

# VIRTUALIZACIÓN

## El camino para gestionar la complejidad de los servicios de red y seguridad



Alberto Domarco  
Consultor Senior de Telindus

**D**urante los últimos años ha ido aumentando el número de componentes y la complejidad de las infraestructuras de interconexión y seguridad de los centros de datos. Hoy en día, a la infraestructura básica se le han añadido multitud de sistemas independientes, como concentradores VPN, balanceadores de carga, aceleradores criptográficos o sistemas IDS. Todas estas herramientas se han ido incorporando para cubrir una demanda creciente de mayores niveles de seguridad, funcionalidades y rendimiento por parte de las organizaciones, pero también han traído consigo un incremento considerable del nivel de complejidad, claramente reflejado a nivel de CAPEX y OPEX de infraestructura.

El caso de los operadores y centros de hosting, que ofrecen sus servicios de alojamiento y aplicativos a múltiples clientes, supone una complejidad adicional que puede llegar a ser inaceptable desde un punto de vista de operatividad, ya que normalmente obliga a mantener infraestructuras de interconexión y seguridad físicamente separadas y 'redundadas' para cada uno de los clientes. En este entorno, la compartición de recursos, como por ejemplo, los sistemas cortafuegos, no es aceptable si no puede garantizarse que un incremento del ancho de banda consumido por un cliente "A" o un ataque contra los sistemas de dicho cliente, no pueden afectar el servicio comprometido

con un cliente "B". Por si esto no fuese suficiente, hay que añadirle la dificultad de aprovisionamiento de servicios. Nuestra era es la del servicio "bajo demanda", y cualquier retardo en la puesta en funcionamiento de un servicio con niveles aceptables de rendimiento y seguridad puede significar la pérdida de un cliente.

La virtualización es la tendencia que nace para resolver estos problemas mediante la unificación de los servicios de red y seguridad tradicionales, garantizando siempre el rendimiento y la autonomía de gestión para cada uno de los servicios ofrecidos sobre una plataforma física común. Permite, por tanto, la definición sobre una única "caja" de múltiples *racks virtuales* en los que a cada uno de los servicios (*firewalling*, detección de intrusos, gestión de contenidos, balanceo de carga, conectividad VLAN, ...), se le asignan recursos de computación de manera óptima, con gestión independiente.

Sin embargo, esta solución, basada en la compartición de recursos físicos, no es nada nuevo. Durante algún tiempo, también vimos cómo proliferaba el número de circuitos de comunicaciones punto a punto en los centros de datos para terminar concentrándose en circuitos Frame-Relay, que en realidad no son más que la "virtualización" de múltiples circuitos independientes convertidos ahora en recursos virtuales (PVCs) y ofreciendo garantías de ren-

dimiento para cada uno de ellos (CIR). En este mismo sentido podemos decir que la propia Internet no es más que la virtualización extrema de una malla de interconexión "todos a todos".

Otro ejemplo de virtualización ya implantado dentro del entorno del *data-center*, se encuentra en las redes de almacenamiento o SAN (Storage Area Network), que permiten la compartición de medios físicos, en este caso elementos de almacenamiento tales como discos duros, garantizando siempre ciertas capacidades a los servidores conectados, ofreciéndoles acceso a volúmenes lógicos. Por tanto, se trata únicamente de definir la forma en que debe aplicarse este proceso dentro de los servicios de red y seguridad. La llegada de soluciones válidas de virtualización era sólo cuestión de tiempo.

El proceso de virtualización de servicios puede afrontarse de varias formas. Lo primero que hay que plantearse es si interesa un enfoque de "multiservicio" o de "multicliente".

La primera, "multiservicio", ha surgido de forma natural como consecuencia de la necesidad de los fabricantes de aumentar su cartera de productos. Prácticamente cualquier sistema cortafuegos del mercado incorpora desde hace tiempo un servicio de concentración de VPNs en la misma solución, ofreciendo una integración funcional y de gestión completas entre cortafuegos y VPN. Dicha integración podría considerarse co-



mo un nivel básico de virtualización de servicios.

La tendencia actual en este sentido es ir incorporando nuevos servicios sobre la misma plataforma. Al margen de la reducción de costes de adquisición y mantenimiento que esta integración permite, la principal ventaja de una solución integrada es la eficiencia en la gestión del tráfico. En un enfoque tradicional, cualquier dispositivo por el que deba circular el flujo de información debe realizar uniones de entrada/salida y análisis básico del formato de los paquetes, como mínimo análisis de cabeceras de nivel 2 y 3, además de las funciones propias de procesamiento del dispositivo. Todas estas tareas implican retardos en la comunicación.

La unificación de servicios permite reducir el número de operaciones de entrada/salida por realizar a un único análisis del paquete a la entrada del dispositivo, con el análisis de las cabeceras de nivel 2 y 3, seguido de todas las etapas de procesamiento necesarias (cortafuegos, antivirus, IDS, ...), y la formación del paquete de salida nuevamente hacia la red. Además, la comunicación interna entre los diversos módulos puede ser realizada por mecanismos más rápidos, como intercambios en memoria. Esto implica que la definición de los flujos inter-dispositivos, o lo que es lo mismo, la definición de la topología de la arquitectura, que antes se hacía físicamente mediante el cableado de los dispositivos, ahora pasa a ser una definición lógica o virtual, facilitando así tanto la instalación inicial como las modificaciones a las definiciones de flujos de información a tra-

vés de diversos antivirus o filtrados de URLs.

En cambio, los sistemas multicliente permiten compartir un único servicio, típicamente el cortafuegos, entre varios clientes, ofreciendo siempre garantías de rendimiento e independencia de gestión para cada uno de ellos en cualquier circunstancia. En la práctica resulta bastante más compleja si se pretende dar cobertura completa al problema. Esto es, la diferenciación de los entornos de los distintos clientes soportados en un mismo dispositivo no puede limitarse al nivel de configuración de los servicios; deben proporcionarse mecanismos de gestión y configuración para cada uno de los clientes de forma que cada uno sólo tenga visibilidad de su servicio. Más aún, el procesamiento de cada uno de los clientes debe quedar garantizado frente al resto.

Una de las ventajas de esta aproximación frente a los sistemas independientes estriba en el aprovechamiento óptimo de los recursos. En un entorno convencional, normalmente existen dispositivos con un aprovechamiento mínimo de los recursos, debido al dimen-

**“Lo primero que hay que plantearse es si interesa un enfoque de “multiservicio” o de “multicliente”**

sionamiento realizado para soportar la carga en pico. Los sistemas de virtualización multicliente, al compartir los recursos físicos de procesamiento, permiten garantizar a cada servicio un rendimiento mínimo y ofrecer rendimiento extra en situaciones de sobrecarga. Esta capacidad extra puede ser compartida entre todos los clientes soportados, con lo que el rendimiento total necesario es menor que en un entorno de sistemas independientes.

La velocidad con la que se pueden realizar configuraciones para nuevos clientes es la segunda ventaja fundamental. Los sistemas multicliente facilitan el proceso de aprovisionamiento al limitarle a una simple configuración lógica, siempre que se disponga del excedente de capacidad de procesamiento necesario. Desaparece por tanto la necesidad de adquisición e instalación de nuevo equipamiento para cada nuevo servicio a prestar.

Evidentemente, las aproximaciones multiservicio y multicliente no son excluyentes y ya se encuentran plataformas en el mercado con esta doble orientación, capaz de soportar cientos de configuraciones independientes incluyendo cada una servicios como *routing*, *firewall*, balanceo de carga, VPNs, IDS o aceleración WEB y SSL.

Si bien parece claro que el futuro inmediato de los servicios de comunicaciones y seguridad para el centro de datos se orienta hacia la virtualización, la forma en que cada fabricante está adaptándose difiere lógicamente según su punto de partida, y en esa misma medida, difieren las soluciones ofrecidas.

La elección de un sistema u otro debe partir de un conocimiento exhaustivo de las necesidades propias. Sea cual sea la elección, las ventajas de incorporar tecnología de virtualización en las infraestructuras deberían ser claras: reducción de los costes de IT, mayor flexibilidad en el desarrollo de nuevos servicios, reducción de la complejidad de la red, mejor aprovechamiento de los recursos de servicios de red disponibles, aumento de la productividad de los operadores y administradores, mayor visibilidad del sistema global, y existencia de un sistema de gestión único para todos los servicios.