

CSCの既知のソフトウェア競合の理解

内容

[はじめに](#)

[Cisco Security Connectorの既知のソフトウェア競合とは何ですか。](#)

はじめに

このドキュメントでは、Cisco Security Connector(CSC)の既知のソフトウェア競合について説明します。

Cisco Security Connectorの既知のソフトウェア競合とは何ですか。

一部のソフトウェアおよび特定のシナリオでは、[Cisco Security Connector\(CSC\)](#)が正しく機能しないことが確認されています。

次の状況では、CSCはProtectedを報告できますが、Webトラフィックにはポリシーが適用されません。

- VPN:Appleの設計では、CSCはVPNに向かうトラフィックのDNSパケットを受信できません。これは正常な動作です。
- モバイルホットスポット：ホットスポットを実行しているiPhoneに接続されているクライアントは、CSCの対象外です。ホットスポットを操作する電話機は、カバレッジを継続できます。
- Wanderaの「ゲートウェイ」:AppleはWanderaプロキシをVPNに似たゲートウェイとして認識します。したがって、Wandera経由で送信されるトラフィックはCSCカバレッジを受信できません。CSCは、Wanderaがアクティブであることを示す兆候として
*.proxy.wandera.comへの多くのDNS要求を確認できます。

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。