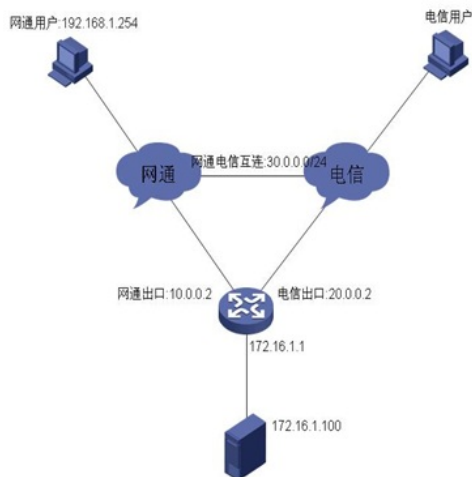


问题描述

nat server多出口问题分析及各种产品的配置案例

解决方法

双出口nat问题



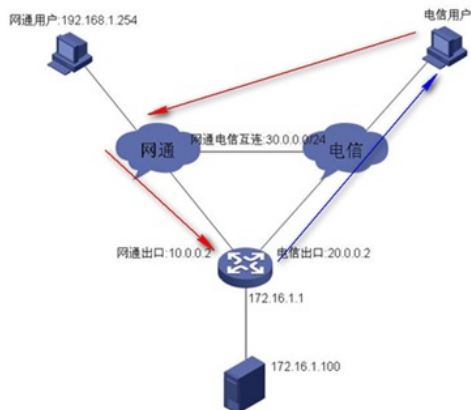
注意：私网服务器不能同时在2个外网口同时映射。（可以将一个服务的同一个网卡配置2个ip地址）
拓扑如上图，用户有两条线路上外网，一条由电信提供，一条由网通提供。内网用户上网要求访问电信网络走电信出口，访问网通网络走网通出口。目前的处理方法都是在路由器上配置网通的具体路由来实现的，访问网通按精确路由转发，访问电信按缺省路由转发。现在有一内部SERVER需要在网通出口对外映射，对整个公网提供服务，映射后网通用户访问正常，而电信用户则无法访问。

一、 过程分析：

由于互联网上网通用户访问该服务器的服务正常，在此有作分析。

这里主要分析互联网上电信用户访问该服务器的一流程。互联网上电信用户通过互联网上的路由到达连接网通的出口，根据该设备上的内部服务器的映射配置，将映射的公网IP地址转换为内部服务器的私网IP地址，再根据设备的路由信息将数据报文送到服务器。

服务器将数据报文返回给电信用户时，在核心交换机上选路时就将该报文送到路由器上，在该路由器上根据路由信息及NAT转换配置，将报文的源地址（内部服务器的地址）转换为网通的地址，从电信的出口发出去。从而导致来回电信用户访问网通接口地址来回路径不一致，数据流程图如下：



从以上分析可以看到数据往返不走同一条路不会影响到业务的，但实现的网络中却有此问题，默认情况下就会造成交互报文在公网走的路径不一致，而一般的公网环境中可能存在对单播报文来回路径进行检测的设备，那样的话就会把这些交互报文过滤掉，导致业务不通。

二、 解决方法：

为了避开运营商的这种检查，只能让SERVER的应答报文从网通出口出去，可以通过策略路由来实现

，保证来回路径一致即可。SR66的可以通过基于反向入接口的接口策略路由，安全产品可以通过“保存上一跳”来实现。如遇到用户有这种组网，具体思路就是保证来回路径一致，具体型号的实现，可以咨询二线。

三、案例

提供3个案例分别是MSR、SR66和SR88如何实现的多出口nat server的问题。

1)MSR的实现方法，通过策略路由实现：

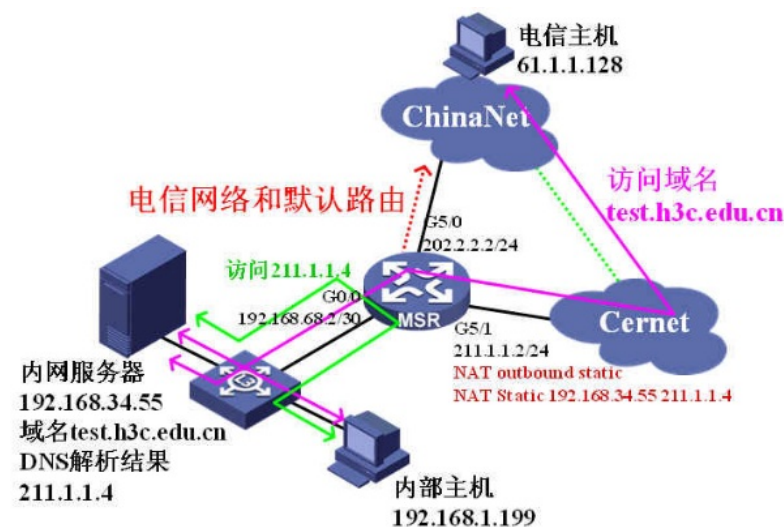
MSR系列路由器教育网双出口NAT服务器的典型配置

一、组网需求：

MSR的G0/0连接某学校内网，G5/0连接电信出口，G5/1连接教育网出口，路由配置：访问教育网地址通过G5/1出去，其余通过默认路由通过G5/0出去。电信网络访问教育网地址都是通过电信和教育网的专用连接互通的，因此电信主机访问该校都是从G5/1进来，如果以教育网源地址（211.1.1.0/24）从G5/0访问电信网络，会被电信过滤。该校内网服务器192.168.34.55需要对外提供访问，其域名是test.h3c.edu.cn，对应DNS解析结果是211.1.1.4。先要求电信主机和校园网内部主机都可以通过域名或211.1.1.4正常访问，且要求校园网内部可以通过NAT任意访问电信网络或教育网络。

设备清单：MSR一台

二、组网图：



三、配置步骤：

适用设备和版本：MSR系列、Version 5.20, Release 1205P01后所有版本。

MSR关键配置(路由部分配置略)

```

#
//地址池0用于访问电信的NAT
nat address-group 0 202.2.2.50 202.2.2.100
//地址池1用于访问教育网的NAT
nat address-group 1 211.1.1.50 211.1.1.100
//静态NAT用于外部访问内部服务器test.h3c.edu.cn
nat static 192.168.34.55 211.1.1.4
#
//ACL 2000用于内网访问教育网和电信的NAT，允许192.168.0.0/0的源
acl number 2000
description "NAT"
rule 10 permit source 192.168.0.0 0.0.255.255
//ACL 2222用于策略路由的允许节点，即内部服务器往外发的HTTP从G5/1出去
acl number 2222
description "policy-based-route permit node"
rule 0 permit source 192.168.34.55 0
#
//用于内部主机访问211.1.1.4的NAT映射
acl number 3000
description "192.168.0.0/24 access 211.1.1.4"
rule 0 permit ip source 192.168.0.0 0.0.255.255 destination 192.168.34.55 0
//ACL 3333用于策略路由拒绝节点，即内部服务器返回内部主机的不需要被策略
acl number 3333
description "policy-based-route deny node"
rule 0 permit ip source 192.168.34.55 0 destination 192.168.0.0 0.0.255.255
#
interface GigabitEthernet0/0
port link-mode route
//内部主机访问211.1.1.4时，将211.1.1.4替换成192.168.34.55
nat outbound static
//内部主机访问211.1.1.4时，将内部主机地址转换成192.168.86.2
nat outbound 3000
description to neibu-Lan
ip address 192.168.86.2 255.255.255.252
//策略路由，内部服务器返回内部的不被策略，返回外部的从G5/1出去
ip policy-based-route aaa
#
interface GigabitEthernet5/0
port link-mode route
//内部访问电信时需要NAT
nat outbound 2000 address-group 0
description connect to ChinaNet
ip address 202.2.2.2 255.255.255.0
tcp mss 1420
#
interface GigabitEthernet5/1
port link-mode route
//外部访问内部服务器211.1.1.4时静态转换成192.168.34.55
nat outbound static
//内部访问教育网时需要NAT
nat outbound 2000 address-group 1
description connect to Cernet
ip address 211.1.1.2 255.255.255.0
tcp mss 1420
#
//策略路由aaa拒绝节点序号3
policy-based-route aaa deny node 3
//匹配条件ACL 3333，即内部服务器返回内部的流量不需要被策略
if-match acl 3333
//策略路由aaa允许节点5
policy-based-route aaa permit node 5
//匹配ACL 2222，即内部服务器发出的流量
if-match acl 2222
//应用下一跳211.1.1.1，即从G5/1出去
apply ip-address next-hop 211.1.1.1
#

```

四、配置关键点：

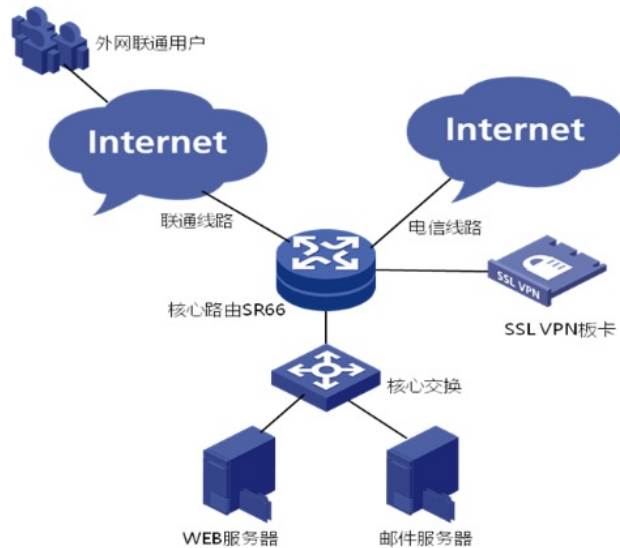
- 1) 此案例所实现之功能只在MSR上验证过，不同设备由于内部处理机制差异不能保证能够实现；
- 2) 策略路由是保证内部服务器返回外网的流量从G5/1出去，如果不使用策略路由会按照普通路由转发从G5/0出去，这样转换后的源地址211.1.1.4会被电信给过滤掉，因此必须使用策略路由从G5/1出去；
- 3) 策略路由的拒绝节点的作用是只要匹配ACL就变成普通路由转发，而不被策略；
- 4) 在G0/0应用2个NAT的作用是使内网可以通过访问211.1.1.4访问内部服务器test.h3c.edu.cn，如果只使用NAT Outbound Static，那么内部主机192.168.1.199发送HTTP请求的源、目的地址对<192.168.1.199, 211.1.1.4>会变成<192.168.1.199, 192.168.34.55>然后发送给内部服务器，那么内部服务器会把HTTP响应以源、目的地址对<192.168.34.55, 192.168.1.199>直接返回给内部主机（192.168.1.199可以经过内部路由不需要经过MSR到达）因此对于内部主机来说始终没有接收到211.1.1.4返回的HTTP响应，因此打开网页失败。解决问题的办法就是让内部服务器返回时经过MSR路由器，让MSR把HTTP响应<192.168.34.55, 192.168.1.199>变成<211.1.1.4, 192.168.1.199>，方法就是再做一次NAT，通过NAT Outbound ACL 3000使HTTP请求变成MSR发送的<192.168.86.2, 192.168.34.55>，这样HTTP响应就会变成<192.168.34.55, 192.168.86.2>发送到MSR，MSR再变成<211.1.1.4, 192.168.1.199>返回给内部主机。

2)SR66的实现方法，通过基于反向入接口的接口策略路由

SR6604双运营商出口对外NAT映射案例（来回路径不一致）

组网环境：

核心路由器SR6604采用联通、电信双出口，为了实现出口负载均衡，通过添加联通网段静态路由，缺省路由指向电信出口。内网服务器（WEB、Mail、SSL VPN）通过联通地址实现一对一静态映射，对外提供服务。



二、问题描述：

客户反馈近期突然部分外网联通用户无法正常访问中心各服务器地址，该类外网用户存在共性：用户地址均不在路由器中的联通静态路由地址段中。而在路由器上添加该的地址段后，就可以进行正常访问。

三、问题原因：

通过排查发现，不能正常访问的用户，数据流量均通过联通线路送达路由器，但内网服务器进行回包时，在路由器上查询NAT表项，以联通外网地址为源进行转换，由于路由表中不存在该目的用户网段明细路由，只能通过电信线路送出，但电信运营商近期添加新策略后，对源地址进行检测，检测到非电信地址会进行丢弃，数据包在电信内部传输的时候被丢弃，所以会有不通的现象发生。总而言之，造成该问题的原因就是数据流从联通进入，电信发出，但NAT转换后的地址为联通地址，电信又将该地址的数据进行丢弃。

四、解决办法：

通过添加在SR66路由器上添加所有联通网段的路由，可以解决该问题，从而实现联通进，联通出。但实际情况联通路由地址段无法收集完全，用户又对外提供服务,无法得知源地址归属，所以该方法解决起来十分复杂且不现实。

通过PBR策略，在路由器连接服务器的接口处调用策略路由，策略路由由中if-match reverse-input-interface Ethernet2/2/0（联通接口），再重定向下一跳至联通线路出口。最终实现，联通外网用户访问的流量从联通线路进入，回程报文再从联通接口送出。其它访问流量均走电信线路，通过该方案既能实现数据流向来回路径一致，又能起到双出口负载均衡的目的。

3)SR88的实现方法，通过策略路由实现。

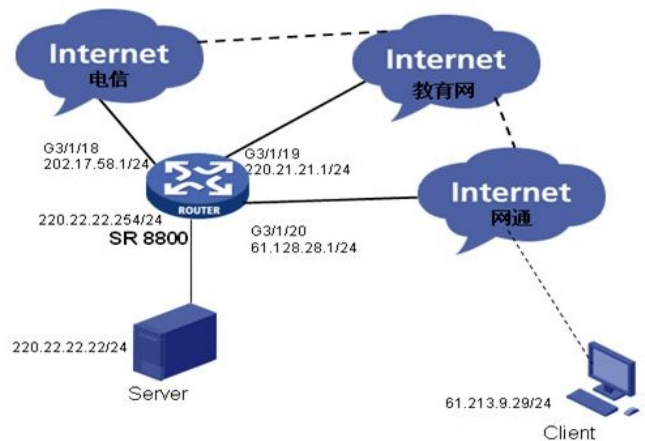
SR8800 NAT应用之保证报文来回公网路径一致的配置

一、组网需求：

某学校用户网络中有多台内部服务器，这些服务器采用的都是教育网地址。该校有三个公网出口，一个电信、一个网通、一个教育网，存在部分网通或电信的公网用户通过教育网地址直接访问这些内部服务器的需求。

二、组网图：

如下组网中，某大学用户内部有一台配置教育网地址220.22.22.22的内部服务器，该服务器在电信、网通两个出口都做了NAT-server的绑定，保证电信、网通的用户也能直接访问这台服务器，教育网的用户则直接通过220.22.22.22访问服务器。同时配置了静态路由，目的地址是网通的从网通走，目的地址是教育网的从教育网出口走，其他目的地址的从电信出口走。



三、配置步骤:

1. 配置思路

首先我们了解下不做特殊处理的情况下，报文的交互过程。

从公网61.213.9.29这台PC机直接通过220.22.22.22这个教育网地址访问内部服务器，正向报文就会从网通跳到教育网，然后再从该校SR88的教育网出口G3/1/19进入，因为G3/1/19上没有配置NAT-Server转换，所以该报文不用经过NAT转换，就直接转发给了内部服务器。内部服务器的回应报文发到SR88后，因为没有匹配的Nat Session，该报文就会直接走路由转发，因为目的地址61.213.9.29是网通地址，就会从网通出口转发出去。

如上分析，默认情况下就会造成交互报文在公网走的路径不一致，而一般的公网环境中可能存在对单播报文来回路径进行检测的设备，那样的话就会把这些交互报文过滤掉，导致业务不通。

所以，我们对配置进行修改的目的就非常明确：将内部服务器发回给公网用户的报文从进来的那个口发回去：

- 1) 因为针对这种特殊的应用时内部服务器的回应报文没有经过NAT转换，所以报文锁定可以通过报文的源地址匹配；
- 2) 因为这项特殊的应用中报文都是从教育网口进来的，所以我们只需把所有锁定的报文重定向到教育网出口；

2. 配置方法

2.1 首先配置用户的当前组网配置（省略，参考其他典型配置）

2.2 配置MQC，保证源地址是Nat-Server教育网地址的报文下一跳指向教育网出口

```
Acl num 200
rule 0 permit source 220.22.22.0
traffic-classifier 123
if-match acl 2000
traffic-behavior 123
redirect next-hop 220.21.21.2
qos policy 123
classifier 123 behavior 123
2.3在网通、电信出口的outbound方向下发qos-policy 123
interface GigabitEthernet3/1/20
qos apply policy 123 outbound
interface GigabitEthernet3/1/18
qos apply policy 123 outbound
```

四、配置关键点:

- 1、如果教育网出口上做了nat-outbound配置，务必注意nat-outbound匹配的私网地址范围，绝对不能包含nat-server的私网地址。
- 2、该重定向MQC策略必须下发在公网出接口的outbound方向。
- 3、对于电信用户直接访问内部服务器网通地址等等之类的应用，也可以使用同样的方法保证来回路径一致。
- 4、如果用户通过nat-static部署内部服务器，使得内部服务器可以主动发起对外网的访问，如果存在多个出口，也需要通过这种方法来保证来回路径一致。
- 5、如果NAT出接口在SPC单板上，则不支持出方向的重定向配置，即不适用该方法。