Firewalls

First notions
Types of outsider attacks

- Intrusions
  - Data compromise
    - confidentiality, integrity
  - Web defacement
    - availability, reputation
  - Zombie recruitment
    - DOS, liability risk
- Denial of Service Attacks
- Sniffing/Information theft
Why firewalls?

- Against firewalls:
  - Host security measures are effective
  - Firewalls increase Internet latency, and impose arbitrary limitations on legitimate Internet usage

- Against host-based security only:
  - administratively hard to enforce consistency
  - firewalls may actually increase internal available bandwidth by blocking bad traffic

- Scalability: network vs. host security model
Internet Firewalls

Firewalls can be configured in many different ways. A common configuration is along the gateway path to the Internet.
Firewalls can

- Enforce security policies to decide which traffic to allow and to not allow through the fire-walled channel
- Log security-related information
- Reduce the visibility of the network
Firewalls cannot

- Prevent against previously unknown attack types
- Protect against insiders/connections that do not go through it.
- Provide full protection against viruses.
Services typically protected

- HTTP/HTTPS
- FTP
- SSH
- SMTP
- DNS
Firewall Configurations
Single-Box Architectures

- Simple to manage, available from vendors
- Single point-of-failure, no defense-in-depth
- Types:
  - Screening Router
  - Dual-homed host
Screening Router

Routes or blocks packets, as determined by site’s security policy.
Dual-Homed Host

Fair-use notice: All images in this presentation are copyrighted property, extracted from Zwicky, Cooper, and Chapman's Building Internet Firewalls, O'Reilly (2002)
Screened Host Architecture
Screened Subnet Architectures

● Adds an extra layer of security to screened host
  ● Perimeter network isolates internal network from Internet
  ● Components:
    ● Perimeter network
    ● bastion host
    ● internal router
    ● external router
Screened network
Services on the Bastion Host

- Incoming connections from the Internet:
  - DNS queries
  - FTP download queries
  - Incoming mail (SMTP) sessions
- Outgoing connections protected either by:
  - Packet filtering (direct access to the Internet via screening routers)
  - Proxy services on bastion host(s)
Split-screened subnet
Multiple Internet Connections

copyrighted property, extracted from Zwicky, Cooper, and Chapman's Building Internet Firewalls, O'Reilly (2002)
Variations

- For high performance, use multiple bastion hosts
- Ok to merge a bastion host with an external router
- Not Ok to merge a bastion host with an internal router
- Bad to have multiple interior routers on the same perimeter network
Internal Firewalls