2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS
CONNECTING POINTS OF OPPORTUNITY

Securing ISP Networks

Dustin Curtis - RVW, Inc.

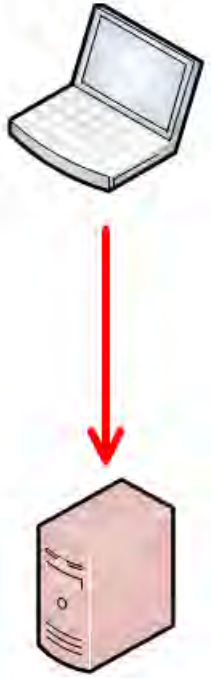
DDoS attacks and ISPs

- Fairly common
- Very effective

What is a DDoS attack?

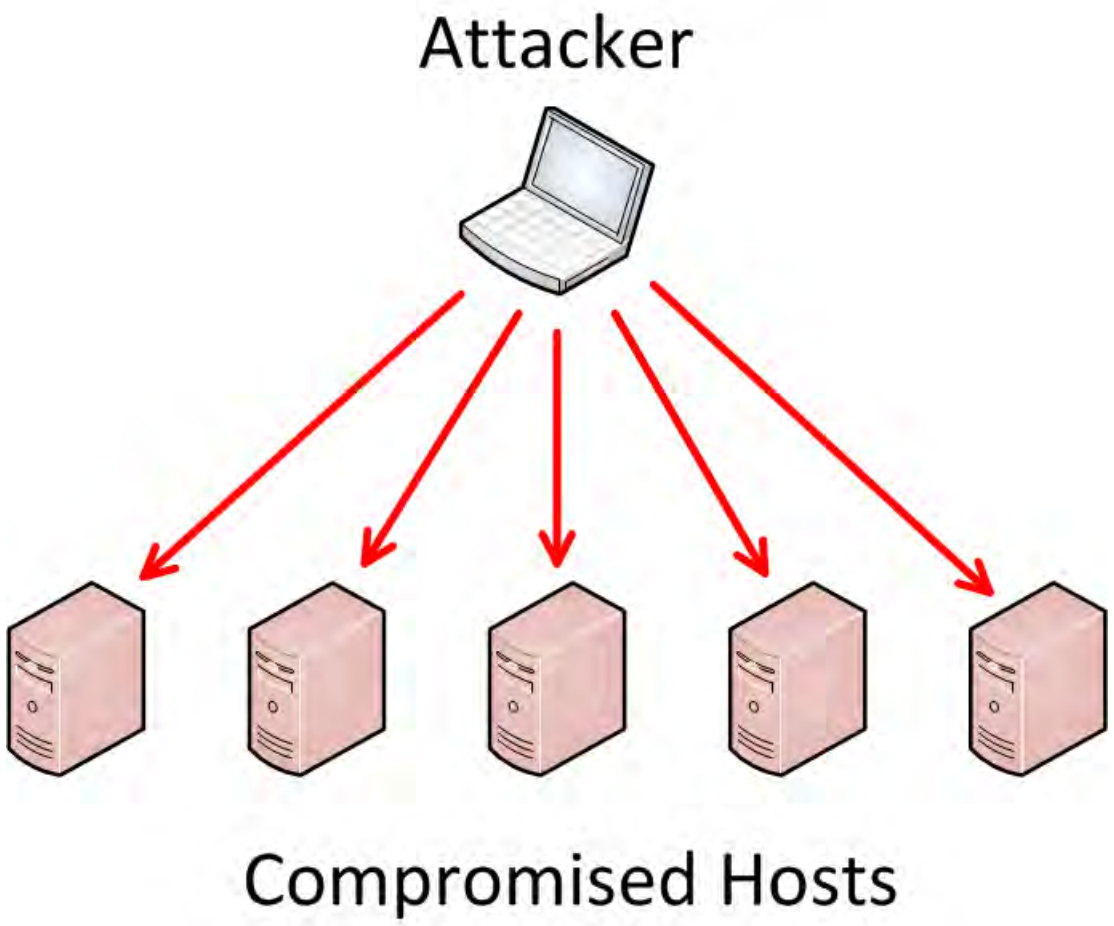
- Malicious
- Target is one host or service typically
- Disrupts service by resource depletion
  - Bandwidth
  - CPU

Attacker

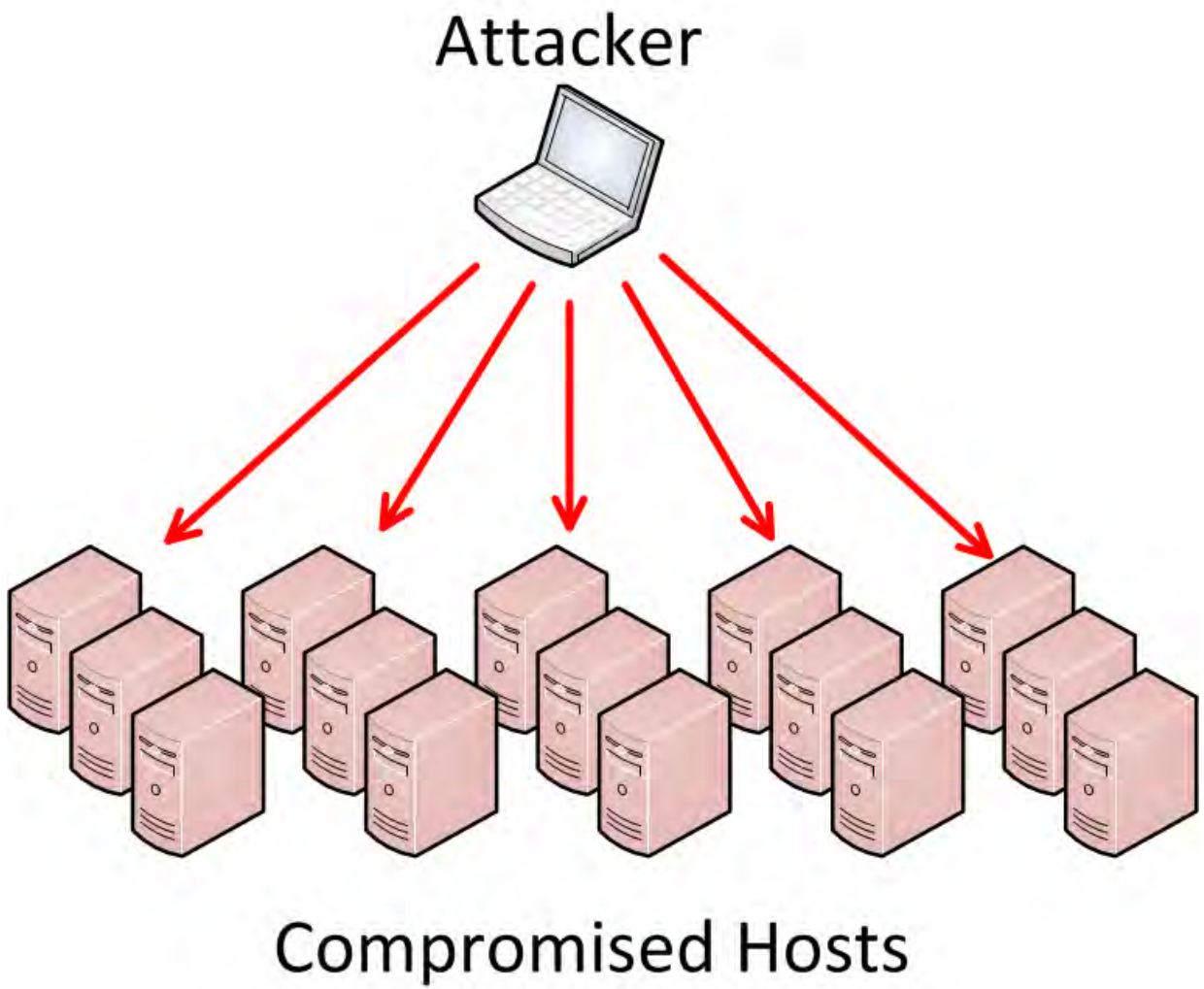


Compromised Host

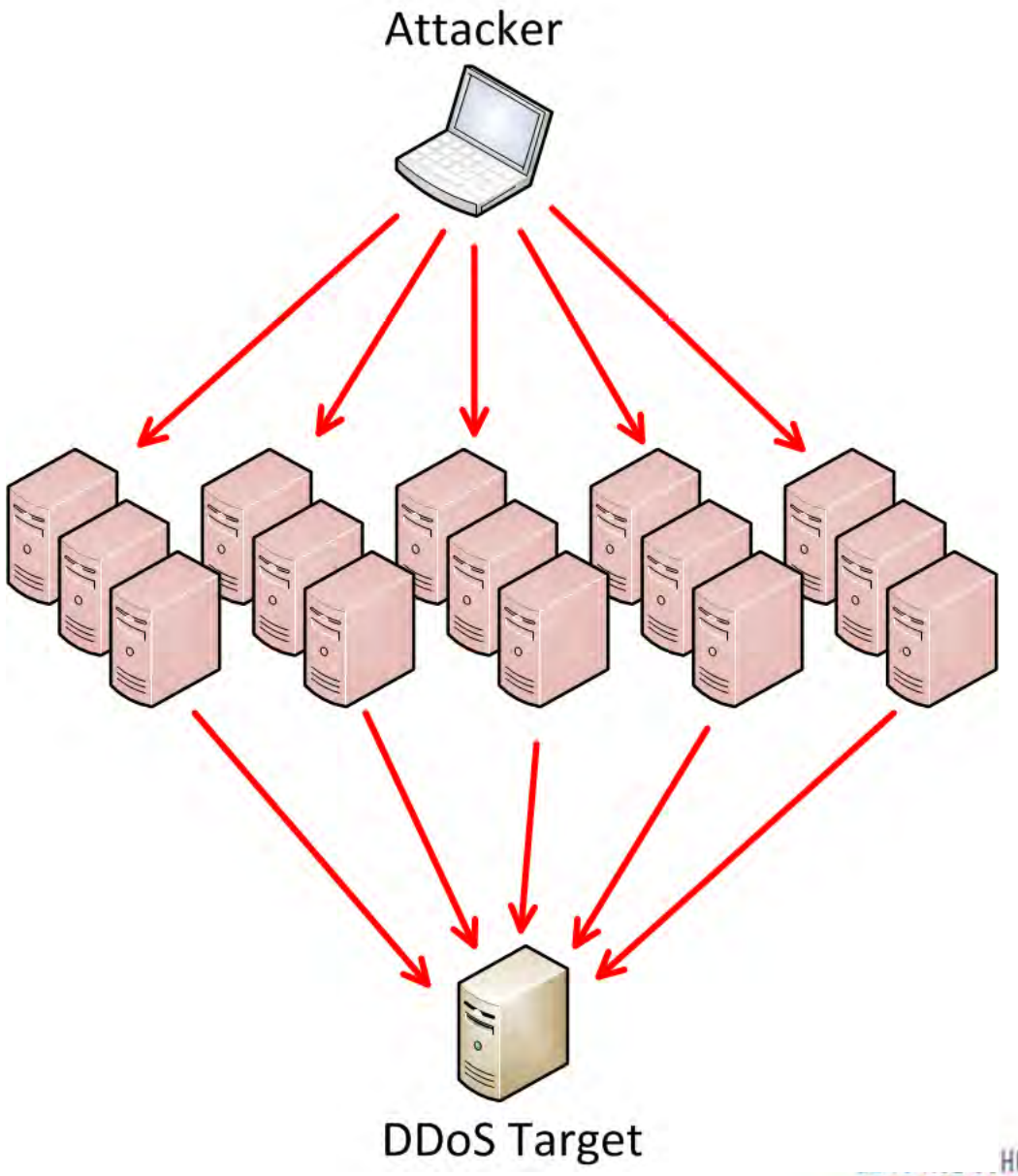
2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY



RVW
2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY
Association of Communication Engineers
ACE



RVW
2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY
Association of Communication Engineers
ACE



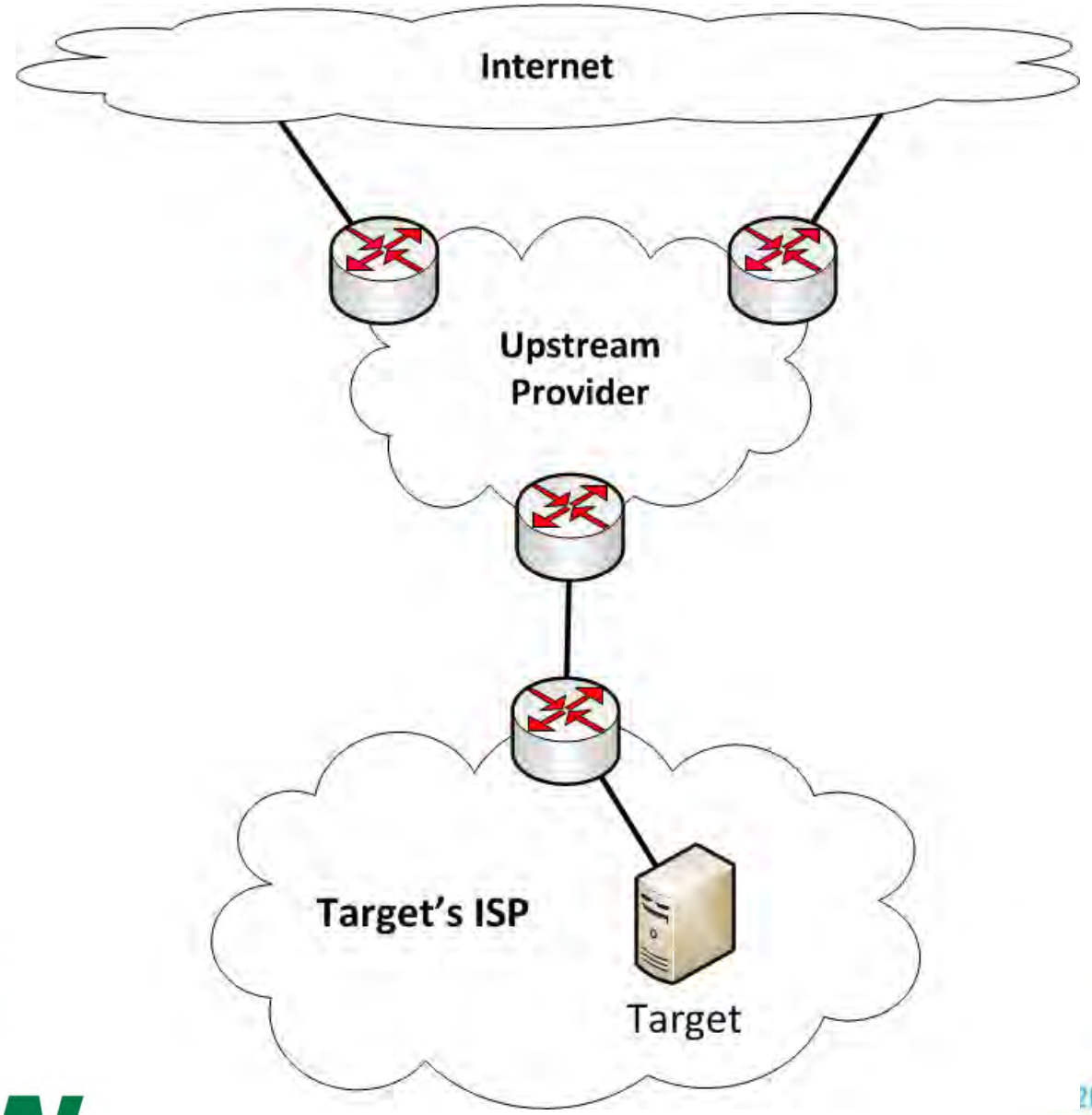
RVW
HOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY
Association of Communication Engineers
ACE

The result…

- Target host's Internet is "down"
  - …and several other subscribers too
- Subscriber QoE is negatively affected
  - Seen as a network outage
  - Can go on for hours
    - …or days ☹

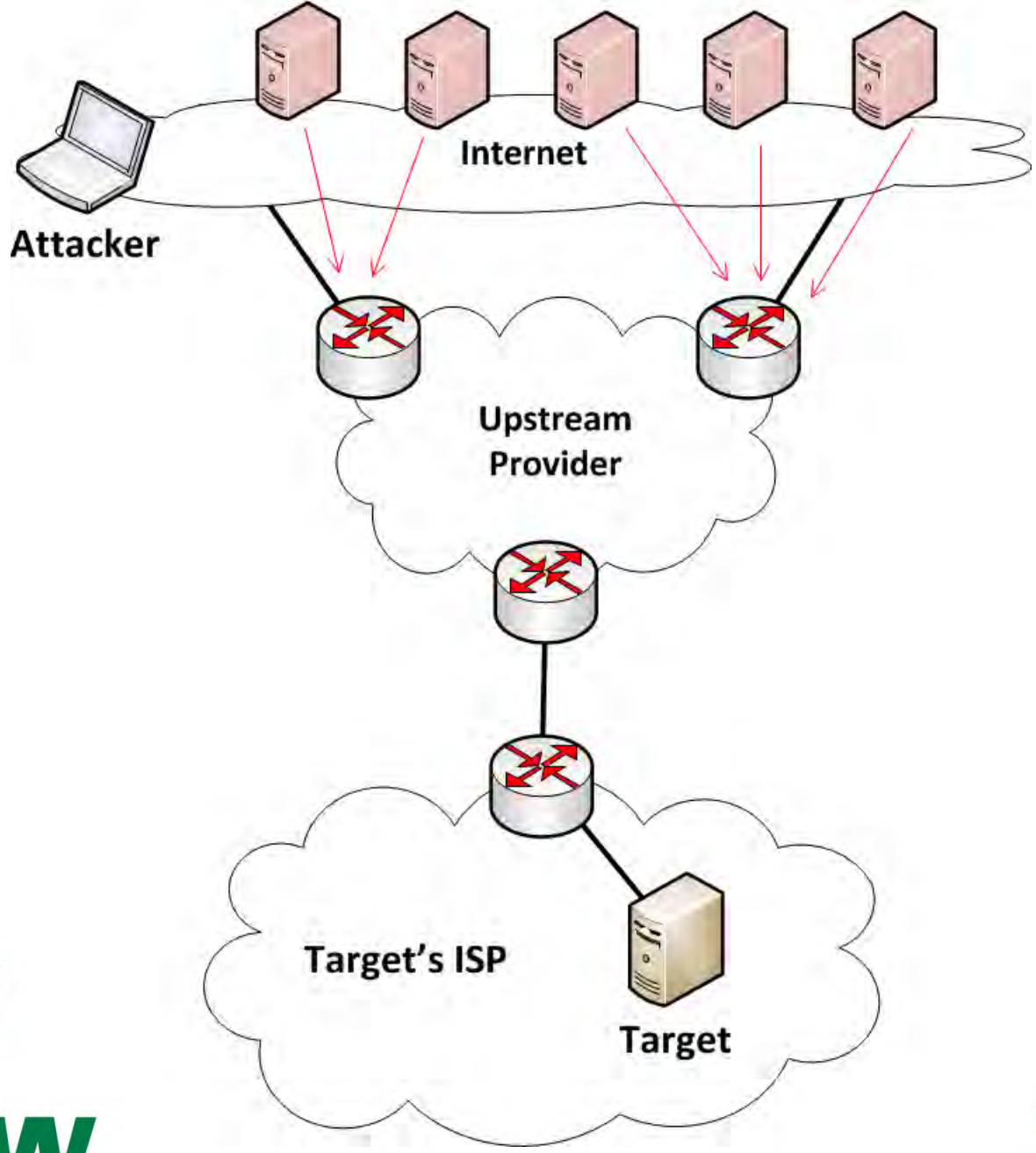
What can be done about it?

- We want the malicious traffic to stop
  - Accomplished with filtering
    - ACL, RTBH, or Flowspec
  - Preferably upstream
- Mitigation Strategies:
  - Manual
  - Autonomous or semi-autonomous



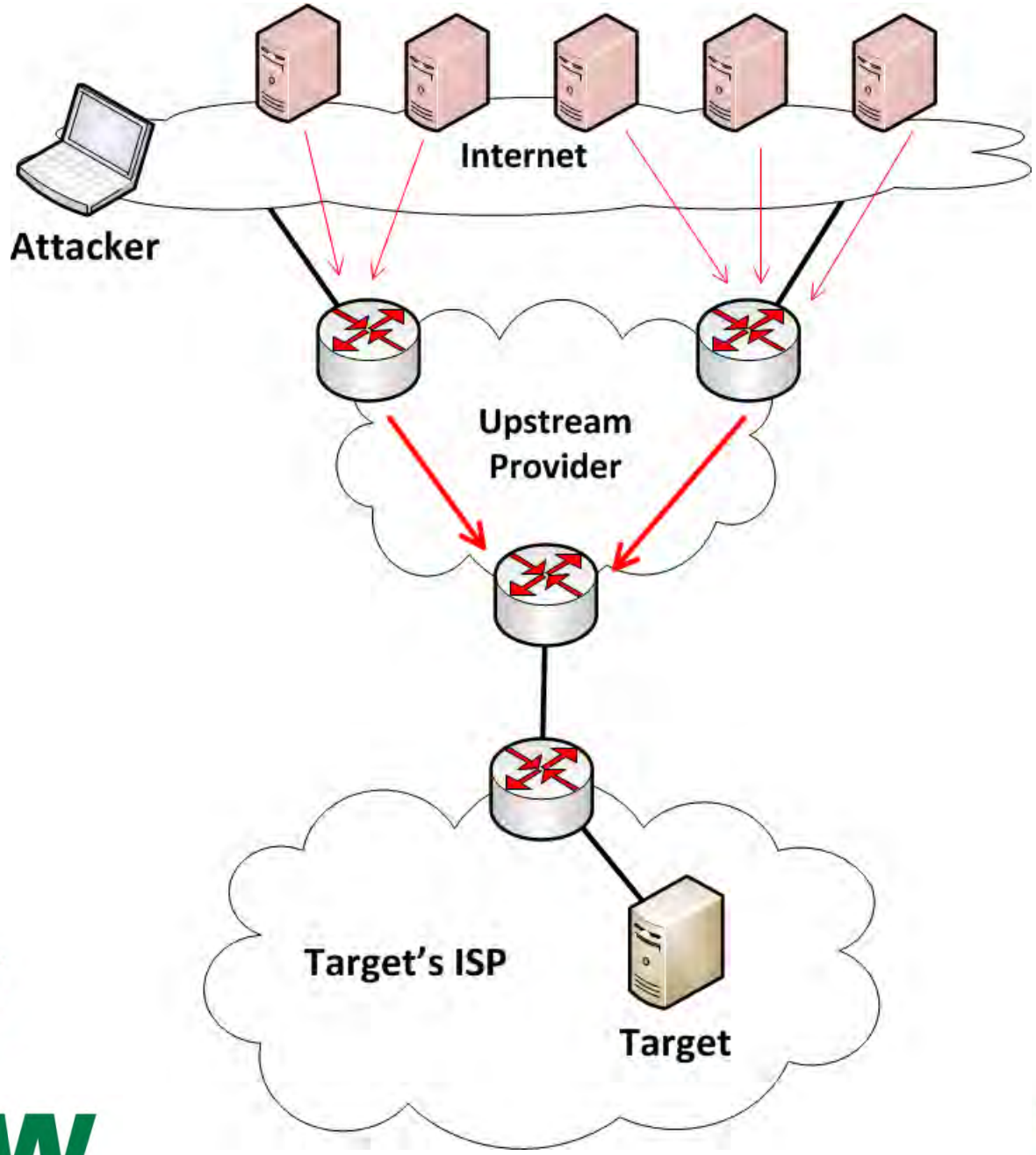
Why filter upstream?

2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY



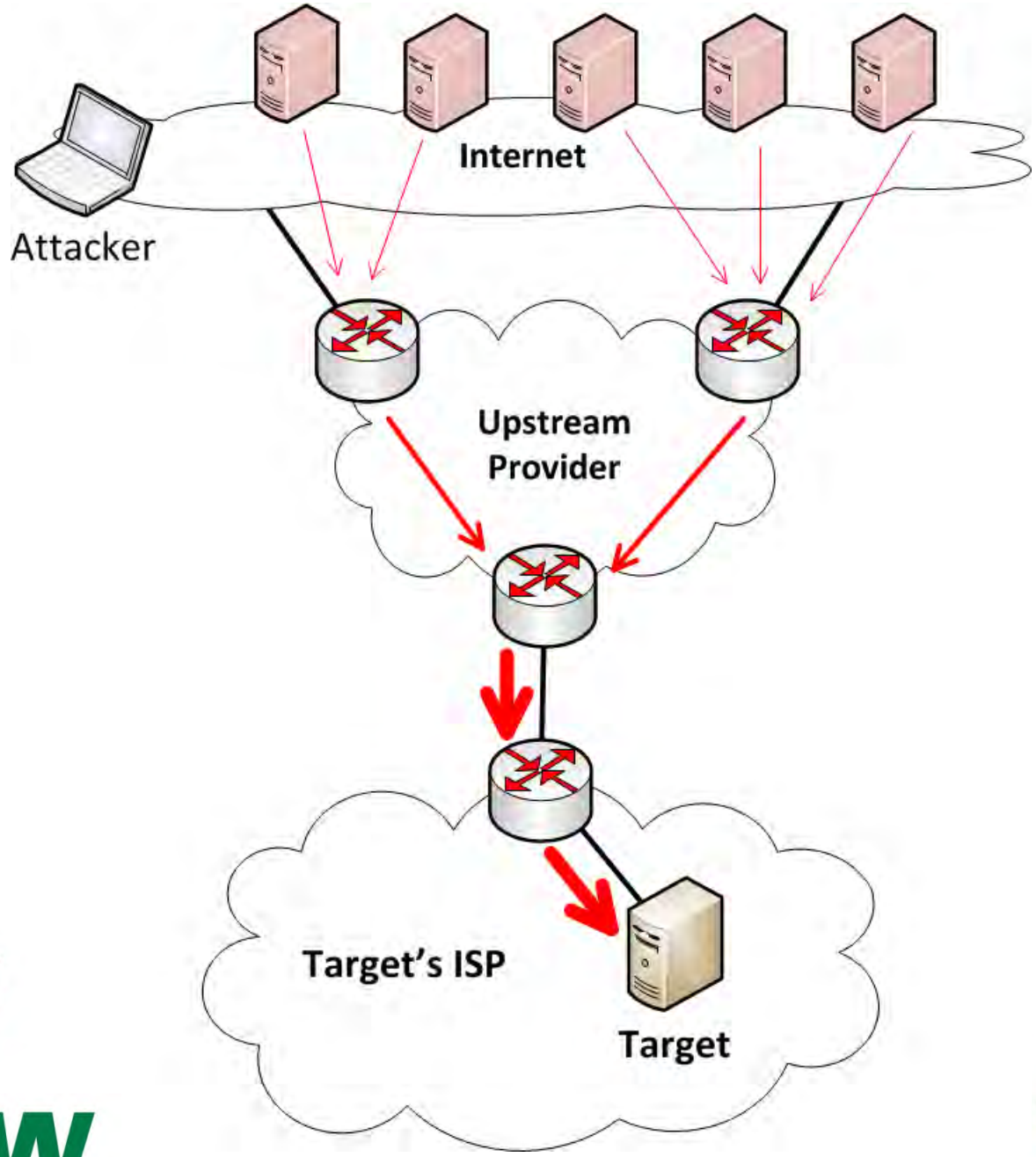
Why filter upstream?

2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY



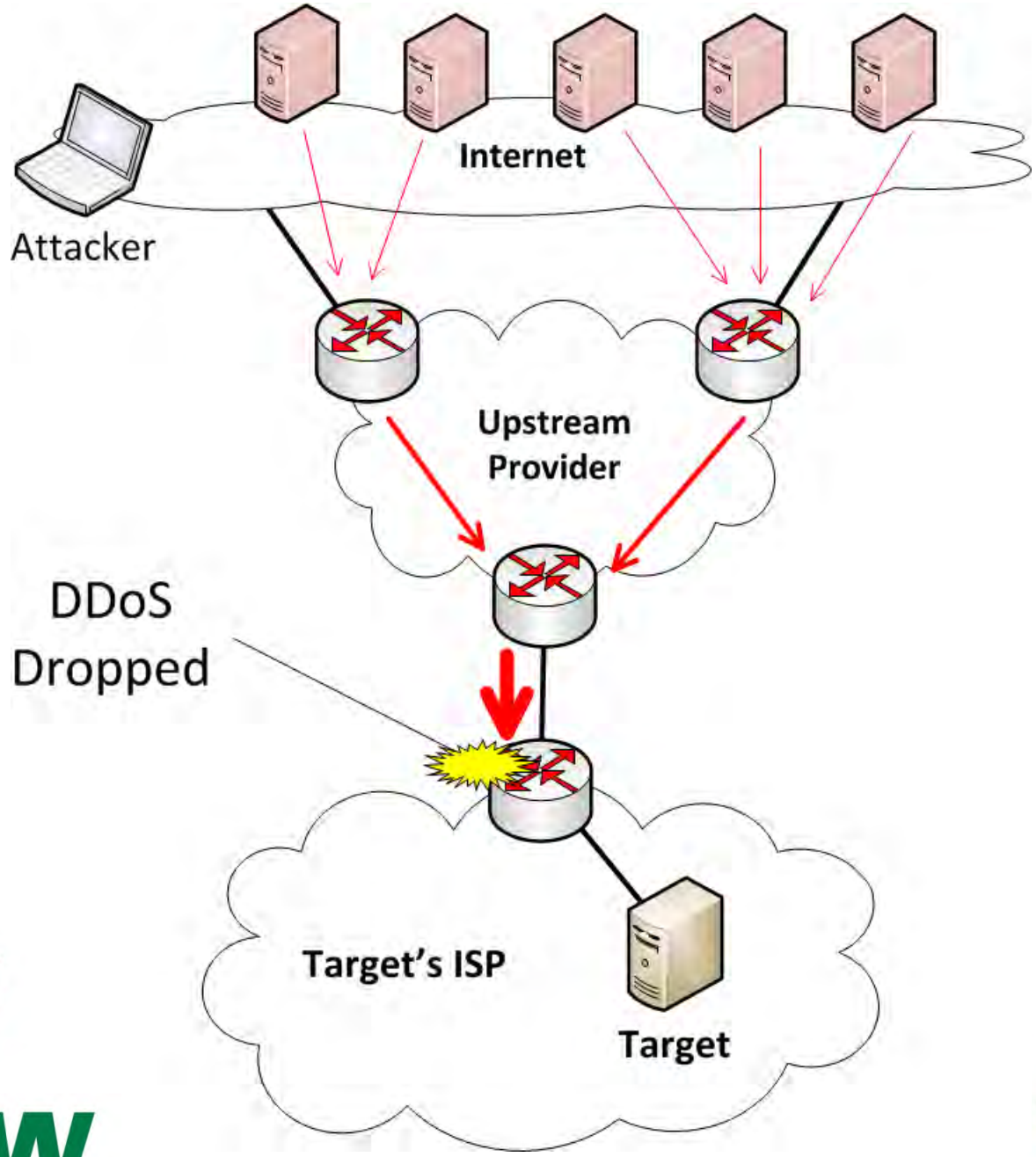
Why filter upstream?

2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY



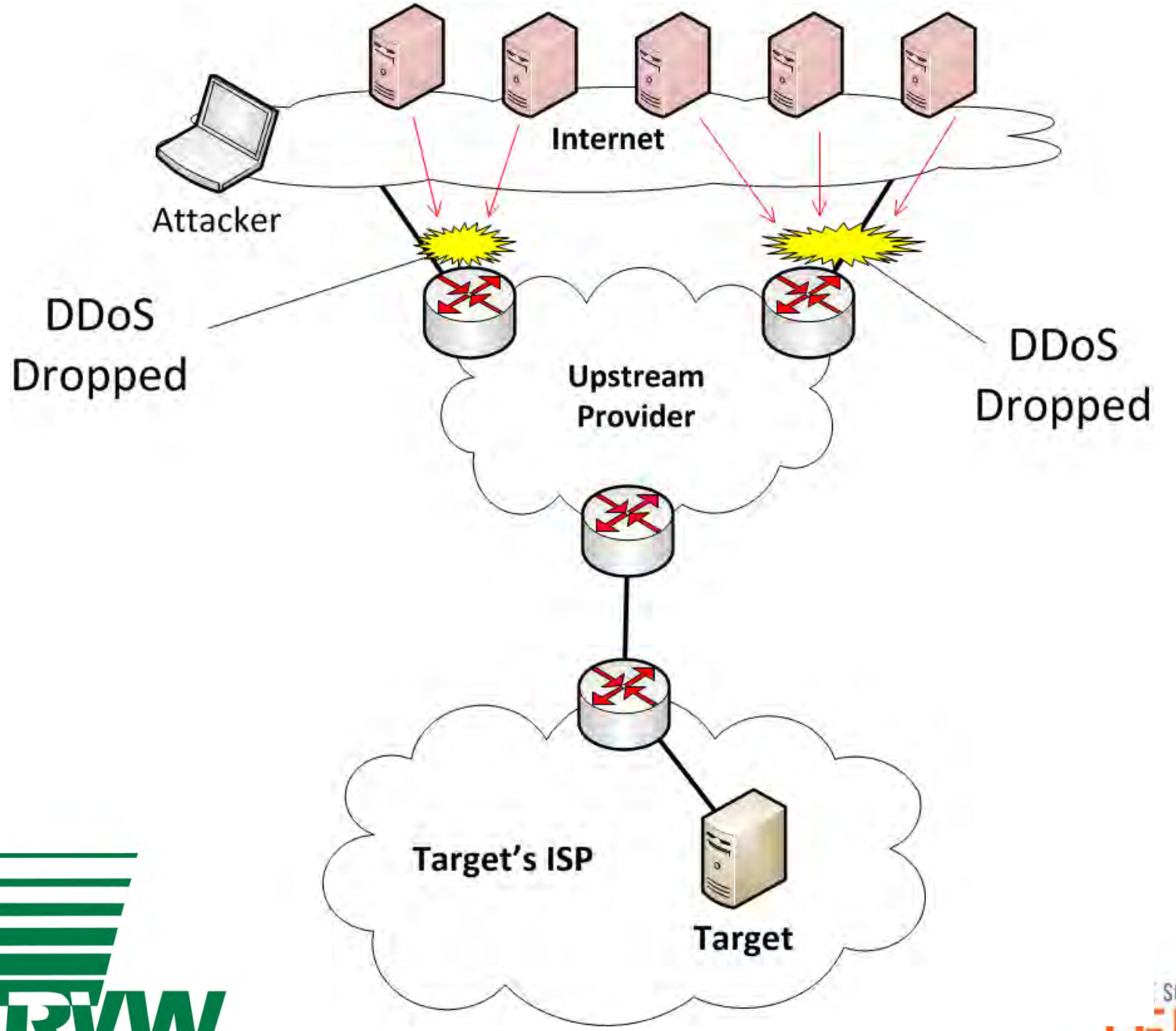
Why filter upstream?

2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY



Why filter upstream?

2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY



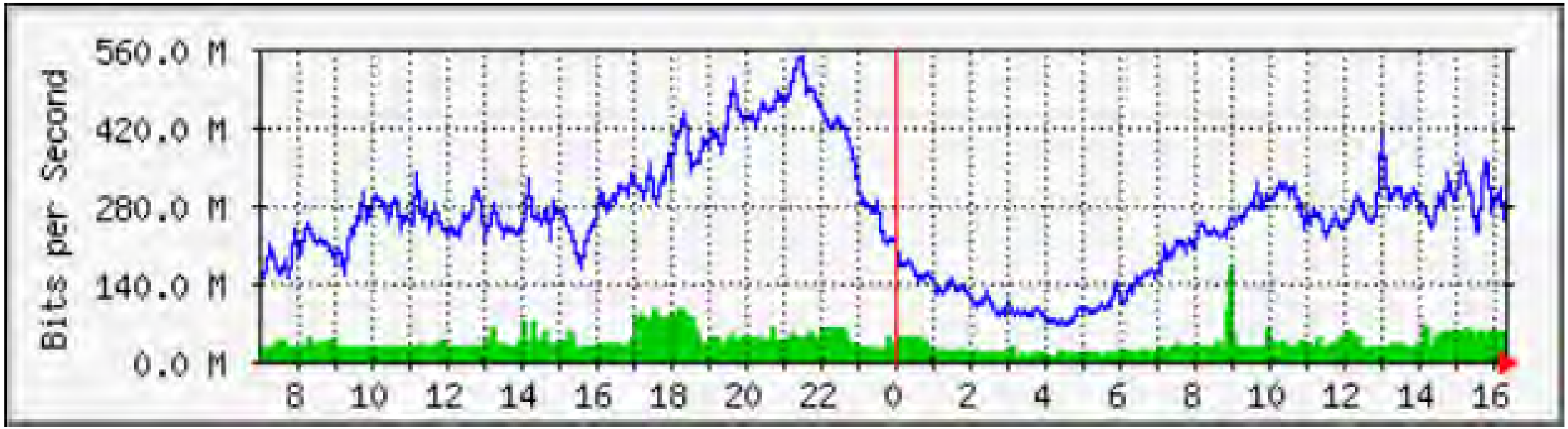
Why filter upstream?

RVW
SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY
ACE
Association of Communication Engineers

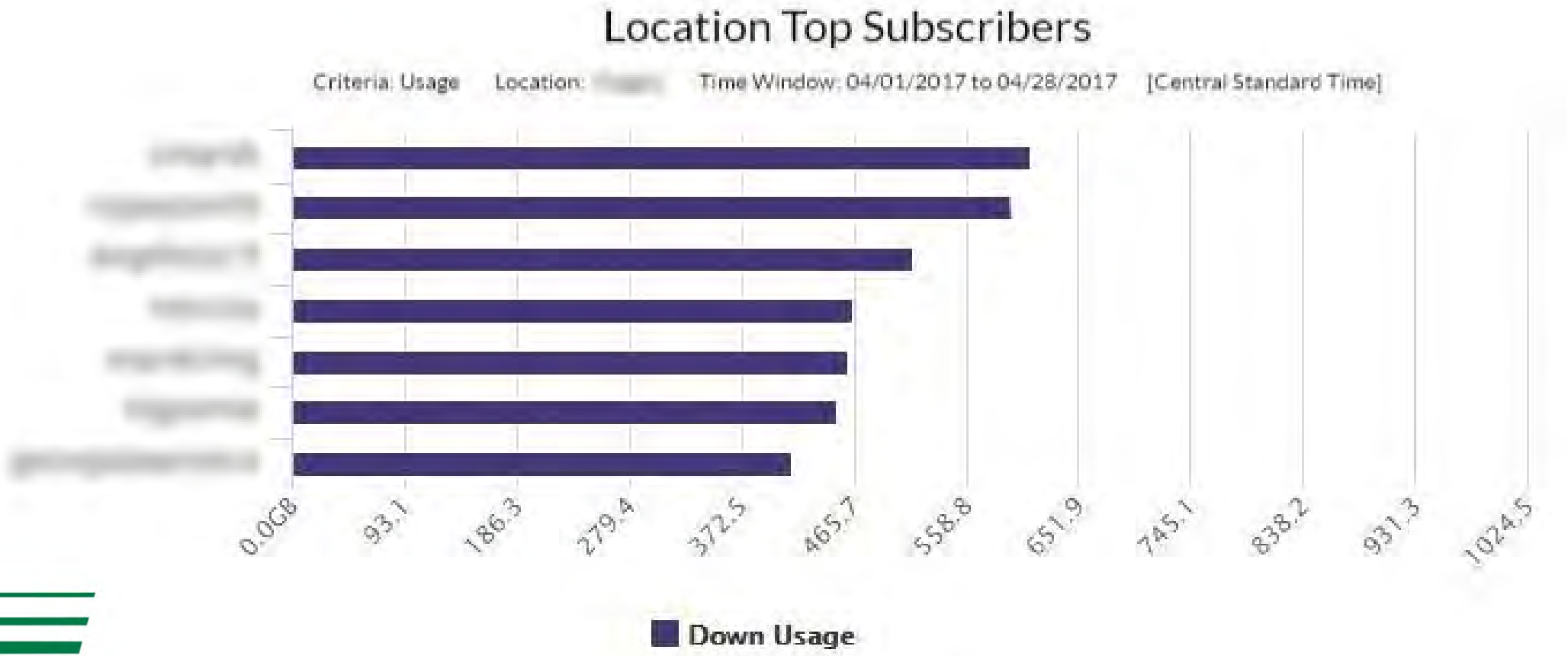
Preparation

- Network Visibility
  - Interface Graphs
    - Router & switch interface statistics graphed over time
  - Sflow
    - Sample, collect, analyze

Interface Graphs



Sflow Analysis



RVW

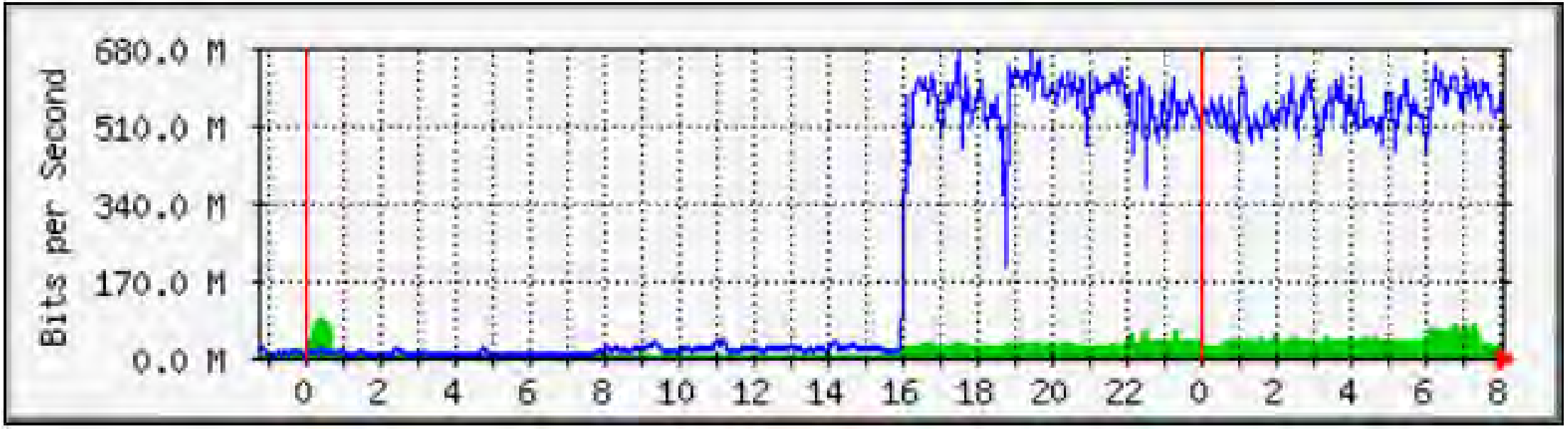
2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY

Association of Communication Engineers ACE

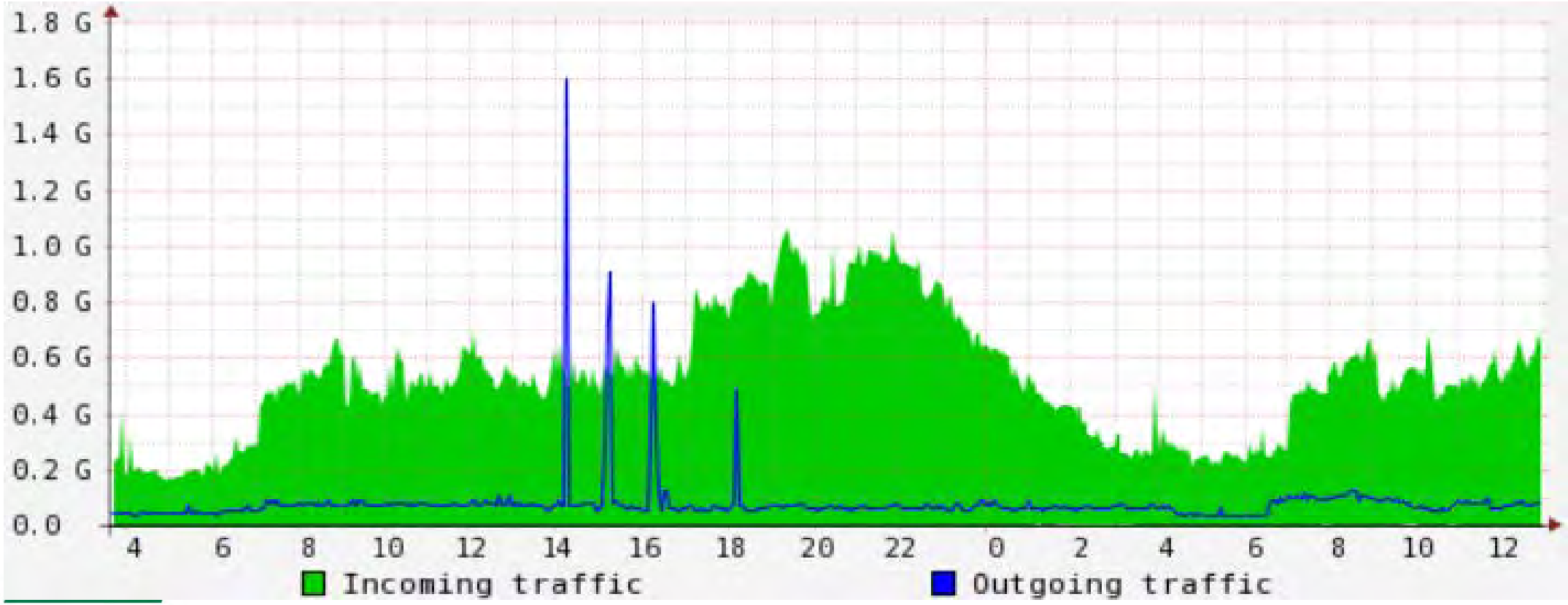
Detection of DDoS

- Recognize attacks based on these graphs
  - Some are subtle, and will missed
  - Others are not…

Not-so-subtle DDoS



DDoS Participation



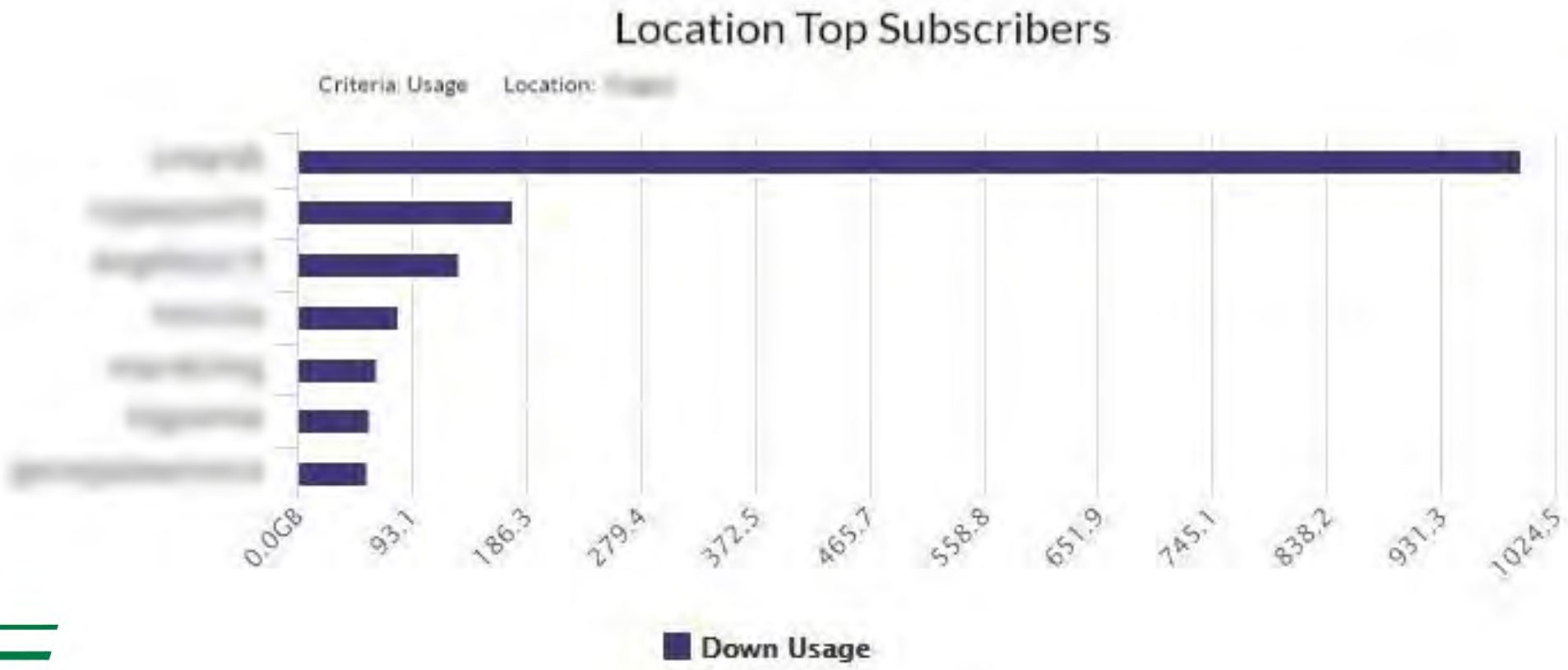
Experience (and Luck) Required

- DDoS starts suddenly
- What <u>should</u> graphs look like?

After Detection…

- Who is the target?
  - Source/Destination IP
  - Source/Destination Port
  - Packet format (fragments, etc…)
  - L4 Flows
- This information is used to define our traffic filter
- Sflow “Top Talkers”
- Wireshark/TCPdump

Who’s the Target?



RVW
2018 ACE SCHOOL & RUS SYMPOSIUM
TERMINUS ATLANTA
CONNECTING POINTS OF OPPORTUNITY
Association of Communication Engineers
ACE

Pick up the phone

- Now that we have actionable data…
  - Call upstream provider(s)
  - Request traffic filtered based on your findings
    - ACL
    - Null route

What could possibly go wrong?

- Manual process is:
  - Time-consuming
  - Error-prone

Automation of the process

- Anti-DDoS Tools
  - Hardware Appliance
    - Can be in-line
  - Software
- Automatic detection of DDoS
  - Sflow

Automated Mitigation - RTBH

- RTBH
  - Requires BGP
  - S/D IP
  - Dynamic null route injection
  - Target effectively disconnected from the Internet
  - Requires upstream cooperation

Automated Mitigation - Flowspec

- Flowspec
  - Also requires upstream capability and cooperation
  - More match criteria than RTBH
    - S/D IP, L4 flow, packet format
  - More actions than RTBH
    - Drop (null route), reroute VRF, Rate limit, QoS Marking
  - Target remains online and only offending traffic is blocked

Be a good Internet Neighbor

- Avoid participating in DDoS attacks
  - Filter egress traffic
    - Prevent IP spoofing
    - Drop malformed packets
  - Use strong passwords on CPE and servers
  - Keep servers patched and configured correctly
    - Vulnerabilities
    - DNS (recursion problems)

Thank You!

Dustin Curtis

RVW, Inc.

(402) 564-2876

dcurtis@rvwinc.com