# (LAN) ةيلحملا ةكبشلا يف مكحتلا ةدحو IPS لماكت ليلدو ةيكلساللا

### المحتويات

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

### <u>المقدمة</u>

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 رائيت من 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 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 HWAPP مع خط منتجات Cisco الميزات هذا الإصدار، يكون الهدف هو السماح لنظام (WLAN) قائم على HWAPP مع خط منتجات Cisco IDS/IPS. في هذا الإصدار، يكون الهدف هو السماح لنظام (Sico IDS/IPS) بإصدار تعليمات إلى قوائم التحكم في المحلية اللاسلكية (MLCs) لحظر وصول عملاء معينين إلى الشبكات اللاسلكية عند اكتشاف هجوم في أي مكان من الطبقة 3 إلى الطبقة 7 التي تتضمن العميل المعني الميزات.

## <u>المتطلبات الأساسية</u>

### <u>المتطلبات</u>

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 IDS (NM-CIDS) 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.

### <u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

# نظرة عامة على <u>Cisco IDS</u>

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 MDL 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 اCL أو MD أو MDE 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.

### <u>تجنب IDS</u>

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 A IP. الآن، عندما يقوم جهاز التحكم باستطلاع معرفات أحداث الإحجام، تقوم معرفات الهوية بإرسال طلب الإحجام إلى جهاز التحكم بعنوان A IP 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 عملاء السود المدرجين على وحدة التحكم. الآن

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.

### <u>تصميم بنية الشبكة</u>



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 Vl	an Id IP	Address	Туре Ар	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
				< I II	

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

```
!
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 يتحلبا انسخة من حركة المرور المراقبة بدلا من

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: الر**سم التخطيطي للبنية المعمارية</u> هو مجرد مثال لإعداد بنية WLC و IPS المدمجة. يشرح مثال التكوين الظاهر هنا واجهة إستشعار IDS التي تعمل في الوضع المختلطة. <u>الرسم التخطيطي</u> المعماري يوضح واجهات الاستشعار التي يتم مزامنتها للعمل في وضع زوج الخطية. راجع <u>الوضع المضمن</u> 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/stgrg.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 <a href="https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet">https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet</a> (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 ان يكون هذا العنوان قابلا للتوجيه إلى واجهة إدارة وحدة التحكم. ولا تتطلب واجهات الاستشعار معالجة. يجب أن تتضمن قائمة الوصول عنوان واجهة إدارة ا 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. انت يستطيع الان 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.

* Cisco IDM 5.0 - 192.168.5.2				
File Help				
	6 1	÷		Cisco Sestens
Configuration Montoring Back Forward	rd Retresh He	•		dr. dr.
Configuration Mentoring  General Selve  General Setting  General Setting	Retreach Per Network Opecity the network Hostname: IP Address: Network Mask Default Route: FTP Timeout Web Server Settin IP Enable TL8/69 Web server pott	and communication parameters for the sensor.	Remote Access Telet is not a secure access service and is disabled by default. If Enable Telet	seconds
IDM is initialized successfully.				cisco administrator

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

Ciscs DW 5.0 - 197.168.5.7					
lle Help					
Configuration Monitoring Back Fo	🕥 💽 📍				Cisco System
Q Sensor Setup - Network - Network - Network - Network - Setup - Setup	Users Specify the users that hav	e access to the sensor. The servi	ce role is a special role that allows you to bypass the CLI if	needed. Only one service account is allowed.	
D G Certificates	U	iemame	Role	Status	
10 Iners	cisco		Administrator Ad	ctive	A00
Q Interface Configuration					Est
- Sinterfaces					
- Plinterface Pairs					Delete
- Seypass					
Traffic Flow Notifications					
Q Analysis Engine		Add User	X		
- Winual Sensor					
Sinestus Defeitice		Usemame:	controller		
Signature Cennison					
-Signature Configuration					
- Ocustom Signature Wizard		User Nole:	Animatic T		
Miscellaneous					
C Event Action Rules					
- Devent Variables		- Password	······································		
- Target Value Rating					
- DEvent Action Overrides		Parament	[mmm]		
- SNEvert Action Filters		Password,			
Concernal Settings					
Selecting		Caster Baserie	[ +++++d		
Source Login Professo		Consim Password.			
- Selocking Devices					
- Router Blocking Device Interfaces					
- Cat 6K Blocking Device Interfaces			Concel Horn		
Master Blocking Sensor		- UK	- Carter Help		
C CAMP	1.1				

6. قم بتمكين واجهات المراقبة.

Cisco IDM 5.0 - 192.168.5.2							- C 0 0
File Help							
Configuration Monitoring Dack Form	vard Refresh Help						Cisco Sestens
G Sensor Setup     Setwork     Mitetwork     Malowed Hosts     G Q SSH     G Certificates	Interfaces A sensing interface mu and clicking Enable or	st be enabled and assigned Disable.	to a virtual sens	or before the se	nsor will monitor that in	erface. You can enable/disable the available sensing interfaces by selecti	ng the row(s)
- NTime - NUsers	Interface Name	Enabled Media Type	Duplex	Speed	Atternate TCP Reset Interface	Description	Select All
Q Interface Configuration	OigabitEthemet0/0	Yes TX (copper)	Auto	Auto	None		Edit
Sinterface Pairs	GigabitEthomet0/1	No TX (copper)	Auto	Auto	None		Eastin
- Departs	OigabitEthemet0/2	No TX (copper)	Auto	Auto	None		Chable
L-STraffic Flow Notifications	OigabitEthemet0/3	No TX (copper)	Auto	Auto	None		Disable

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

Cisco IDM 5.0 - 192.168.5.2				🛛
File Help				
Configuration Montoring Back Forward	and Refresh	nep		Casco Systems
E: Q. Sensor Setup - Nivebook - Nalowed Hosts B: Q. Sent D: Q. Centificables - Nitime	Virtual Sensor The sensor assign and	or monitors traffic that traverses interfaces or interface pa remove interfaces (or pains). You cannot add a new vit	irs assigned to a virtual sensor. Click Edit to change the properties of the default virtual sensor. You can change the ual sensor or change the virtual sensor name.	description or
- NUsers	Name	Assigned Interfaces (or Interface Pains)	Description	Edit
B-S Interface Configuration - Dinterfaces - Dinterface Pairs - Dityairs Diratic Flow Notifications	vs0	OlgabitEthemet00 OlgabitEthemet01 OlgabitEthemet02 OlgabitEthemet03	default virtual sensor	
Analysis Engine     Ninus Engine     Notice State     Notice State				

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

Cisca DH 5.0 - 192.168.5.2											لسريع.
File Help											
Configuration Monitoring Back Forms	nd Retres	n Help									Cisco Sesteus
Q. Sensor Setup     Setwork     SAllowed Hosts	Signature Select Dy	Configuration	on tures 💌 Select Criteria: 🖡	-NA- 💌							
B Q SSH B Q Centificates	Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity Rating	Type	Engine	Refired	Select All
Dusers	1330	2	TCP Drop - Urgent Pointer WI	No	Modify Packet I	informatio	100	Default	Normalizer	No	NSDe Link
D Q Interface Configuration	1330	11	TCP Drop - Timestamp Not A.	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Add
- Ninterfaces	1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Clone
- Dinterface Pairs	1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	
Traffic Flow Notifications	2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Edt
Q Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	Enable
- Wirtual Sensor	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Durable
E G. Signature Definition	2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	
-Signature Variables					Developen Alast	-					Actions
Signature Configuration	2004		ICMP Echo Request		Request Block	High		Tuned	Adomic IP	No	Restore Defaults
Custom Signature Wizard	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	Informatio	100	Default	Atomic IP	No	
D Q Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Dente.
- Devent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Activate
- STarget Value Rating	2008	0	ICMP Timestamo Restly	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Dutra
PAEvent Action Overrides     Sevent Action Educe	1000	0	MAR Information Request	No	Evolution Alast	Information	100	Deduct	Atomic ID	Na	roetre

يجب تمكين التوقيع، وتعيين خطورة التنبيه على **عالي** وتعيين إجراء الحدث **لإنتاج تنبيه** و**مضيف 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									
Sig Description:										
	Signature Name: ICMP Echo Request									
	Alert Notes:									
	User Comments:									
	Alert Traits:									
	Release. St									
Engine:	Atomic IP									
	Event Action:     Produce Alert     Produce Verbose Alert     Request Block Host     Request Simon Trace     Security Request S									
	E Laver 4 Protocol:									
	Specific/OMP Sequence: No									
	■ ICMP Type.  8									
	Specify ICMP Code:									
	Specify ICMP Identifier: No									
	Specify ICMP Total Length: No -									
•	· · · · · · · · · · · · · · · · · · ·									
<ul> <li>Parameter uses the D</li> <li>Parameter uses a Use</li> </ul>	Vefault Value. Click the icon to edit the value. Ver-Defined Value. Click the icon to restore the default value.									
	OK Cancel Help									

### <u>تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)</u>

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

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 t1s fingerprint** MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19

Cinco Seatens	and the second second	and a state of the	Section Section	a building	Anistali - anistanta	Save Co	nfiguration	Ping   Logout	Refresh
Andre Contraction	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Security	CIDS Sensor Add						< Back	Apply	
General RADIUS Authentication RADIUS Accounting	Index	1.							
Local Net Users MAC Filtering Dirabled Clients	Server Address	192.168.5.2							
User Login Policies AP Policies	Port	443							
Access Control Lists	Username	controller							
Network Access Control	Password	•••••							
IPSec Certificates CA Certificate ID Certificate	Confirm Password	·····							
Web Auth Certificate Wireless Protection	Query Interval	15 seco	nds						
Policies Trusted AP Policies	State	R							
Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection	Fingerprint (SHA1 hosh)	1662E996362A9A1	EF08899A7C1	645FSCB56A8	842 40 he	« chars			
Web Login Page									
CIDS Sensors Shunned Clients									

3. تحقق من حالة الاتصال بين مستشعر IPS و WI C

										LC
Core States									Save Configuration   Ping   Lop	out   Re
A.A.	MONITOR WLA	Ns CONTROLLER	WIRELESS	SECURITY I	MANAGEMENT (	COMMANDS F	€LP			
Security	CIDS Sensors L	ist							Nes	#
AAA	Index	Server Address	Port	State	Query Inte	rval Last Qu	ery (count)			
General RADIUS Authentication	1	192.168.5.2	443	Enabled	15	Success	(6083)	Detail Remove		
RADIUS Accounting										
Local Net Users MAC Filtering										
Disabled Clients										
AP Policies										
Access Control Lists										
Network Access Control										
IPSec Certificates										
1D Certificate										
Web Auth Certificate										
Wireless Protection										
Trusted AP Policies										
Rogue Policies Standard Sizeabures										
Custom Signatures										
Signature Events Summary										
Client Exclusion Policies AP Authentication										
Management Frame										
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.

Const Dentes										puration   Ping	Logout   Refre
	MONITOR WEARS CO	INTROLLER WIRELES	SECURITY	MANAGEMENT	COMMANDS	HELP					
WLANS	WLANs > Edit									< Back	Apply
WLANS	WLAN ID	1									
AP Groups VLAN	WLAN SSID	1PS									
	General Policies						Security Policies				
	Radio Policy	All 👻					IPv6 Enable				
	Admin Status	💽 Enabled									
	Session Timeout (secs)	1800					Layer 2 Security	WPA1+WPA2	¥		
	Quality of Service (QoS)	Silver (best effort)	· .					HAC hitering			
	WMM Policy	Disabled 🛩					Layer 3 Security	None	¥		
	7920 Phone Support	Client CAC Limit	AP CAC Limit					Web Policy *			
	Broadcast SSID	😴 Enabled									
	Allow AAA Override	Enabled									
	External Policy Validation	Enabled					<ul> <li>Web Policy cannot be and L2TP.</li> </ul>	used in combination	with IPsec		
	Client Exclusion	Enabled ** 600 Timeo	A Value (secs)				** When client exclusion zero means infinity(will a	n is enabled, a time: require administrati	out value of ve override to	,	
	DHCP Server	Overvide					reset excluded clients)				
	DHCP Addr. Assignment	Required									
	Interface Name	management 💌									
	MFP Version Required	1									
	MFP Signature Generation										
	H-REAP Local Switching										
	* H-REAP Local Switching	p not supported with IPSE	, L2TP, PPTP, C	RANITE and FORTH	RESS authentical	tions.					
	CISCO Client Extension (CCX)										
	Version 1E	Enabled									
	Aironet IE	2									
	Gratuitous Probe Response										
	Radius Servers										
		Authentication Servers	Accounting	Servers							
	Server 1	1P:10.1.1.12, Port:1812	✓ none ✓								

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.

Cisco IDN 5.0 - 192.168.5.2		•• • • • • • • • • • • • • • • • • • •
File Help		
Configuration Monitoring Back Forward Refresh		
- NDeried Attackers - NAttive Hast Blocks - Nitework Blocks - Nitework Blocks - Niteworks	we Host Blocks	
- Diagnostics Report	lource IP Destination IP Destination Port Protocol Minutes Remaining	Timeout (minutes) VLAN Connection Block Enable
- DStatistics DSystem Information	10.99.21 10.10.99.1 0 1 10	10 O false

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

A.A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shur	n List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Local Policies	Re-sync IP Addres 10.10.99.21	s La 1 00	st MAC Address	Expire 326979296	5en 192-	sor IP / Index 168.5.2 / 1		
AP Policies								
Network Access Control								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Regue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

بالمضيف . إضافة المستخدم إلى قائمة "إستبعاد العميل".

Cases Sections									
A. A.	MONITOR	WLANS	CONTROLLER	WIRELESS SEC	URITY MANA	GEMENT CO	DMMANDS HELP		
Monitor	Excluded (	Clients							
Summary	Search by	MAC add	ress	Searc	h				
Controller Ports	Client MAG	Addr	AP Name	AP MAC Adde	WLAN	Туре	Exclusion Reason	Port	
Wireless	00:40:95:8	d:0d:1b	AP1242-2	00:14:15:59:3e:10	IPS	802.11b	UnknownEnum:5	29	Detail LinkTest Disable Remove

يتم إنشاء سجل ملائمة أثناء إضافة عميل إلى قائمة

A.A.	MON	ITOR WLAN	CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Management	32	14:41:00 2006	Regue AP : 00:15:c7:02:03:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(002.11b/g) with RSSI: -03 and SNR: 6
Summary	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
General SNMP V3 Users	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(002.11b/g)
Communities Trap Receivers Trap Controls	35	Tue Apr 11 14:39:44 2006	Regue : 00:0b:85:54:de:Se removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
Trap Logs	36	Tue Apr 11 14:39:44	Rogue : 00:0b:85:54:de:Sf removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface avoid 002-11b.fm3

م أيضاً إنشاء سجل رسائل

يت

Com Series	MONITOR WLANS CON	NTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Management	Message Logs					
Summary	Message Log Level	Significant System events	*			
General SNMP V3 Users Communities Trap Receivers Trap Controls Trap Legs HTTP Telnet-SSH Serial Port Local Management Users User Sessions Sysleg	Tue Apr 11 14/54/01 2006   00:40:96:ad:0d:1b to exclur 10.10.99.21 Tue Apr 11 14:55:59 2006   admin user 'admin' Mon Apr 10 13:11:06 2006 mmDbMgmtVlan60rtUpdate( NULL peinter. Mon Apr 10 13:10:58 2006 @ timerib.c:442: ERROR: 'b Mon Apr 10 13:10:57 2006	SECURITY] mm_listen.c 36 ion 5st as a result of an ID (SECURITY] asa.c 661: Aut (CRITICAL] osapi_sem.c 7: ) @ mm_dir.c:982: ERROR: (CRITICAL] timerib.c 442: (CRITICAL] timerib.c 442: (CRITICAL] osapi_sem.c 7: merSema' is a NULL pointe (CRITICAL] timerib.c 442: (CRITICAL] osapi_sem.c 7: merSema' is a NULL pointe (CRITICAL] bootosc 825: :	(38: Adding S shun event f mentication sux 77: (dbHead)->c Task 3227309 77: osepi8snTi Task 3227309 77: osepi8snTi r. Security Mod Sarting code	for coceeded for mutex' is a (52 unable to merCreate() (52 unable to merCreate() unable to merCreate() (1) (2) (2) (3) (3) (3) (3) (4) (4) (4) (4) (4) (4) (4) (4		
Mgmt Via Wireless Message logs						

يتم إنشاء

للحدث.

Input Options	C Scan Options			
C IP Range C IP List	@ Domain C Act	ive Directory	C WMI API	Scan
G Single Host C Neighborhood	Vin32 OS Version	Users	Patch Level	Exit
10.1.1.12	Null IPC\$ Sessions	Services	MAC Address	Clear
1	₩ NetBIOS Shares	Disks	C Sessions	
	Date and Time	Groups	Event Log	Save
	Ping Host(s)	- RPC	- Show	Help
	Traceroute Host	Bindings	Errors	
General Options				
		TCP Ports	ican Range:	1 1024
				[
Timeout for TCP/UDP/ICMP/SNMP:	5	LIDP Ports	coan Bannei	1 1024
Timeout for TCP/UDP/ICMP/SNMP:	5	C UDP Ports	ican Range:	Dublic
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne	ctions: 1024	C UDP Ports	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Address: 1011112 NAC-ACS omputername: WORKGROUP/NAC-A ID: 5-1-5-21-790525478-158043664	ctions: 1024	SNMP Co	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Maurese: 10.1.1.12 NAC-ACS computername: WORKGROUP/NAC-A ID: S-1-5-21-790525478-158043666 Addresses: 0009658451c2	5 ctions: 1024	SNMP Co	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Mouress: 10.11.12 NAC-ACS omputername: WORKGROUP/NAC-A ID: S-1-5-21-790525478-158043660 AC Addresses: 0009668d51c2 atch Level:	5 ctions: 1024	SNMP Co	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne P HOUPEST 10:11:12 NAC-ACS omputername: WORKGROUP/NAC-A ID: S-1-5-21-790525478-158043660 AC Addresses: 00966bd51c2 atch Level: Operating System: 5.0 Role: NT Member Server	ctions: 1024	SNMP Col	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne ADDRES: 10.1.1.12 NAC-ACS omputername: WORKGROUP/NAC-A ID: 5-1-5-21-790525478-158043666 AC Addresses: 0009668d51c2 atch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Dele: INT Workstation	s ctions: 1024	SNMP Co	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Aduress: 10:1:1:12 NAC-ACS computername: WORKGROUP/NAC-/ ID: 5-1-5-21-790525478-15804366 AC Addresses: 00096bddS1c2 atch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Workstati Role: LAN Manager Server	s ctions: 1024	C UDP Ports	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Maurese: 10.1.1.12 NAC-ACS computername: WORKGROUP/NAC-J ID: S-1-5-21-790525478-158043660 AC Addresses: 00096b8d51c2 atch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstati Role: LAN Manager Workstati Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment:	5 ctions: 1024	C UDP Ports	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Macrosoft International Max Conne AC Addresses: 00096b8d51c2 atch Level: 00096b8d51c2 atch Level: 00096b8d51c2 atch Level: 00096b8d51c2 atch Level: 00096b8d51c2 Addresses: 00096b8d51c2 atch Level: 00096b8d51c2 Addresses: 000	5 ctions: 1024	C UDP Ports	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Aduress: 10.1.1.1 NAC-ACS omputername: WORKGROUP/NAC-A ID: S-1-5-21-790525478-15804366 AC Addresses: 00096b8d51c2 atch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Workstab Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hot KB823182 Windows 2000 Hot	5 ctions: 1024 ACS 57-1343024091 on fix - KB329115 fix - KB329115	F UDP Ports	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Aduress: 10.1.1.11 NAC-ACS omputername: WORKGROUP/NAC-A ID: S-1-5-21-790525478-15804366 AC Addresses: 00096b8d51c2 atch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Workstab Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hot KB823859 Windows 2000 Hot KB823559 Windows 2000 Hot	5 etions: 1024 ACS 57-1343024091 on fix - KB329115 fix - KB329115 fix - KB323182 fix - KB823559	C UDP Ports	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Aduress: 10.1.1.11 NAC-ACS omputername: WORKGROUP/NAC-A ID: S-1-5-21-790525478-158043664 AC Addresses: 00096b8d51c2 atch Level: Operating System: 5.0 Role: NT Member Server Role: IAN Manager Workstab Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB323152 Windows 2000 Hot KB823152 Windows 2000 Hot KB82359 Windows 2000 Hot KB824151 Windows 2000 Hot	5 etions: 1024 ACS 67-1343024091 on fix - KB329115 fix - KB323182 fix - KB823182 fix - KB823559 fix - KB824151	T UDP Ports	scan Range: mmunity String:	public
Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne Aduress: 10.1.1.11 NAC-ACS omputername: WORKGROUP/NAC-A ID: S-1-5-21-790525478-158043664 AC Addresses: 00096b8d51c2 atch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Workstab Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB323152 Windows 2000 Hot KB823152 Windows 2000 Hot KB823159 Windows 2000 Hot KB824151 Windows 2000 Hot	5 etions: 1024 ACS 67-1343024091 on fix - KB329115 fix - KB323182 fix - KB823182 fix - KB823159 fix - KB824151 fix - KB024151 fix - KB025119	C UDP Ports	scan Range: mmunity String:	public

هذا نافذة أحداث ولدت في ال cisco ips مستشعر.

Cisco IDM 5.0 - 192.168.5.2						
File Help						
Configuration Monitoring	O Deck Forward Re	efresh Pleip				
RO enired Attackers     Routive Host Blocks     Onletwork Blocks     Ror Logging     Onletwork Blocks     G. Deport Information     Rotageostics Report     Rotastics     Rotastics	Q. (word Viewer	-D Yes On D	vents u can display the events in t event type and/or time, sele how alert events: how error events: W	te local Event Store. By default all events are displayed. To fite ct the appropriate check boxes. formational IP Low IP Medium IP High aming IP Error IP Fatal	r	×
	# Type	Sensor UTC Ti	Event ID	Events	Sig ID -	100000011
	17 alerthigh:100	April 11, 200	1144003216861913654	ICMP Echo Reply	2000	
	16 alerthigh:100	April 11, 200	1144083216861913652	ICMP Echo Request	2004	
	19 alertiow 32	April 11, 200	1144003216861913656	SMD: ADMINE Hidden Share Access Alternot	3320	
	18 alertinformati	April 11, 200	1144083216861913655	SMD. Windows Share Enumeration	3322	
	20 alert informati	April 11, 200	1144003216861913668	SMB: Windows Share Enumeration	3322	
	21 entrientir	April 11, 200	1144003216061913665	Unable to execute a host block timeout (10.10.99.2) because blocking is disabled		
	22 alert information	April 11, 200	1144063216661913696	TCP SYN Host Sweep	3030	
	23 alert information	April 11, 200	1144083216861913706	TCP SYN Host Sweep	3030	
	25 alerthigh:100	April 11, 200	1144063216661913712	ICMP Echo Reply	2000	
	26 empremor	April 11, 200	1144003216061913714	Unable to execute a host block [10,10,99,22] because blocking is disabled		
	24 alerthigh:100	April 11, 200	1144083216861913710	ICMP Echo Request	2004	
	27 alert medium:	April 11, 200	1144063216861913715	IOS UDP Bomb	4600	
	29 aletmedium.	April 11, 200	1144083216861913717	Back Orifice Ping	4060	
	30 aletmedium.	April 11, 200	1144083216861913718	IOS UDP Bomb	4600	
	31 aletmedium.	April 11, 200	1144003216061913719	Back Orifice Ping	4060	
	32 alertmedium:	April 11, 200	1144083216861913720	IOS UDP Bomb	4600 .	Refesh
	L		-Wiick	Nets Close Help	Last Updated: 4/11	/06 2:52:40 PM

### <u>تكوين عينة مستشعر Cisco IDS</u>

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 10.0.0/8 access-list 40.0.0/8 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



وعلى عكس مستشعر اكتشاف الاقتحام التقليدي، يجب أن يكون ASA دائما في مسار البيانات. ،in other words i 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.

📫 Cisco ASDM 5.1 for ASA - 172.16.26.2	
File Rules Search Options Tools Wizards Help	
Home Configuration Monitoring Back Forward Search	Refresh Save Help
Device Information	Interface Status
General License	Interface IP Address/Mask Line Link Current Kbps
Host Name:     ciscoasa.cisco.com       ASA Version:     7.1(2)       Device Uptime:     2d 5h 24m 51s       ASDM Version:     5.1(2)       Perice Type:     ASA5510       Firewall Mode:     Routed     Context Mode:	Inside 172.16.26.2/24 O up O up 3 management 192.168.1.1/24 O down O down 0 outside 10.10.102.2/24 O up O up 0
Total Flash: 256 MB Total Memory: 256 MB	Select an interface to view input and output Kbps
VPN Status IKE Tunnels: 0 WebVPN Tunnels: 0 SVC Tunnels: 0 System Resources Status CPU CPU Usage (percent)	Traffic Status Connections Per Second Usage
1% 00 1% 07 02 17 07 02 Memory Memory Memory 040	12 07.02 UDP: 0 TCP: 0 Total: 0 "outside' Interface Traffic Usage (Kbps)
64.09 17.02-32 17.07-32 17.07-32 17.07-32	0.6 19 07 02 Input Kbps: 0 Output Kbps: 0

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

	Continues Contract Options Tools Wigard	s Help								
6	-	0	0	Q	0	2				Cinco Sri
Rodry Ro	Anagemention Montering Conceptionation & Information	Name outside manage	Enabled Yes No Yes	Becurity Level	IP Address 10 10 102 2 172 16 26 2 192 166 1 1	Gubret Mask 255 255 255 0 255 255 255 0 255 255 255 0	Mansgement Only Fils Péo Pio Yes	MTU 1500 1500	Description	Add Edd

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

🛍 Cisco ASDM	M 5.1 for ASA - 172.16.26.2	10 10 10 10 10 10 10 10 10 10 10 10 10 1
File Rules S	Search Options Tools Witzards Help	fores foreign
C)	Configuration Monitoring Data Forward Search Referent Save Help	A.A.
	Configuration + Security Policy - Senice Policy Rules	
Ξ,	◆ 出 平1回1日1月 時 総 勤 罰 (金)	
Interfaces	C Access Rules C AAA Rules C Filter Rules C Senice Policy Rules	
Security Policy	Show Rules for interface: All interfaces  Show All	
24	Traffic Classification Pule Actions Description	Add
NAT	Name Enabled Match Source Destination Service Time Range	Edt
3	inside class Do any any traffic Up pormisculus, permit traffic	Delete
VPN		
CSD Manager		
PS PS		
-25		
Routing		
Second Chinese		
Properties		
	Dig Match and C Show Summary C Show D	stait
	Apply Reset Advanced	
	*admin> NA.(15) 🏨 🔒 🔒 7/31/06	3.02.47 PM UTC

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.

🖆 Add Service Policy	Rule Wizard - Service Policy						
Adding a new service r	policy rule requires three steps:						
Sten 1: Configure a service policy							
Step 1. Configure a service pointy.							
Step 3: Configure actio	ons on the traffic classified by the service policy rule.						
. 2							
Create a service poli	cy and apply to:						
Interface:	inside - (create new service policy)						
L Policy Name:	inside policy						
Foncy Name.							
Description:	DS-inside-policy						
C Global - applies	to all interfaces						
Policy Name:	dippal-policy						
i oney 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: inside-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.	
< Back   Next ≻	Cancel Help

6. أتمت هذا AIP-SSM الخاص به.تحقق من تمكين ASA لتوجيه حركة المرور إلى AIP-SSM الخاص به.تحقق من تمكين IPS التدفق 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 من حركة المرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات.طقطقة يسمح حركة مرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات.طقطقة يسمح حركة مرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات.طقطقة يسمح حركة مرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات.طقطقة يسمح حركة مرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات.طقطقة يسمح حركة مرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات.طقطقة يسمح حركة مرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات.طقطقة يسمح حركة مرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات.طقطقة يسمح حركة مرور إلى الوحدة النمطية خارج النطاق بدلا من وضع الوحدة النمطية داخل تدفق البيانات.طقطقة يسمح حركة مرور إلى الماد من وفي إلى حالة فشل-مفتوح في حالة أن الماد منور إلى يفشل.طقطقة إنجاز أن الماد التغيير.

🚰 Add Service Policy I	Rule Wizard - Rule Actions		
Protocol Inspection	Intrusion Prevention Connection Settings	QoS	Ì
Mada	this traπic flow		
In this mode as a result o	e, a packet is directed to IPS and the packet may If IPS operation.	be dropped	
• Promiscous	Mode		
In this mode be dropped	e, a packet is duplicated for IPS and the original p by IPS.	acket cannot	
If IPS card fails	, then		
<ul> <li>Permit traffic</li> </ul>			
C Close traffic			
		< Back Finish	Cancel Help

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.

🛍 Cinco ASDM 🤉	i.1 fer AS	4 - 172,16,2	6.2										
File Rules Se	arch_Opti	ans Tools V	Weards He	sip	=		-	-					
	-	e Mandania	. 9			Carlos Carlos		3					di di
1010	Design fills	in states	i i i i i i i i i i i i i i i i i i i	A 10	- 51415	ato: haree	3818	- map					PILINEITA.
	• •	<b>∓∣</b> α/101	1.5.45 倍	化菜	6								
inter faces	C Acc	ess Rules	C AAA Rules	C FI	ler Rules	C Service Policy	Rules						
6.	Show F	ules for interi	ace: All Inte	dacas	• Bh	ow All							
Security Policy					Traffic (	Classification							Add
12	*	Name	Enabled	Match	Bourbe	Destination	6	service -	Tims Range	Hu e Actions		Description	Edit
100	E M:	face: inside, F	<sup>a</sup> cticy: inside	policy Dec	<b>A</b>	2				101 in the second s	IDS inside policy		Dalata
VPN	- 1	TO DO CHISO			any any	- a 19	: any i	1489.		Gript promotorus, parma re	ant		
<u>A</u>													
CSD Hanager													
۵,													
Section 1													
.en													
Giolad Objects													
3													
Properties													
	1												
	Den N	sich	Don	of match								Show Summary	ary C. Binow Detail
					Apply	Resel		Assess	et.				
Configuration sha	inges save	d successfully		_							<admin></admin>	NA (15)	a 7/31/06 2:54 47 PM UTC

# <u>شكلت AIP-SSM ل حركة مرور تفتيش</u>

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



3. مكنت

														القارن.
Cisco IDM 5	.0 - 172.16.2	6.10												
File Help														
Configuration	Montoring	G Back	Forward	Retresh	? Help									Cesco Systems
G Sensor S     G	Albert States Configuration sates Configuration sates Flow Notification gamma States Sensor Variables Definition sare Variables Definition sare Variables properties Login Profiles sig Devices al Cenfiguration Cenfiguration Sensor selocking Devic Blocking Devic Blocking Devic Blocking Devic Blocking Devic Sensor selocking Devic Sensor selocking Devic Sensor selocking Devic Sensor selocking Devic Sensor selocking Devic Sensor selocking Devic Blocking Devic Sensor selocking Devic Sensor selocking Devic Sensor selocking Devic Sensor selocking Devic Sensor Sen	ins on zard s te interface: or		Interfaces	nterface muu g Enable or ( ce Name hermet2/1	t be enabled inable. Enabled Yes	And assigned to Media Type Elecoptane in	a vitual sensi	In before the set	Abemake TCP Reset Interface -None-	erface. You can enablek	Isable the available sensing	j interfaces by select	Ing the row(s)
OM is initialized	successfully.											1	cisco admin	istrator     🔒

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 sensor show tls fingerprint 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

Come Street on A	MONITOR WI	ANS CONT	OLLER WIF	ELESS S	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Sensor E	dit						
General RADIUS Authentication	Index	2						
RADIUS Accounting Local Net Users	Server Addre	ss 172.16.	26.10					
Disabled Clients User Login Policies	Port	443						
AP Policies Access Control Lists	Username	controlle	ŀf					
IPSec Certificates CA Certificate	Password	•••••			]			
Web Auth Certificate	State							
Wireless Protection Policies Trusted AP Policies	Query Interv	al 10	seconds					
Roque Policies Standard Signatures	Fingerprint (PHA1 back)	98C996	984EFA74F0528	092888C40	13C4584876	CSS 40 hex	chars	
Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MPP Management Frame Protection	Last Query (count)	(hash ki Success	(1400)	ŋ				
Web Login Page								
CIDS Sensors Shunned Clients								

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

										.VVL
A A	MONITOR	WLANS	CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	неця		
Security	CIDS Sens	iors List								
IAA	Index		erver Address	Port	State	Query Int	erval Last	Query (count)		
General RADIUS Authentication	1	1	92.168.5.2	443	Enabled	15	Unau	thorized (1)	Detail	Remove
RADIUS Accounting	2	1	72.16.26.10	443	Enabled	10	Succ	ess (1444)	Detail	Remove
MAC Filtering Disabled Clients User Login Policies AP Policies										
ccess Control Lists										
PSec Certificates CA Certificate ID Certificate										
Veb 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										
Sensors Shunned Clients										

# 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.

ie Help											
enfiguration Monitoring Dack For	ward Refres	📍 h Help									Cisco Si
Q Sensor Setup - SNetwork - SAllowed Hosts	Select By	Configuration	n tures 💌 Select Criteria: 🖡	-104							
e G SSH O Centicates	Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity Rating	Type	Engine	Retired	- Select A
- Sutara	1330	2	TCP Drop - Urgent Pointer WL	No	Modify Packet I	Informatio	100	Default	Normalizer	No	NSDB LK
9, Interface Configuration	1330	11	TCP Drop - Timestamp Not A	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Add
- Ninterfaces	1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Circa
- Sunterface Pairs	1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	
Traffic Flow Notifications	2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Edt
Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Enable
- Nirtual Sensor	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	
Circatus Defailon	2002	0	ICMP Redeert	Vec	Produce Alart	Minh	100	Tuned	Atomic 1D	No	Unsable
Signature Variables	1000		Polar Poroneon	165	Produce Prett	r ng n	100	Tomed	Page of P	140	Actions
Bignature Configuration	2004		ICMP Echo Request		Request Block	High					Restore Det
- OCustom Signature Wizard	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	
- The Miscellaneous	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Defete
Sevent Variables	2007		ICMP Tonestamo Result	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Activate
Target Value Rating	2007	0	CMP Treastane Dask	No	Produce Alert	Induces also	100	Cudwall	Alternation (C)	-40	
-SEvent Action Overrides	2008	ų	nume constants reply	P40	Produce Alert	emperiatop	100	Denaux	Access IP	r#p	Retre

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.
🧣 Edit Signa	sture					devievievieviev	avera esta esta est	×
Name		Value						<u> </u>
Signa	ture ID:	2004						
SubSi	ignature ID:	0						
🔶 Alert S	everity:	High 💌						
📕 Sig Fi	delity Rating:	100						
Promi	iscuous Delta:	0						
Sig D	escription:							
		Signature Name: IOMP	Echo Request					
		Alert Notes:						
		User Comments:						
		alart Traiter						
		Release:						
🕒 Engin	e:	Alomic IP						
		Event Action:	Produce Ale Produce Ver Request Blo Request Blo Request Blo	t Sk Connector				
		Fragment Status:	Any	w.				
		Specify Layer 4 Protoco	Nt Yes -					
			🖯 🗖 Layer	4 Protocol:	ICMP Protocol	<u>*</u>		
					Specify IC	MP Sequence:	No 👻	
					🕒 🔳 Specify IC	MP Type:	Yes v	
							ICMP Type:	8
					Specify IC	MP Code:	No 💌	
					Bpecify IC	MP Identifier:	No 💌	
					Specify IC	MP Total Length:	No 👻	
11		·						•
Parame	eter uses the De	afault Value. Click the icon to ed	lit the value.					
Parame	eter uses a Use	r-Defined Value. Click the icon	to restore the default	value.				
			0K	Cancel	Help	$(2,2)\in \{0,1\}$		

🔍 Edi	it Signature		$\mathbf{X}$
	Name	Value	-
	Signature ID:	2004	
	SubSignature ID:	0	
	Alert Severity:	Informational 💌	
	Sig Fidelity Rating:	100	
	Promiscuous Delta:	0	
Θ	Sig Description:		
		Signature Name: ICMP Echo Request	
		Alert Notes:	
		User Comments:	
		Alert Traits: 0	
		Release: 81	
Θ	Engine:	Atomic IP	
		Event Action:     Request Block Connection     Request Block Host     Request Snmp Trap     Reset Tcp Connection	
•		Franment Status:	•
•	Parameter uses the D Parameter uses a Use	efault Value. Click the icon to edit the value. er-Defined Value. Click the icon to restore the default value.	
		OK Cancel Help	

- 3. طقطقة **ok** in order to أنقذت التوقيع.
- 4. تحقق من أن التوقيع نشط ومن أنه تم تعيينه لتنفيذ إجراء حظر.
  - 5. انقر فُوقٌ **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 على الجانب الأيسر، حدد **كتل المضيف النشطة**. عندما يتم تشغيل توقيع إختبار الاتصال، تظهر نافذة "كتل المضيف النشطة عندما يتم تشغيل توقيع إختبار الاتصال، تظهر نافذة "كتل 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 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.

Cisco IDM 5.0 - 172.16.26.10		
File Help		
Configuration Meniliaring Back Forward Retresh	Pep	Cinco Statues
- Denied Attackers	Active Host Blocks	
- Active Host Blocks		
Network Blocks     Network Blocks	Specify the address to block and the duration for that block.	
- Revents		
E Q Support Information	Source IP Destination IP Destination Port Protocol Minutes Remaining Timeost (minutes) VLAN Connection Block Enable	Add
- Distatistics	50.10.99.26 10.10.10.2.1 0 t 30 36 0 failse	J
System Information		Delete
	Refresh	
	Last Updated, 7721	1/06 3:21:04 PM
IDM is initialized successfully.	cisco admi	nistrator 👘 🙆

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 ع.م

onfiguration Monitoring	Back	Forward	Refresh	📍 Help
Denied Attackers Active Host Blocks Network Blocks NP Logging Network Blocks NP Logging Notation Diagnostics Report Statistics Disystem information				Events         You can display the events in the local Event Store. By default all events are displayed. To filter on event type and/or time, pelect the appropriate check boxes.         Show allert events:       Informational       Low       Medium       High         Show allert events:       Informational       Low       Medium       High         Show allert events:       Informational       Low       Medium       High         Show allert events:       Warning       Error       Fatal         Show Network Access Controller events       Select the number of the rows per page.         Show status events       100       Image: Show all events currently stored on the sensor         Show past events:       1       hours       Image: Start Time (UTC)         Franz       Image: Ima

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

-	1300	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	
						Refres

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

Details for 1145383740954941597 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=0UT 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

التوقيع.

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

Class Brancas	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shu	n List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Re-sync IP Addres 10.10.99.2	is La 6 00	ast NAC Address 0:40:96:ad:0d:1b	Expire 27	Sen: 172.	tor IP / Index 16.26.10 / 2		
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 / MPP Manegement Frame Protection Web Login Page								
CIDS Sensors Shunned Clients								

تتم إضافة المستخدم إلى قائمة "إستبعاد العميل".

Core Presses	MONITOR V	VLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Monitor Summary Statistics Controller Ports Wireless Roque APs Known Roque APs Roque Clients Adhoc Roques 802.311 a Radios 802.311 b/g Radios Clients RADUS Servers	Excluded Clic Search by M Client NAC A 00:40:96:adi0	erits AC address Addr AP 1 Dd:1b AP0	Name 014.6940.81ce	AP NAC Ad 00:14:15:54	Search Idr WLAN h:16:40 IPS	Туре 802.1	Exclusio	n Reason Inum:S	Port 29	Detail UnkTest Disable Remove

# <u>مراقبة الأحداث في WCS</u>

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**.

Cisco Wireless Control S	ystem			Username: root Logout Refresh Print View
Monitor • Configure • J	Location - Administration - Help -			
Alarms	Alarms			Select a command 💌 😡
Severity Critical v Alarm Category All Types v Search	Severite         Failure_Object           Critical         Sadio_ABR:LAP1242AG:AC1           Critical         Radio_ABR:LAP1242AG:AC2           Critical         AP_ABR:LAP1242AG:AC1           Critical         Radio_ABR:LAP1242AG:AC2           Critical         AP_ABR:LAP1242AG:AC1           Critical         AP_ABR:LAP1242AG:AC1           Critical         AP_ABR:LAP1242AG:AC2           Critical         AP_ABR:LAP1242AG:AC1:L15:5141:E0           Critical         Radio_abr:T5:12:e0/20           Critical         AP_ABD:25:12:e0/20:105:57:51:2:e0           Critical         AP_ADD:3:10:92:0622(00:13):55:75:12:e0           Critical         AP_ADD:3:10:92:00:13):55:72:41:40           Critical         AP_ADD:3:10:92:00:13):55:72:41:40           Critical         AP_ADD:3:10:92:00:13):55:72:41:40           Critical         AP_ADD:3:0:92:00:13):55:72:41:40           Critical         AP_AD:acc:c3750:48:1-FE1:0-3/2           Critical         AP_AD:acc:c3750:48:1-FE1:0-3/2           Critical         AP_AD:acc:c3750:48:1-FE1:0-3/1           Critical         AP_AD:acc:c3750:48:1-FE1:0-3/1	Dwner	Date/Time 6/1/06 9:02 AM 6/1/06 9:02 AM 6/1/06 9:02 AM 7/21/06 1:51 PM 7/21/06 1:51 PM 7/21/06 1:51 PM 7/21/06 4:32 PM 7/21/06 6:33 PM 7/21/06 5:25 PM 7/26/06 2:02 PM 7/26/06 2:02 PM	AP 'AIR-LAP1242AG-A', interface '802.11b/g' is         AP 'AIR-LAP1242AG-A', interface '802.11a' is do         AP 'AIR-LAP1242AG-A', disassociated from Control         AP 'api.75121e0', interface '802.11a' is down         AP 'api.40' other attack may be in progress. Rog         Fake AP or other attack may be in progress. Rog         AP 'AP-aco-03750-48-1-FE1-0-3', interface '802         AP 'AP-aco-03750-48-1-FE1-0-3' disassociated fr         AP 'AP-aco-03750-48-1-FE1-0-3' disassociated fr
Reques     0     282       Coverage     0     0       Security     2     0     4       Controllers     1     0     0       Access Points     0     3				

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 آن-

Cisco Wireless Control System Username: root Logout Refresh Print V									
Monitor • Configure • Location • Administration • Help •									
Alarms	Alar	ms					Select a command :		
Severity Minor		Severity	Failure Object	Owner	Date/Time	Message			
Name Calence		Minor	Client 00:09:ef:01:40:46		7/19/06 6:30 PM	The WEP Key configured at the station may be wr			
Security		Minor	Client 00:40:96:ad:0d:1b		7/26/06 2:47 PM	The WEP Key configured at the station may be wr			
(		Minor	Client.00:90:7a:04:6d:04		7/31/06 2:36 PM	Client '00:90:7a:04:6d:04' which was associated			
Search		Minor	Client 00:40:96:ad:0d:1b		7/31/06 4:25 PM	Client '00:40:96:ad:0d:1b' which was associated,			
	Cilent 100,40.985.ed.04116' which was associated with AP 100.14.1br.5a.10.40', interface 10' is excluded. The reason code is "S(Uninown)".								



```
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
                                                                      1
                                     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
                                                                      !
                                                                      Т
                                              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

### <u>تكوين عينة مستشعر نظام منع الاقتحام Cisco Intrusion Prevention System Sensor</u> 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 10.0.0/8 access-list 40.0.0/8 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

## <u>التحقق من الصحة</u>

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

# <u>استكشاف الأخطاء وإصلاحها</u>

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

### <u>معلومات ذات صلة</u>

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

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما