

配置BGP FlowSpec VRF到VRF重定向

目录

[简介](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[FlowSpec客户端PE3配置](#)

[Flowspec服务器PE4配置](#)

[RR P51配置](#)

[验证](#)

[相关信息](#)

简介

本文档介绍如何配置BGP Flowspec VRF到VRF重定向。

要求

- 支持MPLS的有效IGP实施
- 有效的VPNv4实施

使用的组件

此测试在运行Cisco IOS XR 7.8.2版的Cisco ASR 9000系列聚合服务路由器上进行

本文档中的信息都是基于特定实验室环境中的设备编写的。用于本文的所有设备始于初始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

BGP流规范(Flowspec)功能允许您在多个BGP对等路由器之间快速部署和传播过滤和策略功能，以缓解网络上的分布式拒绝服务(DDoS)攻击的影响。

配置

网络图

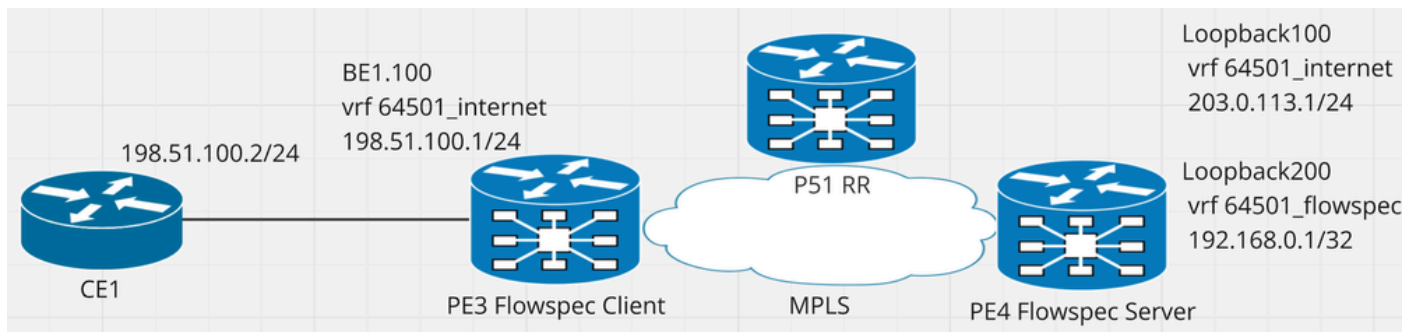


图1具有相关IP地址的网络图。

配置

FlowSpec客户端PE3配置

```
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服务器PE4配置

```

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
!
!

```

```

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
  !
!

```

验证

```

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

```

通过数据包捕获，我们可以观察服务MPLS标签，该标签可确认数据包被重定向

```

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)					
.... 0000. = MPLS Experimental Bits: 0					
.... 0000. = 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)					
> 0000. = 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					

图2显示流量重定向证据的PCAP，请注意服务MPLS标签24005。

与策略64501配的Flowspec客户端上的VRF_internet入口流量将被重定向到64501_flowspec VRF。

相关信息

<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>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。