

Aclarando la defensa LINA de la amenaza de FirePOWER procese la utilización de la CPU

Contenido

[Introducción](#)

[Análisis](#)

[Recomendaciones](#)

Introducción

A: ¿Por qué el proceso de Lina en la defensa de la amenaza de FirePOWER consume el 100% (o más) CPU?

R: Esto es normal porque el proceso de Lina está sondeando constantemente el Network Interface Cards (NIC) para el tráfico de entrada. En fin, la utilización del proceso de Lina puede ser ignorada con seguridad.

Contribuido por Mikis Zafeiroudís, Ignacio Penalva, Haitham Jaradat y David Torres Rivas, ingenieros de Cisco TAC.

Análisis

La defensa de la amenaza de FirePOWER es un sistema operativo unificado que consiste en 2 motores (ASA y Snort).

El FTD CLI muestra que el proceso de “Lina” (motor ASA) consume muchos ciclos de la CPU. Aquí está un ejemplo de un FTD que se ejecuta en el dispositivo 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
23000 root        0  -20 1138m 513m  91m  S   99  13.4 18205:20 lina <--
 2952 admin       20   0 15240 1156  848  R    2   0.0   0:00.02 top
22941 root       20   0  266m 2316 2108  S    2   0.1  47:16.70 ndmain.bin
    1 root       20   0  4232  652  620  S    0   0.0   0:12.40 init
```

En la salida antedicha usted debe tomarnos realmente en la consideración (usuario) + utilización

de la CPU sy (del sistema) junto con el valor identificación (marcha lenta - no usada).

Aquí es de un FTD el ejecutarse en el dispositivo del 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
12772	root	0	-20	24.8g	541m	88m	S	1593	0.2	927288:05	lina <--
12594	mysql	20	0	3063m	150m	9140	S	4	0.1	56:28.39	mysqld
12608	root	20	0	24696	2848	1192	S	2	0.0	422:45.07	pdts_proc
43145	admin	20	0	15648	1484	844	R	2	0.0	0:00.01	top
1	root	20	0	4232	632	552	S	0	0.0	0:15.43	init

Recomendaciones

- En la “utilización del soporte de sistema” ignora la utilización del proceso de “Lina”.
- Para monitorear la utilización de la CPU FTD marque los valores “nosotros” + del “sys” + “identificación”
- En relación con la supervisión del motor ASA usted debe marcar los productos siguientes:

Salida 1

```
> show cpu usage
```

```
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
```

Salida 2

```
> show processes cpu-usage sorted non-zero
```

PC	Thread	5Sec	1Min	5Min	Process
0x00007f42428f1fd9	0x00007f42290b9ea0	0.2%	0.0%	0.0%	ci/console