네트워크 설정 구성

네트워크 설정 구성

네트워크 구성에 따라 다음 포트를 사용하여 액세스를 허용하도록 방화벽을 구성해야 할 수도 있습니다. SMTP 및 DNS 서비스는 인터넷에 액세스해야 합니다.

Web Security Appliance는 다음 포트에서 수신 대기할 수 있어야 합니다.

- FTP: 포트 21, 데이터 포트 TCP 1024 이상
- HTTP(포트 80)
- HTTPS: 포트 443
- 관리 액세스: 포트 8443(HTTPS) 및 8080(HTTP)
- SSH: 포트 22

Web Security Appliance는 다음 포트에서 아웃바운드 연결을 설정할 수 있어야 합니다.

- DNS: 포트 53
- FTP: 포트 21, 데이터 포트 TCP 1024 이상
- HTTP(포트 80)
- HTTPS: 포트 443
- LDAP: 포트 389 또는 3268
- SSL을 통한 LDAP: 포트 636
- 글로벌 카탈로그 쿼리용 SSL을 사용하는 LDAP: 포트 3269
- NTP: 포트 123
- SMTP: 포트 25

참고 포트 80 및 443을 열지 않으면 기능 키를 다운로드할 수 없습니다.

자세한 내용은 사용 중인 버전에 대한 Cisco Web Security Appliances용 AsyncOS 사용 가이드에서 방화벽 정보를 참조하십시오.

구성 요약

항목	설명
관리	https://192.168.42.42:8443 을 입력하거나 시스템 설정 마법사를 완료한 후 관리 인터페이스에 할당된 IP 주소를 사용하여 관리 포트에서 Web Security Appliance를 관리할 수 있습니다. 구성을 공장 기본 설정으로 재설정하는 경우(예: 시스템 설정 마법사를 다시 실행), 관리 포트(https://192.168.42.42:8443)에서만 관리 인터페이스에 액세스할 수 있으므로 관리 포트에 연결되어 있는지 확인합니다. 또한, 관리 인터페이스의 방화벽 포트 80 및 443이 열려 있는지 확인합니다.
데이터	시스템 설정 마법사를 실행하면 네트워크의 클라이언트로부터 웹 트래픽을 수신하도록 어플라이언스의 포트가 하나 이상 구성됩니다(M1만, M1 및 P1, M1, P1 및 P2, P1만, 또는 P1 및 P2). 참고 웹 프록시를 명시적 전달 모드로 구성한 경우, 클라이언트 시스템의 애플리케이션이 데이터에 대해 구성된 IP 주소(M1 또는 P1)를 사용하여 웹 트래픽을 웹 보안 어플라이언스의 웹 프록시로 명시적으로 전달하도록 구성해야 합니다.
트래픽 모니터	시스템 설정 마법사를 실행한 다음, 하나 또는 두 개의 L4 트래픽 모니터 포트(T1만 또는 T1과 T2 모두)가 모든 TCP 포트에서 트래픽을 수신하도록 구성됩니다. L4 트래픽 모니터의 기본 설정은 모니터링 전용입니다. 설정 도중 또는 이후에 의심스러운 트래픽을 모니터링하고 차단하도록 L4 트래픽 모니터를 구성할 수 있습니다.
컴퓨터 주소	컴퓨터 IP 주소 를 "원격 액세스를 위해 일시적으로 IP 주소 변경"에 기록된 원래 설정으로 다시 변경해야 합니다. 참고 **System Administration**(시스템 관리) > **Configuration Summary**(구성 요약) 페이지에서 시스템 설정 요약을 검토할 수 있습니다.