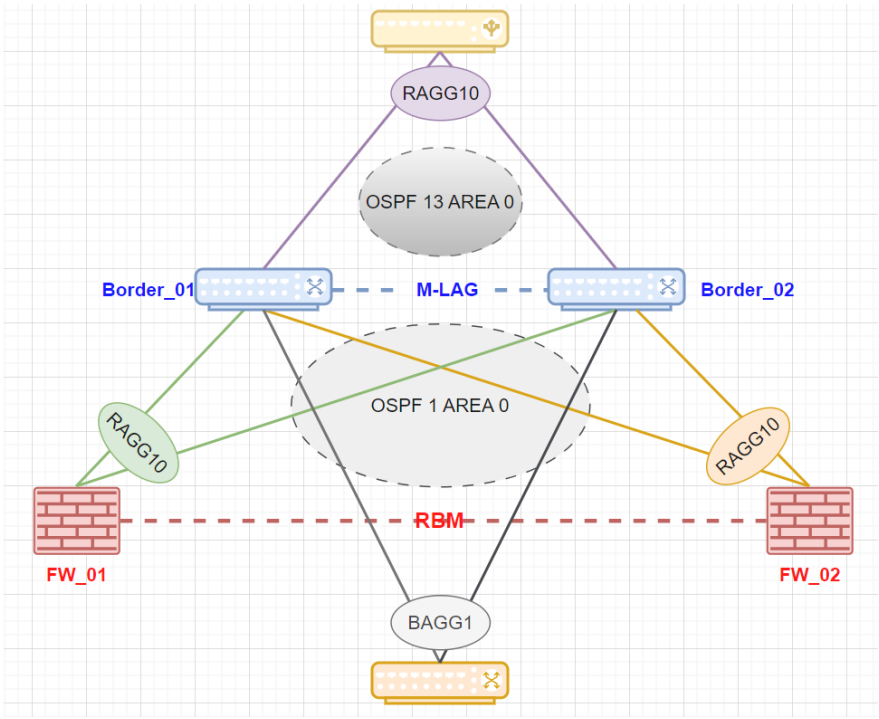
防火墙RBM旁挂对接交换机M-LAG VLAN双活网关动态路由组网典型配置

双机热备 VRRP 孔凡安 2024-08-12 发表

组网及说明



组网说明：

1.FW_01和FW_02采用RBM双机主备部署，交叉互联旁挂在Border上。对接方式和案例（https://zhiliao.h3c.com/theme/details/223781）类似，可以参考。

2.FW使用三层聚合（动态链路聚合）子接口和Border对接，RAGG1.100位于Trust安全域；RAGG1.101位于Untrust安全域。实际组网中建议使用RAGG接口而不是vlan-if接口。

3.Border_01和Border_02 M-LAG双归接入三层网络。配置VRF隔离，分别和FW建立不同的OSPF进程。

4.Border上vlan-if10对接ASW,vlan-if100对接FW Trust域，vlan-if101对接FW Untrust域，vlan-if200对接上行Internet。

5.ASW模拟接入交换机，配置缺省路由下一跳为Border设备VRRP虚地址。模拟测试为访问互联网Internet。

6.防火墙聚合接口编号为1，并非10。图示有点问题懒得改了。

配置步骤

防火墙相关配置：

	FW1	FW2
RBM基础配置	# interface GigabitEthernet1/0/0 port link-mode route combo enable copper port link-aggregation group 64 # interface Route-Aggregation64 ip address 192.168.12.1 255.255.255.252 link-aggregation mode dynamic # remote-backup group data-channel interface Route-Aggregation64 configuration sync-check interval 12 delay-time 30 adjust-cost ospf enable absolute 65535 track 1 track 2 local-ip 192.168.12.1 remote-ip 192.168.12.2 device-role primary #	# interface GigabitEthernet1/0/0 port link-mode route combo enable copper port link-aggregation group 64 # interface Route-Aggregation64 ip address 192.168.12.2 255.255.255.252 link-aggregation mode dynamic # remote-backup group data-channel interface Route-Aggregation64 configuration sync-check interval 12 delay-time 30 adjust-cost ospf enable absolute 65535 track 1 track 2 local-ip 192.168.12.2 remote-ip 192.168.12.1 device-role secondary #

业务接口，安全域，策略	# interface GigabitEthernet1/0/1 port link-mode route combo enable copper port link-aggregation group 1 # interface GigabitEthernet1/0/2 port link-mode route combo enable copper port link-aggregation group 1 # interface Route-Aggregation1 link-aggregation mode dynamic # interface Route-Aggregation1.100 description to_border_v1 ip address 10.134.100.1 255.255.255.0 vlan-type dot1q vid 100 # interface Route-Aggregation1.101 description to_border_v2 ip address 10.134.101.1 255.255.255.0 ospf bfd enable vlan-type dot1q vid 101 # security-zone name Trust import interface Route-Aggregation1.100 # security-zone name Untrust import interface Route-Aggregation1.101 # security-policy ip rule 0 name ospf action pass service ospf rule 1 name ping action pass service ping #	# interface GigabitEthernet1/0/1 port link-mode route combo enable copper port link-aggregation group 1 # interface GigabitEthernet1/0/2 port link-mode route combo enable copper port link-aggregation group 1 # interface Route-Aggregation1 link-aggregation mode dynamic # interface Route-Aggregation1.100 description to_border_v1 ip address 10.134.100.2 255.255.255.0 vlan-type dot1q vid 100 # interface Route-Aggregation1.101 description to_border_v2 ip address 10.134.101.2 255.255.255.0 ospf bfd enable vlan-type dot1q vid 101 # security-zone name Trust import interface Route-Aggregation1.100 # security-zone name Untrust import interface Route-Aggregation1.101 # security-policy ip rule 0 name ospf action pass service ospf rule 1 name ping action pass service ping #
路由配置	# interface LoopBack0 description ospf_r_id ip address 1.1.1.1 255.255.255.255 # ospf 1 router-id 1.1.1.1 area 0.0.0.0 network 10.134.100.0 0.0.0.255 network 10.134.101.0 0.0.0.255 #	# interface LoopBack0 description ospf_r_id ip address 2.2.2.2 255.255.255.255 # ospf 1 router-id 2.2.2.2 area 0.0.0.0 network 10.134.100.0 0.0.0.255 network 10.134.101.0 0.0.0.255 #
可靠性	# track 1 interface Route-Aggregation1.100 # track 2 interface Route-Aggregation1.101 #	# track 1 interface Route-Aggregation1.100 # track 2 interface Route-Aggregation1.101 #

==========

交换机相关配置：

	Border_01	Border_02
系统参数	# interface GigabitEthernet1/0/1 port link-mode route combo enable fiber ip address 192.168.34.3 255.255.255.0 # m-lag mad exclude interface GigabitEthernet1/0/1 m-lag system-mac 0034-0034-0034 m-lag system-number 1 m-lag consistency-check disable m-lag standalone enable m-lag keepalive ip destination 192.168.34.4 source 192.168.34.3 #	# interface GigabitEthernet1/0/1 port link-mode route combo enable fiber ip address 192.168.34.4 255.255.255.0 # m-lag mad exclude interface GigabitEthernet1/0/1 m-lag role priority 65535 m-lag system-mac 0034-0034-0034 m-lag system-number 2 m-lag consistency-check disable m-lag standalone enable m-lag keepalive ip destination 192.168.34.3 source 192.168.34.4

peer-link接口	# interface GigabitEthernet1/0/2 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 100 to 101 200 combo enable fiber port link-aggregation group 1024 # interface Bridge-Aggregation1024 description peerlink port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 100 to 101 200 link-aggregation mode dynamic port m-lag peer-link 1 undo mac-address static source-check enable #	# interface GigabitEthernet1/0/2 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 100 to 101 200 combo enable fiber port link-aggregation group 1024 # interface Bridge-Aggregation1024 description peerlink port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 100 to 101 200 link-aggregation mode dynamic port m-lag peer-link 1 undo mac-address static source-check enable #
m-lag接口	# interface GigabitEthernet1/0/3 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 to 101 combo enable fiber port link-aggregation group 10 # interface GigabitEthernet1/0/4 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 to 101 combo enable fiber port link-aggregation group 11 # interface GigabitEthernet1/0/5 port link-mode bridge port access vlan 200 combo enable fiber port link-aggregation group 100 # interface GigabitEthernet1/0/6 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 combo enable fiber port link-aggregation group 1 # interface Bridge-Aggregation1 description to_asw port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 link-aggregation mode dynamic port lacp system-priority 32 port m-lag group 1 # interface Bridge-Aggregation10 description to_fw01 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 to 101 link-aggregation mode dynamic port lacp system-priority 32 port m-lag group 10 # interface Bridge-Aggregation11 description to_fw02 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 to 101 link-aggregation mode dynamic port lacp system-priority 32 port m-lag group 11 # interface Bridge-Aggregation100 description to_internet port access vlan 200 link-aggregation mode dynamic port lacp system-priority 32 port m-lag group 100 #	# interface GigabitEthernet1/0/3 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 to 101 combo enable fiber port link-aggregation group 11 # interface GigabitEthernet1/0/4 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 to 101 combo enable fiber port link-aggregation group 10 # interface GigabitEthernet1/0/5 port link-mode bridge port access vlan 200 combo enable fiber port link-aggregation group 100 # interface GigabitEthernet1/0/6 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 combo enable fiber port link-aggregation group 1 # interface Bridge-Aggregation1 description to_asw port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 link-aggregation mode dynamic port m-lag group 1 # interface Bridge-Aggregation10 description to_fw01 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 to 101 link-aggregation mode dynamic port m-lag group 10 # interface Bridge-Aggregation11 description to_fw02 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 to 101 link-aggregation mode dynamic port m-lag group 11 # interface Bridge-Aggregation100 description to_internet port access vlan 200 link-aggregation mode dynamic port m-lag group 100 #

OSPF	# ip vpn-instance v1 # ip vpn-instance v2 # interface LoopBack0 description ospf_v1_r_id ip address 3.3.3.3 255.255.255.255 # interface LoopBack10 description ospf_v2_r_id ip address 13.13.13.13 255.255.255.255 # interface Vlan-interface10 ip binding vpn-instance v1 ip address 10.1.10.3 255.255.255.0 vrrp vrid 10 virtual-ip 10.1.10.10 vrrp vrid 10 priority 254 # interface Vlan-interface100 ip binding vpn-instance v1 ip address 10.134.100.10 255.255.255.0 ospf dr-priority 255 ospf peer sub-address enable 10.134.100.13 port m-lag virtual-ip 10.134.100.13 255.255.255.0 active mac-address 0001-0001-0001 # interface Vlan-interface101 ip binding vpn-instance v2 ip address 10.134.101.10 255.255.255.0 ospf dr-priority 255 ospf bfd enable ospf peer sub-address enable 10.134.101.13 port m-lag virtual-ip 10.134.101.13 255.255.255.0 active mac-address 0002-0002-0002 # interface Vlan-interface200 ip binding vpn-instance v2 ip address 10.1.200.10 255.255.255.0 ospf dr-priority 255 ospf bfd enable ospf peer sub-address enable 10.1.200.13 port m-lag virtual-ip 10.1.200.13 255.255.255.0 active mac-address 0003-0003-0003 # ospf 1 router-id 3.3.3.3 vpn-instance v1 area 0.0.0.0 network 10.1.10.0 0.0.0.255 network 10.134.100.0 0.0.0.255 # ospf 13 router-id 13.13.13.13 vpn-instance v2 area 0.0.0.0 network 10.1.200.0 0.0.0.255 network 10.134.101.0 0.0.0.255 #	# ip vpn-instance v1 # ip vpn-instance v2 # interface LoopBack0 description ospf_v1_r_id ip address 4.4.4.4 255.255.255.255 # interface LoopBack10 description ospf_v2_r_id ip address 14.14.14.14 255.255.255.255 # interface Vlan-interface10 ip binding vpn-instance v1 ip address 10.1.10.4 255.255.255.0 vrrp vrid 10 virtual-ip 10.1.10.10 # interface Vlan-interface100 ip binding vpn-instance v1 ip address 10.134.100.10 255.255.255.0 ospf dr-priority 25 ospf peer sub-address enable 10.134.100.14 port m-lag virtual-ip 10.134.100.14 255.255.255.0 active mac-address 0001-0001-0001 # interface Vlan-interface101 ip binding vpn-instance v2 ip address 10.134.101.10 255.255.255.0 ospf dr-priority 25 ospf bfd enable ospf peer sub-address enable 10.134.101.14 port m-lag virtual-ip 10.134.101.14 255.255.255.0 active mac-address 0002-0002-0002 # interface Vlan-interface200 ip binding vpn-instance v2 ip address 10.1.200.10 255.255.255.0 ospf bfd enable ospf peer sub-address enable 10.1.200.14 port m-lag virtual-ip 10.1.200.14 255.255.255.0 active mac-address 0003-0003-0003 # ospf 1 router-id 4.4.4.4 vpn-instance v1 area 0.0.0.0 network 10.1.10.0 0.0.0.255 network 10.134.100.0 0.0.0.255 # ospf 3 router-id 14.14.14.14 vpn-instance v2 area 0.0.0.0 network 10.1.200.0 0.0.0.255 network 10.134.101.0 0.0.0.255 #

==========

接入交换机和公网模拟配置：

ASW	Internet

```
#
interface Bridge-Aggregation10
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10
 link-aggregation mode dynamic
#
interface Vlan-interface10
 ip address 10.1.10.5 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10
 combo enable fiber
 port link-aggregation group 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10
 combo enable fiber
 port link-aggregation group 10
ip route-static 0.0.0.0 0 10.1.10.10 description to_bord
er
#
```

```
#
interface LoopBack0
 description ospf_r_id
 ip address 6.6.6.6 255.255.255.255
#
interface LoopBack1
 description internet
 ip address 114.114.114.114 255.255.255.
255
#
interface Route-Aggregation1
 ip address 10.1.200.6 255.255.255.0
 link-aggregation mode dynamic
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 port link-aggregation group 1
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 port link-aggregation group 1
#
ospf 1 router-id 6.6.6.6
 default-route-advertise always
 area 0.0.0.0
  network 10.1.200.0 0.0.0.255
#
```

==========

以上案例没有考虑出口做NAT的场景，公网侧可以直接学习到私网侧的路由。实际现网中出口设备做NAT，将NAT地址池中路由发布到公网即可。

案例模拟测试ASW ping测试Internet侧环回口地址114.114.114.114即可

公网侧路由：

```
<internet>disp ip routing-table  protocol ospf

Summary count : 9

OSPF Routing table status : <Active>
Summary count : 8

Destination/Mask   Proto   Pre Cost      NextHop         Interface
10.1.10.0/24       O_INTRA 10  4           10.1.200.13     RAGG1
                   O_INTRA 10  4           10.1.200.14     RAGG1
10.134.100.0/24    O_INTRA 10  3           10.1.200.13     RAGG1
                   O_INTRA 10  3           10.1.200.14     RAGG1
10.134.101.0/24    O_INTRA 10  2           10.1.200.13     RAGG1
                   O_INTRA 10  2           10.1.200.14     RAGG1
```

相关表项查看：

设备	路由
Border	

<table>
<tr>
<td></td>
<td>
<table>
<tr>
<td><border_01>disp ospf peer

OSPF Process 1 with Router ID 3.3.3.3
Neighbor Brief Information

Area: 0.0.0.0
Router ID Address Pri Dead-Time State Interface
1.1.1.1 10.134.100.1 1 33 Full/DROther Vlan100
2.2.2.2 10.134.100.2 1 37 Full/DROther Vlan100
4.4.4.4 10.134.100.14 25 36 Full/BDR Vlan100
4.4.4.4 10.1.10.4 1 34 Full/DR Vlan10

OSPF Process 13 with Router ID 13.13.13.13
Neighbor Brief Information

Area: 0.0.0.0
Router ID Address Pri Dead-Time State Interface
1.1.1.1 10.134.101.1 1 35 Full/DROther Vlan101
2.2.2.2 10.134.101.2 1 39 Full/DROther Vlan101
14.14.14.14 10.134.101.14 25 35 Full/BDR Vlan101
6.6.6.6 10.1.200.6 1 32 Full/DROther Vlan200
14.14.14.14 10.1.200.14 1 36 Full/BDR Vlan200</td>
<td><border_02> disp ospf peer

OSPF Process 1 with Router ID 4.4.4.4
Neighbor Brief Information

Area: 0.0.0.0
Router ID Address Pri Dead-Time State Interface
1.1.1.1 10.134.100.1 1 39 Full/DROther Vlan100
2.2.2.2 10.134.100.2 1 33 Full/DROther Vlan100
3.3.3.3 10.134.100.13 255 34 Full/DR Vlan100
3.3.3.3 10.1.10.3 1 32 Full/BDR Vlan10

OSPF Process 3 with Router ID 14.14.14.14
Neighbor Brief Information

Area: 0.0.0.0
Router ID Address Pri Dead-Time State Interface
1.1.1.1 10.134.101.1 1 31 Full/DROther Vlan101
2.2.2.2 10.134.101.2 1 35 Full/DROther Vlan101
13.13.13.13 10.134.101.13 255 33 Full/DR Vlan101
6.6.6.6 10.1.200.6 1 38 Full/DROther Vlan200
13.13.13.13 10.1.200.13 255 34 Full/DR Vlan200</td>
</tr>
<tr>
<td><border_01>disp ip routing-table vpn-instance v1 protocol ospf

Summary count : 6

OSPF Routing table status : <Active>
Summary count : 4

Destination/Mask Proto Pre Cost NextHop Interface
0.0.0.0/0 O_ASE2 150 1 10.134.100.1 Vlan100
10.1.200.0/24 O_INTRA 10 3 10.134.100.1 Vlan100
10.134.101.0/24 O_INTRA 10 2 10.134.100.1 Vlan100
100.1.1.1/32 O_ASE2 150 1 10.134.100.1 Vlan100

OSPF Routing table status : <Inactive>
Summary count : 2

Destination/Mask Proto Pre Cost NextHop Interface
10.1.10.0/24 O_INTRA 10 1 0.0.0.0 Vlan10
10.134.100.0/24 O_INTRA 10 1 0.0.0.0 Vlan100</td>
<td><border_02> disp ip routing-table vpn-instance v1 protocol ospf

Summary count : 6

OSPF Routing table status : <Active>
Summary count : 4

Destination/Mask Proto Pre Cost NextHop Interface
0.0.0.0/0 O_ASE2 150 1 10.134.100.1 Vlan100
10.1.200.0/24 O_INTRA 10 3 10.134.100.1 Vlan100
10.134.101.0/24 O_INTRA 10 2 10.134.100.1 Vlan100
100.1.1.1/32 O_ASE2 150 1 10.134.100.1 Vlan100

OSPF Routing table status : <Inactive>
Summary count : 2

Destination/Mask Proto Pre Cost NextHop Interface
10.1.10.0/24 O_INTRA 10 1 0.0.0.0 Vlan10
10.134.100.0/24 O_INTRA 10 1 0.0.0.0 Vlan100</td>
</tr>
</table>
</td>
</tr>
<tr>
<td>FW</td>
<td></td>
</tr>
</table>

RBM_P<fw_01>disp ospf peer OSPF Process 1 with Router ID 1.1.1.1 Neighbor Brief Information Area: 0.0.0.0 Router ID Address Pri Dead-Time State Interface 2.2.2.2 10.134.100.2 1 31 2-Way/ - RAGG1.100 3.3.3.3 10.134.100.13 255 35 Full/DR RAGG1.100 4.4.4.4 10.134.100.14 25 39 Full/BDR RAGG1.100 2.2.2.2 10.134.101.2 1 32 2-Way/ - RAGG1.101 13.13.13.13 10.134.101.13 255 33 Full/DR RAGG1.101 14.14.14.14 10.134.101.14 25 38 Full/BDR RAGG1.101	RBM_S<fw_02>disp ospf peer OSPF Process 1 with Router ID 2.2.2.2 Neighbor Brief Information Area: 0.0.0.0 Router ID Address Pri Dead-Time State Interface 1.1.1.1 10.134.100.1 1 33 2-Way/ - RAGG1.100 3.3.3.3 10.134.100.13 255 29 Full/DR RAGG1.100 4.4.4.4 10.134.100.14 25 33 Full/BDR RAGG1.100 1.1.1.1 10.134.101.1 1 34 2-Way/ - RAGG1.101 13.13.13.13 10.134.101.13 255 39 Full/DR RAGG1.101 14.14.14.14 10.134.101.14 25 32 Full/BDR RAGG1.101
RBM_P<fw_01>disp ip routing-table protocol ospf Summary count : 10 OSPF Routing table status : <Active> Summary count : 6 Destination/Mask Proto Pre Cost NextHop Interface 0.0.0.0/0 O_ASE2 150 1 10.134.101.13 RAGG1.101 O_ASE2 150 1 10.134.101.14 RAGG1.101 10.1.10.0/24 O_INTRA 10 2 10.134.100.13 RAGG1.100 O_INTRA 10 2 10.134.100.14 RAGG1.100 10.1.200.0/24 O_INTRA 10 2 10.134.101.13 RAGG1.101 O_INTRA 10 2 10.134.101.14 RAGG1.101 OSPF Routing table status : <Inactive> Summary count : 4 Destination/Mask Proto Pre Cost NextHop Interface 10.134.100.0/24 O_INTRA 10 1 0.0.0.0 RAGG1.100 10.134.101.0/24 O_INTRA 10 1 0.0.0.0 RAGG1.101 100.1.1.1/32 O_ASE2 150 65535 10.134.100.2 RAGG1.100 100.1.1.1/32 O_ASE2 150 65535 10.134.101.2 RAGG1.101	RBM_S<fw_02>disp ip routing-table protocol ospf Summary count : 10 OSPF Routing table status : <Active> Summary count : 6 Destination/Mask Proto Pre Cost NextHop Interface 0.0.0.0/0 O_ASE2 150 1 10.134.101.13 RAGG1.101 O_ASE2 150 1 10.134.101.14 RAGG1.101 10.1.10.0/24 O_INTRA 10 65536 10.134.100.13 RAGG1.100 O_INTRA 10 65536 10.134.100.14 RAGG1.100 10.1.200.0/24 O_INTRA 10 65536 10.134.101.13 RAGG1.101 O_INTRA 10 65536 10.134.101.14 RAGG1.101 OSPF Routing table status : <Inactive> Summary count : 4 Destination/Mask Proto Pre Cost NextHop Interface 10.134.100.0/24 O_INTRA 10 65535 0.0.0.0 RAGG1.100 10.134.101.0/24 O_INTRA 10 65535 0.0.0.0 RAGG1.101 100.1.1.1/32 O_ASE2 150 1 10.134.100.1 RAGG1.100 100.1.1.1/32 O_ASE2 150 1 10.134.101.1 RAGG1.101

配置关键点

1.FW并非所有配置都是同步的，常见的：安全域和安全策略可以从RBM_P同步到RBM_S，有些配置无法同步（如接口地址，Track，路由配置等），配置的时候需要对比所有相关配置防止遗漏。
2.FW 安全策略需要针对基础协议OSPF单独放通，否则导致OSPF邻居建立失败。
3.FW使用三层子接口必须配置vlan终结命令，需要对端发出的报文携带对应的vlan标签。如果对端发出的报文不带vlan标签，则使用聚合口对接。
4.Border peer-link链路两端端口上关闭报文入接口与静态MAC地址表项匹配检查功能，以确保三层单播流量转发正常。
5.两台Border作为双活网关时，vlan-if接口存在相同的IP地址和MAC地址，需要配置M-LAG虚拟IP地址建立OSPF邻居，并指定active参数。否则则该虚拟IPv4地址只在角色为Primary的M-LAG设备上处于可用状态。
6.Border配置m-lag独立工作模式，并配置lacp系统优先级。应对peer-link链路和Keepalive链路均发生故障场景。这个感兴趣的可以模拟测试。