Cloudflare vs. Zscaler: Zero Trust, SSE, SASE y otros

Perspectiva comparativa

Este documento es un estudio comparativo funcional entre las soluciones globales de Cloudflare y Zscaler vinculadas a las tendencias de transformación de la red y la seguridad, entre las que se incluyen Zero Trust (ZT), servicio de seguridad en el perímetro (SSE) y perímetro de servicio de acceso seguro (SASE). Existen 37 criterios organizados en torno a 5 grupos: plataforma de red nativa en Internet, plataforma de servicios nativa en la nube, servicios para adoptar una arquitectura SASE, servicios para ampliar Zero Trust, SSE, SASE y otros (las definiciones actuales de estas tendencias del mercado) y accesos directos a redes. Algunas comparaciones requieren más contexto y claridad, por lo que se ha añadido una referencia en la última página.

Si deseas consultar una comparación más conceptual, visita cloudflare.com/products/zero-trust/cloudflare-vs-zscaler

Plataforma de red nativa en Internet

Criterios	Cloudflare	Zscaler	Nota al pie
Ciudades con centros de datos disponibles para cualquier cliente	270	55	1
Nubes distintas (planos de control) en los centros de datos	1	~8	2
Acuerdo de nivel de servicio de tiempo activo	100 %	99,99-99,999 %	3
Inspección de paso único en todos los servicios perimetrales	SÍ	NO	4
Laboratorio de investigación de amenazas	SÍ	SÍ	-

Plataforma de servicios nativa en la nube

Criterios	Cloudflare	Zscaler	Nota al pie
Arquitectura modular	SÍ	NO	5
Interfaz de gestión de un solo panel	SÍ	NO	6
Plataforma de desarrollo de procesos sin servidor	SÍ	NO	7
FedRAMP en curso o autorizado	SÍ	SÍ	8

Servicios para adoptar una arquitectura SASE

Criterios	Cloudflare	Zscaler	Nota al pie
Acceso a la red Zero Trust (ZTNA)	SÍ	SÍ	-
Agente de seguridad de acceso a la nube (CASB)	SÍ	SÍ	-
Puerta de enlace web segura (SWG)	SÍ	SÍ	-
Firewall como servicio (FWaaS)	SÍ	SÍ	-
WAN como servicio con aceleración de tráfico en capas 3 y 7	SÍ	NO	9
SD-WAN local	NO - socio	NO - socio	10

Servicios para ampliar Zero Trust, SSE, SASE y otros

Criterios	Cloudflare	Zscaler	Nota al pie
Seguridad del correo electrónico en la nube (CES)	SÍ	NO	-
Aislamiento remoto del navegador (RBI)	SÍ	SÍ	11
Prevención contra la pérdida de datos (DLP)	SÍ	SÍ	12
Sistema de detección de intrusos (IDS)	SÍ	SÍ	13
Protección contra DDoS para redes y aplicaciones	SÍ	NO	14
Seguridad de aplicaciones: WAF y detección de bots	SÍ	NO	15
Rendimiento de aplicaciones: CDN, DNS y equilibrio de carga	SÍ	NO	-
Seguridad en la nube: CWPP, CPSM y CIEM	NO	SÍ	16
Ciberdefensa: espacio seguro y fraude	NO	SÍ	-
Supervisión de la experiencia digital (DEM)	NO	SÍ	-
Terminales en el navegador para acceso remoto privilegiado	SÍ	SÍ	17
Registro de comandos SSH	SÍ	NO	-

Accesos directos a redes

Criterios	Cloudflare	Zscaler	Nota al pie
Acceso sin cliente basado en el navegador	SÍ	SÍ	-
Software de cliente en dispositivo	SÍ	SÍ	-
Software de conectores de aplicaciones	SÍ	SÍ	18
Software de conectores de filiales	NO	SÍ	19
Túneles DNS Anycast , GRE, IPsec, QUIC, Wireguard	SÍ	NO	20
Interconexión de redes privadas para centros de datos y oficinas	SÍ	NO	-
Tránsito IP entrante (BYOIP)	SÍ	NO	-
Admite conexiones solo IPv6	SÍ	NO	21
Solucionadores de DNS recursivo	SÍ	SÍ	-
Clientes en dispositivo y solucionadores de DNS abiertos al público	SÍ	NO	22

Resultados de la comparación

Puntuación de grupo	Criterios	Cloudflare	Zscaler
General	**37**	**32**	**18**
Plataforma de red nativa en Internet	5	5	1
Plataforma de servicios nativa en la nube	4	4	1
Servicios para adoptar SASE	6	5	4
Servicios para ampliar Zero Trust, SSE, SASE y otros	12	9	7
Accesos directos a redes	10	9	5

Notas al pie

1. Según cloudflarestatus.com y cloudflare.com/network, Cloudflare tiene centros de datos públicos en más de 270 ciudades. Muchas ciudades reciben servicio de más de un centro de datos. A enero de 2022, según trust.zscaler.com y config.zscaler.com, Zscaler cuenta con 73 centros de datos públicos en 55 ciudades. Un total de 13 centros de datos están en nubes no publicadas y 11 centros de datos tienen la proximidad geográfica automática desactivada. Los otros 77 centros de datos que asegura tener no parecen estar documentados públicamente y/o disponibles para ningún cliente.
2. Según config.zscaler.com/zscaler.net/cenr, ZIA (Zscaler Internet Access) tiene siete nubes diferentes, ZPA (Zscaler Private Access) tiene dos nubes distintas, y otros productos como ZDX (Zscaler Digital Experience) tienen más nubes diferentes.
3. La mayoría de los servicios cuentan con el respaldo de un acuerdo de nivel de servicio de tiempo activo del 99,999 %, pero su resolución de DNS solo ofrece un acuerdo de nivel de servicio de tiempo activo del 99,99 % (fuente).
4. Por ejemplo, las soluciones de puerta de enlace web segura (SGW), aislamiento remoto del navegador (RBI), acceso a la red Zero Trust (ZTNA) y los servicios de seguridad para aplicaciones pueden inspeccionar una solicitud de un usuario remoto a una aplicación privada autoalojada en un solo paso en el mismo servidor dentro del mismo centro de datos.
5. Es necesario que la arquitectura modular pueda adoptar cualquier servicio ofrecido en la plataforma en cualquier orden y que sea simultáneamente interoperable con los servicios previamente implementados. Zscaler ha diseñado la arquitectura de algunos de sus servicios para que se ejecuten de forma independiente en la arquitectura única que impide esa modulabilidad, tal y como demuestran estos artículos de Zscaler (fuente 1, fuente 2).
6. Cloudflare adquirió Area 1 en abril de 2022. El plan de desarrollo contempla la integración de la gestión de la seguridad del correo electrónico de Area 1 en la interfaz de gestión de Cloudflare Zero Trust. Zscaler no ofrece seguridad del correo electrónico, por lo que esta no es una diferencia equivalente. Sin embargo, Zscaler tiene interfaces de gestión independientes para sus soluciones ZIA y ZPA, así como para muchos de sus complementos, como RBI.
7. Cloudflare Zero Trust se basa en Cloudflare Workers con tecnología de aislamiento V8 en nuestro perímetro. Zscaler utiliza una arquitectura más antigua basada en contenedores, lo que ralentiza el tiempo de desarrollo y añade costos de sobrecarga cuando se prestan nuevas funciones.
8. A junio de 2022, Cloudflare está en proceso de conseguir la aprobación de FedRAMP, mientras que Zscaler está autorizado por FedRAMP.
9. Zscaler afirma que no puede enrutar y acelerar de forma inteligente el tráfico entre centros de datos a través de su propia red troncal.
10. Aunque Zscaler ofrece software de conector de filiales, no proporciona una funcionalidad SD-WAN completa localmente y no aparece en los estudios de analistas en materia de infraestructura perimetral WAN.
11. La tecnología RBI estándar de Zscaler envía una secuencia de píxeles, mientras que la tecnología patentada de representación de vectores de red de Cloudflare envía una secuencia de comandos de dibujo. Además, a junio de 2022, Zscaler solo ejecuta RBI en 4 centros de datos. La combinación degrada la experiencia de usuario con muchas aplicaciones de Internet y SaaS.
12. Desde 2021, Cloudflare ha estado desarrollando un servicio de protección de pérdida de datos (DLP) de forma nativa dentro de nuestra plataforma Zero Trust. Empezamos a trabajar en la versión beta privada en julio de 2022, únete a nuestra lista de espera si deseas más información. La versión beta pública comenzará en agosto.
13. La detección de intrusiones de Cloudflare ya está disponible en nuestro programa beta privada. Comunícate con tu equipo de cuentas para informarte sobre cómo unirte.
14. Zscaler no ofrece un servicio de protección DDoS. Todos los proveedores de servicios nativos en la nube tienen alguna medida de protección DDoS integrada en su arquitectura, pero no mitigan eficazmente un ataque DDoS moderno. Si bien la implementación de Zero Trust evita que tus aplicaciones se expongan directamente en Internet, no impide que los proveedores u otros usuarios a quienes se les haya concedido acceso ataquen la aplicación a través de la red de proveedores de ZTNA.
15. En marzo de 2022, Zscaler anunció la protección de aplicaciones incorporada a su solución ZTNA, ZPA. Sin embargo, no equivale completamente a un Firewall de aplicaciones web (WAF) para aplicaciones direccionables públicas y privadas. Además, carece de capacidades de detección de bots.
16. En 2020-2021, Zscaler adquirió Edgewise Networks para la plataforma de protección de cargas de trabajo en la nube (CWPP), así como Cloudneeti para la gestión de la postura de seguridad en la nube (CSPM) y Trustdome para la gestión de los derechos de la infraestructura en la nube (CIEM). No ha integrado estos servicios de seguridad en la nube en sus servicios Zero Trust.
17. Cloudflare proporciona terminales en el navegador para SSH y VNC, mientras que Zscaler proporciona terminales en el navegador para SSH y RDP. Muchos clientes de Cloudflare utilizan Apache Guacamole para ejecutar RDP en el navegador.
18. Zscaler requiere una infraestructura de máquinas virtuales para ejecutar su imagen, mientras que Cloudflare ofrece un daemon que se puede ejecutar con o sin máquinas virtuales.
19. Zscaler requiere una infraestructura de máquina virtual para ejecutar su imagen, y el tráfico solo puede pasar a través de ZIA o ZPA, pero no en ambos en un solo paso.
20. Zscaler admite Anycast solo para la resolución de DNS. Para los túneles GRE o IPsec, los clientes deben utilizar una dirección IP única por centro de datos de Zscaler. Además, su conector de aplicaciones y cliente en dispositivo dependen de túneles DTLS no Anycast.
21. El cliente en dispositivo de Zscaler no admite conexiones solo IPv6 según los foros de su comunidad (fuente)
22. Zscaler no ofrece resolución de DNS pública gratuita (p. ej. 1.1.1.1) ni comunicación IP encriptada (p. ej. WARP).