وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية ودليل تكامل IPS

المحتويات

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 مضمن 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 إستخدام 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 التبديل 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 إستخدام 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 إستفادة من حل منع التسلل.
- **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 حلولا 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 متكاملا، 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 Lightweight (LWAPP) 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 المعني.

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 المُحسنة

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

أنظمة Cisco Unified IDS/IPS الأساسية

- أجهزة إستشعار 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 (NM-CIDS 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 المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

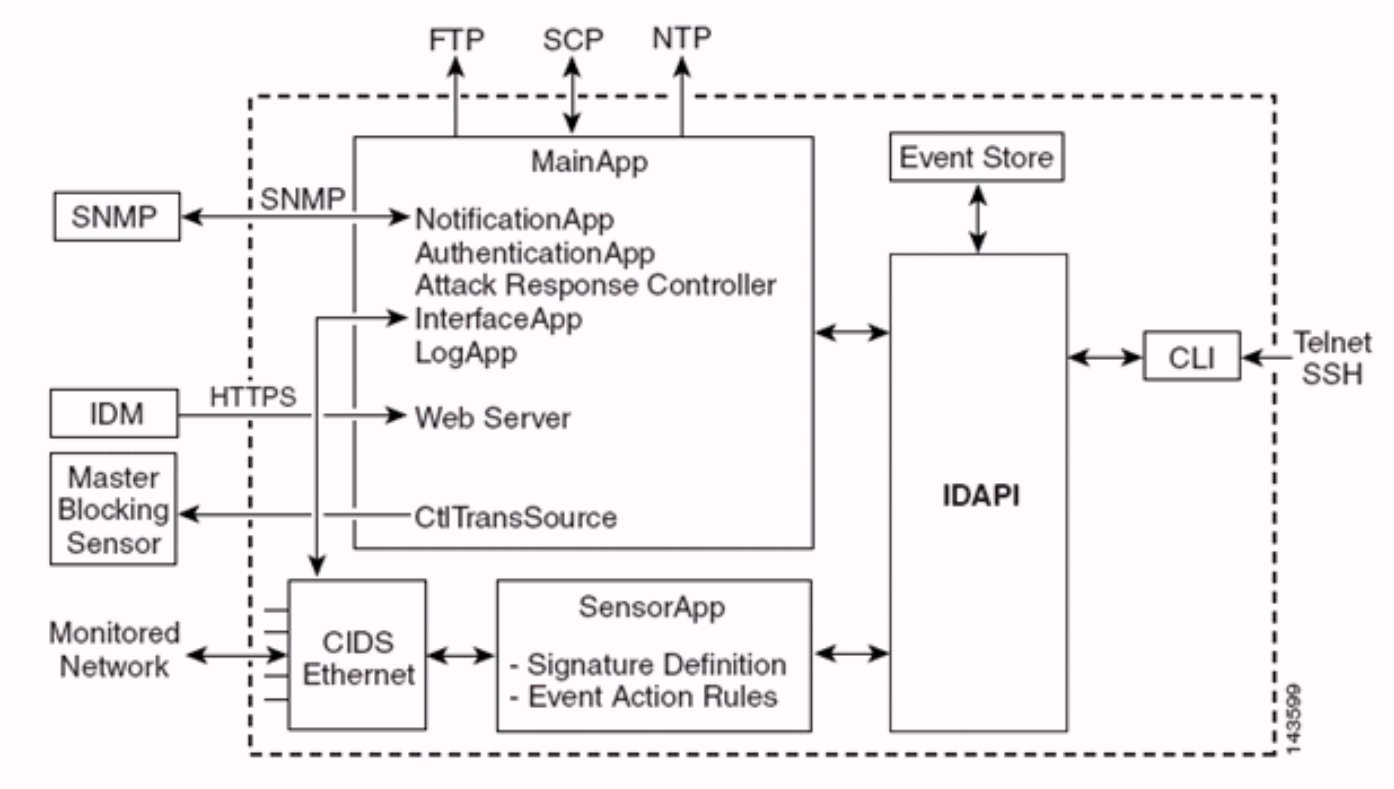
الاصطلاحات

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

نظرة عامة على Cisco IDS

المكونات الرئيسية لمعرفات 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 الترقيات. يحتوي على المكونات التالية:**Control Transaction Server**—يسمح لأجهزة الاستشعار بإرسال حركات التحكم التي يتم إستخدامها لتمكين قدرة مستشعر الحظر الرئيسي لوحدة تحكم إستجابة الهجمات (المعروفة سابقا باسم وحدة تحكم الوصول إلى الشبكة).**مخزن الأحداث** — مخزن مفهرس يستخدم لتخزين أحداث IPS (الأخطاء والحالة ورسائل نظام 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 سابقا 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 الإعلامات**—يرسل إختبارات SNMP عند تشغيلها بواسطة أحداث التنبيه والحالة والخطأ. يستخدم "تطبيق الإعلامات" 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:

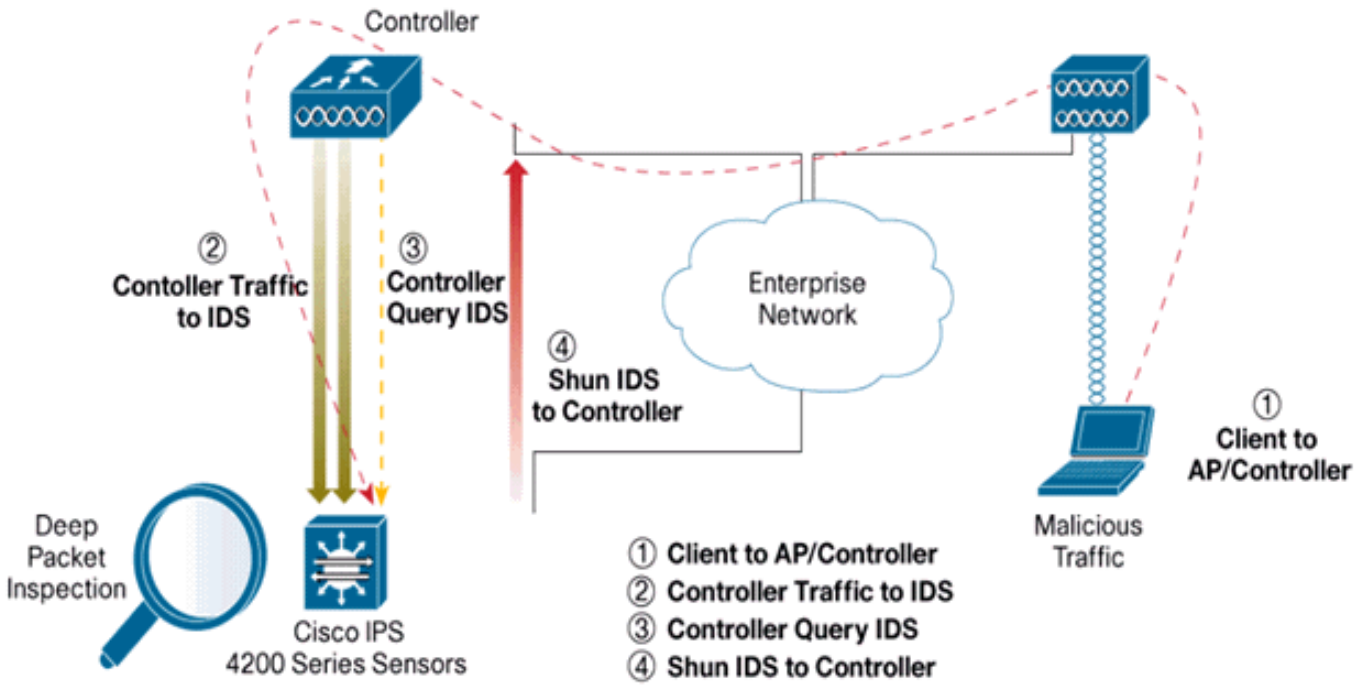
- **قسم التطبيق**—يحتوي على صورة نظام IPS بالكامل.
- **قسم الصيانة** — صورة IPS لأغراض خاصة يتم إستخدامها لإعادة تكوين قسم التطبيق الخاص ب IDSM-2. ينتج عن إعادة صورة لقسم الصيانة إعدادات تكوين مفقودة.
- **قسم الاسترداد** — صورة مخصصة الغرض تستخدم لاسترداد المستشعر. يؤدي التمهيد في قسم الاسترداد إلى تمكين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

Cisco IDS و WLC - نظرة عامة على التكامل

يقدم الإصدار 5.0 من Cisco IDS إمكانية تكوين إجراءات الرفض عند الكشف عن انتهاكات النهج (التوقيعات). 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 لوحدات 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 إستشعار IDS على وحدة تحكم معينة.
- يتم تعريف كل مستشعر IDS تم تكوينه بواسطة عنوان IP الخاص به أو اسم الشبكة المؤهلة وبيانات اعتماد التخويل.
- 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 التنقل 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 لمنح 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 المتجنبين 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 معأق 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.

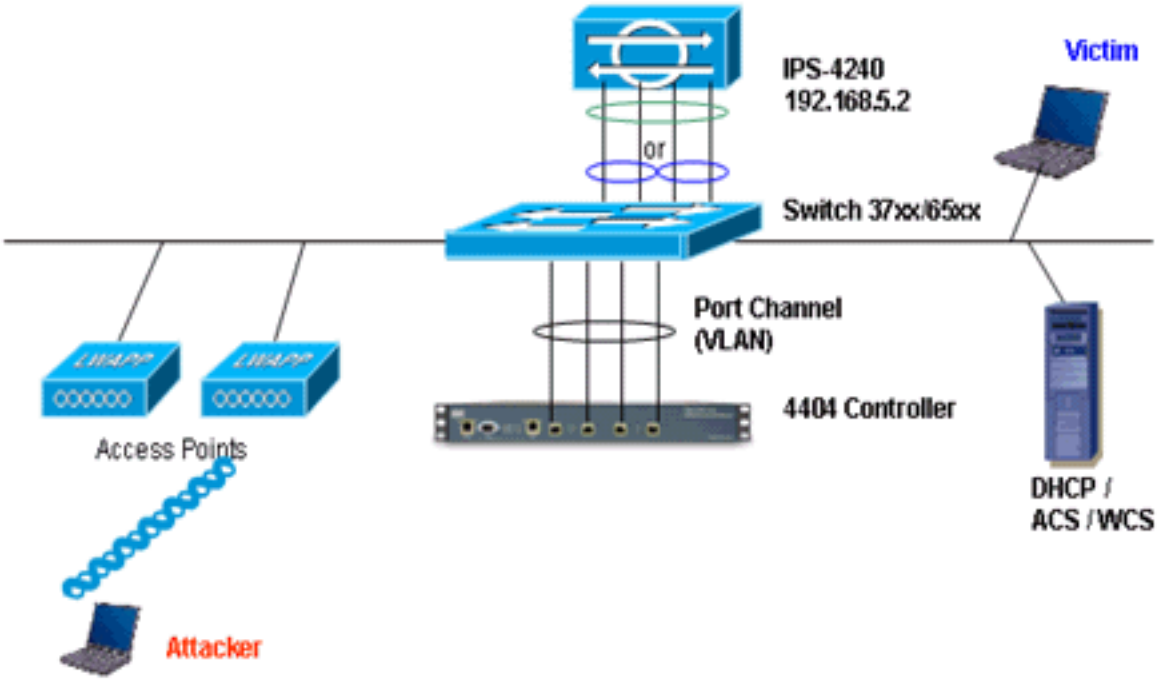
في وحدة التحكم، تظهر صفحة تعطيل العملاء كل عميل تم تعطيله عبر طلب مستشعر IDS. يعرض الأمر CLI **show** أيضا قائمة بالعملاء المدرجة في القائمة السوداء.

في WCS، يتم عرض العملاء المستبعدين تحت علامة التبويب 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 جيجابت وتمكين تجميع 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 تتدفق 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 إستشعار 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 monitore 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 monitore 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

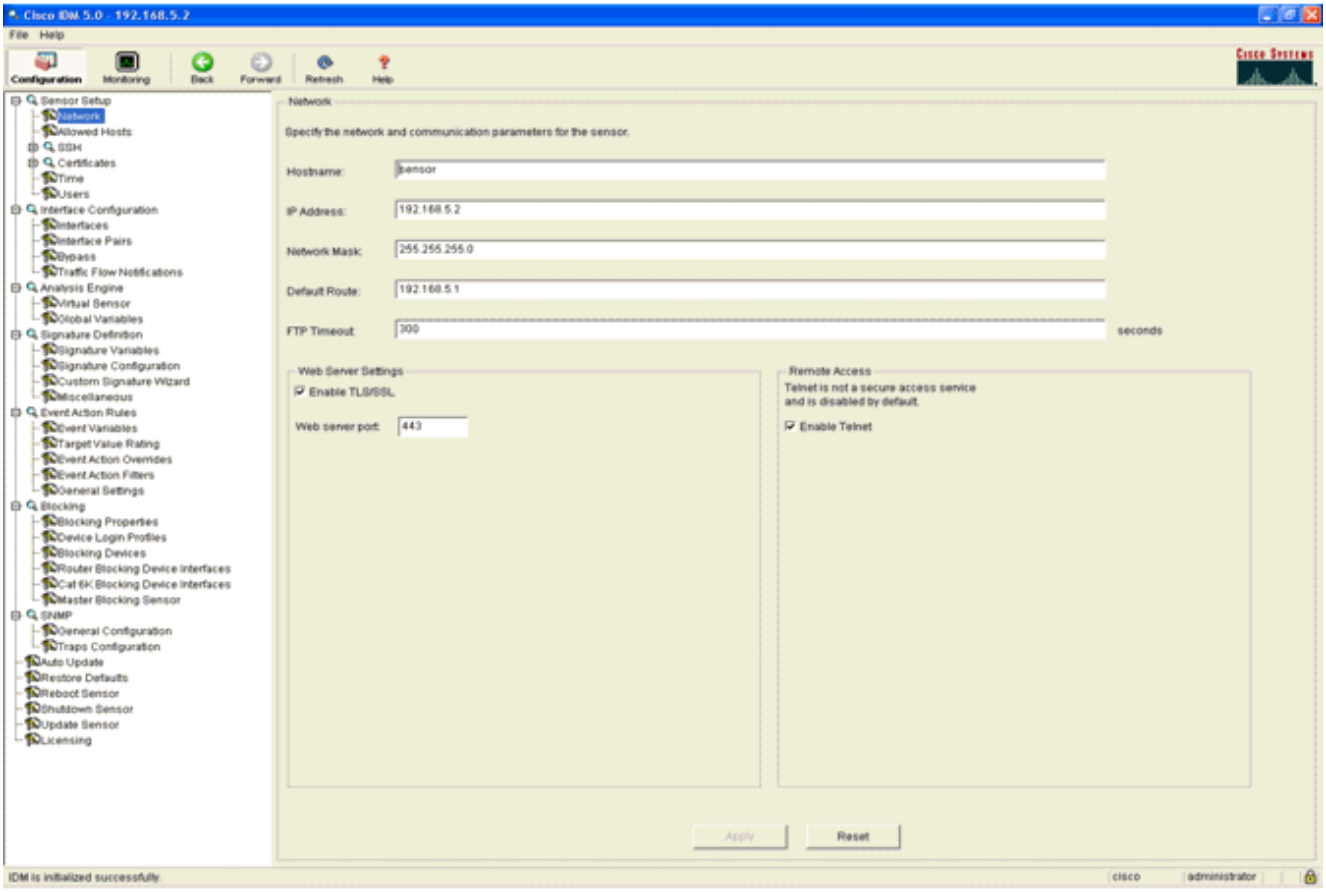
وكلمة كلا cisco. تتم مطالبتك بتغييرها أول مرة تقوم فيها بتسجيل الدخول إلى الجهاز. أنت ينبغي أولا دخلت ال UNIX كلمة، أي يكون cisco. بعد ذلك يجب عليك إدخال كلمة المرور الجديدة مرتين.

```
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
***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
```

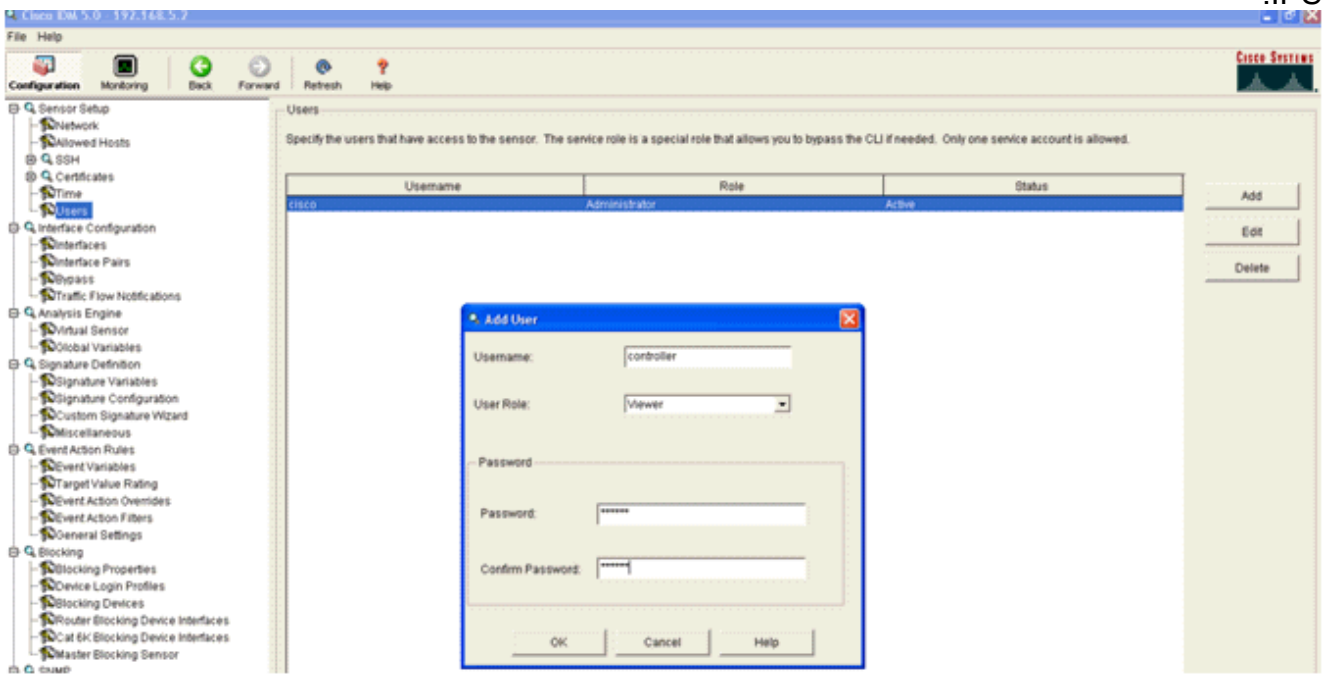
3. قم بتكوين عنوان IP وقناع الشبكة الفرعية وقائمة الوصول على المستشعر.**ملاحظة:** هذه هي واجهة الأمر والتحكم على المعرفات المستخدمة للاتصال بوحدة التحكم. يجب أن يكون هذا العنوان قابلا للتوجيه إلى واجهة إدارة وحدة التحكم. ولا تتطلب واجهات الاستشعار معالجة. يجب أن تتضمن قائمة الوصول عنوان واجهة إدارة وحدة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

```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit
sensor(config-hos)#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
```

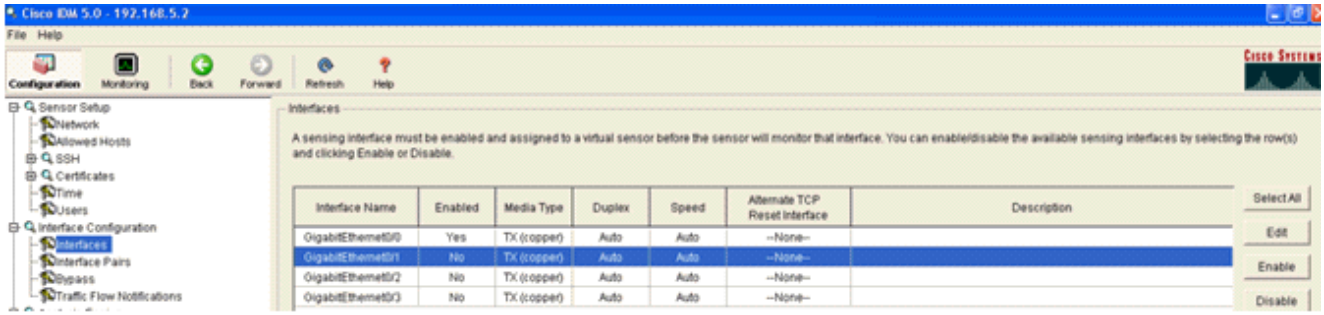
4. أنت يستطيع الآن شكلت ال IPS مستشعر من ال gui. قم بتوجيه المستعرض إلى عنوان IP الخاص بإدارة المستشعر. تعرض هذه الصورة عينة حيث يتم تكوين المستشعر باستخدام 192.168.5.2.



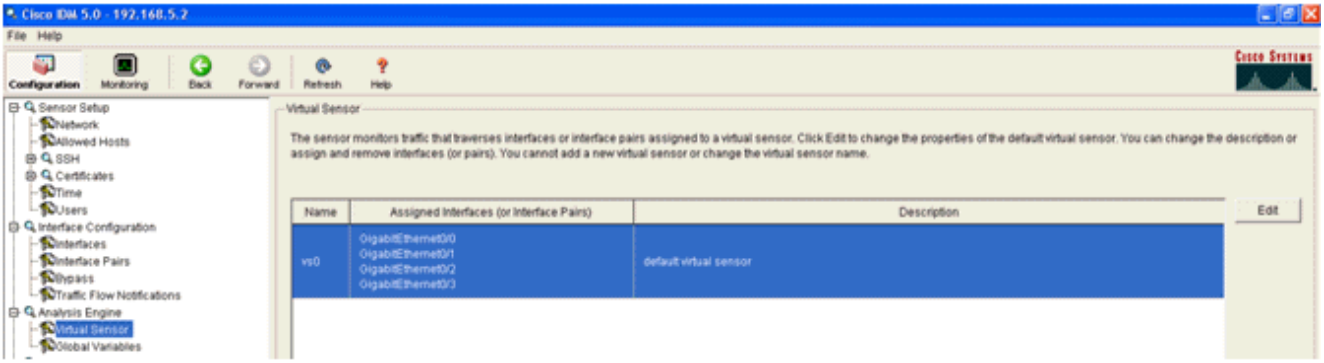
5. إضافة مستخدم يستخدمه عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للوصول إلى أحداث مستشعر IPS.



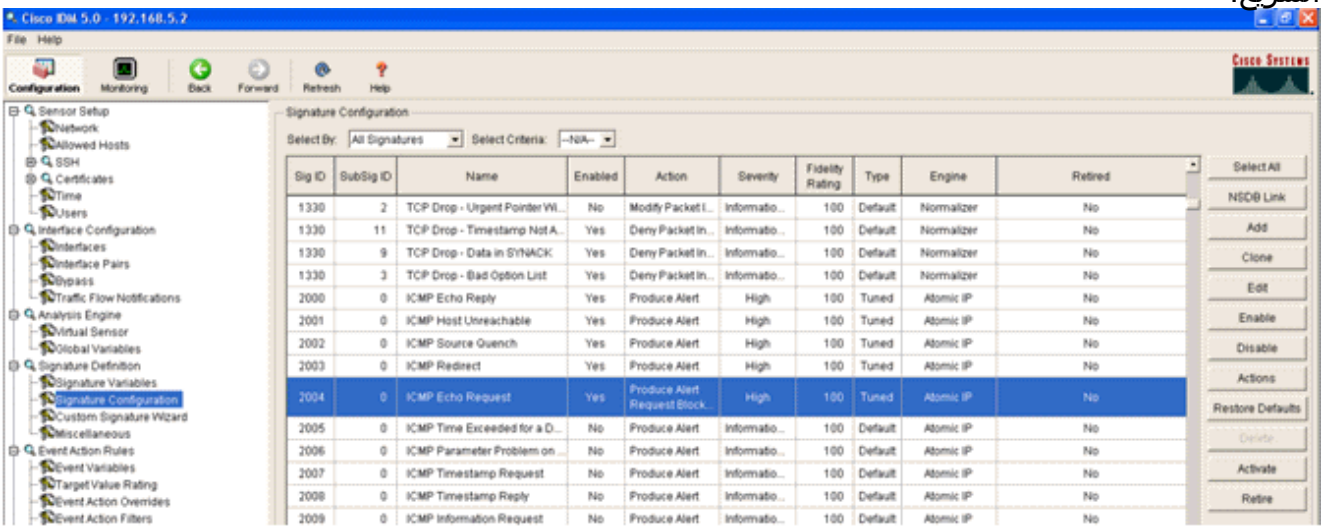
6. قم بتمكين واجهات المراقبة.



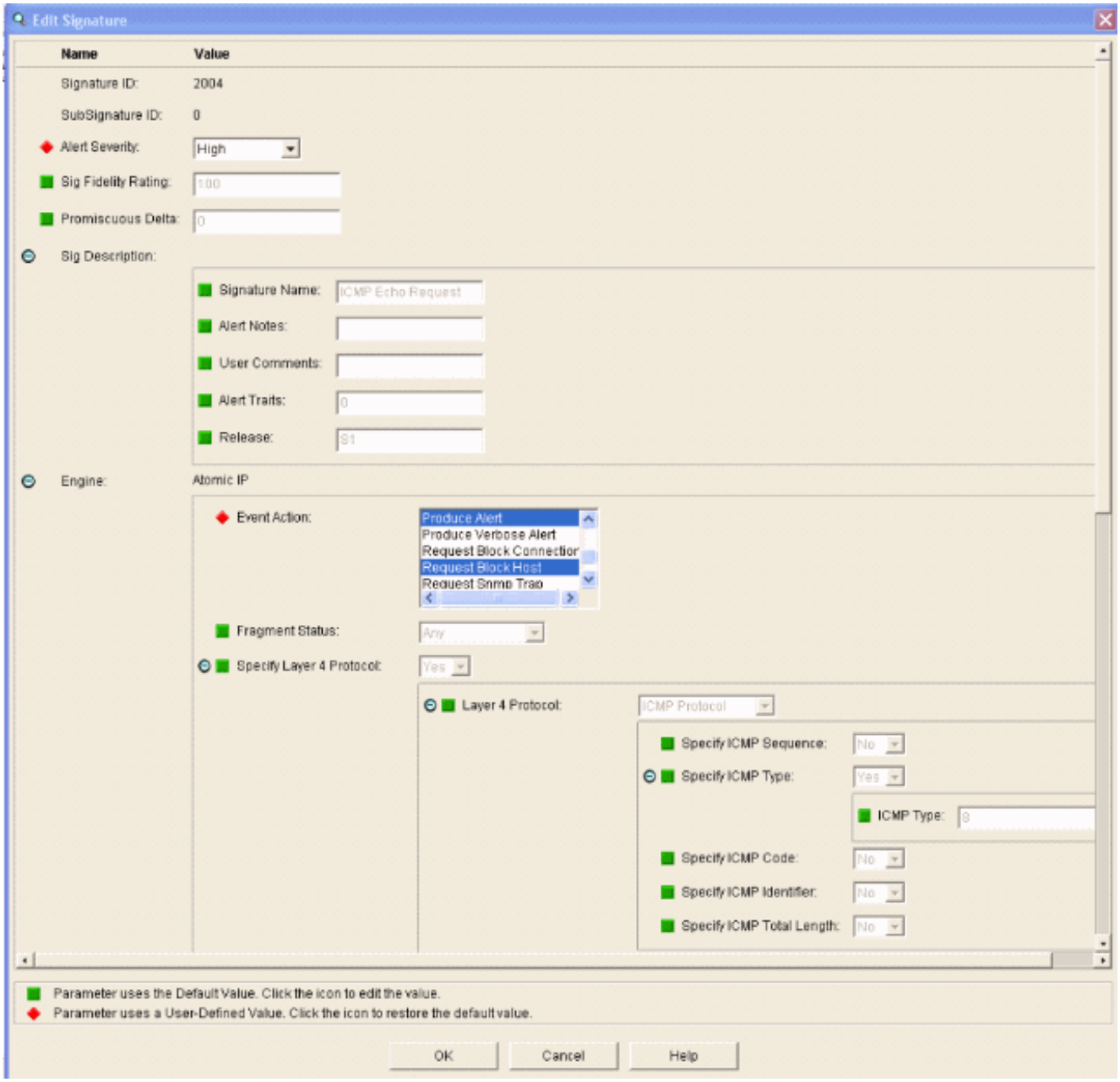
يجب إضافة واجهات المراقبة إلى "محرك التحليل"، كما توضح هذه النافذة:



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** و**مضيف كتلة الطلب** لإتمام خطوة التحقق
هذه.

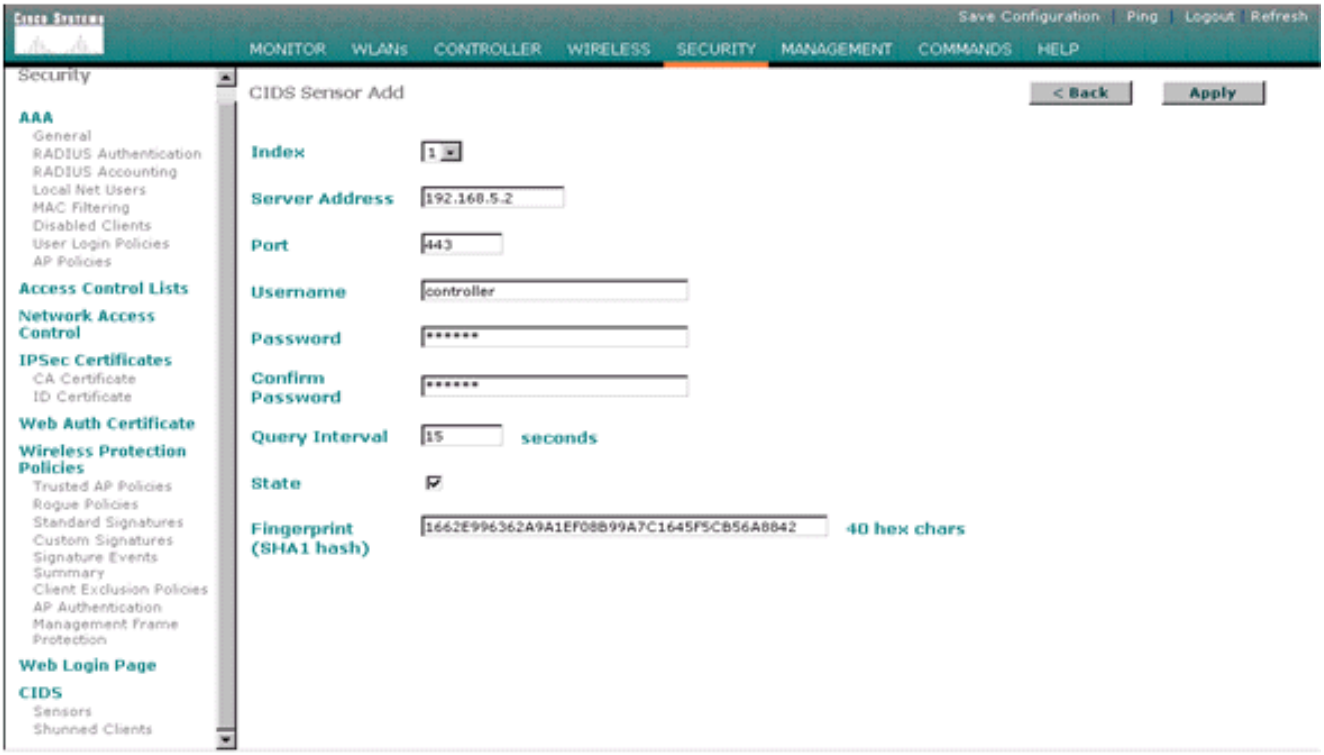


تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

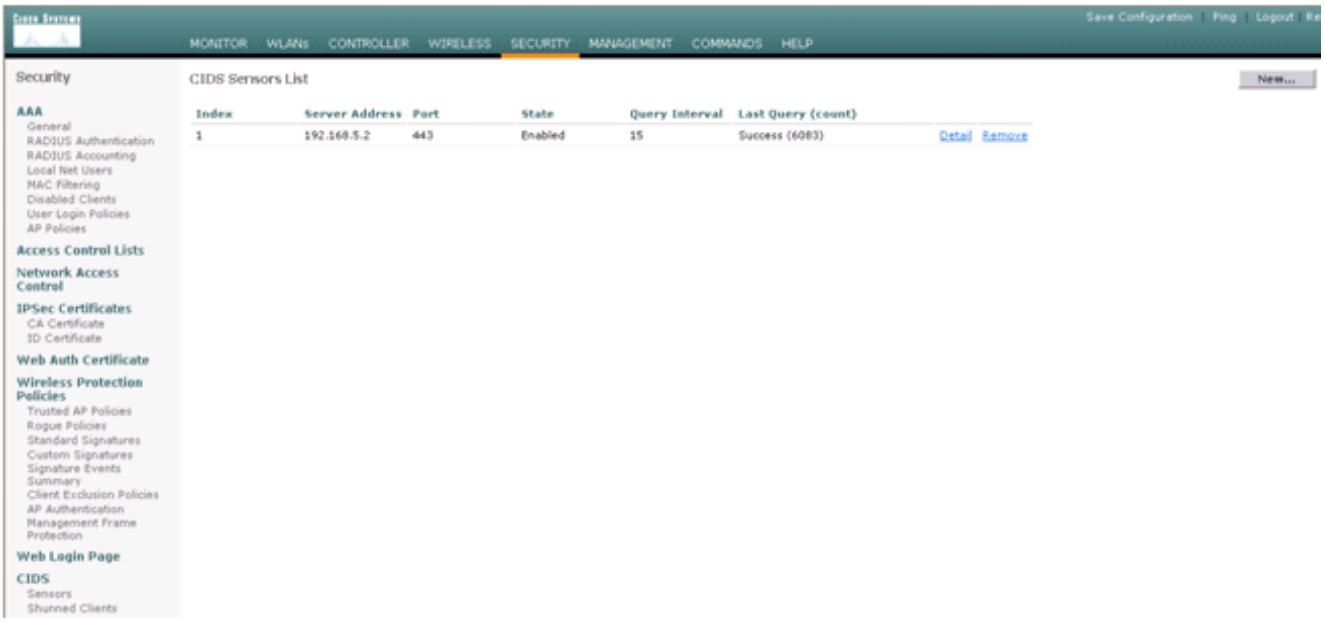
أتمت هذا steps in order to شكلت ال WLC:

1. بمجرد تكوين جهاز IPS واستعداده لإضافة وحدة التحكم، أختر **الأمان > أدوات CIDS > أجهزة الاستشعار > جديد**.
2. قم بإضافة عنوان IP، ورقم منفذ TCP، واسم المستخدم وكلمة المرور التي أنشأتها مسبقا.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.

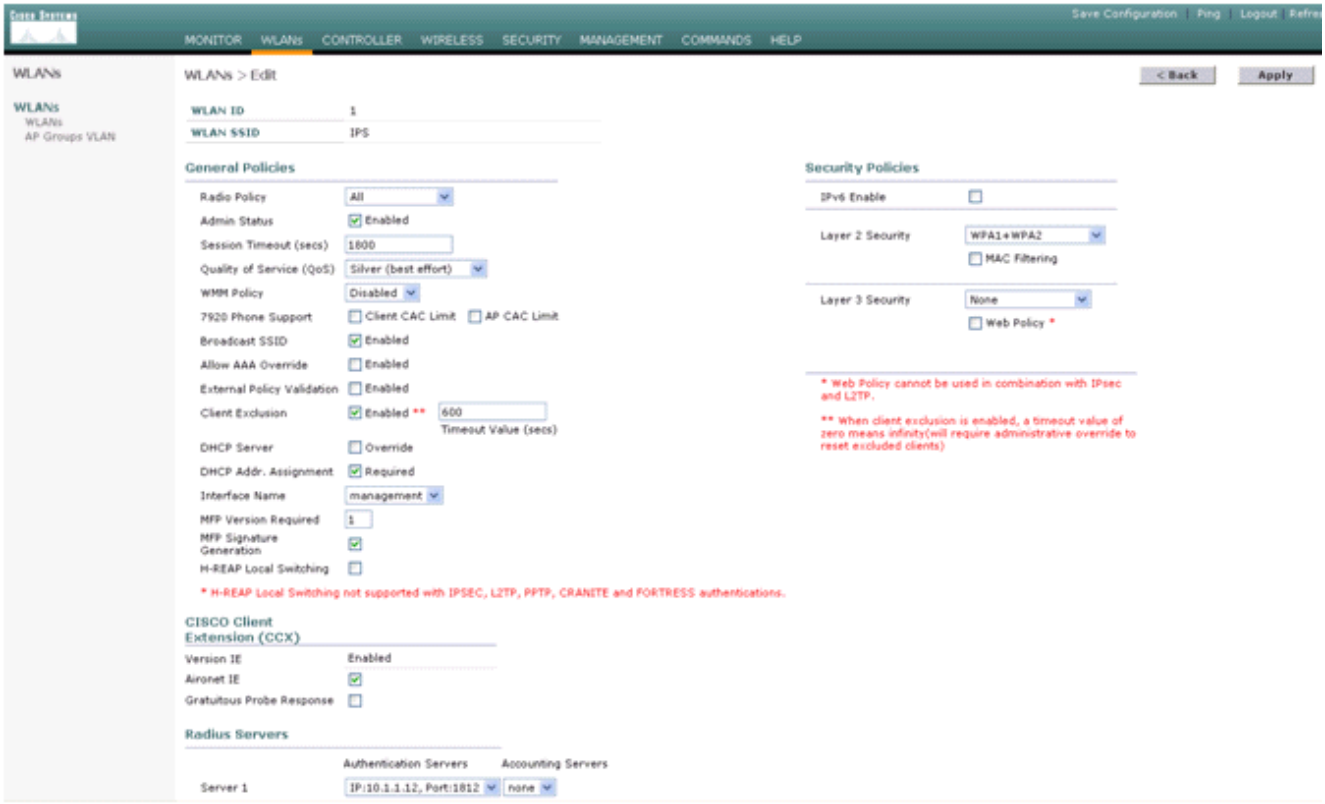
```
sensor#show tls fingerprint
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



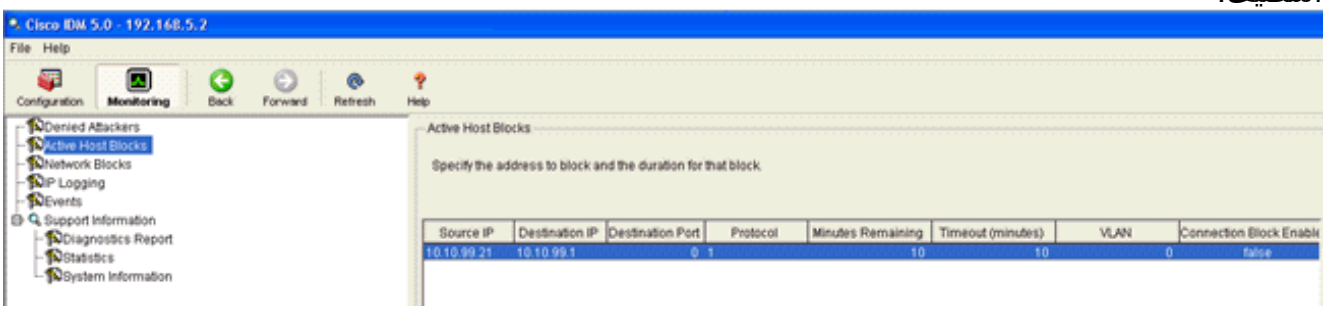
3. تحقق من حالة الاتصال بين مستشعر IPS و WLC.



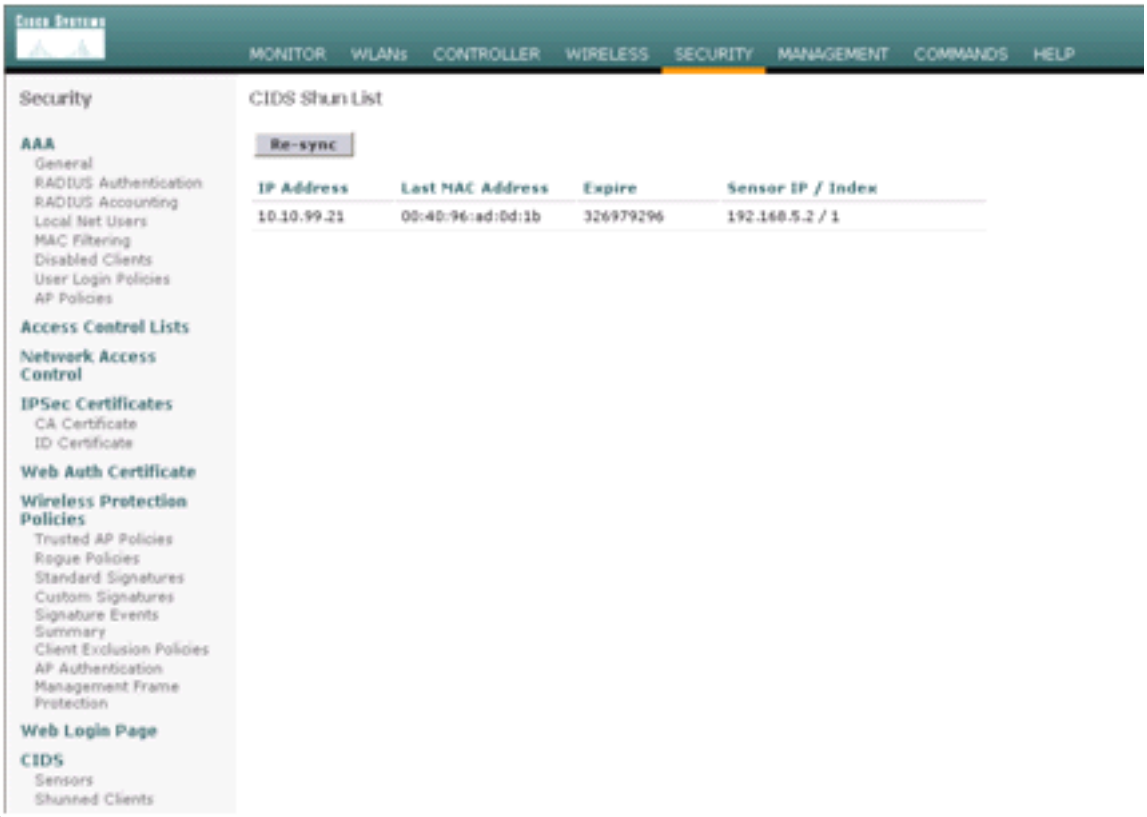
4. بمجرد إنشاء الاتصال باستخدام مستشعر Cisco IPS، تأكد من أن تكوين شبكة WLAN صحيح ومن تمكين **إستثناء العميل**.قيمة مهلة إستثناء العميل الافتراضية هي 60 ثانية. لاحظ أيضا أنه بغض النظر عن مؤقت إستثناء العميل، يستمر إستثناء العميل طالما ظل كتلة العميل التي تم استدعاؤها بواسطة المعرفات نشطا. وقت الحظر الافتراضي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



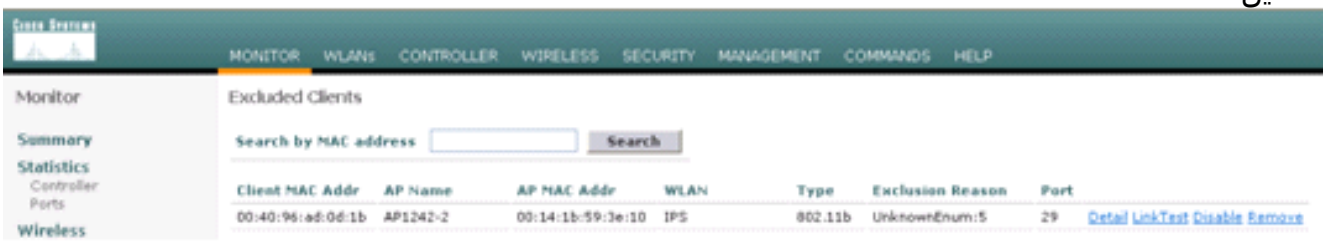
5. يمكنك تشغيل حدث في نظام Cisco IPS إما عند إجراء مسح NMAP لأجهزة معينة في الشبكة أو عند إجراء إختبار اتصال لبعض الأجهزة المضيفة التي تتم مراقبتها بواسطة مستشعر Cisco IPS. بمجرد تشغيل الإنذار في Cisco IPS، انتقل إلى **المراقبة وحواجز المضيف النشطة** للتحقق من تفاصيل حول المضيف.



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

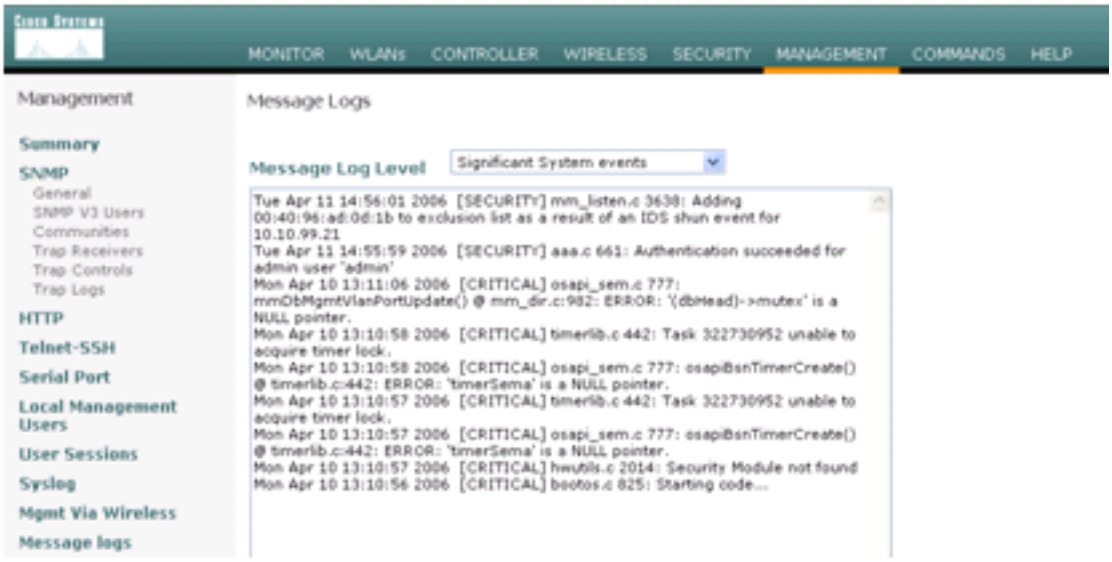


تتم بالمضيف.
إضافة المستخدم إلى قائمة "إستبعاد العميل".



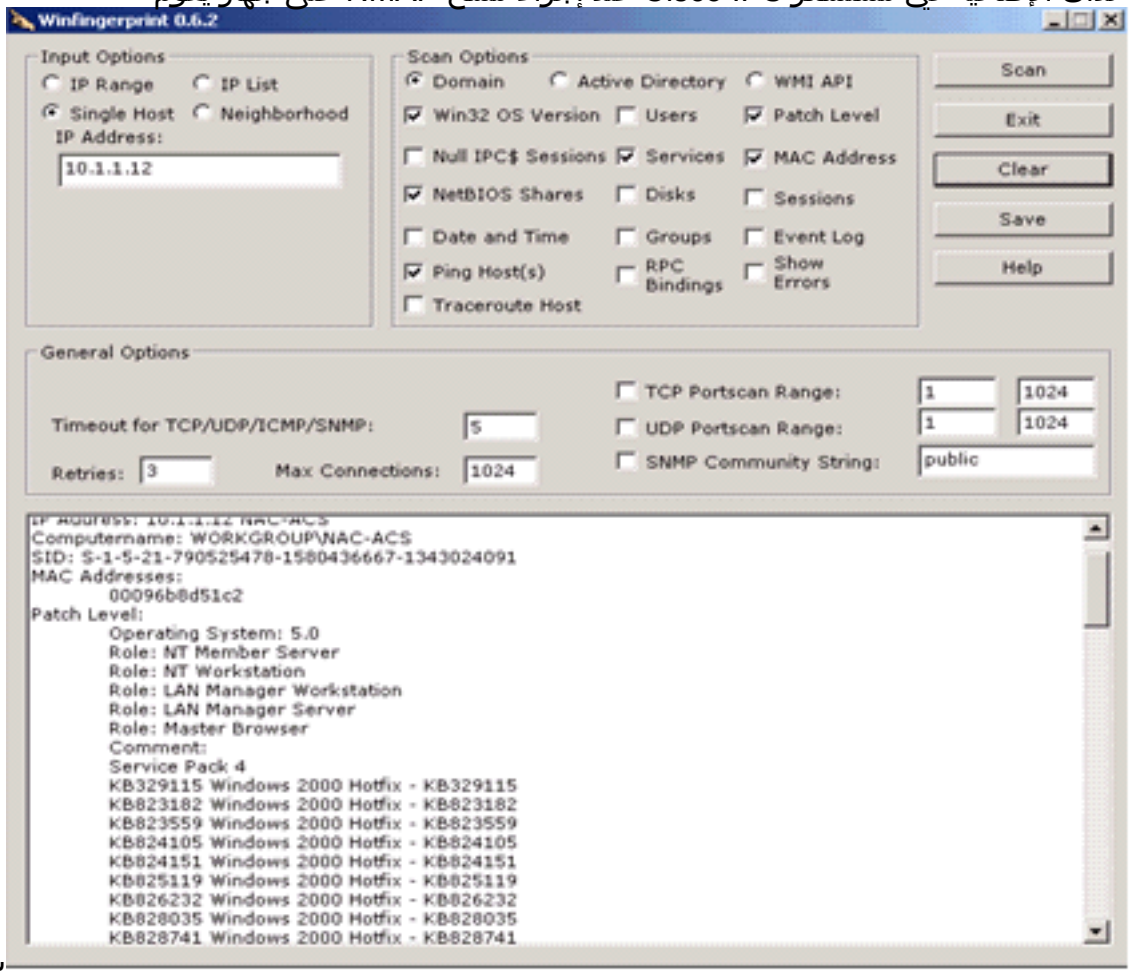
يتم إنشاء سجل ملائمة أثناء إضافة عميل إلى قائمة التجاهل.

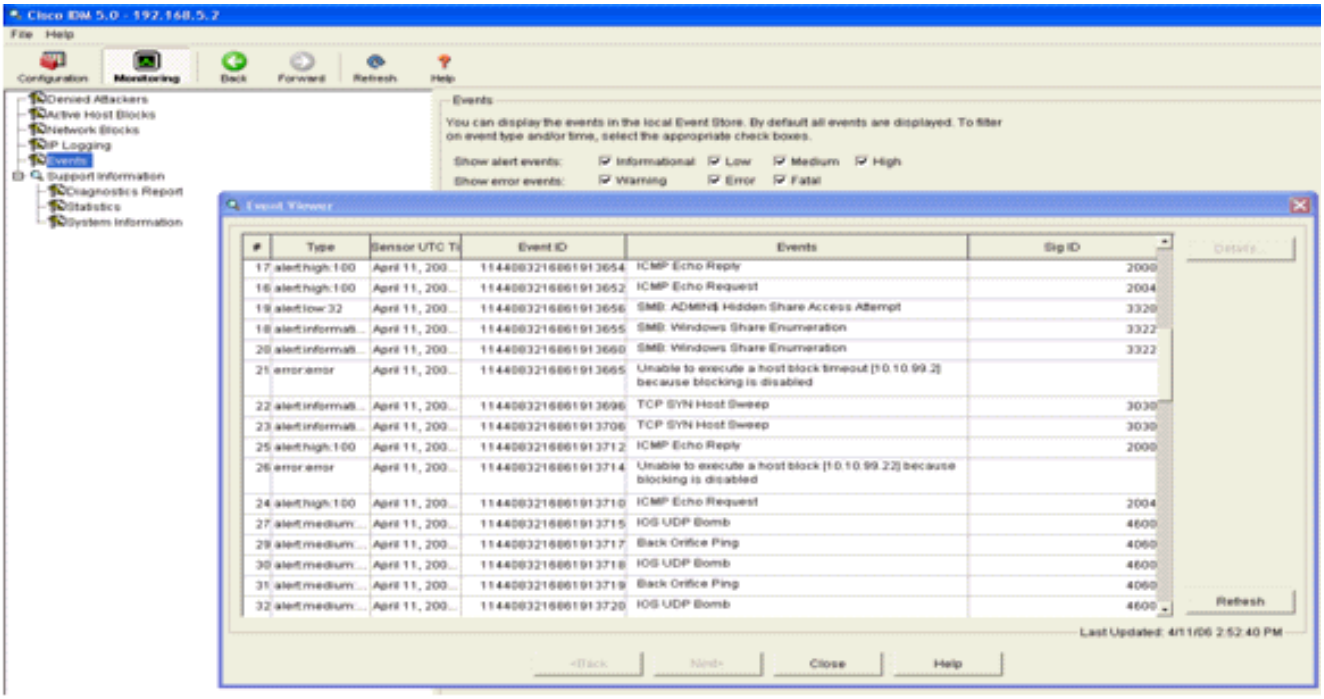
يتم أيضا إنشاء سجل رسائل



يتم إنشاء للحدث.

بعض الأحداث الإضافية في مستشعر Cisco IPS عند إجراء مسح NMAP على جهاز يقوم بمراقبته. يبدي هذا نافذة أحداث ولدت في ال cisco ips مستشعر.





تكوين عينة مستشعر Cisco IDS

هذا هو المخرج من البرنامج النصي للإعداد من التثبيت:

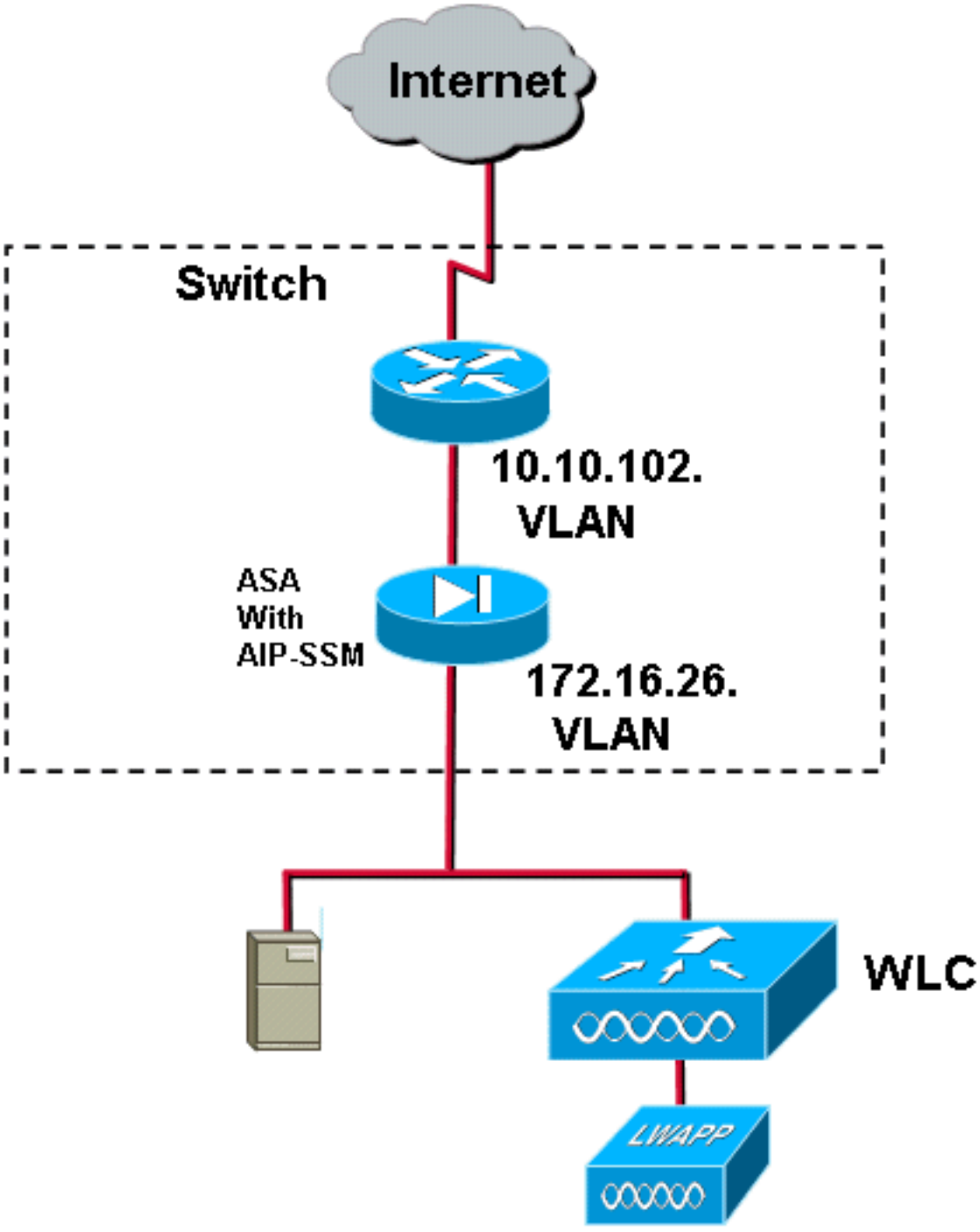
```
sensor#show config
------------------------------ !
(Version 5.0(2 !
Current configuration last modified Mon Apr 03 15:32:07 2006 !
------------------------------ !
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 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

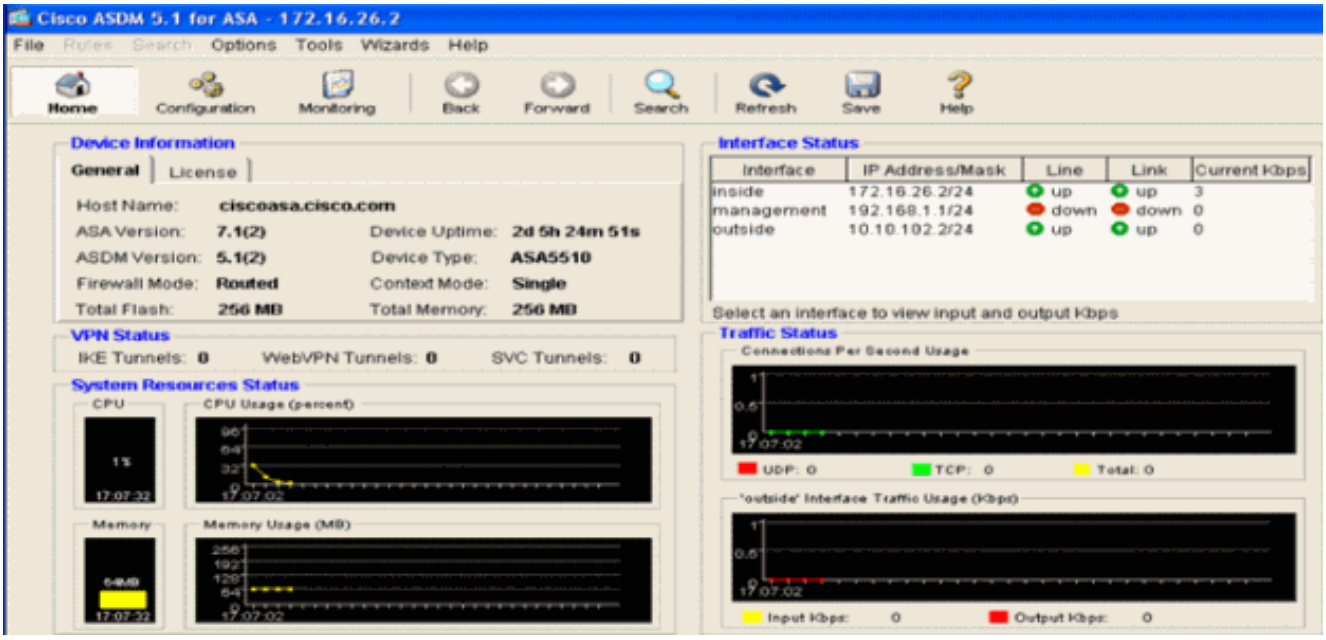
وعلى عكس مستشعر اكتشاف الاقتحام التقليدي، يجب أن يكون ASA دائما في مسار البيانات. ،in other words instead of يجسر حركة مرور من مفتاح ميناء إلى خامل ينشق ميناء على المستشعر، ال ASA ينبغي إستلمت

معطيات على واحد قارن، عملية هو داخليا، وبعد ذلك أرسلت هو خارج آخر ميناء. بالنسبة للمعرفات، أستخدم إطار السياسة النمطية (MPF) لنسخ حركة مرور البيانات التي يستلمها ASA إلى وحدة خدمات الأمان والفحص والمنع المتقدم الداخلية (AIP-SSM) للفحص.

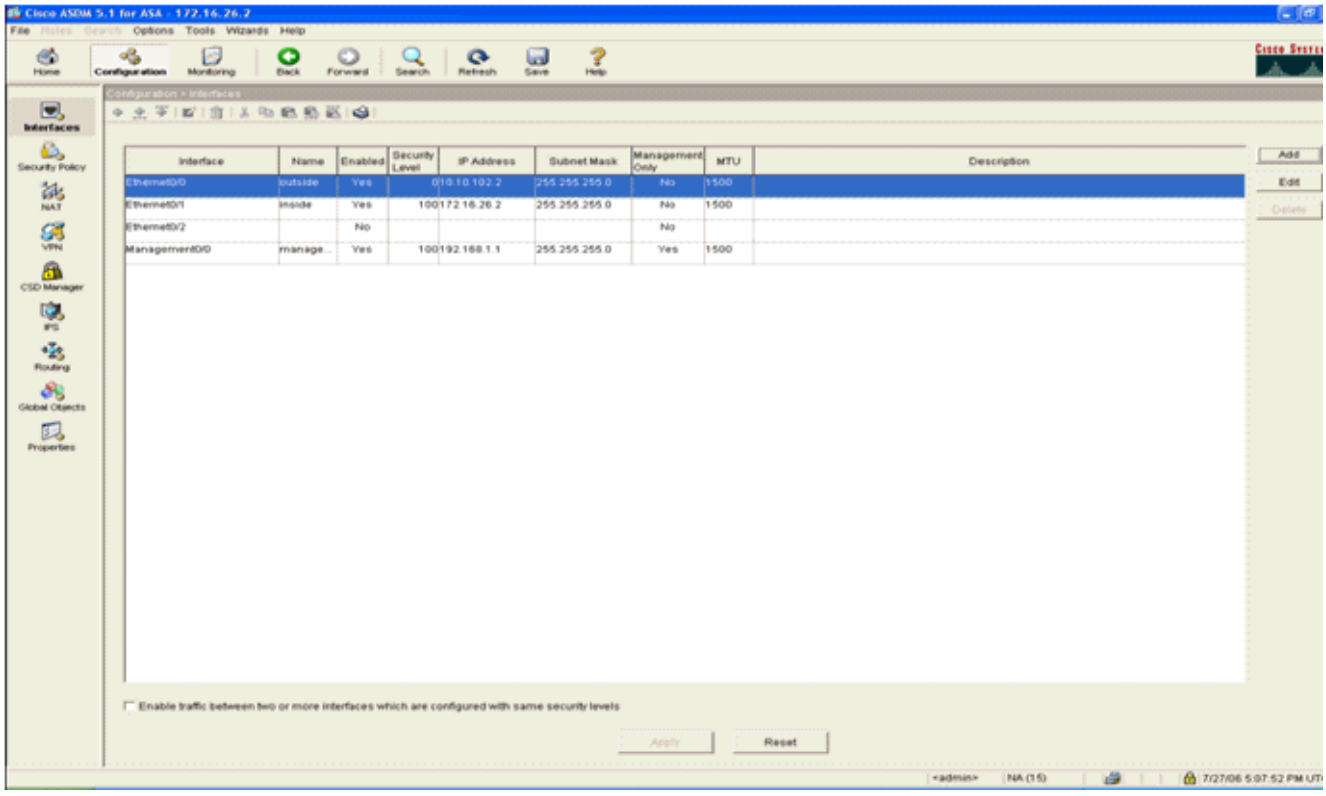


في هذا مثال، ال ASA يستعمل بالفعل setup ويمرر حركة مرور. توضح هذه الخطوات كيفية إنشاء سياسة ترسل البيانات إلى AIP-SSM.

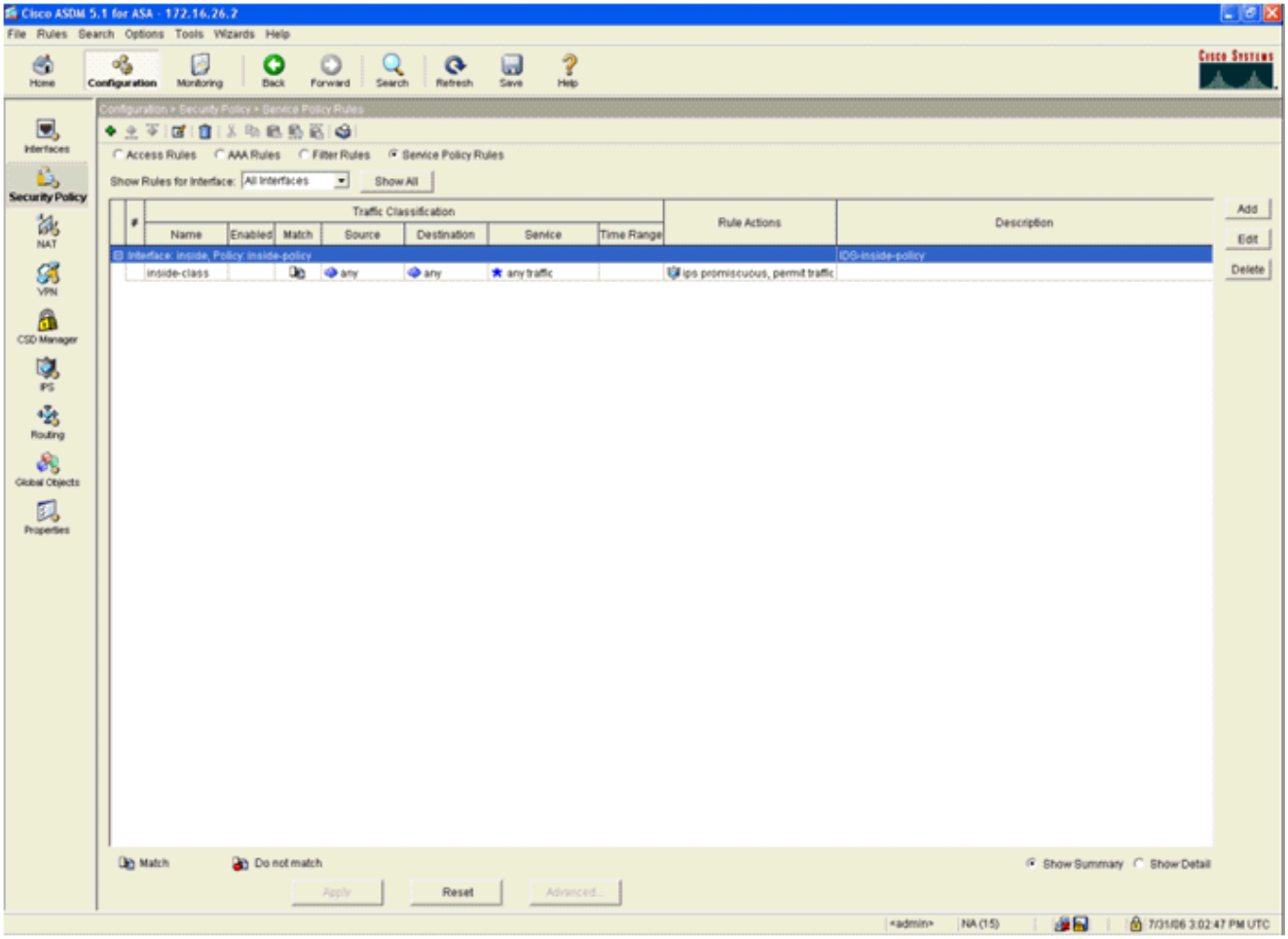
1. قم بتسجيل الدخول إلى ASA باستخدام ASDM. تظهر نافذة نظام ASA الرئيسي عند تسجيل الدخول الناجح.



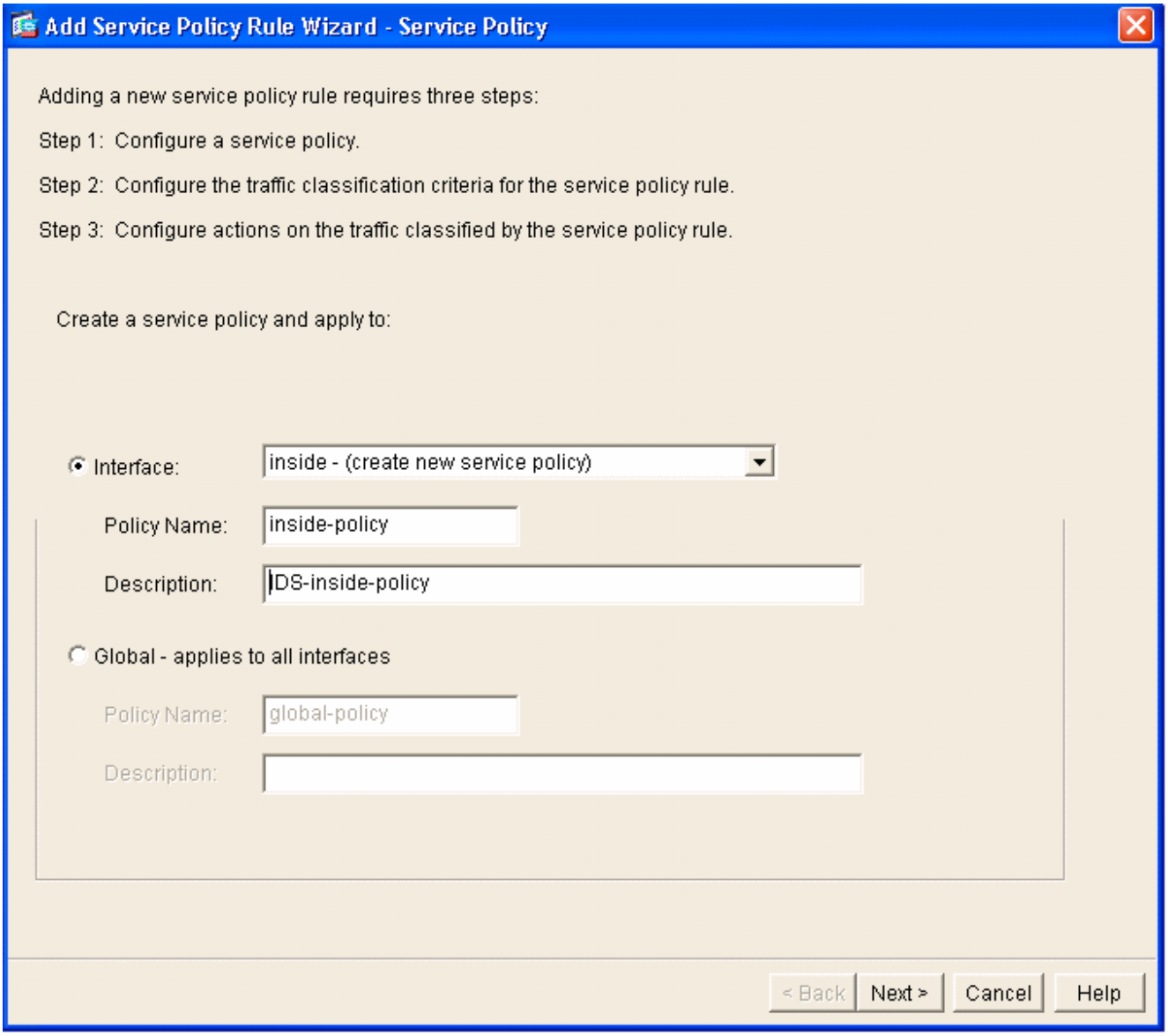
2. انقر فوق **تكوين** في أعلى الصفحة. تبديل النافذة إلى طريقة عرض واجهات ASA.



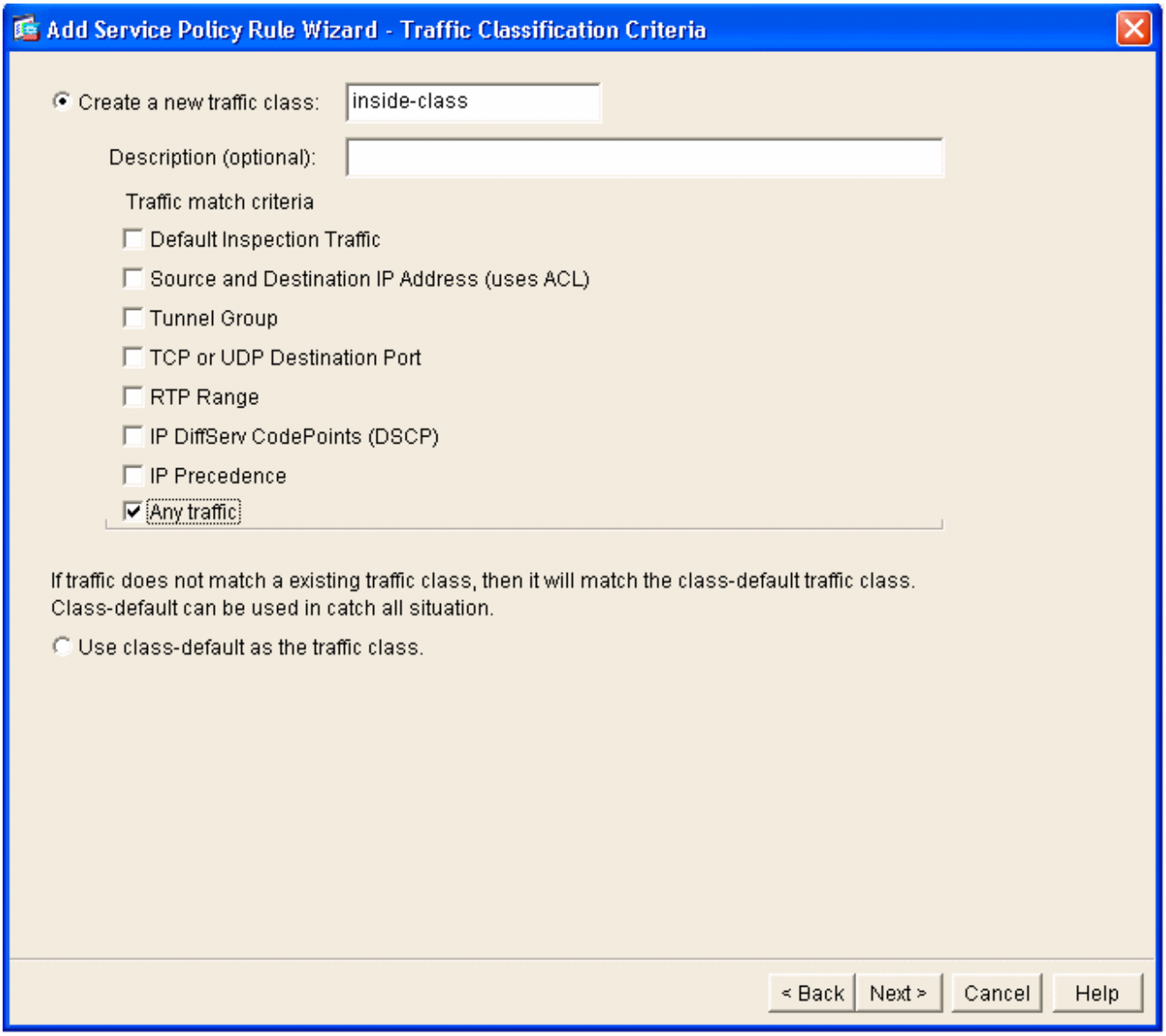
3. انقر فوق **نهج الأمان** في الجانب الأيسر من الإطار. في الإطار الناتج، أختر علامة التبويب **قواعد سياسة الخدمة**.



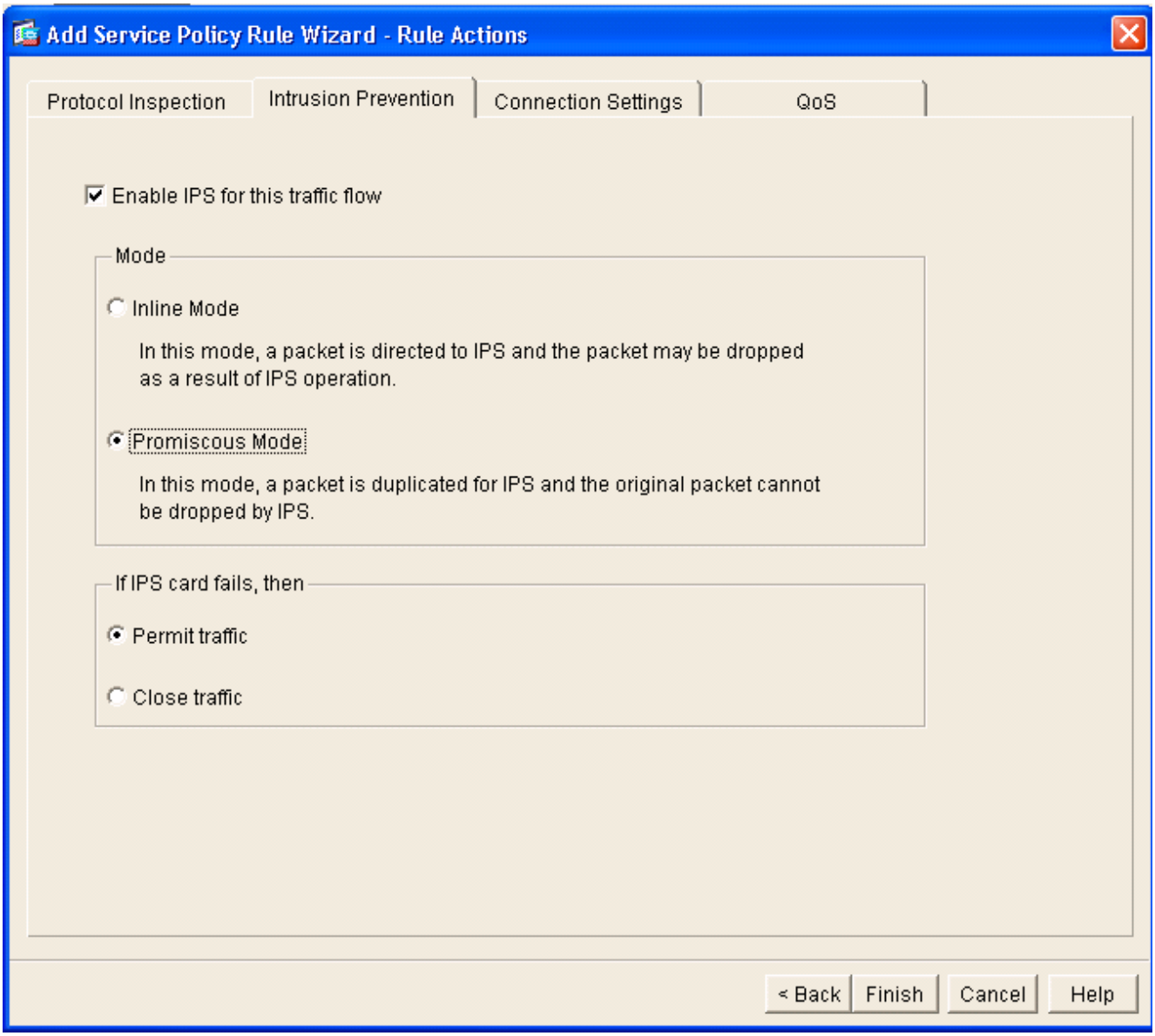
4. انقر فوق **إضافة** لإنشاء سياسة جديدة. يتم تشغيل "معالج إضافة قاعدة سياسة الخدمة" في نافذة جديدة.انقر فوق **الواجهة** ثم أختر الواجهة الصحيحة من القائمة المنسدلة لإنشاء سياسة جديدة مرتبطة بإحدى الواجهات التي تمرر حركة مرور البيانات.قم بتسمية النهج ووصف ما تقوم به السياسة باستخدام مربعي النص.طقطقت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



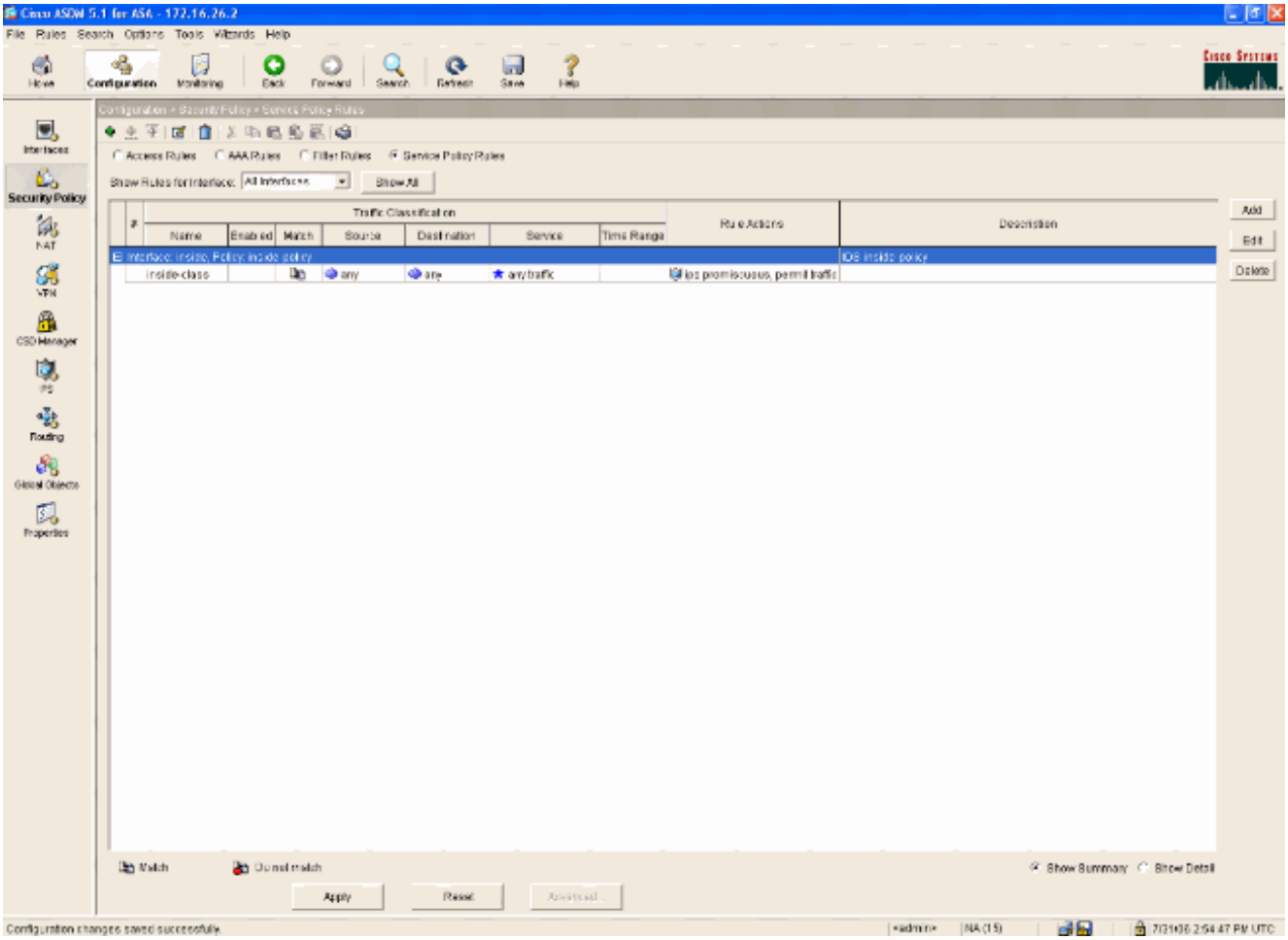
5. قم بإنشاء فئة حركة مرور جديدة لتطبيقها على السياسة.من المنطقي إنشاء فئات معينة للتحقق من أنواع بيانات معينة، ولكن في هذا المثال، يتم تحديد أي حركة مرور للتبسيط. طقطقت **بعد ذلك** in order to باشرت.



6. أتمت هذا steps in order toتوجيه ASA لتوجيه حركة المرور إلى AIP-SSM الخاص به.تحقق من **تمكين IPS لتدفق حركة المرور هذا** لتمكين اكتشاف التسلل.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.



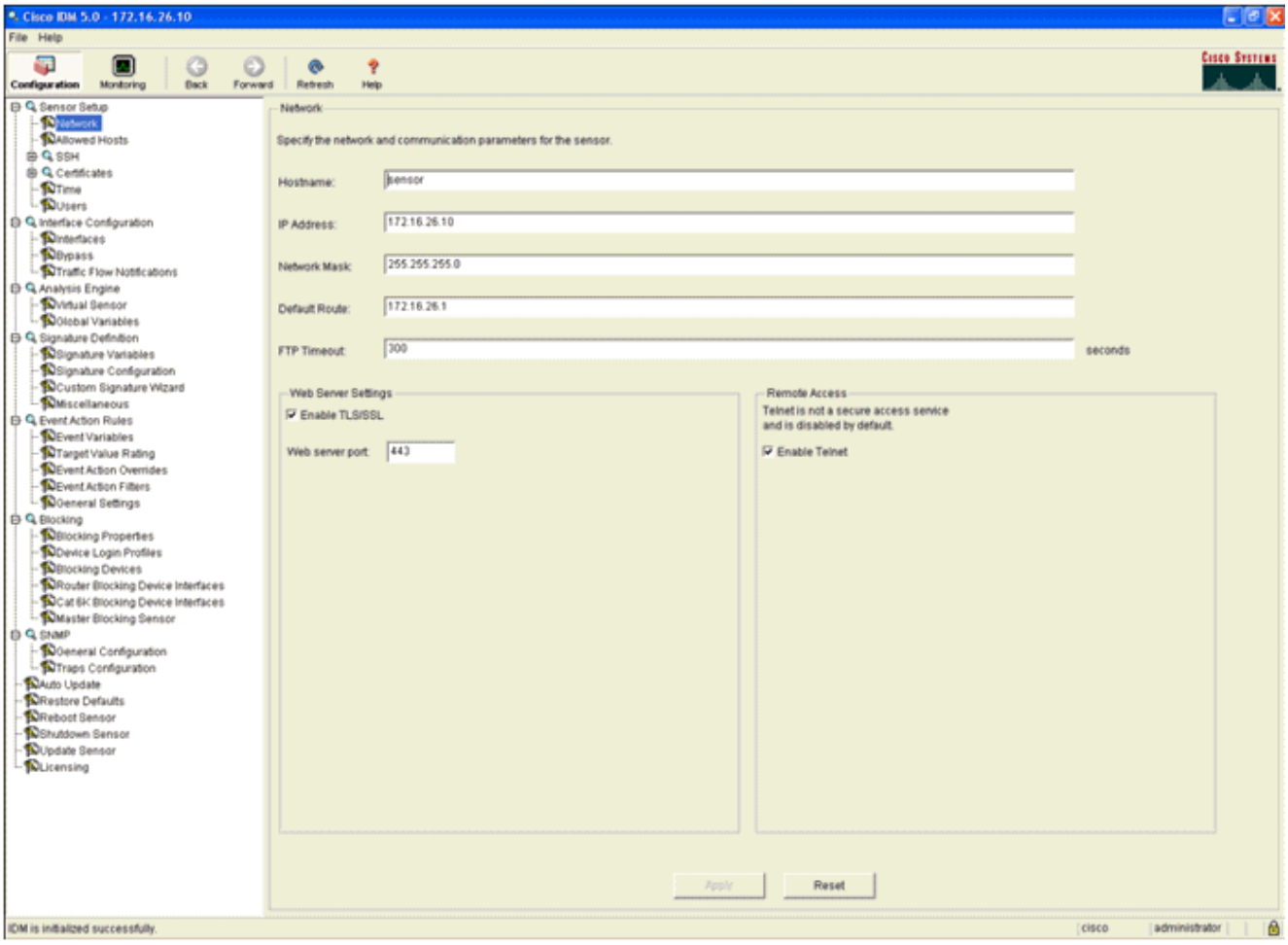
7. تم تكوين ASA الآن لإرسال حركة مرور البيانات إلى وحدة IPS النمطية. طقطقة **حفظ** في الصف الأعلى in order to كتبت التغييرات إلى ال ASA.



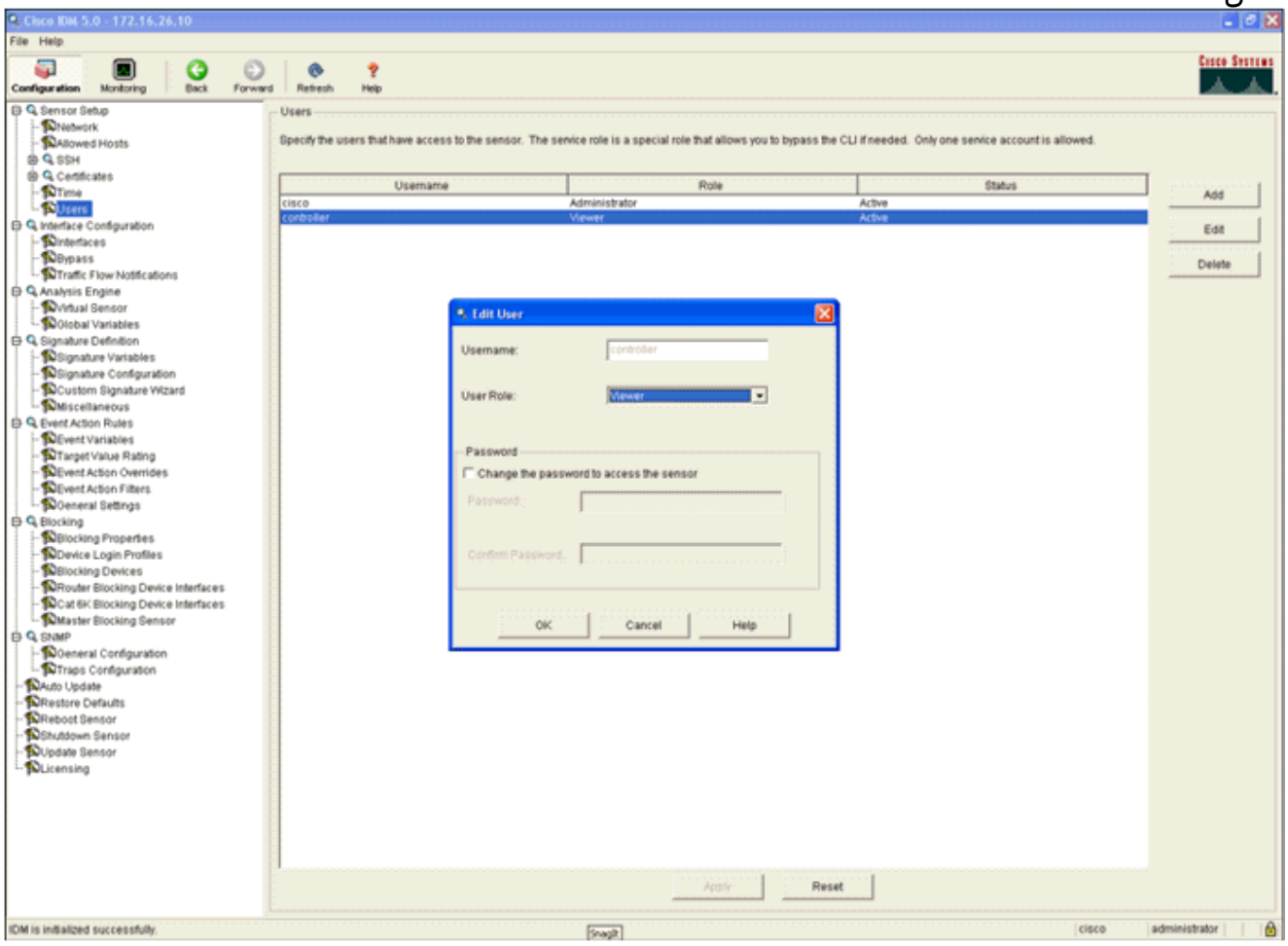
شكلت AIP-SSM ل حركة مرور تفتيش

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

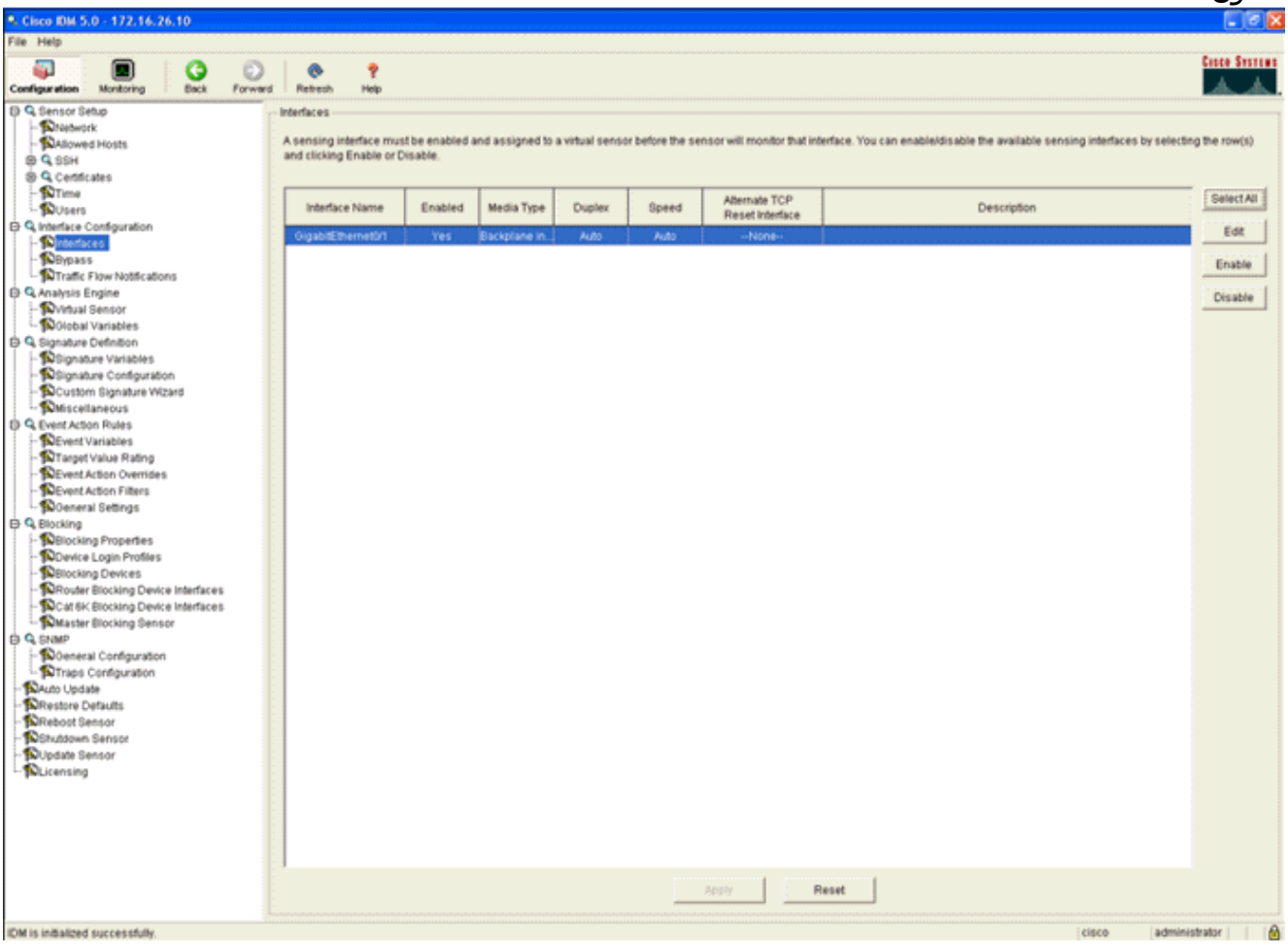
1. قم بتسجيل الدخول إلى AIP-SSM باستخدام IDM.



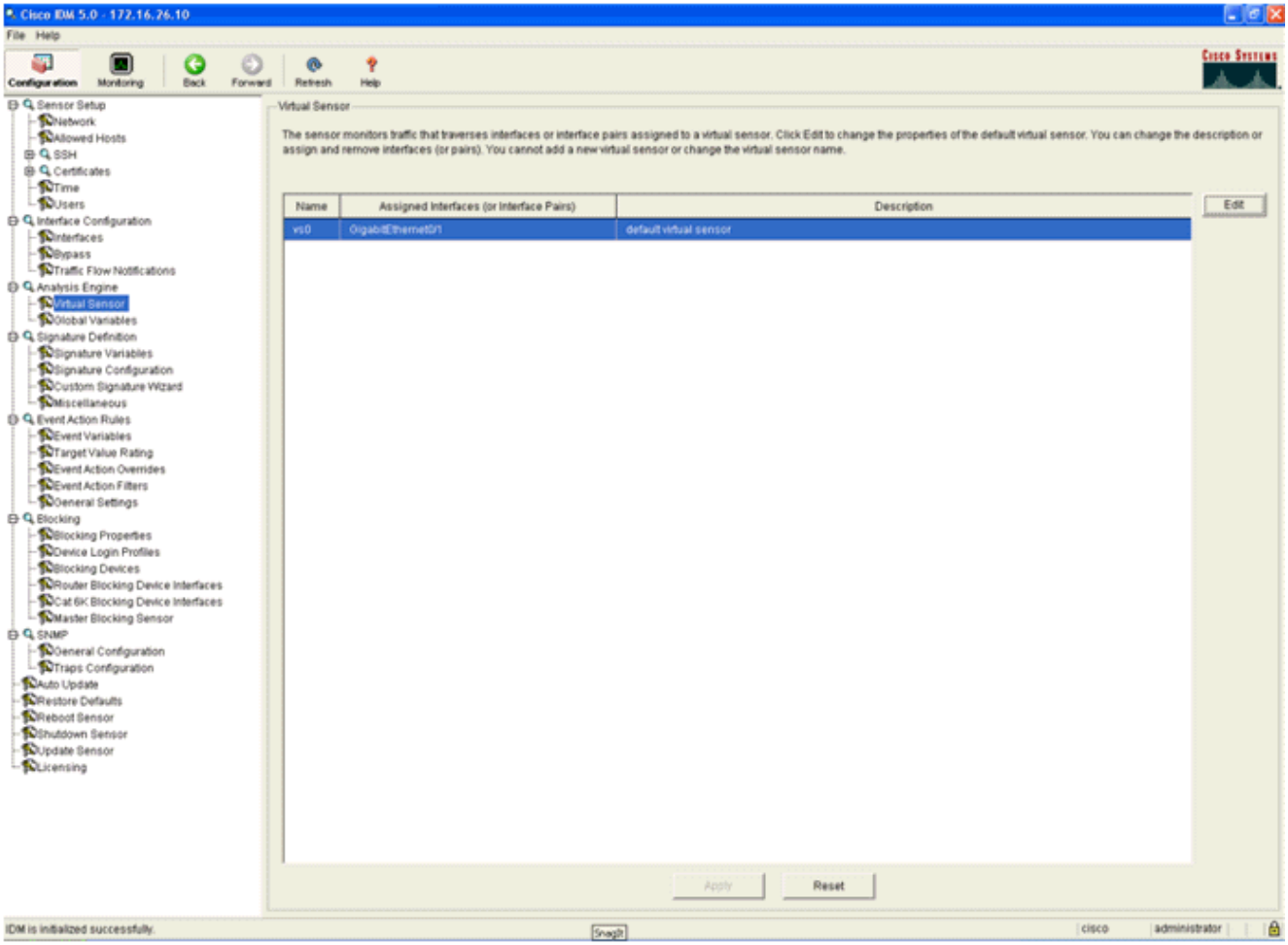
2. إضافة مستخدم بامتيازات عارض على الأقل.



3. مكنت
القارن.



4. تحقق من تكوين المستشعر
الظاهري.

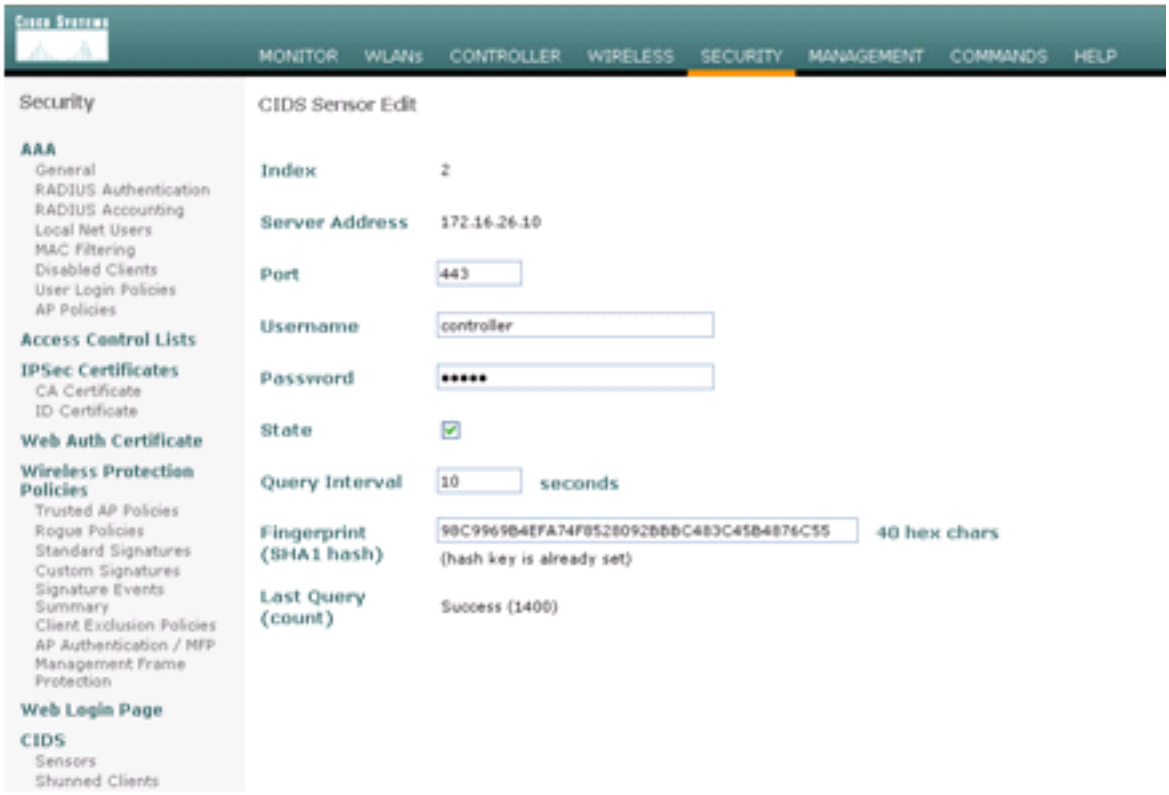


تكوين WLC لاستطلاع AIP-SSM لكتل العميل

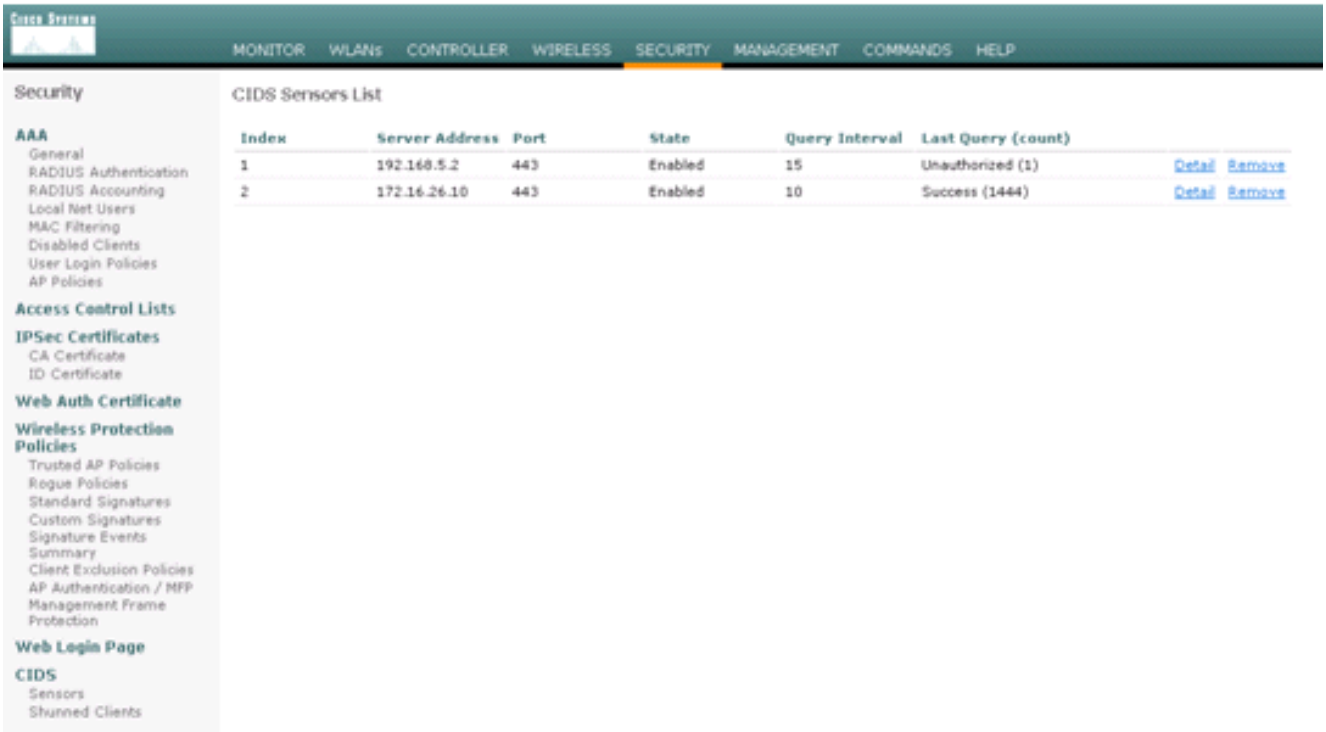
أكمل الخطوات التالية بمجرد تكوين "المستشعر" واستعداده لإضافته في وحدة التحكم:

1. أختر **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
```



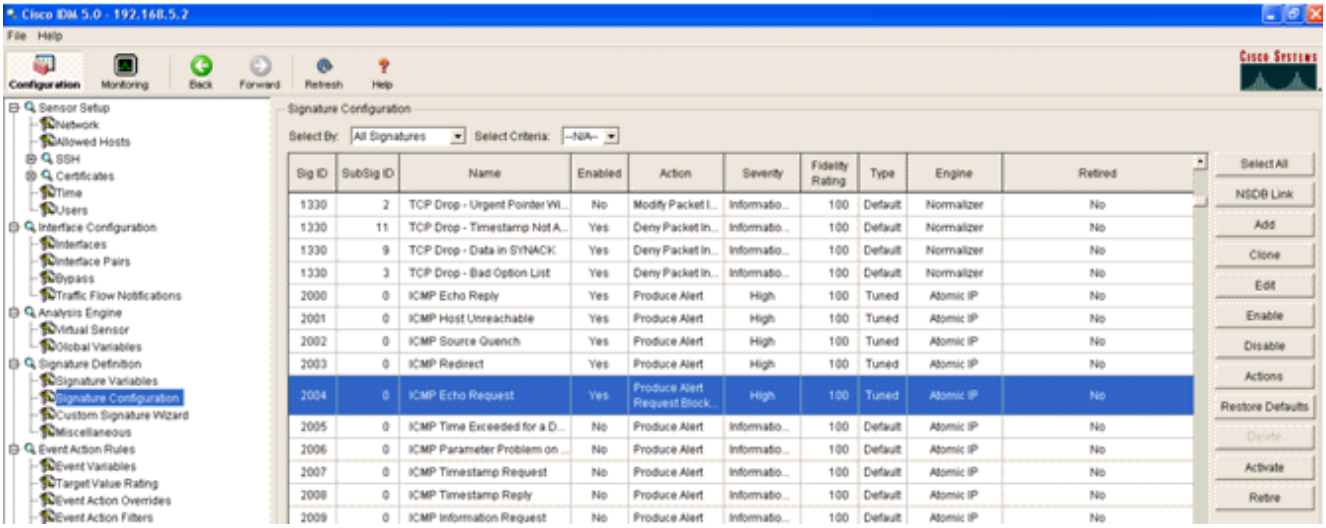
4. تحقق من حالة الاتصال بين AIP-SSM و WLC.



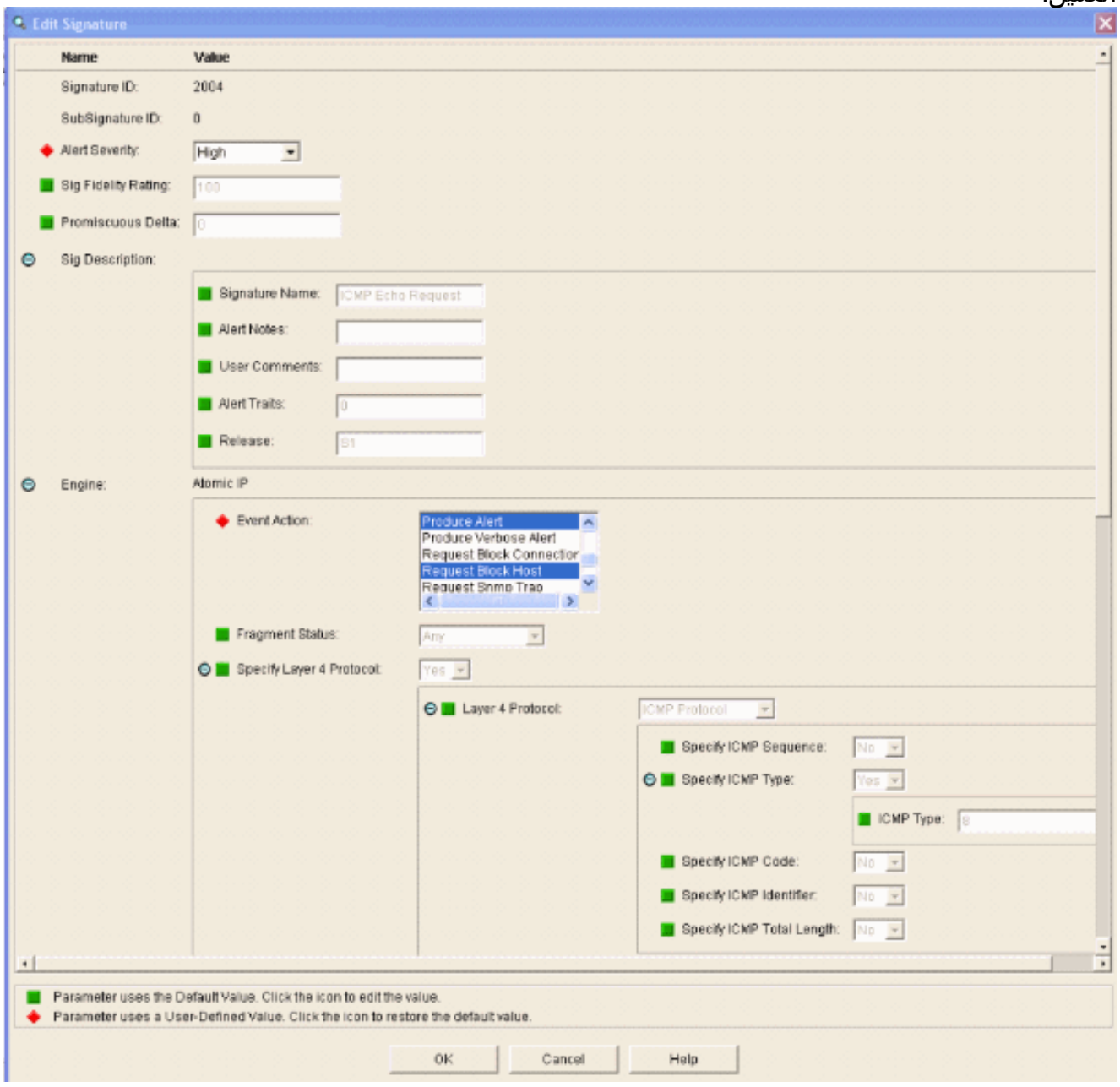
إضافة توقيع حظر إلى AIP-SSM

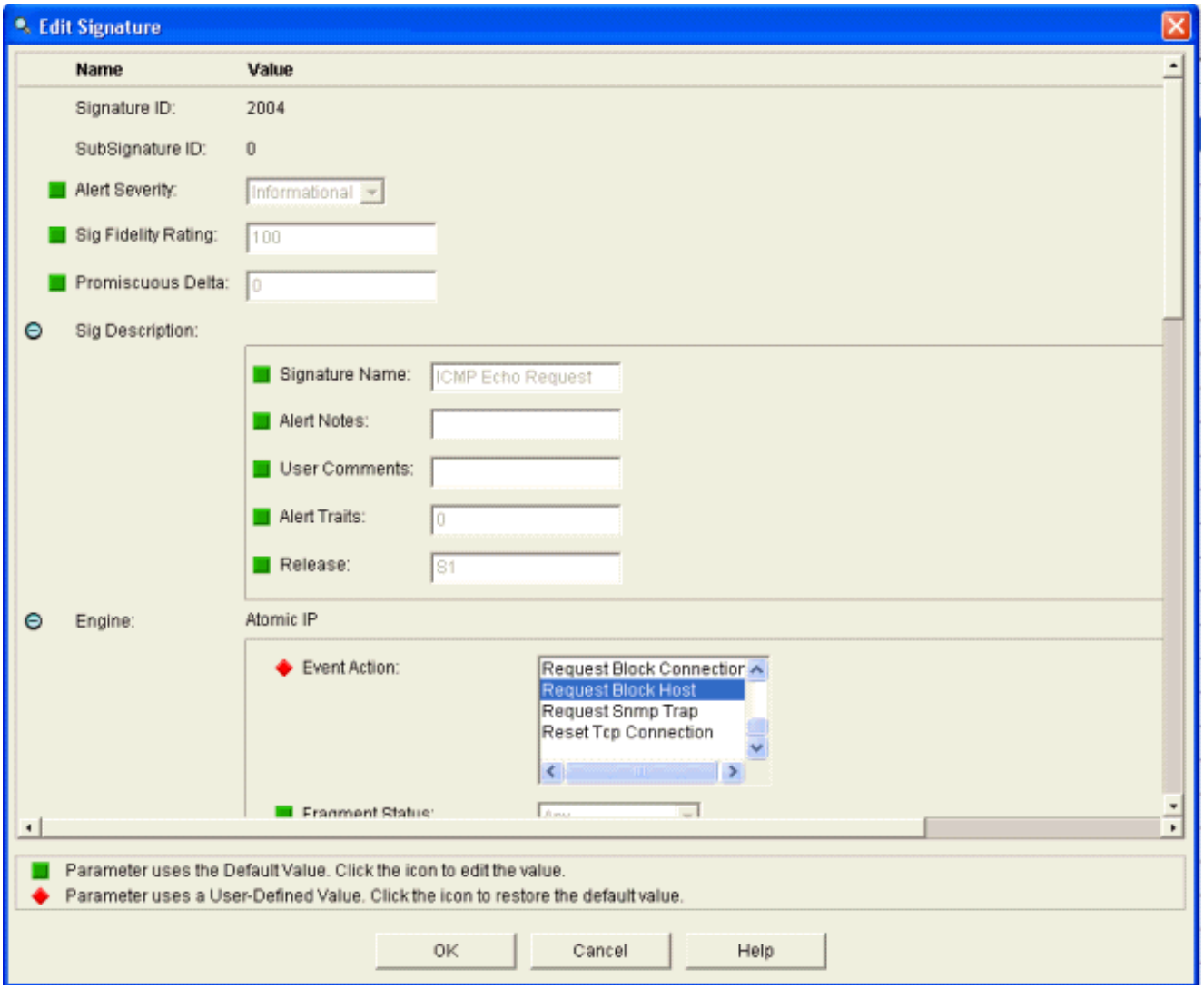
إضافة توقيع فحص لحظر حركة المرور. على الرغم من وجود العديد من التوقيعات التي يمكنها القيام بالمهمة بناء على الأدوات المتاحة، فإن هذا المثال ينشئ توقيعا يمنع حزم إختبار الاتصال.

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



2. قم بتمكين التوقيع وتعيين خطورة التنبيه إلى **عالية** وتعيين إجراء الحدث **لإنتاج تنبيه** و**مضيف 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.



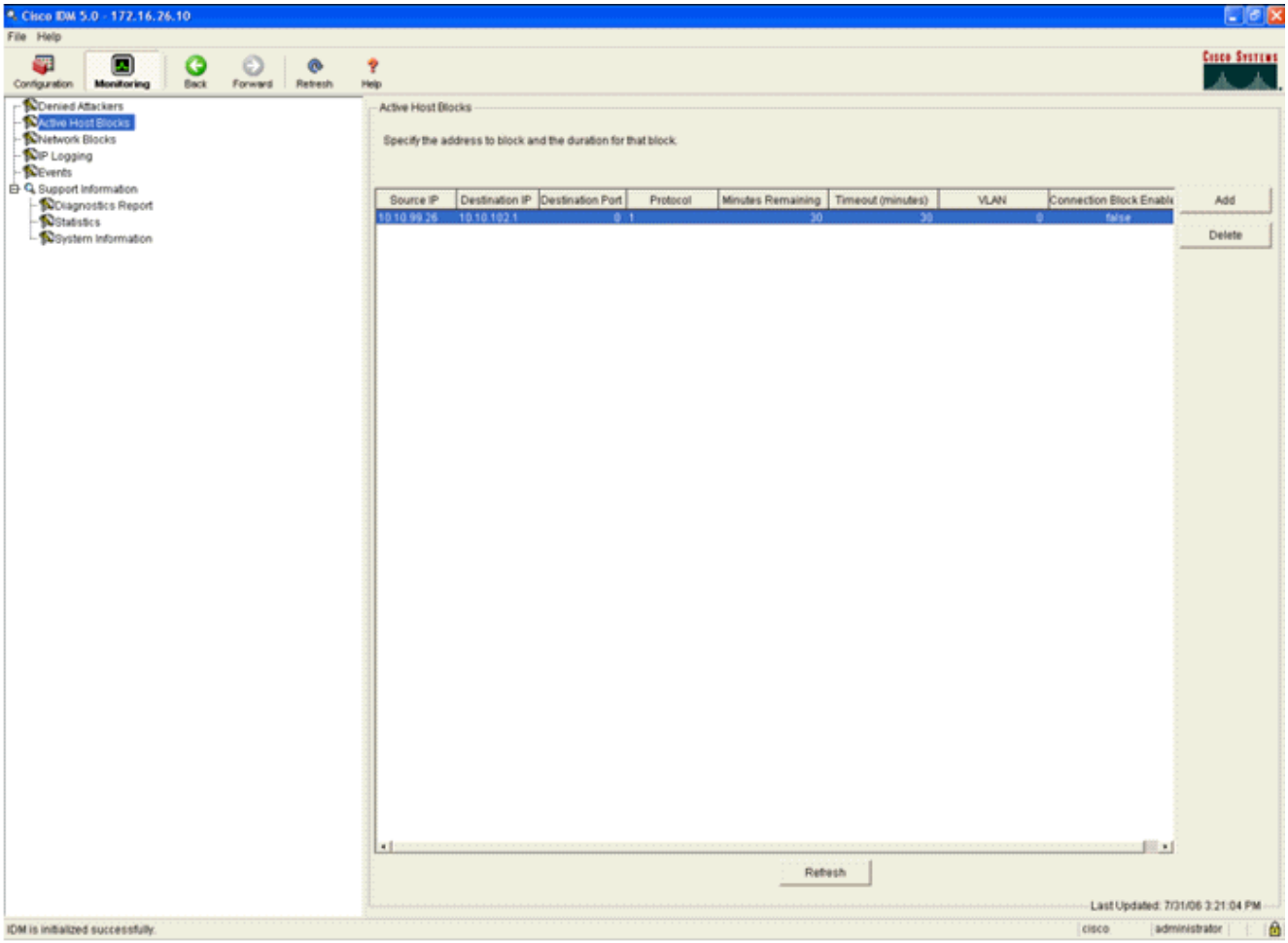


3. طقطقة to order in **ok** أنقذت التوقيع.
4. تحقق من أن التوقيع نشط ومن أنه تم تعيينه لتنفيذ إجراء حظر.
5. انقر فوق **تطبيق** لتنفيذ التوقيع على الوحدة النمطية.

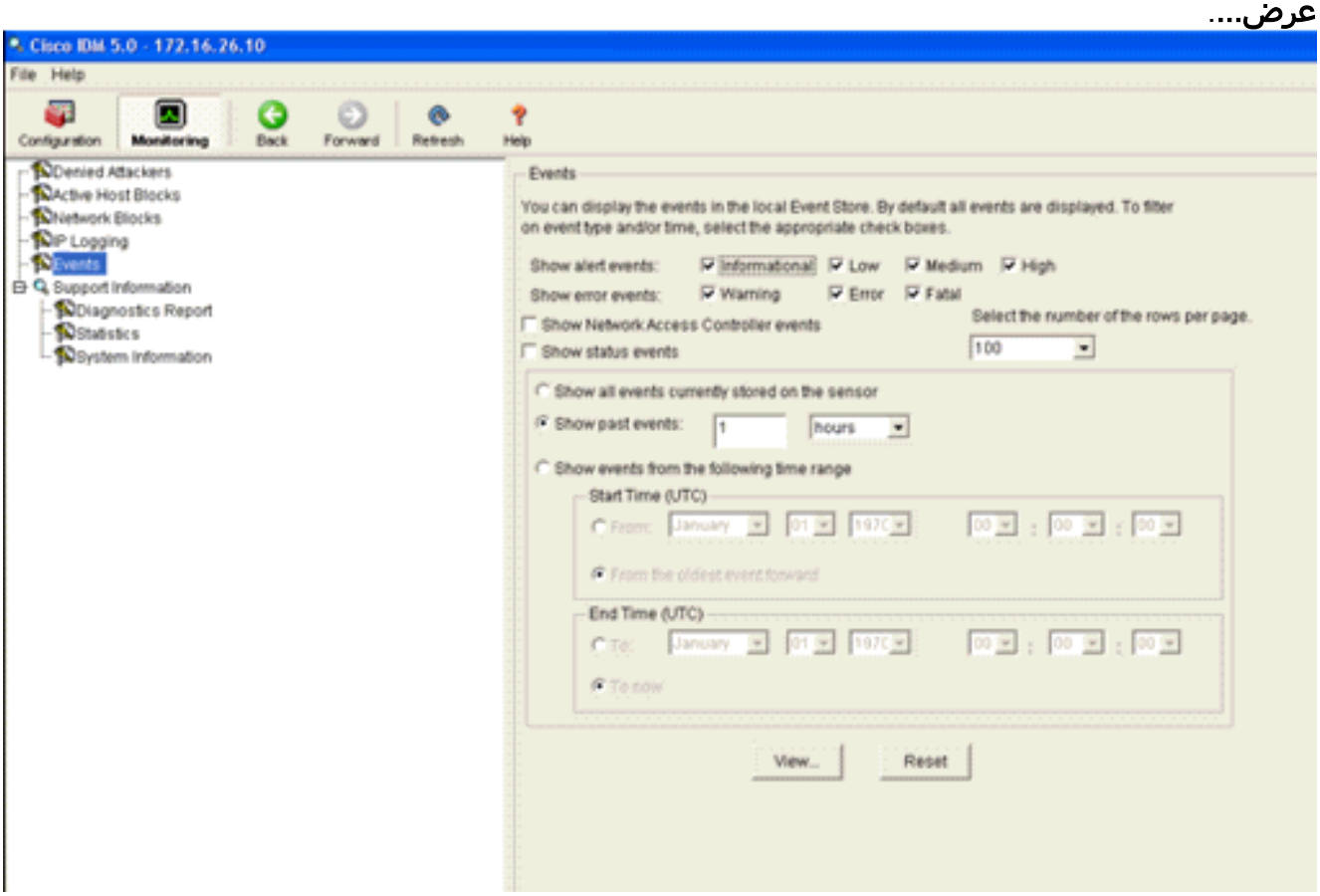
حظر المراقبة والأحداث باستخدام إدارة البيانات الرقمية

أكمل الخطوات التالية:

1. عندما يتم تشغيل التوقيع بنجاح، هناك مكانين داخل IDM لملاحظة ذلك.تعرض الطريقة الأولى الكتل 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 فورا، ثم حددها من القائمة ثم انقر فوق
حذف.

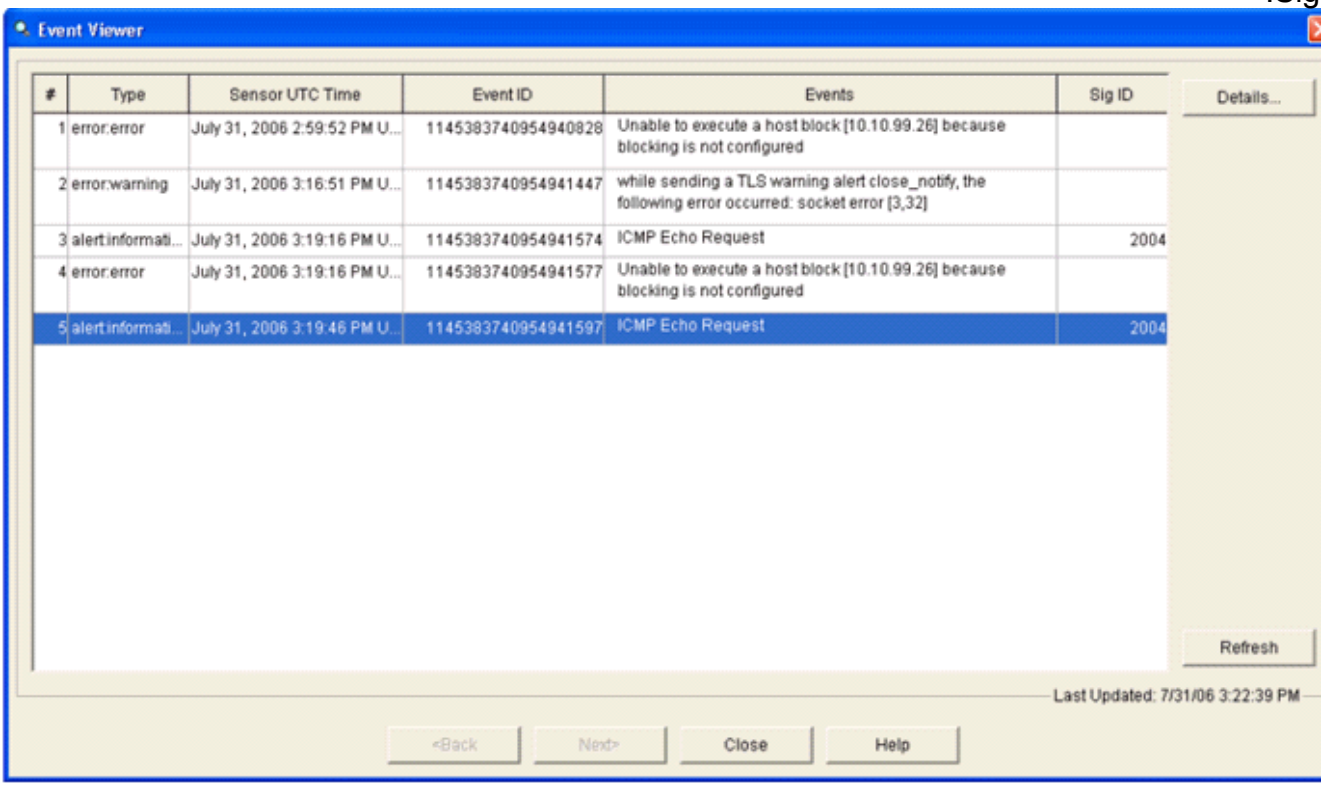


وتستخدم الطريقة الثانية لعرض التوقيعات التي تم تشغيلها المخزن المؤقت لحدث AIP-SSM. من صفحة مراقبة IDM، حدد **أحداث** في قائمة العناصر على الجانب الأيسر. تظهر أداة بحث الأحداث المساعدة. قم بتعيين معايير البحث المناسبة وانقر فوق
عرض...

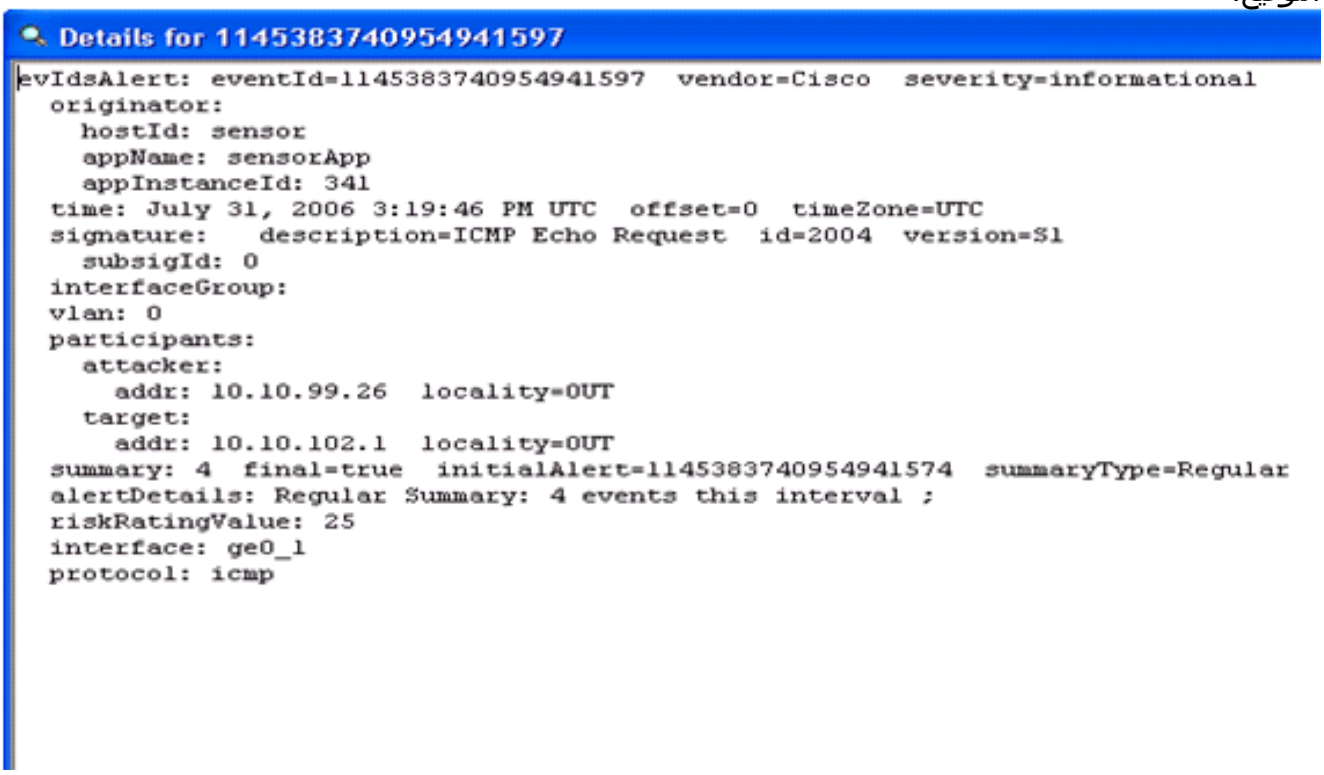


2. ثم يظهر "عارض الأحداث" بقائمة أحداث تطابق المعايير المحددة. قم بالتمرير خلال القائمة والعثور على توقيع

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.

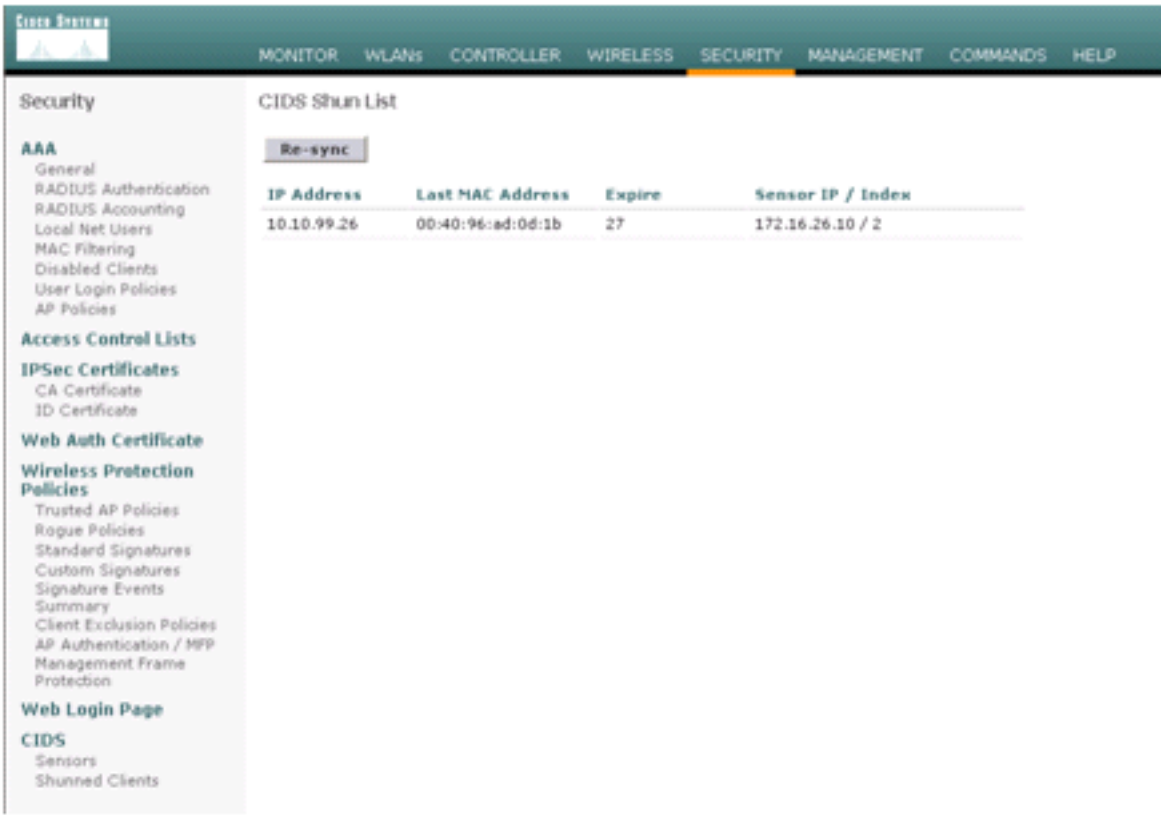


3. بعد أن تقوم بتحديد مكان التوقيع، قم بالنقر المزدوج على الإدخال لفتح نافذة جديدة. يحتوي الإطار الجديد على معلومات تفصيلية حول الحدث الذي قام بتشغيل التوقيع.

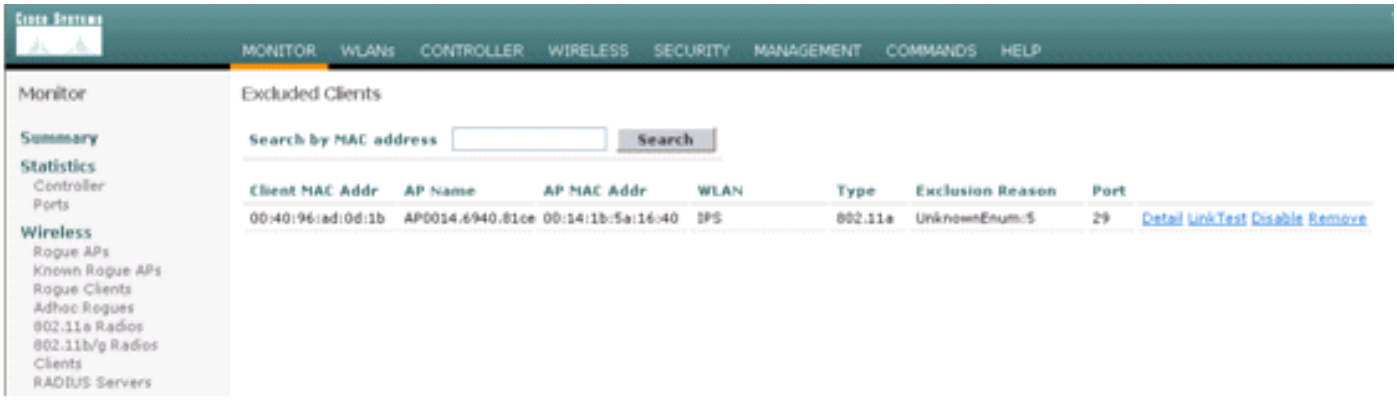


مراقبة إستثناء العميل في وحدة تحكم لاسلكية

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



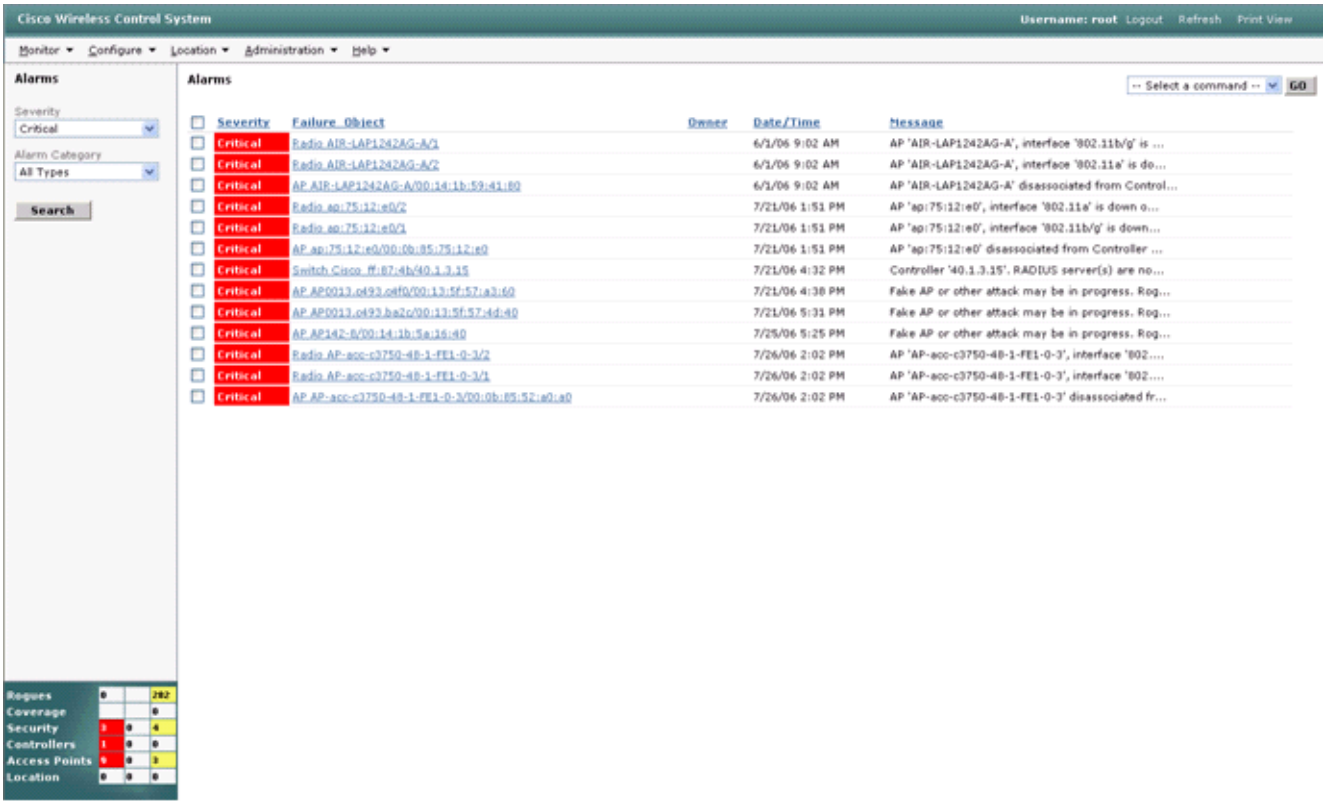
تتم إضافة المستخدم إلى قائمة "إستبعاد العميل".



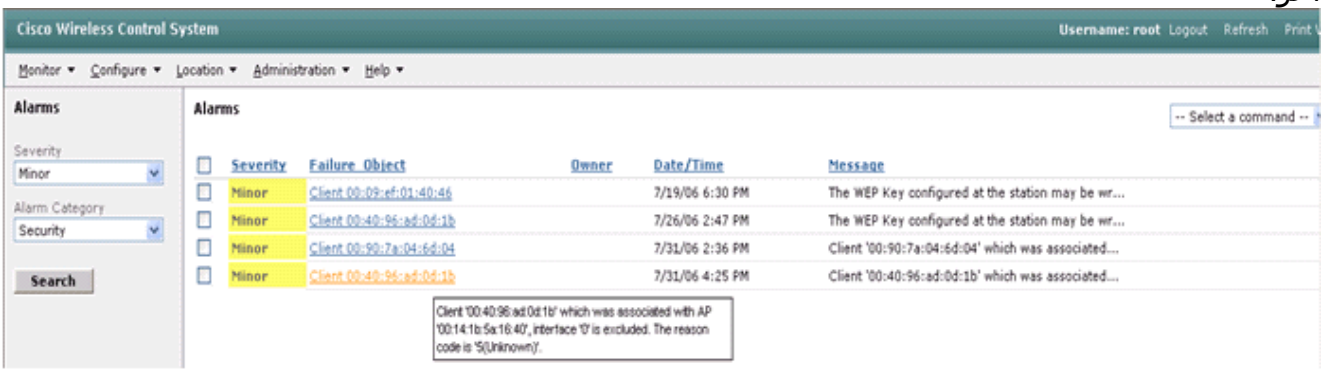
مراقبة الأحداث في WCS

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، أختر **ثانوي**، واضبط أيضا فئة التنبيه على **الأمان**.
3. انقر فوق **بحث**.



4. يسرد نافذة التنبيه بعد ذلك فقط تنبيهات الأمان ذات الخطورة الصغيرة. وجه الماوس عند الحدث الذي أدى إلى تشغيل الكتلة داخل AIP-SSM.تظهر WCS على وجه الخصوص عنوان MAC لمحطة العميل التي سببت الإنذار. من خلال الإشارة إلى العنوان المناسب، يظهر WCS نافذة صغيرة مع تفاصيل الحدث. انقر فوق الارتباط لعرض نفس التفاصيل في إطار
آخر.



تكوين ASA العينة من Cisco

```
ciscoasa#show run
Saved :
:
(ASA Version 7.1(2
!
hostname ciscoasa
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 10.10.102.2 255.255.255.0
!
```

```
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
```

تكوين عينة مستشعر نظام منع الاقتحام Cisco Intrusion Prevention System Sensor 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 التحكّم 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

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).