Zscaler Zero Trust Firewall

Protección Zero Trust segura y adaptable para el tráfico web y no web. 100 % nativo de la nube.

FICHA DE DATOS

Zscaler Zero Trust Firewall protege el tráfico web y no web de todos los usuarios, aplicaciones y ubicaciones con la plataforma Security Service Edge (SSE) nativa de la nube más completa del sector.

El mundo del trabajo está ahora distribuido y es móvil. Las aplicaciones están migrando de los centros de datos a la nube y las nuevas cargas de trabajo digitales se implementan cada vez más de manera nativa en la nube. Además, los usuarios que trabajan desde varias ubicaciones, incluidas oficinas en el hogar, espacios de trabajo compartidos, sucursales y a distancia, pueden tener acceso a las aplicaciones empresariales directamente desde Internet.

Como resultado, los usuarios y las aplicaciones en la nube están produciendo grandes volúmenes de tráfico que se devuelve a los dispositivos de seguridad tradicionales centrados en la red, lo que afecta a la productividad y crea cuellos de botella en la conectividad, al tiempo que aumenta los riesgos para la empresa. Sin una inspección completa del tráfico cifrado SSL, los adversarios están utilizando el cifrado y puertos no estándar para eludir la detección y perpetrar ataques furtivos. Los firewalls virtualizados intentan remediar la situación, pero están diseñados para extender su red hacia los recursos de la nube y presentan las mismas limitaciones de capacidad.

Para garantizar la interconectividad y asegurar las cargas de trabajo, seguirá necesitando recursos dedicados para administrarlas adecuadamente o correrá el riesgo de que se produzcan configuraciones erróneas.

Zscaler Zero Trust Firewall

Zscaler Zero Trust Firewall ofrece protección basada en la nube para el tráfico web (HTTP/HTTPS) y no web (FTP, DNS, RDP, Telnet y más) para todos los usuarios y dispositivos independientemente de donde se conecten. Mejora la conectividad y la disponibilidad dirigiendo el tráfico de manera segura mediante la conexión local a Internet sin redireccionar el tráfico a través de VPN y sin duplicar la pila de dispositivos de seguridad en cada ubicación. Al enrutar las conexiones de Internet y SaaS a Zscaler se garantiza la inspección de todo el tráfico de usuarios, incluido el tráfico cifrado SSL, escalando elásticamente para manejar grandes volúmenes de conexiones de larga duración.

Zero Trust Firewall ayuda a las organizaciones a cumplir fácilmente las normas reglamentarias a la vez que configura, gestiona y aplica de manera universal la protección frente a amenazas y las políticas basadas en riesgos para usuarios y aplicaciones con el fin de garantizar la visibilidad de la red y las aplicaciones con una consola de gestión de políticas centralizada. Como solución de firewall como servicio (FWaaS), la responsabilidad de las actualizaciones, mejoras y parches, incluidos los requisitos de escalabilidad, recae en Zscaler. Esto puede suponer un importante ahorro de costos al sustituir los aparatos y elimina las complejas matrices de configuraciones de políticas y redes que están ligadas a ubicaciones físicas.

Zscaler Zero Trust Firewall registra cada sesión para proporcionar visibilidad a través de todos los usuarios y ubicaciones, asegurando que tenga acceso a la información que necesita, exactamente cuando la necesita. Al transformar sus conexiones híbridas y de sucursales y abordar las necesidades de rendimiento y seguridad actuales, Zscaler admite y escala para satisfacer sus necesidades de transformación en la nube, incluida la migración a aplicaciones nativas de la nube como Microsoft 365.

BENEFICIOS DEL ZSCALER ZERO TRUST FIREWALL:

- **Protección total para los usuarios que trabajan desde cualquier lugar.** Las políticas de seguridad dinámicas basadas en riesgos siguen a sus usuarios siempre que se conectan sin necesidad de una compleja matriz de políticas y configuraciones de red.

- **Inspección completa para detectar ataques ocultos.** La inspección ilimitada del tráfico en línea y el descifrado SSL nativo previenen amenazas ocultas y detienen conexiones maliciosas.

- **Detecte tráfico web evasivo en puertos no estándar.** Identifique e intercepte rápidamente ciberamenazas evasivas y cifradas que utilizan puertos no estándar.

- **Conexiones locales a Internet desde la nube.** Conexiones directas a internet, rápidas y seguras, para todo el tráfico híbrido y de sucursales, escalan elásticamente y mejoran la experiencia del usuario.

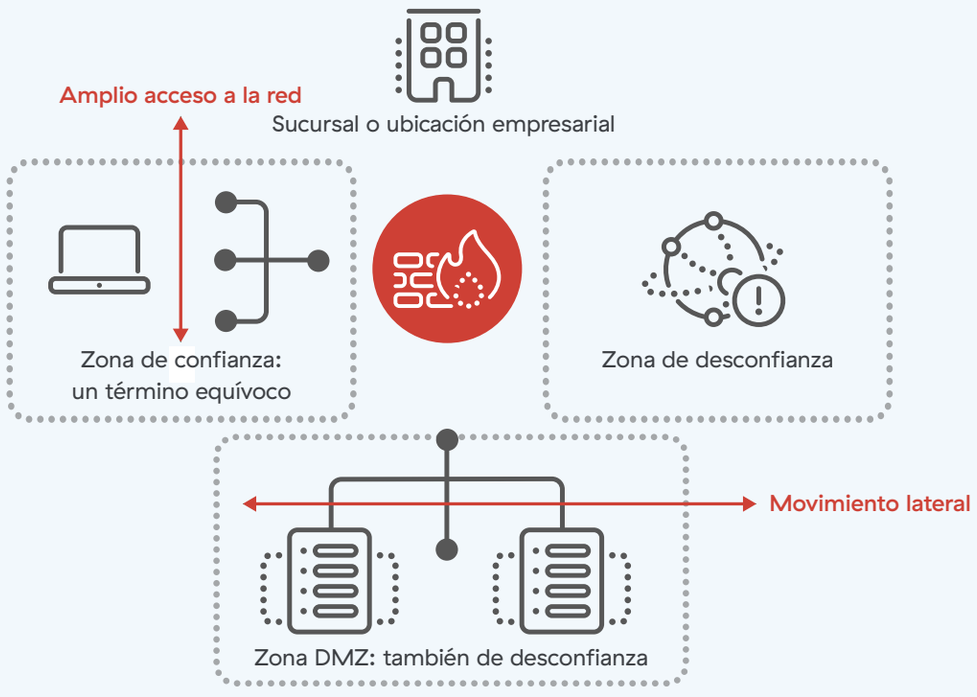
- **Sistema de prevención de intrusiones (IPS) en la nube siempre activo.** Las firmas IPS adaptativas y de comportamiento, gestionadas por Zscaler ThreatLabz, funcionan en tiempo real para enriquecer los flujos de trabajo de SecOps.

- **DNS seguro sin comprometer el rendimiento.** Las resoluciones localizadas garantizan un rendimiento superior, mientras que sus usuarios y puntos finales se mantienen protegidos contra sitios maliciosos y tunelización DNS.

- **Protección proporcionada por la nube con presencia en el perímetro global.** Zscaler Zero Trust Firewall proporciona una seguridad y una experiencia de usuario inigualables, totalmente integradas con Zscaler Internet Access™ y parte de Zscaler Zero Trust Exchange™.

Supere la arquitectura heredada con Zscaler Zero Trust Firewall

Arquitectura heredada de firewall basada en zonas



Plataforma Zscaler Zero Trust

Los firewalls heredados y los de nueva generación son incapaces de cumplir los requisitos Zero Trust del NIST 800-207. La arquitectura de seguridad basada en el perímetro no se diseñó para inspeccionar el tráfico cifrado a escala en redes y dispositivos desprotegidos. La falta de una autenticación estricta de los usuarios y de comprobaciones continuas de las políticas en cada paso podría dar lugar a que un servidor o dispositivo comprometido permitiera a los atacantes un amplio acceso a la red y un movimiento lateral no deseado. Además, utilizar un firewall heredado como puerta de enlace para implementar una red privada virtual (VPN) expone sus redes públicas y privadas. Solo un firewall Zero Trust puede ofrecer un acceso dinámico y con privilegios mínimos para impulsar la transformación de la red y la seguridad.

Beneficios de un firewall nativo de la nube

Zscaler Zero Trust Firewall fue creado específicamente para el mundo digital actual y garantiza el acceso a Internet de manera segura y el manejo de 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 uniforme independientemente del dispositivo que estén utilizando o de dónde se encuentren (en casa, en la oficina central, en sucursales o en la carretera) sin los costos, la complejidad y las limitaciones de rendimiento de los dispositivos tradicionales de seguridad de red y firewall de última generación.

CON UNA PLATAFORMA ZERO TRUST ADAPTABLE

Deje de comprometerse por las inspecciones estáticas, la degradación del rendimiento y los límites de capacidad de los dispositivos firewall físicos. Zscaler Zero Trust Firewall está construido sobre una plataforma nativa de la nube totalmente integrada y se escala elásticamente para manejar el tráfico de aplicaciones en la nube que requieren conexiones de larga duración mientras intercepta e inspecciona de manera nativa el tráfico SSL/TLS (a escala) para detectar malware oculto en el tráfico cifrado.

CONEXIONES QUE TRANSFORMAN EL TRABAJO HÍBRIDO Y LAS SUCURSALES

Evolucione de una infraestructura costosa y centrada en la red a conexiones locales a Internet auténticas a través de la nube. Enrute el tráfico de Internet localmente para proporcionar conexiones directas a la nube y conseguir conexiones rápidas y uniformes, al tiempo que ofrece seguridad y controles de acceso para todos los puertos y protocolos. Sin necesidad de implementar ni gestionar ningún aparato, esto reduce los costos de redireccionamiento MPLS y elimina la costosa y lenta gestión de parches, la coordinación de ventanas de interrupción y la gestión de políticas.

SEGURIDAD SIMULTÁNEA Y EN TODAS PARTES PARA LAS FUERZAS DE TRABAJO MODERNAS

Aproveche las actualizaciones de seguridad en tiempo real informadas por 300 billones de señales diarias y compartidas en toda la nube cada día para una protección idéntica en cualquier dispositivo dondequiera que se conecten los usuarios. Al acercar toda la pila de seguridad al usuario, este experimenta una protección frente a amenazas sin precedentes, consciente del usuario y de las aplicaciones, con políticas dinámicas que le siguen dentro y fuera de la red corporativa.

BLOQUEO PERMANENTE DE ATAQUES MALICIOSOS CONOCIDOS

Llegue donde las soluciones tradicionales no podrían aplicarse con un sistema de prevención de intrusiones (IPS) en la nube, consciente del contexto y con protección contra amenazas gestionado por Zscaler ThreatLabz. Mediante la inspección ilimitada del tráfico en línea, incluido el tráfico IOT/ OT y cifrado dentro y fuera de la red, se aplican firmas IPS de comportamiento en tiempo real cuando se accede a miles de aplicaciones web y no web, independientemente del tipo de conexión o ubicación.

OPTIMICE EL DNS PARA MEJORAR EL RENDIMIENTO Y LA SEGURIDAD

Consiga una resolución más rápida emparejando aplicaciones geográficamente locales, mejorando la experiencia del usuario y el rendimiento de las aplicaciones en la nube al tiempo que aplica políticas de seguridad y control del sistema de nombres de dominio (DNS). Con la inspección SSL a escala, recupere la visibilidad y evite que los atacantes abusen del DNS sobre HTTPS (DoH), protegiendo mejor a los usuarios y empleados para que no lleguen a dominios maliciosos y eludan las políticas de la empresa. Al ofrecer DNS como servicio, Zscaler minimiza la latencia y asegura las fugas locales de Internet utilizando proxies completos para todo el tráfico DNS y aprovecha el aprendizaje automático para detectar y bloquear la actividad del túnel de exfiltración de datos.

ADMINISTRACIÓN DE POLÍTICAS FÁCIL DE ENTENDER

Defina, implemente y aplique inmediatamente políticas de manera universal para todos los usuarios, en todas las ubicaciones y desde una única consola. En lugar de las complejas matrices de políticas, configuraciones de red y recreación de políticas para cada ubicación de los firewalls típicos, Zero Trust Firewall simplifica la gestión de políticas centralizando las reglas granulares del firewall en función del usuario, la aplicación, la ubicación, el grupo y el departamento. Además, los administradores pueden enviar registros completos desde el punto de vista forense, enriquecidos con detalles de usuarios, solicitudes, respuestas, servicios utilizados, etc., a herramientas SIEM y XDR para mejorar la investigación de seguridad y la respuesta a incidentes.

Gartner

Zscaler está posicionado como líder en el Gartner® Magic Quadrant™ para Security Server Edge (SSE), en la posición más alta en capacidad de ejecución.

Más información →

Características principales de Zscaler Zero Trust Firewall

Administración de políticas centralizadas	Defina y haga cumplir 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 entre DLP, APT, entornos aislados y otros servicios para proporcionar una mejor protección y una mayor visibilidad.
Control granular, registro y visibilidad en tiempo real	Registro minucioso que permite tener una visibilidad detallada con registro unificado globalmente e ilimitado durante seis meses, lo que permite el análisis y la correlación para detectar tendencias, analizar la productividad y resolver los problemas.
Protección contra amenazas orientada al usuario	Defina los usuarios por grupos, departamentos o ubicaciones, incluso estableciendo como ubicación a los usuarios que trabajan desde el hogar o a distancia, e integre con los proveedores de identidad y las bases de datos de usuarios locales, para permitir la aplicación de políticas uniformes independientemente de la ubicación física de los usuarios.

Características principales de Zscaler Zero Trust Firewall (cont.)

Protección contra amenazas basada en las aplicaciones	Identifique y clasifique los servicios de aplicación en el primer paquete para habilitar la política de filtrado del firewall y las políticas de reenvío, tomando medidas inmediatas y de mayor prioridad con políticas adaptables y basadas en el contexto. Compatible con los tipos de aplicaciones de todos los servicios de red – puertos y protocolos, aplicaciones de red – SNI (nombre de host), basados en DPI, servicios de aplicaciones – identificación del primer paquete basado en UCaaS, IP, grupos FQDN y otras detecciones basadas en la heurística.
Seguridad y control del IPS adaptable	Ofrezca una protección contra amenazas siempre activa y en la nube con firmas IPS personalizadas y miles de firmas IPS adaptativas y de comportamiento en cualquier puerto y protocolo, independientemente del tipo de conexión o ubicación, inspeccionando todo el tráfico de Internet del usuario. Vea la lista de todas las firmas IPS gestionadas por ThreatLabZ.
Inspección avanzada de seguridad	Realice una inspección avanzada y profunda de paquetes en protocolos no web, incluidos FTP, DNS, RDP, Telnet y muchos otros más, para identificar y evitar el tráfico evasivo en puertos no estándar.

Características principales de Zscaler Zero Trust Firewall (cont.)

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 compromisos mediante el envío de todo el DNS vía un proxy 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 la latencia más baja. • **Filtrado de DNS:** cree reglas de filtrado de DNS personalizadas para bloquear, permitir o redirigir diferentes tipos de solicitudes de DNS contra destinos conocidos y maliciosos. • **Seguridad y exfiltración de datos:** detecte malware, phishing, túneles DNS y exfiltración de datos con ML. • **DNS sobre HTTPS (DoH):** evite los puntos ciegos de DoH y la elusión de los controles organizativos al cifrar las conexiones DNS en el tráfico HTTPs común
Políticas de nombre de dominio completo (FQDN)	Configure y administre fácilmente las políticas de acceso a las aplicaciones alojadas en varias IP.
Control del protocolo de transferencia de archivos (FTP) y soporte de conversión de direcciones de red (NAT)	Soporte para el control de acceso de FTP y FTP en HTTP y soporte para proxy de destino NAT y reenvío NAT
Certificaciones de privacidad y cumplimiento	Cumple con los rigurosos requisitos globales de riesgo, privacidad y normativos, tanto comerciales como gubernamentales.
Normativa del sector y de privacidad de datos	Cumplimiento de las reglas de privacidad de datos específicas del país y del sector
Protección compartida en todo el mundo	Gracias al efecto de la nube, cada vez que se identifica una nueva amenaza en cualquiera de las decenas de miles de millones de solicitudes procesadas diariamente por la nube de Zscaler, se bloquea para todos los usuarios de Zscaler, en cualquier sitio.

Como parte totalmente integrada de Zscaler Internet Access, Zscaler Zero Trust Firewall está incluido en las ediciones ZIA y Zscaler for Users Essentials y Business. Las funciones avanzadas de Zscaler Zero Trust Firewall están incluidas en las ediciones ZIA y Zscaler for Users Transformation y Unlimited, así como un módulo complementario para las ediciones Essentials y Business.

	Standard	Advanced
CRITERIOS DE LA POLÍTICA DE ZERO TRUST FIREWALL		
Servicios de red y aplicaciones	✓ Hasta 10 reglas	✓
Comprobación del filtrado de FQDN		✓
Conciencia de la ubicación		✓
Conciencia del usuario — comprobar	–	✓
Aplicación de red (DPI)	–	✓
Política dinámica basada en el riesgo	–	✓
Reglas del firewall	✓ Hasta 10 reglas	✓ Hasta más de 1000 reglas
CONTROL DE DNS		
Resolutor DNS de confianza	✓	✓
Filtrado DNS y seguridad	✓ Hasta 64 reglas	✓
Detección de aplicaciones y túneles DNS	–	✓
CONTROL DE IPS	–	✓
CONTROL DE FTP	✓	✓
CONTROL DE NAT	✓	✓

CARACTERÍSTICAS DE LA PLATAFORMA		
Inspección SSL completa	✓	✓
Registro en tiempo real	✓ Detalles de registro agregados para acciones de permitir del firewall y detalles de registro detallados para acciones de bloquear con registros DNS completos	✓ Todos los registros de todas las acciones y todas las funciones, incluido el ID de usuario, el ID de la aplicación, el IPS y más
	Incluido con Essentials y licencia de plataforma	Se requiere licencia complementaria adicional

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134** **zscaler.com/mx**

zscaler™

Zero Trust Everywhere