SD-WAN - Résolution des problèmes d'interface GRE

Contenu

Introduction

Ce document décrit comment résoudre les problèmes d'interface GRE (Generic Routing Encapsulation) dans un environnement SD-WAN.

Informations générales

Dans la solution Cisco Viptela, les exemples d'utilisation des interfaces GRE incluent :

- Envoyer le trafic à ZScaler (HTTP-Proxy) via vSmart Data-Policy ou localement.
- Interface GRE de service principal avec sauvegarde par défaut vers le data center.
- Chaînage de service

Il y a des cas où l'interface GRE ne s'active pas et/ou ne fonctionne pas.

Dans ces situations, vérifiez

- L'interface GRE est activée via : show interface gre*
- Keepalives GRE via : show tunnel gre-keepalives

Méthodologie

En cas de problème, configurez une liste de contrôle d'accès (ACL ou access-list) pour voir si les paquets GRE (47) sortent/entrent.

Vous ne pouvez pas voir les paquets GRE via TCP Dump, car les paquets sont générés par le chemin rapide.

Parfois, en raison de la traduction d'adresses réseau (NAT), les keepalives GRE peuvent être supprimés. Dans ce cas, désactivez le keepalive et vérifiez si le tunnel s'active.

En outre, si le tunnel GRE est constamment en train de basculer et de désactiver des keepalives, cela maintient l'interface en état de marche.

Toutefois, il présente un inconvénient, car s'il y a une question légitime, il est difficile de savoir que le GRE ne fonctionne pas.

Voir ici dans le document qui montre un exemple.

Ceci est une configuration d'interface GRE qui fonctionne

IN VPN0

```
vpn 0
 interface gre1
  ip address 192.0.2.1/30
  tunnel-source
  tunnel-destination
  tcp-mss-adjust     1300
  no shutdown
 !
 interface gre2
  ip address 192.0.2.5/30
  tunnel-source
  tunnel-destination
  tcp-mss-adjust     1300
  no shutdown
 !
!
```

Côté service

```
vpn
service FW interface gre1 gre2
```

Dans la solution Cisco SD-WAN basée sur les routes vEdge, les interfaces GRE fonctionnent en mode actif en veille et non actif-actif.

À tout moment, seule l'interface GRE est à l'état Up/Up.

Pratique

Créer une stratégie pour les listes d'accès

```
vEdge# show running-config policy access-list
policy
 access-list GRE-In
  sequence 10
   match
    protocol 47
   !
   action accept
    count gre-in
   !
  !
  default-action accept
 !
 access-list GRE-Out
  sequence 10
   match
    protocol 47
   !
   action accept
    count gre-out
```

```
   !
  !
  default-action accept
 !
!
vEdge#
```

Créez des compteurs **gre-in** et **gre-out** puis vous devez appliquer la liste de contrôle d'accès à l'interface (nos trajets de tunnel sur ge0/0).

La liste de contrôle d'accès ci-dessus peut être appliquée avec l'adresse source de l'interface physique et l'adresse de destination du point de terminaison GRE.

```
vEdge# show running-config vpn 0 interface ge0/0
vpn 0
 interface ge0/0
  ip address 198.51.100.1/24
  tunnel-interface
   encapsulation ipsec
   max-control-connections 1
   allow-service all
   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
  access-list GRE-In in
  access-list GRE-Out out
 !
!
vEdge#
```

Vous pouvez maintenant voir les compteurs des paquets GRE entrants et sortants, car ils sont dans le chemin rapide, on ne peut pas voir avec l'utilitaire **tcpdump**.

```
vEdge# show policy access-list-counters

         COUNTER
NAME     NAME     PACKETS  BYTES
---------------------------------
GRE-In   gre-in   176      10736
GRE-Out  gre-out  88       2112

vEdge#
```

Voici notre tunnel GRE.

```
vEdge# show interface gre1

                                  IF      IF      IF
TCP
                AF                ADMIN   OPER    TRACKER  ENCAP  PORT
SPEED           MSS                RX       TX
VPN  INTERFACE  TYPE  IP ADDRESS  STATUS  STATUS  STATUS   TYPE   TYPE     MTU   HWADDR
MBPS   DUPLEX  ADJUST  UPTIME      PACKETS  PACKETS
```

```
------------------------------------------------------------------------------------------------
-------------------------------------------------------
0    gre1      ipv4  192.0.2.1/30 Up    Up      NA       null   service  1500  05:05:05:05:00:00
1000   full    1420    0:07:10:28  2968     2968

vEdge#

vEdge# show running-config vpn 0 interface gre1
vpn 0
interface gre1
ip address 192.0.2.1/30/30
tunnel-source-interface ge0/0
tunnel-destination 192.0.2.5/30
no shutdown
!
!
vEdge#
```

Vous pouvez vérifier si le trafic est en cours sur l'interface GRE via la commande **show app cflow**.

Voici un exemple de trafic bidirectionnel (en entrée et en sortie) :

```
vEdge# show app cflowd flows

                                                          TCP
                                                TIME    EGRESS  INGRESS
                                  SRC   DEST          IP     CNTRL  ICMP                  TOTAL
TOTAL      MIN  MAX                             TO      INTF    INTF
VPN  SRC IP        DEST IP        PORT  PORT   DSCP  PROTO  BITS   OPCODE  NHOP IP      PKTS
BYTES      LEN  LEN   START TIME                EXPIRE  NAME    NAME
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------
10   203.0.113.1  203.0.113.11  61478 443    0     6      16     0       203.0.113.254 3399
286304     60   1339  Sun Apr  8 10:23:05 2018  599     gre1    ge0/6
10   203.0.113.11  203.0.113.1  443   61478  0     6      24     0       203.0.113.1262556
192965     40   1340  Sun Apr  8 10:23:05 2018  592     ge0/6   gre1
```

Exemple de désactivation des keepalives (KA) sur l'interface GRE :

KA par défaut est 10 (intervalle Hello) et 3 (tolérance)

Un KA de 0 0 désactive le KA sur l'interface GRE.

```
vEdge# show running-config vpn 0 interface gre* | details
vpn 0
interface gre1
  description         "Primary ZEN"
  ip address <ip/mask>
keepalive 0 0
  tunnel-source
  tunnel-destination
  no clear-dont-fragment
  mtu                 1500
  tcp-mss-adjust      1300
  no shutdown
!
```

Une interface GRE UP/Down s'affiche comme UP/UP (en passant la vérification KA).

Voyez, compteur TX ici quand il augmente quand KA est désactivé. Cela signifie que vEdge est TX les paquets, mais vous ne voyez pas l'augmentation du compteur RX, qui pointe sur un

problème distant.

```
vEdge# show interface gre*

                                  IF      IF
        TCP
                                  ADMIN   OPER    ENCAP  PORT                                SPEED
        MSS                 RX          TX
VPN  INTERFACE  IP ADDRESS        STATUS  STATUS  TYPE   TYPE     MTU   HWADDR              MBPS
DUPLEX  ADJUST  UPTIME      PACKETS     PACKETS
-------------------------------------------------------------------------------------------------
-------------------------------------------------
### With KA ON
0    gre1      192.0.2.1/30  Up      Down    null   service  1500  cb:eb:98:02:00:00  -      -
    1300    -           413218129  319299248
### With KA OFF
0    gre1       192.0.2.1/30  Up      Up      null   service  1500  cb:eb:98:02:00:00  100
half    1300    0:00:01:19  413218129  319299280
```