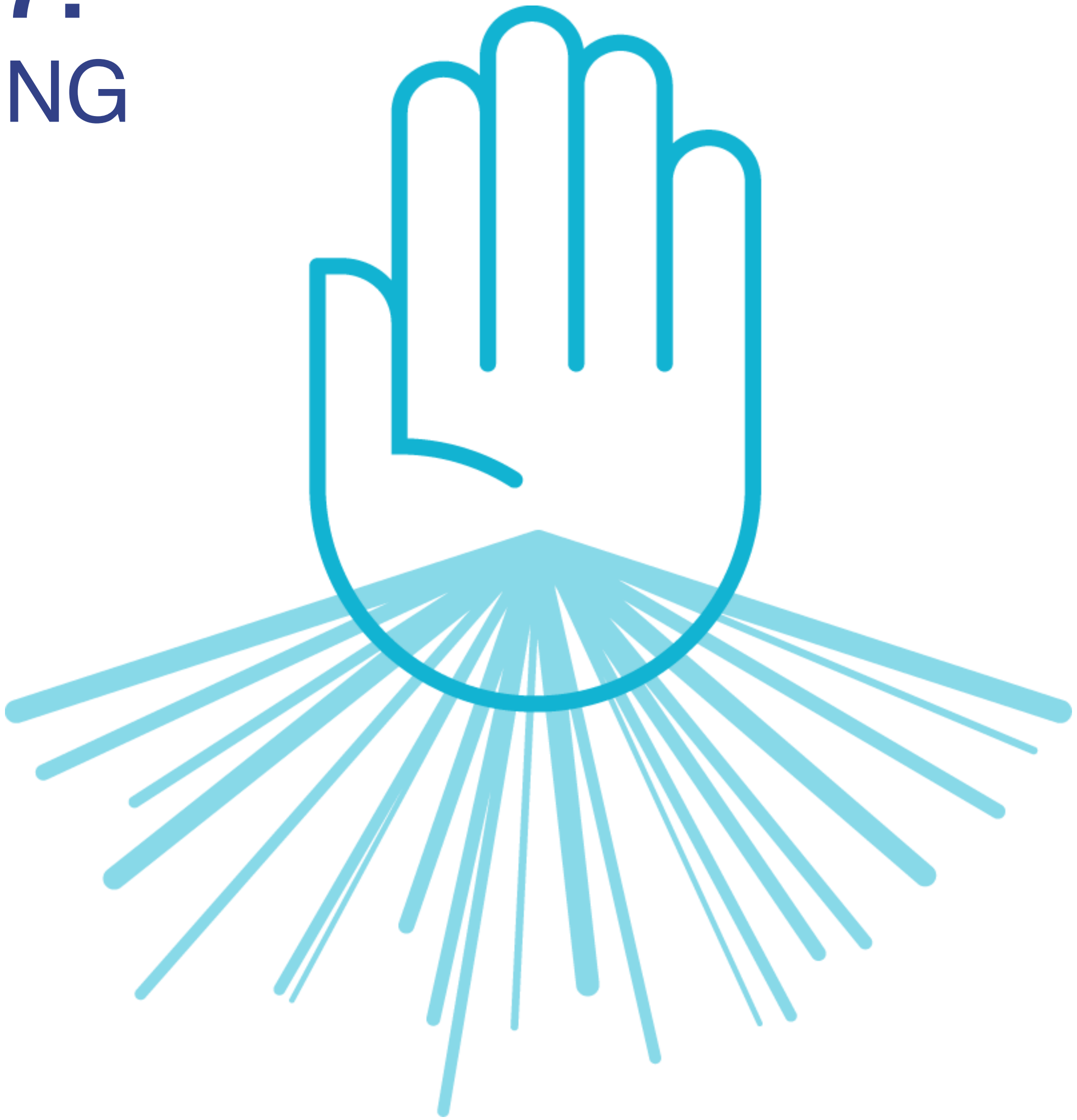
DDOS ATTACKS IN 2017:
BEYOND PACKET FILTERING

Artyom Gavrichenkov

Qrator Labs

ag@qrator.net



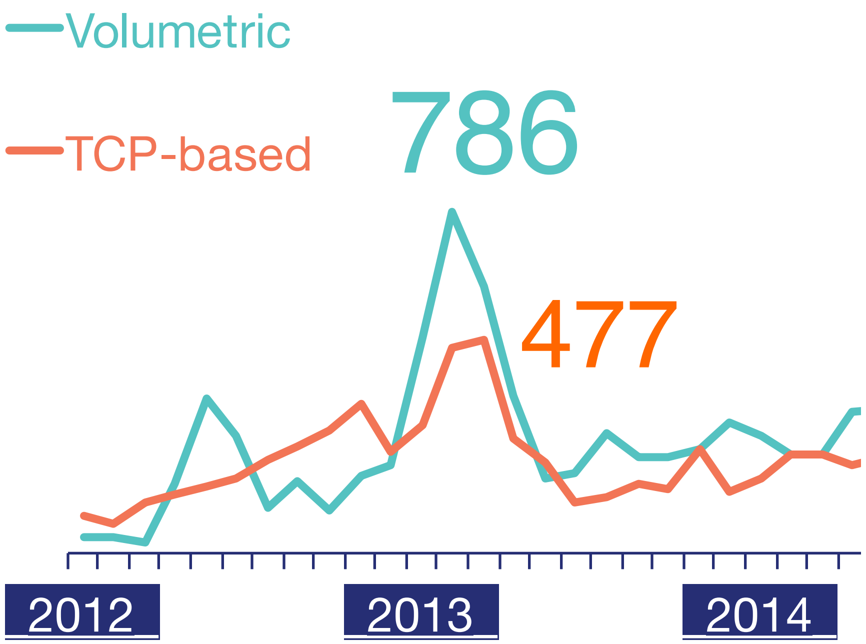
QRATOR

PARENTAL

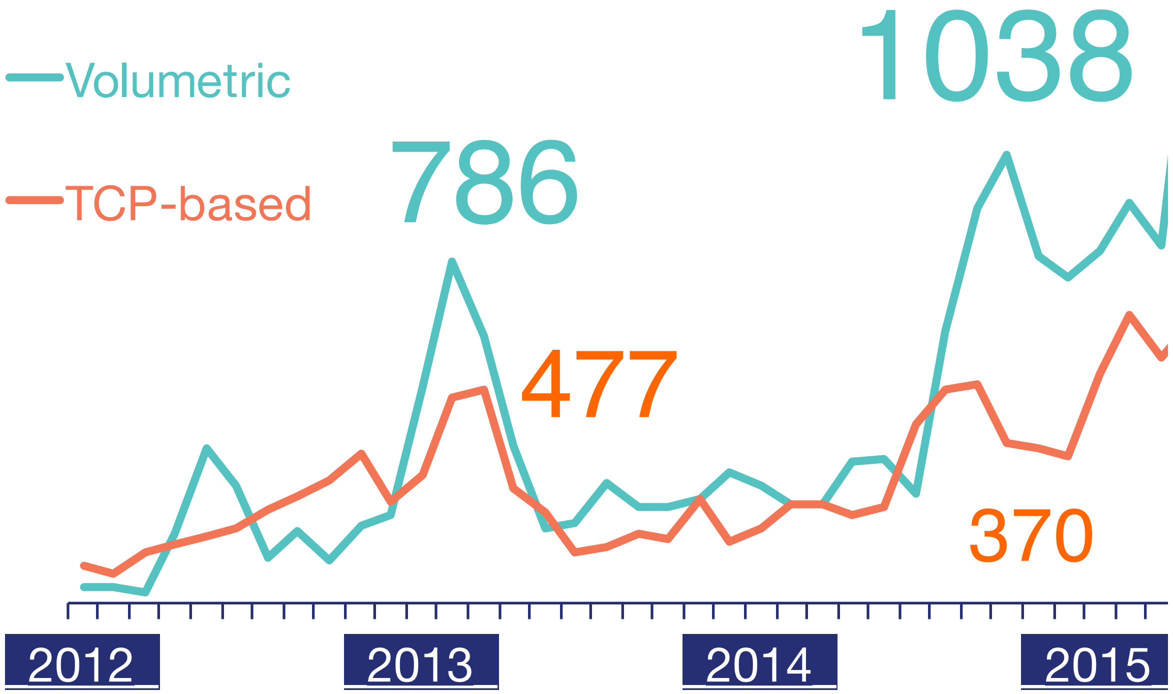
ADVISORY

EXPLICIT CONTENT

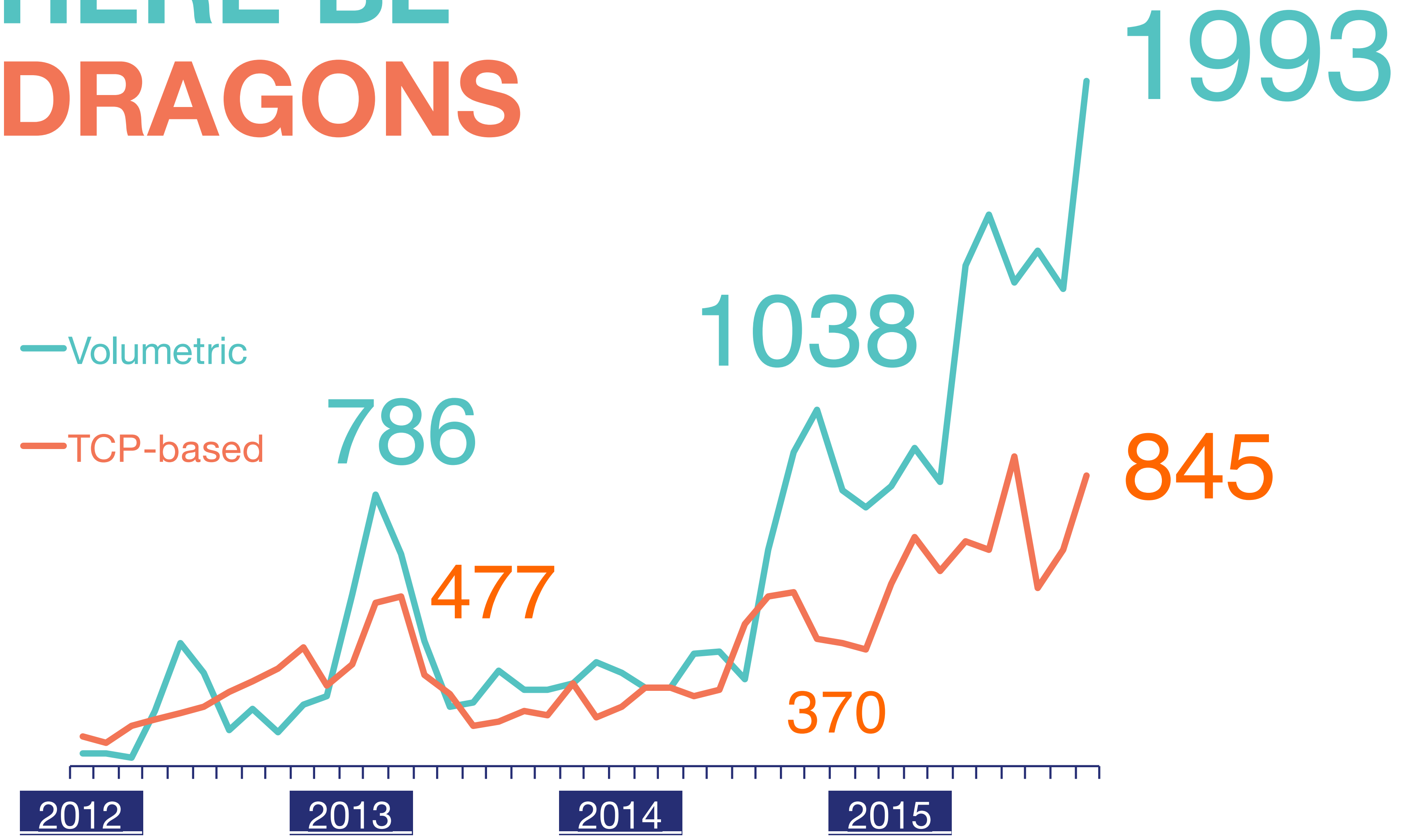
HERE BE DRAGONS



HERE BE DRAGONS



HERE BE DRAGONS



Distributed Denial-of-Service attack

- An attempt to make a network resource unavailable by exhausting its resources

Distributed Denial-of-Service attack

- An attempt to make a network resource unavailable by exhausting its resources:
  - Bandwidth

Distributed Denial-of-Service attack

- An attempt to make a network resource unavailable by exhausting its resources:
  - Bandwidth:
    ICMP flood, UDP flood, SYN flood…

Distributed Denial-of-Service attack

- An attempt to make a network resource unavailable by exhausting its resources:
  - Bandwidth:
    ICMP flood, UDP flood, SYN flood…
    Amplification: NTP, DNS, SNMP, SSDP, ICMP, NetBIOS,
    RIPv1, PORTMAP, CHARGEN, QOTD...

Distributed Denial-of-Service attack

- An attempt to make a network resource unavailable by exhausting its resources:
  - Bandwidth:
    ICMP flood, UDP flood, SYN flood…
    Amplification: NTP, DNS, SNMP, SSDP, ICMP, NetBIOS,
    RIPv1, PORTMAP, CHARGEN, QOTD...
  - TCP finite state machine implementation attacks

Distributed Denial-of-Service attack

- An attempt to make a network resource unavailable by exhausting its resources:
  - Bandwidth:
    ICMP flood, UDP flood, SYN flood…
    Amplification: NTP, DNS, SNMP, SSDP, ICMP, NetBIOS,
    RIPv1, PORTMAP, CHARGEN, QOTD...
  - TCP finite state machine implementation attacks:
    SYN flood, ACK flood, TCP connection flood…

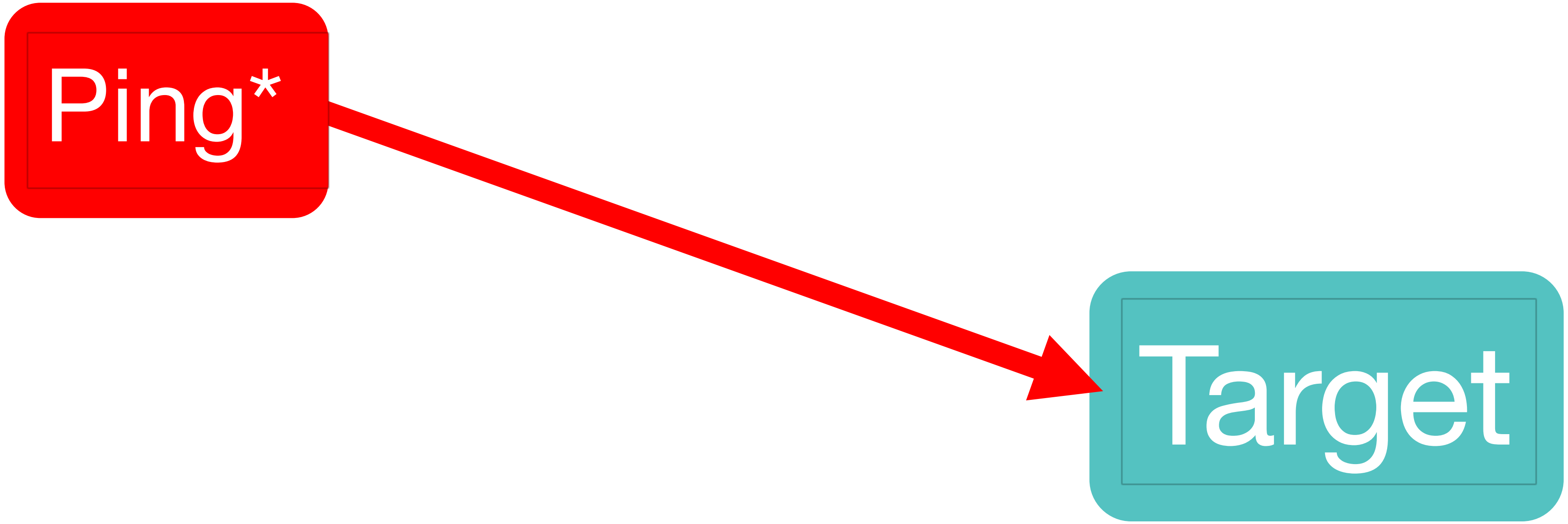
Distributed Denial-of-Service attack

- An attempt to make a network resource unavailable by exhausting its resources:
  - Bandwidth:
    ICMP flood, UDP flood, SYN flood…
    Amplification: NTP, DNS, SNMP, SSDP, ICMP, NetBIOS,
    RIPv1, PORTMAP, CHARGEN, QOTD...
  - TCP finite state machine implementation attacks:
    SYN flood, ACK flood, TCP connection flood…

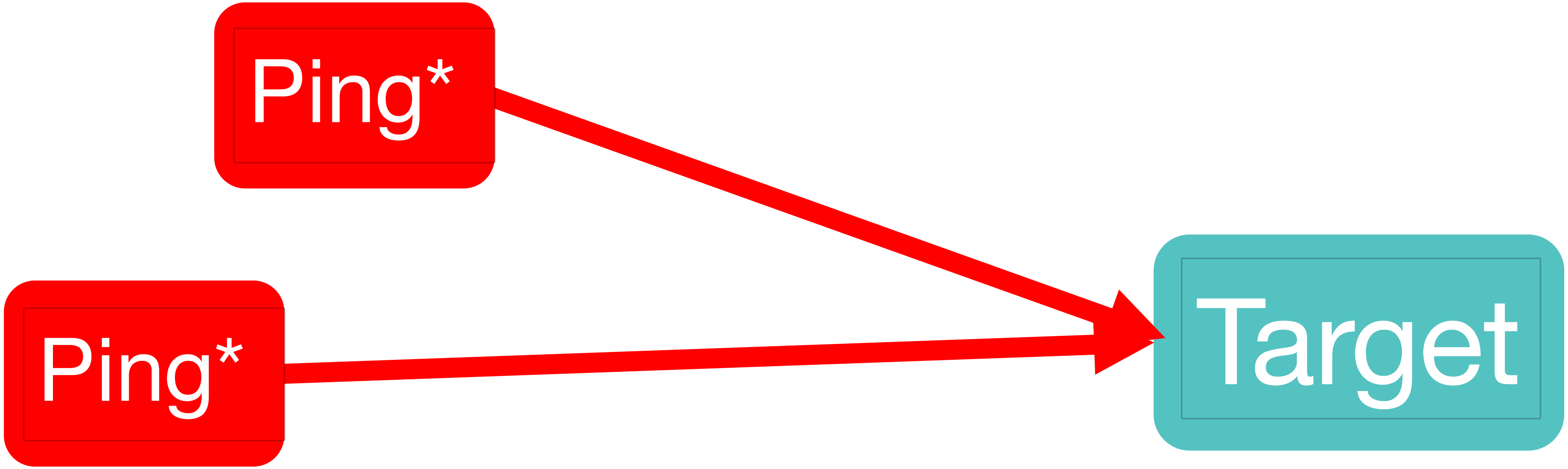
Distributed Denial-of-Service attack

- An attempt to make a network resource unavailable by exhausting its resources:
  - Bandwidth:
    ICMP flood, UDP flood, SYN flood…
    Amplification: NTP, DNS, SNMP, SSDP, ICMP, NetBIOS,
    RIPv1, PORTMAP, CHARGEN, QOTD...
  - TCP finite state machine implementation attacks:
    SYN flood, ACK flood, TCP connection flood…
  - Application-specific bottlenecks (HTTP server, DBMS, caches, etc)

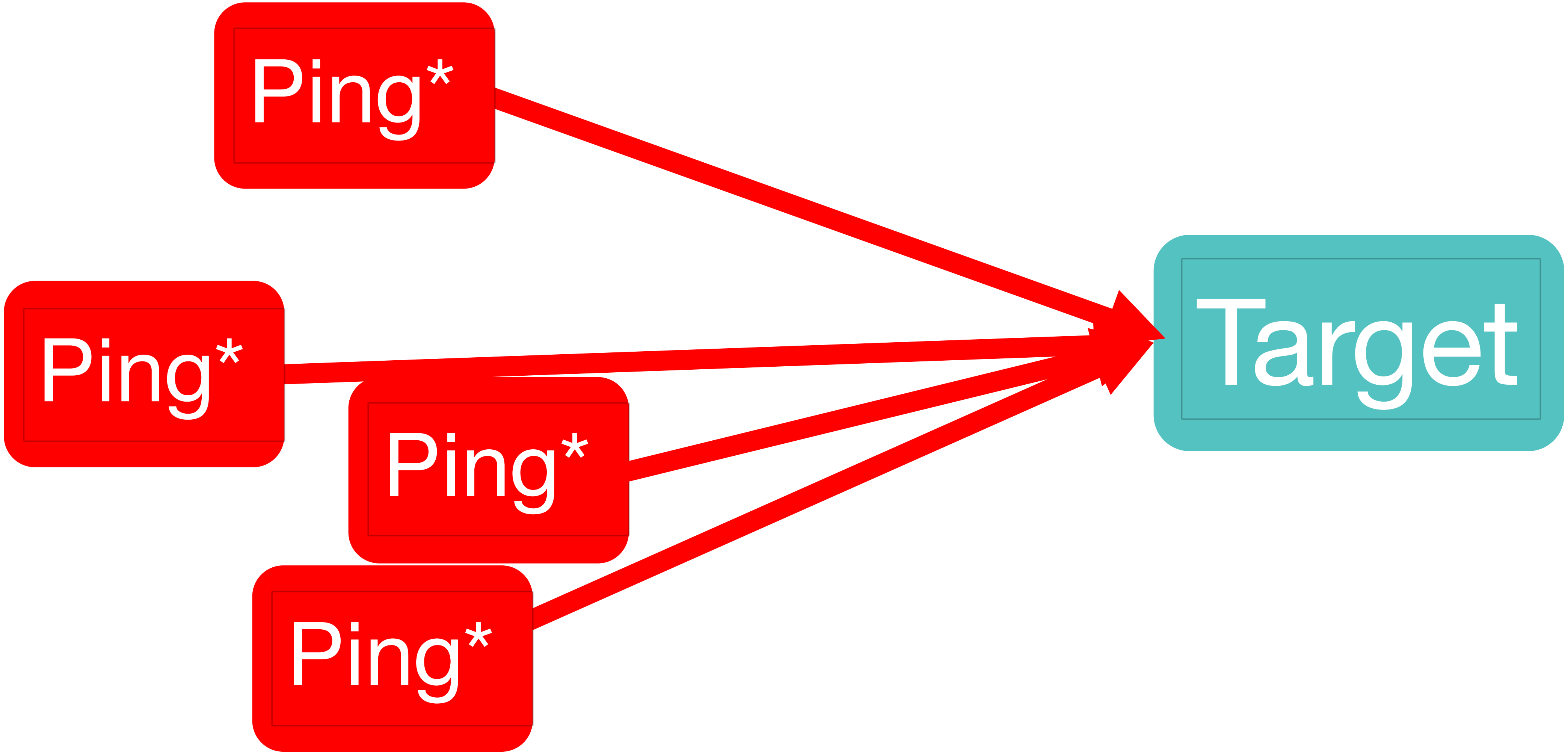
Packet-based DDoS



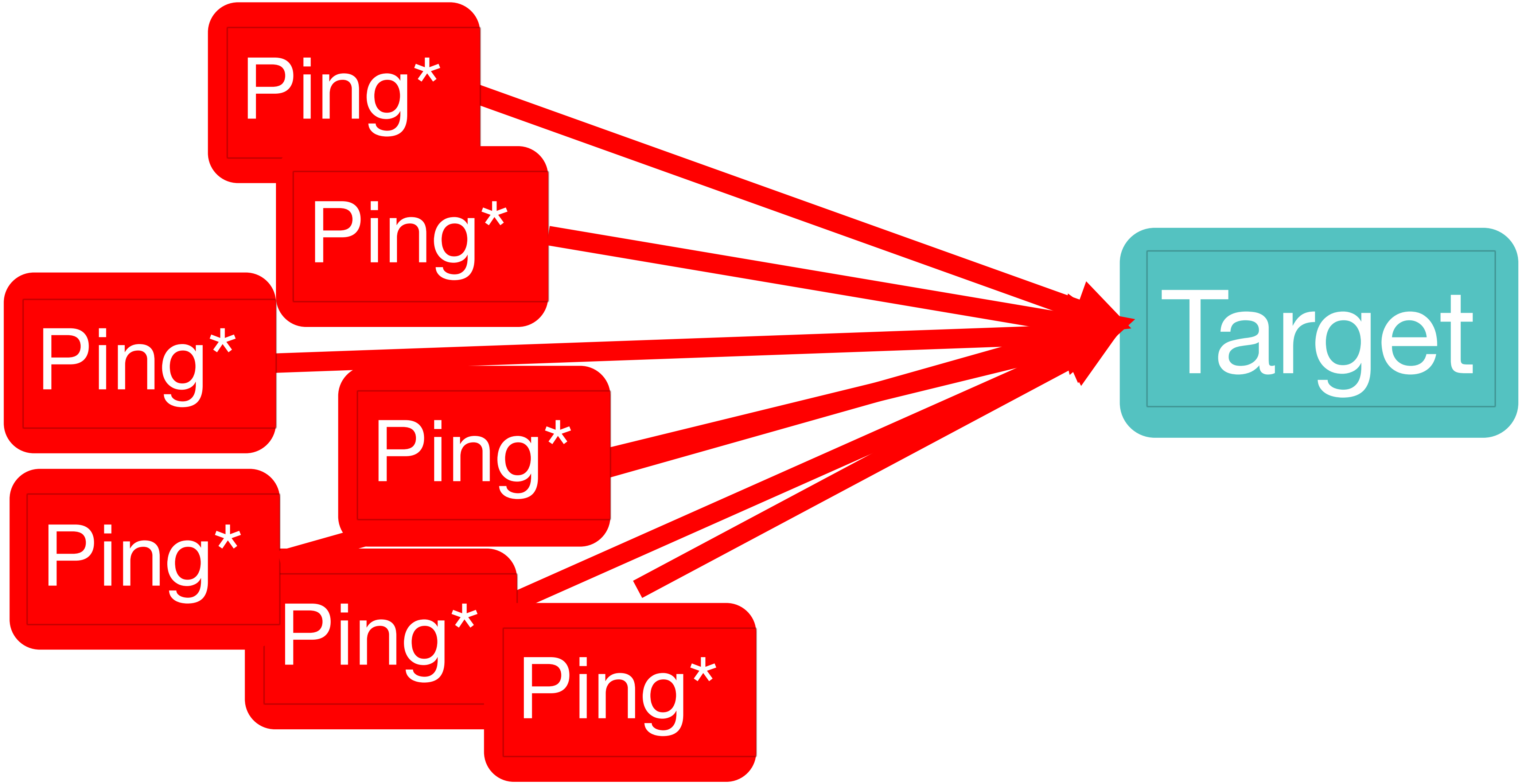
Packet-based DDoS



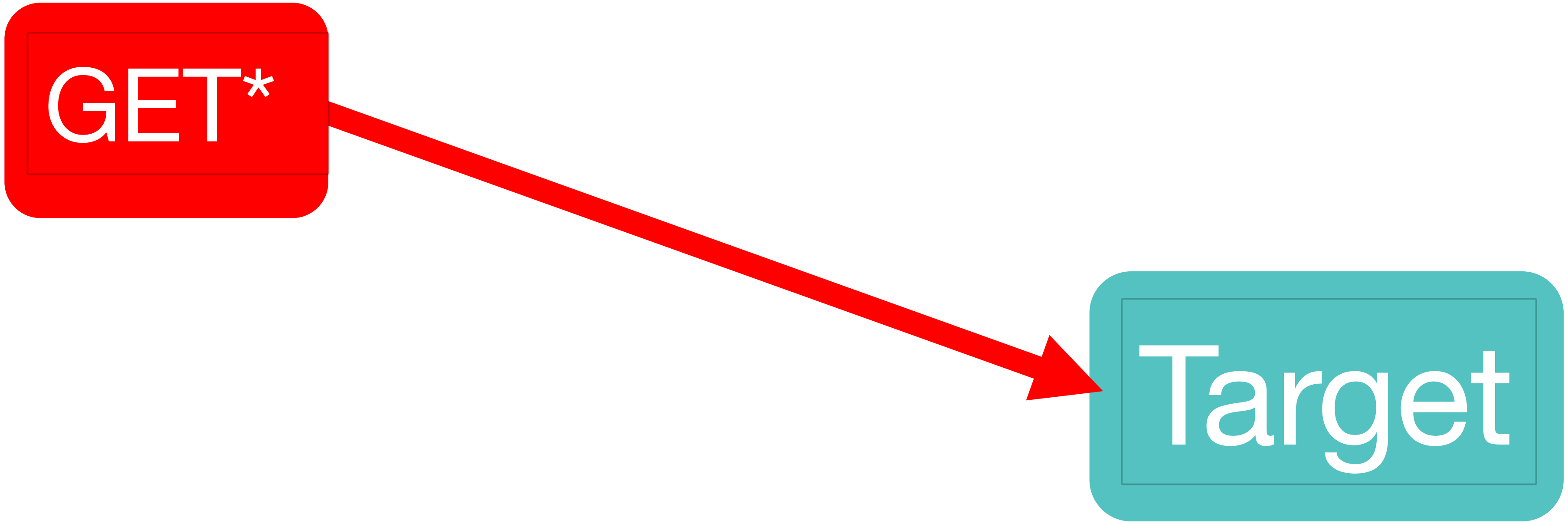
Packet-based DDoS



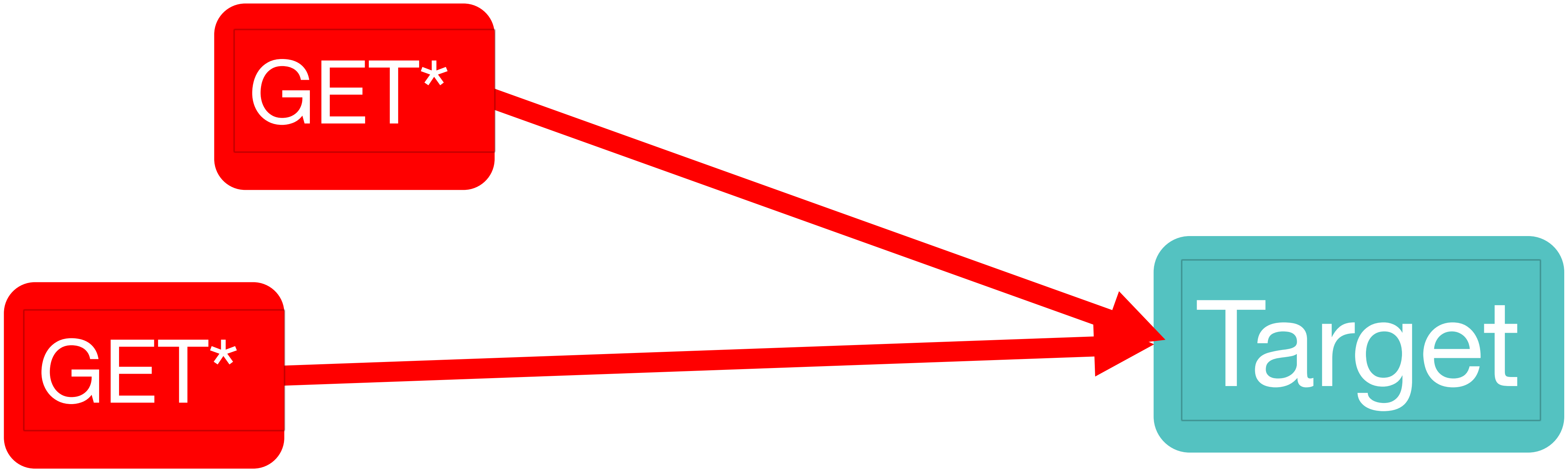
Packet-based DDoS



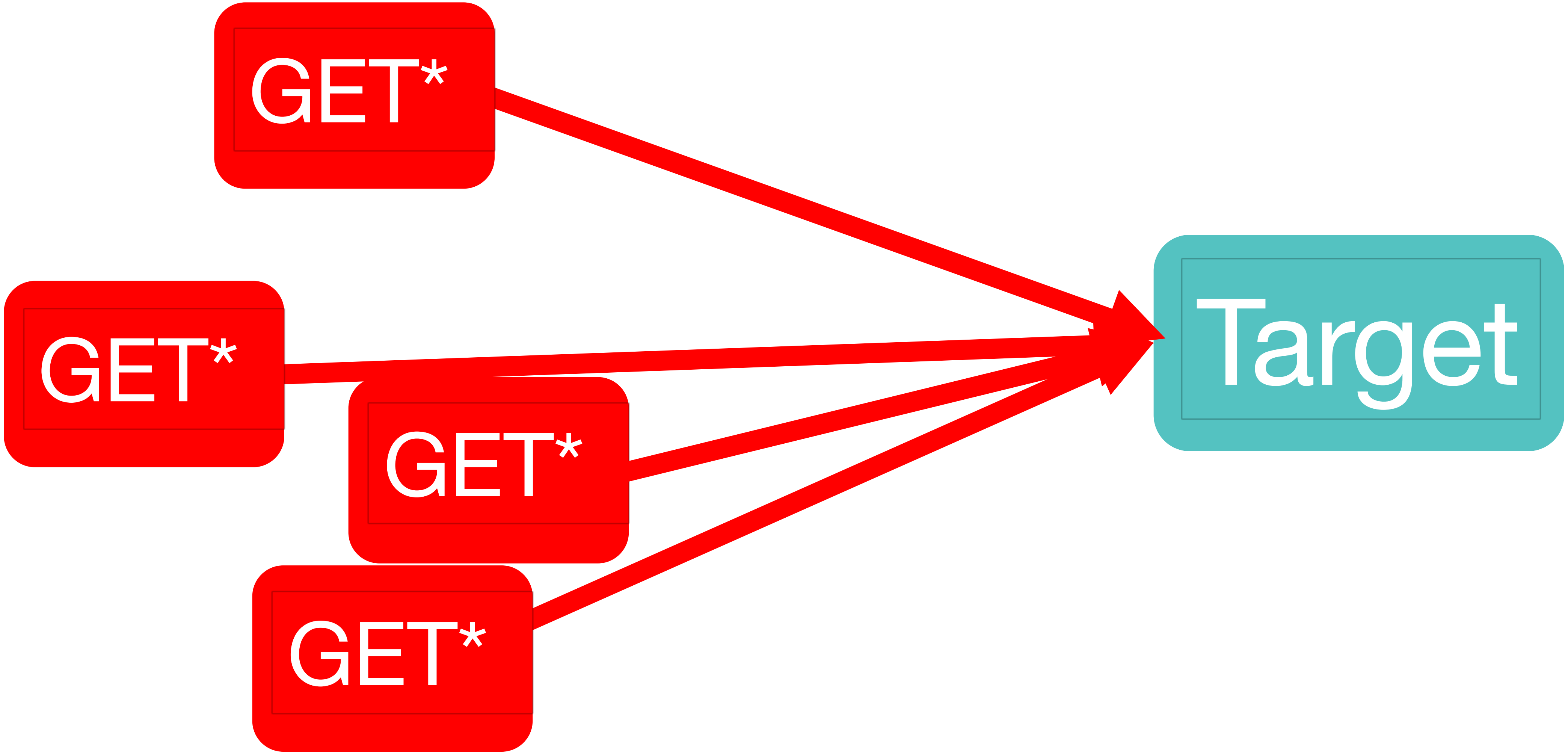
L7 DDoS



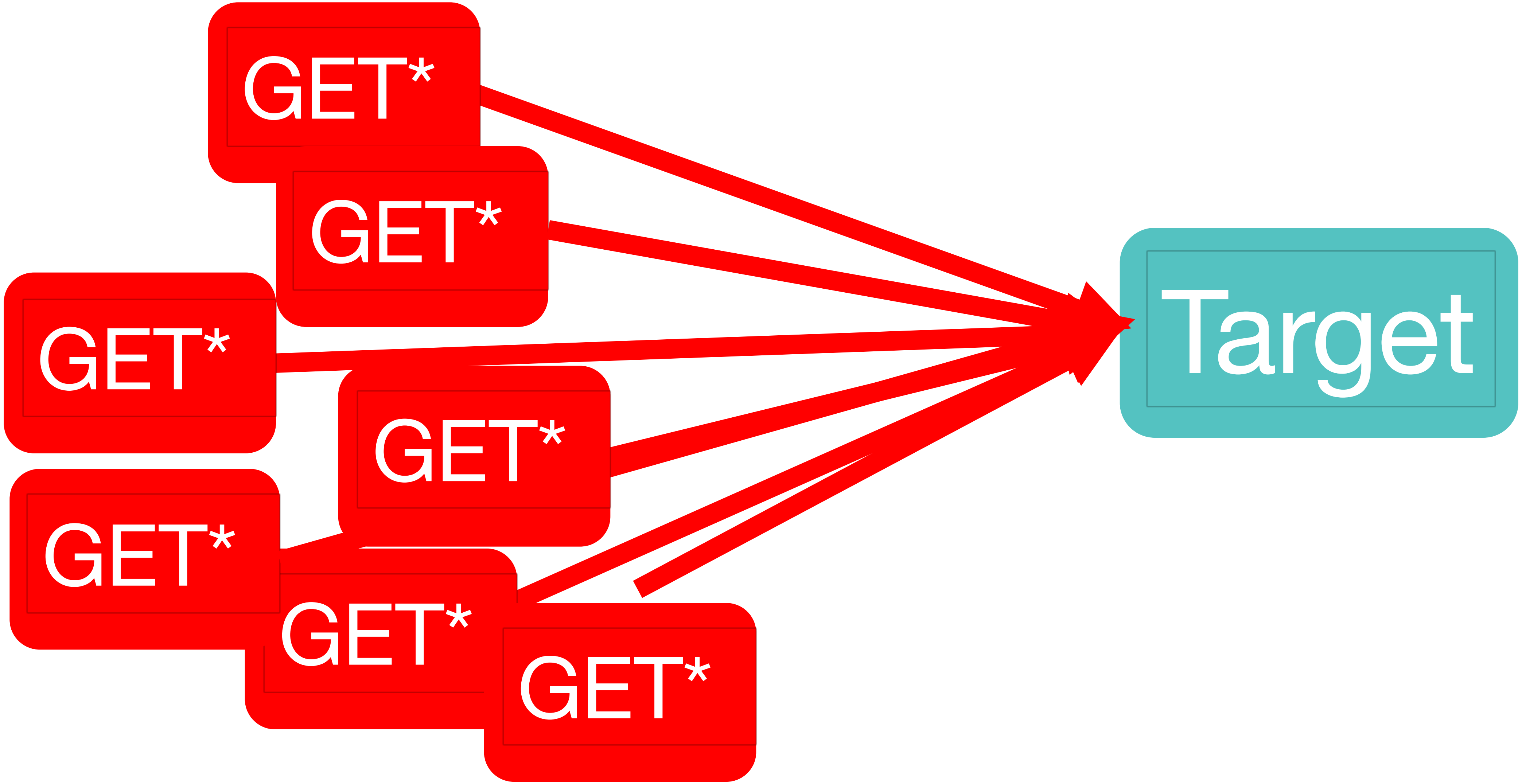
L7 DDoS



L7 DDoS



L7 DDoS



Packet vs Request

- 3-way handshake
  => SYN cookies
  => IP Authentication

Packet vs Request

- 3-way handshake
  => SYN cookies
  => IP Authentication
- IP Authentication not available in most* UDP-based protocols
  => Spoofing
  => UDP Amplification!

Packet vs Request

- 3-way handshake
  => SYN cookies
  => IP Authentication
- IP Authentication not available in most* UDP-based protocols
  => Spoofing
  => UDP Amplification!
- Amp-vulnerable server may be identified by source port
  => Flow Spec solves problems!

BGP Flow Spec?

BGP Flow Spec!

Packet vs Request

- 3-way handshake
  => SYN cookies
  => IP Authentication
- IP Authentication not available in most* UDP-based protocols
  => Spoofing
  => UDP Amplification!
- Amp-vulnerable server may be identified by source port
  => Flow Spec solves problems!

Packet vs Request

- 3-way handshake
    - => SYN
    - => IP [illegible]cation
- IP Authentication not available in most* UDP-based protocols
    - => Spoofing
    - => UDP Amplification!
- Amp-vulnerable server may be identified by source port
    - => Flow Spec solves problems!

FALSE

Packet vs Request

- 3-way handshak
    => SYN
    => IP cation

FALSE

- IP Authenti ation not a n most* UDP-based protocols
    => Spoofing
    => UDP Ampl n!

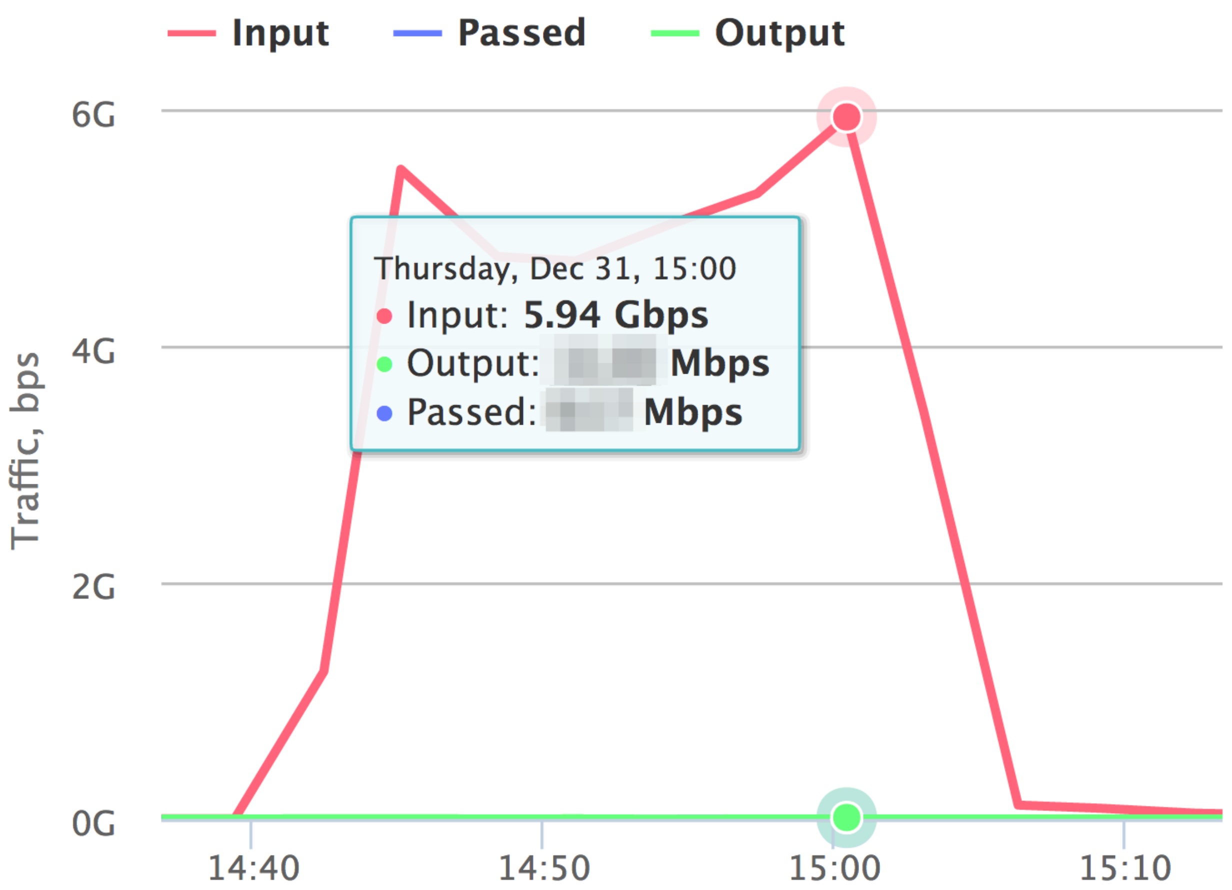
FALSE

- Amp-vulnerable server may be identified by source port
    => Flow Spec solves problems!

Wordpress Pingback

```
GET /whatever
User-Agent: WordPress/3.9.2;
 http://example.com/;
 verifying pingback
 from 192.0.2.150
```

- 150-170 vulnerable servers at once
- SSL/TLS-enabled



Wordpress Pingback

- **Millions** of vulnerable servers

Wordpress Pingback

- **Millions** of vulnerable servers

Drupal?

Wordpress Pingback

- **Millions** of vulnerable servers

Drupal?

Joomla?

Wordpress Pingback

- **Millions** of vulnerable servers

Drupal?

Mediawiki?

Joomla?

Wordpress Pingback

- **Millions** of vulnerable servers

Sharepoint?

Drupal?

Mediawiki?

Joomla?

Wordpress Pingback

- **Millions** of vulnerable servers

Sharepoint?

ModX?

Drupal?

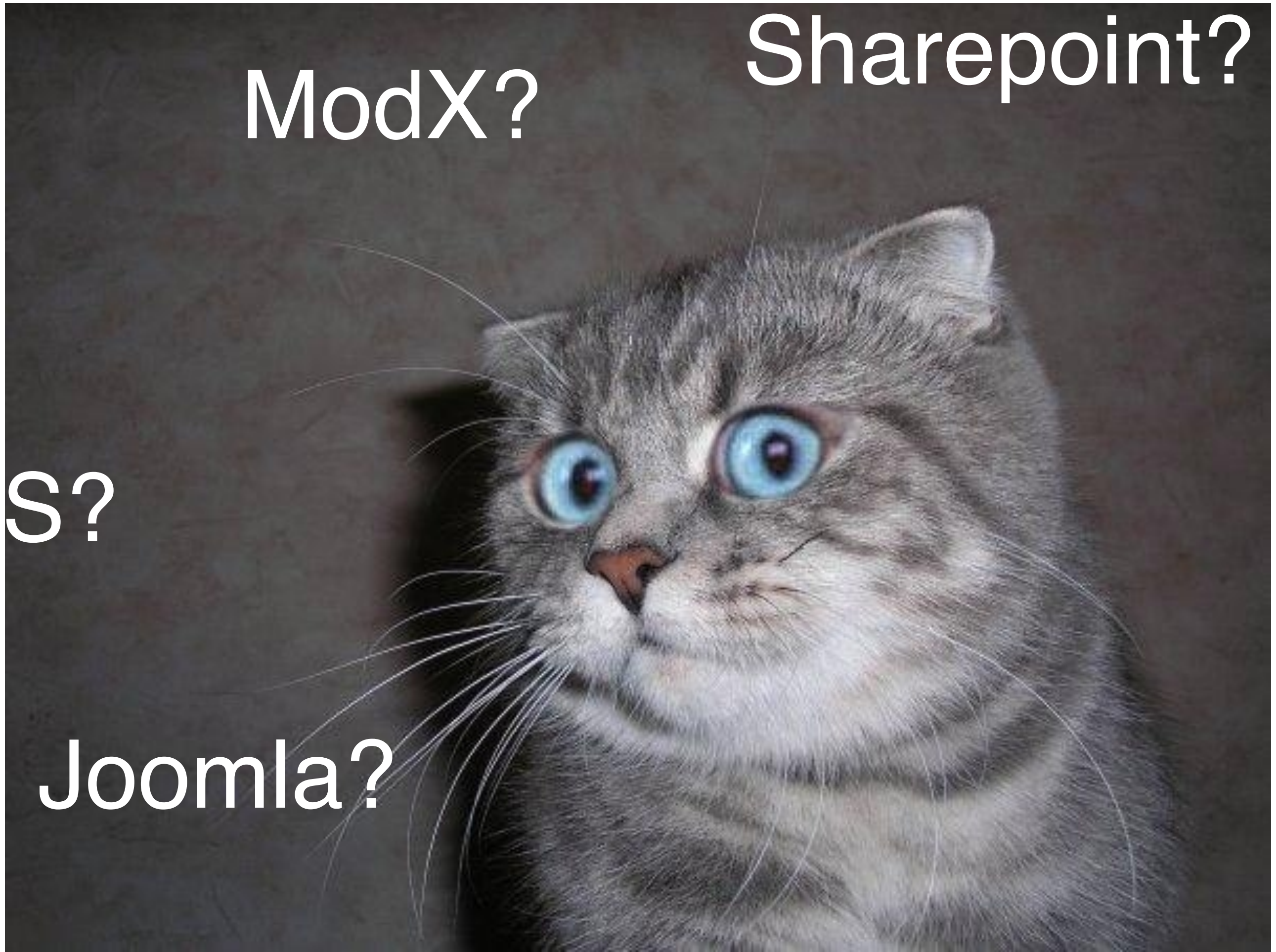
TinyCMS?

Mediawiki?

Joomla?

Wordpress Pingback

- **Millions** of vulnerable servers



Sharepoint?

ModX?

Drupal?

TinyCMS?

Mediawiki?

Joomla?

Packet vs Request

- 3-way handshak
  => SYN
  => IP cation
- IP Authenti ation not a n most* UDP-based protocols
  => Spoofing
  => UDP Ampl on!
- Amp-vulnerable server may be identified by source port
  => Flow Spec solves problems!

FALSE

FALSE

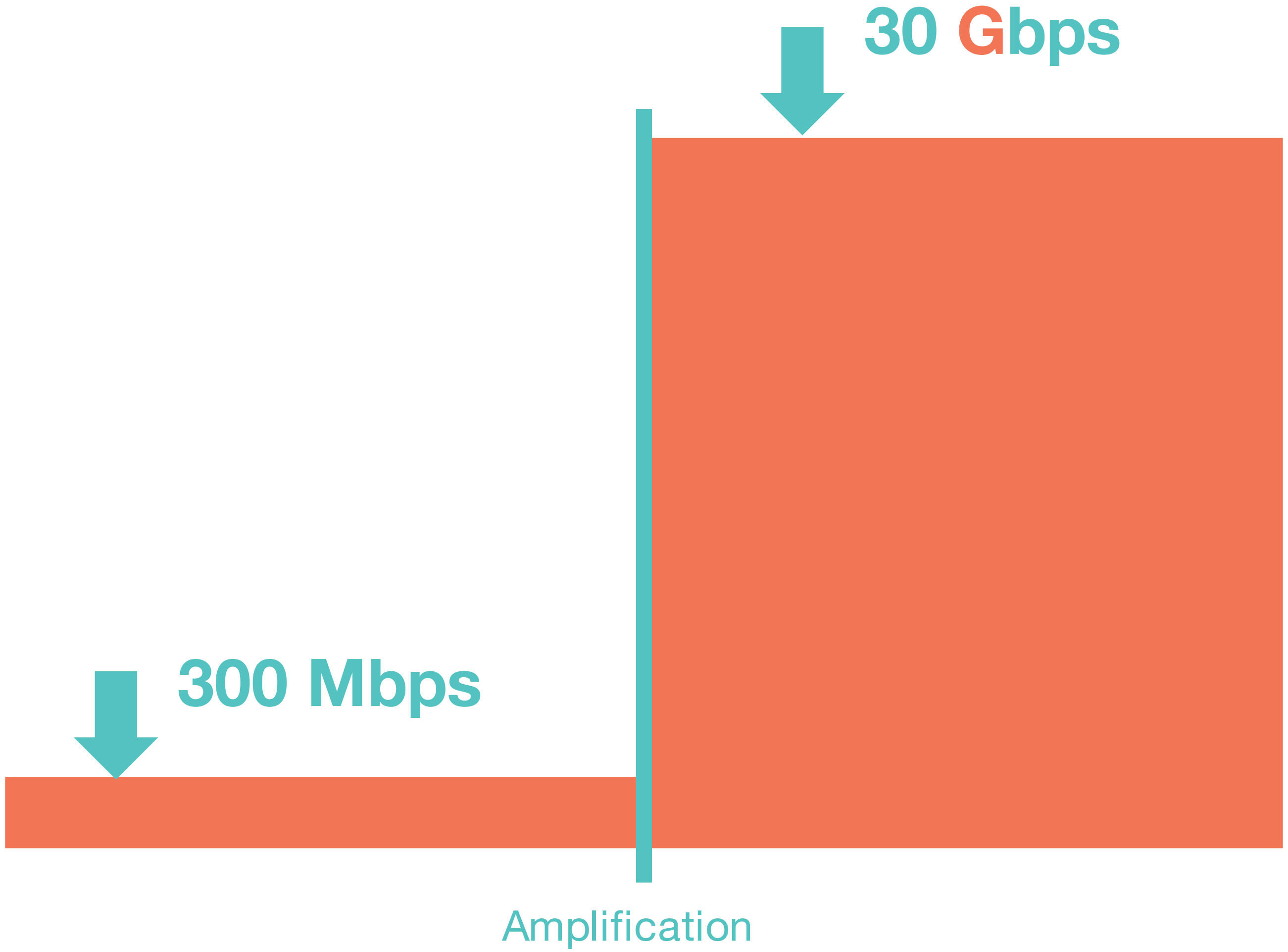
Packet vs Request

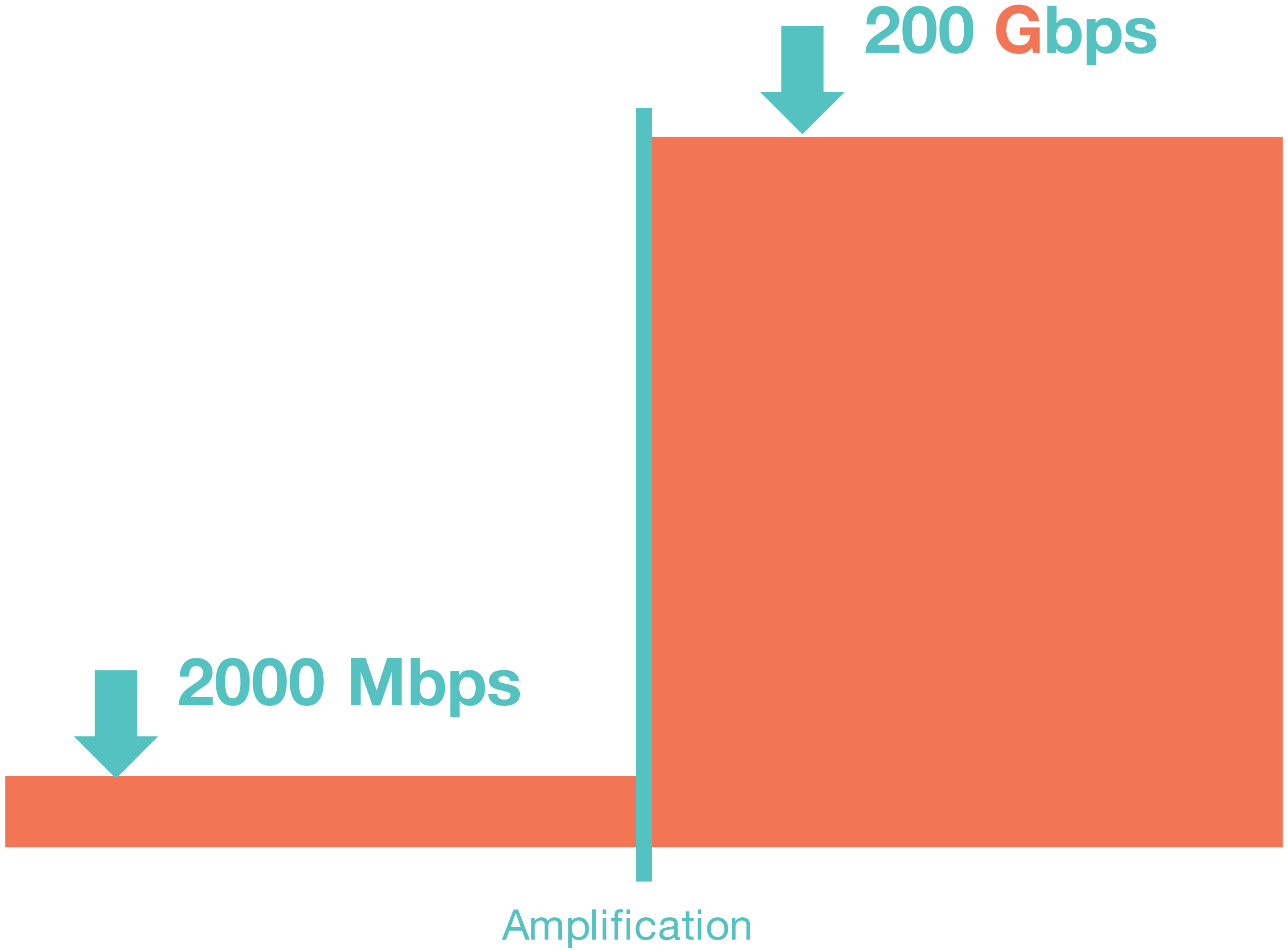
- 3-way handshak
  - => SYN
  - => IP cation
- IP Authenti ation not a n most* UDP-based protocols
  - => Spoofing
  - => UDP Ampl on!
- Amp-vulnerable erver may be identified by source port
  - => Flo solves problems!

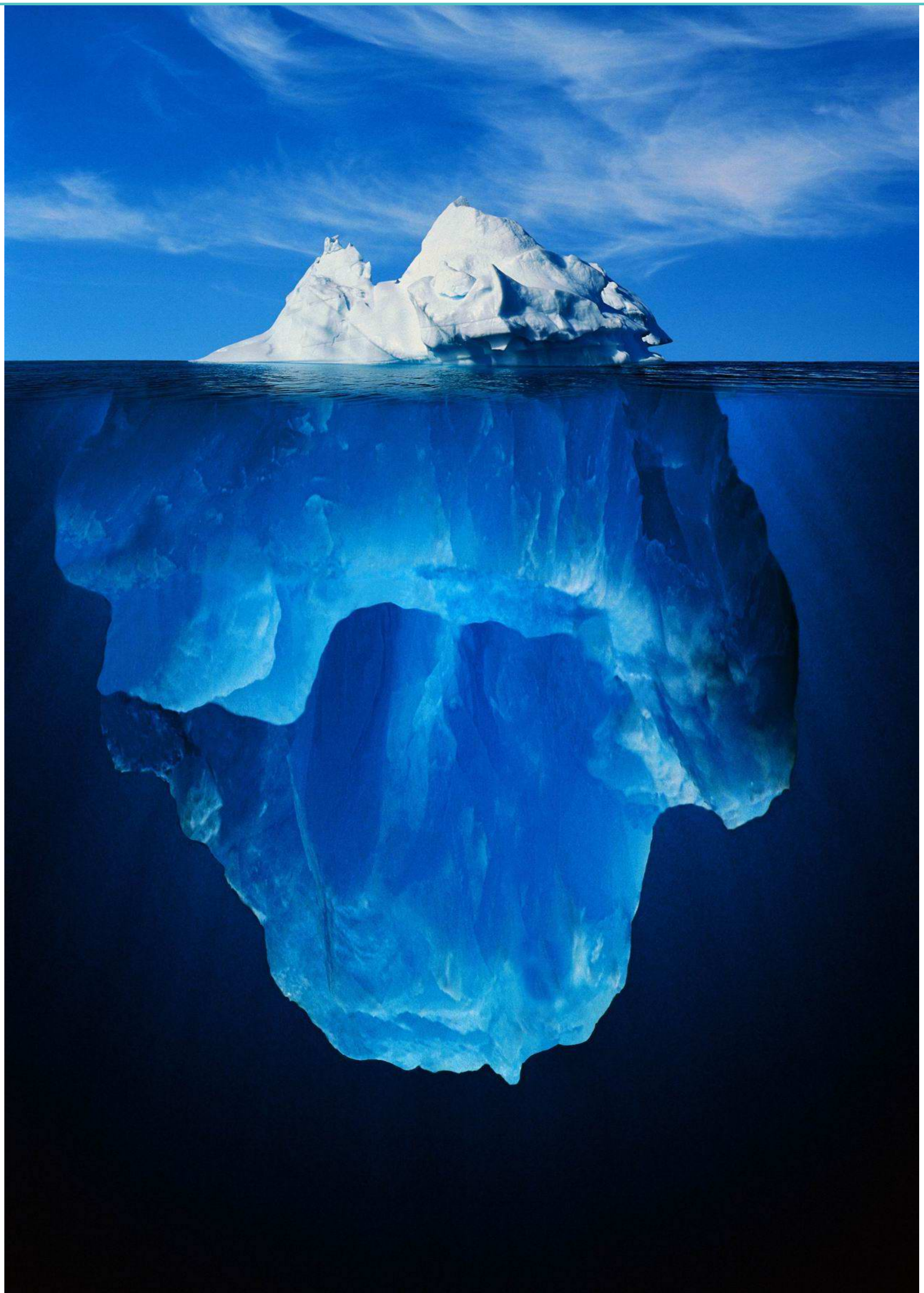
FALSE

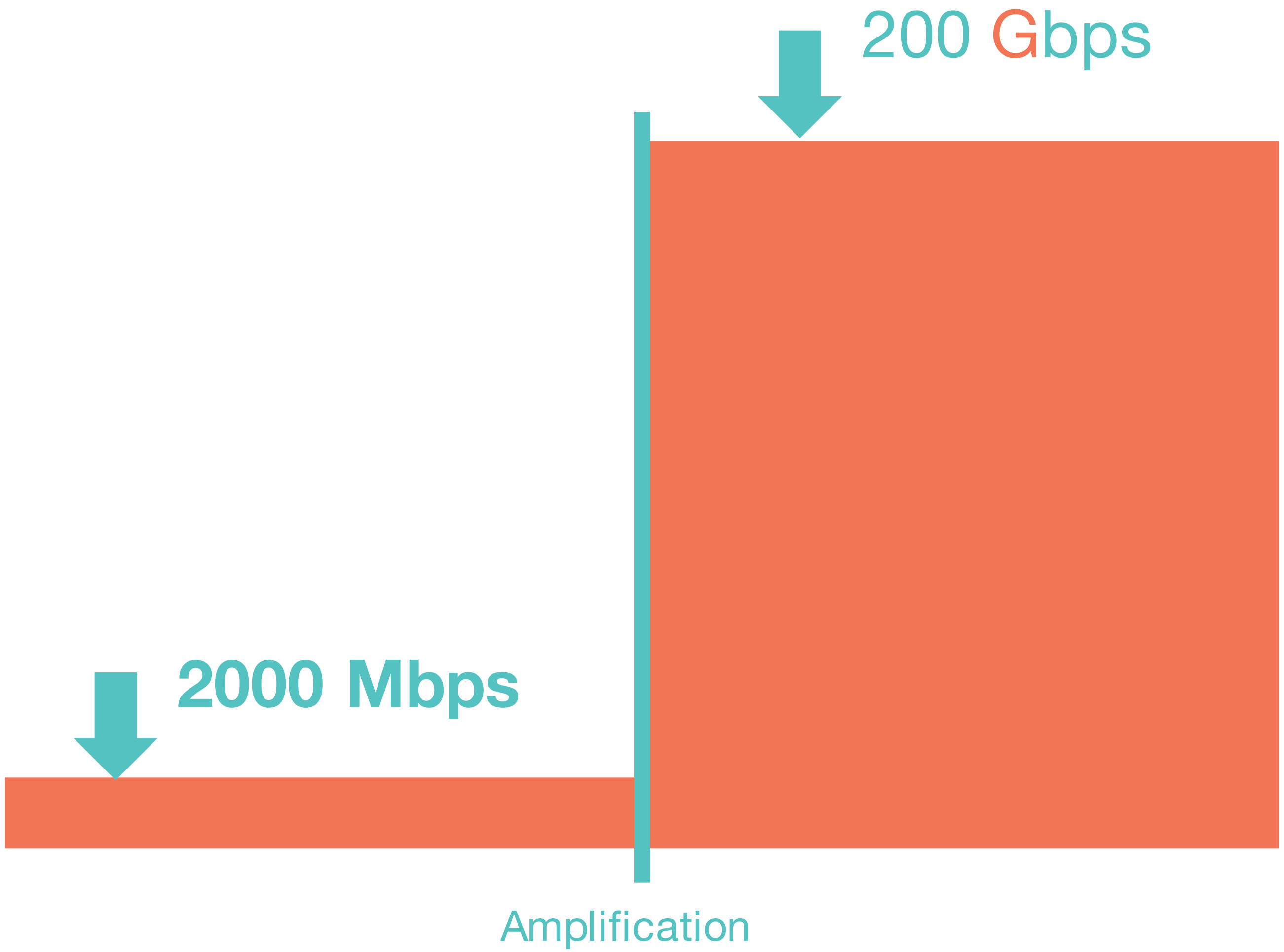
FALSE

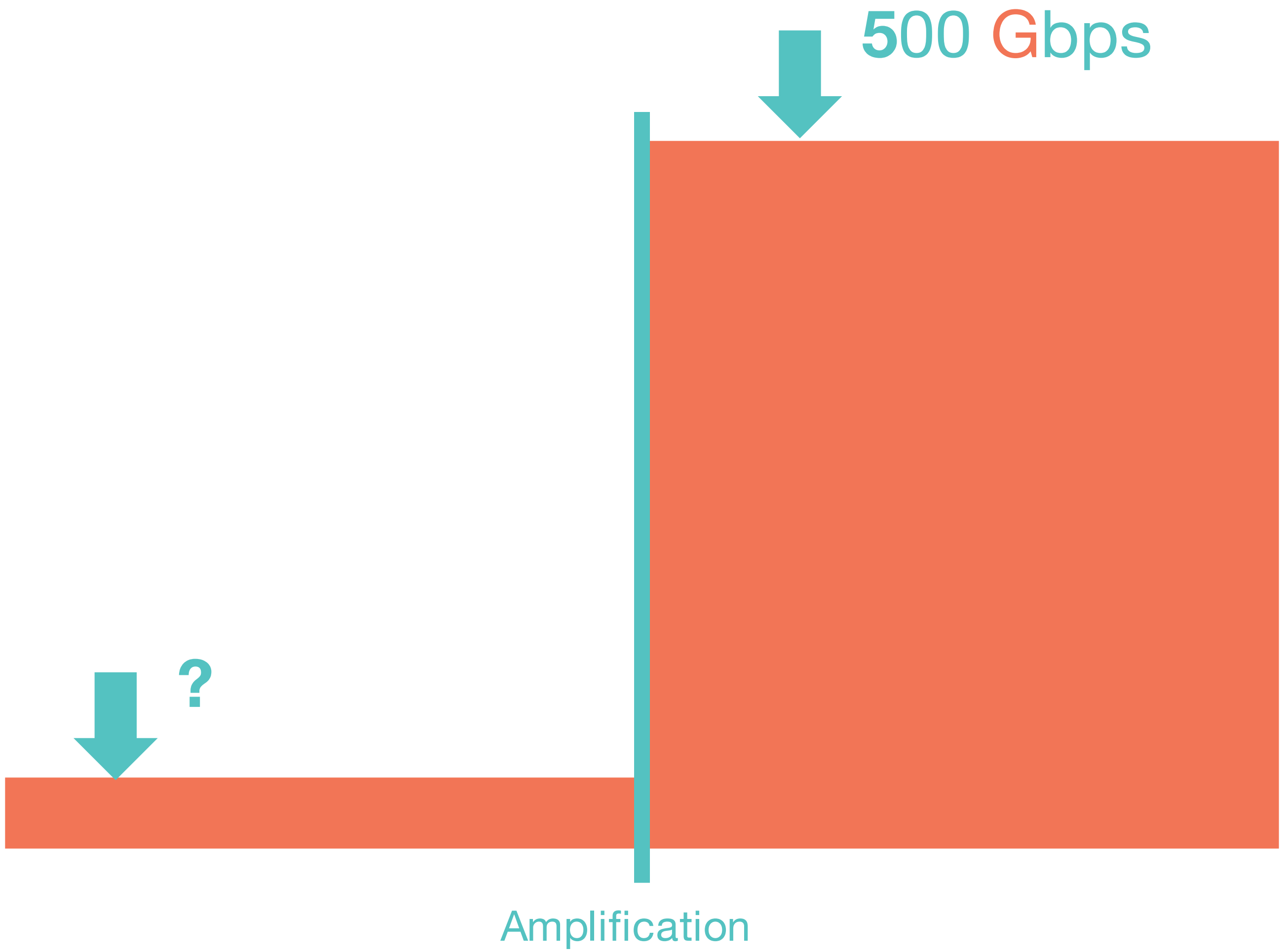
FALSE


30 Gbps
300 Mbps
Amplification

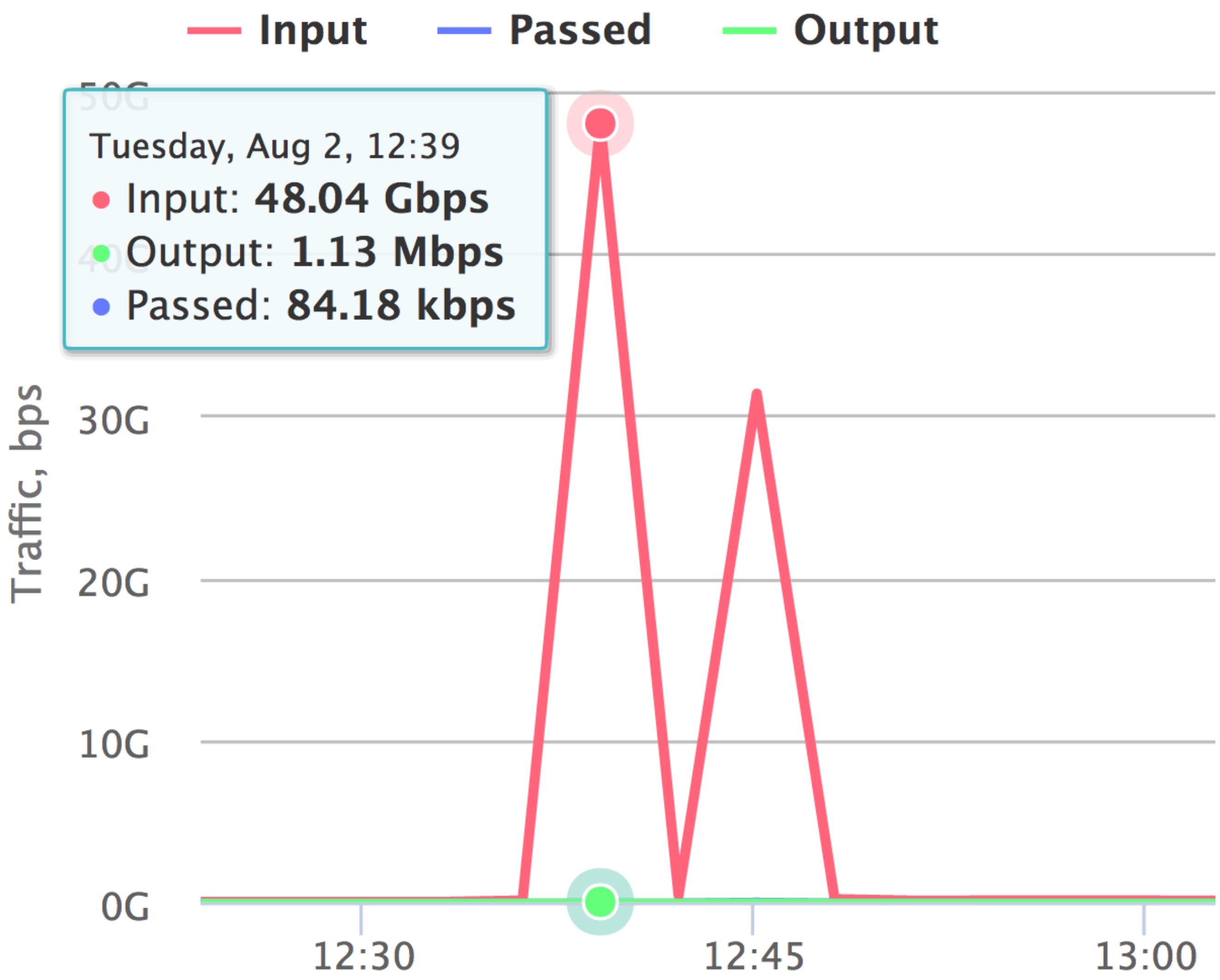

200 Gbps
2000 Mbps
Amplification




200 Gbps
2000 Mbps
Amplification


500 Gbps
?
Amplification

Pure TCP-based attack **today**



The **Void**

- To survive TCP- and HTTPS-based attacks,
  one needs a **session-capable** and **TLS-capable DPI**
- To survive large botnets,
  one needs a **behavioral analysis** and
  correlation analysis built into that DPI
- That’s **extremely expensive** for a large network

The **Void**

- Any service offering SLA **must** do all of this
- A service lacking any of those features is **best effort**
- **No one likes best effort services**

The **Cure**

- BCP 38 is **no cure***
- **IPv6 is no cure**
- Time to fight for yourselves
- Care about other customers
- It’s **every man for himself** now

The Future

the open Net

sine qua non

Vulnerability Risk management for everyone

arkenoi@gmail.com

ENOG12

Thank you, and good luck!

mailto: Artyom Gavrichenkov <ag@qrator.net>