# CS-MARS - إضافة مستشعر IPS وتكوينه إعداد جهاز كمضيف

## المحتويات



## المقدمة

يشرح هذا المستند كيفية إعداد جهاز Cisco لنظام منع التسلل الآمن (IPS) وأي أجهزة إستشعار افتراضية تم تكوينها للعمل كأجهزة إرسال تقارير إلى نظام Cisco لمراقبة الأمان والتحليل والاستجابة (CS-MARS).

## المتطلبات الأساسية

### المتطلبات

بالنسبة لأجهزة Cisco IPS 5.x و 6.x و x.7، تقوم MARS بسحب السجلات باستخدام SDEE عبر SSL. لذلك، يجب أن يكون لدى MARS وصول HTTPS إلى المستشعر. لتجهيز المستشعر، يجب تمكين خادم HTTP على المستشعر، وتمكين TLS للسماح بوصول HTTPS، والتأكد من تعريف عنوان IP الخاص ب MARS كمضيف مسموح به، مضيف يمكنه الوصول إلى أحداث المستشعر والسحب. إذا تم تكوين أجهزة الاستشعار للسماح بالوصول من البيئات المضيفة المحدودة أو الشبكات الفرعية على الشبكة، فيمكنك إستخدام الأمر **access-list ip_address/netmask** لتمكين هذا الوصول.

### المكونات المستخدمة

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

- جهاز Cisco Secure MARS الذي يشغل الإصدار x.4.2 من البرنامج والإصدارات الأحدث
- جهاز Cisco 4200 Series IPS الذي يشغل الإصدار 6.0 من البرنامج والإصدارات الأحدث

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

## المنتجات ذات الصلة

يمكن إستخدام هذا التكوين أيضا مع أجهزة الاستشعار هذه:

- IPS-4240
- الطراز IPS-4255
- IPS-4260
- IPS-4270-20

## الاصطلاحات

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

# التكوين

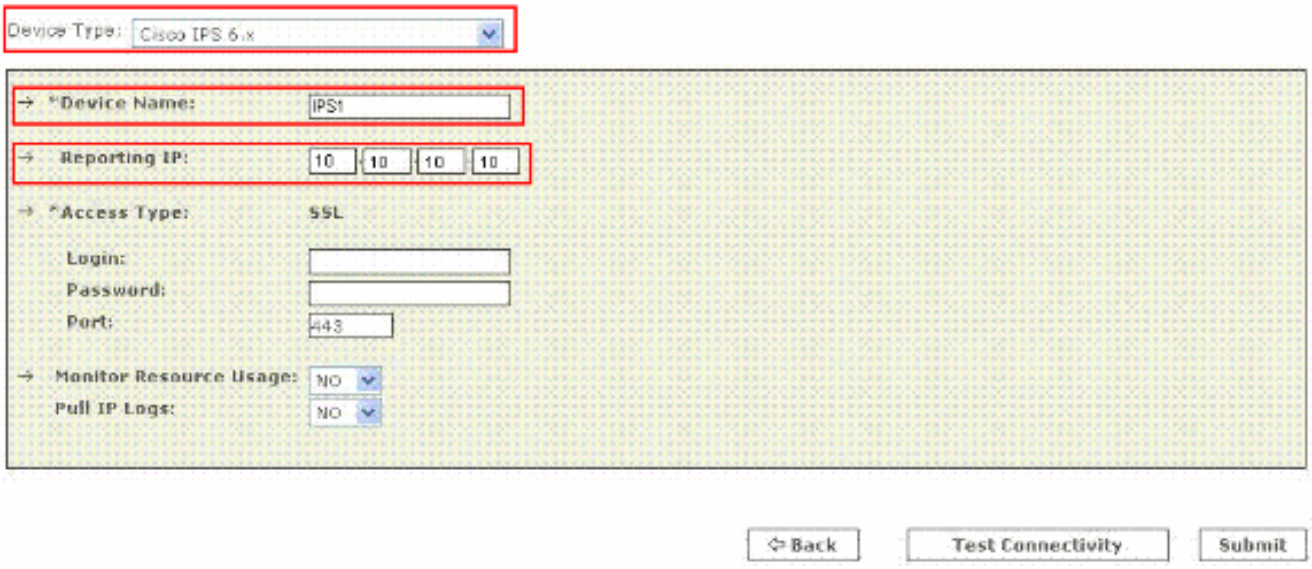
في هذا القسم، تقدم لك معلومات حول كيفية إضافة مستشعر Cisco لنظام منع التسلل الآمن (IPS) وتكوينه إلى جهاز Cisco لمراقبة الأمان والتحليل ونظام الاستجابة (CS-MARS).

## إضافة جهاز Cisco IPS 6.x أو x.7 وتكوينه في MARS

عند تحديد جهاز Cisco IPS 6.x أو x.7 في MARS، يمكنك اكتشاف أي أجهزة إستشعار افتراضية تم تكوينها على الجهاز. وعندما تكتشف هذه المجسات الافتراضية، يسمح هذا ل MARS بفصل الأحداث التي تم الإبلاغ عنها عن طريق المجس الظاهري. كما أنها تسمح لك بضبط قائمة الشبكات المراقبة لكل مستشعر ظاهري، مما يحسن من دقة التقارير المطلوبة.

أتمت هذا steps in order to أضفت وشكلت cisco IPS 6.x أو x.7 أداة في MARS:

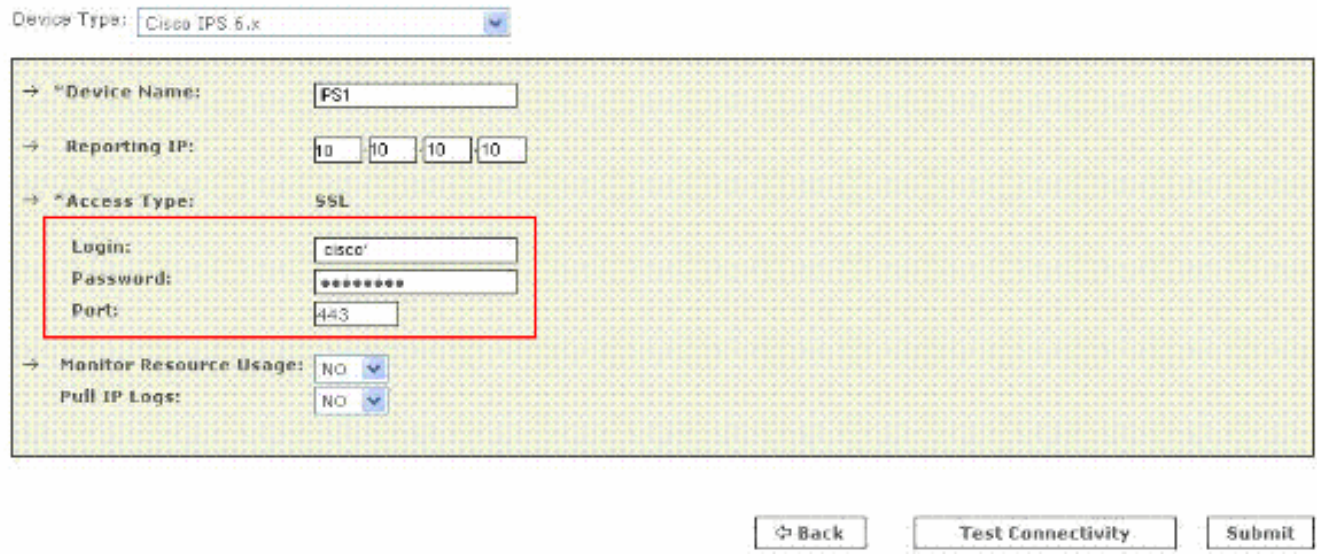
1. أختر **مسؤول > إعداد النظام > الأمان وأجهزة المراقبة**. ثم انقر على **إضافة**.
2. أختر **Cisco IPS 6.x أو Cisco IPS 7.x** من قائمة نوع الجهاز. أدخل الآن اسم المضيف للمستشعر في حقل **اسم الجهاز** كما هو موضح هنا. IPS1 هو اسم الجهاز المستخدم في هذا المثال. يجب أن تكون قيمة اسم الجهاز مطابقة لاسم المستشعر الذي تم تكوينه.




دخلت الآن العنوان إداري في **التقرير ip** مجال. عنوان IP الخاص بالتقارير هو نفس عنوان IP الإداري.

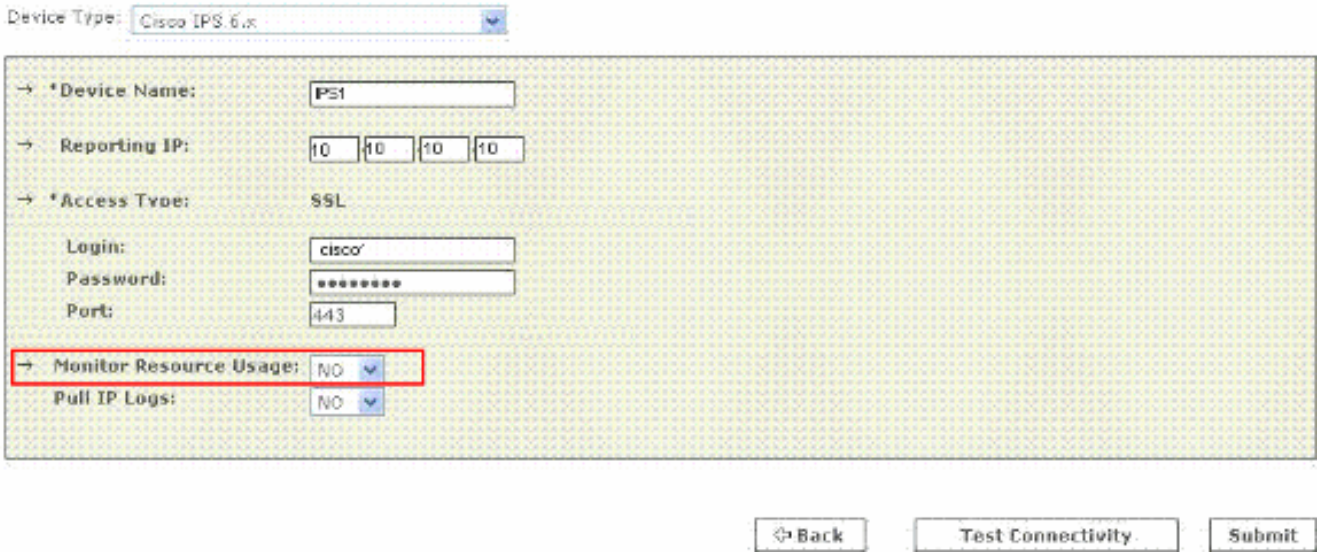
3. في حقل **تسجيل الدخول**، أدخل اسم المستخدم المقترن بالحساب الإداري الذي يتم إستخدامه للوصول إلى

جهاز التقارير. الآن، في **حقل كلمة المرور**، أدخل كلمة المرور المرتبطة باسم المستخدم المحدد في **حقل تسجيل الدخول**. **ال username cisco** وال **كلمة** يستعمل **cisco123** في هذا مثال. أدخل أيضا رقم منفذ TCP الذي يستمع إليه خادم الويب الذي يعمل على المستشعر في **حقل المنفذ**. منفذ HTTPS الافتراضي هو 443.

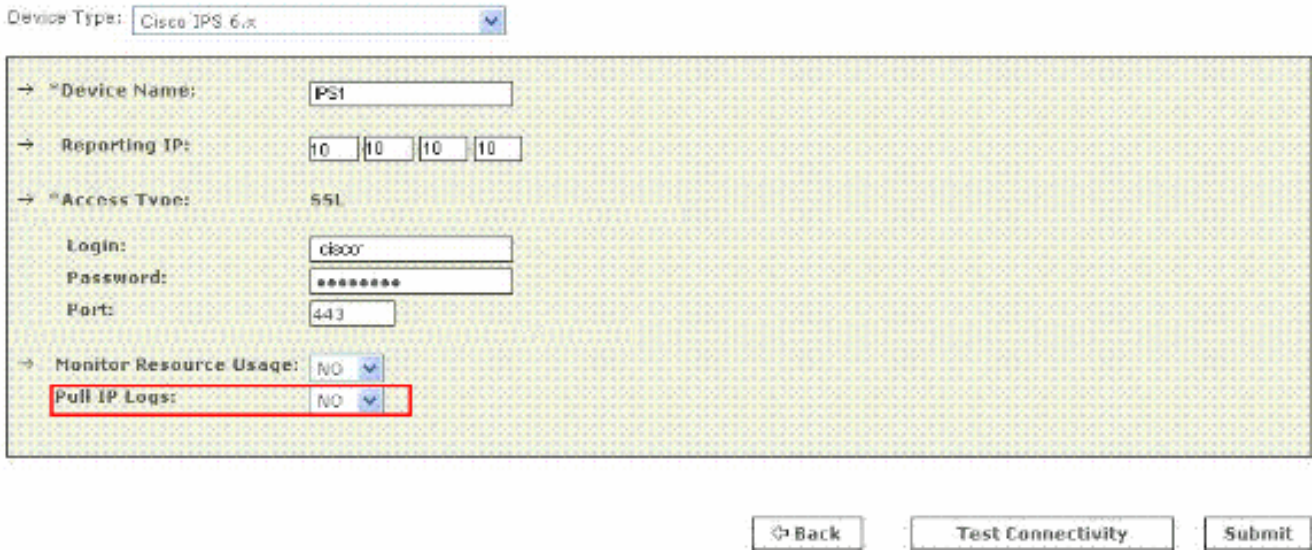



**ملاحظة:** بينما من الممكن تكوين HTTP فقط، فإن MARS يتطلب HTTPS.

4. تحقق الآن من إختيار **NO** في قائمة **إستخدام موارد المراقبة**. بينما يظهر خيار "مراقبة إستخدام الموارد" على هذه الصفحة، فإنه لا يعمل ل Cisco IPS.

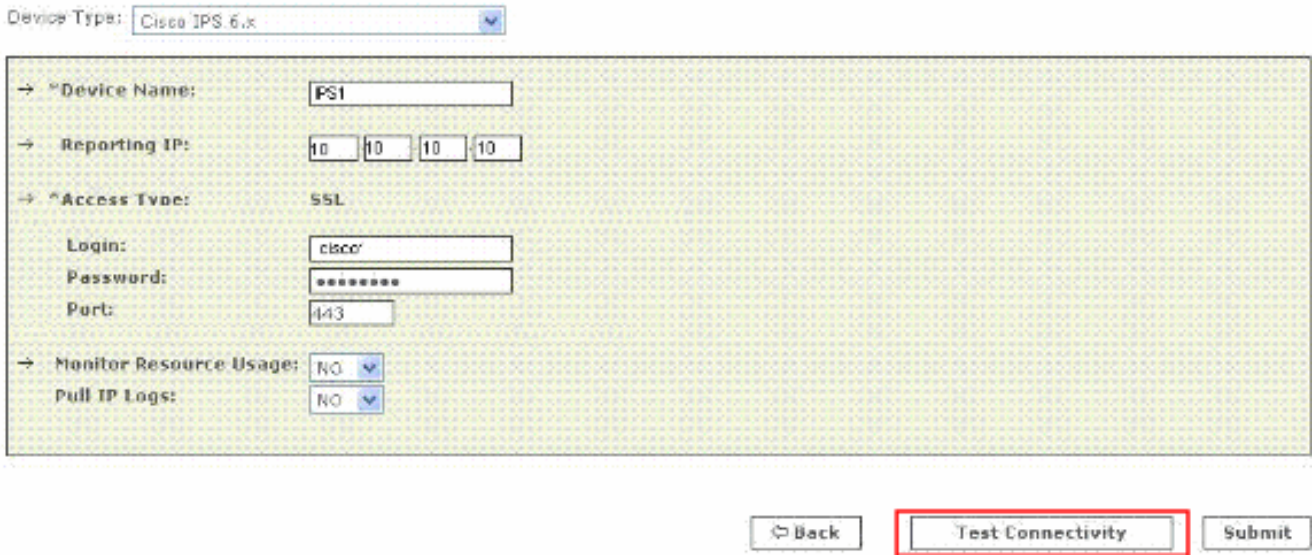



5. لسحب سجلات IP من المستشعر، أختر **نعم** من قائمة **سحب سجلات IP**. هذا سمة إختياري، أي يستطيع كنت استعملت إن يتطلب.

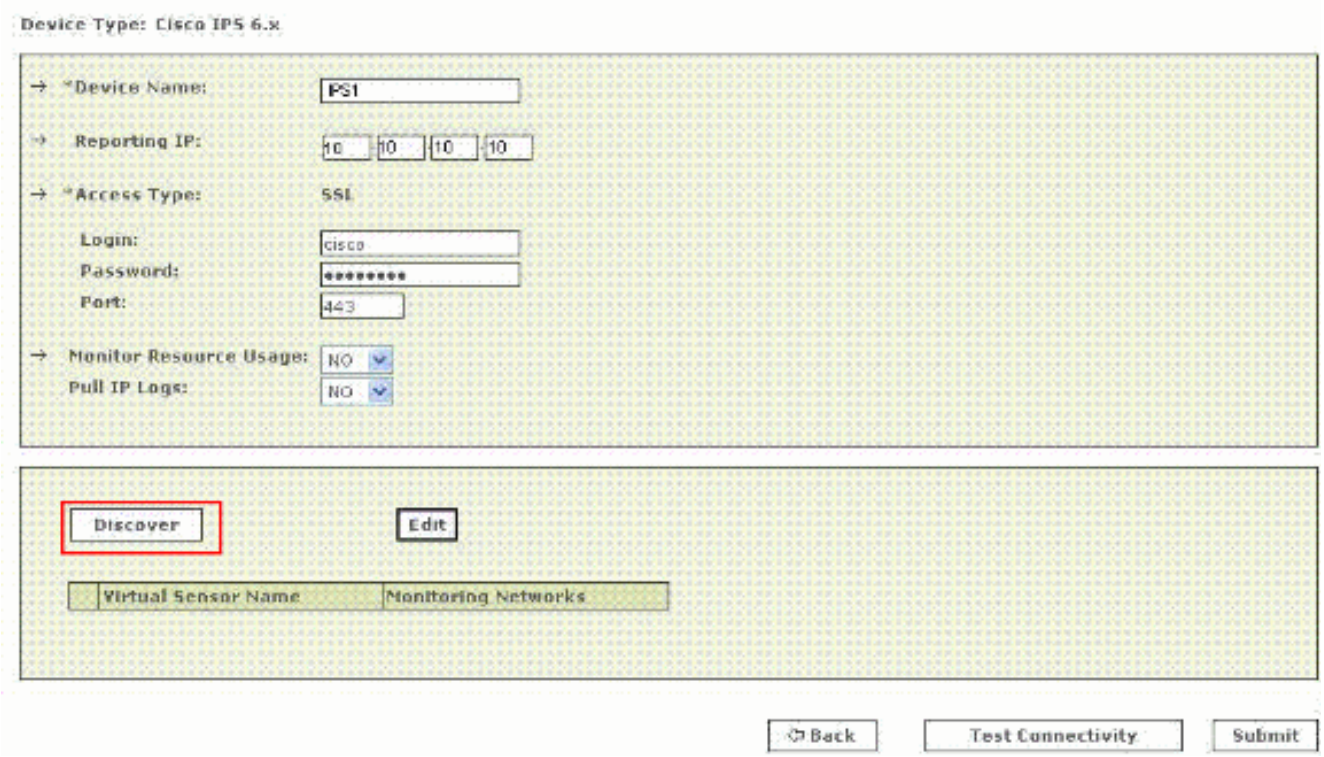



ينطبق هذا الإعداد على المستشعر بأكمله، والذي يتضمن السجلات التي تم إنشاؤها لتنبيهات أجهزة الاستشعار الظاهرية.

6. انقر فوق **إختبار الاتصال** للتحقق من التكوين وتمكين اكتشاف أجهزة الاستشعار الظاهرية.

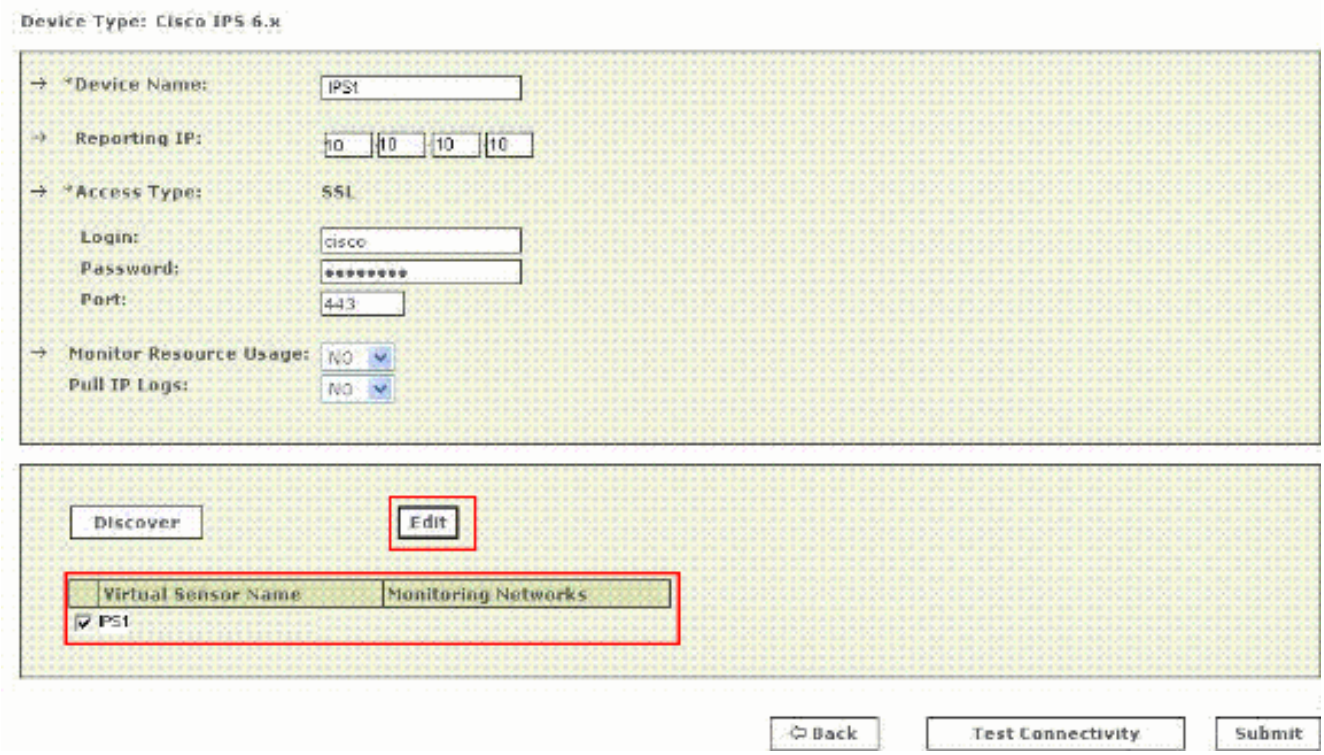



7. انقر فوق **اكتشاف** لاكتشاف أي أجهزة إستشعار افتراضية معرفة.

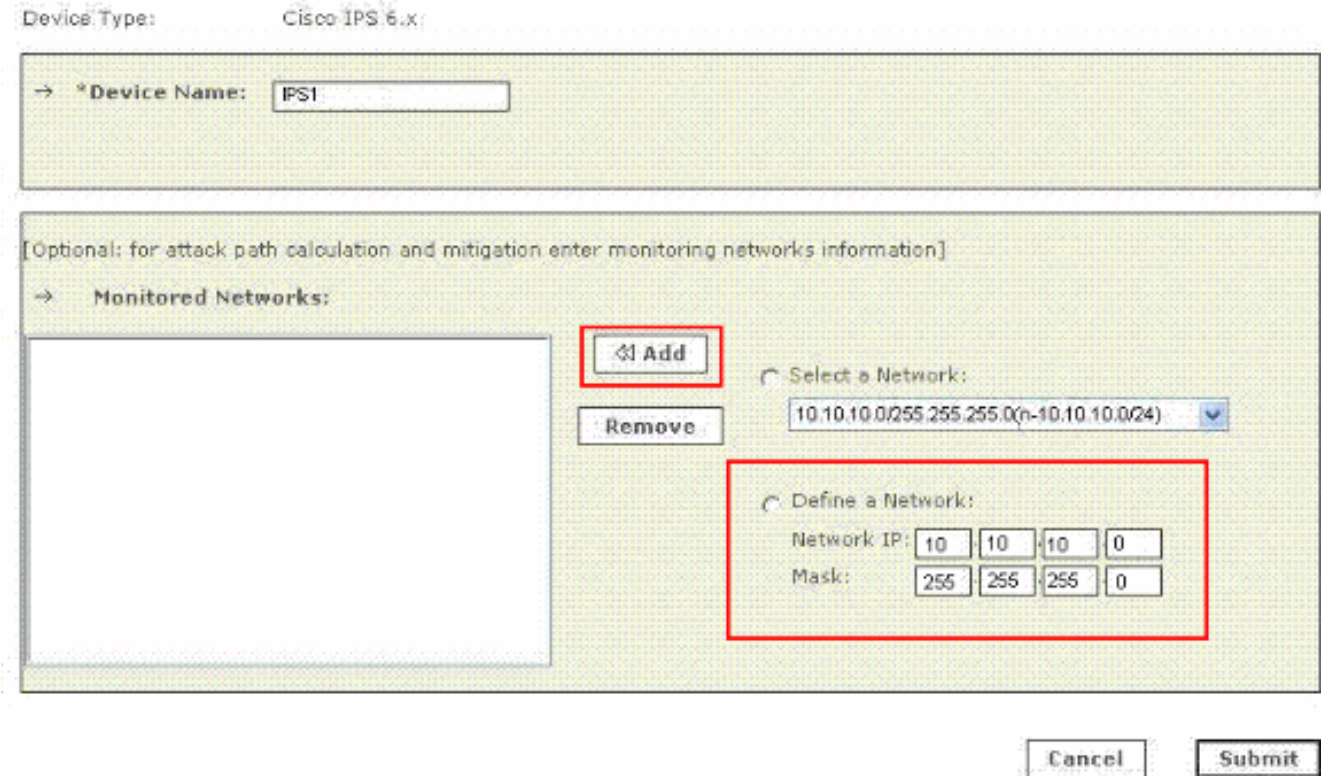



**ملاحظة:** لا يعلم MARS بالتغييرات التي أجريت على المستشعر. في أي وقت تقوم فيه بإجراء تغييرات على إعدادات المستشعر الظاهري، يجب النقر فوق **اكتشاف** في صفحة تكوين المستشعر هذه لتحديث تفاصيل المستشعر الظاهري في MARS.

8. أختر خانة الاختيار المجاورة لاسم المستشعر الظاهري وانقر فوق **تحرير** لتحديد الشبكات المراقبة لكل مستشعر ظاهري. الآن تظهر صفحة وحدة IPS النمطية كما هو موضح هنا.

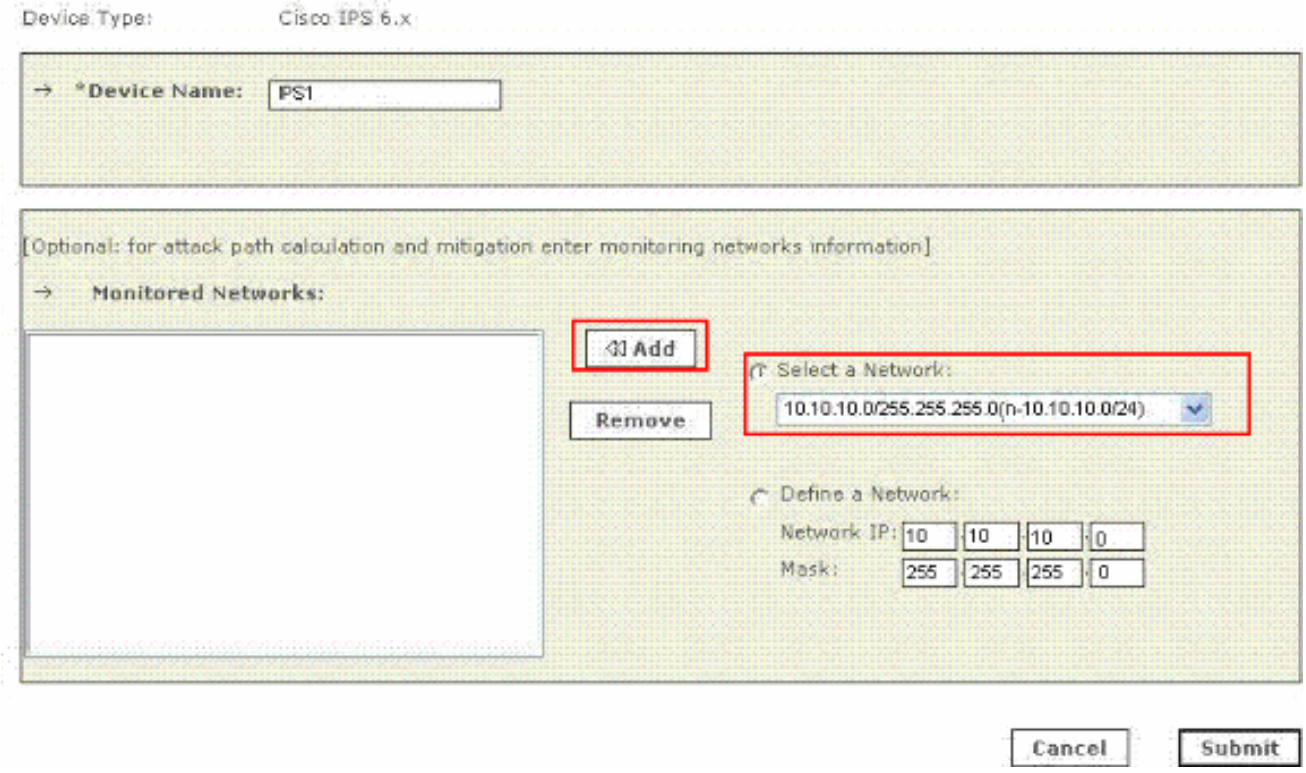



9. لحساب مسار الهجوم والتخفيف من آثاره، حدد الشبكات التي يتم مراقبتها بواسطة المستشعر. أختر زر **تعريف** راديو **شبكة** من أجل تعريف الشبكة يدويا. ثم أكمل الخطوات التالية لتعريف شبكة:دخلت الشبكة عنوان في **الشبكة ip** مجال.أدخل قيمة قناع الشبكة المقابلة في حقل **القناع**.طقطقة **يضيف** in order to نقلت الشبكة يعين داخل ال monitore شبكة مجال.كرر الخطوات السابقة إذا كانت هناك حاجة لتعريف المزيد من الشبكات.




**ملاحظة:** هذه ميزة إختيارية متوفرة ويمكن تخطيها إذا لم تكن مطلوبة.

10. انقر على زر **تحديد** راديو **شبكة** لتحديد الشبكات المتصلة بالجهاز. بعد ذلك أتمت هذا steps in order to أخترت الشبكات:أختر شبكة من قائمة **تحديد شبكة**.طقطقة **يضيف** in order to نقلت الشبكة يعين داخل ال monitore شبكة مجال.كرر الخطوات السابقة إذا كانت هناك حاجة لاختيار المزيد من الشبكات.




**ملاحظة:** هذه ميزة إختيارية متوفرة ويمكن تخطيها إذا لم تكن مطلوبة.

11. كرر **الخطوة 8** حتى **الخطوة 10** لكل مستشعر ظاهري.
12. انقر فوق **إرسال** لحفظ التغييرات التي قمت بها. يظهر اسم الجهاز ضمن قائمة معلومات الأمان والمراقبة. تقوم عملية الإرسال بتسجيل التغييرات في جداول قاعدة البيانات. ولكنه لا يحمل التغييرات في ذاكرة العمل الخاصة بجهاز MARS. قامت عملية التنشيط بإرسال التغييرات إلى ذاكرة العمل.
13. انقر فوق **تنشيط** لتمكين MARS لبدء تجزئة الأحداث من هذا الجهاز.تبدأ MARS في عقد جلسات للأحداث

الناتجة عن هذه الوحدة النمطية وتقييم تلك الأحداث باستخدام قواعد الفحص والإفلات المحددة. يمكن الاستعلام عن أي أحداث تم نشرها بواسطة الجهاز إلى MARS قبل التشيط باستخدام عنوان IP الخاص بالإبلاغ كمعيار مطابقة. ارجع إلى تنشيط أجهزة إعداد التقارير والتخفيف. للحصول على مزيد من المعلومات حول إجراء التشيط.

## التحقق من قيام MARS بسحب الأحداث من جهاز Cisco IPS

من الشائع إنشاء أحداث حميدة على الشبكة للتحقق من تدفق البيانات. أكمل هذه الخطوات للتحقق من تدفق البيانات بين جهاز Cisco IPS و MARS:

1. على جهاز Cisco IPS، قم بتمكين التوقيعات 2000 و 2004 والتنبيه لها. تراقب التوقيعات رسائل ICMP (إختبارات الاتصال).
2. يؤز جهاز على الشبكة الفرعية التي يستمع إليها جهاز Cisco IPS. هذه الأحداث تم توليدها وسحبها بواسطة المريخ.
3. تحقق من ظهور الأحداث في واجهة ويب MARS. يمكنك إجراء استعلام باستخدام جهاز Cisco IPS.
4. بمجرد التحقق من تدفق البيانات، يمكنك تعطيل توقيعات 2000 و 2004 على جهاز Cisco IPS.**ملاحظة:** إذا لم تفشل عملية الاتصال بالاختبار أثناء تكوين جهاز Cisco IPS في واجهة ويب MARS، فسيتم تمكين الاتصالات. تتيح لك هذه المهمة التحقق بشكل إضافي من إنشاء التنبيهات وسحبها بشكل صحيح.

## استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

## معلومات ذات صلة

- صفحة دعم نظام مراقبة الأمان والتحليل والاستجابة من Cisco
- صفحة دعم نظام منع الاقتحام من Cisco
- نظام Cisco لمراقبة الأمان والتحليل والاستجابة - معلومات التوافق
- طلبات التعليقات (RFCs)
- 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).