aruba
a Hewlett Packard Enterprise company

LIBRO ELECTRÓNICO

Seguridad desde el borde a la nube: Una nueva WAN y borde de Seguridad

Guía práctica para implementar una arquitectura Edge de servicio de acceso seguro (SASE)

En un mundo que prioriza la nube, la transformación digital y la posibilidad de trabajar desde cualquier parte afectan a la WAN y a la seguridad.

A medida que las empresas hacen frente a los retos de la pandemia y la nueva normalidad de trabajar desde cualquier parte, la adopción de servicios en la nube es cada vez más rápida. Este cambio intensifica la urgencia de transformar el centro de datos convencional, así como las redes basadas en el MPLS y VPN en un Edge de servicio de acceso seguro (SASE) en la nube, que incluye un aprovisionamiento más dinámico de servicios de red seguros, al tiempo que protege los datos de extremo a extremo en toda la WAN.

Los tres aspectos más importantes que los directivos de TI deben abordar en materia de seguridad de la WAN son:

- ¿Cómo me aseguro de que escojo la arquitectura SD-WAN adecuada para soportar de forma segura las aplicaciones empresariales en un entorno que prioriza la nube?
- ¿Cómo afectará el entorno remoto híbrido permanente a las decisiones de TI para adaptar una arquitectura segura en una infraestructura de SASE?
- ¿Cómo el departamento de TI puede gestionar los retos de seguridad asociados a la proliferación de dispositivos IoT sin agente?

Analicemos cómo evolucionan los requisitos de la red y la seguridad en un mundo que prioriza la nube.

El **50 %**
de los encuestados en 2021 están en proceso de implementar y ejecutar distintas iniciativas de transformación digital o ya lo han hecho en comparación con el 38 % en 2020[1]

El **45 %**
de las empresas tienen una política que prioriza la nube[2]

1, 2. ESG IT Technology Spending Intentions Survey, diciembre de 2020

Zero Trust, ZTNA y SASE en un mundo que prioriza la nube

Las soluciones tradicionales de seguridad no se diseñaron para la nube. El concepto del tráfico de retorno a un centro de datos centralizado funcionaba cuando todas las aplicaciones se ubicaban allí. Sin embargo, debido al aumento del tráfico por parte de los usuarios de las sucursales y el paso de las aplicaciones a la nube, el tráfico de retorno en una red heredada de tipo «hub and spoke» ofrece una experiencia de usuario deficiente y supone un aumento de los riesgos de seguridad, además de ser costoso.

Las soluciones de seguridad de redes heredadas todavía no incorporan el concepto de Zero Trust, un modelo de seguridad de TI para la gestión de identidad y acceso. Funciona con la premisa de que no se confía en ninguna acción de usuario o de software hasta que sea autentificada. En otras palabras, autentificar todo y, después, restringir el acceso solo a las aplicaciones y los datos compatibles con el perfil del usuario o del dispositivo. Zero Trust requiere que los usuarios, los dispositivos y las aplicaciones demuestren su identidad, y que estén autorizados a acceder únicamente a los recursos que buscan, ya estén dentro o fuera de la red o del perímetro.

Zero Trust Network Access (ZTNA) es un conjunto de tecnologías que opera en un marco Zero Trust en el que se otorga, cuando es estrictamente necesario, el principio de mínimo privilegio que se define en las políticas detalladas. ZTNA ofrece a los usuarios conectividad segura y sin incidencias para las aplicaciones privadas sin tener que incluirlas en la red o exponerlas en Internet.

Finalmente, está SASE, un nuevo término acuñado por Gartner. Se entiende por SASE aquella arquitectura Edge que combina las capacidades de WAN integrales con funciones integradas de seguridad proporcionadas en la nube, tales como gateway web segura (SWG), agente de seguridad de acceso a la nube (CASB), cortafuegos como servicio (FWaaS) o ZTNA, entre otros.

Retos relativos a la seguridad de la red y a la WAN

En un mundo que prioriza la nube, las necesidades de seguridad de la red y la WAN son ahora más interdependientes que nunca. Para hacer de la transformación digital prometida una realidad, las empresas deben transformar sus arquitecturas WAN y de seguridad para poder gestionar las aplicaciones de empresa que se alojan y a las que se accede desde cualquier parte y en cualquier red de transporte.

Analicemos los retos de seguridad y de la WAN más importantes a los que se enfrentan los equipos de TI y redes de las empresas:

- ¿Cómo se puede sacar partido de las ventajas operativas y empresariales de la nube sin renunciar a un alto nivel de seguridad y reducir el riesgo general?
- ¿Cómo se puede asegurar una experiencia de usuario uniforme y de calidad para todas las aplicaciones de negocio en la nube en toda la WAN?
- ¿Cómo se pueden implementar y cumplir unas políticas de acceso a la red coherentes para empleados que trabajan en un régimen híbrido (parcialmente desde la oficina o sucursal) o que lo hacen desde cualquier ubicación?
- ¿Cómo se puede estar al día de la seguridad y la conectividad WAN de tantos dispositivos, usuarios y aplicaciones diferentes?
- ¿Puede una elección correcta de plataforma SD-WAN mejorar la integración de red y seguridad?
- ¿Se puede obtener todos los dispositivos de seguridad necesarios de un mismo proveedor?

Cómo abordar la integración de políticas de seguridad y aplicaciones de SD-WAN

En la actual economía globalizada y acelerada, las empresas necesitan la agilidad necesaria para crear rápidamente nuevas sucursales y ajustar las políticas y reglas de seguridad de forma dinámica. La propagación del contexto de las políticas es un requisito esencial para la automatización de las sucursales y una función clave que solo puede proporcionar una solución avanzada de SD-WAN, como la plataforma Edge SD-WAN Aruba EdgeConnect.

Con una solución avanzada de SD-WAN, es posible ayudar a las empresas a no tener que contar con múltiples dispositivos a través de la unificación de las principales funciones de Edge WAN de las sucursales, como:

- SD-WAN
- Enrutamiento
- Cortafuegos basado en zonas y segmentación
- Gestión unificada de amenazas (UTM)
- Visibilidad y control de aplicaciones y redes
- Optimización de WAN

Conseguir consolidar estas funciones simplificará el borde WAN de las sucursales. Gracias a la gestión centralizada, aumentará significativamente la eficacia del personal de TI y permitirá mejorar la calidad del servicio (QoS) y del cumplimiento de las políticas de seguridad.

La organización de SD-WAN centralizada de Aruba EdgeConnect unifica la configuración y la gestión continua. Asimismo, garantiza una aplicación y un cumplimiento coherentes de la calidad del servicio y la seguridad 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.

Cómo la SD-WAN ofrece una seguridad más coherente

La implementación de una arquitectura SASE que combina la seguridad proporcionada en la nube con una solución de SD-WAN más avanzada elimina el coste y la complejidad asociados a la administración de varios cortafuegos de última generación in situ, pero sigue requiriendo un cortafuegos «stateful» basado en zonas en las sucursales para bloquear cualquier amenaza entrante.

La plataforma EdgeConnect incluye lo siguiente:

- Inteligencia y reconocimiento de aplicaciones que reconocen las aplicaciones autorizadas y les permiten acceder a los recursos alojados en la nube directamente
- Integración y organización automatizadas con proveedores de seguridad en la nube desde la sucursal hasta el punto de presencia (PoP) de cumplimiento de seguridad más cercano

Estas son algunas de sus ventajas clave:

- Latencia reducida
- Optimización del rendimiento de las aplicaciones
- Soporte para una experiencia de máxima calidad para aplicaciones de SaaS

La integración de Aruba Threat Defense con la plataforma Edge SD-WAN Aruba EdgeConnect amplía las capacidades avanzadas de los sistemas de detección de intrusiones (IDS) y protección contra intrusiones (IPS) de la SD-WAN. Los dispositivos físicos y virtuales de EdgeConnect aprovechan la infraestructura frente a amenazas de Aruba y la información sobre amenazas de Aruba Central, que permiten a las empresas proporcionar una seguridad lateral este-oeste y proteger el tráfico de Internet local de las sucursales. Se pueden implantar de manera central, in situ o en la nube. El registro de amenazas proporciona análisis de seguridad y de red a Aruba Central, y ofrece capacidades UTM del Edge a la nube integrales.

Zero Trust: Seguridad del borde por perfil, contexto y aplicación

Debido al aumento de los dispositivos móviles, el personal remoto, las aplicaciones alojadas en la nube y dispositivos conectados al Internet de las cosas (IoT), las empresas se ven obligadas a aunar las políticas de seguridad y las políticas de red basadas en intenciones comerciales.

La integración del control de acceso basado en identidad de Aruba ClearPass Policy Manager con la plataforma SD-WAN Aruba EdgeConnect aumenta la inteligencia de la aplicación al incorporar datos sobre la identidad de los usuarios, los dispositivos, los perfiles y la posición de seguridad del Edge WAN seguro.

Esta nueva capa contextual habilita una segmentación más precisa de los tipos de dispositivos basándose en la función que tienen en la empresa sin la complejidad de gestionar miles de VLAN. Por ejemplo, se puede definir una política de segmentación de granularidad fina para evitar que las cámaras de seguridad accedan al procesamiento de transacciones de tarjetas de crédito o a los sistemas de gestión de HVAC. De la misma manera, pueden impedir que las cámaras de seguridad se comuniquen con otras cámaras, pero que sí lo hagan con el sistema de vigilancia de cabecera o los dispositivos de grabación. Esto ayuda al equipo de TI a gestionar el cumplimiento de la seguridad de las aplicaciones y las auditorías de seguridad. Genera también un registro de amenazas que puede exportarse a aplicaciones de información de seguridad y gestión de eventos (SIEM) de terceros.

El **57 %**
de los encuestados afirma que sus organizaciones han implementado o implementarán Zero Trust[3]

El **49 %**
de los encuestados opina que sus organizaciones han implementado o implementarán la arquitectura de seguridad SASE[4]

El **71 %**
de los encuestados seleccionaría el mejor proveedor en la materia para implementar tanto la seguridad proporcionada por la nube como la SD-WAN para una arquitectura SASE[5]

3, 4, 5. Ponemon Institute, The State of SD-WAN, SASE and Zero Trust Security Architectures, abril 2021

ClearPass: Seguridad del IoT con SD-WAN avanzado

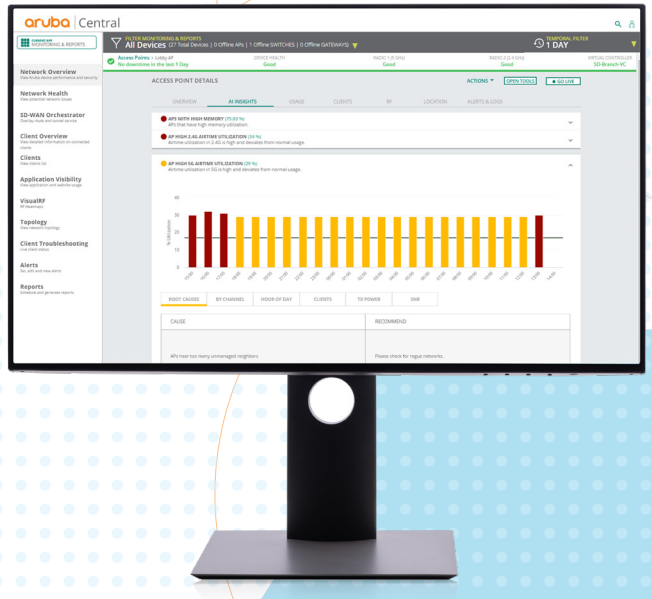
Cualquier dispositivo, como teléfonos móviles, portátiles o tabletas, puede protegerse mediante agentes de software ZTNA, pero los agentes de software de seguridad no se pueden instalar en dispositivos IoT al no contar con un agente. Esto presenta un desafío para la seguridad que SASE no aborda directamente.

Una plataforma SD-WAN Aruba EdgeConnect avanzada puede ayudar a reducir el riesgo asociado a las vulneraciones de seguridad durante la implementación de dispositivos IoT. La plataforma EdgeConnect identifica y clasifica el tráfico de aplicaciones en el primer paquete, lo intercepta en el perímetro de la red y lo dirige a un segmento apropiado. Este tipo de segmentación más amplia lo protege del tráfico restante de la red.

La integración ClearPass con EdgeConnect aumenta la inteligencia de la aplicación con la identidad del usuario y del dispositivo, así como políticas basadas en los perfiles de usuario. Todo ello permite una segmentación aún más precisa. El contexto basado en identidad adicional permite la aplicación de políticas de seguridad, que puede aplicarse en toda la red, desde el Edge hasta la nube.

La segmentación dinámica Zero Trust de Aruba ayuda a las empresas a identificar amenazas de seguridad que provengan de un dispositivo, perfil o aplicación y, a su vez, respeta el cumplimiento de los estándares industriales como PCI, HIPAA y SOX.

La combinación de una SD-WAN avanzada y de una seguridad en la nube mediante un ZTNA basado en políticas garantiza que la WAN, los usuarios, los dispositivos y las aplicaciones de la empresa permanezcan siempre seguros.



Seguridad y WAN de calidad sin compromisos.

Para hacer frente a los retos de seguridad y de costes, han surgido los mejores servicios de seguridad alojados en la nube con organización centralizada, que siguen adoptándose rápidamente. Los servicios de seguridad gestionados centralmente en la nube proporcionan protección a todos los usuarios, con el apoyo de políticas coherentes y la aplicación de políticas en cientos o incluso miles de sitios, sin la complejidad de desplegar o gestionar ningún dispositivo de seguridad físico.

Las soluciones avanzadas de SD WAN, como la plataforma Edge SD-WAN Aruba EdgeConnect, permiten a las empresas interrumpir localmente el tráfico destinado a la nube desde las sucursales en Internet. Admiten, además, funciones de microsegmentación y el cumplimiento exhaustivo de políticas, lo que permite a las empresas proteger sus WAN, seguir las normas de cumplimiento y defenderse frente a posibles vulneraciones.

La organización automatizada de un servicio de seguridad en la nube líder del sector, junto con la plataforma Edge SD-WAN Aruba EdgeConnect, ofrece una solución de SASE potente sin poner en riesgo por ello la funcionalidad de la red o las funciones de seguridad.

El SASE protege a la empresa de amenazas y ofrece el nivel máximo de rendimiento de la aplicación y experiencia del usuario, al tiempo que mantiene la rentabilidad.

Entre los beneficios de esta unión entre la SD-WAN y la seguridad proporcionada en la nube se encuentran los siguientes:

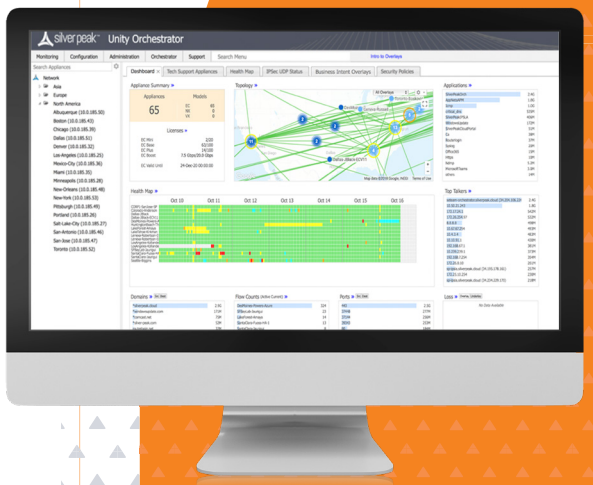
- Aumento de la agilidad empresarial y políticas de TI más simples con una arquitectura SASE que ofrece todas las ventajas de la nube
- Integración simplificada y agilizada de las funciones de seguridad en la nube con funciones de SD-WAN optimizadas
- Libertad para elegir la mejor seguridad de la red y las mejores funciones de SD-WAN
- Evitar la dependencia de un solo proveedor
- Eliminar la necesidad de desplegar costosos y complejos cortafuegos de nueva generación en cada sucursal
- Flexibilidad para adoptar innovaciones de seguridad en el futuro

Automatización de la seguridad en la nube con SD-WAN

Las empresas buscan formas más sencillas de integrar y gestionar sus aplicaciones en toda su WAN y su infraestructura de seguridad. Una de las mejores maneras de simplificar la organización de servicios de seguridad basados en la nube en las sucursales es hacer uso de la automatización con la SD-WAN de Aruba EdgeConnect.

EdgeConnect utiliza interfaces de programación de aplicaciones (API) y servicios de organización de terceros para integrarse con los proveedores líderes de seguridad en la nube, incluidos ZScaler, Check Point, NetSkope y Palo Alto Prisma Access. Aruba Orchestrator valida las credenciales de seguridad en la nube para la conexión y, a continuación, automatiza u organiza el proceso de conexión entre las sucursales en el tejido de la red SD-WAN y los puntos de presencia más cercanos de cumplimiento de la seguridad en la nube principales, y secundarios de manera opcional.

La configuración de políticas de seguridad es una sencilla acción de tipo «arrastrar y soltar» en la intuitiva interfaz de usuario Aruba Orchestrator, lo que permite a las organizaciones especificar un conjunto de políticas de seguridad que se van a adoptar en todas las sucursales con una simple acción.



Flexibilidad y libertad de elección

En un panorama repleto de amenazas en constante evolución, las empresas deben ser lo suficientemente ágiles a la hora de adoptar de forma rápida y rentable nuevas soluciones de seguridad. Las empresas deben 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.

La plataforma SD-WAN Aruba EdgeConnect orientada a los negocios es un pilar clave de una arquitectura SASE de primera clase, que proporciona la capacidad de integrar una plataforma SD-WAN de primera clase con una variedad de servicios de seguridad en la nube de primera clase. Aruba EdgeConnect admite las funciones de seguridad básicas necesarias en las sucursales y complementan la seguridad proporcionada en la nube para ofrecer un Edge de servicio de acceso seguro sin fisuras en toda la empresa.

Para obtener más información, visite www.arubanetworks.com/sdwan

eBook_Aruba-Edge-to-Cloud-Security_DC_062321 a00114994enw

aruba
a Hewlett Packard Enterprise company