Configuración de varios transportes e ingeniería de tráfico con política de control centralizada y política de ruta de aplicaciones

Contenido

Introducción

Este documento describe cómo configurar la política de control centralizado y la política de ruta de la aplicación para lograr la ingeniería de tráfico entre sitios. Podría considerarse también como una directriz de diseño específica para el caso práctico concreto.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

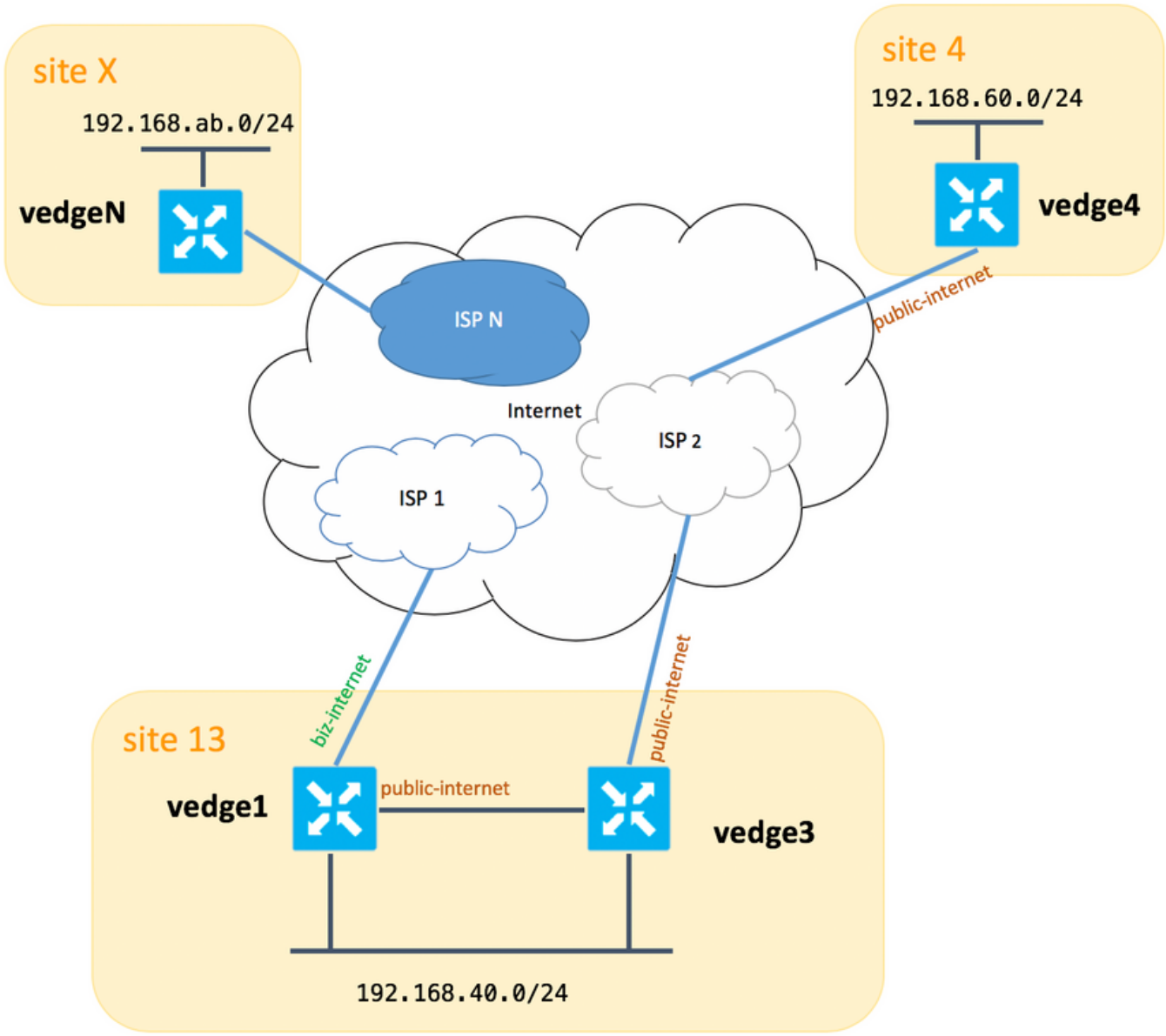
Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración

Para demostrarlo y comprender mejor el problema descrito más adelante, tenga en cuenta la topología mostrada en esta imagen.



Tenga en cuenta que, en general, entre **vedge1** y **vedge3**, debería tener un segundo link/subinterfaz para la **extensión TLOC biz-internet** también, pero aquí por razones de simplicidad no se configuró.

A continuación se indican las configuraciones del sistema correspondientes para vEdges/vSmart (vedge2 representa el resto de sitios):

nombre del host	Site-ID	system-ip
vedge1	13	192.168.30.4
vedge3	13	192.168.30.6
vedge4	4	192.168.30.7
vedgex	X	192.168.30.5
vsmart1	1	192.168.30.3

Aquí puede encontrar las configuraciones del lado del transporte como referencia.

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
!
```

Problema

El usuario desea alcanzar estos objetivos:

El servicio de Internet proporciona **ISP 2** debe ser preferido para comunicarse entre el **sitio 13** y el **sitio 4** por algunas razones. Por ejemplo, es un caso de uso bastante común y un escenario cuando la calidad de conexión/conectividad dentro de un ISP entre sus propios clientes es muy buena, pero hacia el resto de la calidad de conectividad de Internet no cumple con el SLA de la compañía debido a algunos problemas o congestión en un link ascendente ISP y por lo tanto este ISP (**ISP 2** en nuestro caso) debería ser evitado en general.

El sitio 13 debería preferir el enlace ascendente **público-internet** para conectarse al sitio **4**, pero aun así, mantener la redundancia y debería poder alcanzar el sitio 4 si falla la **conexión pública a internet**.

El **sitio 4** debe mantener la conectividad de mejor esfuerzo con todos los demás sitios directamente (por lo tanto, no puede usar la palabra clave **restrict** aquí en **vedge4** para lograr ese objetivo).

El **sitio 13** debe utilizar el enlace de mejor calidad con **biz-internet** color para llegar a todos los demás sitios (representado por el **sitio X en el diagrama de topología).**

Otra razón podría ser los problemas de costo/precio cuando el tráfico dentro del ISP es gratuito, pero mucho más caro cuando el tráfico sale de una red de proveedor (sistema autónomo).

Algunos usuarios que no tienen experiencia con el enfoque de SD-WAN y se acostumbran al ruteo clásico pueden comenzar a configurar el ruteo estático para forzar el tráfico de **vedge1** a **vedge4** dirección de interfaz pública a través de la interfaz de extensión de TLOC entre **vedge1** y **vedge3**, pero no dará el resultado deseado y puede crear confusión porque:

El tráfico del plano de administración (por ejemplo, ping, paquete de utilidad traceroute) sigue la ruta deseada.

Al mismo tiempo, los túneles del plano de datos SD-WAN (túneles de transporte IPsec o gre) ignoran la información de la tabla de ruteo y las conexiones de formulario basadas en **colores** TLOC**.**

Dado que una ruta estática no tiene inteligencia, si TLOC público-internet no funciona en vedge3 (enlace ascendente a ISP 2), entonces vedge1 no notará esto y la conectividad a **vedge4** falla a pesar del hecho de que **vedge1** todavía tiene disponible **biz-internet**.

Por consiguiente, este enfoque debe evitarse y no utilizarse.

Solución

1. Uso de la política de control centralizado para establecer una preferencia para TLOC **de Internet pública** en el controlador vSmart al anunciar las rutas OMP correspondientes a **vedge4.** Ayuda a archivar la trayectoria de tráfico deseada del **sitio 4** al **sitio 13**.

2. Para lograr el trayecto de tráfico deseado en dirección inversa desde el **sitio 13** al **sitio 4** no puede utilizar la política de control centralizado porque **vedge4** sólo tiene un TLOC disponible, por lo que no puede establecer una preferencia en nada, pero puede utilizar la política de ruta de aplicación para lograr este resultado para el tráfico de salida desde el **sitio 13**.

Así es como puede parecer la política de control centralizada en el controlador vSmart para preferir el TLOC **de Internet pública** para alcanzar el **sitio 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
 !
!
```

Y aquí hay un ejemplo de la política de ruta de la aplicación para preferir el enlace ascendente **público-internet** como punto de salida para el tráfico de salida del **sitio 13** al **sitio 4**:

```
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
 !
```

Las políticas deben aplicarse correctamente en el controlador vSmart:

```
apply-policy
 site-list S13
  app-route-policy S13_S4_via_PUB
 !
 site-list S4
  control-policy S4_S13_via_PUB out
 !
!
```

Recuerde también que las políticas de ruta de aplicación no se pueden configurar como una política localizada y deben aplicarse sólo en vSmart.

Verificación

Tenga en cuenta que la política de ruta de la aplicación no se aplicará al tráfico generado localmente por vEdge, por lo que se recomienda verificar si los flujos de tráfico se dirigen según la ruta deseada para generar parte del tráfico de los segmentos LAN de los sitios correspondientes. Como un caso de escenario de prueba de alto nivel, puede utilizar iperf para generar tráfico entre hosts en segmentos LAN del **sitio 13** y **el sitio 4** y luego verificar una estadística de interfaz. Por ejemplo, en mi caso, no hubo tráfico además del generado por el sistema y por lo tanto puede ver que la mayor cantidad de tráfico pasó a través de la interfaz ge0/3 hacia la extensión TLOC en

vedge3:

```
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
```

Troubleshoot

En primer lugar, asegúrese de que se establezcan las sesiones BFD correspondientes (no utilice la palabra clave **restrict** en ninguna parte):

```
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
```

Si no puede lograr el resultado deseado con la ingeniería de tráfico, compruebe que las políticas se hayan aplicado correctamente:

1. En **vedge4** debe verificar que para los prefijos originados en el **sitio 13** se seleccionó el TLOC apropiado:

```
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. En **vedge1** y **vedge3** asegúrese de que se instale la política adecuada de vSmart y de que los paquetes coincidan y se cuenten:

```
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
```

Además de que debería ver muchos más paquetes enviados a través del color **de Internet público** del **sitio 13** (durante mis pruebas no hubo tráfico a través de **biz-internet** TLOC):

```
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
```

Información Relacionada

- 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