Bastion Hosts

- Like the lobby of a building
- Highly exposed. (known to the Internet)
- General principles:
  - Keep it simple
    - The simpler, the more secure
  - Be prepared for the bastion hosts to be compromised
    - Keep asking “what if it is compromised?”
    - Reason: Most accessible from outside.
    - Protect by checking passwords from bastion hosts or use packet filtering

Special Bastion Hosts

- Non-routing dual-homed hosts
  - Do not pass information
  - Do not use it as the whole firewall
- Victim machines
  - For new services (do not know the security holes yet)
  - Keep few services as possible.
  - Key: disposable (no important stuffs there)
- Internal bastion hosts
  - E.g., internal SMTP servers (second bastion hosts), or News servers.

Choose a Machine

- What OS?
  - something you are familiar with (no time for new OS)
  - UNIX (probably the best choice)
    - has already a lot of tools
    - In our talk, we will assume UNIX.
    - Choose the versions you know (maximize your happiness) but least popular (minimize the chance of breakin)

Choose a Machine (cont)

- How fast a machine?
  - In general, no need to be fast. Reasons:
    - costs
    - Most do not need much work (even for T1 lines)
    - E.g., 486-based UNIX platforms, Sparcstation-2.
  - Need more powers for compression/decompression or searches, etc.
  - Reasons for not oversized:
    - a slower machine attracts less intruders
    - less power makes it harder to attack internal systems
    - a slower machine attracts less insiders to compromise. (Should not use it for other purpose.)

Choose a Machine (cont)

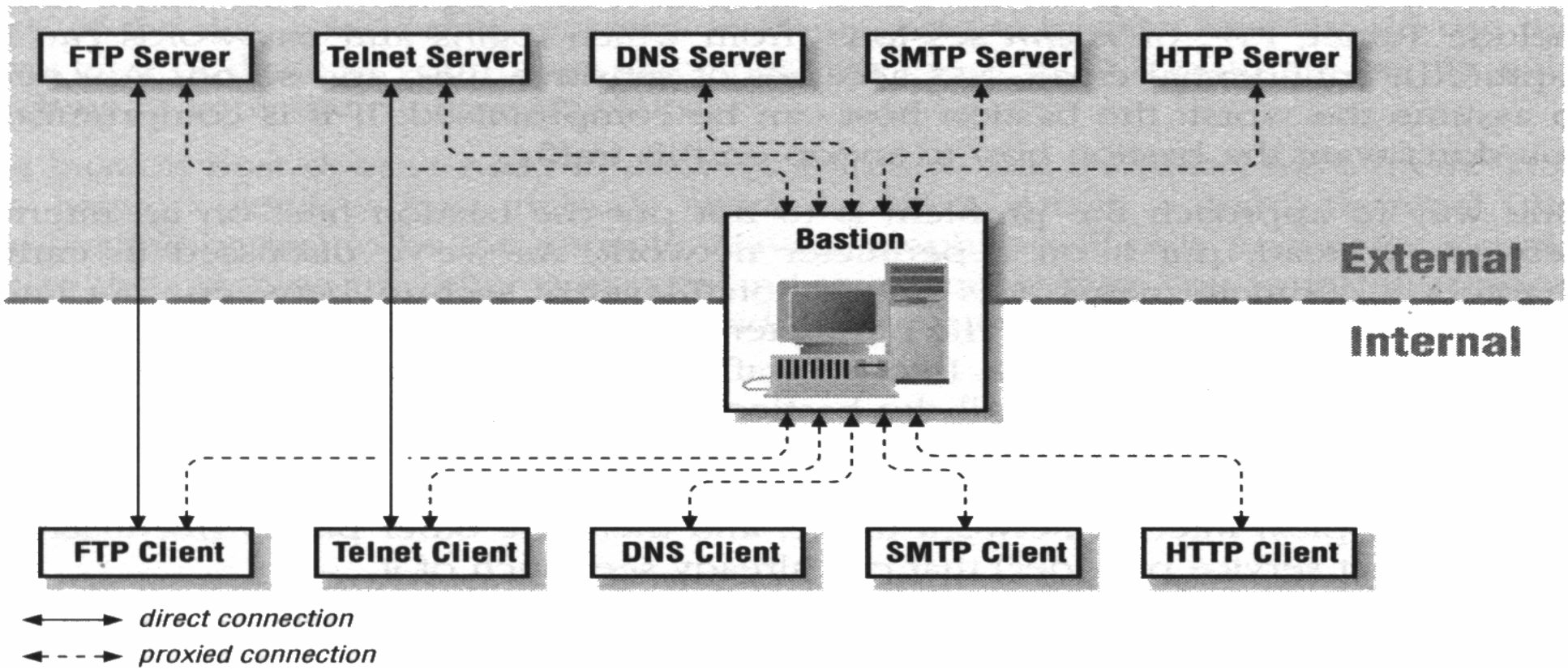
- What Hardware Configuration?
  - memory-intensive
    - keeping connections may need a large amount of memory and swap space.
    - cache proxy may need a large disk space.
  - CD-ROM drive (compare files with those in CD-ROM)
  - Easily add disks for maintenance work
  - The boot disk should be easily removable (for maintenance)
  - Dumb terminal is good enough.

Choose a Machine (cont)

- Locating the bastion host on the network
  - the network should not carry confidential traffic
    - On Ethernet and token rings, all packets are exposed to connected hosts.
    - programs like etherfind and tcpdump
    - so, keep outside internal networks. (usually in perimeter network)

Selecting Services

- Typical set:



Services Catalogues

- Secure services
  - Just use packet filtering, e.g., talk
- Insecure services (normally) but can be secure
  - provided on the bastion hosts, e.g., SMTP, FTP, Gopher, WAIS, HTTP, NNTP (above needs DNS)
- Insecure services (normally) and cannot be secure
  - Disable, or put it in a victim host.
- Services you don’t use
  - Just disable

User Accounts on Bastion Hosts

- If possible, no!!! Reasons:
  - Easy to be attacked.
  - Users may behave unpredictably.
  - Reduce stability and reliability
  - Hard to detect attacks.

Building a Bastion Host

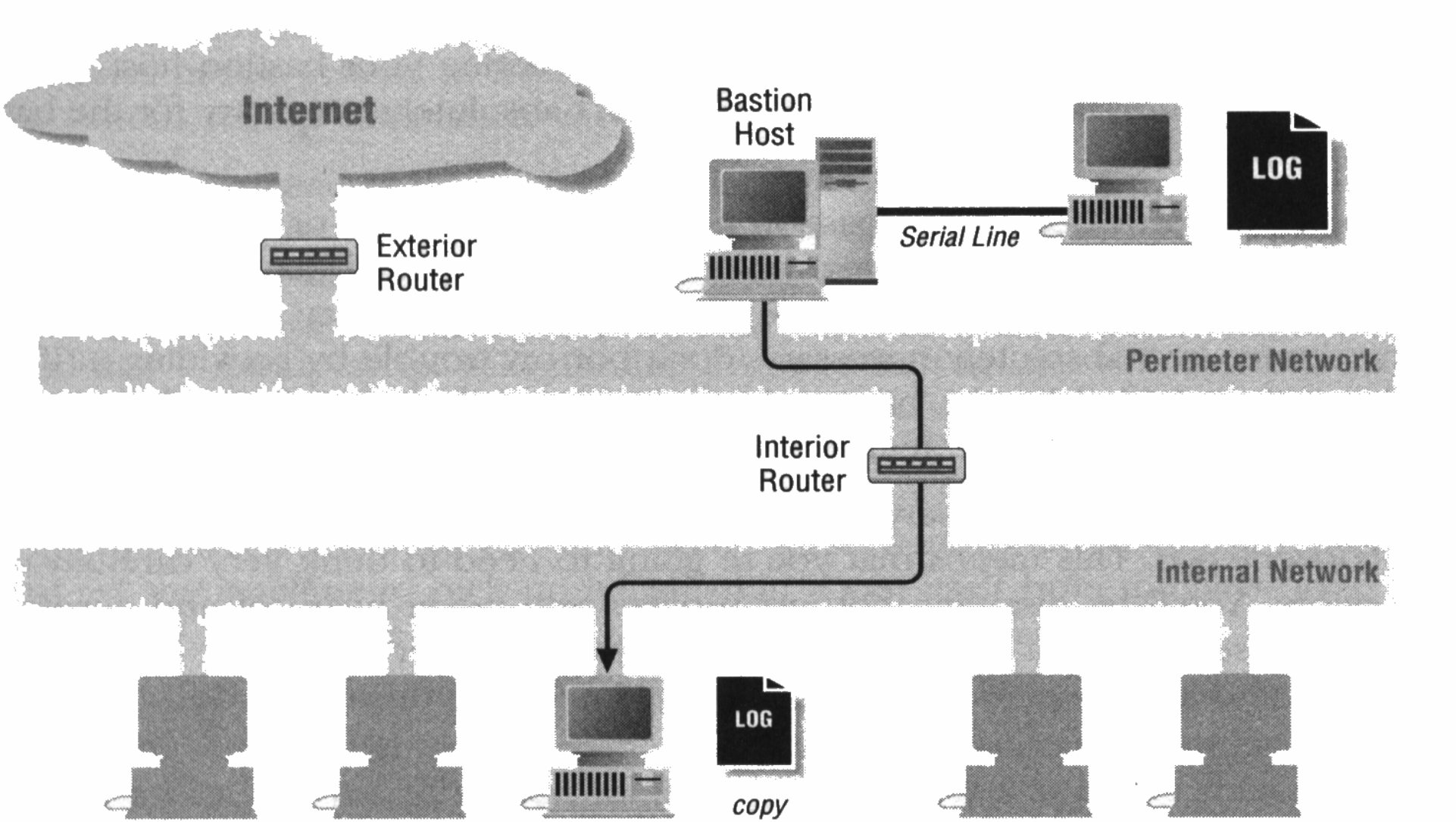
- Secure the machine
- Disable all non-required services
- Install or modify the services to be provided.
- Reconfigure the machine
- Run a security audit to establish a baseline
- Connect the machine to the network

Do not connect till the last step

(can be attacked then)

Securing the Machine

- Minimal clean operating system installation
- fix all known system bugs
  - ftp://ftp.greatcircle.com/pub/firewalls/vendor_security_contacts
- Use a checklist
- Safeguard the system logs
  - system logs for convenience (regular, for analysis)
  - system logs for catastrophes
    - Use dropsafe PC (instead of printer)
  - setting up system logs
    - UNIX: /etc/syslog.conf, others: syslog


Internet
Bastion Host
LOG
Exterior Router
Serial Line
Perimeter Network
Interior Router
Internal Network
LOG
copy

Disabling Non-required Services

- How are services managed?
  - Key files:
    - /etc/rc: initial routines
    - /etc/inetd.conf: services
- How to disable services:
  - comment out
- Which services should be left enabled?
  - init, swap, page, cron, syslogd, inetd
- Which services should you disable?
  - If you don’t need it, don’t know what it does,

Usually Disabled Services

- NFS and related services:
  - nfsd,biod, mountd, statd,lockd, automount, keyserv, rquotad, amd (in /etc/rc)
- RPC Services:
  - ypserv, ypbind, ypupdated, rexd, walld
- Booting services:
  - tftpd, bootd, bootpd
- BSD “r” command services
- ftpd, (if needed, just do another one)
- Others
  - routed, fingerd, uucpd, rwhod, lpd

Installing and Modifying Services

- Use the TCP wrapper package to protect services
  - install the package
  - Reconfigure inetd to run TCP Wrapper (tcpd)
  - tcpd evaluates requests
  - If acceptable, starts “real” server.

  (check more in page 180)
- Use netacl to protect services
  - netperm configuration file.

Reconfiguring for Production

- Reconfigure and rebuild the kernel
- Remove all unnecessary programs
- Mount as many file systems as possible to read-only

Things to be cautious:

- Write all the tools to a tape before delete them
- Setting a small, external, alternate boot disk.

Running a Security Audit

- Auditing packages
  - checking for well-known security holes
  - Establishing a database of checksums of all files.
    - recognize future changes (esp. unauthorized changes)
- Examples
  - COP, Tiger, Tripwire

Operating the Bastion Hosts

- Profiles
  - how many jobs to be run at a time?
  - how much CPU time?
  - What is the typical load?
- Automate Monitoring
  - Must catch break-in as soon as possible.
  - SWATCH (Simple WATCHer).