Informe técnico de negocios

HPE aruba networking

La guía definitiva para la adopción del ZTNA

HPE GreenLake

77 %

El 77 % de las empresas cree que habilitará un entorno de trabajo híbrido en el futuro.

500 %

Las amenazas a la seguridad han aumentado un 500 % año tras año debido a esta nueva realidad laboral.

4 %

Los equipos de TI han experimentado un aumento significativo de la responsabilidad y, sin embargo, los presupuestos de TI solo aumentan un 4 % cada año.

El reto actual del acceso seguro

Puedes estar leyendo esta guía desde la comodidad de tu casa, desde el cubículo de una oficina o en cualquier otro lugar intermedio. La realidad es que el negocio en el que existimos hoy en día funciona de forma muy diferente a como lo hacía hace tan solo un par de años. El panorama empresarial ha cambiado y con él llegan una serie de retos que los equipos de TI deben superar, siendo una de las principales preocupaciones el método de conectividad segura a las aplicaciones empresariales.

Esto puede parecer bastante simple, pero con la dependencia de la tecnología equivocada, lograr un "acceso seguro" se convierte en una hazaña insuperable a medida que los problemas se amplifican frente a la nube y la movilidad. No es de extrañar que quienes efectúan las amenazas aprovechen esta oportunidad para sacar partido de las tecnologías que antes garantizaban la seguridad de las empresas, pero que ahora introducen riesgos.

Por este motivo, tanto los responsables de TI como los de las empresas buscan una solución de acceso moderna que proporcione a las organizaciones una conectividad fluida para los usuarios y sencilla para los responsables de TI. Gartner afirma que esta solución de acceso moderna es el acceso Zero Trust a la red (ZTNA) y estamos de acuerdo.

Para 2023, el 60 % de las empresas eliminarán gradualmente sus redes privadas virtuales (VPN) de acceso remoto en favor de ZTNA.

– Guía de mercado de Gartner para ZTNA

¿Qué es ZTNA y por qué ahora?

Las VPN se diseñaron para resolver un problema más sencillo en una época más sencilla: permitir el acceso seguro de una pequeña parte de la plantilla a aplicaciones controladas por TI en un centro de datos local. Suena sencillo, ¿verdad? Eso fue hace veinte años. Los usuarios instalaban clientes complejos en sus equipos de escritorio y se les concedía acceso a nivel de red a unas pocas aplicaciones. Había un nivel de confianza implícito: los usuarios se ceñirían al uso de las aplicaciones a las que se les concedía acceso y no se desviarían. Y lo que era aún mejor, los actores de amenazas no estaban al acecho esperando para infiltrarse en las redes y filtrar datos.

Las conexiones frágiles, la escalabilidad y el rendimiento limitados, y la complejidad de configuración y mantenimiento son solo algunos de los problemas que rodean a las VPN de acceso remoto. Además, hay otros factores que las organizaciones deben tener en cuenta a la hora de implantar una solución de seguridad de acceso moderna, como la verificación de identidades y dispositivos, el acceso y la aplicación a nivel de aplicación, y la flexibilidad para empleados y terceros dispersos geográficamente (que constituyen ~1/3 de la fuerza de trabajo admitida).

El acceso Zero Trust a la red (ZTNA) es uno de los principales componentes de una plataforma de extremo del servicio de seguridad (SSE) (ZTNA, SWG, CASB y DEM) que ofrece a los equipos de TI una alternativa moderna a las soluciones tradicionales de seguridad de redes. Como tecnología de acceso de elección en la actualidad, ZTNA permite a organizaciones de todos los tamaños conectar de forma segura a los usuarios (independientemente de su ubicación o dispositivo) a aplicaciones en la nube o en el centro de datos. ZTNA se adhiere al principio de Zero Trust "no confíes en nadie" que exige a todos los usuarios que se autentiquen a sí mismos y a sus dispositivos antes de obtener

acceso, lo que reduce significativamente el riesgo de que el malware o los actores de amenazas obtengan acceso no autorizado. Además, ZTNA también aplica el acceso menos privilegiado que restringe el acceso a aplicaciones individuales y autorizadas, incorporando una segmentación basada en políticas y minimizando el potencial de migración de este a oeste en caso de que el malware se introduzca en la red.

A diferencia de las soluciones de seguridad tradicionales, como las VPN, ZTNA ofrece importantes ventajas, entre las que se incluyen las siguientes:

- Rápida incorporación de empleados, contratistas y terceros sin los dolores de cabeza y la complejidad de la incorporación de usuarios a través de VPN
- Acceso optimizado a las aplicaciones para los trabajadores dispersos geográficamente, con el fin de mejorar la productividad y la colaboración
- Acceso sin clientes a numerosas aplicaciones web, RDP, SSH, Git y DB
- Cliente sencillo disponible para el acceso a cualquier puerto/protocolo (sin necesidad de capacitación compleja ni soporte técnico)
- Funciones de seguridad de Zero Trust, incluida la autenticación y autorización continuas de usuarios y dispositivos para impedir la penetración de usuarios no autorizados o programas maliciosos

ZTNA	VPN
✓ Admite trabajadores híbridos	⊘ Admite trabajadores remotos
✓ Experiencia sin interrupciones con integraciones IDP y diseño siempre en funcionamiento.	⊘ Experiencia frustrante con constantes solicitudes de inicio de sesión
✓ Acceso directo a recursos empresariales con intermediación automática	⊘ Experiencia lenta debido a la red de retorno del centro de datos
✓ Acceso de usuarios a aplicaciones autorizadas, no a la red corporativa	⊘ Posibilidad de agregar empleados riesgosos y terceros en la red corporativa
✓ Las aplicaciones y la red no están visibles para usuarios no autorizados	⊘ La infraestructura de VPN está expuesta a amenazas como el ransomware
✓ Gestión simple gracias a la política granular de Zero Trust	⊘ La segmentación de la red es compleja de gestionar

Figura 1. Comparación de las tecnologías ZTNA y VPN

Arquitectura ZTNA

Las soluciones ZTNA, como HPE Aruba Networking ZTNA, comienzan con un punto de control habilitado para la nube. Esto sirve como un punto distribuido de autenticación, autorización y aplicación de políticas que gobierna las transacciones entre usuarios y aplicaciones. ZTNA intermedia todas las conexiones no permitiendo ninguna conexión entrante a las aplicaciones, aumentando la seguridad de las aplicaciones y reduciendo la superficie de ataque.

Modelo conceptual de ZTNA iniciado por servicio

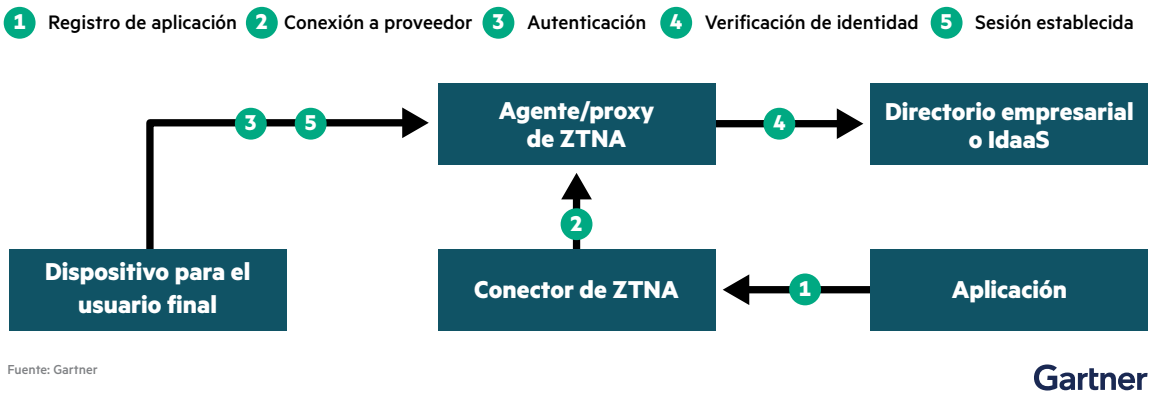

Figura 2. Cómo funciona una plataforma ZTNA iniciada por el servicio

1. Un usuario intenta acceder a una aplicación empresarial

Acceso seguro a las principales aplicaciones, incluso VOIP e ICMP, y soporte con acceso cliente o sin cliente.

2. ZTNA media en la solicitud

Evita las conexiones de paso que pueden conllevar riesgos: un nodo de nube de ZTNA se convierte en la primera parada para todo el tráfico de recursos empresariales.

3. ZTNA valida la identidad y la política

La identidad se integra en la plataforma ZTNA para facilitar el acceso de zero trust y adapta automáticamente los derechos de acceso en función de los cambios de contexto (posición del dispositivo, ubicación, etc.).

4. ZTNA se conecta de forma segura al recurso

La plataforma ZTNA intermedia automáticamente las conexiones con aplicaciones individuales y específicas, al tiempo que mantiene a los usuarios fuera de la red. Las aplicaciones privadas se hacen invisibles a Internet y las conexiones a las aplicaciones SaaS son rápidas y fluidas.

5. ZTNA inspecciona el tráfico y supervisa la experiencia del usuario

La plataforma ZTNA proporciona visibilidad de la actividad de los usuarios, lo que permite detectar cualquier actividad maliciosa y ofrece información sobre la experiencia de acceso del usuario final.

Una vez que el usuario se autentica en el punto de control, se establecen sesiones individuales basadas en el tiempo para aplicaciones específicas. Todas las sesiones se rigen por políticas establecidas por los administradores de TI y siguen a los usuarios independientemente de su ubicación. Además, cada sesión se autoriza y autentica continuamente, y cada dispositivo se evalúa de forma constante; en caso de que el dispositivo cambie de ubicación, se pueden tomar medidas para limitar el acceso a las aplicaciones, restringir las descargas de archivos o incluso poner el dispositivo en cuarentena para su corrección.

Por otra parte, la experiencia del usuario se simplifica enormemente con respecto a las VPN tradicionales o modelos de seguridad similares. La plataforma HPE Aruba Networking SSE ofrece capacidades sin cliente y basadas en cliente para ZTNA. Muchas transacciones pueden realizarse sin utilizar un cliente, incluidas las sesiones web, RDP, SSH y otras. Para el acceso a cualquier puerto o protocolo, existe un cliente ligero ampliamente disponible para el dispositivo elegido que proporciona un acceso rápido y seguro a las aplicaciones y recursos necesarios para seguir siendo productivo.

El resultado es una red mucho más segura que la que proporciona una pila de seguridad tradicional de firewalls, detección de intrusiones y herramientas de gestión de puntos finales. Y, gracias a las funciones de ZTNA como el aislamiento de aplicaciones de HPE Aruba Networkings, las propias aplicaciones son más seguras al tiempo que aprovechan la seguridad inherente de la microsegmentación, donde se restringe el cruce de este a oeste, lo que reduce significativamente la posibilidad de proliferación de malware.

Lograr Zero Trust con la ZTNA

Es importante subrayar que la mayoría de las organizaciones ya han implementado algún nivel de Zero Trust, ya sea en forma de autenticación de dos o múltiples factores, inicio de sesión único o aplicación de políticas. Igualmente importante es que la implementación de Zero Trust es un proceso: no hay dos topologías de red iguales. A menudo, los equipos de seguridad y arquitectura de TI son diferentes, lo que requiere colaboración y trabajo en equipo para aprovechar las importantes ventajas de seguridad y productividad de la ZTNA como paso previo a una estrategia holística del extremo del servicio de seguridad (SSE).

A continuación, se sugiere un proceso de "adopción" en el que los pasos pueden seguirse de manera secuencial a medida que las organizaciones inician el proceso de aumentar su perfil de seguridad, agilizar el acceso de su personal móvil y reducir las posibilidades de penetración de malware y de exfiltración de datos.

Lista de control para la adopción del ZTNA

Pasar de las arquitecturas de seguridad tradicionales a la ZTNA es el primer paso recomendado por Gartner para modernizar el acceso seguro a la empresa. De este modo, los usuarios, y los departamentos de TI, no tendrán que enfrentarse a los complejos problemas de conectividad que imponen las antiguas pilas de seguridad. Los usuarios estarán más contentos y serán más productivos, mientras que los departamentos de TI podrán centrarse en otras tareas críticas. En las siguientes secciones se describen las prácticas recomendadas para los equipos de TI que deseen migrar de las soluciones de acceso tradicionales a una ZTNA moderna.

1. Comprende tu entorno

Las organizaciones actuales suelen tener cientos o miles de aplicaciones en uso (ya sean conocidas o desconocidas), incluidos sistemas CRM y ERP, así como escritorios remotos como RDP y VDI. Disponer de un inventario de las aplicaciones que se utilizan en la actualidad puede ser útil para determinar quién puede acceder a qué aplicaciones; sin embargo, las soluciones ZTNA de primera calidad incorporarán funciones de descubrimiento de aplicaciones que permitirán al departamento de TI descubrir cualquier aplicación de TI en la sombra.

Además, determinar cómo acceden los usuarios a las aplicaciones de la organización puede aportar información. Por ejemplo, ¿algunos usuarios aprovechan más el BYOD que otros? Por otro lado, ¿siguen accediendo los usuarios a las aplicaciones alojadas en las instalaciones?

Es importante obtener una visibilidad inicial del entorno actual para poder evitar cualquier obstáculo que pueda surgir a mitad de la implementación.

2. Comienza por las zonas de alto riesgo, como el acceso remoto

La fuerza de trabajo actual se compone de empleados, terceros, clientes y usuarios fusionados o adquiridos, y muchos de ellos trabajan de forma remota. Todos necesitan un acceso optimizado a los recursos empresariales, preferiblemente sin necesidad de mucha configuración ni de un cliente en el punto final. Considera la posibilidad de iniciar la implementación con un pequeño subconjunto de estos usuarios remotos (como tu equipo ejecutivo, desarrolladores o usuarios de terceros) y aprende a configurar y aplicar políticas de acceso de mínimo privilegio con ZTNA. Realiza un seguimiento de esta implementación con el resto de la fuerza de trabajo remota.

3. Amplía el acceso a los trabajadores de la oficina (y más allá)

Con el 77 % de las organizaciones que adoptan alguna forma de trabajo híbrido, es importante que el acceso a la ZTNA se extienda también al soporte del usuario de oficina. Con trabajadores que entran y salen de la oficina de forma constante mientras acceden a datos confidenciales, es importante que Zero Trust y el acceso con menos privilegios se apliquen de forma universal para no crear brechas de seguridad que pongan en peligro la red. Además, esto proporciona a la fuerza de trabajo híbrida una experiencia de acceso completamente fluida y coherente, ya sea en casa o en la oficina.

Las fusiones y adquisiciones también se benefician de ZTNA. Soluciones como HPE Aruba Networking ZTNA permiten de forma rápida y sencilla un acceso de bajo riesgo y Zero Trust a aplicaciones y recursos en todas las organizaciones antes de fusionar topografías de red. Mediante tecnologías basadas en la nube, HPE Aruba Networking ZTNA ofrece servicios altamente escalables que permiten el acceso basado en agentes o sin agentes a recursos en cualquier lugar, a la vez que los aísla de usuarios, dispositivos y redes potencialmente comprometidos. La implementación es rápida sin grandes cambios en la red, mientras que una consola central en la nube lo gestiona todo mediante políticas entre aplicaciones, garantizando que solo los usuarios autorizados accedan a las aplicaciones a las que tienen derecho.

4. El siguiente paso en la implementación de SSE

En este punto se ha completado 1/4 de la implementación global de SSE. Has minimizado con éxito el riesgo de acceso en las áreas de mayor preocupación y puedes buscar una mayor implementación de la SSE mediante la evaluación de los contratos existentes y la elaboración de un plan de eliminación gradual de las tecnologías de seguridad basadas en el perímetro. El departamento de TI puede consolidar los contratos mediante la selección de un único proveedor de SSE que pueda proporcionar ZTNA, SWG, CASB y DEM. Estas decisiones no solo repercutirán en la infraestructura de la oficina corporativa, sino que también pueden ayudar a acelerar los proyectos de transformación de las sucursales, contribuyendo a minimizar los costos innecesarios de MPLS y, en su lugar, la inversión en servicios de extremo de seguridad basados en la nube en la sucursal.

Moderniza el acceso remoto seguro con ZTNA

Las empresas de hoy requieren un desarrollo rápido, altos niveles de colaboración y trabajo en equipo, y seguridad e integridad de datos. Para cada una de estas necesidades es fundamental una red moderna, flexible, escalable y segura que facilite la comunicación en lugar de obstaculizarla. Aunque las arquitecturas tradicionales, como las VPN, pueden seguir teniendo una relevancia limitada para algunos, la complejidad de gestionar y mantener infraestructuras antiguas solo sirve para consumir recursos mejor invertidos en otro sitio.

ZTNA es el futuro del acceso moderno y supera los retos de la movilidad del personal, la seguridad del acceso a la red y la escalabilidad sin los dolores de cabeza de una configuración e implementación complejas. El lugar de trabajo moderno requiere que el acceso sea fluido a la vez que los recursos sean seguros, y HPE Aruba Networking ZTNA proporciona el camino para conseguir ambas cosas.

Con HPE Aruba Networking ZTNA, los equipos de TI pueden conseguir lo siguiente:

- Implementar en minutos u horas en lugar de semanas o meses
- Ofrecer productividad y colaboración a los trabajadores distribuidos por todo el mundo
- Mejorar la visibilidad y la experiencia mediante información detallada sobre la actividad de los usuarios y las aplicaciones
- Reducir el riesgo de pérdida de datos y penetración de malware al tiempo que se mejora el cumplimiento de la normativa
- Simplificar la gestión de TI mediante políticas intuitivas de Zero Trust y controles de acceso granulares

Comienza a modernizar el acceso para el lugar de trabajo moderno con HPE Aruba Networking SSE. Regístrate y realiza un test drive del extremo del servicio de seguridad (SSE) de HPE Aruba Networking.

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

Comunícate con nosotros

Obtén más información en

arubanetworks.com/sse-test-drive/

Visita **ArubaNetworks.com**

BWP_ZTNA-Adoption_A4_RB_011124 a00136926spl

Hewlett Packard Enterprise