# F5000-X系列防火墙堆叠后透明主备配置举例

IRF　程咪　2019-10-22 发表

## 组网及说明

**1 配置需求及说明**

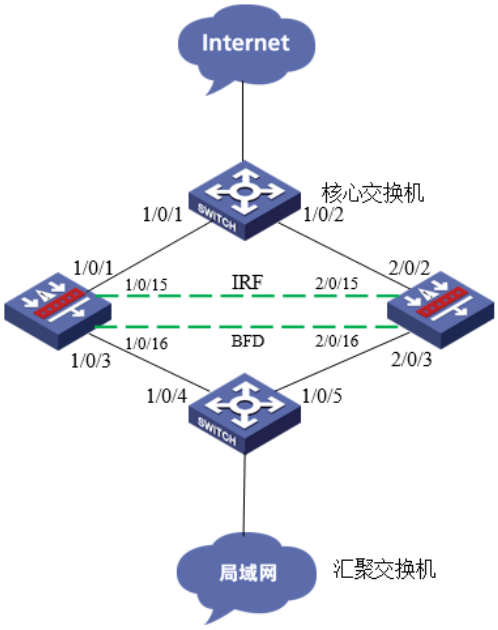
**1.1 适用的产品系列**

本案例适用于如F5080、F5060、F5030、F5000-M等F5000、F5000-X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堆叠后使用透明模式部署在核心交换机与汇聚交换机之间，需要使用目前情况下所有流量通过防火墙A进行转发，如果防火墙A出现宕机再由防火墙B接管所有业务、当防火墙A故障恢复后再次接管所有业务。

**1.3 组网图**




## 配置步骤

**2 配置步骤**

**2.1 核心交换机配置**

#创建三层聚合接口并设置IP地址。

<H3C>system

[H3C]interface Route-Aggregation 1

[H3C-Route-Aggregation1]ip address 192.168.1.1 255.255.255.0

[H3C-Route-Aggregation1]link-aggregation selected-port maximum 1

[H3C-Route-Aggregation1]quit

#将1/0/1接口加入聚合组并设置聚合优先级。

[H3C]interface GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/1]link-aggregation port-priority 10

[H3C-GigabitEthernet1/0/1]port link-aggregation group 1

[H3C-GigabitEthernet1/0/1]quit

#将1/0/2接口加入聚合组并设置聚合优先级。

[H3C]interface GigabitEthernet 1/0/2

[H3C-GigabitEthernet1/0/2]link-aggregation port-priority 100

[H3C-GigabitEthernet1/0/2]port link-aggregation group 1

[H3C-GigabitEthernet1/0/2]quit

**2.2 防火墙配置**

**2.2.1 FWA与FWB建立堆叠并配置BFD MAD检测**

具体配置可参考防火墙虚拟化配置举例，本章不做介绍。

**2.2.2 防火墙开启会话同步并关闭本框优先命令**

#开启本地IP优先转发功能

[Sysname] ip load-sharing local-first enable

#开启会话同步功能

[Sysname] session synchronization enable

#开启会话数据统计功能

[Sysname] session statistics enable

**2.2.3 防火墙聚合配置**

**1. 防火墙上行接口聚合配置**

#创建二层聚合接口并设置聚合最大选中个数。

<H3C>system

[H3C]interface Bridge-Aggregation 1

[H3C-Bridge-Aggregation1]link-aggregation selected-port maximum 1

[H3C-Bridge-Aggregation1]quit

#将1/0/1接口加入聚合组并设置聚合优先级。

[H3C]interface GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/1]link-aggregation port-priority 10

[H3C-GigabitEthernet1/0/1]port link-aggregation group 1

[H3C-GigabitEthernet1/0/1]quit

#将2/0/2接口加入聚合组并设置聚合优先级。

[H3C]interface GigabitEthernet 2/0/2

[H3C-GigabitEthernet2/0/2]link-aggregation port-priority 100

[H3C-GigabitEthernet2/0/2]port link-aggregation group 1

[H3C-GigabitEthernet2/0/2]quit

**2. 防火墙下行接口聚合配置**

#创建二层聚合接口并设置聚合最大选中个数。

<H3C>system

[H3C]interface Bridge-Aggregation 2

[H3C-Bridge-Aggregation2]link-aggregation selected-port maximum 1

[H3C-Bridge-Aggregation2]quit

#将1/0/1接口加入聚合组并设置聚合优先级。

[H3C]interface GigabitEthernet 1/0/3

[H3C-GigabitEthernet1/0/3]link-aggregation port-priority 10

[H3C-GigabitEthernet1/0/3]port link-aggregation group 2

[H3C-GigabitEthernet1/0/3]quit

#将2/0/3接口加入聚合组并设置聚合优先级。

[H3C]interface GigabitEthernet 2/0/3

[H3C-GigabitEthernet2/0/3]link-aggregation port-priority 100

[H3C-GigabitEthernet2/0/3]port link-aggregation group 2

[H3C-GigabitEthernet2/0/3]quit

**2.2.4 防火墙安全域配置**

#将防火墙上行接口接入Untrust区域

[H3C]security-zone name Untrust

[H3C-security-zone-Untrust]import interface Bridge-Aggregation1 vlan 1

[H3C-security-zone-Untrust]import interface GigabitEthernet1/0/1 vlan 1

[H3C-security-zone-Untrust]import interface GigabitEthernet2/0/2 vlan 1

[H3C-security-zone-Untrust]quit

#将防火墙下行接口接入trust区域

[H3C]security-zone name Untrust

[H3C-security-zone-Trust]import interface Bridge-Aggregation2 vlan 1

[H3C-security-zone-Trust]import interface GigabitEthernet1/0/3 vlan 1

[H3C-security-zone-Trust]import interface GigabitEthernet2/0/3 vlan 1

[H3C-security-zone-Trust]quit

**2.2.5 配置端口冗余组配置**

#配置track监控物理端口

[H3C]track 1 interface GigabitEthernet1/0/1 physical

[H3C]track 2 interface GigabitEthernet2/0/2 physical

[H3C]track 3 interface GigabitEthernet1/0/3 physical

[H3C]track 4 interface GigabitEthernet2/0/3 physical

#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 1/0/1

[H3C-redundancy-group-aaa-node1] node-member interface gigabitethernet 1/0/3

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

[H3C-redundancy-group-aaa-node1] track 3 interface gigabitethernet 1/0/3

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

**1. 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 2/0/2
[H3C-redundancy-group-aaa-node2] node-member interface gigabitethernet 2/0/3
[H3C-redundancy-group-aaa-node2] track 2 interface gigabitethernet 2/0/2
[H3C-redundancy-group-aaa-node2] track 4 interface gigabitethernet 2/0/3
[H3C-redundancy-group-aaa-node2] quit

**2.2.6 安全策略配置**

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。

**1. 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

**2. 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

**2.3 汇聚交换机配置**

#创建三层聚合接口并设置IP地址。
<H3C>system
[H3C]interface Route-Aggregation 1
[H3C-Route-Aggregation1]ip address 192.168.1.2 255.255.255.0
[H3C-Route-Aggregation1]link-aggregation selected-port maximum 1
[H3C-Route-Aggregation1]quit
#将1/0/4接口加入聚合组并设置聚合优先级。
[H3C]interface GigabitEthernet 1/0/4
[H3C-GigabitEthernet1/0/4]link-aggregation port-priority 10
[H3C-GigabitEthernet1/0/4]port link-aggregation group 1
[H3C-GigabitEthernet1/0/4]quit
#将1/0/5接口加入聚合组并设置聚合优先级。
[H3C]interface GigabitEthernet 1/0/5

[H3C-GigabitEthernet1/0/5]link-aggregation port-priority 100
[H3C-GigabitEthernet1/0/5]port link-aggregation group 1
[H3C-GigabitEthernet1/0/5]quit

**3 检验配置结果**

**3.1.1 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。

[H3C-redundancy-group-aaa] display redundancy group aaa
Redundancy group aaa (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:

Node 1:

| Node member | Physical status |
|---|---|
| GE1/0/1 | UP |
| GE1/0/3 | UP |

Track info:

| Track | Status | Reduced weight | Interface |
|---|---|---|---|
| 1 | Positive | 255 | GE1/0/1 |
| 2 | Positive | 255 | GE1/0/3 |

Node 2:

| Node member | Physical status |
|---|---|
| GE2/0/2 | UP |
| GE2/0/3 | UP |

Track info:

| Track | Status | Reduced weight | Interface |
|---|---|---|---|
| 3 | Positive | 255 | GE2/0/2 |
| 4 | Positive | 255 | GE2/0/3 |

**3.1.2 手动关闭1/0/1接口后时查看冗余组状态**

查看到主备状态已经发生了变化，并且1/0/1与1/0/3的物理状态全部置为down。

[H3C] display redundancy group aaa
Redundancy group aaa (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:

Node 1:

| Node member | Physical status |
|---|---|
| GE1/0/1 | DOWN(redundancy down) |
| GE1/0/3 | DOWN |

Track info:

| Track | Status | Reduced weight | Interface |
|---|---|---|---|
| 1 | Negative | 255 | GE1/0/1 |
| 2 | Negative | 255 | GE1/0/2 (Fault) |

Node 2:

| Node member | Physical status |
|---|---|
| GE2/0/2 | UP |
| GE2/0/3 | UP |

Track info:

| Track | Status | Reduced weight | Interface |
| --- | --- | --- | --- |
| 3 | Positive | 255 | GE2/0/2 |
| 4 | Positive | 255 | GE2/0/3 |

## 配置关键点

### 3.1.3 注意事项

1、配置冗余组后，所有加入冗余组的物理接口状态必须处于UP状态，否则会造成冗余组主备切换异常。