Network Security
Computer Security

Peter Reiher

February 2, 2021

Some Important Network Characteristics for Security

- Degree of locality
- Media used
- Protocols used

Degree of Locality

- Some networks are very local
  - E.g., an Ethernet
  - Benefits from:
    - Physical locality
    - Small number of users and machines
    - Common goals and interests
- Other networks are very non-local
  - E.g., the Internet backbone
  - Many users/sites share bandwidth

Network Media

- Some networks are wires, cables, or over telephone lines
  - Can be physically protected
- Other networks are satellite links or other radio links
  - Physical protection possibilities more limited

Protocol Types

- TCP/IP is the most used
  - But it only specifies some common intermediate levels
  - Other protocols exist above and below it
- In places, other protocols replace TCP/IP
- And there are lots of supporting protocols
  - Routing protocols, naming and directory protocols, network management protocols
  - And security protocols (IPSec, ssh, tls)

Implications of Protocol Type

- The protocol defines a set of rules that will always be followed
  - But usually not quite complete
  - And they assume everyone is at least trying to play by the rules
  - What if they don't?
- Specific attacks exist against specific protocols

Threats To Networks

- Wiretapping
- Impersonation
- Attacks on message
  - Confidentiality
  - Integrity
- Denial of service attacks

Wiretapping

- **Passive wiretapping** is listening in illicitly on conversations
- **Active wiretapping** is injecting traffic illicitly
- **Packet sniffers** can listen to all traffic on a broadcast medium
  - Ethernet or 802.11, e.g.
- Wiretapping on wireless often just a matter of putting up an antenna

Impersonation

- A packet comes in over the network
  - With some source indicated in its header
- Often, the action to be taken with the packet depends on the source
- But attackers may be able to create packets with false sources

Violations of Message Confidentiality

- Other problems can cause messages to be inappropriately divulged
- Misdelivery can send a message to the wrong place
  - Clever attackers can make it happen
- Message can be read at an intermediate gateway or a router
- Sometimes an intruder can get useful information just by traffic analysis

Message Integrity

- Even if the attacker can’t create the packets he wants, sometimes he can alter proper packets
- To change the effect of what they will do
- Typically requires access to part of the path message takes

Denial of Service

- Attacks that prevent legitimate users from doing their work
- By flooding the network
- Or corrupting routing tables
- Or flooding routers
- Or destroying key packets

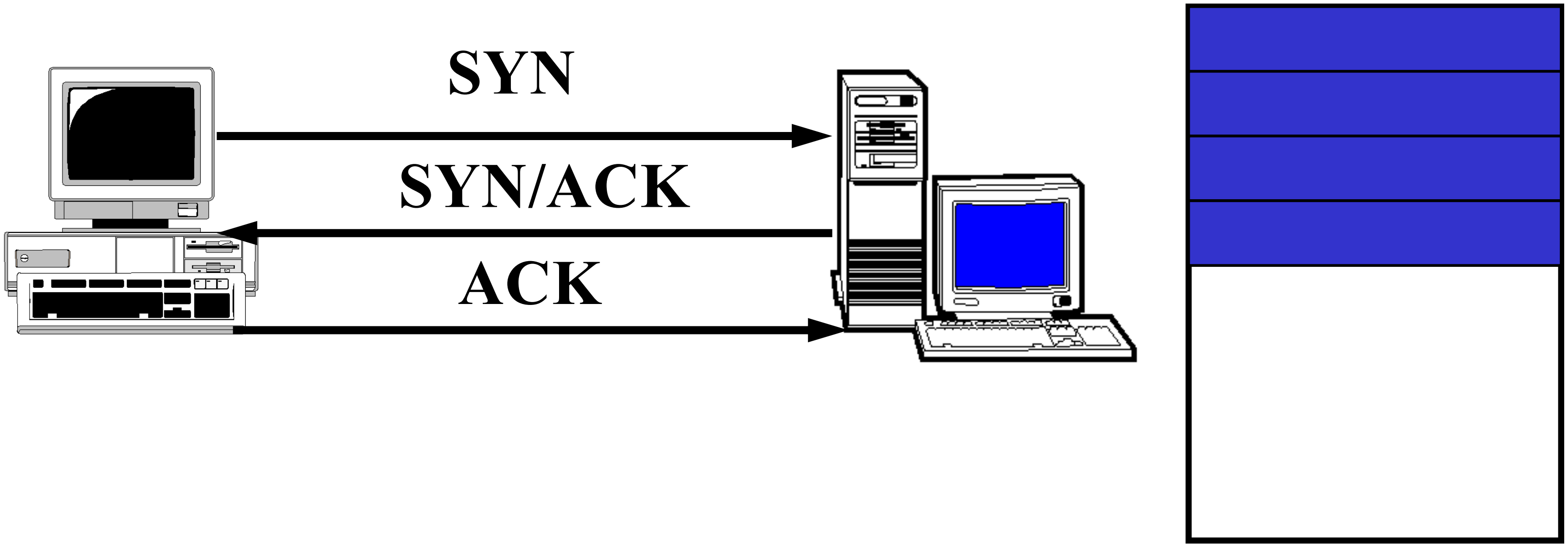
How Do Denial of Service Attacks Occur?

- Basically, the attacker injects some form of traffic
- Most current networks aren’t built to throttle uncooperative parties very well
- All-inclusive nature of the Internet makes basic access trivial
- Universality of IP makes reaching most of the network easy

An Example: SYN Flood

- Based on vulnerability in TCP
- Attacker uses initial request/response to start TCP session to fill a table at the server
- Preventing new real TCP sessions
- SYN cookies and firewalls with massive tables are possible defenses

Normal SYN Behavior



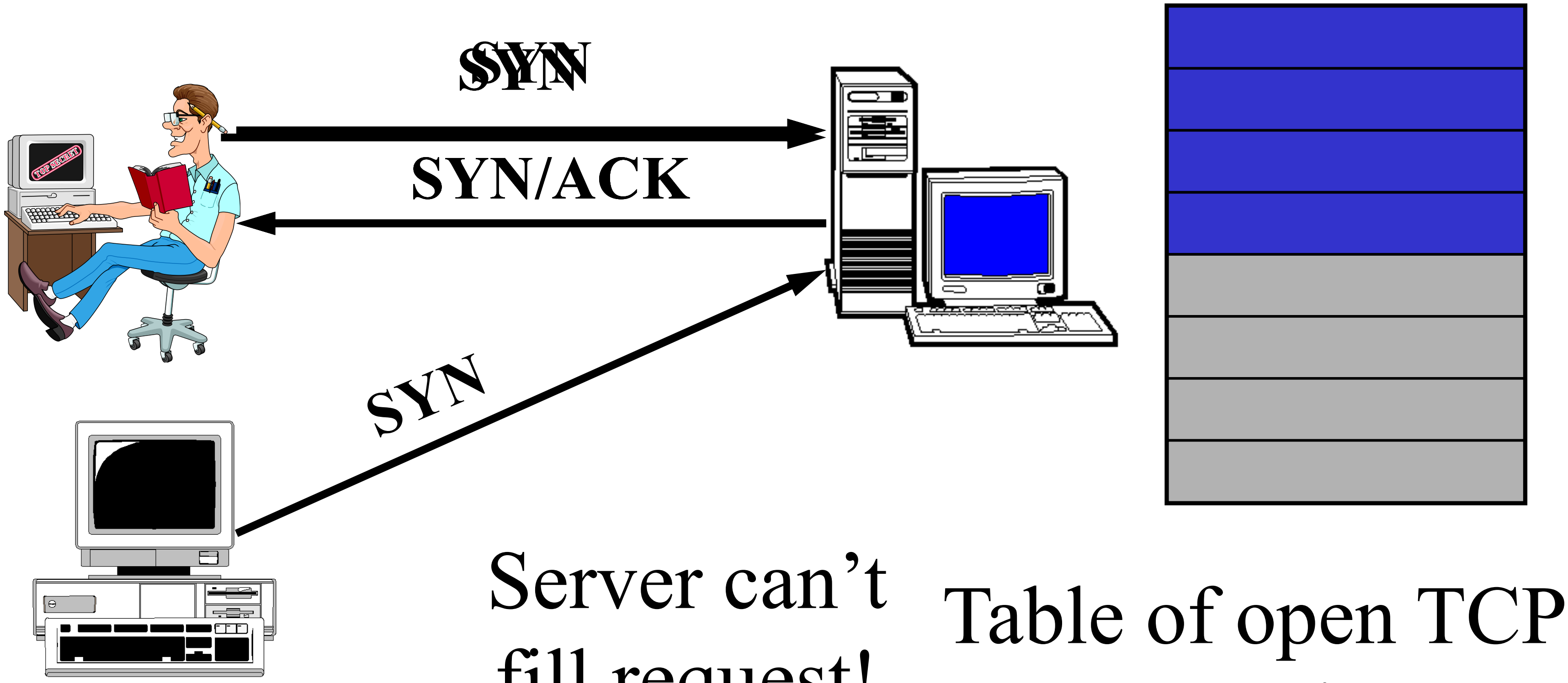
SYN

SYN/ACK

ACK

Table of open TCP connections

A SYN Flood



Server can’t fill request!

Table of open TCP connections

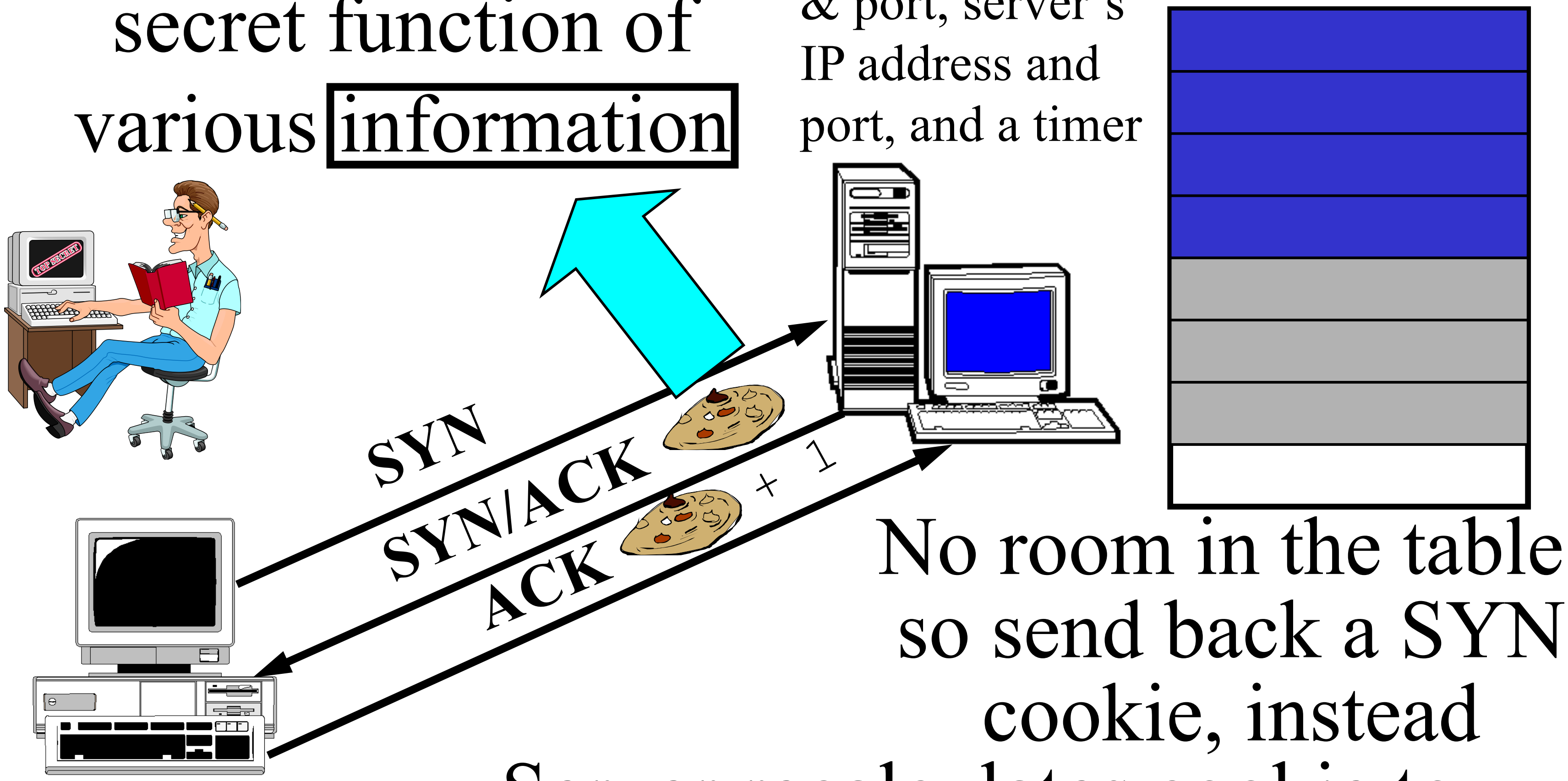
And no changes to TCP protocol itself

SYN Cookies

KEY POINT: Server doesn't need to save cookie value!

SYN/ACK number is secret function of various information

Client IP address & port, server's IP address and port, and a timer



No room in the table, so send back a SYN cookie, instead

Server recalculates cookie to determine if proper response

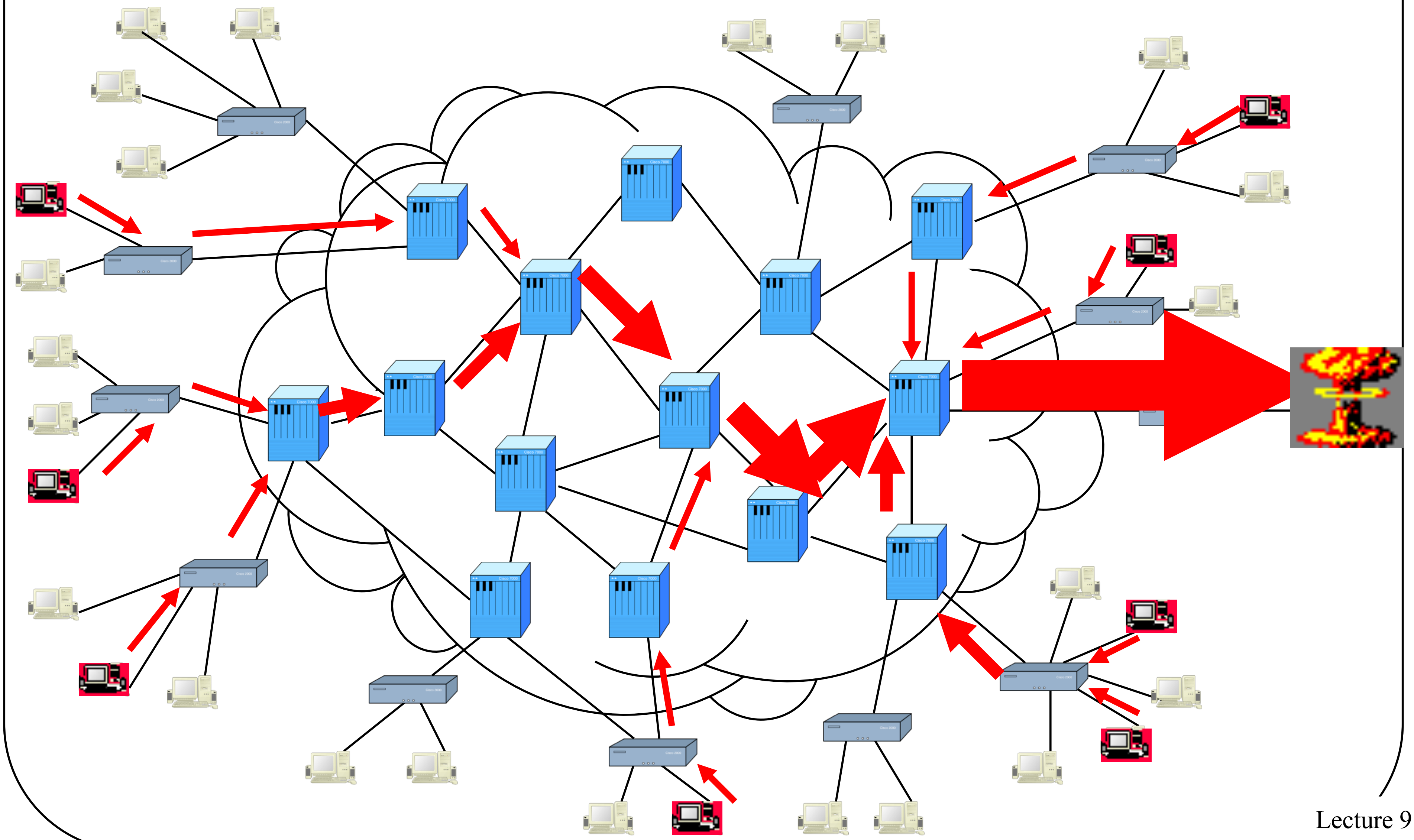
General Network Denial of Service Attacks

- Need not tickle any particular vulnerability
- Can achieve success by mere volume of packets
- If more packets sent than can be handled by target, service is denied
- A hard problem to solve

Distributed Denial of Service Attacks

- Goal: Prevent a network site from doing its normal business
- Method: overwhelm the site with attack traffic
- Response: ?

The Problem



Why Are These Attacks Made?

- Generally to annoy
- Sometimes for extortion
- Sometimes to prevent adversary from doing something important
- If directed at infrastructure, might cripple parts of Internet

Attack Methods

- Pure flooding
  - Of network connection
  - Or of upstream network
- Overwhelm some other resource
  - SYN flood
  - CPU resources
  - Memory resources
  - Application level resource
- Direct or reflection

Why “Distributed”?

- Targets are often highly provisioned servers
- A single machine usually cannot overwhelm such a server
- So harness multiple machines to do so
- Also makes defenses harder

How to Defend?

- A vital characteristic:
  - Don’t just stop a flood
  - ENSURE SERVICE TO LEGITIMATE CLIENTS!!!
- If you deliver a manageable amount of garbage, you haven’t solved the problem
- Nor have you if you prevent a flood by dropping all packets

Complicating Factors

- High availability of compromised machines
  - Millions of zombie machines out there
- Internet is designed to deliver traffic
  - Regardless of its value
- IP spoofing allows easy hiding
- Distributed nature makes legal approaches hard
- Attacker can choose all aspects of his attack packets
  - Can be a lot like good ones

Basic Defense Approaches

- Overprovisioning
- Dynamic increases in provisioning
- Hiding
- Tracking attackers
- Legal approaches
- Reducing volume of attack
- None of these are totally effective

Traffic Control Mechanisms

- Filtering
  - Source address filtering
  - Other forms of filtering
- Rate limits
- Protection against traffic analysis
  - Padding
  - Routing control

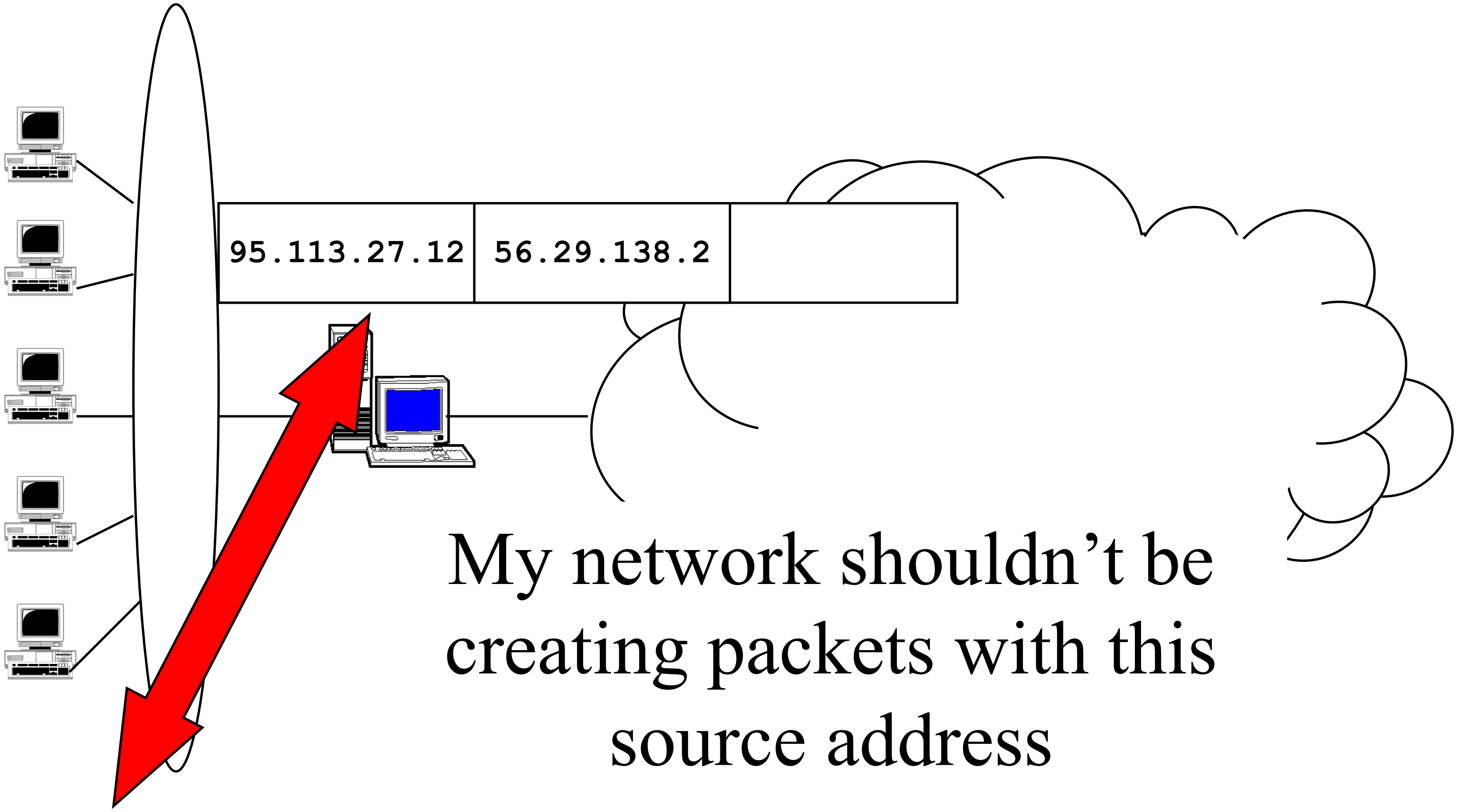
Source Address Filtering

- Filtering out some packets because of their source address value
  - Usually because you believe their source address is spoofed
- Often called ingress filtering
  - Or egress filtering . . .

Source Address Filtering for Address Assurance

- Router "knows" what network it sits in front of
  - In particular, knows IP addresses of machines there
- Filter outgoing packets with source addresses not in that range
- Prevents your users from spoofing other nodes' addresses
  - But not from spoofing each other's

Source Address Filtering Example



128.171.192.*

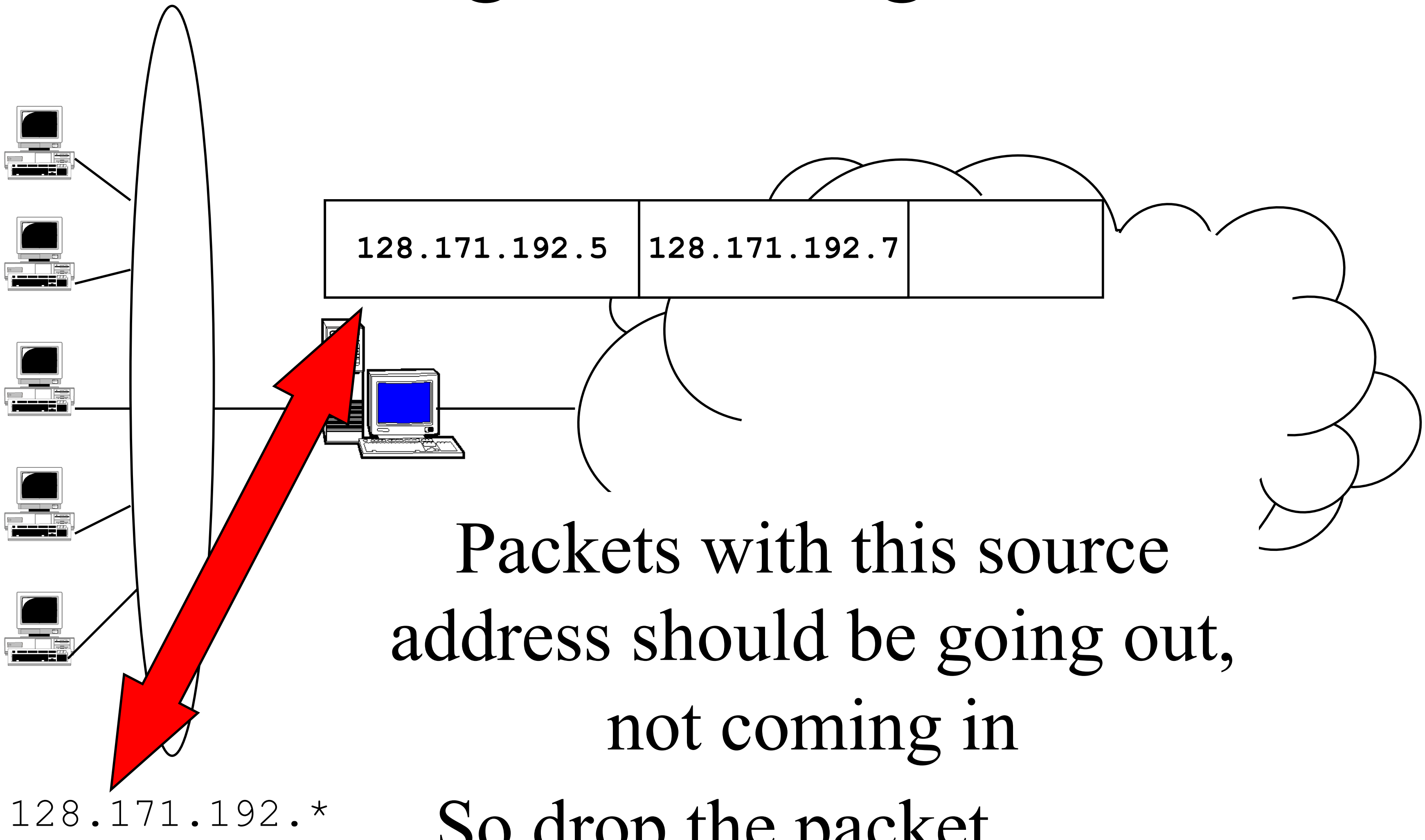
My network shouldn't be creating packets with this source address

So drop the packet

Source Address Filtering in the Other Direction

- Often called egress filtering
  - Or ingress filtering . . .
- Occurs as packets leave the Internet and enter a border router
  - On way to that router's network
- What addresses shouldn't be coming into your local network?

Filtering Incoming Packets



Packets with this source address should be going out, not coming in

So drop the packet

Other Forms of Filtering

- One can filter on things other than source address
  - Such as worm signatures, unknown protocol identifiers, etc.
- Also, there are unallocated IP addresses in IPv4 space
  - Can filter for packets going to or coming from those addresses
- Some source addresses for local use only
  - Internet routers can drop packets to/from them

Realistic Limits on Filtering

- Little filtering possible in Internet core
  - Packets being handled too fast
  - Backbone providers don't want to filter
  - Great damage if you screw it up
- Filtering near edges has its own limits
  - In what's possible
  - In what's affordable
  - In what the router owners will do

Another Filtering Possibility

- Redirect packets to a special filtering site on the edge of the network
- They filter on any basis they want
  - Including packet contents
- What they don't drop they send to you
- Many DDoS defense services work this way
- Incurs serious delay penalties

Rate Limits

- Many routers can place limits on the traffic they send to a destination
- Ensuring that the destination isn't overloaded
  - Popular for denial of service defenses
- Limits can be defined somewhat flexibly
- But often not enough flexibility to let the good traffic through and stop the bad

Padding

- Sometimes you don't want intruders to know what your traffic characteristics are
- Padding adds extra traffic to hide the real stuff
- Fake traffic must look like real traffic
  - Usually means encrypt it all
- Must be done carefully, or clever attackers can tell the good stuff from the noise

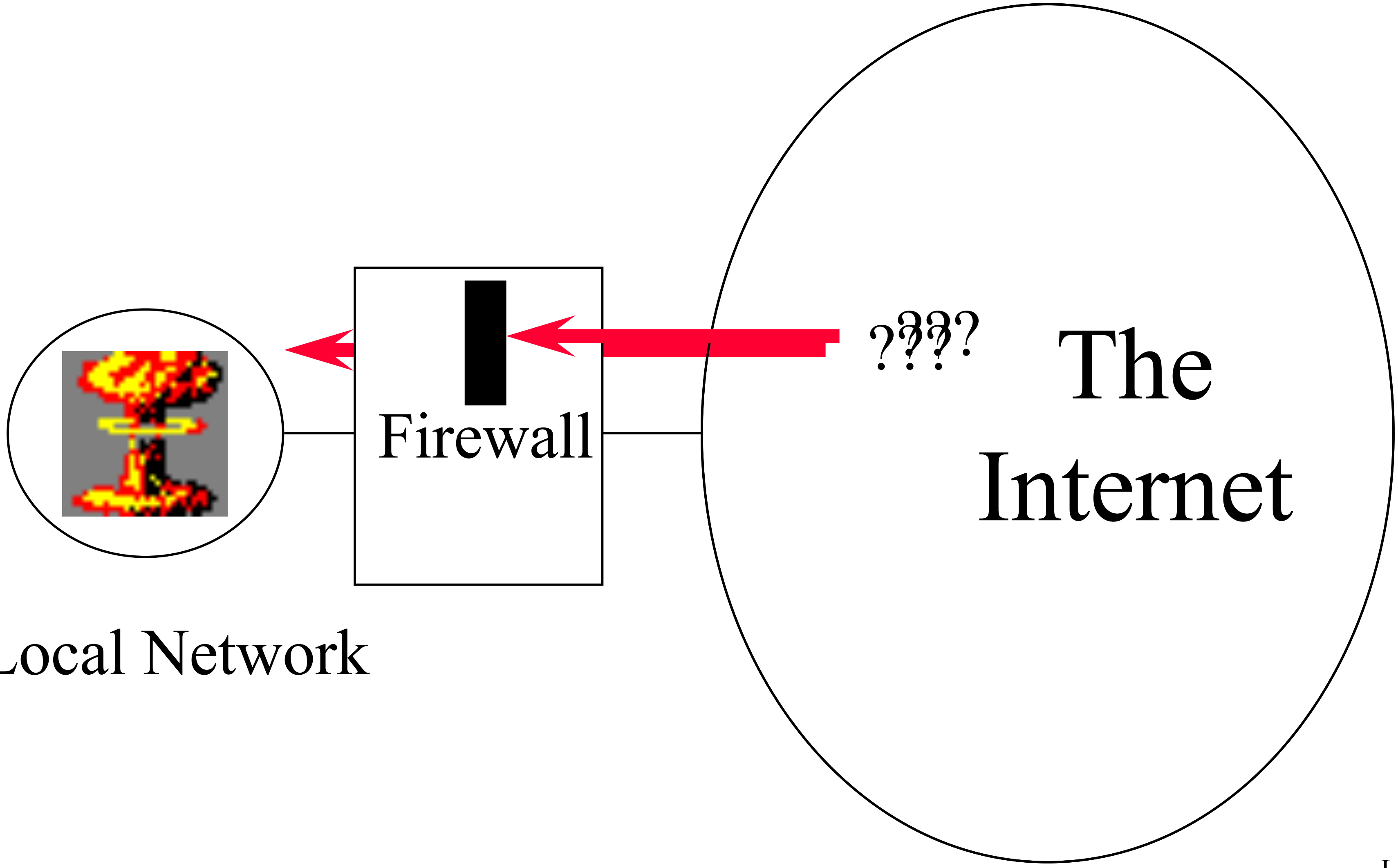
Routing Control

- Use ability to control message routing to conceal the traffic in the network
- Used in *onion routing* to hide who is sending traffic to whom
  - For anonymization purposes
- Routing control also used in some network defense
  - To hide real location of a machine
  - E.g., SOS DDoS defense system

Firewalls

- What is a firewall?
- A machine to protect a network from malicious external attacks
- Typically a machine that sits between a LAN/WAN and the Internet
- Running special software to regulate network traffic

Typical Use of a Firewall



Local Network

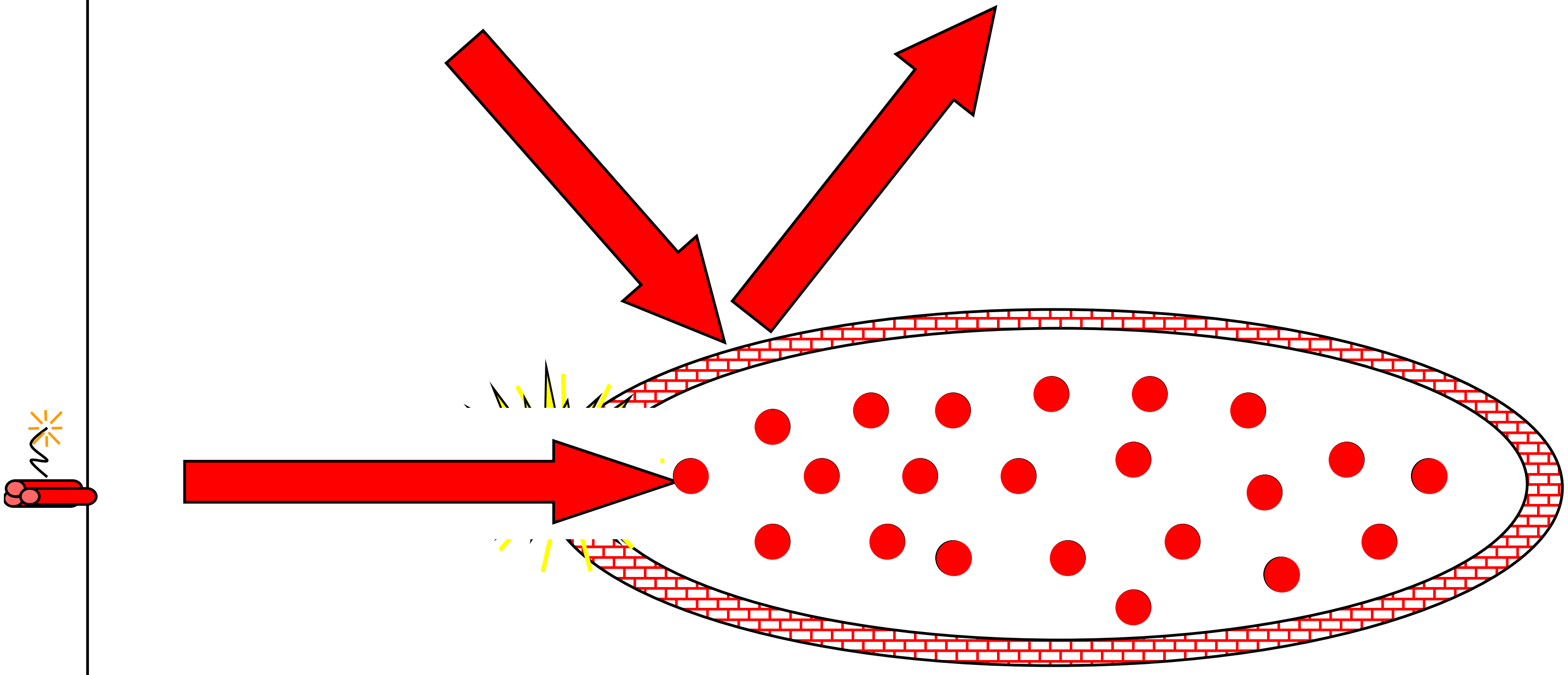
Firewalls and Perimeter Defense

- Firewalls implement a form of security called *perimeter defense*
- Protect the inside of something by defending the outside strongly
  - The firewall machine is often called a *bastion host*
- Control the entry and exit points
- If nothing bad can get in, I'm safe, right?

Weaknesses of Perimeter Defense Models

- Breaching the perimeter compromises all security
- Windows passwords are a form of perimeter defense
  - If you get past the password, you can do anything
- Perimeter defense is part of the solution, not the entire solution

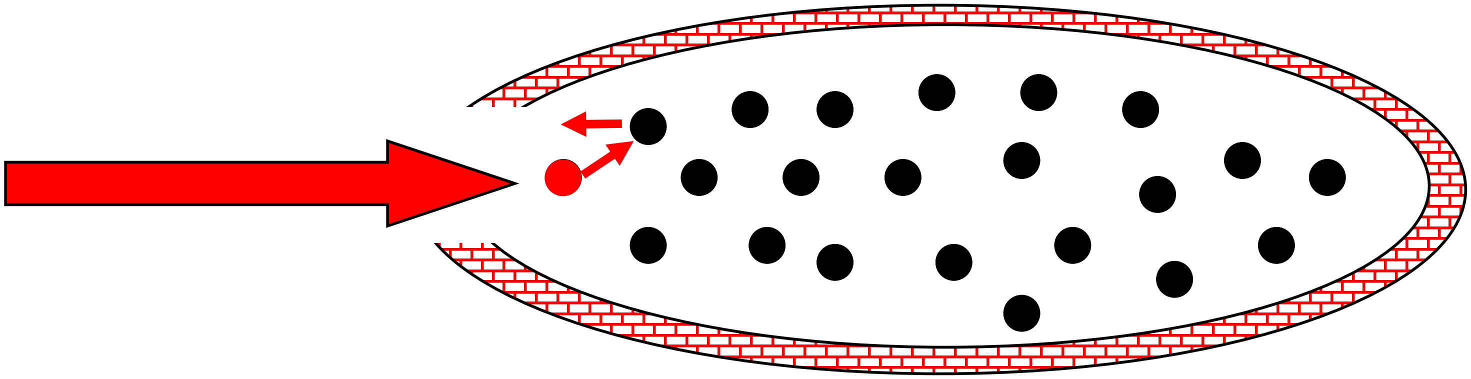
Weaknesses of Perimeter Defense



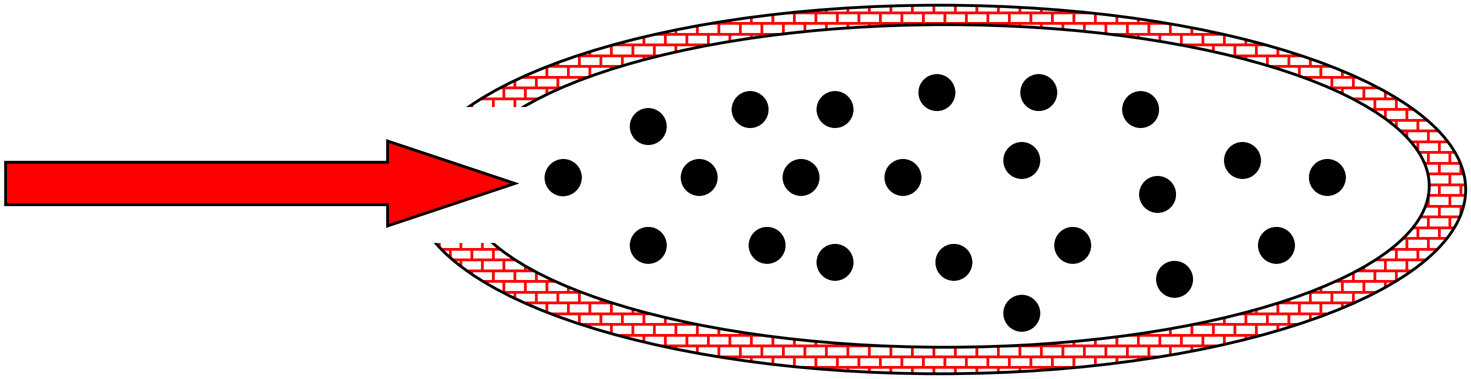
Defense in Depth

- An old principle in warfare
- Don’t rely on a single defensive mechanism or defense at a single point
- Combine different defenses
- Defeating one defense doesn’t defeat your entire plan

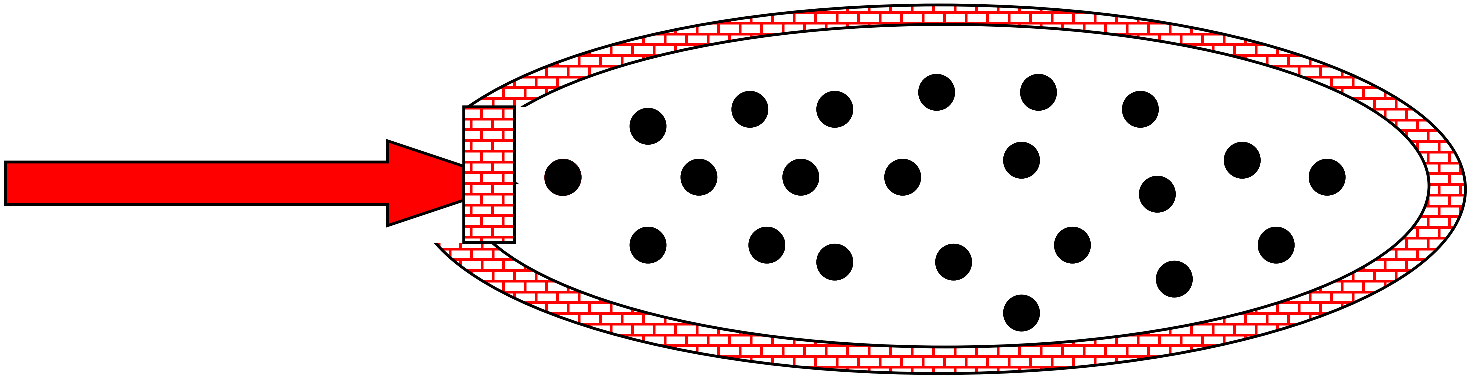
So What Should Happen?



Or, Better



Or, Even Better



So Are Firewalls Any Use?

- Definitely!
- They aren’t the full solution, but they are absolutely part of it
- Anyone who cares about security needs to run a decent firewall
- They just have to do other stuff, too

The Brass Tacks of Firewalls

- What do they really do?
- Examine each incoming packet
- Decide to let the packet through or drop it
  - Criteria could be simple or complex
- Perhaps log the decision
- Maybe send rejected packets elsewhere
- Pretty much all there is to it

Types of Firewalls

- Filtering gateways
  - AKA screening routers
- Application level gateways
  - AKA proxy gateways
- Reverse firewalls

Filtering Gateways

- Based on packet header information
  - Primarily, IP addresses, port numbers, and protocol numbers
- Based on that information, either let the packet through or reject it
- *Stateless* firewalls

Example Use of Filtering Gateways

- Allow particular external machines to telnet into specific internal machines
  - Denying telnet to other machines
- Or allow full access to some external machines
- And none to others

A Fundamental Problem

- IP addresses can be spoofed
- If your filtering firewall trusts packet headers, it offers little protection
- Situation may be improved by IPsec
  - But hasn't been yet
- Firewalls can perform the ingress/egress filtering discussed earlier

Filtering Based on Ports

- Most incoming traffic is destined for a particular machine and port
  - Which can be derived from the IP and TCP headers
- Only let through packets to select machines at specific ports
- Makes it impossible to externally exploit flaws in little-used ports
  - If you configure the firewall right . . .

Pros and Cons of Filtering Gateways

+ Fast
+ Cheap
+ Flexible
+ Transparent
– Limited capabilities
– Dependent on header authentication
– Generally poor logging
– May rely on router security

Application Level Gateways

- Also known as proxy gateways
- Firewalls that understand the application-level details of network traffic
  - To some degree
- Traffic is accepted or rejected based on the probable results of accepting it
- *Stateful* firewalls

How Application Level Gateways Work

- The firewall serves as a general framework
- Various proxies are plugged into the framework
- Incoming packets are examined
  - Handed to the appropriate proxy
- Proxy typically accepts or rejects

Deep Packet Inspection

- Another name for typical activity of application level firewalls
- Looking into packets beyond their headers
  - Especially the IP header
- "Deep" sometimes also means deeper understanding of what's going on
  - Though not always
- It almost always means "expensive"
  - In terms of performance

Firewall Proxies

- Programs capable of understanding particular kinds of traffic
  - E.g., FTP, HTTP, videoconferencing
- Proxies are specialized
- A good proxy has deep understanding of the network application
- Typically limited by complexity and performance issues

Pros and Cons of Application Level Gateways

+ Highly flexible
+ Good logging
+ Content-based filtering
+ Potentially transparent
– Slower
– More complex and expensive
– Highly dependent on proxy quality

Reverse Firewalls

- Normal firewalls keep stuff from the outside from getting inside
- Reverse firewalls keep stuff from the insider from getting outside
- Often colocated with regular firewalls
- Why do we need them?

Possible Uses of Reverse Firewalls

- Concealing details of your network from attackers
- Preventing compromised machines from sending things out
  - E.g., intercepting bot communications or stopping DDoS
  - Preventing data exfiltration

Firewall Characteristics

- Statefulness
- Transparency
- Handling authentication
- Handling encryption

Stateful Firewalls

- Much network traffic is connection-oriented
  - E.g., telnet and videoconferencing
- Proper handling of that traffic requires the firewall to maintain state
- But handling information about connections is more complex

Firewalls and Transparency

- Ideally, the firewall should be invisible
  - Except when it vetoes access
- Users inside should be able to communicate outside without knowing about the firewall
- External users should be able to invoke internal services transparently

Firewalls and Authentication

- Many systems want to give special privileges to specific sites or users
- Firewalls can only support that to the extent that strong authentication is available
  - At the granularity required
- For general use, may not be possible
  - In current systems

Firewalls and Encryption

- Firewalls provide no confidentiality
- Unless the data is encrypted
- But if the data is encrypted, the firewall can't examine it
- So typically the firewall must be able to decrypt
  - Or only work on unencrypted parts of packets
- Can decrypt, analyze, and re-encrypt