Linux Days 2002, Advanced Tutorial

Alain Knaff
alain.knaff@linux.lu

Summary

- 4. System tools
- 5. Configuration files and configuration tools
- 6. Server applications
- 7. Iptables (firewalling)

System tools

- 1. Lsmod
  - List currently loaded modules
  - "Which network card does this machine have?"

System tools

- 2. Netstat
  - List currently active network connections
  - "Who is connected to my server"
  - "Which network daemons are running"
  - Servers that are passively listening
  - Established connections

System tools

- 3. Lsof
  - Lists processes owning given "file" resource
  - "Which process currently hogs the CD drive?"
  - "Which process owns TCP port 25?"
  - "Which files or resources does process 1234 have open?"

```
frisbee:/root # lsof -i tcp:25
COMMAND   PID USER   FD   TYPE DEVICE SIZE NODE NAME
sendmail 1263 root    4u  IPv4   4360       TCP *:smtp (LISTEN)
```

System tools

- 4. Strace
  - Lists all system calls that a given program performs
  - Debugging
  - Finding unknown locations of configuration files

System tools

- 5. (T)ethereal
  - Lists network packets
  - Can show contents of network packets

Configuration files and tools

- Unix files
- /etc/sysconfig files
- Redhat configuration tool
- webmin

Configuration files: Unix files

- /etc/resolv.conf
  - Default domain and name servers

```
search lll.org.lu lll.lu ltnb.lu
nameserver 158.64.28.33
nameserver 158.64.28.10
```

- /etc/hosts
  - Locally defined host-to-ip mappings

```
158.64.28.33 tuxtux.lll.lu tuxtux
127.0.0.1 localhost
::1  ipv6-localhost ipv6-loopback
```

Configuration files: Unix files

- /etc/passwd : User information
  - Login name
  - User Id
  - Main Group Id
  - Full Name
  - Home Directory
  - Login Shell

```
alain:x:500:100:Alain Knaff:/home/aknaff:/usr/bin/zsh
```

- /etc/shadow : Users' passwords
  - Only readable by privileged processes
  - Passwords encrypted
- System users (applications)
- Real users (people)
- Users are usually created with the command `useradd`

Configuration files: Unix files

- /etc/fstab : File systems to mount
  - Device / Origin
  - Mountpoint
  - Filesystem type
  - Options
    - noauto
    - user
- Example:

```
/dev/md5        /       reiserfs        defaults 1 2
/dev/md9        /home   reiserfs        defaults 1 2
proc    /proc   proc    defaults 0 0
...
laptop:/nfs     /ld-2002        nfs     noauto,user
```

- Once this is defined, mount the partition with the following command: `mount /ld-2002`

Configuration files: sysconfig

- /etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=laptop.linuxdays
```

- To set it manually: `hostname laptop.linuxdays`

Configuration files: sysconfig

- /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=192.168.37.255
IPADDR=192.168.37.143
NETMASK=255.255.255.0
NETWORK=192.168.37.0
ONBOOT=yes
```

Configuration tools

- Redhat
- webmin: http://www.webmin.com/
- Demo

Server applications

- Standalone servers: apache, sendmail, ...
- Servers started by `xinetd`: ftpd, telnetd, ...
  - `/etc/services`
  - `/etc/xinetd.d`

Server applications

- Started by `service xyz start`
- Automatic activation using `chkconfig`
  - `chkconfig --list httpd`
  - `chkconfig --level 2345 httpd on`

Server applications

- General
- DNS (name server): bind9
- Apache
- Squid
- Ssh
- Ftp: wuftpd

Server applications: DNS (name service)

- Goal: translate names to IP addresses and vice-versa
- Standalone daemon
- Hierarchical system: delegation
- Master configuration in `/etc/named.conf`
- Configuration for individual domains in `/var/named/*`

Server applications: DNS > named.conf

- Global configuration options
  - `query-source address 158.64.28.33 port 53;`
  - `forwarders { 158.64.1.25; 158.64.1.14 };`
- Domain configuration

```
zone "lll.lu" IN {
        type master;
        file "lll.lu.zone";
        allow-transfer { 213.166.63.242; };
        notify yes;
};
```

- Slave domain (secondary name server):

```
zone "freeducation.org.lu" IN {
        type slave;
        file "slave/freeducation.org.lu";
        masters {  213.166.63.242; };
        transfer-source 158.64.28.33;
};
```

Server applications: DNS > zone file

- Defines individual name-to-IP translations
- Usually located in `/var/named`

Server applications: DNS > zone file

- SOA Record

```
@       1D      IN      SOA     ns.lll.org.lu.  hostmaster.lll.org.lu. (
                 2002092503      ; serial date + 2 digits
                 28800           ; refresh, seconds
                 7200            ; retry, seconds
                 604800          ; expire, seconds
                 86400 )         ; minimum, seconds
```

- NS Record: tells who is nameserver

```
        1D IN NS      ns.lll.lu.
        1D IN NS      sendar.prophecy.lu.     ; secondary nameserver
```

- A Record: name to IP translation

```
tuxtux     1D IN   A       158.64.28.33
```

- MX Record: who handles the mail for this domain?

```
        1D IN MX      10 mail.lll.lu. ; primary mail host
        1D IN MX      20 lll.lgl.lu.  ; backup mail host
```

- CNAME : an alias for a full name

```
www        1D IN   CNAME tuxtux
```

Server applications: DNS > rev. lookup

- In master file (named.conf)

```
zone "28.64.158.in-addr.arpa" IN {
        type master;
        file "158.64.28.zone";
        allow-update { none; };
};
```

- In zone file

```
33      IN PTR   tuxtux.lll.lu.
```

Server applications: Apache

- Serves Web pages
- Standalone daemon
- Configured using `/etc/httpd/conf/httpd.conf` and `.htaccess`
  - `ServerName`
  - `DocumentRoot`
  - `DirectoryIndex`
  - `NameVirtualHost`
  - `<VirtualHost>`
  - `Include`
  - `Options +ExecCGI`
- Documentation at `http://httpd.apache.org/`

Server application: Squid

- Caches Web requests
- Standalone daemon

Server application: Squid > configuration

- Configured via `/etc/squid/squid.conf`:
  - `acl name criterion parameters`
  - `http_access allow|deny [!]aclname`
  - `deny_info FILE aclname`
  - `authenticate_program /usr/lib/squid/ncsa_auth /etc/shadow`
  - Order is important
- Example:
  - Allow all access from inside
  - For outside access, ask for password

```
acl localNets src 10.0.0.0/255.0.0.0 127.0.0.1
acl password proyx_auth REQUIRED
http_access allow localNets
http_access allow password
http_access deny all
```

- Documentation at `http://www.squid-cache.org/`

Server application: Squid > logfile

- Log files can be found in `/var/log/squid/access.log`

- Example:

```
1033291882.682    132 127.0.0.1 TCP_MISS/200 14634 GET http://www.pt.lu/ -
DIRECT/194.154.192.107 text/html


1033377731.635    130 192.168.37.143 TCP_MISS/200 14626 GET
http://www.pt.lu/ aknaff DIRECT/194.154.192.107 text/html
```

Server applications: SSH

- Encrypted remote login to other sites
- Possibility to tunnel X protocol: `ssh -X somehost`
- Possibility to tunnel aribitrary ports (protection against snooping):
  - `ssh -L 5900:localhost:5900 somehost`
  - `ssh -R 6001:localhost:6000 somehost`
- Default configuration suitable for most uses
- Optional key-based authentication

Server applications: Wu.ftpd

- Access to downloadable files
- Started by `xinetd`
- Not encrypted
- Possibility to have "anonymous" users
- `/etc/ftpusers`
- Advanced configuration in `/etc/ftpaccess`
  - guest users
  - classes (limits number of logins)
  - upload directories
  - ...

Server applications: Mail

- Sendmail
  - sends mail to other machines
  - receives mail from other machines
- Imap, Pop
  - allows users to browse their mailbox

Server applications: Mail > Sendmail

- Standalone daemon
- /etc/mail directory

Server applications: Mail > Sendmail (1)

- aliases
  - nice names for users (incoming)
- virtusertable
  - same as aliases, but for managing several mail domains
- genericstable
  - nice names for users (outgoing)
- mailertable
  - "manually" configure paths to certain destinations

Server applications: Mail > Sendmail (2)

- local-host-names (sendmail.cw)
  - Defines which domains are local mailboxes
- access
  - Spam control
- relay-domains
  - Defines who may use this mailer
  - Destination or origin must be local (or both)
- sendmail.mc (linux.mc)
  - Master configuration files

- After changing one of the files, you need to type `make`

Server applications: Mail > Sendmail > sendmail.mc

- MASQUERADE_AS: outgoing domain name
- FEATURE(‘dnsbl’, ..., ...): spamcontrol
- GENERICS_DOMAIN(‘mailhost.test.lu’)

Server applications: Mail > Sendmail

- Documentation at http://www.sendmail.org

Server applications: Mail > Imap

- Started by `xinetd`
- Needs almost no configuration
- For encrypted operation, key File in `/usr/share/ssl/certs/imapd.pem`
- Access by mail client such as `kmail` or `mozilla`

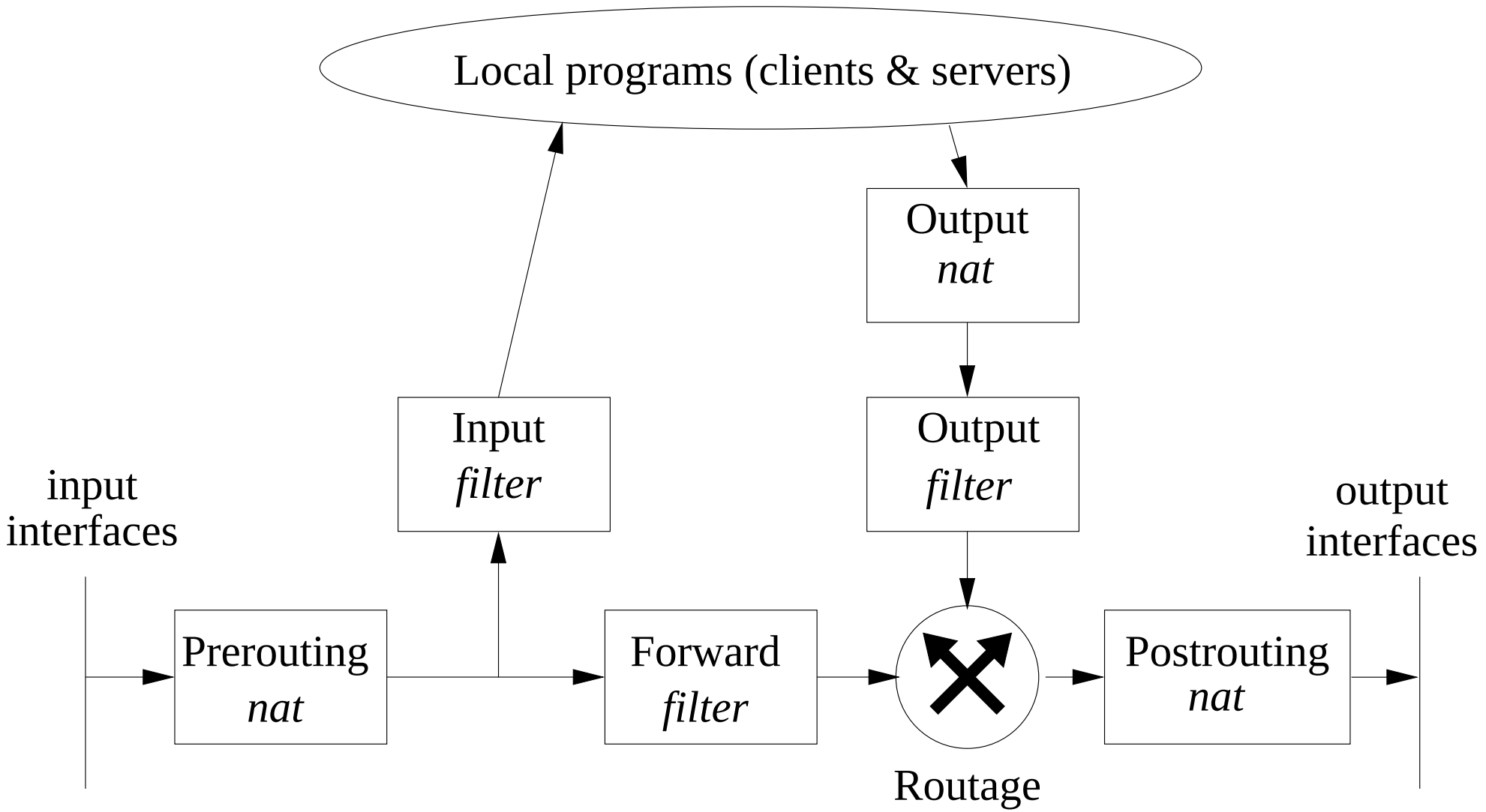
Ip Tables

- *Packet filtering* firewall
- Protects the internal network
- Multiplexes many machines behind a same public IP address
  - Allows to access the Internet from several workstations
  - Marshalls incoming requests towards several servers

Ip Tables, Concepts

- Tables: `filter` (default), `nat`, `mangle`
- Chains: `INPUT`, `OUTPUT`, `FORWARD`, `PREROUTING`, `POSTROUTING`
- Rules

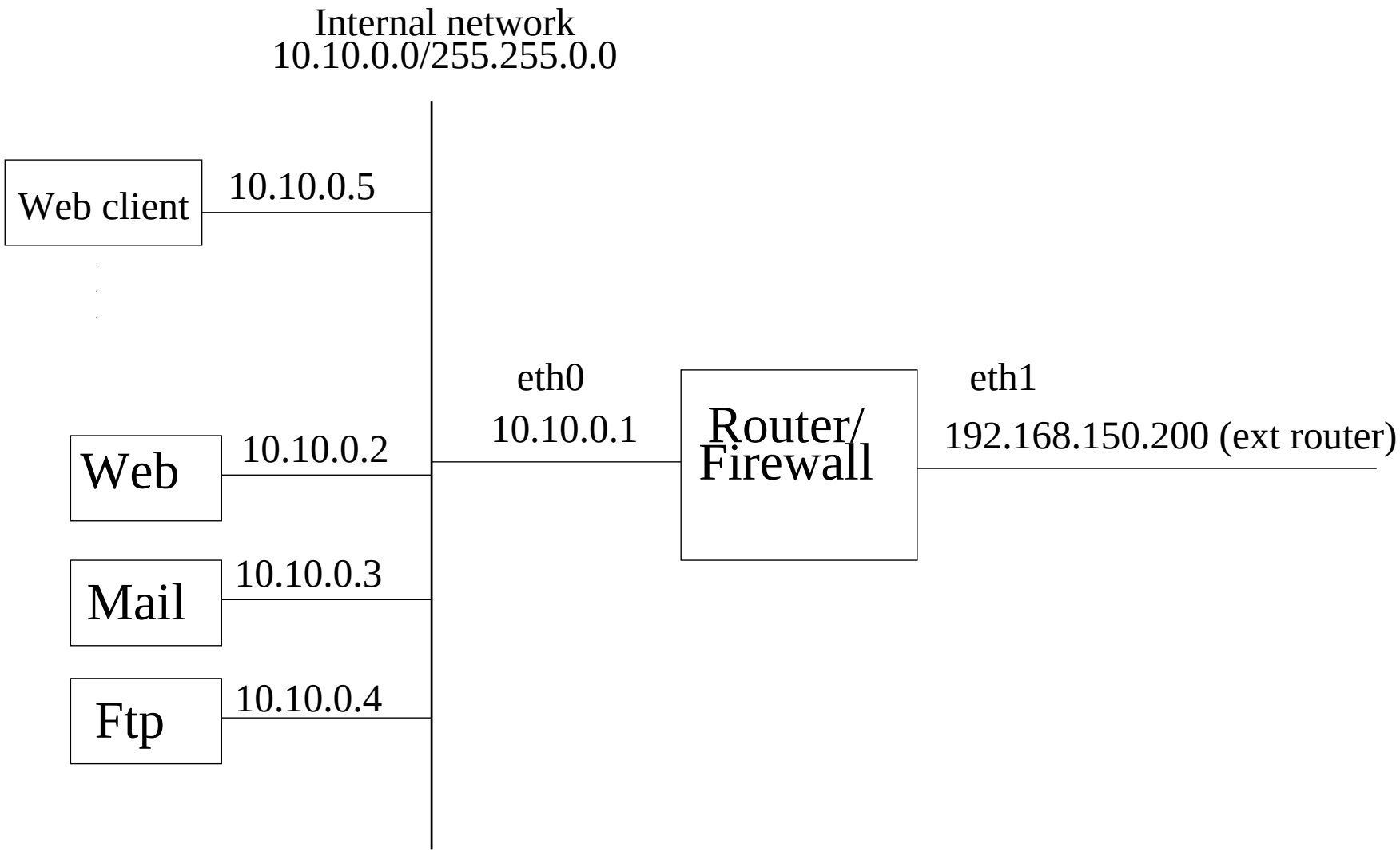
Ip Tables, Packet flow



Ip Tables, Command syntax

- Syntax: `iptables [table] chainspec condition action`
- Actions:
  - -A *chain* append new rule at the end
  - -I *chain* inserts new rule at the top
  - -D *chain* remove the rule
  - -F *chain* removes all rules
- Examples:
  - ```
    iptables  -t nat -A OUTPUT -d 10.10.1.1 \
     -j DNAT --to-destination 1.2.3.4
    ```
  - `iptables -A FORWARD -d 10.10.1.1 -j DROP`
    ```

Ip Tables, Network Diagram



Ip Tables, Protection of the internal network

- Forbid access to outside (eth1)
- Allow ssh access (administrative)
- Allow return channel

```
iptables -A INPUT -i eth1 -j DROP
iptables -I INPUT -p tcp --dport 22 -j ACCEPT
iptables -I INPUT -m state --state ESTABLISHED -j ACCEPT
```

Ip Tables: Outgoing Nat (Web Access)

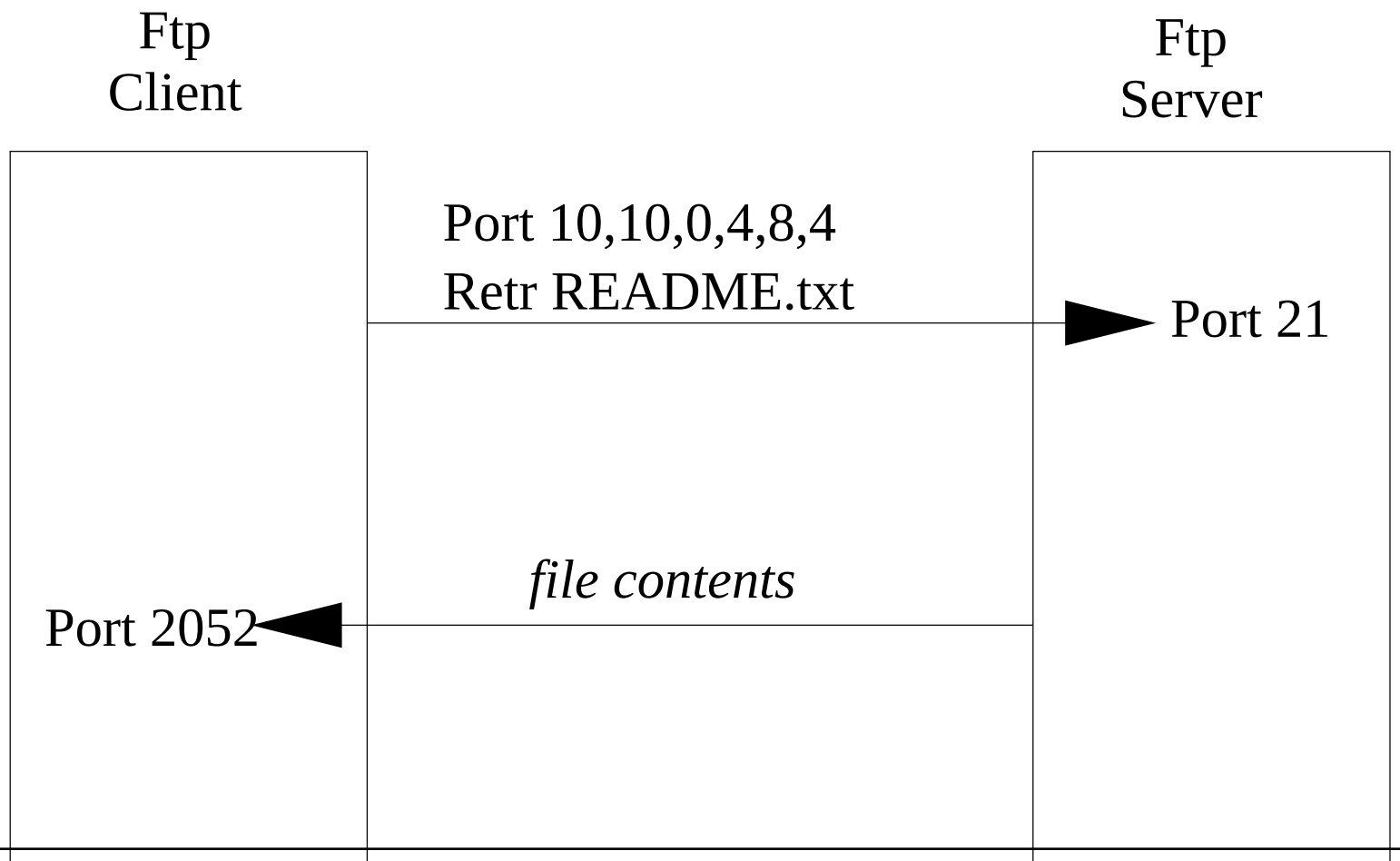
- Internal machines will use the router's address

```
iptables -t nat -A POSTROUTING -s 10.10.0.0/16 \
 -j SNAT ---to-source 158.64.150.200
```

- If the router has a variable IP address (dialup), use the following option: `-j MASQ` instead of `-j DNAT`

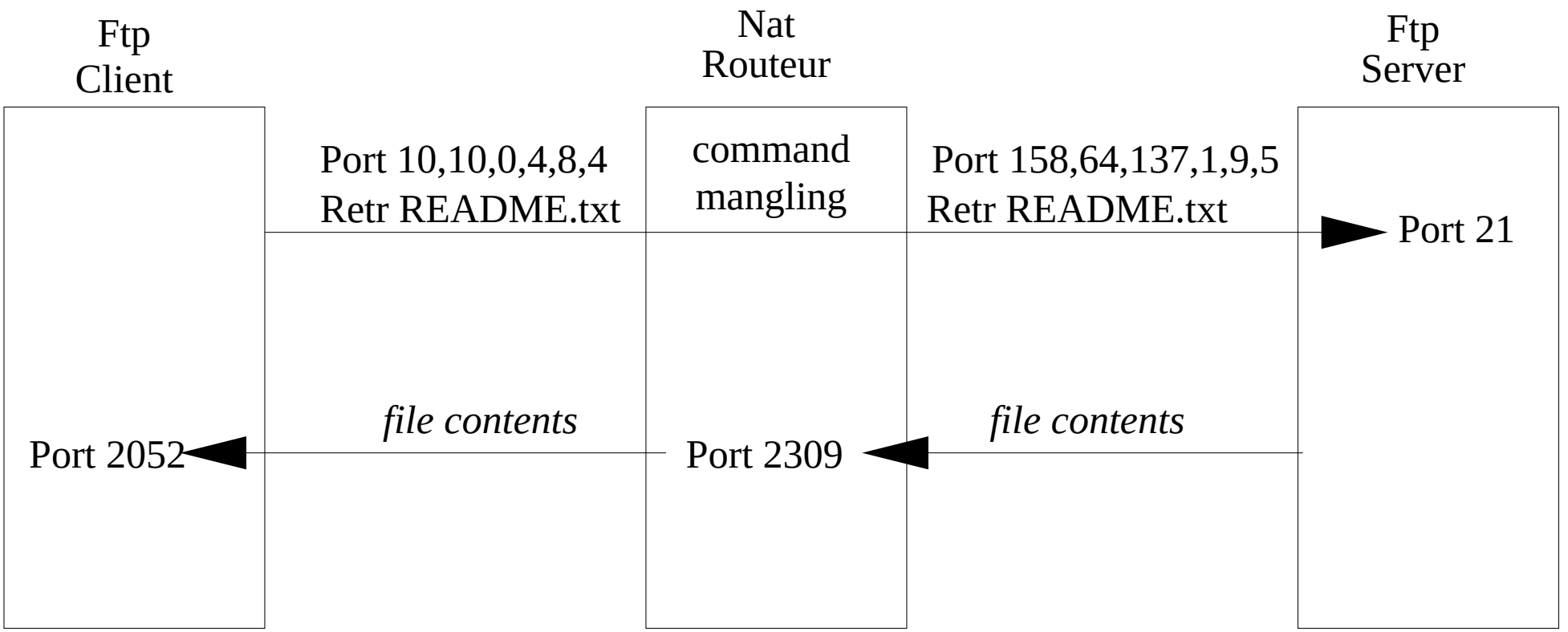
Ip Tables: FTP transfer, without NAT

- In passive mode, the server calls back the client on a client-specified port



Ip Tables: FTP transfer, with NAT

- The NAT router replaces the callback address with the control connection



Ip Tables: Activating Ftp NAT

```
modprobe ip_nat_ftp
modprobe ip_conntrack_ftp
```

Ip Tables: Incoming NAT

- Switch incoming requests towards the correct machines

```
iptables -t nat -I PREROUTING \
 -p tcp -d 158.64.150.200 --dport 80 \
 -j DNAT --to-destination 10.10.0.2
```

- Allowing access

```
iptables -I FORWARD \
 -p tcp -d 10.10.0.2 --dport 80 \
 -j ACCEPT
```

Ip Tables: Transparent proxy, NAT configuration

- The NAT router intercepts all connections meant for external Web servers and pipes them through a local Squid (proxy) process

```
iptables -t nat -I PREROUTING \
 -p tcp --dport 80 -i eth0 \
 -j DNAT --to-destination 10.10.0.1:3128
```

Ip Tables: Transparent proxy, Squid configuration

- The squid proxy must be prepared to access these transparent proxy requests

```
httpd_accel_uses_host_header on
httpd_accel_with_proxy on
httpd_accel_host virtual
```

Ip Tables: URL of this presentation

- This presentation will be placed at the following address

`http://www.lll.lu/ld2002adv/ld2002.pdf`

- A sample script can be found here

`http://www.lll.lu/firewall-presentation/fw.sh`

- There are many "graphical" tools and ad-hoc distributions for managing a firewall. Exemple: Ipcop

`http://www.ipcop.org/`