HPE aruba networking

Informe técnico empresarial

Pasarse de VPN a ZTNA

Ventajas del ZTNA y por dónde empezar

HPE GreenLake

60 %

de las organización cambiarán su VPN por un servicio de ZTNA

El advenimiento del teletrabajo ha supuesto nuevos retos de seguridad para las organizaciones. Con un número cada vez mayor de empleados que trabajan desde cualquier lugar, las organizaciones deben encontrar formas de asegurar el acceso remoto e híbrido a sus redes y datos. Una solución que se ha utilizado tradicionalmente es la red privada virtual (VPN). Sin embargo, a medida que las ciberamenazas siguen evolucionando, las VPN han demostrado ser inadecuadas para protegerse de las amenazas modernas. El acceso a red de confianza cero (ZTNA) y resulta ser una solución más eficaz para proteger el acceso remoto que las VPN.

¿Qué es el ZTNA?

Creado en abril de 2019 por Gartner®, la frase acceso a red de Confianza Cero (ZTNA) representa un conjunto de nuevas tecnologías diseñadas para el acceso seguro a aplicaciones privadas. El ZTNA utiliza políticas de acceso granular para conectar a los usuarios autorizados a aplicaciones específicas, sin conceder acceso a la red, lo que permite un acceso segmentado de mínimo privilegio, sin exponer nunca las ubicaciones de las aplicaciones a Internet, como ocurre con las VPN.

Gartner prevé que para 2023, el 60 % de las organizaciones estarán cambiando su VPN con un servicio de ZTNA. Esto ha llevado al ZTNA a convertirse en el producto de confianza cero que más rápido crece en el sector, con el 47 % de los responsables de TI estableciendo el ZTNA como su punto de partida para aquellos que buscan implementar una plataforma Security Service Edge (SSE) como parte de un marco Secure Access Service Edge (SASE) más amplio.

El ZTNA mejora la seguridad

Una de las principales razones por las que las empresas están adoptando el ZTNA es por la mayor seguridad que proporciona. Con una VPN, los usuarios se incorporan directamente a la red corporativa. Una vez que un usuario obtiene acceso a la red, puede desplazarse lateralmente y acceder potencialmente a datos o recursos confidenciales. No es ninguna sorpresa que “conceder demasiada confianza a los usuarios” sea el mayor problema de las soluciones de acceso seguro existentes, según el informe de adopción de SSE de 2023. Aunque se podría decir que esto importa menos para los usuarios internos, no deja de ser desalentador saber que un atacante se beneficiaría de la falta de segmentación.

En cambio, el ZTNA nunca extiende el acceso a la red y concede acceso en función del contexto: la identidad del usuario, el dispositivo que utiliza y la aplicación y los datos a los que intenta acceder. Esto significa que aunque un atacante intente acceder a la red, no solo no podrá acceder a datos confidenciales sin la autenticación adecuada, sino que el servicio de ZTNA ocultará la existencia misma de la red, haciéndola invisible e imposible de rastrear.

Las soluciones de ZTNA suelen ser menos costosas de implementar y mantener que las soluciones de VPN. El coste de la VPN va más allá del simple coste del equipo.

El ZTNA aumenta la escala y la flexibilidad

Otra razón por la que las empresas están adoptando ZTNA es por la mayor escala y flexibilidad que proporciona. Mientras que las soluciones de VPN suelen basarse en hardware y dispositivos, las soluciones de ZTNA se proporcionan en la nube, lo que significa que los usuarios pueden acceder a ellas fácilmente y los departamentos de TI pueden gestionarlas desde cualquier lugar. Esto es especialmente útil para las empresas con empleados híbridos/remotos o que necesitan acceder a recursos desde distintos lugares. Mientras que las VPN tienen límites de capacidad estáticos basados en el tamaño de los dispositivos, la naturaleza de la arquitectura en la nube de ZTNA permite ampliar o reducir fácilmente su capacidad para satisfacer las necesidades cambiantes de una empresa.

Y lo que es más importante, los servicios de ZTNA proporcionan políticas de control de acceso hipergranulares y flexibles que pueden aplicarse hasta a nivel de usuario y aplicación. La segmentación del acceso con VPN implica una compleja segmentación de red pero, con ZTNA, implementar el acceso de mínimo privilegio es tan sencillo como ajustar una política.

El ZTNA permite mejorar la productividad

Las soluciones de ZTNA proporcionan una experiencia de acceso mejor que las VPN. Las VPN reducen la productividad de las empresas, ya que los usuarios tienen que lidiar con velocidades de conexión lentas (debido a la red de retorno de la VPN), desconexiones incómodas y constantes, e inicios de sesión complejos y repetitivos. Todo ello interrumpe el trabajo de los usuarios y genera frustración.

El ZTNA, en cambio, ofrece una experiencia de uso más sencilla a los usuarios finales. Permite a los usuarios finales acceder fácilmente a aplicaciones privadas eliminando el tráfico de retorno, permaneciendo siempre activo incluso con cambios en la red y creando un proceso de inicio de sesión fluido con integraciones directas con SSO y otras soluciones de gestión de identidades.

El ZTNA es más rentable

Las soluciones de ZTNA suelen ser menos costosas de implementar y mantener que las soluciones de VPN. El coste de las VPN va mucho más allá del simple coste del equipo... Además de los concentradores VPN, las VPN requieren un costoso hardware instalado localmente, como protección DDoS, cortafuegos internos y externos, equilibradores de carga,

etc. Todo esto es para una sola pila de seguridad entrante (las organizaciones tienen de 3 a 5 por término medio). Además, los equipos de seguridad suelen necesitar uno o varios miembros del personal dedicados a la supervisión y gestión de las VPN. Esto resta recursos a otros proyectos más urgentes e importantes. El mantenimiento de este enfoque centrado en el perímetro para proteger el acceso es costoso.

En cambio, las soluciones de ZTNA no requieren la instalación y el mantenimiento locales de hardware o software costosos. Además, las organizaciones quieren plataformas SSE para eliminar la necesidad de concentradores VPN (63 %), inspección SSL (50 %) y protección DDoS (44 %). De hecho, las mejores plataformas SSE ofrecen tecnologías ZTNA que eliminan por completo la VPN y la pila de seguridad entrante, lo que se traduce en un enorme ahorro de costes. ZTNA también es intuitivo y fácil de gestionar, lo que permite a las organizaciones reducir drásticamente el número de recursos y compañeros de equipo necesarios para gestionar el acceso seguro. Por último, las soluciones de ZTNA se basan en un modelo de precios por suscripción que da transparencia a los costes y evita que las organizaciones paguen de más por las licencias.

No dejes que la VPN te frene

A medida que el número de trabajadores remotos e híbridos sigue creciendo, resulta fundamental para las empresas contar con una solución moderna de acceso seguro. El acceso a la red de confianza cero (ZTNA) es una solución moderna que supera las limitaciones de las VPN y proporciona más seguridad, flexibilidad, escalabilidad, rendimiento y rentabilidad en lo que se refiere al acceso remoto.

Lo mejor de ZTNA es que forma parte de una estrategia de seguridad mayor. A medida que las organizaciones buscan adoptar una plataforma Security Service Edge (SSE), vemos que casi el 50 % empieza con la adopción de ZTNA. ¿Por dónde se empieza?

Cambia por completo la VPN por HPE Aruba Networking ZTNA

Descubre más sobre el uso de HPE Aruba Networking ZTNA como una alternativa a la VPN

Echa un vistazo a la plataforma HPE Aruba Networking SSE

arubanetworks.com/products/sse

Visita **ArubaNetworks.com**

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

Comunícate con nosotros

Hewlett Packard Enterprise

BWP_Switch-to-ZTNA_A4_RB_022224 a00136655ese