



## Preparing for a DDoS Attack

Ronan Mullally, Akamai Technologies  
NANOG 67, Chicago, 14th June 2016

# The Cloud...



# What is a DDoS?



Where's your Umbrella?



# 1 - Be Prepared

## Have a Plan

- Know what your options are
- Find out what upstreams can do to help and know how to use it
- Consider AUPs - yours and your upstreams

## Be nimble

- Low DNS TTLs on likely targets
- Put likely targets on independently routable prefixes
- Be able to quickly adapt your routing

## 2 - Be aware

### **Monitor everything**

- Bit rate and packet rate via SNMP
- Netflow, Sflow, etc
- Peering portal stats
- Span ports / Taps

### **Know what's going on on your network**

- Otherwise you're in the dark

### **Know what's going on downstream**

- Your customer might *want* to see 43Gbps of NTP
- Or they might only want 80/tcp.

# 3 - Have a Robust DNS Infrastructure

If you (or your customer's) DNS is broken, so are you.

Don't make it an easy target:

;; ANSWER SECTION:

```
example.com.      14400    IN      NS      ns1.example.com.
example.com.      14400    IN      NS      ns2.example.com.
```

;; ADDITIONAL SECTION:

```
ns1.example.com.  14400    IN      A       a.b.c.10
ns2.example.com.  14400    IN      A       a.b.c.140
```

;; ANSWER SECTION:

```
akamai.com.      300     IN      NS      a20-66.akam.net.
akamai.com.      300     IN      NS      a2-66.akam.net.
akamai.com.      300     IN      NS      a3-66.akam.net.
akamai.com.      300     IN      NS      a9-66.akam.net.
akamai.com.      300     IN      NS      a8-66.akam.net.
akamai.com.      300     IN      NS      a5-66.akam.net.
akamai.com.      300     IN      NS      a11-66.akam.net.
akamai.com.      300     IN      NS      a13-66.akam.net.
akamai.com.      300     IN      NS      a1-66.akam.net.
akamai.com.      300     IN      NS      a16-66.akam.net.
akamai.com.      300     IN      NS      a28-66.akam.net.
akamai.com.      300     IN      NS      a12-66.akam.net.
akamai.com.      300     IN      NS      a7-66.akam.net.
```

;; ADDITIONAL SECTION:

```
a1-66.akam.net.  90000   IN      A       193.108.91.66
a1-66.akam.net.  90000   IN      AAAA    2600:1401:2::42
a2-66.akam.net.  90000   IN      A       95.100.174.66
a3-66.akam.net.  90000   IN      A       96.7.49.66
a5-66.akam.net.  90000   IN      A       95.100.168.66
a7-66.akam.net.  90000   IN      A       23.61.199.66
a8-66.akam.net.  90000   IN      A       2.16.40.66
a8-66.akam.net.  90000   IN      AAAA    2600:1403:a::42
a9-66.akam.net.  90000   IN      A       184.85.248.66
a11-66.akam.net. 90000   IN      A       84.53.139.66
a12-66.akam.net. 90000   IN      A       184.26.160.66
```

## 4 - A Firewall Will Not Save You

### **State Kills**

**The vast number of flows involved in a DDoS attack can easily overwhelm a stateful firewall**

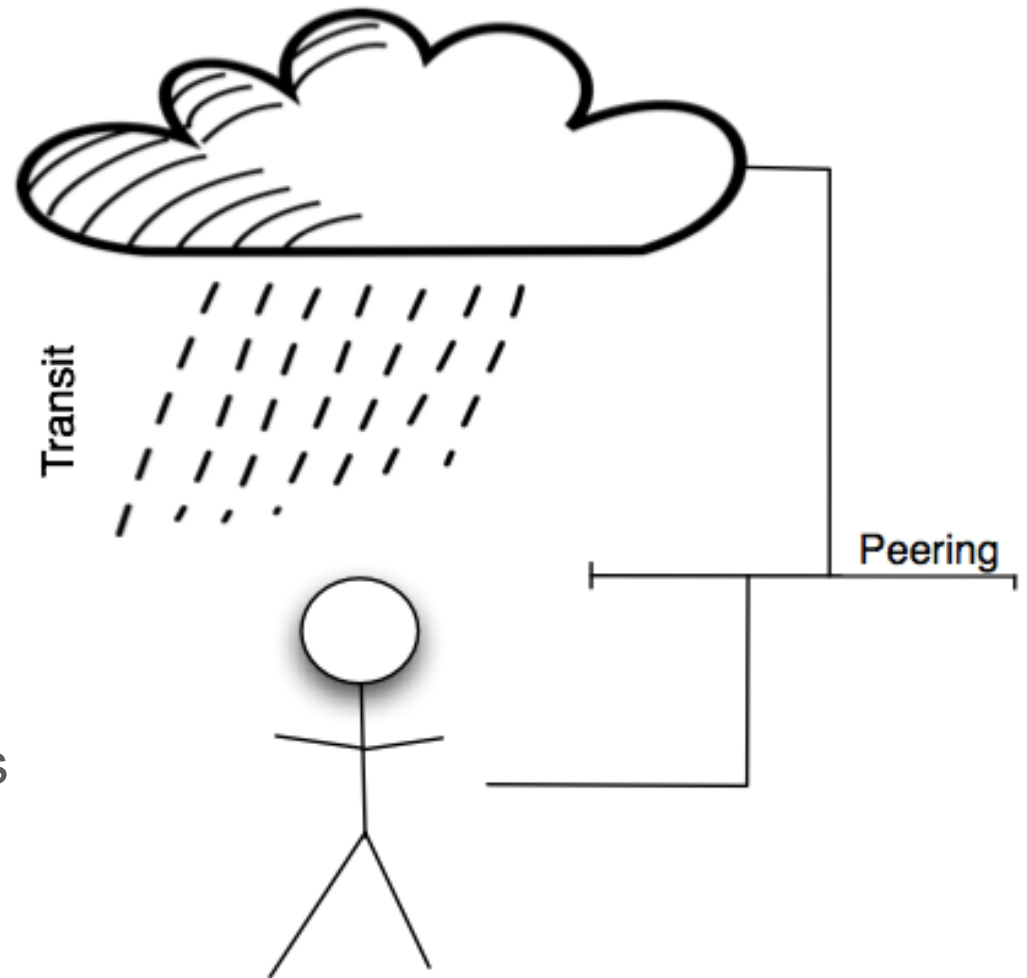


## 5 - Spread the pain

Have multiple paths over which traffic can arrive

A broader 'attack surface' gives you more options

You can apply different measures on different paths



## 6 - Null Routing

The ISP View



The Customer View



## 7 - Mitigation Appliances

Many vendors offer on-premises appliances

- Typically fixed N Gbps of capacity
- Some come with 'cloud' capabilities to use resources upstream

They will help defeat some attacks, but:

- They can be expensive
- You still need big pipes to ingest the traffic
- Not every attack vector will suit every device
- You need a human element to drive effective mitigation
- and...

## 8 - Know your Limits

The N+1<sup>th</sup> Gbps is a killer



Some day you're going to need a bigger boat

## 9 - Use Somebody Else's



There are options to mitigate attacks before they reach your network

Upstream providers may offer a mitigation service, or...

## 10 - Pass the Buck

There are third-party alternatives:

### **Content Distribution Networks**

- Push content out to a vast server footprint
- Primarily an end-user-experience / performance service
- But can also absorb DDoS attacks
- They do not suit all types of (legitimate) traffic

### **DDoS Protection Services**

- Have connectivity and mitigation capacity to absorb large attacks
- They pass 'clean' or 'post mitigation' traffic back to you
- via proxy or a direct link (real or tunnelled)



## Summary

- Be Prepared
- Be Nimble
- Be Aware
- Have Solid DNS
- Don't rely on state
- Know what your limits are
- Consider third party services