使用集中控制策略和应用路由策略配置多个传输和流量工程

目录

简介

本文档介绍如何配置集中式控制策略和应用路由策略以实现站点之间的流量工程。它也可作为特定用例的特定设计指南。
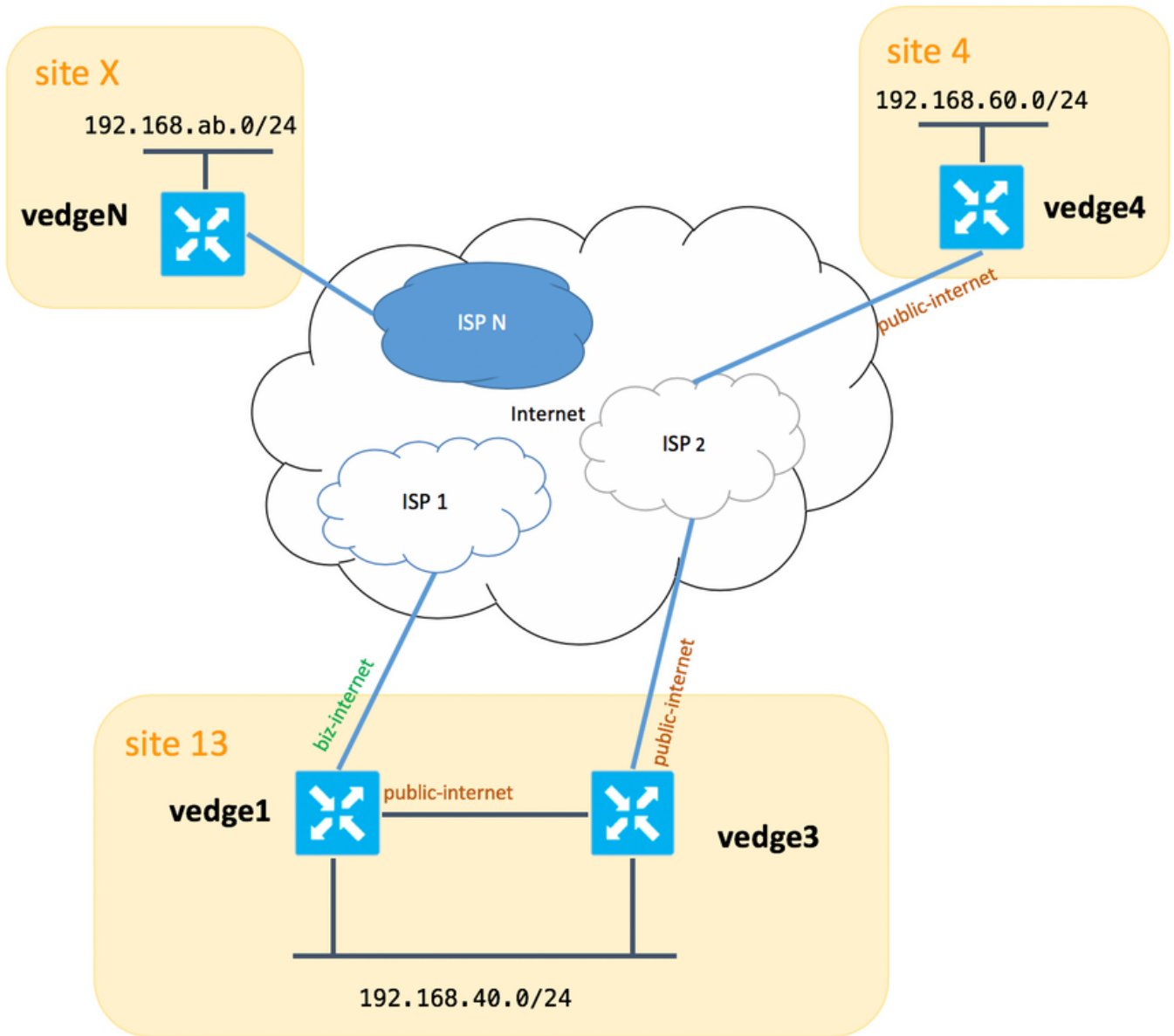
先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

为了演示和更好地了解后面介绍的问题，请考虑此图中显示的拓扑。

请注意，通常在**vedge1** 和**vedge3** 之间，您应该还有第二个链路/子接口用于**biz-internet** TLOC扩展，但为简单起见，此处未配置它。

以下是vEdge/vSmart的相应系统设置（vedge2代表所有其他站点）：

主机名	站点ID	system-ip
vedge1	13 个	192.168.30.4
vedge3	13 个	192.168.30.6
vedge4	4	192.168.30.7
vedgex	X	192.168.30.5
vsmart1	1	192.168.30.3

在此，您可以找到传输端配置以供参考。

vedge1:

```
vedge1# show running-config vpn 0
vpn 0
 interface ge0/0
  description "ISP_1"
```

```
   ip address 192.168.109.4/24
   nat
    respond-to-ping
    !
   tunnel-interface
    encapsulation ipsec
    color biz-internet
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    allow-service stun
    !
   no shutdown
  !
  interface ge0/3
   description "TLOC-extension via vedge3 to ISP_2"
   ip address 192.168.80.4/24
   tunnel-interface
    encapsulation ipsec
    color public-internet
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    allow-service stun
    !
   no shutdown
  !
  !
  ip route 0.0.0.0/0 192.168.80.6
  ip route 0.0.0.0/0 192.168.109.10
 !
```

vedge3:

```
vpn 0
 interface ge0/0
  description "ISP_2"
  ip address 192.168.110.6/24
  nat
   respond-to-ping
   !
  tunnel-interface
   encapsulation ipsec
   color public-internet
   carrier carrier3
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
```

```
  no allow-service stun
  !
  no shutdown
 !
 interface ge0/3
  ip address 192.168.80.6/24
  tloc-extension ge0/0
  no shutdown
 !
 ip route 0.0.0.0/0 192.168.110.10
```

vedge4:

```
vpn 0
 interface ge0/1
  ip address 192.168.103.7/24
  tunnel-interface
   encapsulation ipsec
   color public-internet
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   allow-service ospf
   no allow-service stun
  !
  no shutdown
 !
 ip route 0.0.0.0/0 192.168.103.10
!
```

问题

用户希望实现以下目标：

Internet服务提供ISP 2应优先在站点13和**站点4**之**间通**信，原因如下。例如，ISP内部客户端之间的连接/连接质量非常好，但由于ISP上行链路出现一些故障或拥塞，其余Internet连接质量不符合公司的SLA，因此一般应避免此ISP(本例中为**ISP 2**)。

站点13应首**选公**共互联网上行链路连接到站点4，但仍应保持冗余，并且在公共互联网发生故障时应能**到达站点4。**

站点4仍应直接与所有其他站点保持尽力连接(因此，您不能在vedge4上使用**restrict**关键字**来实现**该目标)。

站点**13**应使用带有**biz-internet**颜色的更优质链接来到达所有其他站点(拓扑图上的**站点X**表示)。

另一个原因可能是ISP内流量免费时的成本/定价问题，但是当流量从提供商网络（自治系统）流出时，成本会高得多。

一些对SD-WAN方法不熟悉并习惯传统路由的用户可能会开始配置静态路由，以强制流量从**vedge1**通过vedge1和**vedge3之间的TLOC扩展接口从vedge4** 公共接口地址发往vedge4 ，但它不会给出预期结果，并会造成混乱，因为：

管理平面流量（例如ping、traceroute实用程序数据包）遵循所需路由。

同时，SD-WAN数据平面隧道（IPsec或gre传输隧道）会忽略路由表信息，并根据TLOC颜色建立**连接。**

由于静态路由没有智能，如果vedge3上的公共互联网TLOC关闭（通往ISP 2的上行链路），则vedge1不会注意到此情况，并且与**vedge4**的连接会失败，尽管vedge1仍具有biz-internet可用。

因此，应避免这种方法，而且不能使用。

解决方案

1.在向vedge4通告相应的OMP路由时，使用集中控制策略在**vSmart控制器上设置**公共Internet TLOC的首选项。它有助于将所需的流量路径从站点4**存档到站点**13。

2.要实现从站点**13**到站点**4**反向的所需流量路径，您无法使用集中控制策略，因为**vedge4** 只有一个可用TLOC，因此不能将首选项设置为任何值，但您可以使用应用路由策略实现来自站点13的出口流量的此结果。

以下是集中控制策略在vSmart控制器上的外观，以便首选公**共互联网TLOC**以访问**站点13**:

```
policy
 control-policy S4_S13_via_PUB
  sequence 10
   match tloc
    color   public-internet
    site-id 13
   !
   action accept
    set
     preference 333
    !
   !
  !
  default-action accept
 !
!
```

下面是一个应用路由策略示例，它首选公共**互联网上**行链路作为出口流量从站点13**到站点4的出口点**:

```
policy
 app-route-policy S13_S4_via_PUB
  vpn-list CORP_VPNs
   sequence 10
    match
     destination-data-prefix-list SITE4_PREFIX
    !
    action
     count                    COUNT_PKT
     sla-class SLA_CL1 preferred-color public-internet
    !
   !
  !
 !
```

```
policy
 lists
  site-list S13
   site-id 13
  !
  site-list S40
   site-id 4
  !
  data-prefix-list SITE4_PREFIX
   ip-prefix 192.168.60.0/24
  !
  vpn-list CORP_VPNs
   vpn 40
  !
 !
 sla-class SLA_CL1
  loss    1
  latency 100
  jitter  100
 !
```

应在vSmart控制器上适当应用策略：

```
apply-policy
 site-list S13
  app-route-policy S13_S4_via_PUB
 !
 site-list S4
  control-policy S4_S13_via_PUB out
 !
!
```
另请记住，应用路由策略不能配置为本地化策略，应仅应用于vSmart。

验证

请注意，应用路由策略不会应用于vEdge本地生成的流量，因此，为了验证是否根据建议从相应站点的LAN网段生成某些流量的所需路径引导的流量。作为高级测试场景，您可以使用iperf在站点13和站点4的LAN网段中的主机之间生成流量，然后检查接口统计信息。例如，在我的案例中，除系统生成外，没有任何流量，因此您可以看到通过ge0/3接口到vedge3上TLOC扩展的大量流量流量：

```
vedge1# show interface statistics
```

PPPOE	PPPOE	DOT1X	DOT1X									
			AF	RX			RX	RX	TX		TX	TX
RX	RX	TX	TX	TX	RX	TX	RX					
VPN	INTERFACE	TYPE	PACKETS	RX OCTETS		ERRORS	DROPS	PACKETS	TX OCTETS		ERRORS	DROPS
PPS	Kbps	PPS	Kbps	PKTS	PKTS	PKTS	PKTS					
0	ge0/0	ipv4	1832	394791		0	167	1934	894680		0	0
26	49	40	229	–	–	0	0					
0	ge0/2	ipv4	0	0		0	0	0	0		0	0
0	0	0	0	–	–	0	0					
0	ge0/3	ipv4	3053034	**4131607715**		0	27	2486248	**3239661783**		0	0
51933	**563383**	**41588**	**432832**	–	–	0	0					

```
0     ge0/4       ipv4  0        0           0      0     0     0          0        0
0     0     0     0     -     -     0     0
```

故障排除

首先，确保建立相应的BFD会话(不要在任何位置**使用**restrict关键字):

```
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
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------
192.168.30.5    2        up       public-internet  public-internet  192.168.80.4
192.168.109.5                   12386      ipsec  7            1000             0:02:10:54      3
192.168.30.5    2        up       biz-internet     public-internet  192.168.109.4
192.168.109.5                   12386      ipsec  7            1000             0:02:10:48      3
192.168.30.7    4        up       public-internet  public-internet  192.168.80.4
192.168.103.7                   12366      ipsec  7            1000             0:02:11:01      2
192.168.30.7    4        up       biz-internet     public-internet  192.168.109.4
192.168.103.7                   12366      ipsec  7            1000             0:02:10:56      2


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
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------
192.168.30.5    2        up       public-internet  public-internet  192.168.110.6
192.168.109.5                   12386      ipsec  7            1000             0:02:11:05      1
192.168.30.7    4        up       public-internet  public-internet  192.168.110.6
192.168.103.7                   12366      ipsec  7            1000             0:02:11:13      2


vedge4# 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
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------
192.168.30.4    13       up       public-internet  biz-internet     192.168.103.7
192.168.109.4                   12346      ipsec  7            1000             0:02:09:11      2
192.168.30.4    13       up       public-internet  public-internet  192.168.103.7
192.168.110.6                   63084      ipsec  7            1000             0:02:09:16      2
192.168.30.5    2        up       public-internet  public-internet  192.168.103.7
192.168.109.5                   12386      ipsec  7            1000             0:02:09:10      3
192.168.30.6    13       up       public-internet  public-internet  192.168.103.7
192.168.110.6                   12386      ipsec  7            1000             0:02:09:07      2
```

如果无法通过流量工程获得预期结果，请检查策略是否正确应用:

1.在vedge4上，您应检查是否选择了从站点13适当的TLOC发起的前缀：

```
vedge4# show omp routes 192.168.40.0/24 detail

---------------------------------------------------
omp route entries for vpn 40 route 192.168.40.0/24
---------------------------------------------------
            RECEIVED FROM:
peer             192.168.30.3
path-id          72
label            1002
status           R
loss-reason      tloc-preference
lost-to-peer     192.168.30.3
lost-to-path-id  74
    Attributes:
     originator      192.168.30.4
     type            installed
     tloc            192.168.30.4, biz-internet, ipsec
     ultimate-tloc   not set
     domain-id       not set
     overlay-id       1
     site-id         13
     preference      not set
     tag             not set
     origin-proto    connected
     origin-metric   0
     as-path         not set
     unknown-attr-len not set
            RECEIVED FROM:
peer             192.168.30.3
path-id          73
label            1002
status           C,I,R
loss-reason      not set
lost-to-peer     not set
lost-to-path-id  not set
    Attributes:
     originator      192.168.30.4
     type            installed
     tloc            192.168.30.4, public-internet, ipsec
     ultimate-tloc   not set
     domain-id       not set
     overlay-id       1
     site-id         13
     preference      not set
     tag             not set
     origin-proto    connected
     origin-metric   0
     as-path         not set
     unknown-attr-len not set
            RECEIVED FROM:
peer             192.168.30.3
path-id          74
label            1002
status           C,I,R
loss-reason      not set
lost-to-peer     not set
lost-to-path-id  not set
    Attributes:
     originator      192.168.30.6
     type            installed
```

```
      tloc            192.168.30.6, public-internet, ipsec
      ultimate-tloc   not set
      domain-id       not set
      overlay-id       1
      site-id         13
      preference      not set
      tag             not set
      origin-proto    connected
      origin-metric   0
      as-path         not set
      unknown-attr-len not set
```

2.在vedge1**和vedge3上**，确保安装vSmart的适当策略，并匹配和计数数据包：

```
vedge1# show policy from-vsmart
from-vsmart sla-class SLA_CL1
 loss    1
 latency 100
 jitter  100
from-vsmart app-route-policy S13_S4_via_PUB
 vpn-list CORP_VPNs
  sequence 10
   match
    destination-data-prefix-list SITE4_PREFIX
   action
    count                    COUNT_PKT
    backup-sla-preferred-color biz-internet
    sla-class         SLA_CL1
    no sla-class strict
    sla-class preferred-color public-internet
from-vsmart lists vpn-list CORP_VPNs
 vpn 40
from-vsmart lists data-prefix-list SITE4_PREFIX
 ip-prefix 192.168.60.0/24


vedge1# show policy app-route-policy-filter


                COUNTER
NAME          NAME  NAME    PACKETS   BYTES
----------------------------------------------------
S13_S4_via_PUB CORP_VPNs  COUNT_PKT   81126791  110610503611
```

 此外，您应该看到站点13通过公**共互联网**颜色发**送的更多数据包**(在我的测试期间，没有通过biz-internet **TLOC的**流量):

```
vedge1# show app-route stats remote-system-ip 192.168.30.7
app-route statistics 192.168.80.4 192.168.103.7 ipsec 12386 12366
 remote-system-ip 192.168.30.7
 local-color      public-internet
 remote-color     public-internet
 mean-loss        0
 mean-latency     1
 mean-jitter      0
 sla-class-index  0,1

        TOTAL            AVERAGE  AVERAGE  TX DATA  RX DATA
INDEX  PACKETS  LOSS  LATENCY  JITTER   PKTS     PKTS
-----------------------------------------------------------
0      600      0     0        0        0        0
```

```
1       600      0     1        0         5061061  6731986
2       600      0     0        0         3187291  3619658
3       600      0     0        0         0        0
4       600      0     2        0         9230960  12707216
5       600      0     1        0         9950840  4541723

app-route statistics 192.168.109.4 192.168.103.7 ipsec 12346 12366
 remote-system-ip 192.168.30.7
 local-color       biz-internet
 remote-color      public-internet
 mean-loss         0
 mean-latency      0
 mean-jitter       0
 sla-class-index   0,1

        TOTAL            AVERAGE  AVERAGE  TX DATA  RX DATA
INDEX   PACKETS  LOSS    LATENCY  JITTER   PKTS     PKTS
--------------------------------------------------------
0       600      0       0        0        0        0
1       600      0       1        0        0        0
2       600      0       0        0        0        0
3       600      0       0        0        0        0
4       600      0       2        0        0        0
5       600      0       0        0        0        0
```

相关信息

- https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.3/07Policy_Applications/01Application-Aware_Routing/01Configuring_Application-Aware_Routing
- https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.3/02System_and_Interfaces/06Configuring_Network_Interfaces
- https://sdwan-docs.cisco.com/Product_Documentation/Command_Reference/Configuration_Commands/color