과도한 원시 연결로 인한 FTD의 연결 문제 및 DATAPATH의 높은 CPU

목차

문제

FTD 장치에서 CPU 사용률이 높으면 연결 문제가 발생하고 사용자가 중요한 비즈니스 애플리케이션에 액세스하지 못하게 되는 현상이 관찰되었습니다. 방화벽은 데이터 경로 및 Snort CPU 사용량이 증가했으며, 사용자는 지연 및 간헐적 액세스 문제를 겪었습니다. 조사 결과, 상당수의 미발달 TCP 연결이 내부 보안 스캐너에서 비롯되어 리소스 소진과 성능 저하가 발생했습니다.

환경

- Cisco Secure Firewall FTD(Firepower 위협 방어)
- 하드웨어: Cisco Firepower 1150
- 소프트웨어 버전: 7.4.2.3
- 관리자: FMC(Firepower Management Center)
- 고가용성(HA) 컨피그레이션
- 데이터 경로 및 Snort CPU가 일관적으로 100% 또는 거의
- 내부 스캐너로 인해 초기 TCP 연결 수가 많음
- 최근 변경 내용: 로그 컬렉터 컨피그레이션이 적용 및 되돌림, 액세스 규칙 배포; 관찰된 장애 조치 이벤트
- 내부 Qualys 스캐너로 식별된 높은 연결을 생성하는 시스템

해결

트래픽 처리에 사용되는 DATAPATH에서 높은 CPU 사용량을 확인했습니다.

```
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
```

FTD CLI에서 내부 자동화 툴에 의한 연결 통계 검토를 위해 show conn detail의 출력을 내보냈습니다.

주의: 연결 수가 100,000을 초과하는 경우 CLI에서 show conn detail의 출력이 매우 길 수 있습니다. 이 컬렉션에 충분한 시간이 할당되었는지 확인하십시오.

disk0은 FTD 백엔드의 /mnt/disk0/ 디렉토리에 해당합니다. 그에 따라 파일을 내보냅니다.

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

원시 연결에 대한 툴 결과의 연결 통계를 다량으로 검토합니다.

```
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%
```

소스 IP(이 경우 내부 보안 스캐너)를 식별한 후에는 소스에서 트래픽을 생성하지 못하게 하고 FTD에서 연결을 지웁니다.

```
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
```

차단 후 CPU 사용률을 모니터링하여 원인이 트래픽으로 인해 유발되었음을 확인합니다.

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

트래픽 연결은 정상으로 되돌려야 하며, 레이턴시는 더 이상 지켜지지 않아야 합니다.

원인

높은 CPU 및 연결 문제의 근본 원인은 내부 보안 스캐너에서 과도한 초기 연결이 생성되었습니다. 이러한 연결, 즉 주로 SYN/ACK 응답이 없는 SYN 패킷은 FTD 데이터 경로 및 Snort 프로세스에 과중한 영향을 주었습니다. 불완전한 연결의 많은 볼륨은 리소스 소진을 초래하여 높은 CPU 사용률, 간헐적 연결 및 업무상 중요한 애플리케이션 액세스에 미치는 영향을 지속했습니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.