Practical Advice for Small and Medium Environment DDoS Survival

Chris "Mac" McEniry

Sony Network Entertainment

@macmceniry

usenix LISA15

November 8–13, 2015 | Washington, D.C.
www.usenix.org/lisa15 #lisa15

Practical Advice for Small and Medium Environment DDoS Survival

Chris "Mac" McEniry
Sony Network Entertainment
@macmceniry

Branson Matheson
Cisco
@sandinak

Who are we?

Chris McEniry

- Network Engineer Sony
- 15+ Year IT Pro
- Mgr Defcon network
- Trainer and Speaker

Branson Matheson

- Tech Lead - Cisco
- 15+ year IT Pro
- Mgr ShmooCon Network
- Trainer and Speaker

Geeks who like to do fun stuff with cool networks

Who is this for?

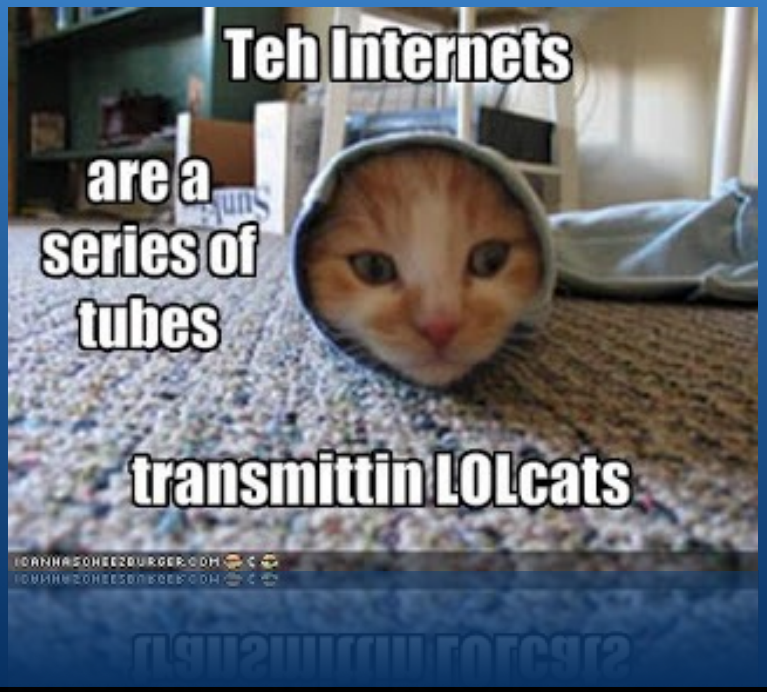
- Online Services
- 1-3 points of presence
- 1Gbps-20Gbps per POP

Topics

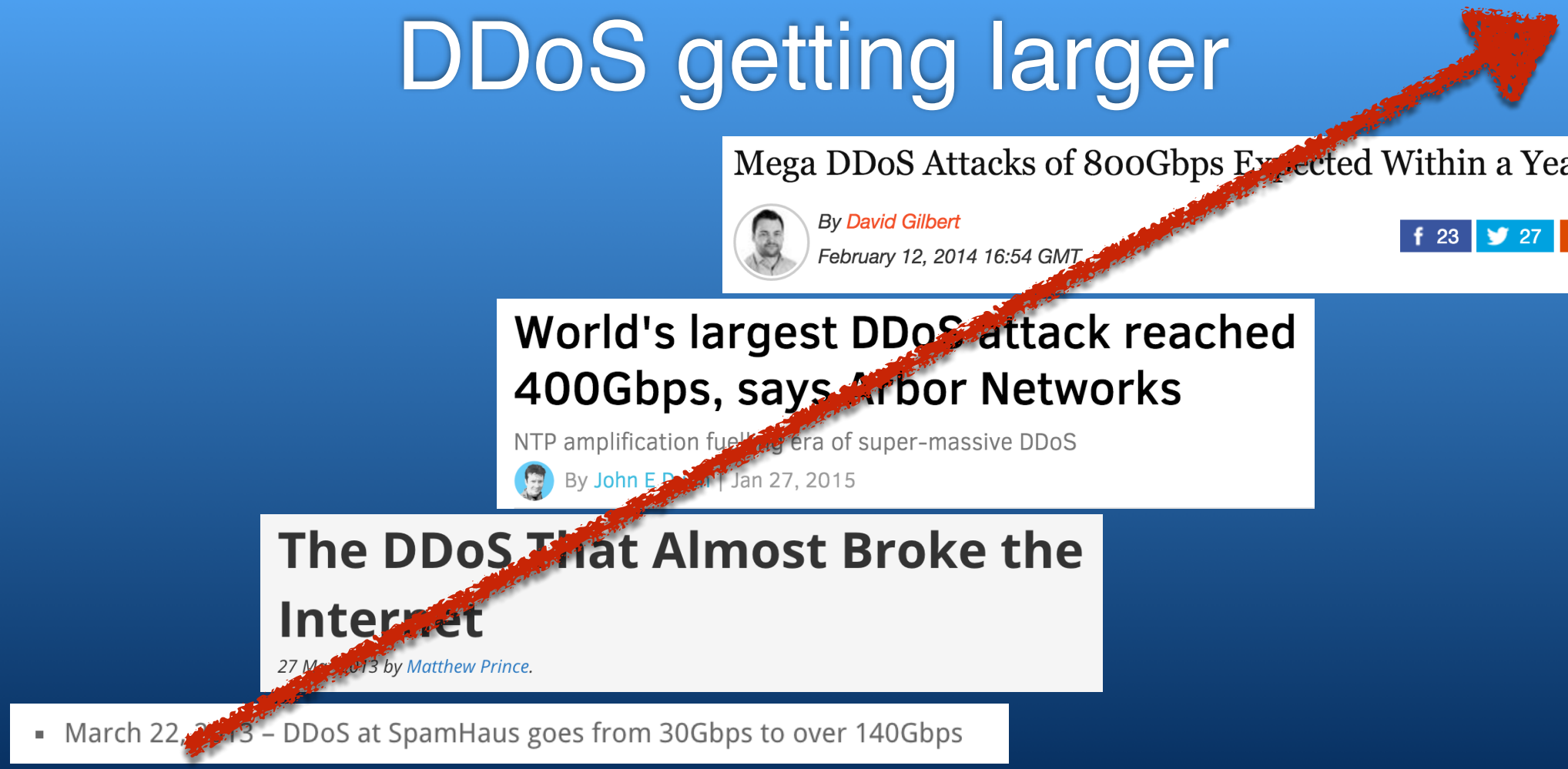
- Defining a DDoS
- Knowing
- Attack Categories
- Defense Strategy

What's a Distributed Denial of Service?

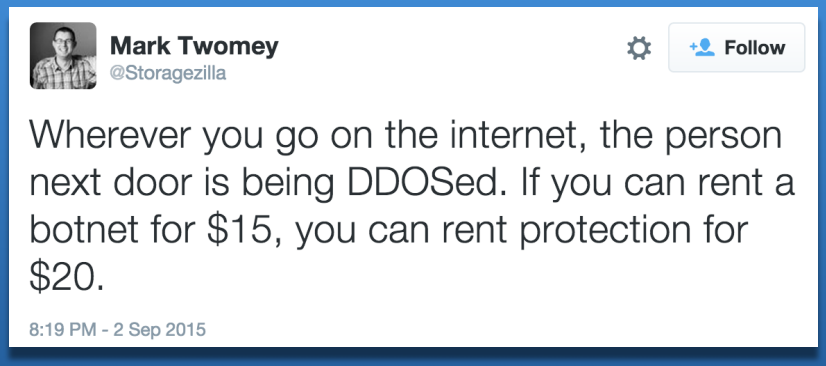
- Attack intended to disrupt access to your service with the following properties:
  - Internet based (multiple sources)
  - Sufficient volume targetting a critical resource
    - Most obvious: Pipes
    - Others: Connection, state tables, CPU, etc

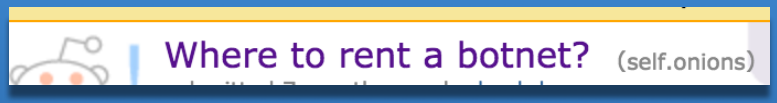


DDoS getting larger



Renting is easy














"Know Thyself"

Know Thyself

What does your traffic look like

- Are you using all the protocols and ports that are likely to be open?
- Using UDP? Only using TCP ports? Only using HTTPS?
- Does everyone need to be able to access you? (E.g. do you really need traffic from China?)

Know Thyself

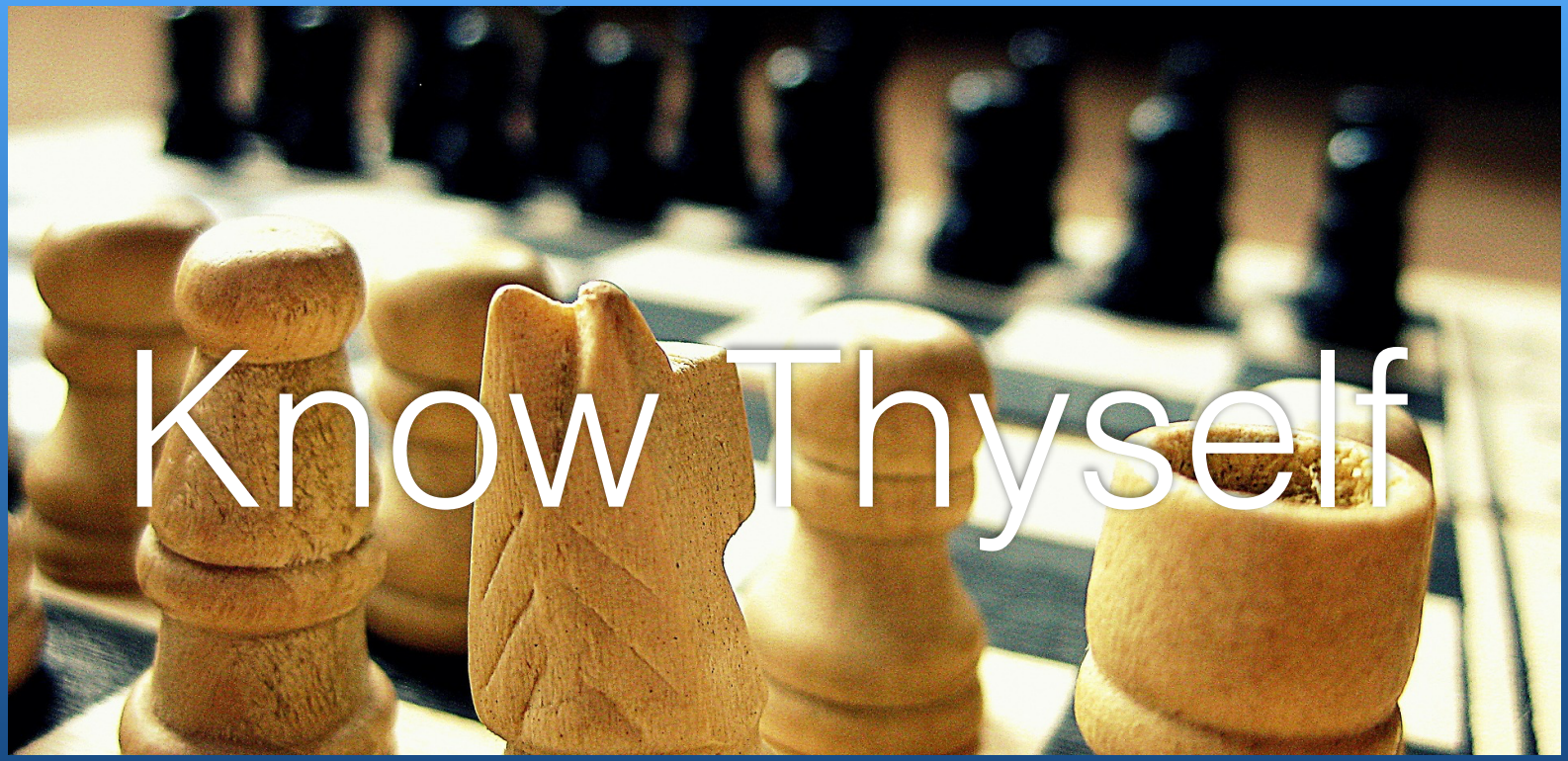
What does recovery look like

- Does it look different than an attack?
- What does it mean to your business model?

Know Thyself

How much downtime can you take

- How much does it cost?
- What parts of your site or infrastructure can be down?
- In what order are you willing to sacrifice functionality to keep some availability?



Your responses to the above will dictate your DDoS Mitigation Strategy.

Know Thy Adversary?

Know Thy Adversary?

- Knowing the attacker thinking can be irrelevant*
- Knowing the attacker methodologies is useful

Know Thy Adversary?

- There's probably multiple attackers
  - Multiple motivations
  - Majority are making a name or statement
  - Some are smarter than you

Know Thy Adversary?

- Can you really game theorize all possible reasoning and vectors?

Know Thy Adversary?

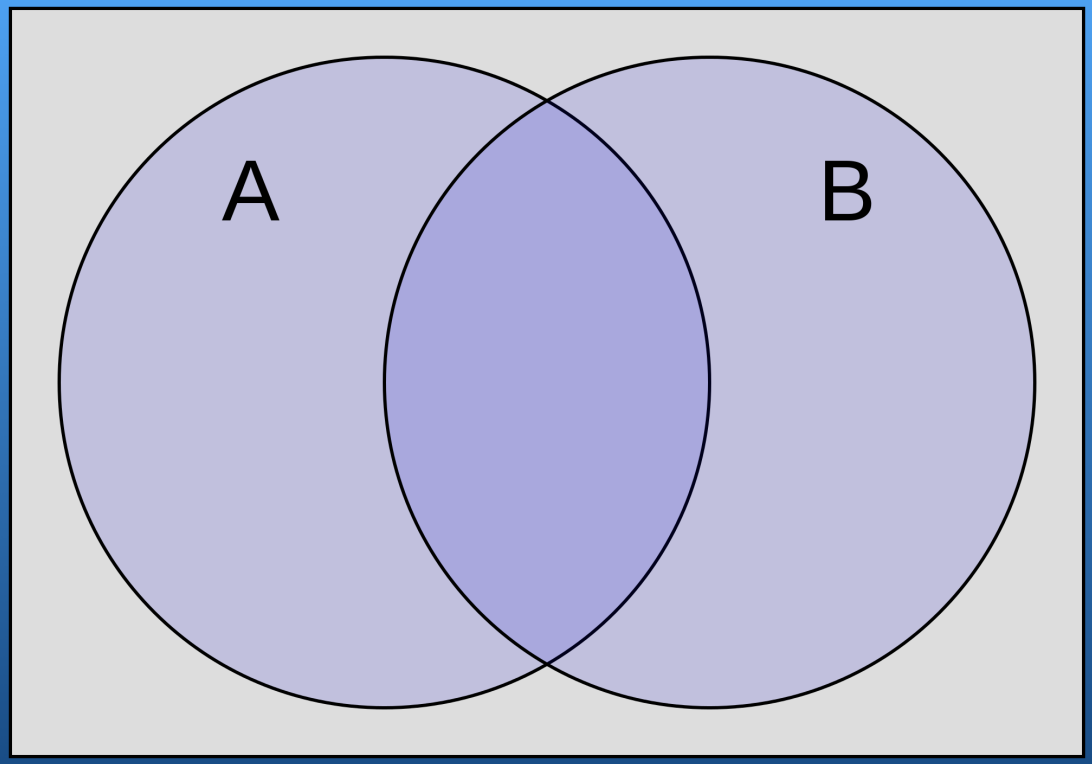
- The mitigations are largely the same
  - And largely determined by "Know Thyself"

The “hows” - not the “whys”

Know Thy Adversary?

Places to look for attack types and volumes

- Verisign DDoS Trends Report
- Neustar DDoS Attacks and Protection Report
- Arbor Atlas - DDoS
- Digital Attack Map
- ISC Storm Center
- And many other reports…



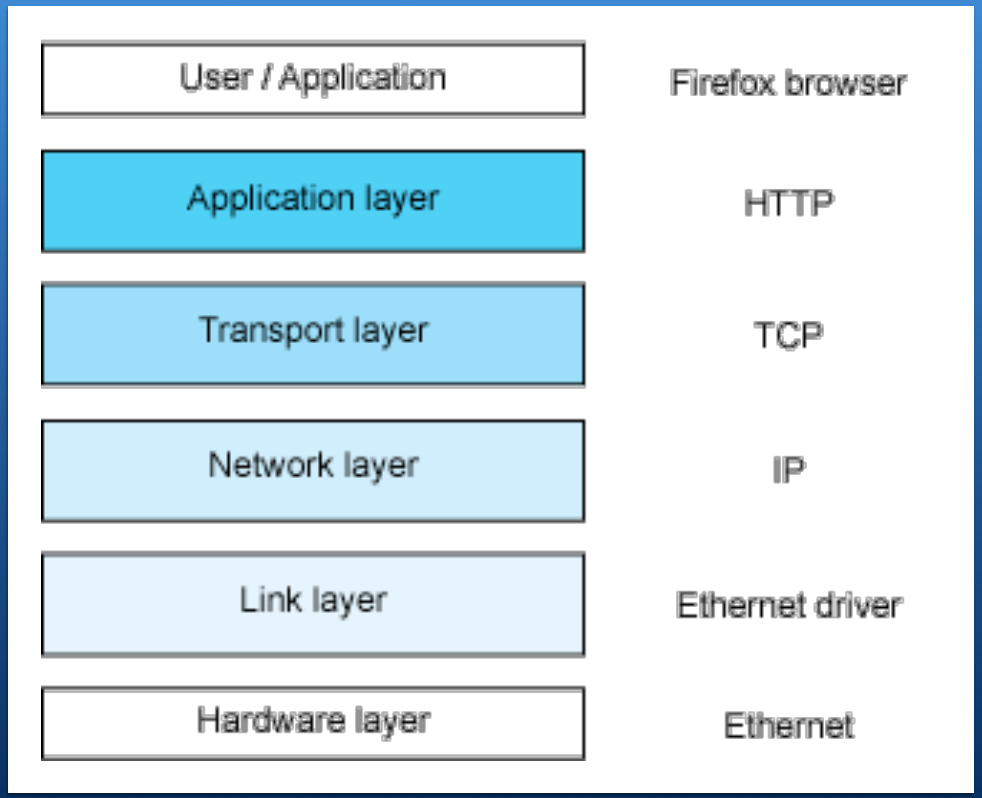
Attack Categories

Attack Categories

- Three Dimensions
  - What Network Layer (Vertical)?
  - What Network Point (Horizontal)?
  - Type of Source?

Attack Categories: Vertical

- What layer of the network stack?
  - "Network": Layer3/4 - IP/UDP/TCP/etc
  - "Application": HTTP



Attack Categories: Horizontal

- How deep are they attacking you?
  - Your border?
  - Your application servers?
  - ***Your ISP's infrastructure?***

Attack Categories : Source

- Direct or indirect?
  - Am I (or my botnet) sending the attack?
  - Am I coercing others into sending the attack?

Common Attacks

- Network Attacks
  - Target Infrastructure - Pipe Capacity, State Tables, Network Device CPU, etc.
  - IP Fragmentation, SYN Flood, Christmas Tree Floods

Common Attacks

- "Application" (and here it's HTTP centric)
  - Target the application servers and consume their CPU, connections, threads, etc
  - HTTP Post, Slow Read

Common Attacks

- Reflection and Amplification Attacks
  - Requires a small amount of input to send a large amount of traffic to target
  - Uses single/multiple third parties to send the actual traffic

Protocol	BAF *all*	BAF 50%	BAF 10%
SNMP v2	6.3	8.6	11.3
NTP	556.9	1083.2	4670.0
DNS_{NS}	54.6	76.7	98.3
DNS_{OR}	28.7	41.2	64.1
NetBios	3.8	4.5	4.9
SSDP	30.8	40.4	75.9
CharGen	358.8	n/a	n/a
QOTD	140.3	n/a	n/a
BitTorrent	3.8	5.3	10.3
Kad	16.3	21.5	22.7
Quake 3	63.9	74.9	82.8
Steam	5.5	6.9	14.7
ZAv2	36.0	36.6	41.1
Sality	37.3	37.9	38.4
Gameover	45.4	45.9	46.2

Common Attacks

- Application Amplification Attacks are starting to happen
  - Being able to change a small amount of HTTP (e.g. javascript) traffic to trigger many requests to the target
  - Great Cannon

Common Attacks

- Intermediaries
  - ISPs
  - Dependent SaaSes (e.g. Image Converters, Code Hosting)
  - Dependent JS libraries

Lifecycle

- Small attackers / Scanners - Firewall is able to Block
- Attackers get bigger - Move to stateless ACLs to solve Network attacks
- Attackers use reflections - Move to vendor who can sustain bandwidth
- Attackers turn to application - IPS/WAF
- Attackers get/sacrifice a large bonnet - Vendor Application Proxies



Defense Strategy

How to defend?

- Its all about reducing the bad traffic which you receive
- Fundamentally, 2 questions:
  - What effort at each level are you going to use?
  - Are you going to do it yourself? or have someone else do it?

Self Defense: Network Level

- Any packet filtering device defends at the Network level
  - However, that packet filtering device can become a bottleneck itself
- ACLs, Firewalls, iptables, "not listening"
- The further upstream you can push these, the better
  - Some ISPs may apply ACLs for you
  - BGP null route advertisements

Self Defense: Network/Application Level

- Intrusion Prevention Systems (IPS)
  - Since can do deep packet inspection, can be considered application level
  - Matches patterns (e.g. regex) and denies
  - But can also do network level protections (SYN Proxy)
  - Likely to be able to handle more bad traffic than similarly classed firewalls
  - Likely to be able to incorporate reputation filters

Self Defense: Application Level

- Web Application Firewalls
- See above - IPS
- Inspect flows in an application context and react
  - Deny bad patterns
  - Rate limit flows
  - Incorporate reputation filters

Self Defense: Pros

- You will have a better understanding of your own traffic
- Always active
- Lower coordination on mitigation

Tipping the scale (Self Defense: Cons)

- Pipes can only handle so much
- At some point, can't even handle the incoming traffic on your pipes, regardless of internal protections
- Consider a vendor solution (beyond ISP cooperation)

Stateful vs Stateless

- Rough comparison: Switch/Router ACLs vs Firewalls
- Rules of thumb:
  - Use stateless to control destination and IP reputation
    - "Of the 64K tcp ports, only allow in to port 443/tcp"
    - "Don't let in Country X"
  - Use stateful to control source (outside IP reputation)
    - "Only allow my offices to hit my port 443/tcp"

Vendor Solutions

- Two main methods:
  - Network Scrubbers
  - Application Proxies



Network Scrubbers

- Route all incoming traffic, at the IP level, through scrubber
- They become your BGP announcer
- Traffic is then sent to you: either direct connection or encapsulated and retransmitted over the Internet
- Can be always-on or on-demand
- Even under always-on, have a static stance (e.g. ACLs) and an under-attack stance (actual mitigation gear)

Application Proxies

- Direct traffic to their endpoints by updating DNS
- Become the endpoint of connection for client connections
- Inspect, and then proxy those connections back to you

Application Proxies

- Typically, always on
- Application specific: "Works if they speak your protocol" - Typically DNS, HTTP/HTTPS, even SMTP/IMAP
- But by nature will front Layer3/4 attacks

Vendor Pros

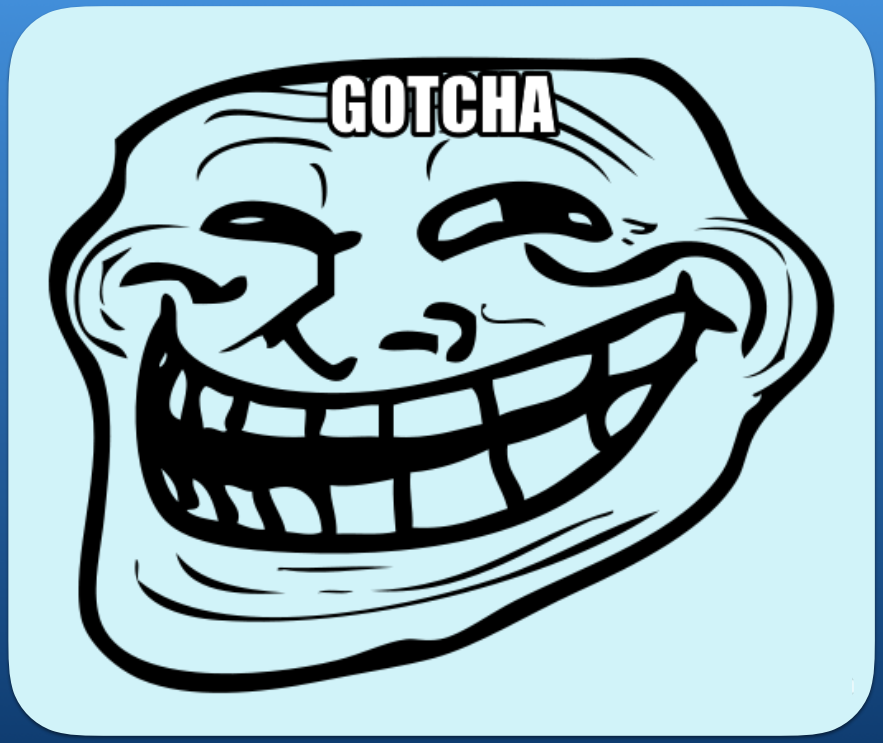
- 1Tbps+ Internet capacity and scrubbing capacity
- 24x7 staff focused on DDoS
- Up to date mitigation software/hardware

Vendor Cons

- Over-subscription: Other customer's attacks can affect you
- Vendors becomes your ISP to a degree
  - Any of their carrier issues become your issues
  - Added bonus: No longer a direct carrier relationship. More coordination

Vendor Gotchas

- What is mitigation going to do to your normal traffic?
  - Most stances are based around browser based web traffic.
  - Native phone apps, embedded devices (IoT) may not like that



Vendor Gotchas

- Cannot stress how important that connection back to you is
- How hidden is your origin?
  - Application to either Network Scrubbers or Application Proxies
  - Do your origin endpoints show up in WHOIS? Reverse DNS?
  - Can one scan your actual network and start to determine where those endpoints really are?

Items to look for in a Vendor

- Internet Capacity vs Scrubbing Capacity
- Points of Presence: Internet facing, and clean traffic to you facing
- Scrubbing Mechanisms
- Configuration, Incident, Maintenance Transparency
- Connection options: GRE or Meet-Me Cross Connects?
- Pricing Model: Always on? Incoming or just clean traffic? Port fees?

Potential Vendors

- A10 Networks
- Akamai
- Amazon AWS
- Arbor Networks
- CloudFlare
- Corero
- F5 / Silverline
- Google Compute Engine
- Imperva / Incapsula
- Level3
- Limelight
- Neustar
- Verisign

No endorsements and not exhaustive. Strictly a starting point.

Which path?

- Depends on where you are in attacker/defender cat mouse game or your budget (time and money)?
- Depends on your applications (e.g. are they already on a vendor CDN?)
- Depends on your whole system (e.g. think about all of your dependencies not just for the running application, but also for your business mechanisms like updating the application)

Parting Shot…

- Amplification attacks are the biggest threats right now
- Don't contribute to the problem
  - Are you running an open NTP server?
  - Do you have any large public DNS records available via UDP?
  - Are you watching your egress traffic? Is it all from you?





Chris "Mac" McEniry
Sony Network Entertainment
@macmceniry

Branson Matheson
Cisco
@sandinak