Elevata CPU su DATAPATH e problemi di connettività su FTD a causa di connessioni embrionali eccessive

Sommario

Problema

Sui dispositivi FTD è stato osservato un elevato utilizzo della CPU, che ha causato problemi di connettività e ha impedito agli utenti di accedere ad applicazioni aziendali critiche. Il firewall ha rilevato un elevato livello di percorso dei dati e un utilizzo elevato della CPU Snort, con gli utenti che hanno riscontrato problemi di latenza e di accesso intermittente. Dalle indagini è emerso un numero elevato di connessioni TCP embrionali, con una parte significativa derivante da scanner di sicurezza interni, che hanno causato l'esaurimento delle risorse e una riduzione delle prestazioni.

Ambiente

- Cisco Secure Firewall Firepower Threat Defense (FTD)
- Hardware: Cisco Firepower 1150
- Versione del software: 7.4.2.3
- Gestito da: Firepower Management Center (FMC)
- Configurazione ad alta disponibilità (HA, High Availability)
- Datapath e Snort CPU sempre al 100% o quasi
- Numero elevato di connessioni TCP embrionali a causa di scanner interni
- Modifiche recenti: Configurazioni del raccoglitore di tronchi applicate e ripristinate. distribuzione delle regole di accesso; evento di failover osservato
- Sistemi che generano connessioni elevate identificate come scanner Qualys interni

Risoluzione

Identificato utilizzo elevato della CPU su DATAPATH utilizzato per l'elaborazione del traffico.

```
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
```

Dalla CLI di FTD, un output di show conn detail è stato esportato per la revisione delle statistiche di connessione da parte degli strumenti di automazione interni.

ATTENZIONE: l'output del comando show conn detail dalla CLI può essere estremamente lungo se il numero di connessioni è superiore a 100.000. Accertarsi che sia stato assegnato tempo sufficiente per questa raccolta.

Il disco0 corrisponde alla directory /mnt/disk0/ nel back-end FTD. Esportare il file di conseguenza.

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

Esaminate le statistiche di connessione dai risultati dello strumento per le connessioni embrionali in grandi quantità:

```
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%
```

Dopo aver identificato gli IP di origine (in questo caso, gli scanner di sicurezza interni), impedire alla sorgente di generare il traffico e cancellare le sue connessioni dall'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
```

Monitorare l'utilizzo della CPU dopo la mitigazione per verificare che la causa sia stata indotta dal traffico.

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

La connettività del traffico deve tornare alla normalità e la latenza non deve più essere osservata.

Causa

La causa principale degli elevati problemi di CPU e connettività sono state le eccessive connessioni embrionali generate dagli scanner di sicurezza interni. Queste connessioni, principalmente pacchetti SYN senza corrispondenti risposte SYN/ACK, hanno sovraccaricato i processi Snort e datapath FTD. L'elevato volume di connessioni incomplete ha portato all'esaurimento delle risorse, con conseguente elevato utilizzo della CPU, connettività intermittente e impatto sull'accesso alle applicazioni business-critical.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).