Gestión de Recursos y Seguridad en Redes
Seguridad en la red con Open Source

Derman Zepeda Vega
dzepeda@unan.edu.ni

Agenda

- Introducción a los Firewall
- Iptables en Linux
- Elaboración de un firewall básico en Linux. (Laboratorio)

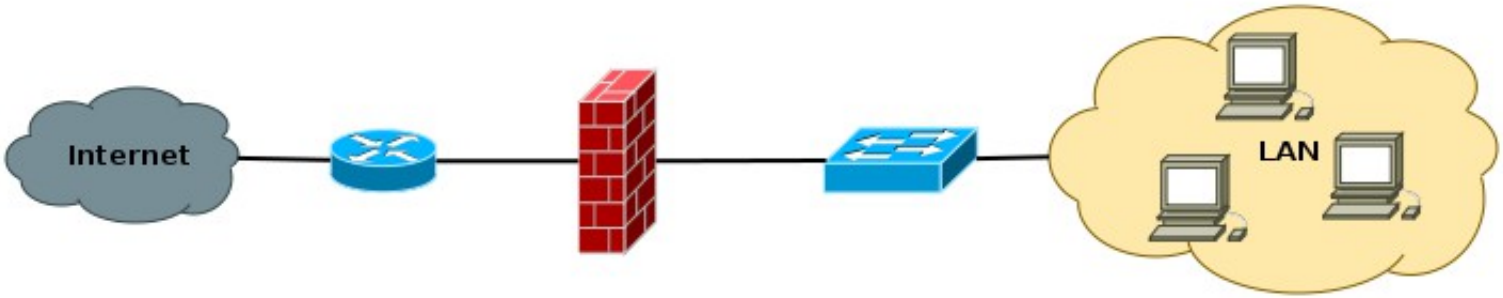
Qué es un firewall? Necesito uno?

- Pocas personas entienden realmente las consecuencias que tiene el abrir sus computadoras a Internet, unas consecuencias que no sólo son de caracter benigno e incluso beneficioso.

- Un firewall es, por lo general, un software (puede ser también un equipo hardware dedicado) a través del cual nos conectamos a una red como Internet, y que sirve como filtro sobre el tráfico que por él pasa, en ambas direcciones.

Esquema típico de un firewall

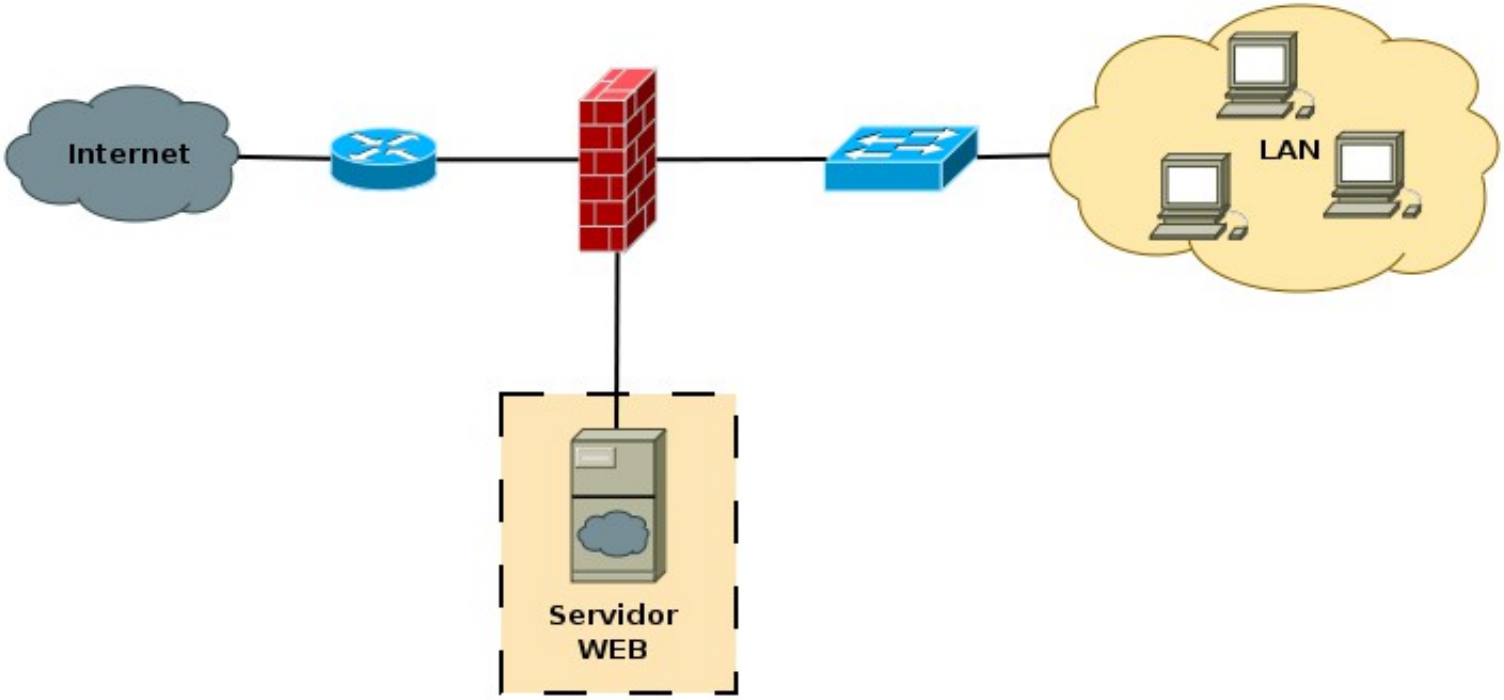
- Esquema típico de firewall para proteger una red local conectada a internet a través de un router. El firewall debe colocarse entre el router (con un único cable) y la red local (conectado al switch o al hub de la LAN)



- Dependiendo de las necesidades de cada red, puede ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema.

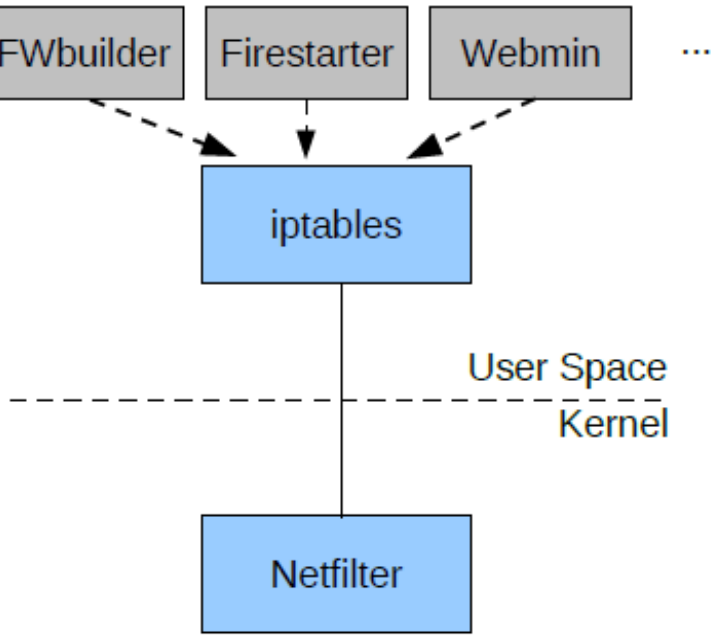
Esquema típico de un firewall (DMZ)

- Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo, etc..), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos.

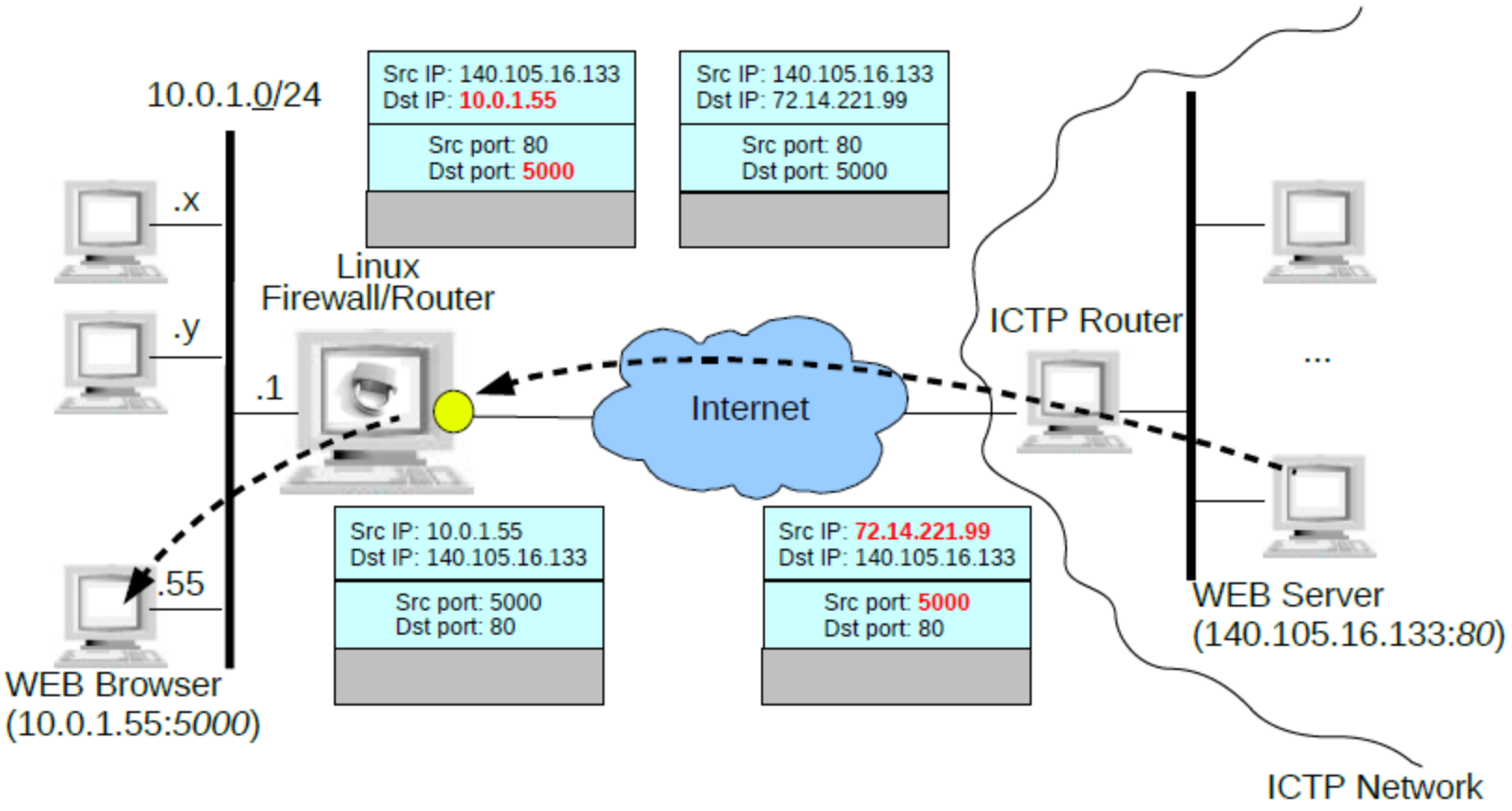


Que es IPTABLES

- IPtables es un sistema de firewall vinculado al kernel de linux que se ha extendido enormemente a partir del kernel 2.4



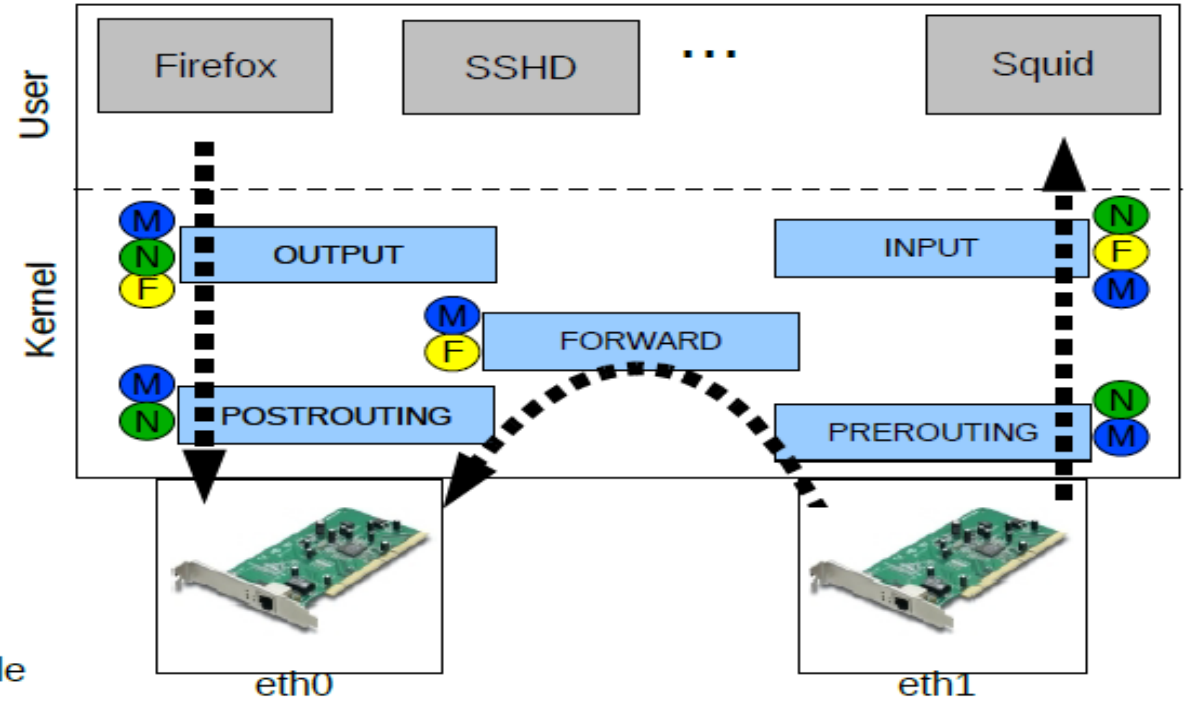
Como funciona Iptables (NAT)



Interface with public IP address 72.14.221.99 that is masqueraded

Como funciona Iptables (Filtering)

- Como se ve en el gráfico, básicamente se mira si el paquete esta destinado a la propia maquina o si va a otra. Para los paquetes (o datagramas) que van a la propia maquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o maquinas se aplican simplemente reglas FORWARD.



Como funciona Iptables

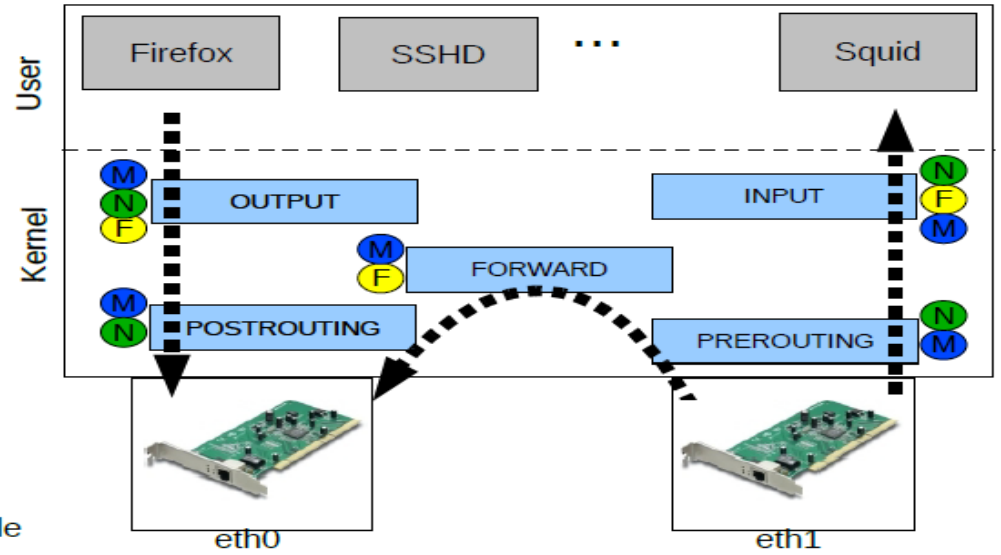
En cuanto a los paquetes, el total del sistema de filtrado de paquetes del kernel se divide en tres tablas, cada una con varias chains a las que puede pertenecer un paquete.

filter: Tabla por defecto, para los paquetes que se refieran a nuestra máquina

INPUT: Paquetes recibidos para nuestro sistema

FORWARD: Paquetes enrutados a través de nuestro sistema

OUTPUT: Paquetes generados en nuestro sistema y que son enviados



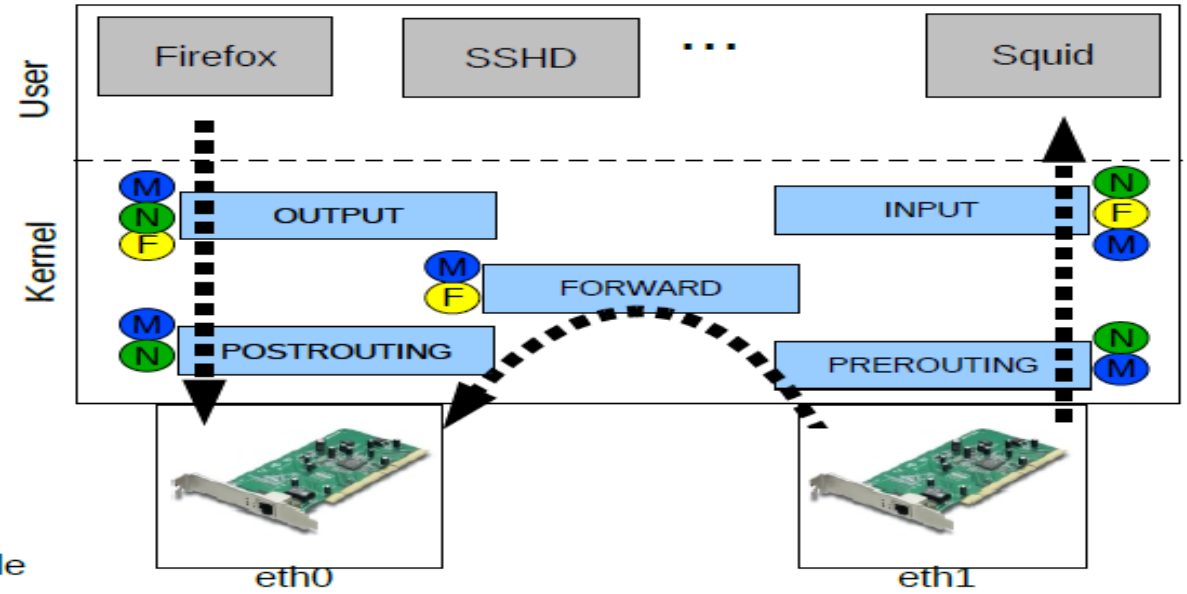
Como funciona Iptables

nat: Tabla referida a los paquetes enrutados en un sistema con Masquerading

PREROUTING: Para alterar los paquetes según entren

OUTPUT: Para alterar paquetes generados localmente antes de enrutar

POSTROUTING: Para alterar los paquetes cuando están a punto para salir

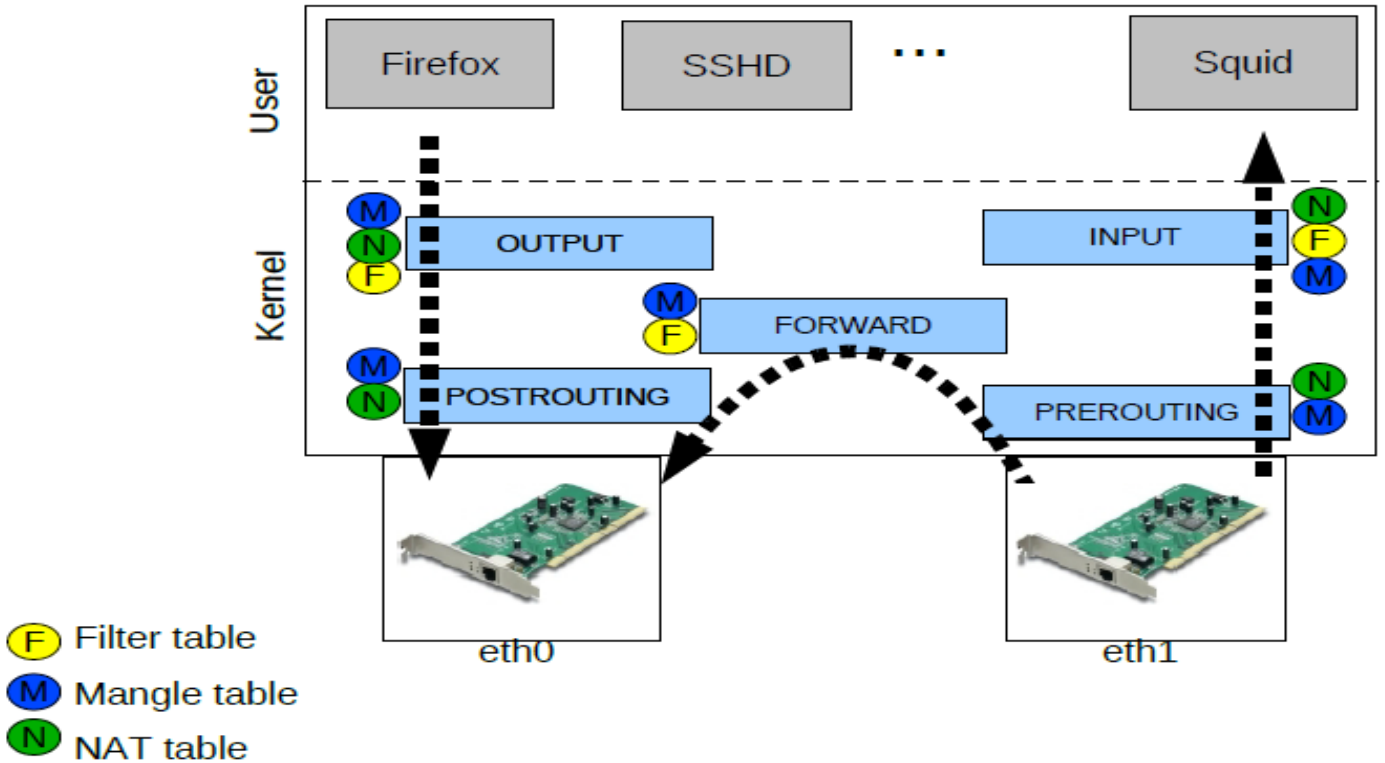


Como funciona Iptables

mangle: Alteraciones más *especiales* de paquetes

PREROUTING: Para alterar los paquetes entrantes antes de enrutar

OUTPUT: Para alterar los paquetes generados localmente antes de enrutar



Como funciona Iptables (Filtering)

- Ejemplo de una linea en Iptables

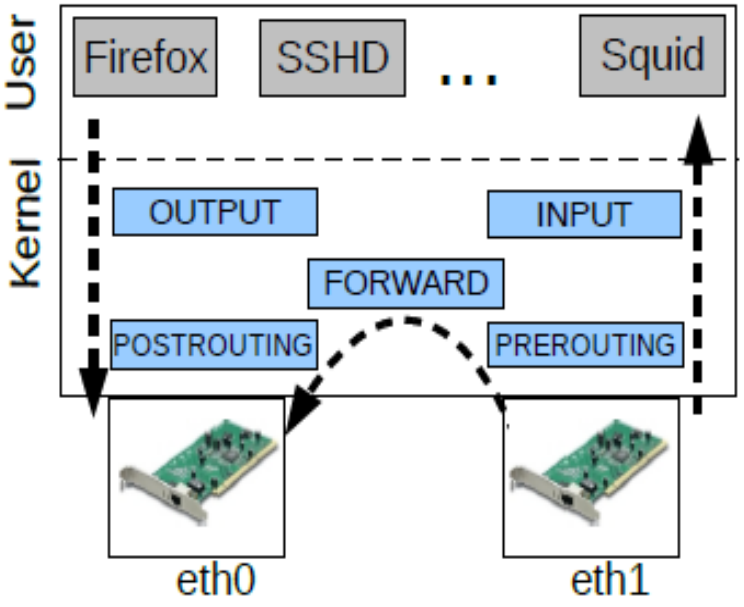


Table	-t filter
Operation	-A
Hook	INPUT
Match/es	-p icmp –icmp-type echo-request
Target	-j DROP

#iptables | -t filter | -A | INPUT | -p icmp --icmp-type echo-request | -j DROP

Como funciona Iptables (Filtering)

- **Ejemplos:**

iptables -A INPUT -i eth0 -p tcp --dport 22 -jACCEPT

iptables -A FORWARD -s 192.168.10.0/24 -i eth1 -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -i eth0 -s 89.19.20.2 -j DROP

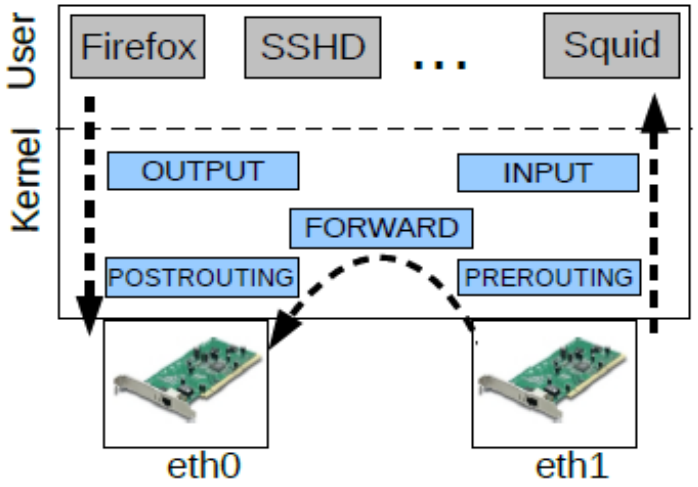


Table	-t filter
Operation	-A
Hook	INPUT
Match/es	-p icmp –icmp-type echo-request
Target	-j DROP

#iptables	-t filter	-A	INPUT	-p icmp --icmp-type echo-request	-j DROP

Especificación de reglas

-p [protocolo]: Protocolo al que pertenece el paquete.

-s [origen]: dirección de origen del paquete, puede ser un nombre de host, una dirección IP normal, o una dirección de red (con máscara, de forma dirección/máscara).

-d [destino]: Al igual que el anterior, puede ser un nombre de host, dirección de red o dirección IP singular.

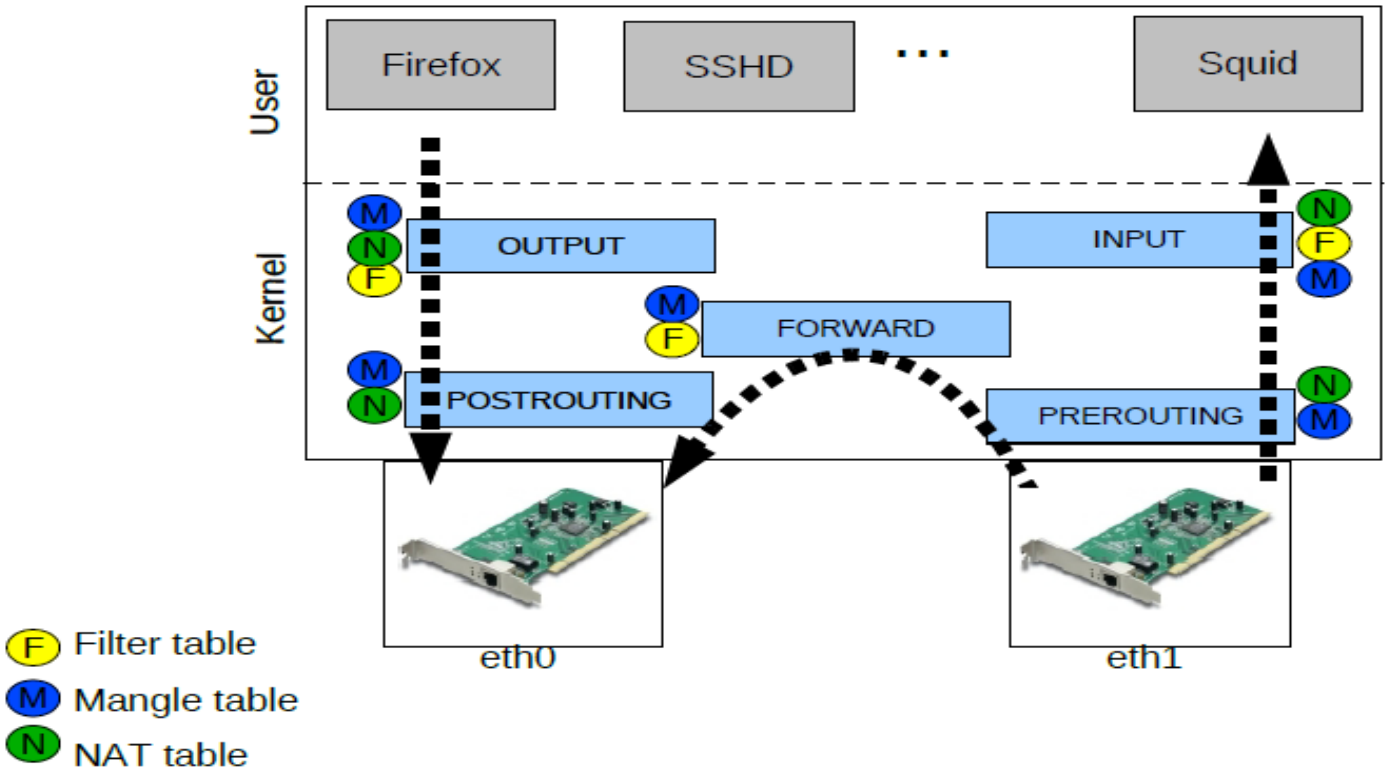
-i [interfaz-entrada]: Especificación del interfaz por el que se recibe el paquete.

-o [interfaz-salida]: Interfaz por el que se va a enviar el paquete.

[!] -f: Especifica que la regla se refiere al segundo y siguientes fragmentos de un paquete fragmentado. Si se antepone !, se refiere sólo al primer paquete, o a los paquetes no fragmentados.

Como funciona Iptables (NAT)

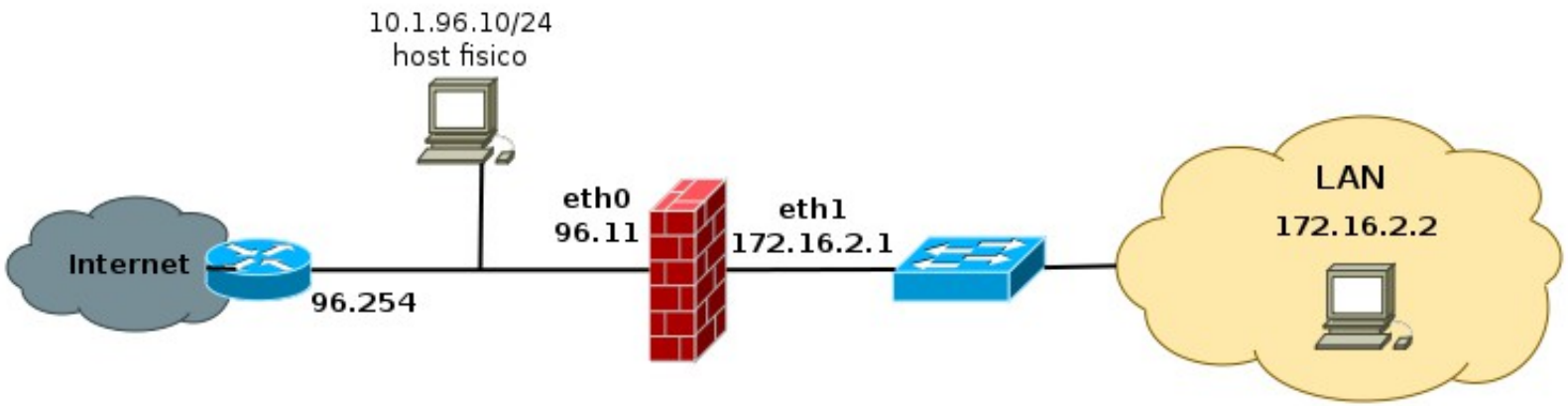
- iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth0 -j MASQUERADE
- iptables -t nat -A POSTROUTING -s 10.1.120.21 -o eth0 -j MASQUERADE
- iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.10.12:80



Ejercicio #1

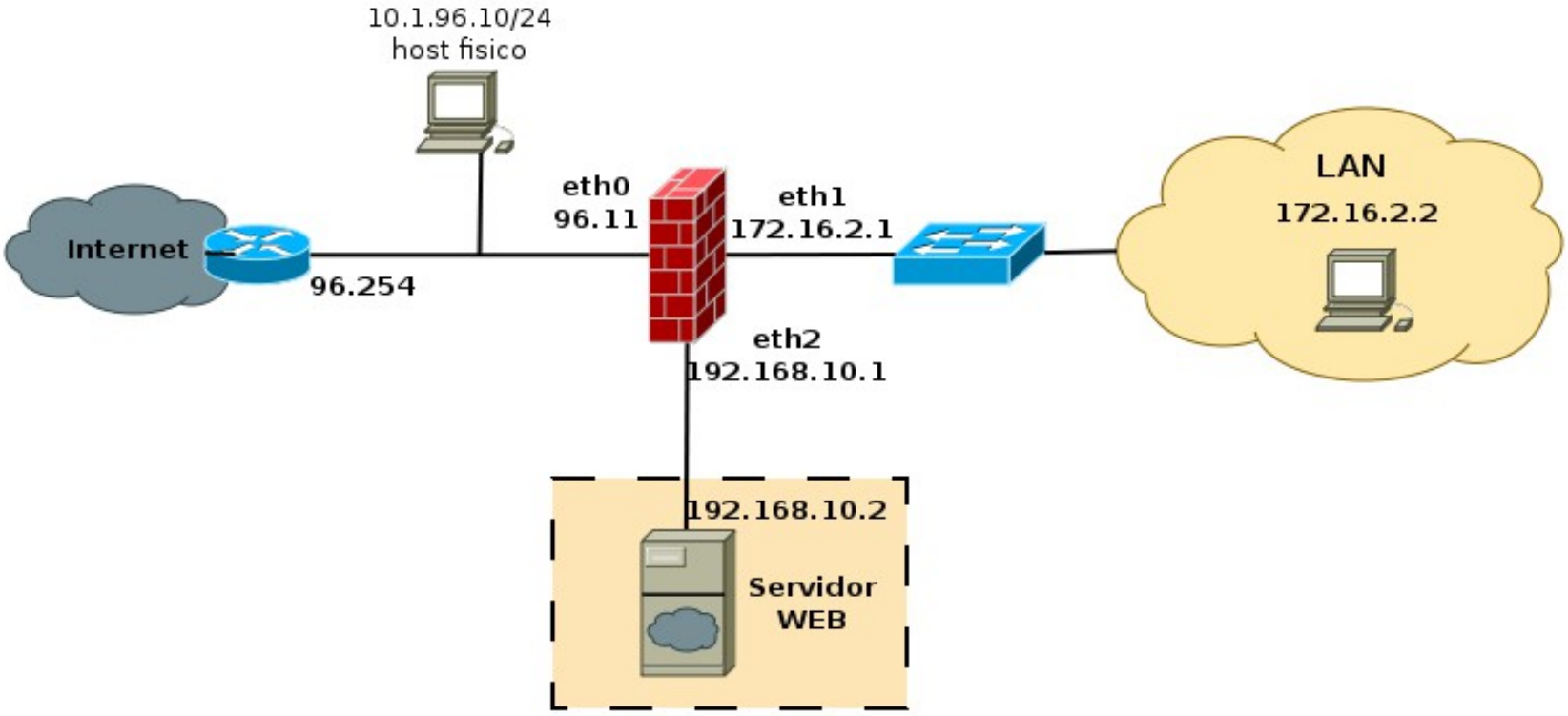
- Creacion de un Firewall LAN, con acceso a Internet.

  –Acceso total a equipos de la LAN
  –NAT, usuarios LAN puedan acceder a Internet.
  –Activar ip forwarding.
  – IP firewall 172.16.2.1 y la PC 172.16.2.2 /24

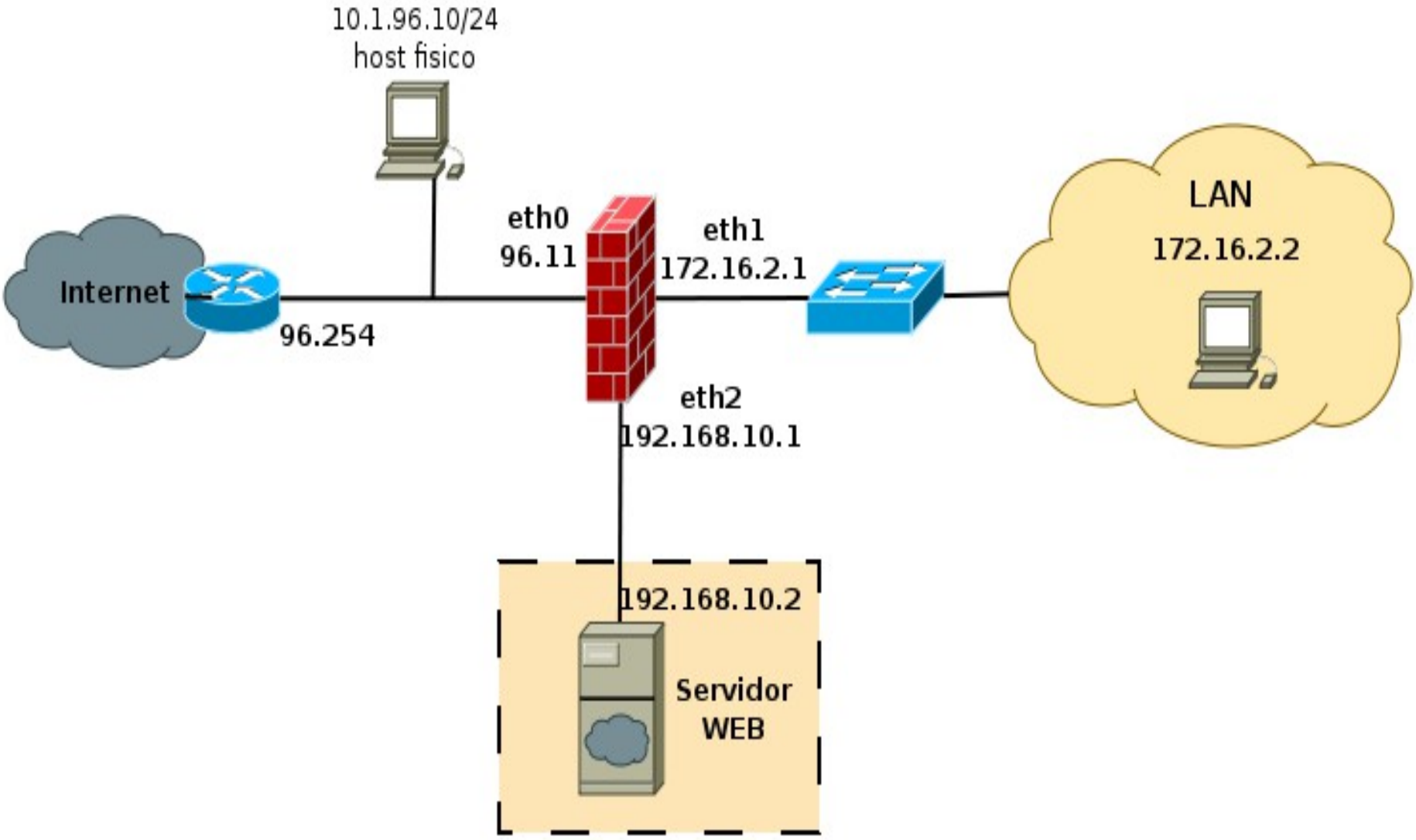


Ejercicio #2

- Creacion de un Firewall LAN, con acceso a Internet.
  - –Acceso por medio ssh desde LAN al DMZ
  - –NAT, usuarios LAN puedan acceder a Internet.
  - –Activar ip forwarding.
  - – Permitir acceso al web desde el exterior.



Topología Ejercicio # 2



Análisis de Topología

- Consideran posible la implementacion de esta herramientas en sus Universidades??
- Que requisitos consideran necesarios, para poder implementar estas soluciones?
- En cuanto tiempo consideran que podrian implementarlo

Ejemplos

```
#!/bin/sh
echo -n Aplicando Reglas de Firewall...
## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

## Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
```

Ejemplos

```
## Nota: eth0 es el interfaz conectado al router y eth1 a la LAN
## acceso al firewall desde la red local
iptables -A INPUT -s 172.16.2.0/24 -i eth1 -j ACCEPT

## Activacion del ip forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

# Ahora hacemos enmascaramiento de la red local
iptables -t nat -A POSTROUTING -s 172.16.2.0/24 -o eth0 -j MASQUERADE

## Permitimos el acceso desde el exterior a los puertos 80 y 443 de DMZ
iptables -A FORWARD -d 192.168.10.2 -p tcp -dport 80 -j ACCEPT
iptables -A FORWARD -d 192.168.10.2 -p tcp -dport 443 -j ACCEPT

echo " OK . Verifique que lo que se aplica con: iptables -L -n
```