

BGP FlowSpec VRF에서 VRF로의 리디렉션 구성

목차

[소개](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[FlowSpec 클라이언트 PE3 구성](#)

[Flowspec 서버 PE4 구성](#)

[RR P51 컨피그레이션](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 BGP Flowspec VRF에서 VRF로의 리디렉션을 구성하는 방법에 대해 설명합니다.

요구 사항

- 작동하는 MPLS 지원 IGP 구현
- 작동하는 VPNv4 구현

사용되는 구성 요소

이 테스트는 Cisco IOS XR 버전 7.8.2를 실행하는 Cisco ASR 9000 Series Aggregation Services Router에서 수행되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

BGP 흐름 사양(FlowSpec) 기능을 사용하면 수많은 BGP 피어 라우터 간에 필터링 및 폴리싱 기능을 신속하게 배포하고 전파하여 네트워크를 통한 DDoS(Distributed Denial-of-Service) 공격의 영향을 완화할 수 있습니다.

구성

네트워크 다이어그램

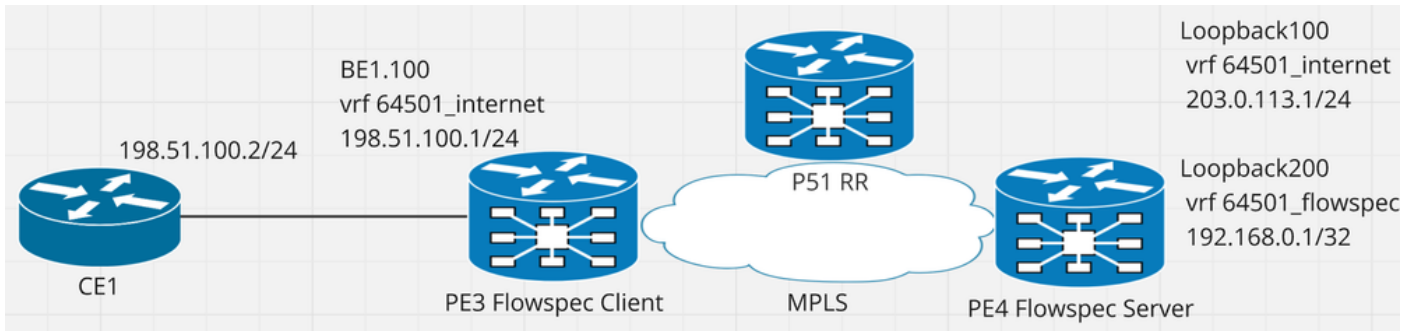


그림 1 관련 IP 주소의 네트워크 다이어그램.

설정

FlowSpec 클라이언트 PE3 구성

```
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 서버 PE4 구성

```

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
  !
!

```

다음을 확인합니다.

```

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

```

패킷 캡처를 통해 서비스 MPLS 레이블을 관찰하여 패킷이 리디렉션되고 있음을 확인할 수 있습니다

```

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
1.0.000000000	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 0001. = 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					

그림 2 트래픽 리디렉션의 증거를 보여주는 PCAP는 서비스 MPLS 레이블 24005.

정책과 일치하는 Flowspec 클라이언트의 VRF 64501_internet Ingress 트래픽이 64501_flowspec VRF로 리디렉션됩니다.

관련 정보

<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>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.