특정 애플리케이션 프로토콜에 대한 보안 액세스 정책 시행

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)

[배경 정보](#)

[문제: TCP 80/443의 특정 애플리케이션 프로토콜에 대한 정책 적용 테스트로 인해 연결 시간 초과가 발생하고 Secure Access에서 로그가 생성되지 않음](#)

[솔루션](#)

[관련 정보](#)

소개

이 문서에서는 특정 애플리케이션 프로토콜을 사용할 때의 보안 액세스 정책 시행에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 보안 액세스
- FTP(File Transfer Protocol)
- TCP(Transmission Control Protocol)
- FWaaS(Firewall as a Service)
- SSH(Secure Shell)
- HTTP(Hyper Text Transfer Protocol)
- 빠른 UDP 인터넷 연결(QUIC)
- SMTP(Secure Mail Transfer Protocol)

배경 정보

애플리케이션 프로토콜 기반 정책 시행을 평가하는 일반적인 FWaaS 테스트는 프로토콜 오용 테스트입니다.

이 시나리오의 테스트에는 일반적으로 비표준 포트에서 FTP/SSH와 같은 특정 애플리케이션 프로토콜을 차단하는 정책이 포함됩니다. 예를 들어 TCP 포트 21에서만 FTP를 허용하고 TCP 포트 80에서는 FTP를 차단합니다.

Secure Access는 OpenAppID 프로토콜 탐지를 사용하여 FTP, SSH, QUIC, SMTP 등의 애플리케이션 프로토콜을 탐지하고 Secure Web Gateway를 사용하여 HTTP(S) 트래픽을 보호합니다.

문제: TCP 80/443의 특정 애플리케이션 프로토콜에 대한 정책 적용 테스트로 인해 연결 시간 초과가 발생하고 Secure Access에서 로그가 생성되지 않음

TCP 포트 80/443에서 FTP와 같은 특정 프로토콜을 허용/차단하려고 시도하는 경우 클라이언트와 서버 간의 초기 연결이 프록시 엔진에 의해 가로채지고 TCP 핸드셰이크가 완료된 다음 Secure Access의 프록시 엔진이 클라이언트에서 트래픽을 보내기를 대기하는 상황이 발생하지만, 이 프로토콜은 클라이언트에 도달하기 위해 서버측 신호가 필요합니다.

이 상황은 클라이언트가 서버 신호를 기다리다 보니 연결이 끊기고 결국 프록시가 연결을 끊어버리게 됩니다. 그리고 Secure Access는 이 세션 유형에 대한 로그를 생성하지 않습니다.

솔루션

이는 Secure Access 아키텍처에서 웹 트래픽을 보호하는 방식 때문에 예상되는 동작이며, 이러한 테스트에는 웹 포트에서 웹 이외의 트래픽(처음에 서버 측 신호에 의존하는 FTP, SSH, 텔넷, SMTP, IMAP 및 기타 프로토콜)이 포함되므로 그러한 세션에 대한 로그는 생성되지 않습니다.

관련 정보

- Secure Access 사용 설명서
- 보안 액세스 커뮤니티 페이지
- 기술 지원 및 문서 – Cisco Systems

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.