



## Zero Trust SD-WAN de un vistazo

### Ventajas de la solución:

#### Complejidad reducida

Elimine la compleja malla de varias VPN de sitio a sitio y las redes superpuestas enrutadas.

#### Experiencia de usuario mejorada

Elimine el innecesario desvío de tráfico o tromboning, y mejore el rendimiento de SaaS y las aplicaciones en la nube sin comprometer la seguridad. Haga cumplir las políticas de seguridad y ancho de banda en más de 150 centros de datos de Zscaler en todo el mundo.

#### Seguridad mejorada

Minimice la superficie de ataque y el riesgo de movimiento lateral de amenazas inherente a la SD-WAN tradicional. Simplifique la segmentación de usuario a aplicación y de aplicación a aplicación utilizando la plataforma Zero Trust Exchange nativa de la nube.

Zero Trust SD-WAN conecta de forma segura sus sucursales, fábricas y centros de datos sin la complejidad de las VPN, lo que garantiza un acceso de confianza cero entre usuarios, dispositivos IoT/OT y aplicaciones en función de las políticas de la organización. 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.

### ¿Por qué conformarse con la SD-WAN tradicional?

Las SD-WAN tradicionales amplían la superficie de ataque y permiten el movimiento lateral de amenazas, que hace que las redes sean vulnerables a estas. Además, las SD-WAN tradicionales conectan varios sitios mediante VPN de sitio a sitio, lo que introduce complejidad en la red, ya que las organizaciones siguen teniendo que administrar tablas de enrutamiento. En estos enrutamientos superpuestos la confianza está implícita, lo que brinda a las entidades que se conectan a la red acceso sin restricciones a recursos esenciales. Hoy en día, muchas amenazas se originan en las sucursales debido a un usuario, dispositivo IoT/OT o servidor comprometido.

### Zero Trust SD-WAN

- 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 al conectar a los usuarios y los dispositivos IoT/OT a aplicaciones a través de Zero Trust Exchange.
- Simplifica drásticamente las comunicaciones de las sucursales al eliminar enrutamiento complejo, las VPN y los cortafuegos, al mismo tiempo que permite un reenvío flexible y una gestión de políticas sencilla mediante el uso del marco probado de ZIA y ZPA.

## Casos de uso de la solución

### Reemplazo de las VPN de sitio a sitio

Reemplace la malla de varias VPN de sitio a sitio que conectan sucursales, fábricas y centros de datos con una conectividad plug and play sencilla que ofrece simplicidad operativa con mayor seguridad.

### Acceso seguro a los recursos IoT/OT

Los empleados y proveedores externos necesitan acceder periódicamente a los activos IoT/OT para maximizar el tiempo de actividad de la producción y evitar interrupciones por fallas de equipos y procesos. SD-WAN de confianza cero simplifica el acceso los recursos IoT/OT sin la necesidad de VPN o puertos expuestos, lo que proporciona un acceso a escritorio remoto sin cliente y completamente aislado a sistemas de destino internos RDP y SSH para proveedores/contratistas.

### Aceleración de integración de fusiones y adquisiciones

Esté operativo desde el primer día sin tener que fusionar dominios de enrutamiento o traducir direcciones IP superpuestas. Conecte nuevos usuarios a recursos críticos como Active Directory simplemente agregando un dispositivos plug and play en nuevos sitios.

### Descubrimiento y clasificación de dispositivos IoT

Los equipos de TI se enfrentan a puntos ciegos a medida que dispositivos IoT desconocidos y no autorizados se conectan a las redes de las sucursales, lo que genera un mayor riesgo de infestaciones de malware en toda la organización. Zscaler identifica y clasifica dispositivos para brindar a los equipos de TI una visibilidad más profunda del comportamiento y poder implementar mejores políticas de control de acceso.

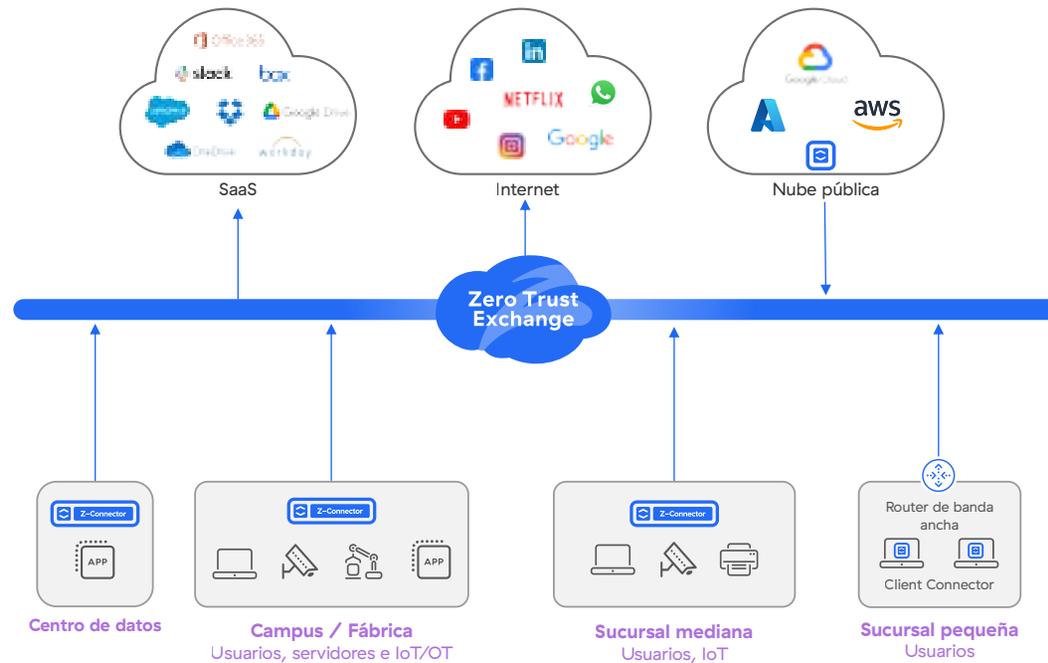


Imagen 1: Zero Trust SD-WAN

Zero Trust SD-WAN es un dispositivo plug and play disponible de forma virtual o física.

## Modelos de hardware y software de Zero Trust SD-WAN

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

 | Experience your world, secured.™

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 SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en [zscaler.es](https://zscaler.es) o siganos en Twitter [@zscaler](https://twitter.com/zscaler).

©2024 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ y ZPA™ y otras marcas comerciales mencionadas en este documento 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/o en otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.