

SWGプロキシによる非標準HTTPS要求の処理方法の理解

内容

[はじめに](#)

[概要](#)

[一般的な質問](#)

[SWGプロキシは非標準HTTPS Web要求を処理できますか。](#)

[HTTPSインスペクションを無効にできるか、または問題のドメインを選択的復号化リストに追加するとヘルプが表示されますか。](#)

[解決方法](#)

はじめに

このドキュメントでは、SWGプロキシが非標準HTTPS要求を処理する方法と、必要なクライアントコンプライアンスの概要について説明します。

概要

Umbrellaは、TLS SNI拡張を使用して宛先ドメインを検出し、HTTPS要求が復号化を必要とするかどうか、または選択的復号化リストを使用して復号化をバイパスするかどうかを判断します。クライアントは、関連するRFCに定義されているTLS標準に準拠する必要があります。ほとんどの有名なブラウザはこれらの標準に準拠しており、Umbrellaはそれらをサポートしています。

一般的な質問

SWGプロキシは非標準HTTPS Web要求を処理できますか。

No. クライアントが基本的な[TLSハンドシェイク](#)を実行しない場合、HTTPS要求は失敗します。たとえば、Client HelloまたはServer Helloの交換がない場合、要求は完了できません。

HTTPSインスペクションを無効にできるか、または問題のドメインを選択的復号化リストに追加するとヘルプが表示されますか。

いいえ。これらの操作では問題は解決しません。

解決方法

該当する非標準HTTPSサイトでは、SWGプロキシを完全にバイパスする必要があります。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。