Configuring a site-to-site VPN tunnel with Coro Network and Cisco Meraki

As part of a virtual office, Coro includes the ability for customers to configure VPNs together with site-to-site VPN tunnels.

This guide describes how to establish a site-to-site VPN tunnel between Coro and a Cisco Meraki appliance through the Cisco Meraki platform, and how to configure Coro to integrate with Cisco Meraki's firewall.

To configure a Cisco Meraki site-to-site VPN tunnel, complete the following processes:

1. **Configure Cisco Meraki to allow traffic from inside and outside the network**
2. **Configure Coro to integrate with Cisco Meraki's firewall**

Prerequisites

Before you start, make sure you have the following:

- Access as an admin user to the Coro console for your workspace
- An active subscription (or trial) for the Coro Network module
- Access to the Cisco Meraki Dashboard

Configuring Cisco Meraki

Configure Cisco Meraki to allow traffic from inside and outside the network:

> **Important**
>
> The Cisco Meraki configuration method is the same whether Virtual MX (VMX) is hosted on Azure/AWS or is a physical device.

1. Sign into your Cisco Meraki Dashboard.
2. Select **Network**: