Come funziona il GRE Keepalives

Sommario

Introduzione

In questo documento viene fornita una panoramica del funzionamento dei pacchetti keepalive GRE (Generic Routing Encapsulation).

Prerequisiti

Requisiti

Questo documento è utile per conoscere i seguenti argomenti:

- Tunnel GRE Keepalive
- Comandi Della Modalità Di Configurazione Keepalive

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 7505 Router
- Software Cisco IOS® che supporta GRE over IPSec

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

La funzione GRE keepalive abilita il comando di interfaccia **keepalive** per i tunnel e consente di configurare i keepalive per i tunnel GRE point-to-point. È possibile configurare i pacchetti keepalive con il comando **keepalive** e, facoltativamente, con la nuova estensione.

I tunnel GRE forniscono un metodo per incapsulare pacchetti arbitrari all'interno di un protocollo di trasporto. Offrono inoltre un'architettura progettata per fornire i servizi richiesti per implementare uno schema di incapsulamento point-to-point standard. Di seguito sono elencati alcuni dei vantaggi dei tunnel GRE:

- I tunnel GRE forniscono reti locali multiprotocollo su una backbone a protocollo singolo.
- I tunnel GRE offrono soluzioni per le reti che contengono protocolli con conteggi degli hop limitati.
- I tunnel GRE connettono reti secondarie discontinue.
- I tunnel GRE permettono le VPN sulle WAN.

Tuttavia, nell'implementazione corrente dei tunnel GRE, un tunnel configurato non è in grado di disattivare il protocollo di linea di nessuno dei due endpoint del tunnel, se l'estremità remota non è raggiungibile. Pertanto, il traffico inviato dal tunnel è bloccato e non può seguire percorsi alternativi perché il tunnel rimane sempre attivo.

Questa situazione si verifica per i tunnel che si basano su route statiche o su protocolli di routing che aggregano le route per trovare una destinazione del tunnel. Ciò è valido anche in situazioni in cui i dati nel piano di controllo seguono un percorso diverso dai dati nel piano dati.

Meccanismo Keepalive tunnel

In questa sezione viene fornita una descrizione funzionale del meccanismo keepalive del tunnel con l'aiuto di un esempio. In questa sezione vengono inoltre elencati gli elementi software modificati da questa funzionalità e viene descritto l'impatto sulla memoria e sulle prestazioni.

Descrizione funzionale

Il meccanismo tunnel keepalive abilita, estende e implementa un comando specifico per l'interfaccia per le interfacce tunnel e consente di disattivare il protocollo di linea di un tunnel. Per ulteriori informazioni, vedere la sezione Comandi e configurazione.

Il meccanismo keepalive del tunnel soddisfa anche questi requisiti aggiuntivi:

- Il meccanismo keepalive del tunnel funziona anche se l'endpoint del tunnel remoto non supporta i pacchetti keepalive.
- Il meccanismo keepalive del tunnel genera i pacchetti keepalive.

- Il meccanismo keepalive del tunnel elabora i pacchetti keepalive.
- Il meccanismo keepalive del tunnel risponde ai pacchetti keepalive dell'estremità remota, anche quando il protocollo di linea del tunnel non è attivo.

Di seguito è riportato un esempio di come funziona il meccanismo keepalive del tunnel (vedere la Figura 1):

Figura 1 - Esempio del meccanismo keepalive del tunnel

Uscita

```
interface tunnel 0                          interface tunnel 0
ip address 1.1.1.1 255.255.255.240          ip address 1.1.1.2 255.255.255.240
tunnel source 128.8.8.8                     tunnel source 129.9.9.9
tunnel destination 129.9.9.9                tunnel destination 128.8.8.8
keepalive 5 4                               keepalive 5 4
interface loopback 0                        interface loopback 0
ip address 128.8.8.8 255.255.255.255       ip address 129.9.9.9 255.255.255.255
```

Un pacchetto keepalive proveniente da A a B

```
---outer IP header---'      ---inner IP header---'
============================================================
|IP | IP src  | IP dst  | GRE | IP | IP src  | IP dst  | GRE |
|   |128.8.8.8|129.9.9.9|PT=IP|    |129.9.9.9|128.8.8.8| PT=0|
============================================================
                         ----'                         ---'
                          GRE header                    GRE header
```

Quando si abilitano i pacchetti keepalive sull'endpoint del tunnel del router A, il router costruisce l'intestazione IP interna a ogni intervallo. Alla fine dell'intestazione, il router aggiunge anche un'intestazione GRE con un Protocol Type (PT) pari a 0 e nessun altro payload. Il router invia quindi il pacchetto attraverso il tunnel, con il risultato che il pacchetto è incapsulato nell'intestazione IP esterna, e in un'intestazione GRE con il bit dell'IP. Il contatore tunnel keepalive aumenta di uno. Se esiste un modo per raggiungere l'endpoint del tunnel all'estremità remota e il protocollo della linea del tunnel non è attivo per altri motivi, il pacchetto arriva sul router B. Viene quindi stabilita una corrispondenza con il tunnel 0, viene decapsulato e inoltrato all'IP di destinazione, che è l'origine del tunnel, il router A. All'arrivo sul router A, il pacchetto viene nuovamente decapsulato e il router PT viene controllato. Se il risultato del controllo PT è 0, il pacchetto è keepalive. In questo caso, il contatore tunnel keepalive viene reimpostato su 0 e il pacchetto viene scartato.

Se il router B non è raggiungibile, il router A continua a costruire e inviare i pacchetti keepalive insieme al traffico normale. Se il protocollo di linea non è attivo, i pacchetti keepalive non tornano al router A. Pertanto, il contatore keepalive continua ad aumentare. Il protocollo della linea del tunnel rimane attivo solo finché il contatore tunnel keepalive rimane zero o inferiore a un valore configurato. Se questa condizione non è vera, al successivo tentativo di inviare un comando keepalive al router B, il protocollo di linea viene interrotto non appena il contatore raggiunge il valore keepalive configurato. Nello stato attivo/inattivo, il tunnel non inoltra o elabora il traffico a

parte i pacchetti keepalive. Affinché questa procedura funzioni solo per i pacchetti keepalive, il tunnel deve essere facile da inoltrare e ricevere. Pertanto, l'algoritmo di ricerca del tunnel deve avere esito positivo in tutti i casi e deve ignorare solo i pacchetti di dati se il protocollo di linea non è attivo. Quando si riceve un pacchetto keepalive, l'endpoint del tunnel è nuovamente raggiungibile. Il contatore tunnel keepalive viene quindi reimpostato su 0 e il protocollo di linea torna attivo.

Impatto su memoria e prestazioni

Questa funzionalità non comporta quasi alcuna richiesta aggiuntiva per la memoria di sistema del router e non dovrebbe influire sulle prestazioni. I pacchetti keepalive vengono trattati come pacchetti normali, quindi è possibile che vengano scartati in condizioni di traffico elevato. Per il momento, è possibile modificare il numero di tentativi per risolvere il problema. Se alla fine questa condizione si dimostra inadeguata, è possibile mettere i pacchetti keepalive generati localmente in una coda ad alta priorità per la trasmissione. È quindi possibile impostare il valore TOS nelle intestazioni IP su un valore più appropriato, diverso da quello predefinito o configurato.

Considerazioni sull'imballaggio

Questa funzionalità è inclusa nel codice del tunnel IP di base e nel sottosistema GRE. Pertanto, deve essere disponibile con un pacchetto IP di base con sottosistemi tunnel e GRE.

Comandi e configurazione

In questa sezione viene descritto il comando **keepalive** abilitato ed esteso da questa funzione solo con l'ID bug Cisco CSCuk26449. Per altri comandi, consultare la documentazione delle *rispettive guide alla configurazione e riferimenti ai comandi di Cisco IOS*. Il comando **[no] keepalive <*period*> <*retries*>**viene abilitato ed esteso con un secondo parametro ed è disponibile nel software Cisco IOS versione 12.2(8)T e successive. È stato inoltre trasferito con ID bug Cisco CSCuk2980 e CSCuk2983 al software Cisco IOS versioni 12.1E e 12.2S.

Poiché **keepalive** è un comando di configurazione interfaccia che abilita i pacchetti keepalive sull'interfaccia del tunnel, al momento sono supportati solo i pacchetti keepalive per la modalità GRE/IP. Il secondo parametro del comando (*retries*) è visibile e disponibile solo per le interfacce tunnel. I valori del primo parametro possono essere compresi tra 1 e 32767. Quando il valore è 0, equivale a "no keepalive". Il valore predefinito di questo parametro è 10. I valori del secondo parametro possono essere compresi tra 1 e 255 e indicano il numero di pacchetti keepalive inviati ma non restituiti, dopodiché l'interfaccia del tunnel riduce il protocollo di linea. Per impostazione predefinita, i pacchetti keepalive sulle interfacce tunnel sono disabilitati.

Output di esempio e formati dello schermo

In questa sezione vengono forniti output di esempio.

```
cisco-7505#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
cisco-7505(config)#interface tunnel 1
cisco-7505(config-if)#?
  access-expression   Build a bridge boolean access expression
  ……
  keepalive           Enable keepalive<=====
```

```
  ..............
  timeout             Define timeout values for this interface

cisco-7505(config-if)#keepalive ?<=====
  <0-32767>  Keepalive period (default 10 seconds)

cisco-7505(config-if)#keepalive 5 ?<=====
  <1-255>    Keepalive retries (default 3 times)
cisco-7505(config-if)#keepalive 5 4<=====
cisco-7505(config-if)#end

cisco-7505#show interfaces tunnel 1

Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.1.1.1/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (5 sec), retries 4<=====
  Tunnel source 9.2.2.1, destination 6.6.6.2
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TOS 0xF, Tunnel TTL 128
  Checksumming of packets disabled, fast tunneling enabled
  Last input never, output 00:57:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 1 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     3 packets output, 1860 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Informazioni correlate

- Tunnel GRE (Generic Routing Encapsulation) Keepalive
- Configurazioni di esempio GRE
- Documentazione e supporto tecnico