ASR9000 Source−based Remotely Triggered Blackhole Filtering with RPL Next−hop Discard Configuration Example

Document ID: 116386

Contributed by Herve Bruyere, Luc De Ghein, and Jayant Kulkarni,
Cisco TAC Engineers.
Jul 29, 2013

Contents

Introduction

This document describes how to configure Remotely Triggered Blackhole (RTBH) on the Aggregation Services Router (ASR) 9000.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This information in this document is based on Cisco IOS−XR® and ASR 9000.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

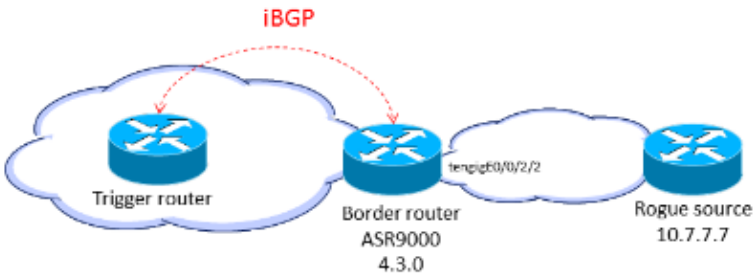
When you know the origin of an attack (for example, by an analysis of NetFlow data), you can apply containment mechanisms, such as Access Control Lists (ACLs). When attack traffic is detected and classified, you can create and deploy appropriate ACLs to the necessary routers. Because this manual process can be

time−consuming and complex, many people use Border Gateway Protocol (BGP) in order to propagate drop information to all routers quickly and efficiently. This technique, RTBH, sets the next hop of the victim's IP address to the null interface. Traffic destined to the victim is dropped on ingress into the network.

Another option is to drop traffic from a particular source. This method is similar to the drop described previously but relies on the previous deployment of Unicast Reverse Path Forwarding (uRPF), which drops a packet if its source is "invalid," which includes routes to null0. With the same mechanism of the destination−based drop, a BGP update is sent, and this update sets the next hop for a source to null0. Now all traffic that enters an interface with uRPF enabled drops traffic from that source.

Source−based RTBH Filtering on the ASR9000

When the feature uRPF is enabled on the ASR9000, the router is unable to do recursive lookup to null0. This means that the Source−based RTBH Filtering configuration used by Cisco IOS cannot directly be used by Cisco IOS−XR on the ASR9000. As an alternative, the Routing Policy Language (RPL) ***set next−hop discard*** option (introduced in Cisco IOS XR Version 4.3.0) is used.



Configure

Configuration on the Trigger Router

Configure a static route redistribution policy that sets a community on static routes marked with a special tag, and apply it in BGP:

```
route−policy RTBH−trigger
  if tag is 777 then
    set community (1234:4321, no−export) additive
    pass
  else
    pass
  endif
  end−policy

router bgp 65001
 address−family ipv4 unicast
  redistribute static route−policy RTBH−trigger
 !
 neighbor 192.168.102.1
  remote−as 65001
  address−family ipv4 unicast
   route−policy bgp_all in
   route−policy bgp_all out
```

Configure a static route with the special tag for the source prefix that needs to be black−holed:

```
router static
 address−family ipv4 unicast
```

```
 10.7.7.7/32 Null0 tag 777
```

Configuration on the Border Router

Configure a route policy that matches the community set on the trigger router and configure ***set next−hop discard***:

```
route−policy RTBH
  if community matches−any (1234:4321) then
    set next−hop discard
  else
    pass
  endif
end−policy
```

Apply the route policy on the iBGP peers:

```
router bgp 65001
 address−family ipv4 unicast
 !
 neighbor 192.168.102.2
  remote−as 65001
  address−family ipv4 unicast
   route−policy RTBH in
   route−policy bgp_all out
```

On the border interfaces, configure uRPF loose mode:

```
interface TenGigE0/0/2/2
 cdp

 ipv4 address 192.168.101.2 255.255.255.0
 ipv4 verify unicast source reachable−via any
```

Note: This uRPF configuration applies to all traffic on this interface.

Verify

On the border router, the prefix ***10.7.7.7/32*** is flagged as ***Nexthop−discard***:

```
RP/0/RSP0/CPU0:router#show bgp
BGP router identifier 10.210.0.5, local AS number 65001
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000   RD version: 12
BGP main routing table version 12
BGP scan interval 60 secs

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
N>i10.7.7.7/32        192.168.102.2            0    100      0 ?

RP/0/RSP0/CPU0:router#show bgp 10.7.7.7/32
BGP routing table entry for 10.7.7.7/32
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                12          12
Last Modified: Jul  4 14:37:29.048 for 00:20:52
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
  Local
    192.168.102.2 (discarded) from 192.168.102.2 (10.210.0.2)
      Origin incomplete, metric 0, localpref 100, valid, internal best, group-best
      Received Path ID 0, Local Path ID 1, version 12
      Community: 1234:4321 no-export

RP/0/RSP0/CPU0:router#show route 10.7.7.7/32

Routing entry for 10.7.7.7/32
  Known via "bgp 65001", distance 200, metric 0, type internal
  Installed Jul 4 14:37:29.394 for 01:47:02
  Routing Descriptor Blocks
    directly connected, via Null0
      Route metric is 0
  No advertising protos.
```

You can verify on the ingress linecards that RPF drops occur:

```
RP/0/RSP0/CPU0:router#show cef drop location 0/0/CPU0
CEF Drop Statistics
Node: 0/0/CPU0
  Unresolved drops     packets :               0
  Unsupported drops    packets :               0
  Null0 drops          packets :              10
  No route drops       packets :              17
  No Adjacency drops   packets :               0
  Checksum error drops packets :               0
  RPF drops            packets :           48505   <=====
  RPF suppressed drops packets :               0
  RP destined drops    packets :               0
  Discard drops        packets :              37
  GRE lookup drops     packets :               0
  GRE processing drops packets :               0
  LISP punt drops      packets :               0
  LISP encap err drops packets :               0
  LISP decap err drops packets :
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- ***REMOTELY TRIGGERED BLACK HOLE FILTERING − DESTINATION BASED AND SOURCE BASED***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Jul 29, 2013 Document ID: 116386