

# VPN 连接 故障处理



腾讯云

## 【 版权声明 】

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

## 【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

## 文档目录

### 故障处理

VPN 通道未联通

VPN 通道已联通但实际内网不通

IPSec VPN 协商失败报错说明

# 故障处理

## VPN 通道未联通

最近更新时间：2024-03-12 10:33:22

### 现象描述

使用 VPN 连接建立 VPC 与 IDC 的通信，完成配置后，发现 VPN 通道状态为**未联通**。



ID/名称	监控	状态	对端网关	所属网络	预共享密钥	操作
[模糊]	[模糊]	已联通	[模糊]	vpc-bslovpcom Default-VPC	[模糊]	重置 更多
vpc-rjvriup test	[模糊]	未联通	[模糊]	vpc-4gxmiok VPC1	[模糊]	重置 更多

### 可能原因

通道状态异常，一般有如下可能原因：

- 无流量激活通道
- VPN 网关公网 IP 不通
- 安全策略配置不正确
- 协商参数、协商模式不一致

### 处理方案

1. 登录 VPC 中的一台服务器，ping 对端 IDC 侧服务器的内网 IP 来激活通道。

#### ① 说明

登录 VPC 中云服务器请参考 [登录 Linux 实例](#) 或 [登录 Windows 实例](#)。

- 如果 ping 通，表示通道已激活，查看 VPN 通道状态是否已联通，如已联通，则问题解决，结束。
- 如果 ping 不通，请直接执行 [步骤2](#)。

2. 请登录 IDC 侧的 VPN 设备，ping 腾讯云侧 VPN 网关的公网 IP（本例假设 VPN 网关公网 IP 为 139.186.120.129），查看是否可以 ping 通。

- 若是，请执行 [步骤4](#)。
- 若否，请执行 [步骤3](#)。

```
[IDC_IPSec] ping 139.186.120.129
PING 139.186.120.129: 56 data bytes, press CTRL_C to break
  Reply from 139.186.120.129: bytes=56 Sequence=1 ttl=255 time=80 ms
  Reply from 139.186.120.129: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 139.186.120.129: bytes=56 Sequence=3 ttl=255 time=50 ms
  Reply from 139.186.120.129: bytes=56 Sequence=4 ttl=255 time=70 ms
  Reply from 139.186.120.129: bytes=56 Sequence=5 ttl=255 time=60 ms

--- 139.186.120.129 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 30/58/80 ms
```

3. 请检查 IDC 侧公网网络连接状态，是否可以正常连接到互联网。

- 若是，请执行 [步骤4](#)。
- 若否，请修复本地网络后，再查看 VPN 通道状态是否已联通，如已联通，则问题解决，结束；如未联通，则继续执行 [步骤4](#)。

4. 查看 IDC 侧 VPN 设备的安全策略，是否放通了腾讯云侧 VPN 网关的公网 IP 地址以及需要互通的内网地址。

```
display current-configuration configuration security-policy //此处以华为防火墙为例
```

- 若是，请执行 [步骤5](#)。
  - 若否，请修改安全策略，放通腾讯云侧 VPN 网关的 IP 以及对应 SPD 策略，再查看 VPN 通道状态是否已联通，如已联通，则问题解决，结束；如未联通，则继续执行 [步骤5](#)。
5. 比对腾讯云侧 VPN 网关与对端 IDC 的 VPN 设备协商参数（IKE、IPsec 配置）及协商模式（主模式 main/野蛮模式 aggressive）是否一致。

#### ⚠ 注意

- 任何一个参数不一致，VPN 通道都无法建立。
- 不同厂家设备、公有云服务提供商的默认 VPN 配置不尽相同。

进入 [VPN 通道控制台](#)，单击实例 ID，进入详情页，在“高级配置”页签中查看：



IDC 侧设备配置参数可通过如下命令获取（此处以华为防火墙为例）：

```
display current-configuration configuration ike profile
display current-configuration configuration ipsec policy
```

- 若是，请执行 [步骤6](#)。
- 若否，请修改相应参数，确保两端配置一致，然后再查看 VPN 通道状态是否已联通，如已联通，则问题解决，结束；如未联通，则继续执行 [步骤6](#)。

6. 请收集以上检查信息，并 [提交工单](#) 或联系设备厂商跟进处理。

# VPN 通道已联通但实际内网不通

最近更新时间：2024-03-12 10:33:22

## 现象描述

使用 VPN 连接建立 VPC 与 IDC 的通信，VPN 通道显示为**已联通**状态，但内网无法联通，现象如下：  
VPN 通道状态为**已联通**：



VPC 侧服务器 ping IDC 侧内网 IP，无法 ping 通：

```
[root@VM-1-11-centos ~]# ping 10.0.0.7
PING 10.0.0.7 (10.0.0.7) 56(84) bytes of data.
[
```

## 可能原因

通道状态正常但内网却无法联通，可能原因如下：

- VPC 子网路由表未添加指向 IDC 侧内网网段的路由
- VPC/IDC 侧的安全策略未放通对应源 IP、目的 IP
- VPN 网关未添加指向 IDC 侧内网网段的通道（路由型）
- VPC/IDC 侧的内网服务器操作系统的防火墙未放行对端网段
- VPC/IDC 侧的 SPD 策略未包含该源 IP、目的 IP
- VPN 网关未配置路由策略

## 处理步骤

1. 检查 VPC 子网路由表中，是否有目的地址为 IDC 侧内网网段，下一跳地址为对应 VPN 网关的路由，同时检查 IDC 侧是否有目的地址为 VPC 网段，下一跳地址为对应 VPN 隧道的路由。

进入 [VPC 子网路由表](#)，单击路由表 ID，进入详情界面检查：

新增路由策略	导出	目标地址	Q			
目的端	下一跳类型	下一跳	备注	启用路由	云联网中状态	操作
				<input checked="" type="checkbox"/>	-	① 发布到云联网
				<input checked="" type="checkbox"/>	-	① 发布到云联网
				<input type="checkbox"/>	-	① 发布到云联网
				<input checked="" type="checkbox"/>	-	编辑 删除 发布到云联网
192.168.0.0/24	VPN网关	vpngw-2gihj15k -test		<input checked="" type="checkbox"/>	-	编辑 删除 发布到云联网

共 7 条 20 条/页 1 / 1 页

IDC 侧执行命令检查路由情况（以华为设备为例）：

```
display ip routing-table //查看是否有对应目的地址为云上 VPC 网段，下一跳为对应 VPN 隧道的路由
```

- 若是，请执行 [步骤3](#)。
- 若否，请根据业务需求，补全相应路由信息，再执行 [步骤2](#)。

2. 检查通信是否恢复正常，即登录 VPC/IDC 中的一台服务器，ping 对端服务器内网 IP。

#### 说明

登录 VPC 中云服务器请参考 [登录 Linux 实例](#) 或 [登录 Windows 实例](#)。

- 若是，通信正常，问题解决，结束。
- 若否，请执行 [步骤3](#)。

3. 检查 VPC 中服务器关联的安全组和子网关联的网络 ACL 是否放通来自云下 IDC 的流量，同时检查 IDC 侧是否放通来自云上 VPC 的流量。

进入 [VPC 中服务器安全组](#) 界面，单击安全组 ID，进入“安全组规则”页检查：

来源	协议端口	策略	备注	修改时间	操作
0.0.0.0	ICMP	允许	放通Ping服务	2021-02-22 14:54:10	编辑 插入 删除
:::0	ICMPv6	允许	放通Ping服务	2021-02-22 14:54:10	编辑 插入 删除

进入 [VPC 子网 ACL 规则](#)，单击网络 ACL ID，进入“基本信息”页，单击“进站规则”页签检查：



规则列表 [编辑](#) [导入规则](#) [导出规则](#)

源IP <sup>①</sup>	协议类型	端口 <sup>①</sup>	策略	备注
192.168.0.0/16	All traffic	ALL	允许	-
0.0.0.0/0	All traffic	ALL	拒绝	-

IDC 侧安全策略检查（此处以华为防火墙为例）：

```
display current-configuration configuration security-policy
```

- 若是，请执行 [步骤5](#)。
- 若否，请放通安全组/网络 ACL/IDC 侧安全设备需要互通的内网地址段，再执行 [步骤4](#)。

4. 检查通信是否恢复正常，即登录 VPC/IDC 中的一台服务器，ping 对端服务器内网 IP。

- 若是，通信正常，问题解决，结束。
- 若否，请执行 [步骤5](#)。

5. 分别检查 VPC 中云服务器和 IDC 侧内网服务器操作系统自带防火墙，是否有放通对端网段的策略。

Linux 服务器查看防火墙：`iptables --list`

Windows 服务器查看防火墙：控制面板/系统和安全/Windows 防火墙/允许的应用

- 若是，请执行 [步骤7](#)。
- 若否，请在内网机器防火墙中放通需要联通的业务网段，再执行 [步骤6](#)。

6. 检查通信是否恢复正常，即登录 VPC/IDC 中的一台服务器，ping 对端服务器内网 IP。

- 若是，通信正常，问题解决，结束。
- 若否，请执行 [步骤7](#)。

7. 分别检查 VPC 和 IDC 侧的 VPN 通道的感兴趣流（SPD 策略）是否包含需要互通的内网网段。

进入 [VPC 侧 SPD 策略](#)，单击 VPN 通道 ID，进入“基本信息”页，即可检查 SPD 策略：

SPD策略 [编辑](#)

规则	本端网段	对端网段
规则1	172.16.0.0/16	192.168.0.0/16

IDC 侧 SPD 策略检查（此处以华为防火墙为例）：

```
display current-configuration configuration acl
```

- 若是，请执行 [步骤8](#)。
- 若否，请补充缺失的 SPD 策略，再执行 [步骤8](#)。

8. 检查 VPN 网关的路由表中是否包含对应的路由策略。进入 VPN 网关，单击 VPN 网关 ID，进入“路由表”页，即可检查路由策略。



- 若是，请执行 [步骤9](#)。
- 若否，请在 VPN 网关 > 路由页签指定下一跳，再执行 [步骤9](#)。



9. 检查通信是否恢复正常，即登录 VPC/IDC 中的一台服务器，ping 对端服务器内网 IP。

- 若是，通信正常，问题解决，结束。
- 若否，请执行 [步骤10](#)。

10. 请收集以上检查信息，并 [提交工单](#) 或联系设备厂商跟进处理。

# IPSec VPN 协商失败报错说明

最近更新时间：2023-06-28 15:45:31

协商阶段	错误提示信息	说明
IKE 协商	no match proposal	云侧和客户侧配置的 IKE 策略不一致，请检查。
	DH group not supported	客户侧配置的 DH 组云侧不支持，请修改您本地配置。
	responder no peer config found by ID payload	云侧配置的本端标识和对端标识与客户侧配置的不一致，致使响应方无应答。
	initiator no peer config found by ID payload	云侧配置的本端标识和对端标识与客户侧配置的不一致，致使请求方无应答。
	received xxx error notify	云侧收到客户侧协商失败的报文。
IPSec 协商	DH group xxx not supported	客户侧配置的 DH 组云侧不支持，请修改您本地的 DH 组。
	reponder no matching CHILD_SA config for TS	云侧和客户侧配置的 ts 不一致，请检查。
	no matching proposal, configured xxx, received xxx	云侧和客户侧配置的 child 不匹配。
	received xxx error notify in the payload	云侧收到客户侧协商失败的报文。