Medición del rendimiento en servidores en la nube con TLS y WireGuard

Enrique Alcalá-Zamora Castro (enriqueaz@correo.ugr.es)
18/06/2025

***Abstract*—Este estudio analiza el impacto de la encriptación en el rendimiento de servidores en la nube de Google Cloud al emplear TLS (Stunnel) y VPN (WireGuard). Se utilizarán técnicas activas y pasivas de medición mediante herramientas como iperf, hping3, traceroute, netflow, vmstat, sar. Se evaluarán métricas clave como delay, throughput y jitter para comparar el efecto de cada tecnología sobre la eficiencia de la red.**

***Index Terms*—TLS, VPN, WireGuard, Stunnel, delay, throughput, jitter, consumo de CPU.**

NOVEDADES CON RESPECTO AL INFORME PRELIMINAR

Se ha ajustado el órden de los análisis para adecuarse mejor al flujo de trabajo recomendado.

Se han revisado los análisis post hoc para los factores significativos en los modelos ANOVA.

Se han añadido casos adicionales de análisis post hoc para interacciones entre dos factores (casos Carga de Red).

Se ha detallado la planificación de la toma de medidas, con fin de justificar la independencia entre *replicates*.

I. DESCRIPCIÓN DE MÉTRICAS Y FUNCIONES A MEDIR

El objetivo de este estudio es el de evaluar el impacto de la encriptación en el rendimiento de servidores en la nube. Para ello, se analizarán las siguientes métricas:

- **Rendimiento:** delay, throughput y jitter.
- **Alcanzabilidad**
- **Consumo de recursos:** uso de CPU y memoria

Adicionalmente, se analizará la carga de la red mediante netflow para estudiar el impacto en el tráfico global.

II. DISCUSIÓN SOBRE TÉCNICAS PASIVAS Y ACTIVAS

Se utilizará una combinación de técnicas activas y pasivas para evaluar el rendimiento de la red, las cuales se muestran en la siguiente tabla:

TABLE I. Detalle del conjunto de técnicas de medición

Métrica	***Herramienta***	***Técnica***	***Medida***	***Fuente***
Delay	*hping3*	Activa, continuity-check	Puntual y/o agregada	Prot. ICMP
Throughput	*iperf3*	Activa, rendimiento	Agregada	Prot. ICMP/TCP/UDP
Jitter	*iperf3*	Activa, rendimiento	Agregada	Prot. UDP
Load	*Netflow, sar*	Pasiva, flujos	Agregada	Prot. Netflow
Consumo de CPU/RAM	*vmstat*	Pasiva, uso de sistema	Agregada	Kernel

El delay se medirá con sondas ICMP a través de hping3, permitiendo obtener una media del round-trip-time y calcular pérdidas para determinar la alcanzabilidad.

El throughput se evaluará mediante iperf3, generando tráfico en TCP y UDP. Se analizará también el jitter en las pruebas UDP.

La carga de la red se estudiará mediante netflow y SAR (*System Activity Report*), recopilando información de flujos de tráfico para evaluar la eficiencia de las conexiones encriptadas.

El consumo de recursos hardware en el servidor será analizado con herramientas de monitoreo del sistema como *vmstat*, permitiendo evaluar la carga adicional generada por TLS y VPN.

III. ANÁLISIS COMPARATIVO ENTRE TLS Y VPN

Las pruebas se llevarán a cabo en los siguientes escenarios:

- **Escenario 1:** Comunicación sin encriptación.
- **Escenario 2:** Comunicación con TLS (Stunnel).
- **Escenario 3:** Comunicación mediante VPN (WireGuard).

Cada escenario se evaluará en diferentes momentos del día para analizar el impacto de la carga horaria en el rendimiento de la red.

Se espera que la encriptación genere un impacto en el rendimiento, aumentando el delay y métricas como el consumo de recursos de red y cpu. Stunnel podría ofrecer un mejor rendimiento en comparación con WireGuard debido a su menor overhead y eficiencia en la encapsulación de paquetes. Se analizará si estas diferencias son significativas y si afectan a la calidad del servicio en escenarios de alta demanda.

IV. DESCRIPCIÓN DE RESPUESTAS, FACTORES Y NIVELES

Se consideran las siguientes **respuestas** en el experimento:

- **Rendimiento de red**: delay, throughput y jitter.
- **Alcanzabilidad**: pérdidas de paquetes y tiempos de respuesta.
- **Consumo de recursos**: uso de CPU y memoria, volumen de tráfico agregado (netflow).

TABLE 2. TABLA CON LAS RESPUESTAS, FACTORES, NIVELES Y REPLICATES DEFINIDOS

Métrica	***Herramienta***	***Factores***	***Niveles***	***Replicates***
Throughput	*hping3*	F1: Hora del día F2: Tipo de día F3: Configuración F4: Rate de tráfico	F1: 8h, 15h, 19h, 22h F2: Laborables/Fin de semana F3: Sin cifrar, TLS, VPN F4: 10Mbps, 100Mbps	4
Delay	*iperf3*	F1,F2,F3	Mismos niveles	4
Jitter	*iperf3*	F1,F2,F3,F4	Mismos niveles	4
Load	*Netflow, sar*	F1,F2,F3	Continua	4
Consumo de CPU/RAM	*vmstat*	F1,F2,F3	Continua	4

Todas las métricas serán registradas considerando diferentes horas del día (factor I, de tipo "estorbo" o nuisance, tratado como cualitativo y fijo), distintas categorías de día (factor II, también nuisance, cualitativo y fijo), diversas configuraciones de comunicación (factor III, factor de diseño cualitativo, correspondiente a conexión sin cifrado, mediante TLS con Stunnel o a través de VPN usando WireGuard) y varios niveles de rate de tráfico (factor IV, que será igualmente tratado como cualitativo y fijo).

V. DISCUSIÓN

Aleatorización: No es posible aleatorizar los factores temporales como la hora del día y el tipo de día (laborable o fin de semana). Sin embargo, sí se ha realizado aleatorización en el orden de medición de las configuraciones de comunicación (sin cifrado, TLS y VPN) y las tasas de tráfico (10 Mbps, 100 Mbps) dentro de cada réplica.

Réplicas: Para cada combinación de factores experimentales, se han realizado cuatro réplicas distribuidas temporalmente para garantizar la independencia de las observaciones. Las pruebas se ejecutaron durante dos semanas consecutivas, en los días martes, jueves, sábado y domingo, abarcando tanto jornadas laborables como fines de semana. Esta planificación temporal introduce variabilidad natural en las condiciones de red y reduce el riesgo de autocorrelación entre réplicas.

Además, se ha respetado un intervalo mínimo de 48 horas entre mediciones consecutivas de una misma combinación y se han configurado las mediciones con esperas (ver sección VI), reforzando la validez de los análisis inferenciales posteriores.

Automatización: Se utilizarán scripts para la ejecución automatizada de mediciones, almacenando los resultados de manera sincronizada con las variables de control del experimento.

Factores y niveles: La elección de distintas horas del día (8h, 15h, 19h, 22h) busca capturar variaciones diarias típicas del tráfico de red. El uso de dos tasas de tráfico (10 Mbps y 100 Mbps) permite representar aplicaciones de bajo y alto consumo de ancho de banda. La comparación entre comunicaciones sin cifrado, con TLS (Stunnel) y con VPN (WireGuard) proporciona una perspectiva completa del impacto de los mecanismos de protección de la comunicación.

VI. CONFIGURACIÓN DEL ESCENARIO EXPERIMENTAL

El escenario experimental ha sido desplegado utilizando la plataforma **Google Cloud Platform (GCP)**, seleccionando dos regiones europeas separadas geográficamente para simular comunicaciones interregionales dentro del continente. Las máquinas virtuales empleadas han sido:

- **Servidor:** ubicado en **Frankfurt, Alemania** (europe-west3)
- **Cliente:** ubicado en **Madrid, España** (europe-southwest1)

Ambas instancias ejecutan un sistema operativo basado en Linux (Ubuntu Server 22.04 LTS), con acceso mediante SSH habilitado (puerto 22). El servidor ha sido configurado para

ejecutar un demonio iperf3 en escucha permanente sobre el puerto 5203, además de aceptar conexiones de stunnel y VPN WireGuard para emular distintos modos de transmisión.

Para permitir el correcto funcionamiento de las herramientas de medida y los distintos modos de comunicación, fue necesario **abrir y configurar específicamente una serie de puertos** en las reglas de firewall de Google Cloud:

- **TCP/UDP 5203:** Para pruebas con iperf3 (modo normal y VPN)
- **TCP 5204:** Canal TLS protegido a través de stunnel
- **UDP 51820:** Puerto por defecto de WireGuard
- **TCP 22:** SSH para gestión remota
- **ICMP / hping3:** Para envío de paquetes tipo SYN (requiere privilegios elevados)

Además, se configuró una **interfaz de red secundaria wg0** en el cliente y el servidor para establecer el túnel VPN mediante WireGuard. Esta interfaz es utilizada de forma exclusiva en el modo "vpn", mientras que en modo "normal" y "tls" se emplea la interfaz principal *ens4*.

Se definieron **tres modos de comunicación** para simular distintos escenarios de red y evaluar cómo afectan al rendimiento:

1. **Modo normal:** Conexión directa al servidor mediante iperf3 en TCP/UDP sin cifrado.
2. **Modo TLS:** Conexión cifrada a través de stunnel, emulando tráfico sobre TLS.
3. **Modo VPN:** Comunicación a través de un túnel cifrado WireGuard (wg0).

Cada uno de estos modos requiere una configuración específica:

- Stunnel se lanza en el cliente antes de cada prueba TLS, con su configuración personalizada.
- wg-quick se utiliza para subir y bajar la interfaz VPN según sea necesario.
- Al final de cada iteración, los túneles son cerrados para evitar interferencias entre pruebas.

El proceso de recolección de datos ha sido completamente **automatizado mediante un script en bash**. Este script verifica que la ejecución se realiza en un día laborable o fin de semana válido, y que la hora actual está dentro de las horas definidas para realizar las pruebas: 08h, 15h, 19h, 22h.

```
mkdir -p resultados/$FECHA/${HORA_ACTUAL}h

for MODO in $(printf "%s\n" "${MODOS[@]}" | shuf); do
  for RATE in $(printf "%s\n" "${RATES[@]}" | shuf); do

    case $MODO in
      "normal")
        DEST=$IP_NORMAL
        PORT=$PUERTO
        ;;
      "tls")
        DEST=$IP_TLS
        PORT=$PUERTO_TLS
        pkill -f stunnel
        stunnel stunnel_client.conf
        sleep 2
        ;;
      "vpn")
        DEST=$IP_VPN
        PORT=$PUERTO
        sudo wg-quick up wg0
        sleep 2
        ;;
    esac

    echo "[$(date)] Modo: $MODO, Rate: $RATE, Hora: $HORA_ACTUAL, Día: $FECHA"
```

Fig. 1. Fragmento del script de medición en el que se definen las configuraciones.

Por cada combinación de:

- Día de la semana (laborable o fin de semana),
- Hora del día,
- **Modo de comunicación** (normal, tls, vpn),
- **Rate de transmisión** (10M, 100M),

se ejecutan las siguientes acciones:

1. **Medidas de rendimiento** mediante iperf3, en **modo TCP y UDP**, durante 60 segundos por prueba.
2. Monitorización simultánea del sistema mediante:
    - vmstat: capturando métricas de uso de CPU, memoria y procesos durante la duración del test.
    - SAR: capturando estadísticas de tráfico en la interfaz principal ens4 y la interfaz VPN wg0 si está activa.
3. **Medidas activas de red** usando hping3, enviando paquetes SYN al puerto utilizado para registrar posibles pérdidas, retardos y comportamiento de la red a bajo nivel.

La salida de cada comando es redirigida a un fichero dentro de una estructura de carpetas jerárquica organizada por día y hora de medición, incluyendo marca temporal en el nombre para facilitar su trazabilidad y análisis posterior.

Los resultados se almacenan en la ruta:

resultados/$FECHA/${HORA_ACTUAL}h/

Con nombres del tipo:

- ${MODO}_${RATE}_tcp_${TIMESTAMP}.txt
- ${MODO}_${RATE}_udp_${TIMESTAMP}.txt
- ${MODO}_${RATE}_vmstat_${TIMESTAMP}.txt
- ${MODO}_${RATE}_vnstat_${TIMESTAMP}.txt
- ${MODO}_${RATE}_hping_${TIMESTAMP}.txt

```
echo "[$(date)] Modo: $MODO, Rate: $RATE, Hora: $HORA_ACTUAL, Dia: $FECHA"

vmstat 1 60 > resultados/$FECHA/${HORA_ACTUAL}h/${MODO}_${RATE}_vmstat_${TIMESTAMP}.txt &
VMSTAT_PID=$!

vnstat -i ens4 -tr 60 > resultados/$FECHA/${HORA_ACTUAL}h/${MODO}_${RATE}_vnstat_${TIMESTAMP}.txt &
VNSTAT_PID=$!

vnstat -i wg0 -tr 60 > resultados/$FECHA/${HORA_ACTUAL}h/${MODO}_${RATE}_vnstatwg0_${TIMESTAMP}.txt &
VNSTAT_PID=$!


# iperf3 TCP
iperf3 -c $DEST -p $PORT -b $RATE -t 60 > resultados/$FECHA/${HORA_ACTUAL}h/${MODO}_${RATE}_tcp_${TIMESTAMP}.txt
sleep 30

# Esperar a que terminen los procesos en segundo plano
wait $VMSTAT_PID
wait $VNSTAT_PID

# iperf3 UDP
iperf3 -c $DEST -p $PORT -u -b $RATE -t 60 > resultados/$FECHA/${HORA_ACTUAL}h/${MODO}_${RATE}_udp_${TIMESTAMP}.txt
sleep 30

if [[ "$MODO" == "tls" ]]; then
sudo hping3 -c 100 -S -p 5204 34.159.101.197 >> resultados/$FECHA/${HORA_ACTUAL}h/${MODO}_${RATE}_hping_${TIMESTAMP}.txt
else
sudo hping3 -c 100 -S -p $PORT $DEST >> resultados/$FECHA/${HORA_ACTUAL}h/${MODO}_${RATE}_hping_${TIMESTAMP}.txt
fi
sleep 10

# Apagar túneles si aplica
[[ "$MODO" == "tls" ]] && pkill -f stunnel
[[ "$MODO" == "vpn" ]] && sudo wg-quick down wg0

sleep 5
```

Fig. 2. Fragmento del script de medición en el que se establecen las herramientas para dicha labor.

Esto permite un análisis estructurado de datos para posterior estudio estadístico o visualización.

- La selección aleatoria de modos (normal, tls, vpn) y tasas de transmisión (10M, 100M) mediante *shuf* en el script introduce **aleatoriedad controlada** en las ejecuciones, mitigando sesgos debidos al orden.
- **Se han programado esperas (*sleep*)** entre pruebas y entre procesos concurrentes para evitar solapamientos y asegurar independencia entre medidas.
- Cada ejecución dura aproximadamente 3–4 minutos, incluyendo tiempo de prueba, limpieza y espera.
- Se ha realizado una monitorización periódica para comprobar que los servicios (stunnel, wg-quick, iperf3) estaban activos en el servidor antes de cada ejecución.

VII. ANÁLISIS DE DATOS

A. ESTUDIO DE LA LATENCIA

Uno de los objetivos principales de este estudio ha sido analizar cómo los mecanismos de cifrado —**TLS (Stunnel)** y **WireGuard (VPN)**— afectan al **retardo (delay)** en entornos cloud. La latencia se midió empleando técnicas activas mediante la herramienta *hping3* replicando las mediciones en cuatro franjas horarias (8h, 15h, 19h y 22h), tanto en días laborables como en fines de semana, y bajo tres configuraciones de red: sin cifrado, cifrado con TLS, y conexión mediante VPN.

El análisis de los residuos del modelo de latencia permite evaluar en profundidad la estabilidad y coherencia del comportamiento de la red bajo distintos factores experimentales. Para ello, se recurrió al uso de diagramas de caja que muestran la dispersión de los residuos en función de cuatro factores clave: configuración de comunicación, hora del día, tasa de transmisión y tipo de día (laborable o fin de semana).

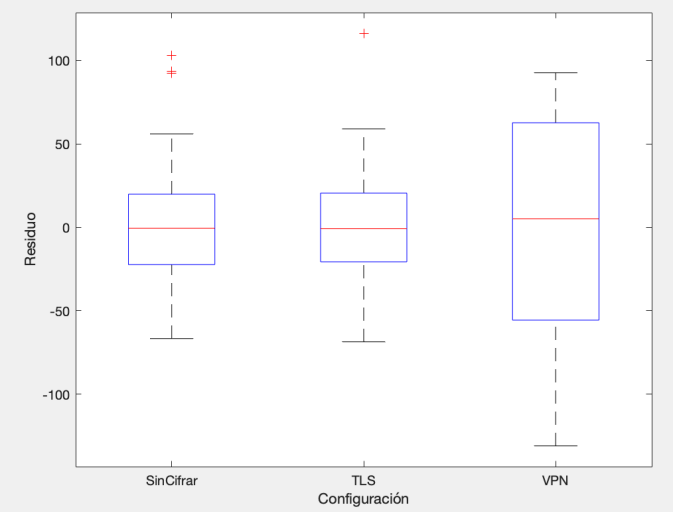

Fig. 3. Residuos frente a configuración (latencia).

En primer lugar, al observar la latencia residual según el tipo de configuración (sin cifrado, TLS y VPN), se aprecia que el uso de VPN introduce una mayor variabilidad en los residuos, con un rango intercuartílico más amplio y presencia de valores atípicos más extremos (**ver Figura 3**). Esta inestabilidad puede atribuirse al overhead adicional generado por el cifrado y encapsulamiento de los paquetes en WireGuard. Por el contrario, las configuraciones sin cifrado y con TLS presentan un comportamiento más compacto, con residuos más concentrados en torno al cero, lo que sugiere que su impacto sobre la latencia es más predecible y menos variable. A pesar de que el análisis estadístico previo no encontró diferencias significativas en los valores promedio de latencia entre configuraciones, este análisis gráfico confirma que existen diferencias en la dispersión que podrían tener relevancia en aplicaciones sensibles a fluctuaciones temporales.

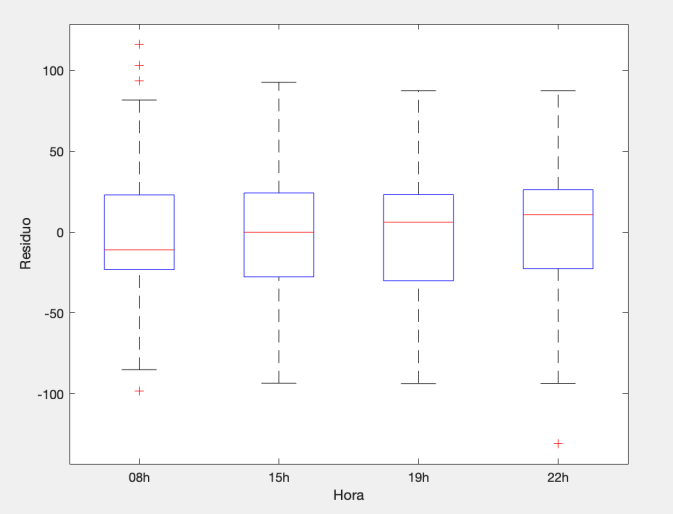

Fig. 4. Residuos frente a hora (latencia).

En cuanto al comportamiento de los residuos a lo largo del día, se ha comparado la latencia en las franjas de 08h, 15h, 19h y 22h (**ver Figura 4**). La variación entre horas es leve, aunque se detecta una ligera tendencia a residuos más elevados a las 22h, posiblemente asociada a patrones de uso nocturnos o procesos automáticos de mantenimiento en la infraestructura de red. No obstante, en general las medianas permanecen próximas a cero, y el modelo parece comportarse con estabilidad a lo largo del día. Este resultado respalda la idea de que, aunque la hora del día tiene un efecto estadísticamente significativo en la latencia (como se demostró en el análisis ANOVA), su influencia sobre la variabilidad del modelo es moderada y, sobre todo, dependiente de su interacción con otros factores.

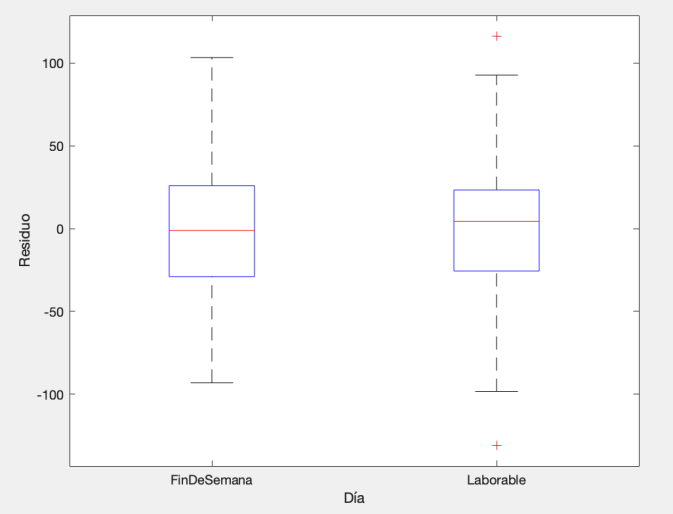

Fig. 5. Residuos frente a días (latencia).

Adicionalmente, se evaluó el efecto del tipo de día (laborable o fin de semana) sobre los residuos (**ver Figura 5**). Las distribuciones obtenidas fueron bastante similares en ambos casos, lo que sugiere que este factor no afecta significativamente la latencia residual.

Skewness	Kurtosis
0.0021	3.0551

El valor de **skewness** (0.0021) indica una distribución prácticamente simétrica, mientras que la **kurtosis** (3.0551) sugiere una forma ligeramente más apuntada que la normal. Estos valores, calculados tras aplicar una transformación *tiedrank* para suavizar la influencia de valores repetidos, confirman que la distribución de residuos es suficientemente cercana a la normalidad para validar los supuestos del modelo ANOVA.

El conjunto de datos recogido ha sido sometido a un análisis mediante ANOVA, para evaluar la significancia de cada uno de los factores y sus posibles interacciones. Previamente, se llevó a cabo un análisis de los **residuos del modelo** para comprobar el cumplimiento del supuesto de normalidad, requisito clave en este tipo de análisis estadístico.

En la **Figura 6** se muestra el gráfico de probabilidad normal (Q-Q plot) de los residuos crudos. Si bien la mayoría de los puntos siguen la diagonal de referencia, se observan ciertas desviaciones en los extremos, lo que sugiere la presencia de valores atípicos o colas pesadas. Esta desviación leve no compromete seriamente la validez del modelo, pero ha sido considerada en la interpretación de los resultados.

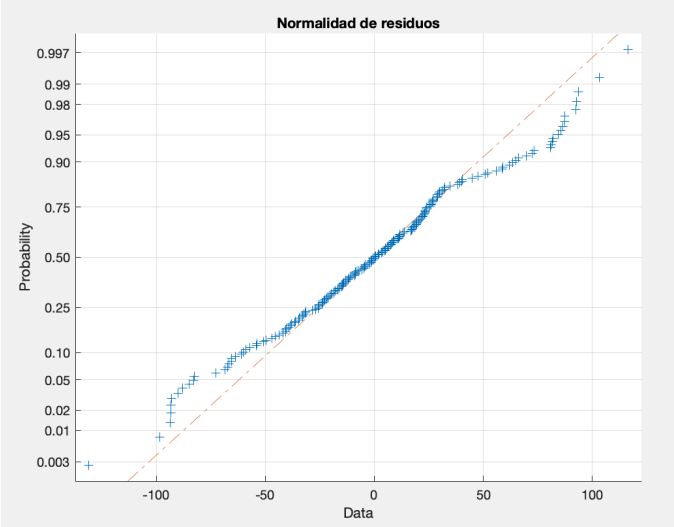

Fig. 6. Gráfico de normalidad de residuos para la latencia.

El análisis de varianza obtenido se resume en la siguiente figura, donde se reportan los valores F y los correspondientes p-valores (Prob > F) para cada factor y sus interacciones dobles. Los resultados indican que el **factor "Hora del día"** tiene un impacto estadísticamente significativo en la latencia observada (p = 0.000), lo cual es coherente con la posible congestión de red o en las infraestructuras del cloud en

determinados horarios. El análisis ANOVA revela que el tipo de **configuración de cifrado (sin cifrado, TLS, VPN) no tiene un efecto estadísticamente significativo sobre la latencia media (p = 0.390).**

Analysis of Variance

Source	Sum Sq.	d.f.	Mean Sq.	F	Prob>F
Hora	118148.4	3	39382.8	17.52	0
Dia	8440.3	1	8440.3	3.75	0.0543
Configuracion	4250.1	2	2125	0.95	0.3906
Hora:Dia	21964.3	3	7321.4	3.26	0.023
Hora:Configuracion	42419.6	6	7069.9	3.14	0.0059
Dia:Configuracion	3280.7	2	1640.3	0.73	0.4836
Error	391198.7	174	2248.3		
Total	589702	191			

Fig. 7. Tabla ANOVA para la latencia (transformación *tiedrank*).

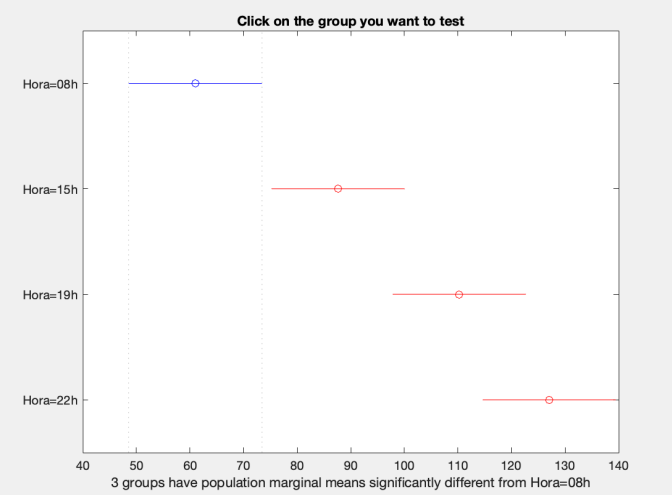

Fig. 8. Multicompare factor hora (latencia).

El gráfico representa el resultado de un análisis post hoc aplicado al factor "Hora" tras la detección de significancia estadística en el modelo ANOVA correspondiente a la **latencia**. Como se indica en el documento, el factor "Hora del día" obtuvo un **p-valor < 0.001** en la tabla ANOVA (ver Figura 7), lo que justificaba aplicar comparaciones múltiples entre sus niveles para determinar en qué franjas horarias se producían diferencias estadísticamente relevantes.

Este gráfico, generado mediante un test de comparaciones múltiples, presenta las **medias marginales de latencia** para cada franja horaria evaluada (08h, 15h, 19h y 22h), junto con sus respectivos **intervalos de confianza al 95%**. El grupo "Hora = 08h" aparece en **color azul**, lo que indica que está siendo utilizado como grupo de referencia en la comparación con el resto.

La visualización confirma que la latencia media a las **08h** es **notablemente más baja** que en el resto de franjas horarias y que los intervalos de confianza para las horas **15h, 19h y 22h** no se solapan con el de las **08h**, lo que confirma que las diferencias son estadísticamente significativas.

B. ESTUDIO DEL JITTER

Además de la latencia, el **jitter** constituye una métrica esencial para evaluar la calidad de una conexión de red, especialmente en aplicaciones en tiempo real como VoIP o streaming.

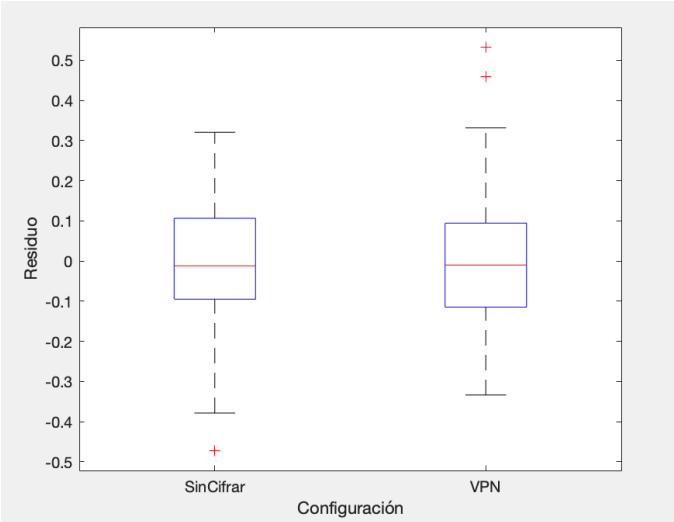

Fig. 9. Residuos frente a configuración (jitter).

En la **Figura 9**, se muestra la comparación del *jitter* residual entre las configuraciones "Sin Cifrar" y "VPN". Aunque se observan ligeras diferencias en la dispersión de los datos, el análisis de comparaciones múltiples indica que no existen diferencias estadísticamente significativas entre ambas configuraciones (p > 0.05).

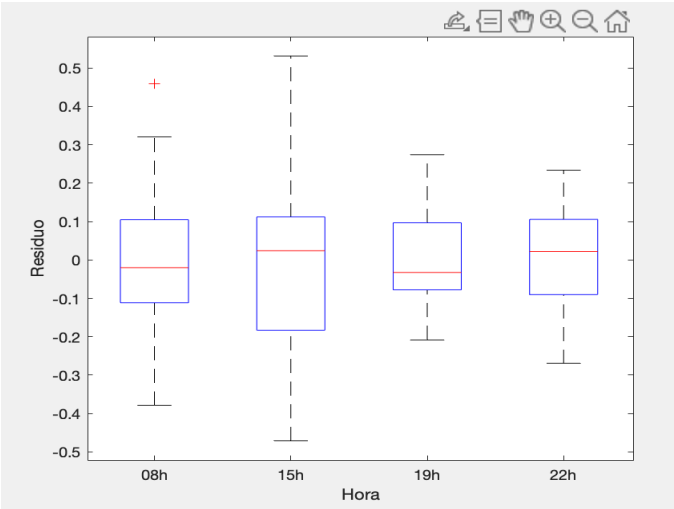

Fig. 10. Residuos frente a la hora (jitter).

La **Figura 10** presenta la distribución del *jitter* en distintos horarios del día (08h, 15h, 19h y 22h). Si bien hay cierta variabilidad en las medianas y los rangos intercuartílicos, las diferencias no son sustanciales. Esto sugiere que la variación del *jitter* a lo largo del día no es estadísticamente significativa dentro del contexto de las pruebas realizadas.

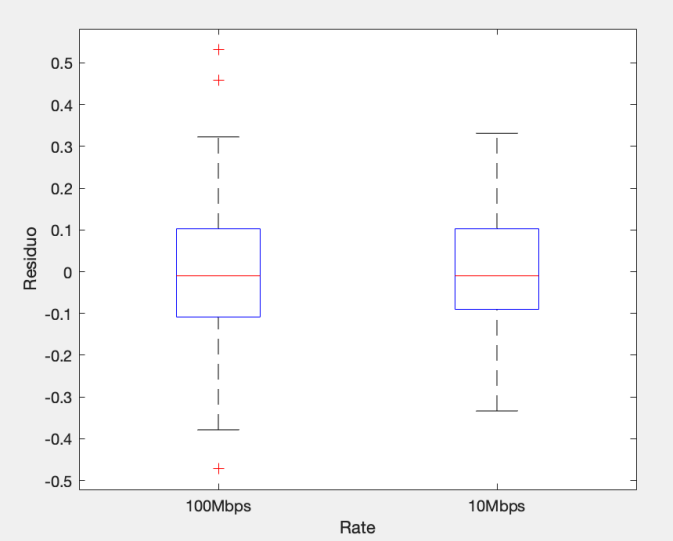

Fig. 11. Residuos frente a la tasa de transmisión (jitter).

En la **Figura 11** se comparan dos tasas de transferencia: 100 Mbps y 10 Mbps. A pesar de que visualmente puede notarse una leve diferencia en la mediana del *jitter*, el análisis no supuso diferencias estadísticamente relevantes. Esto indicaría que, para las condiciones experimentales evaluadas, la tasa de transferencia no afecta de manera significativa la variabilidad temporal del retardo.

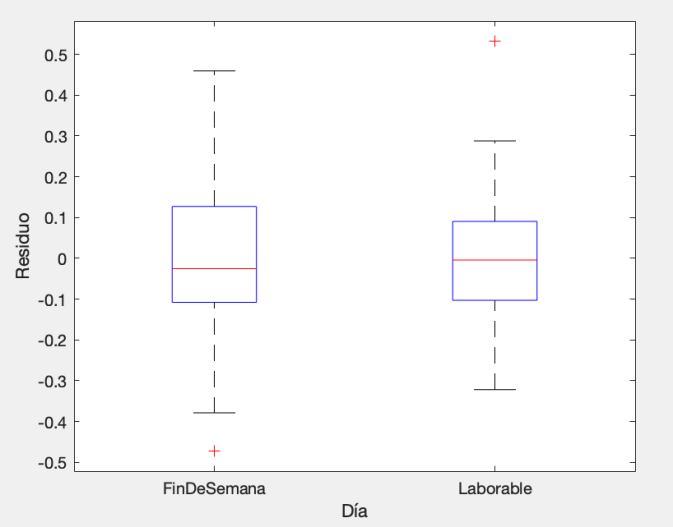

Fig. 12. Residuos frente a días (jitter).

En la **Figura 12** se comparan los resultados obtenidos en días laborables frente a fines de semana. La dispersión de los datos y la mediana son bastante similares en ambas categorías, lo que respalda la hipótesis de que no existe una diferencia significativa en el *jitter* entre días laborables y no laborables.

Skewness	Kurtosis
0.19533	3.4659

Para este análisis se ha empleado una transformación Box-Cox con el fin de estabilizar la varianza y aproximar la normalidad en los residuos. Los valores obtenidos de **Skewness** (0.19533) y **Kurtosis** (3.4659) tras dicha transformación indican que la distribución de los residuos es suficientemente cercana a una normal. En concreto, la asimetría leve y la curtosis moderadamente leptocúrtica no comprometen los supuestos del modelo ANOVA.

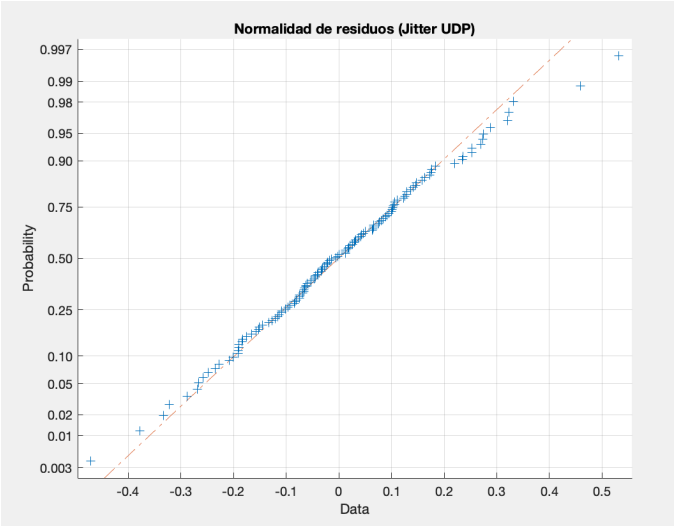

Fig. 13. Gráfico de normalidad de residuos para el jitter.

Con estos supuestos validados, se ha aplicado un análisis de varianza multifactorial para identificar la influencia estadística de cada factor experimental sobre la variabilidad del jitter.

Analysis of Variance

Source	Sum Sq.	d.f.	Mean Sq.	F	Prob>F
Hora	0.15	3	0.05	1.52	0.2136
Dia	0.1046	1	0.1046	3.18	0.0774
Configuracion	0.1163	1	0.1163	3.53	0.0628
Rate	19.3435	1	19.3435	587.94	0
Hora:Dia	0.2109	3	0.0703	2.14	0.0998
Hora:Configuracion	0.0271	3	0.009	0.27	0.8434
Hora:Rate	0.0818	3	0.0273	0.83	0.4809
Dia:Configuracion	0.0471	1	0.0471	1.43	0.2342
Dia:Rate	0.1215	1	0.1215	3.69	0.0572
Configuracion:Rate	0.0207	1	0.0207	0.63	0.4294
Error	3.5862	109	0.0329		
Total	23.8096	127			

Fig. 14. Tabla ANOVA para el jitter (transformación *boxcox*).

Los resultados indican que el **factor "Rate"** (tasa de transmisión) tiene un efecto altamente significativo sobre el jitter ($p < 0.001$), lo que concuerda con la intuición técnica: tasas de tráfico más elevadas tienden a introducir más variabilidad temporal entre paquetes.

Finalmente, se observan interacciones cercanas a la significancia entre **Día** × **Rate** ($p = 0.0572$), lo cual indica que

el jitter podría verse afectado en contextos específicos de tipo de jornada (laboral o festiva), aunque no de manera sistemáticamente significativa.

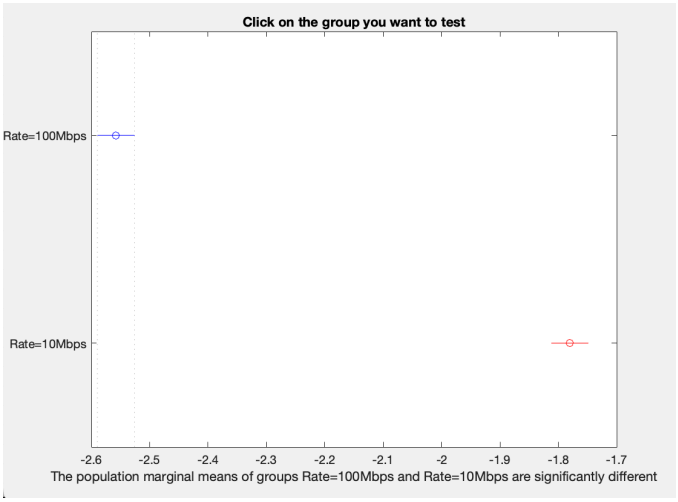

Fig. 15. Multicompare factor tasa de transmisión. (jitter)

La figura muestra el análisis de comparaciones múltiples para el factor "Rate" aplicado a la métrica de jitter, tras aplicar la transformación Box-Cox y validar los supuestos del modelo ANOVA. Dado que este factor presentó una significancia estadística elevada ($p < 0.001$), se procede a examinar con mayor detalle las diferencias entre niveles.

Los resultados indican que existe una diferencia significativa entre las tasas de transmisión de 10 Mbps y 100 Mbps, siendo el jitter claramente inferior en la condición de mayor tasa. Este comportamiento puede explicarse por la mayor eficiencia en la entrega de paquetes cuando el canal dispone de mayor capacidad, reduciendo así la variabilidad temporal entre ellos.

Este hallazgo resulta especialmente relevante para aplicaciones sensibles a la fluctuación temporal del retardo, como servicios de voz o vídeo en tiempo real, donde una menor tasa de transmisión podría degradar la calidad percibida debido al aumento del jitter.

C. ESTUDIO DEL CONSUMO DE RECURSOS DE CPU

El análisis del uso de CPU constituye un aspecto crucial para evaluar el impacto de los mecanismos de cifrado sobre los recursos del sistema. Para este propósito, se realizaron pruebas en condiciones controladas, variando los factores de **hora del día**, **tipo de jornada (laboral o fin de semana)** y **configuración de red** (sin cifrado, con TLS y VPN).

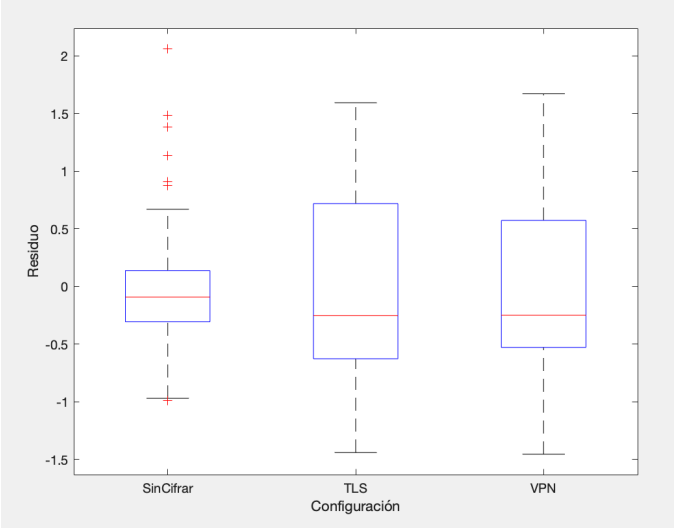

Fig. 16. Residuos frente a configuración (cpu).

La **Figura 16** evidencia diferencias notables en la dispersión de los residuos según el tipo de configuración de cifrado. La configuración **"Sin Cifrar"** presenta una menor variabilidad, con residuos mayormente concentrados cerca de cero. En contraste, tanto **TLS** como **VPN** muestran una mayor dispersión, especialmente VPN, que presenta valores extremos más alejados.

Este comportamiento sugiere que las configuraciones cifradas introducen una mayor inestabilidad en el uso de CPU, posiblemente debido al **overhead computacional asociado al proceso de cifrado y descifrado de paquetes**. No obstante, aunque hay mayor variabilidad, la mediana de los residuos se mantiene próxima a cero en todas las configuraciones, lo que indica que no existe un sesgo sistemático.

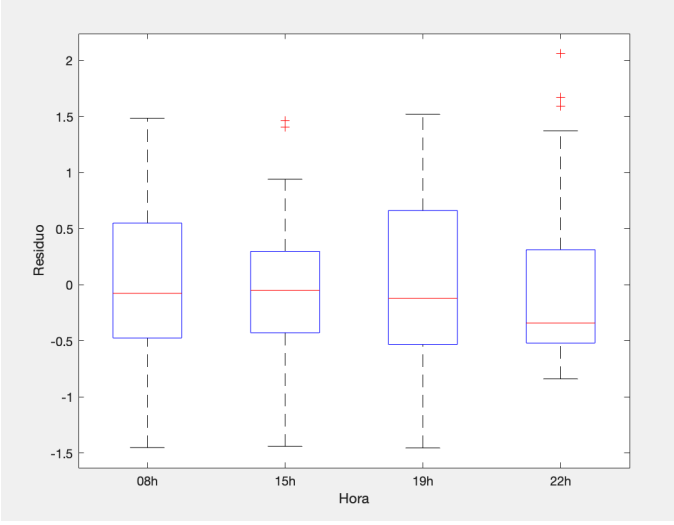

Fig. 17. Residuos frente a la hora (cpu).

La **Figura 17** muestra que la **hora del día** tiene un impacto limitado sobre el patrón de residuos. Si bien se observan ligeras diferencias en la dispersión —siendo las 22h la franja con menor variabilidad—, las medianas son relativamente estables. Esto sugiere que, aunque pueda existir cierta variación en el uso de CPU asociada a la hora, no se identifican patrones de carga claramente dependientes del horario.

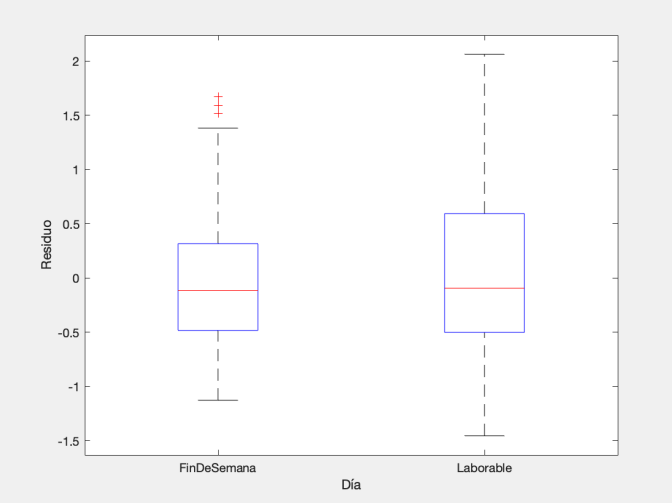

Fig. 18. Residuos frente al día (cpu).

En la **Figura 18** se comparan los residuos en días **laborables** y de **fin de semana**. La distribución de residuos muestra una ligera mayor variabilidad en los días laborables, posiblemente asociada a una mayor carga de trabajo o uso de red durante esos periodos. Sin embargo, las diferencias no son drásticas, y las medianas se mantienen próximas entre ambas categorías, indicando que el tipo de jornada no altera de manera significativa el comportamiento medio del uso de CPU.

Skewness	Kurtosis
0.46863	2.7338

Para este análisis ha sido necesario emplear la transformación logarítmica. Los valores obtenidos de **Skewness** y **Kurtosis** tras dicha transformación indican que la distribución de los residuos es suficientemente cercana a una normal.

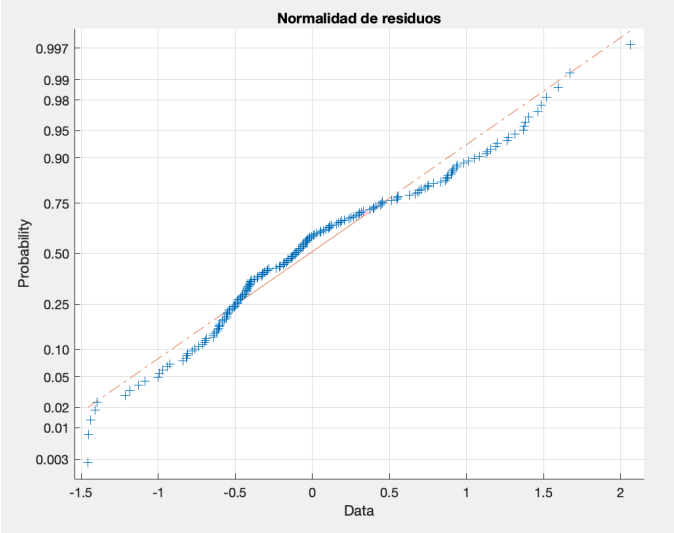

Fig. 19. Gráfico de normalidad de residuos para el consumo de cpu.

Para evaluar la validez de los modelos empleados en el análisis del rendimiento del servidor, es fundamental examinar los supuestos estadísticos sobre los residuos. En este caso, se realizó una prueba de normalidad a los residuos del modelo correspondiente a la métrica **CPU.** En la anterior figura se presenta el gráfico de probabilidad normal (Q-Q plot), el cual compara la distribución de los residuos observados con la distribución teórica normal.

Analysis of Variance

Source	Sum Sq.	d.f.	Mean Sq.	F	Prob>F
Hora	1.242	3	0.4141	0.74	0.527
Dia	11.416	1	11.4164	20.52	0
Configuracion	11.026	2	5.5131	9.91	0.0001
Hora:Dia	5.848	3	1.9494	3.5	0.0166
Hora:Configuracion	3.729	6	0.6215	1.12	0.3541
Dia:Configuracion	0.198	2	0.0992	0.18	0.8367
Error	96.784	174	0.5562		
Total	130.245	191			

Fig. 20. Tabla ANOVA para el consumo de cpu (transformación *log*).

Se observa que las variables *Día* y *Configuración* tienen un efecto estadísticamente significativo sobre el uso de CPU, con valores de *p* menores a 0.05 ($p = 0.0000$ y $p = 0.0001$ respectivamente). Además, la interacción *Hora:Día* también muestra significancia estadística ($p = 0.0166$), lo cual sugiere que el efecto de la hora varía dependiendo del día en que se realiza la medición. Por otro lado, ni la variable *Hora* por sí sola ni sus interacciones con *Configuración* mostraron significancia estadística ($p > 0.05$).

Estos resultados indican que el rendimiento del servidor, medido en términos de uso de CPU, depende de forma importante tanto del día como de la configuración utilizada, así como de su interacción temporal con la hora.

Esta información es esencial para el dimensionamiento de recursos y la planificación de despliegues seguros en entornos cloud, donde es necesario balancear **rendimiento** y **seguridad** sin comprometer la eficiencia operativa del sistema.

En general, el patrón de distribución observado respalda la hipótesis de normalidad de los residuos, permitiendo mantener la validez del análisis inferencial realizado.

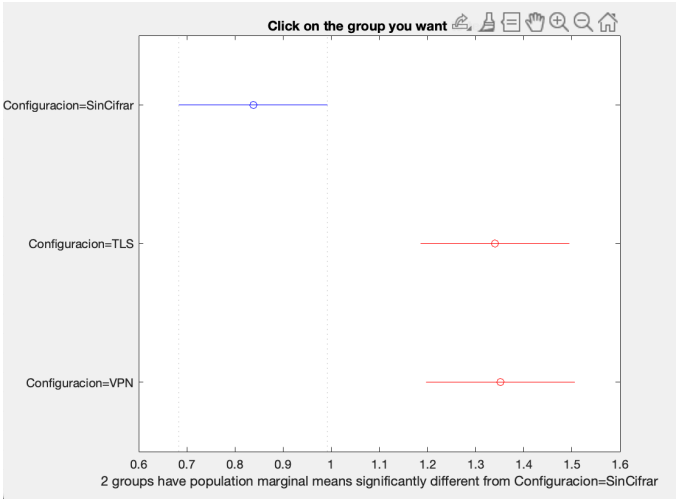

Fig. 21. Multicompare de la configuración (cpu).

La **Figura 21** representa el resultado del análisis de comparaciones múltiples (test post hoc) sobre las **medias marginales de residuos** entre las configuraciones de red. Se observa que existen **diferencias estadísticamente significativas** entre la configuración sin cifrado y las configuraciones con TLS y VPN. Esto confirma que los mecanismos de cifrado **sí impactan significativamente el uso de CPU**, aunque sus efectos pueden ser distintos según el protocolo empleado.

Este hallazgo es relevante, ya que indica que, desde el punto de vista del consumo de recursos del sistema, la seguridad añadida por TLS o VPN no es gratuita: introduce un coste computacional mensurable.

El análisis gráfico y estadístico del comportamiento de los residuos asociados al uso de CPU respalda la hipótesis de que los mecanismos de cifrado impactan en el rendimiento del sistema. Las configuraciones con TLS y VPN muestran **una mayor variabilidad y diferencias significativas** en comparación con una configuración sin cifrado.

En particular, **WireGuard (VPN)** introduce la mayor inestabilidad en los residuos, lo que puede estar relacionado con el proceso de encapsulación de tráfico y el coste de mantenimiento del túnel cifrado. Estos resultados deben considerarse en escenarios donde se requiera garantizar rendimiento predecible y bajo consumo de recursos, especialmente en entornos virtualizados con recursos limitados.

D. ESTUDIO DEL THROUGHPUT

Uno de los objetivos principales de este estudio ha sido evaluar cómo las configuraciones de seguridad —TLS (Stunnel) y WireGuard (VPN)— impactan en el rendimiento efectivo de la red en términos de **throughput**, es decir, la cantidad de datos transmitidos con éxito a través del canal de comunicación. Este análisis permite determinar si los mecanismos de cifrado introducen cuellos de botella o reducciones significativas en el caudal útil, especialmente bajo distintas condiciones de tráfico y temporalidad. Para ello, se llevaron a cabo pruebas sistemáticas en distintos horarios y días, utilizando tasas de transmisión controladas y replicando los experimentos en tres configuraciones de red: sin cifrado, con TLS y con VPN.

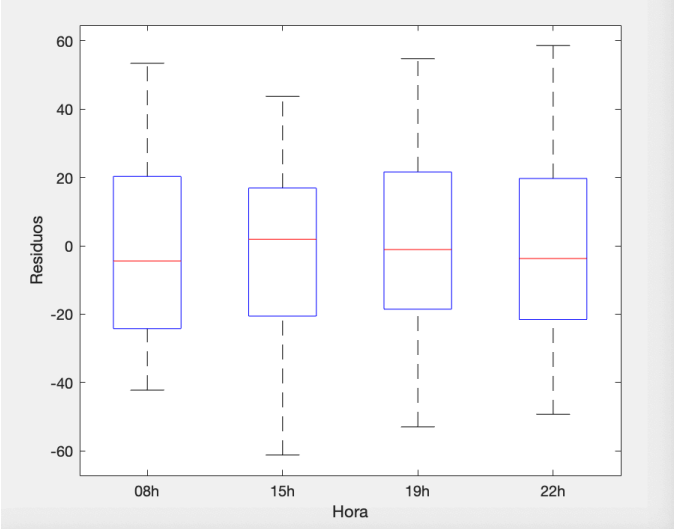

Fig. 22. Residuos frente a la hora (throughput).

La dispersión de residuos es relativamente uniforme entre las distintas horas (08h, 15h, 19h, 22h), con medianas centradas en torno a cero. No se observan cambios sustanciales en la variabilidad entre franjas horarias. Esto sugiere que **la hora del día no afecta de manera significativa la estabilidad del throughput**, aunque en el ANOVA obtuvo un valor F moderado (1.54).

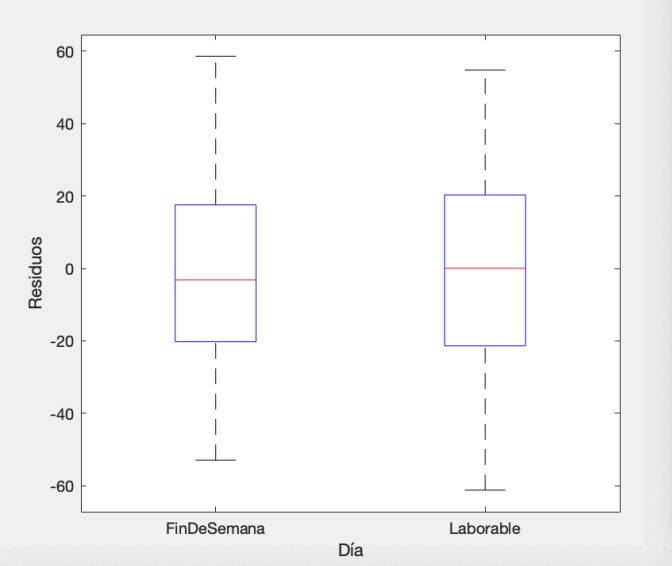

Fig. 23. Residuos frente al día (throughput).

Tanto fines de semana como días laborables muestran distribuciones similares de residuos, con rangos intercuartílicos comparables. Esto respalda los resultados estadísticos que indican que el **tipo de día no tiene un efecto relevante sobre el rendimiento** (p = 0.5956).

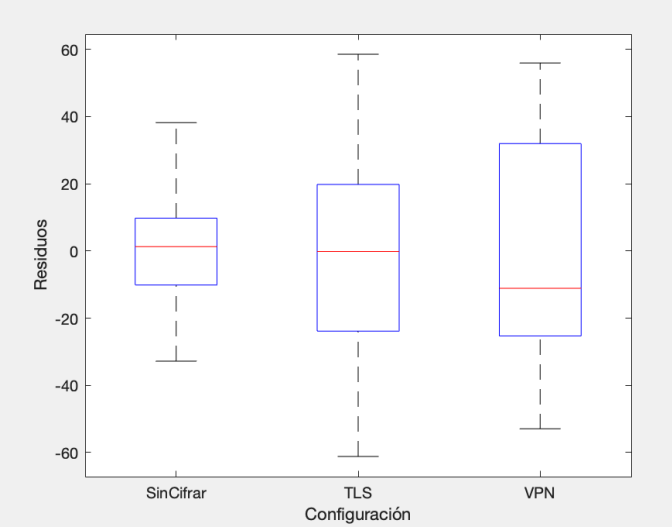

Fig. 24. Residuos frente a configuración (throughput).

Se observa un patrón interesante: la **VPN presenta una mayor dispersión en los residuos** comparada con TLS y sin cifrar, lo que sugiere una **mayor inestabilidad en el throughput cuando se emplea cifrado VPN**. Aunque la media no difiere significativamente (p = 0.308), esta variabilidad extra puede ser relevante en aplicaciones sensibles al rendimiento. La configuración sin cifrado es la más estable.

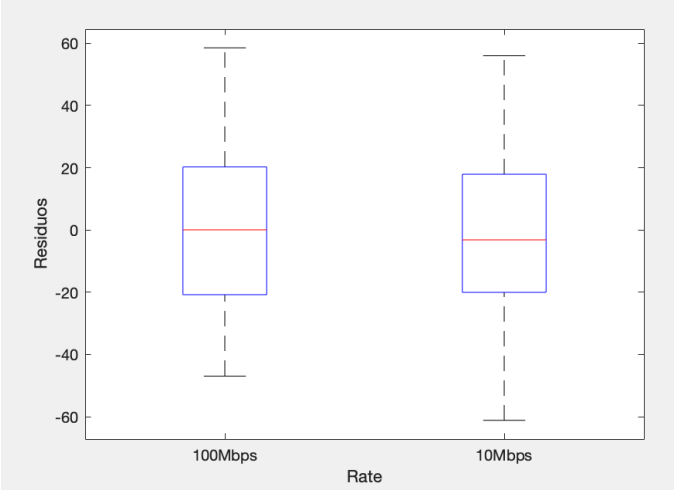

Fig. 25. Residuos frente a la tasa de transmisión (throughput).

Ambos niveles de Rate (10 Mbps y 100 Mbps) muestran una distribución similar, aunque a simple vista puede parecer que **100 Mbps tiene residuos más concentrados**. Sin embargo, el análisis ANOVA mostró que **Rate es el único factor con efecto altamente significativo (p < 0.0001)**, indicando que afecta directamente al throughput. Esto es coherente, ya que a mayor tasa nominal se espera mayor rendimiento observado.

Skewness	Kurtosis
0.18	2.32

En primer lugar, se evaluó la normalidad de los residuos mediante un gráfico de probabilidad normal (Q-Q plot). Tal como se muestra en la figura, los residuos se alinean razonablemente bien con la línea de referencia, lo cual indica que los errores del modelo presentan una distribución aproximadamente normal. No obstante, se observan ligeras desviaciones en las colas, especialmente en los extremos, lo cual podría deberse a la presencia de valores atípicos o efectos no captados por el modelo.

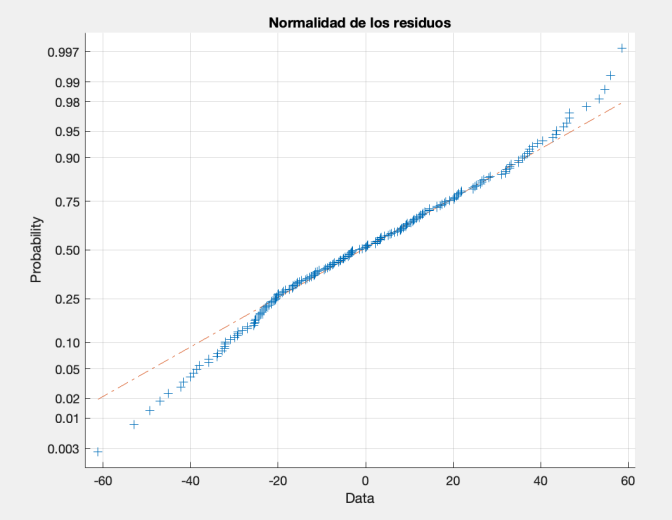

Fig. 26. Gráfico de normalidad de residuos para el throughput.

La tabla ANOVA obtenida se presenta a continuación:

Analysis of Variance

Source	Sum Sq.	d.f.	Mean Sq.	F	Prob>F
Hora	3429.4	3	1143.1	1.54	0.207
Dia	210.4	1	210.4	0.28	0.5956
Configuracion	1765	2	882.5	1.19	0.308
Rate	442368	1	442368	594.52	0
Hora:Dia	3342.6	3	1114.2	1.5	0.2172
Hora:Configuracion	7967.2	6	1327.9	1.78	0.1051
Hora:Rate	2281.1	3	760.4	1.02	0.3845
Dia:Configuracion	1929.4	2	964.7	1.3	0.2762
Dia:Rate	471.9	1	471.9	0.63	0.427
Configuracion:Rate	231.3	2	115.7	0.16	0.8562
Error	124261.3	167	744.1		
Total	588257.5	191			

Fig. 27. Tabla ANOVA para el throughput (transformación *tiedrank*).

Los resultados muestran que el único factor con un efecto estadísticamente significativo sobre el throughput es **Rate** (tasa de transferencia), con un valor de $p < 0.0001$ y un estadístico F elevado (594.52), lo que indica una fuerte influencia sobre la variable de respuesta. El resto de los factores principales (**Hora**, **Día**, **Configuración**) y sus interacciones no presentan significancia estadística ($p > 0.05$), sugiriendo que no afectan de manera individual ni conjunta el rendimiento de forma significativa.

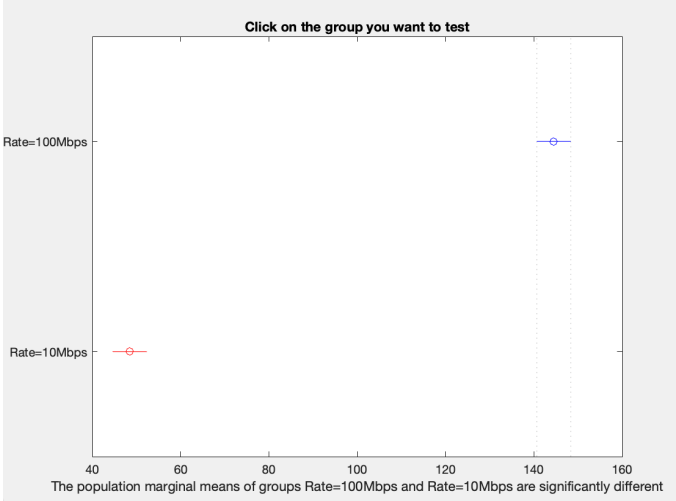

Fig. 28. Multicompare para la tasa (throughput).

La **Figura 28** evidencia diferencias notables entre los niveles del factor **Rate**. Específicamente, los grupos con tasas de transmisión de **100Mbps** y **10Mbps** presentan medias marginales **significativamente diferentes** ($p < 0.001$), siendo el *throughput* considerablemente mayor en el primer caso. Este resultado confirma que la tasa nominal de transmisión tiene un efecto directo y estadísticamente significativo sobre el rendimiento medido.

E. ESTUDIO DE LA CARGA DE RED

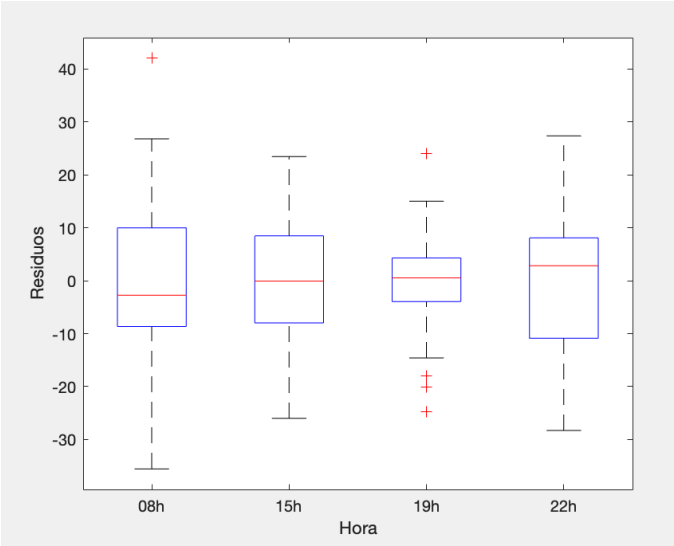

Fig. 29. Residuos frente a la hora (carga de red).

En la **Figura 29**, que muestra la variación de los residuos según la **hora del día** (08h, 15h, 19h, 22h), se aprecia una ligera disminución de la dispersión a las 19h, aunque las diferencias entre franjas horarias no son marcadas. Este resultado concuerda con el análisis ANOVA, donde el factor "Hora" no resultó estadísticamente significativo ($p = 0.1419$),

confirmando que el comportamiento de la carga no varía sustancialmente a lo largo del día.

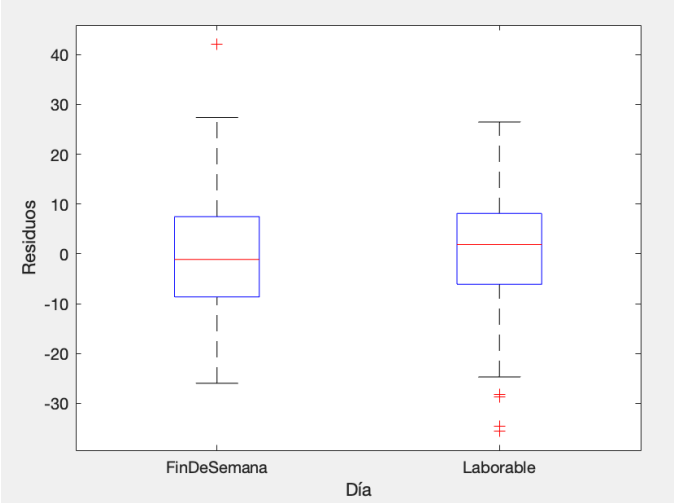

Fig. 30. Residuos frente al día (carga de red).

La **Figura 30** presenta la comparación entre **días laborables y fines de semana**, observándose una dispersión ligeramente mayor en los días laborables. Este resultado es coherente con el valor p = 0 obtenido en el análisis estadístico, lo que confirma que el tipo de día tiene un impacto relevante sobre el tráfico agregado, posiblemente debido a mayores niveles de actividad y uso de red en días laborables.

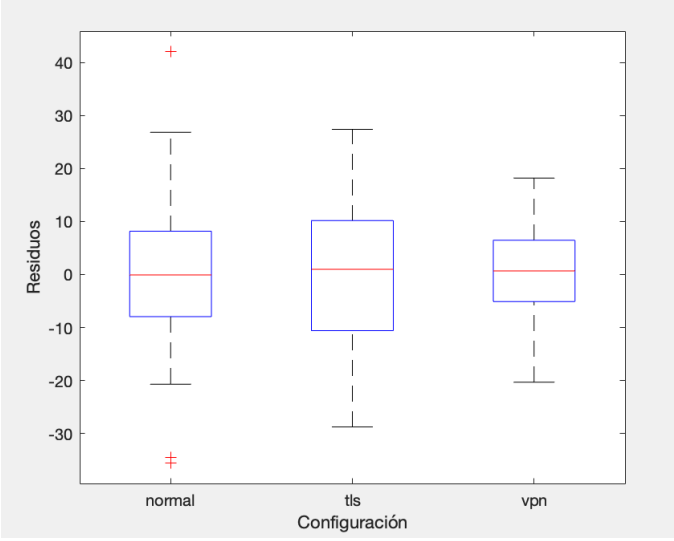

Fig. 31. Residuos frente a la configuración (carga de red).

La **Figura 31** analiza el efecto de la **configuración de cifrado**. Se observa que la configuración con vpn genera residuos con mayor dispersión en comparación a sin cifrado y tls, lo que sugiere que el uso de VPN introduce mayor variabilidad en la carga de red. Esta observación respalda los resultados del modelo ANOVA, donde la configuración tuvo un efecto altamente significativo ($p < 0.0001$). Además, se identificaron interacciones significativas entre Configuración y Día, así como con Hora, lo cual indica que el impacto del cifrado depende del contexto temporal.

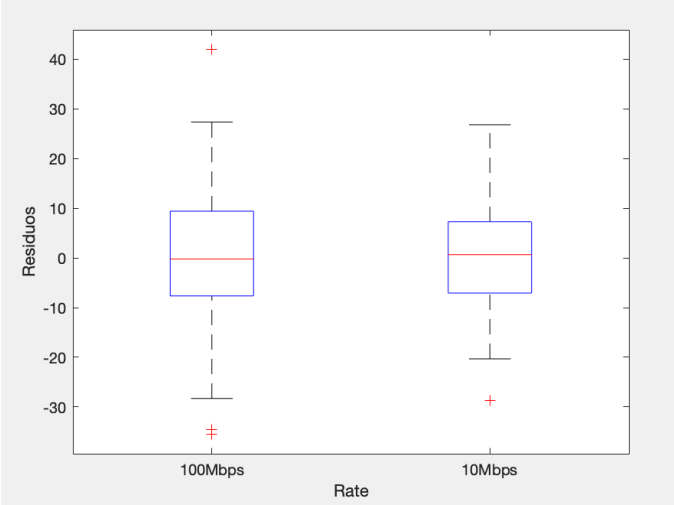

Fig. 32. Residuos frente a la tasa de transmisión (carga de red).

En la **Figura 32**, se comparan los residuos según la **tasa de transferencia (Rate)**: 10 Mbps y 100 Mbps. Se observa que la configuración de 100 Mbps presenta una mayor dispersión, con valores atípicos más extremos. Este resultado es coherente con el hallazgo de que la tasa de transmisión es el factor más determinante en la carga de red ($F = 2605.42$, $p < 0.0001$), ya que un mayor ancho de banda permite mayor volumen de tráfico, lo cual incrementa la variabilidad de los residuos.

Uno de los objetivos principales de este estudio ha sido analizar cómo los distintos factores experimentales —especialmente los mecanismos de cifrado TLS (Stunnel) y VPN (WireGuard)— influyen sobre la **carga de red**, medida como el volumen de tráfico generado y capturado mediante flujos netflow. Esta métrica resulta esencial para comprender el impacto agregado que tiene la seguridad sobre la infraestructura de red, más allá del rendimiento puntual de una conexión individual. El análisis se ha centrado en cuantificar los efectos de la hora del día, el tipo de jornada, la configuración de comunicación y la tasa de transmisión, así como sus interacciones, sobre la carga total observada durante las sesiones de prueba.

Skewness	Kurtosis
-0.04	3.56

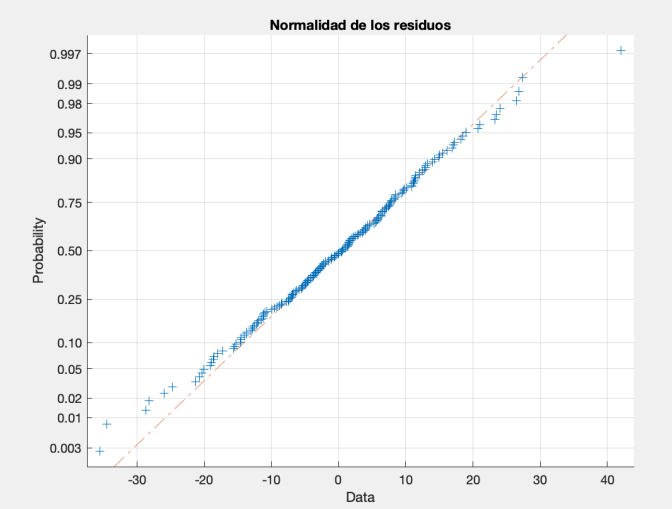

Fig. 33. Gráfico de normalidad de residuos para la carga de red.

Previamente, se evaluó la distribución de los residuos mediante un gráfico de probabilidad normal (Q-Q plot), mostrado en la **Figura 33**. La mayoría de los puntos se alinean adecuadamente sobre la diagonal teórica, lo que indica que los residuos del modelo presentan una distribución aproximadamente normal. No obstante, se observan ligeras desviaciones en los extremos, posiblemente asociadas a valores atípicos, que no comprometen seriamente los supuestos del modelo.

Analysis of Variance

Source	Sum Sq.	d.f.	Mean Sq.	F	Prob>F
Hora	937.2	3	312.4	1.84	0.1419
Dia	13838	1	13838	81.5	0
Configuracion	98304.9	2	49152.5	289.49	0
Rate	442368	1	442368	2605.42	0
Hora:Dia	226.1	3	75.4	0.44	0.722
Hora:Configuracion	2443.3	6	407.2	2.4	0.03
Hora:Rate	645.4	3	215.1	1.27	0.2874
Dia:Configuracion	1453.3	2	726.7	4.28	0.0154
Dia:Rate	1150.5	1	1150.5	6.78	0.0101
Configuracion:Rate	79.7	2	39.8	0.23	0.7911
Error	28354.6	167	169.8		
Total	589801	191			

Fig. 34. Tabla ANOVA para la carga de red (transformación *tiedrank*).

La **Figura 34** presenta el resumen del ANOVA aplicado. Los resultados muestran que el factor **Rate** (tasa de transferencia) tiene un efecto altamente significativo sobre la carga de red (**$F = 2605.42$, $p < 0.0001$**), lo cual es consistente con el hecho de que una mayor tasa nominal genera proporcionalmente mayor volumen de tráfico.

Asimismo, el factor **Configuración** (modo de cifrado) también presenta un impacto estadísticamente significativo (**$F = 289.49$, $p < 0.0001$**), indicando que el mecanismo de seguridad empleado afecta sustancialmente el comportamiento del tráfico. En particular, se observa que las configuraciones con VPN generan una mayor carga de red, probablemente debido a la encapsulación adicional de los paquetes.

El factor **Día** (laborable o. fin de semana) muestra igualmente una influencia relevante (**$F = 81.5$, $p < 0.0001$**), lo que sugiere que las condiciones generales de tráfico varían entre jornadas, posiblemente por diferencias en la actividad de red global.

Además, se detectaron efectos significativos en las interacciones **Hora:Configuración** (**$p = 0.03$**), **Día:Configuración** (**$p = 0.0154$**) y **Día:Rate** (**$p = 0.0101$**). Estas interacciones indican que el impacto del cifrado y la tasa de tráfico no es uniforme, sino que depende del contexto horario y del tipo de jornada. Por el contrario, no se hallaron efectos estadísticamente significativos en el factor **Hora** (**$p = 0.1419$**) ni en la mayoría de sus interacciones, lo que indica que la franja horaria, de forma aislada, no altera significativamente la carga de red.

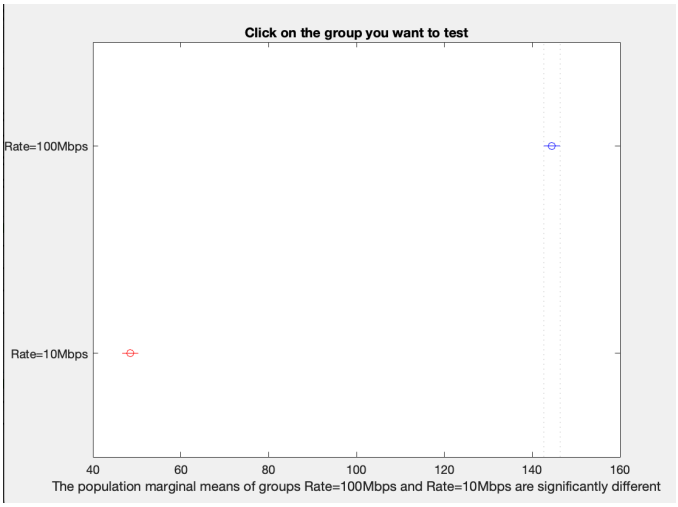

Fig. 35. Multicompare de tasa de transmisión (carga de red).

En esta figura se representa la comparación de medias marginales de carga de red para los dos niveles del factor "Rate" (10 Mbps y 100 Mbps). Los resultados muestran una diferencia estadísticamente significativa entre ambos grupos, siendo la carga considerablemente mayor cuando se emplea una tasa de transmisión de 100 Mbps.

Este hallazgo refuerza los resultados obtenidos en el análisis ANOVA ($p < 0.0001$), donde el factor "Rate" emergió como el principal determinante del volumen de tráfico observado. Dado que una tasa de transmisión más alta permite enviar una mayor cantidad de datos por unidad de tiempo, es natural que la carga total generada durante las pruebas aumente de forma proporcional. No obstante, la diferencia encontrada no sólo es estadísticamente significativa, sino también relevante desde el punto de vista práctico, con implicaciones claras para el dimensionamiento de redes.

Así, este resultado confirma que el efecto de la tasa de transmisión sobre la carga de red no es trivial y debe ser tenido en cuenta en escenarios donde el volumen total de tráfico impacte en la eficiencia, el coste o la capacidad del sistema. En contextos cloud con limitaciones de ancho de banda o tarificación por volumen, emplear tasas más elevadas puede

traducirse en una sobrecarga significativa que comprometa la sostenibilidad operativa del servicio.

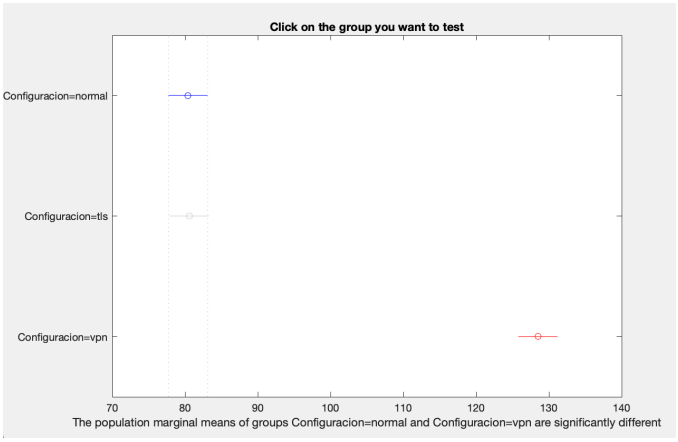

Fig. 36. Multicompare de configuración (carga de red).

Como puede observarse, la configuración con VPN presenta un valor medio significativamente más alto en comparación con las configuraciones sin cifrado o con TLS, diferencia que además es estadísticamente significativa (según se indica en la leyenda inferior del gráfico). Esta diferencia resalta el impacto que tiene la encapsulación adicional de paquetes en WireGuard sobre el volumen total de tráfico transmitido.

La configuración con TLS se sitúa en una posición intermedia, con una media ligeramente superior a la configuración sin cifrado, pero sin diferencias estadísticamente significativas frente a esta ni frente a VPN en este gráfico concreto. Este resultado es coherente con el análisis ANOVA previo, donde el factor *Configuración* resultó altamente significativo ($p < 0.0001$), sugiriendo que el mecanismo de cifrado utilizado influye sustancialmente en la carga de red.

Este hallazgo confirma que las técnicas de cifrado no sólo afectan a nivel de rendimiento puntual, sino que también generan una sobrecarga persistente en términos de tráfico total, especialmente en el caso de VPN, lo que debe tenerse en cuenta en entornos cloud con limitaciones de ancho de banda o con costes asociados al volumen de datos transmitidos.

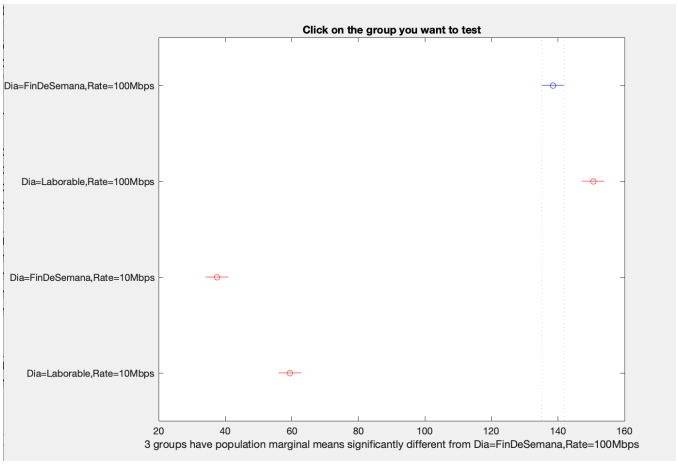

Fig. 37. Multicompare de tasa y día (carga de red).

En esta figura se representa el análisis post hoc sobre las medias marginales de carga de red para los distintos niveles combinados de los factores "Día" (laborable vs. fin de semana) y "Rate" (10 Mbps, 100 Mbps). Dado que el análisis ANOVA identificó un efecto estadísticamente significativo para esta interacción ($p = 0.0101$), se procedió a una exploración detallada mediante comparaciones múltiples.

Los resultados muestran diferencias significativas entre la mayoría de los grupos en comparación con la condición de referencia (Día=FinDeSemana, Rate=100 Mbps), especialmente cuando se utilizan tasas de transmisión más bajas (10 Mbps), donde la carga de red es considerablemente menor. Este patrón sugiere que la tasa de transmisión es el principal determinante del volumen de tráfico observado, pero su impacto se ve modulado por el tipo de jornada.

En concreto, se aprecia que la condición de mayor carga corresponde a días de fin de semana con tasa alta (100 Mbps), lo cual puede deberse a una menor congestión general de red en ese periodo, permitiendo un aprovechamiento más eficiente del canal disponible. Por el contrario, las combinaciones con 10 Mbps —tanto en días laborables como en fines de semana— presentan una carga de red significativamente inferior.

Estos resultados confirman que la interacción entre la tasa de transmisión y el tipo de jornada no es trivial, y que debe considerarse en el diseño de políticas de tráfico o dimensionamiento de redes en contextos con sensibilidad al volumen de datos transmitidos, especialmente en entornos con restricciones de coste o capacidad.

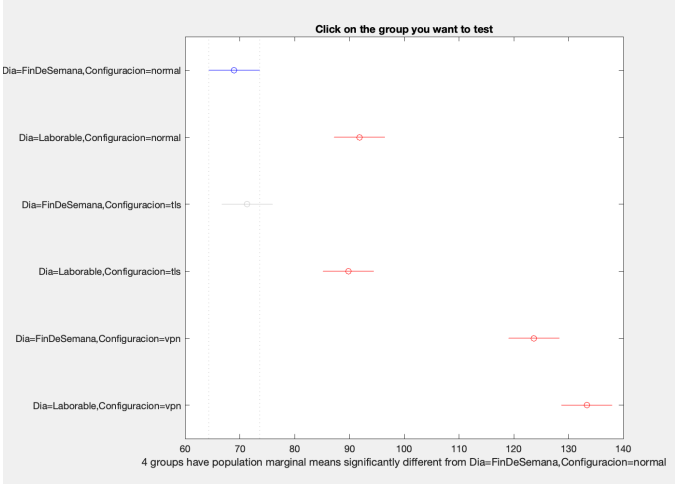

Fig. 38. Multicompare de configuración y día (carga de red).

En esta figura se representa el análisis sobre las medias marginales de carga de red para los distintos niveles combinados de los factores "Día" (laborable vs. fin de semana) y "Configuración" (normal, TLS, VPN).

Los resultados muestran diferencias significativas respecto a la condición de referencia (Día=FinDeSemana, Configuración=normal), especialmente en los escenarios que combinan días laborables con configuraciones cifradas, donde la carga de red es notablemente superior. Este comportamiento puede explicarse por la doble influencia del overhead generado por el cifrado —particularmente en el caso de VPN, que añade encapsulación adicional— y por el incremento en la actividad de red típica de los días laborables.

En cambio, las combinaciones que incluyen días festivos con configuración sin cifrar presentan las menores cargas observadas, lo que sugiere que en ausencia de cifrado y en contextos de menor demanda, el tráfico agregado se mantiene en niveles significativamente más bajos. La configuración TLS muestra un comportamiento intermedio, con aumentos de carga más contenidos en comparación con VPN, pero aún superiores a la conexión normal, especialmente bajo condiciones de mayor tráfico.

Estos resultados, en línea con los observados para la interacción "Día × Rate", refuerzan la idea de que los efectos de la seguridad sobre el tráfico no son uniformes, sino que se ven modulados por el contexto temporal. Así, la interacción entre el tipo de jornada y el mecanismo de cifrado se revela como un factor crítico en la evolución del tráfico agregado, con implicaciones directas para la planificación de redes seguras y eficientes en entornos cloud, particularmente cuando existen restricciones asociadas al volumen total de datos transmitidos

VIII. CONCLUSIONES

Este estudio ha evaluado el impacto de distintas configuraciones de cifrado (sin cifrado, TLS mediante Stunnel y VPN mediante WireGuard) sobre el rendimiento de servidores en la nube, considerando métricas clave como latencia, jitter, throughput, carga de red y uso de CPU. A partir de los resultados obtenidos, se pueden extraer las siguientes conclusiones:

- **Latencia (delay):**
  El análisis estadístico no encontró diferencias significativas entre las configuraciones en cuanto a la media de latencia. Sin embargo, gráficamente se evidenció que **WireGuard presenta mayor variabilidad**, lo que puede ser crítico en aplicaciones sensibles al retardo. TLS y la conexión sin cifrado mostraron un comportamiento más estable y predecible.

- **Jitter:**
  No se detectaron diferencias estadísticamente significativas entre las configuraciones. No obstante, se observó una **ligera tendencia a un jitter más elevado con WireGuard**, en comparación con TLS o conexiones sin cifrado. En contextos de comunicaciones en tiempo real (VoIP, streaming), esta variabilidad podría impactar la calidad del servicio.

- **Throughput:**
  El único factor que influyó de manera significativa en el throughput fue la **tasa de transferencia (Rate)**. Ni el tipo de configuración ni las variables temporales alteraron significativamente el caudal útil de datos. Esto sugiere que, **en términos de volumen de datos transmitidos con éxito, el uso de TLS o VPN WireGuard no introduce una degradación notable** bajo las condiciones evaluadas.

- **Uso de CPU:**
  Se evidenció que **las configuraciones cifradas aumentan significativamente el consumo de CPU**, siendo WireGuard la que introduce mayor carga. Esto refleja el coste computacional asociado al cifrado y mantenimiento de túneles, siendo un aspecto relevante al dimensionar recursos en entornos virtualizados.

- **Carga de red:**
  La carga total de tráfico fue significativamente más alta en las configuraciones con cifrado, especialmente con WireGuard. Esto se debe a la encapsulación adicional de los paquetes. TLS también generó más tráfico que la configuración sin cifrado, aunque en menor medida. Este impacto debe considerarse en entornos donde **el tráfico agregado influye en el coste o rendimiento global del sistema**.

References

[1] Camacho, J, Apuntes del Tema 2 de la asignatura Planificación y Explotación de Redes y Servicios, MUIT.

Enrique Alcalá - Zamora Castro (Estudiante MUIT) Graduado en Ingeniería de Tecnologías de Telecomunicación con especialidad en Telemática por la Universidad de Granada (2020-2024).