보안 방화벽 FTD 이벤트 로깅이 DNS 확인으로 인해 실패함

문제

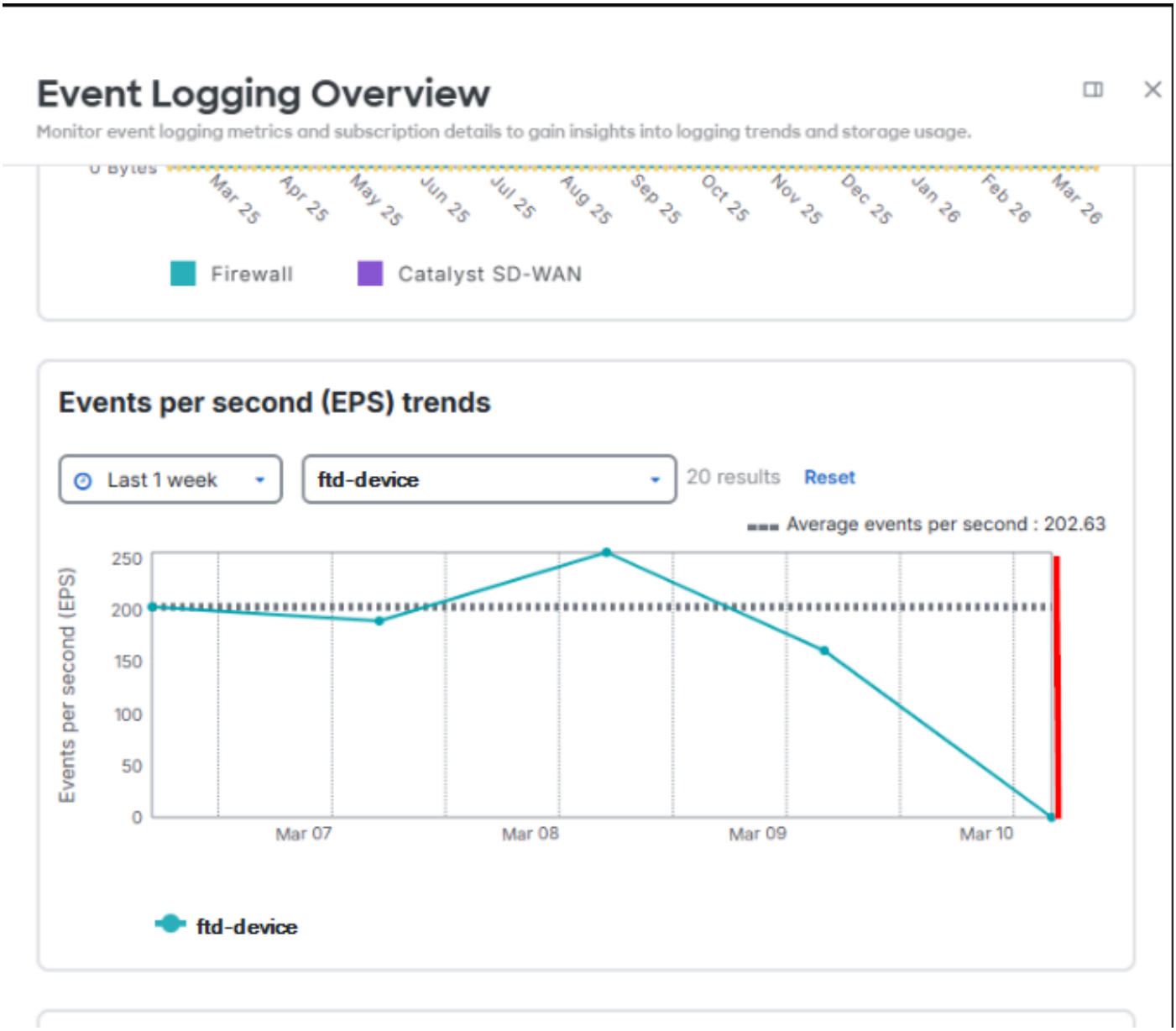
연결 이벤트 로깅이 단일 FTD(Firewall Threat Defense)에 대한 CDO(Cisco Defense Orchestrator) 이벤트 로깅 및 클라우드 제공 cdFMC(Firewall Management Center) 이벤트 페이지에서 중지되었습니다. 영향을 받는 디바이스에서 연결 이벤트 로그를 클라우드 관리 플랫폼으로 전송하지 못하여 프로덕션 가시성 및 문제 해결 기능에 영향을 주었습니다. 분석 결과, FTD에서 일시적인 이름 확인 실패 때문에 Cisco 이벤트 서비스에 연결하는 데 반복적으로 장애가 발생했으며, DNS 확인 실패 타임스탬프는 이벤트 페이지에서 연결 이벤트가 중단된 시점과 정확히 관련이 있었습니다.

환경

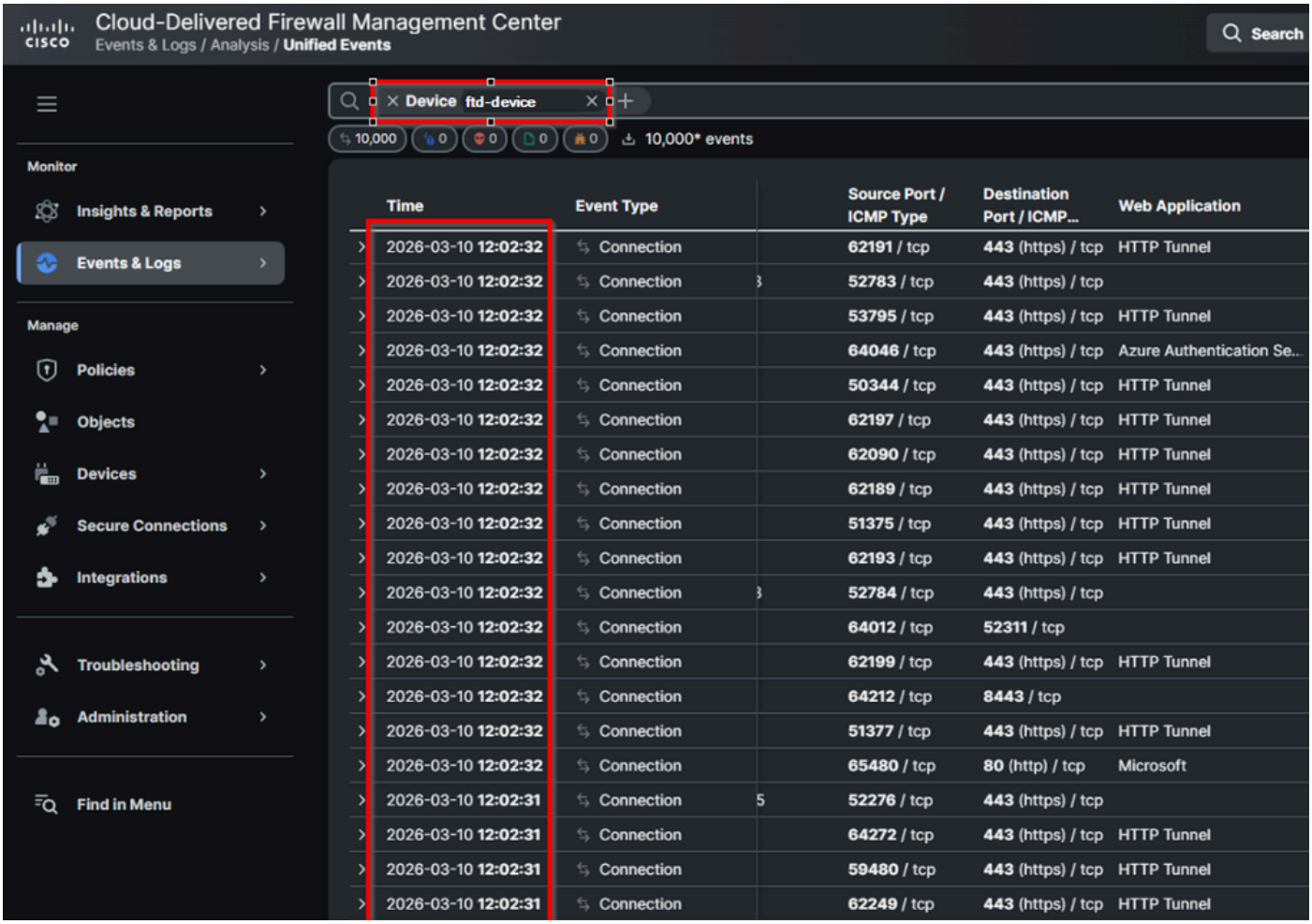
- Cisco Secure Firewall FTD는 cdFMC를 사용하여 CDO에서 관리됨
- FTD 관리 인터페이스에 구성된 DNS 서버
- 문제 해결을 위해 연결 이벤트 가시성이 필요한 프로덕션 환경

해결

1: CDO Event Logging(CDO 이벤트 로깅) 및 cdFMC Unified/Connection Event(cdFMC 통합/연결 이벤트) 페이지에서 이벤트 손실 시간을 확인합니다.



inline_image_0.png



인라인 이미지_1.png

2: 이벤트 생성 및 전송을 허용하는 데 필요한 FTD 프로세스가 실행 중인지 확인합니다.

```
root@ftd-device:/ngfw/var/log# pmtool status | grep Event
Required by: SFDataCorrelator,expire-session,TSS_Daemon,snapshot_manager,fpcollect,Syncd,Pruner,ActionQ
EventHandler (normal) - Running 17453
Command: /ngfw/usr/local/sf/bin/EventHandler
    LD_LIBRARY_PATH=/ngfw/usr/local/sf/lib64/EventHandlerModules
PID File: /ngfw/var/sf/run/EventHandler.pid
Enable File: /ngfw/etc/sf/EventHandler.run
--
root@ftd-device:/ngfw/var/log# pmtool status | grep SSE
SSEConnector (system) - Running 20697
Required by: ngfwManager,ASAConfig,tomcat,SSEConnector,rsyncd,hmdaemon,srt,9a0171ac-8dcf-11ec-9811-c22a
```

3: FTD를 검토하여 원인을 나타내는 EventHandler 및 Connector 로그 데이터의 상관관계를 찾습니다.

```
/ngfw/var/log/EventHandlerStat.* | grep -E "TotalEvents|SSEConnector"
{"Time": "2026-03-10T16:00:25Z", "TotalEvents": 104659, "PerSec": 348, "UserCPUSec": 9.242, "SysCPUSec"
{"Time": "2026-03-10T16:00:25Z", "Consumer": "SSEConnector", "Events": 104649, "PerSec": 348, "CPUSec":
{"Time": "2026-03-10T16:00:25Z", "ConsumerEvent": "SSEConnector-ConnectionEvent", "InTransforms": 10464
```

```
{"Time": "2026-03-10T16:05:25Z", "TotalEvents": 57651, "PerSec": 192, "UserCPUSec": 5.382, "SysCPUSec":
{"Time": "2026-03-10T16:05:25Z", "Consumer": "SSEConnector", "Events": 57641, "PerSec": 192, "CPUSec":
{"Time": "2026-03-10T16:05:25Z", "ConsumerEvent": "SSEConnector-ConnectionEvent", "InTransforms": 57641
{"Time": "2026-03-10T16:10:25Z", "TotalEvents": 24, "PerSec": 0, "UserCPUSec": 0.314, "SysCPUSec": 0.54
{"Time": "2026-03-10T16:10:25Z", "Consumer": "SSEConnector", "Events": 14, "PerSec": 0, "CPUSec": 0.046
{"Time": "2026-03-10T16:10:25Z", "ConsumerEvent": "SSEConnector-ConnectionEvent", "InTransforms": 14, "
{"Time": "2026-03-10T16:15:25Z", "TotalEvents": 10, "PerSec": 0, "UserCPUSec": 0.214, "SysCPUSec": 0.60
{"Time": "2026-03-10T16:15:25Z", "Consumer": "SSEConnector", "Events": 0, "PerSec": 0, "CPUSec": 0.009,
{"Time": "2026-03-10T16:10:25Z", "ConsumerEvent": "SSEConnector-ConnectionEvent", "InTransforms": 0, "O
---
/ngfw/var/log/messages | grep "SSEConnector"
Mar 12 11:36:01 plcdc-edgefw01 SF-IMS[62079]: [62112] EventHandler:EventHandler [ERROR] Consumer SSECon
---
/ngfw/var/log/connector/connector.log | grep "failure in name resolution"
time="2026-03-10T12:02:44.329750985-04:00" level=error msg="[ftd-device][events.go:100 events:connectWe
time="2026-03-10T12:02:44.329830226-04:00" level=warning msg="[ftd-device][events.go:181 events:(*Servi
```

4: FTD가 구성된 DNS 서버 및 연결 가능성을 확인합니다.

```
> show network
===============[System Information]===============
Hostname                : ftd-device
DNS Servers             : 10.0.0.10
DNS from router         : enabled
Management port         : 8305
IPv4 Default route
  Gateway               : 10.0.0.1
==================[management0]===================
Admin State             : Enabled
Admin Speed             : 40gbps
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : A1:A2:A3:A4:A5:A6
----------------------[IPv4]----------------------
Configuration           : Manual
Address                 : 10.0.0.2
Netmask                 : 255.255.255.0
Gateway                 : 10.0.0.1
----------------------[IPv6]----------------------
Configuration           : Disabled
> expert
admin@device:~$ sudo su
Password: [enter admin password]
root@device:/Volume/home/admin# ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=58 time=1.64 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=58 time=1.72 ms
64 bytes from 10.0.0.10: icmp_seq=3 ttl=58 time=1.70 ms
^C
--- 10.0.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 144ms
rtt min/avg/max/mdev = 1.639/1.678/1.724/0.033 ms
```

5: FTD에서 Cisco Eventing Services로의 DNS 확인 및 HTTPS 연결을 확인합니다.

```
root@device:/Volume/home/admin# nslookup eventing-ingest.sse.itd.cisco.com
root@device:/Volume/home/admin# curl -v -k https://eventing-ingest.sse.itd.cisco.com
root@device:/Volume/home/admin# telnet eventing-ingest.sse.itd.cisco.com 443
```

작업

사용자가 DNS 서버의 내부 문제를 확인하고 해결했습니다. DNS 기능이 복원되면

- FTD에서 필요한 Cisco 이벤트 도메인을 확인할 수 있었습니다
- FTD는 자동으로 이벤트 연결 재설정
- 연결 이벤트 로그가 다시 cdFMC에 설계대로 표시됨

모든 시정 조치는 컨피그레이션 변경 없이 사용자가 수행했습니다

원인

근본 원인은 FTD 관리 인터페이스에서 DNS 확인 실패이며, 특히 구성된 DNS 서버의 문제로 인해 발생했습니다. FTD는 eventing-ingest.sse.itd.cisco.com을 비롯한 필수 Cisco 이벤트 도메인을 확인할 수 없으므로 아웃바운드 이벤트 연결을 설정할 수 없으므로 연결 이벤트가 Cisco Security Cloud로 전달되지 않습니다. DNS 확인이 복원된 후 사용자는 연결 이벤트 로깅이 프로덕션 환경에서 정상적으로 작동하고 작동하는 것을 확인했습니다.

관련 콘텐츠

- 보안 방화벽 위협 방어 및 Cisco XDR 통합 정보
- Cisco 기술 지원 및 다운로드
- 이 문서를 넘어서는 가능한 결함: Cisco 버그 ID CSCwr75332 FTD가 보안 클라우드 제어에 이벤트 전달 실패

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.