تطلب نهج إرتباط FMC تمكين أحداث القائمة تمكين نهج اكتشاف الشبكة

المحتويات

مسألة

عند تكوين سياسات الارتباط باستخدام قوائم السماح على مركز إدارة جدار الحماية الآمن (FMC) من Cisco، من المهم ملاحظة أن السماح بأحداث القائمة والسماح بانتهاكات القائمة لا يتم إنشاؤها ما لم يتم تكوين نهج اكتشاف الشبكة لـ الشبكة الهدف IP. بدون هذا التكوين، لا تظهر أي أحداث تحت التحليل > الارتباط > السماح بأحداث القائمة والتحليل > الارتباط > السماح بانتهاكات القائمة.

ولوحظت هذه السلوكيات أثناء الفحص المعملي:

- يتم إنشاء أحداث الارتباط بشكل صحيح للشبكة الهدف التي تم تكوينها.
- لا يسمح بأحداث القائمة أو يسمح بانتهاكات القائمة عندما يصبح مضيف الشبكة الهدف غير متوافق.

البيئة

- برنامج الدفاع ضد تهديد جدار الحماية (FTD) من Cisco المدار من قبل مركز إدارة جدار الحماية الآمن (FMC)
- تم تكوين سياسة الارتباط باستخدام قائمة السماح باستهداف عناوين IP معينة
- السماح بقائمة تم تكوينها للسماح بتطبيق أو تطبيق أو بروتوكول ويب معين

رارق

بعد إجراء اختبارات عملية مكثفة ومشاورات مع فريق التطوير، تم التأكيد على أنه يجب تمكين نهج اكتشاف الشبكة كشرط أساسي للسماح بأحداث القائمة والسماح بإنشاء انتهاكات القائمة.

ويتضمن القرار هذه الخطوات:

الخطوة 1: تمكين نهج اكتشاف الشبكة

انتقل إلى السياسات > اكتشاف الشبكة في واجهة FMC وقم بإنشاء قاعدة إذا لم يكن هناك أي منها موجودا.

الخطوة 2: تكوين قاعدة اكتشاف الشبكة

قم بتكوين قاعدة اكتشاف الشبكة باستخدام إعدادات شبكة المصدر المناسبة:

- حدد الشبكة المصدر كنطاق شبكتك الداخلية.
- إذا كنت تراقب جميع مصادر حركة المرور، أستخدم جميع الشبكات (0.0.0.0/0) بدلا من ذلك.
- تأكد من تغطية القاعدة للشبكات التي تتوقع إنشاء أحداث قائمة السماح.

الخطوة 3: تنشيط قواعد نهج الارتباط

تحقق من أن قواعد سياسة الارتباط نشطة وليست في حالة معطلة.

الخطوة 4: التحقق من السماح بإنشاء حدث القائمة

بعد تمكين اكتشاف الشبكة وتنشيط قواعد سياسة الارتباط:

1.- الوصول إلى مواقع الويب من الشبكة الهدف التي تم تكوينها باستخدام مستعرض (مما يجعل المضيف غير متوافق).

2.- مراقبة التحليل > الارتباط > السماح بأحداث القائمة والتحليل > الارتباط > السماح بانتهاكات القائمة لإنشاء الحدث.

3.- تأكد من علم الأحداث عندما يكون المضيف غير متوافق.

أكدت الاختبارات المخبرية أنه بمجرد تمكين اكتشاف الشبكة، قم بالسماح بأحداث القائمة وبتم إنشاء السماح بانتهاكات القائمة بنجاح للمضيف غير المتوافق.

السبب

السبب الجذري هو أن نهج اكتشاف الشبكة هو شرط أساسي إلزامي لإنشاء السماح بأحداث القائمة في سياسات إرتباط FMC. بدون نهج اكتشاف شبكة نشط، لا يمكن للنظام تقييم توافق المضيف بشكل صحيح مقابل قائمة السماح التي تم تكوينها، مما يؤدي إلى عدم إنشاء أحداث السماح بالقائمة عند عدم توافق مضيف الشبكة الهدف.

المحتوى ذي الصلة

- وثائق قوائم التوافق مع FMC من Cisco
- الدعم الفني والتنزيلات من Cisco

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).