ISSN 0121–1129

# Acceso remoto seguro a cuentas de usuario utilizando plataformas de virtualización

## Safe Remote Access to User Accounts by Using Virtualization Platforms

Fecha de recepción: 30 de agosto de 2010
Fecha de aprobación: 29 de noviembre de 2010

Walter Fuertes*
Maritza Enríquez**
Diego Veloz***

## Resumen

En las universidades persiste el problema de la subutilización de recursos tecnológicos; sin embargo, se sigue incurriendo en gastos por adquisición de servidores, hardware y software. Frente a este escenario, en la industria se han venido desarrollando las tecnologías de virtualización, que ahorran energía y costos de inversión de hardware. En consecuencia, el artículo propone el acceso remoto seguro a cuentas de usuario en un servidor universitario virtualizado; para llevarlo a cabo se diseñaron e implementaron varias topologías de experimentación, utilizando Virtual Box 3.1.3 y VMware Server 2.0.2, y se evaluaron diversas tecnologías de conexiones remotas seguras, bajo idénticas condiciones y parámetros de comprobación. En cada topología se evaluó el rendimiento del servidor, el performance y la seguridad de la red en producción. Los resultados muestran la funcionalidad de este proyecto de investigación que facilita el acceso remoto seguro de usuarios a los recursos informáticos universitarios.

**Palabras clave**: Acceso remoto, Tecnologías de virtualización, Cuentas de usuario

## Abstract

In the universities remains the technological resources underutilizations problem, as expending in servers, hardware and software acquisition, goes on. Facing this backdrop, and as a possible solution, it has been developing virtualization technologies, which save energy and hardware investments' costs.

This paper proposes the secure remote access implementation for user accounts on a virtualized university server. To achieve it, we have designed and implemented several experimental topologies using Virtual Box 3.1.3 and VMware Server 2.0.2, at the same time evaluating various technologies for secure remote connections under similar conditions and check up parameters.

In each topology, it was tested the server performance and the production network's security. Results show this research project's functionality, that facilitates secure remote user access to university computer resources.

**Key words**: Remote Access, Virtualization technologies, User Accounts

* Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, Sangolquí –Ecuador–. wfuertesd@espe.edu.ec
** Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, Sangolquí –Ecuador–. maryenriquez2@hotmail.com
*** Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, Sangolquí –Ecuador–. veloz.diego@gmail.com

## I. Introducción

De acuerdo con Gartner Inc., las Tecnologías de Virtualización son actualmente una de las diez tendencias disruptivas que están modificando el funcionamiento de los centros de procesamiento de datos, que redefinirán esquemas tecnológicos y departamentos de TI, y que rediseñarán la industria de micros y servidores. Estas tecnologías pueden ser usadas para crear entornos de validación y pruebas de software, consolidación de servidores, pruebas de balanceo de carga y dimensionado de servicios de red. Así mismo, estas tecnologías están siendo utilizadas en diversas aplicaciones en la educación universitaria [1].

Sin embargo, a pesar de los potenciales beneficios que las tecnologías de virtualización aportan, como ahorro de energía y de costos de inversión de hardware, su aplicación en ciertos campos está aún en una etapa primitiva. Así, por ejemplo, hoy en las universidades persiste el problema de la subutilización de recursos tecnológicos y se incurre en gastos por adquisición de servidores, hardware y software. Una de las posibles soluciones es conocida como Consolidación de Servidores, que contribuye a reducir el coste total de las instalaciones necesarias para mantener los servicios, y donde los recursos de un equipo son mejor aprovechados en uno o más entornos de ejecución [2].

En los últimos años, la comunidad científica ha mostrado un creciente interés en investigar e implementar soluciones para aprovechar los recursos computacionales. El trabajo propuesto por González Aragón y Oller Arcas [2] describe el desarrollo de una plataforma de virtualización orientada a servicios, enfocada a resolver la problemática actual del desaprovechamiento de los recursos de hardware. Así mismo, González Villalonga [3] efectuó una evaluación de la consolidación de infraestructura y de los consiguientes ahorros en inversiones y costes de mantenimiento. Fernández [4] se centró en la consolidación y simplificación de infraestructuras de sistemas de información virtualizadas y seguras. Por su parte, Alabadalejo *et ál.* [5] presentan la implementación de un sistema encriptado de sesiones remotas en un laboratorio permanente en el que los alumnos puedan realizar prácticas para accesar remotamente a los recursos de virtualización (máquinas virtuales) mediante canales seguros. Mientras que Pujal *et ál.* [6] presentan un esquema de mejoras en costos y productividad empleando la de virtualización de servidores y escritorios remotos.

En este contexto, el presente trabajo propone implementar el acceso remoto seguro a cuentas de usuario en un servidor universitario virtualizado, con el fin de aprovechar los recursos informáticos de un campus universitario. Para llevarlo a cabo, se diseñaron e implementaron varias topologías de experimentación, utilizando Virtual Box 3.1.3 and VMware Server 2.0.2, y evaluándose a la vez diversas tecnologías de conexiones remotas, tales como Virtual Network Connection (VNC), TeamViewer, Virtual Private Network (VPN) y Remote Desktop Protocol (RDP), bajo idénticas condiciones y parámetros de comprobación. En cada topología se evaluó el rendimiento del servidor, el performance y la seguridad de la red en producción. Los resultados muestran la funcionalidad de este proyecto de investigación, que facilita el acceso remoto seguro de usuarios a los recursos informáticos universitarios.

Entre las principales contribuciones de este trabajo se pueden citar: *i)* Se han evaluado diversas funcionalidades de VMware server y VirtualBox, enfocadas en terminales virtuales remotos; *ii)* Se ha demostrado que XRDP otorga mayores utilidades para un entorno real sobre una conexión segura mediante VPN, utilizando cualquiera de las dos plataformas de Virtualización señaladas; *iii)* Se ha implementado un canal de comunicación seguro para acceso a aplicaciones o servicios reales de las redes dentro de un entorno virtual remoto, lo que rentabiliza el coste de los servidores en un centro universitario.

El resto del artículo ha sido organizado de la siguiente manera: La sección 2 describe tanto el marco teórico que sustenta la investigación, como el diseño e implementación de la topología utilizada. La sección 3 presenta los resultados del experimento; en esta misma sección se expone el análisis de los trabajos relacionados. Finalmente, en la sección 4 se

establecen las conclusiones sobre la base de los resultados obtenidos y se describe el trabajo futuro.

## II. Materiales y métodos

En esta sección se describen los fundamentos teóricos de este proyecto; luego se detallan el diseño de la topología de experimentación y la implementación de los canales de comunicación, que fueron validados en una red en producción.

### *A. Infraestructuras virtualizadas*

El concepto de máquina virtual no es nuevo, surge con el sistema VM/370 de IBM en 1972. De acuerdo con los estudios de Popek [7], en 1974, una máquina virtual (VM) es un *duplicado* de una máquina real, *eficiente* y *aislada*. Duplicado, en razón de que la VM se debería comportar de forma idéntica a la máquina real, aun con menos recursos disponibles y con las diferencias de temporización. Aislada: Se pueden ejecutar varias máquinas virtuales sin interferencias y con diversas cargas de trabajo. Eficiente: Debería ejecutarse a una velocidad cercana a la del hardware real, para ello requiere que la mayoría de las instrucciones se ejecuten directamente por el hardware. En todo caso, la idea principal de las infraestructuras virtualizadas es crear varias VM coexistiendo en un único hardware.

En los últimos años, en la industria se ha potenciado el desarrollo de las tecnologías de virtualización [8], [9], [10], [11], por esa razón existen diversas clasificaciones; la siguiente es la más aceptada [12]: *i) Virtualización completa*, que intenta reproducir el funcionamiento de un ordenador origen en otro destino, sin realizar modificaciones en el sistema operativo; *ii) Paravirtualización*, que reduce los problemas de rendimiento con cierta modificación en el sistema operativo; en esta técnica se utiliza un componente denominado hypervisor, que es una capa de virtualización intermedia entre el hardware y los sistemas operativos hospedados, y que hace de árbitro para el acceso de estos a los recursos del computador de forma organizada; *iii) Virtualización a nivel de sistema operativo*, que agrupa procesos y recursos en contenedores especializados, pero que tiene un kernel común, por lo que un fallo en él, compromete a todas las máquinas virtuales; finalmente *iv) Virtualización por hardware*, que es un nuevo enfoque que usa los avances del hardware de procesadores Intel-VT (Virtualization Technology) y AMD-Pacifica (Advanced Micro Devices) para eliminar la necesidad de parches en el sistema operativo. Durante el 2005 y el 2006, Intel y AMD añadieron extensiones independientes a la arquitectura x86 para facilitar las tareas de virtualización.

La aplicación de las tecnologías de virtualización en la empresa continúa despertando mayor interés en la comunidad tecnológica y científica [13], por tanto, varias infraestructuras virtualizadas (de escritorio, de servidores y de aplicaciones) son desarrolladas cada vez con mejores funcionalidades que permiten a los usuarios escoger la más conveniente para sus necesidades [14].

### *B. VirtualBox y VMware server*

Para implementar la infraestructura virtualizada descrita en la subsección anterior se han elegido dos plataformas basadas en tecnología de Virtualización Completa, como son *VMware* y *VirtualBox,* por las siguientes razones:

En el caso de VMware server, porque es una plataforma que provee una abstracción del hardware x86 de 32 y 64 bits, capaz de repartir un servidor físico en múltiples máquinas virtuales, de tal forma que múltiples Sistemas Operativos pueden ejecutarse sin modificación y al mismo tiempo. VMware es un producto de Virtualización que funciona bajo Microsoft Windows, Linux, NetWare y Solaris. Con VMware se facilita el proceso de creación de máquinas virtuales en razón de la existencia de un sistema de gestión propio de máquinas virtuales. Forman parte de estas soluciones: VMware Player, que permite ejecutar, pero no libera ni crea máquinas virtuales; VMware Workstation, que ejecuta múltiples Sistemas operativos en una estación de trabajo y que es una solución comercial; VMware GSX Server, que ejecuta múltiples servers y es el

antecesor de VMware Server. En los últimos años, VMware ESX Server se ha convertido en un producto comercial de alto rendimiento [15].

En el caso de VirtualBox, porque es un software para implementar máquinas virtuales de x86 de 32 y 64 bits, destinado a ordenadores de escritorio y servidores empresariales. Permite ejecutar Sistemas Operativos hospedados sin modificación, incluyendo todo el que esté instalado en el ordenador anfitrión. Últimamente ha sido utilizado para la Consolidación de Servidores. VirtualBox dispone de una interfaz gráfica denominada Virtual Box Manage, la misma que permite crear máquinas virtuales, definiendo sus características virtuales de memoria, disco, teclado, mouse y CD-ROM, así como la respectiva configuración de red. Cabe destacar que permite la ejecución de máquinas virtuales de forma remota a través de RDP. Finalmente, característica relevante de VirtualBox es que posee un diseño modular con interfaces gráficas bien definidas de programación interna, cuya licencia de código abierto bajo los términos de la GNU (GPL) Lesser General Public License (LGPL) la hace accesible para experimentación [16].

### *C. Acceso remoto a infraestructuras virtualizadas*

Un acceso remoto permite tener control sobre otro equipo distante por medio de una aplicación llamada escritorio remoto; por tanto, en el presente proyecto de investigación la utilización de esta aplicación complementa el uso de máquinas virtuales en servidores compartidos, permitiendo aprovechar las ventajas de la infraestructura [5]. El elemento característico en cualquier implementación de escritorio remoto es su protocolo de comunicaciones, que varía dependiendo del programa que se use, como sucede con Independent Computing Architecture (ICA), utilizado por MetaFrame, o Remote Desktop Protocol (RDP), utilizado por Terminal Services, al igual que del producto de Secure Global Desktop (SGD), el Adaptive Internet Protocol (AIP) y el X11, usado por X-Window, sin olvidar a Virtual Network Computing, (VNC), utilizado por el producto del mismo nombre.

### *D. VPN en infraestructuras virtualizadas*

Una red privada virtual (Virtual Private Network, VPN) es un mecanismo de seguridad de red que permite comunicar una red privada sobre un canal público no seguro, ofreciendo seguridad a la infraestructura [17]. En este marco, las VPN verifican la identidad de los usuarios a través de la generación de una clave de encriptación desde el servidor, la cual es comparada con la del cliente, y de esta forma permite o niega el acceso a la red (en este caso al servidor virtualizado), lo cual resulta útil en este estudio.

En esta investigación se ha utilizado VPN, dado que una infraestructura virtualizada incluye también otro conjunto de variables del ambiente, como son el almacenamiento, los sistemas de seguridad, la conectividad, el uso de energía, los perfiles de usuario y los procesos implícitos.

### *E. Acceso XRDP*

XRDP es un servidor RDP de código abierto basado en el trabajo de *rdesktop*. El objetivo del proyecto es crear un servidor de terminal Linux totalmente funcional, el cual permite el acceso remoto a los servidores y equipos Linux y Microsoft [18]. Esta herramienta es adecuada y segura para conexiones remotas en un entorno multiplataforma. Al igual que las VPN, se genera una llave de encriptación, permitiendo una conexión segura, objeto de interés en este estudio.

## III. Diseño e implementación del experimento

### *A. Diseño de la topología*

Para proceder con la experimentación conviene distinguir los diferentes elementos que intervinieron en la topología de prueba. La Fig. 1 resume el diseño base. En el lado del Servidor se distingue el equipo anfitrión, sobre el cual se instalaron VMware server y VirtualBox. Todos los experimentos fueron desarrollados en un Pc Core 2 Quad, con 2 GB de RAM, tarjeta Ethernet, HDD de 320 GB, dedicado a almacenar máquinas virtuales y las plataformas de virtualización.

La red que se utilizó fue una Ethernet en un ambiente de producción segmentado por una VLAN de pruebas. Para proceder con el acceso remoto se configuró el *Firewall* de una red real en producción, de manera que permita hacer un Network Address Translation (NAT) en la LAN/WAN, para poder tener acceso a una dirección IP pública para el servidor de máquinas virtuales. Adicional a esto se configuraron las máquinas virtuales de tal forma que cada una de ellas tenga su propia IP y acceso a Internet.

En el lado del cliente, en cambio, se visualiza una interfaz definida como escritorio remoto (rdesktop), mediante la cual se accede a través de Internet a las máquinas virtuales instaladas en el servidor.

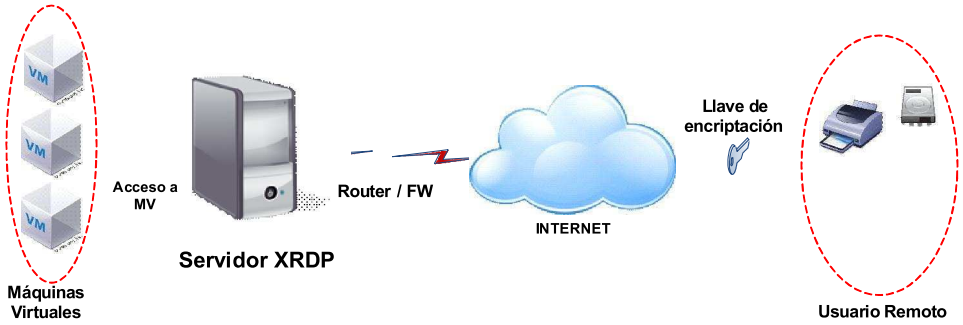


*Fig. 1.* Diseño base de la topología experimental

*B. Implementación del escenario de experimentación*

Para proceder a la implementación, en el lado del servidor se instaló y configuró Centos 5.4 para hospedar las plataformas. Con cada plataforma se crearon e instalaron varias máquinas virtuales, con Linux como Sistema Operativo, en su versión OpenSuse, Windows XP Profesional y la última con Windows 2003 Server, respectivamente. Una vez lista la infraestructura, se procedió a realizar las mediciones del rendimiento del servidor (es decir, se midió el consumo del CPU y la memoria), poniendo en funcionamiento las máquinas virtuales una a una, empleando System Activity Report (SAR). SAR es un software para recopilar y mostrar información sobre el rendimiento del sistema ejecutado desde el servidor, el cual produce informes sobre el uso (consumo) del CPU, memoria, paquetes perdidos, retardo (rtt) y throughput. La Fig. 2 muestra los diferentes elementos en un esquema categorizado por capas.

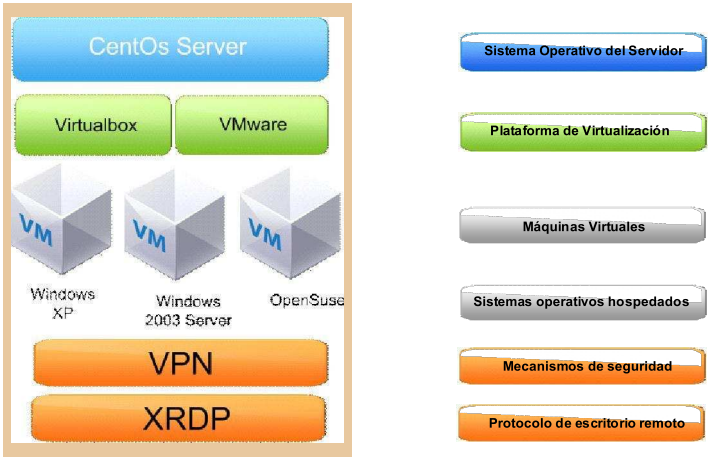


*Fig. 2.* Elementos y componentes por capas en el lado del servidor

*C. Conexión mediante una Red Privada Virtual (VPN) y XRDP*

Continuando con el experimento, se procedió a realizar la conexión remota mediante VPN; para ello se instaló OpenVPN y XRDP. Para este ambiente de pruebas, el Sistema Operativo del equipo anfitrión cumplió las funciones de servidor para las dos aplicaciones mencionadas. En ambos casos fue necesario utilizar en cada máquina virtual un cliente para la conexión remota.

Así, por ejemplo, al instalarlo en el equipo remoto con Windows XP, con las configuraciones de la VPN, el servidor universitario permitió una conexión segura entre los usuarios, conectándolos de tal forma que simularon una red LAN/WAN. Con esta condición se procedió a medir el consumo de CPU y memoria del servidor, así como a monitorear el comportamiento de esta. El diseño lógico y físico de la red en producción se muestra en la Fig. 3.

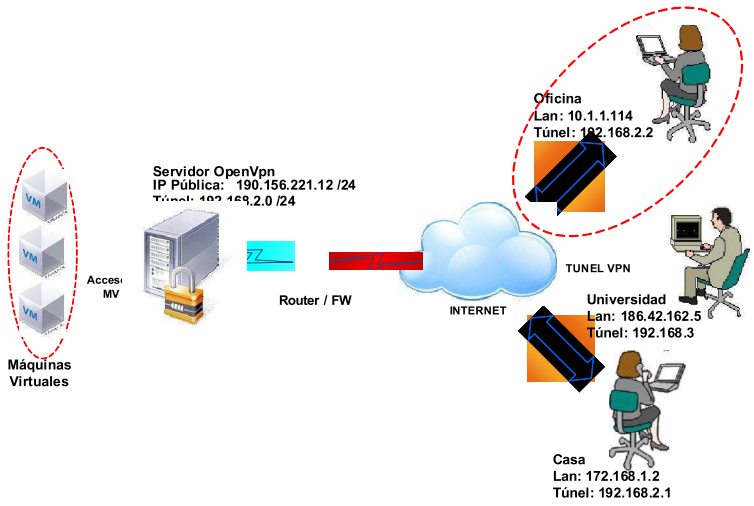


*Fig. 3*. Implementación de la infraestructura de red para conexión remota segura

*Acceso remoto a máquinas virtuales*

Una vez instalada la plataforma base, se procedió a configurar los accesos remotos a las máquinas virtuales. Para esto se utilizó TeamViewer [19], VNC y Remote Desktop de Windows, respectivamente. En primer lugar se configuró el cliente remoto con Windows XP en dos formas: la primera instalando un producto de escritorio remoto gratuito, como es VNC; con este software instalado tanto en el servidor remoto como en la máquina virtual, se probó el estado de la conectividad. En la segunda se procedió con la instalación de TeamViewer; esta aplicación realiza una encriptación y genera una clave privada para el acceso remoto host a host desde la Web.

Continuando con el experimento se realizó la conexión con RDP desde el equipo remoto hacia las máquinas virtuales. Como se puede advertir, la Fig. 4 muestra el esquema de conexión remota con VNC. Luego, se realizó la comparación de funcionalidades de las diferentes plataformas de virtualización, como el acceso a recursos compartidos de discos, unidades de disco externo, USB e impresoras. Los resultados de esta comparación se muestran en la siguiente sección (véase Tabla 3).

## IV. Evaluación de resultados y discusión

*A. Monitoreo del rendimiento del servidor y degradación de la red*

La Tabla 1 muestra los datos recolectados durante la experimentación, calculados con varias medidas mediante el comando *top* de Linux. Como se puede apreciar, *top* despliega diversos campos de

medición, como son: *%user,* que es el porcentaje de CPU utilizado por el proceso a nivel de usuario; *%nice,* que indica la utilización de CPU que se produjo mientras se ejecuta en el nivel de usuario con prioridad; *%system,* que es el porcentaje de consumo de CPU a nivel del kernel; *%iowait,* que calcula el tiempo en que el CPU está en espera de una variable de entrada y salida, e *%idle*, que calcula el tiempo en que el CPU se encuentra inactivo. La Fig. 5 muestra un incremento del consumo del sistema generado por VMware en comparación con VirtualBox.

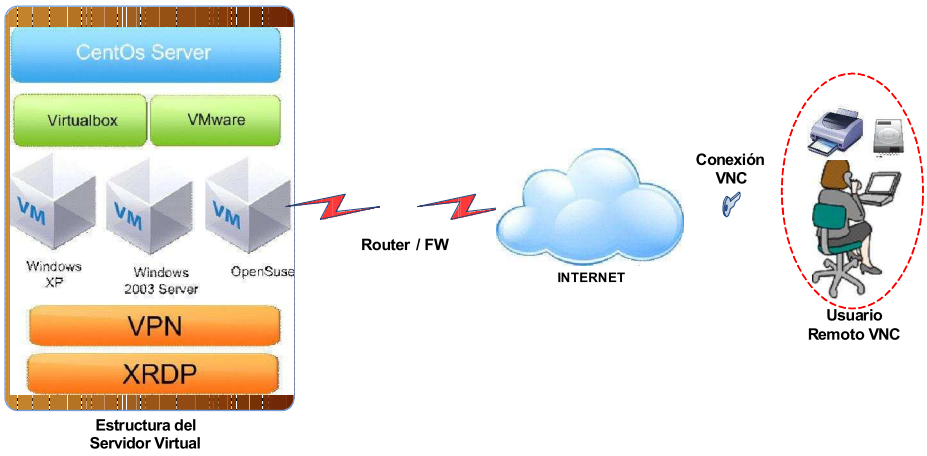


*Fig. 4.* Esquema de conexión remota con VNC

*Tabla 1.* Consumo del CPU durante la experimentación

| | %user | %nice | %system | %iowait | %idle |
|---|---|---|---|---|---|
| Virtual Box | 0,64672609 | 1,18329011 | 4,55619935 | 1,51142626 | 92,103752 |
| VMware | 2,50163904 | 0 | 5,87393186 | 6,82484346 | 84,8005157 |

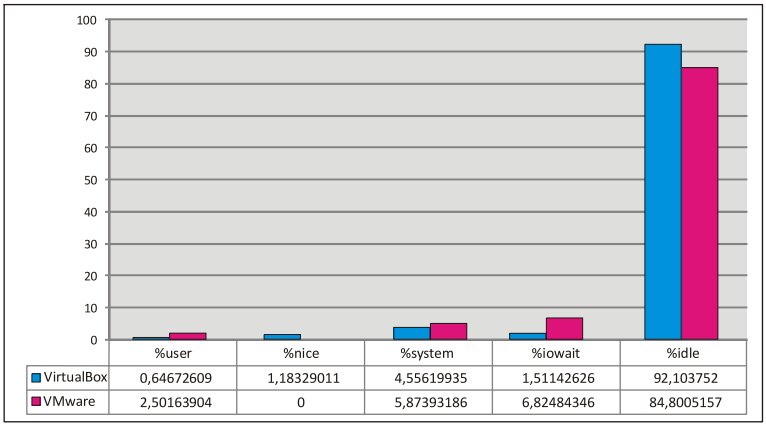


*Fig. 5.* Comportamiento del rendimiento del CPU en el experimento

Adicionalmente, tal como puede observarse en la Fig. 5, cada campo del consumo de CPU se comporta diferente; sin embargo, para las dos herramientas analizadas, su comportamiento del consumo de CPU es menor o igual al 6%, a pesar de haberlo probado con tres usuarios concurrentes.

Continuando con los resultados de los experimentos, desde el cliente la conexión fue satisfactoria, y el performance de la red no obtuvo una penalidad relevante, aunque podría variar si se utilizan aplicaciones con multimedia; sin embargo, al conectar un módem inalámbrico, el ancho de banda se vio comprometido por el uso de los demás recursos. La Tabla 2 y las Figs. 6 y 7 muestran que el performance de la red oscila entre 0,5 pckt/s y 41 pckts/s, observándose una ligera tendencia de mayor consumo por parte de VirtuaBox, comparado con VMware.

*Tabla 2.* Consumo de Red durante la experimentación

| | **rxpck/s** | **txpck/s** | **rxkB/s** | **txkB/s** | **rxmcst/s** |
|---|---|---|---|---|---|
| Virtual Box | 59,365 | 122,9885 | 24,111583 | 48,31375 | 1,2945833 |
| VMware | 64,365 | 135,2885 | 27,561583 | 53,07875 | 2,0595833 |

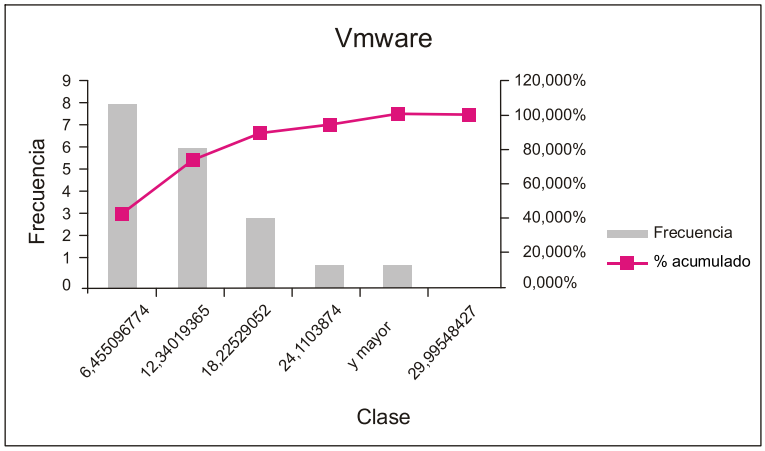


*Fig. 6.* Histograma y frecuencia acumulada de la red utilizando VMware

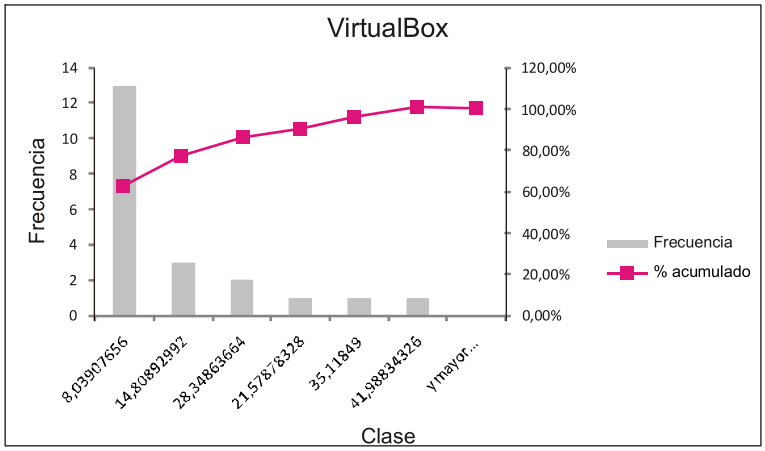


*Fig. 7.* Histograma y frecuencia acumulada de la red utilizando VirtualBox

La siguiente parte del experimento consistió en observar funcionalidades de los escritorios remotos evaluados; así, por ejemplo: *i)* Mediante *VNC,* cuyo algoritmo de encriptación tiene un grado de complejidad media, se obtuvo el control del escritorio del cliente, pero los recursos de impresoras remotas, USB o discos duros no fueron visualizados; *ii)* Con TeamViewer se consiguió el manejo y compartición de archivos en una sesión remota; *iii)* Evaluando la conexión remota con RDP se observó que el escritorio estaba disponible, de igual forma los recursos de disco e impresoras, dando como resultado una aceptable administración de la máquina virtual y sus dispositivos de disco y unidades extraíbles. Por otro lado, es importante notar que en las sesiones remotas con VNC y TeamViewer, utilizando Windows XP, se dispone de mayores privilegios que cuando se utilizan máquinas virtuales con Windows 2003 server hospedado, por el mismo hecho de ser un servidor multiconexiones.

En la verificación de las funcionalidades de los tres casos anteriores se empleó la conexión segura VPN, generando un ambiente de red seguro, con recursos compartidos en el servidor virtualizado. En todo caso, la limitación está dada por el cliente de escritorio remoto que se utilice. Para fortalecer este razonamiento existe la evidencia de que RDP resultó ser eficiente para administración remota, observándose que en una baja conexión de Internet el rendimiento del equipo no disminuyó; por el contrario, con VNC sí se evidenció mayor consumo de recursos del equipo remoto, lo que hizo que se incremente el tiempo de respuesta en la sesión. El resumen de esta validación se verifica en la Tabla 3.

*Tabla 3*. Comparación cualitativa entre los tipos de conexión remota

| Tipo de Conexión | Escritorio | Discos | Impresoras | USB | Conexión segura | Sesión multiusuario |
|---|---|---|---|---|---|---|
| VPN + RDP | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| VPN + VNC | ✓ | × | × | × | ✓ | × |
| XRDP | ✓ | × | × | × | ✓ | ✓ |

Para concretar, con VNC y TeamViewer no es posible que dos usuarios se encuentren simultáneamente en la misma sesión. De igual manera, con VNC el último usuario en conectarse cierra la sesión del antecesor. En el caso de sistemas operativos de servidor, como lo es el Windows 2003 server, se pueden proporcionar varias sesiones a la vez sin que sean desconectados; esta característica también la posee XRDP, que es una implementación de código abierto de RDP, que, como se indicó en la sección 2, es el protocolo utilizado por los Servicios de Terminal de Windows para su conectividad nativa. El paquete XRDP proporciona funcionalidad RDP, junto con un servidor capaz de aceptar conexiones de rdesktop y de clientes del Servidor del Terminal de Windows. Se puede, entonces, determinar que RDP es un protocolo que cuenta con la suficiente capacidad para administrar, con un entorno gráfico, servidores o equipos remotos, que pueden ser máquinas virtuales hospedadas en un servidor universitario.

*B. Trabajos relacionados*

Aunque existan diversos trabajos relacionados, en esta sección se han incluido los más relevantes que se han encontrado durante la investigación; ellos son:

En lo que se refiere a la consolidación de servidores, los trabajos propuestos por [2], [3], [4] describen el desarrollo de una plataforma de virtualización enfocada a resolver la problemática del desaprovechamiento de los recursos de hardware. Comparando con nuestro trabajo, no se especifica la evaluación de los canales de comunicación para acceso remoto a máquinas virtuales.

En relación con investigaciones que utilizaron escritorio de acceso remoto, el trabajo propuesto por Josep Pujal *et ál.* [7] presenta un modelo de plataforma de virtualización distribuida, que integra un servidor de perfiles que caracterizará a los usuarios

con sus perfiles y un interfaz de provisión basado en servicios Web, combinando máquinas virtuales y clientes ligeros. No se muestran resultados mesurables.

En este mismo ámbito, Alabadalejo *et ál.* [5] proponen un laboratorio virtual de acceso remoto para realizar prácticas con ordenador, basados en tecnologías Web; no presentan resultados mesurables. Comparados los dos trabajos anteriores con el nuestro, hemos combinado plataformas de virtualización con escritorios remotos, buscando un canal seguro de acceso a cuentas de usuario. Así mismo, hemos evaluado el rendimiento del servidor, así como la degradación del rendimiento de la red, en función de la plataforma de virtualización y el esquema de conexión seguro con diversas alternativas.

## V. Conclusiones y trabajo futuro

En el presente trabajo se han implementado canales de comunicación de acceso remoto seguro a cuentas de usuario en un servidor universitario virtualizado, con el fin de utilizar aplicaciones o servicios reales de redes, lo que rentabiliza el coste de los servidores en un centro universitario; se han diseñado e implementado varias topologías de experimentación utilizando Virtual Box 3.1.3 y VMware Server 2.0.2, evaluándose a la vez diversas tecnologías de conexiones remotas seguras, bajo idénticas condiciones y parámetros de comprobación; se ha verificado la funcionalidad de las máquinas virtuales observadas como terminales virtuales remotos, y se ha evaluado cuantitativamente el rendimiento del servidor (su comportamiento del consumo de CPU es menor o igual al 6%) y el performance y seguridad de la red en producción (el performance de la red no obtuvo una penalidad relevante, aunque al conectar un módem inalámbrico disminuyó considerablemente el rendimiento).

El análisis estadístico demostró que VMware server sería una plataforma más recomendable que VirtualBox, tanto para el rendimiento del host anfitrión, como en el performance de la red. Finalmente, se ha demostrado que XRDP otorga mayores utilidades para un entorno real sobre una conexión segura mediante VPN, utilizando cualquiera de las dos plataformas de virtualización señaladas.

Los resultados finales muestran la funcionalidad de este proyecto de investigación, que facilita el acceso remoto seguro de usuarios a los recursos informáticos universitarios.

Como trabajo futuro se planea ampliar el grado de pruebas y de usuarios concurrentes conectados, ampliando la capacidad de las máquinas virtuales y limitando el ancho de banda de la red en producción.

## Referencias


[1] W. Fuertes, J. E. López de Vergara, F. Meneses, "Educational Platform Using Virtualization Technologies: Teaching-Learning Applications and Research Uses Cases". In *Proceedings of II ACE Seminar: Knowledge Construction in Online Collaborative Communities*, Albuquerque, NM USA, October 2009.

[2] D. González Aragón, T. Oller Arcas, "Desarrollo de una plataforma de virtualización", Proyecto de Titulación Ingeniería Técnica de Telecomunicaciones, Universidad Politécnica de Cataluña, España, 31 de marzo de 2008.

[3] J. González Villalonga, "Virtualización de la infraestructura informática: impacto en inversiones y costes de explotación", *Revista Anales de Mecánica y Electricidad*, España, noviembre-diciembre, 2006.

[4] J. Fernández-Sanguino, "Hacia una virtualización segura de las infraestructuras", *Revista SIC* (Seguridad en Informática y Comunicaciones), número 77, España, noviembre 2007,

[5] A. Albaladejo Blázquez; A. F. García Quintana, J. A. Gil Martínez-Abarca, "Teleprácticas: Sesiones Remotas vs. Acceso Remoto. Laboratorio de prácticas libres ubicuo en la EPS",

*Servicios electrónicos para la sociedad de la información. Desarrollo de grandes aplicaciones distribuidas sobre internet.* (II Jornadas para el Desarrollo de Grandes Aplicaciones de Gestión de Red), 2005, pp. 107-128.

[6] J. Pujal, A. Oller, J. López, C. Fanning, F. Minerva, J. Alcober, "Escritorios remotos en máquinas virtuales aplicados en grandes corporaciones". *Revista Virtual* [en línea]. Disponible en: http://www.rediris.es/rediris/boletin/85-86, marzo 2009, pp: 42-49

[7] G. J. Popek and R. P. Goldberg, "Formal requirements for virtualizable third generation architectures". *CACM*, 17(7): 413-421, 1974.

[8] F. J. Ruiz, D. Fernández, F. Galán, L. Bellido, *Modelo de Laboratorio Docente de Telemática basado en Virtualización Distribuida*..

[9] W. Fuertes and J. E. López de Vergara, "An emulation of VoD services using virtual network environments". *In Proc. GI/ITG Workshop on Overlay and Network Virtualization NVWS'09*, Kassel-Germany, March 2009.

[10] F. Galán, D. Fernández, W. Fuertes, M. Gómez and J. E. López de Vergara, "Scenario-Based Virtual Network Infrastructure Management in Research and Educationnal Testbeds with VNUML", *Annals of Telecommunications,* 64(5): 305-323, May 2009.

[11] W. M. Fuertes and Jorge E. López de Vergara, "A Quantitative Comparison of Virtual Network Environments Based on Performance Measurements", in *Proceedings of the 14th HP Software University Association Workshop*, Garching, Munich, Germany, 8-11 July 2007.

[12] SCOPE Alliance, "Virtualization: State of the Art". Version 1.0, April 3, 2008.

[13] W. Fuertes, J. E. López de Vergara, F. Meneses, F. Galán, "A Generic Model for the Management of Virtual Network Environments". In *Proceedings of 12th IEEE/IFIP Network Operations and Management Symposium (NOMS -2010)*, Osaka, Japan, 19-23 April 2010.

[14] M. Tim Jones, "Virtual Linux", publicado en IBM Developerworks, fuente original: http://www-128.ibm.com/developerworks/linux/library/l-linuxvirt.

[15] A. García Calahorro, *Estudio de rendimiento y funcionalidad sobre diferentes soluciones de virtualización*, Bellaterra, junio de 2009, pp. 13-14.

[16] Virtual Box, "Características del producto" [En línea]. Disponibele en: http://virtualbox.org, fecha de acceso: 15-abril-2010.

[17] José María Peribáñez, "Virtualización y redes en GNU/Linux" Revisión 1.0, e-book, octubre de 2007.

[18] T. Leichtenstern, "Escritorios remotos", revista virtual *Linux Magazine* N.º 34, pp. 21-26. Disponible en: http://www.linux-magazine.es

[19] TeamViewer "Brochure del product" [Online]. Disponible en: http://www.teamviewer.com/images/pdf/TeamViewer_brochure_es.pdf, [acceso: 15-abril-2010].