Zscaler Zero Trust SD-WAN

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

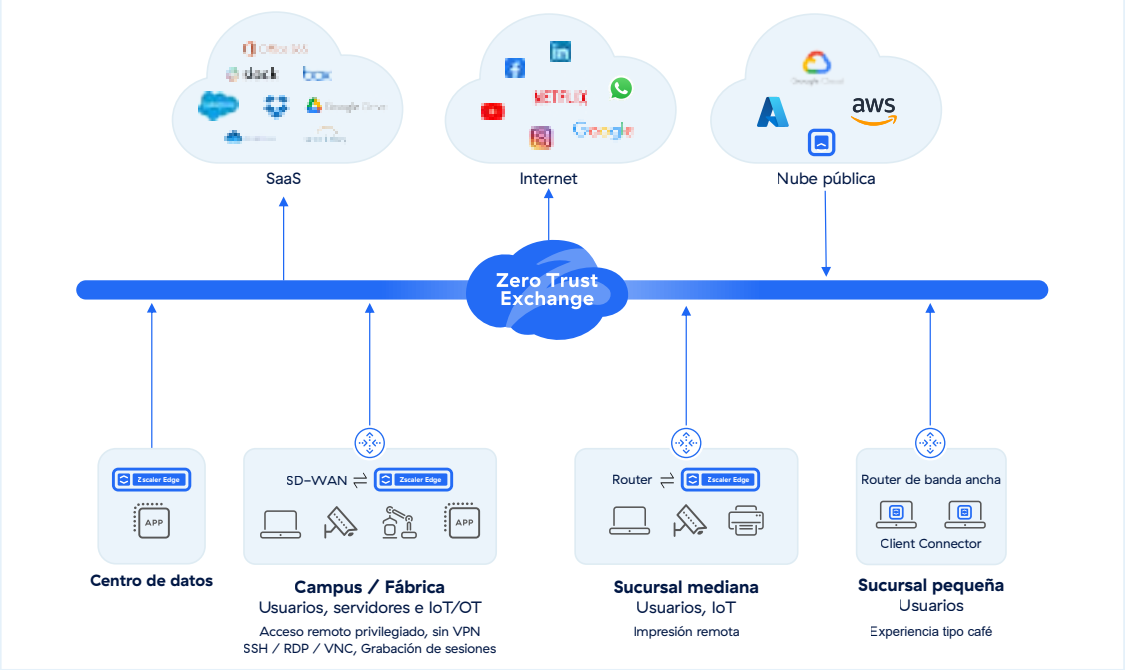
Las SD-WAN tradicionales extienden su red a sucursales remotas y a la nube. Esto amplía su superficie de ataque, permite el movimiento lateral de amenazas y facilita los ataques de ransomware.

Asegurar las redes tradicionales requiere un complejo mosaico de firewalls, proxies, puertas de enlace NAC y agentes de punto final, lo que conlleva un aumento desmesurado de los costos y la complejidad. Al final, sigue siendo vulnerable, ya que los ataques de ransomware continúan aumentando en alcance y frecuencia.

Zscaler Zero Trust SD-WAN ofrece un medio más simple, seguro y rentable para que los usuarios, dispositivos y cargas de trabajo se comuniquen, sin la complejidad y 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 firewalls expuestos
- Reduce los costos 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



© 2024 Zscaler, Inc. Todos los derechos reservados.

Las SD-WAN tradicionales facilitan los ataques de ransomware

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

- **Superficie de ataque ampliada:** La extensión de la red a sucursales remotas ofrece más oportunidades a los atacantes para infiltrarse en su organización. Cada firewall o puerta de enlace VPN es un punto de entrada, y las vulnerabilidades de día cero siguen azotando al sector.
- **Movimiento lateral de amenazas:** un usuario infectado o un dispositivo IoT en una sucursal puede escanear la red y desplazarse lateralmente a otros sitios, centros de datos y nubes privadas virtuales. Los ataques recientes de ransomware han demorado tan solo 45 minutos desde la intrusión inicial hasta las interrupciones paralizantes del servicio, sin dejar tiempo para que los equipos de operaciones reaccionen.
- **Costo y complejidad:** El mosaico de firewalls, proxies, agentes NAC y políticas basadas en IP diseñadas para asegurar y segmentar las SD-WAN añade una enorme complejidad y costo operativos, y perjudica la agilidad de su organización.
- **Rendimiento y experiencia del usuario deficientes:** El retorno del tráfico a los centros de datos y a través de múltiples puntos de inspección de seguridad suele dar lugar a un rendimiento deficiente de las aplicaciones y a una experiencia inconsistente para los usuarios.

Zero Trust SD-WAN elimina el movimiento lateral de amenazas

Zero Trust SD-WAN conecta de manera 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 basado en las políticas de la organización. Combinando la potencia de la plataforma líder del sector Zero Trust Exchange de Zscaler, con una conectividad sin interrupciones para ubicaciones, nubes y usuarios, las organizaciones pueden adoptar un marco de perímetro de servicio de acceso seguro (SASE) y permitir una experiencia de sucursal similar a la de una cafetería.

- Zero Trust SD-WAN proporciona a sucursales, campus y fábricas un acceso rápido y confiable a Internet, SaaS y aplicaciones privadas con una arquitectura directa a la nube que ofrece una gran seguridad y simplicidad operativa.
- Elimina el movimiento lateral de las amenazas y reduce en gran medida el riesgo de ransomware para su organización.
- Reduce drásticamente los costos de infraestructura y funcionamiento al eliminar el enrutamiento complejo, las VPN y los firewalls, al tiempo que garantiza una protección total frente a las ciberamenazas y los datos.

Cómo funciona Zero Trust SD-WAN

Zero Trust SD-WAN utiliza un dispositivo físico o virtual en la sucursal/campus/fábrica para gestionar las conexiones ISP y reenviar el tráfico al Zero Trust Exchange en función de las políticas de la organización. El tráfico de las sucursales se reenvía de manera segura a través de conexiones DTLS efímeras al Zero Trust Exchange, donde puede inspeccionarse en busca de ciberamenazas y pérdida de datos con políticas de seguridad sensibles al 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.

© 2024 Zscaler, Inc. Todos los derechos reservados.

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 a Internet.

Este modelo único ofrece tres ventajas clave:

- **Una organización más segura:** El ransomware no puede desplazarse lateralmente entre sitios; los dispositivos infectados no pueden escanear nada más allá de sus redes locales
- **Una sucursal más sencilla y menos costosa:** No más superposiciones enrutadas, firewalls 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 las VPN:** Elimine la complejidad de las VPN de sitio a sitio y las superposiciones enrutadas con una solución Zero Trust más simple y segura
- **Actualización de SD-WAN:** Ofrezca sucursales tipo cafetería y reduzca el riesgo de ransomware
- **Fusiones y adquisiciones:** Integre usuarios y aplicaciones sin la complejidad y el costo de integrar redes
- **Fábricas seguras:** Elimine el movimiento lateral entre las fábricas y los entornos IT/OT

Modelos de hardware y software de Branch Connector

Características	ZT 400	ZT 600	ZT 800	ZT VM
				Zscaler Edge
Tipo	Sucursales pequeñas–medianas	Sucursal pequeña–mediana	Sucursal mediana–grande	Sucursal y centro de datos
Cifrado completo	200 Mbps	500 Mbps	1 Gbps	Varía
Puertos físicos	4x RJ45 GbE	6x RJ45 GbE	6x RJ45 GbE, 2x SFP	N/A
Aprovisionamiento sin contacto	✓	✓	✓	N/A
Modo puerta de enlace con selección de ruta sensible a las aplicaciones	✓	✓	✓	N/A
Políticas de reenvío granular	✓	✓	✓	✓
Políticas de ciberame-nazas y protección de datos para el tráfico de Internet	✓	✓	✓	✓
Acceso privado seguro para dispositivos IoT/OT	✓	✓	✓	✓

© 2024 Zscaler, Inc. Todos los derechos reservados.

TABLA 1: CAPACIDADES DE ZSCALER ZERO TRUST SD-WAN	
CARACTERÍSTICAS	**DETALLES**
Capacidades	
Aprovisionamiento sin contacto e implementación automatizada	• Aprovisionamiento sin contacto con plantillas predefinidas • Implementación totalmente automatizada • Descubrimiento dinámico de la geolocalización de las sucursales
Política de reenvío granular para el tráfico de Internet y de aplicaciones privadas	• Opciones para enviar el tráfico a ZIA, ZPA o Direct (omitiendo los servicios de Zscaler) • Criterios flexibles de selección de tráfico ubicación, sububicación, grupo de ubicaciones, 5 tuplas o FQDN
Políticas Zero Trust unificadas	• 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 cliente • Políticas basadas en la localización y la 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 IoT/OT y servidores
Alta disponibilidad	• La conmutación automática por error con redundancia N+2 garantiza la continuidad del servicio • Dos instancias de Branch Connector proporcionan soporte adicional para ráfagas de tráfico y redundancia en caso de falla del hardware • Se configura un equilibrador de carga para la tolerancia activa–pasiva de fallas mediante una dirección IP virtual (VIP) utilizando el protocolo común de redundancia de direcciones (CARP)
Visibilidad centralizada y registro granular	• Panel centralizado para el estado del dispositivo y la supervisión del tráfico • 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 DNS públicas y privadas • Integración completa con la infraestructura de NSS: La máquina virtual de firewall de NSS existente puede utilizarse para transmitir los registros a SIEM
Terminación de la interfaz WAN	• Conectividad de doble ISP (Ethernet) • Multi-homing con un único dispositivo
Gestión de interfaz LAN	• Múltiples redes LAN L3 • Soporte de etiquetado 802.1q/VLAN • Servidor DHCP • Puerta de enlace DNS
Políticas de firewall 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 dinámica de rutas para aplicaciones SaaS o privadas de misión crítica • Conectividad POP inteligente de Zscaler • Supervisión y conmutación por error de SLA integrados
Enrutamiento	• Enrutamiento estático
Centros de datos/POP de Zscaler	• Zscaler ha construido su plataforma de seguridad en la nube en más de 150 centros de datos en todo el mundo, estratégicamente situados donde se encuentran los clientes • Disponibilidad integrada con conmutación por error sin interrupciones al siguiente PoP de servicio disponible

zscaler™ | Experience your world, secured.™

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 ataques cibernéticos y pérdida de datos al conectar de forma 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**.

© 2024 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ y otras marcas registradas listadas en **zscaler.com/mx/legal/trademarks** son (i) marcas comerciales o marcas de servicio registradas o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y otros países. Cualquier otra marca comercial pertenece a sus respectivos propietarios.

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