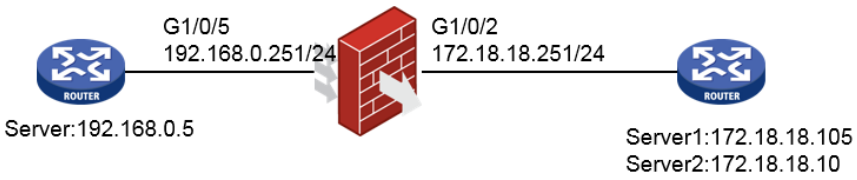
某局点 SecPath F1000-AK125(V7) nat server 双向映射不生效经典案例

NAT 会话 域间策略/安全域 **刺梨** 2018-11-15 发表

组网及说明

如图



问题描述

nat server 双向映射时，源目端口相同可以访问，源目端口不同无法访问，Telnet都是通的，配置如下：

```
interface GigabitEthernet1/0/2
 port link-mode route
 description GuideWan Interface
 ip address 172.18.18.251 255.255.255.0
 nat outbound
 nat server protocol tcp global current-interface 21 inside 192.168.0.5 21      //可以访问
 nat server protocol tcp global current-interface 2121 inside 172.16.1.115 21   /无法访问

interface GigabitEthernet1/0/5
 port link-mode route
 ip address 192.168.0.251 255.255.255.0
 nat outbound
 nat server protocol tcp global current-interface 1934 inside 172.18.18.105 1934
 nat server protocol tcp global current-interface 1936 inside 172.18.18.105 1936
```

过程分析

1、双向映射端口号源目端口相同可以成功，不同不能成功，说明网络没问题。

2、收集访问成功和不成功的会话对比。

a)源目端口一致，访问正常的会话

```
[H3C]disp session table ipv4 source-ip 172.18.18.10 verbose
Slot 1:
Initiator:
  Source      IP/port: 172.18.18.10/59439
  Destination IP/port: 172.18.18.251/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: trust
Responder:
  Source      IP/port: 192.168.0.5/21
  Destination IP/port: 192.168.0.251/1036
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/5
  Source security zone: untrust
State: TCP_TIME_WAIT
Application: FTP
Start time: 2018-11-14 20:54:59  TTL: 0s
Initiator->Responder:          11 packets        511 bytes
Responder->Initiator:          13 packets        847 bytes
```

```
Initiator:
  Source      IP/port: 172.18.18.21/59440
  Destination IP/port: 172.18.18.251/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: trust
Responder:
  Source      IP/port: 192.168.0.5/21
  Destination IP/port: 192.168.0.251/1037
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/5
  Source security zone: untrust
State: TCP_ESTABLISHED
Application: FTP
Start time: 2018-11-14 20:54:59  TTL: 3598s
Initiator->Responder:           13 packets        630 bytes
Responder->Initiator:           15 packets       1055 bytes

Total sessions found: 2
```

b)源目端口不一致，访问不正常的会话

```
[H3C]disp session table ipv4 source-ip 172.18.18.10 verbose
Slot 1:
Initiator:
  Source      IP/port: 172.18.18.10/59453
  Destination IP/port: 172.18.18.251/2121
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: trust
Responder:
  Source      IP/port: 172.16.1.115/21
  Destination IP/port: 172.16.1.251/1026
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/6
  Source security zone: untrust
State: TCP_ESTABLISHED
Application: GENERAL_TCP
Start time: 2018-11-14 20:56:18  TTL: 3570s
Initiator->Responder:           12 packets        585 bytes
Responder->Initiator:           13 packets        903 bytes

Initiator:
  Source      IP/port: 172.18.18.21/59440
  Destination IP/port: 172.18.18.251/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: trust
Responder:
  Source      IP/port: 192.168.0.5/21
  Destination IP/port: 192.168.0.251/1037
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/5
```

Source security zone: untrust
State: TCP_ESTABLISHED
Application: FTP
Start time: 2018-11-14 20:54:59 TTL: 3490s
Initiator->Responder: 13 packets 630 bytes
Responder->Initiator: 15 packets 1055 bytes

Total sessions found: 2

会话转换未看出异常，初步怀疑是映射的服务器出现问题，交叉测试：
nat server protocol tcp global current-interface **21** inside 192.168.0.5 **21** //**成功**
nat server protocol tcp global current-interface **2121** inside 192.168.0.5 **21** //**不成功**
排除服务器故障的可能性

解决方法

添加命令， 不同源目端口成功映射
port-mapping application ftp port 2121
port-mapping application ftp port 2123
port-mapping介绍：
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3456到FTP协议的通用端口映射。
<Sysname> system-view
[Sysname] port-mapping application ftp port 3456
【相关命令】
- display port-mapping user-defined