Windows 7/Vista 클라이언트의 트래픽은 액세스 로그에 사용자 대신 워크스테이션을 표시합니다.

목차

질문

Windows 7/Vista 클라이언트의 트래픽이 액세스 로그에 사용자 대신 워크스테이션을 표시하는 이유는 무엇입니까?

환경

Microsoft Windows 7, Microsoft Windows Vista, Cisco Web Security Appliance(모든 버전), 서로게이트 유형:IP 주소

증상

액세스 로그의 특정 로그 라인에 DOMAIN\USER 대신 컴퓨터 컴퓨터 이름이 표시됩니다.

Microsoft는 Windows 7과 Windows Vista에 "NCSI(Network Connectivity Status Indicator)"라는 새로운 기능을 도입했습니다. 이 기능은 시스템 트레이의 네트워크 인터페이스 아이콘 위에 나타나는 작은 둥근 아이콘으로 표시됩니다.로그인 직후 이 기능은 인터넷 연결이 있는지 확인하기 위해 인터넷에서 데이터를 요청하려고 시도합니다.

NTLM 인증이 필요할 때 사용자 자격 증명 대신 머신 자격 증명을 보내는 NCSI에 알려진 문제가 있습니다.

NCSI는 PC에서 WSA로 첫 번째 요청을 보낼 가능성이 높으므로 아직 서로게이트가 없으며 실제 사용자 이름 대신 머신 이름을 가진 새 IP 기반 서로게이트가 생성됩니다.이 서로게이트는 최초 IP 주소에서 서로게이트가 시간 초과되어 사용자가 다시 인증해야 할 때까지 모든 요청에 사용됩니다(이번에는 실제 자격 증명으로).

시스템 이름이 처음에 의도한 AD 그룹의 구성원이 아닐 수 있으므로 모든 요청은 올바른 액세스/암호 해독 정책을 트리거하지 않으며, 때로는 요청이 차단되기도 합니다.

NCSI에 대한 자세한 내용은 다음 Microsoft KB 문서를 참조하십시오.

문제를 해결하려면 아래 지침을 참조하십시오.

1. 작업 메뉴에서 "regedit"를 검색하여 레지스트리 편집기를 시작합니다.마우스 오른쪽 버튼을 클릭하고 "관리자로 실행"을 선택해야 합니다.

2. 다음으로 이동 :HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet

3. 인터넷 키 아래에서 "EnableActiveProbing"을 두 번 클릭한 다음 값 데이터에서 다음을 입력합니다.0.
4. "확인"을 클릭합니다.

5. 컴퓨터를 다시 시작합니다.

이러한 변경 사항은 도메인 컨트롤러를 사용하여 모든 클라이언트에 GPO(Global Policy Object)로 푸시할 수 있습니다.

WSA의 해결 방법

NCSI에 대한 ID를 생성하고 URL 또는 사용자 에이전트를 기반으로 인증에서 제외합니다.

NCSI가 연결되는 알려진 URL

ncsi.glbdns.microsoft.com
newncsi.glbdns.microsoft.com
www.msftncsi.com

NCSI 사용자 에이전트

Microsoft NCSI