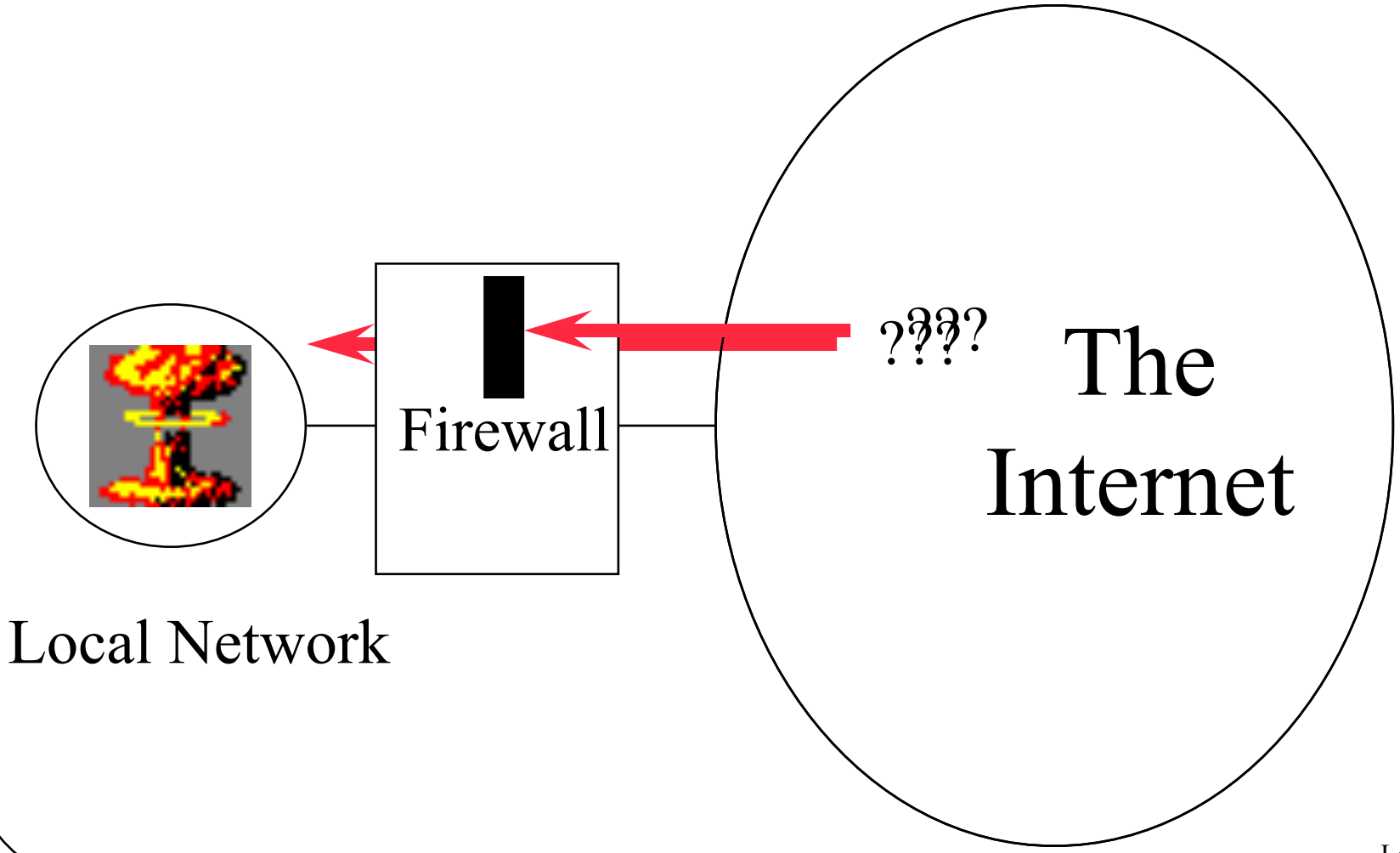
Firewalls

- 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



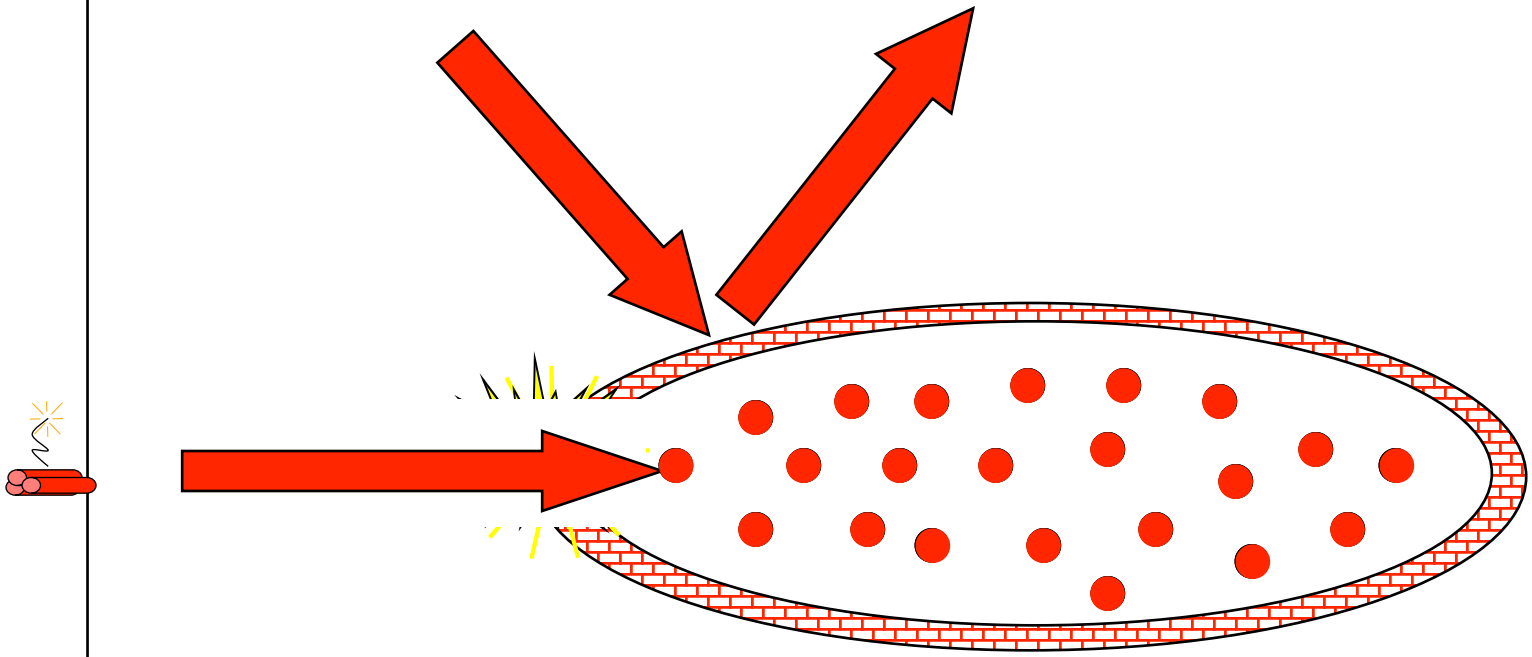
Firewalls and Perimeter Defense

- 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

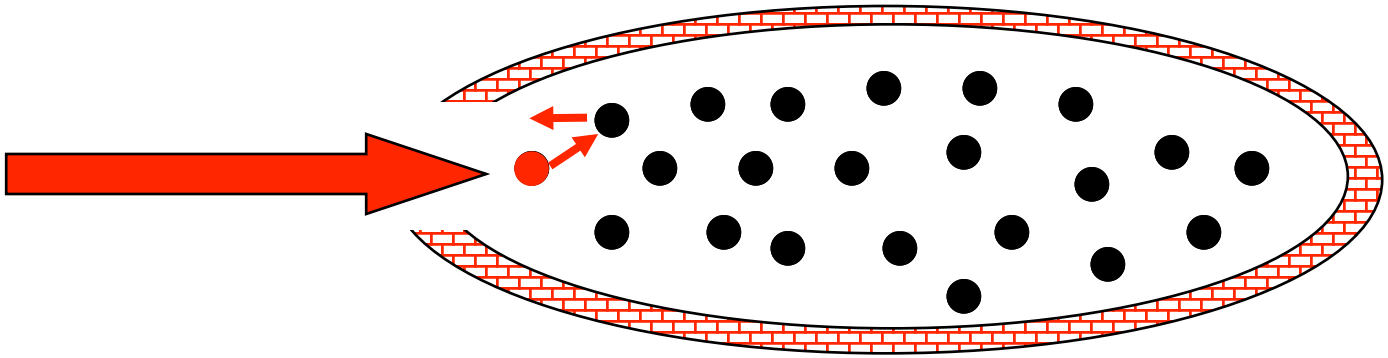
Weaknesses of Perimeter Defense



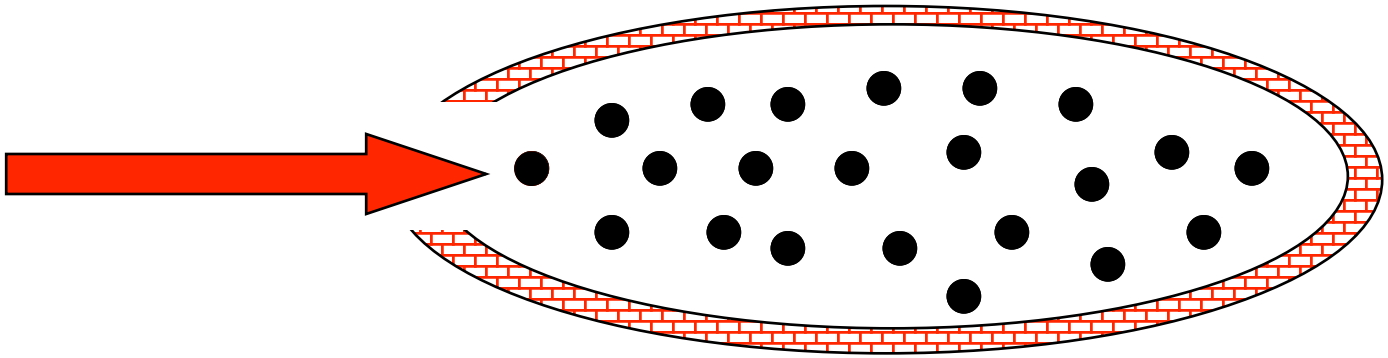
Defense in Depth

- 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

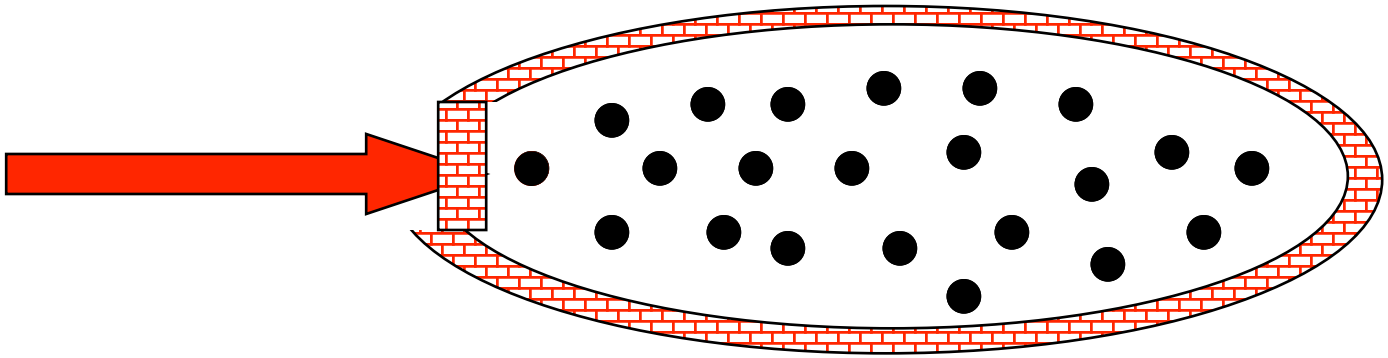
So What Should Happen?



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

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