HPE aruba networking

Informe técnico empresarial

Diseño de SASE con una SD-WAN segura orientada al negocio

HPE

Descubre cómo la plataforma HPE Aruba Networking EdgeConnect Secure SD-WAN ofrece protección inigualable y acelera tu viaje hacia SASE

Resumen ejecutivo

Gracias a las redes de área amplia definidas por software (SD-WAN), las empresas modernas distribuidas en diferentes áreas geográficas pueden hacer realidad la promesa de transformación de la computación en la nube, reducir los costes de capital y operativos, proporcionar una experiencia de mejor calidad a sus empleados y clientes, y adaptarse rápidamente a las necesidades cambiantes del negocio.

Sin embargo, la transformación digital, la computación en la nube y el trabajo híbrido generan nuevos desafíos de seguridad. Entre ellos se incluyen los siguientes:

- Los usuarios que se conectan desde cualquier lugar y dispositivo
- Cada vez más riesgos de ciberseguridad
- Más datos confidenciales alojados en la nube
- Proliferación de dispositivos IoT que aumentan la superficie de ataque
- Cumplimiento de la normativa y los estándares del sector

Una ventaja clave de la SD-WAN es la capacidad de utilizar servicios de banda ancha de bajo coste. Sin embargo, debido a que los servicios de banda ancha son «públicos» en lugar de «privados», es necesario disponer de capacidades avanzadas de seguridad para garantizar la confidencialidad y la integridad del tráfico de las aplicaciones que pasa por esas conexiones. Las SD-WAN seguras, con firewall integrado, ofrecen seguridad avanzada en la sucursal, incluida la protección IDS/IPS y DDoS, para aislar el tráfico del IoT de las aplicaciones para tareas cruciales mediante la segmentación de las redes en zonas y minimizar la superficie de ataque para facilitar el cumplimiento de los estándares del sector.

Además, al trasladar la mayoría de las aplicaciones empresariales a la nube, las organizaciones se enfrentan a nuevos desafíos de seguridad como proporcionar acceso seguro a trabajadores remotos, proteger a usuarios de Internet de las amenazas de la Web y garantizar la protección de los datos corporativos confidenciales alojados en aplicaciones en la nube frente a las filtraciones de datos.

Al integrarse a la perfección con las soluciones SSE (Security Service Edge), la SD-WAN segura y avanzada crea una arquitectura SASE fiable que permite a las organizaciones abordar los desafíos del trabajo híbrido y la computación en la nube.

Este documento describe por qué la SD-WAN es crítica para la seguridad y cómo una implementación de seguridad SD-WAN exhaustiva puede proteger mejor a las dinámicas empresas modernas con enfoque cloud-first. Luego, se abordará el amplio conjunto de prestaciones de seguridad incorporadas a la plataforma HPE Aruba Networking EdgeConnect SD-WAN, entre ellas un firewall de última generación, y cómo la plataforma SD-WAN se integra a la perfección con las capacidades de Security Service Edge (SSE), ya sea con HPE Aruba Networking SSE para formar una solución SASE (Secure Access Service Edge) unificada o con proveedores externos de seguridad en la nube.

A medida que más aplicaciones y cargas de trabajo se migran a la nube, el rol del centro de datos corporativo se reduce significativamente. Con el trabajo híbrido, el perímetro de seguridad también está desapareciendo a medida que los usuarios se conectan desde cualquier lugar y dispositivo, y acceden a datos confidenciales alojados en la nube.

Las organizaciones que intentan gestionar redes WAN empleando enrutadores tradicionales se enfrentan a inconvenientes y limitaciones continuos. Los procesos manuales y las arquitecturas complejas impiden a las organizaciones establecer una arquitectura segura y responder de forma efectiva a amenazas maliciosas como los ataques de denegación de servicio (DoS). Las preocupaciones de seguridad pueden obstaculizar el uso de la banda ancha de bajo coste y frenar el avance de la adopción de la nube en general y las aplicaciones SaaS en particular.

Considerando el impacto de estos cambios, la arquitectura WAN de la empresa también debe cambiar. En agosto de 2019, Gartner definió SASE (Secure Access Service Edge) como la combinación de capacidades avanzadas de red WAN de extremo con funciones de seguridad de red como SWG, CASB, FWaaS y ZTNA que se proporcionan en la nube. Una arquitectura SASE proporciona una forma más segura y flexible de conectarse a aplicaciones alojadas en la nube sin enviar el tráfico de las aplicaciones a un centro de datos (backhauling) antes de reenviarlo a la nube.

Con una arquitectura SASE, la SD-WAN puede direccionar el tráfico de las aplicaciones directamente a un proveedor de SaaS o un servicio de seguridad alojado en la nube de confianza, donde pueden realizarse inspecciones de seguridad más avanzadas antes de reenviarlo al proveedor de SaaS, todo ello de acuerdo con las políticas de seguridad empresarial.

Las opciones de conectividad tradicional de línea privada (como la conmutación de etiquetas multiprotocolo o MPLS) y las prácticas de enrutamiento—en concreto el backhauling— son claramente una opción poco adecuada para las aplicaciones basadas en la nube. Estas opciones presentan inconvenientes clave, como el impacto negativo que producen en el rendimiento (específicamente para el tráfico de Internet o destinado a la nube), el alto coste de estos servicios e infraestructuras de red y el hecho de que requieren mantener una gran cantidad de equipos de seguridad en las sucursales.

La proliferación de dispositivos del Internet de las cosas (IoT) se ha convertido en otra preocupación central para las organizaciones, ya que esto aumenta de forma significativa la superficie de ataque. Por lo general, el diseño simple de estos dispositivos les impide alojar un agente de seguridad y, por tanto, no pueden protegerse fácilmente. Las organizaciones necesitan una solución de seguridad diferente para que los dispositivos IoT puedan proteger sus redes de posibles vulnerabilidades que permitan un acceso indebido a la red. Por esa razón, SASE debe complementarse con un marco de seguridad de control de acceso de confianza cero que segmente el tráfico en función de la identidad, de modo que los usuarios y los dispositivos IoT solo puedan llegar a los destinos de la red en consonancia con su función en la empresa.

«El trabajo híbrido y el viraje inexorable hacia la computación en la nube han acelerado la adopción de SASE».

Gartner[1]

[1] "2024 Strategic Roadmap for SASE Convergence," Gartner, 2023

Por qué la SD-WAN es crítica para la seguridad

Contar con seguridad sólida es un requisito previo y un elemento integral de muchas de las ventajas que ofrece la SD-WAN centrada en el negocio. Por ejemplo, el uso de Internet de banda ancha como opción de conectividad de bajo coste es fundamental para la propuesta de valor de la SD-WAN.

Sin embargo, el hecho de que la banda ancha sea «pública» en lugar de «privada» genera la necesidad de garantizar la confidencialidad y la integridad del tráfico de las aplicaciones que atraviesan estas conexiones.

Aunque el enrutamiento local de Internet es esencial para mejorar el rendimiento y reducir el ancho de banda necesario para el backhauling, también expone a los usuarios de las sucursales y a sus redes locales directamente a Internet y sus numerosas amenazas. Por eso, ahora necesitas una forma de limitar los destinos de salida, bloquear el tráfico entrante no deseado/no solicitado y filtrar el tráfico permitido/esperado para bloquear amenazas.

Sin embargo, no todas las aplicaciones web se crean igual y parte del tráfico web puede exponer a la empresa a los virus, los troyanos, los ataques DDoS y otras vulnerabilidades. Por lo tanto, el enrutamiento directo de Internet también debe ser seguro. Por ejemplo, una política de seguridad de tráfico web podría definirse de la siguiente manera:

- Enviar tráfico SaaS empresarial conocido y de confianza como tráfico de vídeo y voz (comunicaciones unificadas como servicio, UCaaS), directamente a Internet.
- Enviar el resto del tráfico web a una solución Security Service Edge (SSE).
- Enviar el tráfico de las aplicaciones hospedadas en el centro de datos empresarial directamente a la oficina central.

Para implementar dicha política, el tráfico web debe direccionarse granularmente a su destino previsto. Esto requiere identificar la aplicación en el primer paquete porque, una vez que se ha establecido una sesión de aplicación, no se puede redirigir a un destino alternativo sin interrumpir el flujo, lo que provoca la disrupción de la aplicación. Y, debido a que los rangos de direcciones IP que utilizan las aplicaciones SaaS cambian casi continuamente, las actualizaciones de la tabla de direcciones deben automatizarse e implementarse diariamente.

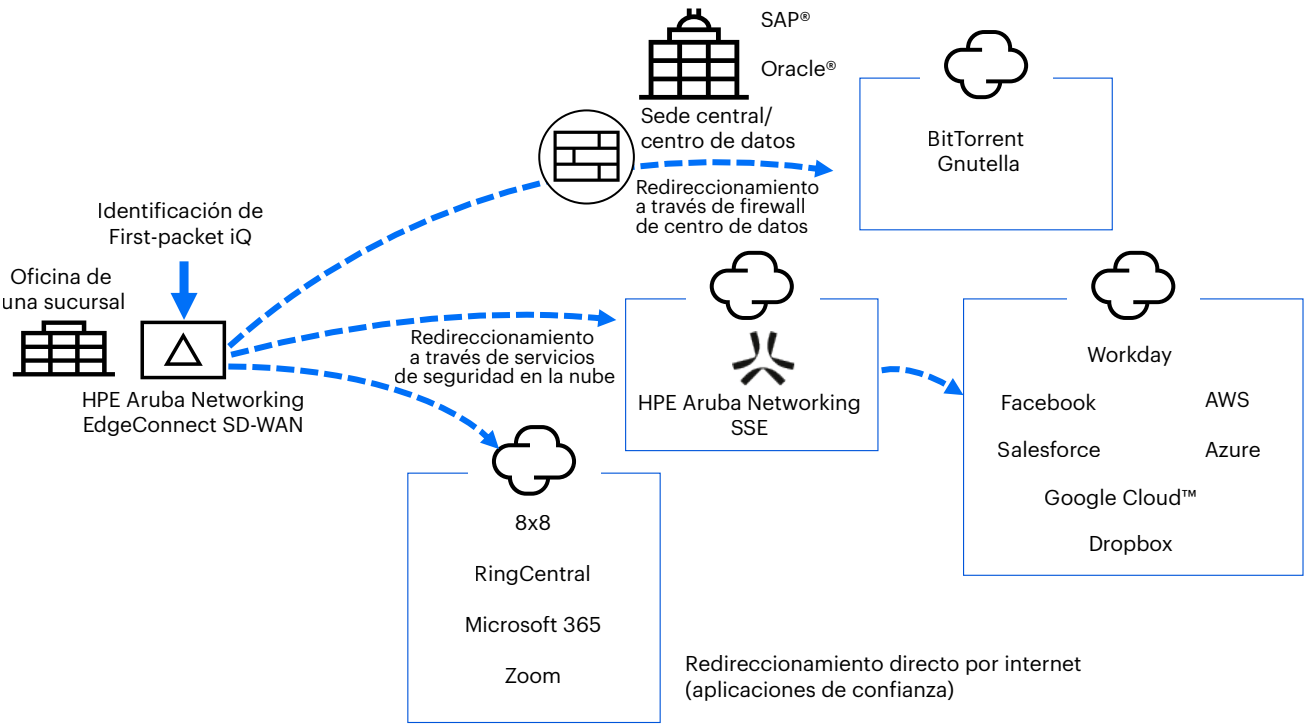


Figura 1. El tráfico de las aplicaciones se identifica en el primer paquete para direccionar el tráfico a su destino correcto con el fin de permitir la aplicación de la política de seguridad granular.

Presentamos HPE Aruba Networking EdgeConnect SD-WAN

La plataforma EdgeConnect SD-WAN proporciona a las empresas la flexibilidad que necesitan para utilizar cualquier combinación de tecnologías de transporte, incluidos los servicios públicos de banda ancha, para conectar a los usuarios a las aplicaciones sin poner en riesgo el rendimiento o la seguridad de las aplicaciones.

Los cuatro componentes principales de la plataforma incluyen:

- Dispositivos físicos o virtuales sin interacción **HPE Aruba Networking EdgeConnect SD-WAN** que se implementan en las sucursales, las oficinas centrales y los centros de datos en la nube de una organización
- **HPE Aruba Networking EdgeConnect SD-WAN Orchestrator**, un sistema de gestión centralizado que permite la configuración y organización simplificadas de toda la WAN y ofrece capacidad de observación completa tanto en las aplicaciones heredadas como en la nube. Las políticas de seguridad y QoS se definen de forma centralizada y se implementan automáticamente a nivel global en todos los dispositivos de la SD-WAN, lo que aumenta la eficiencia operativa y minimiza los errores humanos que pueden poner en peligro la seguridad de la sucursal
- **WAN Optimization**, un paquete de rendimiento de WAN que permite a los equipos de TI utilizar capacidades de optimización de WAN líderes en el mercado cuando sea necesario, simplemente marcando una casilla en la interfaz de Orchestrator
- **Defensa dinámica ante amenazas / Seguridad avanzada**, una licencia de seguridad opcional que habilita las funciones de prevención y detección de intrusiones (IDS/IPS) en los dispositivos Aruba EdgeConnect SD-WAN

EdgeConnect SD-WAN está diseñado con un amplio conjunto de capacidades para abordar todos los desafíos y requisitos de seguridad del extremo de la WAN de la sucursal inherentes a las implementaciones de SD-WAN.

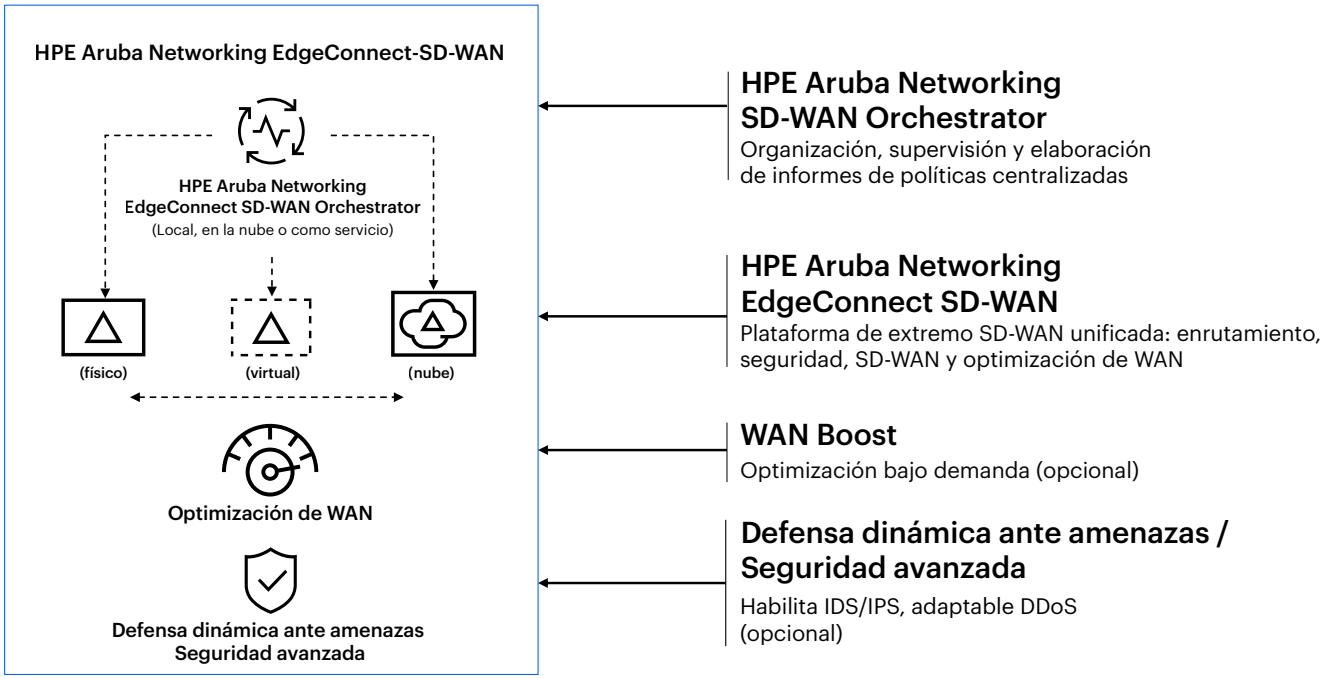


Figura 2. Plataforma HPE Aruba Networking EdgeConnect SD-WAN

Cómo EdgeConnect SD-WAN proporciona una SD-WAN segura

HPE Aruba Networking EdgeConnect SD-WAN no se limita a lo básico a la hora de garantizar la confidencialidad del tráfico de las aplicaciones que atraviesa las redes públicas. Un amplio conjunto de capacidades de seguridad proporciona cobertura en cuatro áreas esenciales: el plano de datos, el plano de gestión, la integración con Security Service Edge (SSE) y el cumplimiento. El resultado neto es el espectro completo de protección necesario para que las empresas obtengan todos los beneficios de una SD-WAN avanzada, como mayor rendimiento de las aplicaciones, menor coste general de la WAN y mayor agilidad empresarial, sin exponerse a mayores riesgos de seguridad.

Seguridad del plano de datos impulsada por aplicaciones

Las diferentes aplicaciones merecen, o quizás incluso requieren, diferentes tratamientos en su gestión desde una perspectiva de seguridad (sin mencionar otras «perspectivas», como QoS, optimización del rendimiento y políticas de tunelización mediante protocolo). Por ejemplo, una aplicación empresarial que procesa transacciones confidenciales puede requerir cifrado independientemente del tipo de transporte que se utilice para cumplir los requisitos de cumplimiento, mientras que las aplicaciones SaaS pueden depender de suspropias capacidades nativas (por ejemplo, TLS). Por eso, es importante tener una SD-WAN basada en aplicaciones que permita implementar políticas y ajustes de configuración por aplicación.

Las capacidades de seguridad relevantes disponibles con HPE Aruba Networking EdgeConnect SD-WAN incluyen:

Firewall de última generación: EdgeConnect SD-WAN incluye un firewall de última generación que proporciona, en una sola entidad, funciones de seguridad avanzadas como la inspección profunda de paquetes y la prevención de intrusiones, así como detección de la identidad de las aplicaciones y los usuarios. Proporciona a los líderes de TI la capacidad de bloquear el acceso de malware a la red en función de la aplicación, la identidad y el contexto, independientemente del puerto/protocolo utilizado. Además, los líderes de TI obtienen mayor visibilidad de la actividad de la red y de los riesgos potenciales.

Prevención y detección de intrusiones (IDS/IPS): EdgeConnect SD-WAN integra un sistema de prevención y detección de intrusiones (IDS/IPS) basado en reglas. El sistema basado en firmas supervisa el tráfico de la red para encontrar patrones que coincidan con una firma de ataque concreta. El sistema, integrado con el firewall de última generación de EdgeConnect, permite una selección para inspección a nivel de la aplicación en función de las zonas del firewall y proporciona acciones como descartar o permitir el tráfico cuando se detecta una intrusión.

El sistema puede funcionar en modo estricto o en modo de alto rendimiento. En el modo estricto, el tráfico pasa a través del sensor, de modo que se bloquea 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 eficiencia sin afectar al rendimiento de la red. En este modo, la intrusión se bloquea una vez detectada. En función de sus requisitos de seguridad, las organizaciones pueden elegir entre el modo estricto o el modo de rendimiento.

El registro de amenazas proporciona análisis de red y seguridad a HPE Aruba Networking Central o a un SIEM (gestión de seguridad de información y eventos) de terceros, como Splunk, para supervisar las amenazas en tiempo real.

La aplicación de seguridad HPE Aruba Networking EdgeConnect SD-WAN para Splunk proporciona una visión en panel de las notificaciones de eventos de seguridad exportadas desde la plataforma (figura 3). Los administradores de TI pueden configurar la plataforma fácilmente para reenviar las notificaciones de eventos de seguridad a Splunk, centralizando el registro, la visualización y el análisis de eventos de seguridad junto con otros eventos de telemetría o de red. Desde Splunk, los usuarios pueden filtrar, ordenar, navegar y ver las notificaciones colectivas de los eventos de seguridad generadas en toda la estructura de la SD-WAN, las tendencias generales y los principales emisores para identificar con mayor facilidad los eventos de red que requieren mayor investigación.

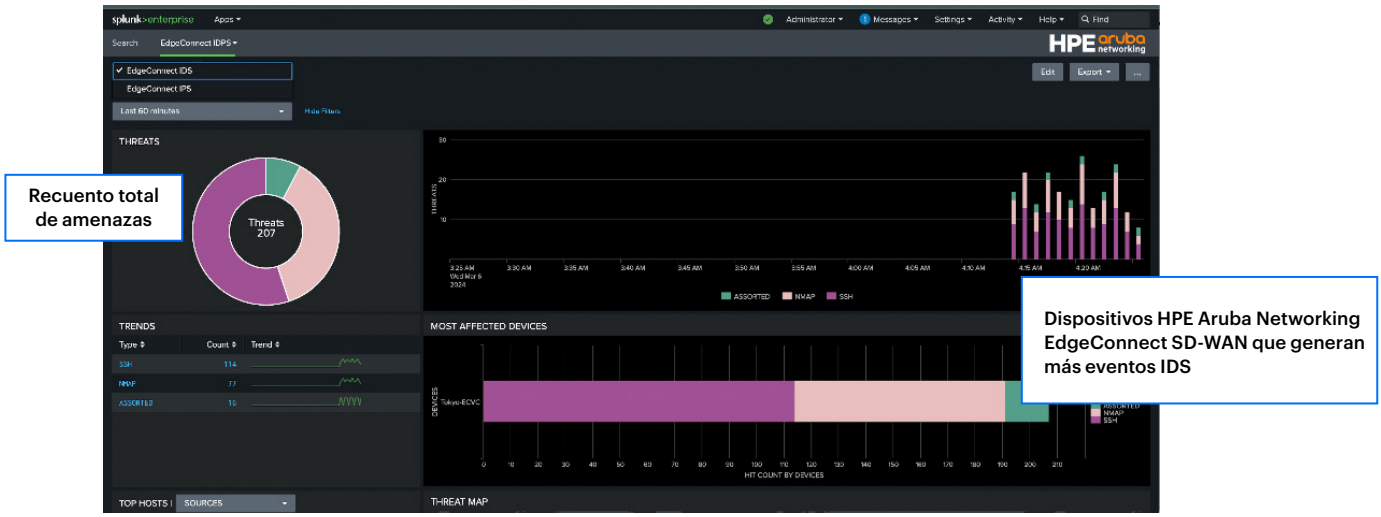


Figura 3. Vista de eventos IDS/IPS en Splunk procedentes de HPE Aruba Networking SD-WAN.

Defensa contra DDoS: Dada la creciente frecuencia de los ataques DDoS, las organizaciones deben tomar medidas de defensa que sean rentables. Implementando HPE Aruba Networking EdgeConnect SD-WAN en las sucursales, esto es precisamente lo que obtienes. En caso de un ataque DDoS, la plataforma limita la cantidad de solicitudes malintencionadas con acciones como el envejecimiento acelerado, el exceso de descarte y el bloqueo de la fuente. Las acciones se generan en umbrales de DoS preestablecidos o configurables para parámetros de tráfico como la velocidad de flujo, los flujos concurrentes y los flujos embrionarios. Los administradores pueden definir umbrales mínimos y máximos. El umbral mínimo ayuda a detectar problemas de forma temprana, mientras que el umbral máximo garantiza que el tráfico no se detenga de forma prematura. Los perfiles de protección mediante cortafuegos permiten a los administradores establecer distintos niveles de protección frente a ataques de DDoS en toda la organización al vincular dichos perfiles a zonas de cortafuegos. La solución también bloquea una lista de direcciones IP de atacantes conocidos y enrutar dinámicamente el tráfico a través de enlaces de red no afectados en caso de un ataque de DDoS, lo que hace posible la continuidad del negocio. La plataforma incluye un conjunto completo de informes para defensa de DoS como violaciones de umbral, caídas de flujo, equipos denegados y recuentos de paquetes, principales emisores de tráfico, y alarmas como superación de umbrales DoS (figura 4).

Las acciones se basan en umbrales de DoS preestablecidos o configurables para parámetros de tráfico como la velocidad de flujo, los flujos concurrentes y los flujos embrionarios. Además, la solución puede enrutar el tráfico dinámicamente a través de enlaces de red no afectados en caso de un ataque DDoS sin degradar el rendimiento de las aplicaciones ni afectar a la capacidad de gestión de la SD-WAN. EdgeConnect no solo se protege a sí mismo, sino que también protege a todos los usuarios y sistemas tanto en la red local como en las conexiones WAN operativas restantes

Figura 4. Número de flujos permitidos y rechazados en cada intervalo de cinco minutos por zona del cortafuegos en HPE Aruba Networking EdgeConnect SD-WAN

Protección de los datos en tránsito: Cada ruta de datos de HPE Aruba Networking EdgeConnect está protegida por túneles IPsec que utilizan cifrado AES de 256 bits para mantener la confidencialidad de la aplicación y los datos. EdgeConnect utiliza un protocolo IPsec UDP sin IKE; es decir, emplea cifrado IPsec UDP basado en estándares, pero no requiere claves precompartidas de Internet Key Exchange. Las claves de cifrado nunca se repiten y son direccionalmente únicas. HPE Aruba Networking SD-WAN Orchestrator administra las claves de cifrado y las rotaciones automáticamente, lo que reduce el tiempo de configuración del túnel sin pérdida de servicio. Este protocolo evita los problemas que surgen al implementar NAT (traducción de direcciones de red) con IKE, como fallas que suceden cuando las sucursales tienen varios dispositivos con diferentes requisitos de VPN. Debido a que los túneles sin IKE usan diferentes puertos a través de IPsec, es poco probable que los firewalls ascendentes los limiten obloqueen. Estas funciones avanzadas para proteger los datos en tránsito aumentan la flexibilidad, la seguridad y la solidez de la comunicación segura entre puntos de conexión remotos.

Protección de los datos en reposo: Todos los bloques de datos que persisten dentro de los dispositivos HPE Aruba Networking EdgeConnect como resultado de la capacidad opcional de deduplicación de datos de WAN Optimization están protegidos con cifrado AES de 128 bits.

Segmentación de confianza cero: EdgeConnect SD-WAN crea zonas seguras integrales en cualquier combinación de usuarios, dispositivos, grupos de aplicaciones y superposiciones virtuales, propagando las actualizaciones de configuración a los sitios de acuerdo con el propósito empresarial. EdgeConnect SD-WAN, junto con HPE Aruba Networking ClearPass Policy Manager, aplica una arquitectura de confianza cero que segmenta dinámicamente la red y aplica principios de acceso con privilegios mínimos. Garantiza que los usuarios y los dispositivos IoT solo se comuniquen con destinos coherentes con su función según la identidad, los derechos de acceso y la posición de seguridad.

Además, EdgeConnect SD-WAN permite a las organizaciones crear múltiples superposiciones de WAN virtual específicas de la aplicación (también llamadas superposiciones de propósito empresarial). Cada superposición virtual especifica los requisitos de prioridad y calidad de servicio para los grupos de aplicaciones en función de los requisitos empresariales. Con estas especificaciones, EdgeConnect automatiza el direccionamiento del tráfico de un extremo a otro en todos los servicios de transporte WAN subyacentes.

Cada superposición virtual se asigna a una zona o zonas del lado de la LAN. Una zona puede estar compuesta por VLAN, interfaces físicas y lógicas y subinterfaces. A cada zona se le pueden asignar políticas de seguridad que limitan la conectividad con otras zonas. Por ejemplo, una política podría permitir solo el tráfico saliente, o permitir el tráfico entrante solo de aplicaciones y servicios aprobados, o bloquear todo el tráfico de zonas menos seguras.

Con la segmentación de confianza cero:

- Los usuarios y los dispositivos IoT acceden a los recursos según el rol y el contexto utilizando principios de acceso con privilegios mínimos
- El tráfico dentro de cada zona se aísla del tráfico en otros segmentos, lo que reduce el acceso no autorizado y limita el alcance de los incidentes
- La microsegmentación se extiende desde la LAN, a través de la WAN y hasta los centros de datos y las plataformas en la nube
- Las aplicaciones de alta prioridad disfrutan de un rendimiento más rápido y fiable en toda la WAN, lo que aumenta la disponibilidad de las aplicaciones y mejora la experiencia y la productividad de los usuarios finales

Creación sencilla de políticas: Los administradores de TI pueden crear segmentos de red en cuestión de minutos utilizando una interfaz gráfica de usuario intuitiva. Estos segmentos pueden conectar redes LAN con otras redes LAN (LAN-WAN-LAN) y con centros de datos (LAN-WAN-centro de datos). Las superposiciones de WAN virtual se definen en función de los requisitos y el propósito empresarial, no de los detalles de la infraestructura, como las direcciones IP. Las políticas de seguridad basadas en zonas se muestran en una matriz de configuración que facilitan su comprensión.

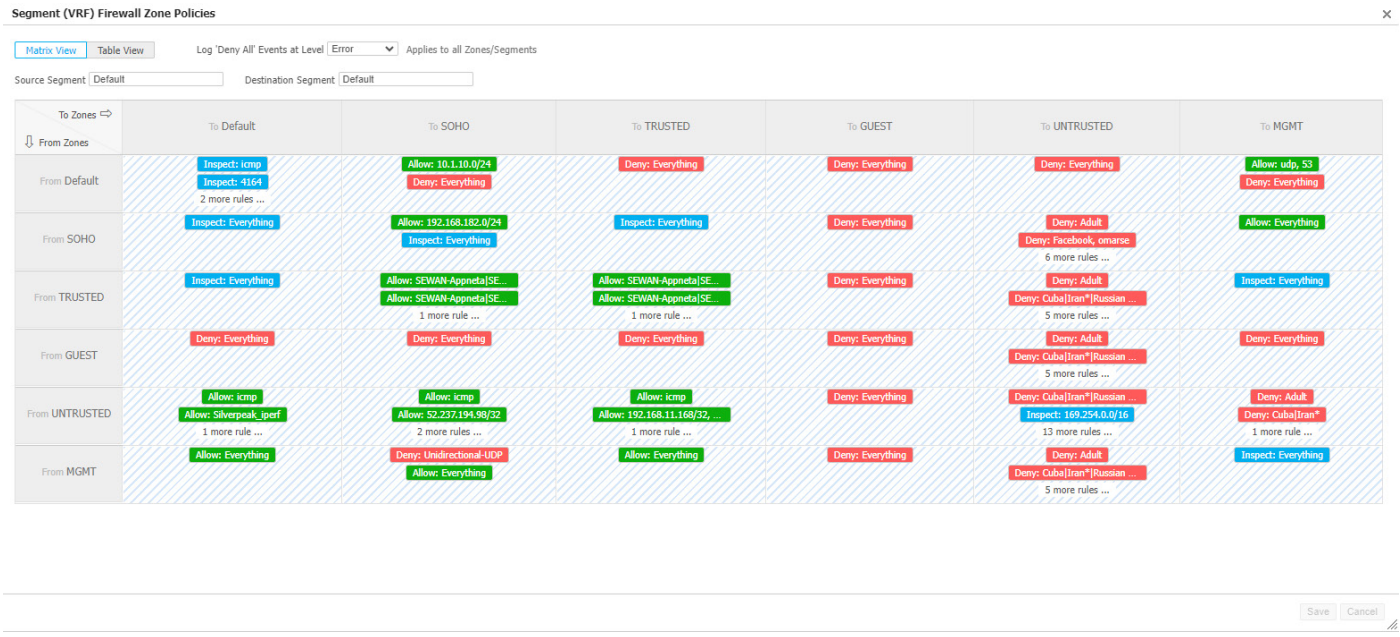
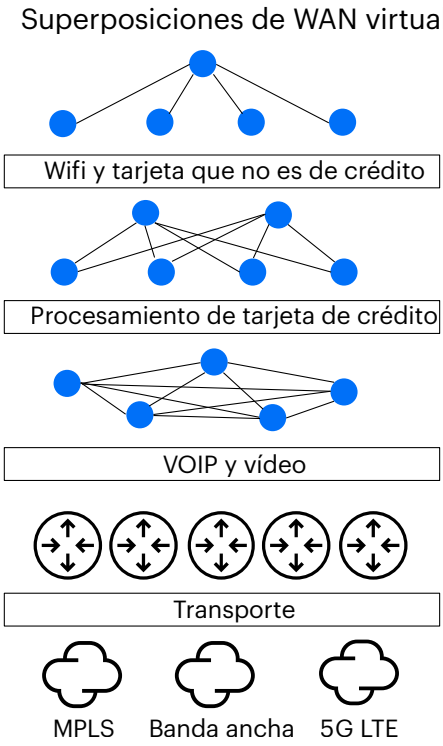


Figura 5. Una matriz de configuración de políticas de seguridad simplifica enormemente la creación y gestión de reglas de segmentación

Organización central y aplicación automatizada: Una vez que se han definido las superposiciones de WAN virtual y las políticas de firewall basadas en zonas, HPE Aruba Networking SD-WAN Orchestrator las implementa en todos los dispositivos EdgeConnect SD-WAN, donde se aplican automáticamente. Esto sustituye a la configuración manual, que consume mucho tiempo, de los enrutadores y firewalls cada vez que cambia una política.

Entre las ventajas se incluyen las siguientes:

— Cumplimiento uniforme de las políticas de seguridad en las redes LAN y WAN
— Menos errores de configuración
— Mayor cumplimiento de las regulaciones y los estándares del sector
— Mayor productividad para el personal de seguridad y de operaciones



Política de acceso	Topología	Conexión	Calidad de servicio (QoS)
VLAN de invitado	Hub-and-spoke	Internet	Mín. Coste
VLAN de datos	Hub-and-spoke doble	MPLS—Internet	Máx. disponibilidad
VLAN de voz	Malla completa	MPLS—Internet—LTE	Máx. calidad

Figura 6. HPE Aruba Networking EdgeConnect SD-WAN que propaga la microsegmentación en toda la WAN

Control de acceso a la red (NAC) seguro: La integración de HPE Aruba Networking ClearPass con HPE Aruba Networking EdgeConnect SD-WAN hace posible que los administradores puedan dar seguridad a los puertos de la plataforma utilizando 802.1X y autenticación MAC. Esto es ideal para ubicaciones pequeñas, oficinas en casa o cualquier lugar donde los puertos de la plataforma puedan ser vulnerables a accesos no autorizados. Con NAC habilitado, la aplicación de la plataforma autentica el tráfico con 802.1X, y soporta los métodos de autenticación EAP-TLS, EAP-TTLS y EAP-PEAP. Autenticación MAC también disponible para dispositivos como IoT que no soporten el protocolo 802.1X.

SASE unificado con HPE Aruba Networking

La solución de SASE unificado de HPE Aruba Networking proporciona una estructura de conectividad que incluye el galardonado HPE Aruba Networking SSE y HPE Aruba Networking EdgeConnect SD-WAN líder del sector en una única solución para satisfacer la creciente demanda de soluciones de red y seguridad integradas. HPE Aruba Networking SSE también está estrechamente integrado con HPE Aruba Networking EdgeConnect SD-Branch y HPE Aruba Networking EdgeConnect Microbranch.

La solución acelera el proceso de las organizaciones hacia SASE. Como solución de SASE unificado, es fácil de implementar gracias a una plataforma única y estrechamente integrada, que incluye una gestión simplificada.

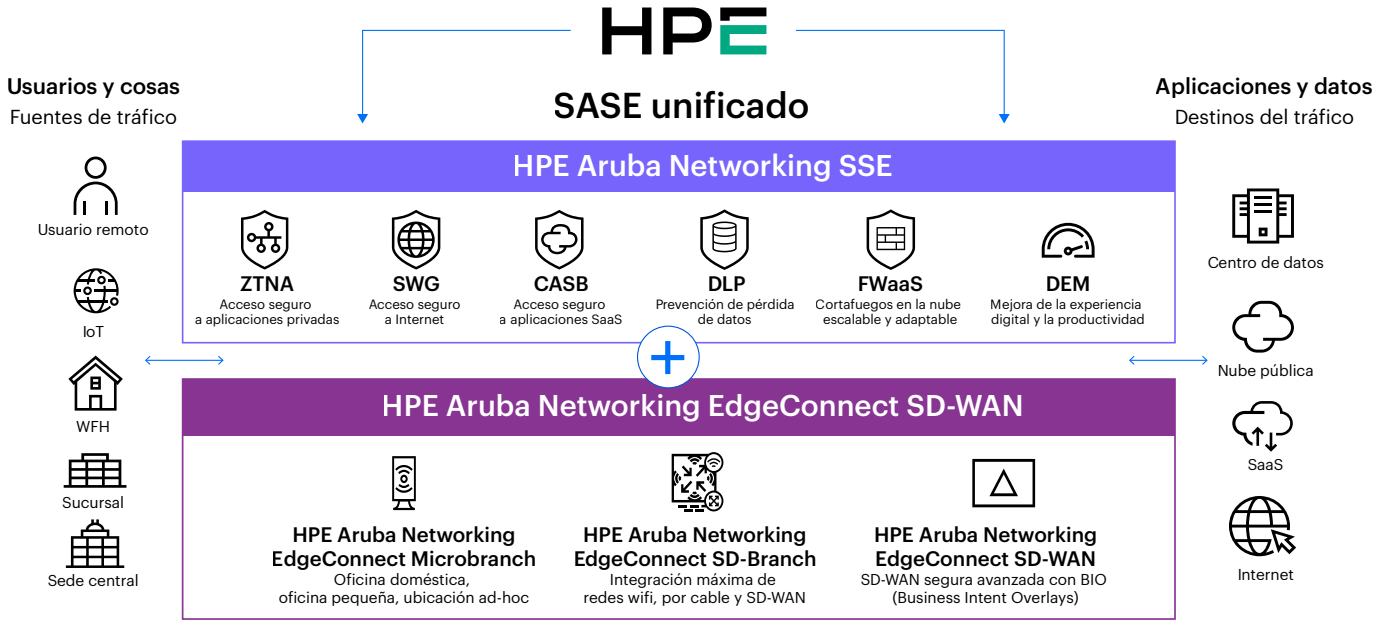


Figura 7. Implementa HPE Aruba Networking EdgeConnect SD-WAN, líder del sector, con la plataforma HPE Aruba Networking SSE nativa de la nube para crear una solución de SASE unificado.

SSE es una plataforma unificada donde ZTNA, SWG y CASB comparten una única base de código. Todas las políticas se administran desde una única interfaz de usuario, lo que facilita enormemente el control de acceso a los administradores de TI. Permite a los usuarios y terceros autorizados acceder a recursos con ZTNA con agentes y sin agentes. Los usuarios están protegidos contra amenazas web con SWG y los datos confidenciales alojados en aplicaciones SaaS se supervisan de forma segura para evitar la filtración de datos con CASB. Además, la solución armoniza el acceso en todo el mundo a través de una red troncal en la nube de Amazon Web Services (AWS), Microsoft Azure, Google y Oracle.

Las funcionalidades de HPE Aruba Networking SSE incluyen:

— **ZTNA (acceso a redes de confianza cero)** se basa en el principio de «nunca confiar, siempre verificar», de modo que un dispositivo que se conecta a la red no es fiable de forma predeterminada. A diferencia de una VPN, que ofrece a los usuarios conectados amplio acceso a la red corporativa, ZTNA limita el acceso de los usuarios solo a aplicaciones o microsegmentos específicos que hayan sido aprobados por el usuario con un acceso de mínimo privilegio. Con ZTNA, los trabajadores remotos pueden conectarse desde cualquier lugar.

Los usuarios de terceros también pueden incorporarse fácilmente a la red con ZTNA sin agente. No es necesario instalar un agente ZTNA en los ordenadores portátiles; los usuarios de terceros simplemente inician sesión en un portal web de ZTNA con sus propias credenciales.

- **SWG (Secure Web Gateway)** se sitúa entre un usuario y un sitio web para protegerlo contra amenazas maliciosas. Realiza varias inspecciones de seguridad, incluido el filtrado de URL, la detección de códigos maliciosos y el control de acceso a la Web, y proporciona políticas que pueden limitar el acceso a sitios para adultos, juegos de apuestas o sitios peligrosos, por ejemplo.
- **CASB (Cloud Access Security Broker)** garantiza que los datos confidenciales alojados en la nube permanecen protegidos. Identifica y detecta datos confidenciales en aplicaciones en la nube y aplica políticas de seguridad como la autenticación y el inicio de sesión único (SSO). Supervisa las actividades de los usuarios en los servicios de nube, identifica posibles riesgos de seguridad e infracciones de políticas para evitar la pérdida de datos y controla las cargas y descargas de bloques de aplicaciones SaaS como Box, SharePoint, Facebook y Salesforce. Evita que los usuarios se registren y utilicen aplicaciones en la nube para las que no están autorizados por las políticas de seguridad y TI de una organización, lo que permite a las organizaciones reducir la TI en la sombra.
- **DEM (Digital Experience Monitoring)** garantiza la productividad del usuario al medir las métricas salto a salto y supervisar el rendimiento de las aplicaciones, los dispositivos y la red. El equipo de TI puede identificar problemas de conectividad fácilmente y reducir el tiempo medio de resolución.

Integración con múltiples partners SASE

HPE Aruba Networking EdgeConnect SD-WAN también puede conectarse sin problemas a diversos servicios de seguridad en la nube de proveedores externos para aquellas organizaciones que prefieren adoptar SASE con servicios de seguridad de su elección o integrarse sin problemas con un ecosistema de seguridad existente.

HPE Aruba Networking mantiene asociaciones tecnológicas con proveedores líderes de SSE (Security Service Edge) que cubren áreas de soluciones como puertas de enlace web seguras (SWG), agente de seguridad de acceso a la nube (CASB), acceso a la red de confianza cero (ZTNA) y aislamiento de navegador remoto (RBI), de empresas de seguridad como Zscaler, Netskope, Check Point, McAfee, Palo Alto Networks y Symantec.

Integración y organización automatizadas: HPE Aruba Networking EdgeConnect automatiza la organización con proveedores de seguridad en la nube (SSE) de terceros y la configuración de túneles IPsec entre EdgeConnect y los proveedores de SSE. Con esta capacidad, la función de clasificación de aplicaciones First-packet iQ™ identifica primero las aplicaciones y los dominios web en función del primer paquete. A continuación, el tráfico se dirige de manera inteligente a los servicios de SSE en función de las políticas de seguridad definidas por la organización. Los administradores también pueden utilizar una sencilla interfaz de arrastrar y soltar que facilita la asignación de políticas al tráfico de aplicaciones específicas y el enrutamiento del tráfico a herramientas de seguridad específicas. Por ejemplo, un tráfico vinculado a Internet se enruta automáticamente a través de servicios de seguridad basados en la nube para el control de acceso de Capa 7, el filtrado de amenazas y el análisis.

Seguridad del plano de gestión y a nivel del sistema

A pesar de ser menos importante que su equivalente del plano de datos, la seguridad del sistema y del plano de gestión no es menos importante. Las capacidades relevantes de HPE Aruba Networking EdgeConnect en esta área incluyen:

Zero-Touch Provisioning seguro: Una parte fundamental de la propuesta de valor de HPE Aruba Networking EdgeConnect SD-WAN es un modelo de implementación plug and play que permite una instalación rápida sin necesidad de la presencia de una TI distribuida. La seguridad de este proceso adopta la forma de un procedimiento de autenticación y autorización de dos pasos. Antes de recibir su configuración y sus políticas y de convertirse en una parte activa de la SD-WAN, cada dispositivo EdgeConnect recién conectado debe ser autenticado en primera instancia por el portal en la nube de HPE Aruba Networking y, a continuación, un administrador de TI debe aprobarlo a través de HPE Aruba Networking SD-WAN Orchestrator.

Además, SD-WAN Orchestrator también puede utilizarse para revocar posteriormente el acceso a un dispositivo determinado (p. ej., si se roba o está en riesgo). Esto da como resultado que se descarte el tráfico en tránsito y que el dispositivo especificado no pueda descargar la información de configuración ni unirse a la SD-WAN.

Comunicaciones de gestión cifradas: Todas las sesiones de comunicación entre los dispositivos EdgeConnect, SD-WAN Orchestrator, el portal en la nube de HPE Aruba Networking y los navegadores web de los administradores están protegidas con TLS 1.2. Además, todos los protocolos débiles (p. ej., SSLv2, SSLv3, TLS 1.0, TLS 1.1), hashes débiles (p. ej., MD5) y algoritmos de cifrado débiles (p. ej., DES, RC4) están deshabilitados de manera predeterminada.

Sistema reforzado: EdgeConnect es un dispositivo reforzado que se suministra con el modo «reforzado» predeterminado de fábrica. Este enfoque garantiza la seguridad inmediata de los dispositivos que se conectan por primera vez.

Otras protecciones del plano de gestión incluyen:

Autenticación y autorización de usuario fiables

- Soporte para local, RADIUS, TACACS+ y Oauth para autenticación y autorización con sistemas de gestión de identidades como Active Directory y Okta.
- Control de acceso granular basado en roles con usuarios de solo lectura y múltiples roles de administrador
- Lista blanca para Orchestrator que restringe el acceso administrativo a un conjunto específico de direcciones IP o subredes

Registro extenso para SD-WAN Orchestrator and EdgeConnect

- **Registros de eventos/alarmas:** — para errores del sistema relacionados con la memoria, la unidad central de procesamiento (CPU), las interfaces de red, el enrutamiento y la conectividad del plano de gestión
- **Alertas de cruce de umbral** — umbrales configurables, umbrales ascendentes y descendentes para señalar condiciones de preocupación inminente o próxima, como el alto uso de memoria o de ancho de banda
- **Registros de auditoría** — para realizar el seguimiento de todos los accesos a una actividad realizada a través de cualquiera de las interfaces de gestión disponibles (CLI, WebUI o REST API)
- **Registros del firewall** — los flujos de tráfico inspeccionados por el firewall de última generación de EdgeConnect generan eventos de denegación, aceptación y eliminación, así como los motivos de dichos eventos. Posteriormente, los registros del firewall se pueden transmitir a una herramienta SIEM de terceros (por ejemplo, Splunk).
- **Registros de Netflow/tráfico** — captura de datos de flujo completos (no muestreados) para que puedan transmitirse a una herramienta de terceros (p. ej., Netflow-collector)

Además de ser críticos para la gestión de redes y la respuesta a incidentes, los datos de registro pueden ser valiosos para cumplir con estándares como HIPAA.

Certificación de seguridad y cumplimiento

A medida que los usuarios se conectan desde cualquier lugar a través de conexiones inseguras por sí mismas, como Internet de banda ancha y 5G, y acceden a datos confidenciales en línea, la necesidad de certificar una SD-WAN para la seguridad se ha vuelto más apremiante. HPE Aruba Networking EdgeConnect SD-WAN ha conseguido la certificación de SD-WAN segura de ICSA Labs gracias a su conjunto integral y fiable de funciones de SD-WAN, y sus requisitos de seguridad de plataforma.

Los requisitos de certificación de SD-WAN segura de ICSA Labs incluyen:

- **Funciones avanzadas de SD-WAN** como tunelización basada en protocolo, selección de rutas dinámicas y Zero Touch Provisioning
- **Soporte nativo (o mediante encadenamiento de servicios) para funciones de seguridad avanzadas como** antimalware, prevención de intrusiones y protección DoS
- **Cifrado** de datos confidenciales, así como de comunicaciones administrativas y operativas
- **Aplicación de políticas** para funciones específicas de WAN y para políticas de seguridad
- **Registro de eventos de seguridad**

Gracias a la seguridad que aporta el uso de una SD-WAN segura y certificada por una organización externa e independiente reconocida a nivel mundial, las empresas pueden simplificar la arquitectura de red en las sucursales al reemplazar los firewalls de las sucursales por EdgeConnect SD-WAN.

La mayoría de las características de seguridad cubiertas hasta ahora son aplicables a múltiples requisitos que abarcan diversas regulaciones. Las capacidades de autenticación, autorización y auditoría, por ejemplo, son un requisito fundamental de la publicación especial 800-53 del NIST (controles de seguridad y privacidad para sistemas de información y organizaciones) y, por lo tanto, de prácticamente todas las reglamentaciones que hacen referencia a ella.

También es notable, especialmente por su singularidad entre las soluciones SD-WAN, la compatibilidad de EdgeConnect SD-WAN con la microsegmentación. La capacidad de crear superposiciones cifradas y específicas de la aplicación puede ayudar a los equipos de TI a controlar el acceso a los sistemas que almacenan y procesan información de salud privada electrónica (ePHI) para respaldar el cumplimiento de HIPAA, segmentar transacciones de crédito y sistemas asociados a fin de reducir sustancialmente el alcance de sus esfuerzos de cumplimiento DSS de PCI y reducir el riesgo de acceso no autorizado a la información sobre los clientes para cumplir con el RGPD y otras normas de privacidad.

Por último, pero no menos importante, existen muchas formas en que EdgeConnect SD-WAN, junto con HPE Aruba Networking SSE, ayuda a aliviar la carga del cumplimiento de las normas relevantes de la industria, que incluyen: Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA), Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), Ley Sarbanes-Oxley (SOX), el RGPD de la Unión Europea y otros.

Por ejemplo, para garantizar el cumplimiento de las normativas sobre protección de datos, CASB y DLP ayudan a aplicar la protección de datos. Ambos supervisan los datos en riesgo y evitan que usuarios carguen datos confidenciales a las aplicaciones en la nube, ya sea de forma intencionada o no. CASB también ayuda a reducir la TI en la sombra y a identificar aplicaciones en la nube no autorizadas, detectar los datos confidenciales en tránsito y aplicar políticas de seguridad como la autenticación y el inicio de sesión único (SSO).

ZTNA protege los datos de las ciberamenazas ocultando los recursos privados en Internet y manteniendo a los usuarios fuera de la red. SWG protege contra el tráfico web malicioso, como el phishing o el ransomware, lo que reduce los riesgos de ciberseguridad y mejora el cumplimiento.

Más información en

HPE.com/sase

Visita HPE.com

Conclusión

Disponer plenamente de los múltiples y convincentes beneficios de una SD-WAN depende, en gran medida, de contar con una solución que tenga en cuenta los problemas de seguridad, los desafíos y las oportunidades que presenta dicho enfoque. En este sentido, las amplias capacidades de seguridad de la plataforma HPE Aruba Networking EdgeConnect SD-WAN van mucho más allá del nivel mínimo requerido de protección que ofrece el cifrado a nivel de transporte y la autenticación de mensajes.

HPE Aruba Networking EdgeConnect SD-WAN con firewall integrado de última generación proporciona características de seguridad avanzadas, como la protección IDS/IPS y DDoS, y permite a las organizaciones reemplazar los firewalls y los enrutadores heredados en las sucursales, reduciendo los requisitos de espacio de hardware, el coste y la complejidad.

Al combinar EdgeConnect SD-WAN, que presenta seguridad fiable del plano de gestión y datos, con el galardonado HPE Aruba Networking SSE, las organizaciones pueden diseñar una solución de SASE unificado y acelerar su proceso hacia el SASE a través de implementación sin fisuras y gestión simplificada. Para las organizaciones que prefieren adoptar SASE con su elección de servicios de seguridad, EdgeConnect SD-WAN admite la integración y la organización automatizadas con soluciones de seguridad de terceros suministradas en la nube.

Por último, con el uso cada vez mayor de dispositivos IoT, EdgeConnect complementa el SASE con una arquitectura de confianza cero que segmenta la red en función de la identidad, de modo que los usuarios y los dispositivos IoT solo puedan alcanzar destinos de la red coherentes con su rol en la empresa.

Iniciar chat ahora

a00126522ESE, rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com