

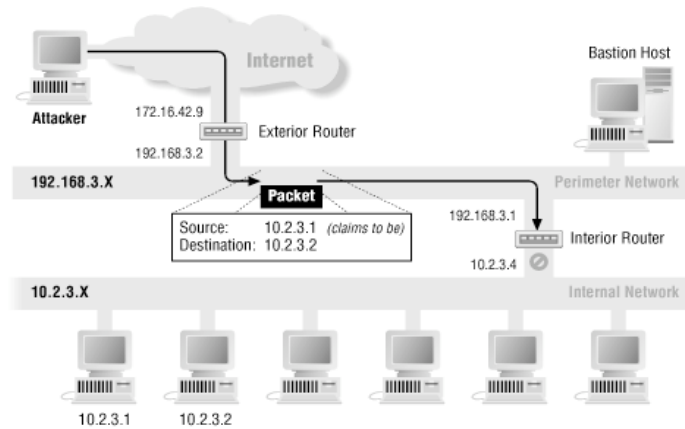
# IP packet filtering

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



Breno de Medeiros

Florida State University  
Fall 2005

From textbook:  
Building Internet Firewalls

## 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

Breno de Medeiros

Florida State University  
Fall 2005

## 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.

Breno de Medeiros

Florida State University  
Fall 2005

## 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

Breno de Medeiros

Florida State University  
Fall 2005

## Default deny/drop

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

Breno de Medeiros

Florida State University  
Fall 2005

## 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 packets for TCP/UDP port 79 (finger)

Breno de Medeiros

Florida State University  
Fall 2005