

配置私有ChatGPT并限制对其他生成AI应用的访问

目录

[简介](#)

[概述](#)

[步骤 1：创建允许私有ChatGPT的Web规则](#)

[步骤 2：阻止所有其他生成AI应用](#)

[DNS策略](#)

[Web策略](#)

简介

本文档介绍如何配置私有ChatGPT并限制对其他生成AI应用的访问。

概述

人工智能领域正在迅速发展，其中最突出的进步就是生成式AI。其中，ChatGPT产生了重大影响。随着组织试图将这些功能强大的工具集成到工作流程中，控制对生成AI应用的访问的需求日益明显。对于已开发自己的私有ChatGPT实例的企业而言，确保这是其团队能够访问的唯一AI工具，同时限制其他Generated AI应用，是一项关键的安全措施。

幸运的是，有直接的方法可以使用Umbrella控制面板实现这一点。本文会引导您完成您需要采取的步骤，以使您的组织从您的私有ChatGPT中获益，同时保持对其他AI应用使用的严格控制。

步骤 1：创建允许私有ChatGPT的Web规则

首先，您需要登录到您的Umbrella控制面板。之后，您可以创建DNS规则或Web规则。此规则必须具有“允许”(Allow)操作和“目标列表”(Destination List)，其中包含您的私有ChatGPT的特定URL。此步骤可确保您组织内的用户能够不受任何限制地访问您的私有ChatGPT。

步骤 2：阻止所有其他生成AI应用

创建“允许”规则后，必须立即创建第二个规则。此规则必须具有“阻止”(Block)操作，并且必须包括包含生成AI类别的“应用列表”(Application List)。这样，您就可以阻止访问各种流行的生成AI应用，包括ChatGPT的公共版本。

DNS策略

为确保这些规则在使用DNS策略而不是Web策略时得到有效实施。

启用智能代理和SSL解密以实现无缝体验至关重要。此外，安装Cisco Umbrella根证书对于SSL解密正常运行是必需的。

有关设置DNS策略的全面指导，请参阅此处的官方[文档](#)。

此外，要优化DNS策略的有效性，请在此处查看最佳[实践](#)。

Web策略

有关管理Web策略并根据组织的要求定制这些策略的更多详细信息，请访问[此链接](#)。

通过实施这些措施，您的组织可以充分利用您的私有ChatGPT，同时降低使用其他生成AI应用时可能带来的数据泄露或干扰的风险。正确平衡安全性和可访问性是充分利用生成AI的潜力同时确保组织数据和资源得到良好保护的关键。

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）。