Documento técnico

Cómo afrontar los cinco principales desafíos de seguridad de la red con la confianza cero

Durante las últimas décadas, las redes radiales han extendido la red corporativa a usuarios y ubicaciones remotas, incluidas las sucursales. Dichas redes se crearon y optimizaron para conectarse a un centro de datos centralizado, donde residía la seguridad. Dado que todo era parte de la red plana, la seguridad se diseñó para colocar una barrera entre la red de confianza y el mundo exterior (internet). Este modelo de seguridad perimetral mediante cortafuegos se conocía como seguridad de castillo y foso. Este modelo funcionó bien en el pasado cuando todos los usuarios y las aplicaciones eran locales, pero las necesidades empresariales han cambiado a medida que el trabajo remoto ha aumentado exponencialmente y más aplicaciones se han trasladado a la nube.

Estos cambios han creado nuevos desafíos para las organizaciones que están aplicando arquitecturas de seguridad de red para proteger a una fuerza laboral híbrida y aplicaciones basadas en la nube.
Exploremos estos desafíos en detalle:

N.º 1 Riesgos desconocidos y no controlados que causan interrupciones y pérdidas empresariales

La ciberseguridad se vuelve más difícil cada día debido a los ataques avanzados y amenazas de atacantes sofisticados que pueden encontrar e infringir cortafuegos, VPN y cortafuegos virtuales basados en la nube. Un cortafuegos orientado a Internet (da igual que esté en el centro de datos, en la nube o en una sucursal) puede ser descubierto, atacado y quedar a merced de los intrusos. Una vez descubierto, los adversarios buscarán vulnerabilidades y puntos débiles para obtener acceso. Una vez que se ha accedido al dispositivo, las puertas están abiertas para que los atacantes roben datos y denieguen el acceso, o pueden optar por trasladarse lateralmente a otros dispositivos de destino en la red y buscar vulnerabilidades.

Las arquitecturas de seguridad tradicionales son incapaces de impedir estos sofisticados ataques. Una vez que un usuario, bueno o malo, entra en una red "segura", se convierte en usuario de confianza y obtiene acceso lateral a todas las aplicaciones, incluso cuando no debería. Los cortafuegos virtuales son tan arriesgados como sus homólogos físicos, porque también se pueden descubrir para llevar a cabo ataques, y sufren ataques en mayor medida que los cortafuegos físicos, lo que aumenta aún más el riesgo.

La mayoría de los adversarios no atacan la primera máquina que encuentran. Lo que sucede es que la amenaza primero estudia el entorno para determinar cómo puede moverse lateralmente a través de la red para infectar recursos adicionales. Puede moverse rápida y silenciosamente por la red para depositar ransomware en más de un sistema. Una vez que se alcanza un número importante, el ransomware cifra todos estos recursos a la vez, lo que supone un golpe catastrófico para la organización. La naturaleza plana de las arquitecturas de seguridad de red permite todo esto.

Como analogía, imagine que unos ladrones entran en su casa a través de la ventana del baño. No tienen nada que robar del cuarto de baño, pero pueden pasar de allí a su dormitorio o a cualquier otro lugar donde se guarden objetos de valor y no hay nada que les detenga, ya que ninguna habitación tiene puertas cerradas con llave u otro tipo de protección.

Cómo prevenir las ciberamenazas con la confianza cero

Para proteger mejor el acceso a las aplicaciones, es necesario eliminar la superficie de ataque de su organización e imponer la seguridad en línea y en el perímetro. 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.

¿Cómo se afronta el movimiento lateral de las amenazas? La confianza cero crea conexiones directas entre entidades autorizadas, como de un usuario autenticado a una aplicación específica.

El 67 % de las organizaciones está muy de acuerdo en que los cortafuegos no son capaces de proporcionar un acceso rápido y seguro eficazmente a los usuarios remotos[1]

Solo el usuario autenticado tiene acceso a esa aplicación solicitada y ningún otro usuario puede acceder a ella. No pueden encontrar la aplicación, lo que no solo elimina la ruta de ataque, sino que también garantiza que las amenazas no puedan propagarse lateralmente para infectar otros dispositivos o aplicaciones.

Volviendo a nuestra analogía con el robo en su hogar, en este caso es casi imposible que los ladrones encuentren la casa porque sin superficie de ataque la casa no se puede encontrar. Incluso si la encuentran de alguna manera, cada parte de la casa, ya sea un baño, una sala de estar o un dormitorio, es independiente y está desconectada del resto, ya que cada una tiene su propio acceso único. De esta manera, los ladrones son incapaces de moverse de una parte de la casa a otra.

Con la confianza cero, se configuran controles para verificar la identidad y el contexto, y el contexto se comprueba continuamente. Una solución de confianza cero debe ser capaz de descifrar todos los datos, identificar la posible pérdida de datos y detener el intercambio de amenazas. Una conexión segura se establece a través de una serie de factores contextuales y espaciales que se validan continuamente para un usuario, como la geolocalización, la dirección IP, la postura del dispositivo y la hora del día. Esto se hace sin que el usuario lo sepa, de modo que no se interrumpe a un usuario autorizado mientras hace su trabajo.

N.º2

Ineficacia operativa debida a la complejidad

Una de las tareas más arduas de proteger a una organización es la distribución de políticas a través de una infraestructura dispersa que incluye infraestructura de hardware y basada en la nube. Las empresas determinan su política empresarial para designar a un alto nivel a qué pueden y no pueden acceder sus empleados. Estas políticas empresariales se traducen en políticas de red, ya que el modelo de seguridad perimetral se basa en el acceso a la red. Para la infraestructura distribuida, donde hay más aplicaciones SaaS o basadas en la nube que en un centro de datos y los usuarios tienen más probabilidades de trabajar remotamente que en la oficina, la aplicación de políticas de red se complica cada vez más porque el perímetro de la red se ha expandido más allá de la infraestructura de hardware del centro de datos, a todas las ubicaciones donde residen las aplicaciones y los usuarios. Considere la posibilidad de que un operador defina las políticas para una red de este tipo: tendría que definir las políticas de acceso cuando el usuario está en la oficina, las políticas para las aplicaciones SaaS, las políticas de cortafuegos, las políticas IPS/IDS, y muchas más. En resumen, es una pesadilla.

Las aplicaciones modernas no solo residen en una única nube, sino que pueden tener dependencias repartidas por un entorno de varias nubes que a menudo deben comunicarse. Administrar aplicaciones en entornos multinube es especialmente más complejo que hacer que la conectividad sea segura en múltiples nubes y centros de datos. Requiere un mosaico de VPN de sitio a sitio, cortafuegos, pasarelas de tránsito y políticas de peering que amplían el desafío de manera exponencial.

Los operadores de red deben predecir los requisitos futuros y llevar a cabo una amplia planificación de sus capacidades para adaptarse a las necesidades futuras de ancho de banda

El 75 % de las organizaciones está de acuerdo en que es difícil administrar hardware de cortafuegos, actualizaciones e implementaciones[1]

y escalado. Subestimar las necesidades de la red ahoga el rendimiento y, por otro lado, sobrestimarlas da lugar a costes innecesariamente elevados y a que los equipos queden inactivos. Además, hay numerosos productos que requieren la intervención periódica de los equipos de seguridad para realizar tareas como las actualizaciones de software, la gestión de parches, la resolución de problemas, etc. Estas tareas pueden ser críticas para mantener la seguridad de una organización, pero pueden tardar semanas, o incluso meses, en ejecutarse.

Cómo disminuir la complejidad con la confianza cero

Un aplicador de políticas de confianza cero se coloca entre las entidades, como dispositivos móviles, IoT, etc. que intentan conectarse y los recursos, como aplicaciones en la nube, aplicaciones SaaS, aplicaciones de Internet, etc. a los que la entidad está tratando de acceder. Aplica políticas empresariales (a lo que pueden y no pueden acceder sus empleados) y contexto de diversas maneras para llegar a una decisión de cumplimiento, y luego los agentes autorizan la conectividad al recurso solicitado. El cumplimiento en línea de las políticas empresariales elimina la complejidad que se ve en modelos basados en perímetros de traducir las políticas empresariales en políticas de red.

Una solución integrada de confianza cero asegura todas las aplicaciones SaaS, de Internet y privadas utilizando una única plataforma, en lugar de múltiples soluciones de seguridad basadas en hardware o virtuales que son difíciles de gestionar y mantener. Una plataforma unificada de confianza cero con una única consola de gestión es mucho más rápida de configurar, más fácil de gestionar, simplifica las políticas y ofrece más seguridad que las soluciones de seguridad perimetral.

Una solución de confianza cero basada en la nube sitúa los controles de seguridad, los usuarios y las aplicaciones en la nube, lo que facilita su ampliación. A medida que aumenta el volumen de usuarios y aplicaciones, garantiza la escalabilidad con una experiencia de usuario consistente, rápida y sin fisuras. Al tener una mayor visibilidad de los usuarios, las nubes y las cargas de trabajo, la confianza cero simplifica las operaciones y la resolución de problemas.

Nº3

Pérdida de productividad y colaboración como consecuencia de la mala experiencia del usuario

Los usuarios esperan que las aplicaciones funcionen cuando las necesitan, tanto si se conectan a través de la wifi de la empresa como si trabajan en casa o mientras están de viaje. No les interesa cómo se accede a una aplicación o qué modelo de red y seguridad se utiliza en el back-end. Cuando las aplicaciones no son accesibles o responden con lentitud, se degrada la productividad y aumenta la frustración de los usuarios.

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.

300 %
de aumento del porcentaje del total de empleados que son usuarios a distancia[4]

Esta arquitectura crea una red plana que se extiende a todas las ubicaciones, que requieren 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 imprevisiblemente la latencia, lo que degrada la experiencia del usuario. El mismo problema ocurre con los cortafuegos virtuales, ya que también forman parte de la arquitectura de red plana que requiere que todo el tráfico de red fluya hacia el cortafuegos virtual que se encuentra en la nube, lo que crea un nuevo cuello de botella en la nube.

Es esencial que las organizaciones brinden la mejor experiencia de usuario posible a todos los usuarios, incluidos empleados, socios, proveedores y clientes, en cualquier ubicación, cuando acceden a las aplicaciones desde cualquier dispositivo. Pero esto puede suponer un reto para los equipos de TI y de seguridad, ya que los usuarios, los datos, las aplicaciones y los dispositivos están más distribuidos que nunca.

Cómo mejorar la experiencia del usuario utilizando la confianza cero

La confianza cero resuelve los problemas de rendimiento de los usuarios aplicando las políticas en línea, en el perímetro, por lo que no se necesitan saltos adicionales, proporcionando conexiones directas a las aplicaciones independientemente de la ubicación del usuario o del dispositivo. Las conexiones directas eliminan la necesidad de retornar el tráfico a través de controles de seguridad centralizados que añaden latencia. 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.

Una solución de confianza cero en el perímetro analiza todo el contenido en una sola pasada sin copiar paquetes ni añadir latencia. Este enfoque es muy diferente del modelo encadenado de los dispositivos físicos o virtuales, en el que cada servicio de seguridad procesa los paquetes de forma independiente, añadiendo una latencia incremental en cada salto. Con una sola exploración, las políticas pueden aplicarse en una variedad de motores de seguridad con una latencia mínima.

Las aplicaciones críticas de comunicaciones unificadas como servicio (UCaaS), como Microsoft Teams y Zoom, exigen latencias bajas para funcionar eficazmente. Una solución eficaz de confianza cero permite a los operadores satisfacer estas demandas de baja latencia y alta disponibilidad mediante el análisis directo con las empresas de aplicaciones para permitir una conexión directa basada en la disponibilidad y la capacidad de la aplicación. Por ejemplo, si un usuario M365 accede a la aplicación desde Texas, se conectará al centro de datos más cercano y se realizará una comprobación de seguridad en línea. Aplica la política en línea, en el perímetro, por lo que no se necesitan saltos adicionales, lo cual es una gran transición desde la arquitectura radial.

Para elevar la colaboración y la productividad de los empleados, la confianza cero debe supervisar estas aplicaciones y remediar los problemas rápidamente con capacidades de supervisión de la experiencia digital (DEM). Al ser una solución en línea que opera en la ruta de datos, es mucho más fácil supervisar cada conexión, y detectar y solucionar problemas de rendimiento de forma automática y rápida.

N.º4 Equipos de TI aislados que ralentizan la transformación

La transformación del negocio requiere también la transformación de las TI. Sin embargo, la transición a una solución de confianza cero basada en la nube y la sustitución de la infraestructura de hardware puede ser una tarea desalentadora. Es un desafío tanto para la organización como para los equipos de TI, seguridad, redes, operaciones y otros.

Uno de los principales obstáculos para la transformación digital en las organizaciones es la falta de comunicación dentro de los equipos de TI. No es intencional: estos equipos se han diseñado para trabajar en diferentes áreas de la red y la infraestructura de seguridad. Trabajan en componentes individuales y no necesariamente trabajan para resolver un problema general. Los equipos están acostumbrados a trabajar en sus respectivas soluciones: por ejemplo, el equipo de seguridad instalará cortafuegos, habilitará redes privadas virtuales y se asegurará de que la pila de seguridad esté en funcionamiento, mientras que el equipo de redes garantizará que el enrutamiento y la conmutación funcionen bien y de que protocolos como MPLS, OSPF y otros estén en funcionamiento. Los dos equipos no suelen colaborar a menos que haya algo relacionado con la interoperabilidad. La modernización de la infraestructura basada en la nube requiere que trabajen juntos, lo que supone un gran cambio de la forma tradicional de operar. Este cambio puede ser difícil de afrontar sin las herramientas, la formación y los procesos adecuados.

El 67 % de los profesionales de la seguridad están de acuerdo en que las operaciones de seguridad en la nube son una mejor trayectoria profesional a largo plazo que la administración de cortafuegos[1]

Por otro lado, las organizaciones han invertido en las arquitecturas de seguridad de red existentes y necesitan una buena justificación para pasar a una nueva arquitectura. Cambiar la mentalidad de los equipos que liderarán la transición a la nube a menudo es un desafío, ya que la seguridad lleva décadas sin cambiar. Los operadores de redes que llevan años operando con cortafuegos y VPN también pueden temer no tener los conocimientos necesarios para operar con soluciones de seguridad basadas en la nube.

Cómo abordar la transformación con la confianza cero

Una plataforma de confianza cero basada en la nube simplifica la gestión y las operaciones de seguridad. Los equipos de red, seguridad y operaciones pueden colaborar para pasar de un enfoque basado en el perímetro a una solución basada en políticas empresariales que transforme la infraestructura de red y seguridad existente con una solución de confianza cero basada en la nube. Reducir esa carga permite a los equipos utilizar el tiempo para proyectos estratégicos, como el análisis de datos, la optimización de la seguridad y otras actividades que dan soporte directamente a los objetivos empresariales generales. Las organizaciones son mucho más seguras cuando los equipos rompen los silos y se comunican y trabajan juntos como uno solo.

La transición a una solución de confianza cero basada en la nube también reduce la carga que supone para el equipo de TI la compra, la gestión, el mantenimiento y la supervisión del hardware, lo que le permite disponer de más tiempo para centrarse en otros proyectos. Los CISO y los CIO ya no son responsables de predecir con precisión el futuro para planificar los requisitos de hardware y los costos de consumo de ancho de banda. A través de una comunicación clara y un plan sólido, las organizaciones pueden ganar la confianza y el apoyo de sus equipos de TI y seguridad, y tener éxito en la transformación de la nube.

N.º5 Costes de infraestructura elevados debido a la ineficiencia de los despliegues

La infraestructura de red necesaria para mantener las arquitecturas radiales (que se ejecutan en protocolos como MPLS) es cara de adquirir y desplegar, y requiere un equipo de TI experimentado para mantenerla. También está el coste adicional de ancho de banda en el que se incurre debido al enrutamiento innecesario del tráfico de retorno al centro de datos, incluso cuando no es necesario, como cuando se accede a una aplicación SaaS basada en la nube. Más allá de la infraestructura de red, el coste de la infraestructura de seguridad (incluidos los cortafuegos, los conmutadores, los equilibradores de carga, los controles de acceso, las redes privadas virtuales (VPN), los sandboxes y los sistemas de prevención de intrusiones) es elevado y supera con creces al considerable precio que conllevan estas tecnologías. También hay que tener en cuenta el coste de la instalación, la configuración, el aprovisionamiento, las pruebas y la resolución de problemas, todo ello acompañado de la carga añadida del mantenimiento final de estos sistemas. Todos estos costes se multiplican cuando se tienen diferentes productos puntuales y se necesita personal altamente cualificado para hacerlos funcionar juntos.

Los CIO y los CISO deben anticipar con precisión la capacidad organizativa futura para tener en cuenta los requisitos de hardware y los costes de consumo de ancho de banda de enviar todo el tráfico por MPLS al centro de datos para su inspección. Es un equilibrio delicado: si planifica de manera insuficiente, usted no será capaz de escalar eficazmente a medida que crezca la demanda; si planifica en exceso, tendrá costes altos e innecesarios. Además, subestimar las necesidades de la red puede impedir la productividad, pero sobrestimarlas puede generar altos costes y equipos que se queden sin utilizar. Por último, es probable que cada ubicación necesite una implementación única de dispositivos, lo que puede generar una afluencia de productos dispares en toda su infraestructura.

Para el tráfico que se dirige a Internet, tiene más sentido utilizar las conexiones de banda ancha, que cuestan una mínima parte de la infraestructura de seguridad de la red; sin embargo, estas conexiones deben estar protegidas. ¿Pero cómo? Implementar la seguridad en la puerta de enlace en todas las sucursales para habilitar las conexiones directas sería igualmente exorbitante.

El 50 %
de todos los datos corporativos se almacenan en la nube[2] y

El 70 %
de las aplicaciones empresariales se basan en SaaS[3]

Cómo reducir los costes con la transformación de la nube de confianza cero

Cambiar a una solución de confianza cero nativa de la nube permite a las organizaciones reducir los costos y, al mismo tiempo, mejorar la seguridad mediante la eliminación de las VPN, los costes de tránsito de la nube pública y las arquitecturas de redes personalizadas. La confianza cero mitiga los costes secundarios asociados con un aumento en el acceso remoto, mientras que las organizaciones con soluciones basadas en perímetros han tenido que escalar sus cortafuegos y VPN existentes invirtiendo en infraestructuras y dispositivos caros que consumen sus presupuestos de TI.

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. Además, una arquitectura de confianza cero basada en la nube agiliza la seguridad y reduce los plazos de implantación a días en lugar de meses, al tiempo que ayuda a detectar, prevenir y evitar costosas infracciones de datos que podrían costar millones a una organización. Una solución de confianza cero basada en la nube es mucho más rentable y fácil para que las empresas escalen rápidamente, ya que pueden comprar según lo necesiten, eliminando la necesidad de una planificación extensa y una compra excesiva.

Logre una verdadera confianza cero con Zscaler

Zscaler Zero Trust Exchange ofrece confianza cero aprovechando la mayor nube de seguridad del planeta para proporcionar conexiones rápidas y seguras que permitan 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. Por ello, las conexiones se autorizan a través de la política de la empresa y se basan en la identidad y el contexto del usuario.
Una vez verificada y aplicada la política empresarial, Zero Trust Exchange proporciona la conexión entre los recursos previstos. Los usuarios y dispositivos se conectan directamente a las aplicaciones, nunca a la red corporativa.

Obtenga más información sobre Zero Trust Exchange: www.zscaler.es/platform/zero-trust-exchange

Vea este seminario web sobre por qué los cortafuegos no son compatibles con la confianza cero:
info.zscaler.com/webinar-why-firewalls-cannot-do-zero-trust?utm_source=digital

Fuentes:
[1]Virtual Intelligence Briefing (ViB) Networks Security Survey 2021
[2]Statista. Percent of data and sensitive data stored in the cloud worldwide.
www.statista.com/statistics/1202541/sensitive-data-cloud-location
[3]Better Cloud. (2021). The State of SaaSOps 2021.
stateofsaasops.bettercloud.com/?_ga=2.164919740.241347015.1636678142-1969514686.1636678142
[4]Grady, John. (2021). El estado de las estrategias de seguridad de confianza cero. Enterprise Strategy Group.
https://info.zscaler.com/resources-industry-report-the-state-of-zero-trust-security-strategies

zscaler™ | Experience your world, secured.™

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**.

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