Defending Computer Networks
Lecture 10: Firewalls

Stuart Staniford

Adjunct Professor of Computer Science

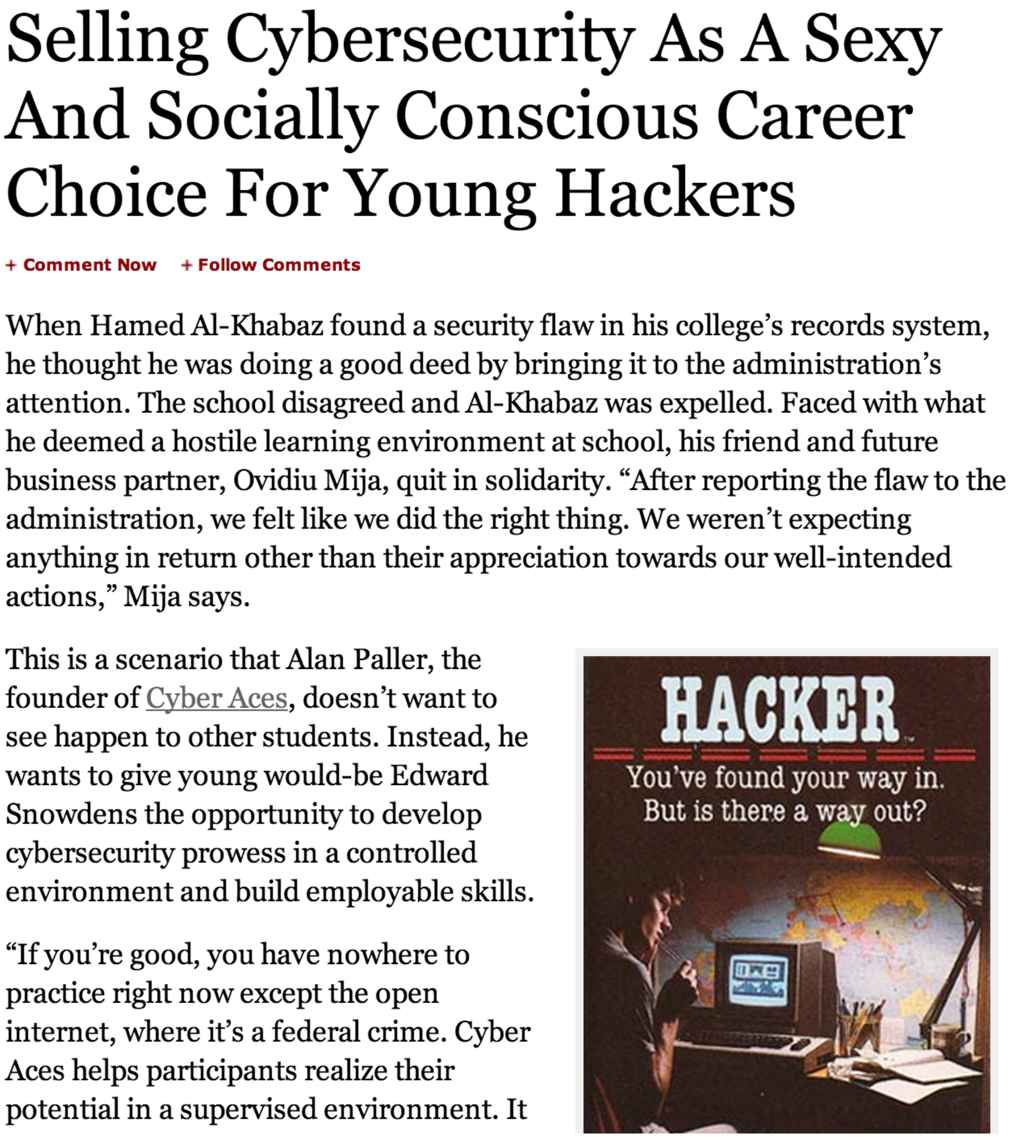
Logistics

- October 8th: Cornell ITSO office guest lecture
  - Wyman Miles/Glenn Larratt/Dan Valenti
- Reminder that guest lectures are part of syllabus and may be quizzed on.

New Assigned Reading

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

Latest News



Selling Cybersecurity As A Sexy And Socially Conscious Career Choice For Young Hackers

+ Comment Now + Follow Comments

When Hamed Al-Khabaz found a security flaw in his college's records system, he thought he was doing a good deed by bringing it to the administration's attention. The school disagreed and Al-Khabaz was expelled. Faced with what he deemed a hostile learning environment at school, his friend and future business partner, Ovidiu Mija, quit in solidarity. "After reporting the flaw to the administration, we felt like we did the right thing. We weren't expecting anything in return other than their appreciation towards our well-intended actions," Mija says.

This is a scenario that Alan Paller, the founder of Cyber Aces, doesn't want to see happen to other students. Instead, he wants to give young would-be Edward Snowdens the opportunity to develop cybersecurity prowess in a controlled environment and build employable skills.

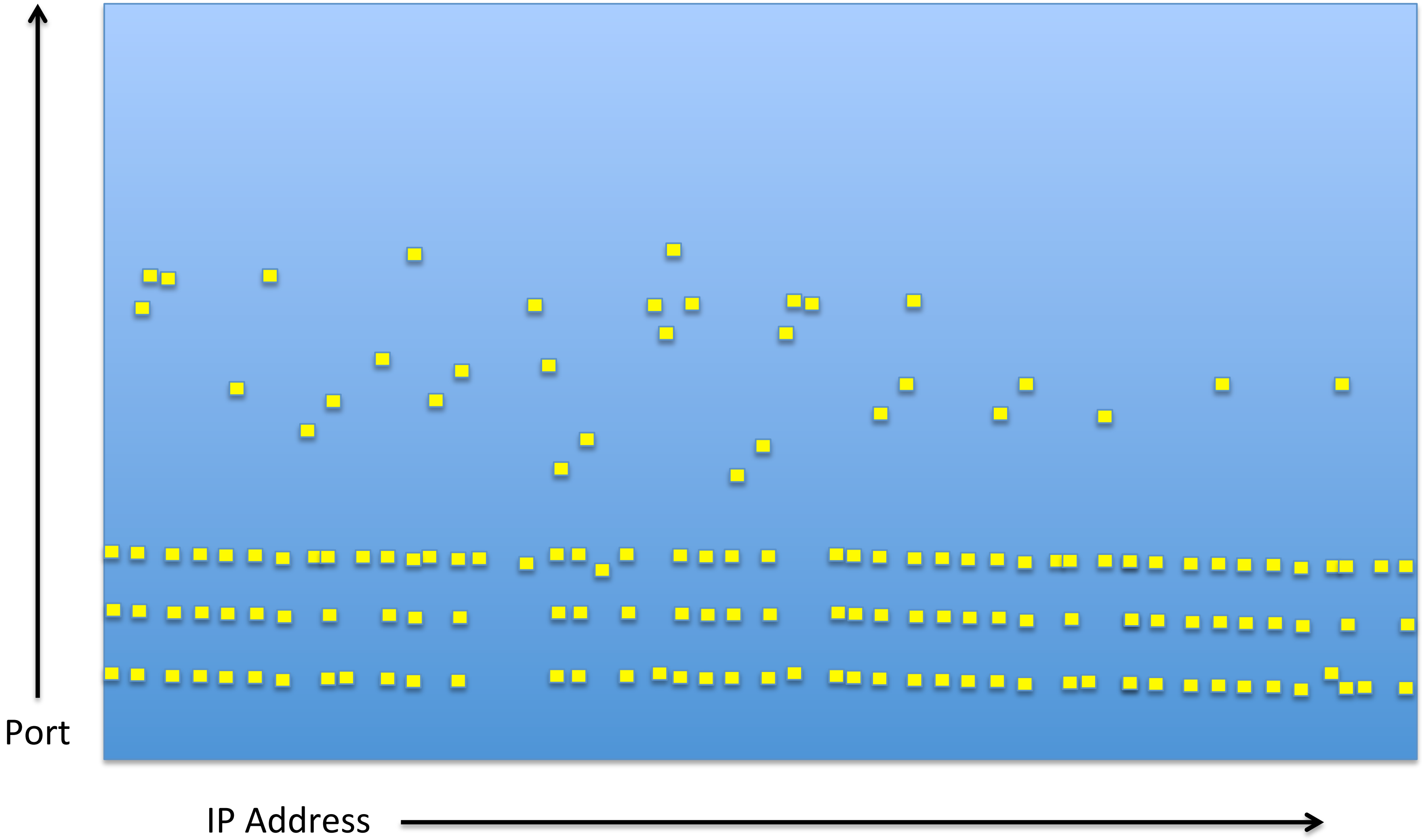
"If you're good, you have nowhere to practice right now except the open internet, where it's a federal crime. Cyber Aces helps participants realize their potential in a supervised environment. It

http://www.forbes.com/sites/jmaureenhenderson/2013/09/30/selling-cybersecurity-as-a-sexy-and-socially-conscious-career-choice-for-young-hackers/

Main Goals for Today

- Introduce the main ideas behind firewalls.

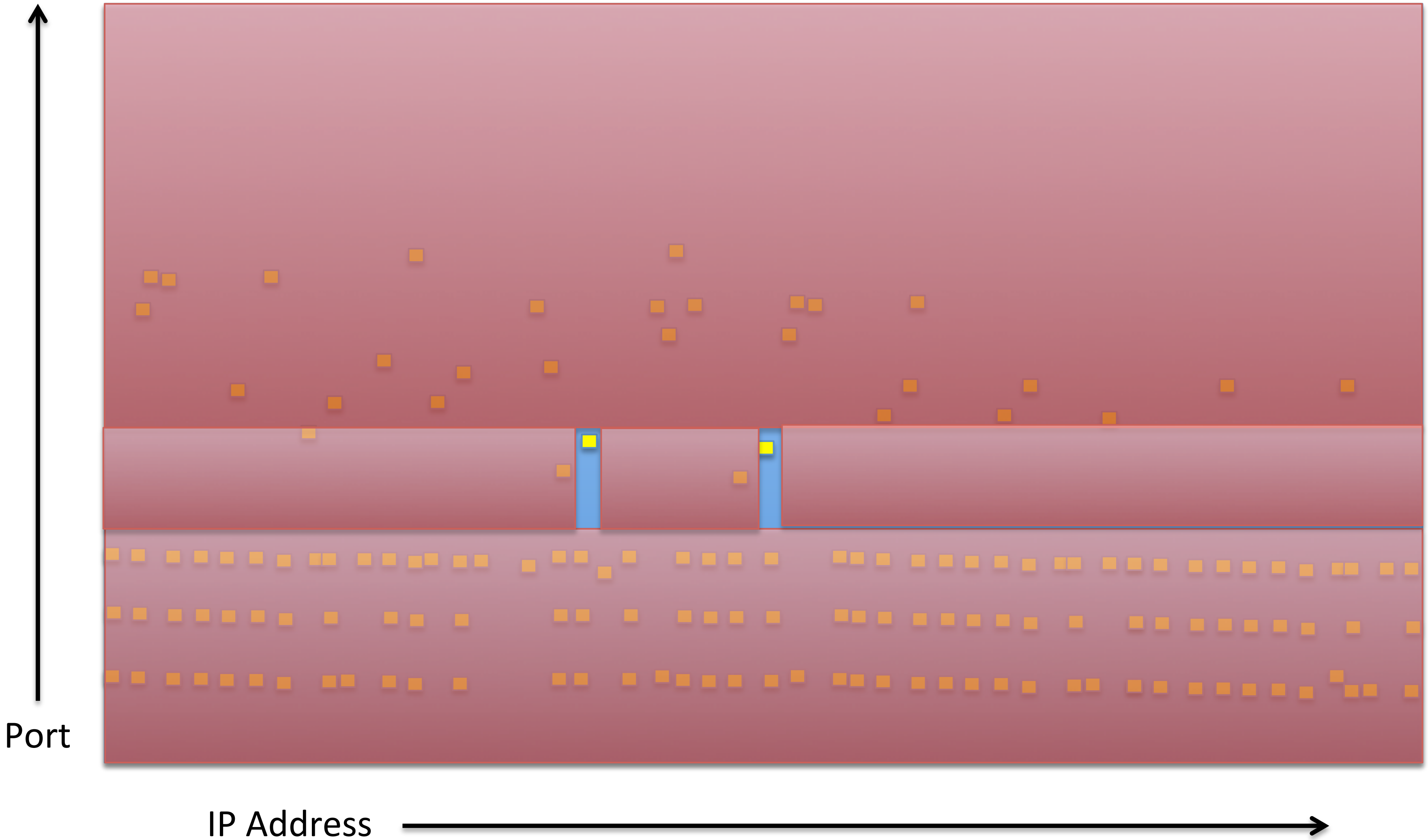
Open Network From the Internet



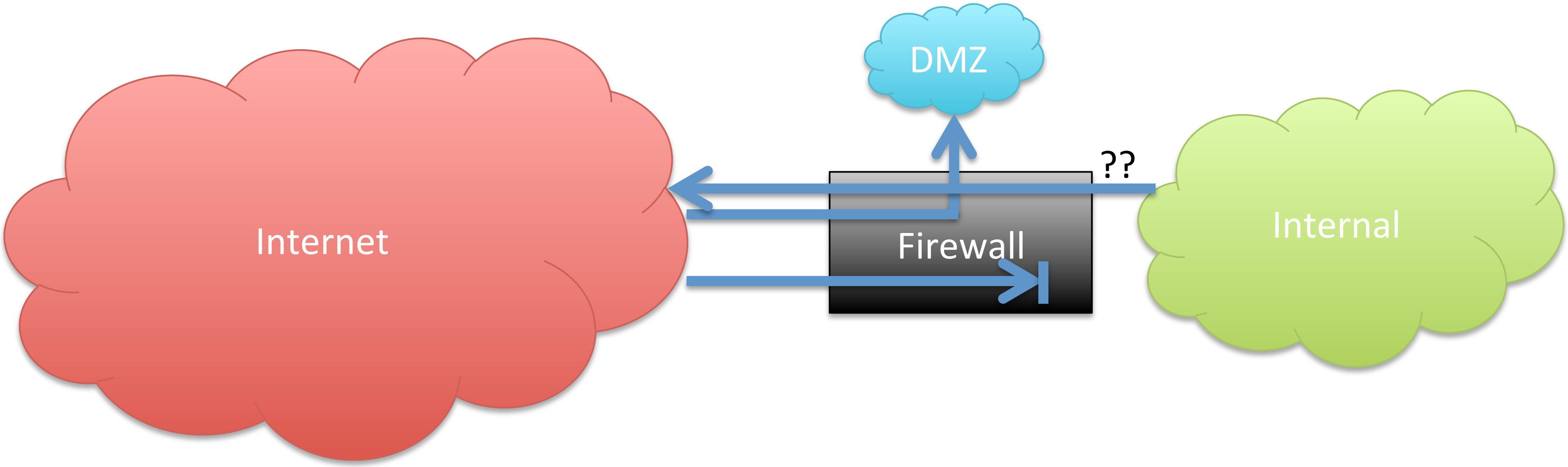
Scale of the Problem

- 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.

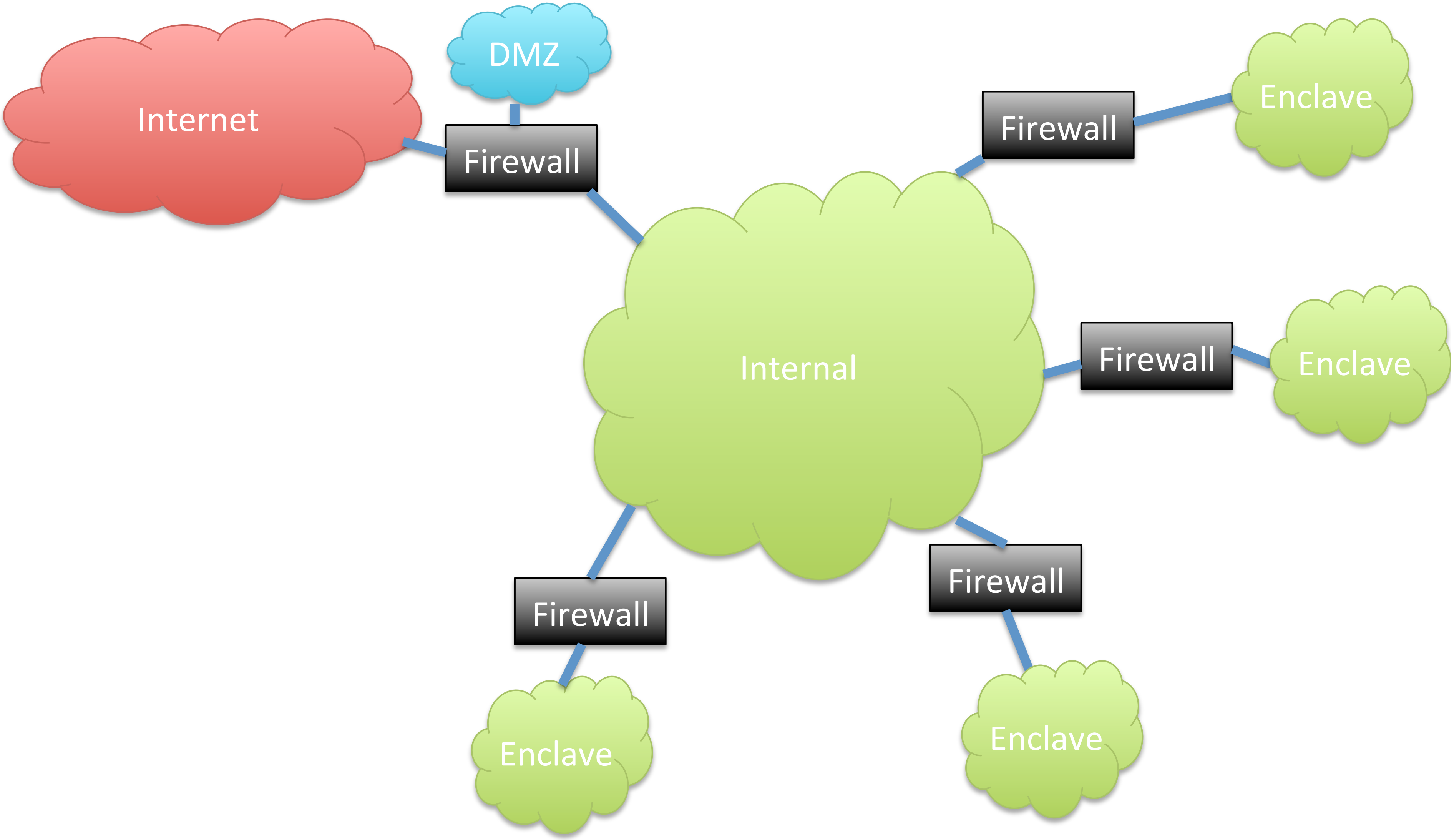
Establish Central Control



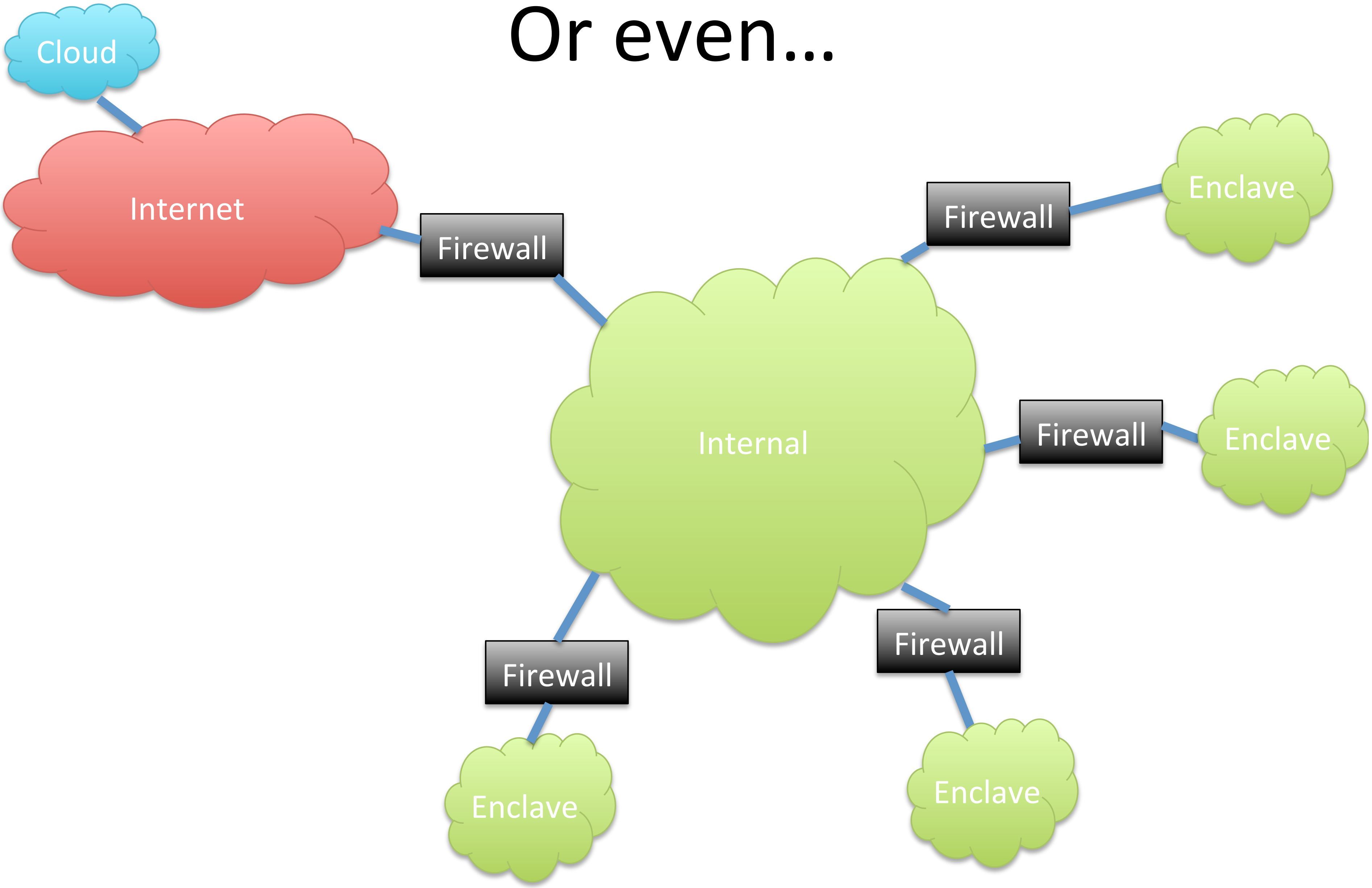
Better Yet



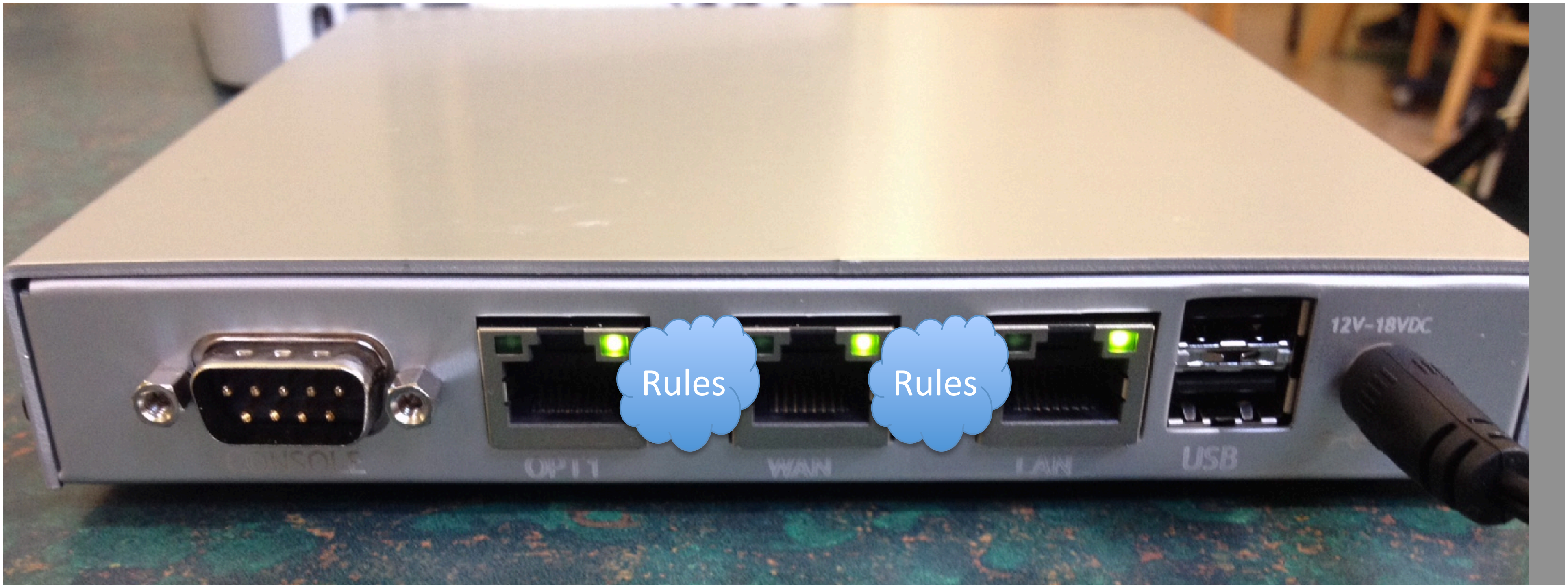
Or…


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.