Understand how SWG Proxy Handles Non-Standard HTTPS Requests

Contents

Introduction

This document describes how SWG Proxy processes non-standard HTTPS requests and outlines required client compliance.

Overview

Umbrella relies on the TLS SNI extension to discover the destination domain and determine if an HTTPS request requires decryption or bypass from decryption using Selective Decryption Lists. The client must comply with TLS standards as defined in relevant RFCs. Most well-known browsers comply with these standards and Umbrella supports them.

Common Questions

Can SWG Proxy Process Non-Standard HTTPS Web Requests?

No. The HTTPS request fails if the client does not perform a basic TLS handshake. For example, if the Client Hello or Server Hello exchange is missing, the request cannot complete.

Can Disabling HTTPS Inspection or Adding the Domain in Question to Selective Decryption List Help?

No, these actions do not resolve the issue.

Solution

You must bypass the SWG Proxy completely for the non-standard HTTPS site in question.