

Configuración de ChatGPT privado y restricción del acceso a otras aplicaciones de IA generativa

Contenido

[Introducción](#)

[Overview](#)

[Paso 1: Crear una regla web para permitir su chat privadoGPT](#)

[Paso 2: Bloquear todas las demás aplicaciones de IA generativa](#)

[Política de DNS](#)

[Política web](#)

Introducción

Este documento describe cómo configurar un ChatGPT privado y restringir el acceso a otras aplicaciones generativas de IA.

Overview

El panorama de la inteligencia artificial está evolucionando rápidamente, y uno de los avances más destacados ha sido el desarrollo de la IA generativa. Entre ellos, ChatGPT ha tenido un impacto significativo.

A medida que las organizaciones buscan integrar estas potentes herramientas en sus flujos de trabajo, la necesidad de controlar el acceso a las aplicaciones de IA generativa se ha hecho cada vez más evidente. Para las empresas que han desarrollado sus propias instancias privadas de ChatGPT, garantizar que esta es la única herramienta de IA accesible para su equipo, mientras que la restricción de otras aplicaciones de IA generativa, es una medida de seguridad crítica.

Afortunadamente, existe una forma sencilla de conseguirlo mediante el panel Umbrella. Este artículo le guía a través de los pasos que debe seguir para permitir que su organización se beneficie de su ChatGPT privado mientras mantiene estrictos controles sobre el uso de otras aplicaciones de IA.

Paso 1: Crear una regla web para permitir su chat privadoGPT

En primer lugar, debe iniciar sesión en el panel de Umbrella. Una vez allí, puede crear una regla DNS o una regla Web.

Esta regla debe tener la acción "Permitir" y una "Lista de Destino" con la URL específica de su ChatGPT privado.

Este paso garantiza que los usuarios de su organización puedan acceder a su ChatGPT privado sin ninguna restricción.

Paso 2: Bloquear todas las demás aplicaciones de IA generativa

Inmediatamente después de la creación de la regla 'Permitir', debe crear una segunda regla. Esta regla debe tener la acción "Bloquear" y debe incluir una "Lista de aplicaciones" que abarque la categoría AI generativa.

De esta manera, puede evitar el acceso a una amplia gama de aplicaciones de IA generativa populares, incluida la versión pública de ChatGPT.

Política de DNS

Para garantizar que estas reglas se aplican de forma eficaz cuando se utiliza la directiva DNS y no la directiva Web.

Es fundamental habilitar el proxy inteligente y el descifrado SSL para lograr una experiencia sin problemas. Además, la instalación del certificado raíz de Cisco Umbrella es necesaria para el correcto funcionamiento del descifrado SSL.

Para obtener una guía completa sobre la configuración de la política de DNS, puede consultar la documentación oficial [aquí](#).

Además, para optimizar la eficacia de las políticas de DNS, consulte las prácticas recomendadas [aquí](#).

Política web

Para obtener más información sobre la gestión de políticas web y su adaptación para satisfacer los requisitos de su organización, diríjase [aquí](#).

La implementación de estas medidas permite que su organización aproveche al máximo su ChatGPT privado al tiempo que mitiga el riesgo de filtración de datos o distracciones que pueden venir con el uso de otras aplicaciones de IA generativa. El equilibrio adecuado entre seguridad y accesibilidad es clave para aprovechar el potencial de la IA generativa y, al mismo tiempo, garantizar que los datos y recursos de su organización están bien protegidos.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).