Informazioni sui pacchetti keepalive del tunnel GRE

Sommario

Introduzione

In questo documento viene descritto cosa sono i pacchetti keepalive GRE (Generic Routing Encapsulation) e come funzionano.

Tunnel GRE

Un tunnel GRE è un'interfaccia logica usata sui router Cisco per incapsulare i pacchetti in un protocollo di trasporto. Si tratta di un'architettura progettata per fornire i servizi e implementare uno schema di incapsulamento point-to-point.

I tunnel GRE sono progettati per essere completamente privi di stato. Ciò significa che ogni endpoint del tunnel non mantiene alcuna informazione sullo stato o sulla disponibilità dell'endpoint del tunnel remoto. Di conseguenza, il router dell'endpoint del tunnel locale non è in grado di disattivare il protocollo di linea dell'interfaccia del tunnel GRE se l'estremità remota del tunnel non è raggiungibile. La possibilità di contrassegnare un'interfaccia come inattiva quando l'estremità remota del collegamento non è disponibile viene usata per rimuovere tutte le route (in particolare le route statiche) nella tabella di routing che usano quell'interfaccia come interfaccia in uscita. In particolare, se il protocollo di linea di un'interfaccia viene modificato in inattivo, tutte le route statiche che puntano all'esterno dell'interfaccia vengono rimosse dalla tabella di routing. In questo modo, è possibile installare un percorso statico alternativo (mobile) o un percorso PBR (Policy Based Routing) per selezionare un hop o un'interfaccia alternativi.

In genere, un'interfaccia del tunnel GRE viene visualizzata non appena configurata e rimane attiva finché è presente un indirizzo di origine del tunnel valido o un'interfaccia attiva. Anche l'indirizzo IP di destinazione del tunnel deve essere instradabile. Ciò vale anche se l'altro lato del tunnel non è stato configurato. Ciò significa che un percorso statico o l'inoltro PBR dei pacchetti tramite

l'interfaccia del tunnel GRE rimane attivo anche se i pacchetti del tunnel GRE non raggiungono l'altra estremità del tunnel.

Prima che i pacchetti keepalive GRE venissero implementati, c'erano solo modi per determinare i problemi locali sul router e non c'era modo di determinare i problemi sulla rete in uso. Ad esempio, il caso in cui i pacchetti del tunnel GRE vengono inoltrati correttamente, ma vengono persi prima di raggiungere l'altra estremità del tunnel. Questi scenari provocherebbero un "buco nero" dei pacchetti di dati che passano attraverso il tunnel GRE, anche se era disponibile un percorso alternativo che usa il PBR o un percorso statico mobile tramite un'altra interfaccia. I pacchetti keepalive sull'interfaccia del tunnel GRE vengono usati per risolvere questo problema allo stesso modo in cui i pacchetti keepalive vengono usati sulle interfacce fisiche.

> **Nota**: in nessun caso i pacchetti keepalive GRE sono supportati insieme alla protezione del tunnel IPsec. In questo documento viene descritto questo problema.

Funzionamento dei pacchetti keepalive del tunnel

Il meccanismo keepalive del tunnel GRE è simile ai pacchetti keepalive PPP in quanto consente a un dispositivo di originare e ricevere pacchetti keepalive da e verso un router remoto anche se il router remoto non supporta i pacchetti keepalive GRE. Poiché GRE è un meccanismo di tunneling dei pacchetti per il tunneling IP all'interno dell'IP, è possibile creare un pacchetto del tunnel GRE IP all'interno di un altro pacchetto del tunnel GRE IP. Per i pacchetti keepalive GRE, il mittente precostruisce il pacchetto di risposta keepalive all'interno del pacchetto di richiesta keepalive originale in modo che l'estremità remota debba solo eseguire la decapsulamento GRE standard dell'intestazione IP GRE esterna e quindi restituire il pacchetto GRE IP interno al mittente. Questi pacchetti spiegano i concetti del tunneling IP con protocollo di incapsulamento GRE e protocollo di trasporto IP. Il protocollo passeggeri è sempre IP, anche se può essere un altro protocollo, ad esempio Decnet, Internetwork Packet Exchange (IPX) o Appletalk.

Pacchetto normale:

Intestazione IP	Intestazione TCP	Telnet

Pacchetto tunneling:

GRE IP Header	GRE	Intestazione IP	Intestazione TCP	Telnet

- IP è il protocollo di trasporto.
- GRE è il protocollo di incapsulamento.
- IP è il protocollo passeggeri.

Di seguito è riportato un esempio di pacchetto keepalive proveniente dal router A e destinato al router B. La risposta keepalive che il router B restituisce al router A è già all'interno dell'intestazione IP interna. Il router B decapsula il pacchetto keepalive e lo invia nuovamente all'interfaccia fisica (S2). Elabora il pacchetto GRE keepalive come qualsiasi altro pacchetto di dati GRE IP.

GRE Keepalives:

GRE IP Header		GRE	Intestazione IP		GRE
Origine A	Destinazione B	PT=IP	Origine B	Destinazione A	PT=0

Questo meccanismo fa sì che la risposta keepalive venga inoltrata sull'interfaccia fisica anziché sull'interfaccia del tunnel. Ciò significa che il pacchetto di risposta GRE keepalive non è influenzato da alcuna funzionalità di output sull'interfaccia del tunnel, ad esempio 'protezione del tunnel ...', QoS, Virtual Routing and Forwarding (VRF), e così via.

> **Nota**: se è configurato un ACL (Access Control List) in entrata sull'interfaccia del tunnel GRE, il pacchetto keepalive del tunnel GRE inviato dal dispositivo opposto deve essere autorizzato. In caso contrario, il tunnel GRE del dispositivo opposto si blocca. (`access-list <numero> allow gre host <origine-tunnel> host <destinazione-tunnel>`)

Un altro attributo dei pacchetti keepalive del tunnel GRE è che i timer keepalive su entrambi i lati sono indipendenti e non devono corrispondere, in modo simile ai pacchetti keepalive PPP.

> **Suggerimento**: il problema con la configurazione dei pacchetti keepalive solo su un lato del tunnel è che solo il router con i pacchetti keepalive configurati contrassegna l'interfaccia del tunnel come inattiva se il timer keepalive scade. L'interfaccia del tunnel GRE sull'altro lato, dove non sono configurati i pacchetti keepalive, rimane attiva anche se l'altro lato del tunnel è inattivo. Il tunnel può diventare un buco nero per i pacchetti diretti nel tunnel dal lato in cui non è stato configurato il supporto dei pacchetti keepalive.

> **Suggerimento**: in una rete di tunnel GRE hub e spoke di grandi dimensioni, è possibile configurare i pacchetti keepalive GRE solo sul lato spoke e non sul lato hub. Questo perché è spesso più importante che lo spoke scopra che l'hub è irraggiungibile e quindi passa a un percorso di backup (ad esempio, Dial Backup).

Keepalive tunnel GRE

Con il software Cisco IOS® versione 12.2(8)T, è possibile configurare i pacchetti keepalive su un'interfaccia del tunnel GRE point-to-point. Con questa modifica, l'interfaccia del tunnel viene chiusa in modo dinamico se i pacchetti keepalive si interrompono per un determinato periodo di tempo.

Per ulteriori informazioni sul funzionamento di altre forme di pacchetti keepalive, consultare la panoramica dei meccanismi keepalive su Cisco IOS.

> **Nota**: i pacchetti keepalive del tunnel GRE sono supportati solo sui tunnel GRE point-to-point. I pacchetti keepalive del tunnel sono configurabili sui tunnel GRE (Multipoint GRE), ma non hanno effetto.

> **Nota**: in generale, i pacchetti keepalive del tunnel non possono funzionare quando i VRF vengono utilizzati sull'interfaccia del tunnel e sull'fVRF ("tunnel vrf ...e iVRF ("inoltro ip vrf ...' sull'interfaccia del tunnel) non corrispondono. Questa condizione è critica sull'endpoint del tunnel che "riflette" il keepalive restituito al richiedente. Quando si riceve la richiesta keepalive, questa viene ricevuta nella fVRF e decapsulata. Ciò rivela la risposta keepalive

predefinita, che deve essere inoltrata nuovamente al mittente, MA che l'inoltro si trova nel contesto del VRF sull'interfaccia del tunnel. Pertanto, se il VRF e il VRF non corrispondono, il pacchetto di risposta keepalive non viene inoltrato indietro al mittente. Ciò è vero anche se si sostituisce iVRF e/o fVRF con "global".

Questo output mostra i comandi utilizzati per configurare i pacchetti keepalive sui tunnel GRE.

```
Router#configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].



!--- Keepalives are sent every 5 seconds and 4 retries.
!--- Keepalives must be missed before the tunnel is shut down.
!--- The default values are 10 seconds for the interval and 3 retries.
```

Per comprendere meglio il funzionamento del meccanismo keepalive del tunnel, prendere in considerazione questo esempio la topologia e la configurazione del tunnel:

Router A

```
interface loopback 0
ip address 192.168.1.1 255.255.255.255
interface tunnel 0
ip address 10.10.10.1 255.255.255.252
tunnel source loopback0
tunnel destination 192.168.1.2
keepalive 5 4
```

Router B

```
interface loopback 0
ip address 192.168.1.2 255.255.255.255
interface tunnel 0
ip address 10.10.10.2 255.255.255.252
tunnel source loopback0
tunnel destination 192.168.1.1
keepalive 5 4
```

In questo scenario, il router A esegue i seguenti passaggi:

1. Costruisce l'intestazione IP interna ogni cinque secondi in cui:

   l'origine è impostata come destinazione locale del tunnel, ossia 192.168.1.2la destinazione è impostata come origine del tunnel locale, ossia 192.168.1.1

   e viene aggiunta un'intestazione GRE con un Protocol Type (PT) pari a 0

   Pacchetto generato dal router A ma non inviato:

2. Invia il pacchetto fuori dall'interfaccia del tunnel, con conseguente incapsulamento del pacchetto con l'intestazione IP esterna, dove:

   l'origine viene impostata come origine locale del tunnel, ossia 192.168.1.1la destinazione è impostata come destinazione del tunnel locale, ossia 192.168.1.2

   e viene aggiunta un'intestazione GRE con PT = IP.

   Pacchetto inviato dal router A al router B:

3. Incrementa di uno il contatore keepalive del tunnel.

4. Presupponendo che ci sia un modo per raggiungere l'endpoint del tunnel all'estremità remota e che il protocollo della linea del tunnel non sia inattivo per altri motivi, il pacchetto arriva sul router B. Viene quindi confrontato con il tunnel 0, viene decapsulato e inoltrato all'IP di destinazione, ossia l'indirizzo IP di origine del tunnel sul router A.

   Inviato dal router B al router A:

5. All'arrivo sul router A, il pacchetto viene decapsulato e il controllo del PT restituisce 0. Ciò significa che si tratta di un pacchetto keepalive. Il contatore tunnel keepalive viene quindi reimpostato su 0 e il pacchetto viene scartato.

Se il router B non è raggiungibile, il router A continua a costruire e inviare pacchetti keepalive e il normale traffico. Se i pacchetti keepalive non tornano, il protocollo della linea del tunnel rimane attivo finché il contatore keepalive del tunnel è inferiore al numero di tentativi, che in questo caso è quattro. Se questa condizione non è vera, al successivo tentativo del router A di inviare un pacchetto keepalive al router B, il protocollo di linea viene interrotto.

> **Nota**: nello stato attivo/inattivo, il tunnel non inoltra né elabora alcun traffico di dati. Tuttavia, continua a inviare pacchetti keepalive. Alla ricezione di una risposta keepalive, con la conseguenza che l'endpoint del tunnel è nuovamente raggiungibile, il contatore keepalive del tunnel viene reimpostato su 0 e viene visualizzato il protocollo di linea sul tunnel.

Per verificare che i pacchetti keepalive siano in azione, abilitare **debug tunnel** ed eseguire il **debug**

tunnel keepalive.

Esempi di debug dal router A:

```
debug tunnel keepalive
Tunnel keepalive debugging is on
01:19:16.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=15
01:19:21.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=16
01:19:26.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=17
```

GRE Keepalives e Unicast Reverse Path Forwarding

Unicast RPF (Unicast Reverse Path Forwarding) è una funzione di sicurezza che permette di rilevare ed eliminare il traffico IP oggetto di spoofing con una convalida dell'indirizzo di origine del pacchetto sulla tabella di routing. Quando si esegue RPF unicast in modalità strict (**ip verify unicast source reachable-via rx**), il pacchetto deve essere ricevuto sull'interfaccia che il router utilizzerebbe per inoltrare il pacchetto restituito. Se l'RPF unicast in modalità rigorosa o libera è abilitato sull'interfaccia tunnel del router che riceve i pacchetti keepalive GRE, i pacchetti keepalive vengono scartati dall'RPF dopo la decapsulazione del tunnel, in quanto il percorso all'indirizzo di origine del pacchetto (indirizzo di origine del tunnel del router) non passa attraverso l'interfaccia tunnel. Le perdite di pacchetti RPF possono essere osservate nell'output del **traffico show ip** come segue:

```
Router#show ip traffic | section Drop
Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
0 no route, 156 unicast RPF, 0 forced drop
0 options denied
```

Di conseguenza, l'iniziatore del tunnel keepalive scarta il tunnel a causa della mancanza dei pacchetti keepalive di ritorno. Pertanto, per il corretto funzionamento dei pacchetti keepalive del tunnel GRE, non è necessario configurare il protocollo RPF unicast in modalità rigorosa o libera. Per ulteriori informazioni su RPF unicast, vedere Informazioni su Inoltro percorso inverso unicast.

IPsec e GRE Keepalives

Tunnel GRE con IPsec

I tunnel GRE vengono talvolta combinati con IPsec perché IPsec non supporta pacchetti IP multicast. Per questo motivo, non è possibile eseguire correttamente i protocolli di routing dinamico su una rete VPN IPsec. Poiché i tunnel GRE supportano il multicast IP, è possibile eseguire un protocollo di routing dinamico su un tunnel GRE. I pacchetti unicast IP GRE risultanti possono essere crittografati da IPsec.

IPsec può crittografare i pacchetti GRE in due modi diversi:

- Un modo è quello di usare una mappa crittografica. Quando si usa una mappa crittografica, questa viene applicata alle interfacce fisiche in uscita per i pacchetti del tunnel GRE. In questo caso, la sequenza dei passaggi è la seguente:

Il pacchetto crittografato raggiunge l'interfaccia fisica.Il pacchetto viene decrittografato e inoltrato all'interfaccia del tunnel.Il pacchetto viene decapsulato e quindi inoltrato alla destinazione IP in formato testo non crittografato.

- L'altro modo è usare la protezione del tunnel. Quando si usa la protezione del tunnel, questa è configurata sull'interfaccia del tunnel GRE. Il comando tunnel Protection è disponibile nel software Cisco IOS versione 12.2(13)T. In questo caso, la sequenza dei passaggi è la seguente:

  Il pacchetto crittografato raggiunge l'interfaccia fisica.Il pacchetto viene inoltrato all'interfaccia del tunnel.Il pacchetto viene decapsulato e quindi inoltrato alla destinazione IP in formato testo non crittografato.

Entrambi i metodi specificano che la crittografia IPsec viene eseguita dopo l'aggiunta dell'incapsulamento GRE. Esistono due differenze fondamentali tra quando si utilizza una mappa crittografica e quando si utilizza la protezione del tunnel:

- La mappa crittografica dell'IPsec è collegata all'interfaccia fisica e viene controllata mano a mano che i pacchetti vengono inoltrati all'esterno dell'interfaccia fisica.

  Il tunnel GRE ha già incapsulato il pacchetto in questo punto.
- La protezione del tunnel lega la funzionalità di crittografia al tunnel GRE e viene controllata dopo l'incapsulamento del pacchetto GRE, ma prima della consegna del pacchetto all'interfaccia fisica.

Problemi con i pacchetti keepalive quando si combinano IPsec e GRE

Dati i due modi per aggiungere la crittografia ai tunnel GRE, sono disponibili tre modi diversi per configurare un tunnel GRE crittografato:

1. Il peer A ha la protezione del tunnel configurata sull'interfaccia del tunnel, mentre il peer B ha la mappa crittografica configurata sull'interfaccia fisica.
2. Sul peer A la mappa crittografica è configurata sull'interfaccia fisica, mentre sul peer B la protezione del tunnel è configurata sull'interfaccia del tunnel.
3. La protezione del tunnel di entrambi i peer è configurata sull'interfaccia del tunnel.

La configurazione descritta negli scenari 1 e 2 viene spesso eseguita in una struttura hub e spoke. La protezione del tunnel è configurata sul router hub per ridurre le dimensioni della configurazione e viene utilizzata una mappa crittografica statica su ciascun spoke.

Prendere in considerazione ognuno di questi scenari con i pacchetti keepalive GRE abilitati sul peer B(spoke) e in cui la modalità tunnel viene utilizzata per la crittografia.

Scenario 1

Impostazione:

—

- Il peer A utilizza la protezione del tunnel.
- Il peer B utilizza mappe crittografiche.

- I pacchetti keepalive sono abilitati sul peer B.
- La crittografia IPsec viene eseguita in modalità tunnel.

In questo scenario, poiché i pacchetti keepalive GRE sono configurati sul peer B, gli eventi di sequenza quando viene generato un pacchetto keepalive sono i seguenti:

1. Il peer B genera un pacchetto keepalive che viene incapsulato dal GRE e quindi inoltrato all'interfaccia fisica dove viene criptato e inviato alla destinazione del tunnel, il peer A.

   Pacchetto inviato dal peer B al peer A:

2. Nel peer A, il GRE keepalive viene ricevuto decrittografato:

   decapsulato:

   Quindi, il pacchetto di risposta keepalive GRE interno viene instradato in base all'indirizzo di destinazione, ossia il peer B. Ciò significa che sul peer A il pacchetto viene immediatamente indirizzato indietro dall'interfaccia fisica al peer B. Poiché il peer A usa la protezione del tunnel sull'interfaccia del tunnel, il pacchetto keepalive non è crittografato.

   Pertanto, il pacchetto inviato dal peer A al peer B:

   Nota: keepalive non è crittografato.

3. Il peer B riceve ora una risposta GRE keepalive che non è crittografata sulla sua interfaccia fisica, ma a causa della mappa crittografica configurata sull'interfaccia fisica, si aspetta un pacchetto crittografato e quindi lo scarta.

Pertanto, anche se il peer A risponde ai pacchetti keepalive e il router Peer B riceve le risposte, non le elabora mai e alla fine modifica il protocollo di linea dell'interfaccia del tunnel in stato di inattività.

Risultato:

—

Se i pacchetti keepalive sono abilitati sul peer B, lo stato del tunnel sul peer B diventa attivo/inattivo.

Scenario 2

Impostazione:

—

- Il peer A utilizza mappe crittografiche.
- Il peer B utilizza la protezione del tunnel.

- I pacchetti keepalive sono abilitati sul peer B.
- La crittografia IPsec viene eseguita in modalità tunnel.

In questo scenario, poiché i pacchetti keepalive GRE sono configurati sul peer B, la sequenza di eventi generata da un pacchetto keepalive è la seguente:

1. Il peer B genera un pacchetto keepalive che viene incapsulato dal GRE e quindi criptato dalla protezione del tunnel sull'interfaccia del tunnel e inoltrato all'interfaccia fisica.

   Pacchetto inviato dal peer B al peer A:

2. Nel peer A, il GRE keepalive viene ricevuto decrittografato:

   decapsulato:

   Quindi, il pacchetto di risposta keepalive GRE interno viene instradato in base all'indirizzo di destinazione, ossia il peer B. Ciò significa che sul Peer A, il pacchetto viene immediatamente rimandato indietro dall'interfaccia fisica al Peer B. Poiché il Peer A utilizza mappe crittografiche sull'interfaccia fisica, prima di inoltrarlo, cripta questo pacchetto.

   Pertanto, il pacchetto inviato dal peer A al peer B:

   Nota: la risposta keepalive è crittografata.

3. Il peer B riceve ora una risposta GRE keepalive crittografata, la cui destinazione viene inoltrata all'interfaccia del tunnel dove viene decrittografata:

   Poiché il tipo di protocollo è impostato su 0, il peer B sa che si tratta di una risposta keepalive e la elabora come tale.

Risultato:

—

I pacchetti keepalive abilitati sul peer B determinano correttamente lo stato del tunnel in base alla disponibilità della destinazione del tunnel.

Scenario 3

Impostazione:

—

- Entrambi i peer utilizzano la protezione del tunnel.
- I pacchetti keepalive sono abilitati sul peer B.

- La crittografia IPsec viene eseguita in modalità tunnel.

Questo scenario è simile allo scenario 1 in quanto, quando il peer A riceve il pacchetto keepalive crittografato, lo decapsula e lo decapsula. Tuttavia, quando la risposta viene inoltrata indietro, non viene crittografata in quanto il peer A usa la protezione del tunnel sull'interfaccia del tunnel. Pertanto, il peer B rifiuta la risposta keepalive non crittografata e non la elabora.

Risultato:

—

Se i pacchetti keepalive sono abilitati sul peer B, lo stato del tunnel sul peer B diventa attivo/inattivo.

Soluzione alternativa

In queste situazioni in cui i pacchetti GRE devono essere crittografati, sono possibili tre soluzioni:

1. Usare una mappa crittografica sul Peer A, proteggere il tunnel sul Peer B e abilitare i pacchetti keepalive sul Peer B.

   Poiché questo tipo di configurazione viene utilizzato principalmente nelle configurazioni hub e spoke e poiché in tali configurazioni è più importante che lo spoke sia consapevole della raggiungibilità degli hub, la soluzione è utilizzare una mappa crittografica dinamica sull'hub (Peer A) e la protezione del tunnel sullo spoke (Peer B) e abilitare i pacchetti keepalive GRE sullo spoke. In questo modo, anche se l'interfaccia del tunnel GRE sull'hub rimane attiva, il router adiacente e i percorsi attraverso il tunnel vengono persi e è possibile stabilire il percorso alternativo. Sul router spoke, il fatto che l'interfaccia del tunnel sia scesa può attivarlo per attivare un'interfaccia di connessione e richiamare all'hub (o un altro router all'hub), quindi stabilire una nuova connessione.

2. Utilizzare un metodo diverso da GRE keepalive per determinare la raggiungibilità del peer.

   Se entrambi i router sono configurati con la protezione del tunnel, non è possibile usare i keymap del tunnel GRE in nessuna direzione. In questo caso, l'unica opzione è utilizzare il protocollo di routing o un altro meccanismo, ad esempio Service Assurance Agent, per verificare se il peer è raggiungibile o meno.

3. Usare le mappe crittografiche sul peer A e sul peer B.

   Se entrambi i router sono configurati con mappe crittografiche, i pacchetti keepalive del tunnel possono passare in entrambe le direzioni e le interfacce del tunnel GRE possono essere arrestate in entrambe le direzioni o in entrambe e attivare una connessione di backup. Si tratta dell'opzione più flessibile.

Informazioni correlate

- RFC 1701, GRE (Generic Router Encapsulation)
- RFC 2890, estensioni chiavi e numeri di sequenza per GRE

- Tunnel GRE (Generic Routing Encapsulation) Keepalive
- Frammentazione IP e PMTUD
- Panoramica dei meccanismi keepalive su Cisco IOS
- Supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).