DOCUMENTO INFORMATIVO

aruba
a Hewlett Packard Enterprise company

LA TRANSFORMACIÓN SATISFACTORIA DE LA WAN Y DE LA SEGURIDAD IMPULSA LA EMPRESA DIGITAL

TABLA DE CONTENIDO

RESUMEN

Las empresas siguen optando por la transformación digital en su intento por 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 parte fundamental de cualquier iniciativa de transformación digital exitosa. ¿Por qué? Actualmente, hay más aplicaciones ejecutándose 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, las empresas globales centradas en la nube deben garantizar que las aplicaciones están accesibles de forma directa y segura en cualquier momento y desde cualquier ubicación a través de un dispositivo. Han de garantizar asimismo que la red proporciona la experiencia de mejor calidad posible a empleados y clientes de manera coherente. Finalmente, el auge de los dispositivos móviles e IoT en la empresa ha incrementado drásticamente la superficie de ataque, lo que ha expuesto a las empresas a vulneraciones de seguridad que pueden poner en riesgo los datos y aumentar el tiempo de inactividad en la red.

Las redes corporativas de hoy en día no se diseñaron para el mundo centrado en la nube y no están preparadas para proporcionar la agilidad y la seguridad necesarias para cumplir los requisitos de la transformación digital. Es esencial que las empresas protejan, además de las aplicaciones de la nube, a los usuarios que se conectan con estas aplicaciones en la red de área extensa (WAN). Al mismo tiempo, el entorno empresarial competitivo actual exige a las empresas proporcionar una experiencia óptima a los clientes a través de una red capaz de mantener el rendimiento y la disponibilidad necesarios para mantener el negocio en funcionamiento.

Para hacer de la transformación digital prometida una realidad, las empresas deben transformar sus arquitecturas WAN y de seguridad, no basta con limitarse a una de ellas. Las empresas ya han realizado inversiones considerables en su cambio a la nube, por lo que el auténtico reto es hallar la forma de conseguir un efecto multiplicador de dichas inversiones. La respuesta es modernizar las arquitecturas WAN y de seguridad de la empresa. Por lo tanto, el imperativo estratégico es adoptar una red de área extensa definida por software (SD-WAN) más inteligente y altamente automatizada que pueda integrarse fácilmente con los servicios de seguridad proporcionados en la nube.

Dado que la transformación de la WAN y de la seguridad es un proceso, las empresas pueden comenzar por modernizar su arquitectura WAN o de seguridad sin dejar nunca de lado el valor real de sus inversiones en la nube, es decir, deben tener en cuenta los dos aspectos. Es igualmente importante evitar limitarse a un solo proveedor, por lo que deben escogerse partners de soluciones tecnológicas que ofrezcan flexibilidad y libertad de elección. Una vez transformadas las arquitecturas WAN y de seguridad, las empresas podrán adoptar nuevas y prácticas innovaciones para acelerar la productividad, el crecimiento de los ingresos y la rentabilidad, sin dejar que se disparen los costes.

Para hacer de la transformación digital y de la nube prometida una realidad, las empresas deben transformar sus arquitecturas WAN y de seguridad, no basta con limitarse a una de ellas. Las empresas ya han realizado inversiones considerables en su cambio a la nube, por lo que el auténtico reto es hallar la forma de conseguir un efecto multiplicador de dichas inversiones.

SI LAS APLICACIONES SE ENTREGAN EN LA NUBE, LA SEGURIDAD TAMBIÉN DEBERÍA

Tradicionalmente, todo el tráfico de las aplicaciones de las sucursales se retornaba a través de servicios MPLS privados al centro de datos corporativo para llevar a cabo las tareas de inspección y verificación de seguridad pertinentes (véase la figura 1). Esta arquitectura tenía sentido siempre que las aplicaciones estuvieran alojadas exclusivamente en el centro de datos corporativo. Sin embargo, con la migración de las aplicaciones y los servicios a la nube, esta arquitectura de red tradicional se ha quedado pequeña, principalmente porque afecta al rendimiento de la aplicación y proporciona una experiencia de usuario incoherente. Esto se debe a que el tráfico destinado a Internet pasa por el centro de datos y el cortafuegos corporativo antes de llegar a su destino.

Además, ante el creciente número de empleados que trabajan fuera de la red corporativa y que 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. Mediante la transformación de sus arquitecturas WAN y de seguridad, las empresas pueden garantizar el acceso seguro a las aplicaciones y a los servicios en entornos de varias nubes, independientemente de la ubicación o de los dispositivos que se utilicen para acceder a ellos.

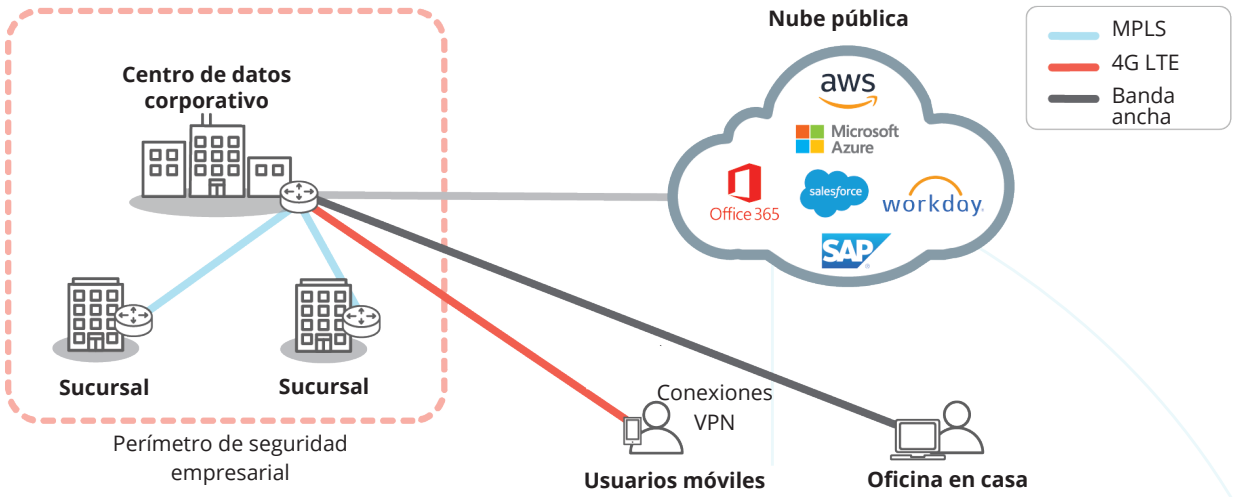

Figura 1: Las WAN empresariales tradicionales y los enfoques de seguridad basados en el perímetro no se diseñaron para la nube. El retorno del tráfico de las aplicaciones de las sucursales al centro de datos afecta al rendimiento y produce una experiencia de usuario incoherente.

Una solución de seguridad proporcionada en la nube admite diversas funciones de seguridad de la red, entre las que pueden incluirse una gateway web segura (SWG), un cortafuegos como servicio (FWaaS), un agente de seguridad de acceso a la nube (CASB) y una arquitectura de red de confianza cero (ZTNA). Anteriormente, cada una de estas funciones eran funciones dedicadas locales exclusivas, pero ahora se pueden suministrar desde la nube de manera unificada tal como se muestra en la figura 2.

Algunas de las primeras empresas en adoptar las soluciones de seguridad proporcionadas en la nube implementaron erróneamente una SD-WAN que no permitía el redireccionamiento a Internet adaptable directamente desde las sucursales. Esto les impidió enviar el tráfico directamente desde la sucursal a la nube. Sin el componente SD-WAN, el tráfico destinado a la nube seguía retornándose al centro de datos, lo que afectaba negativamente al rendimiento de las aplicaciones.

La adopción de una solución de seguridad proporcionada en la nube y de una arquitectura SD-WAN elimina el coste y la complejidad asociados a la administración de varios cortafuegos de próxima generación in situ, pero sigue requiriendo un cortafuegos basado en zonas de datos, en las sucursales para bloquear cualquier amenaza entrante. Como se muestra en la figura 3, el uso de una solución SD-WAN avanzada permite a las empresas conectarse directamente a la nube mediante el redireccionamiento a Internet adaptable a través de conexiones a Internet de banda ancha. La capacidad de reconocer las aplicaciones permitidas hace posible el redireccionamiento local desde la sucursal al punto de presencia (PoP) más cercano, lo que resuelve los problemas de latencia y permite ofrecer una experiencia de calidad óptima para aplicaciones de SaaS y en la nube, como Microsoft Office 365, 8x8 y RingCentral. El reconocimiento de aplicaciones también proporciona la capacidad de enviar otro tráfico de Internet a un proveedor

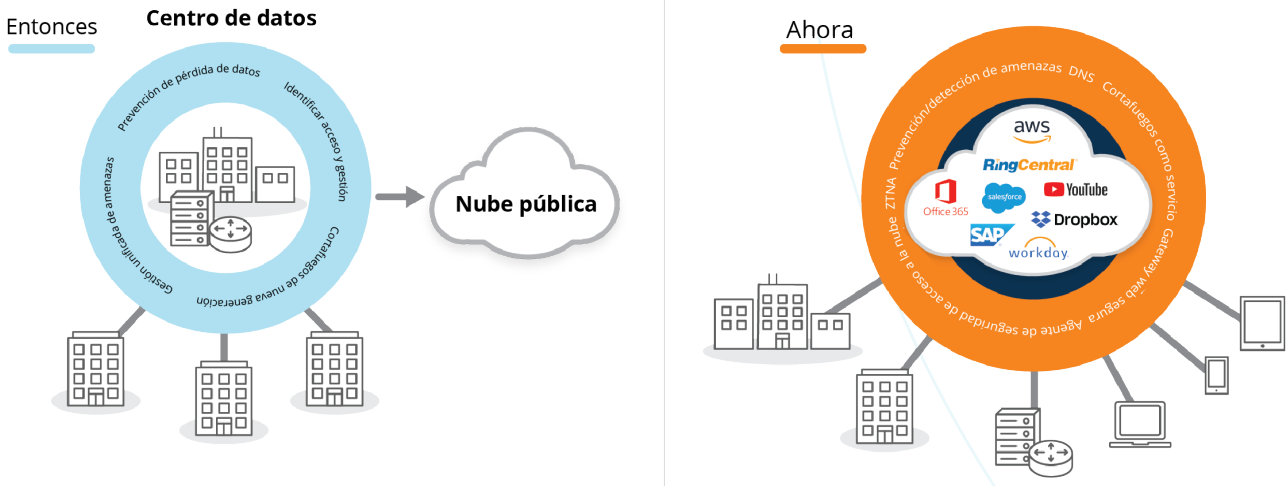

Figura 2: Antiguamente, todo radicaba en proteger el centro de datos empresarial en el que se alojaban exclusivamente las aplicaciones. Ahora que las aplicaciones se han movido a la nube, y se suministran desde esta, la seguridad empresarial basada en el perímetro es cada vez más inefectiva. Es indispensable cambiar la mentalidad y trasladar la seguridad a la nube.

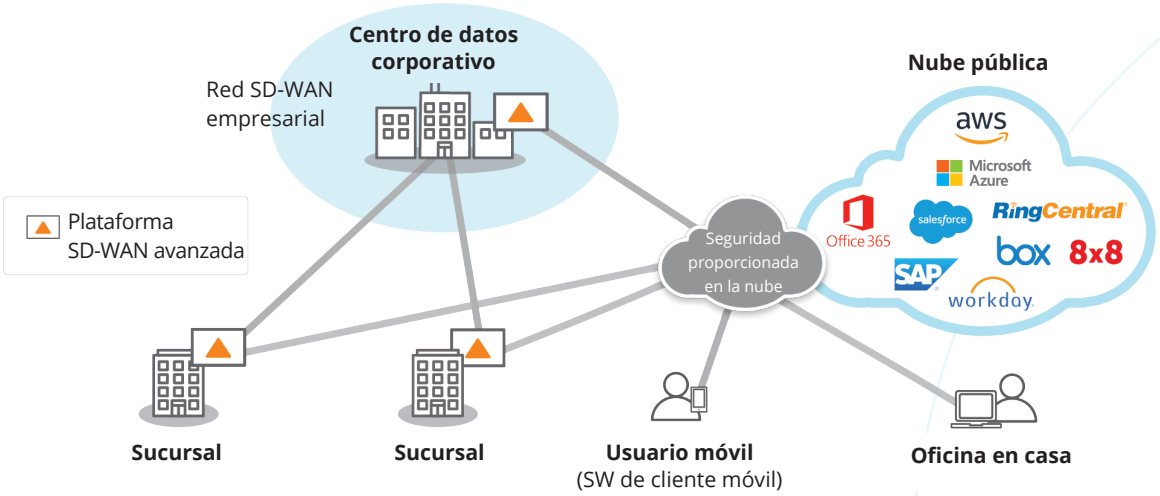

Figura 3: Una SD-WAN avanzada proporciona a las empresas un camino seguro a la nube. Las sucursales pueden utilizar conexiones de banda ancha y capacidades de redireccionamiento a Internet adaptable para conectar directamente a los usuarios con las aplicaciones de la nube, y optimizar así el rendimiento de las aplicaciones y la experiencia de usuario. La combinación de una SD-WAN avanzada y seguridad en la nube mediante un enfoque de red de confianza cero (ZTNA) basado en directivas garantiza que la WAN, los usuarios, los dispositivos y las aplicaciones de la empresa permanezcan siempre seguros.

de seguridad proporcionado en la nube para su inspección avanzada antes de enviarlo a un proveedor de SaaS. Las capacidades de SD-WAN avanzadas integradas en los servicios de seguridad proporcionados en la nube garantizan el cumplimiento coherente de las directivas y el control de acceso para usuarios, dispositivos, aplicaciones e IoT. De este modo, las empresas pueden forzar el cumplimiento, evitar el tiempo de inactividad y mitigar el riesgo de comprometer los datos asociado a posibles vulneraciones de la seguridad.

PROTECCIÓN DEL IOT EMPRESARIAL CON SD-WAN

La proliferación de dispositivos IoT en las empresas ha dado lugar a nuevas formas de supervisar, notificar, alertar, automatizar y optimizar los procesos empresariales, desde las líneas de fabricación a la automatización de sistemas climatización (HVAC) e iluminación para permitir el ahorro energético. La automatización permite al IoT mejorar la eficiencia de las empresas, sin embargo, también aumenta la superficie de ataque al añadir una nueva dimensión de complejidad. Los profesionales de TI afrontan el nuevo y creciente desafío de seguridad asociado a los dispositivos móviles mediante la implementación de una solución de acceso a la red de confianza cero (ZTNA) basada en un modelo de este tipo. Una solución ZTNA funciona mediante la instalación de un agente de punto de conexión en un dispositivo de usuario, como puede ser un portátil, una tableta o un teléfono móvil. Ese agente de software se asegura de que el tráfico del dispositivo se dirija a un servicio de seguridad proporcionado en la nube antes de enviarlo a una aplicación de SaaS o a un proveedor de IaaS. No obstante, a diferencia de las tabletas y los smartphones, los agentes de software ZTNA no se pueden instalar en dispositivos IoT al no contar con un agente, dado que no admiten la instalación de agentes de software de terceros. Por este motivo, las empresas requieren una solución de seguridad distinta para que los dispositivos IoT puedan proteger las redes corporativas de posibles vulnerabilidades que podrían poner en riesgo la seguridad de la red e interrumpir las operaciones comerciales rutinarias.

Una plataforma SD-WAN avanzada para la detección de aplicaciones puede ayudar a las empresas a reducir el riesgo asociado a las vulneraciones de seguridad durante la implementación de dispositivos IoT. Las plataformas SD-WAN avanzadas identifican y clasifican el tráfico de aplicaciones en el primer paquete, lo interceptan en el perímetro de la red y lo dirigen a un segmento apropiado, y lo protegen del tráfico restante de la red. Estas plataformas organizan la segmentación integral del tráfico LAN-WAN-LAN de la empresa y del tráfico LAN-WAN-centro de datos/nube, lo que permite el cumplimiento coherente y automatizado de las directivas de seguridad al disponer de mayor visibilidad. Con la segmentación integral, las empresas pueden crear segmentos aislados para el tráfico de dispositivos IoT. Es posible definir una directiva de seguridad independiente para cada segmento que defina las directivas de seguridad que han de aplicarse para el tráfico del dispositivo. Dado que el tráfico de un segmento está aislado del tráfico de los segmentos restantes, es posible evitar cualquier acceso no autorizado. Incluso si se produjese alguna amenaza, su impacto estaría limitado al segmento en el que esta hubiera surgido. Además, con un cortafuegos unificado basado en zonas de datos, las empresas pueden proteger sitios remotos y dispositivos IoT de cualquier posible amenaza que pudiera bloquear el tráfico.

Veamos un ejemplo. En un sitio remoto en el que se hayan instalado dispositivos IoT sin agente, como sistemas de puntos de venta y HVAC (véase la figura 4 más abajo), una plataforma SD-WAN avanzada puede identificar las aplicaciones utilizadas exclusivamente por estos dispositivos. Una directiva del sistema intercepta el tráfico del punto de venta y lo dirige al centro de datos corporativo donde se aloja la aplicación que procesa las transacciones con

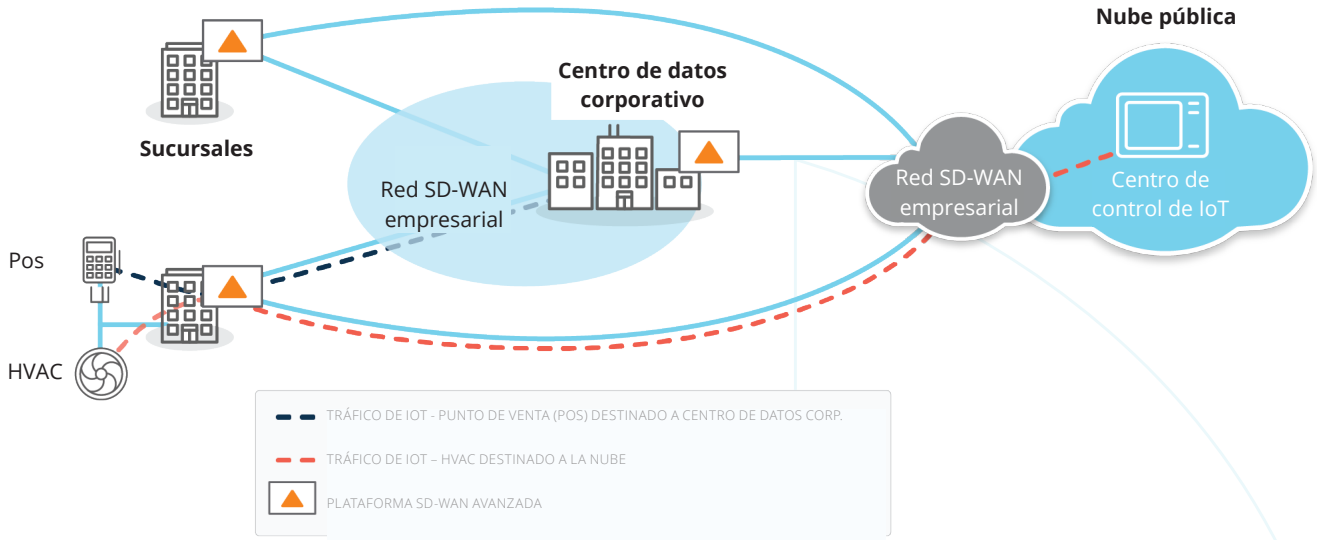

Figura 4: Los puntos de conexión de IoT se están multiplicando, lo que plantea nuevos riesgos de vulneración de la seguridad. Mediante el uso de una plataforma SD-WAN avanzada, las empresas pueden proteger los dispositivos IoT que se encuentran detrás del cortafuegos unificado basado en zonas con datos, identificar de forma dinámica el tráfico de dispositivos IoT y segmentar la red minuciosamente para satisfacer los requisitos de cumplimiento. Una SD-WAN avanzada garantiza que se intercepte el tráfico de IoT en el perímetro de la red y se envíe al destino correcto, incluida la nube, sin poner en riesgo ni comprometer la exposición del negocio. Como se muestra en el diagrama, todos los datos de transacciones del punto de venta de la sucursal se dirigen al centro de datos de la empresa, mientras que el tráfico del sistema HVAC se dirige a un centro de control de IoT en la nube.

tarjeta de crédito. En este ejemplo se aplican los servicios de seguridad de cortafuegos de próxima generación implementados en el centro de datos. Por otro lado, las directivas del sistema HVAC segmentan y dirigen el tráfico de este sistema al servicio de seguridad proporcionado en la nube para su inspección de seguridad adicional antes de enviarlo al centro de datos de IoT alojado en la nube pública. Ya que el tráfico de IoT se aísla de acuerdo con las directivas de la empresa, una vulneración en el segmento del sistema HVAC no pondría en riesgo los datos personales ni de las tarjetas de crédito en el segmento del punto de venta. La segmentación también ayuda a las organizaciones a cumplir las directivas de interconexión de componentes periféricos (PCI) de la empresa. Tal como se muestra en este ejemplo, una implementación de seguridad integral con una plataforma SD-WAN avanzada puede proteger mejor a las empresas dinámicas de hoy en día en su proceso de transformación y permitirles disfrutar a la vez de las ventajas del IoT.

LAS MEJORES SOLUCIONES OFRECEN MAYOR AGILIDAD EMPRESARIAL

Los enfoques para suministrar seguridad en red en constante evolución y la dificultad que entraña la creación de soluciones de red tan complejas confieren especial importancia a evaluar las mejores soluciones de red y de seguridad que ofrecen los proveedores con experiencia y conocimientos probados. No es factible encontrar un solo proveedor capaz de ofrecer las mejores capacidades en ambos dominios y las empresas no tendrían que verse forzadas a elegir entre unas u otras capacidades básicas.

En un panorama repleto de amenazas en constante cambio en el que la seguridad es primordial, las empresas deben ser lo suficientemente ágiles para adoptar de forma rápida y rentable nuevas soluciones de seguridad sin tener que limitarse a un único proveedor de seguridad. Con una solución de red independiente, las empresas tendrán la garantía y la tranquilidad de poder seleccionar e implementar las soluciones de seguridad en la nube que mejor respondan a los cambiantes requisitos comerciales y de seguridad.

La libertad de elegir entre las mejores soluciones del mercado que unifiquen SD-WAN y seguridad en la nube mediante capacidades de automatización, permitirá a las empresas obtener mayor agilidad y velocidad, y reducir la complejidad y los costes mediante la creación de una arquitectura de seguridad coherente capaz de evitar el impacto de los ciberataques. En definitiva, esto permitirá a las empresas lograr un efecto multiplicador de sus inversiones existentes y futuras en aplicaciones y servicios en la nube.

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

Además de todas las ventajas que supone la migración a una arquitectura de seguridad en la nube moderna, el potencial de la transformación de la WAN para las empresas centradas en la nube de hoy en día es enorme. Las WAN basadas en routers tradicionales no se diseñaron para la nube. Las empresas deben modernizar su arquitectura WAN y volver a estudiar la mejor forma de construir las redes de sus sucursales para optimizar el rendimiento y la seguridad de las aplicaciones en la nube. Las empresas utilizan cada vez más la nube y las aplicaciones de SaaS con el objetivo de proporcionar a sus usuarios la mejor experiencia posible.

El propósito de la transformación de la WAN es proporcionar una ruta más eficiente a los usuarios y mejorar la experiencia entre estos y la nube. Como hemos descrito anteriormente,

la adopción de soluciones de redireccionamiento a Internet adaptable para aplicaciones alojadas en la nube y de SaaS directamente desde las sucursales, no solo permite optimizar el ancho de banda disponible, sino que también reduce la latencia responsable de mermar la productividad de los usuarios.

Muchas organizaciones están transformando su perímetro de red y adoptando SD-WAN para conectar sus sucursales a través de conexiones a Internet de banda ancha. SD-WAN proporciona una selección de ruta inteligente para aplicaciones en diversos enlaces WAN (MPLS, Internet de banda ancha, LTE, etc.) basados en directivas definidas centralmente. Una SD-WAN puede ofrecer las siguientes ventajas:

- Proporcionar una solución rentable de acceso a las aplicaciones empresariales
- Mejorar el rendimiento y la disponibilidad de las aplicaciones, y la calidad de la experiencia del usuario final
- Satisfacer los requisitos de las sucursales/sitios o ubicaciones remotos
- Admitir aplicaciones y servicios de SaaS y basados en la nube
- Mejorar la eficiencia de TI mediante el aprovisionamiento de servicios automatizados

CUMPLIMIENTO DE LA DEMANDA DE SLA DE APLICACIONES

Esto repercute directamente en una mayor productividad y agilidad empresariales. Las empresas necesitan una red de alto rendimiento construida sobre la base de una alta disponibilidad capaz de gestionar las aplicaciones críticas para la empresa de forma fiable. La seguridad no debe ser algo secundario. La posibilidad de admitir funciones de microsegmentación y el cumplimiento exhaustivo de las directivas habilitan a las empresas para proteger sus WAN, satisfacer los requisitos de cumplimiento y protegerse frente a posibles vulneraciones.

Las empresas requieren asimismo agilidad para acelerar la implementación de nuevas sucursales y ajustar de forma dinámica las reglas de directivas y de seguridad. La capacidad de propagar el contexto de las directivas es un requisito esencial para la automatización de las sucursales. Esto hace que el concepto de una solución SD-WAN avanzada resulte muy atractivo y puede ayudar a las empresas a eliminar la necesidad de contar con varios dispositivos dedicados específicamente a funciones de seguridad y, a su vez, simplifica y consolida la arquitectura Edge WAN de sus sucursales. Una plataforma Edge SD-WAN avanzada permite a las empresas transformar su WAN unificando SD-WAN, enrutamiento, optimización de WAN, segmentación y seguridad de las sucursales en una plataforma gestionada centralmente.

La orquestación de SD-WAN centralizada y un enfoque orientado específicamente a las aplicaciones garantizan que las prioridades de la empresa se vean siempre reflejadas en el comportamiento de la red. La unificación de la orquestación de la red y las directivas de seguridad garantiza la aplicación de una calidad del servicio y un cumplimiento de las directivas de seguridad coherentes para las aplicaciones, o clases de aplicaciones, independientemente de cómo se acceda a ellas o el lugar desde el que se acceda. El rendimiento y la seguridad de las aplicaciones están determinados por directivas empresariales de carácter descendente, en lugar de por limitaciones tecnológicas de carácter ascendente.

Una SD-WAN avanzada supervisa constantemente el estado de la red y las aplicaciones, detecta las condiciones cambiantes y desencadena respuestas inmediatas automatizadas en tiempo real para evitar el impacto de posibles caídas de tensión, cortes de electricidad y amenazas de seguridad. Además, la automatización de la conectividad de las plataformas en la nube con integraciones a través de interfaces de programación de aplicaciones (API) simplifica las operaciones de TI y proporciona a las empresas un acceso puntual a los servicios de seguridad, los entornos de IaaS y las aplicaciones de SaaS proporcionados en la nube.

La red actual requiere una visibilidad integral, capacidad de programación y automatización para garantizar de forma dinámica el rendimiento, la seguridad y la experiencia de mayor calidad posible necesarias para los entornos de varias nubes. Una arquitectura WAN inteligente diseñada con una SD-WAN de la mejor calidad y soluciones de seguridad proporcionadas en la nube impulsa las iniciativas de transformación digital y favorece el desarrollo de las empresas mediante la adopción oportuna de innovaciones sin limitar su productividad ni su crecimiento, al tiempo que minimiza la exposición a los riesgos de seguridad.

CONCLUSIÓN

Durante el proceso de migración de las aplicaciones del centro de datos a la nube, las empresas deben hacer frente a la transformación de la WAN y de la seguridad si desean obtener la máxima rentabilidad de sus inversiones en la nube. Gartner acuñó el término SASE, o Edge de servicio de acceso seguro (del inglés, Secure Access Service Edge) en el que se ha basado el sector para tomar este rumbo. Como se muestra en la figura 5, es importante que las empresas consideren la transformación de la WAN y de la seguridad a la hora de crear un Edge de servicio de acceso seguro capaz de ofrecer una experiencia incomparable.

En resumen, ningún proveedor va a poder proporcionar realmente las mejores tecnologías de red y seguridad a través de una sola plataforma. En un panorama repleto de amenazas en constante evolución, las empresas deben ser lo suficientemente ágiles para adoptar de forma rápida y rentable nuevas soluciones de seguridad. Las empresas cuentan con los recursos necesarios para evaluar plataformas que ofrezcan libertad de elección para integrar las mejores soluciones de red y de seguridad disponibles. De este modo, no se verán limitadas a utilizar las soluciones desarrolladas por un solo proveedor ni tendrán que conformarse con funciones y capacidades básicas.

Una plataforma SD-WAN avanzada que admita interfaces de programación de aplicaciones (API) integradas puede ofrecer nuevos niveles de automatización a las empresas y

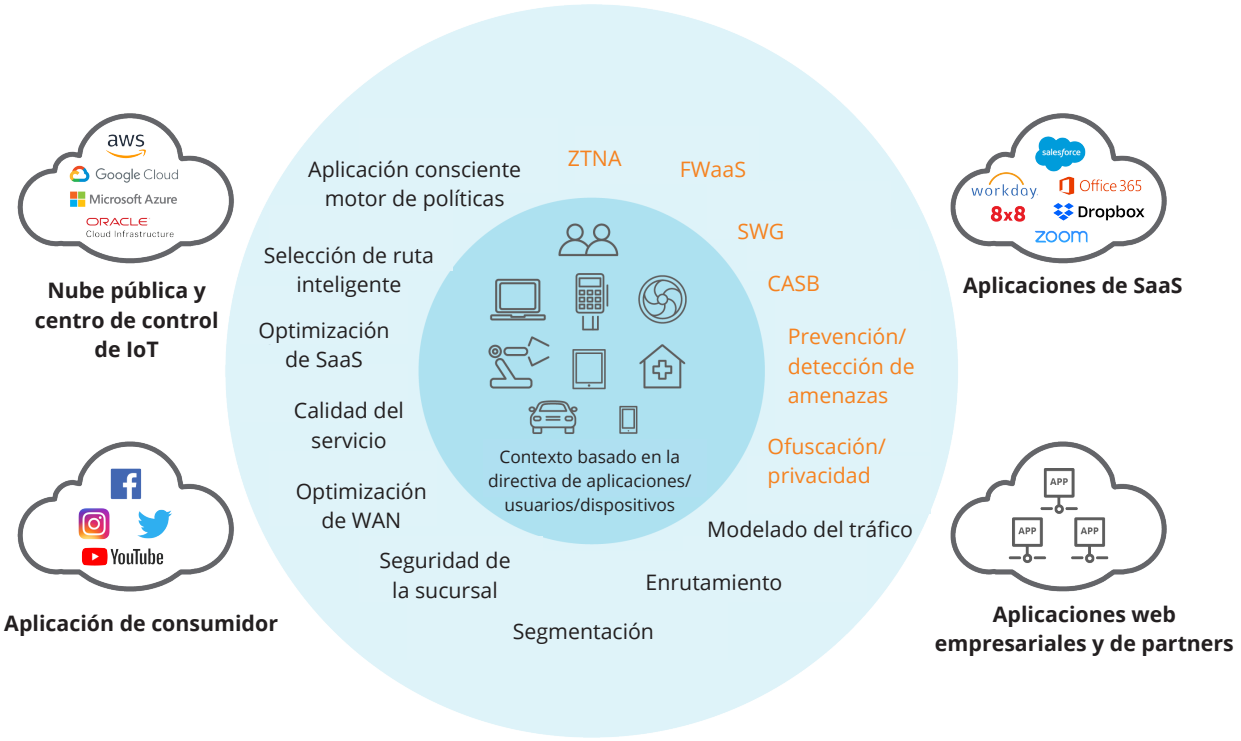

Figura 5: Se requiere un Edge de servicio de acceso seguro para afrontar las iniciativas de transformación digital de la empresa, es decir, la estrategia centrada en la nube y las necesidades de movilidad de la fuerza de trabajo. En una arquitectura SASE sólida, las capacidades WAN integrales deben combinarse con las funciones de seguridad de la red integrales para cubrir las necesidades de acceso seguro dinámico para los usuarios, los dispositivos y las aplicaciones de las empresas digitales.

proporcionarles así la capacidad de conectarse a diversos servicios en la nube de excelente calidad, incluidos los servicios de seguridad. Estas plataformas admiten las funciones de seguridad básicas necesarias en las sucursales y complementan la seguridad proporcionada en la nube para permitir el cumplimiento integral de las directivas de seguridad en toda la empresa. Esto proporciona a las empresas que todavía no están preparadas para transformar completamente sus arquitecturas WAN y de seguridad la oportunidad de evolucionar a una arquitectura WAN moderna centrada en la nube a su propio ritmo y sin riesgos.

Finalmente, para aquellas empresas que puedan no estar preparadas para retirar los cortafuegos de las sucursales y cambiar por completo a un modelo de seguridad proporcionado en la nube, es importante encontrar una plataforma SD-WAN avanzada que ofrezca libertad de elección para poder utilizar soluciones de gestión unificada de amenazas (UTM) de otros proveedores líderes como soluciones integradas en sus sucursales. Esto evita los costes adicionales y la complejidad de gestión generalmente asociados al uso de cortafuegos independientes, además de proporcionar a las empresas la flexibilidad de implementar las mejores soluciones existentes y, en última instancia, ofrecer una migración a un modelo de seguridad en la nube.

Mientras las empresas continúan realizando importantes inversiones en la nube, deben analizar los requisitos de transformación de la WAN y de la seguridad para obtener las herramientas necesarias para proporcionar la mejor experiencia posible a los usuarios y, en consecuencia, aumentar su productividad y hallar nuevas fuentes de ingresos. Por último, la adopción de un enfoque estudiado y sin riesgos para transformar su arquitectura WAN y de seguridad les permitirá lograr un efecto multiplicador de sus inversiones existentes y futuras en la nube.

aruba
a Hewlett Packard Enterprise company

WP_Successful-WAN-and-Security-Transformation_EM_021621 a00110932enw