Secure Web Appliance 로그 액세스

목차

소개

이 문서에서는 SWA(Secure Web Appliance) 로그를 보는 방법에 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.

SWA 로그 유형

Secure Web Appliance는 자체 시스템 및 트래픽 관리 활동을 로그 파일에 기록하여 기록합니다. 관

리자는 이러한 로그 파일을 참조하여 어플라이언스를 모니터링하고 문제를 해결할 수 있습니다.

이 표에서는 Secure Web Appliance 로그 파일 유형에 대해 설명합니다.

로그 파일 유형	설명	Syslog Push를 지원합니까?	기본적으로 활성화되어 있습니까?
액세스 제어 엔진 로그	웹 프록시 ACL(액세스 제어 목록) 평가 엔진과 관련된 메시지를 기록합니다.	아니요	아니요
보안 엔드포인트 엔진 로그	파일 평판 검사 및 파일 분석(보안 엔드포인트)에 대한 정보 기록	예	예
감사 로그	AAA(Authentication, Authorization, and Accounting) 이벤트를 기록합니다. 애플리케이션 및 CLI(Command Line Interface)와의 모든 사용자 상호 작용을 기록하고 커밋된 변경 사항을 캡처합니다. 일부 감사 로그 세부사항은 다음과 같습니다. • 사용자 - 로그온 • 사용자 - 로그온 실패 잘못된 암호 • 사용자 - 로그온 실패 알 수 없는 사용자 이름 • 사용자 - 로그온 실패 계정이 만료됨 • 사용자 - 로그오프 • 사용자 - 잠금 • 사용자 - 활성화됨 • 사용자 - 비밀번호 변경 • 사용자 - 비밀번호 재설정 • 사용자 - 보안 설정/프로필 변경 • 사용자 - 생성됨 • 사용자 - 삭제/수정됨	예	예

로그 파일 유형	설명	Syslog Push를 지원합니까?	기본적으로 활성화되어 있습니까?
	• 그룹/역할 - 삭제/수정됨 • Group /Role - 권한 변경		
액세스 로그	웹 프록시 클라이언트 기록을 기록합니다.	예	예
ADC 엔진 프레임워크 로그	웹 프록시와 ADC 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
ADC 엔진 로그	ADC 엔진의 디버그 메시지를 기록합니다.	예	예
인증 프레임워크 로그	인증 기록 및 메시지를 기록합니다.	아니요	예
AVC 엔진 프레임워크 로그	웹 프록시와 AVC 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
AVC 엔진 로그	AVC 엔진의 디버그 메시지를 기록합니다.	예	예
CLI 감사 로그	명령줄 인터페이스 활동에 대한 기록 감사를 기록합니다.	예	예
컨피그레이션 로그	웹 프록시 구성 관리 시스템과 관련된 메시지를 기록합니다.	아니요	아니요
연결 관리 로그	웹 프록시 연결 관리 시스템과 관련된 메시지를 기록합니다.	아니요	아니요
데이터 보안 로그	Cisco Data Security Filters에서 평가한 업로드 요청에 대한 클라이언트 기록을 기록합니다.	예	예
데이터 보안 모듈 로그	Cisco 데이터 보안 필터와 관련된 메시지를 기록합니다.	아니요	아니요

로그 파일 유형	설명	Syslog Push를 지원합니까?	기본적으로 활성화되어 있습니까?
DCA 엔진 프레임워크 로그 (동적 콘텐츠 분석)	웹 프록시와 Cisco Web Usage Controls Dynamic Content Analysis 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
DCA 엔진 로그 (동적 콘텐츠 분석)	Cisco Web Usage Controls Dynamic Content Analysis 엔진과 관련된 메시지를 기록합니다.	예	예
기본 프록시 로그	웹 프록시와 관련된 오류를 기록합니다. 이는 모든 웹 프록시 관련 로그 중 가장 기본입니다. 웹 프록시와 관련된 특정 문제를 해결하려면 해당 웹 프록시 모듈에 대한 로그 서브스크립션을 생성합니다.	예	예
디스크 관리자 로그	디스크의 캐시에 쓰는 것과 관련된 웹 프록시 메시지를 기록합니다.	아니요	아니요
외부 인증 로그	외부 인증 서버와의 통신 성공 또는 실패와 같은 외부 인증 기능 사용과 관련된 메시지를 기록합니다. 외부 인증이 비활성화된 경우에도 이 로그에는 성공적으로 로그인했거나 실패한 로컬 사용자에 대한 메시지가 포함됩니다.	아니요	예
피드백 로그	잘못 분류된 페이지를 보고하는 웹 사용자를 기록합니다.	예	예
FTP 프록시 로그	FTP 프록시와 관련된 오류 및 경고 메시지를 기록합니다.	아니요	아니요
FTP 서버 로그	FTP를 사용하여 Secure Web Appliance에 업로드되고 Secure Web Appliance에서 다운로드된 모든 파일을 기록합니다.	예	예

로그 파일 유형	설명	Syslog Push를 지원합니까?	기본적으로 활성화되어 있습니까?
GUI 로그 (그래픽 사용자 인터페이스)	웹 인터페이스에서 페이지 새로 고침의 기록을 기록합니다. GUI 로그에는 SMTP 트랜잭션에 대한 정보(예: 어플라이언스에서 이메일로 전송된 예약된 보고서에 대한 정보)도 포함됩니다.	예	예
Haystack 로그	Haystack 로그는 웹 트랜잭션 추적 데이터 처리를 기록합니다.	예	예
HTTPS 로그	HTTPS 프록시(HTTPS 프록시가 활성화된 경우)에 해당하는 웹 프록시 메시지를 기록합니다.	아니요	아니요
ISE 서버 로그	ISE 서버 연결 및 운영 정보를 기록합니다.	예	예
라이센스 모듈 로그	웹 프록시의 라이센스 및 기능 키 처리 시스템과 관련된 메시지를 기록합니다.	아니요	아니요
로깅 프레임워크 로그	웹 프록시의 로깅 시스템과 관련된 메시지를 기록합니다.	아니요	아니요
로그 기록	로그 관리와 관련된 오류를 기록합니다.	예	예
McAfee Integration Framework 로그	웹 프록시와 McAfee 스캐닝 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
McAfee 로그	McAfee 스캐닝 엔진의 안티멀웨어 스캐닝 활동 상태를 기록합니다.	예	예
메모리 관리자 로그	웹 프록시 프로세스에 대한 메모리 내 캐시를 포함하여 모든 메모리 관리와 관련된 웹 프록시 메시지를 기록합니다.	아니요	아니요
기타 프록시 모듈 로그	주로 개발자 또는 고객 지원에서 사용하는 웹 프록시 메시지를 기록합니다.	아니요	아니요

로그 파일 유형	설명	Syslog Push를 지원합니까?	기본적으로 활성화되어 있습니까?
AnyConnect Secure Mobility 데몬 로그	상태 확인을 포함하여 Secure Web Appliance와 AnyConnect 클라이언트 간의 상호 작용을 기록합니다.	예	예
NTP 로그 (Network Time Protocol)	Network Time Protocol에서 수행한 시스템 시간의 변경 사항을 기록합니다.	예	예
PAC 파일 호스팅 데몬 로그	클라이언트의 PAC(프록시 자동 구성) 파일 사용을 기록합니다.	예	예
프록시 Bypass 로그	웹 프록시를 우회하는 트랜잭션을 기록합니다.	아니요	예
보고 로그	보고서 생성 기록을 기록합니다.	예	예
보고 쿼리 로그	보고서 생성과 관련된 오류를 기록합니다.	예	예
디버그 로그 요청	모든 웹 프록시 모듈 로그 유형의 특정 HTTP 트랜잭션에 대한 매우 자세한 디버그 정보를 기록합니다. 다른 모든 프록시 로그 서브스크립션을 생성하지 않고 특정 트랜잭션의 프록시 문제를 트러블슈팅하려면 이 로그 서브스크립션을 생성하는 것이 좋습니다. 참고:이 로그 서브스크립션은 CLI에서만 생성할 수 있습니다.	아니요	아니요
인증 로그	액세스 제어 기능과 관련된 메시지를 기록합니다.	예	예
SHD 로그 (시스템 상태 데몬)	시스템 서비스의 상태 기록 및 예기치 않은 데몬 재시작의 기록을 기록합니다.	예	예

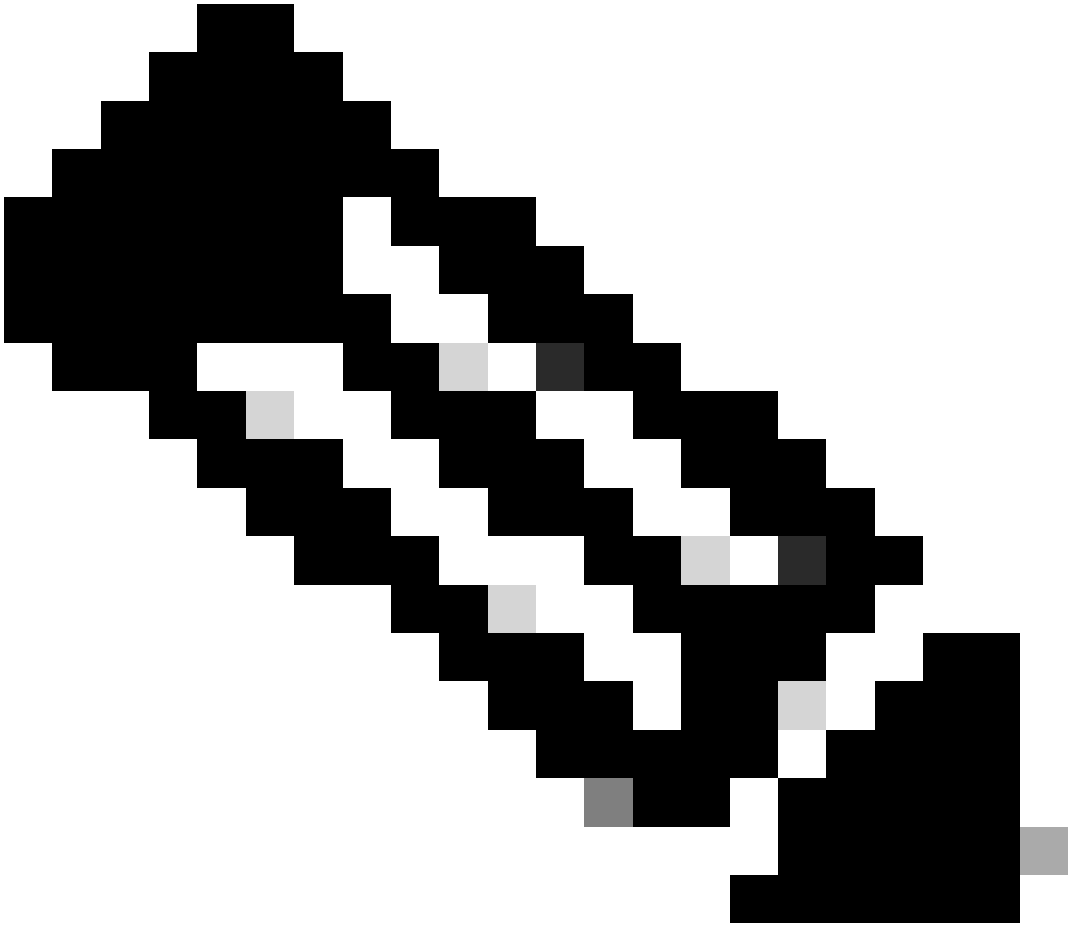
로그 파일 유형	설명	Syslog Push를 지원합니까?	기본적으로 활성화되어 있습니까?
SNMP 로그	SNMP 네트워크 관리 엔진과 관련된 디버그 메시지를 기록합니다.	예	예
SNMP 모듈 로그	SNMP 모니터링 시스템과의 상호 작용과 관련된 웹 프록시 메시지를 기록합니다.	아니요	아니요
Sophos 통합 프레임워크 로그	웹 프록시와 Sophos 스캐닝 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
Sophos 로그	Sophos 스캐닝 엔진의 안티멀웨어 스캐닝 활동 상태를 기록합니다.	예	예
상태 로그	기능 키 다운로드와 같은 시스템과 관련된 정보를 기록합니다.	예	예
시스템 로그	DNS, 오류 및 커밋 활동을 기록합니다.	예	예
트래픽 모니터 오류 로그	L4TM 인터페이스 및 캡처 오류를 기록합니다.	예	예
트래픽 모니터 로그	L4TM 블록 및 허용 목록에 추가된 사이트를 기록합니다.	아니요	예
UDS 로그 (사용자 검색 서비스)	웹 프록시에서 실제 인증을 수행하지 않고 사용자 이름을 검색하는 방법에 대한 데이터를 기록합니다. 여기에는 Secure Mobility를 위한 Cisco ASA와의 상호 작용 및 투명한 사용자 식별을 위한 Novell eDirectory 서버와의 통합에 대한 정보가 포함됩니다.	예	예
업데이터 로그	WBRS 및 기타 업데이트의 기록을 기록합니다.	예	예
W3C 로그	웹 프록시 클라이언트 기록을 W3C 호환 형식으로 기록합니다.	예	아니요

로그 파일 유형	설명	Syslog Push를 지원합니까?	기본적으로 활성화되어 있습니까?
	추가 정보.		
WBNP 로그 (SensorBase 네트워크 참여)	SensorBase 네트워크에 대한 Cisco SensorBase 네트워크 참여 업로드의 기록을 기록합니다.	아니요	예
WBRS 프레임워크 로그 (웹 평판 점수)	웹 프록시와 웹 평판 필터 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
WCCP 모듈 로그	WCCP 구현과 관련된 웹 프록시 메시지를 기록합니다.	아니요	아니요
Webcat 통합 프레임워크 로그	웹 프록시와 Cisco Web Usage Controls와 연결된 URL 필터링 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
Webroot 통합 프레임워크 로그	웹 프록시와 Webroot 스캐닝 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
Webroot 로그	Webroot 스캐닝 엔진의 안티멀웨어 스캐닝 활동 상태를 기록합니다.	예	예
시작 페이지 승인 로그	최종 사용자 승인 페이지에서 Accept(수락) 버튼을 클릭한 웹 클라이언트의 기록을 기록합니다.	예	예

로그 보기

기본적으로 로그는 SWA에 로컬로 저장됩니다. GUI를 통해 로컬로 저장된 로그 파일을 다운로드하거나 CLI에서 로그를 볼 수 있습니다.

GUI를 통해 로그 파일 다운로드



참고: 어플라이언스에서 FTP를 활성화해야 합니다. FTP를 활성화하려면 이 문서의 Enable FTP on Secure Web Appliance를 참조하십시오.

GUI에서 로그 파일을 다운로드할 수 있습니다.

1단계. GUI에 로그인

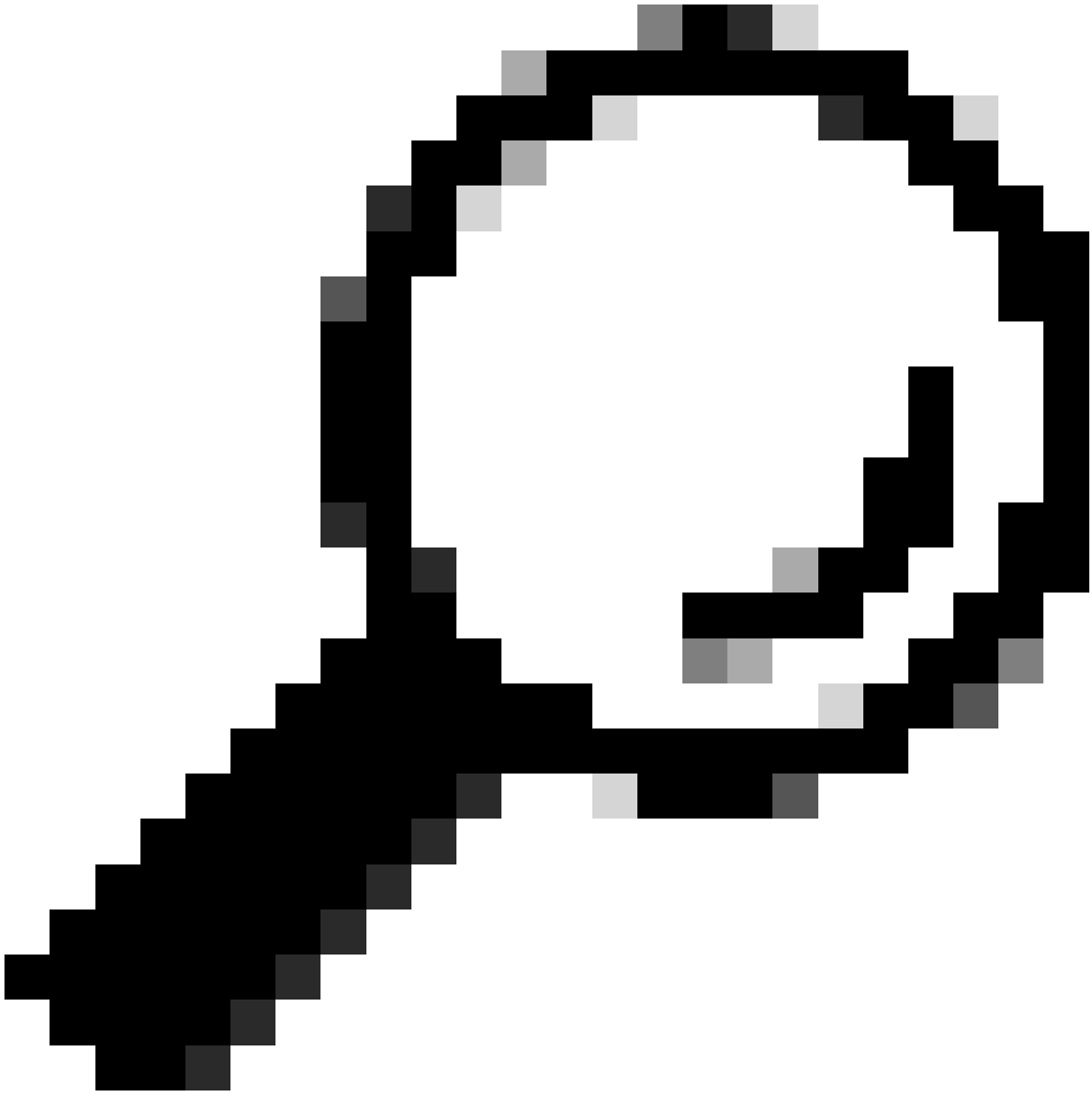
2단계. System Administration(시스템 관리)으로 이동합니다

3단계. 로그 서브스크립션 선택

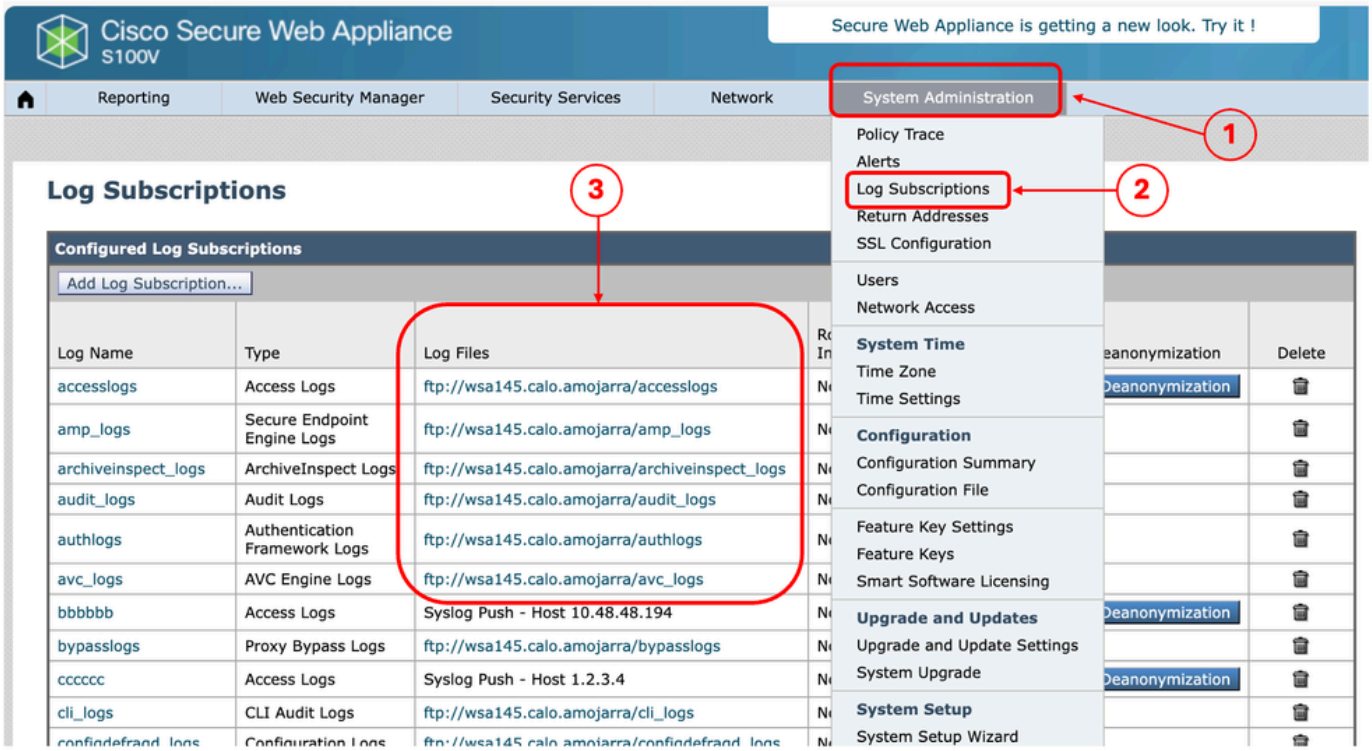
4단계.로그 서브스크립션 목록의 Log Files(로그 파일) 열에서 로그 서브스크립션의 이름을 클릭합니다.

5단계. 프롬프트가 표시되면 어플라이언스에 액세스하기 위한 관리자 사용자 이름 및 비밀번호를 입력합니다.

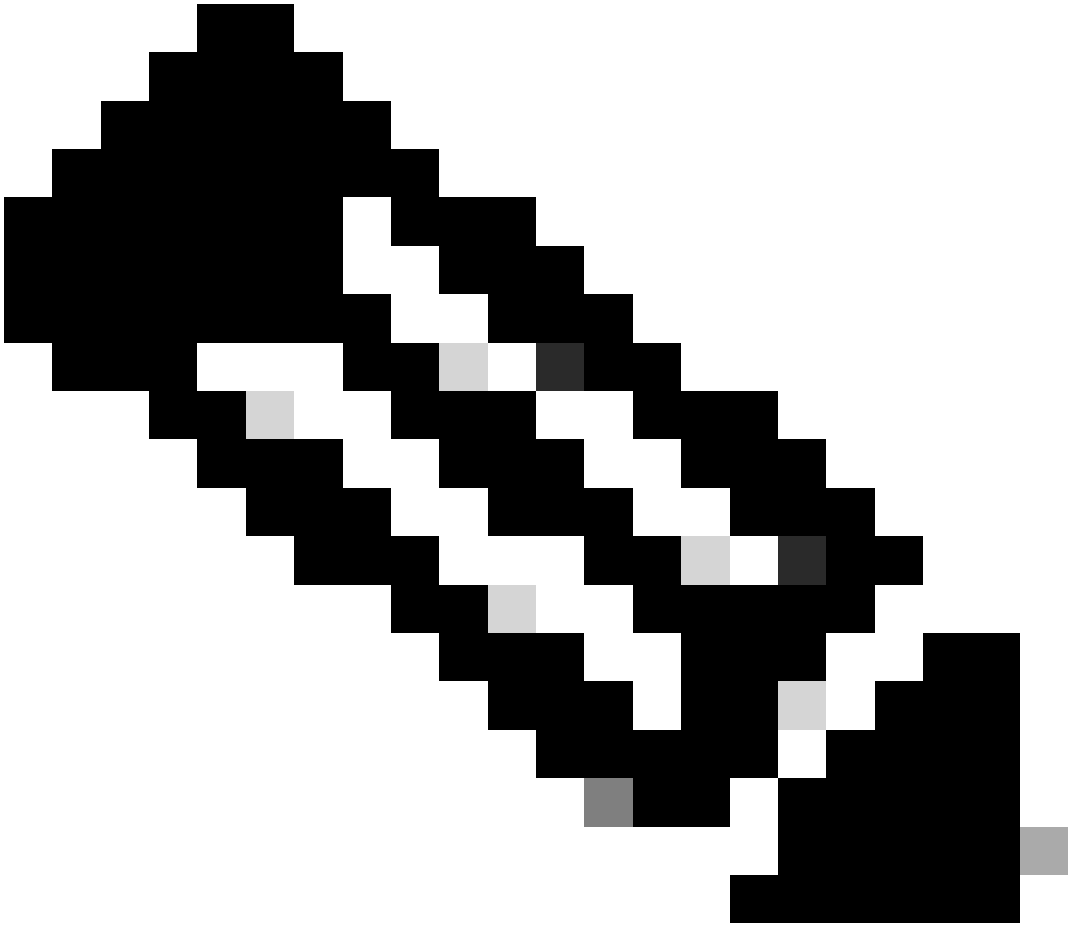
6단계.로그인하면 로그 파일 중 하나를 클릭하여 브라우저에서 보거나 디스크에 저장합니다.



팁: 업데이트된 결과를 보려면 브라우저를 새로 고치십시오.



이미지 - 로그 파일 다운로드



참고: 로그 서브스크립션이 압축되면 다운로드, 압축 풀기, 열어야 합니다.

CLI에서 로그 보기

CLI에서 로그를 볼 수 있습니다. 이 경우 로그에 있는 키워드에 대한 필터링 또는 라이브 로그에 액세스할 수 있습니다.

1단계. CLI에 연결

2단계. grep를 입력하고 Enter 키를 누릅니다.

3단계. 보려는 로그 번호를 입력합니다

4단계(선택 사항) 정규식이나 단어를 정의하여 출력을 필터링할 수 있습니다. 그렇지 않으면 Enter를 누릅니다

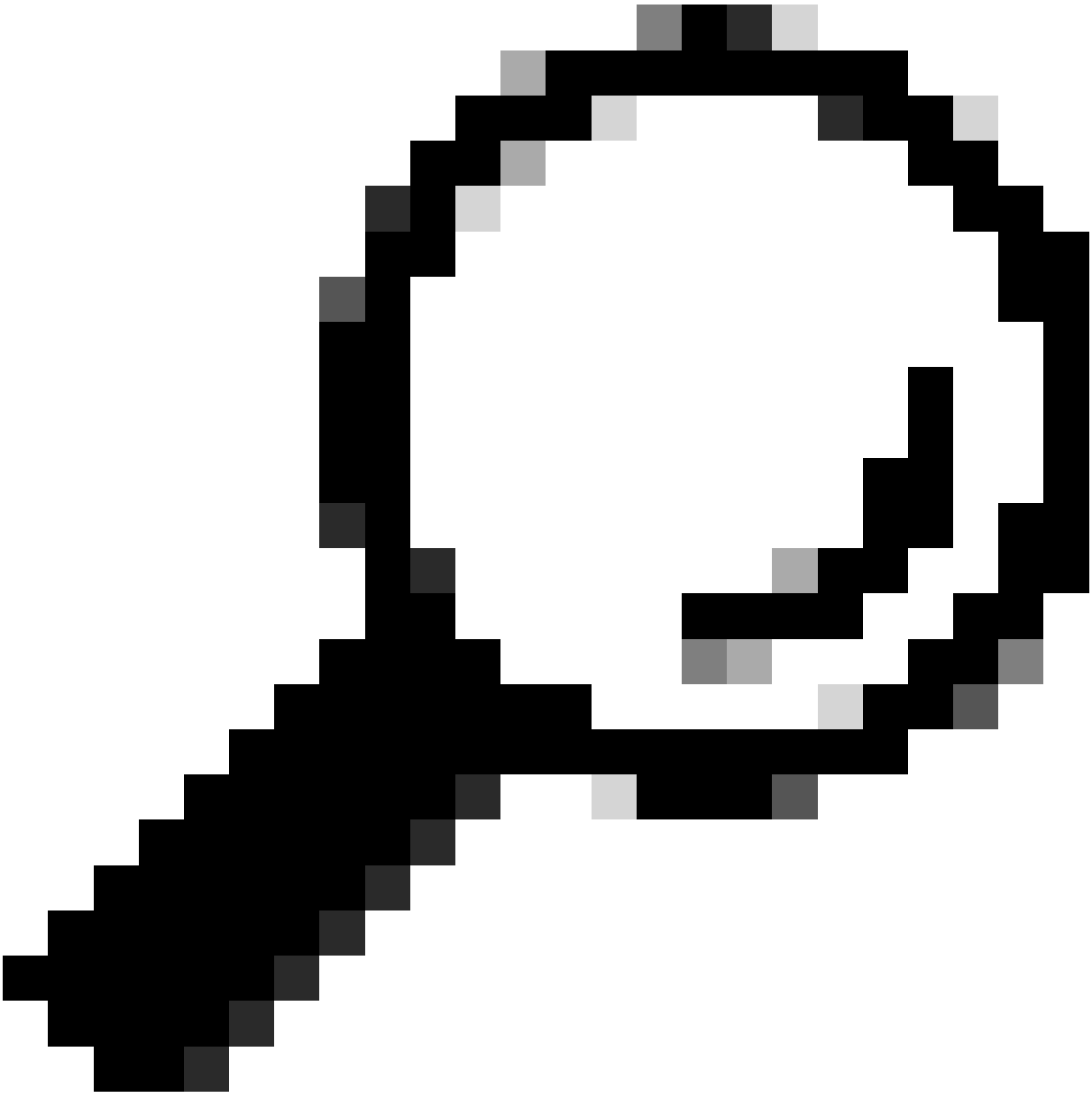
5단계. 4단계에서 입력한 키워드를 대/소문자를 구분하지 않고 검색해야 하는 경우 "Do you want this search to be case insensitive?"에서 Enter를 누릅니다. [Y]>" 또는 "N"을 입력하고 Enter 키를

누릅니다.

6단계. 검색에서 키워드를 제외해야 하는 경우 "일치하지 않는 줄을 검색하시겠습니까?"에 "Y"를 입력하십시오. [N]>" 또는 <Enter>를 누릅니다.

7단계. 라이브 로그를 보려면 "로그를 테일링하시겠습니까?"에 "Y"를 입력합니다. [N]>" 또는 <Enter>를 누릅니다.

8단계. 로그의 페이지 번호를 지정하여 페이지를 보려는 경우 "출력을 페이지 번호로 지정하시겠습니까?"에서 "Y"를 입력합니다. [N]>" 또는 <Enter>를 누릅니다.



팁: 페이지 번호를 지정하는 경우 "q"를 눌러 로그를 종료할 수 있습니다.

다음은 "Warning"이 포함된 모든 행을 보여 주는 샘플 출력입니다.

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "Secure Endpoint Engine Logs" Retrieval: FTP Poll
3. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
4. "audit_logs" Type: "Audit Logs" Retrieval: FTP Poll
5. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
6. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
7. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
8. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
...
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 40

Enter the regular expression to grep.
[]> Warning

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]>

Do you want to paginate the output? [N]>
```

Secure Web Appliance에서 FTP 활성화

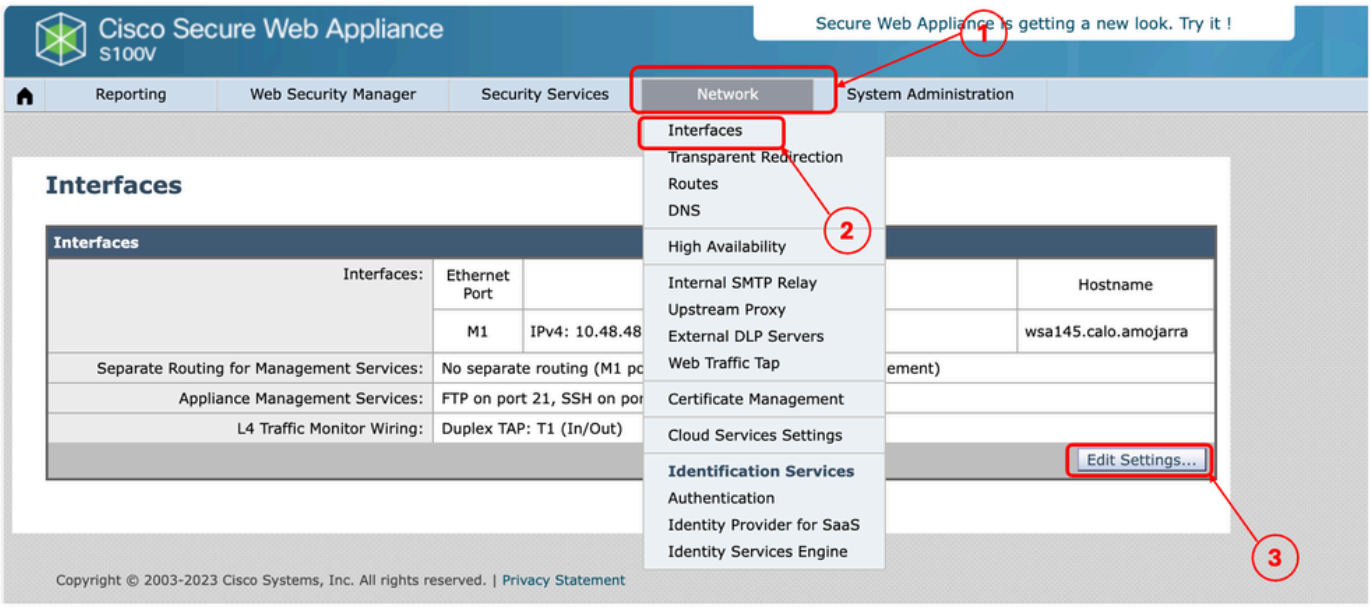
기본적으로 FTP는 SWA에서 활성화되지 않습니다. FTP를 활성화하려면

1단계. GUI에 로그인

2단계. 네트워크 탐색

3단계. 인터페이스 선택

4단계. Edit Settings(설정 편집)를 클릭합니다.

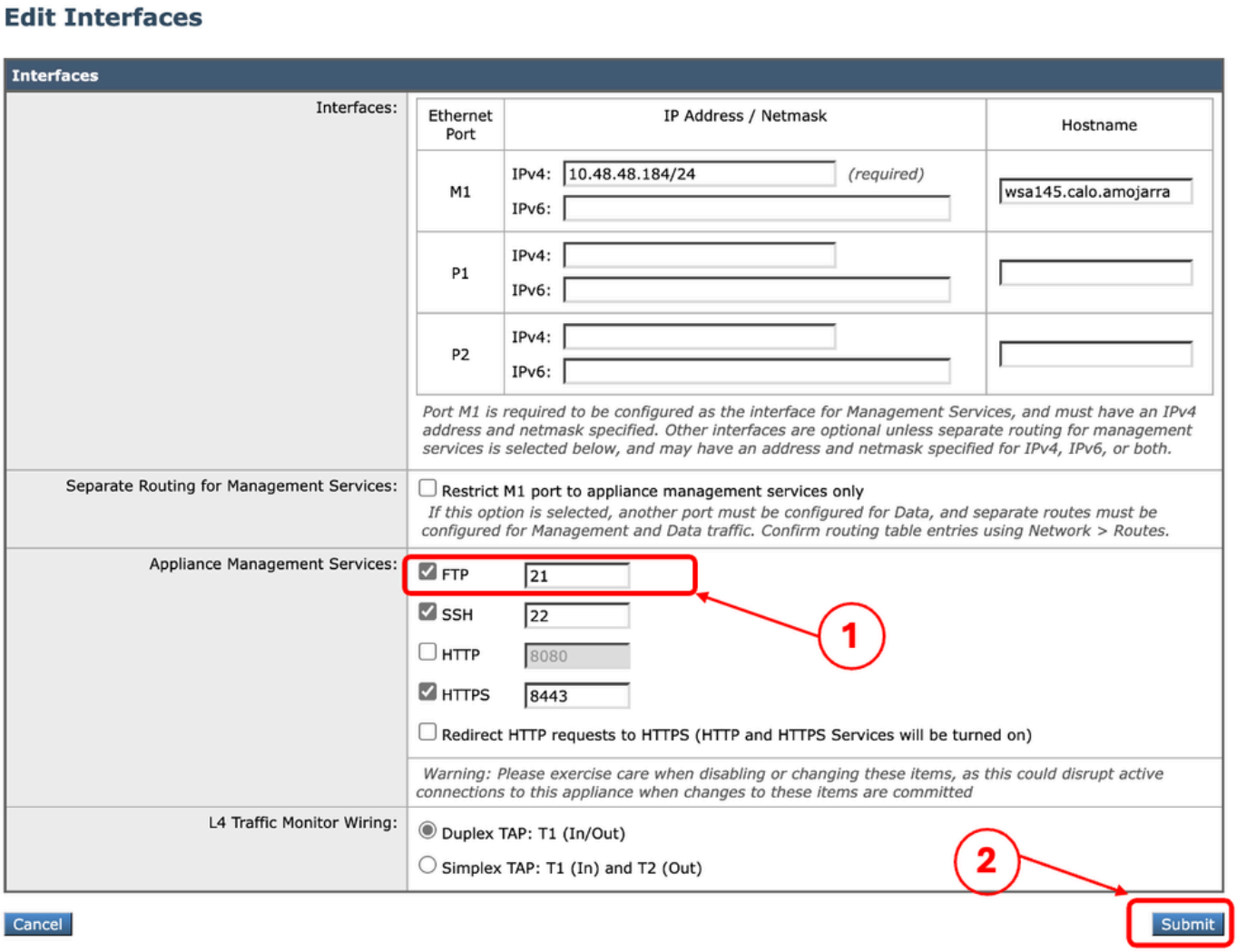


이미지 - SWA에서 FTP 사용

5단계. FTP에 대한 확인란을 선택합니다

6단계. FTP에 대한 TCP 포트 번호 제공(기본 FTP 포트는 21)

7단계. 변경 내용을 제출하고 커밋합니다



이미지 - SWA에서 FTP 매개변수 구성

관련 정보

- [AsyncOS 15.0 for Cisco Secure Web Appliance - LD 사용 설명서(제한적 배포) - 문제 해결 방법...]
- [Microsoft Server - Cisco를 사용하여 Secure Web Appliance에서 SCP 푸시 로그 구성]

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.