Resolve User-IP VA Mappings Jumping Across IPs

Contents

Introduction

This document describes how to resolve user-IP Cisco Umbrella Virtual Appliance (VA) mappings jumping across IPs.

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 is unable to identify end-users properly, and it looks as though the mappings are jumping across IP addresses.

Solution

The solution is to simply exclude shared systems from the Connector by their IP address so that it does not push these events to the appliances. In the Umbrella dashboard under **Deployments > Configuration > Service Account Exceptions**, add the appropriate exception as an IP address.

IP mappings can be cleared from each Virtual Appliance using `config admap` as described in the Umbrella Virtual Appliance Commands knowledge base article.

Cause

Each Virtual Appliance builds a table of mappings between users, machines, and their known IP addresses. It has a function that can "collapse" entries in this table if it sees logon events common across more than one IP. In cases where shared systems generate a large number of logon events across multiple users, those collapsed entries can "drift" their assignment to different users unexpectedly.