

排除故障GRE接口

目录

[简介](#)

[背景信息](#)

[方法](#)

[实践](#)

简介

本文描述如何排除故障通用路由封装(GRE)接口。

背景信息

在Viptela解决方案， GRE接口的使用事例包括：

- 发送流量对ZScaler (本地HTTP代理)通过vSmart数据策略或。
- 主服务GRE接口用对数据中心的默认上一步。
- 服务连锁

当GRE接口可能不出来并且/或者不工作时，有案件。

在那些情况下，请检查

- GRE接口是up/up通过： show interface gre*
- GRE Keepalive通过： 显示通道gre Keepalive

方法

如果有问题，请配置访问控制表(ACL或access-list)发现GRE (47)数据包是否是出去的/in。

因为数据包由快速路径，生成您无法通过TCP发现GRE数据包转存。

有时，由于网络地址转换(NAT)， GRE Keepalive可以丢弃。在这种情况下，请禁用Keepalive并且检查通道是否出来。

并且，如果GRE隧道经常拍动和禁用的Keepalive，这保持接口up/up。

然而，它有一个缺点，如果有一个合法问题，是难找到的GRE不工作。

请参阅此处显示示例的本文。

这是工作的GRE接口设置

IN VPN0

```

vpn 0
interface gre1
 ip address 192.0.2.1/30
 tunnel-source      <SRC-IP>
 tunnel-destination <DST-IP>
 tcp-mss-adjust    1300
 no shutdown
!
interface gre2
 ip address 192.0.2.5/30
 tunnel-source      <SRC-IP>
 tunnel-destination <DST-IP>
 tcp-mss-adjust    1300
 no shutdown
!
!

```

IN服务侧

```

vpn <SRVC-VPN>
service FW interface gre1 gre2

```

在根据vEdge路由的Cisco SD-WAN解决方案，GRE建立接口工作作为激活待机和不主动-主动。

在指定时间，有在UP/UP状态仅的GRE接口。

实践

创建访问列表的一项策略

```

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#

```

创建计数器gre在，并且gre您然后需要应用ACL到接口(我们的通道在ge0/0乘坐)。

上述ACL可以应用与物理接口的GRE终端的源地址和目的地址。

```
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
!
```

现在您能为GRE数据包看到计数器，因为这些在快速路径，一个用tcpdump工具里里外外看不到。

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

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

```
vEdge#
```

这是我们的GRE隧道。

```
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#
如果流量在GRE接口去通过show app cflowd流命令，您能验证。

这是示例显示双向数据流(两个从入口和出口)：

vEdge# show app cflowd flows

TOTAL	MIN	MAX	SRC	DEST	TIME	TCP		EGRESS	INGRESS	TOTAL
						IP	CNTRL			
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	203.0.113.126	2556
192965	40	1340	Sun Apr 8 10:23:05 2018	592	ge0/6	gre1				

示例禁用的Keepalive (KA)在GRE接口：

默认KA是10 (Hello间隔)和3 (容差)

KA 0 0，禁用在GRE接口的KA。

```
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 <SRC-IP-Addr>
  tunnel-destination <DST-IP-Addr>
  no clear-dont-fragment
  mtu 1500
  tcp-mss-adjust 1300
  no shutdown
```

!
UP/Down的GRE接口显示如UP/UP (通过通过KA检查)。

请参阅，TX计数器此处，当增加，当KA是OFF。它含义，vEdge是TX数据包，但是您看不到在RX计数器的增加，指向一个远程问题。

vEdge# show interface gre*

VPN	INTERFACE	IP ADDRESS	RX	TX	ENCAP	PORT	MTU	HWADDR	SPEED
DUPLEX	ADJUST	UPTIME	PACKETS	PACKETS	TYPE	TYPE			MBPS
###	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					