V7防火墙插卡IRF组网案例

冗余组 IRF 张泷文 2015-10-30 发表

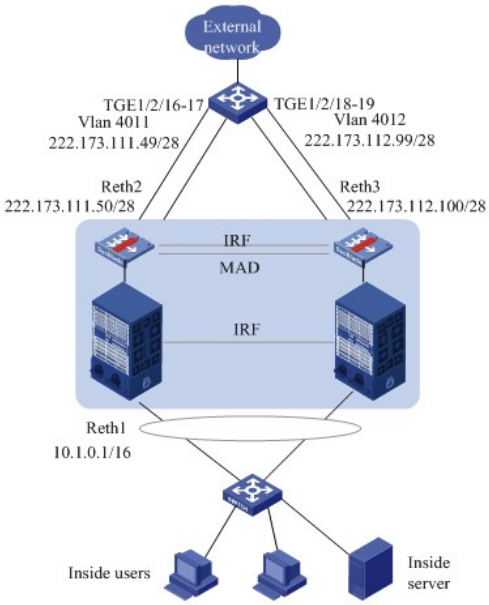
·在两台S105交换机之间建立堆叠。

· 在两台FW板卡之间建立堆叠，FW1的堆叠口为：G1/0/2，FW2的堆叠口为：G2/0/2。

· 为了防止万一IRF链路故障导致IRF分裂，网络中存在两个配置冲突的IRF，因此启用MAD检测功能。将FW1的G1/0/1和FW2的G2/0/1连接用作BFD MAD检测。

· 创建冗余口Reth2和Reth3分别对应于两条link。

· 创建冗余组1，包含冗余成员：Reth1、Reth2、Reth3等。



运营商交换机的配置

· 配置接FW上LB Link1对应的下一跳：把Ten1/2/16、Ten1/2/18允许vlan 4011，用vlan interface 作为网关

[H3Cvlan4011

[H3C]interface Vlan-interface4011

[H3C-Vlan-interface4011]ip address 222.173.111.49 255.255.255.252

[H3C-Vlan-interface4011]quit

#

[H3C]interface Ten-GigabitEthernet 1/2/16

[H3C-Ten-GigabitEthernet1/2/16]port link-type trunk

[H3C-Ten-GigabitEthernet1/2/16]port trunk permit vlan 4011

[H3C]interface Ten-GigabitEthernet 1/2/18

[H3C-Ten-GigabitEthernet1/2/18]port link-type trunk

[H3C-Ten-GigabitEthernet1/2/18]port trunk permit vlan 4011

· 配置接FW上LB Link2对应的下一跳：把Ten1/2/17、Ten1/2/19允许vlan 4012，用vlan interface 作为网关

[H3C]vlan4012

[H3C]interface Vlan-interface 4012

[H3C-Vlan-interface4012]ip address 222.173.112.99 255.255.255.248

[H3C-Vlan-interface4012]quit

#

[H3C]interface Ten-GigabitEthernet 1/2/17

[H3C-Ten-GigabitEthernet1/2/17]port link-type trunk

[H3C-Ten-GigabitEthernet1/2/17]port trunk permit vlan 4012

[H3C]interface Ten-GigabitEthernet 1/2/19

[H3C-Ten-GigabitEthernet1/2/19]port link-type trunk

[H3C-Ten-GigabitEthernet1/2/19]port trunk permit vlan 4012

1.5.2 S105交换机的配置步骤

(1) IRF的配置：

- S105交换机 1的配置：

配置成员号和优先级。

[H3C] irf member 1 priority 32

#配置Chassis 1，配置IRF端口1/1，并将它与物理端口Ten-GigabitEthernet1/7/0/1绑定，并保存配置，激活IRF端口下的配置。

[H3C]interface Ten-GigabitEthernet 1/7/0/1

[H3C-Ten-GigabitEthernet1/7/0/1]shutdown

[H3C-Ten-GigabitEthernet1/7/0/1] quit

[H3C] irf-port 1/1

[H3C-irf-port1/1]port group interface Ten-GigabitEthernet 1/7/0/1

[H3C-irf-port1/1] quit

[H3C] interface Ten-GigabitEthernet 1/7/0/1

[H3C-Ten-GigabitEthernet1/7/0/1] undo shutdown

[H3C-Ten-GigabitEthernet1/7/0/1] quit

[H3C]save

[H3C]irf-port-configuration active

- S105交换机2的配置：

配置成员号和优先级。

[H3C]irf member 2 priority 1

#配置Chassis 2, 将S105交换机2的成员编号配置为2，并重启设备使新编号生效。

[H3C]irf member 1 renumber 2

Warning: Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[H3C]quit

< H3C > reboot

#S105交换机2重新起来后，登录设备，配置IRF端口2/2，并将它与物理端口Ten-GigabitEthernet2/7/0/3绑定，并保存配置，激活IRF端口下的配置。

[H3C]interface Ten-GigabitEthernet 2/7/0/3

[H3C-Ten-GigabitEthernet2/7/0/3]shutdown

[H3C-Ten- GigabitEthernet2/7/0/3]quit

[H3C]irf-port 2/2

[H3C-irf-port2/2] port group interface Ten-GigabitEthernet 2/7/0/3

[H3C-irf-port2/2] quit

[H3C]interface Ten-GigabitEthernet 2/7/0/3

[H3C-Ten-GigabitEthernet2/7/0/3]undo shutdown

[H3C-Ten-GigabitEthernet2/7/0/3]quit

[H3C]save

[H3C]irf-port-configuration active

(2) 接口配置：

#Chassi1连接运营商交换机Ten1/2/16的接口Ten1/6/0/34

[H3C]interface Ten-GigabitEthernet 1/6/0/34

[H3C-Ten-GigabitEthernet1/6/0/34] port link-type trunk

[H3C-Ten-GigabitEthernet1/6/0/34]port trunk permit vlan 4011

[H3C-Ten-GigabitEthernet1/6/0/34]quit

#Chassi1连接运营商交换机Ten1/2/17的接口Ten1/6/0/35

[H3C]interface Ten-GigabitEthernet 1/6/0/35

[H3C-Ten-GigabitEthernet1/6/0/35]port link-type trunk

[H3C-Ten-GigabitEthernet1/6/0/35]port trunk permit vlan 4012

[H3C-Ten-GigabitEthernet1/6/0/35]quit

#Chassi2连接运营商交换机Ten1/2/18的接口Ten2/6/0/34

[H3C]interface Ten-GigabitEthernet 2/6/0/34

[H3C-Ten-GigabitEthernet2/6/0/34]port link-type trunk

[H3C-Ten-GigabitEthernet2/6/0/34]port trunk permit vlan 4011

[H3C-Ten-GigabitEthernet2/6/0/34]quit

#Chassi2连接运营商交换机Ten1/2/19的接口Ten2/6/0/35

[H3C]interface Ten-GigabitEthernet 2/6/0/35

[H3C-Ten-GigabitEthernet2/6/0/35]port link-type trunk

[H3C-Ten-GigabitEthernet2/6/0/35]port trunk permit vlan 4012

[H3C-Ten-GigabitEthernet2/6/0/35]quit

#S105交换机连接到内部用户的接口允许vlan 4010的报文。接口配置略。

#Chassi1连接SecBlade III FW1的内联口组成聚合口BAG1，vlan 4010为连接内部用户的vlan。

#

[H3C]interface Bridge-Aggregation1

[H3C-Bridge-Aggregation1]quit

[H3C]interface Ten-GigabitEthernet 1/1/0/1

[H3C-Ten-GigabitEthernet1/1/0/1]port link-mode bridge

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

[H3C-Ten-GigabitEthernet1/1/0/1]quit

依此再将Ten1/1/0/2，Ten1/1/0/3，Ten1/1/0/4都加入聚合组1。

[H3C]interface Bridge-Aggregation1

[H3C-Bridge-Aggregation1]port link-type trunk

[H3C-Bridge-Aggregation1]undo port trunk permit vlan 1

[H3C-Bridge-Aggregation1]port trunk permit vlan 4010 to 4012

#Chassi2连接SecBlade III FW2的内联口组成聚合口BAG2

[H3C]interface Bridge-Aggregation2

[H3C-Bridge-Aggregation2]quit

[H3C]interface Ten-GigabitEthernet 2/2/0/1

[H3C-Ten-GigabitEthernet2/2/0/1]port link-mode bridge

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

[H3C-Ten-GigabitEthernet2/2/0/1]quit

依此再将Ten2/2/0/2，Ten2/2/0/3，Ten2/2/0/4都加入聚合组2。

[H3C]interface Bridge-Aggregation2

[H3C-Bridge-Aggregation2]port link-type trunk

[H3C-Bridge-Aggregation2]undo port trunk permit vlan 1

[H3C-Bridge-Aggregation2]port trunk permit vlan 4010 to 4012

1.5.3 SecBlade III FW的IRF和MAD检测配置步骤

(1) SecBlade III FW1的IRF配置步骤

配置成员号和优先级。

[H3C] irf member 1 priority 32

#配置FW1，配置IRF端口1/2，并将它与物理端口GigabitEthernet1/0/2绑定，并保存配置，激活IRF端口下的配置。

[H3C] interface GigabitEthernet1/0/2

[H3C- GigabitEthernet1/0/2] shutdown

[H3C- GigabitEthernet1/0/2] quit

[H3C] irf-port 1/2

[H3C-irf-port1/2] port group interface GigabitEthernet1/0/2

[H3C-irf-port1/2] quit

[H3C] interface GigabitEthernet1/0/2

[H3C-GigabitEthernet1/0/2] undo shutdown

[H3C-GigabitEthernet1/0/2] quit

[H3C]save

[H3C]irf-port-configuration active

(2) SecBlade III FW2的IRF配置步骤

配置成员号和优先级。

[H3C]irf member 2 priority 1

#配置FW2, 将FW2的成员编号配置为2，并重启设备使新编号生效。

[H3C]irf member 1 renumber 2

Warning: Renumbering the member ID may result in configuration change or loss. Continue? [Y

/N]:y

[H3C]quit

< H3C > reboot

#FW2重新起来后，登录设备，配置IRF端口2/1，并将它与物理端口GigabitEthernet2/0/2绑定，并保存配置,激活IRF端口下的配置。

[H3C]interface GigabitEthernet2/0/2

[H3C-GigabitEthernet2/0/2]shutdown

[H3C-GigabitEthernet2/0/2]quit

[H3C]irf-port 2/1

[H3C-irf-port2/1] port group interface GigabitEthernet2/0/2

[H3C-irf-port2/1] quit

[H3C]interface GigabitEthernet2/0/2

[H3C-GigabitEthernet2/0/2]undo shutdown

[H3C-GigabitEthernet2/0/2]quit

[H3C]save

[H3C]irf-port-configuration active

#FW1和FW2间将会进行主设备竞选，竞选失败的一方将重启，重启完成后，IRF形成。

(3) 配置BFD MAD检测

创建VLAN 3，并将FW1（成员编号为1）上的端口1/0/1和FW2（成员编号为2）上的端口2/0/1加入VLAN中。

system-view

[H3C] vlan 3

[H3C-vlan3] quit

[H3C]interface GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/1]port link-mode bridge

[H3C-GigabitEthernet1/0/1]port access vlan 3

[H3C-GigabitEthernet1/0/1]quit

[H3C]interface GigabitEthernet 2/0/1

[H3C-GigabitEthernet2/0/1]port link-mode bridge

[H3C-GigabitEthernet2/0/1]port access vlan 3

[H3C-GigabitEthernet2/0/1]quit

创建VLAN接口3，并配置MAD IP地址。

[H3C] interface vlan-interface 3

[H3C-Vlan-interface3] mad bfd enable

[H3C-Vlan-interface3] mad ip address 192.168.2.1 24 member 1

[H3C-Vlan-interface3] mad ip address 192.168.2.2 24 member 2

[H3C-Vlan-interface3] quit

因为BFD MAD和生成树功能互斥，所以在GigabitEthernet1/0/1和GigabitEthernet2/0/1上关闭生成树协议。

[H3C] interface gigabitethernet 1/0/1

[H3C-gigabitethernet-1/0/1] undo stp enable

[H3C-gigabitethernet-1/0/1] quit

[H3C] interface gigabitethernet 2/0/1

[H3C-gigabitethernet-2/0/1] undo stp enable

将接口vlan-interface 3加入安全域trust（步骤略），并配置源域为local，目的为trust的域间策略 。

创建对象组

[H3C]object-group ip address mad

[H3C-obj-grp-ip-mad] 0 network subnet 192.168.2.0 255.255.255.0

[H3C-obj-grp-ip-mad] quit

创建域间策略对象

[H3C]object-policy ip local-trust

[H3C-object-policy-ip-local-trust]rule 1 pass source-ip mad destination-ip mad

[H3C-object-policy-ip-local-trust]quit

创建域间策略，并引用域间策略对象

[H3C]zone-pair security source local destination trust

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

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

1.5.4 SecBlade III FW的接口及LB的配置步骤

（1） 创建ACL，允许内网10.1.0.0/16网段地址

[H3C] acl advanced 3500

[H3C-acl-ipv4-adv-3500] rule 0 permit ip source 10.1.0.0 0.0.255.255

[H3C-acl-ipv4-adv-3500]quit

（2） 创建聚合口RAG1和RAG2，将Slot 1和Slot 2的4个内联口分别加入聚合口RAG1和RAG2

[H3C]interface Route-Aggregation 1

[H3C-Route-Aggregation1]quit

[H3C]interface Ten-GigabitEthernet 1/0/1

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

[H3C-Ten-GigabitEthernet1/0/1]quit

依次将Ten1/0/2，Ten1/0/3，Ten1/0/4都加入聚合组RAG1

#

[H3C]interface Route-Aggregation 2

[H3C-Route-Aggregation2]quit

[H3C]interface Ten-GigabitEthernet 2/0/1

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

[H3C-Ten-GigabitEthernet2/0/1]quit

依次将Ten2/0/2，Ten2/0/3，Ten2/0/4都加入聚合组RAG2

#

创建聚合子接口RAG1.4011,RAG1.4012,RAG2.4011,RAG2.4012

[H3C]interface Route-Aggregation 1.4011

[H3C-Route-Aggregation1.4011]vlan-type dot1q vid 4011

[H3C-Route-Aggregation1.4011]quit

其他聚合子接口的配置略。

（3） 创建冗余口并应用NAT和冗余组的配置

#创建冗余口Reth2，IP地址为222.173.111.50/ 30，成员接口为RAG1.4011和RAG2.4011，其中RAG1.4011的优先级为100，RAG2.4011的优先级为50。开启保存上一跳功能。

[H3C] interface Reth 2

[H3C-Reth2] ip address 222.173.111.50 255.255.255.240

[H3C-Reth2] nat outbound 3500 address-group 1

[H3C-Reth2] nat server global 222.173.111.60 inside 10.1.0.6

[H3C-Reth2] member interface Route-Aggregation1.4011 priority 100

[H3C-Reth2] member interface Route-Aggregation2.4011 priority 50

[H3C-Reth2] ip last-hop hold

创建冗余口Reth3，IP地址为222.173.112.100/28，成员接口为RAG1.4012和RAG2.4012，其中RAG1.4012的优先级为100，RAG2.4012的优先级为50。开启保存上一跳功能。

[H3C] interface Reth 3

[H3C-Reth3] ip address 222.173.112.100 255.255.255.240

[H3C-Reth3] nat outbound 3500 address-group 2

[H3C-Reth3] member interface Route-Aggregation1.4012 priority 100

[H3C-Reth3] member interface Route-Aggregation2.4012 priority 50

[H3C-Reth3] ip last-hop hold

[H3C-Reth3] quit

创建内网入口冗余口Reth1，IP地址为10.1.0.1/16，成员接口为RAG1.4010和RAG2.4010，其中RAG1.4010的优先级为100，RAG2.4010的优先级为50。开启保存上一跳功能。

[H3C] interface Reth 1

[H3C-Reth1] ip address 10.1.0.1 255.255.0.0

[H3C-Reth1] member interface Route-Aggregation1.4010 priority 100

[H3C-Reth1] member interface Route-Aggregation2.4010 priority 50

[H3C-Reth1] ip last-hop hold

[H3C-Reth1] quit

#配置track，监测业务端口端口状态。

[H3C] track 1 interface Route-Aggregation1

[H3C] track 2 interface Route-Aggregation2

#配置冗余组1，创建Node 1，Node 1和FW1绑定，为主节点。关联的Track项为1。

[H3C] redundancy group 1

[H3C-redundancy-group-1] node 1

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

[H3C-redundancy-group-1-node1] priority 100

[H3C-redundancy-group-1-node1] track 1 interface Route-Aggregation1

#配置冗余组1，创建Node 2，Node 2和FW2绑定，为备节点。关联的Track项为2。

[H3C-redundancy-group-1] node 2

[H3C-redundancy-group-1-node2] bind slot 2

[H3C-redundancy-group-1-node2] priority 50

[H3C-redundancy-group-1-node2] track 2 interface Route-Aggregation2

[H3C-redundancy-group-1-node2] quit

将Reth1、Reth2和Reth3添加到冗余组中。

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

[H3C-redundancy-group-1] member interface reth 2

[H3C-redundancy-group-1] member interface reth 3

[H3C-redundancy-group-1] quit

（4） 将冗余口加入安全域并配置域间策略

#将内网接口Reth1和MAD检测接口vlan-interface3加入trust域
[H3C]security-zone name Trust
[H3C-security-zone-Trust]import interface reth 1
[H3C-security-zone-Trust] import interface Vlan-interface3

堆叠的两台设备需采用相同的型号，使用相同的版本。

SecBlade III FW的堆叠口请使用前面板的光口。

防火墙内联口需要聚合，并配置子接口作为上下行，再做冗余。

目前防火墙插卡不允许跨框流量，需要配置冗余组。