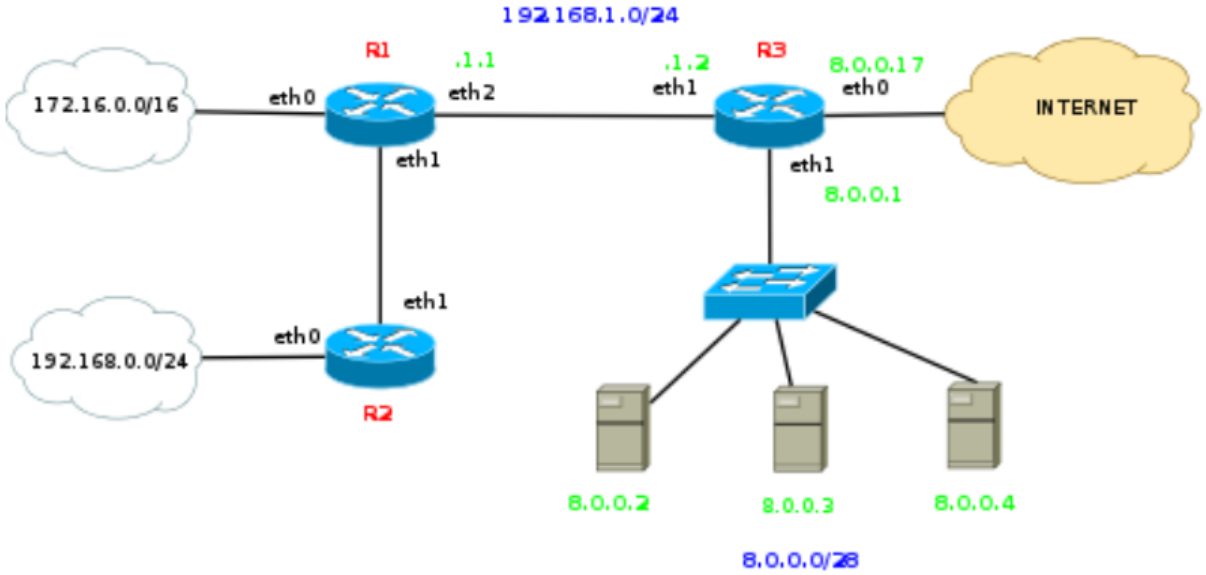
Ejercicios de Firewalls

Ejercicio 1



Desarrolle los firewalls que considere oportunos en cada router MikroTik para que se cumplan los siguientes requisitos:

- La red 192.168.0.0/24 solo deberá poder acceder a Internet y a los servidores web (8.0.0.2) y DNS (8.0.0.3).

En el router 2:
/ip firewall filter
add chain=forward dst-address=8.0.0.2 in-interface=eth0 action=accept
add chain=forward dst-address=8.0.0.3 in-interface=eth0 action=accept
add chain=forward dst-address=8.0.0.0/28 in-interface=eth0 action=drop
    //bloqueo la entrada a DMZ todo lo demás
add chain=forward dst-address=172.16.0.0/16 in-interface=eth0 action=drop
    //bloqueo la entrada a la red 172.16.0.0/16

Al hacer esto estoy dando solo entrada al servidor web y a la DNS y tbn a Internet de forma indirecta bloqueando lo demás.

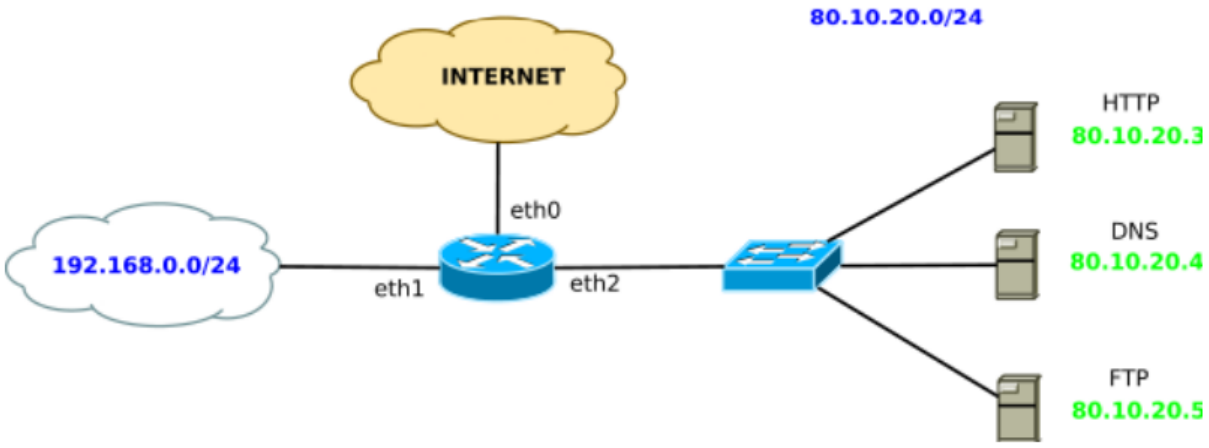
- Desde Internet no se deberá poder acceder al servidor 8.0.0.4, pero sí a los puertos 80 y 443 de TCP del servidor con dirección IP 8.0.0.2 y al puerto 53 mediante UDP del servidor con dirección 8.0.0.3.

En el router 3:
/ip firewall filter
add chain=forward dst-address=8.0.0.2 in-interface=eth0 dst-port=80,443 protocol=tcp action=accept
add chain=forward dst-address=8.0.0.3 in-interface=eth0 dst-port=53 protocolo=udp action=accept
add chain=forward connection-state=established,related in-interface=eth0 action=accept
add chain=forward in-interface=eth0 action=drop

- Se deberá impedir el acceso a los router mediante telnet o SSH de todos los hosts excepto aquellos cuya dirección IP se encuentre en el rango 172.16.0.10-172.16.0.20

En todos los routers:
/ip firewall filter
add chain=input dst-port=22,23 protocol=tcp src-address=172.16.0.10-172.16.0.20 action=accept
add chain=input action=drop

Ejercicio 2



Desarrolle los firewalls que considere oportunos en cada router MikroTik para que se cumplan los siguientes requisitos:

- El PC 192.168.0.2 deberá acceder a todos los servidores y routers ya que es el del administrador de red.

/ip firewall filter
add chain=forward in-interface=eth1 src-address=192.168.0.2 dst-address=80.10.20.0/24 action=accept
add chain=forward in-interface=eth1 action=drop

- Los PC de la red interna que se encuentran en el rango 192.168.0.200-192.168.0.254 deberán tener conexión a internet, el resto no.

/ip firewall filter
add chain=forward src-address=192.168.0.200-192.168.0.254 out-interface=eth0 action=accept
add chain=forward src-address=192.168.0.0/24 out-interface=eth0 action=drop

- Al servidor FTP sólo podrán acceder los PC del rango 192.168.0.32 – 192.168.0.199

/ip firewall filter
add chain=forward in-interface=eth1 src-address=192.168.0.32 – 192.168.0.199 dst-port=21 protocol=tcp dst-address=80.10.20.5 action=accept
add chain=forward in-interface=eth1 src-address=192.168.0.0./24 dst-address=80.20.30.5 dst-port=21 protocol=tcp action=drop

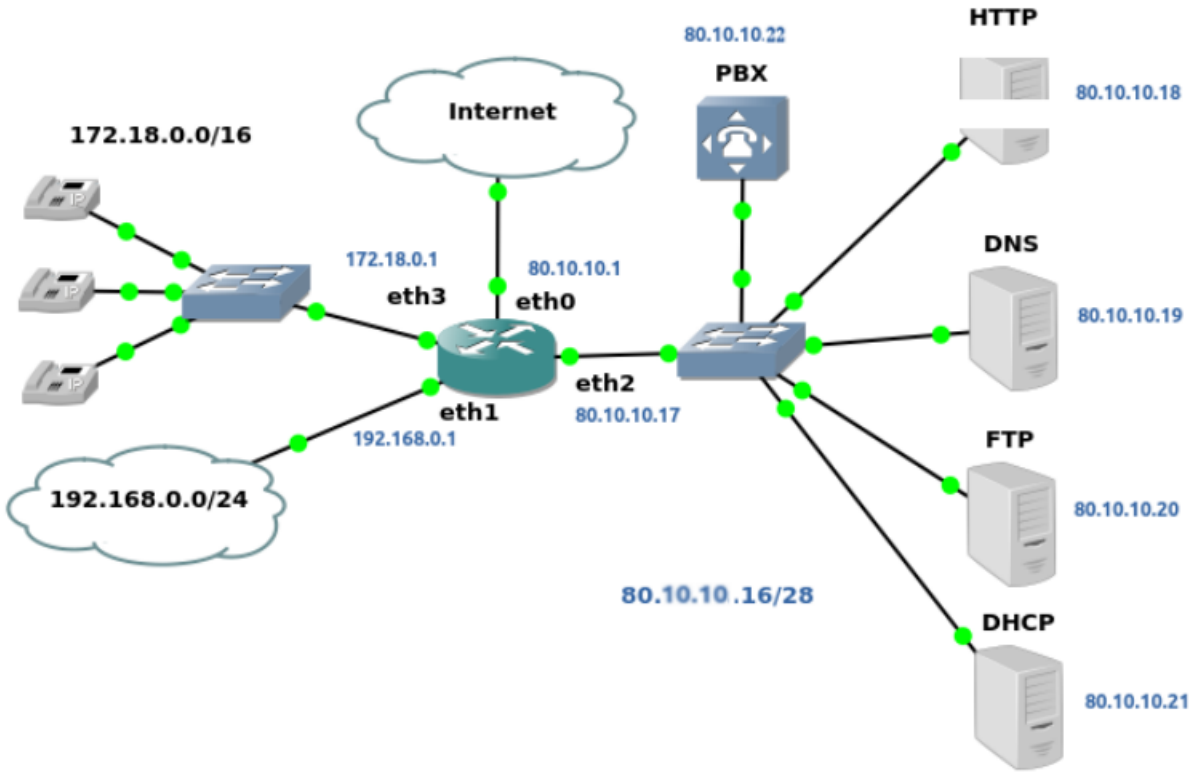
- No se deberá poder acceder al servidor FTP desde internet.

/ip firewall filter
add chain=forward dst-address=80.10.20.5 dst-port=21 protocolo=tcp in-interface=eth0 action=drop

- A los servidores HTTP y DNS se podrá acceder desde Internet.

/ip firewall filter
add chain=forward dst-address=80.10.20.3 dst-port=80,443 protocol=tcp in-interface=eth0 action=accept
add chain=forward dst-address=80.10.20.4 dst-port=53 protocol=udp in-interface=eth0 action=accept
add chain=forward connection-state=established,related in-interface=eth0

Ejercicio 3



- Deberá poderse acceder a los servicios HTTP, DNS, y FTP desde Internet.
- Controlar el acceso de paquetes desde internet hacia la red interna. Sólo deberá permitirse tráfico para conexiones establecidas desde el interior y tráfico relacionado.
- Al router no se deberá poder acceder desde Internet, ni desde la red de telefonía, ni desde servidores.
- Permitir el servicio de VoIP desde internet con la centralita Asterisk:
    - SIP mediante UDP en el puerto 5060.
    - IAX2 mediante el puerto UDP 4569
    - RTP mediante puertos 10000:20000 UDP.
- Controlar acceso desde la red de telefonía: SIP, RTP, DNS, DHCP
- El acceso al servicio DHCP desde la red interna deberá estar permitido (DHCP relay).

Servicio DHCP Relay requiere que se acepten también paquetes entrantes por el puerto 67 y salientes por el puerto 68.add chain=input src-address=192.168.0.0/24 in-interface=eth1 action accept

add chain=input action=drop
/ip firewall filter
add chain=input dst-port=67 protocol=udp in-interface=eth1 action=accept
	//Peticiones de host desde la red de datos
add chain=input dst-port=67 protocol=udp in-interface=eth3 action=accept
	//Peticiones de host desde la red de telefonía
add chain=input dst-port=68 src-port=67 protocol=udp in-interface=eth2 src-address=80.10.10.21
	//Respuestas desde el servidor DHCP
add chain=input src-address=192.168.0.0/24 in-interface=eth1 action accept
add chain=input action=drop

/ip firewall filter
add chain=forward in-interface=eth0 dst-port=80,443 protocol=tcp dst-address=80.10.10.18 action=accept //Publica el servicio HTTP desde Internet

add chain=forward in-interface=eth0 dst-port=53 protocol=udp dst-address=80-10.10.19 action=accept //Publica el servicio DNS desde Internet

add chain=forward in-interface=eth0 dst-port=21 protocol=tcp dst-address=80.10.10.21 action=accept //Publica el servicio FTP desde Internet

add chain=forward in-interface=eth0 dst-port=5060 protocol=udp dst-address=80.10.10.22 action=accept //Publica el servicio SIP desde Internet

add chain=forward in-interface=eth0 dst-port=4569 protocol=udp dst-address=80.10.10.22 action=accept //Publica el servicio IAX2 desde Internet

add chain=forward in-interface=eth0 dst-port=1000-2000 protocol=udp dst-address=80.10.10.22 action=accept //Publica el servicio RTP desde Internet

add chain=forward connection-state=established,related in-interface=eth0 //Permite el tráfico de respuesta desde Internet

add chain=forward in-interface=eth0 action=drop //Todo lo demás que venga desde Internet lo prohibo

add chain=forward in-interface=eth3 dst-port=5060 protocol=udp dst-address=80.10.10.22 action=accept //Publica el servicio SIP desde telefonía

add chain=forward in-interface=eth3 dst-port=1000-2000 protocol=udp dst-address=80.10.10.22 action=accept //Publica el servicio RTP desde telefonía

add chain=forward in-interface=eth3 dst-port=53 protocol=udp dst-address=80.10.10.19 action=accept //Publica el servicio DNS desde telefonía

add chain=forward in-interface=eth3 dst-port=67 protocol=udp dst-address=80.10.10.21 action=accept //Publica el servicio DHCP desde telefonía

add chain=forward in-interface=eth3 action=drop //Todo lo demas que venga desde telefonía lo prohibo

add chain=forward in-interface=eth1 dst-address=80.10.10.22 action=drop //Impide el acceso a la PBX desde la red de datos

add chain=forward in-interface=eth1 dst-port=80,443 protocol=tcp dst-address=80.10.10.18 action=accept //Acceso al servicio HTTP desde la red de datos

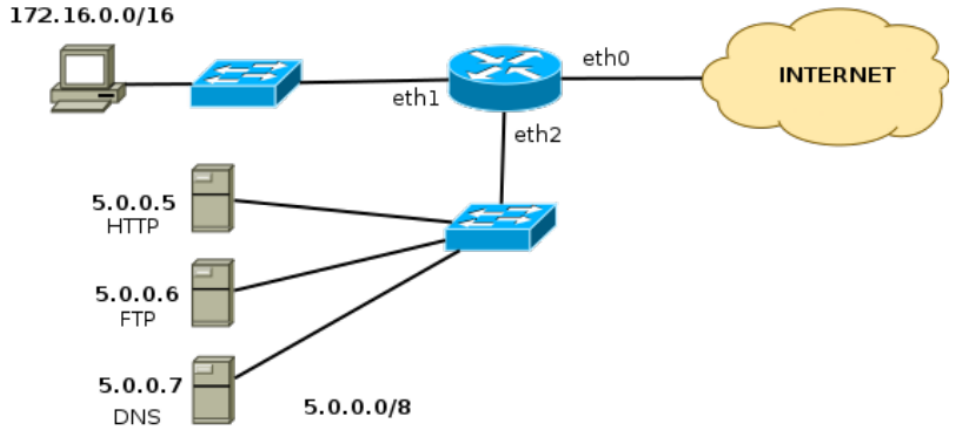
add chain=forward in-interface=eth1 dst-port=53 protocol=udp dst-address=80.10.10.19 action=accept //Acceso al servicio DNS desde la red de datos

add chain=forward in-interface=eth1 dst-port=21 protocol=tcp dst-address=80.10.10.20 action=accept //Acceso al servicio FTP desde la red de datos

add chain=forward in-interface=eth1 dst-port=67 protocol=tcp dst-address=80.10.10.21 action=accept //Acceso al servicio DHCP desde la red de datos

add chain forward in-interface=eth1 out-interface=eth3 action=drop //Deniega el acceso desde la red de datos a la red de telefonía

Ejercicio 4



- Se deberá poder acceder al servicio web y DNS desde Internet. El servidor FTP no deberá tener acceso desde la red externa.
- El host 172.16.0.200 será el único que podrá acceder al router por SSH.
- Los hosts de la red interna tienen prohibido el acceso a cualquier servidor FTP externo.
- Los hosts del rango 172.16.0.5-172.16.0.20 no deben tener acceso a Internet, pero sí a los servidores.
- No se debe permitir ninguna conexión desde el exterior hacia los hosts de la red 172.16.0.0/16. Los paquetes correspondientes a los servicios y a las conexiones previamente establecidas desde la red interna sí deberían dejarse pasar.

/ip firewall filter
add chain=input src-address=172.16.0.200 dst-port=22 protocol=tcp action=accept

add chain=forward in-interface=eth0 dst-port=80,443 protocol=tcp dst-address=5.0.0.5 action=accept

add chain=forward in-interface=eth0 dst-port=53 protocol=udp dst-address=5.0.0.7 action=accept

add chain=forward in-interface=eth2 connection-state=established,related

add chain=forward in-interface=eth1 connection-state=established,related

add chain=forward in-interface=eth1 dst-port=21 protocol=tcp out-interface=eth0 action=drop
//Los host de la red interna tienen prohibido acceso a cualquier servidor FTP externo

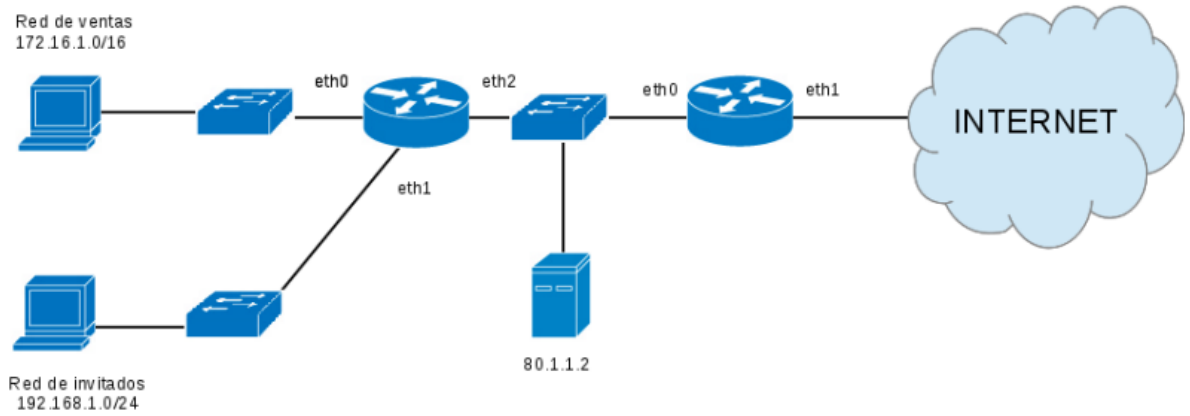
add chain=forward src-address=172.16.0.5-172.16.0.20 out-interface=eth0 action=drop
//Los host del rango no tiene acceso a internet

add chain=forward in-interface=eth0 dst-port=21 protocol=tcp dst-address=5.0.0.6 action=drop

add chain=forward in-interface=eth0 dst-address=172.16.0.0/16 action=drop

add chain=forward action=drop

Ejercicio 5



1. Desarrolle los firewalls que considere oportunos en cada router MikroTik para que se cumplan los siguientes requisitos:

- Impedir el acceso por telnet al router, salvo para el host 172.16.1.5

En todos los routers
/ip firewall filter
add chain=input dst-port=22,23 protocol=tcp src-address=172.16.1.5 action=accept
add chain=input action=drop

- Impedir que el host 192.168.1.5 acceda a Internet, aunque sí deberá conectar con el resto de dispositivos dentro de su red.

En el router 2:
/ip firewall filter
add chain=forward src-address=192.168.1.5 out-interface=eth1 action=drop

- Los host de la red de invitados solo podrán acceder a Internet y al servidor, que es un servidor web.

En el router 1:
/ip firewall filter
add chain=forward src-address=192.168.1.0/24 dst-address=172.16.1.0/24 action=drop

- Desde Internet no se podrá conectar con el servidor, salvo a los puertos 80 y 443.

En el router 2:
/ip firewall filter
add chain=forward in-interface=eth1 dst-port=80,443 protocol=tcp dst-address=80.1.1.2 action=accept
add chain=forward action=drop

- Los hosts del rango 172.16.1.0-172.16.1.255 deberán acceder al servidor a través de ssh, pues son los administradores. Este acceso debería estar vetado para el resto de hosts.

En el router 1:
/ip firewall filter
add chain=input src-address=172.16.1.0-172.16.1.255 dst-port=22 protocol=tcp dst-address=80.1.1.2 action=accept
add chain=input action=drop

- Considere que se utilizan los siguientes protocolos de enrutamiento:
    - RIP como protocolo de pasarela interior.
    - BGP como protocolo de pasarela exterior.

En todos los routers:
/ip firewall filter
add chain=input dst-port=520 protocol=udp action=accept
add chain=input dst-port=179 protocol=tcp action=accept