International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 3, Issue4 (July-August 2015), pp. 339-343

DESTINATION BASED RTBH FILTERING AT ATTACK ORIGINATING INTERNET SERVICE PROVIDER

Sarita Sharma[1], Davender Saini[2]

[1]Student M. Tech. ECE (2013-2015) Gurgaon Institute of Technology Management (M.D.U)
Bilaspur-Tauru Road, Gurgaon (Haryana) India
[2]Assistant Professor Gurgaon Institute of Technology Management (M.D.U)
Bilaspur-Tauru Road, Gurgaon (Haryana) India

[1]saritasharma1791@gmail.com
[2]gitmexperts@gmail.com

***Abstract* - Remote triggered black hole (rtbh) filtering is a popular and effective technique for the mitigation of denial-of-service attacks. this document explains the mitigation of ddos attack at attack originating internet service provider so that other connected service providers remains unaffected and attacked traffic will only drop at attack originating isp.**

Keywords: RTBH, ISP, DDOS attack

I. INTRODUCTION

Network operators have developed a variety of techniques for mitigating denial-of-service (DoS) attacks. While different techniques have varying strengths and weaknesses, from an implementation perspective, the selection of which method to use for each type of attack involves evaluating the tradeoffs associated with each method.

A common DoS attack directed against a customer of a service provider involves generating a greater volume of attack traffic destined for the target than will fit down the links from the service provider(s) to the victim (customer). This traffic "starves out" legitimate traffic and often results in collateral damage or negative effects to other customers or the network infrastructure as well. Rather than having all destinations on their network be affected by the attack, the customer may ask their service provider to filter traffic destined to the target destination IP address(es), or the service provider may determine that this is necessary themselves, in order to preserve network availability.

Most routers are able to forward traffic at a much higher rate than they are able to filter, and they are able to hold many more forwarding table entries and routes than filter entries. RTBH filtering leverages the forwarding performance of modern routers to filter more entries and at a higher rate than access control lists would otherwise allow.

However, with destination-based RTBH filtering, the impact of the attack on the target is complete. That is, destination-based RTBH filtering injects a discard route into the forwarding table for the target prefix. All packets towards that destination, attack traffic and legitimate traffic, are then dropped by the participating routers, thereby taking the target completely offline. The benefit is that collateral damage to other systems or network availability at the customer location or in the ISP network is limited, but the negative impact to the target itself is arguably increased.

This document expands destination-based RTBH filtering, as the purpose is to block the attack from where attack originates, so that it will not affect other connected ISP in internet and protect their connected bandwidth. To deploy we need to implement RTBH technique at all ISPs connected with each other so that they can advertise attacked ip prefix to each **other of** (/32) and the attacked traffic will drop at the edge router of attack originating ISP.

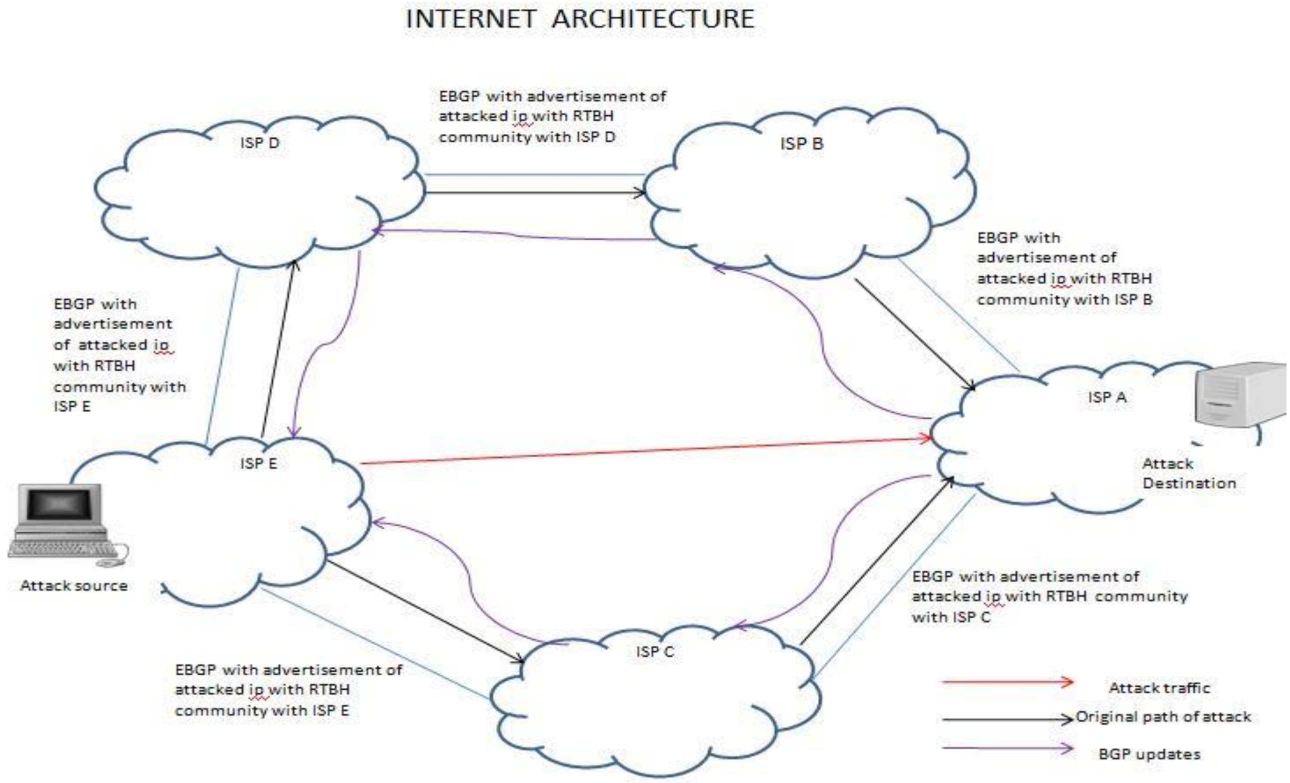
INTERNET ARCHITECTURE
ISP D
EBGP with advertisement of attacked ip with RTBH community with ISP D
ISP B
EBGP with advertisement of attacked ip with RTBH community with ISP B
EBGP with advertisement of attacked ip with RTBH community with ISP E
ISP A
Attack Destination
ISP E
Attack source
EBGP with advertisement of attacked ip with RTBH community with ISP C
ISP C
EBGP with advertisement of attacked ip with RTBH community with ISP E
Attack traffic
Original path of attack
BGP updates

Figure 1: INTERNET ARCHITECTURE OF CONNECTED ISP

Figure 1 shows internet architecture in which all ISP connected to each other .If there is attack on ISP A connected server or its customer which is originated from ISP E then the invalid traffic will move ISP E->ISP D->ISP B -> ISP A and ISP E -> ISP C -> ISP A. In this case bandwidth connected between all ISP can be chocked depends on the volume of attack but if are able to drop traffic from at ISPA which is coming attack source connected with ISP A then it will save the bandwidth and there is no impact to any customer connected any of the ISP.

To implement we need to provide information for the attack destination ip which can be achieve by extended the RTBH destination based filtering throughout the internet.

Method to deploy RTBH FILTERING at originating AS:

Before deploying RTBH filtering, there are some terms need to understand:

1. What is NULL0?
2. What are NULL0 BGP or RTBH communities?
3. PREFIXES length that we can block?

4. Prefixes length that other connected ISP accepted for RTBH?

NULL0: An address is chosen x.x.x.x/32 as discard route which point all the attacked traffic towards NULL 0 interface.

NULL0 BGP or RTBH communities: NULL0 BGP community is provided by the ISP to its peer or customer to identify attacked ip (xxxx:yyyy), and to point traffic for attack destination ip towards discard route.

PREFIXES length that we can block: We can block the attacked ip ranging from longest to smallest. If attack is on /32 then we will only block specific pool of /32 which saves other customer ip belonging to same ip pool.

There is no boundation of prefix length for RTBH.

Prefixes length that other connected ISP accepted for RTBH: As per internet standard policy no ISP accept or advertise bugger than /24 prefix .but For RTBH solution all ISP accepts will accept any prefix length.

STEP 1: Generate a /32 route of attacked ip and trigger RTBH.

There is /24 or smaller pool which is advertise to any ISP .To trigger RTBH need to generate a prefix of /32 by configuring static on the router and advertise it to connected ISP provider with community tag of RTBH community which is used in connected ISP for black hole filtering.

STEP 2: Configuring a discard route in all ISP.

To dump traffic towards null need to configuring a discard route of /32 on ISP's gateway or edge routers.

e.g.: Ip route 192.0.2.1 255.255.255.255 null0

STEP 3: Receiving a route from attack Destination with RTBH community and point it towards discard route.

When ISP receive a prefix with its own RTBH community it set the null route as next-hop the attacked ip prefix and advertise it to edge or gateway routers and the router to which its upstream and other ISP connected.

When traffic hits to the destination from the connected ISP's customer it will point towards null0 and traffic will be black holed.

STEP 4: configuring RTBH solution with its connected upstream and internet service providers.

Attack coming from destination connected ISP's customer will be dropped at edge router and also coming from other upstream provider will drop on gateway router but still the bandwidth connected with other ISP will be chocked, if attack is coming from them.

To mitigate this impact we need to run black holing solution with all connected ISP so that the traffic for impacted destination will dump in that next provider from where attack traffic is coming and will not hit to destination connected ISP.

To deploy this we need to implement RTBH solution with service provider. To provide destination ip need to match destination ISP RTBH community and set community of next upstream provider RTBH community in EBGP session.

STEP 5 Receiving of attacked ip to connected upstream provides from attack destination ISP tagged with their own RTBH community and pointed towards discard route.

Next service provider will receive the attacked ip with RTBH community and pointed towards the discard route to dump traffic in its own cloud if attack coming from its customer and pass the same attacked destination ip to its upstream.

This endless cycle of Black holing will configure between all the ISP connected to each other in the internet to spread the attack destination ip and to dump the traffic in attack originating service provider.

II. CONFIGURATION

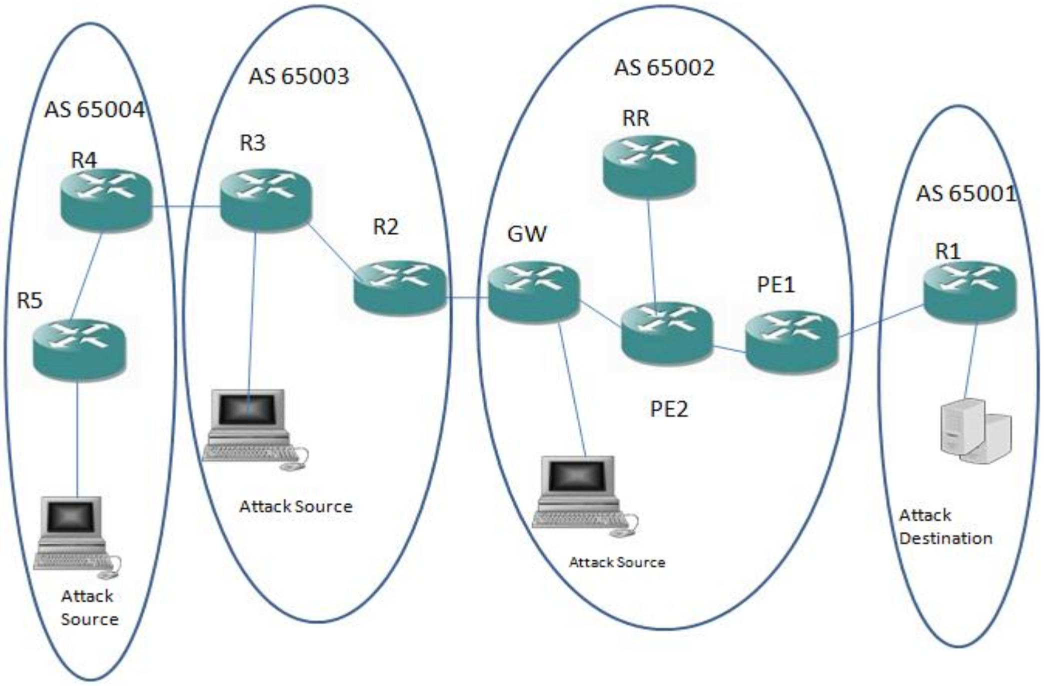

Figure2: Design for destination based RTBH filtering

In the Figure 2 there is a servers which connects with router R1 with ip 10.10.10.0/24 .

Attack hitting one of the server ip 10.10.10.1/32

Router R1:

```
ip route 10.10.10.1 255.255.255.255 null 0 tag 10
route-map PEER-65001-OUT permit 10
 match tag 10
 set community 65002:1
route-map PEER-65001-OUT permit 20
```

EBGP session is configured between R1 and PE1, above route-map configure on R1 where 65002:1 is RTBH community for AS 65002.

Router PE1:

```
 Community-list RTBH permit 65002:1
route-map PEER-65002-IN permit 10
 match community RTBH
 set ip next-hop 192.0.2.1
route-map PEER-65002-OUT permit 20
```

192.0.2.1 is discard route configured in AS 65002

Router GW:

```
ip route 192.0.2.1 255.255.255.255 null 0
```

Configuration from discard route for AS 65002 and redistribute it to IBGP session.

```
Community-list RTBH permit 65002:1
route-map PEER-65002-OUT-TO-AS-65003 permit 10
 match community RTBH
 set  community 65003:1
route-map PEER-65002-OUT-TO-AS-65003 permit 20
```

above route map configured to advertise attacked ip to AS 65003 with its RTBH community 65003:1

In similar way we need to configure the same configuration for AS 65003 and 65004.

III. CONCLUSION

This technology is advancement of RTBH destination filtering to block attacked prefix at originating internet service provider .As DDOS attack can impact all bandwidth from attack source ISP to destination connected ISP. After implementing this solution the bandwidth will not get chock and attacked traffic or legitimate traffic will impact in their own originated ISP for the attack destination.

To black hole a /32 attack destination we no need to impact a pool or /24 or lesser. And only attacked /32 prefix will be out of service and rest of the ip will work.

IV. REFRENCES

[1] Remotely Triggered Black Hole filtering Cisco White Papers

[2] Remotely Triggered Black Hole Filtering With URPF-RFC-5635.

[3] Rekhter, Y., Moskowitz, B., Kornberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[4] Turk, D., "Configuring BGP to Block Denial-of-Service Attacks", RFC 3882, September 2004.

[5] Baker, F. and P. Savola, "Ingress Filtering for Multihued Networks", BCP 84, RFC 3704, March 2004.