

HSTS 문제 해결 및 인증서 오류 피닝

목차

[소개](#)

[인증서 오류](#)

[가능한 솔루션](#)

[정책 관리 및 로밍 클라이언트](#)

[인증서 예외 오류 무시\(Windows의 경우 Chrome 전용\)](#)

[Mac OS X용 Firefox, Safari 및 Chrome](#)

[인터넷 탐색기](#)

소개

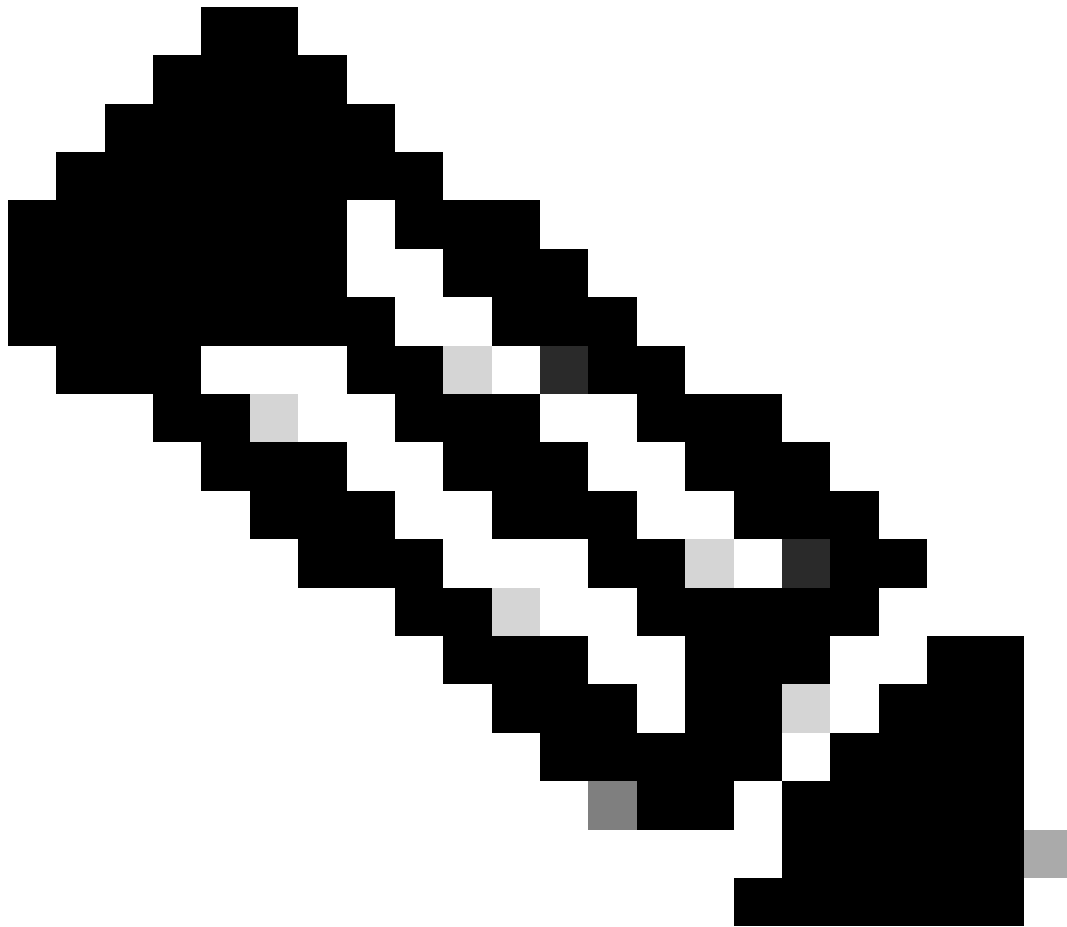
이 문서에서는 우회할 수 없는 "Your Connection is Untrusted/Not Private" 인증서 오류를 지우는 방법을 설명합니다.

인증서 오류

*.opendns.com 또는 *.cisco.com에 대한 인증서 오류가 나타나지만 Cisco Umbrella 설명서에 설명된 대로 인증서 예외를 추가하여 우회할 수 없는 경우 Cisco Umbrella [루트 인증서 관리](#), 인증서 오류를 지우려면 다음 단계를 따르십시오.

예외를 추가하여 인증서 오류를 무시할 수 없는 경우, 이는 최신 브라우저에서 HTTP HSTS(Strict Transport Security) 또는 사전 로드된 인증서 피닝 구현으로 인해 발생합니다. 특정 브라우저와 특정 웹 사이트 간의 통신은 HTTPS 사용 요구 사항을 포함하고 우회 또는 예외가 가능하지 않은 방식으로 수행됩니다. HTTPS 페이지에 대한 이러한 추가 보안은 HSTS가 웹 사이트에 대해 활성 상태일 때 Umbrella 블록 페이지 및 우회 블록 페이지 [메커니즘](#)이 작동하지 않도록 합니다.

그 결과 해당 페이지는 BPB([Block Page Bypass](#))를 통해 액세스할 수 없습니다(사실상 Bypass 화면이 나타나지 않을 수도 있음). 이러한 방법으로 BPB 로그인에 대한 액세스를 허용할 수 있지만, 로그인 후 인증서 오류가 다시 나타나며 액세스를 거부합니다. Google Chrome, Mozilla Firefox, Safari에서 우회할 수 없는 인증서 오류가 발견되어 우회 로그인에 액세스하려는 경우 이 문서의 나머지 부분을 검토하십시오.



참고: 이제 모든 사이트를 더 쉽게 관리하고 지속할 수 있는 이 문제를 해결할 수 있습니다.

그 결과, 이 정보는 여전히 적용 가능하지만, 이제 영구적인 솔루션을 사용하여 작업할 수 있습니다. Cisco Umbrella 설명서를 통해 Cisco Root CA를 설치해 보십시오. [Cisco Umbrella 루트 인증서 관리](#)

중요: 도메인이 HSTS 고정 목록에 있는 경우 Chrome, Safari 또는 Firefox(IE(Internet Explorer)는 영향을 받지 않음)를 실행 중인 경우 목록을 사실상 우회할 수 없으므로 예외를 추가할 수 없습니다. 이러한 사이트에서는 차단 페이지 우회가 작동하지 않습니다. 이 세 가지 브라우저에서 HSTS를 사용하는 전체 서비스 목록을 보려면 [Google Chromium Code Search를 검토하십시오](#). 이 목록에서 주목할 만한 서비스는 다음과 같습니다.

- Google(및 Gmail, Youtube, Google Docs와 같은 Google 리소스)
- 드롭 박스
- 트위터
- Facebook

이로 인해 사용자 또는 사용자에게 문제가 발생하는 경우 이 문제를 완화하기 위해 차단 페이지 우회 변경 사항을 보려면 umbrella-support@cisco.com 또는 계정 관리자에게 이메일을 보내 기능 요청을 제출하십시오. Cisco의 제품 관리 및 엔지니어링 팀은 인증서 및 차단 페이지 우회의 어려움을 인식하고 이 기능의 대체 재설계를 테스트하고 있습니다.

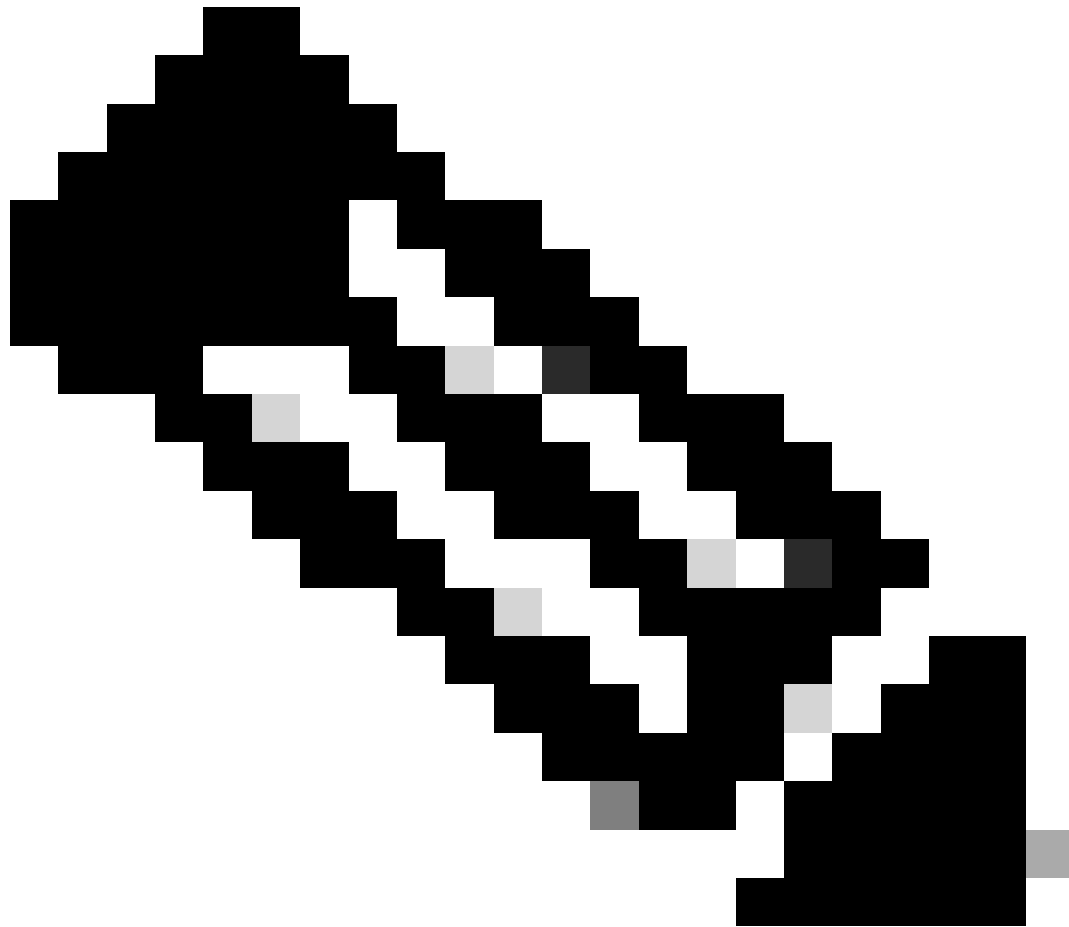
가능한 솔루션

이러한 문제를 해결할 수 있는 몇 가지 방법이 있습니다. 먼저, 이 섹션에서는 이 문제를 해결하기 위해 더욱 세분화된 정책을 사용하는 방법을 시연합니다. 둘째, 브라우저 컨피그레이션을 사용할 수 있지만 이러한 컨피그레이션은 이 문제의 영향을 받는 브라우저의 하위 집합으로 격리됩니다.

정책 관리 및 로밍 클라이언트

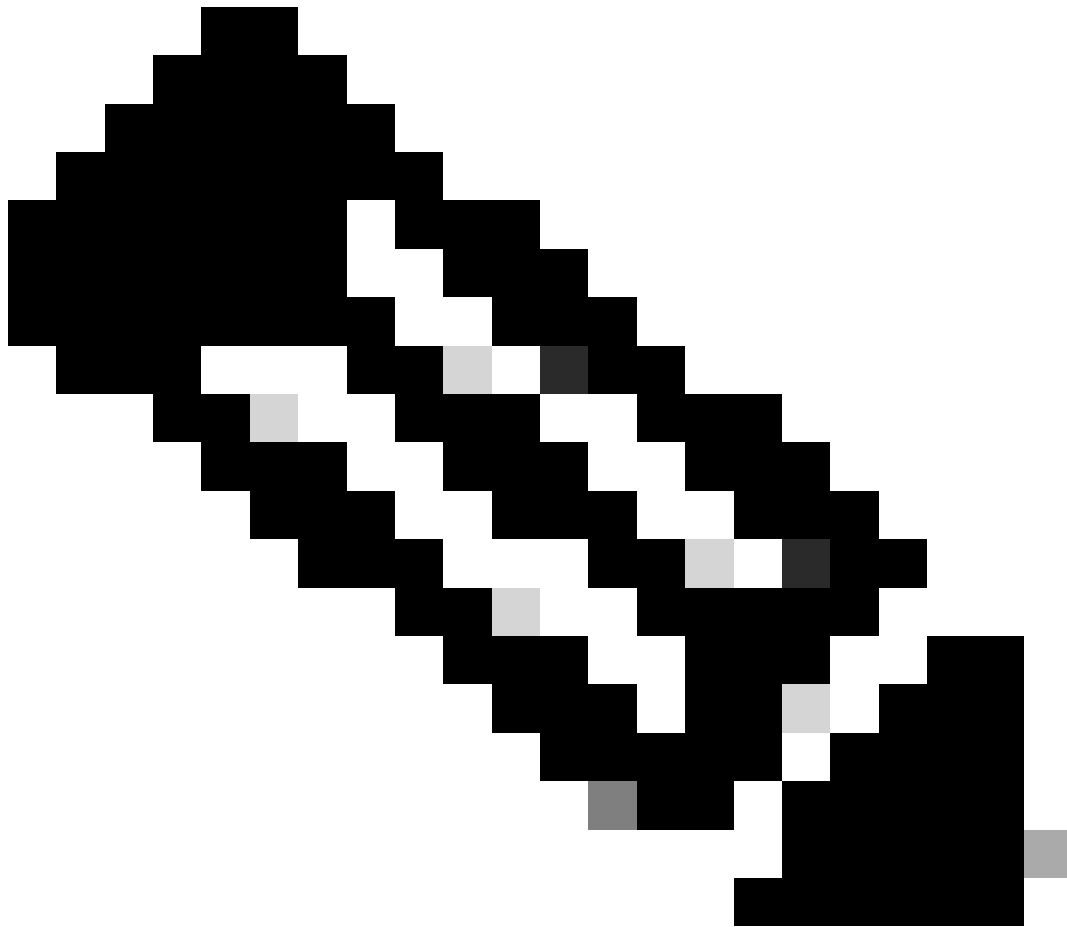
네트워크 컨피그레이션 또는 HR(Acceptable Usage) 정책에 문제가 있어 이 솔루션이 차단될 수 있습니다. 사용자가 정해진 시간(예: 점심시간)에만 이러한 도메인을 방문할 수 있는 경우 정책 관리가 효과적이지 않습니다. Umbrella는 Cisco 서비스와 함께 시간 기반 정책 애플리케이션을 제공할 수 없으므로 사용자가 항상 사이트에 액세스하도록 허용하는 것만으로는 문제가 발생할 수 있습니다. 공용 터미널과 같은 공유 컴퓨터에서는 Umbrella 로밍 클라이언트가 사용자를 구별할 수 없으며 적합한 사용자를 위한 올바른 도메인을 쉽게 허용할 수 없습니다.

정책 관리는 사이트 또는 네트워크와 같이 세분화되지 않은 ID를 고려할 때 효과적이지 않습니다. 관리자가 해당 네트워크의 모든 사용자에게 동일한 액세스 권한을 부여하는 데 익숙하지 않은 경우 그렇습니다. 정책 관리는 네트워크의 나머지가 사이트에 액세스할 수 없는 동안 사이트에 액세스할 수 있는 사용자 하위 집합에 적용하거나, 시스템에 로밍 클라이언트를 설치하고 적절한 정책 계층 구조를 적용하여 해당 사용자를 골라내는 경우에 가장 효과적입니다.



참고: Cisco는 2024년 4월 2일 Umbrella Roaming Client의 End-of-Life를 발표했습니다. Umbrella Roaming Client에 대한 지원 종료일은 2025년 4월 2일입니다. 모든 Umbrella Roaming Client 기능은 현재 Cisco Secure Client에서 사용할 수 있습니다. Cisco는 Cisco Secure Client에서만 미래의 혁신을 제공합니다. 이제 고객이 마이그레이션 계획 및 일정을 수립하는 것이 좋습니다. Umbrella Roaming Client에서 Cisco Secure Client로 마이그레이션하는 방법에 대한 지침은 [이 KB](#) 문서를 참조하십시오.

브라우저가 처음부터 실패한 검증 응답을 받지 못하므로 적절한 정책 관리가 이 문제에 대한 최상의 솔루션입니다. 일부 사용자가 일반적으로 Block Page Bypass를 사용하여 액세스해야 하는 사이트에 액세스하도록 허용된 경우, 대신 이러한 사용자에게 별도의 정책을 구성하고, 이러한 사용자가 사용하도록 허용할 수 있는 도메인을 허용 목록에 추가할 수 있습니다. 사용자의 요청은 차단되지 않으므로, 브라우저는 인증서가 일치하지 않는 도메인의 요청을 수신하지 않습니다. Umbrella [Roaming Client](#)를 사용하여 이러한 특정 정책을 전달할 수 있습니다. 즉, 하루 종일 특정 사용자가 이러한 오류를 해결할 수 있도록 특정 도메인을 허용 목록에 포함시킵니다.



참고: Umbrella 로밍 클라이언트는 특정 정책을 여러 사용자에게 배포하는 효과적인 방법이지만 AD(Active Directory) 통합을 활성화한 경우 특정 AD 사용자에게도 이러한 허용된 정책을 적용할 수 있습니다.

인증서 예외 오류 무시(Windows의 경우 Chrome 전용)

Windows용 Chrome만 인증서 예외 오류를 무시하도록 구성할 수 있습니다. 그러면 이 오류가 완화됩니다. 브라우저에 오류를 무시하라는 메시지가 표시되고 일반 Umbrella 블록 페이지가 대신 표시됩니다.

중요: 브라우저가 인증서 오류를 무시하도록 구성되어 있으므로 이 방법은 정책 관리를 조정하는 것보다 위험합니다. 따라서 브라우저가 MiTM(man-in-the-middle) 공격을 받을 수 있습니다. 따라서 이 오류를 해결하기 위한 안전한 접근 방법으로 이 방법을 권장할 수는 없지만 해결 방법이 됩니다.

이러한 컨피그레이션 변경은 컴퓨터별로 이루어져야 하므로 대규모 환경에서는 어렵지만 제대로 작동됩니다.

Mac OS X용 Firefox, Safari 및 Chrome

Mac OS X용 Firefox, Safari 및 Chrome은 고정된 도메인에 대한 인증서 예외 오류를 무시하도록 구성할 수 없으며 항상 HSTS 목록을 준수합니다. 이 오류에 대해 알려진 해결 방법이 없습니다.

인터넷 탐색기

IE(Internet Explorer)는 HSTS 제한을 구현하지 않습니다. 결과적으로 IE를 구성할 필요가 없으며 이 오류를 표시하지 않습니다. 이는 Microsoft가 브라우저에서 HSTS를 구현하도록 선택하는 경우 IE의 향후 버전에서 변경될 수 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.