使用防火墙规则实施Umbrella DNS并阻止旁路

目录

简介

本文档介绍如何使用防火墙规则和网络策略防止DNS旁路和实施Umbrella DNS保护。

先决条件

- 网络防火墙
- 防火墙访问权限
- 防火墙配置知识

实施Umbrella DNS — 最常用方法

大多数路由器和防火墙允许您通过端口53实施所有DNS流量，要求所有网络设备使用路由器上定义的DNS设置，该设置必须指向Umbrella DNS服务器。

首选方法是将来自非Umbrella IP地址的所有DNS请求转发到下面列出的Umbrella DNS IP。此方法以透明方式转发DNS请求，并防止手动DNS配置简单失败。

或者，创建防火墙规则以仅允许Umbrella DNS服务器的DNS(TCP/UDP)并阻止所有其他DNS流量发送到任何其他IP地址。

防火墙规则示例

1. 将此规则添加到边缘防火墙：

- 允许TCP/UDP入站和出站到208.67.222.222端口53208.67.220.220或端口53。
- 阻止端口53上所有IP地址的TCP/UDP入站和出站。

Umbrella DNS的允许规则优先于阻止规则。允许向Umbrella发出DNS请求，而阻止所有其他DNS请求。

根据您的防火墙配置接口，为每个协议配置单独的规则，或为TCP和UDP配置一条规则。在网络边缘设备上应用规则。您还可以将类似的规则应用于工作站上的软件防火墙，例如Windows或macOS中的内置防火墙。

如果使用漫游客户端和Active Directory组策略，请参阅有关使用组策略锁定企业漫游客户端的文档。

通过HTTPS实施DNS(DoH)

建议的配置

1. 在Umbrella中，启用Proxy/AnonymizerandDoH/DoTcontent类别。
2. 在防火墙上阻止已知DoH提供商的IP地址。

详细信息和背景

Umbrella支持use-application-dns.netMozilla定义的域，以防止Firefox在默认情况下启用DoH。有关Firefox和DoH的信息，请参阅相关文档。

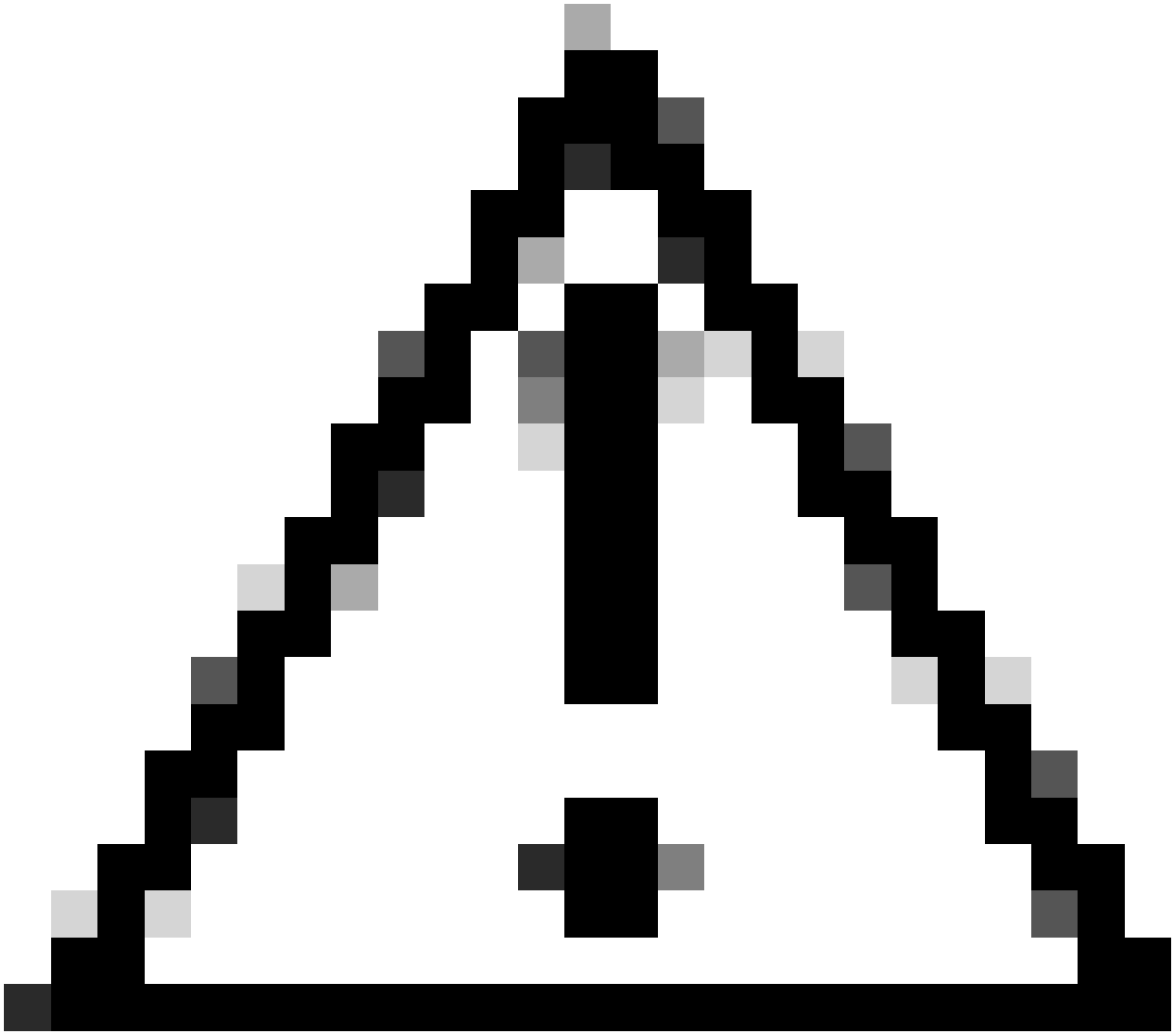
即使在阻止备用DNS提供商后，DNS仍然可以通过DoH绕过。本地DNS解析器将DNS请求转换为HTTPS并使用JSON或POST/GET将其发送到终端。此流量通常可避免DNS检测。

由于DoH可用于绕过Umbrella，因此Umbrella在Proxy/Anonymizer内容类别中包括已知的DoH服务器。此机制有一些限制：

- 它无法阻止尚不了解的全新DoH提供商。
- 它无法阻止通过IP地址直接使用的DoH。

要解决新的DoH提供程序，请监控更新并阻止新发现的域，以扩大覆盖范围。

对于通过IP地址的DoH，场景有限。采用CloudFlare的Firefox就是一个突出的例子。



警告：请勿将Mozilla Kill Switch域添加到阻止列表。阻止这些域将导致阻止页面的A记录，Firefox将此视为有效并自动升级其DoH使用。

通过TLS实施DNS(DoT)

即使在阻止备用DNS提供程序和DoH之后，DNS也可以通过TLS进行绕过，TLS在端口853上使用RFC7858。例如，CloudFlare是DoT提供程序。

实施示例

- 阻止IP地址1.1.1.1,1.0.0.1在端口853(CloudFlare)上。

防火墙支持免责声明

本文档帮助网络管理员实施Umbrella DNS。Cisco Umbrella支持不提供个别防火墙或路由器配置方面的帮助，因为每个设备都有唯一的配置接口。查阅路由器或防火墙文档，或者联系设备制造商确

认是否有可能进行这些配置。

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）。