Defending Computer Networks
Lecture 10: Firewalls

Stuart Staniford

Adjunct Professor of Computer Science

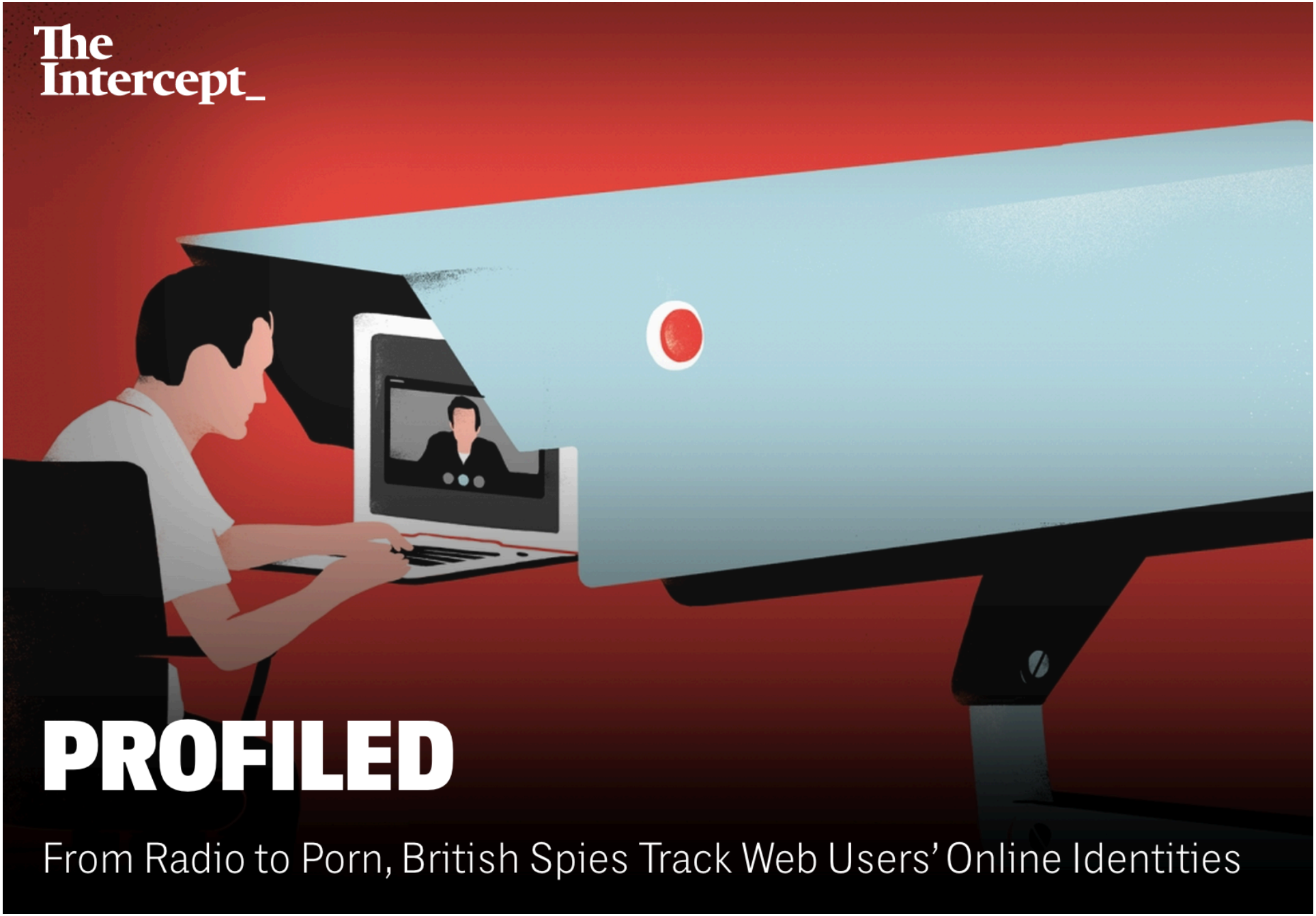
THE WALL STREET JOURNAL.

U.S., China in Pact Over Cyberattacks That Steal Company Records

By DAMIAN PALETTA

Updated Sept. 25, 2015 5:12 p.m. ET

WASHINGTON—The U.S. and China on Friday announced an agreement not to direct or support cyberattacks that steal corporate records for economic benefit, the result of lengthy negotiations and occasional threats from the White House amid a rapid increase in computer breaches.


The Intercept_
PROFILED
From Radio to Porn, British Spies Track Web Users' Online Identities

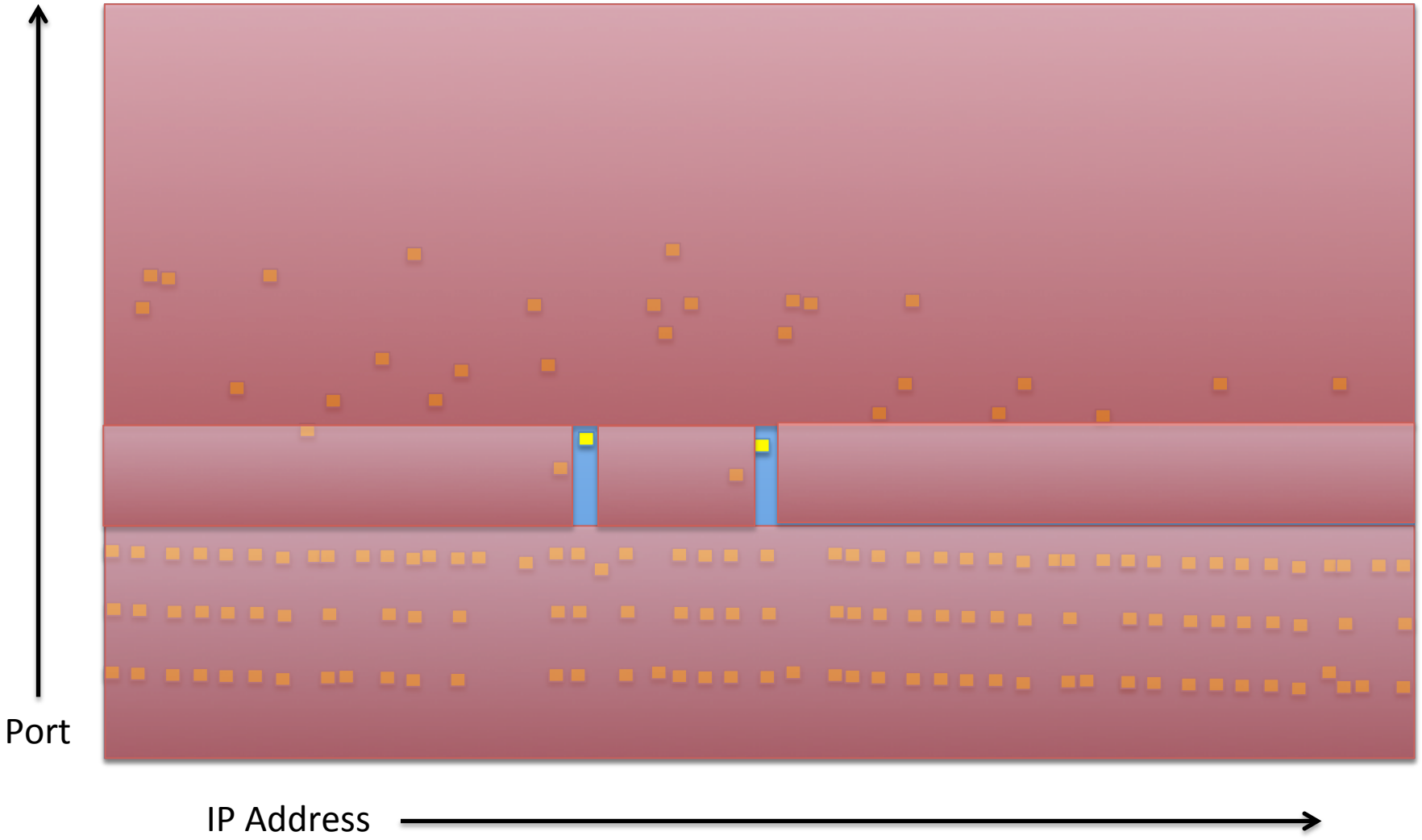
Before long, billions of digital records about ordinary people's online activities were being stored every day. Among them were details cataloging visits to porn, social media and news websites, search engines, chat forums, and blogs.

The mass surveillance operation — code-named KARMA POLICE — was launched by British spies about seven years ago without any public debate or scrutiny. It was just one part of a giant global Internet spying apparatus built by the United Kingdom's electronic eavesdropping agency, Government Communications Headquarters, or GCHQ.

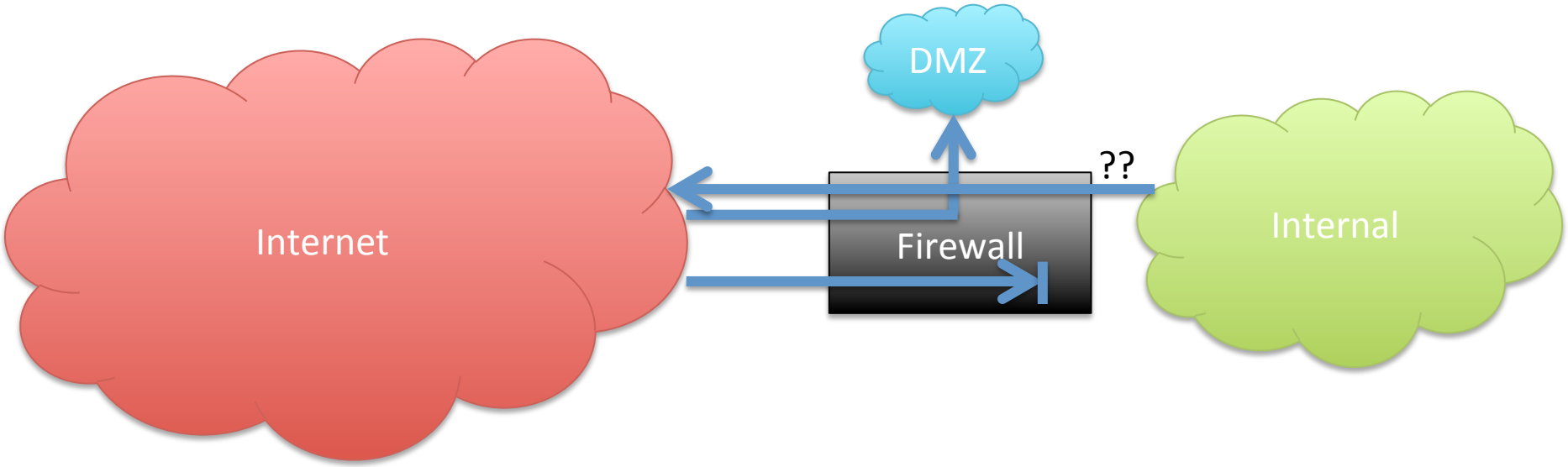
Main Goals for Today

- Firewalls.
- Maybe start Distributed Denial of Service.

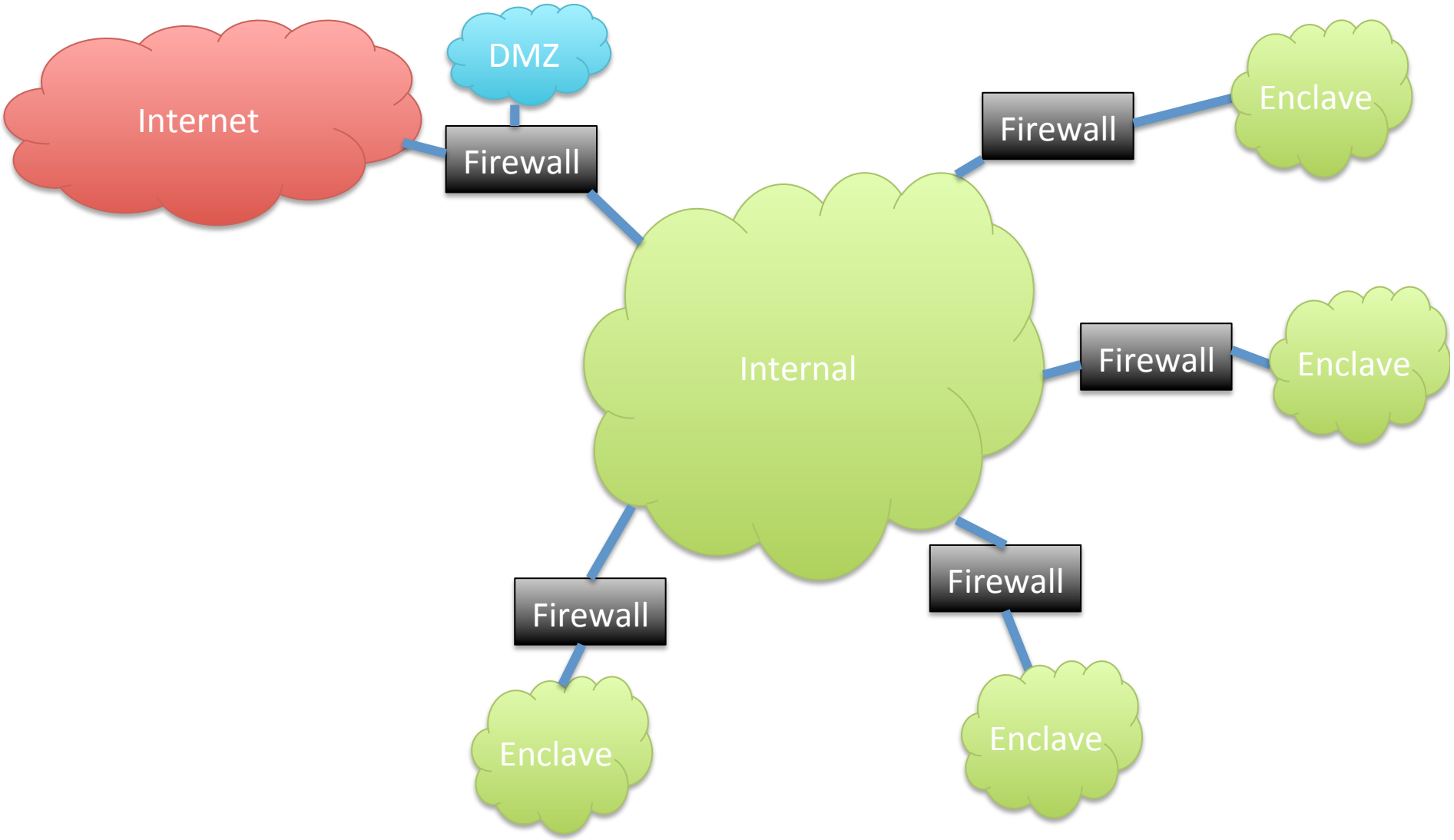
Establish Central Control



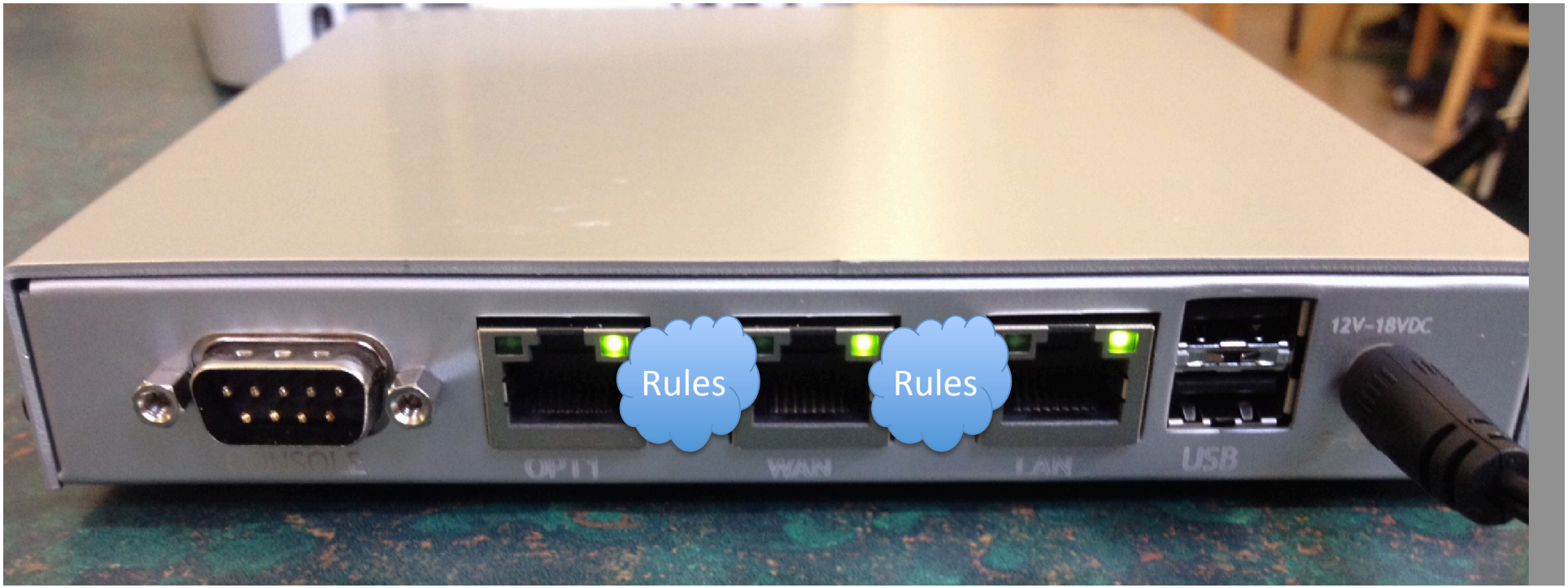
Better Yet



Or…


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

Firewall Basic Concept



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

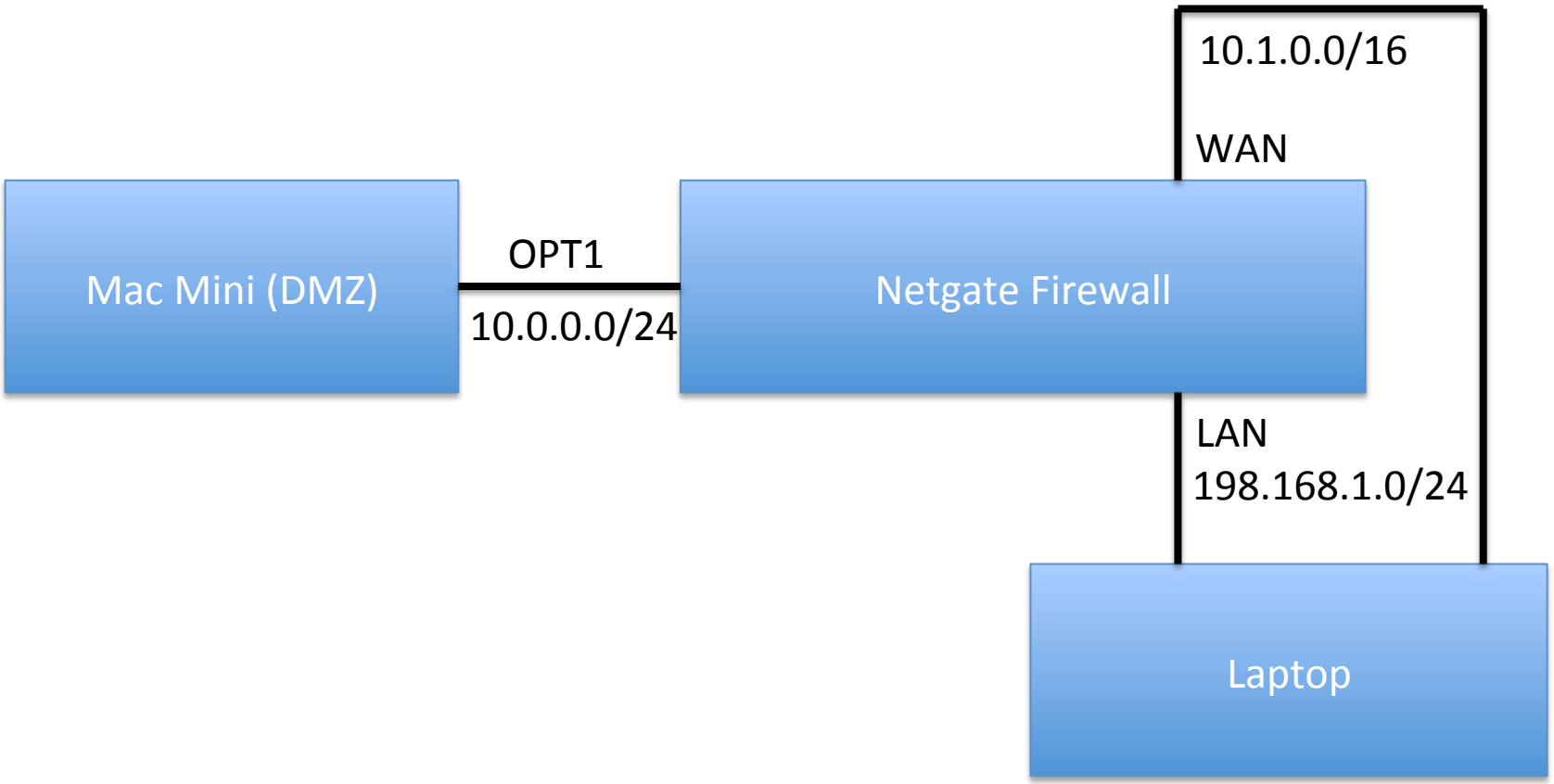
Typical Firewall Rule

- 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.

Firewall Demo Wiring Diagram



Tour of a Firewall GUI

- Dashboard
  - Let's check basic setup
    - Check IP addresses on laptop match
    - Dashboard
    - Routes correct
    - Make sure we can ping Mac Mini from firewall
    - Check arp table
    - Make sure we can ping Mac Mini from LAN network.
    - Have a quick look at state table

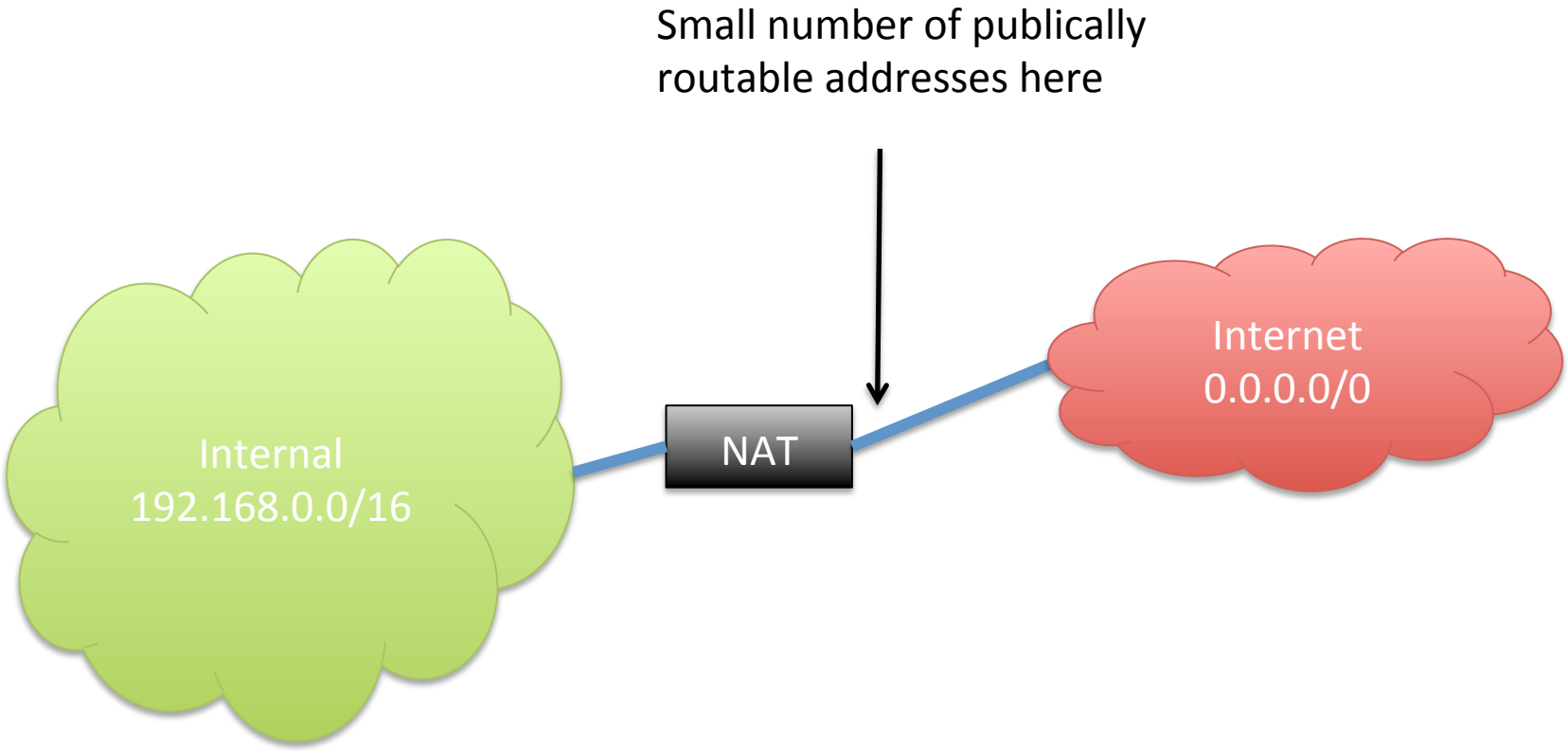
Firewall Rules

- Inspect the Rules
- Nmap through the firewall from WAN
  - Unplug LAN wire
  - sudo nmap -Pn -n -sS –T5 10.0.0.2
  - Replug LAN wire
- Change a rule
- Nmap through the firewall and see we can no longer see ports
- Inspect the state table in the fw
- Add a rule to reject (reset) connections
  - See how the nmap result changes

Network Address Translation (NAT)

- RFC 1918
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- These addresses are not “routable”
- They will not be delivered across the Internet
  - Not allowed on there, technically.
- Need a special translator device at boundary
  - “NAT box” = Network Address Translation
  - Converts them to internet routable addresses

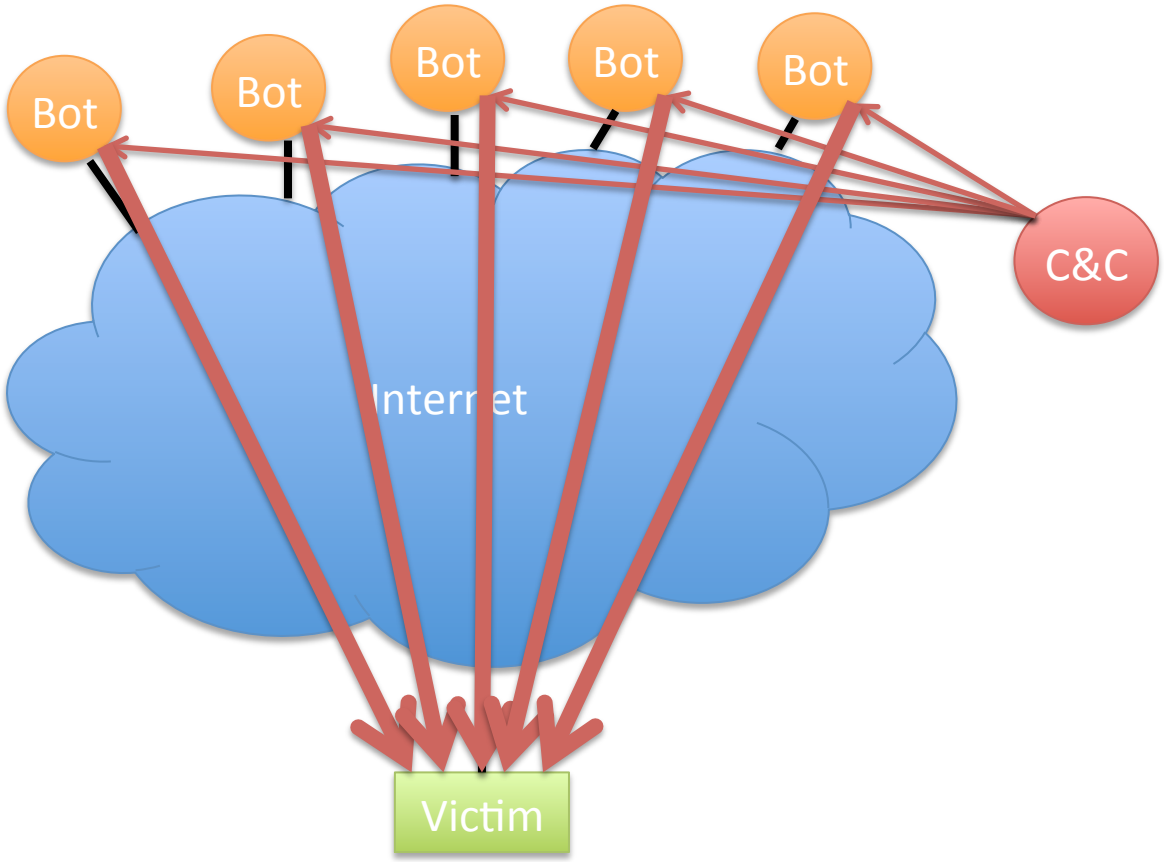
NAT Operation



DDOS – Distributed Denial-Of-Service

- Main goal
  - take out an Internet site (“denial of service”)
  - By flooding with bad traffic
  - From many source (“distributed”)
- Could also be used on internal network,
  - Not seen much so far, if at all.
  - Obvious cyber-war/cyber-terrorism tactic

Basic Setup of a DDOS Botnet



Illustrative only: practical attacks will have many more bots

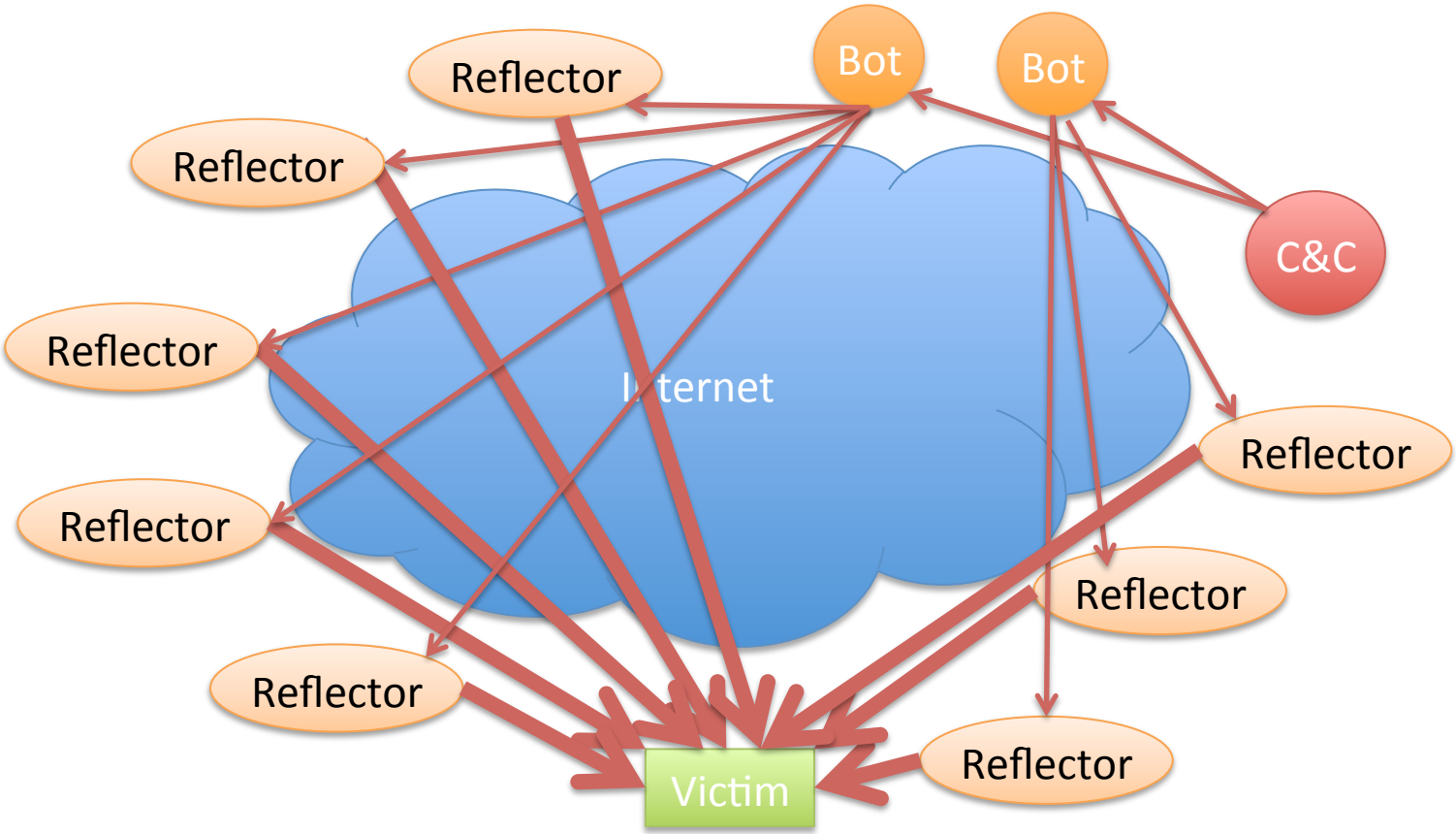
What Packets Should We Send?

- Ping flood
  - ICMP echo request
- Syn flood
  - Exploit limitations in handling of half-open connections in older stacks
- Genuine looking requests
  - The more genuine and randomized, the harder to block
- Application layer exploits
  - ASLR etc will prevent exploitation, but not crash

Reflectors

- A Reflector is anything that
  - If you send it a packet, will respond with pkts
  - Preferably lots of big packets
  - Then send it a packet with src spoofed as the victim
  - Get it to send lots of packets back to the victim
  - Can amplify a DDOS greatly
  - Also makes it harder to trace

Reflection Attacks



Illustrative only: practical attacks will have many more bots/reflectors

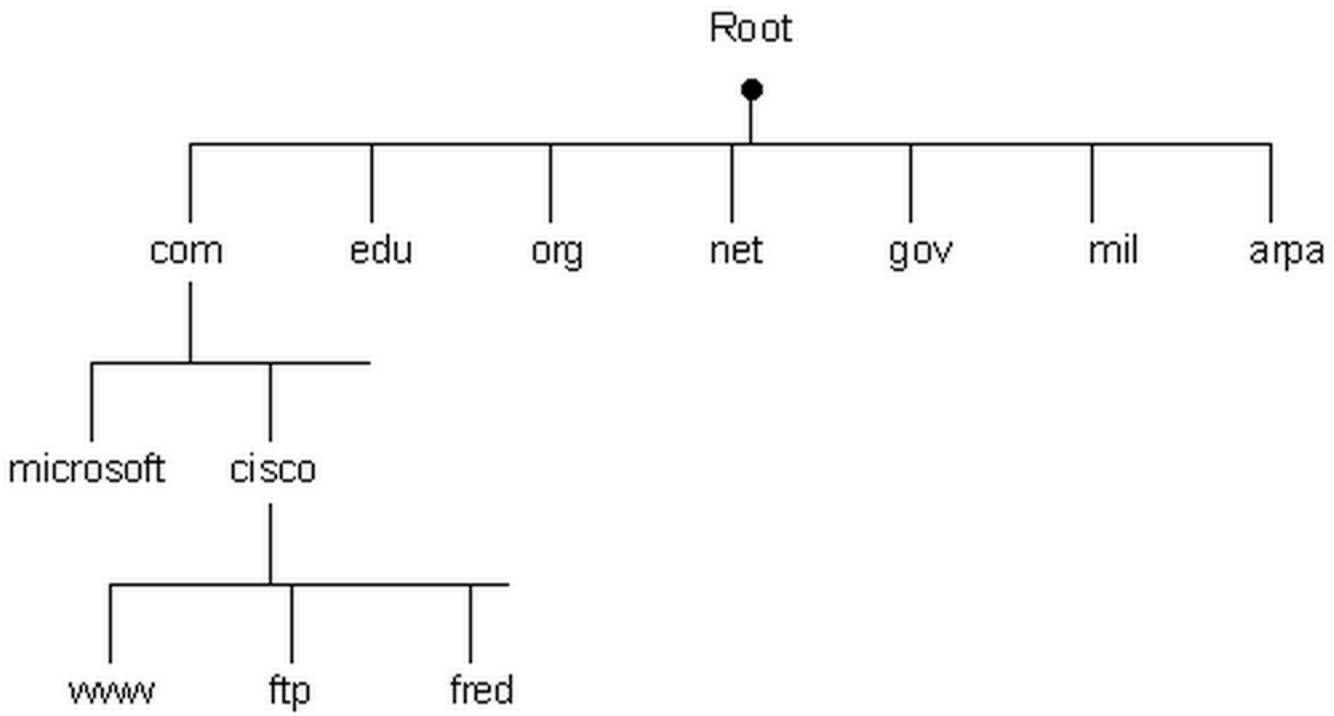
What Will Work as a Reflector?

- Any TCP host (send SA or R in response to S)
- ICMP (eg echo response to echo request)
- DNS – especially with recursion
  - Issue on campus recently
  - Let's look at this in more detail

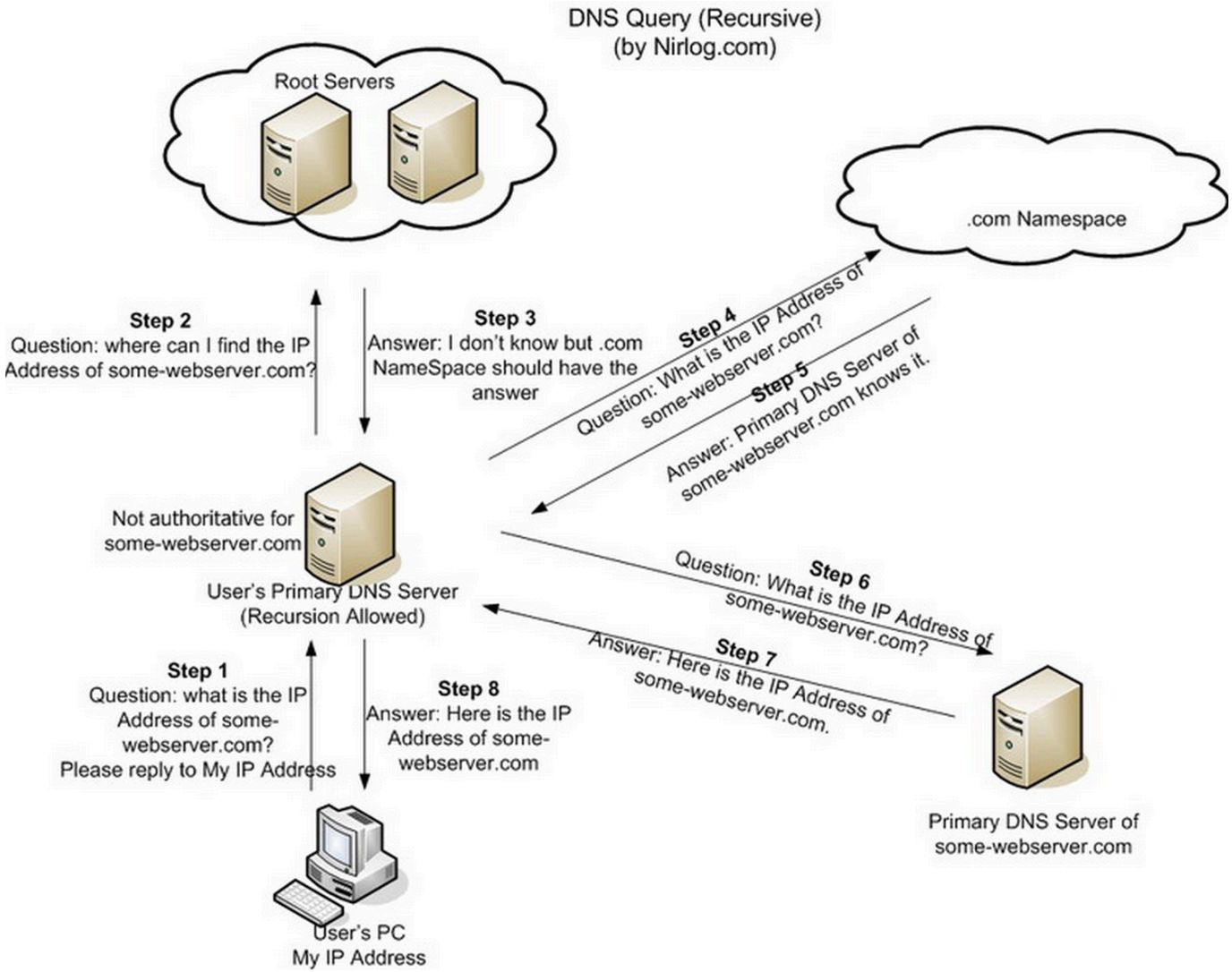
Domain Name Service

- Global Internet service to map names to IP addresses.
- Part of core TCP/IP suite of protocols
  - RFC 882 (1983) updated by RFC 1034 (1987)
  - Replaced manually maintained “hosts.txt” of all Internet connected computer’s IP addresses.
- Let’s do it
  - unplug from fw demo
  - dig www.nytimes.com

The DNS Hierarchical Name Tree

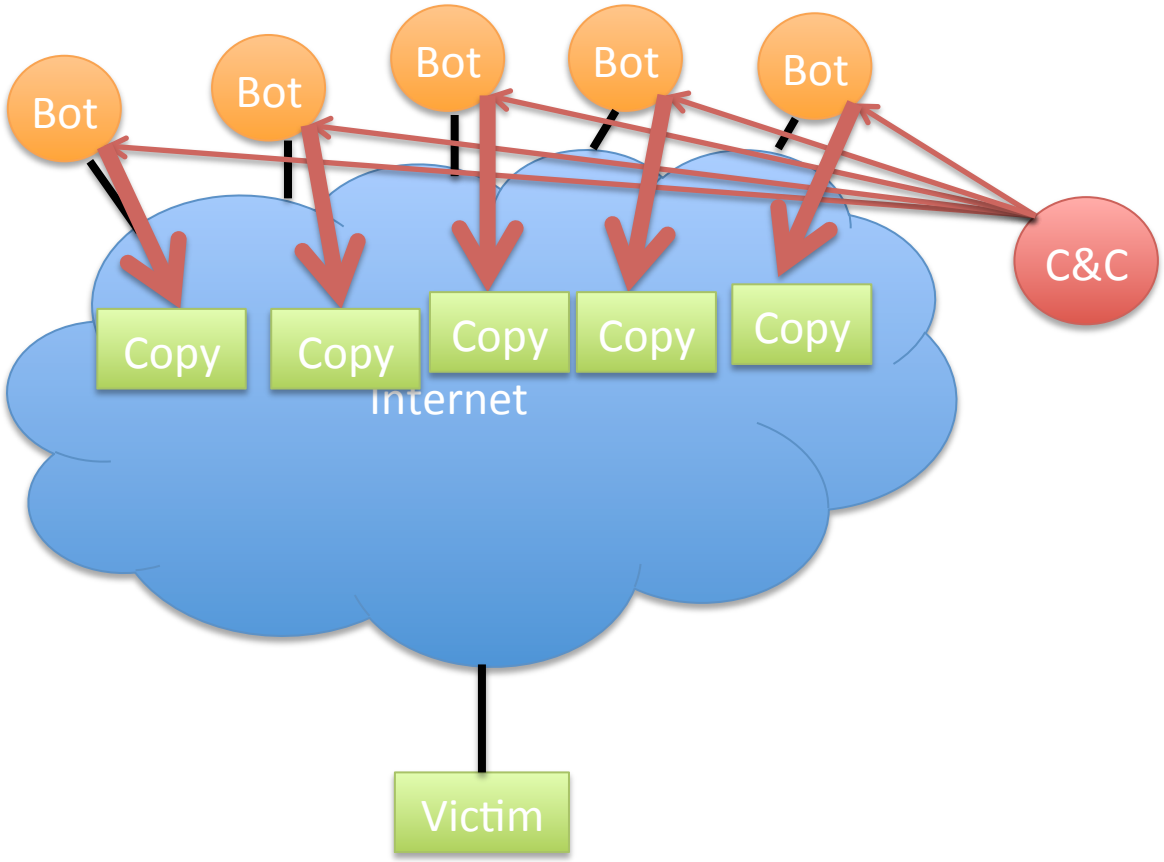


How a DNS Query Works

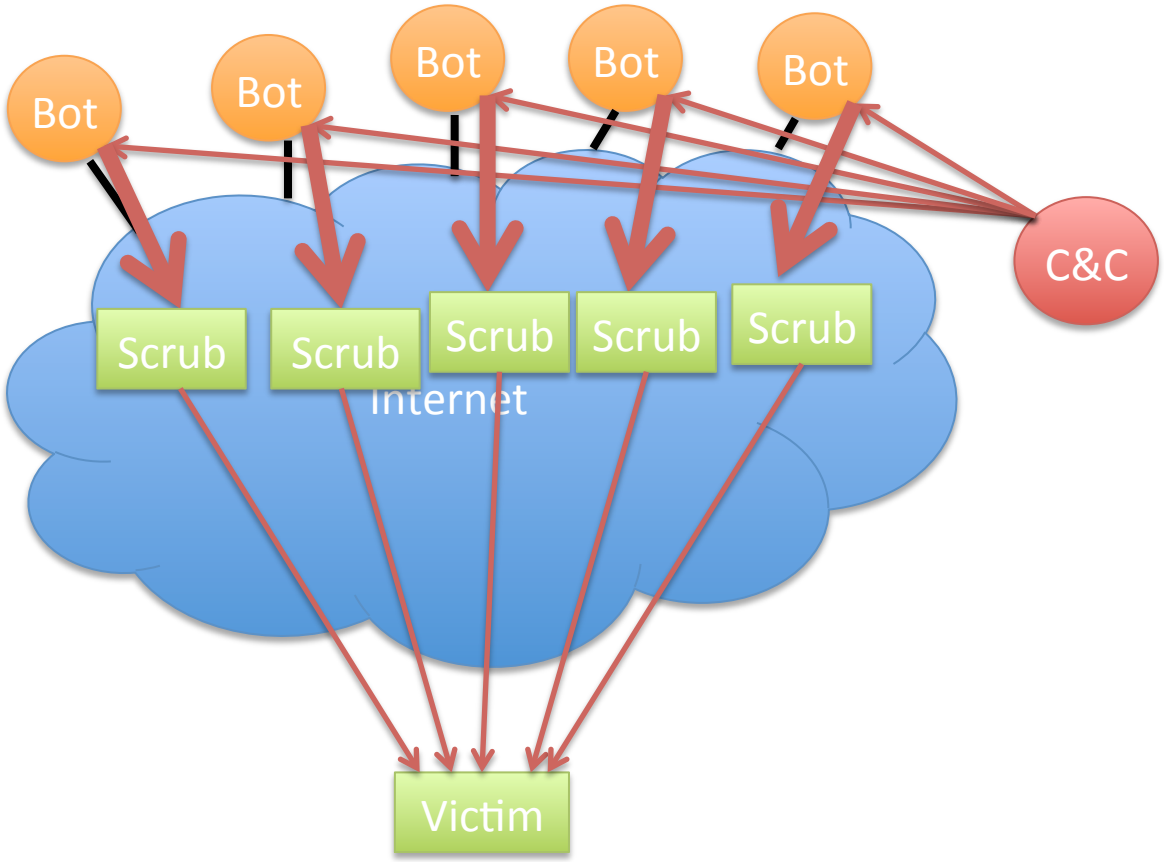


Credit: http://securitytnt.com/dns-amplification-attack/

DDOS Defense: Content Distribution



DDOS Defense: Distributed Scrubbing



Egress Filtering

- Can have many purposes, but in DDOS case:
  - Don’t let spoofed packets out of our network
  - Let’s check the rules on our demo firewall setup