SD-WAN - Identificação e Solução de Problemas de Interface GRE

Contents

Introduction

Este documento descreve como solucionar problemas de interface GRE (Generic Routing Encapsulation) em um ambiente SD-WAN.

Informações de Apoio

Na solução Cisco Viptela, os casos de uso para interfaces GRE incluem:

- Enviar tráfego para ZScaler (HTTP-Proxy) via vSmart Data-Policy ou localmente.
- Interface GRE de serviço principal com backup padrão para o data center.
- Cadeamento de serviços

Há casos em que a interface GRE pode não aparecer e/ou não funcionar.

Nessas situações, verifique se

- A interface GRE está ativa/ativa via: show interface gre*
- GRE Keepalives via: show tunnel gre-keepalives

Metodologia

Se houver um problema, configure uma lista de controle de acesso (ACL ou lista de acesso) para ver se os pacotes GRE (47) estão saindo/entrando.

Você não consegue ver os pacotes GRE através de TCP Dump, pois os pacotes são gerados pelo caminho rápido.

Às vezes, devido à conversão de endereço de rede (NAT), as manutenções de atividade de GRE podem ser descartadas. Nesse caso, desative o keepalive e veja se o túnel aparece.

Além disso, se o túnel GRE estiver constantemente oscilando e desabilitando keepalives, isso manterá a interface ativa/ativa.

No entanto, tem uma desvantagem, em que, se há uma questão legítima, é difícil descobrir que o GRE não funciona.

Veja aqui no documento que mostra um exemplo.

Esta é uma configuração de interface GRE em funcionamento

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
 !
!
```

no lado Serviço

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

Na solução Cisco SD-WAN baseada em rotas vEdge, as interfaces GRE funcionam como Ativo-em espera e não Ativo-Ativo.

A qualquer momento, há apenas a Interface GRE que está no estado Up/Up.

Prática

Criar uma política para listas de acesso

```
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#
```

Crie contadores **gre-in** e **gre-out** e então você precisa aplicar a ACL à interface (nosso túnel caminha sobre ge0/0).

A ACL acima pode ser aplicada com o endereço de origem da interface física e o endereço de destino do ponto de extremidade 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#
```

Agora você pode ver os contadores dos pacotes GRE para dentro e para fora porque eles estão no caminho rápido, não se pode ver com o utilitário **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#
```

Este é o nosso túnel 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#
```

Você pode verificar se o tráfego está indo na interface GRE por meio do comando **show app cflowd flows**.

Este exemplo mostra o tráfego bidirecional (da entrada e da saída):

```
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
```

Um exemplo de desabilitação de keepalives (KA) na interface GRE:

O KA padrão é 10 (intervalo de hello) e 3 (tolerância)

Um KA de 0 0 desativa o KA na 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
!
```

Uma interface GRE que é UP/Down é exibida como UP/UP (passando pela verificação KA).

Veja, contador de TX aqui à medida que aumenta quando o KA está DESLIGADO. Significa que

o vEdge é o TX dos pacotes, mas você não vê o aumento no contador RX, que aponta para um problema remoto.

```
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
```