DDoS Mitigation

Using BGP Flowspec

Justin Ryburn
Consulting Engineer
jryburn@juniper.net

Background

- Who is this guy?
  - http://www.linkedin.com/in/justinryburn
- Why this topic?
  - Experience tracking DDoS “back in the day”

Agenda

- Problem Statement
- Legacy DDoS Mitigation Methods
- BGP Flowspec Overview
- Use Case Examples
- State of the Union

Problem Statement

Is DDoS Really an Issue?

"…taking down a site or preventing transactions is only the tip of the iceberg. A DDoS attack can lead to reputational losses or legal claims over undelivered services."

Kaspersky Lab [1]

Verisign [2]

"Attacks in the 10 Gbps and above category grew by 38% from Q2 … Q3."

NBC News [3]

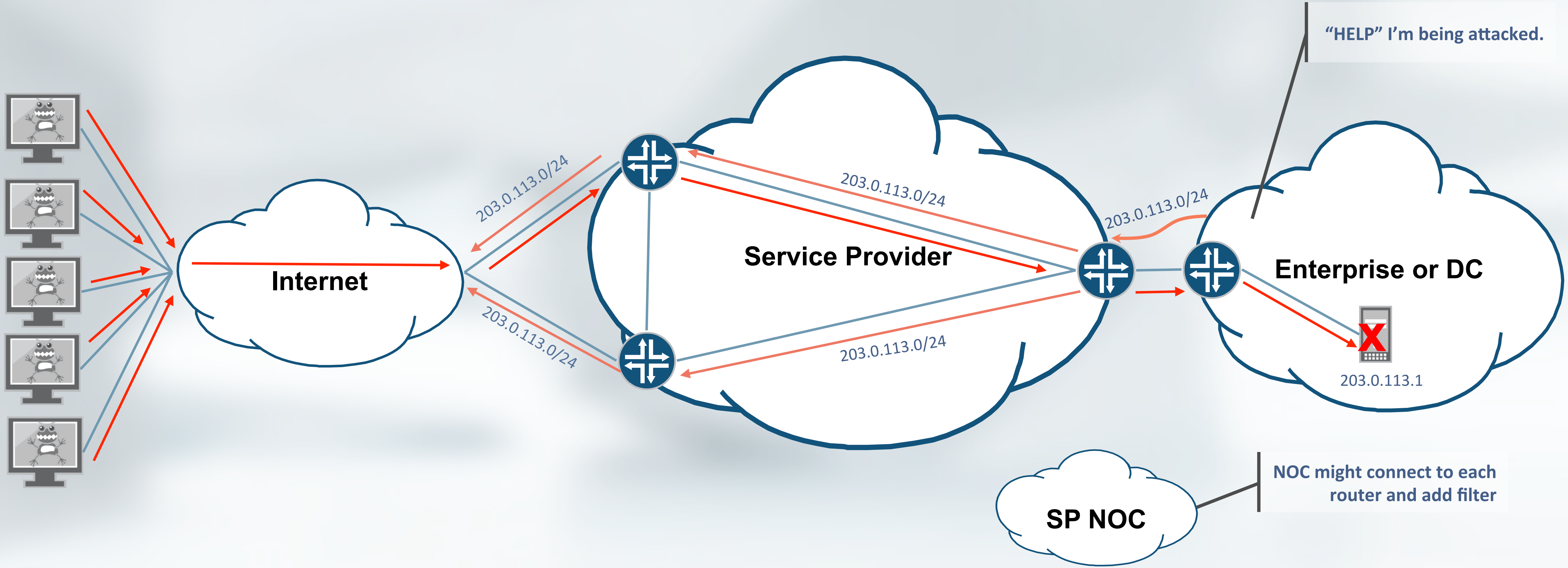
"…more than 40 percent estimated DDoS losses at more than $1 million per day."

Tech Times [4]

"DDoS attack cripples Sony PSN while Microsoft deals with Xbox Live woes"

Legacy DDoS Mitigation Methods

Blocking DDoS in the “Old” Days

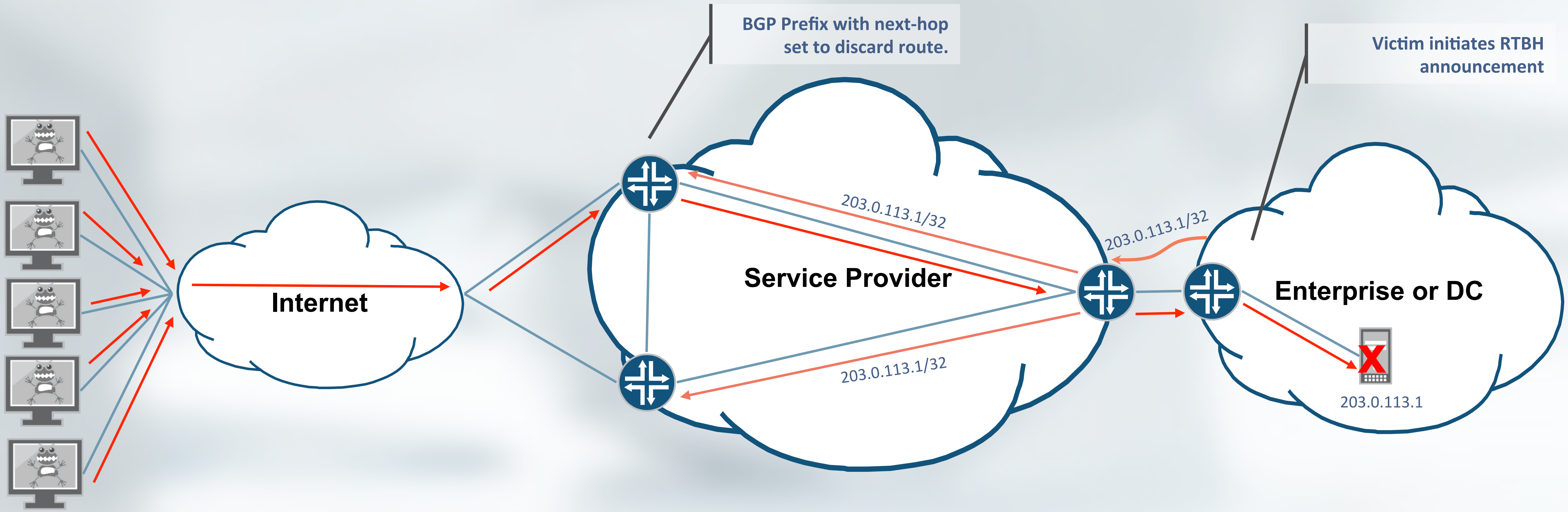


“HELP” I’m being attacked.

NOC might connect to each router and add filter

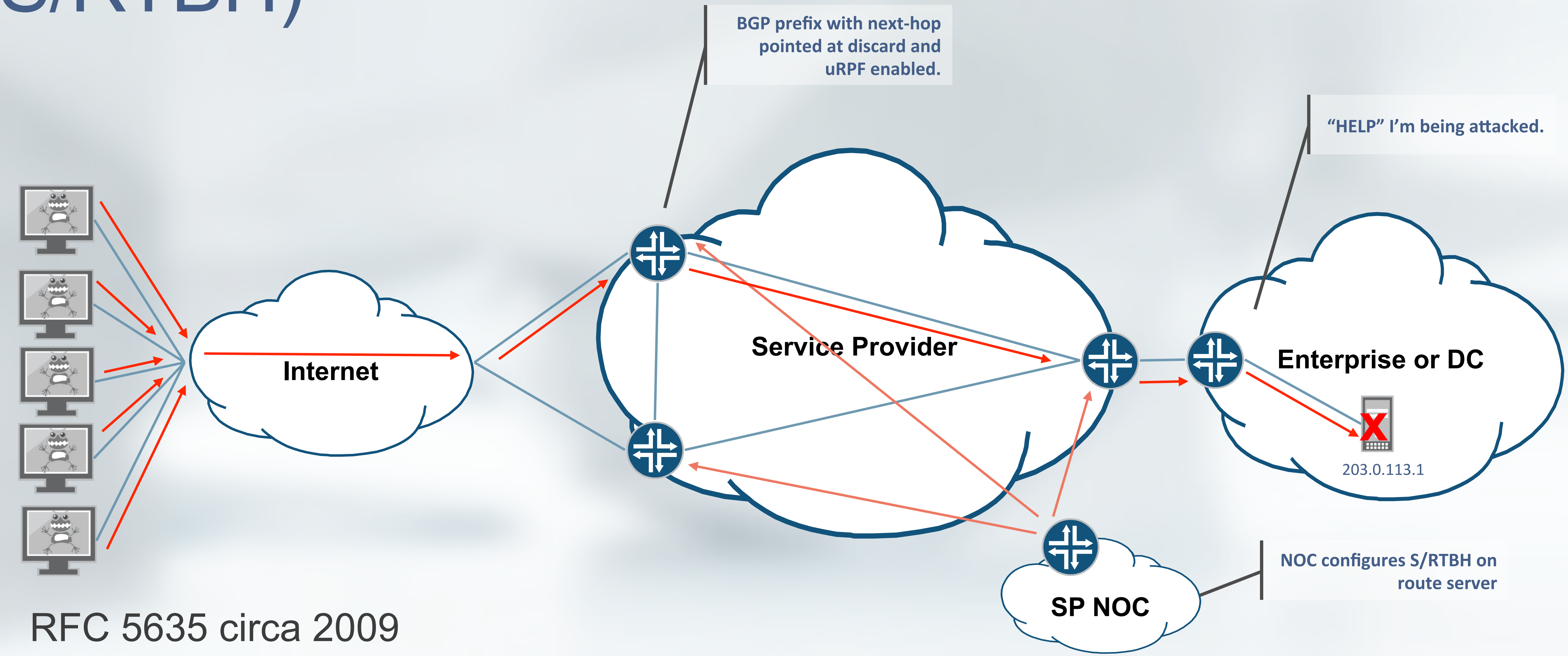
- Easy to implement and uses well understood constructs
- Requires high degree of co-ordination between customer and provider
- Cumbersome to scale in a large network perimeter
- Mis-configuration possible and expensive

Destination Remotely Triggered Black Hole (D/RTBH)



- RFC 3882 circa 2004
- Requires pre-configuration of discard route on all edge routers
- Victim's destination address is completely unreachable but attack (and collateral damage) is stopped.

Source Remotely Triggered Black Hole (S/RTBH)


BGP prefix with next-hop pointed at discard and uRPF enabled.
"HELP" I'm being attacked.
Internet
Service Provider
Enterprise or DC
203.0.113.1
SP NOC
NOC configures S/RTBH on route server

- RFC 5635 circa 2009
- Requires pre-configuration of discard route and uRPF on all edge routers
- Victim's destination address is still useable
- Only works for single (or small number) source.

BGP FlowSpec Overview

BGP Flow Specification

- Specific information about a flow can now be distributed using a BGP NLRI defined in RFC 5575 [5] circa 2009
  - AFI/SAFI = 1/133: Unicast Traffic Filtering Applications
  - AFI/SAFI = 1/134: VPN Traffic Filtering Applications
- Flow routes are automatically validated against unicast routing information or via routing policy framework.
  - Must belong to the longest match unicast prefix.
- Once validated, firewall filter is created based on match and action criteria.

BGP Flow Specification

- BGP Flowspec can include the following information:
  - Type 1 - Destination Prefix
  - Type 2 - Source Prefix
  - Type 3 - IP Protocol
  - Type 4 – Source or Destination Port
  - Type 5 – Destination Port
  - Type 6 - Source Port
  - Type 7 – ICMP Type
  - Type 8 – ICMP Code
  - Type 9 - TCP flags
  - Type 10 - Packet length
  - Type 11 – DSCP
  - Type 12 - Fragment Encoding

BGP Flow Specification

- Actions are defined using BGP Extended Communities:
    - 0x8006 – traffic-rate (set to 0 to drop all traffic)
    - 0x8007 – traffic-action (sampling)
    - 0x8008 – redirect to VRF (route target)
    - 0x8009 – traffic-marking (DSCP value)

Vendor Support

- DDoS Detection Vendors:
  - Arbor Peakflow SP 3.5
  - Accumuli DDoS Secure
- Router Vendors:
  - Alcatel-Lucent SR OS 9.0R1
  - Juniper JUNOS 7.3
  - Cisco 5.2.0 for ASR and CRS [6]
- OpenSource BGP Software:
  - ExaBGP

What Makes BGP Flowspec Better?

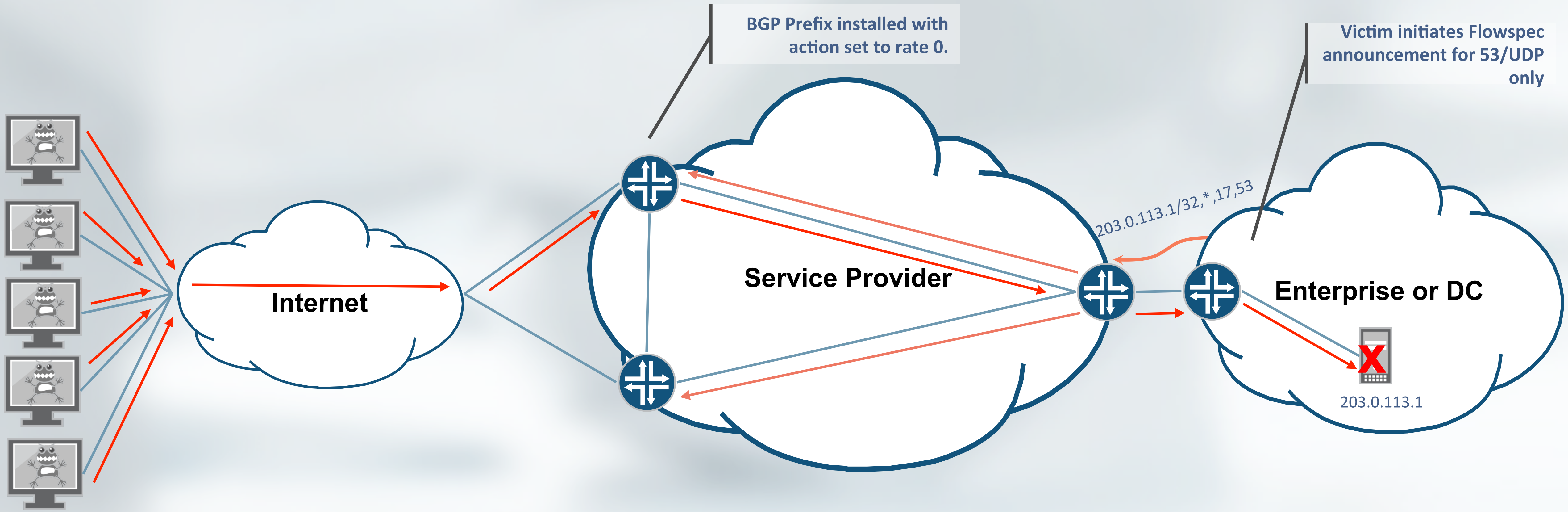
- Same granularity as ACLs
  - Based on n-tuple matching
- Same automation as RTBH
  - Much easier to propagate filters to all edge routers in large networks
- Leverages BGP best practices and policy controls
  - Same filtering and best practices used for RTBH can be applied to BGP Flowspec

Caveats

- Forwarding Plane resources
  - Creating dynamic firewall filters that use these resources
  - More complex FS routes/filters will use more resources
  - Need to test your vendors limits and what happens when it is hit
  - Usually ways to limit the number and complexity of filters to avoid issues
- Not a replacement technology
  - Should be ADDED to existing mitigation methods and not replace them
- When it goes wrong (bugs) it goes wrong fast
  - Cloudflare outage: https://blog.cloudflare.com/todays-outage-post-mortem-82515/

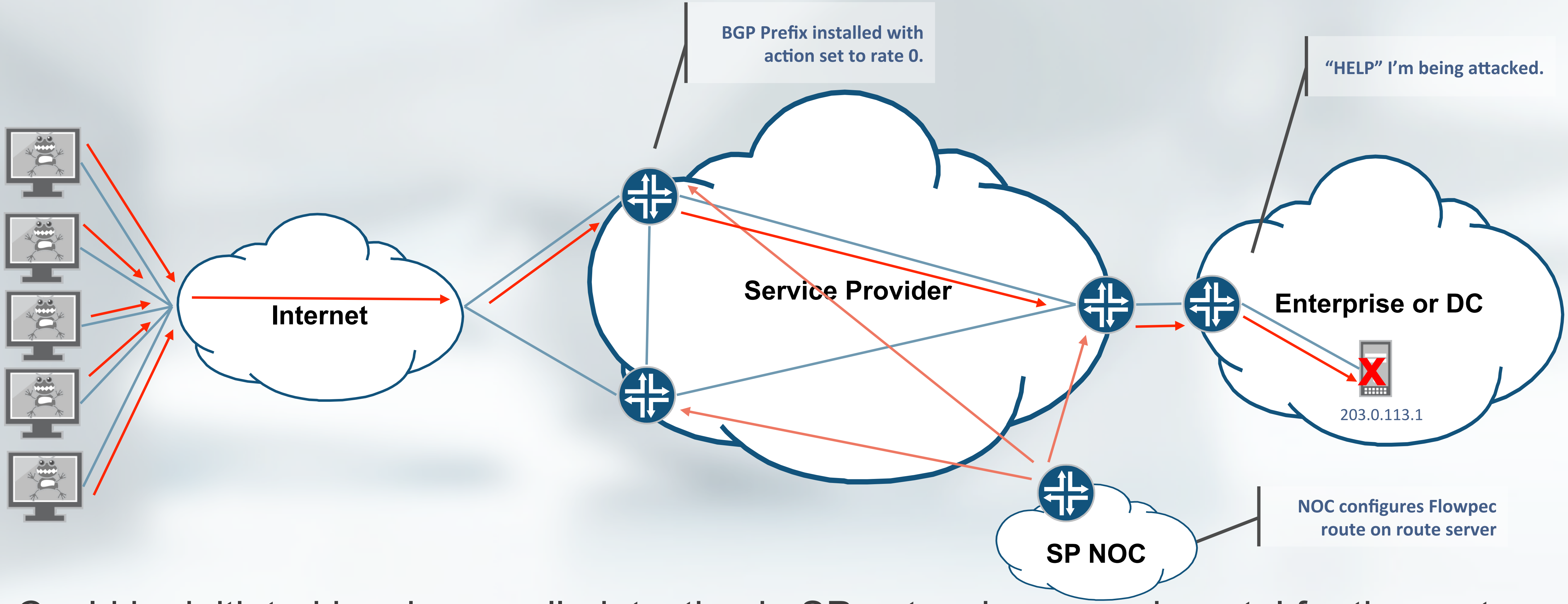
Use Case Examples

Inter-domain DDoS Mitigation Using Flowspec



- Allows ISP customer to initiate the filter.
- Requires sane filtering at customer edge.

Intra-domain DDoS Mitigation Using Flowspec



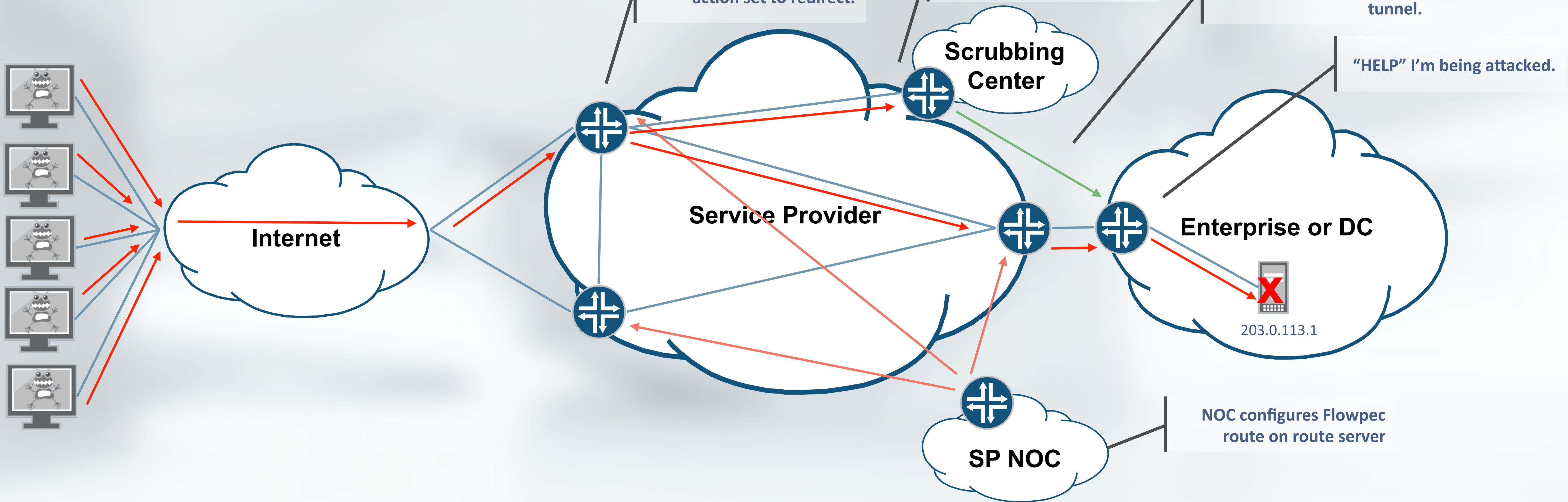
BGP Prefix installed with action set to rate 0.

“HELP” I’m being attacked.

NOC configures Flowpec route on route server

- Could be initiated by phone call, detection in SP network, or a web portal for the customer.
- Requires co-ordination between customer and provider.

DDoS Mitigation Using Scrubbing Center



BGP Prefix installed with action set to redirect.

Attack traffic is scrubbed by DPI appliance.

Legitimate traffic sent to customer via GRE or VRF tunnel.

"HELP" I'm being attacked.

NOC configures Flowpec route on route server

- Could be initiated by phone call, detection in SP network, or a web portal for the customer.
- Allows for mitigating application layer attacks without completing the attack.

Real World Example (TDC)

"Where I think FlowSpec excels, is for protection of our mobile platform.

2 /24s are shared among a million mobile devices with NAT in a firewall.

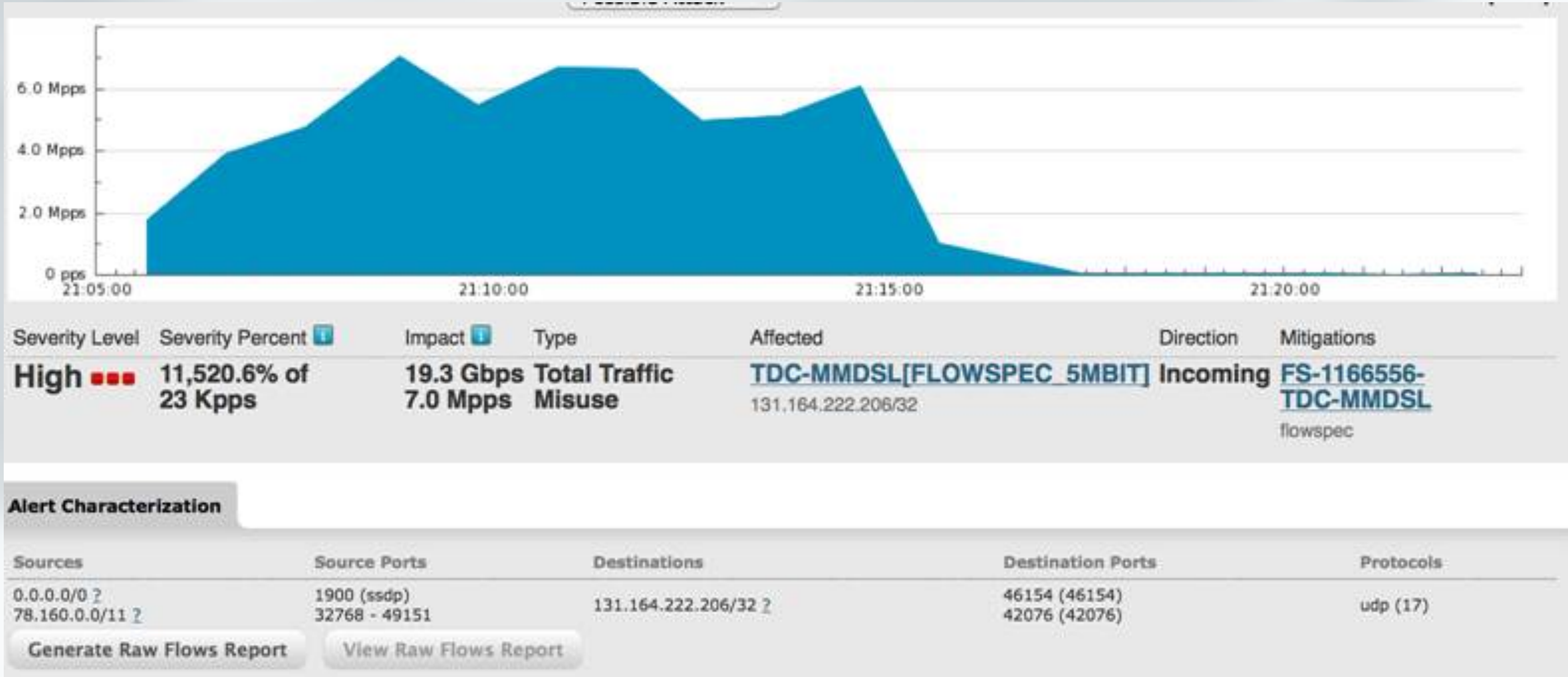
The link capacity (and in part the firewall itself) is overloaded by a simple DDoS attack against just one of these adresses.

The system detects a DoS attack against an address on the firewall.
It will identify total traffic, UDP, fragments, TCP SYN, ICMP, whatever, and depending on what kind of attack it is, a policer is added for the specific protocol/attack on individual peering routers. Protocols are policed with individual policers, so that for instance UDP and TCP SYN can be policed to different throughputs.

Basically, an attack against a single IP on UDP will not affect other customers being NAT'ed to the same address, using anything but UDP - and link capacity is protected."

Real World Example

- Attack on 1/13/16



Severity Level	Severity Percent	Impact	Type	Affected	Direction	Mitigations
High ■■■	11,520.6% of 23 Kpps	19.3 Gbps 7.0 Mpps	Total Traffic Misuse	TDC-MMDSL[FLOWSPEC_5MBIT] 131.164.222.206/32	Incoming	FS-1166556-TDC-MMDSL flowspec

Alert Characterization

Sources	Source Ports	Destinations	Destination Ports	Protocols
0.0.0.0/0 ? 78.160.0.0/11 ?	1900 (ssdp) 32768 - 49151	131.164.222.206/32 ?	46154 (46154) 42076 (42076)	udp (17)

Where Are We Going?

- IPv6 Support
  - http://tools.ietf.org/html/draft-ietf-idr-flow-spec-v6-06
- Relaxing Validation
  - http://tools.ietf.org/html/draft-ietf-idr-bgp-flowspec-oid-02
- Redirect to IP Action
  - https://tools.ietf.org/html/draft-ietf-idr-flowspec-redirect-ip-02

State of the Union

Summary of Survey

- Great idea and would love to see it take off but…
- Enterprises and Content Providers are waiting for ISPs to accept their Flowspec routes.
  - Some would even be willing to switch to an ISP that did this.
- ISPs are waiting for vendors to support it.
  - More vendors supporting it
  - Specific features they need for their environment
  - Better scale or stability

References

- [1] Kaspersky Lab – Every Third Public Facing Company Encounters DDoS Attacks **http://tinyurl.com/neu4zzr**
- [2] Verisign – 2014 DDoS Attack Trends **http://tinyurl.com/oujgx94**
- [3] NBC News – Internet Speeds are Rising Sharply, But So Are Hack Attacks **http://tinyurl.com/q4u2b7m**
- [4] Tech Times – DDoS Attack Cripples Sony PSN While Microsoft Deals with Xbox Live Woes **http://tinyurl.com/kkdczjx**
- [5] RFC 5575 - Dissemination of Flow Specification Rules **http://www.ietf.org/rfc/rfc5575.txt**
- [6] Cisco - Implementing BGP Flowspec **http://tinyurl.com/mm5w7mo**
- [7] Cisco – Understanding BGP Flowspec **http://tinyurl.com/l4kwb3b**

More Information

- NANOG PDF
- NANOG YouTube Video
- Day One Guide

Thank You!