معالجة جلسة كبيرة أحادية الدفق (تدفق الفيل) بواسطة خدمات FirePOWER

المحتويات

المقدمة

يوضح هذا المستند سبب عدم قدرة التدفق الواحد على استهلاك الإنتاجية المقدرة بالكامل لجهاز Cisco FirePOWER.

معلومات أساسية

قد لا تعرض نتيجة أي موقع ويب لاختبار سرعة النطاق الترددي، أو إخراج أي أداة قياس النطاق الترددي (على سبيل المثال، iPERF) تقييم الخرج المعلن لأجهزة Cisco FirePOWER. وبالمثل، فإن نقل ملف كبير جدا عبر أي بروتوكول نقل لا يوضح تقييم الخرج المعلن لجهاز FirePOWER. يحدث ذلك لأن خدمة FirePOWER لا تستخدم تدفق شبكة واحد لتحديد أقصى سعة معالجة لها.

معالجة حركة المرور بواسطة الشيخ

تقنية الكشف الأساسية الخاصة بخدمة FirePOWER هي Snort. تنفيذ نموذج على جهاز أمان FirePOWER من Cisco وهو عملية مؤشر ترابط واحد لمعالجة حركة المرور. يتم تقييم الجهاز للحصول على تقييم معين استنادا إلى إجمالي سعة المعالجة لجميع التدفقات التي تمر عبر الجهاز. ومن المتوقع أن يتم نشر الأجهزة الكهربائية على شبكة الشركة، التي عادة ما تكون بالقرب من الحافة الحدودية، وتعمل بآلاف الاتصالات.

تستخدم Firepower Services موازنة حمل حركة مرور البيانات إلى عدد من العمليات الصغيرة المختلفة باستخدام عملية نقل بيانات واحدة تعمل على كل وحدة معالجة مركزية (CPU) على الجهاز. ومن الناحية المثالية، يقوم حمل النظام بموازنة حركة مرور البيانات بشكل متساوٍ

عبر جميع عمليات النخر. يجب أن يتمكن الشخير من توفير التحليل السياقي المناسب لجدار الحماية من الجيل التالي (NGFW) ونظام منع التسلل (IPS) والفحص المتقدم للحماية من البرامج الضارة (AMP). لضمان أن الشخير أكثر فعالية، فإن حركة المرور من تدفق واحد يتم موازنة الحمل إلى مثيل شخير واحد. إذا لم يتم موازنة جميع حركات المرور من تدفق واحد إلى مثيل وحدة نخر واحد، يمكن تجنب النظام وستنتشر حركة المرور بطريقة قد تجعل احتمال مطابقة قاعدة النخر أقل وأن أجزاء الملف غير متصلة لفحص AMP. وبالتالي، تستند خوارزمية موازنة التحميل إلى معلومات الاتصال التي يمكنها تحديد اتصال معين بشكل فريد.

خوارزمية ذات 2 مجموعة في ASA مع خدمات FirePOWER و NGIPS Virtual

في جهاز الأمان القابل للتكيف (ASA) مع النظام الأساسي لخدمة FirePOWER والنظام الظاهري لنظام منع التسلل من الجيل التالي (NGIPS)، يتم موازنة حمل حركة المرور من أجل التطفل باستخدام خوارزمية مكونة من قطعتين. نقاط البيانات لهذه الخوارزمية هي:

- IP المصدر
- IP الوجهة

خوارزمية 3-مجموعة في الإصدار 5.3 من البرنامج أو أقل في أجهزة FirePOWER و FTD

في جميع الإصدارات السابقة (5.3 أو أقل)، يتم موازنة حمل حركة المرور إلى وحدة التخزين التي تستخدم خوارزمية مكونة من 3 مجموعات. نقاط البيانات لهذه الخوارزمية هي:

- IP المصدر
- IP الوجهة
- بروتوكول IP

أي حركة مرور بنفس المصدر، والوجهة، وبروتوكول IP تكون متوازنة الحمل إلى نفس مثيل الشوت.

خوارزمية 5-مجموعة في البرنامج الإصدار 6.0 و 5.4 والإصدارات الأكبر على أجهزة FirePOWER و FTD

في الإصدار 5.4 أو 6.0 أو أكثر، يتم موازنة حمل حركة المرور إلى وحدة الشبكة باستخدام خوارزمية مكونة من 5 قنوات. نقاط البيانات التي تؤخذ في الاعتبار هي:

- IP المصدر
- منفذ المصدر
- IP الوجهة
- غاية ميناء
- بروتوكول IP

الغرض من إضافة منافذ إلى الخوارزمية هو موازنة حركة المرور بشكل أكثر تساوي عندما يكون هناك أزواج مصدر ووجهة محددة تمثل أجزاء كبيرة من حركة المرور. بإضافة المنافذ، يجب أن تكون منافذ المصدر سريعة الزوال عالية الترتيب مختلفة لكل تدفق، ويجب إضافة انتروبي إضافية بشكل أكثر توازن لحركة المرور إلى مثيلات مختلفة من الشظية.

سعة المعالجة الإجمالية

يتم قياس الخرج الإجمالي للجهاز استنادا إلى الخرج الإجمالي لكل حالات الشخر التي تعمل

بأقصى إمكاناتها. يتم إستخدام الممارسات المتوافقة مع معايير الصناعة لقياس سعة المعالجة من أجل إتصالات HTTP المتعددة ذات أحجام الكائنات المختلفة. على سبيل المثال، تقوم منهجية إختبار NSS NGFW بقياس إجمالي سعة المعالجة للجهاز بكائنات تبلغ 44 و 21 و 10 و 4.4 و 1.7 كيلو. وهذه تترجم إلى نطاق من متوسط أحجام الحزم من حوالي 1 k بايت إلى 128 بايت بسبب الحزم الأخرى المعنية باتصال HTTP.

يمكنك تقدير تقييم أداء مثيل Snort فردي. خذ معدل الإنتاجية المقدر للجهاز وقسمه على عدد حالات الشخير التي تعمل. على سبيل المثال، إذا تم تقييم جهاز ما بسرعة 10 جيجابت في الثانية لنظام منع الاختراقات (IPS) بمتوسط حجم حزمة يبلغ 1 كيلو بايت، وكان هذا الجهاز يحتوي على 20 مثيل للتشذيب، فإن الحد الأقصى للإنتاجية التقريبي لمثيل واحد سيكون 500 ميجابت في الثانية لكل جهاز. يمكن أن تؤدي أنواع حركة المرور المختلفة والبروتوكولات الشبكة وأحجام الحزم بالإضافة إلى الاختلافات في سياسة الأمان العامة أن تؤثر جميعها على سعة المعالجة التي تمت ملاحظتها للجهاز.

نتيجة إختبار أداة الطرف الثالث

عندما تقوم بالاختبار باستخدام أي موقع لاختبار السرعة على الويب أو أي أداة لقياس النطاق الترددي مثل، iPerf، فإنه يتم إنشاء تدفق TCP واحد كبير ومتدفق. يسمى هذا النوع من تدفق TCP الكبير تدفق فيل. التدفق الهائل هو عبارة عن جلسة عمل واحدة ذات معدل بت عالي وطويلة نسبيا ويستهلك مقدارا كبيرا أو غير متناسب من عرض النطاق الترددي. يتم تعيين هذا النوع من التدفق لمثيل Snort واحد، وبالتالي تعرض نتيجة الاختبار معدل إنتاجية مثيل Snort الواحد، وليس تقييم معدل إنتاجية التجميع للجهاز.

الأعراض التي تم رصدها

وحدة معالجة مركزية (CPU) عالية ملحوظة

والتأثير الآخر الظاهر لتدفقات الفيلة يمكن ان يكون ال CPU العالي المثيل. ويمكن ملاحظة ذلك من خلال "show asp inspection-dp snort"، أو باستخدام أداة "top" shell.

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

Id  Pid   Cpu-Usage  Conns   Segs/Pkts  Status tot (usr | sys)
--  ----  ---------  -----   --------   ----------

0  48500  30% ( 28%|  1%)  12.4 K      0        READY
1  48474  24% ( 22%|  1%)  12.4 K      0        READY
2  48475  34% ( 33%|  1%)  12.5 K      1        READY
3  48476  29% ( 28%|  0%)  12.4 K      0        READY
4  48477  32% ( 30%|  1%)  12.5 K      0        READY
5  48478  31% ( 29%|  1%)  12.3 K      0        READY
6  48479  29% ( 27%|  1%)  12.3 K      0        READY
7  48480  23% ( 23%|  0%)  12.2 K      0        READY
8  48501  27% ( 26%|  0%)  12.6 K      1        READY
9  48497  28% ( 27%|  0%)  12.6 K      0        READY
10 48482  28% ( 27%|  1%)  12.3 K      0        READY
11 48481  31% ( 30%|  1%)  12.5 K      0        READY
12 48483  36% ( 36%|  1%)  12.6 K      0        READY
13 48484  30% ( 29%|  1%)  12.4 K      0        READY
14 48485  33% ( 31%|  1%)  12.6 K      0        READY
```

```
15 48486  38% ( 37%|  0%)  12.4 K      0        READY
16 48487  31% ( 30%|  1%)  12.4 K      1        READY
17 48488  37% ( 35%|  1%)  12.7 K      0        READY
18 48489  34% ( 33%|  1%)  12.6 K      0        READY
19 48490  27% ( 26%|  1%)  12.7 K      0        READY
20 48491  24% ( 23%|  0%)  12.6 K      0        READY
21 48492  24% ( 23%|  0%)  12.6 K      0        READY
22 48493  28% ( 27%|  1%)  12.4 K      1        READY
23 48494  27% ( 27%|  0%)  12.2 K      0        READY
24 48495  29% ( 28%|  0%)  12.5 K      0        READY
25 48496  30% ( 30%|  0%)  12.4 K      0        READY
26 48498  29% ( 27%|  1%)  12.6 K      0        READY
27 48517  24% ( 23%|  1%)  12.6 K      0        READY
28 48499  22% ( 21%|  0%)  12.3 K      1        READY
29 48518  31% ( 29%|  1%)  12.4 K      2        READY
30 48502  33% ( 32%|  0%)  12.5 K      0        READY

31 48514 80% ( 80%| 0%) 12.7 K 0 READY <<< CPU 31 is much busier than the rest, and will stay
busy for while with elephant flow.

32 48503  49% ( 48%|  0%)  12.4 K      0        READY
33 48507  27% ( 25%|  1%)  12.5 K      0        READY
34 48513  27% ( 25%|  1%)  12.5 K      0        READY
35 48508  32% ( 31%|  1%)  12.4 K      0        READY
36 48512  31% ( 29%|  1%)  12.4 K      0        READY



$ top

PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND

69470 root       1 -19 9088m 1.0g  96m R   80  0.4 135:33.51 snort     <<<< one snort very busy,
rest below 50%

69468 root       1 -19 9089m 1.0g  99m R   49  0.4 116:08.69 snort
69467 root       1 -19 9078m 1.0g  97m S   47  0.4 118:30.02 snort
69492 root       1 -19 9118m 1.1g  97m R   47  0.4 116:40.15 snort
69469 root       1 -19 9083m 1.0g  96m S   39  0.4 117:13.27 snort
69459 root       1 -19 9228m 1.2g  97m R   37  0.5 107:13.00 snort
69473 root       1 -19 9087m 1.0g  96m R   37  0.4 108:48.32 snort
69475 root       1 -19 9076m 1.0g  96m R   37  0.4 109:01.31 snort
69488 root       1 -19 9089m 1.0g  97m R   37  0.4 105:41.73 snort
69474 root       1 -19 9123m 1.1g  96m S   35  0.4 107:29.65 snort
69462 root       1 -19 9065m 1.0g  99m R   34  0.4 103:09.42 snort
69484 root       1 -19 9050m 1.0g  96m S   34  0.4 104:15.79 snort
69457 root       1 -19 9067m 1.0g  96m S   32  0.4 104:12.92 snort
69460 root       1 -19 9085m 1.0g  97m R   32  0.4 104:16.34 snort
```

مع خوارزمية 5-Tuple الموضحة أعلاه، سيتم إرسال التدفق الذي يستغرق فترة طويلة إلى (AVC) مثيل الشخ نفسه. إذا كانت هناك سياسات شاملة للتوافق الكهرومغناطيسي والتشغيل الفوري (IPS) والملفات وما إلى ذلك نشطة في جهاز التنفس، فيمكن ملاحظة أن وحدة المعالجة المركزية (CPU) مرتفعة (>80٪) على مثيل جهاز تنصت لفترة من الوقت. ستؤدي إضافة سياسة SSL إلى زيادة إستخدام وحدة المعالجة المركزية إلى الطبيعة المكلفة حسابيا لفك تشفير SSL.

الى يعد إرتفاع مستوى وحدة المعالجة المركزية (CPU) في عدد قليل من وحدات المعالجة المركزية التي تحتوي على نسبة تنكس كبيرة سبب للإنذار النقدي. وهو سلوك نظام وهذا يمكن أن يستخدم بشكل في NGFW فحص متعمق للحزم في تدفق البيانات، و إجراء طبيعي أجزاء كبيرة من وحدة المعالجة المركزية (CPU). وكمبدأ توجيهي عام، العيانى الصندوق الوطني من حالة تجويع حرجة في وحدة المعالجة المركزية (CPU) إلى أن يتجاوز

مع ظم وحدات المعالجة المركزية للمشكل 95 في المائة ويظل أكثر من 95 في المائة ويتم مالحظة حاالت انخفاض في الحزم.

وستساعد العالجات الواردة أدناه في إرتفاع حالة وحدة المعالجة المركزية بسبب تدفقات الفيلة.

عالجات

تجاوز التطبيقات الذكية (IAB)

يقدم اإلصدار 6.0 من البرنامج ميزة جديدة تسمى IAB. عندما يصل جهاز أمان FirePOWER إلى حد أداء محدد مسبقا، تبحث ميزة IAB عن التدفقات التي تستوفي معايير محددة من أجل تجاوز هذا المستوى بذكاء مما يخفف الضغط على محركات الكشف.

> **تلميح**: يمكن العثور على مزيد من المعلومات حول تكوين IAB هنا.

تحديد التدفقات الكبيرة والثقة بها

غالبا ما ترتبط التدفقات الكبيرة بحركة مرور ذات قيمة فحص منخفضة عالية االستخدام، على سبيل المثال، عمليات النسخ االحتياطي ونسخ قاعدة البيانات، وما إلى ذلك. العديد من هذه التطبيقات ال يمكن االستفادة منها في الفحص. لتجنب المشاكل المتعلقة بالتدفقات الكبيرة، يمكنك تحديد التدفقات الكبيرة وإنشاء قواعد ثقة التحكم بالوصول لها. ويمكن لهذه القواعد أن تحدد التدفقات الكبيرة على نحو فريد، وأن تسمح لتلك التدفقات بأن تمر دون تفتيش، أو الكون مقيدة بسلوك مثيل الشخير الواحد.

> **مالحظة**: لتحديد التدفقات الكبيرة لقواعد الثقة، اتصل ب TAC FirePOWER من Cisco.

معلومات ذات صلة

- التحكم في الوصول باستخدام تجاوز التطبيقات الذكية
- الدعم التقني والمستندات - Cisco Systems

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).