**ALUMNA: ANA PAOLA NAVA VIVAS**

CONFIGURACIÓN DE UN CORTA FUEGO Y UN SERVIDOR NAT

**INSTITUTO POLITÉCNICO NACIONAL**

**ESCUELA SUPERIOR DE CÓMPUTO**

**MATERIA: REDES COMPUTACOINALES**

**GRUPO: 2CM10**

**Introducción**

El objetivo de este proyecto fue el de implementar una zona desmilitarizada, configurando un servidor NAT y un cortafuego.

Para lograr tal propósito se implementó iptables desde Ubuntu.

¿Qué es un cortafuego?

Es un software o hardware cuyo objetivo es bloquear los accesos no autorizados a nuestra computadora o a nuestra red local según criterios que el usuario define [1].

¿Qué es un servidor NAT?

Internet en sus inicios no fue pensado para ser una red tan extensa, por ese motivo se reservaron “sólo” 32 bits para direcciones, el equivalente a 4.294.967.296 direcciones únicas, pero el hecho es que el número de máquinas conectadas a Internet aumentó exponencialmente y las direcciones IP se agotaban. Por ello surgió la NAT o Network Address Translation (en castellano, Traducción de Direcciones de Red).

La idea es sencilla, hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP (IP pública). Gracias a este “parche”, las grandes empresas sólo utilizarían una dirección IP y no tantas como máquinas hubiese en dicha empresa. También se utiliza para conectar redes domésticas a Internet [2].

¿Qué es iptables?

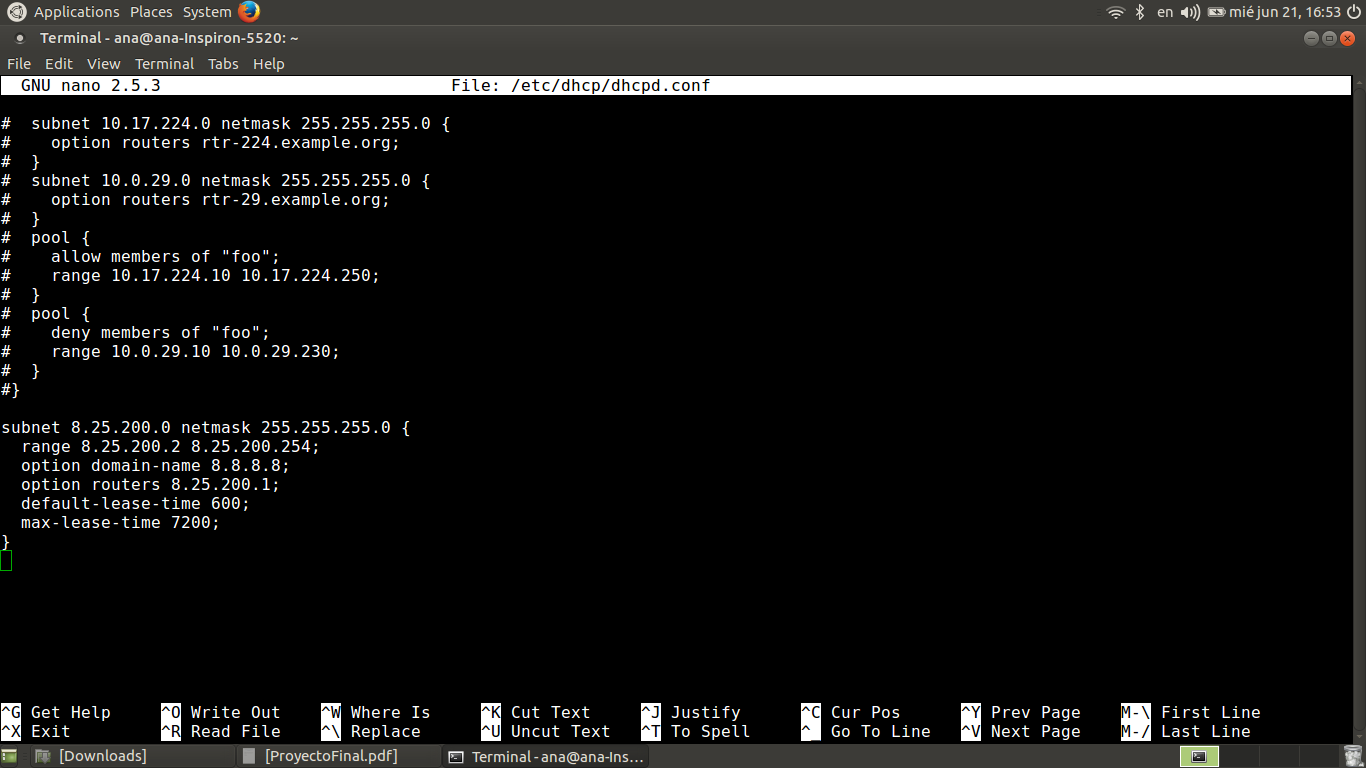
Es un cortafuego instalado por default en todas las distribuciones oficiales de Ubuntu [3]

Iptables permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en cadenas: cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en tablas: cada tabla está asociada con un tipo diferente de procesamiento de paquetes [4]

Desarrollo

Para poder realizar la actividad instalé el paquete: **iptables isc-hdcp-server**, con el comando: **sudo apt-get install isc-hdcp-server**

Entré al archivo de configuración de dhcp: **/etc/dhcp/dhcpd.conf** y edité las últimas líneas agregando unas nuevas y comentando las demás. Es de hacer notar que al editar el archivo y reiniciar la computadora no se guardan los cambios, y vuelve a como era antes.



De lo anterior, La primera línea son la subred y su máscara, la segunda el rango de hosts, la tercera es una dirección IP del DNS.

Después debo designar al puerto cableado como el GW con ifconfig.

Con **sudo ifconfig** puedo ver mis interfaces (generalmente la de ethernet comienza con e y la wifi con w), en mi caso eran enp1s0 y wlp2s0.

Se debe configurar el que vaya a la red desmilitarizada de la siguiente manera: **sudo ifconfig interfaz ippuerto netmask máscaradered**

Y permitir la salida de los datos a través de esa interfaz: *iptables -t nat -A POSTROUTING -o interfazparainternet -j MASQUERADE.*

**iptables -t nat -A POSTROUTING -o wlan2s0 -j MASQUERADE**

Después debo permitir el paso de paquetes a la interfaz de la red privada: *iptables -t nat -A INPUT -s red -i interfazdelared -j ACCEPT*

**iptables -t nat -A INPUT -s 8.25.200.0/24 -i enp1s0 -j ACCEPT**

Luego, sólo queda iniciar el servicio dhcp con:

**sudo systemctl start isc-dhcp-server**

En el caso de que salga como status de failed, seguramente es porque está enmascarado el servicio, suele pasar en Ubuntu.

**sudo systemctl status isc-dhcp-server.service**

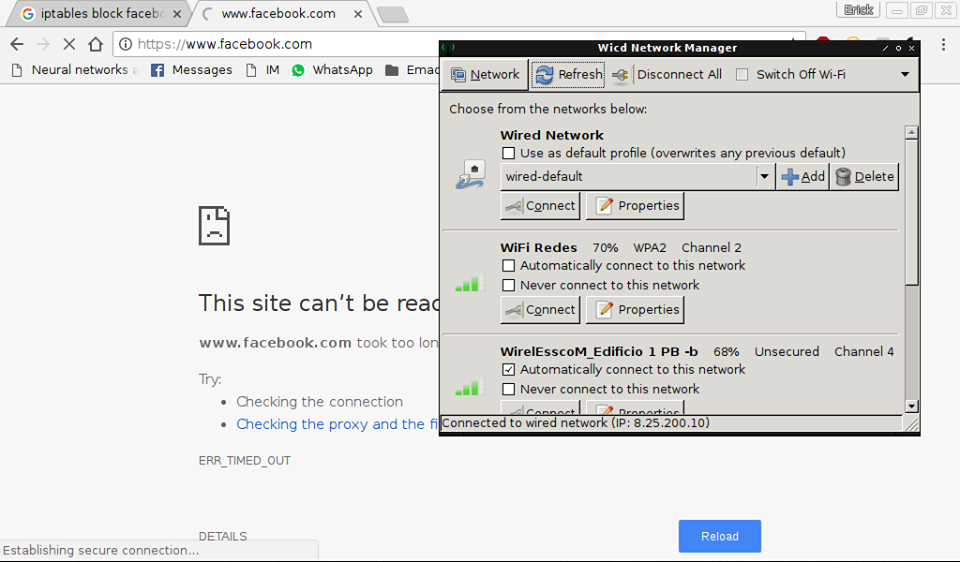
**sudo systemctl unmask isc-dhcp-server.service**

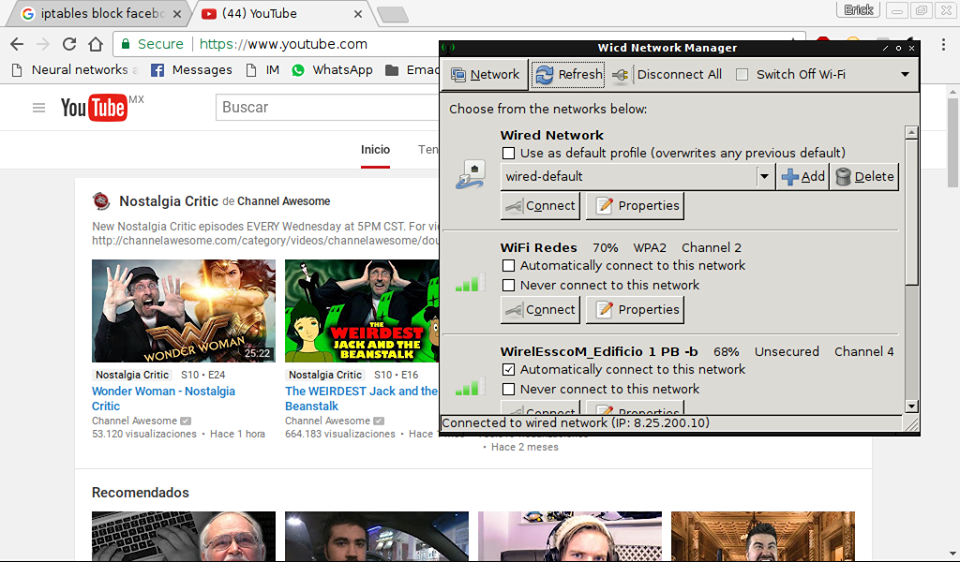
Después de establecer el servidor NAT, procedí a configurar iptables para resolver los siguientes incisos.

a. Debe de bloquear cualquier acceso al cortafuego B desde cualquier lugar (solo permitir manejo directo).

b. No debe de permitir realizar ping a las computadoras de la red 8.25.100.0/24 exceptuando la computadora 8.25.100.201.

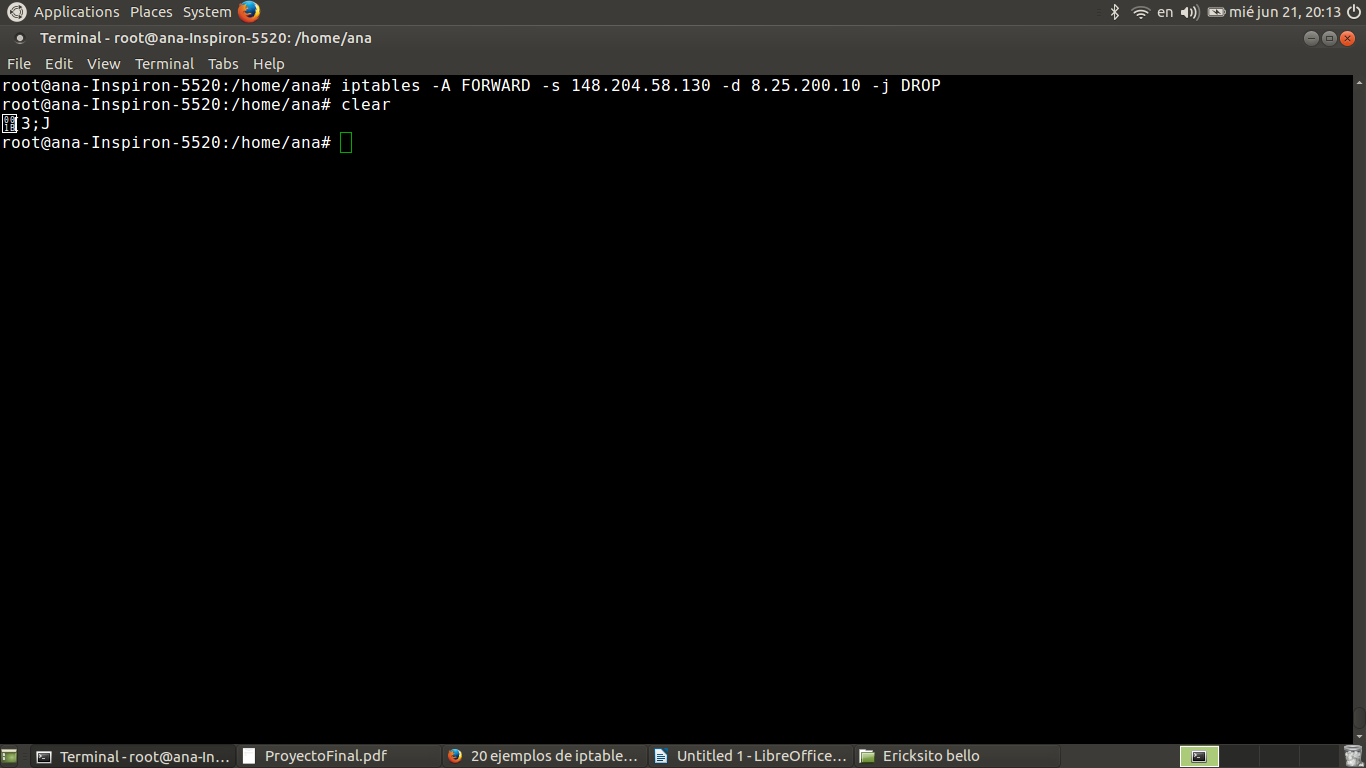
c. Debe de bloquear el acceso a las páginas de www.facebook.com, pero debe de permitir acceder a las de www.google.com y www.youtube.com.



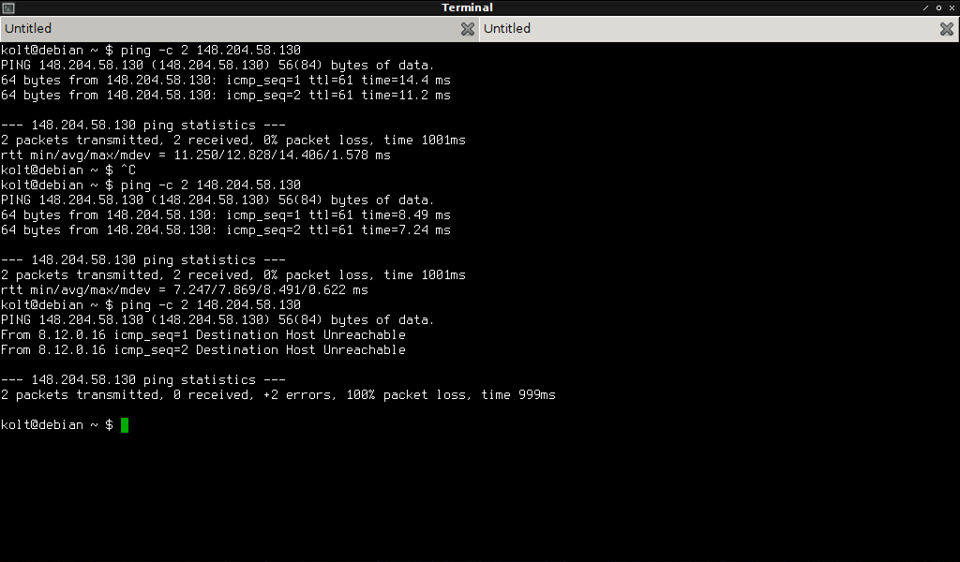


d. Debe de bloquear el acceso a la dirección 148.204.58.130, pero permitirlo para el resto de las computaras de la res de ESCOM.

Desde mi computador introduje el siguiente comando en la terminal.



Y desde otra computadora sucede lo siguiente.



e. Debe de bloquear el acceso a cualquier puerto de la ip 8.25.100.3 menos al puerto tcp 80.

Conclusiones

Entre las ventajas que se pueden encontrar en el uso de los servidores NAT, están:

* La primera y más obvia, el gran ahorro de direcciones IPv4 que supone, recordemos que podemos conectar múltiples máquinas de una red a Internet usando una única dirección IP pública.
* Seguridad. Las máquinas conectadas a la red mediante NAT no son visibles desde el exterior, por lo que un atacante externo no podría averiguar si una máquina está conectada o no a la red.
* Mantenimiento de la red. Sólo sería necesario modificar la tabla de reenvío de un router para desviar todo el tráfico hacia otra máquina mientras se llevan a cabo tareas de mantenimiento.

Sin embargo, hay que recordar que NAT es un parche y no es la verdadera solución al problema.

Referencias

[1] Hugo D. Scolnik. (2014). ¿Qué son los cortafuegos [firewalls]?. En QUÉ ES LA SEGURIDAD INFORMÁTICA(31). Buenos Aires, Argentina: Paidós.

[2] José Luis Alcoba. (24 Agosto 2011). NAT (Network Address Translation): Qué es y cómo funciona., de Xátaka móvil Sitio web: https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona

[3] Daniel U. Thibault. (2017-03-29). IptablesHowTo. ., de ubuntu documentation Sitio web: https://help.ubuntu.com/community/IptablesHowTo

[4] (20/OCTUBRE/2009). IPtables, un cortafuegos en el núcleo de Linux. ., de MicroTeknologías Sitio web: https://microteknologias.wordpress.com/2009/10/20/iptables-un-cortafuegos-en-el-nucleo-de-linux/