HPE aruba networking

Informe técnico de negocios

La guía del arquitecto para el reemplazo de la VPN

HPE GreenLake

Vieja tecnología en un mundo nuevo

En los últimos años, el entorno laboral ha cambiado drásticamente. El panorama ya estaba empezando a cambiar con la invención y el crecimiento de la nube, pero la pandemia de COVID-19 aumentó drásticamente el trabajo remoto.

Esto cambió nuestra forma de pensar sobre nuestros diseños arquitectónicos. Nuestros usuarios ya no están protegidos por un muro perimetral. La fuerza laboral está en todas partes. Y no solo eso, sino que las aplicaciones a las que necesitan acceder diariamente ahora se distribuyen entre ubicaciones SaaS, IaaS y en las instalaciones.

En la actualidad, los equipos deben admitir una conectividad segura con aplicaciones internas y externas para una base de usuarios que pueda ubicarse en cualquier lugar. Los arquitectos deben admitir el acceso seguro a todas las aplicaciones heredadas, además de considerar cómo será el acceso a las aplicaciones en el futuro.

El nuevo mundo de la nube y la movilidad cambia la forma en que nos conectamos y también cómo protegemos esa conectividad. Y las soluciones heredadas, como las VPN tradicionales, no abordan las necesidades actuales de manera adecuada. Muchas organizaciones están reemplazando su VPN con una tecnología moderna que se encuentra en muchas plataformas de extremo del servicio de seguridad (SSE) conocidas como acceso Zero Trust de red (ZTNA).

¿Qué es el SSE y dónde encaja el ZTNA?

El SSE es parte del marco más amplio del extremo de servicio de acceso seguro (SASE), que Gartner® introdujo en 2019. Cuando el trabajo remoto se incrementó exponencialmente durante la pandemia en 2021, Gartner® presentó el SSE.

El marco de SSE es una colección de capacidades de seguridad integradas y centradas en la nube que facilitan el acceso seguro a aplicaciones privadas, aplicaciones de software como servicio (SaaS) e Internet con las siguientes tecnologías: Acceso Zero Trust de red (ZTNA), agente de seguridad de acceso a la nube (CASB) y puerta de enlace a la web segura (SWG).

- **ZTNA** brinda acceso Zero Trust a aplicaciones privadas.
- **CASB** protege el acceso a todas las aplicaciones basadas en SaaS.
- **SWG** garantiza que todo el acceso a Internet sea seguro.

Una plataforma de SSE debe proporcionar una única plataforma unificada para todo el acceso a las aplicaciones y, al mismo tiempo, desacoplar el acceso a las aplicaciones de la red corporativa. Debería servir como una superposición sobre la red existente, lo que permite al departamento de TI modernizar y simplificar la conectividad mientras fortalece la seguridad, sin tener que realizar complejos cambios en la arquitectura de la red.

Dado que una plataforma de SSE consta de varias tecnologías centrales que se pueden implementar de forma independiente, ¿por dónde empiezas? ¿Cómo deberías adoptar el SSE? La respuesta a esta pregunta es la misma que para cualquier proyecto o iniciativa de seguridad: las áreas de mayor riesgo. En el nuevo mundo de aplicaciones y usuarios distribuidos, es necesario empezar por el reemplazo de tu tecnología de VPN y la protección del acceso a tus aplicaciones privadas con ZTNA.

“Para 2025, al menos el 70 % de las nuevas implementaciones de acceso remoto serán atendidas predominantemente por ZTNA en lugar de servicios de VPN”.

— **Gartner® Forecast Analysis:** Information Security and Risk Management, mundial, septiembre de 2022

ZTNA como una alternativa a VPN

Mientras los equipos navegan por las complejidades de proteger entornos de trabajo remotos, el ZTNA ofrece una alternativa convincente a las VPN tradicionales. El ZTNA aborda muchas de las limitaciones de las VPN tradicionales y ofrece a las empresas modernas los siguientes beneficios.

Seguridad

- **Desafío de las VPN:** las VPN exponen las redes a amenazas como malware, ransomware y ataques de DDoS, ya que exponen las IP de la red y permiten a los atacantes acceder a toda la red.
- **Solución de ZTNA:** el ZTNA minimiza el riesgo de ataques basados en Internet, ya que oculta recursos privados de Internet. Las conexiones que son salientes únicamente hacen que tu red y tus aplicaciones sean invisibles y no se puedan rastrear. Además, los usuarios nunca reciben acceso a la red. El acceso se otorga en función de la identidad dinámica del usuario, el dispositivo y el contexto de los datos, lo que evita el movimiento lateral no autorizado de manera efectiva.

Escalamiento y flexibilidad

- **Desafío de las VPN:** debido a que las VPN son dispositivos físicos, escalar la infraestructura puede ser muy complejo y representar un desafío. A medida que crece la fuerza laboral móvil, muchas organizaciones deben escalar su inversión en infraestructura de VPN significativamente para admitir más conexiones y mayor tráfico.
- **Solución de ZTNA:** la arquitectura en la nube de ZTNA facilita la escalabilidad y administración centralizada del acceso remoto. Las políticas de Zero Trust se pueden adaptar a los niveles de usuario y aplicación, y se pueden aplicar globalmente en segundos.

Productividad

- **Desafío de las VPN:** debido a que se redirige el tráfico a través de la red corporativa, las VPN pueden obstaculizar las velocidades de conexión y el rendimiento de las aplicaciones, lo que genera pérdida de productividad y mayores cargas de trabajo para que el departamento de TI administre el acceso.
- **Solución de ZTNA:** el ZTNA optimiza la experiencia del usuario, ya que acerca el acceso lo más posible al usuario mediante ubicaciones globales en el extremo de la nube, que enrutan el tráfico automáticamente por la ruta de acceso más rápida. El ZTNA elimina las ralentizaciones, las desconexiones y los problemas de inicio de sesión relacionados con las VPN mientras se integra perfectamente con sistemas de inicio de sesión únicos (SSO) y de administración de identidades.

Costo

- **Desafío de las VPN:** las VPN generan altos costos debido a que se requiere hardware local costoso y personal dedicado para la supervisión y la administración, sin mencionar la pila de seguridad entrante extendida para minimizar el riesgo de ataques relacionados con las VPN.
- **Solución de ZTNA:** el ZTNA elimina los costos asociados con el hardware tradicional de las VPN, la protección de DDoS y los firewalls, y simplifica la supervisión, ya que libera recursos para otros proyectos críticos.

Comienza tu proceso de SSE con ZTNA

El ZTNA evolucionó más allá de los límites del mero acceso remoto; se convirtió en un concepto fundamental para el acceso a las aplicaciones en su conjunto. No es solo una puerta de entrada. Es un enfoque transformador que allana el camino hacia una visión más amplia e integral. El ZTNA es un servicio único que se presta en la nube y que aborda todos tus requisitos de acceso.

Elige por dónde empezar

Al implementar el ZTNA, es fundamental identificar la fuerza que determina la decisión. ¿El objetivo principal es mejorar la seguridad, optimizar la experiencia del usuario o ahorrar dinero? Comprender la motivación subyacente te guiará a la hora de seleccionar el punto de partida más adecuado para tu traslado al ZTNA.

"Para fines de 2024, el cambio en la naturaleza del trabajo aumentará el mercado total de trabajadores remotos al 60 % de todos los empleados, frente al 52 % en 2020".

— **Gartner® Forecast Analysis:** Information Security and Risk Management, mundial, septiembre de 2022

Si la **seguridad** es tu prioridad, identifica el área con el mayor riesgo y concéntrate en soluciones de acceso seguro para grupos específicos como usuarios o empleados externos. Si el objetivo es **mejorar la experiencia del usuario**, identifica los grupos de usuarios con acceso deficiente (como ejecutivos o trabajadores remotos) y mejora su acceso a aplicaciones privadas. Si el objetivo es **ahorrar costos**, analiza qué tecnologías heredadas son las más costosas (como las VPN) y considera cómo el ZTNA puede reemplazarlas.

Casos de uso de ZTNA

Decidir el caso de uso inicial puede ser una tarea desalentadora. Para ayudarte, hemos identificado tres casos de uso predominantes. Las siguientes secciones describen estos escenarios y su perfecta integración de ZTNA.

Acceso remoto e híbrido seguro para empleados

En el mundo móvil, las VPN tradicionales luchan por mantener el ritmo. Si bien las VPN alguna vez fueron fundamentales para facilitar el acceso remoto a los empleados, ahora plantean importantes riesgos de seguridad en términos de conectividad. Dado que la fuerza laboral actual opera desde casa, la oficina o cualquier espacio de transición, es crucial mantener un enfoque de acceso Zero Trust coherente y discreto.

El siguiente diagrama muestra cómo la tecnología del ZTNA reemplaza los marcos de VPN obsoletos que tradicionalmente se encontraban en centros de datos. El ZTNA actúa como intermediario entre el usuario y la aplicación, y otorga acceso solo a usuarios autorizados y aplicaciones autorizadas, independientemente de su ubicación, ya sea en las instalaciones o la nube pública.

Esto se logra a través de un conector de aplicación liviano ubicado dentro del entorno de la aplicación, que solo permite el acceso si cumple con los requisitos contextuales. Una vez que se cumplen los criterios, se establece una conexión saliente, lo que garantiza que los usuarios no sean colocados directamente en la red y que solo se les otorgue acceso a la aplicación autorizada designada.

Además, la transición del acceso remoto al acceso a la oficina no afecta la experiencia del usuario, ya que el ZTNA funciona sin problemas en segundo plano. Incluso protege la red, ya que impide el acceso de dispositivos potencialmente comprometidos mientras se encuentren en las instalaciones de la empresa.

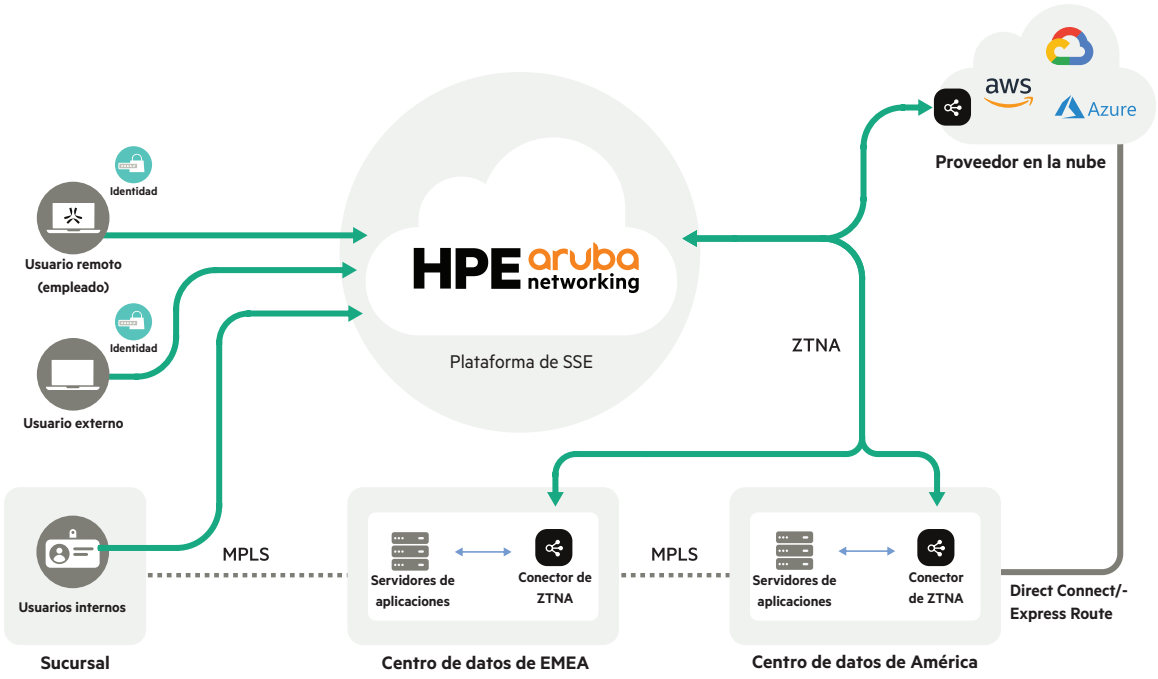

Figura 1. Acceso remoto e híbrido seguro

Acceso seguro de terceros y BYOD

Tradicionalmente, el acceso de terceros dependía de la tecnología de VPN de acceso remoto. Los usuarios tenían que instalar un cliente, esperar a que un administrador actualizara las políticas de ACL y FW manualmente y, luego, intentar conectarse. Las conexiones exitosas otorgaban acceso a activos confidenciales, exponiendo la red a muchos riesgos. La VPN extiende el acceso a la red a usuarios que no son de confianza en dispositivos que no son de confianza desde redes que no son de confianza y, una vez que un usuario externo está en la red, puede acceder libremente a toda la red con frecuencia.

El ZTNA supera los riesgos de este enfoque con sus conexiones exclusivamente salientes. El ZTNA oculta la infraestructura de red, las aplicaciones empresariales y los portales de terceros de Internet, protegiéndolos contra el descubrimiento de ubicaciones y ataques DDoS, ya que no pueden las sondas entrantes no pueden encontrarlos. Las aplicaciones privadas y los portales de terceros se esconden de forma segura detrás de un conector de aplicaciones, que solo permite el tráfico a través de la nube de ZTNA.

El ZTNA también permite la aplicación de políticas de acceso con privilegios mínimos, incluso para usuarios externos de BYOD. Las integraciones perfectas con todas las principales soluciones de SSO facilitan una experiencia de acceso fluida a aplicaciones privadas a través de un navegador web simple, sin comprometer la seguridad.

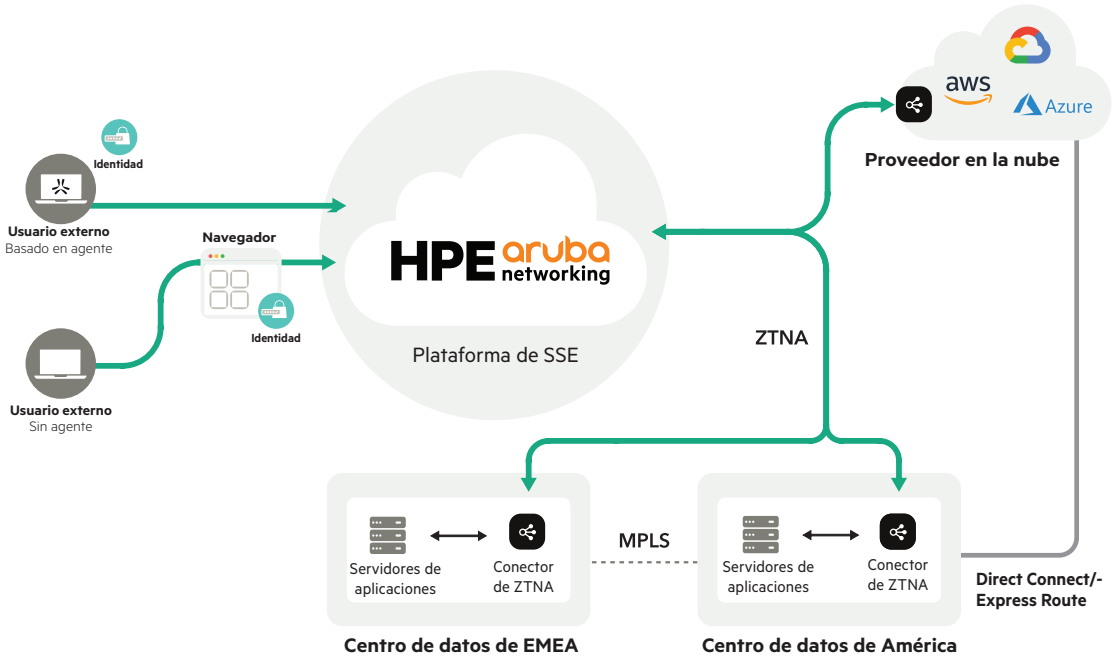

Figura 2. Acceso seguro de terceros y BYOD

Aceleración de fusiones y adquisiciones

Las fusiones y adquisiciones presentan desafíos complejos, pero el ZTNA ofrece una solución optimizada para acceder a aplicaciones críticas de inmediato desde el primer día. Este enfoque elimina la necesidad de las VPN, integración de red o cambios de infraestructura. La estrategia depende de una lista predefinida de aplicaciones esenciales, como sistemas de recursos humanos, sistemas de planificación de recursos empresariales y otras herramientas basadas en la web, accesibles a través de la plataforma de SSE.

El ZTNA incluye una estrategia de identidad sólida, que garantiza que los usuarios puedan autenticarse y acceder a las aplicaciones de forma segura, incluso antes de la consolidación de directorios, usuarios y grupos entre entidades fusionadas. La plataforma de SSE se integra con varios proveedores de identidades, lo que es crucial para satisfacer las diversas necesidades de acceso a aplicaciones de todos los usuarios.

Las capacidades sin agentes de ZTNA aceleran el proceso de fusiones y adquisiciones, ya que proporcionan a los usuarios acceso seguro Zero Trust basado en navegador, lo que acelera los plazos de integración significativamente.

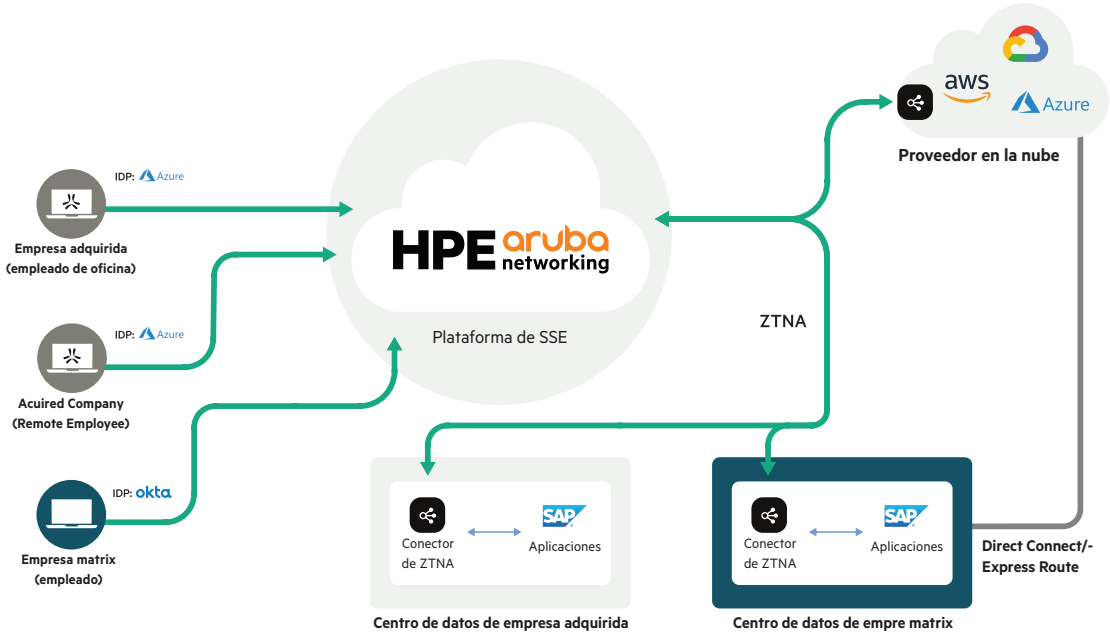

Figura 3. Aceleración de fusiones y adquisiciones

ZTNA de HPE Aruba Networking: el sustituto definitivo de la VPN

Iniciar tu cambio hacia el SSE no tiene por qué ser difícil. Nuestros expertos en SSE están aquí para ayudarte. Estas son solo algunas de las razones por las que equipos como el tuyo han elegido asociarse con HPE Aruba Networking para su cambio hacia el SSE y más allá.

- **Sustitución total de la VPN:** El ZTNA de HPE Aruba Networking supera al mercado con su amplia compatibilidad con aplicaciones privadas. Gestiona todo el tráfico TCP/UDP, incluido VOIP y de pares, y es compatible con aplicaciones web modernas como SSH, RDP, Git y bases de datos.
- **Acceso con privilegios mínimos sin segmentación:** Sin requerir una segmentación de red compleja, nuestro servicio de ZTNA restringe el acceso a recursos específicos, lo que reduce la superficie de ataque y evita el cruce no autorizado de la red.
- **Acceso flexible con agente o sin agente:** Los usuarios pueden acceder a las aplicaciones sin problemas desde cualquier dispositivo, con o sin cliente. Nuestra opción sin cliente facilita las sesiones de protocolo de escritorio remoto (RDP) basadas en navegador, lo que elimina la necesidad de tener que contar con infraestructuras de escritorios virtuales (VDI).
- **Inspección de tráfico granular:** Obtén visibilidad detallada del tráfico de recursos privados. Realiza seguimiento de las acciones de los usuarios, las descargas de archivos y el uso de comandos, y bloquea las actividades dañinas.
- **Controles de acceso adaptables:** Nuestros controles basados en interfaces de programación de aplicaciones (API) ajustan los derechos de acceso según la ubicación del usuario, su identidad y el estado del dispositivo, lo que mejora la seguridad de datos.
- **Arquitectura 100 % en la nube:** Con el SSE de HPE Aruba Networking, las conexiones se administran a través de la mejor ubicación de SSE, lo que garantiza tiempo de actividad constante sin tener que gestionar dispositivos de VPN.

Comienza con ZTNA de HPE Aruba Networking

Evalúa las necesidades de tu caso de uso específico y comunícate con nuestros profesionales experimentados para identificar las áreas donde el ZTNA puede brindar beneficios significativos para tu organización. Comienza a fortalecer tus aplicaciones más críticas hoy mismo con nuestras soluciones de seguridad de vanguardia.

Más información

Comunícate con un experto de SSE

Prueba gratuita de ZTNA durante 24 horas

Visita **ArubaNetworks.com**

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

Comunícate con nosotros

Hewlett Packard Enterprise

BWP_Architect-VPN-Replacement_A4_RB_012624 a00137489spl