HPE aruba networking

Principales tendencias en conectividad de red y seguridad para 2024

Seguridad ante todo, conectividad de red impulsada por IA para tu empresa

HPE GreenLake

Tras un año repleto de innovación, disrupción y condiciones macroeconómicas difíciles, los departamentos de TI siguen estando a la vanguardia de las ambiciones organizativas para acelerar la transformación empresarial. La inteligencia artificial generativa (GenAI), las iniciativas de sustentabilidad y otras prioridades estratégicas están a punto de pasar de la fase de adopción temprana a la aplicación práctica generalizada. Con una arquitectura empresarial cada vez más enfocada en los requisitos híbridos centrados en los datos, la seguridad desde el extremo hasta la nube se convierte en un principio básico de las redes empresariales.

“A medida que más organizaciones optan por estrategias de trabajo programáticas e híbridas, es más probable que los compradores elijan proveedores de firewalls que ofrezcan servicios de seguridad basados en la nube con estrategias de seguridad en la nube creíbles”.

– Gartner® Research, Capacidades críticas para los firewalls de red, Hils, Kaur y Lintemuth, mayo de 2023.

Principales tendencias para 2024

1. La muerte del firewall independiente

El auge de la mano de obra híbrida y el amplio despliegue de dispositivos IoT han erosionado irreversiblemente el perímetro de la red, y el firewall independiente está muriendo con él. Ya no se puede proteger un “interior” seguro de un “exterior” malo mediante un anillo de firewalls. Tratar de tapar las brechas de seguridad desplegando más firewalls dentro de una organización añade complejidad, crea margen para errores y ralentiza a las empresas que quieren avanzar con rapidez.

En consecuencia, el firewall de nueva generación se está convirtiendo rápidamente en el firewall de última generación. Por un lado, Security Service Edge (SSE) —con su capacidad para gestionar la seguridad de los usuarios que acceden a las aplicaciones desde cualquier lugar— está sustituyendo a los firewalls y proxies por una puerta de enlace web segura en la nube, un agente de seguridad de acceso a la nube y acceso a la red de confianza cero. Por otro lado, la seguridad del IoT requiere una segmentación local en el extremo de la red, que se consigue mediante servicios de firewall integrados directamente en los puntos de acceso, los conmutadores y las puertas de enlace de SD-WAN. En el centro de datos, los conmutadores TOR con funciones de seguridad L4-7 ofrecen una segmentación este-oeste mucho más rentable que los firewalls tradicionales de última generación situados al final del pasillo. En los próximos años, el mercado de firewalls de nueva generación seguirá disminuyendo a medida que estas nuevas capacidades integradas y basadas en la nube introduzcan una forma más sencilla de gestionar la conectividad segura.

Cómo podemos ayudar

- Implementación de servicios de seguridad para interacciones de usuario a aplicación con HPE Aruba Networking SSE.
- Integración de políticas basadas en funciones y reconocimiento y control de aplicaciones enriquecidas con HPE Aruba Networking Central.
- Introducción de tecnología de Security Services Edge (SSE) como superposición a la red de cualquier proveedor.
- Posibilidad de utilizar los productos y servicios existentes de HPE Aruba Networking para proteger la inversión.

Más información sobre SSE



“El 96 % de los clientes afirmaron que la seguridad y las redes trabajaron conjuntamente para implantar SASE”

– The Forrester Wave™ Soluciones de confianza cero, 3.º T, 2023 (Holmes y Kindness, 2023)

2. Los principios de confianza cero aceleran la alineación de los objetivos de seguridad y de red

La mayoría de las organizaciones —pero no todas— tienen equipos separados para gestionar la conectividad de red y la seguridad, y en muchos sentidos sus objetivos pueden estar reñidos. En 2024, las empresas líderes utilizarán los principios de confianza cero para alinear los intereses de los dos equipos y ofrecer mejores experiencias al usuario final y mejores resultados de negocio.

En una organización típica, el equipo de conectividad de red mantiene a las personas y los servicios conectados de forma fiable y en funcionamiento con un rendimiento previsiblemente bueno. Su trabajo consiste en facilitar la conexión a cualquier cosa y evitar la complejidad que puede provocar cortes, latencia o ralentizaciones. Por otro lado, la organización de seguridad se encarga de minimizar el riesgo y mantener el cumplimiento. Los usuarios pueden quedar atrapados en medio, ya que una implementación de seguridad demasiado entusiasta puede ralentizar o bloquear el acceso a las aplicaciones y los datos que necesitan, mientras que un equipo de seguridad o de redes poco estricto que pretenda complacer saltándose las medidas de seguridad puede abrir la puerta a la infiltración y al ransomware.

Las empresas líderes adoptarán arquitecturas de confianza cero, en las que el trabajo de la red no se define en términos de conectar algo a algo, sino más bien como una capa de aplicación de la política de seguridad. Para los usuarios que acceden a aplicaciones, la política de seguridad puede aplicarse en la nube, pero para muchos flujos de tráfico (en particular para los dispositivos IoT y sus servicios asociados), es más eficiente aplicar automáticamente la política de seguridad en dispositivos de acceso como puntos de acceso, conmutadores y enrutadores. Con el nivel adecuado de visibilidad compartida, automatización y delimitación clara de las políticas y su aplicación, los equipos de redes y seguridad tendrán objetivos alineados y ofrecerán una mejor experiencia.

Cómo podemos ayudar

- Utilización de un único punto de visibilidad y control con acceso personalizable tanto para los equipos de red como para los de seguridad.
- Implementación de una red unificada y un marco de políticas de seguridad con HPE Aruba Networking Central.
- Perfecta integración de las funciones de seguridad en la nube con las herramientas de gestión de red existentes.

Empieza con una red que prioriza la seguridad e impulsada por IA

“Para 2027, la implementación de DEM aumentará del 60 % al 90 %, ya que las empresas utilizarán la monitorización sintética y real de usuarios para mejorar el recorrido del usuario y comprender mejor las interacciones de los usuarios de aplicaciones y servicios SaaS”.

– Gartner®, Guía de mercado para Supervisión de la experiencia digital, Bangera, Siegfried y Byrne, noviembre de 2023.

3. Medir la experiencia del usuario final se convierte en una obligación para impulsar la excelencia operativa

Métricas comunes de usuario final

- Salud de la red basada en la ubicación (sitio A frente a sitio B)
- Rendimiento de los servicios (Wi-Fi, DHCP, DNS)
- Estado de las aplicaciones internas (VoIP, Workday)
- Estado de las aplicaciones externas (Dropbox, Teams, WhatsApp)

Para ofrecer lo que esperan empleados y clientes, las organizaciones de TI tendrán que cambiar a objetivos de nivel de servicio (SLO) y acuerdos de nivel de servicio (SLA) basados en la experiencia medida del usuario. Garantizar una gran experiencia de usuario significa que las aplicaciones deben funcionar bien y, si no lo hacen, la resolución del problema debe ser rápida.

Para hacer frente a esta situación, las organizaciones desplegarán ampliamente herramientas de gestión de la experiencia digital (DEM) que midan la experiencia real de los usuarios finales y realicen sondeos sintéticos para garantizar la preparación de la infraestructura incluso cuando los usuarios no estén presentes. Lo más probable es que las organizaciones deseen una combinación de mediciones recopiladas por agentes de punto final (como un agente SSE) y mediciones recopiladas por sensores de hardware dedicados, especialmente cuando se supervisa el rendimiento de wifi. En el mejor de los casos, estas mismas mediciones alimentan los AIOps automatizados, que son capaces de aprender y aplicar las mejores prácticas, clasificar rápidamente los problemas y solucionarlos automáticamente.

Cómo podemos ayudar

- Automatización y mejora de las experiencias de usuario y cliente aprovechando plataformas y herramientas como HPE Aruba Networking Central y User Experience Insight.
- Personalización del acceso a la red y la seguridad para quienes más lo necesitan con acceso basado en funciones y segmentación dinámica orquestada a través de NetConductor.
- Supervisión de la experiencia digital (DEM) para probar y solucionar problemas de rendimiento de aplicaciones y redes desde la perspectiva de los usuarios finales con HPE Aruba Networking User Experience Insight.

Descubre cómo actualizar la experiencia de usuario



“HPE Aruba Networking fue pionera en la entrega de Wi-Fi 6E y lidera el sector en envíos totales de puntos de acceso Wi-Fi 6E para empresas”.

– Siân Morgan, analista de WLAN Dell’Oro Group, diciembre de 2023

4. La adopción de Wi-Fi de 6 GHz se dispara y seguirá siendo la principal característica de Wi-Fi 7

Las barreras que ralentizan el despliegue de Wi-Fi en el espectro de 6 GHz desaparecerán en la mayoría de las zonas geográficas y su adopción empezará a dispararse.

Hace un par de años, la norma Wi-Fi 6E introdujo la compatibilidad con la banda de 6 GHz, duplicando con creces la capacidad Wi-Fi y permitiendo más usuarios y velocidades más rápidas. En algunos segmentos se ha adoptado rápidamente, pero otros han sido más cautos. En 2024 se habrán resuelto los últimos obstáculos a la adopción generalizada.

En primer lugar, el uso de la banda de 6 GHz —sobre todo en exteriores— está sujeto a la aprobación de las autoridades gubernamentales. Aunque algunos países, como Estados Unidos, se han apresurado a abrir el espectro para Wi-Fi, otros han sido más lentos. Afortunadamente, se ha avanzado mucho en este terreno, y en 2024 la mayoría de las empresas dispondrán de acceso al espectro de 6 GHz en la mayor parte del mundo.

En segundo lugar, algunas empresas se han mostrado reticentes a adoptar Wi-Fi 6E cuando Wi-Fi 7 está a la vuelta de la esquina. Ahora que Wi-Fi 7 ha sido ratificada, no hay duda de que Wi-Fi 6E y Wi-Fi 7 serán interoperables. Por eso, con los dispositivos y puntos de acceso 6E que se están comercializando en grandes cantidades, las implementaciones de Wi-Fi 6 GHz pueden avanzar a toda máquina.

Por último, la adopción está condicionada por la compatibilidad tanto de los puntos de acceso como de los dispositivos cliente. Estamos presenciando una avalancha de nuevos dispositivos compatibles con Wi-Fi 6E y la generalización de los puntos de acceso 6E. Además, hay más dispositivos Wi-Fi 7 en el horizonte que pueden utilizar la banda de 6 GHz para ofrecer una mejor experiencia de usuario con puntos de acceso Wi-Fi 6E o Wi-Fi 7.

La combinación de estos avances pronostica una gran utilización del espectro de 6 GHz en 2024 y, con él, transferencias más rápidas y una mejor experiencia de usuario.

Cómo podemos ayudar

- Disponibilidad de un portfolio para interiores y remoto de puntos de acceso HPE Aruba Networking Wi-Fi 6E para desbloquear el acceso al espectro de 6 GHz.
- Integración de una variedad de aplicaciones IoT populares a través de un panel de operaciones IoT para ampliar el papel de la infraestructura AP más allá de la conectividad interna para apoyar los despliegues de superposición IoT.
- Desarrollo de un receptor GPS pionero en el sector integrado en los puntos de acceso Wi-Fi 6E con el fin de proporcionar una red preparada para la localización que admita casos de uso emergentes como la cartografía automática de puntos de acceso y la navegación giro a giro.

Descubre las ventajas de 6 GHz y Wi-Fi 6E

“En 2026, la tecnología de inteligencia artificial generativa (GenAI) representará el 20 % de la configuración inicial de la red, lo que supone un aumento desde casi cero en 2023”.

– Gartner®, Research Hoja de ruta estratégica para las redes empresariales. Brown, Munch, Leibovitz y Lerner, octubre de 2023.

5. La inteligencia artificial liberará a los administradores de TI

A veces se cita que no perderás tu trabajo por la inteligencia artificial, sino que lo perderás por alguien que esté utilizando la inteligencia artificial de forma eficaz. Esto es cada vez más preciso para el administrador de TI.

La creciente carga que supone implantar nuevas tecnologías y mantener la ciberseguridad con número de empleados fijo o cada vez más reducido se traduce en que cada administrador debe ocuparse de más cosas. Afortunadamente, la inteligencia artificial y la automatización avanzan con rapidez, lo que permite pasar de la gestión y configuración de dispositivos individuales a la definición de políticas para todo el parque y su aplicación automática y coherente. La inteligencia artificial también es capaz de rastrear enormes volúmenes de datos para identificar anomalías y recomendar (e incluso aplicar) soluciones. Está demostrado que la inteligencia artificial es tan buena como su conjunto de datos, y la clave está en disponer de conjuntos de datos más grandes y de mayor calidad. Los principales proveedores obtendrán información sobre inteligencia artificial a partir de lagos de datos que representan millones de dispositivos gestionados y cientos de millones de puntos finales. Por último, los grandes modelos de lenguaje (LLM) están turboalimentando las interfaces de lenguaje natural existentes y ofreciendo a los administradores una forma más cómoda de obtener la información que necesitan.

La conclusión es que las organizaciones deben asegurarse de que están proporcionando a sus equipos de TI las capacidades de inteligencia artificial que los administradores necesitan para seguir siendo competitivos.

Cómo podemos ayudar

- Acceso a uno de los mayores lagos de datos en red para dotar a tu red de información, recomendaciones y acciones sin precedentes que aumenten el rendimiento y la estabilidad.
- Utilización de redes impulsadas por inteligencia artificial y centradas en la seguridad para simplificar las operaciones del final del proceso, desde la búsqueda hasta las actualizaciones de firmware y otras funciones de mantenimiento y asistencia.
- Implementación de un marco unificado para la creación coherente de políticas de red y seguridad.
- Perfecta integración de las funciones de seguridad en la nube con las herramientas de gestión de red que ya tienes.

Desmitificar las redes impulsadas por inteligencia artificial

Lo que se necesita es un enfoque de la red que dé prioridad a la seguridad y esté impulsado por IA

Independientemente de la estrategia que tengas en marcha para 2024, las implicaciones para la seguridad de la era desde el extremo hasta la nube son un reto común para cualquier organización de TI. Y siempre que se plantean implementaciones de redes seguras, resulta cada vez más evidente para las organizaciones que la experiencia del usuario sigue siendo un factor crítico. ¿Priorizas la seguridad de redes? Descubre más sobre lo que vendrá en 2024.

Más información

Mira el webinario bajo demanda sobre las predicciones principales en conectividad de red y seguridad para 2024

Visita **ArubaNetworks.com**

Toma la decisión de compra correcta. Contacta con nuestros especialistas en preventa.

Comunícate con nosotros

BR_TopNetworkingAndSecurityTrends2024_CT_122023 a00136590ese

Hewlett Packard Enterprise