مدير جهاز IPS 5.1 - توقيع التوليف

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
تواقيع الضبط
الإجراء بالتفصيل
معلومات ذات صلة

المقدمة

يحتوي نظام منع التسلل (IPS) 5.1 على أكثر من 1000 توقيع افتراضي مدمج. لا يمكنك إعادة تسمية أو حذف توقيعات من قائمة التوقيعات المدمجة، لكن يمكنك إيقاف توقيعات لإزالتهم من محرك الاستشعار. يمكنك تنشيط التوقيعات المتقاعدة لاحقا. غير أن هذه العملية تتطلب من محركات الاستشعار إعادة بناء تكوينها، وهو ما يستغرق وقتا وقد يؤخر تجهيز حركة المرور. يمكنك *ضبط* التوقيعات المدمجة عندما تقوم بضبط العديد من معلمات التوقيع. التوقيعات المدمجة التي تم تعديلها تسمى *توقيعات مضبوطة*.

يوضح هذا المستند الخطوات التي يجب إستخدامها لضبط التوقيع باستخدام إدارة أجهزة IDM .(IDM) IPS هو تطبيق جافا يستند إلى الويب يتيح لك تكوين جهاز الاستشعار وإدارته. يوجد خادم ويب الخاص ب IDM على المستشعر. يمكنك الوصول إليها من خلال مستعرضات الويب Internet Explorer أو Netscape أو Mozilla.

ملاحظة: يمكنك إنشاء توقيعات، والتي تسمى *توقيعات مخصصة*. تبدأ معرفات التوقيع المخصص في 60000. يمكنك تكوينها لعدة أشياء، مثل مطابقة السلاسل على إتصالات UDP، وتتبع فيضانات الشبكة، والماسحات. يتم إنشاء كل توقيع باستخدام محرك توقيع مصمم خصيصا لنوع حركة المرور التي يتم مراقبتها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مدير الأجهزة لنظام منع الاقتحام من Cisco الإصدار x.5.

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

الاصطلاحات

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

معلومات أساسية

in order to شكلت مستشعر أن يراقب شبكة حركة مرور لتوقيع خاص، أنت ينبغي مكنت التوقيع. بشكل افتراضي، فإن أكثر التوقيعات أهمية يتم تمكينها عندما تقوم بتثبيت تحديث التوقيع. عند اكتشاف هجوم يطابق توقيعا ممكنا، يقوم المستشعر بإنشاء تنبيه، يتم تخزينه في مخزن أحداث المستشعر. يمكن إسترداد التنبيهات، بالإضافة إلى الأحداث الأخرى، من مخزن الأحداث بواسطة عملاء مستندة إلى الويب. وبشكل افتراضي، يقوم المستشعر بتسجيل جميع التنبيهات المعلوماتية أو أعلى.

تحتوي بعض التوقيعات على توقيعات فرعية. أي أن التوقيع مقسم إلى فئات فرعية. عندما تقوم بتكوين توقيع فرعي، فإن التغييرات التي يتم إجراؤها على معلمات توقيع فرعي واحد تنطبق فقط على ذلك التوقيع الفرعي. على سبيل المثال، إذا قمت بتحرير التوقيع الفرعي 3050 1 وقمت بتغيير الخطورة، فإن تغيير الخطورة ينطبق فقط على التوقيع الفرعي 1 وليس على 3050 2 و 3050 3 و 3050 4.

تواقيع الضبط

تشير أيقونة A + إلى توفر المزيد من الخيارات لهذه المعلمة. انقر فوق أيقونة + لتوسيع المقطع وعرض المعلمات المتبقية.

تشير الأيقونة الخضراء إلى أن المعلمة تستخدم حاليا القيمة الافتراضية. انقر الأيقونة الخضراء لتغييرها إلى الأحمر، والذي ينشط حقل المعلمة بحيث يمكنك تحرير القيمة.

الإجراء بالتفصيل

أتمت هذا steps in order to ضبتت توقيع:

1. قم بتسجيل الدخول إلى IDM باستخدام حساب ذي امتيازات المسؤول أو عامل التشغيل.
2. أختر **التكوين > تعريف التوقيع > تكوين التوقيع**.يظهر جزء تكوين التوقيع.
3. لتحديد موقع توقيع، أختر خيار فرز من القائمة **تحديد حسب**.على سبيل المثال، إذا قمت بالبحث عن توقيع تدفق UDP، أختر **بروتوكول L2/L3/L4** ثم **تفيض UDP**.يقوم جزء تكوين التوقيع بتحديث تلك التوقيعات التي تطابق معايير الفرز الخاصة بك وعرضها فقط.
4. لضبط توقيع موجود، حدد التوقيع وأكمل الخطوات التالية:انقر **تحرير** لفتح شاشة تحرير التوقيع.راجع قيم المعلمات وقم بتغيير قيمة أي معلمة تريد ضبطها.**ملاحظة:** لاختيار أكثر من إجراء حدث واحد، اضغط باستمرار على مفتاح **Ctrl**.تحت الحالة، أختر **نعم** لتمكين التوقيع.**ملاحظة:** يجب تمكين التوقيع لكي يتمكن المستشعر من الكشف الفعلي عن الهجوم الذي يحدده التوقيع.تحت الحالة، حدد ما إذا كان هذا التوقيع موقوفا. انقر فوق **لا** لتنشيط التوقيع. هي بتحط التوقيع بالمحرك.**ملاحظة:** يجب تنشيط توقيع لكي يكتشف المستشعر الهجوم الذي يحدده التوقيع.**ملاحظة:** انقر فوق **إلغاء الأمر** للتراجع عن تغييراتك وإغلاق شاشة تحرير التوقيع.وانقر فوق **OK**.يظهر التوقيع الذي تم تحريره الآن في القائمة مع تعيين النوع إلى "مضبوط".**ملاحظة:** إذا كنت تريد التراجع عن تغييراتك، انقر فوق **إعادة ضبط**.
5. انقر فوق **تطبيق** لتطبيق التغييرات الخاصة بك وحفظ التكوين الذي تمت مراجعته.

معلومات ذات صلة

- نظام Cisco لمنع الاقتحام

- 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).