Configure SWG to Avoid Conflicts with SSL VPN Traffic

Contents

Introduction

This document describes how to resolve incompatibility issues between Secure Web Gateway (SWG) and SSL VPNs using intercepted ports.

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.

Problem

Umbrella SWG for AnyConnect can encounter incompatibility issues with certain SSL VPNs that use ports intercepted by the SWG agent, such as TCP 443. AnyConnect SWG can fail to activate and apply coverage reliably. Network reliability can degrade or become unavailable when SWG is active and VPN traffic passes through SWG. Non-web traffic is dropped in this scenario. This issue affects all SSL VPNs using ports 80 and 443.

Solution

To prevent SWG from intercepting VPN traffic, configure a bypass for your VPN domains and IP addresses:

1. In the Umbrella dashboard, navigate to **Access Deployments > Domain Management > External Domains**.

2. Add the domain and IP address of your VPN head end servers to the **External Domains** list. The IP entry ensures that VPN traffic is never intercepted by the SWG agent due to the large number of connections.

3. Allow one hour for the new setting to propagate.

To use SSL VPN with SWG:

1. Add the VPN domain to the **External Domains** list.

2. If the VPN head end domain is a DNS Search Suffix, the client automatically adds this domain for the duration of the connection.

3. Add the VPN head end IP addresses or IP range to the **External Domains** list.