تكوين منع الهجمات المستندة إلى المعدل باستخدام عامل تصفية معدل Snort 3 على FTD الآمن

مسألة

ويُنصح التركيز على كيفية هيكلة قواعد تغطية شبكات فرعية متعددة، وفهم أفضل الممارسات للتنفيذ، وتحديد قيم العتبة المناسبة (العد في الثانية) للتنبيه أو الحجب، وخاصة في سياق الوقاية من هجمات الفيضانات في النظام.

البيئة

- Cisco Secure Firewall Firepower الذي يشغل FTD 7.4.2.4
- النظام الأساسي للأجهزة Firepower 2110
- مدارة من قبل مركز إدارة Firepower (FMC) 7.6.2.1
- نظام منع الاقتحام SNORT 3 مع تمكين فحص rate_filter
- شبكات فرعية داخلية متعددة تتطلب الحماية من فيضانات SYN
- لا توجد أخطاء نشطة؛ إرشادات التكوين للدفاع الاستباقي

قرار

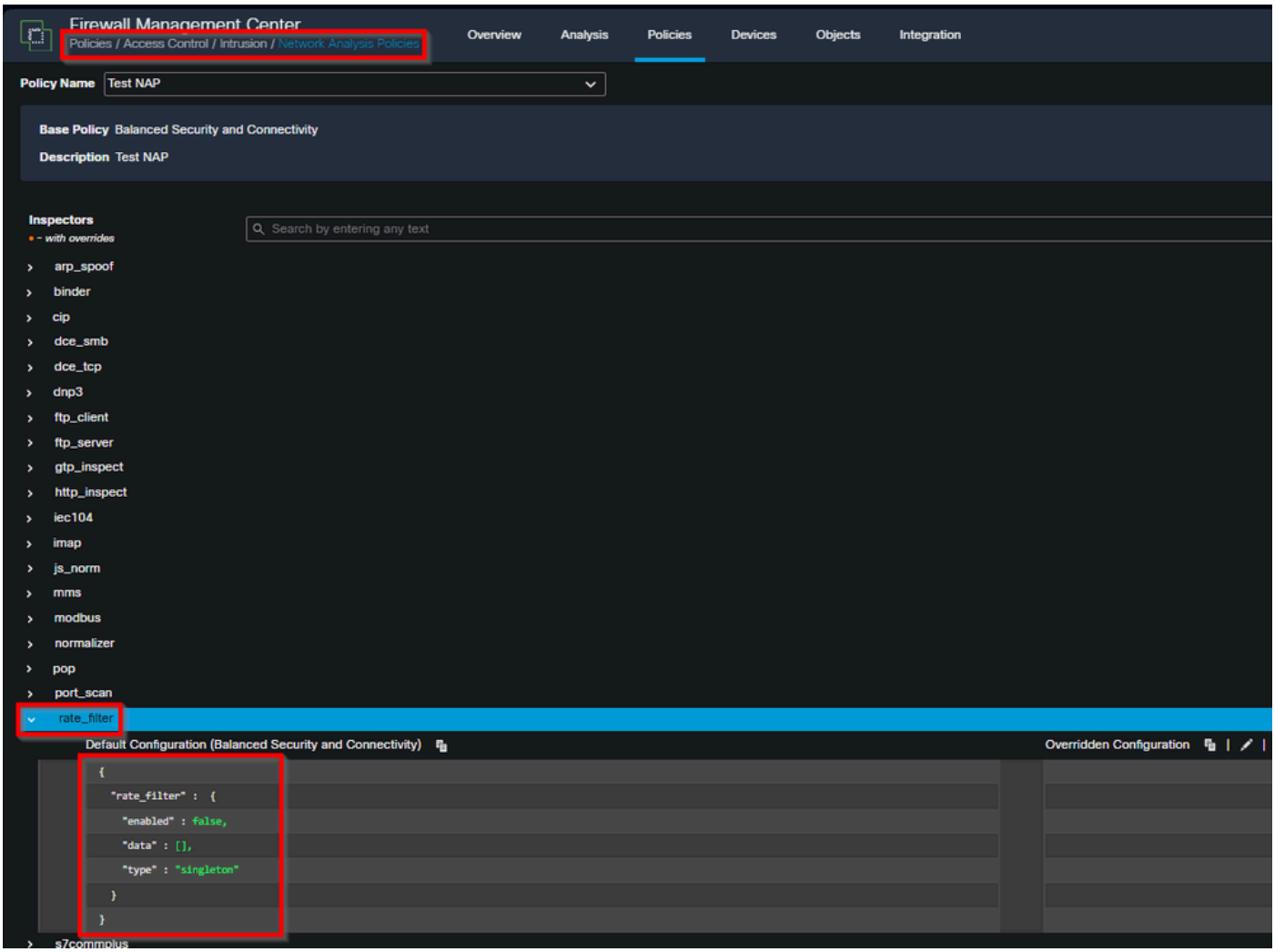
توضح هذه الخطوات كيفية تكوين منع الهجمات المستندة إلى المعدل وتنفيذه باستخدام عامل تصفية معدل_Snort 3 على جدار الحماية الآمن من Cisco (FTD)، بما في ذلك شرح بنية القاعدة للشبكات الفرعية المتعددة وتوصيات أفضل الممارسات. تهدف هذه الإجراءات إلى المساعدة في إنشاء خطوط أساس لحركة المرور العادية وتمكين الكشف أو الحظر الفعالين لهجمات فيضانات SYN.

ملاحظة: ليس ضمن نطاق عمل TAC اقتراح أو التوصية بأي قيم معينة لمرشحات حركة المرور المتعمقة للأنماط التي تتطلب تحليلاً مخصصاً لكل بيئة. هذه القواعد

وتصميم الشبكة لتحديد أفضل القيم لهذه المرشحات.

1: انتقل إلى عامل تصفية_معدل snort 3

يتم تكوين هذه المرشحات ضمن سياسات > التحكم في الوصول: التطفل > سياسات تحليل الشبكة بالنقر فوق إصدار Snort 3 لنهج NAP ثم النقر فوق القائمة المنسدلة rate_filter من اللوحة اليسرى.



inline_image_0.png

2: فهم هيكل قاعدة تصفية معدل snort 3

يسمح لك مفتش rate_filter في Snort 3 بتحديد القواعد التي تراقب أنواع معينة من حركة المرور (مثل حزم SYN) وتتخذ إجراءات (تنبيه أو إسقاط) عند تجاوز الحد المحدد. يمكن إستهداف هذه القواعد بشبكات فرعية متعددة.

مثال تكوين rate_filter للشبكات الفرعية المتعددة:

```
{
"rate_filter": {
"data": [
{
"apply_to": ["10.1.2.0/24", "10.1.3.0/24"],
"count": 5,
"gid": 135,
"sid": 1,
"new_action": "alert",
"seconds": 10,
"timeout": 15,
"track": "by_src"
}
],
"enabled": true,
"type": "singleton"
}
}
```


شرح المعلمات:

- apply_to: قائمة عناوين IP أو الشبكات الفرعية التي ينطبق عليها عامل التصفية (شبكات فرعية متعددة).
- عدد + ثوان: حد الحدث (على سبيل المثال، 5 حزم SYN في غضون 10 ثوان).
- GID / sid: يحدد حدث الشخر (مثل GID 135، SID 1 لاكتشاف فيضانات SYN).
- new_action: الإجراء الذي يجب إتخاذه عند تجاوز الحد (على سبيل المثال، التنبيه، drop).
- المهلة: المدة قبل تشغيل تنبيه/إجراء جديد لنفس الشرط.
- المسار: وضع التعقب (على سبيل المثال، by_src ل IP لكل مصدر، by_dst ل IP لكل وجهة).

3: أفضل الممارسات لضبط العتبة ونشر السياسات

- ابدأ في وضع التنبيه: قم بتعيين new_action إلى التنبيه واستخدم عتبات محافظة (مثل عدد أعلى وثوان) لتجنب الإيجابيات الخاطئة.
- حركة مرور الشبكة الأساسية: تم إنشاء أحداث على الشاشة لفهم ما تبدو عليه معدلات SYN "العادية" لبيئتك والشبكات الفرعية.
- ضبط المعلمات بشكل متكرر: ضبط العدد والثواني والمهلة استنادا إلى أنماط حركة المرور التي تم ملاحظتها واحتياجات التشغيل.
- انتقل إلى الحظر: بمجرد أن تصبح واثقا من أن الحدود تعكس السلوك غير الطبيعي بدقة، قم بتغيير جديد_action من التنبيه إلى الإسقاط أو ما يماثل ذلك لحظر الهجمات بشكل فعال.

- افصل المرشحات حسب الحاجة: ضع في الاعتبار حدود مختلفة للمعدل بالنسبة للمقاطع أو الأدوار المختلفة (على سبيل المثال، الخوادم مقابل الشبكات الفرعية للمستخدم) إذا كانت أنماط حركة مرور البيانات تختلف.
- المراقبة المستمرة:الاحتفاظ بالتنبيه والمراقبة لأحداث rate_filter للتعرف بسرعة على مشكلات الضبط أو التهديدات النشطة.

السبب

ال شيء. تم طلب التكوين لتوفير الأمان الاستباقي والتوجيه بسبب حاد فيضان سابق من قبل SYN.

المحتوى ذي الصلة

- مرجع مفتش Snort 3: عامل تصفية المعدل
- دليل تكوين جهاز مركز إدارة جدار الحماية الآمن من Cisco، الإصدار 7.4: منع الهجمات القائمة على المعدل
- 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).