# عرض التدفقات النشطة في الشخير

## المحتويات



## المقدمة

يوضح هذا المستند كيفية إستخدام الأمر show snort flow لعرض التدفقات النشطة في snort.

## المتطلبات قبل هذا الإصدار

| In Secure Firewall 7.4 and Below | | New to Secure Firewall 7.6 |
|---|---|---|
| • No way to look at active flows in Snort | | • New CLI `show snort flows` can be used to view active flows in Snort |

## نظرة عامة على الميزة

- يتم إستخدام CLI الجديد عرض تدفقات snort لعرض التدفقات النشطة في ذاكرة التخزين المؤقت لتدفق Snort 3.
- يوفر ذلك تفاصيل التدفقات النشطة في عملية Snort 3 قيد التشغيل.
- يزود الإنتاج الحالة من ال snort تدفق، مصدر وغاية ip ومنفذ.
- وتساعد في عزل المشاكل وتصحيح أخطائها في بيئات الإنتاج.

مفس (إبراز إلى القراءة)

ملاحظة: تم تقديم هذه الميزة للحصول على إمكانية النظر إلى تدفقات Snort النشطة والعميل، وحالات تدفق الخادم، والمهلة، والمزيد.

ملاحظة: تم تقديم هذه الميزة للحصول على إمكانية النظر إلى تدفقات Snort النشطة والعميل، وحالات تدفق الخادم، والمهلة، والمزيد.

## الحد الأدنى للبرامج والأجهزة الأساسية

| Manager(s) and Version (s) | Application (FTD) and Minimum Version of Application | Supported Platforms |
|---|---|---|
| • (CLI only) | FTD 7.6.0 | All platforms running FTD and Snort 3 |

## دعم نظام التشغيل Snort 3 و IPv6 و Multi-Instance و HA/Cluster

- يعمل مع كل من IPv4 و IPv6.
- يتطلب أن يكون Snort 3 محرك الكشف

| FTD | |
|---|---|
| Multi-instances supported? | Yes |
| Supported with HA'd devices | Yes |
| Supported with clustered devices? | Yes |

جوانب الدعم الأخرى

| Platforms | |
|---|---|
| FTD | |
| Licenses Required | Essentials |
| Works in Evaluation Mode | Yes |
| IP Addressing | IPv4<br>IPv6 |
| Multi-instances supported? | Yes |
| Supported with HA'd devices | Yes |
| Supported with clustered devices? | Yes |
| Other (only routed mode \| transparent mode), etc. | No Special Notes |

## وصف الميزة والتنقل عبر

يوفر هذا القسم طريقة مرور، بما في ذلك مهلة التدفق، وتفاصيل حول المزيد من الميزات.

### واجهة سطر الأوامر الخاصة بعرض العرض الجديد

<#root>

```
> show snort flows
```

```
TCP 0: x1.x1.x1.2/38148 x1.x1.x1.1/22 pkts/bytes client 9/2323 server 6/2105 idle 7s, uptime 7s, timeou
ICMP 0: x1.x1.x1.2 type 8 x1.x1.x1.1 pkts/bytes client 1/98 server 1/98 idle 0s, uptime 0s, timeout 3m0
UDP 0: x1.x1.x1.1/40101 x1.x1.x1.1/12345 pkts/bytes client 3/141 server 0/0 idle 19s, uptime 58s, timeo
```

يوضح هذا المثال ثلاث تدفقات:TCP و ICMP و UDP.

لتدفق TCP، القيم هي:

- البروتوكول - TCP/ICMP/UDP/IP
- معرف مساحة العنوان - معرف VRF للواجهة
- SourceIP / Port: x1.x1.x1.2/38148
- غاية IP/ميناء: x1.x1.x1.1/22
- وحدات PKTS/بايت العميل - 9/2323
- وحدات PKTS/بايت للخادم - 6/2105
- وضع الخمول - الوقت منذ آخر تدفق للحزمة
- وقت التشغيل - الوقت منذ إعداد التدفق
- المهلة - مهلة التدفق
- حالة العميل (تدفقات TCP فقط) - EST
- حالة الخادم (تدفق TCP فقط) - EST

## حالات تدفق العميل والخادم

- تظهر حالة العميل وحالة الخادم في الإخراج فقط إذا كان البروتوكول هو TCP.
- هذه هي القيم المحتملة وما يعنيه كل إختصار، لكل حالة:

| State Acronym | Description |
|---|---|
| LST | Listen |
| SYS | SYN Sent |
| SYR | SYN received |
| EST | Established |
| MDS | Midstream Sent |
| MDR | Midstream Received |
| FW1 | Final Wait 1 |
| FW2 | Final Wait 2 |
| CLW | Close Wait |
| CLG | Closing |
| LAK | Last ACK |
| TWT | Time wait |
| CLD | Closed |

## خيارات التصفية

يدعم الأمر show snort flow خيارات التصفية حيث تكون التدفقات التي تطابق عوامل التصفية هي المخرج فقط. صياغة الأمر هي

إظهار تدفقات snort <filter option> <value>

خيارات المرشح هي:

- بروتوكول -TCP/UDP/IP/ICMP
- src_ip - تدفقات التصفية حسب مصدر ip
- dst_ip - تدفقات التصفية حسب عنوان IP للوجهة
- src_port - تدفقات التصفية حسب منفذ المصدر

- dst_port - تدفق التصفية حسب منفذ الوجهة

يسرد الأمر > show snort flow proto TCP تدفقات TCP فقط:

```
TCP 0: x1.x1.x1.2/45508 x1.x1.x1.1/22 pkts/bytes client 10/2389 server 7/2171 idle
30s, uptime 150s, timeout 59m30s state client CLW server FW2
```

مفهرس (إلى القراءة)

ملاحظة: أنت يستطيع أيضا استعملت أكثر من واحد مرشح في الأمر. على سبيل المثال,

> show snort flow proto TCP src_ip x1.x1.x1.2 - إخراج تدفقات TCP التي تحتوي على src ip x1.x1.x1.2

ملاحظة: أنت يستطيع أيضا استعملت أكثر من واحد مرشح في الأمر. على سبيل المثال، > show snort flow proto TCP src_ip x1.x1.x1.2 - إخراج تدفقات TCP التي تحتوي على src ip x1.x1.x1.2

## إستجابة الخطأ المحتمل

- يمكن لمستخدم واجهة سطر الأوامر (CLI) الحصول على إستجابة "غير قادر على معالجة الأمر، يرجى المحاولة مرة أخرى لاحقا".
- وهذا يحدث عندما يكون Snort 3 مشغول أو عندما يكون Snort 3 ال مثل معطل أو عندما يكون Snort 3 يقوم بمعالجة أوامر مأخذ التحكم (مثل مؤشرات الترابط في حالة التصق).
- شروط تشغيل واجهة سطر الأوامر (CLI) بنجاح:
  - النورتي 3 قيد التشغيل.
  - يستجيب Snort 3 لأوامر التحكم على مقبس مجال UNIX.

## إيقاف CLI/الإخراج

- مثل أي أمر CLI، يمكنك الحصول على موجه الأمر باضغط على CTRL+C، ولكن الأمر قد تم تمريره بالفعل إلى جميع مؤشرات ترابط الحزمة ويتم تشغيله إلى الإكمال في Snort.
- يتم إكمال الأمر عند تطبيق كل الشرطين:
  - تم عرض كافة التدفقات في ذاكرة التخزين المؤقت للتدفق
  - كل التدفقات التي تطابق عوامل التصفية في أمر CLI تمت كتابتها إلى الملفات التي تعمل كإدخال للأمر أن يتم إخراجه في CLI.

## تأثير الأداء

- هذه واجهة سطر أوامر (CLI) تصحيح أخطاء. في كل حزمة نقوم بتشغيلها، نلقي نظرة على حوالي 100 تدفق من جدول التدفق ونطبع التدفقات التي تطابق المعايير.
- يؤثر تشغيل تدفقات الشروط على الأداء.

# المراجع

## الأسئلة المتداولة

س: هل يمكنني إستخدام أكثر من عامل تصفية في إظهار تدفقات الشبكة؟

ج: نعم، تدعم واجهة سطر الأوامر (CLI) توفير أكثر من عامل تصفية واحد في كل مرة وتنتج تدفقات تطابق كل العوامل التصفية.

س: ما البروتوكولات المدعومة؟

ج: IP/TCP/UDP/ICMP

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).