Plan de regreso a la oficina: modernizar el lugar de trabajo con Zero Trust

DOCUMENTO TÉCNICO

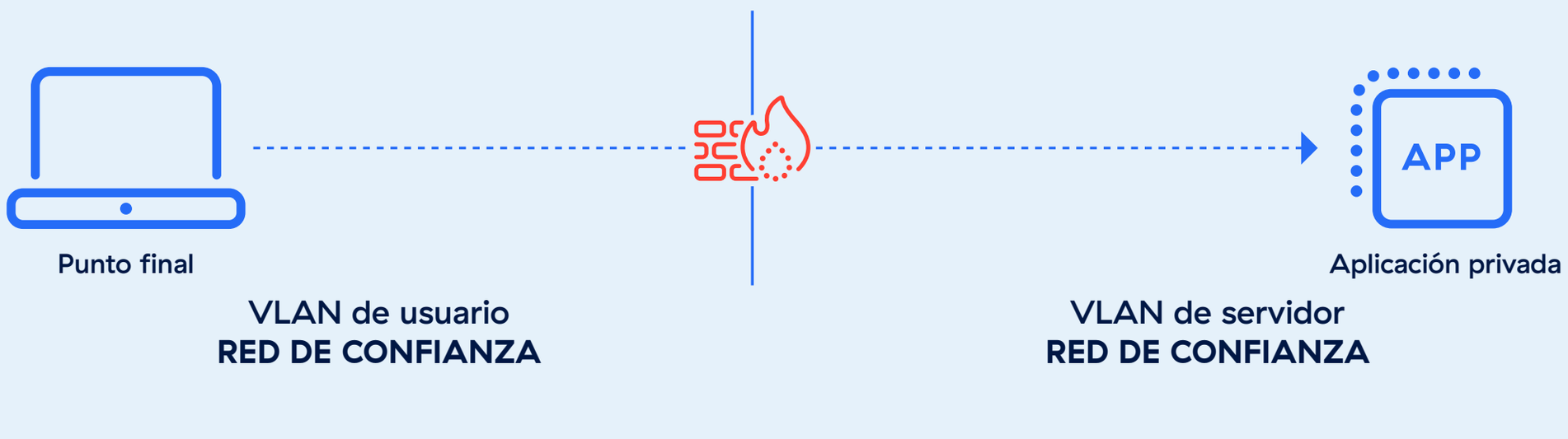
Regresar a la oficina no es volver al pasado. Puede que los empleados estén regresando a las oficinas, pero las aplicaciones y los datos, no. Años de trabajo remoto e híbrido han fomentado la dependencia y la familiaridad de los empleados con las aplicaciones basadas en la nube. Los empleados que regresan a la oficina esperan la misma (o incluso mayor) confiabilidad y capacidad de respuesta de TI. Volver a "la forma en que siempre lo hemos hecho" no cumplirá con esa expectativa.

La migración de aplicaciones y datos a la nube requiere una nueva perspectiva sobre cómo brindar seguridad local sin afectar la productividad. La seguridad Zero Trust, adoptada inicialmente para permitir el trabajo remoto seguro, tiene las mismas ventajas para el personal local y debería considerarse un facilitador clave del lugar de trabajo moderno.

Seguridad tradicional en la oficina: la confianza en las paredes

Históricamente, las redes corporativas fueron diseñadas como fortalezas, donde se asumía la confianza en cualquier usuario o dispositivo que operara dentro de las paredes físicas de la oficina, dentro del "perímetro" de seguridad. Este modelo funcionó cuando los sistemas de oficina eran estáticos y todos estaban conectados a la misma infraestructura.

En el modelo tradicional de seguridad de red basado en perímetro, la conexión a la oficina de la agencia coloca el dispositivo de la estación de trabajo en la red confiable:



En el modelo tradicional, conectarse a la red implicaba acceso a todas las aplicaciones, recursos y datos disponibles en esa red. Para ayudar a mitigar las preocupaciones relacionadas con que un usuario o dispositivo no autorizado se conecte a la red de confianza, puede implementarse una herramienta como el Control de Acceso a la Red (NAC) para gestionar el acceso a la red; por ejemplo, no permitir que un dispositivo no confiable se conecte a menos que tenga un certificado emitido por la PKI de la agencia.

Este es un buen paso, pero deja mucho que desear en un modelo de seguridad de acceso con segmentación y mínimos privilegios, como el que ofrece el enfoque de red confiable:

- Acceso amplio y sin restricciones
- Controles limitados y granulares
- Vulnerabilidades de la red interna

Estos atributos de un enfoque de red confiable (la suposición de amplios privilegios de acceso, la segmentación limitada y la capacidad inherente de descubrimiento de las redes internas) ya no se alinean con las realidades del panorama de amenazas avanzadas de la actualidad. En un mundo de ciberataques cada vez más sofisticados, amenazas internas y proliferación de herramientas de acceso remoto, los modelos de seguridad basados en el perímetro no logran abordar las vulnerabilidades modernas. Los atacantes explotan las deficiencias de las arquitecturas heredadas eludiendo controles de segmentación débiles y obteniendo movimiento lateral una vez dentro de la red, a menudo utilizando credenciales legítimas para evitar ser detectados. Esta realidad requiere un cambio de paradigma en el modo en que las organizaciones abordan la seguridad, pasando de una red de "confianza por defecto" a una que opera con principios Zero Trust: verificar y validar cada intento de acceso de forma dinámica, en todos los usuarios, dispositivos y aplicaciones.

En cambio, las organizaciones necesitan un enfoque que:

- Limita el alcance del acceso con conexiones granulares específicas de la aplicación
- Introduce la aplicación dinámica de políticas basadas en la identidad y la postura del dispositivo.
- Permite una evaluación continua con análisis en cada acceso.

Esta no es una arquitectura pensada para el futuro. Ya está disponible con la arquitectura de red Zero Trust (ZTNA), diseñada para respaldar el trabajo remoto.

Lugar de trabajo con Zero Trust

A medida que los empleados comenzaron a trabajar desde cualquier lugar, las aplicaciones se trasladaron a la nube y las suposiciones tradicionales sobre la confianza se desmoronaron. El enfoque Zero Trust, que reemplaza "asumir confianza" por "verificar siempre", se convirtió en la opción más efectiva para brindar a los usuarios el acceso que necesitaban.

En el contexto del regreso a la oficina, la seguridad Zero Trust, adquiere una nueva urgencia. En los últimos años, la mayoría de las aplicaciones y los servicios de TI se han trasladado a la nube, impulsando mejoras en la productividad y la eficiencia operativa. Volver a prácticas obsoletas, previas a la nube y basadas en el perímetro, es contraproducente e incompatible con el lugar de trabajo moderno.

La seguridad Zero Trust es más que una mejora de la seguridad: es una oportunidad estratégica para reimaginar y preparar la oficina moderna para el futuro. Un enfoque Zero Trust aumenta la agilidad, la escalabilidad y el ahorro de costes de las organizaciones. Ya sea que se trate de establecer una nueva sucursal, construir centros de colaboración temporales o administrar equipos híbridos, la seguridad Zero Trust elimina la necesidad de costosas instalaciones de red como MPLS o soluciones administradas por empresas de telecomunicaciones. También reduce la dependencia innecesaria de complejas infraestructuras de seguridad locales.

Lo más importante es que la seguridad Zero Trust garantiza la relevancia. a medida que las herramientas y los flujos de trabajo continúan evolucionando, las organizaciones con una base Zero Trust pueden integrar sin problemas nuevas tecnologías sin verse limitadas por configuraciones de red obsoletas. Pueden liberarse de los firewalls y otros dispositivos heredados para siempre y preparar su estrategia de seguridad para el futuro.

Los usuarios han vuelto a la oficina, pero sus aplicaciones no.

Hoy en día, la mayor parte del trabajo se realiza a través de aplicaciones basadas en la nube, incluso para los empleados que trabajan en la sede de la empresa. La oficina ya no es el centro de todo lo relacionado con TI. En verdad, los trabajadores de oficina modernos no se diferencian de los empleados remotos en cuanto al modo en que acceden a los recursos.

Este cambio fundamental ha planteado varios desafíos:

- **Las oficinas como cuellos de botella en la conectividad:** los usuarios que regresan a la oficina a menudo reenvían el tráfico hacia la nube a través de la red corporativa, lo que genera latencia e incidentes innecesarios.

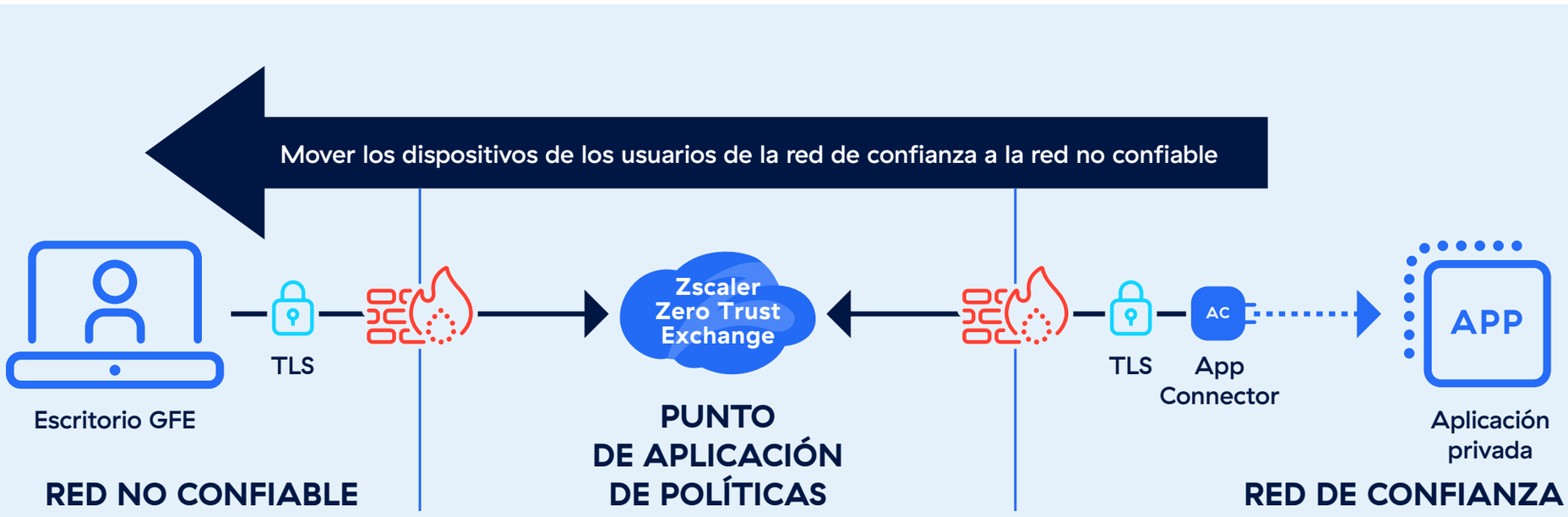
- **Peor experiencia de usuario:** los empleados pueden notar un peor rendimiento de las aplicaciones al trabajar desde la oficina en comparación con sus configuraciones remotas. El problema no siempre reside en la red; puede deberse a cualquier cosa, desde una resolución DNS lenta hasta una conexión Wi-Fi mal optimizada. Pero sin visibilidad, identificar la causa raíz resulta casi imposible para el equipo de TI.

- **Herramientas de supervisión inconexas:** los sistemas de supervisión tradicionales a menudo se centran en la disponibilidad de la red en lugar de en las métricas de experiencia real del usuario, como el rendimiento de la aplicación, la latencia o el estado del punto final.

Repensando las redes de oficinas

Imagine un modelo de Internet "estilo café", donde los empleados se conectan a Internet tal como lo harían desde casa. Si bien esta perspectiva puede ser un cambio radical, la logística para lograrlo ya está disponible con la arquitectura de red Zero Trust.

En este escenario, no existe presunción de confianza al conectarse a la red. Como resultado, las estaciones de trabajo de los usuarios ya no se consideran confiables, sino que ahora están protegidas exactamente de la misma manera que un usuario que trabaja desde casa, utilizando las mismas políticas de acceso.



En última instancia, ingresar a la oficina de una agencia y conectarse a la red no debería proporcionar a los usuarios más acceso a aplicaciones o recursos del que tendrían si trabajaran a través de su ISP doméstico. La red debe funcionar únicamente como medio de transporte, sin otorgar ningún privilegio presunto.

El acceso y la autorización se basan en la identidad, el dispositivo y la aplicación (no la dirección IP) a la que se accede. Un punto de aplicación de políticas (y no las listas de control de acceso (ACL) del firewall de red) arbitra cada decisión de acceso y determina, según las políticas establecidas, qué usuarios pueden acceder a qué aplicaciones y desde qué dispositivos, basándose en el principio de "necesidad de saber".

Este cambio en la arquitectura requiere un cambio en la forma de pensar.

1. **Ampliar las políticas de acceso a los usuarios locales:** la política de acceso sigue al usuario, no a la red a la que está conectado.

2. **Pasar del acceso a la red al acceso a los recursos:** con Zero Trust, los usuarios acceden directamente a las aplicaciones mediante conexiones basadas en políticas e identidades. Esto elimina la necesidad de otorgar acceso generalizado a la red.

3. **Trate la red de oficina como si fuera Internet:** el Wi-Fi de la oficina se convierte en un "Internet estilo cafetería" que simplemente conecta a los usuarios con Zero Trust Exchange, donde las políticas de seguridad asumen el control. Sin tráfico entrante. Sin confianza implícita.

4. **Validación de confianza continua:** Zero Trust evalúa cada solicitud de acceso de forma dinámica, supervisando la postura del dispositivo, el contexto y las señales de riesgo.

La belleza de Zero Trust radica en su capacidad para ofrecer coherencia. Los empleados no necesitan preocuparse de si trabajan "en sus instalaciones" o "de forma remota". Acceden a las aplicaciones de la misma manera sin importar dónde estén trabajando. Esta experiencia unificada no solo garantiza que los usuarios sigan siendo productivos, sino que también simplifica la administración de TI.

Visibilidad mejorada

Un marco sólido Zero Trust garantiza una productividad fluida y al mismo tiempo elimina los riesgos que plantean la confianza implícita y la infraestructura obsoleta. La visibilidad surge como una capacidad crítica, a la par de la identidad, la postura del dispositivo y el control de aplicaciones, para optimizar el rendimiento y resolver problemas rápidamente. La visibilidad permite a los equipos de TI optimizar la entrega de aplicaciones directamente a los usuarios, así como reducir el tiempo de inactividad y solucionar problemas más rápidamente al limitar las causas raíz. La visibilidad desde el punto final hasta el destino proporciona resoluciones rápidas, ya que los administradores pueden ver si el problema es local para el usuario, el transporte o el destino en la nube en sí.

Considere estos escenarios al regresar a las oficinas compartidas:

- **El dilema del Wi-Fi en la oficina:** un empleado que regresa a la oficina conecta su portátil a la red Wi-Fi corporativa. De repente, experimenta una alta latencia al usar Microsoft Teams, una aplicación que funcionaba perfectamente en casa con una simple conexión de banda ancha. ¿Se trata de un problema de cobertura Wi-Fi? ¿De un retraso en el DNS? ¿O de un fallo en el propio servidor de Teams?

- **Latencia de SaaS en la red de retorno corporativa:** un usuario intenta acceder a un CRM basado en SaaS, como Salesforce, desde su escritorio. El tráfico en la nube se fuerza a través de la red corporativa, lo que genera latencia debido a la ruta de retorno.

- **Brechas de visibilidad para fuerzas de trabajo híbridas:** una organización global lucha por lograr una visibilidad constante del estado de los dispositivos, así como del rendimiento de SaaS e ISP, tanto para empleados remotos como locales, lo que genera frecuentes tickets de problemas que consumen valiosos ciclos de TI.

Un elemento clave para lograr una oficina Zero Trust es garantizar la supervisión de la experiencia digital como parte integral de la arquitectura Zero Trust.

¿Por qué Zero Trust Office?

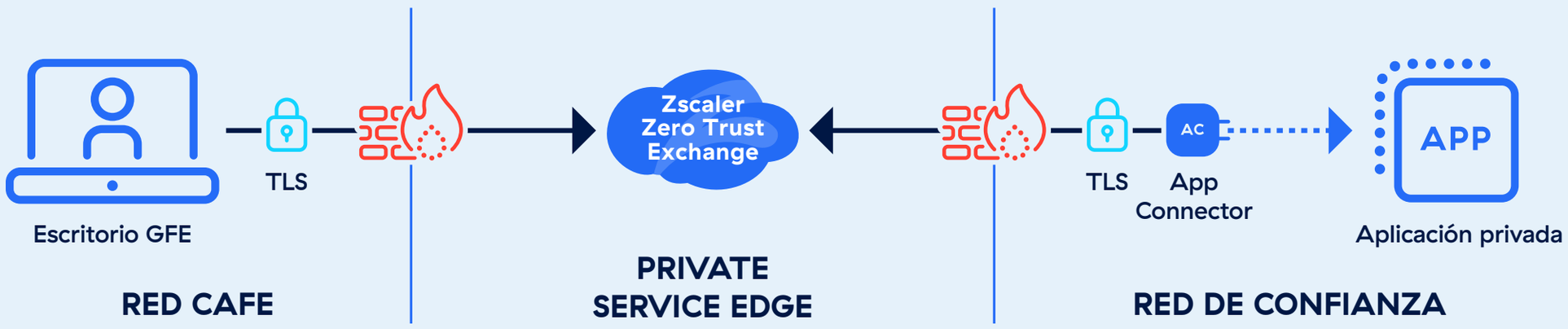
Zscaler ya es un socio comprobado para las organizaciones gubernamentales que abordan esfuerzos de modernización. Como proveedor líder de servicios de seguridad en la nube, Zscaler cuenta con la confianza de 14 de las 15 agencias de nivel ministerial, incluidas el DHS, el DOJ y la GSA, para proteger las redes, simplificar las operaciones y generar ahorros de costes. Estamos protegiendo a millones de usuarios en cientos de instituciones en todos los niveles de gobierno.

Zscaler for Users abarca tres áreas funcionales destinadas a reducir el riesgo, mejorar la productividad y disminuir los costes y la complejidad.

- **Acceso seguro a Internet y SaaS (ZIA):** el punto de acceso de sus usuarios a Internet y a todas las aplicaciones, que los protege contra amenazas avanzadas y pérdidas de datos.

- **Acceso seguro a aplicaciones privadas (ZPA)** garantiza que los usuarios se conecten a través del Private Service Edge local, gestionando la conexión de datos a una aplicación privada mediante la red de la agencia, sin necesidad de salir a Internet y regresar.

- **Experiencia de usuario digital (ZDX):** proporciona visibilidad crítica de las experiencias digitales de los usuarios, proporcionando métricas desde el punto final hasta la aplicación SaaS, lo que garantiza la excelencia operativa dentro y fuera de la oficina.



Modernización del lugar de trabajo facilitada por Zero Trust

A medida que el lugar de trabajo evoluciona, la definición de “oficina” se vuelve cada vez más irrelevante. Ya sea que los usuarios trabajen desde oficinas tradicionales, hogares o estén en movimiento, su experiencia debe seguir siendo fluida y segura.

A medida que los empleados regresan a la oficina, las organizaciones tienen una oportunidad única de modernizar la infraestructura de su lugar de trabajo. Construir sobre una base Zero Trust garantiza no solo una mayor seguridad, sino también escalabilidad, agilidad y resiliencia a largo plazo. Esta es la visión de la oficina Zero Trust plenamente realizada: un entorno donde la productividad prospera.

La oficina Zero Trust es fácilmente alcanzable hoy en día. Al aplicar los mismos principios utilizados para el teletrabajo a las operaciones en la oficina, las organizaciones pueden reducir significativamente el riesgo, mejorar la experiencia del usuario y crear una arquitectura de seguridad preparada para el futuro.

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 ciberataques y de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados 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 línea en la nube del mundo. Para obtener más información, visite **www.zscaler.com/es** o síganos en Twitter**@zscaler**.

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

zscaler™

Zero Trust Everywhere