advania

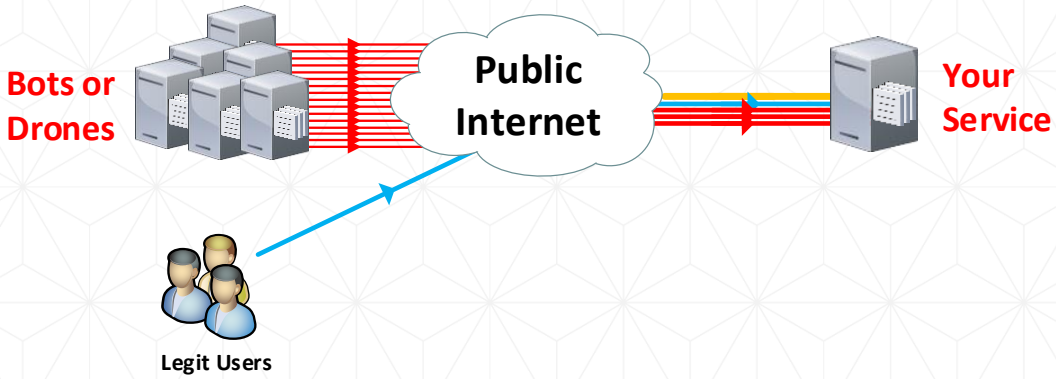
Welcome to IT

DDoS attacks

A brief overview of volumetric attacks and scrubbing solutions.

What is a **DDoS** attack?

- **DDoS** stands for Distributed Denial of Service.
- **DDoS** is commonly used to cover all types of malicious traffic generated to overwhelm your services. *(wether they are distributed or not ;)*



advania

The dangers of DDoS attacks – risk assessment

- We recommend a simple 3 question approach.
  - Do I have services open on the public internet?
    - eCommerce site, customer portal, hosted services etc
  - Do I have software that relies on public internet?
    - Like customer payments for retail stores, trading systems etc
  - How much value is associated with outage because of ddos?
    - 1 hour
    - 1 day
    - 1 week

advania

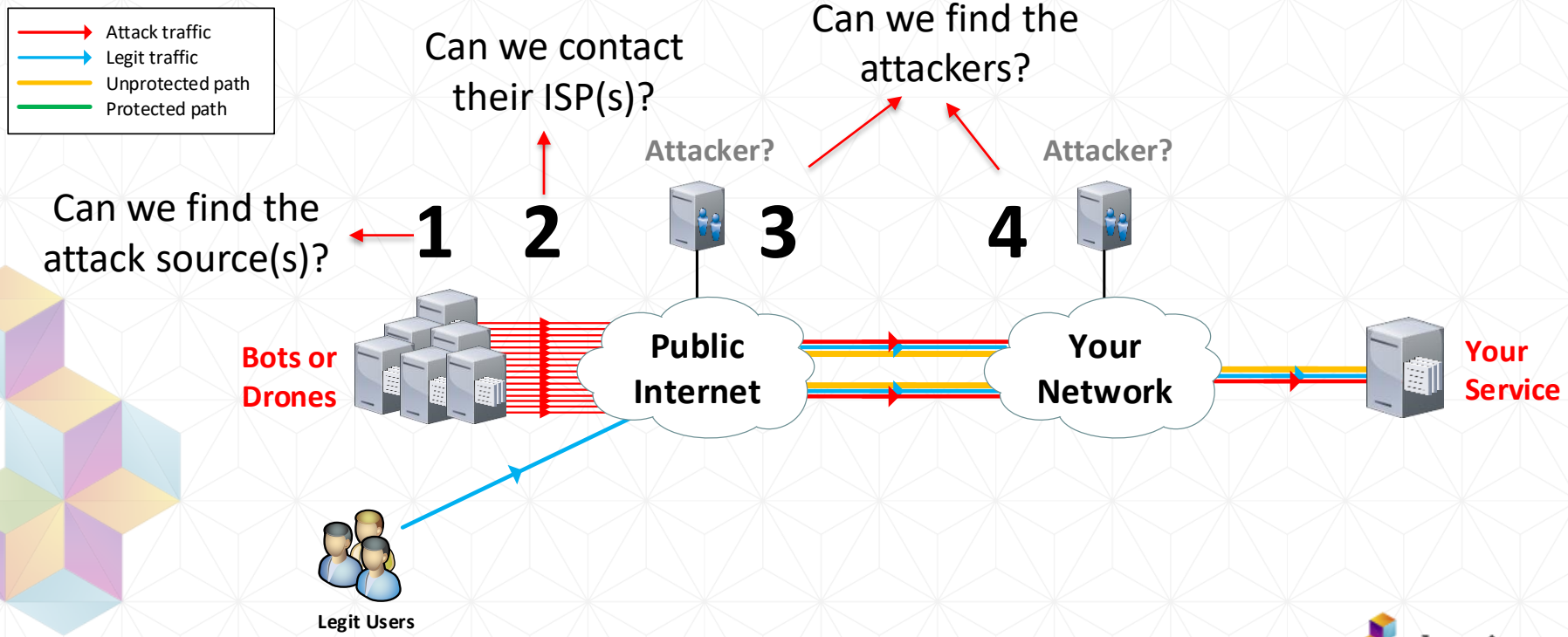
Statistics from Advania : AS30818/AS44515/AS50613

- Attacks by year
  - 2013: 163 attacks : **18Gb/s** average from top3 attacks
  - 2014: 1608 attacks : **35Gb/s** average from top3 attacks
  - 2015: 3541 attacks : **94Gb/s** average from top3 attacks
  - 2016: 5511 attacks : **153Gb/s** average from top3 attacks

- Other stats
  - Largest attacks we have seen:
    - **164.5Gbps** @ 15.8Mpps
    - **68Mpps** (co-ordinated) @ 48.3Gb/s
  - Most attacks happen in: May-June and November.

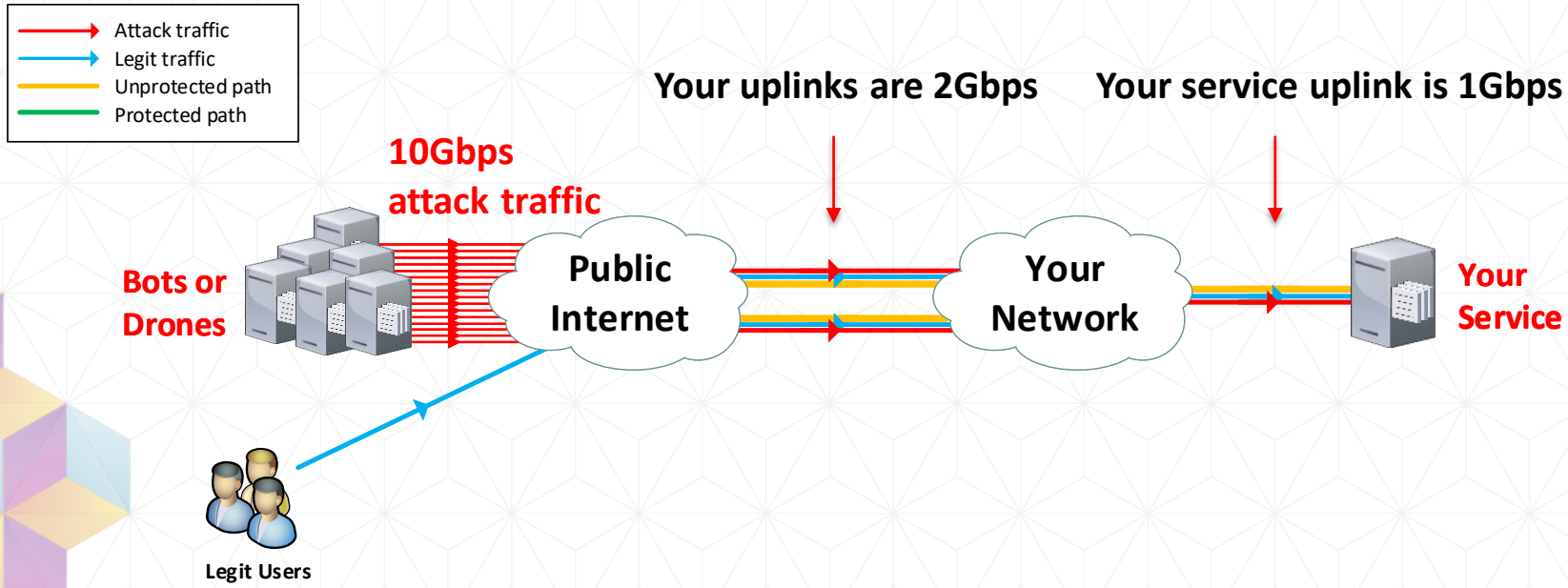
advania

Cant we just stop the attackers?



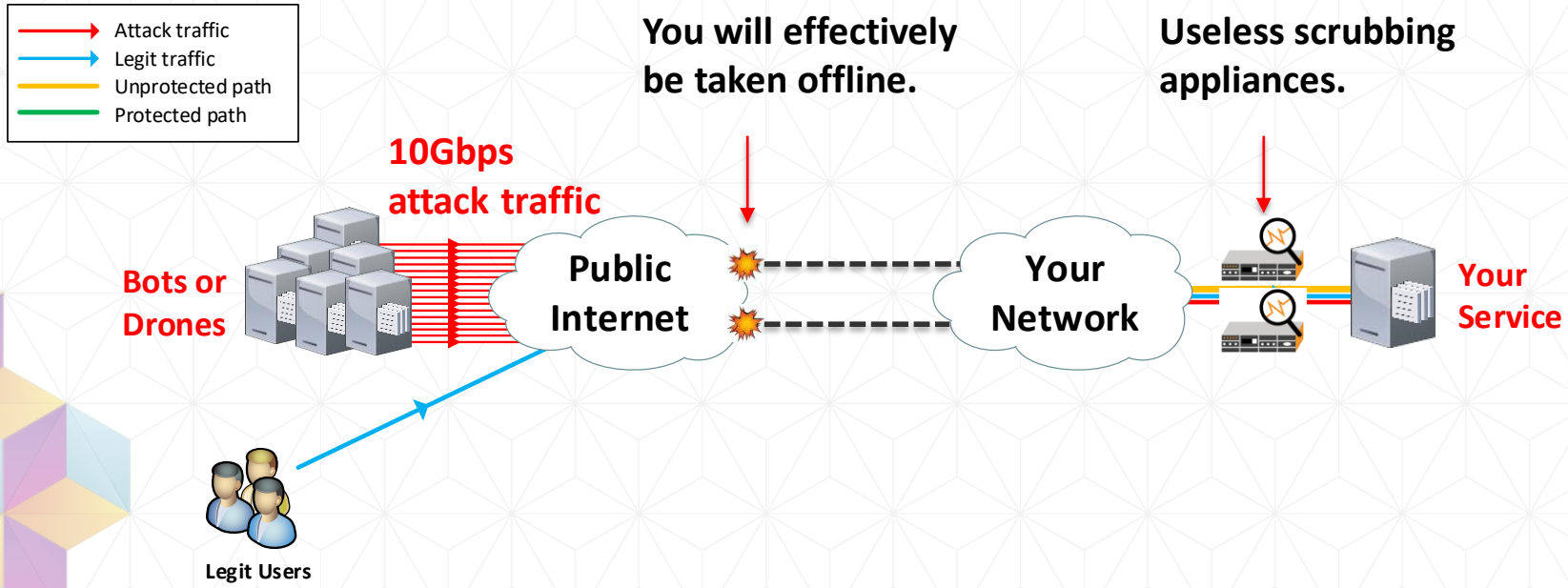
Spoofed sources, foreign ISPs, international law.. not worth the time and effort.

Anything we can do to solve it in-house?



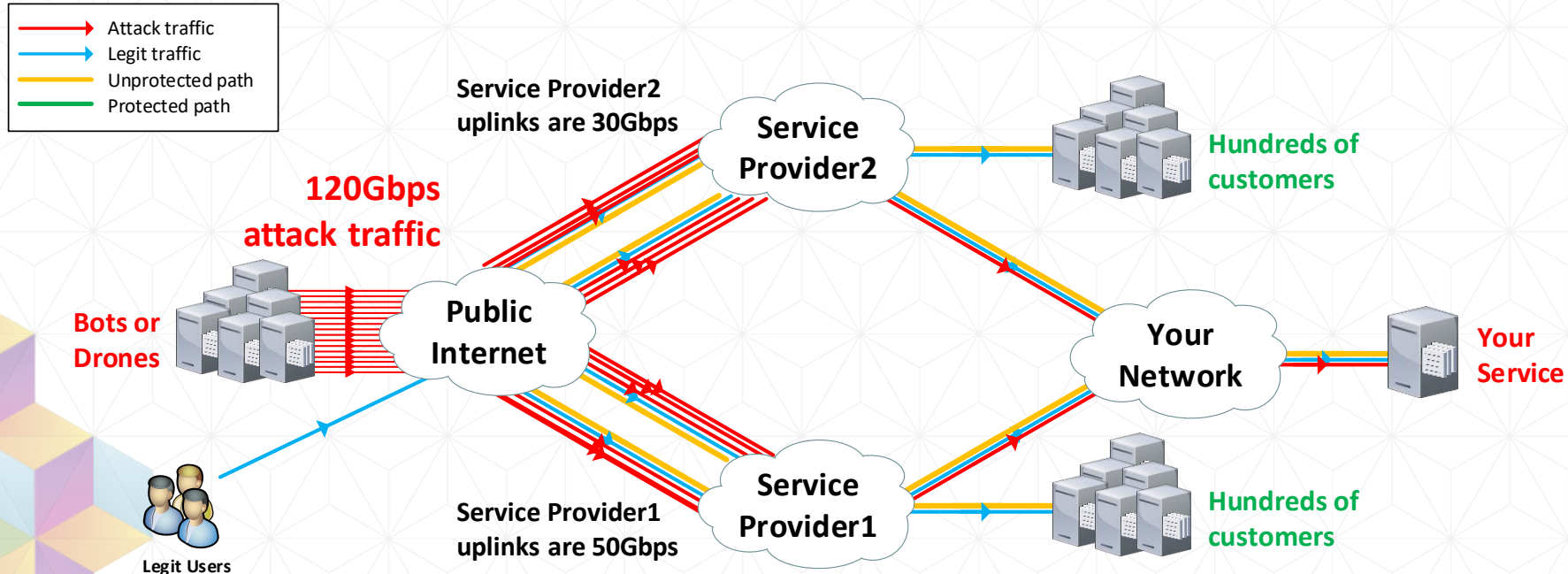
Your links are already overloaded.. you can‘t solve it in-house.

Anything we can do to solve it in-house?



Your links are already overloaded.. you can‘t solve it in-house.

Surely the service providers have me covered?



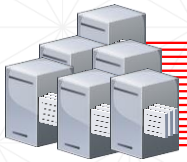
Sometimes, but mostly if you are lucky. **Lets review three attack scenarios:**

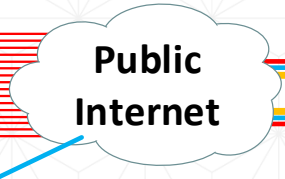
Blackholing example for Single target attack.

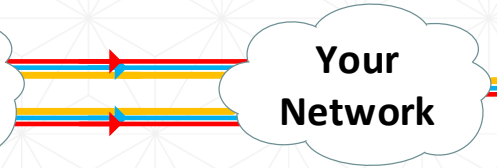
Spoofed SRC IPs:
200.10.20.123
88.103.31.4
199.16.16.2
34.34.22.1
144.204.103.100
...

Single DST IP:
195.140.122.10

Bots or Drones





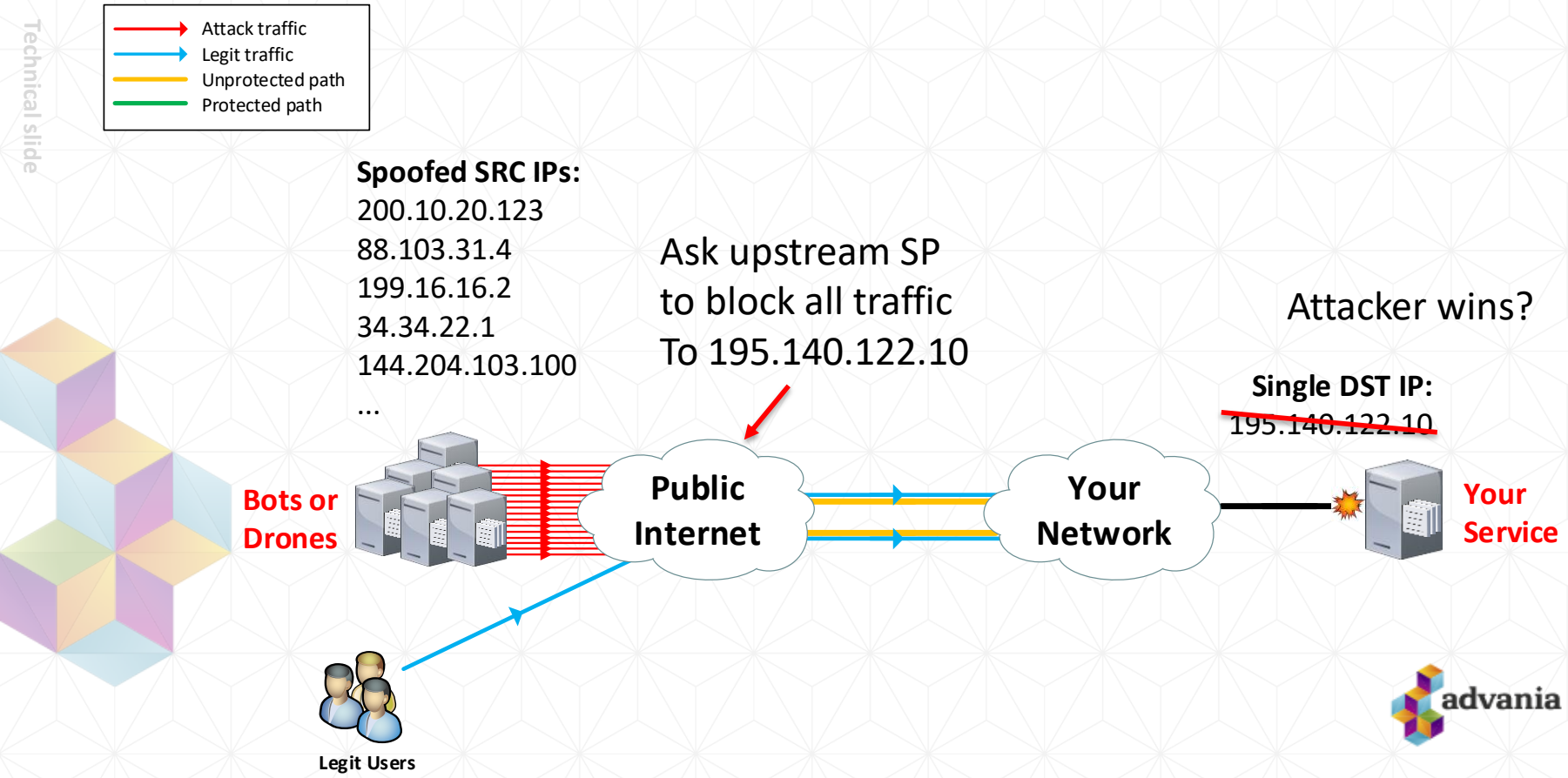


Your Service

Legit Users

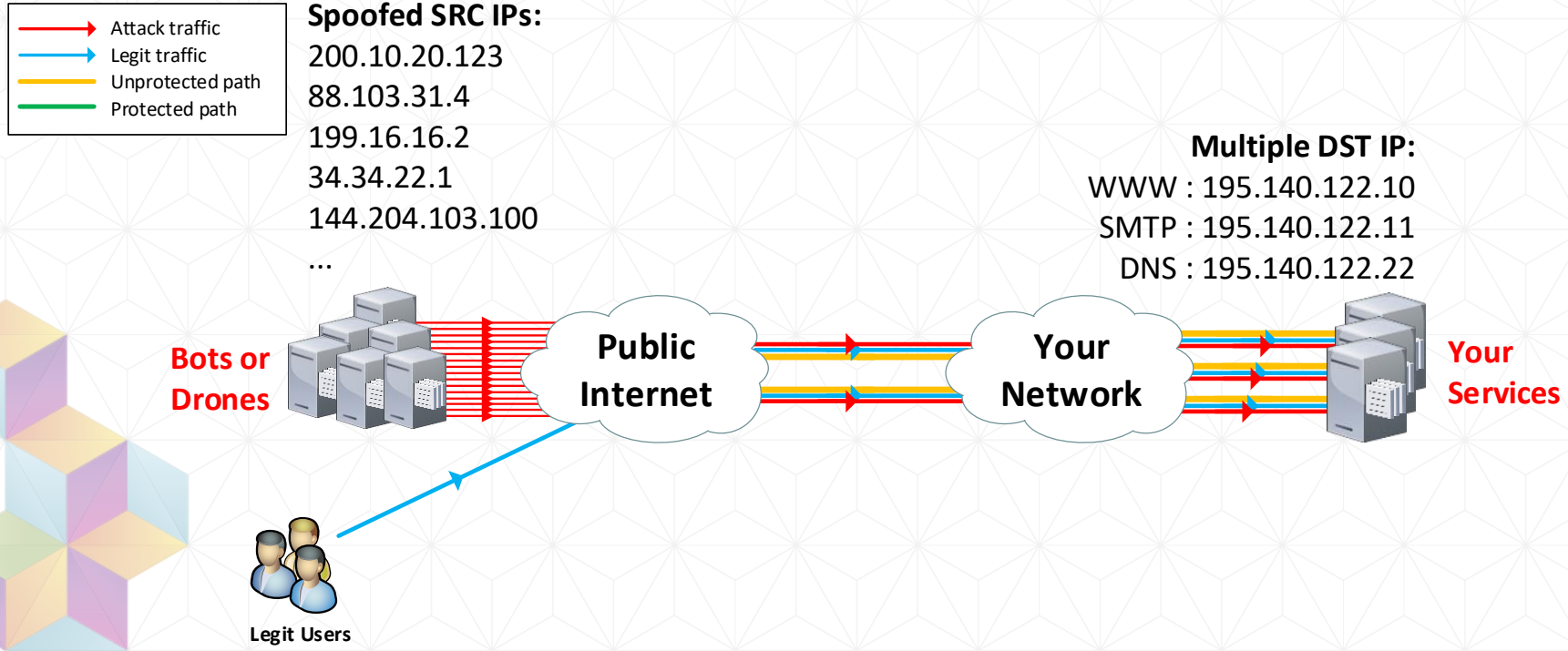
advania

Blackholing example for Single target attack.



advania

Can you blackhole multiple services? What if they are critical?



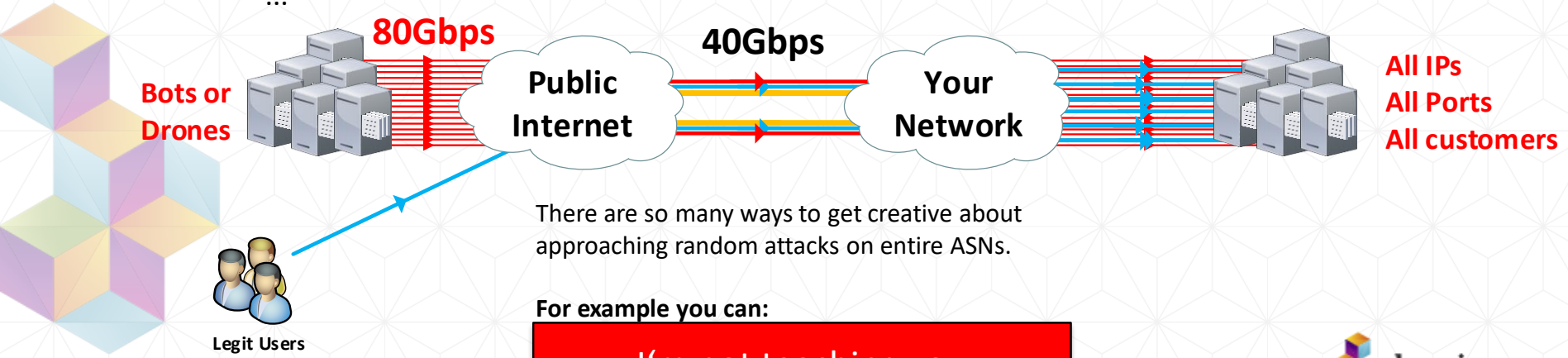
advania

What if they are all your services? All your IPs?

Technical slide

Spoofed SRC IPs:
200.10.20.123
88.103.31.4
199.16.16.2
34.34.22.1
144.204.103.100
...

Random DST:PORT_PROTO
195.140.122.1:80_tcp
195.140.122.2:4141_udp
195.140.122.3:53_udp
195.140.122.4:25_tcp
195.140.122.5:443_tcp
...



There are so many ways to get creative about approaching random attacks on entire ASNs.

For example you can:

I'm not teaching you how to do this. ;-)

advania

The challange for service providers.

- **Pricing and covering “peak time usage bandwidth”.**

1) The only real option is to get a scrubbing solution. Most scrubbing solutions are extremely expensive and cheap solutions are usually crap.

2) The most nasty attacks force SP to move all traffic to scrubbing path, this requires full peak time bandwidth to the scrubbing solution.

These two are very hard to solve together.

advania

The challange for regular companies:

- **Most attacks will take you offline..**

1) **Finding a sensibly priced solution that offers acceptable protection.**
2) **Everyone will convince you their product is amazing.**

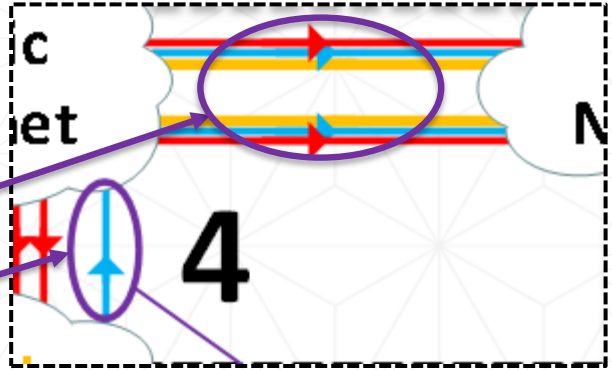
Lets review the flagshit products used by DDoS protection providers.

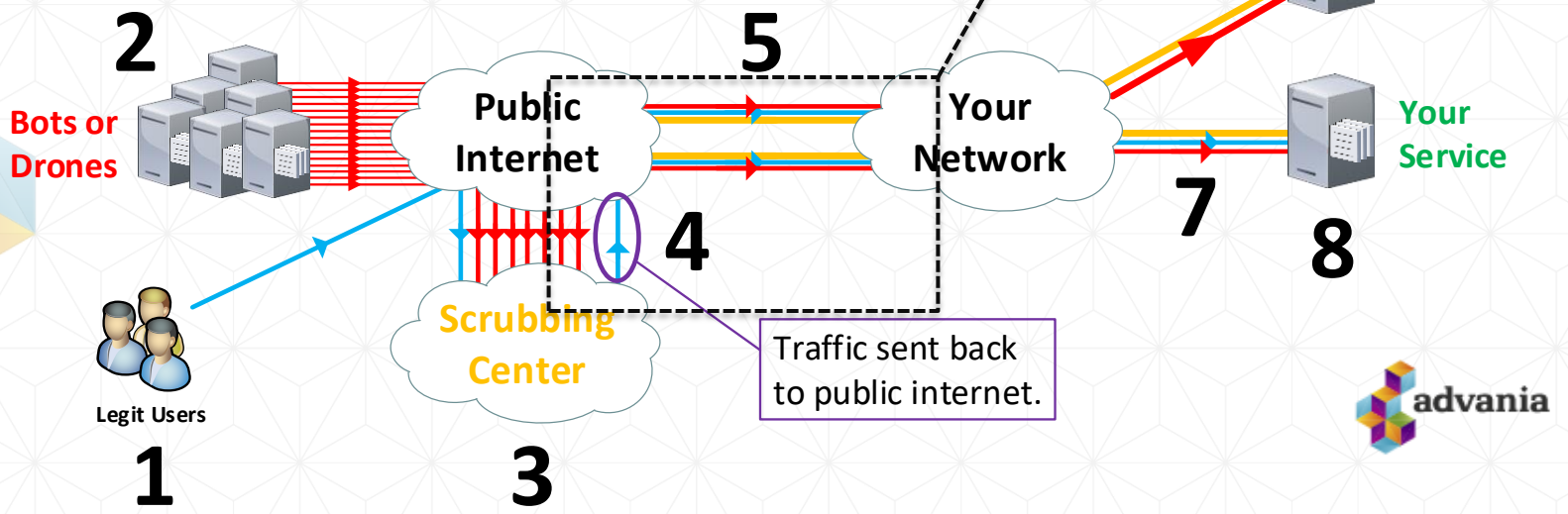
advania

Reverse-Proxy or GRE Tunnel

The way most these protection services are setup it's really easy to break them.

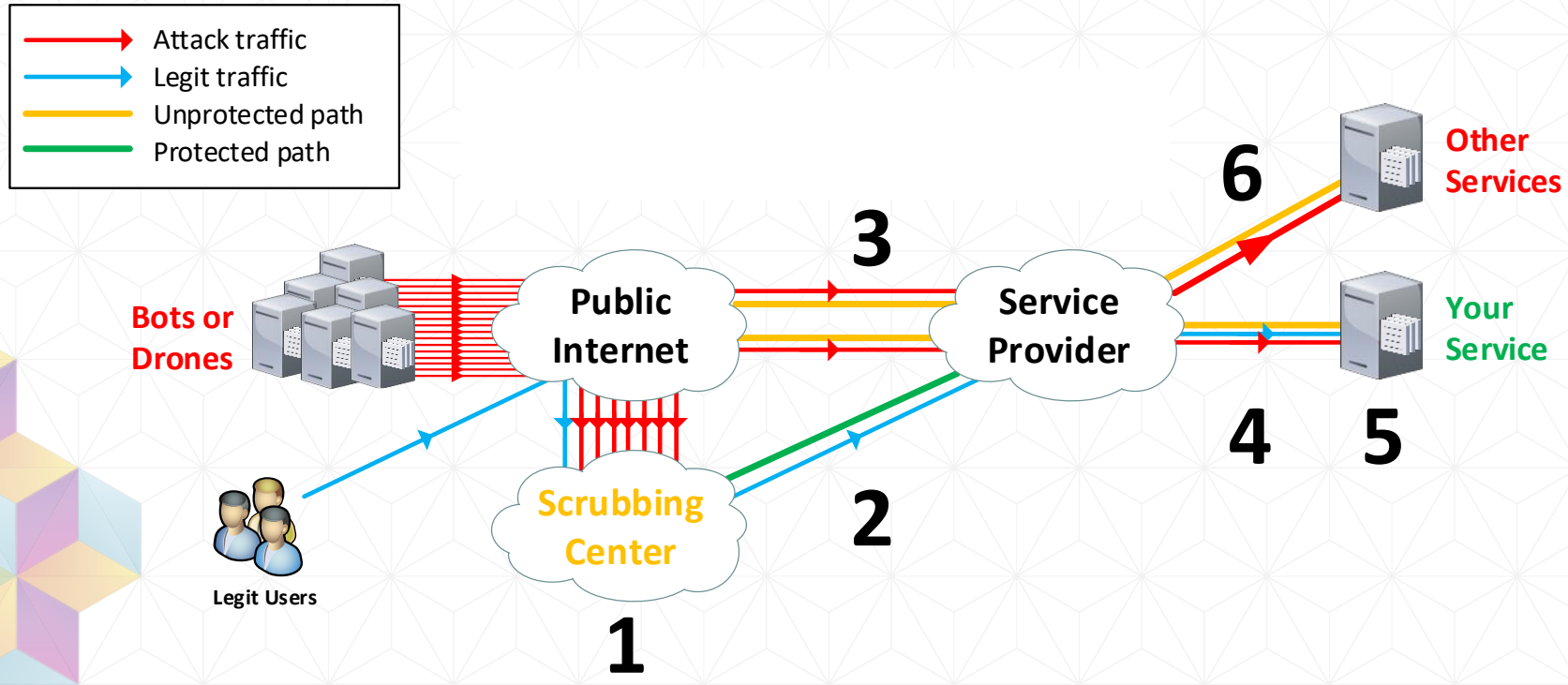
Protected paths to backhaul the traffic cost as much as dedicated cross-connects.





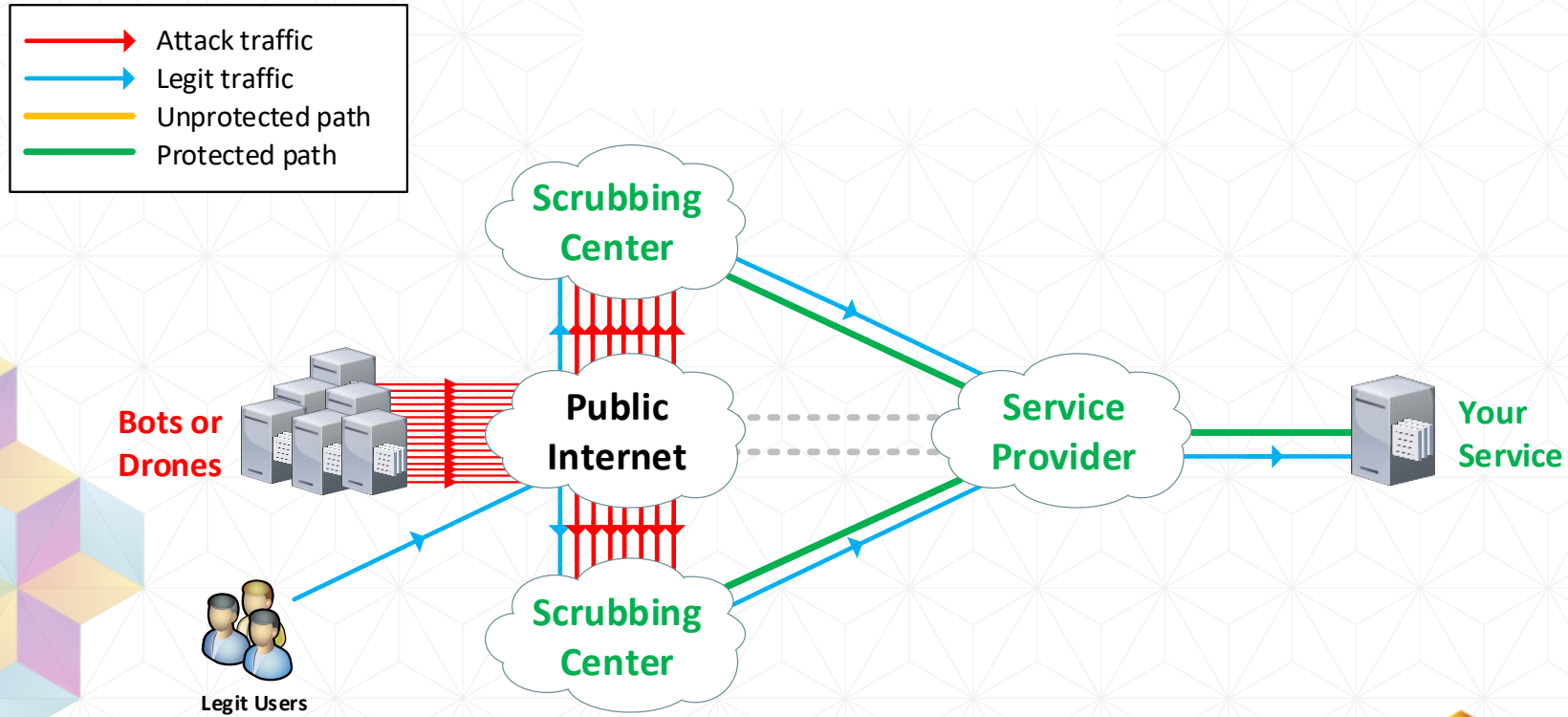
advania

Solutions: Partial dedicated bandwidth



This is good, but not optimal. You can‘t handle peaktime usage.

Optimal solution, two scrubbing centers, full peak time bw.



.. with scrict SLA and service monitoring. And lots and lots of effort to maintain..

Beware of the DDoS scrubbing industry.

- **Unfortunately the dream client is un-protected and desperate with wallet wide open willing to pay anything.**

- **The reason we started focusing on DDoS solutions was that in 2013 we had only black-holing as an option and one of our customers we had to block. He signed for a crappy solution with a major DDoS scrubbing center out of desperation at 03:00 in the morning.**
  - **He signed a contract worth 126.000 USD at $3500 a month locked for 3yrs**
  - **The contract covered a single IP with 10Mbps of clean traffic**
  - **He had to let employees go to pay for the DDoS contract**
  - **This was basically extortion pricing by a major brand company**
    - **Hint, they are still the largest DDoS scrubbing provider**

advania

This concludes the slideshow.

Thank you for your attention.

advania

Does the „attack type“ matter when talking about volumetric attacks?

- Nope.. the first problem is capacity, this is only solved by having more than the attackers.

- The second problem is having the capacity in the right location.
  Ex: a *huge attack sourced 90% from within EU does not benefit from the combined scrubbing capability of EU+US+ASIA.*

- The third problem is **false positives**.

Scrubbing Center solutions.

- The key to defeating volumetric attacks that outrank your capacity is a service with more capactiy.

- Generally easy to filter: if **source port** = **123** then **drop**
- Some carriers allow stateless filters like this.

advania

What does this mean?

- You won‘t be able to solve the first problem. *(statistics to follow)*

  Unless you are Tier1 carrier size or build your own SC business.

- You have to rely on volumetric scrubbing solutions and hope they perform the way you need them to perform.

- Furthermore, you can ‚make them‘ perform the way you want.

So what are the most common tools to deal with DDoS?

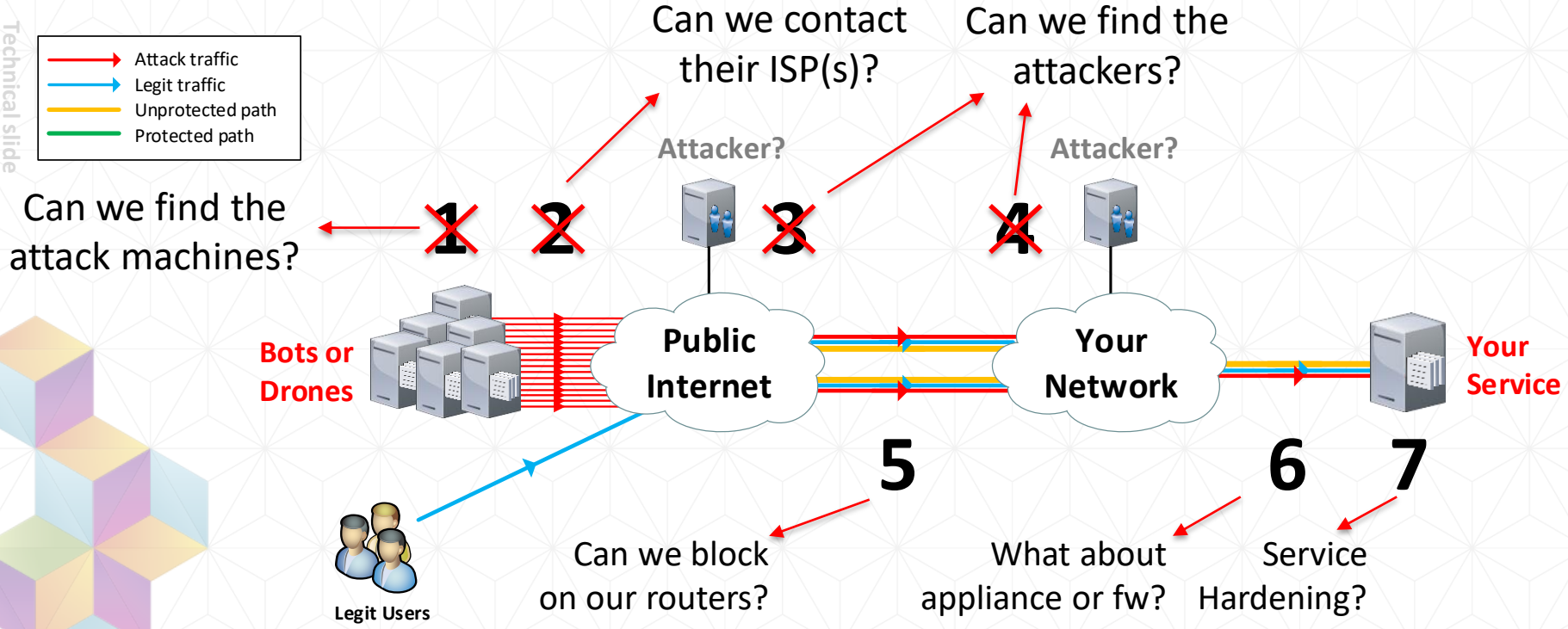
1. Blackholing, null-routes signaled via BGP upstream.
2. Signaling stateless ACLs via BGP or API upstream.

and hope, lots and lots of hope.

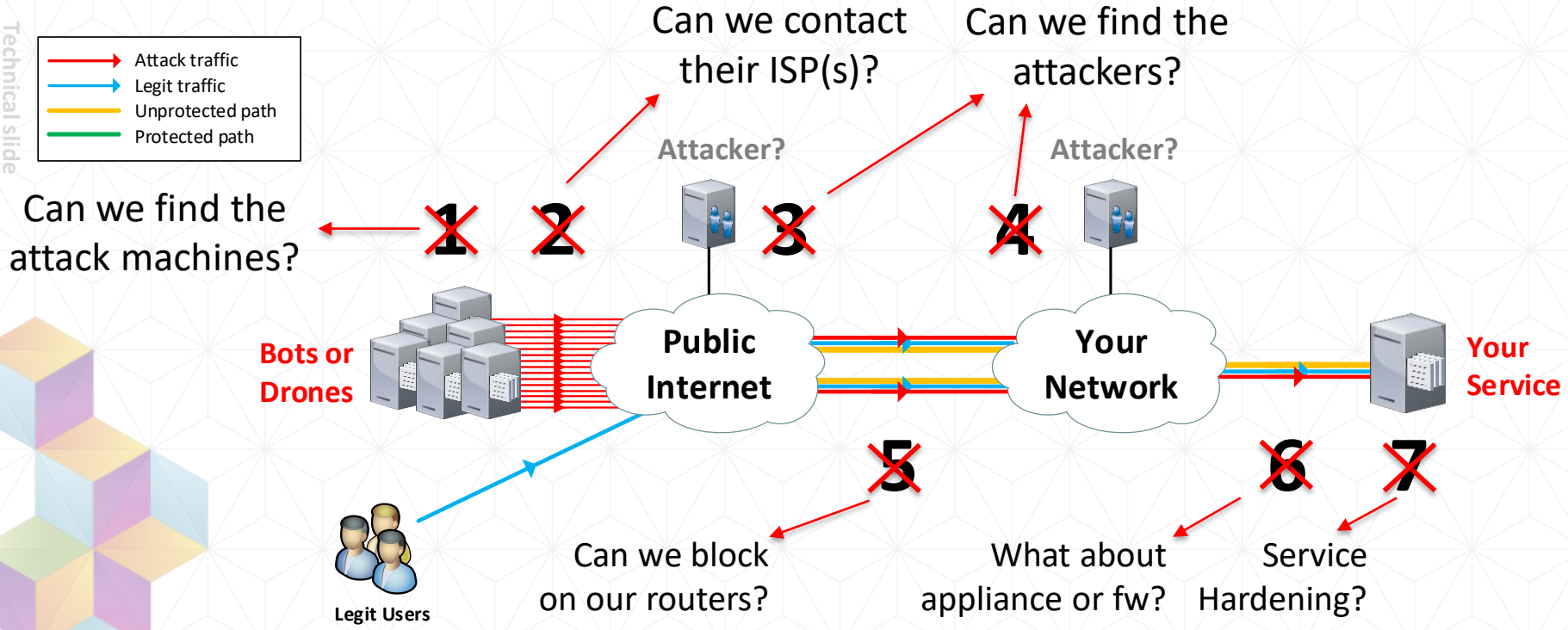
A sensible approach for cutting costs but likely less sensible for your business.

advania

Overview, typical attack



Overview, typical attack



Quick recap of the key points so far:

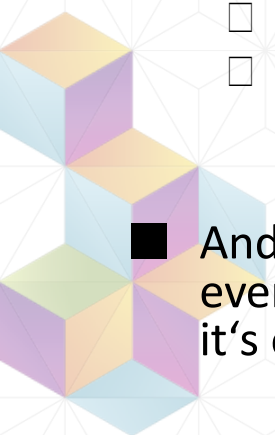
- You won‘t have the capacity in the right places to carry attack traffic reliably so in-house solutions are off the table.
  - This fact is omitted from every DDoS product sales pitch.

- You have to protect against random DST attacks because when they become the norm (and they will) the common approaches to deal with attacks are useless.

advania

So i got a scrubbing solution, all is ok now?

- Not even close, in our experience at Advania this is not a very trustworthy business.
  - They send your traffic through an incredibly intrusive scrubbing engine and provide you wil little or no information about what is being done with the traffic.
  - Not a single one we have talked to monitor false positive rates in any sensible way.
  - We had to solve these tasks ourselves and in co-operation with sensible partners.
    - **This has been a very hard task.**
- And furthermore a single scrubbing center solution won‘t be able to handle everything, they will fail you at some point. It‘s the nature of the business and it‘s ok.
- Planning for failure is the best solution, use more than one SC.



Final note

- The scrubbing centers will at entry level will cost you a lot and provide you with a mediocre service at best.
- This can be solved.

advania

Next up: final slide

Solutions: Appliances for SP or Customer sites.

Foundation slide

- These won‘t solve volumetric attacks „traffic higher than you can handle on your network“.
- You need to carry enough bandwidth to protect yourself. This is expensive and kind of crazy.
- The appliances themselves are expensive.
  - Extreeemely expensive.
  - Really.. Really.. Expensive.
  - Seriously.. pay the ddos attackers if you can.

radware f5 ARBOR NETWORKS Check Point

advania

Solutions: Reverse-Proxy or GRE Tunnel

Foundation slide

Approach: „Quick‘n‘dirty“

radware ARBOR NETWORKS f5 Check Point

- You are not protected against bypass attacks.
- You are not protected from attacks on shared public path.
- You are not protected from all out attack on hosting provider ASn.
- Moving traffic via DNS means the attackers still know your original ASn.
- You go always-on and spent time and effort hiding your source IPs and still get taken out by attacks on other customers.
- When provided as complete solution this is a borderline scam.

DOS arrest neustar VERISIGN CLOUDFLARE

BLOCKDOS ZENEDGE PROLEXIC Now part of Akamai

corero IMPERVA INCAPSULA