Character and GUI forwarding approaches

David Morgan

```
ipables -t filter -A OUTPUT -o eth1 -p tcp --sport 23 --dport 1024:65535
-s 192.168.4/24 --d 0.0.0.0/0 –j ACCEPT
```

- **Table for this rule**
  - **Rule action**
    - -A add rule to chain/list
    - -D delete rule from chain/list
    - -P default policy for chain/list
  - **Rule chain/list** (tables contain chains)
    - INPUT
    - OUTPUT
    - FORWARD

- **Packet qualifiers**
  - By interface and direction
  - protocol
  - source port number(s)
  - destination port number(s)
  - source address (range)
  - destination address (range)

- **Packet disposition**
  - ACCEPT
  - DROP
  - REJECT
  - SNAT
  - DNAT
Functions of **iptables** command

- firewall – drops undesired packets
- masquerading (NAT) – changes source address of outgoing packets
- port forwarding – changes dest address of incoming packets

---

**IP masquerading**

- Machines browse web w/o internet connection
- Gateway/translation service by linux machine
- Implemented as a function of firewalling
  ```bash
  iptables –t nat –A POSTROUTING –j SNAT –to <gateway addr>
  ```
- Clients designate linux machine as gateway
- Is a kernel component – must be compiled in
IP masquerading

- Also known as
  - Network Address Translation (NAT)
  - Internet Connection Sharing (ICS)

- Gateway must have “forwarding” turned on
  - echo 1 > /proc/sys/net/ipv4/ip_forward
Three kinds of forwarding

- packet-rule “regular” forwarding (by iptables)
- ssh port forwarding (by ssh)
- ssh X11 forwarding (by ssh)
packet-rule port forwarding

packet rule (firewall) forwarding:
- corresponds some port on “gateway” (e.g. 12345) to
- some port (e.g. 80) on a machine (eg, “server”) reachable thru “gateway”

Example: http://66...:12345 in client’s browser gets served from 192.168.1.111:80

ssh feature: port forwarding

ssh -L 3000:192.168.1.111:80  66...

ssh port forwarding:
- corresponds some port on “remote” (e.g. 3000) to
- some port (e.g. 80) on a machine (e.g. “server”) reachable from “gateway”

Example: http://127.0.0.1:3000 in client’s browser gets served from 192.168.1.111:80
ssh man page excerpt

“If [appropriately configured] the connection to the X11 display is automatically forwarded to the remote side in such a way that any X11 programs started from the shell (or command) will go through the encrypted channel, and the connection to the real X server will be made from the local machine.”
Accessing remote graphical I/O
-- with VNC or rdesktop

VNC
- RFB (Remote Frame Buffer) protocol
- by AT&T Laboratories, U.K. (defunct)
- server – ports 5900- for displays 0-
- plus http server – 100 ports lower
  - allows a browser as client
rdesktop

- RDP (Remote Desktop) Protocol
  - by Microsoft
- based on ITU T-120 family of protocols
  - “Data protocols for multimedia conferencing”
  - by International Telecommunications Union
- server - port 3389

lin desktop from win desktop (via vnc)

ran VNC viewer against 192.168.3.7:2 (display 2)
192.168.3.7:1 (display 1)
win desktop from lin desktop (via rdesktop)

VNC vis-à-vis X

- X Client/application
- X Server / service
- VNC Client
- VNC Server