MSR系列路由器在FTP中ALG的处理机制的典型配置

高贵贤　2013-07-30 发表

MSR系列路由器在FTP中ALG的处理机制的典型配置

一、　组网需求

Router2和Router3作为FTP服务器，在Router1的G0/1接口配置NAT server映射内部FTP服务器，接口G0/0配置NAT Outbound转换外部源地址，当G0/0口配置两个NAT Outbound时，某些情况下，由于ALG处理机制的问题，会导致FTP的主动模式访问不成功，而被动模式是没有问题的

设备清单：MSR系列路由器4台

二、　组网图

图一 MSR系列路由器在FTP中ALG处理配置组网图

三、　配置步骤

```
[Router1]display  current-configuration
#
 version 5.20, Release 2506, Standard
#
 sysname Router1
#
 nat address-group 1 23.1.1.10 23.1.1.10
 nat address-group 2 23.1.1.20 23.1.1.20
#
acl number 3000
 rule 0 permit ip destination 23.1.1.2 0
 rule 5 deny ip
acl number 3001
 rule 0 permit ip destination 23.1.1.3 0
 rule 5 deny ip
acl number 3002
 rule 0 permit ip destination 23.1.1.2 0
 rule 5 deny ip
#
interface GigabitEthernet0/0
 port link-mode route
 nat outbound 3001 address-group 1
 nat outbound 3000 address-group 2
 ip address 23.1.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 nat server 1 protocol tcp global current-interface ftp inside 23.1.1.2 ftp
 ip address 12.1.1.2 255.255.255.0
 undo ip fast-forwarding
#
```

四、验证过程

```
<client>ftp 12.1.1.2
Trying 12.1.1.2 ...
Press CTRL+K to abort
Connected to 12.1.1.2.
220 FTP service ready.
User(12.1.1.2:(none)):admin                    //输入用户名admin
331 Password required for admin.
Password:                                      //输入密码admin
230 User logged in.

[ftp]dir                                       //默认是被动模式
227 Entering Passive Mode (12,1,1,2,5,239).
125 ASCII mode data connection already open, transfer starting for /*.
drwxrwxrwx   1 noone    nogroup         0 May 23 15:46 logfile
-rwxrwxrwx   1 noone    nogroup     16256 Apr 10  2010 p2p_default.mtd
-rwxrwxrwx   1 noone    nogroup  18324480 Apr 23 10:00 msr30-cmw520-r2311-bi.bin
-rwxrwxrwx   1 noone    nogroup     15966 Jun 24 15:16 config.cwmp
-rwxrwxrwx   1 noone    nogroup  27134976 Jul 24 17:02 msr30-cmw520-r2507-si.bin
-rwxrwxrwx   1 noone    nogroup  25027308 Aug 16  2012 msr30-cmw520-r2209p21-si.bin
drwxrwxrwx   1 noone    nogroup         0 Aug 16  2012 domain1
-rwxrwxrwx   1 noone    nogroup  18323456 May 17 08:31 msr30-cmw520-r2312p20-bi.bin
drwxrwxrwx   1 noone    nogroup         0 Aug 22  2012 wav
-rwxrwxrwx   1 noone    nogroup  23277808 Jul 11 15:51 msr30-cmw520-r2105p31-si.bin
-rwxrwxrwx   1 noone    nogroup  25008460 Oct 10  2012 msr30-cmw520-r2209p35-si.bin
-rwxrwxrwx   1 noone    nogroup  17439796 Dec 28  2012 msr30-cmw520-r2207p14-bi.bin
226 Transfer complete.
FTP: 917 byte(s) received in 0.129 second(s), 7.00K byte(s)/sec.

[ftp]undo passive                              //关闭被动模式，使能主动模式
FTP: passive is off
[ftp]dir
500 Illegal PORT command.

当G0/0口配置修改为：
interface GigabitEthernet0/0
 port link-mode route
 nat outbound 3002 address-group 2
 nat outbound 3001 address-group 1
 ip address 23.1.1.1 255.255.255.0

<client>ftp 12.1.1.2
Trying 12.1.1.2 ...
Press CTRL+K to abort
Connected to 12.1.1.2.
220 FTP service ready.
User(12.1.1.2:(none)):admin
331 Password required for admin.
Password:
230 User logged in.

[ftp]undo passive
FTP: passive is off
```

```
[ftp]dir                    //当修改NAT Outbound的顺序后，主动模式正常
200 Port command okay.
150 Opening ASCII mode data connection for /*.
drwxrwxrwx   1 noone    nogroup          0 May 23 15:46 logfile
-rwxrwxrwx   1 noone    nogroup      16256 Apr 10  2010 p2p_default.mtd
-rwxrwxrwx   1 noone    nogroup   18324480 Apr 23 10:00 msr30-cmw520-r2311-bi.bin
-rwxrwxrwx   1 noone    nogroup      15966 Jun 24 15:16 config.cwmp
-rwxrwxrwx   1 noone    nogroup   27134976 Jul 24 17:02 msr30-cmw520-r2507-si.bin
-rwxrwxrwx   1 noone    nogroup   25027308 Aug 16  2012 msr30-cmw520-r2209p21-si.bin
drwxrwxrwx   1 noone    nogroup          0 Aug 16  2012 domain1
-rwxrwxrwx   1 noone    nogroup   18323456 May 17 08:31 msr30-cmw520-r2312p20-bi.bin
drwxrwxrwx   1 noone    nogroup          0 Aug 22  2012 wav
-rwxrwxrwx   1 noone    nogroup   23277808 Jul 11 15:51 msr30-cmw520-r2105p31-si.bin
-rwxrwxrwx   1 noone    nogroup   25008460 Oct 10  2012 msr30-cmw520-r2209p35-si.bin
-rwxrwxrwx   1 noone    nogroup   17439796 Dec 28  2012 msr30-cmw520-r2207p14-bi.bin
226 Transfer complete.
FTP: 917 byte(s) received in 0.097 second(s), 9.00K byte(s)/sec.
```

原因分析：

原始配置的时候，主动模式下在G0/0口抓包：

图二 主动模式下，G0/0接口抓包

由抓包可以看出，FTP控制报文在进行NAT转换的时候，数据包源地址正常转换为23.1.1.20,但是数据通道的源地址转换为23.1.1.10，这就是导致主动模式数据不能打开的原因；根本原因在于ALG处理机制问题，因为ALG在处理的时候，是不会匹配目的地址的，因此对于

```
acl number 3001
 rule 0 permit ip destination 23.1.1.3 0
```

是识别为：

```
acl number 3001
 rule 0 permit ip
```

从而导致了在ALG的时候，源地址转化为了23.1.1.10

因此修改配置后主动模式和被动模式都可以正常打开数据连接就不难理解了

而被动模式，ALG的动作是对pasv response报文进行修改，是在G0/1进行的，没有上述问题，因此是可以完成的：

图三 被动模式G0/1口抓包信息

五、 配置关键点

1. ALG的处理机制，如果在转换的时候需要匹配ACL，是不会匹配目的地址的；
2. 如果接口有多个NAT outbound，需要注意配置顺序，否则主动模式受影响；
3. 因为被动模式是在NAT server口完成，因此被动模式是不受影响的；
4. R2507版本后，ALG的处理机制，更改为可以匹配目的地址。