# V7防火墙双WAN上网主备模式（命令行）配置案例

设备部署方式 张新姿 2021-06-19 发表

组网及说明

## 1 配置需求或说明

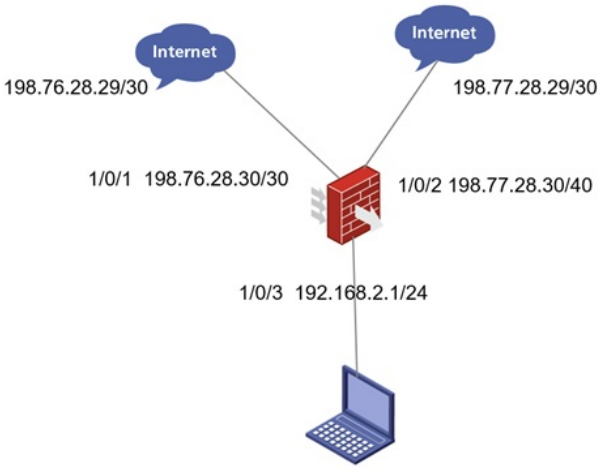
### 1.1 适用产品系列

本案例适用于软件平台为Comware V7系列防火墙：本案例适用于如F1000-A-G2、F1000-S-G2、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙。

### 1.2 配置需求及实现的效果

防火墙F100-A-G2双WAN口上网，WAN口1采用静态地址，地址为198.76.28.30 (运营商下一跳198.76.28.29)，WAN口2采用也采用静态地址，地址为198.77.28.30 (运营商下一跳198.77.28.29)。需要实现内网用户访问外网从WAN1口出去，当WAN1断掉切换到WAN2。

## 2 组网图



配置步骤

# 1 配置步骤

## 3.1配置防火墙基本上网

# 外网接口G1/0/1配置运营商给的静态ip地址
interface GigabitEthernet1/0/1
ip address 198.76.28.30 255.255.255.252
nat outbound
# 外网接口G1/0/2配置运营商给的静态ip地址
interface GigabitEthernet1/0/2
ip address 198.77.28.30 255.255.255.252
nat outbound
# 内网接口G1/0/3配置自定义的内网静态ip地址
interface GigabitEthernet1/0/2
ip address 192.168.2.1 255.255.255.0
#将内网接口加入trust域
security-zone name trust
 import interface GigabitEthernet1/0/3
#将两个外网接口分别加入untrust1和untrust2域
security-zone name Untrust1
 import interface GigabitEthernet1/0/1
security-zone name Untrust2
 import interface GigabitEthernet1/0/2

#配置安全策略
security-policy ip
 rule 0 name trust-untrust（放通内网到外网的访问）
  action pass
  source-zone trust
  destination-zone untrust1
  destination-zone untrust2
 rule 1 name per-nqa　　（放通local安全域到外网探测地址114.114.114.114的访问，如不配置则无法正常使用nqa探测外网地址）
  action pass
  source-zone local
  destination-zone untrust1
  destination-zone untrust2
  destination-ip-host 114.114.114.114

## 3.2 配置链路检测

#创建管理员名为admin、操作标签为test的NQA测试组
[H3C]nqa entry admin test
#配置测试类型为ICMP-echo，ICMP-echo测试利用ICMP协议，根据是否接收到应答报文判断目的端设备的可达性。ICMP-echo测试的功能与ping命令类似，但ICMP-echo测试中可以指定测试的下一跳设备。在源端和目的端设备之间存在多条路径时，通过配置下一跳设备可以指定测试的路径
[H3C-nqa-admin-test-icmp-echo] type icmp-echo
配置监测公网的任意地址如114.114.114.114等，这样就可以规避掉运营商本身出现网络故障的风险
[H3C-nqa-admin-test-icmp-echo] destination ip 114.114.114.114
#配置测试组连续两次测试的时间间隔为3000ms
[H3C-nqa-admin-test-icmp-echo] frequency 3000
#配置探测报文的下一跳IP地址，这个一般在探测的目的地址不是网关地址的时候建议配置，本案例探测的目的地址是直连网关地址，可以不配置下一跳地址
[H3C-nqa-admin-test-icmp-echo] next-hop 198.76.28.29

#配置联动项1（连续失败3次触发联动）
[H3C-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
[H3C-nqa-admin-test-icmp-echo]quit
#启动探测
[H3C] nqa schedule admin test start-time now lifetime forever
#配置Track项1，关联NQA测试组（管理员为admin，操作标签为test）的联动项1
[H3C] track 1 nqa entry admin test reaction 1

3.3配置静态路由

# 进入系统视图，配置两条默认路由，并且修改G1.0.2线路的默认路由优先级为80（默认路由优先级为60，值越大优先级越低）。设备固定IP上网路由与Track项1关联，作为主用路由。实现正常情况下流量全部从WAN1出去，链路出现故障时可切换到WAN2。

[H3C]ip route-static 0.0.0.0 0 198.76.28.29 track 1

配置关键点 te-static 0.0.0.0 0 198.77.28.29 preference 80

# 1 注意事项

## 1 保存配置信息

1、两条默认路由主备使用且备份，因此设置路由优先级，如果负载使用等价路由也可以分流互备的效果，只需将优先级设置一致即可

[H3C]save force 2、双出口做NAT，需要将双出口加入不同安全域。

# 2 查看与验证

# 两条链路都正常的时候track项状态为positive，路由也是走优先级为60的G1/0/1。