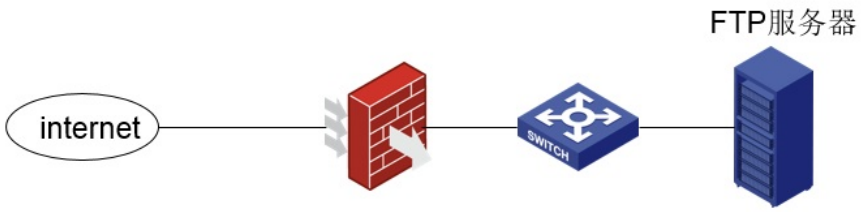
SecPath F1000-C8150(V7)外网访问内网ftp服务器首次连接无法成功

NAT 郭尧 2020-03-24 发表

组网及说明

公网-F1000-核心-ftp服务器



防火墙作出口，进行源目地址转换，实现外网访问内部服务器

问题描述

外网访问内网FTP服务器时，FTP软件首次连接被拒绝，需要刷新重连才可以连接成功

过程分析

收集防火墙诊断信息，查看外网口接口配置，nat server端口映射内网FTP服务器，配置如下：

```
interface GigabitEthernet1/0/2
 port link-mode route
 description 电信固定外网
 mtu 1460
 ip address 220.160.54.204 255.255.255.192
 ip address 220.160.54.220 255.255.255.192 sub
 tcp mss 1280
 nat outbound
 nat server protocol tcp global 220.160.54.204 9091 inside 192.168.0.226 21 rule j双向 counting
  gateway 220.160.54.254
```

接口配置可以看到FTP服务器的端口已经被修改为9091，FTP的缺省端口号为2021

在首次访问过程中查看防火墙会话信息，会话能够正常建立，但是回包报文丢了一个

```
Initiator:
  Source      IP/port: 125.77.89.113/36755
  Destination IP/port: 220.160.54.204/9091
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
Responder:
  Source      IP/port: 192.168.0.226/21
  Destination IP/port: 125.77.89.113/36755
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface10
  Source security zone: Trust
State: TCP_ESTABLISHED
Application: GENERAL_TCP
Rule ID: 0
Rule name: 0
Start time: 2020-03-24 10:19:20  TTL: 3598s
Initiator->Responder:            17 packets         822 bytes
Responder->Initiator:            16 packets        1289 bytes
```

nat server地址转换其实生效了的，下面来分析一下FTP原理：

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。
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。

解决方法

通过以上分析，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，那么问题将得到解决，防火墙可以通过配置通用端口来实现这个需求，如下：

port-mapping

port-mapping命令用来配置通用端口映射。

undo port-mapping命令用来删除指定的通用端口映射。

【命令】

port-mapping application application-name port port-number [protocol protocol-name]

undo port-mapping application application-name port port-number [protocol protocol-name]

【缺省情况】

各应用层协议与其对应的知名端口号映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

application application-name：指定端口映射的应用层协议。application-name表示应用协议名称。为1～63个字符的字符串，不区分大小写，不允许为系统保留的“invalid”和“other”。该应用层协议名称必须标准且能够被设备识别。

port port-number：指定与应用层协议映射的端口。port-number表示端口号，取值范围为0～65535。

protocol protocol-name：指定应用层协议使用的传输层协议名称，其取值及含义如下：

- dccp：表示DCCP（Datagram Congestion Control Protocol，数据报拥塞控制协议）协议。
- sctp：表示SCTP（Stream Control Transmission Protocol，流控制传输协议）协议。
- tcp：表示TCP协议。
- udp：表示UDP协议。
- udp-lite：表示UDP-Lite协议。

【使用指导】

若不指定protocol参数，则表示所有传输层协议的指定报文均可被识别为指定应用层协议的报文。

如果报文的目的端口号与某个通用端口映射匹配，则该报文将被识别为相应的应用层协议报文。

对于端口号、传输层协议参数均相同但是应用层协议名称不相同的两个配置，新的配置会覆盖原有的配置。

指定传输层协议名称的映射优先级高于不指定传输层协议名称的映射。

【举例】

建立端口9091到FTP协议的通用端口映射。

<Sysname> system-view

[Sysname] port-mapping application ftp port 9091