Het Meraki Tunneling Traffic Protocol

Inhoud

Inleiding

Dit document beschrijft het protocol dat Meraki gebruikt voor IPsec-tunnels.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Umbrella gebruikt het IPsec-protocol voor het tunnelen van verkeer. IPsec heeft meerdere componenten en een van de belangrijkste componenten is IKE, dat onderhandeling met de peers, authenticatie en certificaatuitwisselingen beheert. Het onderhoudt ook de sessie met behulp van het Keep Alive-mechanisme. Umbrella ondersteunt alleen IKEv2, dat sneller en veiliger is dan IKEv1. Meraki ondersteunt IKEv1 en IKEv2 voor de IPsec-tunnels.

Stappen om IKEv2 in te schakelen

Voor het succesvol tot stand brengen van een IPsec tunnel tussen Meraki en Umbrella verwijzen wij u naar dit Meraki kennisbank artikel: MX en Umbrella SIG IPSec Tunnel

Als u hulp nodig hebt bij het configureren van de tunnel in het Meraki-dashboard, neem dan contact op met Meraki-ondersteuning.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.