Defending Computer Networks
Lecture 11: Firewalls/DDOS

Stuart Staniford

Adjunct Professor of Computer Science

Latest News

Hot New Social Network Ello Knocked Out By Cyber Attack... Already

Image credit: ***Ello***

KIM LACHANCE SHANDROW

ENTREPRENEUR STAFF

Senior Writer. Frequently covers cryptocurrency, future tech, social media, startups, gadgets and apps.

SEPTEMBER 29, 2014

Just as Ello said hello, it briefly said goodbye.

The ad-free, blatantly anti-Facebook social platform that debuted barely more than a month ago fell victim to a Distributed Denial of Service (DDoS) attack. The knockout punch, which hit yesterday afternoon, caused an outage that lasted 45 minutes.

More News

NASDAQ

NEWS | INVESTING | ADVANCED INVESTING | PERSONAL F

Enter symbol, name or keyword | Search

JAL Customer Data Target of Cyber Attack

By Dow Jones Business News, September 30, 2014, 01:35:00 AM EDT

AAA

Vote up | Comment | Share | Subscribe

TOKYO--Japan Airlines Co. said it has become the latest target of hackers, with the information of up to 750,000 customers possibly stolen.

The airline confirmed Monday it has found evidence of unauthorized access to its Customer Information Management System due to a virus attack on computer terminals within its network. The personal data of JAL Mileage Bank members are stored in the system.

The data that may have been leaked include the names, genders, birth dates, addresses, email address and places of work of JAL's mileage program members.

More News

By Martyn Williams FOLLOW

IDG News Service | Sep 30, 2014 4:37 AM PT

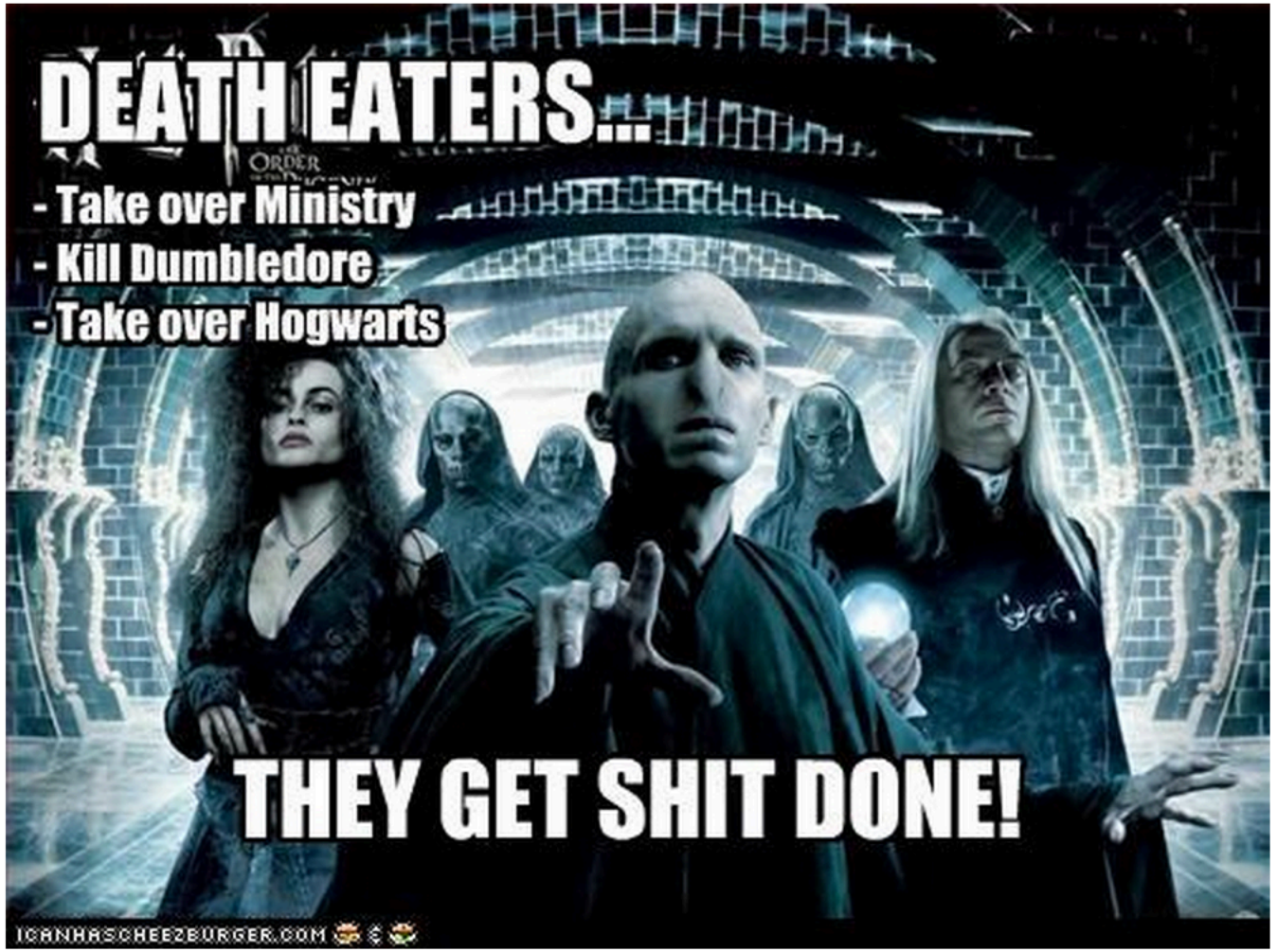
SuperValu, the grocery store operator hit by a cyberattack in June and July, has suffered a second attack on its payment processing system, it said Monday.

The Minnesota-based company said the more recent attack involved different malware installed on the part of its computer network that processes card payments at some of its Shop 'n Save, Shoppers Food & Pharmacy and Cub Foods stores. But the company said it believes that cardholder information is largely safe.

While the second breach is no doubt embarrassing for the company, the severity of the attack was partially mitigated by technology it had deployed since the first breach, it said.

While the malware was installed at numerous stores, it only succeeded in capturing payment card data between Aug. 27 and Sept. 21 from some checkout lanes at four Cub Foods franchise locations in Hastings, Shakopee, Roseville and White Bear Lake, Minnesota.

Dark forces had a busy week…



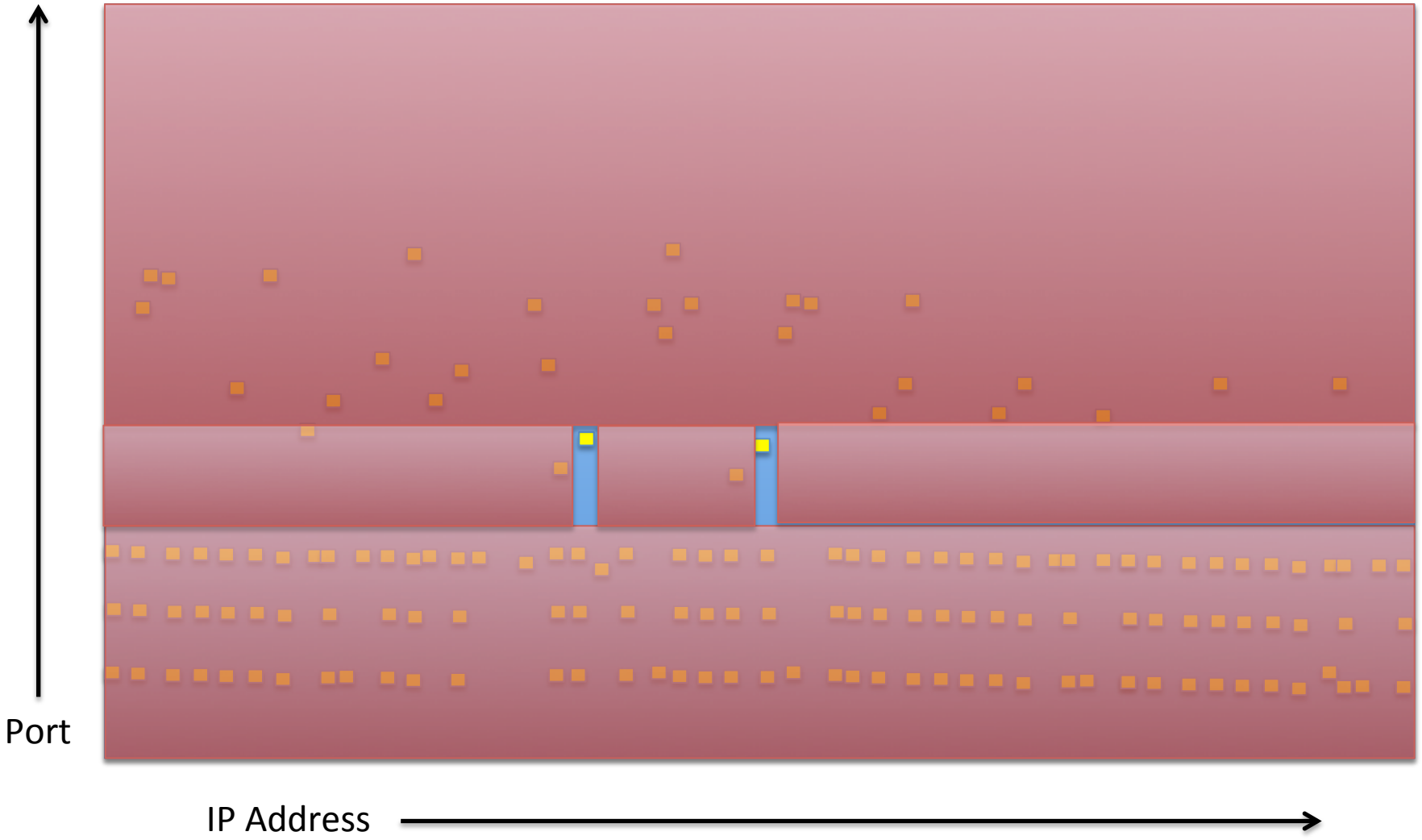
Logistics

- HW1 regrade:
  - "Basically, if their shell code work under gdb, they will get 10 points full bonus and if they mentioned printf vulnerability but not actually exploit it, then will be award 5 points."
- Go through Quiz1 solutions

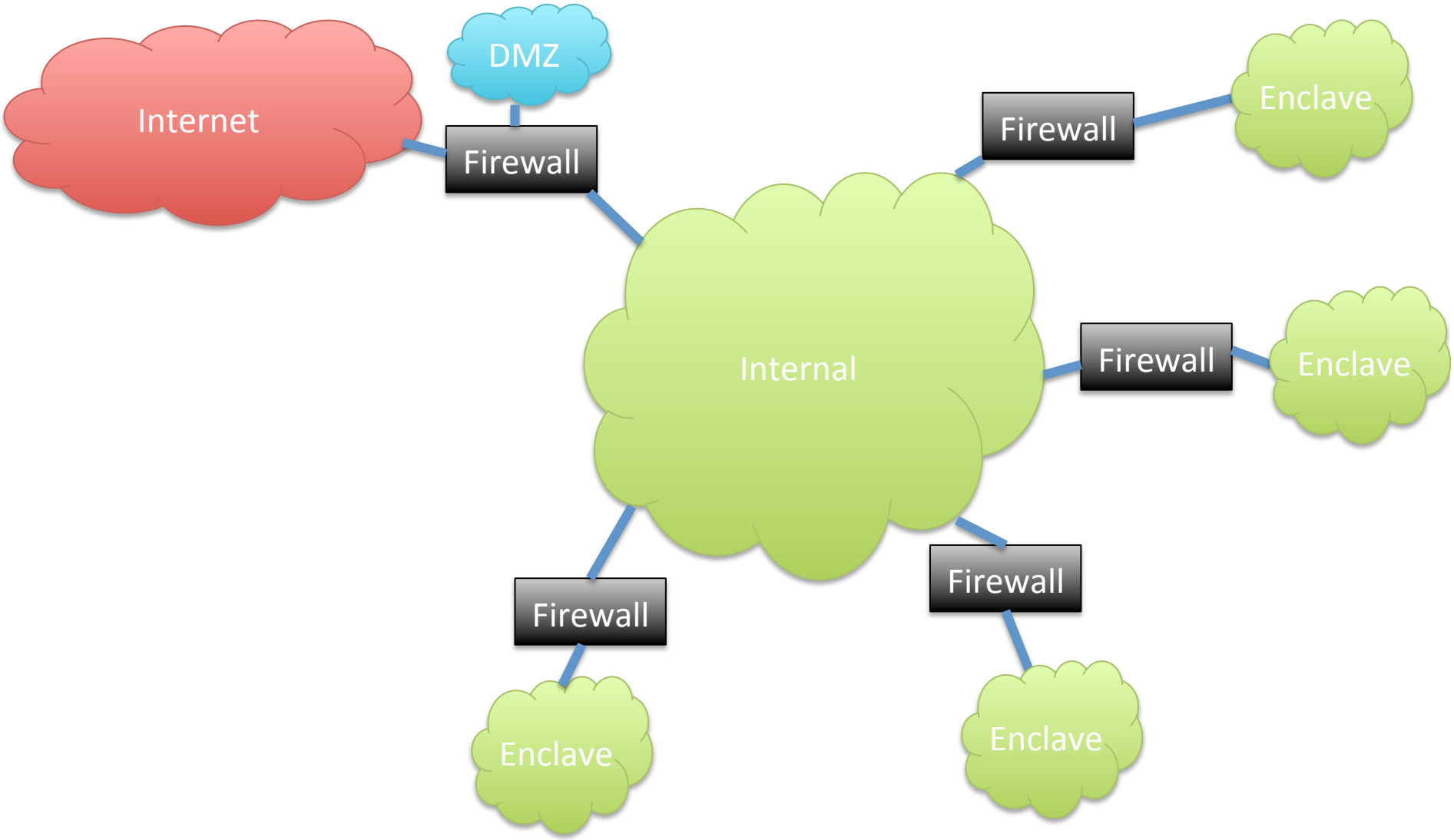
Main Goals for Today

- Firewall Demo redux.
- Network address translation (NAT)
- Distributed Denial of Service.
- Maybe start NIDS.

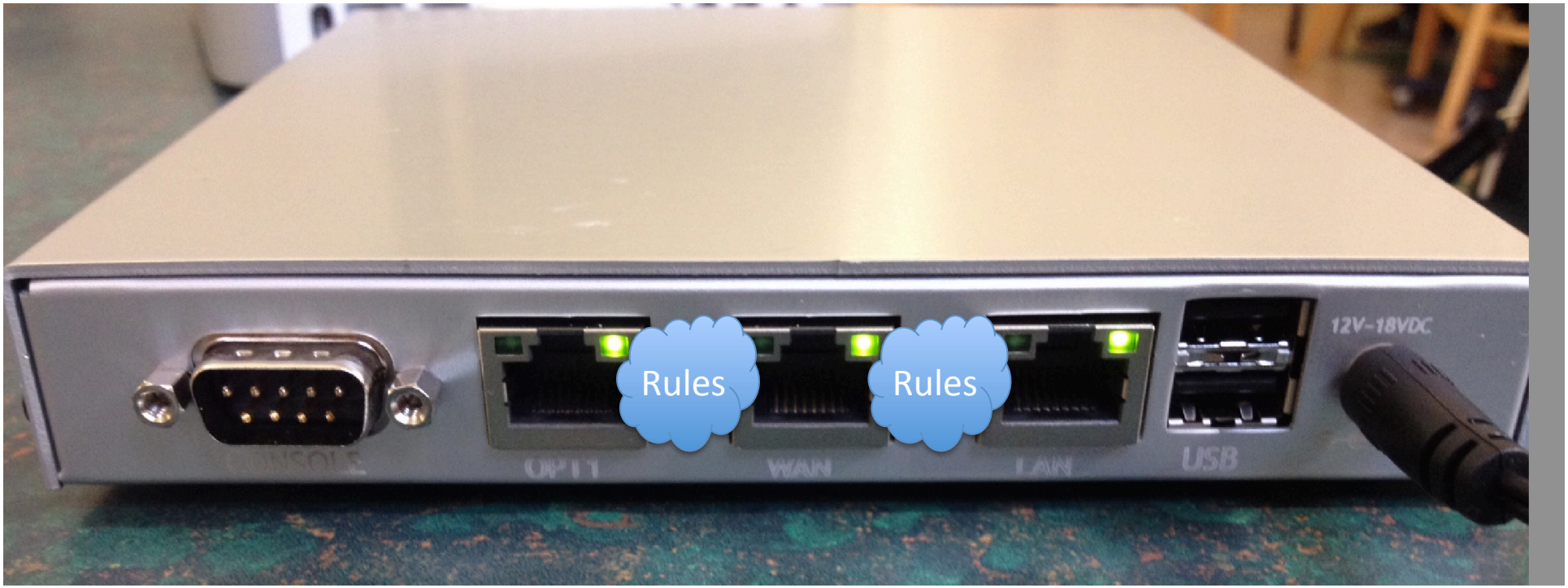
Establish Central Control



Or…


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

Firewall Basic Concept

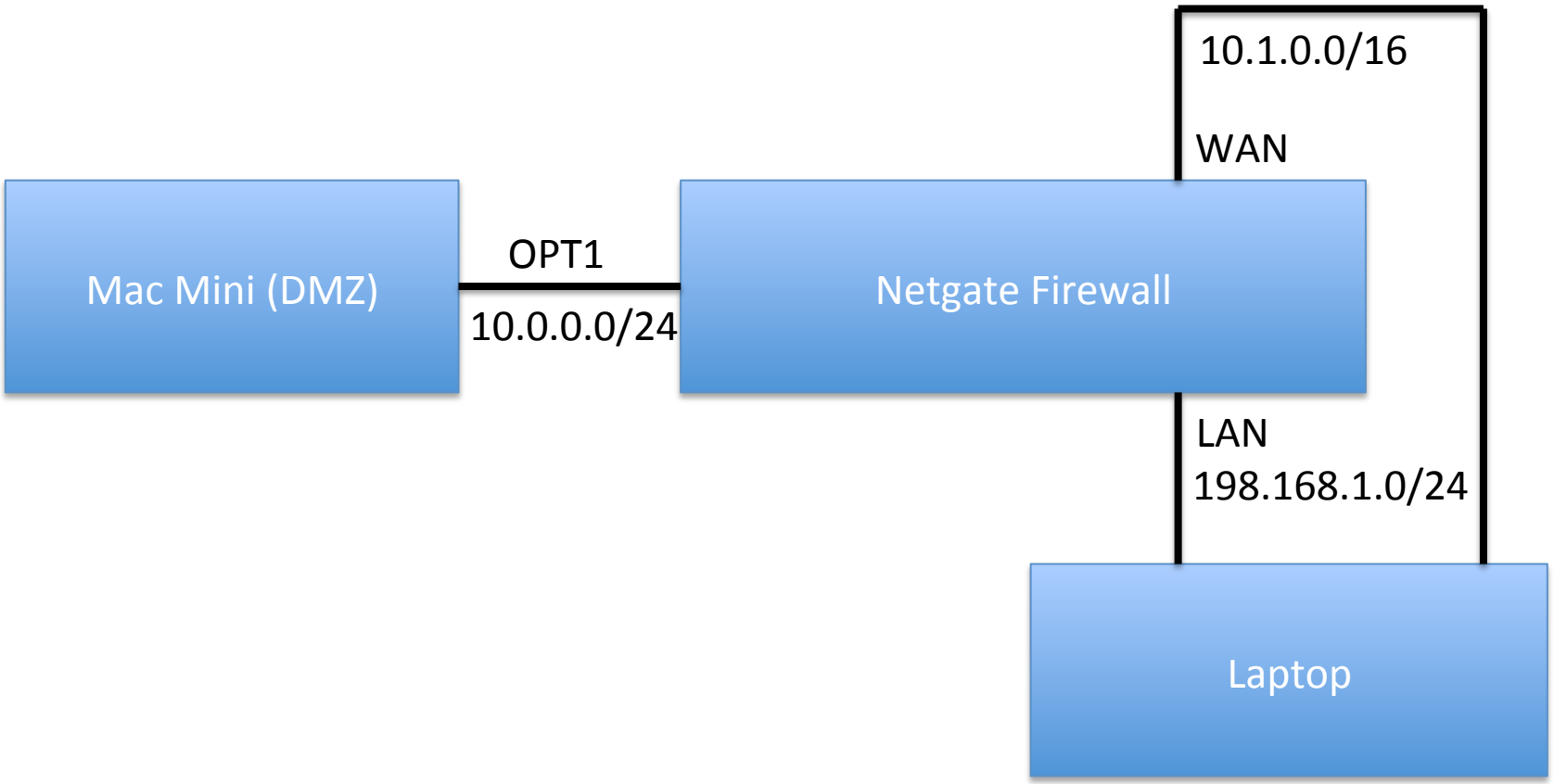


(This is Netgate M1N1Wall – low-cost, low-power open source firewall using FreeBSD/pfSense. Runs on AMD Geode cpu.)

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 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.
      - Unplug the WAN wire first
    - Have a quick look at state table

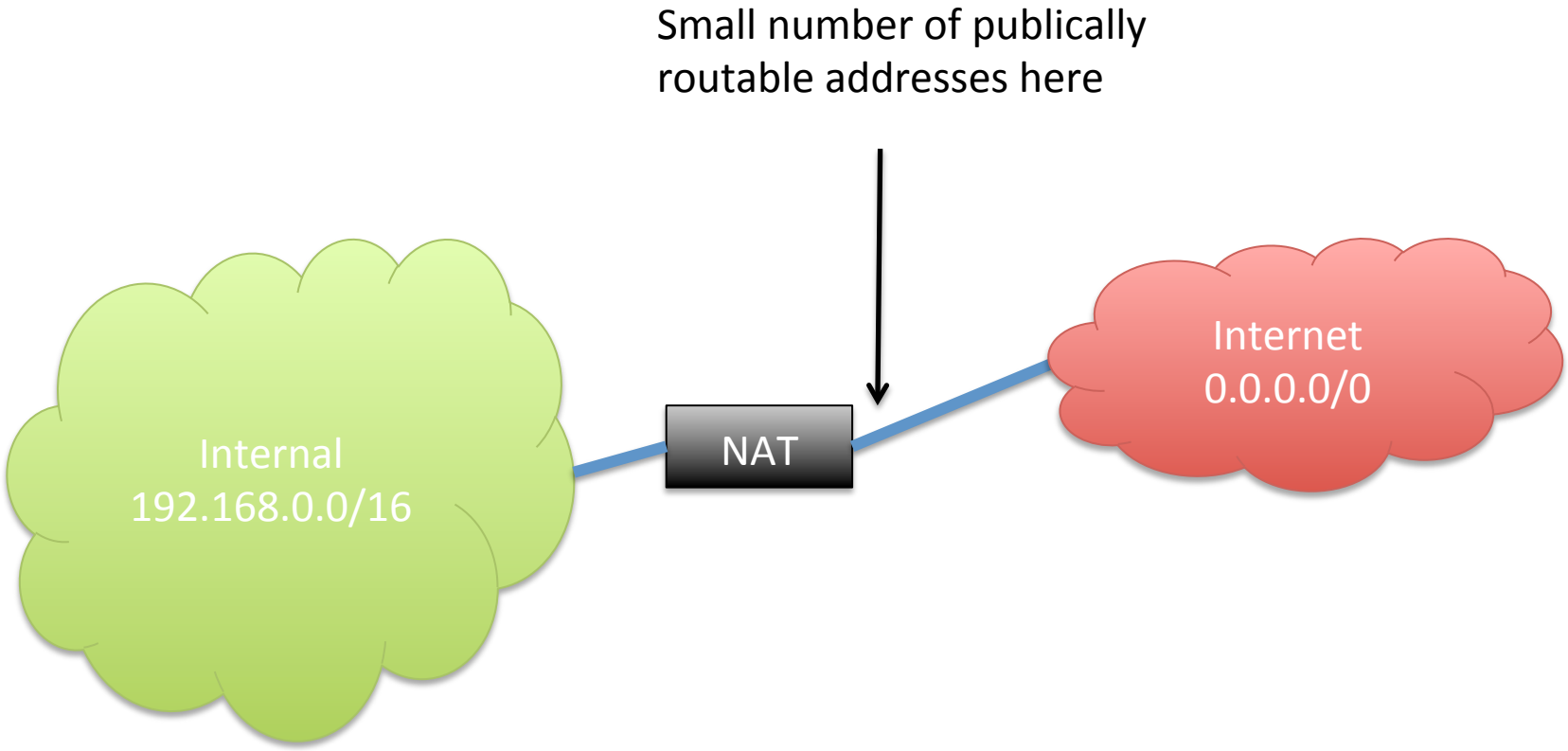
Firewall Rules

- 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 new rule from scratch to allow ssh
  - See how the nmap result changes

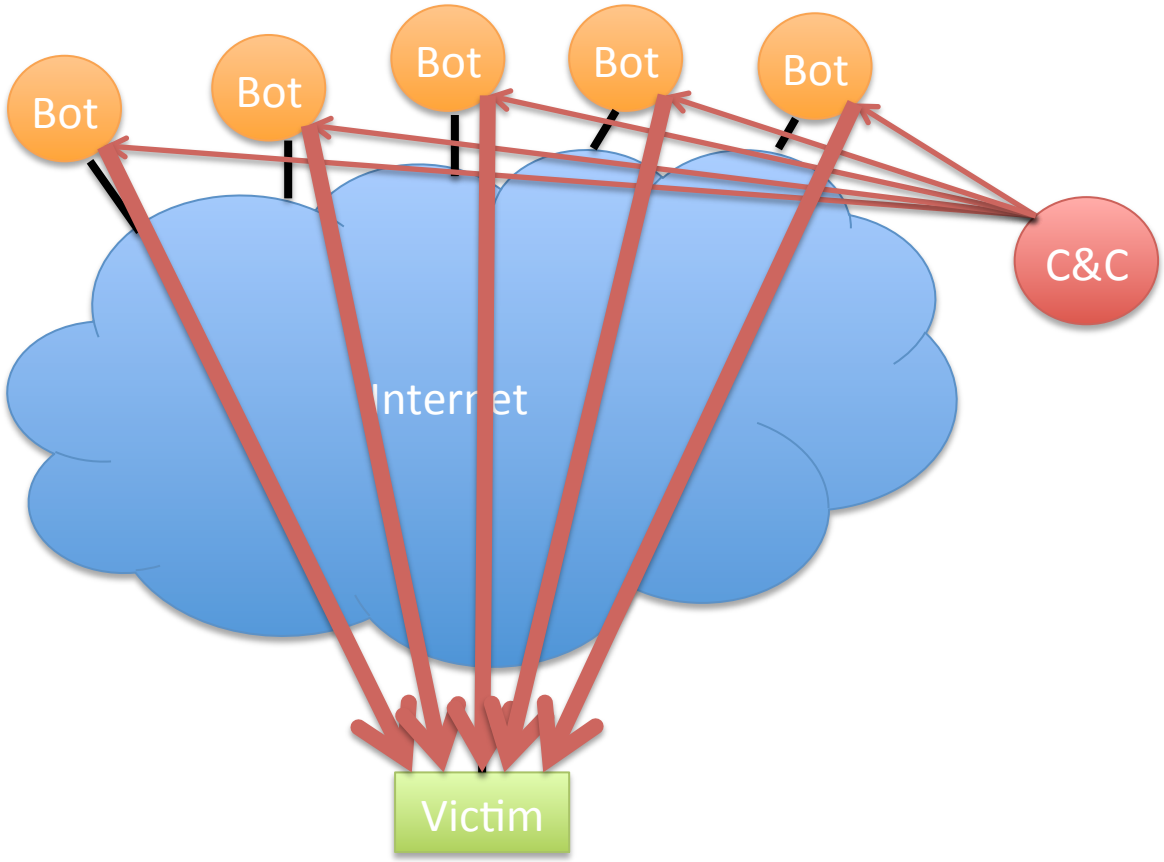
Network Address Translation (NAT)

- 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

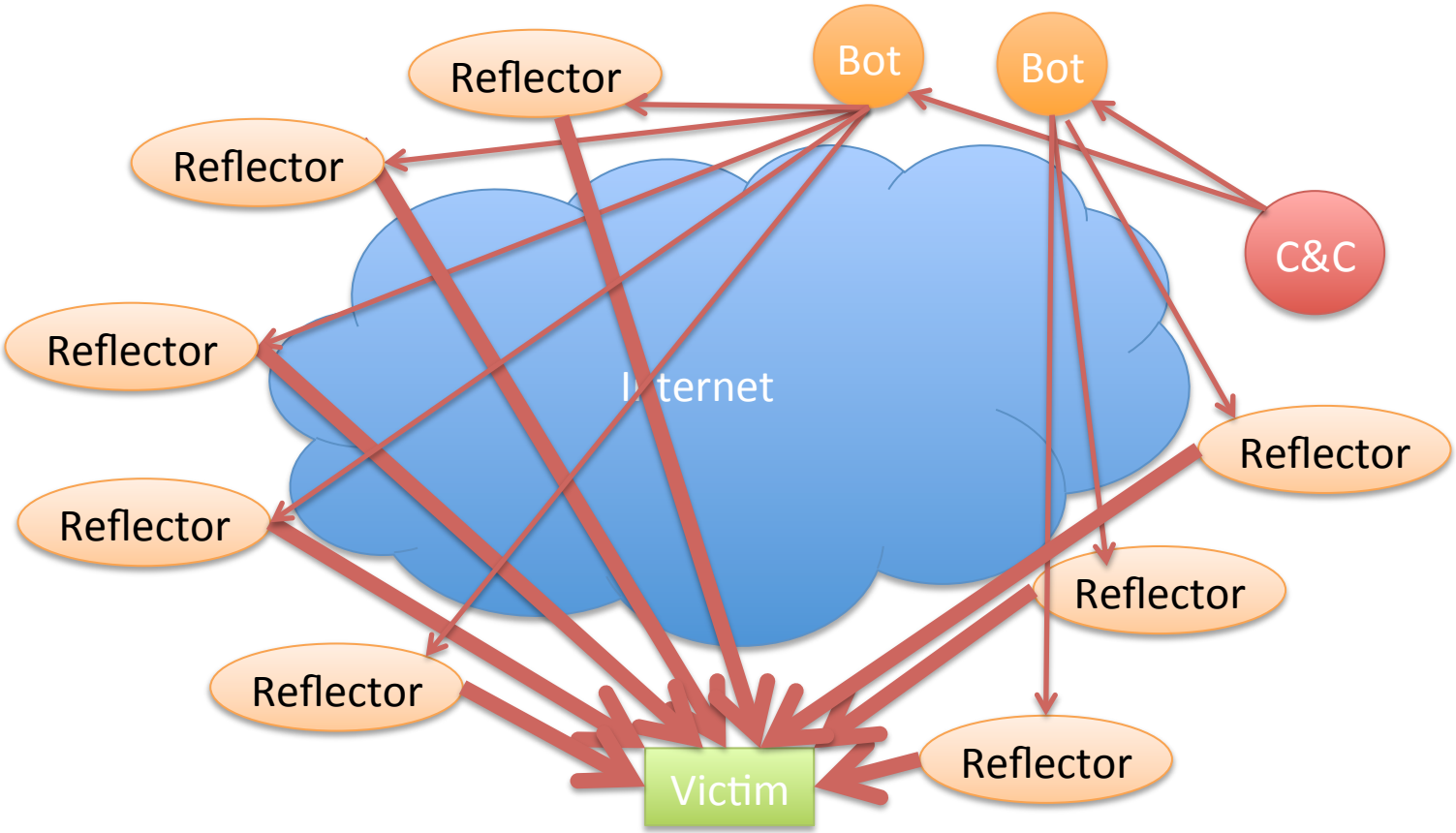


Basic Setup of a DDOS Botnet



Illustrative only: practical attacks will have many more bots

Reflection Attacks



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

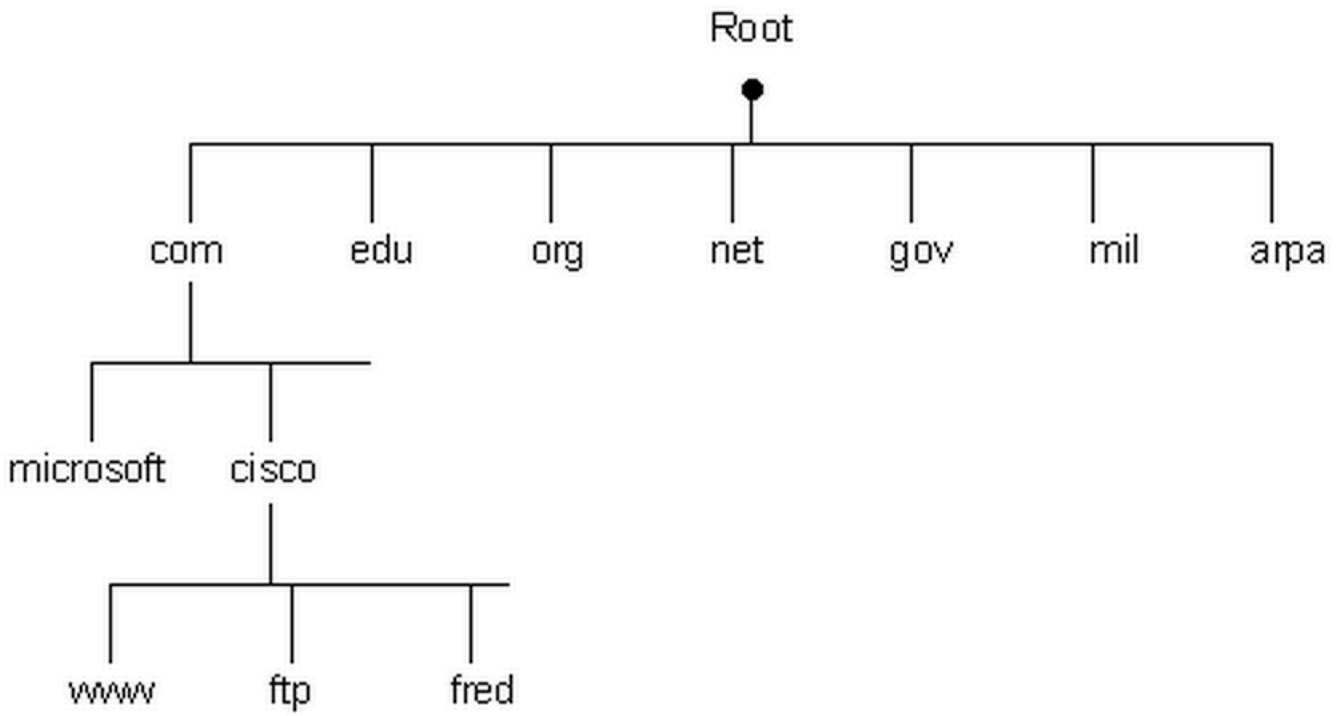
What Will Work as a Reflector?

- 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

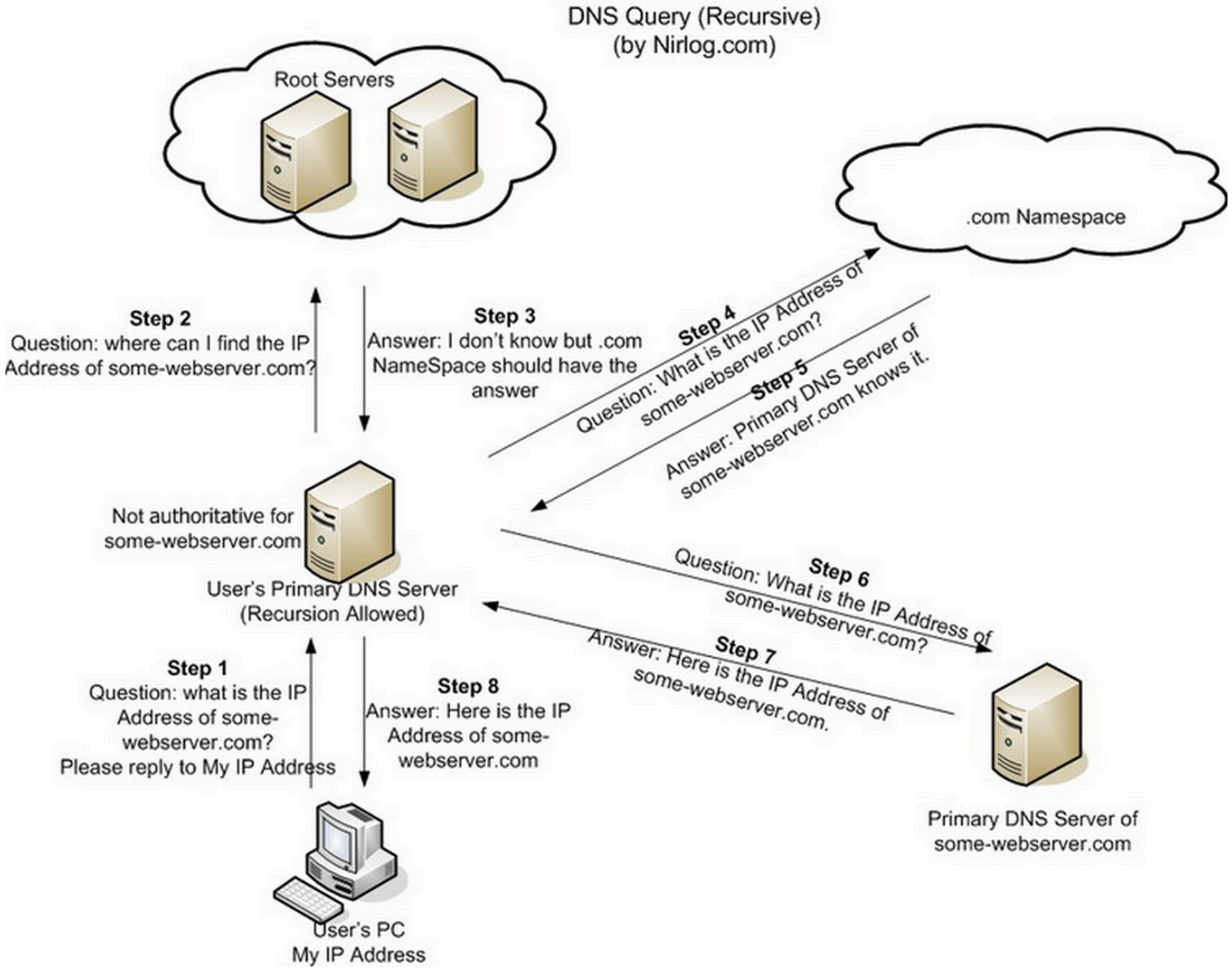
Domain Name Service

- 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
  - Turn on wireless
  - dig www.nytimes.com

The DNS Hierarchical Name Tree

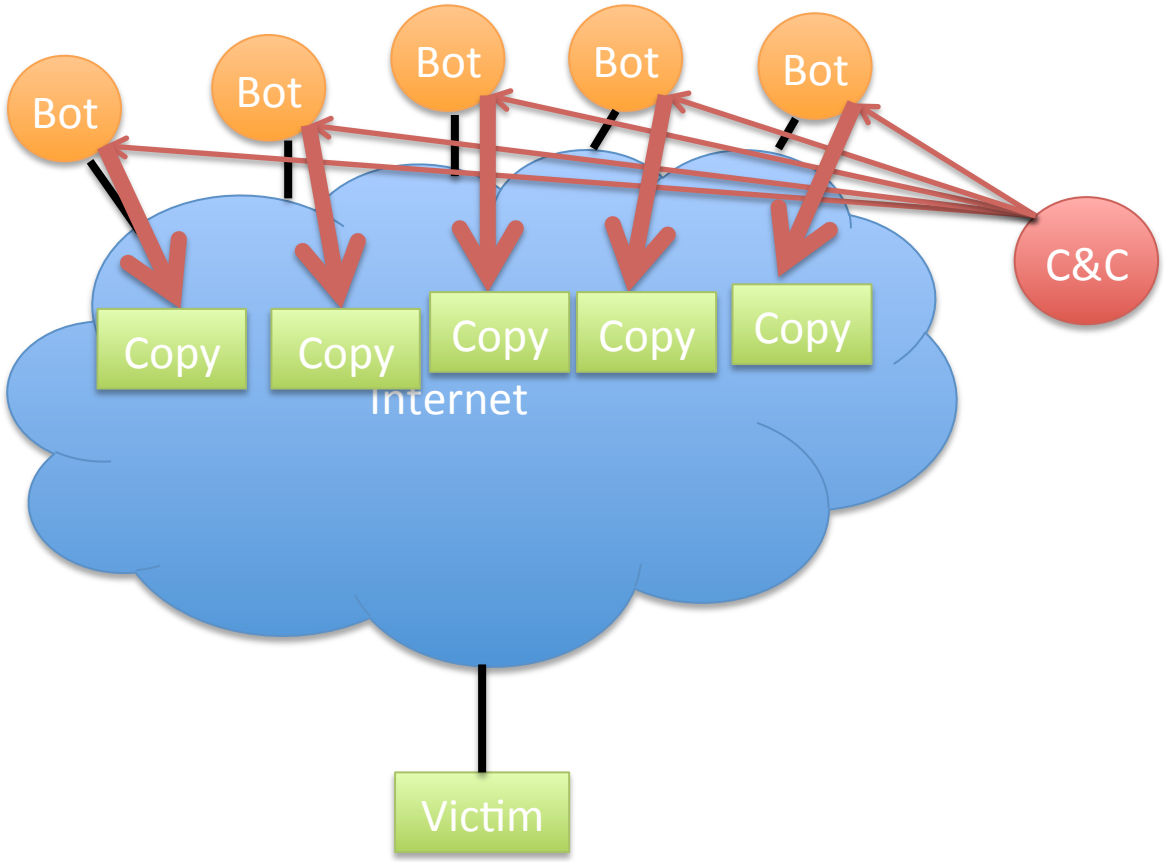


How a DNS Query Works

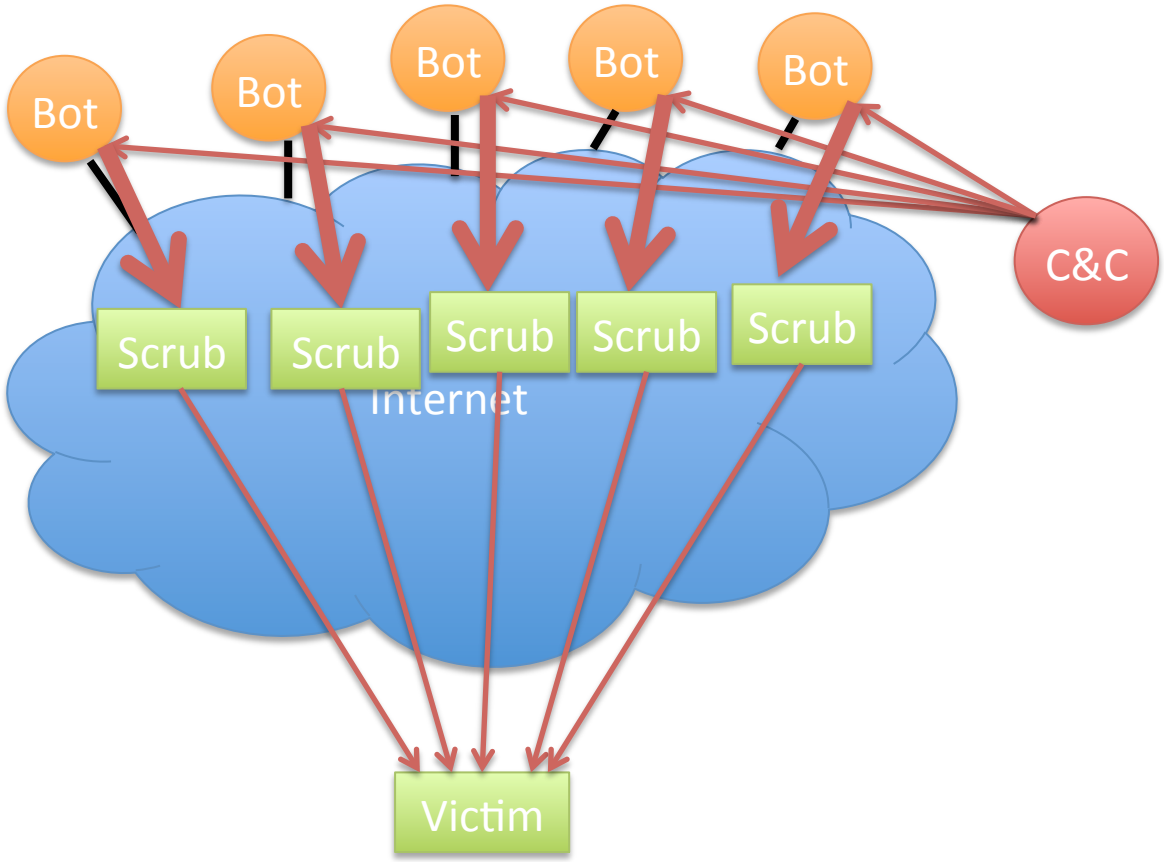


Credit: http://securitytnt.com/dns-amplification-attack/

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