تحديد حركة المرور التي تتم معالجتها بواسطة مثيل وحدة نمطية محدد

المحتويات

المقدمة

يوضح هذا المستند كيفية تحديد حركة المرور التي تتم معالجتها بواسطة مثيل جهاز معين في بيئة Cisco Firepower Threat Defense (FTD).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بهذه المنتجات:

- مركز إدارة FirePOWER الآمن (FMC)
- الدفاع الآمن عن تهديد قوة الحماية (FTD)
- Syslog و SNMP
- واجهة برمجة تطبيقات REST

المكونات المستخدمة

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.

1. إستخدام أوامر CLI

باستخدام واجهة سطر الأوامر (CLI) على جهاز FTD لديك، يمكنك الوصول إلى معلومات تفصيلية حول مثيلات Snort وحركة مرور البيانات التي تتعامل معها.

- يوفر هذا الأمر تفاصيل حول عمليات التطفل الجاري تشغيلها.

show snort instances

هنا مثال لمخرجات الأمر.

> show snort instances

Total number of instances available - 1 +----------+----------+ | INSTANCE | PID | +----------+----------+ | **1** | **4765** | <<< One instance available and its process ID +----------+----------+

- للحصول على معلومات أكثر تفصيلا حول إحصائيات حركة المرور التي تتم معالجتها بواسطة مثيلات Snort، يمكن إستخدام هذه الأوامر. وهذا يعرض إحصائيات مختلفة، بما في ذلك عدد الحزم التي تمت معالجتها وإسقاطها والتنبيهات التي تم إنشاؤها بواسطة كل مثيل SNORT.

show snort statistics

هنا مثال لمخرجات الأمر.

> show snort statistics Packet Counters: Passed Packets 3791881977 Blocked Packets 707722 Injected Packets 87 **Packets bypassed (Snort Down) 253403701** <<< Packets bypassed **Packets bypassed (Snort Busy) 0** Flow Counters: Fast-Forwarded Flows 294816 Blacklisted Flows 227 Miscellaneous Counters: Start-of-Flow events 0 End-of-Flow events 317032 Denied flow events 14230 Frames forwarded to Snort before drop 0 Inject packets dropped 0 TCP Ack bypass Packets 6412936 TCP Meta-Ack Packets 2729907 Portscan Events 0 Packet decode optimized 21608793 Packet decode legacy 6558642

show asp inspect-dp snort

هنا مثال لمخرجات الأمر.

> show asp inspect-dp snort

SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- ----- ---------- ---------- ---------- -- -------- 0 16450 8% (7%| 0%) 2.2 K 0 READY 1 16453 9% (8%| 0%) 2.2 K 0 READY 2 16451 6% (5%| 1%) 2.3 K 0 READY 3 16454 5% (5%| 0%) 2.2 K 1 READY 4 16456 6% (6%| 0%) 2.3 K 0 READY 5 16457 6% (6%| 0%) 2.3 K 0 READY 6 16458 6% (5%| 0%) 2.2 K 1 READY 7 16459 4% (4%| 0%) 2.3 K 0 READY 8 16452 9% (8%| 1%) 2.2 K 0 READY **9 16455 100% (100%| 0%) 2.2 K 5 READY** <<<< High CPU utilization 10 16460 7% (6%| 0%) 2.2 K 0 READY -- ----- ---------- ---------- ---------- ---------- Summary 15% (14%| 0%) 24.6 K 7

-

إستخدام مركز إدارة Firepower (FMC)

إذا كنت تقوم بإدارة أجهزة FTD الخاصة بك من خلال FMC، فيمكنك الحصول على رؤى وتقارير تفصيلية حول مثيلات حركة مرور البيانات والتسجيل من خلال واجهة الويب.

- مراقبة

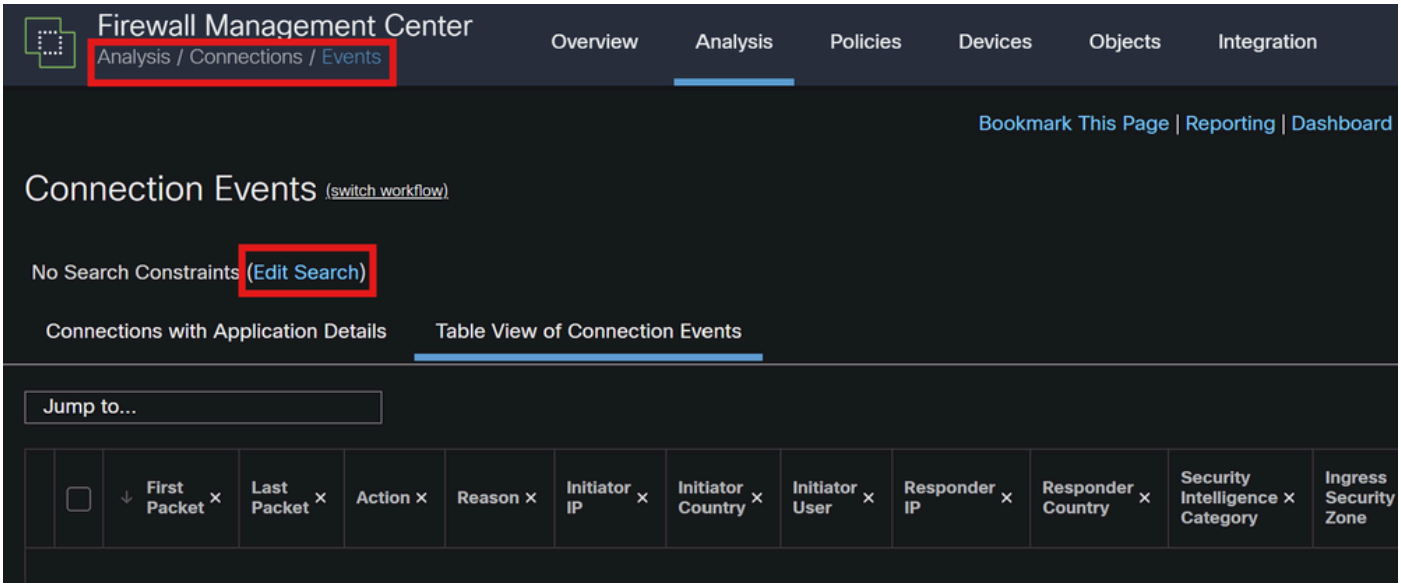
لوحة معلومات FMC: انتقل إلى لوحة المعلومات حيث يمكنك الاطلاع على نظرة عامة على حالة النظام، بما في ذلك مثيلات Snort.

مراقبة الصحة: في قسم المراقبة الصحية، يمكنك الحصول على إحصائيات مفصلة حول عمليات الشيخ، بما في ذلك حركة المرور التي تتم معالجتها.

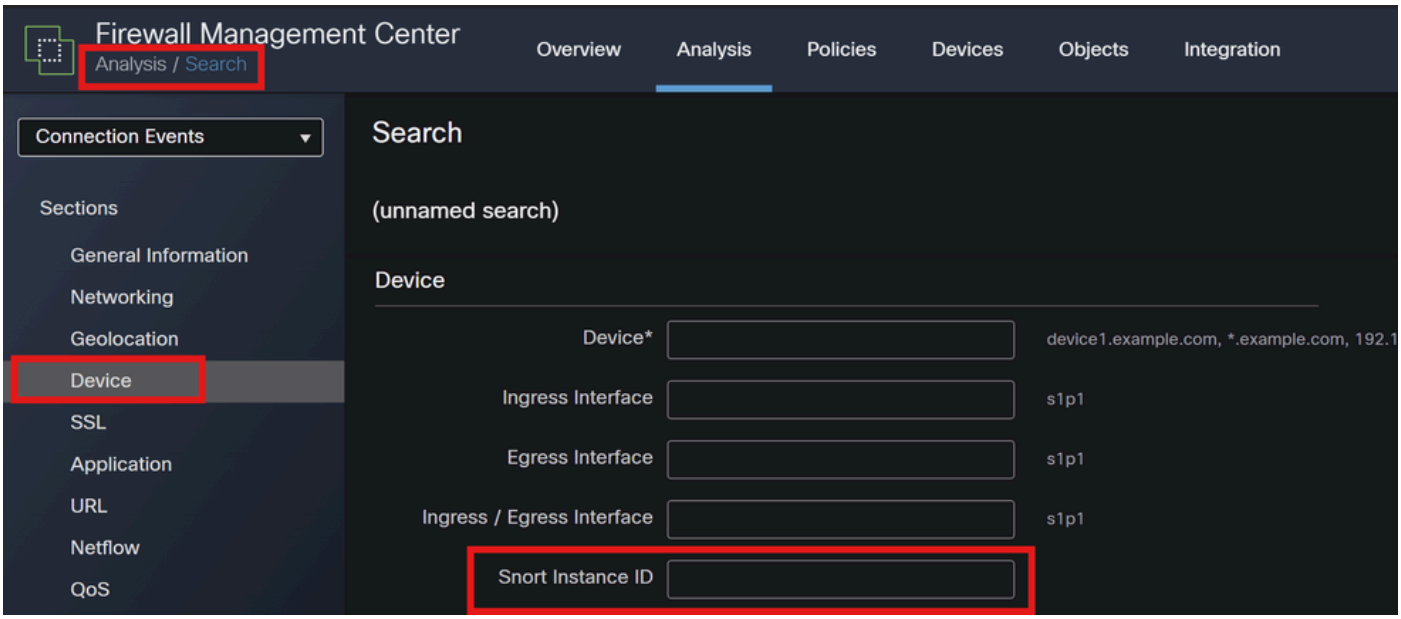
- تحليل

تحليل: انتقل إلى **تحليل > أحداث الاتصال**.

عوامل التصفية: أستخدم عوامل التصفية لتضييق البيانات إلى مثيل Snort أو حركة المرور المحددة التي تهتم بها.



أحداث الاتصال



معرف مثيل *Snort*

- **إستخدام Syslog و SNMP**

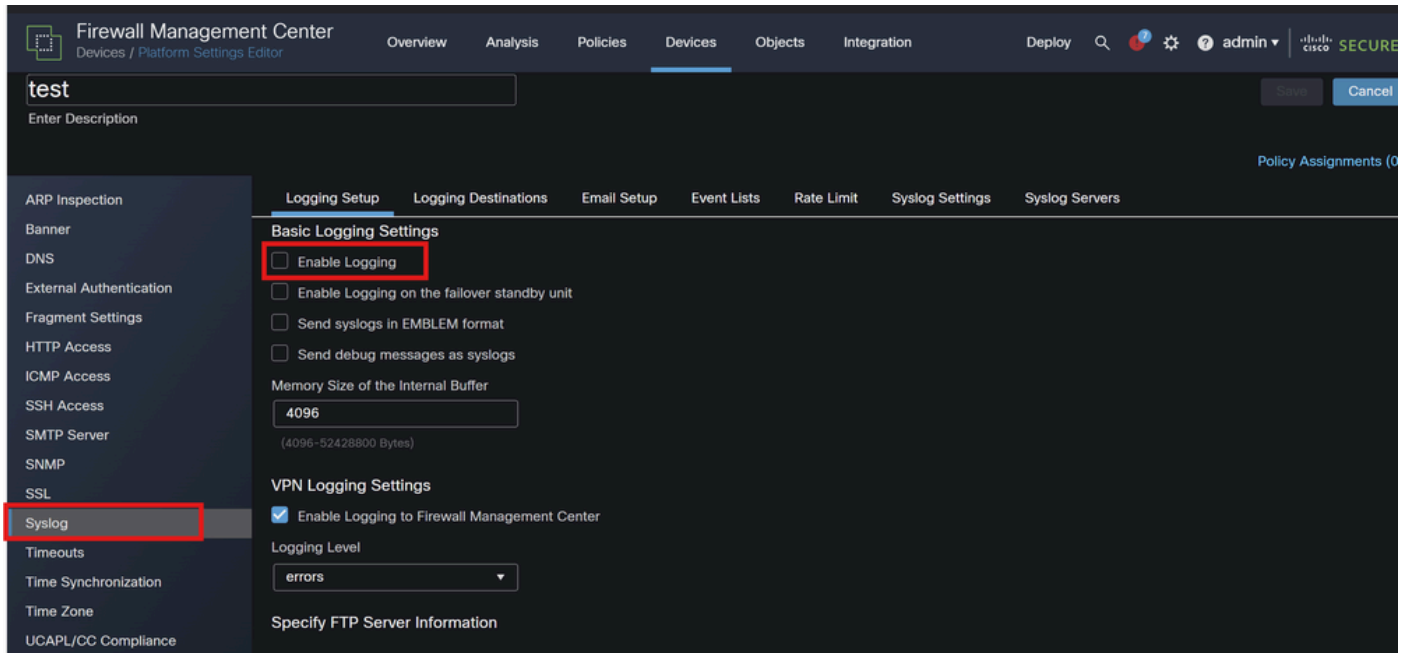
يمكنك تكوين بروتوكول FTD لإرسال رسائل syslog أو إختبارات SNMP إلى نظام مراقبة خارجي حيث يمكنك تحليل بيانات حركة مرور البيانات.

- تكوين Syslog

الأجهزة: في FMC، انتقل إلى **الأجهزة > إعدادات النظام الأساسي**.

إنشاء نهج أو تحريره: أختر نهج إعدادات النظام الأساسي المناسب.

syslog: تكوين إعدادات syslog لتضمين تنبيهات Snort وإحصاءاتها.

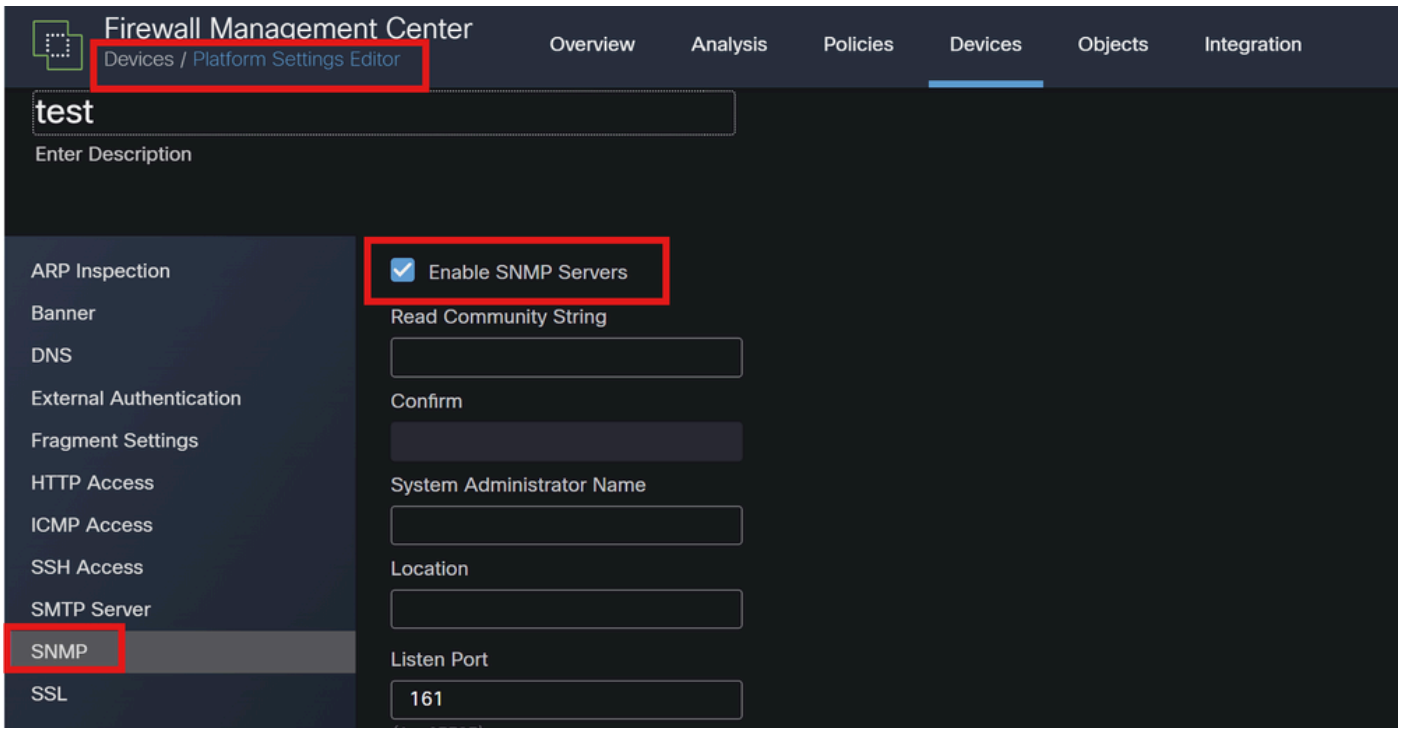


تكوين *Syslog*

- تكوين SNMP

إعدادات SNMP: مثل syslog، قم بتكوين إعدادات SNMP تحت **الأجهزة > إعدادات النظام الأساسي**.

المدائمات: تأكد من تمكين مدائمات SNMP الضرورية لإحصائيات مثيل Snort.



تكوين *SNMP*

4. إستخدام البرامج النصية المخصصة

بالنسبة للمستخدمين المتقدمين، يمكنك كتابة برامج نصية مخصصة تستخدم واجهة برمجة تطبيقات FTD REST API لتجميع إحصائيات حول مثيلات الشيخ. تتطلب هذه الطريقة معرفة استخدام البرمجة النصية وواجهة برمجة التطبيقات.

- واجهة برمجة تطبيقات REST

الوصول إلى واجهة برمجة التطبيقات: تأكد من تمكين وصول واجهة برمجة التطبيقات (API) على FMC لديك.

مكالمات واجهة برمجة التطبيقات (API): أستخدم إستدعاءات واجهة برمجة التطبيقات (API) المناسبة لجلب إحصائيات الشخ وبيانات حركة مرور البيانات.

يؤدي هذا إلى إرجاع بيانات JSON التي يمكنك تحليلها وتحليلها لتحديد حركة المرور التي تتم معالجتها بواسطة مثيلات Snort معينة.

من خلال دمج هذه الطرق، يمكنك الحصول على فهم شامل لحركة مرور البيانات التي تتم معالجتها بواسطة كل مثيل وحدة نمطية في نشر برنامج FTD 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).