HPE aruba networking

Informe técnico de negocios

Hacer el cambio de VPN a ZTNA

Los beneficios de ZTNA y por dónde empezar

HPE GreenLake

El

60 %

de las organizaciones reemplazarán su VPN con un servicio de ZTNA

La llegada del trabajo remoto ha traído consigo nuevos desafíos de seguridad para las organizaciones. Con cada vez más empleados trabajando desde todas partes, las organizaciones deben encontrar formas de proteger el acceso remoto e híbrido a sus redes y datos. Una solución que tradicionalmente se ha usado es la red privada virtual (VPN). Sin embargo, a medida que las amenazas cibernéticas continúan evolucionando, las VPN han demostrado no ser adecuadas para proteger contra las amenazas modernas. El acceso Zero Trust de red (ZTNA) es una solución más eficaz para proteger el acceso remoto.

¿Qué es el ZTNA?

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. El ZTNA utiliza políticas de acceso granular para conectar usuarios autorizados a aplicaciones específicas, sin otorgar acceso a la red, lo que permite el acceso segmentado con menos privilegios, sin exponer las ubicaciones de las aplicaciones a Internet, como ocurre con las VPN.

Gartner espera que el 60 % de las organizaciones reemplacen su VPN con un servicio de ZTNA para 2023. Esto ha llevado al ZTNA a convertirse en el producto Zero Trust de más rápido crecimiento en la industria, con el 47 % de los líderes de TI haciendo que el ZTNA sea el punto de partida para quienes buscan adoptar una plataforma de extremo del servicio de seguridad (SSE) como parte de un mejor marco de extremo de servicio de acceso seguro (SASE).

ZTNA mejora la seguridad

Una de las principales razones por las que las empresas están adoptando el ZTNA es la seguridad mejorada que brinda. Con una VPN, los usuarios acceden directamente a la red corporativa. Una vez que un usuario obtiene acceso a la red, puede moverse lateralmente y potencialmente acceder a datos o recursos confidenciales. Según el informe de adopción de SSE de 2023, no es extraño que se haya determinado que “otorgar demasiada confianza a los usuarios” sea el mayor desafío con las soluciones de acceso seguro existentes. Si bien se podría decir que esto es menos importante para los usuarios internos, es una idea desalentadora saber que un atacante se beneficiaría de la falta de segmentación.

Por el contrario, el ZTNA nunca extiende el acceso a la red y otorga acceso según el contexto: la identidad del usuario, el dispositivo que está utilizando, y la aplicación y los datos a los que intenta acceder. Esto significa que incluso si un atacante intenta obtener acceso a la red, no solo no podrá acceder a datos confidenciales si no cuenta con 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 costo de una VPN va mucho más allá del simple costo de la caja.

El ZTNA aumenta la escala y la flexibilidad

Otra razón por la que las empresas están adoptando el ZTNA es por la mayor escala y flexibilidad que proporciona. Si bien las soluciones de VPN por lo general se basan en hardware y dispositivos, las soluciones de ZTNA se entregan en la nube, lo que significa que los usuarios pueden acceder a ellas con facilidad y el departamento de TI puede administrarlas desde cualquier ubicación. Esto es particularmente útil para empresas con empleados híbridos/remotos o que necesitan acceder a recursos desde diferentes ubicaciones. Si bien las VPN tienen límites de capacidad estática según el tamaño del dispositivo, la naturaleza de la arquitectura de ZTNA entregada en la nube permite que las empresas se agranden o achiquen con facilidad para satisfacer las necesidades cambiantes de una empresa.

Más importante aún, los servicios de ZTNA brindan políticas de control de acceso hipergranulares y flexibles que se pueden aplicar según el nivel de usuario y aplicación. La segmentación de acceso con VPN significa que la segmentación de red es compleja. Sin embargo, con ZTNA, implementar un acceso con privilegios mínimos es tan simple como la modificación de una política.

El ZTNA permite lograr mejor productividad

Las soluciones de ZTNA permiten que la experiencia de acceso sea mejor que las de VPN. Las VPN reducen la productividad empresarial, ya que los usuarios deben lidiar con velocidades de conexión lentas (debido al retroceso de las VPN), desconexiones inconvenientes y constantes, e inicios de sesión complejos y repetitivos. Todo esto perturba el trabajo de los usuarios y genera frustración.

Por otro lado, el ZTNA permite que la experiencia de los usuarios finales sea más fácil. Permite a los usuarios finales acceder a aplicaciones privadas con facilidad, ya que elimina el tráfico de retorno, permanece siempre en funcionamiento incluso durante cambios en la red y crea un proceso de inicio de sesión sin inconvenientes con integraciones profundas con las SSO y otras soluciones de gestión de identidad.

El ZTNA es más rentable

Las soluciones de ZTNA suelen ser menos costosas de implementar y mantener que las soluciones de VPN. El costo de una VPN va mucho más allá del simple costo de la caja... Además de los concentradores de VPN, las VPN requieren hardware costoso en las instalaciones, como protección contra DDoS, firewalls internos y externos, balanceadores de carga, etc. Todo esto es para una única pila de seguridad entrante (las organizaciones tienen entre 3 y 5 en promedio). Además, los equipos de seguridad generalmente requieren que uno o más empleados se dediquen a la supervisión y gestión de la VPN. Esto ocupa recursos de otros proyectos más urgentes e importantes. Mantener este enfoque centrado en el perímetro para proteger el acceso es costoso de mantener.

Por el contrario, las soluciones de ZTNA no requieren la instalación ni el mantenimiento de hardware o software costosos en las instalaciones. Además, las organizaciones quieren que las plataformas de SSE eliminen la necesidad de concentradores de VPN (63 %), inspecciones de SSL (50 %) y la protección contra DDoS (44 %). De hecho, las mejores plataformas de SSE ofrecen tecnologías de ZTNA que eliminan la VPN y la pila de seguridad entrante por completo, lo que genera enormes ahorros en los costos. El ZTNA también es intuitivo y fácil de administrar, lo que permite a las organizaciones reducir drásticamente la cantidad de recursos y compañeros de equipo necesarios para administrar el acceso seguro. Por último, las soluciones de ZTNA aprovechan un modelo de precios basado en suscripciones que brinda transparencia a los costos y significa que las organizaciones no pagan de más por las licencias.

No dejes que la VPN te detenga

Debido a que la cantidad de personas que trabajan de forma remota e híbrida sigue creciendo, es fundamental que las empresas cuenten con una solución moderna de acceso seguro. El acceso Zero Trust a la red (ZTN) es una solución moderna que aborda las limitaciones de las redes privadas virtuales (VPN) y brinda mejor seguridad, flexibilidad, escalabilidad, rendimiento y rentabilidad para el acceso remoto.

La mejor parte sobre el ZTNA es que es parte de una estrategia de seguridad más grande. A medida que las organizaciones buscan adoptar una plataforma de extremo de servicio de seguridad (SSE), vemos que casi el 50 % está comenzando con la adopción del ZTNA. ¿Por dónde vas a empezar?

Reemplaza la VPN con ZTNA de HPE Aruba Networking por completo

Obtén más información sobre el uso de ZTNA de HPE Aruba Networking como alternativa a una VPN

Echa un vistazo a la plataforma de SSE de HPE Aruba Networking

arubanetworks.com/products/sse

Visita **ArubaNetworks.com**

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

Comunícate con nosotros

BWP_Switch-to-ZTNA_A4_RB_022224 a00136655spl

Hewlett Packard Enterprise