Meervoudige transport- en traffic engineering configureren met gecentraliseerd beheerbeleid en beleid voor App

Inhoud

Inleiding

In dit document wordt beschreven hoe u gecentraliseerd controlebeleid en beleid van de app-route kunt configureren om verkeerstechniek tussen verschillende sites te bereiken. Het kan ook worden beschouwd als een specifieke ontwerprichtlijn voor het specifieke geval van gebruik.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

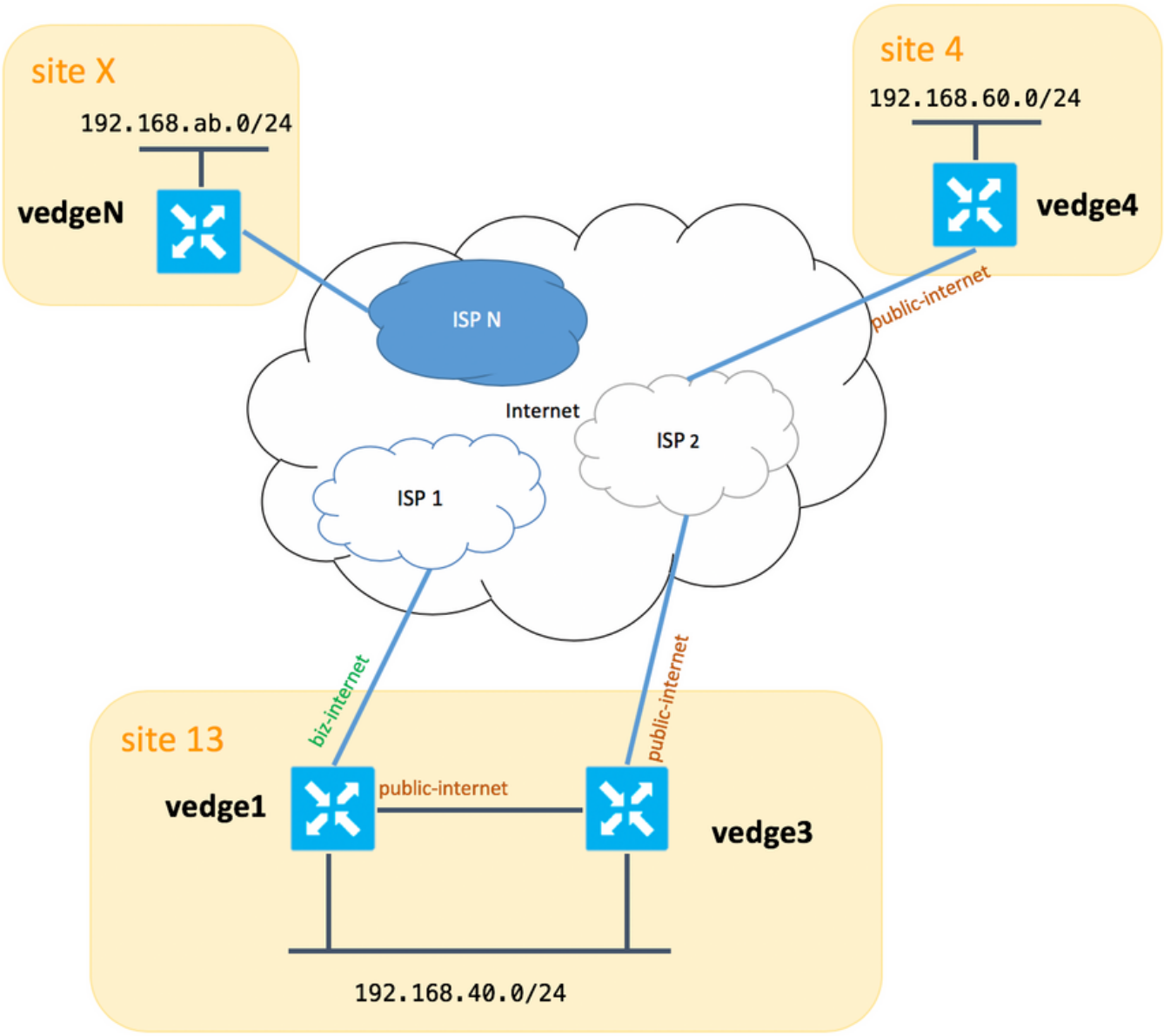
Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configuratie

Met het oog op demonstratie en een beter begrip van het later beschreven probleem, kunt u de topologie in deze afbeelding bekijken.



Houd er rekening mee dat u in het algemeen tussen **vEdge1** en **vEdge3** moet beschikken over een tweede link/subinterface voor de TLOC-extensie via **biz-internet**, maar dit was eenvoudigweg niet zo ingesteld.

Hier zijn corresponderende systeeminstellingen voor vEdge/vSmart (vEdge2 geeft alle andere sites weer):

hostname	steunpunt	systeemip
rand1	13	192.168.30.4
rand3	13	192.168.30.6
rand4	4	192.168.30.7
vedgex	X	192.168.30.5
vernuftig	1	192.168.30.3

Hier vindt u de vervoerszijconfiguraties ter referentie.

Afstand1:

```
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
!
```

Afstand3:

```
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
```

rand4:

```
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
!
```

Probleem

De gebruiker wil deze doelstellingen bereiken:

Internet service biedt **ISP 2** zou om bepaalde redenen de voorkeur moeten geven aan de communicatie tussen **site 13** en **site 4**. Bijvoorbeeld, het is nogal een gebruiks geval en een scenario wanneer de verbinding/connectiviteit kwaliteit binnen een ISP tussen zijn eigen cliënten zeer goed is, maar naar de rest van de internetconnectiviteit voldoet de kwaliteit van de connectiviteit niet aan SLA van het bedrijf door sommige problemen of congestie op een ISP uplink en daarom zou deze ISP (**ISP 2** in ons geval) in het algemeen moeten worden vermeden.

Site **site 13** zou bij voorkeur **publiek-internet**-uplink moeten gebruiken om verbinding te maken met site **site 4**, maar dan toch redundantie handhaven en **site 4** moeten kunnen bereiken indien **het openbare internet** mislukt.

Site **site 4** zou de best-inspanning connectiviteit met alle andere sites direct moeten onderhouden (dus u kunt sleutelwoord hier op **versie 4** niet **beperken** om dat doel te bereiken).

Site **site 13** zou gebruik moeten maken van de kwaliteitslink met **biz-internet** colorum om alle andere sites te bereiken (weergegeven door **site X** op het topologiediagram).

Een andere reden kan zijn kosten/prijskwesties wanneer het verkeer binnen ISP gratis is, maar veel duurder wanneer het verkeer een provider-netwerk verlaat (autonoom systeem).

Sommige gebruikers die niet ervaren zijn met SD-WAN benadering en die gebruikt worden voor de **klassieke** routing, kunnen beginnen statische routing te configureren om verkeer te forceren van **versie1** naar **versie4** openbare interfaceadres via TLOC-extensie interface tussen **edge1** en **vEdge3, maar het geeft niet het gewenste resultaat en kan verwarring creëren omdat:**

Het vliegtuigverkeer van het beheer (b.v. pingelen, Tracoute nutspakket) volgt de gewenste route.

Tegelijkertijd negeert SD-WAN dataloclips (IPsec of Gigabit transporttunnels) de routing van tabelinformatie en formulierverbindingen op basis van **kleuren** van TLOC**'s.**

Aangezien een statische route geen intelligentie heeft, als TLOC tussen **publiek en internet** op **vEdge3** is (verbinding met ISP 2), zal **vEdge1** dit niet opmerken en **v**4 niet **aangesloten** is **op vInternet1.**

Daarom moet deze benadering worden vermeden en niet bruikbaar zijn.

Oplossing

1. Gebruik van een gecentraliseerd controlebeleid om een voorkeur voor TLOC op **publiek-internet** op de vSmart-controller vast te stellen bij het aankondigen van corresponderende OMP-routes naar **Vedge4.** Hierdoor wordt het gewenste verkeerspad van **site 4** naar **site 13** gearchiveerd.

2. Om het gewenste verkeerspad in omgekeerde richting van **site 13** naar **site 4** te bereiken kunt u geen gecentraliseerd controlebeleid gebruiken omdat **v4** slechts één TLOC beschikbaar heeft. U kunt dus geen voorkeur aan iets geven, maar u kunt een app route-beleid gebruiken om dit resultaat te bereiken voor nieuwsverkeer vanaf **site 13**.

Zo kan een gecentraliseerd controlebeleid er op vSmart-controller uitzien als u liever TLOC **op publiek-internet** gebruikt om **site 13** te bereiken:

```
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
 !
!
```

En hier is een voorbeeld van het app-routebeleid om de voorkeur te geven aan openbare **internet**-uplink als exitpunt voor drukverkeer van **site 13** naar **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
 !
```

Het beleid moet correct worden toegepast op vSmart-controller:

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

Denk er ook aan dat app-route beleid niet kan worden geconfigureerd als lokaal beleid en alleen op vSmart moet worden toegepast.

Verifiëren

Let op dat het app-routebeleid niet wordt toegepast op lokaal gegenereerd vEdge-verkeer, dus om te controleren of de verkeersstromen volgens het gewenste pad worden verzonden. Het is aanbevolen om wat verkeer te genereren uit LAN-segmenten van corresponderende sites. Als een testscenario op hoog niveau kunt u iperf gebruiken om verkeer tussen hosts in LAN segmenten van **site 13** en **site 4** te genereren en vervolgens een interfacestatistiek te controleren. Bijvoorbeeld, in mijn geval was er geen verkeer behalve het gegenereerde systeem. Daarom zie je dat grote hoeveelheid verkeer door de ge0/3 interface naar de TLOC-extensie op **v3** liep:

```
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
```

Problemen oplossen

Zorg eerst en vooral dat de overeenkomende BFD-sessies worden ingericht (gebruik geen sleutelwoord ergens **beperken**):

```
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
```

Als u met traffic engineering het gewenste resultaat niet kunt bereiken, moet u vervolgens controleren of het beleid correct wordt toegepast:

1. Op **vEdge4** dient u te controleren of voor prefixes afkomstig zijn van **site 13** geschikte TLOC is geselecteerd:

```
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. Zorg er bij vSmart opv1 en vEdge3 voor dat het juiste beleid van vSmart wordt geïnstalleerd en dat pakketten worden afgestemd en geteld:

```
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
```

Afgezien van het feit dat je veel meer pakketten ziet die vanaf **site 13** via **het openbare internet** worden verzonden (tijdens mijn testen was er geen verkeer 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
```

Gerelateerde informatie

- 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/col

or