UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Evaluación del Rendimiento de una red IPv6 utilizando IPSec en Modo Túnel

Evaluation of the Performance of an IPv6 network using IPSec in Tunneling Mode

Autores

[1]* *Yumber Alejandro Ponce Loor*

[2] *Jorge Sergio Herrera Tapia*

[1]Instituto de Posgrado, Universidad Técnica de Manabí, Portoviejo, Ecuador.
[2]Dirección de Postgrado, Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador.

* Autor para correspondencia

Resumen

El espacio de direcciones IPv4 está a punto de llegar a su límite y podría colapsar, para corregir este evento muchos proponen que las redes existentes deberán realizar la migración definitiva a IPv6, tomando como referencia que este protocolo permitirá un mayor espacio de direcciones IP, brindando nuevas oportunidades y corrigiendo los problemas existentes en el protocolo de la versión anterior. Sin embargo, debido al aumento de la sobrecarga en IPv6 y su interacción con routers de borde y sistemas operativos que alojan este protocolo de comunicación, se pueden ocasionar evidentemente problemas de rendimiento en la red. El presente artículo se basa en una investigación cuantitativa utilizando un método que permite analizar el rendimiento de redes basadas en IPv6 con IPSec haciendo uso de la simulación con GNS3, con dicha herramienta compara resultados con tres escenarios típicos de implementación en relación a la topología original del presente trabajo, su evaluación determina la diferencia de rendimiento entre escenarios cuando se genera tráfico de una red a otra y se obtiene de entre ellos el un escenario con mejor estabilidad y rendimiento utilizando una metodología experimental, con lo que logramos constatar que su escenario homólogo con utilización de túneles en más óptimo en relación al propuesto en esta investigación, tomando en consideración que las métricas analizadas son ancho de banda, latencia y jitter.

Palabras clave: IPv6; IPSec; ancho de banda; latencia; jitter.

Comó citar el artículo:
Ponce Loor, Y. A. & Herrera Tapia, J. S. (2023). Evaluación del Rendimiento de una red IPv6 utilizando IPSec en Modo Túnel. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 7*(2), 63-70.
https://doi.org/10.33936/isrtic.v7i2.5710

Abstract

IPv4 address space is about to reach its limit and could collapse. To correct this event, many propose that existing networks should make the definitive migration to IPv6, taking as a reference that this protocol will allow a larger IP address space, providing new opportunities and correcting the existing problems in the protocol of the previous version. However, due to the increased overhead in IPv6 and its interaction with edge routers and operating systems that host this communication protocol, network performance problems can obviously occur. This article is based on a quantitative research using a method that allows analyzing the performance of networks based on IPv6 with IPSec using simulation with GNS3, with this tool compares results with three typical scenarios of implementation in relation to the original topology of this work, Its evaluation determines the difference in performance between scenarios when traffic is generated from one network to another and a scenario with better stability and performance is obtained from among them using an experimental methodology, with which we will be able to verify that its counterpart scenario with the use of tunnels is more optimal in relation to the one proposed in this research, taking into consideration that the metrics analyzed are bandwidth, latency and jitter.

Keywords: IPv6; IPSec; bandwidth; latency; Jitter.

Enviado: 23/04/2023
Aceptado: 28/06/2023
Publicado: 03/10/2023

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introducción

El protocolo de Internet fue diseñado sin módulo de seguridad, el mismo que hace evidente que para la comunicación en entornos hostiles los ataques son recurrentes (Shah & Parvez, 2015), en la actualidad hay la necesidad de que se exija como principal requisito en la implementación de una infraestructura lógica de red, el cifrado y la protección de datos con el objetivo de lograr la integridad, confidencialidad y autenticidad de estos (Hogg & Vyncke, 2009). El presente trabajo de investigación tiene como objetivo principal la búsqueda de un método óptimo para analizar y evaluar el rendimiento del protocolo de Internet versión 6 (IPv6) específicamente sobre protocolo de Internet-Seguro (IPSec) en modo túnel, todo esto implementado con una red informática virtual de referencia, dicha infraestructura virtual se la implementará con el uso de VMware, cabe mencionar que esta herramienta tiene muchas opciones de configuración de red permitiendo así implementar una amplia variedad de arquitecturas de red. Básicamente, la virtualización proporciona un entorno en el que se pueden ejecutar varias máquinas virtuales en una sola máquina física, y cada máquina virtual comparte los recursos de esa computadora física en varios entornos (Golden, 2011).

Para cumplir con el objetivo de la presente investigación se creó una topología con dos redes locales, denominada matriz y sucursal respectivamente, esta topología se configuró con cuatro escenarios diferentes IPv6 puro, Pila Doble, IPv6 sobre IPv4 y el modo de túnel IPSec para comunicarse, este último forma una conexión privada entre los dos enrutadores de borde que se encuentran en cada lado de esta comunicación. De forma predeterminada, todos los routers que admiten el protocolo IPv6 también deben ser compatibles con IPSec, como también en el Protocolo de Internet versión 4 (IPv4) pero considerando que este soporte es opcional (Thiruvasagam & George, 2019).

2. Estado del Arte

Para lograr con éxito la presente investigación se consideró la revisión bibliográfica de Trabajos relacionados, los mismo que pudieron notar una amplia demostración de diferencias en lo referente a rendimiento medibles entre las redes IPv4 e IPv6, especialmente cuando se consideran tamaños de paquetes más pequeños (Fiuczynski, Lam, & Bershad, 2018). Como el tamaño del encabezado de IPv6 es el doble que el de Ipv4 (Hogg & Vyncke, 2009).

En la obra creada por Santos (2014), el autor expone un estudio sobre los impactos de IPv6, sus problemas y limitaciones, así como las estrategias de transición entre IPv4 e IPv6. El uso de IPSec, en modo transporte, para interconectar entornos cooperativos, es decir, una red segura que integraría varias organizaciones.

En el trabajo de investigación elaborado por Castro (2014), se evidencia que el objetivo general fue analizar diversas soluciones VPN, que incluyen el uso de un túnel seguro entre diferentes redes. Se centra en el uso de IPSec con IPv4, para proporcionar una VPN. Sin embargo, no se llevó a cabo una implementación efectiva.

La investigación de Falconi & Guedes (2015), analiza el uso dinámico de IPSec con IPv6, para el uso de IPSec solo en casos específicos, y deshabilitarlo en otros que no requieren el uso de IPSec. Solo se realizaron pruebas de tipo de conexión actividad de equipo a equipo, es decir, el modo de transporte IPSec.

El estudio de realizado por Pinheiro (2020), tuvo como objetivo la realización de un análisis protocolos IP versión 4, IP versión 6 e IP versión 4 con IPSec. Como puede ser identificado en este trabajo no se realizaron pruebas con IP versión 6 configurada para IPSec. Otro trabajo que involucra el uso de IPSec es el de que realizó Adeyinka (2018), quien presenta el despliegue de VPN con IPSec. También realiza una demostración de los modelos de conexión como host-a-host, host-to-gateway y gateway-to-gateway. Finalmente, muestra que el modo Gateway-to-Gateway (modo de túnel entre dos enrutadores de borde en una red) puede implementar múltiples conexiones IPSec, para diferentes tipos o clases de tráfico.

El trabajo realizado por Nogueira & Abreu (2017), también hace un análisis general de IPv6, así como la ejecución de pruebas entre dos hosts, interconectados. Los experimentos incluyeron el uso de IPSec y no el uso de este. El modo IPSec implementado para las pruebas fue el transporte.

En el trabajo realizado por Basso (2015), analizan el uso de IPv6 con IPSec. Un análisis de desempeño es sólo con modo de transporte. No se realizaron pruebas de seguridad. Una de las conclusiones presentadas es que archivos de hasta 100 MB tuvieron el mismo tiempo de transferencia de una computadora a otra, usando IPSec y sin IPSec, es decir, no hubo pérdidas en el rendimiento de transferencia cuando se utiliza IPSec.

Finalmente, en el estudio realizado por Godinho (2017), proponen usar IPSec para crear una VPN entre enrutadores, usando el modo de túnel IPSec. Sin embargo, este trabajo utilizó el protocolo IPv4. Se hace referencia en la parte de trabajos futuros de este trabajo, hay una sugerencia para estudiar una implementación de IPv6.

Se toma como referencia la exposición de una matriz de trabajos relacionados tal y como sugiere Wazlawick (2017), quien resume la información en una matriz de referencia. La matriz documental de los trabajos investigados se representa en la Tabla 1, donde se proporciona una descripción general de ellos. Es posible identificar que el presente trabajo complementa el investigado, ya que estudia el protocolo IPv6, así como IPSec en modo túnel

e-ISNN 2550-6730 | Vol. 7, Núm. 2 (71-78): Julio-Diciembre, 2023 | DOI: 10.33936/isrtic.v7i2.5710

y también realiza la implementación para experimentos con estos protocolos.

Tabla 1. Matriz Documental de los Trabajos Investigados

Autor	Protocolo Estudiado	Modo IPSec Estudiado	Había implementación para las pruebas
Dos Santos, 2014	IPv4, IPv6	Transporte	Si
Castro, 2014	IPv4	Túnel	No
Falconi & Guedes, 2015	IPv6	Transporte	Si
Pinheiro, 2020	IPv4, IPv6	Túnel	Si, Excepto IPv6
Adeyinka, 2018	IPv4, IPv6	Transporte, Túnel	No
Nogueira & Abreu, 2017	IPv4, IPv6	Transporte	Si
Basso, 2015	IPv6	Transporte	Si
Godinho, 2017	IPv4	Túnel	Si

Fuente: Propia

En los siguientes apartados de este trabajo de investigación se presentan: la Sección de Materiales y métodos, seguido de Resultados y Discusión y para finalizar la sección de Conclusiones.

3. Materiales y Métodos

A continuación, se presenta la metodología empleada en esta investigación de característica cuantitativa la cual permite capturar datos numéricos de herramientas empleadas para tal fin, además es necesario manifestar que es netamente experimental, con su debido sustento teórico. Ta investigación

Equipos de Cómputo

Configuración de hardware (Host Anfitrión)

• PC HP Compaq Elite 8300

• Sistema Operativo Windows 10 Professional

• Procesador Intel® Core™ i5-3470 CPU © 3.20GHz 3.20 GHz

• 20 GB de RAM

• Adaptador de pantalla NVIDIA GeForce GT710

• Adaptadores de red 10/100/1000

• Configuración de Máquinas Virtuales (VMware Workstation 16.2.2)

• Debian 10 (X2)

• vCPU

• 1 GB de vRAM

Simulador de Redes

GNS3 es ideal para simular entornos de redes en un ambiente lo más real posible, ya que utiliza el sistema operativo de dispositivos CISCO y evalúa el rendimiento de redes en escenarios complejos. Esta herramienta puede ser usada para capturar tráfico de red y detectar cualquier defecto en la simulación con la ayuda del software llamado Wireshark, el mismo que tiene la capacidad de capturar paquetes con la ayuda de PCAP para una mayor comprensión y análisis estadístico de estos. Los dispositivos que se utilizaron en el simulador son:

• Router Cisco c3725 (c3725-adventerprisek9-mz.124-15.T5)

• Docker (AlpineLinux)

En la primera fase de los experimentos, para obtener datos sobre el rendimiento se utilizó la herramienta JPerf. La misma que es una interfaz Java para la versión de línea de comandos de IPerf , que simplifica las pruebas y el análisis. IPerf es una herramienta de análisis de red que es útil para medir el rendimiento de un enlace de red.

Para realizar las pruebas que permitan comparar los protocolos se utilizó la herramienta IPerf3 por el soporte que da al protocolo IPv6, no fue posible realizar la fusión con IPerf ya que estas dos tienen inconvenientes de compatibilidad y semántica del comando o instrucción entre versiones.

Para medir el rendimiento de IPv6 en sus diferentes escenarios simulando situaciones reales, se configuró dos computadores Debian en VMware las mismas que están conectadas a los routers de borde, en esta fase se utilizó Iperf. Como se esperaba, la sobrecarga de salida adicional de nuestro nodo de envío TCP es muy reducida. Sin embargo, el tráfico de retorno, en su mayoría pequeños paquetes de TCP ACK con cargas útiles vacías, contiene una cantidad significativa de sobrecarga adicional.

Escenarios de Evaluación

Con el objetivo de evaluar el rendimiento de IPv6, se configuraron 3 escenarios (descritos posteriormente), los mismos que están basados en el escenario de la Figura 1 que es el escenario principal a comparar original de la presente investigación.

Procedimiento

Para analizar el rendimiento, utilización del ancho de banda y el cálculo de latencia. Los datos se transmitieron de una máquina a otra utilizando las herramientas IPerf, en varios tamaños de archivos que van desde KBytes hasta GBytes durante periodos de 30 segundos.

Cada uno de los computadores tenía instalado las tres herramientas de evaluación: JPerf se utilizó para probar el

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

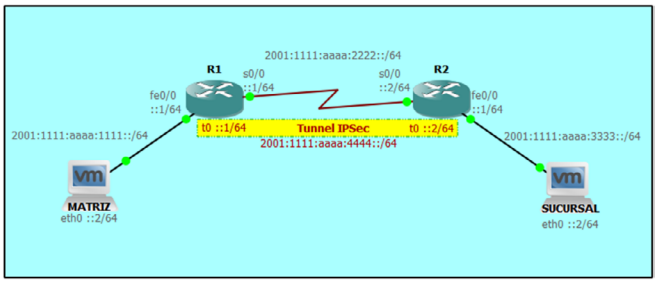

Figura 1. Escenario de una red IPv6 con IPSec.

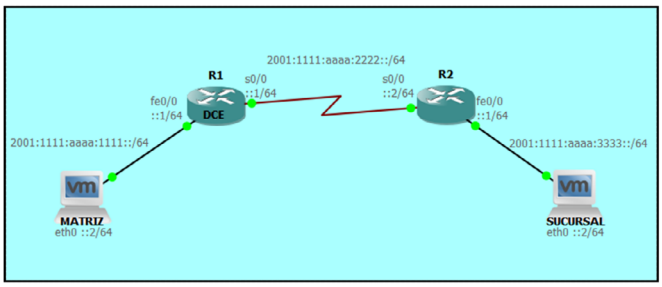

Figura 2. Escenario de red IPv6-Pura.

rendimiento máximo de los sistemas. Se utilizó Iperf para probar las propiedades estadísticas del tráfico centrándose en el delay y el jitter en varios tamaños de carga útil. Los experimentos se ejecutaron sistemáticamente, se repitieron muchas veces, para trabajar con el valor promedio resultante. Cada ejecución se produjo durante treinta segundos. Los experimentos se centraron en tres estadísticas importantes: rendimiento máximo, retardo y fluctuación.

El rendimiento máximo se define como la cantidad máxima de datos que se pueden pasar entre dos hosts. El retraso se define como el tiempo que tarda un paquete en atravesar dos hosts en una red. Jitter es la diferencia o cambio en el retraso con el tiempo. Cada una de estas estadísticas es importante para medir el rendimiento de las redes.

Escenarios

Para la evaluación se utilizaron 3 escenarios, estos se describen a continuación:

El primer escenario Figura 2, se refiere a la transmisión de paquetes sin el uso de IPSec en otras palabras IPv6 Puro. El segundo escenario Figura 3, tuvo la implementación de la pila doble en una arquitectura IPv6, en el tercero escenario Figura 4, se evaluó una red que utiliza IPv6 que trabaja sobre IPv4 utilizando un túnel para la transmisión de datos. Finalmente, el cuarto escenario Figura 1 contó con la configuración de Carga útil de seguridad encapsulada (ESP) en IPSec.

En todos los escenarios, para las pruebas se utilizó la herramienta IPerf3, la misma que generó un flujo de datos, simulando la transferencia de un archivo desde la red de sucursal a la red Matriz. Se consideran las medidas de cuánto tiempo tomó una transferencia de archivo en segundos, sin embargo, la conversión a minutos puede facilitar la comprensión de los resultados. Por lo tanto, se transfieren archivos del tamaño de 50, 100, 200, 400, 800, 1600, 3200 y 6400 MB desde una red a la otra, las mismas que están atrás de los enrutadores de borde R1 y R2 indicados en

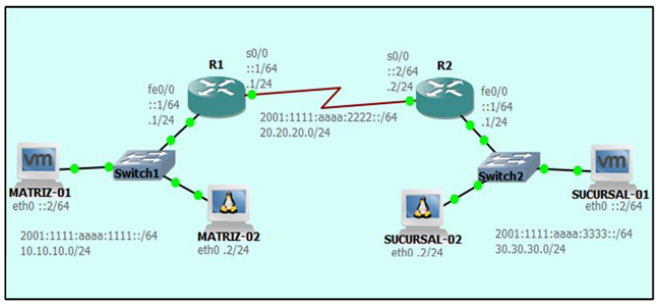

Figura 3. Escenario de red Doble Pila

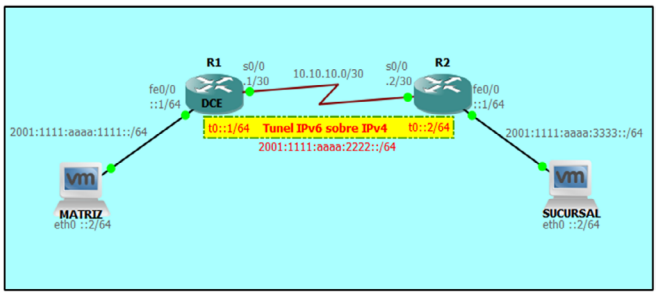

Figura 4. Escenario de red IPv6 over IPv4.

las figuras que está en R2, La herramienta de análisis Wireshark permitió verificar los paquetes IP.

Finalmente, en el último escenario, los paquetes IP usaban IPSec con el encabezado ESP. De esta forma, como en el párrafo anterior, la herramienta Wireshark permitió la verificación del uso de ESP, que garantiza el cifrado de datos, ver Figura 5.

4. Resultados y Discusión

En esta sección se presentan los resultados de la evaluación de los diferentes escenarios de implementación de IPv6.

e-ISNN 2550-6730 | Vol. 7, Núm. 2 (71-78): Julio-Diciembre, 2023 | DOI: 10.33936/isrtic.v7i2.5710

Rendimiento IPv6 & IPv6 con IPSec

Tomando como referencia los resultados mostrados en las Figura 6 y 7 se puede evidenciar que, las métricas ancho de banda y latencia (jitter) de una red IPv6 pura son superiores cuando se utiliza protocolo seguro IPSec en la misma red, teniendo en cuenta que el tráfico generado correspondería archivos multimedia es decir que sean transferidos vía UDP. Para este caso, se deduce que los resultados de IPv6 con IPSec decrecen en comparación con IPv6 pura, consecuentemente debido al uso de la cabecera que utiliza IPSec (ESP), las mismas que afectarían

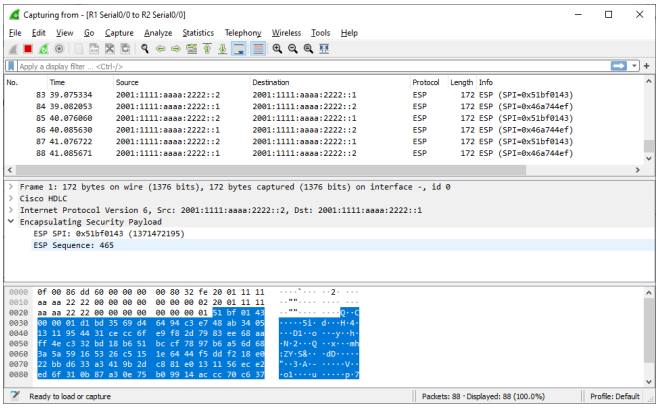

Figura 5. Captura de Tráfico del encabezado ESP IPv6 con IPSec.

a los resultados que se esperaban al general tráfico multimedia.

Comparación de entre escenarios

La Tabla 2 proporciona los resultados de los experimentos de rendimiento que se llevaron a cabo con 2 enrutadores, los mismos que se representan en la Figura 8. Cabe indicar que los paquetes eran del tipo TCP, con un tamaño de ventana de 16 KBytes, es decir, el receptor de los datos confirmó la recepción de los datos cada 16 KBytes transferidos. Con respecto a la transmisión de datos, esto fue igual a aproximadamente 1 Mbits por segundo. De esto modo que, 1 Mbit equivale a 128 Kilobytes, que dividido por 16 KBytes de la ventana, da como resultado 8 acuses de recibo de datos por segundo.

Como se puede observar el tiempo es similar en cada uno de los escenarios, para un mejor análisis de resultados se utiliza la varianza entre los resultados de los diferentes escenarios en relación con el que utiliza IPSec, junto con las proyecciones de tendencia que se muestran en las siguientes figuras, para la obtener estos se ha empleado la siguiente formula de comparación.

%Δ= Relación de Cambio Porcentual

V0: dato del escenario a comparar (IPv6 - Pila doble – IPv6 over IPv4)

V1: datos del escenario en cuestión (IPv6 con IPSec)

La Figura 12 presenta, la variación entre los experimentos descritos anteriormente.

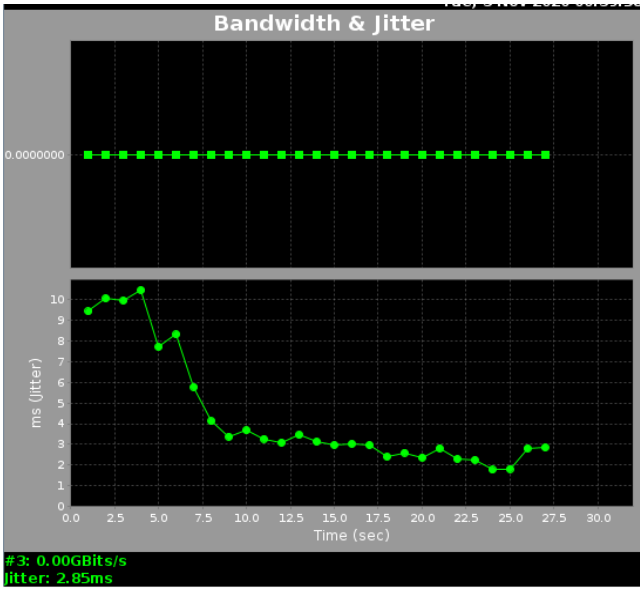

Figura 6. IPv6 Ancho de Banda & Jitter en Gbps.

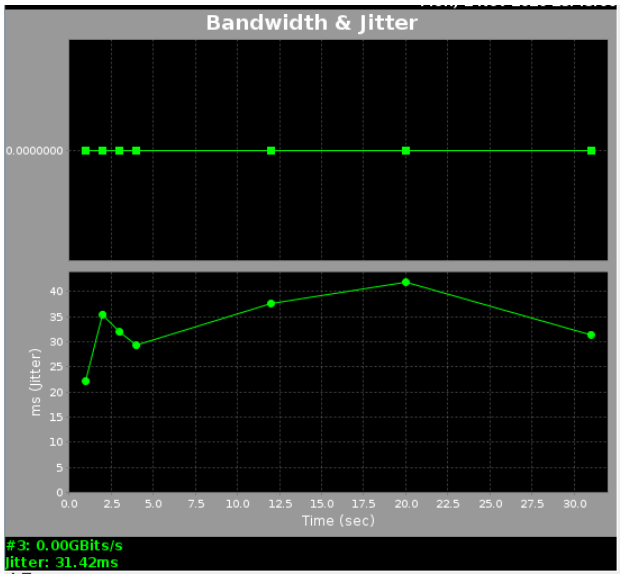

Figura 7. IPv6 con IPSec Ancho de Banda & Jitter en Gbps.

De acuerdo con la comparación, se puede evidenciar que, los resultados del experimento con la topología IPv6-over- IPv4 en varianza con IPv6 con IPSec tienen proporciones equivalentes de estabilidad en relación con los otros escenarios lo cual se puede ver con más detalle en la Figura 11.

Discusión

Tomando como referencia los datos sobre el rendimiento mostrados en la sección anterior, se presenta la Tabla 3, donde se puede evidenciar que, con un mayor rendimiento, los retrasos varían. Se encuentra que los parámetros de utilización del ancho

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Tabla 2. Matriz con los resultados Obtenidos en minutos

Tamaño de Archivo (MB)	Tiempo en minutos IPv6	Pila Doble	IPv6 over IPv4	IPv6 IPSec
50	6	7	7	7
100	13	13	13	14
200	27	26	27	29
400	52	52	54	57
800	107	107	109	118
1600	211	213	217	235
3200	427	422	436	457
6400	858	847	868	911

Fuente: Propia

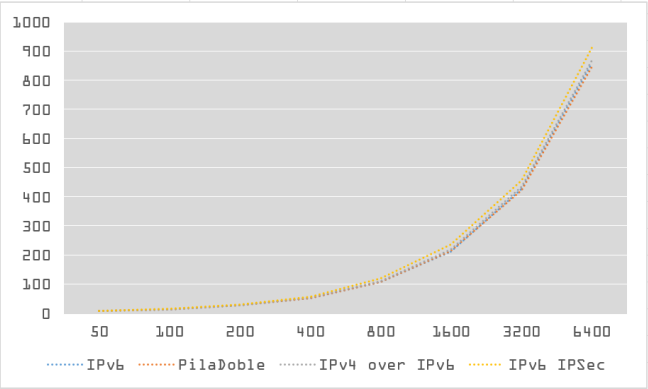

Figura 8. Resultados Obtenidos del retardo según tráfico generado en MB.

de banda y latencia (jitter) de una red IPv6 pura son superiores cuando se utiliza protocolo seguro IPSec en la misma red. Para este caso, se deduce que los resultados de IPv6 con IPSec son un poco más pobres en comparación con IPv6 pura debido al uso de la cabecera que utiliza IPSec (ESP). Es importante poner especial énfasis a estas métricas porque determina la precisión de la prueba la misma afecta el resultado de rendimiento. La

$$\%\Delta = \frac{V_1 - V_0}{V_0} \times 100\%$$

configuración de la prueba se diseñó de tal manera que se obtenga un resultado comparativo preciso del rendimiento de la red IPv6 Pura e IPv6 con IPSec en un entorno de red virtual controlado.

Se observa que la varianza relacionada con IPv6 over IPv4 es la más óptima esto debido al túnel que ambas implementan para

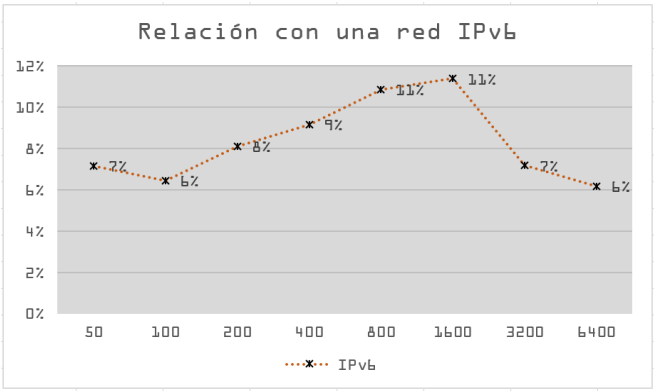

Figura 9. Relación de cambio y variación con una red IPv6 Pura Vs IPv6 IPSec

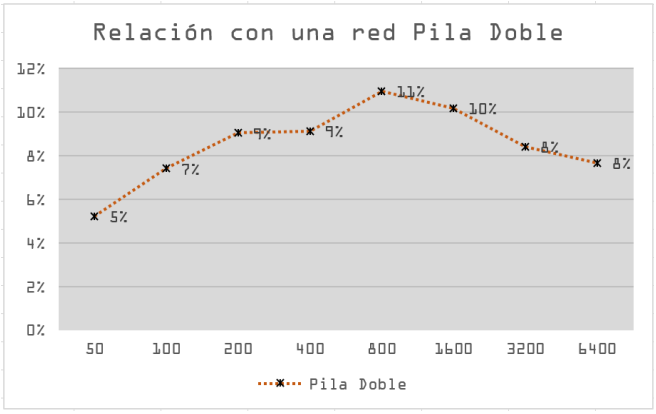

Figura 10. Relación de cambio y variación con una red Pila doble Vs IPv6 IPSec.

la línea dedicada al transporte de datos, de una u otra forma esto hace que el cifrado sea más seguro y dichos datos sean entregado de forma íntegra tal y como se originaron desde una red a la otra. Si observamos la Figura 11 podemos corroborar lo dicho anteriormente, el grado de estabilidad lo realiza la implementación del túnel.

e-ISNN 2550-6730 | Vol. 7, Núm. 2 (71-78): Julio-Diciembre, 2023 | DOI: 10.33936/isrtic.v7i2.5710

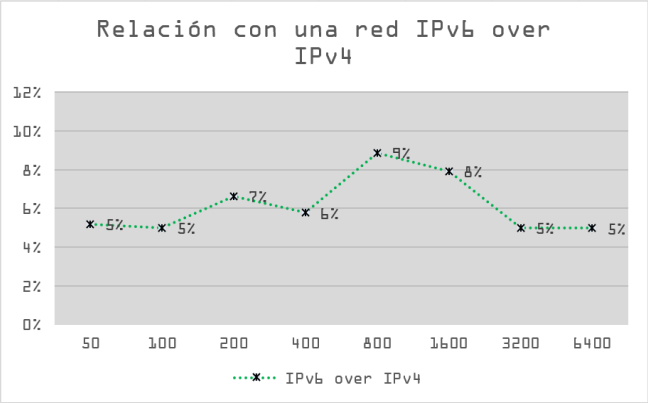

Figura 11. Relación de cambio y variación con una red IPv6 over IPv4 Vs IPv6 IPSec.

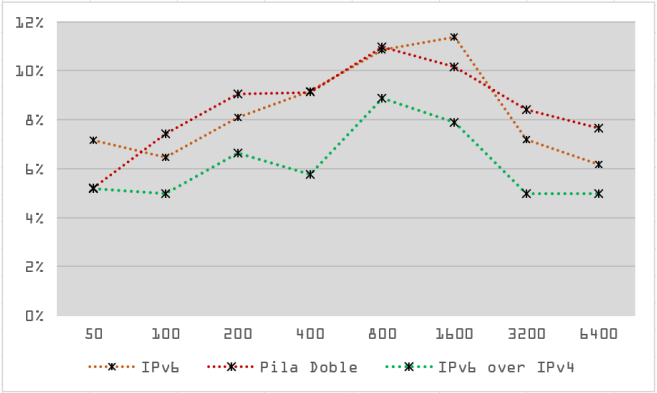

Figura 12. Variación entre escenarios.

5. Conclusiones

El resultado de las diferentes pruebas muestra una diferencia de rendimiento sustancial entre los escenarios propuestos. Durante el proceso de evaluación de las herramientas, se evidenció las incompatibilidades que había entre versiones de Iperf y Jperf donde se deseaba descubrir el rendimiento promedio, tomando en consideración que estos no cambian incluso cuando las herramientas alcanzan la condición de estado estable o se transfiere un tamaño de archivo grande. También se descubrió con la herramienta Wireshark que el rendimiento máximo real de IPv6 para el enlace serial no alcanzaba el máximo debido a la sobrecarga del Protocolo de control de transmisión (TCP) durante el proceso de transferencia de archivos, este no permite monitorear el estado de los equipos durante la ejecución de la simulación.

La ejecución de las pruebas comparativas permitió la verificación de la viabilidad de usar el protocolo IPSec con su encabezado ESP. En lo que se refiere al rendimiento con el uso de encabezado ESP (túnel), en los diferentes escenarios, se recomienda su uso para aquellos interesados en la autenticación, integridad y confidencialidad de los paquetes.

Tabla 3. Rendimiento entre IPv6 & IPv6 con IPSec

Rendimiento logrado en UDP	Promedio Bytes/seg.	Promedio Jitter.
IPv6	0.00 Gbits/s	2.85 ms
IPv6 con IPSec	0.00 Gbits/s	31.42 ms

Fuente: Propia

Tabla 4. Resumen de varianzas entre escenarios

Tamaño de Archivo (MB)	IPv6 Pura	Pila Doble	IPv6 over IPv4
50	7%	5%	5%
100	6%	7%	5%
200	8%	9%	7%
400	9%	9%	6%
800	11%	11%	9%
1600	11%	10%	8%
3200	7%	8%	5%
6400	6%	8%	5%

Fuente: Propia

La prueba de simulación arrojó que relacionando el escenario IPSec con IPv6 over IPv4 se tienen resultados más óptimos esto debido al túnel que ambas escenarios implementan para la línea dedicada al transporte de datos, hay que considerar que este es el más eficiente ya que la misma hace que el cifrado sea más seguro y dichos datos sean entregado de forma íntegra tal y como se originaron desde una red a la otra.

Las contribuciones del presente trabajo de investigación son para fomentar el uso de IPSec y túneles en un entorno IPv6, el mismo que cuando es utilizado con su encabezado ESP, garantiza, que el paquete conserve la integridad en la red. En cuanto a las limitaciones de esta investigación fue la no utilización de equipos reales por motivo económicos y los relacionados al Covid-19. Sin embargo, la herramienta GNS3 aseguró que los experimentos tengan la misma credibilidad que los equipos reales, mediante la virtualización de routers, que utilizó fielmente el mismo sistema operativo (IOS) que el equipo real.

Finalmente, la oportunidad de investigación futura estaría relacionado con realizar un estudios con los mismos experimentos con enrutadores en el paradigma de redes definidas por software (SDN), que básicamente eliminan la capa de control (responsable de definir los procesos de enrutamiento e ingeniería de tráfico, políticas de seguridad), que estaba en la red y colocarlo en un servidor SDN centralizando, así se tendría el control de una red completa que convendría fielmente para monitorear uno de los problemas en la ejecución del experimento.

e-ISNN 2550-6730 | **Vol. 7, Núm. 2 (71-78): Julio-Diciembre, 2023** | **DOI: 10.33936/isrtic.v7i2.5710**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Contribución de los autores

Yumber Alejandro Ponce Loor: Conceptualización, Curación de datos, Análisis formal, Adquisición de fondos, Investigación, Metodología, Administración del proyecto, Recursos, Software, Supervisión, Validación, Visualización, Redacción – borrador original, Redacción – revisión y edición. **Jorge Herrera-Tapia:** Análisis formal, Administración del proyecto, Recursos, Software, Supervisión, Visualización, Redacción – borrador original, Redacción – revisión y edición.

Conflictos de interés

Los autores declaran no tener ningún conflicto de interés.

Referencias bibliográficas

Adeyinka, O. (2018, julio 1). IPSec Mechanism for Implementing VPN.

Basso, C. (2015). Implementação de IPSEC integrado com o IPv6. Recuperado de http://repositorio.roca.utfpr.edu.br:8080/jspui/handle/1/198

Castro, R. de A. e. (2014). Uma analise de soluções VPN em redes corporativas de alta capilaridade.

Falconi, A. P., & Guedes, U. T. V. (2015). *Proposta de Uso Dinâmico do IPSec no IPv6. 3.*

Fiuczynski, M. E., Lam, V. K., & Bershad, B. N. (2018). The Design and Implementation of an IPv6/IPv4 Network Address. *USENIX Annual Technical Conference,* 11.

Godinho, M. E. M. (2017). Uma arquitetura de implementação de redes virtuais privadas sobre a estrutura da Universidade do Contestado—UnC. 79.

Golden, B. (2011). *Virtualization For Dummies.* John Wiley & Sons.

Hogg, S., & Vyncke, E. (2009). *IPv6 security (1.a ed.).* Indianapolis, IN: Cisco Press. Recuperado de ciscopress.com

Nogueira, E., & Abreu, O. (2017). Introdução ao IPv6 e Desempenho do IPSec com IPv4 e IPv6. Recuperado de https://fdocumentos.tips/document/introducao-ao-ipv6-e-desempenho-do-ipsec-com-ipv4-e-ipv6.html

Pinheiro, A. (2020, octubre). Estudo comparativo e análise de desempenho entre os protocolos de comunicaçao IPv4 e IPv6. https://doi.org/10.13140/RG.2.2.24026.57280/1

Santos, C. R. (2014). *Integração de ipv6 em um ambiente cooperativo seguro* (Tesis). Universidade Estadual de Campinas, Instituto de Computação.

Shah, J. L., & Parvez, J. (2015). Security Issues in Next Generation IP and Migration Networks. *Journal of Computer Engineering, 17*(6). https://doi.org/10.9790/0661-17131318

Thiruvasagam, P., & George, K. J. (2019). IPSec: Performance Analysis in IPv4 and IPv6. *Journal of ICT Standardization, 7*(1), 59-76. https://doi.org/10.13052/jicts2245-800X.714

Wazlawick, R. (2017). *Metodologia de Pesquisa para Ciência da Computação* (2o edição). GEN LTC.

e-ISNN 2550-6730 | Vol. 7, Núm. 2 (71-78): Julio-Diciembre, 2023 | DOI: 10.33936/isrtic.v7i2.5710