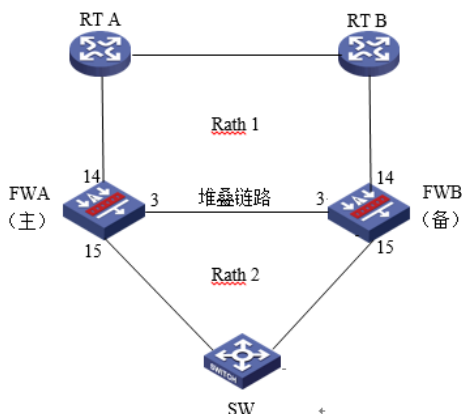## 组网及说明

1 配置需求及说明

1.1 适用的产品系列

本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

1.2 配置需求及实现的效果

防火墙A与防火墙B堆叠后上联路由器A、B下联交换机，应用户业务需求：

1、 防火墙做主备运行

2、 正常情况下业务流量全部负载在FWA，FWA出现故障后流量全部切到FWB运行

2 组网图

配置步骤

3 配置步骤

3.1 路由器A配置

3.1.1 配置路由器A下联防火墙接口

system

[H3C]interface GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/1] ip address 1.1.1.1 24

[H3C-GigabitEthernet1/0/1]quit

[H3C]ospf 1

[H3C-ospf-1]area 0

[H3C-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0

路由器B除IP地址外，配置相同不再赘述。

3.2 交换机配置

3.2.1 配置交换机上联防火墙接口

交换机配置vlan 10将上联防火墙的14和15接口加入vlan10，并创建vlan10接口IP地址为3.3.3.1。

system

[H3C]vlan20

[H3C-vlan20]port GigabitEthernet 1/0/14 GigabitEthernet 1/0/15

[H3C]interface Vlan-interface 10

[H3C-Vlan-interface10]ip address 3.3.3.1 24

配置默认路由到防火墙Reth2接口地址。

[H3C]ip route-static 0.0.0.0 0 3.3.3.2

3.3 防火墙配置

3.3.1 FWA与FWB建立堆叠

具体配置可参考防火墙虚拟化配置举例，本章不做介绍。

3.3.2 配置track联动上下行接口的物理状态

配置track检测上下行端口的物理状态

[H3C] track 1 interface gigabitethernet 1/0/15 physical

[H3C-track-1] quit

[H3C] track 2 interface gigabitethernet 1/0/14 physical

[H3C-track-2] quit

[H3C] track 3 interface gigabitethernet 2/0/14 physical

[H3C-track-3] quit

[H3C] track 4 interface gigabitethernet 2/0/15 physical

[H3C-track-4] quit

3.3.3 配置冗余组关联冗余接口

1. 创建Reth1接口关联下联防火墙的接口

创建Reth1接口配置IP地址为3.3.3.2/24，并配置1/0/15成员优先级为255，2/0/15成员优先级为50。

system-view

[H3C] interface reth 1

[H3C-Reth1] ip address 3.3.3.2 24

[H3C-Reth1] member interface gigabitethernet 1/0/15 priority 255

[H3C-Reth1] member interface gigabitethernet 2/0/15 priority 50

[H3C-Reth1] quit

2. 创建节点1与防火墙A所有接口绑定

[H3C] redundancy group aaa

[H3C-redundancy-group-aaa] node 1

[H3C-redundancy-group-aaa-node1] bind slot 1

[H3C-redundancy-group-aaa-node1] priority 100

[H3C-redundancy-group-aaa-node1] node-member interface gigabitethernet 1/0/14

[H3C-redundancy-group-aaa-node1] track 1 interface gigabitethernet 1/0/15

[H3C-redundancy-group-aaa-node1] track 2 interface gigabitethernet 1/0/14

[H3C-redundancy-group-aaa-node1] quit

3. 创建节点2与防火墙B所有接口绑定

[H3C-redundancy-group-aaa] node 2

[H3C-redundancy-group-aaa-node2] bind slot 2

[H3C-redundancy-group-aaa-node2] priority 50

 [H3C-redundancy-group-aaa-node2] node-member interface gigabitethernet 2/0/14

[H3C-redundancy-group-aaa-node2] track 3 interface gigabitethernet 2/0/15

[H3C-redundancy-group-aaa-node2] track 4 interface gigabitethernet 2/0/14

[H3C-redundancy-group-aaa-node2] quit

4. 将Reth1添加到冗余组

[H3C-redundancy-group-aaa] member interface reth 1

3.3.4 开启会话热备

[H3C] session synchronization enable

3.3.5 安全策略配置

1. 将接口加入安全域

将1/0/1与2/0/1加入Untrust区域

[H3C]security-zone name Untrust

[H3C-security-zone-Untrust]import interface GigabitEthernet 1/0/14

[H3C-security-zone-Untrust]import interface GigabitEthernet 2/0/14

将1/0/2与2/0/2加入trust区域

[H3C]security-zone name trust

[H3C-security-zone-trust]import interface Reth1

[H3C-security-zone-trust]quit

防火墙目前版本存在两套安全策略，请在放通安全策略前确认设备运行那种类型的安全策略？以下配置任选其一。

2. 通过命令"display cu | in security-policy"如果查到命令行存在"security-policy disable"或者没有查到任何信息，则使用下面策略配置。

[H3C]display cu | in security-policy

 security-policy disable

#创建对象策略pass。

[H3C]object-policy ip pass

[H3C-object-policy-ip-pass] rule 0 pass

[H3C-object-policy-ip-pass]quit

#创建Trust到Untrust域的域间策略调用pass策略。

[H3C]zone-pair security source Trust destination local

[H3C-zone-pair-security-Trust- local]object-policy apply ip pass

[H3C-zone-pair-security-Trust- local]quit

[H3C]zone-pair security source local destination Trust

[H3C-zone-pair-security-local -trust]object-policy apply ip pass

[H3C-zone-pair-security-local -trust]quit

[H3C]zone-pair security source Untrust destination local

[H3C-zone-pair-security-Untrust- local]object-policy apply ip pass

[H3C-zone-pair-security-Untrust- local]quit

[H3C]zone-pair security source local destination Untrust

[H3C-zone-pair-security-local -Untrust]object-policy apply ip pass

[H3C-zone-pair-security-local -Untrust]quit

[H3C]zone-pair security source Trust destination Untrust

[H3C-zone-pair-security-Trust -Untrust]object-policy apply ip pass

[H3C-zone-pair-security-Trust -Untrust]quit

3. 通过命令"display cu | in security-policy"如果查到命令行存在"security-policy ip"并且没有查到"
security-policy disable"，则使用下面策略配置。

[H3C]display cu | in security-policy

security-policy ip

创建安全策略并放通local到trust和trust到local的安全策略。

[H3C]security-policy ip

[H3C-security-policy-ip]rule 10 name test

[H3C-security-policy-ip-10-test]action pass

[H3C-security-policy-ip-10-test]source-zone local

[H3C-security-policy-ip-10-test]source-zone Trust

[H3C-security-policy-ip-10-test]source-zone Untrust

[H3C-security-policy-ip-10-test]destination-zone local

[H3C-security-policy-ip-10-test]destination-zone Trust

[H3C-security-policy-ip-10-test]destination-zone Untrust

[H3C-security-policy-ip-10-test]quit

4 检验配置结果

4.1.1 正常时查看冗余组状态

节点1为主用状态，节点二为备用状态。

```
[F1060]dis redundancy group bin
Redundancy group bin (ID 1):
   Node ID      Slot         Priority   Status      Track weight
   1            Slot1        100        Primary     255
   2            Slot2        50         Secondary   255

Preempt delay time remained   : 0    min
Preempt delay timer setting   : 1    min
Remaining hold-down time       : 0    sec
Hold-down timer setting        : 1    sec
Manual switchover request      : No

Member interfaces:
    Reth1

Node 1:
   Node member     Physical status
   GE1/0/14        UP
   Track info:
   Track      Status      Reduced weight      Interface
   1          Positive    255                 GE1/0/15
   2          Positive    255                 GE1/0/14
Node 2:
   Node member     Physical status
   GE2/0/14        UP
   Track info:
   Track      Status      Reduced weight      Interface
   3          Positive    255                 GE2/0/15
   4          Positive    255                 GE2/0/14
[F1060]
```

显示Reth信息。可以看到Reth1中优先级高的成员接口处于激活状态。

```
[F1060]dis reth interface Reth 1
Reth1 :
   Redundancy group  : bin
   Member       Physical status      Forwarding status   Presence status
   GE1/0/15     UP                   Active              Normal
   GE2/0/15     UP                   Inactive            Normal
```

4.1.2 异常时查看冗余组状态

手动关闭1/0/14接口后时查看冗余组状态,

```
[F1060]dis redundancy group bin
Redundancy group bin (ID 1):
   Node ID      Slot         Priority   Status      Track weight
   1            Slot1        100        Secondary   -255
   2            Slot2        50         Primary     255

Preempt delay time remained   : 0    min
Preempt delay timer setting   : 1    min
Remaining hold-down time       : 0    sec
Hold-down timer setting        : 1    sec
Manual switchover request      : No

Member interfaces:
    Reth1

Node 1:
   Node member     Physical status
   GE1/0/14        DOWN
   Track info:
   Track      Status      Reduced weight      Interface
   1          Negative    255                 GE1/0/15
   2          Negative    255                 GE1/0/14(Fault)
Node 2:
   Node member     Physical status
   GE2/0/14        UP
   Track info:
   Track      Status      Reduced weight      Interface
   3          Positive    255                 GE2/0/15
   4          Positive    255                 GE2/0/14
```

配置关键点

4.1.3 注意事项

1、配置冗余组后需要加入冗余接口的物理口全部连接，否则会造成冗余组异常。