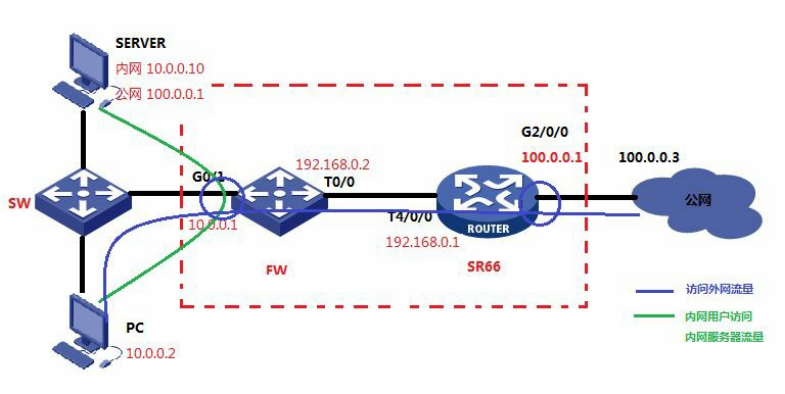
SR66系列路由器作为出口网关NAT+FW插卡配合使用经验案例

NAT 何理 2014-05-08 发表

一、组网

客户在网络出口部署了一台SR66路由器作为出口路由器，网络内部有一台服务器，客户希望可以在外网访问这台服务器，同时内网用户也可以在内网通过公网地址访问该服务器。作为网络出口，为保证网络安全性，客户同时为该SR66路由器配置了一块防火墙插卡，但是防火墙插卡在与NAT配合使用时存在一定的限制，本文将为大家介绍一下几种不同的使用方法。



1. 配置说明

在普通情况下，既没有防火墙插卡时，我们仅需在G2/0/0与G2/0/1配置相关NAT，即：

1）外网口配置：NAT Server（外网用户访问内网服务器）；
NAT OUTbound（内网用户访问外网）；

2）内网口配置：NAT Server（将公网服务器地址转换为私网地址）；
NAT OUTbound（将源IP改为网关IP地址，保证内网用户使用公网地址访问内网服务器时来回路径一致）；

二、 问题描述：

1. 公网口与内网口不在同一个线卡上

当SR66插上防火墙插卡，且内外网口不在同一个线卡上，当我们按照上述没有防火墙插卡时的配置进行配置时，可以正常使用，内网外网均可正常访问。

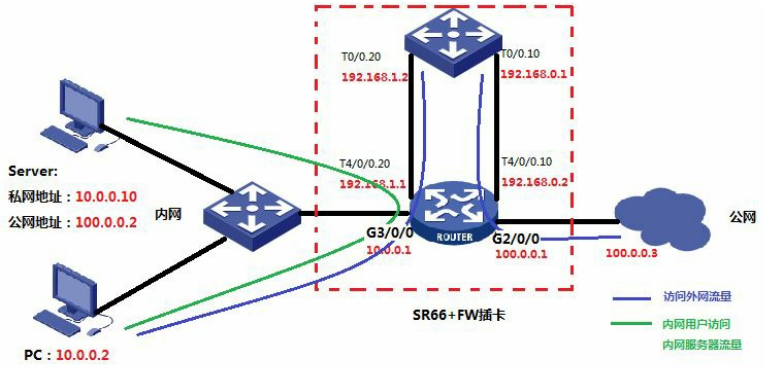
2. 公网口与内网口在同一线卡上

当SR66插上防火墙插卡，但是内外网口在同一个线卡上时，如果我们继续按照上述方式配置NAT，那么我们便会发现，虽然可以使用公网地址访问内网服务器，但是此时会出现不能访问外网的问题。

三、过程分析：

1. 公网口与内网口不在同一个线卡上

当公网口与内网口不在同一个线卡上，我们也仅需按照正常配置即可，其内网用户访问Server流量与内网用户访问外网流量如图所示：



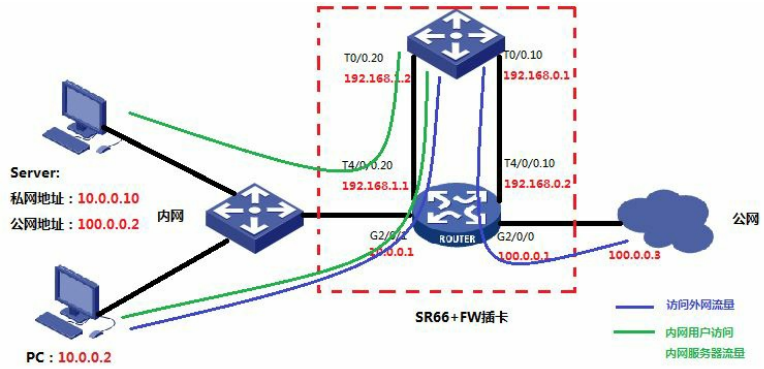
上图中G3/0/0为内网口，G2/0/0为公网口，内网用户10.0.0.2通过公网地址100.0.0.2，访问内网Server，报文地址转换过程如下：

过程	源地址	目的地址	作用
PC	10.0.0.2	100.0.0.2	PC通过公网地址访问内网服务器器
G3/0/0 NAT Server	10.0.0.2	10.0.0.10	将公网地址为私网地址
G3/0/0 NAT Outbound	10.0.0.1	10.0.0.10	将源地址转换为网关地址，保证来回路径一致
Server回复	10.0.0.10	10.0.0.1	回复给网关
之后为逆向转换			

访问到外网的报文，到达G3/0/0后，经过匹配策略路由经T4/0/0.20上防火墙，在防火墙上通过静态路由由T0/0.10回到路由器，然后到达G2/0/0接口，通过NAT OUTbound将源地址转换为公网地址访问公网。

2. 公网口与内网口在同一个线卡上

当内网口与外网口在同一线卡上时，此时重定向到Firewall的流量，回到该线卡会出现session被命中而直接转发流量的现象，导致外网口未作NAT转换就把流量转发出去，私网地址流出到公网，从而导致不能访问外网。此时需要将内网口的NAT配置转移到T0/0.20，如图所示：



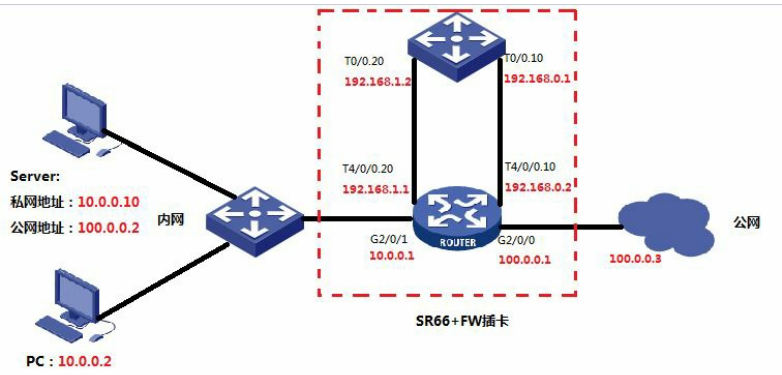
上图中，我们将内网口的NAT配置移到了防火墙的T0/0.20接口，这样就避免了同一块线卡的session冲突，报文通过G2/0/1接口的PBR后上送到防火墙进行NAT转换，转换过程见下表：

过程	源地址	目的地址	作用
PC	10.0.0.2	100.0.0.2	PC通过公网地址访问内网服务器器
T0/0.20 NAT Server	10.0.0.2	10.0.0.10	将公网地址为私网地址
T0/0.20 NAT Outbound	192.168.1.2	10.0.0.10	将源地址转换为网关地址，保证来回路径一致
Server回复	10.0.0.10	192.168.1.2	回复给网关
回复给网关，需要保证中间有路由可以让报文送到SR66路由器。			

注意：使用这种方式时，需要内网服务器公网地址（100.0.0.2）与公网接口地址（100.0.0.1）为不同的地址，这样报文可以被PBR上送到防火墙从而进行NAT转换。
当公网接口地址与内网服务器地址为同一个地址时，当报文到达路由器内网接口G2/0/1，因为目的地址为本地地址，所以不会匹配PBR，从而不能到达防火墙进行NAT。这种情况下，需要对客户组网进行改动使用另一种方式。

3. 单线卡+公网接口地址与内网服务器地址为同一个地址

如果只有一块线卡，但是公网接口地址与服务器公网地址相同时，需要将内网接口移到防火墙的面板接口上，使用防火墙的接口作为内网口，相关的NAT配置在防火墙接口上，公网口配置不变。如图所示：



按照这种组网，内网流量直接上防火墙，不需经过内联口引流。

1）内网用户通过公网地址访问内网服务器时，报文到达防火墙G0/1口直接进行NAT Server与NAT OUTbound，从而访问内网服务器；

2）访问公网的流量直接经过G0/1口到达防火墙，经路由通过内联口到达SR66路由器，然后从G2/0/0口经过NAT OUTbound访问公网，因为此时内网口与公网口不在一个线卡上，所以不存在之前session的问题；

3）使用这样的组网时需要将防火墙插卡的内网口加入到正确的域中，并配置好相应的域间策略。

四、 解决方法

已在分析过程中详细介绍，在此不再赘述。