네트워크 중단 후 WSA 업스트림 프록시 상태 확인 문제

목차

문제

네트워크 중단이 장기화되면 FQDN으로 지정된 업스트림 프록시를 사용하도록 구성된 Cisco WSA(Web Security Appliance)에서 업스트림 프록시로의 포워딩 트래픽을 재개하지 못하고 대신 트래픽을 직접 전송할 수 있습니다. 이 문제는 WSA가 네트워크 중단 중에 업스트림 프록시를 "비활성"으로 표시할 때 발생하지만, 네트워크 연결이 복원된 후에도 업스트림 프록시를 다시 사용할 수 있게 되는 시점을 인식하지 못합니다.

관찰된 특정 증상은 다음과 같습니다.

- FQDN 및 "Failure Handling = go Direct"를 통해 업스트림 프록시로 WSA 구성
- 업스트림 프록시 및 DNS 서버 모두에 대한 연결에 영향을 주는 장기적인 네트워크 중단
- 네트워크 복구 후 액세스 로그에 DEFAULT_PARENT 태그가 표시되지 않습니다. 이는 트래픽이 업스트림 프록시를 계속 우회함을 나타냅니다
- 동일한 환경의 다른 어플라이언스가 정상적으로 작동하는 동안 한 WSA 어플라이언스에서 문제가 발생합니다

환경

- Cisco WSA(Web Security Appliance) S-Series
- AsyncOS 14.5.2-011(영향 받는 버전)
- 하드웨어: S695
- FQDN 사양으로 구성된 업스트림 프록시
- "직접 이동"으로 구성된 실패 처리

- L2 스위치 인프라가 있는 네트워크 환경

해결

이 문제는 AsyncOS를 CSCwi13124용 수정 사항이 포함된 버전으로 업그레이드하여 해결되었습니다. 이 버그는 다음 AsyncOS 버전에서 수정되었습니다.

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

현재 버전에 대한 임시 해결 방법

즉시 업그레이드할 수 없는 환경의 경우, 응답하지 않는 업스트림 프록시를 확인하기 위한 최대 유휴 시간 제한을 조정하여 일시적인 완화를 사용할 수 있습니다.

1단계: CLI에 액세스하여 고급 프록시 컨피그레이션으로 이동합니다.

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

2단계: 최대 유휴 시간 제한 설정을 수정합니다.

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

3단계: 기본 최대값(86400초/24시간)을 더 작은 값으로 줄여 상태 확인 간격을 줄입니다.

즉시 복구 방법

문제가 현재 트래픽 흐름에 영향을 미치는 경우 다음 명령은 즉시 업스트림 프록시 기능을 복원할 수 있습니다.

1단계: 진단 메뉴에 액세스합니다.

```
CLI > diagnostic > PROXY > kick
```

그러면 프록시 프로세스가 다시 시작되고 정상적인 업스트림 프록시 작업이 복원됩니다.

검증 및 테스트 절차

문제가 있는지 또는 업그레이드 후 해결되었는지 테스트하려면 다음 단계를 검토하십시오.

1단계: 기준 모니터링 설정

액세스 로그 및 프록시 로그를 모니터링하여 WSA가 트래픽을 업스트림 프록시로 전송하는지 확인합니다. 트래픽이 업스트림 프록시 측에 도달하고 있는지 확인합니다.

2단계: 네트워크 중단 시뮬레이션

업스트림 프록시에 대한 정상적인 트래픽 흐름을 확인한 후 다음 연결을 끊습니다.

- WSA에서 업스트림 프록시 연결
- WSA와 DNS 서버 연결

3단계: 장애 감지 모니터링

프록시 로그 및 시스템 로그에서 다음 지표를 확인합니다.

- 프록시 로그는 업스트림 프록시를 "... dead 선언됨"으로 표시할 수 있습니다.
- 시스템 로그에 "Critical: DNS 서버를 쿼리하는 동안 최대 실패에 도달했습니다..."

4단계: 중단 상태 유지

프록시 프로세스를 다시 시작하지 않고 2단계에서 연결 끊김 상태를 유지하고 약 10시간 동안 요청을 계속 생성합니다.

5단계: 연결 복원

약 10시간 후 2단계에서 연결이 끊긴 연결을 복원합니다.

6단계: 복구 동작 모니터링

5단계를 완료한 후 프록시 프로세스를 다시 시작하지 않고 액세스 로그 및 프록시 로그를 모니터링합니다.

- 고정 시스템에서: 트래픽은 업스트림 프록시를 통해 흐름을 재개하며 프록시 로그는 정상적인 상태 전환을 표시합니다
- 영향을 받는 시스템에서: 액세스 로그는 업스트림 프록시를 계속 우회하는 트래픽을 보여주며, 프록시 로그는 ".. was sick, now healthy" 또는 "... was healthy, now sick" 메시지를 표시하지 않습니다

원인

이 문제의 근본 원인은 업스트림 프록시 상태 점검 메커니즘의 논리 결함입니다. WSA는 구성된 업스트림 프록시가 "dead"(응답하지 않음)라고 결정할 때, 각 실패 후 상태 확인 간격을 두 배로 만드는 지수 백오프 알고리즘을 구현합니다. 이 간격은 최대 24시간(86400초)에 도달할 수 있습니다.

이 문제는 이러한 확장 간격 중 하나에서 업스트림 프록시를 다시 사용할 수 있게 될 때 발생합니다. 프록시가 복구되어 정상적으로 응답하더라도 WSA는 구성된 전체 시간 간격이 경과할 때까지 상태 확인을 수행하지 않습니다. 따라서 업스트림 프록시 사용을 재개하는 대신 최대 24시간 동안 직접 트래픽 라우팅을 계속할 수 있습니다.

이 동작은 다음과 같은 경우 WSA 컨피그레이션에 영향을 미칩니다.

- 업스트림 프록시가 DNS 호스트 이름/FQDN(IP 주소가 아님)에 의해 지정되었습니다.
- 장애 처리가 "직접 실행"으로 설정되어 있습니다.
- 확장된 네트워크 중단은 업스트림 프록시 및 DNS 서버 연결에 모두 영향을 미침

Cisco 버그 ID: CSCwi 13124

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.