الأسئلة المتكررة حول نظام كشاف الاقتحام الآمن من Cisco (الإصدار 3.1 والإصدارات الأقدم)

المحتويات

المقدمة
عام
مستشعر IDS
مدير UNIX
(IDS Cisco Secure Policy Manager (CSPM
معلومات ذات صلة

المقدمة

يحتوي هذا المستند على الأسئلة المتداولة (FAQs) حول نظام اكتشاف الاقتحام الآمن (IDS) من Cisco، المعروف سابقا باسم NetRanger، الإصدارات 3.1 والإصدارات الأقدم.

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

عام

q. أين يمكنني العثور على معلومات إضافية حول معرفات Cisco الآمنة؟

أ. راجع المجموعة الكاملة لوثائق المنتج للحصول على مزيد من المعلومات حول معرفات Cisco الآمنة.

س. كيف يمكنني تحديث التوقيعات الخاصة بنظام IDS الخاص بي بالكامل (مستشعر IDS + برنامج إدارة IDS)؟

أ. عليك ترقية توقيعات النظام الأساسي "للمستشعر" و"الإدارة" بشكل منفصل. لاحظ أن برنامج الإدارة غير قادر على *التعرف* على التوقيعات من المستشعر، لذا يجب تحديثه أيضا. قم بتنزيل ملف تحديث التوقيع الأحدث لكل تطبيق من Cisco Secure Downloads (العملاء المسجلون فقط). تحتوي ملفات القراءة المتوفرة في نفس الموقع على إرشادات لإجراء الترقية.

س. أين يمكنني العثور على قائمة كاملة من التوقيعات؟

أ. تتوفر قائمة توقيعات المعرفات من خلال موسوعة Cisco الآمنة (العملاء المسجلون فقط).

س. ما هي كلمة المرور الافتراضية للمستخدمين في UNIX IDS والمستشعر المستقل؟

أ. في المستشعر المستقل لنظام UNIX وبرنامج إدارة IDS، كلمة المرور الافتراضية هي "هجوم" للمستخدمين **عبر**

الإنترنت وroot. عند إصدار الأمر **su** ليصبح المستخدم الجذري، تكون كلمة المرور الافتراضية هي "هجوم." في الخادم النصلي لوحدة نظام اكتشاف الاقتحام (IDSM)، كلمة المرور الافتراضية هي "هجوم" لاسم المستخدم **CiscoIDs**.

س. كيف يمكنني الحصول على خادم نصلي لوحدة نظام اكتشاف الاقتحام (IDSM) للتخلص من تكويناته؟

a. تحتاج إلى خادم FTP محلي حتى يمكنك تحميل التكوينات.

1. أدخل هذا الأمر من وضع diag على الخادم النصلي.

```
report systemstatus site user dir
```

2. اكتب **y** للمتابعة عند الطلب "متابعة إنشاء تقرير النظام؟ ".
3. اكتب كلمة مرور FTP الخاصة بالمستخدم المحدد عند مطالبتك بذلك. عند اكتمال العملية، تتلقى رسالة تشير إلى ما إذا فشلت العملية أو إذا تم إرسال الملف.

س. عند تثبيت/إزالة تثبيت المعرفات، أين توجد ملفات السجل؟

أ. يمكن العثور على سجلات التثبيت/التحديث في هذه المواقع:

- توجد سجلات تثبيت المدير في /var/adm/nrInstall.log.
- توجد سجلات تحديث Sensor Service Pack في /usr/nr/sp-update/.
- توجد سجلات تحديث التوقيع في /usr/nr/sig-update/.

س. ما هي التواقيع المتوفرة على PIX للمعرفات؟

أ. المعرفات متاحة فقط ل PIX 6.0 والإصدارات الأحدث. تحتوي التوقيعات على رسائل syslog من 400000 إلى 400051، ويشار إليها باسم رسائل توقيع معرفات الأمان من Cisco. ارجع إلى وثائق رسائل سجل نظام PIX للحصول على مزيد من المعلومات حول كل توقيع.

س. هل يمكن إعلامي عند إصدار تحديثات التوقيع؟

أ. قم بالتسجيل للحصول على إخطارات التحديث النشطة لمعرف Cisco IDS لتلقي تنبيهات عبر البريد الإلكتروني لأخبار المنتج المتعلقة بمعرفات Cisco الآمنة.

س. ما التطبيقات التي يجب إستخدامها لإدارة مستشعر بطاقات الهوية، وما الفرق بينها؟

a. قبل الإصدار 3.1، تكون خيارات الإدارة هي إستخدام مدير السياسة الآمنة (CSPM) من Cisco أو مدير UNIX. يكمن الاختلاف الرئيسي بين الطرازين في تشغيل CSPM كتطبيق مستقل على خادم Windows، بينما يعمل مدير UNIX فوق OpenView من HP على خادم UNIX Solaris. باستخدام IDS 3.1، يمكن أيضا إدارة أجهزة الاستشعار من خلال عارض أحداث IDS (IEV) المثبت على جهاز الكمبيوتر أو باستخدام مدير أجهزة IDS، والذي هو جزء من مستشعر الإصدار 3.1. يتم تمكين "إدارة الأجهزة" بشكل افتراضي باستخدام طبقة مأخذ التوصيل الآمنة (SSL) بعد إعداد المستشعر.

س. من أين يمكنني الحصول على برنامج مجموعة أدوات تطوير البرامج (SDK)؟

ألف - برنامج SDK غير متاح للجمهور.

مستشعر IDS

س. ما هو الفرق بين الإصدارين x.3 و x.4 من المستشعر؟

ألف - يقدم الإصدار 4.0 عدة ميزات جديدة. الميزة الجديدة الأكثر وضوحا هي واجهة سطر الأوامر (CLI) مماثلة ل Cisco IOS®.

س. كيف يمكنني ترميز سرعة الواجهة على المعرفات؟

أ. الإعداد الثابت للسرعة/الإرسال ثنائي الإتجاه في x.3 و 4.0 رمز غير مدعوم وهناك خطأ مقابل طلب الميزة (معرف تصحيح الأخطاء من Cisco CSCdy43054 (العملاء المسجلون فقط). تتوفر الميزة في الرمز 5.0، والذي يتوفر الآن في تكوين الواجهات.

س. كيف يمكنني ترقية برنامج المستشعر من الإصدار 3.0 إلى 3.1؟

أ. يمكن للعملاء تنزيل ملف التحديث للإصدار 3.1 من Cisco Secure Downloads (للعملاء المسجلين فقط).

س. كيف يمكنني ترقية برنامج المستشعر من الإصدار 2.5 إلى 3.0؟

أ. يمكن للعملاء تنزيل ملف التحديث للإصدار 3.0 من Cisco Secure Downloads (للعملاء المسجلين فقط). قم بتثبيت تحديث البرنامج بنفس الطريقة التي يتم بها تثبيت تحديثات مجموعة الخدمة والتوقيع في الإصدار 2.5. يتم وصف الإجراء بالتفصيل في مذكرة تكوين مستشعر Cisco IDS، الإصدار 3.0.

س. كيف يمكنني ترقية برنامج المستشعر من الإصدار 2.2 إلى 3.0؟

a. يمكن تنزيل ملف الترقية 3.0 من تنزيلات Cisco الآمنة (العملاء المسجلون فقط)، ولكن هذا الملف غير قادر على تحديث الإصدارات قبل 2.5. يجب إستخدام القرص المضغوط الخاص بالتحديث/الاسترداد المتوفر من خلال أداة ترقية المنتج (العملاء المسجلون فقط) للترقية من الإصدار 2.2 إلى 3.0. رقم الجزء لهذا القرص المضغوط هو IDS-SW-U.

ملاحظة: يجب أن يكون لديك عقد دعم صالح لطلب القرص المضغوط الخاص بالترقية/الاسترداد.

س. لقد قمت بتوصيل لوحة مفاتيح وجهاز مراقبة بالمستشعر، ولكنه لا يتم تحميله بشكل صحيح. ماذا علي أن أفعل؟

أ. تأكد من أنك تستخدم لوحة مفاتيح وشاشة مدعومين. لا تتوافق بعض العلامات التجارية والطرز مع معرفات Cisco الآمنة وتمنع مستشعر IDS من التمهيد بشكل صحيح. ارجع إلى فشل تمهيد جهاز المعرفات الآمنة من Cisco للحصول على تفاصيل العلامة التجارية المحددة.

q. في قسم المعرفات الخاص ب Cisco Secure Downloads، أرى نوعين من ملفات التحديث (حزمة الخدمة والتوقيع). ما هو الفرق بين هذه الملفات؟

ألف - يحتوي كل ملف من هذه الملفات على مجموعة محددة من تحديثات البرامج أو إضافاتها، على النحو المبين في اصطلاحات التسمية الموضحة هنا.

- يحتوي تحديث حزمة الخدمة لبرنامج جهاز مستشعر IDS على تحسين لبرنامج تطبيق IDS Sensor core بالإضافة إلى إصلاح الأخطاء. على سبيل المثال، يتضمن ملف باسم **IDSk9-SP-3.0-5-S17.bin** تحديثات لإصدار البرنامج 3.0(5) بالإضافة إلى مجموعة التوقيع رقم 17.
- يحتوي ملف تحديث التوقيع على تحديثات التواقيع فقط (بصمات الأصابع الهجومية). على سبيل المثال، يحتوي ملف باسم **IDSk9-sig-3.0-5-S18.bin** على رقم مجموعة توقيع 18 لبرنامج المستشعر 3.0(5).

يمكن للعملاء تنزيل هذه الملفات من موقع التنزيلات الآمنة من Cisco (العملاء المسجلون فقط).

س. كيف يمكنني معرفة ما إذا تم تكوين جهاز إستشعار بشكل صحيح لتجنب الموجه؟

أ. سجل الدخول إلى المستشعر كشبكة **مستخدم** ونفذ هذا الأمر:

```
nrgetbulk
```

يجب أن تتلقى إستجابة مماثلة ل <Active>*IP_ADDRESS*، التي تظهر عنوان IP الخاص بجهاز الرفض المستخدم لحظر الهجمات. يعرض هذا الإخراج مثالا على صياغة الأمر والاستجابة المتوقعة:

```
netrangr@sensor:/usr/nr
nrgetbulk 10003 38 1000 1 NetDeviceStatus<
Active 10.48.66.68
Success
```

يمكنك أيضا تسجيل الدخول إلى الموجه وإصدار الأمر **WHO** لمعرفة ما إذا كان المستشعر قد سجل الدخول.

Q. أنا أستلم رسالة خطأ أن يشير إلى "القيمة لم يتم تعيينها" عند إصدار الأمر nrconns. كيف يستطيع أنا حللت هذا إصدار؟

أ. تشير رسالة الخطأ هذه إلى وجود مشاكل محتملة في ملفات /usr/nr/etc/route/ و/أو /usr/nr/etc/host على جهاز الاستشعار. يعرض الأمر.../route files/ تعرف الاتصالات التي تم تعيينها مؤقتا بين "المستشعر" و"المدير". يعرض الأمر.../hosts files/ تعرف الأسماء وعناوين IP لأجهزة الاستشعار والمخرجين.

يمكنك أيضا تسجيل الدخول كجذر مستخدم، وتشغيل الأمر **sysconfig-sensor**، وإدخال معلومات البنية الأساسية لاتصالات IDS مرة أخرى.

س. كيف يمكنني إستخدام بروتوكول FTP لنسخ ملفات السجلات من أداة الاستشعار لتخزينها في مكان آخر؟

أ. راجع نسخ ملفات سجل IP لعرضها للحصول على مزيد من المعلومات حول هذا الإجراء.

س. ماذا حدث للخوادم المكونة في إصداري برامج المستشعر 2.5 و 3.1؟

أ. Configd هو البرنامج الذي يقوم بمعالجة جميع الأوامر على كل من مديري UNIX وكذلك أجهزة الاستشعار في قاعدة الترميز x.2.2. في قاعدة الرموز 2.5 و 3.0، تم امتصاص هذه الوظيفة في البرامج الأخرى ولم يعد البرنامج الخفي الذي تم تكوينه موجودا.

س. عندما أقوم بتحديث التوقيعات على المستشعر، أحصل على : `NetRanger` . ." رسالة الخطأ. ماذا يجب أن أفعل حيال هذا؟

أ. قم بتحرير ملف /usr/nr/etc/daemons على المستشعر لضمان أن nr.packetD موجود في قائمة الأجهزة المساعدة. ثم قم بإيقاف تشغيل الخدمات.

س. على ال IDS 4210، أي هو التحكم قارن وما هو ال sniffing قارن؟

a. ال control قارن على الأعلى **iprb1**:، وال sniffing قارن على القاع **iprb0**:.

Q. لماذا أرى واجهة واحدة فقط عند إصدار الأمر a - `ifconfig` على المستشعر؟

a. يجب أن يعرض الأمر **ifconfig** واجهة التحكم فقط. الآخر قارن (ال sniffing قارن) بعد استعملت بالمستشعر، غير أن المستعمل لا يفترض أن يكون قادر أن يراها. إذا كنت بحاجة إلى رؤية هذه الواجهة، فقم بتسجيل الدخول كجذر وأصدر الأمر **ifconfig -a** لتحديد أسماء الواجهة. قم بإصدار الأمر **ifconfig *<interface>*plumb** للتحقق من حالة واجهة معينة.

س. كيف يمكنني ترميز سرعة الواجهة على المستشعر؟

أ. يجب ألا يكون الترميز الثابت لسرعة الواجهة على المستشعر ضروريا ولا يدعمه دعم Cisco التقني. إذا تم تعيين المحول التفاوض التلقائي، فإن الواجهة تتفاوض على السرعة مع المحول الذي ترتبط به. حركة المرور من الشبكة إلى المستشعر أحادية الإتجاه (بمعنى أن المستشعر يستلم). لذلك، يكون مناسبا بشكل عام إذا أظهر المحول أن 100 half-duplex تم التفاوض عليه (افتراض أن منفذ المحول هو 100 م).

مدير UNIX

س. هل يمكنني إستخدام المستشعر 3.0 الجديد مع نسخة x.2.2 من Director؟

أ. نعم، ولكن يجب ترقية برنامج Director إلى الإصدار 2.2.3 أو إصدار أحدث. يمكن للعملاء المسجلين تنزيل هذه الملفات من Cisco Secure Downloads (العملاء المسجلون فقط).

س. كيف يمكنني أن أعرف أي نسخة لمدير الشياطين الذي أستخدمه؟

a. أصدرت **cat /usr/nr/version** أمر وفحصت الإصدار رقم أن الإنتاج يحتوي.

ملاحظة: يخبرك إخراج الأمر **NRVER** على المدير بإصدار الأوامر التي تعمل على المدير، ولكنه لا يخبرك بإصدار برنامج Director نفسه.

س. كيف يمكنني الحصول على مدير للتخلص من تشكيله؟

أ. سجل الدخول كشبكة **مستخدم** وقم بتنفيذ الأمر /usr/nr/bin/director/nrCollectInfo لإرسال معلومات التكوين إلى ملف باسم /usr/nr/var/tmp/Report_For_Director.html.

س. لدي العديد من الأخطاء (ربما أكثر من 1000) على شاشة العرض OpenView من HP. أحذفهم، لكنهم يستمرون في العودة. لماذا؟

أ. إذا تم إغراق مدير IDS بالأخطاء وتعذر عليه عرضها كلها، فإنه يبدأ في التخزين المؤقت لملف. قم بإيقاف ملفات تعريف IDS وإنهاء أي خرائط OpenView التي قمت بفتحها للتخلص من الملف. احذف الملف **/usr/nr/var/nrDirmap.buffer.default**، ثم أعد تشغيل برنامج IDS والخريطة OpenView.

س. أواجه مشكلات في توصيل أجهزة الإنذار إلى خريطة برنامج OpenView من HP. أستمر في الحصول على الأخطاء في /usr/nr/var/errors.nrdirmap. ماذا علي أن أفعل؟

أ. في إصدارات IDS قبل 2.2.2، أسهل شيء للقيام به هو مسح قاعدة بيانات OpenView. توجد قاعدة البيانات في /var/opt/ov/share/database/openView. أكمل الخطوات التالية لحذف قاعدة بيانات OpenView.

1. قم بإغلاق جميع خرائط OpenView باستخدام الأمر **ovstop**، ثم قم بإيقاف خدمات IDS باستخدام الأمر **nrstop**.
2. قم بتسجيل الدخول **كجذر** وإصدار للمستخدم **/usr/nr/bin/director/nrDeleteOVwDb**.
3. قم بإزالة كافة الملفات "*.error" الموجودة في الدليل /usr/nr/var (على سبيل المثال، errors.configd).

4. قم بإعادة تشغيل الخدمات باستخدام الأمر **nrstart**، ثم قم بإعادة تشغيل OpenView باستخدام الأمر **ovstart**. **ملاحظة:** في الإصدار 2.2.2 من Director، يمكنك إزالة جزء IDS فقط من قاعدة بيانات OpenView بدلا من قاعدة البيانات بأكملها. ويتم وصف هذا الإجراء في دليل تكوين مدير IDS.

س. لا يمكنني الحصول على إنذارات على خريطة OpenView الخاصة بي. يحتوي الملف /usr/nr/var/errors.postofficed على Director على رسائل تقول إن خريطة المرور غير مرخصة للتشغيل على هذا الجهاز. كيف يمكنني إصلاح هذا؟

أ. قم بتنفيذ هذا الأمر.

```
cp /usr/nr/etc/.lt/license-all.lic /usr/nr/etc/licenses
```

تأكد من امتلاك **شبكة** المستخدم للملفات، ثم أعد تشغيل خدمات IDS.

س. عند تشغيل الأداة المساعدة nrConfigure والنقر نقرا مزدوجا فوق Director، تصل إلي هذه الرسالة: "يتعذر العثور على نوع أداة الاستشعار ل *<director_name>*. الرجاء التحقق من أن PostOffice و PacketD قيد التشغيل. ماذا علي أن أفعل؟

a. المشكلة يقع لأن nrConfigure يرى العملية ربط في المدير مبرد (أي لا ينبغي هو). عندما يستعلم NrConfigure المدير عن إصداره كما لو كان مستشعر، لا يمكن للمدير الاستجابة باستخدام إصدار مستشعر.

أتمت هذا steps أن يحل هذا إصدار.

1. قم بتحرير ملف /usr/nr/etc/daemons وأزال الإدخالات ل nr.packetD و nr.sensord و nr.managed، نظرا لأن هذه العمليات يجب أن تعمل فقط على المستشعر.
2. قم بإيقاف الخدمات باستخدام الأمر **nrstop**، ثم قم بإعادة تشغيل الخدمات باستخدام الأمر **nrstart**.
3. تأكد من إيقاف تشغيل NRconfigure.
4. بدء تشغيل OpenView باستخدام الأمر **ovw**.
5. حدد **تأمين > متقدم > nrConfigure DB > حذف** لحذف قاعدة بيانات nrConfigure التالفة.
6. أدخل **نعم** عند الطلب للمتابعة.
7. قم بتمييز المدير وجميع أجهزة الاستشعار الخاصة بك في نافذة OpenView الرئيسية.
8. حدد **تأمين > متقدم > nrConfigure DB>إنشاء** لإنشاء قاعدة بيانات nrConfigure جديدة باستخدام إصدارات التكوين الحالية من الأجهزة.

س. كيف يمكنني الحفاظ على تمكين تطبيق الخريطة الرقمية بشكل افتراضي على خرائط OpenView؟

أ. يمكن للمستخدمين الذين يقومون بتشغيل تطبيق IDS على مدير UNIX أيضا تشغيل تطبيقات أخرى على OpenView. ولا ينصح بذلك، ولكن لا يمكن تجنبه في بعض الحالات. المشكلة هي أن NRDIRMAP يتم تمكينها بشكل افتراضي لكل خريطة OpenView، وهو أمر غير مرغوب فيه عند تشغيل تطبيقات أخرى على OpenView.

أتمت هذا steps على ال UNIX Director أن يغير التقصير لذلك أنت يستطيع أخترت أي خرائط يتلقى NRDIRMAP يمكن على هم.

1. تسجيل الدخول كشبكة **مستخدم**.
2. اكتب (OV_REGISTER) **cd$ov_register/C**. هو جزء من المتغير البيئي الخاص بك. المسار المعتاد هو /etc/opt/ov/share/register/c/).

3. اكتب **su root**.
4. قم بتحرير ملف الخريطة النقطية وتغيير سطر "الأمر" كما يوضح هذا الإخراج:

```
;"Command -Shared -Initial "nrdirmap
;"Changes to: Command -Shared -Initial "nrdirmap -d ---!
```

5. قم بحفظ ملف الخريطة الرقمية.
6. إعادة تدوير OpenView. الآن، عندما يتم إحضار خريطة باستخدام الأمر **OVW**، **تكتب ps -ef |خريطة GREP** ينبغي أن ينتج مخرجات مماثلة لتلك الموضحة هنا. لاحظ باستخدام المحول -d.

```
ps -ef | grep dirmap<
netrangr 7175 6820 0 09:50:47 pts/2 0:00 grep dirmap
netrangr 7158 7152 0 09:50:21 ? 0:00 nrdirmap -d
```

لا تحتوي الخرائط الجديدة التي تم إنشاؤها في OpenView الآن على NRdirMap ممكن بشكل افتراضي. إذا كنت ترغب في إنشاء خريطة مع تثبيت الخريطة، يجب أن تقوم بذلك من واجهة المستخدم الرسومية OpenView، كما يوضح هذا الإجراء.

1. من قائمة OpenView الرئيسية، أختر **خريطة > جديد** وأدخل اسم للخريطة الجديدة.
2. تحت التطبيقات القابلة للتكوين، يجب أن ترى NetRanger/Director. أخترت **NetRanger/Director** وطقطقة **يشكل ل هذا خريطة**.
3. للخيار الذي يقول "هل يجب تمكين خريطة الموارد لهذه الخريطة؟ "، أختر **صحيح** إذا كنت تريد تمكين خريطة الموارد.
4. أخترت **دقق** وطقطقة **ok**.

Q. لقد تمت ترقيتي إلى Director version 2.2.3، والآن لا يمكنني تعيين خطورة الحدث إلى مستوى أعلى من 5، على الرغم من أنه يمكنني القيام بذلك في إصدارات سابقة. لماذا هذا؟

أ. تم تغيير مستويات الخطورة في الإصدار 2.2.3 من المدير لدعم النطاق من 1 إلى 5 فقط.

(IDS Cisco Secure Policy Manager (CSPM

س. أي إصدار من CSPM يجب أن أستخدمه لإدارة مستشعر الهويات الخاص بي؟

أ. الإصدار 2.3i من CSPM حاليا هو الإصدار الذي يمكنه إدارة مستشعر IDS، في حين لا يمكن CSPM 3.0. إذا كنت تستخدم CSPM لإدارة المستشعر وأجهزة Cisco الآمنة الأخرى (مثل PIXs، الموجهات)، فيجب تثبيت الإصدارين المختلفين ل CSPM (2.3i و x.3) على خادمين Windows منفصلين. يمكنك إستخدام كل خادم لإدارة الأجهزة المقابلة: CSPM 2.3i لأجهزة الاستشعار و CSPM 3.x لأجهزة PIX والموجهات وما إلى ذلك.

س. كيف أقوم بتكوين CSPM لإدارة مستشعر IDS والتأكد من عمل الاتصال؟

a. راجع تكوين مستشعر Cisco Secure IDS في CSPM للحصول على مزيد من المعلومات حول كيفية تكوين CSPM لإدارة مستشعر IDS لديك وضمان عمل الاتصال.

س. هل يمكنني ضبط تواقيع الجهاز بواسطة CSPM؟

أ. يتضمن الضبط تغيير ما يتطلبه الأمر لإطلاق التوقيع (مثل عدد البيئات المضيفة في عملية مسح) ولا يعني تحديد الإجراءات ومستويات الخطورة.

يتعذر على CSPM (في أي إصدار) ضبط توقيعات الجهاز. يمكن فقط أن تحدد أفعال التوقيع ومراحله. بمعنى آخر، يمكن ل CSPM تعيين الخطورة وأي إجراء للاقتران بالتوقيع ولكن لا يمكن تعيين ما يطلق ذلك التوقيع. يجب

إستخدام قائمة SigWizMenu الموجودة على جهاز الاستشعار لضبط أجهزة الاستشعار. يمكن إستخدام كل من SigWizMenu و CSPM لتكوين المستشعر نفسه نظرا لأنهما يؤثران على أجزاء مختلفة من التكوين.

ملاحظة: إذا كنت تستخدم الإصدار 2.2.3 من مدير UNIX أو إصدار أحدث، فإن الأداة المساعدة nrConfigure قادرة على تكوين كل شيء تقوم SigWizMenu بتكوينه. بعد الترقية إلى 2.2.3، يجب إستخدام nrConfigure بدلا من SigWizMenu لضبط التوقيعات.

معلومات ذات صلة

- دعم منتجات نظام منع التسلل من Cisco
- وثائق نظام اكتشاف الاقتحام الآمن من Cisco
- الإعلامات الميدانية لنظام اكتشاف الاقتحام الآمن من Cisco
- 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).