Migre a AWS de forma sencilla y segura con Zscaler

Asignación de Zscaler Private Access al marco de adopción de la nube de AWS

Índice

Introducción

Este documento pretende mostrar cómo Zscaler™ acelera la adopción por parte del usuario eliminando la fricción asociada a la consecución de los objetivos de red y seguridad. Explorar cómo Zscaler Private Access™ (ZPA™) se aplica a los casos de uso de la migración de AWS ayudará a proporcionar un enfoque estructurado de la solución global e ilustrará cómo ZPA acelera la migración de aplicaciones.

Cuando Zscaler se compromete con proyectos del sector comercial y público, la arquitectura ZPA se posiciona como un habilitador para mejorar la agilidad de los usuarios y las aplicaciones, lo que acelera la migración de aplicaciones.

La función principal de ZPA es gestionar activamente el acceso de los usuarios autorizados a las cargas de trabajo (y su interacción con ellas) antes, durante y después de la migración a la nube, mejorando al mismo tiempo la experiencia general del usuario final.

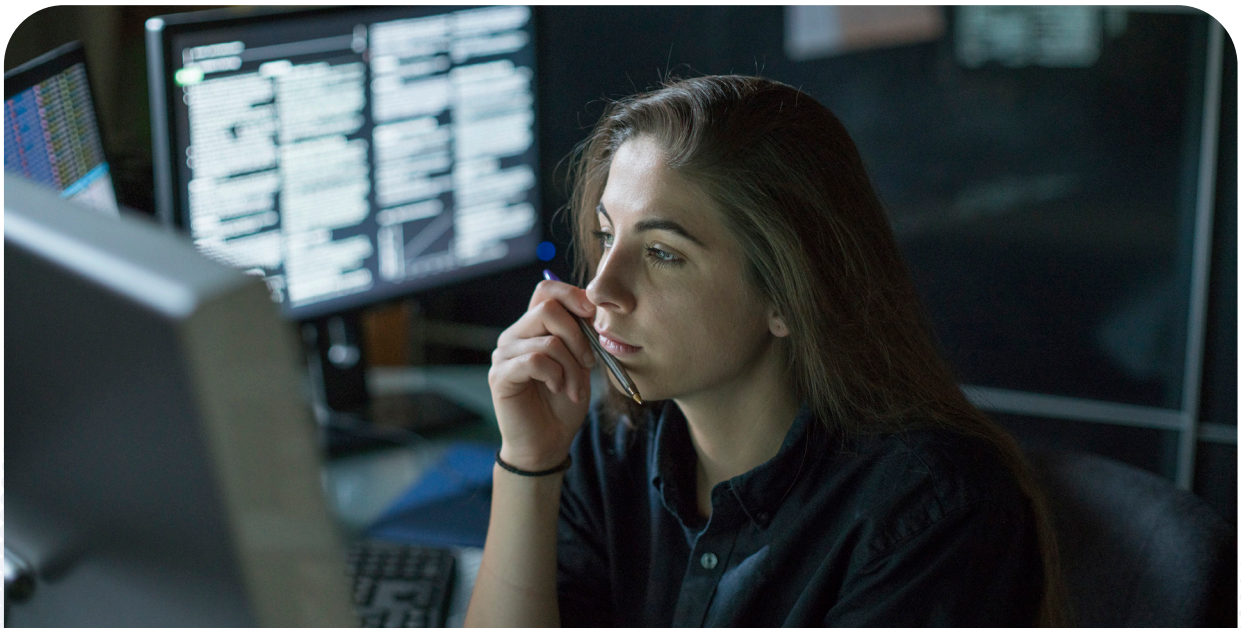
Las mejores prácticas arquitectónicas de Zscaler Private Access desempeñan una función esencial en las fases de migración a la nube del cliente, incluidas:

- Preparación y planificación
- Portafolio y descubrimiento
- Planificación y entrega operativa
- Migración y validación
- Funciones operativas en curso

Aunque este documento se centra en la migración de cargas de trabajo a AWS, la solución ZPA y las soluciones de perímetro definido por software relacionadas no son específicas de las implementaciones de AWS. ZPA admite entornos de TI híbridos y puede utilizarse para aumentar los marcos de migración de aplicaciones definidos por las prácticas de consultoría.

Ventajas de Zscaler Private Access (ZPA):

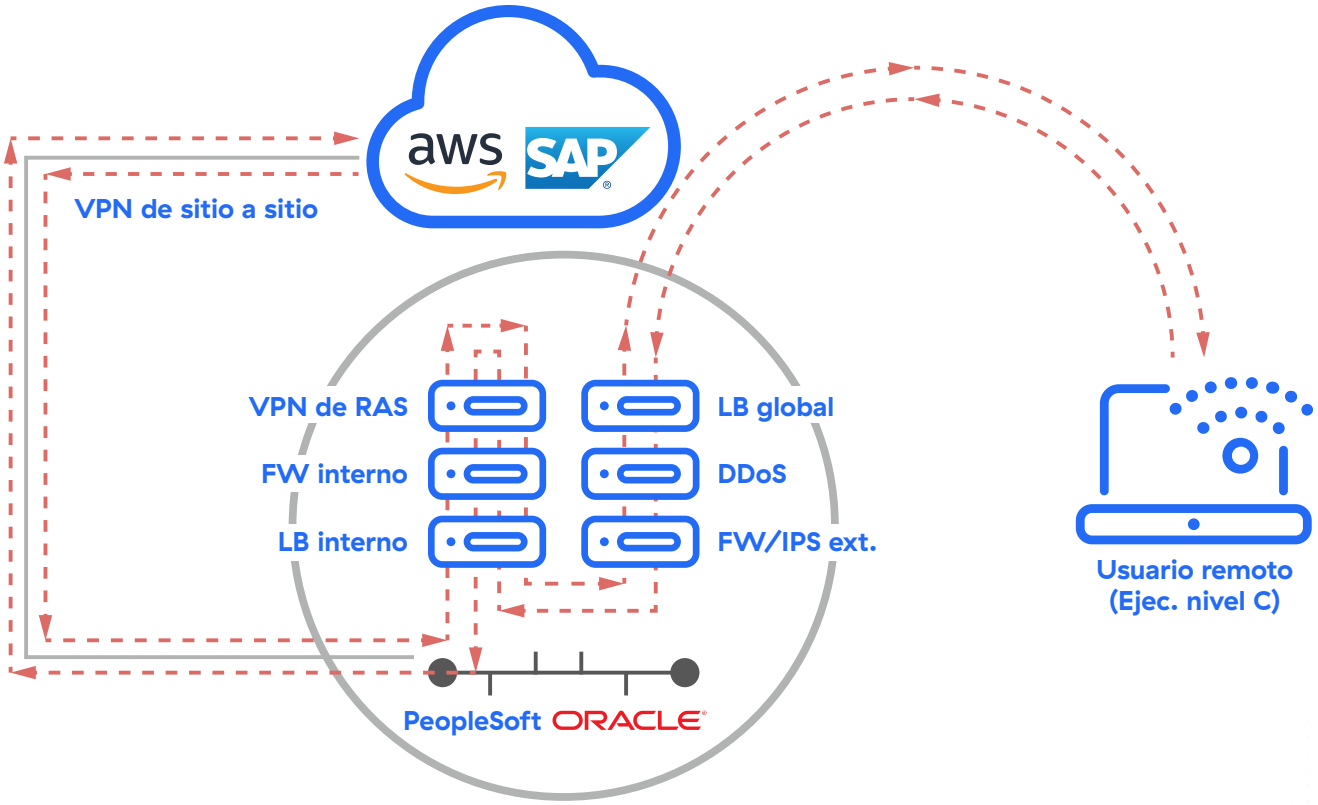
- **Acelere la migración de aplicaciones y la adopción de la nube**
- **Habilite el control granular de acceso de los usuarios a las aplicaciones alojadas en AWS**
- **Gestione activamente el acceso a la carga de trabajo antes y después de la migración**
- **Aporte visibilidad de extremo a extremo de la aplicación y mejore la experiencia del usuario**



Zscaler Private Access: proteger el acceso a las aplicaciones internas

Zscaler Private Access proporciona un acceso seguro a las aplicaciones internas, tanto si se alojan en su centro de datos privado como en la nube pública. Zscaler reduce el coste y la complejidad de las redes heredadas y los retos de seguridad, a la vez que mejora la experiencia de usuario del acceso a la red tradicional basado en VPN.

La mayoría de los clientes comienzan con una infraestructura de red local tradicional, centrada en el centro de datos y basada en hardware, con soluciones de acceso remoto centralizado que se ven así:



ANTES DE ZSCALER: enfoque tradicional de acceso remoto centrado en el centro de datos

Zscaler Private Access ofrece una solución de perímetro definido por software (SDP). Esta metodología centrada en la experiencia del usuario está diseñada específicamente para abordar el escalamiento y otras necesidades de una comunidad empresarial ágil y moderna, que se traslada a la nube, y es completamente diferente de las soluciones tradicionales de VPN de acceso remoto.

Zscaler Private Access aprovecha nuestra arquitectura de nube global y establece un acceso de confianza cero a las aplicaciones privadas. La confianza no se asume nunca, sino que se basa en la autenticación de usuarios y dispositivos a través de SAML. Cuando los usuarios se autentican, se establece una conexión de dentro a fuera desde un conector de aplicaciones en AWS a la nube de Zscaler, donde se establece una conexión segura entre los usuarios autorizados y sus aplicaciones.

Con ZScaler Private Access, el acceso a las aplicaciones está gestionado a través de una nube de seguridad global, y la red se convierte en un mero transporte. Se utiliza acceso granular basado en políticas para conectar a los usuarios autentificados con las aplicaciones para las que están autorizados, de modo que los clientes pueden mantener su nube pública privada.

CON ZSCALER: acceso seguro basado en políticas, con usuarios fuera de la red

Dado que la postura de seguridad del usuario y del dispositivo se evalúa antes de otorgar acceso a la aplicación, las aplicaciones son invisibles para los usuarios que no tienen permiso de acceso. Además, dado que las aplicaciones se gestionan a través de la nube de Zscaler, no hay conexiones entrantes a la instancia de AWS ni con el centro de datos del cliente, por lo que las ACL y los Grupos de seguridad se simplifican. La política se basa en la información del usuario/dispositivo en lugar de los objetos de la red, lo que proporciona una mayor visibilidad y flexibilidad.

Zscaler Private Access permite a un usuario acceder a aplicaciones permitidas simultáneamente tanto en sus VPC de AWS como en sus centros de datos físicos. Abstraer la red del usuario y proporcionar una conexión de ruta más corta a la aplicación mejora la experiencia del usuario, simplifica la arquitectura de red y proporciona mayor visibilidad y control de la seguridad.

Aceleración de la migración de aplicaciones

Zscaler Private Access puede ser muy útil para realizar un análisis empresarial preliminar para determinar la necesidad de una migración. Los retos de cuantificar una infraestructura de aplicaciones existente son amplios; con este enfoque, Zscaler ofrece un marco para una experiencia de usuario sin fisuras tanto en los entornos heredados como en los de AWS. El control de acceso basado en políticas reemplaza a la infraestructura tradicional y la configuración relacionada, así como a la administración continua.

El responsable de arquitectura o el responsable de consultoría pueden reducir potencialmente el plazo general de la migración. ZPA proporciona una plataforma desde la cual se puede controlar el acceso de los usuarios durante la migración de cargas de trabajo a AWS sin ningún cambio en la infraestructura de red heredada. Se puede evitar la necesidad de contar con hardware de VPN tradicional como requisito previo para conectar a los usuarios a las aplicaciones privadas alojadas en AWS, así como la necesidad de que AWS Direct Connect gestione las rutas de tráfico no óptimas para llevar a los usuarios remotos a través del centro de datos al entorno de AWS.

La adopción de la plataforma ZPA permite el control granular del acceso de los usuarios a las aplicaciones alojadas en AWS, en múltiples regiones y en un entorno híbrido. En la práctica, este enfoque puede simplificar la adopción de la nube y permitir al cliente fomentar la confianza con su comunidad de usuarios durante la migración.

Gestión mejorada de identidad y acceso:

- **Las aplicaciones no pueden ser visualizadas por los usuarios/dispositivos que no han sido autorizados previamente**
- **Ayuda a abordar amenazas de seguridad modernas como ataques DDoS y el acceso fraudulento de terceros**
- **Restringe la capacidad de los programas maliciosos de moverse horizontalmente a través de su red interna**

Al mejorar la experiencia del usuario, reducir drásticamente los procesos de control de cambios, ofrecer visibilidad de las aplicaciones de extremo a extremo y proporcionar la capacidad de elegir grupos/ubicaciones discretos para que la migración se lleve a cabo simplemente mediante el uso de la gestión de políticas centralizada, ZPA permite a las empresas migrar más rápidamente y ofrecer la mejor experiencia de usuario.

Cuando las aplicaciones empresariales como SAP, Oracle o Microsoft se migran a AWS, a menudo los enfoques de red y seguridad se aplazan para resolverse más tarde en el ciclo de planificación y ejecución de la migración. Los arquitectos de soluciones de los socios consultores de AWS y APN informan regularmente que, como consecuencia, se enfrentan a fricciones y retrasos. Al contar con una solución elegante y bien entendida como ZPA en la caja de herramientas de planificación al inicio del proyecto, dichas fricciones se pueden entender, anticipar y evitar.

Este proceso a menudo reúne a los arquitectos de la nube, a los responsables de TI, redes y seguridad en un discurso positivo que, de otro modo, no suele formar parte de la fase de preparación y planificación.

Para esas aplicaciones, la migración a IaaS será atractiva y, a menudo, obvia dado el tamaño y el alcance de sus implementaciones. Sin embargo, creemos que un desafío inicial común es identificar todas las aplicaciones a las que acceden los usuarios y que también son candidatas para la migración. En ocasiones, el número de aplicaciones descubiertas es mucho mayor al que los ejecutivos de TI estiman. ZPA realiza informes y facilita la detección de aplicaciones privadas para proporcionar a los clientes visibilidad de todas las aplicaciones a las que se accede en su centro de datos físico. Esto ayuda a la organización consultora y al cliente a priorizar qué aplicaciones se deben migrar a la nube de IaaS y a mejorar los controles de seguridad en torno a esas aplicaciones.

Los clientes pueden identificar más fácilmente las cargas de trabajo que se deben migrar a AWS, pero tendrán que decidir cómo proporcionar las aplicaciones a sus usuarios de forma segura, un reto importante si la aplicación no está diseñada para la entrega basada en la nube.

La gestión de identidades y accesos es clave para cumplir con IaaS. Sin embargo, este control de acceso puede mejorarse aún más, haciendo que las aplicaciones solo puedan ser visibilizadas por los usuarios/dispositivos que hayan sido previamente autorizados. Esto ayuda a abordar las amenazas de seguridad modernas, incluidos los ataques DDoS, el acceso fraudulento desde fuentes de terceros y la capacidad de que el malware se mueva horizontalmente a través de la red interna.

Pudimos implantar un modelo de confianza cero... y sustituimos los enfoques tradicionales por esta implantación moderna, segura y que da prioridad a la nube. También tenemos un control granular sobre los permisos de los usuarios: cada empleado y contratista obtiene acceso solo a lo que necesita tener acceso.

Tony Fergusson, arquitecto de Infraestructura de TI de MAN Energy Solutions

Seguridad mejorada

Zscaler Private Access proporciona un marco de políticas granular para conectar a los usuarios con las aplicaciones, independientemente de dónde residan dichas aplicaciones. ZPA no conecta a los usuarios a la red, sino que abstrae la red por completo del usuario. Esta conectividad de la aplicación tiene múltiples ventajas:

- Los usuarios pueden acceder a las aplicaciones en varios entornos (AWS, en las instalaciones o híbridos) a través de túneles TLS cifrados que se activan a demanda.
- Los usuarios tienen acceso a las aplicaciones internas sin necesidad de entrar en la red.
- El direccionamiento IP puede traslaparse en los centros de datos. Como la red se abstrae del usuario, no se producen superposiciones relevantes.
- La política de acceso a aplicaciones se evalúa en la nube de Zscaler. Cuando se autentica el acceso de usuario y dispositivo, se establece una conexión de aplicación saliente a través del conector de aplicaciones que se ejecuta en el entorno de la aplicación. El entorno de la aplicación es opaco en lo referente a Internet, lo que significa que no hay conexiones entrantes al dispositivo ni al entorno de la aplicación.
- El cliente o un MSP pueden redactar y mantener una política granular por aplicación y por usuario/atributo.

Al conceder a los usuarios acceso exclusivamente a las aplicaciones que necesitan para su función, en lugar de a toda la red, ZPA aporta mayor seguridad que un enfoque tradicional de VPN. Este enfoque permite una postura de seguridad que es inherentemente más eficaz contra las formas más comunes de intrusión y malware. Además, Zscaler aceptará y acelerará la adopción de un enfoque de confianza cero para los clientes de AWS.

En relación con el marco de migración de AWS, ZPA permite el acceso de los usuarios a aplicaciones específicas, dando un enfoque coherente para todas las cargas de trabajo implementadas en AWS. Restringir el acceso de los usuarios solo a las aplicaciones específicas que necesitan para su función mejora la postura de seguridad de la empresa. Además del rol de usuario, el estado de administración de dispositivos también se puede utilizar como contexto para una solicitud a una aplicación. ZPA ayuda a los clientes de AWS a cumplir con su parte del modelo de responsabilidad compartida de AWS al dar mecanismos y metodologías para administrar el control granular sobre qué aplicaciones pueden ser accedidas por los usuarios correspondientes, y en qué dispositivos se puede realizar dicho acceso.

Cómo Zscaler Private Access acelera la migración a AWS

Preparación y planificación

Zscaler Private Access se puede utilizar para acelerar la adopción de AWS y evitar múltiples fases de proyectos tradicionales que, de lo contrario, serían necesarias para cumplir con este objetivo. En concreto, estableciendo una línea de base para la parte más exigente e importante, aunque a menudo olvidada, de cualquier migración: sus usuarios.

ZPA permitirá al cliente:

- Aprovechar la "identidad" como el nuevo perímetro, dando una capa de abstracción entre los usuarios y las aplicaciones que intentan consumir.
- Asume una postura de seguridad que no confía intrínsecamente en los usuarios en función de si están dentro o fuera del perímetro de la red de la empresa. En su lugar, los usuarios se autentican a través de su solución de gestión de identidades y accesos (IAM) y se les concede acceso a sus aplicaciones, teniendo en cuenta una serie de controles de políticas. Los controles se pueden basar en atributos SAML producidos por la solución IAM.
- Habilite un enfoque basado en riesgos utilizando autenticación multifactor (MFA).
- Reduzca la necesidad de un acceso privilegiado elevado y minimice drásticamente la superficie de ataque para cualquier acceso entrante. Esto se logra interceptando las solicitudes de los usuarios de acceder a aplicaciones internas y aplicando la política antes de conectar al usuario a la aplicación, básicamente haciendo que las aplicaciones sean "opacas" tanto en lo referente a Internet como para los usuarios internos no autorizados.
- Ofrezca una experiencia de usuario sin fricciones integrándose de forma transparente en el flujo de trabajo normal de los usuarios, independientemente de si el usuario está en una red corporativa o pública. Con Zscaler Client Connector (antes Zscaler App) instalado, no se requiere ninguna acción del usuario para conectarse a las aplicaciones, independientemente de su ubicación o del dispositivo que haya elegido utilizar.

En esta sección se describen más detalles y ventajas para cada uno de los siguientes pasos, a los que se hace referencia en las recomendaciones de prácticas de migración a la nube de AWS, que suelen ser adoptadas por los clientes y las consultorías:

- **Preparación y planificación**
- **Portafolio y detección**
- **Planificación y entrega operativa**
- **Migración y validación**
- **Operaciones en curso e inversiones futuras**

Portafolio y descubrimiento

Muchos clientes ya están en pleno proceso de convertirse en empresas que priorizan la nube. En Zscaler entendemos que los desafíos que los clientes quieren evitar en las iniciativas de migración a la nube incluyen:

- Experiencia de usuario deficiente a medida que las aplicaciones se trasladan de los centros de datos privados a la nube pública; tanto por tener que educar continuamente a los usuarios sobre cómo consumir aplicaciones como por la complejidad relativa al rendimiento de las aplicaciones.
- Complejidad de la red causada por la conexión de centros de datos privados a la nube pública.
- Coste y complejidad del dimensionamiento, la gestión y la predicción de la capacidad deseada que requiere su negocio global.
- Importante amenaza para la seguridad e incertidumbre que supone permitir la entrada de usuarios de confianza y no de confianza en la red de la empresa

Zscaler Private Access supera estos retos ofreciendo visibilidad en las aplicaciones internas en las siguientes tres fases clave de diseño de seguridad:

- Detección: la detección de aplicaciones basado en el acceso del usuario ilustra qué aplicaciones internas se consumen dentro de una organización y, posteriormente, qué aplicaciones se consumen de AWS.
- Ajuste: una vez que se ha detectado una aplicación, puede realizar ajustes de la política para establecer un punto de referencia antes de la migración. Esto evita la exposición una vez trasladada a AWS y también reduce el tiempo hasta la entrega final.
- Producción: la segmentación de aplicaciones le permite aplicar políticas rápida y granularmente para que coincidan con la postura de seguridad y entrega que se requiere para la producción completa.

Cliente destacado:

Para un gran productor global de bebidas, el proceso de detección reveló más de 500 aplicaciones en las instalaciones. Zscaler activó el departamento de TI en 95 minutos; la puesta a punto incluía MFA y otros atributos. La producción ha cambiado poco desde la implementación inicial.

Zscaler Private Access ayuda a acelerar la fase de detección al integrarse de forma transparente en el flujo de trabajo de los usuarios. Los usuarios simplemente acceden a la aplicación que desean utilizar, sin necesidad de interactuar primero con ningún software de seguridad, como un cliente de punto final. Los usuarios ya no necesitan comprender cómo se accede a una aplicación, ya sea nueva o heredada, y los administradores tienen visibilidad total de los flujos de aplicaciones.

Planificación y entrega operativa

A medida que los clientes identifican qué aplicaciones migrar a AWS, toman la decisión de cómo brindar la aplicación a los usuarios. Esto adopta esencialmente una de las tres formas:

Virtualizar – Mantener la privacidad

- Comprenda la arquitectura actual de la aplicación. En un entorno de tres niveles (servidor web, servidor de aplicaciones, servidor de bases de datos), cada componente se virtualizaría y migraría a AWS sucesivamente.
- El front-end se puede migrar primero, y el servidor de aplicaciones/base de datos puede permanecer disponible a través de VPN o una conexión de dedicación como Direct Connect.
- La aplicación permanece “privada" y solo se puede acceder a ella a través de la VPN o de una conexión dedicada.

Gracias a Zscaler, pudimos ser muy ágiles. No hemos recibido más que elogios de otros departamentos, ya que pueden continuar su trabajo desde casa. Zscaler básicamente acaba con la idea de una VPN tradicional".

Marc De Serio, CTO, Henry M. Jackson Foundation (HJF)

Virtualizar – Hacer pública

- Similar a la primera forma; sin embargo, el servidor web front-end está disponible en Internet directamente
- La solicitud se puede resolver públicamente.
- Requiere implementar un cortafuegos de aplicaciones web (WAF) para controlar el contenido entrante/saliente de la aplicación, protecciones DDoS, e implantar la gestión de identidades y accesos para restringir el acceso de los usuarios.

Recrear para la nube

- Aplicaciones que no pueden o no van a ser migradas en su forma actual.
- El front-end pasará a EC2 o Serverless con CloudFront: reuso y recodificación del servidor web.
- La capa media pasará a EC2 o Serverless; reutilizar el middleware.
- El back-end pasará a RDS/Aurora/etc. – actualizar esquema, DB, etc.
- IAM controla el acceso; WAF controla el contenido.
- La experiencia y el acceso del usuario cambian en función de la migración a una nueva arquitectura.

Hacer pública la aplicación tiene un riesgo para la seguridad, que se puede cuantificar. Para algunas aplicaciones, este riesgo, tanto con la reestructuración como con la virtualización, puede ser aceptable para la empresa. ZPA puede permitir a los clientes anunciar aplicaciones públicamente y, al mismo tiempo, dar la misma arquitectura de seguridad mediante el aprovechamiento del acceso basado en el navegador. Esto requiere la misma autenticación SAML en ZPA, utiliza la misma arquitectura ZPA para el acceso no entrante y proporciona la misma visibilidad y el mismo marco de políticas.

No obstante, para una serie de aplicaciones, como SAP, el riesgo de exponer la aplicación directamente a Internet es demasiado grande. De hecho, la seguridad debe mejorarse como parte de la migración a AWS. ZPA permite a los clientes planificar su migración, mejorar la seguridad como parte de esa migración y mantener las aplicaciones privadas.

Migración y validación

Como parte de la migración, es importante comprender dónde se está mejorando. Zscaler Private Access proporciona visibilidad en lo referente a dónde se consumen las aplicaciones y la política de seguridad que las rodea.

Zscaler Private Access actúa como una capa de abstracción entre el usuario y la aplicación. La ubicación de la aplicación se puede cambiar de centro de datos a nube pública o de VPC a VPC, sin ningún efecto negativo en la experiencia del usuario. Los usuarios nunca se conectan directamente a las aplicaciones; el tráfico debe pasar por el servicio en la nube de ZPA. Además, los usuarios nunca se colocan en la red, lo que da como resultado una postura de seguridad más sólida. Todas las comunicaciones ZPA son conexiones salientes desde el centro de datos o la nube pública hasta el servicio en la nube ZPA. En consecuencia, los cortafuegos o ACL del centro de datos se pueden configurar para denegar todas las conexiones entrantes, y el centro de datos/VPC puede ocultarse completamente.

Zscaler Private Access se integra con el centro de operaciones de seguridad (SOC) de un cliente para la entrada y la producción de informes/análisis de SIEM. La consola de gestión de la ZPA ofrece una representación gráfica de las aplicaciones y los usuarios, y se pueden realizar cambios en las políticas para controlar el acceso de los usuarios a las aplicaciones.

Zscaler no proporciona servicios de migración; sin embargo, Zscaler refuerza el proceso de validación de la migración y garantiza que la experiencia del usuario está en línea con los requisitos de la empresa. La visibilidad del cliente y del consultor sobre el progreso de las migraciones de las aplicaciones es un elemento clave apoyado por ZPA.

Cliente destacado:

Para el gobierno del Reino Unido, ZPA es ahora una herramienta integral utilizada para proporcionar aplicaciones y acceso en AWS. Este cliente ha adoptado un modelo de confianza cero: TODAS las aplicaciones se consumen únicamente a través de ZPA.

Operaciones en curso e inversiones futuras

Zscaler Private Access permite que AWS y los administradores de nuestro cliente creen políticas personalizadas por aplicación y por usuario, a escala global. Esto puede reducir la complejidad impuesta por la segmentación basada en la red.

- Políticas sencillas para segmentar el acceso en función de la identidad y la aplicación.
- Evite la necesidad de crear e implementar políticas basadas en direcciones IP difíciles de administrar. En otras palabras, las operaciones pueden ser ágiles internamente, pero el consumidor de la aplicación no se ve afectado. Aproveche las DevSecOps para migrar aplicaciones de la nube privada a la pública, manteniendo la nube pública como privada.
- Proporcione a los clientes mayor visibilidad y control sobre las aplicaciones a las que pueden acceder terceros y contratistas.
- Zscaler invierte continuamente en la nube de Zscaler y en el avance de sus capacidades. Estos avances se basan en los aprendizajes y requisitos de los clientes que abarcan el tráfico de muchas organizaciones mundiales, lo que proporciona un alcance y una visibilidad que ninguna organización puede reproducir por sí sola. Esto proporcionará un valor añadido continuo con la inversión en ZPA.

La infraestructura tradicional de VPN de acceso remoto presenta un riesgo para cualquier estrategia de migración, ya que amplía la superficie de amenazas al poner siempre a un usuario dentro de la red. Zscaler Private Access supera este riesgo mediante la implementación de los siguientes cuatro principios clave de seguridad:

- Conexión de usuarios a aplicaciones privadas (en VPC o DC físico) sin llevarlos a ninguna red interna
- Nunca exponer las aplicaciones a usuarios no autorizados
- Permitir la segmentación de aplicaciones sin depender de una segmentación de red costosa y compleja, pero estrechamente alineada con VPC, grupos de seguridad y/u otras funciones de servicio
- Utilizar Internet como un transporte de red seguro sin depender de las VPN que pueden aumentar la superficie de ataque y complicar la experiencia del usuario

Este enfoque significa que no puede haber movimiento lateral a aplicaciones no autorizadas. Además, esas aplicaciones a las que el usuario no tiene acceso permanecen completamente ocultas; no se pueden descubrir a través de análisis de puertos ni ningún otro mecanismo, ya sea local o de Internet dirigido al entorno alojado. Las aplicaciones no reciben ninguna conexión entrante directamente de los usuarios.

Cliente destacado:

MAN Energy Solutions es ahora un desarrollador asociado que solo tiene acceso a los entornos y aplicaciones DevOps necesarios. El acceso de los socios en el pasado representaba una superficie de ataque potencial; ahora está contenida, ya que sus controles de acceso basados en la identidad mantienen a estos usuarios y sus dispositivos fuera de la red.

Conclusión

La función principal de ZPA es gestionar activamente el acceso de los usuarios autorizados a las cargas de trabajo (y su interacción con ellas) antes, durante y después de la migración a la nube, mejorando al mismo tiempo la experiencia general del usuario final.

Entre las principales ventajas de la transformación se incluyen:

- Reducción de los plazos de los proyectos de transformación y migración
- Mejora de la postura de seguridad con las aplicaciones migradas
- Experiencia de usuario mejorada durante y después de la migración de aplicaciones

Entre los casos de uso de la adopción de ZPA se incluyen

- Adopción de la nube y migración de aplicaciones
- Fusiones y adquisiciones
- Acceso de terceros

Zscaler Private Access puede implementarse en modalidades específicas o de forma integral. ZPA se basa en AWS, y ZPA Public Service Edge se implementa en AWS y en otras ubicaciones en todo el mundo. Las VPC cuentan con Zscaler App Connectors. Zscaler Client Connector es una aplicación ligera compatible con los principales sistemas operativos de PC y dispositivos móviles. Póngase en contacto con nosotros para solicitar una prueba gratuita, un POC formal o una implementación de producción incremental que sustituya al POC. ZPA está disponible en AWS Marketplace como contrato de SaaS, con ofertas privadas.

Referencias

Recursos adicionales para su información:

Página de inicio de Zscaler: www.zscaler.es

Página de inicio de ZPA: www.zscaler.es/products/zscaler-private-access

Página de inicio de ZPA para AWS: www.zscaler.es/products/zpa-for-aws

Soporte y documentación técnica: help.zscaler.com/zia?filter=documentation

MAN Energy Solutions: www.zscaler.es/resources/case-studies/man-energy-solutions.pdf

Marco de adopción de la nube de AWS: aws.amazon.com/professional-services/CAF/

Modelo de responsabilidad compartida de AWS: aws.amazon.com/compliance/shared-responsibility-model/

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