F5000-X系列V7防火墙多WAN链路负载均衡配置方法（命令行）

全局负载均衡 zhiliao_FO3qD 2018-11-25 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。

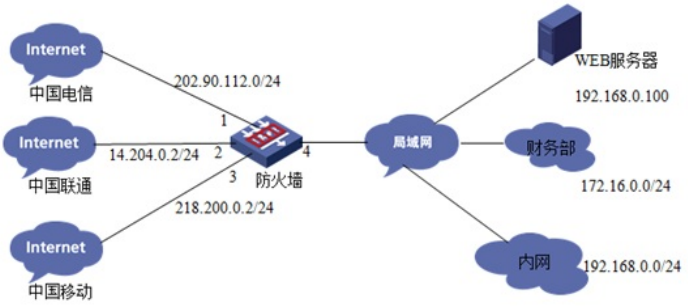
1.2 配置需求及实现的效果

某公司为达到业务流量快速转发和链路冗余需求申请了三条不同运营商的外网线路，需要实现如下需求：

1）要求内网用户访问目的地址为移动链路数据从移动链路转发、访问目的地址为联通链路数据从联通链路转发、访问目的地址为电信链路数据从电信链路转发需求。

2）财务部门因为经常访问网银等支付平台，目前不希望出口IP地址经常变化。指定财务数据从电信转发并希望当电信流量负载到带宽的90%后，后面流量负载到联通链路上。

2 组网图



说明：

ISP	外网接口	公网地址/掩码	公网网关
移动	1/0/3	218.200.5.8/24	218.200.5.9
联通	1/0/2	14.204.0.2/24	14.204.0.1
电信	1/0/1	202.90.112.2/24	202.90.112.1

配置步骤

3 配置步骤

3.1 创建NQA探测组用于链路探测

探测组名称为nqa，描述为test。用于检测链路健康性。

<H3C>system

[H3C]nqa template icmp nqa

[H3C-nqatplt-icmp-nqa]description test

[H3C-nqatplt-icmp-nqa]reaction trigger per-probe

[H3C-nqatplt-icmp-nqa]quit

3.2 基本组网配置

3.2.1 外网接口配置

配置电信链路接口地址，并开启保存上一跳功能。

[H3C]interface GigabitEthernet1/0/1

[H3C-GigabitEthernet1/0/1]ip address 202.90.112.2 255.255.255.0

[H3C-GigabitEthernet1/0/1]ip last-hop hold

[H3C-GigabitEthernet1/0/1]nat outbound

[H3C-GigabitEthernet1/0/1]quit

配置联通链路接口地址，并开启保存上一跳功能。

[H3C]interface GigabitEthernet1/0/2

[H3C-GigabitEthernet1/0/2]ip address 14.204.0.2 255.255.255.0

[H3C-GigabitEthernet1/0/2]ip last-hop hold

[H3C-GigabitEthernet1/0/2]nat outbound

[H3C-GigabitEthernet1/0/2]quit

配置移动链路接口地址，并开启保存上一跳功能。

[H3C]interface GigabitEthernet1/0/3

[H3C-GigabitEthernet1/0/3]ip address 218.200.5.8 255.255.255.0

[H3C-GigabitEthernet1/0/3]ip last-hop hold
[H3C-GigabitEthernet1/0/3]nat outbound
[H3C-GigabitEthernet1/0/3]quit

3.2.2 安全域及安全策略配置

将外网接口加入不信任区域
[H3C]security-zone name Untrust
[H3C-security-zone-Untrust]import interface Dialer1
[H3C-security-zone-Untrust]import interface GigabitEthernet1/0/1
[H3C-security-zone-Untrust]import interface GigabitEthernet1/0/2
[H3C-security-zone-Untrust]import interface GigabitEthernet1/0/3
[H3C-security-zone-Untrust]quit
创建对象策略pass，因为本章内容主要介绍负载均衡，域间策略采用最简配置请见谅。
[H3C]object-policy ip pass
[H3C-object-policy-ip-pass] rule 0 pass
[H3C-object-policy-ip-pass]quit
创建any到any域的域间策略调用pass策略。
[H3C]zone-pair security source any destination any
[H3C-zone-pair-security- Any-Any]object-policy apply ip pass
[H3C-zone-pair-security- Any-Any]quit

3.2.3 路由设置

设置路由防止在负载均衡配置前或者负载均衡失效后网络不通问题
[H3C]ip route-static 0.0.0.0 0 218.200.5.9 preference 80
[H3C]ip route-static 0.0.0.0 0 14.204.0.1 preference 70
[H3C]ip route-static 0.0.0.0 0 202.90.112.1

3.3 配置链路组

设置链路失败的reschedule：重定向连接，即把连接重定向到链路组中其它可用的链路上。并使用tran
sparent enable关闭链路组本身的NAT功能并绑定nqa探测组。

3.3.1 配置移动链路组

[H3C]loadbalance link-group cmcc
[H3C-lb-lgroup-cmcc]fail-action reschedule
[H3C-lb-lgroup-cmcc]transparent enable
[H3C-lb-lgroup-cmcc]probe nqa.
[H3C-lb-lgroup-cmcc]quit

3.3.2 配置联通链路组

[H3C]loadbalance link-group cnc
[H3C-lb-lgroup-cnc]fail-action reschedule
[H3C-lb-lgroup-cnc]transparent enable
[H3C-lb-lgroup-cnc]probe nqa.
[H3C-lb-lgroup-cnc]quit

3.3.3 配置电信链路组

[H3C]loadbalance link-group china-isp
[H3C-lb-lgroup-china-isp]fail-action reschedule
[H3C-lb-lgroup-china-isp]transparent enable
[H3C-lb-lgroup-china-isp]probe nqa
[H3C-lb-lgroup-china-isp]quit

3.3.4 配置财务链路组

[H3C]loadbalance link-group caiwu
[H3C-lb-lgroup-caiwu]fail-action reschedule
[H3C-lb-lgroup-caiwu]transparent enable
[H3C-lb-lgroup-caiwu]probe nqa
[H3C-lb-lgroup-caiwu]quit

3.4 配置链路

router ip指链路的网关地址，将链路绑定链路组后该链路才能生效。

3.4.1 配置移动链路

[H3C]loadbalance link cmcc-link
[H3C-lb-link-cmcc-link]router ip 218.200.5.9
[H3C-lb-link-cmcc-link]link-group cmcc

[H3C-lb-link-cmcc-link]probe nqa
[H3C-lb-link-cmcc-link]quit

3.4.2 配置联通链路

[H3C]loadbalance link cnc-link
[H3C-lb-link-cnc-link]router ip 14.204.0.1
[H3C-lb-link-cnc-link]link-group cnc
[H3C-lb-link-cnc-link]probe nqa
[H3C-lb-link-cnc-link]quit

3.4.3 配置电信链路

将电信链路带宽调整为100M，设置带宽繁忙比当带宽利用率超过90%*100M=90M，新建session会负载到其他链路。

[H3C]loadbalance link chinanet-link
[H3C-lb-link-cnc-chinanet-link]router ip 202.90.112.1
[H3C-lb-link-cnc-chinanet-link]link-group china-isp
[H3C-lb-link-cnc-chinanet-link]probe nqa
[H3C-lb-link-cnc-chinanet-link]max-bandwidth outbound 102400
[H3C-lb-link-cnc-chinanet-link]bandwidth outbound busy-rate 90
[H3C-lb-link-cnc-chinanet-link]quit

3.4.4 配置财务链路

[H3C]loadbalance link link-caiwu
[H3C-lb-link- link-caiwu] router ip 202.90.112.1
[H3C-lb-link- link-caiwu] link-group caiwu
[H3C-lb-link- link-caiwu]quit

3.5 配置负载均衡规则匹配运营商路由表

3.5.1 建立移动负载规则匹配移动数据

[H3C]loadbalance class cmcc type link-generic match-any
[H3C-lbc-link-generic-cmcc]match 1 isp cmcc
[H3C-lbc-link-generic-cmcc]quit

3.5.2 建立联通负载规则匹配联通数据

[H3C]loadbalance class cnc type link-generic match-any
[H3C-lbc-link-generic-cnc]match 1 isp cnc
[H3C-lbc-link-generic-cnc]quit

3.5.3 建立电信负载规则匹配电信数据

[H3C]loadbalance class chinanet type link-generic match-any
[H3C-lbc-link-generic-chinanet]match 1 isp chinatel
[H3C-lbc-link-generic-chinanet]quit

3.5.4 建立财务负载规则匹配172.16.0.0财务网段

[H3C] loadbalance class caiwu type link-generic match-any
[H3C-lbc-link-generic-caiwu]match 1 source ip address 172.16.0.0 24
[H3C-lbc-link-generic-caiwu]quit

3.6 配置负载均衡行为匹配各链路组

配置负载行为绑定各链路组，设置转发失败规则为继续匹配。

3.6.1 建立移动负载均衡行为匹配移动链路组

[H3C]loadbalance action cmcc type link-generic
[H3C-lbc-link-generic- cmcc]link-group cmcc
[H3C-lbc-link-generic- cmcc]fallback-action continue
[H3C-lbc-link-generic- cmcc]quit

3.6.2 建立联通均衡行为匹配联通链路组

[H3C]loadbalance action cnc type link-generic
[H3C-lbc-link-generic-cnc]link-group cnc
[H3C-lbc-link-generic-cnc]fallback-action continue
[H3C-lbc-link-generic-cnc]quit

3.6.3 建立电信负载均衡行为匹配电信链路组

[H3C]loadbalance action chinanet type link-generic

[H3C-lbc-link-generic-chinanet]link-group china-isp
[H3C-lbc-link-generic-chinanet]fallback-action continue
[H3C-lbc-link-generic-chinanet]quit

3.6.4 建立财务负载均衡行为匹配财务链路组

[H3C]loadbalance action caiwu type link-generic
[H3C-lbc-link-generic-caiwu]link-group caiwu
[H3C-lbc-link-generic-caiwu]fallback-action continue
[H3C-lbc-link-generic-caiwu]quit

3.7 配置负载均衡策略

负载均衡策略严格按照配置顺序进行匹配，如果需要财务数据优先匹配需要将优先配置。
[H3C]loadbalance policy 1 type link-generic
[H3C-lbp-link-generic-1]class caiwu action caiwu
[H3C-lbp-link-generic-1]class chinanet action chinanet
[H3C-lbp-link-generic-1]class cmcc action cmcc
[H3C-lbp-link-generic-1]class cnc action cnc

3.8 配置虚服务策略

配置LB虚服务，虚服务地址为0.0.0.0/0表示内网访问所有的数据将会匹配虚服务进行转发，lb策略调用之前创建的策略1，如果无法匹配运营商的数据缺省从移动转发。
[H3C]virtual-server outbound type link-ip
[H3C-vs-link-ip-outbound]virtual ip address 0.0.0.0 0
[H3C-vs-link-ip-outbound]lb-policy 1
[H3C-vs-link-ip-outbound]default link-group cmcc
[H3C-vs-link-ip-outbound]service enable
[H3C-vs-link-ip-outbound]quit

3.9 保存配置

[H3C]quit
<H3C>save force

3.10 配置验证

3.10.1 测试电信链路

在内网找一台地址为192.168.0.2的电脑，访问外网一个地址看是从哪个接口出？用来判断ISP路由是否配置正确？将外网模拟设备的IP地址修改为1.4.1.1进行测试。
设备内置的电信路由表：

```
<FW>display loadbalance isp name chinatel
(*) - User-defined object

LB ISP: chinatel
    Description: ChinaTel
    IPv4 address/Mask length:
        1.0.1.0/24              1.0.2.0/23              1.0.8.0/21
        1.0.32.0/19             1.1.0.0/24              1.1.2.0/23
        1.1.4.0/22              1.1.9.0/24              1.1.10.0/23
        1.1.12.0/22             1.1.16.0/20             1.1.32.0/19
        1.2.0.0/23              1.2.5.0/24              1.2.6.0/23
        1.2.9.0/24              1.2.10.0/23             1.2.12.0/22
        1.2.16.0/20             1.2.32.0/19             1.2.64.0/18
        1.3.0.0/16              1.4.1.0/24              1.4.2.0/23
```

Teacert结果：

```
C:\Users\Administrator>tracert 1.4.1.1

通过最多 30 个跃点跟踪到 1.4.1.1 的路由

  1    <1 毫秒   <1 毫秒   <1 毫秒 192.168.0.1
  2     1 ms     <1 毫秒   <1 毫秒 202.90.112.1
  3    <1 毫秒   <1 毫秒   <1 毫秒 1.4.1.1

跟踪完成。
```

防火墙会话：

```
Initiator:
  Source      IP/port: 192.168.0.2/1
  Destination IP/port: 1.4.1.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/15
  Source security zone: Trust
Responder:
  Source      IP/port: 1.4.1.1/5
  Destination IP/port: 202.90.112.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Start time: 2017-11-24 18:09:27  TTL: 29s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes
```

查看数据是否从对应链路组转发。

```
<FW>display loadbalance link statistics
Slot 1:
Loadbalance link: chinanet-isp
  Total connections: 1
  Active connections: 1
  Max connections: 1
  Connections per second: 0
  Max connections per second: 1
  Downstream traffic: 240 bytes
  Upstream traffic: 240 bytes
  Throughput: 0 bytes/s
  Inbound throughput: 0 bytes/s
  Outbound throughput: 0 bytes/s
  Max throughput: 120 bytes/s
  Max inbound throughput: 60 bytes/s
  Max outbound throughput: 60 bytes/s
  Received packets: 4
  Sent packets: 4
  Dropped packets: 0
```

3.10.2 测试联通链路

在内网找一台地址为192.168.0.2的电脑，访问外网一个地址看是从哪个接口出？用来判断ISP路由是否配置正确？将外网模拟设备的IP地址修改为27.50.128.1进行测试。

设备内置的联通路由表：

```
<FW>display loadbalance isp name cnc
(*) - User-defined object

LB ISP: cnc
    Description: CNC
    IPv4 address/Mask length:
        1.24.0.0/13             1.56.0.0/13             1.116.0.0/15
        1.188.0.0/14            14.204.0.0/15           27.0.128.0/22
        27.0.132.0/22           27.8.0.0/13             27.36.0.0/14
        27.40.0.0/13            27.50.128.0/17          27.54.192.0/18
        27.98.224.0/19          27.112.0.0/18           27.115.0.0/17
        27.192.0.0/11           36.32.0.0/14            36.248.0.0/14
```

Teacert结果：

```
C:\Users\Administrator>tracert 27.50.128.1

通过最多 30 个跃点跟踪到 27.50.128.1 的路由

  1    <1 毫秒   <1 毫秒   <1 毫秒 192.168.0.1
  2    <1 毫秒   <1 毫秒   <1 毫秒 14.204.0.1
  3    <1 毫秒    2 ms    <1 毫秒 27.50.128.1

跟踪完成。
```

防火墙会话：

```
Initiator:
  Source      IP/port: 192.168.0.2/1
  Destination IP/port: 27.50.128.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/15
  Source security zone: Trust
Responder:
  Source      IP/port: 27.50.128.1/22
  Destination IP/port: 14.204.0.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Start time: 2017-11-24 18:23:32  TTL: 29s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes
```

.

3.10.3 测试移动链路

在内网找一台地址为192.168.0.2的电脑，访问外网一个地址看是从哪个接口出？用来判断ISP路由是否配置正确？将外网模拟设备的IP地址修改为43.251.244.1进行测试。

设备内置的移动路由表：

```
<FW>display loadbalance isp name cmcc
(*) - User-defined object

LB ISP: cmcc
    Description: CMCC
    IPv4 address/Mask length:
        36.128.0.0/10           36.192.0.0/11           39.128.0.0/10
        43.239.172.0/22         43.247.240.0/22         43.251.244.0/22
        45.121.68.0/22          45.121.72.0/22          45.121.172.0/22
        45.121.176.0/22         45.122.96.0/21          45.123.152.0/22
        45.124.36.0/22          45.125.24.0/22          61.232.0.0/14
        61.236.0.0/15           101.144.0.0/12          103.3.128.0/22
        103.20.112.0/22         103.21.176.0/22         103.35.104.0/22
        103.61.156.0/22         103.61.160.0/22         103.62.24.0/22
```

Teacert结果：

```
C:\Users\Administrator>tracert 43.251.244.1

通过最多 30 个跃点跟踪到 43.251.244.1 的路由

  1    <1 毫秒   <1 毫秒   <1 毫秒 192.168.0.1
  2    <1 毫秒   <1 毫秒   <1 毫秒 218.200.5.8
  3    <1 毫秒   <1 毫秒   <1 毫秒 43.251.244.1

跟踪完成。
```

防火墙会话：

```
Initiator:
  Source      IP/port: 192.168.0.2/1
  Destination IP/port: 43.251.244.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/15
  Source security zone: Trust
Responder:
  Source      IP/port: 43.251.244.1/2
  Destination IP/port: 218.200.5.9/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Start time: 2017-11-24 18:17:10  TTL: 29s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes
```

3.10.4 测试总结

测试结果符合需求预期，可以达到数据的准确转发。

配置关键点