了解Umbrella和您的MTA电子邮件服务器

目录

简介

本文档介绍有关防止处理电子邮件的MTA（邮件传输代理）使用Umbrella过滤的建议。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

目前，我们不建议处理电子邮件的邮件传输代理(MTA)使用Cisco Umbrella过滤。此配置不受支持，可能会出现意外结果。

说明

有几个原因可以避免在MTA上使用Umbrella过滤。下面将简要介绍以下内容：

- 分类过滤规则可以阻止合法邮件。例如，如果不允许使用社交媒体类别，则发送到user@facebook.com的电子邮件将被阻止。邮件传送可能是合法的，但您希望阻止员工使用Facebook。

- 安全筛选:可以阻止域来应对安全威胁。但是，仍希望向此域发送电子邮件。当站点暂时受到危害并被标记时，可能会出现这种情况
- 恶意软件，但仍需要将邮件发送到其域。
  由于我们的DNS解析器可能会发生大量查询，某些DNSBL不允许我们进行查询。这可能会影响您的垃圾邮件捕获率。

解决方案

遗憾的是，由于我们的服务与多机构贸易协定的互动方式，目前没有从我们的保护服务中获益的解决方案。因此，您可以在策略中将它们分配到没有过滤的身份，从而利用您的ISP或其他DNS服务。

实用链接

Exchange 2010
本文（步骤6）介绍Exchange 2010中的DNS配置：

Exchange 2007

Exchange 2003

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。