BLOG POST

Symantec ZTNA

Proteja su negocio sin afectar a la productividad

Stephen Hearty
Head of Symantec Product Marketing EMEA, Arrow

Alan Hall
Product Marketing Enterprise Security Group, Broadcom

La forma en que abordamos la seguridad de las redes está experimentando una dramática transformación. A medida que las organizaciones se enfrentan a los desafíos de proteger a una plantilla distribuida y los datos de naturaleza delicada, está surgiendo un nuevo paradigma: acceso a la red de confianza cero (Zero Trust Network Access, ZTNA). Este enfoque innovador no es sólo una alternativa a las redes privadas virtuales (VPN) tradicionales, sino un salto adelante en la gestión de accesos segura, eficaz y fácil de usar. Descubre aquí por qué.

Descifrar la sopa de letras: ZTNA frente a VPN

ZTNA es un modelo de seguridad que funciona según el principio de "no confiarse nunca, verificar siempre". Proporciona un acceso seguro a aplicaciones y servicios basado en políticas de control de acceso, independientemente de dónde se encuentre el usuario, el dispositivo o la aplicación. Por el contrario, las VPN tradicionales crean un túnel cifrado entre el dispositivo de un usuario y la red corporativa, concediendo un amplio acceso una vez que el usuario se autentica.

ZTNA se centra en las aplicaciones y en la identidad, mientras que las VPN se centran en la red y el perímetro. Esta distinción fundamental sienta las bases para las numerosas ventajas de ZTNA.

Cómo refuerza ZTNA la ciberseguridad

Cuando se trata de seguridad, ZTNA deja a las VPN tradicionales completamente atrás. Proporciona acceso a nivel de aplicación, a diferencia del amplio acceso a la red de las VPN. Esto significa que los usuarios sólo tienen acceso a las aplicaciones específicas que necesitan, y no a toda la red. Es como darle a alguien la llave de una habitación concreta en lugar de la llave maestra de todo el edificio.

ZTNA también reduce la superficie de ataque. A diferencia de las VPN, que a menudo exponen los puertos a internet, ZTNA mantiene ocultas las direcciones IP, lo que hace que la red corporativa sea invisible para los usuarios no autorizados. Este manto de invisibilidad reduce drásticamente el riesgo de ataques basados en la red.

Si bien las VPN suelen autenticarse una sola vez al inicio de una sesión, ZTNA emplea la autenticación continua, verificando constantemente a los usuarios y los dispositivos.

Esta tecnología también ofrece una visibilidad y un control que las VPN tradicionales simplemente no pueden igualar. Proporciona información detallada sobre las actividades de los usuarios y aplica políticas de acceso granulares, ofreciendo a los equipos de seguridad una imagen más clara de lo que está sucediendo en su red. Estas políticas de acceso centradas en el usuario son más rápidas de administrar y menos propensas a errores que las complejas configuraciones de VPN, lo que permite a las organizaciones configurarlas para toda la base de usuarios a escala.

Mejorar la experiencia del usuario

Aunque la seguridad es primordial, la experiencia del usuario puede hacer o deshacer la adopción de cualquier tecnología. Aquí también, ZTNA brilla con luz propia en comparación con las VPN.

Más información sobre Symantec Network Protection

BLOG POST

Symantec ZTNA: Proteja su negocio sin afectar a la productividad

ZTNA ofrece un acceso perfecto desde cualquier lugar, eliminando la compleja configuración que suele asociarse a las VPN. Los usuarios pueden acceder de forma segura a las aplicaciones sin tener que preocuparse por establecer una conexión VPN o de saber dónde se encuentra una aplicación. Por eso, la Guía de mercado para el acceso de confianza cero de Gartner predijo que para 2025 al menos el 70 % de las nuevas implementaciones de acceso remoto se realizarán principalmente mediante ZTNA en lugar de servicios VPN para 2025, frente a menos del 10 % a finales de 2021.

El proceso de conexión con ZTNA también es mucho más sencillo en comparación con los clientes de VPN tradicionales. No es necesario acordarse de encender la VPN ni esperar a que se conecte: el acceso es rápido y sencillo.

Este nuevo enfoque mejora el rendimiento y la fiabilidad al optimizar el enrutamiento del tráfico y eliminar la necesidad de redirigir todo el tráfico por una ubicación central (un cuello de botella habitual en las VPN).

Por último, ZTNA ofrece un soporte excelente para las realidades del trabajo moderno, incluidas las políticas de "Lleve su propio dispositivo" (BYOD) y las situaciones de teletrabajo. Se adapta más fácilmente a diversos dispositivos y ubicaciones que las VPN tradicionales, lo que la convierte en una solución más realista para los entornos de trabajo flexibles de hoy en día.

Seguridad basada en la nube sin compromisos

Si bien algunas soluciones ZTNA están diseñadas para su implementación en las instalaciones, la solución Symantec Security Service Edge (SSE) basada en la nube de Symantec incorpora ZTNA para ofrecer todas estas ventajas en la nube.

Mientras que la tecnología en la instalación suele requerir la compra y mantenimiento continuo de servidores y software cliente, las operaciones basadas en la nube reducen los costes.

ZTNA en Symantec SSE minimiza la configuración y los gastos operativos gracias a la implementación sin agentes, la integración perfecta con los sistemas de gestión de acceso e identidades existentes y la compatibilidad con dispositivos gestionados y no gestionados. Estas capacidades hacen que a las organizaciones le resulte más sencilla la implantación de ZTNA y conseguir beneficios rápidamente.

Una característica es el control de acceso basado en funciones (role-based access control, RBAC), que le permite asignar funciones específicas a equipos o usuarios individuales. Esto simplifica la gestión, reduciendo la complejidad y creando al mismo tiempo una solución más escalable. A medida que las empresas se expanden, RBAC facilita la gestión y el ajuste de los permisos en toda la organización, lo que proporciona un mayor control y visibilidad sobre los derechos de acceso.

ZTNA de Symantec también forma parte de un ecosistema de seguridad más amplio e integrado que permite una prevención de amenazas, una protección de datos y una gestión del cumplimiento más completas, creando una postura de seguridad que es mayor que la suma de sus partes.

Esta escalabilidad es fundamental para las organizaciones que experimentan crecimiento. A medida que su negocio se expande, RBAC facilita el ajuste de los permisos en grupos enteros, garantizando que el acceso a las aplicaciones y los recursos se mantenga estrechamente controlado y alineado con las políticas de la organización.

Trazando el rumbo de la seguridad futura

La transición de las VPN a ZTNA no es sólo una tendencia; es una evolución necesaria en nuestra forma de abordar el acceso seguro. A medida que las organizaciones sigan adoptando la transformación digital, la adopción de la nube y el teletrabajo, ZTNA desempeñará un papel cada vez más fundamental para garantizar que nuestros activos digitales permanezcan protegidos, nuestros usuarios sigan siendo productivos y nuestras operaciones sigan siendo eficientes.

A fin de cuentas, ZTNA no consiste únicamente en reemplazar a las VPN, sino en reimaginar lo que es posible en la seguridad de la red. Se trata de crear un futuro en el que la seguridad mejore en vez de crear dificultades, donde la protección sea generalizada pero invisible y en el que la confianza se gane continuamente, y no se dé a ciegas. Esa es la promesa de ZTNA, y es un futuro que merece la pena abrazar.

Suscribir Regístrese ahora para recibir las últimas actualizaciones del equipo de Symantec y Arrow