SWA에서 암호 해독 속도 확인

목차

소개

이 문서에서는 이전에 WSA로 알려진 SWA(Secure Web Appliance)에서 해독된 트래픽의 백분율을 계산하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 물리적 또는 가상 SWA(Secure Web Appliance)가 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.

암호 해독 성능 영향

SWA에서 수행하는 모든 서비스 중 HTTPS(Hypertext Transfer Protocol Secure) 트래픽의 평가는 성능 측면에서 가장 중요합니다.

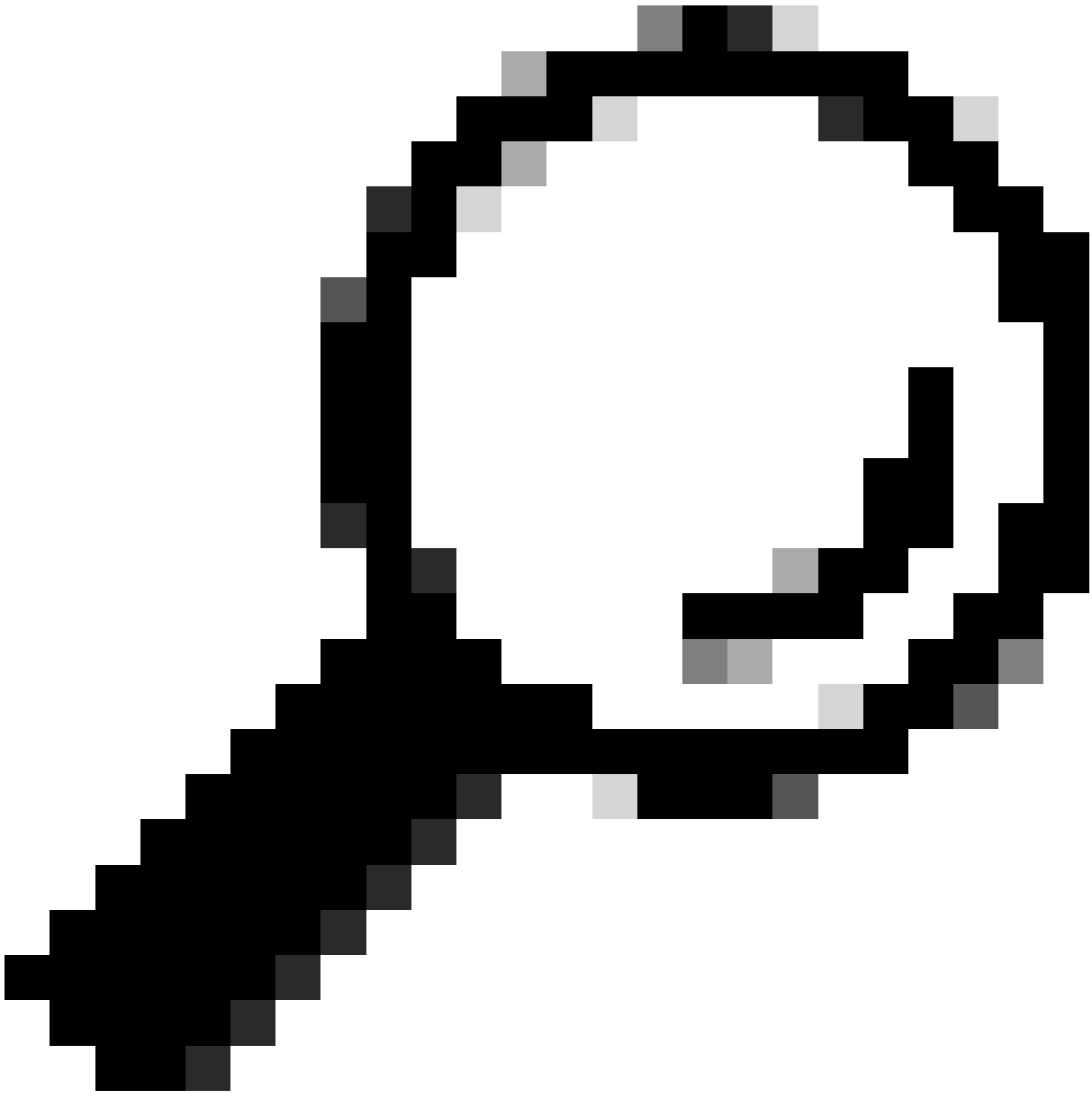
해독된 트래픽의 비율은 어플라이언스의 크기를 조정하는 방법에 직접적인 영향을 미칩니다. 관리

자는 웹 트래픽의 75% 이상을 HTTPS로 간주할 수 있습니다.

초기 설치 후 해독된 트래픽의 비율을 결정해야 향후 성장에 대한 기대치가 정확하게 설정됩니다. 구축 후에는 분기당 한 번씩 이 수를 확인해야 합니다.

암호 해독 속도가 30% 이상이고 SWA에 성능 문제가 있는 경우 다음 중 하나를 수행하는 것이 좋습니다.

- 암호 해독 정책에서 다양한 카테고리 또는 신뢰할 수 있는 URL(예: Microsoft 업데이트 또는 안티바이러스 업데이트)의 암호 해독 제거
- 부하 분산을 위해 더 많은 SWA에 부하 분산



팁: SWA에서 암호 해독을 우회하는 방법에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-to-exempt-office-365-traffic-from-au.html을 참조하십시오.

암호 해독 비율 계산 단계

모든 HTTPS 트래픽과 비교에서 해독된 HTTPS 트래픽의 백분율을 찾으려면 SWA FTP(File Transfer Protocol)에서 access_logs를 복사합니다.

Simple Bash 또는 PowerShell 명령을 사용하여 이 숫자를 얻을 수 있습니다. 각 환경에 대해 설명된 단계는 다음과 같습니다.

1. 총 HTTPS 연결 수 찾기(명시적 및 투명 모두):

```
Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT').length
```

2. 암호 해독된 HTTPS 연결 수를 찾습니다.

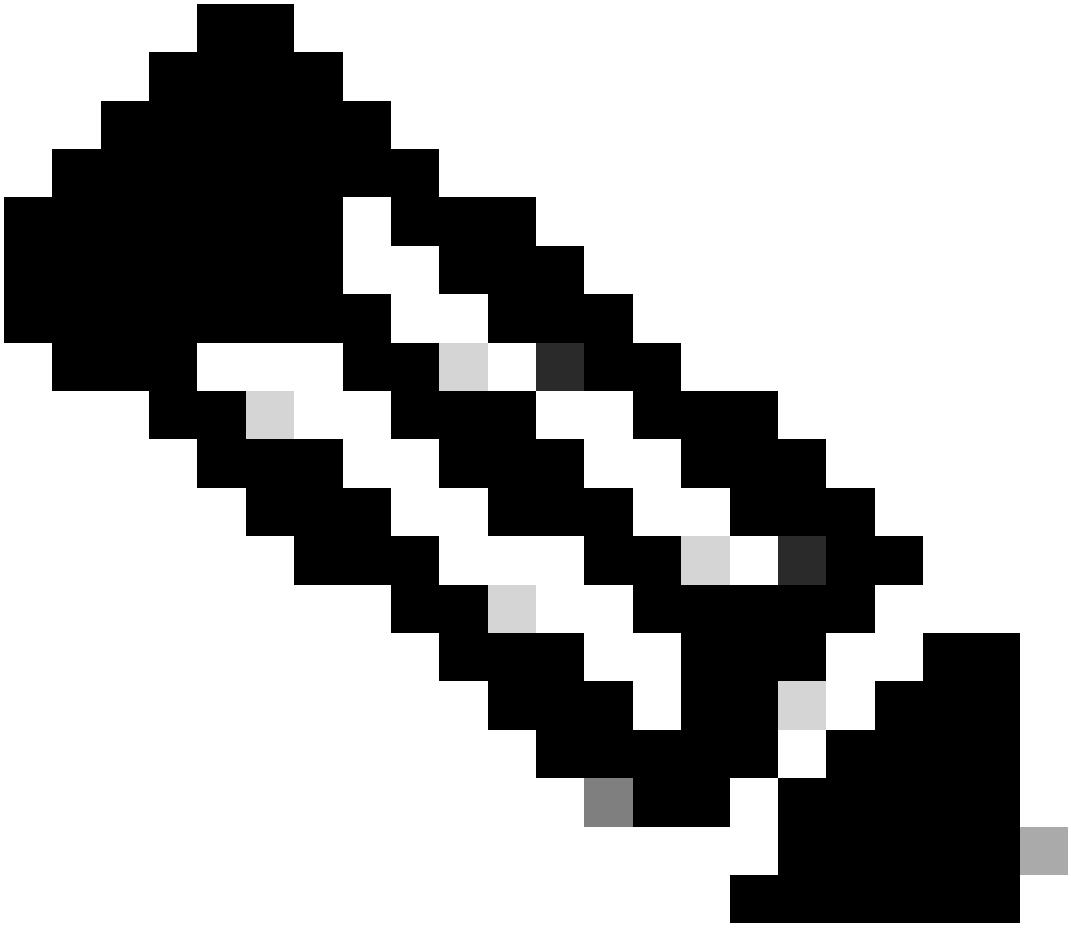
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT’| Select-String -Pattern ‘DE
```

3. 두 번째 값을 첫 번째 값으로 나눈 후 100을 곱합니다.

CLI의 전체 트래픽 통계

CLI에서 트래픽 통계를 볼 수 있으며, accessloganalyzer 명령을 사용하여 보고서에 대해 시간 범위 또는 N시간 경과를 선택할 수 있습니다.



참고: 명령의 실행 시간은 선택한 기간에 따라 달라집니다.

```
SWA_CLI> accessloganalyzer

Choose the option to define the time range:
- HOURS - Last N hours.
- RANGE - Time range with start and end specified in  MM/DD/YYYY HH:MM:SS format.
[]> HOURS

Analyze logs upto N hours old (oldest on this WSA is N = 312 hours). Enter N:
[]> 10

The log processing might take more than 15 secs. Do you want to continue: (Yes/No)
[No]> yes



-------------------------------------------------------------------------------------------------
                                       HTTP                HTTPS               Cumulative
---------------------------------------- ------------------- ------------------- -------------------
Num transactions                       1512509             4170261             5682770
```

Transaction/sec	42	115	157
Bandwidth (Mbps)	0.0001	0.0004	0.0003
Max Resp time (ms)	643269	285036670	285036670
Average Resp time(ms)	95663	141715	129458
Max Object size (KB)	92246	1215832	1215832
Avg Object size (Total Trans)(KB)	5	54	41
Avg Object size (Allowed Trans) (KB)	20	67	62
Methods			
GET	1295658	0	1295658
POST	34968	0	34968
CONNECT	0	4170261	4170261
Others	181883	0	181883
Status Codes			
1xx	0	0	0
2xx	319799	3351382	3671181
3xx	75011	0	75011
4xx	11697	115467	127164
5xx	1105999	703412	1809411

관련 정보

AsyncOSAsyncOS또는 Cisco SCisco Web Appliance - LD(LimLDed Deployment) 사용 설명서 - Cisco

UC보안 웹 어플라이언스 모범 사례 - Cisco

HCcisco WSA(Cisco Unified Appliance)의 인증 및 해독에서 Office 365 트래픽 제외 - WSAco

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.