كيفية تحديد حركة المرور التي تتم معالجتها بواسطة مثيل مثيل شبكة محدد

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
التكوين
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها

المقدمة

يوضح هذا المستند كيفية تحديد حركة مرور البيانات التي تتم معالجتها بواسطة مثيل شخر محدد. هذه التفاصيل مفيدة جدا أثناء أستكشاف أخطاء إستخدام وحدة المعالجة المركزية (CPU) العالي وإصلاحها على مثيل وحدة معالجة مركزية محدد.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة تقنية FirePOWER

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- مركز إدارة Firepower 6.x وأعلى
- قابل للتطبيق على جميع الأجهزة المدارة التي تتضمن الدفاع ضد تهديد الطاقة النارية، وحدات FirePOWER، وأجهزة إستشعار FirePOWER

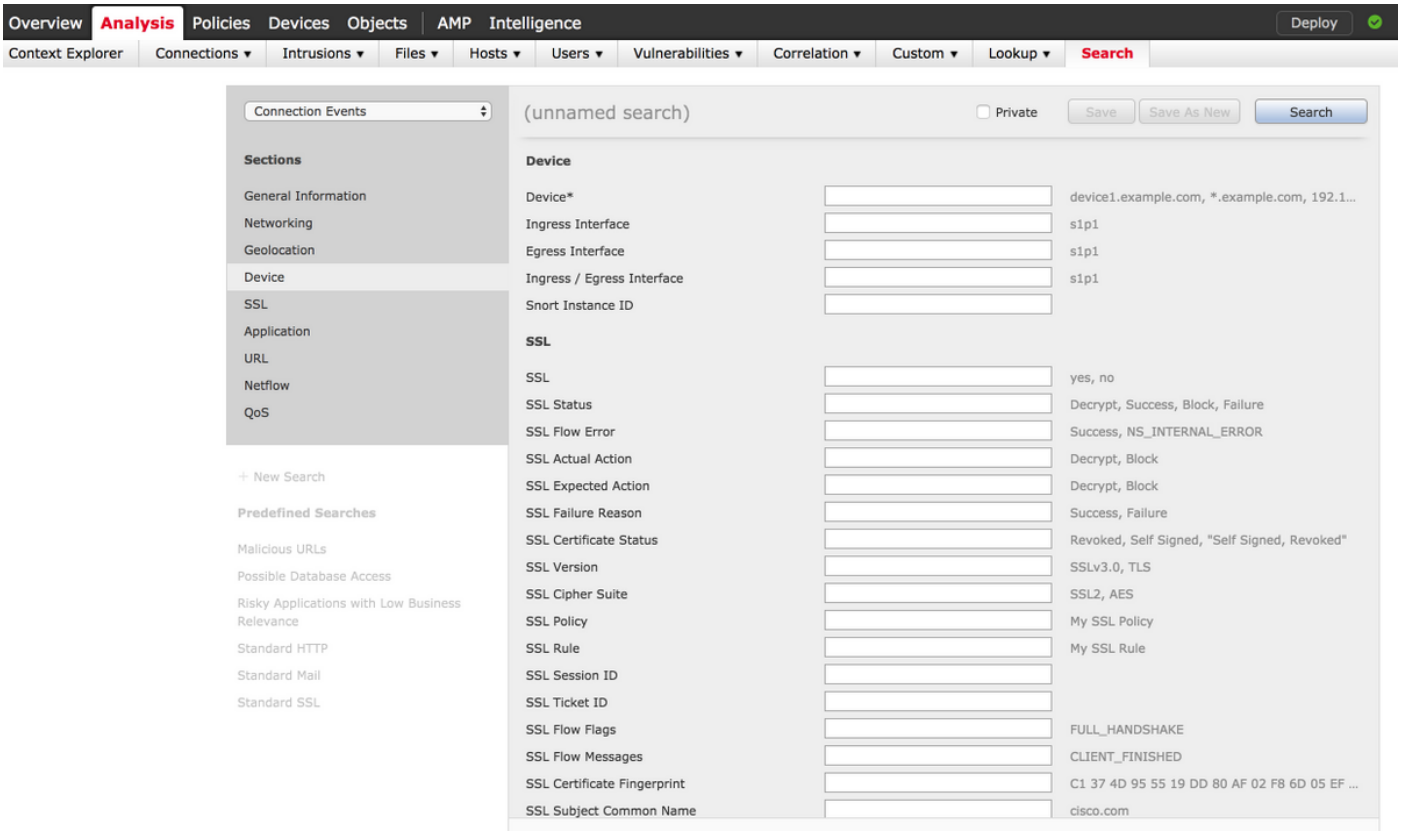
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

التكوينات

تسجيل الدخول إلى مركز إدارة Firepower باستخدام امتيازات الإدارة.

بمجرد نجاح تسجيل الدخول، انتقل إلى **Analysis (التحليل) > Search (البحث)**، كما هو موضح في الصورة:



تأكد من إختيار جدول **أحداث الاتصال** من القائمة المنسدلة ثم حدد **الجهاز** من القسم. قم بإدخال قيم لحقل الجهاز ومعرف مثيل Snort (من 0 إلى N، يعتمد عدد مثيلات الشخير على الجهاز الذي تتم إدارته)، كما هو موضح في الصورة:

بمجرد إدخال القيم، انقر فوق **بحث** وسوف تكون النتيجة أحداث اتصال يتم تشغيلها بواسطة مثيل snort المحدد.

ملاحظة: إذا كان الجهاز المدار حماية ضد تهديد FirePOWER، فيمكنك تحديد مثيلات الشبح باستخدام وضع

.FTD CLISH

```
show asp inspect-dp snort <
SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- --
--- ---------------- ---------- ---------- ---------- 0 5266 0% ( 0%| 0%) 0 0 READY 1 5268 0% (
0%| 0%) 0 0 READY 2 5267 0% ( 0%| 0%) 0 0 READY 3 5270 0% ( 0%| 0%) 0 0 READY 4 5269 0% ( 0%|
0%) 0 0 READY
```

ملاحظة: إذا كان الجهاز المدار هو وحدة FirePOWER النمطية أو مستشعر FirePOWER، فيمكنك تحديد مثيلات الشخص باستخدام وضع الخبير والأمر **العلوي** القائم على نظام التشغيل Linux.

```
admin@firepower:~$ top
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    5247 root      20   0 15248 1272  932 S    0  0.0   0:03.05 top
    5264 root       1 -19 1685m 461m  17m S    0  2.9   1:05.26 snort
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

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).