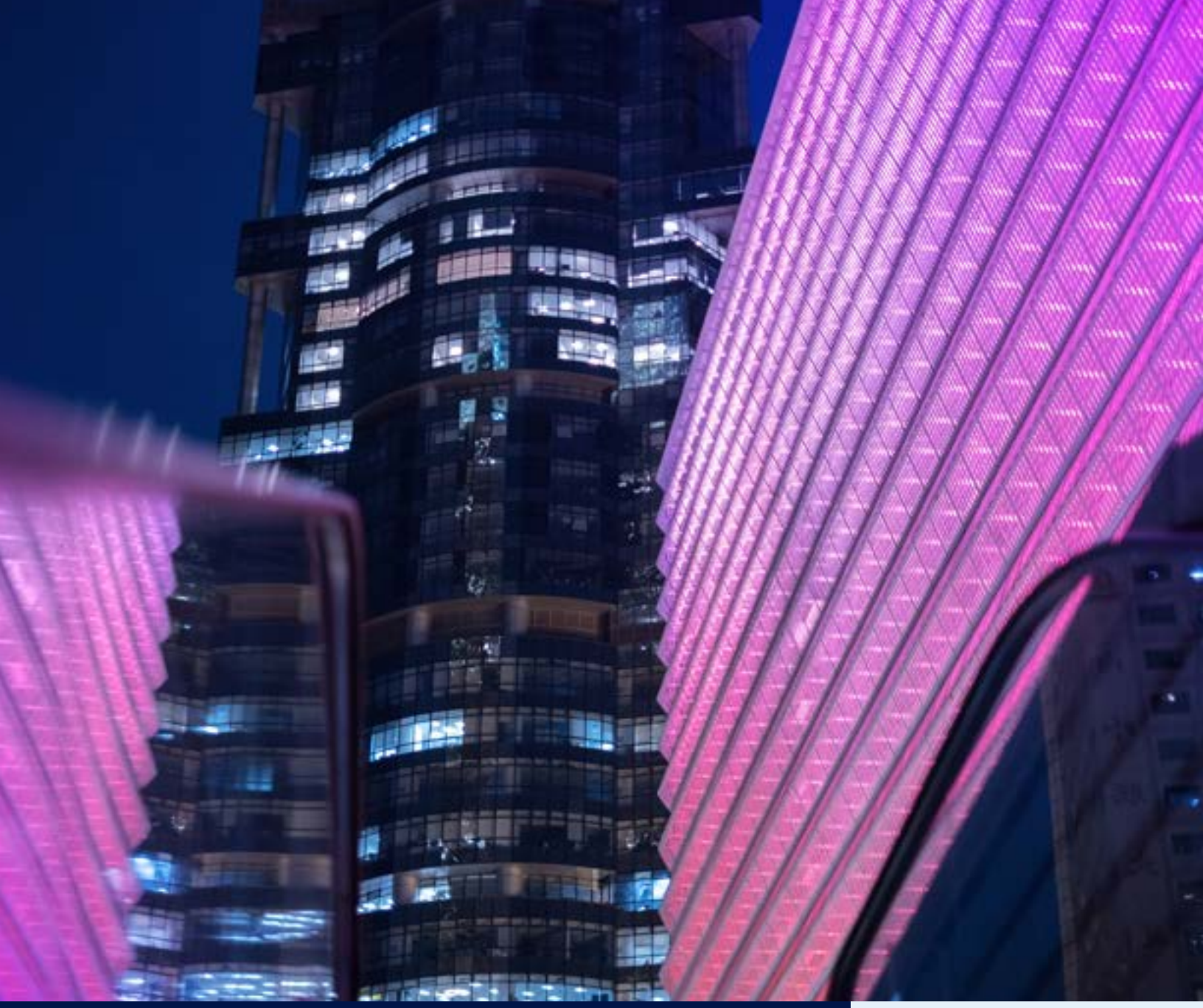


Zscaler Resilience™

Continuidad empresarial ininterrumpida durante blackout, brownout y eventos catastróficos

Resumen de la solución

© 2024 Zscaler, Inc. Todos los derechos reservados.

La continuidad de la actividad es fundamental para los responsables de TI

Nuestro modo de trabajar ha cambiado y, con este cambio, la continuidad empresarial se ha convertido en una prioridad absoluta para los responsables de TI. Ahora, los responsables de TI deben centrarse en prevenir las interrupciones de los servicios de misión crítica y facilitar la continuidad de la productividad como si todo siguiera igual. Con las herramientas, los procesos y la tecnología adecuados, los equipos de TI pueden restablecer rápida y fácilmente la funcionalidad total de sus organizaciones, incluso en caso de desastres.

El cambio hacia los servicios prestados en la nube para el almacenamiento, la informática y la seguridad ha aportado a las organizaciones sistemas flexibles y escalables, mejor continuidad empresarial, reducción de los costos de TI y menor complejidad. Incluso con estas ventajas, las organizaciones buscan optimizar la continuidad empresarial ante eventos catastróficos como desastres naturales, ataques físicos o amenazas de estados-nación.

Zscaler Resilience es un conjunto completo de capacidades de resiliencia que garantiza la continuidad empresarial ininterrumpida para los clientes durante blackout, brownout y eventos catastróficos. Está construido sobre la arquitectura avanzada del Zscaler Zero Trust Exchange™ y mejorado por la excelencia operativa para ofrecer alta disponibilidad y capacidad de servicio a los clientes en todo momento. Las capacidades de recuperación de desastres controladas por el cliente de Zscaler, en combinación con un sólido conjunto de opciones de conmutación por error, respaldan los esfuerzos de planificación de continuidad empresarial de los clientes en todos los escenarios de fallas. Este amplio conjunto de capacidades de recuperación convierte a la nube de seguridad Zscaler en la nube más segura y resistente del sector.

Resiliencia en la nube: ¿Por qué es necesaria?

Los líderes empresariales se focalizan en proporcionar un entorno que propicie la máxima productividad. Los equipos de TI deben permitir la continuidad empresarial y la productividad incluso cuando los problemas de conectividad, los eventos de escalado o los fallas del servicio interrumpan la normalidad de la actividad empresarial.

El tráfico de usuarios a aplicaciones de misión crítica, tanto SaaS como internas y privadas, debe circular siempre para garantizar la continuidad empresarial. Las interrupciones pueden provenir de una falla en la nube o en la conectividad con las aplicaciones. La resiliencia de la nube reúne ambas cosas: la resiliencia de la nube y la resiliencia a la nube.

Resiliencia de la nube
La resiliencia de la nube garantiza que la propia nube está construida sobre una infraestructura eficaz y cuenta con sólidos procesos operativos para las funciones empresariales diarias. La nube de Zscaler gestiona de manera autónoma muchas fallas menores (caída de nodos, problemas de disco, etc.) sin ninguna interacción con el cliente, pérdida de conectividad o disminución del rendimiento. Nuestros robustos sistemas de hardware construidos a medida garantizan que la nube de Zscaler funcione a la perfección.

Resiliencia a la nube
La resiliencia a la nube es un aspecto esencial de una solución integral de resiliencia a la nube. La conectividad a la nube depende de su disponibilidad y de los medios de conexión para que los usuarios puedan llegar a las aplicaciones o los datos. Cuando se interrumpe el acceso a la nube, es necesario encontrar una ruta alternativa y óptima para llegar a las aplicaciones. Esta optimización representa una colección de acciones manuales o autónomas que pueden aplicarse para hacer frente a fallas que van desde una caída en el rendimiento de la red hasta interrupciones completas. Zscaler Resilience es un conjunto completo de capacidades que garantiza la continuidad empresarial ininterrumpida para cualquier tipo de fallas, desde fallas menores a fallas catastróficas.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Garantiza la resiliencia de la nube frente a escenarios de fallas

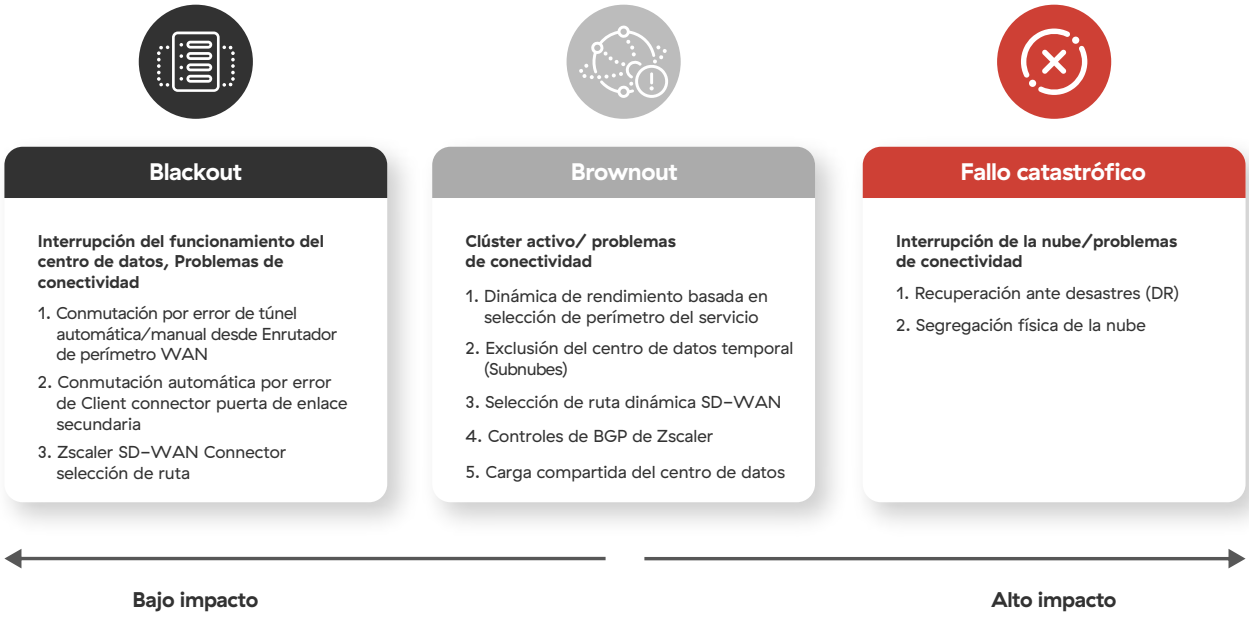


Figura 1: Múltiples opciones para responder a escenarios de fallas

Fallas menores

Los fallas menores incluyen fallas de rendimiento, problemas de compatibilidad y problemas operativos o de calidad que no son fallas graves o críticas, las caídas de nodos o los problemas de disco podrían ser las razones principales de fallas aisladas. Los fallas menores son los más frecuentes y suelen pasar desapercibidas. Estos fallas pueden provocar ralentizaciones, problemas operativos y pueden frustrar a los usuarios. La resiliente arquitectura en la nube de Zscaler y la excelencia operativa pueden evitarlas. Los fallas menores se gestionan en segundo plano con una interacción mínima con el cliente, al tiempo que se garantiza una productividad continua.

Beneficios clave de Zscaler Resilience

Continuidad del negocio con seguridad ininterrumpida

Aplique políticas de seguridad críticas mientras otorga acceso Zero Trust a Internet, SaaS y aplicaciones privadas, incluso durante catástrofes.

Experiencias sin interrupciones en todos los escenarios de fallas

Gestione blackout, brownout y fallas catastróficas con facilidad aprovechando la mejor arquitectura de su clase y la excelencia operativa del Zscaler Zero Trust Exchange.

Costos y complejidad reducidos

Evite las interrupciones comerciales y las pérdidas de productividad causadas por la falta de acceso a aplicaciones críticas y, al mismo tiempo, elimine los costos de la infraestructura de respaldo heredada y las VPN locales.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Blackout

Las interrupciones de los centros de datos (por ejemplo, la interrupción de enero de 2022 en las instalaciones de Interxion en Londres) o los problemas graves de conectividad, como la interrupción de los proveedores de transporte/tránsito, se consideran escenarios de apagón en los que las organizaciones no pueden reenviar tráfico al centro de datos de Zscaler afectado. Nuestra arquitectura redundante; centros de datos neutrales en cuanto al operador con múltiples proveedores e intercambio de Internet (IX), es muy eficaz para minimizar las interrupciones en caso de pérdida de un único operador y otros problemas de conectividad. Independientemente del tiempo de restablecimiento, el problema para nuestros clientes es la imposibilidad de seguir utilizando los servicios del centro de datos afectado.

Para continuar con la actividad, los clientes deben redirigir el tráfico a un centro de datos secundario cercano de Zscaler. Utilizamos una combinación de operadores y proveedores de centros de datos para mitigar eficazmente las interrupciones de cualquier distribuidor, garantizando que el centro de datos secundario esté disponible. También aprovisionamos más de lo necesario y mantenemos capacidad de reserva en el centro de datos para soportar carga transitoria adicional.

Adoptar la continuidad empresarial consiste en pensar y planificar diferentes escenarios posibles de fallas. La infraestructura de Zscaler es de clase mundial y está diseñada para ofrecer una disponibilidad del 100 %.

Tráfico desde la oficina utilizando un dispositivo SD-WAN Cuando se envía tráfico desde una oficina utilizando un dispositivo de enrutamiento/SD-WAN, los clientes deben seguir las mejores prácticas de implementación de Zscaler teniendo un túnel IPsec/GRE de respaldo listo para funcionar cuando el principal sea inaccesible. La maneera de activar la conmutación por error depende de las capacidades del dispositivo y del diseño de la red. Por ejemplo, una SD-WAN con circuitos de Internet duales podría conmutar por error al túnel de reserva en un circuito secundario automáticamente cuando el túnel activo se vuelva inaccesible o supere un umbral de latencia (con las comprobaciones de estado L7 activadas). En el caso de dispositivos más primitivos, los clientes tendrían que habilitar manualmente el túnel de copia de seguridad. Una vez que el centro de datos primario vuelva a funcionar, es responsabilidad del cliente volver a conmutar.

Tráfico mediante Zscaler Client Connector Cuando se envía tráfico mediante Zscaler Client Connector, Zscaler controla ambos perímetros del túnel y realizará la conmutación por error automáticamente de la puerta de enlace primaria a la secundaria utilizando la lógica del archivo PAC de App Profile. Zscaler Client Connector (ZCC) volverá a la puerta de enlace primaria una vez que sea accesible. En ciertos casos, los clientes pueden optar por modificar manualmente los archivos PAC para activar una conmutación por error.

Brownout

Una caída involuntaria o inesperada de la calidad del servicio de la red suele constituir una brownout. La mala gestión de una brownout puede ser costosa, tanto en términos de pérdida de ingresos como de productividad: si los usuarios informan de una brownout antes de que el equipo de TI la haya descubierto y comenzado a trabajar para resolverla, puede generarse una gran frustración en los usuarios, lo que ralentizará todo. Además de las maneras de solucionar los blackout, Zscaler ayuda a mitigar las brownout de otras maneras que se mencionan a continuación.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Selección dinámica del Service Edge basada en el rendimiento de Zscaler

Zscaler Client Connector selecciona la ruta óptima entre el Service Edge ZIA principal y el secundario, independientemente de la proximidad geográfica, y se basa en el estado de cada Service Edge de ZIA, como se muestra en la figura 2. Una conexión HTTP de extremo a extremo calcula la latencia mediante un ping continuo a ambas puertas de enlace. Con esto, Zscaler ofrece una selección de centro de datos basada en la latencia para abordar eficazmente las brownout.

Exclusión del centro de datos controlada por el cliente

Otra manera de mantener la continuidad empresarial durante las brownout es a través de la selección del centro de datos controlada por el cliente, como se muestra en la figura 3. Cuando un cliente experimenta problemas de capacidad en un centro de datos, como un problema de peering de una aplicación SaaS en LAX (que podría tardar horas en solucionarse), ese centro de datos puede excluirse de la subnube en el portal de administración.

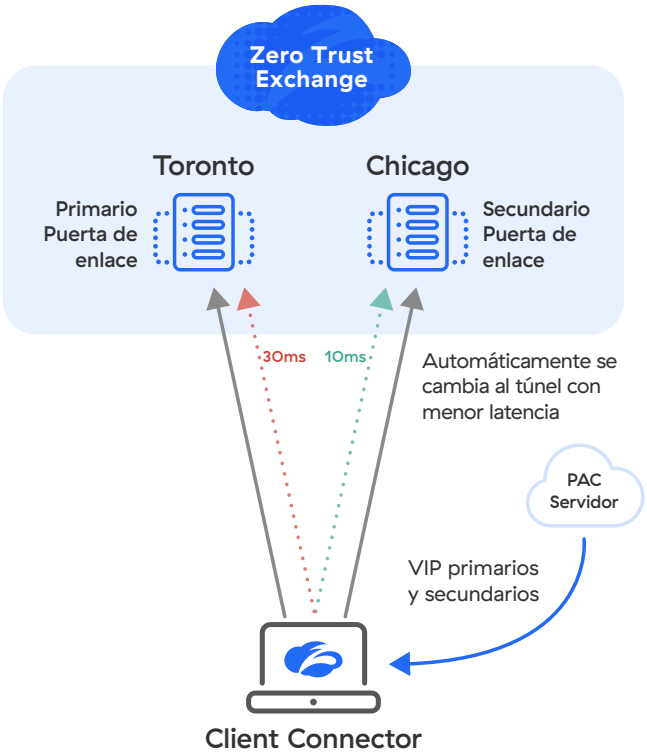


Figura 2: Selección dinámica del perímetro de servicio basada en el rendimiento

Zscaler Client Connector entonces obtiene la nueva puerta de enlace primaria y secundaria y establece un Z-tunnel a un nuevo centro de datos. Esta exclusión del centro de datos controlada por el cliente tiene un límite de tiempo y vuelve a la selección original del centro de datos después de un tiempo predeterminado.

Conmutación por error del túnel desde dispositivos de enrutamiento conscientes de las brownout

Cuando se envía tráfico desde una oficina utilizando un dispositivo de enrutamiento/SD-WAN sobre el que Zscaler no tiene control directo, las opciones de un cliente están limitadas a las capacidades del dispositivo perimetral.Por ejemplo, un enrutador SD-WAN puede detectar la degradación del servicio utilizando algoritmos propietarios basados en comprobaciones de estado L7 a puntos finales de sonda Zscaler. Una vez detectada una posible caída del servicio, el dispositivo SD-WAN puede conmutar automáticamente a un túnel de reserva en el mismo enlace o en un enlace secundario. El dispositivo volverá al túnel primario una vez que las comprobaciones de estado arrojen mejores resultados.

Controles BGP de Zscaler

Nuestra arquitectura redundante, basada en centros de datos neutrales con múltiples proveedores e interconexiones a Internet (IX), es muy eficaz para minimizar las brownout, la congestión u otros problemas con transportistas únicos. Cuando Zscaler CloudOps descubre que un ISP ascendente proporciona un enrutamiento subóptimo, podemos redirigir el tráfico a través de un ISP secundario mientras trabajamos con el principal para resolver el problema.

Distribución de la carga del centro de datos de Zscaler

En caso de congestión de la red u otros problemas de conectividad a un centro de datos en particular, Zscaler puede redirigir proactivamente a los clientes que ejecutan Zscaler Client Connector a centros de datos secundarios en la proximidad geográfica sin utilizar un método estadístico.

© 2024 Zscaler, Inc. Todos los derechos reservados.

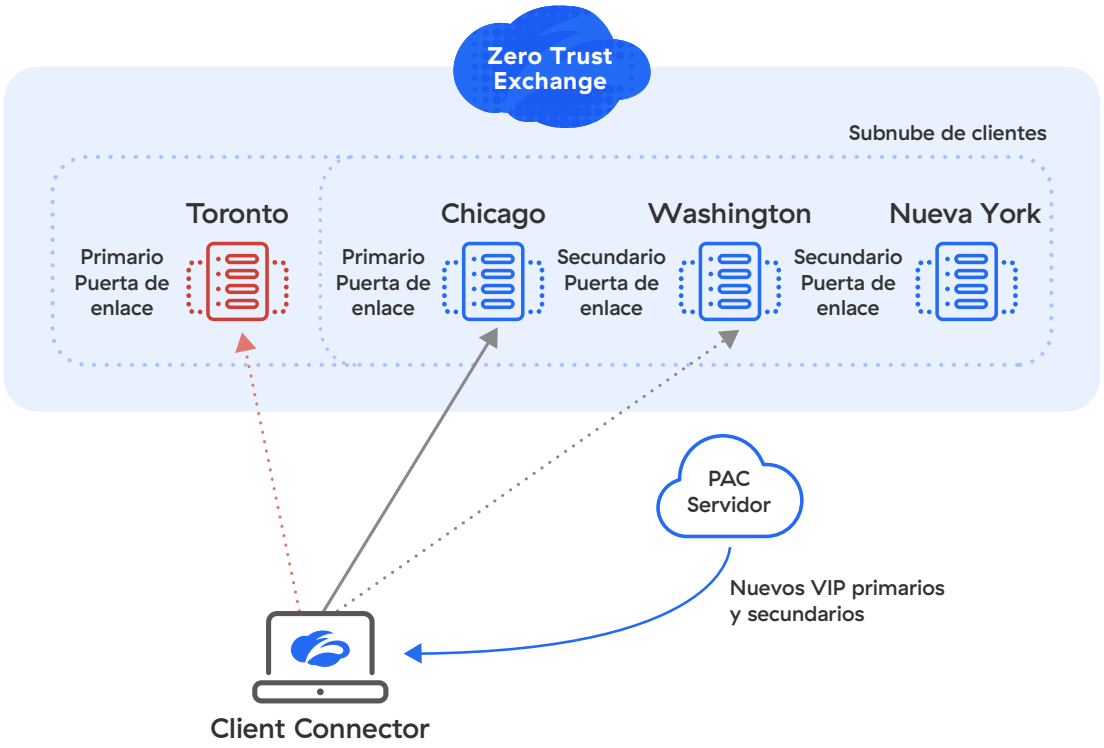


Figura 3: Exclusión del centro de datos controlada por el cliente

Fallas catastróficas

Zscaler Business Continuity para ZIA/ZPA

Zscaler Business Continuity para la nube facilita operaciones ininterrumpidas a los usuarios, garantizando que puedan acceder a las aplicaciones de misión crítica incluso durante un evento de cisne negro.

Las organizaciones necesitan un acceso ininterrumpido a las aplicaciones, sin comprometer la seguridad Zero Trust durante catástrofes o períodos de acceso degradado a la infraestructura. Además, los estándares regulatorios y de cumplimiento para la continuidad empresarial deben cumplirse comúnmente en muchas industrias.

Para satisfacer estas necesidades, Zscaler ofrece la opción de una nube privada para la continuidad empresarial con el fin de mantener operativas a las organizaciones, incluso durante un evento catastrófico que pueda afectar a la nube pública de Zscaler.

Si la nube pública de Zscaler no está disponible o no se puede acceder a ella, los clientes pueden cambiar al modo de continuidad empresarial. En este estado, las políticas y la autenticación de usuarios continúan siendo aplicadas por los servicios de Zscaler, que se ejecutan en una máquina virtual alojada por el cliente.

Business Continuity para ZIA

Con el fin de proporcionar un acceso ininterrumpido a Internet y a las aplicaciones SaaS, y seguir cumpliendo las normativas, Zscaler ofrece la posibilidad de conmutación por error a una nube privada de continuidad empresarial que comprende perímetros de servicio privados ZIA alojados por el cliente, y un caché de políticas privado.

Los PSE ofrecen un procesamiento de tráfico uniforme, con funciones como la inspección de tráfico y el firewall, para los usuarios que ejecutan Client Connector de Zscaler. En caso de interrupción del servicio, estos perímetros de servicio privados se sustentan en un caché de políticas privadas que mantiene una copia en caché de la configuración del cliente.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Para los clientes que no deseen implementar capacidades autoalojadas, la solución estándar de continuidad empresarial de Zscaler permite el acceso continuo a la web y a las aplicaciones SaaS en caso de interrupción del servicio. Los clientes pueden elegir una de las tres opciones en este escenario:

Falla Abierta: Acceso ilimitado a Internet sin restricciones de seguridad

Lista de permitidos predefinida: Acceso sin restricciones a un conjunto limitado de aplicaciones comunes

Cerrado a prueba de fallas: todo acceso a Internet queda bloqueado mientras se mantenga la interrupción.

Continuidad empresarial para ZPA

Para tener acceso ininterrumpido a aplicaciones privadas durante una interrupción, los clientes pueden optar por implementar su propia nube privada de continuidad empresarial, que son agrupaciones lógicas de los siguientes componentes, cada uno de los cuales se puede implementar en un grupo para redundancia adicional:

Controladores de nube privada que sincronizan continuamente la configuración y las políticas con la nube de Zscaler,

Perímetros de servicio privados de ZPA que proporcionan funcionalidad ZPA pública en el entorno de una organización

App Connectors para acceso seguro a servicios privados

Receptores de registro para capturar salidas de registro de otros componentes

En caso de una interrupción catastrófica o de que la nube Zscaler quede inaccesible, los usuarios se conectarán automáticamente a los Private Cloud Controllers para autenticarse y redirigirse a los perímetros de servicio privados de ZPA. Una vez conectado al PSE, el canal de control y de datos será con el PSE de ZPA.

Los controladores de la nube privada, implementados como una máquina virtual, proporcionan funciones críticas en caso de interrupción:

- Redirección de autenticación
- Redirección de usuarios
- Servicio de transmisión de registros
- Sincronización de la configuración del cliente
- Sincronización de políticas del cliente

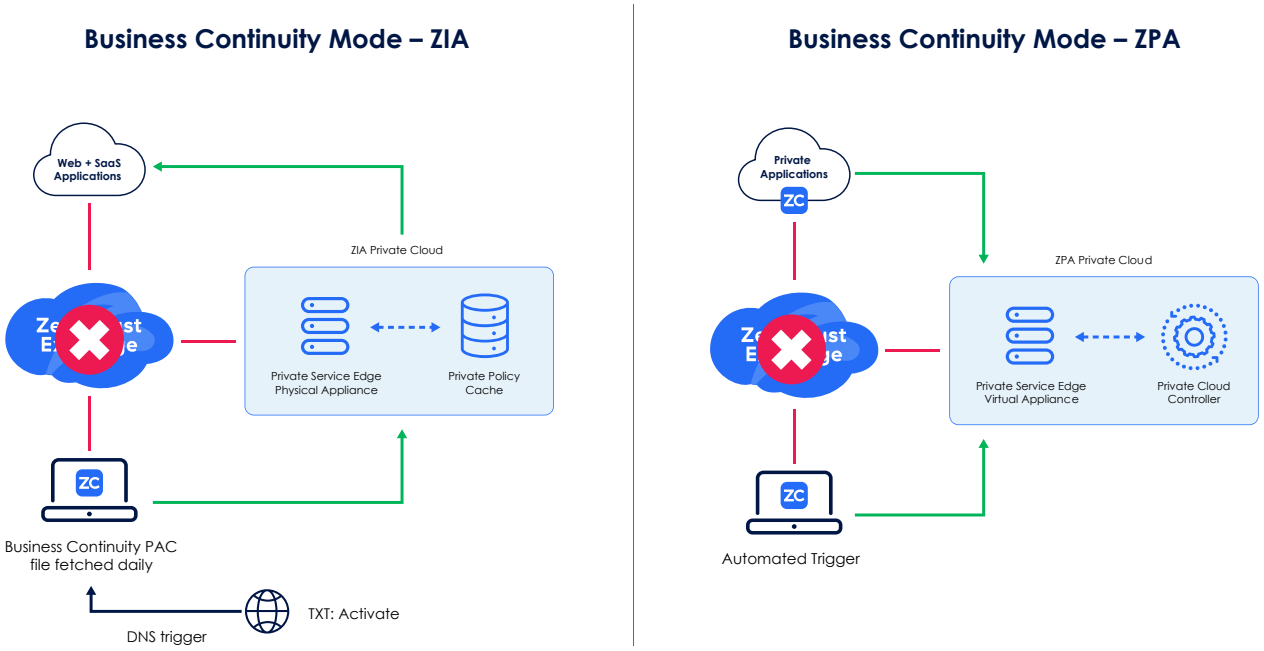


Figura 4: Nubes privadas de continuidad empresarial para acceder a todas las aplicaciones con total seguridad

© 2024 Zscaler, Inc. Todos los derechos reservados.

Continuidad empresarial para puntos finales

Otro problema que puede resultar catastrófico para una organización es la imposibilidad de utilizar sus puntos finales habituales (laptops, computadoras, etc.) cuando estos no están disponibles por cualquier motivo: mal funcionamiento, ausencia o peligro. Para hacer frente a este escenario, Zscaler Cloud Browser Isolation se puede implementar para proporcionar un acceso seguro basado en el navegador a aplicaciones privadas, web o SaaS desde puntos finales no gestionados (como BYoD), sin riesgo de pérdida de datos.

Zscaler Business Continuity, en conclusión

Una vez restablecida la funcionalidad de Zscaler Cloud, el producto puede volver a su funcionamiento normal para aprovechar al máximo la seguridad y la conectividad Zero Trust que proporciona el Zero Trust Exchange. Zscaler Digital Experience detecta fallas menores, caídas de tensión y blackout para ayudar a los clientes a solucionarlos antes de que afecten drásticamente a los usuarios. La plataforma Zscaler proporciona una flexibilidad total para la continuidad empresarial con una seguridad inigualable y una experiencia de usuario sin fisuras.

Zscaler Business Continuity, como parte de la plataforma general Zscaler, brinda a los clientes redundancia dentro de la plataforma sin la necesidad de soluciones adicionales de terceros. Zscaler se compromete a proporcionar una experiencia fluida y continua para usuarios y equipos de TI con inversiones continuas en las soluciones Zscaler Resilience.

Beneficios clave de las soluciones de continuidad empresarial de Zscaler

- Interrupción mínima de las operaciones para los clientes durante un evento catastrófico
- Acceso a aplicaciones de misión crítica incluso durante un evento de cisne negro
- Mayor confiabilidad de la solución para el acceso a las aplicaciones con Zscaler
- Ahorro de costos al disponer de una plataforma que gestionar para el acceso a las aplicaciones tanto durante el funcionamiento normal como durante las interrupciones.
- Ahorro potencial al evitar la pérdida de productividad por interrupciones durante un desastre

Para conocer las últimas novedades sobre Zscaler Resilience, visite zscaler.com/mx/resilience.

zscaler™ | Experience your world, secured.™

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 pérdida de datos al conectar de manera 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**.

© 2024 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ y otras marcas registradas listadas en **zscaler.com/mx/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 otros países. Cualquier otra marca comercial pertenece a sus respectivos propietarios.

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