MSR810-W-LM IPSEC VPN隧道建立后80端口不通的解决办法

IPSec VPN　高子军　2019-06-23 发表

组网及说明

无

问题描述

某行业需要在两个站点之间建立IPSEC VPN，来实现分部主机访问总部服务器的需求。配置完成后，隧道正常建立，分部主机能访问到总部的服务器业务，但是80端口的业务无法正常访问。

过程分析

1．IPSEC VPN已经正常建立，说明两端设备的IPSEC相关配置没有问题，查看两端的隧道信息：

分部MSR810-W-LM：

```
<MSR810>display ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------
  -----------------------------
  IPsec policy: v7
  Sequence number: 1
  Mode: Template
  -----------------------------
    Tunnel id: 2
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1444
    Tunnel:
        local  address: X.X.228.82
        remote address: X.X.159.252
    Flow:
        sour addr: 10.10.10.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 192.168.10.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 2411258305 (0x8fb8e1c1)
      Connection ID: 279172874247
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/648
      Max received sequence-number: 0
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 2906870646 (0xad435376)
      Connection ID: 227633266694
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/648
      Max sent sequence-number: 0
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

总部MSR930：

```
<MSR930>display ipsec sa
  -----------------------------
  IPsec policy name: "3120"
  sequence number: 10
```

```
 acl version: ACL4
 mode: isakmp
 -----------------------------
  PFS: N, DH group: none
  inside VRF:
  tunnel:
     local  address: X.X.72.13
     remote address: X.X.228.82
  flow:
     sour addr: 10.10.10.0/255.255.255.0  port: 0  protocol: IP
     dest addr: 10.254.1.0/255.255.255.0  port: 0  protocol: IP

  [inbound ESP SAs]
    spi: 0xEBF4441D(3958653981)
    transform: ESP-ENCRYPT-3DES ESP-AUTH-MD5
    in use setting: Tunnel
    connection id: 201
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1841247/3234
    anti-replay detection: Enabled
      anti-replay window size(counter based): 32
    udp encapsulation used for nat traversal: N

  [outbound ESP SAs]
    spi: 0xF9D43EE4(4191436516)
    transform: ESP-ENCRYPT-3DES ESP-AUTH-MD5
    in use setting: Tunnel
    connection id: 202
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1708168/3234
    anti-replay detection: Enabled
      anti-replay window size(counter based): 32
    udp encapsulation used for nat traversal: N
```

2.通过隧道信息查看得知两端的感兴趣流配置一致，并且在设备上也没有做限制。经过进一步测试，Ping服务器地址能通，3389端口能正常通信，只有80端口无法通信。

3.查看总部设备的配置发现在公网口下配置了80端口的映射，由于现场映射业务是一直在使用的，不能进行更改测试；所以新增加了3389端口的映射业务，再次测试发现3389的业务也不能正常访问。

```
interface GigabitEthernet0/3
 port link-mode route
 nat outbound 3001
 nat server 1 protocol tcp global current-interface www inside 10.10.10.10 www
 ip address X.X.X.X 255.255.255.240
 ipsec policy 3120
```

4.由第三步测试得知，80端口的业务无法访问是由于NAT映射导致的，NAT将不该转换的地址做了转换，导致访问服务器的业务异常。

解决方法

在总部设备的公网口下增加如下配置：

```
ipsec no-nat-process enable
```

在某些特殊的应用环境下，用户要求需要被IPSec业务处理的报文，不经过NAT业务处理，即不做NAT地址转换，而直接由IPSec业务进行处理。对于这种情况，可以通过使能本命令，允许接口下的NAT业务将报文透传给IPSec业务处理，不进行NAT转换。

注意：V5平台设备支持该命令，V7平台设备不涉及该问题。

附件下载：MSR810-W-LM ipsec vpn隧道建立后80端口不通的问题.rar