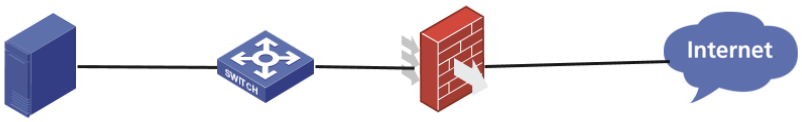
某局点通过nat映射ftp端口号登录服务器失败问题处理案例分析

NAT wangqi 2018-11-12 发表

组网及说明



服务器--交换机--防火墙--公网

问题描述

问题现象：内网ftp可以正常登录服务器，公网ftp登录服务器时无法访问，显示服务器拒绝连接

过程分析

1、检查防火墙配置：

```
#
 version 7.1.064, Release 9323P1801
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 112.27.225.57 255.255.255.0
 nat outbound 2000
 nat server protocol tcp global 112.27.225.57 1024 inside 172.66.100.100 20
 nat server protocol tcp global 112.27.225.57 1025 inside 172.66.100.100 21
 nat server protocol tcp global 112.27.225.57 1033 inside 172.66.100.100 80
#
```

防火墙配置了net server将服务器的21和20端口号分别映射为防火墙的1025和1024端口号

2、根据反馈的信息可以看到客户将标准的端口映射为非标准端口号，查阅资料，发现这种映射方式还缺少两条配置命令

（1）port-mapping application ftp port 1025

port-mapping：用来配置通用端口映射

application application-name：指定端口映射的应用层协议

（2）nat alg ftp

nat alg 用来开启指定或所有协议类型的NAT ALG功能

缺省情况下：DNS、FTP、ICMP差错报文、RTSP、PPTP协议类型的NAT ALG功能处于开启状态，其他协议类型的NAT ALG功能处于关闭状态。

解决方法

配置 port-mapping application ftp port 1025 和 nat alg ftp