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 de Internet para todos los usuarios, aplicaciones y ubicaciones con la plataforma de perímetro de servicio de seguridad (SSE) nativa de la nube más completa del sector

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.

Como resultado, los usuarios y las aplicaciones en la nube están produciendo grandes volúmenes de tráfico que se devuelven a dispositivos de seguridad tradicionales centrados en la red, lo que afecta la productividad y crea cuellos de botella en la conectividad, además de agregar riesgos empresariales. Sin una inspección completa del tráfico cifrado con SSL, los adversarios usan cifrado y puertos no estándar para evadir la detección y lanzar ataques sigilosos. Los cortafuegos virtualizados intentan solucionar 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 proteger las cargas de trabajo, aún necesitará recursos dedicados a administrarlas adecuadamente o correrá el riesgo de configuraciones incorrectas.

Zscaler Zero Trust Firewall

Zscaler Zero Trust Firewall ofrece protección basada en la nube para la web (HTTP/HTTPS) y tráfico no web (FTP, DNS, RDP, Telnet, etc.) para todos los usuarios y dispositivos, independientemente de dónde se conecten. Mejora la conectividad y la disponibilidad al dirigir el tráfico de forma segura utilizando una conexión a Internet local sin necesidad de retorno mediante 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 del usuario, incluido el tráfico cifrado con SSL, y se escala de forma elástica para manejar grandes volúmenes de conexiones de larga duración.

Zero Trust Firewall ayuda a las organizaciones a cumplir fácilmente con los estándares regulatorios mientras configura, administra y aplica de manera universal protección frente a amenazas conscientes de las aplicaciones y los usuarios, y políticas basadas en riesgos para garantizar la visibilidad de la red y las aplicaciones con una consola de administración de políticas centralizada. Como solución de corta-fuegos como servicio (FWaaS), la responsabilidad de las actualizaciones, mejoras y revisiones, incluidos los requisitos de escalabilidad, recae en Zscaler. Esto puede generar importantes ahorros de costes al reemplazar dispositivos y eliminar matrices complejas de políticas y configuraciones de red vinculadas a ubicaciones físicas.

Zscaler Zero Trust Firewall registra cada sesión para brindar visibilidad entre todos los usuarios y ubicaciones, lo que garantiza 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 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 DE ZSCALER ZERO TRUST FIREWALL:

- **Protección completa para usuarios que trabajan desde cualquier lugar.** Las políticas de seguridad dinámicas basadas en riesgos siguen a sus usuarios cada vez que se conectan, sin 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.

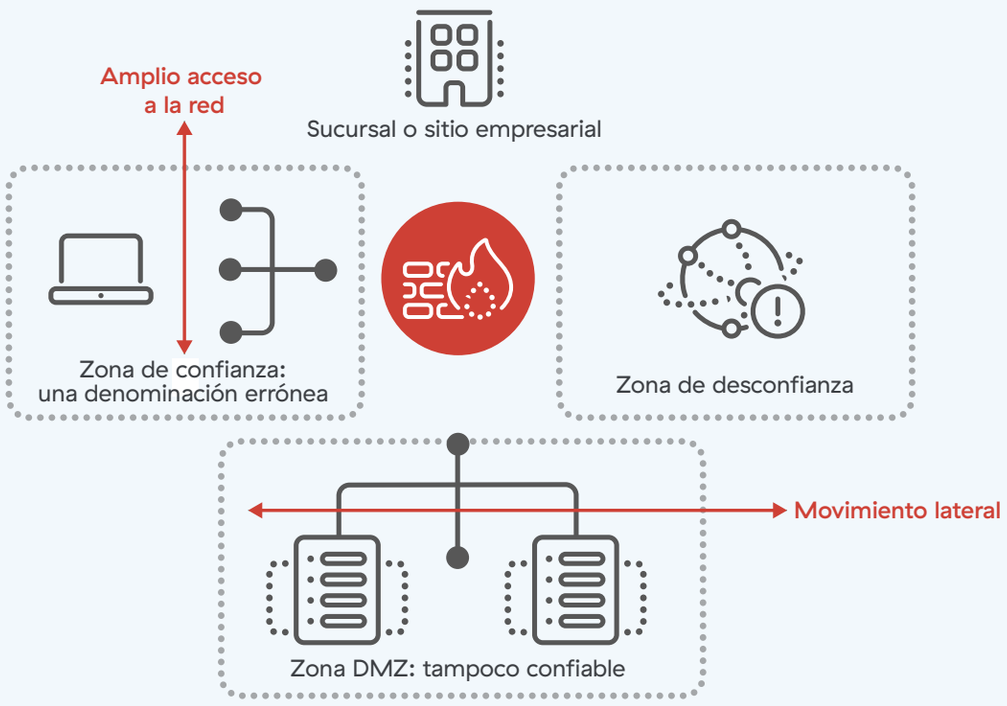
- **Sistema de prevención de intrusiones (IPS) en la nube siempre activo.** Las firmas IPS adaptativas y de comportamiento, gestionadas por Zscaler ThreatLabz, funcionan en tiempo real para enriquecer los flujos de trabajo de SecOps.

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

- **Protección brindada en la nube con presencia global en el perímetro** Obtenga seguridad y experiencia de usuario totalmente integradas e inigualables con Zscaler Internet Access™ como parte de Zscaler Zero Trust Exchange™.

Vaya más allá de la arquitectura heredada con un cortafuegos de zero trust

Arquitectura de cortafuegos heredada basada en zonas



Plataforma Zscaler Zero Trust

Los cortafuegos tradicionales y de próxima generación no pueden cumplir con los requisitos de zero trust de NIST 800-207. La arquitectura de seguridad basada en perímetro no fue diseñada para inspeccionar el tráfico cifrado a escala en redes y dispositivos desprotegidos. La falta de una autenticación estricta de usuarios y de controles de políticas continuos en cada paso podría dar lugar a que un servidor o dispositivo esté comprometido, lo que permite a los atacantes un amplio acceso a la red y movimientos laterales no deseados. Además, utilizar un cortafuegos heredado como puerta de enlace para implementar una red privada virtual (VPN) expone sus redes públicas y privadas. Solo un cortafuegos de zero trust puede brindar acceso dinámico y con mínimos privilegios para impulsar la transformación de la red y la seguridad.

Beneficios de un cortafuegos nativo de la nube

Creado específicamente para el mundo digital actual, Zscaler Zero Trust 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.

CON UNA PLATAFORMA DE CONFIANZA CERO ADAPTABLE

Deje de conformarse con inspecciones estáticas, degradación del rendimiento y límites de capacidad de los dispositivos de cortafuegos físicos. Construido sobre una plataforma nativa de la nube totalmente integrada, Zscaler Zero Trust Firewall se escala elásticamente para manejar el tráfico de aplicaciones en la nube que requiere conexiones de larga duración mientras intercepta e inspecciona de forma 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 desde una infraestructura costosa y centrada en la red a verdaderas conexiones a Internet locales distribuidas desde la nube. Enrute el tráfico de Internet localmente para proporcionar conexiones directas a la nube con el fin de lograr conexiones rápidas constantes al tiempo que brindan seguridad y controles de acceso para todos los puertos y protocolos. Sin la necesidad de implementar o administrar ningún dispositivo, esto reduce los costes de retorno de MPLS y elimina la costosa y lenta administración de revisiones, la coordinación de ventanas de interrupción y la administración de políticas.

SEGURIDAD UBICUA PARA EL PERSONAL MODERNO

Aproveche las actualizaciones de seguridad en tiempo real basadas en 300 billones de señales diarias y compartidas en toda la nube cada día para obtener una protección idéntica en cualquier dispositivo donde sea que se conecten los usuarios. Al acercar toda la pila de seguridad al usuario, este experimenta una protección contra amenazas inigualable, tanto para el usuario como para la aplicación, con políticas dinámicas de seguimiento dentro y fuera de la red corporativa.

BLOQUEO PERMANENTE DE ATAQUES MALICIOSOS CONOCIDOS

Llegue donde las soluciones tradicionales no se pueden aplicar con un sistema de prevención de intrusiones (IPS) con protección contra amenazas basado en el contexto y distribuido en la nube administrado por Zscaler ThreatLabz. A través de una inspección de tráfico en línea ilimitada, que incluye IOT/OT y tráfico cifrado dentro y fuera de la red, se aplican firmas IPS de comportamiento en tiempo real al acceder a miles de aplicaciones web y no web, independientemente del tipo de conexión o la ubicación.

OPTIMICE DNS PARA MAYOR RENDIMIENTO Y SEGURIDAD

Logre una resolución más rápida emparejando aplicaciones geográficamente locales, mejorando la experiencia del usuario y el rendimiento de la aplicación en la nube mientras implementa políticas de control y seguridad de DNS. Con la inspección SSL a escala, recupere visibilidad y evite que los atacantes abusen de DNS sobre HTTPS (DoH), protegiendo mejor a los usuarios y empleados para que no lleguen a dominios maliciosos ni eludan las políticas empresariales. Al ofrecer DNS como servicio, Zscaler minimiza la latencia, optimiza el rendimiento de las aplicaciones en la nube, protege las conexiones locales de Internet utilizando proxies completos para todo el tráfico de 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 de forma universal e inmediata políticas para todos los usuarios, en todas las ubicaciones desde una única consola. En lugar de matrices complejas de políticas, configuraciones de red y recreación de políticas para cada ubicación de cortafuegos típicos, Zero Trust Firewall simplifica la administración de políticas al centralizar reglas de cortafuegos granulares basadas en el usuario, la aplicación, la ubicación, el grupo y el departamento. Además, los administradores pueden enviar registros forenses completos enriquecidos con detalles del usuario, solicitudes, respuestas, servicios utilizados y más a las herramientas SIEM y XDR para mejorar la investigación de seguridad y la respuesta a incidentes.

Gartner®

Zscaler es nombrado uno de los líderes en el Cuadrante Mágico para SSE de Gartner, posicionado en lo más alto en capacidad de ejecución.

Más información →

Características principales del Zscaler Zero Trust Firewall

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 Zscaler Zero Trust Firewall (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 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. Consulte la lista de todas las firmas IPS gestionadas por 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.

Características principales del 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 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 automática-mente 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 en relación con 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 la elusión de los controles organizacionales al cifrar conexiones DNS en el tráfico HTTPS común
Políticas de nombres de dominio completos (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.

Como parte totalmente integrada de Zscaler Internet Access, Zscaler Zero Trust Firewall está incluido en las ediciones Essentials y Business de ZIA y Zscaler for Users. 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.

	Estándar	Avanzado
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 — check	–	✓
Aplicación de red (DPI)	–	✓
Política dinámica basada en el riesgo	–	✓
Reglas del cortafuegos	✓ Hasta 10 reglas	✓ Hasta más de 1000 reglas
CONTROL DE DNS		
Resolutores de DNS confiables	✓	✓
Seguridad y filtrado de DNS	✓ Hasta 64 reglas	✓
Detección de aplicaciones y túneles DNS	–	✓
CONTROLAR IPS	–	✓
CONTROL FTP	✓	✓
CONTROL DE NAT	✓	✓

CARACTERÍSTICAS DE LA PLATAFORMA		
Inspección SSL completa	✓	✓
Registro en tiempo real	✓ Detalles de registro agregados para permitir acciones de cortafuegos y detalles de registro detallados para bloquear acciones 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 de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo , Zero Trust Exchange™ basada en SSE es la mayor plataforma de seguridad en línea en la nube del mundo. Para obtener más información, visite **www.zscaler.com/es** o síganos en Twitter**@zscaler**.

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

zscaler™

Zero Trust Everywhere