CS155 - Firewalls

Simon Cooper <sc@sgi.com>

CS155 – Firewalls
22 May 2003

Why Firewalls?

- Need for the exchange of information; education, business, recreation, social and political
- Need to do something useful with your computer
- Drawbacks; unsolicited attention and bugs

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
- With the Internet...
  - Everyone is in your backyard!
  - You can be scoped out at any time from anywhere
  - The community discourages neighborhood watch like activities (a hot potato!)

Bugs, Bugs, 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**

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 <- Important!!

What is a Firewall?

- Logically
  - A separator, a restrictor and an analyzer
- Rarely a single physical object!
- Practically any place where internal and external data can meet

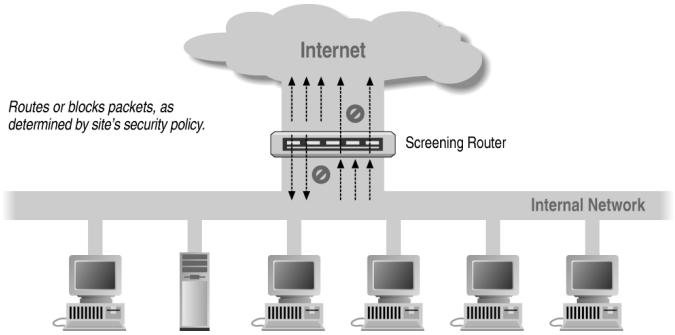
Where do you put a Firewall?

- 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 (very important)
- Choke point
- Weakest links
- Fail-safe stance
- Universal participation
- Diversity of defense
- Simplicity

Firewall Architectures



Using a Screening Router to do Packet Filtering

Packet Filtering: IPv4 Packet Header

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

http://www.faqs.org/rfcs/rfc760.html

Packet Filtering: UDP Packets

```
 0      7 8     15 16    23 24    31
+--------+--------+--------+--------+
|     Source      |   Destination   |
|      Port       |      Port       |
+--------+--------+--------+--------+
|                 |                 |
|     Length      |    Checksum     |
+--------+--------+--------+--------+
|
|          data octets ...
+---------------- ...

        User Datagram Header Format
```

http://www.faqs.org/rfcs/rfc768.html

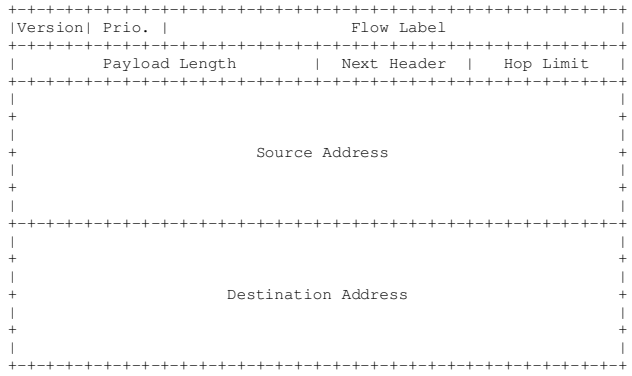
Packet Filtering: TCP packet structure

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|E|R|S|F|                               |
| Offset| Reserved  |R|C|O|S|Y|I|            Window             |
|       |           |G|K|L|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                    TCP Header Format
```

http://www.faqs.org/rfcs/rfc761.html

Packet Filtering: Ipv6 Packet Header



http://www.faqs.org/rfcs/rfc1883.html

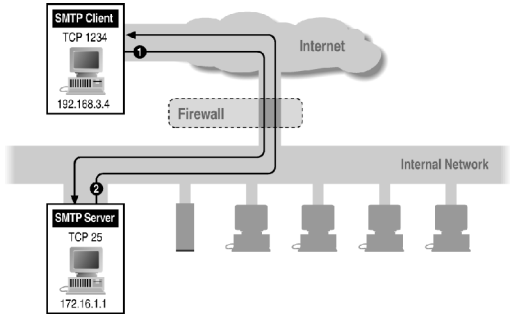
Packet Filtering: Summary

- IP Source Address
- IP 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
- Packet size
- Fragmentation

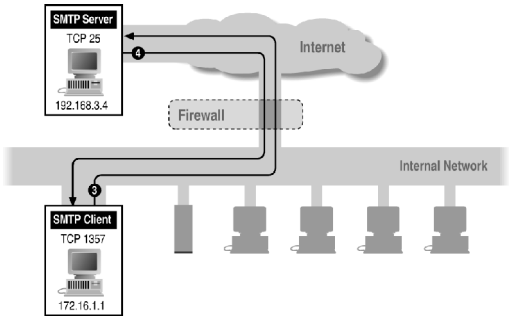
Router Knowledge

- Interface packet arrives on
- Interface a 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?

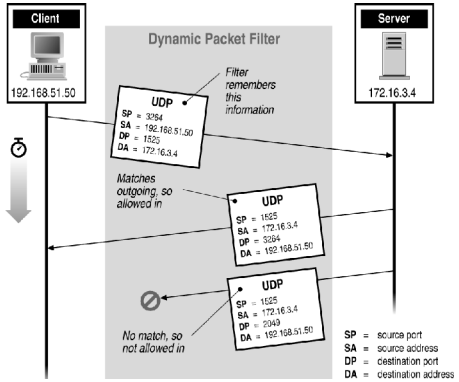
Filtering Example: Inbound SMTP



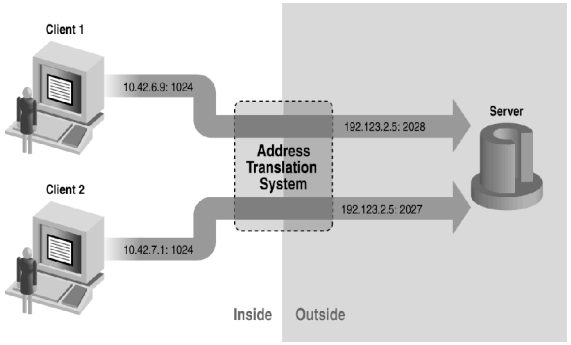
Filtering Example: Outbound SMTP



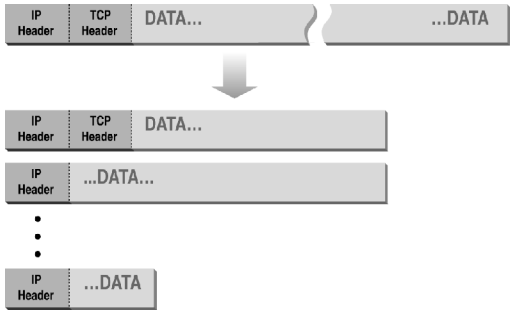
Stateful or Dynamic Packet Filtering



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

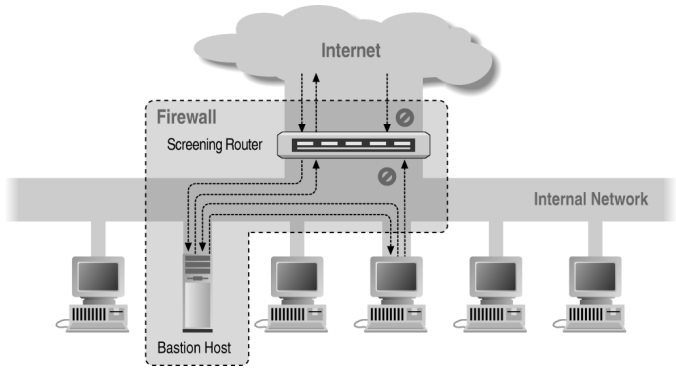


Normal Fragmentation



Abnormal Fragmentation

Firewall Architectures

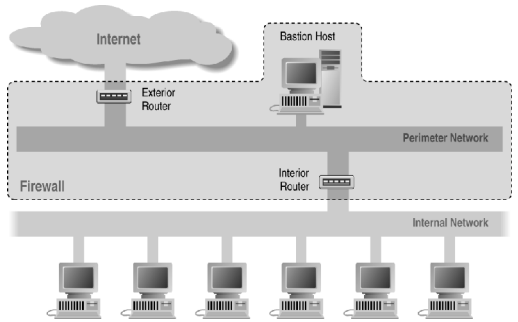


Screened Host Architecture

Bastion Host

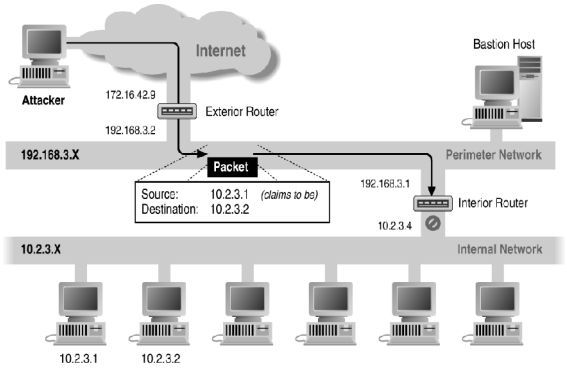
- A secured system (it will interact/accepts data from the Internet)
- Disable all non-required services; keep it simple
- Install/modify services you want
- Run security audit to establish baseline
- Connect system to network <- important
- Be prepared for the system to be compromised

Firewall Architectures



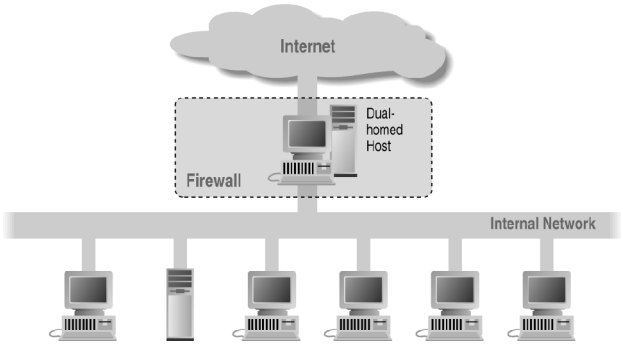
Screened Subnet Architecture Using Two Routers

Firewall Architectures



Source/Destination Address Forgery

Firewall Architectures

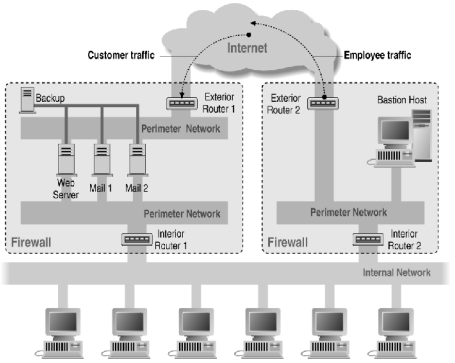


Dual Homed Host Architecture

Proxies

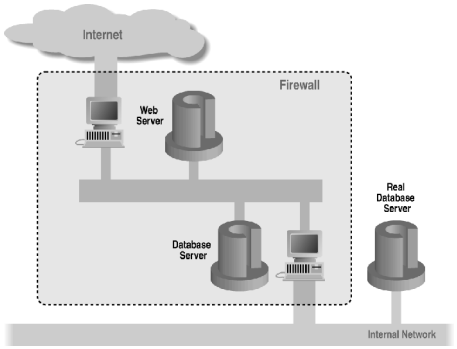
- Application level; dedicated proxy (HTTP)
- Circuit level; generic proxy
  - SOCKS
  - WinSock – almost generic proxy for Microsoft
- Some protocols are "natural" to proxy
  - SMTP (E-Mail)
  - NNTP (Net news)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)

Firewall Architectures



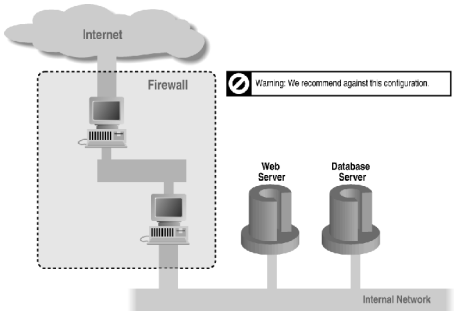
A Complex Firewall Setup

Firewall Architectures



A web server using a database on a perimeter network

Firewall Architectures

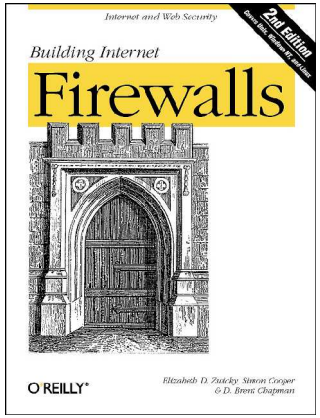


A web server and database server on an internal network

Problems with Firewalls

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

Elizabeth D. Zwicky, Simon Cooper
D. Brent Chapman



Questions?

Simon Cooper <sc@sgi.com>