MÓDULO 7 | FIREWALL

- Es un sistema de seguridad de red que protege la red interna del exterior (por ejempo internet)
- Se basa en una serie de reglas que son analizadas de forma secuencial hasta que se produce una coincidencia
- Las reglas de firewall, en RouterOS, se gestionan desde las secciones de ‘*Filter*’ y ‘*NAT*’ en el menú *IP* → *Firewall*

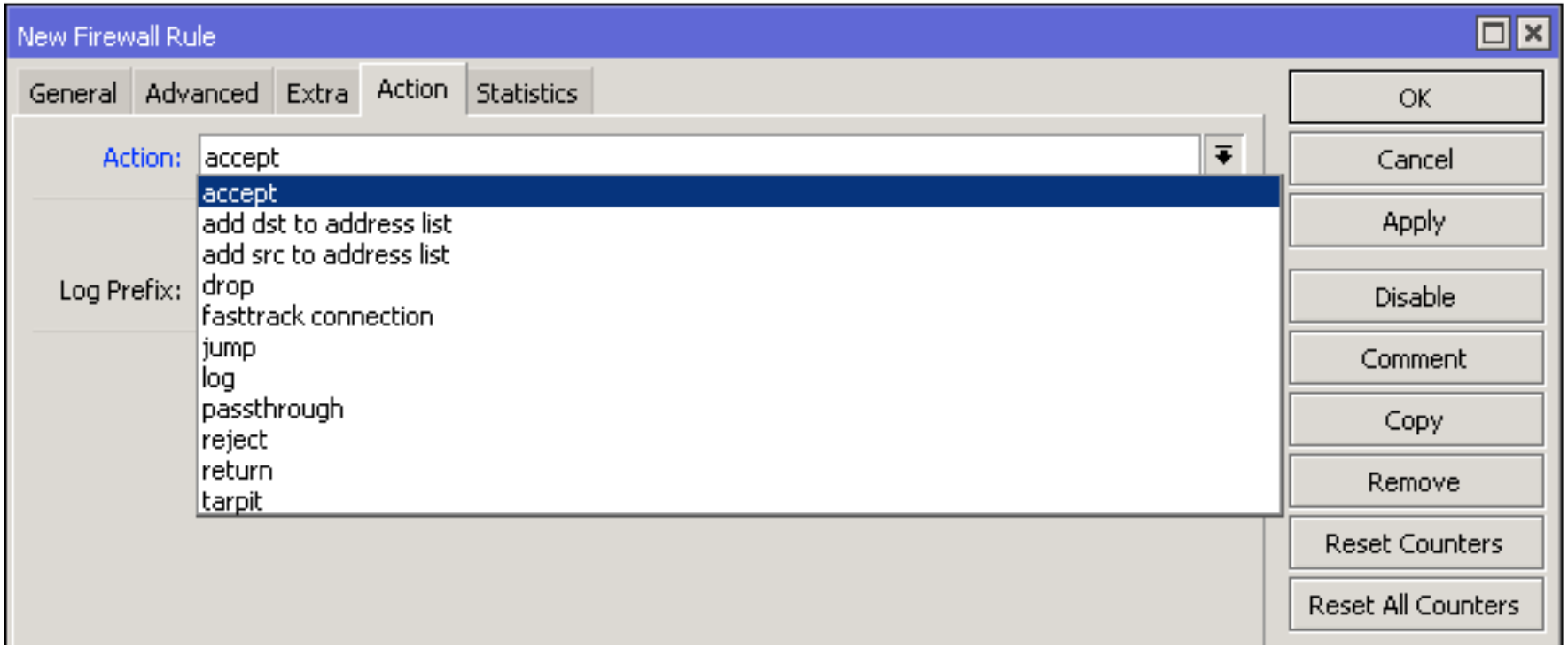
- Funciona según el principio '*Si … entonces*'
- Estructurado en cadenas
- Hay una serie de cadenas predefinidas
- Podemos crear nuevas cadenas, según nuestras necesidades

  - Un paquete que pase por nuestro firewall recorrerá las cadenas de "arriba abajo" hasta que cumpla una de las condiciones (en este caso, "saldrá" del firewall y no seguirá recorriendo las cadenas).

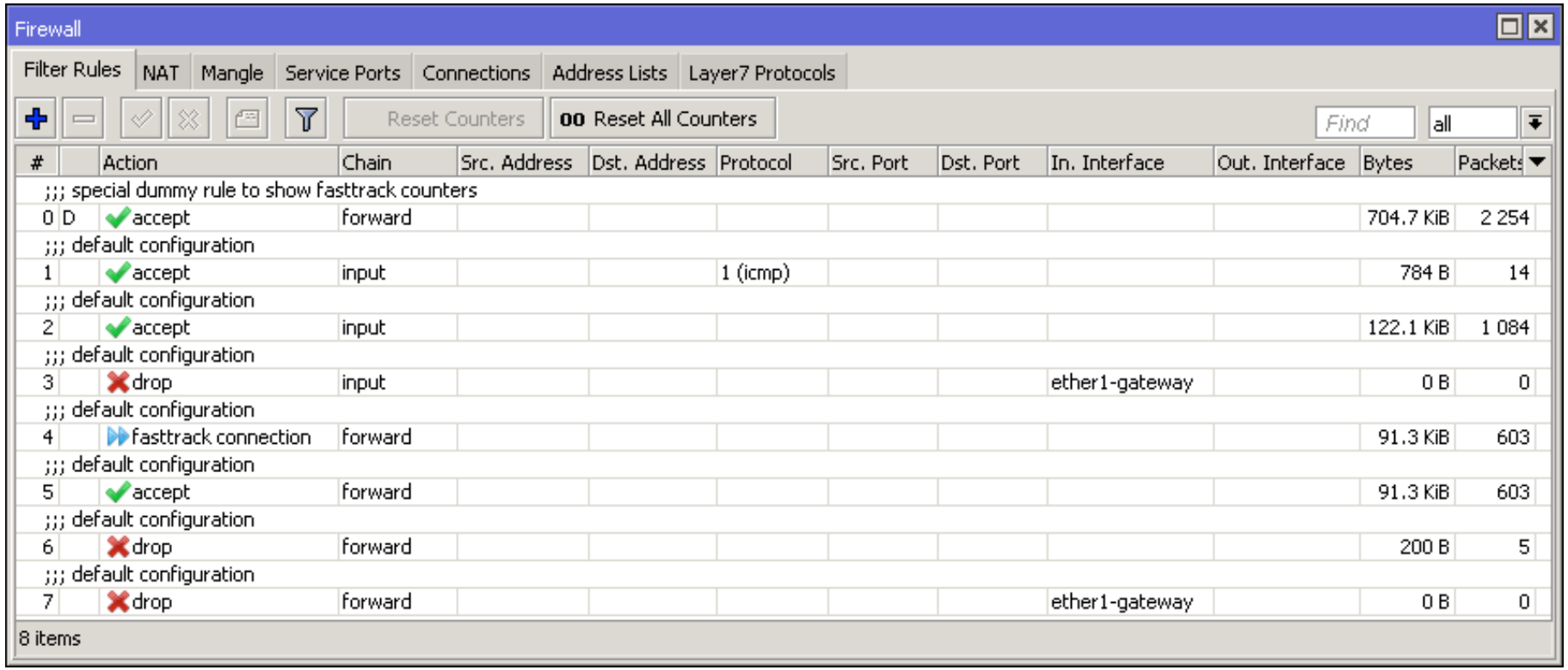
Acciones de las Cadenas Filter

- Cada regla tiene una acción que se ejecuta cuando un paquete coincide con la condición de la regla:
  - Accept
  - Drop
  - Reject : envía un mensaje ICMP de rechazo
  - Jump to : salta a una regla definida por el usuario
  - Return from : vuelve de una cadena de usuario
  - Y, … hay más ! , mirar la página web:
  - http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter#Properties

Acciones de las Cadenas Filter

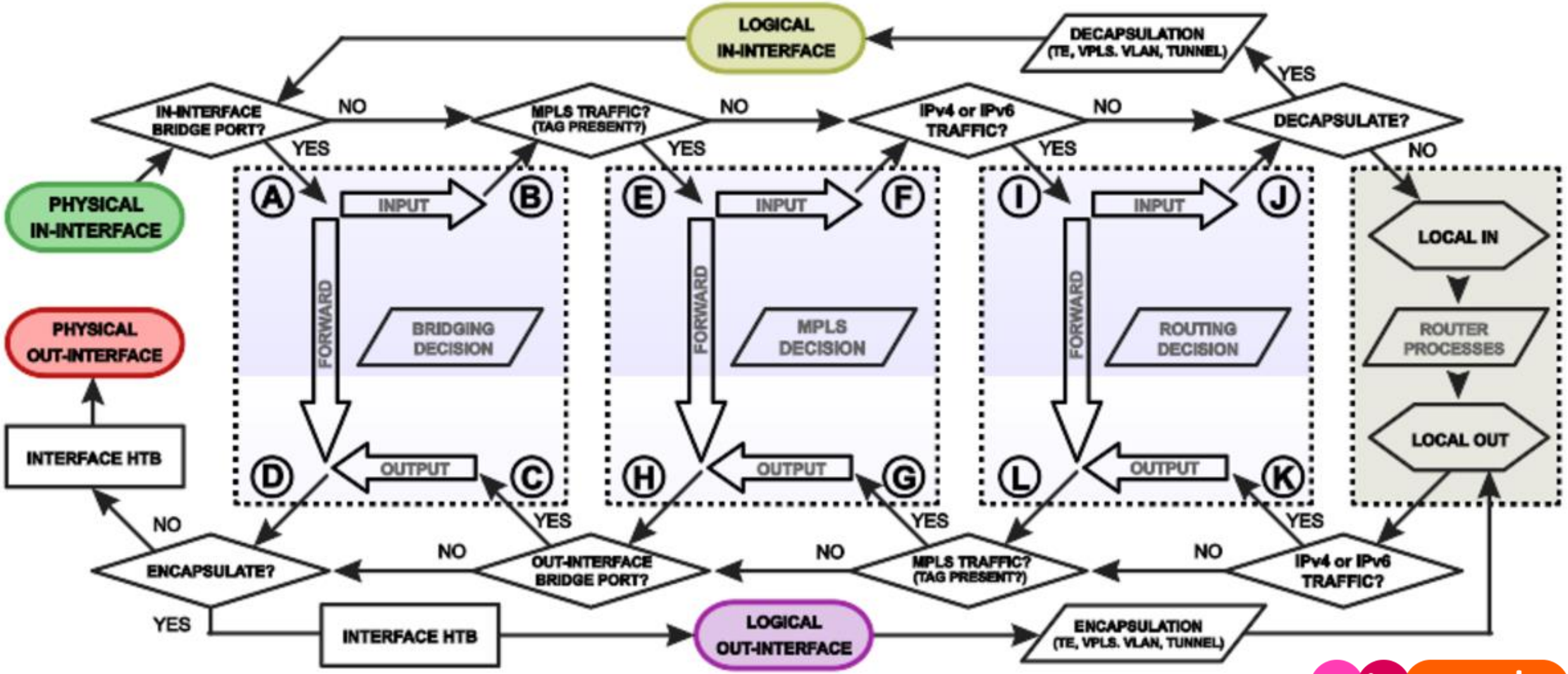


MTCNA módulo 7 Cadenas de Filter

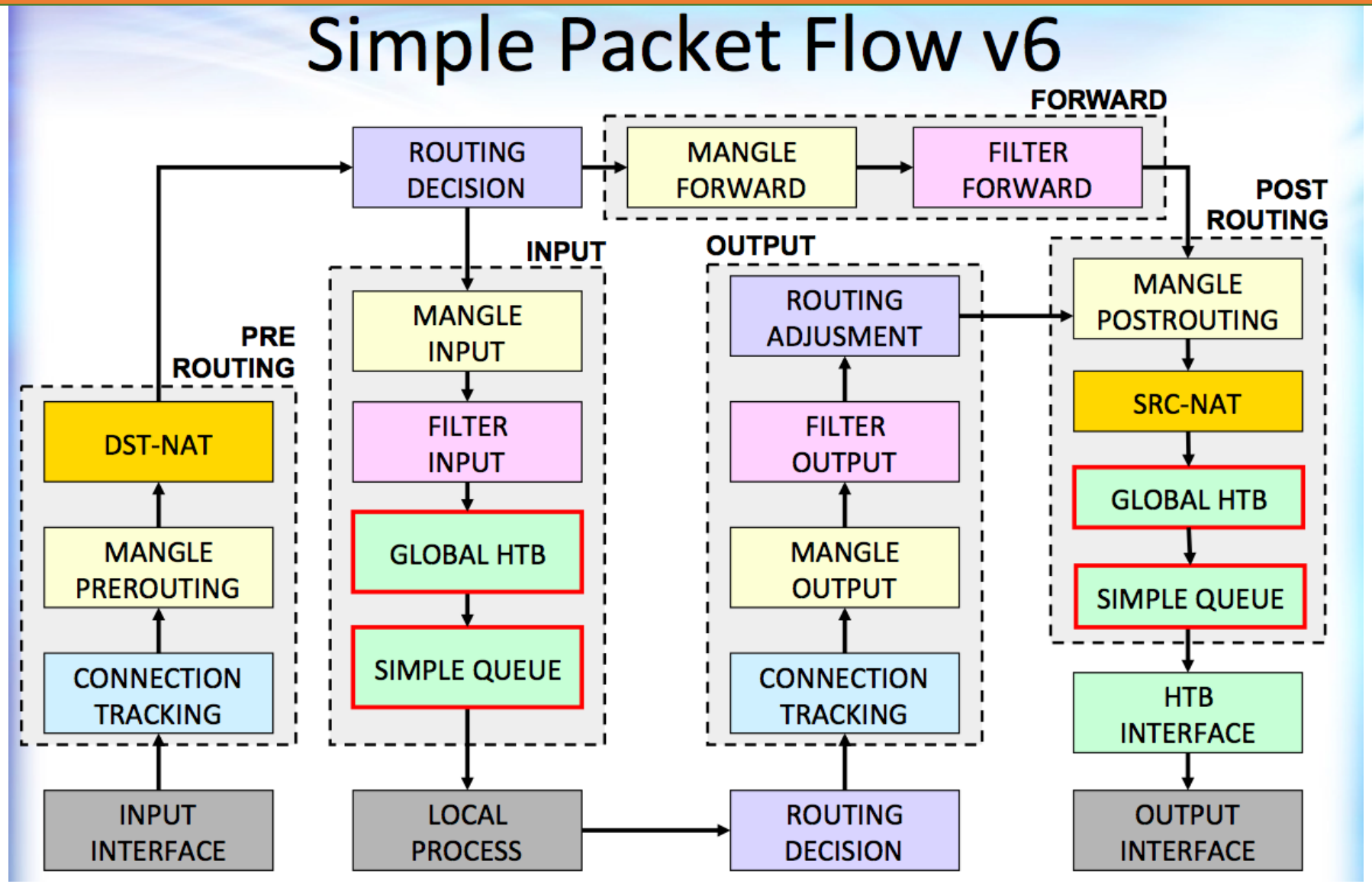


- Consejillo: para mejorar la lectura de las reglas, ordenalas secuencialmente y por cadenas y agrega comentarios

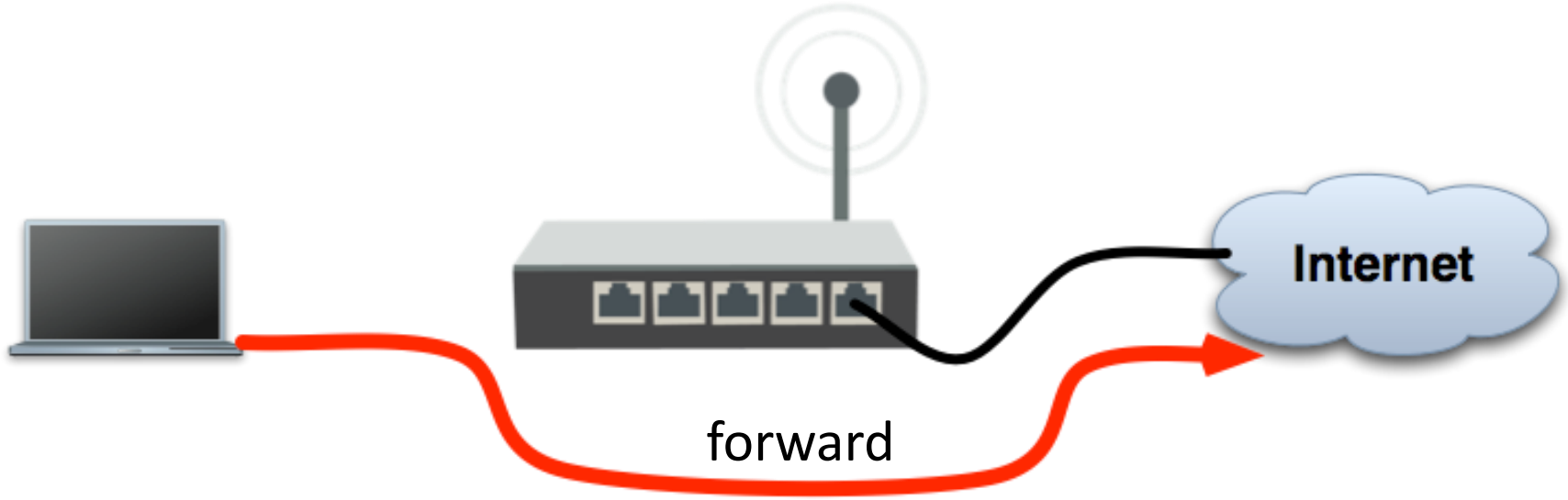
MTCNA módulo 7 Paquet Flow



https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

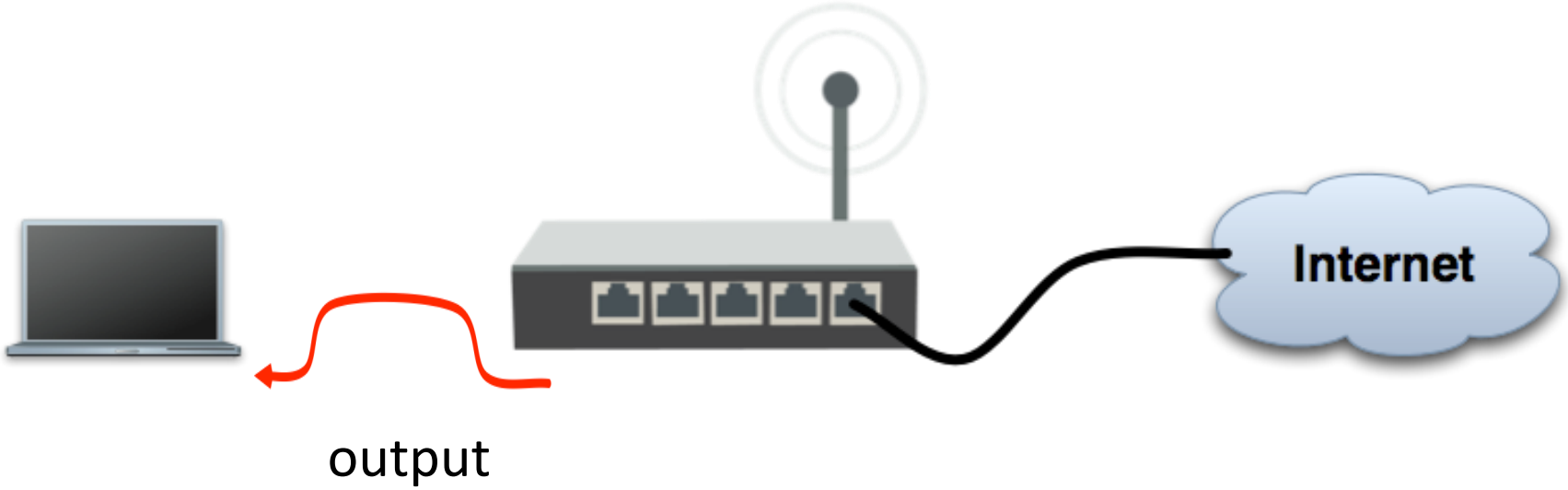

Simple Packet Flow v6
FORWARD
ROUTING DECISION
MANGLE FORWARD
FILTER FORWARD
POST ROUTING
INPUT
OUTPUT
PRE ROUTING
MANGLE INPUT
ROUTING ADJUSMENT
MANGLE POSTROUTING
DST-NAT
FILTER INPUT
FILTER OUTPUT
SRC-NAT
MANGLE PREROUTING
GLOBAL HTB
MANGLE OUTPUT
GLOBAL HTB
SIMPLE QUEUE
CONNECTION TRACKING
SIMPLE QUEUE
CONNECTION TRACKING
HTB INTERFACE
INPUT INTERFACE
LOCAL PROCESS
ROUTING DECISION
OUTPUT INTERFACE

- Contiene las reglas que controlan los paquetes que fluyen a través del router
- Controla el tráfico entre los clientes e Internet, entre Internet y los clientes y entre los propios clientes



- Contiene las reglas cuyo destino sea el propio router
  - Por ejemplo cuando accedemos al winbox

- Contiene las reglas cuyo origen es el router
- Procesos creados en el propio router.
  - Por ejemplo un webproxy

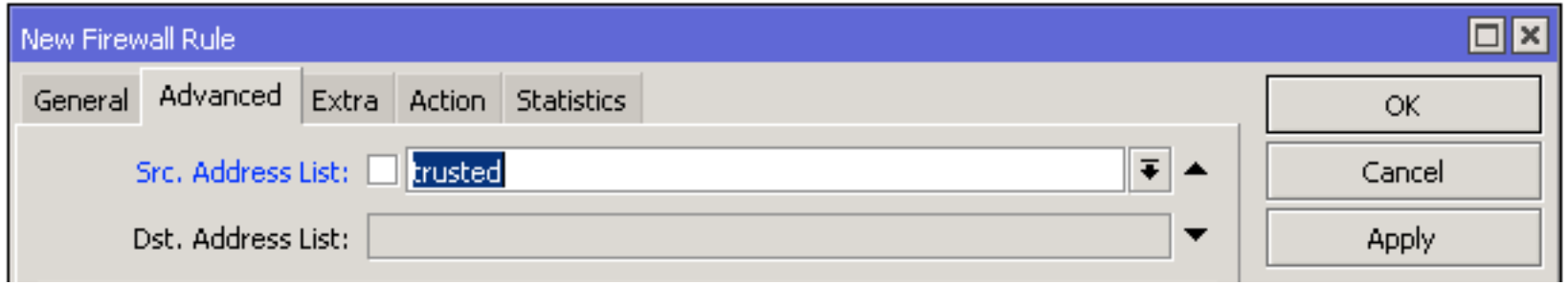


Puerto	Servicio
80/tcp	HTTP
443/tcp	HTTPS
22/tcp	SSH
23/tcp	Telnet
20,21/tcp	FTP
8291/tcp	WinBox
5678/udp	MikroTik Neighbor Discovery
20561/udp	MAC WinBox

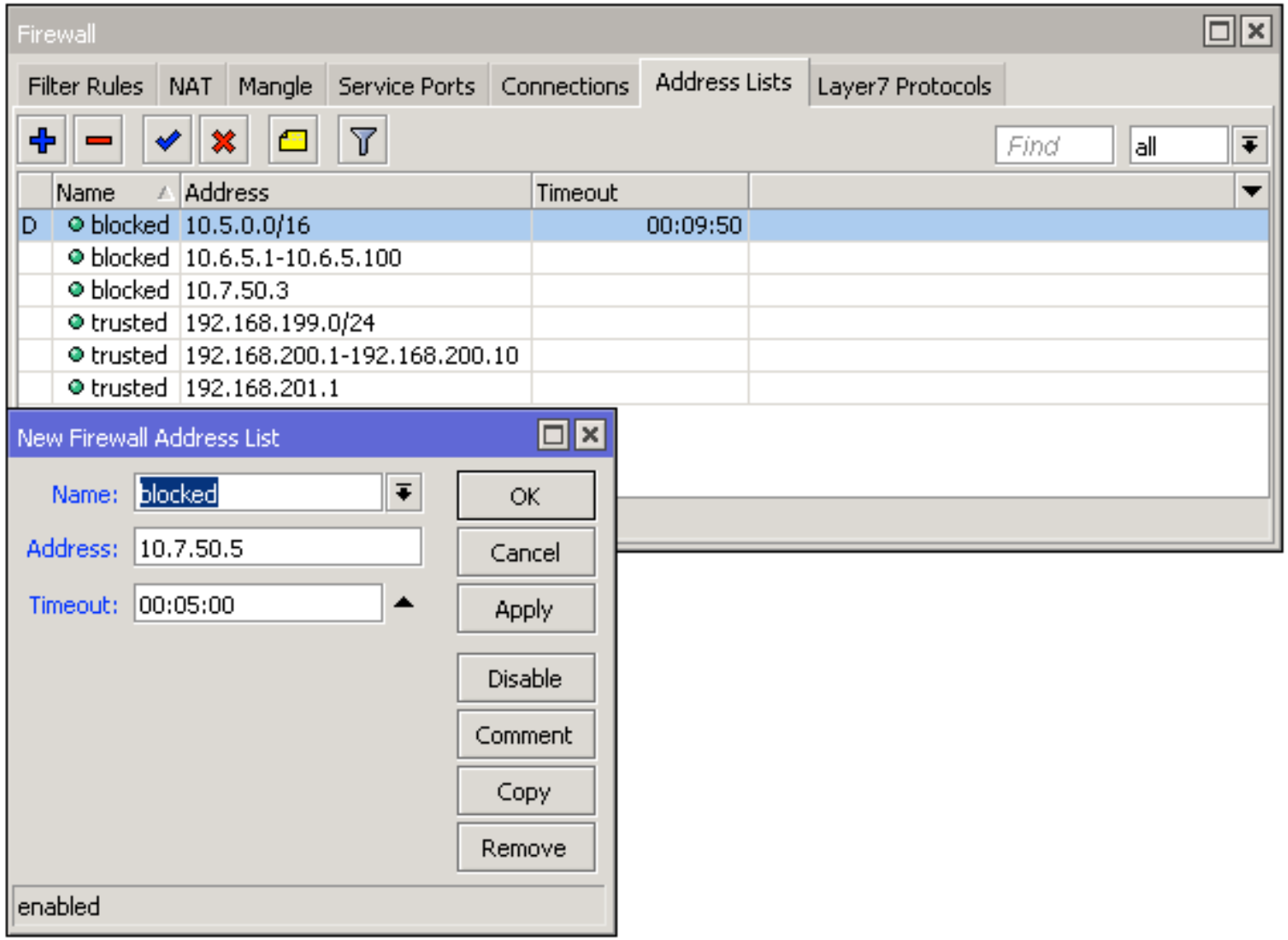
MTCNA módulo 7 Address List

- Las listas de direcciones permiten crear una acción para múltiples direcciones IP de golpe
- Se puede agregar de forma automática una dirección IP a una lista
- La dirección IP se puede agregar de forma indefinida o por un tiempo definido
- Las listas de direcciones pueden contener una dirección IP, un rango IP o toda una subred

- En lugar de especificar una dirección IP en la pestaña de General, ir a la pestaña de Advanced y elegir *Address List* (Src o Dst según el sentido de la regla)

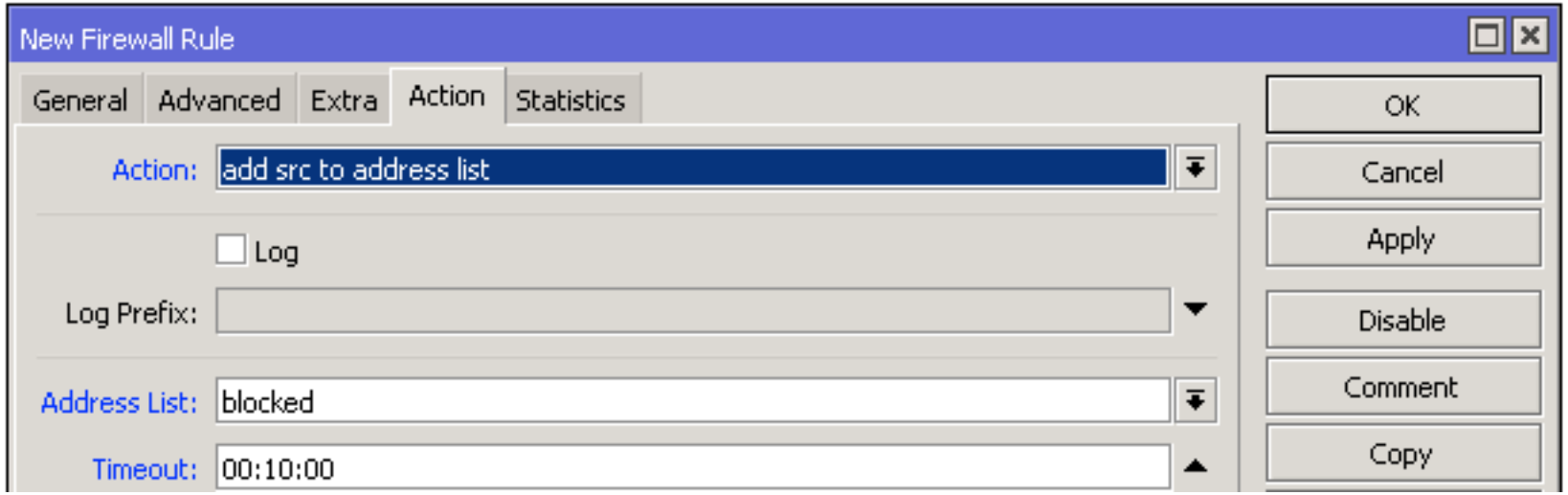


MTCNA módulo 7 Address List



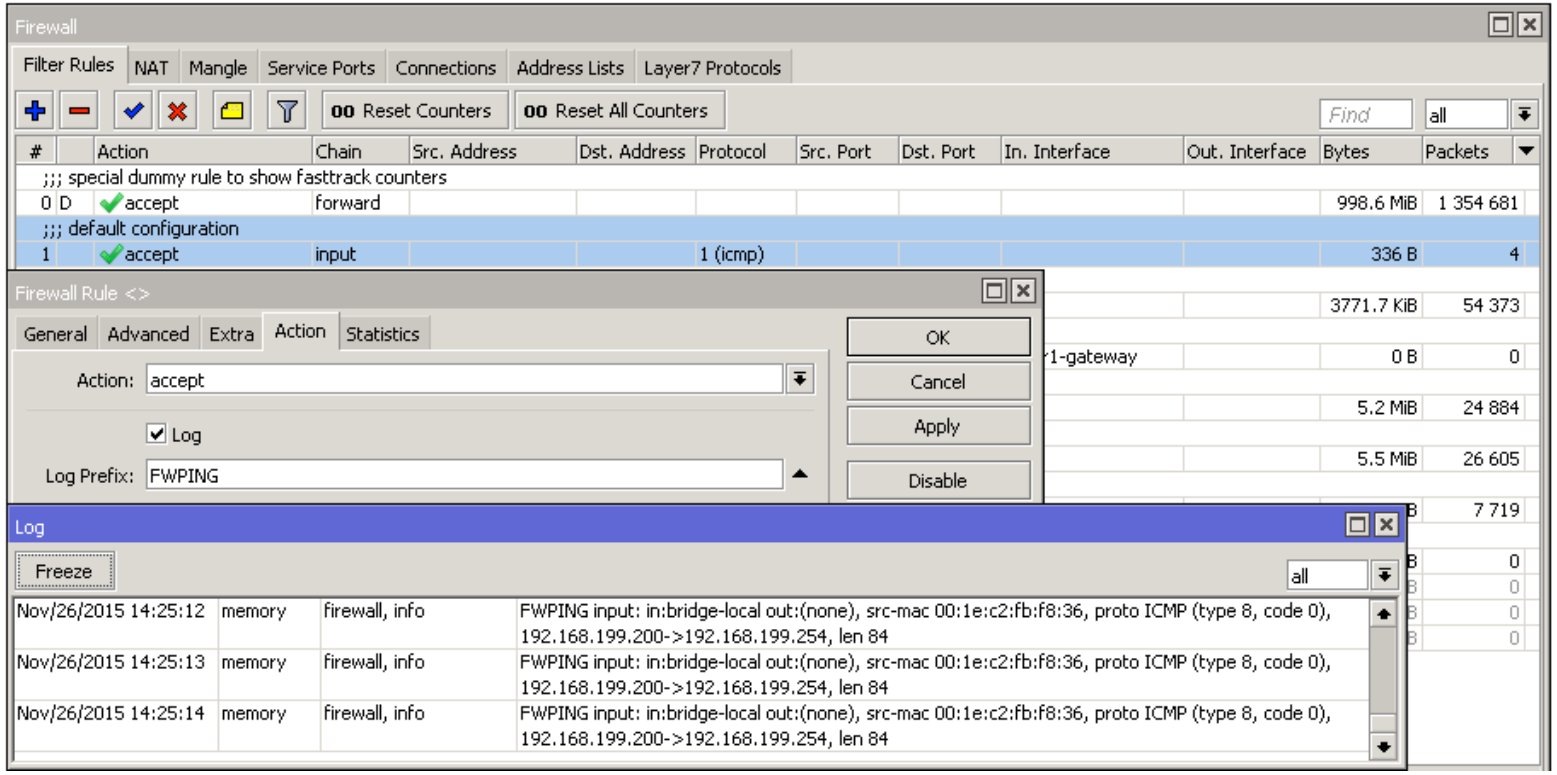
MTCNA módulo 7 Address List

- La acción de la regla del firewall se puede utilizar para agregar la dirección a la lista de direcciones
- De forma permanente, o durante un tiempo

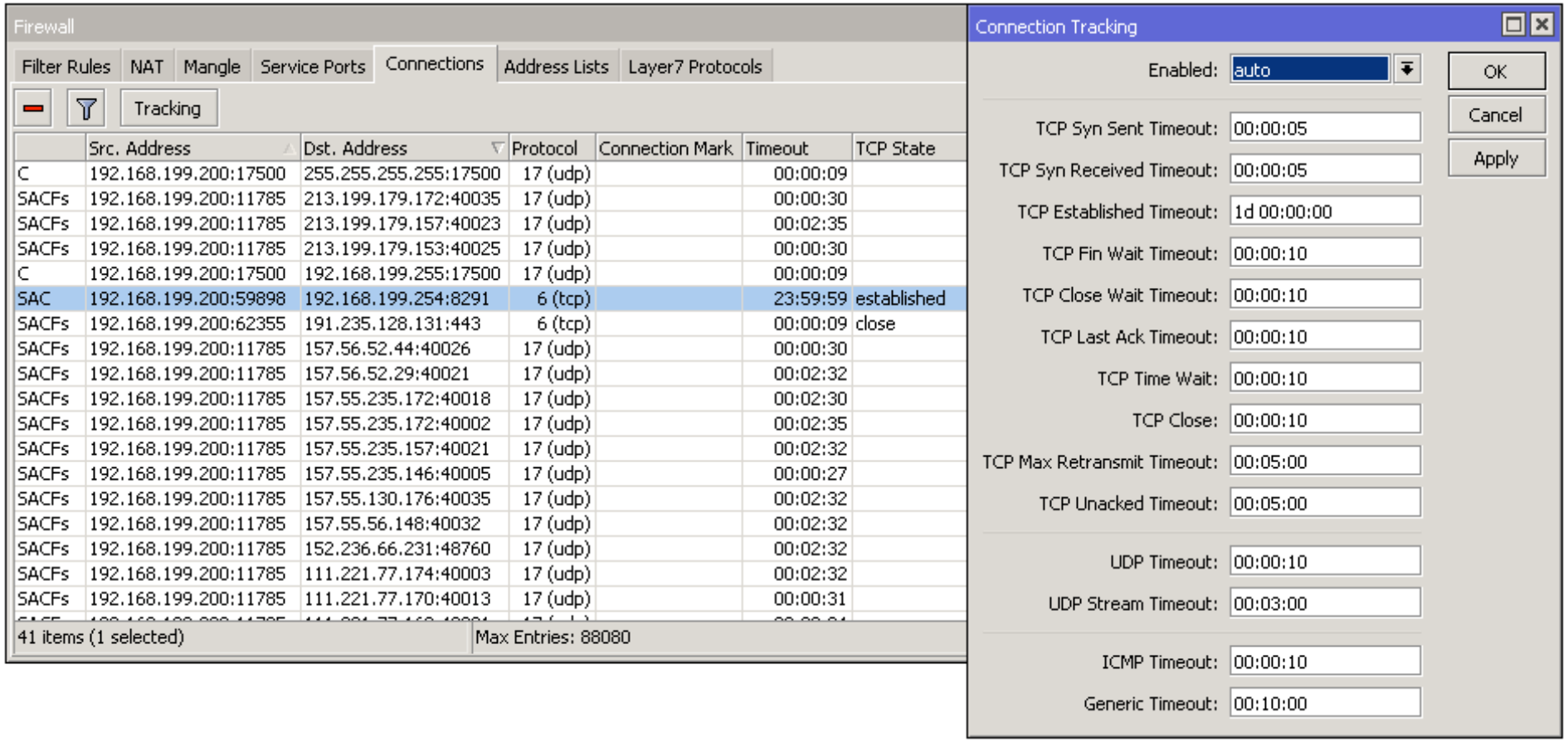


MTCNA módulo 7 Firewall Log

- Cada regla del firewall se puede registrar en el log cuando se cumpla la condición
- Se puede especificar un prefijo para, de esta forma, poder identificar el registro de una forma más clara



- Gestiona información acerca de todas las conexiones activas
- Debe estar activado si queremos usar el firewall


Firewall
Filter Rules
NAT
Mangle
Service Ports
Connections
Address Lists
Layer7 Protocols
Tracking
Src. Address
Dst. Address
Protocol
Connection Mark
Timeout
TCP State
C 192.168.199.200:17500 255.255.255.255:17500 17 (udp) 00:00:09
SACFs 192.168.199.200:11785 213.199.179.172:40035 17 (udp) 00:00:30
SACFs 192.168.199.200:11785 213.199.179.157:40023 17 (udp) 00:02:35
SACFs 192.168.199.200:11785 213.199.179.153:40025 17 (udp) 00:00:30
C 192.168.199.200:17500 192.168.199.255:17500 17 (udp) 00:00:09
SAC 192.168.199.200:59898 192.168.199.254:8291 6 (tcp) 23:59:59 established
SACFs 192.168.199.200:62355 191.235.128.131:443 6 (tcp) 00:00:09 close
SACFs 192.168.199.200:11785 157.56.52.44:40026 17 (udp) 00:00:30
SACFs 192.168.199.200:11785 157.56.52.29:40021 17 (udp) 00:02:32
SACFs 192.168.199.200:11785 157.55.235.172:40018 17 (udp) 00:02:30
SACFs 192.168.199.200:11785 157.55.235.172:40002 17 (udp) 00:02:35
SACFs 192.168.199.200:11785 157.55.235.157:40021 17 (udp) 00:02:32
SACFs 192.168.199.200:11785 157.55.235.146:40005 17 (udp) 00:00:27
SACFs 192.168.199.200:11785 157.55.130.176:40035 17 (udp) 00:02:32
SACFs 192.168.199.200:11785 157.55.56.148:40032 17 (udp) 00:02:32
SACFs 192.168.199.200:11785 152.236.66.231:48760 17 (udp) 00:02:32
SACFs 192.168.199.200:11785 111.221.77.174:40003 17 (udp) 00:02:32
SACFs 192.168.199.200:11785 111.221.77.170:40013 17 (udp) 00:00:31
41 items (1 selected)
Max Entries: 88080
Connection Tracking
Enabled: auto
OK
Cancel
Apply
TCP Syn Sent Timeout: 00:00:05
TCP Syn Received Timeout: 00:00:05
TCP Established Timeout: 1d 00:00:00
TCP Fin Wait Timeout: 00:00:10
TCP Close Wait Timeout: 00:00:10
TCP Last Ack Timeout: 00:00:10
TCP Time Wait: 00:00:10
TCP Close: 00:00:10
TCP Max Retransmit Timeout: 00:05:00
TCP Unacked Timeout: 00:05:00
UDP Timeout: 00:00:10
UDP Stream Timeout: 00:03:00
ICMP Timeout: 00:00:10
Generic Timeout: 00:10:00

- En el firewall una conexión puede tener los siguientes estados:
  - **New**: el paquete está iniciando una nueva conexión
  - **Established**: el paquete pertenece a una conexión ya establecida
  - **Related**: el paquete está iniciando una nueva conexión, pero tiene relación con una conexión conocida
  - **Invalid**: el paquete no pertenece a ninguna de las conexiones conocidas

- Es una buena práctica aceptar en las cadenas de input y forward:
  - Conexiónes establecidas
  - Conexiones relacionadas

- Drop conexiones inválidas en input y forward

- Es un método para acelerar el flujo de paquetes dentro del router
- Una conexión establecida o relacionada puede ser marcada para fasttrack
- Se salta el firewall, el connection tracking, las colas simples y otras funcionalidades ;)
- Actualmente unicamente está soportado para los protocolos TCP y UDP

Sin	Con
360Mbps	**890Mbps**
Uso Total de CPU 100%	Uso Total de CPU 86%
44% de CPU usada en el firewall	6% CPU usada en el firewall

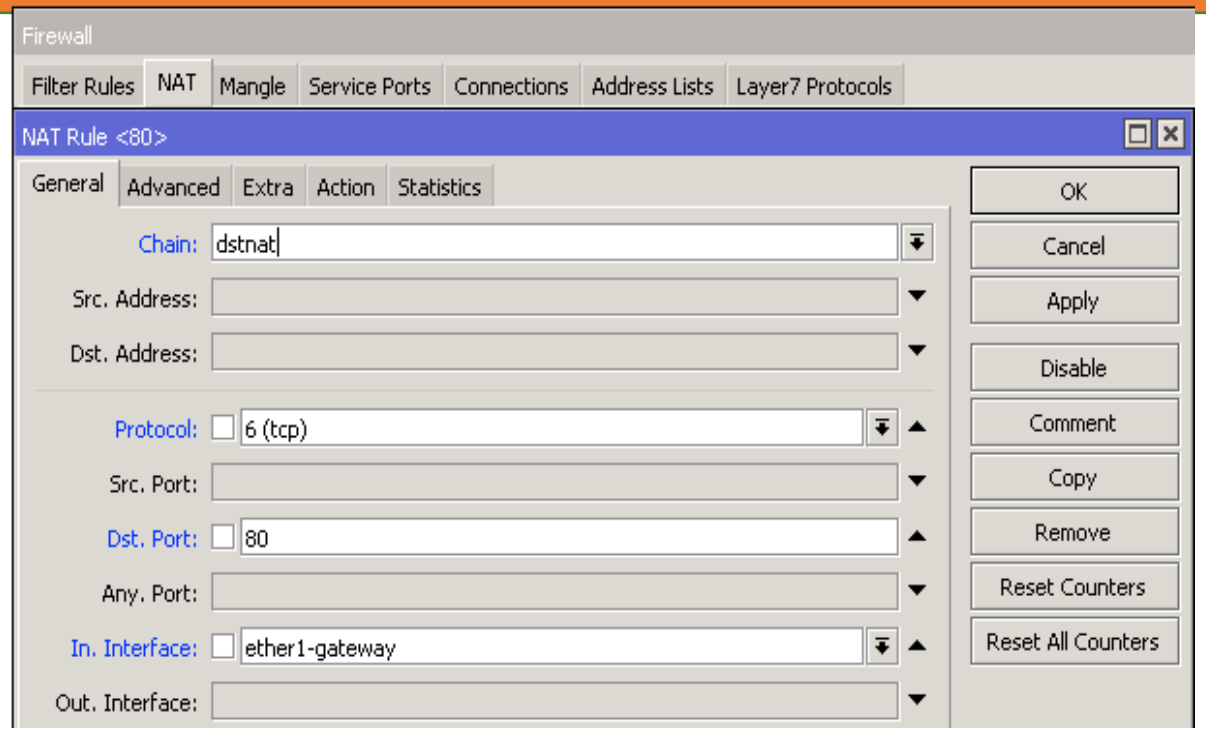
- Para más información consultar la página web
- http://wiki.mikrotik.com/wiki/Manual:Wiki/Fasttrack

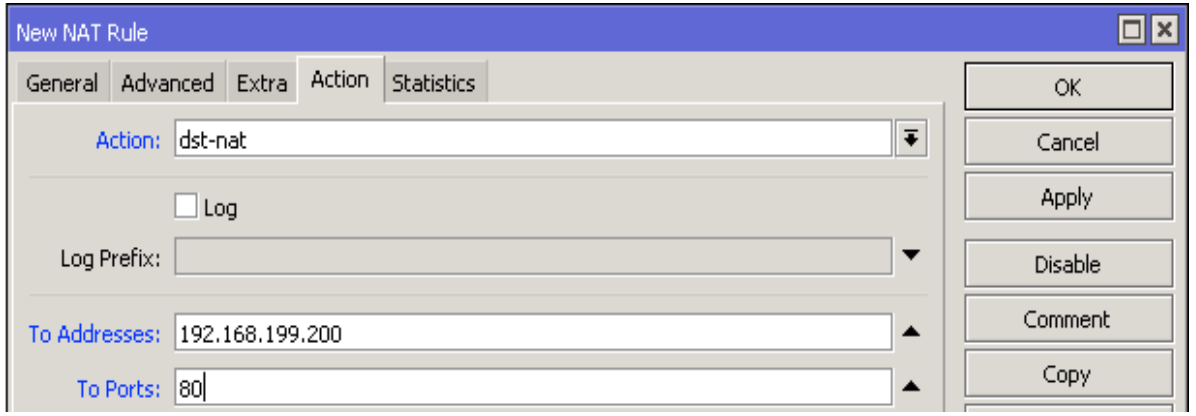
- Network Address Translation (NAT) es un método para modificar la dirección IP origen o destino de un paquete
- Hay dos tipos de NAT:
  - Source NAT
  - Destination NAT

- El NAT de origen (src-nat) es utilizado habitualmente para proporcionar acceso a una red externa desde una red que utiliza direcciones IP privadas
- El NAT de destino (dst-nat) es utilizado para poporcionar acceso desde una red externa a un recurso en nuestra red interna

- Las cadenas srcnat y dstnat del Firewall se utilizan para implementar la funcionalidad del NAT
- Al igual que en Filters, las reglas funcionan según el principio de Si …. entonces
- Son analizadas de forma secuencial hasta que se cumpla la condición de alguna de las reglas

MTCNA módulo 7 Ejemplo de NAT





MTCNA módulo 7 Redirect

- Es un caso especial de dstnat
- Esta acción redirige los paquetes al propio router
- Se puede utilizar para crear servicios proxy de forma transparente (por ejemplo DNS y HTTP)

- La acción src-nat de la cadena srcnat se utiliza para reescribir la dirección IP y/o el puerto

- Por ejemplo: dos empresas se han fusionado. Ambas empresas utilizan el mismo direccionamiento interno. Así pues, definirán un direccionamiento intermedio diferente, para usarlo como buffer. Ambas redes necesitarán aplicar reglas de src-nat y dst-nat

- Algunos protocolos requiren de los llamados nat helpers para poder funcionar correctamente en entornos que existe NAT