Cisco Web Security Appliance(5.2.0 이상 실행)에서 웹 페이지를 화이트리스트에 수동으로 추가하여 WBRS, WebRoot 또는 McAfee 스캔을 우회하려면 어떻게 해야 합니까?

TAC **문서 ID: 117932**

기고자: Simon Putz 및 Siddharth Rajpathak, Cisco TAC 엔지니어

2014년 7월 14일

목차

질문:

Cisco Web Security Appliance(5.2.0 이상 실행)에서 웹 페이지를 화이트리스트에 수동으로 추가하여 WBRS, WebRoot 또는 McAfee 스캔을 우회하려면 어떻게 해야 합니까?

증상:

사용자가 정상적인 사이트에 액세스하려고 하지만 WBRS 점수가 낮거나(웹 서버의 바이러스 감염, 웹 서버 IP를 통한 스팸 전송 등), 해당 페이지에서 악성코드 차단 엔진 중 하나가 실행되어 해당 사이트가 차단됩니다.

낮은 WBRS 점수로 인해 사용자가 차단된 경우 MALWARE_GENERAL 차단 메시지가 표시됩니다. 액세스 로그에 차단 임계값 이하의 WBRS 점수가 표시됩니다(기본값은 −6.0).

영구적인 해결책이 필요한 경우, Cisco TAC에 문의하면 해당 페이지를 검토하여 WBRS를 조정하거나 안티바이러스 및 악성코드 차단 공급업체에 오탐 사항을 보고할 수 있습니다.

또한 Cisco TAC에 문의하면 사이트가 차단된 이유에 대해 자세한 정보를 수집할 수 있으며, 해당 웹 사이트의 기술 담당자 또는 관리자에게 이러한 내용을 알리고 필요한 조치를 취할 수 있습니다.
Cisco TAC에 문의할 경우, 관련 차단 코드 및 액세스 로그 행을 반드시 제공하도록 합니다.

WBRS를 우회하려면:

1. 차단하지 않으려는 모든 사이트가 포함된 맞춤형 URL 범주를 생성합니다(GUI −> Web Security Manager −> Custom URL Categories(맞춤형 URL 범주)).

2. 새 ID를 생성하고 새로운 맞춤형 URL 범주에 이를 구성원으로 추가합니다(GUI −> Web Security Manager −> Identities).
   설정에 따라, 해당 그룹/사용자 멤버십 설정에 대해 'authentication required'(인증 필요) 또는 'no authentication'(인증 없음)을 선택해야 합니다.
3. 새로운 웹 액세스 정책을 생성하고(GUI −> Web Security Manager −> Web Access Policies(웹 액세스 정책)), 새 ID를 Policy Member Definition(정책 구성원 정의)의 액세스 정책과 연결합니다.

4. 새로 생성한 웹 액세스 정책(지금까지는 'global policy'(글로벌 정책)로 표시됨)의 "Web Reputation and Anti−Malware Filtering"(웹 평판 및 악성코드 차단 필터링) 열에서 링크를 클릭합니다.
5. 'Define Web Reputation and Anti−Malware Custom Settings'(웹 평판 및 악성코드 차단 맞춤형 설정 정의)를 선택합니다.
6. WBRS 검사를 사용하지 않도록 설정하고 필요에 따라 다른 악성코드 검사 매개변수도 조정합니다.
7. 변경 사항을 제출하고 커밋합니다.

참고: URL 범주에서 작업을 "허용"으로 설정할 경우, 악성코드 차단/안티바이러스 검사를 우회하게 됩니다.

WBRS 및 악성코드 차단 검사를 우회하려면:

참고: 악성코드 차단 검사(Webroot 및/또는 McAfee)를 우회하면 잠재적인 보안 위험으로 이어질 수 있습니다. 악성코드가 포함되어 있지 않은 신뢰할 수 있는 사이트에 한해서만 이러한 우회를 설정해야 합니다.

1. 차단하지 않으려는 모든 사이트가 포함된 맞춤형 URL 범주를 생성합니다(GUI −> Web Security Manager −> Custom URL Categories(맞춤형 URL 범주)).
2. 새 ID를 생성하고 새로운 맞춤형 URL 범주에 이를 구성원으로 추가합니다(GUI −> Web Security Manager −> Identities).
3. 새로운 웹 액세스 정책을 생성하고(GUI −> Web Security Manager −> Web Access Policies(웹 액세스 정책)), 새 ID를 Policy Member Definition(정책 구성원 정의)의 액세스 정책과 연결합니다.
4. WBRS 및 악성코드 차단을 완전히 우회할 새로운 웹 액세스 정책에서 "URL Categories"(URL 범주) 열의 링크를 클릭합니다.
5. 이전에 생성한 맞춤형 URL 범주의 경우, 'allow'(허용) 작업을 선택합니다.
6. 변경 사항을 제출하고 커밋합니다.

업데이트 날짜: 2014년 7월 14일 문서 ID: 117932