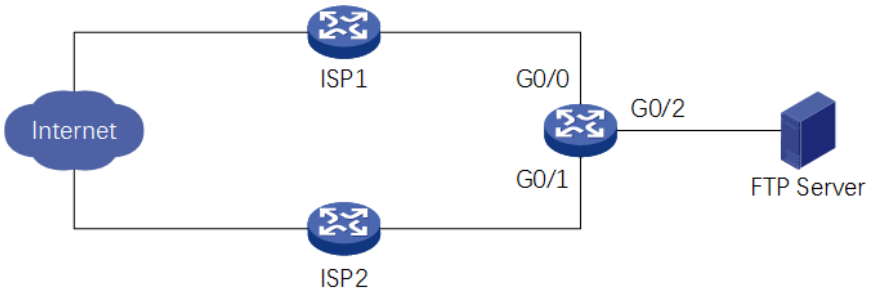
NAT内部FTP over TLS服务器无法从Internet访问经验案例

戴荣忻 2017-05-22 发表



某双线动态IP接入Internet的用户，内网有一台支持FTP over TLS的FTP服务器，通过其中一个运营商的Internet地址对外提供FTP服务，但是从Internet无法访问FTP over TLS服务，只能访问明文FTP服务。

设备的配置如下：

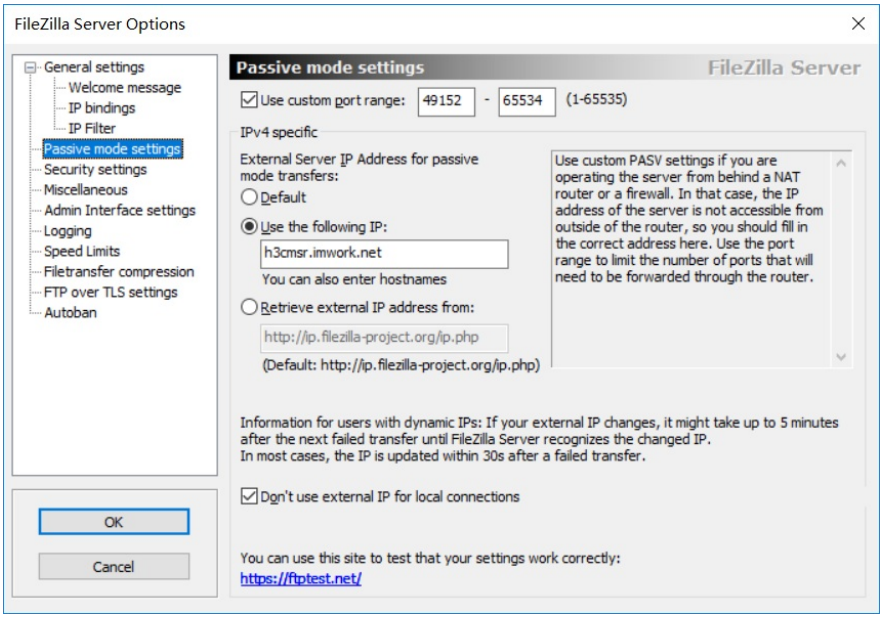
```
#
 sysname CPE
#
interface GigabitEthernet0/0
 ip address dhcp-alloc // 从ISP1动态获取Internet地址
 nat outbound // 出方向动态地址转换
 nat server protocol tcp global current-interface 21 inside 192.168.0.254 21 // 明文FTP、显式FTP over TLS的端口映射
 nat server protocol tcp global current-interface 990 inside 192.168.0.254 990 // 隐式FTP over TLS的端口映射
#
interface GigabitEthernet0/1
 ip address dhcp-alloc // 从ISP2动态获取Internet地址
 nat outbound // 出方向动态地址转换
#
interface GigabitEthernet0/2
 ip address 192.168.0.1 255.255.255.0 // 内网设备的网关地址
#
return
```

告警信息如下：

```
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> Connected on port 21, sending welcome message...
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> 220-FileZilla Server 0.9.60 beta
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> 220 Please visit https://filezilla-project.org/
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> AUTH TLS
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> 234 Using authentication type TLS
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> TLS connection established
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> USER anonymous
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> 331 Password required for anonymous
(000001)2017/5/20 13:14:25 - (not logged in) (111.194.0.224)> PASS **********
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> 230 Logged on
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> PBSZ 0
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> 200 PBSZ=0
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> PROT P
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> 200 Protection level set to P
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> PWD
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> 257 "/" is current directory.
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> TYPE I
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> 200 Type set to I
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> PASV
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> 227 Entering Passive Mode
```

(192,168,0,254,205,242)
错误: 严重错误: 无法连接到服务器
(000001)2017/5/20 13:14:25 - anonymous (111.194.0.224)> disconnected.

由于FTP服务器支持FTP over TLS，所以FTP客户端发起了PROT P隐私保护指令，后续报文从明文改变为密文。之后FTP客户端希望发起MLSD指令获取FTP服务器上的文件列表，需要先发起PASV指令进入被动模式建立数据连接，但是因为使用的是密文，NAT FTP ALG无法转换227响应中携带的服务器地址信息，所以导致无法连接到服务器。



在FTP服务器被动模式设置界面，有为被动模式指定外部服务器IP地址的配置选项，缺省情况是Default，服务器在227响应中携带的是私网地址，还有2个选项分别是指定IP地址和从某个HTTP API获取IP地址。从某个HTTP API获取IP地址的方式，由于CPE设备同时接入2个运营商，形成了ECMP负载分担路由，所以不一定获取到的IP地址就是对外提供FTP服务的Internet地址。指定IP地址的方式，由于FileZilla Server支持配置IP地址和域名，所以可以结合DDNS功能实现动态IP地址。

壳域名

域名

h3cmsr.imwork.net

h3cmsr.iok.la

在此处我们到花生壳网站申请了一个免费的支持DDNS的壳域名h3cmsr.imwork.net，并将它配置到FileZilla Server设置界面上。
同时我们还需要在MSR设备上面再增加如下配置：
[CPE] ddns policy hsk // 创建DDNS策略
[CPE-ddns-policy-hsk] url oray://phservice2.oray.net // 指定花生壳的DDNS更新请求URL地址
[CPE-ddns-policy-hsk] username h3cmsr // 配置用户名
[CPE-ddns-policy-hsk] password simple P@ssw0rd // 配置密码
[CPE-ddns-policy-hsk] interval 0 0 1 // 配置更新时间间隔
[CPE-GigabitEthernet0/0] ddns apply policy hsk fqdn h3cmsr.imwork.net // 在对外提供FTP服务的接口上应用DDNS策略
配置好之后，检验域名解析结果是否与CPE设备上的GigabitEthernet0/0接口地址相同：
nslookup h3cmsr.iwork.net 8.8.8.8
服务器: google-public-dns-a.google.com
Address: 8.8.8.8
非权威应答:
名称: h3cmsr.iwork.net
Address: 59.65.174.240
再次尝试从Internet加密访问FTP服务器，可以看到227响应中携带的IP地址已经变成了公网地址：
227 Entering Passive Mode (59,65,174,240,196,204)
但是此时数据连接仍然无法建立，这是因为NAT FTP ALG不能从加密的227响应中读取到服务器打开

的端口信息，并为FTP客户端打开相应的端口。

可以再在CPE设备上增加如下配置，将FileZilla Server上配置的被动模式端口范围全部映射到Internet：

[CPE-GigabitEthernet0/0] nat server protocol tcp global current-interface 49152 65534 inside 192.168.0.254 49152 65534

此时再次尝试从Internet加密访问FTP服务器，控制连接和数据连接均可正常建立，问题解决。

内网向外网映射方式提供FTP over TLS这种协议的服务时，无法使用NAT FTP ALG直接解决问题，需要对NAT设备进行特殊配置，还需要在FTP服务器上进行特殊配置，共同解决PASV的227响应中携带的地址问题和数据连接的建立问题。