اكتشاف تدفق الفيلة على أجهزة الطاقة النارية

المحتويات

المقدمة

يوضح هذا المستند كيفية إجراء اكتشاف تدفق الفيلة في بيئة Cisco Firepower Threat Defense (FTD).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بهذه المنتجات:

- مركز إدارة Firepower (FMC)
- Firepower Threat Defense (FTD)
- Netflow

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على FMC أن يركض برمجية صيغة 7،1 أو متأخر. 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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يعد اكتشاف تدفق الفيلة في Cisco Firepower أمرا بالغ الأهمية لتحديد وإدارة التدفقات الكبيرة طويلة العمر التي يمكن أن تستهلك موارد شبكة كبيرة وتؤثر على الأداء. يمكن

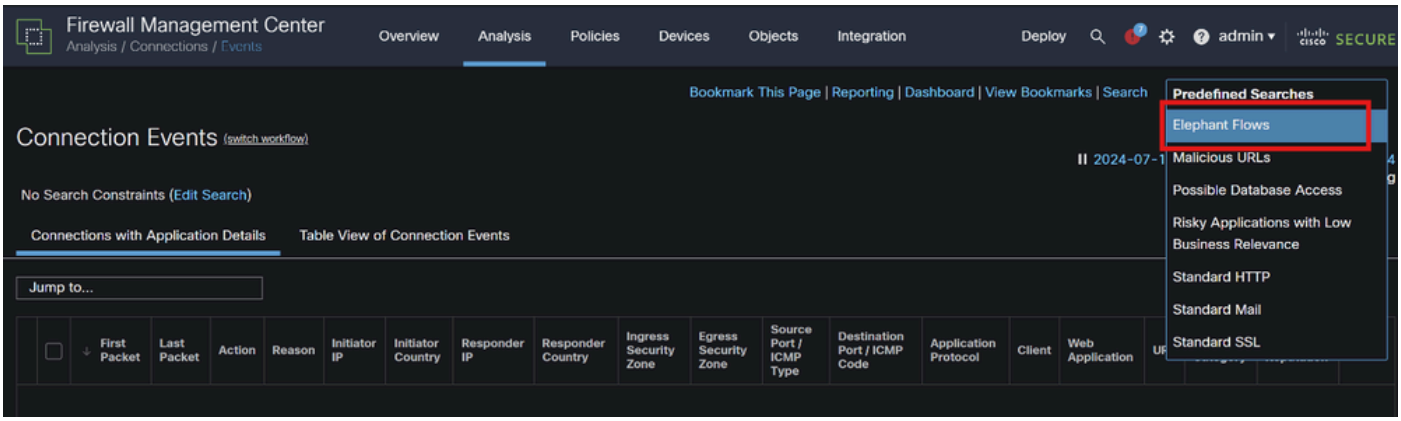
أن تحدث تدفقات كبيرة من الملفات في تطبيقات البيانات الكثيفة مثل نقل مقاطع الفيديو ونقل الملفات على نطاق واسع والنسخ المتماثل لقاعدة البيانات. يمكن تعريف هذه باستخدام الأساليب التالية:

الأساليب

1. إستخدام FMC

وأدخل اكتشاف تدفق الفيلة في الإصدار 7-1. يتيح الإصدار 7.2 إمكانية التخصيص بسهولة أكبر، كما يتيح خيار تجاوز تدفقات الفيلة أو حتى خنقها. تم إدخال ميزة Intelligent Application Bypass (IAB) من الإصدار 7.2.0 وما بعده بالنسبة لأجهزة Snort 3.

اكتشاف تدفق الفيل يمكن القيام به تحت التحليل > الاتصالات > الأحداث > البحث المحدد مسبقا > تدفقات الفيل.



أحداث الاتصال

يقدم هذا المستند عملية تدريجية لتكوين تدفق الفيل على سياسة التحكم في الوصول

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/elephant-flow.html#task_sxp_h2d_jsb

2. إستخدام واجهة سطر الأوامر (CLI)

أ. يمكن أن يشير الارتفاع الحاد في وحدة المعالجة المركزية لمثيل الشخير أيضا إلى أن الشبكة تتعامل مع تدفق الفيل الذي يمكن التعرف عليه باستخدام الأمر التالي:

show asp inspection-dp snort

هنا مثال لمخرجات الأمر.

> إظهار فحص بروتوكول ASP-DP

معرف معرف معلومات حالة مثيل فحص SNORT

إستخدام وحدة المعالجة المركزية (CPU) يحتوي على SEGS/PKTS الحالة TOT (usr | النظام)

— — — — — —

0 16450 8٪ (7٪| 0٪) 2.2 كيلوبايت 0 جاهزة

9٪ (8٪| 0٪) 2.2 كيلوبايت 0 جاهزة

6٪ (5٪| 1٪) 2.3 كيلوبايت 0 جاهزة

3 16454 5٪ (5٪| 0٪) 2.2 كيلوبايت 1 جاهزة

4 16456 6٪ (6٪| 0٪) 2.3 كيلوبايت 0 جاهزة

5 16457 6٪ (6٪| 0٪) 2.3 كيلوبايت 0 جاهزة

6 16458 6٪ (5٪| 0٪) 2.2 كيلوبايت 1 جاهزة

7 16459 4٪ (4٪| 0٪) 2.3 كيلوبايت 0 جاهزة

8 16452 9٪ (8٪| 1٪) 2.2 كيلو 0 جاهزة

9 16455 100٪ (100٪| 0٪) 2.2 k 5 جاهزة <<<< إستخدام عال لوحدة المعالجة المركزية 10 16460 7٪ (6٪| 0٪) 2.2 كيلوبايت 0 جاهزة

— — — — — —

الملخص 15٪ (14٪| 0٪) 24.6 كيلوبايت 7

ب. أيضا، يمكن أن يساعد إخراج الأمر "top" من وضع الجذر في فحص أي مثيل ل Snort يرتفع.

ج. تصدير تفاصيل الاتصال باستخدام هذا الأمر للتحقق من حركة المرور العليا التي تمر عبر جدار الحماية.

show asp inspection-dp snort

إظهار تفاصيل المخطط | إعادة توجيه القرص0:/con-detail.txt

يمكن العثور على الملف ضمن "/mnt/disk0" من وضع Linux. انسخ الأمر نفسه إلى **/ngfw/var/common** لتنزيله من FMC.

خبير cp

/mnt/disk0/<file name> /ngfw/var/common/

هنا مثال لمخرج تفاصيل الاتصال.

UDP بالداخل: 10.x.x.x/137 بالداخل: 10.x.43/137، العلامات - N1، 0idle، وقت التشغيل 6D2h، المهلة 2m0s، وحدات البايت 12313166926 <<</123 غيغابايت ويبدو أن وقت التشغيل يبلغ 6 أيام في ساعتين

معرف مفتاح بحث الاتصال: 2255619827

UDP بالداخل: 10.x.x.255/137 بالداخل: 10.x.x.42/137، العلامات - N1، 0s خامل، وقت التشغيل 7D5h، المهلة 2m0s، البايت 116338988274

معرف مفتاح بحث الاتصال: 1522768243

UDP في الداخل: 10.x.x.255/137 في الداخل: 10.x.x.39/137، العلامات - N1، 0s خامل، وقت التشغيل 8D1h، المهلة 2m0s، البايت 60930791876

معرف مفتاح البحث عن الاتصال: 120873687

UDP في الداخل: 10.x.x.255/137 في الداخل: 10.x.x0.34/137، العلامات - N1، 0s خامل، وقت التشغيل 9D5h، المهلة 2m0s، البايت 59310023420

معرف مفتاح بحث الاتصال: 59774515

3. إستخدام NetFlow

تدفقات الفيلة هي تدفقات حركة مرور كبيرة الحجم يمكن أن تؤثر على أداء الشبكة. ويشتمل اكتشاف هذه التدفقات على مراقبة حركة مرور الشبكة لتحديد الأنماط التي تشير إلى التدفقات الكبيرة والمستمرة. يوفر Cisco Firepower الأدوات والميزات لاكتشاف حركة مرور الشبكة وتحليلها، بما في ذلك تدفقات الفيلة. تساعد أداة NetFlow على تجميع معلومات حركة مرور IP للمراقبة.

يقدم هذا المستند عملية بالتفصيل لتكوين سياسة NetFlow على FMC

https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-management-center-virtual/221612-htz-01-2024-configure-netflow-in-fmc.html

أستخدم مجمع NetFlow ومحلل (على سبيل المثال: Cisco Stealthwatch أو SolarWind أو أي أداة تحليل NetFlow أخرى) لتحليل البيانات المجمعة. وبمجرد التعرف على تدفقات الفيلة، فيوسعك أن تتخذ الخطوات اللازمة لتخفيف تأثيرها:

- تنظيم حركة البيانات و جودة الخدمة: تطبيق سياسات جودة الخدمة (QoS) لتحديد أولوية حركة المرور والحد من النطاق الترددي العريض لتدفقات الفيلة.

- سياسات التحكم بالوصول: إنشاء سياسات للتحكم بالوصول لإدارة وتقييد تدفقات الفيلة.

- التجزئة: أستخدم تقسيم الشبكة لعزل تدفقات كبيرة الحجم وتقليل تأثيرها على باقي الشبكة إلى الحد الأدنى.

- موازنة الأحمال: تنفيذ موازنة الأحمال لتوزيع حركة المرور بشكل أكثر تساويا عبر موارد الشبكة.

4 - الرصد والتعديل المستمران

راقب حركة مرور الشبكة لديك بشكل منتظم لاكتشاف تدفقات الفيلة الجديدة وتعديل سياساتك وتكويناتك حسب الحاجة.

وم ع هذه العملية، يمكنك اكتشاف تدفقات الفيلة وإدارتها بفعالية في نشر Cisco Firepower، مما يضمن أداءً أفضل للشبكة واستخدام الموارد.

معلومات ذات صلة

دليل تكوين جهاز مركز إدارة جدار الحماية الآمن من Cisco، الإصدار 7.2

تكوين NetFlow في FMC

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).