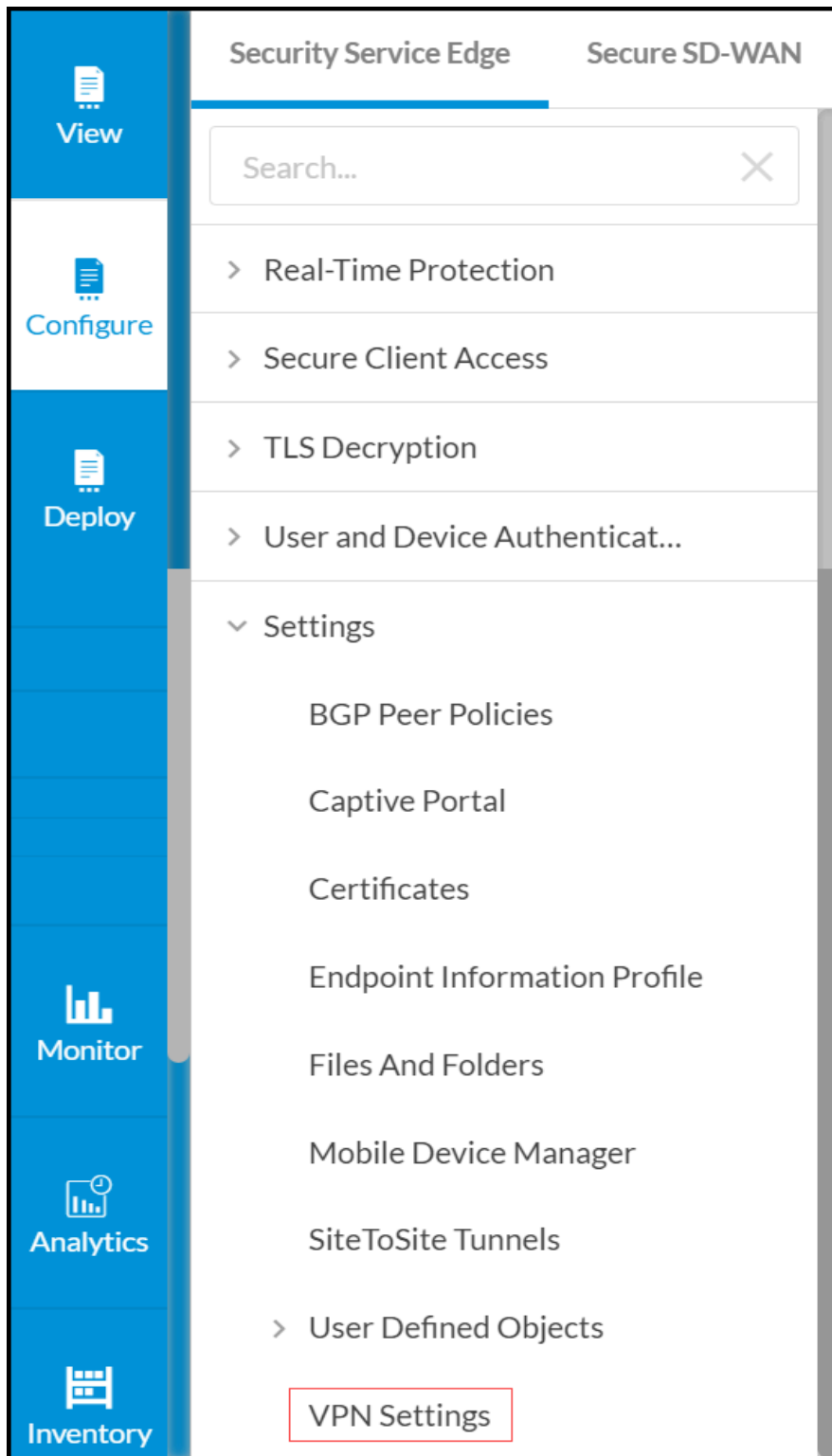# Configure Detection of Trusted Networks for SASE Gateways

For supported software information, click here.

When you connect a device to a trusted network and connect an edge device to a SASE gateway using an IPsec tunnel or a SD-WAN tunnel, you do not need to establish an IPsec tunnel connection to the SASE gateway for a SASE client. You can enable trusted-network detection to perform gateway-assisted trusted-network detection. You must configure trusted-network detection after you configure secure client access profile rules. Otherwise, you need to enable it manually.

To enable trusted-network detection:

1. Go to Configure > Settings > VPN Settings.

2. In the VPN Settings screen, click the name of a VPN.

3. Click the slider to enable or disable trusted-network detection, and then click Save.

4. Click Publish.

5. In the Publish Status screen, select the gateway, and then click Publish.

Supported Software Information

Releases 11.4.1 and later support all content described in this article.

Additional Information

Configure SASE Secure Client Access Rules