
# DP Service Provider Series

## BGP Security

### Remotely Triggered Black Hole Filtering

# Agenda

- RTBH Filtering Introduction
- Destination Based RTBH
- Source Based RTBH

# RTBH Introduction

- DoS mitigation technique
- Applicable within a single AS, usually the provider
- Leverages two main BGP attributes
  - BGP Next-Hop attribute
  - BGP Community attribute (Optional)
- Two separate implementations
  - First takes the victim offline – Destination Based RTBH
  - Second blocks the attacker – Source Based RTBH

# BGP Next-Hop Attribute

- Typically an IPv4 or an IPv6 address
- Affects the installation of the NLRI in the FIB
  - The NH is resolved via a recursive routing lookup
  - Ultimately an exit interface must be determined

```
 ~/packet_captures
▶ tshark -r NH_ATTRIBUTE.pcap -T json | grep "next_h\|nlri_pre"
              "bgp.update.path_attribute.next_hop": ”4.4.4.4"
              "bgp.nlri_prefix": "100.100.100.0"
```

```
RR6#show ip route 100.100.100.0
Routing entry for 100.100.100.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 8, type internal
  Last update from 4.4.4.4 00:00:17 ago
  Routing Descriptor Blocks:
  * 4.4.4.4, from 4.4.4.4, 00:00:17 ago
      Route metric is 0, traffic share count is 1
 AS Hops 1
      Route tag 8
      MPLS label: none
!
RR6#show ip cef 100.100.100.0/24 det
100.100.100.0/24, epoch 2, flags [rib only nolabel, rib defined all labels]
  recursive via 4.4.4.4
    nexthop 10.5.6.5 GigabitEthernet3 label 18-(local:22)
```



DecodingPackets

# BGP "Discard Route"

- A discard route is used to drop traffic
  - Usually a static route
  - All traffic that maps to this route in the FIB is dropped
  - Also called a Bit Bucket or a Null 0 route
- For BGP NLRIs, this can be achieved in two ways:
  - Programmatically (IOS-XR, Junos)
  - Setting the NH to a Discard Route (Most)

```
Routing entry for 100.100.100.0/24
  Known via "bgp 1", distance 200, metric 0, type internal
  Last update from 192.0.0.1 00:00:13 ago
  Routing Descriptor Blocks:
  * 192.0.2.1, from 1.1.1.3, 00:00:13 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: none
!
R1#show ip cef 100.100.100.0/24
100.100.100.0/24
  nexthop 192.0.2.1 Null0
```

# BGP Community Attribute

- An optional transitive BGP attribute
- Just a numerical value
  - Standard (32 Bits)
  - Extended (64 Bits)
- Used to group NLRIs associated with common policy
  - E.g. Set Local Preference to 500
  - E.g. Set Next Hop to discard
- Well-Known Communities
  - NO_EXPORT (65535:65281) is applicable to RTBH

# Destination Based RTBH

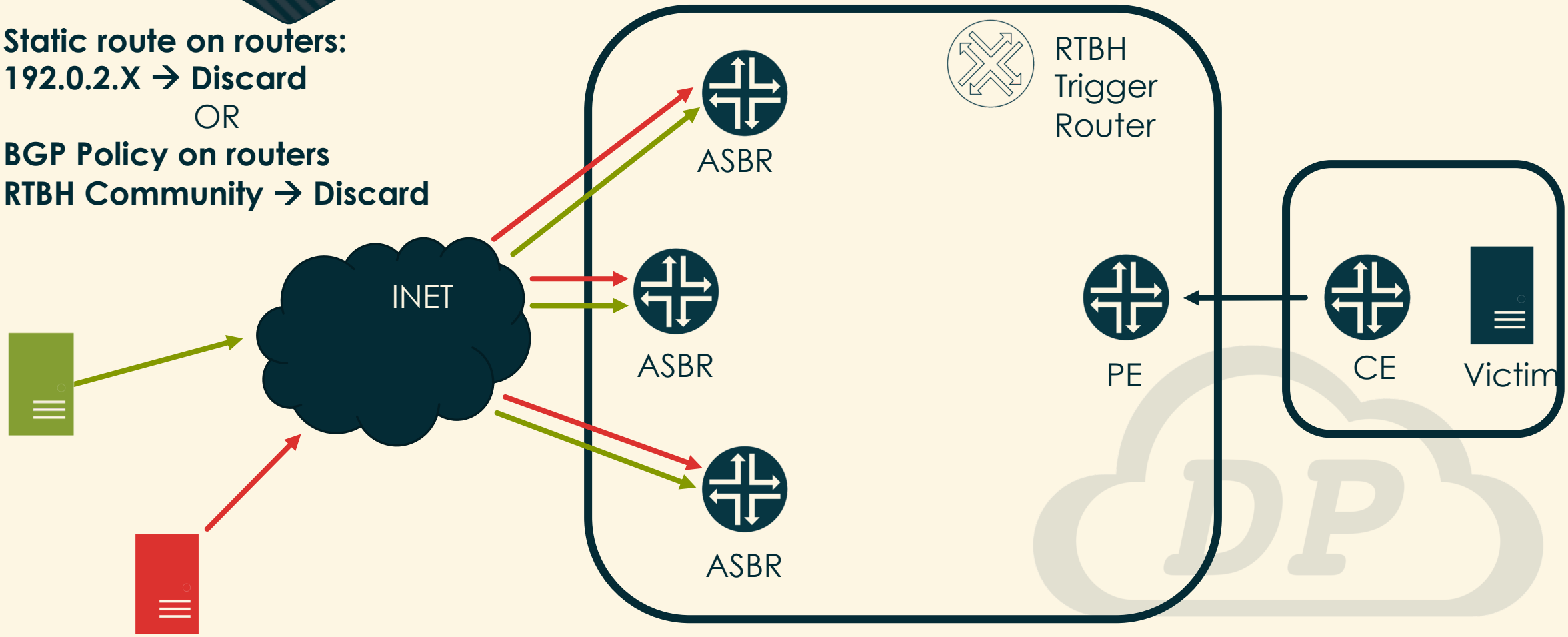
- Original implementation
- Filters/Drops all traffic to a particular destination
  - Typically, the victim of the DoS attack(s)
- The trigger router can be:
  - The CE
  - A dedicated RTBH Trigger Router
- Customer uses communities to signal
- Trigger router has multiple options
  - Communities or Next-Hop alteration

# Destination Based RTBH Operation

1. **Static route on routers:**
   **192.0.2.X → Discard**

   OR

2. **BGP Policy on routers**
   **RTBH Community → Discard**






DecodingPackets

# In Our Next Video…

- Destination Based RTBH Demo


# DP Service Provider Series

## BGP Security

Destination Based RTBH Demo

# Scenarios

- Topology overview
- Next-Hop attribute based RTBH
  - Trigger Router Originated
  - Customer Signaled
- Community attribute based RTBH
  - Trigger Router Originated
  - Customer Signaled

# In Our Next Video…

- Source Based RTBH
- Source Based RTBH Demo


# DP Service Provider Series

## BGP Security

Source Based RTBH

# Agenda

- Source Based RTBH Filtering Introduction
- Source Based RTBH Concepts
- Source Based RTBH Demo

# Source Based RTBH

- More granular (somewhat) implementation
- Filters/Drops all traffic from a particular source
  - Identified source of the DoS attack
- A dedicated Trigger router becomes necessary
- Trigger router has multiple options
  - Communities
  - Next-Hop alteration

# Source Based RTBH Concepts

- All concepts of Destination based RTBH apply
  - BGP discard route
  - BGP communities
- Additional concept of uRPF check is leveraged

# Unicast Reverse Path Forwarding Check

- General security feature (unrelated to RTBH)
- Router verifies reachability of **source** IP address
  - Strict Mode – **Egress** route must point out the **ingress** interface
  - Loose Mode – A **route must exist** in the FIB
    - S/RTBH implementations will consider "discard" routes invalid
    - The exact feature leveraged by S/RTBH
- Trigger router will originate an NLRI for malicious source
  - Edge routers will program a discard route in FIB
  - uRPF feature will drop the malicious traffic

# Source Based RTBH Operation

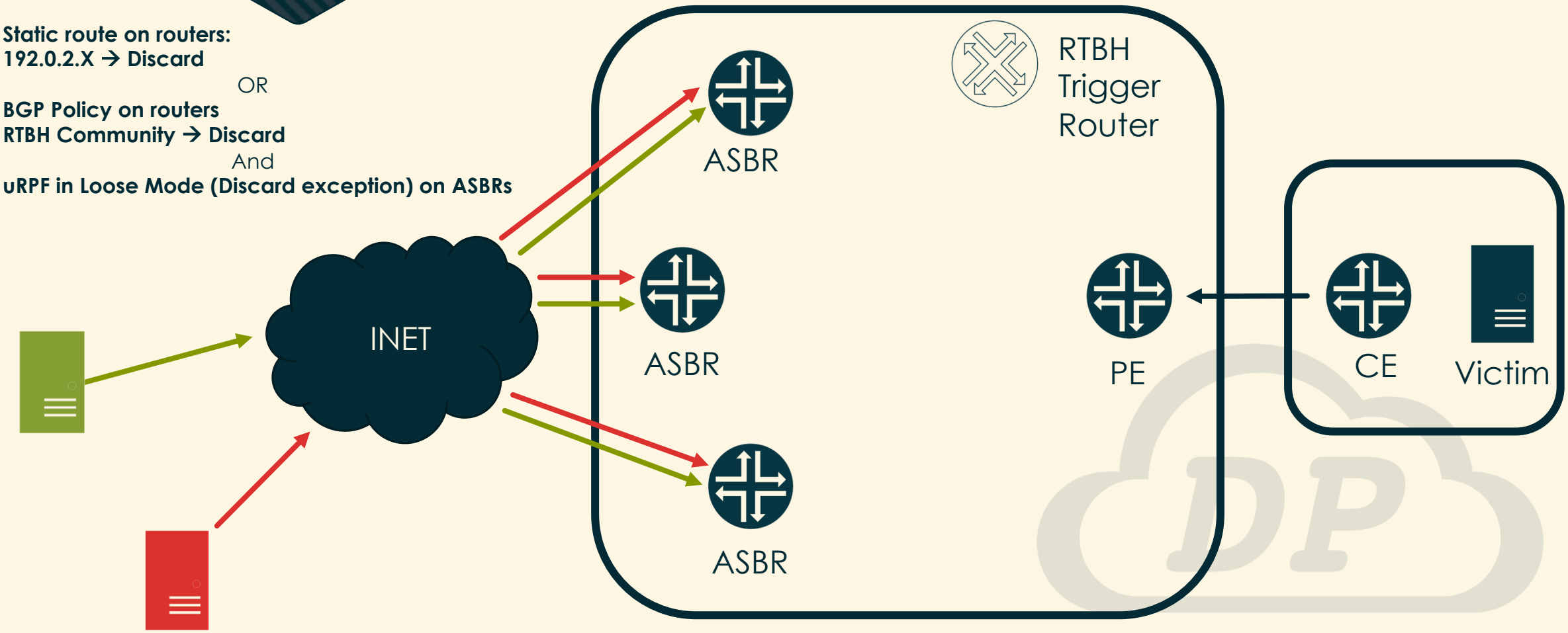
1. **Static route on routers:**
   **192.0.2.X → Discard**

OR

2. **BGP Policy on routers**
   **RTBH Community → Discard**

And

3. **uRPF in Loose Mode (Discard exception) on ASBRs**






DecodingPackets


# DP Service Provider Series

## BGP Security

Source Based RTBH Demo

# Scenarios

- Topology overview
- Next-Hop attribute based RTBH
  - Trigger Router Originated
  - ~~Customer Signaled~~
- Community attribute based RTBH
  - Trigger Router Originated
  - ~~Customer Signaled~~

# In Our Next Video…

- Introduction to BGP Flow Specification