보안 방화벽 FTD 구축 실패

문제

Cisco Firewall FTD(Firewall Threat Defense)에서 네트워크 중단 및 가동 중단이 관찰되었습니다. 반복되는 사고로 인해 SNMP 통신을 비롯한 트래픽이 거부되었으며, 근본 원인을 파악하고 추가 영향을 완화하기 위해 디바이스 재부팅 및 지속적인 모니터링이 필요했습니다.

환경

- Cisco Secure Firewall Firepower 1140 어플라이언스(모든 FTD 모델에 영향)
- FTD 소프트웨어 버전: 7.4.2.4(다른 버전도 적용)
- 동적 객체 기반 ACP(Access Control Policy)
- 빈번한 정책 구축

해결

Cisco Secure Firewall FTD 장치에서 반복되는 장애 조치 및 정책 배포 문제를 해결하려면 종합적인 문제 해결 및 치료 단계를 수행해야 합니다. 나열된 워크플로는 모니터링, 데이터 수집, 진단 및 업그레이드 지침을 포함하여 각 단계에 대한 명확한 구분과 설명을 제공하도록 구성됩니다.

1: 패킷 추적기를 사용하여 원하는 트래픽에 대한 라우팅 및 액세스를 확인합니다.

```
firepower# packet-tracer input INPUTNAMEIF tcp SRCIP 54321 DSTIP 443
firepower# packet-tracer input INPUTNAMEIF icmp SRCIP 8 0 DSTIP
```

2: FTD에서 캡처를 사용하여 트래픽에 대해 유효한 규칙 및 경로가 존재하더라도 '구성된 규칙별' 엔트리 시 패킷이 삭제되는지 여부를 확인합니다.

```
firepower# capture 1 interface INPUTIFNAME trace detail trace-count 1000 match ip host SRCIP host DSTIP
firepower# capture x type asp-drop all match ip host SRCIP host DSTIP
firepower# show capture
capture 1 type raw-data trace detail trace-count 1000 interface inside [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
capture x type asp-drop all [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
```

3: FTD 메시지 로그에서 결함 CSCwo78475의 증거를 확인합니다.

```
> expert
admin@FTD-1:~$ sudo su
Password:
root@FTD-1:/Volume/home/admin# cat /ngfw/var/log/messages | grep -E "New inspector|did not finish|swapp
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector is not initializing Identity API because it's a
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector has different policy groups or ABP name to ID m
Feb 10 18:35:10 FTD-device SF-IMS[28366]: Reading the muster data snapshot did not finish in time: 4 se
Feb 10 18:36:22 FTD-device SF-IMS[28366]: Identity API state swapped
```

4: 이 로그의 타임스탬프를 FTD의 구축 로그의 타임스탬프와 일치시킵니다.

```
Feb 10 18:34:45 FTD-device policy_apply.pl[18923]: INFO  Deployment type is NORMAL_DEPLOYMENT and devic
Feb 10 18:37:03 FTD-device policy_apply.pl[30894]: INFO  finalizeDeviceDeployment - sandbox = /var/cisc
```

5: FTD가 HA에 있는 경우 대기 FTD로 장애 조치하고 이후 동일한 상태를 확인하여 트래픽 복구를 확인합니다.

6: 일치하는 로그와 조건이 FTD에 있는 경우, 디바이스는 결함의 영향을 받으며 7.4.3으로 업그레이드할 수 있습니다. 그 동안 구축 시간을 시간 이후로 제한하여 트래픽에 대한 영향을 줄일 수 있습니다.

원인

관찰된 트래픽 영향 및 정책 구축 문제의 근본적인 원인은 FTD 소프트웨어에 영향을 미치는 알려진 결함 때문입니다.

- Cisco 버그 ID CSCwo78475: 동적 개체가 있는 FTD 장치에서 정책을 배포하는 동안 트래픽이 잘못된 ACP(액세스 제어 정책) 규칙을 발견합니다. 이로 인해 실행 중인 구성에 적절한 규

칙이 있는 경우에도 합법적인 트래픽이 거부될 수 있습니다. 버전 7.4.3에서 수정되었습니다.

관련 콘텐츠

- Cisco 버그 ID CSCwo78475: 동적 객체를 사용하여 FTD에서 정책을 구축하는 동안 트래픽이 잘못된 ACP 규칙에 도달함
- Cisco 기술 지원 및 다운로드: 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.