zscaler™

7 síntomas que le indican que su cortafuegos heredado no es apto para la confianza cero

Libro electrónico

La adopción de la confianza cero va en aumento...

Las partes interesadas de la seguridad informática de hoy en día son muy conscientes de que la confianza cero es el modelo de seguridad adecuado para las empresas digitales modernas. Las encuestas muestran que hasta el 78 % de los programas de seguridad de las empresas han adoptado el acceso a la red de confianza cero o están planeando hacerlo en el futuro.[1] Saben que centrarse directamente en la seguridad de los usuarios, los datos y las aplicaciones (en lugar de la red) es la clave para proteger a las empresas actuales impulsadas por los datos y que han habilitado el trabajo remoto.

Hace décadas, cuando los diseños de redes radiales eran lo más moderno, los cortafuegos y las infraestructuras de red construidos en torno a ellos eran jóvenes, ágiles y saludables. Fueron la opción tecnológica adecuada para esa época, sirvieron fielmente e hicieron bien su trabajo. Sin embargo, en la era moderna de la informática en la nube, su presencia es una carga, y los diseños de arquitectura de castillo y foso son fundamentalmente incompatibles con el paradigma de la confianza cero.

Esta es una guía diagnóstica que describe siete síntomas de que su cortafuegos no es apto para el mundo de la seguridad de confianza cero de hoy en día. Cualquiera de estos siete síntomas es una señal de que su organización necesita una cura de seguridad en la nube.

1. Fuente: Cybersecurity Insiders, Informe de adopción de la confianza cero, 2019.

SÍNTOMA N.º 1

La falta de visibilidad al tratar de inspeccionar el tráfico a escala

Independientemente de su forma, los cortafuegos basados en dispositivos simplemente no pueden inspeccionar el tráfico cifrado SSL de la capa de sockets cifrados (SSL) a escala. Esto se convierte en un problema cada vez mayor a medida que aumenta el porcentaje de tráfico de Internet global que está cifrado por SSL. Los atacantes conocen este aumento y ocultan cada vez más amenazas avanzadas dentro del tráfico cifrado.

Si su cortafuegos tiene este problema, notará una degradación del rendimiento del 50 % o más cada vez que intente activar la inspección SSL. Tendrá que obtener un cortafuegos de mayor capacidad o añadir más dispositivos (o instancias de cortafuegos virtuales) simplemente para mantener un rendimiento aceptable para sus usuarios.

El 85 %
del tráfico mundial de Internet está cifrado en la actualidad.[2]

¿CUÁL ES EL REMEDIO?

- Pase a un servicio suministrado en la nube que pueda proporcionar capacidades de cortafuegos nativas en la nube en lugar de intentar aprovechar y escalar versiones de máquinas virtuales (VM) de dispositivos físicos obsoletos. Únicamente los verdaderos servicios y soluciones en la nube son infinitamente escalables para satisfacer las necesidades de tráfico actuales.

El 85 %
de los administradores de redes están de acuerdo en que las capacidades del cortafuegos se ofrecen mejor a través de la nube.[3]

2. Fuente: Agencia de Ciberseguridad de la Unión Europea, Análisis del tráfico cifrado
3. Fuente: Zscaler, Encuesta sobre los cortafuegos de red

SÍNTOMA N.º 2

Desconocimiento del movimiento lateral

Los cortafuegos fueron diseñados para proteger el perímetro de las redes de tipo castillo y foso. La idea era que una vez que el cortafuegos había tomado una decisión sobre si permitir o no su entrada, todo el tráfico dentro de ese perímetro podría ser de confianza incondicional. En tales arquitecturas, la mayoría de los usuarios trabajaban localmente, más infraestructura estaba ubicada en las instalaciones y la mayoría de las aplicaciones residían en el centro de datos. Nada de todo esto es así ya.

La realidad actual es que el 70 % del tráfico es interno a la red, lo que significa que fluye entre servidores y aplicaciones dentro de la nube privada o el centro de datos de la empresa. Las defensas basadas en el perímetro dejan pocos medios, o ninguno, para inspeccionar o bloquear este tráfico, lo que da rienda suelta a los atacantes una vez que han entrado en la red.

Una vez que se obtiene acceso a este tipo de red, es trivial descubrir todos los activos a los que está conectado. El usuario no necesita más que una herramienta de exploración de código abierto para encontrar todas las direcciones IP de la red. A partir de ahí, difundir ransomware (o exfiltrar datos valiosos) es algo sencillo, y no hay nada que un cortafuegos pueda hacer para detenerlo.

El 64 %
de los administradores de red actuales cree que los cortafuegos son ineficaces para detener el movimiento lateral.[4]

El 57 %
de los responsables de la toma de decisiones de TI cree firmemente que los cortafuegos no pueden detener los ataques de ransomware.[4]

¿CUÁL ES EL REMEDIO?

- Implemente un acceso a la red de confianza cero que permita las conexiones solo después de verificar las identidades de los dispositivos y de los usuarios, de verificar el estado de seguridad y de aplicar las políticas de seguridad, para cada conexión, cada vez. Esto permite establecer conexiones directas y seguras entre los usuarios y las aplicaciones, en lugar de conexiones desprotegidas a una red.

4. Fuente: Zscaler, Encuesta sobre los cortafuegos de red

SÍNTOMA N.º 3

Grave aumento de políticas

Los equipos de seguridad están intentando lograr la confianza cero en las arquitecturas de red heredadas mediante la configuración de políticas que segmentan las redes en piezas cada vez más pequeñas. En teoría, esto es la microsegmentación, pero el trabajo y el esfuerzo administrativo necesarios para su mantenimiento se vuelven rápidamente inmanejables en la práctica.

Para proteger las aplicaciones actuales, las empresas deben desplegar un número creciente de cortafuegos virtuales por toda la red. Esto da lugar a un tsunami de políticas que requiere una configuración y reconfiguración infinitas para construir algo parecido a la aplicación de confianza cero.

Al igual que sus antepasados, los dispositivos físicos, los cortafuegos virtuales no se pueden ajustar más allá de un determinado punto. Con el tiempo, necesitará miles, si no decenas de miles de políticas, lo que hace que la administración sea una pesadilla.

¿CUÁL ES EL REMEDIO?

- El secreto es separar las redes de las aplicaciones y el control de acceso a los recursos. El acceso a la red de confianza cero permite otorgar a los usuarios individuales acceso directo y seguro a las aplicaciones, no a los segmentos de la red. Esto significa que los usuarios pueden conectarse directamente a las aplicaciones que necesitan mientras el tráfico sigue la ruta más corta posible y que los administradores y los equipos de seguridad ya no tienen que preocuparse por los conductos subyacentes.

No se puede implementar de un día para otro, pero si se hace de forma diligente, puede simplificar la administración de TI, redes y seguridad, al tiempo que ofrece un mejor rendimiento para los usuarios finales.

SÍNTOMA N.º 4

El riesgo de que la infección se propague por sus activos de la nube pública

Los proveedores de nube pública ofrecen cortafuegos virtuales en sus mercados de software en línea que supuestamente están certificados para satisfacer las necesidades de sus clientes. Estos cortafuegos a menudo no son más que versiones virtuales de cortafuegos basados en dispositivos que se ejecutan como instancias de VM en la nube pública.

La ejecución de uno de estos cortafuegos en la nube amplía esencialmente su arquitectura de red heredada para abarcar los recursos de la nube. Esto brinda a los atacantes que pueden infringir sus defensas basadas en el cortafuegos la oportunidad de moverse libremente dentro de una red ampliada y da acceso a sus activos en la nube a cualquier persona dentro de su red.

Además, configurar políticas para gobernar el tráfico entre las cargas de trabajo en la nube pública y las nubes privadas virtuales es complicado y engorroso. Necesitará instancias de cortafuegos virtuales en cada punto de entrada y salida de su arquitectura de nube. Piense por un momento en la interconectividad inherente a la nube y entenderá rápidamente por qué este diseño es tan poco manejable.

Además, tendrá que gestionar una intrincada infraestructura de enrutamiento y redes para que esta arquitectura de nube funcione con el resto de su red heredada.

Recuerde que los cortafuegos no fueron diseñados para detener el movimiento lateral.

¿CUÁL ES EL REMEDIO?

- Invierta en una plataforma moderna que sirva de intercambio entre las cargas de trabajo, independientemente de su ubicación. Esto evita que los atacantes se desplacen lateralmente para acceder a los recursos de la red y simplifica la gestión y la resolución de problemas. Además, ofrece a los administradores un control de acceso granular y condicional que se puede revocar si se cambia el contexto.

SÍNTOMA N.º 5

La adicción a los permisos descontrolados se va de las manos

La transformación de la nube está cambiando la actividad empresarial a escala global, y las organizaciones de todos los sectores están aprovechando la agilidad y libertad para innovar que ofrece la nube. Si forma parte de un equipo de TI o de seguridad, es simplemente cuestión de tiempo que se ocupe de un proyecto de migración a la nube, si aún no lo ha hecho.

El problema es que resulta agotador y farragoso configurar las arquitecturas heredadas basadas en cortafuegos para proteger los activos en la nube. Las políticas proliferan, abundan las complejidades y, además, los usuarios necesitan acceso a las aplicaciones para ser productivos. ¿Qué puede hacer?

El 90 % de los administradores de TI y seguridad admiten que han aplicado políticas altamente permisivas* (al menos temporalmente) para acelerar proyectos y brindar a los usuarios el acceso que necesitan. Con el tiempo, las políticas permisivas se van acumulando y finalmente se ignoran u olvidan, lo que aumenta el riesgo de la organización de sufrir una violación o de ser víctima de un devastador ataque de ransomware. Por supuesto, estas prácticas contradicen directamente las de un enfoque de acceso de confianza cero con privilegios mínimos.

El 85 %
de las organizaciones habrá adoptado una estrategia centrada en la nube para 2025.[5]

El 95 %
de las nuevas cargas de trabajo digitales se despliegan hoy en día en plataformas nativas de la nube.[5]

¿CUÁL ES EL REMEDIO?

- Busque una solución de confianza cero basada en la nube que sea sencilla de implementar y operar. Una plataforma unificada de confianza cero con una única consola de gestión no solo será más fácil de configurar y gestionar, sino que ofrecerá una seguridad más sólida que un cortafuegos perimetral heredado.

5. Fuente: Gartner, "Gartner afirma que la nube será la pieza central de las nuevas experiencias digitales"

SÍNTOMA N.º 6

Exposición a Internet potencialmente infecciosa

Los cortafuegos perimetrales se diseñaron para servir como extremos frontales de red. Son activos expuestos a Internet por naturaleza, lo que permite el acceso directo a las redes y recursos internos en caso de ser vulnerados. Esto significa que el uso de un cortafuegos heredado como puerta de enlace para desplegar servicios de red privada virtual (VPN) pone intrínsecamente en riesgo su red.

La gravedad de estos riesgos se pone de manifiesto en una serie de infracciones recientes realizadas con éxito por atacantes que aprovecharon las vulnerabilidades de las VPN heredadas. El ataque de ransomware a Colonial Pipeline, el mayor ciberataque contra infraestructuras críticas divulgado públicamente que ha tenido lugar en Estados Unidos, se produjo cuando los atacantes "explotaron una VPN heredada que no debería haber estado en uso", según el director general de la empresa.[6]

Las VPN basadas en cortafuegos no ofrecen ninguna manera de implementar controles de acceso granulares ni de restringir qué usuarios pueden conectarse a recursos específicos. Por lo tanto, confiar en las VPN es un enfoque en el que o lo arriesgas todo o nada, pues amplía la superficie de ataque de su red desde la nube hasta los enrutadores y redes inalámbricos domésticos de los empleados individuales. Y cuanto más abarque su red, más daño pueden hacer los atacantes y más rápido pueden hacerlo.

Las VPN basadas en cortafuegos no ofrecen ninguna manera de implementar controles de acceso granulares ni de restringir qué usuarios pueden conectarse a recursos específicos.

¿CUÁL ES EL REMEDIO?

- Busque una alternativa a la VPN que permita un acceso seguro a las aplicaciones estableciendo conexiones uno a uno entre los usuarios y las aplicaciones sobre la base de una identidad dinámica y que tenga en cuenta el contexto. Estas soluciones utilizan conexiones internas que hacen que las aplicaciones sean invisibles a la Internet pública, lo que ofrece un mejor rendimiento que las VPN, además de importantes mejoras en la seguridad.

6. Fuente: "Todo lo que necesita saber sobre cómo fue el ataque cibernético a Colonial Pipeline", TechTarget, abril de 2022.

SÍNTOMA N.º 7

Congestión del tráfico

La empresa distribuida se ha convertido en el estándar, y la mayoría de las empresas están adoptando modelos de trabajo híbridos y remotos para mantenerse al día. Pero cuando hay un gran número de usuarios remotos y usted sigue confiando en una arquitectura de red heredada de castillo y foso, tiene que retornar grandes cantidades de tráfico al centro de datos corporativo para que lo inspeccione su cortafuegos.

No hace falta decir que esta arquitectura es ilógica y compleja. Los cortafuegos antiguos y las pilas de seguridad basadas en dispositivos consumen mucho tiempo y son engorrosos de gestionar. Si utiliza líneas MPLS alquiladas, está pagando una prima por una compleja infraestructura de enrutamiento, conmutación y segmentación del tráfico. Es por ello que el interés en las redes de área amplia definida por software (SD–WAN) está aumentando, pero agregar superposiciones de red solo sirve para aumentar la complejidad y los costos asociados con la administración de cortafuegos.

Tanto el rendimiento de las aplicaciones como las experiencias del usuario final sufren cuando tiene que retornar el tráfico. Por no mencionar la latencia, un problema perenne que se convierte en un problema aún mayor, ya que las organizaciones dependen más de aplicaciones de comunicación que consumen mucho ancho de banda, como Zoom y Microsoft Teams.

¿CUÁL ES EL REMEDIO?

- Una solución de confianza cero basada en la nube coloca los controles de seguridad donde residen los usuarios y las aplicaciones actuales: en la nube. Aplica políticas en línea y en el perímetro para que el tráfico no tenga que hacer ningún salto adicional. Y dado que opera en la ruta de los datos, una plataforma de confianza cero puede supervisar cada conexión y detectar y remediar automáticamente los problemas de rendimiento.

LA CURA DE CONFIANZA CERO

Cómo Zscaler puede sanar su red y su arquitectura

Zscaler Zero Trust Exchange™ es una plataforma nativa en la nube especialmente diseñada para la confianza cero. Zero Trust Exchange permite conexiones directas y seguras basadas en el principio de acceso con privilegios mínimos, inspecciona el contenido en profundidad y verifica los derechos de acceso en función de la identidad y el contexto antes de permitir que se realice cualquier conexión.

El motor de políticas basado en IA/ML de Zscaler, impulsado por la mayor nube de seguridad del mundo, entiende el contexto basado en la información de usuarios, dispositivos y aplicaciones y utiliza este contexto para tomar decisiones inteligentes sobre los niveles de acceso y las restricciones a fin de mantener seguros a los usuarios y los datos. Y Zero Trust Exchange establece conexiones directas uno a uno entre los usuarios y las aplicaciones, lo cual garantiza que las aplicaciones sean invisibles a Internet y, por lo tanto, elimina la superficie de ataque.

Nuestro enfoque hace que la seguridad de confianza cero sea accesible y sencilla para nuestros clientes. Por eso, los líderes del sector y los analistas expertos coinciden en que Zero Trust Exchange es la plataforma de confianza cero más madura y fácil de usar.

Implementar Zscaler Zero Trust Exchange es rápido y fácil, y ofrece una amplia gama de productos de seguridad integrados en línea que sobrealimenta sus capacidades de vanguardia de perímetro de servicio de seguridad (SSE).
Estos incluyen:

- **Cortafuegos de generación en la nube**
- **Sandboxing avanzado en la nube**
- **Puerta de enlace web segura (SWG)**
- **Prevención de pérdida de datos (DLP)**
- **CASB**
- **y más**

Para obtener más información, visite la siguiente página:
www.zscaler.es/products/zscaler-internet-access

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. 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 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