

# 「ポリシーアクションセットtloc-list」の不適切な使用によるトラフィックのブラックホール化

## 内容

[概要](#)

[背景説明](#)

[問題](#)

[通常の状態](#)

[障害状態](#)

[解決方法](#)

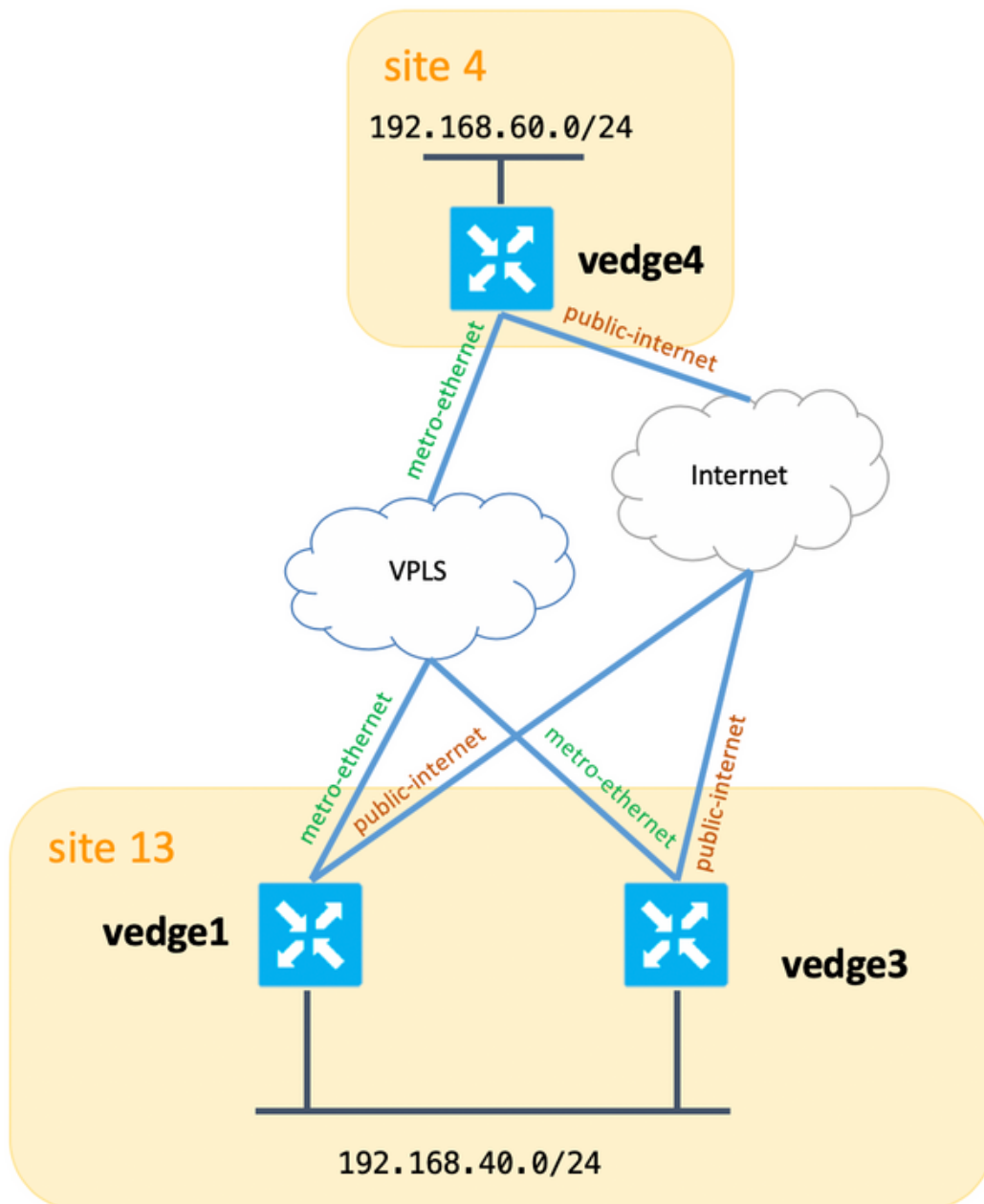
## 概要

このドキュメントでは、優先リンクがダウンしてもバックアップパスが使用可能な特定の状況でトラフィックブラックホールを引き起こす、**set tloc-list**アクションの不適切なポリシーアプリケーションについて説明します。

注：このドキュメントに記載されているすべてのコマンド出力は、vEdgeルータのものであります。ただし、IOS®-XE SDWANソフトウェアを実行するルータのトラブルシューティングアプローチは同じです。IOS®-XE SDWANソフトウェアで同じ出力を取得するには、**sdwan**キーワードを使用します。たとえば、**show omp routes**の代わりに**show sdwan omp routes**を使用します。

## 背景説明

デモンストレーションの目的で、また後で説明する問題をよりよく理解するために、次のトポロジ図を検討してください。



その他に、次の表にシステム設定をまとめます。

ホスト名	site-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

vEdge1とvEdge3の両方に、サービス側VPNのネクストホップを指すスタティックルートが設定されています。

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

!

これらの目標を達成するには、次のようにします。

1. vEdge1メトロイーサネットリンクを、「サイト13」に入る入カトラフィックの優先リンクにします。
- 2.M「サイト13」に入る入カトラフィックの2番目の優先リンクとして、vEdge3メトロイーサネットリンクを使用します。
3. vEdge1パブリックインターネットリンクを、「サイト13」に入る入カトラフィックの3番目の優先リンクにします。
4. vEdge3 public-internetリンクを、「サイト13」に入る入カトラフィックに対するleast優先リンクにします。

次のvSmart制御ポリシーが設定されます。

```
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
 !
 !
```

## 問題

### 通常の状態

vSmartは、次の4つのTLOCをネクストホップとして使用してこれらのルートを取得します。

```
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 metro-ethernet ipsec	10.155.0.118 -	35	1002	C,R	installed	10.155.0.118
		10.155.0.118	37	1002	C,R	installed	10.155.0.118
public-internet	ipsec	-					
metro-ethernet	ipsec	-	35	1002	C,R	installed	10.155.0.120
public-internet	ipsec	-	37	1002	C,R	installed	10.155.0.120

アドバタイズされたルートのプリファレンスを設定します。

```
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は適切なTLOCを選択し、このルートをルーティングテーブルにインストールします。

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

トラフィック転送は意図したとおりに動作します。

```
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
```

## 障害状態

最終的には、vEdge1で障害が発生し、サービス側のLAN側インターフェイスがダウンします (ま

たは、テストを実行するために管理者によってシャットダウンされます。たとえば、結果は同じになります)。

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

TCP	IF	IF	IF	ADMIN	OPER	TRACKER	ENCAP	PORT	MTU	HWADDR
SPEED	AF	RX	TX	STATUS	STATUS	STATUS	TYPE	TYPE		
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				

vEdge1には10.223.115.101/32ルートの有効なネクストホップがないため、このルートはルーティングテーブルと転送テーブルから削除され、vSmartにアドバタイズされなくなります。

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

VPN	PREFIX	PROTOCOL	PROTOCOL	NEXTHOP	NEXTHOP	NEXTHOP	TLOC
IP	COLOR	ENCAP	STATUS	SUB TYPE	IF NAME	ADDR	VPN
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#
```

同時に、vEdge3は引き続きこのルートをアドバタイズします (これは予想どおりです)。

```
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は、予想どおりvEdge3から2つのルートを取得します。

```

vsmart1# show omp routes 10.223.115.101/32 | b PATH

```

VPN	PREFIX	FROM PEER	PATH	ID	LABEL	STATUS	ATTRIBUTE	TLOC IP
COLOR	ENCAP	PREFERENCE					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

しかし同時に、vSmartは次のことをアドバタイズし続けます。

```

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

```

ご覧のように、唯一の発信元が変更されています。tloc-listアクションは（おおまかに言えば）「set next-hop」と同様に動作し、誤ったTLOCを強制的に設定するため、到達可能性が失われるので、これは予期された動作です。

```

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 * * *
```

## 解決方法

解決策として、誤ったTLOCネクストホップ情報の設定を避けるために、次の方法が提案されています。

```
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
```

!  
!

このようなポリシーにより、状況が改善され、誤ったTLOCネクストホップを持つルートのアドバタイズメントが防止されます。

```
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
```

その結果、障害シナリオ全体を通じて到達可能性が維持されます。

```
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
```



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。