تكوين قاعدة مرور على نظام Cisco FirePOWER

المحتويات

المقدمة

يصف هذا المستند قاعدة المرور، وكيفية إنشائها، وكيفية تمكينها في سياسة الاقتحام.

يمكنك إنشاء قواعد المرور لمنع الحزم التي تطابق المعايير المحددة في قاعدة المرور من إطلاق قاعدة التنبيه في حالات محددة، بدلا من تعطيل قاعدة التنبيه. بشكل افتراضي، تتجاوز قواعد المرور قواعد التنبيه. يقوم نظام FirePOWER بمقارنة الحزم بالشروط المحددة في كل قاعدة، وإذا تطابقت بيانات الحزمة مع جميع الشروط المحددة في القاعدة، تقوم القاعدة بتشغيل. إذا كانت القاعدة قاعدة تنبيه، فإنها تولد حدث إقتحام. إذا كانت قاعدة تمرير، فإنها تتجاهل حركة المرور.

على سبيل المثال، قد تحتاج إلى قاعدة تبحث عن محاولات تسجيل الدخول إلى خادم FTP حيث يبقى المستخدم "مجهول" نشطا. ومع ذلك، إذا كانت شبكتك تحتوي على خادم واحد أو أكثر من خوادم FTP الشرعية المجهولة، فيمكنك كتابة قاعدة تمرير وتنشيطها تحدد أنه بالنسبة لتلك الخوادم المحددة، لا يقوم المستخدمون المجهولون بتشغيل القاعدة الأصلية.

تحذير: عندما تتلقى قاعدة أصلية تستند إلى قاعدة المرور مراجعة، لا يتم تحديث قاعدة المرور تلقائيا. لذلك قد يكون من الصعب الحفاظ على قواعد المرور.

ملاحظة: إذا قمت بتمكين ميزة "القمع" لقاعدة، فإنها تقمع إعلامات الأحداث لهذه القاعدة. ومع ذلك، لا تزال القاعدة قيد التقييم. على سبيل المثال، إذا قمت بضغط قاعدة إسقاط، يتم إسقاط الحزم التي تطابق القاعدة بصمت.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

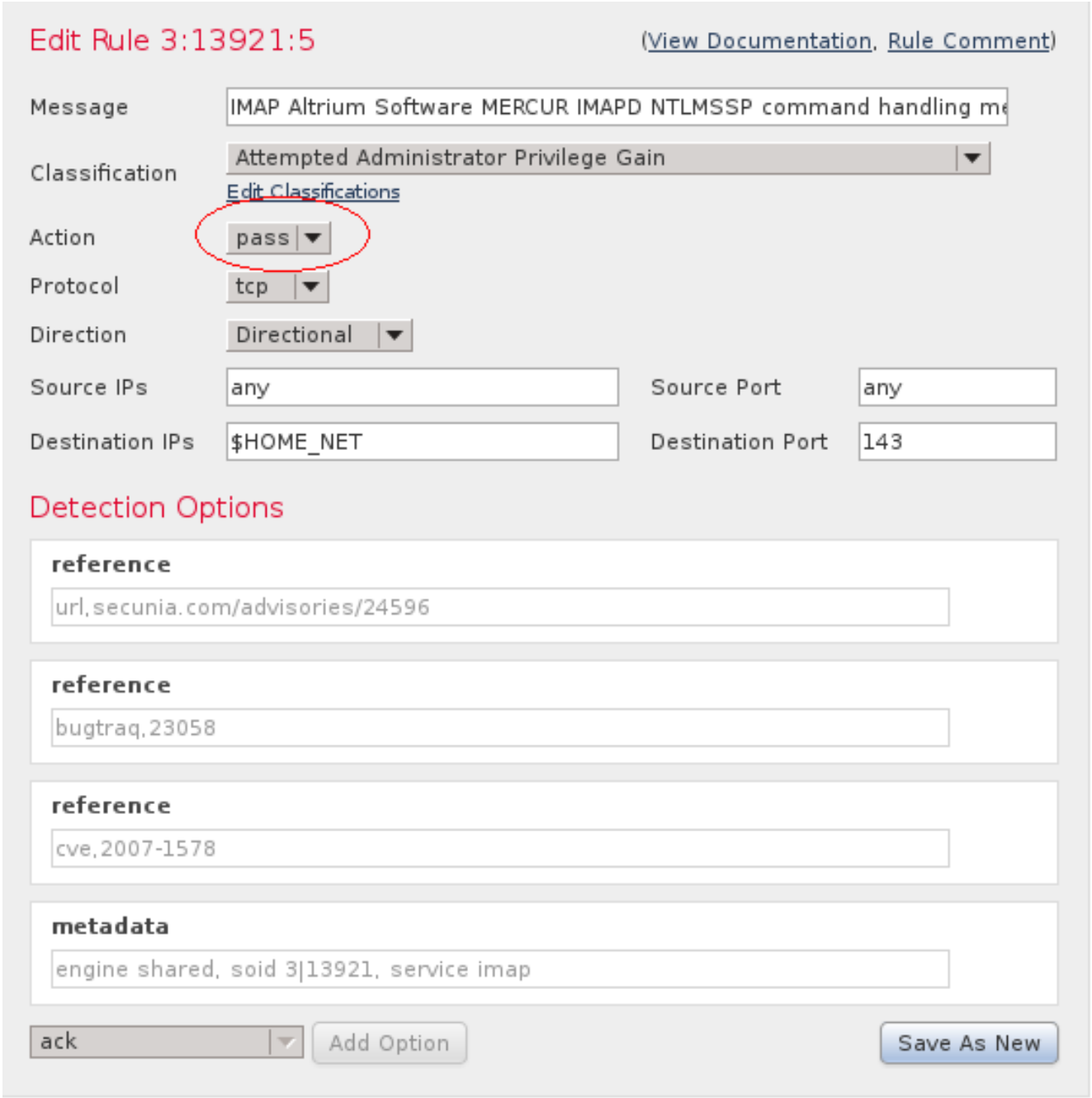
لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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.

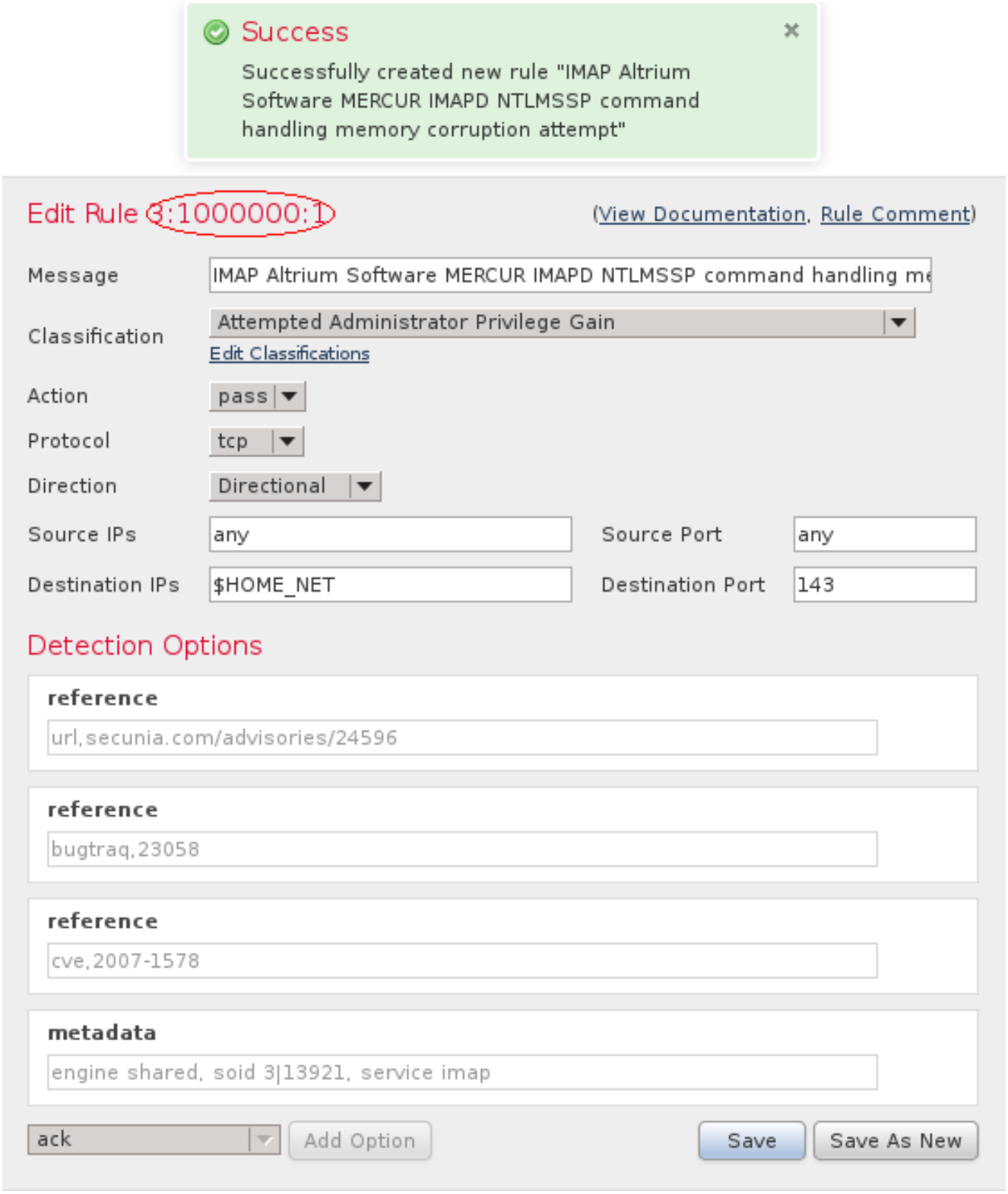
التكوين

إنشاء قاعدة تمرير

1. انتقل إلى **الكائنات > قواعد التطفل**. تظهر قائمة فئات القواعد.
2. العثور على فئة القاعدة المقترنة بالقاعدة التي تريد تصفيتها. أستخدم رمز السهم لتوسيع فئة القاعدة من قوائم الفئات والعثور على القاعدة التي تريد إنشاء قاعدة مرور لها. بدلا من ذلك، يمكنك إستخدام مربع البحث عن القاعدة.
3. بمجرد أن تجد القاعدة المرغوبة، انقر أيقونة القلم الرصاص المجاورة لها لتحرير القاعدة.
4. عندما تقوم بتحرير قاعدة، أكمل الخطوات التالية: انقر فوق زر **تحرير** الذي يتوافق مع القاعدة.في القائمة المنسدلة "إجراء"، أختر **pass**.قم بتغيير حقل IPs المصدر وحقل IPs الوجهة إلى البيئات المضيفة أو الشبكات التي لا تريد أن تنبه القاعدة إليها.انقر فوق **حفظ باسم جديد**.



5. لاحظ رقم معرف القاعدة الجديدة. على سبيل المثال، 100000.



تمكين قاعدة المرور

يجب تمكين القاعدة الجديدة الخاصة بك في سياسة الاقتحام المناسبة لتمرير حركة مرور البيانات على عناوين المصدر أو الوجهة التي حددتها. اتبع هذه الخطوات لتمكين قاعدة المرور:

1. تعديل نهج التطفل النشط: انتقل إلى **السياسات > التحكم في الوصول > التطفل**.انقر فوق **تحرير** بجوار نهج التطفل النشط.
2. إضافة القاعدة الجديدة إلى قائمة القواعد: انقر فوق **القواعد** في الجزء الأيسر.أدخل معرف القاعدة الذي لاحظته سابقا في مربع التصفية.حدد خانة الاختيار القواعد، ثم قم بتغيير حالة القاعدة **لإنشاء أحداث**.انقر فوق **معلومات النهج** في الجزء الأيسر. انقر فوق **تنفيذ التغييرات**.

3. انقر فوق **نشر** لنشر التغييرات على الجهاز.

التحقق من الصحة

يجب مراقبة الأحداث الجديدة لبعض الوقت للتأكد من عدم إنشاء أي أحداث لهذه القاعدة المحددة لعنوان IP للمصدر أو الوجهة المحدد.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

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).