

Merakiトンネリングトラフィックプロトコルの理解

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[概要](#)

[IKEv2を有効にする手順](#)

はじめに

このドキュメントでは、MerakiがIPSecトンネルに使用するプロトコルについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Umbrellaは、トラフィックのトンネリングにIPsecプロトコルを使用します。IPsecには複数のコンポーネントがあり、重要なコンポーネントの1つは、ピアとのネゴシエーション、認証、および証明書交換を管理するIKEです。また、キープアライブメカニズムを使用してセッションを維持します。UmbrellaはIKEv2のみをサポートします。IKEv2はIKEv1よりも高速で安全です。Merakiは、IPsecトンネルに対してIKEv1およびIKEv2をサポートします。

IKEv2を有効にする手順

MerakiとUmbrellaの間にIPSecトンネルを正常に確立するには、Merakiナレッジベースの記事「

[MX and Umbrella SIG IPsec Tunnel](#)」を参照してください。

Merakiダッシュボードでトンネルを設定する際にサポートが必要な場合は、Merakiサポートにお問い合わせください。

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。