

1、这是一个项目上的实施案例，网络图如上，项目现场有两个外网出口，一个是电信出口（port5），另一个是联通出口(port6)。内网中有一台服务器10.10.10.171，通过配置虚拟IP把它映射到电信出口port5上。

客户的需求是，无论是内网用户还是外网用户，都统一使用port5的公网IP（58.213.63.170）来访问10.10.10.171那台内网服务器。

2、而且，客户还有别的需求，客户的内网有很多网段，客户把它们划分成了两组（如下图），第一组是走电信出口（port5），第二组是走联通出口(port6)。

例如，拓扑图中的PC1是属于10.10.30.0网段（23位掩码），所以它访问外网走的是联通出口(port6)。而拓扑图中的PC2是属于10.10.14.0网段，所以它走的是电信出口（port5）。

这个项目的特殊之处就在于，PC1访问外网地址时有时候会出现问题，为什么呢？因为按照客户的规划，PC1访问外网是要走联通出口(port6)，但是，上面我们又说到，内网那台服务器10.10.10.171，映射到了电信出口port5的公网IP上，这种情况下，PC1通过公网IP访问内网服务器，就有可能出问题。

所以，为了规避问题，并实现客户所有的目标，配置防火墙的时候，要费些周折。



3、首先，是关于路由的配置，对于电信IP组的那些内网网段，通过“静态路由”指引它们从电信出口（port5）出去；而对于联通IP组的那些内网网段，通过“策略路由”指引它们从联通出口(port6)出去。

我们先看看电信IP组的静态路由，如下：



然后，再看看联通IP组的策略路由，如下：



4、此外，我们还要考虑“内网用户通过公网IP访问内网服务器”这个需求，这个业务的过程是这样的，例如，内网PC1请求电信出口port5的公网IP，请求报文刚离开PC1时，目的地址是公网IP，后来从port2口进入了防火墙，然后防火墙把目的地址的公网IP做了NAT，转换成内网服务器地址10.10.10.171，接下来再从port2发出去。

所以，为了让所有内网用户，都能通过port5的公网IP访问内网服务器，需要配置一条策略路由，让内网请求报文从port2进去，然后做了NAT之后，再从port2出来回到内网，防止它从外网口跑掉。

为啥说还要防止内网请求报文从外网口跑掉？因为在上面的第3步，对于联通IP组的那些内网网段，配置了“策略路由”指引它们从联通出口(port6)出去。而PC1请求电信出口port5的公网IP时，防火墙做了目的NAT转换，但是请求报文中的源IP现在还是10.10.30.0网段，它会匹配第3步的那条策略路由。

所以，既要新增一条“内网通过公网IP访问内网服务器”的策略路由，还要保证这条策略路由会优先被匹配，也就是说比第3步的那条策略路由更优先，只需要把它排在策略路由表的最上面就行。



这条策略路由的详情如下：



5、配置虚拟IP，让电信出口port5的地址，映射到内网服务器10.10.10.171。



6、配置“由外到内”的策略，目的地址是上面那个虚拟IP



7、然后再配置“由内到外”的策略。前面说到，客户把内网划分成了两组，第一组是走电信出口（port5），第二组是走联通出口(port6)。所以，你可能认为，策略的源地址应该配置成下面这个样子：电信IP从port5走，联通IP从port6走。

但是，实践证明，下面的配置是错误的，这种配置会导致一个问题，那就是，对于联通IP组的那些内网网段，不能通过公网IP访问内网服务器，业务不通。因为内网服务器映射的公网IP是在电信出口port5上。



为了让所有内网用户，都能通过port5的公网IP访问内网服务器，那么正确的配置如下，你懂的！

