O uso inadequado da "lista de permissão do conjunto de ações de política" leva à prática de "buraco negro de tráfego"

Contents

[Introduction](#)
[Informações de Apoio](#)
[Problema](#)
[Condições normais](#)
[Condições de falha](#)
[Solução](#)

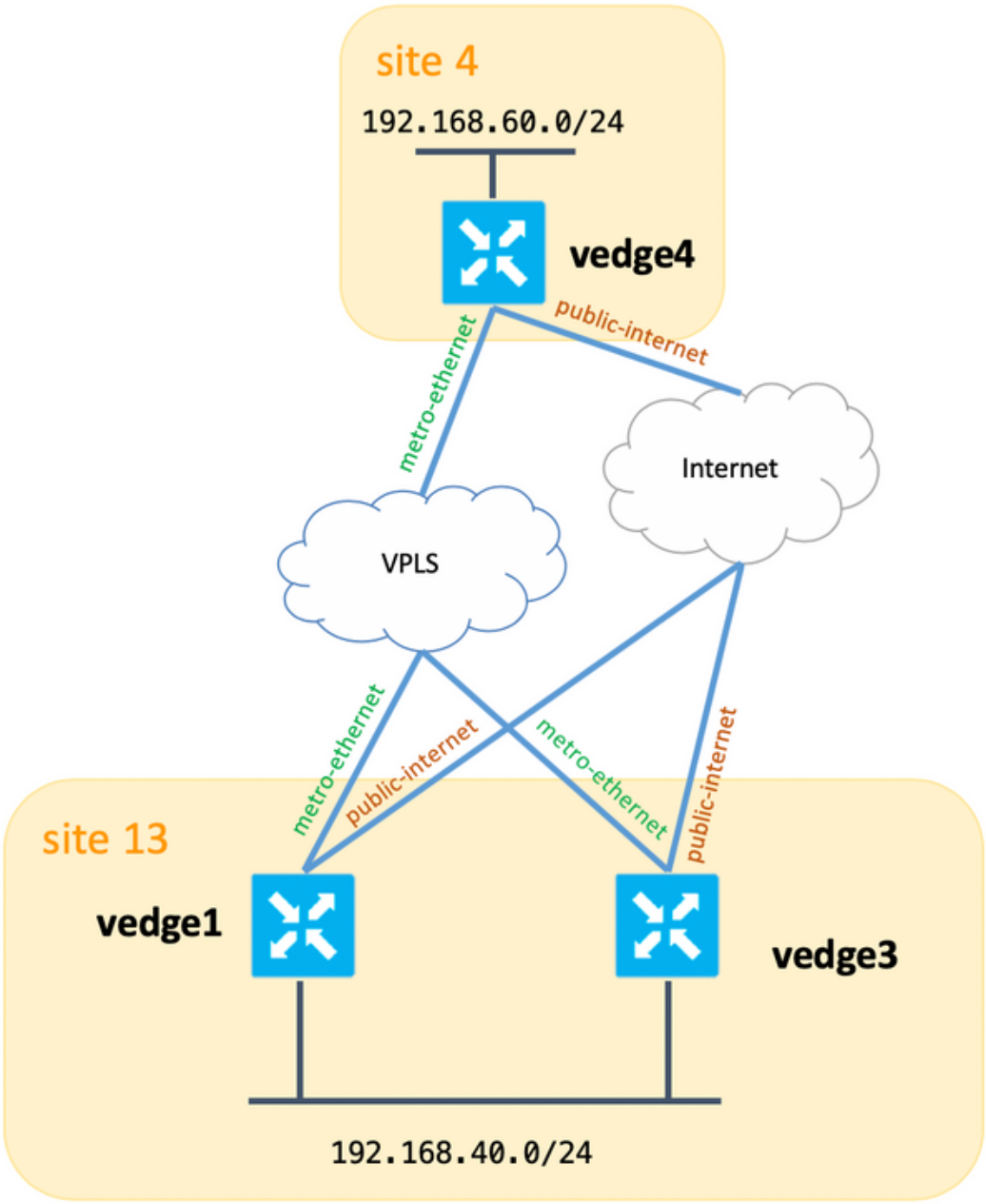
Introduction

Este documento descreve a aplicação de política inapropriada da ação **set tloc-list** que leva a blackholing de tráfego em certas situações quando o link preferencial fica inativo, mas os caminhos de backup ainda estão disponíveis.

> **Note**: Todas as saídas de comando apresentadas neste documento são de roteadores vEdge. No entanto, a abordagem de identificação e solução de problemas permanece a mesma para um roteador que executa o software SDWAN IOS®-XE. Use a palavra-chave **sdwan** para obter as mesmas saídas no software SDWAN IOS®-XE. Por exemplo, **show sdwan omp routes** em vez de **show omp routes**.

Informações de Apoio

Para fins de demonstração e para compreender melhor o problema descrito posteriormente, considere este diagrama de topologia:



Além disso, aqui está a tabela que resume as configurações do sistema:

hostname	ID do site	system-ip
védge1	13	10.155.0.118
Védge3	13	10.155.0.120
Védge4	4	10.155.0.50
vsmart1	1	10.155.0.3

O vEdge1 e o vEdge3 têm uma rota estática configurada que aponta para algum próximo salto na VPN do lado do serviço:

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

Para atingir esses objetivos:

1. Torne o link metro-ethernet do vEdge1 o link preferencial para tráfego de entrada no "site 13".

2. MUse o link metro-ethernet vEdge3 como o segundo link preferencial para tráfego de entrada no "site 13".

3. Torne o link público-internet do vEdge1 o terceiro link preferencial para tráfego de entrada no "site 13".

4. Faça com que o link de internet pública vEdge3 seja o link menos preferencial para o tráfego de entrada que entra no "site 13".

Esta política de controle vSmart está configurada:

```
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
 !
!
```

Problema

Condições normais

A vSmart obtém essas rotas com 4 TLOCs possíveis como próximos saltos:

```
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  -
```

E define uma preferência para rotas anunciadas de acordo:

```
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
```

O vEdge4 seleciona um TLOC apropriado e instala essa rota na tabela de roteamento:

```
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
```

O encaminhamento de tráfego funciona conforme o esperado:

```
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
```

Condições de falha

Eventualmente, uma falha ocorre no vEdge1 e a interface da LAN do lado do serviço é desativada (ou é desativada pelo administrador para executar um teste, por exemplo, o resultado será o mesmo):

```
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
```

Como o vEdge1 não tem um próximo salto válido para a rota 10.223.115.101/32, essa rota é removida das tabelas de roteamento e encaminhamento e não a anuncia mais ao 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#
```

Ao mesmo tempo, o vEdge3 ainda anuncia essa rota (isso é esperado):

```
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
```

O vSmart obtém 2 rotas agora do vEdge3 conforme esperado:

```
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  -
```

Mas, ao mesmo tempo, a vSmart continua a anunciar isso:

```
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
```

Como você pode ver, o único originador foi alterado e esse é o comportamento esperado porque a ação **tloc-list** age semelhante a (grosso modo) "set next-hop" e define com força o TLOC errado, portanto, a acessibilidade é perdida.

```
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  * * *
```

Solução

Como solução, essa abordagem é proposta para evitar a configuração de informações erradas do próximo salto do TLOC:

```
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
 !
!
```

Essa política melhora a situação e impede o anúncio da rota com o próximo salto TLOC errado:

```
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
```

E, como resultado, a acessibilidade em todos os cenários de falha é preservada:

```
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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.