SOPHOS
Cybersecurity evolved.

Las seis principales ventajas de ZTNA

Comparación con la VPN de acceso remoto

Monográficos de Sophos. Octubre de 2021

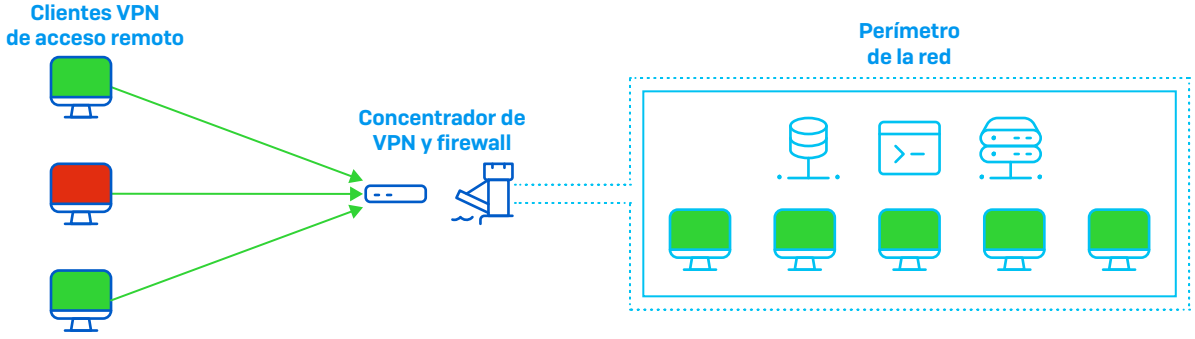
La VPN de acceso remoto nos ha hecho un buen servicio durante mucho tiempo, pero el reciente aumento del teletrabajo ha puesto de manifiesto las limitaciones de esta tecnología anticuada. Mientras que algunas organizaciones siguen exprimiendo al máximo las posibilidades de la VPN, muchas buscan una alternativa mejor, algo que resuelva los problemas de la VPN de acceso remoto. Varias organizaciones ya han empezado a adoptar plenamente la nueva generación de tecnología de acceso remoto: ZTNA o acceso a la red de confianza cero. ZTNA ofrece una mejor seguridad, un control más granular, una mayor visibilidad y una experiencia de usuario transparente en comparación con la VPN de acceso remoto tradicional.

En esta guía para la adquisición de ZTNA analizaremos las limitaciones y los retos de la VPN de acceso remoto tradicional y las ventajas que puede aportar Zero Trust Network Access, además de compartir una lista de funciones críticas que debe incluir su nueva solución ZTNA.

Retos de la VPN de acceso remoto

La VPN de acceso remoto ha sido un elemento fundamental en la mayoría de redes durante décadas, ofreciendo un método seguro para acceder de forma remota a los sistemas y recursos de la red. Sin embargo, se desarrolló durante una época en la que la red corporativa se asemejaba a una fortificación medieval: la proverbial muralla del castillo y el foso que formaban un perímetro seguro alrededor de los recursos de la red. La VPN proporcionaba el equivalente a una garita custodiada para que los usuarios autorizados entraran en el perímetro seguro, pero una vez dentro, tenían acceso completo a todo lo que había dentro.

VPN de acceso remoto tradicional



Por supuesto, las redes han evolucionado considerablemente y están más distribuidas que nunca. Las aplicaciones y los datos residen ahora en la nube, los usuarios trabajan a distancia y las redes son asediadas por atacantes y hackers que buscan cualquier punto débil que explotar.

Administrar una solución de acceso remoto basada en una VPN tradicional (IPSec/SSL) en cualquier tipo de entorno moderno puede resultar sumamente complicado. Hay que lidiar con la gestión de IP, los flujos de tráfico y el enrutamiento y las reglas de acceso al firewall, así como con el despliegue y la configuración de clientes y certificados. Todo lo que supere un puñado de nodos y unas pocas decenas de usuarios lo convierte en un trabajo innecesario a tiempo completo, y solo para mantenerlo en funcionamiento. Por si esto fuera poco, supervisar y controlar la seguridad se convierte en una auténtica pesadilla.

En resumen, la VPN de acceso remoto tradicional conlleva una serie de limitaciones y retos innecesarios:

1. **Confianza implícita**: la VPN de acceso remoto cumple con su cometido de permitirle atravesar el perímetro y entrar en la red corporativa como si estuviera físicamente allí, pero llegados a ese punto, se le otorga una confianza implícita y se le da un amplio acceso a los recursos de esa red, lo que puede suponer enormes e innecesarios riesgos de seguridad.
2. **Vector potencial de amenazas**: la VPN de acceso remoto desconoce el estado del dispositivo utilizado para conectarse a la red corporativa, lo que crea un conducto potencial para que las amenazas entren en la red desde dispositivos que pueden haberse visto comprometidos.
3. **Redireccionamiento ineficiente**: la VPN de acceso remoto proporciona un único punto de presencia en la red, lo que podría requerir el redireccionamiento del tráfico desde múltiples ubicaciones, centros de datos o aplicaciones a través del túnel VPN de acceso remoto.
4. **Falta de visibilidad**: la VPN de acceso remoto desconoce el tráfico y los patrones de uso que facilita, lo que dificulta la visibilidad de la actividad de los usuarios y el uso de las aplicaciones.
5. **Experiencia del usuario**: los clientes VPN de acceso remoto son conocidos por ofrecer una experiencia de usuario deficiente, añadir latencia o afectar negativamente al rendimiento, sufrir problemas de conectividad y, en general, ser una carga para el servicio de soporte.
6. **Administración, despliegue e inscripción**: los clientes VPN de acceso remoto son difíciles de configurar y desplegar, y también hacen complicadas la inscripción y baja de usuarios. La VPN también es un reto para administrar en el lado del firewall o la puerta de enlace, especialmente con múltiples nodos, reglas de acceso al firewall, gestión de IP y flujos de tráfico y enrutamiento. Rápidamente se convierte en un trabajo a tiempo completo.

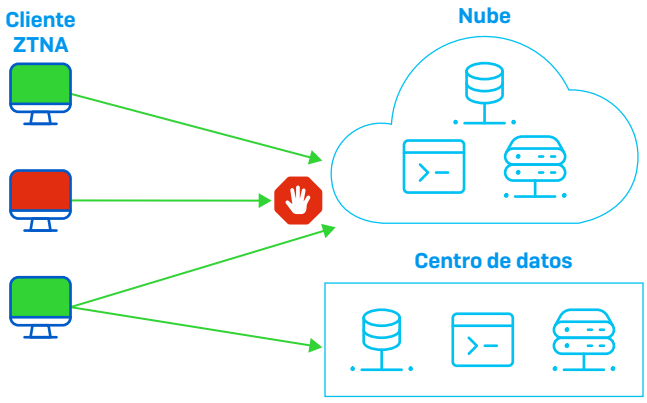
Qué es ZTNA y cómo funciona

ZTNA o acceso a la red de confianza cero ha sido diseñado desde un principio para hacer frente a los desafíos y las limitaciones que presentan las VPN de acceso remoto: ofrece una solución mejor para que los usuarios se conecten desde cualquier ubicación de forma segura a las aplicaciones y los datos que necesitan para hacer su trabajo, y a nada más. Hay varias diferencias fundamentales entre ZTNA y la VPN de acceso remoto.

Como su nombre indica, ZTNA se basa en los principios de confianza cero, es decir, no confiar en nada y verificarlo todo. En esencia, la confianza cero elimina el concepto del antiguo perímetro de muralla y foso de castillo medieval para convertir a cada usuario, cada dispositivo y cada aplicación en red en su propio perímetro y solo interconectarlos después de validar las credenciales, verificar el estado del dispositivo y comprobar las políticas de acceso. De este modo, se mejora drásticamente la seguridad, la segmentación y el control.

Otra diferencia clave en cuanto al funcionamiento de ZTNA es que no se deja entrar a los usuarios en la red con total libertad de movimiento. En lugar de ello, se establecen túneles individuales entre el usuario y la puerta de enlace específica para la aplicación a la que está autorizado a acceder, y nada más, lo que proporciona un nivel de microsegmentación mucho más seguro. Esto tiene una serie de ventajas para la seguridad, el control, la visibilidad, la eficiencia y el rendimiento. Por ejemplo, la VPN de acceso remoto no aporta ninguna información sobre las aplicaciones a las que acceden los usuarios, mientras que ZTNA puede proporcionar el estado y la actividad en tiempo real de todas sus aplicaciones, lo que resulta muy valioso para identificar posibles problemas y realizar auditorías de licencias. La microsegmentación adicional que ofrece ZTNA garantiza que no haya movimiento lateral de acceso de dispositivos o usuarios entre los recursos de la red. Cada usuario, dispositivo y aplicación o recurso es literalmente su propio perímetro seguro y ya no existe el concepto de confianza implícita.

Zero Trust Network Access



Además, ZTNA es intrínsecamente más dinámico y transparente por naturaleza, ya que funciona en segundo plano sin requerir la interacción del usuario más allá de la validación inicial de la identidad. Esta experiencia puede ser tan ágil y fluida que los usuarios ni siquiera se darán cuenta de que se están conectando a las aplicaciones a través de túneles cifrados seguros.

Ventajas de ZTNA

Zero Trust Network Access ofrece enormes ventajas en muchos sentidos, pero se está adoptando principalmente por una o varias de estas razones:

- **Teletrabajo:** con las soluciones ZTNA es mucho más fácil gestionar el acceso remoto del personal que trabaja desde casa. Hacen que el despliegue y la inscripción sean más fáciles y flexibles, convirtiendo lo que podría haber sido un trabajo a tiempo completo con una VPN en algo que consume muchos menos recursos. También es más transparente y sencillo para el personal que teletrabaja.
- **Microsegmentación de aplicaciones:** las soluciones ZTNA mejoran notablemente la seguridad de las aplicaciones gracias a la microsegmentación, la integración del estado del dispositivo en las políticas de acceso, la verificación continua de la autenticación y la mera eliminación de la confianza implícita y el movimiento lateral que conlleva la VPN.
- **Protección contra el ransomware:** las soluciones ZTNA eliminan un vector de ataque común para el ransomware y otros ataques de infiltración en la red. Dado que los usuarios de ZTNA ya no están "en la red", las amenazas que de otro modo podrían afianzarse a través de la VPN no tienen nada que hacer con ZTNA.
- **Rápida incorporación de aplicaciones y usuarios nuevos:** ZTNA permite una mayor seguridad y agilidad en entornos que cambian rápidamente con usuarios que van y vienen. Ponga en marcha nuevas aplicaciones de forma rápida y segura, inscriba o retire fácilmente usuarios y dispositivos, y obtenga información detallada sobre el estado y el uso de las aplicaciones.

En resumen, las ventajas de ZTNA con respecto a las soluciones VPN de acceso remoto tradicionales incluyen:

1. **Confianza cero**: ZTNA se basa en el principio de confianza cero, es decir, no confiar en nada y verificarlo todo. Al tratar en la práctica a cada usuario y dispositivo como su propio perímetro y al evaluar y verificar constantemente la identidad y el estado de seguridad para obtener acceso a las aplicaciones y los datos corporativos, se mejora considerablemente la seguridad y la microsegmentación. Los usuarios solo tienen acceso a las aplicaciones y los datos definidos explícitamente por sus políticas, lo que reduce el movimiento lateral y los riesgos que conlleva.
2. **Estado de seguridad del dispositivo**: ZTNA integra el cumplimiento y el estado de los dispositivos en las políticas de acceso, lo que le da la opción de excluir los sistemas no conformes, infectados o comprometidos del acceso a las aplicaciones y los datos corporativos, eliminando así un importante vector de amenazas y reduciendo el riesgo de robo o fuga de datos.
3. **Funciona en cualquier lugar**: ZTNA no está vinculado a redes específicas, por lo que puede funcionar con la misma eficacia y seguridad desde cualquier red, ya sea en casa, en un hotel, en una cafetería o en la oficina. La gestión de la conexión es segura y transparente, independientemente de dónde se encuentren el usuario y el dispositivo, lo que hace que la experiencia sea ágil sin importar dónde esté trabajando el usuario.
4. **Más transparente**: ZTNA ofrece una experiencia de usuario final fluida y sin fricciones, ya que establece automáticamente conexiones seguras bajo demanda en segundo plano a medida que se necesitan. La mayoría de los usuarios ni siquiera serán conscientes de la solución ZTNA que está ayudando a proteger sus datos.
5. **Mayor visibilidad**: ZTNA puede ofrecer una mayor visibilidad de la actividad de las aplicaciones que puede ser importante para el seguimiento del estado de las mismas, la planificación de la capacidad y la gestión y auditoría de las licencias.
6. **Administración más sencilla**: las soluciones ZTNA suelen ser mucho más eficientes y limpias y, por tanto, más fáciles de desplegar y gestionar. También pueden ser más ágiles en entornos que cambian rápidamente, con usuarios que entran y salen, lo que hace que la administración diaria sea una tarea rápida y sencilla y no un trabajo a tiempo completo.

Guía para la adquisición de soluciones: Qué debe ofrecer una solución ZTNA

Al examinar la lista de comprobación obvia de plataformas compatibles con clientes, puertas de enlace y proveedores de identidad, tenga en cuenta estas importantes funciones al comparar las soluciones ZTNA de diferentes proveedores:

Solución gestionada e implementada en la nube

La gestión en la nube ofrece enormes ventajas, desde la posibilidad de ponerse en marcha al instante hasta la reducción de la infraestructura de gestión, pasando por el despliegue y la inscripción y permitir el acceso en cualquier lugar. Una de las principales ventajas de la gestión en la nube es poder conectarse y empezar de inmediato, sin necesidad de añadir servidores de administración o infraestructura adicionales. La gestión en la nube también ofrece un acceso seguro e instantáneo desde cualquier lugar y en cualquier dispositivo, lo que permite trabajar de la forma que se desee. También facilita la inscripción de usuarios nuevos dondequiera que se encuentren en el mundo.

Integración con sus otras soluciones de ciberseguridad

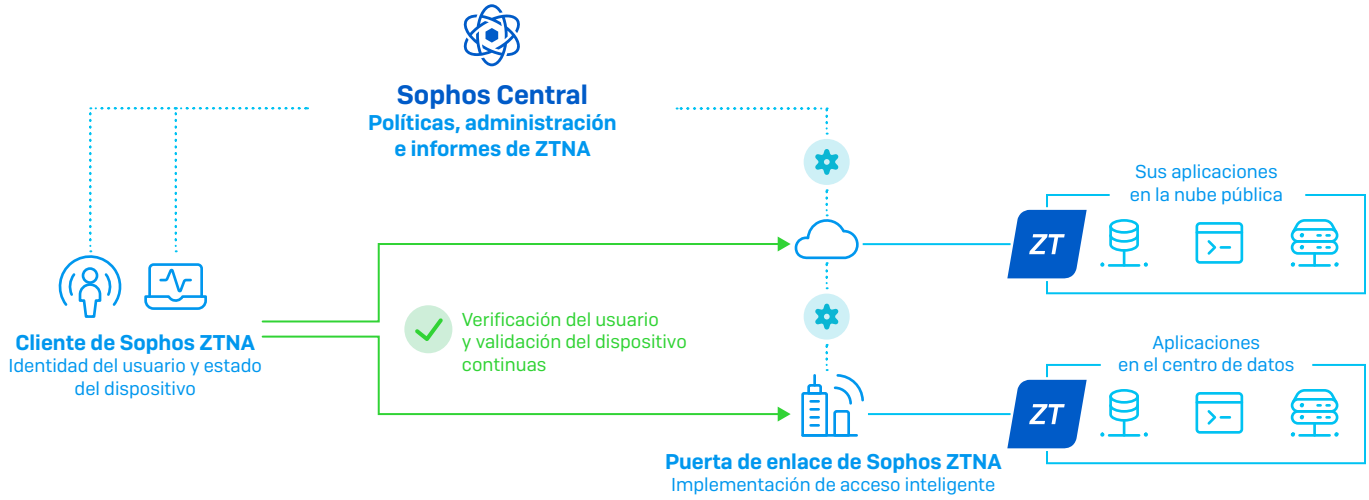
Si bien la mayoría de soluciones ZTNA pueden funcionar perfectamente como productos independientes, existen importantes ventajas si se cuenta con una solución estrechamente integrada con los demás productos de ciberseguridad, como el firewall y los endpoints. Una consola de gestión en la nube común e integrada puede ser una fuerza multiplicadora para usted o su equipo. Usar un único panel de control intuitivo para gestionar toda la seguridad TI, incluida la solución ZTNA, en un solo lugar, puede reducir el tiempo de formación y los gastos de gestión diarios. También puede aportar información única sobre sus diversos productos de seguridad TI, especialmente si comparten telemetría, lo que refuerza enormemente la seguridad y ofrece una respuesta en tiempo real cuando una amenaza o un dispositivo comprometido entran en la red. Pueden operar de forma conjunta para responder instantáneamente a la presencia de un ataque o una amenaza y evitar que se desplace lateralmente, se propague o robe datos.

Experiencia de usuario y de gestión

Asegúrese de que la solución que contempla ofrezca una excelente experiencia para el usuario final y además facilite la administración y la gestión. Actualmente, con el aumento de usuarios que teletrabajan desde cualquier parte del mundo, la inscripción y la configuración eficientes de los dispositivos es fundamental para que los nuevos usuarios sean productivos lo antes posible. Preste atención a cómo se despliega el agente ZTNA y a si resulta fácil añadir usuarios nuevos a las políticas. Asegúrese también de que la solución en la que invierta ofrezca una experiencia fluida y sin fricciones para los usuarios finales y proporcione la visibilidad que usted espera, como información detallada en tiempo real de la actividad de las aplicaciones que le ayude a ser proactivo a la hora de identificar los periodos de demanda máxima, la capacidad, el uso de licencias e incluso problemas de las aplicaciones.

Sophos ZTNA

Sophos ZTNA se ha diseñado desde el principio para que el acceso a la red de confianza cero sea fácil, integrado y seguro. Sophos ZTNA se distribuye y gestiona en la nube y se integra en Sophos Central, la plataforma de generación de informes y gestión de ciberseguridad en la nube en la que más confía el mundo. Desde Sophos Central, no solo puede gestionar ZTNA, sino también sus dispositivos Sophos Firewall, endpoints, protección de servidores, dispositivos móviles, seguridad en la nube, protección del correo electrónico y mucho más.



Sophos ZTNA también es único porque se integra perfectamente con Sophos Firewall y los endpoints de Sophos Intercept X. Esto permite sacar partido de la Seguridad Sincronizada y Security Heartbeat para compartir el estado de los dispositivos entre el firewall, el dispositivo, ZTNA y Sophos Central a fin de responder automáticamente a las amenazas o a los dispositivos no conformes. Limite automáticamente el acceso y contenga los sistemas comprometidos hasta que se limpien.

Los clientes de Sophos coinciden en que las ventajas de ahorro de tiempo con una solución de ciberseguridad de Sophos totalmente integrada son enormes. Afirman que utilizar el conjunto de productos de Sophos, gestionados desde Sophos Central, y servirse de la Seguridad Sincronizada para la identificación y respuesta automáticas a amenazas es como duplicar el tamaño de su equipo de TI. Por supuesto, Sophos ZTNA funcionará con los productos de seguridad de cualquier otro proveedor, pero es único al trabajar mejor junto al resto del ecosistema de Sophos para ofrecer ventajas tangibles en el mundo real en cuanto a visibilidad, protección y respuesta.

Más información en

es.sophos.com/ztna

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

21-10-07 ES (DD)

SOPHOS