Akamai

WHITE PAPER

Una guía para el acceso de red Zero Trust

¿A quién va dirigida esta guía?

Los arquitectos de redes, ingenieros de seguridad, directores de tecnología (CTO), directores de seguridad de la información (CISO) y otros encargados de tomar decisiones con respecto a la TI y a la seguridad se beneficiarán del contenido de esta guía.

Esta guía proporcionará una revisión completa de los posibles beneficios y las diferencias entre los diferentes sistemas para todo aquel que sea responsable de definir, configurar, implementar y gestionar un proyecto de acceso de red Zero Trust (ZTNA). La guía incluye:

- Las limitaciones y los fallos de seguridad de los enfoques heredados para el acceso a las aplicaciones y por qué se necesita la arquitectura ZTNA.
- Los componentes de la arquitectura ZTNA y cómo funciona.
- Cómo Akamai Enterprise Application Access y Akamai MFA pueden ofrecer la arquitectura ZTNA de forma rápida y sencilla.

A medida que el mundo empresarial cambia y las ciberamenazas aumentan, las empresas están revisando sus ciberdefensas. Muchos se han dado cuenta de que la arquitectura de red tradicional, que dependía de una ubicación centralizada en la que todas las partes podían acceder a las aplicaciones, las hace vulnerables. Este enfoque de seguridad casi medieval, que protege el perímetro y da por hecho que todo está a salvo dentro de él, deja a las empresas expuestas al riesgo de sufrir ciberataques en el panorama actual, en el que predominan las conexiones móviles y la nube. En su lugar, las empresas con visión de futuro están recurriendo al concepto de arquitectura Zero Trust para proteger los activos vitales. Un principio fundamental de cualquier proyecto Zero Trust es la protección de la red. En este white paper se explica cómo los enfoques de red radial tradicionales ya no son suficientes y cómo cambiar a una solución ZTNA puede proporcionar una mejor defensa de los activos esenciales y servir como eje clave para una arquitectura Zero Trust integral.

El ritmo de cambio para las empresas nunca había sido tan rápido

La forma en que las empresas operan y utilizan la tecnología está evolucionando, y a un ritmo cada vez más rápido. La evolución de la informática ha impulsado una rápida transición del alojamiento de aplicaciones empresariales en centros de datos locales al uso de varias nubes públicas, nubes privadas o un enfoque híbrido (tanto en el entorno local como en la nube pública y privada).

La evolución del modelo de negocio también ha impulsado una mayor colaboración entre las entidades y la necesidad de proporcionar a los partners y proveedores acceso a las aplicaciones y los recursos.

Por último, a medida que las empresas siguen adoptando el trabajo remoto o híbrido, los usuarios acceden ahora a las aplicaciones y los recursos empresariales desde cualquier lugar, tanto en dispositivos gestionados como no gestionados.

Con estos cambios, los enfoques heredados para gestionar el acceso a las aplicaciones ya no son suficientes, y las empresas deben adoptar ahora un nuevo enfoque que permita un acceso seguro, independientemente del lugar en que se alojen las aplicaciones o se encuentren los usuarios.

Acceso a las aplicaciones heredadas

Durante más de 20 años, las empresas han usado firewalls para crear un perímetro de seguridad sólido y han confiado en los usuarios que se encuentran dentro de ese perímetro. Este enfoque es similar a tratar las redes como castillos con fosos: paredes gruesas y puertas muy seguras forman el perímetro para proteger el castillo (o, en este caso, la red) y solo se permite el acceso a los usuarios con las credenciales adecuadas. Una vez dentro, los usuarios pueden acceder a aplicaciones específicas en función de su identidad, que se proporciona a través de soluciones de proveedor de identidades (IdP) como Microsoft Active Directory.

Sin embargo, con las redes planas, los usuarios tienen acceso IP a toda la red, lo que significa que pueden detectar otros servidores y aplicaciones. Por ejemplo, si el IdP está configurado correctamente, un usuario podría encontrar el servidor en el que se aloja la aplicación de nóminas, pero cuando intente iniciar sesión en la aplicación, se le denegará el acceso.

Para solucionar este problema de movimiento lateral sin restricciones, las empresas dividieron las aplicaciones a través de redes de acceso local virtuales (VLAN) en segmentos independientes detrás de un firewall y aplicaron reglas basadas en rangos de IP, ahora arcaicas, para usuarios individuales o grupos. Este proceso es vulnerable y propenso a errores. Por ejemplo, imagine el escenario en el que una persona de mantenimiento haya desplazado los equipos para colocarlos en otro estante o haya tenido que restablecer la IP en un nuevo rango. De repente, los usuarios quedan bloqueados y comienzan a generarse las llamadas de asistencia. O tal vez una actualización de software requiera cambios en la arquitectura de una aplicación y los usuarios se redirigen a otro equipo como parte del flujo de trabajo. A continuación, es posible que determinados usuarios o grupos no puedan acceder a ese equipo porque no se han actualizado las reglas del firewall.

Esta arquitectura es extremadamente compleja y requiere que haya un sistema que permita a los propietarios de las aplicaciones, los administradores de red y los grupos de seguridad comunicarse entre sí cuando se produzcan estos cambios, con el objetivo de evitar que haya periodos de inactividad.

Sabemos lo que sucede a menudo cuando esa coordinación falla. Los administradores tratan de seguir las prácticas recomendadas, pero, en un momento de desesperación como este, implantan la temida regla de IP "ANY/ANY ALLOW" como una solución rápida hasta que el problema se diagnostique y solucione, la cual permite que los usuarios afectados tengan acceso a todo. Sin embargo, a menudo no hay tiempo para retroceder y revertir estos cambios, y estas soluciones rápidas limitan la estrategia de seguridad de una empresa con el tiempo.

Las VPN añaden desafíos en términos de complejidad, rendimiento y seguridad

Para los usuarios remotos, una red privada virtual (VPN) normalmente proporciona acceso a las aplicaciones locales alojadas dentro del perímetro, que a su vez proporcionan acceso directo por túnel a la red de la empresa.

Para gestionar el acceso de los usuarios a las aplicaciones, las empresas suelen añadir controladores de entrega de aplicaciones (ADC) dedicados o utilizar los controles de acceso integrados en sus soluciones de VPN. El objetivo es alinear los permisos de acceso a las aplicaciones independientemente de dónde se encuentre el usuario. Si a un usuario se le deniega el acceso a la aplicación de gestión de relaciones con los clientes (CRM) cuando se encuentra dentro del perímetro, se le debe denegar el acceso cuando esté conectado a través de la VPN. Aunque ese es el objetivo, la complejidad de sincronizar los permisos de las aplicaciones entre los dos casos de uso y la implementación de soluciones rápidas pueden ocasionar que los usuarios obtengan acceso no intencionado a las aplicaciones.

Acceso a las aplicaciones para contratistas, partners y proveedores

Las empresas también suelen utilizar la VPN para permitir el acceso remoto a las aplicaciones a contratistas, empresas asociadas o proveedores. Por ejemplo, una empresa puede permitir el acceso externo a sus sistemas financieros para permitir que los proveedores envíen facturas. Permitir el acceso a aplicaciones de terceros a través de una VPN conlleva riesgos adicionales en materia de seguridad, porque la empresa ya no tiene un control integral de tal seguridad. Si un dispositivo de terceros con acceso a la VPN se ve comprometido, los atacantes pueden obtener acceso a la red de la empresa.

Las VPN y el rendimiento

Lo mismo ocurre con el rendimiento. En la VPN más sencilla, todo el tráfico se redirige a la infraestructura del centro de datos, lo cual puede ralentizar en gran medida el acceso a los activos de Internet y el software como servicio (SaaS) como consecuencia de las conexiones, que duplican el tráfico.

Para solucionar este problema de rendimiento, los administradores suelen emplear túneles divididos para marcar los rangos de IP que pueden conectarse a la VPN y los rangos que deberían salir directamente a Internet. Esta solución puede ser muy eficaz y sencilla cuando solo se cuenta con un perímetro interno. Sin embargo, la cosa empieza a complicarse a medida que se añaden varios centros de datos y proveedores de nubes privadas virtuales. En este caso, los administradores deben decidir si instalarán agregadores de VPN en todos los centros de datos y determinar cómo gestionarán los túneles multipunto divididos de forma eficaz.

Esto no quiere decir que las VPN no sean útiles; todo lo contrario. En el caso de las infraestructuras de centros de datos múltiples, de hecho, el acceso de sitio a sitio puede ser muy eficaz. Sin embargo, el acceso a nivel de red no es la mejor solución para los usuarios que acceden a las aplicaciones, ya que dicho acceso compromete de forma antinatural la seguridad y el rendimiento en aras de la simplicidad.

El acceso a las aplicaciones basado en la red es una buena noticia para los atacantes

Hasta ahora, nos hemos centrado en los riesgos y desafíos asociados a la concesión de acceso a nivel de red a todos los empleados. Sin embargo, este enfoque también expone a las empresas a otro riesgo: los ciberdelincuentes que aprovechan las credenciales de usuario robadas o una vulnerabilidad de seguridad también tienen el potencial de obtener acceso sin restricciones en toda la red. Por ejemplo, si un atacante obtiene acceso VPN mediante credenciales de empleados comprometidas, puede moverse lateralmente por la red para encontrar objetivos de gran valor, acceder a ellos y atacarlos.

Estos enfoques abren las puertas a la posibilidad de que se produzca una filtración catastrófica

Teóricamente es posible gestionar el acceso a las aplicaciones de forma segura y con una fricción mínima mediante estos enfoques, e incluso puede que usted esté utilizando una combinación de los mismos. El problema es que implementarlos correctamente, mantenerlos y, al mismo tiempo, ofrecer una seguridad y un rendimiento adecuados de forma permanente suele ser demasiado complejo desde el punto de vista operativo. En muchos casos, las empresas se convencen a sí mismas de que, como los empleados pueden acceder a sus aplicaciones, todo debería funcionar sin problemas. Hasta que, un día, una de las soluciones rápidas descritas anteriormente desemboca en una brecha de seguridad catastrófica o en una degradación tan severa del rendimiento que provoca una interrupción en la red o una considerable disminución de la productividad de los empleados.

Un enfoque Zero Trust para el acceso a las aplicaciones

Dados los defectos inherentes a los enfoques de seguridad perimetral y los desafíos específicos que presentan a la hora de gestionar el acceso a las aplicaciones, el modelo emergente de ciberseguridad Zero Trust supone una alternativa mejor. Presentado por primera vez por Forrester Research en 2010, es un marco que las empresas utilizan para transformar su infraestructura de TI, sus políticas de seguridad y sus procesos empresariales.

El principio detrás de este concepto es bastante sencillo, pero muy efectivo: la confianza no es una cualidad de la ubicación. No se debe confiar en algo simplemente porque está detrás del firewall. En su lugar, solo se debe confiar en una acción, independientemente de dónde ocurra, si se ha permitido de manera explícita. En definitiva, solo *puede* suceder aquello que está *previsto* que suceda. Retire toda la confianza implícita en acciones que no son necesarias porque crean riesgo, pero no valor.

Esto requiere un control estricto de autenticación y autorización, y los sistemas no deben transferir ningún dato hasta que se sepa bien que no existe ningún peligro. Además, se deben emplear métodos de análisis, filtrado y registro para comprobar el comportamiento, y prestar siempre atención a las posibles señales de riesgo.

Este cambio radical podría evitar muchos de los riesgos de seguridad que hemos observado en la última década. Los atacantes ya no podrían aprovechar las debilidades de su perímetro y, posteriormente, obtener acceso a sus datos y aplicaciones confidenciales simplemente porque han logrado entrar en el castillo. Ahora ya no habría ningún foso que superar para obtener acceso. Solo habría aplicaciones y usuarios, cada uno de los cuales debe autenticarse mutuamente y cuya autorización debe verificarse antes de concederse cualquier acceso.

Acceso de red Zero Trust

ZTNA es una arquitectura basada en estos principios que concede un acceso seguro a las aplicaciones y los recursos a partir de una autenticación, una autorización y un contexto sólidos. Una arquitectura ZTNA proporciona acceso solo a las aplicaciones que los usuarios necesitan para realizar su trabajo, no a toda la red. Con un enfoque ZTNA, ya no importa dónde se encuentran los usuarios; ya no existe el concepto de dentro o fuera del perímetro. El lugar en el que se aloja una aplicación es irrelevante, ya sea en el entorno local, en la nube pública o en la nube privada, puesto que los usuarios autenticados solo tienen acceso a las aplicaciones que están autorizados a utilizar.

Por ejemplo, un empleado de ventas solo tendrá acceso a las aplicaciones relacionadas con su función de ventas, no a las aplicaciones de recursos humanos o finanzas.

Cómo funciona la arquitectura ZTNA de Akamai

Akamai Enterprise Application Access y Akamai MFA le permiten migrar a una arquitectura ZTNA, que puede ser un paso importante y fundamental en su transición hacia una arquitectura Zero Trust.

Enterprise Application Access es un proxy con reconocimiento de identidades (IAP) en la nube. Se trata de un servicio flexible y adaptable, con toma de decisiones basada en señales en tiempo real, como inteligencia ante amenazas, perfiles de dispositivo e información de identidad. Akamai MFA es un servicio de autenticación multifactorial que proporciona los niveles más sólidos de autenticación para garantizar que el usuario que solicita acceso es quien afirma ser.

Para empezar, se ejecuta una pequeña máquina virtual denominada conector de Enterprise Application Access detrás del firewall, pero con conectividad a sus aplicaciones. No es necesario que esté, ni *tiene* que estar, dentro de la DMZ. Su dirección debe estar en un espacio de IP privada y no debe ser accesible directamente desde Internet. De hecho, debe parecer exactamente igual que cualquier otra aplicación situada detrás del firewall.

Para admitir entornos multinube, se puede implementar un conector dentro del centro de datos local o en una nube privada o pública.

El conector de Enterprise Application Access establece inmediatamente una conexión cifrada saliente con el IAP en Akamai Connected Cloud. Una vez conectado al IAP, el conector descarga su configuración y se prepara para establecer conexiones. La conexión entre el conector y el IAP es saliente, lo que le permite cerrar todas las conexiones entrantes del firewall, haciendo que las aplicaciones sean casi invisibles en la red pública de Internet.

El IAP lleva a cabo todo el procesamiento previo que se produce antes de que un usuario se conecte a la aplicación, incluida la autenticación, la autorización y las comprobaciones de seguridad y del perfil del dispositivo. Cuando un usuario trata de acceder a una aplicación, se le redirige a Akamai a través de un CNAME de DNS y se le conecta al IAP. Si el usuario final y el dispositivo superan todas las comprobaciones, se le dirige a un servicio de autenticación, autenticación multifactorial y de inicio de sesión único, y luego se llevan a cabo las operaciones para identificar el dispositivo.

Si el usuario y el equipo están autorizados, la conexión del usuario final se vincula a la conexión saliente del conector de Enterprise Application Access. El tráfico de la sesión del usuario fluye a través de este IAP vinculado y, posteriormente, se conecta a la aplicación o al servicio solicitados, A continuación, se establece una ruta de datos completa, y todas las decisiones de acceso se toman de forma continua y dinámica según la identidad, el dispositivo y el contexto del usuario.

Este método de acceso tiene claras e importantes ventajas. Las actividades que requieren un mayor nivel de rendimiento y seguridad se llevan a cabo en el Edge, más cerca del usuario final, donde Akamai tiene más de 4200 ubicaciones distribuidas por todo el mundo.

Además, la entrada vulnerable a la aplicación se realiza a través de un túnel de aplicaciones invertido, lo que elimina de forma eficaz la visibilidad de la IP del perímetro y reduce el riesgo de sufrir ataques volumétricos.

Puesto que Enterprise Application Access se puede integrar directamente con la infraestructura de identidades de una empresa incluso si utiliza varios directorios y proveedores de servicios de identidad, el servicio ZTNA se puede implementar rápidamente sin necesidad de cambiar la infraestructura o arquitectura de identidad existente.

Para las aplicaciones heredadas que no son compatibles con los protocolos de autenticación modernos, Enterprise Application Access tiene una función de conexión de IdP que proporciona autenticación a los IdP basados en SAML y traduce el token de autenticación al protocolo de autenticación compatible con las aplicaciones heredadas.

Lo que hace que los enfoques basados en IAP, como Enterprise Application Access, llamen tanto la atención es el acceso a nivel de aplicación. Con el acceso a nivel de aplicación, el rendimiento y la seguridad *se desvinculan* de la complejidad.

Simplemente hay que agrupar todas las aplicaciones que comparten una localidad (alojadas en el mismo centro de datos o en la misma nube privada virtual, por ejemplo), alojarlas en un espacio de IP de red privada o en una VLAN restringida e introducir un proxy de acceso en ese microperímetro. Eso es todo.

Los propietarios de las aplicaciones establecen sus propias políticas de seguridad para el proxy de acceso, como quién puede tener acceso y por qué, y lo que es más interesante: los usuarios pueden estar en cualquier lugar. No se hace una distinción entre "dentro" y "fuera" del entorno local, ya que no hay ningún perímetro de red que incluya a los usuarios finales. Lo mismo es que un empleado trabaje desde una cafetería que desde una oficina; lo único que importa es si el usuario está autorizado y si el equipo es seguro.

Con el acceso a nivel de aplicación, el rendimiento es óptimo, a pesar de la facilidad de implementación y uso. Los usuarios simplemente utilizan una conexión a Internet para acceder a las aplicaciones directamente, con independencia de dónde estén alojadas o de dónde se ubiquen. De esta forma, Internet enruta paquetes de destino sin tener que pasar por agregadores ni intermediarios que no estén en la ruta.

De hecho, con el acceso a nivel de aplicación, las redes internas suelen funcionar como Wi-Fi de invitados. Recuerde que, para que Zero Trust sea eficaz, no se puede tratar a los usuarios internos y externos de forma diferente: de forma predeterminada, no se confía en nadie.

Estado final deseado de la arquitectura ZTNA

Independientemente de si los usuarios están dentro o fuera del entorno local, se les debería obligar a acceder a todas las aplicaciones a través de proxies de acceso con reconocimiento de identidades. No importa dónde estén alojadas las aplicaciones. Estos proxies no solo deben realizar una autenticación estándar, sino que también deben utilizar una autenticación multifactorial a prueba de phishing, como Akamai MFA. Además, deben existir unas funciones sólidas de análisis de dispositivos para determinar los criterios de tales dispositivos y autorizar el acceso a determinadas aplicaciones.

Tenemos la firme convicción de que la arquitectura ZTNA no termina con la autenticación y autorización. Para respaldar los principios Zero Trust, todos los parámetros que se comprueban en la fase inicial de autenticación y autorización deben supervisarse continuamente durante la sesión de activación. Cualquier cambio detectado debe activar una acción, por ejemplo, volver a autenticar al usuario, eliminar el acceso a la aplicación o limitar el acceso a la aplicación.

Un sistema de seguridad crucial que debe añadirse a los proxies de acceso es la protección de API y aplicaciones web (WAAP), que garantizará que los usuarios finales no lancen ataques a nivel de aplicación (de forma intencionada o no) a sus aplicaciones internas. También se pueden utilizar otros sistemas avanzados, como la detección de humanos o bots, para los sitios sin API, con el objetivo de garantizar que no haya malware oculto en forma de terminales válidos. Es en el IAP donde Akamai puede aplicar capas en WAAP, detección de bots, análisis de comportamiento y almacenamiento en caché. De este modo, se obtiene un rendimiento óptimo y la capacidad de mantener los agentes maliciosos potenciales lo más lejos posible de las ubicaciones, aplicaciones y datos físicos.

La prevención de ataques distribuidos de denegación de servicio (DDoS) cobra especial relevancia cuando sube sus aplicaciones a Internet y las hace accesibles a través de proxies de acceso. Debe asociarse con proveedores que puedan contrarrestar los ataques lanzados contra sus microperímetros y proxies de acceso; de este modo, no tendrá que detener las operaciones en ningún momento.

Por último, para garantizar que sus aplicaciones tengan un rendimiento óptimo y que los usuarios no solo acepten este cambio de acceso, sino que también estén a favor del mismo, los proxies de acceso deberán estar protegidos por redes que potencien el rendimiento. Concretamente, las redes de distribución de contenido y las superposiciones de enrutamiento de Internet deberían formar parte de su arsenal, no solo para facilitar el acceso, sino también para mejorar el rendimiento de una forma nunca antes vista.

Protección contra amenazas

Las soluciones como Akamai Enterprise Application Access pueden proteger sus aplicaciones frente a agentes maliciosos. ¿Pero qué ocurre con la protección de los usuarios para que no se conviertan por accidente en dichos agentes debido a peligros tales como un dispositivo infectado con malware o el robo de las credenciales mediante un enlace de phishing vinculado a una página de destino falsa? A este respecto, la prevención y la detección juegan un papel crucial en el tráfico web.

Existe una estrategia que consiste en implementar una solución de firewall de DNS basada en la nube, como Akamai Secure Internet Access. Este producto se encarga de inspeccionar todas las solicitudes de DNS que realizan los usuarios y aplica inteligencia contra amenazas en tiempo real para que las solicitudes legítimas se resuelvan con normalidad, pero que cualquier solicitud a dominios maliciosos se bloquee de forma proactiva. Esto reduce el riesgo de que los dispositivos de los empleados se vean comprometidos por malware o ransomware, o que sean víctimas de un ataque de phishing.

Resumen

Las arquitecturas de red radial tradicionales, junto con el perímetro de seguridad "castillo y foso", no pueden garantizar un rendimiento ni una seguridad óptimos en el entorno móvil y basado en la nube de hoy en día. Este es un problema que todas las empresas deben empezar a abordar si no quieren ser vulnerables. El rechazo a adoptar arquitecturas de seguridad empresariales más sólidas es la causa número uno de las brechas que se producen actualmente, y el número de filtraciones solo va a empeorar. En pocas palabras, no se puede estar seguro detrás del perímetro, ya que dicho perímetro ya no existe.

Siguientes pasos

¿Cómo comenzar la transición a una arquitectura Zero Trust Network Access?

Los servicios de seguridad en la nube de Akamai pueden combinarse para crear una arquitectura ZTNA integral que no solo facilita un acceso seguro a las aplicaciones en un entorno multinube, sino que también saca partido de la nube para eliminar casi por completo la necesidad de utilizar redes empresariales internas.

Si utiliza nuestra solución de IAP avanzada y distribuida, y nuestra autenticación multifactor a prueba de phishing junto con la potencia de Akamai Connected Cloud, por fin podrá migrar a un mundo sin perímetro de una forma increíblemente fácil, introduciendo sus aplicaciones gradualmente una por una, reduciendo el riesgo de la migración casi a cero y beneficiándose de la larga experiencia de Akamai ofreciendo soluciones de rendimiento y seguridad de eficacia demostrada.

A medida que avance hacia una arquitectura Zero Trust, le aseguramos que Akamai estará con usted durante todo el recorrido, ayudándole en el proceso de adopción de una arquitectura de red que no solo facilita acceso a sus aplicaciones y datos, sino que lo hace de una manera verdaderamente fácil de gestionar y manteniendo en todo momento los más altos niveles de seguridad y rendimiento.

Descubra cómo puede satisfacer sus necesidades empresariales con la cartera de soluciones Zero Trust de Akamai.

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Akamai Connected Cloud, una plataforma de Edge y en la nube de distribución masiva, acerca las aplicaciones y las experiencias a los usuarios y aleja las amenazas. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Publicado el 24 de febrero.