集中制御ポリシーとアプリケーションルートポリシーによる複数のトランスポートおよびトラフィックエンジニアリングの設定

内容

概要

このドキュメントでは、サイト間のトラフィックエンジニアリングを実現するために、集中制御ポリシーとアプリケーションルートポリシーを設定する方法について説明します。特定のユースケースに対する特定の設計ガイドラインとしても考慮できます。

前提条件

要件

このドキュメントに特有の要件はありません。

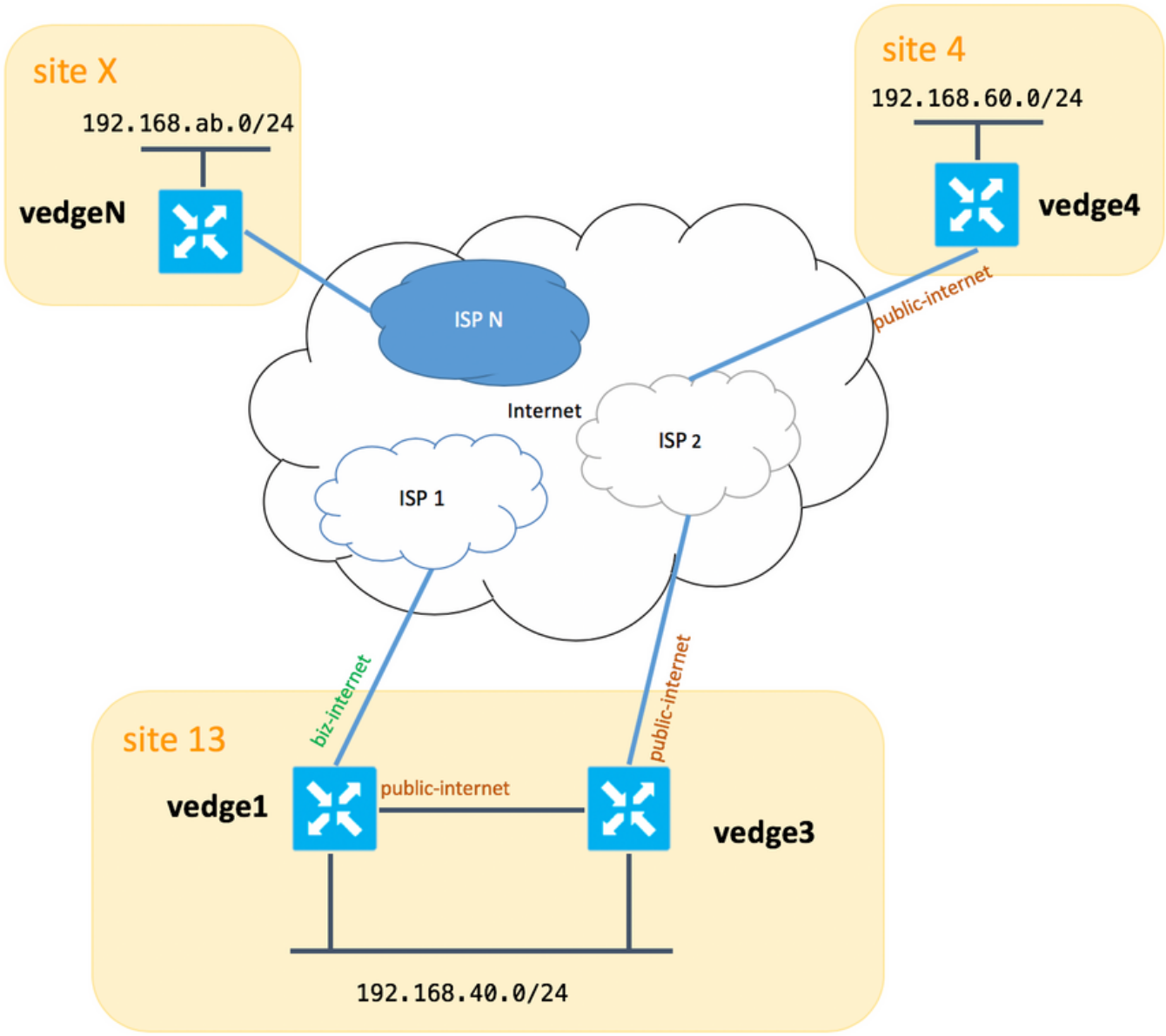
使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

コンフィギュレーション

デモンストレーションの目的と、後述する問題の理解を深めるために、次の図に示すトポロジを検討してください。



一般的にvedge1と**vedge3**の間には、**biz-internet** TLOC拡張に**も2つ目のリンク/サブインターフェイスが必要です**。しかし、ここでは簡単に設定されていません。

vEdges/vSmartの対応するシステム設定を次に示します（vedge2は他のすべてのサイトを表します）。

ホスト名	site-id	system-ip
vedge1	13	192.168.30.4
vedge3	13	192.168.30.6
vedge4	4	192.168.30.7
エジックス	X	192.168.30.5
vsmart1	1	192.168.30.3

ここでは、トランスポート側の設定を参照できます。

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
!
```

問題

ユーザは次の目標を達成したいと考えています。

インターネットサービス提供ISP 2は、いくつかの理由からサイト13とサイト4の間の通信に優先する必要があります。例えば、ISP内の接続/接続品質が非常に良好な場合の一般的な使用例とシナリオです。ただし、ISPのアップリンクに問題や輻輳が発生するため、残りのインターネット接続品質は会社のSLAを満たしません。そのため、一般ににISP 2はは回避です。

サイト13は、サイト4に接続する場合は、パブリックインターネットアップリンクを選択する必要があります。ただし、冗長性を維持し、パブリックインターネットに障害が発生した場合はサイト4にアクセスできる必要があります。

サイトサイト4は、他のすべてのサイトとのベストエフォート接続を直接維持する必要があります(したがって、vedge4でrestrictキーワードを使用してこの目標を達成することはできません)。

サイトサイト13は、他のすべてのサイトに到達するために、ビズズ – インターネットカラーと高品質のリンクを使用する必要があります(トポロジ図でサイトX)。

別の理由として、ISP内のトラフィックが無料の場合はコスト/価格の問題が考えられますが、プロバイダーネットワーク（自律システム）を通過する場合はコストが高くなる可能性があります。

SD-WANアプローチに慣れていない一部のユーザは、vedge1とvedge3の間のTLOC拡張インターフェイスを介してvedge1からvedge4パブリックインターフェイスアドレスへのトラフィックを強制的に設定し始ます。

管理プレーントラフィック（ping、tracerouteユーティリティパケットなど）は、目的のルートに従います。

同時に、SD-WANデータプレーントンネル（IPsecまたはgreトランスポートトンネル）はルーティングテーブル情報を無視し、TLOCの色に基づいて接続を形成します。

スタティックルートにはインテリジェンスがないため、パブリックインターネットTLOCがvedge3（ISP 2へのアップリンク）でダウンしている場合、vedge1 が勝利し、vedge4への接続はvedge1 がまだbiz-internetで失敗します。

したがって、このアプローチは避け、使用することはできません。

解決方法

1.集中制御ポリシーを使用して、対応するOMPルートをvedge4にアナウンスする際に、vSmartコントローラ上でパブリックインターネットTLOCのプリファレンスを設定します。サイト4からサイト13。

2. site 13からsite 4までの逆方向で目的のトラフィックパスを実現するには、vedge4には1つのTLOCしか使用できないため、中央制御ポリシーを使用できません。そのため、任意の設定を行うことができます。

次に、中央集中型の制御ポリシーがvSmartコントローラでサイト13に到達するためにパブリックインターネットTLOCを好むように見えることを示します。

```
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
 !
!
```

次に、サイト13からサイト4への出力トラフィックの出口ポイントとしてパブリックインターネットアップリンクを優先するアプリルートポリシーの例を示します。

```
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
 !
```

ポリシーは、vSmartコントローラに適切に適用する必要があります。

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

app-routeポリシーはローカライズされたポリシーとして設定できず、vSmartのみに適用する必要があることに注意してください。

確認

アプリケーションルートポリシーはvEdgeローカルで生成されたトラフィックには適用されないため、トラフィックフローが目的のパスに従って制御されているかどうかを確認するには、対応するサイトのLANセグメントからトラフィックを生成することをお勧めします。高レベルのテストシナリオの場合は、iperfを使用してサイト**13とサイト4のLANセグメントのホスト間のトラフィックを生成し**て、インター**フェイスの統計情報を確認**できます。たとえば、私の場合は、システムが生成した以外にトラフィックが存在しなかったため、**vedge3のTLOC拡張に向けてge0/3インターフェイスを通過した大量のトラフィックが表示されます**。

```
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
```

トラブルシュート

まず、対応するBFDセッションが確立されていることを確認します(**restrictキーワードを任意の場所で使用しないでください**)。

```
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
```

トラフィックエンジニアリングで望ましい結果を得られない場合は、ポリシーが正しく適用されていることを確認します。

1. vedge4で、**サイト13から発**生したプレフィックスに対して適切なTLOCが**選択されている**ことを確認します。

```
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.vedge1とvedge3で、vSmartから適切なポリシーがインストールされ、パケットが一致してカウントされていることを確認します。

```
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
```

さらに、サイト13からパブリックインターネットカラーで送信されるパケットが多く表示される必要があります(テスト中に、biz-internet TLOCを介してトラフィックが送信されなかった)。

```
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
```

関連情報

- 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