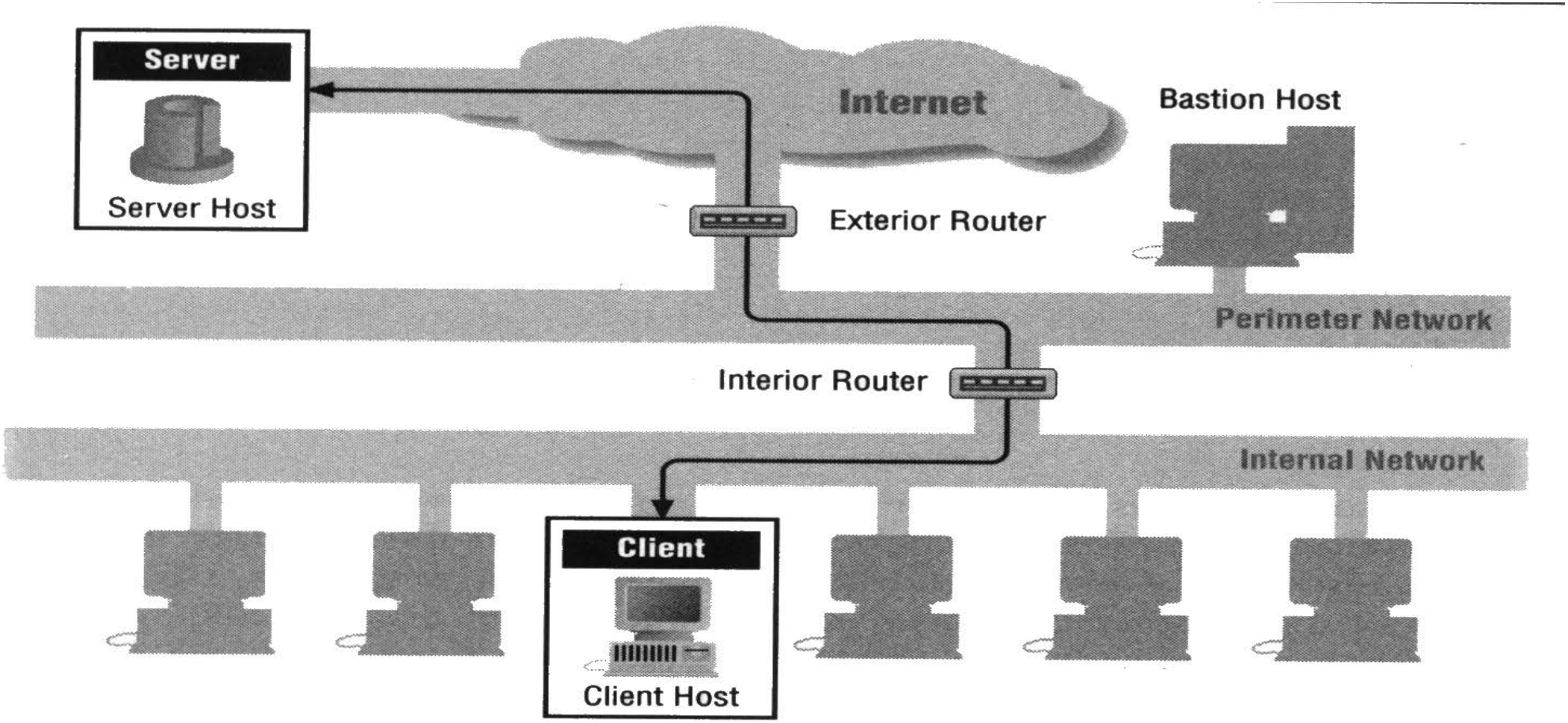
Internet Services

- Electronic Mail: SMTP
- File transfer: FTP, TFTP, UUCP, FSP, rcp
- News: NNTP
- Remote terminal access: telnet, rsh, rlogin, rexec
- World-Wide Web access: HTTP
- Other information services: gopher, archie, wais, finger, whois.
- Real-time conferencing: talk, IRC, Mud (based on mbone/multicast)

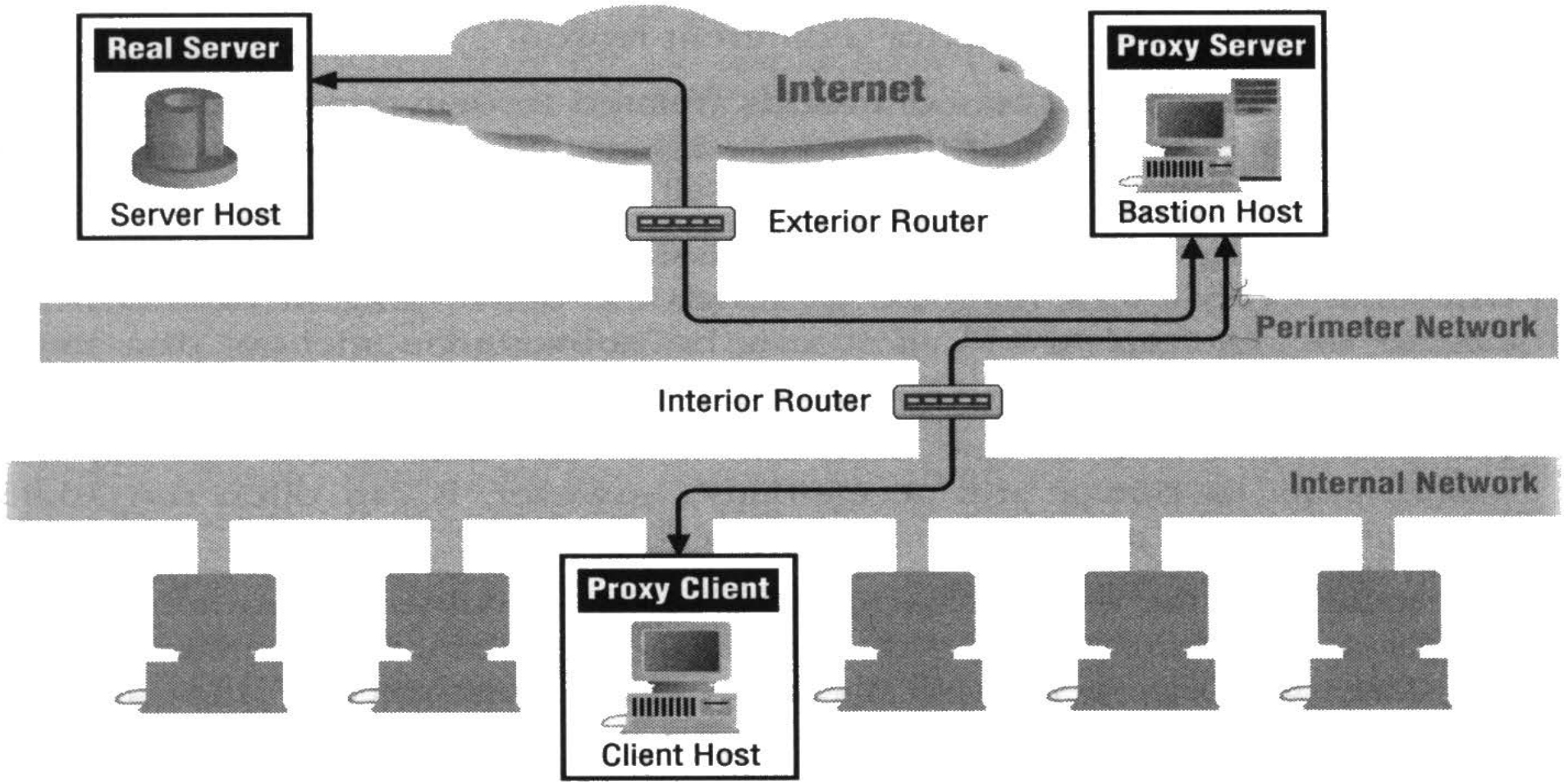
Internet Services (cont)

- Name services: DNS, NIS/YP (not important)
- Network Management Services: ping, traceroute (based on ICMP), SNMP
- Time services: NTP
- Network File Systems: NFS, AFS.
- Window systems: X11
- Printing systems: lpr.

Generic Direct Service



Generic Proxy Service



Electronic Mail

- A server accepts mails from external hosts.
  - if the server isn't secure, it will give an attacker all the access.
- A delivery agent puts the mail in the mailbox.
  - needs special permissions to store mail. This makes intruder broader access.
- A user agent lets the recipient read the mail and compose outgoing mail.
  - it can run arbitrarily other problems to response a message.

To: victim@target.com

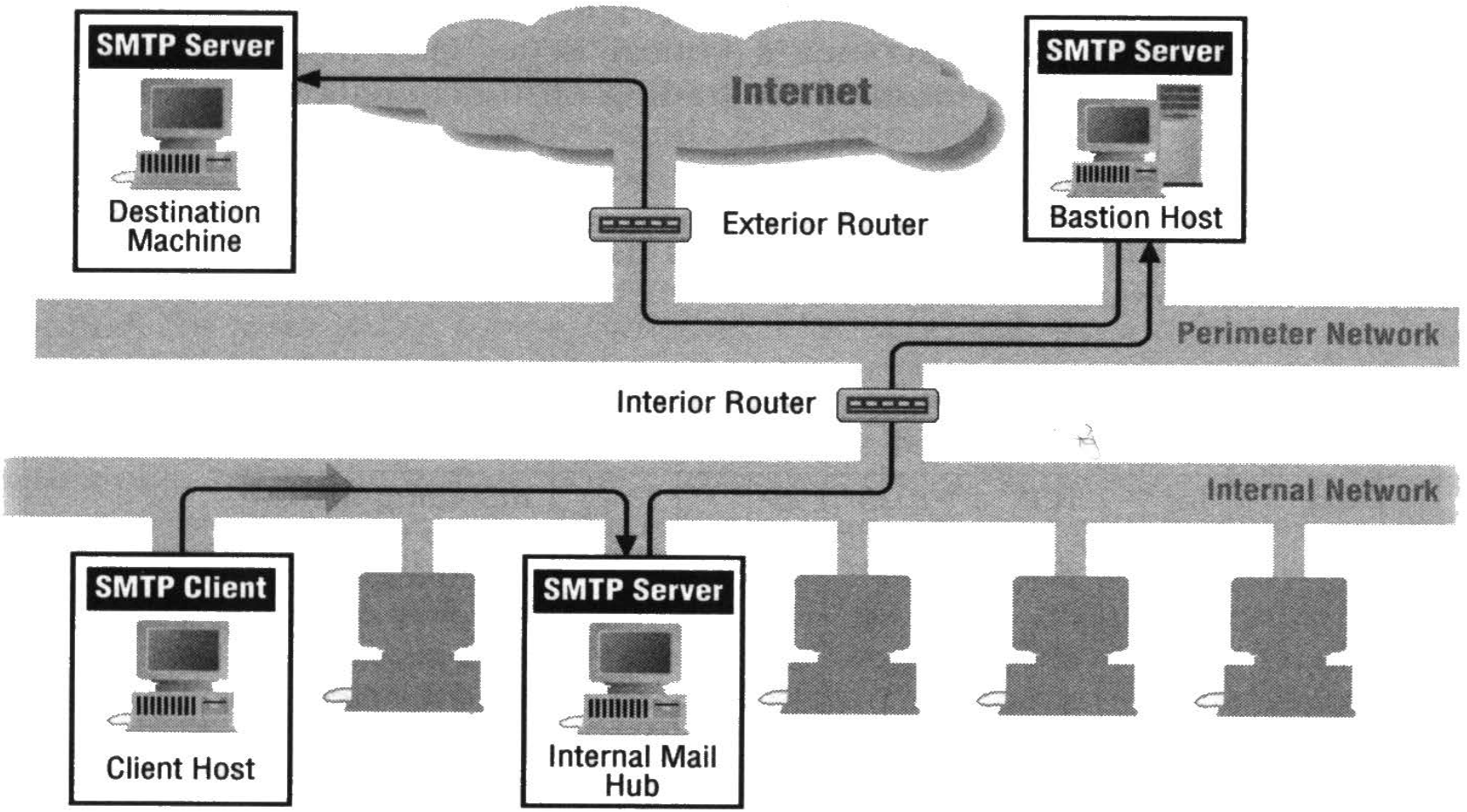
From: ``| /bin/sed `1,/^$/d' | sh''

SMTP

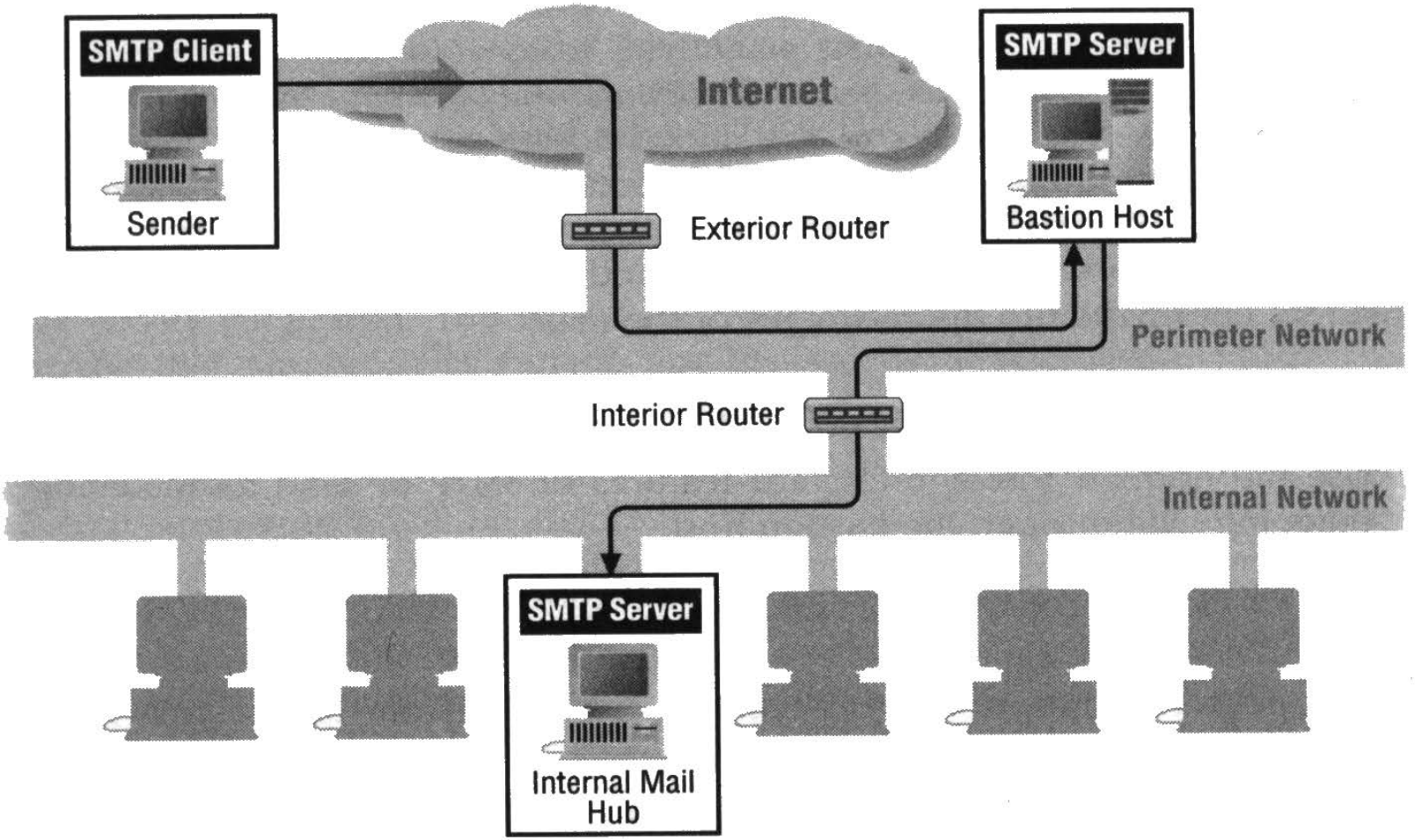
- Philosophy:
  - many people use it --> a lot security holes.
  - many people use it --> a lot holes fixed.
- Security Problems:

  Sendmail needs root privileges
  - Listen on port 25
  - read each user's .forward.
  - execute kernel system calls, e.g., free disk space available.
  - Protect files in the mail queue.
- Bastion Hosts (not to be root)
  - use Smap package (only 700 lines)
  - no need to read .forward (no users on it)
  - set uid to the owner of the queue directory.

Outbound


SMTP Server
Destination Machine
Internet
Exterior Router
SMTP Server
Bastion Host
Perimeter Network
Interior Router
Internal Network
SMTP Client
Client Host
SMTP Server
Internal Mail Hub

Inbound

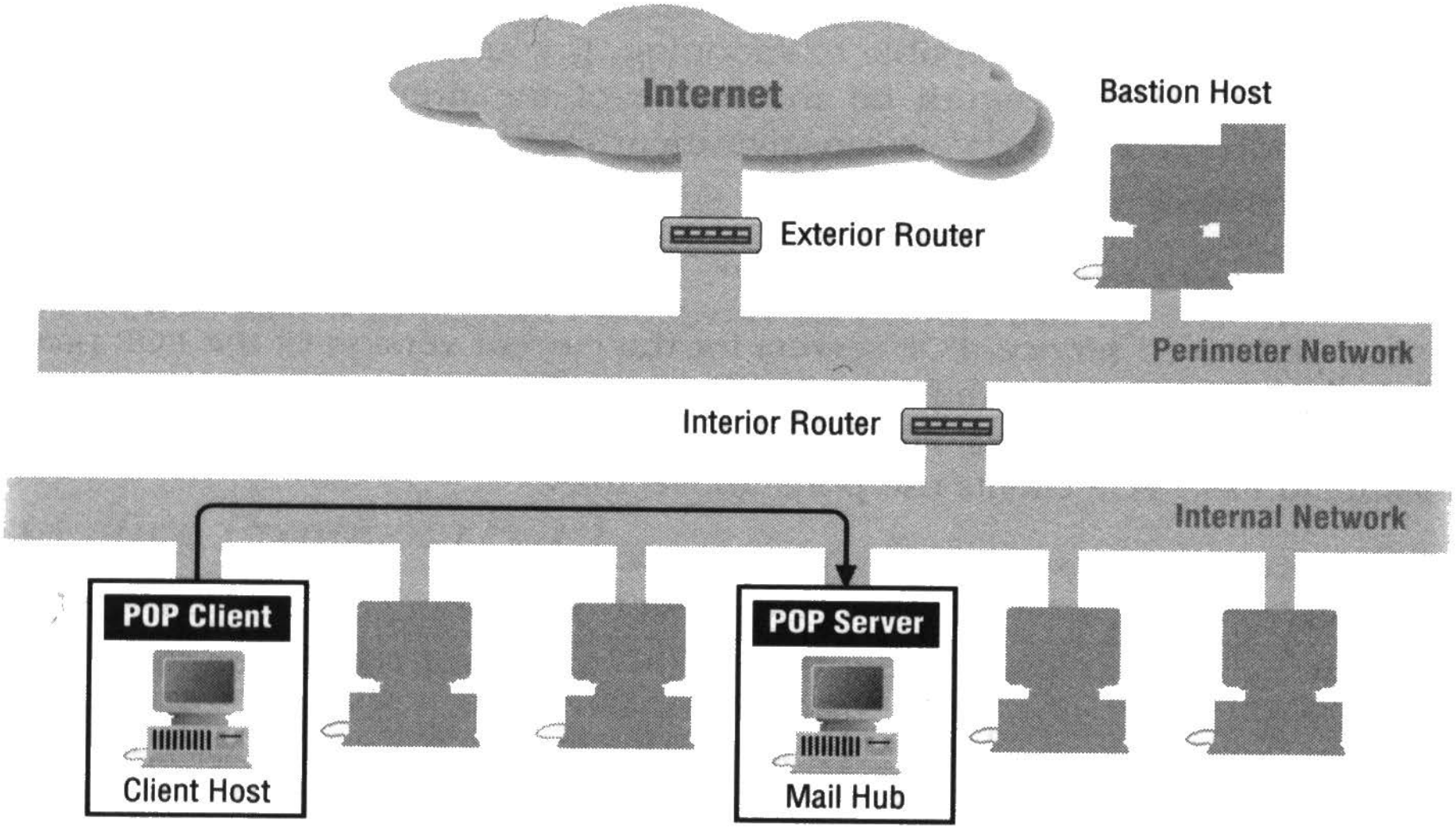

SMTP Client
Sender
Internet
Exterior Router
SMTP Server
Bastion Host
Perimeter Network
Interior Router
Internal Network
SMTP Server
Internal Mail Hub

Recommendation for SMTP

- Use bastion host as proxy
- Use packet filtering to restrict SMTP from external hosts to the bastion host only.
- Use packet filtering to restrict SMTP from the bastion host to specific internal SMTP servers.
- Use smap instead of Sendmail in the bastion host.
- Keep up-to-date patches for delivery agents and user agents.
- Educate users.

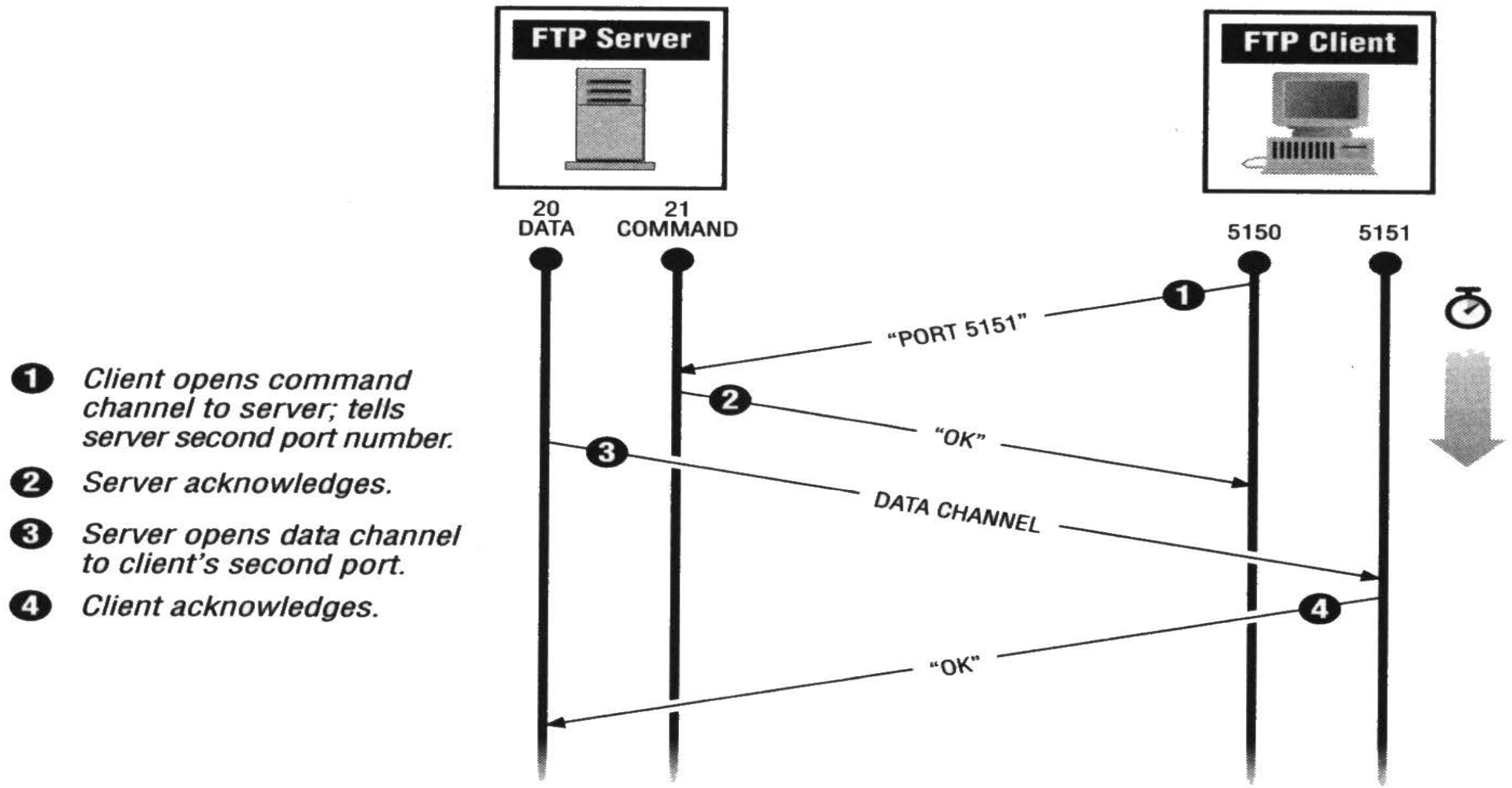
Recommendation for POP

- Do not allow users to transfer your site's mail over the Internet via POP.
  - Because it may reveal passwords.
- If necessary, designate specific sites (external) for packet filtering.
- use proxying services.


Internet
Bastion Host
Exterior Router
Perimeter Network
Interior Router
Internal Network
POP Client
Client Host
POP Server
Mail Hub

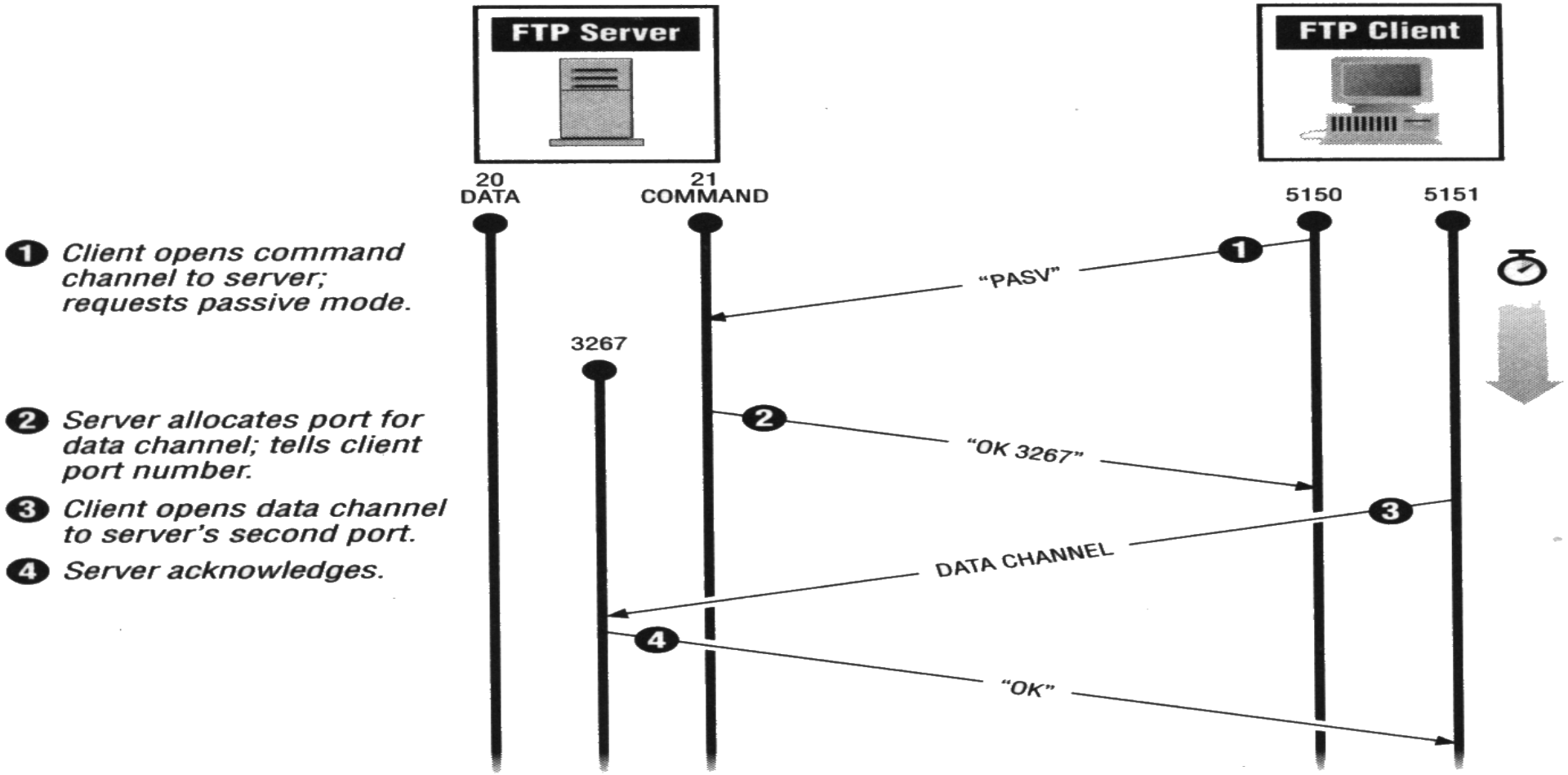
FTP

- Connections (normal mode):
  - Command: Client (>1023) to Server (port 21)
  - Data: Server (port 20) to Client (> 1023)


FTP Server
FTP Client
20
DATA
21
COMMAND
5150
5151
1
"PORT 5151"
2
"OK"
3
DATA CHANNEL
4
"OK"
1 Client opens command channel to server; tells server second port number.
2 Server acknowledges.
3 Server opens data channel to client's second port.
4 Client acknowledges.

Passive Mode

- Data: Client to Server (> 1024)


FTP Server
FTP Client
20
DATA
21
COMMAND
5150
5151
1 Client opens command channel to server; requests passive mode.
"PASV"
3267
2 Server allocates port for data channel; tells client port number.
"OK 3267"
3 Client opens data channel to server's second port.
DATA CHANNEL
4 Server acknowledges.
"OK"

Direction	Source Addr.	Dest. Addr.	Protocol	Source Port	Dest. Port	ACK Set	Notes
In	Ext	Int	TCP	>1023	21	[a]	Incoming FTP request
Out	Int	Ext	TCP	21	>1023	Yes	Response to incoming request
Out	Int	Ext	TCP	20	>1023	[a]	Data channel creation for incoming FTP request, normal mode
In	Ext	Int	TCP	>1023	20	Yes	Data channel responses for incoming FTP request, normal mode
In	Ext	Int	TCP	>1023	>1023	[a]	Data channel creation for incoming FTP request, passive mode
Out	Int	Ext	TCP	>1023	>1023	Yes	Data channel responses for incoming FTP request, passive mode
Out	Int	Ext	TCP	>1023	21	[a]	Outgoing FTP request
In	Ext	Int	TCP	21	>1023	Yes	Response to outgoing request
In	Ext	Int	TCP	20	>1023	[a]	Data channel creation for outgoing FTP request, normal mode
Out	Int	Ext	TCP	>1023	20	Yes	Data channel responses for outgoing FTP request, normal mode
Out	Int	Ext	TCP	>1023	>1023	[a]	Data channel creation for outgoing FTP request, passive mode
In	Ext	Int	TCP	>1023	>1023	Yes	Data channel responses for outgoing FTP request, passive mode

[a] ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

Proxying for FTP

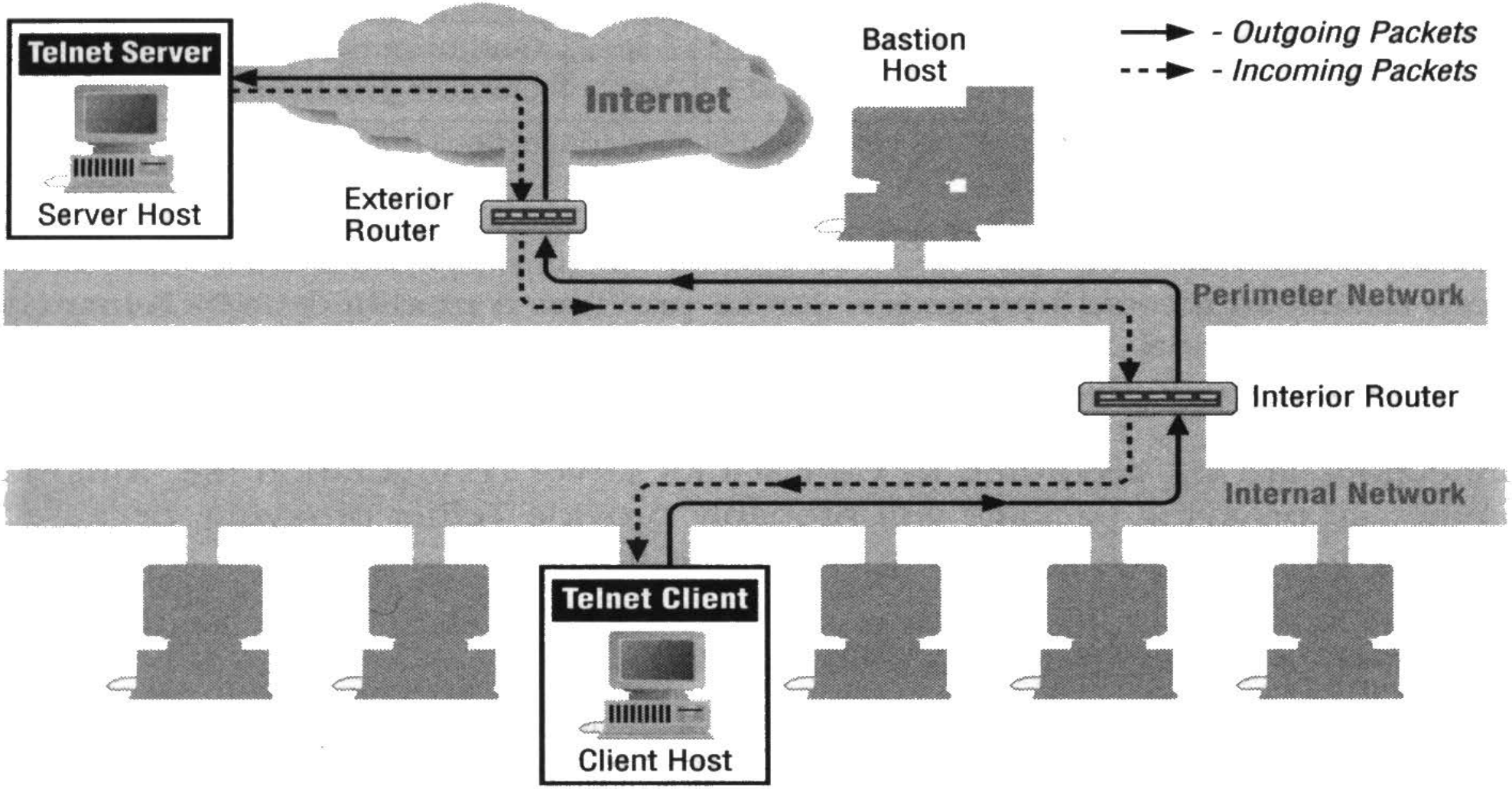
- Must use Proxy: if not,
  - Normal mode:
    - Allow external hosts to connect internal hosts (with any port above 1023)
  - Passive mode:
    - Not every FTP servers support this.
    - Hard for external to defend.
- Proxying: the most attractive solution for outbound FTP.
  - Normal mode between bastion host and external hosts. (SOCKS)
- Another Possible Solution:
  - Passive mode

Inbound FTP

- Use packet filters to allow incoming FTP only to bastion hosts.
- If allow upload, protect the writable area from third parties.
  - make the directory write-only (-wx)
  - disable creating directories and certain files
  - upload by prearrangement
  - Remove files constantly.
- Be sure about the upload persons.
  - not for phorno, or illegal software packages.

Telnet

- Telnet is a cleartext protocol.
- Recommendation
  - Restrict incoming telnet as far as possible.
  - Outgoing telnet can safely be allowed via packet filtering or proxying.
    - packet filtering is fine.
  - if you’re concerned about the sensitivity of the data accessed over telnet sessions, use encrypting versions of telnet.


Telnet Server
Server Host
Internet
Exterior Router
Bastion Host
- Outgoing Packets
- Incoming Packets
Perimeter Network
Interior Router
Internal Network
Telnet Client
Client Host

Remote Command Execution

- Connections:
  - Normal: Client (>1023) to Server (513 or 514)
    - 513: rlogin
    - 514: rsh, rcp, rdump, rrestore, and rdist
  - Error report for rsh: Client (<1023) to Server (<1023)
- Problems:
  - Since error report uses randomed ports below 1023, it is hard for firewall to deal with.
- Recommendations:
  - Do not allow “r” commands, except outbound by proxy (like SOCKS).
  - No outbound rsh service, because it uses all ports below 1023. (just no way to protect in firewall)
  - Beware disclosure of reusable passwords.

Filtering Policy

Direction	Source Addr.	Dest. Addr.	Protocol	Source Port	Dest. Port	ACK Set	Notes
In	Ext	Int	TCP	<1023	513	[a]	Incoming *rlogin*, client to server
Out	Int	Ext	TCP	513	<1023	Yes	Incoming *rlogin*, server to client
Out	Int	Ext	TCP	<1023	513	[a]	Outgoing *rlogin*, client to server
In	Ext	Int	TCP	513	<1023	Yes	Outgoing *rlogin*, server to client
In	Ext	Int	TCP	<1023	514	[a]	Incoming *rsh/rcp/rdump/rrestore/rdist*, client to server
Out	Int	Ext	TCP	514	<1023	Yes	Incoming *rsh/rcp/rdump/rrestore/rdist*, server to client
In	Ext	Int	TCP	<1023	<1023	Yes	Incoming *rsh*, error channel, client to server
Out	Int	Ext	TCP	<1023	<1023	[a]	Incoming *rsh*, error channel, server to client
Out	Int	Ext	TCP	<1023	514	[a]	Outgoing *rsh/rcp/rdump/rrestore/rdist*, client to server

Recommendations of NNTP

- Don’t use a bastion host as a news servers
  - news server absorbs all disk space and processing time.
  - you can not have any private or propritery groups for internal discussions
  - if necessary,
    - let users log into the bastion host (bad)
    - use only NNTP clients to read news
    - Export news to clients via NFS
    - Relay news through bastion hosts.
- Don’t allow automated group creation
- Allow external NNTP connections only from the sites you exchange news with.
- Use packet filtering or proxying to connect trusted external NNTP servers to an internal news server, and vice versa.

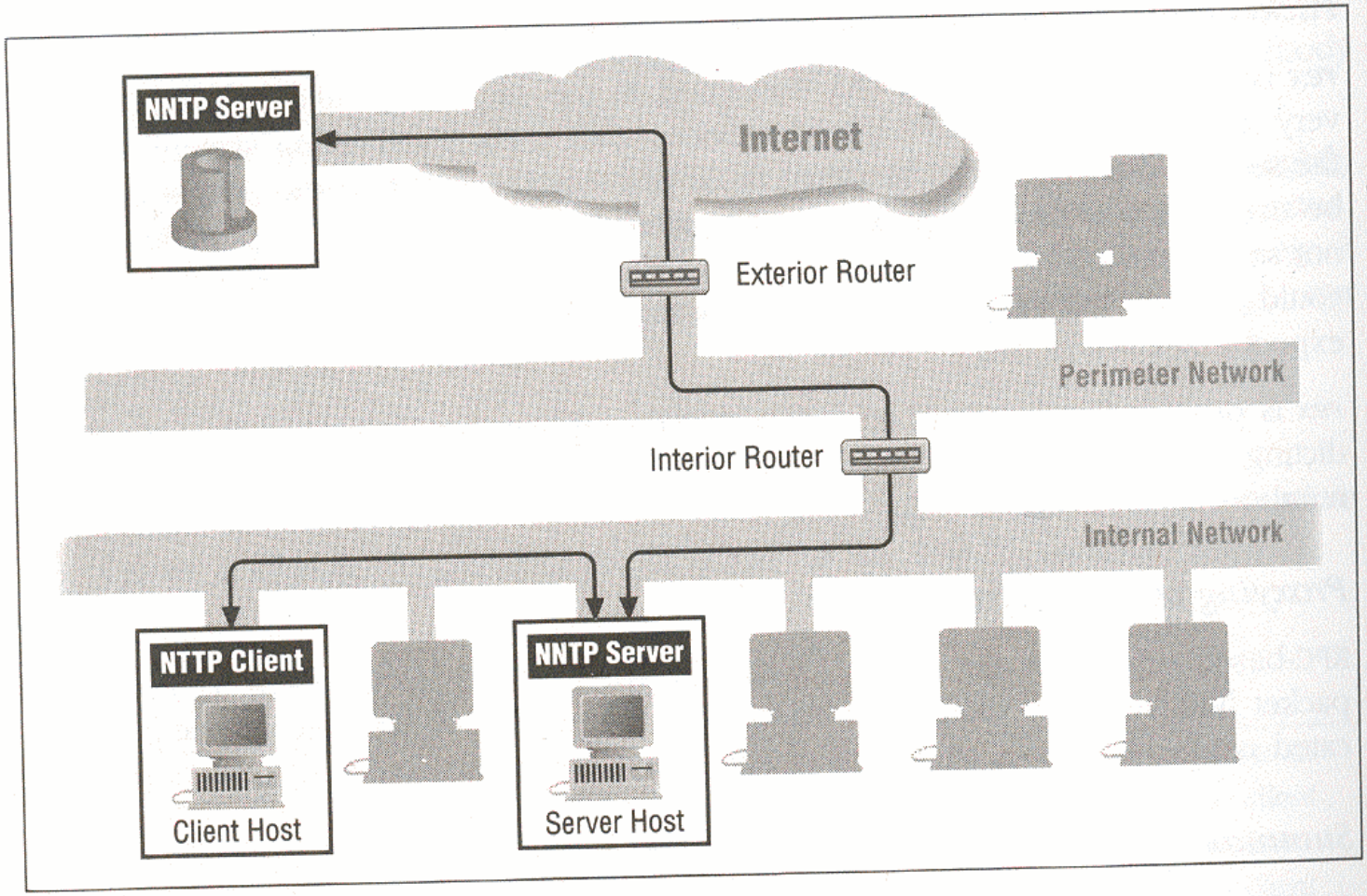


Figure 8-9: NNTP via packet filtering

NNTP via Proxy Services

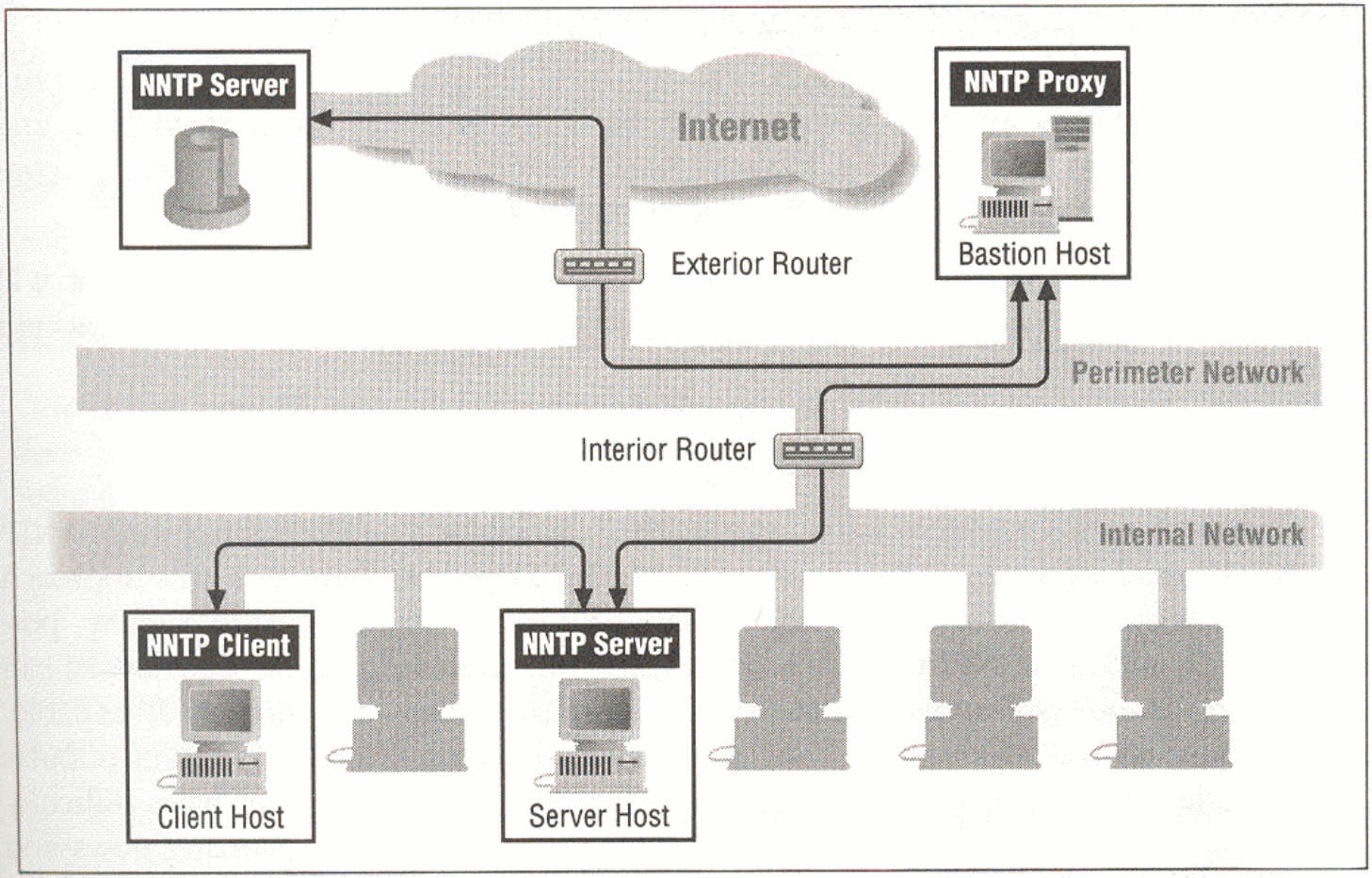


Figure 8-10: NNTP via proxy services

Filtering Policy

Direction	Source Addr.	Dest. Addr.	Protocol	Source Port	Dest. Port	ACK Set	Notes
In	Ext	Int	TCP	>1023	119	[a]	Incoming news
Out	Int	Ext	TCP	119	>1023	Yes	Incoming news responses
Out	Int	Ext	TCP	>1023	119	[a]	Outgoing news
In	Ext	Int	TCP	119	>1023	Yes	Outgoing news responses
[b]	Int	News Server	TCP	>1023	119	[a]	Newsreader client reading news
[b]	News Server	Int	TCP	119	>1023	Yes	Server sending articles to news-reader client

[a] ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.
[b] Both ends are internal in most cases.

WWW and HTTP

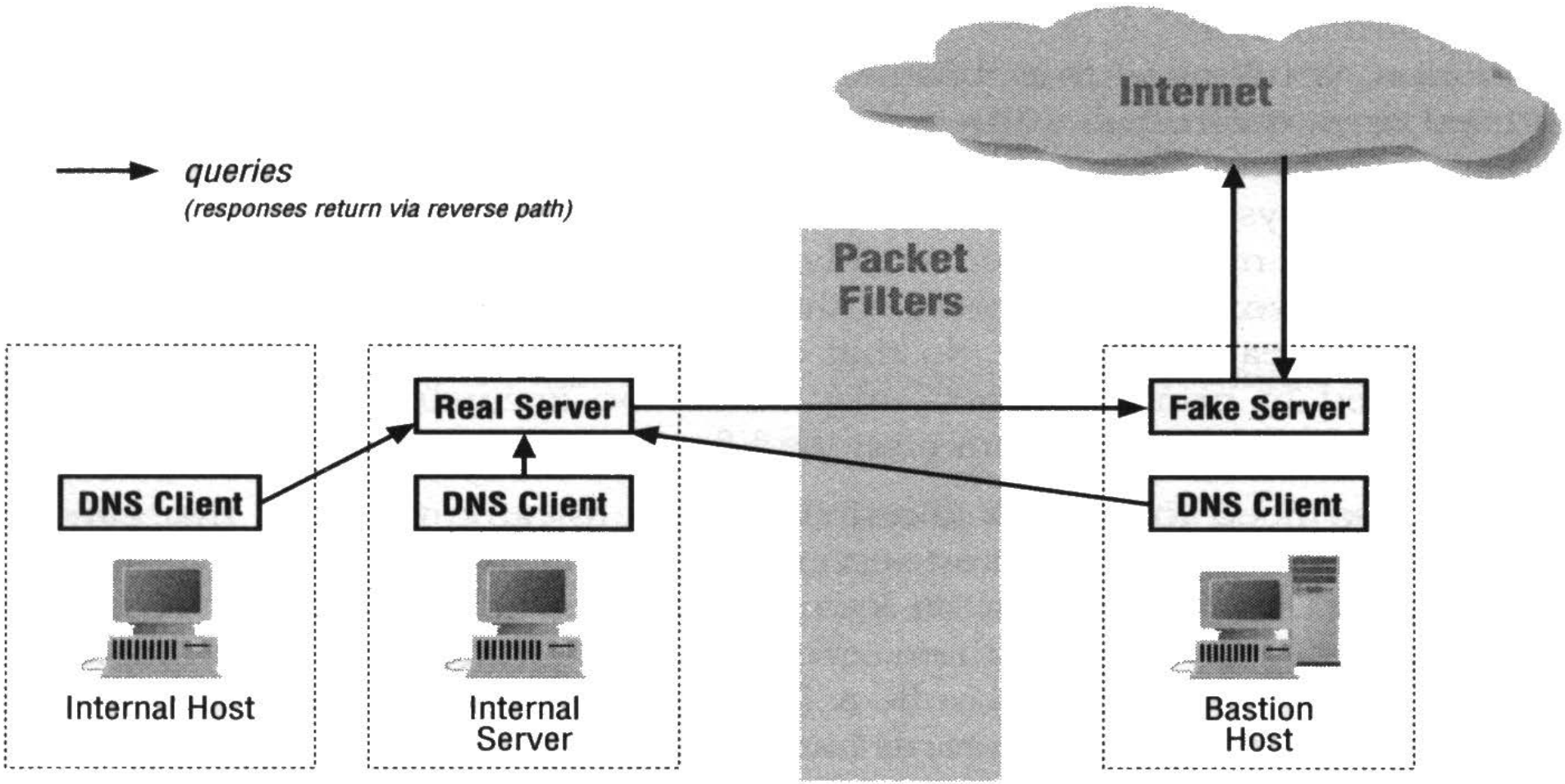
- Outbound Problems for packet filtering:
  - port is not always 80. ==> need proxying on bastion hosts.
- Inbound services:

- Recommendations:
  - use bastion hosts as a proxy to access external.
  - use a dedicated bastion host for an HTTP server.
  - configure the HTTP server to control what it has access to.

DNS

- Basic functions:
  - translate a hostname to an IP address.
  - Translate an IP address to a hostname.
  - Obtain other published information about a host.
- How does it work?
  - For a request, it asks its local DNS server for the information.
  - If not, the local DNS server asks other DNS servers.
  - When knows the answer, return.
- Security Problems:
  - Bogus answers to DNS queries.
  - Mismatched data between the hostname and IP address DNS trees.
  - Reveal too much information to attackers.

Hide Information



Forwarders

- Help packet filtering.