Configurazione di più trasporti e progettazione del traffico con criteri di controllo centralizzati e criteri di route delle applicazioni

Sommario

Introduzione

In questo documento viene descritto come configurare i criteri di controllo centralizzato e i criteri route dell'app per ottenere la progettazione del traffico tra i siti. Può anche essere considerata una specifica linea guida di progettazione per un particolare caso di utilizzo.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

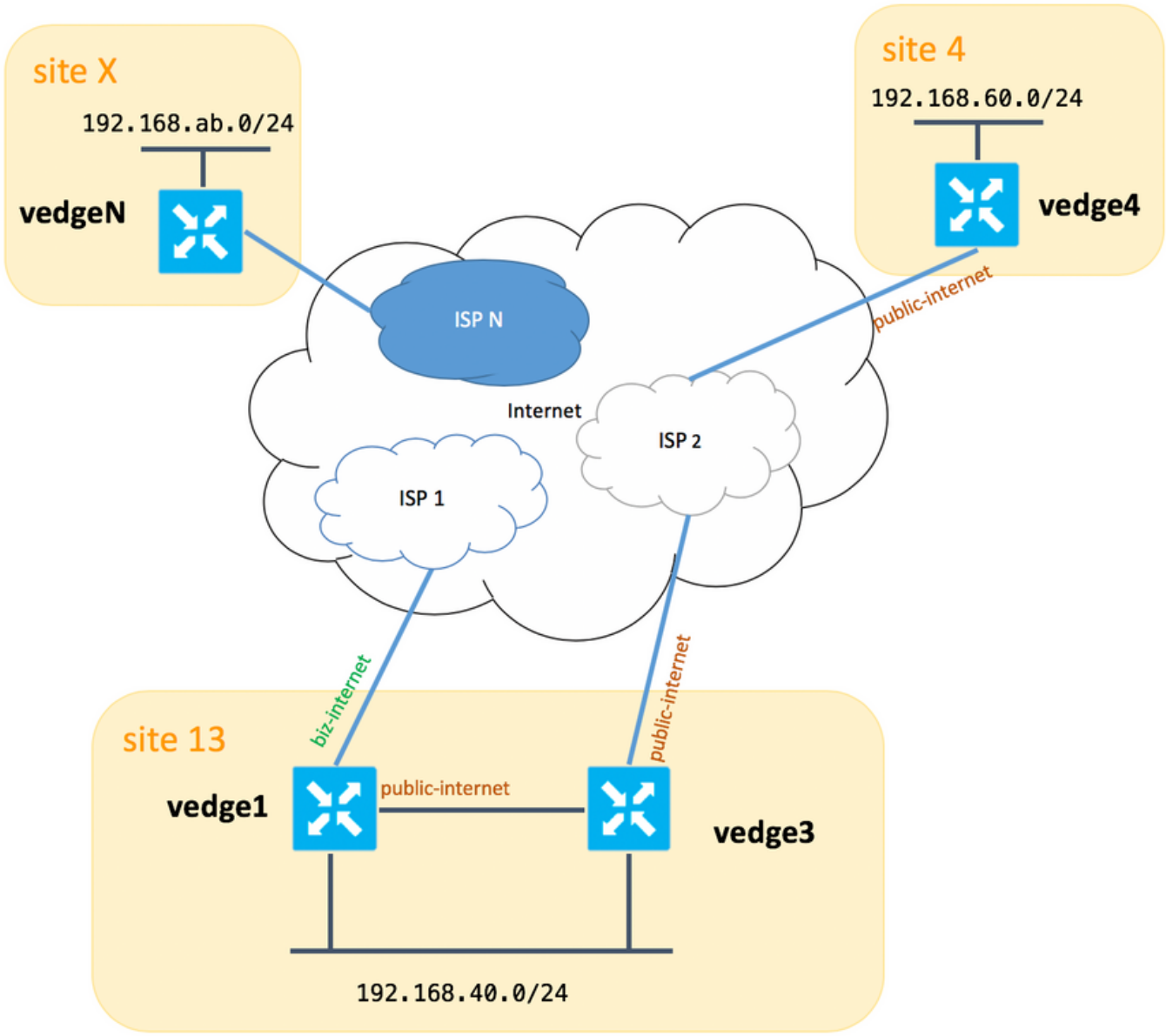
Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Per una dimostrazione e una migliore comprensione del problema descritto più avanti, considerare la topologia mostrata in questa immagine.



Notare che in generale tra **vedge1** e **vedge3** si dovrebbe avere anche un secondo collegamento/sottointerfaccia per l'estensione TLOC **biz-internet**, ma qui per semplicità non è stato configurato.

Di seguito sono riportate le impostazioni di sistema corrispondenti per vEdges/vSmart (vedge2 rappresenta tutti gli altri siti):

hostname	id-sito	ip-sistema
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

Qui è possibile trovare configurazioni lato trasporto per riferimento.

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

L'utente desidera raggiungere i seguenti obiettivi:

Il servizio Internet fornisce l'**ISP 2** e per alcuni motivi è preferibile preferire la comunicazione tra il **sito 13** e il **sito 4**. Ad esempio, è un caso di utilizzo piuttosto comune e uno scenario in cui la qualità della connessione/connettività all'interno di un ISP tra i propri client è molto buona, ma verso il resto della qualità della connettività Internet non soddisfa lo SLA aziendale a causa di alcuni problemi o congestione su un uplink ISP e quindi questo ISP (**ISP 2** nel nostro caso) dovrebbe essere evitato in generale.

Il sito 13 dovrebbe preferire l'uplink **pubblico-internet** per collegarsi al **sito 4**, ma comunque mantenere la ridondanza e dovrebbe essere in grado di raggiungere il **sito 4** se **internet-pubblico** non riesce.

Il **sito 4** deve comunque mantenere la connettività ottimale con tutti gli altri siti direttamente (pertanto non è possibile utilizzare la parola chiave **restrictingqui** su **vedge4** per raggiungere tale obiettivo).

Il **sito 13** dovrebbe utilizzare il collegamento di migliore qualità con il colore **biz-internet** per raggiungere tutti gli altri siti (rappresentato dal **sito X** nel diagramma topologico).

Un altro motivo potrebbe essere costituito da problemi di costo/prezzo quando il traffico all'interno dell'ISP è gratuito, ma molto più costoso quando il traffico che esce da una rete del provider (sistema autonomo).

Alcuni utenti che non hanno esperienza con l'approccio SD-WAN e si abituano al routing classico possono iniziare a configurare il routing statico per forzare il traffico tra **vedge1** e l'indirizzo dell'interfaccia pubblica **vedge4** tramite l'interfaccia di estensione TLOC tra **vedge1** e **vedge3**, ma non daranno il risultato desiderato e possono creare confusione perché:

Il traffico del piano di gestione (ad esempio, ping, pacchetto di utilità traceroute) segue il percorso desiderato.

Allo stesso tempo, i tunnel del piano dati SD-WAN (tunnel IPsec o gre) ignorano le informazioni della tabella di routing e le connessioni dei moduli basate sui **colori** TLOC**.**

Poiché una route statica non dispone di informazioni, se TLOC pubblico-Internet non è attivo su vedge3 (uplink su ISP 2), vedge1 non noterà questa condizione e la connettività a **vedge4** non riuscirà, nonostante **vedge1** disponga ancora di **biz-internet**.

Questo approccio dovrebbe quindi essere evitato e non utilizzabile.

Soluzione

1. Uso di criteri di controllo centralizzati per impostare una preferenza per il TLOC **Internet pubblico** sul controller vSmart quando si annunciano le route OMP corrispondenti per **vedge4.** Aiuta ad archiviare il percorso del traffico desiderato dal **sito 4** al **sito 13**.

2. Per ottenere il percorso del traffico desiderato in direzione inversa dal **sito 13** al **sito 4**, non è possibile usare i criteri di controllo centralizzato perché **vedge4** ha solo un TLOC disponibile, quindi non è possibile impostare una preferenza su niente, ma è possibile usare i criteri di route dell'app per ottenere questo risultato per il traffico in uscita dal **sito 13.**

Di seguito è riportato l'aspetto dei criteri di controllo centralizzati sul controller vSmart per preferire il TLOC **Internet pubblico** al **sito 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 qui c'è un esempio di criteri di route delle app che preferiscono l'uplink **Internet pubblico** come punto di uscita per il traffico in uscita dal **sito 13** al **sito 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
 !
```

I criteri devono essere applicati correttamente sul controller vSmart:

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

I criteri di route dell'app non possono essere configurati come criteri localizzati e devono essere applicati solo a vSmart.

Verifica

Nota: i criteri di route dell'app non verranno applicati al traffico generato localmente da vEdge. Per verificare se i flussi di traffico sono indirizzati in base al percorso desiderato, è consigliabile generare traffico dai segmenti LAN dei siti corrispondenti. Come scenario di test di alto livello, è possibile utilizzare iperf per generare il traffico tra gli host nei segmenti LAN del **sito 13** e del **sito 4** e quindi controllare le statistiche di un'interfaccia. Ad esempio, nel mio caso, non c'era traffico oltre a quello generato dal sistema e quindi potete vedere che la maggior parte del traffico è passata attraverso l'interfaccia ge0/3 verso l'estensione TLOC sul **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
```

Risoluzione dei problemi

Prima di tutto, assicurarsi che le sessioni BFD corrispondenti siano stabilite (non utilizzare parole chiave **restrictes** in nessun punto):

```
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 non è possibile ottenere il risultato desiderato con la progettazione del traffico, verificare che i criteri siano stati applicati correttamente:

1. In vedge4 verificare che per i prefissi originati dal sito 13 sia stato selezionato il valore TLOC appropriato:

```
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. Su **vedge1** e **vedge3** verificare che sia installata la policy appropriata di vSmart e che i pacchetti siano abbinati e conteggiati:

```
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
```

Inoltre, si dovrebbero vedere molti più pacchetti inviati tramite **public-internet** color dal **sito 13** (durante il mio test non c'è stato traffico tramite **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
```

Informazioni correlate

- 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