Comprendre le protocole Meraki Tunneling Traffic

Table des matières

Introduction

Ce document décrit le protocole que Meraki utilise pour les tunnels IPsec.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Umbrella utilise le protocole IPsec pour le trafic de tunnellisation. IPsec a plusieurs composants, et l'un des composants clés est IKE qui gère la négociation avec les homologues, l'authentification et les échanges de certificats. Il gère également la session à l'aide du mécanisme keep alive. Umbrella prend uniquement en charge IKEv2, qui est plus rapide et plus sécurisé que IKEv1. Meraki prend en charge IKEv1 et IKEv2 pour les tunnels IPsec.

Étapes pour activer IKEv2

Pour établir un tunnel IPsec entre Meraki et Umbrella, reportez-vous à l'article suivant de la base de connaissances Meraki : Tunnel IPSec MX et Umbrella SIG

Si vous avez besoin d'aide pour configurer le tunnel dans le tableau de bord Meraki, contactez le support technique de Meraki.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.