Zscaler Zero Trust SD-WAN

Conecte de forma segura sucursales, fábricas y centros de datos sin superposiciones enrutadas ni movimiento lateral de amenazas.

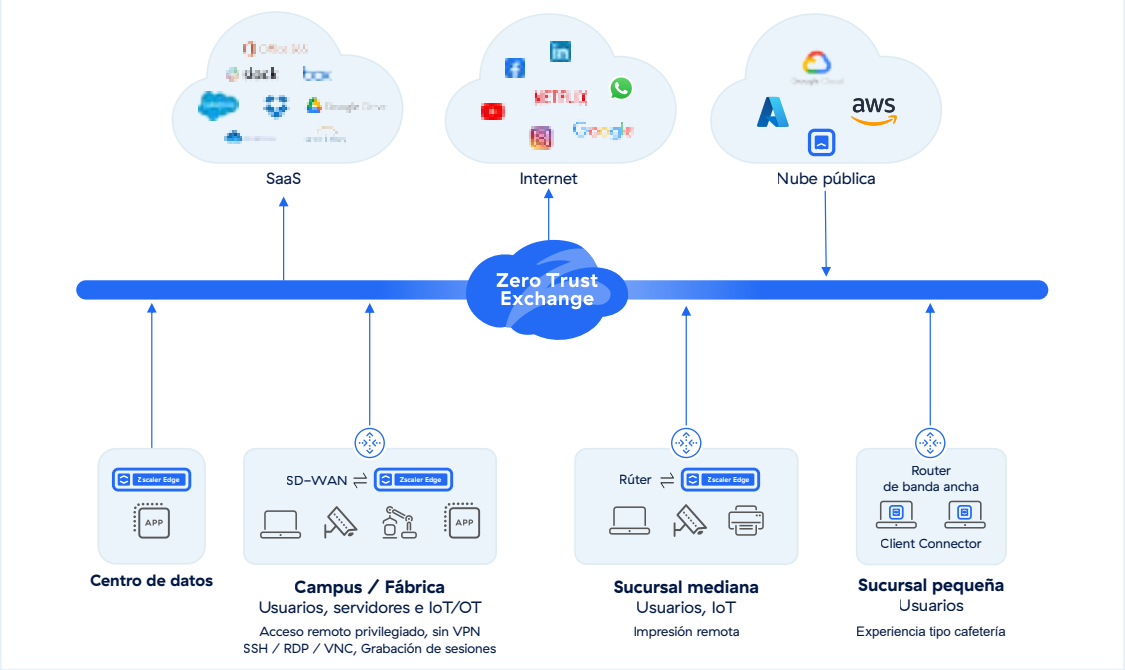
Las SD-WAN tradicionales extienden su red a sucursales remotas y a la nube. Esto amplía su superficie de ataque, permite el movimiento lateral de amenazas y facilita los ataques de ransomware

La protección de las redes tradicionales requiere un complejo conjunto de cortafuegos, servidores proxy, puertas de enlace NAC y agentes de terminales, lo que genera aumentos descontrolados en los costes y la complejidad. Al final, usted sigue siendo vulnerable, ya que los ataques de ransomware continúan aumentando en alcance y frecuencia.

Zscaler Zero Trust SD-WAN ofrece un medio más sencillo, seguro y rentable para que los usuarios, dispositivos y cargas de trabajo se comuniquen, sin la complejidad ni los desafíos de seguridad de las redes superpuestas enrutadas.

Zscaler Zero Trust SD-WAN:

- Permite sucursales tipo cafetería, sin extender su red a todas partes
- Reduce el riesgo de ransomware al eliminar el movimiento lateral de amenazas
- Reduce la superficie de ataque al eliminar los puertos VPN y cortafuegos expuestos
- Reduce los costes de infraestructura al simplificar radicalmente la arquitectura de su red
- Mejora el rendimiento de las aplicaciones al eliminar el tráfico de retorno a los centros de datos
- Garantiza la protección de datos y las ciberamenazas inspeccionando todo el tráfico



Las SD-WAN tradicionales facilitan los ataques de ransomware

Las organizaciones se enfrentan a varios desafíos cuando utilizan arquitecturas de seguridad y redes heredadas para conectar una sucursal a Internet o a sus otras aplicaciones en un entorno de centro de datos o nube pública.

- **Superficie de ataque ampliada:** ampliar la red a sucursales remotas ofrece más oportunidades para que los atacantes se infiltren en su organización. Cada cortafuegos o puerta de enlace VPN es un punto de entrada y las vulnerabilidades de día cero siguen plagando la industria.
- **Movimiento lateral de amenazas:** un usuario o un dispositivo IoT infectado en una sucursal puede analizar la red y moverse lateralmente a otros sitios, centros de datos y nubes privadas virtuales. Los ataques recientes de ransomware han tardado tan solo 45 minutos desde la intrusión inicial hasta las interrupciones paralizantes del servicio, sin dejar tiempo para que los equipos de operaciones reaccionen.
- **Coste y complejidad:** el conjunto de cortafuegos, servidores proxy, agentes NAC y políticas basadas en IP diseñadas para proteger y segmentar las SD-WAN agrega una enorme complejidad y coste operativo, y perjudica la agilidad de su organización.
- **Bajo rendimiento y mala experiencia del usuario:** el tráfico de retorno a los centros de datos y a través de múltiples puntos de inspección de seguridad a menudo genera un bajo rendimiento de la aplicación y una experiencia inconsistente para los usuarios.

Zero Trust SD-WAN elimina el movimiento lateral de amenazas

Zero Trust SD-WAN conecta de forma segura sus sucursales, fábricas y centros de datos sin la complejidad de las VPN o el enrutamiento superpuesto. Garantiza un acceso zero trust entre usuarios, dispositivos IoT/OT y aplicaciones basados en políticas organizacionales. Al combinar el poder de la plataforma líder en la industria Zero Trust Exchange de Zscaler con una conectividad perfecta para ubicaciones, nubes y usuarios, las organizaciones pueden adoptar un marco de perímetro de servicio de acceso seguro (SASE) y permitir que la experiencia en una cafetería sea la misma que en una sucursal.

- Zero Trust SD-WAN proporciona a sucursales y fábricas acceso rápido y confiable a Internet, SaaS y aplicaciones privadas con una arquitectura directa a la nube que brinda alta seguridad y simplicidad operativa.
- Elimina el movimiento lateral de amenazas y reduce en gran medida el riesgo de ransomware para su organización.
- Reduce los costes de infraestructuras y operaciones al eliminar enrutamiento complejo, VPN y cortafuegos, al tiempo que garantiza protección total contra ciberamenazas y datos.

Cómo funciona Zero Trust SD-WAN

Zero Trust SD-WAN utiliza un dispositivo físico o virtual en sucursales, centro educativos y fábricas, para administrar las conexiones del ISP y reenviar el tráfico al Zero Trust Exchange según las políticas de la organización. El tráfico de la sucursal se reenvía de forma segura a través de conexiones DTLS efímeras al Zero Trust Exchange, donde se puede inspeccionar para detectar ciberamenazas y pérdida de datos con políticas de seguridad conscientes del contexto.

Zero Trust Exchange facilita la comunicación bidireccional entre dispositivos y aplicaciones de Internet o aplicaciones privadas que se ejecutan en otras ubicaciones, centros de datos o la nube.

Por ejemplo, un servidor de impresión en un centro de datos puede enviar trabajos de impresión a una impresora en una sucursal remota a través de Zero Trust Exchange, sin necesidad de redes enrutadas, VPN o puertos expuestos. El tráfico de aplicaciones confiables se puede enviar directamente a través de Internet con una conexión directa.

Este enfoque exclusivo ofrece tres ventajas fundamentales:

- **Una organización más segura:** el ransomware no puede moverse lateralmente entre sitios; los dispositivos infectados no pueden analizar nada más allá de sus redes locales
- **Una sucursal más sencilla y menos costosa:** no más superposiciones enrutadas, cortafuegos o VPN de sitio a sitio
- **Experiencia de usuario mejorada:** las aplicaciones se ejecutan más rápido sin retorno de tráfico ni múltiples puntos de congestión de seguridad

Casos de uso de Zero Trust SD-WAN

- **Reemplazo de VPN:** elimine la complejidad de las VPN de sitio a sitio y las superposiciones enrutadas con una solución zero trust más sencilla y segura
- **Actualización de SD-WAN:** proporcione sucursales tipo cafetería y reduzca el riesgo de ransomware
- **Fusiones y adquisiciones:** integre usuarios y aplicaciones sin la complejidad y el coste de integrar redes
- **Fábricas seguras:** elimine el movimiento lateral entre fábricas y proteja los entornos TI/OT

Modelos de hardware y software de Branch Connector

Característica	ZT 400	ZT 600	ZT 800	ZT VM
				Zscaler Edge
Acción de Política	Sucursales pequeñas o medianas	Sucursal pequeña a mediana	Sucursal mediana a grande	Sucursal y centro de datos
Rendimiento cifrado	200 Mbps	500 Mbps	1 Gbps	Varía
Puertos físicos	4x RJ45 GbE	6x RJ45 GbE	6x RJ45 GbE, 2x SFP	N/A
Aprovisionamiento sin intervención	✓	✓	✓	N/A
Modo de puerta de enlace con selección de ruta basada en aplicaciones	✓	✓	✓	N/A
Políticas de reenvío granular	✓	✓	✓	✓
Políticas de ciberamenazas y protección de datos para el tráfico de Internet	✓	✓	✓	✓
Acceso privado seguro para dispositivos IoT/OT	✓	✓	✓	✓

TABLA 1: CAPACIDADES DE ZSCALER ZERO TRUST SD-WAN	
CARACTERÍSTICA	**DETALLES**
Capacidades	
Aprovisionamiento sin contacto e implementación automatizada	• Aprovisionamiento sin intervención con plantillas predefinidas • Implementación totalmente automatizada • Descubrimiento dinámico de la geolocalización de las sucursales
Política de reenvío granular para tráfico de aplicaciones privadas y de Internet	• Opciones de envío del tráfico a ZIA, ZPA o Direct (omitiendo los servicios de Zscaler) • Criterios de selección de tráfico flexibles por ubicación, sububicación, grupo de ubicación, 5 tuplas o FQDN
Políticas unificadas de confianza cero	• Política unificada para usuario a aplicación, dispositivo IoT a aplicación y servidor a servidor a través de la política mejorada de ZPA para incluir nuevos tipos de clientes • Ubicación y políticas basadas en geografía • Habilitación de políticas de seguridad que incluyen IPS, proxy SSL, filtrado de URL y protección de datos • Pila de seguridad completa con postura configurada para servidores y IoT/OT
Alta disponibilidad	• La redundancia de conmutación por error automática con N+2 garantiza la continuidad del servicio • Dos instancias de Branch Connector brindan soporte adicional para ráfagas de tráfico y redundancia en caso de un error de hardware. • Un equilibrador de carga está configurado para tolerancia a fallos activo–pasivo utilizando una dirección IP virtual (VIP) mediante el protocolo de redundancia de dirección común (CARP)
Visibilidad centralizada y registro granular	• Panel de control centralizado para supervisar el estado y el tráfico de los dispositivos • Filtrado disponible para implementaciones en la nube, centros de datos y sucursales • Registro detallado de cada sesión y transacción para todos los puertos y protocolos, incluidas todas las transacciones de DNS públicas y privadas • Totalmente integrado con la infraestructura NSS, la VM de cortafuegos NSS existente se puede utilizar para transmitir los registros a SIEM
Terminación de la interfaz WAN	• Conectividad ISP dual (Ethernet) • Multihoming con un solo aparato
Gestión de interfaz LAN	• Múltiples redes LAN L3 • Soporte de etiquetado 802.1q/VLAN • Servidor DHCP • Puerta de enlace DNS
Políticas de cortafuegos en el dispositivo	• Control de acceso granular para el tráfico local de LAN a LAN (este–oeste) • Listas de control de acceso (ACL) L3/L4
Selección de ruta que tiene en cuenta la aplicación	• Selección de ruta dinámica para SaaS o aplicaciones privadas de misión crítica • Conectividad POP inteligente de Zscaler • Supervisión y conmutación SLA integrados
Enrutado	• Enrutamiento estático
Centros de datos de Zscaler/POP	• Zscaler ha construido su plataforma de seguridad en la nube en más de 150 centros de datos en todo el mundo, ubicados estratégicamente donde se encuentran los clientes • Disponibilidad integrada con conmutación por error sin fisuras al siguiente servicio disponible

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. 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 la nube en línea del mundo. Obtenga más información en **zscaler.com/es** o síganos en Twitter **@**

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