Artículo Original

Virtualización de Redes y Servidores Emulando Infraestructuras Tecnológicas

Network and Server Virtualization Emulating Technological Infrastructures

Juan Casierra Cavada, Xavier Quiñónez Ku, Luis Herrera Izquierdo y Carlos Egas Acosta

Pontificia Universidad Católica del Ecuador, sede Esmeraldas.

La correspondencia sobre este artículo debe ser dirigida al Juan Casierra Cavada.

Email: juan.casierrac@pucese.edu.ec

Fecha de recepción: 6 de octubre de 2017.

Fecha de aceptación: 13 de marzo de 2018.

¿Cómo citar este artículo? (Normas APA): Casierra Cavada, J., Quiñonez Ku, X., Herrera Izquierdo, L., Egas Acosta, C. (2018). Virtualización de Redes y Servidores Emulando Infraestructuras Tecnológicas*. Revista Científica Hallazgos21, 3* (Suplemento Especial). Recuperado de http://revistas.pucese.edu.ec/hallazgos21

Resumen

La necesidad de desarrollar destrezas en el área de tecnologías de la información y comunicación es algo imperioso en las empresas. También el crecimiento de requerimientos en tecnologías de virtualización aplicadas a centros de datos, gestionando plataformas tales como Xen Server, Vmware, Proxmox, entre otros. Se plantea el objetivo de formular escenarios tecnológicos que permitan la ejecución de prácticas profesionales en ambientes virtuales y, así, mantener actualizados conceptos para afrontar los desafíos de la industria tecnológica. Se realizó´un estudio cuali-cuantitativo, descriptivo, bibliográfico, y analítico –donde se trabajó con dos profesionales de la Escuela de Sistemas y Computación de la Pontificia Universidad Católica del Ecuador, Sede Esmeraldas (PUCESE)-, validando la gestión de routers, servidores y centrales de comunicación, sin costo de licenciamiento. Los resultados obtenidos demostraron la efectividad de los procedimientos virtuales de forma considerable, permitiendo la gestión de comunicaciones, compartición y balanceo de recursos de hardware, en base a requerimientos; lo que se convierte en una opción fundamental en el ámbito de redes de comunicaciones empresariales, con algunas mínimas limitaciones de compatibilidad.

Palabras clave: virtualización de redes; interfaces virtuales; contenedores virtuales; acceso a tecnologías de la información.

Abstract

The need to develop skills in the area of information and communication technologies is something imperious in the companies, as well as the growth of requirements in virtualization technologies applied to data centers, managing platforms such as Xen Server, Vmware, Proxmox, among others; therefore, the objective of formulate technological scenarios that allow the execution of professional practices in virtual environments and so keep updated concepts to face the challenges of the technology industry. For this purpose, a qualitative and quantitative study was carried out, descriptive, bibliographical and analytical work with two professionals from the School of Systems and Computation of the Pontifical Catholic University of Ecuador (PUCESE), validating the management of routers, servers and central communication, without licensing costs. The results obtained demonstrated the effectiveness of virtual procedures considerably, allowing the management of communications, sharing and balancing hardware resources based on requirements, which becomes a fundamental option in the field of business communications networks, with some minimal compatibility limitations.

Keywords: virtualization networking; virtual interfaces; virtual containers; access to information technology.

Virtualización de Redes y Servidores Emulando Infraestructuras Tecnológicas

La virtualización es una tecnología en apogeo con gran potencial, que permite administrar de forma eficiente los recursos de hardware, software, consolidación de servidores, costos, espacio físico, y recurso humano en una infraestructura de TI, mejorando de igual manera la capacidad de gestión y seguridad de los escritorios virtuales (Fuertes, Vilac, y Gallov, 2012).

Según Correa, Fletscher, y Botero (2015), en la actualidad, la implementación de centros de datos en las empresas se ha

incrementado por su gran capacidad de almacenamiento de información. También por su capacidad de procesar aplicaciones y servicios de grandes dimensiones.

Para la optimización de los costos de operación de las infraestructuras tecnológicas de los centros de datos, surge, lo que se conoce hoy como, virtualización de servidores que permite instanciar varias máquinas virtuales en una sola máquina física.

Hoy en día se dan diversas definiciones de lo que se denomina virtualización de servidores, aunque todas coinciden en que consiste básicamente en agrupar diferentes aplicaciones y servicios de sistemas heterogéneos dentro de un mismo hardware. De esta forma, los usuarios y el propio sistema los ven como máquinas independientes dedicadas. Para ello, el sistema operativo virtualizado debe ver el hardware de la máquina real como un conjunto normalizado de recursos, independientemente de los componentes reales que lo formen (Doña, García, López, Pascual & Pacual, 2012).

Se procede a la virtualización de la infraestructura de redes (conmutadores, enlaces y enrutadores), para mejorar la calidad de servicio en las aplicaciones en la nube, mitigar los riesgos en la seguridad física y de las aplicaciones, facilitar la migración de las aplicaciones existentes en los clientes, mejorar el soporte en la red, entre otros.

Según Lugo (2014), la virtualización de red es la segmentación o partición lógica de una única red física para usar los recursos de la red. Ésta es lograda instalando software junto con los servicios para gestionar el almacenamiento compartido, los ciclos de computación, además de las aplicaciones. La virtualización de red trata a todos los servidores y servicios en la red como un único grupo de recursos al que pueden acceder sin considerar sus componentes físicos. Se pueden tener varios tipos de virtualización de redes, entre los que se puede mencionar principalmente: Virtual LAN, Virtual IP y Virtual Private Network.

Como lo manifiestan Cueva, Pozo, e Iturralde (2016), el desarrollo de Software para diseño fácil de redes (ENDS), que permite realizar la virtualización de la red y la configuración remota de los parámetros básicos –así como la publicación de Ruiz, Marín, Pereñíguez-García, Ruiz, y Gómez (2010) con herramientas en modo de usuario de red virtual Linux (VNUML)-, enfocan al desarrollo de prácticas virtuales de redes de comunicación. En consecuencia, este artículo va un paso más adelante, al introducir múltiples tecnologías de virtualización, tanto libres como propietarias, definiendo interfaces virtuales físicamente unidas y lógicamente independientes, permitiendo analizar tasas de transferencias con protocolos como el SNMP, con interfaces lógicamente independientes, y software ejecutado en el ambiente virtual.

La zona desmilitarizada (DMZ), comprende un conjunto probado de patrones de diseño de redes que abordan, colectivamente, estos problemas para los científicos. Explicamos el modelo DMZ de la Ciencia, incluyendo arquitectura de red, configuración del sistema, seguridad cibernética, y herramientas de rendimiento, que crea un entorno de red optimizado para la ciencia (Dart, 2014).

El modelo de zona dinámica desmilitarizada (DMZ) considera tanto el rendimiento de la red cuanto la seguridad;

y, responde dinámicamente a las demandas de tráfico en tiempo real (Wu, 2015).

Método

Se realizó un estudio cuali-cuantitativo en donde se emplearon varios métodos. En el ámbito teórico, el analítico-sintético con su valoración individual; así como la interrelacionada, para un adecuado desarrollo de habilidades en la búsqueda de soluciones para los problemas en la carencia de prácticas personalizadas. El método inductivo-deductivo, como complemento al análisis de forma, reflexivo del progreso individual, y colectivo de las habilidades requeridas en la especialidad de redes. Análisis documental valorando las iniciativas previas, y revisión bibliográfica para definir los fundamentos principales de la investigación. En concordancia con el ímpetu del ser humano en adquirir de las experiencias nuevos conocimientos aplicando en la práctica lo expuesto en la cátedra universitaria.

En el desarrollo de la investigación se generó el análisis de los servicios expuestos en la infraestructura de comunicación existente, desde el enfoque de conservar calidad de servicio y valor real de tráfico requerido, orientado al buen funcionamiento de la infraestructura de red.

El centro de datos de la Pontificia Universidad Católica del Ecuador sufrió cambios radicales al incrementar la cantidad de usuarios en la unidad académica. También los requerimientos en procesos de acreditación institucional de sistemas y recursos tecnológicos que en él se alojan. Considerando lo expuesto, más la evolución y crecimiento de procedimientos relacionados a los ataques informáticos, era imperiosa la necesidad de crear un ambiente de seguridad a sus servicios.

Resultados

Técnicas y Procedimientos

Diseño de infraestructura de comunicaciones.

Se inició con un análisis del estado actual de la infraestructura, para lo cual se solicitó la colaboración del departamento de Tics.

Se evidenció que en los procesos de comunicaciones se presentaban ataques de denegación de servicios, desde equipos con identidades alteradas y conectados a la infraestructura.

El diseño que se detalla en la Figura 1, representa la infraestructura de comunicaciones del centro de datos.

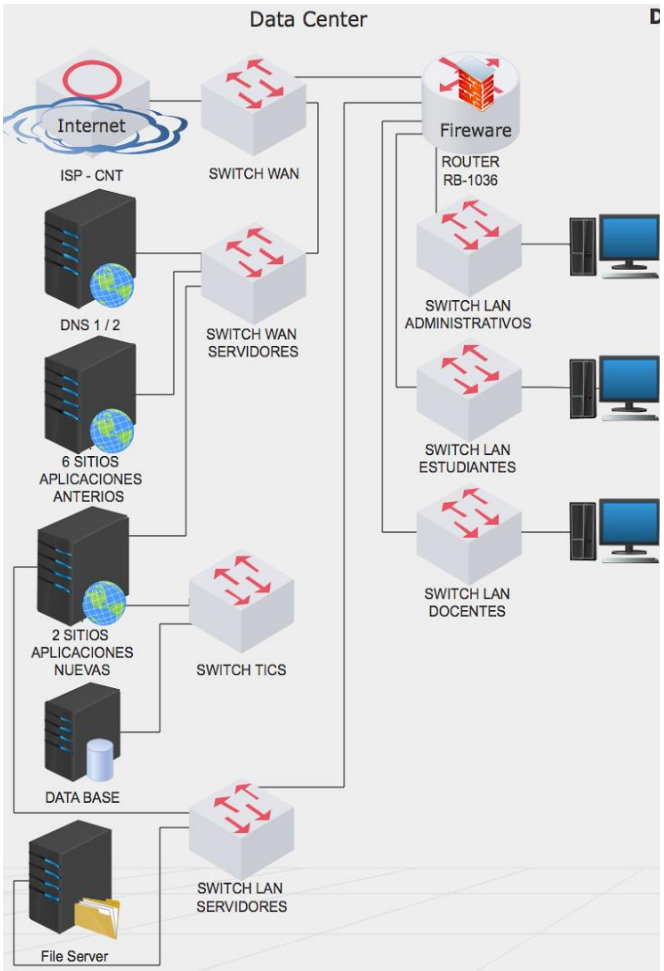

Figura 1. Escenario de red inicial sin DMZ.
Fuente: Elaboración propia.

Analizando la infraestructura detallada se encuentran las condiciones de vulnerabilidad citadas en la Tabla 1.

Tabla 1
Detalles de infraestructura inicial

Equipo	Detalle
Router Core	Equipo Mikrotik CCR1036 sin políticas eficientes en el Firewall
Servidores DNS	Equipo con puertos como el SSH abiertos y expuestos al internet
Servidor de Aplicaciones históricos	
Servidor de aplicaciones Nuevo	Equipo con puertos como el SSH, FTP y otros abiertos y expuestos al internet
Servidor de Bases de datos	
Servidor de Archivos	

Fuente: Elaboración propia.

Como se aprecia en la tabla de detalles de la infraestructura inicial, los equipos presentaban condiciones de inseguridad en cuanto a plataformas y continuidad de negocio. Por ello, la creación de un nuevo diseño de infraestructura, mediante el uso de recursos de virtualización, orientada a garantizar la calidad de servicios, tanto en accesibilidad cuanto en conectividad, es algo recomendado.

Definición de Implementación en el Centro de Datos.

Se desarrolló el diseño de una zona desmilitarizada utilizando un equipo existente, usando Citrix Xen Server como plataforma central de virtualización. En ella se ingresaron 4 máquinas virtuales, que se detallan en la Tabla 2.

Tabla 2
Máquinas virtuales implementadas en la DMZ

Función	Sistema Operativo	Recursos en % del servidor
Firewall	RouterOS	10%
DNS2		15%
Data Base	Debian 8.0	25%
Aplicaciones nuevas		35%

Fuente: Elaboración propia.

Luego de la recolección de información, se evidenció la falta de protección a los servidores de bases de datos y aplicaciones, así como la existencia de puertos abiertos como el del servicio de SSH puerto 22, FTP puerto 21 entre otros. Ello convierte al servicio vulnerable y susceptible a ataques entre otros factores, lo que no garantiza la continuidad de operaciones, o continuidad del servicio tecnológico. Se agregó la zona desmilitarizada que, en un proceso de migración planificada, logró habilitar los servicios con el menor impacto adquiriendo los recursos de software libre como lo evidencia la Tabla 3.

Tabla 3
Datos requeridos para la implementación

Detalle	Acceso
Citrix Xen Server	http://xenserver.org/open-source-virtualization-download.html
RouterOS	https://download2.mikrotik.com/routeros/6.38.7/mikrotik-6.38.7.iso
Debian 8.0	www.debian.org/ports/amd64

Fuente: Elaboración propia.

Adicionalmente, se realizó una migración inicial de equipos físicos a máquinas virtuales y contenedores, para garantizar

una movilidad y continuidad del negocio, como lo refleja la Figura 2.

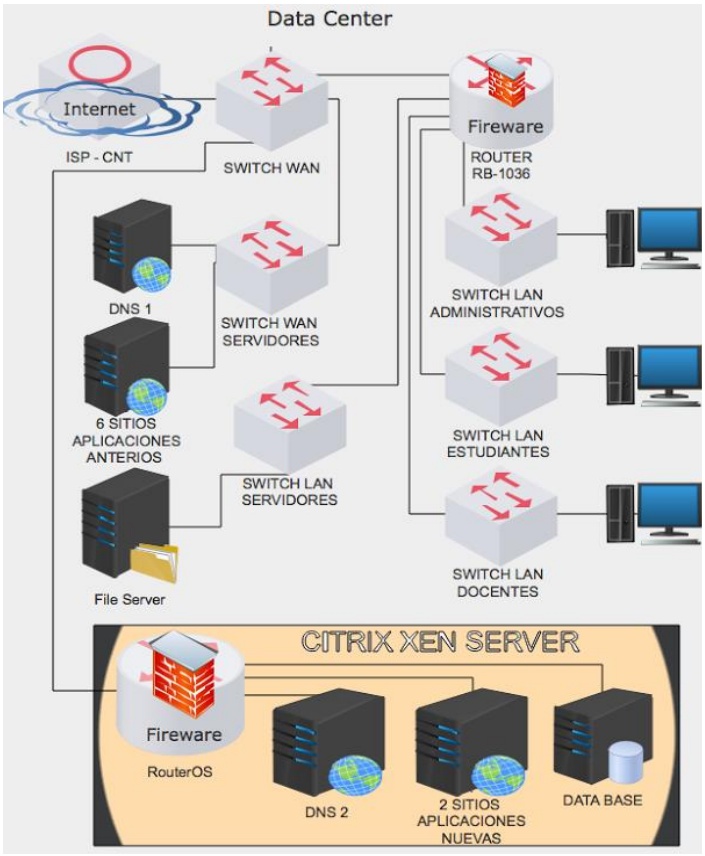

Figura 2. Escenario de red virtual con aplicación Xen Server. Fuente: Elaboración propia.

Configuración de Interfaces de Red

Se establecen los dominios de propagación requeridos para la comunicación interna, así como la configuración de direcciones públicas para el acceso a los servicios en la zona desmilitarizada. Se procedió a etiquetar con comentarios en interfaces como lo indica la Tabla 4.

Se asignan tres interfaces lógicas a la física # 1, conectada en el Switch de Core WAN, lo que permite tener diferentes servicios controlados desde el equipo administrador como lo ilustra la Figura 3.

Tabla 4
Definición de interfaces con direccionamiento IPv4

Estado	Dirección TCP/IP	Tipo de interface Comentario
R	186.42.x.x1	Ether_1_Wan1
R	186.42.x.x2	Ether_2_Wan2
R	186.42.x.x3	Ether_3_Wan3

Fuente: Elaboración propia.

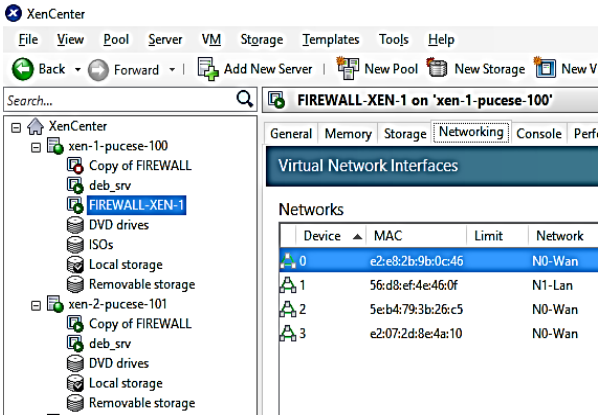

Figura 3. Visor de servidor Xen Server con DMZ Implementada. Fuente: Elaboración propia.

Configuración de servidor de nombres de dominio (DNS).

En la zona desmilitarizada se define la configuración DNS y la opción de permitir los requerimientos remotos de usuarios. Se definieron como DNS alternativos los del servicio de sitio web www.google.com, considerando los DNS del proveedor de internet como prioritario lo que se ilustra en la Tabla 5.

Tabla 5
Configuración de DNS en ambiente virtual DMZ

DNS-Address	Src-Server
200.107.10.62	CNT. EP.
200.107.60.58	CNT. EP.
8.8.8.8	Google Inc.
4.4.4.4	Google Inc.

Fuente: Elaboración propia.

Configuración de Rutas.

Para garantizar el flujo de la información se define las diferentes rutas las cuales son generadas de forma dinámica. A diferencia de la ruta correspondiente a la puerta de enlace para el tráfico de salida, como lo ilustra la Tabla 6.

Tabla 6
Definición de puerta de enlace y rutas

Tipo.	Dst. Address	Gateway
AS	0.0.0.0/0	182.42.x.3 reachable WAN-3
DAC	10.0.0.0/24	DMZ-1 reachable
DAC	186.42.x.x/28	Wan-9 reachable, WAN -3

Fuente: Elaboración propia.

Detalles de Desarrollo

En el desarrollo de la implementación se identificaron ataques concurrentes desde fuentes internas y externas a la infraestructura. La definición de una tabla ARP, con su respectivo direccionamiento IP, y la definición de reglas de firewall, colas de tráfico y control de ancho de banda, la definición de los equipos virtuales en la infraestructura, están representadas en la Figura 4a.

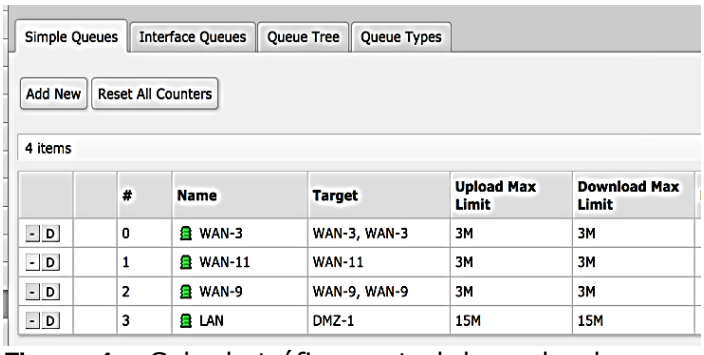

Figura 4a. Cola de tráfico control de ancho de banda. Fuente: Elaboración propia.

En el proceso de la investigación se analizó el tráfico inicial y final de la implementación de la DMZ. Específicamente, el concurrente del servidor y servicios que presta en la infraestructura de tecnologías, como lo refleja la Figura 4b. En esta se aprecia una reducción en el uso de ancho de banda, considerando que en la DMZ se filtró, mediante reglas de firewall, el tráfico no válido y ataques recibidos que generan consumo de recursos. En la infraestructura virtual se tiene una mejor apreciación del uso de recursos en proceso del equipo, uso de memoria, transmisión de datos, entre otros. Ello indica que las infraestructuras de comunicaciones, con su definición de tráfico requerido, y de uso de recursos de hardware y software bien administrados, generan eficiencia en su capacidad de usabilidad.

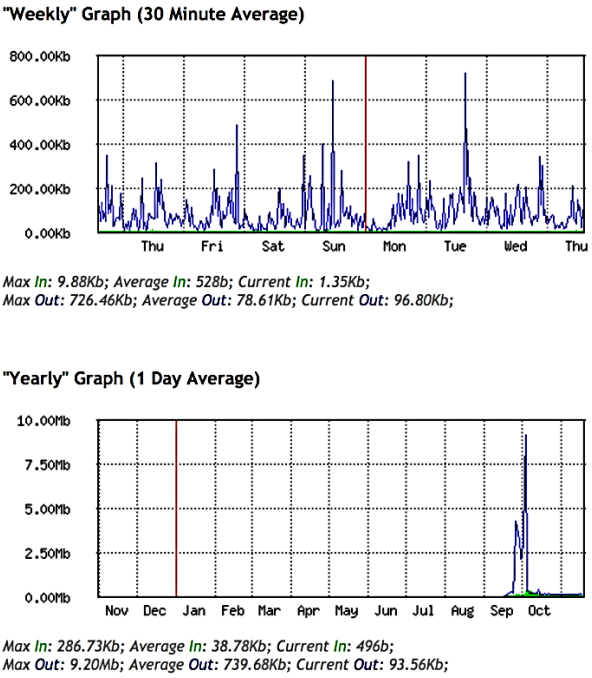

Figura 4b. Detalle de tráfico efectivo en la infraestructura de comunicaciones específicamente en servidor de aplicación. Fuente: Elaboración propia.

Para garantizar la respuesta en eventos en los que no responda el servidor de DNS local principal, se generó un servidor de DNS secundario, o alternativo, utilizando la plataforma descrita en la investigación con el sistema operativo RouterOS, en la configuración de DNS Static de la aplicación, según lo ilustrado en la Figura 5.

D		3	siabuc.pucese.edu	186.42.182.
D		4	revistas.pucese.ec	186.42.182.
D		5	prueba.pucese.edu	186.42.182.
D		6	router.pucese.net	186.42.182.
D		7	ns1.pucese.net	186.42.182.
D		8	ns2.pucese.net	186.42.182.
D		9	ns.pucese.net	186.42.182.
D		10	ns3.pucese.net	186.42.182.
D		11	servicios.pucese.n	186.42.182.
D		12	backup.pucese.ne	186.42.182.
D		13	moodle.pucese.ne	186.42.182.
D		14	admin.pucese.net	186.42.182.
D		15	kleber.pucese.net	186.42.182.
D		16	repositorio.pucese	186.42.182.
D		17	revistas.pucese.ne	186.42.182.

Figura 5. Declaración de servidor de DNS estáticos RouterOS. Fuente: Elaboración propia.

Considerando que, al iniciar el cambio en la infraestructura, no se aplicaban las reglas de firewall, se genera un nivel alto de tráfico que, al ser controlado con las reglas de firewall, muestra su nivel requerido. Este se encuentra muy por debajo del inicial, demostrando la efectividad del proceso, y el uso real de recursos del servidor en la plataforma virtual, como se observa en la Figura 6. Al mencionar reglas de firewall, se tienen las aplicadas, orientadas a crear listas de direcciones problemáticas que, al bloquearlas de forma automática por un tiempo considerable, permitirán liberar el tráfico atacante desde esos orígenes hacia la infraestructura.

Se implementaron reglas para bloquear las consultas recursivas de DNS, desde los host de la infraestructura por las direcciones públicas que no genera este servicio.

Regla 1:

//ip firewall filter add action=drop chain=input comment="Para el Bloqueo DNS cache externo" disabled=no dst-port=53 in-interface=ether1-Wan protocol=udp

Regla2:

/ip firewall filter add action=drop chain=forward comment="Para el Bloqueo DNS cache externo" disabled=no dst-port=53 in-interface=ether1-Wan protocol=udp

No controlar las peticiones recursivas realizadas por hosts o direcciones IP, que no corresponden al dominio de los servidores DNS, puede ser aprovechada para abusar por un posible atacante que realice un gran número de consultas al servidor. Esto provocaría una situación de denegación de

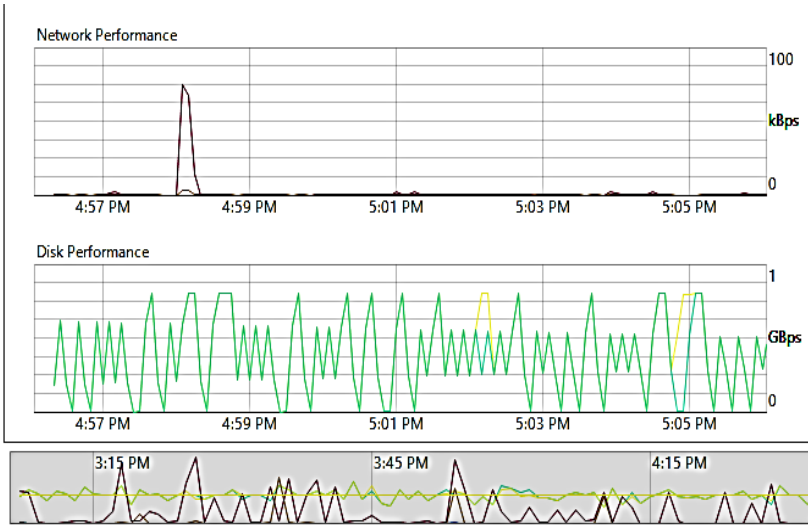

Figura 6. Detalle de tráfico inicial en la infraestructura virtual. Fuente: Elaboración propia.

servicio, al consumir todos los recursos del servidor, intentando responder a estas consultas. Un servidor con esta mala configuración puede ser utilizado en ataques para la denegación de servicio, a fin de afectar a terceras partes.

Conclusiones

Al realizar la virtualización de una infraestructura de tecnologías, y romper los paradigmas de implementación de los procesos tradicionales, como lo evidenció esta investigación, permite la continuidad del funcionamiento de la infraestructura de tecnologías, dada su facilidad de redundancia y tiempos de recuperación. También permite mayor protección de los datos, y el conocimiento de la cantidad de recursos necesarios. En la práctica, las diferentes aplicaciones y, en un futuro migrar, la plataforma a servidores externos con la contratación de infraestructura como servicio (IaaS), generaría un mayor ahorro en el mantenimiento de la infraestructura. Si se suman los costos directos e indirectos anuales, se genera un ahorro que permitirá invertir en mayor ancho de banda, e implementaciones intranet en la institución. Adicionalmente, conocer los recursos disponibles, y una estadística de crecimiento, permite crear zonas de prueba y redundancia en equipos que antes se encontraban subutilizados. Esto implica una pérdida, considerando que en el periodo de vida útil del equipo se debe aprovechar al máximo.

Referencias

Armengol, M. C., & Stojanovic, L. (2005). Innovación y virtualización progresivas de las universidades iberoamericanas hacia la sociedad del conocimiento. *Revista Iberoamericana de Educación a distancia*, *8*(1/2), 127.

Correa, E., Fletscher, L., & Botero, J. (2015). Virtual Data Center Embedding: A Survey. IEEE Latin America Transactions, 1661-1670.

Cueva, H., Pozo, F., & Iturralde, D. (2016). Cross-platform network visualization software for MikroTik devices. https://doi.org/10.1109/ANDESCON.2016.7836222

Dart, E. R. (2014). The science DMZ: A network design pattern for data-intensive science. *Scientific Programming*, 185.

Doña, J., García, J., López, J., Pascual, F., & Pacual, R. (2012). Virtualización de servidores. Una solución de futuro. Málaga.

Fuertes, W., Vilac, J., & Gallov, D. (2012). Laboratorios de computación multiplataforma aplicando tecnologías de virtualización. XVI Congreso Internacional de Contaduría, Administración e Informática. México.

Lugo, N. (2014). Tecnologías de virtualización en los sistemas informáticos de las organizaciones empresariales del Estado Zulia. Revista Electrónica de Estudios Telemáticos, 13, 49-67.

Ruiz, A., Marín, R., Pereñíguez-García, F., Ruiz, A. F., & Gómez, P. M. (2010). Experiencia con la herramienta de virtualización VNUML. Jornadas de Enseñanza Universitaria de la Informática.

Wu, H. L. (2015). Size-based flow management prototype for dynamic DMZ. *2015 11th International Conference on the Design of Reliable Communication Networks, DRCN 2015*, 85.