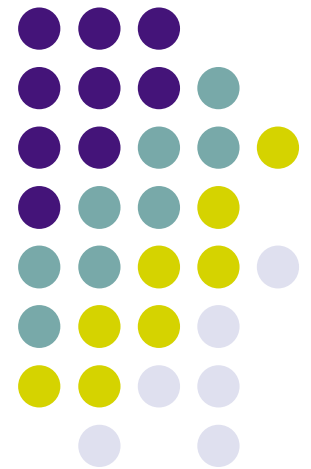
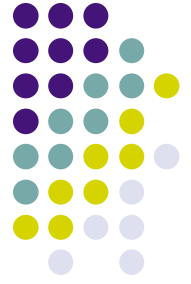


# IP packet filtering

---

Breno de Medeiros

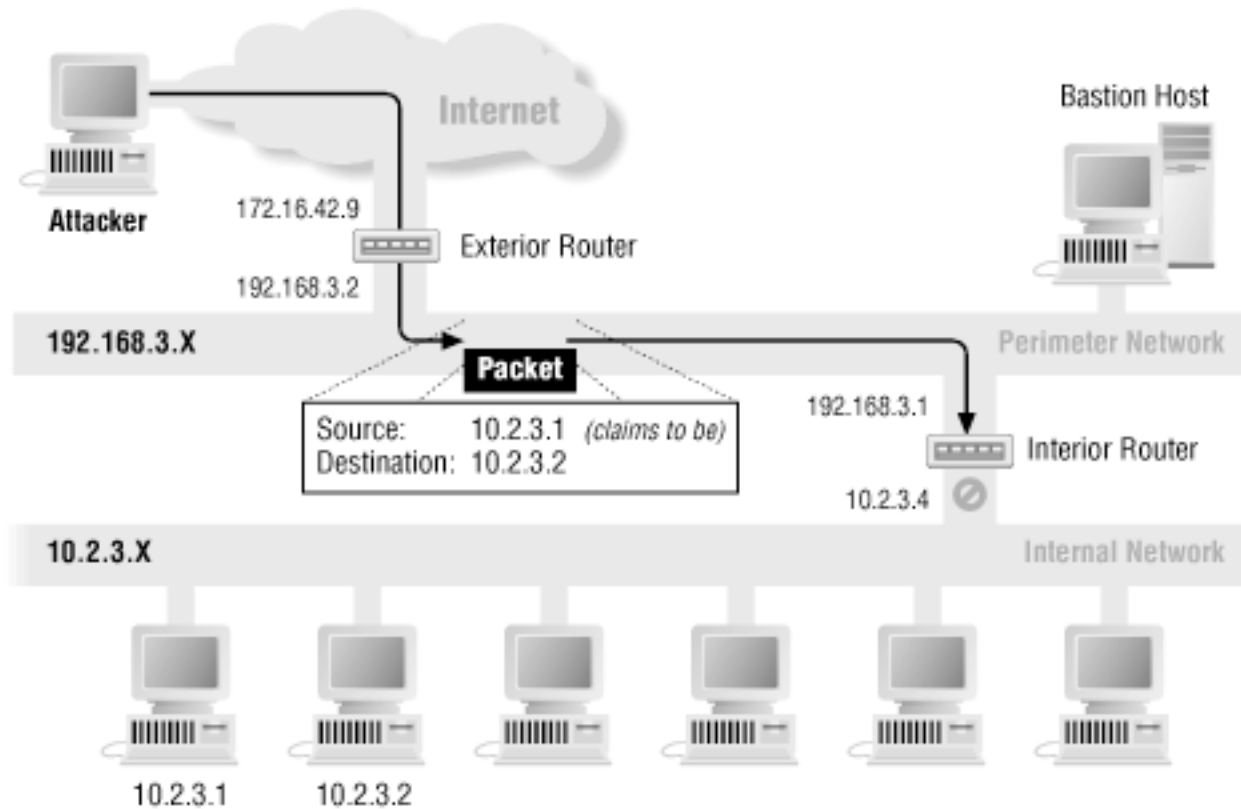
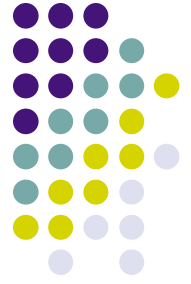




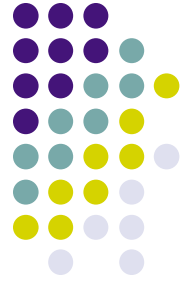
# Packet filtering

- Packet filtering is a network security mechanism that works by controlling what data can flow to and from a network.
  - Packet filtering occurs at routers
  - A router inspects each packet entering and/or leaving the network to make routing decisions.
  - A filtering router also makes policy decisions.

# Dropping spoofed/malformed packets

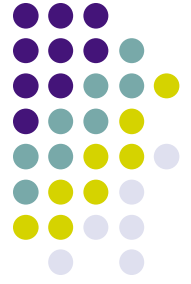


Fair-use notice: All images in this presentation are copyrighted property, extracted from Zwicky, Cooper, and Chapman's Building Internet Firewalls, O'Reilly (2002)



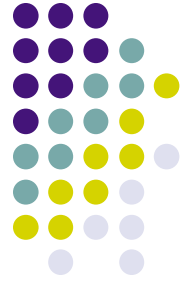
# Basic ip-filtering policies

- Source and destination addresses
- Session and application ports
  - enforce visibility/connectivity policies of internal network to the Internet
  - prevent certain protocols from being executed between specific hosts in different networks
- Maintains no state information about connections



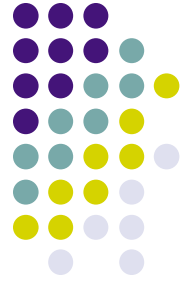
# Examples

- Allow outgoing TCP port 80 requests
- Allow incoming SMTP to mail server only
- Disallow outgoing packets with external source addresses
- Disallow incoming packets with internal source addresses
- Disallow incoming TCP port 17 packets



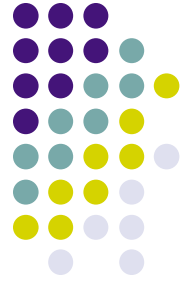
# Stateful packet filtering

- Allows for more complex policies based on current state of connections between two machines.
  - Let incoming UDP packets through only if they are responses to outgoing UDP packets you have seen.
  - Accept TCP packets with SYN set only as part of TCP connection initiation.



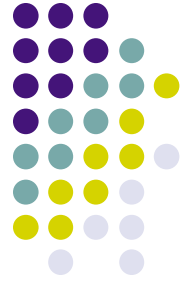
# Stateful/dynamic filtering

- Routers must keep state information
  - For how long?
- If multiple routers are used, they need to synchronize the state information very fast, or else there will be incorrect decisions.
- Protocol-based filtering:
  - ensure that packets contain properly formed protocol data
  - prevent protocols being run on other ports



# Default deny

- Disallow all by default; add rules to permit traffic explicitly
- Log dropped packets
- Log some allowed packets
- For some protocols, such as mail authentication, it is ok to send an ICMP error message in response to a disallowed packet. In most cases, better to drop the packet and say nothing to sender.



# Formatting addresses

- IPv4 addresses are specified as 4-octets (unsigned bytes) in point-separated decimal notation:
  - 128.186.120.2      diablo.cs.fsu.edu
- A whole range of addresses is denoted by adding a '/' followed by the number of prefix bits to consider:
  - 128.186.120.0/24 matches 128.186.120.x
  - 128.186.0.0/16 matches 128.186.x.x



# IPv6 addresses

- These are 16-octets, written in 8 colon-separated groups of 4-digit hexadecimal characters:
  - 2001:218:420:0:a00:5aff:fe38:6f86
- Prefixes are usually of length 64, or 48.