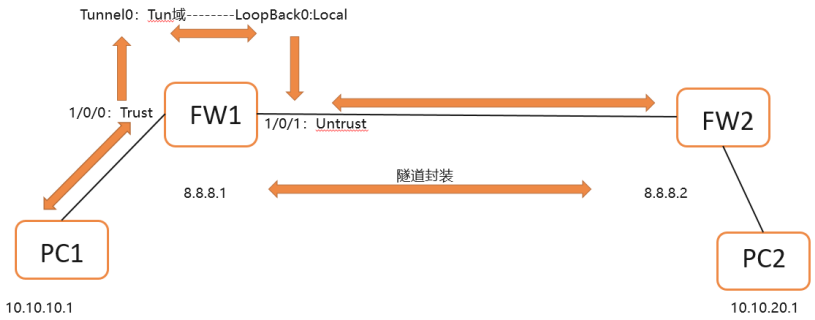
GRE的KeepLive中的会话

GRE VPN　孔梦龙　2022-04-30 发表

组网及说明



两个PC如图，隧道的封装地址如图，各接口的安全域如图

假设只从10.10.10.1　ping　10.10.20.1

此时的安全策略配置：

```
Security-policy ip

 rule 0 name 00
  action pass
  source-zone trust
  source-zone local
  destination-zone tun
  destination-zone untrust
```

```
#
interface Tunnel0 mode gre
 ip address 10.10.12.1 255.255.255.0
 source LoopBack0
 destination 8.8.8.2
#
```

```
#
interface LoopBack0
 ip address 8.8.8.1 255.255.255.0
#
```

问题描述

背景测试一：

此时10.10.10.1　ping　10.10.20.1 的会话

内层的会话：源域是trust，目的接口是tunnel口的Tun域

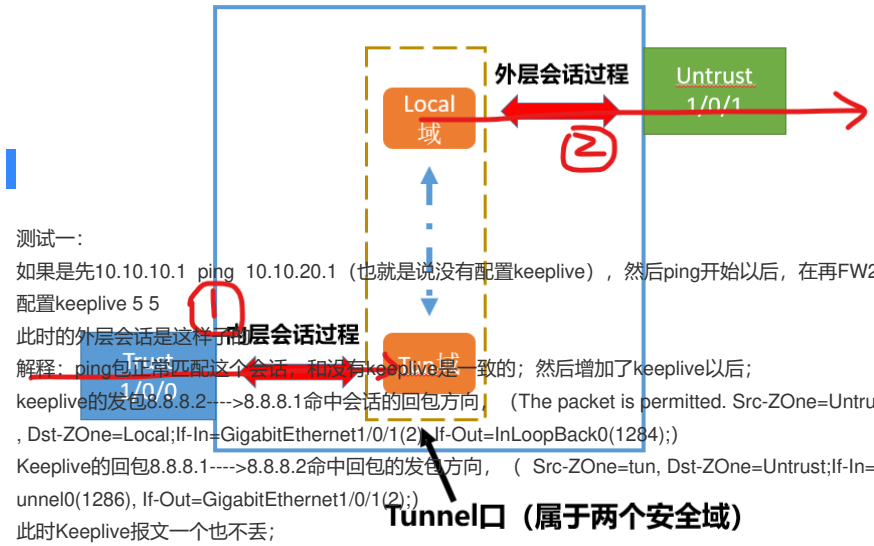
```
<H3C>dis session table ipv4 verbose
Slot 1:
Initiator:
  Source      IP/port: 10.10.10.1/154
  Destination IP/port: 10.10.20.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/0
  Source security zone: Trust
Responder:
  Source      IP/port: 10.10.20.1/154
  Destination IP/port: 10.10.10.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Tunnel0
  Source security zone: tun
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: 00
Start time: 2022-04-29 20:07:29  TTL: 22s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes
```

外层GRE的会话：

发包的源接口是tunnel 口，但是安全域用的是Local（原本应该是Tun域的）；目的接口是出公网的接口Untrust

```
Initiator:
  Source      IP/port: 8.8.8.1/0
  Destination IP/port: 8.8.8.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: Tunnel0
  Source security zone: Local
Responder:
  Source      IP/port: 8.8.8.2/0
  Destination IP/port: 8.8.8.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Untrust
State: RAWIP_READY
Application: OTHER
Rule ID: 0
Rule name: 00
Start time: 2022-04-29 20:07:29  TTL: 52s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes
```

总结ping过程的会话过程理解如下图，分为两段；段一内层，段二外层



测试一：

如果是先10.10.10.1 ping 10.10.20.1（也就是说没有配置keeplive），然后ping开始以后，在再FW2配置keeplive 5 5

此时的外层会话是这样的

解释：ping包正常匹配这个会话，和没有keeplive是一致的；然后增加了keeplive以后；

keeplive的发包8.8.8.2---->8.8.8.1命中会话的回包方向，（The packet is permitted. Src-ZOne=Untrust, Dst-ZOne=Local;If-In=GigabitEthernet1/0/1(2), If-Out=InLoopBack0(1284);）

Keeplive的回包8.8.8.1---->8.8.8.2命中回包的发包方向，（Src-ZOne=tun, Dst-ZOne=Untrust;If-In=Tunnel0(1286), If-Out=GigabitEthernet1/0/1(2);）

此时Keeplive报文一个也不丢；

```
<H3C>dis session table ipv4 verbose
Slot 1:
Initiator:
  Source      IP/port: 8.8.8.1/0
  Destination IP/port: 8.8.8.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: Tunnel0
  Source security zone: Local
Responder:
  Source      IP/port: 8.8.8.2/0
  Destination IP/port: 8.8.8.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Untrust
State: RAWIP_READY
Application: OTHER
Rule ID: 0
Rule name: 00
Start time: 2022-04-29 23:23:55  TTL: 52s
Initiator->Responder:          278 packets      27420 bytes
Responder->Initiator:          278 packets      28164 bytes
```

```
rule 1 name 11
<H3C>dis session table ipv4 verbose
Slot 1:
Initiator:
  Source      IP/port: 8.8.8.1/0
  Destination IP/port: 8.8.8.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: Tunnel0
  Source security zone: Local
Responder:
  Source      IP/port: 8.8.8.2/0
  Destination IP/port: 8.8.8.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Untrust
State: RAWIP_READY
Application: OTHER
Rule ID: 0
Rule name: 00
Start time: 2022-04-29 23:23:55  TTL: 52s
Initiator->Responder:          278 packets      27420 bytes
Responder->Initiator:          278 packets      28164 bytes
```

385 95.974504	8.8.8.1	8.8.8.2	GRE	62	0x009e (158),0x009d (157)
386 95.974884	8.8.8.1	8.8.8.2	GRE	38	0x009d (157)
387 96.153593	10.10.10.1	10.10.20.1	ICMP	122	0x009d (157),0x009d (157)
388 96.156773	10.10.20.1	10.10.10.1	ICMP	122	0x009f (159),0x009d (157)
390 96.361673	10.10.10.1	10.10.20.1	ICMP	122	0x009e (158),0x009e (158)
391 96.364181	10.10.20.1	10.10.10.1	ICMP	122	0x00a0 (160),0x009e (158)

```
Frame 711: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: 9a:8f:d5:e7:05:05 (9a:8f:d5:e7:05:05), Dst: 9a:8f:8d:a9:03:06 (9a:8f:8d:a9:03:06)
Internet Protocol Version 4, Src: 8.8.8.2, Dst: 8.8.8.1
Generic Routing Encapsulation (IP)
Internet Protocol Version 4, Src: 8.8.8.1, Dst: 8.8.8.2
Generic Routing Encapsulation (Possible GRE keepalive packet)
```

不涉及

测试二：

没ping之前的会话：

首先FW收到keeplive的第一个报文，然后回包被丢：

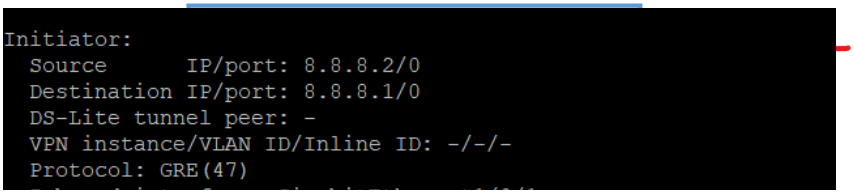
```
Responder:
  Source       IP/port: 8.8.8.1/0
  Destination  IP/port: 8.8.8.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: Tunnel0
<H3C>*Apr 29 23:49:30:004 2022 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = GigabitEthernet1/0/1
version = 4, headlen = 20, tos = 192
pktlen = 48, pktid = 2, offset = 0, ttl = 254, protocol = 47
checksum = 39882, s = 8.8.8.2, d = 8.8.8.1
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/1.
Payload: 00 00 08 00 45 C0 00 18 00 01 00 00 FF 2F 9A E3 08 08 08 01


*Apr 29 23:49:30:004 2022 H3C IPFW/7/IPFW_PACKET: -Context=1;
Delivering, interface = GigabitEthernet1/0/1
version = 4, headlen = 20, tos = 192
pktlen = 48, pktid = 2, offset = 0, ttl = 254, protocol = 47
checksum = 39882, s = 8.8.8.2, d = 8.8.8.1
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Forwarding IP packet to upper layer.
Payload: 00 00 08 00 45 C0 00 18 00 01 00 00 FF 2F 9A E3 08 08 08 01
```

```
  Protocol: GRE(47)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Untrust
Responder:
  Source       IP/port: 8.8.8.1/0
  Destination  IP/port: 8.8.8.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: Tunnel0
  Source security zone: tun
State: RAWIP_READY
Application: OTHER
Rule ID: 1
<H3C>dis session table ipv4 verbose
Slot 1:
Initiator:
  Source       IP/port: 8.8.8.2/0
  Destination  IP/port: 8.8.8.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Untrust
Responder:
  Source       IP/port: 8.8.8.1/0
  Destination  IP/port: 8.8.8.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: GRE(47)
  Inbound interface: Tunnel0
  Source security zone: tun
State: RAWIP_READY
Application: OTHER
Rule ID: 1
Rule name: 11
Start time: 2022-04-29 23:49:30  TTL: 58s
Initiator->Responder:            31 packets        1488 bytes
Responder->Initiator:            30 packets         720 bytes
```

然后会话：（此时已经刷新了接口，参考下图和背景测试一、只丢了一个包）

此时再开始ping，ping的外层会话也走了keeplive的会话，不刷新；（按道理说ping单独发包时候，8.8.8.1到8.2，接口是Tunnel，安全域是Local，但是此时也匹配上了）


Initiator:
Source IP/port: 8.8.8.2/0
Destination IP/port: 8.8.8.1/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: GRE(47)