

Onjuist gebruik van "beleidsactie set tloc-list" leidt tot Traffic Blackholing

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Normale omstandigheden](#)

[Foutomstandigheden](#)

[Oplossing](#)

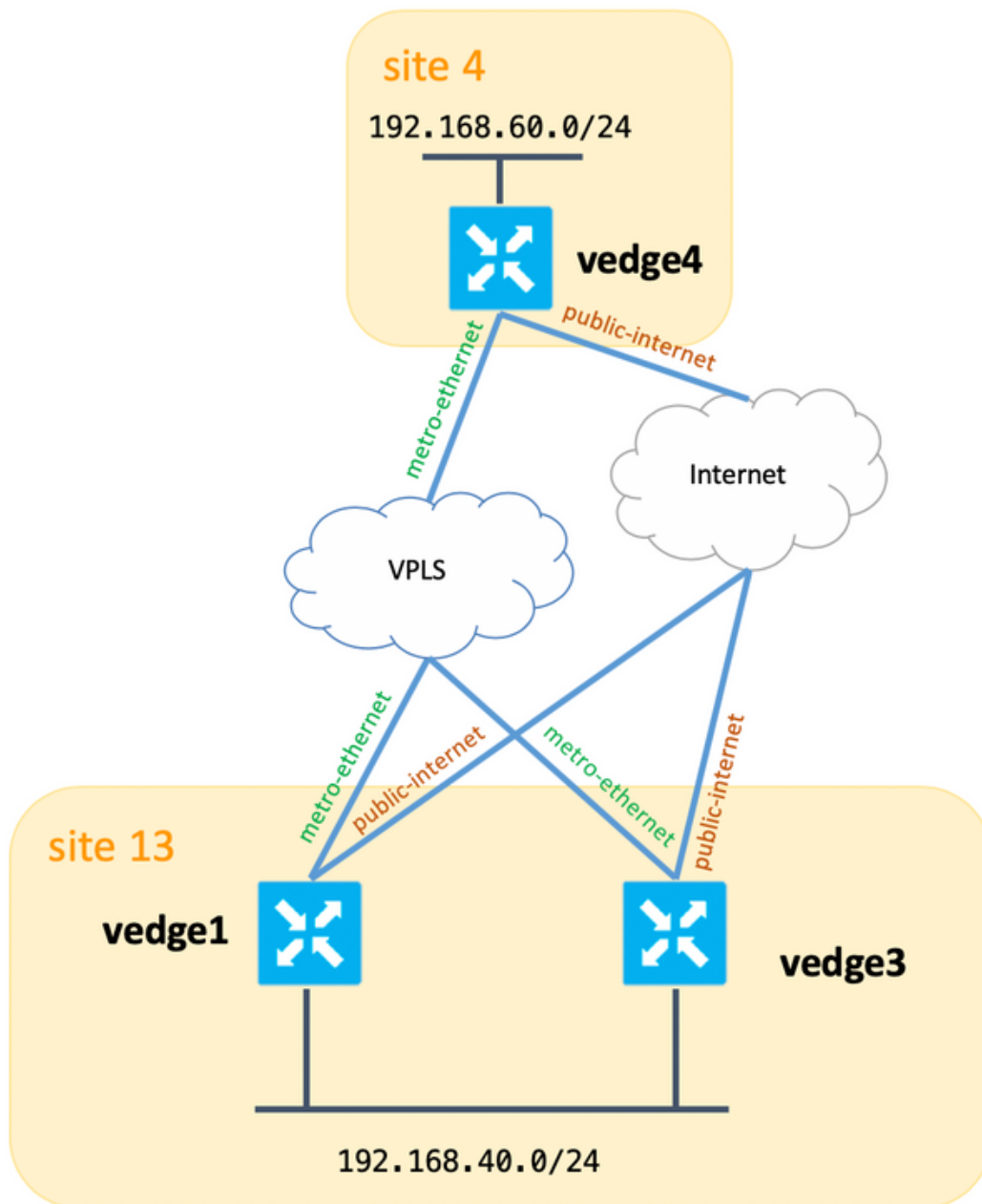
Inleiding

In dit document wordt de ongepaste beleidstoepassing beschreven van acties op **een** tabellijst die in bepaalde situaties tot verkeersblokkering leiden wanneer de voorkeurslink naar beneden gaat maar er nog back-uppaden beschikbaar zijn.

Opmerking: Alle opdrachtoutput die in dit document wordt gepresenteerd, is afkomstig van vEdge-routers. De probleemoplossing blijft echter hetzelfde voor een router die de IOS®-XE SDWAN-software uitvoert. Gebruik **het** trefwoord **sdwan** om dezelfde uitgangen te krijgen op IOS®-XE SDWAN-software. Bijvoorbeeld, **toon sdwan omp routes** in plaats van **toon omp routes**.

Achtergrondinformatie

Voor demonstratiedoeleinden en om het later beschreven probleem beter te begrijpen, overweeg dit topologiediagram:



Daarnaast is hier de tabel die de systeeminstellingen samenvat:

hostnaam	site-id	systemip
vEdge1	13	10.155.0.118
vEdge3	13	10.155.0.120
vEdge4	4	10.155.0.50
smart1	1	10.155.0.3

Zowel vEdge1 als vEdge3 hebben een statische route geconfigureerd die naar enige volgende hop in de service-side VPN wijst:

```
vpn 40
 ip route 10.223.115.101/32 192.168.40.10
!
```

Om deze doelstellingen te bereiken:

1. Maak dat de vEdge1 metro-ethernetlink de voorkeur heeft voor indringingsverkeer dat "site 13" invoert.
2. MMaak vEdge3 metro-ethernetlink een tweede voorkeurslink voor toegangsverkeer dat "site 13" invoert.
3. Maak van vEdge1 een openbare internetlink naar de derde voorkeurslink voor toegangsverkeer die "site 13" invoert.
4. Maak van vEdge3 een publiek-internet link die de minst gewenste link is voor toegangsverkeer dat "site 13" invoert.

Dit vSmart-controlebeleid is ingesteld op:

```

policy
  lists
    tloc-list SITE13_TLOC_PREF
      tloc 10.155.0.118 color metro-ethernet encaps ipsec preference 200
      tloc 10.155.0.118 color public-internet encaps ipsec preference 100
      tloc 10.155.0.120 color metro-ethernet encaps ipsec preference 150
      tloc 10.155.0.120 color public-internet encaps ipsec preference 50
    !
    prefix-list SITE13_PREFIX
      ip-prefix 10.223.115.101/32
    !
    site-list site13
      site-id 13
    !
  control-policy TE_POLICY_2_SITE4
    sequence 10
    match route
      prefix-list SITE13_PREFIX
    !
    action accept
      set
        tloc-list SITE13_TLOC_PREF
      !
    !
    !
    default-action accept
  !
!
apply-policy
  site-list site4
  control-policy TE_POLICY_2_SITE4 out
!
!

```

Probleem

Normale omstandigheden

vSmart krijgt deze routes met 4 mogelijke TLOC's als next-hop:

```
vsmart1# show omp routes 10.223.115.101/32 | b PATH
PATH
```

ATTRIBUTE

VPN COLOR	PREFIX	ENCAP	FROM PEER PREFERENCE	ID	LABEL	STATUS	TYPE	TLOC IP
40	10.223.115.101/32	ipsec	-	35	1002	C,R	installed	10.155.0.118
metro-ethernet								
public-internet								
40	10.223.115.101/32	ipsec	-	37	1002	C,R	installed	10.155.0.118
metro-ethernet								
public-internet								
40	10.223.115.101/32	ipsec	-	35	1002	C,R	installed	10.155.0.120
metro-ethernet								
public-internet								
40	10.223.115.101/32	ipsec	-	37	1002	C,R	installed	10.155.0.120
metro-ethernet								
public-internet								

En stelt dienovereenkomstig een voorkeur voor geadverteerde routes vast:

```
vsmart1# show omp routes 10.223.115.101/32 detail | nomore | b ADVERTISED | b "peer 10.155.0.50" | i Attributes\|originator\|\ tloc\|preference
Attributes:
  originator      10.155.0.118
  tloc            10.155.0.120, public-internet, ipsec
  preference      50
Attributes:
  originator      10.155.0.118
  tloc            10.155.0.120, metro-ethernet, ipsec
  preference      150
Attributes:
  originator      10.155.0.118
  tloc            10.155.0.118, public-internet, ipsec
  preference      100
Attributes:
  originator      10.155.0.118
  tloc            10.155.0.118, metro-ethernet, ipsec
  preference      200
```

vEdge4 selecteert een juiste TLOC en installeert deze route in de routingstabel:

```
vedge4# show ip routes 10.223.115.101/32 | b PROTOCOL
VPN      PREFIX      PROTOCOL      SUB TYPE  IF NAME  NEXTHOP  NEXTHOP  NEXTHOP
IP       COLOR      ENCAP  STATUS
-----
40       10.223.115.101/32  omp          -        -        -        -        -
10.155.0.118  metro-ethernet  ipsec  F,S
```

Verkeersinrichting werkt zoals bedoeld:

```
vedge4# traceroute vpn 40 10.223.115.101
Traceroute 10.223.115.101 in VPN 40
traceroute to 10.223.115.101 (10.223.115.101), 30 hops max, 60 byte packets
 1 192.168.40.4 (192.168.40.4) 0.835 ms 0.984 ms 1.097 ms
 2 192.168.40.10 (192.168.40.10) 2.955 ms 3.056 ms 3.218 ms
```

Foutomstandigheden

Uiteindelijk treedt een fout op op vEdge1 en gaat de interface aan de servicekant van het LAN

naar beneden (of wordt door de beheerder uitgeschakeld om een test uit te voeren; het resultaat zal bijvoorbeeld hetzelfde zijn):

```
vedge1# show interface vpn 40
```

```

          IF      IF      IF
TCP
          AF
SPEED      MSS      RX      TX
VPN  INTERFACE  TYPE  IP ADDRESS  STATUS  STATUS  STATUS  TYPE  TYPE  MTU  HWADDR
MBPS  DUPLEX  ADJUST  UPTIME  PACKETS  PACKETS
-----
40   ge0/4     ipv4  192.168.40.4/24  Up      Down    NA      null  service  1500
00:50:56:be:91:36  -      -      1420      -      129768  0

```

Omdat vEdge1 geen geldige next-hop voor 10.223.115.101/32 route heeft, wordt deze route verwijderd uit de routing- en Forwarding-tabellen en wordt deze niet meer geadverteerd naar vSmart:

```
vedge1# show ip routes 10.223.115.101/32 | b PROTO
```

```

          PROTOCOL  NEXTHOP      NEXTHOP      NEXTHOP
VPN  PREFIX      PROTOCOL      SUB TYPE  IF NAME      ADDR      VPN      TLOC
IP      COLOR      ENCAP  STATUS
-----
40     10.223.115.101/32  static      -      -      192.168.40.21  -      -
-      -      I

```

```
vedge1# show ip fib vpn 40 | i 10.223.115.101/32
```

```
vedge1#
```

```
vedge1# show omp routes 10.223.115.101/32 detail | nomore | b ADVERTISED
```

```
vedge1#
```

Tegelijkertijd adverteert vEdge3 nog steeds deze route (dit wordt verwacht):

```
vedge3# show omp routes 10.223.115.101/32 detail | nomore | b ADVERTISED
```

```
ADVERTISED TO:
```

```
peer 10.155.0.3
```

```
Attributes:
```

```
originator 10.155.0.120
label      1002
path-id    35
tloc       10.155.0.120, metro-ethernet, ipsec
ultimate-tloc not set
domain-id  not set
site-id    13
overlay-id 1
preference not set
tag        not set
origin-proto static
origin-metric 0
as-path    not set
unknown-attr-len not set
```

```
Attributes:
```

```

originator      10.155.0.120
label           1002
path-id        37
tloc           10.155.0.120, public-internet, ipsec
ultimate-tloc  not set
domain-id      not set
site-id        13
overlay-id     1
preference     not set
tag            not set
origin-proto   static
origin-metric  0
as-path        not set
unknown-attr-len not set

```

vSmart krijgt nu 2 routes van vEdge3 zoals verwacht:

```

vsmart1# show omp routes 10.223.115.101/32 | b PATH

```

VPN	PREFIX	FROM PEER	PATH	STATUS	ATTRIBUTE	TLOC IP
COLOR	ENCAP	PREFERENCE	ID LABEL		TYPE	
40	10.223.115.101/32	10.155.0.120	35 1002	C,R	installed	10.155.0.120
metro-ethernet	ipsec	-				
public-internet	ipsec	-	37 1002	C,R	installed	10.155.0.120

Maar tegelijkertijd blijft vSmart dit adverteren:

```

vsmart1# show omp routes 10.223.115.101/32 detail | nomore | b ADVERTISED | b "peer
10.155.0.50" | i Attributes\|originator\|\ tloc\|preference
Attributes:
originator      10.155.0.120
tloc           10.155.0.120, public-internet, ipsec
preference     50
Attributes:
originator      10.155.0.120
tloc           10.155.0.120, metro-ethernet, ipsec
preference     150
Attributes:
originator      10.155.0.120
tloc           10.155.0.118, public-internet, ipsec
preference     100
Attributes:
originator      10.155.0.120
tloc           10.155.0.118, metro-ethernet, ipsec
preference     200

```

Zoals je kunt zien, is de enige originator veranderd en dit is verwacht gedrag omdat **toc-lijst** actie handelt vergelijkbaar met (grofweg gesproken) "stel volgende-hop" en zet krachtig de verkeerde TLOC, dus bereikbaarheid is verloren.

```

vedge4# ping vpn 40 10.223.115.101 count 5
Ping in VPN 40
PING 10.223.115.101 (10.223.115.101) 56(84) bytes of data.
^C

```

```
--- 10.223.115.101 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 3999ms
```

```
vedge4# traceroute vpn 40 10.223.115.101
Traceroute 10.223.115.101 in VPN 40
traceroute to 10.223.115.101 (10.223.115.101), 30 hops max, 60 byte packets
 1 * * *
 2 * * *
 3 * * *
 4 * * *
 5 * * *
```

Oplossing

Als oplossing wordt deze benadering voorgesteld om te voorkomen dat de verkeerde TLOC-next-hop-informatie wordt vastgesteld:

```
policy
 lists
  tloc-list vedge1-tlocs
    tloc 10.155.0.118 color metro-ethernet encaps ipsec
    tloc 10.155.0.118 color public-internet encaps ipsec
  !
  tloc-list vedge1-tlocs-preference
    tloc 10.155.0.118 color metro-ethernet encaps ipsec preference 200
    tloc 10.155.0.118 color public-internet encaps ipsec preference 100
  !
  tloc-list vedge3-tlocs
    tloc 10.155.0.120 color metro-ethernet encaps ipsec
    tloc 10.155.0.120 color public-internet encaps ipsec
  !
  tloc-list vedge3-tlocs-preference
    tloc 10.155.0.120 color metro-ethernet encaps ipsec preference 150
    tloc 10.155.0.120 color public-internet encaps ipsec preference 50
  !
  !
  !
policy
 control-policy TE_POLICY_2_SITE4
  sequence 10
  match route
    prefix-list SITE13_PREFIX
    tloc-list vedge1-tlocs
  !
  action accept
  set
    tloc-list vedge1-tlocs-preference
  !
  !
  !
  sequence 20
  match route
    prefix-list SITE13_PREFIX
    tloc-list vedge3-tlocs
  !
  action accept
  set
    tloc-list vedge3-tlocs-preference
  !
  !
  !
```

```
default-action accept
```

```
!
```

```
!
```

Zo'n beleid verbetert de situatie en voorkomt reclame voor de route met de verkeerde TLOC next-hop:

```
vsmart1# show omp routes 10.223.115.101/32 detail | nomore | b ADVERTISED | b "peer 10.155.0.50" | i Attributes\|originator\|\ tloc\|preference
```

```
Attributes:
```

```
originator      10.155.0.120
tloc            10.155.0.120, public-internet, ipsec
preference      50
```

```
Attributes:
```

```
originator      10.155.0.120
tloc            10.155.0.120, metro-ethernet, ipsec
preference      150
```

```
Attributes:
```

```
originator      10.155.0.120
tloc            10.155.0.120, public-internet, ipsec
preference      not set
```

En als resultaat hiervan blijft de bereikbaarheid in alle foutsenario's behouden:

```
vedge4# traceroute vpn 40 10.223.115.101
```

```
Traceroute 10.223.115.101 in VPN 40
```

```
traceroute to 10.223.115.101 (10.223.115.101), 30 hops max, 60 byte packets
```

```
 1 192.168.40.6 (192.168.40.6) 0.458 ms 0.507 ms 0.617 ms
 2 192.168.40.10 (192.168.40.10) 1.928 ms 1.976 ms 2.069 ms
```

```
vedge4# ping vpn 40 10.223.115.101
```

```
Ping in VPN 40
```

```
PING 10.223.115.101 (10.223.115.101) 56(84) bytes of data.
```

```
64 bytes from 10.223.115.101: icmp_seq=1 ttl=254 time=0.702 ms
```

```
64 bytes from 10.223.115.101: icmp_seq=2 ttl=254 time=0.645 ms
```

```
64 bytes from 10.223.115.101: icmp_seq=3 ttl=254 time=0.691 ms
```

```
64 bytes from 10.223.115.101: icmp_seq=4 ttl=254 time=0.715 ms
```

```
64 bytes from 10.223.115.101: icmp_seq=5 ttl=254 time=0.603 ms
```

```
^C
```

```
--- 10.223.115.101 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
```

```
rtt min/avg/max/mdev = 0.603/0.671/0.715/0.044 ms
```


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.