双向NAT典型配置技术案例

NAT　刘志伟　2015-11-16 发表

A单位是保密单位，搭建了IP信息专网，有多个分部。社会单位通过A单位的外网接入进来，希望能够共享A单位的信息。同时，A单位希望也能够通过新建网访问社会单位信息。在互相访问时，双方都希望互相隐藏服务器的实际地址。

为了安全起见，在双方地址都不可以见的情况下，实现互通，在配置NAT时，需要使用双向NAT。举例来说，实现原本A地址访问B地址，经过设备后，最终实现源和目的都被转换，数据包变为A’地址访问B’地址，实现隐藏双方地址进行互通的目的。

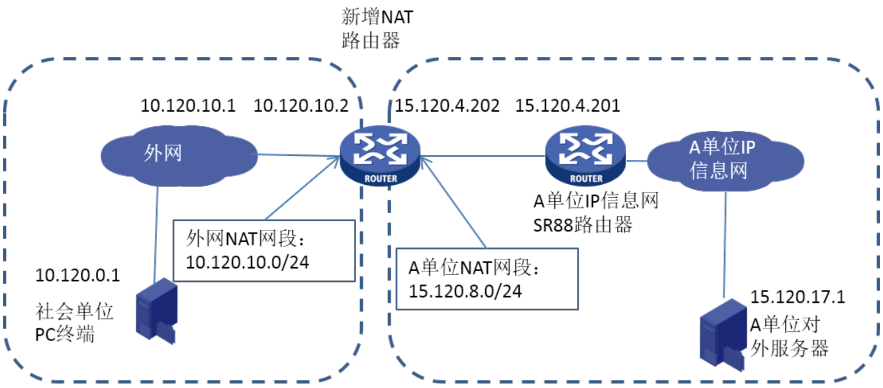

图1 社会单位共享A客户IP信息网配置说明图

详细双向NAT过程结合图1双向NAT详图说明如下：

社会单位内网主机（10.120.0.1）访问A客户IP信息网服务器（15.120.17.1）的资源时：

1） 需要对A客户网服务器地址进行隐藏，让社会单位主机访问的地址为10.120.10.10，也就是说社会单位内网主机发起的连接为：10.120.0.1——10.120.10.10；
2） 在进入NAT设备时，将这个数据流目的地址转换，变为10.120.0.1——15.120.17.1；
3） 在流出NAT设备时，将这个数据流源地址转换，变为15.120.8.1——15.120.17.1；
4） 在A客户网服务器看来是15.120.8.1访问了它，这样就实现了隐藏社会单位内网主机地址的目的。

A客户IP信息网服务器（15.120.17.1）访问社会单位内网主机（10.120.0.1）的资源时，情况类似，访问的目的地址为15.120.8.1，不再赘述。

另外，A客户网服务器（15.120.17.1）和社会单位内网主机（10.120.0.1）对应的地址，需要在NAT设备上添加静态路由，使得交互报文能够找到对应的出接口，正确地进行NAT转换。

同时，在A客户SR88路由器上回指新增A客户网的NAT网段到新增NAT路由器设备；需要在外网与新增NAT路由器设备相连的路由设备上，回指新增外网的NAT网段到新增NAT路由器设备。

结合社会单位共享A客户IP信息网配置说明图（图1），新增NAT路由器上，相关双向NAT和路由配置举例如下。

```
#
nat static outbound 15.120.17.1 10.120.10.10
nat static outbound 10.120.0.1 15.120.8.1
#
interface GiAbitEthernet0/0
port link-mode route
ip address 10.120.10.2 255.255.255.252
nat static enable
#
interface GiAbitEthernet0/1
port link-mode route
ip address 15.120.4.202 255.255.255.252
nat static enable
#
ip route-static 15.0.0.0 255.0.0.0 15.120.4.201
```

```
ip route-static 10.0.0.0 255.0.0.0 10.120.10.1
#
```

A客户IP信息网分部SR8808路由器上需要添加地址和路由相关配置举例如下:

```
#
interface GiAbitEthernet2/1/2
 port link-mode route
 ip address 15.120.4.201 255.255.255.252
#
ip route-static 15.120.8.0 255.255.255.0 15.120.4.202
#
```

当外网地址充足时，利用原有网段即可，此时不需要新增路由和接口配置；如果外网地址不足，新增网段，则需要在与新增NAT路由器设备相连的外网路由设备上增加指向新增外网的NAT网段的路由。简单的说就是需要考虑清楚社会单位的路由，确保数据流能够有路由。