Community tools to fight against DDoS

Fakrul Alam
Senior Training Officer

SANOG 27 & APNIC Regional Meeting, Kathmandu, Nepal
25 Jan - 01 Feb, 2016

Issue Date: 26-12-2015
Revision: 1.3

APNIC

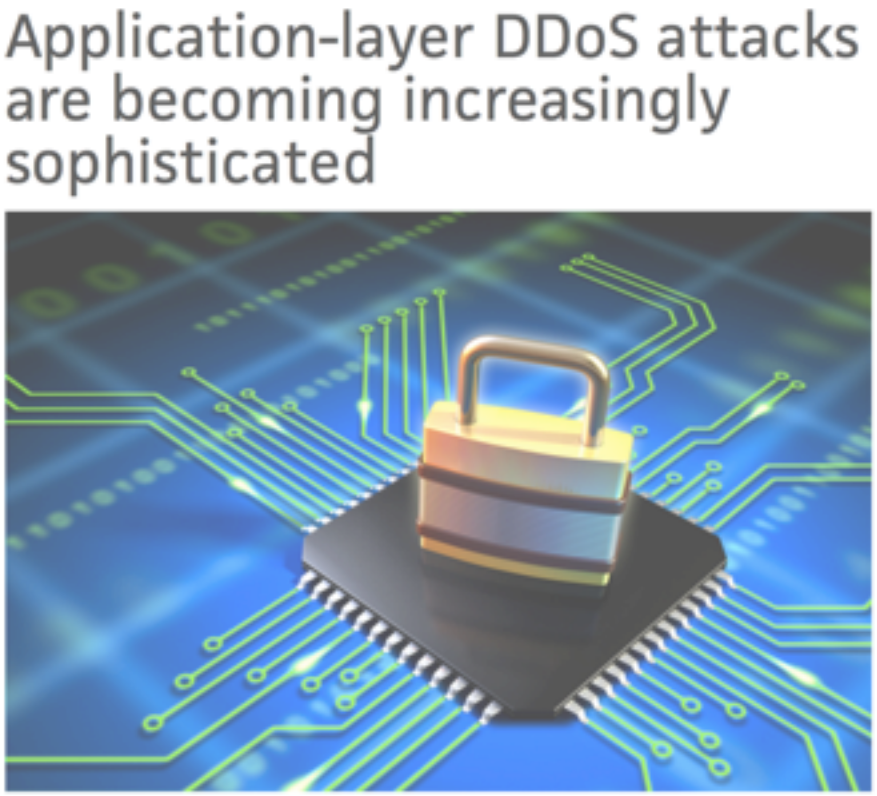
DDoS

- Denial of Service (DoS) / Distributed Denial of Service (DDoS) is the act of
  - performing an attack which prevents the system from providing services to legitimate users
- Denial of Service attacks take many forms, and utilize many attack vectors
- Used to cover up other attack vectors

Types of Attacks

- Volume Based Attacks
- Application Layer Attacks

http://thehackernews.com/2016/01/biggest-ddos-attack.html



Addressing DDoS attacks

- Preparation
  - Deploy necessary tools and grab list
- Detection
  - Detect incoming fake requests
- Mitigation
  - Diversion : Send traffic to a specialized device that removes the fake packets from the traffic stream while retaining the legitimate packets
  - Return : Send back the clean traffic to the server

3 Community tools

- Bogon Filter
  - https://www.team-cymru.org/bogon-reference.html
- Flow Sonar
  - https://www.team-cymru.org/Flow-Sonar.html
- UTRS (Unwanted Traffic Removal Service)
  - https://www.team-cymru.org/UTRS/index.html

1. Bogon Filter

Bogon Filter

- A bogon prefix is a route that should never appear in the Internet routing table
  - Bogons are defined as Martians (private and reserved addresses defined by RFC 1918, RFC 5735, and RFC 6598) and netblocks that have not been allocated to a RIR by the IANA
- These are commonly found as the source addresses of DDoS attacks
- Study shows 60% of the naughty packets were obvious bogons
- Bogon and fullbogon lists are NOT static lists

Bogon Filter : Configuration IPv4

```
router bgp 17821
 neighbor 38.229.xxx.xxx remote-as 65332
 neighbor 38.229.xxx.xxx description CYMRUBOGONS
 neighbor 38.229.xxx.xxx ebgp-multihop 255
 neighbor 38.229.xxx.xxx password 7 070C134D575F0A5116
 neighbor 38.229.xxx.xxx update-source Loopback0
 !
 address-family ipv4
  neighbor 38.229.xxx.xxx activate
  neighbor 38.229.xxx.xxx soft-reconfiguration inbound
  neighbor 38.229.xxx.xxx prefix-list CYMRU-OUT-V4 out
  neighbor 38.229.xxx.xxx route-map CYMRUBOGONS-V4 in
 !
!configure community list to accept the bogon prefixes into the route-map
ip community-list 100 permit 65332:17821
!
!configure route-map. Remember to apply it to the proper peering sessions.
route-map CYMRUBOGONS-V4 permit 10
 description IPv4 Filter bogons learned from cymru.com bogon route-servers
 match community 100
 set ip next-hop 192.0.2.1
!
!set a bogon next-hop on all routers that receive the bogons
ip route 192.0.2.1 255.255.255.255 Null0
!
ip prefix-list CYMRU-OUT-V4 seq 5 deny 0.0.0.0/0 le 32
```

Bogon Filter : Configuration IPv6

```
router bgp 17821
 neighbor 2620:0:6B0::xxxx:xxxx remote-as 65332
 neighbor 2620:0:6B0::xxxx:xxxx description CYMRUBOGONS
 neighbor 2620:0:6B0::xxxx:xxxx ebgp-multihop 255
 neighbor 2620:0:6B0::xxxx:xxxx password 7 0458390716775F1A08
 neighbor 2620:0:6B0::xxxx:xxxx update-source Loopback0
 !
 address-family ipv6
  neighbor 2620:0:6B0::xxxx:xxxx activate
  neighbor 2620:0:6B0::xxxx:xxxx soft-reconfiguration inbound
  neighbor 2620:0:6B0::xxxx:xxxx prefix-list CYMRU-OUT-V6 out
  neighbor 2620:0:6B0::xxxx:xxxx route-map CYMRUBOGONS-V6 in
!
!configure community list to accept the bogon prefixes into the route-map
ip community-list 100 permit 65332:17821
!
!configure route-map. Remember to apply it to the proper peering sessions.
route-map CYMRUBOGONS-V6 permit 10
 description IPv6 Filter bogons learned from cymru.com bogon route-servers
 match community 100
 set ipv6 next-hop 2001:DB8:0:DEAD:BEEF::1
!
!set a bogon next-hop on all routers that receive the bogons
ipv6 route 2001:DB8:0:DEAD:BEEF::1/128 Null0
!
ipv6 prefix-list CYMRU-OUT-V6 seq 5 deny ::/0 le 128
```

Bogon Filter : Output

```
APNIC-Training-Lab01#show ip bgp 31.22.8.0/21
BGP routing table entry for 31.22.8.0/21, version 175332535
Paths: (1 available, best #1, table default, not advertised
to EBGP peer)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  65332, (received & used)
    192.0.2.1 from 38.229.66.20 (38.229.66.20)
      Origin IGP, localpref 100, valid, external, best
      Community: 65332:17821 no-export
      rx pathid: 0, tx pathid: 0x0
```

Bogon Filter : Status

- The IPv4 fullbogons list is approximately 3,714 prefixes.
  - [date : 26th January, 2016]

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
38.229.xxx.xxx    4        65332   12017   12017 186072391    0
0 1w0d         3733
```

- The IPv6 fullbogons list is approximately 65,788 prefixes.
  - [date : 26th January, 2016]

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
2404:A800:xxxx:xx::xxxx
                4         9498 3239994   72131 40075514    0    0
3w1d        65788
```

Bogon Filter : Peering

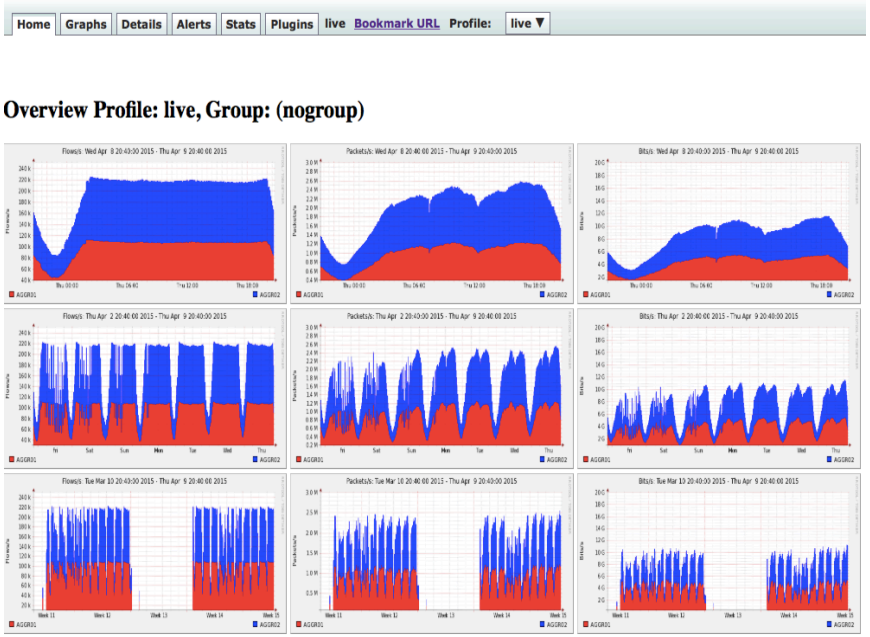
- Contact bogonrs@cymru.com
  1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4 fullbogons, and/or IPv6 fullbogons)
  2. Your AS number
  3. The IP address(es) you want us to peer with
  4. Does your equipment support MD5 passwords for BGP sessions?
  5. Optional: your GPG/PGP public key
- https://www.team-cymru.org/bogon-reference-bgp.html

2. Flow Sonar

Flow Sonar

- The Team Cymru Flow Sonar system is a powerful tool for network managers to visually identify and understand what is happening on their network at any given time
- Leveraging the free and open-source framework provided by Peter Haag of SWITCH
- Special plugins "dosrannu" developed by Team Cymru to track malicious activity on your network
- Unique dosrannu feeds alerted to DDoS attacks, compromised machines, and the presence of connections to C&C hosts

Flow Sonar



Flow Stats

icmp trend is 99.87% (down) | tcp trend is 95.71% (down) | udp trend is 97.85% (down)

timestamp	icmp flows	icmp % diff	tcp flows	tcp % diff	udp flows	udp % diff
2015-04-09 20:35:00	1646735	99.12%	38134875	94.66%	12262785	97.83%
2015-04-09 20:30:00	1661393	99.1%	40287852	95.49%	12534361	94.89%
2015-04-09 20:25:00	1676511	97.2%	42190036	94.08%	13209615	96.85%
2015-04-09 20:20:00	1724813	100.45%	44845575	96.22%	13639839	99.02%
2015-04-09 20:15:00	1717073	104.76%	46606550	99.78%	13775167	102.24%
2015-04-09 20:10:00	1639111	98.62%	46708743	94.03%	13472789	96.29%

Latest Flow Alerts

Latest Flow Alerts

timestamp	count	src ip	src port	dst ip	dst port	protocol	alert source	type
2015-04-09 20:55:01	4	***202.59.132.4**	33356	113.107.239.158	8080	6	ip reputation	proxy
2015-04-09 20:55:01	4	***116.193.217.35**	8080	100.43.160.132	1425	6	ip reputation	proxy
2015-04-09 20:55:01	8	103.243.222.100	80	***116.193.217.35**	60689	6	ip reputation	proxy
2015-04-09 20:55:01	4	113.107.239.163	8081	***202.59.132.4**	49278	6	ip reputation	proxy
2015-04-09 20:55:01	4	183.61.179.151	8081	***202.59.132.4**	46173	6	ip reputation	proxy
2015-04-09 20:55:01	4	100.43.169.4	3619	***116.193.217.35**	8080	6	ip reputation	proxy
2015-04-09 20:55:01	8	61.160.207.170	55142	***202.59.132.4**	8080	6	ip reputation	proxy
2015-04-09 20:55:01	4	100.43.132.148	2076	***116.193.217.35**	8080	6	ip reputation	proxy
2015-04-09 20:55:01	4	***116.193.217.35**	8080	100.43.161.12	1079	6	ip reputation	proxy
2015-04-09 20:55:01	4	***116.193.217.35**	58642	61.57.227.181	80	6	ip reputation	proxy
2015-04-09 20:55:01	4	***116.68.199.110**	36293	122.225.38.197	81	6	ip reputation	proxy
2015-04-09 20:55:01	4	***116.193.217.35**	8080	79.141.173.52	51093	6	ip reputation	proxy
2015-04-09 20:55:01	4	60.169.77.106	62030	***115.127.26.1**	8080	6	ip reputation	proxy
2015-04-09 20:55:01	28	***202.191.122.250**	8080	222.186.26.34	13109	6	ip reputation	proxy
2015-04-09 20:55:01	12	61.160.207.204	16502	***115.127.26.3**	8080	6	ip reputation	proxy
2015-04-09 20:55:01	8	61.160.6.105	16991	***202.59.132.4**	8080	6	ip reputation	proxy
2015-04-09 20:55:01	8	***202.59.132.4**	8080	60.169.77.116	16040	6	ip reputation	proxy
2015-04-09 20:55:01	4	***202.59.132.4**	8080	222.186.26.34	58493	6	ip reputation	proxy
2015-04-09 20:55:01	4	120.195.155.69	801	***202.59.132.4**	48362	6	ip reputation	proxy

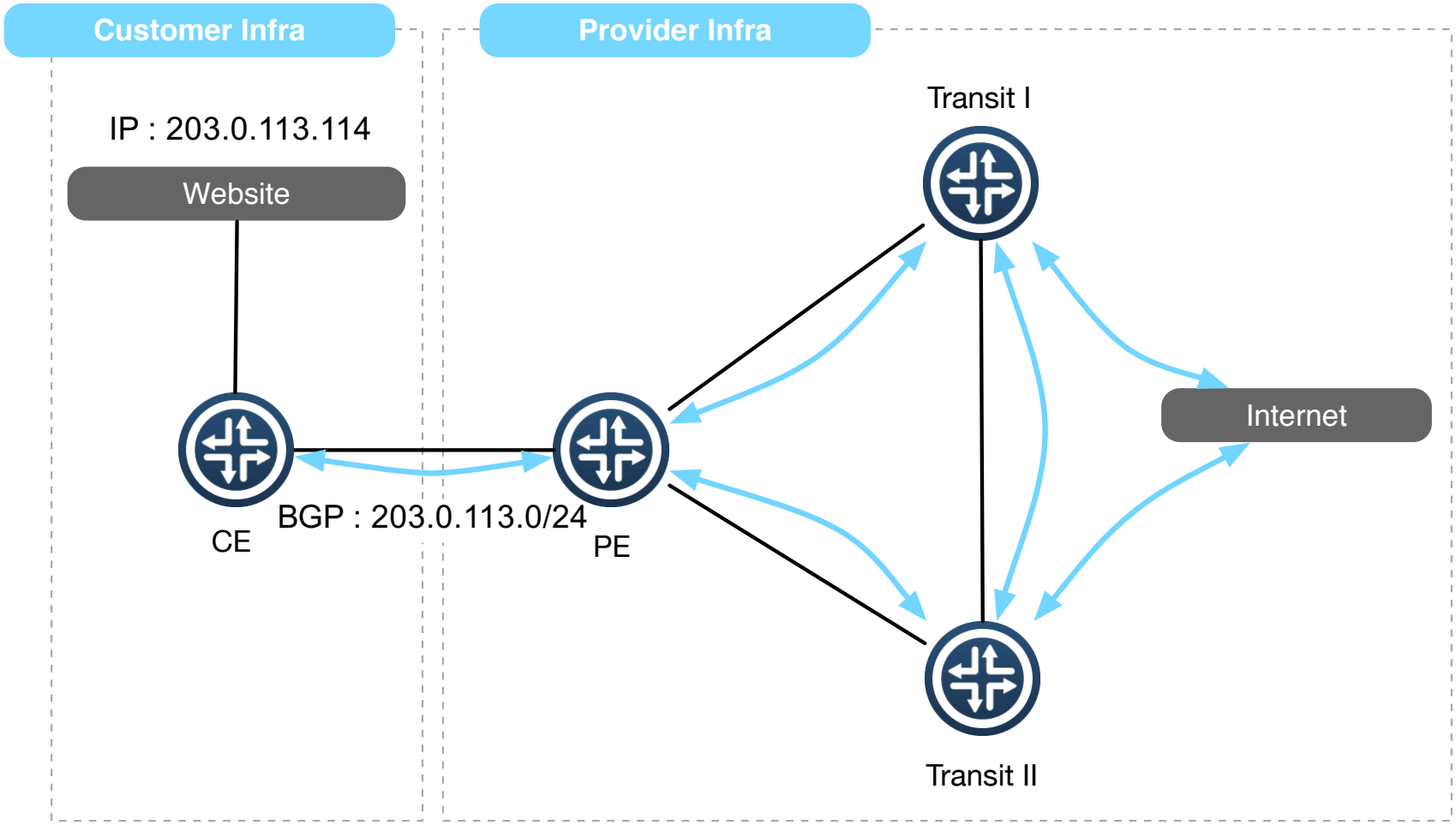
It's nfsens/nfdump!!!

Flow Sonar : Get It

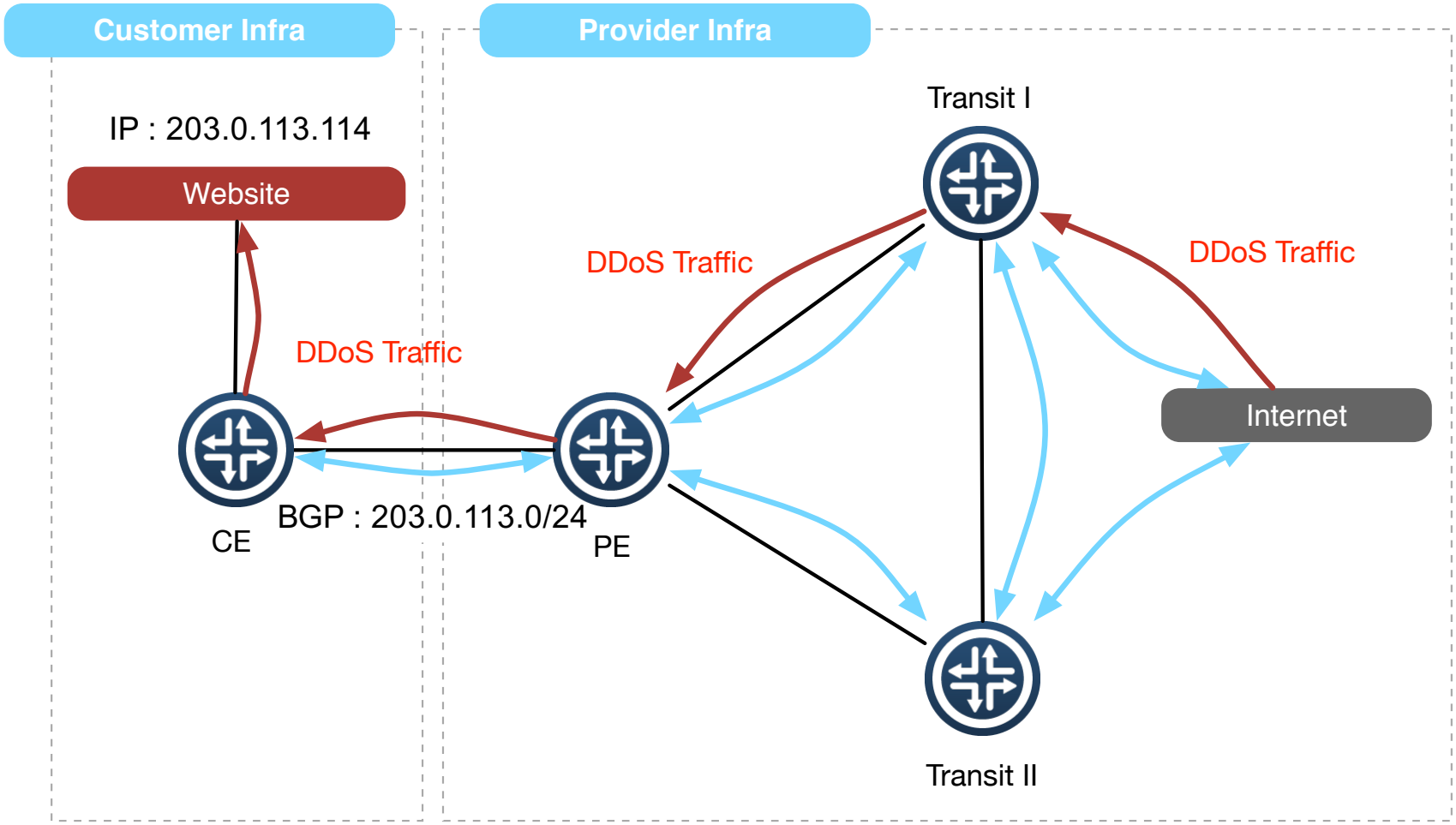
- Contact outreach@cymru.com
  1. Team Cymru will send hardware
     - 1 Server
     - 1 Router
- https://www.team-cymru.org/Flow-Sonar.html

3. UTRS (Unwanted Traffic Removal Service)

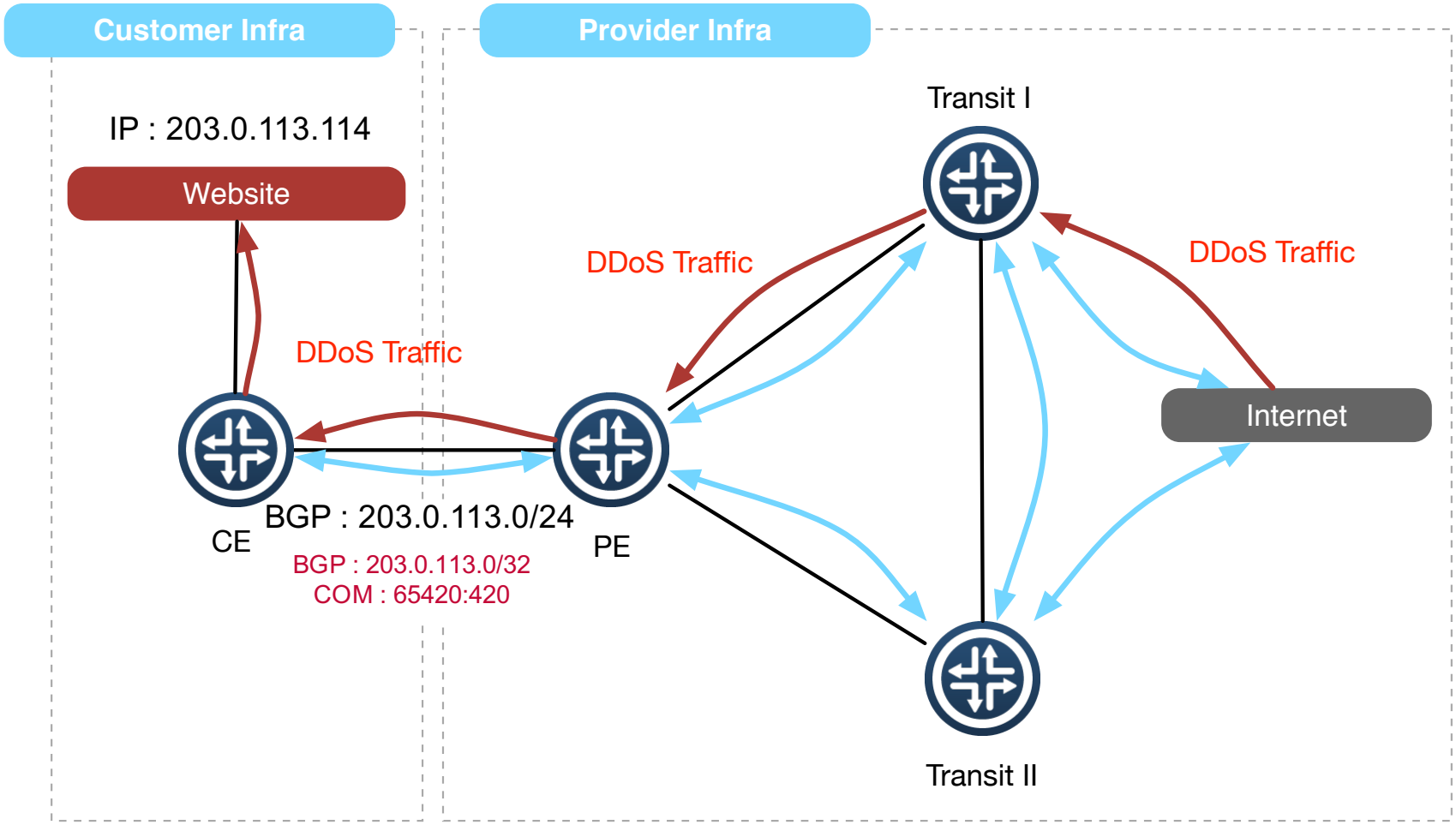
RTBH 101


Customer Infra
Provider Infra
IP : 203.0.113.114
Website
Transit I
Internet
CE
BGP : 203.0.113.0/24
PE
Transit II

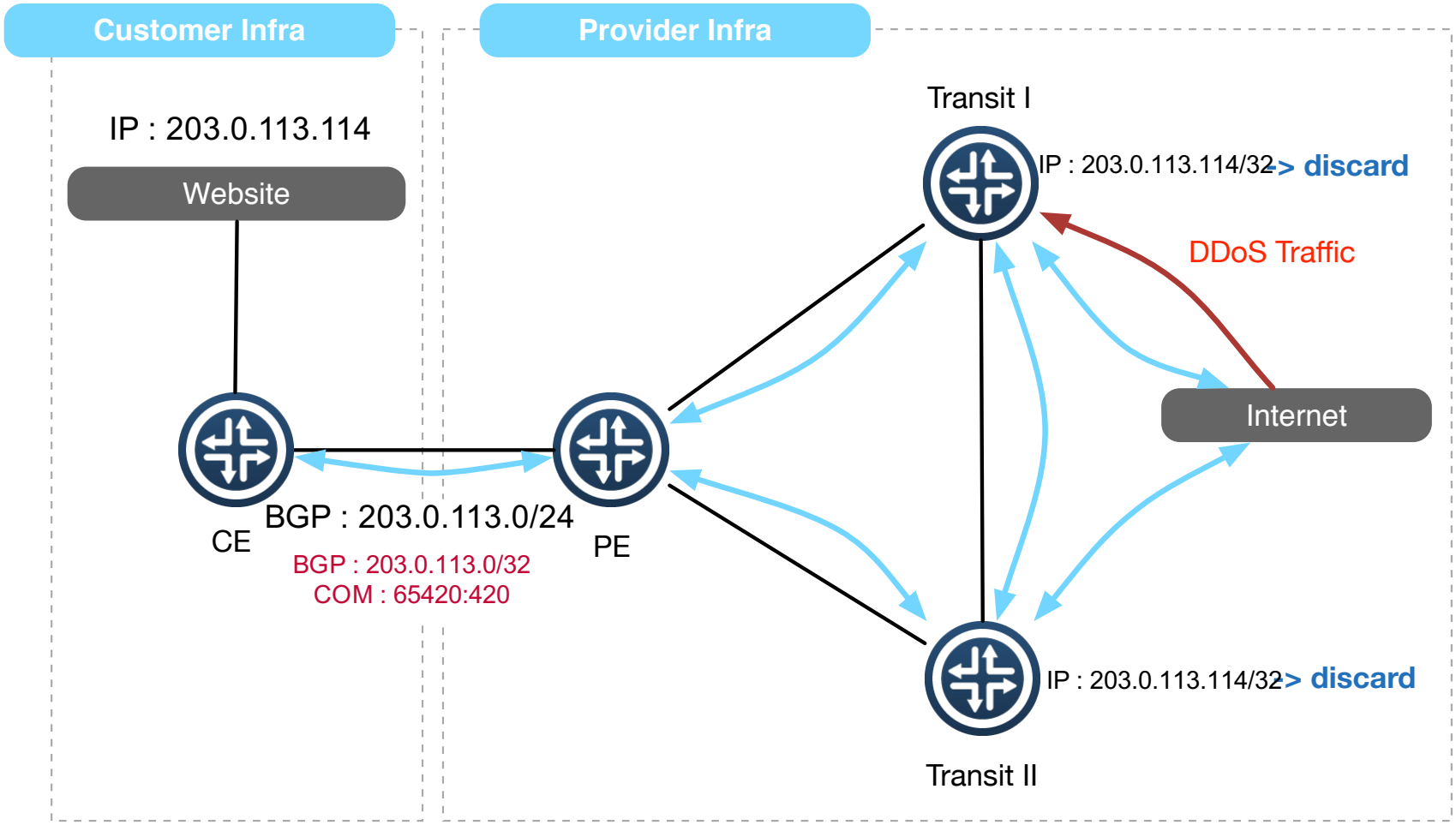
RTBH 101


Customer Infra
Provider Infra
IP : 203.0.113.114
Website
Transit I
DDoS Traffic
DDoS Traffic
DDoS Traffic
Internet
CE
BGP : 203.0.113.0/24
PE
Transit II

RTBH 101


Customer Infra
Provider Infra
IP : 203.0.113.114
Website
Transit I
DDoS Traffic
DDoS Traffic
DDoS Traffic
Internet
CE
BGP : 203.0.113.0/24
PE
BGP : 203.0.113.0/32
COM : 65420:420
Transit II

RTBH 101


Customer Infra
Provider Infra
IP : 203.0.113.114
Website
Transit I
IP : 203.0.113.114/32
> discard
DDoS Traffic
Internet
CE
BGP : 203.0.113.0/24
BGP : 203.0.113.0/32
COM : 65420:420
PE
IP : 203.0.113.114/32
> discard
Transit II

RTBH Upstream

- Check whether your upsteam provider support RTBH
- Configure & Test RTBH before incident
- Only announce IPv4 /32's from address space you originate or your customer

UTRS

- It's based on the basic principle of DDoS filtering; Remotely Triggered Black Hole Filtering
- UTRS is a system that helps mitigate large infrastructure attacks by leveraging:
  - an existing network of cooperating BGP speakers such as ISPs, hosting providers and educational institutions
  - that automatically distributes verified BGP-based filter rules from victim to cooperating networks

UTRS : Configuration

```
router bgp 17821
 neighbor 154.35.xxx.xxx remote-as 64496
 neighbor 154.35.xxx.xxx description CYMRUBOGONS-UTRS
 neighbor 154.35.xxx.xxx ebgp-multihop 255
 neighbor 154.35.xxx.xxx transport connection-mode passive
 neighbor 154.35.xxx.xxx password 7 xxxxxxxxxxxxxxxxxxxxx
 neighbor 154.35.xxx.xxx update-source Loopback0
 !
address-family ipv4
  neighbor 154.35.xxx.xxx activate
  neighbor 154.35.xxx.xxx send-community
  neighbor 154.35.xxx.xxx soft-reconfiguration inbound
  neighbor 154.35.xxx.xxx route-map UTRS-OUT out
  neighbor 154.35.xxx.xxx route-map UTRS-IN in
!
access-list 1 remark utility ACL to deny everything
access-list 1 deny any
!
ip prefix-list 32-only permit 0.0.0.0/0 ge 32
ip community-list standard RTBH permit 17821:0
!
route-map UTRS-IN permit 10
   match ip address prefix-list 32-only
route-map UTRS-IN deny 100
   match ip address 1
!
route-map UTRS-OUT permit 10
   match ip address prefix-list 32-only
   match community RTBH
route-map UTRS-OUT deny 100
   match ip address 1
```

```
ip route 203.176.189.10 255.255.255.255 null0
```

UTRS : Apply

- Newly launched service
  - Quite picky to choose whom to peer
  - Do organization verification
- https://www.team-cymru.org/UTRS/index.html
- FAQ:
  - https://www.cymru.com/jtk/misc/utrs.html

How UTRS varies from RTBH with upstream!

APNIC

Other Efforts

- NANOG BCOP : DDoS-DoS-attack-BCOP
  - http://bcop.nanog.org/index.php/DDoS-DoS-attack-BCOP
- Routing Resilience Manifesto
  - Mutually Agreed Norms for Routing Security (MANRS)
  - https://www.routingmanifesto.org/manrs/


KEEP
CALM
IT'S
JUST A
DDOS

Questions!