Acceso de confianza cero a aplicaciones privadas desde dentro y fuera de la oficina con Zscaler™

Hemos visto a miles de organizaciones adoptar con éxito el trabajo desde cualquier lugar, superando muchos desafíos en torno a la protección de datos, el acceso remoto seguro y la ampliación de recursos para permitir la continuidad empresarial. Sin duda, muchos se vieron sorprendidos por la urgencia y la rapidez necesarias para hacer que la mayoría del personal de oficina pasase a ser personal remoto a tiempo completo, pero en medio del caos muchos recurrieron a los servicios de confianza cero para acceder a los recursos empresariales como alternativa a los métodos tradicionales centrados en la red. Ahora, cuando los equipos de TI comienzan a planificar para los próximos años, muchos se preguntan cómo será el futuro del trabajo y si el trabajo desde casa o el híbrido (en la oficina y hogar), ha llegado para quedarse.

zscaler™

Desde el punto de vista de la seguridad, los usuarios que se conectan desde sus equipos portátiles dentro y fuera de la oficina pueden aumentar los riesgos de seguridad, especialmente si los usuarios se consideran de confianza automáticamente y tienen acceso a la red. Desde el punto de vista del usuario, acceder debe ser igual de fácil trabaje donde trabaje.

Tres consideraciones para los equipos de TI en el futuro

Aunque los gobiernos locales están tomando las medidas adecuadas para volver a abrir las ubicaciones físicas, hay tres elementos clave que un líder de seguridad y/o red debe considerar antes de hacerlo.

1 Proporcione acceso de confianza cero a aplicaciones privadas desde cualquier ubicación

Muchas empresas cometen el error de pensar que la confianza cero es solo clave cuando se proporciona acceso remoto a aplicaciones privadas. Utilizan servicios de confianza cero como alternativa a las tecnologías de acceso remoto, como la VPN o la VDI, que colocan a los usuarios en la red. La mayoría de los empleados de la oficina pueden conectarse a los recursos de la red debido a que el usuario ya está dentro del perímetro y es de confianza implícita. El equipo puede haber implementado la segmentación de la red como una medida de seguridad adicional, lo que hace que la red sea extremadamente compleja. Dicho esto, la segmentación de red ya no es necesaria si se utilizan los servicios de confianza cero adecuados. El mismo servicio de confianza cero se puede utilizar cuando un usuario trabaja en remoto o cuando está en la oficina, y se puede utilizar para proporcionar un nivel de segmentación de la aplicación, sin la necesidad de administrar o lidiar con la complejidad de la segmentación de la red en las instalaciones.

2 Ofrezca la mejor experiencia de usuario posible priorizando la consistencia

Varias encuestas han demostrado que tanto empleadores como empleados se sienten cómodos trabajando a distancia. Muchas organizaciones indican que la productividad continúa aumentando a pesar de que su personal principal trabaje a distancia, mientras que los empleados, con más frecuencia que nunca, gozan de la flexibilidad de poder trabajar desde cualquier lugar. Es por eso que varios clientes con los que hablamos se inclinan hacia un modelo híbrido de trabajo en el que los empleados dividen su tiempo entre la oficina y el hogar. Por lo tanto, los responsables de la red y la seguridad deben garantizar que los empleados tengan una experiencia fluida y homogénea al acceder a las aplicaciones desde cualquier lugar, incluso en la oficina.

3 Evite que los dispositivos sin validar accedan a la red corporativa

También es clave la creciente popularidad de los servicios de seguridad de puntos finales, como CrowdStrike, Microsoft y Carbon Black, durante la realización de tareas de forma remota. Durante un tiempo, los usuarios de ordenadores portátiles y smartphones han estado accediendo a las aplicaciones desde casa en sus redes personales. Puesto que esos mismos dispositivos se llevan a la oficina, es importante que los líderes de TI no les permitan entrar en la red corporativa. En su lugar, TI debe asegurarse de que todos los dispositivos que regresan a la oficina estén limpios, para reducir la superficie de ataque general y minimizar las amenazas. Por lo tanto, comprender la postura y el estado del dispositivo es una consideración clave, especialmente a medida que el concepto de trabajo híbrido comienza a tomar forma.

Utilizar la confianza cero para trabajar dentro y fuera de la oficina

La confianza cero se basa en dos elementos fundamentales: la identidad y las políticas empresariales.

En lugar de usar una dirección IP, la identidad proporciona el contexto para saber quién es el usuario. Las políticas empresariales, establecidas por el equipo de red o de seguridad, determinan a qué aplicación privada puede acceder un usuario autorizado. La plataforma Zscaler Zero Trust Exchange™ aloja estas políticas, las aplica y, si se permite, realiza la conexión de aplicación a usuario de forma individual, por aplicación y por sesión.

Dado que la ubicación de los usuarios seguirá cambiando, ya no es necesario hacer hincapié en la red. A medida que los usuarios se preparan para volver a la oficina, es aún más esencial romper con la confianza implícita y aplicar políticas de confianza cero. El acceso a la red de confianza cero garantiza la seguridad, la velocidad, la coherencia y la comodidad para los usuarios, y proporciona flexibilidad y escalabilidad para el departamento de TI.

Zscaler Private Access para el acceso de empleados de la oficina o remotos a aplicaciones privadas

Zscaler Private Access™ (ZPA™) es un servicio en la nube de Zscaler que proporciona un acceso sin fisuras de confianza cero a las aplicaciones privadas que se ejecutan en la nube pública o dentro del centro de datos. Es compatible con aplicaciones heredadas y con aplicaciones basadas en la web. El servicio usa información de un proveedor de ID basado en SAML, y conecta al usuario autorizado a una determinada aplicación según las políticas empresariales definidas por el cliente. A diferencia de VPN o VDI, esto se logra sin colocar al usuario en la red corporativa, lo que elimina la necesidad de la pila de la puerta de enlace entrante. El servicio nunca expone la aplicación a Internet, lo que hace que la aplicación sea invisible para los atacantes, algo especialmente importante para el acceso remoto.

ZPA utiliza túneles internos cifrados (uno desde la aplicación y otro desde el usuario) y, a continuación, realiza las conexiones en tiempo real dentro de una de sus ubicaciones de perímetro de servicio en función de la ubicación del usuario y del dispositivo. Esto se hace de tal manera que se garantiza la ruta de usuario a aplicación más rápida posible y elimina la necesidad de hacer revisiones en una ubicación central del centro de datos. El perímetro del servicio está alojado públicamente por Zscaler o alojado de forma privada por el cliente, en cuyo caso se extiende a la sucursal local del cliente o al centro de datos para su aplicación local. En cualquier caso, los perímetros de servicio son gestionados por Zscaler.

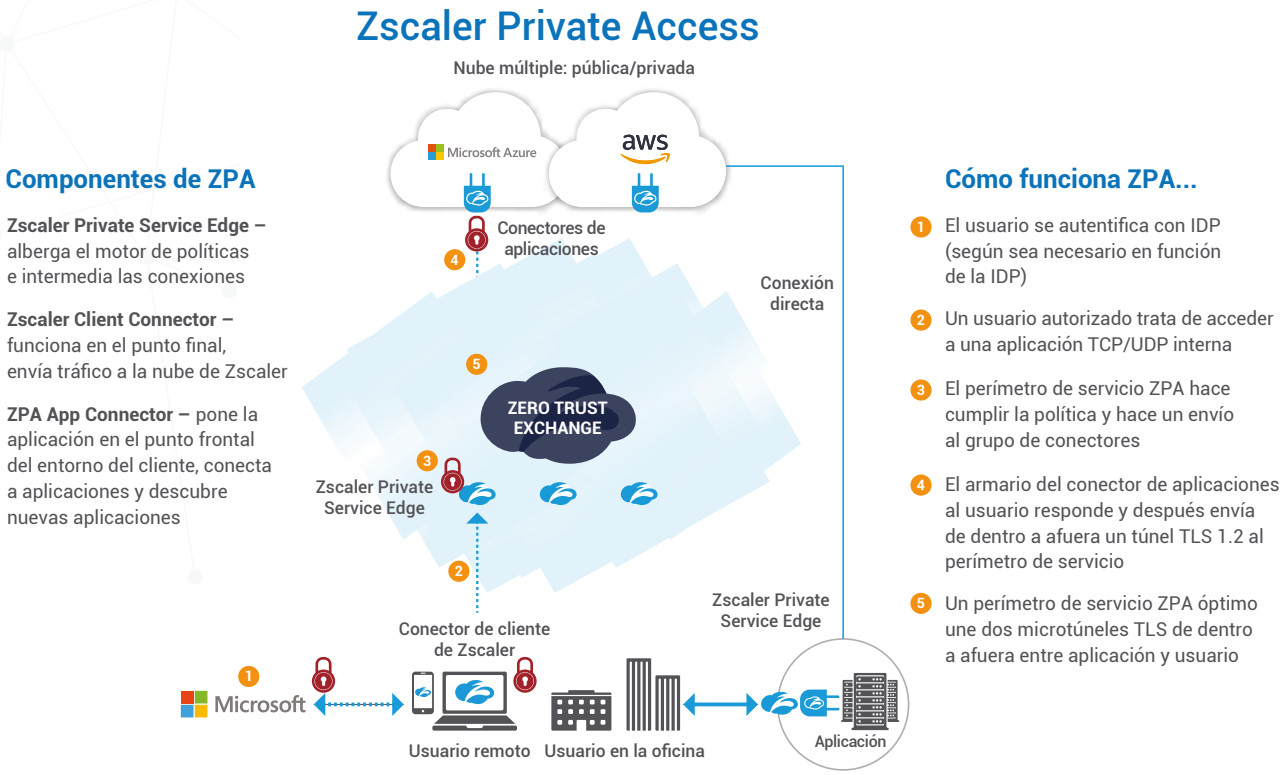
Dado que el servicio se conecta por usuario y por aplicación, proporciona una segmentación de las aplicaciones sin necesidad de segmentación de la red. Esto simplifica la segmentación, lo que permite a TI definir políticas por nombre de usuario y nombre de host en lugar de hacerlo por IP de origen e IP de destino.

ZPA utiliza túneles internos cifrados (uno desde la aplicación y otro desde el usuario) y, a continuación, realiza las conexiones en tiempo real dentro de una de sus ubicaciones de perímetro de servicio en función de la ubicación del usuario y del dispositivo.

La misma ventaja de la arquitectura de confianza cero, pero alojada en las instalaciones

Para las empresas que prefieren alojar un perímetro de servicio ZPA ellos mismos, hemos introducido ZPA Private Service Edge. ZPA Private Service Edge es una instancia privada de un solo inquilino que proporciona la funcionalidad completa de un ZPA Service Edge público en el propio entorno de una organización. El cliente aloja ZPA Private Service Edge in situ o en un servicio en la nube, y es administrado por Zscaler. ZPA Private Service Edge descarga las políticas y configuraciones relevantes de la nube, a fin de poder aplicar todas las políticas de ZPA de forma local.

Los servicios ZPA Private Service Edge y los servicios clásicos ZPA que aloja Zscaler se pueden utilizar en conjunto. ZPA elegirá automáticamente la ruta más rápida entre el usuario y el destino para eliminar la latencia.



Principales beneficios de ZPA Private Service Edge

Reducción de la complejidad y los costes

Con ZPA Private Service Edge, ya no son necesarios cortafuegos internos ni dispositivos adicionales. Esto no solo reduce los costes, sino también la necesidad de construir segmentos de red complejos para proporcionar acceso a las aplicaciones a los usuarios locales.

Alta disponibilidad

ZPA Private Service Edge almacena en memoria caché las políticas de acceso durante semanas, lo que permite a los usuarios conectarse de forma segura, incluso si se pierde la conexión a Internet. Esto garantiza la disponibilidad continua del acceso a las aplicaciones independientemente de la conectividad.

Experiencias de usuario rápidas

ZPA decide automáticamente cuál ruta es la más corta y rápida para que el usuario se conecte a las aplicaciones, priorizando el perímetro de servicio local de ZPA. Las capacidades de doble acceso en las instalaciones y la intermediación en la nube pública optimizan automáticamente el rendimiento para el usuario, independientemente de dónde se encuentren el usuario y las aplicaciones.

Cumplimiento

Sectores como la banca y los servicios financieros exigen pautas estrictas sobre el uso de servicios basados en la nube. ZPA Private Service Edge ayuda a las empresas a cumplir con estas regulaciones al permitirles alojar el servicio en las instalaciones.

Política centralizada con aplicación local

ZPA Private Service Edge se mantiene al día de las políticas comerciales al conectarse con el servicio en la nube ZPA. Así se garantiza que se aplican todas las políticas y configuraciones relevantes. Por si se produce una interrupción de la conexión a Internet, ZPA Private Service Edge almacena en memoria caché todas las políticas durante 14 días para garantizar que se siga aplicando el acceso de los usuarios locales a las aplicaciones privadas.

ZPA Private Service Edge ofrece una forma más sencilla de permitir el acceso seguro a las aplicaciones privadas y facilita una experiencia idéntica para los usuarios locales o remotos que acceden a las aplicaciones en el centro de datos o en la nube.

¿Quiere saber más sobre ZPA? Póngase en contacto con nuestro equipo en cualquier momento: **sales@zscaler.com**.

Más información sobre **ZPA Private Service Edge**

Solicitar una demo

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 basado en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San José, CA 95134
+1 408.533.0288
www.zscaler.es