Case Study # 3

The AT&T firewall

A system in transition

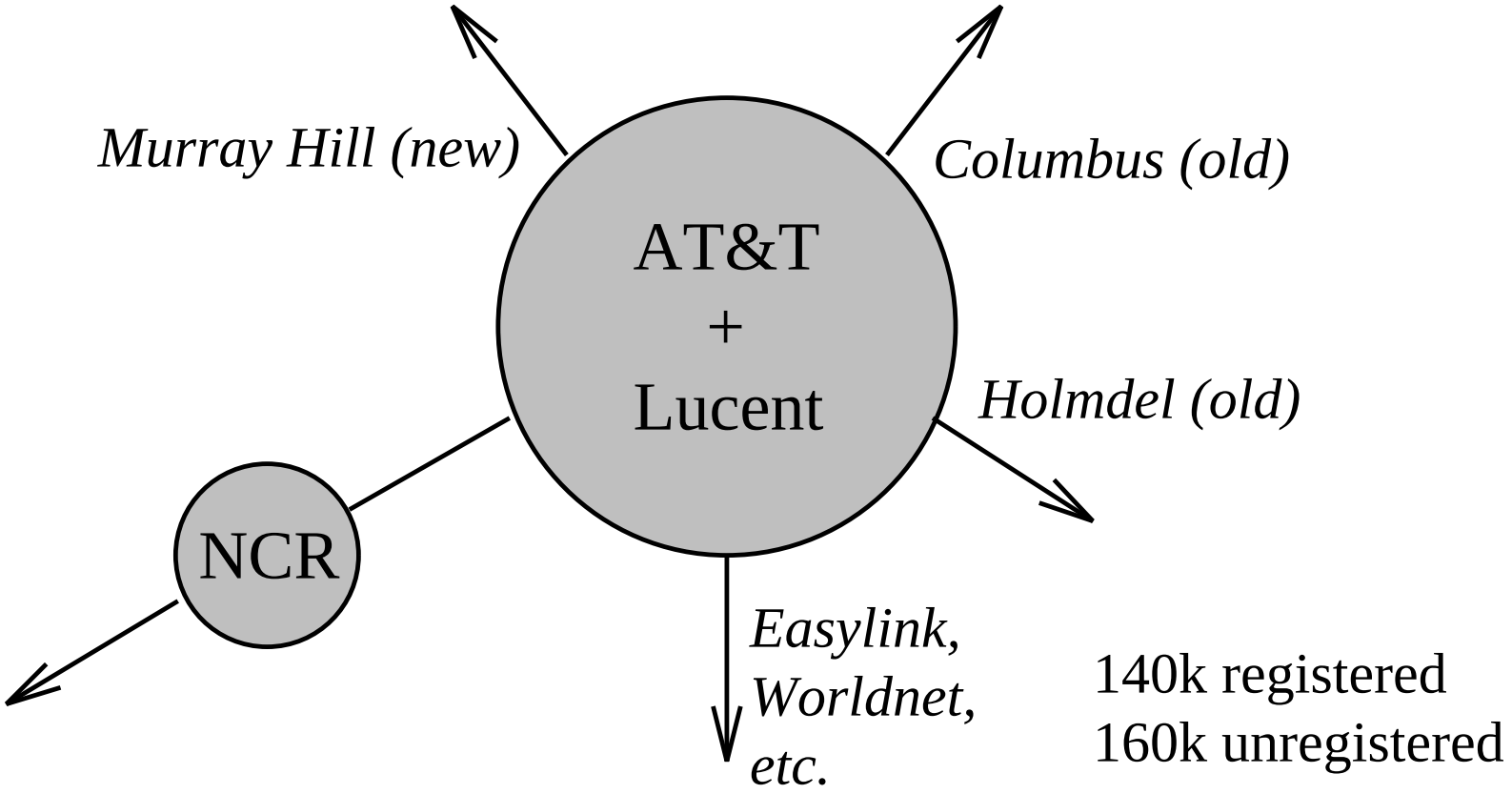
title.fig

Case study - the AT&T firewall

- Current and future architecture
- Some interesting new tools
- How things really are done

overview.fig

300k+ hosts, 2% of internet address space



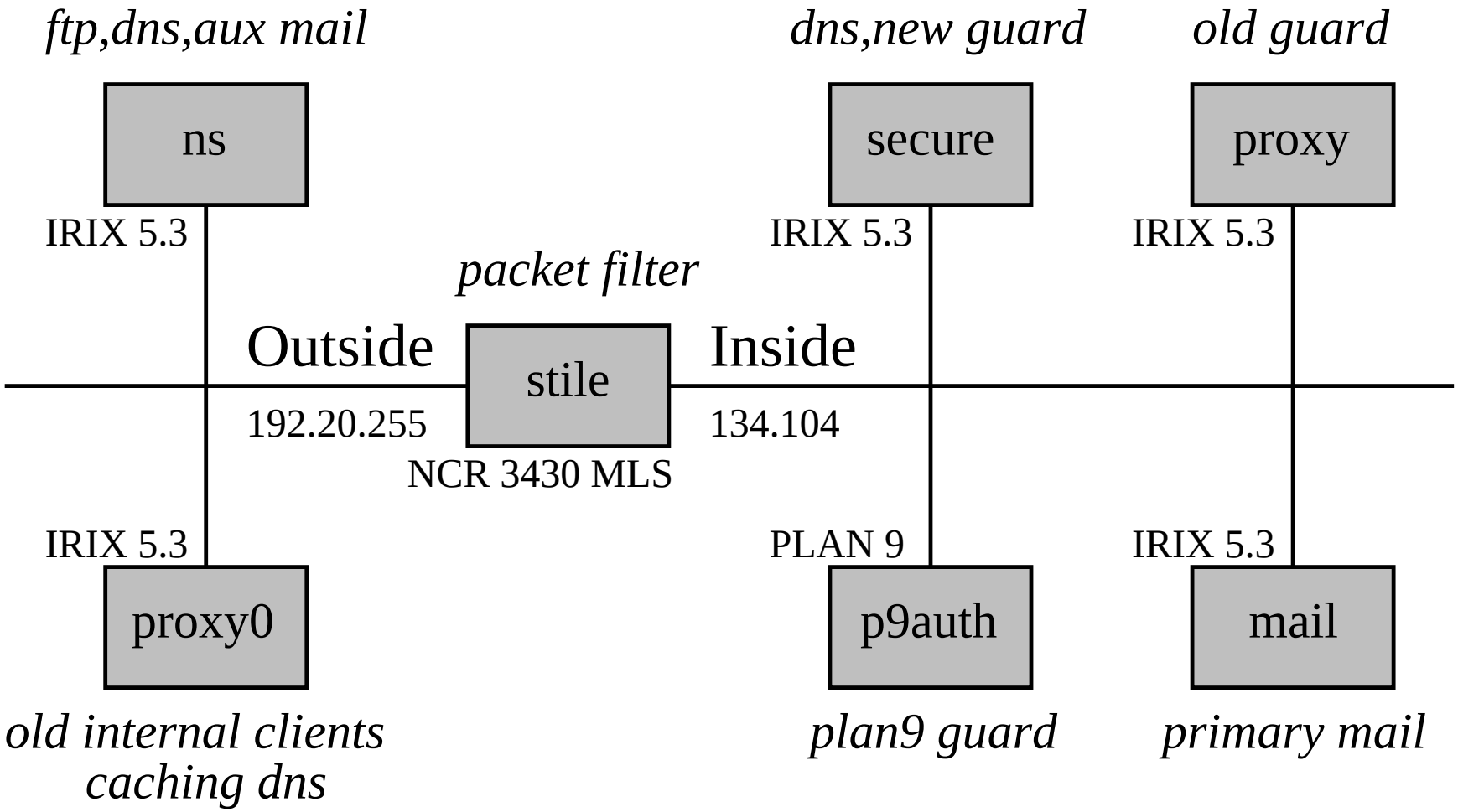
large.fig

New firewall goals

- High throughput (no more proxies)
- Assemble firewall from high-security industrial parts
- Understand issues of commercialization of (2)
- Workbench for new firewall book chapter
- Medium-grade firewall for internal use

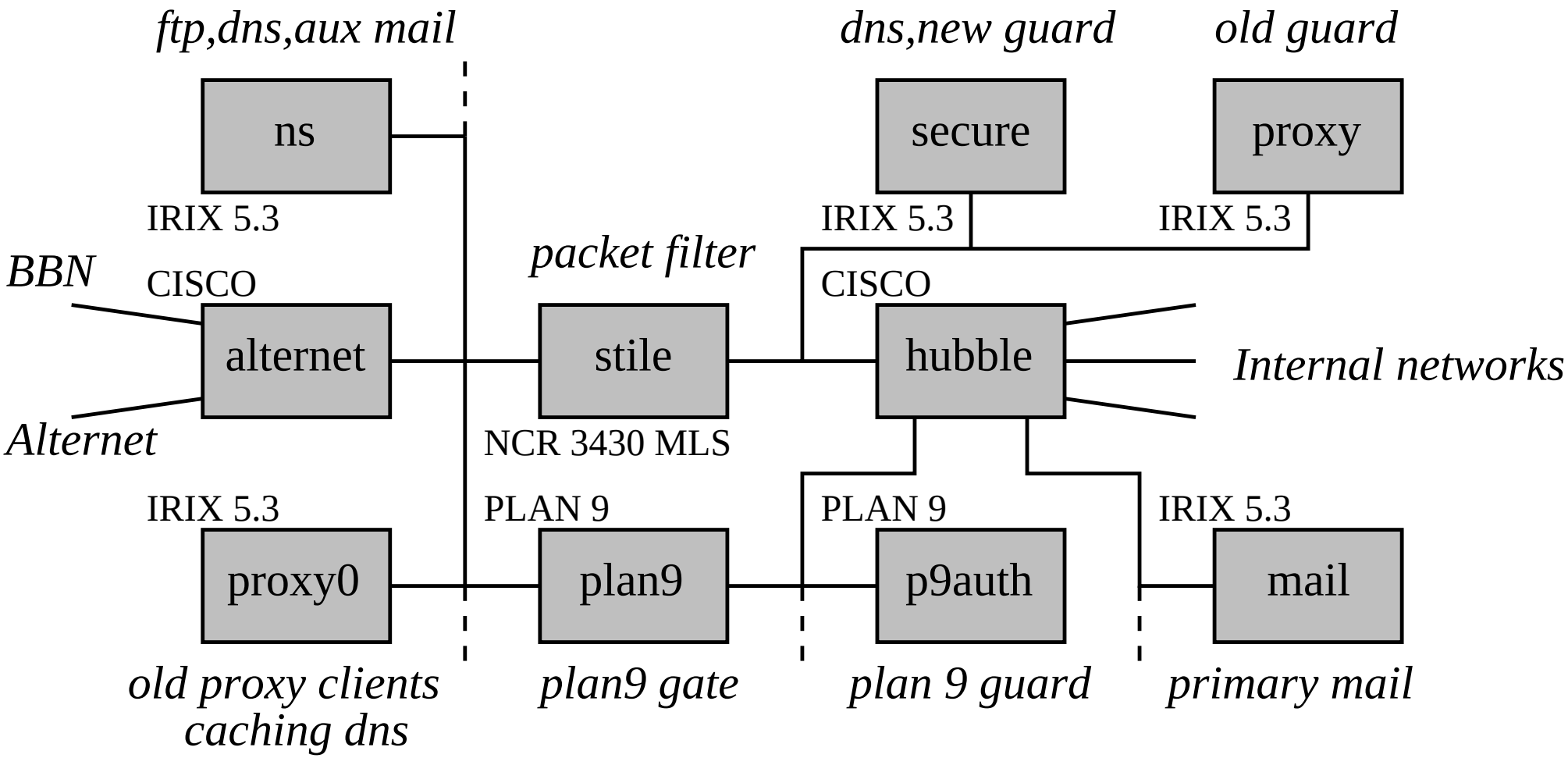
goals.fig

research.att.com firewall



firewall.fig

research.att.com firewall network (partial)



network.fig

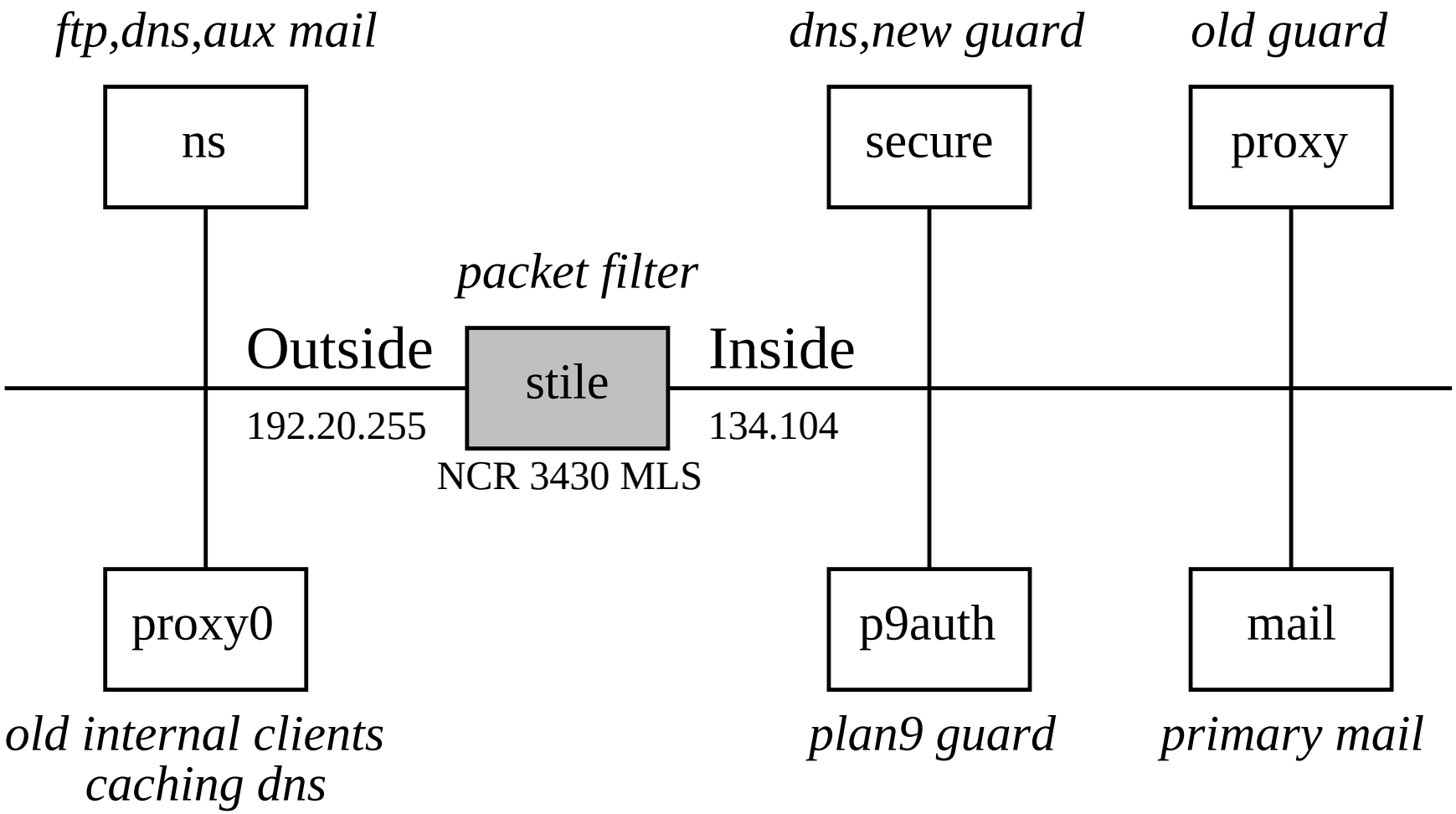
Small print...

Warning Notice

This system is restricted solely to AT&T authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modification of this system is strictly prohibited by AT&T. Unauthorized users are subject to Company disciplinary proceedings and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, AT&T may provide the evidence of such activity to law enforcement officials. All users must comply with AT&T Corporate Instructions regarding the protection of AT&T information assets.

So there.

stile - dynamic packet filter



stile.fig

stile - dynamic packet filter

- Dual 60 MHZ Pentium system
- NCR 3420 MLS, derived from B1 System V
- Kernel-based packet filter
  - Remembers existing connections (not TCP ACK)
  - Remembers UDP "connections"
  - No ftp PORT commands

stile-what.fig

Packet filter policy

- No inbound TCP connections (passive FTP)
- Inbound logins via guard service
- No UDP from/to Internet
- Inbound-only multicast
- 24 Rules

stile-policy.fig

Packet filter problems

- Needs X-based GUI (no textual config file)
- Remote admin via telnet (no usable serial port)
- Tweaking of timeout params (ftp command)

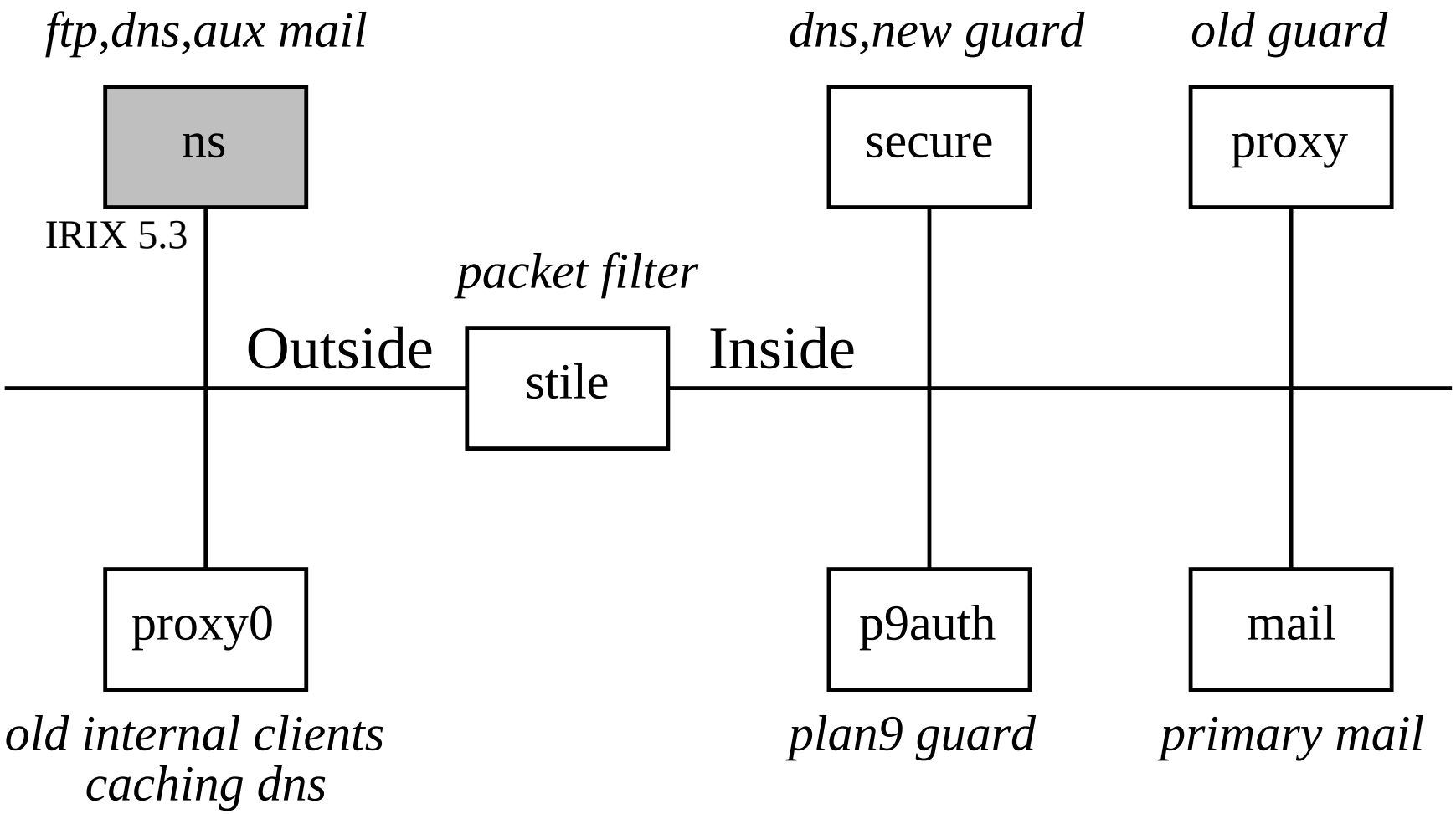
stile-problems.fig

Impact of using packet filter instead of proxy

- Internal addresses appear in packets on the outside
- Outside world needs DNS info about internal networks
- External addresses appear in packets on the inside
- Inside world needs DNS info about external networks

impact.fig

ns - external information services



ns.fig

ns - external information services

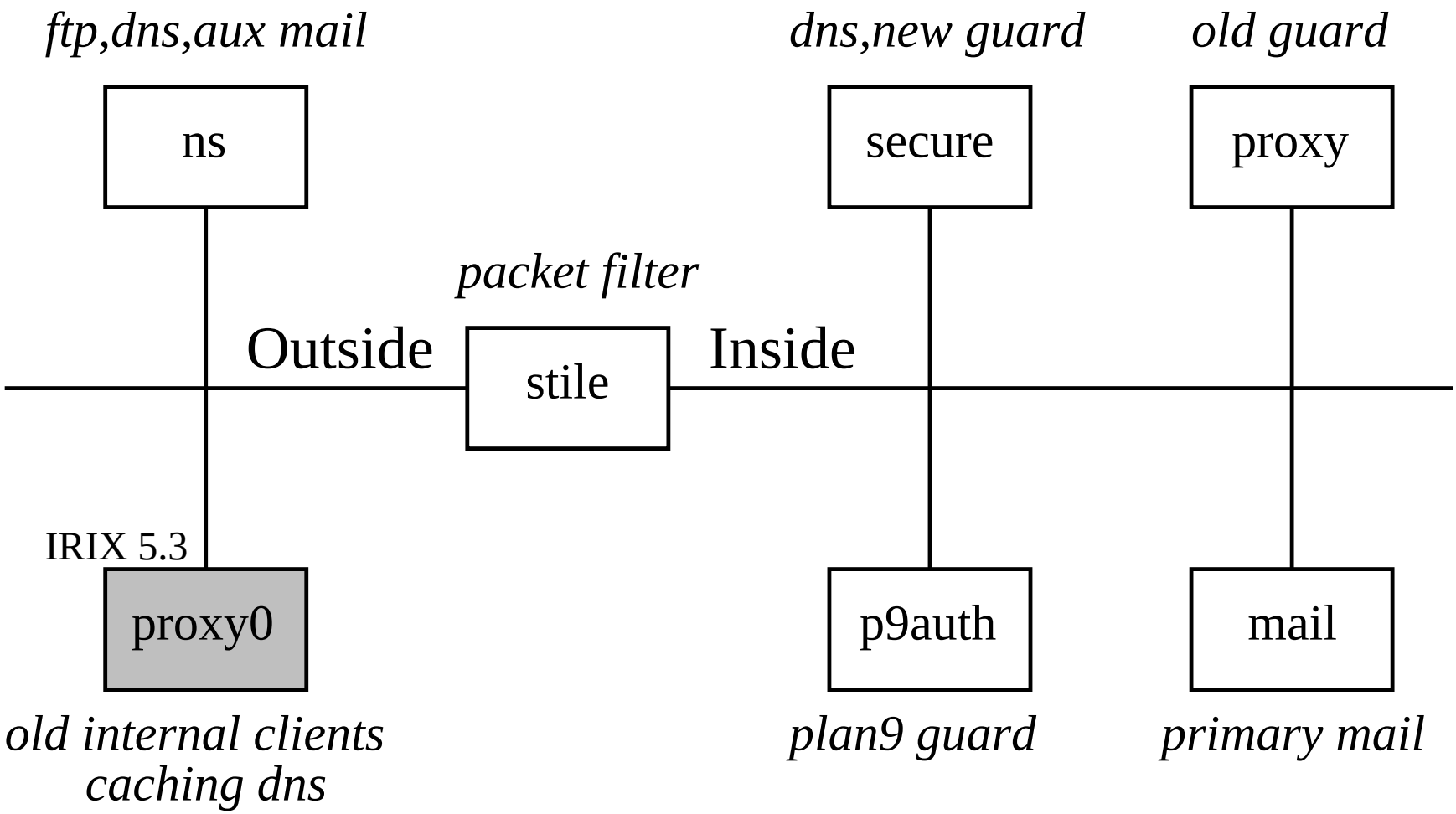
- Anonymous ftp archive (aftpd by ches/mjr)
- Outside DNS service (bind 4.9.3-beta26)
- Secondary MX service (upas)
- Experimental ANSI Z39.50 database query service

ns-what.fig

Z39.50 service possible weak spot

- Executed from inetd:
  chroot /usr/wald /bin/su - wald -c /tree/bin/z39server
- Enters the jail as root
- root depends on integrity of files inside jail:
  shared libs, /bin/su, /etc/passwd, /etc/group
- User owns login "shell"

proxy0 - proxy and auxiliary dns server



proxy0.fig

proxy0 - services and problems

Services for internal clients:

- Cacheing DNS server
- Old-style proxy service

Services not appropriate for exposed system:

- plan9 network file system server enabled
- snmp listener enabled

proxy0-what.fig

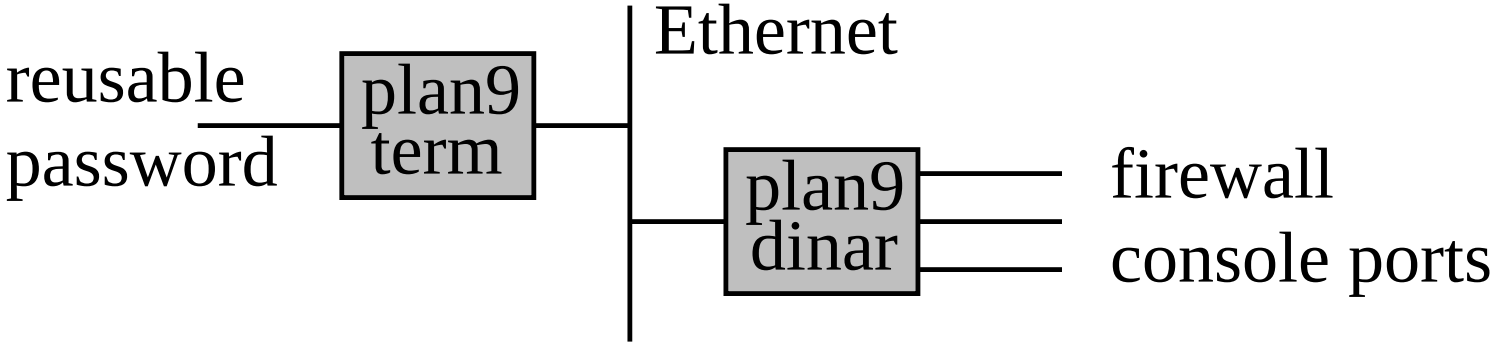
Remote file update services

- cget, cput: remote file read and write
- stage: restricted rdist service
- Servers run chrooted
- Servers run at user privilege (configurable per jail)
- One DES key per host-host pair

rdist.fig

Superuser access on the research firewall

- Unpassworded root accounts
- Console ports hooked up to group-accessible plan9 connection box



root.fig

Miscellanea

- No internal physical security (3000 MH employees)
- Backup as needed, no off-site backups
- Gateway accepts plain telnet from outside
- No syslogging to central system

misc.fig

Future

- Using SYSV/MLS for a packet filter makes no sense
- Use something simple based on plan9/brazil
- The COBOL of packet fitering - GUIs are evil