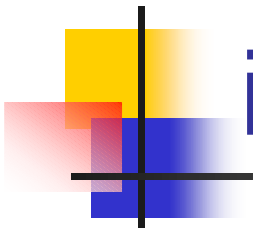
# ESLARED 2001

IPChain

# Las cadenas

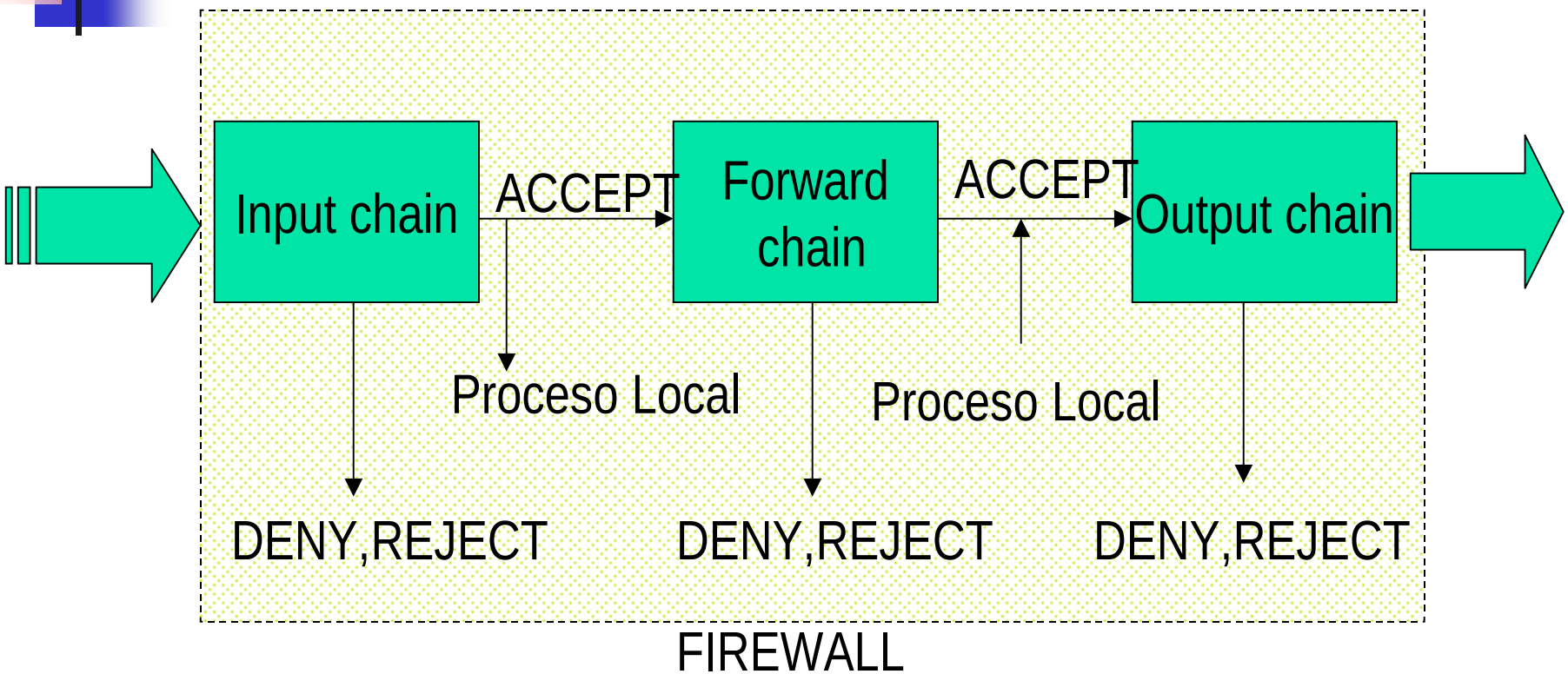
- Una cadena es un conjunto de condiciones a probar
  - Ej: Si el paquete viene de XXXX y va a DDDD no lo deje pasar.
- Si al final de una cadena no se encuentran coincidencias, se ejecuta la política de la cadena.



# ipchains

- Por omisión existen tres cadenas:input, forward,output.
- Cuando un paquete llega siempre pasa a la cadena input
- Si sobrevive al primer filtro una etapa de enrutamiento decide si es local o debe ser enviado a otro equipo
- En el último caso se pasa a la cadena forward
- Finalmente antes de que el paquete salga es pasado a la cadena output.

# El camino de un paquete



# Comandos para manipular las cadenas

- Crear una nueva cadena (-N).
- Borrar una cadena vacía (-X).
- Cambiar la política de una cadena. (-P).
- Listar las reglas de una cadena(-L).
- Eliminar reglas de una cadena(-F).
- Reiniciar los contadores de una cadena(-Z).

# Comandos para manipular las reglas de una cadena

- -A: Introducir una regla en una cadena
- -I: Insertar una regla en una cadena
- -R: Remplazar una regla en una cadena
- -D: Borrar una regla de una cadena

# El primer ejemplo

- ipchains -A input -s 127.0.0.1 -p icmp -j DENY

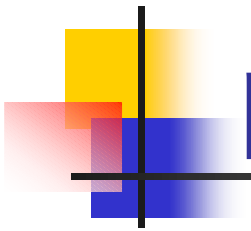
- El resultado:
  - ping -c 1 127.0.0.1
    PING 127.0.0.1 (127.0.0.1): 56 data bytes

    --- 127.0.0.1 ping statistics ---
    1 packets transmitted, 0 packets received, 100% packet loss

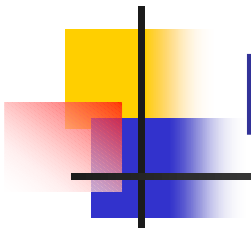
# Comandos dentro de una regla

- -s :dirección de origen.
  - Ej:www.mail.ula.ve, 150.130.130.1/24
- -d: direccción de destino
- -j:acción
- !:inversión
  - Ej: !120.120.120.1:Cualquier host excepto 120.120.120.1
- -p:protocolo
- Ej: ICMP,TCP,UDP

# Especificando el número de puerto



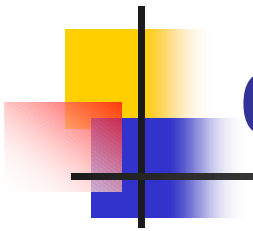
- Solo válido para conexiones TCP o UDP
  - Ej: -p TCP –s 0.0.0.0/0 23
  - -p TCP –d 150.185.128.0/18 ! www
  - -p TCP –d ! 150.185.128.0/18 !www
  - -p TCP –d 0.0.0.0/0 :1023
  - -p UDP –s 0.0.0.0/0 1023:



# Especificando la interfaz

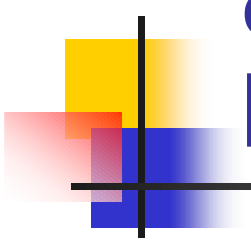
- -i : Especifica una interfaz sobre la que la regla es válida.
  - Ej: -i eth0
  - -i eth+

# Especificando el sentido de la conexión



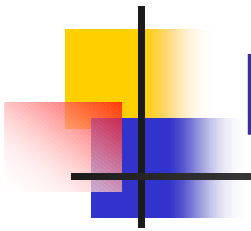
- Solo válido para conexiones TCP
- -Y : permite que sólo pasen paquetes de reconocimento pero no de solicitudes.
- Ej:
  - ipchains -A input  -p TCP -s 192.168.1.1 23 -y  -j DENY

# ¿qué hacer con el paquete? ... De nuevo....

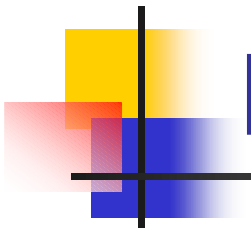


- -j: indica que hacer con el paquete
  - Opciones:
    - ACCEPT
    - DENY
    - REJECT
    - RETURN
    - REDIRECT

# Manejando Prioridades



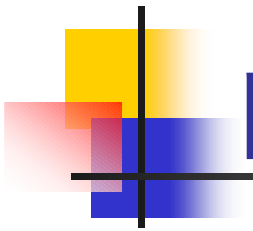
- Utiliza el bit de TOS de la cabecera de los paquetes IP
- Posee dos valores, el primero se utiliza para realizar un AND con el bit de TOS mientras que el segundo se utiliza para realizar un XOR
- Ej:
  - ipchains -A output -p tcp -d 0.0.0.0/0 ftp -t 0x01 0x10



# Ejemplo

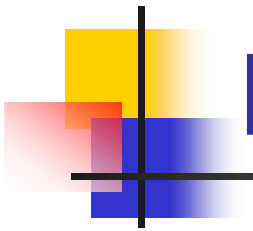
- No permitir tráfico de salida a la red 150.120.130.0/24
- No permitir tráfico de entrada via telnet de cualquier sitio a la red local : 140.130.120.0/24
- Permitir tráfico saliente (de la red local) al puerto 25 pero no entrante (a la red local)
- Permitir todo el resto del tráfico

# Ejemplo: Configurando las políticas de las cadenas



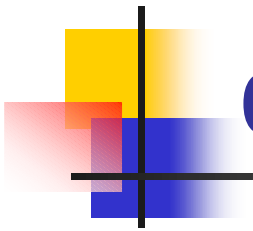
- ipchains -P input ACCEPT
- ipchains -P output ACCEPT
- ipchains -P forward ACCEPT

# Ejemplo: Solución



- ipchains –A output –d 150.120.130.0/24 –j DENY
- ipchains –A input –p TCP –s 0/0 –d 140.130.120.0/24 23 –j DENY
- ipchains –A input  -P TCP –s 0/0 –d 140.130.120.0/24 25 –j DENY

# Salvando y restableciendo las cadenas



- ipchains-save >/etc/mi_firewall
- ipchains-restore < /etc/mi_firewall