DDOS MITIGATION

1. **Mục tiêu**

- Hỗ trợ các thành viên, điều hướng lưu lượng tấn công DDoS giữa các hệ thống mạng của thành viên kết nối đa phương, song phương trên VNIX sử dụng dịch vụ Blackholing.

2. **Dịch vụ Blackholing tại VNIX**

- Dịch vụ Blackholing VNIX được triển khai tại các điểm ở Hà Nội, Hồ Chí Minh và Đà Nẵng để giảm thiểu và điều hướng lưu lượng tấn công DDoS qua các thành viên kết nối VNIX. Sử dụng kỹ thuật RTBH (Remote Triggered Black Hole Filtering) dựa trên địa chỉ IP bị tấn công. Gán nhãn thuộc tính BGP Communities (Blackhole Community được mô tả theo RFC 7999); chuyển các gói tin bị tấn công tới địa chỉ Blackhole và loại bỏ chúng.
- Hoạt động trên mô hình kết nối đa phương, song phương VNIX

3. **Nguyên lý hoạt động**

- Trên hạ tầng VNIX xây dựng hệ Trigger Router với nhiệm vụ nhận, thay đổi thông tin định tuyến và quảng bá các thông tin định tuyến của nạn nhân, nhằm hỗ trợ lái lưu lương tấn công DDoS vào Blackhole
- Thành viên tham gia vào hệ thống Blackholing VNIX cần thực hiện peering với Trigger Router VNIX theo thông tin cụ thể như sau:

VNIX	ASN	Trigger-VNIX IPv4	Trigger-VNIX IPv6	Blackhole next-hop IPv4	Blackhole next-hop IPv6	BGP Blackhole Community
HÀ NỘI	23899	218.100.10.252	2001:7FA:6::252	218.100.10.253	2001:7FA:6::253	65535:666
HỒ CHÍ MINH	23962	218.100.14.252	2001:DE8:A::252	218.100.14.253	2001:DE8:A::253	
ĐÀ NẴNG	56156	218.100.60.252	2001:DE8:3::252	218.100.60.253	2001:DE8:3::253	

- Khi hoạt động, các thông tin định tuyến gán nhãn blackhole sẽ được Trigger Router VNIX chấp nhận và thay đổi địa chỉ IP Next-hop bởi địa chỉ Blackhole và quảng bá lại cho Router của thành viên. Router của thành viên cập nhật bảng định tuyến mới với thông tin, lúc này các lưu lượng tấn công sẽ được lái về Blackhole .

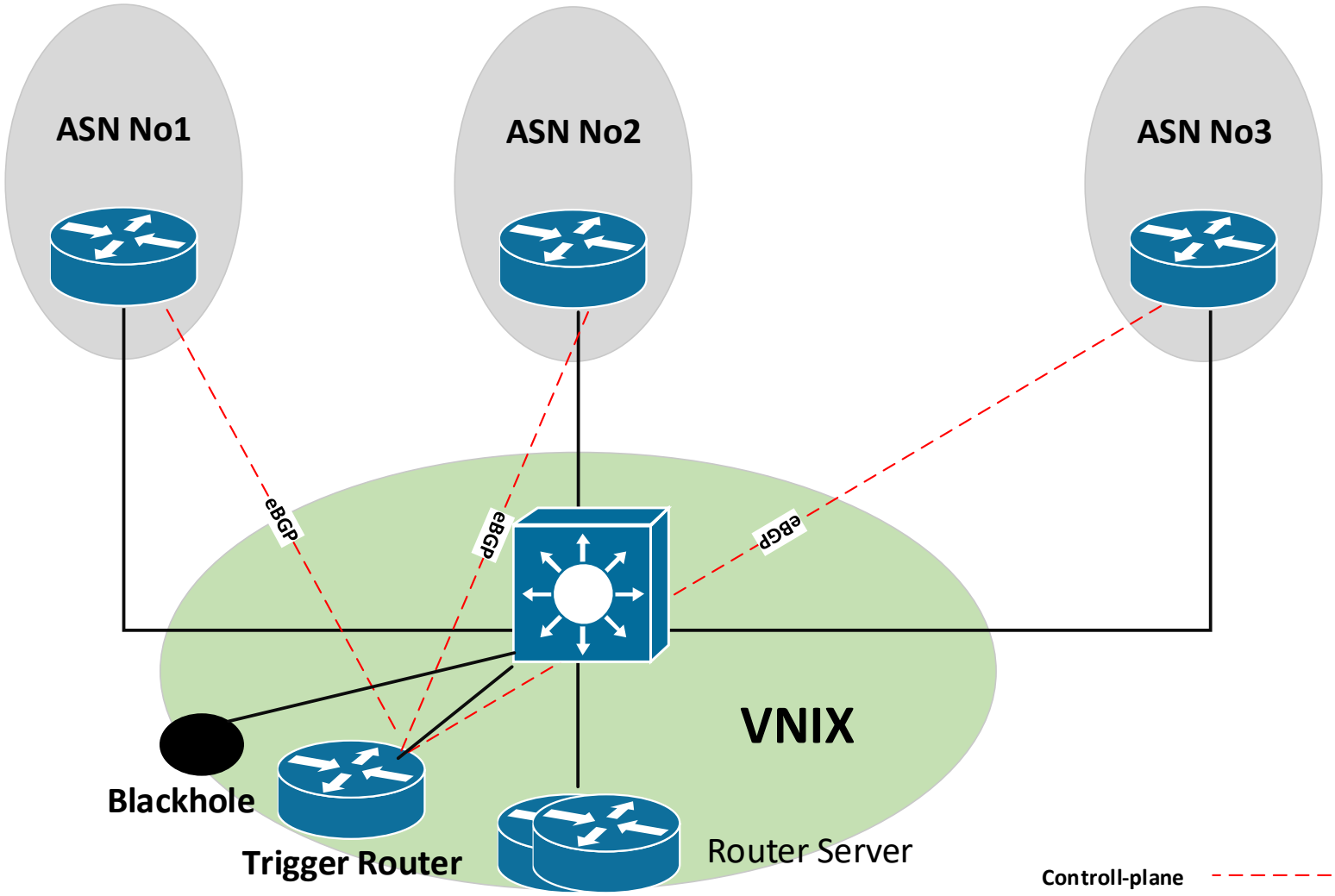
Lưu lượng tấn công gửi tới MAC Address Blackhole VNIX sẻ được loại bỏ.

Trigger Router VNIX chấp nhận các thông tin quảng bá như sau:

- Các thông tin định tuyến được gắn nhãn 65535:666
- /24 = < IPv4 prefix length = < /32
- /64 = < IPv6 prefix length = < /128

4. Mô tả hoạt động thực tế

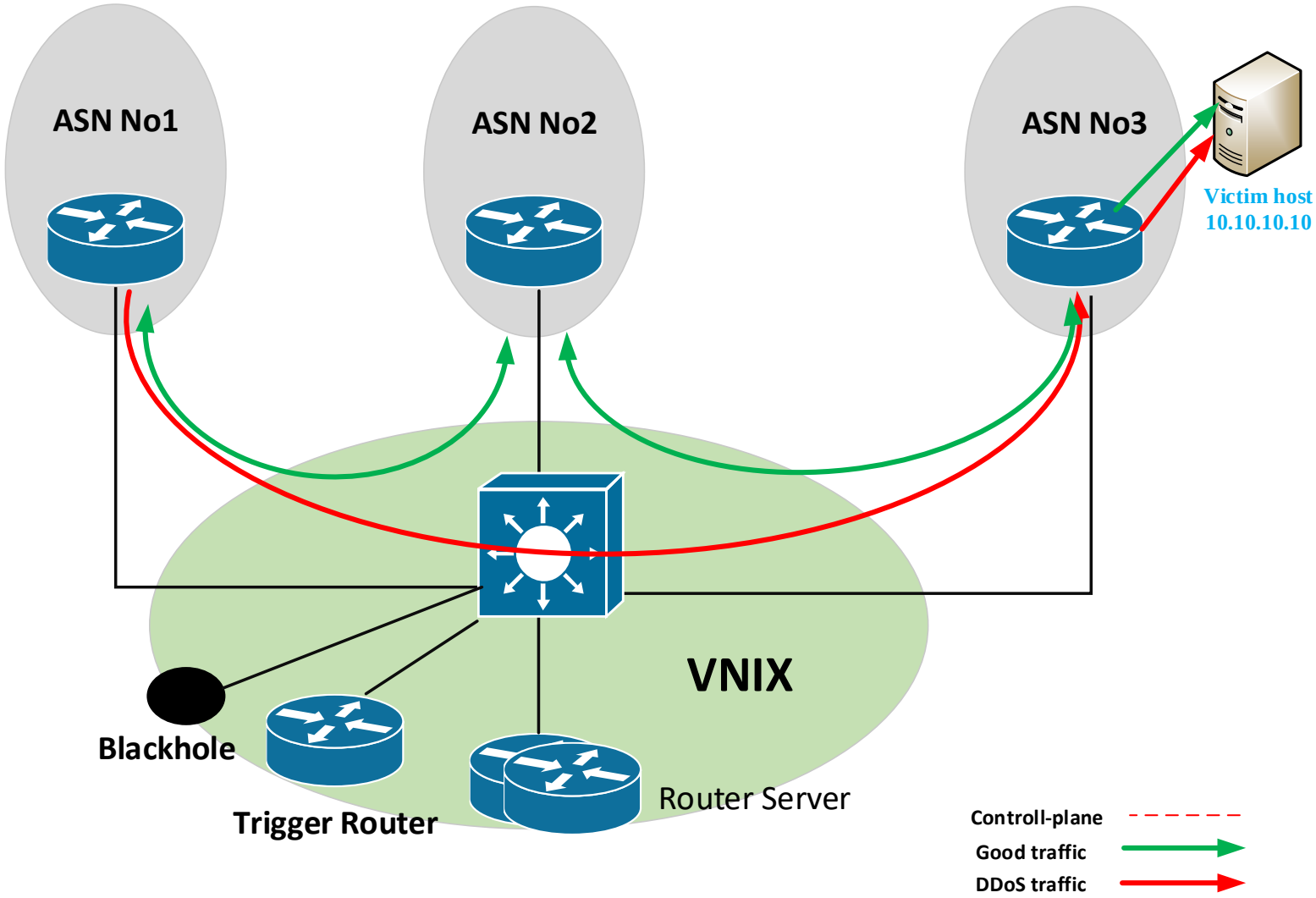
- Mô hình peering: Để tham gia vào hệ thống **Blackholing VNIX** , các Router biên của thành viên thực hiện peering eBGP với Trigger Router VNIX (Cấu hình theo hướng dẫn tại mục 6)



- Trạng thái hoạt động bình thường: Trong trạng thái bình thường (không xảy ra tấn công DDoS) trên VNIX, Router biên của các thành viên không quảng bá và nhận thông tin định tuyến từ Trigger Router VNIX; Hoạt động trao đổi lưu lượng diễn ra

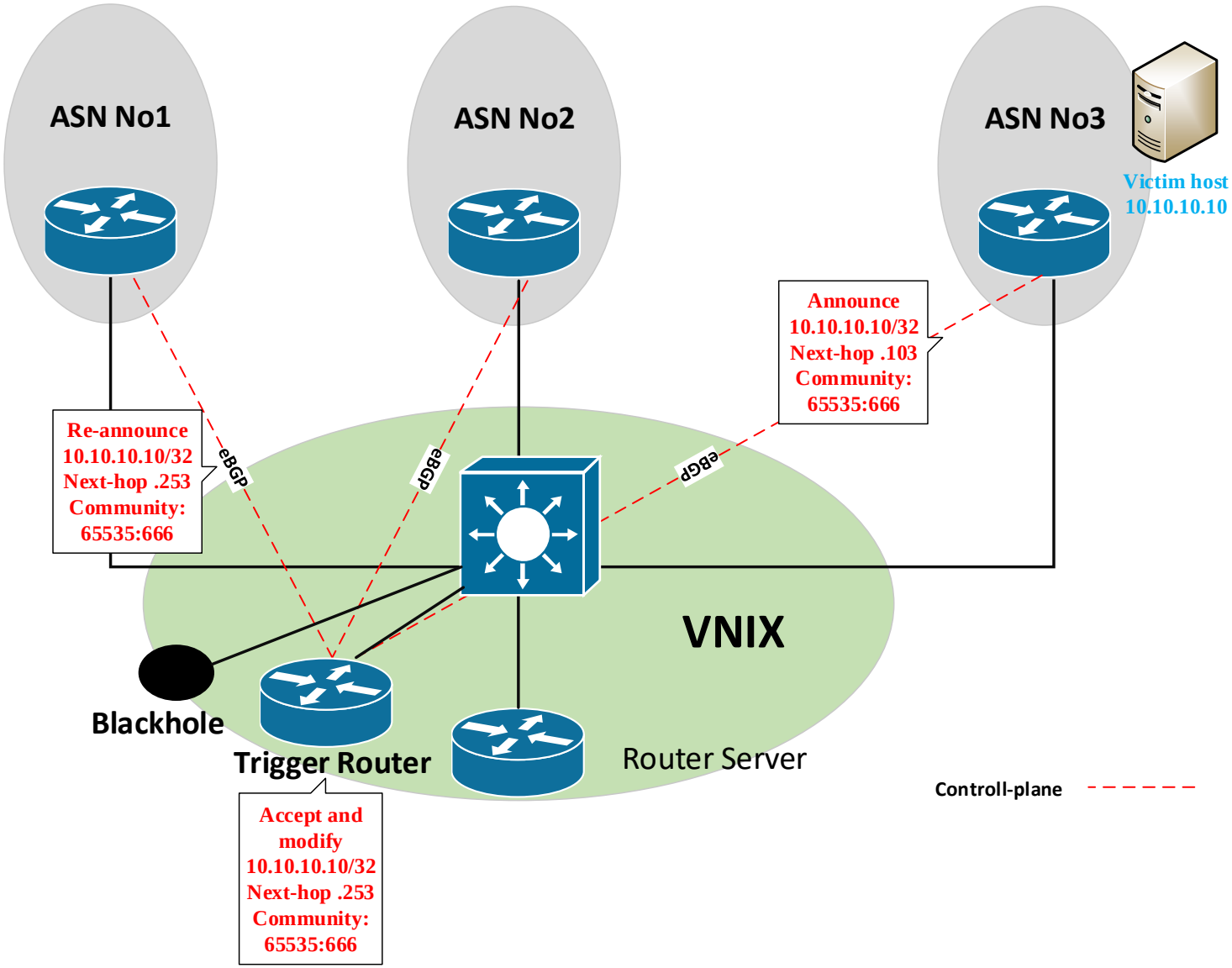
bình thường (Router Rerver điều khiển định tuyến, lưu lượng trao đổi chuyển tiếp giữa các thành viên thông qua hệ thống chuyển mạch trung tâm VNIX)

- Trong trạng thái bị tấn công: **Victim** tại ASN No3 phát hiện lưu lượng tấn công DDoS vào máy chủ dịch vụ thuộc hệ thống mạng của mình có địa chỉ 10.10.10.10

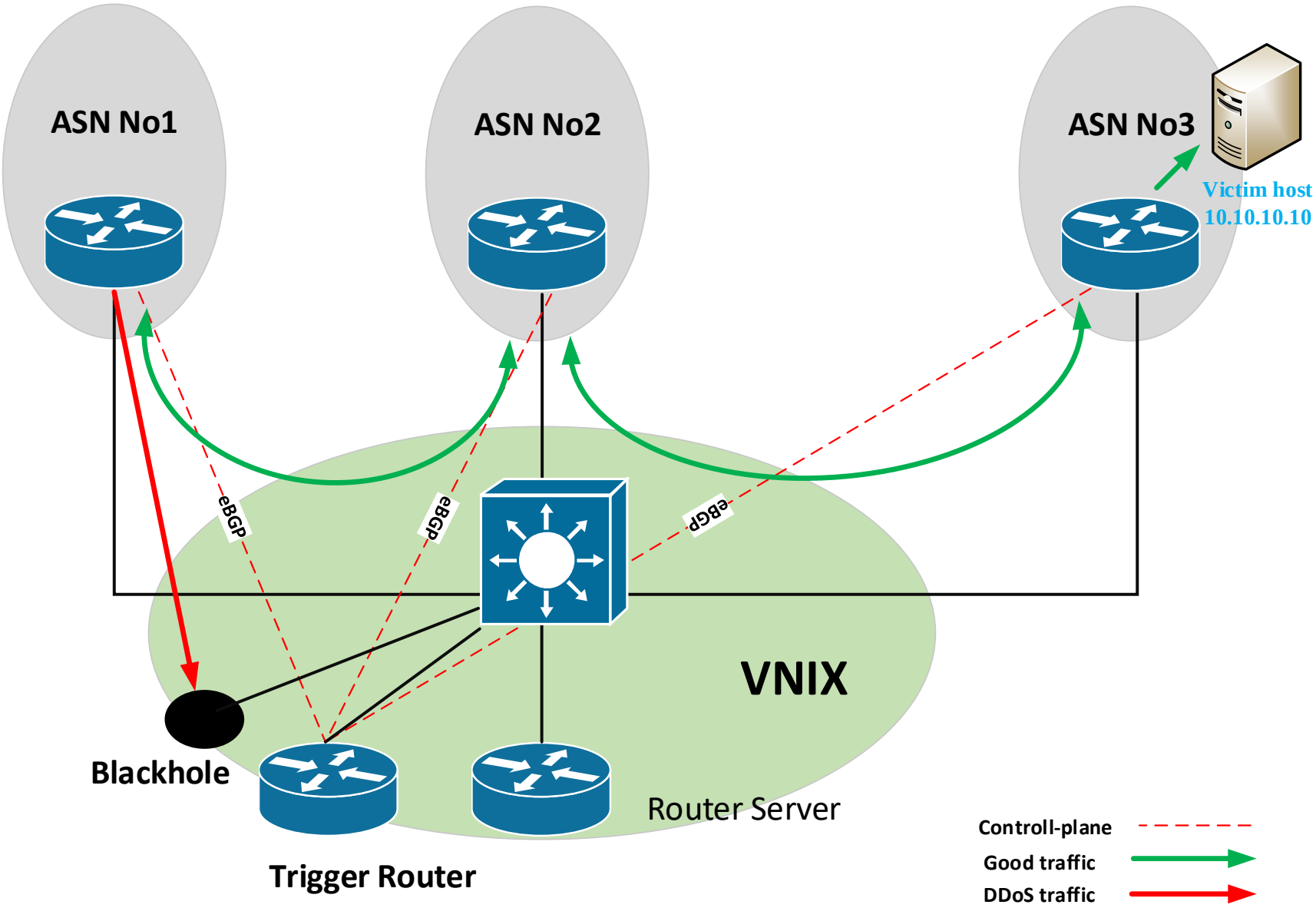


- Xử lý tấn công DDoS:

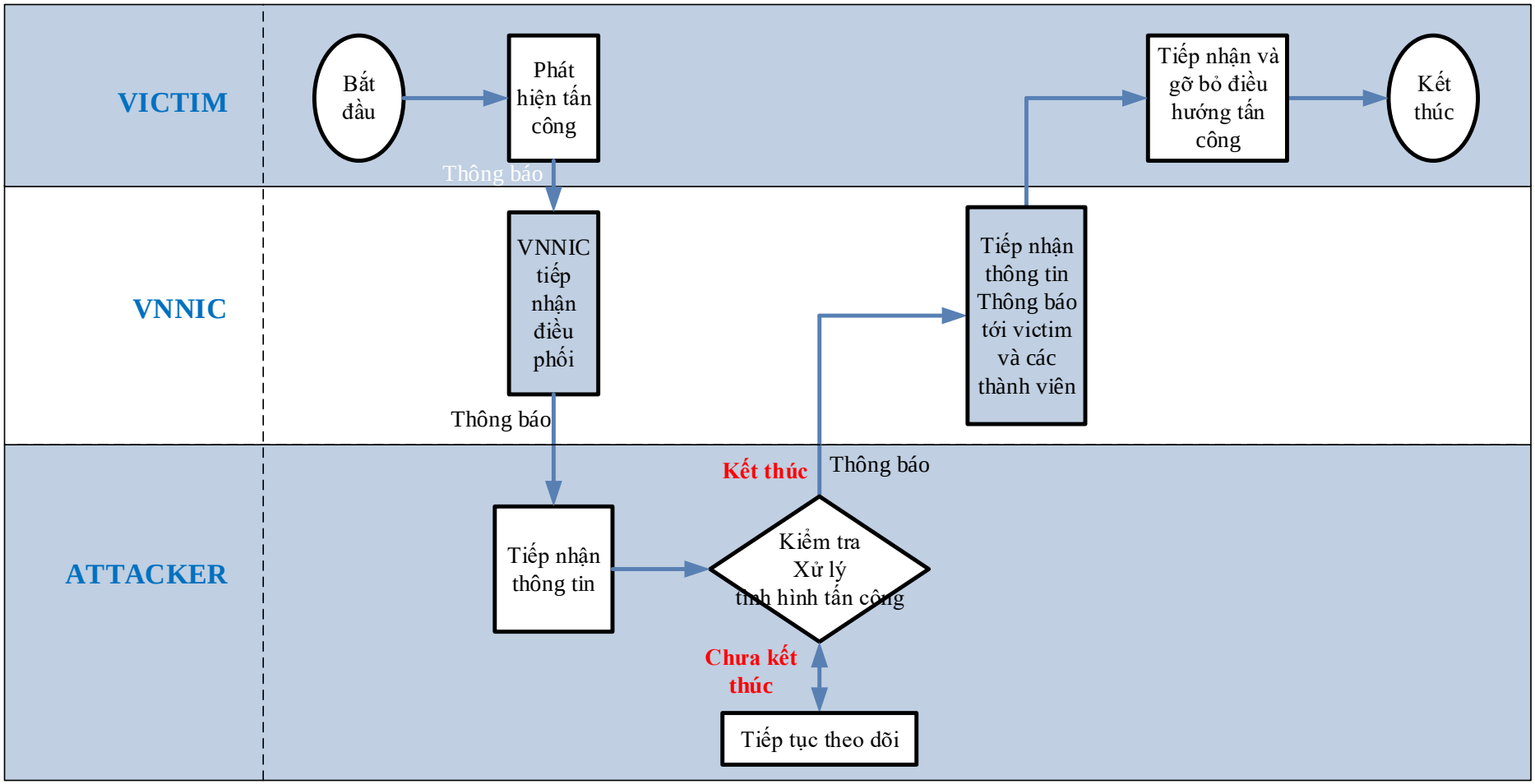
- **VICTIM:**
  - Để ngăn chặn tấn công đến với hệ thống mạng của mình, tại Router ASN No3 thực hiện quảng bá IP 10.10.10.10/32 với community 65535:666 tới Trigger Router VNIX
  - Để chặn tấn công từ một thành viên xác định thì sử dụng với community 65535:666 kèm với các community do Trigger Router VNIX (ví dụ trường hợp này là *community 65535:666 ASN-VNIX: ASNNo1*)


ASN No1
ASN No2
ASN No3
Victim host
10.10.10.10
Announce
10.10.10.10/32
Next-hop .103
Community:
65535:666
Re-announce
10.10.10.10/32
Next-hop .253
Community:
65535:666
eBGP
eBGP
eBGP
VNIX
Blackhole
Trigger Router
Router Server
Accept and
modify
10.10.10.10/32
Next-hop .253
Community:
65535:666
Controll-plane

- **VNNIC:**
  - Trigger Router VNIX tiếp nhận thông tin định tuyến và thực hiện thay đổi ip next-hop
  - Tự động quảng bá tới các thành viên do VICTIM định nghĩa trong thuộc tính community.
- **Attacker:**
  - Tự động điều chỉnh định tuyến theo cơ chế hoạt động (đã thiết lập ban đầu)


ASN No1
ASN No2
ASN No3
Victim host
10.10.10.10
eBGP
eBGP
eBGP
VNIX
Blackhole
Router Server
Trigger Router
Controll-plane
Good traffic
DDoS traffic

5. Quy trình thực hiện phối hợp xử lý tấn công:
   Các thành phần tham gia:
   - Thành viên có hệ thống mạng dịch vụ bị tấn công: VICTIM
   - Đơn vị quản lý VNIX, điều phối: VNNIC
   - Thành viên có hệ thống mạng là nguồn tấn công: ATTACKER



Bước 1: Bắt đầu phát hiện tấn công DDoS

- Victim: thành viên bị tấn công DDoS thông báo tới VNNIC

Bước 2: VNNIC tiếp nhận thông tin và điều phối

- Victim: thông báo VNNIC hỗ trợ xử lý thông qua điện thoại, email và servicedesk. Mô tả về cuộc tấn công: hình ảnh giám sát, IP tấn công/IP bị tấn công.
- VNNIC tiếp nhận thông tin và thông báo tới các thành viên liên quan để phối hợp xử lý

Bước 3: Kiểm tra và xử lý tấn công:

- Victim: thực hiện cầu hình điều hướng lưu lượng tấn công về Blackhole của VNIX (*tham khảo hướng dẫn tại mục 6*)
- Attacker: tiếp nhận thông tin và truy vết nguồn tấn công để xử lý
- Các bên liên quan theo dõi cuộc tấn công và triển khai các biện pháp ngăn chặn

Bước 4: Kết thúc cuộc tấn công

Khi không còn lưu lượng tấn công từ vùng mạng của các thành viên đi qua VNIX tới victim.

- Attacker: xác nhận đã truy vết và xử lý dứt điểm nguồn tấn công, thông báo về VNNIC
- VNNIC: thông báo kết thúc tấn công DDoS
- Victim: thực hiện cấu hình trả lại hoạt động định tuyến ban đầu.

Bước 5: kết thúc

6. Hướng dẫn cài đặt

a. Thiết lập Peering BGP Trigger Router VNIX

```
router bgp <ASN-ISP>
neighbor <IPv4-Trigger-VNIX> remote-as <ASN-VNIX>      /" để peering IPv6 với Router Trigger"/
```

neighbor <IPv4-Trigger-VNIX> description Peer-RTBH-VNIX-v4 /" Mô tả peering"/

neighbor <IPv4-Trigger-VNIX> version 4 /"Xác định version BGP"/

neighbor <IPv6-Trigger-VNIX> remote-as <ASN-VNIX> /"để peering IPv6 với Router Trigger"/

neighbor <IPv6-Trigger-VNIX> description Peer-RTBH-VNIX-v6 /" Mô tả peering "/

neighbor <IPv6-Trigger-VNIX> version 4 /" Xác định version BGP"/

address-family ipv4

neighbor <IPv4-Trigger-VNIX> activate /"Kích hoạt peering"/

neighbor <IPv4-Trigger-VNIX> send-community /" gửi thuộc tính comunity"/

neighbor <IPv4-Trigger-VNIX> route-map RM_VNIX_BLACKHOLE_IN_v4 in /" chính sách nhận định tuyến"/

neighbor <IPv4-Trigger-VNIX> route-map RM_VNIX_BLACKHOLE_OUT_v4 out /" chính sách quảng bá"/

address-family ipv6 /"tương tự IPv4"/

neighbor <IPv6-Trigger-VNIX> activate

neighbor <IPv6-Trigger-VNIX> send-community

neighbor <IPv6-Trigger-VNIX> route-map RM_VNIX_BLACKHOLE_IN_v6 in

neighbor <IPv6-Trigger-VNIX> route-map RM_VNIX_BLACKHOLE_OUT_v6 out

----------IPv4----------

route-map RM_VNIX_BLACKHOLE_OUT_v4 permit 10

match ip address prefix-list PL_VNIX_BLACKHOLE_OUT_4

set community 65535:666 /"thuộc tính community quảng bá cho tất cả - Các thuộc tính khác xem công bố trên website"/

----------IPv6----------

route-map RM_VNIX_BLACKHOLE_OUT_v6 permit 10

match ipv6 address prefix-list PL_VNIX_BLACKHOLE_OUT_6

set community 65535:666 /"thuộc tính community quảng bá cho tất cả - Các thuộc tính khác xem công bố trên website"/

----------IPv4----------

route-map RM_VNIX_BLACKHOLE_IN_v4 permit 10

match ip address prefix-list PL_VNIX_BLACKHOLE_IN_4

match community Blackhole

route-map RM_VNIX_BLACKHOLE_IN_v4 deny 20

match ip address prefix-list PL_VNIX_BLACKHOLE_IN_4

route-map RM_VNIX_BLACKHOLE_IN_v4 permit 30

----------IPv6----------

route-map RM_VNIX_BLACKHOLE_IN_v6 permit 10

match ipv6 address prefix-list PL_VNIX_BLACKHOLE_IN_6

match community Blackhole

route-map RM_VNIX_BLACKHOLE_IN_v6 deny 20

match ipv6 address prefix-list PL_VNIX_BLACKHOLE_IN_6

route-map RM_VNIX_BLACKHOLE_IN_v6 permit 30

----------Prefix-list-Fillter-BLACKHOLE-v4-IN----------

ip prefix-list PL_VNIX_BLACKHOLE_IN_4 seq 10 permit 0.0.0.0/24 le 32

----------Prefix-list-Fillter-BLACKHOLE-v6-IN----------

ipv6 prefix-list PL_VNIX_BLACKHOLE_IN_6 seq 10 permit ::/64 le 128

b. Cấu hình quảng bá route khi xảy ra tấn công DDoS

router bgp <ASN-ISP>

address-family ipv4

network <IP victim> mask 255.255.255.255

address-family ipv6

network <IP victim>/128

----------Prefix-list-Fillter-BLACKHOLE-v4-OUT----------

ip prefix-list PL_VNIX_BLACKHOLE_OUT_4 seq 10 permit <IPv4 victim/32>

ip route <ipv4 victim/32> null 0

----------Prefix-list-Fillter-BLACKHOLE-v6-OUT----------

ipv6 prefix-list PL_VNIX_BLACKHOLE_OUT_6 seq 10 permit <IPv6 victim/128>

ipv6 route <ipv6 victim/128> null 0