توضيح إستخدام وحدة المعالجة المركزية (CPU) الخاصة بعملية دفاع تهديد الطاقة النارية

المحتويات

المقدمة

س: لماذا تستهلك عملية lina الخاصة بالدفاع عن تهديد الطاقة النارية 100٪ (أو أكثر) من وحدة المعالجة المركزية؟

أ: هذا عادي لأن عملية lina تحقق باستمرار في بطاقات واجهة الشبكة (NICs) لحركة مرور الإدخال. وباختصار، يمكن تجاهل إستخدام عملية لينا بأمان.

تمت المساهمة من قبل ميكيس زافيروديس، و إجناسيو بينالفا، و هيثم جرادات و ديفيد توريس ريفاس، و مهندسي TAC من Cisco.

تحليل

الدفاع ضد تهديد Firepower هو نظام تشغيل موحد يتكون من محركين (ASA و Snort).

يوضح واجهة سطر الأوامر في FTD أن عملية 'lina' (محرك ASA) تستهلك الكثير من دورات وحدة المعالجة المركزية. وفيما يلي مثال على FTD يعمل على جهاز ASA5506-X:

```
> system support utilization
top - 01:26:40 up 12 days, 16:00,  1 user,  load average: 22.08, 22.10, 22.10
Tasks: 161 total,   1 running, 159 sleeping,   0 stopped,   1 zombie
Cpu(s): 22.6%us,  4.1%sy,  0.0%ni, 73.2%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   3927684k total,  2793860k used,   120904k free,   181548k buffers
Swap:  3996668k total,   257632k used,  3739036k free,   831372k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
--> root       0 -20 1138m 513m  91m S   99 13.4  18205:20 lina 23000
    admin     20   0 15240 1156  848 R    2  0.0   0:00.02 top 2952
root      20   0  266m 2316 2108 S    2  0.1  47:16.70 ndmain.bin 22941
    root      20   0  4232  652  620 S    0  0.0   0:12.40 init 1
```

في الإخراج المذكور أعلاه، يجب أن تأخذ بعين الاعتبار إستخدام وحدة المعالجة المركزية (CPU) (النظام) + sy للولايات المتحدة الأمريكية مع قيمة المعرف (خامل - غير مستخدم).

هنا من FTD يعمل على جهاز FPR-9300:

```
> system support utilization
top - 04:30:22 up 40 days,  5:22,  0 users,  load average: 26.12, 26.10, 26.13
          Tasks: 568 total,   1 running, 566 sleeping,   0 stopped,   1 zombie
Cpu(s): 22.1%us,  0.2%sy,  0.0%ni, 77.6%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
    Mem:  264374828k total, 28976700k used, 234868048k free,      268k buffers
       Swap:        0k total,        0k used,        0k free,   529812k cached

          PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
           --> root       0 -20 24.8g 541m  88m S 1593 0.2 927288:05lina 12772
           mysql     20   0 3063m 150m 9140 S    4  0.1  56:28.39 mysqld 12594
         root      20   0 24696 2848 1192 S    2  0.0 422:45.07 pdts_proc 12608
              admin     20   0 15648 1484  844 R    2  0.0   0:00.01 top 43145
             root      20   0  4232  632  552 S    0  0.0   0:15.43 init 1
```

التوصيات

- في 'إستخدام دعم النظام' تجاهل إستخدام العملية 'lina'.
- لمراقبة إستخدام وحدة المعالجة المركزية (CPU) الخاصة ب FTD، تحقق من قيم 'id' + 'sys' + 'us'
- فيما يتعلق بمراقبة محرك ASA، يجب عليك التحقق من المخرجات التالية:

الناتج 1

```
> show cpu usage
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
```

الناتج 2

```
> show processes cpu-usage sorted non-zero
  PC                 Thread             5Sec     1Min     5Min   Process
0x00007f42428f1fd9   0x00007f42290b9ea0  0.2%     0.0%     0.0%   ci/console
```

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).