Linux Networking: some miscellaneous essentials

The important details

- “Private” ip addresses
- Packet filter firewalling
- IP masquerading
- Packet sniffing
- IP aliasing
- Translation/resolution
  - IP address – to – ethernet address
  - domain name – to – IP address
IP addresses - private IPs

- Certain ranges are reserved
  - 10.x.x.x
  - 172.16.x.x  ...  172.31.x.x
  - 192.168.0.x  ...  192.168.255.x
- Commercial routers refuse to handle them
- For non-internet/intraLAN (private) purposes

IP Firewalling

- Filter for packets
  - set up in memory as series of if/then’s
  - by some user interface (command, dialog)
- iptables (or ipchains) implements in linux
- Block/permit packet passage by
  - Address of source and/or destination
  - Port number
  - Interface
  - Protocol
iptables -t filter -A OUTPUT -o eth1 -p tcp --sport 23 --dport 1024:65535 -s 192.168.4.0/24 -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
  - PREROUTING
  - OUTPUT
  - POSTROUTING
  - 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

---

**IP masquerading**

- Machines browse web w/o internet connection
- Gateway/translation service by linux machine
- Implemented as a function of firewalling
  - 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

© David Morgan 2003-2011
IP forwarding

Gateway replaces addresses and forwards

Inbound contact:

11.22.33.44 to 131.22.33.44

Outbound reply:

192.168.3.19 to 11.22.33.44

From:

11.22.33.44
12.168.3.19

To:

66.159.240.70
66.159.240.70

Effected by the iptables command

iptables $filter -A OUTPUT -o eth1 -p tcp --sport 23 --dport 1024:65535 -s 192.168.4.0/24 -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

© David Morgan 2003-2011
nat table: rules that alter packet

- Masquerading
  
  ```bash
  iptables -t nat -A POSTROUTING
  -o eth1 -s 10.0.0.0/8
  -j SNAT --to 216.83.185.193
  ```

- Pinholing (port forwarding)
  
  ```bash
  iptables -t nat -A PREROUTING
  -i eth1 -d 216.83.185.193/32 -p tcp --dport 5631
  -j DNAT --to 10.0.0.15
  ```

Parallel ways to do the same thing (port forward)

```bash
iptables -t nat -A PREROUTING
-i eth1 -d 216.83.185.193/32 -p tcp --dport 5631
-j DNAT --to 192.168.1.15:22
```
Gateway designation – Windows client

(linux equivalent: route add default gw 192.168.3.2)

Tcpdump - packet sniffing

- prints packet header info
- captures packets passing through an interface
- e.g., tcpdump –i eth1

© David Morgan 2003-2011
IP Aliasing

- multiple addresses on a single interface
- suffix :n onto interface name
  - ifconfig eth0:1 192.168.0.11
  - ifconfig eth0:2 192.168.0.12
  - ifconfig eth0:3 192.168.0.13
- gives eth0 a (presumed) 2\textsuperscript{nd}, 3\textsuperscript{rd}, 4\textsuperscript{th} address
- eth0 answers to all its addresses

Translation – domain name-to-IP
DNS
(domain name service)

- /etc/hosts to specify locally
  192.168.4.21 jimmy
  192.168.4.22 harry
  192.168.4.23 hertsel

- /etc/resolv.conf to use DNS
  nameserver 206.13.29.12
  nameserver 206.13.30.12