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 lugar.

El trabajo híbrido y la transformación de la nube han revolucionado los modelos de red y seguridad basados en perímetros, pues ahora las aplicaciones privadas migran a la nube y los usuarios acceden a ellas a través de la Internet pública, en cualquier dispositivo y desde cualquier ubicación.

En el panorama actual, muchas empresas también aprovechan los dispositivos IoT/OT en varias ubicaciones, incluidas sucursales, fábricas y centros de datos, para optimizar sus operaciones. Además, un número considerable de clientes dependen de la comunicación de cargas de trabajo de servidor a cliente. Los enfoques tradicionales que dependen de WAN heredadas, VPN de malla y cortafuegos para administrar el acceso a las aplicaciones se han vuelto ineficaces en un mundo que prioriza las tecnologías móviles y en la nube.

Sin embargo, a medida que los requisitos de las organizaciones han evolucionado, las soluciones WAN heredadas se esfuerzan por estar a la altura. SD-WAN presenta varios desafíos, como una seguridad limitada del acceso basado en la red, una superficie de ataque expansiva, amplios privilegios de movimiento lateral y complejidades de enrutamiento. Aplicar principios de confianza cero a este tipo de red suele requerir agregar dispositivos de cortafuegos adicionales, lo que aumenta el coste y la complejidad.

SD-WAN Zero Trust de Zscaler:

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

© 2023 Zscaler, Inc. Todos los derechos reservados.

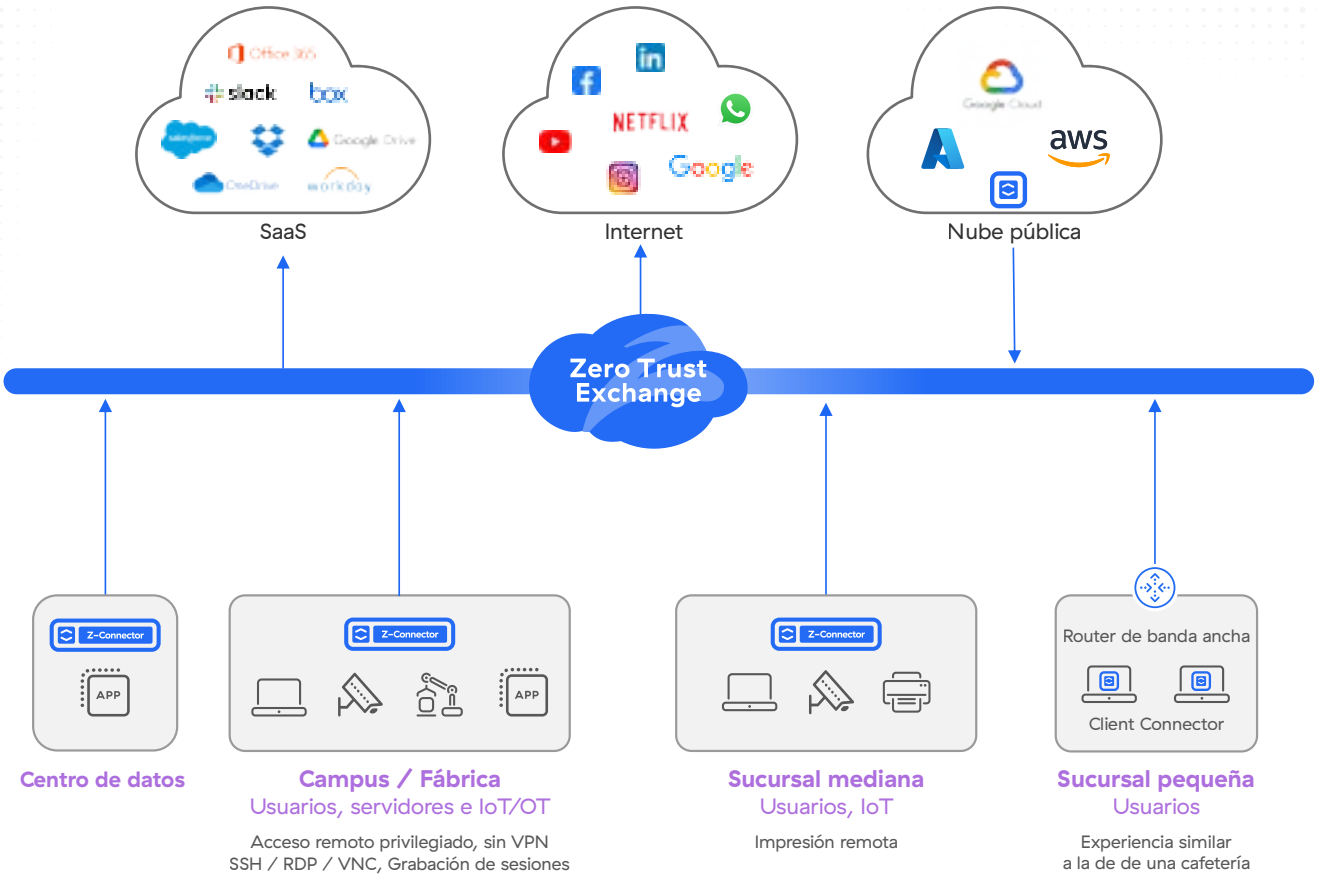

Imagen 1: SD-WAN de confianza cero

SD-WAN de confianza cero 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.

La SD-WAN tradicional no es de confianza cero

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, entre los que se incluyen:

- **Mayor riesgo de amenazas laterales y ataques basados en Internet** debido al uso de soluciones de conectividad heredadas centradas en la red, como las VPN de sitio a sitio, los cortafuegos o las SD-WAN tradicionales. Estas soluciones extienden excesivamente la red confiable de un cliente a través de Internet a otras nubes y entornos locales, lo que aumenta la superficie de ataque. Un mosaico de dispositivos, herramientas y políticas no estándar de seguridad conducen a un mayor riesgo de seguridad debido a brechas conocidas y desconocidas en la cobertura de seguridad.

© 2023 Zscaler, Inc. Todos los derechos reservados.

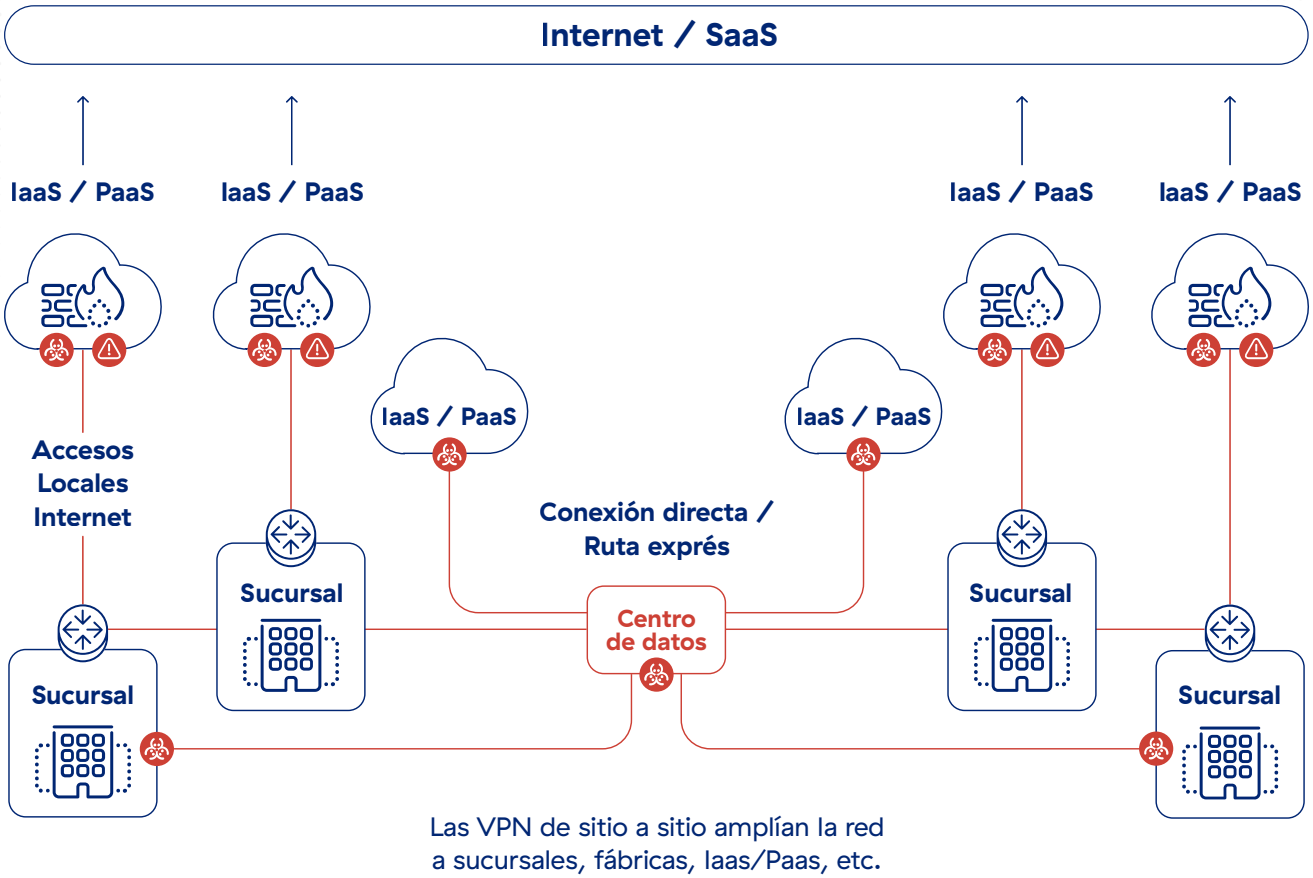

Imagen 2: Mayor riesgo de amenazas laterales y ataques basados en Internet con las SD-WAN tradicionales

- **Mayor complejidad** debido al enrutamiento complejo, los múltiples saltos de red y dispositivos, y la gestión de políticas fragmentada derivada de la introducción de modelos heredados en la nube. Gestionar esta complejidad es una tarea difícil para los equipos de redes y seguridad mientras se esfuerzan por estandarizar la conectividad y hacer cumplir las políticas 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 dentro de entornos de sucursales y centros de datos, los bucles invertidos de tráfico y los puntos de estrangulamiento para la inspección y el control de seguridad centralizados.
- **Altos costes** debido a los dispositivos de seguridad y redes heredados (por ejemplo, cortafuegos, IPS, enrutadores y otros productos puntuales), el sobreaprovisionamiento de servicios de red para compensar la falta de escalabilidad y el mayor uso de servicios nativos de la nube.

© 2023 Zscaler, Inc. Todos los derechos reservados.

Cómo funciona la SD-WAN de confianza cero

La SD-WAN de confianza cero permite a las organizaciones crear una sucursal menos sobrecargada al eliminar múltiples productos como enrutadores, cortafuegos y VPN con un dispositivo simple plug and play que se puede implementar rápidamente usando solo una conexión a Internet. Esto permite a las organizaciones reducir la complejidad asociada con la administración 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 de políticas sencilla mediante el uso del marco de políticas probado de ZIA y ZPA.

El tráfico de las sucursales se reenvía de forma segura directamente a Zero Trust Exchange, donde se pueden aplicar políticas ZIA o ZPA para una inspección de seguridad completa y un control de acceso basado en la identidad de las comunicaciones de las sucursales y del centro de datos. El tráfico de aplicaciones confiables se puede enviar directamente a través de Internet con una conexión directa. Este enfoque exclusivo ofrece tres ventajas fundamentales:

- Deja 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 con el fin de lograr una verdadera seguridad de confianza cero.
- Elimina la arquitectura heredada de castillo y foso sin comprometer la seguridad; no se necesitan productos heredados como proxies Squid, pasarelas NAT, IPS, etc.
- Proporciona conectividad distribuida y escalable dondequiera que sea necesaria, con gestión de políticas centralizada y automatizada para simplificar las comunicaciones de sucursales y centros de datos.

Casos de uso de SD-WAN de confianza cero

Reemplazo de VPN de sitio a sitio

Conecte sucursales directamente a aplicaciones privadas sin extender su WAN ni depender de las VPN, lo que aumenta la superficie de ataque de una red. Las aplicaciones están ocultas tras las sucursales para que no se puedan detectar y el acceso se restringe a través de Zero Trust Exchange a un conjunto de entidades nombradas. 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 distintas es un desafío y requiere mucho tiempo. Los problemas que pueden encontrarse van desde superposiciones de IP y problemas de enrutamiento hasta un mayor riesgo de seguridad debido a una superficie de ataque de red ampliada. Con la SD-WAN de confianza cero, las redes pueden permanecer separadas y las sucursales de un entorno pueden conectarse rápidamente a aplicaciones privadas de otro, sin interrupciones.

Habilitación del acceso directo a Internet para sucursales

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

© 2023 Zscaler, Inc. Todos los derechos reservados.

Confianza cero para la conectividad de servidores e IoT/OT

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

Descubrimiento y visibilidad del IoT/OT en la sombra

Los equipos de TI se enfrentan a puntos ciegos a medida que dispositivos no autorizados y no detectables se conectan a las redes de las sucursales. El resultado es un aumento de la vulnerabilidad del dispositivo y una superficie de ataque más amplia. Zscaler identifica y clasifica dispositivos para brindar a los equipos de TI una visibilidad más profunda de los comportamientos para aplicar mejores políticas de control de acceso.

Dispositivos Z-Connector Plug & Play

Característica	ZT 400	ZT 600	ZT 800	ZT VM
				Z-Connector
Acción de Política	Sucursales pequeñas a medianas	Sucursal pequeña a mediana	Sucursal mediana a grande	Sucursal y centro de datos
Rendimiento/hipervisor	200 Mbps	500 Mbps	1 Gbps	KVM, ESXi
Puertos físicos	4 GbE	6 GbE	8 GbE	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	✓	✓	✓	✓

© 2023 Zscaler, Inc. Todos los derechos reservados.

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 para enviar el tráfico a ZIA, ZPA o directamente a través de Internet • 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 IoT/OT y servidores
Alta disponibilidad	• Dos instancias de SD-WAN de confianza cero que funcionan en modo HA brindan soporte adicional para ráfagas de tráfico y redundancia en caso de un error de hardware. • Tolerancia a errores activa-pasiva utilizando una dirección IP virtual (VIP) basada en el protocolo de redundancia de direcciones comunes (CARP) • Circuitos activo-activo (un solo dispositivo) • Circuitos activo-activo (dispositivo dual al equilibrar FHRP)
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. • Integración completa con la infraestructura de Nanolog Streaming Service con opción de transmitir registros a SIEM propiedad del cliente
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
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. Distribuido 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.es** o síganos en Twitter **@zscaler**.

© 2023 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ y otras marcas comerciales que aparecen en **zscaler.es/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/o en otros países. Cualquier otra marca comercial es propiedad de sus respectivos propietarios.

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