Understand Unidentified Requests in Umbrella Reports

Contents

Introduction

This document describes what Unidentified Requests are in Reports in Cisco Umbrella.

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.

Overview

Looking at the **Activity Search** report or **Top Identities** in the **Overview** section of the Umbrella dashboard, you see **Unidentified Requests** and want to know how to get more information about them.

Explanation

Unidentified Requests are DNS requests that were sent to a Virtual Appliance, but not associated with any Active Directory identity (User/Group/Computer) or Internal Network in your account.

A common case is that you can have Wi-Fi access for Guest or Internal purposes where smartphones and other non-AD devices are using the Virtual Appliance(s) for DNS resolution.

The best way to identify non-AD devices is to register Internal Network IPs or IP ranges to compliment the Active Directory aspect of the deployment. This way, if there is no AD identity associated with the DNS request, you can label the requests by Internal IP address.