사용자가 UltraSurf를 사용하지 못하도록 방지

목차

소개

이 문서에서는 사용자가 UltraSurf를 사용하지 못하도록 하는 방법에 대해 설명합니다.

문제

사용자가 UltraSurf 프록시를 사용하여 콘텐츠 필터링 및 보안 컨피그레이션을 우회합니다.

원인

UltraSurf는 일반적인 콘텐츠 필터링 솔루션을 우회할 수 있도록 여러 가지 수단을 결합합니다. SSL을 사용하여 원격 호스트에 대한 연결을 생성하여 데이터를 암호화하고 대부분의 솔루션에서 "훔쳐보기"를 방지합니다.

현재 UltraSurf는 유효하지 않은 SSL 인증서를 사용하여 이러한 연결을 설정하므로 브라우저의 보안 설정을 낮추도록 변경합니다. 이전 버전에서 UltraSurf는 DNS를 콘텐츠 필터링 솔루션을 우회하는 메커니즘으로 사용했으며 Umbrella는 이러한 DNS 서버를 식별하여 액세스를 차단함으로써 DNS를 늦출 수 있었습니다. 그러나 UltraSurf를 지원하는 그룹은 지속적으로 새로운 버전의 소프트웨어를 출시하고 있으므로 접근 방식을 다시 변경하는 것은 시간 문제일 뿐입니다.

솔루션

UltraSurf에서 사용하는 것으로 알려진 서브넷을 차단하는 것을 포함하여 추가적인 조치를 취할 수 있습니다. 일반적으로 ISP에 할당된 동적 IP 범위이며 비즈니스 사용자에게는 적법한 사용이 거의 또는 전혀 없습니다. 또한 Active Directory 환경에서는 소프트웨어 제한 정책을 사용하여 애플리케이션을 제한할 수 있습니다. 이 기능은 현재 및 이전 버전의 UltraSurf 소프트웨어가 네트워크에서 실행되는 것을 제한하는 데 사용할 수 있습니다.

새 버전이 출시되면 소프트웨어 제한 정책을 추가해야 합니다. 또한 사용자가 Internet Explorer의 보안 옵션을 변경할 수 있는 사항을 제한하여 유효하지 않은 보안 인증서를 사용하지 못하도록 할 수 있습니다. Cisco는 Ultrasurf가 각 개정판에서 수행하는 버전과 변경 사항을 지속적으로 모니터링하고 Ultrasurf 액세스를 방지하는 데 Umbrella가 도움이 될 수 있는 방법을 모색하고 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.