BGP FlowSpec VRF naar VRF omleiden configureren

Inhoud

Inleiding

In dit document wordt beschreven hoe u BGP Flowspec VRF naar VRF-omleiding kunt configureren.

Vereisten

- Een werkende MPLS ingeschakeld IGP implementatie
- Een werkende VPNv4-implementatie

Gebruikte componenten

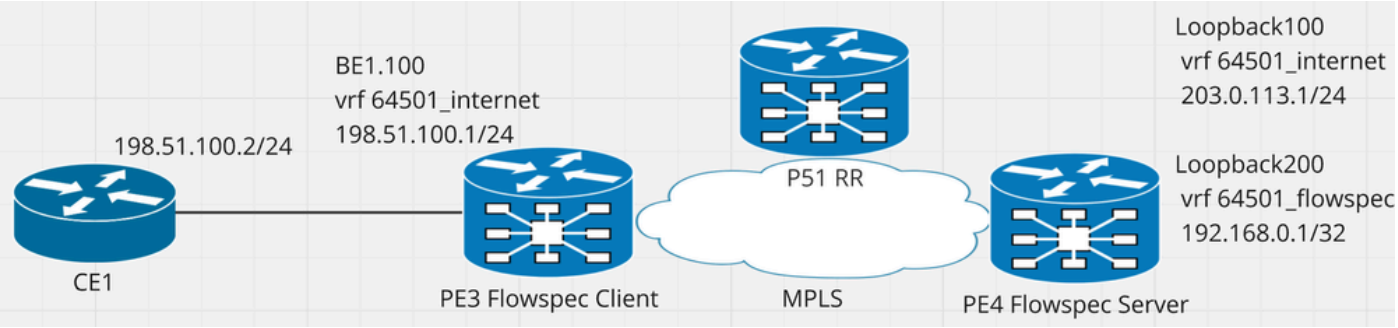
Dit is getest op Cisco ASR 9000 Series Aggregation Services Routers met Cisco IOS XR versie 7.8.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een uitgeklaarde (standaard) configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Met de BGP-stroomspecificatie (Flowspec)-functie kunt u snel filtering- en politiefunctionaliteit implementeren en verspreiden onder tal van BGP-peer-routers om de effecten van een DDoS-aanval (Distributed Denial-of-Service) over uw netwerk te beperken.

Configureren

Netwerkdiagram



Afbeelding 1 Netwerkdiagram met relevante IP-adressen.

Configuraties

PE3-configuraties van FlowSpec-client

```
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 policie
  !
!
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 configuraties

```
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 serv
  !
!
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 policie
  !
!
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-configuraties

```
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
  !
!
```

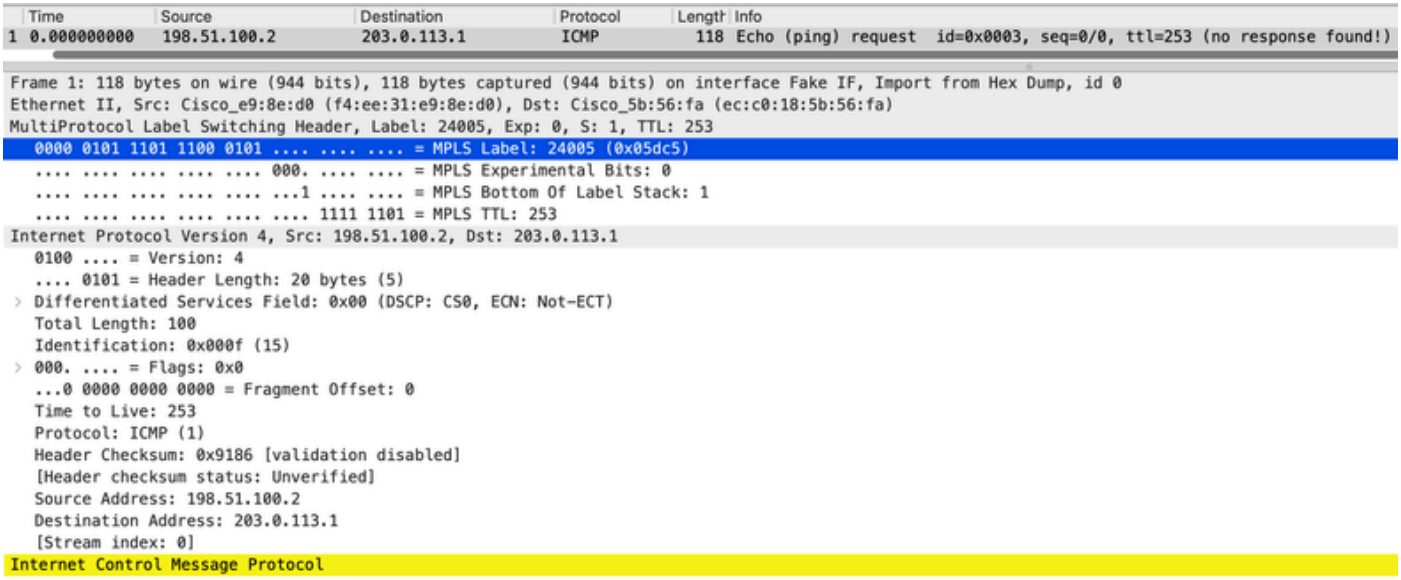
Verifiëren

```
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
```

Met een packet capture kunnen we het service MPLS label waarnemen dat bevestigt dat de pakketten worden omgeleid

```
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                    Switched
------ ----------- ------------------ ------------ --------------- ------------
24005  Aggregate   64501_flowspec: Per-VRF Aggr[V]   \
                                      64501_flowspec                1500
```



Figuur 2 PCAP toont bewijs van omleiding van het verkeer, let op het service MPLS-label 24005.

Het VRF 64501_internet Ingress-verkeer op Flowspec-client dat overeenkomt met het beleid wordt omgeleid naar 64501_flowspec VRF.

Gerelateerde informatie

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.