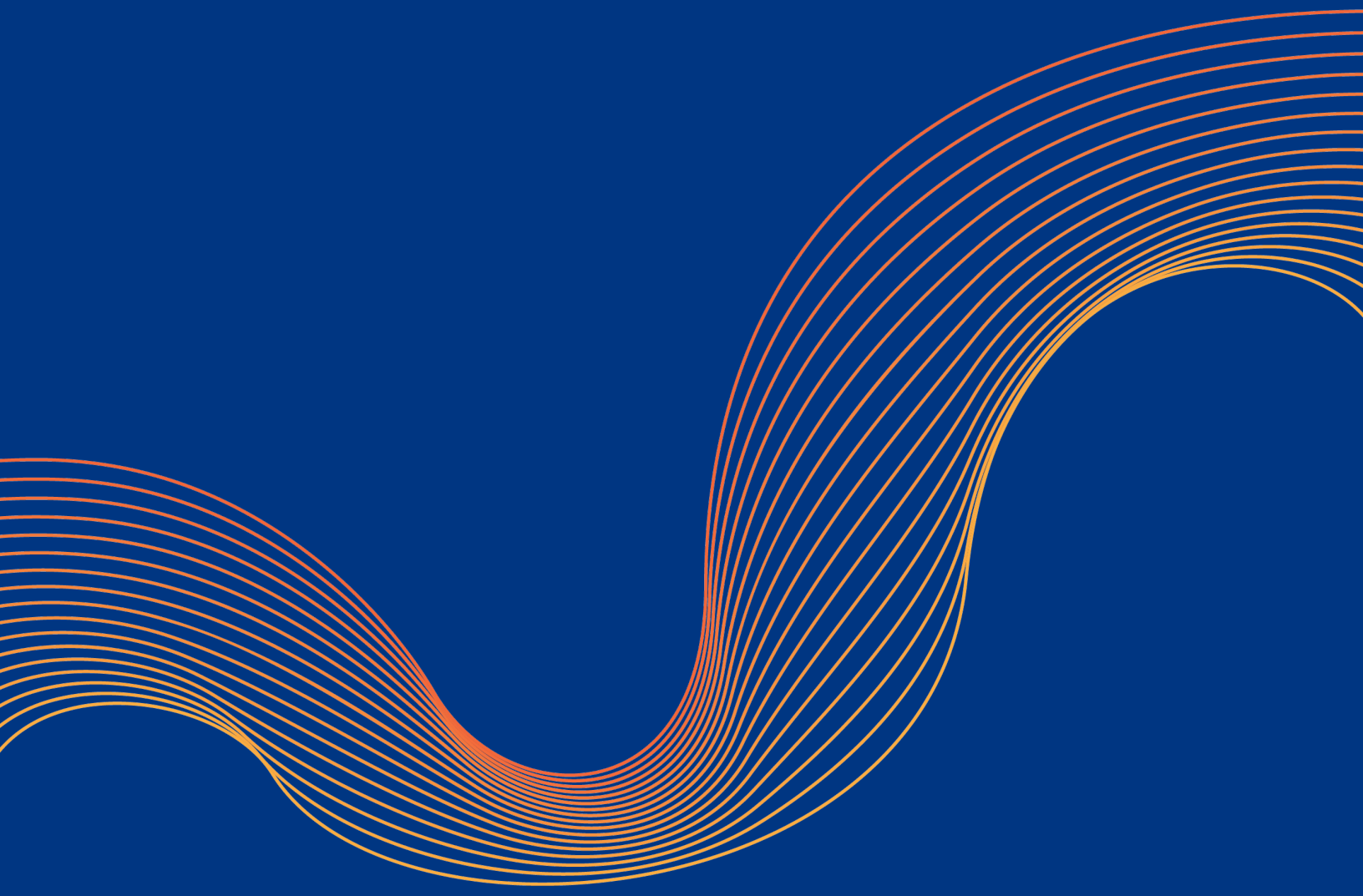
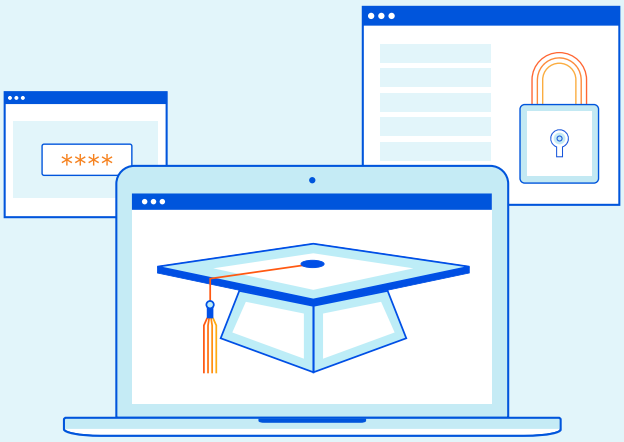
DOCUMENTO TÉCNICO

CLOUDFLARE

Cómo desarrollar una infraestructura segura y escalable para la educación a distancia



+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/



Introducción

En los últimos años, la educación a distancia se ha convertido en un modelo educativo cada vez más extendido. La pandemia de la COVID-19, que obligó a muchas instituciones a iniciar un proceso de transición hacia la teleeducación para evitar contagios entre estudiantes y profesores, aceleró la transformación a modelos de enseñanza híbrida y totalmente a distancia.

La educación a distancia requiere un enfoque muy diferente al de la enseñanza presencial convencional. Los docentes necesitan la capacidad de ofrecer una variedad de estilos de aprendizaje y tipos de contenido, tales como conferencias, vídeos, contenido interactivo, entre otros. En lo que respecta a la educación a distancia, todos los alumnos del aula deben poder acceder rápida y simultáneamente al contenido compartido.

Desde el punto de vista técnico, un centro educativo tiene que ser capaz de ofrecer esta amplia variedad de tipos de contenido y garantizar el funcionamiento de los sistemas cuando los estudiantes los necesiten.
Para ello es necesario abordar una serie de cuestiones, entre las que se incluyen:

- Capacidad de ofrecer contenidos a escala
- Mitigación de ataques de denegación de servicio distribuidos
- Soluciones para impedir la apropiación fraudulenta de cuentas
- Soluciones para detener los contenidos maliciosos y el *malware*

Capacidad de ofrecer contenidos a escala

La educación a distancia convierte la infraestructura informática de los centros educativos en un componente vital de la capacidad de funcionamiento de la organización. Los docentes necesitan poder ofrecer contenidos a muchos estudiantes simultáneamente, garantizando al mismo tiempo que les llegan con una latencia mínima.

Es necesario que los profesores puedan ofrecer una amplia variedad de contenidos a sus alumnos. Pueden ser tanto páginas web estáticas como contenidos dinámicos, incluidas herramientas interactivas de aprendizaje en línea y vídeos en tiempo real. La infraestructura informática de un centro de enseñanza debe ser capaz de ofrecer este contenido a sus estudiantes a distancia de forma eficiente y escalable.

Contenido estático

Algunos de los contenidos que los profesores deben proporcionar a sus alumnos son estáticos, como páginas web en las que la información incluida en la página no cambia y no requiere actualizaciones frecuentes.

Los principales desafíos informáticos asociados a este tipo de contenido son la escalabilidad y la latencia. Si muchos estudiantes intentan acceder al mismo contenido a la vez, ¿tendrá el servidor web capacidad de respuesta? Además, la ubicación del servidor web puede ser una cuestión muy importante para la educación a distancia. Cuanto más lejos esté el estudiante del servidor, mayor será la latencia de entrega del contenido.

En el caso de los contenidos estáticos, la capacidad de crear memoria caché local de contenidos puede ayudar a atenuar estos problemas. Si un alumno visita una página concreta con frecuencia, es posible que una copia de esta se almacene de forma local, lo que le permitirá acceder a ella rápidamente cuando la necesite.

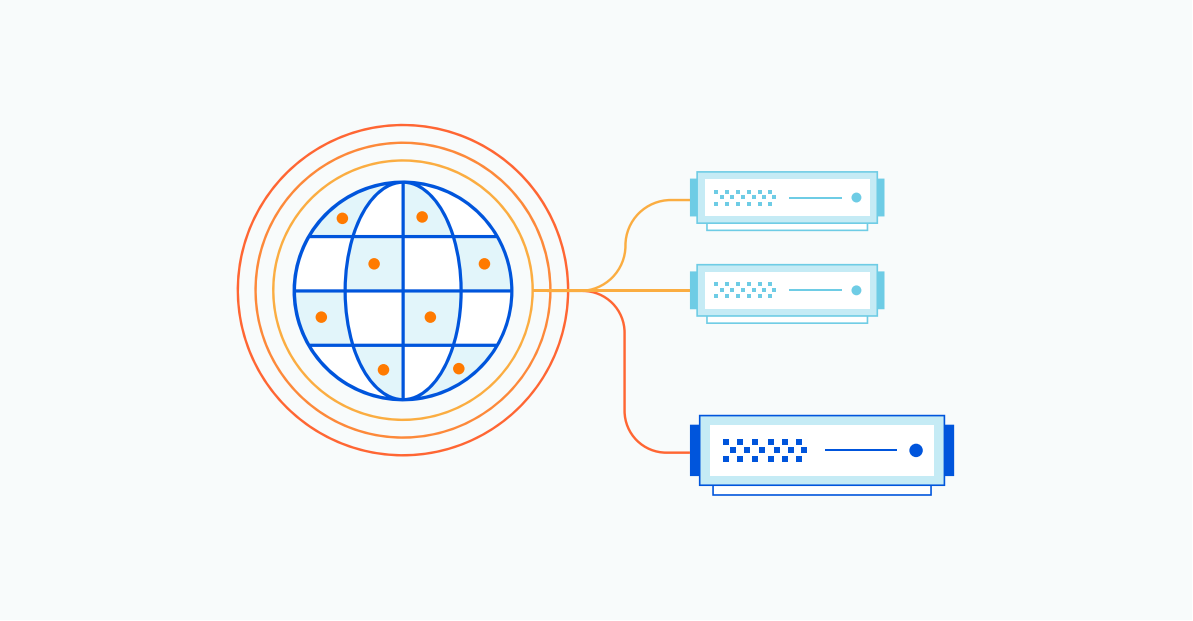
El almacenamiento en caché también se puede implementar a escala utilizando una red de entrega de contenido (CDN). Una CDN consiste en una red de nodos que almacenan copias locales de contenidos estáticos y comprueban las actualizaciones de forma periódica. Una CDN de alcance global ofrece la escalabilidad y la baja latencia necesarias para una enseñanza a distancia eficaz.

Contenido dinámico e interactivo

Al igual que los contenidos estáticos, los contenidos interactivos de aprendizaje en línea y de otro tipo tienen problemas potenciales de escalabilidad. Sin embargo, el uso de una red de nodos de la CDN no funciona tan bien para este tipo de contenidos. Si el contenido requiere actualizaciones frecuentes o casi constantes, los nodos de la CDN estarán consultando continuamente al servidor web principal para obtener una versión actualizada. Este proceso aumenta la latencia de red para los usuarios y puede saturar el servidor web principal.

En cambio, los problemas relacionados con la escalabilidad de los contenidos dinámicos pueden resolverse mediante el equilibrio de carga. En lugar de utilizar un único servidor para responder a las peticiones de los estudiantes, se utilizan varios servidores con el tráfico distribuido entre ellos. Así se garantiza que ningún servidor se sature y se minimiza la latencia.

Para ser eficaz, un servidor de carga equilibrada debe ser capaz de actuar de forma completamente independiente o depender únicamente de otros dispositivos de carga equilibrada. Si todos los servidores están configurados para utilizar el mismo servidor de base de datos, es posible que este se convierta en el cuello de botella y los servidores de carga equilibrada adicionales ofrezcan poco o ningún beneficio. Es preciso diseñar soluciones de educación a distancia cuidadosamente para garantizar que se dispone, en caso necesario, de la escala requerida y que el diseño del sistema brinda todas las ventajas del equilibrio de carga.

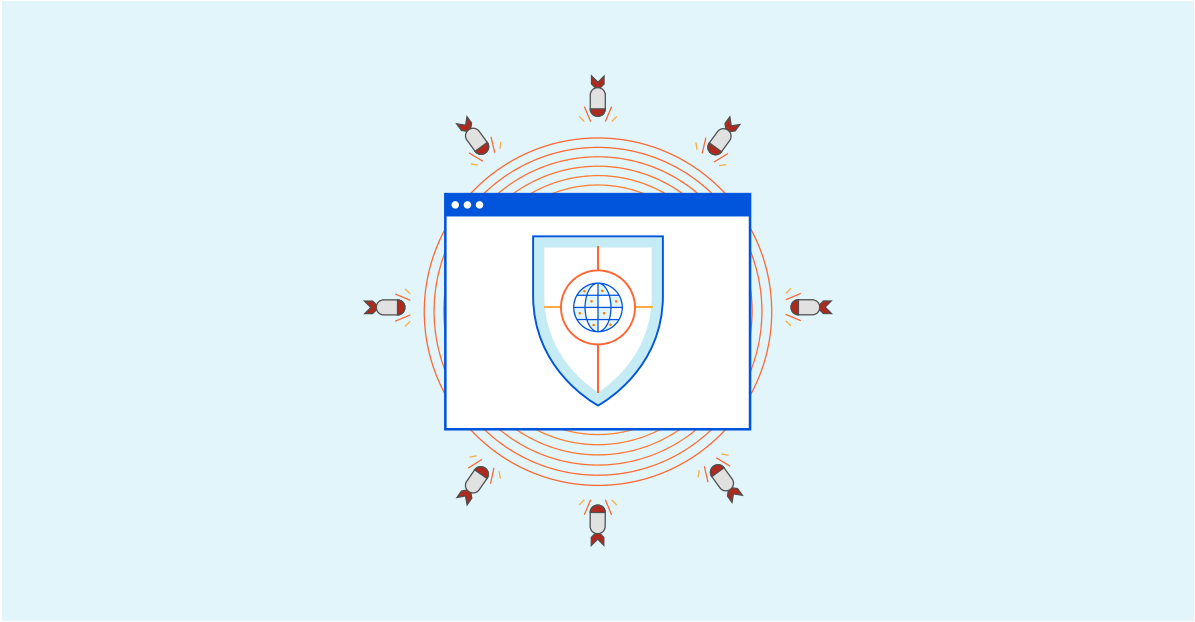


Ataques de denegación de servicio distribuidos

Los ataques de denegación de servicio distribuidos (DDoS) son cada vez más frecuentes. A medida que el Internet de las cosas (IoT) y la computación en la nube se expanden, a los atacantes les resulta más barato y más fácil obtener acceso a los servicios informáticos conectados a Internet. Estos dispositivos en riesgo pueden utilizarse para enviar tráfico malicioso a un servicio, impidiendo que pueda responder a las solicitudes legítimas.

En la educación a distancia, los ataques DDoS plantean un riesgo importante a la capacidad de prestar servicios. En la primera mitad de 2020, cuando muchas organizaciones adoptaron el modelo de educación a distancia, los ataques DDoS contra los recursos educativos en línea aumentaron un 350 %[1].

Además, algunos ataques DDoS han evolucionado para incorporar un componente de rescate. Un atacante puede amenazar a una organización con un ataque DDoS y exigir un rescate para detenerlo. Muchas de estas amenazas son infundadas, pero un centro educativo sin protección DDoS puede considerar que el riesgo para su infraestructura es demasiado grande como para ignorarlo.

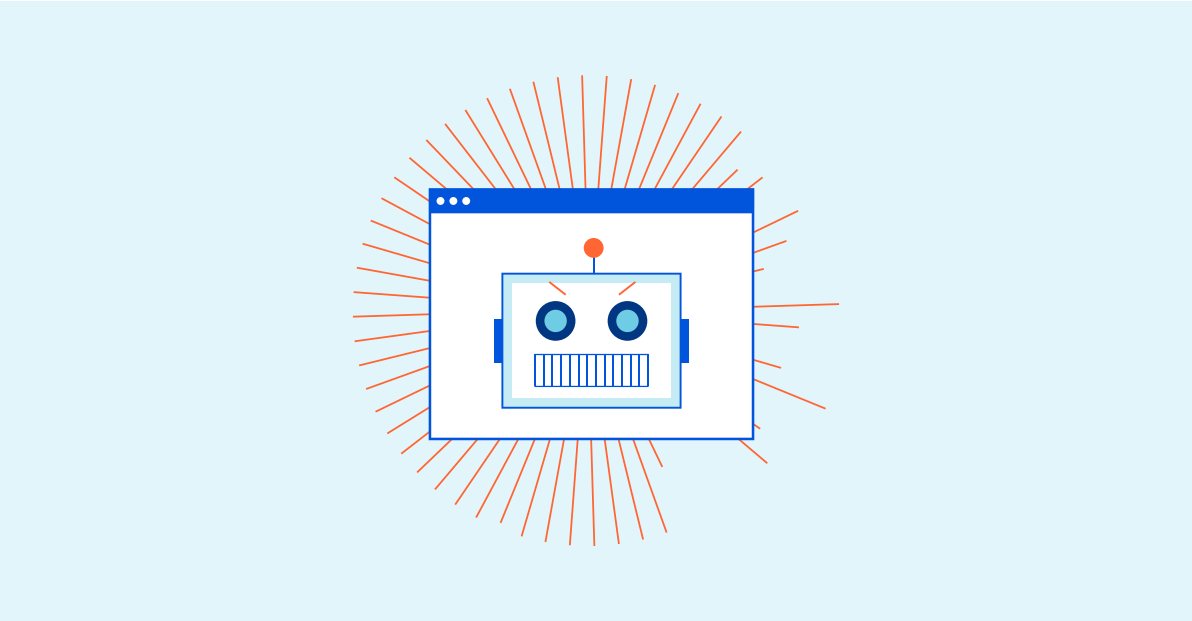


Afortunadamente, incluso las organizaciones educativas con presupuestos comparativamente inflexibles siguen teniendo acceso a una variedad de tácticas efectivas de mitigación de DDoS. Las organizaciones deberían considerar:

- Alta capacidad de mitigación: puede ser tentador pagar solo por la protección que tu organización prevé necesitar, pero si se produce un ataque inesperado a gran escala, el tiempo que se necesita para actualizar tu servicio puede acarrear más tiempo de inactividad.
- Mitigación distribuida: el filtrado del tráfico DDoS debe ser distribuido, ya que enrutar todo el tráfico de una organización a través de un único punto central para el filtrado puede ser poco escalable y aumentar la latencia de la red.
- Protección bajo demanda frente a protección siempre activa: en la mitigación de DDoS bajo demanda, el flujo de tráfico desde la red pública hacia los servidores o la infraestructura de red de una organización es normal hasta que se detecta un posible ataque, momento en el que se inspecciona y filtra con mayor rigor. En cambio, la protección siempre activa filtra continuamente todo el tráfico. Aunque puede ser más cara que los servicios bajo demanda, ofrece una protección ininterrumpida y permite tiempos de respuesta más rápidos, ya que el servicio nunca tiene que ser activado de forma manual.

Si deseas más información sobre las estrategias de mitigación de DDoS, consulta el documento "Five Best Practices for Mitigating DDoS Attacks" (Las 5 mejores prácticas para mitigar los ataques DDoS) en el centro de recursos de Cloudflare.

[1] *https://www.infosecurity-magazine.com/news/ddos-attacks-on-virtual-education/*



Apropiación fraudulenta de cuenta

Muchos ciberataques comienzan con la apropiación de la cuenta de un usuario legítimo en el sistema. Los ataques de apropiación de cuentas comprometen las credenciales de usuarios legítimos en una red, aplicación u otros sistemas. Un atacante puede obtener acceso a las credenciales de la cuenta de diferentes maneras, como por ejemplo ataques de *phishing* y relleno de credenciales.

Con estas credenciales, el atacante puede hacerse pasar por un usuario legítimo y descargar *malware*, robar datos o lograr otros objetivos en el sistema objeto de ataque. Todo ello puede permitir a un atacante acceder a datos protegidos por normativas como la Ley de Protección de la Privacidad Infantil en Internet (COPPA) y la Ley de Derechos Educativos y Privacidad de la Familia (FERPA). Por otra parte, este acceso podría permitir a los atacantes eliminar expedientes escolares críticos o pedir un rescate de *ransomware*.

Los centros de enseñanza deben desarrollar una solución de mitigación del *phishing* capaz de detectar ataques, basándose tanto en el contenido malicioso conocido como en el uso del aprendizaje automático para detectar el lenguaje sospechoso y otras amenazas desconocidas. El escaneo del correo electrónico es uno de estos enfoques. Otro es el uso de una puerta de enlace segura para bloquear sitios maliciosos conocidos y evitar que los usuarios descarguen ciertos tipos de archivos.

Relleno de credenciales

Por otra parte, un atacante puede aprovechar los sistemas de inicio de sesión públicos de una organización, como las redes privadas virtuales (VPN), el protocolo de escritorio remoto (RDP) o los portales de acceso web, para poner en riesgo las credenciales de los usuarios. De media, una persona utiliza las mismas credenciales de inicio de sesión para 13 cuentas en línea[2], y el uso de contraseñas vulnerables y fáciles de adivinar es común. Los ataques de relleno de credenciales utilizan bots automatizados para intentar adivinar la contraseña de un usuario en estos portales de autenticación. Si lo consigue, el atacante obtiene acceso a la cuenta del usuario legítimo porque ahora conoce sus auténticas credenciales de inicio de sesión.

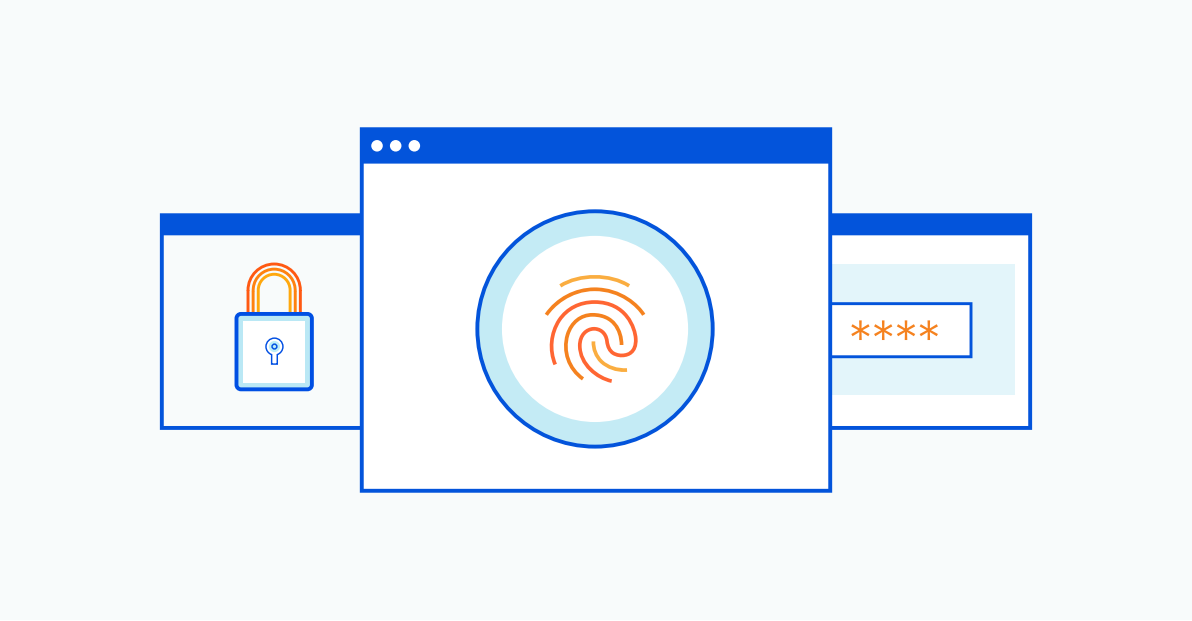
[2] *https://www.lastpass.com/state-of-the-password/global-password-security-report-2019*

Los ataques de relleno de credenciales se aprovechan de la automatización. La protección contra este tipo de ataques requiere soluciones de detección de bots. Sin embargo, también es vital diferenciar entre los bots buenos y los malos.

Los bots pueden detectarse y bloquearse a través de diferentes métodos. Entre los elementos básicos de una estrategia de mitigación de bots maliciosos se incluyen:

- **Limitación de velocidad,** es decir, limitar el número de veces que una dirección IP puede enviar solicitudes a su sitio o red. Esta estrategia es más eficaz para los ataques de bots más simples y por fuerza bruta.
- **CAPTCHA y autenticación en dos fases:** ambas tácticas pueden evitar que muchos bots puedan acceder a las páginas de inicio de sesión. Sin embargo, también pueden afectar negativamente a la experiencia del usuario.
- **Mantener una lista de bloqueo de bots y una lista de permitidos** para hacer un seguimiento de los bots maliciosos conocidos, y garantizar que los rastreadores de los motores de búsqueda y otros bots buenos puedan seguir realizando sus tareas.

Sin embargo, puede que estas estrategias no sean tan eficaces para los bots más desarrollados y especializados. Para obtener más información sobre la mitigación de bots, consulta "Malicious Bot Playbook" (Manual de bots maliciosos) en el centro de recursos de Cloudflare.

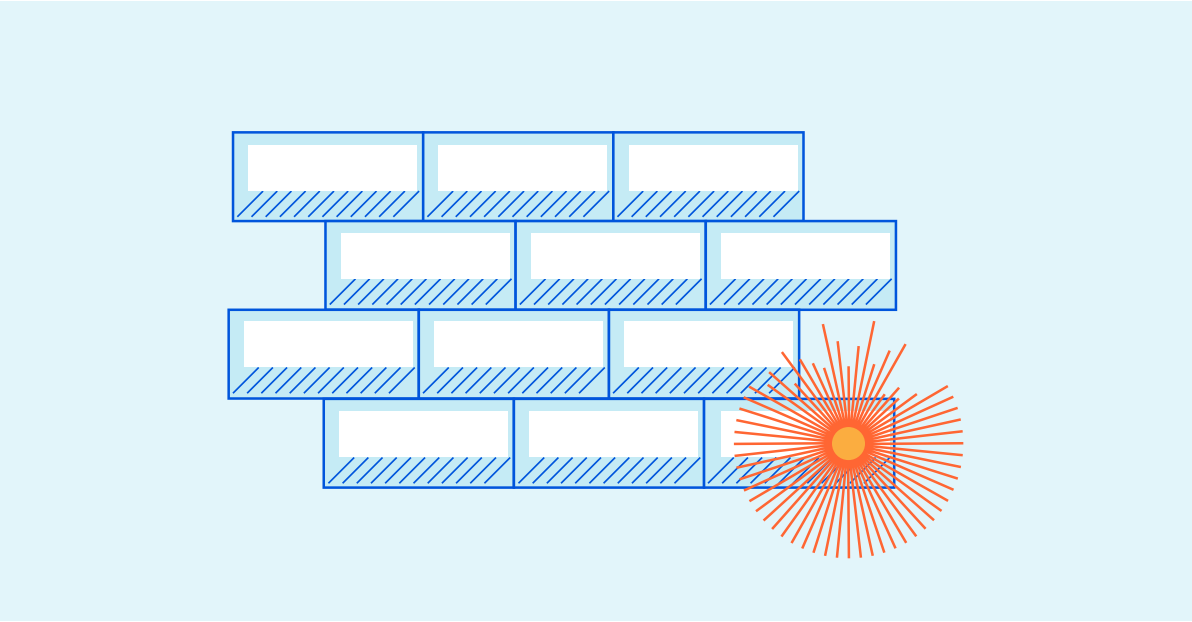


Contenido malicioso y *malware*

A medida que los docentes adoptan el sistema de educación a distancia, un número cada vez mayor de sistemas quedará expuesto a la red pública. Los alumnos pueden aprovechar el aprendizaje en línea a través de aplicaciones web. Los estudiantes y profesores a distancia también pueden tener acceso remoto a la red y a los ordenadores mediante las VPN, el RDP y soluciones similares. Estos sistemas también deben estar protegidos contra las ciberamenazas.

Seguridad de aplicaciones web

Las aplicaciones web educativas pueden tener acceso a una amplia variedad de datos confidenciales. Los datos de los estudiantes con arreglo a la COPPA, la FERPA y otras legislaciones similares pueden almacenarse en estas plataformas, por lo que es vital que los centros educativos las protejan adecuadamente.



Estas aplicaciones son *software* propiamente dicho, por lo que podrían estar expuestas a vulnerabilidades. Con el fin de proteger estas aplicaciones contra los ciberataques es necesario inspeccionar el tráfico de la red para detectar y bloquear los intentos de aprovechar estos fallos de *software*.

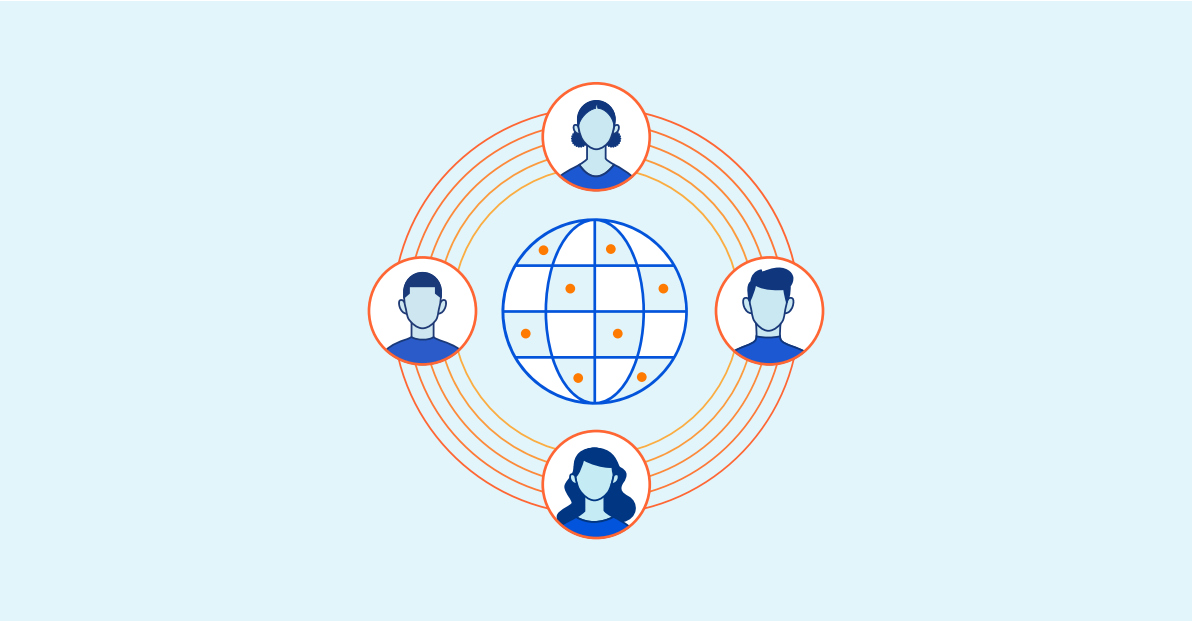
Un servicio de WAF (web application firewall) brinda protección contra una amplia variedad de vulnerabilidades de las aplicaciones web. Puede utilizar una combinación de detección basada en firmas y aprendizaje automático para identificar tanto ataques conocidos como nuevos. Este enfoque permite una protección incluso contra los ataques de día cero en la infraestructura basada en la web de una organización.

Protección contra el *ransomware*

El *ransomware* es uno de los tipos de *malware* de mayor crecimiento. Una vez que el *ransomware* tiene acceso a un equipo, cifra los archivos almacenados en él y exige un pago para restablecer el acceso. Incluso aunque el centro educativo pueda pagar inmediatamente el rescate, el tiempo y el gasto necesarios para restablecer los sistemas afectados pueden ser significativos.

El *ransomware* se distribuye cada vez más a través de tecnologías de acceso remoto, tales como las VPN y el RDP. Un atacante con acceso a las credenciales de inicio de sesión legítimas puede utilizarlas para iniciar sesión en un ordenador e instalar *malware* en él. Una vez dentro de la red de la organización, el *malware* suele propagarse para infectar otros equipos de la red.

Los centros de enseñanza necesitan una solución de *firewall* que les permita inspeccionar todo el tráfico de la red de la organización. De esta manera podrán detectar el contenido malicioso entrante (como el *ransomware*) antes de que infecte los ordenadores de la organización y bloquear los intentos de exfiltración de datos (incluidos los datos personales protegidos de los alumnos).



Cómo garantizar la educación a distancia con Cloudflare

Si bien la pandemia de la COVID-19 se superará, la capacidad para gestionar fácilmente la transición a la educación a distancia es un complemento valioso para una institución educativa. Los recursos de aprendizaje en línea son también un activo útil para la educación presencial, y contar con la infraestructura necesaria para facilitar la enseñanza a distancia permite a una organización ser capaz de hacer frente a interrupciones causadas por las inclemencias del tiempo y otros eventos imprevistos.

Cloudflare ofrece una plataforma consolidada y sencilla con soluciones para todos los desafíos informáticos y de seguridad más comunes de los centros educativos. Al aprovechar una solución única e integrada como la de Cloudflare, los centros de enseñanza evitan la complejidad innecesaria y se vuelven más adaptables y resistentes a escenarios inesperados. La oferta de Cloudflare incluye:

- **Una red global de entrega de contenido**, con centros de datos en más de 200 ciudades del mundo.
- **47 Tbps de capacidad de mitigación de DDoS**, con una mitigación siempre activa en el perímetro de la red.
- **Una solución WAF**, que aprende continuamente de la información de amenazas de aproximadamente 25 millones de propiedades de Internet en la red de Cloudflare.
- **Mitigación avanzada de bots**, que utiliza el aprendizaje automático y las huellas digitales para analizar los patrones de tráfico en nuestra red y detectar los bots más avanzados.
- **Una puerta de enlace segura,** que opera en el perímetro de la red, reduciendo la latencia que se produce al reenviar el tráfico a un centro de datos geográficamente aislado.

Consulta más información en www.cloudflare.com.