

SD-WAN:GREインターフェイスの問題のトラブルシューティング

内容

[概要](#)

[背景説明](#)

[方法](#)

[実践](#)

概要

このドキュメントでは、SD-WAN環境でGeneric Routing Encapsulation(GRE)インターフェイスの問題をトラブルシューティングする方法について説明します。

背景説明

Cisco Viptelaソリューションでは、GREインターフェイスの使用例は次のとおりです。

- トラフィックをvSmart Data-Policy経由またはローカルでZScaler (HTTPプロキシ) に送信します。
- プライマリサービスGREインターフェイスと、データセンターへのデフォルトバックアップ
- サービスチェーン

GREインターフェイスが起動しない、または動作しない場合があります。

このような場合は、

- GREインターフェイスがアップ/アップ状態の場合 : `show interface gre*`
- GREキープアライブ : `show tunnel gre-keepalives`

方法

問題がある場合は、アクセスコントロールリスト (ACLまたはアクセスリスト) を設定して、GRE(47)パケットが発信/着信しているかどうかを確認します。

パケットは高速パスによって生成されるため、TCPダンプを介してGREパケットを表示できません。

ネットワークアドレス変換(NAT)が原因で、GREキープアライブがドロップされることがあります。この場合は、キープアライブを無効にして、トンネルがアップするかどうかを確認します。

また、GREトンネルが常にフラッピングし、キープアライブを無効にしている場合は、インターフェイスのアップ/アップが維持されます。

ただし、これは欠点があり、正当な問題がある場合は、GREが機能しないことを確認するのは困難です。

例を示すドキュメントの中で、ここを参照してください。

これは動作中のGREインターフェイス設定です

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
!
```

インサービス側

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

vEdgeルートに基づくCisco SD-WANソリューションでは、GREインターフェイスはアクティブ-スタンバイとして動作し、アクティブ-アクティブではありません。

常に、Up/Up状態のGREインターフェイスしかありません。

実践

アクセスリストのポリシーの作成

```
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
```



```
-----
-----
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#

トラフィックがGREインターフェイスで行われているかどうかは、**show app cflowd flows**コマンドで確認できます。

次の例は、双方向トラフィック (入力と出力の両方) を示しています。

```
vEdge# show app cflowd flows
```

```
-----
-----
                                TCP
                                TIME  EGRESS INGRESS
                                SRC  DEST   IP      CNTRL  ICMP
TOTAL      MIN  MAX
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
```

GREインターフェイスでキープアライブ(KA)を無効にする例を次に示します。

デフォルトのKAは10(hello-interval)および3(tolerance)です

0のKAは、GREインターフェイスのKAを無効にします。

```
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
!
```

UP/DownのGREインターフェイスは、(KAチェックを渡すことによって) UP/UPと表示されま

す。

KAがオフの場合はカウンタが増加するため、ここでTXカウンタを参照してください。つまり、vEdgeはパケットをTXしますが、RXカウンタの増加は確認できず、リモートの問題を示しています。

```
vEdge# show interface gre*
```

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