# Understand SWG Traffic Decryption with Enabled HTTPS Decryption

## Contents



## Introduction

This document describes how Cisco Secure Web Gateway (SWG) handles traffic decryption when HTTPS decryption is enabled.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on Cisco Secure Web Gateway.

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

In a web policy rule set  with HTTPS decryption enabled, traffic is decrypted only if a Server Name Indicator (SNI) is present in the TLS handshake.

## Solution

Security and Acceptable Use Policies can still be applied based on the destination servers where the request is being sent to. Destination lists can be created for these destination servers and rules can be enforced accordingly.

Any blocks for DNS policies for Tunnels and AnyConnect can still apply.

## Cause

This behavior is by design.