Defending Computer Networks
Lecture 9: Worms/Firewalls

Stuart Staniford

Adjunct Professor of Computer Science

Quiz

- Half hour (10:12-10:42am)
- No notes/laptops/tablets/phones/etc
- Write name/net-id at top

New Assigned Reading

- Bellovin and Cheswick. *Network Firewalls*. http://people.scs.carleton.ca/~soma/id/readings/bellovin-firewalls.pdf

Latest News

US regulator raises alarm for 'Armageddon-type' cyber attack

Several prominent US firms including Target, Home Depot and JP Morgan have suffered data breaches in the past year

After a year of prominent hackings of millions of US credit and debit cards, one of the top regulators regulators of the American financial system has said that the prospect of an "Armageddon-type cyber event" is one of the most significant issues he plans to address in the next year.

New York State Department of Financial Services chief Benjamin Lawsky presides over an agency that is three years old and has pushed for harsher fines and executive accountability for banks including Standard Chartered and BNP Paribas.

On Monday, Lawsky said the technological vulnerabilities of the financial system are a pressing and potentially catastrophic problem.

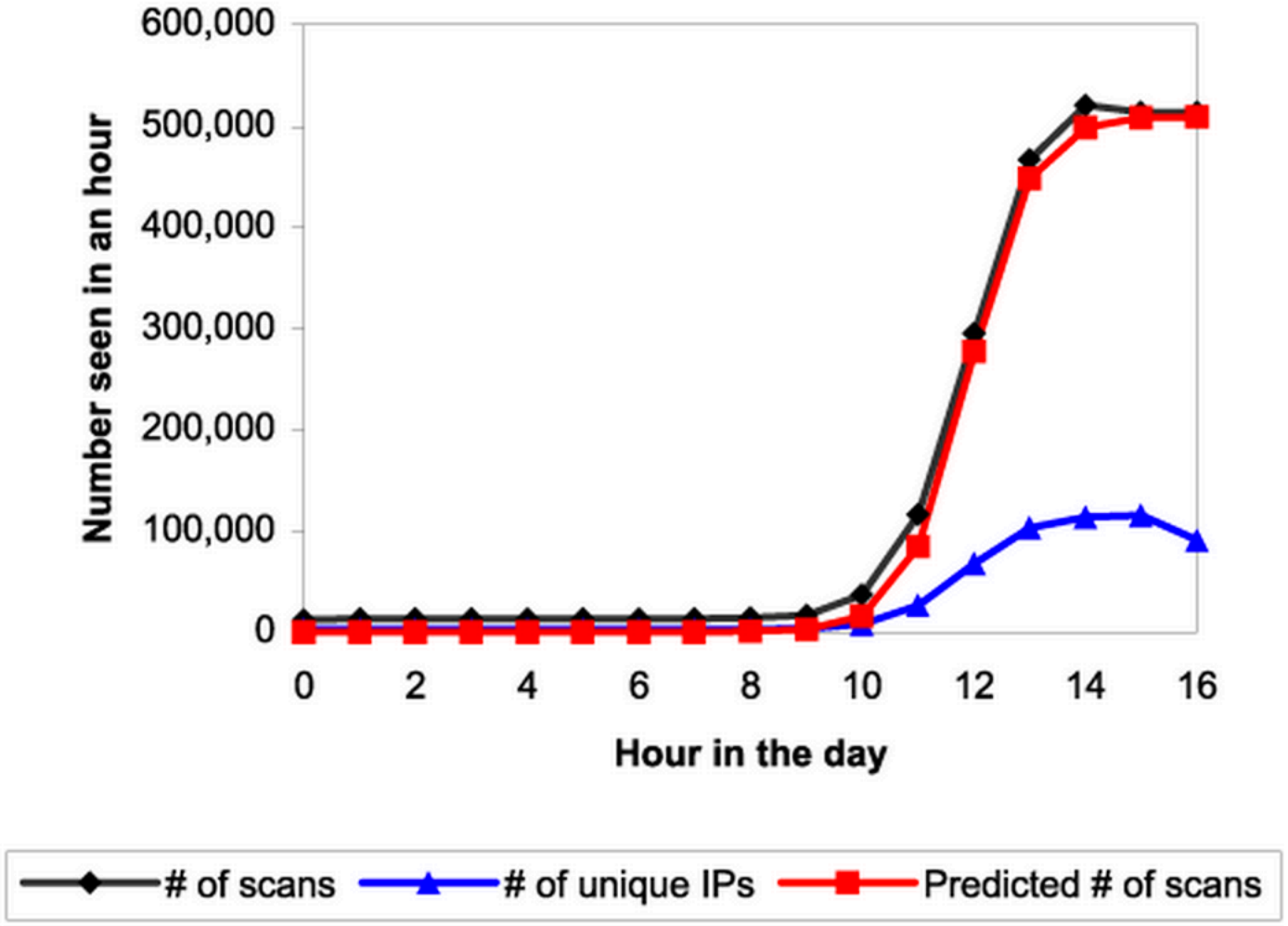
"I worry that we're going to have some sort of major cyber event in the financial system that's going to cause us all to shudder, an Armageddon-type cyber event," Lawsky said at the Bloomberg Link Most Influential Summit.

http://www.theguardian.com/technology/2014/sep/22/us-regulator-armageddon-type-cyber-attack

Main Goals for Today

- Finish up worms
- Maybe start firewalls.

Refresh on Scanning Worms



K = 1.8/hr

Defenses for Scanning Worms

- Host-level:
  - ASLR/DEP/Canaries/etc
  - Limit outbound connections
- Network level
  - Detect/block scanning
    - Firewalls
    - Packet filtering in routers
    - Intrusion prevention systems
    - In-switch security measures

Overall Dynamic

- Suppose each worm finds r children to infect
  - Total before containment/remediation.
- Successive generations:
  - 1, r, r^2, r^3,…
  - $1 + r + r^2 + r^3 + \ldots = 1/(1-r)$ if $r<1$
  - Eg if r = 0.9, total is 1/(1-0.9) = 10
  - If r > 1, series diverges.
- So must ensure each worm instance finds on average less than 1 child
  - Epidemic peters out
  - Known as “epidemic threshold”
  - Similar to critical mass in nuclear explosions

Email Worms (1999)

- Mostly scourge of late 90s/early 2000s
  - Melissa – Microsoft Word Macro "Worm"
    - Word document attachment to email
    - Used a large variety of enticing subject lines to emails to try to get users to open attachment.
      - Very first version claimed to have passwords to porn sites.
      - Various 'social engineering' hooks to get you to open it
    - Some say not a worm, depending on whether macro language is a "program" or not.
    - Stole address book and mailed itself out

I Love You (2000)

- Subject ILOVEYOU
- Attachment “LOVE-LETTER-FOR-YOU.txt.vbs”
- Scoured address book, so appeared to come from someone you knew.
  - *Many* people opened.
  - Believed to have affected tens of millions of computers.

Email Worms in General

- Are “topological” worms
  - Find their victims using the natural topology of a protocol communication graph
    - In this case email address books
- Use ‘social engineering’
  - Tricking human users into doing something they shouldn’t.
  - In theory could use exploit in mail client, but hasn’t been seen on a large scale.

Email Worm Defenses

- Anti-virus scanning of attachments
- Anti-spam screening of inbound emails
- User education.
  - Including warnings when opening strange attachments.
- Email worms appear not to spread as much any more.
  - Defenses must keep below epidemic threshold.
  - Except…

Storm Worm (2007)

- Used subject lines like
  - "230 dead as storm batters Europe"
  - And many, many others tied to current events
- Had an executable attachment.
  - Defeated AV by "repacking" the exe every 10 minutes.
- Successfully built a large botnet
  - Probably for Russian organized crime.
  - Millions, maybe tens of millions of infected IPs.
- So email worm probably not permanently dead.

Stuxnet Worm

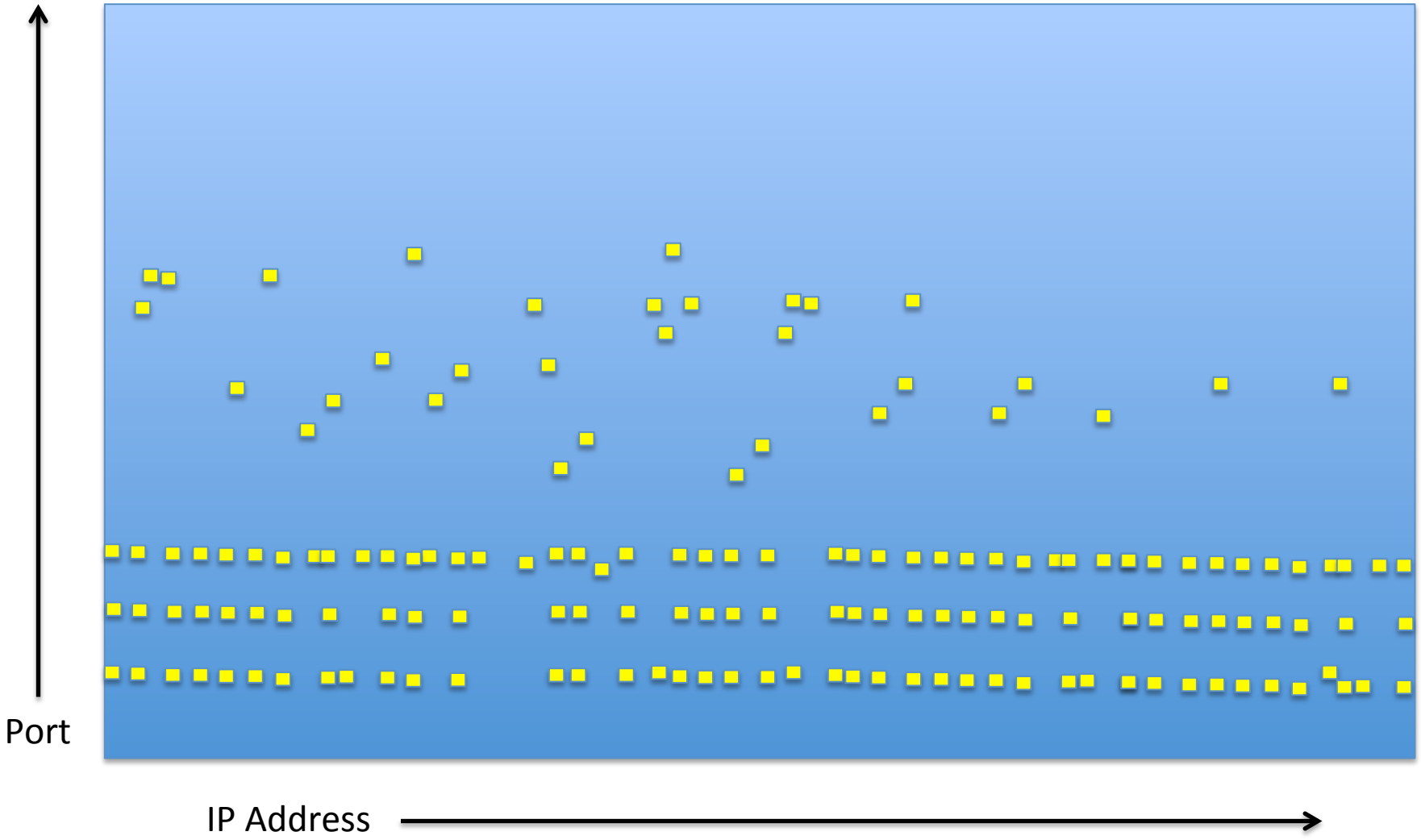
- Discussion today is focussed on spread, not payload.
- Likely target of worm:
  - industrial controllers for centrifuges in Iranian nuclear plant (goal: damage/destroy them).
- Need to
  - Get on internal corporate networks of Iranian entities
  - Get on air-gapped SCADA networks.
  - Find machines attached to right controllers
  - Execute real payload.
- Worm was used as the search strategy to find and cross the bottlenecks.
  - Apparently worked: caused extensive delay to Iranians.

Stuxnet Strategies

- Propagate through any network shares identifiable on accounts of infected computer.
- Zero-day print spooler vulnerability.
- Target hard-coded password in Siemens WinCC (SQL database) product.
- Windows server service vulnerability.
- Ability to infect USB drives.
  - Targetted a Windows vulnerability when viewing the folder on the drive.

Firewalls

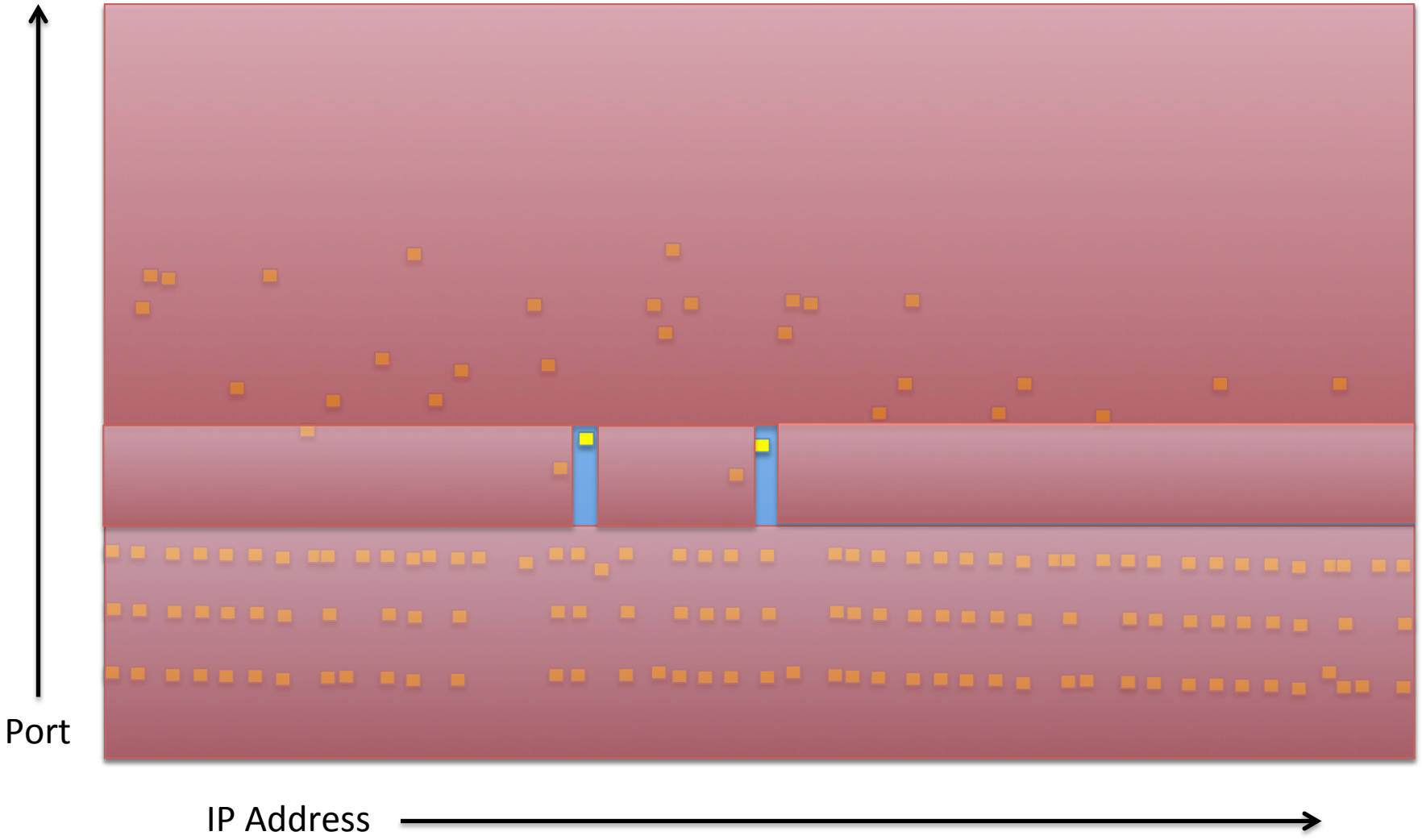
Open Network From the Internet



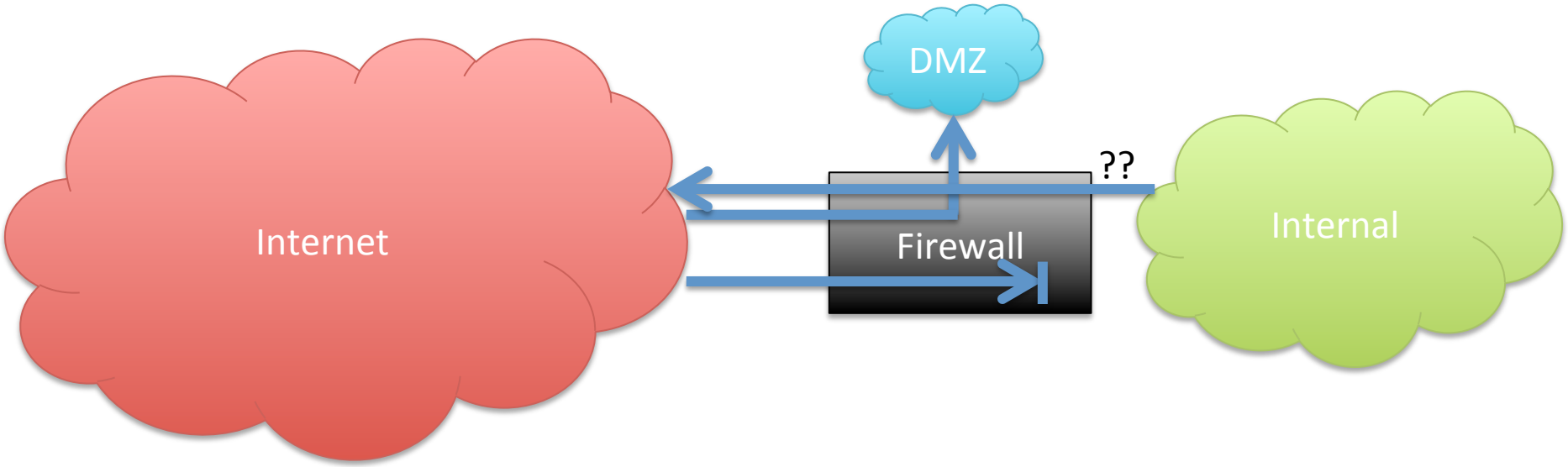
Scale of the Problem

- Big network might have $O(10^5)$-(10^8) machines
- Most will have some open ports
- Many, many versions of many, many codebases.
- Many different departments with differing needs/politics.
- Extremely hard to keep everything patched/ configured correctly
- But trivial to scan/exploit from the internet.

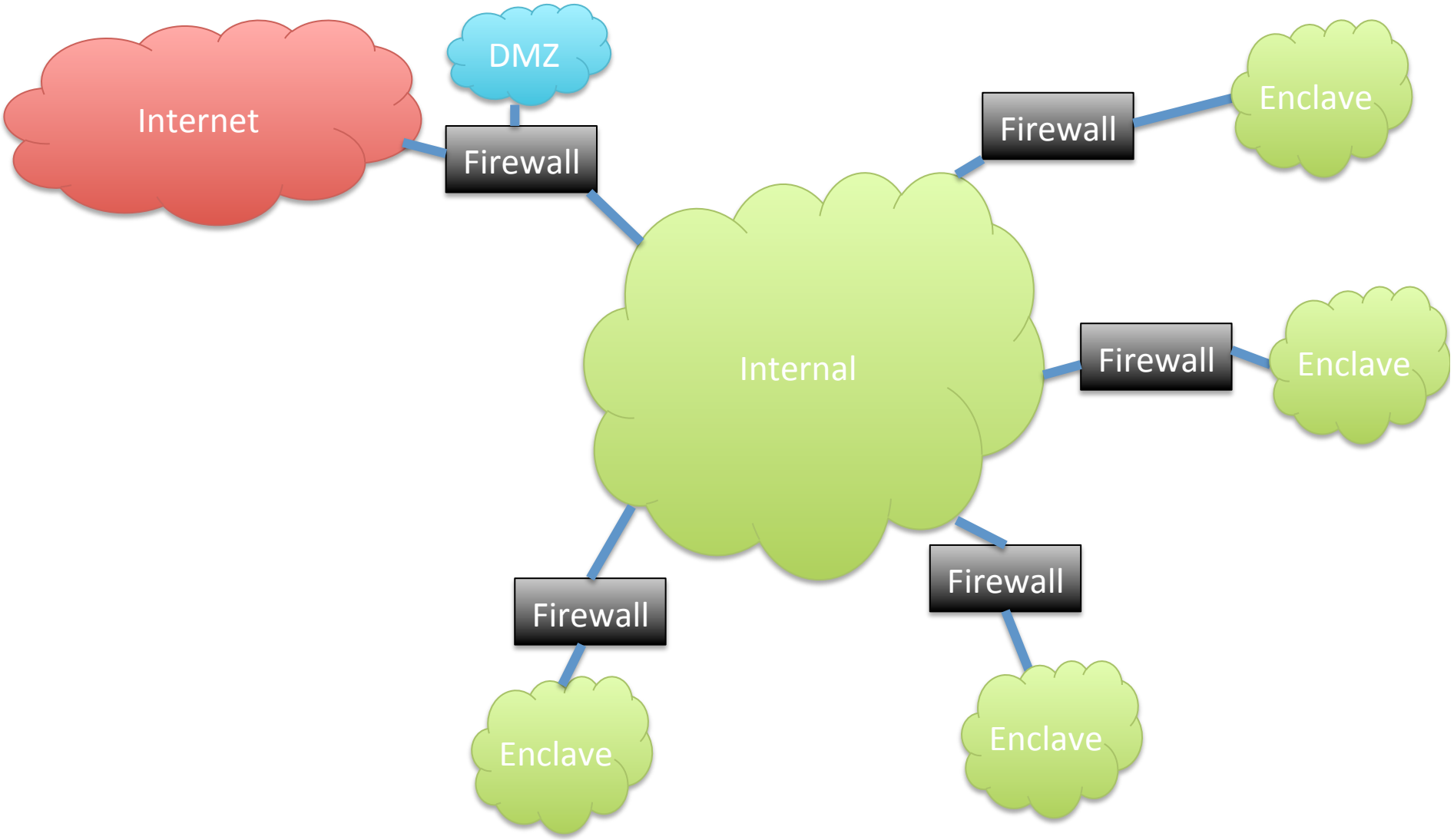
Establish Central Control



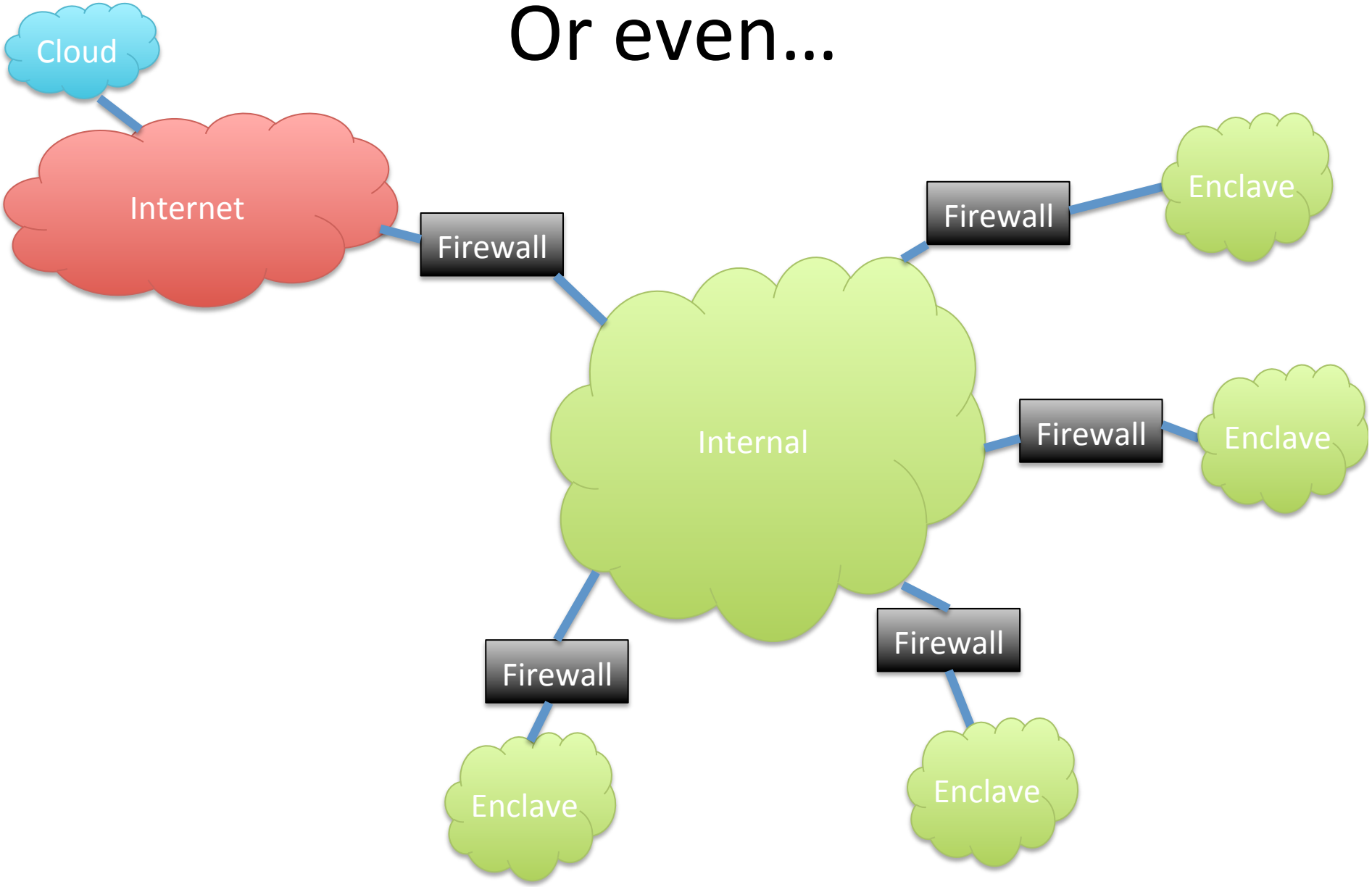
Better Yet



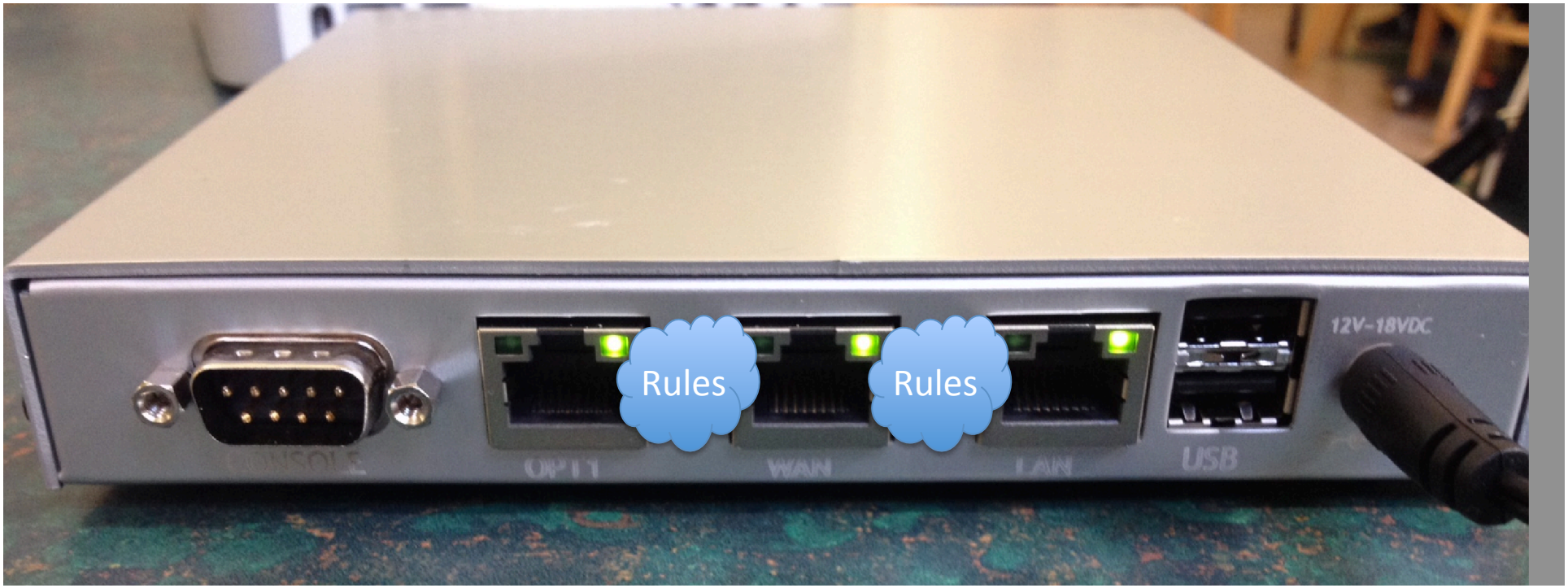
Or…


Internet
DMZ
Firewall
Firewall
Enclave
Internal
Firewall
Enclave
Firewall
Firewall
Enclave
Enclave

Or even…


Cloud
Internet
Firewall
Internal
Firewall
Enclave
Firewall
Enclave
Firewall
Enclave
Firewall
Enclave

Firewall Basic Concept



(This is Netgate M1N1Wall – low-cost, low-power open source firewall using FreeBSD/pfSense. Runs on AMD Geode cpu.)

Typical Firewall Rule

- Block in on LAN from 192.168.1.0/24 port any to 0.0.0.0/0 port 53
  - Any packets coming from LAN to port 53 will be dropped.
    - Effect of rule in isolation
    - Could be part of strategy to force clients to use only officially sanctioned DNS servers

Firewall Rulesets

- Typically a significant number of rules, that together enforce the policy.
- Some firewalls take “last match” as dispositive, others take “first match”.
- Generally want first/last to be “block all” to ensure only permitted traffic is allowed.
- Stateful firewalls apply rules only to first packet of connection,
  - then will allow rest of connection to proceed
  - Performance benefit: looking up in flow table much faster than applying all of rules to packet.