¿Por qué no funciona establecer la acción de bloqueo en una política de control centralizada?

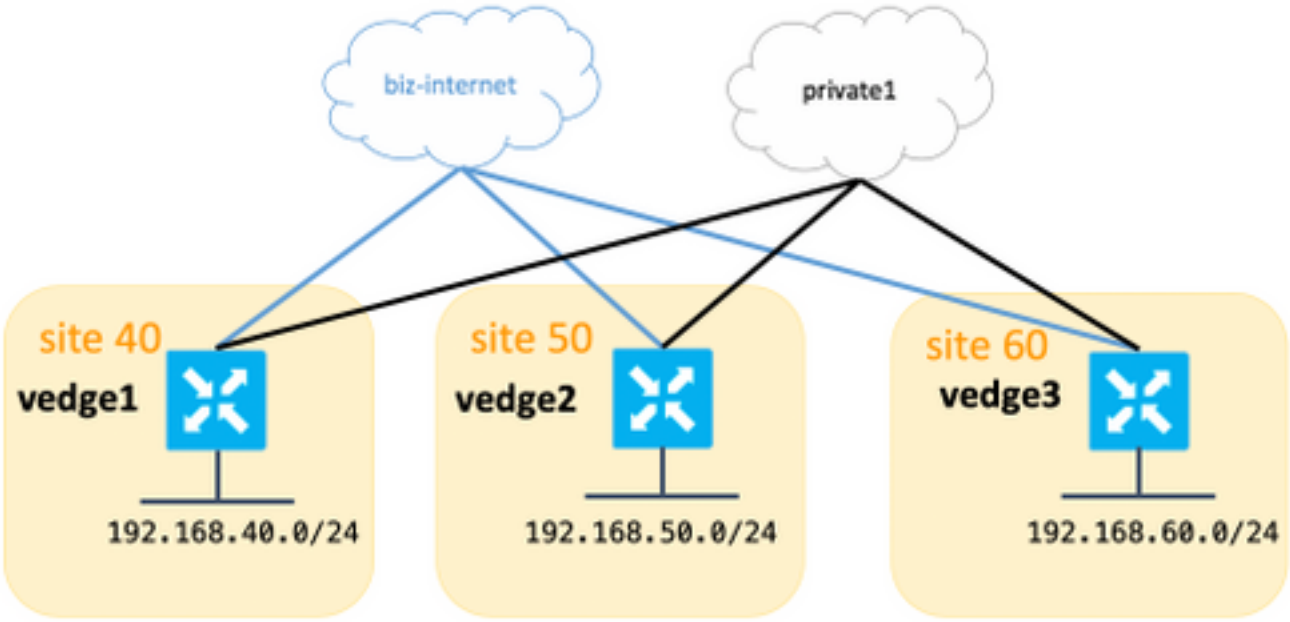
Contenido

Introducción

Este documento describe el problema que ocurre con las rutas del protocolo de administración superpuesta (OMP) si se utiliza el comando **set tloc-action** en la política de control centralizado y explica la razón por la que ocurre y cómo resolverlo.

Topología

Para entender mejor el problema, consulte este diagrama de topología simple que describe la configuración:



Configuración

A los efectos de este artículo, se utilizaron vEdge y el software de controladores versión 18.3.5.

Todos los sitios tienen conexión a **internet biz** y **colores privados**, esta tabla resume la

configuración.

nombre del host	Site-ID	system-ip	ip-address en el enlace biz-internet	ip-address en 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		

No hay configuraciones especiales en los bordes. La configuración con dos rutas predeterminadas es bastante sencilla y se omite aquí por brevedad.

En vSmart, se aplicó esta configuración:

```
 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
 !
!
```

El objetivo principal de esta política es redirigir el tráfico del sitio 40 al sitio 60 a través del sitio de destino intermedio 50 y utilizar **biz-internet** preferiblemente.

Problema

En la salida **show omp routes** , verá que las rutas a través de **biz-internet** no se pueden instalar en vEdge1, vEdge3 y el estado se establece en Invalid and unResolution (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 -
```

Al mismo tiempo, verá túneles del plano de datos en **Internet biz** en funcionamiento entre vEdge1 y 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
```

En el resultado detallado de show omp route, verá el **tloc** configurado correctamente y también el **untimate-tloc** está configurado, pero el estado es **Inv,U** y el motivo de pérdida es 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
```

> **Nota:** Un finalmente trloc es el TLOC al que el salto intermedio construye el túnel del plano de datos (IPsec o Generic Routing Encapsulation (GRE)) para llegar al destino final.

> **Nota: tloc-action** sólo se admite de extremo a extremo si el color de transporte es el mismo desde un sitio al salto intermedio y desde el salto intermedio al destino final. Si el transporte utilizado para llegar al salto intermedio desde un sitio es de un color diferente al transporte utilizado desde el salto intermedio para llegar al destino final, esto causará un problema con tloc-action.

Puede ver que el objetivo principal no se alcanza y el tráfico sigue la ruta directa como se puede ver en el host desde la subred 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
```

Solución

Como causa principal, inicialmente se sospechó que el defecto del software CSCvm64622 fue atacada, pero después de una investigación adicional, se encontró que fue una configuración errónea debido al hecho de que la documentación del producto no estaba clara acerca de los requisitos **de acción de bloqueo**. Por lo tanto, la sección de documentación con respecto a la acción TLOC se actualiza con esto:

> **Nota**: Si la acción es **accept set tloc-action, configure el servicio TE en el destino intermedio.**

Por lo tanto, en el escenario actual se requiere la configuración **TE del servicio** en vEdge2 para que funcione la política de control centralizado, ya que se utiliza la ingeniería de tráfico (TE) básicamente mediante la dirección a través de una ruta arbitraria:

```
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.
```

Resuelve el problema con la política de control, ya que vEdge2 comienza a anunciar el servicio 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
```

vEdge1 y vEdge3 instalan las rutas correctamente ahora, tenga en cuenta que el estado está establecido en **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
```