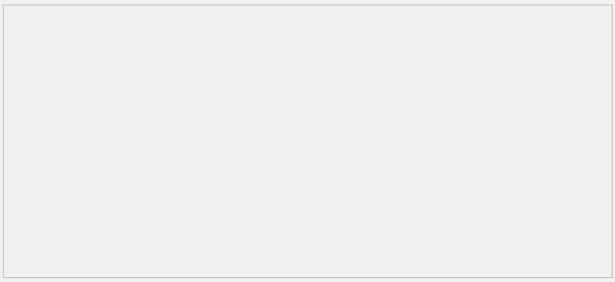
内网FTP服务使用其他端口号，无法通过Nat Server映射此FTP服务问题解决方法

魏添 2012-07-26 发表

内网FTP服务使用其他端口号，无法通过Nat Server映射此FTP服务问题解决方法

一、 组网：

内部对外提供FTP服务，FTP服务器地址为10.10.10.10/24，公网出口地址为1.1.1.1/24,内网网关地址为10.10.10.1/24，外网PC的地址为1.1.1.2/24，具体组网如图1所示。



二、 问题描述：

内网FTP服务器使用非21的特殊端口号向外提供FTP服务，在Router上将内网的特殊端口号通过Nat Server映射到外网，发现FTP服务无法正常提供，但是在这种组网方式下，我们可以通过特殊的配置来解决。

三、 过程分析：

MSR路由器主要配置：

```
version 5.20, Release 2209P21
interface Ethernet0/0
 port link-mode route
 nat outbound
 nat server protocol tcp global 1.1.1.1 8021 inside 10.10.10.10 6293
ip address 1.1.1.1 255.255.255.0
interface Ethernet0/1
 port link-mode route
 ip address 10.10.10.1 255.255.255.0
```

可以看到配置很简单，只是在外网口配置了nat server将外网1.1.1.1的8021端口映射到内网的10.10.10.10的6293，内网服务器的6293为我们提供FTP服务，我们在外网使用FTP软件访问1.1.1.1 8021 发现无法成功访问FTP服务，并且软件提示无法打开数据通道，查看debug nat packet 信息：

```
 (Ethernet0/0-in  :)Pro : TCP  is to NAT server
(       1.1.1.2:55544 -         1.1.1.1: 8021) ------>
(       1.1.1.2:55544 -     10.10.10.10: 6293)
*Jan  1 00:07:15:883 2007 H3C NAT/7/debug:
(Ethernet0/0-out :)Pro : TCP  is from NAT server
(    10.10.10.10: 6293 -         1.1.1.2:55544) ------>
(       1.1.1.1: 8021 -         1.1.1.2:55544)
```

可以看到是没有问题的，nat server 很好地完成了转换。但是为什么无法成功访问FTP服务呢？具体原因我们可以从FTP的原理出发来分析。

首先FTP有主动模式和被动模式的区别，第一种主动模式分析：

主动模式的工作原理是FTP客户端向服务器发送PORT命令，告诉服务器该客户端用于传输数据的临时端口号。当需要传输数据时，服务器通过TCP20端口与客户端的临时端口建立数据传输通道，完成数据传输，这个临时端口是由P1*256+P2算出来的。PORT命令主要发送的就是这个参数，格式为（x,x,x,x,p1,p2）x,x,x,x为服务器IP，而p1,p2是服务器随机生成的参数。

此时我们发现，如果客户端的数据连接的端口号是变化的，而服务器被NAT设备挡在里面，服务器知道这个端口号，而NAT设备不知道，若不改变FTP的端口号，这时候NAT设备收到的报文是源端口为新算出端口号，而数据连接的第一个源端口号是20的报文，此时无法将报文通过路由器送到客户端的，因为没这个NAT Session，这种是主动模式的情况。

第二种PASV模式分析：

前面的控制连接基本一样，不同在于控制连接最后一个报文，FTP服务器将PORT参数发送给客户端，然后客户端使用这个参数计算的临时端口号向内网发起数据连接。同样的NAT设备如果不知道修改过后的FTP服务端口，那么就无法通过ALG计算出客

户端使用的临时端口，生成NAT Session。

我们设想，如果在外网口做这么一条命令是不是可以解决问题？

[H3C-Ethernet0/0]nat server protocol tcp global 1.1.1.1 20 inside 10.10.10.10 20

Error: Can't use ftp's data connection!

但是遗憾的发现，ftp的数据连接不能被映射出去。分析一下，NAT ALG的工作原理是，在FTP的主动模式，最后一个控制连接的报文发送的时候，检查报文的PORT命令，将PORT的参数生成的新端口号拿出来，生成NAT Session。这有个前提条件是，NAT ALG必须要认识这个报文是FTP的控制连接，而分辨出这个报文的依据是端口号，所以在目的端口号是21的报文，我们认为是FTP服务， NAT ALG才能正常工作。如果我们将FTP端口号修改，那么在建立数据连接的时候就会出现问题。

四、 解决方法：

分析的时候，我们已经知道为什么不能建立数据连接的原因，是因为我们不能认识已经被修改控制连接端口号FTP的报文，NAT ALG无法正常工作，我们现在如果能够让路由器也能够认识到FTP的控制连接报文，那么一切都迎刃而解，在MSR的标准版软件中，我们可以做到这样的功能，我们需要在全局下配置一条port-mapping ftp port XX命令即可。XX即为服务器端被修改的端口号。

此时路由器的配置如下：

```
version 5.20, Release 2209P21
interface Ethernet0/0
 port link-mode route
 nat outbound
 nat server protocol tcp global 1.1.1.1 8021 inside 10.10.10.10 6293
ip address 1.1.1.1 255.255.255.0
interface Ethernet0/1
 port link-mode route
 ip address 10.10.10.1 255.255.255.0
port-mapping ftp port 6293
```

PASV模式下的NAT PACKET：

```
(Ethernet0/0-in  :)Pro : TCP  is to NAT server
(        1.1.1.2:55711 -         1.1.1.1: 8021) ------>
(        1.1.1.2:55711 -     10.10.10.10: 6293)
*Jan  1 00:22:09:103 2007 H3C NAT/7/debug:
(Ethernet0/0-out :)Pro : TCP  is from NAT server
(    10.10.10.10: 6293 -         1.1.1.2:55711) ------>
(        1.1.1.1: 8021 -         1.1.1.2:55711)
```

PASV模式的情况下修改过后的nat session：

```
There are currently 2 NAT sessions:
Pro    GlobalAddr:Port        LocalAddr:Port         DestAddr:Port
TCP    1.1.1.1:54904          10.10.10.10:54904      1.1.1.2:55712
       GlobalVPN: ---         LocalVPN: ---
       status: 10241          TTL: 00:05:00          Left: 00:04:48

TCP    1.1.1.1:54904          10.10.10.10:54904      ---
       GlobalVPN: ---         LocalVPN: ---
       status: 18241          TTL: ---               Left: ---
```

路由器上用54904建立了TCP的连接。54904怎么得来的？我们看下FTP的参数：

```
PASV
227 Entering Passive Mode (1.1.1.1 214,120)
```

正打开数据连接IP：1.1.1.1 端口54904

可以在FTP客户端上看到PORT 参数为（1,1,1,1,214,120）那么我们客户端使用的临时端口号则应该为：214*256+120=54904，我们发现NAT ALG生效了，设备通过port-mapping ftp port 6293认识了此报文。