# Unangemessene Verwendung von "policy action set tloc-list" führt zu Datenverkehrs-Blackholing

## Inhalt



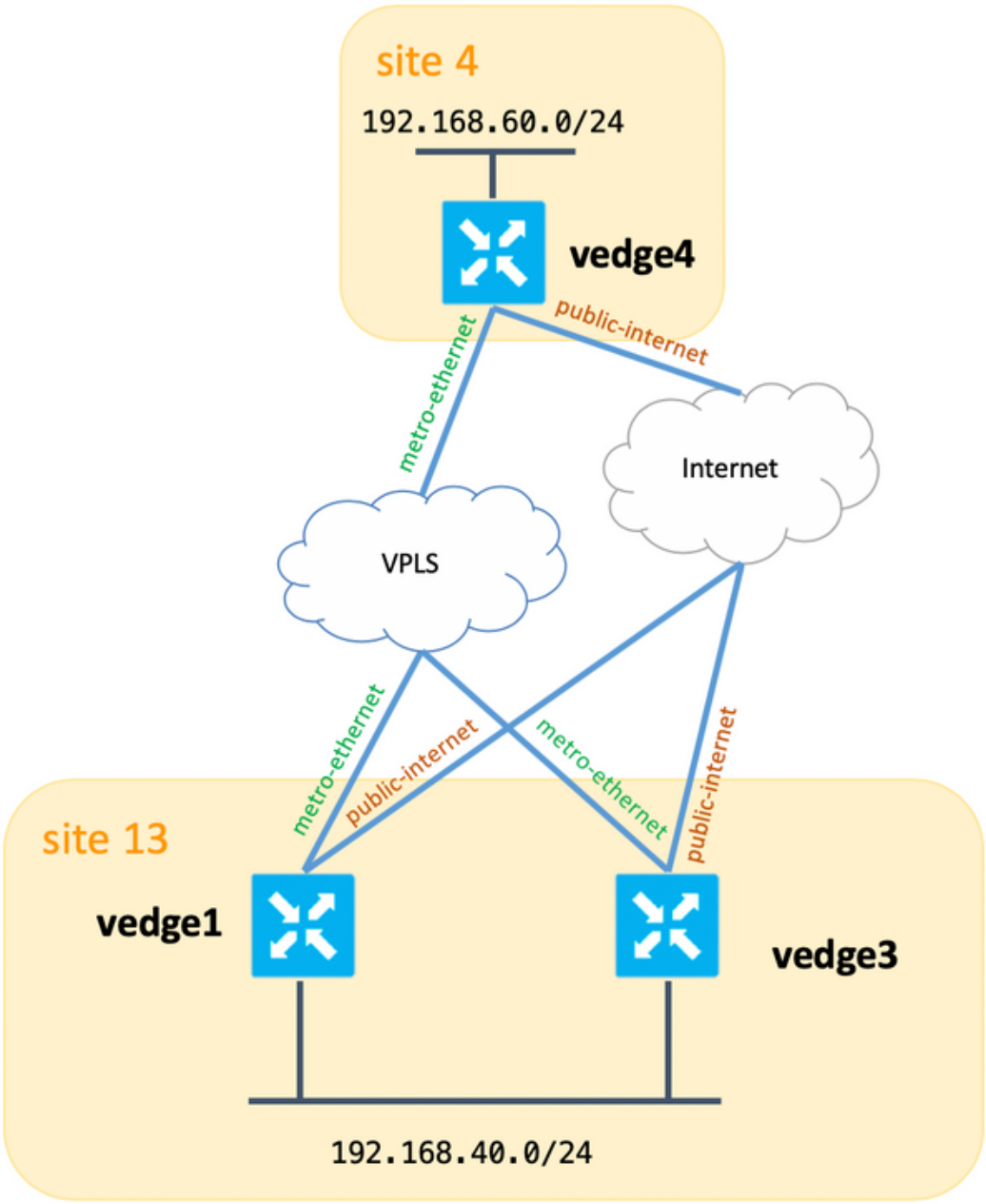
## Einleitung

Dieses Dokument beschreibt die unangemessene Richtlinienanwendung der **Aktion "set tloc-list",** die in bestimmten Situationen zu Blackholing des Datenverkehrs führt, wenn die bevorzugte Verbindung ausfällt, aber immer noch Backup-Pfade verfügbar sind.

> **Anmerkung:** Alle in diesem Dokument aufgeführten Befehlsausgaben stammen von vEdge-Routern. Die Vorgehensweise zur Fehlerbehebung bleibt jedoch bei einem Router, auf dem die IOS®-XE SDWAN-Software ausgeführt wird, dieselbe. Verwenden Sie das Schlüsselwort **sdwan**, um die gleichen Ergebnisse für die IOS®-XE SDWAN-Software zu erhalten. Beispiel: **sdwan omp-Routen** statt **show omp-Routen anzeigen**.

## Hintergrundinformationen

Zur Veranschaulichung und um das später beschriebene Problem besser zu verstehen, sehen Sie sich dieses Topologiediagramm an:




Außerdem finden Sie in der folgenden Tabelle eine Zusammenfassung der Systemeinstellungen:

| Hostname | Standort-ID | System-IP |
|---|---|---|
| vEdge1 | 13 | 10.155.0.118 |
| vedge3 | 13 | 10.155.0.120 |
| vedge4 | 4 | 10.155.0.50 |
| vsmart1 | 1 | 10.155.0.3 |

Sowohl vEdge1 als auch vEdge3 haben eine statische Route konfiguriert, die auf einen nächsten Hop im serviceseitigen VPN verweist:

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

Um diese Ziele zu erreichen,

1. Festlegen der vEdge1-Metro-Ethernet-Verbindung als bevorzugte Verbindung für eingehenden Datenverkehr, der auf "Standort 13" eingeht

2. mStellen Sie die vEdge3-Metro-Ethernet-Verbindung als zweite bevorzugte Verbindung für eingehenden Datenverkehr am "Standort 13" ein.

3. Machen Sie aus der vEdge1-Verbindung für das öffentliche Internet die dritte bevorzugte Verbindung für eingehenden Datenverkehr, der auf "Standort 13" eingeht.

4. Stellen Sie sicher, dass vEdge3-Links für das öffentliche Internet die am wenigsten bevorzugte Verbindung für eingehenden Datenverkehr sind, der auf "Site 13" eingeht.

Diese vSmart-Steuerungsrichtlinie ist konfiguriert:

```
policy
 lists
  tloc-list SITE13_TLOC_PREF
   tloc 10.155.0.118 color metro-ethernet encap ipsec preference 200
   tloc 10.155.0.118 color public-internet encap ipsec preference 100
   tloc 10.155.0.120 color metro-ethernet encap ipsec preference 150
   tloc 10.155.0.120 color public-internet encap 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
 !
!
```

# Problem

## Normale Bedingungen

vSmart erhält diese Routen mit vier möglichen TLOCs als Next-Hops:

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

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

Legt eine entsprechende Präferenz für die angegebenen Routen fest:

```
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 wählt eine geeignete TLOC aus und installiert diese Route in der Routing-Tabelle:

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

Verkehrsweiterleitung wie vorgesehen:

```
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
```

## Fehlerbedingungen

Schließlich tritt ein Fehler auf vEdge1 auf, und die Schnittstelle zur serviceseitigen LAN-

Verbindung fällt aus (oder wird vom Administrator deaktiviert, um einen Test durchzuführen. Das Ergebnis ist beispielsweise dasselbe):

```
vedge1# show interface vpn 40

                                       IF      IF      IF
TCP
                AF                     ADMIN   OPER    TRACKER  ENCAP  PORT
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
```

Da vEdge1 über keinen gültigen Next-Hop für die Route 10.223.115.101/32 verfügt, wird diese Route aus den Routing- und Weiterleitungstabellen entfernt und nicht mehr an vSmart gemeldet:

```
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#
```

Gleichzeitig kündigt der vEdge3 diese Route an (dies wird erwartet):

```
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 erhält jetzt wie erwartet 2 Routen vom vEdge3:

```
vsmart1# show omp routes 10.223.115.101/32 | b PATH
                                          PATH                      ATTRIBUTE
VPN    PREFIX              FROM PEER      ID     LABEL    STATUS    TYPE       TLOC IP
COLOR            ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------
-------------------------------------
40     10.223.115.101/32   10.155.0.120     35     1002     C,R       installed  10.155.0.120
metro-ethernet   ipsec  -
                           10.155.0.120     37     1002     C,R       installed  10.155.0.120
public-internet  ipsec  -
```

vSmart kündigt jedoch weiterhin Folgendes an:

```
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
```

Wie Sie sehen können, wurde der einzige Ausgangspunkt geändert, und dies ist ein erwartetes Verhalten, da die **tloc-list-**Aktion ähnlich wie (grob gesagt) "set next-hop" agiert und den falschen TLOC mit Gewalt setzt, wodurch die Erreichbarkeit verloren geht.

```
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  * * *
```

# Lösung

Als Lösung wird dieser Ansatz vorgeschlagen, um zu verhindern, dass falsche TLOC-Next-Hop-Informationen festgelegt werden:

```
policy
 lists
  tloc-list vedge1-tlocs
   tloc 10.155.0.118 color metro-ethernet encap ipsec
   tloc 10.155.0.118 color public-internet encap ipsec
  !
  tloc-list vedge1-tlocs-preference
   tloc 10.155.0.118 color metro-ethernet encap ipsec preference 200
   tloc 10.155.0.118 color public-internet encap ipsec preference 100
  !
  tloc-list vedge3-tlocs
   tloc 10.155.0.120 color metro-ethernet encap ipsec
   tloc 10.155.0.120 color public-internet encap ipsec
  !
  tloc-list vedge3-tlocs-preference
   tloc 10.155.0.120 color metro-ethernet encap ipsec preference 150
   tloc 10.155.0.120 color public-internet encap 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
```

```
 !
!
```

Eine solche Richtlinie verbessert die Situation und verhindert die Werbung für die Route mit dem falschen 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
```

Dadurch bleibt die Erreichbarkeit in allen Ausfallszenarien erhalten:

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.