Resolve Missing SWG Traffic on the Umbrella Dashboard

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Problem

Solution

Cause

Introduction

This document describes why traffic from a new Secure Web Gateway (SWG) connection can be missing from the Umbrella dashboard.

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

After setting up an SWG connection, you can observe that traffic does not appear in the activity search on the Umbrella dashboard. Traffic remains protected, but visibility is delayed.

Solution

1. Wait up to 2 hours for the new identity's activity to appear on the Umbrella Dashboard.

2. If traffic does not appear after 2 hours:

- Submit a ticket to Cisco Umbrella Support.
- Include the diagnostic result from tests found at: Troubleshooting Umbrella Secure Web Gateway: Policy Debug and Diagnostic Tests.

Cause

Newly created identities, such as Network Tunnels and AnyConnect SWG clients, can take time to initiate activity in the database for the first time. This process typically takes up to 2 hours.

CDFW traffic does not experience this restriction, and firewall-related traffic appears almost immediately.