Por que a ação de bloqueio em uma política de controle centralizada não funciona?

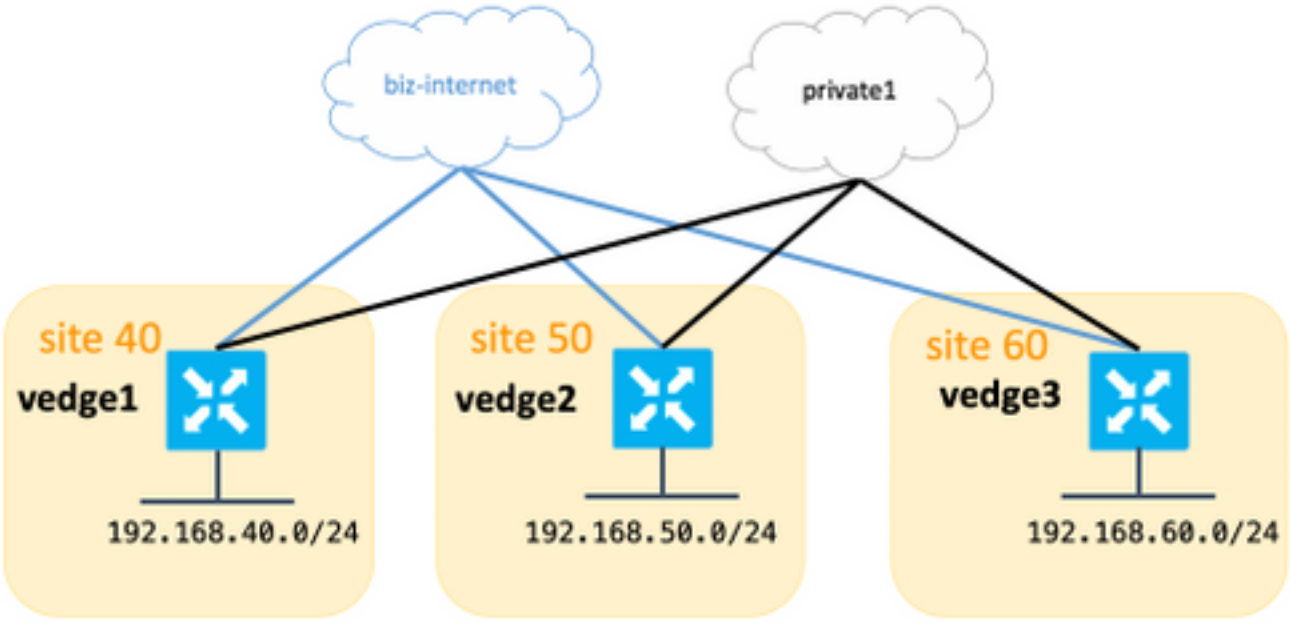
Contents

Introduction

Este documento descreve o problema que ocorre com as rotas do Protocolo de Gerenciamento de Sobreposição (OMP - Overlay Management Protocol) se o comando **set-action** na política de controle centralizada for usado e explica o motivo pelo qual isso acontece e como resolvê-lo.

Topologia

Para entender melhor o problema, consulte este diagrama de topologia simples que descreve a configuração:



Configuração

Para os fins deste artigo, o vEdge e a versão 18.3.5 do software da controladora foram usados.

Todos os sites têm conexão com a **Internet de empresas** e com cores **privadas**, esta tabela

resume a configuração.

hostname	ID do site	system-ip	ip-address no link biz-internet	ip-address no link private1
vEdge1	40	192.168.30.104	192.168.109.181	192.168.110.181
vEdge2	50	192.168.30.105	192.168.109.182	192.168.110.182
vEdge3	60	192.168.30.106	192.168.109.183	192.168.110.183
vSmart	1	192.168.30.103		

Não há configurações especiais em Bordas. A configuração com duas rotas padrão é bem simples e omitida aqui para ser breve.

No vSmart, essa configuração foi aplicada:

```
 lists
  vpn-list VPN_40
   vpn 40
  !
  site-list sites_40_60
   site-id 40
   site-id 60
  !
  prefix-list SITE_40
   ip-prefix 192.168.40.0/24
  !
  prefix-list SITE_60
   ip-prefix 192.168.60.0/24
  !
 !
control-policy REDIRECT_VIA_VEDGE2
  sequence 10
   match route
    prefix-list SITE_40
   !
   action accept
    set
     tloc-action primary
     tloc 192.168.30.105 color biz-internet encap ipsec
```

```
    !
   !
  !
  sequence 20
   match route
    prefix-list SITE_60
   !
   action accept
    set
     tloc-action primary
     tloc 192.168.30.105 color biz-internet encap ipsec
    !
   !
  !
  default-action accept
 !
apply-policy
 site-list sites_40_60
  control-policy REDIRECT_VIA_VEDGE2 out
 !
!
```

O objetivo principal dessa política é redirecionar o tráfego do site 40 para o site 60 através do site de destino intermediário 50 e usar a **internet** preferencialmente.

Problema

Na saída **show omp routes**, você vê que as rotas via **biz-internet** não podem ser instaladas no vEdge1, vEdge3 e o status está definido como Inválido e Não Resolvido (**Inv,U**):

```
vedge1# show omp routes | b PATH
                                          PATH                      ATTRIBUTE
VPN    PREFIX              FROM PEER      ID     LABEL    STATUS    TYPE       TLOC IP
COLOR            ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------
-------------------------------------
40     192.168.40.0/24     0.0.0.0        68     1002     C,Red,R   installed  192.168.30.104
biz-internet     ipsec  -
                           0.0.0.0        81     1002     C,Red,R   installed  192.168.30.104
private1         ipsec  -
40     192.168.50.0/24     192.168.30.103 4      1002     C,I,R     installed  192.168.30.105
biz-internet     ipsec  -
                           192.168.30.103 10     1002     C,I,R     installed  192.168.30.105
private1         ipsec  -
40 192.168.60.0/24 192.168.30.103 8 1002 Inv,U installed 192.168.30.105 biz-internet ipsec -
192.168.30.103 9 1002 C,I,R installed 192.168.30.106 biz-internet ipsec -

vedge3# show omp routes | b PATH
                                          PATH                      ATTRIBUTE
VPN    PREFIX              FROM PEER      ID     LABEL    STATUS    TYPE       TLOC IP
COLOR            ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------
-------------------------------------
40 192.168.40.0/24 192.168.30.103 19 1002 Inv,U installed 192.168.30.105 biz-internet ipsec -
192.168.30.103 20 1002 C,I,R installed 192.168.30.104 biz-internet ipsec - 40 192.168.50.0/24
192.168.30.103 16 1002 C,I,R installed 192.168.30.105 biz-internet ipsec - 192.168.30.103 21
1002 C,I,R installed 192.168.30.105 private1 ipsec - 40 192.168.60.0/24 0.0.0.0 68 1002 C,Red,R
installed 192.168.30.106 biz-internet ipsec - 0.0.0.0 81 1002 C,Red,R installed 192.168.30.106
private1 ipsec -
```

Ao mesmo tempo, você vê túneis de plano de dados na **Internet de base** funcionando entre vEdge1 e vEdge3:

```
vedge1# show bfd sessions
                                      SOURCE TLOC      REMOTE TLOC
DST PUBLIC                       DST PUBLIC         DETECT      TX
SYSTEM IP        SITE ID  STATE       COLOR            COLOR           SOURCE IP
IP                               PORT        ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME
TRANSITIONS
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-------------
192.168.30.105   50       up          biz-internet     biz-internet     192.168.109.181
192.168.109.182                  12366       ipsec  7           1000           0:02:52:22      0
192.168.30.105   50       up          private1         private1         192.168.110.181
192.168.110.182                  12366       ipsec  7           1000           0:00:00:12      1
192.168.30.106   60       up          biz-internet     biz-internet     192.168.109.181
192.168.109.183                  12366       ipsec  7           1000           0:02:52:22      0
192.168.30.106   60       up          private1         private1         192.168.110.181
192.168.110.183                  12366       ipsec  7           1000           0:00:56:28      0


vedge3# show bfd sessions
                                      SOURCE TLOC      REMOTE TLOC
DST PUBLIC                       DST PUBLIC         DETECT      TX
SYSTEM IP        SITE ID  STATE       COLOR            COLOR           SOURCE IP
IP                               PORT        ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME
TRANSITIONS
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-------------
192.168.30.104   40       up          biz-internet     biz-internet     192.168.109.183
192.168.109.181                  12366       ipsec  7           1000           0:02:54:25      0
192.168.30.104   40       up          private1         private1         192.168.110.183
192.168.110.181                  12366       ipsec  7           1000           0:00:58:30      0
192.168.30.105   50       up          biz-internet     biz-internet     192.168.109.183
192.168.109.182                  12366       ipsec  7           1000           0:02:54:25      0
192.168.30.105   50       up          private1         private1         192.168.110.183
192.168.110.182                  12366       ipsec  7           1000           0:00:57:26      0
```

Na saída detalhada do comando show omp route, você vê o **tloc** definido corretamente e também o **untimate-tloc** está definido, mas o status é **Inv,U** e o motivo da perda é **inválido**:

```
vedge3# show omp routes 192.168.40.0/24 detail

---------------------------------------------------
omp route entries for vpn 40 route 192.168.40.0/24
---------------------------------------------------
            RECEIVED FROM:
peer            192.168.30.103
path-id         19
label 1002 status Inv,U loss-reason invalid lost-to-peer 192.168.30.103 lost-to-path-id 20
Attributes: originator 192.168.30.104 type installed tloc 192.168.30.105, biz-internet, ipsec
ultimate-tloc 192.168.30.104, biz-internet, ipsec -- primary domain-id not set overlay-id 1
site-id 40 preference not set tag not set origin-proto connected origin-metric 0 as-path not set
unknown-attr-len not set RECEIVED FROM: peer 192.168.30.103 path-id 20 label 1002 status C,I,R
loss-reason not set lost-to-peer not set lost-to-path-id not set Attributes: originator
192.168.30.104 type installed tloc 192.168.30.104, biz-internet, ipsec ultimate-tloc not set
domain-id not set overlay-id 1 site-id 40 preference not set tag not set origin-proto connected
```

```
origin-metric 0 as-path not set unknown-attr-len not set
```

> **Note**: Um bloco final é o TLOC ao qual o salto intermediário cria um túnel de plano de dados (IPsec ou Generic Routing Encapsulation (GRE)) para chegar ao destino final.

> **Note: a ação de bloqueio** só é suportada de ponta a ponta se a cor de transporte for a mesma de um local para o salto intermediário e do salto intermediário para o destino final. Se o transporte usado para chegar ao salto intermediário de um local for de uma cor diferente do transporte usado do salto intermediário para chegar ao destino final, isso causará um problema com ação de bloqueio.

Você pode ver que o objetivo principal não é alcançado e que o tráfego segue o caminho direto como pode ser visto no host da sub-rede 192.168.40.0/24:

```
traceroute -n 192.168.60.20
traceroute to 192.168.60.20 (192.168.60.20), 30 hops max, 60 byte packets
 1  192.168.40.104  0.288 ms  0.314 ms  0.266 ms
 2  192.168.60.106  0.911 ms  1.045 ms  1.140 ms
 3  192.168.60.20  1.213 ms !X  1.289 ms !X  1.224 ms !X
```

Solução

Como causa raiz, inicialmente suspeitava-se que o defeito de software CSCvm64622 foi atingido, mas após uma investigação adicional, concluiu-se que não tinha sido configurado corretamente devido ao fato de a documentação do produto não ser clara sobre os requisitos **de ação de bloqueio**. Portanto, a seção de documentação sobre a ação da TLOC é atualizada com este:

> **Observação**: se a ação for **aceitar set-action**, configure o **TE de serviço** no destino intermediário.

Portanto, no cenário atual, a configuração **de serviço TE** é necessária no vEdge2 para fazer com que a política de controle centralizado funcione porque você usa a Engenharia de Tráfego (TE) essencialmente por meio de um caminho arbitrário:

```
vedge2(config)# vpn 40
vedge2(config-vpn-40)# service ?
Possible completions:
  FW  IDP  IDS  TE  netsvc1  netsvc2  netsvc3  netsvc4
vedge2(config-vpn-40)# service TE
vedge2(config-vpn-40)# commit
Commit complete.
```

Ele resolve o problema com a política de controle desde que o vEdge2 começa a anunciar o serviço TE:

```
vsmart1# show omp services | b PATH
                                                  PATH
VPN     SERVICE   ORIGINATOR      FROM PEER        ID      LABEL     STATUS
-----------------------------------------------------------------------------
40      VPN       192.168.30.104  192.168.30.104   68      1002      C,I,R
                                  192.168.30.104   81      1002      C,I,R
40      VPN       192.168.30.105  192.168.30.105   68      1002      C,I,R
```

```
                                192.168.30.105   81     1002     C,I,R
40     VPN      192.168.30.106  192.168.30.106   68     1002     C,I,R
                                192.168.30.106   81     1002     C,I,R
40     TE 192.168.30.105 192.168.30.105 68 1007 C,I,R 192.168.30.105 81 1007 C,I,R
```

O vEdge1 e o vEdge3 instalam as rotas com êxito agora, observe que o status está definido como **C,I,R**:

```
vedge3# show omp routes 192.168.40.0/24 detail

---------------------------------------------------
omp route entries for vpn 40 route 192.168.40.0/24
---------------------------------------------------
            RECEIVED FROM:
peer            192.168.30.103
path-id      19 label 1002 status C,I,R loss-reason not set lost-to-peer not set lost-to-path-id
not set Attributes: originator 192.168.30.104 type installed tloc 192.168.30.105, biz-internet,
ipsec ultimate-tloc 192.168.30.104, biz-internet, ipsec -- primary domain-id not set overlay-id
1 site-id 40 preference not set tag not set origin-proto connected origin-metric 0 as-path not
set unknown-attr-len not set RECEIVED FROM: peer 192.168.30.103 path-id 20 label 1002 status R
loss-reason tloc-action lost-to-peer 192.168.30.103 lost-to-path-id 19 Attributes: originator
192.168.30.104 type installed tloc 192.168.30.104, biz-internet, ipsec ultimate-tloc not set
domain-id not set overlay-id 1 site-id 40 preference not set tag not set origin-proto connected
origin-metric 0 as-path not set unknown-attr-len not set vedge3# show ip routes 192.168.40.0/24
| b PROTOCOL PROTOCOL NEXTHOP NEXTHOP NEXTHOP VPN PREFIX PROTOCOL SUB TYPE IF NAME ADDR VPN TLOC
IP COLOR ENCAP STATUS ----------------------------------------------------------------------------
------------------------------------------------------------------ 40 192.168.40.0/24 omp - - -
- 192.168.30.105 biz-internet ipsec F,S
```