CS 155 May 20, 2004

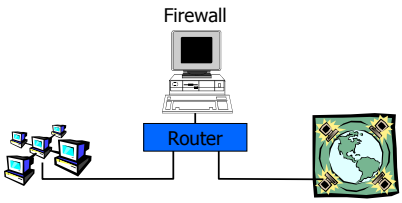
Firewalls

John Mitchell

Credit: some text, illustrations from Simon Cooper

Basic Firewall Concept

- Separate local area net from internet



All packets between LAN and internet routed through firewall

Why firewalls?

- Need to exchange information
  - Education, business, recreation, social and political
- Attacks
  - Drawbacks; unsolicited attention and bugs
- Program bugs
  - All programs contain bugs
  - Larger programs contain more bugs!
  - Network protocols contain;
    - Design weaknesses (SSH CRC)
    - Implementation flaws (SSL, NTP, FTP, SMTP…)
  - Careful (defensive) programming & protocol design is **hard**

Firewall goals

- What is a firewall ?
  - Logically
    - A separator, a restrictor and an analyzer
  - Rarely a single physical object!
    - Any place where internal and external data can meet
    - Can be distributed (although this is not common now)
- Castle & Moat Analogy
  - Restricts access from the outside
  - Prevents attackers from getting too close
  - Restricts people from leaving <- Important!!

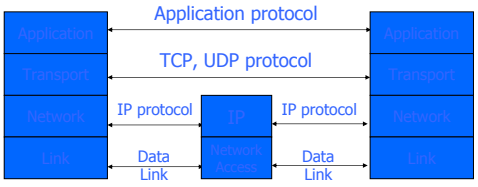
Firewall Design & Architecture Issues

- Least privilege
- Defense in depth (very important)
- Choke point
- Weakest links
- Fail-safe stance
- Universal participation
- Diversity of defense
- Simplicity

Two Separable Topics

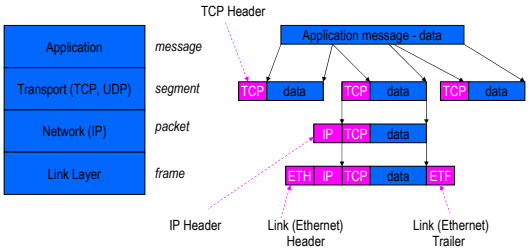
- Arrangement of firewall and routers
  - Several different network configurations
    - Separate internal LAN from external Internet
    - Wall off subnetwork within an organization
      - Test networks, financial records, secret projects
    - Intermediate zone for web server, etc.
  - Personal firewall on end-user machine
- How does the firewall process data
  - Packet filtering router
  - Application-level gateway
    - Proxy for protocols such as ftp, smtp, http, etc.
  - Circuit-level gateway
  - Personal firewall also knows which application
    - E.g., disallow telnet connection from email client

TCP Protocol Stack

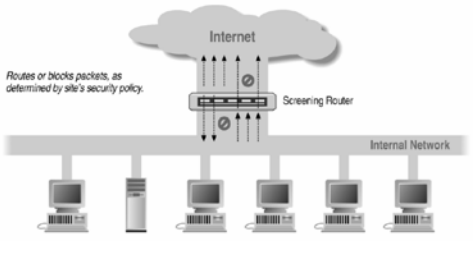


Transport layer provides *ports*, logical channels identified by number

Data Formats



Screening router for packet filtering



Packet Filtering

- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Examples
  - DNS uses port 53
    - No incoming port 53 packets except known trusted servers
- Issues
  - Stateful filtering
  - Encapsulation: address translation, …
  - Fragmentation

Packet filtering examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

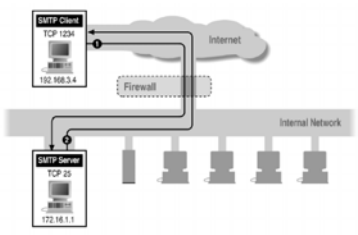
E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

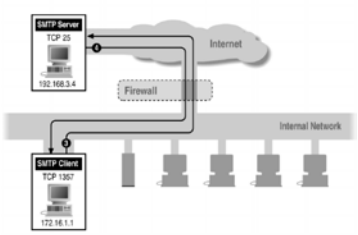
Port numbering

- TCP connection
  - Server port is number less than 1024
  - Client port is number between 1024 and 16383
- Permanent assignment
  - Ports <1024 assigned permanently
    - 20,21 for FTP 23 for Telnet
    - 25 for server SMTP 80 for HTTP
- Variable use
  - Ports >1024 must be available for client to make any connection
  - This presents a limitation for stateless packet filtering
    - If client wants to use port 2048, firewall must allow *incoming* traffic on this port
  - Better: stateful filtering knows outgoing requests

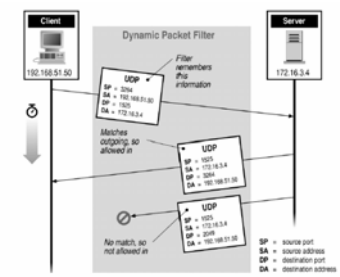
Filtering Example: Inbound SMTP



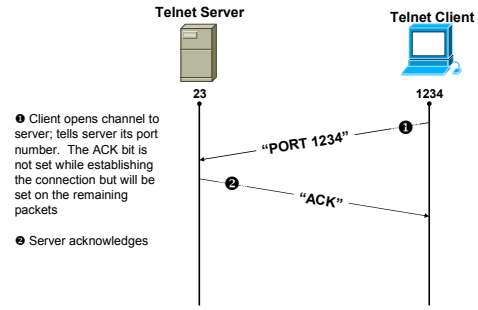
Filtering Example: Outbound SMTP



Stateful or Dynamic Packet Filtering



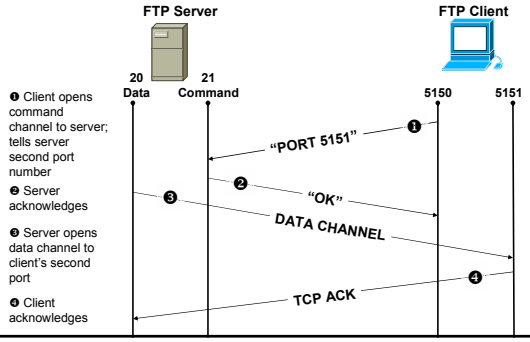
Telnet



❶ Client opens channel to server; tells server its port number. The ACK bit is not set while establishing the connection but will be set on the remaining packets

❷ Server acknowledges

FTP



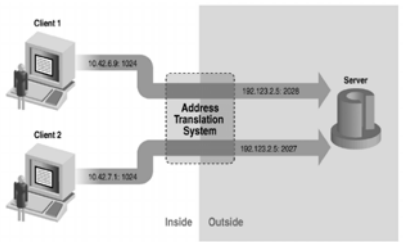
❶ Client opens command channel to server; tells server second port number

❷ Server acknowledges

❸ Server opens data channel to client's second port

❹ Client acknowledges

Network Address Translation (NAT) Port & Address Translation (PAT)



Normal Fragmentation

Abnormal Fragmentation

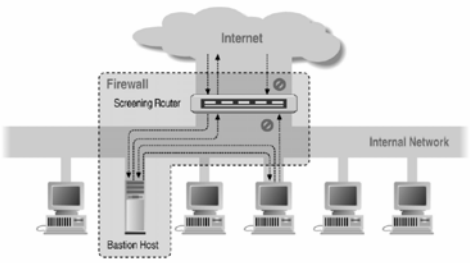
Application-level proxies

- Use "bastion host"
  - Computer running protocol stack
- Enforce policy for specific protocols
  - E.g., Virus scanning for SMTP
    - Need to understand MIME, encoding, Zip archives

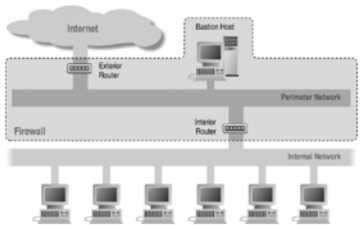
Bastion Host

- A secured system
  - Will interact/accepts data from the Internet
- Disable all non-required services; keep it simple
- Install/modify services you want
- Run security audit to establish baseline
- Connect system to network <- important
- Be prepared for the system to be compromised

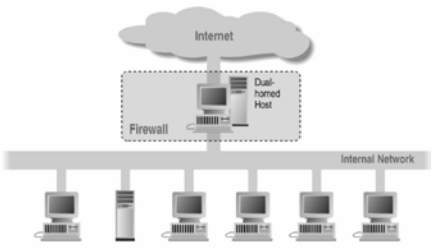
Screened Host Architecture



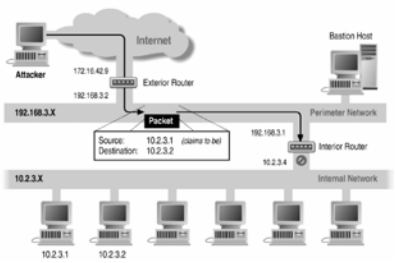
Screened Subnet Using Two Routers



Dual Homed Host Architecture



Source/Destination Address Forgery



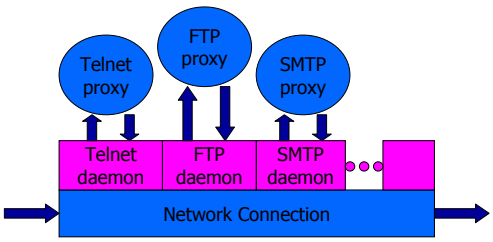
Firewall mechanism

- Firewall runs set of proxy programs
  - Proxies filter incoming, outgoing packets
  - All incoming traffic directed to firewall
  - All outgoing traffic appears to come from firewall
- Policy embedded in proxy programs
- Two kinds of proxies
  - Application-level proxies
    - Tailored to http, ftp, smtp, etc.
  - Circuit-level proxies
    - Decisions based on header information

Proxies

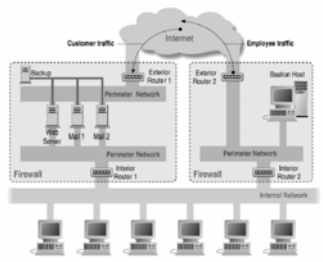
- Application level; dedicated proxy (HTTP)
- Circuit level; generic proxy
  - SOCKS
  - WinSock – almost generic proxy for Microsoft
- Some protocols are natural to proxy
  - SMTP (E-Mail)
  - NNTP (Net news)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)

Firewall architecture

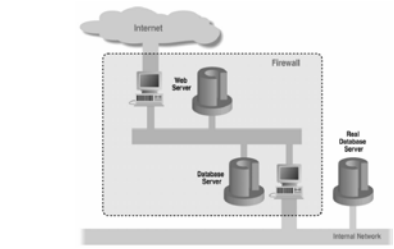


Daemon spawns proxy when communication detected ...

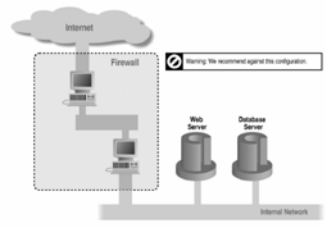
A Complex Firewall Setup



Web server, database on perimeter network



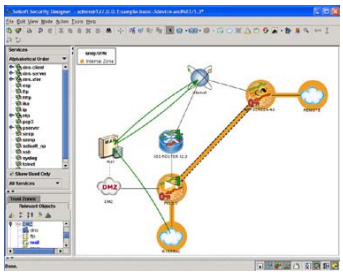
Web server, database on internal network



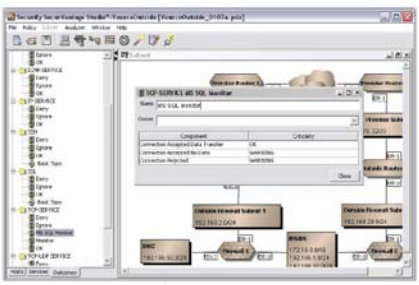
Not a good idea !!!

Configuration issues

Solsoft



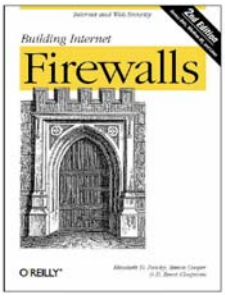
Securify



Problems with Firewalls

- They interfere with the Internet
- They don't solve the real problems
  - Buggy software
  - Bad protocols
- Generally cannot prevent Denial of Service
- Firewalls do not prevent insider attacks
- Are becoming more complicated
- Many commercial firewalls permit very, very complex configurations

Reference 1



Elizabeth D. Zwicky
Simon Cooper
D. Brent Chapman

Reference 2

William R Cheswick
Steven M Bellovin
Aviel D Rubin