Configurer plusieurs transports et l'ingénierie du trafic avec la politique de contrôle centralisée et la politique de routage des applications

Contenu

Introduction

Ce document décrit comment configurer la stratégie de contrôle centralisé et la stratégie de route d'application pour réaliser l'ingénierie de trafic entre les sites. Il pourrait également être considéré comme une ligne directrice de conception spécifique pour le cas d'utilisation particulier.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

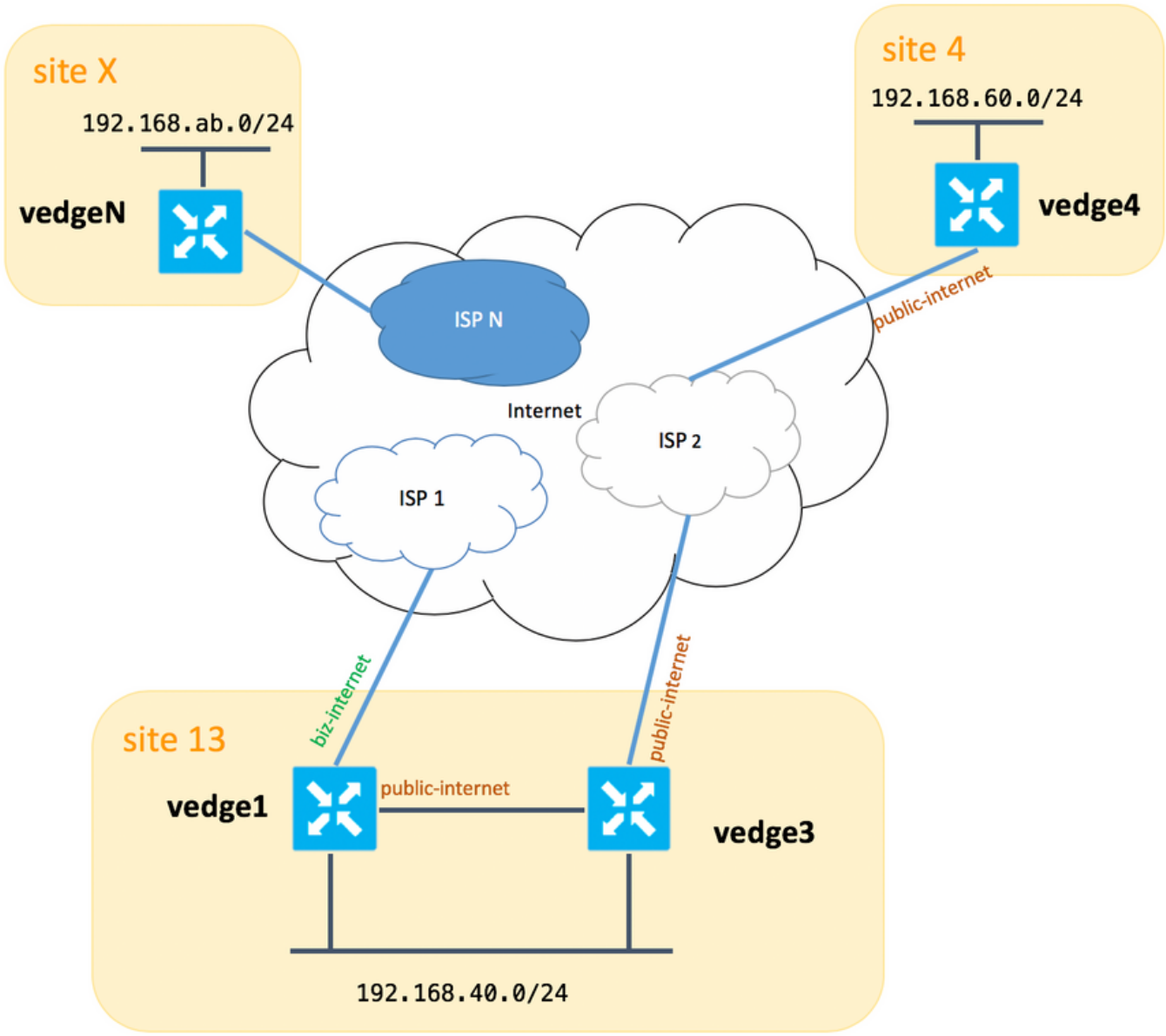
Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration

Pour une démonstration et une meilleure compréhension du problème décrit plus loin, examinez la topologie illustrée dans cette image.



Veuillez noter qu'en général entre **vedge1** et **vedge3** vous devriez avoir une deuxième liaison/sous-interface pour l'extension TLOC **biz-internet** également, mais ici par souci de simplicité, il n'a pas été configuré.

Voici les paramètres système correspondants pour vEdges/vSmart (vedge2 représente tous les autres sites) :

nom de l'hôte	id-site	system-ip
évitement1	13	192.168.30.4
veine3	13	192.168.30.6
vase4	4	192.168.30.7
véguin	X	192.168.30.5
vsmart1	1	192.168.30.3

Vous trouverez ici les configurations côté transport à titre de référence.

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
!
```

Problème

L'utilisateur souhaite atteindre ces objectifs :

Le service Internet fournit **ISP 2** devrait être préféré pour communiquer entre le **site 13** et **le site 4** pour certaines raisons. Par exemple, il s'agit d'un cas d'utilisation assez courant et d'un scénario où la qualité de connexion/connectivité au sein d'un FAI entre ses propres clients est très bonne, mais vers le reste de la qualité de connectivité Internet ne répond pas au SLA de l'entreprise en raison de certains problèmes ou de la congestion sur une liaison ascendante du FAI et donc ce FAI (**FAI 2** dans notre cas) doit être évité en général.

Le site 13 devrait préférer la liaison ascendante **Internet publique** pour se connecter au **site 4**, mais tout de même maintenir la redondance et devrait être en mesure d'atteindre **le site 4** si **Internet public** échoue.

Le **site 4** doit conserver une connectivité au mieux avec tous les autres sites directement (vous ne pouvez donc pas utiliser le mot clé **restriction** ici sur **vedge4** pour atteindre cet objectif).

Le **site 13** devrait utiliser le lien de meilleure qualité avec **biz-internet** coloris pour atteindre tous les autres sites (représenté par **le site X** sur le schéma de topologie).

Une autre raison pourrait être les problèmes de coût/prix lorsque le trafic au sein du FAI est gratuit, mais beaucoup plus cher lorsque le trafic sortant d'un réseau de fournisseur (système autonome).

Certains utilisateurs qui ne sont pas familiarisés avec l'approche SD-WAN et qui s'habituent au routage classique peuvent commencer à configurer le routage statique pour forcer le trafic de **vedge1** à **vedge4** adresse d'interface publique via l'interface d'extension TLOC entre **vedge1** et **vedge3**.

Le trafic du plan de gestion (par exemple, ping, paquet de l'utilitaire traceroute) suit la route souhaitée.

En même temps, les tunnels de plan de données SD-WAN (tunnels de transport IPsec ou gre) ignorent les informations de table de routage et les connexions de formulaire en fonction des **couleurs** TLOC**.**

Comme une route statique n'a aucune intelligence, si le TLOC d'Internet public est désactivé sur vedge3 (liaison ascendante vers ISP 2), vedge1 ne le remarquera pas et la connectivité à **vedge4** échoue malgré le fait que **vedge1** a encore **biz-internet** disponible.

Cette approche doit donc être évitée et inutilisable.

Solution

1. Utilisation d'une stratégie de contrôle centralisé pour définir une préférence pour TLOC **Internet public** sur le contrôleur vSmart lors de l'annonce des routes OMP correspondantes à **vedge4.** Il permet d'archiver le chemin de trafic souhaité du **site 4** au **site 13**.

2. Pour obtenir le chemin de trafic souhaité en sens inverse du **site 13** au **site 4**, vous ne pouvez pas utiliser la stratégie de contrôle centralisé car **vedge4** n'a qu'un seul TLOC disponible, vous ne pouvez donc pas définir de préférence pour quoi que ce soit, mais vous pouvez utiliser la stratégie de routage d'application pour obtenir ce résultat pour le trafic sortant du **site 13**.

Voici à quoi ressemble la politique de contrôle centralisé sur le contrôleur vSmart pour préférer le TLOC **Internet public** pour atteindre **le site 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
 !
!
```

Et voici un exemple de stratégie de routage d'application pour préférer la liaison ascendante

Internet publique comme point de sortie pour le trafic de sortie du **site 13** au **site 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
 !
```

Les stratégies doivent être appliquées de manière appropriée sur le contrôleur vSmart :

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

N'oubliez pas que les stratégies app-route ne peuvent pas être configurées en tant que stratégie localisée et doivent être appliquées uniquement sur vSmart.

Vérification

Notez que la stratégie de routage d'application ne sera pas appliquée au trafic généré localement par vEdge, donc pour vérifier si les flux de trafic sont dirigés selon le chemin souhaité, il est recommandé de générer du trafic à partir des segments LAN des sites correspondants. Comme scénario de test de haut niveau, vous pouvez utiliser iperf pour générer du trafic entre les hôtes dans les segments LAN des **sites 13** et **4**, puis vérifier les statistiques d'interface. Par exemple,

dans mon cas, il n'y a pas eu de trafic en dehors du système généré et donc vous pouvez voir que la majeure partie du trafic passe par l'interface ge0/3 vers l'extension TLOC sur **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
```

Dépannage

Tout d'abord, assurez-vous que les sessions BFD correspondantes sont établies (n'utilisez **restriction** nulle part) :

```
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 vous ne parvenez pas à atteindre le résultat souhaité avec l'ingénierie de trafic, vérifiez que les stratégies ont été correctement appliquées :

1. Sur **vedge4** vous devez vérifier que pour les préfixes provenant du **site 13** TLOC approprié a été sélectionné :

```
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. Sur **vedge1** et **vedge3** assurez-vous que la stratégie appropriée de vSmart est installée et que les paquets sont appariés et comptés :

```
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
```

En outre, vous devriez voir beaucoup plus de paquets envoyés via la couleur **internet public** du **site 13** (pendant mon test il n'y avait pas de trafic via **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
```

Informations connexes

- 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_Int

erfaces/06Configuring_Network_Interfaces
- https://sdwan-docs.cisco.com/Product_Documentation/Command_Reference/Configuration_Commands/color