Secure Web Appliance의 HTTPS 액세스 로그 형식 이해

목차

소개

이 문서에서는 HTTPS 트래픽용 SWA(Secure Web Appliance) 액세스 로그에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 물리적 또는 가상 SWA가 설치되었습니다.
- 라이센스가 활성화되었거나 설치되었습니다.
- SSH(Secure Shell) 클라이언트.
- 설치 마법사가 완료되었습니다.

- SWA에 대한 관리 액세스.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

액세스 로그의 Cisco SWA HTTPS 트래픽 로그 방식은 일반 HTTP 트래픽과 다릅니다.

참고: 로그는 프록시 구축 모드에 따라 다르며 명시적 전달 모드 또는 투명 모드에서 로그는 다릅니다.

Accesslogs의 키워드

다음은 액세스 로그에서 볼 수 있는 몇 가지 중요한 키워드입니다.

TCP_CONNECT: 이는 트래픽이 투명하게 수신되었음을 보여줍니다(WCCP, L4 리디렉션 또는 기타 투명 리디렉션 방법을 통해).
연결: 이는 트래픽이 명시적으로 수신되었음을 보여줍니다.
DECRYPT_WBRS: 이는 SWA가 WBRS(Web Reputation Score) 점수로 인한 Decrypt traffic을 가지고 있음을 보여줍니다.
PASSTHRU_WBRS: 이는 SWA가 WBRS 점수로 인해 트래픽을 통과했음을 보여줍니다.
DROP_WBRS: 이는 SWA가 WBRS 점수로 인해 Drop(삭제) 트래픽을 가짐을 보여줍니다

액세스 로그의 HTTPS 로그

HTTPS 트래픽이 해독되면 WSA는 두 개의 엔트리를 로깅합니다.

- TCP_CONNECT tunnel:// 또는 CONNECT tunnel://는 수신된 요청의 유형에 따라 다릅니다. 즉, 트래픽이 암호화됩니다(아직 해독되지 않음).
- 암호 해독된 URL이 표시된 https://을 가져옵니다.

참고: 투명 모드의 전체 URL은 SWA가 트래픽을 해독하는 경우에만 표시됩니다.

```
1706174571.215 582 10.61.70.23 TCP_MISS_SSL/200 39 CONNECT tunnel://www.example.com:443/ - DIRECT/www.e
1706174571.486 270 10.61.70.23 TCP_MISS_SSL/200 1106 GET https://www.example.com:443/ - DIRECT/www.exam
```

참고: 투명 모드에서 SWA는 트래픽이 리디렉션될 때 처음에 목적지 IP 주소를 갖습니다.

다음은 액세스 로그에 표시되는 항목의 예입니다.

투명한 구축 - 암호 해독된 트래픽
1252543170.769 386 192.168.30.103 TCP_MISS_SSL/200 0 TCP_CONNECT 192.168.34.32:443/ - DIRECT/192.168.34.32 - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-> -

1252543171.166 395 192.168.30.103 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/192.168.34.32 image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,-,-,-,-> -

투명한 구축 - 통과 트래픽
1252543337.373 690 192.168.30.103 TCP_MISS/200 2044 TCP_CONNECT 192.168.34.32:443/ - 직접/192.168.34.32 - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-> -
투명한 배포 - 삭제
1252543418.175 430 192.168.30.103 TCP_DENIED/403 0 TCP_CONNECT 192.168.34.32:443/ - 직접/192.168.34.32 - DROP_WBRS-DefaultGroup-test.id-NONE-DefaultRouting <Sear,-9.1.0,-,-,-,-,-,-,-,-,-,-> -
명시적 구축 - 암호 해독된 트래픽
252543558.405 385 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/200 40 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-> - 1252543559.535 1127 10.66.71.105 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/www.example.com image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,-,-,-,-> -
명시적 구축 - 통과 트래픽
1252543491.302 568 10.66.71.105 TCP_CLIENT_REFRESH_MISS/200 2256 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-> -
명시적 구축 - 삭제
1252543668.375 1 10.66.71.105 TCP_DENIED/403 1578 CONNECT tunnel://www.example.com:443/ - NONE/- - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE-NONE <Sear,-9.1,-,-,-,-,-,-,-,-,-> -

관련 정보

- AsyncOS 15.0 for Cisco Secure Web Appliance - LD 사용 설명서(제한적 배포) - 문제 해결 방법...
- 액세스 로그의 성능 매개변수 구성 - Cisco

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.