HPE aruba networking

Reemplaza por completo la VPN con ZTNA de HPE Aruba Networking

El espacio de trabajo moderno requiere un nuevo enfoque para el acceso remoto

El término “acceso Zero Trust a la red” (ZTNA), que fue creado en abril de 2019 por Gartner®, representa un conjunto de tecnologías nuevas diseñadas para acceder de forma segura a aplicaciones privadas. También conocidas como “perímetro definido por software” (SDP), las tecnologías de ZTNA usan políticas de acceso granular para conectar a los usuarios autorizados a aplicaciones específicas sin necesitar acceso a la red corporativa. Además, establecen una segmentación a nivel de aplicaciones con menos privilegios como reemplazo de la segmentación de la red, sin exponer la ubicación de la aplicación a la Internet pública.

Acelerar la adopción de un espacio de trabajo moderno significa despedirte de la VPN

Impulsadas por la necesidad de garantizar la continuidad de los negocios durante la pandemia y superar a la competencia, todas las organizaciones están en una carrera para adoptar las soluciones digitales adecuadas y así mantener a sus usuarios felices, motivados y productivos. Ya han adoptado nuevas aplicaciones de colaboración, como Zoom y Microsoft Teams, duplicaron sus servicios de nube pública escalables e implementaron entornos de trabajo más flexibles. Con esta modernización en marcha, muchos líderes de TI están considerando mejores formas de proporcionar acceso remoto a aplicaciones privadas para sus empleados y terceros, y alejarse de la red privada virtual (VPN).

Antes de la pandemia, tan solo el 30 % de los empleados trabajaban desde casa. En la actualidad, el 77 % de las empresas tienen planificado implementar el trabajo híbrido para conservar a los mejores empleados que ahora prefieren trabajar desde casa y acceder a nuevos grupos de talentos menos costosos. Sin embargo, las VPN tienden a entorpecer la productividad y frustrar a los empleados.

Socios, proveedores, vendedores y clientes también desempeñan un papel clave a la hora de generar ingresos para el negocio. Uno de cada tres usuarios que requieren acceso a recursos son externos y, muy raramente, permiten que se implemente una VPN en sus dispositivos.

Como puedes imaginar, este lugar de trabajo moderno también tiene un costo. Se estima que el gasto en TI alcance los USD 2 billones en 2022, gran parte del cual se destinará a modernizar la infraestructura de TI y hacer que admita este nuevo entorno de trabajo. Sin embargo, esto solo representa un aumento del 4 % en los presupuestos promedio de TI, por lo que seguir gastando mucho en tecnologías heredadas de acceso remoto no es una opción.

HPE GreenLake

Además de permitir el trabajo desde cualquier lugar, asegurar el acceso de terceros y modernizar la infraestructura, las empresas deben proteger sus recursos y su reputación. Con cada usuario, dispositivo y aplicación que se conecta a Internet, la superficie de posible ataque aumenta exponencialmente y colocar a los usuarios en la red corporativa a través de una VPN se ha convertido en el mayor riesgo de todos.

Para admitir este nuevo entorno, el 60 % de las empresas reemplazará su VPN con ZTNA para 2023.

La diferencia entre VPN y ZTNA de HPE Aruba Networking

VPN de acceso remoto

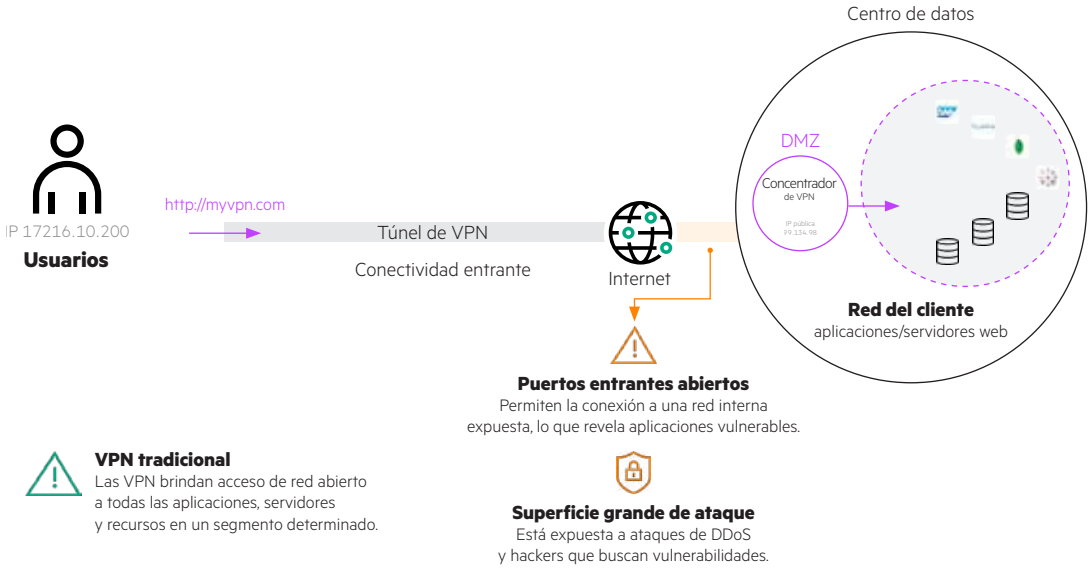

Figura 1. VPN tradicional

Durante los últimos 20 años, la VPN ha permitido a empleados remotos y terceros acceder a la red y los recursos privados que se ejecutan en ella. Los concentradores de VPN escuchan las llamadas entrantes de los clientes VPN y sirven como baliza para los clientes, lo que brinda un punto de entrada a la red corporativa. Para minimizar el riesgo de esta arquitectura defectuosa, las organizaciones requieren firewalls, balanceadores de carga, prevención de DDoS y concentradores de VPN para conectar a los usuarios remotos con aplicaciones privadas, lo que genera mayor complejidad, costos y riesgos. En los últimos años, se han aprovechado los servicios de VPN populares de empresas reconocidas gracias a esta arquitectura.

ZTNA de HPE Aruba Networking

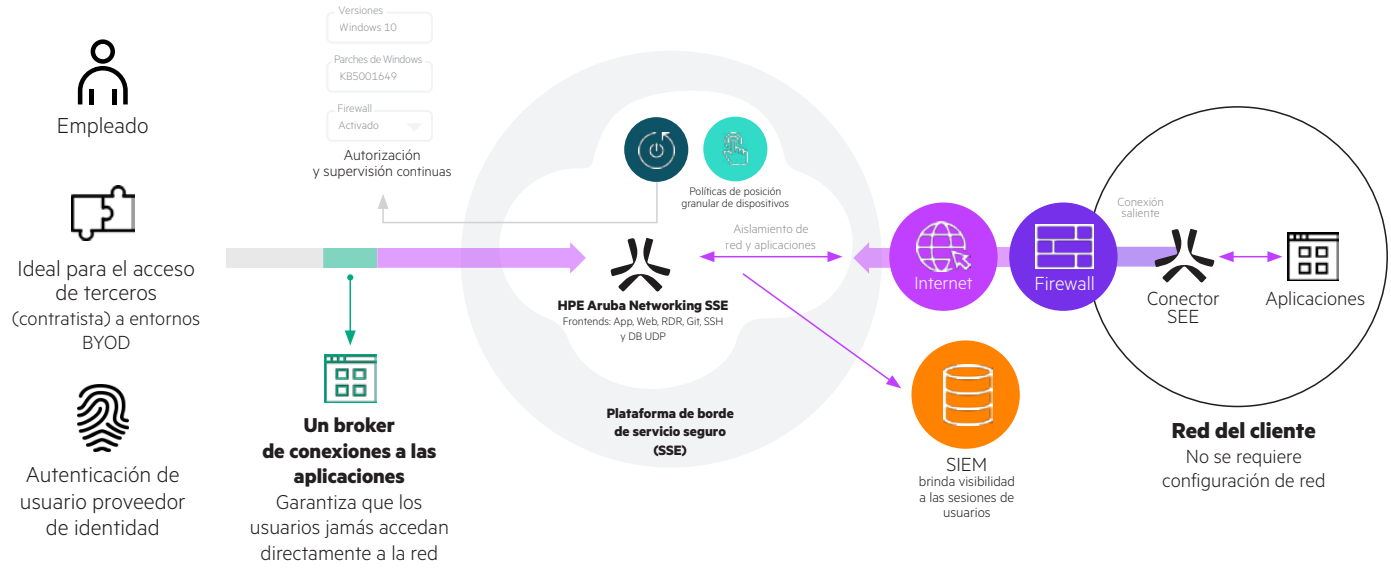

Figura 2. ZTNA de HPE Aruba Networking

Con más de 500 ubicaciones perimetrales en todo el mundo, la plataforma SSE de HPE Aruba Networking es una de las soluciones Zero Trust más confiables, disponibles y escalables, que se diseñó para lograr la conectividad segura a los recursos empresariales.

El servicio ZTNA de HPE Aruba Networking brinda a los usuarios acceso rápido, seguro y confiable a recursos privados. Esto es lo que sucede en tiempo real cuando alguien se conecta a través de la funcionalidad sin cliente.

1. El usuario solicita acceso a una aplicación interna, como hr-app-tenant.axisapps.io.
2. Si el usuario inicia sesión activamente en una aplicación administrada por HPE Aruba Networking, se lo redirige al proveedor de identidad de la aplicación asociada.
3. ZTNA de HPE Aruba Networking verifica que la solicitud de acceso del usuario cumpla con las políticas definidas por el cliente.
4. El usuario cuenta con autorización continua en función de su identidad, su grupo y otros criterios contextuales. NOTA: La plataforma SSE de HPE Aruba Networking puede inspeccionar el tráfico activamente y cierra la sesión si ocurre un evento de seguridad.
5. ZTNA de HPE Aruba Networking verifica si existe una conexión actual a la aplicación para una posible reutilización.
6. Cuando hay una conexión nueva, el conector de SSE más cercano identifica la aplicación autorizada y responde con una conexión saliente a la nube SSE de HPE Aruba Networking mediante un puerto especificado.
7. La nube SSE de HPE Aruba Networking hace que la conexión nueva regrese al front-end dedicado.

8. El front-end web establece una conexión a la aplicación.
9. Luego, el acceso a la aplicación interna solicitada se extiende al usuario a través de una conectividad basada en navegador.

El ZTNA de HPE Aruba Networking garantiza que el acceso a la aplicación esté garantizado sin requerir acceso a la red corporativa. Esta disociación reduce los riesgos de seguridad de la red, como amenazas internas o propagación de ransomware, ya que minimiza el movimiento lateral a través de la segmentación a nivel de aplicación.

A diferencia de un concentrador de VPN, el ZTNA de HPE Aruba Networking usa una arquitectura iniciada por servicio para aprovechar lo que llamamos conexiones únicamente salientes. Este tipo de conexión garantiza que la infraestructura de red y las aplicaciones empresariales estén ocultas de Internet y no puedan localizarse ni verificarse porque no escuchan ningún ping entrante. Se encuentran detrás del conector de SSE, que se comunica exclusivamente con la plataforma SSE de HPE Aruba Networking. Piensa en la plataforma SSE como el intermediario entre la entidad (usuario o aplicación) y la aplicación.

HPE Aruba Networking trata a Internet como la nueva red corporativa y garantiza que los microtúneles cifrados dinámicos basados en Internet reemplacen las conexiones de red tradicionales como VPN siempre en funcionamiento, MPLS y conexiones dedicadas de sitio a sitio para la nube pública. Esto reduce los costos y libera tiempo para que los equipos de red y seguridad se concentren en proyectos más estratégicos en lugar de administrar dispositivos costosos, actualizar versiones, implementar hardware y planificar renovaciones.

Tabla 1.

	Concentrador	vs.	ZTNA de HPE Aruba Networking
Experiencia del usuario Los usuarios esperan que acceder a aplicaciones privadas sea como acceder a aplicaciones SaaS.	**Mala experiencia para los usuarios** Las VPN obligan a los usuarios a implementar un cliente en su dispositivo y volver a conectarse a la red corporativa cada vez que cambian de ubicación. Debido a que las puertas de enlace de las VPN tienen puntos o presencia limitados, los flujos subóptimos añaden latencia, lo que reduce la productividad del usuario.	vs.	**Experiencia de usuario sin problemas** SSE de HPE Aruba Networking ofrece métodos de acceso con y sin cliente. Una única política Zero Trust sigue al usuario y garantiza que solo tenga acceso a los recursos específicos que necesita. La experiencia del usuario siempre en funcionamiento permite a los clientes simplemente trabajar y no preocuparse por volver a conectarse a una red. Los servicios de ZTNA proporcionados en la nube ofrecen PoP globales que extienden la conectividad de forma segura a todas las ubicaciones de los usuarios, a través de Internet.
Seguridad La empresa debe proteger los datos de los ciberataques, a toda costa.	**Más riesgo** Los criminales cibernéticos atacan activamente tecnologías de red privada virtual (VPN) y virtualización de escritorio (VDI) con ataques basados en Internet. Estos métodos de acceso centrados en la red colocan a los usuarios en la red corporativa y exponen la infraestructura a la Internet abierta. Con un simple escaneo de puertos, un adversario puede atacar infraestructuras con una posición desactualizada, robar credenciales y acceder a la red corporativa como si fuera un usuario legítimo.	vs.	**Cero superficie de ataque** SSE de HPE Aruba Networking se diseñó para nunca confiar inherentemente en nada. Únicamente después de que se lleven a cabo una inspección y validación adecuadas, el servicio de ZTNA conecta a los usuarios con recursos específicos. Estas conexiones individuales son de salida únicamente desde el recurso hasta el usuario autorizado, sin colocar a los usuarios en la red corporativa. Este diseño de acceso con privilegios mínimos garantiza que no se puedan propagar los usuarios y las amenazas lateralmente por el entorno. HPE Aruba Networking también protege los recursos, ya que los coloca detrás del servicio de ZTNA y los hace invisibles para Internet. Luego, los derechos de acceso se adaptan automáticamente en función de los cambios en el contexto, como la relación con la empresa, la posición del dispositivo, la ubicación, etc.
Facilidad de uso A medida que la empresa crece y continua con la adopción de la nube, la simpleza y el escalamiento se vuelven prioritarios.	**Más complejidad y costos** Escalar los servicios de VPN requiere agregar capacidad a toda la puerta de enlace entrante, incluida la compra, implementación y administración de más dispositivos. Muchas veces, son necesarios equilibradores de carga, firewalls externos e internos, servicios DDos y otros dispositivos. Este aumento en la cantidad de dispositivos es un desafío de administrar y aumenta los costos cuando se consideran los gastos de capital y operativos en el mantenimiento de toda la puerta de enlace.	vs.	**Fáciles de administrar** Los servicios que se ofrecen en la nube no requieren dispositivos y son mantenidos por el propio proveedor. Los servicios se diseñaron para brindar confiabilidad, disponibilidad y escalabilidad a medida que aumentan las demandas de tráfico. Garantizan la experiencia más rápida posible sin interrumpir el negocio. Las integraciones de API con servicios clave del ecosistema, como IDP, seguridad de terminales y SIEM, ayudan a acelerar el proceso de implementación. Estos servicios se cobran por usuario y por año, por lo que los costos de capacidad y electrodomésticos ya no son un factor. El departamento de TI puede emplear menos tiempo y gastar menos dinero en servicios de conectividad y, en cambio, centrarse en proyectos estratégicos que son clave para sus iniciativas para el lugar de trabajo moderno.

Capacidades únicas de ZTNA de HPE Aruba Networking

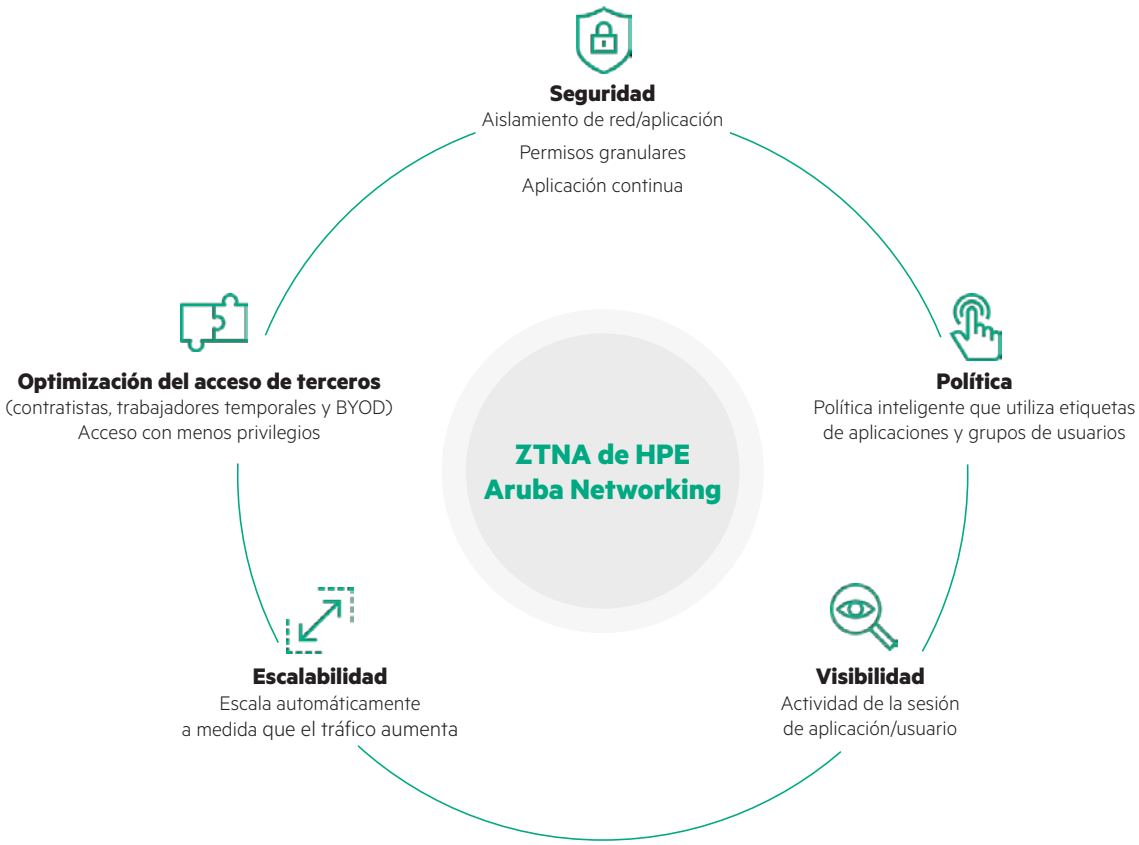

Figura 3. Diferenciadores únicos de ZTNA

Permite la segmentación granular a nivel de aplicación, sin segmentación de red
Reduce la posible superficie de ataque permitiendo solo el acceso a recursos específicos. Esto limita el movimiento lateral a través de la red, elimina la necesidad de complejos esfuerzos de segmentación de la red y reduce la posible superficie de ataque del negocio.

Admite acceso fluido a aplicaciones desde cualquier dispositivo con o sin cliente
Permite que los empleados remotos autorizados y terceros accedan de forma segura a los recursos empresariales desde el dispositivo de tu elección de la manera más fluida posible. El método sin cliente también admite sesiones RDP basadas en navegador, lo que reduce la necesidad de VDI.

Adapta el acceso a partir de controles contextuales basados en API
Adapta los derechos de acceso automáticamente en función de los cambios en criterios clave, incluida la ubicación del usuario, su identidad y la postura del dispositivo. Esta evaluación de riesgos adaptativa continua ayuda a proteger mejor los datos comerciales.

Simplifica la seguridad con una arquitectura 100 % entregada en la nube en 500 extremos globales
El departamento de TI puede dejar de dedicar tiempo a la administración de dispositivos de VPN. Con SSE de HPE Aruba Networking, se administra cada conexión en la ubicación de extremo de SSE más adecuada para proporcionar la conexión, incluso en caso de desastre. El departamento de TI puede estar seguro de que podrá minimizar las interrupciones y maximizar el tiempo de actividad.

Reemplaza la tecnología de VPN heredada
El ZTNA de HPE Aruba Networking tiene el soporte más amplio de aplicaciones privadas del mercado. El servicio de ZTNA no solo admite todo el tráfico TCP y UDP, incluidos VoIP, flujos de trabajo del mismo nivel y de servidor a cliente (que son difíciles para la mayoría de los proveedores de ZTNA), sino también todas las aplicaciones web modernas, como SSH, RDP, Git, DB, etc. Ahora, los equipos de TI pueden reemplazar su VPN por completo para siempre.

Inspecciona todo el tráfico que fluye hacia y desde recursos privados
Por primera vez, obtén profunda visibilidad de a qué acceden los empleados y terceros. Revisa la actividad del usuario, las descargas de archivos, los registros de movimientos y los comandos utilizados durante una sesión y bloquea cualquier acción maliciosa.

Comencemos

Obtén más información sobre el ZTNA de HPE Aruba Networking y cómo puedes utilizarlo como alternativa a tu VPN. Para ello, conéctate con uno de nuestros expertos en SSE. O experimenta tú mismo el poder de HPE Aruba Networking con nuestra prueba gratuita de SSE.

arubanetworks.com

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

Comunícate con nosotros

Visita **arubanetworks.com**

SB_VPNWithHPEArubaNetworkingZTNA_DTA_013024 a00136658ese

Hewlett Packard Enterprise