RESUMEN EJECUTIVO

¿Son sus oficinas remotas una puerta abierta a los ciberataques?

Por qué el aumento de la exposición, los recursos limitados y el aumento de los costes exigen una solución SD-Branch segura

Resumen

Los métodos tradicionales para implementar y mantener la seguridad en las oficinas remotas se han vuelto ineficaces, caros e imposibles de gestionar. Una solución SD-Branch puede ser la piedra angular para una seguridad sin límites en entornos empresariales distribuidos.

Un auge de los puntos de exposición

Los investigadores de amenazas de Capture Labs de SonicWall registraron 9 900 millones de ataques de *malware* en 2019. Durante los últimos cinco años, los ciberdelincuentes han avasallado a las organizaciones con un ingente volumen de ataques. Su objetivo era sencillo: lanzar una red lo más grande posible y recoger los frutos. Y a medida que las defensas cibernéticas han evolucionado, los ataques se han vuelto más selectivos, con mayor grado de éxito.

Además, el panorama de las redes y la seguridad está experimentando una transformación digital con el auge de los dispositivos móviles e IoT. De ahí que haya una tendencia a que las empresas confíen en los clientes móviles, creando redes «mobile-first». Otro catalizador de este cambio es la migración a la nube y la adopción de aplicaciones en la nube. Con el traslado a la nube de aplicaciones críticas para el negocio como MS Office y dado que las empresas se aprovechan de aplicaciones en la nube como Salesforce o Workday para sus tareas diarias, resulta esencial proteger estas aplicaciones en la nube. Esta transformación digital aumenta la demanda de aparatos de alto rendimiento que puedan estar a la altura de las crecientes demandas de datos.

El coste cada vez mayor de la conectividad

Las oficinas principales y remotas que utilizan la tecnología *Mobile First* dependen en gran medida de aplicaciones con un gran ancho de banda para realizar las actividades diarias. Puede ser algo tan simple como reproducir un vídeo u otro contenido o trabajar en Office 365. De estas aplicaciones con un gran ancho de banda, algunas pueden ser críticas para el negocio, mientras que otras no. Es esencial segregar este tráfico de manera eficiente o su coste será prohibitivo: imagínese tener que hacer retornar todo el tráfico de la oficina remota a través de costosos enlaces MPLS hasta la sede central corporativa.

Afortunadamente, los gastos se pueden reducir utilizando el acceso a Internet de bajo coste para el tráfico de datos no críticos, mientras que el tráfico de datos críticos para el negocio se puede priorizar mediante un mecanismo dinámico de selección de rutas. Sin embargo, algunas de estas aplicaciones, críticas para la operación de una empresa o sucursal distribuida, requerirían una conectividad redundante para garantizar un funcionamiento constante.

Una forma de garantizar una conectividad redundante para estas sedes remotas consiste en tener una solución que proporcione una alta disponibilidad y unas WAN de alto rendimiento con equilibrio de carga WAN. Esto puede lograrse utilizando tecnología WAN definida por software (SD-WAN).

Mediante el uso de un acceso a Internet de bajo coste (banda ancha, 3G/4G/LTE, fibra), las organizaciones pueden sustituir de forma rentable las costosas tecnologías de conexión WAN, como MPLS, por SD-WAN. Sin embargo,

proporcionar todo esto al tiempo que se gestiona toda la solución de seguridad de red desde un único panel a menudo resulta difícil.

Lidiar con unos recursos cada vez más escasos

El coste de la seguridad convencional es cada vez más prohibitivo y la escasez de personal cualificado se agrava. Los limitados recursos presupuestarios y de personal no pueden seguir el ritmo y han creado una brecha comercial en materia de ciberseguridad.

Los productos de múltiples puntos hacen que las oficinas remotas tengan dificultades para implementar, configurar y gestionar la solución y para diagnosticar sus problemas. Tener una pila de seguridad integral puede unificar los *firewalls*, los *switches*, los *access points*, la seguridad en la nube y los clientes *end-point* para proporcionar una gestión a través de un único panel que aumente la visibilidad y el control entre productos. Esta pila de seguridad integral ofrece una posición de seguridad sólida y unificada.

Es fundamental que cambie la forma en la que mantiene las redes. Puede seguir el ritmo de esta transformación digital ofreciendo una posición de seguridad sólida. No ofrecer una posición de seguridad unificada dará lugar a que las organizaciones tengan dificultades para gestionar y controlar el creciente número de dispositivos en la red. Algunas amenazas no se identificarían y las empresas se verían obligadas a adoptar un enfoque reactivo en lugar de uno proactivo.

Además, la implementación a escala puede ser difícil sin tecnologías como la implementación Zero Touch. Los técnicos tendrían que desplazarse a las sucursales para configurar manualmente cada uno de estos dispositivos. Esto se suma al coste general y al tiempo dedicado a implementar la solución en las oficinas remotas, tal vez distribuidas por todo el mundo.

Además, las sedes remotas, al igual que la sede central corporativa, deben ofrecer un acceso inalámbrico seguro que proporcione un alto rendimiento y una experiencia de usuario superior. Dado que la tecnología Wi-Fi está generalizada, tanto los empleados como los visitantes esperan un rendimiento rápido y fiable de la conexión Wi-Fi.

Por qué necesita una solución SD-Branch

En la actualidad, la evolución de la tecnología en la oficina remota es fundamental. Las oficinas remotas tradicionales no pueden estar a la altura de las crecientes demandas del cada vez mayor número de dispositivos móviles e IoT. Con la proliferación de dispositivos, la gestión y la seguridad se convierten en un desafío, ya que pueden necesitar políticas diferentes. Contar con una política unificada en su LAN y WAN desde un único panel (SPOG) resulta fundamental.

Además, la gestión del SPOG puede proporcionar análisis exhaustivos en todo el ecosistema de seguridad. A medida que la adopción de la nube avanza, la conectividad WAN entre las oficinas remotas debe diseñarse de manera inteligente para aprovechar los enlaces de Internet más baratos frente a los enlaces MPLS más caros, además de permitir la Implementación Zero-Touch..

Esto aporta agilidad operativa. Las organizaciones pueden implementar y desplegar rápidamente dispositivos con capacidad de Implementación sin necesidad de intervención, eliminando o reduciendo la necesidad de que personal de TI cualificado visite múltiples sucursales para configurar e implementar estas soluciones. Para garantizar la continuidad, la integración y la escalabilidad, las organizaciones deberían buscar de manera óptima una gestión SPOG simplificada con servicios de un único proveedor.

Una solución SD-Branch aumenta la SD-WAN para ofrecer el siguiente nivel de conectividad y flexibilidad. La solución SD-Branch transforma la tecnología SD-WAN en una solución personalizada para su implementación en las oficinas remotas. Añade más funciones y va más allá de encargarse de la conectividad entre sedes remotas. SD-Branch engloba SD-WAN, conectividad LAN y seguridad. Además, la implementación Zero-Touch y la gestión SPOG disminuyen la necesidad de personal de TI, lo que reduce aún más los costes operativos.

Conclusión

Las empresas distribuidas tienen dificultades para proteger las oficinas remotas debido a un mayor número de puntos de exposición, los recursos limitados y el aumento de los costes. Todo esto contribuye a una creciente brecha comercial en materia de ciberseguridad.

Una solución eficaz combina la agilidad de SD-Branch con la seguridad integral, la segmentación de la red y el cumplimiento. Esto permite aplicar políticas unificadas en todo el ecosistema de la red, proporcionando controles de seguridad pormenorizados para identificar y evitar que los ataques más sigilosos y nunca antes vistos pongan en peligro su red.

SonicWall considera que una solución SD-Branch constituye una piedra angular para la seguridad sin límites y sin perímetro en la era hiperdistribuida. La solución SD-Branch de SonicWall protege la conectividad y transforma la experiencia del usuario en la oficina remota ofreciendo una plataforma integrada que les permite aprovechar una conectividad más económica (SD-WAN), permitir un enfoque BYOD, adoptar aplicaciones SaaS y conectarse a la sede central o a otras sedes. Integra SD-WAN, implementación Zero-Touch, gestión desde un único panel, visibilidad unificada y detección de amenazas, *firewalls* de última generación, *switches* seguros, *access points* inalámbricos, seguridad de *endpoint* y seguridad de aplicaciones en la nube.

Más información: Lea nuestro Resumen de la solución SD-Branch de SonicWall.

Acerca de SonicWall

SonicWall ofrece Boundless Cybersecurity (sin Perímetro) para la era hiperdistribuida y una realidad laboral en la que todo el mundo usa tecnología móvil, a distancia y poco segura. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y posibilitar una economía revolucionaria, SonicWall cierra la brecha comercial en materia de ciberseguridad para empresas, gobiernos y pymes de todo el mundo. Para obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 (Estados Unidos)
Encontrará más información en nuestro sitio web.
www.sonicwall.com

ExecutiveBrief-AreYourBranchSites-US-VG-1980