Firewalls

Steven M. Bellovin
https://www.cs.columbia.edu/~smb

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

What’s a Firewall?

- A barrier between “us” and the Internet
- All traffic, inbound or outbound, must pass through it
- Firewalls enforce *policy*: only certain traffic is allowed to flow

inside and outside

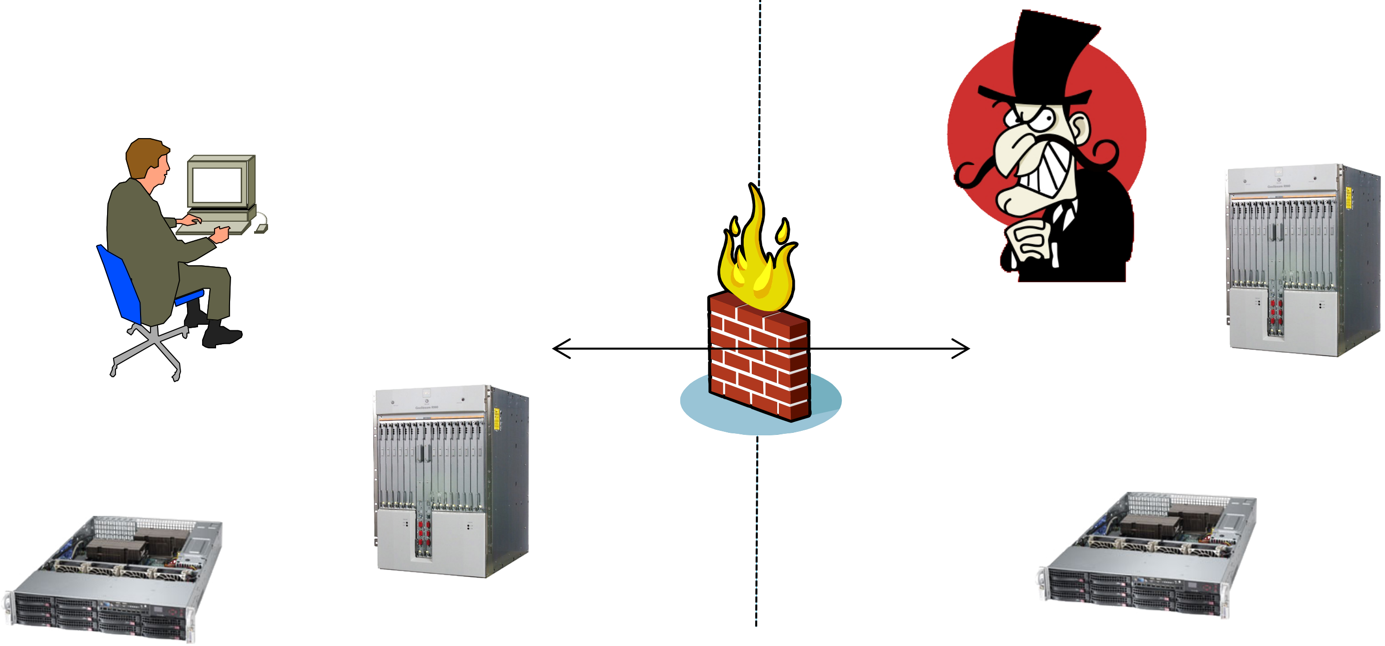
Firewall

Inside

- “good” users
- the same security policy

Outside

- bad/untrusted users



Why Use Firewalls?

- Firewalls are a *scalable* solution: you don’t have to manage many boxes
- Firewalls are under your control
- Usual purpose: keep attackers away from buggy code on hosts
- Generally speaking, firewalls are *not* network security devices; they’re the network’s response to buggy, insecure hosts
  - A suitably hardened host isn’t helped much by a firewall

Policies

- Firewalls can enforce policies at any layer of the network stack
- Accept/reject MAC addresses, IP addresses, port numbers, various forms of application content, etc.
- Policies reflect organizational needs
  - General philosophy: accept “safe”, *necessary* traffic; reject all else

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Link
1	Physical

Firewalls Implement Policy

- If you do not have a security policy, a firewall can’t help you
  - Firewalls are not magic security devices
  - Simply having one doesn’t protect you; what matters is the policy they enforce
- If there is no single policy for the entire network, a firewall doesn’t do much good
  - Example: ISP networks can’t be firewalled, because every customer has different security needs and policies
  - But—the ISP’s own computers can be firewalled

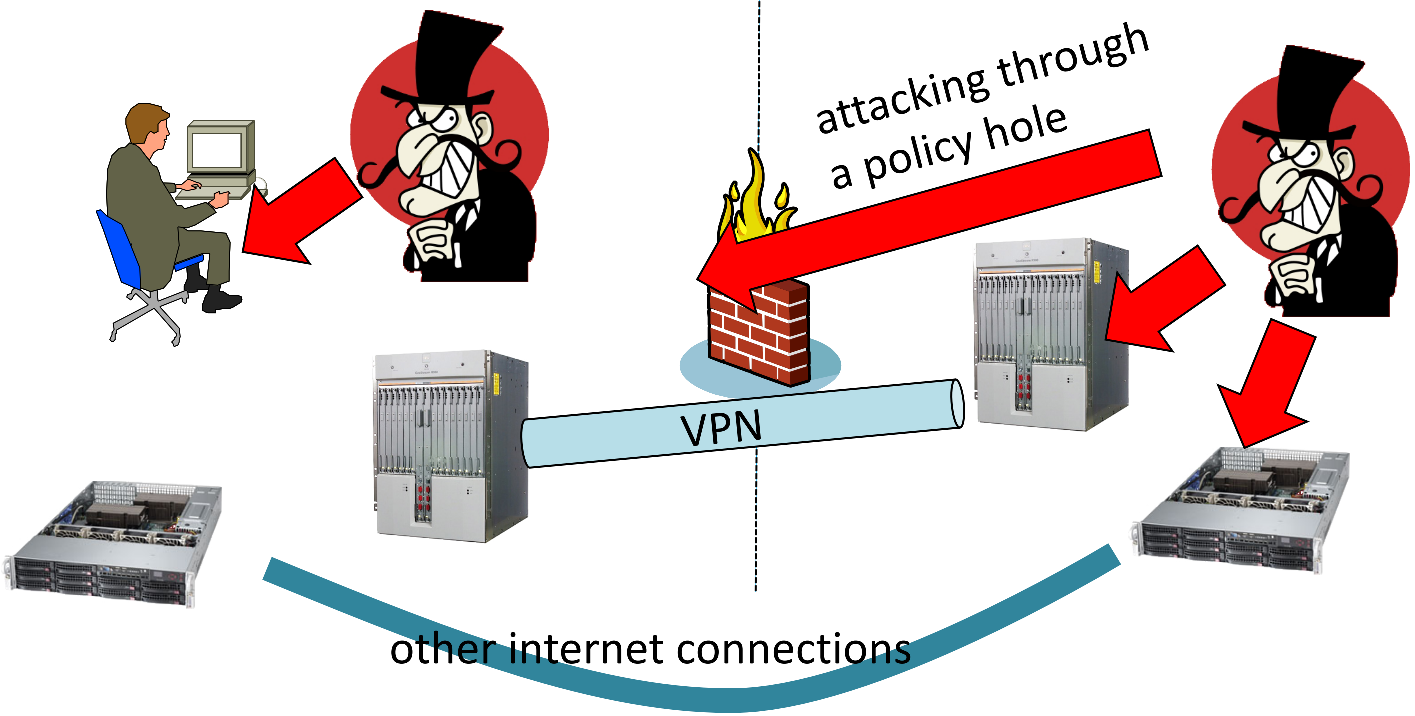
failure models

Inside

Firewall

Outside

- “good” and “bad” users
- exceptions and complex policy



attacking through a policy hole

VPN

other internet connections

Some Sample Policy Rules

- Allow inbound TCP port 25 (SMTP) destined for the mail host
- Block and log outbound TCP port 25 unless it’s from the authorized mail host
- Allow outbound TCP ports 80 or 443

or…

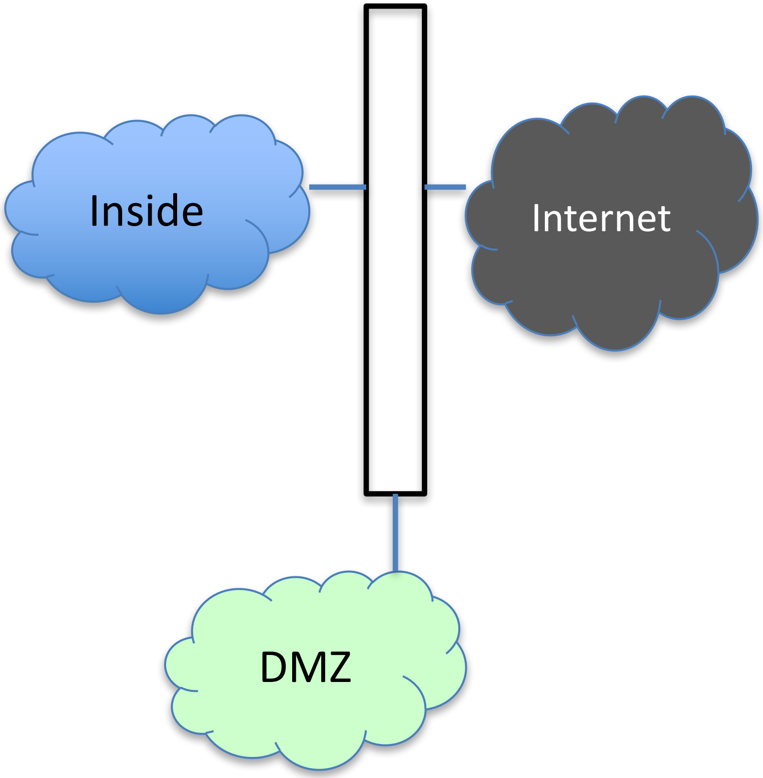
Allow outbound TCP ports 80 or 443 only from the designated web proxy

Crafting Policy Rules

- A complex process: must balance business needs against network threats
  - Both are constantly changing
  - Generally, no single person knows both well
- It’s easy to get it wrong; both the policy and its implementation can have errors
- Iterative process: deploy a set of rules, and watch for errors and complaints
  - Check your log files and flow records!

Topology

- Three classes of nets: untrusted (the outside), trusted, and semi-trusted (DMZ="Demilitarized Zone")
- Service hosts—mail, DNS, web, etc.—go in the DMZ
  - Mostly protected from the outside, but not fully trusted because of outside exposure



Implementing Firewalls

- Any router or Linux/BSD host can filter at layers 3 and 4
- The real troubles are higher up: emailed viruses, infected PDFs, web pages with Javascript that exploits browser bugs, and more
- Some protocols, e.g., FTP and SIP, can’t be handled just at the lower layers, because they require other ports to be opened up dynamically
- *Must* have application proxies for many protocols; either rules or mechanisms must be able to divert traffic to these proxies

The Trouble with Firewalls

- There is too much connectivity that doesn’t fit the simple model
  - Special links to customers, suppliers, joint venture partners, contractors, etc.
  - Very many connections to the outside
  - Branch offices
  - Laptops and smartphones!
- Different threat models
- The classic model of the firewall doesn’t work that well any more for large organizations

Mobile Devices

- By definition, mobile devices sometimes live outside the firewall
- This is necessary if people are to get their jobs done
- But they have to have inside connectivity (or at least sensitive inside data), too
- Risk: devices can be compromised when outside, and bring the infection home
- Risk: devices can be stolen

Firewalls and Threat Models

- Firewalls generally (but not always) deflect unskilled hackers
- Opportunistic hackers may or may not be kept out; they can often penetrate a single inside host and work from there
- Disgruntled employees are already on the inside
- Intelligence agencies won’t be kept out by simple schemes
  - The NSA reputedly has canned tools to attack common commercial firewalls

What to Do?

- Multiple layers of defense
  - Large, enterprise firewall to protect the company, complete with central service hosts
  - Departmental firewalls to isolate printers, file servers, etc.
  - Hardened hosts, plus automated tools to maintain them
  - Lots of logging and monitoring