Understand Umbrella and Your MTA Email Server

Contents

Introduction

This document describes advice against using Umbrella filtering by an MTA (Mail Transfer Agent) that is handling email.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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

Currently, we do not recommend that Cisco Umbrella filtering be used by a Mail Transfer Agent (MTA) that is handling email. It is not a supported configuration and **unexpected results can occur.**

Explanation

There are several reasons to avoid using Umbrella filtering on your MTA. These are briefly covered here:

- Categorization filtering rules can block legitimate mail. For example, an email to user@facebook.com is blocked if the social media category is not allowed. The mail delivery can be legitimate, but you want to block employees from using Facebook.

- Security filtering: domains can be blocked for a Security Threat. However, email is still desired to be sent to this domain. This can occur when a site is temporarily compromised and is flagged for
- Malware but still needs to have mail send to its domain.
  Due to the large number of queries that can occur from our DNS resolvers, some DNSBLs do not allow queries from us. This can potentially affect your spam catch rate.

Solution

Unfortunately, due to the way our services interact with MTAs, there currently is no solution for them benefiting from our protective services. As such, you could have them assigned to an identity in your policies that has no filtering, utilize your ISPs or another DNS service.

Useful Links

Exchange 2010
This article (step 6) deals with the configuration of DNS in Exchange 2010:

Exchange 2007

Exchange 2003