TechTarget

Cómo cumplir con los requisitos de una buena red

Ante el crecimiento de la movilidad, nube, analítica e internet de las cosas, las redes deben cumplir con ciertos requisitos de flexibilidad, escalabilidad, disponibilidad y seguridad. ¿Su red está lista?

Transformando el modelo de las redes en centros de datos

El manejo de las redes en la industria se ha visto transformado por dinámicas como las soluciones SDN, la puesta en común de diversos recursos de red, las superposiciones, el tráfico de información este-oeste y la computación en nube. Todos estos factores exigen una nueva forma dentro del modelo de redes tradicionales basadas en chasis de tres niveles, lo cual abre el camino para considerar las siguientes opciones:

1. **Replantear el rol del chasis:** Cambiar las arquitecturas de los centros de datos convencionales implica replantear el rol de los switches ante los chasis monolíticos que prevalecen. Las arquitecturas que utilizan interruptores fijos de menor tamaño como columna vertebral se están convirtiendo en la tendencia para los centros de datos.

   El modelo Active Fabric, por ejemplo, elimina la complejidad de los conocimientos tradicionales respecto a las redes de tres niveles y ofrece una solución más eficiente, económica y escalable. Gartner ratifica esto en su estudio "Rightsizing the Enterprise Data Center Network", el cual señala que los switches de factor de forma fija pueden reducir la larga dependencia que tiene la red central del data center en los grandes y costosos switches basados en chasis.

2. **Simplificar la gestión:** De poco sirve hacer más eficientes los componentes que forman el tejido de la red del centro de datos, si no se les puede gestionar de manera eficiente. Con el próximo lanzamiento de Active Fabric Manager, la configuración, implementación, administración y seguimiento del funcionamiento de la plataforma se verá simplificado y automatizado, permitiendo afianzar este modelo de centro de datos.

Active Fabric Manager permite una programación de servidores conectados a la red mediante secuencias de comandos y otras herramientas de uso común. Su interfaz guía a los usuarios desde el diseño de la red —a través del esquema de conexión— hasta la configuración de los switches, simplificando las repeticiones y el tiempo de consumo en las tareas manuales mediante un solo panel, que brinda una administración visible de toda la red.

3. **Desvincular el plano de control y los elementos del plano de datos dentro de los switches:** Los usuarios están buscando superposiciones de red dentro de una variedad de productos para conseguir este tipo de funcionalidad.

4. **Desacoplar el plano de datos entre hardware y software:** El paso final en esta nueva configuración sería desacoplar el software de plano de datos desde el interruptor físico. Esto permitiría mezclar y combinar aspectos relacionados con el software de plano de datos de diferentes proveedores con switches físicos.

Así, se transforma la cadena de valor orientada a los centros de datos, desde la adquisición de soluciones de redes, hasta la implementación, administración y soporte del crecimiento global con una arquitectura de red totalmente desagregada, basada en switches.

Esto facilitaría un cambio hacia la creación de redes abiertas, que dirigir los ecosistemas de redes a un nuevo nivel de potencia y rendimiento. ¿El siguiente paso? El diseño de redes integradas verticalmente. —*Oscar Valencia*

¿Cuál es la mejor topología de red para el centro de datos?

Conozca las principales *topologías de la red de centros de datos y eche un vistazo a otras alternativas que esperan tras bastidores.*

No hay una sola mejor topología de red de centros de datos para todas las empresas. Una vez que entienda las principales opciones de topologías, es fácil ver cuál funciona mejor para su tráfico de red u obtener ideas para solucionar problemas en su red existente.

¿Cuáles son las topologías importantes de red del centro de datos que debe conocer?

Las redes actuales de centros de datos son principalmente topologías de tres capas. Esto comprende un núcleo de switches de centros de datos que se conectan entre sí y con el proveedor (o los proveedores) de redes externo(s), una capa de usuario o de acceso y la capa de agregación entre estos dos que mueve información principalmente al norte y al sur.

Leaf-spine es una topología de red de centro de datos que es popular en los centros de datos que tienen más tráfico de red de este a oeste. Esta topología aumenta la capa spine con más switches para manejar el tráfico en el centro de datos, tal como el tráfico de datos de la red de área de almacenamiento.

TOPOLOGÍAS DE RED ALTERNATIVAS Y EMERGENTES

Estos diseños abordan cuestiones específicas para aplicaciones específicas. Alternativamente, los nuevos diseños reformulan la teoría del diseño de la red completamente, moviendo la inteligencia de red a los hosts y usando esos anfitriones como nodos de reenvío, además de switches tradicionales. Las redes líderes podrían no necesitar ese tipo de capacidad hoy en día, pero las tendencias emergentes a menudo gotean hacia las tendencias

principales. Si bien podrían no ser lo que hay ahora, podrían ser lo que viene.

Hay algunas otras topologías de redes de centros de datos generalmente aceptadas más allá de la red de tres capas tradicional y las opciones de "hojas de espinas" (*leaf-spine*). Si bien se encuentran con menor frecuencia en las implementaciones del mundo real, son relevantes y bien comprendidas.

***Leaf-spine* multinivel.** Un enfoque para escalar una red leaf-spine horizontalmente, mientras se mantiene una relación de sobresuscripción aceptable, es añadir una segunda capa de hoja (leaf) vertical.

Hipercubo. Una red hipercubo 3D simple es en realidad solo un cubo: una caja de seis caras con switches en cada esquina. Un hipercubo 4D (también conocido como teseracto o tesseract) es un cubo dentro de un cubo, con los switches en las esquinas conectándose entre sí —el cubo interior se conecta al cubo exterior en las esquinas. Los hosts se conectan a los switches en el cubo exterior. Una organización necesita entender sus flujos de tráfico de aplicaciones en detalle para saber si vale la pena considerar una topología hipercubo o no.

Toroidal. Este término se refiere a cualquier topología en forma de anillo. Un toroide (torus) 3D es una red interconectada de anillos altamente estructurada. Los toroides son una opción popular en los entornos de computación de alto rendimiento y pueden confiar en los switches para interconectarse entre nodos de computación.

Medusa (*Jellyfish*). La topología de Medusa es en gran parte aleatoria. En este diseño, los switches están interconectados con base en la preferencia del diseñador de la red. En los estudios de investigación, las pruebas de los diseños de Medusa resultaron en 25% más de capacidad que las topologías de red tradicionales.

Scafida. Las topologías de red libres de escala o Scafida son algo así como las Medusa respecto a que hay aleatoriedad sobre ellas, pero, paradójicamente, en ese azar se hace evidente más estructura. La idea es que ciertos switches terminan como sitios hub densamente conectados, similares a la forma en que una aerolínea gestiona los patrones de vuelo.

DCell. Muchos servidores se embarcan con múltiples tarjetas de interfaz de red (NIC). Algunas de estas NIC se conectan en una celda directamente desde un servidor a otro, mientras que otras se interconectan a través de un switch a otras células. DCell asume que un servidor tiene cuatro o más tarjetas de red.

FiConn. Similar a DCell, FiConn utiliza una jerarquía de interconexiones y células de servidor a servidor, pero solo asume dos NIC.

BCube. Como DCell y FiConn, Bcube utiliza los puertos de servidor adicionales para la comunicación directa, pero está optimizada específicamente para centros de datos modulares que se implementan como contenedores de embarque. Microsoft, el poder detrás de BCube, construyó el protocolo de enrutamiento de origen Bcube para gestionar el reenvío a través de esta topología de red de centro de datos.

CamCube. Esta topología es efectivamente un toroide 3D ejecutando CamCubeOS de Microsoft en la parte superior. El propósito es optimizar el flujo de tráfico a través del toroide mientras está siendo utilizado para interconectar grupos de hosts. CamCubeOS asume que los paradigmas de reenvío de red tradicionales no son eficaces en esta aplicación y los reemplaza.

Mariposa (*Butterfly*). La Mariposa plana de Google es una construcción de red específica similar a un tablero de ajedrez. En esta rejilla de switches, el tráfico puede moverse a cualquier switch en una dimensión dada. El objetivo es reducir el consumo de energía, una gran preocupación de Google.

—Ethan Banks

Es tiempo de que la red esté lista para la nube

Conforme las redes empresariales modernas se mueven hacia el mundo de la computación en nube pública, ciertos hechos salen a la luz. Uno es que los administradores de red empresarial se ven obligados a trabajar con proveedores de nube pública para asegurar que la red sigue soportando las necesidades del negocio. Esto significa que algunos de los fundamentos de TI están experimentando cambios.

En primer lugar, las arquitecturas de red de nube deben ser más flexibles: las redes estáticas limitan drásticamente el uso de la nube. En segundo lugar, los servicios de red necesitan ser desacoplados de una sola ubicación física, ya que la entrega de datos, cómputo e interfaces de usuario son ahora omnipresentes. Por último, muchos recursos de red necesitan ser abstraídos para que el aprovisionamiento pueda ser automatizado y orquestado.

LA NUEVA ARQUITECTURA DE RED DE NUBE

La realidad es que muchas empresas no están preparadas para aprovechar las nubes públicas o híbridas. Con los años, la infraestructura de red de la empresa no ha recibido los fondos necesarios para actualizar la infraestructura para soportar la velocidad y las capas de gestión necesarias.

Más a menudo, la naturaleza estática de las redes tradicionales limita la capacidad de los administradores de red para adaptar sus redes a la nube.

Los requisitos de red para el uso exitoso de la nube son los siguientes:

Al trabajar con recursos de nube, las redes son más eficaces cuando pueden ser desconectadas de los recursos físicos o geografías.

- La capacidad de asegurar segmentos específicos de la red en diferentes formas, para satisfacer los requisitos de los datos que fluyen a través de la red. En muchos casos, esto requiere el cifrado basado en red. Las redes deben configurarse para satisfacer una variedad de requisitos de rendimiento y seguridad.

- La capacidad de proporcionar priorización de red (conformación de paquetes) para aplicaciones y datos específicos que fluyen a través de la red. Si las nubes públicas contienen datos críticos para el negocio, esos sistemas deben tener acceso prioritario a los recursos de red, incluyendo la tolerancia a fallos y subsistemas resilientes.

- La capacidad de tener redes conscientes de las aplicaciones. Las nubes privadas, las nubes públicas y los sistemas tradicionales usan la red de diferentes maneras, dependiendo de la aplicación, los datos y la interfaz de usuario y cómo se comunican entre sí y con los servidores basados en la nube. Una red que puede ajustarse a esos patrones de uso es, sin duda, más eficaz cuando la computación en nube entra en juego.

CONFIGURACIÓN DE LOS RECURSOS DE RED

Cuando se trabaja con recursos de nube, las redes son más eficaces cuando pueden ser desconectadas de los recursos físicos o geografías. Esto apoya el concepto de la computación ubicua, uno de los principios de la computación en nube. Las ubicaciones de las instancias de servicios se ocultan de las máquinas o de los usuarios que acceden a ellas, haciendo la ubicación física insignificante.

La computación ubicua y las redes que la soportan se centran en eliminar la complejidad de la computación y aumentar la eficiencia. Como resultado, el acceso a las instancias del servidor podría ir a cualquier número de diferentes lugares físicos (si está permitido) en la búsqueda de los recursos disponibles.

Las aplicaciones, por ejemplo, podrían tener más de cien instancias de servidor de cómputo ejecutándose en 12 centros de datos diferentes, conectados a cuatro servidores de datos que se ejecutan en dos centros de datos diferentes. Todos estos servidores están conectados, ya sea usando la infraestructura de red que ofrece el proveedor de servicios de nube, o necesitan al arquitecto de la infraestructura empresarial de la misma manera.

Las empresas deben ser capaces de configurar los servicios de red para proporcionar la flexibilidad necesaria para soportar la computación de nube ubicua.

ABSTRACCIÓN DE LOS RECURSOS

La mayoría de los cambios necesarios se reducen a la capacidad de gestionar las redes a través de una capa de abstracción. Esto significa que los recursos físicos no necesitan ser gestionados como lo eran en el pasado. En lugar de ello, los profesionales de redes pueden utilizar herramientas de gestión y automatización para agrupar objetos que representan agrupaciones lógicas de recursos, no dispositivos físicos distribuidos ampliamente.

La idea es ocultar la complejidad que la computación en la nube trae a los administradores de red. En lugar de tener que lidiar con miles de servidores dispersos en toda la infraestructura de la empresa y la de varios proveedores de nube pública, el concepto es gestionar aplicaciones, datos y similares como representaciones lógicas individuales. Con este enfoque, las empresas pueden gestionar mejor los recursos, ya sea que estén en las instalaciones, en la nube o en ambos.

Los administradores de red encontrarán que la computación en nube añade retos adicionales. Con un poco de planificación y mayores presupuestos, sin embargo, la adición de recursos basados en la nube a la red debe ser una actualización eficiente, que reduce en gran medida los costos y aumenta la agilidad para el negocio. Si su organización no ha creado un plan de computación en la nube aún, ahora es el momento. —*David Linthicum*

Defensa a profundidad, mecanismo para asegurar la red

La defensa en profundidad describe el concepto de protección de una red de ordenadores con una serie de mecanismos de defensa organizados de tal manera que, si uno de ellos falla, otro está disponible para tomar su lugar. Este consejo se centra en un ejemplo de una implementación de profundidad práctica de defensa que utiliza las tecnologías existentes y explora cómo pueden ser vinculadas para formar una red de arquitectura de seguridad empresarial amplia y efectiva.

Con el fin de demostrar cómo implementar la defensa en profundidad, consideremos el siguiente escenario, lo cual es una configuración común de una empresa de IT. Muchas empresas utilizan a terceros como proveedores de infraestructura de alojamiento, y lo hacen por varias razones.

Mediante el uso de hospedajes externos, las empresas son capaces de aprovechar bien el espacio tradicional o la potencia del modelo (también llamado colocación) en un entorno físicamente seguro en el proveedor de alojamiento, mientras gestionan el sistema ellos mismos, o compran los servicios gestionados de hosting del proveedor, que incluyen servicios de redes, de sistemas y de seguridad.

Estos entornos suelen estar diseñados para albergar los sistemas de acceso públicos de una empresa, que podrían variar desde los servicios de correo o de transferencia de archivos para usuarios corporativos, hasta la plataforma de comercio electrónico de la empresa.

Al igual que con cualquier colocación o implementación gestionada, la seguridad juega un papel importante en el entorno. Un enfoque típico para el diseño de la seguridad de un entorno comienza con la red. Para los propósitos de esta discusión, supongamos que la empresa está alojando su plataforma de comercio electrónico en este entorno.

La plataforma de comercio electrónico (muy simplificada para esta discusión) consiste en el

nivel web que actúa como el carro de la compra o como un portal de facturación para varias operaciones. Esto, a su vez, está soportado por el middleware (servidores de aplicación) y los niveles de base de datos. El diseño requiere que cada uno de los niveles se encuentre alojado en su propia red dedicada, principalmente las redes locales virtuales de área o VLAN. Esto se realiza generalmente mediante la segmentación de los niveles, utilizando un dispositivo de filtración (como un firewall) en los servidores web en la interfaz de baja seguridad, mientras que los niveles de middleware y la base de datos se alojan en el interfaz de alta seguridad.

Los niveles de middleware y base de datos no son accesibles directamente desde la red pública. En algunos diseños de escenarios, los niveles de middleware y bases de datos están detrás de la misma interfaz de firewall pero en VLANs separadas. En tales escenarios, no hay filtrado de tráfico entre los dos niveles a menos que sea forzado por los conmutadores.

El firewall en este caso actúa como la principal, y potencialmente la única, línea de defensa contra amenazas basadas en Internet. Vamos a utilizar este entorno como base para implementar una estrategia de defensa en profundidad usando tecnologías de seguridad existentes.

DEFENSA EN PROFUNDIDAD EN PRÁCTICA

He tomado un enfoque universal para implementar la seguridad del entorno descrito anteriormente, con el fin de que cada pieza pueda ser implementada independientemente de las demás, dependiendo de los requisitos particulares de cada empresa.

La pieza inicial del rompecabezas de la defensa en profundidad se aplica fuera del entorno de la empresa, en la infraestructura de red del proveedor. Este componente tecnológico es responsable de proteger el entorno contra distribuidores de denegación de servicio (DDoS). La tecnología de mitigación de ataques DDoS consiste típicamente de dos componentes: El primer componente es responsable de detectar un ataque mediante el monitoreo de desviaciones en el flujo normal de tráfico, y el segundo componente es responsable de mitigar el ataque a través de un comportamiento de tráfico aprendido (por ejemplo, un

sistema de gestión de amenazas, o TMS).

La protección contra ataques DDoS se logra a través de desviaciones casi instantáneas del tráfico utilizando el Border Gateway Protocol (BGP) desde el enrutador núcleo hasta el centro de limpieza (TMS) de ataques DDoS. La mitigación de ataques DDoS más eficaz se logra en la infraestructura de un proveedor (contra corriente), por lo que el riesgo de saturación de enlaces y el aumento de los costes de ancho de banda se ven reducidos.

Un firewall es eficaz en la protección contra determinadas amenazas de red, pero, en entornos alojados donde determinados puertos están abiertos a Internet (HTTP (80/tcp) y HTTPS (443/TCP) su eficacia es limitada. En un entorno así, es una buena idea ampliar el firewall con una herramienta firewall de aplicación web (WAF).

La WAF servirá principalmente para proteger el entorno contra específicos ataques a la aplicación, como filtros de scripts de sitios (XSS), inyecciones de código SQL y manipulación de parámetros, entre muchos otros. Estos dispositivos suelen ser configurados linealmente a lo largo del enlace físico entre el firewall y los conmutadores de núcleo de red del entorno hospedado.

Allí, una WAF funciona como un dispositivo de derivación que puede bloquear el tráfico que coincide con ataques en la capa de aplicación conocidos y aprendidos. También tiene la capacidad de dejarlo abierto en el caso de un fallo de hardware, asegurando así que el tráfico continúe fluyendo a los servidores de web. Algunos vendedores de WAF también ofrecen prestaciones de protección y de monitoreo de bases de datos que gestionan las amenazas a las mismas. La protección es ejercida mediante la utilización de agentes, instalados en los servidores que hospedan la instancia de la base de datos.

Como los WAFs suele centrarse en los ataques que se producen en la capa de aplicación, su eficacia en el bloqueo de ataques al centro de la red, como los gusanos de Internet, es limitada. Una WAF puede ser usada en conjunción con un sistema de prevención de intrusiones (IPS), cuyo enfoque principal es la mitigación basada en firma en la capa de red, para aumentar esta deficiencia. Estos dispositivos están disponibles como módulos que pueden ser integrados linealmente con los firewalls y que bloquean las amenazas cuando salen del mismo.

A medida que nos acercamos a la plataforma del servidor, la protección contra amenazas de malware y la vigilancia del sistema de archivos se convierten en algo crucial para una efectiva estrategia de defensa en profundidad. Esto se puede lograr mediante el uso de una combinación de productos antivirus/antimalware convencionales y de sistemas de monitorización de integridad de contenido (CIMS), que rastrean y alertan en tiempo real sobre los cambios del sistema de archivos.

Lo que mantendría todo esto unido sería un sistema centralizado de gestión de registros (Log Management System- LMS), que sirve como un almacén para los registros de estos componentes de seguridad individuales, además de funcionar como un almacén para los registros tradicionales de los servidores. Un LMS también tiene la capacidad de generar alertas en tiempo real sobre filtros de eventos pre configurados, además de proporcionar una interfaz de búsqueda flexible para registros de datos de los distintos componentes de seguridad.

Otra familia de productos que tiene sus raíces en la gestión de registros, llamado sistema de gestión de eventos y de seguridad de la información (Security Information Event Management- SIEM) puede también ser usado en lugar del LMS. El SIEM amplía las capacidades del LMS para proporcionar análisis inteligente y mitigación de amenazas.

COMBINACIÓN DE TODOS LOS ELEMENTOS

Como puede ver, hemos identificado las tecnologías específicas de seguridad que se pueden utilizar para proteger cada componente del entorno alojado de una empresa, empezando con la mitigación de ataques DDoS en la infraestructura del proveedor, seguido de firewall y tecnologías IPS para la protección de la red, de herramientas WAF para la protección de la capa de aplicación, de CIMS para proteger la integridad del sistema de archivos y, finalmente, de LMS, que sirve como depósito de información de registro para los distintos componentes de seguridad y del servidor.

Mediante la práctica de la defensa en profundidad, o incluso implementando algunos de los componentes (por ejemplo, LMS), la empresa habrá dado un paso gigantesco hacia su objetivo de tener una plataforma de seguridad resistente que pueda visualizar en tiempo real las amenazas contra la seguridad. —*Anand Sastry*

Mejores prácticas para la recuperación de la red

Con la recuperación de desastres para redes de área amplia (WAN) o LAN, se debe identificar y satisfacer ciertos criterios antes de elegir un enfoque.

Para las WAN, los criterios clave para la recuperación de la red son:

- Diversidad física a nivel de área local y amplia;
- Disponibilidad de varios proveedores de servicio;
- Ancho de banda escalable que puede adaptarse a requisitos de recuperación de desastres (DR) de emergencia en tiempo real, sin multas.

También debe desarrollar un mapa exacto de la red para identificar cualquier punto único de fallo. Si se utiliza un software o un aparato de optimización de WAN, aproveche las capacidades de respaldo y recuperación que puede ofrecer.

Para las LAN, los criterios clave de recuperación de la red son:

- Cableado de red con ancho de banda suficiente;
- Servidores, switches, routers y hubs de respaldo;
- Suministros de energía de respaldo;
- Vías de cables que corren verticalmente en los elevadores del edificio, y horizontalmente a través de los pisos.

Para las WAN, las pérdidas o daños a los dispositivos de conectividad de red en los edificios interrumpirán el servicio. La pérdida de la conectividad del edificio desde la LAN del operador (por ejemplo, un corte de cable) también hará que la red se caiga. Las interrupciones del servicio de los operadores en la "nube" WAN pueden tener consecuencias de gran alcance para su organización y muchas otras.

Para las LAN, el daño a los servidores, switches, ruteadores, hubs y cableado interno interrumpirá el servicio. La mejor manera de hacer frente a un corte de LAN es tener un mapa detallado de la red

de todos los componentes de LAN. Este puede ser generado por una herramienta de escaneado de red, el cual se puede obtener a partir de productos

Conocer la configuración de cada dispositivo en una red es esencial para la recuperación del dispositivo.

comerciales y de código abierto. El mapa de red de referencia le ayudará a determinar qué dispositivos deben estar en un inventario de componentes LAN de repuesto, como servidores, switches, ruteadores, hubs y un suministro de cables y conectores. Los detalles de configuración para cada dispositivo de la LAN son esenciales para la recuperación de un dispositivo.

Los respaldos de los datos de configuración, mapas de red e inventarios de dispositivos deben ser procesados por adelantado de modo que la información crítica de TI pueda ser accedida en caso de un desastre. Los planes de recuperación de red documentados, con procedimientos detallados para la recuperación de activos WAN y LAN, también son importantes.

—Paul Kirvan

SOBRE LOS AUTORES

ETHAN BANKS *es un profesional de redes que ha diseñado, construido y dado mantenimiento a redes para organizaciones de todo tipo. Es coanfitrión de un programa técnico que cubre el diseño práctico de redes, temas de virtualización, redes definidas por software y protocolos de capas de red.*

PAUL KIRVAN *es un consultor/auditor de TI independiente con más de 25 años de experiencia en continuidad de negocios, recuperación de desastres, seguridad, gestión de riesgos empresarial, telecomunicaciones, auditoría de TI.*

DAVID LINTHICUM *es un experto reconocido en la industria de la nube. Es autor de 13 libros de computación y orador en muchas conferencias de tecnología sobre temas de SOA, cómputo de nube, integración de aplicaciones empresariales y arquitectura empresarial.*

ANAND SASTRY *es un arquitecto de seguridad con experiencia en pruebas de penetración de aplicaciones y red, diseño de arquitectura de seguridad, seguridad inalámbrica, sistemas de detección de intrusos en la red, análisis de malware y sistemas de negación de distribución de servicios.*

OSCAR VALENCIA *es profesional de TI con más de 20 años de experiencia en la venta e integración de soluciones complejas de redes y centros de datos.*

TechTarget

Cómo cumplir con los requisitos de una buena red
es una publicación de SearchDataCenter.Es

Rich Castagna | *Vicepresidente editorial*

Lizzette Pérez Arbesú | *Editora ejecutiva*

Melisa Osores | *Editora adjunta*

Linda Koury | *Director de diseño online*

Neva Maniscalco | *Diseñador gráfico*

Joseph Hebert | *Editor de producción*

Bill Crowley | *Publisher*
BCrowley@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com