1. **ACTIVAR IP\_FORWARD EN EL GATEWAY (En los 2 Gateway’s)**

*Permite el Puente entre lo que sale de la red hacia el exterior. Comando solo comprueba.*

**cat /proc/sys/net/ipv4/ip\_forward**

1. **Activar enmascaramiento (router – dentro de activaEmmascarament.sh)**

***Postrouting****: para los paquetes que salen*

*-t nat: utilizaremos nat para poder enmascarar*

*-o eth2: enmascarar todo lo que sale por esta interfaz*

**iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE**

1. ***Conseguiremos que los departamentos tengan acceso a internet, paso necesario(router)***

***Postrouting****: para los paquetes que salen*

***192.168.2.0/24:*** *la red desde donde salen los paquetes*

***192.168.1.2:*** *quien tiene que marcar los paquetes, en este caso el gateway, ip publica*

**iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth1 -j SNAT --to 192.168.1.2**

1. **DEFINIR UN DEFAULT GATEWAY EN LAS WORKSTATIONS**

*Para que el gateway pueda hacer de Pasarela entre los nodos e internet*

route add default gw 192.168.2.1 dev eth0

1. **Añadimos un camino por defecto al router, para que pueda tener salida a internet(En router)**

ip route add default via 192.168.1.1 dev eth1

1. **Forward (en router, no segura)**

**-t [Nombre de table]: le damos un nombre a la tabla donde agregaremos la regla, en caso de no poner nada, se agregara a la table predefinida”filter”**

**-A [Tipo de regla]: Añadir nueva regla a la tabla. En este caso Forward para enrutamiento.**

**-s [IP origen] : ip de origen, en este caso la red de origen desde donde obtenemos salida de una IP en concreto de nodo.**

**-j []: aceptar la regla cuando se cumpla la condición de origen.**

iptables -A FORWARD -s 192.168.2.32/27 -j ACCEPT

1. Agregar regla en Router

ip route add 192.168.2.32/27 dev eth2

4. LIMITACIÓ DE L’AMPLE DE BANDA UTILITZAT PER CADA SUBXARXA (12.2. El clasificador route)

¡No confunda esta qdisc sencilla y sin clases con la PRIO con clases! Aunque se comportan de manera similar.

Cada token que llega toma un paquete de datos entrante de la cola de datos y se elimina del bucket. Asociar este algoritmo con los dos flujos (tokens y datos).

Primero tenemos que marcar los paquetes y asi poder activar el ancho de banda, según cada subred de origen(función marcar() )

# ip route add Máquina/Red via Pasarela dev Dispositivo realm NúmeroDominio

tc qdisc add dev ppp0 root tbf rate 220kbit latency 50ms burst 1540

15.10.2. Clasifición de paquetes

Referencias

<https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-iptables>

<https://netfilter.org/documentation/HOWTO/es/NAT-HOWTO-7.html>