案例库

退出登录 >

# AR1220-S ipsec vpn 隧道建立成功后数据不通

发布时间: 2019-07-17 | 浏览次数: 1472 | 下载次数: 0 | 文档编号: EKB1000115551

## 目录



## 问题描述

拓扑如下:
192.168.14.10----------对端IPSEC加密设备----------AR1220S---------192.168.9.253。AR1220S与对端设备建立IPSEC VPN,隧道建立成功后,从192.168.9.253 ping 192.168.14.10可以通,但是从192.168.9.253 telnet 192.168.14.10 1054端口不成功。

## 处理过程

1. 检查两端的加密数据流以及IPSEC SA隧道信息,正常,相关信息如下:
[1]dis ipsec sa

```
==============================
Interface: GigabitEthernet0/0/0
Path MTU: 1500
==============================

  ------------------------------
  IPSec policy name: "center_vpn"
  Sequence number  : 1
  Acl group        : 0
  Acl rule         : 0
  Mode             : Template
  ------------------------------
    Connection ID     : 1481
    Encapsulation mode: Tunnel
    Tunnel local      : 172.x.20.10
    Tunnel remote     : 172.x.10.10
    Flow source       : 192.168.9.0/255.255.255.0 0/0
    Flow destination  : 192.168.14.0/255.255.255.0 0/0
    Qos pre-classify  : Disable
    Qos group         : -

    [Outbound ESP SAs]
      SPI: 3354115212 (0xc7ebbc8c)
      Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-MD5
      SA remaining key duration (bytes/sec): 0/2949
      Outpacket count       : 0
```

UDP encapsulation used for NAT traversal: N

[Inbound ESP SAs]
SPI: 1560642734 (0x5d0584ae)
Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-MD5
SA remaining key duration (bytes/sec): 0/2949
Inpacket count : 0
Inpacket decap count : 0
Inpacket drop count : 0
Max received sequence-number: 0
Anti-replay window size: 32
UDP encapsulation used for NAT traversal: N

退出登录 >

[1]dis ike sa

| Conn-ID | Peer | VPN | Flag(s) | Phase |
|---|---|---|---|---|
| 1481 | 172.x.10.10 | 0 | RD | 2 |
| 1478 | 172.x.10.10 | 0 | RD | 1 |

2. 在AR1220-S上display ipsec statis esp,telnet测试无报文统计,ping测试有报文统计;

3. 192.168.9.253接在Ehternet 0/0/1口上,用了一台台式机接在Ethernet 0/0/2口上,将Ethernet 0/0/2作为观察口,Ehternet 0/0/1做镜像到2上,通过报文头获取

可以看到有到1054端口的报文;

4. 同时在路由器上做1054的流量统计,抓取到了报文,如下:

Interface: Vlanif1
Traffic policy inbound: a
Rule number: 1
Current status: OK!

| Item | Sum(Packets/Bytes) | Rate(pps/bps) |
|---|---|---|
| Matched | 1/90 | 1/96 |
| Passed | 1/90 | 1/96 |
| Dropped | 0/0 | 0/0 |
| Filter | 0/0 | 0/0 |
| CAR | 0/0 | 0/0 |
| Queue Matched | 0/0 | 0/0 |
| Enqueued | 0/0 | 0/0 |
| Discarded | 0/0 | 0/0 |
| CAR | 0/0 | 0/0 |
| Green packets | 0/0 | 0/0 |
| Yellow packets | 0/0 | 0/0 |
| Red packets | 0/0 | 0/0 |

5. 在步骤4的同时display ipsec statistic esp 无报文,如下:

[1]dis ipsec statistics esp
Inpacket count : 0
Inpacket auth count : 0
Inpacket decap count : 0
Outpacket count : 0
Outpacket auth count : 0
Outpacket encap count : 0
Inpacket drop count : 0
Outpacket drop count : 0
BadAuthLen count : 0
AuthFail count : 0
InSAAclCheckFail count : 0
PktDuplicateDrop count : 0
PktSeqNoTooSmallDrop count: 0
PktInSAMissDrop count : 0

以上信息表明AR1220收到了从192.168.9.253发送的telnet报文,但是没有通过IPSEC加密进行转发;192.168.9.253 ping 192.168.14.10则能够进行正常的转发。怀疑设备对于ICMP类报文进行了正常的IPSEC加密,而对于非ICMP报文走了其他的转发流程。

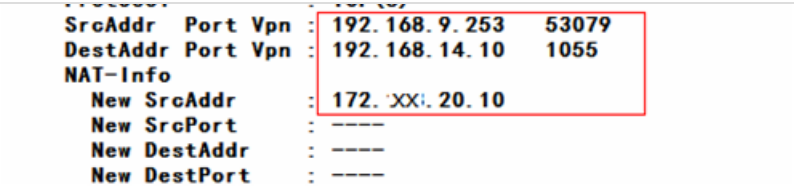
6. 进行一步核实配置,发现在nat outbound中已经排除了两个局域网网段的相互访问,如下:

acl number 3000
rule 5 deny ip source 192.168.9.0 0.0.0.255 destination 192.168.14.0 0.0.0.255
rule 10 permit ip

7. 查看接口上的配置,发现192.168.9.253 地址配置了NAT SERVER,以便外网访问该接口的公网地址和端口号达到访问内网地址192.168.9.253及其端口号的目的。如下:

interface GigabitEthernet0/0/0
description 1_Internet_R_gigabitethernet0/0/0
tcp adjust-mss 1200
ip address 172.XX.20.10 255.255.255.0
nat server protocol tcp global current-interface 8080 inside 192.168.9.253 8080
nat outbound 3000
ipsec policy center_vpn

查看该地址的NAT 会话,显示192.168.9.253访问对端地址时数据报文被转换到了公网,如下:




8. 修改nat server 为nat static再次测试telnet正常:
nat static protocol tcp global current-interface 8080 inside 192.168.9.253 8080

退出登录

## 根因

公网出接口配置为nat server protocol tcp global current-interface 8080 inside 192.168.9.253 8080

该命令会将从192.168.9.253发出的TCP报文都做nat将报文转换掉,所以经转换后的报文无法进IPSec隧道。

将配置修改为nat static protocol tcp global current-interface 8080 inside 192.168.9.253 8080后,业务正常。

Nat static只有是源地址为192.168.9.253且TCP端口号为8080的才会做nat转换,所以修改nat static后可以正常通信。

## 解决方案

修改nat server为nat static protocol tcp global current-interface 8080 inside 192.168.9.253 8080后,业务正常。

上一篇: AR1220的BGP邻居每个半个小时左右就中断一次 下一篇: AR1200 ssh登录掉线问题

## 评论和回复

z******eng 2017-11-18 10:00:38

该用户未发表意见

何** 2016-12-05 11:45:45

非常好的案例，很清楚的解释了nat server与nat static的区别

展开

退出登录 >

S******760 2016-10-18 14:29:56

该用户未发表意见

展开

S******666 2016-10-18 13:46:10

该用户未发表意见

展开

杨* 2016-05-31 09:19:28

该用户未发表意见

王** 2016-05-03 15:58:06

该用户未发表意见

1 到第

意见反馈 | 收藏此案例

## 相关资源

文档
软件
产品公告
工具

## 帮助我们改进

贡献案例

快速链接

华为亿家 App 华为亿企飞 App