



# Handling of DDos attacks

By Kajetan Staszkiwicz, SysAdmin @ InnoGames

# About me

- Neighbourhood network admin since 1999.
- Worked for various local ISPs in Kraków.
- Currently Директор Интернета at InnoGames GmbH.



**1**

What is a DDoS attack and how does it work?

**2**

Why are we attacked?

**3**

How do DDoS attacks affect (hard|soft)ware?

**4**

How do we detect DDoS attacks?

**5**

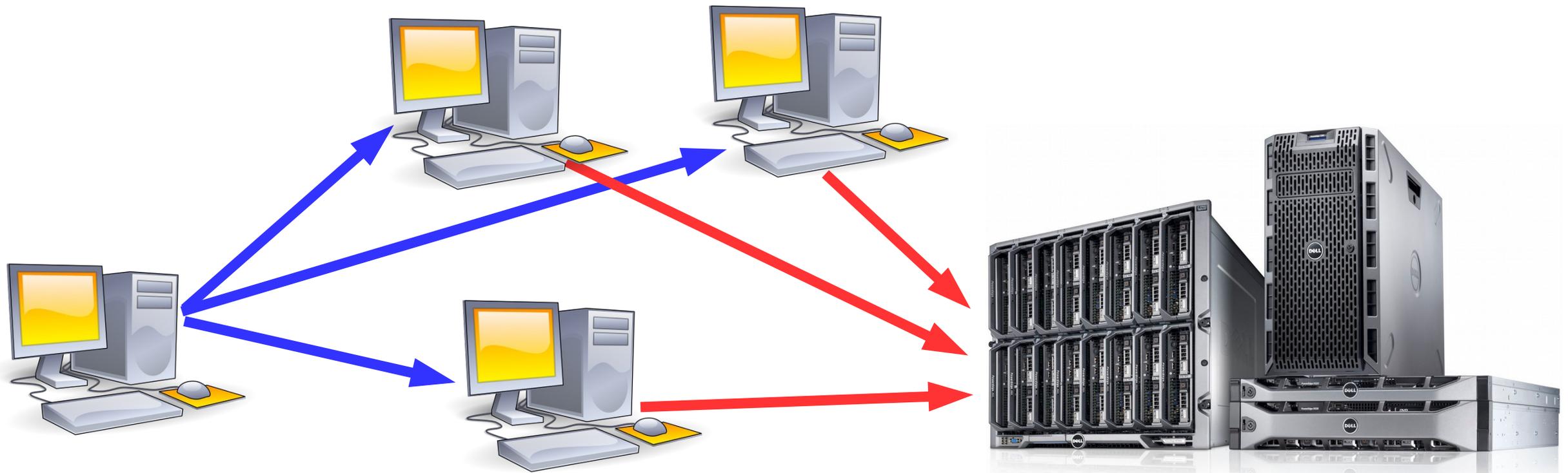
How do we protect against DDoS attacks?

What is a DDoS attack and how does it work?



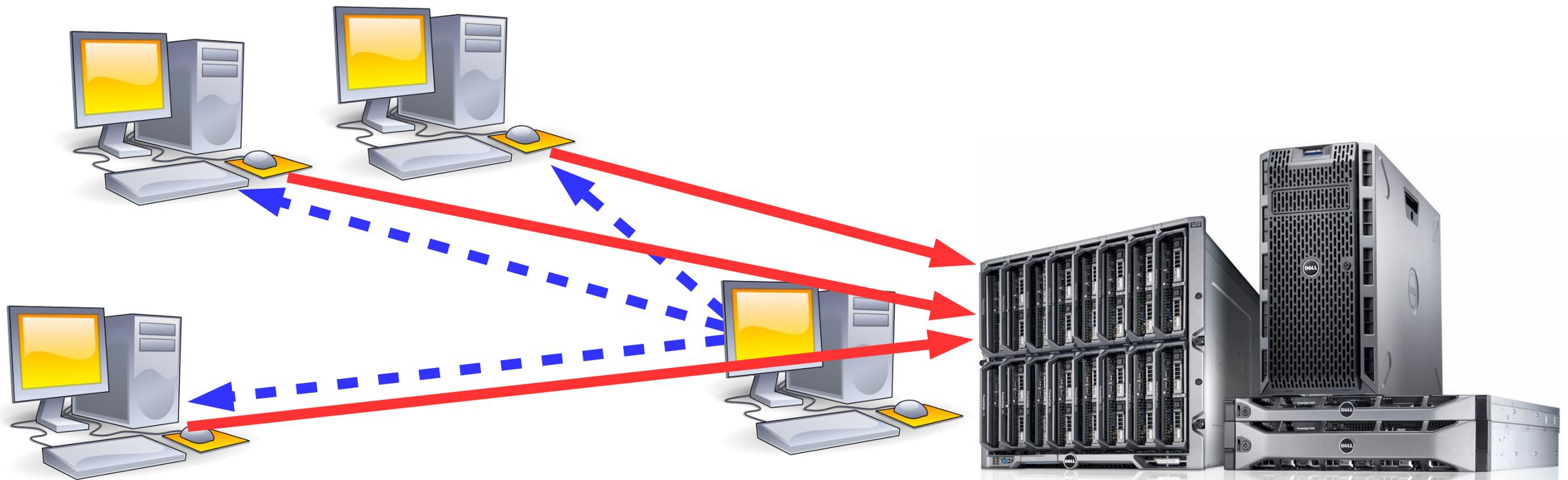
### Direct attack:

- Attack force (pps, rps) limited by computer and Internet connection of attacker
- Source Datacenter might filter attack.



Distributed Denial of Service:

- Attack force (pps, rps) is multiplied.
- Attacker needs control over attacking machines.



### Distributed Denial of Service with Reflection:

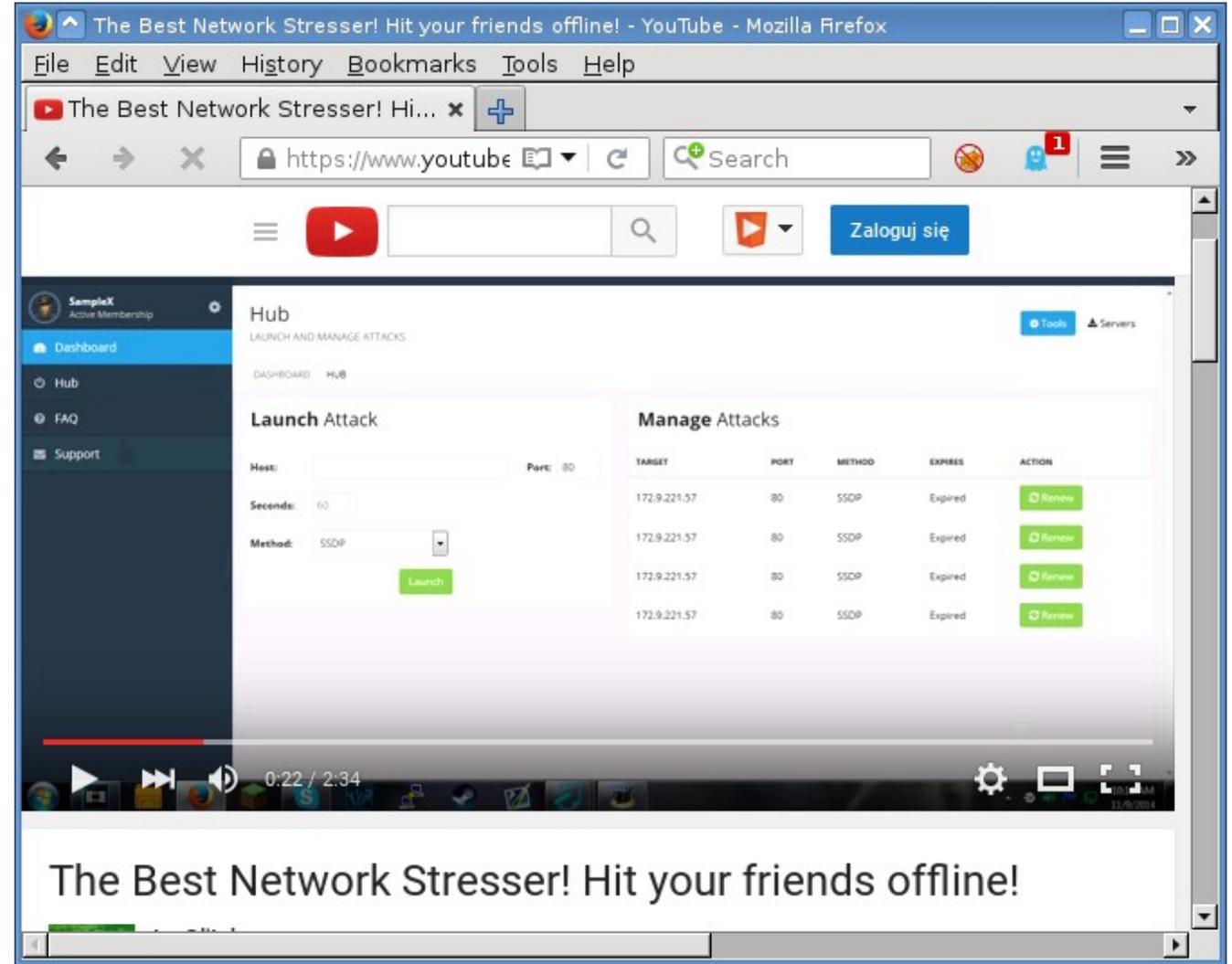
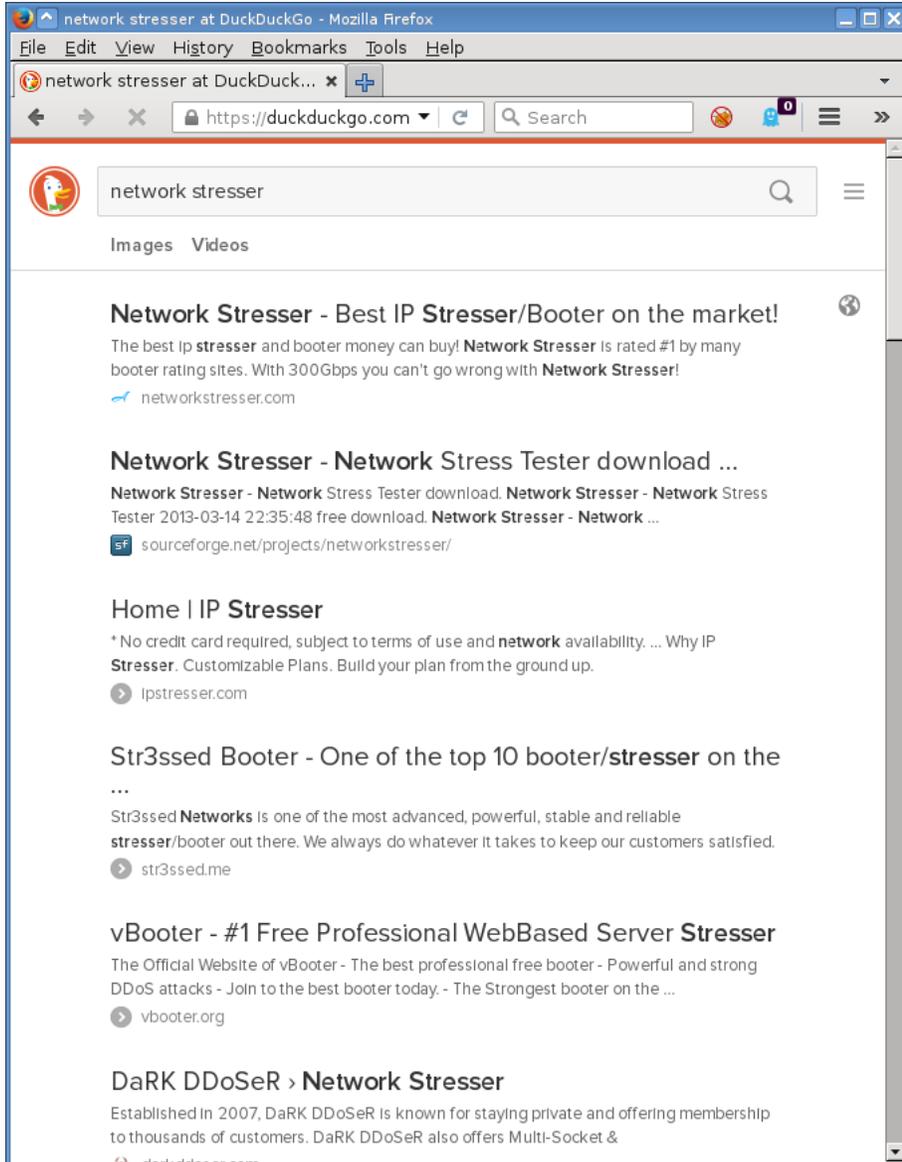
- Attack force (pps, rps) is multiplied.
- Innocent, uninfected machines perform attack for the attacker.
- Attack sources think that we attack them – extra paperwork.

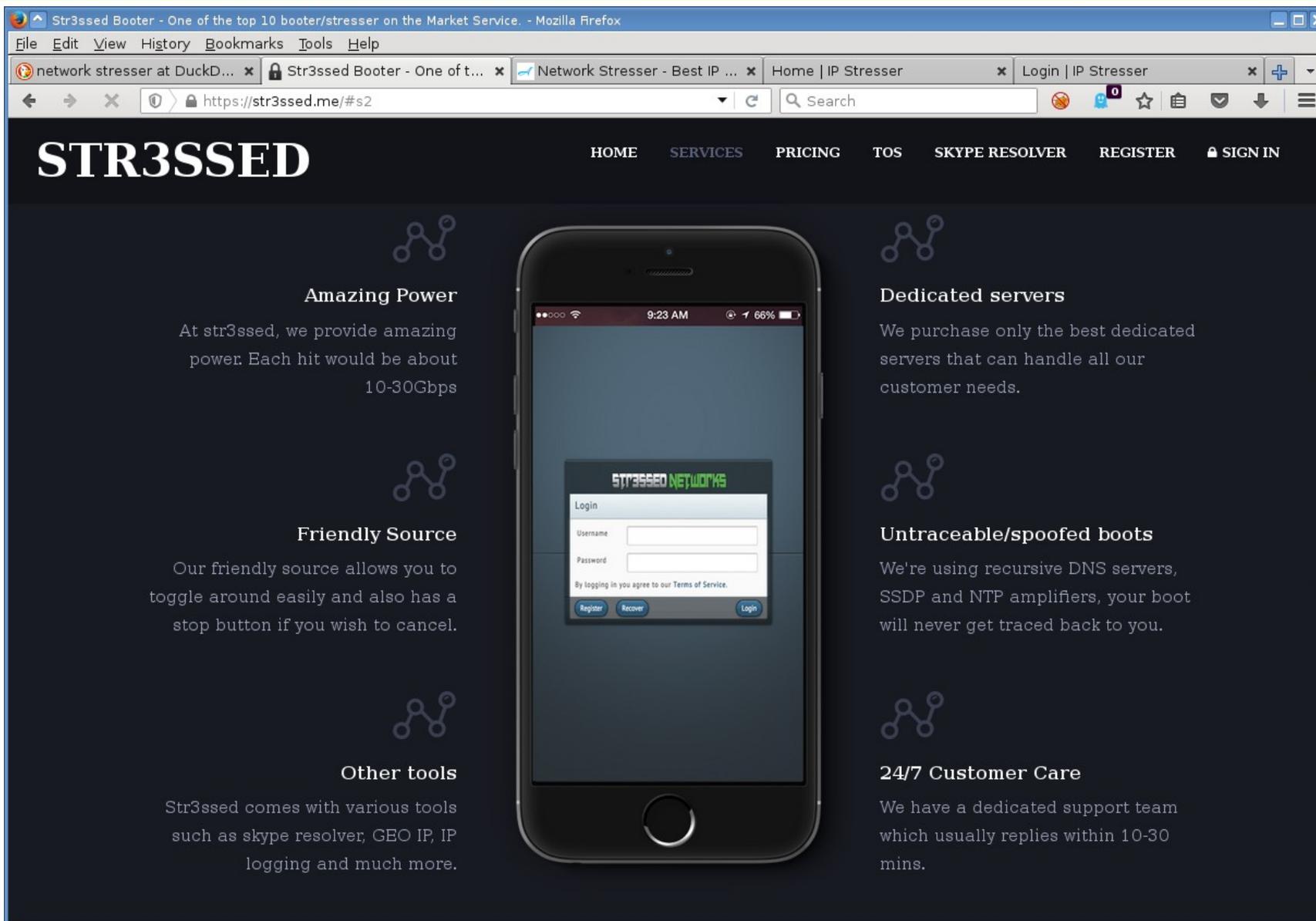
## How is it possible?

- Internet providers and Datacenters don't always verify source addresses of packets from their networks.
- For reflection attack connectionless, UDP-based services (DNS, SNMP, NTP) are used:
  - DNS – up to 54×, 179× with DNSSEC
  - NTP – up to 556×
  - 300Gb/s attack can be performed.

## How to attack?

- Maybe having own server with big link?
- Maybe searching in TOR/Darknet?
- Maybe asking your friends to constantly hit F5 in web browsers?





Str3ssed Booter - One of the top 10 booter/stresser on the Market Service. - Mozilla Firefox

network stresser at DuckD... x Str3ssed Booter - One of t... x Network Stresser - Best IP ... x Home | IP Stresser x Login | IP Stresser x

https://str3ssed.me/#s2

## STR3SSED

HOME SERVICES PRICING TOS SKYPE RESOLVER REGISTER SIGN IN

### Amazing Power

At str3ssed, we provide amazing power. Each hit would be about 10-30Gbps

### Friendly Source

Our friendly source allows you to toggle around easily and also has a stop button if you wish to cancel.

### Other tools

Str3ssed comes with various tools such as skype resolver, GEO IP, IP logging and much more.

### Dedicated servers

We purchase only the best dedicated servers that can handle all our customer needs.

### Untraceable/spoofed boots

We're using recursive DNS servers, SSDP and NTP amplifiers, your boot will never get traced back to you.

### 24/7 Customer Care

We have a dedicated support team which usually replies within 10-30 mins.

STR3SSED NETWORKS

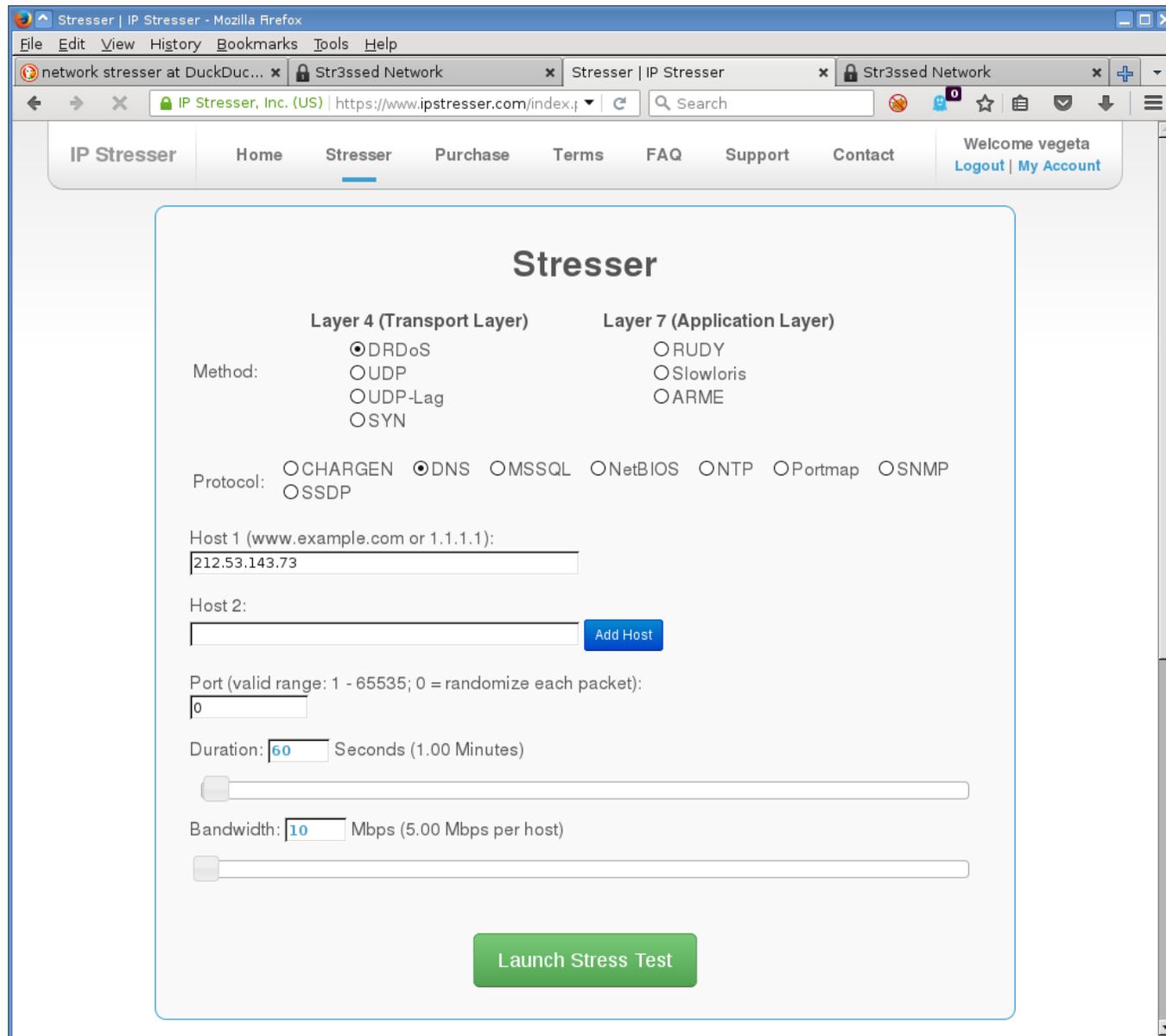
Login

Username

Password

By logging in you agree to our Terms of Service.

Register Recover Login



The screenshot shows the IP Stresser website interface. The browser window title is "Stresser | IP Stresser - Mozilla Firefox". The address bar shows "https://www.ipstresser.com/index.js". The navigation menu includes "IP Stresser", "Home", "Stresser", "Purchase", "Terms", "FAQ", "Support", and "Contact". A user is logged in as "vegeta" with options for "Logout" and "My Account".

## Stresser

**Layer 4 (Transport Layer)**

Method:

- DRDoS
- UDP
- UDP-Lag
- SYN

**Layer 7 (Application Layer)**

- RUDY
- Slowloris
- ARME

Protocol:

- CHARGEN
- DNS
- MSSQL
- NetBIOS
- NTTP
- Portmap
- SNMP
- SSDP

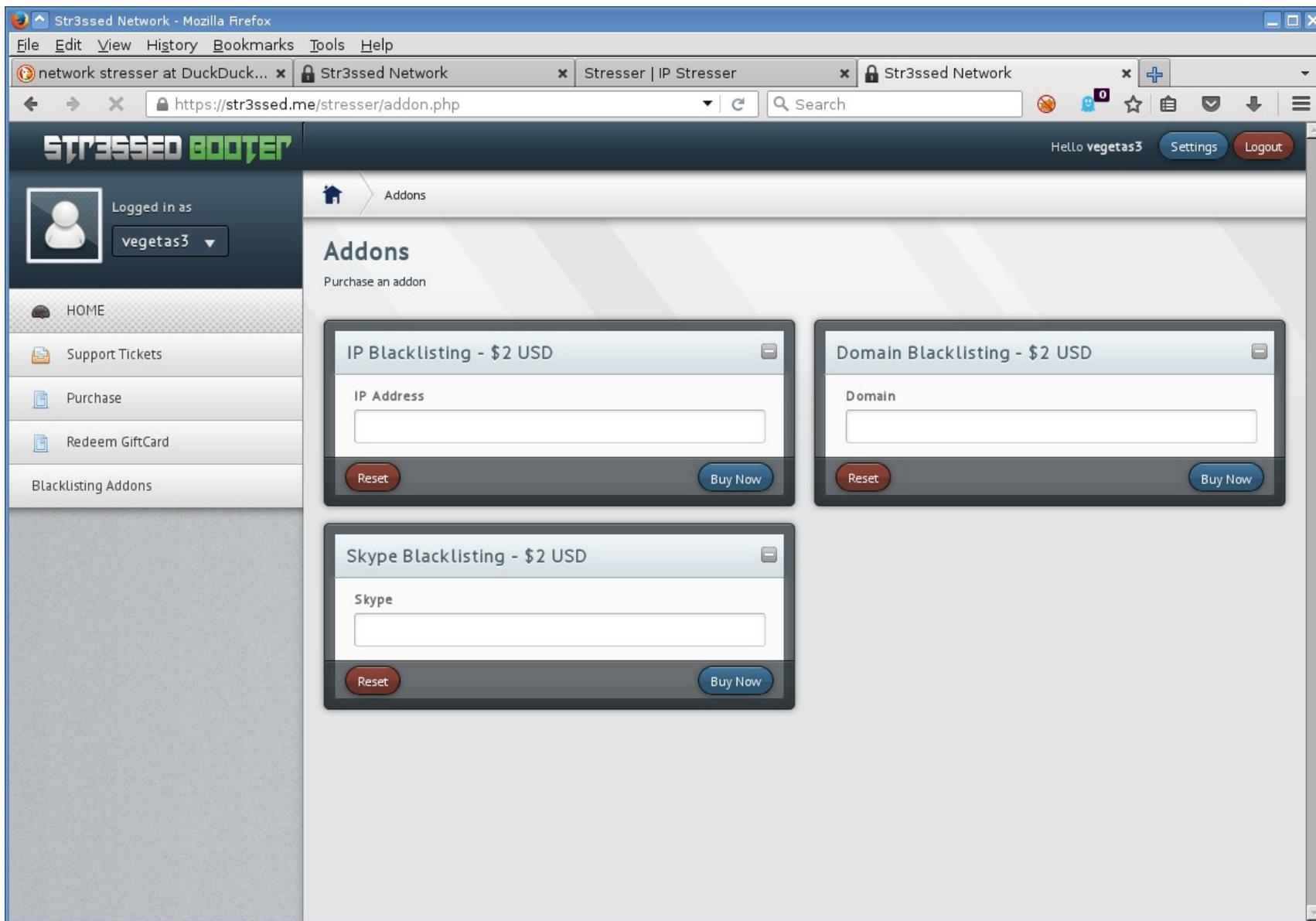
Host 1 (www.example.com or 1.1.1.1):

Host 2:

Port (valid range: 1 - 65535; 0 = randomize each packet):

Duration:  Seconds (1.00 Minutes)

Bandwidth:  Mbps (5.00 Mbps per host)



The screenshot displays a web browser window with the URL `https://str3ssed.me/stresser/addon.php`. The page is titled "STRESSED BOOTER" and shows a user logged in as "vegetas3". The main content area is titled "Addons" and contains three purchase options, each for \$2 USD:

- IP Blacklisting - \$2 USD**: Includes a text input field for "IP Address", a "Reset" button, and a "Buy Now" button.
- Domain Blacklisting - \$2 USD**: Includes a text input field for "Domain", a "Reset" button, and a "Buy Now" button.
- Skype Blacklisting - \$2 USD**: Includes a text input field for "Skype", a "Reset" button, and a "Buy Now" button.

The left sidebar contains navigation links: HOME, Support Tickets, Purchase, Redeem GiftCard, and Blacklisting Addons. The top right corner shows "Hello vegetas3" with "Settings" and "Logout" buttons.

# What is targeted?

- UDP-based reflection: volumetric attack saturating network links.
- TCP SYN flood: web, mail servers, loadbalancers, firewalls: resource depletion.
- ICMP floods: no idea, probably side effect.

# SYN Flood

- For each SYN kernel accepts a connection
- TCP stack resource shortage.
- Legitimate clients won't be able to connect.
- Maybe something crashes and does not recover even if the attack is stopped
- Does not affect stateless routers nor switches.

# UDP Flood

- Does not affect particular application directly.
- Saturates network links: ours and datacenter's.
- Can drop Datacenter from Internet if BGP sessions break.
- Can cause trouble only for some customers.

Why are we attacked?

# Attacks you read about

- Days long.
- Ransom demands.
- Check blogs of Arbor, CloudFlare, Incapsula etc.

# Why are we attacked?

- Attacks are short (minutes, tens of minutes).
  - AFAIK nobody ever wanted money.
  - Particular markets and worlds are attacked more often.
- Advantage of blocking other players from playing?

How do DDoS attacks affect (hard|soft)ware?

## What we see at InnoGames

- SYN Floods
- UDP Floods – recently the most popular thing.
- Usually some combination of the above.

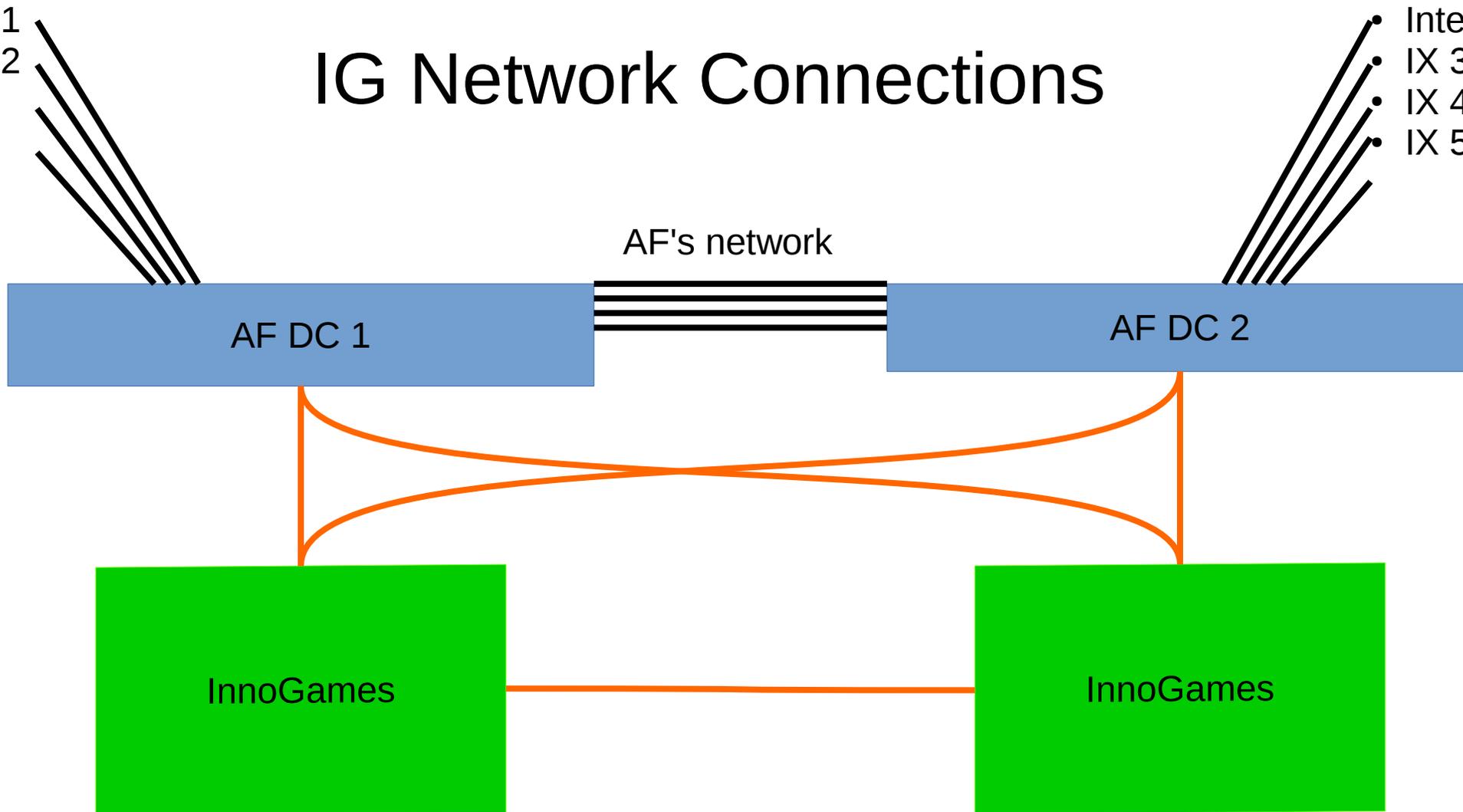
## Other possibilities

- Long & Slow Layer7 attacks – not really seen but maybe they happen?

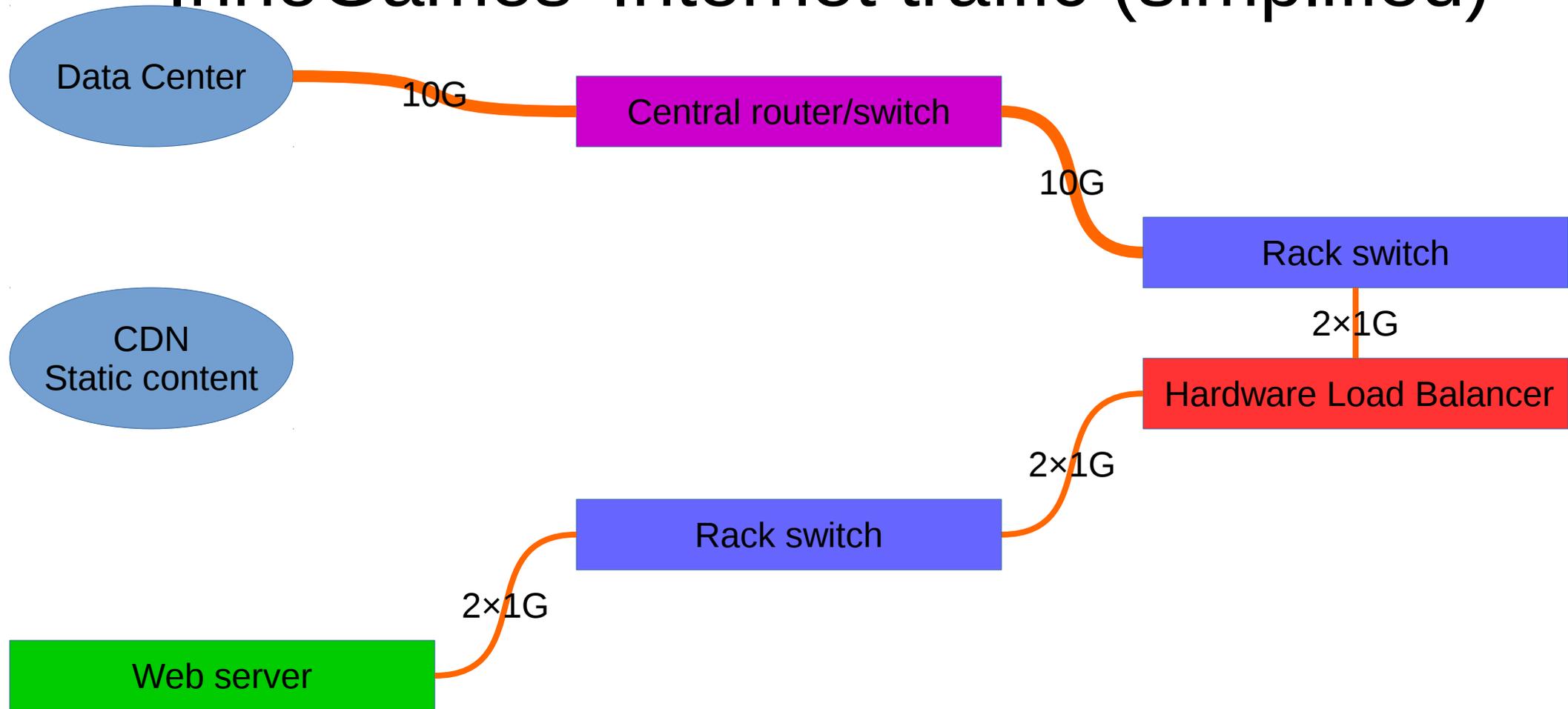
- Internet 1
- Internet 2
- IX 1
- IX 2

# IG Network Connections

- Internet 3
- IX 3
- IX 4
- IX 5



# InnoGames' Internet traffic (simplified)



## Effects on Datacenter

- Huge UDP Floods can drop whole Datacenter from the Internet (dead BGP).
- Or just make it unreachable from only some ISPs.
- Attacks on other customers can (will) influence us.
- You might not encounter any problems from home or office.

# Effects on Network

- UDP Floods only.
- Saturation of links.
- Other projects affected when one is under attack.
- Generally the same type of trouble as in Datacenter.

## Effects on LoadBalancers

- 36 HWLBs running FreeBSD and pf.
- 2 or 3 HWLBs per game.
- SYN Floods: state and source table overflow.
- UDP Floods: link ( $n \times 1G$ ) bandwidth overflow.
- Other projects affected when one is under attack.

# Effects on Servers

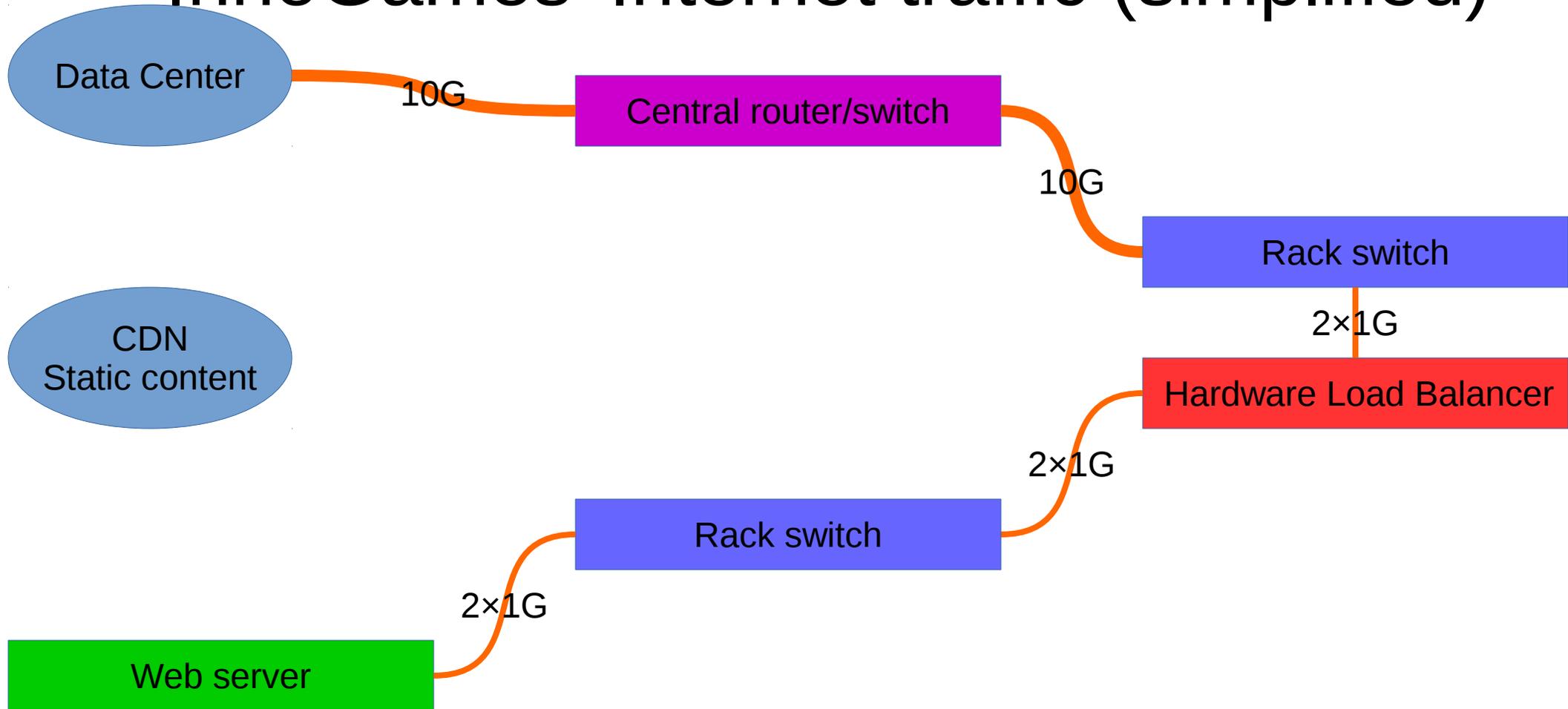
- Attacks stop on LoadBalancers and never really reach servers.

How do we detect DDoS attacks?

## How is an attack seen by us?

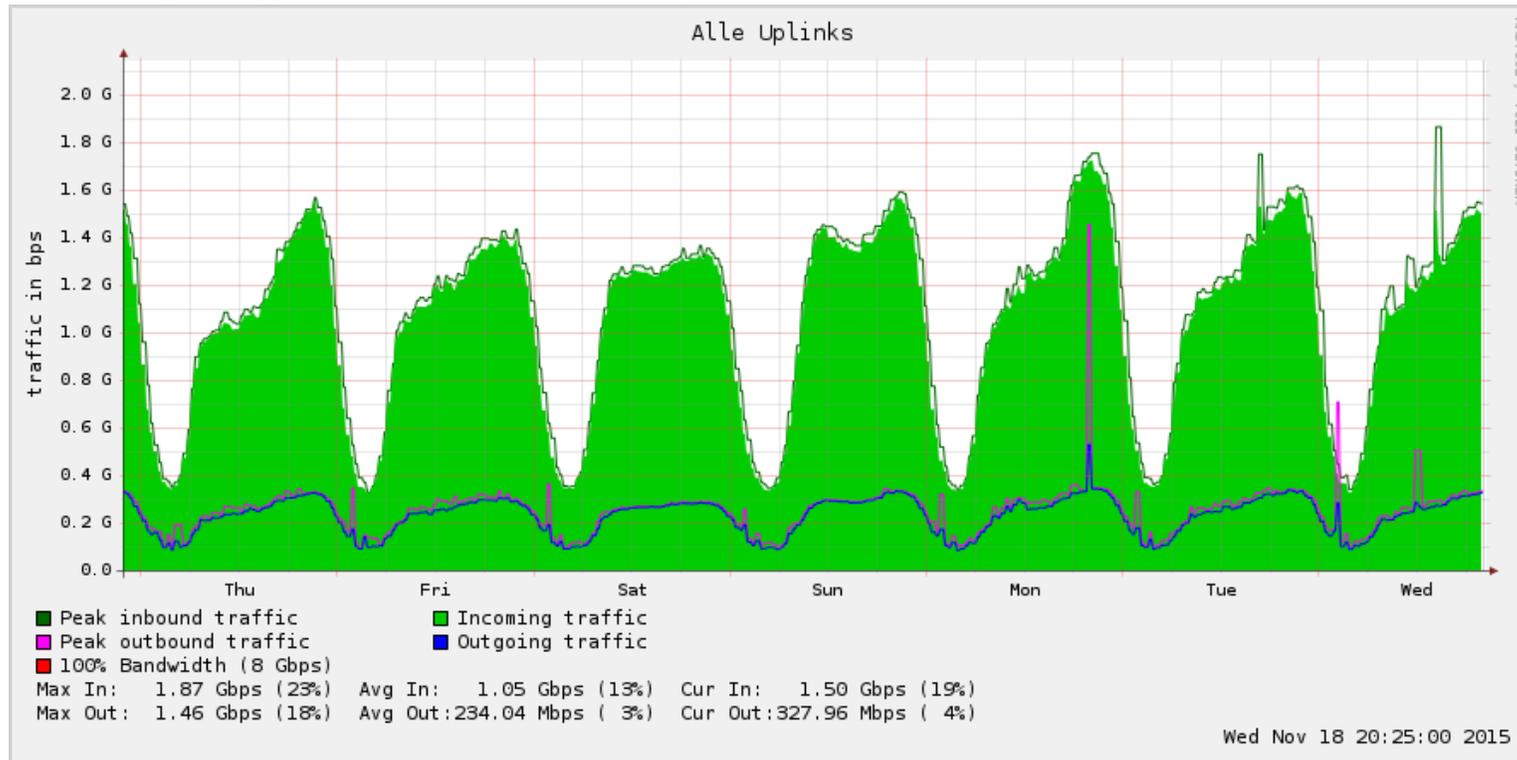
- Call at night.
- Monitoring: Servers fine but Services unreachable.
- High CPU load on LoadBalancers.
- High traffic on switches and uplinks, normally we fit within a few Gb/s total.
- Attacks on DC's other customers are harder to detect and prove.

# InnoGames' Internet traffic (simplified)



# Monitoring Internet uplinks

- Uplink bandwidth does not point out attack target.
- Graph averaging kills short spikes.



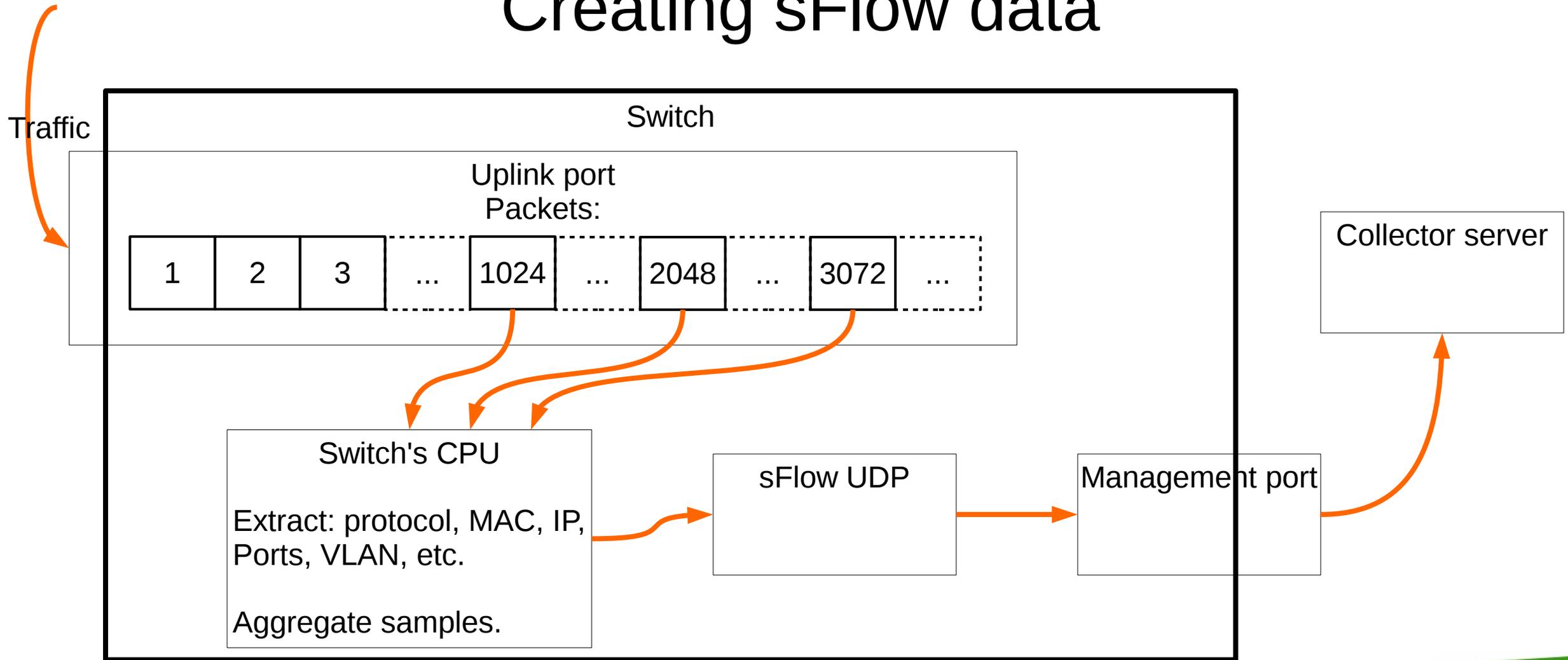
## Monitoring traffic within our network

- On Servers – UDP attacks will not be passed by LoadBalancers, TCP will be limited and seen smaller than they really are.
- On LoadBalancers – monitoring will fail if they fail, detectable size limited to uplinks bandwidth.
- On links – limited to their bandwidth.

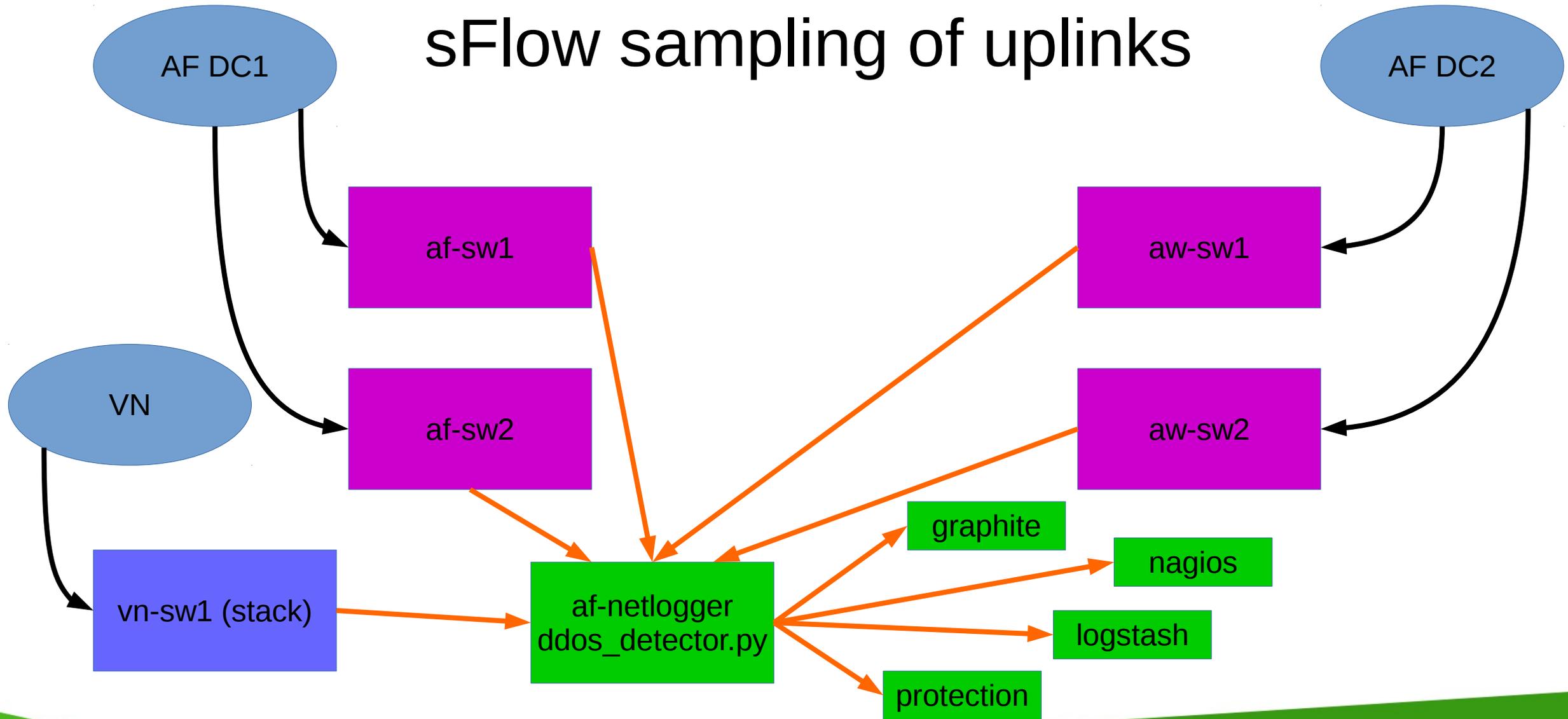
## Monitoring Internet uplinks

- Impossible to log every packet.
- sFlow – sampling of traffic incoming links.
- Not accurate but approximate.
- But for EVERY target IP address in our network (currently ~6k addresses in Graphite)

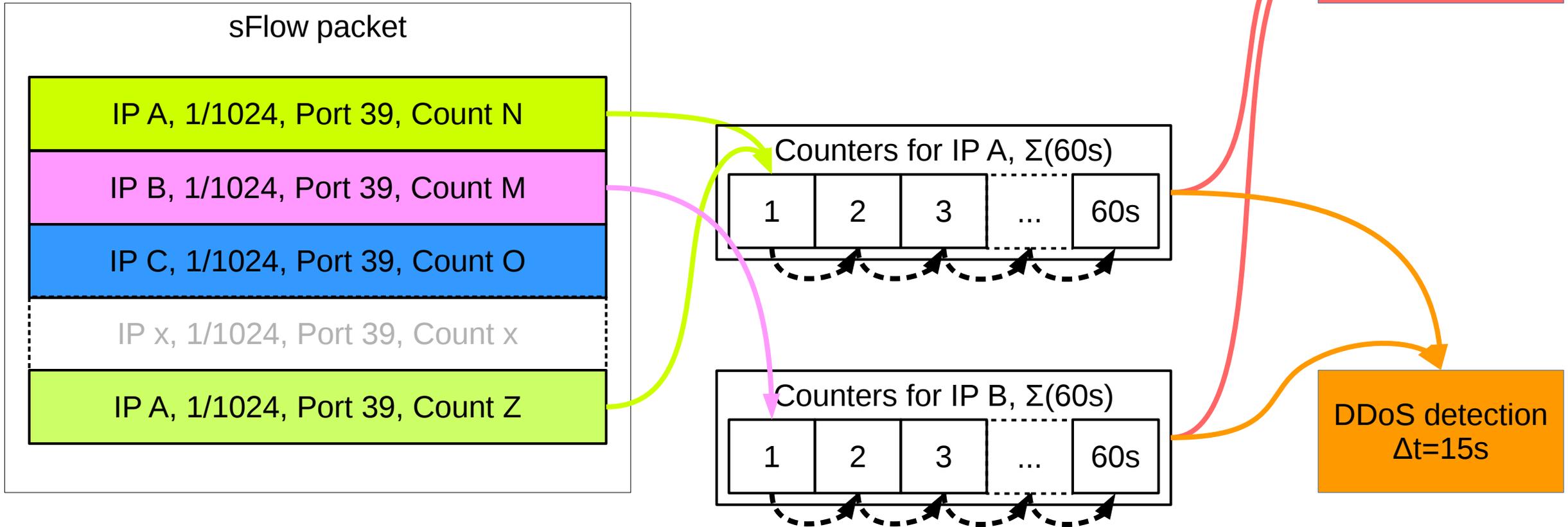
# Creating sFlow data



# sFlow sampling of uplinks

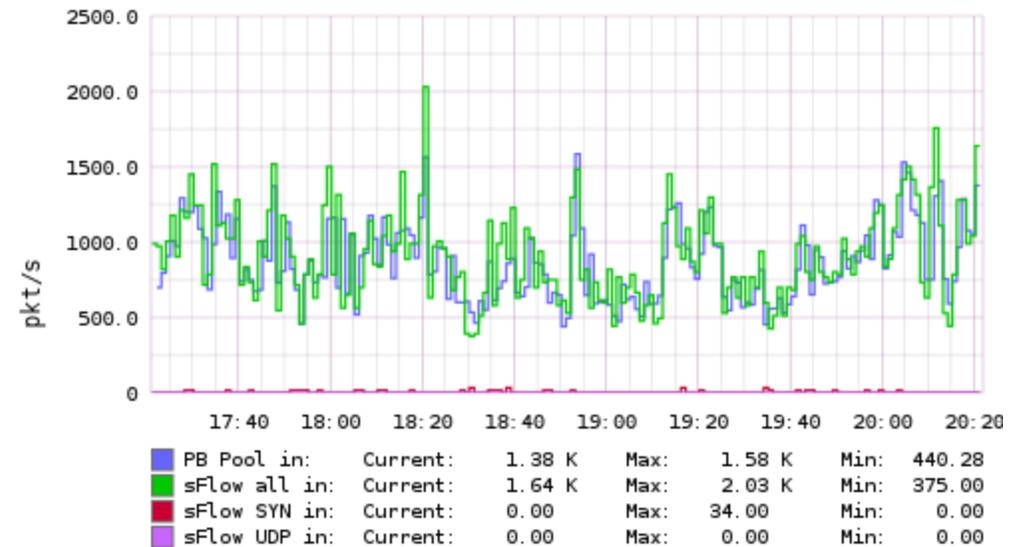
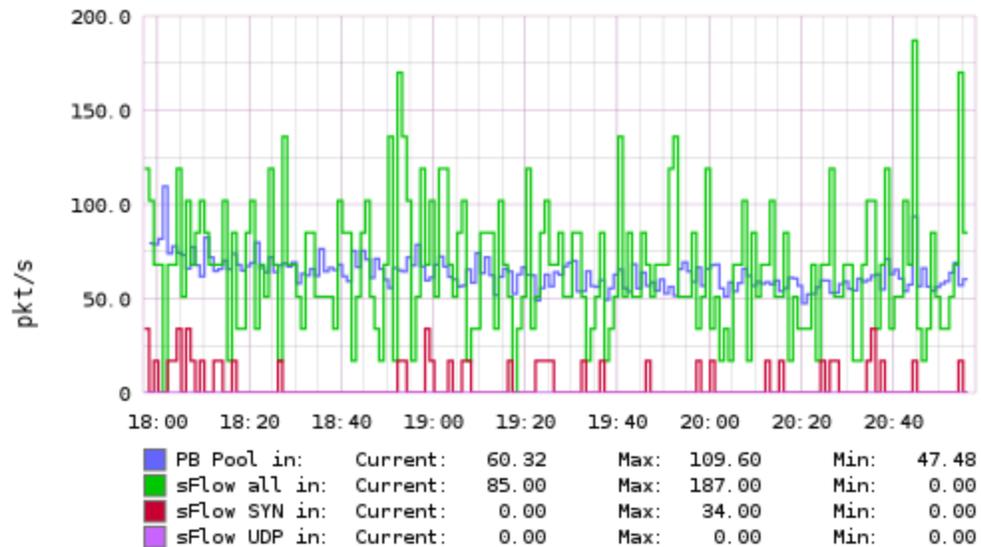


# Analyzing sFlow data



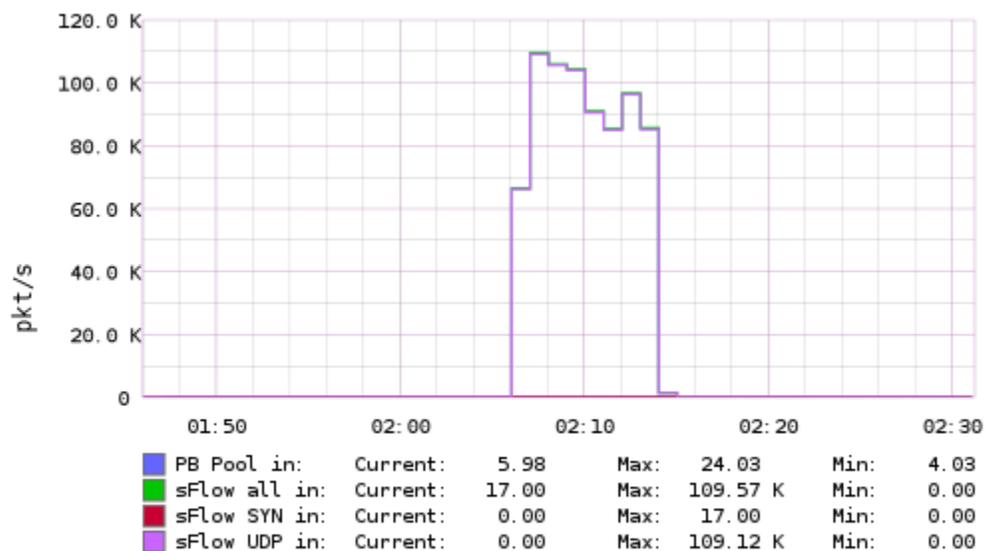
## sFlow results

Accuracy improves with amount of traffic.



# sFlow results

- UDP Flood around 100kp/s.
- sFlow from all 4 uplinks.



# What is considered an attack?

- Any UDP over 85kp/s (around 1Gb/s).
- TCP with SYN flag over 25kp/s.

How do we protect against DDoS attacks?

# General defense mechanisms

- SYN Proxy – do not pass traffic to target server until Firewall fully establishes connection.
- SYN Cookies – do not store state about half-established connection, wait for client to respond with SYN+ACK.
- RST Cookies – reject new connections at first, valid clients will reconnect.
- What about UDP Floods?

# How to defend on LoadBalancers?

- Improving pf ruleset:
  - Early blocking non-matching traffic.
  - State lifetime, especially for internal states.
  - Limiting effects of attacks to given LB Pool by limiting states per target IP.
  - No SYN Cookie mechanism in pf at the moment.
  - SYN Proxy useless because it creates full states.

# How to defend on LoadBalancers?

- Improving pf code:
  - $O(n^2)$  algorithms ([PR#176763](#))
  - Traffic leaking from rules blocked due to too many states ([PR#177810](#))
  - Source tracking only after state is established.
  - Performance improvements ([PR#184003](#))
  - Many more bugs and features not related to DDoS.

## How to defend in network?

- Upgrading to 10Gb/s links. Or  $n \times 10\text{Gb/s}$ .
- Rate limiting on central switches / routers:
  - Limiting UDP traffic on core switches (DNS uses separate subnet, NTP is not crucial).
  - Limiting any traffic to attacked IP on core switches.

# Rate limiting on Extreme switches

```
# configure qosscheduler weighted-round-robin

# configure qosprofile QP1 maxbuffer 100 weight 3
# configure qosprofile QP2 maxbuffer 100 weight 2
# configure qosprofile QP3 maxbuffer 100 weight 1
# configure qosprofile QP5 maxbuffer 100 weight 3
# configure qosprofile QP8 maxbuffer 100 weight 3

# configure qosprofile QP3 minbw 0 peak_rate 50000 K ports all

# enable dot1p replacement port all

# show dot1p replacement
QOSProfile      VPri
  QP1 -> 0
  QP2 -> 1
  QP3 -> 2
  QP5 -> 4
  QP8 -> 7
```

# Rate limiting on Extreme switches

```
# create access-list network-zone ddos_detector

# edit policy ddos_udp_flood

entry ddos_detector {
  if match all {
    destination-zone ddos_detector ;
  }
  then {
    qosprofile qp3 ;
  }
}

# configure access-list ddos_udp_flood ports 47 ingress
```

# Rate limiting on Extreme switches

```
# configure access-list network-zone ddos_detector add ipaddress 42.1.2.3  
# configure access-list network-zone ddos_detector delete ipaddress 42.1.2.3  
# refresh access-list network-zone ddos_detector
```

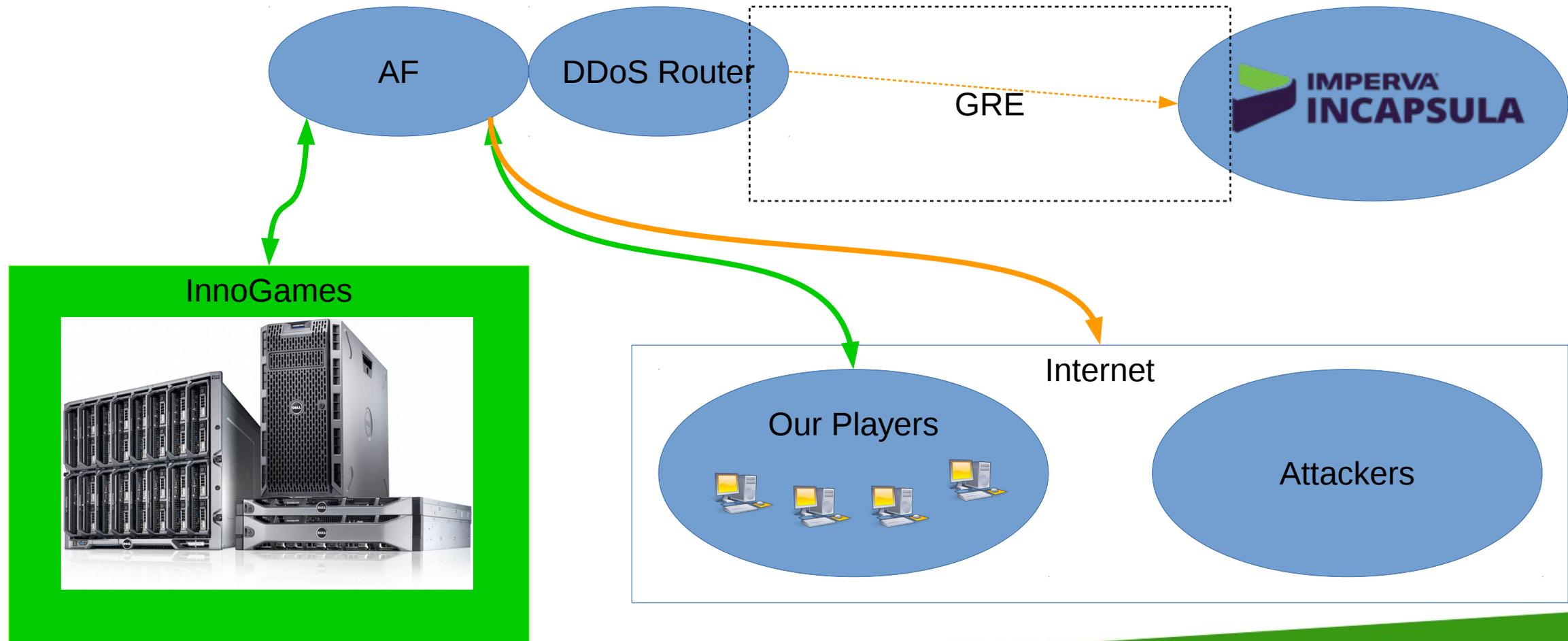
## Using external protection provider

- Announces our /24 prefixes, intercepts traffic, filters it, tunnels clean traffic to us.
- Currently it is Incapsula.
- They can handle attacks bigger than sum of our or uplink capacity.
- Our network must survive only short period of attacks before we use their service.

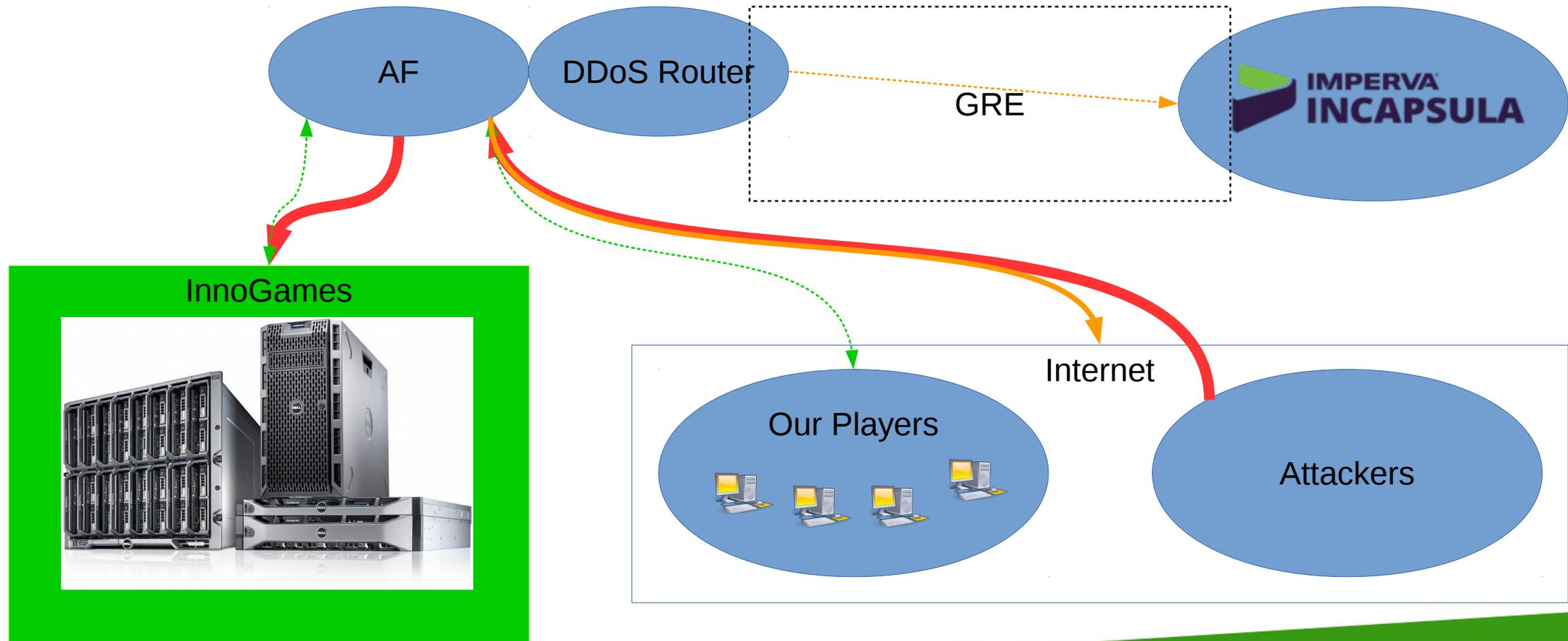
## External provider's problems

- False positives.
- Increased latency.
- Not catching an attack and tunnelling >>Gb/s of dirty traffic, killing our Cisco router.
- Their own problems when they handle some other big attacks.
- Tunnels+BGP die if attack saturates Datacenter's links.

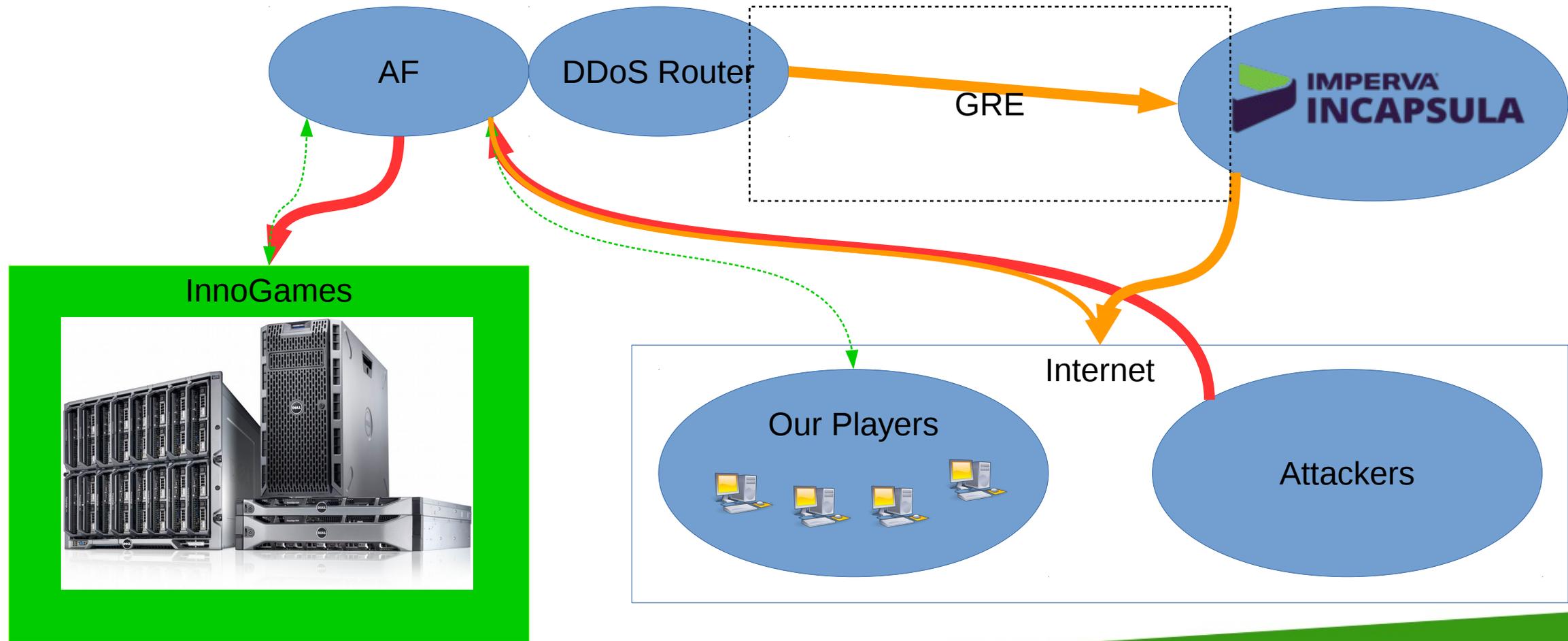
# External tunneling protection



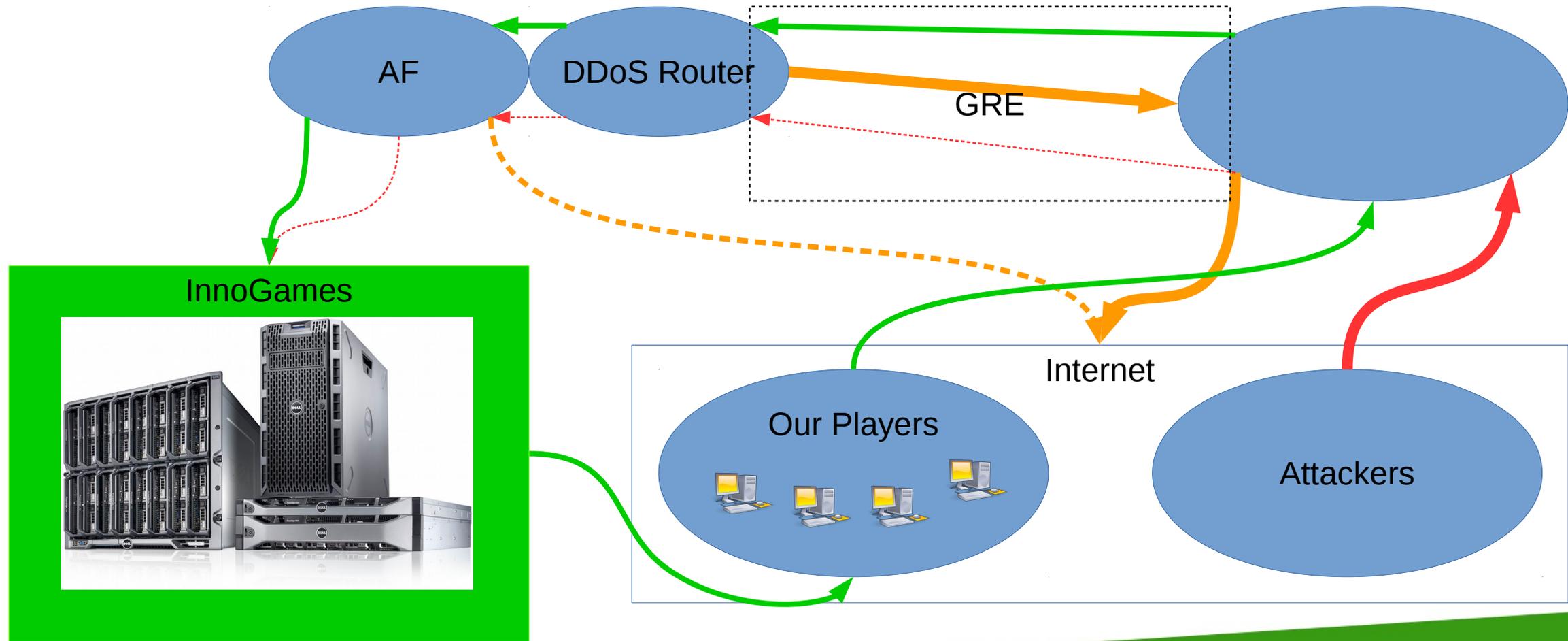
# External tunneling protection



# External tunneling protection



# External tunneling protection



# Automatic protection

- `ddos_detector.py` is capable of:
  - Configuring traffic shaping on central switches.
  - Enabling external protection service.

# Summary

- External protection is a must.
- Fast reaction thanks to in-house detection tools.
- Software has (had) bugs.
- Dynamic network configuration.
- Network upgrades.

<applause>



*Fin*