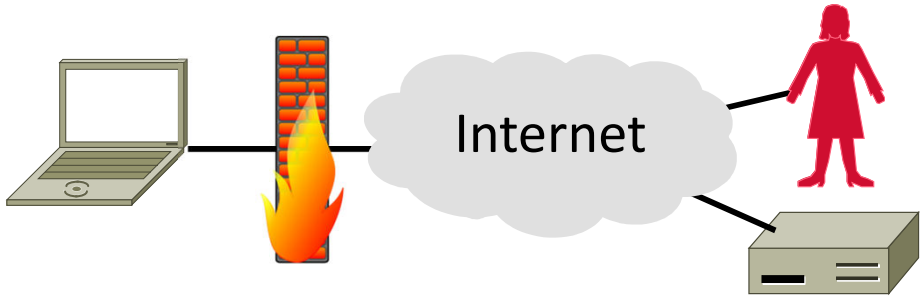
Introduction to Computer Networks

Firewalls (§8.6.2)

David Wetherall (djw@uw.edu)
Professor of Computer Science & Engineering
UNIVERSITY of WASHINGTON

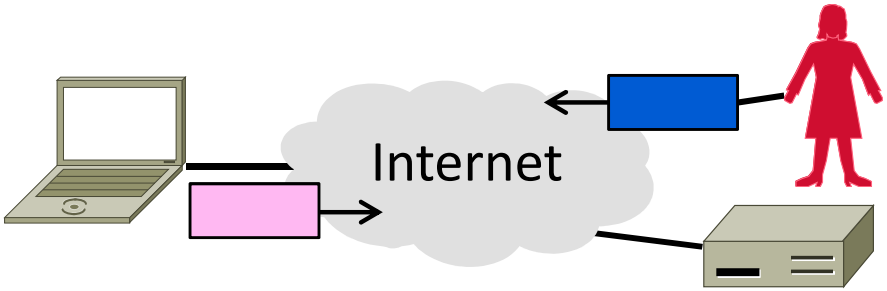
Topic

- Firewalls
  - Protecting hosts by restricting network connectivity



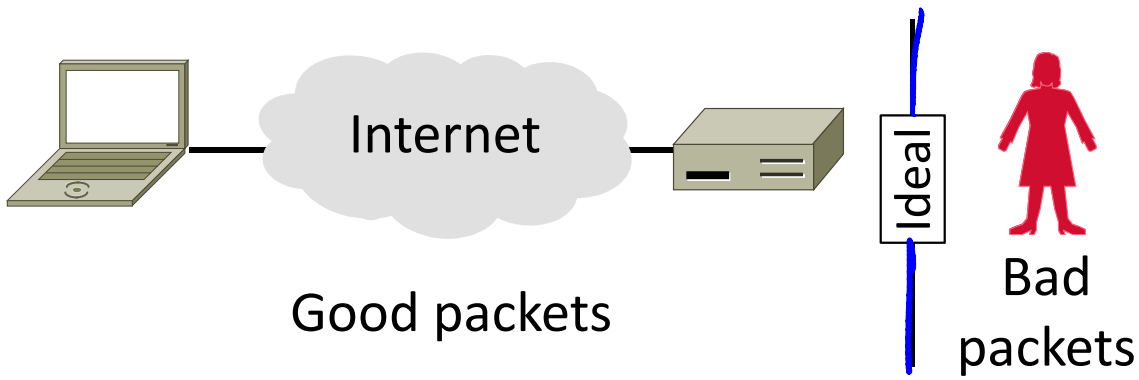
Motivation

- The best part of IP connectivity
  - You can send to any other host
- The worst part of IP connectivity
  - Any host can send packets to you!
  - There's nasty stuff out there …



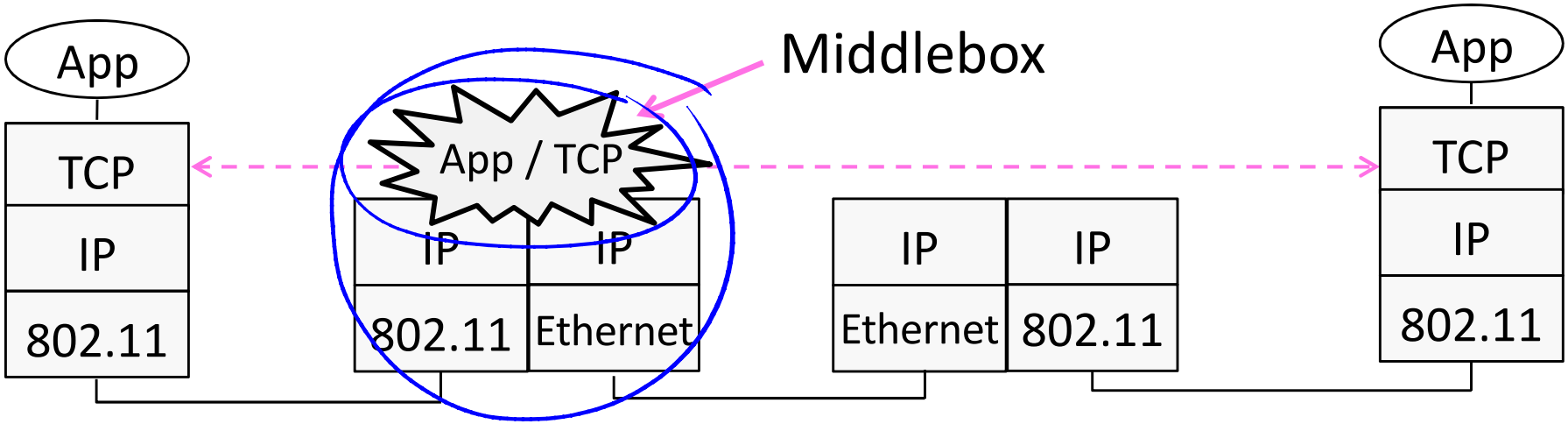
Goal and Threat Model

- Goal of firewall is to implement a boundary to restrict IP connectivity:
  - You can talk to hosts as intended
  - Trudy can't talk to you over network

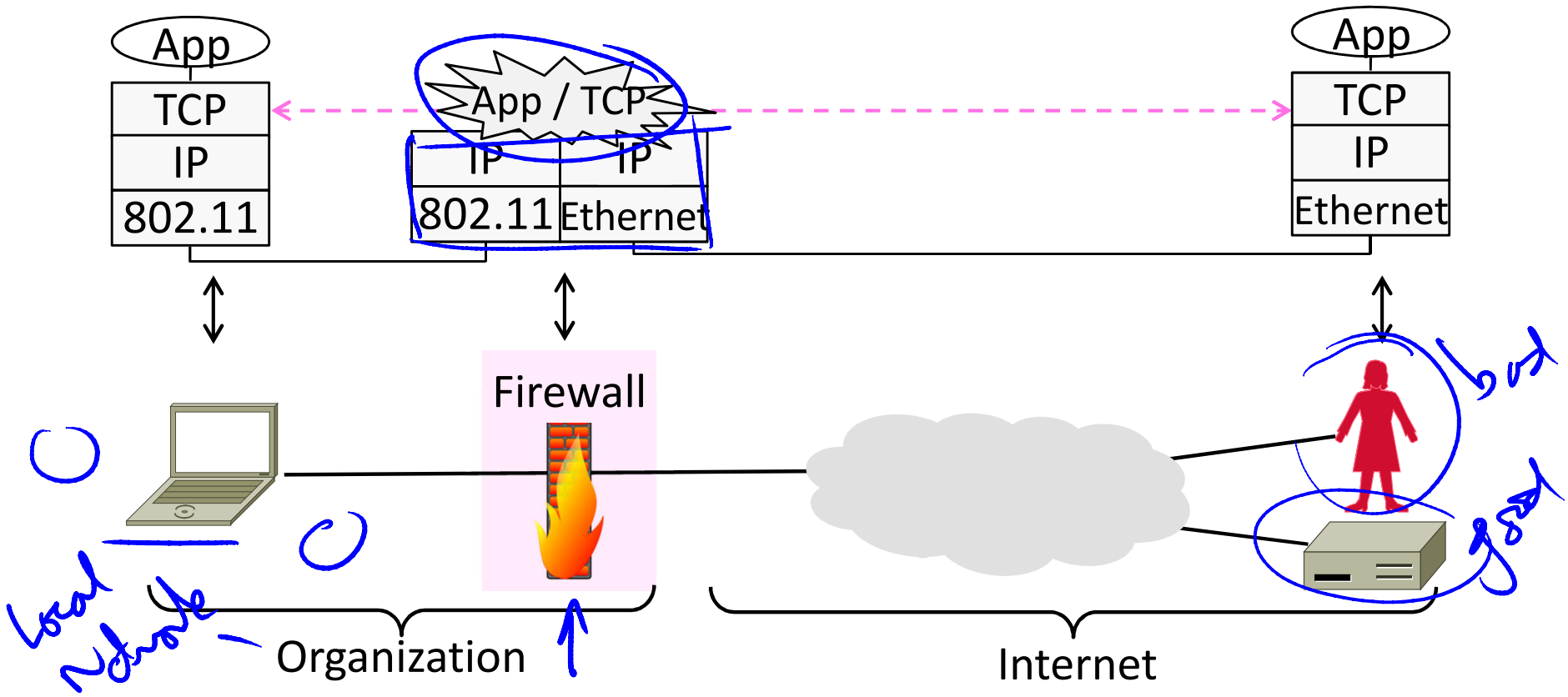


Recall Middleboxes

- Sit "inside the network" but perform "more than IP" processing on packets to add new functionality
  - NAT box, Firewall / Intrusion Detection System

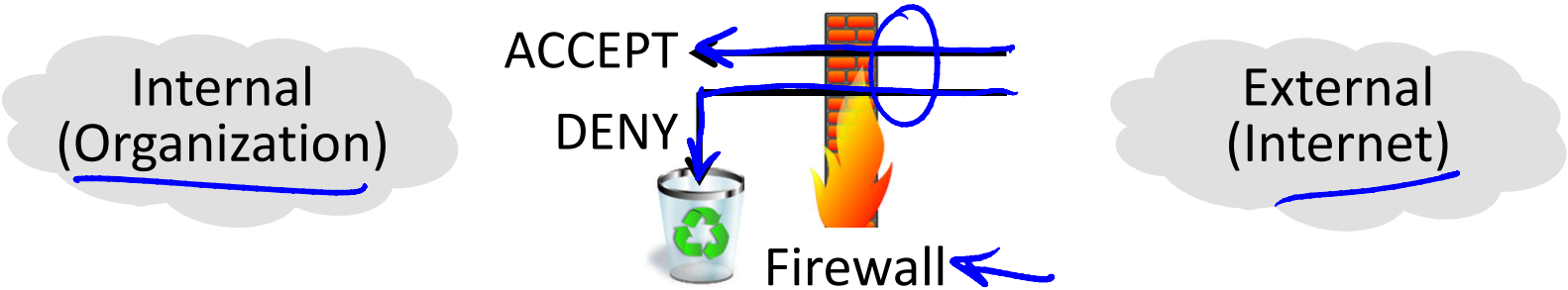


Firewall as Middlebox



Operation

- Firewall has two sides:
  - Internal (organization) and external (Internet)
- For each packet that tries to cross, decide whether to:
  - ACCEPT = pass unaltered; or DENY = discard silently
  - Decision is a local policy; firewall centralizes IT job



Design

- Key tension:
  - How to translate desired policies into packet filtering rules
- Policies are high-level statements
  - Relate to usage of apps, content
- Packet filtering is low-level
  - Limited viewpoint in the network, e.g., no app messages, encryption

Design (2)

- Stateless firewall
  - Simplest kind of firewall
  - Implements static packet filter rules
  - Typically using TCP/UDP ports
  - E.g., deny TCP port 22 (telnet)
  - Can allow/disallow many types of services and destinations

Design (3)

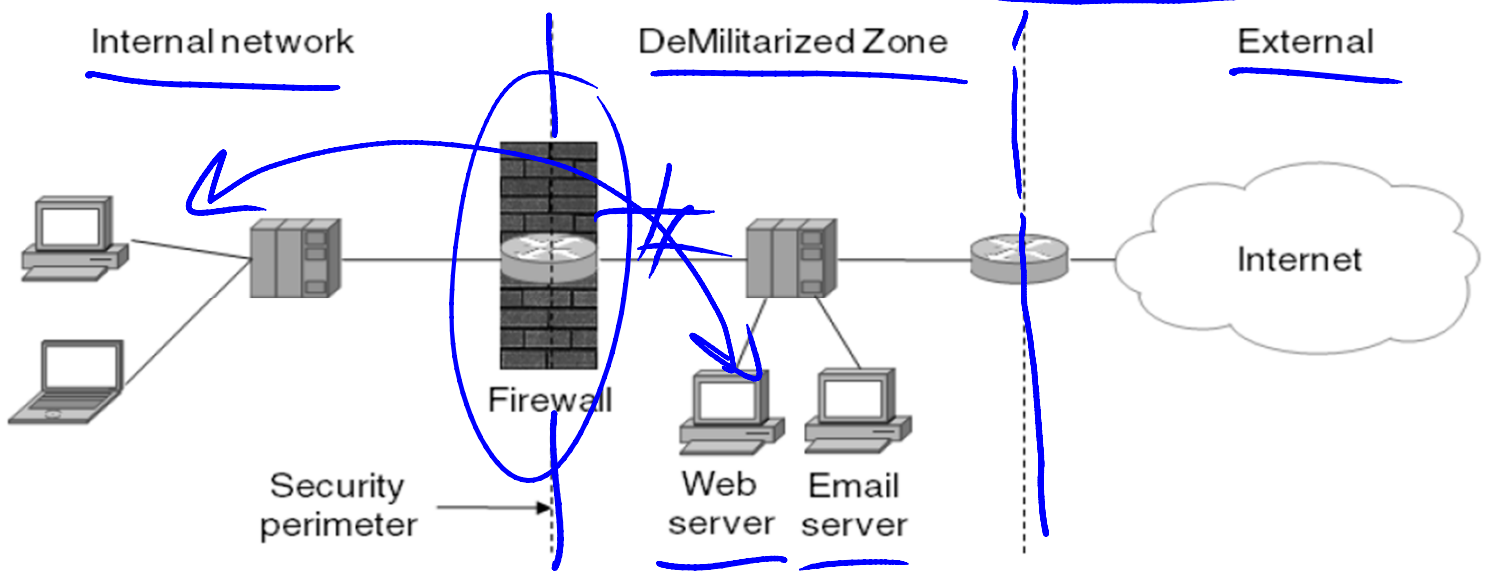
- Stateful firewall
  - A step up from stateless
  - Implements stateful packet filter rules that track packet exchanges
  - NAT example: accept incoming TCP packets after internal host connects

Design (4)

- Application layer firewall:
  - Another step up
  - Implements rules based on app usage and content
  - E.g., inspect content for viruses
  - Tries to look beyond packets by emulating higher layers, e.g., by reassembling app messages

Deployment

- Firewall is placed around internal/external boundary
  - Classic setup includes DMZ (DeMilitarized Zone) to put busy Internet hosts on the outside for better separation



Deployment (2)

- Various device options:
  - Specialized network firewall
  - Firewall in boundary device, e.g., AP
  - Firewall as part of host, e.g., in OS
- Tradeoff:
  - Centralizing simplifies IT job
  - Distributing improves protection, visibility into apps, and performance

END