GRE-Tunnel-Keepalives verstehen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, was Generic Routing Encapsulation (GRE) Keepalives sind und wie sie funktionieren.

GRE-Tunnel

Ein GRE-Tunnel ist eine logische Schnittstelle auf einem Cisco Router, über die Passagierpakete in ein Transportprotokoll gekapselt werden können. Es handelt sich um eine Architektur, die darauf ausgelegt ist, die Services bereitzustellen, um ein Punkt-zu-Punkt-Kapselungsschema zu implementieren.

GRE-Tunnel sind vollständig stateless. Das bedeutet, dass jeder Tunnelendpunkt keine Informationen über den Status oder die Verfügbarkeit des entfernten Tunnelendpunkts speichert. Dies hat zur Folge, dass der lokale Tunnel-Endpunkt-Router nicht in der Lage ist, das Leitungsprotokoll der GRE-Tunnelschnittstelle herunterzufahren, wenn das Remote-Ende des Tunnels nicht erreichbar ist. Die Möglichkeit, eine Schnittstelle als ausgefallen zu markieren, wenn das Remote-Ende der Verbindung nicht verfügbar ist, wird verwendet, um Routen (insbesondere statische Routen) in der Routing-Tabelle zu entfernen, die diese Schnittstelle als ausgehende Schnittstelle verwenden. Wenn das Leitungsprotokoll für eine Schnittstelle in "Down" (Heruntergefahren) geändert wird, werden alle statischen Routen, die auf diese Schnittstelle hinweisen, aus der Routing-Tabelle entfernt. Dies ermöglicht die Installation einer alternativen (schwebenden) statischen Route oder eines richtlinienbasierten Routing (Policy Based Routing, PBR), um einen alternativen Next-Hop oder eine alternative Schnittstelle auszuwählen.

Normalerweise wird eine GRE-Tunnelschnittstelle sofort nach ihrer Konfiguration aktiviert und bleibt aktiv, solange eine gültige Tunnelquellenadresse oder Schnittstelle verfügbar ist. Die IP-Adresse des Tunnelziels muss ebenfalls routbar sein. Dies gilt auch dann, wenn die andere Seite des Tunnels nicht konfiguriert wurde. Dies bedeutet, dass eine statische Route oder PBR-

Weiterleitung von Paketen über die GRE-Tunnelschnittstelle in Kraft bleibt, obwohl die GRE-Tunnelpakete das andere Ende des Tunnels nicht erreichen.

Vor der Implementierung von GRE-Keepalives gab es nur Möglichkeiten, lokale Probleme auf dem Router zu ermitteln, nicht aber Probleme im dazwischen liegenden Netzwerk. Dies ist beispielsweise der Fall, wenn GRE-getunnelte Pakete erfolgreich weitergeleitet werden, aber verloren gehen, bevor sie das andere Ende des Tunnels erreichen. Solche Szenarien würden dazu führen, dass Datenpakete, die den GRE-Tunnel durchlaufen, "schwarz durchlöchert" werden, obwohl eine alternative Route, die PBR verwendet, oder eine variable statische Route über eine andere Schnittstelle verfügbar war. Keepalives an der GRE-Tunnelschnittstelle werden verwendet, um dieses Problem auf die gleiche Weise zu lösen wie Keepalives an physischen Schnittstellen.

> **Hinweis**: GRE-Keepalives werden unter keinen Umständen zusammen mit IPsec-Tunnelschutz unterstützt. In diesem Dokument wird dieses Problem behandelt.

Funktionsweise von Tunnel Keepalive

Der GRE-Tunnel-Keepalive-Mechanismus ähnelt PPP-Keepalives, da er es einer Seite ermöglicht, Keepalive-Pakete von und an einen Remote-Router zu senden und zu empfangen, auch wenn der Remote-Router keine GRE-Keepalives unterstützt. Da GRE ein Paket-Tunneling-Mechanismus für das Tunneling von IP innerhalb von IP ist, kann ein GRE-IP-Tunnelpaket in einem anderen GRE-IP-Tunnelpaket erstellt werden. Bei GRE-Keepalives erstellt der Absender das Keepalive-Antwortpaket im ursprünglichen Keepalive-Anforderungspaket vorab, sodass das Remote-Ende nur die standardmäßige GRE-Entkapselung des äußeren GRE-IP-Headers durchführen muss und das innere IP-GRE-Paket dann an den Absender zurücksetzt. Diese Pakete veranschaulichen die IP-Tunneling-Konzepte, wobei GRE das Kapselungsprotokoll und IP das Transportprotokoll ist. Das Passagierprotokoll ist ebenfalls IP (obwohl es auch ein anderes Protokoll wie Decnet, Internetwork Packet Exchange (IPX) oder Appletalk sein kann).

Normales Paket:

IP-Header	TCP-Header	Telnet

Getunneltes Paket:

GRE	IP-Header	GRE	IP-Header	TCP-Header	Telnet

- IP ist das Transportprotokoll.
- GRE ist das Kapselprotokoll.
- IP ist das Passagierprotokoll.

Das folgende Beispiel zeigt ein Keepalive-Paket, das von Router A stammt und für Router B bestimmt ist. Die Keepalive-Antwort, die Router B an Router A zurückgibt, befindet sich bereits im inneren IP-Header. Router B entkapselt einfach das Keepalive-Paket und sendet es zurück an die physische Schnittstelle (S2). Er verarbeitet das GRE-Keepalive-Paket genau wie jedes andere GRE-IP-Datenpaket.

GRE-Keepalive:

GRE IP-Header		GRE	IP-Header		GRE
Quelle A	Ziel B	PT = IP	Quelle B	Ziel A	PT = 0

Dieser Mechanismus veranlasst die Keepalive-Antwort, die physische Schnittstelle und nicht die Tunnelschnittstelle weiterzuleiten. Das bedeutet, dass das GRE-Keepalive-Antwortpaket nicht durch Ausgabefunktionen an der Tunnelschnittstelle beeinflusst wird, z. B. Tunnelschutz, QoS, Virtual Routing and Forwarding (VRF) usw.

> **Hinweis**: Wenn eine eingehende Zugriffskontrollliste (ACL) auf der GRE-Tunnelschnittstelle konfiguriert ist, muss das vom gegenüberliegenden Gerät gesendete GRE-Tunnel-Keepalive-Paket zugelassen werden. Andernfalls wird der GRE-Tunnel des anderen Geräts ausfallen. (`access-list <Nummer> permit gre host <tunnel-source> host <tunnel-destination>`)

Ein weiteres Attribut von GRE-Tunnelkeepalives ist, dass die Keepalive-Timer auf jeder Seite unabhängig sind und nicht übereinstimmen müssen, ähnlich wie PPP-Keepalives.

> **Tipp:** Das Problem bei der Konfiguration von Keepalives nur auf einer Seite des Tunnels besteht darin, dass nur der Router mit konfiguriertem Keepalives seine Tunnelschnittstelle als ausgefallen markiert, wenn der Keepalive-Timer abläuft. Die GRE-Tunnelschnittstelle auf der anderen Seite, auf der keine Keepalives konfiguriert sind, bleibt auch dann aktiv, wenn die andere Seite des Tunnels ausgefallen ist. Der Tunnel kann zu einem schwarzen Loch für Pakete werden, die von der Seite in den Tunnel geleitet werden und für die keine Keepalives konfiguriert wurden.

> **Tipp:** In einem großen Hub-and-Spoke-GRE-Tunnelnetzwerk kann es sinnvoll sein, GRE-Keepalives nur auf der Spoke-Seite und nicht auf der Hub-Seite zu konfigurieren. Dies liegt daran, dass es für die Spoke-Topologie oft wichtiger ist, festzustellen, dass der Hub nicht erreichbar ist, und daher auf einen Backup-Pfad umzuschalten (z. B. Einwahl-Backup).

GRE-Tunnel-Keepalive

Mit der Cisco IOS® Software-Version 12.2(8)T ist es möglich, Keepalives auf einer Punkt-zu-Punkt-GRE-Tunnelschnittstelle zu konfigurieren. Mit dieser Änderung wird die Tunnelschnittstelle dynamisch heruntergefahren, wenn die Keepalives für eine bestimmte Zeit fehlschlagen.

Weitere Informationen zur Funktionsweise anderer Formen von Keepalives finden Sie unter Übersicht über die Keepalive-Mechanismen in Cisco IOS.

> **Hinweis**: GRE-Tunnel-Keepalives werden nur auf Punkt-zu-Punkt-GRE-Tunneln unterstützt. Tunnel-Keepalives können für mGRE-Tunnel (Multipoint GRE) konfiguriert werden, haben jedoch keine Auswirkungen.

> **Hinweis**: Tunnel-Keepalives können im Allgemeinen nicht funktionieren, wenn VRFs an der Tunnelschnittstelle verwendet werden und fVRF ("tunnel vrf ...') und iVRF ("ip vrf forwarding ...' an der Tunnelschnittstelle) nicht übereinstimmen. Dies ist für den Tunnelendpunkt, der die Keepalive-Nachricht an den Anforderer zurückgibt, von entscheidender Bedeutung. Wenn die Keepalive-Anfrage eingeht, wird sie in der fVRF-Instanz empfangen und entkapselt. Daraus ergibt sich die vorgefertigte Keepalive-Antwort, die dann zurück an den

Absender weitergeleitet werden muss. Die Weiterleitung erfolgt JEDOCH im Kontext der iVRF-Instanz an der Tunnelschnittstelle. Wenn also iVRF und fVRF nicht übereinstimmen, wird das Keepalive-Antwortpaket nicht an den Absender zurückgeleitet. Dies gilt auch dann, wenn Sie iVRF und/oder fVRF durch "global" ersetzen.

Diese Ausgabe zeigt die Befehle, die Sie verwenden, um Keepalives in GRE-Tunneln zu konfigurieren.

```
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.
```

Um besser zu verstehen, wie der Tunnel-Keepalive-Mechanismus funktioniert, sollten Sie sich folgendes Beispiel für die Tunneltopologie und -konfiguration ansehen:

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 diesem Szenario führt Router A die folgenden Schritte aus:

1. Konstruiert den inneren IP-Header alle fünf Sekunden, wobei:

   Die Quelle wird als lokales Tunnelziel festgelegt, das 192.168.1.2 lautet.Das Ziel wird als lokale Tunnelquelle festgelegt, die 192.168.1.1 lautet.

   und ein GRE-Header wird mit einem Protokolltyp (PT) von 0 hinzugefügt

   Paket von Router A generiert, aber nicht gesendet:

2. Sendet das Paket aus seiner Tunnelschnittstelle, was zur Kapselung des Pakets mit dem äußeren IP-Header führt, wobei:

   Die Quelle wird als lokale Tunnelquelle festgelegt, die 192.168.1.1 lautet.Das Ziel wird als lokales Tunnelziel festgelegt, das 192.168.1.2 lautet.

   und ein GRE-Header wird mit PT = IP hinzugefügt.

   Paket von Router A an Router B gesendet:

3. Erhöht den Tunnel-Keepalive-Zähler um eins.

4. Wenn davon ausgegangen wird, dass es möglich ist, den Endpunkt des Tunnels am anderen Ende zu erreichen, und das Tunnelleitungsprotokoll aus anderen Gründen nicht ausgefallen ist, erreicht das Paket Router B. Dieser wird dann mit Tunnel 0 abgeglichen, entkapselt und an die Ziel-IP-Adresse weitergeleitet, die die Tunnel-Quell-IP-Adresse auf Router A ist.

   Von Router B an Router A gesendet:

5. Bei Ankunft auf Router A wird das Paket entkapselt, und die Prüfung des PT ergibt 0. Dies bedeutet, dass es sich um ein Keepalive-Paket handelt. Der Tunnel-Keepalive-Zähler wird dann auf 0 zurückgesetzt, und das Paket wird verworfen.

Wenn Router B nicht erreichbar ist, erstellt und sendet Router A weiterhin Keepalive-Pakete sowie normalen Datenverkehr. Wenn die Keepalives nicht zurückkommen, bleibt das Tunnelleitungsprotokoll so lange aktiv, wie der Tunnel-Keepalive-Zähler kleiner ist als die Anzahl der Wiederholungsversuche, die in diesem Fall vier beträgt. Wenn diese Bedingung nicht zutrifft, wird das Leitungsprotokoll deaktiviert, wenn Router A das nächste Mal versucht, einen Keepalive an Router B zu senden.

> **Hinweis**: Im Status "Auf/Ab" leitet und verarbeitet der Tunnel keinen Datenverkehr weiter. Es werden jedoch weiterhin Keepalive-Pakete gesendet. Beim Empfang einer Keepalive-Antwort mit der Implikation, dass der Tunnel-Endpunkt wieder erreichbar ist, wird der Tunnel-Keepalive-Zähler auf 0 zurückgesetzt, und das Leitungsprotokoll auf dem Tunnel wird aktiviert.

Um Keepalives in Aktion zu sehen, aktivieren Sie **debug tunnel** und **debug tunnel keepalive**.

Beispiel für Debugging von 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-Keepalive und Unicast Reverse Path Forwarding

Unicast RPF (Unicast Reverse Path Forwarding) ist eine Sicherheitsfunktion, mit der gefälschter IP-Datenverkehr erkannt und mithilfe einer Validierung der Paketquellenadresse anhand der Routing-Tabelle gelöscht wird. Wenn Unicast-RPF im strikten Modus ausgeführt wird (**ip verify unicast source reachable-via rx)**, muss das Paket über die Schnittstelle empfangen werden, die der Router zum Weiterleiten des Rückgabepakets verwenden würde. Wenn Unicast-RPF im strikten Modus oder im losen Modus auf der Tunnelschnittstelle des Routers aktiviert ist, der die GRE-Keepalive-Pakete empfängt, werden die Keepalives-Pakete nach der Tunnelentkapselung von RPF verworfen, da die Route zur Quelladresse des Pakets (tunneleigene Adresse des Routers) nicht durch die Tunnelschnittstelle verläuft. RPF-Paketverluste können in der Ausgabe von **show ip traffic** wie folgt beobachtet werden:

```
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
```

Der Initiator des Tunnel-Keepalives stürzt den Tunnel aufgrund von fehlenden Keepalives-Rückgabepaketen ab. Unicast-RPF darf daher nicht im strikten oder losen Modus konfiguriert werden, damit GRE-Tunnel-Keepalives funktionieren. Weitere Informationen zu Unicast RPF finden Sie unter Understanding Unicast Reverse Path Forwarding.

IPsec- und GRE-Keepalive

GRE-Tunnel mit IPsec

GRE-Tunnel werden manchmal mit IPsec kombiniert, da IPsec IP-Multicast-Pakete nicht unterstützt. Daher können dynamische Routing-Protokolle nicht erfolgreich über ein IPsec-VPN-Netzwerk ausgeführt werden. Da GRE-Tunnel IP-Multicast unterstützen, kann ein dynamisches Routing-Protokoll über einen GRE-Tunnel ausgeführt werden. Die resultierenden GRE-IP-Unicast-Pakete können mit IPsec verschlüsselt werden.

Es gibt zwei verschiedene Möglichkeiten, wie IPsec GRE-Pakete verschlüsseln kann:

- Eine Möglichkeit ist die Verwendung einer Crypto Map. Wenn eine Crypto Map verwendet wird, wird diese auf die ausgehenden physischen Schnittstellen für die GRE-Tunnelpakete angewendet. In diesem Fall ist die Reihenfolge der Schritte wie folgt:

Das verschlüsselte Paket erreicht die physische Schnittstelle.Das Paket wird entschlüsselt und an die Tunnelschnittstelle weitergeleitet.Das Paket wird entkapselt und dann im Klartext an das IP-Ziel weitergeleitet.

- Die andere Möglichkeit besteht darin, den Tunnelschutz zu verwenden. Wenn der Tunnelschutz verwendet wird, wird er an der GRE-Tunnelschnittstelle konfiguriert. Der Befehl tunnel protection ist ab Version 12.2(13)T der Cisco IOS-Software verfügbar. In diesem Fall ist die Reihenfolge der Schritte wie folgt:

  Verschlüsseltes Paket erreicht physische Schnittstelle.Paket wird an die Tunnelschnittstelle weitergeleitet.Das Paket wird entschlüsselt, entkapselt und dann im Klartext an das IP-Ziel weitergeleitet.

Beide Methoden geben an, dass die IPsec-Verschlüsselung nach dem Hinzufügen der GRE-Kapselung ausgeführt wird. Wenn Sie eine Crypto Map verwenden, und wenn Sie den Tunnelschutz verwenden, bestehen zwei Hauptunterschiede:

- Die IPsec-Kryptografiezuordnung ist an die physische Schnittstelle gebunden und wird geprüft, während Pakete von der physischen Schnittstelle weitergeleitet werden.

  Der GRE-Tunnel hat das Paket bis zu diesem Punkt bereits GRE gekapselt.
- Der Tunnelschutz verknüpft die Verschlüsselungsfunktionalität mit dem GRE-Tunnel und wird geprüft, nachdem das Paket GRE-gekapselt wurde, aber bevor das Paket an die physische Schnittstelle übergeben wird.

Probleme mit Keepalives bei der Kombination von IPsec und GRE

Wenn GRE-Tunnel verschlüsselt werden sollen, gibt es drei Möglichkeiten, einen verschlüsselten GRE-Tunnel einzurichten:

1. Für Peer A ist der Tunnelschutz auf der Tunnelschnittstelle konfiguriert, während für Peer B die Crypto Map auf der physischen Schnittstelle konfiguriert ist.
2. Peer A verfügt über eine auf der physischen Schnittstelle konfigurierte Crypto Map, während Peer B über einen auf der Tunnelschnittstelle konfigurierten Tunnelschutz verfügt.
3. Für beide Peers ist auf der Tunnelschnittstelle ein Tunnelschutz konfiguriert.

Die in Szenario 1 und 2 beschriebene Konfiguration erfolgt häufig in einem Hub-and-Spoke-Design. Der Tunnelschutz wird auf dem Hub-Router konfiguriert, um die Größe der Konfiguration zu reduzieren. Außerdem wird eine statische Crypto Map für jede Spoke verwendet.

Betrachten Sie jedes dieser Szenarien mit GRE-Keepalives, die auf Peer B(Spoke) aktiviert sind, und bei denen der Tunnelmodus für die Verschlüsselung verwendet wird.

Szenario 1

Einstellung:

- Peer A verwendet den Tunnelschutz.
- Peer B verwendet Crypto Maps.

- Keepalives sind auf Peer B aktiviert.
- Die IPsec-Verschlüsselung erfolgt im Tunnelmodus.

Da in diesem Szenario die GRE-Keepalives für Peer B konfiguriert sind, werden beim Generieren eines Keepalive folgende Sequenzereignisse generiert:

1. Peer B generiert ein Keepalive-Paket, das GRE-gekapselt und dann an die physische Schnittstelle weitergeleitet wird, wo es verschlüsselt wird und an das Tunnelziel, Peer A, gesendet wird.

   Paket von Peer B an Peer A gesendet:

2. Bei Peer A wird der GRE-Keepalive entschlüsselt empfangen:

   entkapselt:

   Anschließend wird das interne GRE-Keepalive-Antwortpaket basierend auf seiner Zieladresse geroutet, die Peer B lautet. Das heißt, auf Peer A wird das Paket sofort zurück von der physischen Schnittstelle zu Peer B geroutet. Da Peer A Tunnelschutz auf der Tunnelschnittstelle verwendet, wird das Keepalive-Paket nicht verschlüsselt.

   Daher wird ein Paket von Peer A an Peer B gesendet:

   Hinweis: Der Keepalive ist nicht verschlüsselt.

3. Peer B erhält nun eine GRE-Keepalive-Antwort, die nicht auf seiner physischen Schnittstelle verschlüsselt ist. Aufgrund der auf der physischen Schnittstelle konfigurierten Crypto Map erwartet er jedoch ein verschlüsseltes Paket und verwirft es daher.

Obwohl also Peer A auf die Keepailves reagiert und Router Peer B die Antworten empfängt, werden diese niemals verarbeitet, und schließlich wird das Leitungsprotokoll der Tunnelschnittstelle in den deaktivierten Zustand geändert.

Ergebnis:

Keepalives, die für Peer B aktiviert sind, bewirken, dass der Tunnelstatus für Peer B in "up/down" (aktiv/inaktiv) geändert wird.

Szenario 2

Einstellung:

- Peer A verwendet Crypto Maps.

- Peer B verwendet den Tunnelschutz.
- Keepalives sind auf Peer B aktiviert.
- Die IPsec-Verschlüsselung erfolgt im Tunnelmodus.

Da in diesem Szenario die GRE-Keepalives auf Peer B konfiguriert sind, werden beim Generieren eines Keepalive folgende Sequenzereignisse generiert:

1. Peer B generiert ein Keepalive-Paket, das GRE-gekapselt und dann durch den Tunnelschutz an der Tunnelschnittstelle verschlüsselt und dann an die physische Schnittstelle weitergeleitet wird.

   Paket von Peer B an Peer A gesendet:

2. Bei Peer A wird der GRE-Keepalive entschlüsselt empfangen:

   entkapselt:

   Anschließend wird das interne GRE-Keepalive-Antwortpaket basierend auf seiner Zieladresse geroutet, die Peer B lautet. Das bedeutet, dass auf Peer A das Paket sofort von der physischen Schnittstelle zurück zu Peer B geroutet wird. Da Peer A Crypto-Maps auf der physischen Schnittstelle verwendet, verschlüsselt es zuerst dieses Paket, bevor es es weitergeleitet wird.

   Daher wird ein Paket von Peer A an Peer B gesendet:

   Hinweis: Die Keepalive-Antwort ist verschlüsselt.

3. Peer B erhält nun eine verschlüsselte GRE-Keepalive-Antwort, deren Ziel an die Tunnelschnittstelle weitergeleitet wird, wo sie entschlüsselt wird:

   Da der Prototyp auf 0 festgelegt ist, weiß Peer B, dass es sich um eine Keepalive-Antwort handelt, und verarbeitet sie als solche.

Ergebnis:

Mit den auf Peer B aktivierten Keepalives wird anhand der Verfügbarkeit des Tunnelziels erfolgreich bestimmt, welcher Tunnelzustand möglich ist.

Szenario 3

Einstellung:

- Beide Peers verwenden den Tunnelschutz.
- Keepalives sind auf Peer B aktiviert.
- Die IPsec-Verschlüsselung erfolgt im Tunnelmodus.

Dieses Szenario ähnelt Szenario 1 insofern, als Peer A den verschlüsselten Keepalive entschlüsselt und entkapselt. Wenn die Antwort jedoch wieder nach außen weitergeleitet wird, ist sie nicht verschlüsselt, da Peer A den Tunnelschutz an der Tunnelschnittstelle verwendet. Daher verwirft Peer B die unverschlüsselte Keepalive-Antwort und verarbeitet sie nicht.

Ergebnis:

Keepalives, die für Peer B aktiviert sind, bewirken, dass der Tunnelstatus für Peer B in "up/down" (aktiv/inaktiv) geändert wird.

Problemumgehung

In solchen Situationen, in denen die GRE-Pakete verschlüsselt werden müssen, gibt es drei mögliche Lösungen:

1. Verwenden Sie eine Crypto-Map für Peer A, Tunnelschutz für Peer B und aktivieren Sie Keepalives für Peer B.

   Da diese Art der Konfiguration hauptsächlich in Hub-and-Spoke-Konfigurationen verwendet wird und es in solchen Konfigurationen wichtiger ist, dass die Spoke die Erreichbarkeit der Hubs erkennt, besteht die Lösung darin, eine dynamische Crypto Map auf dem Hub (Peer A) und einen Tunnelschutz auf der Spoke (Peer B) zu verwenden und GRE-Keepalives auf der Spoke zu aktivieren. Auf diese Weise bleibt die GRE-Tunnelschnittstelle am Hub zwar aktiv, der Routing-Nachbar und die Routen durch den Tunnel gehen jedoch verloren, und es kann eine alternative Route eingerichtet werden. Wenn die Tunnelschnittstelle ausgefallen ist, kann dies zur Aktivierung einer Dialer-Schnittstelle und zum Rückruf beim Hub (oder einem anderen Router am Hub) sowie zur Herstellung einer neuen Verbindung führen.

2. Verwenden Sie andere als GRE-Keepalives, um die Peer-Erreichbarkeit zu ermitteln.

   Wenn beide Router mit Tunnelschutz konfiguriert sind, können GRE-Tunnel-Keeplives in beiden Richtungen nicht verwendet werden. In diesem Fall besteht die einzige Option darin, das Routing-Protokoll oder andere Mechanismen wie den Service Assurance Agent zu verwenden, um festzustellen, ob der Peer erreichbar ist.

3. Verwenden Sie Crypto Maps für Peer A und Peer B.

   Wenn beide Router mit Crypto Maps konfiguriert sind, können die Tunnel-Keepalives in beide Richtungen passieren, und die GRE-Tunnelschnittstellen können in eine oder beide Richtungen heruntergefahren werden und eine Backup-Verbindung auslösen. Dies ist die flexibelste Option.

Zugehörige Informationen

- RFC 1701, Generic Router Encapsulation (GRE)
- RFC 2890, Key and Sequence Number Extensions to GRE
- Generic Routing Encapsulation (GRE) Tunnel Keepalive
- IP-Fragmentierung und PMTUD
- Überblick über die Keepalive-Mechanismen in Cisco IOS
- Technischer Support – Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.