Understand the Meraki Tunneling Traffic Protocol

Contents

Introduction

This document describes the protocol that Meraki uses for IPsec tunnels.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on 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. If your network is live, ensure that you understand the potential impact of any command.

Overview

Umbrella uses the IPsec protocol for tunneling traffic. IPsec has multiple components, and one of the key components is IKE which manages negotiation with the peers, authenticating, and certificate exchanges. It also maintains the session by using the keep alive mechanism. Umbrella only supports IKEv2, which is faster and more secure than IKEv1. Meraki supports IKEv1 and IKEv2 for the IPsec tunnels.

Steps to Enable IKEv2

To successfully establish an IPsec tunnel between Meraki and Umbrella, please refer to this Meraki knowledge base article: MX and Umbrella SIG IPSec Tunnel

If you need assistance with configuring the tunnel in the Meraki dashboard, please contact Meraki support.