Destination Based RTBH

Farklı ISP'lerin arkalarındaki PC'ler IP adresi 8.8.8.8 olan Server'a erişim sağlamaktadır.

```
PC01#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/7 ms
PC01#
PC02#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/6 ms
PC02#
PC-03#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/8 ms
PC-03#
VPCS> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=250 time=8.484 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=250 time=4.614 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=250 time=4.547 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=250 time=4.920 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=250 time=4.702 ms

VPCS>
```

Olurda bir gün bu Server'a (8.8.8.8) birileri DDOS yaparsa diye AS500 çalışanları AS100 den destek ister. Ve aralarında bir uzlaşmaya varılır. Bu noktada iki farklı uzlaşı vardır:

Birinde AS500 çalışanları AS100'e DDOS'un başladığını ve gerekli önlemin alınması gerektiğini telefonda söyleyecektir ve AS100 çalışanları hem DDOS öncesinde önlemlerini alacak hem de DDOS anında gerekli bütün işi yani tetiklemeyi yapacaktır.

Diğer uzlaşı yönteminde ise AS100 çalışanları aynen önceki senaryodaki gibi DDOS öncesi önlemlerini alacak lakin DDOS anında AS500 tetiklemeyi yapacak ve AS100 otomatik olarak DDOS kesimini otomatik gerçekleştirecektir.

Gelin önce AS100'ün DDOS öncesi alması gereken önlemleri görelim. AS100 bütün çıkış router'larında 192.0.2.0/24 bloğunu Null0 ya statik olarak yönlendirir. XR01, XR02, XR03, XR04, XR05, XR06 ve RR`da bu statik route girilir:

```
!
router static
 address-family ipv4 unicast
  192.0.2.0/24 Null0
 !
!
```

AS100 de bilgiyi taşıyan Route-Reflector olan RR da esas şartlı konfig yapılır:

```
!
route-policy RTBH
  if tag is 666 then
    set next-hop 192.0.2.1
    set community (100:666)
    set local-preference 1000
  endif
  if destination in (192.0.2.0/24) then
    drop
  endif
  pass
end-policy
!
router bgp 100
 address-family ipv4 unicast
  redistribute static route-policy RTBH
 !
!
```

Burada dikkat edilirse özel bir durum/koşul izlenmektedir. Şayet BGP'ye bir ifade TAG 666 ile gelirse (ki bu uygulama, tetiklemenin AS100 tarafından yapılacağı senaryo için geçerlidir) bu prefix'in next-hop bilgisini 192.0.2.1 yapacaktır. (ki bu ip az önce null0 ya yönlendirilmişti.) Ayrıca anons edilirken 100:666 community değeri ile anons edilecek ve local-preference değeri 1000 yapılıp baskın bir değer olması sağlanacak. Ve tabidir ki statik route'ları BGP ye sokarken de bu RPL'I kullanmaktayız. Tüm bunlar AS100'ün saldırı öncesi hazırlıkları idi.

DDOS başladığında, o kara gün yaşandığında, server ağladığında, AS500 çalışanları AS100 çalışanlarını arayacak ve acı haberi verecekler. Bunu öğrenen AS100 çalışanları hemen RR routerlarına gidecek ve şöyle bir statik route yazacaklar:

```
!
router static
 address-family ipv4 unicast
  8.8.8.8/32 Null0 tag 666
 !
!
```

Görüldüğü gibi RR 8.8.8.8/32'yi Null0'ya yönlendirmekte ve bunu yaparken de özel bir etiket kullanmaktadır: Tag 666.

Artık AS100'ün bütün çıkış routerlarına bu özel bilgi gitmekte ve hepsi 8.8.8.8'i 192.0.2.1'e yani dolaylı olarak Null0'a yönlendirmekteler.

```
RP/0/0/CPU0:XR02#sh bgp ipv4 unicast
Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
*>i8.8.8.0/24         3.3.3.3                  0    100      0 500 i
*>i8.8.8.8/32         192.0.2.1                0   1000      0 ?
*>i172.16.1.0/24      4.4.4.4                  0    100      0 200 i
*>i172.16.2.0/24      5.5.5.5                  0    100      0 300 i
*>i172.16.3.0/24      6.6.6.6                  0    100      0 400 i
*>i172.16.4.0/24      1.1.1.1                  0    100      0 700 i
*>i192.0.2.0/24       9.9.9.9                  0    100      0 ?

Processed 7 prefixes, 7 paths
RP/0/0/CPU0:XR02#

RP/0/0/CPU0:XR02#sh route ipv4 unicast bgp

B    8.8.8.0/24 [200/0] via 3.3.3.3, 00:21:30
B    8.8.8.8/32 [200/0] via 192.0.2.1, 00:18:28
B    172.16.1.0/24 [200/0] via 4.4.4.4, 00:21:30
B    172.16.2.0/24 [200/0] via 5.5.5.5, 00:21:30
B    172.16.3.0/24 [200/0] via 6.6.6.6, 00:21:30
B    172.16.4.0/24 [200/0] via 1.1.1.1, 00:21:30
RP/0/0/CPU0:XR02#
```

Dünya artık 8.8.8.8'e erişememekte lakin 8.8.8.0/24'ün geri kalan IP adreslerine erişebilmektedir.

```
PC02#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC02#ping 8.8.8.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/4/5 ms
PC02#
```

Bu noktada AS100 trafiği üzerine çekmeye devam etmektedir. Bunun önüne geçmek için AS100 esas çıkış bacağı olan ve bütün interneti öğrenmekte olduğu AS700'e (bu noktada AS700'ü yurt dışı çıkışı ya da Tier 1 ISP gibi düşünebiliriz) bu bilgiyi ulaştırması ve 8.8.8.8/32 networküne giden paketlerin kendisine gelmemesini sağlamalıdır. Daha önceden AS100 çalışanları AS700 ile konuşmuş ve olası bir DDOS saldırısında AS100 den giden BGP anonslarının içinde herhangi bir prefix'in 100:666 community değerini taşıması halinde o prefix'e doğru olan trafiği kendilerine göndermemelerini talep etmişlerdi. Zaten RR bilgiyi gönderirken 100:666 community değerini göndermektedir. XR01 de tek yapılması gereken iş, bu community değerinin eBGP komşusu olan XR07 ye ulaşmasını sağlamak. XR01 de şu komutlar girilir:

```
!
router bgp 100
!
 neighbor 10.10.71.77
  address-family ipv4 unicast
   send-community-ebgp
  !
!
```

Daha önceden hazırlığını yapmış olan AS700 deki XR07 router'ı aldığı anonsta 100:666'yı yakalar yakalamaz aşağıdaki RPL'i işletecektir. XR07 deki genel koruma konfiği aşağıdaki gibidir:

```
!
route-policy RTBH
  if community matches-any (100:666) then
    set next-hop 192.0.2.1
    set community (no-export) additive
    set local-preference 1000
  endif
  pass
end-policy
!
router static
 address-family ipv4 unicast
  192.0.2.0/24 Null0
!
router bgp 700
 neighbor 10.10.71.1
  address-family ipv4 unicast
   route-policy RTBH in
!
```

XR07 deki BGP anonslarına bakacak olursak:

```
RP/0/0/CPU0:XR07#show bgp ipv4 unicast 8.8.8.8/32
BGP routing table entry for 8.8.8.8/32
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 27          27
Last Modified: Dec 13 22:26:50.223 for 00:00:40
Paths: (1 available, best #1, not advertised to EBGP peer)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  100
    192.0.2.1 from 10.10.71.1 (1.1.1.1)
      Origin incomplete, localpref 1000, valid, external, best, group-best
      Received Path ID 0, Local Path ID 0, version 27
      Community: 100:666 no-export
      Origin-AS validity: not-found
RP/0/0/CPU0:XR07#
```

Community'i aldığını ve dolaylı olarak 8.8.8.8/32 ye olan trafiği Null0'ya yönlendirdiğini görmekteyiz.

Atak kesilir kesilmez RR da girdiğimiz statik route'u kaldırarak 8.8.8.8'i dünyada erişilebilir hale getiririz.

```
RP/0/0/CPU0:RR#conf t
RP/0/0/CPU0:RR(config)#router static
RP/0/0/CPU0:RR(config-static)# address-family ipv4 unicast
RP/0/0/CPU0:RR(config-static-afi)# no 8.8.8.8/32 Null0 tag 666
RP/0/0/CPU0:RR(config-static-afi)#commit
```

Ve artık erişim sağlanmaktadır:

```
PC02#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
PC02#
```

Hatırlarsanız DDOS anında black-hole tetiklemenin müşteri (AS500) tarafından da yapılabileceğini söylemiştik. Şimdi o senaryoyu inceleyelim:

Bu durum için öncelikle AS100'de DDOS öncesi alınması gereken önlemleri görelim:

AS100 den 100:666 community değerini alan XR03 bu community'i RR'a otomatik olarak yollayacaktır. RR'da XR03'den 100:666 community değerini alması halinde ilgili prefixin Null0'ya yönlendirilmesini şu şekilde sağlayabilir:

```
!
route-policy RTBH-666
  if community matches-any (100:666) then
    set next-hop 192.0.2.1
    set local-preference 1000
  endif
  pass
end-policy
!
router bgp 100
 !
 neighbor 3.3.3.3
  address-family ipv4 unicast
   route-policy RTBH-666 in
!
```

AS500'ün çıkış router'ı olan CE-01'de 8.8.8.8/32 prefix'i anons ederken ilave bir community değeri olarak 100:666'yı ekleyecektir BGP anonsuna. Ve XR03'e bu ilave community'yi gönderebilmesi için BGP komşuluğunda buna izin vermesi gerekecektir.

```
!
ip bgp-community new-format
!
route-map RTBH permit 10
 match tag 666
 set community 100:666
!
route-map RTBH permit 20
!
```

```
!
router bgp 500
 redistribute static route-map RTBH
 neighbor 10.10.13.3 send-community
!
```

Gün gelir devran döner 8.8.8.8 IP adresli server'ımıza DDOS saldırısı başlar. Server yorgun, server şişik, server ağlıyor. Haşmetli bir bandwidth ile yapılan saldırı AS500'ü de yormakta. Ama AS500 çalışanları hazırlıklı. Hemen aşağıdaki konfig ile tetiklemeyi başlatıyorlar:

```
!
ip route 8.8.8.8 255.255.255.255 Null0
!
```

Ve dünyanın 8.8.8.8'e erişimi yine kesiliyor:

```
PC02#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC02#
```

Atak kesildikten sonra ise CE-01 şu işlemleri yaparak erişimi açar:

```
!
no ip route 8.8.8.8 255.255.255.255 Null0
!
```

Ve artık erişim sağlanmaktadır:

```
PC02#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
PC02#
```