Internet2 Security Working Group 2/18/2016

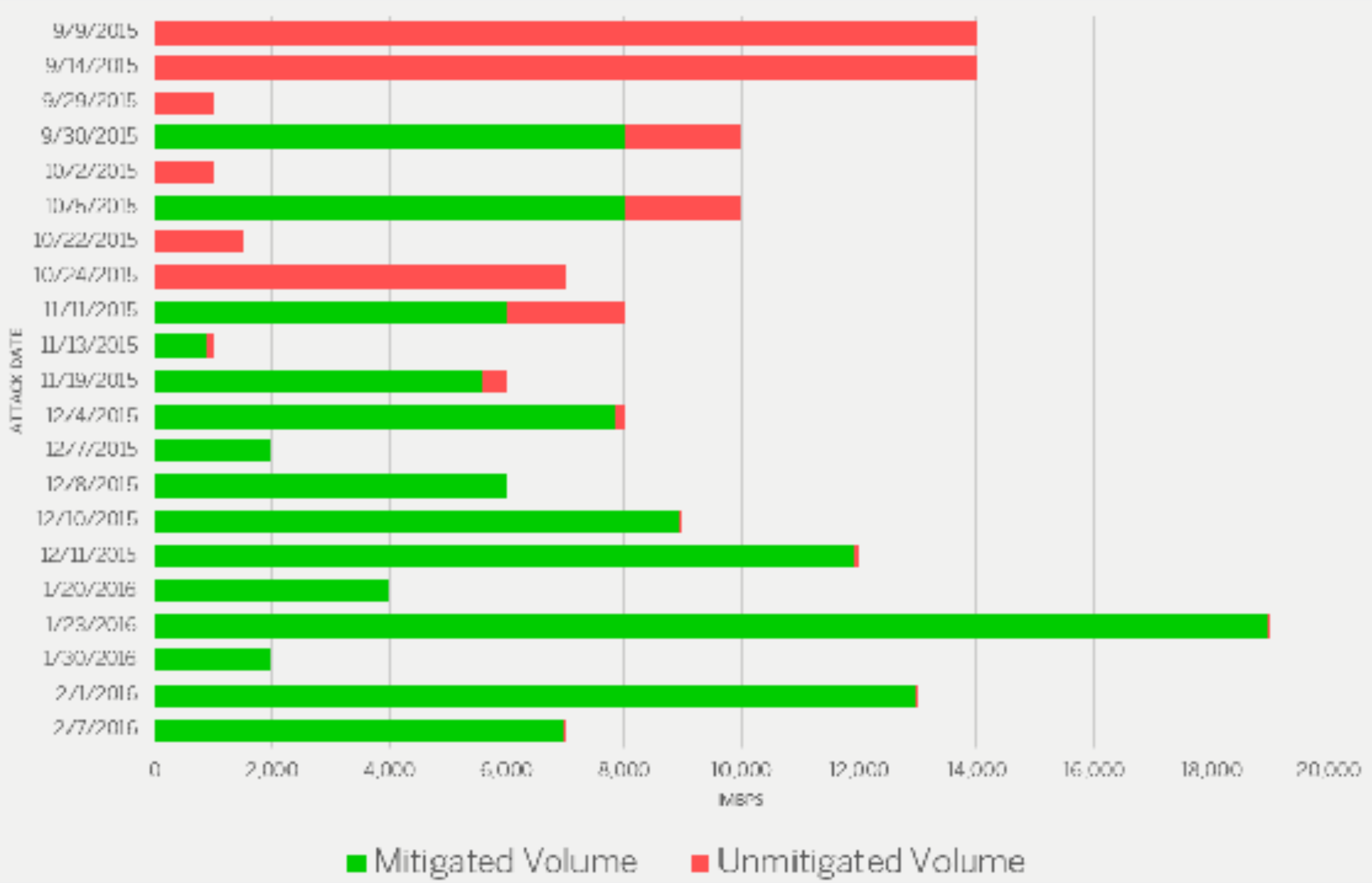
Basic DRDoS Mitigation / uRPF Overview

Seth Garrett, Principal Network Engineer
Indiana University Campus Networks

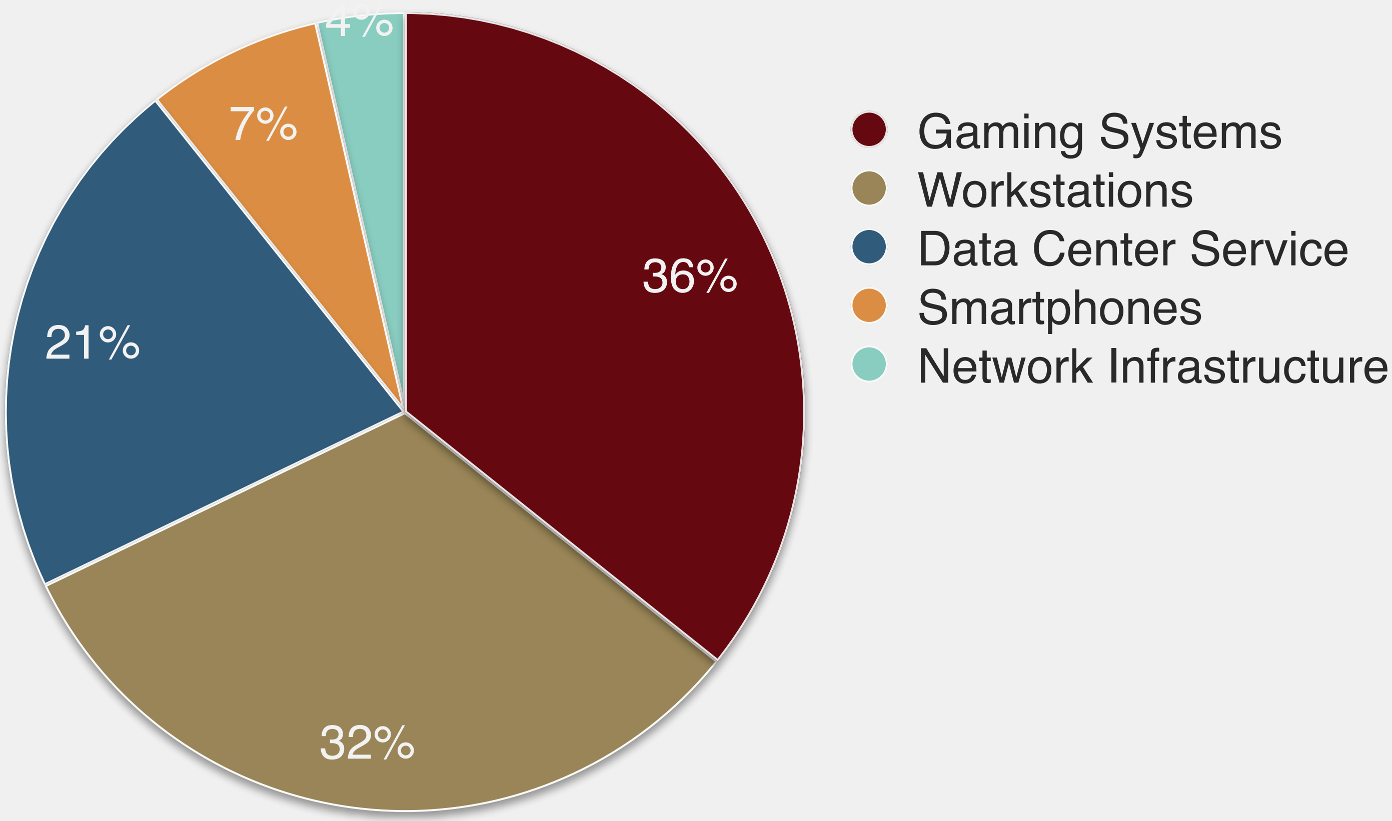
DRDoS Concern: Why?

- They are easy to launch.
- They utilize well known services.
- Most can be mitigated proactively.
  - Initial mitigation techniques can be effective, simple, and inexpensive.
  - Gain experience and improve understanding of DDoS in general.
- If you're not looking, you wont see them.
  - As a target or a source of an attack.

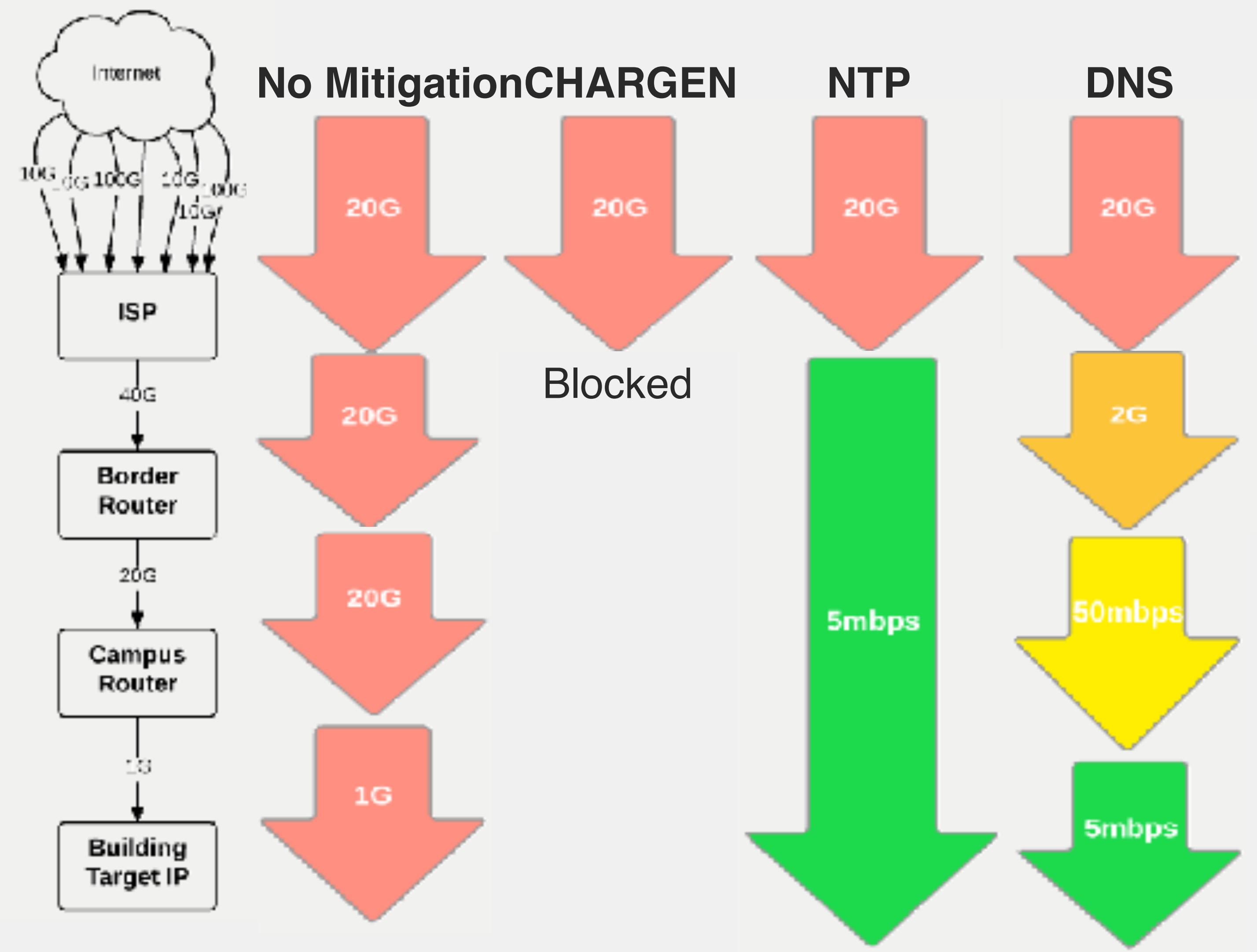
Recent Attack History



Recent Attack Targets



Areas of Mitigation Concern



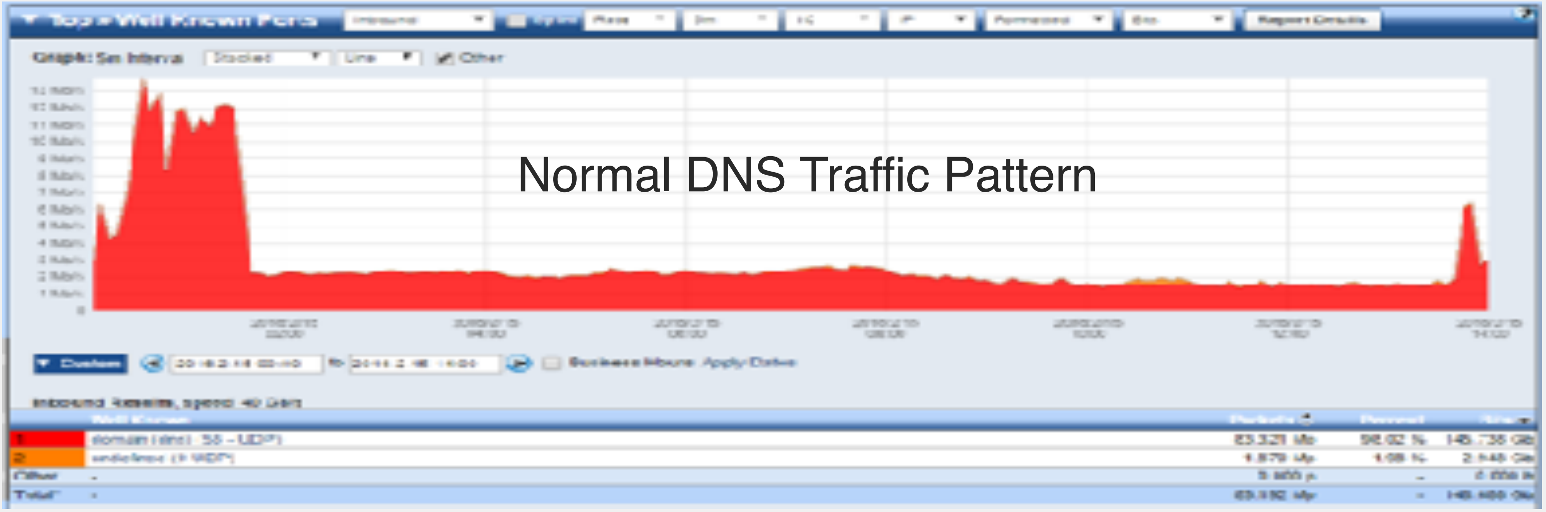
No Mitigation CHARGEN NTP DNS

Blocked

Traffic volume values are for demonstration purposes only.

Understand Your Traffic

Having a way to analyze your traffic patterns is critical to DDoS planning & de



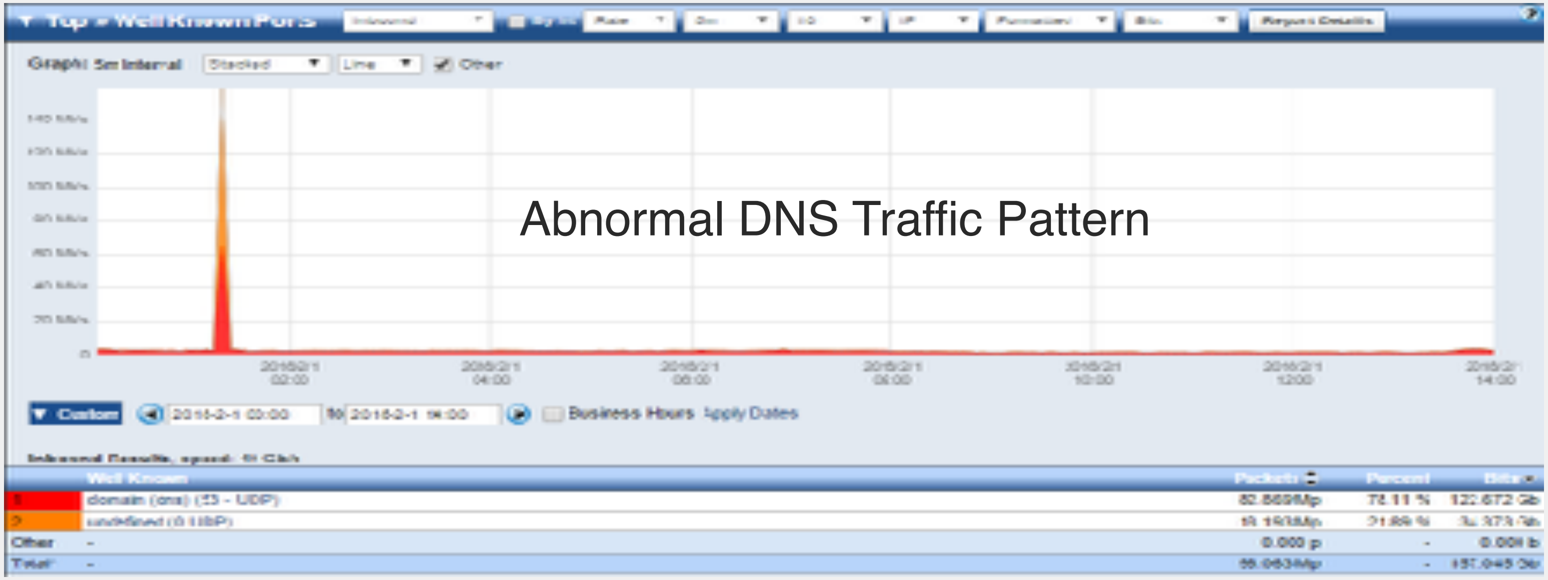
Graph: 5m Interval Stacked Line ☑ Other

Normal DNS Traffic Pattern

[illegible] to [illegible] □ Business Hours Apply Dates

Inbound Results, speed: 40 Gb/s

	Well Known	Packets	Percent	Bits
1	domain (dns) (53 – UDP)	83.321 Mp	98.02 %	145.735 Gb
2	undefined (0 UDP)	1.679 Mp	1.98 %	2.548 Gb
Other	-	0.000 p	-	0.000 b
Total	-	[illegible]	-	[illegible]



Graph: 5m Interval Stacked Line ☑ Other

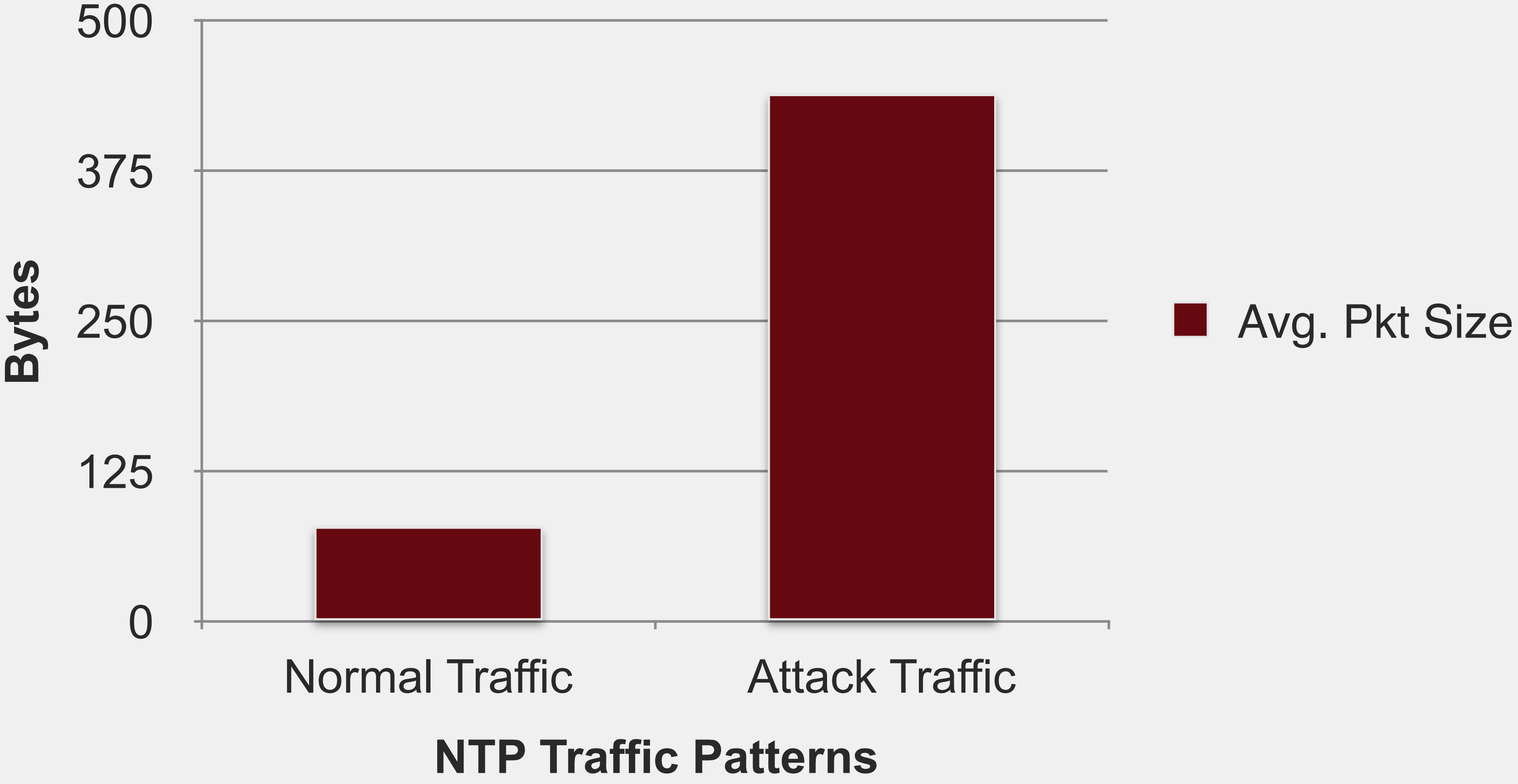
Abnormal DNS Traffic Pattern

2016-2-1 00:00 to 2016-2-1 14:00 □ Business Hours Apply Dates

Inbound Results, speed: 10 Gb/s

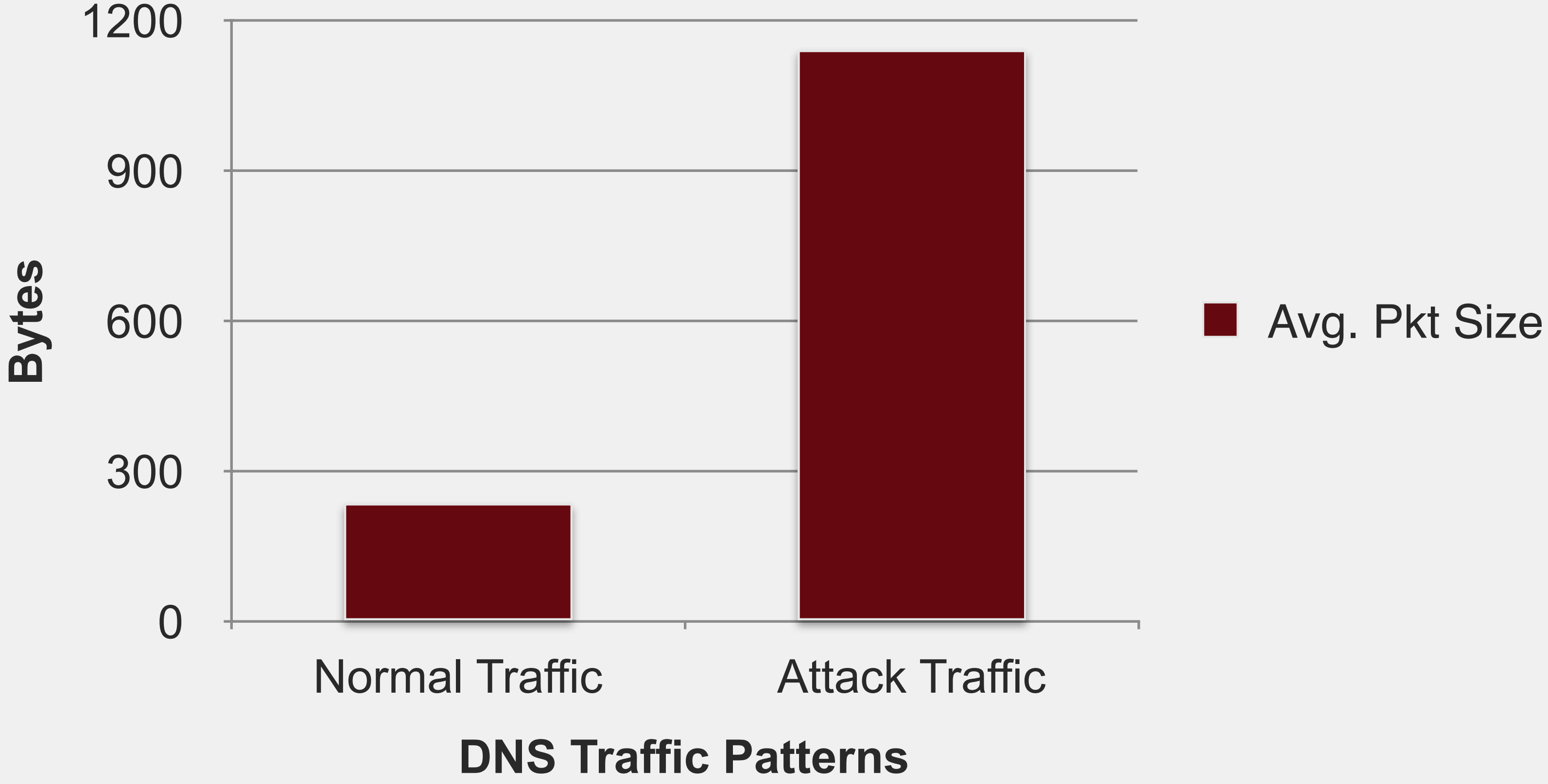
	Well Known	Packets	Percent	Bits
1	domain (dns) (53 - UDP)	82.869Mp	78.11 %	122.672 Gb
2	undefined (0 UDP)	18.193Mp	21.89 %	34.373 Gb
Other	-	0.000 p	-	0.000 b
Total	-	[illegible]	-	157.045 Gb

NTP DRDoS Traffic Patterns



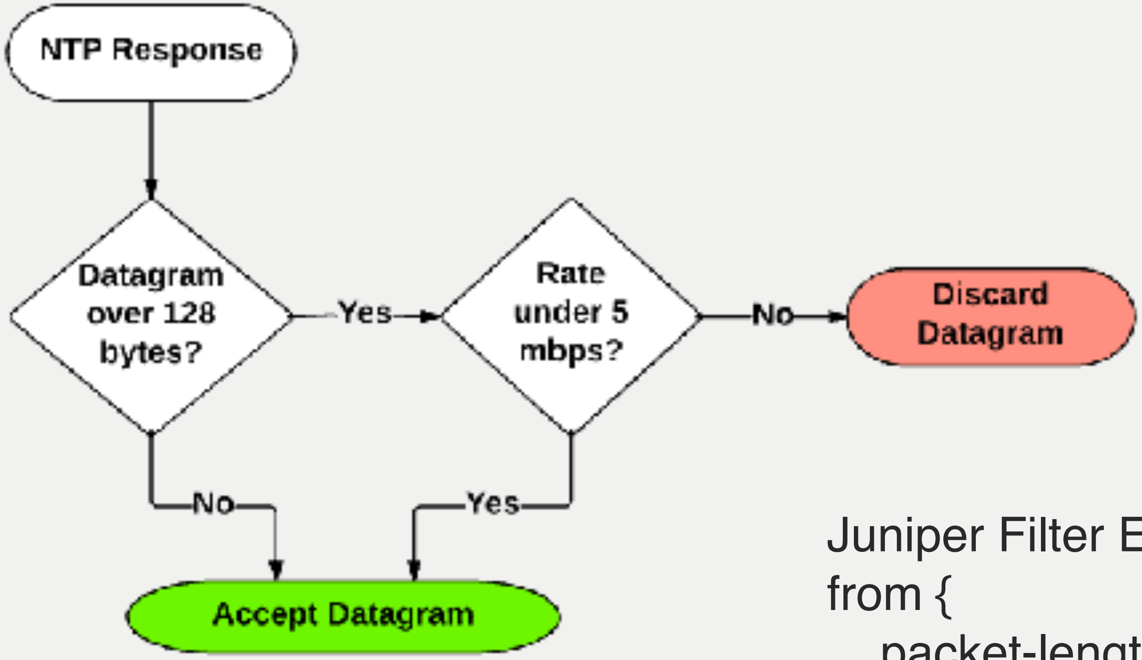
Data from real attacks since September 2015

DNS DRDoS Traffic Patterns



Data from real attacks since September 2015

Mitigate with Router Filters



Juniper Filter Example:

```
from {
    packet-length-except 0-128;
    protocol udp;
    port 123;
}
then {
    policer 5M-DROP;
    count POLICE-NTP;
    accept;
```

Using Multiple Policers

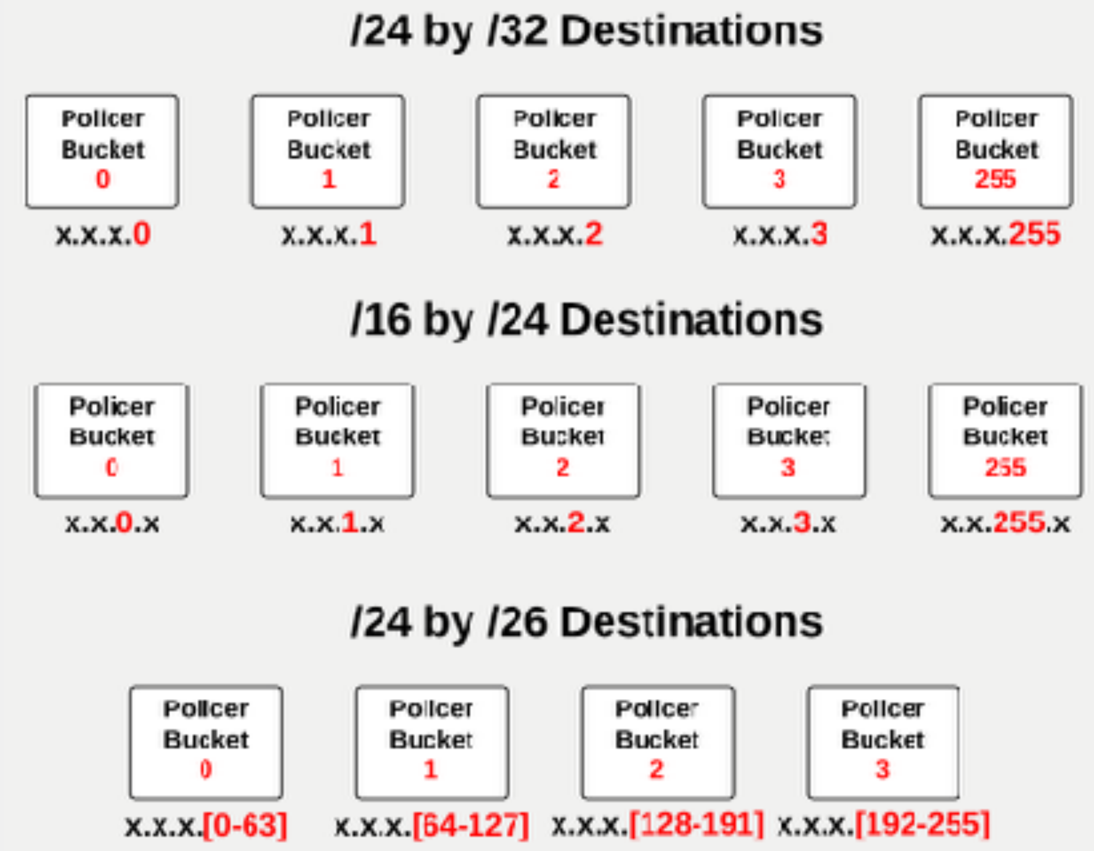
Setting a single limit for all matching traffic is not always ideal. Juniper’s prefix-action can be used to create thousands of policers for a single match term based off of the destination IP.

```
from {
    packet-length-except 0-128;
    protocol udp;
    port 123;
}
then {
    prefix-action DDOS-5M-PER-DESTINATION-24-32;
    accept;
```

```
prefix-action DDOS-5M-PER-DESTINATION-24-32;
        policer 5M-DROP;
        count;
        subnet-prefix-length 24;
        destination-prefix-length 32;
```

Prefix-Action Destination Breakdown

Prefix-actions create a large set of buckets that the destinations IPs are divided up into. Below are a few examples using different settings that shows how elements of the destination IP are used.



/24 by /32 Destinations

Policer Bucket 0 — x.x.x.0
Policer Bucket 1 — x.x.x.1
Policer Bucket 2 — x.x.x.2
Policer Bucket 3 — x.x.x.3
Policer Bucket 255 — x.x.x.255

/16 by /24 Destinations

Policer Bucket 0 — x.x.0.x
Policer Bucket 1 — x.x.1.x
Policer Bucket 2 — x.x.2.x
Policer Bucket 3 — x.x.3.x
Policer Bucket 255 — x.x.255.x

/24 by /26 Destinations

Policer Bucket 0 — x.x.x.[0-63]
Policer Bucket 1 — x.x.x.[64-127]
Policer Bucket 2 — x.x.x.[128-191]
Policer Bucket 3 — x.x.x.[192-255]

Suggested Mitigation Starting Point

Below are some suggestions to get you started with mitigating some of the common DRDoS attack types. Router filters can defeat most UDP based DRDoS attacks when combined with a thorough evaluation of your normal traffic patterns.

- **Rate Limit Based on Characteristics:**
  - **NTP (UDP 123)**
    - Recommendation: Rate limit NTP over 128 bytes. Most reflective DDoS attacks using NTP will have datagrams of 400 bytes or more. Legitimate NTP traffic often falls under 128 bytes.
  - **DNS (UDP 53) & IP Fragments**
    - Recommendation: Identify and make exceptions for legitimate DNS traffic to servers on your network. Rate limit all other DNS traffic. Apply limits for large sized datagrams separately from smaller sizes.
    - Reflective DDoS attacks using DNS will also be composed of IP fragments. These fragments will be a large portion of the attack. You should evaluate both your DNS and fragment traffic patterns to determine the proper rate limits.
- **Block if you can:**
  - **SSDP (UDP 1900)**
  - **RIPv1 (UDP 520)**
  - **NETBIOS (UDP 137)**
  - **SNMP (UDP 161)**
  - **CHARGEN (UDP 19)**
  - **RPC Portmapper (UDP 111)**

*If you cannot block then rate limit and/or whitelist good traffic patterns.

Other Mitigation Considerations

- Vendor Solutions
- FlowSpec
- RTBH & S/RTBH
- Quagga & ExaBGP
- <Insert detection methods here>
- Relationship with your ISP
- Your ISP's Relationships
- Make time for DDoS

uRPF Overview

- Unicast Reverse Path Forwarding
- Source IP Verification
- Helps Prevent IP Spoofing
- Requires thoughtful design implementation
- Friends don’t let friends run networks without using use uRPF when possible.
- uRPF uses more memory on the routers.

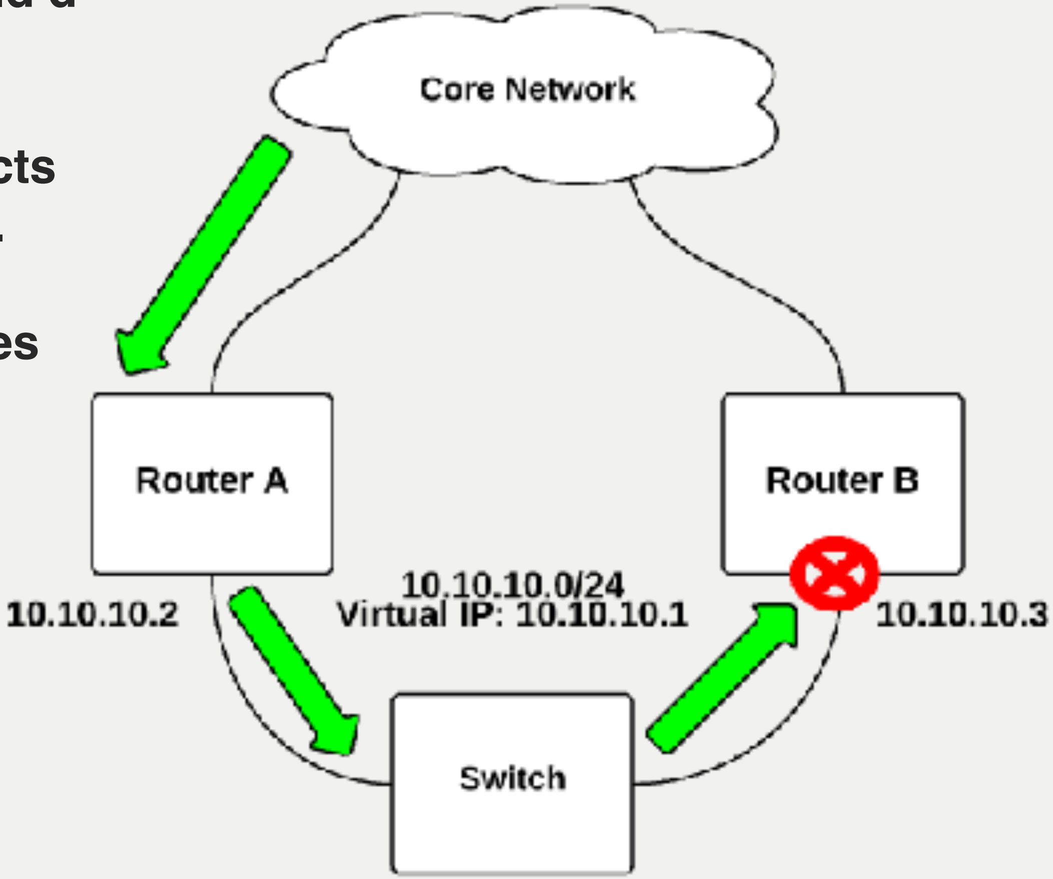
Strict Mode

- The source IP must be the best path for the route on that interface.
- Most useful at the edge of your networks.
- Asymmetric traffic patterns do not get along with uRPF in strict mode.
- Can be used on dual-homed networks with design considerations.
- DHCP requests from 0.0.0.0 must have an exception granted to pass RPF.
- Can be combined with a feasible-paths option to be more ISP friendly for multi-homed customers.

Dual-Home Scenario: Interface IPs

- **Interface IPs as destinations can enter via the dual-homed peer router.**
- **uRPF in strict mode would d traffic entering Router B because of the source IP 192.168.0.1. It only expects 10.10.10.0/24 IPs ingress.**
- **Areas of concern:**
  - **DHCP relay responses**
  - **Pings**

Source IP: 192.168.0.1
Destination: 10.10.10.3



Loose Mode

- The source IP only has to be in the FIB. Does not have to source on the active path.
- Useful or asymmetric traffic patterns.
- Can be used to create a S/RTBH setup.
- May not respect a default route. Can be different even between vendor cards.

Loose Mode Internet + RTBH

Router C & D

- Have full BGP table
- uRPF loose mode on uplinks
- Installs RTBH routes as discard.
- Has rpf-loose-mode-discard configured

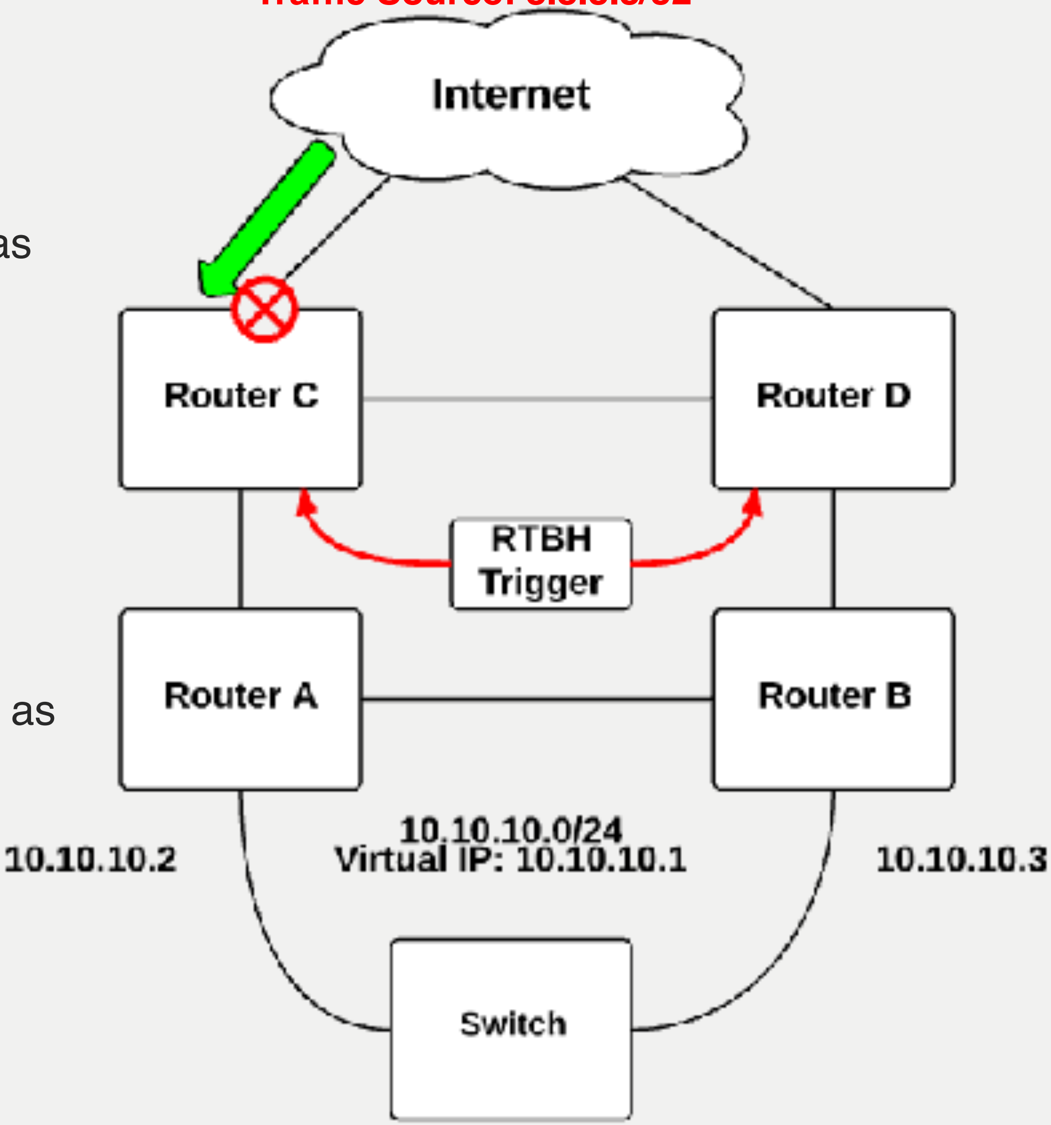
RTBH Trigger

- Advertising routers:
  - 8.8.8.8/32

Result

- 8.8.8.8 traffic dropped as a source IP
- S/RTBH

Traffic Source: 8.8.8.8/32



RTBH + Strict Mode: Internal Source

Router C

- Installs RTBH routes as discard.
- Advertises RTBH routes to Router A

Router A

- Has RPF strict mode running on edge.

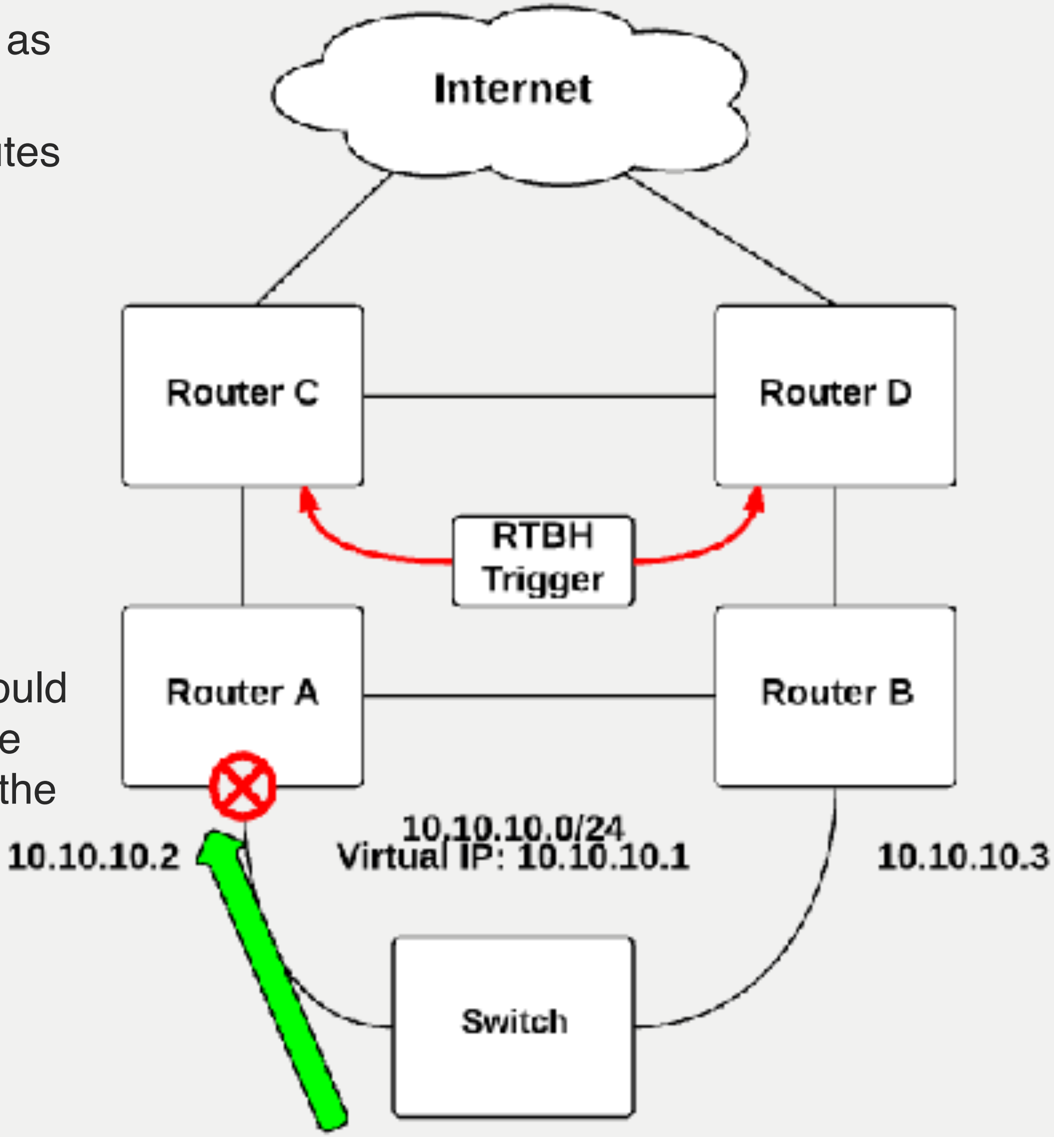
RTBH Trigger

- Advertising routers:
  - 10.10.10.10/32

Result

- 10.10.10.10 traffic would be dropped due to the active path being on the Router C path.

Traffic Source: 10.10.10.10/32



Junos Fail-Filter

- **Junos has an optional fail-filter for RPF check. You can run all traffic failing RPF through a user created filter to grant RPF exceptions.**

```
term ALLOW-DHCP-BOOTP {
    from {
        source-address {
            0.0.0.0/32;
        }
        destination-address {
            255.255.255.255/32;
        }
    }
    then {
        count RPF-DHCP-BOOTP-TRAFFIC;
        accept;
    }
}
term ALLOW-DHCP-SERVERS {
    from {
        source-prefix-list {
            DHCP-SERVERS;
        }
    }
    then {
        count ALLOW-DHCP-SERVERS;
        accept;
    }
}
term DENY-ALL {
    then {
        discard;
```