CS155 Firewalls

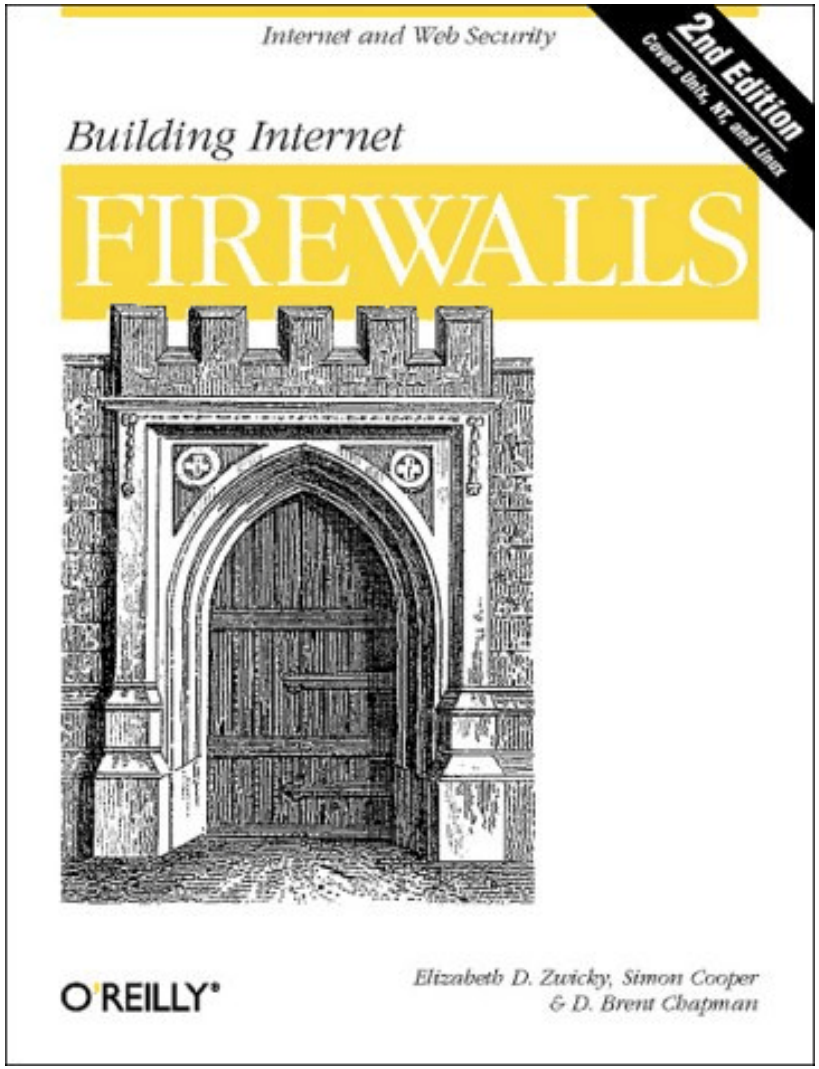
Simon Cooper <sc@sgi.com>

CS155 - Firewalls

23 May 2002

Plug! Building Internet Firewalls 2nd Edition, O'Reilly

Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman



What Is A Firewall?

- Literally? Prevents fire from spreading!
- The Castle Moat Analogy
  - Restricts access from the outside
  - Prevents attackers from getting too close
  - Restricts people from leaving
- Logically; a separator, a restrictor and an analyzer
- Rarely a single physical object
- Any place where internal and external data can meet

Why Firewalls?

- There are a lot of people on the Internet
- Millions of people together; bad things happen
- True for cities; it is true for the Internet
- Exchange of information; Education, Business Recreation, Social and Political
- Want to do something useful with your computer
- However; Unsolicited attention and bugs

Bugs, Bugs, Bugs

- All programs contain bugs
- Larger programs contain more bugs
- Network protocols contain design weaknesses and implementation flaws
- Careful (defensive) programming & protocol design is hard

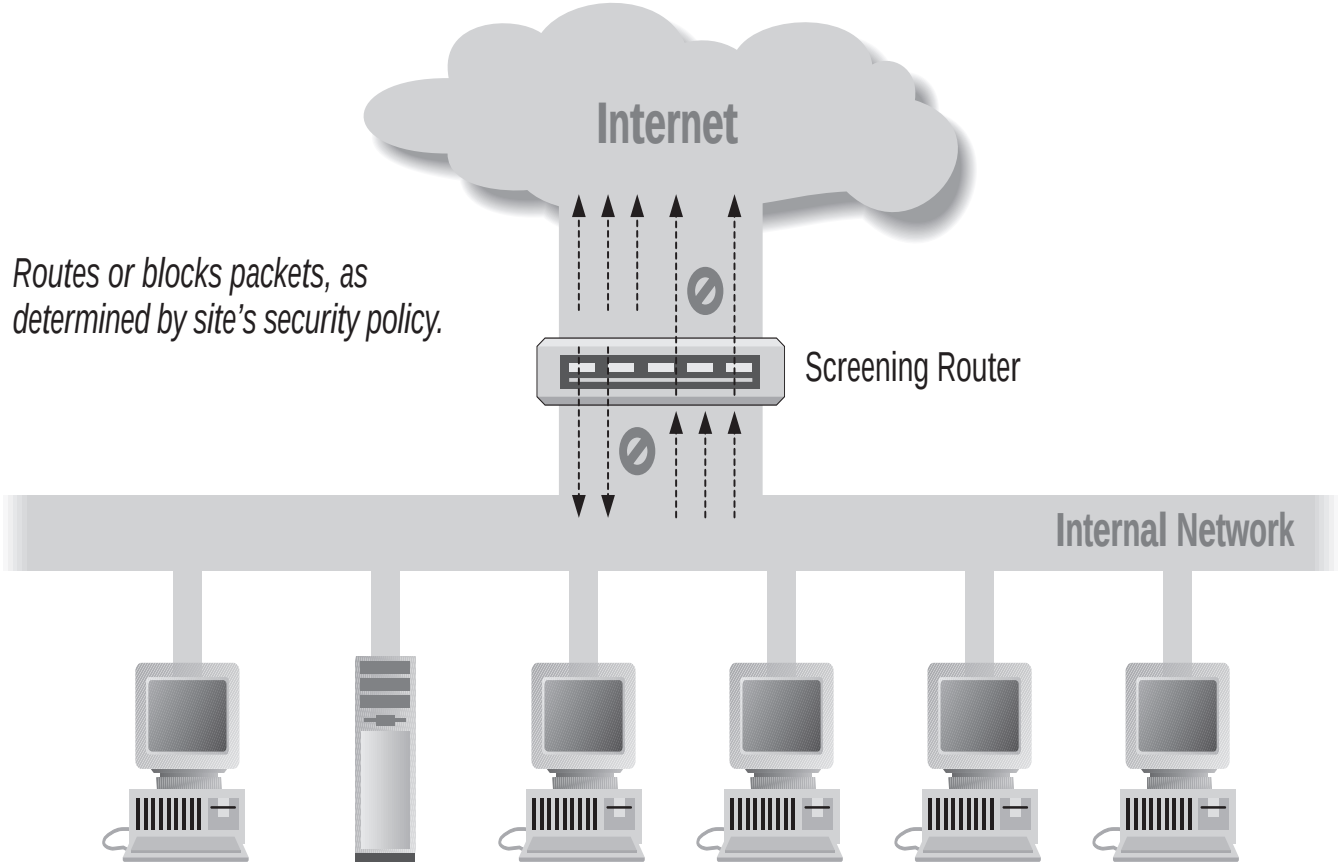
Where Do You Put A Firewall?

- Between insecure systems & the Internet
- To separate test or lab networks
- For networks with more sensitive data;
  - Financial records
  - Student grades
  - Secret Projects
- Partner or joint venture networks

Firewall Design & Architecture Issues

- Least Privilege
- Defense in Depth
- Choke Point
- Weakest Link
- Fail-Safe Stance
- Universal Participation
- Diversity of Defense
- Simplicity

Firewall Architectures



Using A Screening Router to do Packet Filtering

Packet Filtering
IP Packet Header

version	length	type of service	16-bit total length (in bytes)	
16-bit identification			flags	13-bit fragmentation offset
8-bit Time To Live		8-bit protocol	16-bit header checksum	
32-bit source IP address				
32-bit destination IP address				
IP options (if any)				

Packet Filtering
UDP Packet Structure

version	length	type of service	16-bit total length (in bytes)	
16-bit identification			flags	13-bit fragmentation offset
8-bit Time To Live		8-bit protocol	16-bit header checksum	
32-bit source IP address				
32-bit destination IP address				
IP options (if any)				
16-bit source port number			16-bit destination port number	
16-bit UDP length			16-bit UDP checksum	
Data (if any)				

Packet Filtering
TCP Packet Structure

version	length	type of service	16-bit total length (in bytes)
16-bit identification		flags	13-bit fragmentation offset
8-bit Time To Live	8-bit protocol		16-bit header checksum
32-bit source IP address			
32-bit destination IP address			
IP options (if any)			
16-bit source port number			16-bit destination port number
32-bit sequence number			
32-bit acknowledgement number			
h length	reserved	Flags	16-bit window size
16-bit TCP checksum			16-bit urgent pointer

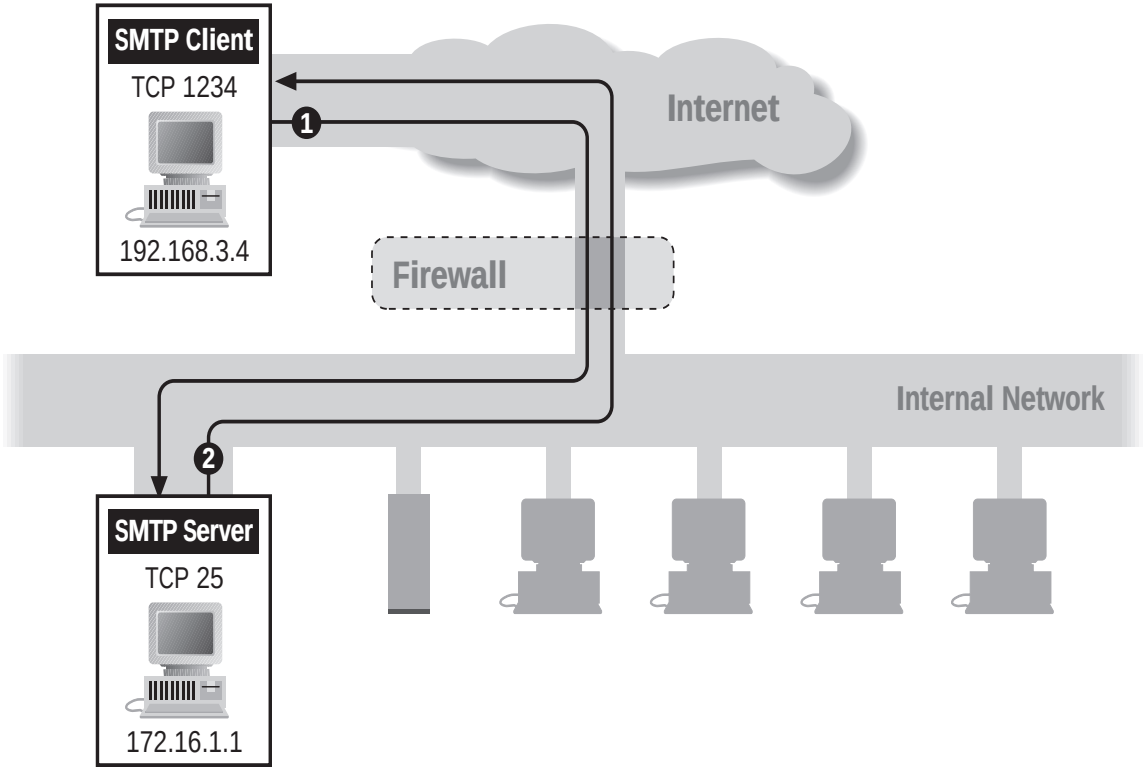
Packet Filtering Summary

- IP Source Address
- IP Destination Address
- Protocol (TCP, UDP, ICMP, etc.)
- TCP or UDP Source & Destination Ports
- TCP Flags (SYN, ACK, etc.)
- ICMP message type
- Packet Size

Router Knowledge

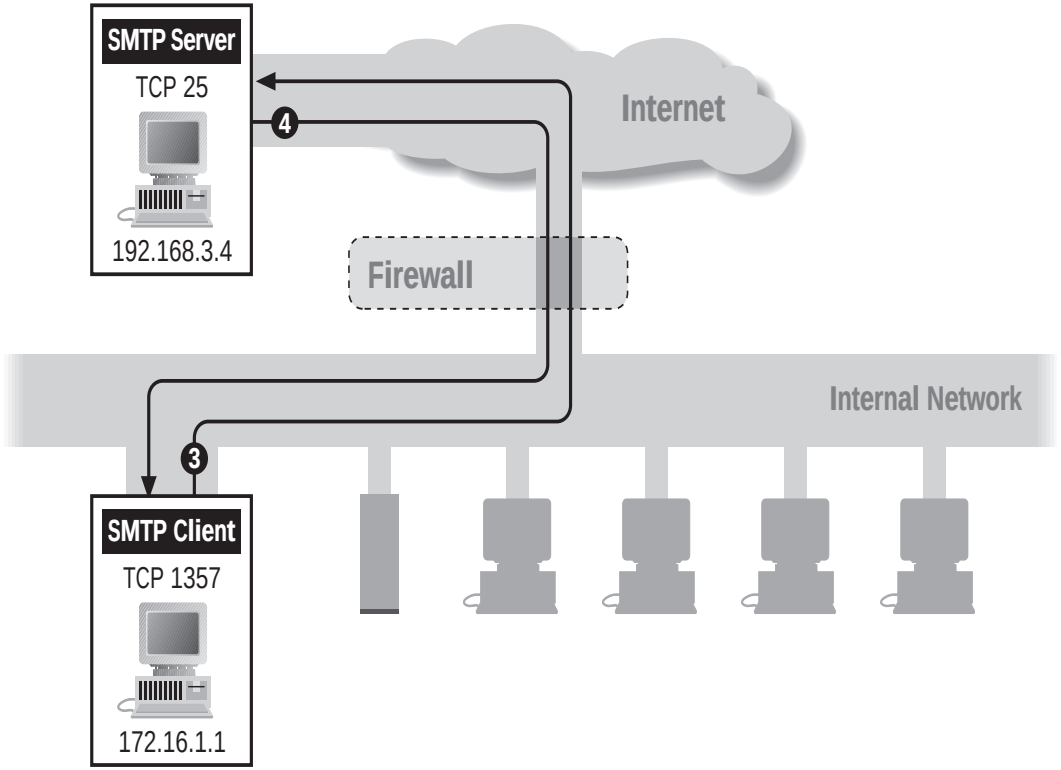
- Interface packet arrives on
- Interface packet will go out
- Is the packet in response to another one?
- How many packets have been seen recently?
- Is the packet a duplicate?
- Is the packet an IP fragment?

Filtering Example Inbound SMTP



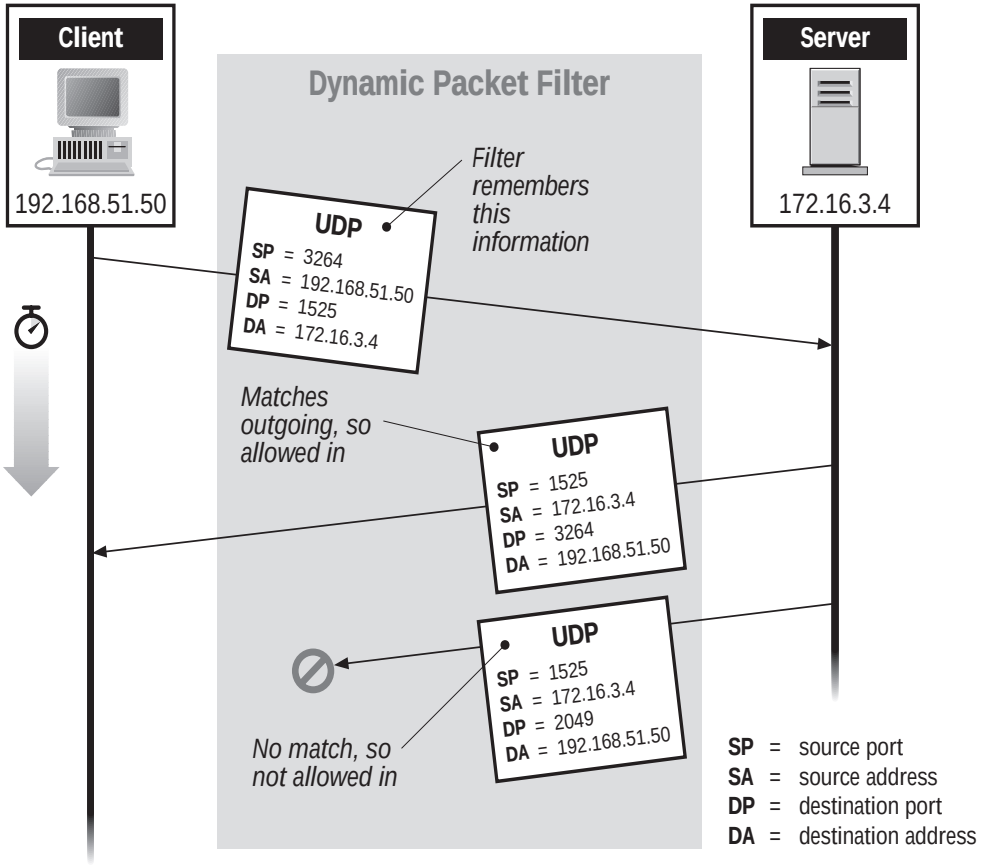
Packet	Direction	Source Address	Dest Address	Protocol	Dest Port
1	In	192.168.3.4	172.16.1.1	TCP	25
2	Out	172.16.1.1	192.168.3.4	TCP	1234

Filtering Example Outbound SMTP

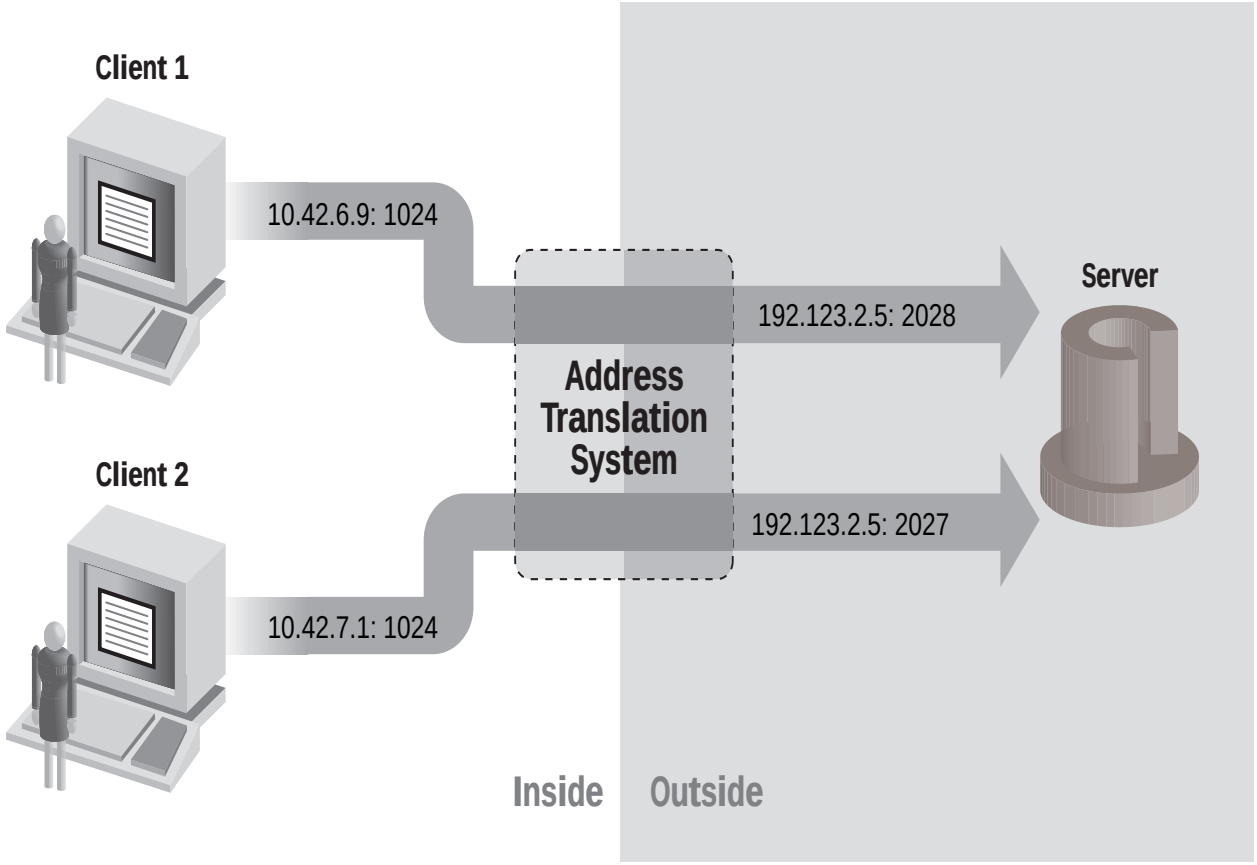


Packet	Direction	Source Address	Dest Address	Protocol	Dest Port
3	Out	172.16.1.1	192.168.3.4	TCP	25
4	In	192.168.3.4	172.16.1.1	TCP	1357

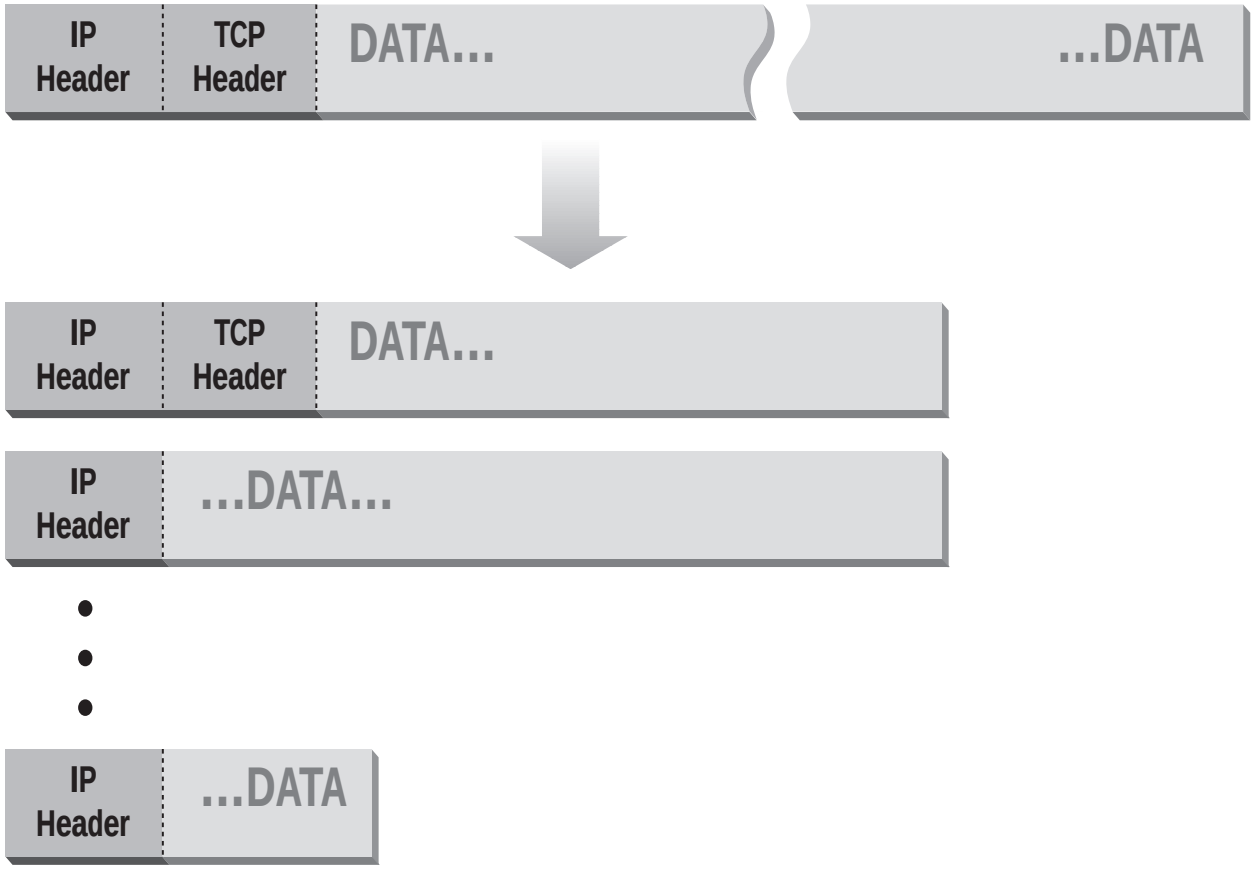
Stateful or Dynamic Packet Filtering



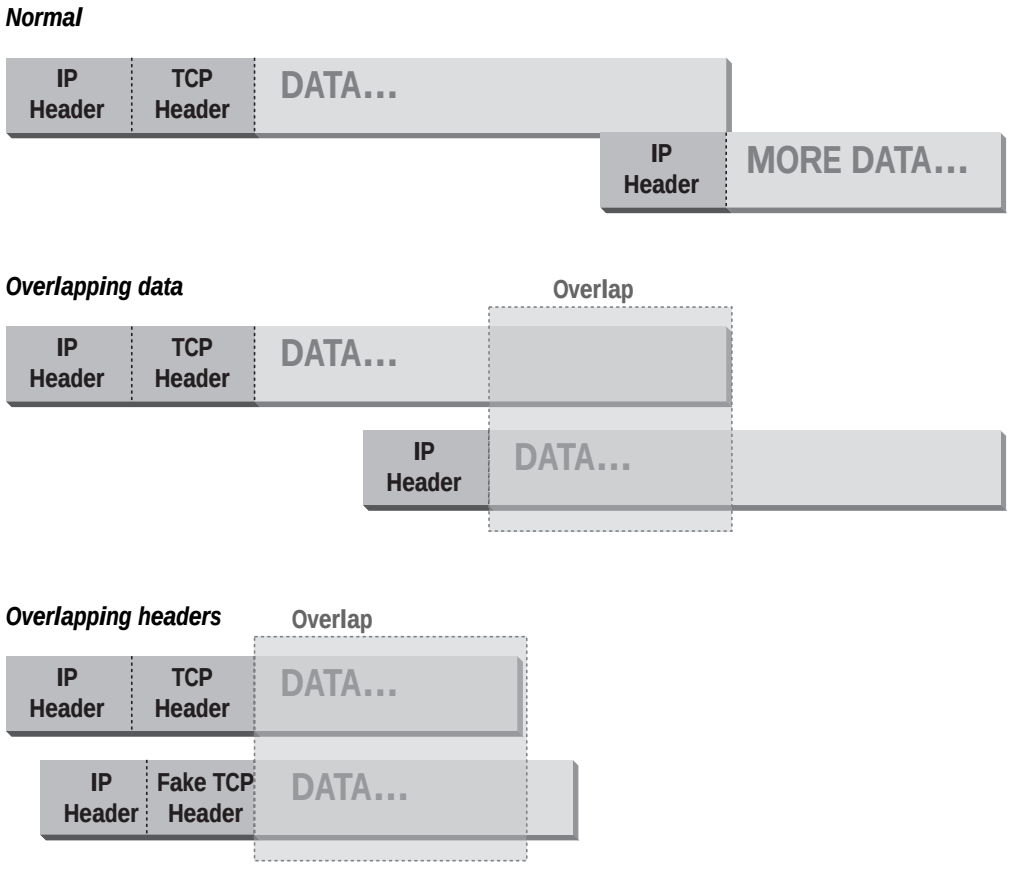
Network Address Translation (NAT) Port and Address Translation (PAT)



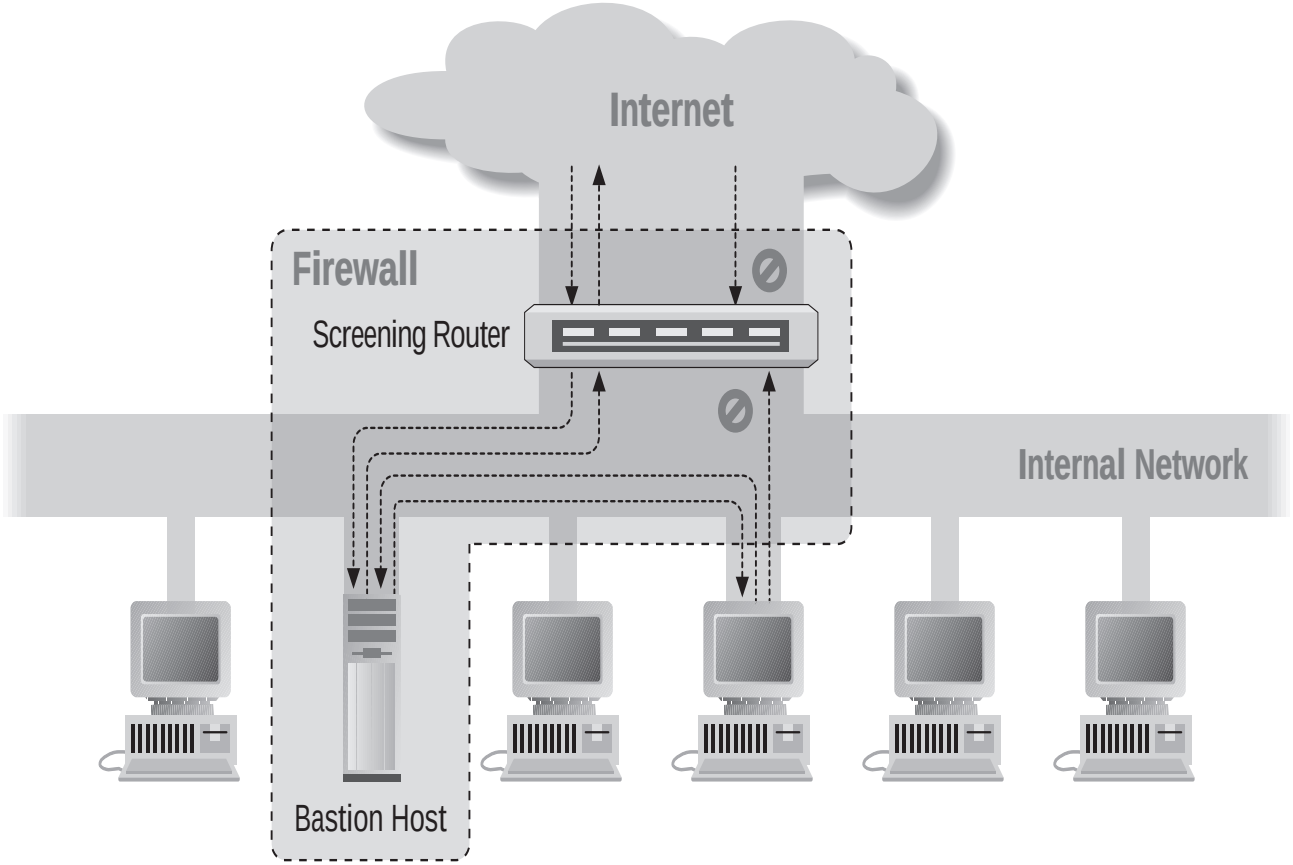
Normal Fragmentation



Abnormal Fragmentation



Firewall Architectures

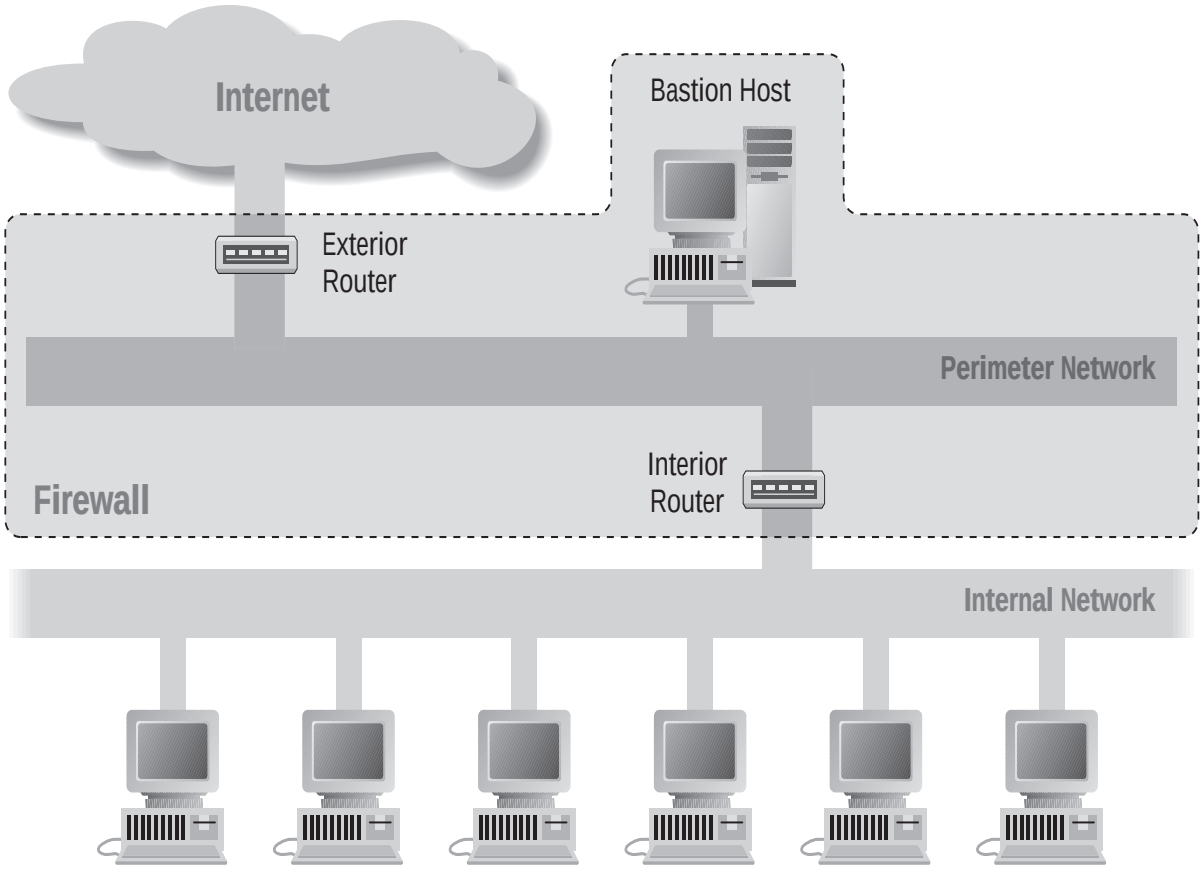


Screened Host Architecture

Bastion Host

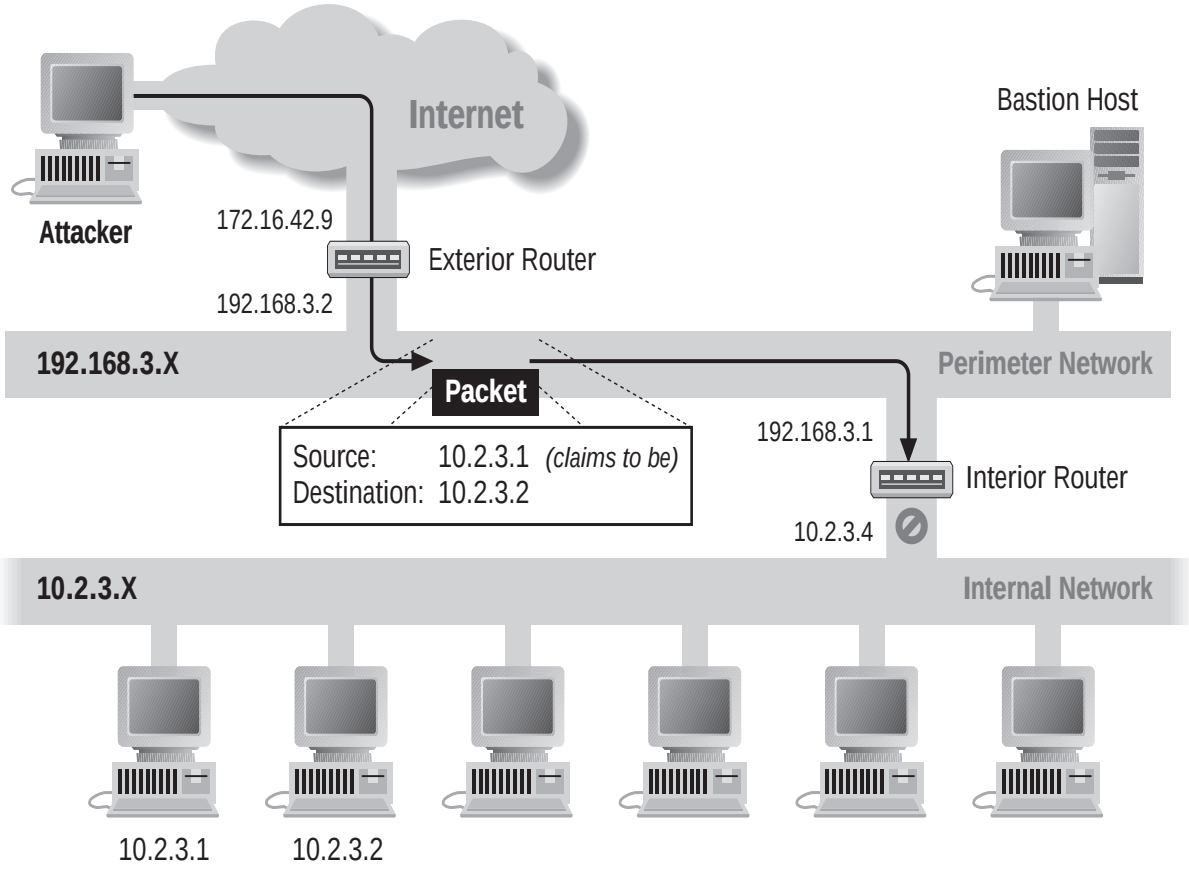
- A secured system
- Disable all non-required services; keep it simple
- Install/modify services you want
- Run security audit to establish baseline
- Connect system to the network
- Be prepared for system to be compromised

Firewall Architectures



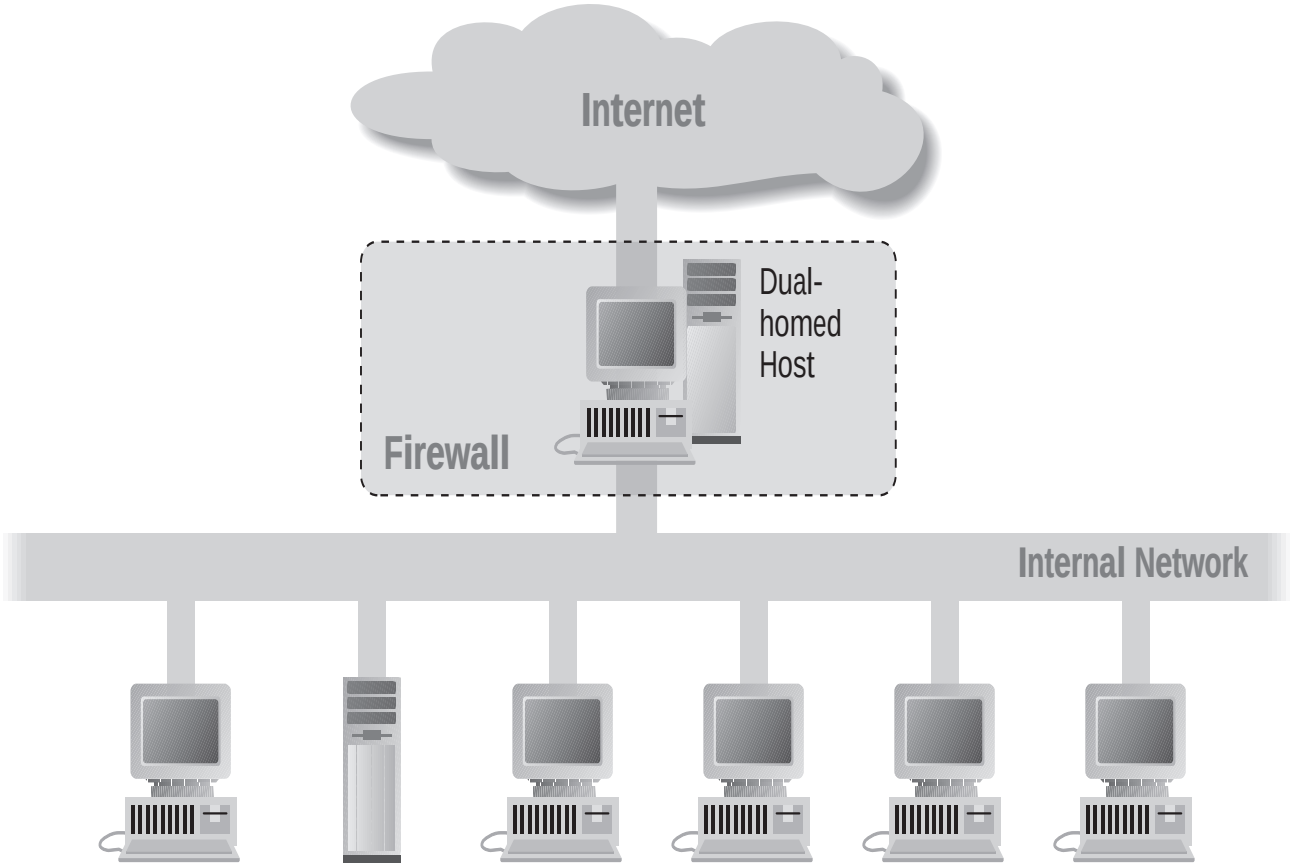
Screened Subnet Architecture Using Two Routers

Firewall Architectures



Source/Destination Address Forgery

Firewall Architectures

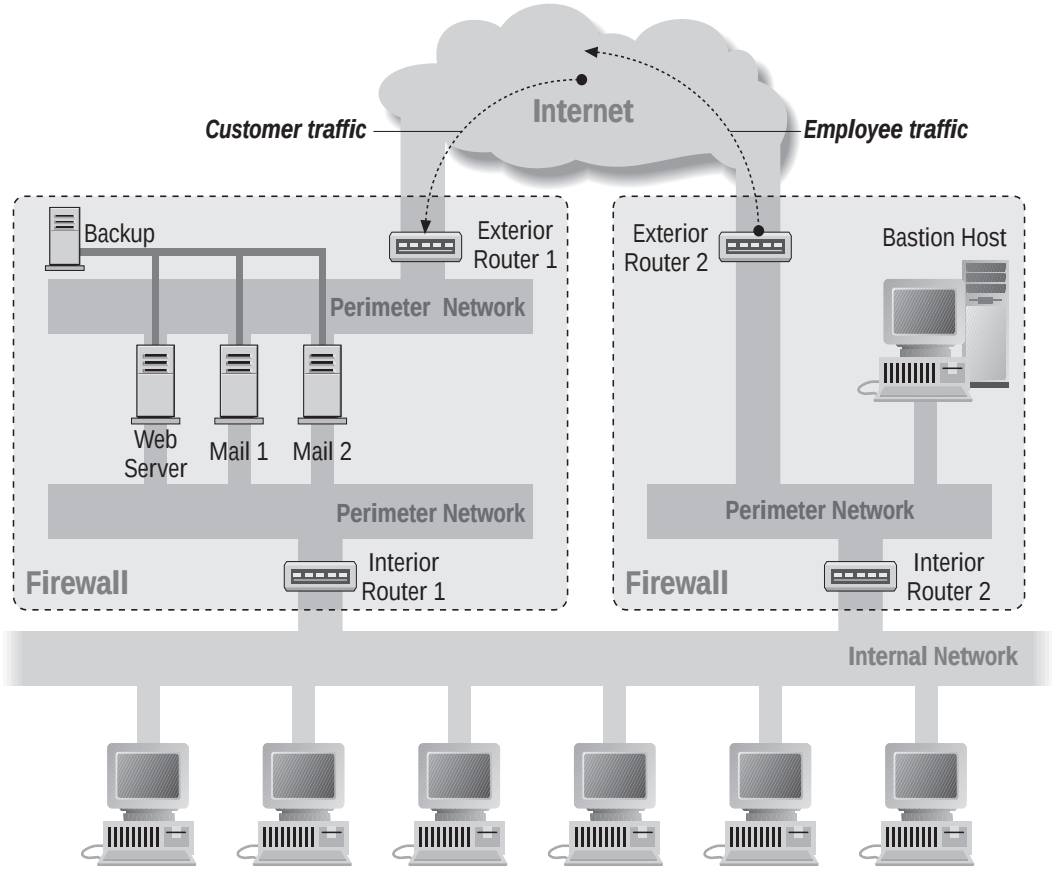


Dual Homed Host Architecture

Proxies

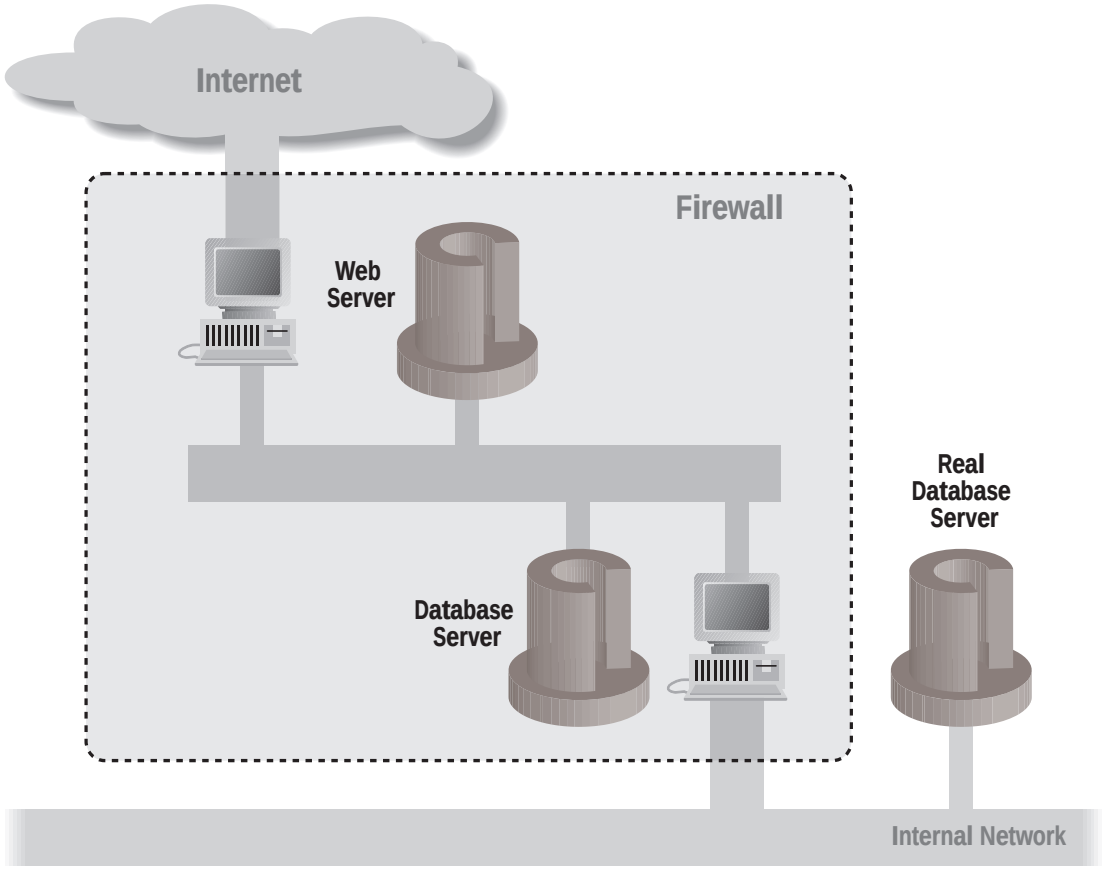
- Application level; Dedicated proxy
- Circuit level; “generic proxy”
- Some protocols are natural to proxy
  - SMTP (E-Mail)
  - NNTP (Netnews)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)
- SOCKS - a generic proxy
- WinSock - almost generic proxy for Microsoft

Firewall Architectures



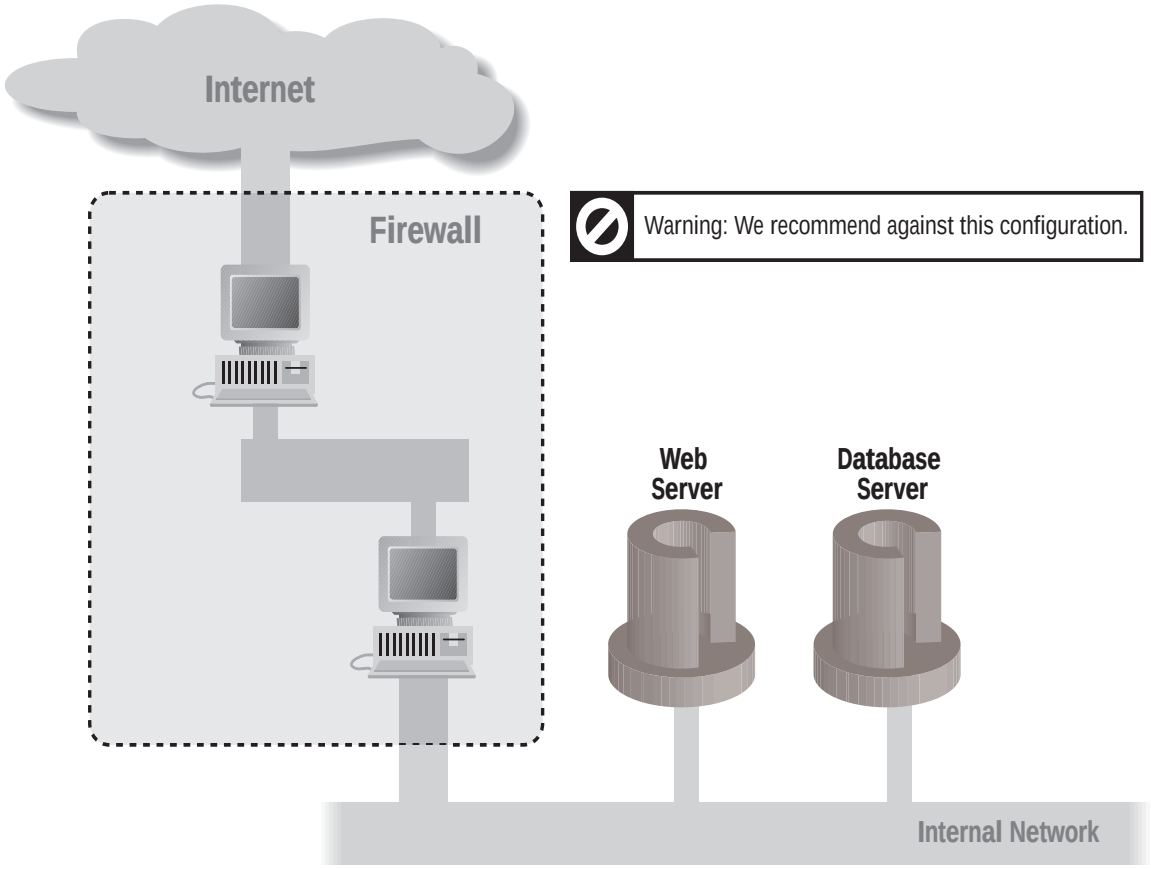
An Intricate Firewall Setup

Firewall Architectures



A web server using a database on a perimeter network

Firewall Architectures



A web and database server on an internal network

Problems With Firewalls

- They interfere with the Internet
- They don’t solve the real problems;
  - buggy software
  - bad protocols
- Denial of Service
- They are becoming more complicated
- Many commercial firewalls permit very complex configurations

CS155 - Firewalls
Simon Cooper <sc@sgi.com>

Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman