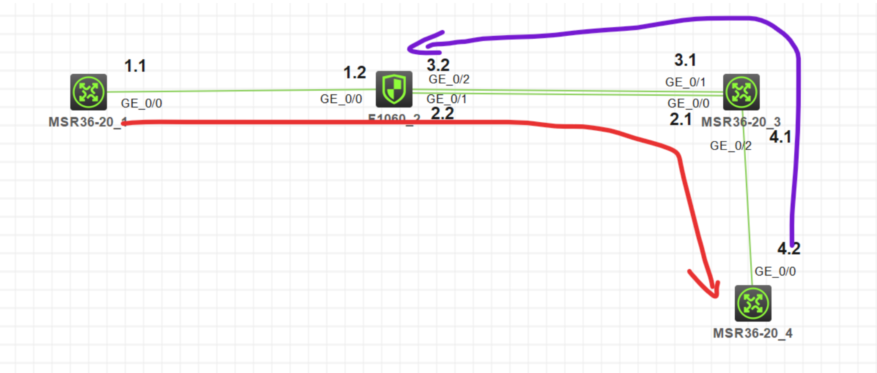
防火墙V7来回路径不一致时候的正常通信

域间策略/安全域 **孔梦龙** 2021-12-08 发表

组网及说明



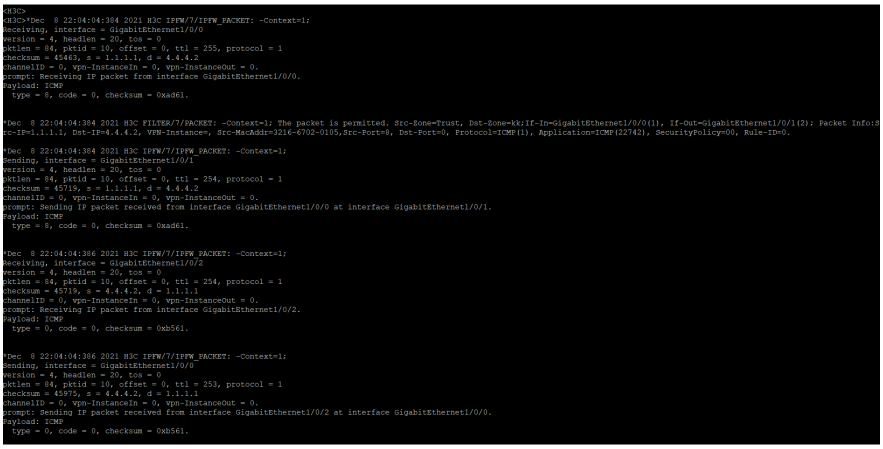
如上图组网

配置步骤

1.1 ping 4.2

纯靠明细路由控制报文的走向，去程走防火墙的0/1口到RT3的0/0口，回程走RT3到防火墙的0/2

此时在防火墙上全通策略，不开启宽松模式，正常通，此时的debug和会话：



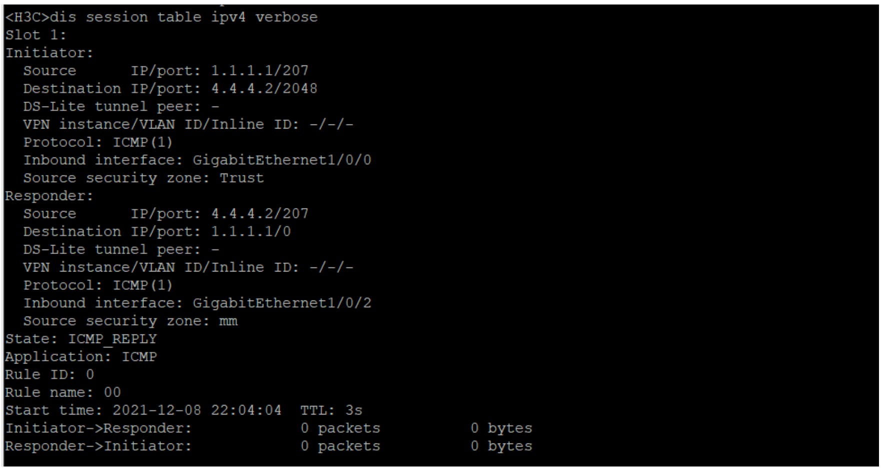
```
<H3C>
<H3C>*Dec  8 22:04:04:384 2021 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 10, offset = 0, ttl = 255, protocol = 1
checksum = 45463, s = 1.1.1.1, d = 4.4.4.2
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/0.
Payload: ICMP
  type = 8, code = 0, checksum = 0xad61.


*Dec  8 22:04:04:384 2021 H3C FILTER/7/PACKET: -Context=1; The packet is permitted. Src-Zone=Trust, Dst-Zone=kk;If-In=GigabitEthernet1/0/0(1), If-Out=GigabitEthernet1/0/1(2); Packet Info:S
rc-IP=1.1.1.1, Dst-IP=4.4.4.2, VPN-Instance=, Src-MacAddr=3216-6702-0105,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), SecurityPolicy=00, Rule-ID=0.

*Dec  8 22:04:04:384 2021 H3C IPFW/7/IPFW_PACKET: -Context=1;
Sending, interface = GigabitEthernet1/0/1
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 10, offset = 0, ttl = 254, protocol = 1
checksum = 45719, s = 1.1.1.1, d = 4.4.4.2
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet1/0/0 at interface GigabitEthernet1/0/1.
Payload: ICMP
  type = 8, code = 0, checksum = 0xad61.


*Dec  8 22:04:04:386 2021 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = GigabitEthernet1/0/2
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 10, offset = 0, ttl = 254, protocol = 1
checksum = 45719, s = 4.4.4.2, d = 1.1.1.1
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/2.
Payload: ICMP
  type = 0, code = 0, checksum = 0xb561.


*Dec  8 22:04:04:386 2021 H3C IPFW/7/IPFW_PACKET: -Context=1;
Sending, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 10, offset = 0, ttl = 253, protocol = 1
checksum = 45975, s = 4.4.4.2, d = 1.1.1.1
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet1/0/2 at interface GigabitEthernet1/0/0.
Payload: ICMP
  type = 0, code = 0, checksum = 0xb561.
```



```
<H3C>dis session table ipv4 verbose
Slot 1:
Initiator:
  Source      IP/port: 1.1.1.1/207
  Destination IP/port: 4.4.4.2/2048
  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: 4.4.4.2/207
  Destination IP/port: 1.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: mm
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: 00
Start time: 2021-12-08 22:04:04  TTL: 3s
Initiator->Responder:            0 packets           0 bytes
Responder->Initiator:            0 packets           0 bytes
```

配置关键点

（1）报文正向和回包不上同一个接口，回包刷新了会话接口成0/2口

会话不关心接口，这样的话只要，正常情况下放通去向的安全测策略，来回路径不一致的，还要放通反向策略，不开启宽松模式情况下就可以正常。

（2）测试验证，不放通反向策略，开启宽松模式的时候，也是正常的。