

Filters and Firewalls

Goal: More secure system.

Action: Block or filter network packets.

Goal: Private subnet.

Action: rewrite network packet headers.

Tool: iptables

Chains:

INPUT: actions taken on inbound packets

OUTPUT: actions taken on outbound packets

FORWARD: actions taken on packets that are forwarded

Rules in a chain are applied sequentially

Samples:

Block all inbound ssh connections.

```
iptables -A INPUT -p tcp --dport ssh -j REJECT
```

Allow ssh from campus, reject all other ssh.

```
iptables -A INPUT -p tcp --dport ssh \  
-s 134.139.0.0/16 -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport ssh -j REJECT
```

No web browsing.

```
iptables -A OUTPUT -p tcp --dport www -j REJECT
```

Iptables Basic Editing Options

-A, --append: appends the rule to the end of the chain

-L, --list: list all rules in a chain

`iptables -L OUTPUT` list the rules in the output chain

-D, --delete: delete a rule

`iptables -D INPUT 2`

delete rule 2 from the input chain

-I, --insert: specify the rule at which to insert

`iptables -I INPUT 2 -p tcp --dport ftp -j REJECT`

insert this rule at position 2

Other rules are moved down.

-R, --replace: replace a rule, delete then insert

-F, --flush: delete all rules from a chain

Tables

4 tables: `raw`, `nat`, `mangle`, `filter`.

Each table has separate chains; for example, the output chain for `filter` is distinct from the output chain for `nat`.

The default table is `filter`.

You can specify a chain in a command:

```
iptables -t filter -A OUTPUT --dport www -j REJECT
```

What the Tables Do

`nat` Network Address Translation: allows the firewall to hide a server, yet forward packets to it

`filter` allows packets to be rejected, dropped or accepted

`mangle` modifies the packet header fields, such as the quality of service field

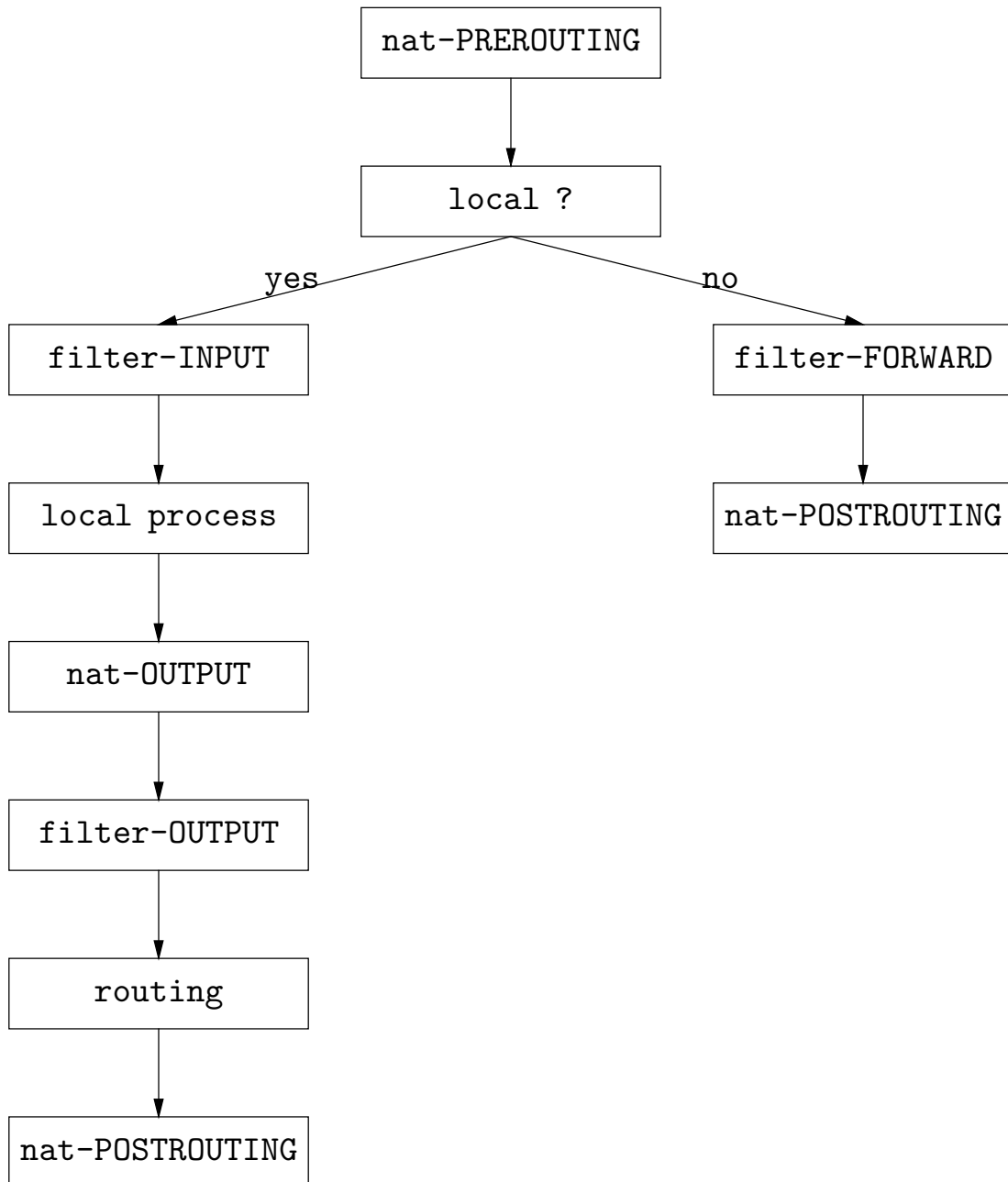
The `nat` table turns your gateway in to a firewall.

The `filter` table can be used to limit access to certain outside services (no web browsing).

Like `tcp wrappers` (`hosts.allow`/`hosts.deny`) it can limit in bound access to certain machines on the net.

`iptables` advantages: at the kernel level (blocks always), more robust against denial of service attacks.

Flow of Processing



Some Targets

ACCEPT: the packet is good

DROP: discard the packet

REJECT: discard the packet, inform the sender

LOG: send info to syslog

DNAT: rewrite the destination address

SNAT: rewrite the source address

MASQUERADE: rewrite source address (nat table only)

A Service Behind a Firewall

Suppose your web server is behind a firewall.

Detail:

firewall outside address 134.139.248.2

firewall outside interface eth0

firewall inside interface eth1

web server address 134.139.248.18

Tactic: block all inbound traffic except web requests.

```
iptables -A FORWARD -i eth0 -d 134.139.248.18 -p tcp \  
        --dports 80,443 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -d 134.139.248.18 -j REJECT
```

Notice inside traffic is not blocked.

So if you have a database on the web server you may access it from any machine behind the firewall.

A Service Behind a Firewall

Suppose your web server is on a private subnet.

Detail:

firewall outside address 134.139.248.2

firewall outside interface eth0

firewall inside interface eth1

web server address 192.168.1.18

On the outside,

all web traffic appears to be to or from the firewall.

Inbound web packets forwarded to the web server.

Outbound web packets appear to be from the firewall.

```
iptables -t nat -A PREROUTING -d 134.139.248.2 \  
-i eth0 -p tcp --dport 80 -j DNAT --to 192.168.1.18:80  
iptables -t nat -A PREROUTING -s 192.168.1.18 \  
-i eth1 -p tcp --sport 80 \  
-j SNAT --from 134.139.248.2:80
```

Outbound Packets Through a Firewall

Want to allow connections originating in the private subnet to go out.

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 \  
    -o eth0 -d 0/0 -j MASQUERADE  
iptables -A FORWARD -o eth0 -m state \  
    --state NEW,ESTABLISHED,RELATED -j ACCEPT  
iptables -A FORWARD -i eth0 -m state \  
    --state ESTABLISHED,RELATED -j ACCEPT
```

Masquerade always rewrites the source to the firewall IP address.

There is a state machine to track connection states.
Outbound stuff is allowed.

Inbound allowed only on established connections or connections getting established (related).