

[**Desarrollo**](#_hll29uyol5mq) **3**

[Informe acerca de firewalls](#_2j2rpr15lmvu) 3

[Ataques que se pueden producir](#_2xhb3za3telq) 6

[Uso de iptables](#_p4k6v4965v2a) 7

[**Conclusiones**](#_9gd37u9e8v0c) **12**

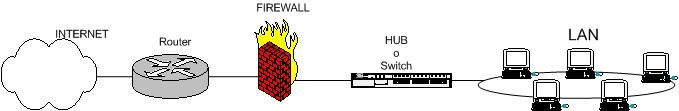
# 

# **Desarrollo**

## *Informe acerca de firewalls*

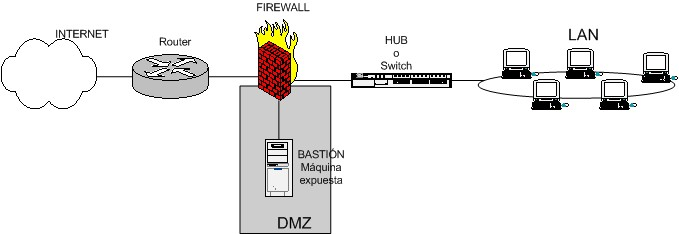
Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.

A continuación, se presentará el esquema clásico de un firewall:



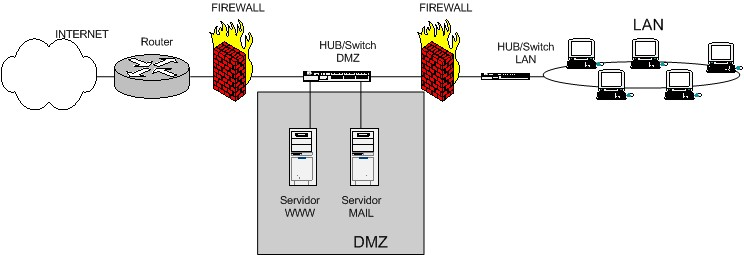
Tal como puede observarse, el firewall debe colocarse entre el router que provee el acceso a Internet (con un único cable) y el HUB o Switch al que está conectada la red local. De esta manera, este podrá administrar los paquetes que entran y salen de la red interna.

En muchos casos, es necesario exponer servidores a Internet (servidores web, servidores de correo, etc.). Aquí se recomienda configurar una DMZ (demilitarized zone) o zona desmilitarizada, en la que los servidores se encuentran expuestos (estos se denominan *bastiones*). El firewall pasaría a tener 3 entradas:



Con esta estructura, el servidor presente en la DMZ tiene acceso a la red externa y la interna es protegida por el firewall.

También puede configurarse un doble firewall (el que se utilizará en la parte práctica), teniendo más de un servidor en la DMZ y protegiendo el dispositivo que los administra:



Para qué sirve un firewall?

La función de un firewall no es otra que la de registrar el tráfico en internet de un dispositivo con el objeto de proteger una red informática privada impidiendo el acceso de usuarios no autorizados a ella, para que no se produzca el robo de información confidencial o se instale un virus en la computadora. Por consiguiente, un cortafuegos sirve, en esencia, para preservar la seguridad y privacidad de los navegantes, proteger una red empresarial o doméstica de malévolos ataques y salvaguardar la información y los archivos en un buen estado.

Cómo funciona un firewall?

Un firewall se sitúa en el punto de unión entre Internet y un ordenador o red de ordenadores. Su funcionamiento se basa en controlar toda la información y el tráfico que, a través del router, se transmite de una red a otra. Si, al efectuar un rápido análisis, el cortafuegos considera que dichos datos cumplen unas reglas de seguridad y protocolo, éstos podrán entrar en la red privada; pero, en caso contrario, de que no satisfagan las normas, el firewall se encarga de bloquear el acceso de ese usuario o información no fiable.

Maneras de implementar un firewall

* Por defecto, todo el tráfico entrante y saliente por el firewall se ACEPTA, y solo se deniega lo que se diga explícitamente.
* Por defecto, todo el tráfico entrante y saliente por el firewall se RECHAZA, y solo se acepta lo que se diga explícitamente (comportamiento que adoptamos en nuestro cortafuegos).

## 

## *Ataques que se pueden producir*

En esta sección, explicaremos algunos de los ataques que se pueden producir y a los que el firewall apunta a evitar, aunque haciendo hincapié en el Escaneo de puertos, que fue el tratado en esta implementación.

Ping Flood

*Ping flood* se basa en enviar a la víctima una cantidad abrumadora de paquetes ping, usualmente usando el comando "ping" de UNIX como hosts. Es muy simple de lanzar, el requisito principal es tener acceso a un ancho de banda mayor que la víctima.

“Ping de la muerte”

El atacante envía un paquete ICMP de más de 65.536 bytes. Como el sistema operativo no sabe cómo manejar un paquete tan grande, se congela o se cuelga en el momento de volver a montarlo. Hoy en día, el sistema operativo descarta dichos paquetes por sí mismo. Es decir, el ataque quedó obsoleto, pero no está de más nombrarlo ya que es mítico en cuanto al aspecto de ataques.

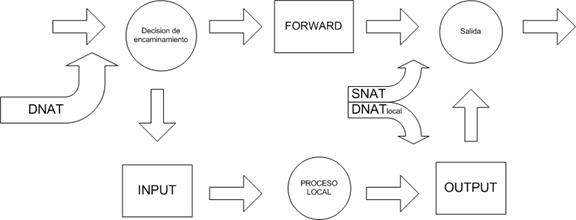
Escaneo de puertos

El escaneo de puertos es una de las técnicas de reconocimiento más populares que utilizan los atacantes para descubrir los servicios expuestos a posibles ataques. Todas las máquinas conectadas a una red de área local (LAN) o Internet ejecutan muchos servicios que escuchan en puertos conocidos y no tan conocidos.

Un escaneo de puertos ayuda al atacante a encontrar qué puertos están disponibles (es decir, qué servicio podría estar enumerando un puerto). Esencialmente, consiste en enviar un mensaje a cada puerto, uno a uno. El tipo de respuesta recibida indica si el puerto está a la escucha y, por lo tanto, puede probarse más detalladamente para detectar debilidades.

## *Uso de iptables*

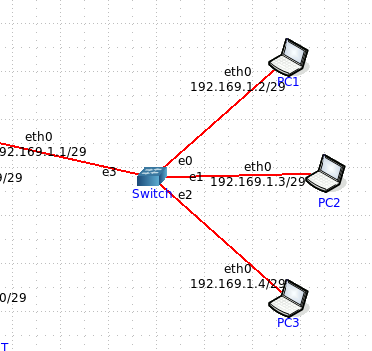
Iptables es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red.



Como se observa en el gráfico, hay dos caminos posibles: que el paquete este destinado a la propia máquina o que vaya a otra. Para los que estén destinados a la propia, se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que se van a otras redes o máquinas, se aplican las reglas FORWARD. Estas tres (INPUT, OUTPUT y FORWARD), son los tres tipos de reglas de filtrados (FILTER) pertenecientes a iptables. Antes de aplicar este tipo de reglas, es posible aplicar las reglas de NAT (PREROUTING, OUTPUT Y POSTROUTING), las cuales se utilizan para hacer redirecciones de puertos, cambios de IPs, etc. Es posible también, utilizar reglas de tipo MANGLE para modificar paquetes.

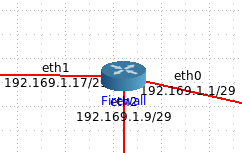
*Experiencia de topología con Firewall*

Para comenzar con la topología, se implementó en ella una red interna de 3 computadoras (PC1, PC2, PC3) administradas por un Switch, como se puede ver en la Figura 1. Esta será la red protegida por el Firewall, administrando la entrada/salida de paquetes desde/hacia Internet.

**

*Figura 1: Red interna*

Actuando como cortafuegos se dispuso un Router que tiene desde sus interfaces acceso a la red Interna, a Internet, y la DMZ o Zona Desmilitarizada, como se puede ver en la Figura 2.



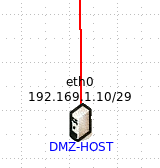
*Figura 2: Cortafuegos*

Es en éste router donde se aplicarán las reglas y políticas que se desea que el cortafuegos siga para mantener la red a resguardo.

En este cortafuegos, se estableció una política por defecto del mismo, la cual es es rechazar todos los paquetes entrantes y salientes.

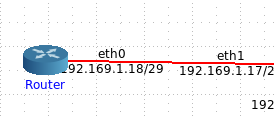
|  |
| --- |
| iptables -P FORWARD DROP |

La DMZ mencionada recientemente es la red en donde los servidores se encontrarán expuestos ya que siempre deben tener comunicación con la red externa. Como puede verse en la Figura 3, se dispuso en esta red un sólo bastion, el servidor DMZ-Host.

**

*Figura 3: DMZ*

Por último, se tiene la red externa representada por un Router (Figura 4), el que se supone como el origen de las amenazas para la red interna.

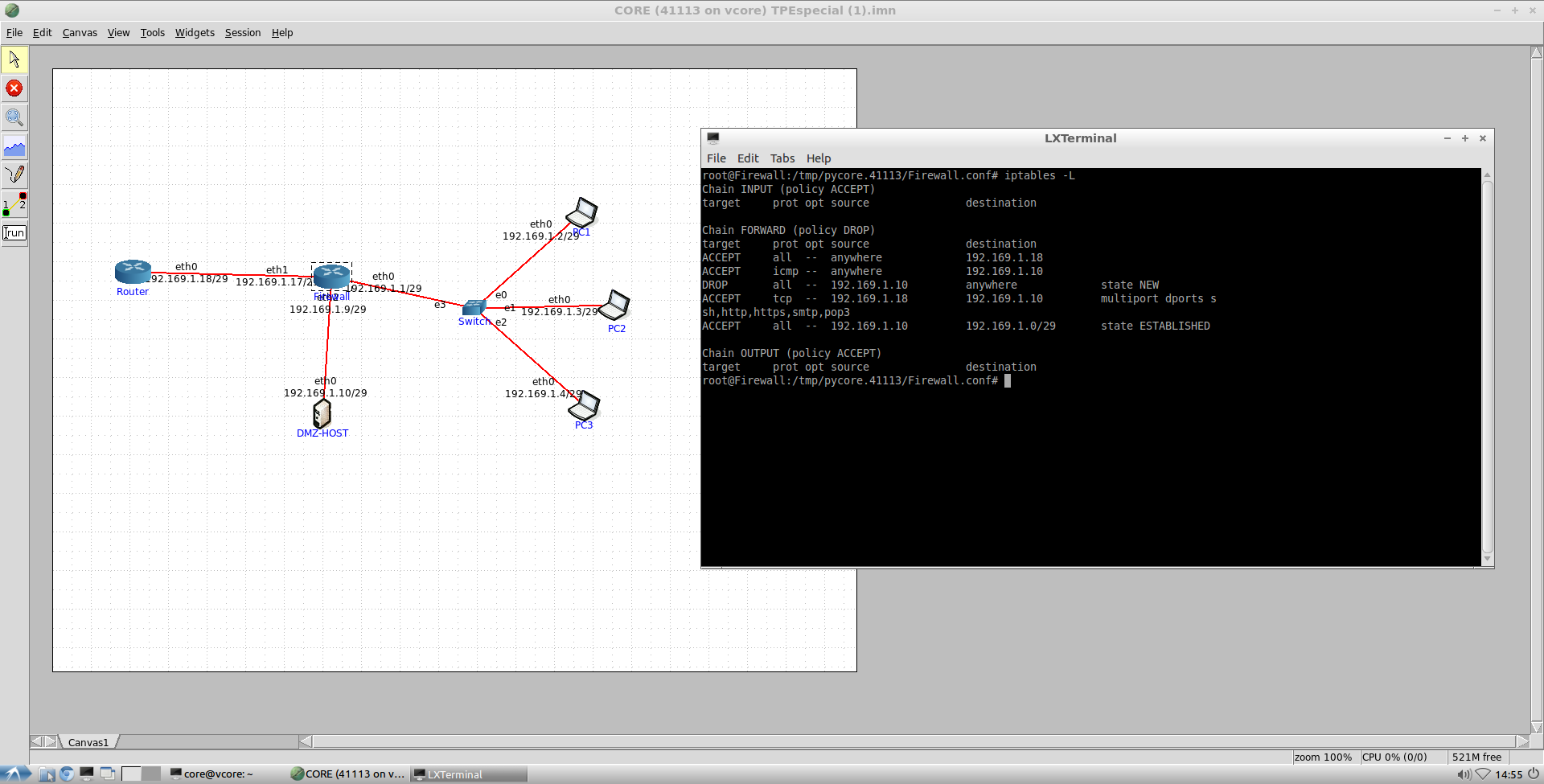
**

*Figura 4: Red externa*

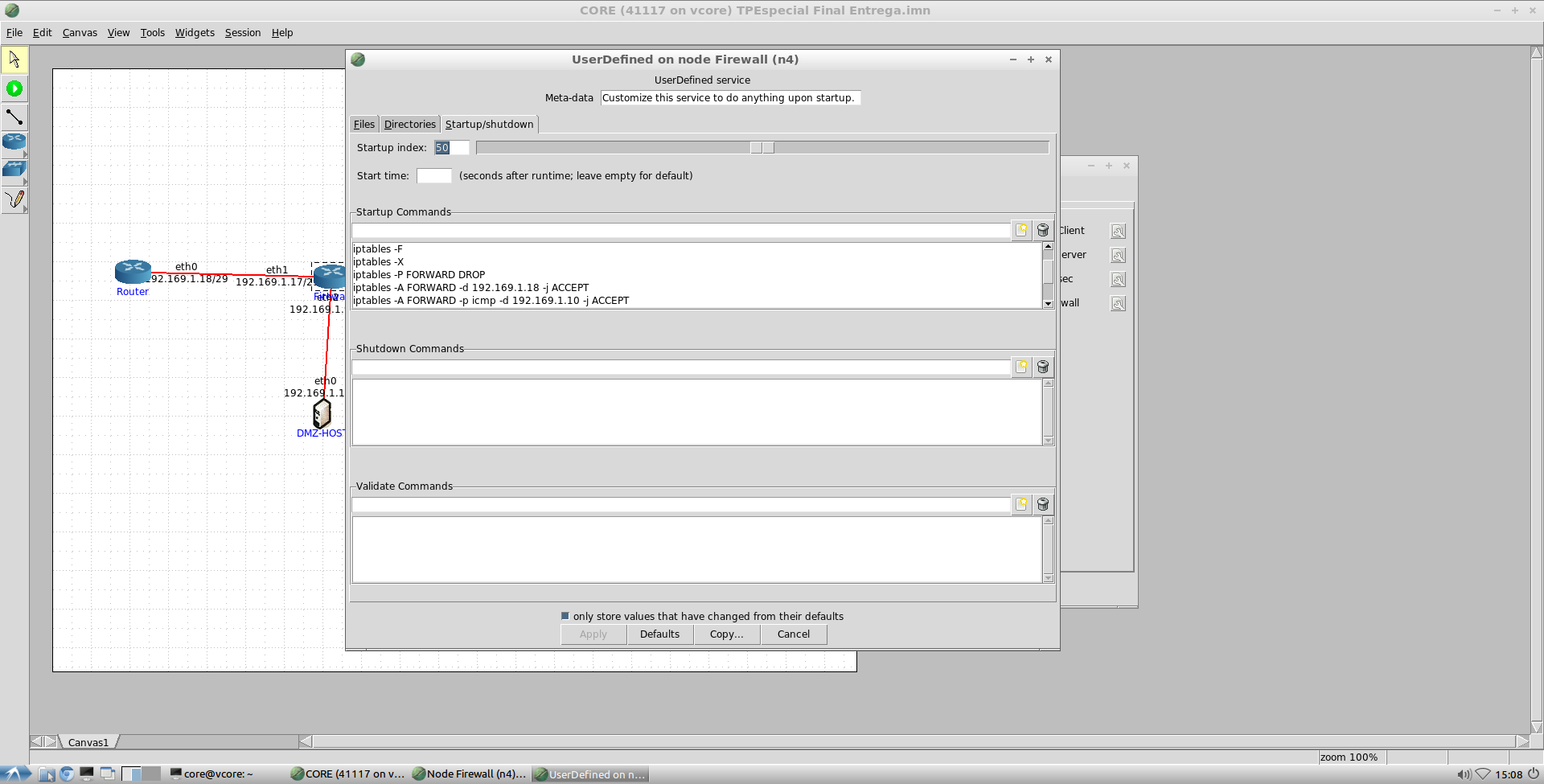
Las especificaciones del Firewall a implementar son:

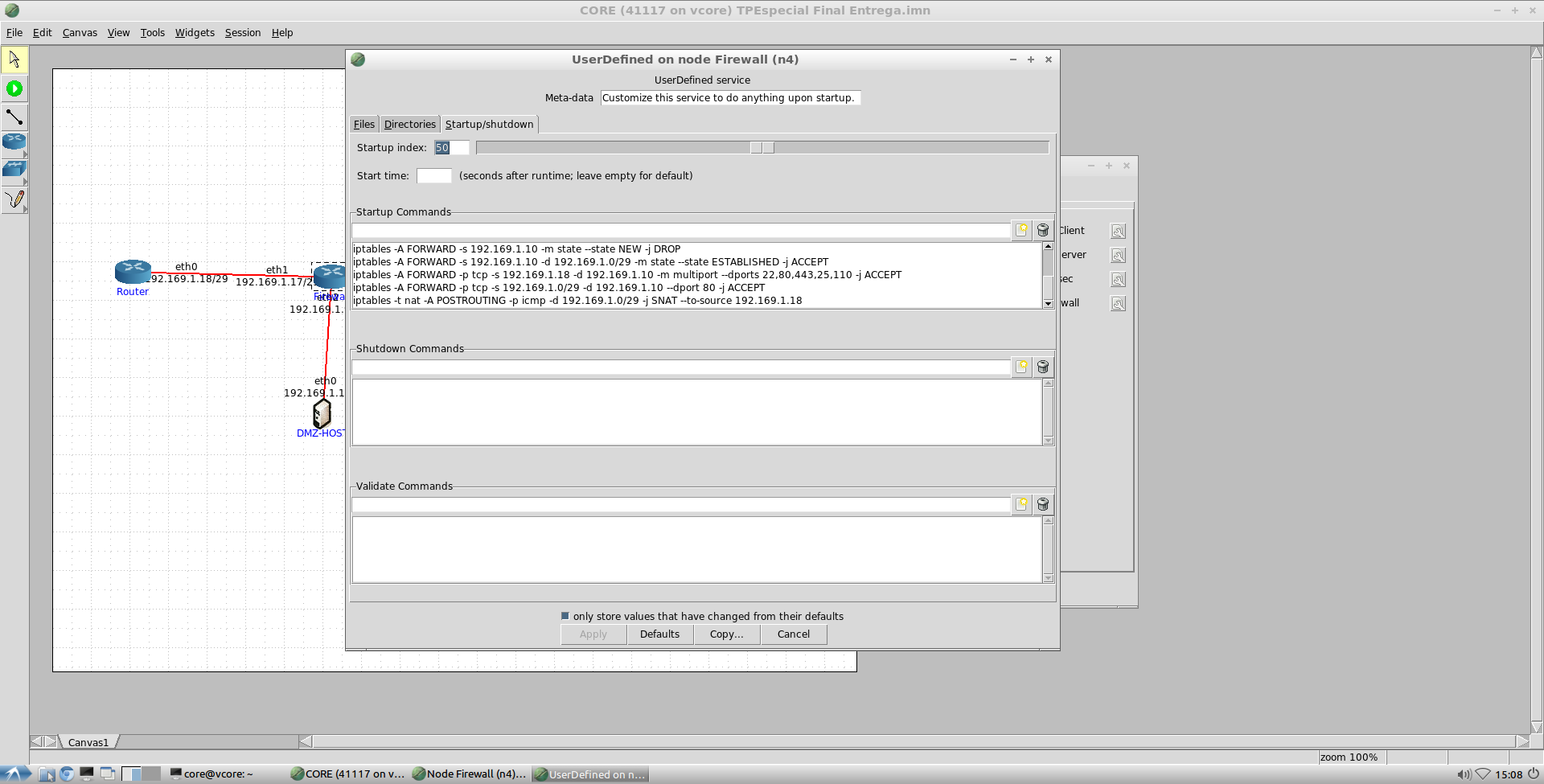
* En el server, sólo se debe permitir acceso a los servicios específicos ofrecidos, desde el exterior y desde la intranet.
* El server no puede iniciar ningún tipo de comunicación (ni con el exterior, ni con la intranet)
* Los equipos dentro de la intranet, pueden iniciar comunicaciones con el exterior, pero no responderá ningún requerimiento.
* Los pings (icmp echo request) realizados a equipos de la intranet o al server, deben ser respondidos por el router.

A continuación se observarán una serie de capturas. La primera pertenece a la consola utilizando el comando “iptables -L”, que nos otorga la posibilidad de ver las tablas utilizadas.



La segunda y la tercer captura, muestran los comandos utilizados.





* iptables -F e iptables -X: Flush de reglas.
* iptables -P FORWARD DROP: Actualizar la politica por defecto a “DROP”, significa rechazar todo, de la cadena FORWARD.
* iptables -A FORWARD -d 192.169.1.18 -j ACCEPT: Todo paquete destino que vaya a esa IP (Router externo), se acepta.
* iptables -A FORWARD -p icmp -d 192.169.1.10 -j ACCEPT: Todo paquete icmp, es decir, todo ping que vaya a esa IP (DMZ), se acepta.
* iptables -A FORWARD -s 192.169.1.10 -m state --state -NEW -j DROP: Todo paquete que salga de la DMZ y sea NUEVO, se rechaza. Por consiguiente, la DMZ no puede iniciar comunicación con nadie.
* iptables -A FORWARD -s 192.169.1.10 -d 192.169.1.0/29 -m -state --state ESTABLISHED -j ACCEPT: Los paquetes desde la DMZ a la Intranet pasan, siempre y cuando, ya haya una conexión previa. Se usa para que la DMZ no pueda iniciar conexión con la Intranet, pero si pueda responder cuando la Intranet inicie una conexión con ella.
* iptables -A FORWARD -p tcp -s 192.169.1.18 -d 192.169.1.10 -m multiport --dports 22,80,443,25,110 -j ACCEPT: Los paquetes del protocolo tcp que vayan desde el Router externo con destino la DMZ, en los puertos dados, se aceptan.
* iptables -A FORWARD -p tcp -s 192.169.1.0/29 -d 192.169.1.10 --dport 80 -j ACCEPT: Los paquetes tcp que vayan desde la Intranet con destino la DMZ, en el port 80, se acepta.
* iptables -t nat -A POSTROUTING -p icmp -d 192.169.1.0/29 -j SNAT --to-source 192.169.1.18: Se utiliza para que los pings que se envían a la Intranet, los responda el Router.

Los puertos 22,80,443,25,110 corresponden a: ssh, http, https, smtp, pop3, respectivamente.

Básicamente lo que se puede hacer pasando por el Firewall, es:

Dentro de lo que es protocolo ICMP;

* El server DMZ puede pinguear al Router externo y no a la intranet.
* El Router externo puede ping al DMZ y no a la Intranet.
* La Intranet puede pinguear al DMZ y no al Router.

Dentro de lo que es protocolo TCP;

* El Router externo no puede iniciar conexión con la Intranet pero si con el DMZ en los puertos seleccionados.
* El DMZ no puede iniciar conexión, ni con la Intranet, ni con el Router externo. (Aquí agregamos lo de connection tracking, NEW).
* La Intranet no puede iniciar conexión con el Router externo y si con el DMZ (Solamente el puerto 80). (Utilizando connection tracking otra vez, pero en este caso la regla ESTABLISHED para que pueda responder el DMZ a la Intranet).

# **Conclusiones**

En conclusión, este trabajo nos ha gustado y sido de utilidad para darle un cierre a todo lo aprendido en la materia. Si bien en el aspecto teórico y práctico se adquieren todos los conceptos necesarios para configurar redes, testearlas, y entender la totalidad de su funcionamiento, viene bien llevar todos ellos a una aplicación práctica como lo es un Firewall, analizando ataques reales.

Por último, otro punto a destacar que nos deja este proyecto es que como usuario de internet en general, uno suele sentirse más seguro navegando en Internet de lo que debería. Este tipo de ataques pueden ser más frecuentes y probables de lo que parece, con lo cual nuestra información puede estar en riesgo en todo momento; más que nada cuando se realizan conexiones a redes públicas (muy común en estos tiempos).