Community tools to fight against DDoS

Fakrul Alam
fakrul@apnic.net

BKNIX Peering Forum

15-16 May 2017, Bangkok

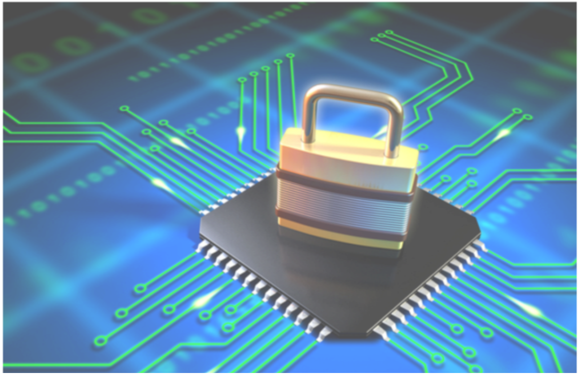
DDoS

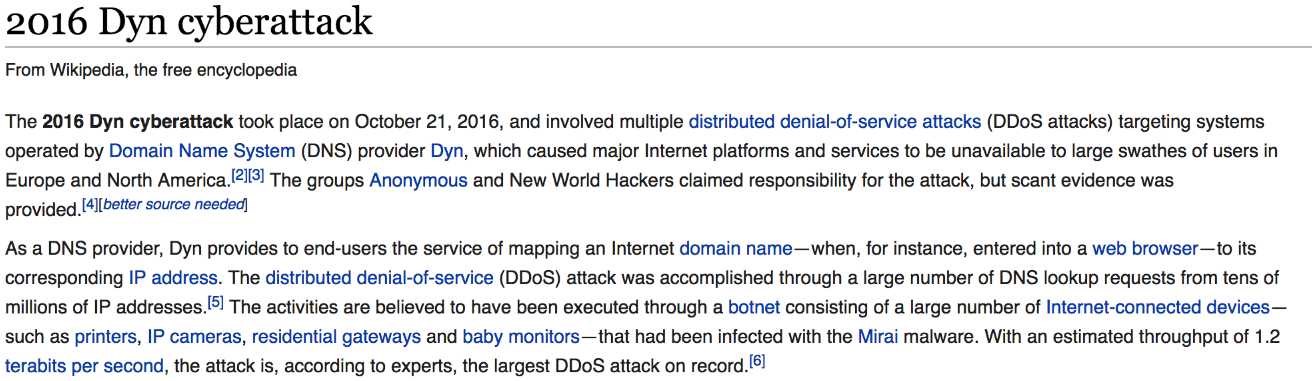
- Denial of Service (DoS) / Distributed Denial of Service (DDoS) is the act of
  - performing an attack which prevents the system from providing services to legitimate users
- Denial of Service attacks take many forms, and utilize many attack vectors
- Used to cover up other attack vectors

Types of Attacks

- Volume Based Attacks
- Application Layer Attacks

Application-layer DDoS attacks are becoming increasingly sophisticated





2016 Dyn cyberattack

From Wikipedia, the free encyclopedia

The **2016 Dyn cyberattack** took place on October 21, 2016, and involved multiple distributed denial-of-service attacks (DDoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn, which caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America.[2][3] The groups Anonymous and New World Hackers claimed responsibility for the attack, but scant evidence was provided.[4][*better source needed*]

As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name—when, for instance, entered into a web browser—to its corresponding IP address. The distributed denial-of-service (DDoS) attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses.[5] The activities are believed to have been executed through a botnet consisting of a large number of Internet-connected devices—such as printers, IP cameras, residential gateways and baby monitors—that had been infected with the Mirai malware. With an estimated throughput of 1.2 terabits per second, the attack is, according to experts, the largest DDoS attack on record.[6]

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 5
 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 5
 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 3,803 prefixes.
  - [date : 10th May 2017]

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
38.229.xxx.xxx    4        65332   12017   12017 186072391    0    0
1w0d         3803
```

- The IPv6 fullbogons list is approximately 84,908 prefixes.
  - [date : 10th May 2017]

```
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
84908
```

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

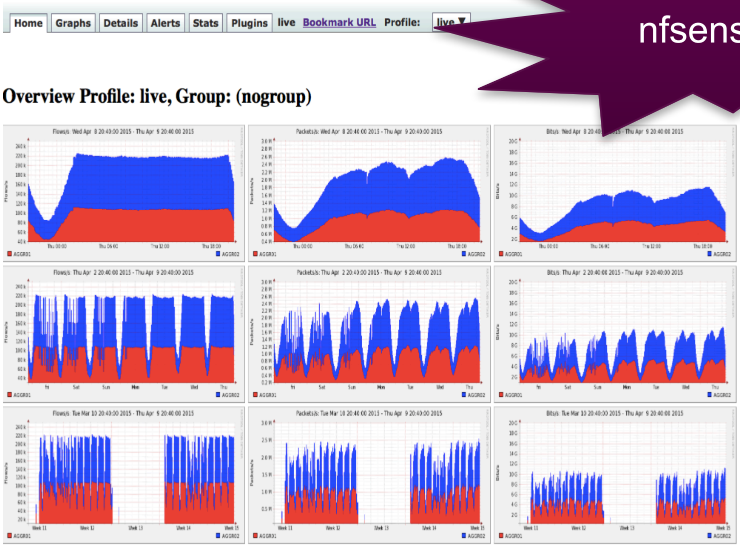
2. Flow Sonar

Flow Sonar

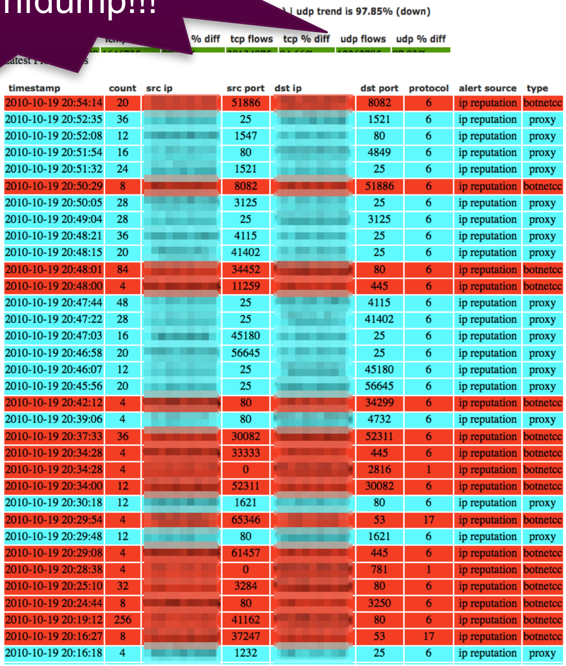
- The Team Cymru Flow Sonar system is a powerful tool for network managers to visually identify and understand what is happening on their network at any given time
- Leveraging the free and open-source framework provided by Peter Haag of SWITCH
- Special plugins "dosrannu" developed by Team Cymru to 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

It’s nfsens/nfdump!!!


Home
Graphs
Details
Alerts
Stats
Plugins
live
Bookmark URL
Profile:
live ▼
Flows/s: Wed Apr 8 20:40:00 2015 - Thu Apr 9 20:40:00 2015
Packets/s: Wed Apr 8 20:40:00 2015 - Thu Apr 9 20:40:00 2015
Bits/s: Wed Apr 8 20:40
Flows/s: Thu Apr 2 20:40:00 2015 - Thu Apr 9 20:40:00 2015
Packets/s: Thu Apr 2 20:40:00 2015 - Thu Apr 9 20:40:00 2015
Bits/s: Thu Apr 2 20:40:00 2015 - Thu Apr 9 20:40:00 2015
Flows/s: Tue Mar 10 20:40:00 2015 - Thu Apr 9 20:40:00 2015
Packets/s: Tue Mar 10 20:40:00 2015 - Thu Apr 9 20:40:00 2015
Bits/s: Tue Mar 10 20:40:00 2015 - Thu Apr 9 20:40:00 2015
AGGR01
AGGR02

Overview Profile: live, Group: (nogroup)



| udp trend is 97.85% (down)

% diff tcp flows tcp % diff udp flows udp % diff

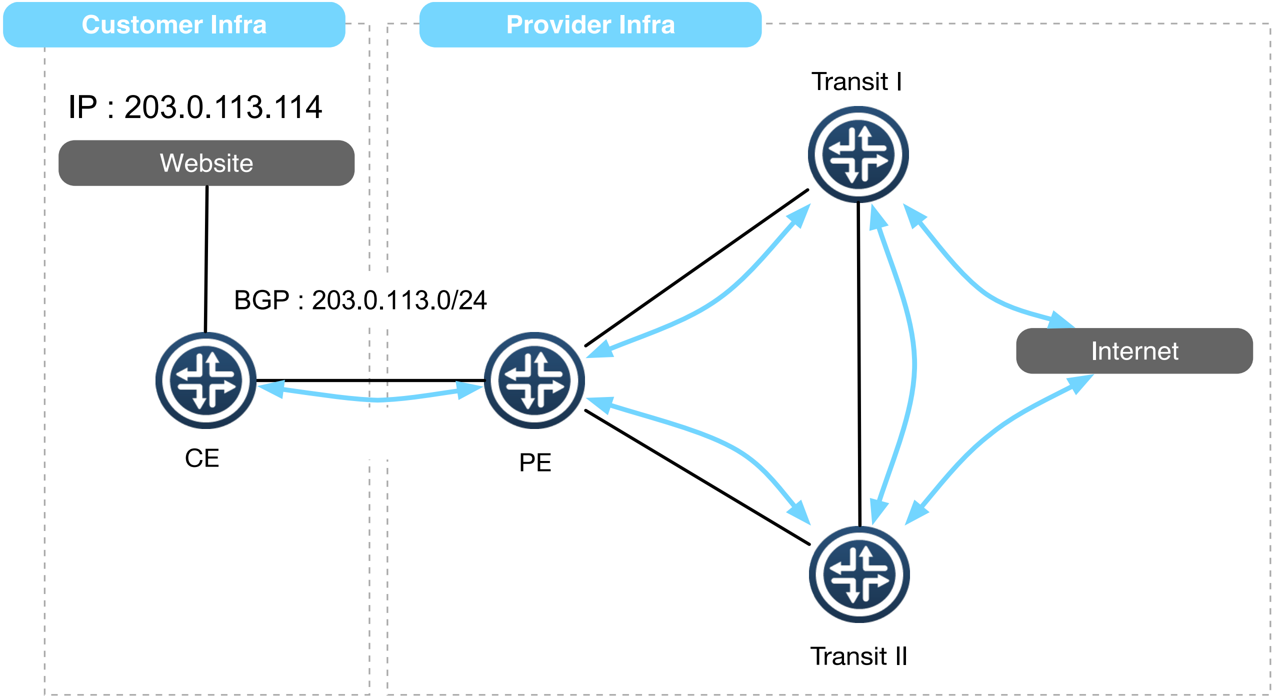
timestamp	count	src ip	src port	dst ip	dst port	protocol	alert source	type
2010-10-19 20:54:14	20	[redacted]	51886	[redacted]	8082	6	ip reputation	botnetcc
2010-10-19 20:52:35	36	[redacted]	25	[redacted]	1521	6	ip reputation	proxy
2010-10-19 20:52:08	12	[redacted]	1547	[redacted]	80	6	ip reputation	proxy
2010-10-19 20:51:54	16	[redacted]	80	[redacted]	4849	6	ip reputation	proxy
2010-10-19 20:51:32	24	[redacted]	1521	[redacted]	25	6	ip reputation	proxy
2010-10-19 20:50:29	8	[redacted]	8082	[redacted]	51886	6	ip reputation	botnetcc
2010-10-19 20:50:05	28	[redacted]	3125	[redacted]	25	6	ip reputation	proxy
2010-10-19 20:49:04	28	[redacted]	25	[redacted]	3125	6	ip reputation	proxy
2010-10-19 20:48:21	36	[redacted]	4115	[redacted]	25	6	ip reputation	proxy
2010-10-19 20:48:15	20	[redacted]	41402	[redacted]	25	6	ip reputation	proxy
2010-10-19 20:48:01	84	[redacted]	34452	[redacted]	80	6	ip reputation	botnetcc
2010-10-19 20:48:00	4	[redacted]	11259	[redacted]	445	6	ip reputation	botnetcc
2010-10-19 20:47:44	48	[redacted]	25	[redacted]	4115	6	ip reputation	proxy
2010-10-19 20:47:22	28	[redacted]	25	[redacted]	41402	6	ip reputation	proxy
2010-10-19 20:47:03	16	[redacted]	45180	[redacted]	25	6	ip reputation	proxy
2010-10-19 20:46:58	20	[redacted]	56645	[redacted]	25	6	ip reputation	proxy
2010-10-19 20:46:07	12	[redacted]	25	[redacted]	45180	6	ip reputation	proxy
2010-10-19 20:45:56	20	[redacted]	25	[redacted]	56645	6	ip reputation	proxy
2010-10-19 20:42:12	4	[redacted]	80	[redacted]	34299	6	ip reputation	botnetcc
2010-10-19 20:39:06	4	[redacted]	80	[redacted]	4732	6	ip reputation	proxy
2010-10-19 20:37:33	36	[redacted]	30082	[redacted]	52311	6	ip reputation	botnetcc
2010-10-19 20:34:28	4	[redacted]	33333	[redacted]	445	6	ip reputation	botnetcc
2010-10-19 20:34:28	4	[redacted]	0	[redacted]	2816	1	ip reputation	botnetcc
2010-10-19 20:34:00	12	[redacted]	52311	[redacted]	30082	6	ip reputation	botnetcc
2010-10-19 20:30:18	12	[redacted]	1621	[redacted]	80	6	ip reputation	proxy
2010-10-19 20:29:54	4	[redacted]	65346	[redacted]	53	17	ip reputation	botnetcc
2010-10-19 20:29:48	12	[redacted]	80	[redacted]	1621	6	ip reputation	proxy
2010-10-19 20:29:08	4	[redacted]	61457	[redacted]	445	6	ip reputation	botnetcc
2010-10-19 20:28:38	4	[redacted]	0	[redacted]	781	1	ip reputation	botnetcc
2010-10-19 20:25:10	32	[redacted]	3284	[redacted]	80	6	ip reputation	botnetcc
2010-10-19 20:24:44	8	[redacted]	80	[redacted]	3250	6	ip reputation	botnetcc
2010-10-19 20:19:12	256	[redacted]	41162	[redacted]	80	6	ip reputation	botnetcc
2010-10-19 20:16:27	8	[redacted]	37247	[redacted]	53	17	ip reputation	botnetcc
2010-10-19 20:16:18	4	[redacted]	1232	[redacted]	25	6	ip reputation	proxy

Flow Sonar : Get It

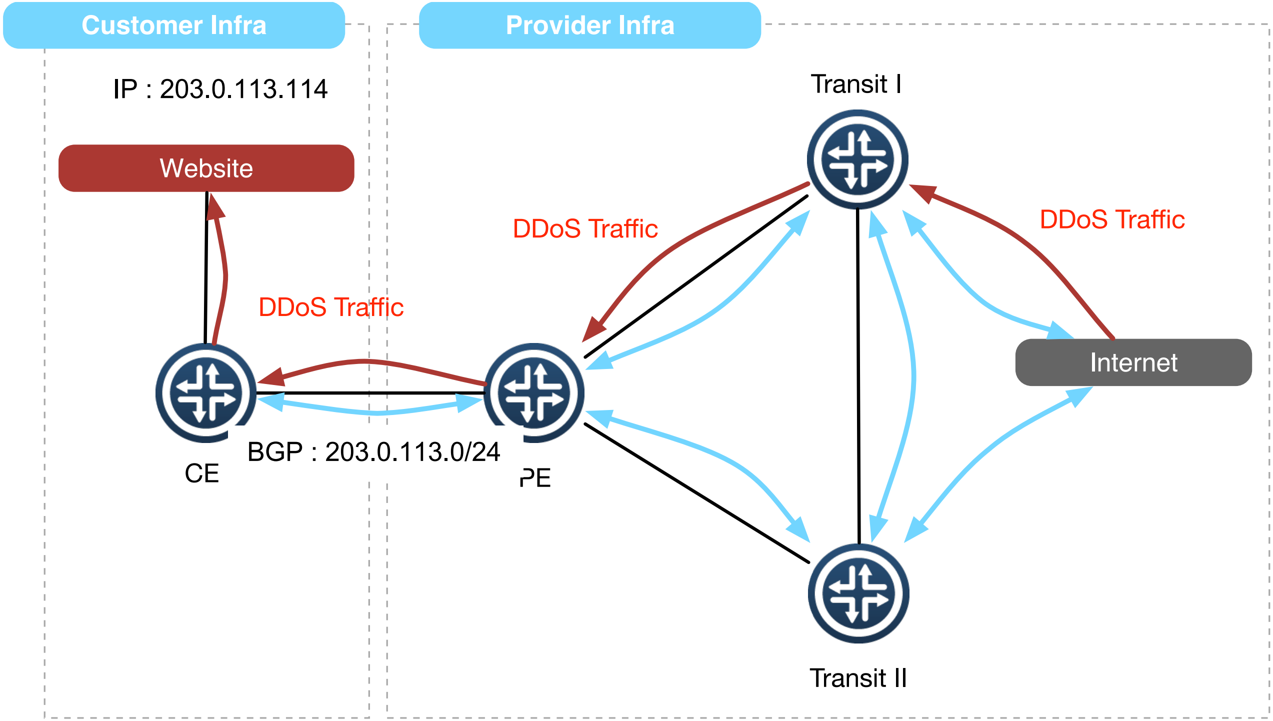
- Contact outreach@cymru.com
  1. Team Cymru will send hardware
     - 1 Server
     - 1 Router
- https://www.team-cymru.org/Flow-Sonar.html

3. UTRS (Unwanted Traffic Removal Service)

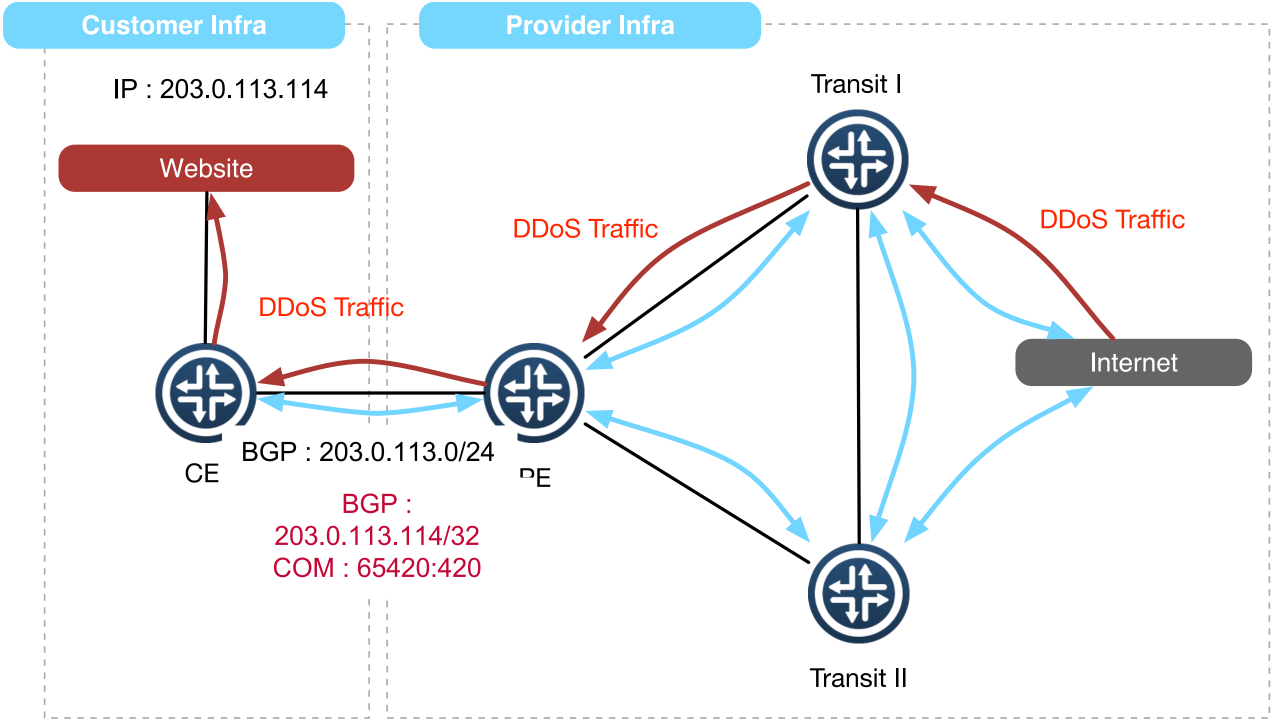
RTBH 101


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

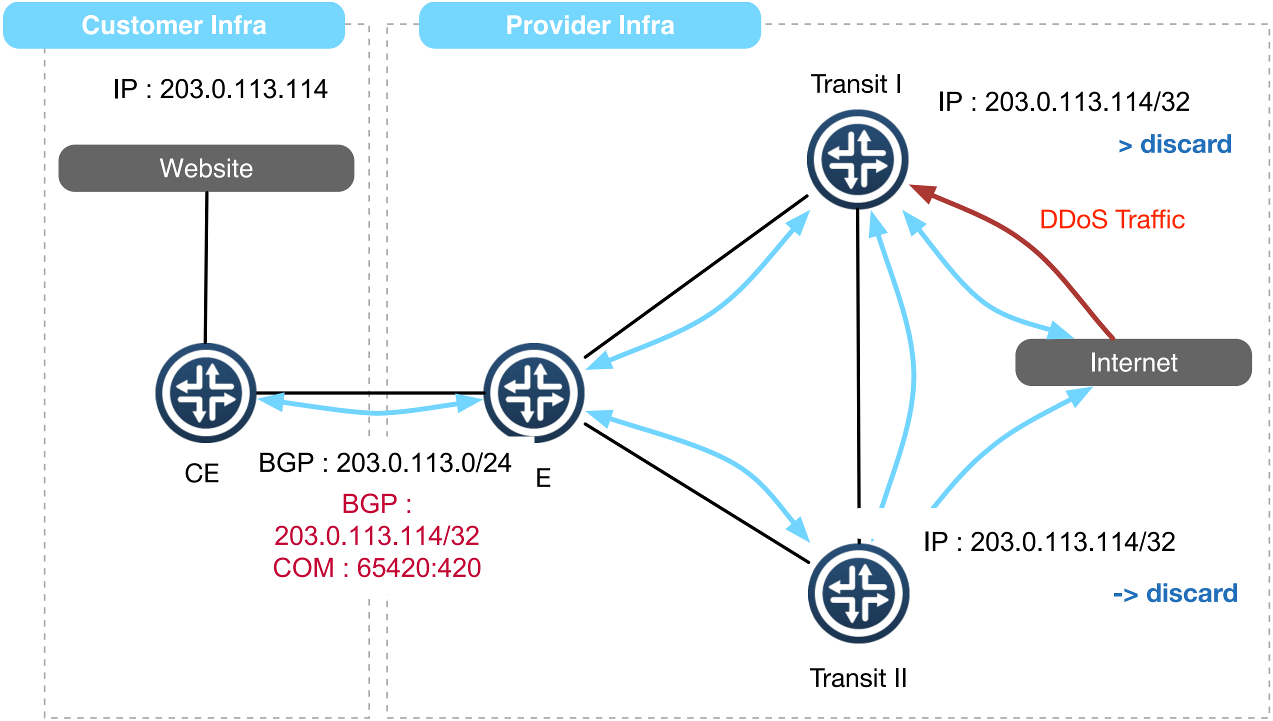
RTBH 101


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 :
203.0.113.114/32
COM : 65420:420
Transit II

RTBH 101


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

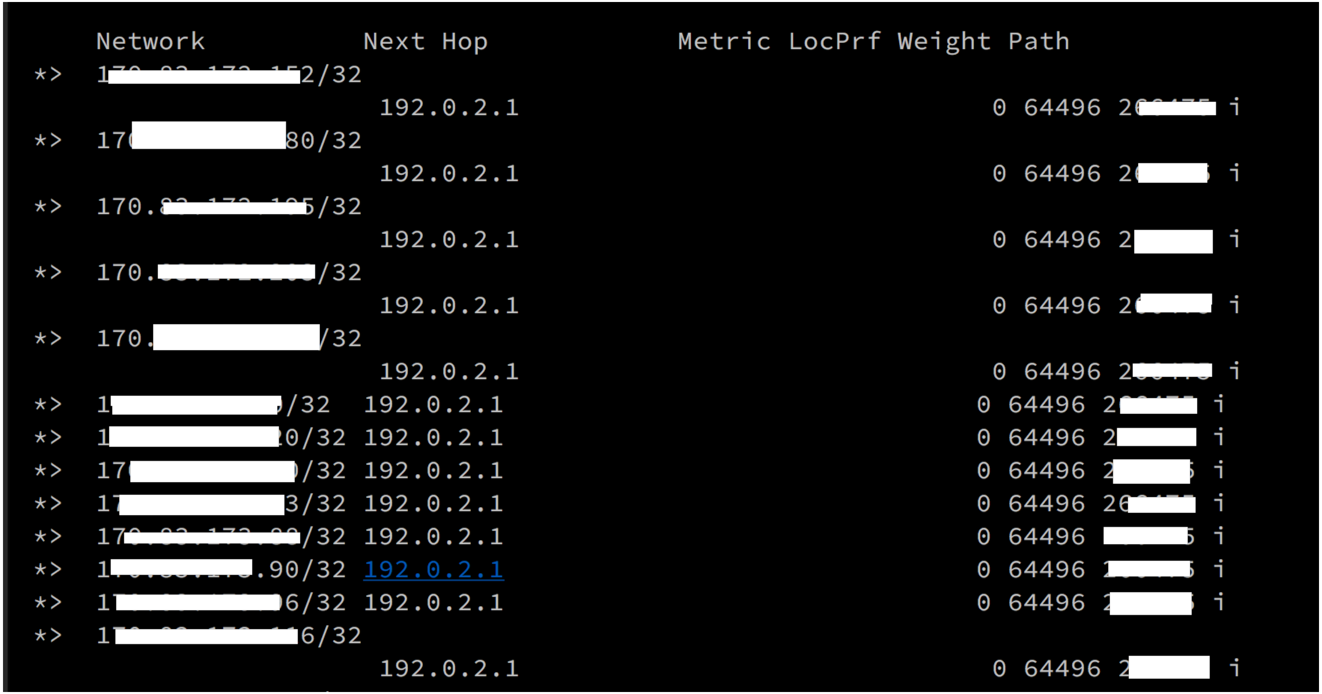
- It’s based on the basic principle of DDoS filtering; Remotely Triggered Black Hole Filtering
- UTRS is a system that helps mitigate large infrastructure attacks by leveraging:
  - an existing network of cooperating BGP speakers such as ISPs, hosting providers and educational institutions
  - that automatically 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 5
 neighbor 154.35.xxx.xxx transport connection-mode passive
 neighbor 154.35.xxx.xxx password 7 xxxxxxxxxxxxxxxxxxxxxx
 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 : Output



```
     Network          Next Hop            Metric LocPrf Weight Path
 *>  1[redacted]2/32
                       192.0.2.1                             0 64496 2[redacted] i
 *>  17[redacted]80/32
                       192.0.2.1                             0 64496 2[redacted] i
 *>  170.[redacted]/32
                       192.0.2.1                             0 64496 2[redacted] i
 *>  170.[redacted]/32
                       192.0.2.1                             0 64496 2[redacted] i
 *>  170.[redacted]/32
                       192.0.2.1                             0 64496 2[redacted] i
 *>  1[redacted]/32   192.0.2.1                             0 64496 2[redacted] i
 *>  1[redacted]0/32 192.0.2.1                             0 64496 2[redacted] i
 *>  17[redacted]/32 192.0.2.1                             0 64496 2[redacted] i
 *>  17[redacted]3/32 192.0.2.1                             0 64496 2[redacted] i
 *>  17[redacted]/32 192.0.2.1                             0 64496 [redacted] i
 *>  1[redacted].90/32 192.0.2.1                             0 64496 [redacted] i
 *>  1[redacted]6/32 192.0.2.1                             0 64496 2[redacted] i
 *>  1[redacted]6/32
                       192.0.2.1                             0 64496 2[redacted] i
```

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!

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!

Fakrul Alam

fakrul@apnic.net