Ficha de datos

SD-WAN Zero Trust de Zscaler

Conecte de forma segura sucursales, fábricas y centros de datos y extienda la seguridad de confianza cero a servidores y dispositivos IoT/OT en cualquier ubicación.

El trabajo híbrido y la transformación de la nube han puesto patas arriba los modelos de red y seguridad basados en el perímetro, con el traslado de las aplicaciones privadas a la nube y el acceso de los usuarios a las aplicaciones a través de la Internet pública, en cualquier dispositivo y desde cualquier lugar.

En el panorama actual, muchas empresas también aprovechan los dispositivos IoT/OT en diversas ubicaciones (incluidas sucursales, fábricas y centros de datos) para agilizar sus operaciones. Además, un número considerable de clientes confía en la comunicación de la carga de trabajo de servidor a cliente. Los modelos tradicionales que dependen de las WAN heredadas, las VPN de malla y los firewalls para gestionar el acceso a las aplicaciones se han vuelto ineficaces en un mundo que da prioridad a las tecnologías móviles y en la nube.

Sin embargo, a medida que los requisitos de las organizaciones han ido evolucionando, a las soluciones WAN heredadas les cuesta seguir el ritmo. SD-WAN presenta varios problemas, como por ejemplo, una seguridad limitada a través del acceso basado en la red, una superficie de ataque expansiva, amplios privilegios de movimiento lateral y complejidades de enrutamiento. La incorporación de principios de confianza cero a esta red suele requerir la adición de dispositivos firewalls adicionales, lo que añade costos y complejidad.

SD-WAN Zero Trust de Zscaler:

- **Permite la confianza cero en todas partes** para todos los usuarios, dispositivos, servidores e IoT/OT, independientemente de su ubicación.
- **Mejora el rendimiento de las aplicaciones** enviando el tráfico de las sucursales directamente al Zero Trust Exchange y el tráfico de las aplicaciones de confianza directamente a través de Internet con conexión directa a Internet.
- **Evita el movimiento lateral de las amenazas:** La confianza cero sienta las bases de una conectividad segura que permite la segmentación este-oeste.
- **Elimina la superficie de ataque** conectando sucursales y centros de datos a través de Zero Trust Exchange independientemente del transporte subyacente
- **Permite el descubrimiento y la clasificación de dispositivos IoT sombra** con clasificación automática de dispositivos basada en perfiles de tráfico
- **Simplifica el acceso seguro a los recursos de OT** con acceso basado en navegador sin cliente a los puertos SSH/RDP/VNC de los activos de OT.
- **Hace cumplir políticas de reenvío de gran precisión** para el tráfico de Internet y fuera de Internet mediante ZIA o ZPA
- **Introduce la implementación plug-and-play:** El aprovisionamiento sin intervención (ZTP) simplifica la implementación y reduce el tiempo de integración

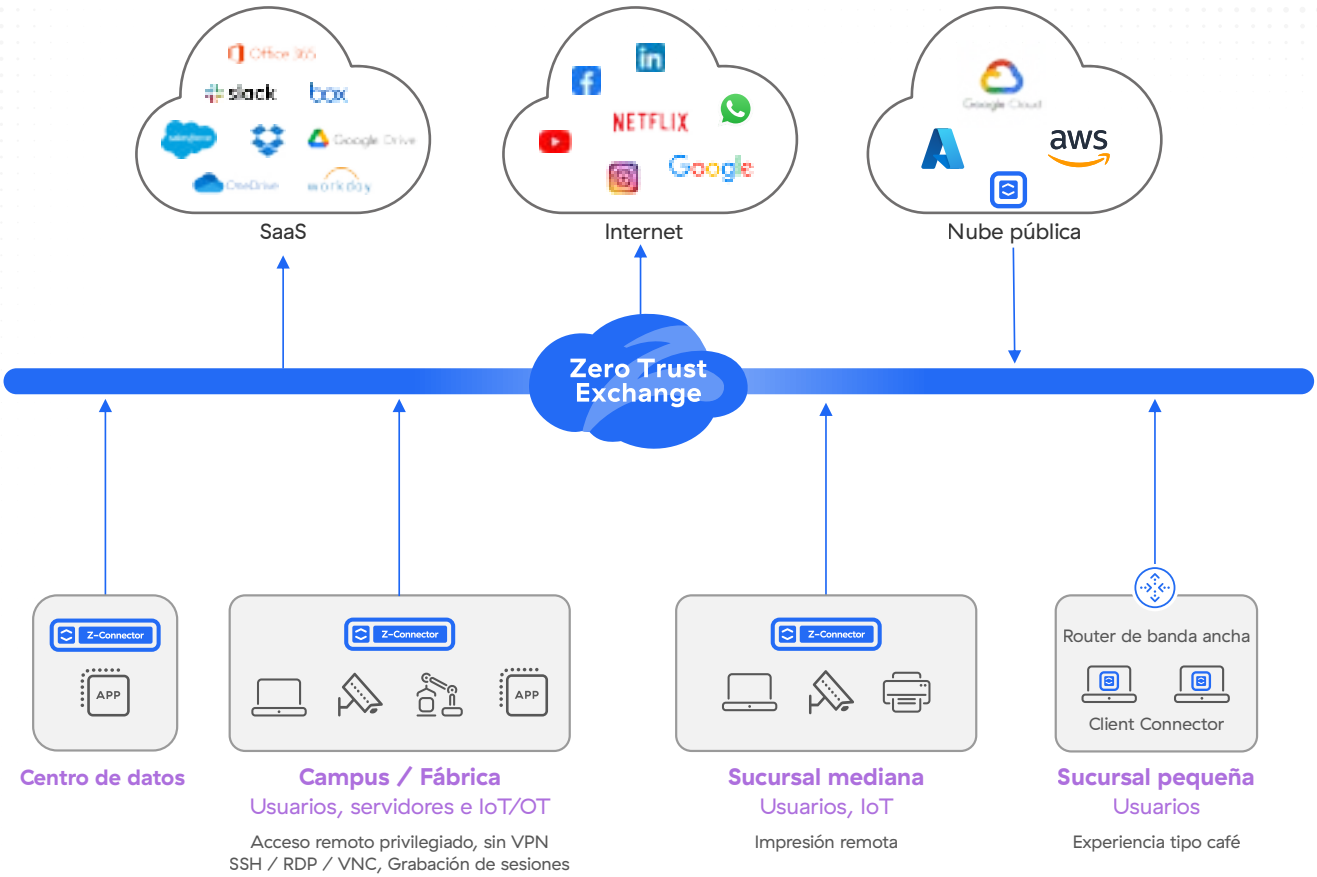

Figura 1: Zero Trust SD-WAN

La SD-WAN de confianza cero conecta de forma segura sus sucursales, fábricas y centros de datos sin la complejidad de las VPN, garantizando un acceso de confianza cero entre usuarios, dispositivos IoT/OT y aplicaciones basado en las políticas de la organización.

La SD-WAN tradicional no es de confianza cero

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, entre ellos:

- **Mayor riesgo de amenazas laterales y ataques basados en Internet** por el uso de soluciones de conectividad heredadas y centradas en la red, como VPN de sitio a sitio, firewalls o SD-WAN tradicionales. Estas soluciones extienden en exceso la red de confianza del cliente a través de Internet a otras nubes y entornos locales, lo que aumenta la superficie de ataque. Un conjunto de parches de dispositivos de seguridad, herramientas y políticas no estándar conducen a un mayor riesgo de seguridad debido a lagunas conocidas y desconocidas en la cobertura de seguridad.

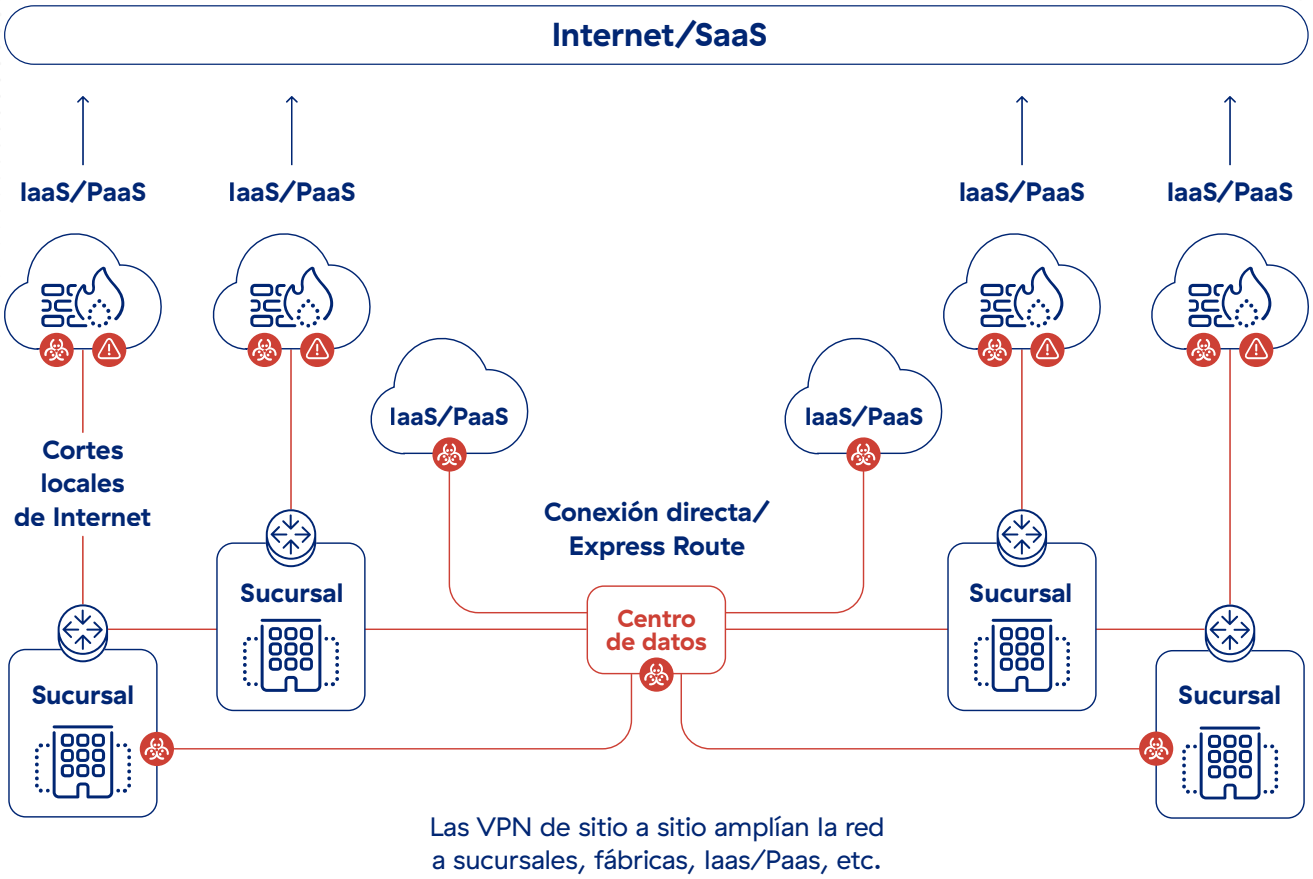

Figura 2: Mayor riesgo de amenazas laterales y ataques basados en Internet con las SD-WAN tradicionales

- **Aumento de la complejidad** debido a un enrutamiento complicado, múltiples saltos de red y dispositivos, y una gestión de políticas fragmentada por la introducción de modelos heredados en la nube. Gestionar esta complejidad es una tarea difícil para los equipos de redes y seguridad, ya que tienen dificultades para estandarizar la conectividad y aplicar la política de seguridad en las sucursales, la nube y los centros de datos.
- **Falta de visibilidad** en las rutas de conectividad de las sucursales, los centros de datos y la nube, lo que crea puntos ciegos en la red y la seguridad.
- **Rendimiento y escalabilidad deficientes** debido al creciente número de servicios de red y seguridad en los entornos de sucursales y centros de datos, al retorno del tráfico y a los puntos de congestión para la inspección y el control centralizados de la seguridad.
- **Costos elevados** debidos a los dispositivos de red y seguridad heredados (por ejemplo, firewalls, IPS, enrutadores y otros productos puntuales), al aprovisionamiento excesivo de servicios de red para compensar la falta de escalabilidad y al mayor uso de servicios nativos en la nube.

Cómo funciona la SD-WAN de confianza cero

La SD-WAN de confianza cero permite a las organizaciones construir una sucursal pequeña eliminando múltiples productos como enrutadores, firewalls y VPN con un sencillo dispositivo plug-and-play que puede implementarse rápidamente utilizando solo una conexión a Internet. Esto permite a las organizaciones reducir la complejidad asociada a la gestión de múltiples dispositivos y optimizar la funcionalidad general de la sucursal. La SD-WAN de confianza cero simplifica drásticamente las comunicaciones de las sucursales con una superposición de red de confianza cero que permite un reenvío flexible y una gestión sencilla de las políticas mediante el uso del reconocido marco de políticas ZIA y ZPA.

El tráfico de las sucursales puede reenviarse de forma segura directamente al Zero Trust Exchange, donde pueden utilizarse las políticas ZIA o ZPA para una inspección de seguridad completa y un control basado en la identidad de acceso de las comunicaciones entre sucursales y centros de datos. 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:

- Dejará de lado la conectividad VPN de sitio a sitio basada en la red para pasar a una comunicación basada en la identidad y en las aplicaciones para una verdadera seguridad de confianza cero.
- Elimina una arquitectura heredada de castillo y foso sin comprometer la seguridad; no necesita productos heredados como proxies Squid, pasarelas NAT, IPS, etc.
- Proporciona una conectividad distribuida y escalable donde sea necesaria, con una gestión de políticas centralizada y automatizada para simplificar las comunicaciones entre sucursales y centros de datos.

Casos de uso de SD-WAN Zero Trust

Reemplazo de VPN de sitio a sitio

Conecte las sucursales directamente a las aplicaciones privadas sin ampliar su WAN ni depender de VPN, ya que ambas opciones aumentan la superficie de ataque de una red. Las aplicaciones se ocultan del descubrimiento detrás de las sucursales, y el acceso se restringe a través del Zero Trust Exchange a un conjunto de entidades designadas. La identidad, el contexto y el cumplimiento de las políticas de los participantes especificados se verifican antes de permitir el acceso, lo que prohíbe el movimiento lateral en otras partes de la red.

Fusiones y adquisiciones

Fusionar dos redes separadas supone un reto y requiere mucho tiempo. Los problemas van desde superposiciones de IP y problemas de enrutamiento hasta un mayor riesgo de seguridad por la ampliación de la superficie de ataque de la red. Con la SD-WAN de confianza cero, las redes pueden permanecer separadas y las sucursales de un entorno pueden conectarse rápidamente a las aplicaciones privadas de otro, sin interrupciones.

Habilitación de acceso directo a Internet para sucursales

Los modelos de redes y seguridad locales pierden eficacia a medida que las organizaciones migran sus aplicaciones a la nube y crean aplicaciones nativas de la nube. La SD-WAN Zero Trust de Zscaler es una solución creada específicamente para la transformación de las sucursales, que marca el comienzo de un nuevo modelo que permite a las sucursales comunicarse con cualquier destino de forma segura e independiente de la red subyacente.

Confianza cero para la conectividad de servidores, IoT/OT

Los activos IoT/OT necesitan que los empleados y proveedores externos accedan a ellos con regularidad para maximizar el tiempo de actividad de la producción y evitar interrupciones por fallos en los equipos y procesos. La SD-WAN de confianza cero para IoT/OT proporciona un acceso de escritorio remoto totalmente aislado y sin clientes a los sistemas de destino RDP y SSH, sin tener que instalar un cliente en su dispositivo mediante hosts de salto y VPN heredadas.

Descubrimiento y visibilidad de IoT/OT sombra

Los equipos de TI se enfrentan a puntos ciegos a medida que dispositivos no autorizados y no descubiertos se conectan a las redes de las sucursales, y el resultado es un aumento de la vulnerabilidad de los dispositivos y una superficie de ataque más amplia. Zscaler identifica y clasifica los dispositivos para dar a los equipos de TI una visibilidad más profunda del comportamiento con el fin de mejorar las políticas de control de acceso.

Dispositivos Z-Connector Plug & Play

Características	ZT 400	ZT 600	ZT 800	ZT VM
				Z-Connector
Tipo	Sucursales pequeñas-medianas	Sucursal pequeña-mediana	Sucursal mediana-grande	Sucursal y centro de datos
Rendimiento/ hipervisor	200 Mbps	500 Mbps	1 Gbps	KVM, ESXi
Puertos físicos	4 x GbE	6 x GbE	8 x GbE	N/A
Aprovisionamiento sin contacto	✓	✓	✓	✓
Política de reenvío granular para Internet, aplicaciones privadas y tráfico WAN directo	✓	✓	✓	✓
Aproveche el filtrado de URL, el control del tipo de archivo y las políticas de firewalls en la nube para el tráfico vinculado a Internet	✓	✓	✓	✓
Políticas ZPA de confianza cero para dispositivos IoT, servidores	✓	✓	✓	✓
Visibilidad y registro centralizados	✓	✓	✓	✓

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 la ZIA, la ZPA o directamente a través de Internet • Criterios flexibles de selección de tráfico ubicación, subububicación, grupo de ubicaciones, 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 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	• Dos instancias de SD-WAN de Confianza Cero que funcionan en modo HA proporcionan soporte adicional para ráfagas de tráfico y redundancia en caso de fallo del hardware. • Tolerancia activa-pasiva a fallas mediante una dirección IP virtual (VIP) basada en el protocolo común de redundancia de direcciones (CARP) • Circuitos activo-activo (aparato único) • Circuitos activo-activo (aparato dual al equilibrar FHRP)
Visibilidad centralizada y registro granular	• Panel centralizado para el estado del dispositivo y el monitoreo 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 total con la infraestructura de Nanolog Streaming Service con opción de transmitir los registros al SIEM propiedad del cliente
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 firewalls en el dispositivo	• Control de acceso granular para el tráfico local de LAN a LAN (este-oeste) • Listas de control de acceso (ACL) L3
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, fuertes 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**.

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