# Los cinco principales riesgos de los cortafuegos perimetrales y la única forma de superarlos

Los cortafuegos han sido durante mucho tiempo una parte integral de la arquitectura de red empresarial. Pero con el cambio a los modelos de negocio digitales, el cortafuegos, en su día muy resistente, ha pasado de ser un elemento básico de seguridad a ser un riesgo para esta. He aquí los motivos.

En una arquitectura de seguridad tradicional basada en perímetros que aprovecha los cortafuegos y la VPN, la seguridad está limitada al perímetro o la zona de confianza. Cualquier usuario o aplicación que está dentro del perímetro o zona de confianza se considera bueno y los que están fuera se consideran malos. Este modelo funcionaba bien cuando la mayoría de los usuarios y aplicaciones estaban dentro del perímetro. Para introducir en el perímetro a cualquier persona que estuviera fuera de él, era necesario ampliarlo hasta ella. Se la trataba como una excepción para incluirla en la zona de confianza.

La actividad empresarial ha cambiado significativamente desde la introducción del cortafuegos. Los empleados de las empresas actuales pueden trabajar en cualquier lugar y en cualquier sitio (en una oficina en casa, en espacios de trabajo compartidos, en sucursales y en muchos otros lugares) siempre que haya una conexión a Internet y una fuente de energía. Ampliar el perímetro para cada usuario remoto ya no funciona cuando lo que antes era la excepción, tener a usuarios y aplicaciones distribuidos, es ahora la norma. El concepto de zona de confianza ya no es relevante porque las aplicaciones y los usuarios ahora pueden estar en cualquier lugar, lo que requiere cambiar a un modelo de confianza cero. No obstante, los cortafuegos y las redes privadas virtuales (VPN) no son capaces de lograr una verdadera confianza cero y plantean varios riesgos cuando lo intentan.

En este documento técnico, detallaremos los cinco riesgos principales que presentan los cortafuegos en un mundo móvil y en la nube, y cómo relegarlos al pasado con un enfoque moderno de confianza cero.

RIESGO n.º 1

# Gran superficie de ataque

Una superficie de ataque es la suma de todos los puntos expuestos, como las direcciones IP, que pueden permitir a los adversarios descubrir vulnerabilidades, dirigirse a ellas y explotarlas para acceder a un sistema y extraer datos valiosos. En pocas palabras, cuanto más reducida sea la superficie de ataque, más difícil será que los atacantes accedan. Pero la distribución de las aplicaciones en la nube y una plantilla móvil han ampliado exponencialmente la superficie de ataque y han dejado a las organizaciones más vulnerables que nunca. El uso de cortafuegos físicos y virtuales basados en el perímetro no solo no resuelve este problema, sino que empeora las cosas al aumentar la superficie de ataque de su organización, lo que permite a los ciberdelincuentes introducirse en su red o instancia en la nube.

¿Cómo? Los cortafuegos publican las direcciones IP de sus servidores y aplicaciones en Internet para que sus empleados y socios puedan encontrarlas, pero esto significa que los atacantes también pueden hacerlo. Cada cortafuegos orientado a Internet, ya esté en el centro de datos, en la nube o en una sucursal, se puede descubrir, atacar y explotar. Los cortafuegos virtuales son tan arriesgados como sus homólogos físicos, ya que también exponen las IP a Internet y, a menudo, exponen muchas más que los cortafuegos físicos, lo que aumenta aún más el riesgo.

## Cómo eliminar la superficie de ataque con la confianza cero

Eliminar con éxito su superficie de ataque es el secreto para proteger su red, sus aplicaciones y, sobre todo, sus datos. Una verdadera propuesta de confianza cero hace que las aplicaciones no enrutables sean invisibles para los posibles atacantes, de modo que sus recursos no se puedan descubrir en Internet. Una verdadera plataforma de confianza cero se interpone entre el usuario y la aplicación, de modo que toda la comunicación pasa por la plataforma y nada llega a las aplicaciones sin que la plataforma lo permita.

Este enfoque es fundamentalmente diferente de los cortafuegos perimetrales, ya que solo se permiten las conexiones de dentro a fuera, frente al enfoque tradicional de fuera a dentro que requiere la publicación de las direcciones. Al hacer que las aplicaciones sean invisibles para los adversarios y que solo puedan acceder a ellas los usuarios autorizados, la superficie de ataque prácticamente se elimina y acceder a las aplicaciones (en Internet, en SaaS o en nubes públicas o privadas) es siempre seguro.

### *Detección de la superficie de ataque*

*Las superficies de ataque pueden ser difíciles de encontrar manualmente, pero servicios como el análisis de la superficie de ataque de Internet proporcionan visibilidad de la superficie de ataque global, descubriendo los servidores, espacios de nombres, vulnerabilidades e instancias de la nube que son visibles en Internet. La evaluación consulta fuentes públicas para revelar cualquier área de exposición que le ponga en riesgo. De este modo, las organizaciones pueden evaluar las superficies de ataque, analizarlas y eliminarlas con la confianza cero.*

RIESGO n.º 2

# Saturación del rendimiento de la aplicación

Los usuarios se han acostumbrado a esperar un cierto nivel de respuesta y tiempo de actividad de las aplicaciones en la nube que utilizan en su vida personal. Sin embargo, los empleados suelen experimentar una experiencia significativamente peor cuando acceden a las aplicaciones corporativas utilizando las soluciones de acceso a la red de la empresa porque ya no tienen un acceso rápido y directo a las aplicaciones en la nube. De hecho, los usuarios pierden productividad y la capacidad de colaborar eficazmente con sus homólogos debido a la lentitud del rendimiento de las aplicaciones. Esto obliga a muchos usuarios a saltarse los controles de seguridad, lo que resulta especialmente arriesgado cuando se utilizan dispositivos no gestionados o redes wifi y domésticas no seguras. También surgen problemas de rendimiento de los usuarios finales debido a la disponibilidad de las aplicaciones SaaS o en la nube, a la capacidad de los dispositivos, a las interrupciones de la ruta de la red o a la congestión de la red, que el operador no puede aislar y diagnosticar fácilmente.

¿Por qué? La arquitectura de red radial requiere que las oficinas remotas y las sucursales se conecten a la oficina central (centro de datos) a través de cortafuegos con MPLS y a los usuarios remotos con VPN. Esta arquitectura crea una red plana que se extiende a todas las ubicaciones, lo que requiere que todo el tráfico de red fluya hacia una pila de seguridad central. Enviar el tráfico desde un usuario remoto a través del centro de datos y hacia la nube antes de volver al usuario, y seguir la misma ruta a la inversa, aumenta considerablemente la latencia, lo que degrada la experiencia del usuario. Los cortafuegos virtuales en la nube corren la misma suerte, ya que hay que redirigir el tráfico hacia ellos de la misma manera que en los centros de datos físicos, puesto que no están en línea con los servidores de aplicaciones.

Las aplicaciones en la nube se diseñaron para acceder a ellas directamente, con el menor número de saltos posible, para maximizar así el rendimiento. Como tal, muchos proveedores de aplicaciones SaaS (como Microsoft 365) señalan específicamente que no se deben interponer cortafuegos si quieren que sean totalmente compatibles.

## Cómo superar los problemas de rendimiento con la confianza cero

Una arquitectura de confianza cero se aleja de la tradicional red radial y de la seguridad de castillo y foso. Proporciona conectividad directa con las aplicaciones y reduce el riesgo a la vez que proporciona una mejor experiencia de usuario.

Una plataforma de confianza cero eficaz aplica políticas en línea, en el perímetro, de modo que no se necesitan saltos adicionales. La interconexión directa con las empresas de aplicaciones permite la conexión directa dependiendo de la disponibilidad y la capacidad. Al operar en la ruta de datos, una plataforma de confianza cero también puede supervisar todas las conexiones y detectar y solucionar automáticamente los problemas de rendimiento. Esta capacidad es crucial para las aplicaciones de baja latencia, como las aplicaciones de comunicaciones unificadas como servicio (UCaaS) del tipo Microsoft Teams y Zoom. La capacidad de supervisar estas aplicaciones y solucionar los problemas rápidamente con las capacidades de supervisión de la experiencia digital (DEM) permite a las organizaciones identificar y resolver los problemas antes de que los usuarios los perciban, lo que mejora posteriormente la colaboración y productividad de los empleados.

### *Medición de la experiencia del usuario*

*La experiencia del usuario se puede medir utilizando una herramienta de supervisión avanzada que brinda información estratégica sobre la experiencia digital para comprender, diagnosticar y mejorar los problemas de experiencia del usuario dentro de su organización. La puntuación le ayuda a identificar anomalías de rendimiento utilizando el aprendizaje automático y las alertas accionables.*

# RIESGO n.º 3 Alta complejidad y costes operativos

Utilizar cortafuegos, MPLS y VPN, o incluso dispositivos virtuales, no es un enfoque realista para implementar la confianza cero. Administrar e implementar cortafuegos perimetrales para ofrecer una seguridad consistente a todos los usuarios, todas las aplicaciones, todos los dispositivos y todas las ubicaciones es demasiado complejo y costoso operativamente. El personal no puede llegar a gestionar el despliegue de políticas perimetrales, actualizaciones y parches. Hay que adquirir e implementar cortafuegos virtuales y de hardware para los peores escenarios posibles y retornar el tráfico a una única pila de seguridad requiere un ancho de banda y una capacidad de seguridad innecesarios.

Planificar la capacidad requiere que los CIO y los CISO predigan con precisión el futuro para planificar los requisitos de hardware y los costes de consumo de ancho de banda necesarios para enviar todo el tráfico a través de MPLS al centro de datos para su inspección. Subestimar las necesidades de la red asfixia el rendimiento y, por otro lado, sobrestimarlas da lugar a costes innecesariamente altos y equipos inactivos. Por no mencionar que no es práctico implementar exactamente la misma pila de dispositivos en cada ubicación, lo que da como resultado una colección de productos dispares en toda su infraestructura. Recopilar y seleccionar registros para todos estos dispositivos es otro desafío, y los operadores a menudo pasan por alto registros críticos, lo que lleva a un riesgo potencial de seguridad. Un asombroso 75 % de los operadores está de acuerdo en que administrar el hardware de cortafuegos, las actualizaciones y las implementaciones supone todo un reto.[2]

Y esto es solo una pequeña parte del desafío. Este enfoque fragmentado requiere que el personal de seguridad utilice suscripciones y plataformas de gestión separadas para aplicar diferentes políticas, y gestionar diferentes zonas con segmentación de red. Hay que hacer un esfuerzo adicional para unir la visibilidad por usuario, aplicación y ubicación. Los empleados deben centrar sus esfuerzos a tiempo completo en implementar parches, actualizaciones de seguridad y de hardware, y administrar políticas en esta desparejada recopilación de cortafuegos y dispositivos de seguridad. El resultado es una gran carga para sus finanzas, además de que su productividad no se puede mantener.

## Cómo evitar la complejidad con la confianza cero

En lugar de tener múltiples soluciones basadas en hardware o soluciones de productos en la nube que son difíciles de gestionar y mantener, una solución de confianza cero integrada asegura todas las aplicaciones SaaS, de Internet y privadas con una única plataforma. La confianza cero elimina la necesidad de tener costosas redes MPLS que necesitan complejas labores de enrutamiento, conmutación, segmentación de red, etc., con un acceso rápido, seguro, directo a la nube, y una conectividad segura de nube a nube. Esencialmente, elimina la necesidad de retornar el tráfico al centro de datos para inspeccionarlo. Una plataforma unificada de confianza cero con una única consola de gestión es mucho más rápida de configurar, más fácil de gestionar, tiene políticas simplificadas y ofrece mayor protección que la seguridad perimetral tradicional.

Una solución de confianza cero basada en la nube coloca controles de seguridad allí donde se encuentran los usuarios y las aplicaciones: en la nube. Gracias a la visibilidad de todos los usuarios, nubes y cargas de trabajo, la confianza cero simplifica las operaciones y la resolución de problemas. La transición a la nube reduce la carga que supone para el equipo de TI la compra, gestión, mantenimiento y supervisión de los cortafuegos y otro hardware de seguridad, lo que le permite disponer de más tiempo para centrarse en otros proyectos. Y lo que es más importante, una solución de confianza cero basada en la nube facilita a las empresas una rápida adaptación a medida que aumenta el volumen de usuarios y aplicaciones.

## *Sensibilidad a los costes*

*El informe sobre riesgos de la VPN de 2021 concluyó que el alto coste de los dispositivos de seguridad y la infraestructura era el segundo mayor reto al que se enfrentan las organizaciones al implantar su solución de acceso remoto. Las organizaciones que han adoptado la confianza cero a través de Zero Trust Exchange han recibido un retorno de la inversión del 139 por ciento y 4,1 millones de dólares de media en beneficios, junto con un aumento de la productividad y una reducción de incidentes y del número de dispositivos.*[3]

# Movimiento lateral de amenazas



Los atacantes utilizan diversos medios para obtener acceso a la red de una organización y lo suelen hacer mediante ataques de phishing o infecciones por malware. Una vez en la red, su objetivo es moverse lateralmente a través de la organización en busca de acceso a datos confidenciales para exfiltrarlos, cifrarlos para el rescate o causar otras interrupciones. El movimiento lateral permite que un atacante evite la detección y mantenga el acceso, incluso si se descubre en el equipo en el que se produjo la primera infección. Y dado que el tiempo de permanencia es largo, el robo de datos podría no producirse hasta pasadas semanas, o incluso meses, después de la infracción original.

Las organizaciones han confiado en un enfoque de seguridad de "castillo y foso" (también conocido como seguridad perimetral) para proteger los datos de los ataques maliciosos. Al igual que los castillos medievales, protegidos por muros de piedra, fosos y portones, la seguridad perimetral invierte mucho en fortificar los perímetros de la red con cortafuegos y otras herramientas. La seguridad perimetral protege los puntos de entrada y salida de la red verificando los paquetes de datos y la identidad de los usuarios que entran y salen de la red de la organización, y posteriormente asume que la actividad dentro de este perímetro reforzado es relativamente segura.

Las arquitecturas de seguridad tradicionales son incapaces de detener estos sofisticados ataques porque una vez que el usuario, bueno o malo, entra en una red "segura", se convierte en un usuario de confianza y obtiene acceso lateral a todas las aplicaciones, aunque no deba tenerlo. La reducción del movimiento lateral este-oeste en las arquitecturas basadas en el perímetro requiere la segmentación de la red (perímetros internos), algo que es una pesadilla operativa, ya que exige que las organizaciones desplieguen y gestionen más cortafuegos con más políticas, lo cual no resuelve adecuadamente el problema subyacente.

## Cómo superar el movimiento lateral con la confianza cero

La confianza cero impide el movimiento lateral, ya que conecta a los usuarios y las cargas de trabajo con las aplicaciones directamente, nunca con la red corporativa. Esto significa que las amenazas no se pueden propagar lateralmente para infectar otros dispositivos y aplicaciones, todo ello sin la necesidad de una segmentación de red compleja. Esto no solo se aplica a los usuarios que acceden a las aplicaciones, sino que puede aplicarse a todas las conexiones dentro de la organización, desde máquinas de IoT hasta aplicaciones que hablan entre sí, donde una aplicación en una ubicación (nube o centro de datos) puede conectarse de forma segura a otra aplicación dondequiera que se encuentre. Gracias a estas conexiones seguras uno a uno se elimina el riesgo de movimiento lateral.

El modelo de confianza cero parte de la base de que todo es hostil y solo establece la confianza en función de la identidad y el contexto. Este enfoque autoriza las conexiones basándose en el conocimiento de las entidades que se conectan y el contexto de sus conexiones garantiza que el acceso se limita en todo momento solo a lo que se necesita. Esta forma de proceder elimina una carga importante de los equipos de seguridad y de TI, ya que ocurre automáticamente y puede cambiar dinámicamente cuando las condiciones se modifican para dichas entidades y sus conexiones.

Por último, la confianza cero proporciona controles granulares con acceso condicional. Un administrador puede configurar políticas para que los usuarios puedan acceder a ciertas aplicaciones únicamente si su tráfico se origina en una ubicación de confianza, como una red corporativa, y si han proporcionado autenticación multifactor. El administrador también puede bloquear el tráfico de usuarios procedente de determinadas ubicaciones o ámbitos geográficos, de un dispositivo que no sea de confianza o si los datos que se solicitan van más allá de los permisos específicos de un usuario. Todas las conexiones se basan en el contexto y, a medida que cambia el contexto, se vuelve a evaluar la confianza.

### *La nueva segmentación*

*El coste, la complejidad y el tiempo que conlleva la segmentación de la red mediante cortafuegos virtuales superan al beneficio en materia de seguridad.* La segmentación de la carga de trabajo *es una nueva forma de segmentar las cargas de trabajo de las aplicaciones. Con un solo clic, se puede mejorar la seguridad permitiendo que la segmentación de la carga de trabajo revele el riesgo y aplique la protección basada en la identidad a las cargas de trabajo sin hacer ningún cambio en la red. La tecnología de segmentación de la carga de trabajo basada en la identidad proporciona una protección sin fisuras con políticas que se adaptan automáticamente a los cambios del entorno.*

RIESGO n.º 5

# Pérdida de datos

Los datos son cruciales para las organizaciones por motivos estratégicos, financieros y de seguridad, entre otros; y en algunos casos pueden ser fundamentales para la seguridad nacional. Incluso con los perímetros de seguridad de la red, los datos pueden filtrarse debido a la falta de conocimiento, las acciones involuntarias de los usuarios, los fallos del sistema y las actividades maliciosas cada vez más sofisticadas. La filtración puede causar una serie de problemas, como multas, pérdida de clientes, ramificaciones legales, incumplimiento de la normativa y daños a la marca de la empresa. Veamos los diferentes tipos de datos y cómo pueden estar en peligro:

- **Datos en movimiento:** los datos en tránsito a través de Internet constituyen la mayor parte de los datos en movimiento hoy en día, ya que ahora se accede a las aplicaciones principalmente a través de la web; esto se aplica a las aplicaciones SaaS, las aplicaciones en el centro de datos y las de las nubes públicas. Que los usuarios accedan a Internet y a destinos de riesgo en los que se puede exfiltrar información confidencial supone una amenaza para los datos de la empresa. Los cortafuegos no pueden seguir a los usuarios fuera de la red ni proteger su tráfico web esencial en movimiento. Hay menos datos y aplicaciones en los puntos finales y se confiere más importancia a la seguridad de los datos que fluyen entre los puntos finales, las aplicaciones en la nube y el almacenamiento con una solución de datos en movimiento.
- **Datos en reposo:** los datos que residen dentro de los centros de datos, las aplicaciones SaaS y las nubes públicas representan la gran mayoría de los datos en reposo. En particular, proteger los datos en reposo en las aplicaciones SaaS es fundamental para la seguridad; incluso si están protegidos con cortafuegos, solo son necesarios unos pocos clics para compartir los datos con un usuario no autorizado a través de aplicaciones como Microsoft OneDrive. Además, las brechas en la nube pueden deberse a malas configuraciones o permisos peligrosos. Dado que SaaS e IaaS son muy dinámicos y los suelen configurar personas que no son expertas en seguridad, estas brechas se pasan por alto y se aprovechan con frecuencia.

El objetivo final de cualquier tecnología de seguridad es proteger los datos confidenciales, pero los cortafuegos no son capaces de identificar y controlar eficazmente los datos en movimiento o en reposo, y eso pone en riesgo los datos de la organización. Lo más importante es que no pueden inspeccionar eficazmente el tráfico cifrado (más del 90 por ciento de todo el tráfico[1]), lo que permite que el tráfico cifrado SSL/TLS pase sin inspeccionar.

## Cómo evitar la pérdida de datos con la confianza cero

Una verdadera plataforma de confianza cero puede inspeccionar todo el tráfico, tanto dentro como fuera de la red, incluido todo el tráfico cifrado. Cierra las lagunas de visibilidad e inspección para proporcionar una prevención de la pérdida de datos (DLP) y una protección contra ciberamenazas eficaces. Es capaz de descifrar todos los datos, determinar la integridad de los mismos y, a continuación, autorizar las conexiones mediante el contexto, teniendo en cuenta el usuario, la geolocalización, la dirección IP, la postura del dispositivo, la hora del día, etc. Las políticas de DLP de una solución de confianza cero protegen los datos en movimiento, mientras que los usuarios de todas partes obtienen una seguridad rápida y consistente.

Una solución de confianza cero en línea ofrece un completo descubrimiento y control de la TI en la sombra. Protege de las amenazas basadas en la web y los datos con un aislamiento del navegador que permite el acceso de dispositivos no gestionados sin los problemas de rendimiento. El aislamiento del navegador transmite datos en forma de píxeles desde una sesión aislada en un entorno en contenedores, lo que permite el uso de los dispositivos propios, pero evita la pérdida de datos mediante la descarga, la copia, el pegado y la impresión. El DLP fuera de banda y la protección avanzada contra amenazas (ATP) acaban con el riesgo de compartir archivos y el malware en reposo en la nube. Para proteger los datos en la nube, también soluciona los posibles errores de configuración, las infracciones de cumplimiento, los permisos y los derechos potencialmente fatales. En resumen, la confianza cero proporciona una seguridad coherente y unificada para los datos en reposo y en movimiento (incluido el tráfico cifrado) a través de Internet, SaaS y aplicaciones de nube pública a escala, independientemente del dispositivo del usuario.

### *Vulnerabilidad del navegador web*

*El porcentaje de tráfico web cifrado en Internet ha aumentado de forma constante del 50 % en 2014 a un asombroso 95 % en la actualidad.[1] Incluso con estos datos, los navegadores web son el principal objetivo para los atacantes, ya que el 98 %de los ataques se llevan a cabo a través de la Internet pública y el 80 % de esos ataques se dirigen a los usuarios finales a través de los navegadores, según Gartner. Las herramientas de aislamiento del navegador, como el aislamiento del navegador en la nube, ayudan a mitigar estas vulnerabilidades, especialmente allí donde se pueden implementar sin instalaciones de software en el entorno del cliente, lo que las convierte en una mejor opción para los dispositivos no gestionados que acceden a los recursos de TI corporativos.*

## Logre una verdadera confianza cero con Zscaler

Zscaler ofrece confianza cero con Zscaler Zero Trust Exchange, una plataforma nativa de la nube, que opera en 150 centros de datos en todo el mundo, que aprovecha la mayor nube de seguridad del planeta para proporcionar conexiones rápidas y seguras y que permite a sus empleados trabajar de forma segura desde cualquier lugar, en cualquier dispositivo, utilizando Internet como red corporativa. A diferencia de los cortafuegos y las VPN, Zero Trust Exchange se basa en el principio del acceso con menos privilegios y en la idea de que ningún usuario o aplicación es intrínsecamente fiable. En su lugar, las conexiones se autorizan en función de la identidad y el contexto del usuario, incluida su ubicación, la postura de seguridad del dispositivo, la aplicación a la que se accede y el contenido que se intercambia.

¿Cómo? Lo primero que hace Zero Trust Exchange es terminar la conexión para permitir que el contenido se inspeccione con profundidad (incluido el tráfico cifrado), ejecutando datos profundos y análisis de amenazas. A continuación, determina la identidad y el dispositivo y verifica los derechos de acceso mediante políticas empresariales basadas en el contexto, en el que se incluye el usuario, el dispositivo y la aplicación que se solicitan y el tipo de contenido. Una vez verificada y aplicada la política empresarial, Zero Trust Exchange intermedia la conexión entre los recursos previstos. Los usuarios y dispositivos se conectan directamente a las aplicaciones, nunca a la red corporativa.

# Más información

Si desea más información sobre la confianza cero y sobre cómo Zscaler puede ayudarle, visite la página **Zero Trust Exchange**.

Fuentes

[1] *Informe de transparencia de Google https://transparencyreport.google.com/https/overview?hl=es*
[2] *Encuesta de seguridad de redes de Zscaler 2020*
[3] *Estudio de validación económica de ESG 2021*

### Acerca de Zscaler

Zscaler permite a las organizaciones transformar de forma segura sus redes y aplicaciones para un mundomóvil y ser pioneros en la nube. Zscaler conecta a los usuarios con aplicaciones y servicios en la nube, independientemente del dispositivo, la ubicación o la red, a la vez que proporciona seguridad integral y una experiencia de usuario rápida. Todo ello sin dispositivos de entrada costosos y complejos.