Konfiguration mehrerer Transporte und Traffic Engineering mit zentralisierten Kontrollrichtlinien und Anwendungsrouten

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine zentrale Kontrollrichtlinie und eine App-Routing-Richtlinie konfiguriert werden, um Traffic Engineering zwischen Standorten zu ermöglichen. Sie kann auch als spezifische Designrichtlinie für den jeweiligen Anwendungsfall angesehen werden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

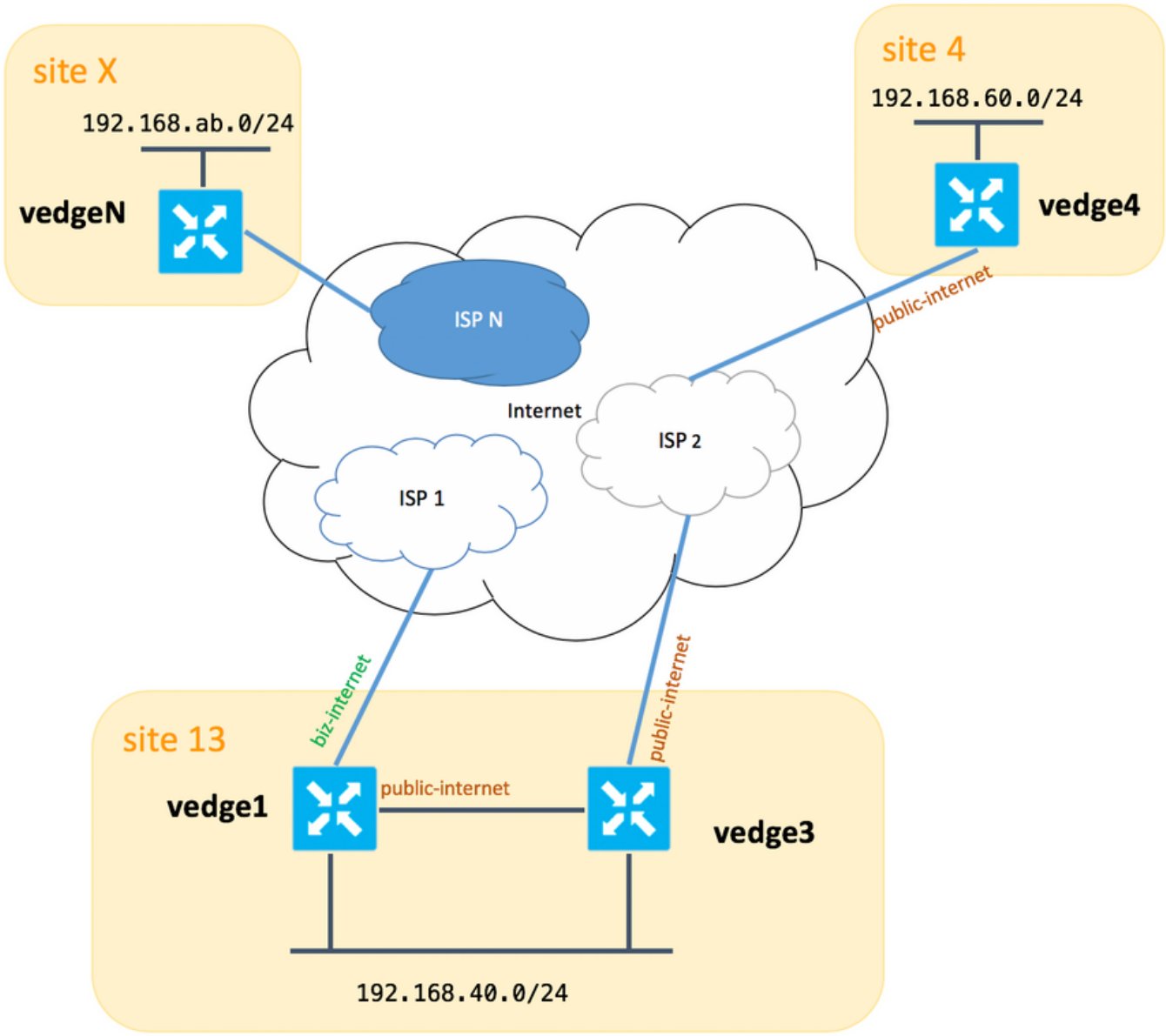
Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfiguration

Zur Veranschaulichung und zum besseren Verständnis des weiter unten beschriebenen Problems sollten Sie die in diesem Bild dargestellte Topologie berücksichtigen.



Bitte beachten Sie, dass Sie im Allgemeinen zwischen **vedge1** und **vedge3** eine zweite Verbindung/Subschnittstelle auch für **biz-internet** TLOC-Erweiterung haben sollten, aber aus Gründen der Einfachheit wurde diese nicht konfiguriert.

Nachfolgend sind die entsprechenden Systemeinstellungen für vEdges/vSmart aufgeführt (vedge2 repräsentiert alle anderen Standorte):

Hostname	Standort-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

Hier finden Sie Transportseitenkonfigurationen als Referenz.

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
!
```

Problem

Der Benutzer möchte folgende Ziele erreichen:

Internet-Service-Provider **ISP 2** sollten aus bestimmten Gründen der Kommunikation zwischen **Standort 13** und **Standort 4** vorgezogen werden. So ist es z. B. ein gängiges Anwendungsbeispiel und ein Szenario, in dem die Verbindungs-/Verbindungsqualität innerhalb eines ISP zwischen den eigenen Clients sehr gut ist, aber in Bezug auf die restliche Internetkonnektivitätsqualität das SLA des Unternehmens wegen einiger Probleme oder Überlastungen an einem ISP-Uplink nicht erfüllt. Daher sollte dieser ISP (in unserem Fall **ISP 2**) im Allgemeinen vermieden werden.

Die Site **13** sollte einen **Public-Internet-**Uplink bevorzugen, um eine Verbindung mit der **Website 4 herzustellen**, jedoch gleichzeitig Redundanz beibehalten und bei Ausfall des **öffentlichen Internets** die **Website 4 erreichen können.**

Site **Site 4** sollte weiterhin die bestmögliche Verbindung mit allen anderen Sites direkt aufrechterhalten (daher können Sie hier auf **vedge4** kein Schlüsselwort **einschränken**, um dieses Ziel zu erreichen).

Site **13** sollte die bessere Verknüpfung mit **biz-internet** verwenden, um alle anderen Standorte zu erreichen (dargestellt durch **Site X** im Topologiediagramm).

Ein weiterer Grund können Kosten-/Preisprobleme sein, wenn der Datenverkehr innerhalb eines ISP kostenlos ist, aber viel teurer, wenn der Datenverkehr aus einem Anbieternetzwerk (autonomes System) ausläuft.

Einige Benutzer, die mit dem SD-WAN-Ansatz nicht vertraut sind und sich an das **klassische** Routing gewöhnt haben, konfigurieren möglicherweise statisches Routing, um Datenverkehr von **vedge1** zu **vedge4** über die TLOC-Erweiterungs-Schnittstelle zwischen **vedge1 und vedge3** zu zwingen, das gewünschte Ergebnis jedoch nicht und kann Verwirrung verursachen, da:

Datenverkehr auf Verwaltungsebene (z. B. Ping, Traceroute-Dienstpaket) folgt der gewünschten Route.

Gleichzeitig ignorieren SD-WAN-Datenebenen-Tunnel (IPsec- oder Gre-Transport-Tunnel) Routing-Tabellen-Informationen und bilden Verbindungen, die auf TLOCs-**Farben** basieren.

Da eine statische Route über keine Intelligenz verfügt, wird **vedge3** (Uplink zu ISP 2) bei **Public-Internet-**TLOC **vedge1** dies nicht bemerken, und die Verbindung zu **vedge4** scheitert, obwohl **vedge1 noch über Biz-Internet verfügt.**

Daher sollte dieser Ansatz vermieden und nicht genutzt werden.

Lösung

1. Verwendung einer zentralisierten Kontrollrichtlinie, um eine Präferenz für **Public-Internet-**TLOC auf dem vSmart-Controller festzulegen, wenn entsprechende OMP-Routen zu **vedge4** angekündigt werden. Es hilft, den gewünschten Datenverkehrspfad von **Standort 4** bis **Standort 13** zu archivieren.

2. Um den gewünschten Datenverkehrspfad in umgekehrter Richtung von **Standort 13** zu **Standort 4** zu erreichen, können Sie keine zentrale Kontrollrichtlinie verwenden, da **vedge4** nur einen TLOC zur Verfügung hat. Daher können Sie keine Präferenz für irgendetwas festlegen, aber eine App-Route-Richtlinie verwenden, um dieses Ergebnis für Ausgangs-Datenverkehr von **Standort 13** zu erreichen.

So könnte eine zentrale Kontrollrichtlinie für den vSmart Controller aussehen, wenn der **Public-Internet-**TLOC **Standort 13** erreicht:

```
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
 !
!
```

Hier sehen Sie ein Beispiel für eine App-Routing-Richtlinie, die einen **Public-Internet-**Uplink als Ausgangspunkt für den ausgehenden Datenverkehr von **Standort 13** zu **Standort 4** vorzieht:

```
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
 !
```

Richtlinien sollten auf dem vSmart Controller angemessen angewendet werden:

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

Beachten Sie auch, dass App-Route-Richtlinien nicht als lokalisierte Richtlinie konfiguriert werden können und nur auf vSmart angewendet werden sollten.

Überprüfen

Beachten Sie, dass die App-Routing-Richtlinie nicht auf lokal generierten vEdge-Datenverkehr angewendet wird. Daher wird empfohlen, einen Teil des Datenverkehrs von LAN-Segmenten der entsprechenden Standorte zu generieren, um zu überprüfen, ob der Datenverkehr entsprechend dem gewünschten Pfad geleitet wird. Als High-Level-Testszenario können Sie iperf verwenden,

um Datenverkehr zwischen Hosts in LAN-Segmenten von **Standort 13** und **Standort 4** zu generieren und anschließend eine Schnittstellenstatistik zu überprüfen. In meinem Fall gab es beispielsweise keinen Datenverkehr, der über das generierte System hinausging. Daher können Sie sehen, dass ein Großteil des Datenverkehrs über die GE0/3-Schnittstelle an die TLOC-Erweiterung auf **vedge3** weitergeleitet wurde:

```
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
```

Fehlerbehebung

Stellen Sie zunächst sicher, dass entsprechende BFD-Sitzungen eingerichtet werden (verwenden Sie kein Schlüsselwort überall):

```
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
```

Wenn Sie mit Traffic Engineering das gewünschte Ergebnis nicht erzielen können, überprüfen Sie, ob die Richtlinien korrekt angewendet wurden:

1. Auf **vedge4** sollten Sie überprüfen, ob für Präfixe, die vom **Standort 13** stammen, der entsprechende TLOC ausgewählt wurde:

```
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. Auf **vedge1** und **vedge3** stellen Sie sicher, dass die entsprechenden Richtlinien von vSmart installiert und Pakete abgeglichen und gezählt werden:

```
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
```

Außerdem sollten Sie viel mehr Pakete sehen, die von **Seite 13** aus über **das öffentliche Internet** gesendet wurden (während meiner Tests gab es keinen Datenverkehr über **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
```

Zugehörige Informationen

- https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.3/07Policy_Applicati

ons/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