ficha de datos

Zscaler Cloud Firewall

Protección segura y adaptable de confianza cero para todo el tráfico de Internet

Zscaler Cloud Firewall protege el tráfico de Internet para todos los usuarios, aplicaciones y ubicaciones.

El mundo laboral ahora está distribuido y es móvil. Las aplicaciones están migrando de los centros de datos a la nube, mientras que las nuevas cargas de trabajo digitales se están implementando cada vez más de forma nativa en la nube. Además, los usuarios que trabajan desde varias ubicaciones, incluidas oficinas en el hogar, espacios de trabajo compartidos, sucursales y de forma remota, acceden a las aplicaciones empresariales directamente desde Internet.

Esto ha dado lugar a que los usuarios y las aplicaciones en la nube produzcan grandes volúmenes de tráfico. Incapaces de manejar el ancho de banda adicional con el retorno del tráfico de Internet y de SaaS de los usuarios, las reglas tradicionales de seguridad centradas en la red afectan la productividad y crean cuellos de botella en la conectividad. Mientras que los cortafuegos virtuales intentan poner remedio a la situación, están limitados a las ubicaciones físicas de los proveedores de la nube y a menudo requieren recursos empresariales dedicados para administrarlos adecuadamente. Para echar más leña al fuego, los malos actores están utilizando el cifrado y puertos no estándar para evadir la detección y provocar ataques en las redes de las víctimas.

Beneficios de Zscaler Cloud Firewall:

- **Protección completa para los usuarios que trabajan desde cualquier lugar.**
  Las políticas de seguridad dinámicas basadas en riesgos siguen a sus usuarios a todas partes sin una matriz compleja de políticas y configuraciones de red.
- **Inspección completa para encontrar ataques ocultos.**
  La inspección de tráfico en línea ilimitada y el descifrado SSL nativo acaban con las conexiones maliciosas y evitan las amenazas.
- **Detección del tráfico web evasivo en puertos no estándar.**
  Identifique e intercepte rápidamente las ciberamenazas evasivas y cifradas que se esconden en el tráfico de los puertos no estándar.
- **Conexiones locales a Internet en la nube.**
  Conexiones directas a Internet rápidas y seguras para todo el tráfico híbrido y de sucursales, que escalan de forma elástica y mejoran la experiencia del usuario.
- **Sistema de prevención de intrusiones en la nube (IPS) siempre activo.**
  Las firmas IPS de comportamiento adaptables, administradas por Zscaler ThreatLabz, trabajan en tiempo real y son fáciles de compartir para enriquecer los flujos de trabajo de SecOps.
- **DNS seguro sin comprometer el rendimiento.**
  Las resoluciones localizadas mantienen un rendimiento superior mientras sus usuarios y puntos finales permanecen a salvo de sitios maliciosos y de la tunelización del DNS.
- **Protección entregada en la nube con presencia en el perímetro global.**
  Zscaler Cloud Firewall proporciona una seguridad y una experiencia de usuario inigualables, ya que está totalmente integrado con Zscaler Internet Access™ y forma parte de Zscaler Zero Trust Exchange™.

A fin de inspeccionar completamente el tráfico cifrado con SSL y el tráfico que atraviesa puertos y protocolos no estándar, los equipos de red y seguridad a menudo sacrifican el rendimiento y la velocidad.

Esto se convierte en un problema, ya que los cortafuegos físicos pueden alcanzar rápidamente los límites de capacidad, incapaces de inspeccionar completamente el tráfico cifrado por SSL o los puertos y protocolos no estándar sin que los recursos adicionales afecten al rendimiento. Los cortafuegos virtuales se limitan a las ubicaciones físicas de los proveedores de la nube y a menudo requieren recursos empresariales dedicados para su correcta administración.

Zscaler Cloud Firewall

Para mejorar la conectividad y la disponibilidad, las organizaciones deben dirigir de forma segura el tráfico de los usuarios mediante accesos locales a Internet sin necesidad de realizar revisiones a través de las VPN y sin duplicar la pila de dispositivos de seguridad en cada ubicación. **El cortafuegos Zscaler Cloud Firewall** permite que el tráfico de Internet se establezca de forma local y segura para todos los puertos y protocolos.

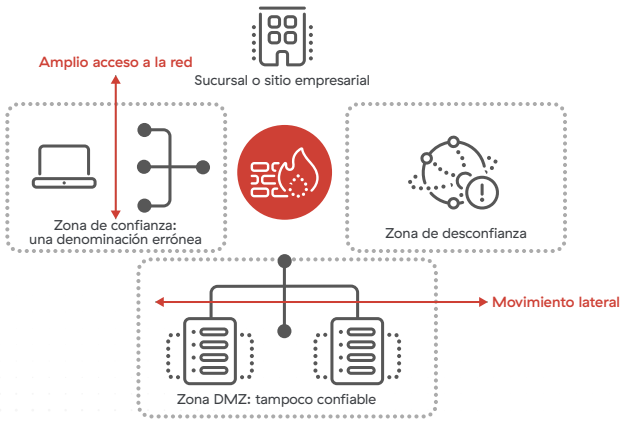
Al enrutar las conexiones con Internet y SaaS a Zscaler, el cortafuegos de generación de la nube inspecciona de forma nativa todo el tráfico de los usuarios, incluido el tráfico cifrado SSL, y se expande de manera elástica para manejar grandes volúmenes de conexiones de larga duración.

Sin actualizaciones de hardware y software, la responsabilidad de actualizaciones, mejoras o parches, incluidos los requisitos de escalabilidad, del cortafuegos basado en la nube recae en Zscaler. Al eliminar matrices complejas de políticas y configuraciones de red que están vinculadas a ubicaciones físicas, la administración de políticas de cortafuegos se simplifica radicalmente. Con políticas adaptables y basadas en riesgos que siguen a sus usuarios a todas partes, dentro y fuera de la red corporativa, Zscaler Cloud Firewall brinda una protección consistente independientemente del dispositivo que se utilice o de dónde se conecten.

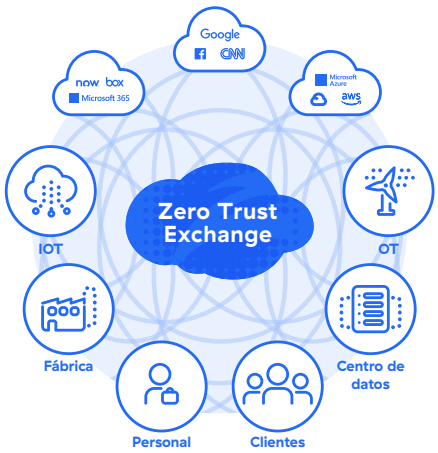
Como parte de una funcionalidad de cortafuegos, Zscaler Cloud Firewall registra cada sesión para proporcionar visibilidad de todos los usuarios y ubicaciones, lo que garantiza que tenga acceso a la información que necesita, exactamente cuando la necesita.

Confianza cero con cortafuegos de generación de la nube

Arquitectura de cortafuegos heredada basada en zonas



Plataforma Zscaler Zero Trust



Al transformar sus conexiones híbridas y de sucursales y abordar las necesidades de seguridad de rendimiento de la actualidad, Zscaler apoya y escala para satisfacer sus necesidades de transformación en la nube, incluido el paso a aplicaciones basadas en la nube, como Office 365.

Ventajas del cortafuegos de generación de la nube

Creado específicamente para el mundo digital actual, Zscaler Cloud Firewall garantiza que pueda acceder de forma segura a Internet y manejar todo el tráfico web y no web, en todos los puertos y protocolos, con una escalabilidad elástica infinita y un rendimiento insuperable. Sus usuarios obtienen una protección constante independientemente del dispositivo que utilicen o del lugar en el que se encuentren (en casa, en la sede central, en las sucursales o de viaje), sin las limitaciones de coste, complejidad y rendimiento de la seguridad de red tradicional y de los dispositivos de cortafuegos de nueva generación.

Impulsado por una plataforma adaptativa de confianza cero
Deje de comprometerse con inspecciones estáticas, degradación del rendimiento y límites de capacidad de los dispositivos de cortafuegos físicos. Construido en una plataforma totalmente integrada y nativa de la nube, Zscaler Cloud Firewall escala de forma elástica para manejar el tráfico de aplicaciones en la nube que requieren conexiones de larga duración, mientras intercepta e inspecciona de forma nativa el tráfico SSL/TLS, a escala, para detectar el malware oculto en el tráfico cifrado.

Conexiones híbridas y de sucursales transformadoras
Evolucione de una infraestructura costosa y centrada en la red a verdaderos accesos locales a Internet proporcionados por la nube. Enrute el tráfico de Internet localmente para proporcionar conexiones directas a la nube y obtener conexiones rápidas y constantes, a la vez que ofrece seguridad y controles de acceso para todos los puertos y protocolos. Sin necesidad de desplegar o gestionar ningún dispositivo, esto reduce los costes de retorno de MPLS y elimina la costosa y lenta gestión de parches, la coordinación de ventanas de interrupción y la gestión de políticas.

Seguridad omnipresente para el personal moderno
Aproveche las actualizaciones de seguridad en tiempo real obtenidas a través de 300 billones de señales diarias y compartidas en toda la nube todos los días para una protección idéntica en cualquier dispositivo dondequiera que se conecten los usuarios (desde oficinas en casa, espacios de trabajo compartidos, sucursales o de viaje). Al acercar toda la pila de seguridad al usuario, experimenta una protección inigualable frente a amenazas basadas en aplicaciones y usuarios con políticas dinámicas de seguimiento dentro y fuera de la red corporativa.

Bloqueo siempre activo de ataques maliciosos conocidos
Vaya allí donde las soluciones tradicionales no se pudieron aplicar con una protección frente a amenazas del sistema de prevención de intrusiones (IPS) basada en contexto y entregada en la nube administrada por Zscaler ThreatLabz. A través de una inspección de tráfico en línea ilimitada, incluidos IoT/OT, y de tráfico cifrado dentro y fuera de la red, las firmas IPS de comportamiento se aplican en tiempo real al acceder a miles de aplicaciones web y no web, independientemente del tipo de conexión o de la ubicación.

Optimización de DNS para obtener rendimiento y seguridad
Consiga una resolución más rápida vinculando las aplicaciones locales geográficamente e impulsando una mejor experiencia de usuario y el rendimiento de las aplicaciones en la nube, al tiempo que implementa políticas de seguridad y control del sistema de nombres de dominio (DNS). Esto protege a los usuarios de acceder a dominios maliciosos y evita la creación de túneles DNS. Al ofrecer DNS como servicio, Zscaler minimiza la latencia y protege los accesos locales a Internet utilizando proxies completos para todo el tráfico DNS y aprovechando el aprendizaje automático para detectar y bloquear la actividad de túneles de exfiltración de datos.

Administración de políticas fácil de entender
Defina, implemente y aplique inmediatamente políticas para todos los usuarios, en todas las ubicaciones desde una única consola. En lugar de matrices complejas de políticas, configuraciones de red y políticas de recreación para cada ubicación de cortafuegos típicos, el cortafuegos de generación de la nube simplifica la administración de políticas centralizando reglas granulares de cortafuegos basadas en el usuario, la aplicación, la ubicación, el grupo y el departamento. Además, los administradores pueden enviar registros forenses completos enriquecidos con detalles de usuario, solicitud, respuestas, servicios utilizados y más a las herramientas SIEM y XDR para mejorar la investigación de seguridad y la respuesta ante incidentes.

Características principales del cortafuegos de generación de la nube

Gestión centralizada de políticas	Defina y aplique inmediatamente las políticas en todas las ubicaciones sin necesidad de volver a crear políticas para cada ubicación.
Servicios de seguridad totalmente integrados	La información contextual se comparte en DLP, APT, sandbox y otros servicios para brindar una mejor protección y una visibilidad más profunda.
Control granular, registro y visibilidad en tiempo real	Registro de gran riqueza forense para una visibilidad detallada con registro unificado globalmente e ilimitado durante seis meses, lo que permite el análisis y la correlación para el descubrimiento de tendencias, el análisis de la productividad y la resolución de problemas.
Protección frente a amenazas basada en el usuario	Defina los usuarios por grupos, departamentos o ubicaciones, incluso estableciendo como ubicación a los usuarios que trabajan desde casa o a los usuarios remotos, e integre los proveedores de identidad y las bases de datos de usuarios locales, permitiendo políticas coherentes independientemente de la ubicación física de los usuarios.

Características principales del cortafuegos de generación de la nube (cont.)

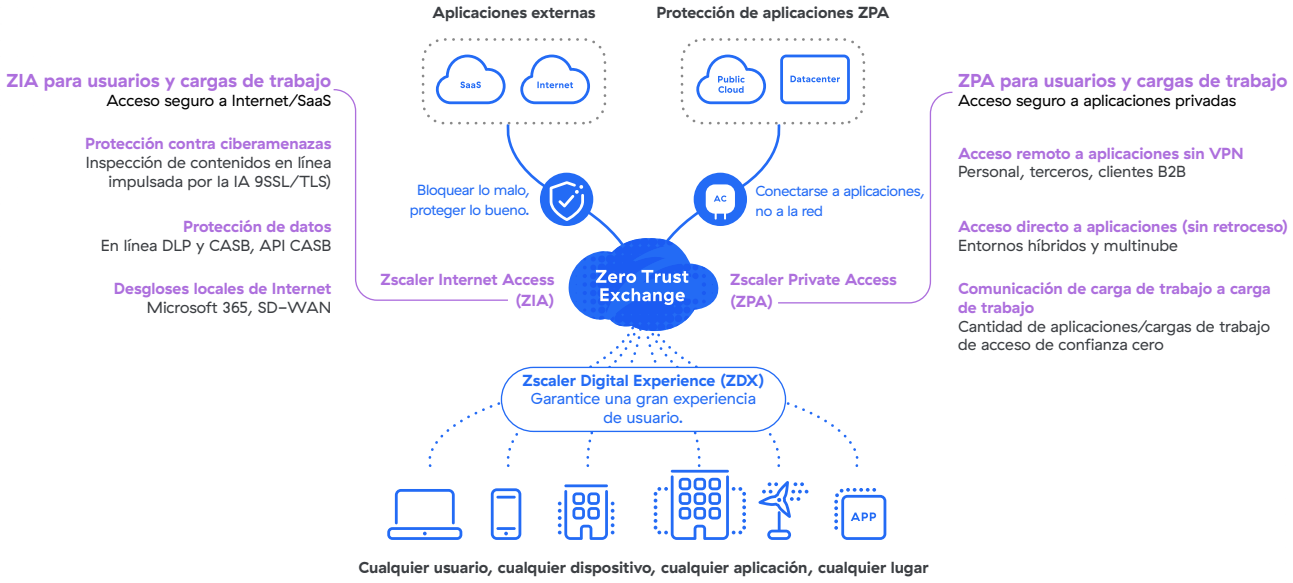
Protección frente a amenazas basada en las aplicaciones	Identifique y clasifique los servicios de aplicaciones en el primer paquete para permitir políticas de reenvío y filtrado de cortafuegos, tomando medidas inmediatas y de mayor prioridad con políticas adaptables y sensibles al contexto. Compatible con tipos de aplicaciones en todos los servicios de red: puertos y protocolos, aplicaciones de red – SNI (nombre de host), DPI, servicios de aplicaciones – UCaaS basado en la identificación de primer paquete, IP, grupos de FQDN y otras detecciones heurísticas.
Seguridad y control adaptables de IPS	Ofrezca protección frente a amenazas siempre activa y entregada en la nube con firmas IPS personalizadas y miles de firmas IPS adaptativas y conductuales en cualquier puerto y protocolo, independientemente del tipo de conexión o ubicación, mediante la inspección de todo el tráfico de Internet del usuario. **Consulte la lista de todas las firmas IPS que administra ThreatLabZ.**
Inspección de seguridad avanzada	Aplique la inspección profunda de paquetes avanzada en protocolos no web, como FTP, DNS, RDP, Telnet y otros, para identificar y evitar el tráfico evasivo en puertos no estándar.
Seguridad y control de DNS	Optimice el rendimiento de las aplicaciones en la nube y minimice la latencia al tiempo que garantiza una seguridad sin concesiones mediante el proxy de todos los DNS a través de Zscaler. Habilite políticas basadas en el usuario, la aplicación, la ubicación y el país de la IP resuelta para bloquear automáticamente a los usuarios de los dominios maliciosos y detectar y evitar la creación de túneles DNS. **Resolución:** DNS como servicio proporciona una resolución óptima con localización, tenencia y menor latencia. **Filtrado DNS:** crea reglas personalizadas de filtrado DNS para bloquear, permitir o redirigir diferentes tipos de solicitudes DNS ante destinos conocidos y maliciosos. **Seguridad y exfiltración de datos:** detecte malware, phishing, tunelización de DNS y exfiltración de datos mediante ML. **DNS sobre HTTPS (DoH):** evite los puntos ciegos de DoH y que se eludan los controles de la organización al cifrar las conexiones DNS en el tráfico HTTPS común.
Nombre de dominio totalmente calificado Políticas (FQDN)	Configure y gestione fácilmente las políticas de acceso a las aplicaciones alojadas en varias IP.
Control del protocolo de transferencia de archivos (FTP) y soporte de traducción de direcciones de red (NAT)	Soporte para el control de acceso de FTP y FTP a través de HTTP, y soporte para proxy de destino NAT y reenvío NAT.
Certificaciones de privacidad y cumplimiento de la normativa	Cumple con los rigurosos requisitos de riesgo, privacidad y cumplimiento de la normativa comercial y gubernamental a nivel mundial. 
Normativas industriales y de privacidad de datos	Cumplimiento de las normativas de privacidad de datos específicas del sector y el país. 
Protección compartida a nivel mundial	Aprovechando el efecto de la nube, cada vez que se identifica una nueva amenaza en cualquiera de las decenas de miles de millones de solicitudes que procesa diariamente la nube de Zscaler, dicha amenaza se bloquea para todos los usuarios de Zscaler, en todas partes.

Zscaler Cloud Firewall está totalmente integrado con Zscaler Internet Access™ y forma parte de la plataforma global Zero Trust Exchange.

Zscaler Zero Trust Exchange habilita conexiones rápidas y seguras y permite a sus empleados trabajar desde cualquier lugar utilizando Internet como la red corporativa. Basado en el principio de confianza cero de acceso con menos privilegios, proporciona una seguridad integral utilizando la identidad basada en el contexto y la aplicación de políticas.

Cómo Zscaler ofrece confianza cero para usuarios, cargas de trabajo y IIoT/OT

Despliegue en cuestión de semanas para mejorar la protección cibernética y la experiencia del usuario



zscaler™ | Experience your world, secured.™

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SASE es la mayor plataforma de seguridad en la nube en línea del mundo.
Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.es