Uso elevado de la CPU en DATAPATH y problemas de conectividad en FTD debido a conexiones embrionarias excesivas

Contenido

Problema

Se observó un uso elevado de la CPU en los dispositivos FTD, lo que provocó problemas de conectividad e impidió que los usuarios accedieran a las aplicaciones empresariales críticas. El firewall mostró un uso elevado de la CPU de Snort y de la ruta de datos, con usuarios que experimentaban problemas de latencia y de acceso intermitente. La investigación reveló un gran número de conexiones TCP embrionarias, con una parte significativa originada en los analizadores de seguridad internos, lo que provocó el agotamiento de los recursos y la degradación del rendimiento.

Entorno

- Cisco Secure Firewall Firepower Threat Defense (FTD)
- Hardware Cisco Firepower 1150
- Versión del software: 7.4.2.3
- Administrado por: Centro de administración Firepower (FMC)
- Configuración de alta disponibilidad (HA)
- Datapath y CPU Snort consistentemente al 100% o cerca de él
- Gran número de conexiones TCP embrionarias debido a los escáneres internos
- Cambios recientes: Configuraciones del recolector de registros aplicadas y revertidas; implementación de reglas de acceso; evento de failover observado
- Sistemas que generan conexiones altas identificados como analizadores Qualys internos

Resolución

Uso elevado de la CPU identificado en DATAPATH utilizado para el procesamiento del tráfico.

```
device# show processes cpu-usage sorted non-zero
Hardware:   FPR-1150
Cisco Adaptive Security Appliance Software Version 9.20(2)43
ASLR enabled, text region 562a19048000-562a1e49126d
PC         Thread       5Sec     1Min     5Min   Process
   -          -        99.7%    99.7%    99.7%   DATAPATH-4-22658
   -          -        99.7%    99.7%    99.6%   DATAPATH-3-22657
   -          -        99.7%    99.6%    99.6%   DATAPATH-2-22656
```

```
   -          -        99.6%    99.7%    99.7%   DATAPATH-5-22659
   -          -        97.5%    97.1%    97.1%   DATAPATH-1-22655
   -          -        97.4%    97.1%    97.1%   DATAPATH-0-22654
0x0000562a1b8c55e3   0x0000151e97f523e0     1.1%     1.6%     1.6%   CP Processing
0x0000562a1d408771   0x0000151e97f434a0     0.4%     0.2%     0.0%   Unicorn Proxy Thread
0x0000562a1b6ba40a   0x0000151e97f3cb80     0.3%     0.3%     0.3%   appagent_async_client_receive_thre
0x0000562a1cfebc65   0x0000151e97f43f80     0.1%     0.1%     0.1%   IP SLA Mon Event Processor
0x0000562a1d328a89   0x0000151e97f64240     0.1%     0.1%     0.1%   lina logclient Rx data thread
0x0000562a1d72eb46   0x0000151e97f417a0     0.0%     0.1%     0.0%   cli_xml_request_process
0x0000562a1df983a5   0x0000151e97f69940     0.0%     0.1%     0.0%   Checkheaps
```

Desde la CLI de FTD, se exportó una salida de show conn detail para que las herramientas de automatización interna revisen las estadísticas de conexión.

PRECAUCIÓN: la salida de show conn detail de la CLI puede ser extremadamente larga si el recuento de conexiones es superior a 100.000. Asegúrese de que se asigne tiempo suficiente para esta recopilación.

El disk0 se corresponde con el directorio /mnt/disk0/ del motor FTD. Exporte el archivo en consecuencia.

```
device# show conn detail | redirect disk0:/shconndetMMDDYY.txt
```

Revise las estadísticas de conexión de los resultados de la herramienta para conexiones embrionarias en grandes cantidades:

```
Total Emryonic Conns: 121611. This is 87.984% of the total conns (138219)
--
Top-5  Embryonic IPs (SYN, but not SYN/ACK - 'aA' flags) going through the device
IP                                              Count    Percent
-----------------------------------------------------------------
10.5.30.77                                      81519    33.517%
10.1.30.102                                     40042    16.463%
10.1.212.14                                       907     0.373%
10.1.204.4                                        837     0.344%
10.1.21.122                                       804     0.331%
```

Después de identificar las IP de origen (en este caso, los escáneres de seguridad interna), evite que el origen genere el tráfico y borre sus conexiones del FTD.

```
device# clear conn add 10.5.30.77
4563 connection(s) deleted.
device# show conn count
5936 in use, 465189 most used
Inspect Snort:
        preserve-connection: 4451 enabled, 0 in effect, 432406 most enabled, 0 most in effect
```

Supervise el uso de la CPU después de la mitigación para confirmar que la causa fue el tráfico inducido.

```
device# show cpu
CPU utilization for 5 seconds = 9%; 1 minute: 28%; 5 minutes: 70%
```

La conectividad del tráfico debería volver a la normalidad y ya no debería observarse la latencia.

Causa

La causa principal de los problemas de CPU y conectividad elevados fueron las conexiones embrionarias excesivas generadas por los analizadores de seguridad internos. Estas conexiones, principalmente paquetes SYN sin las correspondientes respuestas SYN/ACK, saturaron los procesos Snort y de ruta de datos FTD. El alto volumen de conexiones incompletas condujo al agotamiento de los recursos, lo que dio como resultado una alta utilización continua de la CPU, conectividad intermitente y un impacto en el acceso a las aplicaciones críticas para la empresa.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).