CPU élevé sur DATAPATH et problèmes de connectivité sur FTD en raison de connexions embryonnaires excessives

Table des matières

Problème

Une utilisation élevée de l'UC a été observée sur les périphériques FTD, entraînant des problèmes de connectivité et empêchant les utilisateurs d'accéder aux applications métier critiques. Le pare-feu présentait une utilisation élevée du chemin de données et de l'UC Snort, avec des utilisateurs rencontrant des problèmes de latence et d'accès intermittents. L'enquête a révélé un grand nombre de connexions TCP embryonnaires, dont une partie importante provenait d'analyseurs de sécurité internes, entraînant une épuisement des ressources et une dégradation des performances.

Environnement

- Cisco Secure Firewall Firepower Threat Defense (FTD)
- Matériel : Cisco Firepower 1150
- Version du logiciel: 7.4.2.3
- Géré par : Firepower Management Center (FMC)
- Configuration haute disponibilité (HA)
- Datapath et Snort CPU toujours à 100 % ou presque
- Nombre élevé de connexions TCP embryonnaires en raison de scanners internes
- Modifications récentes : Configurations du collecteur de journaux appliquées et réinitialisées ; déploiement des règles d'accès ; événement de basculement observé
- Systèmes générant des connexions élevées identifiés comme scanners Qualys internes

Résolution

Utilisation CPU élevée identifiée sur DATAPATH utilisée pour le traitement du trafic.

```
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
```

À partir de l'interface de ligne de commande FTD, une sortie de show conn detail a été exportée pour la révision des statistiques de connexion par les outils d'automatisation internes.

ATTENTION : le résultat de la commande show conn detail de l'interface de ligne de commande peut être extrêmement long si le nombre de connexions est supérieur à 100 000. Assurez-vous que le temps alloué à cette collecte est suffisant.

Le disk0 correspond au répertoire /mnt/disk0/ du serveur principal FTD. Exportez le fichier en conséquence.

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

Examinez les statistiques de connexion à partir des résultats de l'outil pour les connexions embryonnaires en grandes quantités :

```
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%
```

Après avoir identifié les adresses IP source (dans ce cas, des scanners de sécurité internes), empêchez la source de générer le trafic et effacez ses connexions du 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
```

Surveillez l'utilisation du processeur après la réduction pour confirmer que la cause est due au trafic.

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

La connectivité du trafic doit revenir à la normale et la latence ne doit plus être observée.

Motif

La cause principale des problèmes de CPU et de connectivité élevés était un nombre excessif de connexions embryonnaires générées par les scanners de sécurité internes. Ces connexions, principalement des paquets SYN sans réponses SYN/ACK correspondantes, ont submergé les processus FTD datapath et Snort. Le volume élevé de connexions incomplètes a conduit à l'épuisement des ressources, ce qui a entraîné une utilisation élevée et soutenue du CPU, une connectivité intermittente et un impact sur l'accès aux applications critiques de l'entreprise.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.