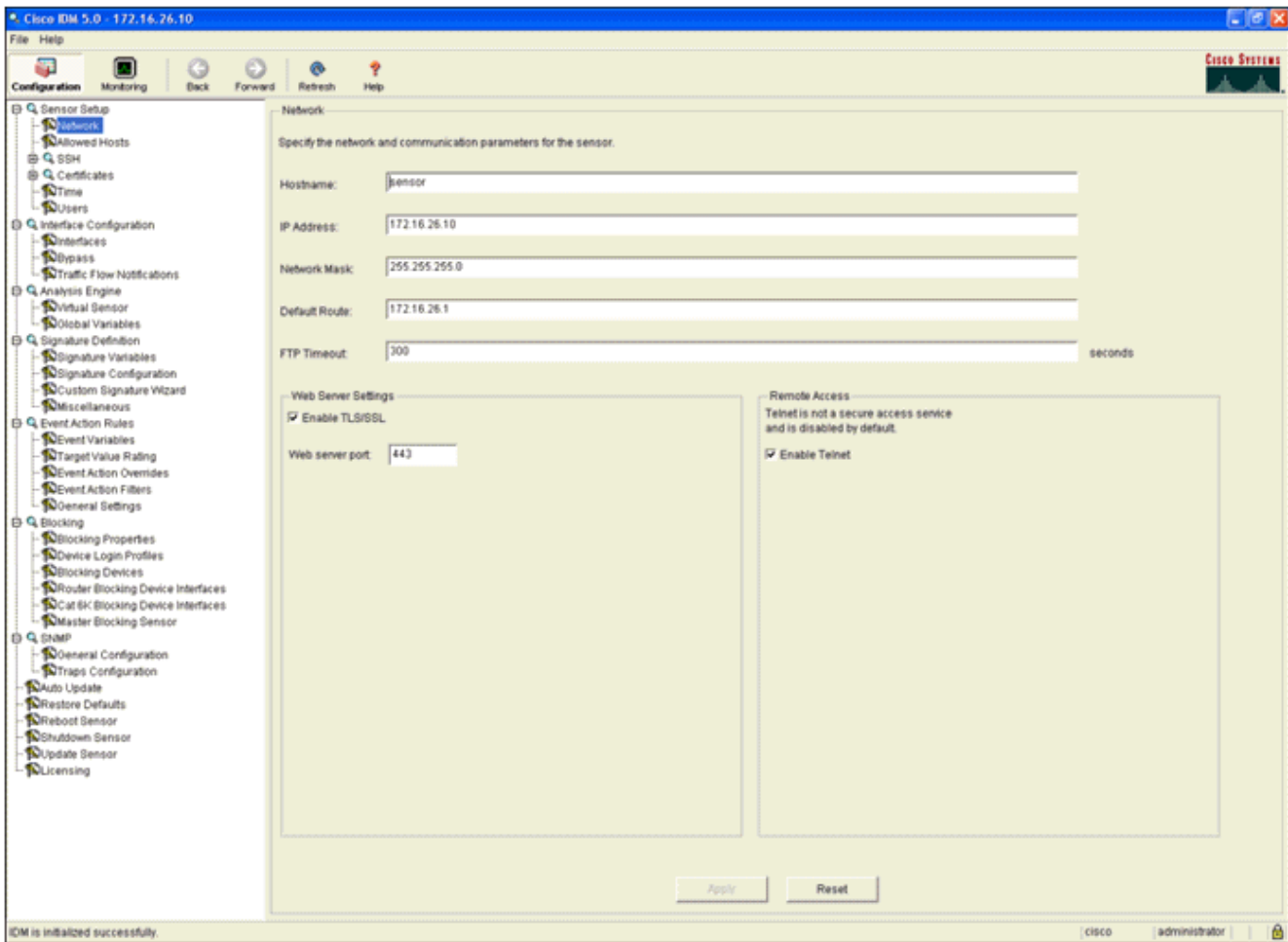
7. تم تكوين ASA الآن لإرسال حركة مرور البيانات إلى وحدة IPS النمطية. طقطقة حفظ في الصف الأعلى in order to كتبت التغييرات إلى ال .ASA



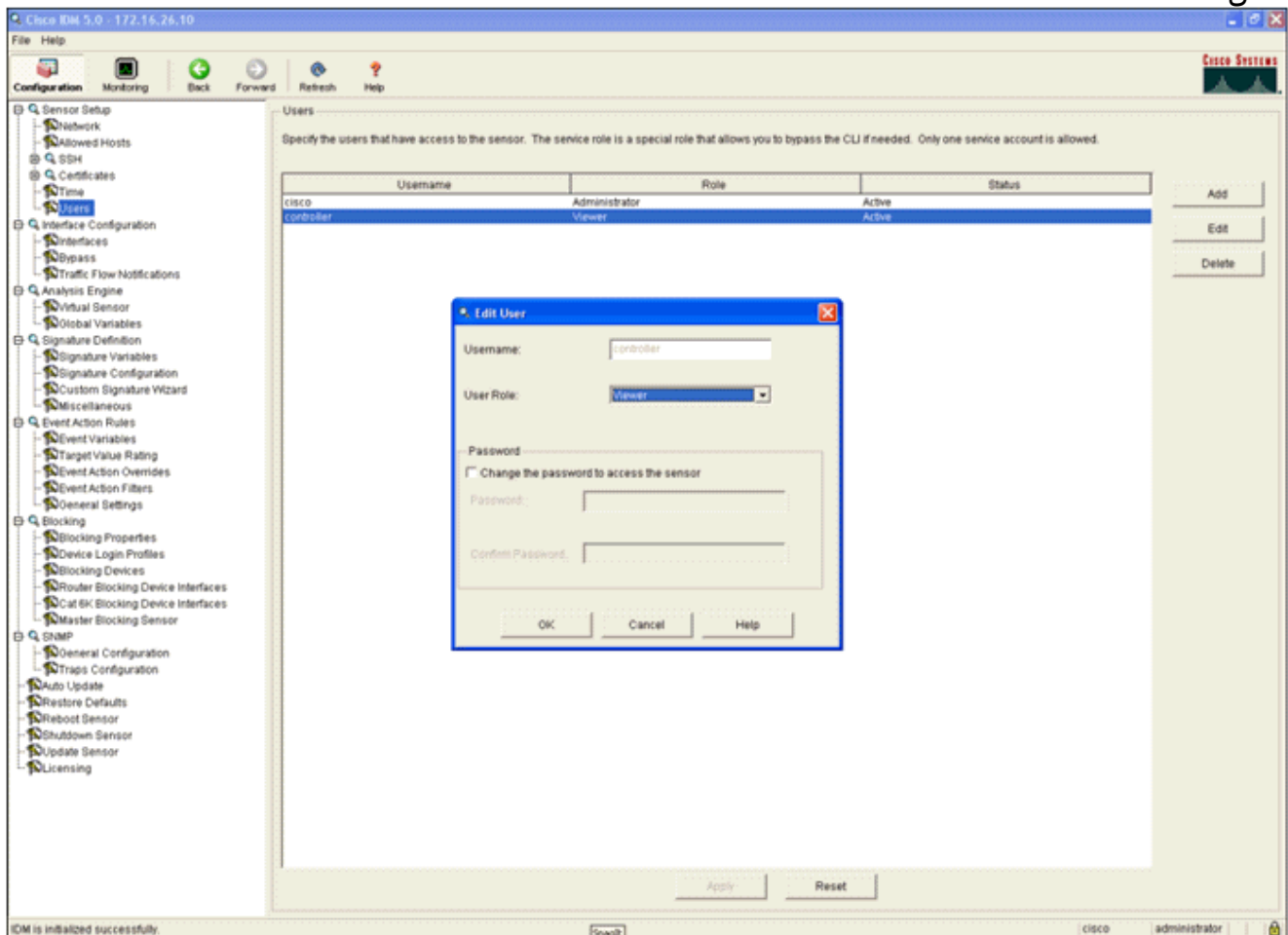
## شكلت AIP-SSM ل حركة مرور تفتيش

بينما يقوم ASA بإرسال البيانات إلى الوحدة النمطية IPS، قم بإقران واجهة AIP-SSM بمحرك المستشعر الظاهري الخاص بها.

1. قم بتسجيل الدخول إلى AIP-SSM باستخدام .IDM



2. إضافة مستخدم بامتيازات عارض على الأقل.



### 3. مكنت القارن.

Interfaces

A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

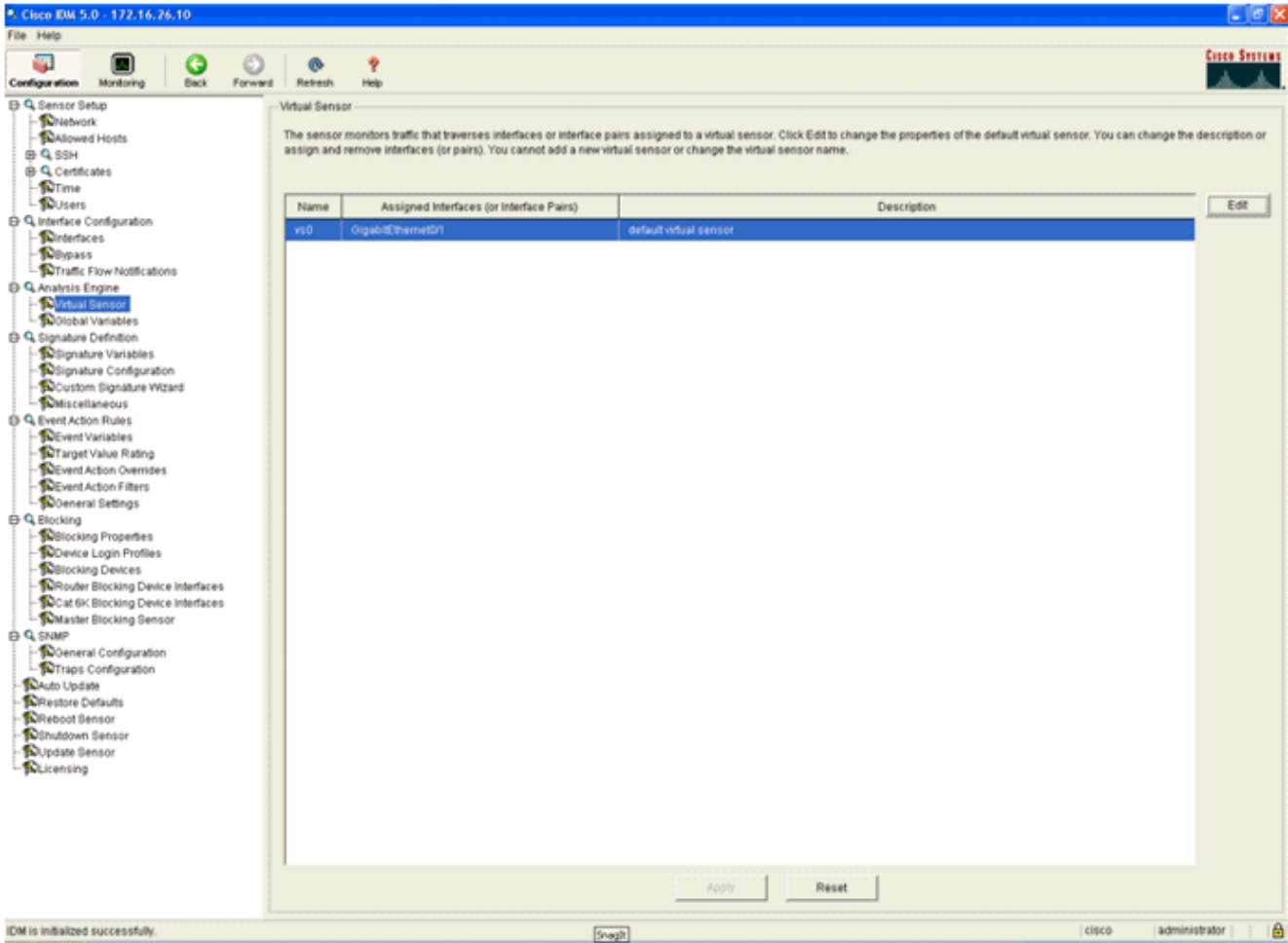
Interface Name	Enabled	Media Type	Duplex	Speed	Alternate TCP Reset Interface	Description
GigabitEthernet0/1	Yes	Backplane in...	Auto	Auto	--None--	

Select All  
Edit  
Enable  
Disable

Apply Reset

IDM is initialized successfully | cisco administrator

### 4. تحقق من تكوين المستشعر الظاهري.



## تكوين WLC لاستطلاع AIP-SSM لكتل العميل

أكمل الخطوات التالية بمجرد تكوين "المستشعر" واستعداده لإضافته في وحدة التحكم:

1. أختار التأمين < CIDS < أجهزة إستشعار < جديد في WLC.
2. أضفت العنوان، TCP ميناء رقم، username وكلمة أنت خلقت في الفرع السابق.
3. من أجل الحصول على بصمة الإصبع من المستشعر، قم بتنفيذ هذا الأمر في المستشعر وقم بإضافة بصمة SHA1 على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) (بدون علامة القولون). يستخدم هذا لتأمين اتصال اقتراع وحدة التحكم إلى ID.

```
sensor#show tls fingerprint
```

```
MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E
```

```
SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55
```

Cisco Systems

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Signature Events
- Summary
- Client Exclusion Policies
- AP Authentication / MFP
- Management Frame Protection

Web Login Page

CIDS

- Sensors
- Shunned Clients

CIDS Sensor Edit

Index 2

Server Address 172.16.26.10

Port 443

Username controller

Password \*\*\*\*\*

State

Query Interval 10 seconds

Fingerprint (SHA1 hash) 98C9969B4EFA74F8528092BDBC483C45B4876C55 40 hex chars  
(hash key is already set)

Last Query (count) Success (1400)

4. تحقق من حالة الاتصال بين AIP-SSM و WLC.

Cisco Systems

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Signature Events
- Summary
- Client Exclusion Policies
- AP Authentication / MFP
- Management Frame Protection

Web Login Page

CIDS

- Sensors
- Shunned Clients

CIDS Sensors List

Index	Server Address	Port	State	Query Interval	Last Query (count)	
1	192.168.5.2	443	Enabled	15	Unauthorized (1)	<a href="#">Detail</a> <a href="#">Remove</a>
2	172.16.26.10	443	Enabled	10	Success (1444)	<a href="#">Detail</a> <a href="#">Remove</a>

## إضافة توقيع حظر إلى AIP-SSM

إضافة توقيع فحص لحظر حركة المرور. على الرغم من وجود العديد من التوقيعات التي يمكنها القيام بالمهمة بناء على الأدوات المتاحة، فإن هذا المثال ينشئ توقيعاً يمنع حزم إختبار الاتصال.

1. حدد توقيع 2004 (طلب صدى ICMP) لإجراء التحقق من الإعداد السريع.



Cisco SDM 5.0 - 192.168.5.2

File Help

Configuration Monitoring Back Forward Refresh Help

Sensor Setup

- Network
- Allowed Hosts
- SSH
- Certificates
- Time
- Users

Interface Configuration

- Interfaces
- Interface Pairs
- Bypass
- Traffic Flow Notifications

Analysis Engine

- Virtual Sensor
- Global Variables
- Signature Definition
- Signature Variables
- Signature Configuration
- Custom Signature Wizard
- Miscellaneous

Event Action Rules

- Event Variables
- Target Value Rating
- Event Action Overrides
- Event Action Filters

Signature Configuration

Select By: All Signatures Select Criteria: --N/A--

Sig ID	SubSig ID	Name	Enabled	Action	Severity	Fidelity Rating	Type	Engine	Retired
1330	2	TCP Drop - Urgent Pointer Wl...	No	Modify Packet L...	Informatio...	100	Default	Normalizer	No
1330	11	TCP Drop - Timestamp Not A...	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2004	0	ICMP Echo Request	Yes	Produce Alert Request Block...	High	100	Tuned	Atomic IP	No
2005	0	ICMP Time Exceeded for a D...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2006	0	ICMP Parameter Problem on...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2008	0	ICMP Timestamp Reply	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2009	0	ICMP Information Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No

Actions: Select All, NSOB Link, Add, Clone, Edit, Enable, Disable, Actions, Restore Defaults, Delete, Activate, Retire

2. قم بتمكين التوقيع وتعيين خطورة التنبيه إلى عالية وتعيين إجراء الحدث لإنتاج تنبيه ومضيف كتلة الطلب من أجل إكمال خطوة التحقق هذه. لاحظ أن إجراء مضيف حظر الطلب هو المفتاح لإرسال إشارة إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإنشاء إستثناءات العميل.

Edit Signature

Name Value

Signature ID: 2004

SubSignature ID: 0

Alert Severity: High

Sig Fidelity Rating: 100

Promiscuous Delta: 0

Sig Description:

Signature Name: ICMP Echo Request

Alert Notes:

User Comments:

Alert Traits: 0

Release: S1

Engine: Atomic IP

Event Action: Produce Alert, Produce Verbose Alert, Request Block Connector, Request Block Host, Request Snmp Trap

Fragment Status: Any

Specify Layer 4 Protocol: Yes

Layer 4 Protocol: ICMP Protocol

Specify ICMP Sequence: No

Specify ICMP Type: Yes

ICMP Type: 8

Specify ICMP Code: No

Specify ICMP Identifier: No

Specify ICMP Total Length: No

Parameter uses the Default Value. Click the icon to edit the value.

Parameter uses a User-Defined Value. Click the icon to restore the default value.

OK Cancel Help

**Edit Signature**

Name	Value
Signature ID:	2004
SubSignature ID:	0
Alert Severity:	Informational
Sig Fidelity Rating:	100
Promiscuous Delta:	0
<b>Sig Description:</b>	
Signature Name:	ICMP Echo Request
Alert Notes:	
User Comments:	
Alert Traits:	0
Release:	S1
<b>Engine:</b> Atomic IP	
Event Action:	Request Block Connector Request Block Host Request Snmp Trap Reset Tcp Connection
Fragment Status:	

Parameter uses the Default Value. Click the icon to edit the value.  
Parameter uses a User-Defined Value. Click the icon to restore the default value.

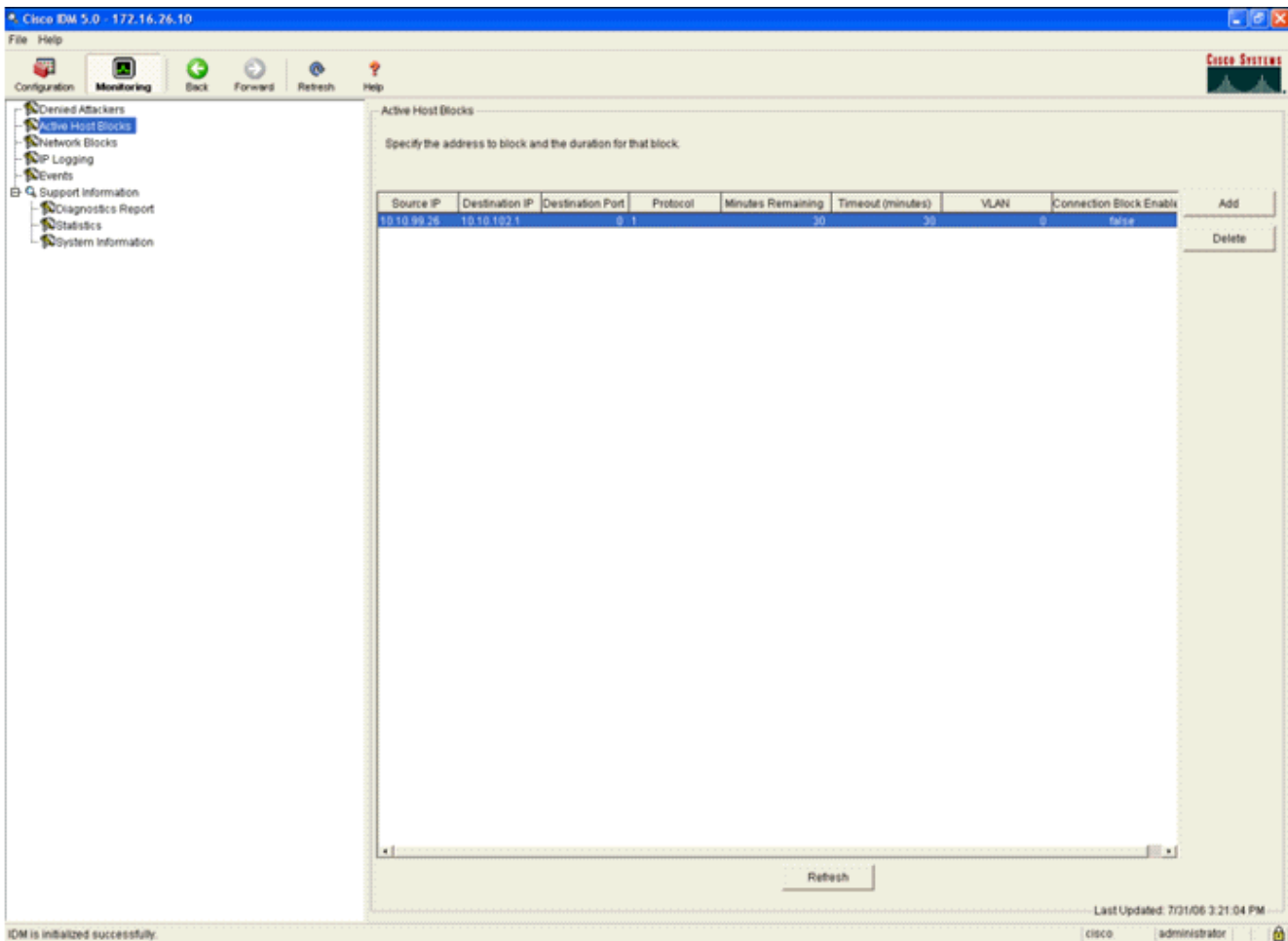
OK Cancel Help

3. طقطقة ok in order to أنفذت التوقيع.
4. تحقق من أن التوقيع نشط ومن أنه تم تعيينه لتنفيذ إجراء حظر.
5. انقر فوق تطبيق لتنفيذ التوقيع على الوحدة النمطية.

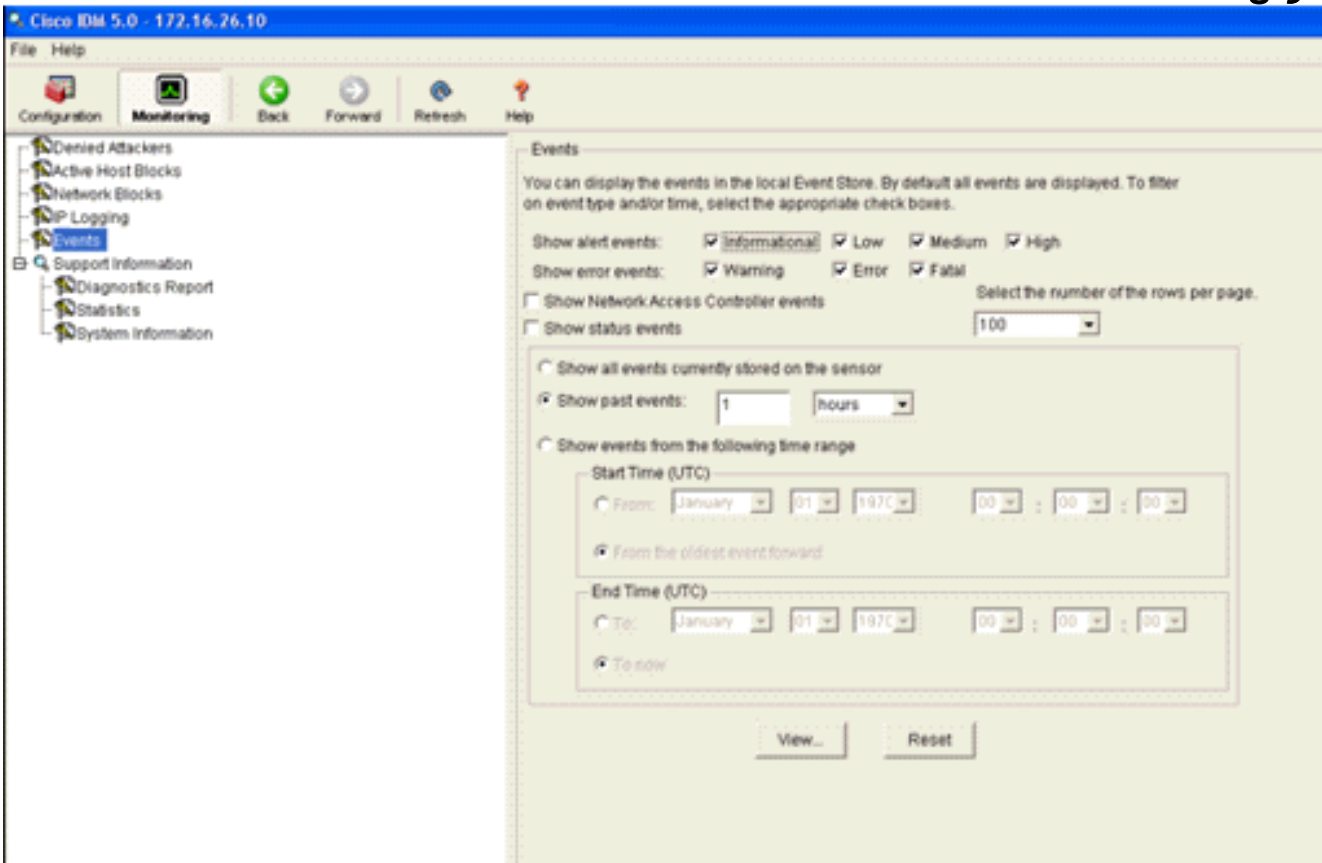
## حظر المراقبة والأحداث باستخدام إدارة البيانات الرقمية

أكمل الخطوات التالية:

1. عندما يتم تشغيل التوقيع بنجاح، هناك مكانين داخل IDM لملاحظة ذلك. تعرض الطريقة الأولى كتل النشطة التي قام AIP-SSM بتثبيتها. انقر فوق مراقبة في الصف العلوي من الإجراءات. ضمن قائمة العناصر التي تظهر على الجانب الأيسر، حدد كتل المضيف النشطة. عندما يتم تشغيل توقيع إختبار الاتصال، تظهر نافذة "كتل المضيف النشطة" عنوان IP الخاص بالمنشئ، وعنوان الجهاز الخاضع للهجوم، والوقت المتبقي الذي يتم تطبيق الكتلة له. وقت الحظر الافتراضي هو 30 دقيقة ويمكن ضبطه. ومع ذلك، لا تتم مناقشة تغيير هذه القيمة في هذا المستند. راجع وثائق تكوين ASA حسب الضرورة للحصول على معلومات حول كيفية تغيير هذه المعلمة. قم بإزالة الكتلة فوراً، ثم حددها من القائمة ثم انقر فوق حذف.



وتستخدم الطريقة الثانية لعرض التوقعات التي تم تشغيلها المخزن المؤقت لحدث AIP-SSM. من صفحة مراقبة IDM، حدد أحداث في قائمة العناصر على الجانب الأيسر. تظهر أداة بحث الأحداث المساعدة. قم بتعيين معايير البحث المناسبة وانقر فوق عرض....



2. ثم يظهر "عارض الأحداث" بقائمة أحداث تطابق المعايير المحددة. قم بالتمرير خلال القائمة والعمود على توقيع

طلب صدى ICMP الذي تم تعديله في خطوات التكوين السابقة. ابحث في عمود "الأحداث" عن اسم التوقيع، أو ابحث عن رقم تعريف التوقيع تحت عمود معرف .Sig

#	Type	Sensor UTC Time	Event ID	Events	Sig ID	Details...
1	error.error	July 31, 2006 2:59:52 PM U...	1145383740954940828	Unable to execute a host block [10.10.99.26] because blocking is not configured		
2	error.warning	July 31, 2006 3:16:51 PM U...	1145383740954941447	while sending a TLS warning alert close_notify, the following error occurred: socket error [3,32]		
3	alert.informati...	July 31, 2006 3:19:16 PM U...	1145383740954941574	ICMP Echo Request	2004	
4	error.error	July 31, 2006 3:19:16 PM U...	1145383740954941577	Unable to execute a host block [10.10.99.26] because blocking is not configured		
5	alert.informati...	July 31, 2006 3:19:46 PM U...	1145383740954941597	ICMP Echo Request	2004	

Refresh

Last Updated: 7/31/06 3:22:39 PM

<Back Next> Close Help

3. بعد أن تقوم بتحديد مكان التوقيع، قم بالنقر المزدوج على الإدخال لفتح نافذة جديدة. يحتوي الإطار الجديد على معلومات تفصيلية حول الحدث الذي قام بتشغيل التوقيع.

```

evIdsAlert: eventId=1145383740954941597 vendor=Cisco severity=informational
originator:
  hostId: sensor
  appName: sensorApp
  appInstanceId: 341
time: July 31, 2006 3:19:46 PM UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Request id=2004 version=S1
  subSigId: 0
interfaceGroup:
vlan: 0
participants:
  attacker:
    addr: 10.10.99.26 locality=OUT
  target:
    addr: 10.10.102.1 locality=OUT
summary: 4 final=true initialAlert=1145383740954941574 summaryType=Regular
alertDetails: Regular Summary: 4 events this interval ;
riskRatingValue: 25
interface: ge0_1
protocol: icmp
  
```

## مراقبة إستثناء العميل في وحدة تحكم لاسلكية

يتم ملء قائمة العملاء المبعدين في وحدة التحكم في هذه النقطة من الوقت باستخدام عنوان IP و MAC الخاص بالمضيف.

The screenshot shows the Cisco Meraki Security page. The left sidebar contains a navigation menu with categories like AAA, Access Control Lists, IPSec Certificates, Web Auth Certificate, Wireless Protection Policies, and Web Login Page. The main content area is titled "CIDS Shun List" and features a "Re-sync" button. Below the button is a table with the following data:

IP Address	Last MAC Address	Expire	Sensor IP / Index
10.10.99.26	00:40:96:ad:06:1b	27	172.16.26.10 / 2

تم إضافة المستخدم إلى قائمة "إستبعاد العميل".

The screenshot shows the Cisco Meraki Monitor page. The left sidebar contains a navigation menu with categories like Summary, Statistics, and Wireless. The main content area is titled "Excluded Clients" and features a search bar labeled "Search by MAC address" with a "Search" button. Below the search bar is a table with the following data:

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Exclusion Reason	Port	
00:40:96:ad:06:1b	AP0014.6940.81ce	00:14:1b:5a:16:40	IPS	802.11a	UnknownEnum:5	29	<a href="#">Detail</a> <a href="#">Link</a> <a href="#">Test</a> <a href="#">Disable</a> <a href="#">Remove</a>

## مراقبة الأحداث في WCS

تتسبب أحداث الأمان التي تؤدي إلى تشغيل كتلة داخل AIP-SSM في قيام وحدة التحكم بإضافة عنوان المخالف إلى قائمة إستبعاد العميل. يتم إنشاء حدث أيضا داخل WCS.

1. أستخدم الأداة المساعدة **Monitor > Alarms** من قائمة WCS الرئيسية لعرض حدث الاستبعاد. تعرض WCS في البداية جميع الإنذارات غير المقطوعة كما تقدم وظيفة بحث على الجانب الأيسر من النافذة.
2. قم بتعديل معايير البحث للعثور على كتلة العميل. تحت مستوى الخطورة، أختَر **ثانوي**، واضبط أيضا فئة التنبيه على **الأمان**.
3. انقر فوق **بحث**.



```

        interface Ethernet0/1
            nameif inside
            security-level 100
ip address 172.16.26.2 255.255.255.0
        !
        interface Ethernet0/2
            shutdown
            no nameif
            no security-level
            no ip address
        !
        interface Management0/0
            nameif management
            security-level 100
ip address 192.168.1.1 255.255.255.0
            management-only
        !
        passwd 2KFQnbNIdI.2KYOU encrypted
            ftp mode passive
        dns server-group DefaultDNS
            domain-name cisco.com
            pager lines 24
        logging asdm informational
            mtu inside 1500
            mtu management 1500
            mtu outside 1500
        asdm image disk0:/asdm512-k8.bin
            no asdm history enable
            arp timeout 14400
            nat-control
                global (outside) 102 interface
nat (inside) 102 172.16.26.0 255.255.255.0
                nat (inside) 102 0.0.0.0 0.0.0.0
            route inside 0.0.0.0 0.0.0.0 172.16.26.1 1
            timeout xlate 3:00:00
        timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
            timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
            timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
            timeout uauth 0:05:00 absolute
            http server enable
            http 10.1.1.12 255.255.255.255 inside
            http 0.0.0.0 0.0.0.0 inside
            http 192.168.1.0 255.255.255.0 management
            no snmp-server location
            no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
            telnet 0.0.0.0 0.0.0.0 inside
            telnet timeout 5
            ssh timeout 5
            console timeout 0
        dhcpd address 192.168.1.2-192.168.1.254 management
            dhcpd lease 3600
            dhcpd ping_timeout 50
            dhcpd enable management
        !
        class-map inside-class
            match any
        !
        !
        policy-map inside-policy
description IDS-inside-policy
            class inside-class
            ips promiscuous fail-open
        !

```



```
service-policy inside-policy interface inside
Cryptochecksum:699d110f988e006f6c5c907473939b29
end :
#ciscoasa
```

## Cisco Intrusion Prevention System Sensor تكوين عينة مستشعر نظام منع الاقتحام Sample

```
sensor#show config
----- !
              (Version 5.0(2 !
Current configuration last modified Tue Jul 25 12:15:19 2006 !
----- !
              service host
              network-settings
host-ip 172.16.26.10/24,172.16.26.1
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
exit
exit
----- !
              service notification
              exit
----- !
service signature-definition sig0
              signatures 2004 0
              engine atomic-ip
event-action produce-alert|request-block-host
exit
              status
              enabled true
exit
exit
exit
----- !
service event-action-rules rules0
              exit
----- !
              service logger
              exit
----- !
              service network-access
              exit
----- !
              service authentication
              exit
----- !
              service web-server
              exit
----- !
              service ssh-known-hosts
              exit
----- !
              service analysis-engine
              virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/1
exit
exit
----- !
              service interface
```

```
exit
----- !
service trusted-certificates
exit
#sensor
```

## التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

## استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

## معلومات ذات صلة

- [تثبيت مدير الجهاز بنظام منع الاقتحام Cisco Intrusion Prevention System Device Manager 5.1](#)
- [أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances - أدلة التكوين](#)
- [تكوين مستشعر نظام منع الاقتحام من Cisco باستخدام واجهة سطر الأوامر 5.0 - تكوين الواجهات](#)
- [دليل التكوين WLC، الإصدار 4.0](#)
- [الدعم الفني اللاسلكي](#)
- [الأسئلة المتداولة حول وحدة التحكم في الشبكة المحلية اللاسلكية \(WLC\)](#)
- [مثال التكوين الأساسي لنقطة الوصول في الوضع Lightweight ووحدة تحكم الشبكة المحلية \(LAN\) اللاسلكية](#)
- [تكوين حلول الأمان](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دق ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل  
ىل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل  
(رفوتم طبارل) ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل