Escuela Politécnica Superior de Linares

GRADO EN INGENIERÍA TELEMÁTICA

Universidad de Jaén

Escuela Politécnica Superior de Linares

CONFIGURACIÓN DE UN ENTORNO DE RED UTILIZANDO UN SOFTWARE DE VIRTUALIZACIÓN

Alumno: **Juan Carlos Molina Mantero**

Tutor: Prof. D. Francisco Javier Sánchez-Roselly

Depto.: Ingeniería de Telecomunicación

Noviembre, 2015

AGRADECIMIENTOS

En primer lugar quisiera agradecer a mis padres y familiares más cercanos, por todo su apoyo incondicional y por estar a mi lado cada vez que les he necesitado.

También quisiera hacer partícipes a mis compañeros y amigos de clase, sin los cuales estoy seguro que mi paso por "Peritos" y Linares no hubiera tenido nada que ver con todas y cada una de las experiencias vividas.

Y no quiero olvidarme de mi tío Pedro que, sin lugar a dudas allá donde esté, me sigue encaminando día tras día.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO DE TÉRMINOS:

- Ordenador central / Ordenador físico: es la infraestructura física y tangible en la que se instala el host anfitrión.
- Host anfitrión / Anfitrión: es el sistema operativo del ordenador físico en el que está instalado VirtualBox.
- Host invitado / Invitado: este es el sistema operativo que está funcionando dentro de la máquina virtual creada.
- Máquina virtual (MV): consiste en un entorno especial que VirtualBox crea para el host invitado, simulando los recursos hardware necesarios para que este pueda funcionar. De un modo más técnico, para VirtualBox, una máquina virtual es un conjunto de parámetros que determinan su comportamiento. Para ello se incluyen configuraciones hardware tales como memoria de la MV, espacio de disco, tipo de comportamiento del disco duro, montaje de un CD para que pueda ser leído por el invitado, etc.
- Hipervisor o monitor de máquina virtual (VMM): son aplicaciones que presentan, a los sistemas operativos virtualizados, una plataforma operativa virtual (hardware virtual) mientras que ocultan a dicho sistema operativo virtualizado las características físicas reales del equipo sobre el que operan. Además de esto, también son los encargados de monitorizar la ejecución de los sistemas operativos invitados.
- Guest Additions: es un paquete especial de software que se integra en VirtualBox, pero que se instala dentro del invitado con la finalidad de mejorar su ejecución y añadir opciones extra como por ejemplo compartir carpetas entre anfitrión e invitado o redimensionar la pantalla, entre otras.
- Backup plan: serie de procedimientos para mantener a salvo siempre una copia de seguridad actualizada de la información alojada en un sistema.
- Disaster recovery plan: son una serie de procedimientos previstos para que en el caso de un fallo total o parcial del sistema, este pueda volver a ponerse en funcionamiento de nuevo y en el menor tiempo posible.
- Zona desmilitarizada (DMZ): De esta forma se conoce a la zona segura que se encuentra entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ únicamente se permitan a la red externa.
- MAC: identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física y es única para cada dispositivo.

- DHCP (Dynamic Host Configuration Protocol): este protocolo de red permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres.
- Red virtual: es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.
- Red real: es la encargada de establecer conexiones entre equipos de manera física.
- NAT (Network Address Traslation): mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.

1. RESUMEN

En este trabajo fin de grado se pretende diseñar e implementar un entorno de red virtualizado, y para ello se ha utilizado como software de virtualización VirtualBox versión 4.3.18. Gracias a esta plataforma de virtualización se pueden realizar varias tareas como virtualizar sistemas operativos de diferente naturaleza (FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris y MS-DOS), realizar copias de seguridad, clonar los recursos virtualizados, importar y exportar estos recursos; entre otras.

Se han investigado las capacidades de implementación de red que ofrece esta plataforma y se ha comprobado que ofrece soluciones viables para la puesta en marcha del sistema de red que posteriormente se describirá.

En primer lugar, es necesario tener constancia de que esta plataforma es adecuada, para posteriormente plantear las necesidades técnicas, tanto hardware como software, que requerirá el desarrollo del trabajo. Para ello se comprueba el hardware del que se dispone y se compara con los requisitos hardware que consumirán los sistemas operativos que se virtualizarán en nuestro diseño y que se tendrán que ejecutar simultáneamente. Una vez comparados se determina la necesidad, o no, de ampliar algún recurso hardware.

Posteriormente, se crearán las diferentes máquinas virtuales, especificando en cada una de ellas los recursos hardware (sistema operativo a instalar, periféricos de entrada/salida de los que dispondrá esa máquina, memoria disponible, procesador, disco duro, tarjetas de red,…) y el comportamiento que tendrán estos recursos (modo de operación de las tarjetas de red, reserva de memoria del disco duro dinámica o estática, aceleración 3D en la tarjeta gráfica,…). Una vez creadas y configuradas las máquinas virtuales, se instalarán los diferentes sistemas operativos que serán invitados. Estos mismos, junto con algún software extra que se instalará en algunos de ellos, serán configurados para poner a prueba el sistema de red diseñado.

Se comienza constituyendo los sistemas operativos, en los cuales se realizará la configuración de direcciones IP que, a poder ser, serán fijas. También se configurarán las reglas de enrutamiento necesarias, se desactivarán los sistemas de seguridad implementados por defecto en algunos invitados, y cualquier otra configuración pertinente que dependa del invitado. Una vez estas configuraciones del invitado estén finalizadas, se instalarán las diferentes aplicaciones de terceros que se necesiten en cada equipo, como por ejemplo un analizador de tráfico como Wireshark, un servidor web y un servidor ftp.

En el diseño de red se proponen dos escenarios independientes, cada uno de ellos con una misión diferente. En el primer escenario se simula una red de paquetes con varios nodos finales, así como varios nodos que actúan como enrutadores. Estos paquetes viajarán por distintos nodos hasta alcanzar el nodo final siguiendo el paquete de respuesta del mismo, trazando un camino diferente al seguido en el paquete de envío hacia el inicial. En cambio el segundo escenario, consta de un firewall que gestiona tres zonas de seguridad distintas entre las que se comparte información. Se ha de tener en cuenta que las peticiones de esa información únicamente se permiten hacer desde una de las zonas con un nivel de seguridad superior a la que se le realiza la petición, exceptuando la zona desmilitarizada, que es la única que acepta peticiones desde una zona de seguridad con un nivel de seguridad más bajo.

2. INTRODUCCIÓN

2.1. CONCEPTO DE VIRTUALIZACIÓN

Este concepto hace referencia a la abstracción de los recursos de un ordenador y su puesta en funcionamiento como máquina virtual en otra máquina física. Un sistema de virtualización debe ser capaz de ofrecer una interfaz en el anfitrión para poder interactuar con el sistema operativo de la máquina virtual, o invitado. Además, el anfitrión debe ser capaz de ofrecer una serie de recursos a la máquina virtual para que esta pueda utilizarlos. De estas interfaces de comunicación se encarga un monitor de máquina virtual, que se instala en el anfitrión y desde donde se pueden ejecutar las máquinas virtuales [1].

2.2. BREVE HISTORIA DE LA VIRTUALIZACIÓN

La virtualización es una tecnología que fue desarrollada por IBM en los años 60. El primer ordenador diseñado específicamente para virtualización fue el mainframe IBM S/360 Modelo 67. Esta característica de virtualización ha sido un estándar de la línea que siguió (IBM S/370) y también en sus sucesoras (incluyendo la serie actual).

Fueron muy populares durante los 60 y los 70, pero estas máquinas virtuales desaparecieron prácticamente durante las décadas de los 80 y los 90. No fue hasta el final de los 90 cuando volvió a resurgir la tecnología de las máquinas virtuales [2]. Los actos más relevantes desde entonces, han sido los siguientes [3]:

- 1998: se funda la empresa VMware.
- 1999: VMware lanza su primer producto, VMware Workstation.
- 2003: se lanza la primera versión de Xen.
- 2005: Intel introduce su tecnología VT-x (Vanderpool) en arquitecturas x86.
- 2006: AMD introduce su tecnolog´ıa AMD-V (Pacifica).
- 2007: KVM se integra en la rama oficial del kernel de Linux 2.6.20.
- 2007: VirtualBox Open Source Edition (OSE) se libera como software libre.
- 2008: Qumranet, la empresa detrás de KVM, es comprada por Red Hat.
- 2008: Innotek, la empresa detrás de Virtual Box, es comprada por Sun Microsystems.

- 2008: VMware decide convertir VMware ESXi en freeware.
- 2008: Microsoft lanza la versión final de Hyper-V.
- 2010: VirtualBox pasa a llamarse Oracle VM VirtualBox.
- 2011: se empiezan a incluir ciertas partes de Xen en la rama oficial del kernel de Linux 2.6.37. Integración completa en la versión 3.0.

2.3. VENTAJAS Y BENEFICIOS DE LA VIRTUALIZACIÓN

Hoy día, y gracias en parte a la situación actual que estamos atravesando, la gran mayoría de empresas (independientemente del sector en el que operen) están muy concienciadas con el ahorro de costes. Es por esto por lo que el ahorro en sistemas virtualizados (con respecto a los sistemas físicos) ha sido una de las cuestiones por las cuales más se han interesado las empresas en la virtualización, ya que donde antes se necesitaban dos máquinas ahora solamente es necesario utilizar una. A todo esto hay que añadir que además es mucho el tiempo que se ahorra gracias a la facilidad de administración y de clonación de los discos duros virtuales (que se realizarán como cualquier otro archivo) con todas las ventajas que esto tiene asociado.

Sin lugar a dudas, la seguridad de estos sistemas virtualizados ha sido otra motivación para el estudio e implantación de los mismos. Si por ejemplo se quisiera probar versiones beta o programas de software que pensamos que serán útiles, tal vez interese virtualizar un sistema para realizar todas estas instalaciones en el sistema virtual y dejar nuestro sistema anfitrión limpio, instalando sólo aquello que definitivamente vamos a usar.

Sin dejar de lado la seguridad, también se ha de resaltar que es muy frecuente encontrar empresas interesadas en crear un sistema aislado donde las únicas conexiones con internet se hagan en entornos seguros y donde la navegación sea de confianza. Muchos coinciden en señalar la virtualización como una excelente estrategia de seguridad al momento de elaborar un *backup plan* o un *disaster recovery plan*.

En cuanto a la compatibilidad de software, también es interesante usar virtualización ya que a veces no es posible encontrar el programa que se necesita para los sistemas operativos Linux o Mac; por lo que la solución sería la de instalar Windows o buscar otra alternativa. Afortunadamente este tipo de cosas cada vez pasan menos, pero continúan pasando, con lo cual tener virtualizado Windows dentro de un Mac o Linux puede ahorrar una buena cantidad de problemas y tiempo buscando el equivalente de un programa para estos sistemas.

Las configuraciones también se simplifican ya que la gestión se centraliza en el nodo anfitrión, desde donde se realizarán todas las configuraciones de las distintas máquinas virtuales alojadas en este.

Otra ventaja a destacar es que existe un consumo menor de energía y un ahorro de espacio considerable, ya que no se necesita un equipo físico por cada sistema operativo o estación de trabajo. Con la virtualización el consumo de recursos y energía se reduce porque únicamente existe un hardware muy potente que aloja todo el entorno virtual, que aunque consume bastante energía, esta es mucho menor que el consumo generado en el caso de tener todos los recursos virtualizados físicamente.

Para acabar con este apartado, es justo señalar que la protección contra errores de hardware también juega un papel importante, ya que uno de los mayores problemas que se le puede presentar a un administrador de sistemas es que falle un componente crítico del servidor, el disco duro por ejemplo. Si esto ocurriese, la única solución es la de sustituir este elemento fallido y habría que reinstalar todo el sistema operativo, configurarlo, instalar los programas, y cargar las copias de seguridad para poder seguir trabajando. Aunque para alguien experto no supondría un gran problema, todo esto tiene un coste en tiempo y esfuerzo bastante elevado. Sin embargo, si se está trabajando con máquinas virtuales y falla el servidor, se podrá sustituir o copiar las máquinas virtuales y posteriormente arrancarlas. Esta solución no supondría ni una décima parte de tiempo que si se tuviera que reconfigurarlo todo como ya se detalló en renglones anteriores. [4] [5] [6]

3. OBJETIVOS

El objetivo principal de este trabajo fin de grado es la familiarización con el software de virtualización VirtualBox y el estudio en profundidad de todo el sistema de simulación de red que este software ofrece. También es objetivo del trabajo realizar pruebas con diferentes configuraciones de red, y para ello se ha propuesto un diseño que trata de la configuración y puesta en marcha de un sistema de red. En este se realizarán saltos de paquetes entre diferentes enrutadores existentes en el escenario, así como un sistema de seguridad que cuenta con un firewall con varias redes y donde se aplican las políticas de seguridad necesarias para poder tener acceso a ciertas zonas y restringir el acceso a otras. Todo ello, obviamente, implementado en un entorno totalmente virtual.

En el desarrollo del trabajo se proponen la consecución de los siguientes objetivos:

- Instalación de un software de virtualización (VirtualBox) en el anfitrión.
- Creación de máquinas virtuales dimensionadas en base a los requisitos del sistema del host invitado.
- Elegir la configuración de red adecuada en la máquina virtual para poder realizar el diseño que se especifica y que este funcione.
- Instalación de los diferentes sistemas operativos en las máquinas virtuales.
- Configurar los nodos invitados para ponerlo en funcionamiento y que puedan establecer conexión con los demás equipos que precisen conexión.
- Configurar las tablas de rutas, políticas de seguridad y demás configuraciones propias del sistema operativo que sean necesarias.
- Instalar y configurar software de terceros, como un servidor web, un servidor FTP y un analizador de tráfico.
- Realizar pruebas para comprobar que la configuración de la red cumple con los requisitos del diseño.

4. MATERIALES Y MÉTODOS

4.1. CARACTERÍSTICAS TÉCNICAS

4.1.1. MÁQUINA FÍSICA

El monitor de máquina virtual, VirtualBox, está alojado en un Toshiba Satellite A-300 con las siguientes características técnicas [7]:

Tecnología	Tipo: Tecnología de procesador Intel® Centrino® 2 con Procesador Intel® Core™2 Duo P8400, chipset Intel® PM45 Express e Intel® WiFi Link 5100 Velocidad de reloj: 2.26 GHz Front side bus: 1066 MHz Caché de 2º nivel: 3 MB
Sistema operativo / plataforma	**Debian 8 Jessie**
Memoria principal	Estándar: 8,192 (4,096 + 4,096) MB Tecnología: DDR2 RAM (800 MHz)
Disco duro	Capacidad formateado: 1 TB Velocidad de rotación: 7.200 rpm
Pantalla	Tamaño: 15,4 " Tipo: Pantalla Toshiba TruBrite® WXGA Resolución: 1.280 x 800
Adaptador Gráfico	Tipo: ATI Mobility Radeon™ HD 3470 con soporte Tecnología HyperMemory™ Memoria: 256 MB de VRAM dedicada (hasta 2.046 MB total disponible de memoria de gráficos usando la tecnología HyperMemory ™ con 4 GB de memoria del sistema) Tipo de memoria: GDDR2 (500 MHz) Video RAM (resp. Video RAM y memoria de sistema combinada) Conexión del bus: 16x PCI Express
Modos de vídeo interno	Los siguientes modos internos de vídeo son compatibles: : Resolución: 1.280 x 800
Modos de vídeo externo (Max)	Resolución máxima: 2.048 x 1.536 Máxima frecuencia de refresco: 85 Hz Resolución no entrelazada con la máxima frecuencia de refresco: 1,600 x 1,200
Comunicaciones sin cables	Wireless Technology: Wireless LAN (802.11a/g/Draft-N) Version: Intel® WiFi Link 5100
Comunicaciones con cables	Tipología: Fast Ethernet LAN Velocidad: 10BASE-T/100BASE-TX

Tabla 4.1.1.1: Descripción técnica de la máquina física

4.1.2. MÁQUINAS VIRTUALES

En este apartado se describirán los requisitos mínimos que tiene cada host invitado usado en la implementación con el fin de dimensionar cada máquina virtual en base a esas circunstancias. En el caso que se aprecie que los requisitos mínimos no son suficientes, sería necesario cambiar la configuración y aumentar las características técnicas de la máquina virtual en cuestión.

4.1.2.1. UBUNTU SERVER 14.04

Ubuntu Server es la versión para servidores de Ubuntu, y el sistema operativo de Canonical basado en Linux. Canonical, lo ofrece de manera gratuita y se financia por medio de servicios vinculados al sistema operativo y del soporte técnico. Cada seis meses se publica una nueva versión de Ubuntu, y durante los siguientes dieciocho meses Canonical ofrece soporte en forma de actualizaciones de seguridad, parches para errores críticos y actualizaciones menores de programas. Llegados a este punto, cabe destacar que las versiones LTS (Long Term Support o Soporte de Larga Duración) se liberan cada dos años y reciben soporte durante cinco años.

Velocidad del procesador	Memoria RAM	Capacidad de disco duro
1 GHz	512 MB	1,75 GB

Tabla 4.1.2.1.1: Requisitos mínimos de Ubuntu Server 14.04 [8]

4.1.2.2. UBUNTU DESKTOP 14.04

En el sistema operativo que nos ocupa predomina su facilidad de uso e instalación. También es destacable la libertad de los usuarios así como los lanzamientos regulares, siendo estos dos anuales.

El eslogan de Ubuntu, ***Linux para seres humanos****,* resume a la perfección lo anteriormente explicado: “hacer de Linux un sistema operativo más accesible y fácil de usar”.

Velocidad del procesador	Memoria RAM	Capacidad de disco duro
700 MHz	512 MB	5 GB

Tabla 4.1.2.2.1: Requisitos mínimos de Ubuntu Desktop 14.04 [9]

4.1.2.3. WINDOWS XP PROFESSIONAL SERVICE PACK 3

Esta versión de Microsoft Windows representa el sistema operativo más avanzado de Microsoft y fue lanzado al mercado el 25 de octubre de 2001. Dispone de versiones para varios entornos informáticos (PC domésticos o de negocios), incluyendo obviamente también a los equipos portátiles, netbooks, tabletas y centros multimedia. Sucesor de Windows 2000 junto con Windows ME, y antecesor de Windows Vista; es el primer sistema operativo de Microsoft orientado al consumidor que se construye con un núcleo y arquitectura de Windows NT disponible en versiones para plataformas de 32 y 64 bits.

Velocidad del procesador	Memoria RAM	Capacidad de disco duro
300 MHz	128 MB	1,5 GB

Tabla 4.1.2.3.1: Requisitos mínimos de Windows XP Professional SP3 [10]

4.1.2.4. IP-FIRE V.2.17

IP-Fire es una distribución muy probada que incluye componentes bastante maduros. Ofrece protección a una red independientemente de sus dimensiones, por lo que es apta tanto para redes domésticas como para grandes redes corporativas. IP-Fire tiene el foco puesto en la seguridad, la estabilidad y la facilidad de configuración; y para ello incluye múltiples herramientas que añaden nuevas características al software base.

Su diseño gira en torno a la flexibilidad y la modularidad haciendo posible su puesta en servicio para entornos con necesidades muy distintas. Lo mismo proporciona un cortafuegos que un servidor proxy o una VPN. De esa forma se consigue que la instalación quede ajustada exclusivamente al uso que se le va a dar.

El cortafuegos que se incluye usa SPI (Stateful Packet Inspection) y funciona sobre netfilter, el filtro de paquetes de Linux [11].

Velocidad del procesador	Memoria RAM	Capacidad de disco duro
1 GHz	512 MB	2 GB

Tabla 4.1.2.4.1: Requisitos mínimos de IP-Fire v.2.17 [12]

4.2. MÉTODOS SEGUIDOS EN LOS ESCENARIOS PLANTEADOS

4.2.1. CONFIGURACIÓN DE VIRTUAL BOX

Antes de comenzar, es justo aclarar que para que los escenarios propuestos se puedan desarrollar se tiene que tener un buen conocimiento sobre los modos de operación de red en VirtualBox versión 4.3.18, los cuales se pueden conocer y estudiar en los manuales disponibles en su página oficial. Aunque la creación de la máquina virtual es muy intuitiva con este software, el tema de las configuraciones de redes virtuales resulta ser algo más complejo debido a los diferentes modos de operación de las tarjetas de red que se ofrecen en VirtualBox.

En primer lugar se configura el entorno de virtualización, se crea la máquina virtual y se le asignan unos recursos específicos dependiendo del sistema que vaya a soportar y del uso que le vayamos a dar.

A continuación se configura la red con varios modos de operación diferentes. Aunque afortunadamente hay algunas opciones en común para todos sus modos de operación, como *Habilitar adaptador de red*, sirviendo para activar o desactivar el adaptador de red configurado en esa máquina virtual. Otra de las opciones en común es la regeneración de una nueva MAC. Muy útil si hemos importado una máquina virtual y la máquina desde la que se exportó está trabajando en la misma red porque se podrían duplicar las direcciones físicas.

Por último, hay una opción en común más que da la posibilidad de seleccionar el tipo de adaptador. Actualmente se ofrecen 6 tipos de adaptadores:

- AMD PCNet PCI II (Am79C970A)
- AMD PCNet FAST III (Am79C973, por defecto)
- Intel PRO/1000 MT Desktop (82540EM)
- Intel PRO/1000 T Server (82543GC)
- Intel PRO/1000 MT Server (82545EM)
- Red paravirtualizada (virtio-net)

VirtualBox también permite utilizar un controlador de red paravirtualizado, es decir, un software de red específico para el sistema de virtualización en lugar de una simple emulación. Concretamente se puede elegir como interfaz de red el controlador Virtio-Net, que es un software libre del proyecto KVM. Es en la propia página de KVM donde se pueden obtener controladores para Linux y para Windows; aunque la mayoría de

distribuciones de Linux ya proveen estos controladores por sí mismas. La ventaja de este tipo de controlador es que se simplifica el trabajo extra que VirtualBox hace para emular el hardware, dado que Virtio está pensado específicamente para usarse en sistemas virtualizados y no corresponde a ningún hardware real [13].

. A continuación se describen los modos de operación de red que ofrece este software:

- **No conectado**

Con esta opción la tarjeta de red está instalada en el nodo invitado, aunque esta no dispone de conectividad. Con otras palabras, actúa como si de una tarjeta de red sin cable introducido o con un cable cortado se tratase [14].

- **NAT (Network Address Translation)**

Network Address Translation (NAT) es una técnica propia de los enrutadores IP para interconectar equipos que no tienen direcciones IP compatibles entre sí.

Generalmente los equipos a un lado del enrutador utilizan direcciones públicas (válidas para conectar a Internet), mientras que los del otro lado utilizan direcciones privadas (únicamente pueden usarse dentro de una red local). A mismo tiempo, el enrutador traduce automáticamente las direcciones de los paquetes a medida que pasan de un lado a otro y viceversa.

VirtualBox propicia que el anfitrión funcione de manera similar a un enrutador, dando acceso a una o varias máquinas virtuales a través de la propia dirección IP del anfitrión.

El sistema NAT de VirtualBox incluye un servicio de DHCP que asignará a cada máquina su dirección IP privada, generalmente de la forma 10.0.X.X. La primera X corresponde a la tarjeta de la máquina virtual (empezando por 2 y aumentado en una unidad por cada red virtual configurada en modo NAT. Por ejemplo la primera tarjeta de red configurada en una máquina virtual en modo NAT obtendría la dirección 10.0.2.X) y la segunda tarjeta de red obtendría la dirección 10.0.3.X, y así sucesivamente). Este rango de direcciones IP están reservados por los organismos de control de Internet para que nunca se usen fuera de las redes locales, asegurándose de este modo que nunca van a coincidir con la de ningún otro equipo de Internet. El host invitado que contenga la máquina virtual con la red en modo NAT deberá estar esperando la configuración mediante DHCP, de lo contrario esta configuración no sería válida.

Como se puede comprobar, a pesar de que el NAT es un modo complejo internamente, es el más fácil de usar dado que no requiere configurar nada especial ni en los invitados ni en el anfitrión.

Un inconveniente (o ventaja según se mire) de este modo de operación es que, de la misma manera que en los enrutadores reales, no permite las conexiones entrantes que puedan provenir del exterior de la interfaz anfitrión. Esto es consecuencia del propio funcionamiento del NAT porque al estar compartiendo varias máquinas la misma dirección IP pública, el sistema no tiene manera de identificar a qué máquina corresponde la conexión que está entrando, salvo que se haya hecho previamente una tabla de asignación de puertos (port forwarding). [13] [14]

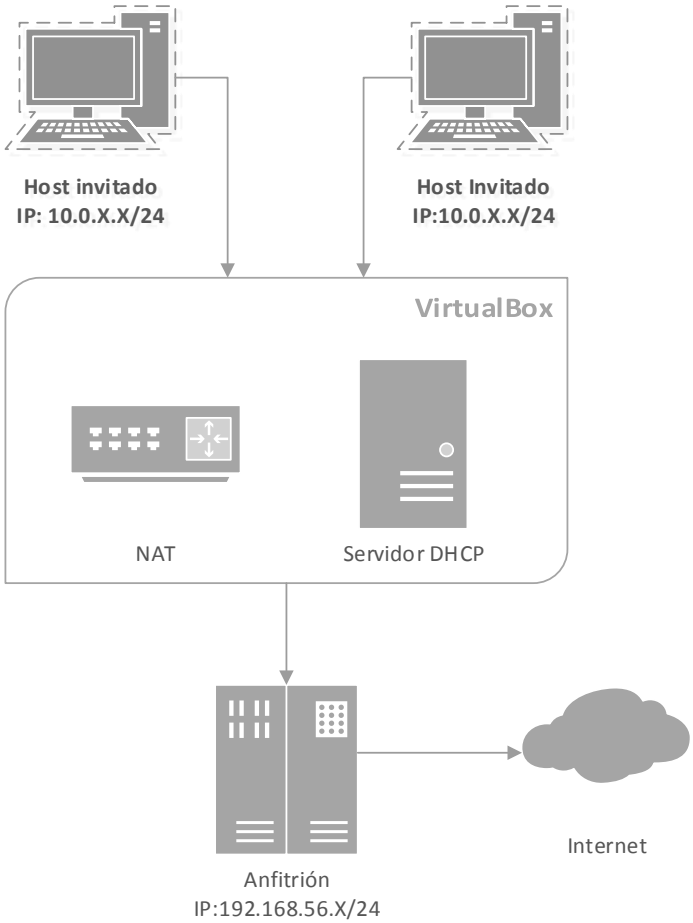


Figura 4.2.1.1: Esquema de red y direccionamiento IP de una configuración NAT en VirtualBox

- **Adaptador Puente.**

Cuando se selecciona este modo en la configuración de una máquina virtual, se muestra una lista de las interfaces de red que tiene el anfitrión para que asignemos cuál de ellas se va a ser la encargada de gestionar y compartir con la red virtual su capacidad. A partir de ese momento, VirtualBox accederá a la interfaz seleccionada y la pondrá en

un modo tal que usará dos direcciones físicas (MAC): una real y otra virtual (se configura en la sección *Avanzadas*).

Cada una de las direcciones MAC podrá tener asociada una dirección IP. Lógicamente, se tiene que tener disponibles tantas direcciones IP libres como interfaces de red configuradas en modo puente en VirtualBox para poder acceder a la red en la que nos encontremos.

Si por el contrario estamos frente una red privada, el enrutador asignará una dirección privada a cada MAC, como si se tratara de interfaces separadas. En este caso, dado que se cuenta con una interfaz que accede directamente a la red, es posible tener conexiones salientes y entrantes de la misma manera que si se tratara de una máquina física.

Por tanto, este sería el modo adecuado si queremos que la máquina ofrezca servicios a la red [13]. El esquema y el direccionamiento de la red se muestran en la figura 4.2.1.2. Las direcciones IP, que se muestran en la figura 4.2.1.2, pueden variar dependiendo del rango de direcciones que tengamos configurado en el enrutador. Para una mejor comprensión, se han configurado estas direcciones de ejemplo simplemente para que se entienda la dinámica de funcionamiento de este modo de operación de red.

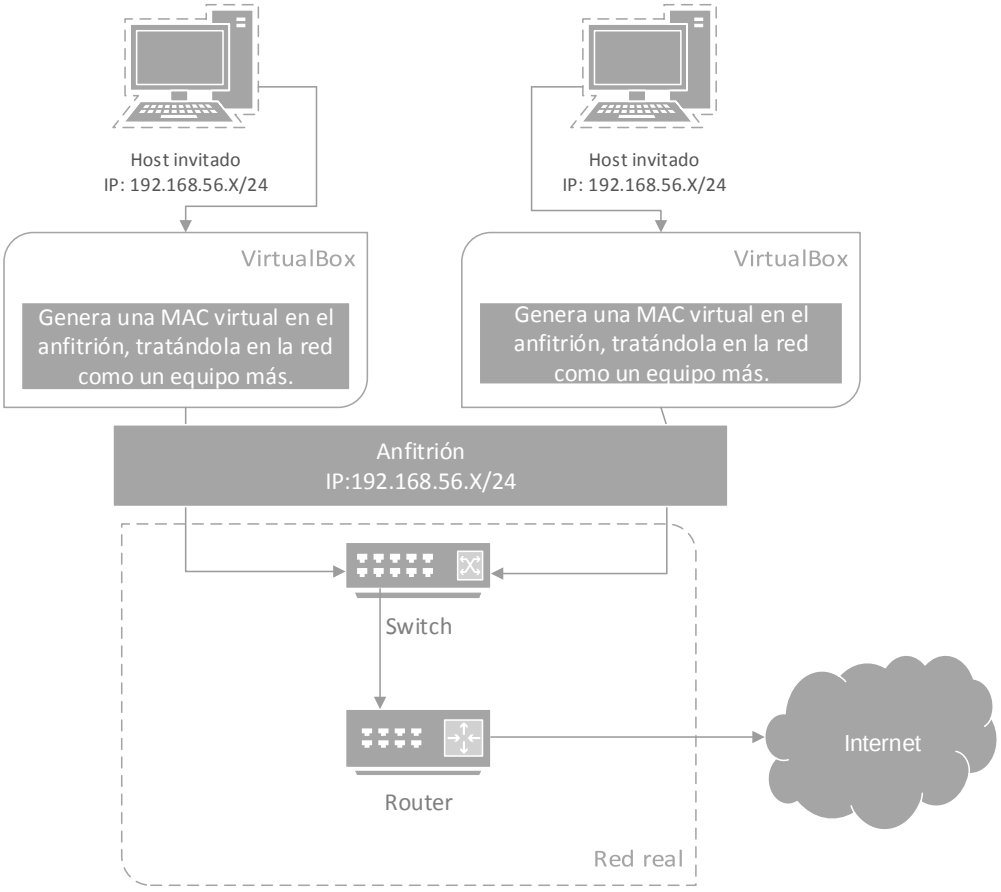


Figura 4.2.1.2: Esquema de red y direccionamiento IP de una configuración Puente en VirtualBox

- **Red Interna**

En este modo de operación las máquinas virtuales pueden comunicarse entre sí siempre que estén configuradas con el mismo nombre de red interna. Esta dinámica de trabajo es muy similar a la del modo de configuración puente, ya explicado, pero trae algunas ventajas de seguridad añadidas. En modo puente todo el tráfico viaja por la red a través de la interfaz física configurada en el anfitrión pudiendo ser capturada por un analizador de tráfico que esté instalado en la red. Si se prefiere tener varias máquinas virtuales comunicadas entre sí y evitar que el tráfico pueda ser analizado por alguien externo este sería la mejor configuración.

Cada red interna es identificada únicamente por su nombre; por tanto, si se quiere conectar varias máquinas virtuales en la misma red interna, habrá que asignarle el mismo nombre a la hora de configurar el apartado de red en VirtualBox. Al existir más de una máquina virtual configurada en modo red interna y con el mismo nombre de red se simularía el trabajo de un switch [14].

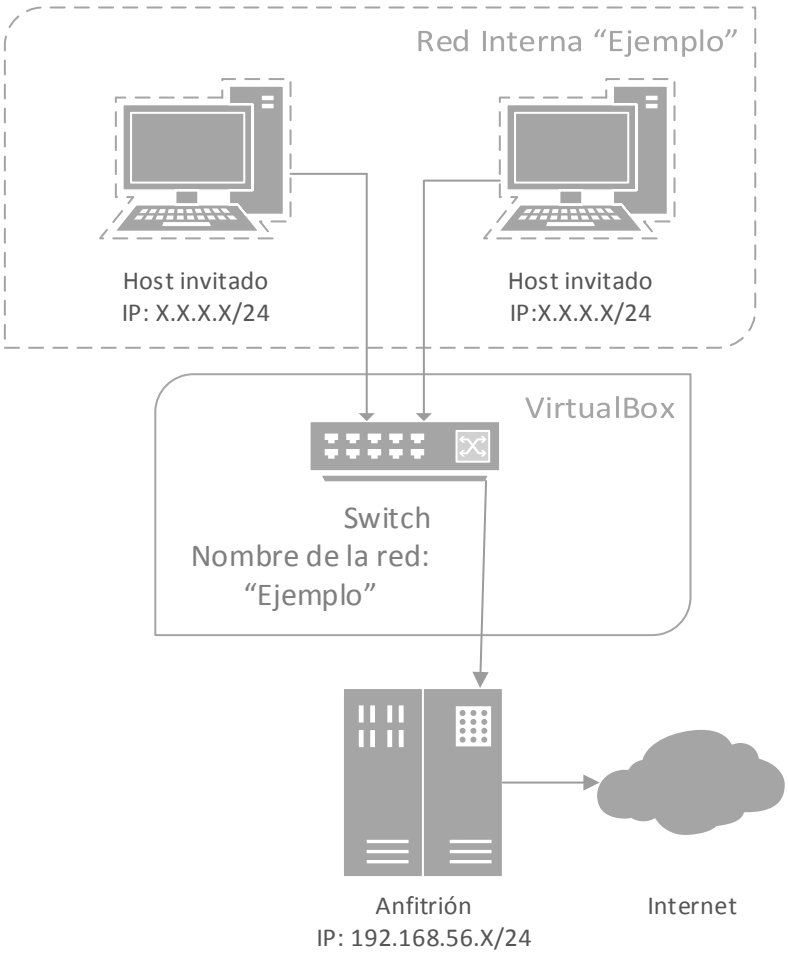


Figura 4.2.1.3: Esquema de red y direccionamiento IP de una configuración Red Interna en VirtualBox

- **Adaptador sólo-anfitrión**

Este modo de operación de red de VirtualBox puede ser pensado como un “híbrido” entre los modos de operación puente y de red interna. Como puente, la máquina virtual puede comunicarse con el anfitrión como si ambos estuvieran conectados a un switch, pero únicamente con el host anfitrión dentro de la red real. En cambio, con el resto de equipo de la red real no se podrá establecer comunicación alguna. La explicación de esto es porque en el nodo anfitrión se crea un adaptador virtual, además del adaptador físico que hay instalado, y este a su vez está conectado internamente con el adaptador de la máquina virtual configurado en modo sólo anfitrión. Lo que lo asemeja a la configuración de red interna es que todas las máquinas virtuales con adaptadores configurados en este modo de operación pueden establecer conexión entre sí, además de tener conectividad con el nodo anfitrión. Todo esto se puede apreciar en la figura 4.2.1.4, que representa una esquematización de este modo de operación de red en VirtualBox. Hay que aclarar, que las direcciones IP que se muestran en dicha figura pueden variar dependiendo del rango de direcciones que tengamos configurado en el enrutador. Se han configurado estas direcciones de ejemplo, simplemente para poder entender la dinámica de funcionamiento de este modo de operación de red [14].

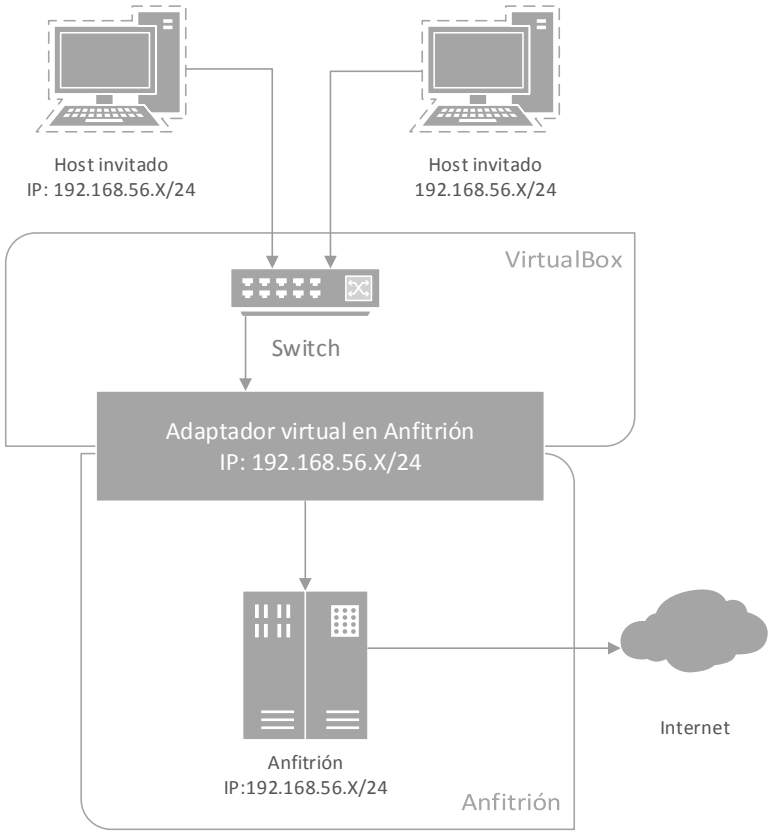


Figura 4.2.1.4: Esquema de red y direccionamiento IP de una configuración Sólo Anfitrión en VirtualBox

Otra herramienta muy útil de VirtualBox son las Guest Additions. Se trata de módulos, controladores y aplicaciones del sistema que mejoran el rendimiento y la usabilidad de la máquina virtual. Estas ya están alojadas en el servidor y simplemente hay que instalarlas en el servidor virtualizado [15].

Las mejoras que presentan son:

- Mejor integración con el mouse
- Carpetas compartidas entre el servidor y la máquina virtual
- Mejor soporte de vídeo
- Mejores canales de comunicación entre el servidor y la máquina virtual
- Mejor sincronización de la hora de la máquina virtual con el servidor
- Compartición del portapapeles entre Anfitrión e Invitado

4.2.2. ESCENARIO 1 – DISEÑO DE UNA RED DE PAQUETES

4.2.2.1. DESCRIPCIÓN DEL ESCENARIO

En este escenario se cuenta con tres hosts invitados con Ubuntu Server que actúan como enrutadores, otros tres host invitados con Windows XP, que actúan como equipos finales; y seis redes virtuales (E1, E2, E3, I1, I2 e I3). Se describe gráficamente el escenario en la figura 4.2.2.1.1.

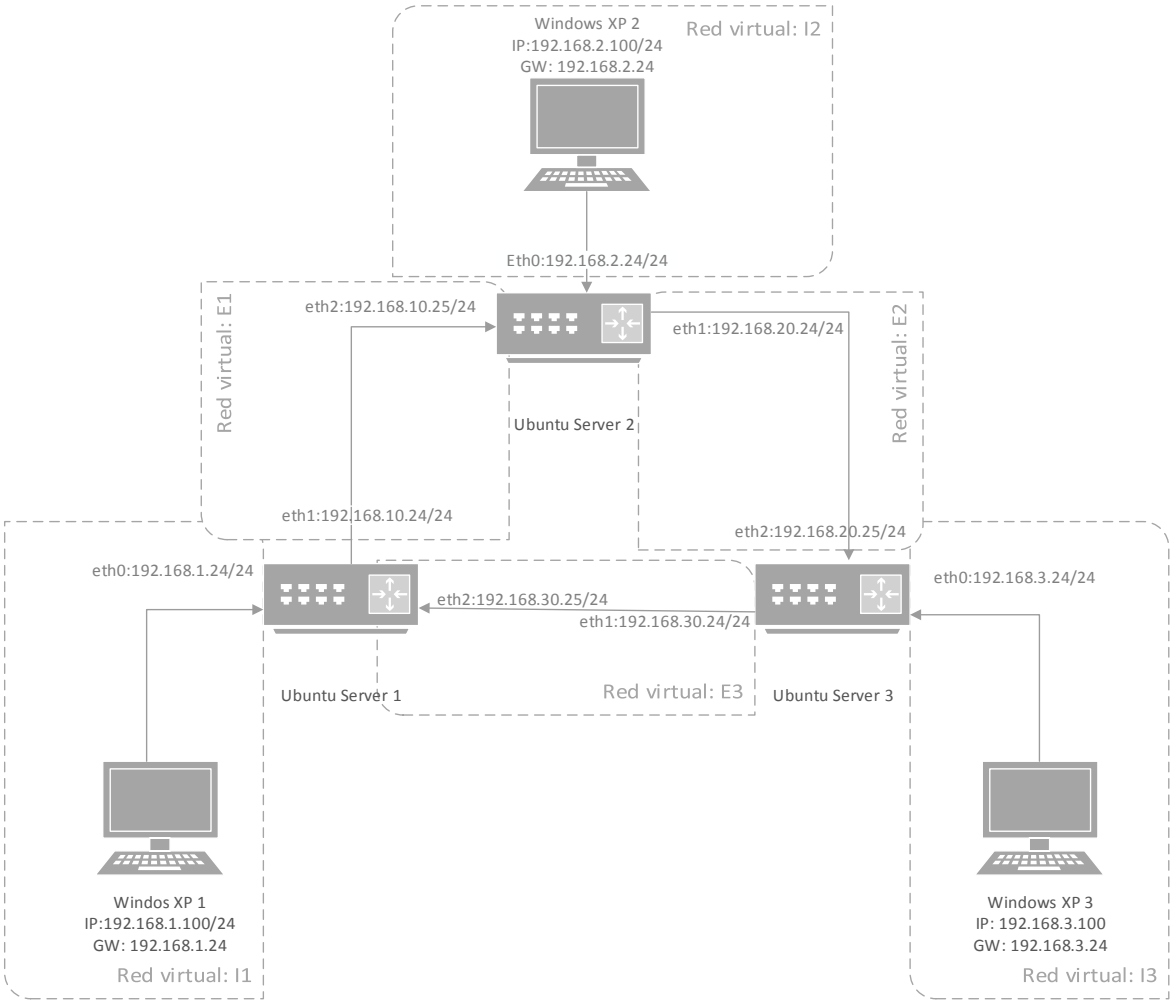


Figura 4.2.2.1.1: Descripción del escenario 1- Red de paquetes

La sugerencia de funcionamiento que se propuso para de este escenario se basa en que cualquier paquete generado por algún equipo final del escenario tiene que viajar en el sentido de las agujas del reloj (tomando como referencia el escenario que anteriormente se muestra). Es decir, si se quisiera hacer ping (ICMP Echo Request) desde el equipo Windows XP 1 hacia el equipo Windows XP 3, entonces el paquete de petición ICMP tendría que viajar a través del enrutador Ubuntu Server 1 para luego pasar por el enrutador Ubuntu Server 2 seguido por Ubuntu Server 3, llegando finalmente al destino final Windows XP 3. En este caso, la respuesta (ICMP Echo Reply) que genera el equipo Windows XP 3 tendría que viajar por el enrutador Ubuntu Server 3 y por el enrutador Ubuntu Server 1 antes de alcanzar su destino final Windows XP 1; comprobando así que el tráfico sigue el sentido de las agujas de reloj tal y como se había planteado.

4.2.2.2. CONFIGURACIÓN DE RED

Para la creación de las redes virtuales se han configurado todas las máquinas virtuales con todos sus interfaces de red y con el modo de operación *red interna*. Se ha elegido este modo de funcionamiento porque es el único modo de operación que nos permite crear tal variedad de redes sin disponer de una infraestructura física que pueda simular este esquema de red. En caso de poseer infraestructura física para implementar el escenario descrito podrían haberse configurado otros modos de operación como el modo *puente*.

La configuración de la máquina virtual que aloja al invitado Ubuntu Server 1 se puede apreciar en la figura 4.2.2.2.1. En el resto de equipos habrá que configurarlos de esta misma forma, pero obviamente con sus correspondientes nombres de red.

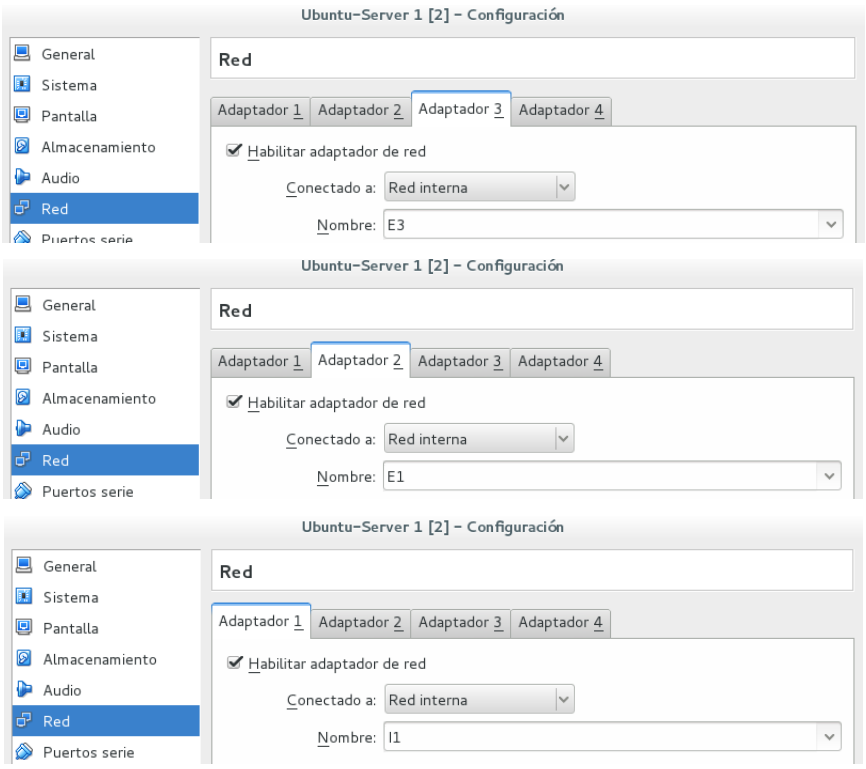


Figura 4.2.2.2.1: Modo de funcionamiento *Red Interna* y asignación del nombre de red virtual en las tres interfaces de la máquina virtual que aloja el host invitado Ubuntu Server 1

Si se pretende que los paquetes puedan conmutar de una red a otra, dentro de los enrutadores; habrá que activar el reenvío de paquetes, que en Ubuntu Server y en Linux (en general), viene desactivado por defecto. Esta opción posibilita reenviar información de la red desde una interfaz a otra. En el escenario planteado se necesita esta opción, o de lo contrario el enrutador no cumplirá su función. Para poder comprobar que está activada,

se tiene que consultar la variable del núcleo sysctl net.ipv4.ip_forward. Dicha variable puede ser consultada con el siguiente comando:

```
sysctl net.ipv4.ip_forward
```

Y se obtendrá como respuesta:

```
net.ipv4.ip_forward = 0
```

O

```
net.ipv4.ip_forward = 1
```

Si el resultado es igual a cero significa que esta opción esta desactivada. Para activarla de manera permanente y mantener los cambios después del reinicio de la máquina se han de seguir los siguientes pasos [16]:

Editamos el fichero sysctl.conf ubicado en /etc donde se añade una línea que contiene **net.ipv4.ip_forward = 1**

```
/etc/sysctl.conf:
net.ipv4.ip_forward = 1
```

Si la línea ya existía y pone 0 como valor, se cambia el valor a 1. Si la línea está comentada con un **#**, simplemente descomentamos la línea quitando la almohadilla.

Para activar los cambios realizados en el archivo sysctl.conf ejecutaremos el comando:

```
sysctl -p /etc/sysctl.conf
```

Por otro lado debido a que la topología de este escenario es en anillo se deberá desactivar un filtro de paquetes que tiene configurado el kernel de Linux para que no descarte los paquetes que viajan a través de la red. Este filtro de paquetes implementado en Linux trata de evitar ataques ARP Spoffing, un tipo de ataque que se basa en cambiar la dirección física de la interfaz de red del atacante para hacerse pasar por un miembro de la red para obtener beneficios de manera maliciosa. La forma de comprobar esto en este sistema (Ubuntu Server) y en Linux en general es comprobar en su tabla de rutas que existe una ruta específica para establecer contacto con la red desde la que se reciben los paquetes, si no existe dicha ruta descarta el paquete. Debido a la topología en anillo que presenta este escenario no existe una ruta directa desde el enrutador en el que se reciben los paquetes hasta la red desde la que se reciben esos paquetes (en el caso de la comunicación entre los enrutadores), por tanto si no configuramos este parámetro no se conseguirá realizar el enrutamiento que se describe en los requisitos del escenario [18].

Para desactivar este filtro de paquetes habrá que editar el fichero de configuración sysctl.conf:

```
sudo nano /etc/sysctl.conf
```

Y allí se decomentan las líneas net.ipv4.conf.default.rp_filter, net.ipv4.conf.all.rp_filter y se igualan a 0:

```
net.ipv4.conf.default.rp_filter=0
net.ipv4.conf.all.rp_filter=0
```

Una vez configurado el reenvío de paquetes y desactivado el filtro de paquetes, se hace lo propio con las IP's de los diferentes equipos que se han visto en la figura 4.2.2.1.1. En Ubuntu Server se harán mediante consola ya que por defecto, no trae instalada interface gráfica. Por esto se han de seguir estos pasos [17]:

```
sudo nano /etc/network/interfaces
```

Editando este fichero se configura la dirección. A continuación se muestra la configuración del equipo Ubuntu Server 1 para ver un ejemplo, ya que el resto de equipos Ubuntu Server se configurarán con la misma mecánica pero con sus direcciones pertinentes:

```
auto eth0
iface eth0 inet static
  address 192.168.1.24
  netmask 255.255.255.0
  network 192.168.1.0
  broadcast 192.168.1.255

iface eth1 inet static
  address 192.168.10.24
  netmask 255.255.255.0
  network 192.168.10.0
  broadcast 192.168.10.255

iface eth2 inet static
  address 192.168.30.25
  netmask 255.255.255.0
  network 192.168.30.0
  broadcast 192.168.30.255
```

Y por último, es necesario reiniciar el servicio de red para que así la configuración tenga efecto:

```
sudo /etc/init.d/networking restart
```

En Windows XP se puede configurar accediendo al Panel de control, conexiones de red y sobre el adaptador que se quiere configurar se cliquea con el botón derecho del ratón. En el menú desplegable que aparece marcamos propiedades, Protocolo Internet (TCP/IP) y ahí se configurará la dirección que se desee.

4.2.2.3. CONFIGURACIÓN DE ENCAMINAMIENTO

Lo primero que habrá que configurar en los equipos que actúan como enrutadores es el camino que deberán coger en el caso de que un paquete lleve una dirección que no se contemple en la tabla de rutas. Para ello habrá que especificar una puerta de enlace predeterminada con la ayuda del siguiente comando:

```
route add default gw XX.XX.XX.XX
```

La IP XX.XX.XX.XX variará en cada enrutador, siendo en cada uno de ellos las siguientes:

- Ubuntu Server 1: 192.168.10.25
- Ubuntu Server 2: 192.168.20.25
- Ubuntu Server 3: 192.168.30.25

Para que estas rutas permanezcan de manera indefinida habrá que adjuntarlas en el fichero de configuración de red ubicado en /etc/network/interfaces, previamente a añadir la línea habrá que escribir el prefijo post-up, para indicar que la ruta se añade después de levantar las interfaces de red. Quedarían así al final del fichero mencionado:

```
post-up route add default gw XX.XX.XX.XX
```

Las tablas de ruta de los diferentes equipos que actúan como enrutadores se muestran en las siguientes imágenes:

```
root@ubuntu-server:/home/user# route -n
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic Métric Ref    Uso Interfaz
0.0.0.0         192.168.10.25   0.0.0.0         UG    0      0        0 eth1
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Figura 4.2.2.1.2: Tabla de rutas del equipo Ubuntu Server 1

```
root@ubuntu-server:/home/user# route -n
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic Métric Ref    Uso Interfaz
0.0.0.0         192.168.20.25   0.0.0.0         UG    0      0        0 eth1
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Figura 4.2.2.1.3: Tabla de rutas del equipo Ubuntu Server 2

```
root@ubuntu-server:/home/user# route -n
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic Métric Ref    Uso Interfaz
0.0.0.0         192.168.30.25   0.0.0.0         UG    0      0        0 eth1
192.168.3.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Figura 4.2.2.1.4: Tabla de rutas del equipo Ubuntu Server 3

Con esto quedaría configurado el escenario 1.

4.2.2.4. PRUEBAS LLEVADAS A CABO EN EL ESCENARIO 1

Se realiza un ping desde el equipo con IP 192.168.1.100 hacia el equipo con IP 192.168.3.100 y se captura el tráfico que viaja a través de cada interfaz de salida de cada enrutador.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrador>
C:\Documents and Settings\Administrador>ping 192.168.3.100

Haciendo ping a 192.168.3.100 con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.3.100:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Documents and Settings\Administrador>
```

Figura 4.2.2.4.1: Ping hacia la dirección I 192.168.3.100

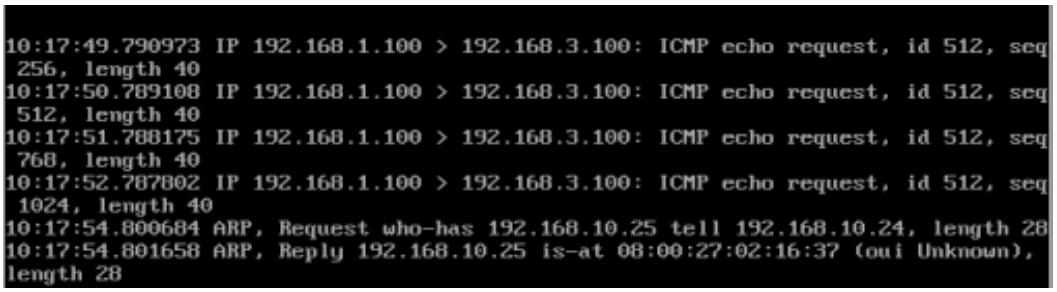


Figura 4.2.2.4.2: Captura de tráfico en la interfaz de salida (eth1) del enrutador Ubuntu Server 1

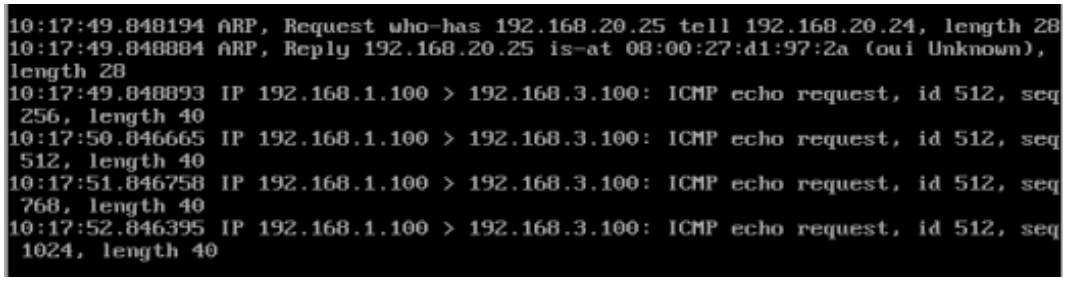


Figura 4.2.2.4.3: Captura de tráfico en la interfaz de salida (eth1) del enrutador Ubuntu Server 2

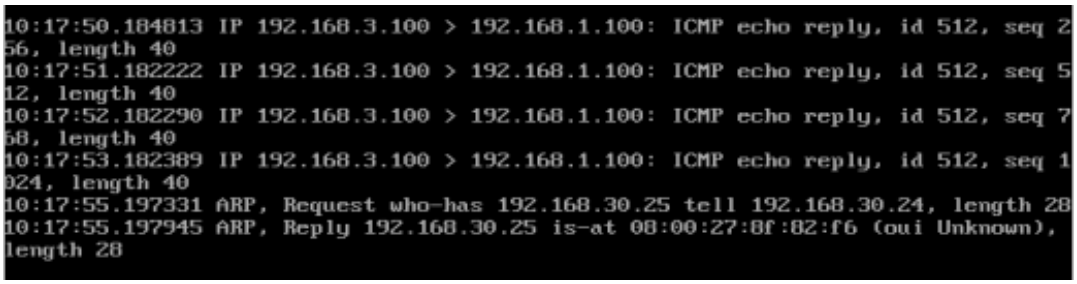


Figura 4.2.2.4.4: Captura de tráfico en la interfaz de salida (eth1) del enrutador Ubuntu Server 3

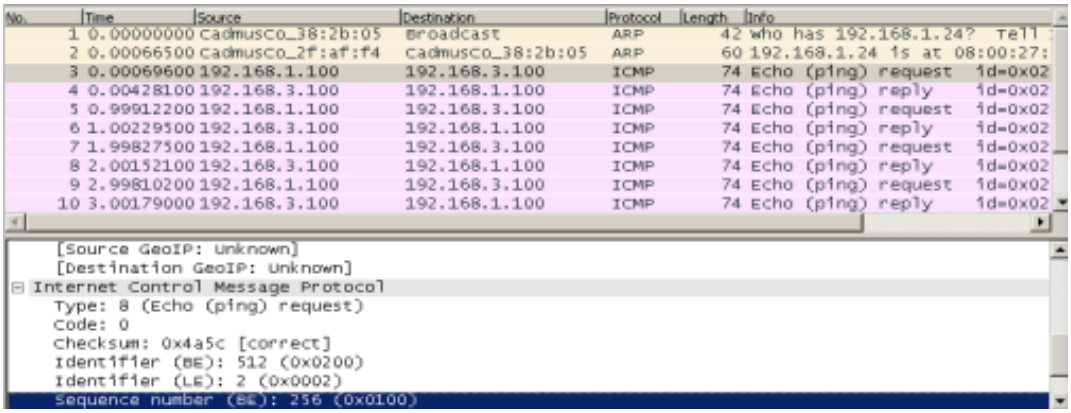


Figura 4.2.2.4.5: Captura de tráfico en la interfaz del equipo 192.168.1.100

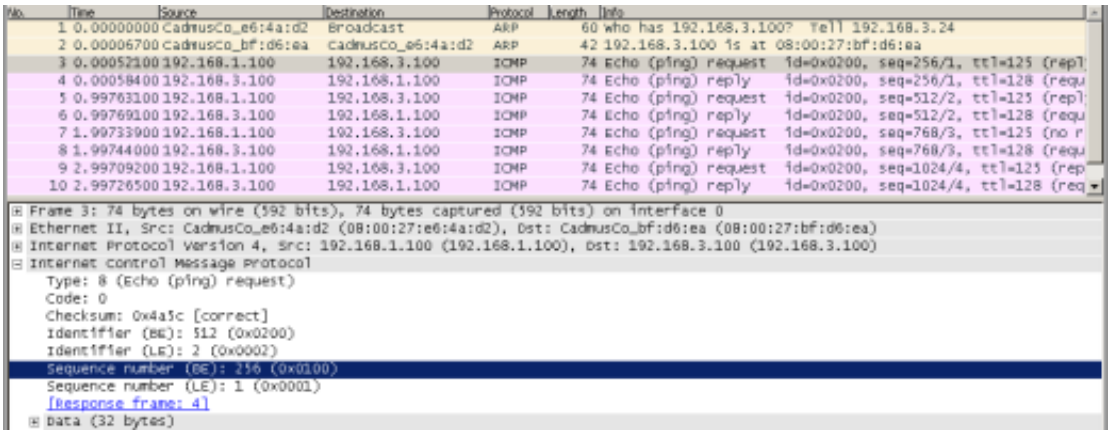


Figura 4.2.2.4.6: Captura de tráfico en la interfaz del equipo 192.168.3.100

Como se puede apreciar en las pruebas realizadas, se realiza un ping desde el equipo 192.168.1.100 hacia el equipo 192.168.3.100. El paquete llega hasta el primer enrutador (Ubuntu Server 1), luego pasa por el segundo enrutador (Ubuntu Server 2) y por último llega al tercer enrutador antes de alcanzar su destino. El paquete de respuesta que genera el equipo 192.168.3.100 viaja tan solo por el enrutador 2 y el enrutador 3 antes de alcanzar su destino, 192.168.1.100. Así se cierra el anillo, y se verifica que se está trabajando con una topología en anillo

4.2.3. ESCENARIO 2 – DISEÑO DE UNA RED CON VARIOS NIVELES DE PROTECCIÓN GESTIONADA POR UN FIREWALL

4.2.3.1. DESCRIPCIÓN DEL ESCENARIO

En este escenario se implementa un firewall,Ip-Fire versión 2.17, que será el que juegue un papel principal, ya que es el encargado de gestionar todas las conexiones permitiendo o denegando servicios, protocolos, haciendo NAT, redireccionando puertos y demás funciones que se le puedan exigir a un firewall.

Se cuenta con tres redes virtuales (GREEN, ORANGE Y RED). Cada una de ellas posee un nivel se seguridad diferente que serán explicados más adelante.

La red virtual RED se configura en el adaptador de la máquina virtual en modo de operación *puente*, simulando por tanto estar conectado físicamente al switch físico donde también está conectado el anfitrión.

En cambio, tanto la red ORANGE como la red GREEN están configuradas en modo de operación *red interna* para conseguir simular dos redes diferentes sin una infraestructura física.

En la zona ORANGE hay un servidor web implementado sobre un Windows XP que será accesible desde todas las redes. Y en la zona GREEN hay dos equipos, un host invitado con Windows XP y otro con Ubuntu, que no podrán ser accesibles ni por la red RED ni por la red ORANGE.

Por último se ha de indicar que a la zona RED se pueden conectar desde cualquier equipo físico (conectado al switch desde se conecta el anfitrión) o virtual. Para poder verlo todo de una forma más gráfica, se ha incluido el escenario en la figura 4.2.3.1.1.

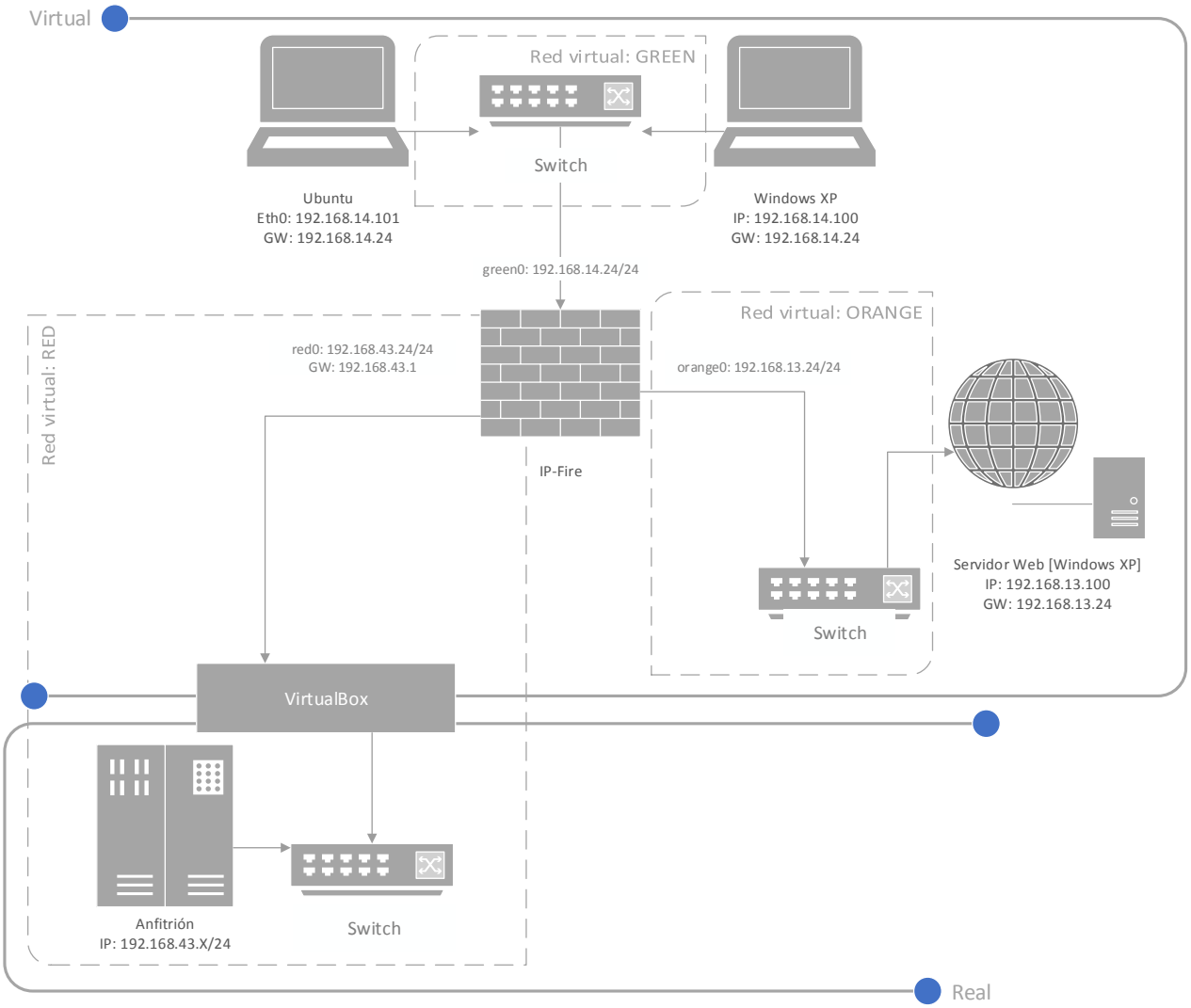


Figura 4.2.3.1.1: Descripción del escenario 2- Diferentes redes gestionadas por firewall

4.2.3.2. CONFIGURACIÓN DE RED

En todas las máquinas virtuales se configura un único adaptador excepto el firewall, (IP-Fire) que necesita tres adaptadores tal y como se puede ver en la figura 4.2.3.1.1. Uno para la red GREEN (configurado como red interna y que renombra la propia red), otro para la red ORANGE (configurado como red interna y que asigna el nombre de ORANGE a la red); y por último, otro para la red RED (configurado, en esta ocasión, como adaptador puente y con la salvedad de que este tipo de configuración no necesita ser renombrada ya que forma parte de la red real pasando a ser nuestro switch físico). Como vemos, cada máquina virtual tiene su adaptador configurado para pertenecer a la red virtual correspondiente tal y como se muestra en la figura 4.2.3.1.1.

Antes de finalizar este apartado, es justo matizar que las configuraciones IP no se explicarán porque apenas sufren variación y el procedimiento de configuración ya fue explicado con anterioridad en el apartado 4.2.2.2.

4.2.3.3. INSTALACIÓN Y CONFIGURACIÓN DE IP-FIRE

El primer paso será descargar la imagen de IP-Fire que se puede encontrar en su página oficial (http://www.ipfire.org). Una vez realizado este paso, se procederá a la instalación donde se configuran los aspectos más generales tales como el formato del disco, el idioma o la contraseña de administrador por ejemplo. Las configuraciones más específicas de esta distribución Linux fueron las siguientes:

- Selección del tipo de configuración de red que queremos configurar en el firewall, es decir, cuántas redes vamos a tener. Para ello se elige la opción GREEN+RED+ORANGE. Cada una de estas redes hace referencia a un nivel de seguridad diferente. En la tabla 4.2.3.3.1 se puede leer un breve análisis de cada una de estas redes, mientras que en la tabla 4.2.3.3.2 se aprecia la relación que existen entre ellas.

Red	WAN	Red externa conectada a internet (normalmente la conexión contratada con tu proveedor de servicios de internet)
Green	LAN	Red privada/interna. Conectada internamente.
Orange	DMZ	Red desmilitarizada, una red desprotegida para que puedan acceder desde internet. Será la red que albergue los servidores.
Blue	WLAN	Red inalámbrica, separada del resto de redes sólo para los clientes

		inalámbricos.

Tabla 4.2.3.3.1: Significado de cada una de las posibles redes en IP-Fire [19]

Direction		Status	
Red	→	**Firewall**	Closed, Use external access
Red	→	**Orange**	Closed. Use port forwarding
Red	→	**Blue**	Closed. Use port forwarding or VPN
Red	→	**Green**	Closed. Use port forwarding or VPN
Orange	→	**Firewall**	Closed, No DNS nor DHCP for **Orange**
Orange	→	**Red**	Open
Orange	→	**Blue**	Closed, use DMZ pinholes
Orange	→	**Green**	Closed, use DMZ pinholes
Blue	→	**Firewall**	Closed, no access for **Blue**
Blue	→	**Red**	Closed, no access for **Blue**
Blue	→	**Orange**	Closed, no access for **Blue**
Blue	→	**Green**	Closed, use DMZ pinholes or VPN
Green	→	**Firewall**	Open
Green	→	**Red**	Open
Green	→	**Orange**	Open
Green	→	**Blue**	Open

Tabla 4.2.3.3.2: Visibilidad de una red con otra, por defecto implementado por IP-Fire [19]

- Una vez hecha la configuración, es fundamental la asignación de la tarjeta de red para cada una de ellas. Es decir, se tendrá que emparejar cada red (GREEN, RED y ORANGE) con los adaptadores disponibles en la máquina virtual, mediante la opción de configuración de IP-Fire *Drivers and card assignments.* Más tarde se selecciona la red y por último se elige la tarjeta de red que tendrá asignada esta.

- El siguiente paso será el de configurar las direcciones IP en las diferentes redes. Para ello se usa la opción de configuración *Address settings*, desde donde se permitirá elegir la red a configurar, y se acaba asignando la dirección. A cada una de las interfaces de red del invitado IP-Fire se le asignarán direcciones que se encuentren en diferentes subredes, puesto que la configuración de este sistema operativo obliga a ello.

- La instalación finaliza configurando la puerta de enlace de la red RED, ya que es la única que tiene puerta de enlace en el firewall, y configurando los DNS. Para esto se emplea la opción de configuración *DNS and Gateway settings*.

4.2.3.4. SERVIDOR WEB Y FTP

El servidor web y FTP se encuentra instalado en un Windows XP ubicado la red desmilitarizada (ORANGE). Esto permite que sea accesible tanto desde la red GREEN como desde la red RED (haciendo port forwarding, que posteriormente se explicará).

En esta ocasión, se ha optado por un servidor web básico de código abierto llamado Miniweb HTTP Server (http://miniweb.sourceforge.net/), que ocupa 115KB aproximadamente, y un servidor FTP sencillo llamado Xlight (http://www.xlightftpd.com/).

Se ha optado por estos servidores básicos principalmente por su bajo uso de recursos. Hay que tener en cuenta que al levantar todas las máquinas virtuales existentes en el escenario, la máquina anfitriona se ve ralentizada debido al alto uso de sus recursos hardware; por lo que todo el ahorro de recursos influye positivamente.

4.2.3.5. GESTIÓN DE IP-FIRE

Para la gestión de IP-Fire se accede a la interfaz de gestión vía web por el puerto 444. En el escenario implementado la dirección que encontramos es https://192.168.14.24:444, y cuando se accede a dicha dirección se tiene que aceptar un certificado de seguridad. También hay que identificarse, y si la autenticación es satisfactoria se accede entonces a la interfaz de gestión. Lo que se muestra en este apartado es información básica acerca de las redes activas en el firewall.

Para el escenario implementado sólo se trabajará con la opción *Firewall* del menú de configuración; y de forma más específica, con los apartados *Firewall Rules* y *Opciones de Firewall*.

Para una mejor comprensión, a continuación se describe brevemente la función de cada uno de estos apartados:

- **Firewall Rules:** en esta sección se configuran las reglas del firewall para permitir (o denegar, si fuera el caso) conexiones entre los distintos equipos, conectados en las redes, e incluso entre MAC's [20].

- **Firewall Groups:** Permite configurar grupos de equipos, de redes e incluso de países (mediante GeoIP), facilitando la gestión de estos. Esto se consigue gracias a que se puede aplicar directamente reglas sobre estos grupos, formados por varios nodos. Esto es de gran utilidad si la red es grande y existen varios grupos con diferentes políticas de seguridad. No sería el caso en el escenario que nos ocupa, al no existir un número de equipos muy elevado [20].
- **Opciones de Firewall:** este apartado es muy interesante ya que, a través de este, se configuran el comportamiento por defecto que tendrá el firewall. Entre ellas podemos optar a opciones tan importantes sobre el comportamiento, como por ejemplo permitir o no el enmascaramiento en las diferentes redes, guardar los registros en el log, posibilitar el forwarding y el outgoing… Para nuestro escenario, se dejarán las opciones que vienen por defecto [20].
- **P2P Networks:** permite o deniega el tráfico P2P; y en el caso que se permita habrá que especificar qué programa se usará (Ares, Edonkey, Bittorrent, Kazaa…) [20].
- **GeoIP Block:** con esta opción se puede seleccionar uno o varios países, y denegarle el acceso al sistema. Dicha selección se realiza mediante filtrado IP.
- **Iptables:** en este apartado se pueden añadir reglas iptables para algunas configuraciones muy específicas. Son por ellas por donde pasarán los paquetes antes de dirigirse a las reglas iptables internas del sistema. Como aclaración, he de decir que esto se implementó para no tener que modificar las reglas iptables activas en el sistema, ya que eso puede ser muy peligroso en un firewall si se cometiera cualquier tipo de error.

4.2.3.6. REGLAS IMPLEMENTADAS EN EL FIREWALL

En primer lugar hay que especificar que con la configuración por defecto del firewall se cumplen las reglas de visibilidad descritas en la figura 4.2.3.3.3. Las mismas reglas que permiten esas comunicaciones y que vienen implícitamente configuradas.

En cada regla que se quiera configurar habrá que especificar el **origen**, que puede ser una red, una dirección Ip, una dirección MAC, una GeoIP o un grupo (definido previamente). También habrá que indicar si queremos hacer **NAT** (o no) y una dirección **destino**, que de la misma forma que ocurría con el origen, puede ser una red, una dirección Ip, una dirección MAC, una GeoIP o un grupo. También existen unas opciones adicionales que permiten: describir la regla con una frase, activar/desactivar la regla definida, activar el log para esa regla, poner un temporizador de activación de esa regla,

limitar las conexiones simultáneas desde una dirección IP y limitar las conexiones por segundo. Estas últimas opciones se ven de una forma más gráfica la imagen 4.2.3.6.1.

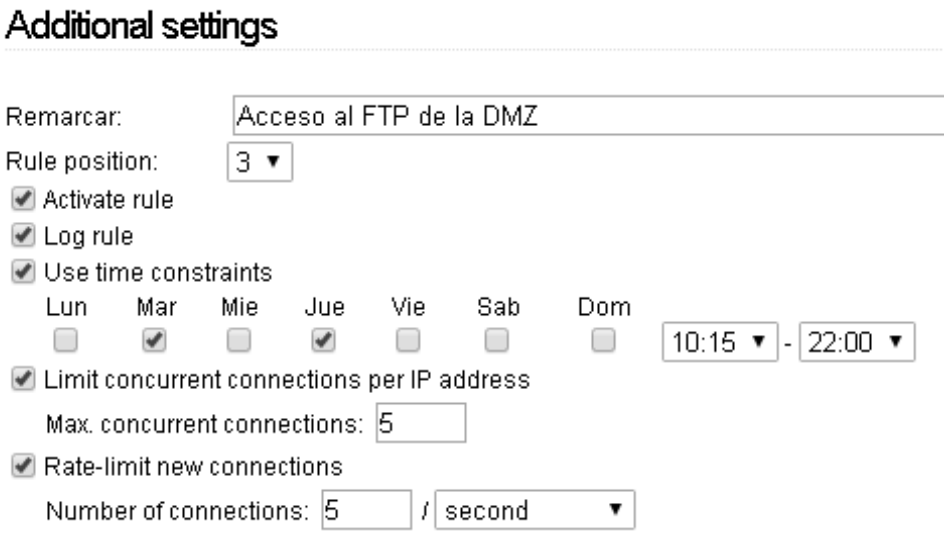


Figura 4.2.3.6.1: Opciones adicionales que se pueden añadir en la declaración de una regla

Este firewall concretamente cuenta con cuatro reglas implementadas tal y como se pueden ver en la figura 4.2.3.6.2., y cuya finalidad es la de:

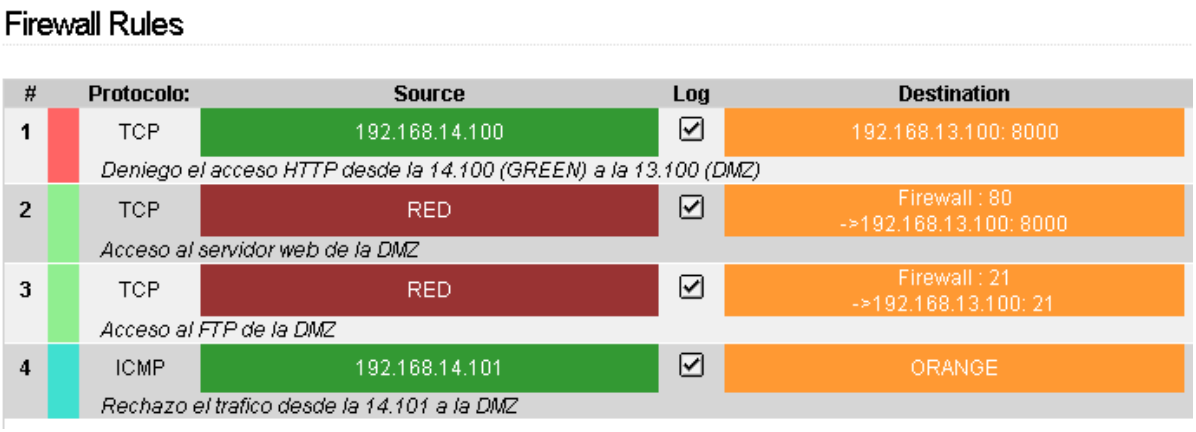


Figura 4.2.3.6.2: Reglas implementadas en el firewall

- Denegar al host de la red GREEN con dirección 192.168.14.100 (Windows XP) el acceso web al servidor de la zona desmilitarizada. Para comprobarlo se puede consultar la captura de tráfico en la figura 4.2.3.6.3. En esa captura se ve al equipo intentando acceder al servidor web y no recibiendo ninguna respuesta por parte de este.

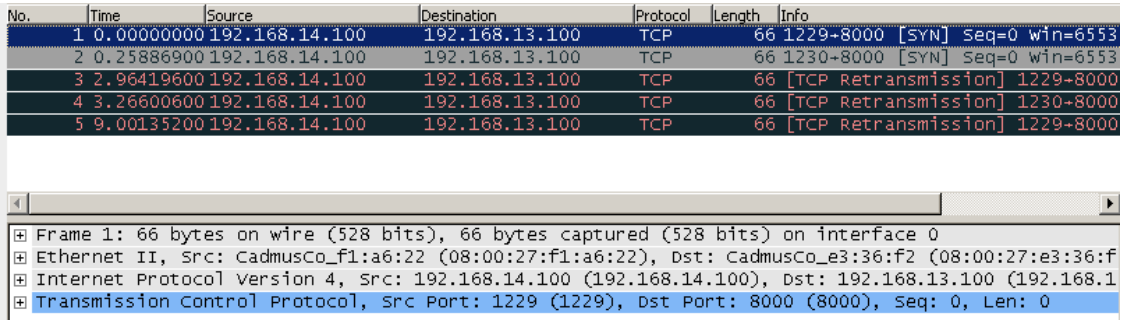


Figura 4.2.3.6.3: Captura de tráfico del equipo 192.168.14.100 intentado acceder al servidor web

Si se desactiva esa regla en el firewall se comprueba que el acceso al servidor web está permitido. Se puede apreciar mejor en la captura de tráfico inmediatamente más abajo.

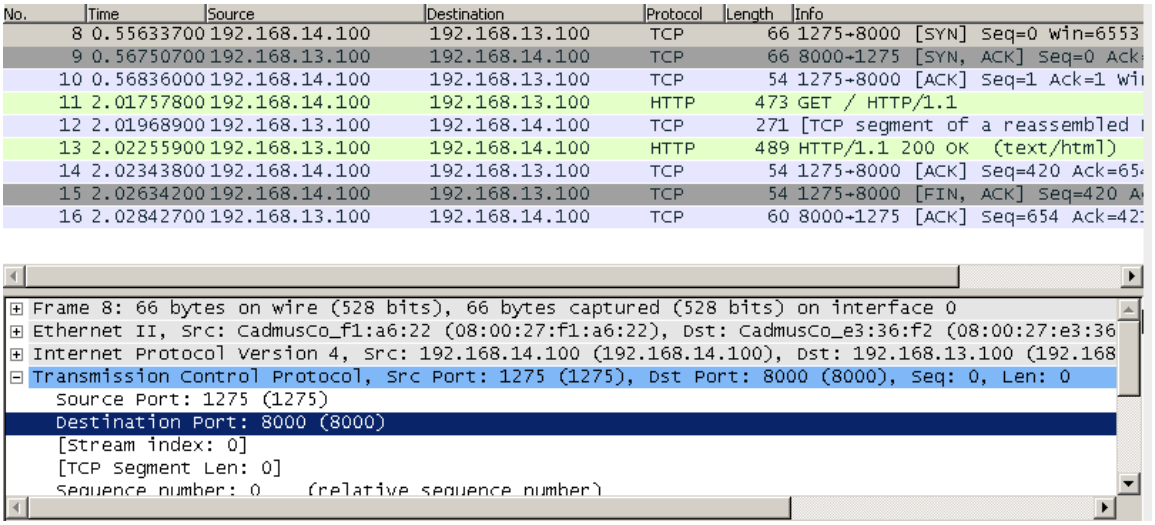


Figura 4.2.3.6.4: Captura de tráfico del equipo 192.168.14.100 accediendo al servidor web

- También permite a los host de la red exterior (red RED) establecer comunicación con el servidor web de la DMZ (red ORANGE). Si se presta atención a la tabla 4.2.3.3.2., se ve que la única forma de comunicarnos es haciendo “port forwarding”. Para ello nos vamos a la opción *Firewall Rules* del firewall y añadimos una nueva regla, eligiendo como dirección origen la red externa, a la vez que se especifica que vamos a hacer NAT. También se ha de indicar que la dirección destino será la IP del host Servidor; y se finaliza haciendo un reenvío de puertos ya que el servidor web está escuchando en el puerto 8000 y las peticiones queremos que se hagan desde el puerto 80. Esto se configuraría tal y como queda en la figura 4.2.3.6.5.

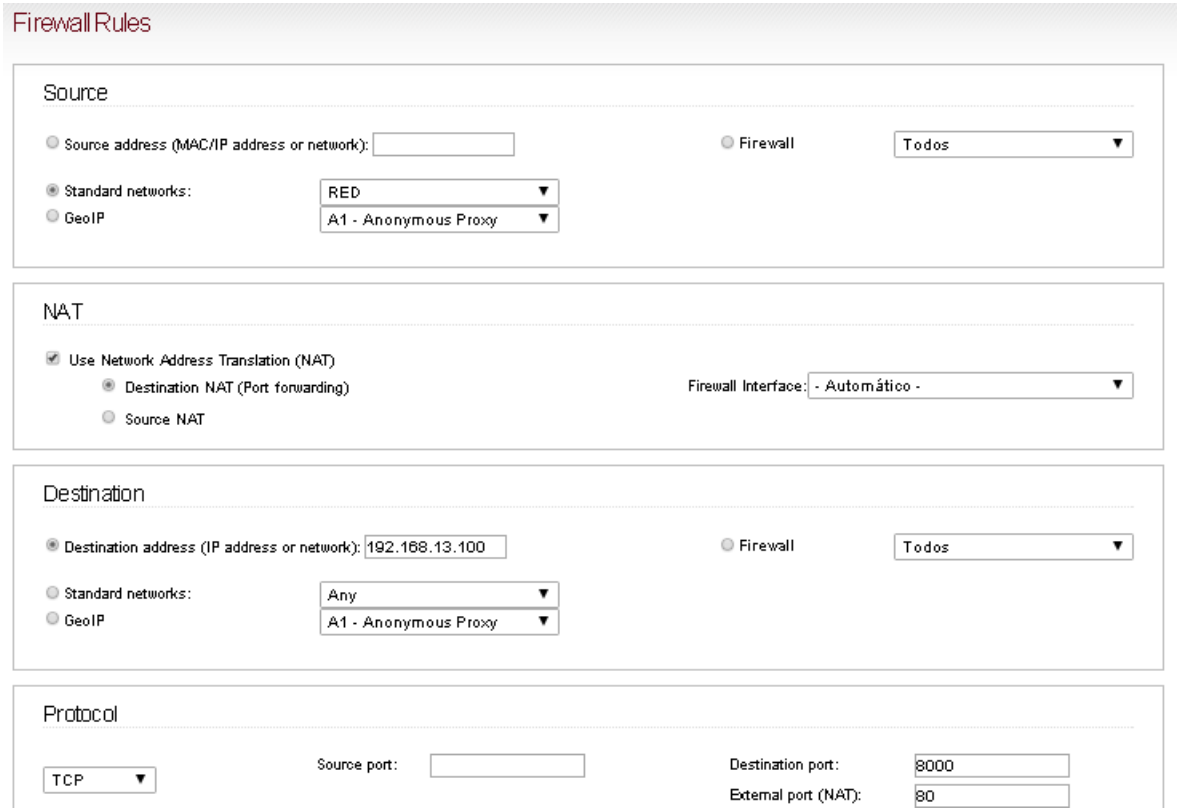


Figura 4.2.3.6.5: Regla para comunicar con el servidor web la red externa con la DMZ

También se ha de comprobar si esta regla funciona, y para ello se captura tráfico desde el anfitrión a la vez que intentamos acceder a la web (por la interfaz de la red RED 192.168.43.24). Todos estos pasos descritos en los reglones más arriba, se pueden ver en la figura 4.2.3.6.6.

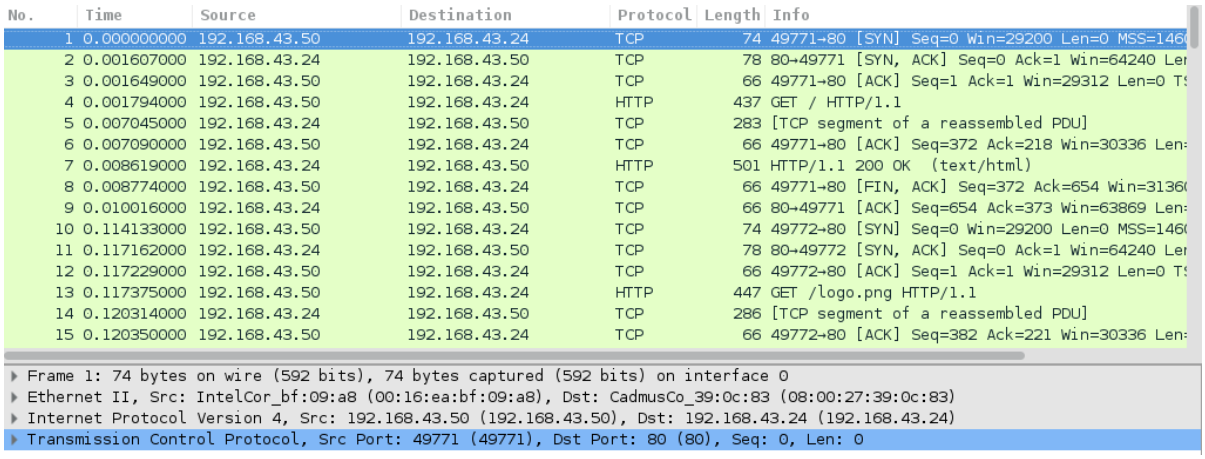
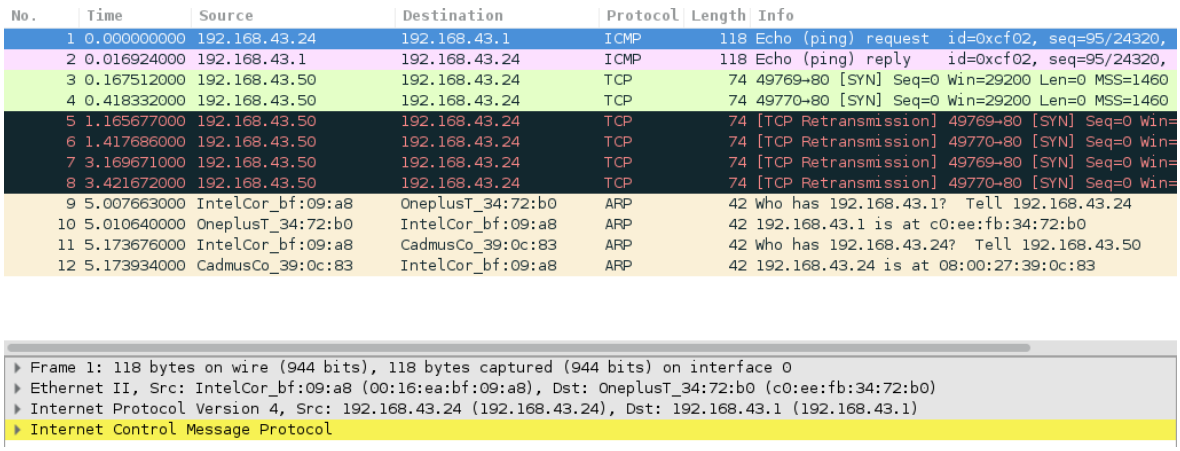


Figura 4.2.3.6.6: Anfitrión accediendo al servidor web

En el caso de deshabilitar esta regla no se podría acceder al servidor web desde la red RED como comprobamos en la figura 4.2.3.6.7.

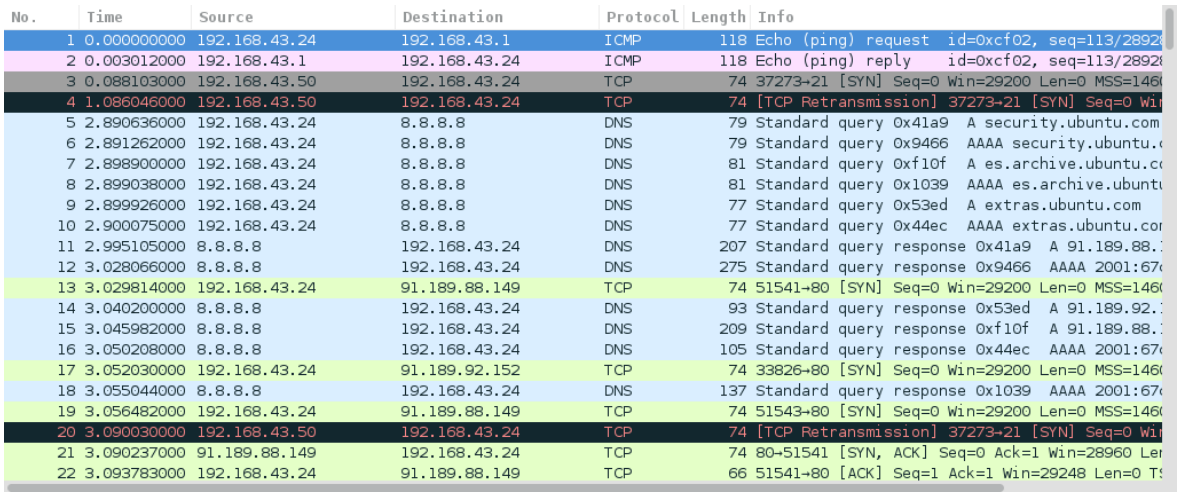


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.24	192.168.43.1	ICMP	118	Echo (ping) request id=0xcf02, seq=95/24320,
2	0.016924000	192.168.43.1	192.168.43.24	ICMP	118	Echo (ping) reply id=0xcf02, seq=95/24320,
3	0.167512000	192.168.43.50	192.168.43.24	TCP	74	49769→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
4	0.418332000	192.168.43.50	192.168.43.24	TCP	74	49770→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
5	1.165677000	192.168.43.50	192.168.43.24	TCP	74	[TCP Retransmission] 49769→80 [SYN] Seq=0 Win=
6	1.417686000	192.168.43.50	192.168.43.24	TCP	74	[TCP Retransmission] 49770→80 [SYN] Seq=0 Win=
7	3.169671000	192.168.43.50	192.168.43.24	TCP	74	[TCP Retransmission] 49769→80 [SYN] Seq=0 Win=
8	3.421672000	192.168.43.50	192.168.43.24	TCP	74	[TCP Retransmission] 49770→80 [SYN] Seq=0 Win=
9	5.007663000	IntelCor_bf:09:a8	OneplusT_34:72:b0	ARP	42	Who has 192.168.43.1? Tell 192.168.43.24
10	5.010640000	OneplusT_34:72:b0	IntelCor_bf:09:a8	ARP	42	192.168.43.1 is at c0:ee:fb:34:72:b0
11	5.173676000	IntelCor_bf:09:a8	CadmusCo_39:0c:83	ARP	42	Who has 192.168.43.24? Tell 192.168.43.50
12	5.173934000	CadmusCo_39:0c:83	IntelCor_bf:09:a8	ARP	42	192.168.43.24 is at 08:00:27:39:0c:83


```
▸ Frame 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
▸ Ethernet II, Src: IntelCor_bf:09:a8 (00:16:ea:bf:09:a8), Dst: OneplusT_34:72:b0 (c0:ee:fb:34:72:b0)
▸ Internet Protocol Version 4, Src: 192.168.43.24 (192.168.43.24), Dst: 192.168.43.1 (192.168.43.1)
▸ Internet Control Message Protocol
```

Figura 4.2.3.6.7: Anfitrión intentado acceder al servidor web

- Por supuesto, también tolera el acceso FTP desde la red externa hasta el servidor de la zona desmilitarizada. Se comprueba que sin configurar la regla no es posible el acceso al servidor ftp (figura 4.2.3.6.8); pero si se activa la regla configurada como la del apartado anterior pero cambiando únicamente el número del puerto al que hace referencia el servicio, se comprueba que si se puede conectar como se aprecia en la figura 4.2.3.6.9.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.24	192.168.43.1	ICMP	118	Echo (ping) request id=0xcf02, seq=113/2892
2	0.003012000	192.168.43.1	192.168.43.24	ICMP	118	Echo (ping) reply id=0xcf02, seq=113/2892
3	0.088103000	192.168.43.50	192.168.43.24	TCP	74	37273→21 [SYN] Seq=0 Win=29200 Len=0 MSS=146
4	1.086046000	192.168.43.50	192.168.43.24	TCP	74	[TCP Retransmission] 37273→21 [SYN] Seq=0 Wi
5	2.890636000	192.168.43.24	8.8.8.8	DNS	79	Standard query 0x41a9 A security.ubuntu.com
6	2.891262000	192.168.43.24	8.8.8.8	DNS	79	Standard query 0x9466 AAAA security.ubuntu.c
7	2.898900000	192.168.43.24	8.8.8.8	DNS	81	Standard query 0xf10f A es.archive.ubuntu.c
8	2.899038000	192.168.43.24	8.8.8.8	DNS	81	Standard query 0x1039 AAAA es.archive.ubuntu
9	2.899926000	192.168.43.24	8.8.8.8	DNS	77	Standard query 0x53ed A extras.ubuntu.com
10	2.900075000	192.168.43.24	8.8.8.8	DNS	77	Standard query 0x44ec AAAA extras.ubuntu.com
11	2.995105000	8.8.8.8	192.168.43.24	DNS	207	Standard query response 0x41a9 A 91.189.88.1
12	3.028066000	8.8.8.8	192.168.43.24	DNS	275	Standard query response 0x9466 AAAA 2001:67
13	3.029814000	192.168.43.24	91.189.88.149	TCP	74	51541→80 [SYN] Seq=0 Win=29200 Len=0 MSS=146
14	3.040200000	8.8.8.8	192.168.43.24	DNS	93	Standard query response 0x53ed A 91.189.92.1
15	3.045982000	8.8.8.8	192.168.43.24	DNS	209	Standard query response 0xf10f A 91.189.88.1
16	3.050208000	8.8.8.8	192.168.43.24	DNS	105	Standard query response 0x44ec AAAA 2001:67
17	3.052030000	192.168.43.24	91.189.92.152	TCP	74	33826→80 [SYN] Seq=0 Win=29200 Len=0 MSS=146
18	3.055044000	8.8.8.8	192.168.43.24	DNS	137	Standard query response 0x1039 AAAA 2001:67
19	3.056482000	192.168.43.24	91.189.88.149	TCP	74	51543→80 [SYN] Seq=0 Win=29200 Len=0 MSS=146
20	3.090030000	192.168.43.50	192.168.43.24	TCP	74	[TCP Retransmission] 37273→21 [SYN] Seq=0 Wi
21	3.090237000	91.189.88.149	192.168.43.24	TCP	74	80→51541 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
22	3.093783000	192.168.43.24	91.189.88.149	TCP	66	51541→80 [ACK] Seq=1 Ack=1 Win=29248 Len=0 T

Figura 4.2.3.6.8: Anfitrión intentado acceder al servidor ftp

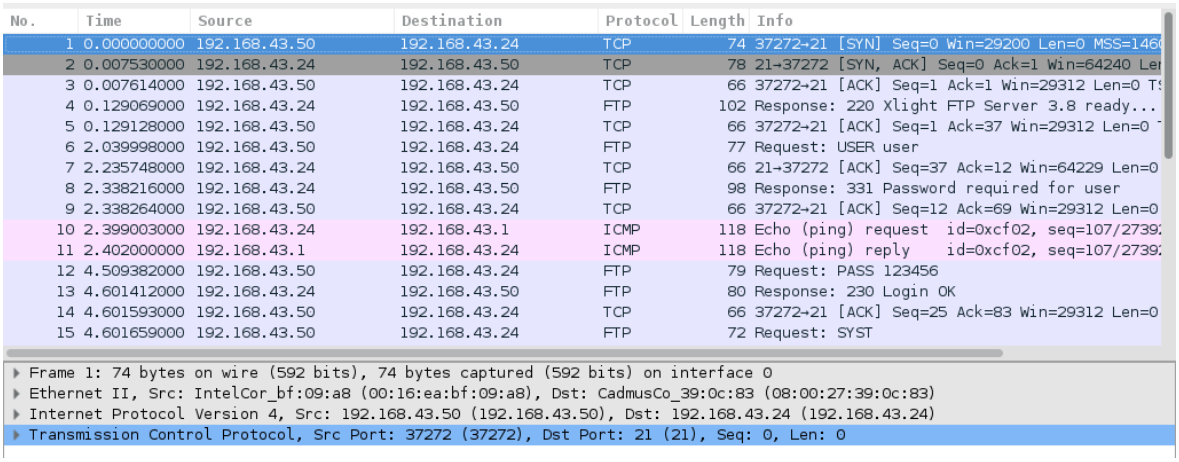


Figura 4.2.3.6.9: Anfitrión accediendo al servidor ftp

- La última regla rechaza (REJECT) todo el tráfico ICMP desde el host de la red GREEN 192.168.14.101 (Ubuntu), hacia la zona desmilitarizada (incluyendo toda la red ORANGE).

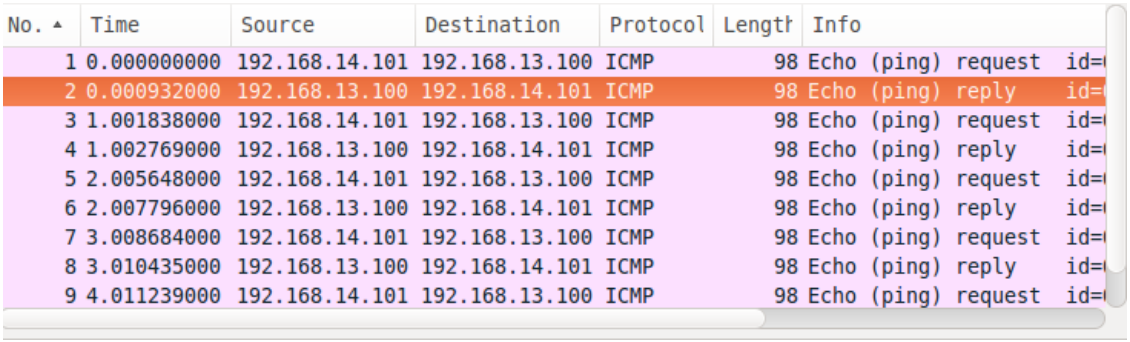


Figura 4.2.3.6.10: Equipo Ubuntu (192.168.14.101) haciendo ping a equipo de la red ORANGE (192.168.13.100)

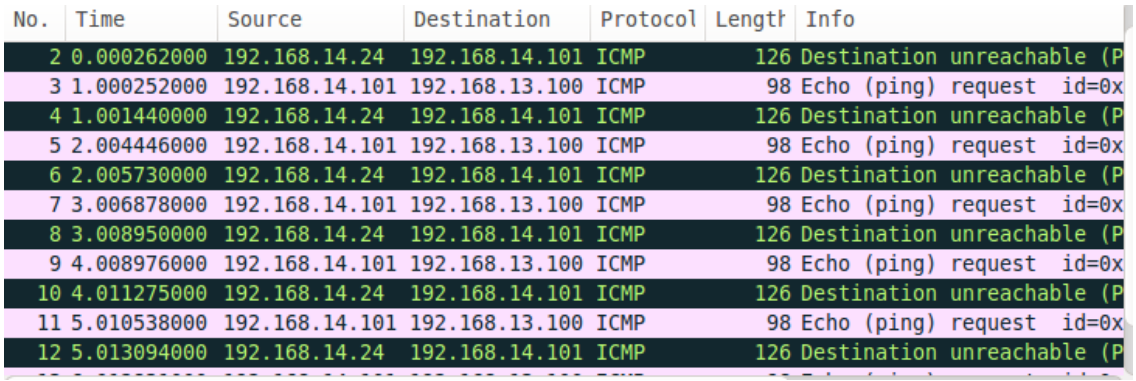


Figura 4.2.3.6.11: Equipo Ubuntu (192.168.14.101) intentando hacer ping a equipo de la red ORANGE (192.168.13.100) después de aplicarse la regla de restricción

5. RESULTADOS Y DISCUSIÓN

Las expectativas con las que partíamos en esta investigación se han visto cumplidas íntegramente con el resultado obtenido.

Es cierto que en el primer escenario, aunque parezca sencillo de implementar, se invirtió gran parte de tiempo debido a que por su topología en anillo y la forma en la que esta topología trabaja hacía que el sistema operativo que se utiliza como enrutador (Ubuntu Server) interpretara que se estaba realizando un ataque denominado ARP Spoofing y por tanto descartaba los paquetes. Finalmente se consiguió configurar el sistema para indicarle que no se trataba de un ataque, y así se consiguió hacer posible que los paquetes siguieran la ruta deseada.

En el segundo escenario en cambio todos los requisitos propuestos inicialmente se han ratificado, siendo lo más complejo la configuración y familiarización con el software de gestión del firewall debido a que existen varios procedimientos de configuración a la hora de crear reglas en este.

Sin lugar a dudas, el estudio en profundidad del software de virtualización (VirtualBox), que recordemos fue elegido por ser un software libre de código abierto y muy extendido; ha contribuido en gran parte al éxito obtenido por la seguridad que daba y la información con la que se partía. A pesar de todo ello, es justo decir que trabajando más en profundidad con él, se han percibido ciertas debilidades. Como por ejemplo el hecho de que no permite el reenvio de puertos menores del 1024, o que el tráfico UDP broadcast no está disponible y que cuenta con algunas herramientas basadas en ICMP que desde la web de VirtualBox se advierte que pueden fallar. Todas estas restricciones bien podrían ser investigadas en líneas futuras, con idea de mejorar este software gratuito en ámbitos donde esas limitaciones sean críticas.

En cuanto a la virtualización, queda de manifiesto con este trabajo, que tiene un futuro muy prometedor en esta era digital que nos está tocando vivir. Son mucho mayores las ventajas que los inconvenientes que presenta, y gracias a esta investigación queda claro que estos últimos pueden ser fácilmente subsanados.

Quisiera finalizar resaltando algunos aspectos negativos que he detectado durante todas mis horas de trabajo. Existe una limitación importante que es consecuencia del uso exclusivo del hardware gestionado por el monitor de máquina virtual (o hipervisor). También quisiera acusar el inferior rendimiento que presenta el uso de hardware simulado con respecto al hardware real, pero como contrapartida existe una mejora en la ejecución de la situación de dispositivos gracias al nuevo campo que se abre con los controladores paravirtualizados.

6. REFERENCIAS BIBLIOGRÁFICAS

[1] Martín, D. et al. Virtualización, una solución para la eficiencia, seguridad y administración de intranet. El profesional de la información. Mayo-junio 2011, V. 20, núm. 3, (p. 348-354)

http://www.elprofesionaldelainformacion.com/contenidos/2011/mayo/16.pdf

[2] M. Tim Jones (IBM). Virtualización de aplicaciones, pasado y futuro. Biblioteca técnica IBM. Julio 2011.

http://www.ibm.com/developerworks/ssa/linux/library/l-virtual-machine-architectures/

[3] http://www.gonzalonazareno.org/cloud/material/IntroVirtualizacion.pdf

[4] VMWare, Virtualization.

http://www.vmware.com/virtualization.html

[5] Thomas Burger (Intel). The Advantages of Using Virtualization Technology in the Enterprise. Intel Technology Journal: Special issue on virtualization technology, Volume 10, Issue 03, Marzo 2012

https://software.intel.com/en-us/articles/the-advantages-of-using-virtualization-technology-in-the-enterprise

[6] Joshua Hoffman (Microsoft). Virtualization: Virtualization in and Beyond the Cloud. TechNet Magazine, Marzo 2012.

https://technet.microsoft.com/en-us/magazine/hh855066.aspx

[7] Descripción técnica Toshiba Satellite A300-1II.

http://www.toshiba.es/discontinued-products/satellite-a300-1ii/

[8] Guía de Ubuntu Server, 2014.

https://help.ubuntu.com/lts/serverguide/serverguide.pdf

[9] Documentación oficial de Ubuntu Desktop.

https://help.ubuntu.com/community/Installation/SystemRequirements

[10] Requisitos del sistema para los sistemas operativos Windows XP.

https://support.microsoft.com/es-es/kb/314865

[11] Descripción del sistema operativo IP-Fire.

http://www.ipfire.org/features

[12] Requisitos del Sistema para IP-Fire (wiki oficial de IP-Fire)

http://wiki.ipfire.org/en/hardware/requirements

[13] Curso: FT433 - Introducción a la virtualización con VirtualBox.

http://www.forumtecnico.com/pluginfile.php/48/mod_resource/content/1/forumtecnico.com%20FT433%20VirtualBox%20Tema%205%20Configuracion%20de%20red.pdf

[14] Manual de VirtualBox. Redes Virtuales.

https://www.virtualbox.org/manual/ch06.html

[15] Manual de VirtualBox.Guest Additions.

https://www.virtualbox.org/manual/ch04.html

[16] Activar Forwarding permanentemente.

https://www.centos.org/docs/5/html/5.2/Deployment_Guide/s1-firewall-ipt-fwd.html

[17] Configuración de la red mediante línea de comandos.

https://help.ubuntu.com/community/NetworkConfigurationCommandLine/Automatic

[18] Solucione para habilitar el tráfico de salida en Linux.

https://access.redhat.com/solutions/53031

[19] Configuración de red en IP-Fire.

http://wiki.ipfire.org/en/installation/step5

[20] Documentación del Firewall en IP-Fire.

http://wiki.ipfire.org/en/configuration/firewall/start