중앙 집중식 제어 정책 및 앱 경로 정책으로 다중 전송 및 트래픽 엔지니어링 구성

목차

소개

이 문서에서는 사이트 간 트래픽 엔지니어링을 위해 중앙 집중식 제어 정책 및 앱 경로 정책을 구성하는 방법에 대해 설명합니다.특정 활용 사례에 대한 특정 설계 지침으로 간주할 수도 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

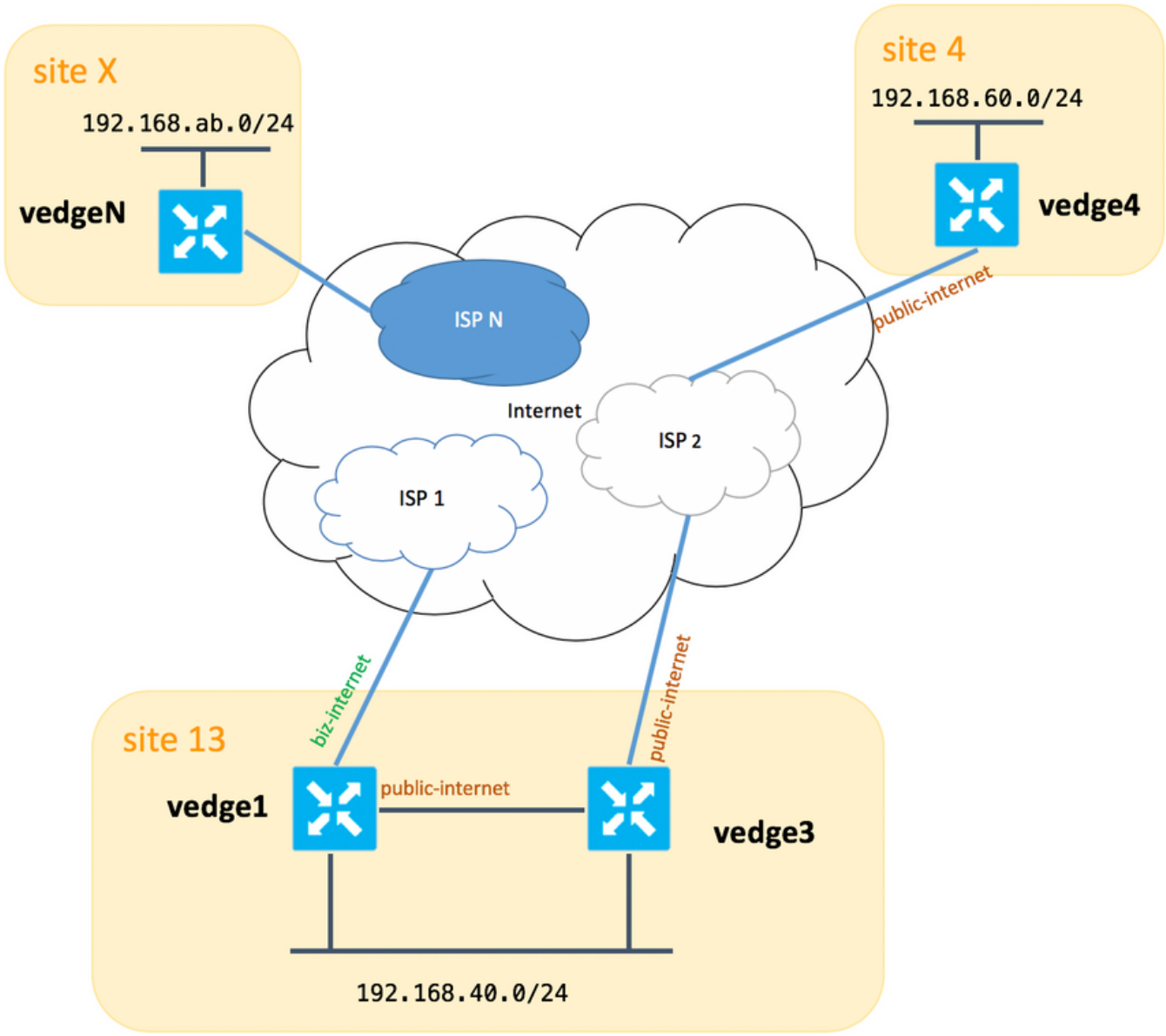
사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

데모를 위해 그리고 나중에 설명한 문제를 더 잘 이해하려면 이 이미지에 표시된 토폴로지를 고려해 주십시오.



일반적으로 vedge1과 vedge3 사이에 **비즈니스 인터넷 TLOC** 확장을 위한 두 번째 링크/하위 인터페이스가 있어야 하지만 간소화를 위해 구성되지 않았습니다.

vEdge/vSmart(vedge2는 다른 모든 사이트를 나타냅니다)에 해당하는 시스템 설정은 다음과 같습니다.

호스트 이름	사이트 ID	시스템 IP
vedge1	13	192.168.30.4
vedge3	13	192.168.30.6
vedge4	4	192.168.30.7
베게엑스	X	192.168.30.5
vsmart1	1	192.168.30.3

여기에서 참조할 전송 측 컨피그레이션을 찾을 수 있습니다.

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
!
```

문제

사용자는 다음과 같은 목표를 달성하고자 합니다.

인터넷 서비스는 **사이트 13**과 **사이트 4** 간 통신을 선호해야 합니다.예를 들어, ISP에서 자체적인 클라이언트 간에 연결/연결 품질이 매우 좋은 경우 일반적인 활용 사례이며, 나머지 인터넷 연결 품질로 인해 ISP 업링크에서 문제가 발생하거나 혼잡 때문에 회사의 SLA를 충족하지 않는 경우 이 ISP(**ISP 2**)는 일반적으로 피해야 합니다.

사이트 **사이트 13**은 **공용 인터넷** 업링크를 통해 사이트 **4**에 연결하는 것을 선호하지만 여전히 이중화를 유지하며 **공용 인터넷**이 **실패할** 경우 **사이트 4에 연결할 수 있어야 합니다.**

사이트 **4**는 다른 모든 사이트와의 최선형 연결을 직접 유지해야 합니다. 따라서 **vedge4**에서 여기서 **restrict** 키워드를 사용하여 이러한 목표를 달성할 수 없습니다.

사이트 **13**은 **비즈니스 인터넷** 색과 함께 더 우수한 품질의 링크를 사용하여 다른 모든 사이트(토폴로지 다이어그램의 **사이트** X로 표시됨)에 연결해야 합니다.

또 다른 이유는 ISP 내 트래픽이 무료로 제공되지만, 사업자 네트워크(자율 시스템)에서 트래픽이 나가는 경우 비용이 훨씬 더 많이 드는 경우 비용/가격 문제가 발생할 수 있습니다.

SD-WAN 접근 방식에 익숙하지 않고 **기존** 라우팅에 익숙지 않은 일부 사용자는 vedge**1**과 vedge**3**

사이의 TLOC 확장 인터페이스를 통해 vedge1에서 **vedge4** 공용 인터페이스 주소로 트래픽을 강제 처리하도록 정적 라우팅을 구성할 수 있지만, 원하는 결과를 주지 **않고 혼동을 일으킬 수 있습니다.**

관리 플레인 트래픽(예: ping, traceroute 유틸리티 패킷)은 원하는 경로를 따릅니다.

동시에 SD-WAN 데이터 플레인 터널(IPsec 또는 gre 전송 터널)은 TLOCs **색상**을 기반으로 라우팅 테이블 정보 및 양식 연결을 무시합니다.

고정 경로에는 인텔리전스가 없으므로 **공용 인터넷 TLOC가 vedge3**(ISP 2**에** 업링크)에서 다운된 경우 vedge**1은** vedge**1에서 여전히 Biz-Internet을 사용할 수** 있는 상태에도 불구하고 **vedge4**에 대한 연결**이 실패했음을** 인식하지 못합니다.

따라서 이러한 접근 방식을 사용하지 않고 사용해야 합니다.

솔루션

1. vEdge4에 해당하는 OMP 경로를 발표할 때 vSmart 컨트롤러에서 **공용 인터넷 TLOC**에 대한 기본 설정을 설정하려면 중앙 집중식 제어 정책을 사용합니다. 이 정책을 사용하면 **사이트 4**에서 **사이트 13**로 원하는 트래픽 경로를 아카이브할 수 있습니다.

2. **사이트 13**에서 **사이트 4로** 원하는 트래픽 경로를 역방향으로 달성하기 위해 vedge**4는 TLOC가 하나만 사용 가능하므로 중앙 집중식 제어 정책을 사용할 수 없습니다. 따라서 어떤 TLOC로 기본 설정을 지정할 수는 없지만 사이트 13에서 이그레스 트래픽에 대해 이 결과를 얻기 위해 앱 경로 정책을 사용할 수 있습니다.**

다음은 vSmart 컨트롤러에서 중앙 집중식 제어 정책이 **사이트 13**에 연결하기 위해 **공용 인터넷** TLOC를 선호하는 방식입니다.

```
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
 !
!
```

다음은 **사이트 13**에서 **사이트 4**로 이그레스(egress) 트래픽의 출구 지점으로 **공용 인터넷** 업링크를 선호하는 앱 경로 정책의 예입니다.

```
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
 !
```

vSmart 컨트롤러에서 정책을 적절하게 적용해야 합니다.

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

앱 경로 정책은 현지화된 정책으로 구성할 수 없으며 vSmart에만 적용해야 합니다.

다음을 확인합니다.

앱 경로 정책은 vEdge에서 로컬로 생성된 트래픽에 적용되지 않으므로, 트래픽 흐름이 해당 사이트의 LAN 세그먼트에서 일부 트래픽을 생성하는 것이 권장되는 경로에 따라 조정되었는지 확인하십시오.고급 테스트 시나리오 사례로서 iperf를 사용하여 **사이트 13**과 **사이트 4**의 LAN 세그먼트의 호스트 간 트래픽을 생성한 다음 인터페이스 통계를 확인할 수 있습니다.예를 들어, 시스템 생성 외에 트래픽이 없으므로 vedge**3**의 TLOC 확장을 위해 ge0/3 인터페이스를 통과하는 주요 트래픽 양이 **표시됩니다**.

```
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
```

문제 해결

먼저 해당 BFD 세션이 설정되었는지 확인합니다(어디에서도 **restrict** 키워드를 사용하지 않음).

```
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
```

트래픽 엔지니어링으로 원하는 결과를 달성할 수 없는 경우 정책이 올바르게 적용되었는지 확인합니다.

1. vedge**4에서 사이트 13**에서 생성된 접두사에 대해 적절한 TLOC를 선택했는지 확인해야 합니다.

```
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 및 vedge3에서 vSmart의 적절한 정책이 설치되고 패킷이 일치하고 계산되었는지 확인합니다.

```
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
```

또한 사이트 13에서 공용 인터넷 색상을 통해 전송되는 훨씬 더 많은 패킷을 볼 수 있어야 합니다(테스트 중에 biz-internet TLOC를 통한 트래픽이 없음).

```
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
```

관련 정보

- 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