Configure Private ChatGPT and Restrict Access to Other Generative AI Apps

Contents

Introduction

This document describes how to configure a private ChatGPT and restrict access to other generative AI apps.

Overview

The landscape of artificial intelligence is rapidly evolving, and one of the standout advancements has been the development of Generative AI. Among these, ChatGPT has made a significant impact.
As organizations seek to integrate these powerful tools into their workflows, the need for controlling access to Generative AI applications has become increasingly evident. For businesses that have developed their own private ChatGPT instances, ensuring that this is the only AI tool accessible to their team while restricting other Generative AI apps, is a critical security measure.

Fortunately, there is a straightforward way to achieve this using the Umbrella dashboard. This article walks you through the steps you need to take to allow your organization to benefit from your private ChatGPT while maintaining strict controls over the use of other AI applications.

Step 1: Create a Web Rule to Allow Your Private ChatGPT

Firstly, you need to log in to your Umbrella dashboard. Once there, you can create a DNS rule or a web rule.

This rule must have the action "Allow" and a Destination List" with the specific URL of your private ChatGPT.
This step ensures that users within your organization can access your private ChatGPT without any restrictions.

Step 2: Block All Other Generative AI Apps

Immediately after the creation of the 'Allow' rule, you must create a second rule.
This rule must have the "Block" action and must include an "Application List" that encompasses the Generative AI category.
By doing so, you are able to prevent access to a wide array of popular Generative AI applications, including the public version of ChatGPT.

DNS Policy

To ensure these rules are effectively enforced when using the DNS policy and not the Web policy.
It is crucial to enable the intelligent proxy and SSL decryption for a seamless experience. Additionally, the installation of the Cisco Umbrella root certificate is necessary for the proper functioning of the SSL decryption.

For comprehensive guidance on setting up the DNS policy, you can refer to the official documentation here.
Additionally, to optimize the effectiveness of your DNS policies, check out the best practices here.

Web Policy

For more details on managing web policies and tailoring them to meet your organization's requirements, head over here.

Implementing these measures allows your organization to take full advantage of your private ChatGPT while mitigating the risk of data leakage or distractions that can come with the use of other Generative AI apps. The right balance of security and accessibility is key to harnessing the potential of Generative AI while ensuring your organization's data and resources are well-protected.