ANÁLISIS DE RENDIMIENTO Y CALIDAD DE SERVICIO (QoS) EN TRES ARQUITECTURAS DE SEGURIDAD BASADAS EN FIREWALL

NURY JULIETH ALVAREZ ROA
Código 1400296

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES
BOGOTA, 2010

ANÁLISIS DE RENDIMIENTO Y CALIDAD DE SERVICIO (QoS) EN TRES ARQUITECTURAS DE SEGURIDAD BASADAS EN FIREWALL

NURY JULIETH ALVAREZ ROA
Código 1400296

Trabajo final como Auxiliar de Investigación presentado como requisito para optar por el título de Ingeniero en Telecomunicaciones

DIRECTOR:
EDWARD PAUL GUILLEN PINTO, M. Sc.

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES
BOGOTA, 2010

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

_____

Ciudad y Fecha

AGRADECIMIENTOS

A Dios por las bendiciones con que me cubre cada día, y por esta oportunidad de formarme como ingeniera.

A todos los docentes que con sus aportes de conocimientos y experiencias fueron partícipes de mi formación.

A Luis José Mendoza Bermúdez, quien fue un apoyo importante para alcanzar esta meta en mi vida.

A mi madre por darme la vida y estar siempre a mi lado

A mis hermanas por su apoyo incondicional

CONTENIDO

1. INTRODUCCIÓN 14

1.1. PLANTEAMIENTO DEL PROBLEMA 15
1.2. OBJETIVOS 16
1.2.1. OBJETIVO GENERAL 16
1.2.2. OBJETIVOS ESPECÍFICOS 16
1.3. ANTECEDENTES 17
1.3.1 LOCALES 17
1.3.2 INTERNACIONALES 17

2. MARCO TEÓRICO 19

2.1. MARCO TEÓRICO CONCEPTUAL 19
2.1.1 Análisis de Ingeniería. 19
2.1.2 Vulnerabilidad. 19
2.1.3 Desempeño. 19
2.1.4 Seguridad. 20
2.1.5 Software de Código Abierto. 20
2.2. MARCO TEÓRICO REFERENCIAL 21
2.2.1 Desempeño de la red. 21
2.2.2 Throughput 24
2.2.3 Teoría de Colas 25
2.2.4 TCP/IP 25
2.2.5 Puertos TCP 25
2.2.6 Aplicaciones de red 25
2.2.7 Firewall 27

3. INGENIERÍA DEL PROYECTO 29

3.1. ESTADO DEL ARTE 29
3.2. REQUERIMIENTOS DE DISEÑO 30
3.3. ANÁLISIS DE VARIABLES DE INGENIERÍA 30

3.3.1. Variables de Selección de Arquitecturas 31
- Escalabilidad 31
- Transparencia para la red 31
- Facilidad de Implementación 31
- Facilidad de Administración 31
- Punto crítico de vulnerabilidad 32
- Existencia de DMZ 32

3.3.2. Variables de Evaluación de Arquitecturas 32
- Throughput 32
- Latencia 33
- Jitter 33
- Paquetes perdidos. 33

3.4. DESARROLLO DEL PROYECTO 33
3.4.1 Metodología 34
3.4.2 Documentación y Selección 34
3.4.3 Selección de las arquitecturas a implementar 41
3.4.4 Documentación y elección del firewall que permita la implementación de las arquitecturas seleccionadas. 47
3.4.5. Diseño e implementación 55
4. PRUEBAS Y ANÁLISIS DE RESULTADOS 64
4.1. PRUEBAS REALIZADAS 64
4.1.1. Pruebas de Rendimiento de la red: 65
4.1.2. Pruebas de QoS: Llamada de 1 minuto desde y hacia diferentes zonas del firewall 71
4.1.3. Pruebas de Rendimiento y QoS 85
CONCLUSIONES Y RECOMENDACIONES 107
BIBLIOGRAFÍA 110

LISTA DE FIGURAS

Figura 1: Zonas de Protección de un Firewall 30
Figura 2: Metodología de Ejecución del Proyecto 34
Figura 3: Dual homed-host 35
Figura 4: Screened Subnet 36
Figura 5: Dual Firewall 38
Figura 6: Dos Firewall Dos DMZ 40
Figura 7: Porcentaje de Evaluación Variables 45
Figura 8: Arquitecturas de Firewall a implementar 47
Figura 9: Metodología de Elección del Firewall 48
Figura 10: Vectores de Confiabilidad Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre" 54
Figura 11: Diseño de red "Escenario 0" 55
Figura 12: Diseño de red de Screened Subnet 57
Figura 13: Diseño de red Dual Firewall 59
Figura 14: Diseño de red "Dual Firewall, Dual DMZ" 61
Figura 15: Comparación Throughput DMZ a MZ (Prueba de Rendimiento) 66
Figura 16: Porcentaje de afectación del Throughput DMZ a MZ (Pruebas de Rendimiento) 67
Figura 17: Comparación Throughput DMZ a WAN (Prueba de Rendimiento) 68
Figura 18: Porcentaje de afectación del Throughput DMZ a WAN (Pruebas de Rendimiento) 69
Figura 19: Comparación Throughput WAN a MZ (Prueba de Rendimiento) 70
Figura 20: Porcentaje de afectación del Throughput WAN a MZ (Pruebas de Rendimiento) 71
Figura 21: Latencia MZ a DMZ (Prueba de QoS) 73
Figura 22: Porcentaje de incremento Latencia MZ a DMZ (Prueba QoS) 74
Figura 23: Latencia WAN a DMZ (Prueba de QoS) 75
Figura 24: Porcentaje de incremento Latencia WAN a DMZ (Prueba QoS) 76
Figura 25: Latencia MZ a WAN (Prueba de QoS) 77
Figura 26: Porcentaje de incremento Latencia MZ a WAN (Prueba QoS) 78
Figura 27:Jitter MZ a DMZ (Prueba de QoS) 79
Figura 28: Jitter WAN a DMZ (Prueba de QoS) 81
Figura 29: Porcentaje de incremento Jitter WAN a DMZ (Prueba QoS) 82
Figura 30: Jitter MZ a WAN (Prueba de QoS) 83
Figura 31: Porcentaje de incremento Jitter MZ a WAN (Prueba QoS) 84
Figura 32: Comparación Throughput DMZ a MZ (Pruebas de Rendimiento y QoS) 86
Figura 33: Porcentaje de afectación del Throughput DMZ a MZ (Pruebas de Rendimiento y QoS) 87

Figura 34: Comparación Throughput DMZ a WAN (Pruebas de Rendimiento y QoS) 88
Figura 35: Porcentaje de afectación del Throughput DMZ a WAN (Pruebas de Rendimiento y QoS) 89
Figura 36: Comparación Throughput WAN a MZ (Pruebas de Rendimiento y QoS) 90
Figura 37: Porcentaje de afectación del Throughput MZ a WAN (Pruebas de Rendimiento y QoS) 91
Figura 38: Latencia MZ a DMZ (Prueba de Rendimiento y QoS) 93
Figura 39: Porcentaje de incremento Latencia MZ a DMZ (Prueba de Rendimiento y QoS) 94
Figura 40: Latencia WAN a DMZ (Prueba de Rendimiento y QoS) 95
Figura 41: Porcentaje de incremento Latencia WAN a DMZ (Prueba de Rendimiento y QoS) 96
Figura 42: Latencia MZ a WAN (Prueba de Rendimiento y QoS) 97
Figura 43: Porcentaje de incremento Latencia MZ a WAN (Prueba de Rendimiento y QoS) 98
Figura 44: Jitter MZ a DMZ (Prueba de Rendimiento y QoS) 99
Figura 45: Porcentaje de incremento Jitter MZ a DMZ (Pruebas de Rendimiento y QoS) 100
Figura 46: Jitter WAN a DMZ (Prueba de Rendimiento y QoS) 101
Figura 47: Porcentaje de incremento Jitter WAN a DMZ (Pruebas de Rendimiento y QoS) 101
Figura 48: Jitter MZ a WAN (Prueba de Rendimiento y QoS) 102
Figura 49: Porcentaje de incremento Jitter MZ a WAN (Pruebas de Rendimiento y QoS) 102
Figura 50: Pérdida de paquetes DMZ --> WAN Pruebas Rendimiento y QoS 104
Figura 51: Porcentaje de Incremento en la Pérdida de Paquetes DMZ --> WAN respecto de Escenario 0 105
Figura 52: Pérdida de paquetes MZ --> WAN Pruebas Rendimiento y QoS 105
Figura 53: Porcentaje de Incremento en la Pérdida de Paquetes MZ --> WAN respecto de Escenario 0 106

LISTA DE TABLAS

Tabla 1: Existencia de DMZ en las Arquitecturas de Firewall..... 42
Tabla 2: Existencia de Punto Único de Fallo en las Arquitecturas de Firewall..... 43
Tabla 3: Transparencia para la red de las Arquitecturas de Firewall 43
Tabla 4: Facilidad de Implementación de las Arquitecturas de Firewall 44
Tabla 5: Facilidad de Administración de las Arquitecturas de Firewall 44
Tabla 6: Nivel de Seguridad de las Arquitecturas de Firewall 45
Tabla 7: Puntaje Final de las Arquitecturas de Firewall (Variables Cuantitativas) . 46
Tabla 8: Orden por suma de puntajes de variables cauntitativas de las Arquitecturas de Firewall..... 46
Tabla 9: Orden por suma de puntajes de variables cuantitativas y cualitativas de las Arquitecturas de Firewall 47
Tabla 10:Firewalls a estudiar en tesis: "Análisis de Vulnerabilides y Fortalezas en 5 firewalls de plataforma libre"..... 48
Tabla 11:Número de Vulnerabilidades encontradas en la tesis: "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"..... 49
Tabla 12: Vulnerabilidades con actualización de los firewall a estudiar en la tesis"Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre" 50
Tabla 13: Número de Fortalezas encontradas en la tesis: "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"..... 50
Tabla 14: Valores de cercanía vulnerabilidades, peor caso, Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"..... 51
Tabla 15: Valores de cercanía vulnerabilidades, mejor caso, Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"..... 52
Tabla 16: Valores de cercanía fortalezas, peor caso, Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"..... 52
Tabla 17: Valores de cercanía fortalezas, mejor caso, Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"..... 53
Tabla 18: Valores de puntos por posición y vectores Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"..... 53
Tabla 19: Especificaciones Técnicas Equipos de red, Escenario0..... 56
Tabla 20: Direccionamiento Escenario 0..... 56
Tabla 21: Especificaciones técnicas dispositivos de red Dual Firewall..... 58
Tabla 22: Direccionamiento "Screned Subnet" 58
Tabla 23: Especificaciones técnicas equipos "Dual Firewall" 60
Tabla 24: Direccionamiento "Dual Firewall"..... 60
Tabla 25: Especificaciones técnicas equipos "Dual Firewall, Dual DMZ" 62
Tabla 26: Direccionamiento "Dual Firewall, Dual DMZ"..... 62

Tabla 27: PORCENTAJE DE AUMENTO DE LATENCIA Y JITTER respecto del Escenario 0..... 80
Tabla 28: Porcentajes de Incremento del Jitter de MZ hacia DMZ y de WAN hacia DMZ Respecto de Escenario 0 (Pruebas de QoS):..... 83
Tabla 29: Porcentajes de Incremento del Jitter de MZ hacia DMZ y de WAN hacia DMZ (Pruebas de QoS)..... 85
Tabla 30: Porcentajes de decremento Throughput de DMZ a MZ (Solo FTP Y FTP+VOIP)..... 87
Tabla 31: Porcentajes de decremento Throughput de WAN a MZ (Solo FTP Y FTP+VOIP)..... 92
Tabla 32: Latencia MZ --> DMZ (Pruebas de Rendimiento Vs. Pruebas de Rendimiento y QoS)..... 93
Tabla 33: Latencia DMZ --> MZ (Pruebas de Rendimiento Vs. Pruebas de Rendimiento y QoS)..... 94
Tabla 34: Latencia WAN--> DMZ (Pruebas de Rendimiento Vs. Pruebas de Rendimiento y QoS)..... 95
Tabla 35: Tabla 33: Latencia DMZ --> WAN (Pruebas de Rendimiento Vs. Pruebas de Rendimiento y QoS)..... 96
Tabla 36: PORCENTAJE DE AUMENTO DE LATENCIA Y JITTER respecto del Escenario 0 (Pruebas de Rendimiento y QoS)..... 100
Tabla 37: Pérdida de paquetes DMZ -->MZ Pruebas Rendimiento y QoS..... 103
Tabla 38: Porcentaje de Incremento en la Pérdida de Paquetes DMZ --> MZ respecto de Escenario 0..... 104

LISTA DE ANEXOS

ANEXO A: INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA OPERATIVO FREEBSD

ANEXO B: INSTALACIÓN Y CONFIGURACIÓN DEL IPFW

ANEXO H: RESULTADOS PRUEBAS ESCENARIO 0

ANEXO I: RESULTADOS PRUEBAS ARQUITECTURA “SCREENED SUBNET”

ANEXO J: RESULTADOS PRUEBAS ARQUITECTURA “DUAL FIREWALL”

ANEXO K: RESULTADOS PRUEBAS ARQUITECTURA “DUAL FIREWALL – DUAL DMZ”

1. INTRODUCCIÓN

Debido a la importancia de implementar seguridad efectiva en las redes de las organizaciones haciendo uso de los firewalls, se hace necesario realizar la correcta elección, implementación y configuración de una arquitectura adecuada que satisfaga las necesidades de las organizaciones y que brinde un equilibrio en cuanto al rendimiento y la seguridad para que de esta manera no se vea afectado el desempeño de las redes. En el documento que se presenta a continuación , se realiza un análisis comparativo de tres arquitecturas de firewall existentes y como resultado final, se presenta un cuadro comparativo basado en una relación Rendimiento – QoS, que permita al administrador de red realizar una correcta elección de la arquitectura de firewall que mejor se ajuste a las necesidades de la red de su organización.

El análisis comparativo de las arquitecturas de firewalls del cual se habla, se enmarca dentro del área de los sistemas, las redes de datos y las telecomunicaciones, más específicamente en el área de la seguridad informática, que brinda el soporte necesario y adecuado a los administradores de red, para lograr la máxima protección de los datos en las redes de área local LAN de forma óptima.

En el documento del que se habla, se establece una comparación de tres arquitecturas de firewall, las cuales son: Screened Subnet, Dual Firewall y Dual Firewall – Dual DMZ, en cuanto al rendimiento y QoS inherentes a cada una de ellas, luego de realizar el diseño e implmentación de las mismas.

Como resultado final se presenta un cuadro comparativo de selección basado en una relación Rendimiento/Qos, el cual brinda al administrador de red, bajo las características y requerimientos propios de la red a proteger, parámetros para la toma de decisiones al momento de pensar en implementar seguridad basada en firewall.

El libro de grado que se expone en las siguientes páginas contiene el resultado del estudio funcional del manejo de la seguridad informática mediante la implementación y análisis de las tres arquitecturas de firewall. El proceso de investigación y los resultados obtenidos de la misma se plasman en el presente documento dividido en seis capítulos a conocer.

En el primero de ellos se explica brevemente el proyecto desarrollado, el contexto en el que se realizó, y se establece la importancia del mismo. A continuación, se establecen los lineamientos conceptuales y referenciales claves en el desarrollo del proyecto. En el tercer capítulo, se analiza el estado del arte, los requerimientos del diseño, el análisis de las variables de ingeniería y se establece la metodología usada en el desarrollo de la investigación. Como cuarto capítulo, se presentan las pruebas realizadas, los resultados obtenidos para cada una de las arquitecturas de redes seguras basadas en firewalls y el análisis de las mismas. Conclusiones y recomendaciones, capítulo en el que se establecen los comentarios finales arrojados por el proceso investigativo. Y finalmente, bibliografía, en el que se especifican fuentes claves de información para llevar a cabo posteriores referencias o ampliaciones del tema.

1.1. PLANTEAMIENTO DEL PROBLEMA

Actualmente los administradores de red, a la hora de planear la seguridad, lo hacen centrándose básicamente en el firewall a implementar: sus vulnerabilidades y fortalezas orientadas a la seguridad; no cuentan con herramientas de decisión con las que puedan elegir la mejor opción a la hora de implementar una arquitectura de seguridad basada en firewall, pasando por alto que esta puede afectar la calidad de servicio y el rendimiento en una red. El administrador se ve en la obligación de elegir arbitrariamente una de ellas sin tener certeza que con esta pueda proveer la mejor relación rendimiento/seguridad.

En el contexto de la ingeniería el problema anteriormente descrito implica la implementación de tres tipos de arquitecturas de seguridad basadas en firewall, para de esta forma poder analizar y comparar su desempeño y seguridad dentro de la infraestructura de la red.

1.2. OBJETIVOS

A continuación se presentan las metas a alcanzar durante el desarrollo de este proyecto:

1.2.1. OBJETIVO GENERAL

Analizar el rendimiento y calidad de servicio (QoS) en tres arquitecturas de red con seguridad basadas en firewall.

1.2.2. OBJETIVOS ESPECÍFICOS

- Analizar arquitecturas de redes seguras basadas en firewall y elegir tres.
- Estudiar la información acerca de firewalls basados en software y hardware disponibles para la implementación y arquitecturas de seguridad relacionadas.
- Seleccionar el firewall que permita la implementación de las arquitecturas seleccionadas.
- Realizar el diseño de red para cada una de las arquitecturas de seguridad e implementarlo.
- Ejecutar pruebas de rendimiento y QoS de red en la tres arquitecturas y analizar las medidas obtenidas
- Analizar el nivel de rendimiento respecto de la seguridad, de cada una de las tres arquitecturas.
- Realizar un cuadro comparativo de selección de acuerdo a una relación rendimiento/seguridad.

1.3. ANTECEDENTES

A continuación se cita la de influencia más puntual dentro del tema a tratar.

1.3.1 LOCALES

- En el año 2008, tras un completo trabajo investigativo, Daniel Eduardo Padilla Báez, estudiante de Ingeniería de la Universidad Militar Nueva Granada, dio a conocer su trabajo de grado titulado: "Análisis de Vulnerabilidades y Desempeño de un firewall de plataforma libre contra uno de plataforma licenciada" con el que obtuvo su título de Ingeniero en Telecomunicaciones. [1]
- En el año 2007, luego de un estudio de investigación y análisis, Ricardo Andrés Pertuz de las Salas, estudiante de Ingeniería de la Universidad Militar Nueva Granada, miembro activo del grupo de investigación de la misma, GISSIC[1], publicó los resultados de su estudio bajo el nombre: "*Análisis de Vulnerabilidades y Fortalezas en cinco firewalls de plataforma libre"* con el que obtuvo su título como Ingeniero en Telecomunicaciones. [2]

1.3.2 INTERNACIONALES

- En el año 2005, Vassilis Prevelakis de la Universidad: Drexel University, publica un paper bajo el nombre: "*The Virtual Firewall"* [3] donde explica el funcionamiento de firewalls basados en software.
- En el año 2003, Seny Kamara, Sonia Fahmy y Eugene Schultz, de la Universidad Purdue de Estados Unidos, publicaron un paper bajo el nombre de "*Analysis of Vulnerabilities in Internet Firewalls"*; [4] aquí explicaron, luego de un estudio, los métodos usados para analizar 20 vulnerabilidades de la estructura interna de los firewalls en general.
- En el año 2001, Shawn Grimes publica un estudio bajo el nombre de "*Firewalling for free*" [5], en el cual explica el porqué de usar firewalls gratuitos dando a conocer sus ventajas y desventajas y bajo que situaciones es

[1] GISSIC: Grupo de Investigación en Seguridad y Sistemas de Comunicaciones

preferible usar un firewall de estas características. También explica sus vulnerabilidades.

2. MARCO TEÓRICO

Este capítulo tiene la intención de aclarar al lector los conceptos claves para la correcta interpretación de este documento. A su vez se subdivide en Marco Teórico Conceptual y Marco Teórico Referencial.

2.1. MARCO TEÓRICO CONCEPTUAL

En el Marco Teórico Conceptual se definen los siguientes conceptos:

2.1.1 Análisis de Ingeniería.

En el contexto de la ingeniería, el análisis comprende la aplicación de métodos analíticos y científicos, con el fin de efectuar las descomposiciones pertinentes y de esta manera, definir las propiedades y el estado del sistema analizado.

El proceso de análisis de ingeniería, comprende la descomposición del diseño de ingeniería en los respectivos mecanismos de operación y fallos, de manera que se puedan estudiar cada uno de forma independiente, para finalmente establecer las conclusiones respectivas del caso. [9]

2.1.2 Vulnerabilidad.

En el campo de la seguridad informática, una vulnerabilidad es el fallo de seguridad o la debilidad de un determinado sistema que permite a un intruso pasar las restricciones propias impuestas por el sistema dentro de la red.

Las vulnerabilidades pueden ser producidas por factores como: contraseñas débiles o configuradas por defecto, errores en el diseño de software, virus o ataques más estructurados. [2]

2.1.3 Desempeño.

El término Desempeño hace referencia a la eficiencia en la realización de las funciones propias de un trabajo. El nivel de medición del desempeño es

inherente a los máximos y mínimos que han sido estipulados con anterioridad por expertos en el tema en el que se hace uso de este término.

Este término se puede aplicar directamente en el campo de las telecomunicaciones para hacer medición del estado de las redes, servidores, antenas entre otros.

2.1.4 Seguridad.

En el área de las telecomunicaciones el término seguridad es una condición, producto del correcto establecimiento y mantenimiento de medidas de protección que aseguren que el elemento a custodiar este a salvo de cualquier influencia indeseada; en otras palabras, es aquella condición resultado del establecimiento de unas medidas de protección que aseguren que el elemento esté a salvo de intervenciones no deseadas.

En la seguridad informática, se deben tener en cuenta las siguientes los siguientes aspectos: Confidencialidad, Integridad y la Autenticación además de: amenazas, vulnerabilidades, protocolos, hacking, cracking, herramientas y procedimientos de seguridad y criptografía.

Las medidas de protección que se deben tener en cuenta son básicamente las políticas de seguridad que se deseen implementar. [7]

2.1.5 Software de Código Abierto.

Según la Free Software Foundation [8] el software de código abierto se conoce como aquel usado, estudiado y modificado sin restricciones por lo cual su código se encuentra a disposición de todo el público y si así se requiere puede ser copiado, mejorado y distribuido pero sin alterar los permisos de modificación y distribución. Además se establecen para este los siguientes permisos:

• Puede ser usado para cualquier propósito.

• Puede ser estudiado y modificado.

• Puede ser copiado y distribuido.

• Puede ser mejorado siempre que se hagan públicas las modificaciones realizadas.

Los sistemas operativos más populares de código abierto son: Linux, BSD, Darwin, OpenSolaris.

2.2. MARCO TEÓRICO REFERENCIAL

2.2.1 Desempeño de la red.

La evaluación del desempeño de la red, consiste básicamente en un proceso en el que se estudia el tráfico circulante en una red, con el fin de llevar a cabo un estudio concreto de la capacidad real de la red actual y la planeación de la capacidad de la misma a mediano y largo plazo. [9]

El proceso de evaluación del desempeño de una red concreta varios tipos de mediciones, entre las cuales se nombran y explican las siguientes:

- **Utilización del ancho de banda.** Generalmente expresado como un porcentaje, expresa la relación de ancho de banda ocupado con respecto al ancho de banda total disponible de la red.
- **Paquetes por segundo**. Determina de manera cuantitativa, la cantidad de paquetes que pasan por un punto dado de la red en un lapso de tiempo de un segundo.
- **Round Trip Time (RTT).** Es la cantidad de tiempo que le toma a un paquete en viajar desde un origen, a través de la red, hasta un destino, y regresar.
- **Pérdida de paquetes por segundo.** Establece el número de paquetes que no llegan a su destino.
- **Tasa de errores por segundo.** Determina la cantidad de bits errados con relación al total de bits que pasan por un punto dado de la red en un segundo.
- **QoS**: Se define como la medida del rendimiento de un sistema de transmisión reflejado en su calidad de transmisión y disponibilidad de los

servicios. Desde el punto de vista del usuario, la calidad de servicio, abarca un número de medidas de servicio objetivas y subjetivas determinado por la secuencia de eventos del sistema hasta la terminación del servicio. [15]

La QoS se evalúa mediante la medida de parámetros como: Latencia, Jitter, y Pérdida de Paquetes:

1. ***Latencia:*** El término Latencia hace referencia a los retardos existentes en la transmisión de datos en una red, más exactamente el retardo entre paquetes a la hora de transmitir datos de un punto a otro.

   La latencia se tiene en cuenta con mayor grado de importancia en las transmisiones de servicios que requieran QoS como lo es Voz IP ya que:

   El retardo de una llamada está determinado por la Ecuación *(1)*, en la que tres factores influyen en el total: Retardo en el emisor, Retardo en la red y retardo en el receptor.

$$D = D_{transmisor} + D_{red} + D_{receptor} \quad (1)$$

   Donde:

   $D_{transmisor}$: Latencia producida por el proceso de paquetización en la fuente además se incluye el retardo que se produce por la codificación de las muestras y el retardo de la encapsulación de los paquetes por parte del terminal para ser enviados a través de la red.

   D_{red}: Latencia de la red y está compuesto por 3 factores que son: transmisión, encolamiento y propagación. El retardo de propagación es generalmente despreciado en un enlace LAN, sin embargo éste no lo es en una red WAN.

$D_{receptor}$: Latencia en el receptor, en la cual se incluyen también varios retardos como el de playback, en el cual se incluye el retardo por buffer-jitter, además del retardo de procesamiento.

En el análisis de las variables de la calidad de servicio, se tiene en un principio el retardo proporcionado por el emisor, ya que éste se puede detallar para cada paquete mediante el analizador de protocolos y posteriormente en una hoja de cálculo. Posteriormente, el retardo proporcionado por el receptor se compone de despaquetización, decodificación y el retardo del buffer-jitter. Asimismo, este retardo es bastante difícil de medir, si se quisiera realizar una medición de latencia de "boca a oído", es decir el retardo verdadero. [12]

2. Jitter: El Jitter hace referencia a la variación de la latencia, la cual puede desencadenar una pérdida de paquetes, este se describe en la Ecuación *(2)* , la cual es especificad en la en la RFC 3550. [13]

$$J_{(i)} = J_{(i-1)} + \frac{D_{(i-1,i)} - J_{(i-1)}}{16} \qquad (2)$$

El jitter tenido en cuenta para efectos de pruebas y simulaciones, consiste en el promedio del mismo, muchas veces llamado mean jitter; este valor está determinado por el valor medio de todos los J_i de los paquetes de voz durante una llamada.

3. Pérdida de Paquetes: La pérdida de paquetes, hace referencia a la pérdida de alguna de las unidades de información, que componen un mensaje transmitido a través de una red.

La pérdida de paquetes en el servicio de Voz sobre IP, en una red, se puede presentar por diversos motivos: el primero de estos, por la congestión en la misma, al momento de transmitir diferentes tipos de

tráfico; para solucionar esto, se puede implementar en la red, la Teoría de Colas para dar prioridad al tráfico que requiera mayor prioridad, por requerir QoS o si las políticas de la organización así lo requieren.

Lo anterior no se puede cumplir, cuando se establece encripción en señalización, ya que los paquetes son reconocidos como trafico UDP simplemente.

Para la pérdida de paquetes se tienen límites de QoS acorde con la red que se evalúa, en la red LAN, éste límite debe ser menor al 1% mientras que en una red WAN, éste porcentaje no debe superar el 5%.

Otra causa de pérdida de paquetes de VoZ IP en la red, es la sobrecarga del buffer-jitter, ya que este aumenta a medida que aumenta el número de llamadas en la red; cuando esto sucede, el emisor deja de enviar paquetes al destino y estos se consideran perdidos, ya que no se hace un envío correcto y en secuencia. [14]

2.2.2 Throughput

El Throughput es la medida de la capacidad de canal inherente a una red, y determina la cantidad de información que se puede enviar por un canal de comunicaciones.

Para realizar análisis de Throughput como primera medida se debe establecer la longitud de los paquetes con que se envía la información por dos aspectos importantes: si esta longitud es pequeña, el sistema estará trabajando con eficiencia baja y si es muy grande se incrementa la posibilidad que los paquetes se dañen y por ende se hagan retransmisiones innecesarias que reducirían el desempeño de la red; es por esto que debe existir un tamaño de paquetes adecuado que no afecte el rendimiento de la red, este tamaño adecuado debe

tener en cuenta las características de error del enlace y la cantidad de bits de control que use. Las unidades de media del Throughput son Bits por segundo. [11]

2.2.3 Teoría de Colas

Para el proyecto se utilizará priorización de tráfico; es decir, el IPFW, brinda la posibilidad de crear diferentes colas dependiendo del tipo de tráfico, para nuestro caso se crean dos colas: una para tráfico de VOZ IP y la otra para tráfico FTP; la cola que contenga tráfico de VOIP tendrá una prioridad del 80% dejando para FTP una prioridad del 20%, para de esta manera lograr una QoS adecuada para el servicio que lo requiere, es decir Voz IP

2.2.4 TCP/IP

Como definición de TCP/IP, según [10], se dice que hace referencia al conjunto o pila de protocolos que hace posible una comunicación de extremo a extremo dentro de Internet permitiendo el envío de datos entre diferentes lugares del mundo. El nombre TCP/IP es debido a que TCP e IP son los protocolos pilares sobre los cuales Internet ha crecido de forma acelerada.

2.2.5 Puertos TCP

La implementación y administración de sistemas de seguridad basados en firewall requieren el uso de puertos TCP, los cuales se definen como el punto final de una conexión lógica y el medio por el cual un cliente se comunica con un programa específico en una red. La IANA a preasignado números a algunos puertos, estos números especifican el puerto usado por el puerto del servidor como puerto de contacto.

El acceso a estos puertos para los clientes es definido en los servidores por el administrador de la red. [10]

2.2.6 Aplicaciones de red

Son servicios que se prestan mediante aplicaciones montadas en los diferentes servidores en la red. Las aplicaciones más conocidas son: [10]

- **FTP (File Transfer Protocol):** Protocolo de Transferencia de Archivos, es un servicio corriendo como una aplicación en un servidor y da la facilidad de transferir archivos entre una máquina y otra; dependiendo de la configuración establecida se puede incluso borrar, crear, renombrar dichos archivos de un lado a otro. La máquina que presta este servicio se conoce como servidor.
- **HTTP (Hypertext Transfer Protocol):** Protocolo de Transferencia de Hipertexto, es el protocolo más usado en internet, ya que sobre él se envía todo el contenido de las páginas web. Cuando un cliente desea ver una página web en particular, realiza una petición al servidor (por medio de su navegador) que posee dicha página, el cual responde a la petición mediante el protocolo HTTP y el contenido de dicha página es decodificado por el navegador del cliente.
- **TELNET**: Es un software que permite la emulación de terminal para acceder a una máquina remota y de esta forma introducir comandos para manejar dicha máquina desde otro computador.
- **SMTP (Simple Mail Transfer Protocol):** Protocolo de Transferencia Simple de Correo, permite que los servidores presten servicio de correo electrónico a sus clientes, ya que mediante él se envían y reciben correos electrónicos en el servidor, los correos que recibe los envía de la misma manera; cuando un cliente desea ver un correo que se le ha enviado, utiliza otros protocolos como son POP3 e IMAP4.

Otras aplicaciones existentes y que ayudan a medir el rendimiento de una red son:

- **Voz sobre IP:** El envío de voz sobre IP se realiza de manera digital a diferencia de la telefonía tradicional; este envío es posible gracias a la aceptable tasa de transmisión de información multimedia con que empiezan a transmitir las redes de datos. En las redes de voz sobre IP existe un control de llamadas encargado de la traducción de direcciones IP y planes de marcación telefónica, con el fin de relacionarlos y lograr establecer la

comunicación. El funcionamiento de la redes de Voz sobre IP se basa en la conmutación de paquetes, donde el ancho de banda de las redes es aprovechado al máximo. Este factor es determinante en la preferencia de la redes Voz sobre IP sobre la red tradicional de conmutación de circuitos, ya que esta última hace desperdicio de ancho de banda puesto que hace uso de un ancho de banda constante durante toda la transmisión sin importar que esta transmita o no información. El objetivo de la voz sobre IP es unificar la red de voz y de datos, adquiriendo variados beneficios como la disminución de costos invertidos en la red y la centralización en una misma infraestructura de la red de datos y un conjunto de servicios telefónicos propios de la red telefónica pública básica conmutada de las redes analógicas existentes. La transmisión de Voz sobre IP se basa principalmente en tres protocolos: SIP, H.323. e IAX. [17]

Los principales problemas en cuanto a la calidad del servicio (QoS) de una una red de VoIP, son la Latencia, el Jitter, la pérdida de paquetes y el Eco.

2.2.7 Firewall

Se define como un dispositivo de red, que tiene como fin proteger una red privada del tráfico no deseado y controlan qué recursos externos pueden utilizar los usuarios de la red privada. [16]

Conceptualmente hay dos tipos de firewalls: de nivel de red y de nivel de aplicación:

Los firewalls de nivel de red toman sus acciones en función del origen, la dirección de destino y el número de puerto en cada paquete IP. Los modernos firewalls de este tipo se han sofisticado y mantienen información respecto del estado de las conexiones que están activas a través de él, etc. Este tipo de firewall tiende a ser muy rápido y es transparente al usuario

Los firewalls de nivel de aplicación por lo general son hosts corriendo proxy servers, que no permiten el tráfico directo entre redes, manteniendo una

elaborada auditoria y logeo del tráfico que pasa a través de él. Este tipo de firewall puede ser utilizado para realizar las tareas relativas al NAT[2], debido a que como las comunicaciones van de un lado hacia el otro se puede enmascarar la ubicación original. Este tipo tiende a proveer un mayor grado de seguridad que los de nivel de red. [1]

[2] NAT (Network Addres Translation): proceso de reemplazo de una direccion IP por otra en la cabecera IP.

3. INGENIERÍA DEL PROYECTO

En este capítulo se establecerá el estado del arte enfocado a las arquitecturas de redes seguras basadas en firewall así como su rendimiento y calidad de servicio. De la misma forma se establecerán los requerimientos de diseño y las variables de ingeniería a tener en cuenta para la realización del presente proyecto.

3.1. ESTADO DEL ARTE

Actualmente para la elección de una red segura basada en firewall para implementar en las organizaciones, se maneja básicamente una sola posibilidad de elección: el criterio del administrador.

Por su parte, el tipo de firewall a implementar tiene criterios de elección documentados: La primera de ellas hace referencia al tipo de firewall a implementar en la red, el cual puede ser mediante un equipo dedicado de hardware, específicamente diseñado para cumplir sus funciones como firewall ó un sistema de seguridad basado en software implementado en un computador exclusivamente dedicado a las funciones de filtrado para la red. Como segunda posibilidad de selección, se tienen los firewalls de código abierto y plataforma libre, los cuales generalmente se asocian con una licencia de distribución gratuita. O bien, por otro lado se encuentran los firewalls comerciales, de licencia propietaria, plataforma licenciada y distribución restringida directamente por el fabricante del software. Y como última opción un documento que muestra vulnerabilidades y desempeño de un firewall libre contra uno licenciado. [4] [6].

Es en la ausencia de criterios de elección de arquitecturas seguras para los administradores de red que tiene cabida la realización de este proyecto, recolectando toda la información necesaria acerca de las diferentes arquitecturas así como los diferentes tipos de firewall para su implementación.

3.2. REQUERIMIENTOS DE DISEÑO

En un entorno de red real, se tienen mínimo tres niveles de seguridad a implementar mediante la instalación de un firewall; los cuales se denominan zonas y a menudo se relacionan con los colores verde, anaranjado y rojo, para hacer referencia a las zonas militarizada, desmilitarizada y WAN, en su orden respectivo de protección; estas zonas se muestran en la *Figura 1*:

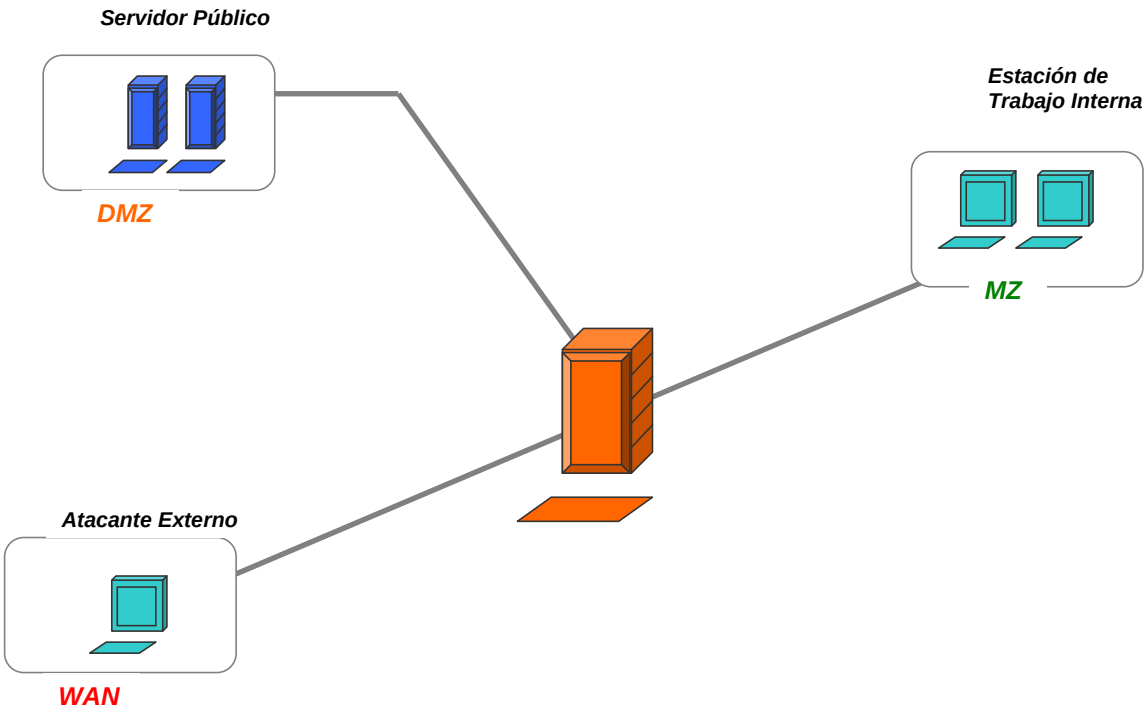


Figura 1: Zonas de Protección de un Firewall

Para llevar a cabo la realización de este proyecto, se toma en cuenta la configuración de cada una de las arquitecturas seleccionadas para la implementación de las diferentes zonas.

3.3. ANÁLISIS DE VARIABLES DE INGENIERÍA

A continuación se citan y explica cada uno de los criterios de evaluación de las diferentes arquitecturas a implementar para realizar el correspondiente análisis de rendimiento y QoS.

3.3.1. Variables de Selección de Arquitecturas

- **Escalabilidad**

Se define como la característica de la arquitectura a tratar, que permite el crecimiento continuo de trabajo con fluidez, o en estos casos, muestra la preparación que tiene la arquitectura para crecer manteniendo su calidad y rendimiento. En otras palabras, se puede definir como la característica que tiene la arquitectura de modificar su tamaño para ajustarse a los cambios de la organización.

- **Transparencia para la red**

Esta variable hace referencia a la capacidad que tiene la arquitectura, al momento de conectar más equipos, de continuar funcionando con la misma configuración o si se requiere reprogramación.

- **Facilidad de Implementación**

Esta variable representa un criterio importante a la hora de hacer la elección de las arquitecturas, y define la sencillez que tiene la arquitectura al momento de realizar su implementación.

- **Facilidad de Administración**

Esta variable representa un criterio importante a la hora de hacer la elección de las arquitecturas, y define la sencillez que tiene la arquitectura al momento de realizar su administración.

- **Nivel de seguridad**

Esta Variable hace referencia al grado de seguridad, teniendo en cuenta los equipos a utilizar para la implementación de la arquitectura, que esta brinda a la red a proteger.

- **Punto crítico de vulnerabilidad**

Esta característica, se refiere básicamente a la existencia de un componente en la arquitectura, que cuando ocurre un fallo en su funcionamiento, esto ocasiona un fallo global en el sistema.

- **Existencia de DMZ**

La DMZ, también conocida como red perimetral, se define como una red local ubicada entre la red interna de una organización y una red externa, por ejemplo internet. El objetivo de implementar estas DMZ, es controlar el tráfico saliente de la red interna, el cual se permite, mientras que el tráfico entrante de la red externa es denegado. En esta red, generalmente se ubican servidores que deben ser accesibles desde una red externa, por ejemplo: servidores web, ftp, de correo electrónico. [4]

3.3.2. Variables de Evaluación de Arquitecturas

- **Throughput**

Para obtener un valor de Throughput fiable en las pruebas de Rendimiento y Rendimiento/Qos, se realizan 50 descargas de un archivo de 136MB desde y hacia diferentes zonas, dependiendo de la arquitectura a evaluar; se realiza la captura con el analizador de protocolos Wireshark, y se toma el tiempo desde el inicio de la descarga hasta el último byte transmitido correctamente; luego de tener estos datos se aplica la siguiente fórmula:

$$Throughput = \frac{Tamañodelarchivo(bits)}{Tiempototaltransmisión} \quad (3)$$

Con los datos obtenidos de cada uno de los cálculos con la (3), se realiza un análisis estadístico de Media y Mediana y se obtiene el resultado final de cada prueba.

- **Latencia**

El valor de Latencia para las pruebas de QoS y Rendimiento/Qos, se obtiene realizando 50 llamadas de 1 minuto desde y hacia diferentes zonas dependiendo de la arquitectura a evaluar. Con el analizador de protocolos Wireshark se toman las capturas desde la zona del servidor y del cliente respectivamente y el valor es arrojado por el mismo analizador, el cual realiza el cálculo aplicando la Ecuación (1), para cada una de las capturas tomadas. De igual forma se realiza el análisis estadístico de Media y Mediana para obtener datos más acertados.

- **Jitter**

El jitter para cada una de las arquitecturas se obtiene realizando 50 llamadas de 1 minuto desde y hacia diferentes zonas dependiendo de la arquitectura a evaluar y tomando las capturas con el Analizador de protocolos Wireshark, el cual se encarga de realizar el cálculo haciendo uso de la Ecuación (2); estos datos obtenidos del Wireshark se analizan estadísticamente y se obtiene el resultado final para cada prueba en cada arquitectura.

- **Paquetes perdidos.**

De la misma manera que se obtienen Jitter y Latencia mediante el analizador de protocolos Wireshark luego de realizar las 50 llamadas correspondientes a cada prueba, reobtiene el porcentaje de paquetes perdidos mediante una relación Paquetes Enviados/Paquetes Recibidos; este dato es arrojado por el Wireshark.

3.4. DESARROLLO DEL PROYECTO

En este apartado se describirá el desarrollo completo del proyecto, dando inicio en la metodología empleada para la solución, seguido de la ejecución de cada una de las fases para terminar en el posterior análisis planteado en el siguiente capítulo.

3.4.1 Metodología

Basado en los objetivos específicos, el proyecto titulado: “Análisis de Rendimiento y QoS en tres arquitecturas de seguridad basadas en firewall”, se plantea la metodología como pasos consecutivos y se muestran en la *Figura 2*:

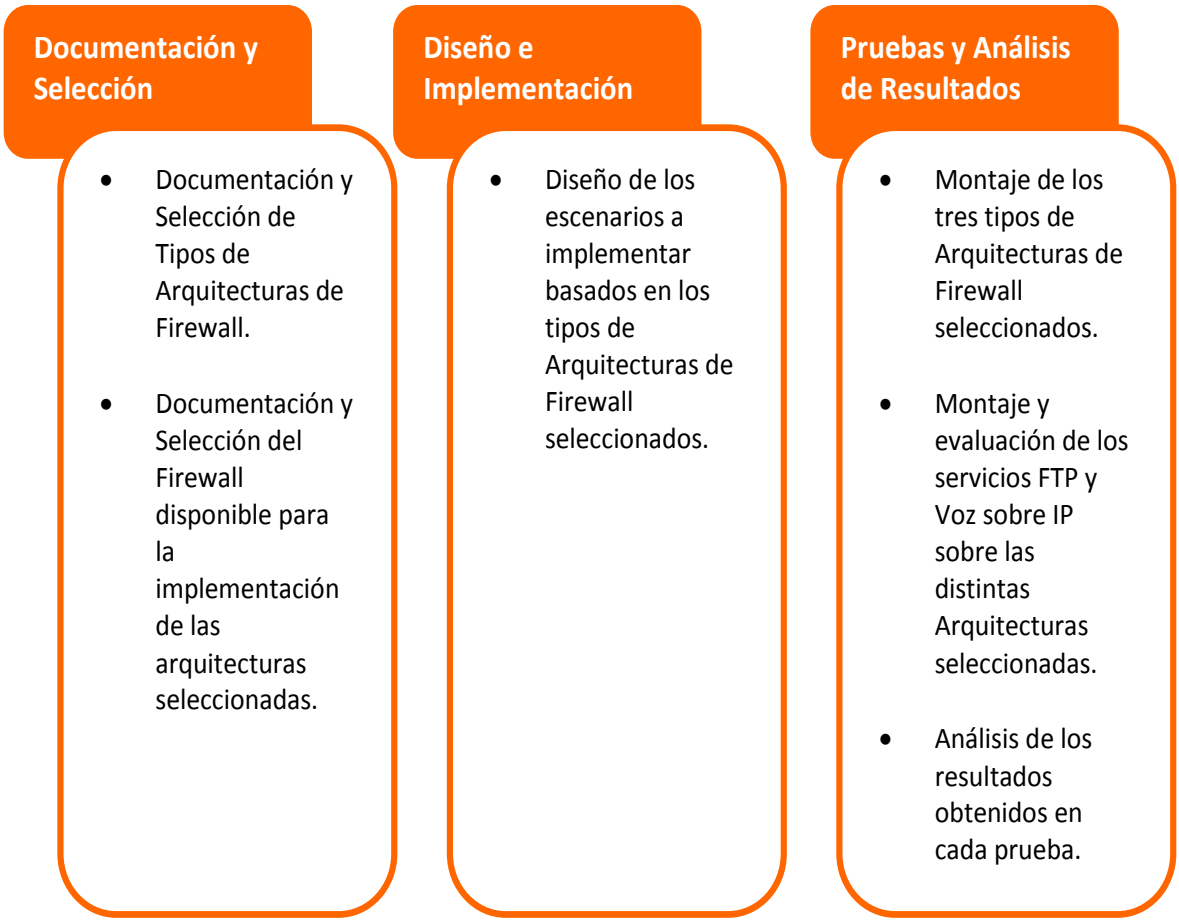


Figura 2: Metodología de Ejecución del Proyecto

3.4.2 Documentación y Selección

Este proceso es de vital importancia para la realización del proyecto, ya que es el punto de partida del mismo; contiene diferentes aspectos de carácter investigativo y teórico.

ARQUITECTURAS DE FIREWALL

1. ***Dual homed-Host (Dual home Gateway):*** Esta primera arquitectura se presenta en la Figura 3:

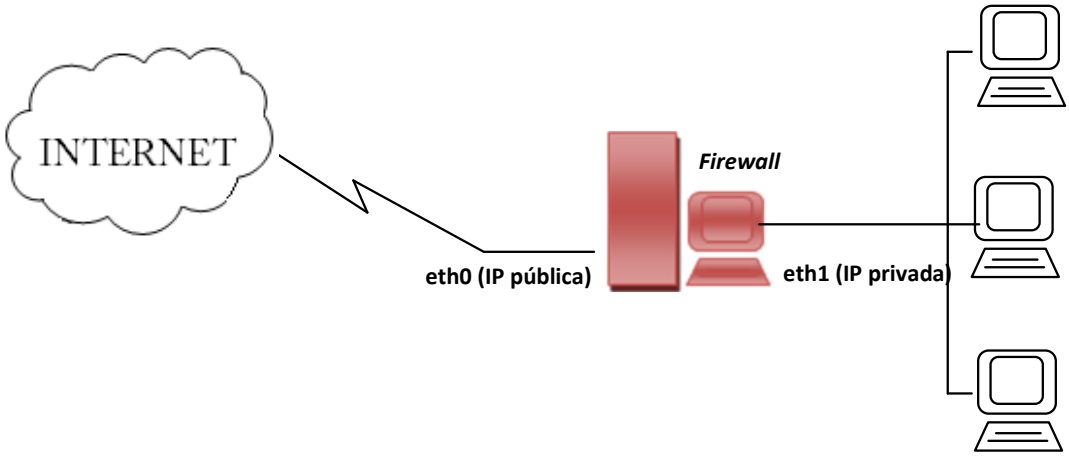


Figura 3: Dual homed-host

Básicamente se trata de un host con dos tarjetas de red, cada una de ellas conectada a una red diferente. En principio un sistema instalado sobre un host con estas características enrutará paquetes de una red a otra. Para aislar las dos redes es necesario deshabilitar la función de enrutamiento. Tiene una gran ventaja y es su sencillez pues solo requieren de un ordenador. La desventaja es que solo soportan servicios mediante proxy y no filtro de paquetes ya que al tener la función de enrutamiento deshabilitada, se forza a que el tráfico deba ser tratado por una aplicación en el propio host.[18]

Esta arquitectura puede ser utilizada en las redes para separar los componentes del servidor de seguridad en los sistemas por separado, logrando así un mayor rendimiento y flexibilidad, aunque a costa de la simplicidad A medida que cada componente del sistema del servidor deba desempeñar sólo una tarea específica, la configuración de la arquitectura resulta más sencilla de realizar.[19]

2. ***Screened subnet:*** Esta arquitectura es mostrada en la Figura 4:

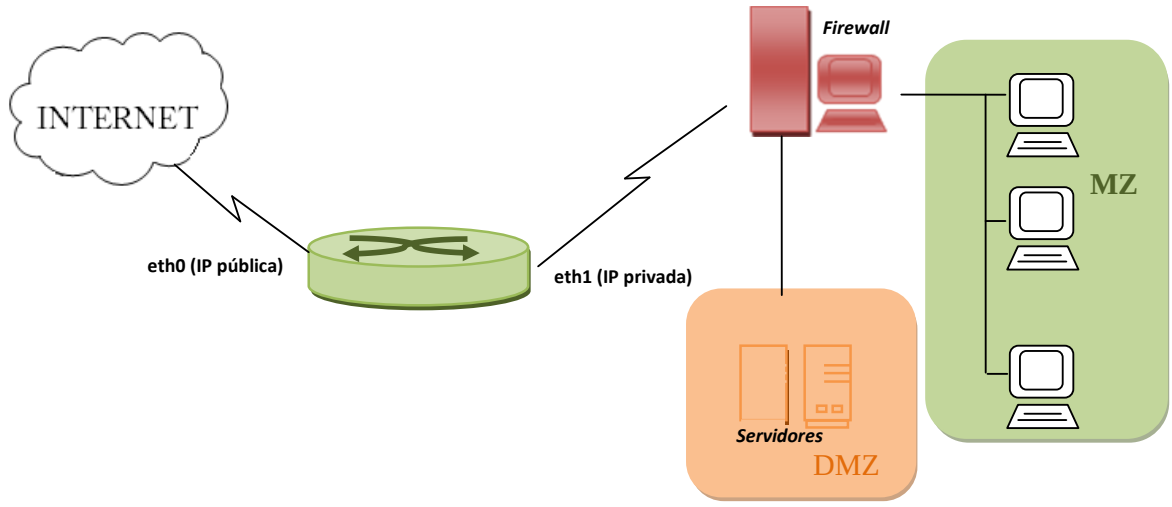


Figura 4: Screened Subnet

La arquitectura Screened Subnet, también conocida como red perimétrica o De-Militarized Zone (DMZ) es la más utilizada e implantada hoy en día, ya que añade un nivel de seguridad en las arquitecturas de cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al firewall: como se puede ver en el modelo anterior toda la seguridad se centraba en el firewall, de forma que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red. Como el firewall es un objetivo interesante para muchos piratas, la arquitectura DMZ intenta aislar una red perimétrica de forma que un intruso que accede a esta máquina no consiga un acceso total a la subred protegida. [18]

En esta red perimétrica, que constituye el sistema cortafuegos, se incluye el firewall y también se podrían incluir sistemas que requieran un acceso controlado, como baterías de módems o el servidor de correo, que serán los únicos elementos visibles desde fuera de nuestra red. El router exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red

externa), También es posible, si se necesita mayores niveles de seguridad, definir varias redes perimétricas en serie, situando los servicios que requieran de menor fiabilidad en las redes más externas: así, el atacante habrá de saltar por todas y cada una de ellas para acceder a los equipos; evidentemente, si en cada red perimétrica se siguen las mismas reglas de filtrado, niveles adicionales no proporcionan mayor seguridad.

Esta arquitectura de cortafuegos elimina los puntos únicos de fallo: antes de llegar al firewall (por definición, el sistema más vulnerable) un atacante ha de saltarse las medidas de seguridad impuestas por el enrutador externo. Si lo consigue, como se ha aislado la DMZ en una subred se está reduciendo el impacto de un atacante que logre controlar la red, ya que antes de llegar a la red interna ha de comprometer también al segundo router; en este caso extremo (si un pirata logra comprometer el segundo router), la arquitectura DMZ no es mejor que un Dual homed-host. Por supuesto, en cualquiera de los tres casos (compromiso del router externo, o del firewall) las actividades de un pirata pueden violar la seguridad, pero de forma parcial: por ejemplo, simplemente accediendo al primer enrutador puede aislar toda nuestra organización del exterior, creando una negación de servicio importante, pero esto suele ser menos grave que si lograra acceso a la red protegida.

Aunque, la arquitectura DMZ es la que mayores niveles de seguridad puede proporcionar, no se trata de la panacea de los cortafuegos. Evidentemente existen problemas relacionados con este modelo: por ejemplo, que la mayor parte de la seguridad reside en los routers utilizados; como hemos dicho antes las reglas de filtrado sobre estos elementos pueden ser complicadas de configurar y comprobar, lo que puede dar lugar a errores que abran importantes brechas de seguridad en nuestro sistema. [18][19]

3. Dual Firewall: Se observa la arquitectura Dual Firewall en la Figura 5:

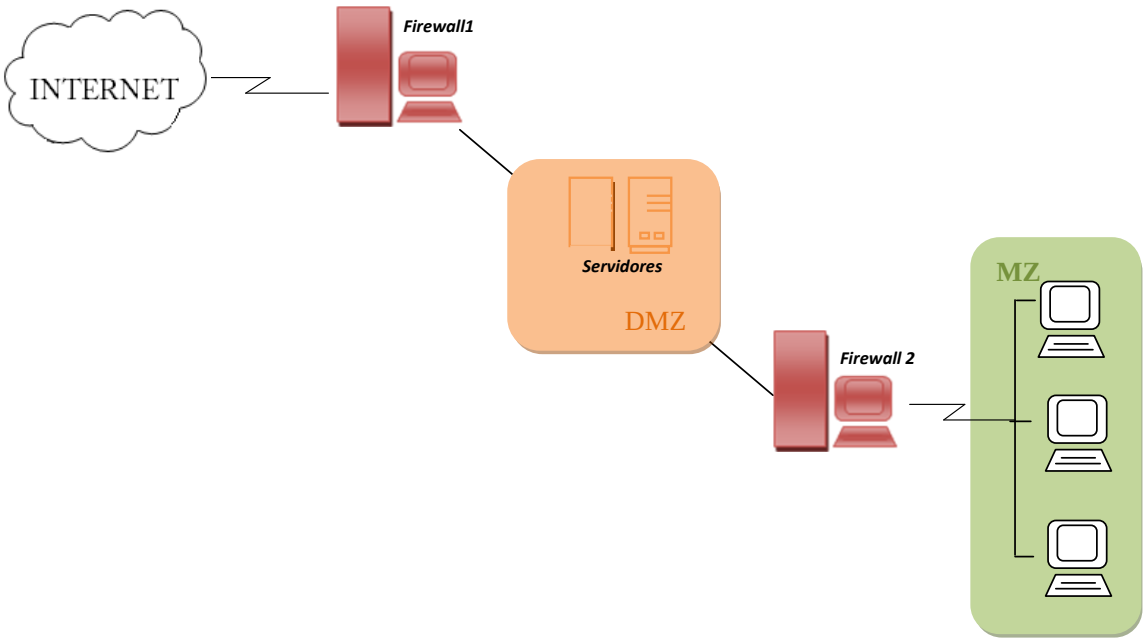


Figura 5: Dual Firewall

La arquitectura dual-firewall es más compleja que la arquitectura de un solo servidor de seguridad, pero también es un diseño más seguro y proporciona un nivel de seguridad extra; esto se debe a que la arquitectura utiliza dos servidores de seguridad; lo mejor para la implementación es que sean de distintos fabricantes y modelos, para actuar como servidores de seguridad interior y exterior y proporcionar un segmento "zona de distensión" entre los dos servidores de seguridad, como se muestra en la *Figura 5*. Al igual que las arquitecturas anteriores, el tráfico está permitido en el segmento de zona DMZ, así como de la red interna hacia la red externa, pero no hay tráfico de la red externa que esté permitido directamente a la red interna.

El control en una arquitectura de doble firewall viene del hecho de que cada uno de los servidores de seguridad proporciona un subconjunto de restricciones para todo el tráfico que entra y sale de una red. Debido a que no son de confianza (es

decir, externa) el tráfico no se debe permitir acceder directamente a la red interna; el servidor de seguridad exterior puede ser configurado específicamente para permitir el acceso desde y hacia el segmento de la zona DMZ y sistemas externos. Del mismo modo, el servidor de seguridad interior puede ser configurado para permitir el acceso desde y hacia el segmento de la zona DMZ y de los recursos internos. Esto permite la creación de dos puntos distintos e independientes de control de todo el tráfico de entrada y salida de todos los segmentos de la red, tanto si son segmentos DMZ o segmentos de la red interna.

Cuando una arquitectura de doble cortafuegos se lleva a cabo con distintos modelos de servidor de seguridad (por ejemplo, un servidor de seguridad Cisco PIX y un servidor de seguridad de Microsoft ISA Server), también adquieren la seguridad adicional, ya que el atacante tendría necesidad de comprometer dos servidores de seguridad por separado para obtener acceso a recursos protegidos. Además, un atacante también tiene que estar bien informado en el funcionamiento de dos tipos diferentes de servidores de seguridad para manipular las configuraciones.

Las desventajas de una arquitectura de doble firewall se refieren a la complejidad de la aplicación y el costo. Con respecto a la complejidad, una arquitectura de doble cortafuegos con frecuencia requiere de algún tipo de enrutamiento que se ejecutará en los diferentes segmentos de red dependiendo de las políticas de seguridad de cada organización. Aunque muchas empresas sólo tienen que utilizar las declaraciones de enrutamiento estático en los servidores propios, mayor será el número de servidores en la DMZ, más difícil se hace para gestionar y mantener las declaraciones de enrutamiento.

Aparte de los obvios costos relacionados con la implementación y mantenimiento de múltiples cortafuegos, también es más costoso de implementar y gestionar una arquitectura de doble firewall, ya que necesita la gente que entiende las tecnologías de servidor de seguridad múltiples.

Debido al costo y la complejidad de la arquitectura de doble firewall, suele aplicarse en entornos con requisitos de seguridad críticos, tales como banca, administración pública, las finanzas, y las organizaciones más grandes médicos.

4. Dual firewall Dual DMZ: Se presenta en la Figura 6:

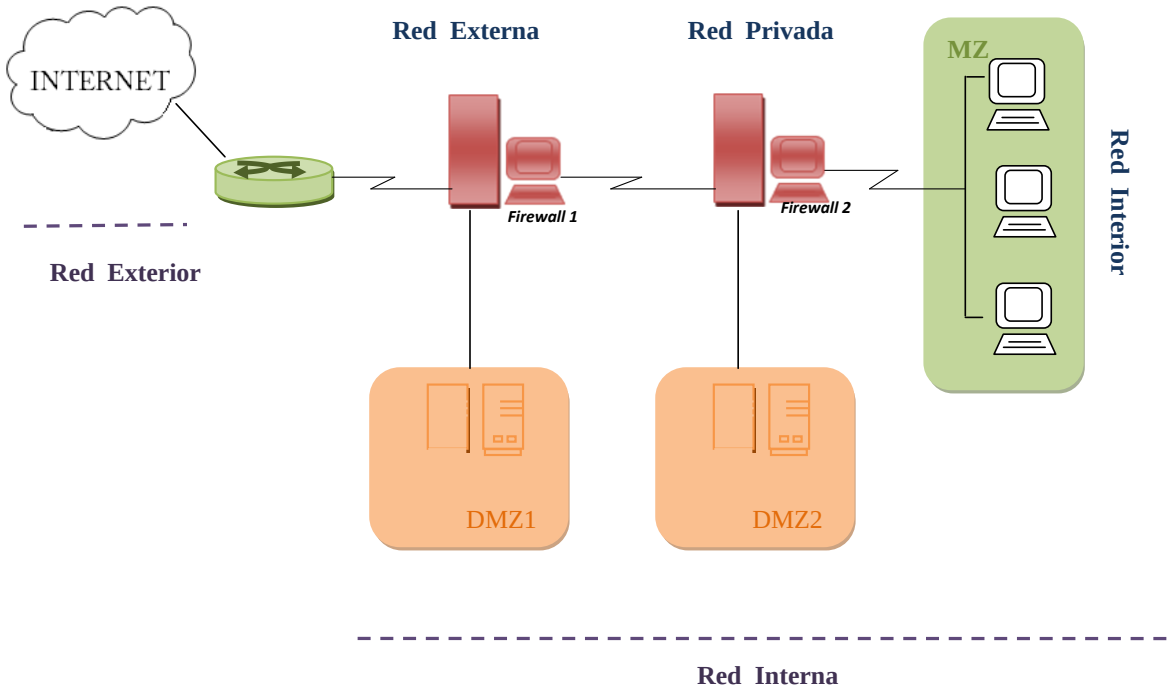


Figura 6: Dos Firewall Dos DMZ

En este caso ambas interfaces de los firewalls se encuentran configuradas. Tres zonas de red están formadas en la red interna: la red exterior, la red privada y la red interior.

Existe una red privada entre los firewalls interior y exterior. Una organización puede colocar algunos servidores en la red privada y mantener los más delicados detrás del firewall interior. Por otra parte, una organización quizá desee una seguridad máxima y usar la red privada como una segunda zona de buffer o DMZ interior, además de mantener todos los servidores en la red interior.

Si una empresa quiere proporcionar acceso completo a una gran variedad de servicios, como FTP anónimo (protocolo de transferencia de archivos), Gopher y

WWW (World Wide Web), puede proveer ciertos servidores de sacrificio en la DMZ exterior. Los firewalls no deben confiar en ningún tráfico generado desde estos servidores de sacrificio.

El router de selección debe estar configurado para enviar todo el tráfico recibido desde las redes externas para la red interna hacia el firewall interior. Antes de mandar el tráfico, el router aplicará las reglas de filtro de paquetes. Sólo el tráfico de la red que pasa esas reglas se dirigirá al firewall exterior; el resto será rechazado. Un intruso debe penetrar primero el router y, si lo hace, se enfrentará al firewall exterior.

Sin que le importe violar las defensas de la red exterior, el intruso penetra en el firewall interior. Por ello, si los recursos lo permiten, tal vez se desee dar a cada firewall la responsabilidad de un grupo administrativo diferente. Esto asegura que los errores de un grupo de administradores no los repitan los demás administradores. También se debe garantizar que los dos grupos compartan información acerca de debilidades descubiertas en los firewalls.

Otro tipo de configuración de red se obtiene al utilizar dos firewalls, pero sólo una interfaz de red de cada uno. Un segundo router llamado ”drowner” se agrega entre la DMZ y las redes interiores. Se debe asegurar que los firewalls no se ignoren y que los routers usen rutas estáticas.

A partir de estos elementos, firewalls con una o dos interfaces de red y routers, se pueden lograr diferentes configuraciones que surgen de la combinación de ellos. Cuando sólo esté en uso una interfaz de red del firewall, se deben utilizar rutas estáticas en los routers y configurar bien las entradas de las tablas de enrutamiento para asegurar que los firewalls no se ignoren.

3.4.3 Selección de las arquitecturas a implementar

En esta parte del proyecto y haciendo uso de variables anteriormente citadas y explicadas, se realiza la selección de las arquitecturas a implementar para la ejecución de pruebas, así:

A cada variable dependiendo de cuál sea esta, se le asigna un valor, dependiendo de características propias de la misma:

1. **Existencia de DMZ**: Los únicos valores posibles de esta variable son: SI y NO, correspondientes a si existe o no zona Desmilitarizada en la Arquitectura a evaluar. Por no tener valor cuantitativo, esta variable actuará como valor agregado al momento de realizar la elección de las arquitecturas a implementar.

   El puntaje correspondiente a cada arquitectura según esta variable se muestra en la *Tabla 1*:

ARQUITECTURA DE FIREWALL	EXISTENCIA DE DMZ
Dual homed-host	NO
Screened subset	SI
Dual firewall	SI
Dual firewall, Dual DMZ	SI

Tabla 1: Existencia de DMZ en las Arquitecturas de Firewall

2. **Punto crítico de Vulnerabilidad:** Esta variable, al igual que la anterior es de tipo cualitativo y puede tener únicamente dos valores: SI correspondiente a si existe un punto único de fallo, es decir, una única línea de defensa y NO correspondiente a si la arquitectura a evaluar tiene más de una línea de defensa; de igual forma se utilizará como valor agregado al momento de llevar a cabo la selección; el valor para cada arquitectura se muestra en la *Tabla 2*:

ARQUITECTURA DE FIREWALL	PUNTO CRÍTICO DE VULNERABILIDAD
Dual homed-host	SI
Screened subset	NO
Dual firewall	NO
Dual firewall, Dual DMZ	NO

Tabla 2: Existencia de Punto Único de Fallo en las Arquitecturas de Firewall

Las 3 variables siguientes son de tipo cuantitativo y se calificarán de 1 a 4 siendo 1 el valor más bajo y 4 el valor más alto posible, arrojando los resultados para cada una de las arquitecturas a evaluar, dependiendo de características propias de las mismas:

3. **Transparencia para la red:** La descripción correspondiente a la calificación de la variable "Transparencia para la red" se presenta en la *Tabla 3*:

Puntaje	*Descripción*
1	Posibilidad de conectar equipos sin cambiar la configuración de los ya instalados.
2	Posibilidad de conectar equipos, cambiando la configuración de la primera línea de defensa.
3	Posibilidad de conectar equipos cambiando la configuración de las tarjetas de red de los equipos conectados.
4	Posibilidad de conectar equipos cambiando la configuración total de la red.

Tabla 3: Transparencia para la red de las Arquitecturas de Firewall

4. **Facilidad de implementación:** La descripción correspondiente a la calificación de la variable “Facilidad de implementación” se presenta en la *Tabla 4*:

Puntaje	***Descripción***
1	Implementación de la arquitectura con una única línea de defensa
2	Implementación de la arquitectura con dos líneas de defensa
3	Implementación de la arquitectura con más de dos líneas de defensa
4	Implementación de la arquitectura con más de dos líneas de defensa y equipos de protección adicionales.

Tabla 4: Facilidad de Implementación de las Arquitecturas de Firewall

5. **Facilidad de administración:** La descripción correspondiente a la calificación de la variable “Facilidad de implementación” se presenta en la *Tabla 5*:

Puntaje	***Descripción***
1	Administración y mantenimiento de un único equipo de seguridad, sin cambio periódico de configuraciones
2	Administración y mantenimiento de dos equipos involucrados en la seguridad sin cambio periódico de configuraciones
3	Administración y mantenimiento de dos equipos involucrados en la seguridad con cambio periódico de configuraciones
4	Administración y mantenimiento de más de dos equipos involucrados en la seguridad

Tabla 5: Facilidad de Administración de las Arquitecturas de Firewall

6. **Nivel de seguridad:** La descripción correspondiente a la calificación de la variable “Facilidad de implementación” se presenta en la *Tabla 6*:

Puntaje	***Descripción***
4	Muy seguro
3	Seguro con un posible punto vulnerable sin que comprometa la seguridad de la red interna de la organización
2	Seguro con puntos vulnerables que comprometan la seguridad de la red interna de la organización
1	Muy vulnerable

Tabla 6: Nivel de Seguridad de las Arquitecturas de Firewall

Para realizar la selección de las arquitecturas, a cada variable se le asigna un porcentaje dependiendo del grado de importancia en las características de las arquitecturas anteriormente nombradas; esta distribución de porcentajes es presentada en la *Figura 7*:

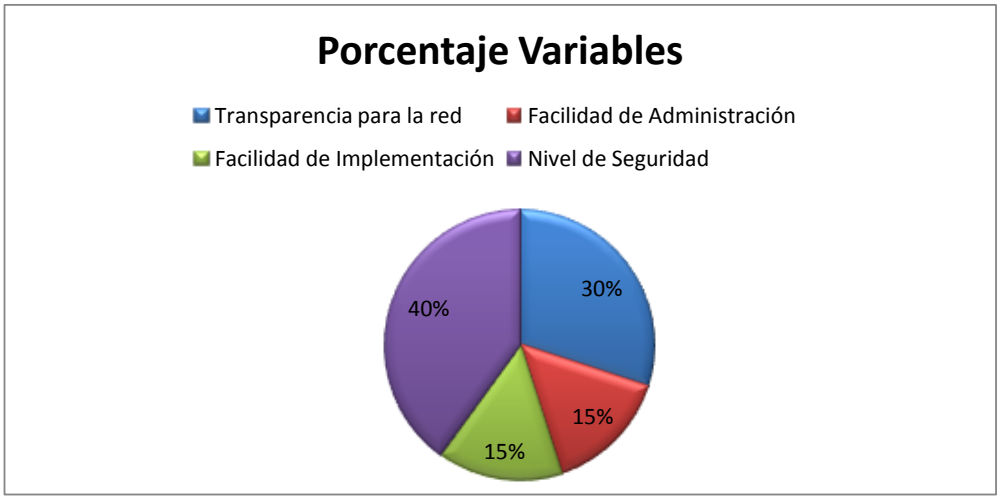


Figura 7: Porcentaje de Evaluación Variables

Los puntajes correspondientes a cada arquitectura según las variables anteriormente explicadas se muestran en la *Tabla 7*:

Arquitectura de Firewall	Transparencia para la red	Facilidad Administración	Nivel de Seguridad	Facilidad Implementación
Dual homed-host	4	1	2	1
Screened subset	3	2	2	2
Dual firewall	2	2	3	3
Dual firewall - Dual DMZ	2	4	4	4

Tabla 7: Puntaje Final de las Arquitecturas de Firewall (Variables Cuantitativas)

El orden por suma de puntajes de las variables cuantitativas, de las arquitecturas, es presentada en la *Tabla 8*:

Posición	ARQUITECTURA	PUNTAJE TOTAL
1	Dual firewall, Dual DMZ	3,40
2	Dual firewall	2,85
3	Screened Subnet	2,7
4	Dual homed-host	1,90

Tabla 8: Orden por suma de puntajes de variables cauntitativas de las Arquitecturas de Firewall

Quedando eliminada la arquitectura: “Dual homed-host”.

De igual forma teniendo en cuenta las variables cuantitativas y tomándolas como criterio de exclusión, el orden final según el total de las variables a evaluar en cada arquitectura es el mostrado en la *Tabla 9*:

Posición	ARQUITECTURA DE FIREWALL
1	Dual firewall - Dual DMZ
2	Dual firewall
3	Screened Subnet
4	~~Dual homed-host~~

Tabla 9: Orden por suma de puntajes de variables cuantitativas y cualitativas de las Arquitecturas de Firewall

Dejando eliminada la arquitectura “Dual homed-host”. Finalmente las arquitecturas a implementar para la ejecución de pruebas se presentan en la *Figura 8*:

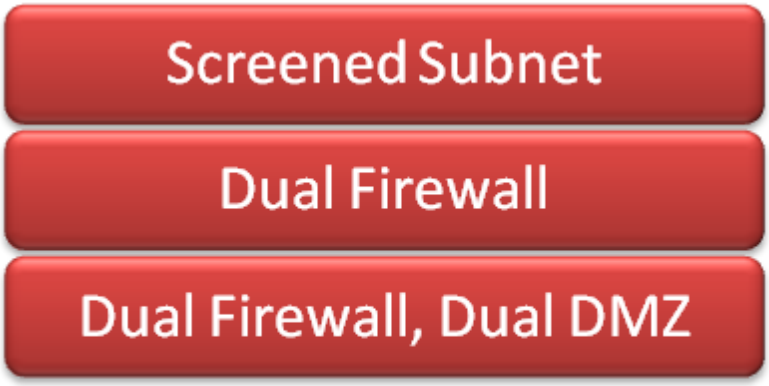


Figura 8: Arquitecturas de Firewall a implementar

3.4.4 Documentación y elección del firewall que permita la implementación de las arquitecturas seleccionadas.

Tomando como referencia la tesis bajo el nombre “Análisis de Fortalezas y Vulnerabilidades en 5 firewalls de plataforma libre”, realizada en el año 2008 por el Ingeniero Ricardo Pertuz, la cual arroja como resultado el mejor de estos en cuanto a seguridad se refiere, se define el firewall a implementar.

El desarrollo de esta investigación se llevó a cabo con la siguiente metodología:

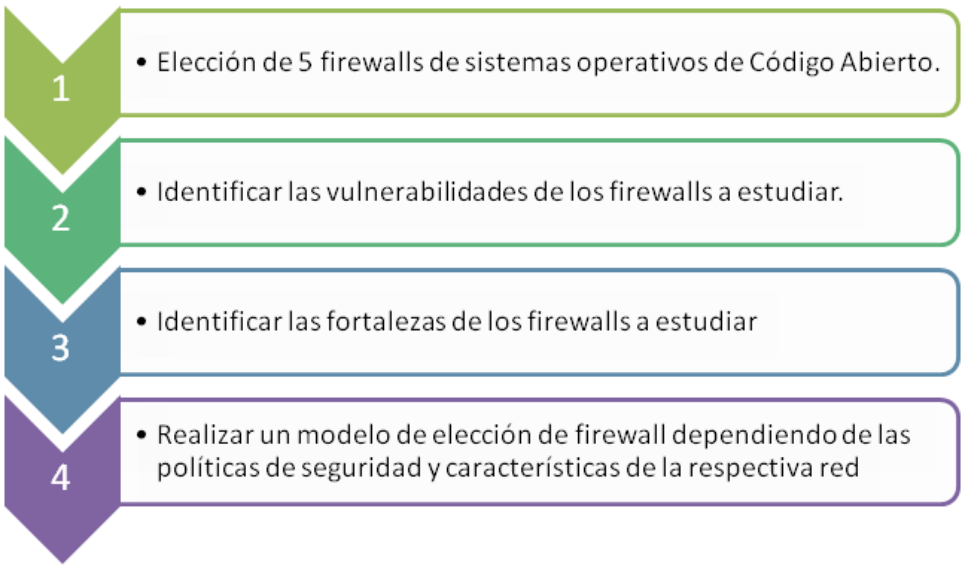


Figura 9: Metodología de Elección del Firewall

La primera fase de esta investigación arrojó como resultado los 5 firewalls a estudiar los cuales se muestran en la *Tabla 10*:

NOMBRE	PLATAFORMA
IPTABLES	LINUX
IPFILTER	FreeBSD, HP-UX, OpenBSD, Dragon FlyBSD, NetBSD
PACKET FILTER (PF)	NetBSD, OpenBSD, FreeBSD, Dragon FlyBSD
IPFIREWALL (IPFW)	FreeBSD, Dragon FlyBSD
NETDEFENDER	Windows2000 – WindowsXP

Tabla 10:Firewalls a estudiar en tesis: "Análisis de Vulnerabilides y Fortalezas en 5 firewalls de plataforma libre"

En la segunda fase de esta investigación, se recopiló, de bases de datos existentes en Internet: MITRE Common Vulnerabilities and Exposures (CVE), X-Force, SecurityFocus y Secunia las vulnerabilidades de los firewalls a estudiar; el resultado se muestra en la *Tabla 11*:

Firewall	Número de Vulnerabilidades	Valor total de riesgo
IPTABLES	11	45,35
IPFILTER	5	22,6
PACKET FILTER	8	34,5
IPFIREWALL	5	14,9
NETDEFENDER	9	36

Tabla 11:Número de Vulnerabilidades encontradas en la tesis: "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"

La casilla “Valor de Riesgo” Representa el daño potencial que tiene cada vulnerabilidad, para esta investigación se maneja una escala de 1 a 5:

- Bajo Riesgo = 1
- Riesgo Potencial = 2
- Riesgo Moderado = 3
- Riesgo Significante = 4
- Alto Riesgo = 5

Sabiendo que muchas de las vulnerabilidades encontradas en las bases de datos hoy día presentan algún tipo de solución ya sea a través de parches y/o actualizaciones, se hizo el mismo análisis teniendo en cuenta este criterio se obtuvo los resultados de la *Tabla 12*:

Firewall	Número de Vulnerabilidades	Valor total de riesgo
IPTABLES	0	0
IPFILTER	3	14
PACKET FILTER	2	9,7
IPFIREWALL	0	0
NETDEFENDER	9	36

Tabla 12: Vulnerabilidades con actualización de los firewall a estudiar en la tesis"Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"

La tercera fase de esta investigación, correspondiente a la identificación de fortalezas de los firewalls seleccionados, se presenta en la *Tabla 13*

Firewall	Número de Fortalezas	Valor total de eficacia
IPTABLES	10	34,2
IPFILTER	7	24
PACKET FILTER	4	10,4
IPFIREWALL	10	36,3
NETDEFENDER	1	1,4

Tabla 13: Número de Fortalezas encontradas en la tesis: "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"

La tercera columna de la Tabla 13 muestra el valor total de eficacia, este valor se obtiene primero sacando el valor de eficacia de cada fortaleza que es la suma del resultado de la calificación de las tres variables para evaluar una fortaleza (Capacidad para evitar ataques (60%) + Nivel de innovación de la tecnología (30%) + Facilidad de uso (10%)), luego de tener este valor para cada fortaleza se

suma con las demás fortalezas para cada firewall y así se da con el resultado obtenido en la Tabla 13.

Teniendo en cuenta una de las variables establecidas para esta investigación, la Variable de Cercanía, la cual define qué porcentaje se acerca un punto del otro; por ejemplo: ¿Qué tanto se acerca o qué porcentaje es 75,8 de 87,4?; la solución es presentada en la *(4)*

$$X = \frac{(75{,}8 * 100)}{87{,}4} = 86{,}72\% \quad (4)$$

Se obtienen los resultados presentados en las Tablas 14 a 17:

- ***VULNERABILIDADES***

Los primeros resultados teniendo en cuenta la variable de cercanía anteriormente explicada, corresponden a cuánto se acerca el puntaje obtenido de cada firewall en sus vulnerabilidades al peor de los casos y es presentado en la *Tabla 14*:

Puesto	Firewall	Real	Peor	Valor % Peor	Puntos por Posición
1	IpFirewall	14,9	25	59,60%	5
2	NetDefender	36	45	80,00%	4
3	IpTables	45,35	55	82,45%	3
4	IpFilter	34,5	40	86,25%	2
5	Packet Filter	22,6	25	90,40%	1

Tabla 14: Valores de cercanía vulnerabilidades, peor caso, Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"

Los valores correspondientes a cuánto se acerca el puntaje obtenido para cada uno de los firewalls en sus vulnerabilidades, al mejor de los casos es presentado en la *Tabla 15*:

Puesto	Firewall	Real	Peor	Valor % (Mejor)	Puntos por Posición
1	IpFirewall	14,9	5	33,55%	5
2	NetDefender	36	9	25,00%	4
3	IpTables	45,35	11	24,25%	3
4	IpFilter	34,5	8	23,18%	2
5	Packet Filter	22,6	5	22,12%	1

Tabla 15: Valores de cercanía vulnerabilidades, mejor caso, Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"

- ***FORTALEZAS***

Los valores correspondientes a cuánto se acerca el puntaje obtenido para cada uno de los firewalls en sus fortalezas, al peor de los casos es presentado en la *Tabla 16*:

Puesto	Firewall	Real	Peor	Valor % (Peor)	Puntos por Posición
1	IpFirewall	36,3	10	27,54%	5
2	Packet Filter	24	7	29,16%	4
3	IpTables	34,2	10	29,24%	3
4	IpFilter	10,4	4	38,46%	2
5	NetDefender	1,4	1	71,42%	1

Tabla 16: Valores de cercanía fortalezas, peor caso, Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"

Los valores correspondientes a cuánto se acerca el puntaje obtenido para cada uno de los firewalls en sus fortalezas, al mejor de los casos es presentado en la *Tabla 17*:

Puesto	Firewall	Real	Peor	Valor % (Mejor)	Puntos por Posición
1	IpFirewall	36,3	0	72,60%	5
2	Packet Filter	24	0	68,57%	4
3	IpTables	34,2	9	68,40%	3
4	IpFilter	10,4	3	52,00%	2
5	NetDefender	1,4	2	28,00%	1

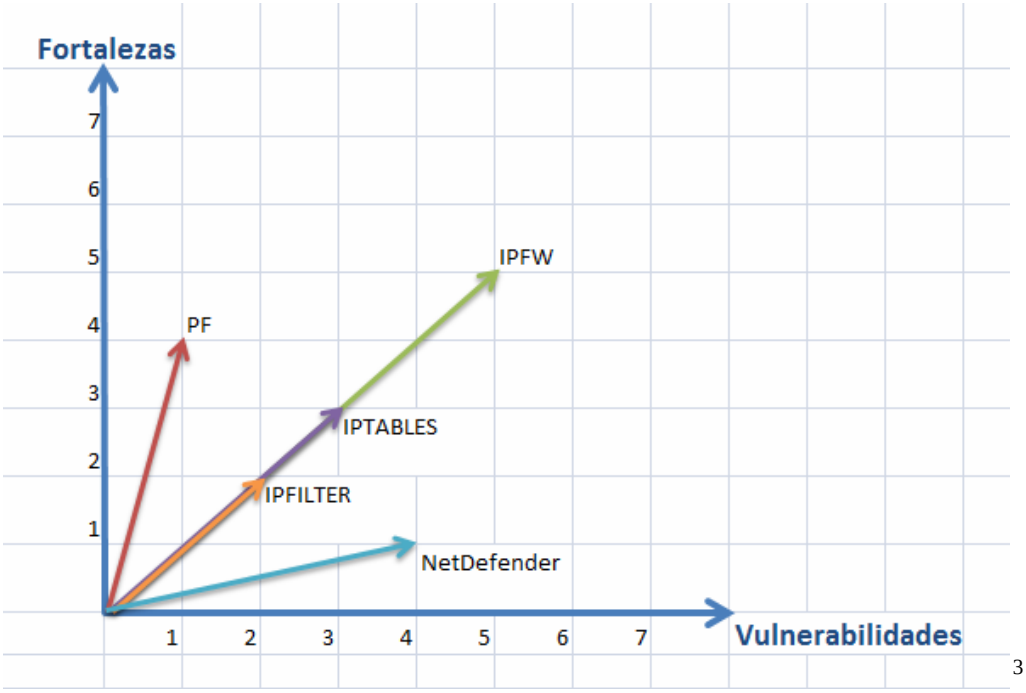
Tabla 17: Valores de cercanía fortalezas, mejor caso, Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"

Luego de obtener los puntos por posición para cada firewall, tanto para sus vulnerabilidades como para sus fortalezas se relacionan teniendo en cuenta que dichos puntos por posición se pueden considerar como ortogonales, por lo tanto se realizó un análisis vectorial, como lo indica la *Tabla 18*:

Firewall	Ptos Vulnerabilidades	Ptos Fortalezas	Vector	Magnitud	Ángulo (α)
IpFirewall	5	5	5V+5F	5	45°
IpTables	3	3	3V+3F	4	45°
Packet Filter	1	4	1V+4F	3	75°
NetDefender	4	1	4V+1F	2	14°
IpFilter	2	2	2V+2F	1	45°

Tabla 18: Valores de puntos por posición y vectores Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"

Gráficamente se obtiene lo mostrado en la *Figura 10*:



[3]

Figura 10: Vectores de Confiabilidad Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre"

De la investigación llevada a cabo, el firewall que obtuvo la mejor posición respecto de sus fortalezas y vulnerabilidades fue: IPFW, siendo este el firewall a implementar no solo por su nivel de seguridad, si no por permitir la implementación de las tres zonas a trabajar (MZ, DMZ y WAN) y por ser adecuado para implementar en medianas y grandes empresas.

[3] Tomada de la Tesis: Tesis: : "Análisis de Vulnerabilidades y Fortalezas en 5 FIrewalls de plataforma libre" año 2008 por Ricardo Pertuz de las Casas

3.4.5. Diseño e implementación

En esta parte de la investigación, se tienen en cuenta las arquitecturas seleccionadas junto con el firewall, para realizar los diseños de red correspondientes.

El primer escenario de red a implementar, tomado como Escenario 0, es el presentado en la *Figura 11*:

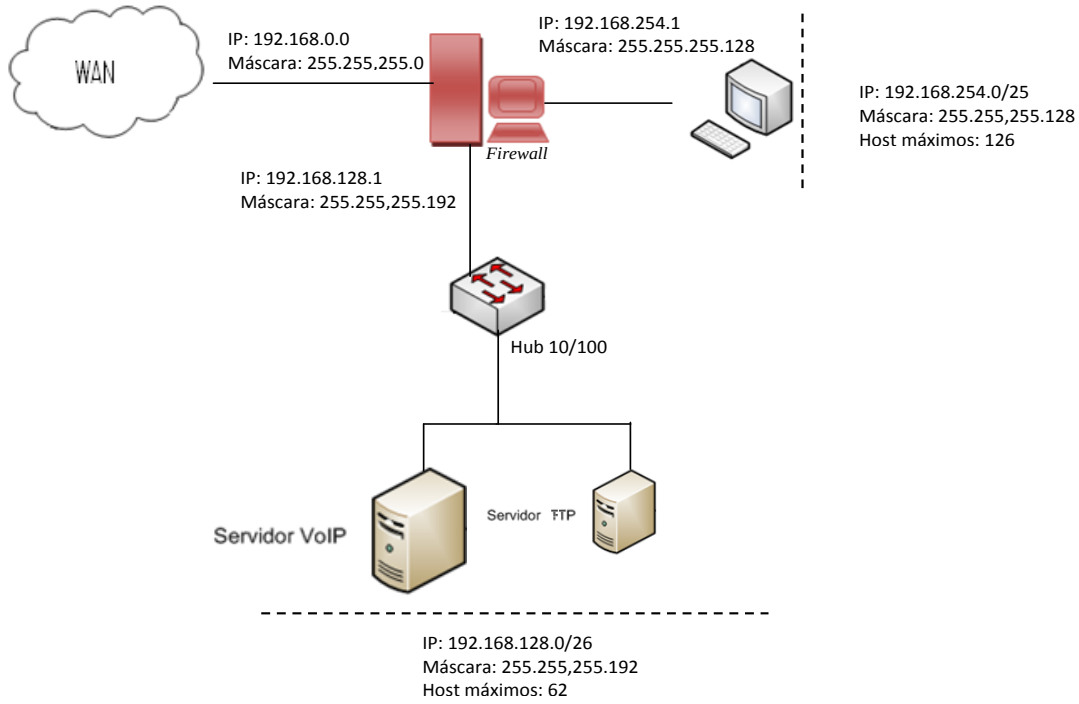


Figura 11: Diseño de red "Escenario 0"

Este escenario, tomado como Escenario 0, se implementa con el fin de identificar la influencia del IPFW en la red, y de esta forma descartar que esta influencia sea inherente a la arquitectura a evaluar; las especificaciones técnicas de los equipos de este escenario se muestran en la *Tabla 19*:

DISPOSITIVO	ESPECIFICACIONES TÉCNICAS
IPFirewall	AMD Sempron 1,99GHz, Disco duro de 160GB Memoria RAM de 2GB
Cliente LAN	AMD Turion 2,21GHz, Disco Duro de 120GB, Memoria RAM de 1GB
Hub	Hub Catalyst 10/100
Servidor Asterisk VOIP	Celeron 500 MHz, 254MB de RAM, Disco Duro de 20GB
Servidor FTP	AMD Turion 2,21GHz,Disco Duro de 120GB, Memoria RAM de 1GB
Cliente WAN	Intel Pentium Dual Core de 1,73GHz, Disco Duro de 160GB, Memoria RAM de 3GB.

Tabla 19: Especificaciones Técnicas Equipos de red, Escenario0

El direccionamiento utilizado para este escenario se presenta en la *Tabla 20*:

ZONA	RANGO DE DIRECCIONES IP	Número Máximo de Clientes
Zona de Servidores	192.168.128.0/26	60
Clientes LAN	192.168.254.0/25	124
Zona WAN	192.168.0.0/24	254

Tabla 20: Direccionamiento Escenario 0

El segundo escenario de red a implementar corresponde a la primera arquitectura de firewall seleccionada: “Screened Subnet”; el diseño de red es el presentado en la *Figura 12*:

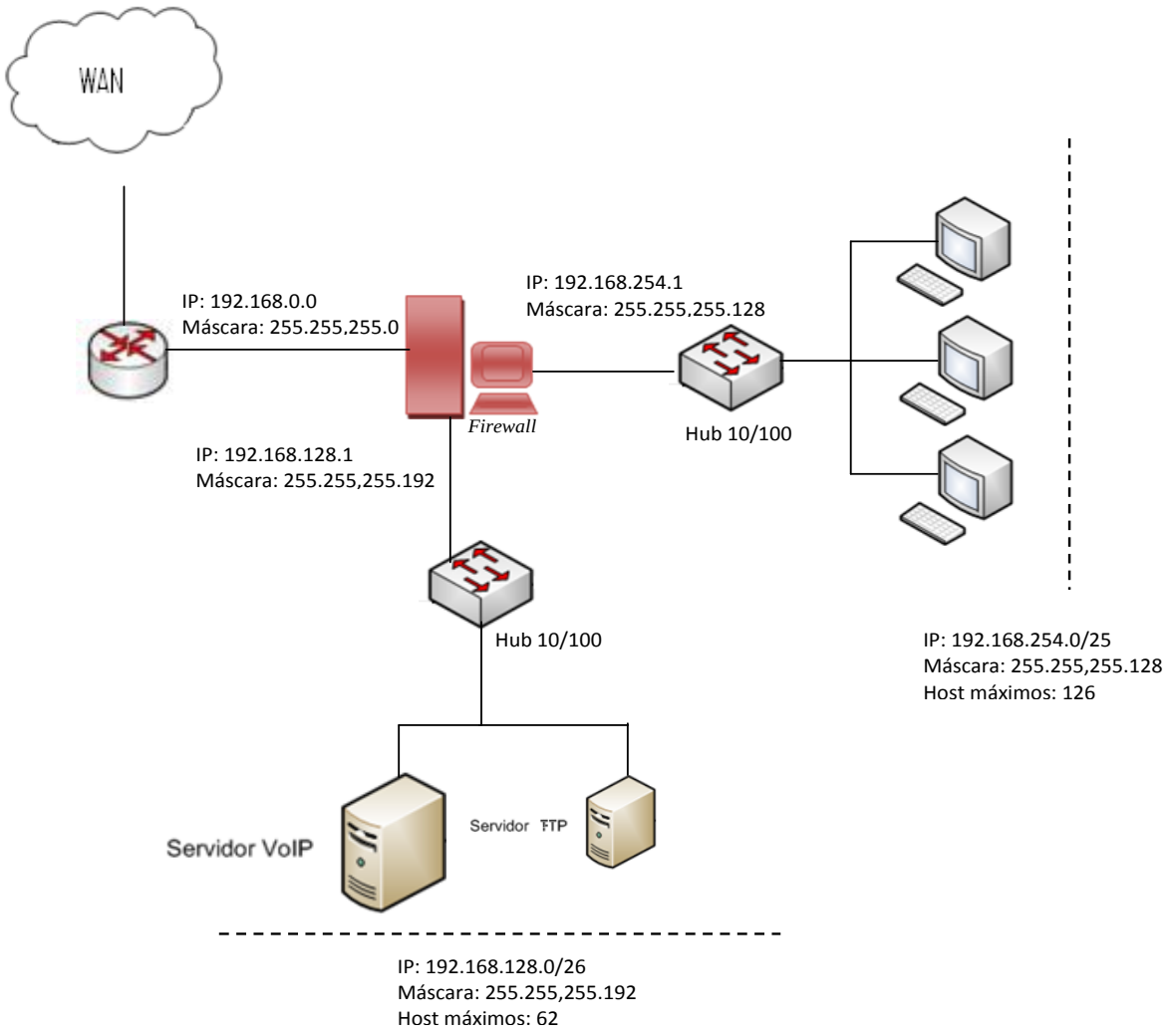


Figura 12: Diseño de red de Screened Subnet

Este segundo escenario, como se puede observar en la *Figura 12*, consta de un router, con dos interfaces de red una conectada hacia la WAN y la otra al Firewall; el IPFW con tres interfaces de red, una conectada a la zona de servidores, tomada para este escenario como la DMZ, la es conformada por un servidor Asterisk y un servidor FTP; otra interfaz de red conectad al router, y la última de estas conectada a la LAN. El enlace LAN se configuró con un ancho de banda de

100Mbps para efectos de pruebas. Para el direccionamiento se utilizó Subneteo de redes.

Las especificaciones técnicas de los equipos se presentan en la *Tabla 21*:

DISPOSITIVO	ESPECIFICACIONES TÉCNICAS
IPFirewall	AMD Sempron 1,99GHz, Disco duro de 160GB Memoria RAM de 2GB
Cliente LAN	AMD Turion 2,21GHz, Disco Duro de 120GB, Memoria RAM de 1GB
Hub	Hub Catalyst 10/100
Servidor Asterisk VOIP	Celeron 500 MHz, 254MB de RAM, Disco Duro de 20GB
Servidor FTP	AMD Turion 2,21GHz,Disco Duro de 120GB, Memoria RAM de 1GB
Cliente WAN	Intel Pentium Dual Core de 1,73GHz, Disco Duro de 160GB, Memoria RAM de 3GB.

Tabla 21: Especificaciones técnicas dispositivos de red Dual Firewall

El direccionamiento de este escenario es el presentado en la *Tabla 22*:

ZONA	RANGO DE DIRECCIONES IP	Número Máximo de Clientes
Zona de Servidores	192.168.128.0/26	60
Clientes LAN	192.168.254.0/25	124
Zona WAN	192.168.0.0/24	254

Tabla 22: Direccionamiento "Screned Subnet"

El tercer escenario de red corresponde a la arquitectura de red segura bajo el nombre “Dual Firewall” y se muestra en la *Figura 13*:

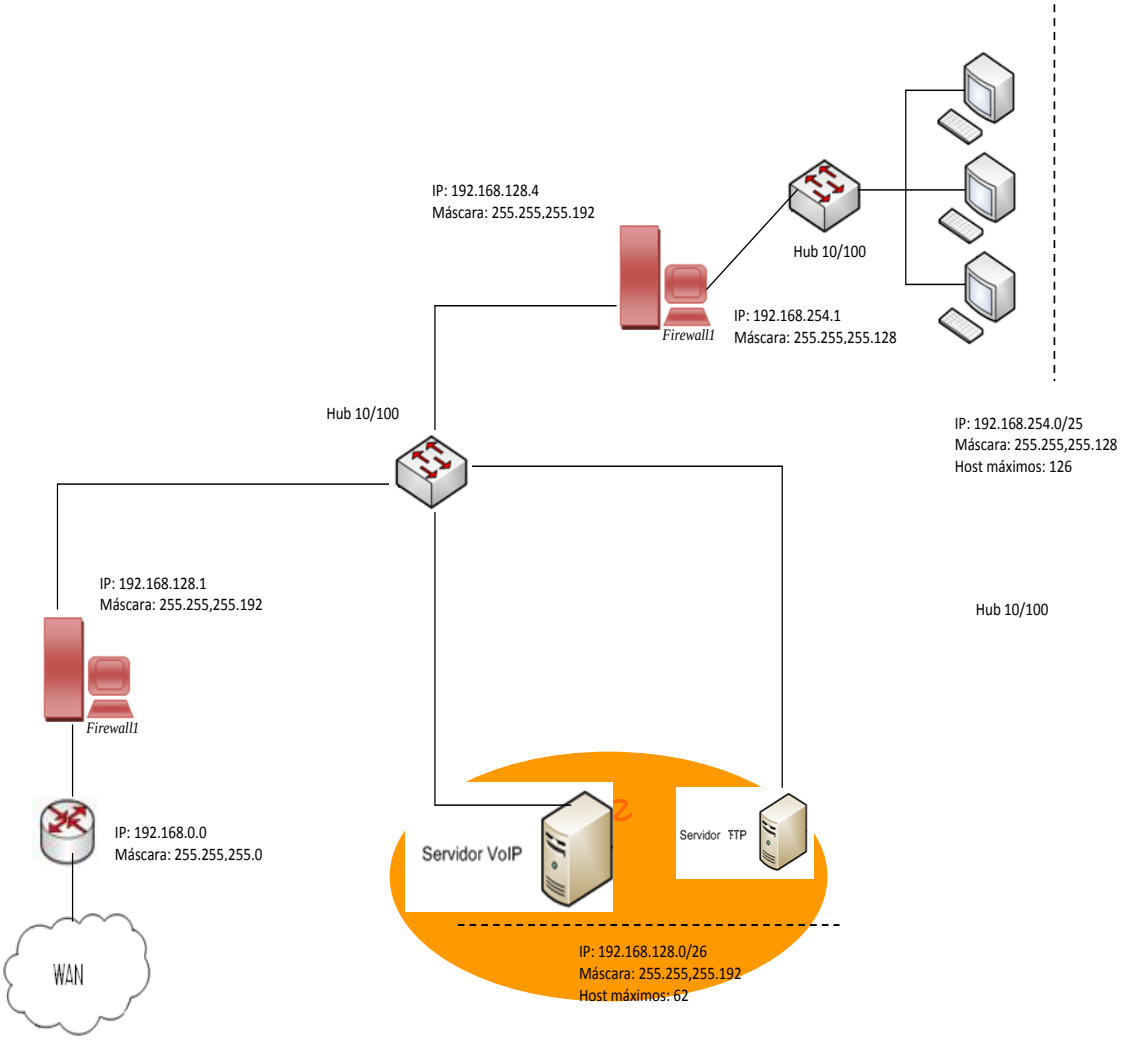


Figura 13: Diseño de red Dual Firewall

Este tercer escenario, como se puede observar, consta de Dos Firewalls, cada uno con dos tarjetas de red; el primero de ellos conectado por una de sus tarjetas a la WAN y por la otra a la zona de servidores (DMZ); el segundo firewall, llamado también firewall interno, está conectado por una de sus tarjetas a la zona de servidores (DMZ) y por la otra a la LAN.

Las especificaciones técnicas de los equipos que conforman este escenario se presentan en la *Tabla 23*:

DISPOSITIVO	ESPECIFICACIONES TÉCNICAS
IPFirewall Externo	AMD Sempron 1,99GHz, Disco duro de 160GB Memoria RAM de 2GB
IPFirewall Interno	AMD Sempron 1,99GHz, Disco duro de 160GB Memoria RAM de 2GB
Cliente LAN	AMD Turion 2,21GHz, Disco Duro de 120GB, Memoria RAM de 1GB
Hub	Hub Catalyst 10/100
Servidor Asterisk VOIP	Celeron 500 MHz, 254MB de RAM, Disco Duro de 20GB
Servidor FTP	AMD Turion 2,21GHz,Disco Duro de 120GB, Memoria RAM de 1GB
Cliente WAN	Intel Pentium Dual Core de 1,73GHz, Disco Duro de 160GB, Memoria RAM de 3GB.

Tabla 23: Especificaciones técnicas equipos "Dual Firewall"

El direccionamiento es presentado en la *Tabla 24*:

ZONA	RANGO DE DIRECCIONES IP	Número Máximo de Clientes
Zona de Servidores	192.168.128.0/26	60
Clientes LAN	192.168.254.0/25	124
Zona WAN	192.168.0.0/24	254

Tabla 24: Direccionamiento "Dual Firewall"

El último escenario a implementar corresponde a la tercera arquitectura seleccionada, bajo el nombre “Dual firewall, Dual DMZ” y es presentado en la *Figura 14*:

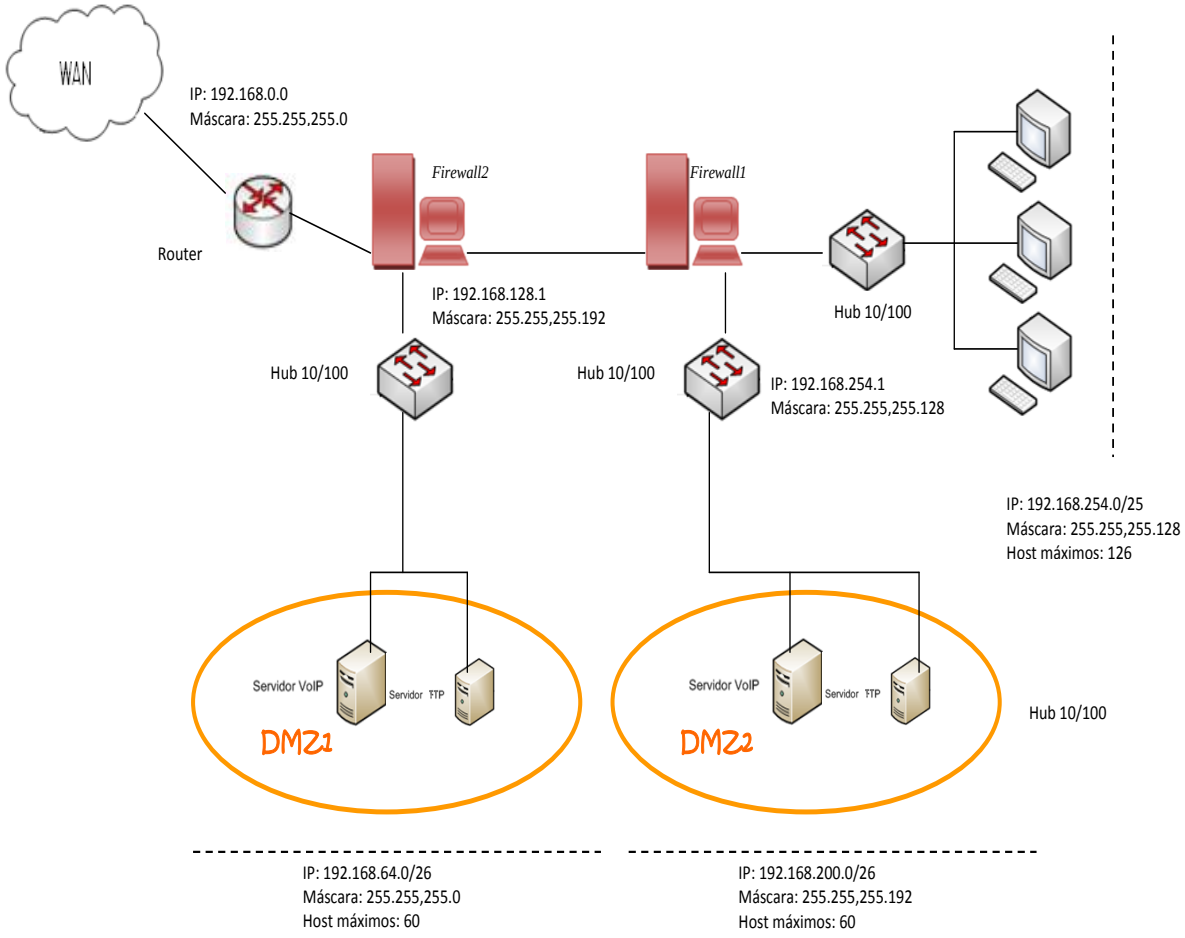


Figura 14: Diseño de red "Dual Firewall, Dual DMZ"

Este último escenario, está conformado por Dos Firewalls, al igual que el escenario anterior, pero la diferencia radica en que cada uno de estos tienen 3 tarjetas de red; el Firewall externo tiene su primer tarjeta conectada a la WAN, la segunda de ellas a la primera zona de servidores (DMZ1), llamada Zona de Servidores Externos y la última de estas al firewall interno; este firewall interno tiene su primera tarjeta de red conectada al Firewall externo, la segunda tarjeta

conectada a la segunda zona de servidores (DMZ2), llamada también Zona de Servidores Internos y la última de sus tarjetas de red, es conectada a la LAN.

Las especificaciones técnicas de los equipos que conforman este escenario se presentan en la *Tabla 25*:

DISPOSITIVO	ESPECIFICACIONES TÉCNICAS
IPFirewall Externo	AMD Sempron 1,99GHz, Disco duro de 160GB Memoria RAM de 2GB
IPFirewall Interno	AMD Sempron 1,99GHz, Disco duro de 160GB Memoria RAM de 2GB
Cliente LAN	AMD Turion 2,21GHz, Disco Duro de 120GB, Memoria RAM de 1GB
Hub	Hub Catalyst 10/100
Servidor Asterisk VOIP	Celeron 500 MHz, 254MB de RAM, Disco Duro de 20GB
Servidor FTP	AMD Turion 2,21GHz,Disco Duro de 120GB, Memoria RAM de 1GB
Cliente WAN	Intel Pentium Dual Core de 1,73GHz, Disco Duro de 160GB, Memoria RAM de 3GB.

Tabla 25: Especificaciones técnicas equipos "Dual Firewall, Dual DMZ"

El direccionamiento de la Arquitectura “Dual Firewall – Dual DMZ” para la ejecución de pruebas es presentado en la *Tabla 26*:

ZONA	RANGO DE DIRECCIONES IP	Número Máximo de Clientes
Zona de Servidores1	192.168.128.0/26	60
Zona de Servidores2	192.168.64.0/26	60
Clientes LAN	192.168.254.0/25	124
Zona WAN	192.168.0.0/24	254

Tabla 26: Direccionamiento "Dual Firewall, Dual DMZ"

La interconexión de los equipos, tanto terminales como Servidores, en todas y cada una de las arquitecturas fue realizada mediante cableado estructurado Categoría 5e, siguiendo la normatividad EIA/TIA-568B.

4. PRUEBAS Y ANÁLISIS DE RESULTADOS

En este capítulo de la Investigación se tratan en detalle las actividades llevadas a cabo con las que se obtienen los resultados que serán analizados a profundidad. A continuación se presentan las pruebas realizadas en las arquitecturas de redes seguras basadas en firewall seleccionadas, en donde se tomarán medidas de parámetros de rendimiento y calidad de servicio para los diferentes escenarios. El análisis de QoS se realizará sobre el flujo de datos que contiene la carga útil (paquetes de voz) y no sobre el de señalización.

4.1. PRUEBAS REALIZADAS

El conjunto de pruebas se divide en:

- Pruebas de Rendimiento: hacen referencia al uso del servidor FTP para descarga de archivos desde y hacia diferentes zonas de las arquitecturas; para este conjunto de pruebas, el servicio FTP dispone del 100% del canal, es decir, se está ejecutando como único servicio en la red; como resultado de la ejecución de este conjunto de pruebas se evalúa la variable Throughput.
- Pruebas de QoS: Para este conjunto de pruebas, se realizan llamadas de Voz sobre IP de 1 minuto,haciendo uso del Servidor Asterisk, desde y hacia diferentes zonas de las arquitecturas; al igual que para el anterior conjunto de pruebas, este servicio dispone del 100% del canal y como resultado se evalúa el Jitter y la Latencia del mismo.
- Pruebas de Rendimiento y QoS: En este conjunto de pruebas, los dos servicios nombrados en las pruebas anteriores, comparten el 100% del canal; para implementar QoS en la red, se asigna prioridad dependiendo del tipo de tráfico: 70% para Voz sobre IP y 30% para FTP. De igual forma se evalúa el

Throughput, la Latencia, el Jitter y como adicional la Pérdida de Paquetes generada por la ejecución de los servicios de manera simultánea.

4.1.1. Pruebas de Rendimiento de la red:

La ejecución de pruebas toma como punto de partida la descarga de Archivos contenidos en el servidor FTP hacia las diferentes zonas de la arquitectura a evaluar, ya que brinda la posibilidad de medir el rendimiento de la red; en esta prueba, se realizan 50 descargas de un archivo de tamaño 136MB, para de esta forma obtener un análisis estadístico acertado.

Cuando se efectúa la transferencia de datos a través de una red pública como es la de Internet, se está supeditado a las condiciones de la red de datos del ISP, las cuales son extremadamente variables y totalmente ajenas al desempeño de la arquitectura de Firewall utilizada. Sin embargo, sí se ven reflejadas y afectan de manera directa el desempeño de la red LAN cuando se establece una conexión con el exterior.

De manera que, en este orden de ideas, llevar a cabo el análisis de los datos obtenidos para la prueba de la Zona Militarizada hacia la WAN, implica tener en cuenta las extremadamente variantes condiciones externas a la red, y no es el caso de esta investigación.

No obstante, los resultados obtenidos en la transferencia interna de archivos con las Zonas Militarizadas y Desmilitarizadas, sí nos reflejan de manera directa la influencia de la arquitectura de firewall, en términos de velocidades de transferencia y tiempos de respuesta.

Uno de los puntos más importantes de análisis del desempeño de la red LAN con la implementación de las diferentes arquitecturas, está en el tiempo de transferencia de los archivos ya que con este se puede calcular fácilmente el Throughput de la misma.

- Descarga de archivo contenido en el servidor FTP en la Zona Desmilitarizada hacia la Zona Militarizada de la arquitectura:

En la *Figura 15*, se muestra el Throughput calculado haciendo uso del tiempo de transferencia del archivo de 136MB desde el servidor FTP interno ubicado en la Zona Desmilitarizada hacia la estación de trabajo de la Zona Militarizada de las diferentes arquitecturas:

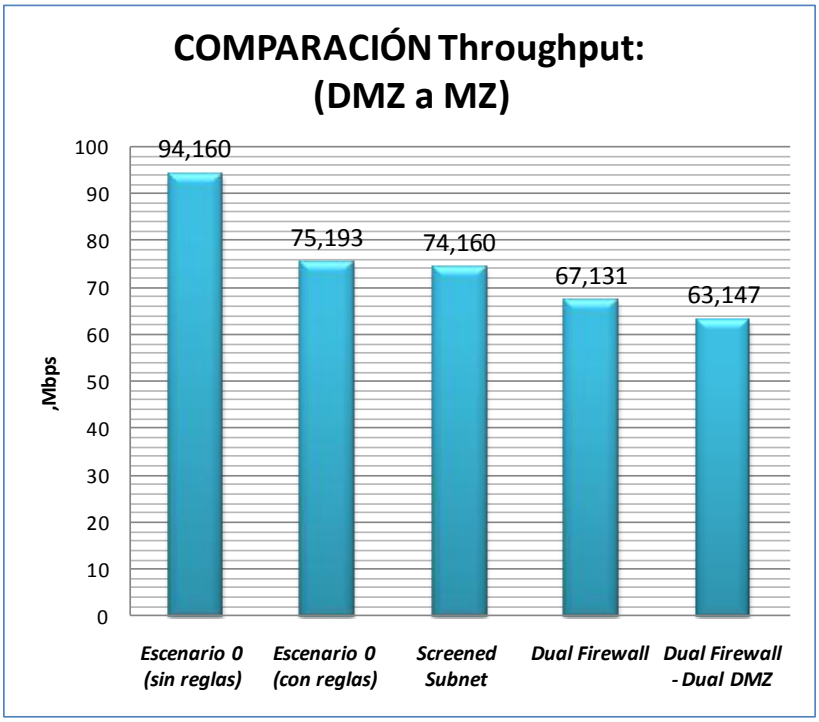


Figura 15: Comparación Throughput DMZ a MZ (Prueba de Rendimiento)

Como se puede observar en la *Figura 15*, el valor de Throughput sufre una baja tan solo implementando el IPFW en la red, es decir el Escenario 0, teniendo en cuenta que el ancho de banda de la red es de 100Mbps; ahora, tomando como 100% el valor de Throughput correspondiente al Escenario 0, se obtiene el porcentaje en que se baja el Throughput de la red (evaluado haciendo uso del servicio FTP) por la implementación de las diferentes arquitecturas; este porcentaje es presentado en la *Figura 16*:

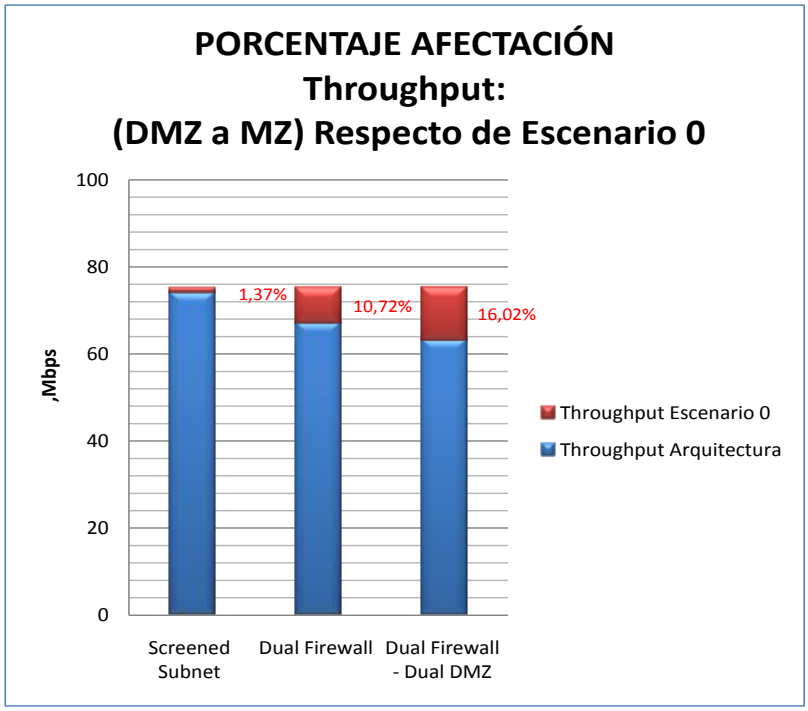


Figura 16: Porcentaje de afectación del Throughput DMZ a MZ (Pruebas de Rendimiento)

En la *Figura 16*, se puede observar cómo la arquitectura "Screened Subnet" como tal no ocasiona una baja considerable en el rendimiento de la red si se toma como referencia la prueba realizada con el Escenario 0. Es decir, para este caso la baja en el rendimiento de la arquitectura es de tan solo el 1,37%; este resultado era de esperarse, ya que esta arquitectura no añade gran cantidad de equipos a la red, y las reglas implementadas en el firewall coinciden con las del Escenario 0.

Por otra parte, se puede observar cómo la Arquitectura "Dual Firewall", si afecta en un porcentaje considerable el rendimiento de la red obtenido mediante el Throughput; este valor correspondiente al 10,72% del Escenario es resultado de un aumento en el porcentaje de reglas de filtrado para estas dos zonas respecto al Escenario 0 por el incremento de equipos involucrados en la seguridad.

De igual manera ocurre con la Arquitectura "Dual Firewall – Dual DMZ" la cual afecta el rendimiento de la red por involucrar más líneas de defensa en la seguridad de la misma y por ende mayor número de reglas de filtrado.

- Descarga del archivo contenido en el servidor FTP en la Zona Desmilitarizada de la arquitectura hacia la WAN:

En la *Figura 17*, se muestra el Throughput calculado haciendo uso del tiempo de transferencia del archivo de 136MB desde el servidor FTP interno ubicado en la Zona Desmilitarizada de las diferentes arquitecturas hacia la WAN:

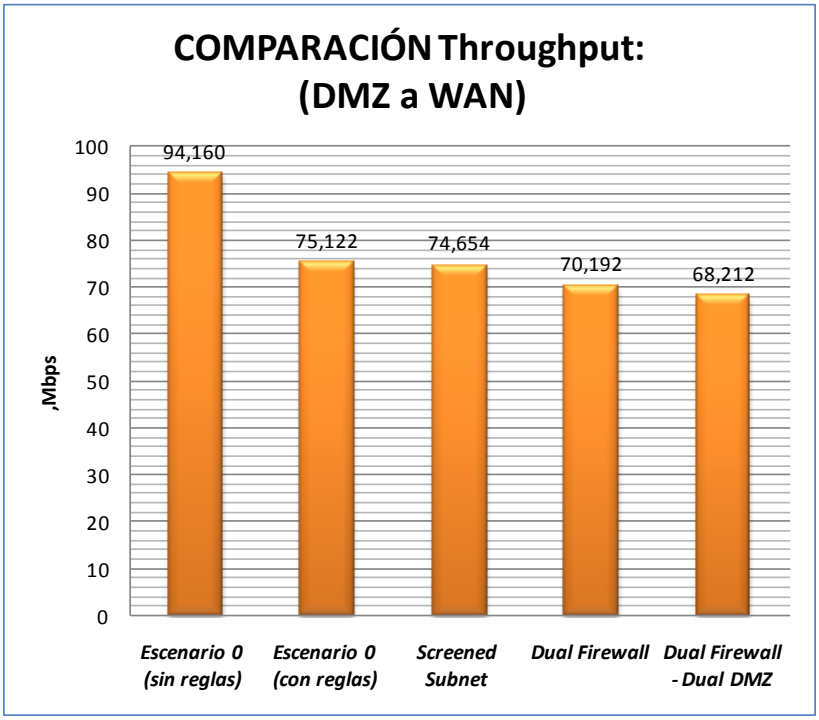


Figura 17: Comparación Throughput DMZ a WAN (Prueba de Rendimiento)

Nuevamente la Arquitectura Screened Subnet presenta la menor baja de Throughput respecto del Escenario 0, y la Arquitectura Dual Firewall – Dual DMZ la mayor afectación del Throughput; pero en esta prueba, cabe resaltar que el porcentaje de afectación del Throughput de todas y cada una de las arquitecturas es menor respecto del observado en la prueba anterior; tomando como referencia el Escenario 0; esto se ve claramente en la *Figura 18*:

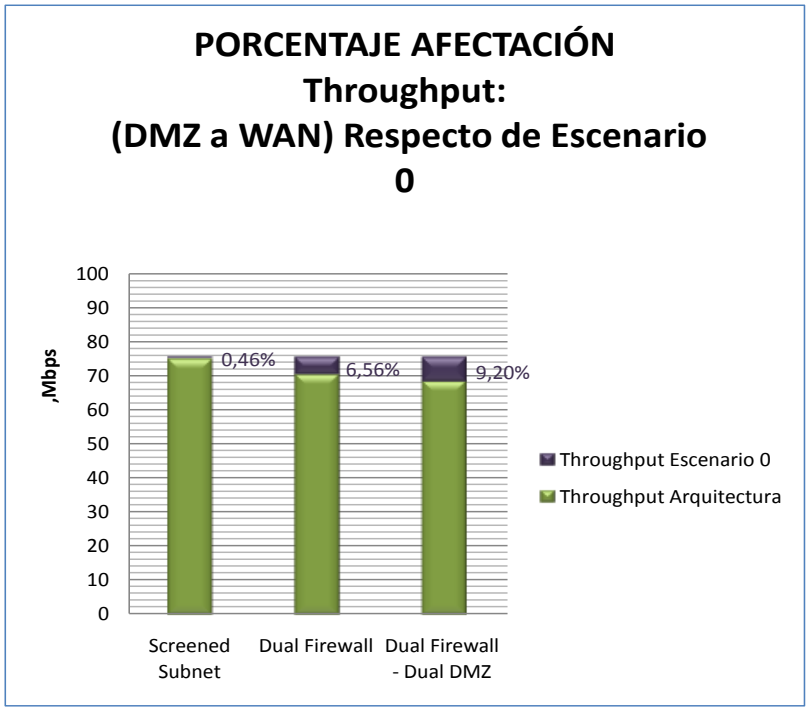


Figura 18: Porcentaje de afectación del Throughput DMZ a WAN (Pruebas de Rendimiento)

En esta figura se puede observar, cómo los porcentajes de afectación del Throughput en las arquitecturas "Dual Firewall" y "Dual Firewall – Dual DMZ" son menores respectos de los observados para la descarga de la Zona Desmilitarizada hacia la Zona Militarizada, tomando como referencia el Escenario 0, esto debido a que en este segmento de red se tiene un menor número de reglas de filtrado implementadas; para el caso de la arquitectura "Screened Subnet" no se reduce el número de reglas de filtrado por tener un solo firewall involucrado en la seguridad de la red, así que el porcentaje de afectación para estas dos pruebas, resulta ser idéntico.

- Descarga del archivo contenido en el servidor FTP en la WAN hacia la Zona Militarizada de la arquitectura.

En la *Figura 19*, se muestra el Throughput calculado haciendo uso del tiempo de transferencia del archivo de 136MB desde el servidor FTP interno ubicado en la WAN hacia la Zona Militarizada de las diferentes arquitecturas:

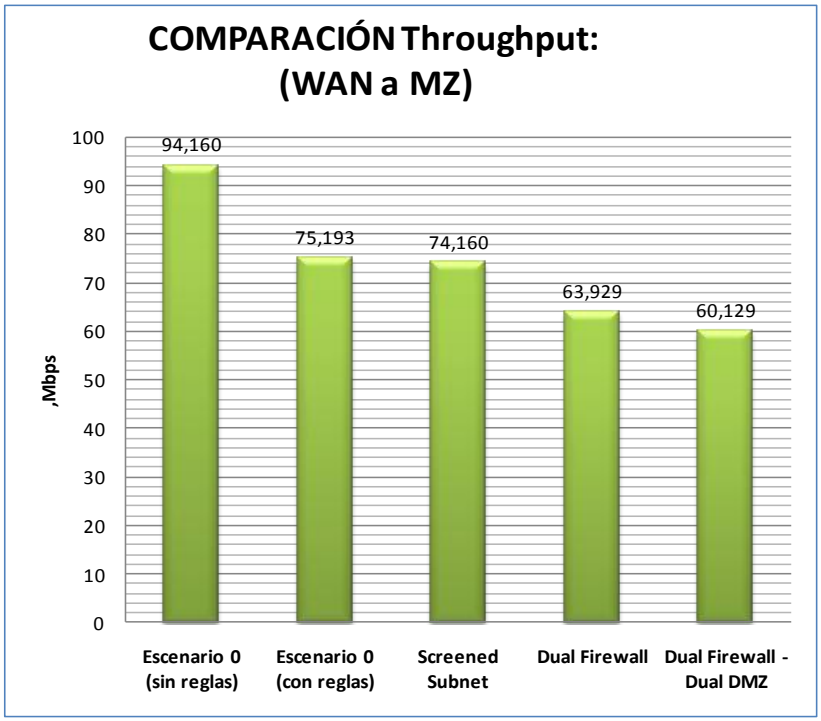


Figura 19: Comparación Throughput WAN a MZ (Prueba de Rendimiento)

Finalmente se presenta la descarga del Archivo de extremo a extremo (WAN a Zona Militarizada) de cada arquitectura; se puede observar cómo la Arquitectura que menor afecta el Rendimiento de la red es “Screened Subnet”, debido a que la seguridad que brinda es menor respecto de las otras dos arquitecturas, las cuales afectan en mayor porcentaje el rendimiento de la red; el porcentaje de afectación de cada una de ellas es presentada en la *Figura 20*:

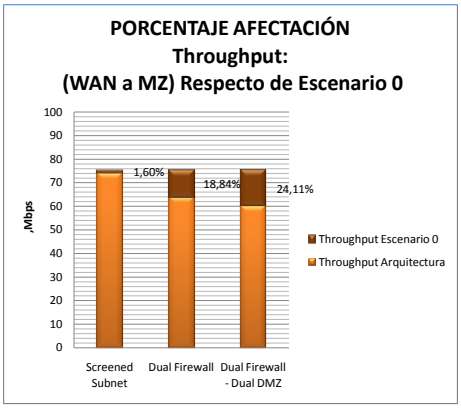


Figura 20: Porcentaje de afectación del Throughput WAN a MZ (Pruebas de Rendimiento)

En esta figura podemos observar cómo la arquitectura que más afecta el rendimiento de la red es Dual Firewall – Dual DMZ, en segundo lugar aparece "Dual Firewall" con tan solo el 6,38% menos de afectación del Throughput; los porcentajes de baja del rendimiento de estas dos arquitecturas corresponden a que el tráfico tiene que pasar por dos firewalls antes de llegar al destino, situación que no ocurre con la arquitectura "Screened Subnet" la cual solo dispone de una línea de seguridad y por ende el porcentaje de afectación del rendimiento es menor: 17,6% menos que para "Dual Firewall" y 23,98% menos que para la arquitectura "Dual Firewall – Dual DMZ".

4.1.2. Pruebas de QoS: Llamada de 1 minuto desde y hacia diferentes zonas del firewall

En este conjunto de pruebas, se realiza la evaluación de parámetros de QoS mediante la realización de llamadas de Voz sobre IP haciendo uso del servidor Asterisk. El protocolo de VoIP, sobre el cual se realizan las pruebas para las

diferentes arquitecturas, es el protocolo RTP. Las pruebas efectúan según lo planteado en el anterior capitulo, donde los escenarios se muestran en las figuras *11,12, 13 y 14*, sobre los cuales se realizan 50 pruebas, con las cuales se realiza un estudio estadístico para mostrar sus resultados en cuanto a Latencia, Jitter y pérdida de paquetes durante la llamada.

Todas las pruebas realizadas en los diferentes escenarios, se encuentran adjuntas en el Anexo A, donde se puede apreciar principalmente el retardo y el jitter durante una llamada, a continuación se detalla cada aspecto de la calidad de servicio en VoIP, realizando comparaciones entre las diferentes arquitecturas:

4.1.2.1. RESULTADOS LATENCIA

El análisis de los resultados de QoS en las diferentes arquitecturas se realiza promediando los resultados obtenidos en las 50 pruebas por arquitectura, como se explicaba anteriormente, en donde las capturas son realizadas con el analizador de protocolos Wireshark. En un principio se analiza el retardo que se da en el emisor, el cual se evalúa en las dos vías, tanto de ida como de vuelta; estas 50 pruebas corresponden a llamadas de 1 minuto desde y hacia diferentes zonas de la arquitectura a evaluar:

- Llamada desde la Zona Militarizada hacia la Zona Desmilitarizada de la arquitectura:

En la *Figura 21* se muestra los resultados de Latencia para la llamada realizada entre estas dos zonas:

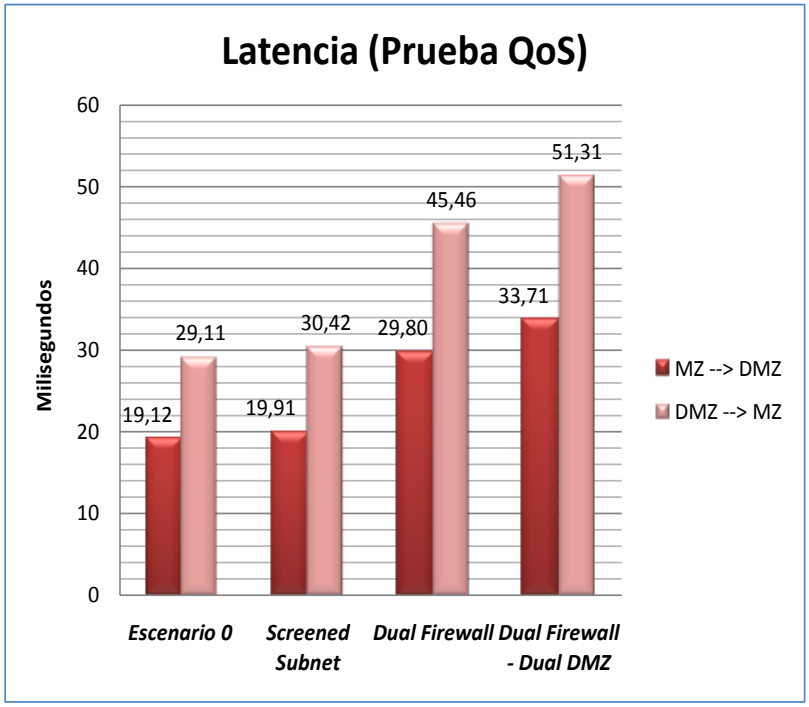


Figura 21: Latencia MZ a DMZ (Prueba de QoS)

Se puede apreciar claramente que “Dual Firewall” y “Dual Firewall – Dual DMZ” son las arquitecturas que más afectan la latencia en la red. Ambas arquitecturas brindan un alto grado de seguridad, por lo que se puede deducir que el incremento en la seguridad de la red altera de manera significativa el retardo entre los paquetes de Voz sobre IP.

Igualmente se observa que las tres arquitecturas tiene un comportamiento similar en cuanto a la latencia, en todos los casos se puede apreciar que la latencia de DMZ a MZ (Servidor→ Cliente) es mayor. .Además de esto la diferencia de retardos de ida y de vuelta de igual forma también se comporta de manera similar.

Para realizar una comparación entre los valores de latencia de las diferentes arquitecturas respecto del Escenario 0, se presenta la *Figura 22* en la que se que presentan los porcentajes de afectación de las diferentes arquitecturas de MZ hacia DMZ y viceversa:

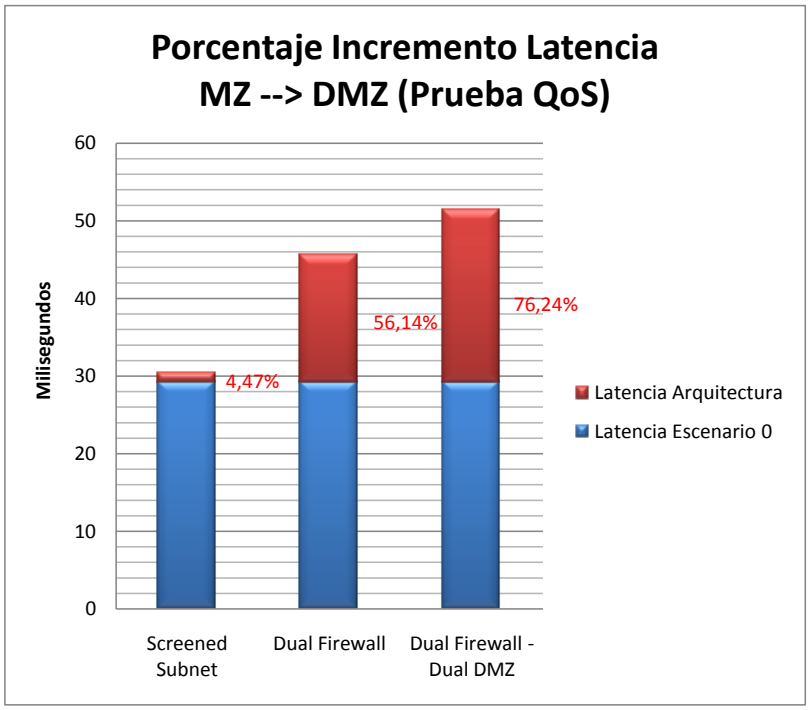


Figura 22: Porcentaje de incremento Latencia MZ a DMZ (Prueba QoS)

En esta figura se puede observar cómo el incremento de Latencia para todas y cada una de las arquitecturas es similar; es decir, el porcentaje de incremento de la Latencia desde la Zona Desmilitarizada hacia la Zona Militarizada y viceversa es el mismo para cada una de ellas; pero respecto del Escenario 0, se observa un incremento mayor de Latencia para la arquitectura que brinda mayor seguridad, la cual es “Dual Firewall – Dual DMZ” y de igual forma un menor incremento de Latencia para la arquitectura de menor seguridad: “Screened Subnet”.

- Llamada desde la WAN hacia la Zona Desmilitarizada de la arquitectura:

En la *Figura 23* se muestra los resultados de Latencia para estas dos zonas:

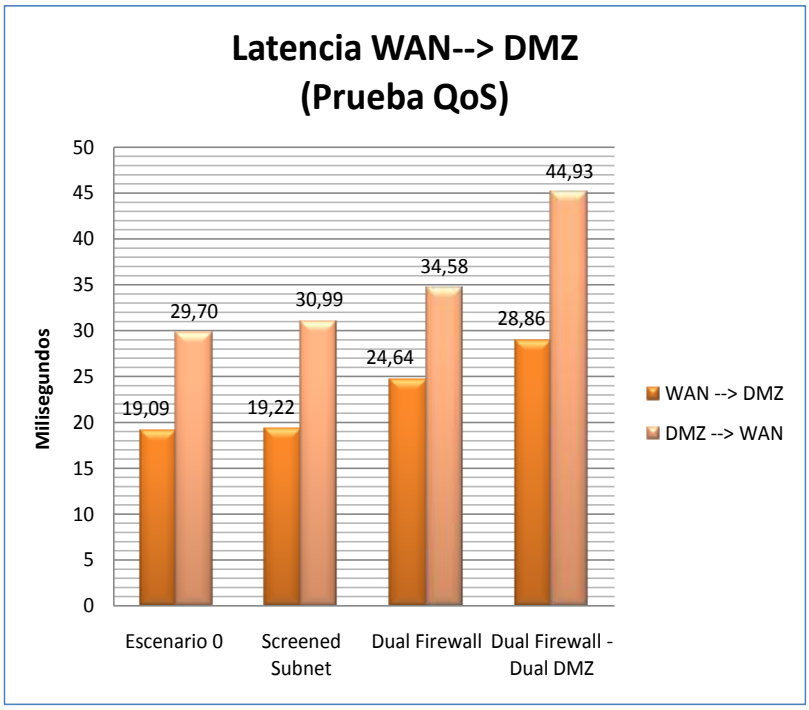


Figura 23: Latencia WAN a DMZ (Prueba de QoS)

En esta figura se puede observar un comportamiento similar respecto de la prueba realizada desde la Zona Militarizada hacia la Zona Desmilitarizada; nuevamente el mayor incremento de Latencia es para la arquitectura “Dual Firewall – Dual DMZ”, y el menor para la arquitectura “Screened Subnet”, todo esto, respecto del Escenario 0; pero para este conjunto de pruebas cabe resaltar que el incremento en la Latencia es menor respecto de la prueba anterior, esto dado por un número de reglas de filtrado menor, presentes para estas dos zonas; en la *Figura 24* se observa el incremento para cada una de las arquitecturas:

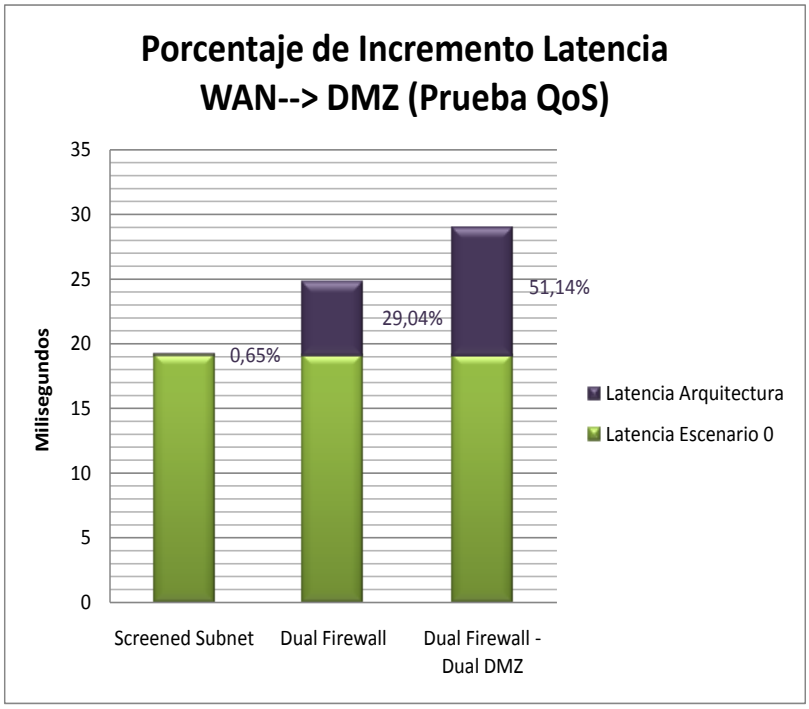


Figura 24: Porcentaje de incremento Latencia WAN a DMZ (Prueba QoS)

Como se decía anteriormente, el incremento de Latencia para las arquitecturas "Dual Firewall" y "Dual Firewall – Dual DMZ" es menor respecto de la prueba anterior; esto debido a que el Firewall involucrado en el control de tráfico de estas dos zonas, que es el Firewall exterior tiene un menor número de reglas de filtrado que el firewall interior, el cual fue usado en la prueba anterior.

- Llamada desde la Zona Militarizada de la arquitectura hacia la WAN.

Finalmente se presenta la llamada de extremo a extremo de cada una de las arquitecturas; nuevamente es "Dual Firewall – Dual DMZ" la que mayor incremento tiene respecto del Escenario 0 y "Screened Subnet" la que menos retardo entre los paquetes de Voz sobre IP ocasiona.

En la *Figura 25* se muestra los resultados de Latencia para estas dos zonas:

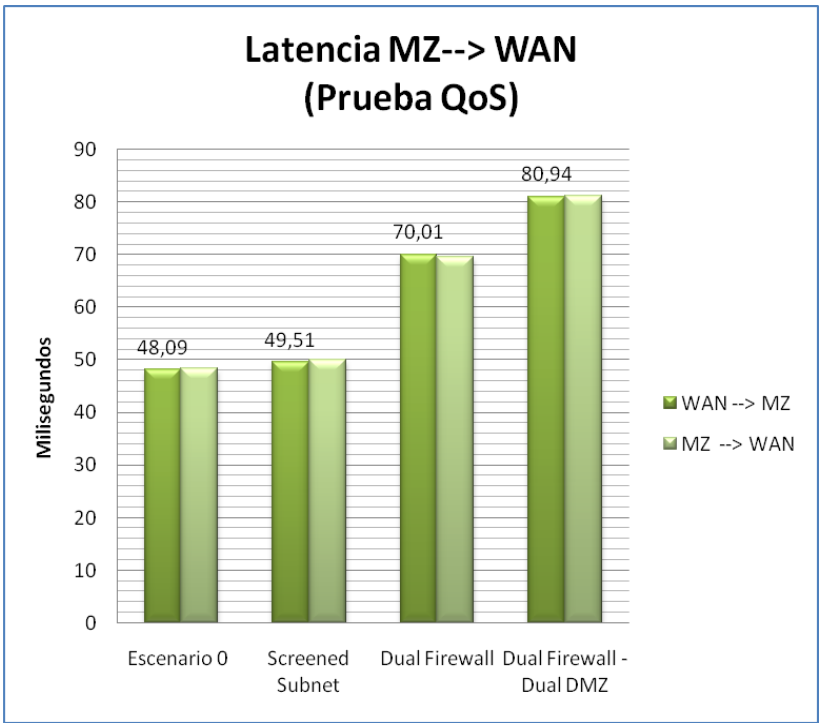


Figura 25: Latencia MZ a WAN (Prueba de QoS)

Existe un incremento significativo en la Latencia para las arquitecturas “Dual Firewall” y “Dual Firewall – Dual DMZ”, este ocasionado por la presencia de dos firewalls en la protección de la red, a diferencia de la arquitectura “Screened Subnet” la cual solo dispone de un solo firewall de protección.

Aunque la Latencia haya aumentado para todas las arquitecturas, estas siguen teniendo valores aceptables de este parámetro según el estándar, ya que no supera los 150ms de retardo entre paquetes.

El porcentaje de incremento de latencia para cada arquitectura es presentado en la *Figura 26*. En esta se observa cómo el porcentaje de incremento de las dos últimas arquitecturas, que corresponden a las más seguras, es realmente alto, pero no supera el 100% del valor del Escenario 0; esto nos permite concluir, que entre más seguridad se le brinde a la red, la QoS se ve afectada de manera significativa.

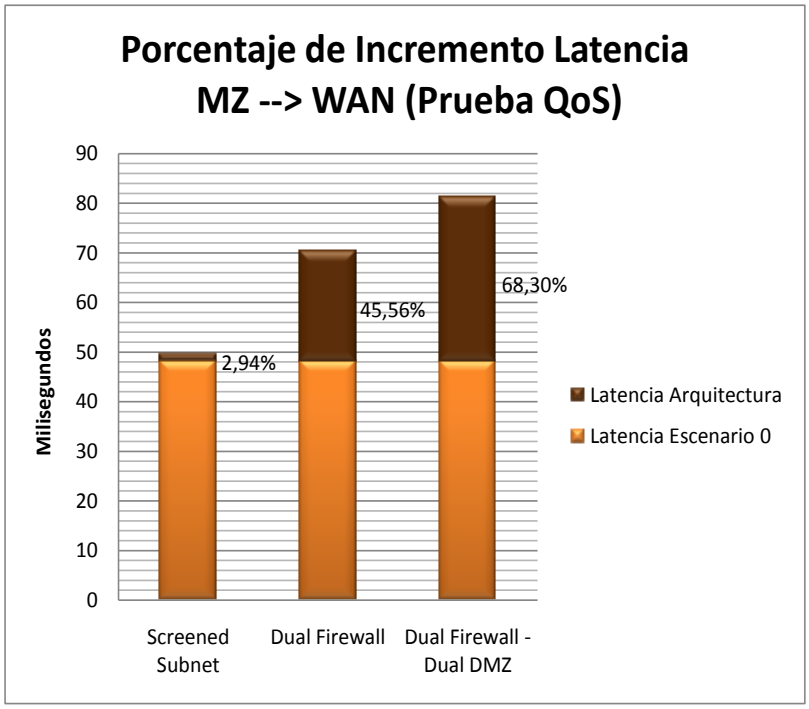


Figura 26: Porcentaje de incremento Latencia MZ a WAN (Prueba QoS)

Se puede observar cómo al igual que para las pruebas anteriores, los porcentajes de incremento de la zona origen al destino y viceversa son los mismos.

4.1.2.2. RESULTADOS JITTER

El jitter es una medida que al igual que la latencia es afectado cuando se establece seguridad en las redes; este parámetro crece en una medida no despreciable con lo que tiene que ver con tráfico de voz sobre IP.

La medida de este parámetro se realiza con llamadas desde y hacia las diferentes zonas de las arquitecturas a evaluar.

- Llamada desde la Zona Militarizada hacia la Zona Desmilitarizada de la arquitectura:

En la *Figura 27* se muestra los resultados de Jitter para estas dos zonas:

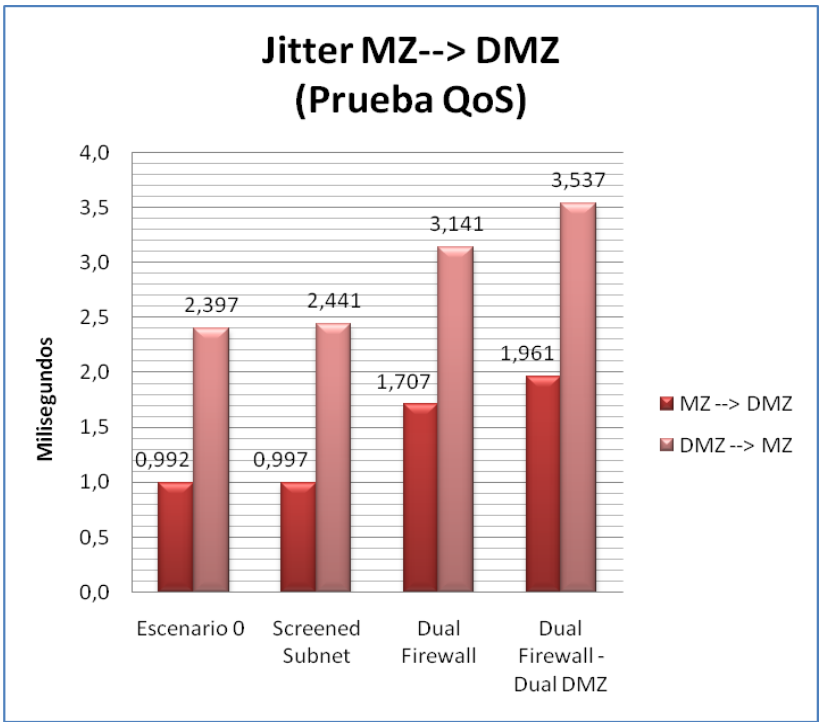


Figura 27:Jitter MZ a DMZ (Prueba de QoS)

Esta figura nos muestra cómo el Jitter sufre un aumento significativo para cada una de las arquitecturas, claro está un aumento mayor en "Dual Firewall – Dual DMZ" y el menor registrado para "Screened Subnet"; estos resultados, relacionados con el nivel de seguridad que cada arquitectura le ofrece a la red a proteger; pero cabe aclarar que ninguno de estos resultados sobrepasan el valor aceptado según el estándar para comunicaciones de Voz sobre IP, el cual establece un valor de 75,5ms para una buena comunicación.

Sin embargo, se presentan porcentajes significativos de aumento en los valores registrados, respecto del Escenario 0; en la *Figura 28* se presenta claramente el porcentaje de incremento del Jitter para cada una de las arquitecturas implementadas, respecto del Escenario 0.

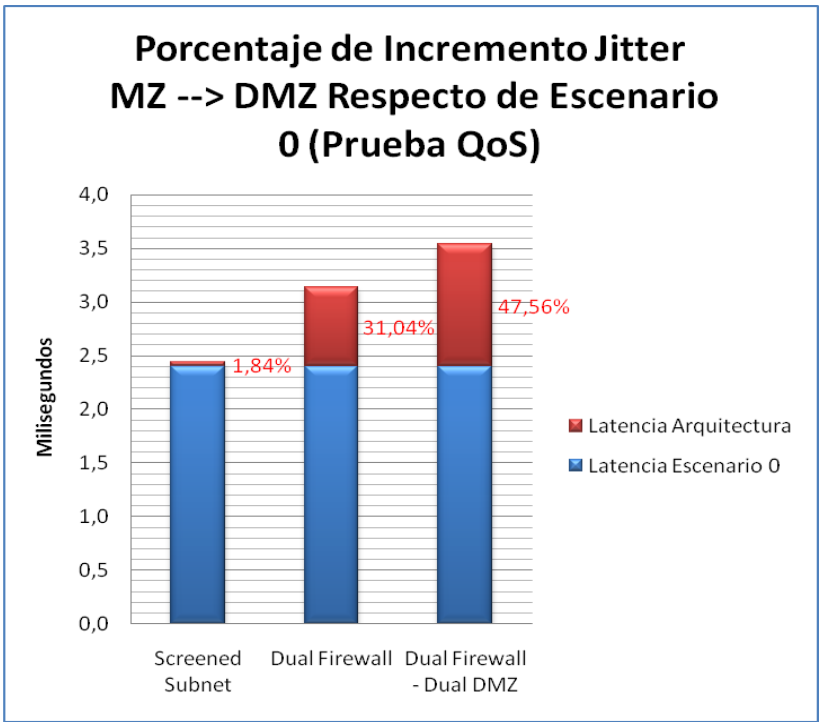


Figura 28: Porcentaje de incremento Jitter MZ a DMZ Respecto de Escenario 0 (Prueba QoS)

Se puede apreciar aumentos significativos de Jitter para las dos últimas arquitecturas, y un aumento casi imperceptible de la arquitectura "Screened Subnet", debido al poco cambio respecto del Escenario 0. Por otra parte, tomando como referencia el Escenario 0 para las medidas de Latencia y Jitter respectivamente, se puede ver cómo el primero de estos dos parámetros sufre un mayor incremento cuando se implementan las arquitecturas de seguridad; la *Tabla 27* nos ayuda a entenderlo mejor:

ARQUITECTURA	PORCENTAJE DE AUMENTO DE LATENCIA (Respecto del Escenario 0)	PORCENTAJE DE AUMENTO DE JITTER (Respecto del Escenario 0)
SCREENED SUBNET	4,47%	1,84%
DUAL FIREWALL	56,14%	31,04%
DUAL FIREWALL – DUAL DMZ	76,24%	47,56%

Tabla 27: PORCENTAJE DE AUMENTO DE LATENCIA Y JITTER respecto del Escenario 0

En este orden de ideas, se aprecia cómo se afecta en mayor grado el Jitter cuando se implementan arquitecturas de seguridad basadas en firewall, que la Latencia, sin embargo los valores siguen siendo aceptables según el estándar.

- Llamada desde la WAN hacia la Zona Desmilitarizada de la arquitectura:

En la *Figura 29* se muestra los resultados de Jitter para estas dos zonas:

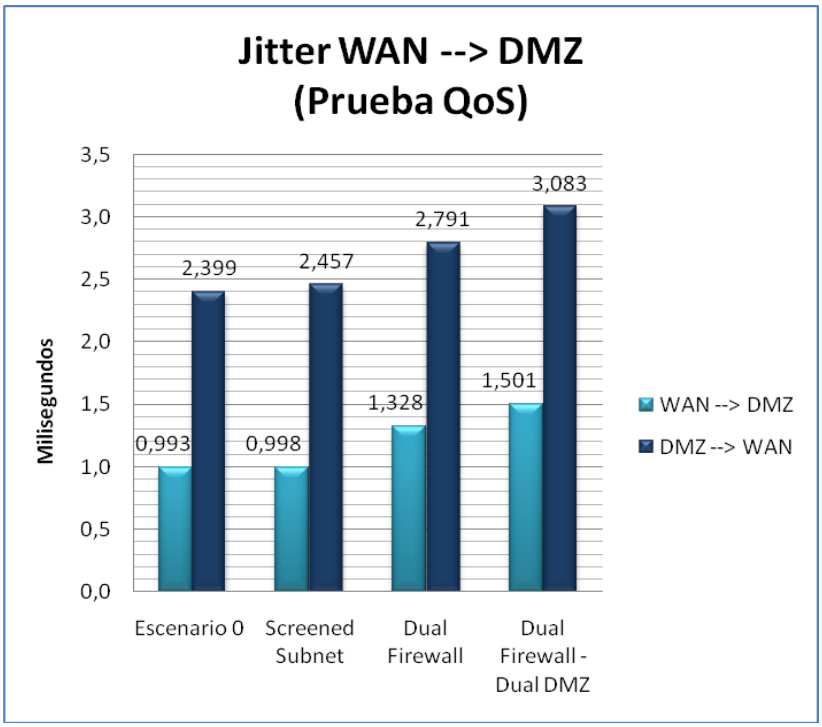


Figura 29: Jitter WAN a DMZ (Prueba de QoS)

Nuevamente se observa que la arquitectura que más incrementa el valor de Jitter respecto del Escenario 0 es “Dual Firewall – Dual DMZ” y la que menos lo incrementa es “Screened Subnet” igual por las razones fundamentadas anteriormente; por otra parte resulta el mismo comportamiento respecto del incremento que sufre el Jitter de la DMZ hacia la WAN, tomando como referencia el registrado de la WAN hacia la DMZ; es un incremento significativo para todas y cada una de las arquitecturas, incluyendo el Escenario 0.

En la *Figura 30,* se presenta el porcentaje de incremento del Jitter tomando como referencia el Escenario 0 para cada una de las arquitecturas:

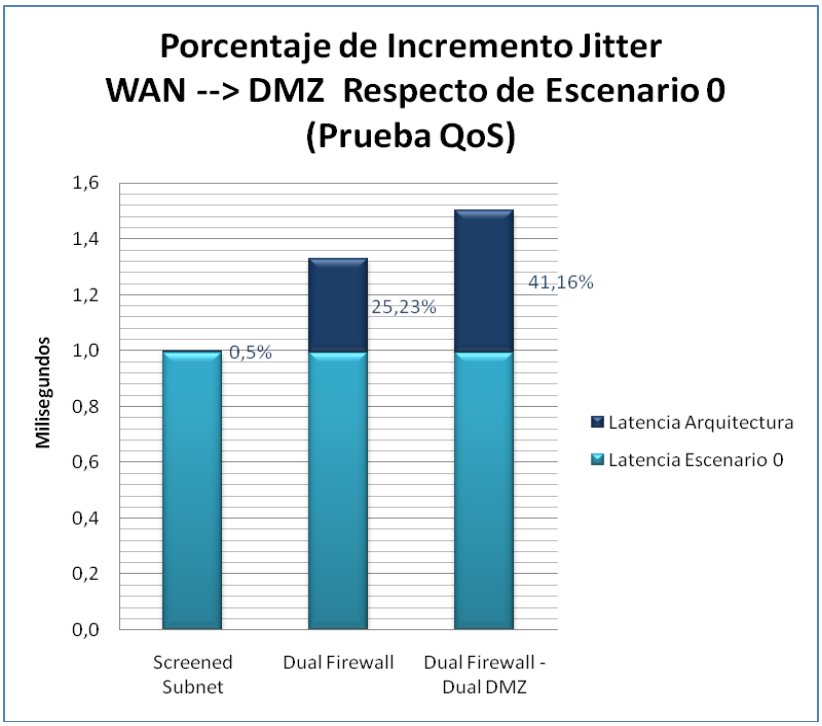


Figura 30: Porcentaje de incremento Jitter WAN a DMZ (Prueba QoS)

Esta figura muestra dos aspectos importantes: el primero de ellos, como se explicó anteriormente, que la arquitectura "Screened Subnet" presenta el menor incremento de Jitter de todas las arquitecturas y "Dual Firewall – Dual DMZ" el mayor, ambos tomando como referencia el Escenario 0; por otro lado, que el incremento del valor de Jitter cuando se realiza la llamada desde la WAN hacia la Zona Desmilitarizada, que es este caso, en las arquitecturas "Dual Firewall" y "Dual Firewall – Dual DMZ" es menor que el registrado cuando se realizaba la llamada desde la Zona Militarizada hacia la Zona Desmilitarizada de las arquitecturas, igualmente respecto del Escenario 0, ya que el equipo involucrado en la seguridad presenta menor cantidad de reglas de filtrado. Por su parte la arquitectura "Screened Subnet" presenta un incremento similar en los dos casos, ya que el firewall para los dos casos tiene las mismas características de filtrado.

La *Tabla 28* nos ayuda a entenderlo mejor:

ARQUITECTURA	PORCENTAJE DE INCREMENTO JITTER MZ a DMZ (Respecto del Escenario 0)	PORCENTAJE DE INCREMENTO JITTER WAN a DMZ (Respecto del Escenario 0)
SCREENED SUBNET	1,84%	0,5%
DUAL FIREWALL	31,04%	25,23%
DUAL FIREWALL – DUAL DMZ	47,56%	41,16%

Tabla 28: Porcentajes de Incremento del Jitter de MZ hacia DMZ y de WAN hacia DMZ Respecto de Escenario 0 (Pruebas de QoS):

- Llamada desde la Zona Militarizada de la arquitectura hacia la WAN:

En la *Figura 31* se muestra los resultados de Jitter para la llamada realizada entre estas dos zonas:

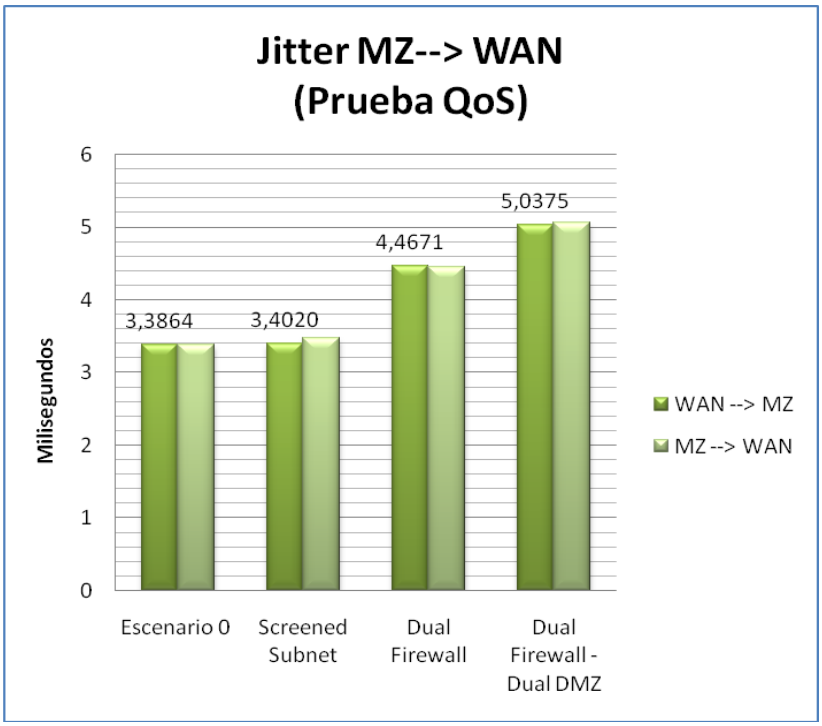


Figura 31: Jitter MZ a WAN (Prueba de QoS)

En esta figura se puede observar un aumento significativo del Jitter para las arquitecturas de la gráfica; esto debido a que para completar la llamada de un extremo al otro de estas arquitecturas, el tráfico tiene que pasar por dos firewalls;

en el caso de “Dual Firewall” y “Dual Firewall – Dual DMZ” de los firewalls interno y externo y para el caso de “Screened Subnet” del único existente; el incremento del Jitter para esta última arquitectura está asociado con las mismas reglas de filtrado por las que tiene que pasar el tráfico dos veces, y para las arquitecturas restantes, por reglas de filtrado diferentes, implementadas en equipos diferentes (firewall interno y externo); Pero finalmente la arquitectura que más incrementa el Jitter en la red respecto del Escenario 0 sigue siendo “Dual Firewall - Dual DMZ”.

A continuación, en la *Figura 32* se presentan los porcentajes de incremento de Jitter para cada una de las arquitecturas cuando se realiza la llamada desde la Zona Militarizada de las arquitecturas hacia la WAN:

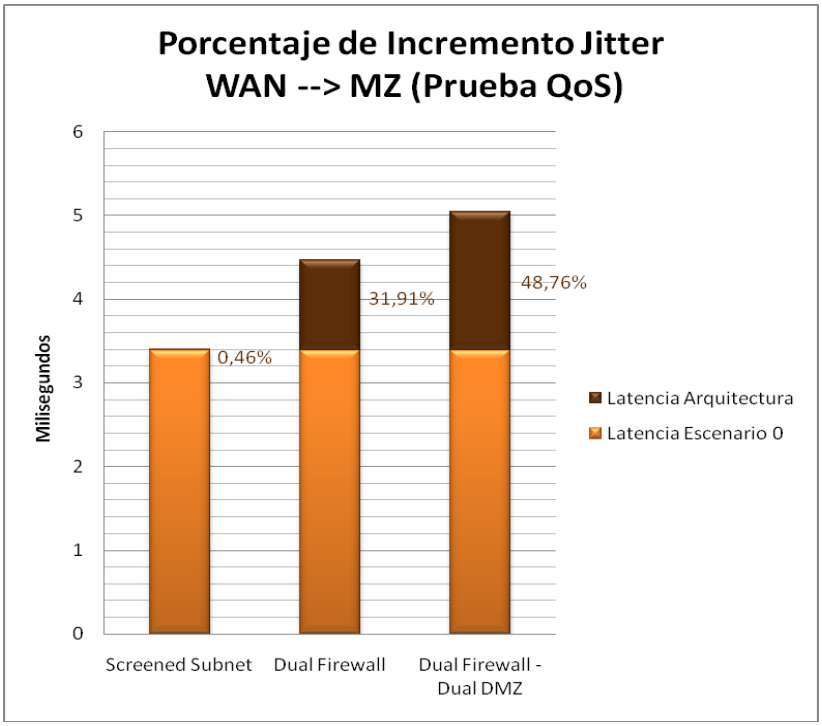


Figura 32: Porcentaje de incremento Jitter MZ a WAN (Prueba QoS)

En esta figura se ve de manera clara, cómo el Jitter aumenta de manera significativa para estas dos arquitecturas (Dual Firewall y Dual Firewall – Dual DMZ); pero al igual que se explicó anteriormente, este incremento en el Jitter es

menor que el incremento que sufre la Latencia cuando se realiza la llamada entre estas mismas zonas.

El aumento de cada uno de estos parámetros cuando se realiza la llamada entre estas dos zonas es presentado en la *Tabla 29*:

ARQUITECTURA	PORCENTAJE DE INCREMENTO LATENCIA MZ a WAN (Respecto del Escenario 0)	PORCENTAJE DE INCREMENTO JITTER MZ a WAN (Respecto del Escenario 0)
SCREENED SUBNET	2,94%	0,46%
DUAL FIREWALL	45,56%	31,91%
DUAL FIREWALL – DUAL DMZ	68,30%	48,76%

Tabla 29: Porcentajes de Incremento del Jitter de MZ hacia DMZ y de WAN hacia DMZ (Pruebas de QoS)

4.1.3. Pruebas de Rendimiento y QoS

Las últimas pruebas para las arquitecturas de redes seguras basadas en firewall, consisten en la ejecución de los dos servicios anteriormente medidos esta vez corriendo de manera simultánea; es decir, la descarga del Archivo de 136MB contenido en el servidor FTP desde diferentes zonas de la arquitectura y la llamada de 1 minuto, ejecutándose simultáneamente.

4.1.3.1 Comportamiento de las diferentes arquitecturas respecto al servicio FTP

- Descarga de archivo contenido en el servidor FTP en la Zona Desmilitarizada hacia la Zona Militarizada de la arquitectura:

En la *Figura 33*, se muestra el Throughput calculado haciendo uso del tiempo de transferencia del archivo de 136MB desde el servidor FTP interno ubicado en la Zona Desmilitarizada hacia la estación de trabajo de la Zona Militarizada de las diferentes arquitecturas:

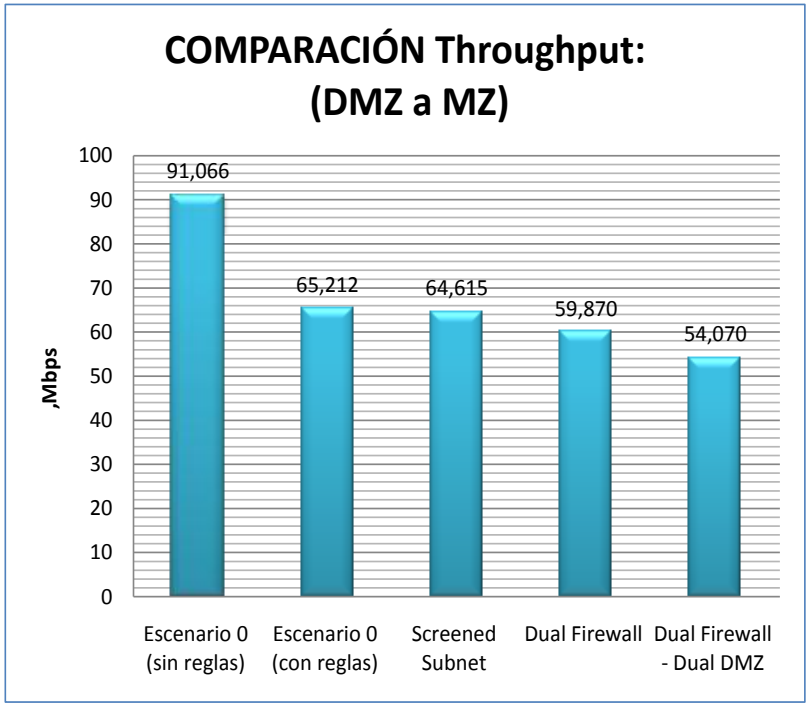


Figura 33: Comparación Throughput DMZ a MZ (Pruebas de Rendimiento y QoS)

Como se observa en esta figura, nuevamente la arquitectura “Dual Firewall – Dual DMZ” presenta la mayor baja de Throughput y “Screened Subnet” la menor, respecto del Escenario 0; esto causado por el nivel de seguridad que cada una de estas ofrece a la red.

Por su parte, la Arquitectura “Dual Firewall” también afecta el rendimiento de la red, ya que baja el Throughput en la misma en un porcentaje considerable.

Estos porcentajes de decremento cuando los dos servicios están actuando de manera simultánea se presentan en la *Figura 34*:

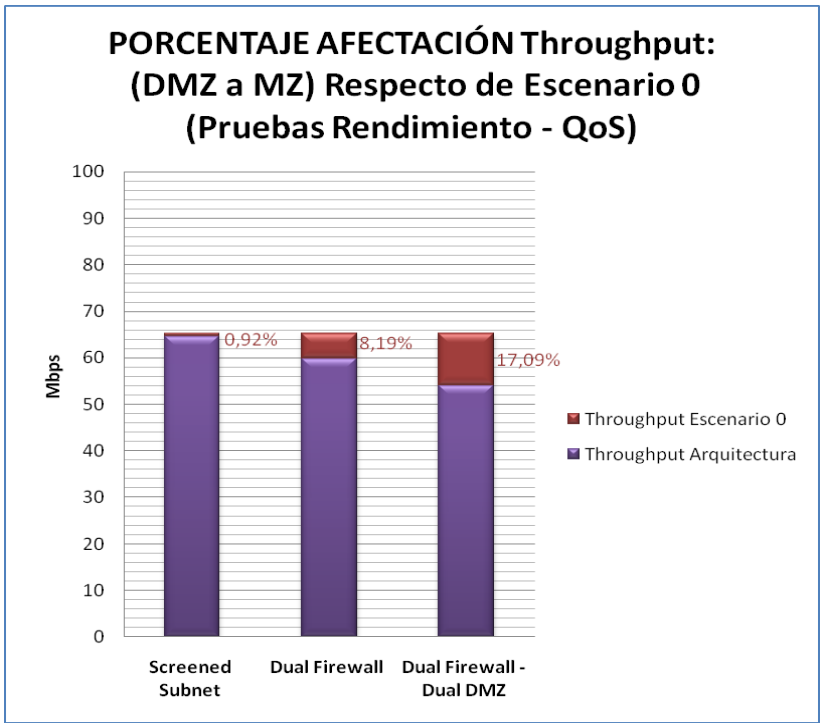


Figura 34: Porcentaje de afectación del Throughput DMZ a MZ (Pruebas de Rendimiento y QoS)

Al igual que para la prueba anterior, se registra un decremento del Throughput debido a la implementación de las diferentes arquitecturas, pero para estas pruebas, cuando los dos servicios están actuando de manera simultánea, este decremento es mayor respecto de los 100Mbps del canal ya que este servicio tiene que compartir canal con el de Voz sobre IP, y por la implementación de la QoS en la red, dispone de tan sólo el 30% de este. Para verlo de una manera más clara, se presenta la *Figura 33*:

ARQUITECTURA	DECREMENTO THROUGHPUT Solo FTP (Respecto de los 100Mbps del Canal)	DECREMENTO THROUGHPUT FTP + Voz sobre IP (Respecto de los 100Mbps del Canal)
SCREENED SUBNET	25,84%	35,39%
DUAL FIREWALL	32,87%	40,13%
DUAL FIREWALL – DUAL DMZ	36,85%	45,93%

Tabla 30: Porcentajes de decremento Throughput de DMZ a MZ (Solo FTP Y FTP+VOIP)

- Descarga de archivo contenido en el servidor FTP en la Zona Desmilitarizada de la arquitectura hacia la WAN.

En la *Figura 35*, se muestra el Throughput calculado haciendo uso del tiempo de transferencia del archivo de 136MB desde el servidor FTP interno ubicado en la Zona Desmilitarizada de las diferentes arquitecturas hacia la estación de trabajo de la WAN.

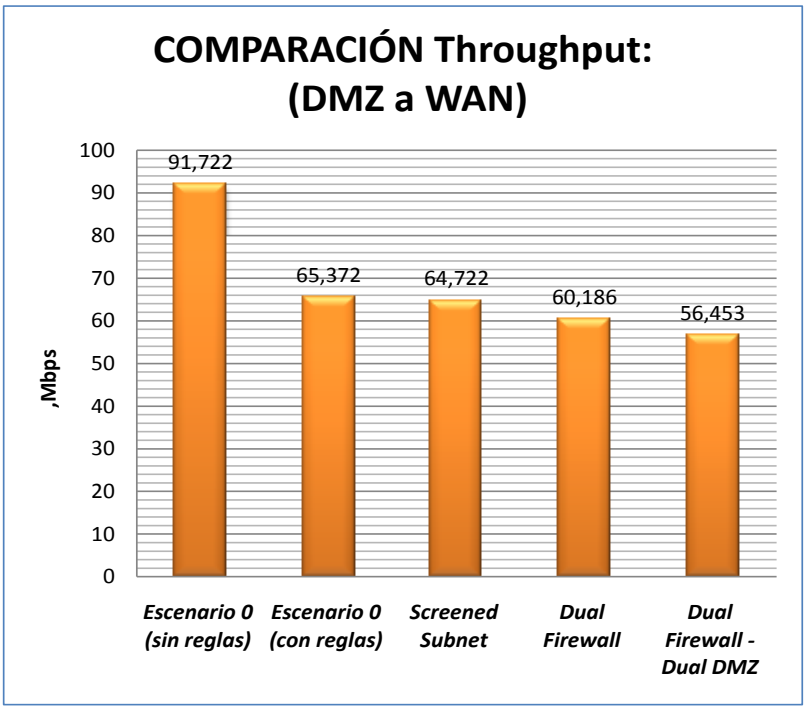


Figura 35: Comparación Throughput DMZ a WAN (Pruebas de Rendimiento y QoS)

Como se puede observar nuevamente la arquitectura “Dual Firewall – Dual DMZ” es la que más afecta el rendimiento de la red.

Los porcentajes de decremento del Throughput respecto del Escenario 0 cuando se realiza la descarga del archivo entre estas dos zonas, es presentado en la *Figura 36*:

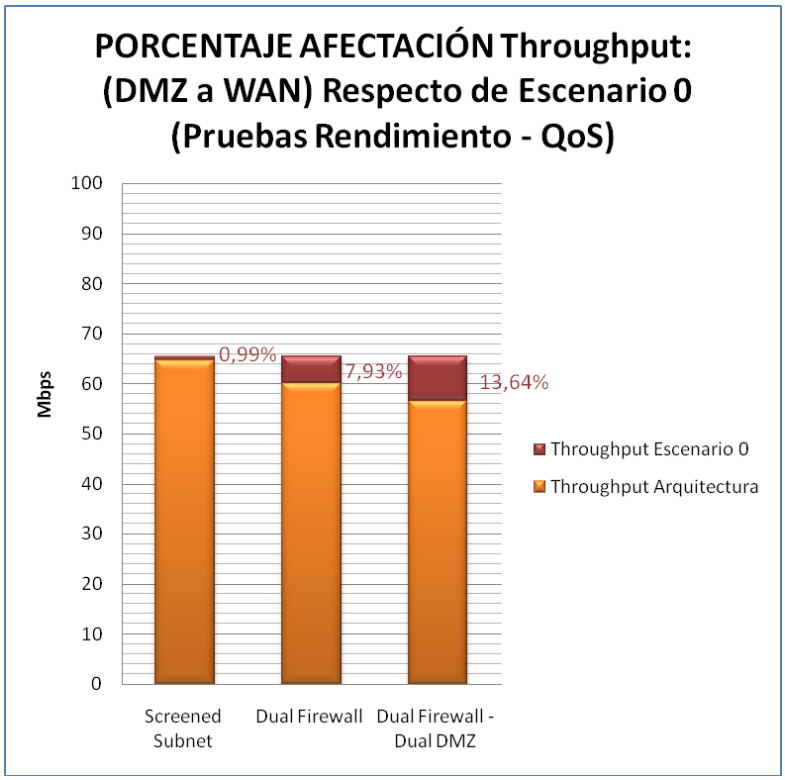


Figura 36: Porcentaje de afectación del Throughput DMZ a WAN (Pruebas de Rendimiento y QoS)

Nuevamente se nota un porcentaje mayor de afectación del Throughput que cuando el servicio FTP disponía del 100% del canal para esta misma prueba; esto debido nuevamente a que tiene que compartirlo con el servicio de Voz sobre IP.

- Descarga de archivo contenido en el servidor FTP en la WAN hacia la Zona Militarizada de las arquitecturas.

En la *Figura 37*, se muestra el Throughput calculado haciendo uso del tiempo de transferencia del archivo de 136MB desde el servidor FTP interno ubicado en la WAN hacia la estación de trabajo de la Zona Militarizada de las diferentes arquitecturas:

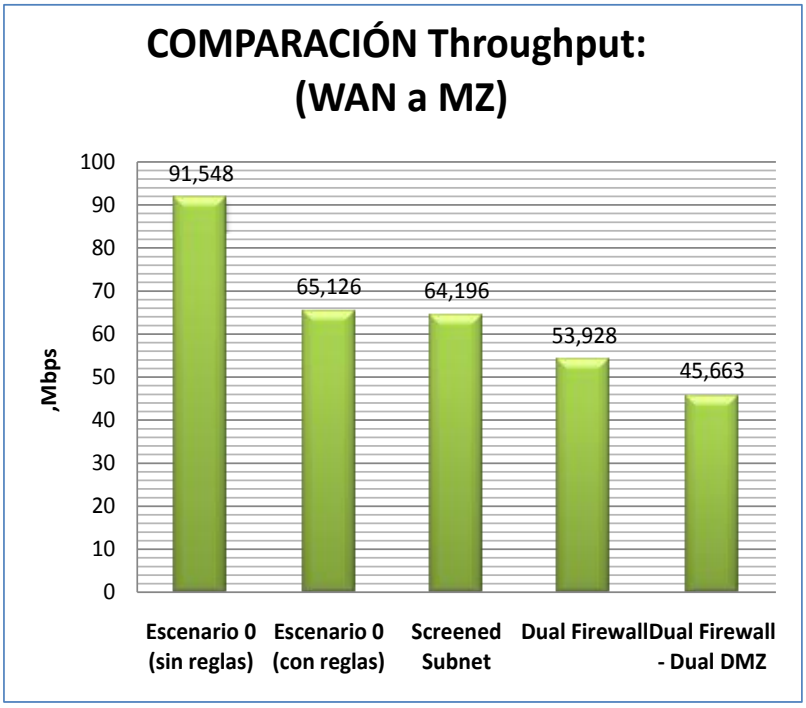


Figura 37: Comparación Throughput WAN a MZ (Pruebas de Rendimiento y QoS)

En esta figura se aprecia claramente cómo el tener más de un firewall actuando como defensa en una red, afecta de manera significativa el Throughput en la misma; para la arquitectura Screened Subnet, se presenta una baja menor que la registrada para las arquitecturas restantes, era de esperarse ya que esta arquitectura cuenta con un solo firewall y una única línea de defensa, mientras que las otras dos cuentan con dos firewalls y por ende dos líneas fuertes de defensa.

Los porcentajes de afectación del Throughput de las diferentes arquitecturas, son presentados en la *Figura 38:*

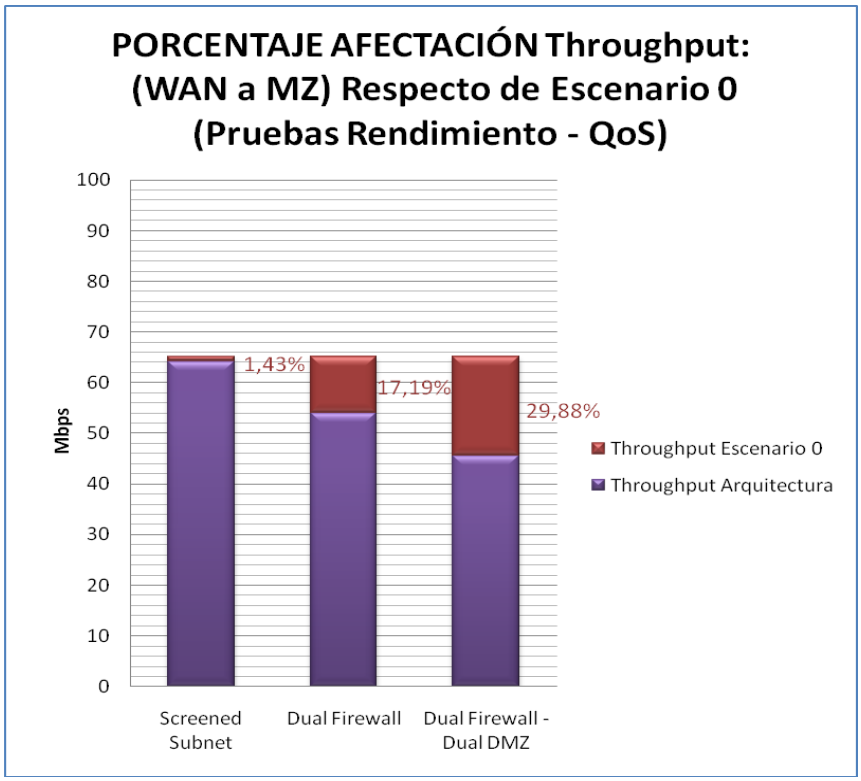


Figura 38: Porcentaje de afectación del Throughput MZ a WAN (Pruebas de Rendimiento y QoS)

En las dos figuras anteriores se puede observar cómo el valor de Throughput para las arquitecturas “Dual Firewall” y “Dual Firewall - Dual DMZ” baja en un porcentaje considerable respecto del escenario 0, como se ha dicho en las explicaciones anteriores, esto debido a que el tráfico tiene que pasar por dos firewalls antes de llegar a su destino, situación que no ocurre para “Screened Subnet” que es la que registra la menor baja de Throughput.

De igual forma se puede observar cómo se baja el Throughput por la ejecución de dos servicios de manera simultánea; esto se muestra en la *Tabla 31*, en la que se muestran los porcentajes en que baja el Throughput de la red para las dos pruebas: Cuando el FTP dispone del 100% del canal y cuando tiene tan solo el 30% de este:

ARQUITECTURA	DECREMENTO THROUGHPUT Solo FTP (Respecto de los 100Mbps del Canal)	DECREMENTO THROUGHPUT FTP + Voz sobre IP (Respecto de los 100Mbps del Canal)
SCREENED SUBNET	25,84%	35,804%
DUAL FIREWALL	36,071%	46,072%
DUAL FIREWALL – DUAL DMZ	39,871%	54,337%

Tabla 31: Porcentajes de decremento Throughput de WAN a MZ (Solo FTP Y FTP+VOIP)

4.1.3.2 Comportamiento de las diferentes arquitecturas respecto al servicio de Voz sobre IP

En el servicio de Voz IP para este conjunto de pruebas, al igual que cuando el servicio disponía del 100% del canal (Pruebas de Rendimiento) se miden 3 variables las cuales son: Latencia, Jitter y Pérdida de Paquetes

4.1.3.2.1. RESULTADOS LATENCIA

Los resultados de esta variable cuando se evalúa el servicio FTP y Voz sobre IP de manera simultánea son obtenidos mediante la llamada entre diferentes zonas.

Las medidas obtenidas para cada una de las pruebas, (cuando se realiza la llamada desde la Zona Militarizada hacia la Zona Desmilitarizada, desde la WAN hacia la Zona Militarizada y desde la Zona Militarizada hacia la WAN) tienen un comportamiento similar a las pruebas de QoS correspondientes a la ejecución del Servicio de Voz sobre IP de manera individual: la arquitectura que más incrementa el valor de Latencia respecto del Escenario 0 es “Dual Firewall – Dual Firewall”, seguida por “Dual Firewall “ y finalmente “Screened Subnet que presenta un aumento bajo respecto del Escenario 0. Estos porcentajes de incremento varían dependen de las Zonas en que se está realizando la llamada ya que influye la cantidad de reglas de filtrado presentes.

A continuación se presenta el incremento de Latencia para cada una de las arquitecturas:

- Llamada desde la Zona Militarizada hacia la Zona Desmilitarizada de la arquitectura:

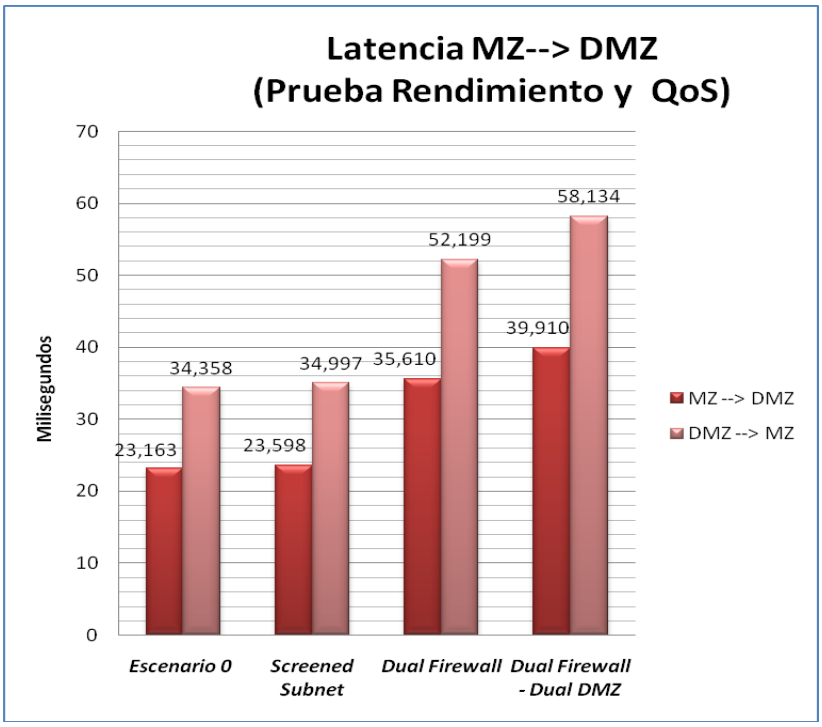


Figura 39: Latencia MZ a DMZ (Prueba de Rendimiento y QoS)

De esta gráfica se puede determinar cómo el valor de Latencia para los paquetes de Voz sobre IP es mayor cuando el servicio tiene que compartir el canal con FTP; a continuación se presenta las *Tablas 34 y 35*, las cual permiten observar este comportamiento de manera más sencilla:

ARQUITECTURA	LATENCIA MZ → DMZ (Solo VoIP)	LATENCIA MZ → DMZ (VoIP + FTP de manera simultánea)
SCREENED SUBNET	19,91ms	23,598ms
DUAL FIREWALL	29,80ms	35,610ms
DUAL FIREWALL – DUAL DMZ	33,71ms	39,910ms

Tabla 32: Latencia MZ --> DMZ (Pruebas de Rendimiento Vs. Pruebas de Rendimiento y QoS)

ARQUITECTURA	LATENCIA DMZ → MZ (Solo VoIP)	LATENCIA DMZ → MZ (VoIP + FTP de manera simultánea)
SCREENED SUBNET	30,42ms	34,997ms
DUAL FIREWALL	45,46ms	52,199ms
DUAL FIREWALL – DUAL DMZ	51,31ms	58,134ms

Tabla 33: Latencia DMZ --> MZ (Pruebas de Rendimiento Vs. Pruebas de Rendimiento y QoS)

En la Figura 40, se puede observar el incremento de Latencia para cada una de las arquitecturas respecto del Escenario 0 cuando se realiza la llamada desde la Zona Militarizada hacia la Zona Desmilitarizada de las respectivas arquitecturas:

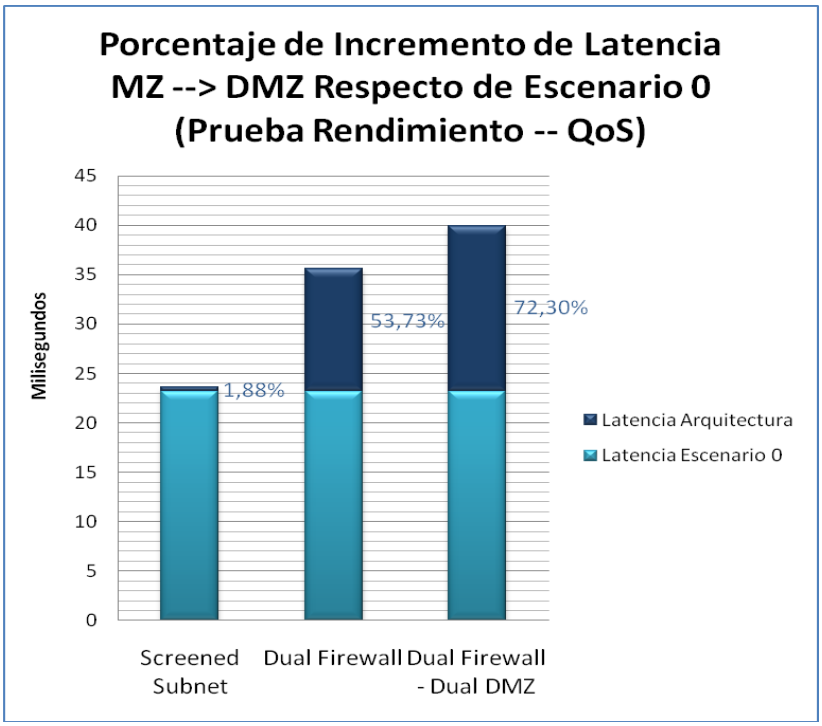


Figura 40: Porcentaje de incremento Latencia MZ a DMZ (Prueba de Rendimiento y QoS)

Este incremento de Latencia cuando el Servicio de Voz sobre IP comparte el canal con FTP respecto de cuando disponía del 100% del canal, se presenta de igual manera para la llamada entre los otros conjuntos de zonas; es decir, de la WAN hacia la Zona Desmilitarizada y desde la Zona Militarizada hacia la WAN.

- Llamada desde la WAN hacia la Zona Desmilitarizada de la arquitectura:

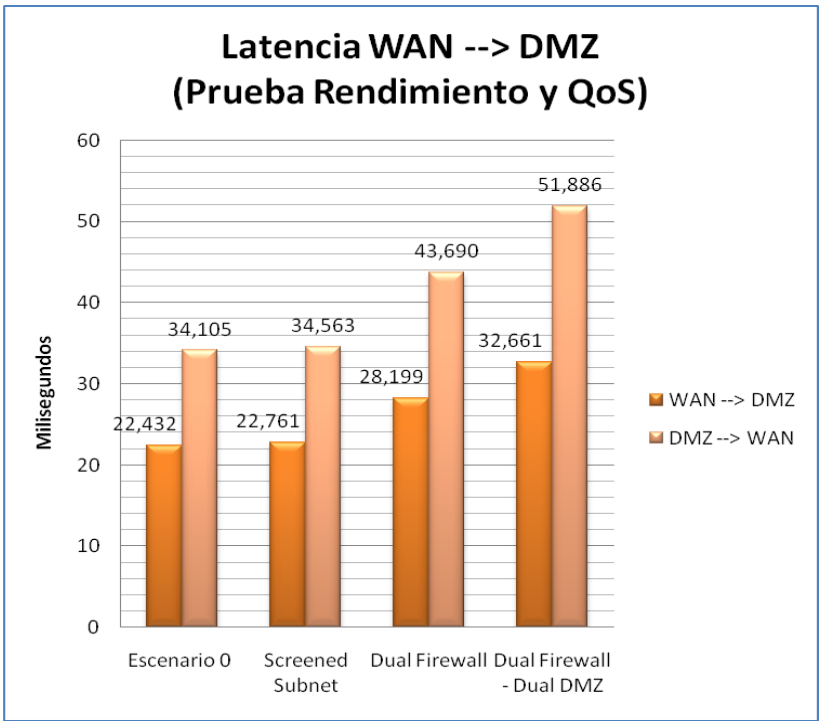


Figura 41: Latencia WAN a DMZ (Prueba de Rendimiento y QoS)

Al igual que para la prueba anterior, de esta gráfica se puede determinar cómo el valor de Latencia para los paquetes de Voz sobre IP es mayor cuando el servicio tiene que compartir el canal con FTP; a continuación se presenta las *Tablas 34 y 35*, las cual permiten observar este comportamiento de manera más sencilla:

ARQUITECTURA	LATENCIA WAN → DMZ (Solo VoIP)	LATENCIA WAN → DMZ (VoIP + FTP de manera simultánea)
SCREENED SUBNET	19,22ms	22,76ms
DUAL FIREWALL	24,64ms	28,19ms
DUAL FIREWALL – DUAL DMZ	28,86ms	32,66ms

Tabla 34: Latencia WAN--> DMZ (Pruebas de Rendimiento Vs. Pruebas de Rendimiento y QoS)

ARQUITECTURA	LATENCIA DMZ → WAN (Solo VoIP)	LATENCIA DMZ → WAN (VoIP + FTP de manera simultánea)
SCREENED SUBNET	30,99ms	34,563ms
DUAL FIREWALL	39,58ms	43,690ms
DUAL FIREWALL – DUAL DMZ	47,93ms	51,886

Tabla 35: Tabla 33: Latencia DMZ --> WAN (Pruebas de Rendimiento Vs. Pruebas de Rendimiento y QoS)

En la Figura 42, se puede observar el incremento de Latencia para cada una de las arquitecturas respecto del Escenario 0 cuando se realiza la llamada desde la Zona Militarizada hacia la Zona Desmilitarizada de las respectivas arquitecturas:

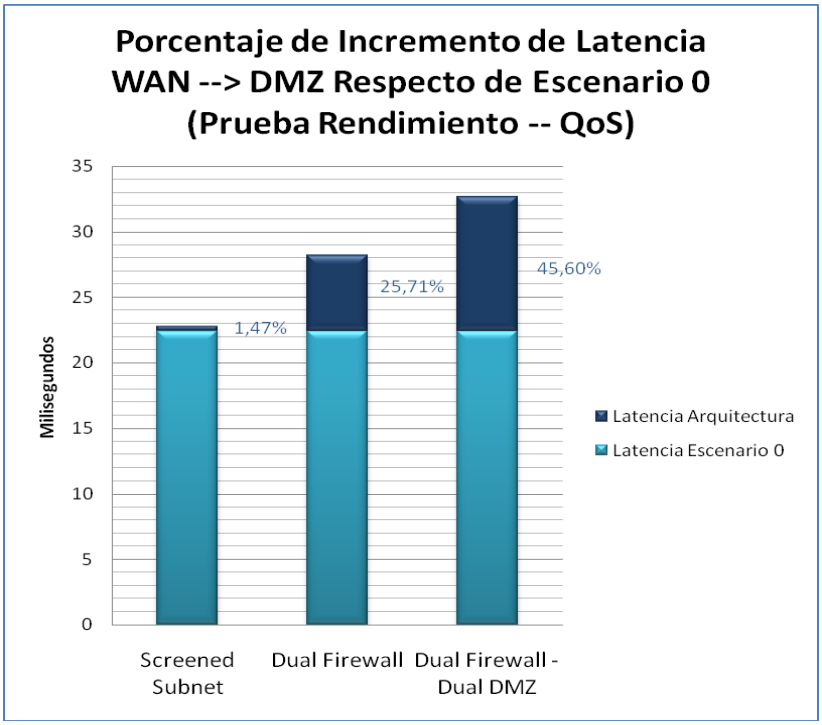


Figura 42: Porcentaje de incremento Latencia WAN a DMZ (Prueba de Rendimiento y QoS)

- Llamada desde la Zona Militarizada de la arquitectura hacia la WAN:

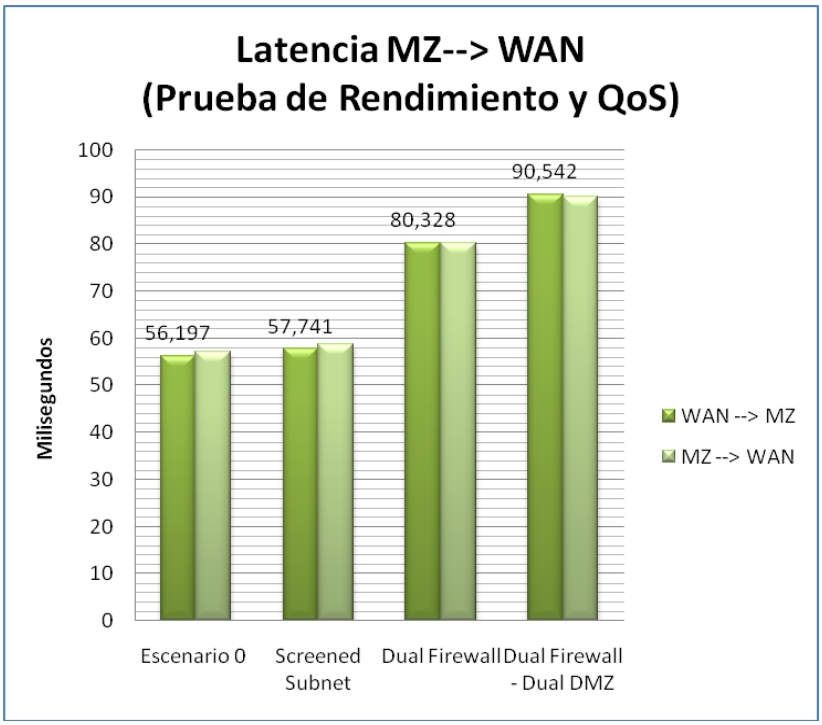


Figura 43: Latencia MZ a WAN (Prueba de Rendimiento y QoS)

En esta gráfica se puede apreciar, cómo a diferencia de las anteriores, los valores de Emisor a Receptor y viceversa son iguales, esto, producto de que en ninguna de las zonas se encontraba el servidor de Voz IP, sino que para llegar desde el origen hasta el destino para completar la llamada, se tiene que pasar primero: de Emisor a Servidor de Voz IP, y luego Servidor de Voz IP a Receptor.

A Continuación se presentan los porcentajes de incremento para los dos casos (WAN a MZ) y viceversa:

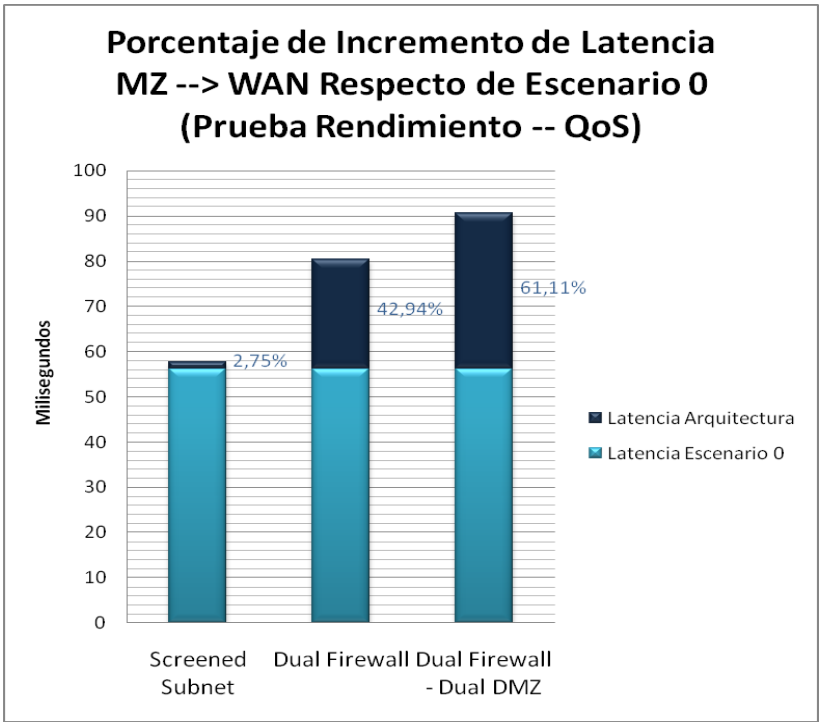


Figura 44: Porcentaje de incremento Latencia MZ a WAN (Prueba de Rendimiento y QoS)

4.1.3.2.2. RESULTADOS JITTER

Los resultados de esta variable cuando se evalúa el servicio FTP y Voz sobre IP de manera simultánea son obtenidos mediante la llamada entre diferentes zonas.

Las medidas obtenidas para cada una de las pruebas, (cuando se realiza la llamada desde la Zona Militarizada hacia la Zona Desmilitarizada, desde la WAN hacia la Zona Militarizada y desde la Zona Militarizada hacia la WAN) tienen un comportamiento similar; la arquitectura que más incrementa el valor de Jitter respecto del Escenario 0 es “Dual Firewall – Dual Firewall”, seguida por “Dual Firewall “ y finalmente “Screened Subnet que presenta un aumento bajo respecto del Escenario 0. Estos porcentajes de incremento varían dependen de las Zonas en que se está realizando la llamada ya que influye la cantidad de reglas de

filtrado presentes. A continuación se presenta el incremento de Jitter para cada una de las arquitecturas en las diferentes pruebas:

- Llamada desde la Zona Militarizada hacia la Zona Desmilitarizada.

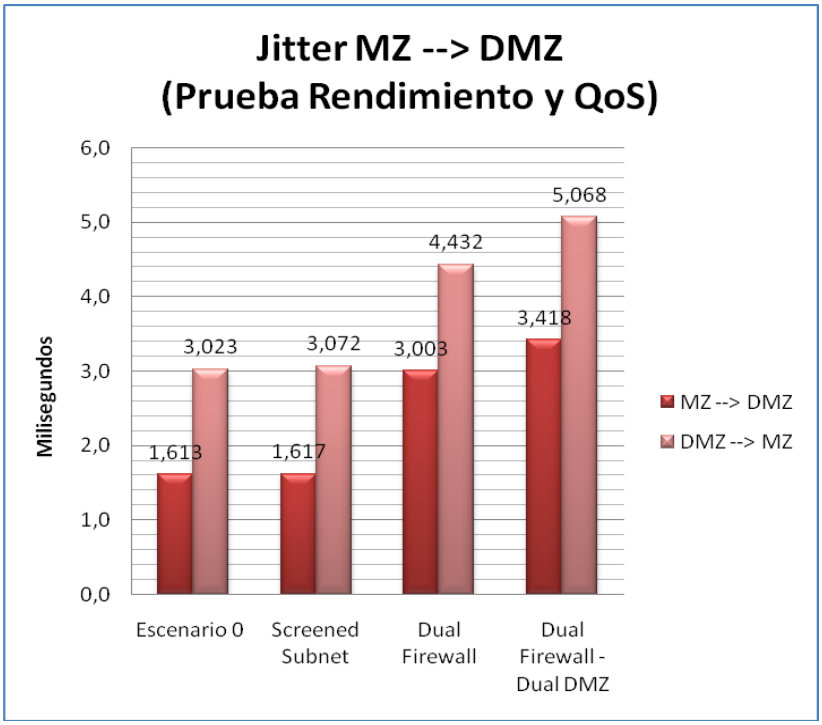


Figura 45: Jitter MZ a DMZ (Prueba de Rendimiento y QoS)

En esta figura se aprecia el mismo comportamiento para cada una de las arquitecturas, que se venía observando anteriormente; la arquitectura que más presenta incremento de Jitter es “Dual Firewall – Dual DMZ”.

A continuación, se presentan los porcentajes de incremento del Jitter para cada una de las arquitecturas

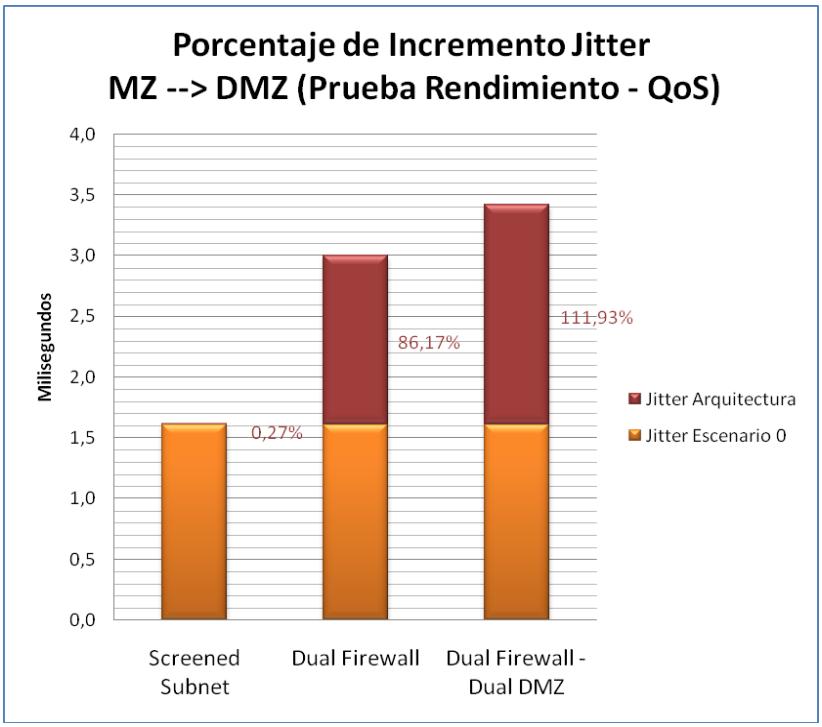


Figura 46: Porcentaje de incremento Jitter MZ a DMZ (Pruebas de Rendimiento y QoS)

En esta prueba, relacionando el Jitter y la Latencia de cada una de las arquitecturas, se puede observar cómo a diferencia de la prueba anterior, cuando el servicio de Voz sobre IP disponía del 100% del canal, el Jitter es el parámetro que se ve más afectado con la implementación de las arquitecturas, ya que se incrementa en un porcentaje mayor que el porcentaje en que se incrementa la Latencia; la tabla nos ayuda a entenderlo mejor:

ARQUITECTURA	PORCENTAJE DE AUMENTO DE LATENCIA (Respecto del Escenario 0)	PORCENTAJE DE AUMENTO DE JITTER (Respecto del Escenario 0)
SCREENED SUBNET	0,08%	0,27%
DUAL FIREWALL	53,73%%	86,17%
DUAL FIREWALL – DUAL DMZ	72,30%	111,93%

Tabla 36: PORCENTAJE DE AUMENTO DE LATENCIA Y JITTER respecto del Escenario 0 (Pruebas de Rendimiento y QoS)

Este mismo comportamiento se observa para las dos pruebas siguientes:

- Llamada desde la WAN hacia la Zona Desmilitarizada.

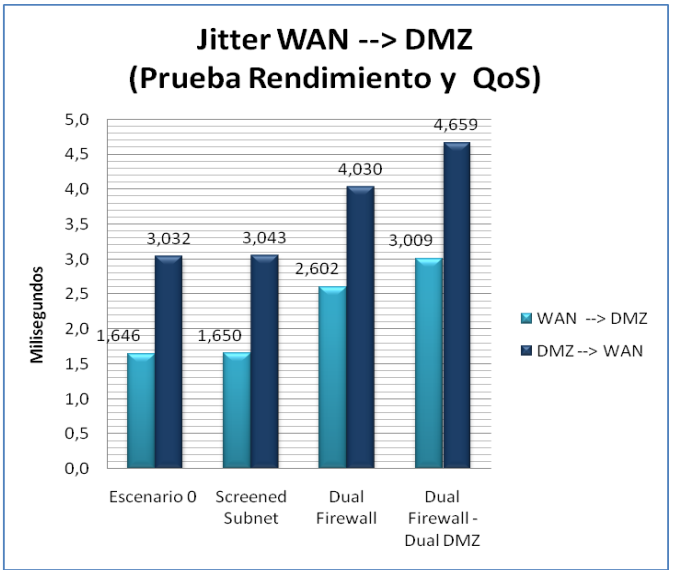


Figura 47: Jitter WAN a DMZ (Prueba de Rendimiento y QoS)

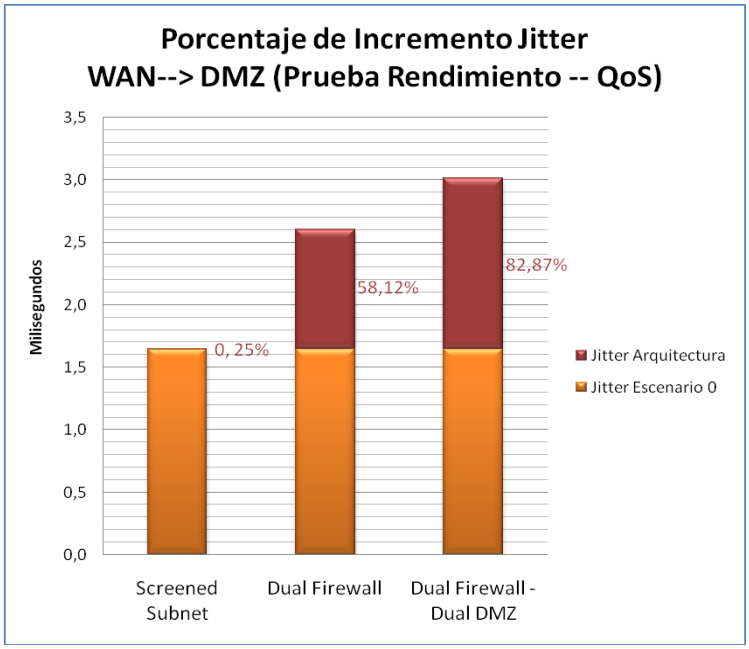


Figura 48: Porcentaje de incremento Jitter WAN a DMZ (Pruebas de Rendimiento y QoS)

- Llamada desde la Zona Militarizada hacia la WAN.

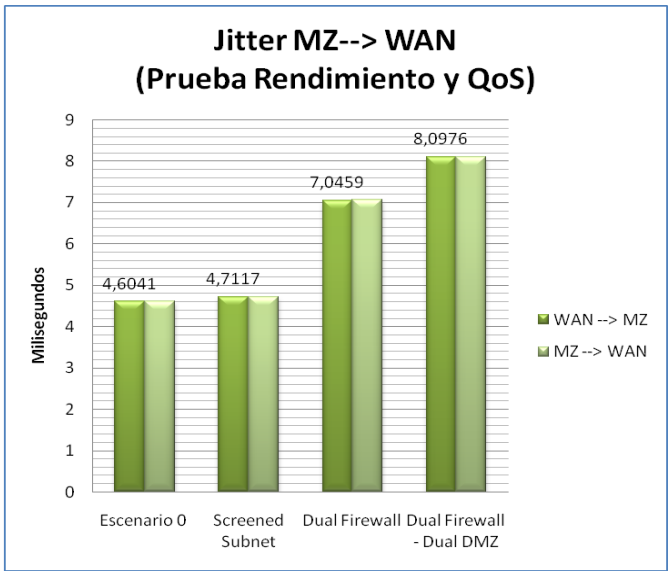


Figura 49: Jitter MZ a WAN (Prueba de Rendimiento y QoS)

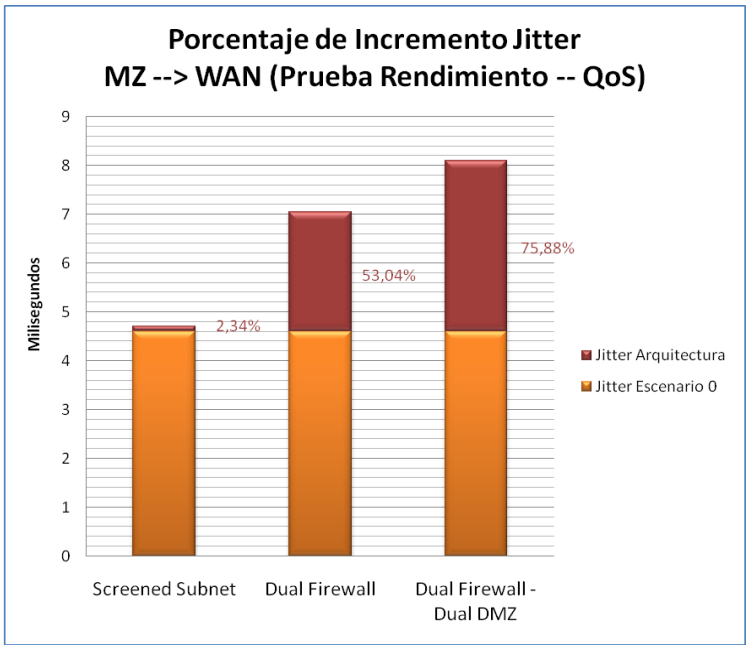


Figura 50: Porcentaje de incremento Jitter MZ a WAN (Pruebas de Rendimiento y QoS)

Al igual que la Latencia, el Jitter es mayor en los tres casos (de la Zona Militarizada hacia la Zona Desmilitarizada, de la WAN hacia la Zona

Desmilitarizada y de la Zona Militarizada hacia la WAN) que cuando el servicio disponía del 100% del canal.

4.1.3.2.3. RESULTADOS PÉRDIDA DE PAQUETES

Para la llamada de Voz sobre IP desde y hacia diferentes zonas, se pudo observar cómo no se presenta pérdida de paquetes desde el Cliente hacia el Servidor, pero si se registra desde el Servidor hacia el Cliente; este porcentaje de pérdida de paquetes es mayor cuando las zonas involucradas en la llamada tienen mayor número de reglas de filtrado; nuevamente es la arquitectura "Dual Firewall - Dual DMZ" la que presenta mayor pérdida de paquetes seguida por "Dual Firewall" que registra un porcentaje menor de pérdida de paquetes y finalmente "Screened Subnet" que presenta el menor porcentaje de pérdida de paquetes de las arquitecturas a evaluar.

Estos porcentajes son presentados a continuación para las diferentes pruebas:

- Llamada desde la Zona Militarizada hacia la Zona Desmilitarizada de la Arquitectura:

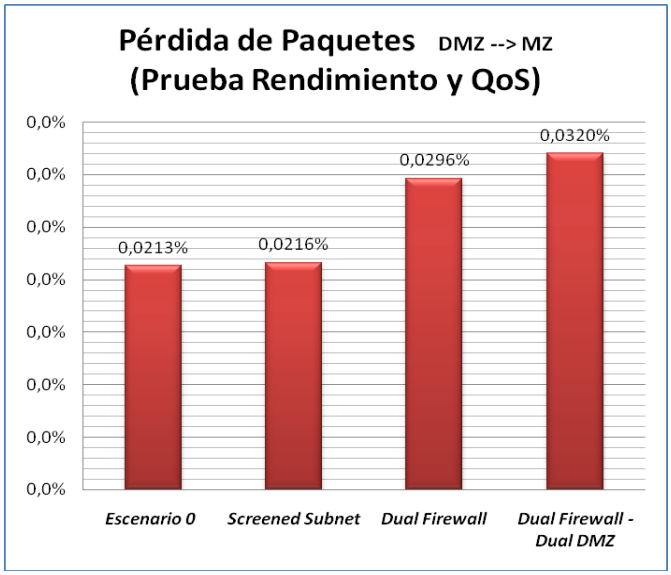


Tabla 37: Pérdida de paquetes DMZ -->MZ Pruebas Rendimiento y QoS

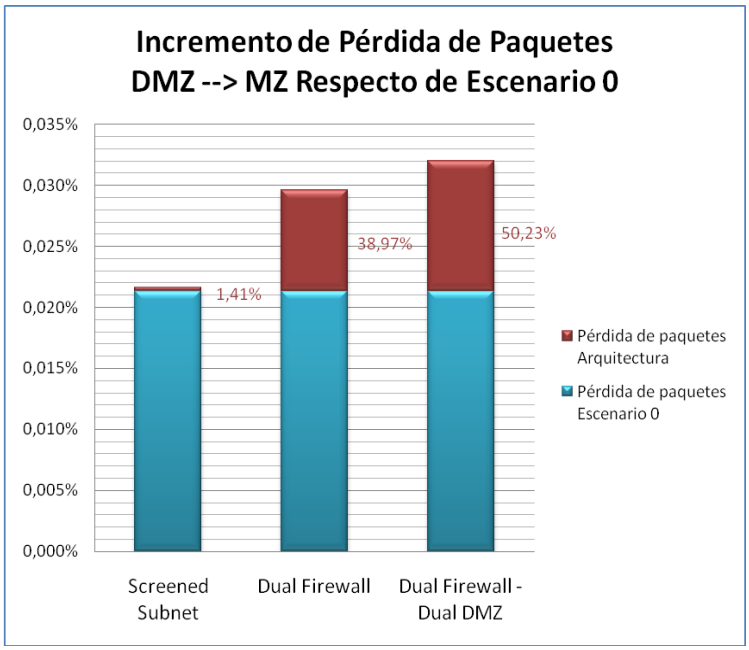


Tabla 38: Porcentaje de Incremento en la Pérdida de Paquetes DMZ --> MZ respecto de Escenario 0

- Llamada desde la WAN hacia la Zona Desmilitarizada de la Arquitectura:

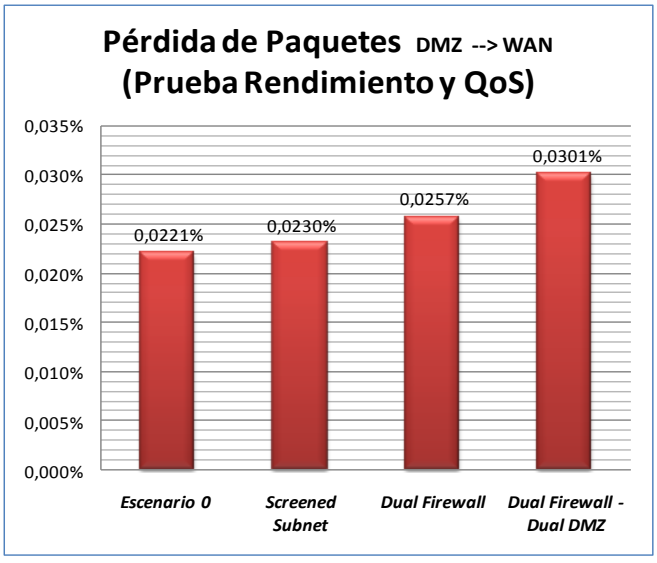


Figura 51: Pérdida de paquetes DMZ --> WAN Pruebas Rendimiento y QoS

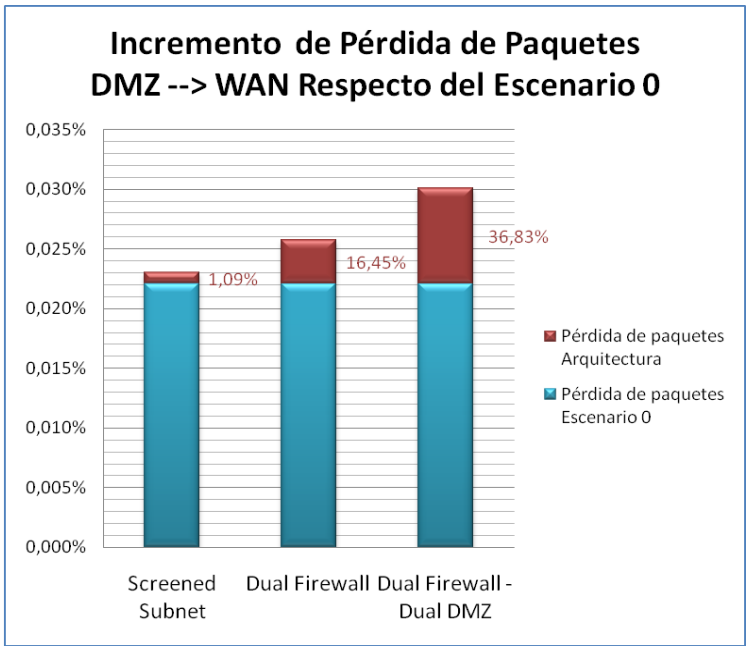


Figura 52: Porcentaje de Incremento en la Pérdida de Paquetes DMZ --> WAN respecto de Escenario 0

- Llamada desde la Zona Militarizada hacia la Zona Desmilitarizada de la Arquitectura:

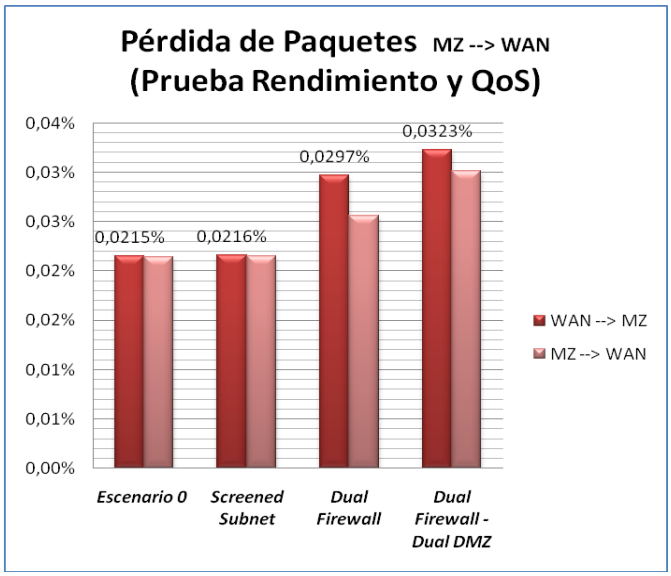


Figura 53: Pérdida de paquetes MZ --> WAN Pruebas Rendimiento y QoS

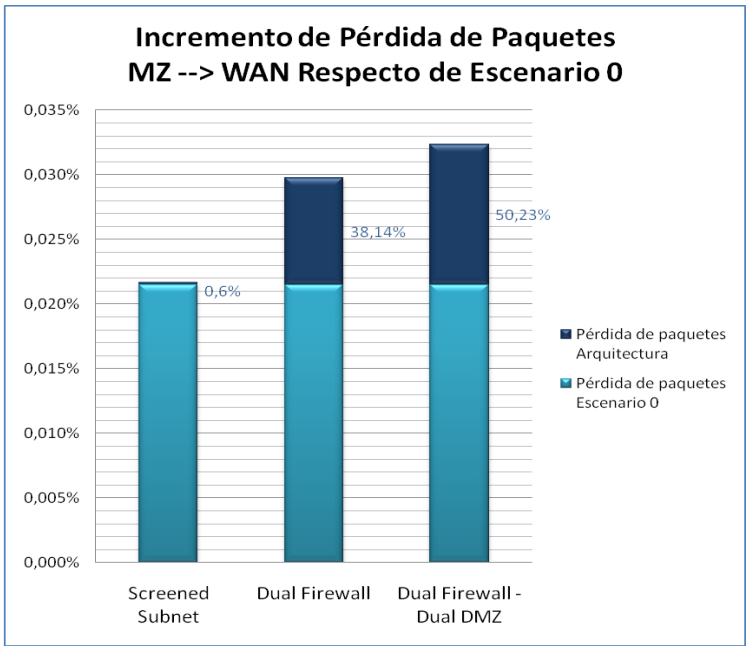


Figura 54: Porcentaje de Incremento en la Pérdida de Paquetes MZ --> WAN respecto de Escenario 0

Para este conjunto de pruebas, cuando se realiza la llamada desde la Zona Militarizada de la arquitectura hacia la WAN, se presenta pérdida de paquetes en los dos sentidos, como se observa en las figuras anteriores, correspondientes al trayecto que tiene que seguir el tráfico para llegar desde el origen hasta el destino, pasando por el Servidor de Voz sobre IP.

Finalmente en la *Figura 55,* y como producto final de esta investigación, se presenta el modelo de Elección de Arquitecturas de Firewall, dependiendo de una relación Rendimiento/QoS y de las necesidades de la red a proteger.

MODELO DE SELECCIÓN DE LA ARQUITECTURA

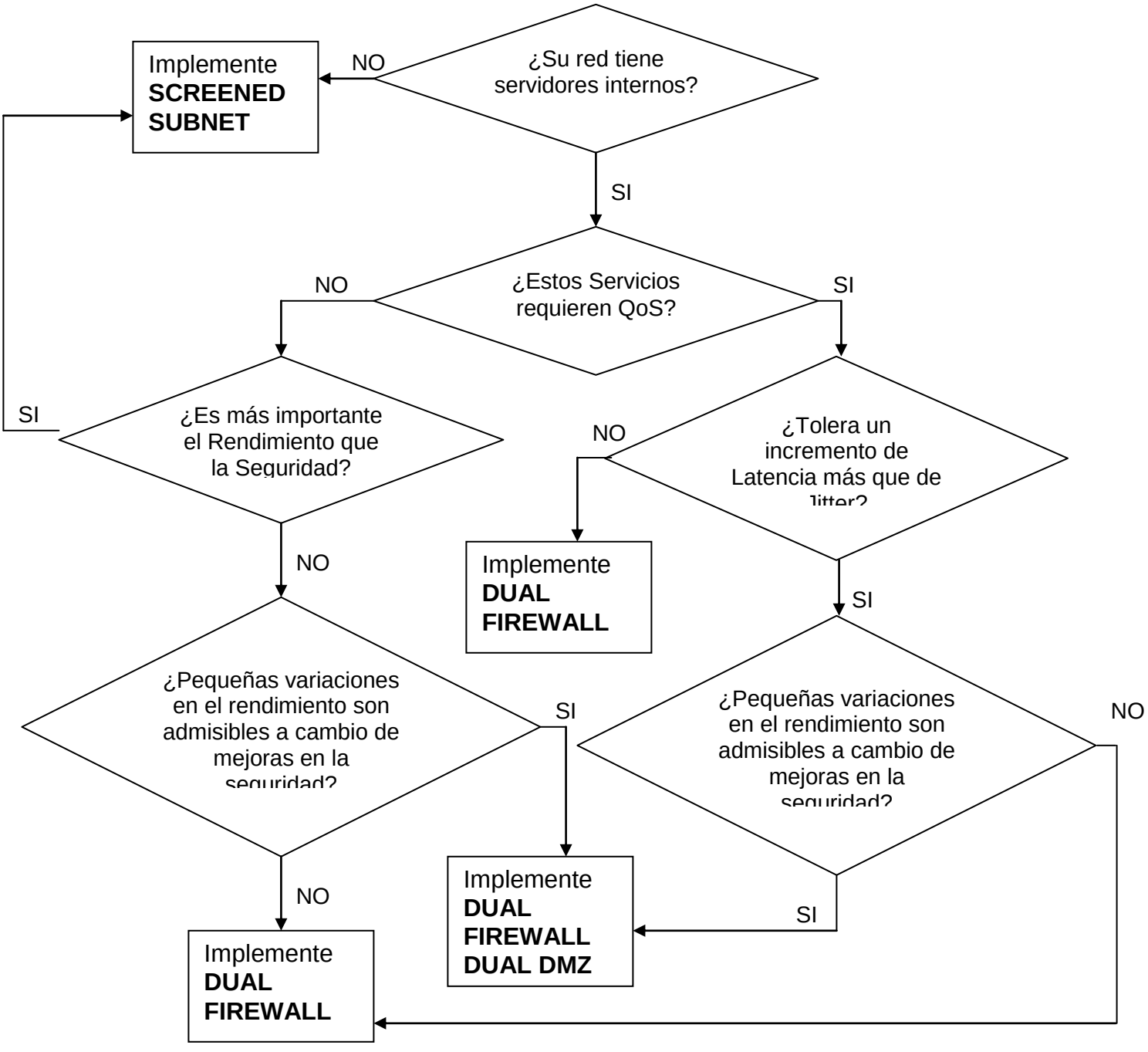


Figura 55: Modelo de Elección de Arquitectura

CONCLUSIONES Y RECOMENDACIONES

- En el momento de implementar una arquitectura de red segura basada en firewall en una organización, se debe prestar gran atención al equipo en que se va a implementar el firewall como tal; es decir, sus especificaciones técnicas, para de esta manera conseguir que la arquitectura montada no afecte en un porcentaje considerable el rendimiento y QoS de la red a proteger.
- El número de reglas de filtrado dependientes de la política de seguridad de la organización, implementadas en la arquitectura, influyen de manera negativa en el rendimiento y QoS de la misma; entre más reglas se implementen mayor será la baja en el rendimiento y Calidad.
- Las organizaciones que ofrecen la tecnología de voz sobre IP deben tener especial cuidado en implementar QoS en la arquitectura implementada, pues de esta decisión dependerá en gran parte el desempeño en ancho de banda y calidad de servicio a largo plazo cuando se piense en brindar un sistema de comunicación segura.
- La arquitectura Screened Subnet es recomendada para organizaciones que no requieran un grado de seguridad alto, pero sí un rendimiento y QoS de su red, óptimos.
- Para medianas y grandes empresas que planeen establecer seguridad en sus redes y que ofrezcan servicios que requieran QoS, pero que por falta de planeamiento no presenten una gestión de la seguridad informática desde el principio, se recomienda el uso de la arquitectura “Dual Firewall”, la cual ofrece niveles equiparables en ancho de banda, calidad de servicio y seguridad.

- Para grandes empresas que requieran mayor protección de sus datos con un rendimiento y QoS de su red, aceptable, se recomienda la implementación de la Arquitectura “Dual Firewall – Dual DMZ”, la cual ofrece un mayor grado de seguridad que las demás presentes en este estudio, y además niveles en rendimiento y QoS aceptables.
- Es necesario realizar el estudio del rendimiento de los equipos cuando se implementa el firewall, y de sus características técnicas
- Se recomienda realizar el análisis de desempeño de Arquitecturas con firewalls basados en Hardware.

BIBLIOGRAFÍA

[1] Análisis de Vulnerabilidades y desempeño de un firewall de plataforma libre contra uno de plataforma licenciada. Daniel Eduardo Padilla Baez. Tesis de grado. Proyecto del Grupo de Investigación en Seguridad de Comunicación GISSIC del programa de Ingeniería en Telecomunicaciones de la Universidad Militar Nueva Granada.

[2] Análisis de vulnerabilidades y fortalezas en cinco firewalls de plataforma libre. Ricardo Andrés Pertúz de las Salas. Tesis de grado. Proyecto del Grupo de Investigación en Seguridad y Sistemas de Comunicación GISSIC del programa de Ingeniería en Telecomunicaciones de la Universidad Militar Nueva Granada.

[3] http://www.prevelakis.net/Papers/VirtualFirewall.pdf. Drexel University, Hipervínculo PDF, “The Virtual Firewall” por Vassilis Prevelakis

[4] Analysis of Vulnerabilities in Internet Firewalls. Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum y Michael Frantzen. Center for Education and Research in Information Assurance and Security – CERIAS.Purdue University. Paper en Línea. Consultado el día 22 de Febrero de 2008.

[5] http:// www.think-future.de/DOCUMENTATION/Ethernet-Bridge-netfilter-HOWTO_de/additional_docs/Firewalling_for_Free.pdf#search=%22%22open%20source%20firewall%22%20filetype%3Apdf%22. Tutorial, Hipervínculo PDF, “Firewalling for free” , por Shawn Grimes

[6] Reliability of systems equipment and components – Guide to failure modes effects and criticality analysis. British Standards Institution. Estándar británico. BSI/BC-5760, Sección 5

[7] Microsoft Encyclopedia of Security. Mitch Tulloch. Microsoft Press. 2003.p 115, 116.

[8] Free Software Foundation. Página Web Oficial de la Fundación Internacional de Software Libre y de Código Abierto. Consultada el día 28 de Octubre de 2009 http://www.fsf.org/

[9] Reliability of systems equipment and components – Guide to failure modes effects and criticality analysis. British Standards Institution. Estándar británico. BSI/BC-5760, Sección 3.

[10] Cisco Systems, “Academia de Networking de Cisco Systems, Guía del primer año” 2004, tercera edición, pagina 65, ISBN: 84-205-4079-2

[11] C. B. Rorabaugh, "Continuous-Time Signals and Their Spectra," in DSP Primer: McGraw-Hill Professional, 1999.

[12] Almashari, Meshal Abdulaziz. Tesis de Maestría en ciencias de Computadores. An Analytical Simulator For Deploying IP Telephony. Mayo de 2006.

[13] Schulzrinne, H., Casner, S., Frederick R., Jacobson, V. RTP: A Transport Protocol for Real-Time Applications. IETF RFC 3550. Julio 2003.

[14] Página web donde se describe el comportamiento de la pérdida de paquetes la calidad de servicio (QoS). Página actualizada el 1 de Enero de 2007, todos los derechos son de Alejandro Torres Aguilera. http://atorresa.wordpress.com/category/qos/

[15] Bharat T. Doshi, Dominik Eggenschwiler, Aswath Rao, Behrokh Samadi, Y. T. Wang, and James Wolfson. VoIP Network Architectures and QoS Strategy. Lucent Technologies Inc. 2003.

[16] Brian Komar, Ronald Beekelaar y Joern Wettern, “Firewalls for dummies”, pp.71-160, Wiley Publishing Segunda edición, 2003.

[17] Méndez Esquivel. Inbound para enlaces PSTN con VoIP. Tesis Licenciatura. Ingeniería en Electrónica y Comunicaciones. Departamento de Ingeniería

Electrónica, Escuela de Ingeniería, Universidad de las Américas Puebla. Mayo 2005.

[18] BRIHUEGA MARTÍNEZ Pedro. Arquitecturas Avanzadas de Firewall. Universidad de Alcalá: Ediciones Paidós,2003.120p.

[19] LABORDA LADRÓN DE GUEVARA Eduardo. Firewalls: Arquitecturas de Seguridad para Internet. Escuela Politécnica Superior, 2000.