FTD에서 SSL/TLS 암호 해독에 대한 성능 영향 및 모범 사례 확인

목차

문제

사용자는 FTD(Firewall Threat Defense) 디바이스에서 SSL/TLS 암호 해독을 활성화할 계획이며 구현 전에 디바이스 성능에 미칠 수 있는 영향을 이해해야 합니다. 주요 우려 사항은 다음과 같습니다.

- 방화벽 처리량, 레이턴시, 전반적인 트래픽 처리 성능에 영향을 줍니다.
- 암호 해독을 활성화한 후 예상 CPU 및 메모리 사용률이 증가합니다.
- 특정 FTD 모델에 대한 크기 조정 지침 및 성능 벤치마크
- 동시 암호 해독된 세션에 대한 권장 제한.
- 프로덕션 구축을 위한 모범 사례 및 사전 요구 사항

환경

- Firepower 4115. 다른 하드웨어 플랫폼도 영향을 받을 수 있습니다.
- FTD 버전 7.4.2(빌드 172). 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- SSL/TLS 암호 해독 기능을 고려해야 합니다.
- 프로덕션 환경 구축 계획.

해결

SSL/TLS 해독은 처리 오버헤드를 Firepower(4115)에 추가하지만, 실제 영향은 얼마나 많은 트래픽

이 해독되고, 해독 후 어떤 검사가 적용되는지에 크게 의존한다.

성능 영향 분석

SSL/TLS 해독 영향은 다음과 같습니다.

- 더 낮은 유효 처리량.
- 더 높은 레이턴시.
- Snort/검사 CPU 사용량 증가
- CPU 및 메모리 증가는 실제 트래픽 프로필 분석 없이 고정된 비율로 정확하게 예측할 수 없습니다.

FPR 4115 성능 벤치마크

Cisco에서 게시한 Firepower 4115 벤치마크 사양:

- TLS 하드웨어 암호 해독 처리량: 6.5Gbps.
- FW + AVC 처리량: 33Gbps.
- AVC를 통한 최대 동시 세션 수: 1,500만
- AVC를 통한 초당 최대 신규 연결 수: 210K.

중요한 크기 조정 참고 사항: 6.5Gbps TLS 하드웨어 암호 해독 벤치마크는 특정 테스트 조건을 기반으로 합니다. 트래픽의 상당 부분을 해독하거나, 해독된 트래픽을 침입/파일/악성코드 정책으로 검사하거나, 수명이 짧은 TLS 세션을 많이 처리할 경우 프로덕션 처리량이 낮아질 수 있습니다.

Cisco는 FTD 7.4.2의 Firepower 4115에 대해 별도의 "동시 암호 해독된 최대 세션 수"를 게시하지 않습니다. 실제로 트래픽 믹스, 동시 세션, 연결 속도, 암호 그룹 및 검사 정책 로드를 사용하여 용량을 검증합니다.

권장 프로덕션 구축 방식

1단계: 제한된 파일럿으로 시작

- 초기에 광범위한 "decrypt all" 규칙을 활성화하지 마십시오.
- 선택한 사용자, 서브넷 또는 대상 카테고리로 시작합니다.
- 검사가 필요하지 않은 트래픽에 대해서는 Do Not Decrypt를 사용하여 기본 처리 보수성을 유지합니다.

2단계: 일반적으로 암호 해독으로 중단되는 트래픽 제외

- 금융 사이트.
- 의료 포털.
- 인증서 고정 애플리케이션.
- 일부 SaaS(Software as a Service) 및 엔드포인트 보안/클라우드 애플리케이션
- 명시적으로 테스트하지 않는 한 중요한 비즈니스 크리티컬 애플리케이션.

3단계: SSL 규칙을 간단하게 유지하고 신중하게 순서 지정

- 특정 Do Not Decrypt 제외를 더 광범위한 암호 해독 규칙 위에 둡니다.
- 가능한 경우 지나치게 광범위하거나 복잡한 일치를 피하십시오.
- Decrypt-Resign/Known-Key 규칙에는 TLS 버전 또는 암호 그룹 조건을 사용하지 마십시오. Cisco 문서에서는 이 경우 예기치 않은 동작이 발생할 수 있습니다.

4단계: 인증서 준비 상태 검증

- 아웃바운드 Decrypt-Resign의 경우 클라이언트 엔드포인트에서 서명 CA 인증서를 신뢰해야 합니다.
- 인바운드 Known-Key 암호 해독의 경우 방화벽에 올바른 서버 인증서/개인 키 자료가 있어야 합니다.

5단계: 배포 중 모니터링

- 전체 CPU 및 더욱 중요한 Snort/검사 CPU 사용률을 추적합니다.
- 동시 연결 및 초당 새 연결 추적
- 연결 이벤트에서 SSL 흐름 상태/핸드셰이크 오류를 검토합니다.
- TLS 오버서브스크립션 지표 및 애플리케이션별 오류를 확인합니다.

CPU를 모니터링하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- TAC 엔지니어처럼 생각하십시오. Cisco Secure Firewall에 대한 가장 일반적인 고충

연결 추적 및 초당 새 연결 확인:

- 로깅 모범 사례

연결 이벤트 검사 및 TLS 오버서브스크립션 표시기 검사에서 SSL 흐름 상태/핸드셰이크 오류를 추적하려면

- TLS/SSL 오버서브스크립션 문제 해결

6단계: 다음과 같은 경우 롤백하거나 범위를 좁힙니다.

- 지속적인 검사 CPU 포화.
- 사용자가 볼 수 있는 레이턴시가 증가합니다.
- TLS 핸드셰이크 실패.
- 암호 해독 후 비즈니스 애플리케이션이 실패했습니다.
- 오버서브스크립션 또는 과도한 SSL 오류입니다.

7단계: TLS 1.3의 영향 고려

TLS 1.3 채택은 특정 핸드셰이크 및 검사 특성이 TLS 1.2와 다르므로 가시성 및 동작에 영향을 미칠 수 있습니다.

원인

SSL/TLS 해독에는 트래픽 흐름을 해독, 검사 및 다시 암호화하는 데 추가 계산 리소스가 필요합니다. 성능 영향은 트래픽 패턴, 해독된 트래픽에 적용된 검사 정책, 특정 구축 컨피그레이션에 따라 크게 달라집니다. 적절한 계획과 점진적인 구현이 없으면 기업은 생산 환경에서 예기치 않은 성능 저하를 겪을 수 있습니다.

관련 콘텐츠

- Cisco Secure Firewall Management Center Device Configuration Guide - 암호 해독 규칙
- Cisco Secure Firewall 암호 해독 정책 지침
- 암호 해독 정책 규칙 순서에 대한 모범 사례
- Cisco Secure Firewall 7.7로 암호 해독 간소화
- 암호 해독 규칙 모범 사례
- Cisco Firepower 4100 Series 데이터 시트
- 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.