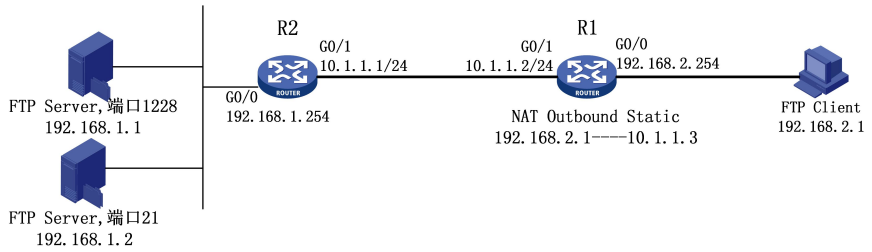
某局点MSR G2路由器NAT后FTP业务不通经验案例

NAT FTP/TFTP 吕甲南 2015-12-28 发表

某局点存在多台FTP服务器，某些FTP服务器基于业务和安全等方面的考虑，需要将某些FTP端口进行变更。

FTP客户端网关设备R1有NAT，将FTP客户端的地址静态转换为10.1.1.3。

FTP服务器网关设备R2没有关于FTP客户端192.168.2.0网段的路由。



当客户将FTP的端口号变更后，发现FTP客户端无法查看FTP服务器上的文件，并且无法进行数据传输。

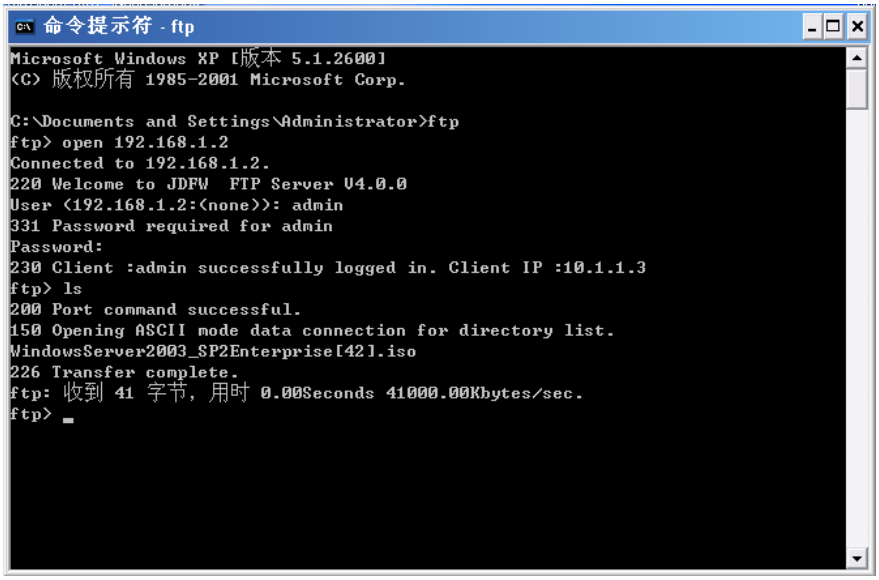
对于未更改端口号的FTP服务器可以正常访问。将该FTP服务器FTP的端口号更改回默认的端口号业务即可正常。

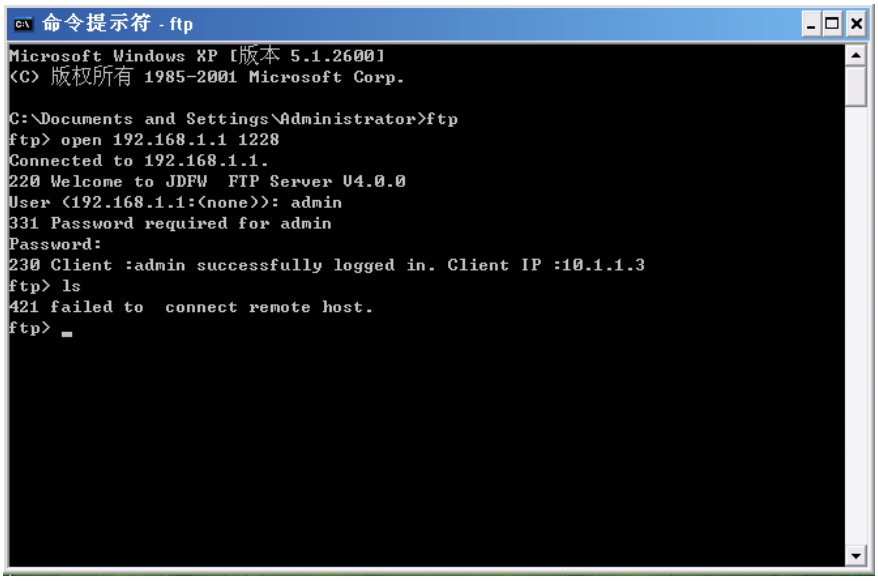
将客户端的模式更改为被动FTP模式，FTP服务也可以正常访问。

1. 查看R1设备的配置

```
display current-configuration
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 192.168.2.254 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
  ip address 10.1.1.2 255.255.255.0
 nat static enable
#
 ip route-static 0.0.0.0 0 10.1.1.1
#
  nat static outbound 192.168.2.1 10.1.1.3
```

2. 在FTP客户端进行FTP测试





此时发现未更改FTP端口号的192.168.1.2服务器可以正常访问，更改FTP端口的192.168.1.1服务器不能正常访问

3. 在R1上debugging nat alg all, debugging nat packet，并在FTP客户端测试，查看debug输出

debugging nat alg all

debugging nat packet

terminal monitor

The current terminal is enabled to display logs.

terminal debugging

The current terminal is enabled to display debugging logs

*Dec 27 15:28:40:703 2015 R1 NAT/7/COMMON:

PACKET: (GigabitEthernet0/1-out) Protocol: TCP

192.168.2.1: 2148 - 192.168.1.1: 1228(VPN: 0) ------>

10.1.1.3: 2148 - 192.168.1.1: 1228(VPN: 0)

*Dec 27 15:28:40:704 2015 R1 NAT/7/COMMON:

PACKET: (GigabitEthernet0/1-in) Protocol: TCP

192.168.1.1: 1228 - 10.1.1.3: 2148(VPN: 0) ------>

192.168.1.1: 1228 - 192.168.2.1: 2148(VPN: 0)

*Dec 27 15:29:24:503 2015 R1 NAT/7/COMMON:

PACKET: (GigabitEthernet0/1-out) Protocol: TCP

192.168.2.1: 2151 - 192.168.1.2: 21(VPN: 0) ------>

10.1.1.3: 2151 - 192.168.1.2: 21(VPN: 0)

*Dec 27 15:29:24:504 2015 R1 NAT/7/COMMON:

PACKET: (GigabitEthernet0/1-in) Protocol: TCP

192.168.1.2: 21 - 10.1.1.3: 2151(VPN: 0) ------>

192.168.1.2: 21 - 192.168.2.1: 2151(VPN: 0)

*Dec 27 15:29:30:934 2015 R1 NAT/7/ALG:

PACKET: (GigabitEthernet0/1) ALG payload was translated according to configuration:

192.168.2.1/2152(VPN: 0) ---> 10.1.1.3/2152(VPN: 0)

*Dec 27 15:29:30:937 2015 R1 NAT/7/COMMON:

PACKET: (GigabitEthernet0/1-in) Protocol: TCP

192.168.1.2:49358 - 10.1.1.3: 2152(VPN: 0) ------>

192.168.1.2:49358 - 192.168.2.1: 2152(VPN: 0)

*Dec 27 15:29:30:937 2015 R1 NAT/7/COMMON:

PACKET: (GigabitEthernet0/1-out) Protocol: TCP

192.168.2.1: 2152 - 192.168.1.2:49358(VPN: 0) ------>

10.1.1.3: 2152 - 192.168.1.2:49358(VPN: 0)

此时，通过debugging输出可以看出，192.168.2.1访问192.168.1.1的FTP服务时，控制连接可以正常建立。当FTP客户端发送Port报文的时候，没有发生NAT ALG，FTP的Port报文载荷仍然为192.168.2.1私网地址。FTP服务器向FTP客户端发起数据连接的时候数据包发送给192.168.2.1，由于R2没有192.168.1.0网段的路由，导致FTP访问异常。

而192.168.2.1访问192.168.1.2的FTP服务时，控制连接建立完成后，FTP客户端发送Port报文，R1正确转换了FTP的载荷，将载荷的192.168.2.1转换为10.1.1.3，FTP服务器发起数据连接的时候，报文转发给10.1.1.3,R1通过session表项，将数据转换后发送给FTP客户端，此时FTP服务可以正常访问。

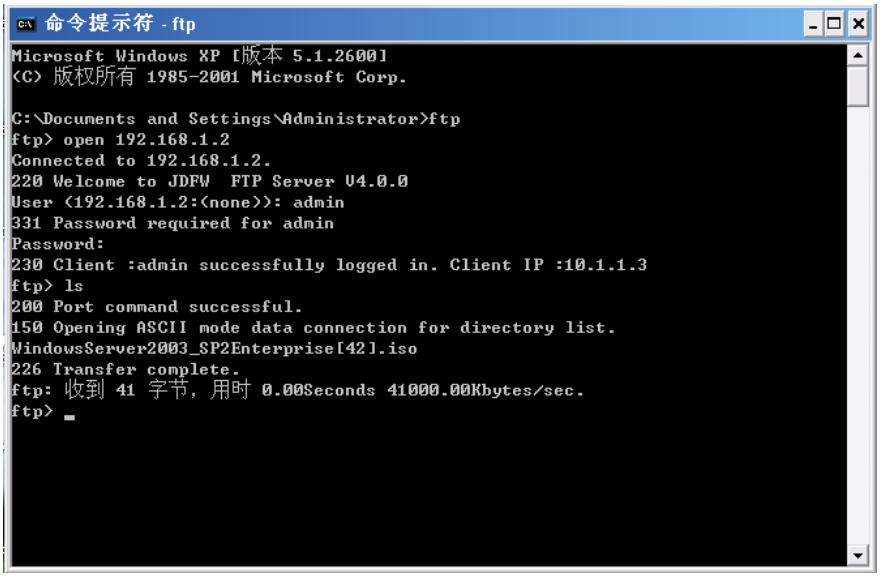
问题的原因在于路由器没有正确识别更改FTP端口号的应用层协议，不认为该报文为FTP报文，没有执行NAT ALG，导致FTP服务访问异常，可以通过命令建立端口号与应用层协议的映射关系，让路由器可以识别该协议，正确的执行NAT ALG。

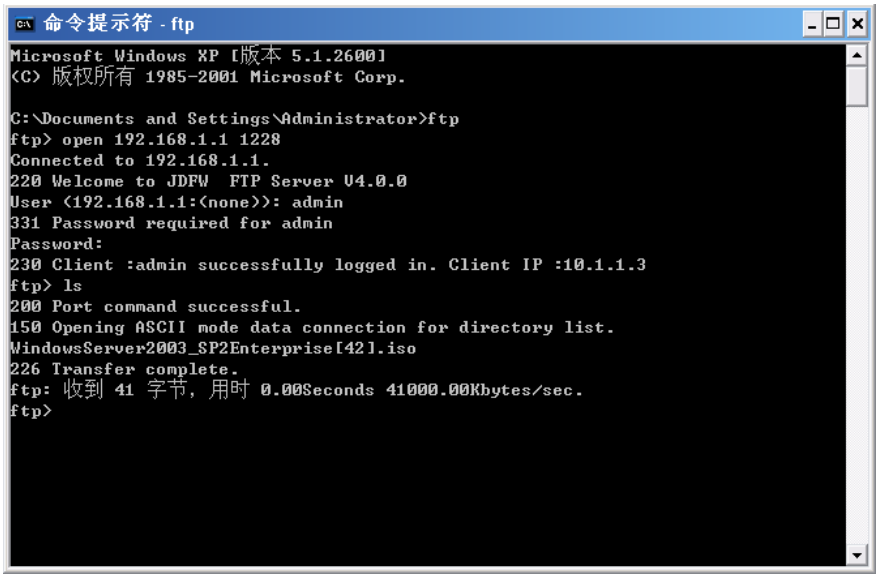
配置基于ACL的主机端口映射

[R1]acl basic 2000

[R1-acl-ipv4-basic-2000]rule permit source 192.168.1.1 0

[R1]port-mapping application ftp port 1228 acl 2000





*Dec 27 16:01:14:072 2015 R1 NAT/7/COMMON:

PACKET: (GigabitEthernet0/1-out) Protocol: TCP

192.168.2.1: 2166 - 192.168.1.1: 1228(VPN: 0) ------>

10.1.1.3: 2166 - 192.168.1.1: 1228(VPN: 0)

*Dec 27 16:01:14:074 2015 R1 NAT/7/COMMON:

PACKET: (GigabitEthernet0/1-in) Protocol: TCP

192.168.1.1: 1228 - 10.1.1.3: 2166(VPN: 0) ------>

192.168.1.1: 1228 - 192.168.2.1: 2166(VPN: 0)

*Dec 27 16:01:17:703 2015 R1 NAT/7/ALG:

PACKET: (GigabitEthernet0/1) ALG payload was translated according to configuration:

192.168.2.1/2167(VPN: 0) ---> 10.1.1.3/2167(VPN: 0)

*Dec 27 16:01:17:705 2015 R1 NAT/7/COMMON:

PACKET: (GigabitEthernet0/1-in) Protocol: TCP

192.168.1.1: 1083 - 10.1.1.3: 2167(VPN: 0) ------>

192.168.1.1: 1083 - 192.168.2.1: 2167(VPN: 0)

*Dec 27 16:01:17:705 2015 R1 NAT/7/COMMON:

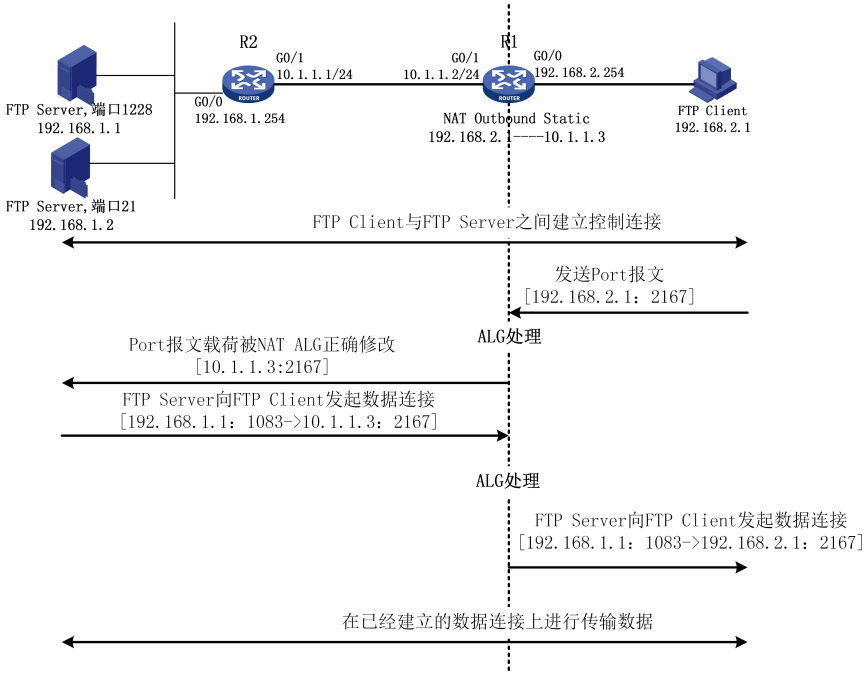
PACKET: (GigabitEthernet0/1-out) Protocol: TCP

192.168.2.1: 2167 - 192.168.1.1: 1083(VPN: 0) ------>

10.1.1.3: 2167 - 192.168.1.1: 1083(VPN: 0)

此时问题已经解决，使用默认FTP端口号的服务器和更改FTP端口号的服务器都可以正常访问。

FTP主动模式数据连接由服务器主动发起。
FTP被动模式数据连接由客户端主动发起。
下图为FTP主动模式 NAT ALG的应用示意图:


R2
R1
G0/1
10.1.1.1/24
G0/1
10.1.1.2/24
G0/0
192.168.2.254
FTP Server,端口1228
192.168.1.1
G0/0
192.168.1.254
NAT Outbound Static
192.168.2.1----10.1.1.3
FTP Client
192.168.2.1
FTP Server,端口21
192.168.1.2
FTP Client与FTP Server之间建立控制连接
发送Port报文
[192.168.2.1：2167]
ALG处理
Port报文载荷被NAT ALG正确修改
[10.1.1.3:2167]
FTP Server向FTP Client发起数据连接
[192.168.1.1：1083->10.1.1.3：2167]
ALG处理
FTP Server向FTP Client发起数据连接
[192.168.1.1：1083->192.168.2.1：2167]
在已经建立的数据连接上进行传输数据