

# SD-WAN - Risoluzione dei problemi dell'interfaccia GRE

## Sommario

[Introduzione](#)

[Premesse](#)

[Metodologia](#)

[Esercitazione](#)

## Introduzione

Questo documento descrive come risolvere i problemi dell'interfaccia GRE (Generic Routing Encapsulation) in un ambiente SD-WAN.

## Premesse

Nella soluzione Cisco Viptela, gli scenari di utilizzo delle interfacce GRE includono:

- Inviare il traffico a ZScaler (HTTP-Proxy) tramite vSmart Data-Policy o in locale.
- Interfaccia GRE di servizio principale con backup predefinito nel centro dati.
- Concatenamento dei servizi

In alcuni casi, l'interfaccia GRE potrebbe non venire e/o non funzionare.

In tali situazioni, verificare

- L'interfaccia GRE è attiva/attiva tramite: `show interface gre*`
- GRE Keepalives tramite: `mostra tunnel gre-keepalives`

## Metodologia

In caso di problemi, configurare un Access Control List (ACL o access-list) per verificare se i pacchetti GRE (47) stanno uscendo o entrando.

Non è possibile visualizzare i pacchetti GRE tramite dump TCP, in quanto i pacchetti sono generati dal percorso rapido.

A volte, a causa della NAT (Network Address Translation), i pacchetti keepalive GRE possono essere eliminati. In questo caso, disabilitare l'opzione keepalive e verificare se il tunnel viene attivato.

Inoltre, se il tunnel GRE sposta e disabilita continuamente i pacchetti keepalive, l'interfaccia rimane attiva/attiva.

Tuttavia, ha un inconveniente, dove se c'è un problema legittimo, è difficile scoprire che il GRE non funziona.

Fare riferimento a questo punto del documento che mostra un esempio.

Questa è una configurazione dell'interfaccia GRE funzionante

## 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
 !
 !
```

## Lato servizio

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

In una soluzione Cisco SD-WAN basata su route vEdge, le interfacce GRE funzionano come active-standby e non attive-attive.

In qualsiasi momento, solo l'interfaccia GRE è nello stato Up/Up.

## Esercitazione

Creare un criterio per gli elenchi degli accessi

```
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#

```

Creare i contatori **gre-in** e **gre-out** e quindi applicare l'ACL all'interfaccia (il tunnel supera ge0/0).

Questo ACL può essere applicato con l'indirizzo di origine dell'interfaccia fisica e l'indirizzo di destinazione dell'endpoint 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#

```

Ora è possibile vedere i contatori per i pacchetti GRE in entrata e in uscita perché questi si trovano nel percorso rapido, non si può vedere con l'utilità **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#
```

Questo è il nostro tunnel GRE.

```
vEdge# show interface gre1
```

										IF	IF	IF		
										ADMIN	OPER	TRACKER	ENCAP	PORT
										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
!
!
```

È possibile verificare se il traffico è in corso sull'interfaccia GRE tramite il comando **show app cflow**.

Nell'esempio seguente viene mostrato un traffico bidirezionale (sia in entrata che in uscita):

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

TOTAL		MIN	MAX	SRC		DEST	TIME	TCP		EGRESS		INGRESS		TOTAL
VPN	SRC IP	LEN	LEN	DEST IP	PORT	PORT	TO	IP	CNTRL	ICMP	INTF	INTF	NHOP IP	PKTS
BYTES				START TIME			EXPIRE	PROTO	BITS	OPCODE	NAME	NAME		
10	203.0.113.1	60	1339	203.0.113.11	443	0	6	16	0		203.0.113.254	ge0/6	203.0.113.254	3399
286304				Sun Apr 8 10:23:05 2018			599	gre1			gre1	ge0/6		
10	203.0.113.11	40	1340	203.0.113.1	443	61478	0	24	0		203.0.113.126	gre1	203.0.113.126	2556
192965				Sun Apr 8 10:23:05 2018			592	ge0/6			gre1	gre1		

Ad esempio, è possibile disabilitare l'invio dei pacchetti keepalive (KA) sull'interfaccia GRE:

Il valore predefinito per KA è 10 (intervallo hello) e 3 (tolleranza)

Un KA pari a 0,0 disabilita il KA sull'interfaccia 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
!
```

Un'interfaccia GRE con direzione UP/DOWN viene visualizzata come UP/UP (passando il controllo KA).

Vedere, contatore TX qui come aumenta quando KA è OFF. In altre parole, vEdge imposta la trasmissione dei pacchetti, ma non viene visualizzato l'aumento del contatore RX, che indica un

problema remoto.

vEdge# show interface gre\*

VPN	INTERFACE	IP ADDRESS	RX	TX	ADMIN	OPER	ENCAP	PORT	MTU	HWADDR	SPEED
DUPLEX	ADJUST	UPTIME	PACKETS	PACKETS	STATUS	STATUS	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							