WBRS, WebRoot 또는 McAfee 검사를 우회하도록 Cisco Web Security Appliance(5.2.0 이상 실행)에서 웹 페이지를 수동으로 화이트리스트하려면 어떻게 해야 합니까?

목차

질문:

WBRS, WebRoot 또는 McAfee 검사를 우회하도록 Cisco Web Security Appliance(5.2.0 이상 실행)에서 웹 페이지를 수동으로 화이트리스트하려면 어떻게 해야 합니까?

증상:

사용자가 합법적인 사이트에 액세스하려고 하지만 WBRS 점수(웹 서버의 바이러스 감염, 웹 서버 IP를 통해 전송되는 스팸 등)가 낮거나 해당 페이지에서 트리거되는 안티멀웨어 엔진 중 하나로 인해 차단되고 있습니다.

낮은 WBRS로 인해 사용자가 차단된 경우 MALWARE_GENERAL 차단 메시지가 표시됩니다.액세스 로그에는 차단 임계값(기본값: -6.0)보다 낮은 WBRS가 표시됩니다.

영구 솔루션의 경우, WBRS를 조정하거나 안티바이러스 및 안티멀웨어 벤더에 오탐(false positives)을 보고하기 위해 페이지를 검토할 수 있도록 Cisco TAC에 문의하십시오.

또한 Cisco TAC에 문의하여 사이트가 차단된 이유에 대한 자세한 정보를 수집하여 기술 담당자 또는 웹 사이트 관리자에게 알리고 필요한 단계를 수행할 수 있습니다.
Cisco TAC에 문의할 때 관련 차단 코드 및 액세스 로그 라인을 제공해야 합니다.

WBRS를 우회하려면

4. 새로 생성된 웹 액세스 정책의 "Web Reputation and Anti-Malware Filtering(웹 평판 및 안티멀웨어 필터링)" 열에서 링크를 클릭합니다(지금까지는 '글로벌 정책'을 읽어야 함).
5. '웹 평판 및 안티멀웨어 맞춤형 설정 정의'를 선택합니다.

참고: URL Category(URL 카테고리)에서 작업을 "Allow(허용)"로 설정하면 안티멀웨어/바이러스 검사를 우회하게 됩니다.

WBRS 및 안티멀웨어 검사를 우회하려면

참고:안티멀웨어 스캐닝(Webroot 및/또는 McAfee)을 비활성화하면 잠재적인 보안 위험이 발생할 수 있습니다.이는 악성코드를 포함하지 않을 수 있는 신뢰할 수 있는 사이트에 대해서만 수행해야 합니다.