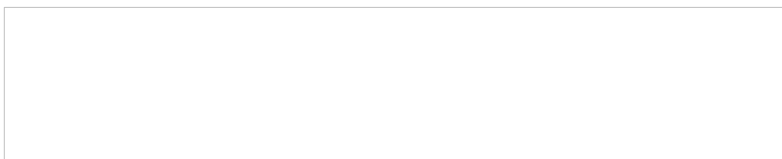


MSR系列路由器

Nat outbound和Nat server同时使用注意问题

一、组网



二、问题描述

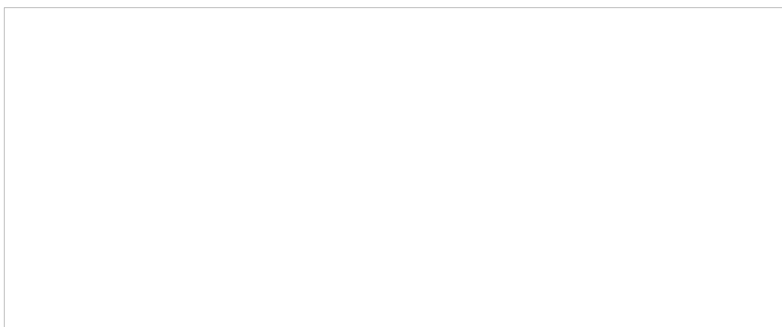
某公司路由器上的出接口同时配置了nat outbound和nat server，为的是外网人员可以访问到内网的服务器，内部人员也可以正常访问公网，客户发现当内网服务器访问公网其他地址时，在MSR上看不到相应的nat session，客户感觉很奇怪。

使用如下拓扑来模拟客户的网络，PC地址为1.1.1.2，在出口路由器上同时配置nat outbound和nat server，看一下是否如客户所说，内网服务器主动访问公网时，没有nat session。

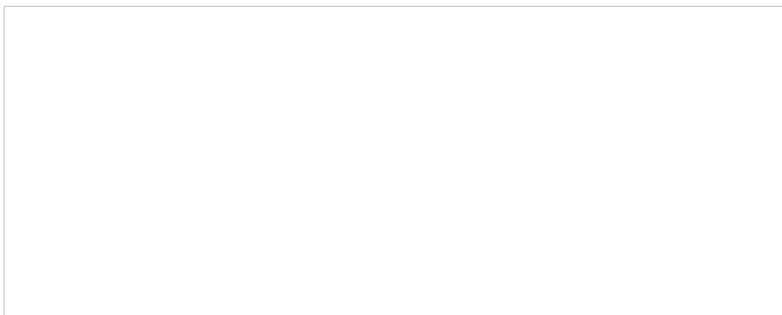
三、过程分析

如果PC机 1.1.1.2去PING INTERNET中一个地址，是走NAT SERVER，还是 nat outbound 3004？

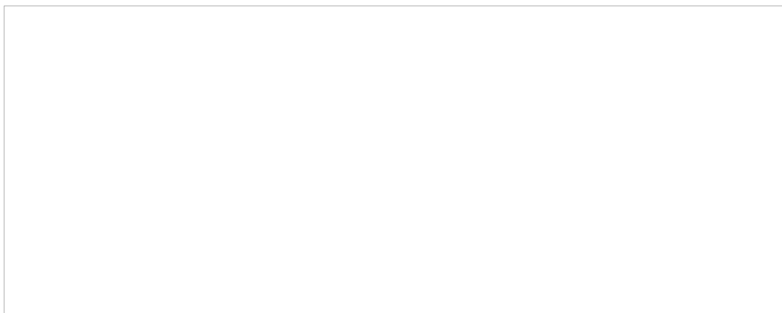
1) 如果内网主机地址为1.1.1.2 ping 外网2.2.2.2，可以ping通，但是不会匹配nat outbound，在一直ping通的状态下查看nat session中无数据,这时应该匹配的是nat server。如图1所示。



2) 如果内网主机地址1.1.1.2 telnet到外网设备2.2.2.2上，因为使用的协议是tcp而不是icmp,这是就会匹配到nat outbound 3004，在nat session中存在地址转换的会话。如图2所示



3) 如果内网主机地址不为1.1.1.2为其他，比如说1.1.1.3，此时ping外网2.2.2.2可以ping通，这时候会匹配nat outbound，进行地址转换，如图3所示。



我们普遍认为nat server只是匹配从公网过来的入方向的数据流，但是nat server其实是匹配双向的，当配置了nat server后，系统就已经生成了一条静态的会话表项，使用上述例子中的配置，接口下配置

了nat server protocol icmp global 2.2.2.1 any inside 1.1.1.2 icmp后，在系统中就以生成了如下nat会话：

Protocol	globaladdr	insideaddr
ICMP	2.2.2.1	1.1.1.2

如果是对于接口是入方向的报文，若协议为ICMP且目的地址为2.2.2.1，则改变该IP报文的目的地址为1.1.1.2，即正常的nat server的作用；

如果对于接口是出方向的报文，若协议为ICMP且源地址为1.1.1.2，则改变该IP报文的源地址为2.2.2.1发送出去。

四、配置参考

Nat 设备配置

```
#
acl number 3004 //配置nat outbound的感兴趣流
rule 0 permit ip source 1.1.1.0 0.0.0.255
#
interface Ethernet0/0
port link-mode route
nat outbound 3004 //配置nat outbound 3004
//配置nat server匹配的流为ICMP报文
nat server protocol icmp global 2.2.2.1 any inside 1.1.1.2 icmp
#
```

五、结论：

在接口下同时配置nat outbound和nat server，若内网过来一条数据流，既匹配nat outbound，又匹配nat server的服务映射，那这条数据流匹配的是nat server的映射，如果不匹配nat server或者不匹配nat server中的具体协议，就会匹配nat outbound