Configurar vários transportes e engenharia de tráfego com política de controle centralizada e política de rota de aplicativo

Contents

Introduction

Este documento descreve como configurar a política de controle centralizado e a política de rota de aplicativo para obter a engenharia de tráfego entre sites. Ele pode ser considerado uma diretriz de projeto específica para o caso de uso específico também.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

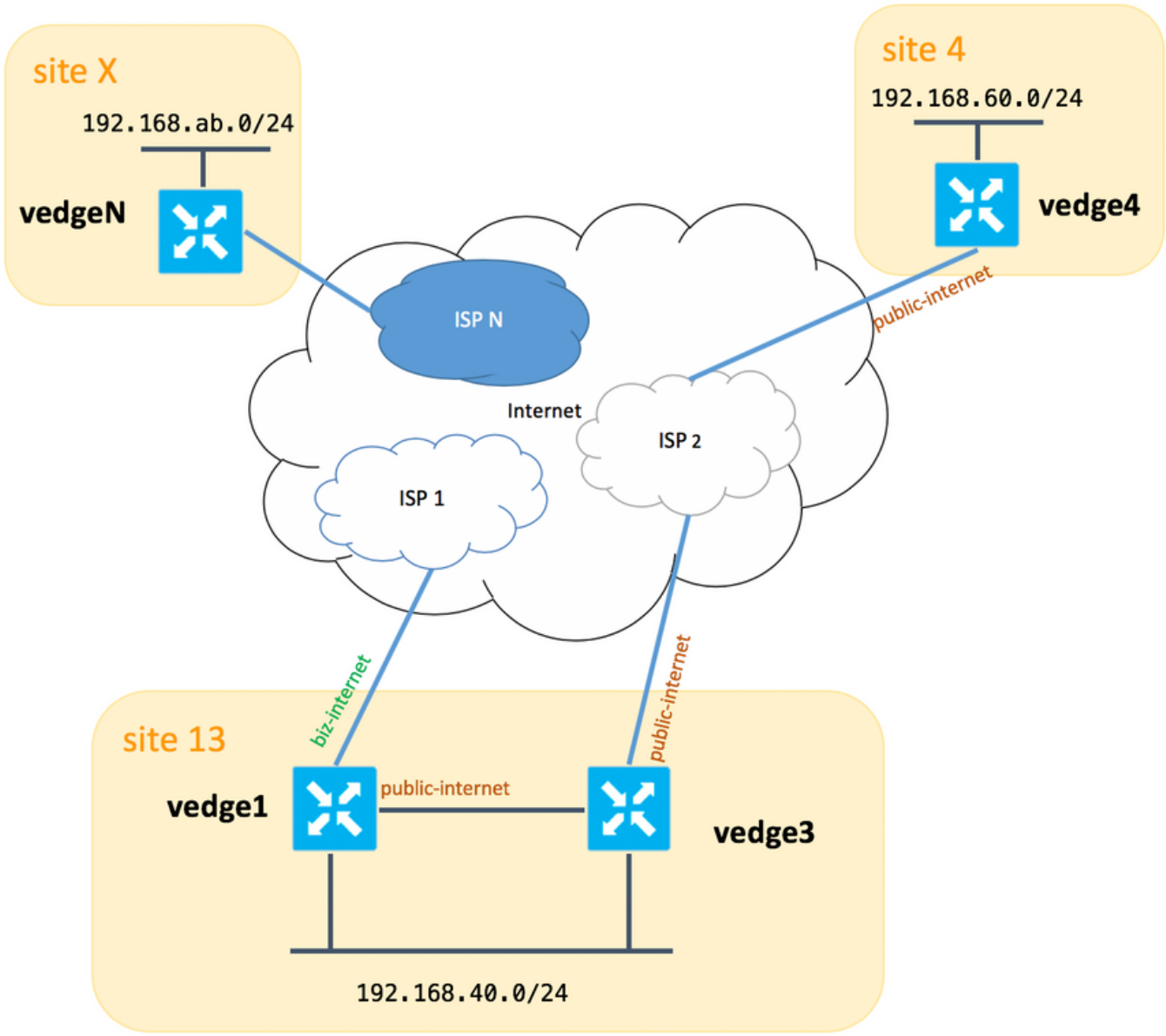
Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuração

Para fins de demonstração e melhor entendimento do problema descrito posteriormente, considere a topologia mostrada nesta imagem.



Observe que, em geral, entre o **vedge1** e o **vedge3** você deve ter a segunda conexão/subinterface para a extensão **Biz-Internet** TLOC também, mas aqui, por uma questão de simplicidade, ela não foi configurada.

Aqui estão as configurações de sistema correspondentes para vEdges/vSmart (vedge2 representa todos os outros sites):

hostname	ID do site	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

Aqui você pode encontrar as configurações do lado do transporte para referência.

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
!
```

Problema

O usuário deseja atingir essas metas:

O serviço de Internet fornece ao **ISP 2** deve ser preferido comunicar entre o **site 13** e o **site 4** por alguns motivos. Por exemplo, é um caso de uso bastante comum e um cenário em que a qualidade de conexão/conectividade em um ISP entre seus próprios clientes é muito boa, mas em relação ao restante da qualidade da conectividade com a Internet não atende ao SLA da empresa devido a alguns problemas ou congestionamento em um uplink do ISP e, portanto, esse ISP (**ISP 2** no nosso caso) deve ser evitado em geral.

O site 13 deve preferir o uplink **público-internet** para conectar-se ao site **4**, mas ainda assim manter a redundância e deve conseguir acessar o **site 4** se a **internet pública** falhar.

O **site 4** ainda deve manter a conectividade de melhor esforço com todos os outros sites diretamente (portanto, você não pode usar a palavra-chave **restrita** aqui no **vedge4** para atingir esse objetivo).

O **site** do site **13** deve usar o link de melhor qualidade com cores **da internet** para acessar todos os outros sites (representado pelo **site X** no diagrama de topologia).

Outra razão pode ser problemas de custo/preço quando o tráfego dentro do ISP é gratuito, mas muito mais caro quando o tráfego sai de uma rede de provedor (sistema autônomo).

Alguns usuários que não têm experiência com a abordagem SD-WAN e se acostumam com o roteamento clássico podem começar a configurar o roteamento estático para forçar o tráfego do **vedge1** ao **vedge4** interface pública via interface TLOC-extension entre **vedge1** e **vedge3**, mas não obtêm o resultado desejado e podem gerar confusão porque:

O tráfego do plano de gerenciamento (por exemplo, ping, pacote utilitário traceroute) segue a rota desejada.

Ao mesmo tempo, os túneis de plano de dados SD-WAN (IPsec ou túneis de transporte gre) ignoram as informações da tabela de roteamento e formam conexões com base nas **cores** de TLOCs**.**

Como uma rota estática não tem inteligência, se a TLOC público-Internet estiver inoperante no vedge3 (uplink para ISP 2), então o vedge1 não perceberá isso e a conectividade com o **vedge4** falha apesar do **vedge1** ainda ter **biz-internet** disponível.

Por conseguinte, esta abordagem deve ser evitada e não utilizável.

Solução

1. Uso de política de controle centralizado para definir uma preferência para a TLOC **público-Internet** no controlador vSmart ao anunciar rotas OMP correspondentes para **vedge4.** Ele ajuda a arquivar o caminho de tráfego desejado do **site 4** para o **site 13**.

2. Para alcançar o caminho de tráfego desejado no sentido inverso do **site 13** para o **site 4**, você não pode usar a política de controle centralizada porque o **vedge4** tem apenas uma TLOC disponível, portanto, você não pode definir uma preferência para nada, mas pode usar a política de rota de aplicativo para alcançar esse resultado para o tráfego de saída do **site 13**.

Veja como a política de controle centralizado pode ser no controlador vSmart para preferir a TLOC **público-Internet** para acessar o **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
 !
!
```

E aqui está um exemplo de política de rota de aplicativos para preferir o **uplink público-internet** como um ponto de saída para o tráfego de saída do **site 13** para o **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
 !
```

As políticas devem ser aplicadas adequadamente no controlador vSmart:

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

Lembre-se também de que as políticas de rota de aplicativo não podem ser configuradas como uma política localizada e devem ser aplicadas somente no vSmart.

Verificar

Observe que a política de rota do aplicativo não será aplicada ao tráfego gerado localmente pelo vEdge, portanto, para verificar se os fluxos de tráfego são direcionados de acordo com o caminho desejado, é recomendável gerar algum tráfego de segmentos de LAN de sites correspondentes. Como um cenário de teste de alto nível, você pode usar o iperf para gerar tráfego entre hosts em segmentos de LAN do **site 13** e do **site 4** e, em seguida, verificar as estatísticas de uma interface. Por exemplo, no meu caso, não havia tráfego além do sistema gerado e, portanto, você pode ver que a maior quantidade de tráfego passou pela interface ge0/3 em direção à extensão TLOC no

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
```

Troubleshoot

Em primeiro lugar, assegure-se de que as sessões BFD correspondentes sejam estabelecidas (não use **restringir** palavra-chave em qualquer lugar):

```
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
```

Se você não conseguir alcançar o resultado desejado com a engenharia de tráfego, verifique se as políticas foram aplicadas corretamente:

1. No **vedge4** você deve verificar se para prefixos originados do **site 13** foi selecionada a TLOC apropriada:

```
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. No vedge1 e vedge3 garantem que a política apropriada do vSmart seja instalada e que os pacotes sejam correspondidos e contados:

```
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
```

Além disso, você deve ver muito mais pacotes enviados através da cor **da internet pública** do **site 13** (durante meu teste não houve tráfego via **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
```

Informações Relacionadas

- 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