**REGLAS: 👍 😂**

* Tienen dos partes principales
  + “Matchers” → Condiciones
  + “Actions” → Acciones
* Se analizan en orden
  + Si no se cumple la condición, no se sigue con la siguiente
  + Si se cumple, se ejecuta la acción y no se siguen mirando las siguientes reglas
* En MikroTik las reglas se escriben para una “chain”
  + “input” → Paquetes que van dirigidos al router
  + “output” → Paquetes enviados por el propio router
  + “forward” → Paquetes que atraviesan el router
* Acciones:
  + Accept
  + Reject
  + Drop
* Print stats
* Reset-counters
* Condiciones:
  + src-address, dst-address
  + protocol
  + in-interface, out-interface
  + in-bridge-port, out-bridge-port

**PROTOCOLOS**

**Modelo OSI Modelo TCP/IP DIR PDU**

1. Fisica 1. Enlace MAC TRAMA
2. Acceso al Medio 2. Internet IP PAQUETE
3. Red 3. Transporte Puerto Segmento
4. Transporte 4. Aplicación
5. Sesión
6. Presentación
7. Aplicación

**Protocolos de capas de transporte: TCP, UDP**

* Ambos protocolos permiten multiplexar comunicaciones

**TCP:**

* Orientado a la conexión
* Garantía de orden en la recepción
* Comprobación de entrega
* Control de flujo

**Clientes (requieren de un determinado servicio)**

* Buscan un servidor que les proporcione el servicio
* Usan como destino la IP y el puerto del servicio
* Como origen mi IP y un puerto “al azar”

**El puerto es un número de 16 bits (0-65535)**

* 0-1023 Denominados puertos bien conocidos

Uso restringido

* 1024-40algo
* 40algo-65535

**CONEXIÓN:**

* Son los paquetes de una conversación
* En TCP y UDP se identifican porque tenemos:
  + *IPa: PuertoA → IPa: PuertoB*
  + *IPa: PuertoB → IPa: PuertoA*

En otros protocolos (ICMP) se identifican por otros valores internos

En FW es capaz de reconocer Conexiones. Y cuando se ve un paquete de una conexión, tenemos una propiedad que es el.

**ESTADO DE LA CONEXIÓN:**

* **NEW:** Primer paquete que se ve de una conexión
* **ESTABLISHED:** Conexión que ya se ha visto antes
* **INVALID:** Paquete que no casa bien con lo que espero de una conexión ya establecida

**PORT KNOCKING :**

38,455,99

1. Bloqueamos a todo el que no esté en PERMITIDOS
2. Si se detecta un toque en el puerto 38, añadimos la IP origen a TOQUE1
3. SI alguien de TOQUE1 ‘toca’ en el puerto 455, añadimos IP de origen a TOQUE2
4. Si alguien de TOQUE2 ‘toca’ en el puerto 99, añadimos la IP de origen a PERMITIDOS

action=add-src-to-address-list address-list=nombre protocol=tcp dst-port=elquesea

src-address-list=TOQUE1

src-address-list=!PERMITIDOS

**PRUEBA ROUTER:**

/ip dhcp-client

add interface=ether1

/ip firewall filter

add action=drop chain=input dst-port=8291 protocol=tcp src-address-list=!PERMITIDOS

/ip firewall address-list

add address=192.168.122.1 list=PERMITIDOS

/ip firewall filter

add action=drop chain=input dst-port=8291 protocol=tcp src-address-list=\

!PERMITIDOS

add action=add-src-to-address-list address-list=juan chain=input dst-port=38 \

protocol=tcp

add action=add-src-to-address-list address-list=juan chain=input dst-port=455 \

protocol=tcp

ip/firewall/filter/set 1,2 address-list-timeout=5



