INFORME COMERCIAL

aruba
a Hewlett Packard Enterprise company

LOS MEJORES SD-WAN Y SASE DE SU CLASE CON ZERO-TRUST IMPULSAN LA EMPRESA DIGITAL

TABLA DE CONTENIDO

RESUMEN EJECUTIVO 3

LAS APLICACIONES SE PROPORCIONAN EN LA NUBE; LA SEGURIDAD TAMBIÉN DEBERÍA 3

LA MEJOR SASE DE SU CLASE BRINDA LIBERTAD DE ELECCIÓN 5

PROTEGER LA IOT EMPRESARIAL CON UN ENFOQUE ZERO-TRUST 5

PROTEGER LAS SUCURSALES DE AMENAZAS EXTERNAS CON UNA SD-WAN AVANZADA 7

LA TRANSFORMACIÓN DE LA WAN ES FUNDAMENTAL PARA EL ÉXITO DE LA TRANSFORMACIÓN DIGITAL 7

SATISFACER LAS EXIGENCIAS DE LOS SLA DE APLICACIONES 8

CONCLUSIÓN 8

RESUMEN EJECUTIVO

Las empresas continúan adoptando la transformación digital con la intención de aumentar la eficiencia, mejorar la satisfacción del cliente, buscar nuevas oportunidades de mercado, impulsar la rentabilidad y mantener una ventaja competitiva. La migración de las aplicaciones empresariales a la nube es fundamental para el éxito de cualquier iniciativa de transformación digital. ¿Por qué? Hoy en día, hay más aplicaciones que se ejecutan en la nube que en los centros de datos empresariales tradicionales, y la mayoría de estas aplicaciones se consumen como software como servicio (SaaS). Además, en el mundo del enfoque cloud-first, las empresas deben garantizar que las aplicaciones sean accesibles de forma directa y segura en cualquier momento, desde cualquier lugar y con cualquier dispositivo. También necesitan asegurarse de que la red ofrezca siempre la máxima calidad de experiencia tanto a los empleados como a los clientes. Por último, la explosión de los dispositivos móviles y la IoT en la empresa ha aumentado drásticamente la superficie de ataque, y expone a las empresas a violaciones de la seguridad que pueden comprometer los datos y dar lugar a tiempo de inactividad de la red.

Las redes corporativas actuales nunca se diseñaron para el mundo con un enfoque cloud-first y se quedan cortas a la hora de abordar los desafíos de ciberseguridad de la transformación digital. Es fundamental que las empresas no solo protejan las aplicaciones en la nube, sino también a los usuarios que se conectan a ellas en una red de área amplia (WAN). Al mismo tiempo, la proliferación de dispositivos de la IoT ha aumentado la superficie de ataque significativamente y exponen a las organizaciones a crecientes amenazas de ciberseguridad.

Por lo tanto, el imperativo estratégico es adoptar una red de área amplia definida por software (SD-WAN) más inteligente, más segura y altamente automatizada que pueda integrarse a la perfección con los servicios de seguridad proporcionados en la nube para formar la mejor arquitectura de borde de servicio de acceso seguro (SASE) de su clase. La SASE debe ser complementada con seguridad Zero Trust basada en la identidad para imponer la segmentación de manera que los usuarios y los dispositivos de la IoT solo puedan acceder a los destinos de la red que correspondan a su función en la empresa.

Dado que la transformación de la WAN y la seguridad es un largo camino, una empresa puede empezar por modernizar su WAN o su seguridad, pero para obtener verdadero valor de las inversiones en la nube, deben abordarse ambos aspectos.

Las redes corporativas actuales nunca se diseñaron para el mundo con un enfoque cloud-first y se quedan cortas a la hora de abordar los desafíos de ciberseguridad de la transformación digital. Es fundamental que las empresas no solo protejan las aplicaciones en la nube, sino también a los usuarios que se conectan a ellas. Al mismo tiempo, la proliferación de dispositivos de la IoT ha aumentado la superficie de ataque significativamente y exponen a las organizaciones a crecientes amenazas de ciberseguridad.

Y es igualmente importante evitar la dependencia de un proveedor eligiendo socios de soluciones tecnológicas que proporcionen flexibilidad y libertad de elección. Con arquitecturas de red y seguridad transformadas, las empresas pueden adoptar nuevas innovaciones oportunas para acelerar la productividad, el crecimiento de los ingresos y la rentabilidad, mientras se conservan los costos.

LAS APLICACIONES SE PROPORCIONAN EN LA NUBE; LA SEGURIDAD TAMBIÉN DEBERÍA

Tradicionalmente, todo el tráfico de las aplicaciones procedente de las sucursales se redireccionaba a través de los servicios MPLS privados hasta el centro de datos corporativo para su inspección y verificación de seguridad (ver figura 1). Esta arquitectura tenía sentido cuando las aplicaciones se hospedaban exclusivamente en el centro de datos corporativo. Pero con la migración de las aplicaciones y los servicios a la nube, esta arquitectura de red tradicional se queda corta, principalmente porque perjudica el rendimiento de las aplicaciones y ofrece una experiencia de usuario incoherente, ya que el tráfico destinado a Internet pasa primero por el centro de datos y el firewall corporativo antes de llegar a destino.

Además, con cada vez más empleados que trabajan fuera de la red corporativa y se conectan directamente a las aplicaciones en la nube, la seguridad tradicional basada en el perímetro es insuficiente. La nube y el SaaS han cambiado para siempre la forma en que los usuarios se conectan e interactúan con las aplicaciones. Al transformar las arquitecturas WAN y de seguridad, las empresas pueden garantizar acceso directo y seguro a las aplicaciones y los servicios a través de entornos de varias nubes, independientemente de la ubicación o los dispositivos que se utilizan para acceder.

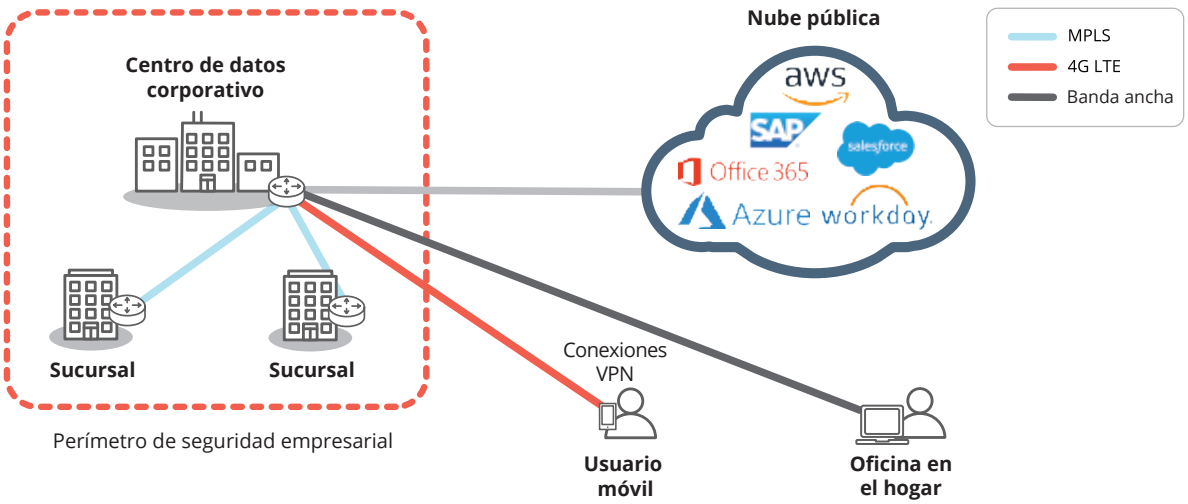

Figura 1: Las WAN empresariales tradicionales y los enfoques de seguridad basados en el perímetro no están diseñados para la nube. Redirigir el tráfico de las aplicaciones desde las sucursales a los centros de datos perjudica el rendimiento y brinda una experiencia de usuario incoherente.

En 2019, Gartner acuñó el término SASE o Secure Access Service Edge para un marco que combina SD-WAN con las funciones de Security Service Edge (SSE) proporcionadas en la nube, incluida la gateway web segura (SWG), el firewall como servicio (FWaaS), un agente de seguridad de acceso a la nube (CASB) y el acceso a la red Zero Trust (ZTNA). Anteriormente, cada una era una función única y dedicada, pero ahora pueden ofrecerse desde la nube de forma unificada, como se muestra en la Figura 2.

Algunos de los primeros que adoptaron las soluciones SSE no lograron implementar una SD-WAN que no pudiera aplicar la desconexión adaptativa de Internet directamente desde las sucursales. Por lo tanto, no podían dirigir el tráfico directamente de la sucursal a la nube. Sin el componente SD-WAN, el tráfico destinado a la nube seguía redireccionándose al centro de datos, lo que afectaba al rendimiento de las aplicaciones negativamente.

La adopción de soluciones Security Service Edge y SD-WAN elimina el costo y la complejidad que se asocian con la gestión de múltiples firewalls locales, aunque sigue siendo necesaria la funcionalidad del firewall en las sucursales para bloquear la entrada de amenazas. Como se muestra en la Figura 3, con una solución SD-WAN avanzada, las empresas pueden conectarse directamente a la nube a través de la desconexión adaptativa de Internet utilizando conexiones de Internet de banda ancha. La inteligencia para reconocer las aplicaciones de la lista blanca permite la desconexión local desde la sucursal hasta el punto de presencia (PoP) más cercano, elimina la latencia y ofrece la máxima calidad de experiencia para aplicaciones SaaS y en la nube de confianza, como Microsoft Office 365, 8x8 y RingCentral. El conocimiento de las aplicaciones también brinda la posibilidad de enviar el resto del tráfico de Internet primero a un proveedor de seguridad en la nube para una inspección

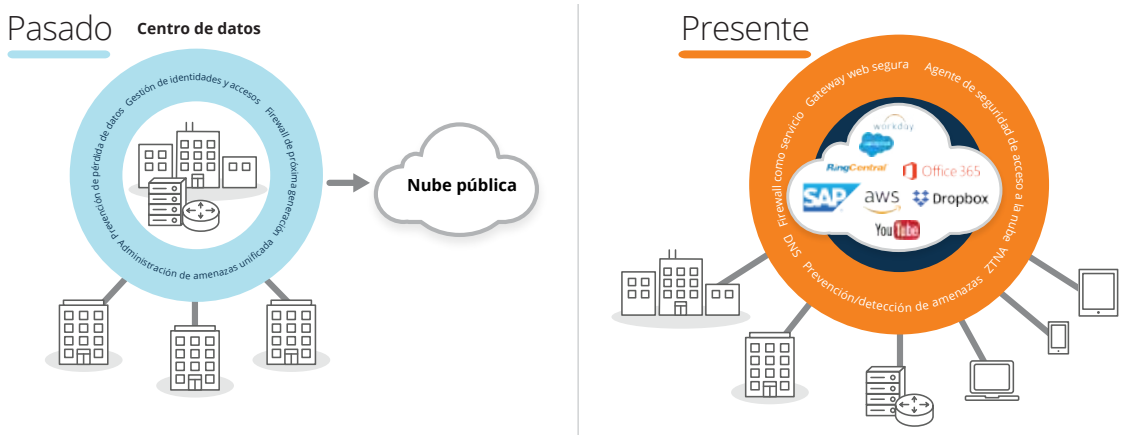

Figura 2: En el pasado, se trataba de proteger el centro de datos de la empresa donde se hospedaban exclusivamente las aplicaciones. Ahora que las aplicaciones han pasado a la nube y se proporcionan allí mismo, la seguridad basada en el perímetro de la empresa es cada vez más ineficaz. Es imperativo pensar diferente y trasladar la seguridad a la nube.

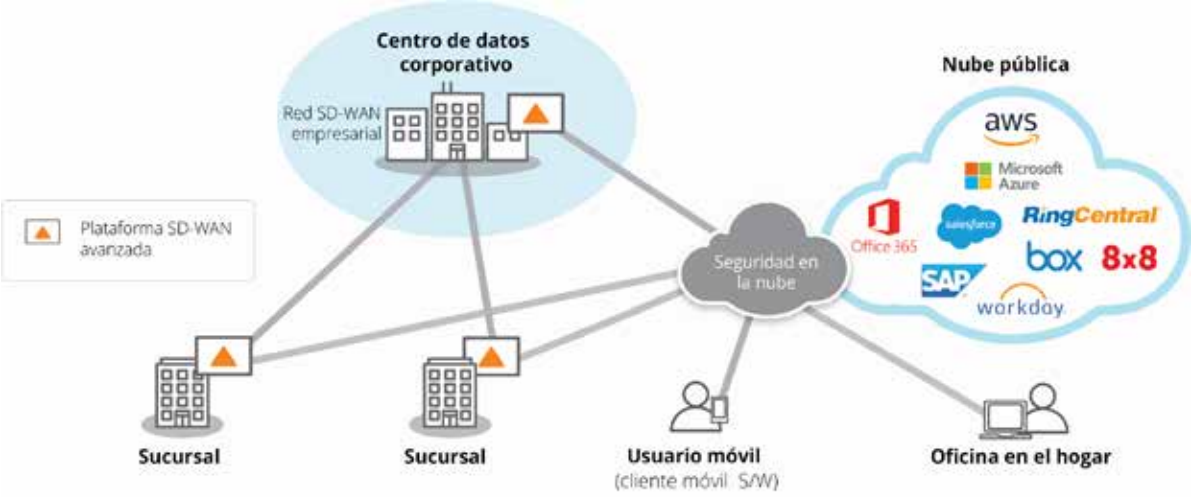

Figura 3: Una SD-WAN avanzada proporciona a las empresas fácil acceso a una nube segura. Las sucursales pueden utilizar las conexiones de banda ancha y la desconexión adaptativa de Internet para conectar a los usuarios directamente con las aplicaciones en la nube y optimizar el rendimiento de las aplicaciones y la experiencia del usuario. La combinación de la SD-WAN avanzada y la seguridad en la nube crea un borde de servicio de acceso seguro (SASE) que garantiza que los usuarios, los dispositivos y las aplicaciones estén siempre protegidos.

avanzada antes de reenviarlo a un proveedor de SaaS. Las capacidades avanzadas de la SD-WAN integradas con los modernos servicios de seguridad en la nube garantizan la aplicación de políticas coherentes y el control de acceso para usuarios, dispositivos, aplicaciones y la IoT. Esto permite a las empresas cumplir con las normativas, evitar el tiempo de inactividad y mitigar el riesgo de que los datos se vean comprometidos por una violación de seguridad.

LA MEJOR SASE DE SU CLASE BRINDA LIBERTAD DE ELECCIÓN

Dados los enfoques de seguridad en la red en constante evolución y la dificultad de la creación de soluciones de red complejas, es importante evaluar las mejores soluciones de seguridad y de red de los proveedores con experiencia y foco demostrados. Es poco realista encontrar un único proveedor que pueda ofrecer las mejores capacidades de SASE de su clase en ambos dominios. Además, las empresas no deberían verse obligadas a conformarse con las capacidades básicas de ninguno.

Dado que la seguridad es una de las principales preocupaciones por la continua evolución de las amenazas, las empresas deben conservar la agilidad necesaria para adoptar rápidamente y de forma rentable nuevas soluciones de seguridad sin depender de la solución de un único proveedor. Disponer de una solución de red independiente permite a las empresas contar con la garantía y tranquilidad necesarias para seleccionar e implementar las soluciones de seguridad en la nube que mejor se adapten a sus necesidades empresariales y de seguridad en evolución.

Una solución SD-WAN avanzada se integra bien con varios proveedores de SSE y ofrece la libertad de elegir las mejores soluciones de proveedores de su clase que unifican la SD-WAN y la seguridad en la nube mediante la orquestación automatizada. Con la mejor SASE de su clase, las empresas construyen una arquitectura de seguridad coherente que bloquea el impacto de los ciberataques y a la vez aumenta la agilidad empresarial y reduce la complejidad. En última instancia, esto permite a las empresas obtener un efecto multiplicador de sus inversiones existentes y en curso en aplicaciones y servicios en la nube.

PROTEGER LA IOT EMPRESARIAL CON UN ENFOQUE ZERO-TRUST

La proliferación de dispositivos de la IoT en las empresas aporta nuevas formas de supervisar, informar, alertar, automatizar y optimizar los procesos empresariales, desde las líneas de fabricación hasta la automatización de HVAC y la iluminación para ahorrar energía. La IoT hace que las empresas sean más eficientes a través de la automatización; no obstante, también aumenta la superficie de ataque al agregar una nueva dimensión de complejidad. La manera en que las TI abordan el creciente desafío de la seguridad de los dispositivos móviles es implementando una solución de acceso a la red Zero Trust (ZTNA) basada en el modelo Zero Trust. Una solución ZTNA funciona instalando un agente de terminales en el dispositivo de un usuario, como una laptop, una tablet o un teléfono móvil.

Ese agente de software garantiza que el tráfico del dispositivo se dirija a un servicio de seguridad en la nube

antes de dirigirse a una aplicación SaaS o a un proveedor de IaaS. Sin embargo, a diferencia de las tablets y los teléfonos inteligentes, los agentes de software de ZTNA no pueden instalarse en los dispositivos de la IoT, ya que son sin agente; no admiten la instalación de agentes de software de terceros. Por ello, las empresas necesitan una solución de seguridad diferente para los dispositivos de la IoT que proteja las redes corporativas de posibles vulnerabilidades de la red que interrumpan las operaciones empresariales cotidianas.

Una SD-WAN avanzada que admite una arquitectura Zero Trust segmenta dinámicamente la red y aplica los principios de acceso menos privilegiado, lo que permite a las empresas reducir el riesgo asociado a las violaciones al implementar dispositivos de la IoT. Garantiza que los usuarios y los dispositivos solo se comuniquen con destinos coherentes con su función según la identidad, los derechos de acceso y la postura de seguridad. Orquesta la segmentación de seguridad integral que abarca la LAN-WAN-LAN y la LAN-WAN-Centro de Datos/Nube de la empresa, lo que permite aplicar políticas de seguridad coherentes y automatizadas con mayor visibilidad. Con la segmentación de seguridad integral, las empresas pueden crear segmentos aislados para el tráfico de dispositivos de la IoT. Se puede definir una política de seguridad independiente para cada segmento que delinee la política de seguridad aplicable al tráfico del dispositivo. Dado que el tráfico de un segmento está aislado del tráfico de todos los demás segmentos, se impide el acceso no autorizado. Aunque apareciera una amenaza, su impacto sería contenido en el segmento en el que surgió.

Veamos un ejemplo. En un sitio remoto en el que se instalan dispositivos de la IoT sin agente, como sistemas PoS y HVAC (Figura 4 a continuación), una plataforma SD-WAN avanzada identifica las aplicaciones utilizadas por los dispositivos de forma única. Una política del sistema intercepta el tráfico del PoS y lo dirige al centro de datos corporativo donde se hospeda la aplicación de procesamiento de transacciones de tarjetas de crédito. Se aplican los servicios de seguridad de firewall existentes implementados en el centro de datos de este ejemplo. Por otro lado, las políticas del sistema HVAC segmentan y dirigen el tráfico de HVAC al servicio de seguridad en la nube para una inspección de seguridad adicional antes de llegar al centro de control de la IoT alojado en la nube pública. Dado que el tráfico de la IoT se aísla de acuerdo con la política empresarial, una infracción en el segmento de HVAC no compromete ni pone en riesgo los datos de las tarjetas de crédito y personales en el segmento de PoS. La segmentación también ayuda a las organizaciones a cumplir con las exigencias de conformidad de PCI (u otro) para su negocio. Como se muestra en este ejemplo, una implementación de seguridad integral con una plataforma SD-WAN avanzada puede salvaguardar mejor a las empresas dinámicas de hoy en día en su camino hacia la transformación a medida que adoptan los beneficios de la IoT.

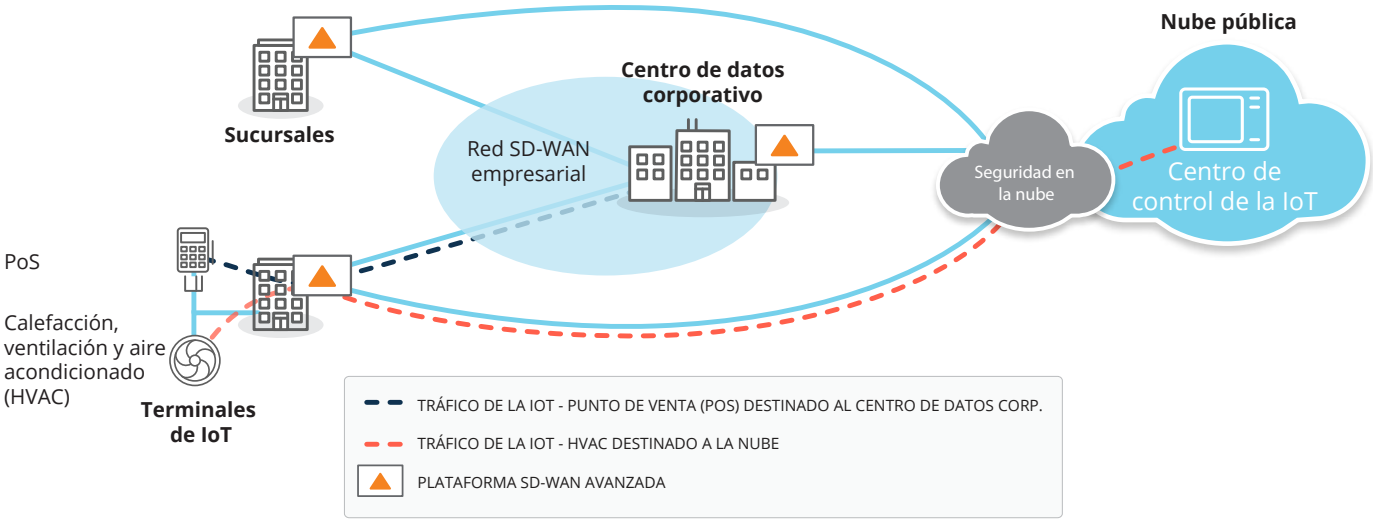

Figura 4: Los extremos de la IoT se multiplican y plantean nuevos riesgos de violación de seguridad. Con una plataforma SD-WAN avanzada, las empresas pueden proteger los dispositivos de la IoT si implementan una arquitectura Zero Trust y segmentan la red dinámicamente. Como se muestra en el diagrama, todos los datos de transacciones de PoS de la sucursal se destinan al centro de datos de la empresa, mientras que el tráfico de HVAC se dirige a un centro de control de la IoT en la nube.

PROTEGER LAS SUCURSALES DE AMENAZAS EXTERNAS CON UNA SD-WAN AVANZADA

Con la digitalización de las empresas, el riesgo de ciberataques aumentó considerablemente en la última década. En los entornos de red tradicionales basados en enrutadores, las sucursales han apilado una multitud de equipos de red y seguridad, pero estos equipos son difíciles de configurar, mantener y actualizar con la información más reciente sobre amenazas. Los sitios remotos también carecen de personal de TI experimentado, lo que las expone a posibles infracciones de seguridad.

Además de proteger las operaciones en la nube con la mejor SASE de su clase, una solución SD-WAN avanzada protege a las sucursales de amenazas maliciosas. Está construida con un firewall de próxima generación que incluye funciones de defensa contra amenazas, como detección y prevención de intrusiones (IDS/IPS) y DDoS, para proteger las sucursales de amenazas maliciosas.

Un sistema IDS basado en firmas suele supervisar el tráfico de la red para encontrar patrones que coincidan con una firma de ataque concreta. Cuando se detecta una intrusión, el sensor proporciona acciones tales como abandonar, inspeccionar y permitir el tráfico. Los sistemas de prevención de intrusiones pueden funcionar en modo estricto o de alto rendimiento. En el modo estricto, el tráfico pasa a través del sensor de modo que se bloquee inmediatamente cuando se produce una intrusión. En el modo de alto rendimiento, se envía una copia del tráfico para su análisis, lo que proporciona más eficacia sin afectar al rendimiento de la red. Una vez detectada, la intrusión se bloquea. En función de sus requisitos de seguridad, las organizaciones pueden elegir entre el modo estricto o el de alto rendimiento.

Una SD-WAN avanzada también puede detectar dinámicamente los ataques DDoS, como los ataques de protocolo, las inundaciones ICMP, las inundaciones SYN y los ataques de spoofing de IP. Tras detectar un comportamiento anormal de la red, la solución limita el número de solicitudes mediante acciones como el vencimiento rápido, el corte de exceso y el bloqueo de la fuente. Además, puede enrutar el tráfico a través de enlaces de red no afectados en caso de un ataque DDoS, lo que asegura la continuidad de los negocios.

Al integrar las capacidades avanzadas de red y seguridad en una única solución SD-WAN, como el enrutamiento, la optimización de la WAN y el firewall de próxima generación, las organizaciones pueden simplificar mucho sus operaciones de red en las sucursales. Además, las políticas de seguridad pueden enviarse automáticamente a las sucursales desde una ubicación central con Zero Touch Provisioning, que facilita la configuración de las políticas de red y seguridad. Las nuevas sucursales se configuran de forma rápida y sencilla, y los cambios en las políticas de seguridad pueden distribuirse automáticamente a cientos o miles de sucursales en minutos, y así minimizar los errores.

LA TRANSFORMACIÓN DE LA WAN ES FUNDAMENTAL PARA EL ÉXITO DE LA TRANSFORMACIÓN DIGITAL

Además de todas las ventajas de migrar a una arquitectura moderna de seguridad en la nube, la transformación de la WAN para las empresas actuales con un enfoque cloud-first es sumamente valiosa. Las WAN tradicionales centradas en los enrutadores nunca se diseñaron para la nube. Las empresas deben modernizar su arquitectura WAN y replantearse cuál es la mejor manera de diseñar las redes de sus sucursales para mejorar el rendimiento y la seguridad de las aplicaciones en la nube. Las empresas están usando cada vez más la nube y el SaaS, y centrándose en ofrecer una experiencia de máxima calidad a los usuarios.

La transformación de la WAN consiste en proporcionar una ruta más eficiente y una mejor experiencia entre los usuarios y la nube. Como se describió anteriormente, la adopción de la desconexión adaptativa de Internet para las aplicaciones alojadas en la nube y el SaaS directamente desde las sucursales no solo optimiza el ancho de banda disponible, sino que también reduce cualquier latencia que pueda afectar la productividad del usuario.

Muchas organizaciones están transformando el borde de su red y adoptando la SD-WAN para conectar las sucursales mediante conexiones de Internet de banda ancha. La SD-WAN proporciona una selección inteligente de rutas impulsada por las aplicaciones a través de varios enlaces WAN (MPLS, Internet de banda ancha, LTE, etc.) basada en políticas definidas de forma centralizada. Algunos de los beneficios de la SD-WAN incluyen:

- Proporcionar las aplicaciones empresariales de forma rentable
- Mejorar el rendimiento de las aplicaciones, la disponibilidad y la calidad de la experiencia del usuario final
- Satisfacer los requisitos de las modernas sucursales o ubicaciones remotas
- Adaptar aplicaciones y servicios basados en SaaS y en la nube
- Mejorar la eficiencia de TI de las sucursales mediante el suministro automatizado de servicios

SATISFACER LAS EXIGENCIAS DE LOS SLA DE APLICACIONES

Esto se traduce directamente en una mayor productividad de la empresa y agilidad empresarial. Las empresas necesitan una red de alto rendimiento construida sobre una base de alta disponibilidad que pueda admitir las aplicaciones críticas para los negocios de forma fiable. La seguridad nunca debe dejarse en segundo plano. La capacidad de admitir funciones de microsegmentación y la aplicación de políticas granulares brinda a las empresas la capacidad de proteger la WAN, cumplir los requisitos de cumplimiento y defenderse de violaciones.

Las empresas necesitan agilidad para crear nuevas sucursales y ajustar dinámicamente las políticas y reglas de seguridad. La capacidad de propagar el contexto de las políticas es un requisito fundamental para la automatización de las sucursales. Esto hace que el concepto de una solución SD-WAN avanzada sea muy atractivo y ayude a las empresas a eliminar la necesidad de varios dispositivos que realicen funciones de seguridad dedicadas y, a su vez, simplificar y consolidar, o "afinar", la arquitectura de borde WAN de las sucursales. Una avanzada plataforma de borde SD-WAN permite a las empresas transformar su WAN unificando la SD-WAN, el enrutamiento, la optimización de la WAN, la segmentación y la seguridad de las sucursales en una única plataforma gestionada de forma centralizada.

La orquestación centralizada de la SD-WAN y un enfoque específico de la aplicación garantizan que las prioridades de la empresa se reflejen siempre en el comportamiento de la red. La unificación de las políticas de orquestación de la red y la seguridad también garantiza que la calidad del servicio y la seguridad se apliquen y se hagan cumplir de manera uniforme en todas las aplicaciones (o clases de aplicaciones), independientemente de la manera en que se accede a ellas o del lugar desde donde se accede a ellas. Permite que el rendimiento y la seguridad de las aplicaciones se establezcan mediante políticas empresariales de arriba hacia abajo, en vez de definirse de abajo hacia arriba según los límites tecnológicos. Una SD-WAN avanzada supervisa continuamente el estado de la red y las aplicaciones, detecta las condiciones cambiantes y activa respuestas inmediatas y automatizadas en tiempo real para eliminar el impacto de los cortes de tensión, los apagones y los eventos de amenazas a la seguridad. Además, la automatización de la conectividad de la plataforma en la nube con integraciones a través de interfaces programables de aplicaciones (API) simplifica las operaciones de TI, proporciona a las empresas acceso oportuno a los servicios de seguridad en la nube, IaaS y SaaS. La red actual requiere visibilidad de seguridad integral, programabilidad y automatización para garantizar dinámicamente el rendimiento, la seguridad y la máxima calidad de la experiencia necesaria para los entornos de varios nubes. Una WAN inteligente diseñada con las mejores soluciones de seguridad SD-WAN de su clase y en la nube avanza en las iniciativas de transformación digital. Además, permite a las empresas evolucionar y adoptar innovaciones oportunamente sin limitar su productividad y crecimiento, todo ello minimizando la exposición a los riesgos de seguridad.

CONCLUSIÓN

A medida que las empresas modernas con un enfoque cloud-first siguen migrando aplicaciones del centro de datos a la nube, deben adoptar la transformación de la WAN y la seguridad para obtener el máximo rendimiento de sus inversiones en la nube. SASE o Secure Access Service Edge lleva a la industria hacia esta dirección. Como se muestra en la Figura 5, es importante que las empresas tengan en cuenta tanto la transformación de la WAN como la de la seguridad a la hora de diseñar un borde de servicio de acceso seguro que permita una experiencia perfecta.

Una plataforma SD-WAN avanzada proporciona la capacidad de conectarse sin inconvenientes a una variedad de servicios de seguridad en la nube de los mejores de su clase y ofrece la mejor arquitectura SASE de su clase. En última instancia, ningún proveedor de SASE tendrá la capacidad de ofrecer realmente las mejores tecnologías de red y seguridad de su clase en una sola plataforma. Ante la continua evolución de las amenazas, las empresas deben conservar la agilidad necesaria para adoptar nuevas soluciones de seguridad rápidamente y de forma rentable. Las empresas cuentan con servicios para evaluar las plataformas que ofrecen la libertad de elección para integrar la mejor SASE de su clase. Al hacerlo, las empresas evitan estar obligadas a adquirir soluciones de propiedad de un único proveedor ni tendrán que conformarse con funciones y capacidades básicas.

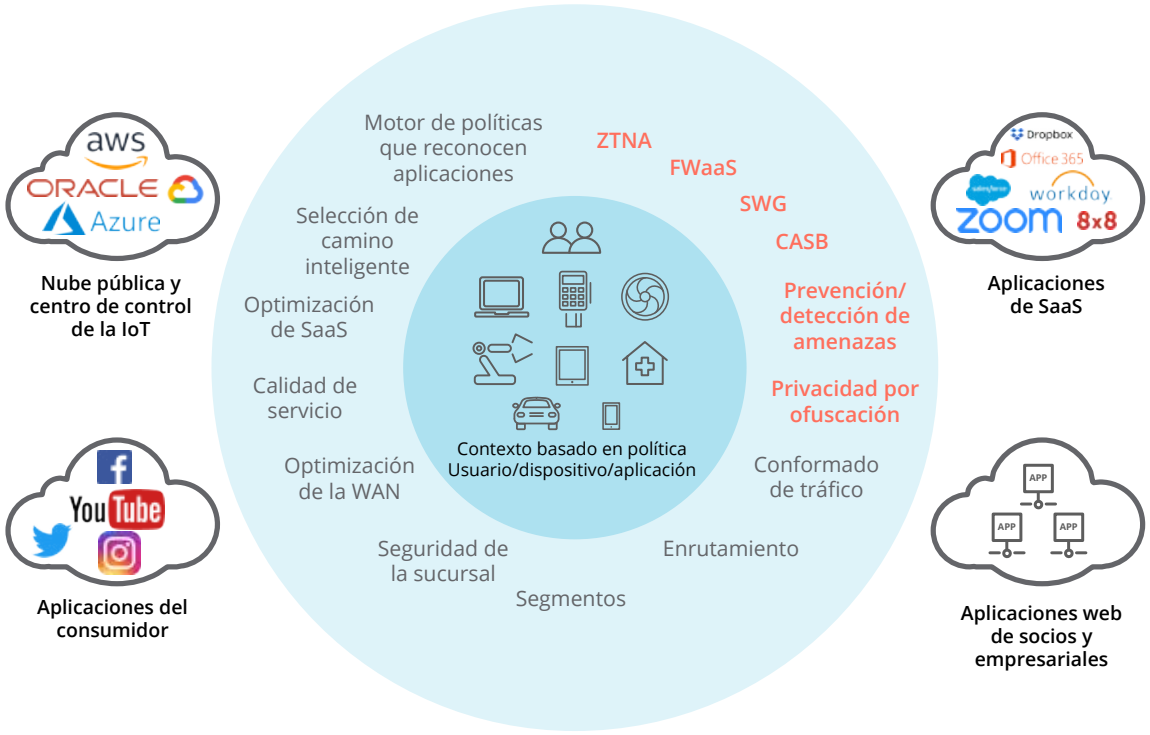

Figura 5: Se necesita un servicio de acceso seguro para admitir las iniciativas de transformación digital de la empresa, es decir, la estrategia de "enfoque cloud-first" y las necesidades de movilidad de los trabajadores. En una arquitectura SASE robusta, las capacidades integrales de la WAN deben trabajar en conjunto con las funciones integrales de seguridad de la red para satisfacer las necesidades de acceso dinámico y seguro de las empresas digitales para los usuarios, dispositivos y aplicaciones.

Además, con la proliferación de dispositivos de la IoT, la SASE debe complementarse con un marco de seguridad Zero Trust que segmente dinámicamente el tráfico en función de la identidad, de modo que los usuarios y los dispositivos de la IoT solo puedan llegar a los destinos de la red en consonancia con su función en la empresa.

Una SD-WAN avanzada puede admitir las funciones de seguridad fundamentales necesarias en la sucursal integrando un firewall de próxima generación con capacidades IDS/IPS y complementar la seguridad en la nube para ofrecer una aplicación de políticas de seguridad integral sin inconvenientes en toda la empresa. Esto permite a las empresas simplificar su infraestructura de red con la oportunidad de hacer la transición a una arquitectura WAN moderna y segura con un enfoque cloud-first a su propio ritmo y sin concesiones.

Por último, para las empresas que no estén preparadas para retirar los firewalls de las sucursales y pasar por completo a un modelo de seguridad en la nube, es importante encontrar una plataforma SD-WAN avanzada que ofrezca libertad de elección para admitir las principales soluciones de software de administración de amenazas unificada (UTM) de terceros que se ejecuten como una solución integrada en las sucursales. Esto elimina el costo adicional y la complejidad de la administración que normalmente se produciría con firewalls dedicados por separado, pero también proporciona a las empresas la flexibilidad para implementar las mejores soluciones, ofreciendo en última instancia una migración sin inconvenientes a un modelo de seguridad en la nube.

A medida que las empresas siguen realizando importantes inversiones en la nube, el hecho de considerar los requisitos para la transformación de la WAN y la seguridad acabará por situarlas camino a ofrecer una experiencia de máxima calidad a los usuarios, a la vez que se enfrentan a los desafíos actuales de ciberseguridad. Embarcarse en un camino de transformación de la WAN y la seguridad bien delineado y sin concesiones permitirá a las empresas, en última instancia, proteger sus activos digitales y lograr un efecto multiplicador de sus inversiones en la nube, tanto existentes como en curso.

aruba
a Hewlett Packard Enterprise company

BP_Successful-WAN-and-Security-Transformation_RVK_080422 a00110932spl

Comunícate con nosotros en www.arubanetworks.com/contact.