BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

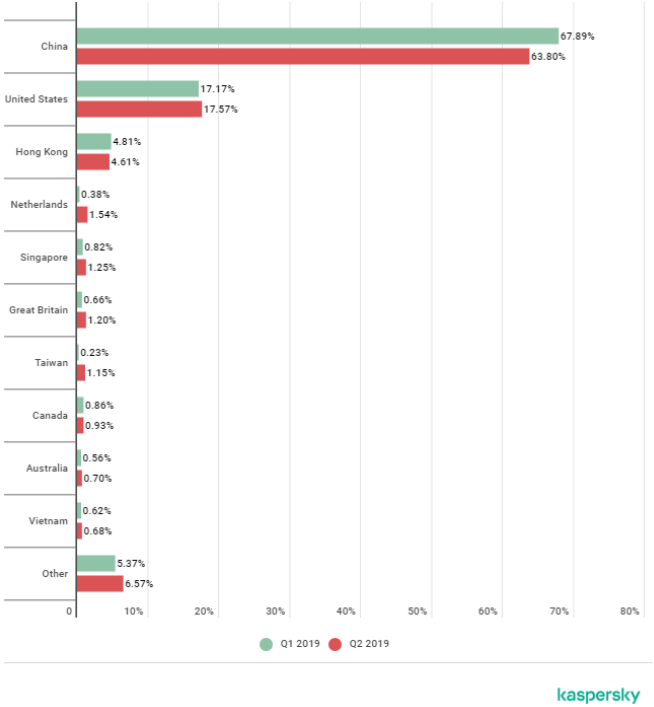
MINISTRY OF INFORMATION AND COMUNICATIONS
VIETNAM INTERNET NETWORK INFORMATION CENTER

DDOS MITIGATION AT VNIX PLATFORM

Nha Trang | Aug, 2019

DDoS Overview

- DDoS Overview



VNEXPRESS
Báo tiếng Việt nhiều người xem nhất

CƠ HỘI
CHUYẾN DU LỊCH
& XEM BÓNG ĐÁ

Video | Thời sự | Góc nhìn | Thế giới | Kinh doanh | Giải trí | Thể thao | Pháp luật | Giác

Đời sống số | Sản phẩm | Điện tử gia dụng | Kinh nghiệm | Video | OPPO Renc

Số hóa | Đời sống số | Bảo mật | Làng game

Thứ sáu, 3/5/2019, 15:10 (GMT+7)

Số cuộc tấn công DDoS từ Việt Nam nhiều thứ sáu thế giới

Số lượng các cuộc tấn công từ chối dịch vụ (DDoS) xuất phát từ Việt Nam chỉ đứng sau các nước Trung Quốc, Mỹ, Pháp, Nga và Brazil.

Tại hội thảo chuyên về tấn công DDoS do Cục An toàn Thông tin - Bộ Thông tin và Truyền thông tổ chức ngày 3/5, công ty an ninh mạng Nexusguard cho biết Việt Nam đang có vị trí "đáng quan ngại" trong bức tranh DDoS toàn cầu.

Cụ thể, Việt Nam chiếm tỷ lệ 3,53% về nguồn tấn công DDoS trên toàn thế giới trong quý IV/2018, đứng thứ sáu toàn cầu và thứ hai tại khu vực châu Á - Thái Bình Dương sau Trung Quốc (9,52%) và trên Ấn Độ, Indonesia.

Ông Nguyễn Huy Dũng, Quyền Cục trưởng Cục An toàn Thông tin, cho biết, các cuộc tấn công DDoS ngày càng dễ thực hiện nên việc phòng thủ rất khó. Cục An toàn thông tin và Trung tâm Giám sát an toàn không gian mạng quốc gia đã xây dựng hệ thống chống tấn công mạng Internet Việt Nam. Trong hệ thống đó có một chức năng là liên kết với các doanh nghiệp và nhà mạng để điều phối, xử lý những cuộc tấn công từ chối dịch vụ nhằm vào hệ thống thông tin quan trọng tại Việt Nam.

ictnews 0888.911.911

THỜI SỰ | VIỄN THÔNG | INTERNET | CNTT | KINH DOANH

Quản lý công việ
hằng ngày

Mới nhất:

Trang chủ › CNTT › Cuộc sống thông minh
› Tủ lạnh, nồi cơm điện, tivi thông minh... cũng là nguồn tấn công DDoS

19:59, 04/05/2019

Phản hồi với ICTnews

Tủ lạnh, nồi cơm điện, tivi thông minh... cũng là nguồn tấn công DDoS

lạnh, nồi cơm điện, tivi thông minh... cũng là nguồn tấn 00:00

ICTNEWS **Nhấn mạnh nguy cơ bị tấn công mạng, trở thành nguồn tấn công DDoS của các thiết bị IoT ngày càng nghiêm trọng, nghiên cứu của NexusGuard chỉ ra rằng, các thiết bị gia dụng thông minh như tủ lạnh, nồi cơm điện, tivi thông minh... cũng là nguồn tấn công DDoS tiêu biểu.**

https://securelist.com/ddos-report-q2-2019/91934/

DDoS Mitigation at VNIX platform

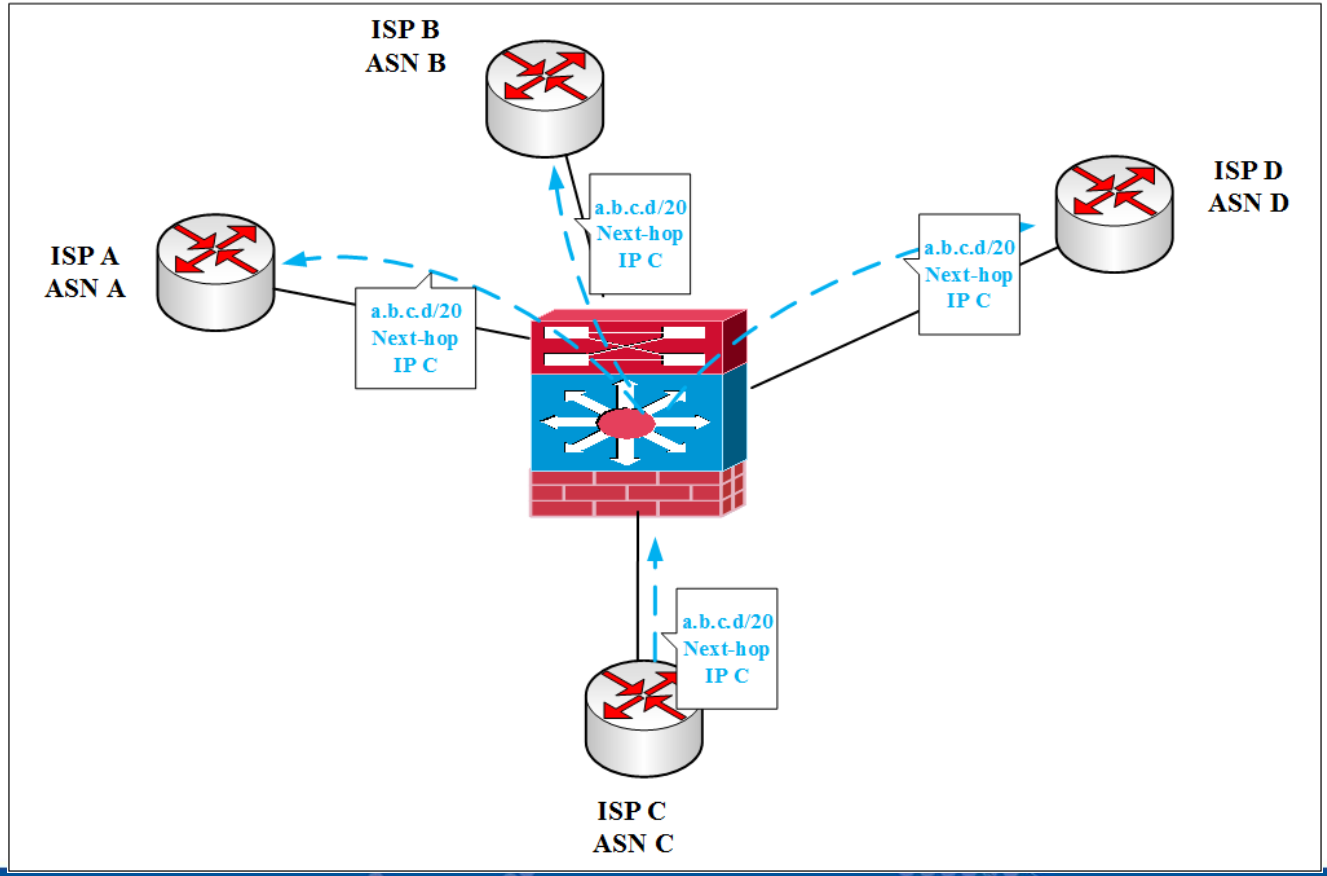
- Purpose
  - Develop a community with aim to minimize DDoS attacks on VNIX.
  - Help to minimize DDoS attack traffic amongst members' network systems over VNIX infrastructure.

- Deployment status
  - Blackholing has already been rolled out in 3 VNIX locations.
  - RTBH, also referred to as BGP blackholing, is an operational DDoS mitigation technique.
  - Builds upon the BGP communities attribute, to discards attack traffic.

DDoS Mitigation at VNIX platform

- How it works
  - Initially

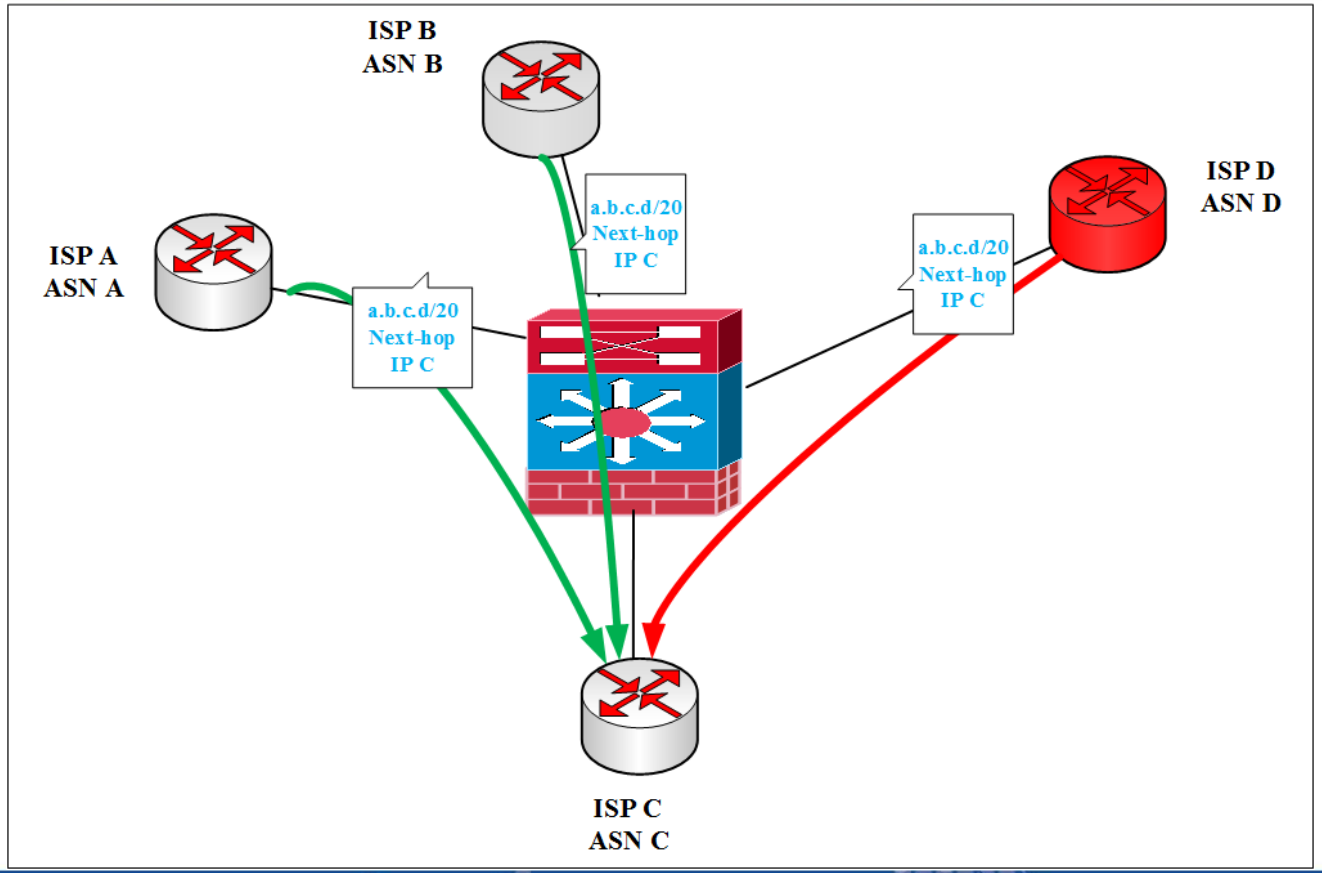
Control-Plane



DDoS Mitigation at VNIX platform

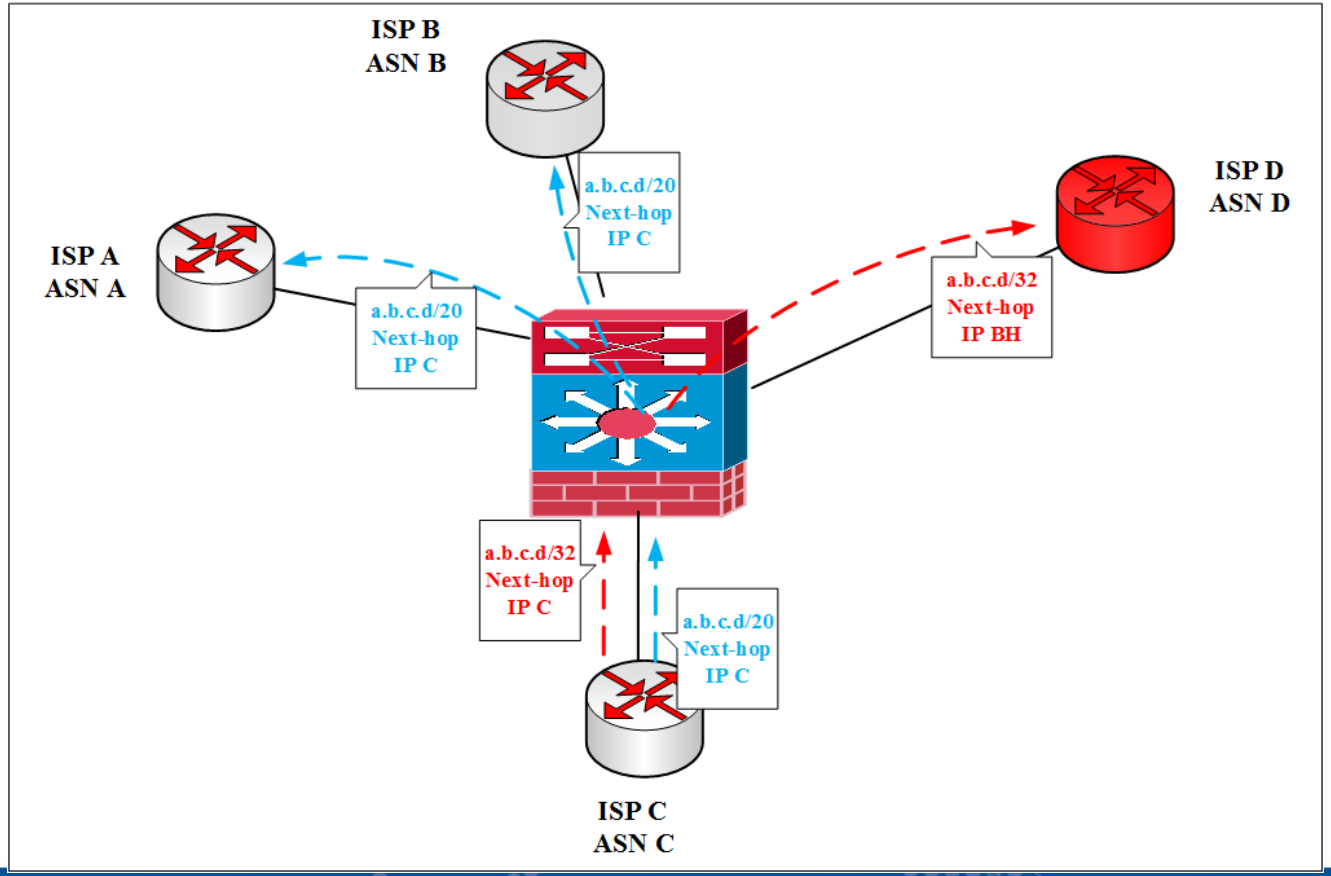
- How it works
  - Initially

Data-Plane



DDoS Mitigation at VNIX platform

- How it works
  - Under DDoS Attack Control-Plane

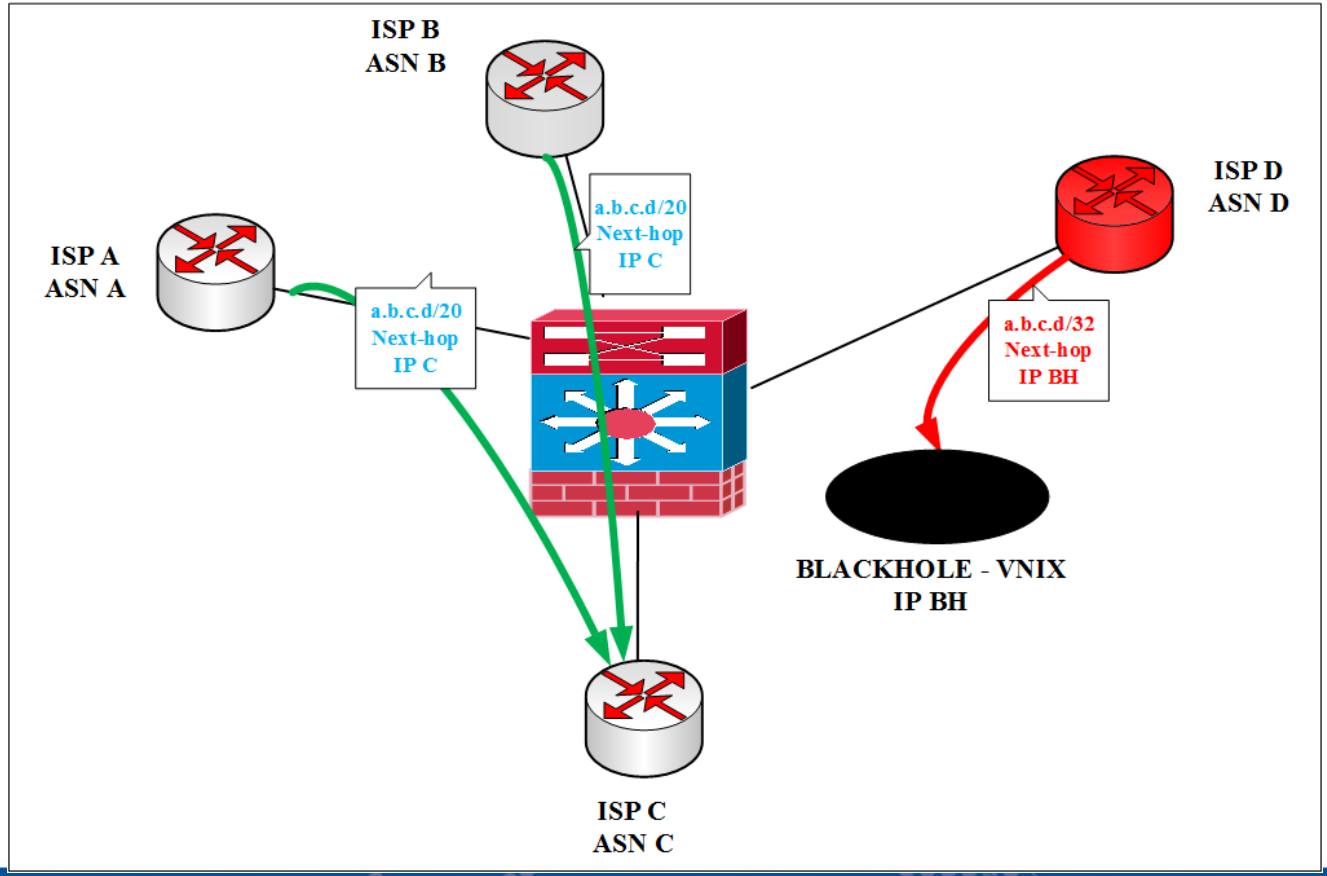


DDoS Mitigation at VNIX platform

- How it works
  - Under DDoS Attack

Data-Plane

Traffic attack into blackhole



DDoS Mitigation at VNIX platform

- Peering information

VNIX	RS-VNIX IPv4	RS-VNIX IPv6	Trigger-VNIX IPv4	Trigger-VNIX IPv6	Blackhole next-hop IPv4	Blackhole next-hop IPv6	BGP Blackhole Community
HÀ NỘI	218.100.10.1 218.100.10.254	2001:7FA:6::1 2001:7FA:6::254	218.100.10.252	2001:7FA:6::252	218.100.10.253	2001:7FA:6::253	65535:666
HỒ CHÍ MINH	218.100.14.1 218.100.14.254	2001:DE8:A::1 2001:DE8:A::254	218.100.14.252	2001:DE8:A::252	218.100.14.253	2001:DE8:A::253	
ĐÀ NẴNG	218.100.60.1 218.100.60.254	2001:DE8:3:1 2001:DE8:3::254	218.100.60.252	2001:DE8:3::252	218.100.60.253	2001:DE8:3::253	

- Allow Blackhole IP prefix
  - /24 = < IPv4 prefix length = < /32
  - /64 = < IPv6 prefix length = < /128

DDoS Mitigation at VNIX platform

➢ Configuration Guidelines

Peering BGP - Trigger-VNIX

```
router bgp <ASN-ISP>
 neighbor <IPv6-Trigger-VNIX> remote-as <ASN-VNIX>
 neighbor <IPv6-Trigger-VNIX> description Peer-RTBH-VNIX-v6
 neighbor <IPv6-Trigger-VNIX> version 4
 neighbor <IPv4-Trigger-VNIX> remote-as <ASN-VNIX>
 neighbor <IPv4-Trigger-VNIX> description Peer-RTBH-VNIX-v4
 neighbor <IPv4-Trigger-VNIX> version 4
address-family ipv4
 network <ipv4> mask <255.255.255.255>
 neighbor <IPv4-Trigger-VNIX> activate
 neighbor <IPv4-Trigger-VNIX> send-community
 neighbor <IPv4-Trigger-VNIX> route-map RM_VNIX_BLACKHOLE_IN_v4 in
 neighbor <IPv4-Trigger-VNIX> route-map RM_VNIX_BLACKHOLE_OUT_v4 out
address-family ipv6
 network <ipv6>/128
 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
```

DDoS Mitigation at VNIX platform

➢ Configuration Guidelines

Sending RTBH announcement

```
----------IPv4----------------------------------------------------
route-map RM_VNIX_BLACKHOLE_OUT_v4 permit 10
 match ip address prefix-list PL_VNIX_BLACKHOLE_OUT_4
 set community 65535:666
--------------------Prefix-list-Fillter-BLACKHOLE-v4-OUT----------------
ip prefix-list PL_VNIX_BLACKHOLE_OUT_4 seq 10 permit <IPv4/32>
ip route <ipv4/32> null 0


----------IPv6----------------------------------------------------
route-map RM_VNIX_BLACKHOLE_OUT_v6 permit 10
 match ipv6 address prefix-list PL_VNIX_BLACKHOLE_OUT_6
 set community 65535:666
--------------------Prefix-list-Fillter-BLACKHOLE-v6-OUT----------------
ipv6 prefix-list PL_VNIX_BLACKHOLE_OUT_6 seq 10 permit <IPv6/128>
ipv6 route <ipv6/128> null 0
```

Accept RTBH announcements by other peers

```
----------IPv4----------------------------------------------------
route-map RM_VNIX_BLACKHOLE_IN_v4 permit 10
 match ip address prefix-list PL_VNIX_BLACKHOLE_IN_4
 match community Blackhole-VNIX
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
--------------------Prefix-list-Fillter-BLACKHOLE-v4-IN----------------
ip prefix-list PL_VNIX_BLACKHOLE_IN_4 seq 10 permit 0.0.0.0/24 le 32

----------IPv6----------------------------------------------------
route-map RM_VNIX_BLACKHOLE_IN_v6 permit 10
 match ipv6 address prefix-list PL_VNIX_BLACKHOLE_IN_6
 match community Blackhole-VNIX
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-v6-IN----------------
ipv6 prefix-list PL_VNIX_BLACKHOLE_IN_6 seq 10 permit ::/64 le 128
```

DDoS Mitigation at VNIX platform

➢ Verification

Initially

```
Router-ISP#show ip bgp summary
Neighbor    V   AS  MsgRcvd  MsgSent   TblVer  InQ OutQ Up/Down   State/PfxRcd
218.100.14.252  4       23962    4305    8754   974339    0    0 2d23h          0

Router-ISP#show bgp ipv6 unicast summary
Neighbor      V   AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down   State/PfxRcd
2001:DE8:A::252 4       23962     581     655 1376672568    0    0 09:42:19       0

Router-ISP#show ip bgp neighbors 218.100.14.252 received-routes
Total number of prefixes 0

Router-ISP#show bgp ipv6 unicast neighbors 2001:de8:a::252 received-routes

Total number of prefixes 0
```

Under DDoS Attack

```
Router-ISP#show ip bgp summary
Neighbor    V   AS  MsgRcvd  MsgSent   TblVer  InQ OutQ Up/Down   State/PfxRcd
218.100.14.252  4       23962    4305    8754   974339    0    0 2d23h          1

Router-ISP#show bgp ipv6 unicast summary
Neighbor      V   AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down   State/PfxRcd
2001:DE8:A::252 4       23962     581     655 1376672568    0    0 09:42:19       1

Router-ISP#show ip bgp neighbors 218.100.14.252 received-routes
Network          Next Hop            Metric LocPrf Weight Path
 *>  112.78.13.237/32 218.100.14.253                       0 23962 45538 i

Total number of prefixes 1

Router-ISP#show bgp ipv6 unicast neighbors 2001:de8:a::252 received-routes
 Network          Next Hop            Metric LocPrf Weight Path
 *>  2405:9D80:4::5A/128
                    2001:DE8:A::253                       0 23962 45538 i

Total number of prefixes 1
```

THANKS YOU!