Understand Secure Web Gateway Connection Methods

Contents

Introduction

This document describes four methods when deploying SWG to forward and transport web traffic to Umbrella.

Background Information

There are a number of different ways that web traffic can be forwarded and transported to Umbrella. This document contains a list of the four different methods you can consider when deploying your Secure Web Gateway (SWG). When troubleshooting your SWG web policies, you need to indicate which method of connection you are using for web traffic forwarding.

Sending Web Traffic to Umbrella

- Edge device tunnels (IPSec tunnels): Umbrella supports IKEv2 IPSec tunnels for web traffic forwarding. You can find instructions on IPSec Tunnels here: Supported IPSec Parameters.
- Proxy Chaining: You can use proxy chaining in your environment for easier migration or proxy transparency. Instructions on how to manage proxy chaining can be found here: Manage Proxy Chaining.
- PAC File: The Proxy Auto-Config files are another traditional SWG traffic forwarding methods. They are used to configure browsers to send traffic to SWG proxies. If PAC is used with direct network access the company needs to have stable/static external IPs, so it is be possible to create network policies. Click here for instructions on how to deploy Umbrella's PAC file: Manage Umbrella's PAC File.
- AnyConnect SWG Agent: The Cisco Anyconnect client can now redirect HTTP(s) traffic to SWG proxies. The SWG traffic redirect function is supported in Anyconnect in Windows and Mac versions, and instructions can be found here: Enable the AnyConnect SWG Agent.

Want to learn more? Check out our tutorials: Overview of Deployment via Tunnels, PAC File Deployment, and AnyConnect SWG Deployment.