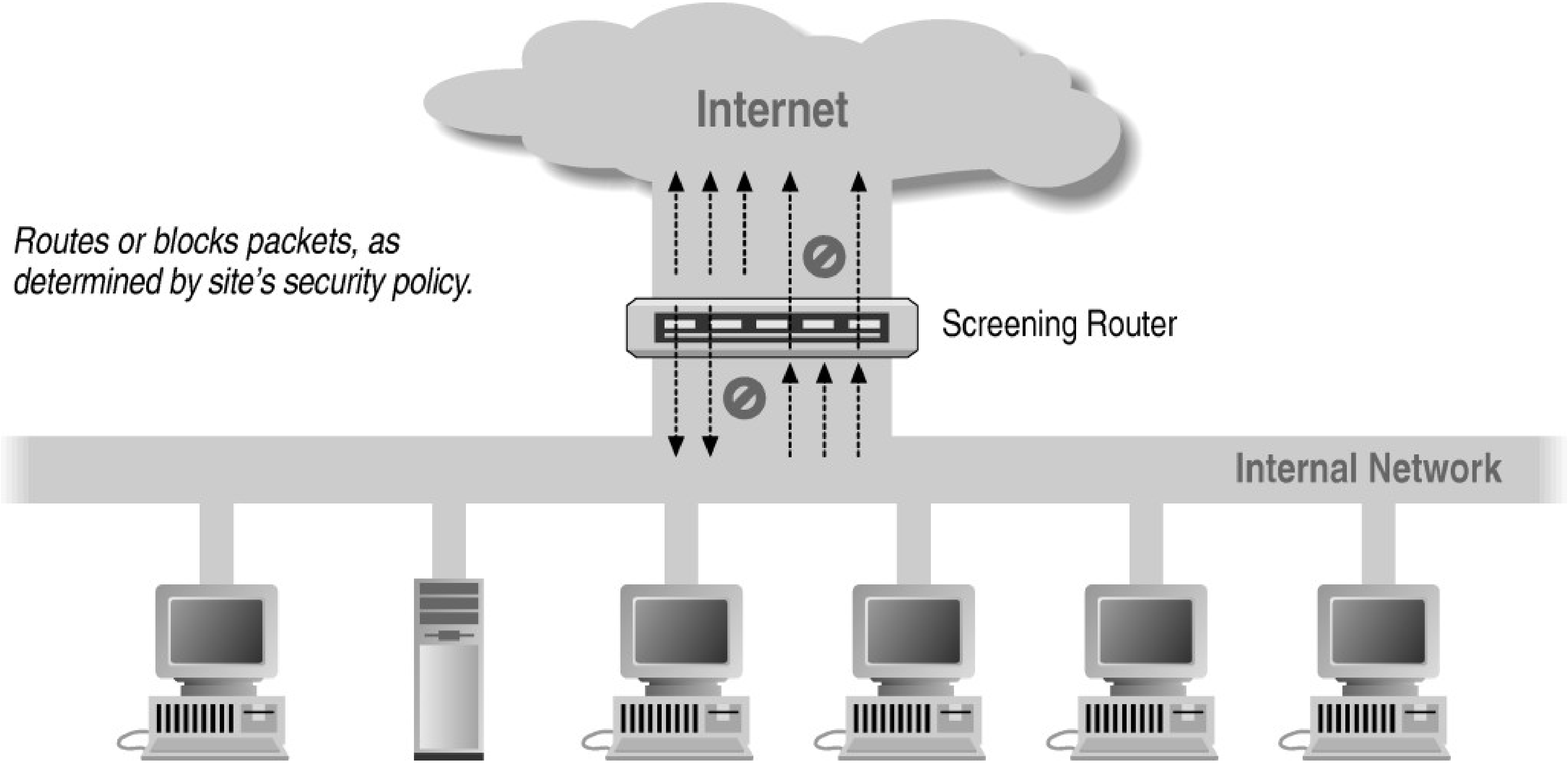
Screening router (ACL-based)

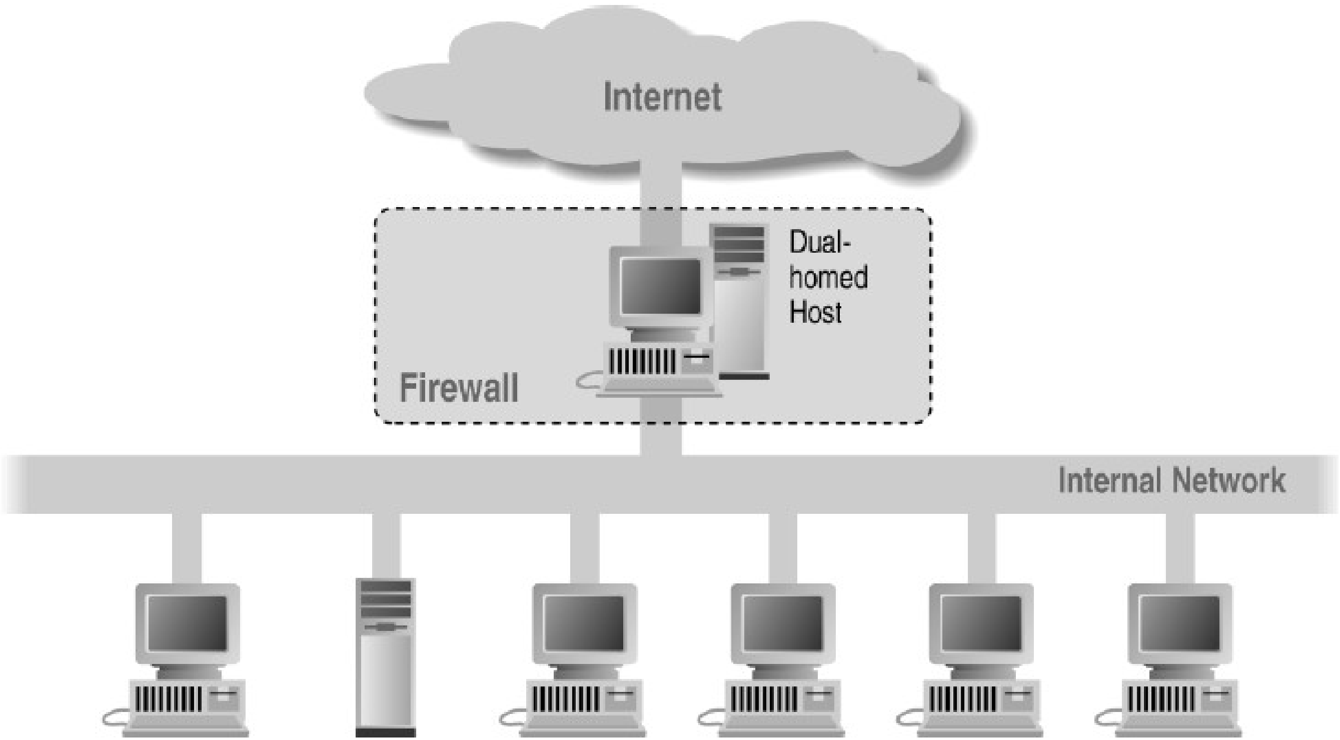


Internet
Routes or blocks packets, as determined by site's security policy.
Screening Router
Internal Network

Network Access Control Lists

- List the rights for accessing/using networks
  - Extensively used in switches, routers and firewalls
- Usually distinguish between incoming and outgoing traffic, per interface/port
  - Ex: lists of IP addresses that can send packets to an interface/port
- Stateless: every packet is treated independently, without any knowledge of what has come before

Dual-homed host



Bastion host

- Hardened computer used to deal with all traffic coming to a protected network from outside
  - Hardening is the task of reducing or removing vulnerabilities in a computer system:
    - Shutting down unused or dangerous services
    - Strengthening access controls on vital files
    - Removing unnecessary accounts and permissions
    - Using "stricter" configurations for vulnerable components, such as DNS, sendmail, FTP, Apache, Tomcat, etc.
- Specially suitable for use as Application Proxy Gateways

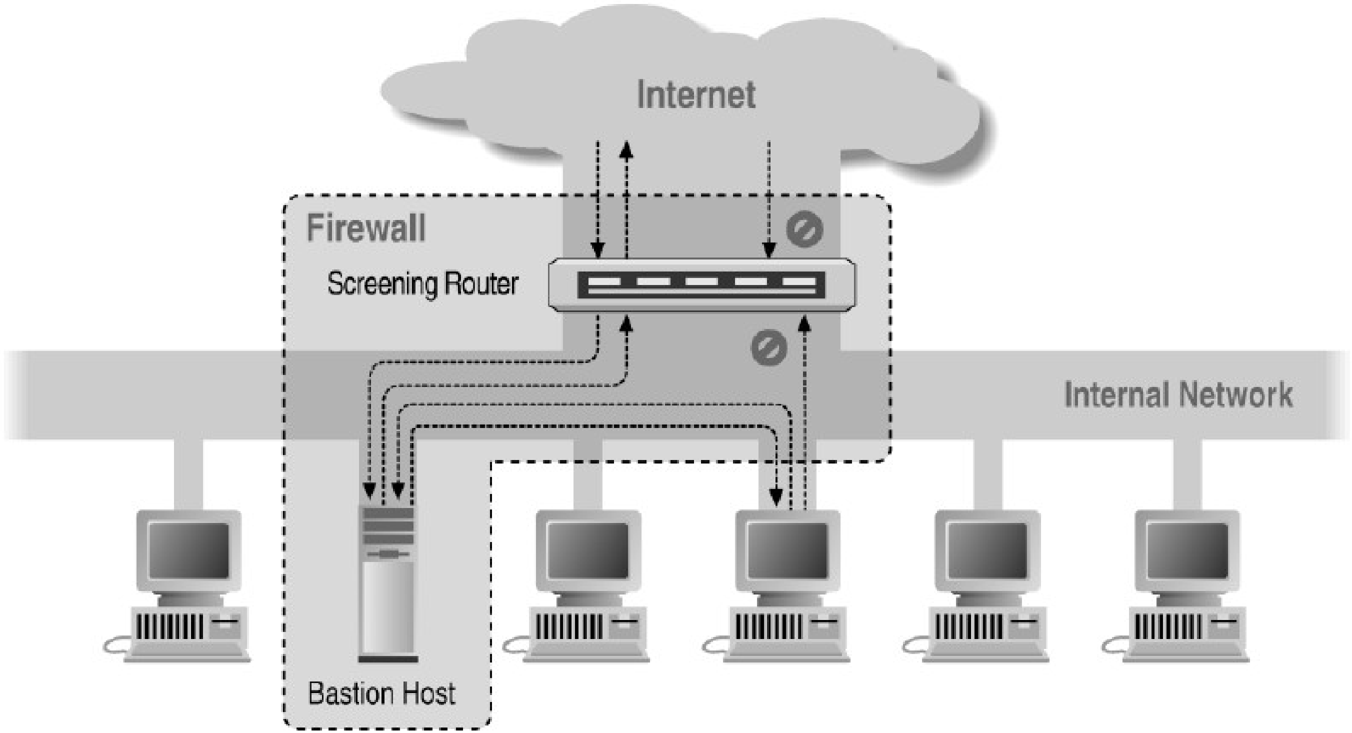
What is a DMZ

- DMZ (demilitarized zone)
  - Computer host or small network inserted as a “neutral zone” between a company’s private network and the outside public network
  - Network construct that provides secure segregation of networks that host services for users, visitors, or partners
- DMZ use has become a necessary method of providing a multilayered, **defense-in-depth** approach to security
- Reduce and regulate the access to internal (private) components of the IT system

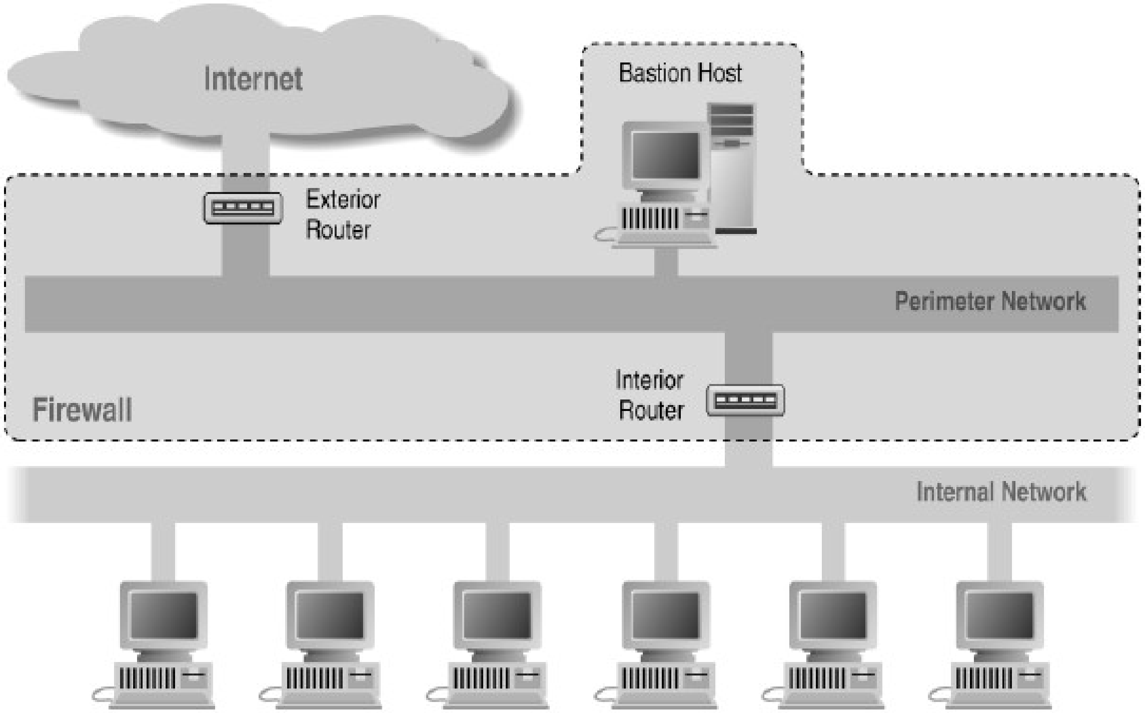
Defense in depth

- A security approach in which IT systems are protected using **multiple overlapping** systems
  - Add redundancy to the defensive measures
  - Aim to remove the single point of failure
  - Find the right balance between complexity and multiplicity of defense measures
- In order to compromise the system, an attacker has to find multiple vulnerabilities, in different components

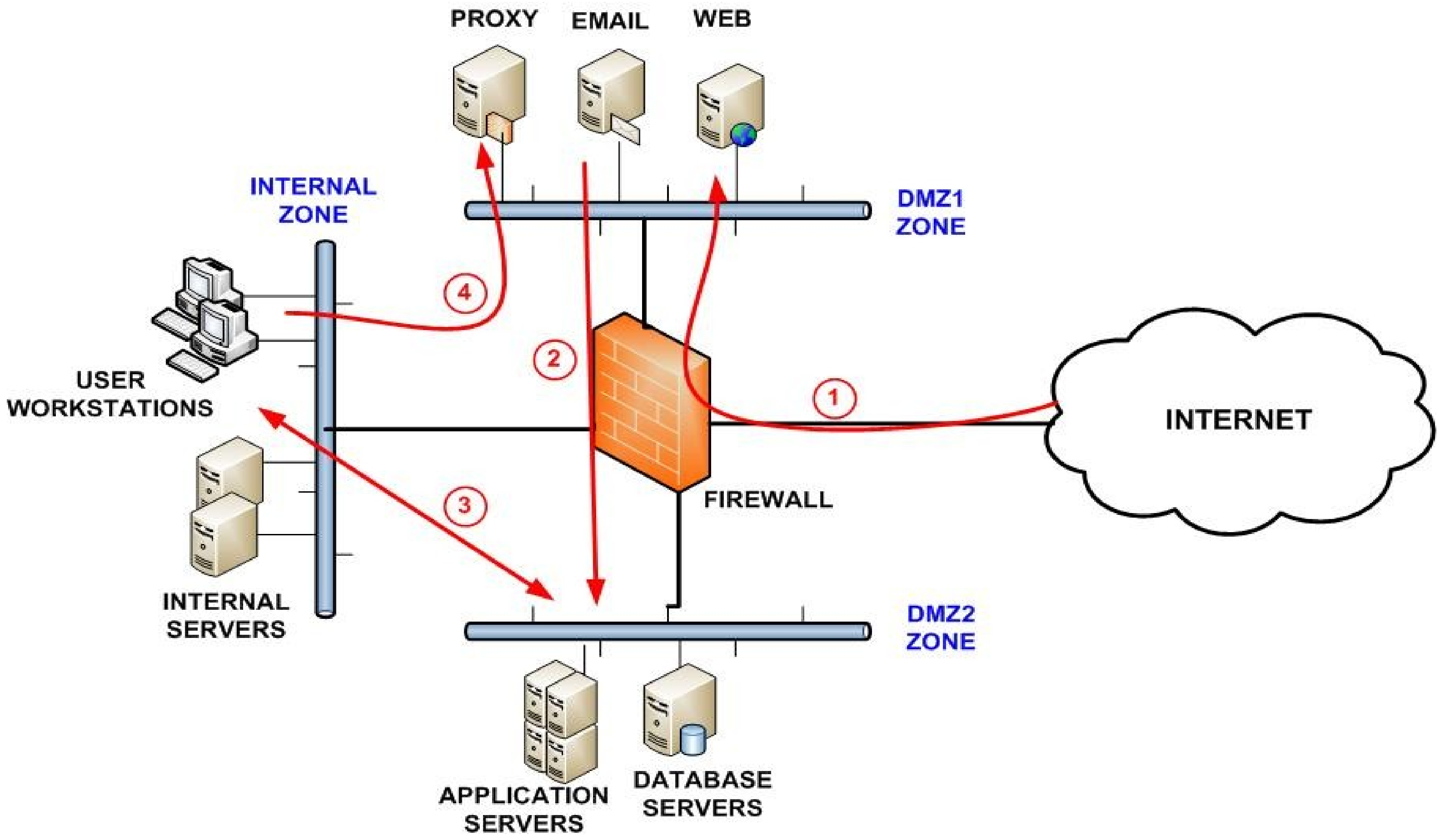
DMZ as a screened Host



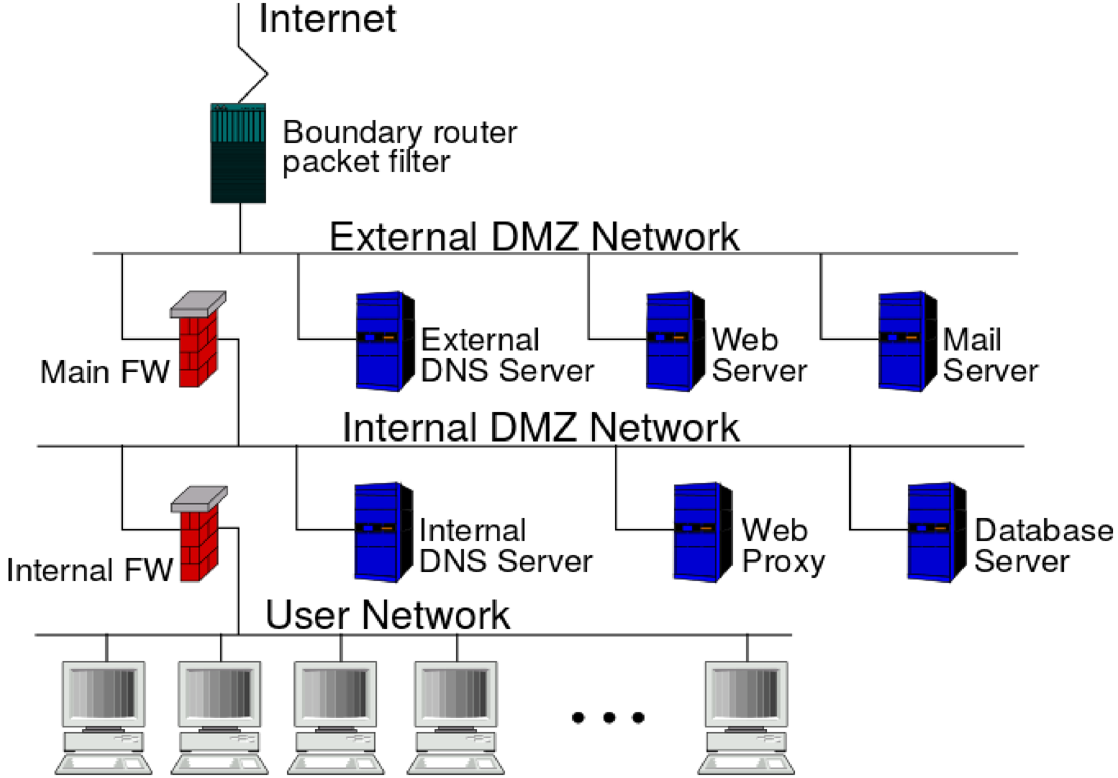
Screened Subnet Using Two Routers/Firewalls



DMZ to segment the network

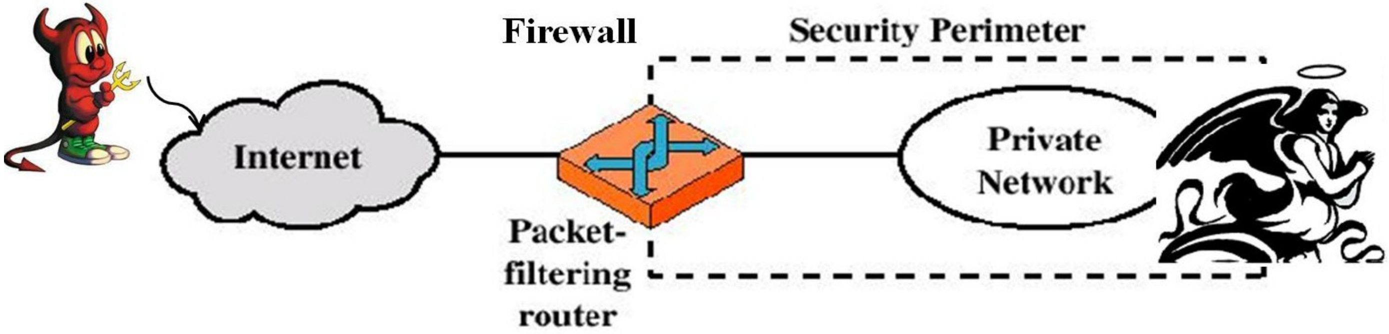


Security in depth: split DMZ



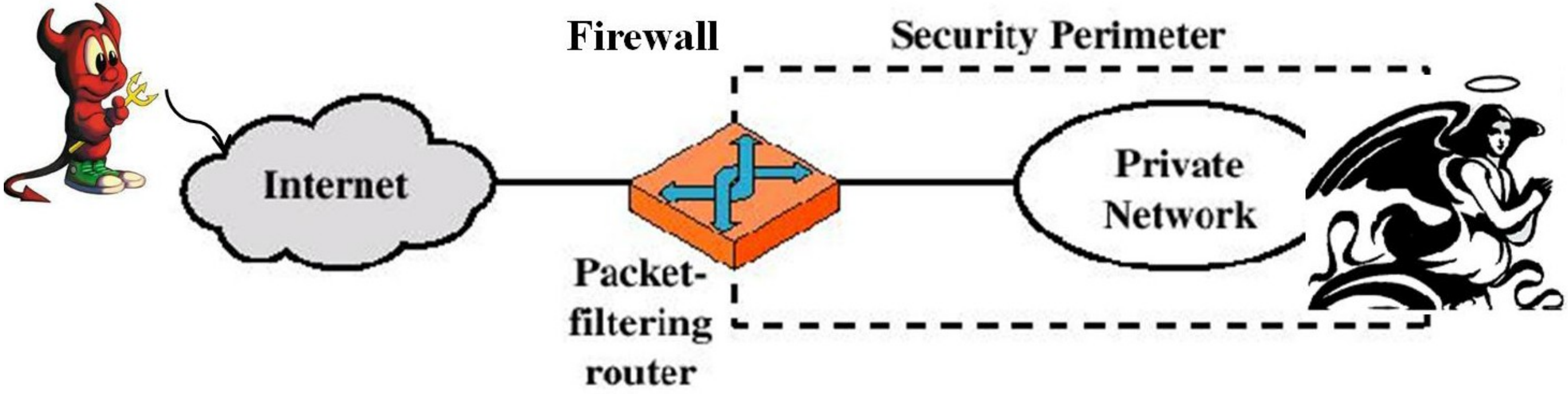
A simple plan for network security

- Use a firewall to filter ingoing and outgoing traffic between “your” network (or individual PC) and the Internet



Assumptions

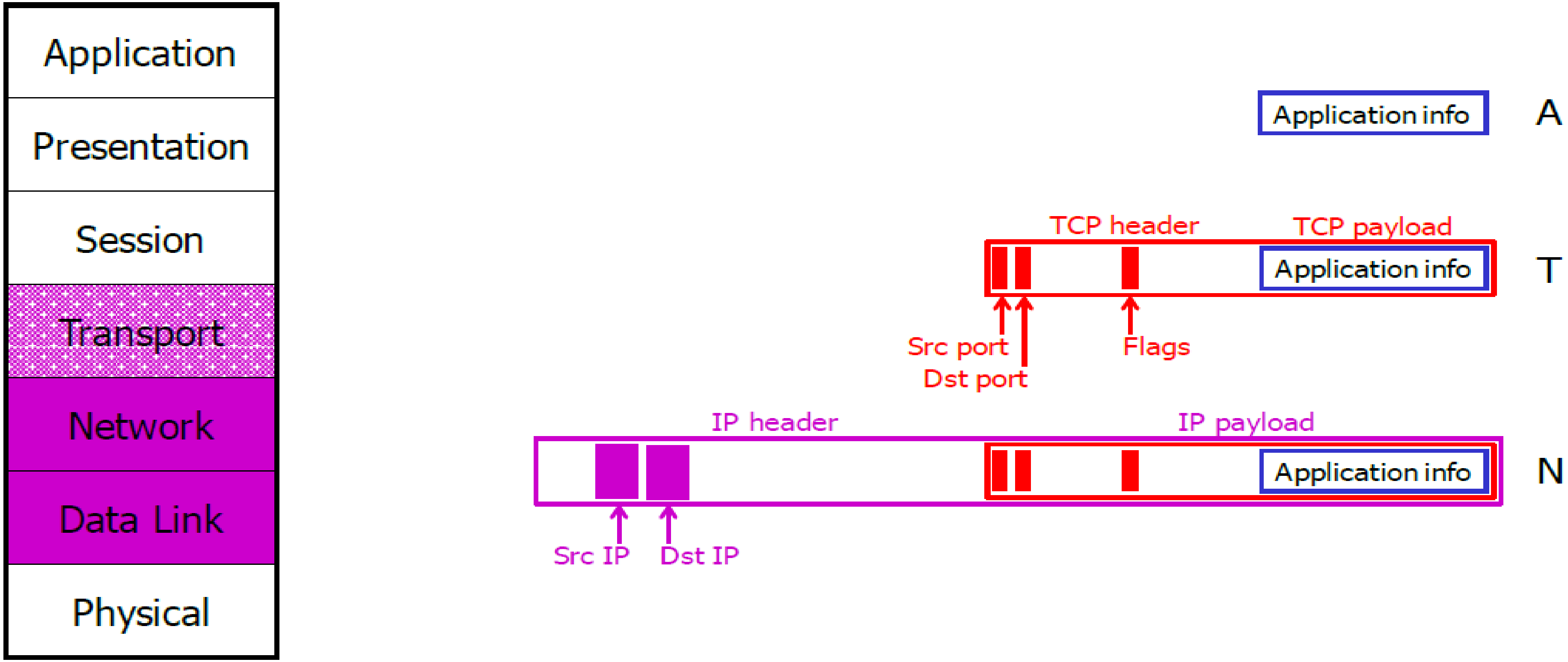
1. You have security policy stating what is allowed and not allowed.
2. You can identify the “good” and the “bad” traffic by its IP-address, TCP port numbers, etc, …
3. The firewall itself is immune to penetration.
   - A question of assurance – needs for a trusted system, secure OS etc.



Packet filters (stateless firewall)

- Drop packets based on their source or destination addresses or port numbers or flags
- No context, only contents
- Can operate on
  - incoming interface
  - outgoing interface
  - both
- Check packets with fake IP addresses:
  - from outside ("ingress filtering")
  - from inside ("egress filtering")

Packet filters operating layers


Application
Presentation
Session
Transport
Network
Data Link
Physical
Application info
A
TCP header
TCP payload
Application info
T
Src port
Dst port
Flags
IP header
IP payload
Application info
N
Src IP
Dst IP