Case Study # 1

A Simple Firewall Audit

With Data Inspired by Real Life

A simple firewall audit

- Firewall architecture
- Audit procedure
- Typical results
- Typical problems

overview.fig

Firewall audit aspects

- Policies (what they actually wanted)
- Functional (what hoped they would get)
- Implementation (what they actually got)
- Organizational (who gets blamed for what)
- Procedural (how they’re supposed to run it)

audit-aspects.fig

Firewall functions

Services

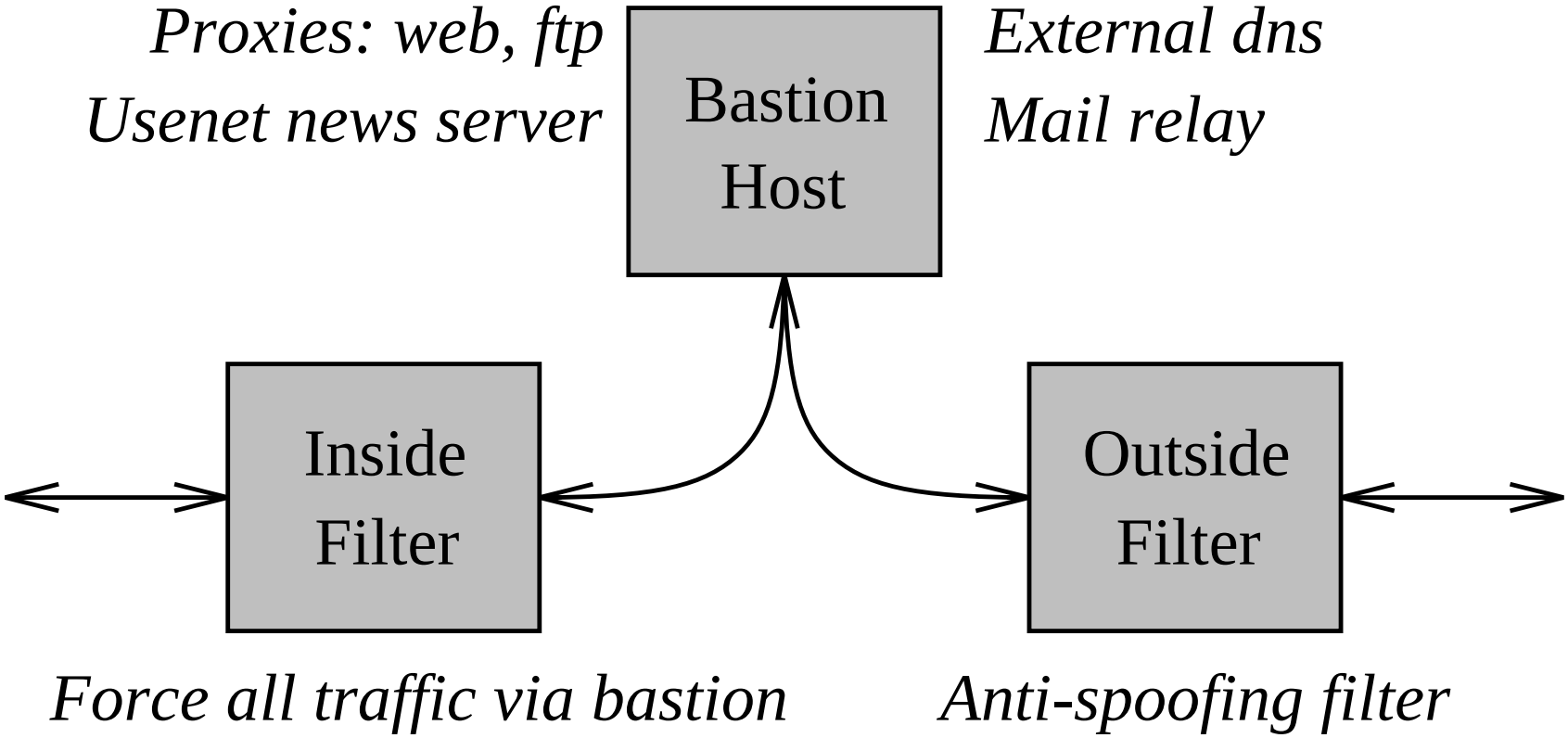
- From outside: Usenet news feed
- To outside: email, name service
- To inside: email, name service, ftp, web, news

Logging

- Accounting
- Audit trail

functions.fig

Firewall architecture



architecture.fig

Firewall ‘de facto’ policy

- Controlled access via specific services only
  - no random applications across firewall
- Internal network is invisible from outside
  - no disclosure of network structure etc.
- No inbound logins across firewall
  - no disclosure of internal data etc.

What does the system do?

- System startup
- Resident processes
- Configuration files
- Network services
- Users (admin/other)

what.fig

How does the system work?

- How are services protected?
- Dependencies on other services?
- Appropriate service architecture?
- Does service work adequately?
- Does protection work?
- Does service log adequately?

how.fig

System snapshot - startup procedure

Look for "window of opportunity" during system startup:

- When is networking turned on?
- When is routing turned on?
- When is security turned on?
- What if security turn-on fails?

startup.fig

System snapshot - accounts

Who has access to the system and by what method?

- Administrative accounts
- Other accounts (not on firewall!)
- Network logins (not on firewall!)
- Passwords (token, sealed envelope, etc.)

users.fig

System snapshot - processes (ps)

```
  PID TTY S    TIME COMMAND
    0 ??  R <  2:25 [kernel idle]
    1 ??  I    0:40 /sbin/init -a
   26 ??  S   10:05 /sbin/update
  130 ??  S    0:05 /usr/sbin/syslogd
  216 ??  I    0:25 /sbin/named -b /etc/namedb/named.boot
  283 ??  I    0:13 -accepting connections (sendmail)
  302 ??  S <  0:13 /usr/sbin/xntpd -c /etc/ntp.conf
  323 ??  I    0:00 /usr/sbin/inetd
  326 ??  I    2:13 /usr/bin/httpd
  331 ??  I    0:14 /usr/sbin/cron
  374 ??  I    0:14 /newslib/etc/innd -p4 -r -i0
  394 ??  I   14:03 sh /newslib/bin/innwatch
11841 ??  I    0:00 sleep 600
12060 ??  I    0:00 -154.8 (ftp-proxy)
```

proc-example.fig

System snapshot - processes

Collect critical information about processes on the system:

- Purpose
- Privilege level
- Configuration files
- Logfiles and/or accounting

proc-purpose.fig

System snapshot - recursion

Repeat procedure for processes run from other processes:

- init (runs startup, shutdown, logins)
- cron (runs administrative tasks)
- inetd (runs proxy services)
- innd (runs nnrpd servers)
- sendmail (runs none hopefully :-)

proc-recurse.fig

System snapshot - network services (lsof)

```
syslogd     130     root    4u  inet UDP *:syslog
named       216     root    4u  inet TCP *:domain
named       216     root    5u  inet UDP bastion:domain
named       216     root    6u  inet UDP localhost:domain
named       216     root    7u  inet UDP *:domain
sendmail    283     root    5u  inet TCP *:smtp
xntpd       302     root    4u  inet UDP *:ntp
xntpd       302     root    5u  inet UDP bastion:ntp
xntpd       302     root    6u  inet UDP localhost:ntp
inetd       323     root    4u  inet TCP *:ftp-proxy
httpd       326     root    5u  inet TCP *:http-proxy
innd        374     news    4u  inet TCP *:nntp
ftpxd     12060   ftpxd     0u  inet TCP bastion:ftpx->...
ftpxd     12060   ftpxd     0u  inet TCP bastion:ftpx->...
ftpxd     12060   ftpxd     0u  inet TCP bastion:ftpx->...
```

net-example.fig

System snapshot - network services

Collect critical information about network services:

- Services used from the network
- Services offered to the network
- Protection mechanisms
  - Access control
  - Reduced privilege
  - Chroot jail
- Logging method

net-purpose.fig

System snapshot - network

What does system know about:

- Other hosts on the network (chatty proxies!)
  - /etc/hosts, /etc/resolv.conf
  - /etc/nsswitch.conf, /etc/svcorder
- Other IP networks (routing)
  - default routes (especially on inside network!)
  - netstat -nr
- Other networking protocols (not on firewall!)
  - decnet, x25, ...

Unprotected service - syslogd

Purpose:

- Collects (forwards) logging information

Problem:

- Will accept data from any host on the network
- Origin is trivial to spoof

Recommendation:

- Configure packet filter to block syslog

syslog.fig

Inappropriate design and privileges - httpd

CERN http server in proxy mode:

- Large and complex program
- Erroneously configured to run as root

Recommendations:

- Run dedicated proxy server
- Run at reduced privilege level

Incomplete proxy access controls

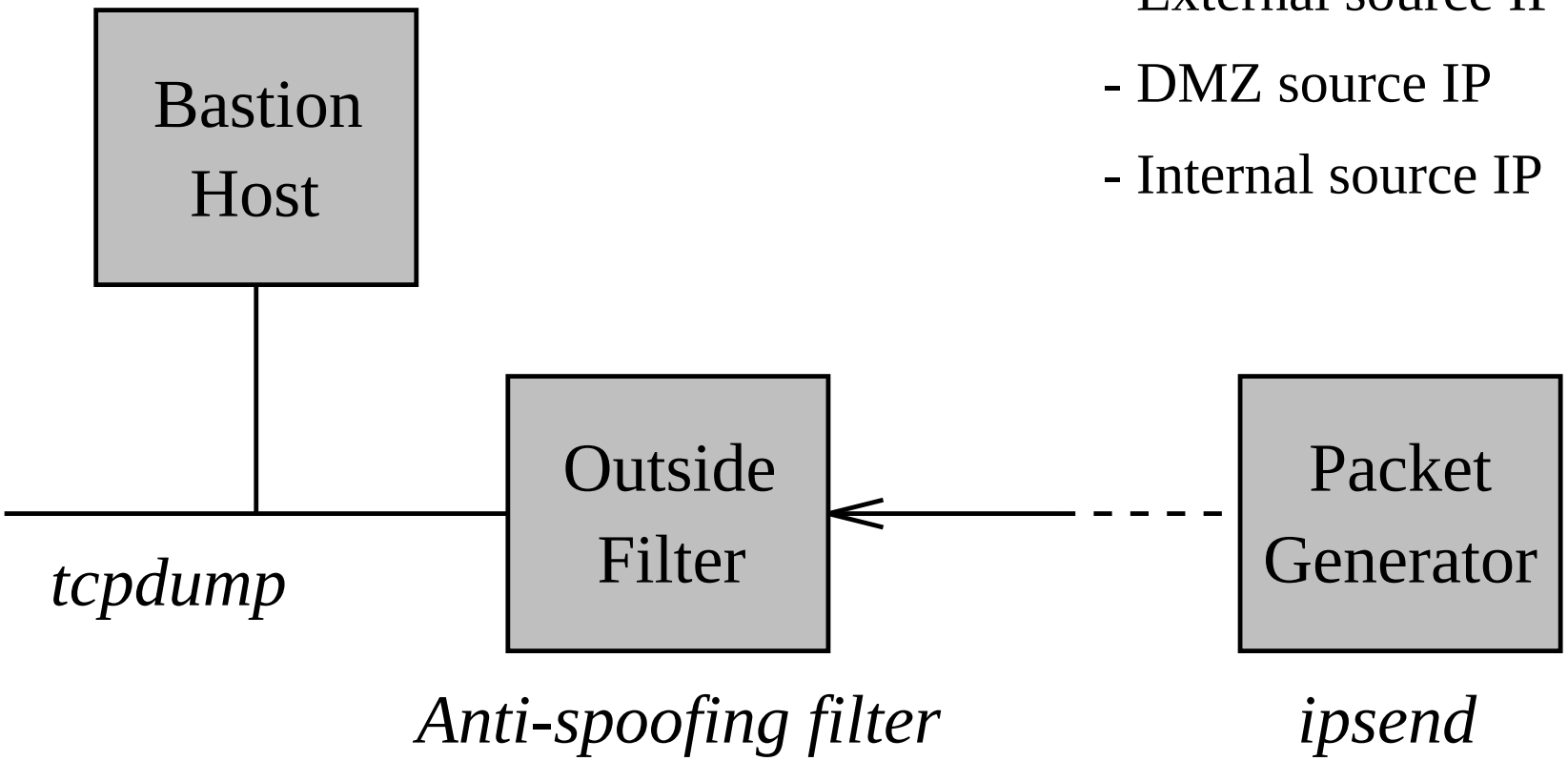
Connect from:	Outside network (hole!)
	Inside network
Connect to:	Outside network
	Inside network (hole!)
	Bastion network (hole!)
	Localhost interface (hole!)
Destination as:	Host name
	Host address (hole!)
	Host address of unnamed host (hole!)

proxy-test.fig

Anti-spoofing filter test

Generate packets with:

- External source IP
- DMZ source IP
- Internal source IP



spoof-test.fig

Technical problems

- Unprotected services
  - syslogd
- Servers running at too high privilege level
  - proxy servers as root
- Loopholes in proxy access rules
- Programs too complex for security
  - INN usenet news server
  - CERN http (proxy) server
- Achilles heel: sendmail

Procedural problems

Missing / incomplete / inadequate procedures for:

- Applying security patches
  - sendmail bug of the month
- Security monitoring
  - off-line logfile analysis
- Incident handling
  - pull the plug

Organizational/HR problems

Poor introduction of new technology:

- Lack of administrative personnel training
  - the prototypical pc/mainframe shop
- Lack of administrative personnel resources
  - intruders work only during office hours
- Lack of user training and support
  - toy for the techies