



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“Metodología integral para evaluar el rendimiento de firewalls”

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

Rogelio Joseph Pacotaype Huaman

ASESOR:

Mg. Reneé Rivera Crisóstomo

LÍNEA DE INVESTIGACIÓN:

Auditoría de sistemas y seguridad de la información

LIMA – PERÚ

2018

Página del jurado

 UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE LA TESIS	Código : F07-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1
--	---------------------------------------	---

El Jurado encargado de evaluar la tesis presentada por don (a) **PACOTAYPE HUAMAN ROGELIO JOSEPH** cuyo título es:

Metodología integral para evaluar el rendimiento de firewalls

Reunido en la fecha, escuchó la sustentación y la resolución de preguntas por el estudiante, otorgándole el calificativo de: 13 (número) TRECE (letras).

Lima, San Juan de Lurigancho 16 de diciembre del 2018


.....
Mg. René Rivera Crisóstomo
PRESIDENTE


.....
Dr. Manuel Hilario Falcón
SECRETARIO


.....
María Acuña Meléndez
VOCAL

 SECCION DE INVESTIGACION UCV UNIVERSIDAD CÉSAR VALLEJO PERU	 Dirección de Investigación	Revisó	 Responsable del SGC	 VICERECTORADO DE INVESTIGACION UCV UNIVERSIDAD CÉSAR VALLEJO TRUJILLO	 Vicerrectorado de Investigación
--	--	--------	--	---	---

Dedicatoria

Esta tesis va dedicada a las personas que me apoyaron y motivaron a lo largo de mi vida, mis padres, esposa y en especial a mi hija Flavia Camila que es mi razón de ser y principal motivación.

Agradecimientos

Al Dr. Emigdio Antonio Alfaro Paredes por su motivación, paciencia y apoyo constante en el desarrollo del presente trabajo de investigación a través de sus asesorías.

Declaratoria de autenticidad

Yo Rogelio Joseph Pacotaype Huaman con DNI N° 46232493, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad César Vallejo, Facultad de Ingeniería, Escuela Profesional de Ingeniería de Sistemas, declaro bajo juramento que toda la documentación que acompaño es veraz y auténtica.

Asimismo, declaro también bajo juramento que todos los datos e información que se presenta en la presente tesis son auténticos y veraces. En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada por lo cual me someto a lo dispuesto en las normas académicas de la Universidad César Vallejo.

Lima, 16 de diciembre de 2018



Rogelio Joseph Pacotaype Huaman

DNI: 46232493

Presentación

Señores miembros del Jurado:

En cumplimiento del Reglamento de Grados y Títulos de la Universidad César Vallejo presento ante ustedes la tesis titulada “Metodología integral para evaluar el rendimiento de firewalls”, con el objetivo de “Determinar que los firewalls de *hardware* tienen mayor rendimiento que los firewalls de *software*”. En el primer capítulo, se detalla la introducción del proyecto en el cual se expone la realidad problemática, los trabajos previos y teorías relacionadas que son el sustento de esta tesis, además de manifestarse las justificaciones, los objetivos e hipótesis generales y específicas que persigue la investigación. En el capítulo dos, se detalla la metodología aplicada describiendo el tipo de investigación y diseño aplicado, además se determina la población y muestra sobre la cual se realizaron las pruebas y se plantearon los métodos de análisis de datos y desarrollaron las técnicas e instrumentos de recolección de datos. En el capítulo tres, se muestran los resultados obtenidos por cada indicador planteado al realizar las pruebas respectivas definidas en la metodología integral propuesta para evaluar el rendimiento de firewalls, con sus respectivos gráficos y tablas para hacer la explicación más entendible para el lector. En el capítulo cuatro, se hicieron las comparaciones de los resultados del trabajo con los resultados obtenidos en otras investigaciones con la intención de respaldar estos trabajos o discrepar de ellos en el caso de no coincidir con la solución planteada. En el capítulo cinco, fueron expuestas las conclusiones finales del proyecto de investigación por cada indicador basados en los resultados obtenidos en el capítulo anterior. Finalmente, en el capítulo seis están las recomendaciones dadas a futuras investigaciones tomando como base la experiencia del proyecto y las observaciones que surgieron en su desarrollo.



Rogelio Joseph Pacotaype Huaman

Resumen

La presente investigación se desarrolló con el objetivo de elaborar una metodología para la evaluación de rendimiento de *firewalls* y aplicarla para determinar que los *firewalls* de *hardware* tienen mayor rendimiento que los *firewalls* de *software*. Para lograr este objetivo, se desarrolló un estudio cuantitativo, pre-experimental, en el que la población estuvo conformada por cuatro (04) *firewalls*, dos (02) *firewalls* de *hardware* (Paloalto y Fortinet) y dos *firewalls* de *software* (Endian y Sophos) que fueron comparados. Para evaluar el rendimiento, los criterios de evaluación fueron desempeño en la red (*throughput* y latencia), eficacia de la seguridad (filtro URL y filtro *antimalware*) y consumo de recursos (CPU y memoria RAM), se hizo uso de aplicaciones especiales para tal finalidad.

Para analizar los datos obtenidos de las pruebas de evaluación del desempeño de los *firewalls*, se realizó la prueba de normalidad de Kolmogorov-Smirnov para muestras iguales o superiores a cincuenta datos y Shapiro-Wilk para muestras menores a cincuenta, se aplicó la prueba T como método de análisis estadístico para muestras con distribución normal y la prueba de Mann-Whitney para muestras con datos que no siguen una distribución normal. Finalmente, con la interpretación de dicho análisis, se pudo determinar que los *firewalls* de *hardware* (Paloalto y Fortinet) tienen mejor rendimiento que los *firewalls* de *software* (Endian y Sophos), bajo las condiciones indicadas en esta investigación.

Palabras clave: metodología, *firewall*, rendimiento, *hardware*, *software*.

Abstract

The present investigation was developed with the objective of developing a methodology for evaluating the performance of firewalls and applying it to determine that hardware firewalls have a higher performance than software firewalls. To achieve this objective, a quantitative, pre-experimental study was developed, in which the population consisted of four (04) firewalls, two (02) hardware firewalls (Paloalto and Fortinet) and two software firewalls (Endian and Sophos) that were compared. To evaluate the performance, the evaluation criteria were performance in the network (throughput and latency), security effectiveness (URL filter and antimalware filter) and consumption of resources (CPU and RAM), special applications were used for such purpose

To analyze the data obtained from the tests, the Kolmogorov-Smirnov normality test was performed for samples equal to or greater than fifty data and Shapiro-Wilk for samples less than fifty, the Student's T test was applied as a statistical analysis method for samples with normal distribution and the Mann-Whitney test for samples with data that do not follow a normal distribution. Finally, with the interpretation of this analysis, it was determined that hardware Firewalls (Paloalto and Fortinet) have better performance than software Firewalls (Endian and Sophos), under the conditions indicated in this research.

Keywords: *methodology, firewall, performance, hardware, software.*

Índice general

Página del jurado.....	II
Dedicatoria.....	III
Agradecimientos.....	IV
Declaratoria de autenticidad.....	V
Presentación.....	VI
Resumen.....	VII
Abstract.....	VIII
I. INTRODUCCIÓN.....	15
1.1 Realidad problemática.....	16
1.2 Trabajos previos	18
1.2.1 Antecedentes nacionales	18
1.2.2 Antecedentes internacionales	19
1.3 Teorías relacionadas al tema	25
1.3.1 Definición de términos	25
1.3.2 Definición de roles	27
1.3.3 Definición de políticas	29
1.3.4 Rendimiento de <i>Firewall</i>	31
1.3.5 Desempeño en la red.....	34
1.3.6 Eficacia de la seguridad.....	42
1.3.7 Consumo de recursos	51
1.3.8 Herramientas de medición.....	58
1.4 Formulación del problema	61
1.5 Justificación del estudio	61
1.5.1 Justificación operativa.....	61
1.5.2 Justificación tecnológica	62
1.5.3 Justificación económica	63
1.6 Hipótesis.....	64
1.7 Objetivos	66
II. MÉTODO	67
2.1 Diseño de la investigación.....	68
2.2 Variables, operacionalización.....	68
2.2.1 Definición conceptual	68
2.2.2 Definición operacional	69

2.2.3	Operacionalización de las variables	69
2.2.4	Indicadores	71
2.3	Población y muestra	72
2.4	Técnicas e instrumentos de recolección de datos, validez y confiabilidad	73
2.4.1	Técnicas e instrumentos de recolección de datos	73
2.4.2	Validez	73
2.4.3	Confiabilidad	73
2.5	Métodos de análisis de datos	74
2.6	Aspectos éticos	74
III.	RESULTADOS	75
3.1	Prueba de normalidad	76
3.1.1	Prueba de normalidad para la dimensión desempeño en la red	76
3.1.2	Prueba de normalidad para la dimensión consumo de recursos	79
3.2	Descriptivos	80
3.2.1	Dimensión desempeño en la red	80
3.2.2	Dimensión eficacia de la seguridad	89
3.2.3	Dimensión consumo de recursos.	90
3.3	Prueba de Hipótesis	92
3.3.1	Dimensión desempeño en la red.	92
3.3.2	Dimensión eficacia de la seguridad	96
3.3.3	Dimensión consumo de recursos.	97
IV.	DISCUSIÓN	100
V.	CONCLUSIONES	104
VI.	RECOMENDACIONES	107
VII.	REFERENCIAS	109

Índice de tablas

Tabla 1: Matriz operacional de las variables	70
Tabla 2: Indicadores.....	71
Tabla 3: Resultados de prueba de normalidad para indicador <i>throughput</i> con paq. 64KB	76
Tabla 4: Resultados de prueba de normalidad para indicador <i>throughput</i> con paq. 128KB	77
Tabla 5: Resultados de prueba de normalidad para indicador <i>throughput</i> con paq. 256KB	77
Tabla 6: Resultados de prueba de normalidad para indicador <i>throughput</i> con paq. 512KB	77
Tabla 7: Resultados de prueba de normalidad para indicador <i>throughput</i> con paq. 1024KB	78
Tabla 8: Resultados de prueba de normalidad para indicador <i>throughput</i> con paq. 1280KB	78
Tabla 9: Resultados de prueba de normalidad para indicador <i>throughput</i> con paq. 1518KB	78
Tabla 10: Resultados de prueba de normalidad del indicador latencia	79
Tabla 11: Resultados de prueba de normalidad del indicador CPU.....	79
Tabla 12: Resultados de prueba de normalidad del indicador memoria RAM.....	80
Tabla 13: Datos descriptivos del indicador <i>throughput</i> con paq. de 64KB.....	81
Tabla 14: Datos descriptivos del indicador <i>throughput</i> con paq. de 128KB.....	82
Tabla 15: Datos descriptivos del indicador <i>throughput</i> con paq. de 256KB.....	83
Tabla 16: Datos descriptivos del indicador <i>throughput</i> con paq. de 512KB.....	84
Tabla 17: Datos descriptivos del indicador <i>throughput</i> con paq. de 1024KB.....	85
Tabla 18: Datos descriptivos del indicador <i>throughput</i> con paq. de 1280KB.....	86
Tabla 19: Datos descriptivos del indicador <i>throughput</i> con paq. de 1518KB.....	87
Tabla 20: Datos descriptivos del indicador latencia	88
Tabla 21: Datos descriptivos del indicador filtro <i>antimalware</i> en tabulación cruzada	89
Tabla 22: Datos descriptivos del indicador filtro URL en tabulación cruzada.....	89
Tabla 23: Datos descriptivos del indicador memoria RAM	90
Tabla 24: Datos descriptivos del indicador CPU.....	91
Tabla 25: Prueba U de Mann-Whitney para el indicador <i>throughput</i> tamaño de paq. 64KB.....	92
Tabla 26: Prueba U de Mann-Whitney para el indicador <i>throughput</i> tamaño de paq. 128KB....	93
Tabla 27: Prueba U de Mann-Whitney para el indicador <i>throughput</i> tamaño de paq. 256KB....	93
Tabla 28: Prueba U de Mann-Whitney para el indicador <i>throughput</i> tamaño de paq. 512KB....	93
Tabla 29: Prueba U de Mann-Whitney para el indicador <i>throughput</i> tamaño de paq. 1024KB..	94
Tabla 30: Prueba U de Mann-Whitney para el indicador <i>throughput</i> tamaño de paq. 1280KB..	94
Tabla 31: Prueba U de Mann-Whitney para el indicador <i>throughput</i> tamaño de paq. 1518KB..	94
Tabla 32: Prueba T para muestras independientes para el indicador latencia	95

Tabla 33: Prueba Chi cuadrado para el indicador filtro URL.....	96
Tabla 34: Prueba Chi cuadrado para el indicador filtro <i>antimalware</i>	97
Tabla 35: Prueba T para muestras independientes para el indicador CPU.....	98
Tabla 36: Prueba T para muestras independientes para el indicador memoria RAM	99
Tabla 37: Cuadro comparativo de metodologías de evaluación de <i>Firewalls</i>	124
Tabla 38: Criterios de rendimientos y parámetros de medición	128
Tabla 39: Políticas a implementar en el <i>Firewall</i>	132
Tabla 40: Características de los <i>Firewalls</i>	133
Tabla 41: Tamaños de paquetes a enviar según RFC N° 2544	139
Tabla 42: Ejemplo de tabla de tabulación de datos de Filtrado URL	148
Tabla 43: Ejemplo de tabla de tabulación de datos de filtro <i>antimalware</i>	150
Tabla 44: Tabulación de datos de dimensión desempeño en la red	155
Tabla 45: Tabulación de datos de dimensión eficacia de la seguridad	157
Tabla 46: Tabulación de datos de dimensión consumo de recursos	158

Índice de figuras

Figura 1. Fases de la metodología de evaluación de rendimiento de <i>Firewall</i>	126
Figura 2. Estructura de las fases de la metodología MERF.....	127
Figura 3. Escenario con <i>Firewall</i> de intermediario.....	134
Figura 4. Herramienta Ejecutar.....	136
Figura 5. Prueba de conectividad al servidor web.	137
Figura 6. Icono de la herramienta Jperf.....	137
Figura 7. Panel de configuración de la herramienta Jperf modo server.	138
Figura 8. Panel de configuración de la herramienta Jperf modo cliente.	138
Figura 9. Panel application layer options de la herramienta Jperf.	138
Figura 10. Panel transport layer options de la herramienta Jperf.....	139
Figura 11. Resultado de prueba de <i>throughput</i> con la herramienta Jperf.....	140
Figura 12. Prueba de conectividad al servidor.....	141
Figura 13. Icono Lan Speed Test.	142
Figura 14. Plataforma Lan Speed Test.	142
Figura 15. Lan Speed Test resultados.	143
Figura 16. Visión general del filtrado URL.....	145
Figura 17. Prueba de conectividad a internet.....	146
Figura 18. Barra de direcciones del navegador web.	146
Figura 19. Página web bloqueada por filtro URL.....	147
Figura 20. Página web de categoría adultos.	147
Figura 21. Prueba de conectividad a internet.....	149
Figura 22. Barra de direcciones del navegador web.	149
Figura 23. Página web bloqueada por archivo malicioso.	149
Figura 24. Página web maliciosa.	150
Figura 25. Icono del terminal (agente de ataque).....	152
Figura 26. Ventana del terminal del agente de ataque.	153
Figura 27. Ataque de denegación de servicios con herramienta hping.	153
Figura 28. Panel de monitoreo del <i>Firewall</i> Sophos.....	154

Índice de anexos

Anexo 1: Matriz de consistencia.....	121
Anexo 2: MERF: Metodología para evaluar el rendimiento de <i>Firewall</i> - Estructura .	122
Anexo 3: Hoja de tabulacion de datos del indicador <i>throughput</i>	160
Anexo 4: Hoja de tabulacion de datos del indicador latencia	158
Anexo 5: Hoja de tabulacion de datos del indicador filtro URL.....	170
Anexo 6: Hoja de tabulacion de datos del indicador filtro <i>antimalware</i>	181
Anexo 7: Hoja de tabulacion de datos del indicador consumo CPU	192
Anexo 8: Hoja de tabulacion de datos del indicador consumo RAM.....	193
Anexo 9: Acta de aprobación de originalidad de tesis.....	194
Anexo 10: Resultados de Turnitin	195
Anexo 11: Acta de autorización de publicación de tesis.....	196
Anexo 12: Autorización de la version final del trabajo de investigación	197

Anexo 9: Acta de aprobación de originalidad de tesis

	ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS	Código : F06-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1
---	--	---

Yo, **RENEÉ RIVERA CRISÓSTOMO**, docente de la Facultad de Ingeniería y carrera Profesional de Ingeniería Sistemas de la Universidad César Vallejo campus Lima Este, revisor (a) de la tesis titulada:

"METODOLOGÍA INTEGRAL PARA EVALUAR EL RENDIMIENTO DE FIREWALL", del estudiante **ROGELIO JOSEPH PACOTAYE HUAMAN**, constato que la investigación tiene un índice de similitud de **20 %** verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito(a) analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

San Juan de Lurigancho, 16 de diciembre del 2018



RENEÉ RIVERA CRISÓSTOMO
 DNI: 08554321

 PERU Dirección de Investigación	Revisó	 Responsable del SGC	 VICERECTORADO de Investigación
--	--------	--	--