

虚拟专用网络

故障排除

文档版本 01
发布日期 2025-02-05



版权所有 © 华为技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

1 站点入云 VPN 企业版

1.1 VPN 连接状态显示“未连接”

故障现象



在“虚拟专用网络 > 企业版-VPN连接”页面，VPN连接状态显示为“未连接”。

可能原因

- VPN连接两端的连接配置不正确。
- 华为云安全组和客户设备侧ACL配置不正确。
- IPsec-VPN连接协商失败或连接断连。

处理步骤

- 检查VPN连接两端的连接配置。
 - 确认两端配置的网关IP参数是否为镜像。
 - VPN网关的主/备EIP可以选择“虚拟专用网络 > 企业版-VPN网关”，在网关IP栏下查看。
 - 客户设备侧网关的公网IP可以选择“虚拟专用网络 > 企业版-对端网关”，在网关IP栏下查看。
 - 确认IKE策略、IPsec策略协商参数是否一致。
 - IKE策略、IPsec策略协商参数可以选择“虚拟专用网络 > 企业版-VPN连接”，单击“修改策略配置”查看。
 - 确认预共享密钥是否一致。
 - 预共享密钥无法在云上直接查看。如果不确认预共享密钥，建议根据客户设备侧的预共享密钥对VPN连接的预共享密钥进行重置。
可以选择“虚拟专用网络 > 企业版-VPN连接”，选择“更多 > 重置密钥”进行重置。
 - 如果连接模式采用策略模式，请确认两端策略规则中的源网段和目的网段是否为镜像。

- 策略规则可以选择“虚拟专用网络 > 企业版-VPN连接”，单击“修改连接信息”查看。
- 如果连接模式采用静态路由模式且云侧开启了NQA功能，请确认客户设备侧是否已经正确配置Tunnel隧道的IP地址。
 - 是否开启NQA功能，可以选择“虚拟专用网络 > 企业版-VPN连接”，单击VPN连接名称，在“基本信息”页签查看“检测机制”。
 - 客户设备侧在华为云VPN连接已设置的Tunnel隧道的IP地址，可以选择“虚拟专用网络 > 企业版-VPN连接”，单击“修改连接信息”，查看本端接口地址和对端接口地址。华为云VPN连接的本端接口地址和对端接口地址需要和客户设备的本端接口地址和对端接口地址互为镜像配置。
 - 如果连接模式采用BGP路由模式，请确认两端的BGP ASN是否为镜像。
 - VPN网关的BGP ASN可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称，在“基本信息”页签查看。
 - 客户设备侧网关的BGP ASN可以选择“虚拟专用网络 > 企业版-对端网关”，在BGP ASN栏下查看。
 - 检查华为云安全组和客户设备侧ACL配置。
 - 确认华为云default安全组已经放通客户设备侧公网IP的端口。
华为云default安全组查看步骤如下：
 - i. 选择“虚拟专用网络 > 企业版-VPN网关”，单击关联的VPC名称。
 - ii. 单击VPC对应的路由表。
 - iii. 单击路由表的名称。
 - iv. 找到VPN网关主或备EIP的下一跳，单击下一跳名称。
 - v. 在“关联安全组”页签，检查端口放通情况。
 - 确认客户设备侧安全组已经放通VPN网关主备EIP的端口。
 - 查看IPsec连接日志。
 - a. 登录管理控制台。
 - b. 在管理控制台左上角单击  图标，选择区域和项目。
 - c. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
 - d. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
 - e. 在“VPN连接”界面，找到目标VPN连接，选择“更多 > 查看日志”，查看相关日志信息。

查看IPsec连接日志的过程中，您可以根据日志关键字对照[表 VPN未连接的常见原因](#)中的错误码自主排查问题。

表 1-1 VPN 未连接的常见原因

| 分类 | 错误码 | 描述 |
|-----------------|---------------------------------|--------------------------------------|
| IPsec-VPN连接协商失败 | phase1 proposal mismatch | 两端IKE安全提议参数不匹配。 |
| | phase2 proposal or pfs mismatch | 两端IPSec安全提议参数、PFS算法或Security ACL不匹配。 |

| 分类 | 错误码 | 描述 |
|----|-----------------------------|-------------------------------|
| | responder dh mismatch | 响应方的DH算法不匹配。 |
| | initiator dh mismatch | 发起方的DH算法不匹配。 |
| | encapsulation mode mismatch | 封装模式不匹配。 |
| | flow or peer mismatch | 两端Security ACL或IKE Peer地址不匹配。 |
| | version mismatch | 两端IKE版本号不匹配。 |
| | peer address mismatch | 两端的IKE Peer地址不匹配。 |
| | config ID mismatch | 根据ID未找到匹配的IKE Peer。 |
| | exchange mode mismatch | 两端的协商模式不匹配。 |
| | authentication fail | 身份认证失败。 |
| | construct local ID fail | 构造本端ID失败。 |
| | rekey no find old sa | 重协商时找不到旧的SA。 |
| | rekey fail | 重协商时旧的SA正在下线。 |
| | first packet limited | 首包限速。 |
| | unsupported version | 不支持的IKE版本号。 |
| | malformed message | 畸形消息。 |
| | malformed payload | 畸形载荷。 |
| | critical drop | 未识别的critical载荷。 |
| | cookie mismatch | Cookie不匹配。 |
| | invalid cookie | 无效Cookie。 |
| | invalid length | 报文长度非法。 |
| | unknown exchange type | 未知的协商模式。 |
| | uncritical drop | 未识别的非critical载荷。 |
| | route limit | 路由注入的数目达到规格。 |
| | ip assigned fail | IP地址分配失败。 |
| | eap authentication timeout | EAP认证超时。 |
| | eap authentication fail | EAP认证失败。 |

| 分类 | 错误码 | 描述 |
|---------------|--|----------------------------|
| | xauth authentication fail | XAUTH认证失败。 |
| | xauth authentication timeout | XAUTH认证超时。 |
| | license or specification limited | License限制。 |
| | local address mismatch | IKE协商时的本端IP地址和接口IP地址不匹配。 |
| | dynamic peers number reaches limitation | IKE对等体数达到规格。 |
| | ipsec tunnel number reaches limitation | IPSec隧道数达到规格。 |
| | netmask mismatch | 开启IPSec掩码过滤功能后，掩码不匹配。 |
| | flow confict | 数据流冲突。 |
| | proposal mismatch or use sm in ikev2 | IPSec安全提议不匹配或者IKEv2使用SM算法。 |
| | ikev2 not support sm in ipsec proposal ikev2 | IKEv2不支持IPSec安全提议的SM算法。 |
| | no policy applied on interface | 没有策略应用到接口上。 |
| | nat detection fail | NAT探测失败。 |
| | fragment packet limit | 分片报文超规格。 |
| | fragment packet reassemble timeout | 分片报文重组超时。 |
| IPsec-VPN连接断连 | dpd timeout | DPD探测超时。 |
| | peer request | 对端发送删除消息。 |
| | config modify or manual offline | 修改配置导致SA被删除或者手动清除SA。 |
| | phase1 hard expiry | 第一阶段硬超时（没有新的SA协商成功）。 |
| | phase2 hard expiry | 第二阶段硬超时。 |
| | heartbeat timeout | heartbeat探测超时。 |
| | re-auth timeout | 重认证超时导致SA被删除。 |
| | aaa cut user | AAA模块强制用户下线导致SA被删除。 |

| 分类 | 错误码 | 描述 |
|----|--|------------------------------|
| | ip address syn failed | IP地址同步失败。 |
| | hard expiry triggered by port mismatch | NAT端口不匹配导致硬超时。 |
| | kick old sa with same flow | 相同的流接入时删除老的SA。 |
| | cpu table updated | 插拔SPU板时删除非本CPU的SA。 |
| | flow overlap | 加密流中的IP地址与对端的IP地址冲突。 |
| | spi conflict | SPI冲突。 |
| | phase1 sa replace | 新IKE SA替换老的IKE SA。 |
| | phase2 sa replace | 新IPSec SA替换老的IPSec SA。 |
| | nhrp notify | NHRP通知删除SA。 |
| | receive backup delete info | 备机收到主机的SA备份删除消息。 |
| | eap delete old sa | 对端设备重复进行EAP认证时本端设备删除老的SA。 |
| | receive invalid spi notify | 收到无效SPI通知。 |
| | dns resolution status change | DNS解析状态发生改变。 |
| | ikev1 phase1-phase2 sa dependent offline | 设备删除IKEv1 SA时删除其关联的IPSec SA。 |
| | exchange timeout | 报文交互超时。 |
| | hash gene adjusted | Hash因子调整导致IPSec隧道被删除。 |

如果上述场景均正确且异常仍然存在，请[提交工单](#)联系华为工程师。

1.2 云上云下无法 Ping 通

故障现象

- 云下数据中心服务器无法Ping通华为云VPC上的ECS服务器。
- 华为云VPC上的ECS服务器无法Ping通云下数据中心服务器。

可能原因

- 华为云安全组配置不正确

- 互联子网的ACL规则配置不正确
- 客户设备侧放通策略配置不正确
- 客户设备侧路由配置不正确

处理步骤


- 检查华为云安全组配置
 - 确认华为云default安全组已经放通去往对端子网数据流。
华为云default安全组查看步骤如下：
 - i. 选择“虚拟专用网络 > 企业版-VPN网关”，单击关联的VPC名称。
 - ii. 单击VPC对应的路由表。
 - iii. 单击路由表的名称。
 - iv. 找到VPN网关主或备EIP的下一跳，单击下一跳名称。
 - v. 在“关联安全组”页签，检查端口放通情况。
 - 确认华为云default安全组已经放通来自对端子网数据流。
 - 确认华为云default安全组已经放通去往本端子网数据流。
 - 确认华为云default安全组已经放通来自本端子网数据流。
 - 确认华为云ECS所在的安全组已经放通去往对端子网数据流。
ECS安全组可以选择“计算 > 虚拟弹性云服务器”，单击ECS名称，选择“安全组”，单击“配置规则”查看。
 - 确认华为云ECS所在的安全组已经放通来自对端子网数据流。
- 互联子网的ACL规则配置不正确
 - 确认互联子网的ACL规则中，是否已放通所有本端子网到对端子网的端口。
 - i. 选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称。
 - ii. 在“基本信息”页签，记录互联子网信息。
 - iii. 在“基本信息”页签，单击关联模式对应的VPC名称。
 - iv. 在VPC“基本信息”页签右边“网络互通概览”区域，单击子网个数。
 - v. 根据网段匹配互联子网，并单击“网络ACL”的ACL名称。
 - vi. 放通所有本端子网到对端子网的端口。
- 检查客户设备侧放通策略
 - 确认客户设备侧已经放通去往华为云VPN本端子网的数据流。
 - 确认客户设备侧已经放通来自华为云VPN本端子网的数据流。
华为云本端子网可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称，在“基本信息”页签查看。
- 检查客户设备侧路由配置
 - 确认公网路由配置正确：目的地址为华为云VPN网关EIP地址，下一跳为设备出口地址。
 - 确认私网路由配置正确：目的地址为华为云VPN本端子网，下一跳为设备出口地址。
华为云本端子网可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称，在“基本信息”页签查看。

1.3 流量丢包

故障现象

- 云下数据中心服务器对华为云VPC上的ECS服务器执行Ping操作时，存在流量丢包。
- 华为云VPC上的ECS服务器对云下数据中心服务器执行Ping操作时，存在流量丢包。

处理步骤

- 检查客户侧组网和带宽情况
 - 确认客户网络的组网是否多出口，是否因为负载分担组网将流量分配到非VPN连接出口导致流量丢包，确保数据流恒定走特定出口访问华为云。
 - 使用客户侧VPN网关地址Ping华为云VPN网关IP以及其他公网（例如：114.114.114.114），检查公网时延、丢包率。
如果公网网络质量存在问题，建议向所在网络提供运营商进行求助。
 - 检查客户出口设备带宽是否超限。
- 检查华为云侧组网和带宽情况
 - 检查华为云VPN网关的带宽是否超限。
 - i. VPN网关主/备EIP带宽规格大小，可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称查看。
 - ii. VPN网关实际带宽使用情况可以选择“虚拟专用网络 > 企业版-VPN网关”，单击公网IP栏主/备EIP对应的，查看带宽是否达到上限。
如果超限，可以通过扩容VPN网关的带宽进行解决。
- 如果上述场景均正确且异常仍然存在，请[提交工单](#)联系华为工程师。

2 站点入云 VPN 经典版

2.1 常规检查项

用户在华为云VPN产品使用过程中，通常会出现由于配置错误（华为云侧或用户侧协商策略、防火墙、路由表、域间策略、NAT配置、安全组等信息配置）而导致连接故障或无法PING通。

通常可使用以下方式排除故障：

- [检查VPN两侧协商信息](#)
- [检查客户防火墙ACL和云端安全组配置](#)
- [检查防火墙路由表](#)
- [检查客户防火墙域间策略](#)
- [检查防火墙NAT配置](#)

检查 VPN 两侧协商信息

- 确认PSK共享密钥是否一致。
- 确认IKE策略、IPsec策略协商参数是否一致。
- 确认两侧的本地子网和远端子网配置是否互为镜像。

检查客户防火墙 ACL 和云端安全组配置

- 确认放行去往华为云VPC子网的数据流。
- 确认放行来自华为云VPC子网的数据流。

检查防火墙路由表

确认存在目标地址为华为云VPC子网的路由信息：

- 确认配置去往华为云目标网络的路由信息，路由表或VPN路由表中存在路由信息。
- 确认路由转发表状态正常。

📖 说明

路由易错配置：

1. 目的网段与华为云VPC网段不一致，导致前往华为云的流量无法路由到配置IPsec策略的公网口。
2. 配置静态路由时指定出接口，而非指定下一跳。
在ethernet类型的网络中，出接口会因为无法学习到对端的ARP信息而导致路由转发失败。
3. 将路由的下一跳地址指定为华为云端的VPN网关地址。
部分友商设备会因为路由信息无法自动迭代而不可行；由于VPN流量是要从公网口发出的，因此下一跳地址必须是运营商提供的网关地址。

检查客户防火墙域间策略

- trust到untrust：放行本地VPC到云上VPC子网访问策略。
- untrust到trust：放行云上VPC到本地VPC子网访问策略。

检查防火墙 NAT 配置

确认本地VPN网关是否在NAT设备后（一般是边界防火墙）进行部署，即VPN网关的出接口使用私有地址，然后在NAT设备上做公网地址转换。

这种场景也被称为IPsec nat穿越。

2.2 常见配置问题及解决方案

- PSK不一致：单独更新预共享密钥会在下一次IKE协商时生效，最长等待一个IKE的生命周期，须确认两端更新密钥一致。
- 协商策略不一致：请仔细排查IKE中的认证算法、加密算法、版本、DH组、协商模式和IPsec中的认证算法、加密算法、封装格式、PFS算法，特别注意PFS和云下配置一致，部分设备默认关闭了PFS配置。
- 感兴趣流：两端ACL配置不互为镜像，特别注意云下的ACL配置不能采用地址组名称，要使用真实的IP地址+掩码。
- NAT配置：云下子网访问云上子网配置为NONAT，云下公网IP不能被二次NAT为设备的接口IP。
- 安全策略：放行云下子网访问云上子网的所有协议，放行两个公网IP间的ESP、AH及UDP的500和4500端口。
- 路由配置：添加访问云上子网的出接口路由为隧道接口或IPsec协商出口，注意出接口的下一跳ARP解析要可达。

更多故障排除案例请详细查看[连接故障或无法PING通](#)。

3 终端入云 VPN

3.1 客户端连接失败

3.1.1 客户端日志显示“Connection failed to establish within given time”

适用的客户端

Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
Connection failed to establish within given time
```

可能原因

- 客户端设备无法正常访问Internet网络。
- 现有客户端配置文件与VPN网关“服务端”页签中的客户端配置文件不一致。

处理步骤

1. 请在客户端设备上尝试访问其他Internet服务，查看网络是否正常。
如果无法访问，请联系运营商排除网络问题。
2. 请登录华为云管理控制台。
3. 找到对应的VPN网关，查看网关的地址、服务端的端口和协议与客户端配置文件中的信息是否一致。
如果不一致，请重新下载客户端配置文件或直接修改客户端配置文件中对应的信息，客户端使用新的配置重新接入。

3.1.2 客户端日志显示“Cannot load CA certificate file [[INLINE]](no entries were read)”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
Cannot load CA certificate file [[INLINE]](no entries were read)
```

可能原因

客户端配置文件中缺少客户端证书和私钥。

处理步骤

请复制客户端证书和私钥到客户端配置文件中，再重新接入。示例如下：

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

3.1.3 客户端日志显示“error:068000A8:asn1 encoding routines:wrong tag”

适用的客户端

- Linux
- Windows OpenVPN GUI
- Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
error:068000A8:asn1 encoding routines:wrong tag
```

可能原因

客户端证书和私钥不匹配。

处理步骤

检查并复制匹配的客户端证书和私钥到客户端配置文件中，再重新接入。示例如下：

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

3.1.4 客户端日志显示“OpenSSL: error:0A000086:SSL routines::certificate verify failed”

适用的客户端

- Linux
- Windows OpenVPN GUI
- Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
OpenSSL: error:0A000086:SSL routines::certificate verify failed
```

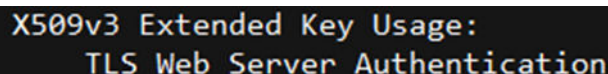
可能原因

VPN网关使用的服务端证书缺少Extended Key Usage扩展属性，导致验证失败。

处理步骤

1. 请检查并确保生成的服务端证书中包含Extended Key Usage扩展属性，如[图3-1](#)所示。

图 3-1 Extended Key Usage



X509v3 Extended Key Usage:
TLS Web Server Authentication

- 使用Easy-RSA的shell命令“`./easymrsa build-server-full`”生成的服务端证书默认携带此属性。
 - 使用OpenSSL自签发的服务端证书不携带此扩展属性，需要在证书文件中补充配置“`extendedKeyUsage = serverAuth`”。
2. 将包含该属性的服务端证书托管到云证书管理服务中，在VPN网关的“服务端”页签中更换服务端证书，客户端再重新接入。

3.1.5 客户端日志显示“TLS Error: TLS handshake failed”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
TLS Error: TLS handshake failed
```

可能原因

客户端配置文件中的证书和私钥与VPN网关“服务端”页签中导入的客户端CA证书不匹配。

处理步骤

1. 请检查导入的客户端CA证书是否正确。
如果配置文件中的证书和私钥与导入的客户端CA证书不匹配，请在VPN网关的“服务端”页签中导入正确的CA证书，并删除错误的CA证书，再使用客户端重新接入。
2. 请检查配置文件中的证书和私钥是否正确。
如果配置文件中的证书和私钥不匹配，请重新复制客户端证书和私钥到客户端配置文件中，再使用客户端重新接入。

3.1.6 客户端日志显示“Options error: Unrecognized option or missing or extra parameter(s) in XXX: disable-dco”

适用的客户端

Linux

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
Options error: Unrecognized option or missing or extra parameter(s) in XXX: disable-dco
```

可能原因

OpenVPN 2.6版本之前的客户端软件，无法识别“disable-dco”配置项。

处理步骤

1. 登录华为云管理控制台。
2. 下载客户端配置，会生成“client_config.ovpn”文件。
3. 打开“client_config.ovpn”文件，在“**disable-dco**”配置项前加上“#”注释。

4. 保存配置文件后，客户端使用新的配置重新接入。

3.1.7 客户端日志显示“TCP: connect to [AF_INET] *.*.*.*:**** failed: Unknown error”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
TCP: connect to [AF_INET] *.*.*.*:**** failed: Unknown error
```

可能原因

- 客户端设备无法正常访问Internet网络。
- 现有客户端配置文件中的协议或端口与VPN网关的“服务端”页签中配置的不一致。

处理步骤

1. 请在客户端设备上尝试访问其他Internet服务，查看网络是否正常。
如果无法访问，请联系运营商排除网络问题。
2. 登录华为云管理控制台。
3. 找到对应的VPN网关，查看服务端的协议和端口与客户端配置文件中的信息是否一致。
如果不一致，请重新下载客户端配置文件或直接修改客户端配置文件中对应的信息，客户端使用新的配置重新接入。

3.1.8 客户端日志显示“AUTH: Received control message: AUTH_FAILED”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
AUTH: Received control message: AUTH_FAILED
```

可能原因

- 用户名和用户密码不匹配。
- 使用同一个用户名连续输入5次错误密码后，用户会被锁定。

- 如果用户配置了静态IP，用户只能建立1个客户端连接，其他的客户端连接会建连失败。

处理步骤

1. 登录华为云管理控制台。
2. 请检查登录客户端使用的用户名和密码。
如果是用户在多次输入错误密码而被系统锁定的情况下，请等待大概5分钟，再重新使用用户名密码登录客户端。
3. 请检查客户端是否配置了静态IP。
请在对应VPN网关操作列单击“查看服务端”，选择“用户管理 > 用户”，查看用户是否配置了静态IP。

如果上述操作仍然无法解决客户端登录问题，请[提交工单](#)联系华为工程师。

3.1.9 客户端日志显示“AUTH_FAILED”

适用的客户端

Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
AUTH_FAILED
```

可能原因

- 用户名和用户密码不匹配。
- 使用同一个用户名连续输入5次错误密码后，用户会处于被锁定中。
- 客户端配置文件中的证书和私钥与VPN网关“服务端”页签中导入的客户端CA证书不匹配。
- 如果用户配置了静态IP，用户只能建立1个客户端连接，其他的客户端连接会建连失败。

处理步骤

1. 请检查登录客户端使用的用户名和密码。
如果是用户在多次输入错误密码而被系统锁定的情况下，请等待大概5分钟，再重新使用用户名密码登录客户端。
2. 请检查导入的客户端CA证书是否正确。
如果配置文件中的证书和私钥与导入的客户端CA证书不匹配，请在VPN网关的服务端中导入正确的CA证书，并删除错误的CA证书，再使用客户端重新接入。
3. 请检查配置文件中的证书和私钥是否正确。
如果配置文件中的证书和私钥不匹配，请重新复制客户端证书和私钥到客户端配置文件中，再使用客户端重新接入。
4. 请检查客户端是否配置了静态IP。
请在对应VPN网关操作列单击“查看服务端”，选择“用户管理 > 用户”，查看用户是否配置了静态IP。

如果上述操作仍然无法解决客户端登录问题，请[提交工单](#)联系华为工程师。

3.2 客户端连接成功，业务无法正常使用

3.2.1 客户端无法 ping 通 ECS 的 IP 地址

故障现象

客户端正常连接终端入云VPN网关，但不能ping通需要访问的ECS的IP地址。

可能原因

- 客户端设备或ECS禁止ping探测。
- ECS安全组禁止ping探测。
- VPN网关本端网段未包含需要访问的ECS的IP地址。
- 没有配置用户所属用户组，或者用户组没有配置对应访问策略。
- 当用户修改指定IP，客户端自动重连后，Windows系统的路由表中未生成目的地为本端子网的路由。

处理步骤

1. 确认客户端设备和ECS的访问控制策略是否禁止ping探测。
如果禁止，请修改策略放通ping探测。Windows操作系统还需要修改防火墙的入站规则，允许ICMPv4-In。
2. 请确认ECS安全组的出方向和入方向规则都放通ICMP。
3. 在VPN网关的“服务端”页签中修改本端网段，使其包含需要访问的ECS的IP地址，然后断开客户端连接，重新接入，并查看客户端设备是否可以接收到VPN网关推送的路由。
 - Windows：使用`route print`命令。
 - Linux：使用`ip route show all`命令。
4. 在服务端配置的用户管理中，配置用户所属用户组，或者在用户组中配置对应访问策略。
5. 查看服务端配置的本端网段和客户端地址池。
 - 本端网段为192.168.1.XX。
 - 客户端地址池为172.16.0.0。
6. 在客户端系统上查看本端网段对应的路由是否生成。
 - 如果生成对应的路由，客户端分配到的IP为172.16.0.5。

回显信息如下：

```
IPv4 路由表
=====
活动路由:
网络目标      网络掩码      网关      接口  跃点数
192.168.1.XX  255.255.255.0  172.16.0.0  172.16.0.5  281
192.168.2.XX  255.255.255.0  172.16.0.0  172.16.0.5  281
192.168.3.XX  255.255.255.0  172.16.0.0  172.16.0.5  281
=====
```

 - 如果未生成对应的路由，请断开客户端连接，重新接入。

3.2.2 客户端业务访问过程中出现丢包

故障现象

客户端正常连接终端入云VPN网关，但业务访问过程中出现丢包。

可能原因

- 业务流量有突发或持续超过VPN网关实例的带宽规格。
- VPN网关绑定的EIP带宽不足。
- Internet网络质量不佳。

处理步骤

1. 在VPN网关列表页跳转到流量监控视图，确认流量是否突发或持续接近VPN网关的带宽规格。
2. 在VPN网关的“基本信息”页面查看EIP带宽大小，并结合流量监控视图，排查是否超过EIP的带宽规格。
如果因EIP带宽规格偏小导致流量超限，请修改EIP的带宽。
3. 通过在客户端ping VPN网关的公网IP地址探测公网链路质量。
若探测结果不佳，请联系运营商进行网络问题排查。