추가 구성

다음 주제에서는 어플라이언스에서 구성할 수 있는 몇 가지 추가 기능에 대해 설명합니다. 자세한 내용은 해당 AsyncOS 릴리스의 온라인 도움말 또는 사용 가이드를 참조하십시오.

사용자 정책

웹 인터페이스를 사용하여 필요에 따라 어떤 사용자가 어떤 웹 리소스에 액세스할 수 있는지 정의하는 정책을 생성합니다.

- 사용자 식별 - **Web Security Manager(**웹 보안 관리자**)** > **Identities(ID)**를 선택하여, 인터넷에 액세스할 수 있는 사용자 그룹을 정의합니다.
- 액세스 정책 정의 - **Web Security Manager** > **Access Policies(**액세스 정책**)**을 선택하여, 허용하거나 차단할 개체 및 애플리케이션, 모니터링 또는 차단할 URL 범주, 웹 신뢰도 및 악성코드 차단 설정을 구성하여 인터넷에 대한 사용자 액세스를 제어합니다.

또한 인터넷에 대한 액세스를 제어하여 조직의 사용 제한 정책을 적용하는 몇 가지 다른 정책 유형을 정의할 수 있습니다. 예를 들어 HTTPS 트랜잭션의 암호 해독을 위한 정책과 업로드 요청을 제어하는 기타 정책을 정의할 수 있습니다.

Cisco Web Security Appliance 어플라이언스에서의 정책 구성에 대한 자세한 내용은 의 *Cisco Web Security Appliance*용 *AsyncOS* 사용 가이드의 "정책 사용" 장을 참조하십시오.

보고

웹 인터페이스에서 사용 가능한 보고서를 확인하여 네트워크에서 차단되고 모니터링된 웹 트래픽에 대한 통계를 볼 수 있습니다. 가장 많이 차단된 URL 범주, 클라이언트 활동, 시스템 상태 등에 대한 보고서를 볼 수 있습니다.

추가 정보

Cisco Web Security Appliance에 대해 구성할 수 있는 다른 기능이 있습니다. 기능 키, 최종 사용자 알림, 로깅 구성에 대한 자세한 내용 및 사용 가능한 다른 Web Security Appliance 기능에 대한 자세한 내용은 Cisco Web Security Appliance S196, S396, S696 및 S696F 설명서를 참조하십시오.