

Configure BGP FlowSpec VRF to VRF Redirection

Contents

[Introduction](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[FlowSpec client PE3 configurations](#)

[Flowspec server PE4 configurations](#)

[RR P51 configurations](#)

[Verify](#)

[Related information](#)

Introduction

This document describes how to configure BGP Flowspec VRF to VRF Redirection.

Requirements

- A working MPLS enabled IGP implementation
- A working VPNv4 implementation

Components Used

This was tested on Cisco ASR 9000 Series Aggregation Services Routers running Cisco IOS XR version 7.8.2

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

The BGP flow specification (Flowspec) feature allows you to rapidly deploy and propagate filtering and policing functionality among numerous BGP peer routers to mitigate the effects of a distributed denial-of-service (DDoS) attack over your network.

Configure

Network Diagram

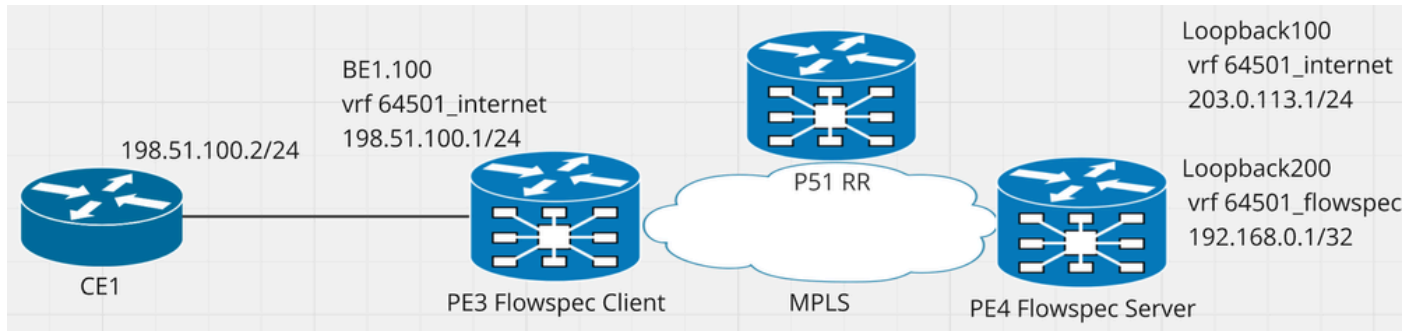


Figure 1 Network Diagram with relevant IP addresses.

Configurations

FlowSpec client PE3 configurations

```
vrf 64501_internet
address-family ipv4 unicast
  import route-target
    64501:100
  !
  export route-target
    64501:100
  !
!
address-family ipv4 flowspec <<<<< Since traffic ingresses on a VRF interface we need to enable VPNV
  import route-target
    64501:100
  !
  export route-target
    64501:100
  !
!
vrf 64501_flowspec <<<<< The honeypot VRF to redirect dirty traffic to
address-family ipv4 unicast
  import route-target
    64501:200
  !
  export route-target
    64501:200
  !
!
interface Bundle-Ether1.100
vrf 64501_internet
ipv4 address 198.51.100.1 255.255.255.0
encapsulation dot1q 100
!
flowspec
vrf 64501_internet
  address-family ipv4
    local-install interface-all <<<<< To install VPNV4 flowspec policies on the vrf interface
  !
!
router bgp 64501
bgp router-id 10.3.3.3
address-family vpnv4 unicast
!
```

```

address-family vpnv4 flowspec <<<< Enable VPNV4 flowspec on global BGP
!
neighbor 10.51.51.51
  remote-as 64501
  update-source Loopback0
  address-family vpnv4 unicast
    soft-reconfiguration inbound always
  !
  address-family vpnv4 flowspec <<<<
    soft-reconfiguration inbound always
  !
vrf 64501_internet
  rd 64501:103
  address-family ipv4 unicast
    redistribute connected
  !
  address-family ipv4 flowspec <<<< Enable VPNV4 on the VRF for which we are going to receive policies
  !
!
vrf 64501_flowspec <<<< This is just the honeypot VRF to redirect the dirty traffic to
  rd 64501:203
  address-family ipv4 unicast
  !
!
router static
vrf 64501_flowspec
  address-family ipv4 unicast
    0.0.0.0/0 192.168.0.1 <<<< We need a default route on the honeypot VRF to be able to forward the
  !
!

```

Flowspec server PE4 configurations

```

vrf 64501_internet
address-family ipv4 unicast
  import route-target
    64501:100
  !
  export route-target
    64501:100
  !
!
address-family ipv4 flowspec <<<<<< We are going to advertise VPNV4 flowspec policies for this VRF w
  import route-target
    64501:100
  !
  export route-target
    64501:100
  !
!
vrf 64501_flowspec <<<< The honeypot VRF to redirect dirty traffic to
address-family ipv4 unicast
  import route-target
    64501:200
  !
  export route-target
    64501:200
  !

```

```

!
interface Loopback100 <<<< Traffic destination prefix for testing
vrf 64501_internet
ipv4 address 203.0.113.1 255.255.255.0
!
interface Loopback200 <<<< Just for testing purposes, this is where we are redirecting the traffic to
vrf 64501_flowspec
ipv4 address 192.168.0.1 255.255.255.255
!
class-map type traffic match-all 64501_flow
match source-address ipv4 198.51.100.2 255.255.255.255
end-class-map
!
policy-map type pbr 64501_flow
class type traffic 64501_flow
  redirect nexthop route-target 64501:200 <<<< honeypot vrf 64501_flowspec RT
!
class type traffic class-default
!
end-policy-map
!
flowspec
vrf 64501_internet
  address-family ipv4
    service-policy type pbr 64501_flow <<<< Advertise the policy within the VRF context in the ser
!
!
router bgp 64501
bgp router-id 10.4.4.4
address-family vpnv4 unicast
!
address-family vpnv4 flowspec <<<< Enable VPNV4 flowspec on global BGP
!
neighbor 10.51.51.51
  address-family vpnv4 unicast
  soft-reconfiguration inbound always
!
  address-family vpnv4 flowspec <<<<
  soft-reconfiguration inbound always
!
!
vrf 64501_internet
  rd 64501:104
  address-family ipv4 unicast
  redistribute connected
!
  address-family ipv4 flowspec <<<< Enable VPNV4 on the VRF for which we are going to advertise polici
!
!
vrf 64501_flowspec <<<< This is just the honeypot VRF to redirect the dirty traffic to
  rd 64501:204
  address-family ipv4 unicast
  redistribute connected
!
!

```

RR P51 configurations

```

router bgp 64501
  bgp router-id 10.51.51.51
  address-family vpnv4 unicast
  !
  address-family vpnv4 flowspec
  !
  neighbor 10.3.3.3
    remote-as 64501
    update-source Loopback0
    address-family vpnv4 unicast
      route-reflector-client
      soft-reconfiguration inbound always
    !
    address-family vpnv4 flowspec
      route-reflector-client
      soft-reconfiguration inbound
    !
  !
  neighbor 10.4.4.4
    remote-as 64501
    update-source Loopback0
    address-family vpnv4 unicast
      route-reflector-client
      soft-reconfiguration inbound always
    !
    address-family vpnv4 flowspec
      route-reflector-client
      soft-reconfiguration inbound
    !
  !

```

Verify

```

RP/0/RP0/CPU0:PE3#show flowspec vrf 64501_internet ipv4 detail
Tue Oct 1 16:54:51.990 CDT
VRF: 64501_internet      AFI: IPv4
  Flow      :Source:198.51.100.2/32
  Actions   :Redirect: VRF 64501_flowspec Route-target: ASN2-64501:200 (bgp.1)
  Statistics (packets/bytes)
    Matched      : 5/610 <<<<<<<
    Dropped      : 0/0

```

```

RP/0/RP0/CPU0:PE3#show bgp vpnv4 flowspec
Tue Oct 1 16:54:57.352 CDT
BGP router identifier 10.3.3.3, local AS number 64501
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0
BGP main routing table version 7
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
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

```

```

Route Distinguisher: 64501:103 (default for vrf 64501_internet)
Route Distinguisher Version: 7
*>iSource:198.51.100.2/32/48
                                0.0.0.0          100      0 i
Route Distinguisher: 64501:104
Route Distinguisher Version: 6
*>iSource:198.51.100.2/32/48
                                0.0.0.0          100      0 i
Processed 2 prefixes, 2 paths

RP/0/RP0/CPU0:PE3#show bgp vpnv4 flowspec vrf 64501_internet Source:198.51.100.2/32/48
BGP routing table entry for Source:198.51.100.2/32/48, Route Distinguisher: 64501:103
Versions:
  Process          bRIB/RIB  SendTblVer
  Speaker          7         7
Last Modified: Oct  1 16:52:12.083 for 00:02:55
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local, (received & used)
    0.0.0.0 from 10.51.51.51 (10.4.4.4)
    Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported
    Received Path ID 0, Local Path ID 1, version 7
    Extended community: FLOWSPEC Redirect-RT:64501:200 RT:64501:100    <<<<<<
    Originator: 10.4.4.4, Cluster list: 0.0.253.233
    Source AFI: VPNv4 Flowspec, Source VRF: default, Source Route Distinguisher: 64501:104

```

With a packet capture we can observe the service MPLS label which confirms that the packets are being redirected

```

RP/0/RP0/CPU0:PE4#show mpls forwarding labels 24005
Tue Oct  1 16:45:21.743 CST
Local  Outgoing  Prefix      Outgoing    Next Hop    Bytes
Label  Label      or ID      Interface   \
-----
24005  Aggregate   64501_flowspec: Per-VRF Aggr[V]  \
                                64501_flowspec                    1500

```

Time	Source	Destination	Protocol	Length	Info
1.0.0.00000000	198.51.100.2	203.0.113.1	ICMP	118	Echo (ping) request id=0x0003, seq=0/0, ttl=253 (no response found!)

Frame 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface Fake IF, Import from Hex Dump, id 0
Ethernet II, Src: Cisco_e9:8e:d0 (f4:ee:31:e9:8e:d0), Dst: Cisco_5b:56:fa (ec:c0:18:5b:56:fa)
MultiProtocol Label Switching Header, Label: 24005, Exp: 0, S: 1, TTL: 253

0000 0101 1101 1100 0101 = MPLS Label: 24005 (0x05dc5)
.... = MPLS Experimental Bits: 0
....1 = MPLS Bottom Of Label Stack: 1
.... 1111 1101 = MPLS TTL: 253

Internet Protocol Version 4, Src: 198.51.100.2, Dst: 203.0.113.1

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 100
Identification: 0x000f (15)
> 000. = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 253
Protocol: ICMP (1)
Header Checksum: 0x9186 [validation disabled]
[Header checksum status: Unverified]
Source Address: 198.51.100.2
Destination Address: 203.0.113.1
[Stream index: 0]

Internet Control Message Protocol

Figure 2 PCAP showing evidence of traffic redirection, notice the service MPLS label 24005.

The VRF 64501_internet Ingress traffic on Flowspec client that matches the policy is being redirected to 64501_flowspec VRF.

Related information

<https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-8/routing/configuration/guide/b-routing-cg-asr9000-78x/implementing-bgp-flowspec.html>