Prevent Outbound NetBIOS Traffic to OpenDNS

Contents

Introduction

This document describes how to stop outbound NetBIOS traffic directed to OpenDNS.

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

Windows systems can attempt to send NetBIOS traffic to OpenDNS when OpenDNS returns the IP address of a controlled host instead of a standard NXDOMAIN response. Windows interprets this as a valid response and initiates NetBIOS communication with OpenDNS.

Solution

To prevent outbound NetBIOS traffic to OpenDNS, complete these steps:

1. Access the **Advanced Settings** in your dashboard.

2. Navigate to **Domain Typos > Exceptions for VPN users**.

3. Add the full hostnames of systems on your network to the exceptions list.

Hostnames added to this list do not get looked up by OpenDNS services.