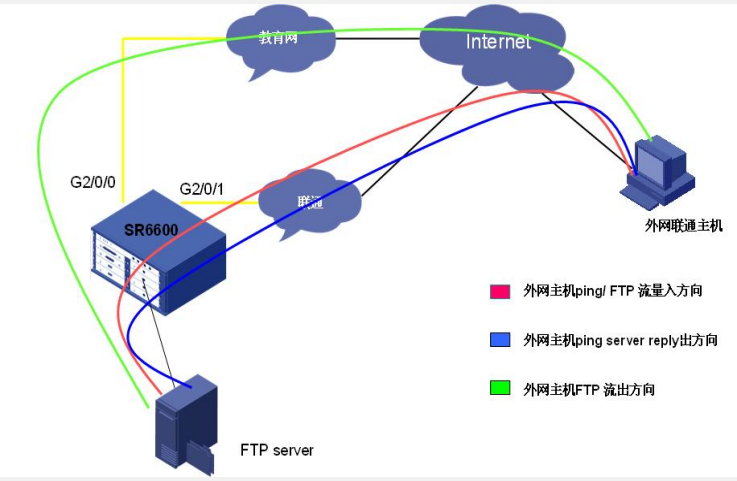
SR6600系列路由器接口下 session 建立机制

张盛楠　2010-09-02 发表

SR6600系列路由器接口下session的建立机制

一、　组网：



二、　组网及问题描述：

某大学采用教育网及联通线路双出口，网内FTP server IP 地址为公网承认的IP 地址。在G2/0/0接口上无nat配置。G2/0/1口上配置nat 将来自server地址的流量源地址转换为G2/0/1的接口地址。

在SR6600的内网网关接口上配置策略路由如下：

1. 如流量匹配tcp 端口号 FTP 则下一跳重定向到教育网出口（绿色线路）
2. 如流量为其它流量 则重定向到联通出口（ 蓝色线路）

配置目的：使外网主机只能对server 进行FTP的相关操作。

如果外网联通主机对server 进行ftp 访问、操作，流量可以经教育网正常返回至主机；如果从外网主机上对server 进行其它操作 （ping等） 流量在返回过程中经过 G2/0/1 是地址被转换，导致报文收发不一致，最终使主机丢弃ping 报文。

三、　过程分析：

按照理论分析，这种组网的方式是可以达到阻断外网主机对server进行除FTP以外的操作的（在MSR上进行了实验，可以成功阻断）。

但在SR66上实际操作一下便可以发现问题：从外网主机上还是可以ping通FTP server 。此时 display nat session 表项为空，很明显没有进行nat转换。从server ping 外网主机时 nat session 建立正常，nat成功转换。

问题原因剖析：SR6600路由器上对于Nat、Firewall 的处理是基于session的，而icmp 、TCP、UDP的处理不是基于session的。但当在接口下配置了NAT、packe-filter、ASPF后 该接口下icmp、TCP、UDP会因受到前者的影响而建立session表项。上面的问题正是由于在联通出口上配置了NAT，外网联通主机在ping server 时 icmp request 经过联通出口时建立了以下session表项

具体如下：

```
<SR6602 >display session table
Initiator:
  Source IP/Port : 100.1.1.1/2048      （外网主机地址）
  Dest IP/Port   : 219.218.80.77/44321 （server 地址 ）
  Pro            : ICMP(1)
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 219.218.80.77/0
  Dest IP/Port   : 100.1.1.1/44425
  VPN-Instance/VLAN ID/VLL ID:
```

Pro: ICMP(1) App: unknown State: ICMP-CLOSED
Start time: 2010-08-26 15:35:54 TTL: 29s
Received packet(s)(Init): 14 packet(s) 1176 byte(s)
Received packet(s)(Reply): 14 packet(s) 1176 byte(s)
且SR66接口下各个应用（包含nat）的session 统一由一张session table 维护，不对具体应用进行区分。
此时当 icmp reply 报文从G2/0/1接口返回时发现接口下的session table中已存在对应此源目的的session，因此直接经过此session 进行转发而就不去建立新的nat session 这导致nat 地址不进行转换。联通主机就能ping通server了。

四、 解决方法：
这个问题是66上对于session 处理的机制，无论是23xx版本还是24xx版本处理方式均是如此，因此无法在版本上解决。
建议解决办法：在内网网关或者外网出口上配置相应的包过滤防火墙配置进行规避。