CPU alta em DATAPATH e problemas de conectividade em FTD devido ao excesso de conexões embrionárias

Contents

Problema

Foi observada uma alta utilização da CPU em dispositivos FTD, levando a problemas de conectividade e impedindo que os usuários acessem aplicativos empresariais críticos. O firewall exibiu um caminho de dados elevado e uso da CPU Snort, com os usuários tendo problemas de latência e acesso intermitente. A investigação revelou um grande número de conexões TCP embrionárias, com uma parte significativa originada de verificadores de segurança internos, resultando no esgotamento de recursos e no desempenho degradado.

Ambiente

- Defesa contra ameaças (FTD) do Cisco Secure Firewall Firepower
- Hardware: Cisco Firepower 1150
- Versão de software: 7.4.2.3
- Gerenciado por: Firepower Management Center (FMC)
- Configuração de alta disponibilidade (HA)
- Datapath e Snort CPU consistentemente em ou perto de 100%
- Alto número de conexões TCP embrionárias devido a scanners internos
- Alterações recentes: Configurações do coletor de logs aplicadas e revertidas; implantação de regra de acesso; evento de failover observado
- Sistemas que geram conexões elevadas identificadas como scanners Qualys internos

Resolução

Alto Uso de CPU Identificado em DATAPATH usado para processamento de tráfego.

```
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
```

Na CLI do FTD, uma saída de show conn detail foi exportada para revisão das estatísticas de conexão por ferramentas de automação internas.

CUIDADO: a saída de show conn detail da CLI poderá ser extremamente longa se a contagem de conexões for superior a 100.000. Certifique-se de que haja tempo suficiente alocado para essa coleção.

O disk0 corresponde ao diretório /mnt/disk0/ no back-end do FTD. Exporte o arquivo adequadamente.

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

Revise as estatísticas de conexão a partir dos resultados da ferramenta para conexões embrionárias em grandes quantidades:

```
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%
```

Depois de identificar os IPs de origem (neste caso, os scanners de segurança internos), impeça a origem de gerar o tráfego e limpe suas conexões do 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
```

Monitore a utilização da CPU após a mitigação para confirmar se a causa foi induzida pelo tráfego.

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

A conectividade de tráfego deve voltar ao normal e a latência não deve mais ser observada.

Causa

A causa principal de problemas de CPU e conectividade altas foi o excesso de conexões embrionárias geradas por verificadores de segurança internos. Essas conexões, principalmente pacotes SYN sem respostas SYN/ACK correspondentes, sobrecarregaram os processos de caminho de dados FTD e Snort. O alto volume de conexões incompletas levou à exaustão de recursos, resultando em alta utilização sustentada da CPU, conectividade intermitente e impacto no acesso de aplicativos críticos para os negócios.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.