تكوين إجراءات قواعد Snort 3 الإضافية على FMC

المحتويات

المقدمة

يصف هذا المستند دعم مركز إدارة Firepower (FMC) لميزة "إجراءات قواعد Snort 3" الإضافية التي تمت إضافتها في الإصدار 7.1.

معلومات أساسية

على الرغم من أن الدفاع ضد تهديد الطاقة النارية (FTD) يدعم سبعة إجراءات لقواعد سياسة التسلل وهي التنبيه/التعطيل/الحظر/الرفض/إعادة الكتابة/المرور/الإسقاط في 7.0، إلا أن وحدة التحكم في الإدارة الموحدة (FMC) دعمت ثلاثة إجراءات فقط لقواعد snort 3: "تنبيه" و"تعطيل" و"حظر".

من Firepower 7.1.0، تدعم FMC تكوين إجراءات قواعد جديدة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:
· معرفة الشخير مفتوح المصدر
· مركز إدارة Firepower (FMC) 7.1.0+
· برنامج الدفاع ضد تهديد الطاقة النارية (FTD) 7.0.0+

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:
· ينطبق هذا المستند على جميع منصات FirePOWER التي تشغل الإصدار 3
· برنامج الدفاع الظاهري (FTD) الذي يدعم تهديد FirePOWER من Cisco الذي يعمل بإصدار البرنامج 7.4.2
· Firepower Management Center Virtual (FMC) الذي يشغل الإصدار 7.4.2 من البرنامج

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تفاصيل الميزة

تمت إضافة إجراءات قاعدة Snort 3 الجديدة ووصفاتها كما يلي:

مرور: لم يتم إنشاء حدث، يسمح للحزمة بالمرور دون مزيد من التقييم من قبل أي قواعد snort لاحقة.

إسقاط: إنشاء حدث، وإسقاط الحزمة المطابقة وعدم حظر حركة مرور أخرى في هذا الاتصال.

رفض: يولد حدث، ويقطع الحزمة المطابقة، ويمنع حركة مرور البيانات الإضافية في هذا الاتصال ويرسل إعادة ضبط TCP أو منفذ ICMP الذي يتعذر الوصول إليه إلى مضيف المصدر والوجهة.

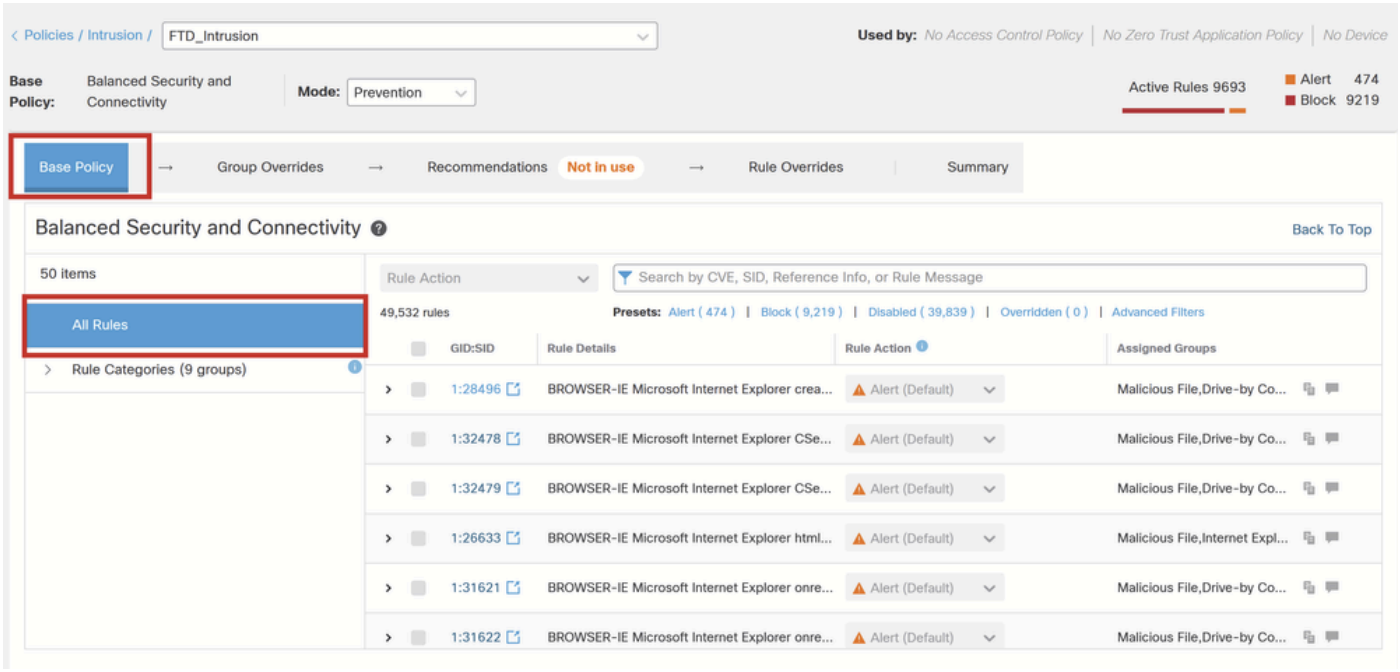
إعادة الكتابة: يولد حدث ويستبدل محتويات الحزمة بناء على خيار الاستبدال في القاعدة.

إف إم سي والكب

لعرض قواعد Snort 3 في سياسة إقتحام، انتقل إلىFMC Policies > Access Control > Intrusion,ما بعد ذلك انقر على خيار إصدار Snort 3 في الركن العلوي الأيمن من السياسة، كما هو موضح في الصورة:

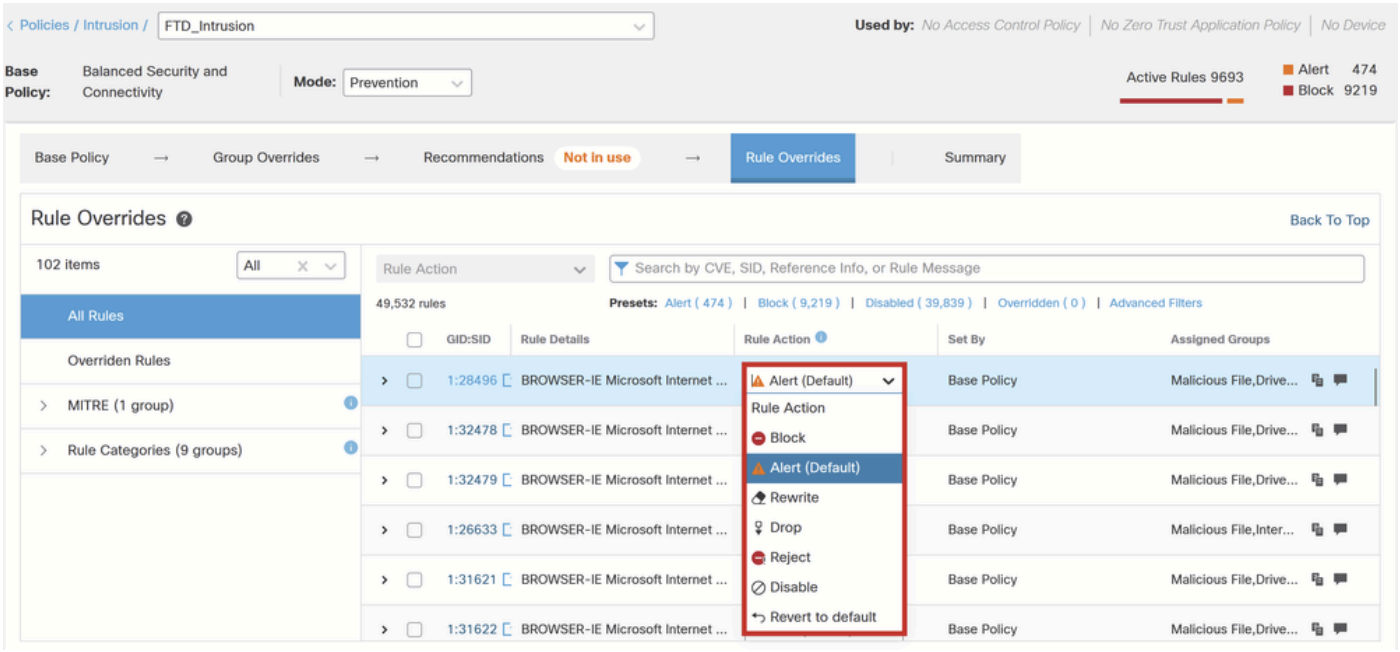
إصدار Snort 3

انقر فوق نهج أساسي > جميع القواعد، يمكنك مشاهدة الإجراءات الافتراضية لكافة قواعد Snort 3 المعرفة بواسطة النظام.

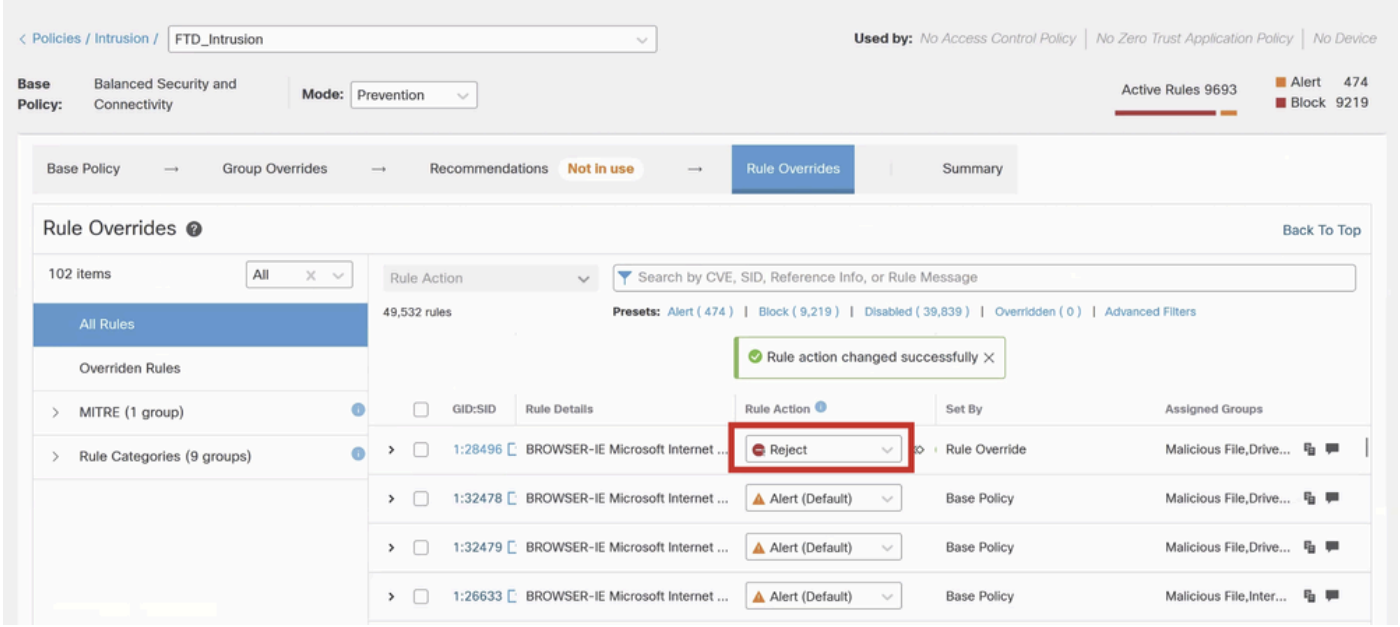


السياسة الأساسية

لتغيير إجراء القاعدة إلى أي من إجراءات القاعدة الجديدة هذه، انتقل إلى تخطيات القاعدة > كافة القواعد وحدد إجراء القاعدة من القائمة المنسدلة للقاعدة المحددة.

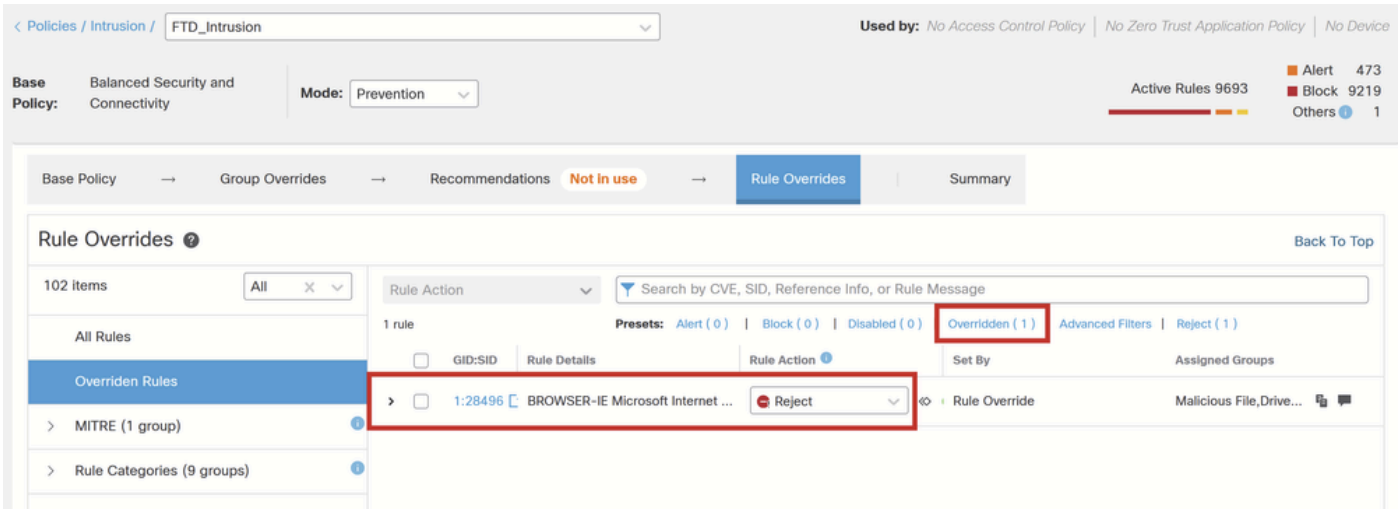


إجراءات قواعد إضافية



تغييرإجراءالقاعدة

يمكن العثور على القواعد التي تم تجاوزها ضمن التخطيات > القواعد التي تم تجاوزها.



القواعد التي تم تجاوزها

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).