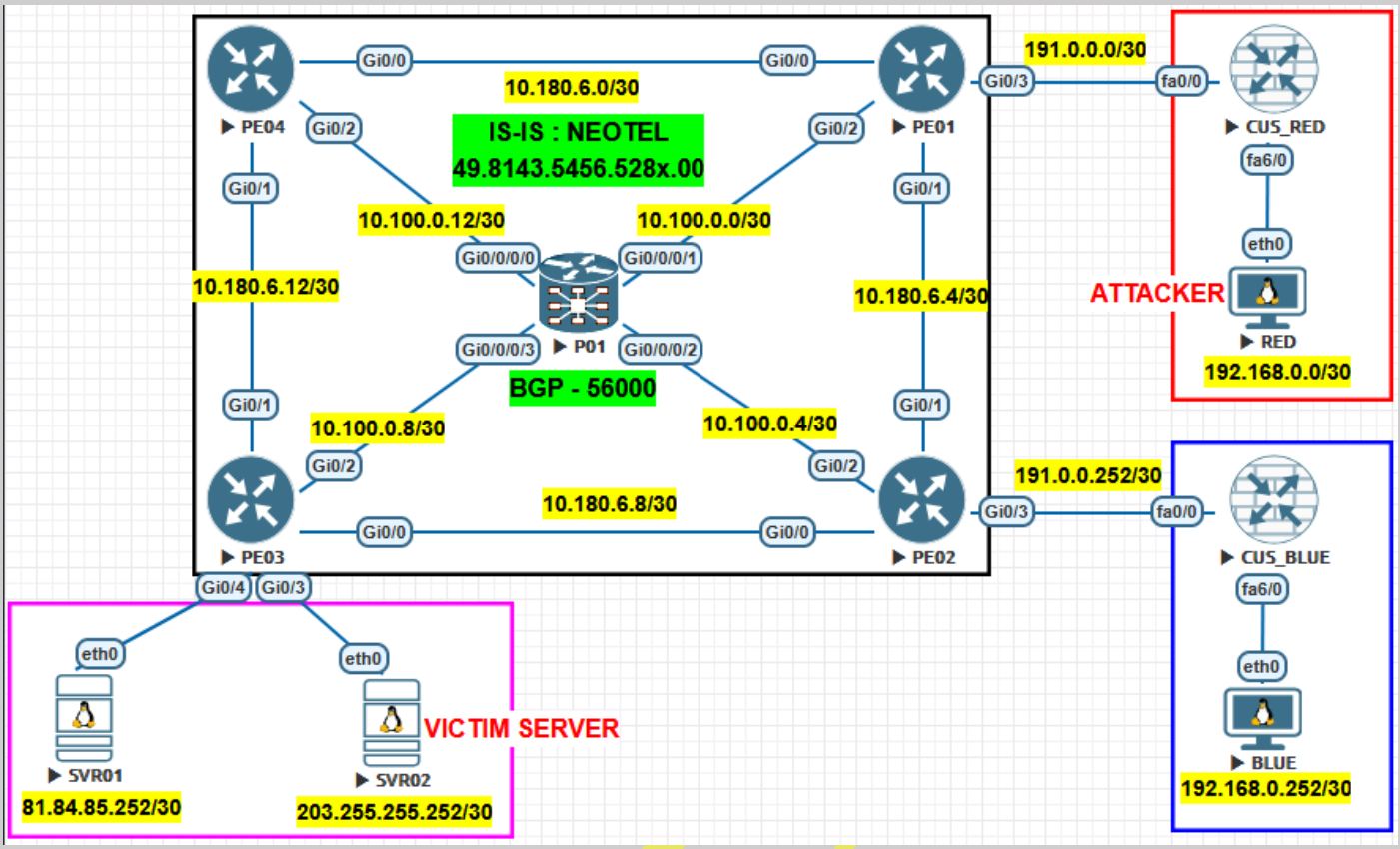
Destination–Based Remotely Triggered Black Hole (RTBH)



Lab Requirements

1. Configure iBGP under AS 56000 with full reachability between PE routers, ensuring customers receive only a default route while advertising server prefixes into BGP.
2. Prepare the network for Destination–Based RTBH by implementing blackhole community tagging, policy–based route filtering, and next–hop nullification to enable DDoS mitigation.

Configuration

Underlay Routing Protocol : IS–IS

PE01

router isis **NEOTEL**

net 49.8143.5456.5281.00

is–type level–2–only

```
 metric–style wide
!
interface range gigabitEthernet 0/0–2
ip router isis NEOTEL
isis network point–to–point
 isis hello–multiplier 5
 isis hello–interval 3
!
interface Loopback2028
ip router isis NEOTEL
!
```

PE02

```
router isis NEOTEL
 net 49.8143.5456.5282.00
 is–type level–2–only
 metric–style wide
!
interface range gigabitEthernet 0/0–2
ip router isis NEOTEL
isis network point–to–point
 isis hello–multiplier 5
 isis hello–interval 3
!
interface Loopback2028
```

ka-net

ip router isis **NEOTEL**

!

PE03

router isis **NEOTEL**

net 49.8143.5456.5283.00

is-type level-2-only

metric-style wide

!

interface range gigabitEthernet 0/0-2

ip router isis **NEOTEL**

isis network point-to-point

isis hello-multiplier 5

isis hello-interval 3

!

interface Loopback2028

ip router isis **NEOTEL**

!

interface range gigabitEthernet 0/3-4

ip router isis **NEOTEL**

!

PE04

router isis **NEOTEL**

net 49.8143.5456.5284.00

is-type level-2-only

ka-net

```
 metric-style wide
!
interface range gigabitEthernet 0/0-2
ip router isis NEOTEL
isis network point-to-point
 isis hello-multiplier 5
 isis hello-interval 3
!
interface Loopback2028
ip router isis NEOTEL
!
P01
router isis NEOTEL
 is-type level-2-only
 net 49.8143.5456.5285.00
 address-family ipv4 unicast
  metric-style wide
 !
 interface Loopback2028
  address-family ipv4 unicast
 !
 interface GigabitEthernet0/0/0/0
  point-to-point
  hello-interval 3
```

lka-net

```
 hello-multiplier 5
 address-family ipv4 unicast
!
interface GigabitEthernet0/0/0/1
 point-to-point
 hello-interval 3
 hello-multiplier 5
 address-family ipv4 unicast
!
interface GigabitEthernet0/0/0/2
 point-to-point
 hello-interval 3
 hello-multiplier 5
 address-family ipv4 unicast
!
interface GigabitEthernet0/0/0/3
 point-to-point
 hello-interval 3
 hello-multiplier 5
 address-family ipv4 unicast
!
```

BGP Configuration

PE01

```
router bgp 56000
```

lka-net

```
 bgp router-id 172.16.255.1
 neighbor 172.16.255.254 remote-as 56000
 neighbor 172.16.255.254 password kolwin!!!!
 neighbor 172.16.255.254 update-source Loopback2028
 !
 address-family ipv4
  network 191.0.0.0 mask 255.255.255.252
  neighbor 172.16.255.254 activate
exit-address-family
!
ip bgp-community new-format
!
```

PE02

```
router bgp 56000
 bgp router-id 172.16.255.2
 neighbor 172.16.255.254 remote-as 56000
 neighbor 172.16.255.254 password kolwin!!!!
 neighbor 172.16.255.254 update-source Loopback2028
 !
 address-family ipv4
  network 191.0.0.252 mask 255.255.255.252
  neighbor 172.16.255.254 activate
 exit-address-family
!
```

ka-net

```
ip bgp-community new-format
!
```

PE03

```
router bgp 56000
 bgp router-id 172.16.255.3
 neighbor 172.16.255.254 remote-as 56000
 neighbor 172.16.255.254 password kolwin!!!!
 neighbor 172.16.255.254 update-source Loopback2028
 !
 address-family ipv4
  network 81.84.85.252 mask 255.255.255.252
  network 203.255.255.252 mask 255.255.255.252
  neighbor 172.16.255.254 activate
 exit-address-family
!
ip bgp-community new-format
!
```

PE04

```
router bgp 56000
 bgp router-id 172.16.255.4
 neighbor 172.16.255.254 remote-as 56000
 neighbor 172.16.255.254 password kolwin!!!!
 neighbor 172.16.255.254 update-source Loopback2028
 !
```

lka-net

```
 address-family ipv4
  neighbor 172.16.255.254 activate
 exit-address-family
!
ip bgp-community new-format
!
```

P01 (RR)

```
router bgp 56000
 bgp router-id 172.16.255.254
 address-family ipv4 unicast
 !
 neighbor-group RR
  remote-as 56000
  password kolwin!!!!
  update-source Loopback2028
  address-family ipv4 unicast
   route-reflector-client
 !
 neighbor 172.16.255.1
  use neighbor-group RR
 !
 neighbor 172.16.255.2
  use neighbor-group RR
 !
```

ka-net

```
 neighbor 172.16.255.3
  use neighbor-group RR
 !
 neighbor 172.16.255.4
  use neighbor-group RR
!
```

RTBH Configuration

PE01

1. Static Route via Null0

```
ip route 192.0.2.254 255.255.255.255 Null0
!
```

2. Community List

```
ip community-list standard NEO-RTBH-COM permit 56000:24
!
```

3. Route-map

```
route-map NEO-RTBH-RM permit 10
match community NEO-RTBH-COM
set ip next-hop 192.0.2.254
route-map NEO-RTBH-RM permit 1000
!
```

4. Apply in BGP

```
router bgp 56000
address-family ipv4
  neighbor 172.16.255.254 route-map NEO-RTBH-RM in
```

ka-net

!

PE02

1. Static Route via Null0

ip route 192.0.2.254 255.255.255.255 Null0

!

2. Community List

ip community-list standard **NEO-RTBH-COM** permit 56000:24

!

3. Route-map

route-map **NEO-RTBH-RM** permit 10

match community **NEO-RTBH-COM**

set ip next-hop **192.0.2.254**

route-map **NEO-RTBH-RM** permit 1000

!

4. Apply in BGP

router bgp 56000

address-family ipv4

neighbor 172.16.255.254 route-map **NEO-RTBH-RM** in

!

PE04 (Trigger Router)

1. Route-map

route-map **NEO-TRIGGER** permit 10

match tag **24**

set community **56000:24** ***no-export***

ka-net

!

2. Apply in BGP

router bgp 56000

address-family ipv4

redistribute static route-map **NEO-TRIGGER**

neighbor 172.16.255.254 **send-community**

!

3. Trigger Static Route When Server 203.255.255.254 is attacked

ip route 203.255.255.254 255.255.255.255 Null0 tag 24

!

Verification

Before the attack against 203.255.255.254 begins,

PE01

```
PE01#sh ip route bgp | be Gate
Gateway of last resort is not set

      81.0.0.0/30 is subnetted, 1 subnets
B        81.84.85.252 [200/0] via 172.16.255.3, 00:03:25
      191.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
B        191.0.0.252/30 [200/0] via 172.16.255.2, 00:03:04
      203.255.255.0/30 is subnetted, 1 subnets
B        203.255.255.252 [200/0] via 172.16.255.3, 00:03:25
```

PE02

```
PE02#sh ip route bgp | be Gate
Gateway of last resort is not set

      81.0.0.0/30 is subnetted, 1 subnets
B        81.84.85.252 [200/0] via 172.16.255.3, 00:04:47
      191.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
B        191.0.0.0/30 [200/0] via 172.16.255.1, 00:04:38
      203.255.255.0/30 is subnetted, 1 subnets
B        203.255.255.252 [200/0] via 172.16.255.3, 00:04:47
```

ATTACKER PC RED

```
RED> ping 203.255.255.254

84 bytes from 203.255.255.254 icmp_seq=1 ttl=60 time=19.860 ms
84 bytes from 203.255.255.254 icmp_seq=2 ttl=60 time=14.609 ms
84 bytes from 203.255.255.254 icmp_seq=3 ttl=60 time=11.124 ms
84 bytes from 203.255.255.254 icmp_seq=4 ttl=60 time=12.656 ms
84 bytes from 203.255.255.254 icmp_seq=5 ttl=60 time=10.696 ms

RED> ping 81.84.85.254

84 bytes from 81.84.85.254 icmp_seq=1 ttl=60 time=12.816 ms
84 bytes from 81.84.85.254 icmp_seq=2 ttl=60 time=15.303 ms
84 bytes from 81.84.85.254 icmp_seq=3 ttl=60 time=11.485 ms
84 bytes from 81.84.85.254 icmp_seq=4 ttl=60 time=13.514 ms
84 bytes from 81.84.85.254 icmp_seq=5 ttl=60 time=10.775 ms
```

USER PC BLUE

```
BLUE> ping 81.84.85.254

84 bytes from 81.84.85.254 icmp_seq=1 ttl=61 time=19.467 ms
84 bytes from 81.84.85.254 icmp_seq=2 ttl=61 time=20.972 ms
84 bytes from 81.84.85.254 icmp_seq=3 ttl=61 time=11.805 ms
84 bytes from 81.84.85.254 icmp_seq=4 ttl=61 time=12.410 ms
84 bytes from 81.84.85.254 icmp_seq=5 ttl=61 time=15.258 ms

BLUE> ping 203.255.255.254

84 bytes from 203.255.255.254 icmp_seq=1 ttl=61 time=19.550 ms
84 bytes from 203.255.255.254 icmp_seq=2 ttl=61 time=17.639 ms
84 bytes from 203.255.255.254 icmp_seq=3 ttl=61 time=14.777 ms
84 bytes from 203.255.255.254 icmp_seq=4 ttl=61 time=13.373 ms
84 bytes from 203.255.255.254 icmp_seq=5 ttl=61 time=20.828 ms
```

After the attack against 203.255.255.254 began and the trigger was enabled,

PE01

```
PE01#sh ip route bgp | be Gate
Gateway of last resort is not set

      81.0.0.0/30 is subnetted, 1 subnets
B        81.84.85.252 [200/0] via 172.16.255.3, 00:08:14
      191.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
B        191.0.0.252/30 [200/0] via 172.16.255.2, 00:07:53
      203.255.255.0/24 is variably subnetted, 2 subnets, 2 masks
B        203.255.255.252/30 [200/0] via 172.16.255.3, 00:08:14
B        203.255.255.254/32 [200/0] via 192.0.2.254, 00:00:08
```

PE02

```
PE02#sh ip route bgp | be Gate
Gateway of last resort is not set

      81.0.0.0/30 is subnetted, 1 subnets
B        81.84.85.252 [200/0] via 172.16.255.3, 00:08:58
      191.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
B        191.0.0.0/30 [200/0] via 172.16.255.1, 00:08:49
      203.255.255.0/24 is variably subnetted, 2 subnets, 2 masks
B        203.255.255.252/30 [200/0] via 172.16.255.3, 00:08:58
B        203.255.255.254/32 [200/0] via 192.0.2.254, 00:00:53
```

ATTACKER PC RED

```
RED> ping 203.255.255.254

*191.0.0.1 icmp_seq=1 ttl=254 time=20.072 ms (ICMP type:3, code:1, Destination host unreachable)
*191.0.0.1 icmp_seq=2 ttl=254 time=13.725 ms (ICMP type:3, code:1, Destination host unreachable)
*191.0.0.1 icmp_seq=3 ttl=254 time=13.380 ms (ICMP type:3, code:1, Destination host unreachable)
*191.0.0.1 icmp_seq=4 ttl=254 time=21.391 ms (ICMP type:3, code:1, Destination host unreachable)
*191.0.0.1 icmp_seq=5 ttl=254 time=21.077 ms (ICMP type:3, code:1, Destination host unreachable)

RED> ping 81.84.85.254

84 bytes from 81.84.85.254 icmp_seq=1 ttl=60 time=53.564 ms
84 bytes from 81.84.85.254 icmp_seq=2 ttl=60 time=13.224 ms
84 bytes from 81.84.85.254 icmp_seq=3 ttl=60 time=17.186 ms
84 bytes from 81.84.85.254 icmp_seq=4 ttl=60 time=17.265 ms
84 bytes from 81.84.85.254 icmp_seq=5 ttl=60 time=12.368 ms
```

USER PC BLUE

```
BLUE> ping 203.255.255.254

*191.0.0.253 icmp_seq=1 ttl=254 time=20.084 ms (ICMP type:3, code:1, Destination host unreachable)
*191.0.0.253 icmp_seq=2 ttl=254 time=14.663 ms (ICMP type:3, code:1, Destination host unreachable)
*191.0.0.253 icmp_seq=3 ttl=254 time=19.936 ms (ICMP type:3, code:1, Destination host unreachable)
*191.0.0.253 icmp_seq=4 ttl=254 time=11.711 ms (ICMP type:3, code:1, Destination host unreachable)
*191.0.0.253 icmp_seq=5 ttl=254 time=13.574 ms (ICMP type:3, code:1, Destination host unreachable)

BLUE> ping 81.84.85.254

84 bytes from 81.84.85.254 icmp_seq=1 ttl=61 time=19.921 ms
84 bytes from 81.84.85.254 icmp_seq=2 ttl=61 time=11.724 ms
84 bytes from 81.84.85.254 icmp_seq=3 ttl=61 time=10.833 ms
84 bytes from 81.84.85.254 icmp_seq=4 ttl=61 time=11.420 ms
84 bytes from 81.84.85.254 icmp_seq=5 ttl=61 time=14.234 ms
```

23:23, Fri, Jun 26, 2026, GMT+3 **Ko Lwin (Network)**