FORTINET
NSE Training Institute

NSE 2 SD-WAN Scripts—Spanish Version

¡Hola! En esta clase, veremos qué son las redes SD-WAN y cómo han evolucionado.

Una SD-WAN es una red de área extensa definida por software (*software-defined wide-area network*), que aprovecha las WAN corporativas y la conectividad multinube para ofrecer un rendimiento de aplicaciones de alta velocidad.

Anteriormente, las organizaciones compraban y operaban servidores propios para ejecutar aplicaciones y almacenar datos empresariales críticos. En consecuencia, tenían un gasto de capital inicial y debían contratar un equipo de técnicos expertos para operar los servidores. Si bien eran costosos, las ventajas competitivas con respecto a quienes no informatizaban sus actividades hacían que valieran la pena. Uno de los retos iniciales fue hacer que estos servidores estuvieran disponibles en varias redes distribuidas geográficamente, conocidas como redes de área local (*local area networks*, LAN).

Recordemos que una WAN es una red informática que abarca un área geográfica extensa y que, en general, consta de dos o más redes LAN. Por ejemplo, si Acme Corporation abarcara varias ciudades y continentes, cada uno con una red de área local propia, ¿cómo se conectarían estas LAN para que alguien en una oficina de Londres pudiera acceder a un servidor de base de datos en Singapur? Normalmente, las empresas conectaban las redes LAN por medio de un único proveedor de servicio dedicado. Aunque era caro, este método les permitía controlar y proteger la conexión y, al mismo tiempo, brindar acceso a recursos críticos. Sin embargo, tenía sus limitaciones. Su único punto de conectividad sufría cortes frecuentes, por lo que no era fiable. Además, como había una demanda cada vez mayor para alojar aplicaciones empresariales en la nube, conocidas como software como servicio (*software as a service*, SaaS), la latencia elevada se convirtió en un problema. Las aplicaciones de este tipo, como Salesforce, Dropbox y Google Apps, y el mayor uso de conferencias de video y voz agravaron la congestión. Para ampliar la conectividad, las empresas comenzaron a utilizar múltiples proveedores o a buscar redes de banda ancha más accesibles y otros medios de conectividad a internet. La tendencia hacia el aumento de las conexiones híbridas y el crecimiento de las aplicaciones en la

nube para respaldar decisiones empresariales inteligentes derivaron en la primera generación de redes de tipo SD-WAN.

Las empresas incorporaron múltiples enlaces dedicados y balanceadores de carga por tráfico de aplicación, según el ancho de banda disponible. Aunque este enfoque parecía resolver unos pocos problemas relacionados con el ancho de banda, sumó un producto más para resolver otro reto de la red. Estos productos puntuales escalan la complejidad de la infraestructura de red. ¿Por qué? Porque al incorporar diversos productos de diversos proveedores, que tienen sus propias consolas de administración y que no se integran del todo a otros productos, la tarea de los administradores de seguridad de TI se vuelve una pesadilla. Aun así, la primera generación de redes SD-WAN resolvió una necesidad acuciante para las empresas. Las técnicas básicas de balanceo de carga permitieron a la red tomar decisiones empresariales inteligentes sobre aplicaciones en enlaces WAN híbridos, incluido el proveedor de servicio, la banda ancha y la evolución a largo plazo (*long-term evolution*, LTE), un estándar de comunicaciones inalámbricas por banda ancha para dispositivos móviles y terminales de datos.

Gracias a la identificación precisa de aplicaciones, la visibilidad del rendimiento de la red y una transición fiable del tráfico de aplicaciones entre los enlaces WAN de mejor rendimiento, las redes SD-WAN pasaron a ser las preferidas de todas las empresas para este tipo de tecnologías.

Sin embargo, la seguridad seguía siendo un aspecto importante para tener en cuenta. Incluso después de la adopción de las redes SD-WAN, las empresas continuaron enviando la información confidencial y el tráfico de las aplicaciones críticas a centros de datos por razones de seguridad. La otra opción era instalar un firewall complejo para inspeccionar el acceso directo a internet. Esto sumó otro producto puntual para fines de seguridad, lo que hizo que la red fuera aun más compleja y más difícil de administrar, a la vez que retrasó la adopción de la nube.

Las empresas tenían la necesidad de hacer frente a este reto mediante la integración de las funcionalidades de seguridad y de redes en un único dispositivo SD-WAN que fuera seguro. Esto les permitió reemplazar los múltiples productos puntuales por un único dispositivo de

seguridad potente, más económico y de fácil administración. Este enfoque de seguridad sólido contribuyó a que las aplicaciones en la nube fueran más accesibles para las empresas, que tuvieran una latencia menor y una conexión directa a internet para garantizar su rendimiento óptimo y una mejor experiencia de usuario. Las continuas comprobaciones del rendimiento de la red aseguraban que se eligiera el mejor enlace WAN disponible, según los acuerdos de nivel de servicio de la aplicación definidos por el usuario. Si un enlace en particular se degradaba, el dispositivo SD-WAN sabía que debía cambiar la conexión al enlace WAN de mejor rendimiento.

Hoy, en las redes SD-WAN seguras, los flujos de trabajo intuitivos sujetos a las políticas de la empresa facilitan la configuración y administración de las necesidades con respecto a las aplicaciones, y tienen la flexibilidad para priorizar las aplicaciones críticas. Una consola de administración centralizada brinda una telemetría y una visibilidad unificada y transparente para identificar y resolver problemas de red con una plantilla de personal de TI reducida. El análisis exhaustivo de la utilización del ancho de banda, la definición de la aplicación, la selección de la ruta y el escenario de amenazas de seguridad no solo proporciona una visibilidad de la red extendida sino que, además, ayuda a los administradores a rediseñar las políticas rápidamente y de acuerdo con estadísticas históricas, a fin de mejorar el rendimiento de la red y de las aplicaciones.

En términos generales, los resultados positivos de una solución de SD-WAN segura son la simplificación, la consolidación y la reducción de costos. Al mismo tiempo, responden a la necesidad de un rendimiento óptimo de las aplicaciones y de una mejor experiencia de usuario, tanto para las aplicaciones empresariales como para las de software como servicio (SaaS) y de Comunicaciones unificadas como servicio (UCaaS). Los tiempos de ejecución de las tareas de análisis y telemetría ayudan a los equipos de infraestructura a coordinar y resolver problemas de manera más ágil, lo que reduce la cantidad de solicitudes de soporte y de cortes en la red.

Fortinet introdujo el término Secure SD-WAN, cuyo núcleo es FortiGate®, el firewall de última generación (NGFW) de Fortinet. Además del dispositivo FortiGate®, la solución Secure SD-WAN incluye otras características de red avanzadas.

Gracias por su tiempo, y no olvide responder las preguntas a continuación.