天翼云·VPN 连接

用户指南

天翼云科技有限公司

目 录

1 产品介绍.....12
1.1 什么是 VPN 连接.....12
1.2 产品优势.....13
1.3 产品功能.....13
1.4 应用场景.....15
1.4.1 场景 1：混合云部署.....15
1.4.2 场景 2：跨地域 VPC 互联.....16
1.4.3 场景 3：多企业分支互联.....16
1.4.4 场景 4：VPN 和专线互备.....17
1.5 产品规格.....18
1.6 企业版 VPN 与经典版 VPN 的区别.....19
1.7 约束与限制.....20
1.8 权限管理.....21
1.9 与其他服务的关系.....24
1.10 基本概念.....25
1.10.1 IPsec VPN.....25
1.10.2 VPN 网关.....25
1.10.3 VPN 连接.....25
1.10.4 VPN 网关带宽.....25
1.10.5 本端子网.....26
1.10.6 对端网关.....26
1.10.7 对端子网.....26
1.10.8 预共享密钥.....26
1.11 参考标准和协议.....26
2 快速入门.....28
2.1 通过企业版 VPN 实现数据中心和 VPC 互通.....28
2.1.1 入门指引.....28
2.1.2 步骤一：创建 VPN 网关.....31
2.1.3 步骤二：创建对端网关.....32
2.1.4 步骤三：创建第一条 VPN 连接.....32

2.1.5 步骤四：创建第二条 VPN 连接.....34
2.1.6 步骤五：配置对端网关设备.....35
2.1.7 步骤六：验证网络互通情况.....38
2.2 经典版 VPN 创建流程.....39
2.2.1 创建 VPN 网关.....39
2.2.2 创建 VPN 连接.....39
2.2.3 配置对端设备.....39
3 权限管理.....41
3.1 创建用户并授权使用 VPN.....41
3.2 VPN 自定义策略.....42
4 用户指南.....45
4.1 企业版 VPN 网关管理.....45
4.1.1 创建 VPN 网关.....45
4.1.2 查看已创建的 VPN 网关.....50
4.1.3 修改已创建的 VPN 网关.....50
4.1.4 修改 VPN 网关策略模板.....51
4.1.5 绑定弹性公网 IP.....54
4.1.6 解绑弹性公网 IP.....54
4.1.7 删除 VPN 网关.....54
4.1.8 上传 VPN 网关证书.....55
4.1.9 更换 VPN 网关证书.....56
4.1.10 按标签搜索 VPN 网关.....58
4.2 企业版对端网关管理.....58
4.2.1 创建对端网关.....58
4.2.2 查看已创建的对端网关.....60
4.2.3 修改已创建的对端网关.....60
4.2.4 删除对端网关.....60
4.2.5 上传对端网关证书.....61
4.2.6 更换对端网关证书.....61
4.2.7 按标签搜索对端网关.....62
4.3 企业版 VPN 连接管理.....63
4.3.1 创建 VPN 连接.....63
4.3.2 创建健康检查.....73
4.3.3 查看已创建的 VPN 连接.....73
4.3.4 修改已创建的 VPN 连接.....74
4.3.5 删除 VPN 连接.....76
4.3.6 按标签搜索 VPN 连接.....76
4.4 经典版 VPN 网关管理.....77
4.4.1 创建 VPN 网关.....77

4.4.2 查看已创建的 VPN 网关.....78
4.4.3 修改已创建的 VPN 网关.....78
4.4.4 删除 VPN 网关.....79
4.5 经典版 VPN 连接管理.....79
4.5.1 创建 VPN 连接.....79
4.5.1 查看已创建的 VPN 连接.....84
4.5.2 修改已创建的 VPN 连接.....84
4.5.3 删除 VPN 连接.....85
4.6 监控.....85
4.6.1 监控 VPN.....85
4.6.2 支持的监控指标（企业版 VPN）.....86
4.6.3 支持的监控指标（经典版 VPN）.....88
4.6.4 查看监控指标.....90
4.6.5 创建告警规则.....92
4.7 审计.....92
4.7.1 云审计服务支持的 VPN 操作列表.....92
4.7.2 查看云审计日志.....93
5 故障排除.....94
5.1 VPN 连接状态显示“未连接”.....94
5.2 云上云下无法 Ping 通.....95
5.3 流量丢包.....96
5.4 适用于经典版 VPN.....97
5.4.1 常规检查项.....97
5.4.2 常见配置问题及解决方案.....98
6 常见问题.....99
6.1 热点问题.....99
6.1.1 哪些设备可以与云进行 VPN 对接？.....99
6.1.2 VPN 协商参数有哪些？默认值是什么？.....100
6.1.3 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联？.....102
6.1.4 是否可以通过 VPN 实现跨境访问网站？.....102
6.1.5 VPN 连接是什么？用户在购买 VPN 网关时如何选择 VPN 连接数？.....102
6.1.6 VPN 连接中断后会通知我吗？.....103
6.1.7 建立 IPsec VPN 连接需要账户名和密码吗？.....103
6.1.8 IPsec VPN 是否会自动建立连接？.....103
6.1.9 VPN 网关删除后公网地址是否可以保留？.....103
6.1.10 VPN 监控可以监控哪些内容？.....103
6.1.11 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？.....104
6.1.12 如何测试 VPN 速率情况？.....104
6.1.13 VPC、VPN 网关、VPN 连接之间有什么关系？.....106

6.1.14 如何理解 VPN 连接中的对端网关和对端子网？ 106
6.1.15 连接云下的多台服务器需要购买几个连接？ 107
6.1.16 VPN 支持将两个 VPC 互连吗？ 107
6.1.17 使用 VPN 会对本地网络造成哪些影响，访问云端主机在路由上会有哪些变化？ 107
6.1.18 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置？ 107
6.1.19 如何防止 VPN 连接出现中断情况？ 107
6.1.20 如何解决 VPN 连接无法建立连接问题？ 108
6.1.21 EIP 能作为 VPN 的网关 IP 吗？ 108
6.1.22 VPN 配置完成了，为什么连接一直处于未连接状态？ 108
6.1.23 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置？ 109
6.2 组网与使用场景 109
6.2.1 是否可以通过 VPN 实现跨境访问网站？ 109
6.2.2 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联？ 109
6.2.3 连接云下的多台服务器需要购买几个连接？ 109
6.2.4 VPN 支持将两个 VPC 互连吗？ 110
6.2.5 使用 VPN 会对本地网络造成哪些影响，访问云端主机在路由上会有哪些变化？ 110
6.2.6 通过 VPN 来实现云下 IDC 与云端 VPC 的互通，两端分别需要做哪些配置？ 110
6.2.7 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置？ 110
6.2.8 同一个 Region 的两个 VPC 可以通过 VPN 连通吗？ 111
6.2.9 可以通过哪些方式连通同一个 Region 的两个 VPC？ 111
6.2.10 云端创建了两个 VPC，如何与云下的 IDC 网络互通？ 111
6.2.11 云端两个 Region，每 Region 有两个子网，是否可以创建两个 VPN 连接，分别连通不同子网？ 111
6.2.12 VPN 和 OBS 可以直接通信吗？ 111
6.2.13 用户本地电脑如何连接云上 VPN？ 111
6.2.14 公司网络已通过 VPN 连通了云，我如何在家访问云 ECS？ 112
6.2.15 购买 VPN 网关和连接后，发现云下没有支持 IPsec 的设备，如何临时建立 VPN 连接？ 112
6.2.16 如何选择在云上的哪个区域创建 VPN 网关？ 112
6.3 产品与使用 112
6.3.1 VPC、VPN 网关、VPN 连接之间有什么关系？ 112
6.3.2 VPN 配置下发后，多久能够生效？ 112
6.3.3 VPN 配置完成了，为什么连接一直处于未连接状态？ 113
6.3.4 VPN 网关删除后公网地址是否可以保留？ 113
6.3.5 已经创建的 VPN 哪些信息可以修改，哪些信息不可以修改？ 113
6.3.6 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置？ 114
6.3.7 创建 VPN 连接时添加对端子网，提示系统异常，如何处理？ 114
6.3.8 Console 界面在哪添加 VPN 远端路由？ 115
6.3.9 如何理解 VPN 连接中的对端网关和对端子网？ 115
6.3.10 创建 VPN 连接时如何关闭 PFS？ 115
6.3.11 VPN 本端子网和对端子网的数量有限制吗？ 115

6.3.12 配置 VPN 连接的本端子网和对端子网时需要注意什么？ 115
6.3.13 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接？ 115
6.3.14 修改协商策略后，页面显示资源不存在，如何处理？ 116
6.3.15 VPN 网关最大支持多大带宽？ 116
6.3.16 创建 VPN 连接时如何选择 IKE 的版本？ 116
6.3.17 建立 IPsec VPN 连接需要账户名和密码吗？ 118
6.3.18 VPN 监控可以监控哪些内容？ 118
6.3.19 VPN 连接中断后会通知我吗？ 118
6.4 VPN 协商与对接 119
6.4.1 哪些设备可以与云进行 VPN 对接？ 119
6.4.2 VPN 协商参数有哪些？默认值是什么？ 119
6.4.3 IPsec VPN 是否会自动建立连接？ 121
6.4.4 如何配置 VPN 对端设备？（HUAWEI USG6600 配置示例） 121
6.4.5 VPN 支持对端网关域名对接吗？ 123
6.4.6 我创建的 VPN 连接有几个隧道？ 123
6.4.7 如何在已创建的 VPN 连接中，限定特定的主机访问云上子网？ 124
6.4.8 VPN 是否启动了 DPD 检测机制？ 124
6.4.9 如何通过安全组控制使 VPN 不能访问 VPC 上的部分虚拟机，实现安全隔离？ 124
6.4.10 修改 VPN 连接的配置会造成连接重建吗？ 125
6.4.11 云对接 AWS 后，为何不可以从 AWS 向云发起协商？ 125
6.4.12 对接云时，如何配置 DPD 信息？ 125
6.4.13 本地防火墙无法收到 VPN 网关的 IKE 第一阶段的回复包怎么解决？ 125
6.4.14 本地防火墙无法收到 VPN 子网的回复包怎么解决？ 126
6.4.15 VPN 使用的 DH group 对应的比特位是多少？ 126
6.5 连接故障或无法 PING 通 127
6.5.1 VPN 配置完成了，为什么连接一直处于未连接状态？ 127
6.5.2 如何防止 VPN 连接出现中断情况？ 127
6.5.3 使用中 IPsec VPN 连接中断后如何快速恢复？ 127
6.5.4 VPN 网关带宽到达限额时有什么影响？ 128
6.5.5 IPsec VPN 是否会自动建立连接？ 128
6.5.6 两个 Region 创建的 VPN 连接状态正常，为什么不能 ping 通对端 ECS？ 128
6.5.7 IDC 与云端对接，VPN 连接正常，子网间业务无法互相访问？ 128
6.5.8 正在使用 VPN 出现了连接中断，提示数据流不匹配，如何排查？ 128
6.5.9 正在使用 VPN 出现了连接中断，提示 DPD 超时，如何排查？ 129
6.5.10 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接？ 129
6.5.11 VPN 连接中断后会通知我吗？ 129
6.5.12 如何解决 VPN 连接无法建立连接问题？ 129
6.5.13 VPN 建立后您的数据中心或局域网无法访问弹性云主机？ 130
6.5.14 为什么 VPN 创建成功后状态显示未连接？ 130

6.5.15 VPN 是否启动了 DPD 检测机制？ 130
6.6 公网地址 130
6.6.1 VPN 网关删除后公网地址是否可以保留？ 130
6.6.2 EIP 能作为 VPN 的网关 IP 吗？ 130
6.6.3 通过 VPN 互访的主机需要购买 EIP 吗？ 130
6.6.4 为什么我开通 VPN 后，云端 ECS 会有公网 IP 的访问信息？ 131
6.6.5 用户侧数据中心的网关设备没有固定的公网 IP 可以吗？ 131
6.7 路由设置 131
6.7.1 如何理解 VPN 连接中的对端网关和对端子网？ 131
6.7.2 Console 界面在哪添加 VPN 远端路由？ 131
6.7.3 ECS 主机多网卡是否需要添加去往线下网络的路由？ 131
6.7.4 什么是 NQA 131
6.8 VPN 子网设置 132
6.8.1 配置 VPN 连接的本端子网和对端子网时需要注意什么？ 132
6.8.2 VPN 本端子网和对端子网的数量有限制吗？ 132
6.8.3 创建 VPN 连接时添加对端子网，提示系统异常，如何处理？ 132
6.8.4 VPN 网关删除后公网地址是否可以保留？ 133
6.8.5 VPN 接入 VPC 的网络地址如何规划？ 133
6.8.6 创建 VPN 网关时 IP 是如何分配的？ 133
6.9 VPN 感兴趣流 133
6.9.1 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置？ 133
6.9.2 如何配置和修改云上 VPN 的感兴趣流？ 133
6.10 VPN 连接保活 134
6.10.1 如何防止 VPN 连接出现中断情况？ 134
6.11 监控 134
6.11.1 VPN 监控可以监控哪些内容？ 134
6.11.2 VPN 连接中断后会通知我吗？ 135
6.11.3 VPN 监控能不能查看每条连接的流量？ 135
6.11.4 当 VPN 监控结果异常时，可以发送提醒信息吗？ 135
6.12 带宽与网速 135
6.12.1 如何测试 VPN 速率情况？ 135
6.12.2 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？ 137
6.12.3 VPN 网关带宽到达限额时有什么影响？ 137
6.12.4 修改了 VPN 带宽大小，为什么测试没有生效？ 137
6.12.5 如何选择购买 VPN 带宽的大小？ 138
6.13 配额 138
6.13.1 虚拟专用网络的配额是什么？ 138
6.13.2 创建 VPN 网关和连接的缺省配额是多少？ 138
6.14 账号权限 139

6.14.1 建立 IPsec VPN 连接需要账户名和密码吗？ 139
6.14.2 创建 VPN 时系统提示权限不足，如何处理？ 139
6.14.3 如何确定我的账号是因为权限不足而无法创建 VPN 的？ 139
6.15 经典版 VPN 139
6.15.1 产品咨询 139
6.15.1.1 IPsec VPN 适用连接典型组网结构有哪些？ 139
6.15.1.2 什么是 VPC、VPN 网关、VPN 连接？ 140
6.15.1.3 VPC、VPN 网关、VPN 连接之间有什么关系？ 140
6.15.1.4 如何理解 VPN 连接中的远端网关和远端子网？ 140
6.15.1.5 VPN 接入 VPC 的网络地址如何规划？ 140
6.15.1.6 IPsec VPN 是否会自动进行协商？ 141
6.15.1.7 VPN 协商参数有哪些？默认值是什么？ 141
6.15.1.8 哪些设备可以与云进行 VPN 对接？ 143
6.15.1.9 建立 IPsec VPN 连接需要账户名和密码吗？ 143
6.15.1.10 如何在已创建的 VPN 连接中，限定特定的主机访问云上子网？ 144
6.15.1.11 VPN 监控可以监控哪些内容？ 144
6.15.1.12 EIP 能作为 VPN 的网关 IP 吗？ 144
6.15.1.13 通过 VPN 互访的主机需要购买 EIP 吗？ 144
6.15.1.14 如何选择购买 VPN 带宽的大小？ 144
6.15.1.15 创建 VPN 连接时如何选择 IKE 的版本？ 145
6.15.1.16 VPN 使用的 DH group 对应的比特位是多少？ 146
6.15.1.17 是否可以通过 VPN 实现跨境访问网站？ 147
6.15.1.18 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联？ 147
6.15.1.19 IPsec VPN 和 SSL VPN 在使用场景和连接方式上有什么区别？ 147
6.15.1.20 通过 VPN 互访的主机需要购买 EIP 吗？ 148
6.15.1.21 Console 界面在哪添加 VPN 远端路由？ 148
6.15.1.22 VPN 连接中断后会通知我吗？ 148
6.15.1.23 如何解决 VPN 无法建立连接问题？ 148
6.15.1.24 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？ 149
6.15.2 组网与使用场景 149
6.15.2.1 连接云下的多台服务器需要购买几个连接？ 149
6.15.2.2 多人访问 ECS，是否可以给每个客户机安装一套 IPsec 软件和云端建立 VPN 连接？ 149
6.15.2.3 VPN 支持将两个 VPC 互连吗？ 149
6.15.2.4 使用 VPN 会对本地网络造成哪些影响，访问云端主机在路由上会有哪些变化？ 150
6.15.2.5 通过 VPN 来实现云下 IDC 与云端 VPC 的互通，两端分别需要做哪些配置？ 150
6.15.2.6 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置？ 150
6.15.2.7 同一个 Region 的两个 VPC 可以通过 VPN 连通吗？ 150
6.15.2.8 使用 VPN 替换专线该如何配置？ 150
6.15.2.9 云端创建了两个 VPC，如何与云下的 IDC 网络互通？ 151

6.15.2.10 组网拓扑如（IDC1-VPC1-VPC2-IDC2），如何实现四个子网互联？ 151
6.15.2.11 云端两个 Region，每 Region 有两个子网，是否可以创建两个 VPN 连接，分别连通不同子网？ 152
6.15.2.12 VPN 和 OBS 可以直接通信吗？ 152
6.15.2.13 用户本地电脑如何连接云上 VPN？ 152
6.15.2.14 公司网络已通过 VPN 连通了云，我如何在家访问 ECS？ 152
6.15.2.15 购买 VPN 网关和连接后，发现云下没有支持 IPsec 的设备，如何临时建立 VPN 连接？ 152
6.15.2.16 如何选择在云上的哪个区域创建 VPN 网关？ 152
6.15.3 Console 与页面使用 153
6.15.3.1 VPN 配置下发后，多久能够生效？ 153
6.15.3.2 VPN 配置完成了，为什么连接一直处于未连接状态？ 153
6.15.3.3 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置？ 153
6.15.3.4 Console 界面在哪添加 VPN 远端路由？ 153
6.15.3.5 创建 VPN 连接时如何关闭 PFS 的 Group 配置？ 153
6.15.3.6 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接？ 154
6.15.3.7 修改协商策略后，页面显示资源不存在，如何处理？ 154
6.15.3.8 如何重置已经建立的 VPN 连接？ 154
6.15.4 VPN 协商与对接 154
6.15.4.1 使用 VPN 连通云端 VPC 网络，云下设备如何配置？ 154
6.15.4.2 VPN 支持远端网关域名对接吗？ 155
6.15.4.3 我创建的 VPN 连接有几个隧道？ 155
6.15.4.4 如何通过安全组控制使 VPN 不能访问 VPC 上的部分虚拟机，实现安全隔离？ 155
6.15.4.5 修改 VPN 连接的配置会造成连接重建吗？ 155
6.15.4.6 云对接 AWS 后，为何不可以从 AWS 向云发起协商？ 155
6.15.4.7 对接云时，如何配置 DPD 信息？ 155
6.15.4.8 本地防火墙无法收到 VPN 网关的 IKE 第一阶段的回复包怎么解决？ 156
6.15.4.9 本地防火墙无法收到 VPN 子网的回复包怎么解决？ 156
6.15.5 连接故障或无法 PING 通 156
6.15.5.1 如何防止 VPN 连接出现中断情况？ 156
6.15.5.2 使用中 IPsec VPN 连接中断后如何快速恢复？ 158
6.15.5.3 VPN 网关带宽到达限额时有什么影响？ 158
6.15.5.4 两个 Region 创建的 VPN 连接状态正常，为什么不能 ping 通对端 ECS？ 158
6.15.5.5 IDC 与云端对接，VPN 连接正常，子网间业务无法互相访问？ 158
6.15.5.6 正在使用 VPN 出现了连接中断，提示数据流不匹配，如何排查？ 159
6.15.5.7 正在使用 VPN 出现了连接中断，提示 DPD 超时，如何排查？ 159
6.15.5.8 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接？ 159
6.15.5.9 VPN 建立后您的数据中心或局域网无法访问弹性云主机？ 159
6.15.5.10 为什么 VPN 创建成功后状态显示未连接？ 159
6.15.5.11 VPN 是否启动了 DPD 检测机制？ 159
6.15.6 公网地址 160

6.15.6.1 VPN 网关删除后公网地址是否可以保留？ 160
6.15.6.2 EIP 能作为 VPN 的网关 IP 吗？ 160
6.15.6.3 通过 VPN 互访的主机需要购买 EIP 吗？ 160
6.15.6.4 为什么我开通 VPN 后，云端 ECS 会有公网 IP 的访问信息？ 160
6.15.6.5 用户侧数据中心的网关设备没有固定的公网 IP 可以吗？ 161
6.15.7 路由设置 161
6.15.7.1 如何理解 VPN 连接中的远端网关和远端子网？ 161
6.15.7.2 Console 界面在哪添加 VPN 远端路由？ 161
6.15.7.3 ECS 主机多网卡是否需要添加去往线下网络的路由？ 161
6.15.8 VPN 子网设置 161
6.15.8.1 配置 VPN 连接的本端子网和远端子网时需要注意什么？ 161
6.15.8.2 VPN 本端子网和远端子网的数量有限制吗，为什么我选择网段更新本地子网提示报错？ 162
6.15.8.3 创建 VPN 连接时添加远端子网，提示系统异常，如何处理？ 162
6.15.8.4 VPN 接入 VPC 的网络地址如何规划？ 162
6.15.8.5 创建 VPN 网关时 IP 是如何分配的？ 162
6.15.9 VPN 感兴趣流 162
6.15.9.1 本地设备配置 VPN 时需要设置 ACL，为何在 Console 上找不到对应的配置？ 162
6.15.9.2 如何配置和修改云上 VPN 的感兴趣流？ 162
6.15.10 VPN 连接保活 163
6.15.10.1 如何防止 VPN 连接出现中断情况？ 163
6.15.11 监控类 164
6.15.11.1 VPN 监控可以监控哪些内容？ 164
6.15.11.2 VPN 连接中断后会通知我吗？ 164
6.15.11.3 VPN 监控能不能查看每条连接的流量？ 164
6.15.12 带宽与网速 164
6.15.12.1 如何测试 VPN 速率情况？ 164
6.15.12.2 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？ 166
6.15.12.3 如何修改 VPN 的带宽大小？ 166
6.15.12.4 VPN 网关带宽到达限额时有什么影响？ 166
6.15.12.5 修改了 VPN 带宽大小，为什么测试没有生效？ 167
6.15.12.6 VPN 能否共用 EIP 的带宽？ 167
6.15.12.7 VPN 产品中的带宽和云专线的带宽有什么区别？ 167
6.15.12.8 如何选择购买 VPN 带宽的大小？ 167
6.15.13 配额类 167
6.15.13.1 虚拟专用网络的配额是什么？ 167
6.15.13.2 创建 VPN 网关和连接的缺省配额是多少？ 168
6.15.13.3 一个用户下支持多少个 IPsec VPN？ 168
6.15.14 账号权限 168
6.15.14.1 建立 IPsec VPN 连接需要账户名和密码吗？ 168

6.15.14.2 创建 VPN 时系统提示权限不足，如何处理？ 168
6.15.14.3 如何确定我的账号是因为权限不足而无法创建 VPN 的？ 168

1 产品介绍

1.1 什么是 VPN 连接

产品概述

VPN 连接（Virtual Private Network Connection，以下简称 VPN），用于在企业用户本地网络、数据中心与云上网络之间搭建安全、可靠、高性价比的加密连接通道。

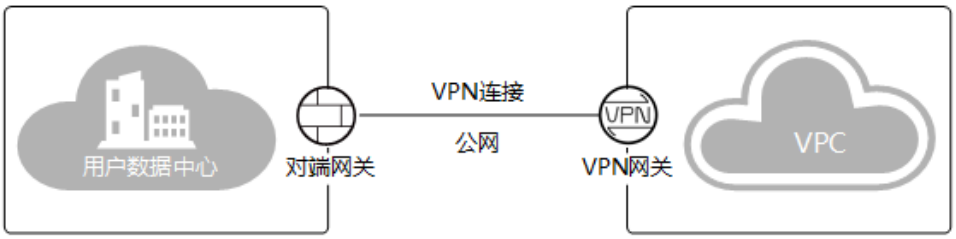
说明

VPN 仅支持建立非跨境连接，不支持建立跨境连接。

- VPN 网关提供了 VPC 的公网出口，与用户数据中心的对端网关对应。
- VPN 连接通过加密技术，将 VPN 网关与对端网关相关联，使数据中心与 VPC 通信，更快速、更安全地构建混合云环境。

VPN 组网图如图 1-1 所示。

图1-1 VPN 组网图



组成部分

- **VPN 网关**：虚拟专用网络在云上的虚拟网关，与用户本地网络、数据中心的对端网关建立安全私有连接。
- **对端网关**：用户数据中心的 VPN 设备或软件应用程序。控制台上创建的对端网关是云上虚拟对象，用于记录用户数据中心实体设备的配置信息。
- **VPN 连接**：VPN 网关和对端网关之间的安全通道，使用 IKE 和 IPsec 协议对传输数据进行加密。

1.2 产品优势

VPN 连接具有以下几大产品优势：

- **更安全**
  - 基于 IKE、IPsec 对传输数据加密，保证用户数据传输安全。
  - 支持国密型网关，遵循《GB／T 36968-2018 信息安全技术 IPSec VPN 技术规范》。
  - 企业版 VPN 支持为每个用户创建独立的 VPN 网关，提供租户网关隔离防护能力。
- **高可用**
  - 双连接：网关提供两个接入地址，支持一个对端网关创建两条相互独立的 VPN 连接，一条连接中断后流量可快速切换到另一条连接。
  - 主备模式：正常情况下，VPN 网关和对端网关通过主连接进行通信；当主连接发生故障时，VPN 连接会自动切换到备连接；故障恢复后，VPN 连接会自动切回到主连接。
  - 双活网关：企业版 VPN 网关可双活部署在不同的 AZ 区域，实现 AZ 级高可用保障。
- **低成本**
  - 利用 Internet 构建 IPsec 加密通道，使用费用相对云专线服务更便宜。
  - 企业版 VPN 支持绑定同一共享带宽下的 EIP 实例，从而节省带宽使用成本。
  - 支持在创建 EIP 实例时，按需配置带宽大小。
- **灵活易用**
  - 即开即用：部署快速，实时生效，在用户数据中心的 VPN 设备进行简单配置即可完成对接
  - 支持分支互访：支持云上 VPN 网关作为 VPN Hub，云下站点通过 VPN Hub 实现分支互访。
  - 支持多种连接模式：企业版 VPN 网关支持配置策略、静态路由和 BGP 路由多种连接模式，满足不同对端网关的接入需要。
  - 支持私网类型网关：企业版 VPN 支持对专线私有网络进行加密传输，提升数据传输安全。

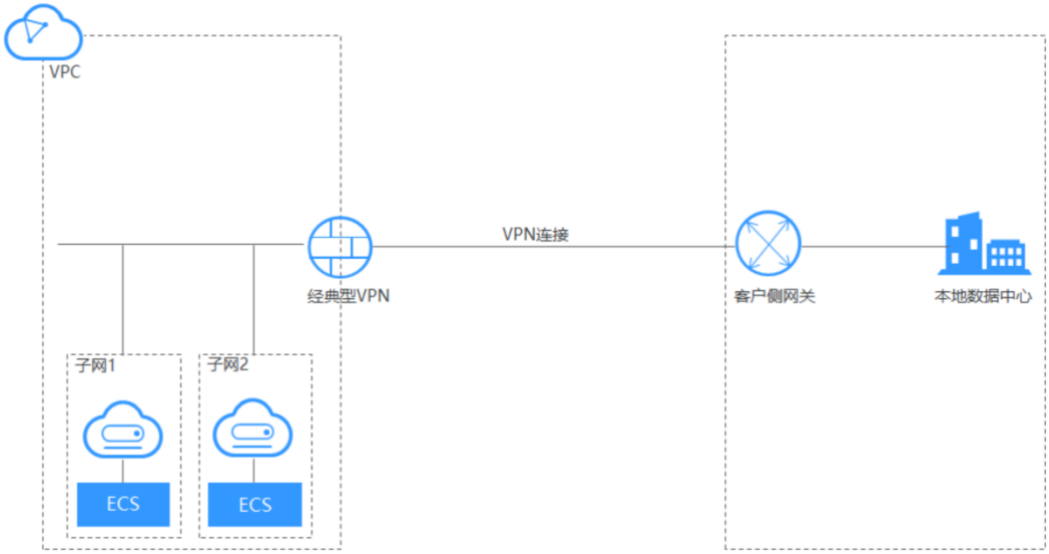
1.3 产品功能

VPN 连接（Virtual Private Network Connections，以下简称 VPN），用于在远端用户和虚拟私有云（Virtual Private Cloud，以下简称 VPC）之间建立一条安全加密的公网通信隧道。当您作为远端用户需要访问 VPC 的业务资源时，您可以通过 VPN 连通 VPC。

默认情况下，在虚拟私有云（VPC）中的弹性云主机无法与您自己的数据中心或私有网络进行通信。如果您需要将 VPC 中的弹性云主机和您的数据中心或私有网络连通，可以启用 VPN 功能。

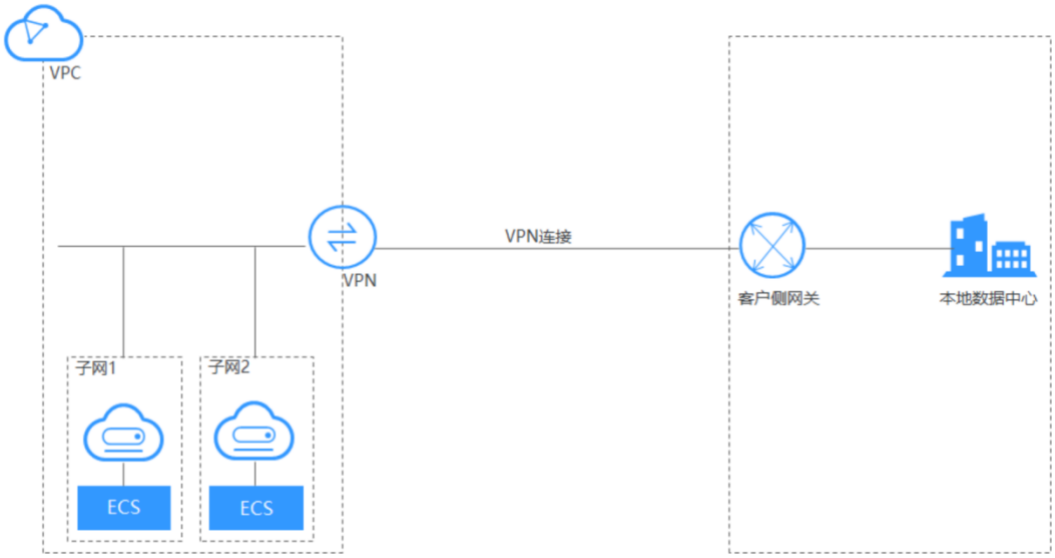
经典版 VPN

经典版 VPN 采用硬件防火墙作为网关，所有租户共享 IPSec 隧道资源；一个租户业务触发故障将会影响其他租户业务。



企业版 VPN

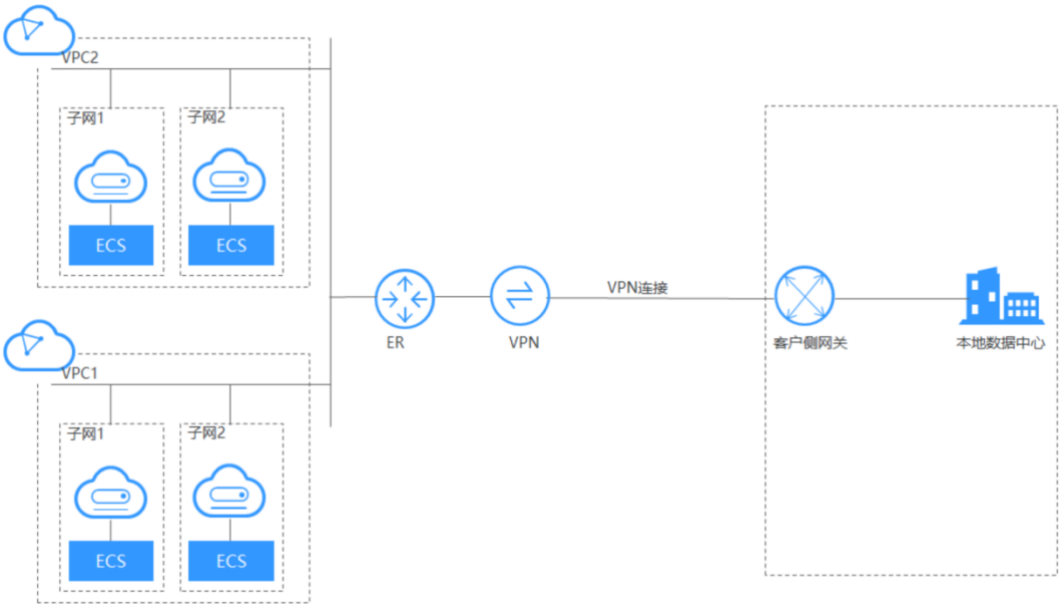
企业版 VPN 采用虚拟网关软件作为网关，VPN 网关由租户独占，不与其他租户共享，带宽、连接数可保障；一个租户网关故障时，不会影响其他租户网关。



VPN 关联 ER

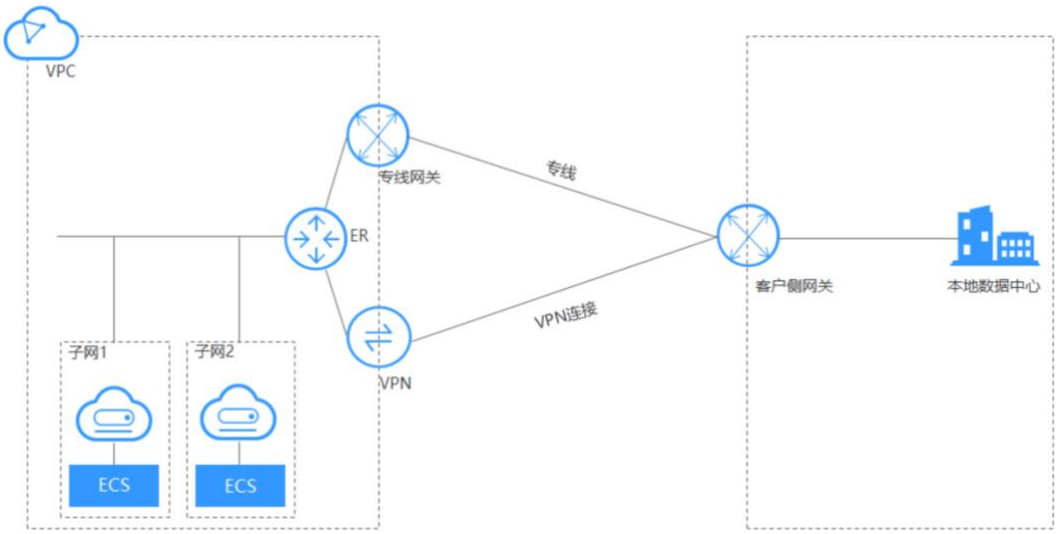
传统方式下，本地数据中心同时对接不同 VPC 时，VPN 侧需要配置多条 VPN 连接，分别对应到不同 VPC。

使用 VPN 关联 ER（Enterprise Router，企业路由器）功能后，VPN 只需要对接到 ER，VPC 之间的网络路由通信均由 ER 实现，从而简化网络配置。



VPN 和云专线互备

VPN 和云专线支持本地数据中心与云上 VPC 同时建立专线连接和 VPN 连接，在专线链路故障时通过 VPN 连接提供保护。

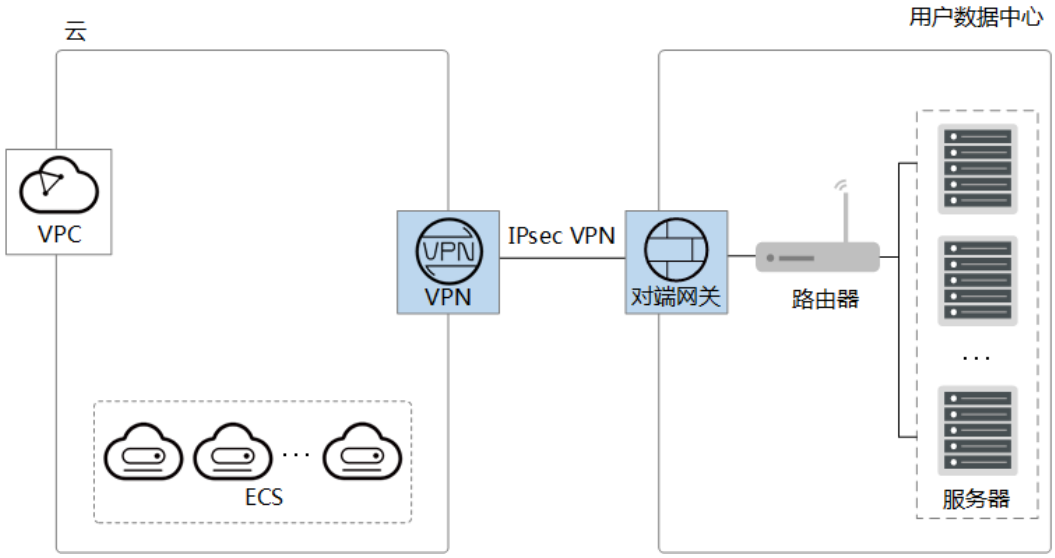


1.4 应用场景

1.4.1 场景 1：混合云部署

通过 VPN 将用户数据中心和云上 VPC 互联，利用云上弹性和快速伸缩能力，扩展应用计算能力，如图 1-2 所示。

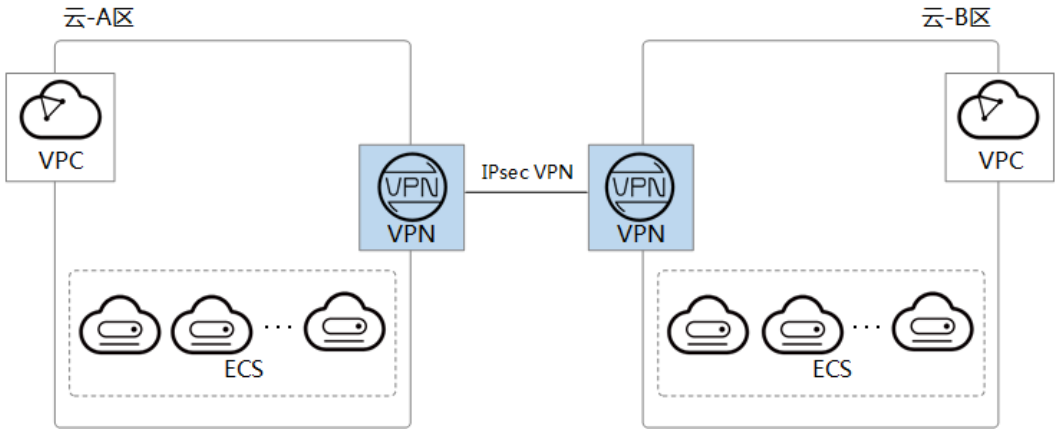
图1-2 混合云部署



1.4.2 场景 2：跨地域 VPC 互联

通过 VPN 将云上的不同 region 的 VPC 连接，使得用户的数据和服务在不同地域能够互联互通，如图 1-3 所示。

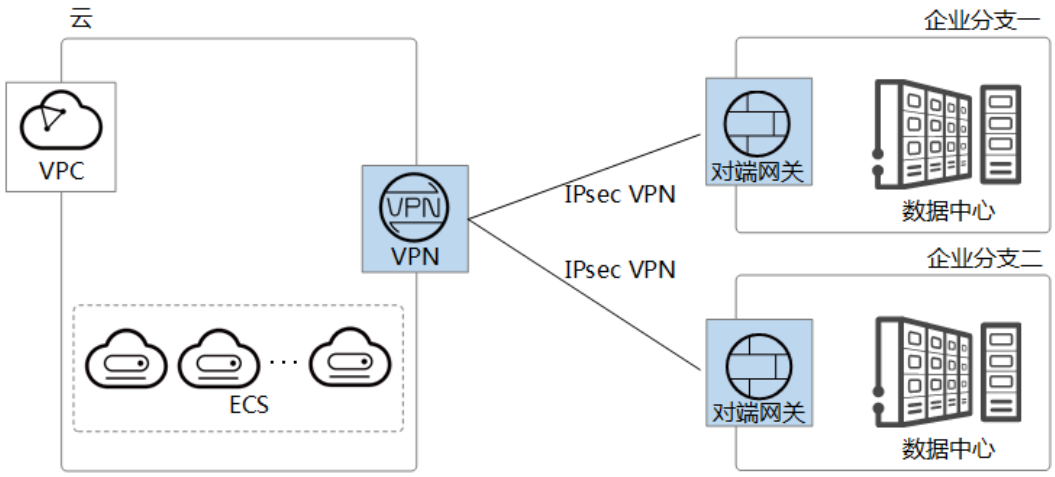
图1-3 跨地域 VPC 互联



1.4.3 场景 3：多企业分支互联

通过 VPN Hub 实现企业分支间互访，避免两两分支之间配置 VPN 连接，如图 1-4 所示。

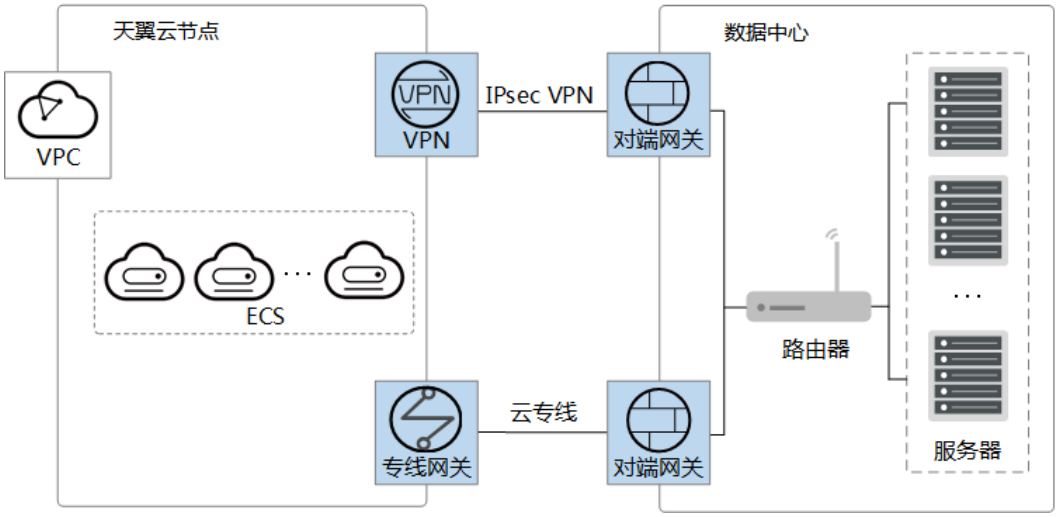
图1-4 多企业分支互联



1.4.4 场景 4：VPN 和专线互备

用户数据中心与云上 VPC 通过专线连接，同时建立 VPN 连接实现备份，提高网络可靠性。

图1-5 VPN 和专线互备



1.5 产品规格

说明

- 基础型和专业型 1 网关规格，支持相互变更。
- 专业型 1、专业型 2 网关规格，支持相互变更。
- 专业型 1-非固定 IP VPN 网关规格不支持变更为专业型 1；
- 专业型 2-非固定 IP VPN 网关规格不支持变更为专业型 2。

以上产品规格升降配，实际情况以 console 显示为准。

表1-1 企业版 VPN 不同规格的区别

对比项	基础型	专业型 1	专业型 1-非固定 IP	专业型 2	专业型 2-非固定 IP	国密型
独享网关资源	支持	支持	支持	支持	支持	支持
双连接	支持	支持	支持	支持	支持	支持
双活网关	支持	支持	支持	支持	支持	支持
主备网关	支持	支持	支持	支持	支持	支持
策略模式	支持	支持	支持	支持	支持	支持
路由模式-静态路由	支持	支持	支持	支持	支持	支持
路由模式-BGP 路由	支持	支持	支持	支持	支持	支持
策略模板模式	不支持	不支持	支持	不支持	支持	不支持
最大转发带宽	100Mbps	300Mbps	300Mbps	1Gbps	1Gbps	500Mbps
最大 VPN 连接组数	10 个	100 个	100 个	100 个	100 个	100 个
对接企业路由器	不支持	支持	支持	支持	支持	支持
接入私网地址	不支持	支持	不支持	支持	不支持	支持
非固定 IP 接入	不支持	不支持	支持	不支持	支持	不支持

对比项	基础型	专业型 1	专业型 1-非固定 IP	专业型 2	专业型 2-非固定 IP	国密型
支持区域	以控制台实际上线区域为准。	以控制台实际上线区域为准。	以控制台实际上线区域为准。	以控制台实际上线区域为准。	以控制台实际上线区域为准。	以控制台实际上线区域为准。

1.6 企业版 VPN 与经典版 VPN 的区别

表1-2 企业版 VPN 和经典版 VPN 的区别

类别	对比项	企业版 VPN	经典版 VPN
租户隔离	租户独享网关	支持	不支持
功能&特性	策略模式	支持	支持
	路由模式	静态路由/BGP 路由	不支持
	VPN Hub	支持	不支持
	企业路由器	支持	不支持
	网络类型	公网/私网	公网
容量&性能	子网数量	• 路由模式：50 • 策略模式：5	策略模式：5
	更多信息，请参见表 1-1。		
可靠性	网关保护方式	主备/双活	-
	网关跨 AZ 部署	支持	不支持
	双线路双活	支持	不支持
	与专线互备	支持	不支持

1.7 约束与限制

VPN 网关限制

表1-3 VPN 网关限制

VPN 网关类型	资源	默认限制
企业版 VPN	每租户在每区域支持创建的 VPN 网关数量	50 • 如果您只有一个 VPC，则该 VPC 最大创建 50 个 VPN 网关。 • 如果您有多个 VPC，则多个 VPC 创建的 VPN 网关数量最大为 50 个。
	每 VPN 网关支持配置的 VPN 连接组数量	100 如果 VPN 网关支持非固定 IP 接入，则该 VPN 网关支持配置的非固定 IP 接入、固定 IP 接入的 VPN 连接组数量合计最多为 100 个。
	每 VPN 网关支持配置的本地子网数量	50
	每 VPN 网关支持通过每连接接收对端网关发布的 BGP 路由数量	100
经典版 VPN	每租户在每区域支持创建的 VPN 网关数量	2 每个 VPC 最多创建 1 个 VPN 网关。

- VPN 网关 TCP 协议的最大报文长度默认设置为 1300 字节。

对端网关限制

表1-4 对端网关限制

VPN 网关类型	资源	默认限制
企业版 VPN	每租户在每区域支持创建的对端网关数量	100

- 对端网关必须开启 NAT 穿越。
- 对端网关必须使能 DPD（Dead Peer Detection，失效对等体检测）。

- 对端网关必须支持 IPsec Tunnel 接口，并使能对应的安全策略。
- 静态路由模式连接开启 NQA（Network Quality Analysis，网络质量分析）时，对端网关的 IPsec Tunnel 接口必须配置 IP 地址，并响应 ICMP 请求。
- 对端网关 TCP 协议的最大报文段长度建议设置为小于 1399，避免因增加 IPsec 认证头开销导致分片的问题。

VPN 连接限制

表1-5 VPN 连接限制

VPN 网关类型	资源	默认限制	如何提升配额
企业版 VPN	每 VPN 连接支持配置的策略规则数量	5	不支持修改。
	每 VPN 连接支持配置的对端子网数量	50	
经典版 VPN	每租户在每区域支持创建的 VPN 连接数量	12	不支持修改。

- 多子网场景下，VPN 连接建议使用路由模式。策略模式/策略模板模式下，VPN 网关默认为每对本地子网和对端子网创建一个通信隧道，当一条策略模式连接的本地或对端为多子网场景下实际占用了多个通信隧道。

  VPN 网关每个网关 IP 和对端网关建连时，最大提供 100 个通信隧道。

  - 路由模式下，每个 VPN 连接占用网关 IP 的 1 个通信隧道。
  - 策略模式/策略模板模式下，每个 VPN 连接占用网关 IP 的 M*N 个通信隧道。M 为本端待通信子网数，N 为对端待通信子网数。

  当所有涉及该网关 IP 的 VPN 连接模式占用的通信隧道超过 100 个时，会导致超出部分对应的 VPN 连接创建失败。
- 使用策略模式创建 VPN 连接时，若添加多条策略规则，不同策略规则的源、目的网段需要避免出现重叠，以免造成数据流误匹配或 IPsec 隧道震荡。

1.8 权限管理

如果您需要对云服务平台上创建的 VPN 资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称 IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制资源的访问。

通过 IAM，您可以在账号中给员工创建 IAM 用户，并授权控制员工对云服务资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有 VPN 的使用权限，但是不希望他们拥有删除 VPN 等高危操作的权限，那么您可以使用 IAM 为开发人员

创建用户，通过授予仅能使用 VPN，但是不允许删除 VPN 的权限，控制他们对 VPN 资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的 IAM 用户进行权限管理，您可以跳过本章节，不影响您使用 VPN 服务的其它功能。

IAM 是云服务平台提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

关于 IAM 的详细介绍，请参见《统一身份认证服务用户指南》。

VPN 权限

默认情况下，管理员创建的 IAM 用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

VPN 部署时通过物理区域划分，为项目级服务。授权时，“授权范围”需要选择“指定区域项目资源”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果“授权范围”选择“所有资源”，则该权限在所有区域项目中都生效。访问 VPN 时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM 最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云服务平台各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM 最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对 VPN 服务，管理员能够控制 IAM 用户仅能对某一类 VPN 资源进行指定的管理操作。

如表 1-6 所示，包括了 VPN 的所有系统权限。

表1-6 VPN 系统权限

系统角色/策略名称	描述	依赖关系
VPN Administrator	VPN 服务的管理员权限，拥有该权限的用户拥有 VPN 服务所有执行权限。 拥有该权限的用户默认拥有 Tenant Guest、VPC Administrator 权限。 • VPC Administrator：项目级策略，在同项目中勾选。 • Tenant Guest：项目级策略，在同项目中勾选。	-
VPN FullAccess（推荐使用）	VPN 服务的所有执行权限。	-

系统角色/策略名称	描述	依赖关系
VPN ReadOnlyAccess	VPN 服务只读权限，拥有该权限的用户仅能查看 VPN 服务下的资源信息。	-

表 1-7 列出了 VPN 常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表1-7 常用操作与系统权限的关系

操作	VPN Administrator	VPN FullAccess	VPN ReadOnlyAccess
创建 VPN 网关	√	• 企业版 VPN：√ • 经典版 VPN：×	×
查询 VPN 网关	√	√	√
修改 VPN 网关	√	• 企业版 VPN：√ • 经典版 VPN：×	×
删除 VPN 网关	√	• 企业版 VPN：√ • 经典版 VPN：×	×
创建 VPN 连接	√	• 企业版 VPN：× • 经典版 VPN：√	×
查询 VPN 连接	√	√	√
修改 VPN 连接	√	• 企业版 VPN：× • 经典版 VPN：√	×
删除 VPN 连接	√	• 企业版 VPN：× • 经典版 VPN：√	×
创建对端网关	√	• 企业版 VPN：√ • 经典版 VPN：不涉及	×
查询对端网关	√	• 企业版 VPN：√ • 经典版 VPN：不涉及	√
修改对端网关	√	• 企业版 VPN：√ • 经典版 VPN：不涉及	×

操作	VPN Administrator	VPN FullAccess	VPN ReadOnlyAccess
删除对端网关	√	• 企业版 VPN：√ • 经典版 VPN：不涉及	×

1.9 与其他服务的关系

VPN 连接服务与其他云服务的关系如下表所示。

表1-8 VPN 连接与其他服务的关系

服务名称	交互功能
虚拟私有云（Virtual Private Cloud，VPC）	通过 VPC 服务，创建 VPC，用户数据中心才可以通过 VPN 上云。
弹性云主机（Elastic Cloud Server，ECS）	通过 ECS 服务，定义安全组中的规则，将 VPC 中的弹性云主机划分成不同的安全域，以提升弹性云主机访问的安全性。
企业路由器（Enterprise Router，ER）	通过企业路由器 ER，用户数据中心上云可以实现 VPN 和专线双通道互备。 仅企业版 VPN 网关支持，经典版 VPN 网关不支持。
NAT 网关（NAT Gateway）	通过 NAT 网关服务，可以实现用户数据中心服务器访问公网或为公网提供服务。
弹性公网 IP（EIP）	通过弹性公网 IP，可以实现 VPN 网关通过公网和对端网关进行网络互通。 仅企业版 VPN 支持，经典版 VPN 不支持。
云监控（Cloud Eye）	通过云监控服务，查看 VPN 资源的监控数据，还可以获取可视化监控图表。
统一身份认证服务（Identity and Access Management，IAM）	通过 IAM 服务，针对您在云上创建的 VPN 资源，向不同用户设置不同的使用权限，可以帮助您安全地控制 VPN 资源的访问权限。
标签管理服务（Tag Management Service，TMS）	使用标签来标识虚拟专用网络，便于分类和搜索。
云审计服务（Cloud Trace Service，CTS）	记录与 VPN 服务相关的操作事件。

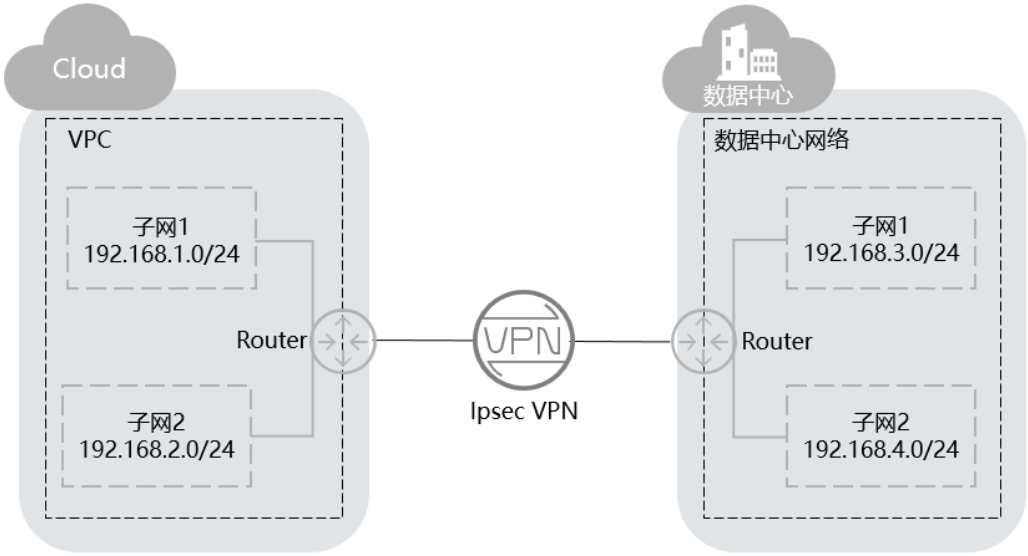
1.10 基本概念

1.10.1 IPsec VPN

IPsec VPN 是一种加密的隧道技术，通过使用加密的安全服务在不同的网络之间建立保密而安全的通讯隧道。

如图 1-6 所示，假设您在云上已经申请了 VPC，并申请了 2 个子网（192.168.1.0/24，192.168.2.0/24），同时您在自己的数据中心也有 2 个子网（192.168.3.0/24，192.168.4.0/24），那么您可以通过 VPN 使 VPC 内的子网与数据中心的子网互相通信。

图1-6 IPsec VPN



支持站点到站点 VPN（Site-to-Site VPN），可实现 VPC 子网和数据中心局域网互访。

1.10.2 VPN 网关

VPN 网关是虚拟专用网络在云上的虚拟网关，与用户本地网络、数据中心的对端网关建立安全私有连接。

VPN 网关需要与用户数据中心的对端网关配合使用。

1.10.3 VPN 连接

VPN 连接是 VPN 网关和对端网关之间的安全通道，使用 IKE 和 IPsec 协议对传输数据进行加密。

VPN 连接使用 IKE 和 IPsec 协议对传输数据进行加密，保证数据安全可靠。

1.10.4 VPN 网关带宽

VPN 网关带宽指的是出云方向的带宽，即从 VPC 发往用户侧数据中心的带宽。

1.10.5 本端子网

本端子网通过 VPN 与用户侧网络进行互通，有两种输入方式。

- 子网方式 ：使用下拉列表选择要进行 VPN 通信的子网。如果要进行 VPN 通信的子网都在该 VPC 中，建议采用这种方式。
- 网段方式 ：用户在输入框中手工输入网段信息，格式为点分十进制加掩码长度，如 192.168.0.0/16； 如果有多个网段，则使用逗号分隔。使用这种方式可以添加不属于该 VPC 的网段，如通过 VPC peering 特性连接进来的非该 VPN 网关关联的 VPC 内的网段（如 0.0.0.0/0 等）。

1.10.6 对端网关

对端网关是用户数据中心的 VPN 设备或软件应用程序。控制台上创建的对端网关是云上虚拟对象，用于记录用户数据中心实体设备的配置信息。

1.10.7 对端子网

对端子网即用户侧数据中心的网段，该网段需要通过 VPN 与云上 VPC 网络进行互通。用户需手工输入网段信息，格式为点分十进制加掩码长度，如 192.168.0.0/16；如果有多个网段，则使用逗号分隔。

用户在设置完对端子网后，无需在 VPC 中增加路由信息，VPN 服务会自动在 VPC 中下发到达对端子网的路由。

说明

子网不支持 D 类组播地址，E 类保留地址和 127 开头的环回地址。

1.10.8 预共享密钥

预共享密钥（Pre Shared Key），指配置在云上 VPN 连接的密钥，用于双方 VPN 设备的 IKE 协商，需要确保双方配置一致，否则会导致 IKE 协商失败。

1.11 参考标准和协议

与 VPN 相关的参考标准与协议如下：

- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
- RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)

- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4302: IP Authentication Header
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4306: Internet Key Exchange (IKEv2)Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308: Cryptographic Suites for IPsec
- RFC 5282: Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
- RFC 6989: Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7321: Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 8247: Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 4271: A Border Gateway Protocol 4 (BGP-4)

2 快速入门

2.1 通过企业版 VPN 实现数据中心和 VPC 互通

2.1.1 入门指引

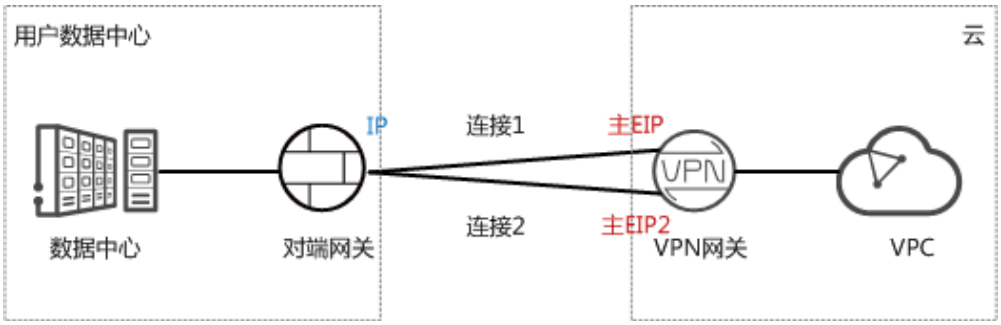
场景描述

由于业务发展，企业 A 需要将数据中心和 VPC 的数据进行互通。此时企业 A 可以通过 VPN 服务创建数据中心和 VPC 的连接，实现云上和云下数据互通。

- 如果用户数据中心仅有一个对端网关，且对端网关只能配置一个 IP 地址，推荐 VPN 网关使用双活模式，组网如图 2-1 所示。

  双活模式下，如果连接 1 链路故障，流量自动切换至连接 2 进行传输，企业业务不受影响；连接 1 恢复正常后，VPN 仍使用连接 2 进行数据交互。

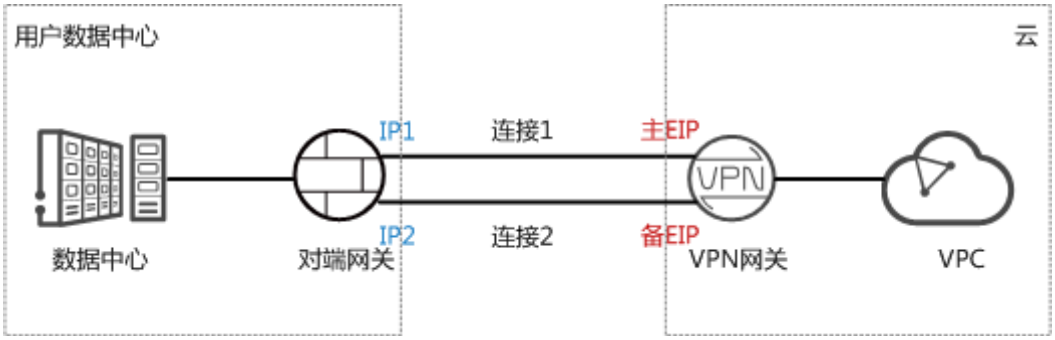
  图2-1 双活模式



- 如果用户数据中心存在两个对端网关，或一个对端网关可以配置两个 IP 地址，推荐 VPN 网关使用主备模式，组网如图 2-2 所示。

  主备模式下，连接 1 和连接 2 互为主备，主链路为连接 1，备链路为连接 2。默认情况下流量仅通过主链路进行传输，如果主链路故障，流量自动切换至备链路进行传输，企业业务不受影响；主链路恢复正常后，VPN 回切至主链路进行数据交互。

图2-2 主备模式



约束与限制

- 对端网关需要支持标准 IKE 和 IPsec 协议。
- 本地数据中心和 VPC 间互通的子网需要没有重叠，且数据中心待互通的子网中不能包含 100.64.0.0/10 和 214.0.0.0/8。

  如果 VPC 使用云专线服务和其他 VPC 互通，则本地数据中心的子网也不能和其他 VPC 包含的子网存在重叠。

数据规划

表2-1 规划数据

类别	规划项	规划值
VPC	待互通子网	192.168.0.0/16
VPN 网关	互联子网	用于 VPN 网关和 VPC 通信，请确保选择的互联子网存在 4 个及以上可分配的 IP 地址。 192.168.2.0/24
	HA 模式	双活
	EIP 地址	EIP 地址在购买 EIP 时由系统自动生成，VPN 网关默认使用 2 个 EIP。本示例假设 EIP 地址生成如下： • 主 EIP：11.xx.xx.11 • 主 EIP2：11.xx.xx.12
VPN 连接	Tunnel 接口地址	用于 VPN 网关和对端网关建立 IPsec 隧道，配置时两边需要互为镜像。 • VPN 连接 1：169.254.70.1/30 • VPN 连接 2：169.254.71.1/30
数据中心	待互通子网	172.16.0.0/16

类别	规划项	规划值
对端网关	网关 IP 地址	网关 IP 地址由运营商统一分配。本示例假设网关 IP 地址如下： 22.xx.xx.22
	Tunnel 接口地址	• VPN 连接 1：169.254.70.2/30 • VPN 连接 2：169.254.71.2/30

操作流程

通过 VPN 实现数据中心和 VPC 互通的操作流程如图 2-3 所示。

图2-3 操作流程

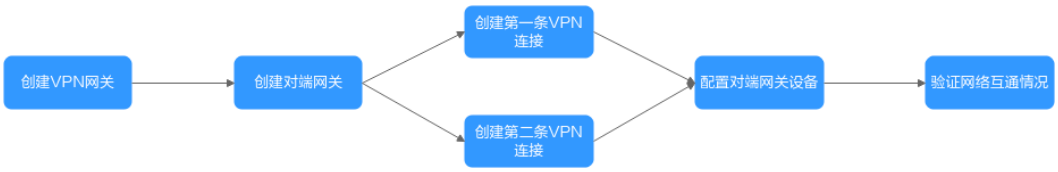


表2-2 操作流程说明

序号	步骤	说明
1	步骤一：创建 VPN 网关	VPN 网关需要绑定两个 EIP 作为出口公网 IP。 如果您已经购买 EIP，则此处可以直接绑定使用。
2	步骤二：创建对端网关	添加数据中心的 VPN 设备为对端网关。
3	步骤三：创建第一条 VPN 连接	VPN 网关的主 EIP 和对端网关组建第一条 VPN 连接。
4	步骤四：创建第二条 VPN 连接	VPN 网关的主 EIP2 和对端网关组建第二条 VPN 连接。 第二条 VPN 连接的路由模式、预共享密钥、IKE/IPsec 策略建议和第一条 VPN 连接配置保持一致。
5	步骤五：配置对端网关设备	• 对端网关配置的本端隧道接口地址/对端隧道接口地址需要和 VPN 连接配置互为镜像配置。 • 对端网关配置的路由模式、预共享密钥、IKE/IPsec 策略需要和 VPN 连接配置保持一致。
6	步骤六：验证网络互通情况	登录 ECS，执行 **ping** 命令，验证网络互通情况。

2.1.2 步骤一：创建 VPN 网关

前提条件

- 虚拟私有云 VPC 已经创建完成。如何创建虚拟私有云 VPC，请参见《虚拟私有云用户指南》。
- 虚拟私有云 VPC 中 ECS 的安全组规则已经配置，并确保安全组规则允许数据中心的对端网关可以访问 VPC 资源。如何配置安全组规则，请参见《虚拟私有云用户指南》。

操作步骤

步骤 1 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。

步骤 2 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。

步骤 3 在“VPN 网关”界面，单击“创建 VPN 网关”。

步骤 4 根据界面提示配置参数，然后单击“立即购买”并完成支付。

本示例仅对关键参数进行说明。

表2-3 VPN 网关关键参数说明

参数	说明	参数取值
计费模式	支持“按需计费”计费模式。	按需
区域	选择靠近您所在地域的区域。	-
名称	输入 VPN 网关的名称。	vpngw-001
网络类型	• 公网：VPN 网关通过公网建立 VPN 连接。 • 私网：VPN 网关通过私网建立 VPN 连接。	公网
协议类型	支持“IPv4”和“IPv6”两种类型。	IPv4
关联模式	支持“虚拟私有云”和“企业路由器”两种方式。	虚拟私有云
本端子网	配置 VPC 待和数据中心互通的子网。 支持“输入网段”和“选择子网”两种方式。	192.168.0.0/24
规格	选择“专业型 1”。	专业型 1
HA 模式	选择“双活”。	双活
主 EIP	支持“现在创建”和“使用已有”两种方	11.xx.xx.11

参数	说明	参数取值
主 EIP2	式。	11.xx.xx.12

----结束

结果验证

在“VPN 网关”页面生成新创建的 VPN 网关信息，初始状态为“创建中”；当 VPN 网关状态变为“正常”，表示 VPN 网关创建完成。

2.1.3 步骤二：创建对端网关

操作步骤

步骤 1 在左侧导航栏，单击“虚拟专用网络 > 企业版-对端网关”。

步骤 2 在“对端网关”界面，单击“创建对端网关”。

步骤 3 根据界面提示配置参数，然后单击“确定”。

本示例仅对关键参数进行说明。

表2-4 对端网关参数说明

参数	说明	参数取值
名称	输入对端网关的名称。	cgw-001
标识	输入对端网关的 IP。	IP Address，22.xx.xx.22。

----结束

结果验证

在“对端网关”页面生成新创建的对端网关信息。

2.1.4 步骤三：创建第一条 VPN 连接

操作步骤

步骤 1 在左侧导航栏，单击“虚拟专用网络 > 企业版-VPN 连接”。

步骤 2 在“VPN 连接”页面，单击“创建 VPN 连接”。

步骤 3 根据界面提示配置第一条 VPN 连接参数，然后单击“提交”。

本示例仅对关键参数进行说明。

表2-5 第一条 VPN 连接参数说明

参数	说明	参数取值
名称	输入 VPN 连接的名称。	vpn-001
VPN 网关	选择步骤一：创建 VPN 网关创建的 VPN 网关。	vpngw-001
网关 IP	选择 VPN 网关的**主 EIP**。	11.xx.xx.11
对端网关	选择步骤二：创建对端网关创建的对端网关。	cgw-001
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	输入数据中心待和 VPC 互通的子网。	172.16.0.0/16
接口分配方式	支持“手动分配”和“自动分配”两种方式。	手动分配
本端隧道接口地址	配置在 VPN 网关上的 tunnel 接口地址。 说明 对端网关需要对此处的本端隧道接口地址/对端隧道接口地址做镜像配置。	169.254.70.2/30
对端隧道接口地址	配置在用户侧设备上的 tunnel 接口地址。	169.254.70.1/30
检测机制	用于多链路场景下路由可靠性检测。 说明 功能开启前，请确认对端网关支持 ICMP 功能，且对端接口地址已在对端网关上正确配置，否则会导致 VPN 流量不通。	勾选“使能 NQA”
预共享密钥、确认密钥	VPN 连接协商密钥。 VPN 连接和对端网关配置的预共享密钥需要一致。	Test@123
策略配置	包含 IKE 策略和 IPsec 策略，用于指定 VPN 隧道加密算法。 VPN 连接和对端网关配置的策略信息需要一致。	默认配置

----结束

结果验证

在“VPN 连接”页面生成新创建的 VPN 连接信息，初始状态为“创建中”；由于此时对端网关尚未配置，无法建立有效的连接，所以大约 2 分钟后，VPN 连接状态会变成“未连接”。

2.1.5 步骤四：创建第二条 VPN 连接

操作步骤

步骤 1 在左侧导航栏，单击“虚拟专用网络 > 企业版-VPN 连接”。

步骤 2 在“VPN 连接”页面，单击“创建 VPN 连接”。

和第一条 VPN 连接相比，除了名称、网关 IP、本端隧道接口地址和对端隧道接口地址不同，其他配置建议保持一致。

表2-6 第二条 VPN 连接参数说明

参数	说明	参数取值
名称	输入 VPN 连接的名称。	vpn-002
VPN 网关	选择2.1.2 步骤一：创建 VPN 网关创建的 VPN 网关。	vpngw-001
网关 IP	选择 VPN 网关的**主 EIP2**。	11.xx.xx.12
对端网关	选择2.1.3 步骤二：创建对端网关创建的对端网关。	cgw-001
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	输入数据中心待和 VPC 互通的子网。	172.16.0.0/16
接口分配方式	支持“手动分配”和“自动分配”两种方式。	手动分配
本端隧道接口地址	配置在 VPN 网关上的 tunnel 接口地址。 说明 对端网关需要对此处的本端隧道接口地址/对端隧道接口地址做镜像配置。	169.254.71.2/30
对端隧道接口地址	配置在用户侧设备上的 tunnel 接口地址。	169.254.71.1/30
检测机制	用于多链路场景下路由可靠性检测。 说明 功能开启前，请确认对端网关支持 ICMP 功能，且对端接口地址已在对端网关上正确配置，否则会导致 VPN 流量不通。	勾选“使能 NQA”

参数	说明	参数取值
预共享密钥、确认密钥	VPN 连接协商密钥。 VPN 连接和对端网关配置的预共享密钥需要一致。	Test@123
策略配置	包含 IKE 策略和 IPsec 策略，用于指定 VPN 隧道加密算法。 VPN 连接和对端网关配置的策略信息需要一致。	默认配置

----结束

结果验证

在“VPN 连接”页面生成新创建的 VPN 连接信息，初始状态为“创建中”；由于此时对端网关尚未配置，无法建立有效的连接，所以大约 2 分钟后，VPN 连接状态会变成“未连接”。

2.1.6 步骤五：配置对端网关设备

操作步骤

说明

本示例对端网关以华为 AR 路由器为例。

步骤 1 登录 AR 路由器配置界面。

步骤 2 进入系统视图。

```
<AR651>system-view
```

步骤 3 配置公网接口的 IP 地址。本示例假设 AR 路由器 GigabitEthernet 0/0/8 为公网接口。

```
[AR651]interface GigabitEthernet 0/0/8
[AR651-GigabitEthernet0/0/8]ip address 22.xx.xx.22 255.255.255.0
[AR651-GigabitEthernet0/0/8]quit
```

步骤 4 配置默认路由。

```
[AR651]ip route-static 0.0.0.0 0.0.0.0 22.xx.xx.1
```

其中，*22.xx.xx.1* 为 AR 路由器公网 IP 的网关地址，请根据实际替换。

步骤 5 开启 SHA-2 算法兼容 RFC 标准算法功能。

```
[AR651]IPsec authentication sha2 compatible enable
```

步骤 6 配置 IPsec 安全提议。

```
[AR651]IPsec proposal hwproposal1
[AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256
```

```
[AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128
[AR651-IPsec-proposal-hwproposal1]quit
```

步骤 7 配置 IKE 安全提议。

```
[AR651]ike proposal 2
[AR651-ike-proposal-2]encryption-algorithm aes-128
[AR651-ike-proposal-2]dh group14
[AR651-ike-proposal-2]authentication-algorithm sha2-256
[AR651-ike-proposal-2]authentication-method pre-share
[AR651-ike-proposal-2]integrity-algorithm hmac-sha2-256
[AR651-ike-proposal-2]prf hmac-sha2-256
[AR651-ike-proposal-2]quit
```

步骤 8 配置 IKE 对等体。

```
[AR651]ike peer hwpeer1
[AR651-ike-peer-hwpeer1]undo version 1
[AR651-ike-peer-hwpeer1]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer1]ike-proposal 2
[AR651-ike-peer-hwpeer1]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer1]remote-address 11.xx.xx.11
[AR651-ike-peer-hwpeer1]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer1]rsa signature-padding pss
[AR651-ike-peer-hwpeer1]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer1]quit
[AR651]ike peer hwpeer2
[AR651-ike-peer-hwpeer2]undo version 1
[AR651-ike-peer-hwpeer2]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer2]ike-proposal 2
[AR651-ike-peer-hwpeer2]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer2]remote-address 11.xx.xx.12
[AR651-ike-peer-hwpeer2]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer2]rsa signature-padding pss
[AR651-ike-peer-hwpeer2]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer2]quit
```

相关命令说明如下：

- pre-shared-key cipher：预共享密钥，需要和 VPN 连接配置的预共享密钥保持一致。
- local-address：AR 路由器的公网地址。
- remote-address：VPN 网关的主 EIP/主 EIP2。

步骤 9 配置 IPsec 安全框架。

```
[AR651]IPsec profile hwpro1
[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1
[AR651-IPsec-profile-hwpro1]proposal hwproposal1
[AR651-IPsec-profile-hwpro1]pfs dh-group14
[AR651-IPsec-profile-hwpro1]quit
[AR651]IPsec profile hwpro2
[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2
[AR651-IPsec-profile-hwpro2]proposal hwproposal1
[AR651-IPsec-profile-hwpro2]pfs dh-group14
[AR651-IPsec-profile-hwpro2]quit
```

步骤 10 配置虚拟隧道接口。

```
[AR651]interface Tunnel0/0/1
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]source 22.xx.xx.22
[AR651-Tunnel0/0/1]destination 11.xx.xx.11
[AR651-Tunnel0/0/1]IPsec profile hwpro1
[AR651-Tunnel0/0/1]quit
[AR651]interface Tunnel0/0/2
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 22.xx.xx.22
[AR651-Tunnel0/0/2]destination 11.xx.xx.12
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

相关命令说明如下：

- interface Tunnel0/0/1、interface Tunnel0/0/2：两条 VPN 连接对应的 Tunnel 隧道。

  本示例中，Tunnel0/0/1 对应 VPN 网关主 EIP 所在的 VPN 连接；Tunnel0/0/2 对应 VPN 网关主 EIP2 所在的 VPN 连接。
- ip address：AR 路由器的 Tunnel 接口地址。
- source：AR 路由器的公网地址。
- destination：VPN 网关的主 EIP/主 EIP2。

步骤 11 配置 NQA。

```
[AR651]nqa test-instance IPsec_nqa1 IPsec_nqa1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]test-type icmp
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]destination-address ipv4 169.254.70.2
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit
[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]destination-address ipv4 169.254.71.2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]frequency 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]quit
```

相关命令说明如下：

- nqa test-instance IPsec_nqa1 IPsec_nqa1、nqa test-instance IPsec_nqa2 IPsec_nqa2：NQA 名称。

  本示例中，IPsec_nqa1 对应 VPN 网关主 EIP 所在的 VPN 连接；IPsec_nqa2 对应 VPN 网关主 EIP2 所在的 VPN 连接。
- destination-address：VPN 网关的 Tunnel 接口地址。

- source-address：AR 路由器的 Tunnel 接口地址。

步骤 12 配置静态路由联动 NQA 功能。

```
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1
IPsec_nqa1
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/2 track nqa IPsec_nqa2
IPsec_nqa2
```

相关参数说明如下：

- 192.168.0.0：VPC 的本端子网。
- 同一条命令中，Tunnel*x* 和 IPsec_nqa*x* 需要同属于一条 VPN 连接。

----结束

结果验证

步骤 1 登录管理控制台，单击“网络 > VPN”进入 VPN 控制台。

步骤 2 在左侧导航栏，单击“虚拟专用网络 > 企业版-VPN 连接”。

此时可以看到两条 VPN 连接状态均变为“正常”。

----结束

2.1.7 步骤六：验证网络互通情况

操作步骤

步骤 1 登录管理控制台，单击“计算 > 弹性云主机”。

步骤 2 登录弹性云主机。

本示例是通过管理控制台远程登录（VNC 方式）。

步骤 3 在弹性云主机的远程登录窗口，执行以下命令，验证网络互通情况。

ping 172.16.0.100

其中，172.16.0.100 为数据中心服务器的 IP 地址，请根据实际替换。

回显如下信息，表示网络已通。

```
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=27ms TTL=245
```

----结束

2.2 经典版 VPN 创建流程

2.2.1 创建 VPN 网关

操作场景

您需要将 VPC 中的弹性云主机和您的数据中心或私有网络连通，需要先创建 VPN 网关。

前置条件

- 请确认虚拟私有云 VPC 已经创建完成。如何创建虚拟私有云 VPC，请参见《虚拟私有云用户指南》。
- 请确认虚拟私有云 VPC 的安全组规则已经配置，ECS 通信正常。如何配置安全组规则，请参见《虚拟私有云用户指南》。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 网关”。
   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”。
3. 在“VPN 网关”界面，单击“创建 VPN 网关”。
4. 根据界面提示配置参数，并单击“立即创建”。
5. 确认创建的 VPN 网关规格，单击“确认申请”。

2.2.2 创建 VPN 连接

操作场景

您需要将 VPC 中的弹性云主机和您的数据中心或私有网络连通，创建 VPN 网关后需要创建 VPN 连接。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 连接”。
   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”。
3. 在“VPN 连接”页面，单击“创建 VPN 连接”。
4. 根据界面提示配置参数，并单击“立即创建”。
5. 因为隧道的对称性，还需要在您自己数据中心的路由器或者防火墙上进行 IPsec VPN 隧道配置。

2.2.3 配置对端设备

配置对端设备详细请参见《虚拟专用网络管理员指南》，该指南可以帮助您配置本地的 VPN 设备，实现您本地网络与 VPC 子网的互联互通。

3 权限管理

3.1 创建用户并授权使用 VPN

如果您需要对您所拥有的 VPN 进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称 IAM），通过 IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建 IAM 用户，让员工拥有唯一安全凭证，并使用 VPN 资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将 VPN 资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，不需要创建独立的 IAM 用户，您可以跳过本章节，不影响您使用 VPN 服务的其它功能。

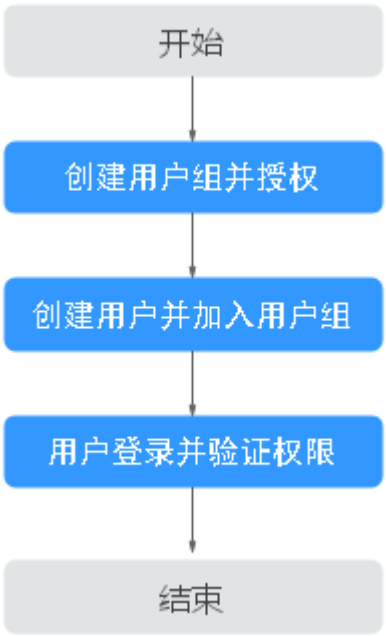
本章节为您介绍对用户授权的方法，操作流程如图 3-1 所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的 VPN 权限，并结合实际需求进行选择。

示例流程

图3-1 给用户授予 VPN 权限流程



1. 创建用户组并授权

   在 IAM 控制台创建用户组，并授予虚拟专用网络服务权限“VPN Administrator”。

2. 创建用户并加入用户组

   在 IAM 控制台创建用户，并将其加入 1 中创建的用户组。

3. 用户登录并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

   - 在“服务列表”中选择“网络 > 虚拟专用网络”，进入“虚拟专用网络 > 企业版-VPN 网关”页面，单击右上角“创建 VPN 网关”，尝试创建 VPN 网关，如果创建成功，表示“VPN Administrator”已生效。
   - 在“服务列表”中选择除 VPN 服务外（假设当前权限仅包含 VPN Administrator）的任一服务，若提示权限不足，表示“VPN Administrator”已生效。

3.2 VPN 自定义策略

如果系统预置的 VPN 权限，不满足您的授权要求，可以创建自定义策略。

目前云服务平台支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。

- JSON 视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写 JSON 格式的策略内容。

具体创建步骤请参见：《统一身份认证服务用户指南》的“创建自定义策略”章节。本章为您介绍常用的 VPN 自定义策略样例。

VPN 自定义策略样例

- 示例 1：授权用户删除 VPN 网关

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpn:vpnGateways:delete"
            ]
        }
    ]
}
```

- 示例 2：拒绝用户删除 VPN 连接

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在 Allow 和 Deny，则遵循 **Deny 优先原则**。

  如果您给用户授予 VPN FullAccess 的系统策略，但不希望用户拥有 VPN FullAccess 中定义的删除 VPN 连接权限，您可以创建一条拒绝删除 VPN 连接的自定义策略，然后同时将 VPN FullAccess 和拒绝策略授予用户，根据 Deny 优先原则，则用户可以对 VPN 执行除了删除 VPN 连接外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "vpn:vpnGateways:delete"
            ]
        }
    ]
}
```

- 示例 3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpn:vpnGateways:create",
                "vpn:vpnConnections:create",
```

```
                "vpn:customerGateways:create"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "vpn:vpnGateways:delete",
                "vpn:vpnConnections:delete",
                "vpn:customerGateways:create"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "vpc:vpcs:list",
                "vpc:subnets:get"
            ]
        }
    ]
}
```

4 用户指南

4.1 企业版 VPN 网关管理

4.1.1 创建 VPN 网关

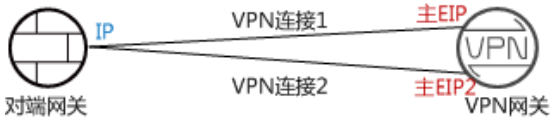
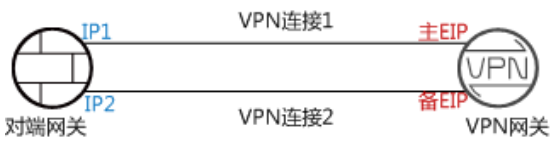
场景描述

如果您需要将 VPC 中的弹性云主机和您的数据中心或私有网络连通，创建 VPN 连接之前，需要创建 VPN 网关。

背景信息

根据对端网关 IP 地址个数不同，推荐的组网如表 4-1 所示。

表4-1 组网关系

对端网关 IP 个数	推荐组网	说明
1		VPN 网关推荐使用双活模式，该场景占用 1 个 VPN 连接组配额。
2		VPN 网关推荐使用主备模式，该场景占用 2 个 VPN 连接组配额。

- 如果用户数据中心仅有一个对端网关，且对端网关只能配置一个 IP 地址，VPN 网关推荐使用双活模式，主 EIP、主 EIP2 各创建一条 VPN 连接，对接同一个对端网关的同一个 IP 地址。该场景下仅占用一个 VPN 连接组配额。
- 如果用户数据中心存在两个对端网关，或一个对端网关可以配置两个 IP 地址，VPN 网关推荐使用主备模式，主 EIP、备 EIP 各创建一条 VPN 连接，对接到对端网关的不同 IP 地址。该场景下占用两个 VPN 连接组配额。

约束与限制

- 非国密型网关不支持变更为国密型网关。
- 关联企业路由器场景下，需要关注企业路由器的路由表条数规格限制。

前提条件

- 请确认虚拟私有云 VPC 已经创建完成。如何创建虚拟私有云 VPC，请参见《虚拟私有云用户指南》。
- 请确认虚拟私有云 VPC 的安全组规则已经配置，ECS 通信正常。如何配置安全组规则，请参见《虚拟私有云用户指南》。
- 如果通过企业路由器 ER 关联 VPN 网关，请确认企业路由器 ER 已经创建完成。如何创建企业路由器 ER，请参见《企业路由器 ER 用户指南》。

操作步骤

步骤 1 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。

步骤 2 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。

步骤 3 在“VPN 网关”界面，单击“创建 VPN 网关”。

步骤 4 根据界面提示配置参数，单击“立即创建”。

VPN 网关参数请参见表 4-2。

表4-2 VPN 网关参数说明

参数	说明	取值样例
计费模式	• 按需计费：后付费方式，VPN 网关和 VPN 连接组按使用时长收取费用，计费周期为 1 小时。	按需计费
区域	选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。 不同区域的资源之间网络不互通。	请根据实际需要进行选择
名称	VPN 网关的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	vpngw-001
网络类型	• 公网：VPN 网关通过公网建立 VPN 连接。 • 私网：VPN 网关通过私网建立 VPN 连接。	公网
协议类型	支持“IPv4”和“IPv6”两种类型。	IPv6

参数	说明	取值样例
关联模式	• 虚拟私有云 通过 VPC 向对端网关或本端子网内服务器发送通信消息。 • 企业路由器 通过 ER 向对端网关或 ER 下所有 VPC 所在子网发送通信消息。 说明 该场景下需要关注企业路由器的路由表条数规格限制。如果对端网关和 VPN 网关发送的路由条数超过企业路由器的规格，则企业路由器将无法学习到超出部分的路由信息，最终导致 VPN 网关和对端网关之间的流量不通。	虚拟私有云
虚拟私有云	选择虚拟私有云 VPC 信息。	vpc-001(192.168.0.0/16)
企业路由器	仅“关联模式”采用“企业路由器”时需要配置。 选择企业路由器 ER 信息。	er-001
互联子网	用于 VPN 网关和 VPC 通信，请确保选择的互联子网存在 4 个及以上可分配的 IP 地址。	192.168.66.0/24
本端子网	VPC 与对端网关对应数据中心互通的子网。 • 选择子网 选择本 VPC 子网信息。 • 输入网段 可以输入本 VPC 下的子网信息；也可以输入与本 VPC 建立了对等网络的 VPC 子网信息。	192.168.1.0/24,192.168.2.0/24
BGP ASN	VPN 网关会根据输入值创建相应的 ASN，VPN 网关和对端网关的 BGP ASN 需要不同。	64512
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一 VPC 网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 • 当存在两个及以上可用区时，必须选择两个可用区。 部署在两个可用区的 VPN 网关具备更高的可用性。建议您根据 VPC 内资源所在的可用区选择网关的可用区。 • 当仅存在一个可用区时，可选择此可用区创建 VPN 网关。	可用区 1、可用区 2

参数	说明	取值样例
VPN 连接组数	VPN 网关默认提供 10 个免费的 VPN 连接组。 • 如果用户侧数据中心只有一个公网出口网关，所有服务器（或用户主机）都通过该网关连接至 Internet：这种情况需要配置一个 VPN 连接组，即 VPN 网关的两个 EIP 分别配置一条 VPN 连接和用户侧出口网关通信。 • 如果用户侧数据中心有两个公网出口网关，所有服务器（或用户主机）通过两个网关连接至 Internet：这种情况需要配置两个 VPN 连接组，即 VPN 网关的两个 EIP 分别配置一条 VPN 连接和两个用户侧出口网关通信。	10
HA 模式	• 双活：主 EIP 和主 EIP2 均与对端网关建立 VPN 连接，但只有一条 VPN 连接进行数据交互。当其中一条 VPN 连接发生故障时，数据交互切换至另一条 VPN 连接。 • 主备：主 EIP 与备 EIP 均与对端网关建立 VPN 连接，默认情况下流量仅通过主链路进行传输。如果主链路故障，流量自动切换至备链路进行传输；主链路恢复正常后，流量回切至主链路进行传输。	双活
主 EIP	用于 VPN 网关和对端网关进行网络连接。 • 现在创建：创建新 EIP。 • 使用已有：使用已有 EIP。	现在创建
带宽大小	EIP 对应带宽大小，单位：Mbit/s。 • 所有使用该 EIP 创建的 VPN 连接均会分摊占用该 EIP 的带宽大小，所有 VPN 连接的带宽总和不能超过该 EIP 的带宽大小。 当网络流量超过 EIP 的带宽大小时，有可能造成网络拥塞导致 VPN 连接中断，请提前做好带宽规划。 • 支持在云监控中配置告警规则对带宽进行监控。 • 支持用户在允许的带宽范围内自定义带宽大小。	10 Mbit/s
带宽名称	EIP 对应带宽对象的名称。	Vpngw-bandwidth1
主 EIP2	一个 VPN 网关需要绑定一组弹性公网 IP（即主 EIP、主 EIP2），每个公网 IP 可以独立规划带宽。	现在创建

参数	说明	取值样例
备 EIP	一个 VPN 网关需要绑定一组弹性公网 IP（即主/备 EIP），每个公网 IP 可以独立规划带宽。 说明 VPN 网关“计费模式”为“按需计费”场景下，若备 EIP 为按流量计费，强烈建议用户在云监控中配置告警规则对备 EIP 进行监控，避免因 VPN 连接故障、主链路切换至备链路导致的流量费用超支问题。 如何在云监控中对 EIP 配置告警规则，请参见《弹性公网 IP 用户指南》。	现在创建
公网带宽	按需计费支持两种计费方式：按带宽计费/按流量计费。 • 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 • 按流量计费：指定带宽上限，按实际使用的出云流量计费，与使用时间无关。	按流量计费
带宽大小	EIP 对应带宽大小，单位 Mbit/s。 • 所有使用该 EIP 创建的 VPN 连接均会分摊占用该 EIP 的带宽大小，所有 VPN 连接的带宽总和不能超过该 EIP 的带宽大小。 当网络流量超过 EIP 的带宽大小时，有可能造成网络拥塞导致 VPN 连接中断，请提前做好带宽规划。 • 支持在云监控中配置告警规则对带宽进行监控。 • 支持用户在允许的带宽范围内自定义带宽大小。	10 Mbit/s
带宽名称	EIP 对应带宽对象的名称。	Vpngw-bandwidth2
企业项目	创建 VPN 时，可以将 VPN 加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为 default。 关于创建和管理企业项目的详情，请参见《企业项目管理用户指南》。	default
高级配置	仅“网络类型”为“私网”、“关联模式”采用“虚拟私有云”时需要配置。 • 选择：适用于同租户场景，选择本租户下接入虚拟私有云、接入子网、接入 IP。 • 输入：适用于跨租户场景，填写接入项目、接入账号、接入虚拟私有云和接入子网。	选择

参数	说明	取值样例
接入虚拟私有云	当 VPN 网关的南北向需要连接不同的虚拟私有云时，设置北向的虚拟私有云为该接入虚拟私有云。VPN 网关关联的虚拟私有云为南向业务虚拟私有云。	选择“与网关关联的虚拟私有云一致”
接入子网	缺省情况下，VPN 网关从关联的虚拟私有云的互联子网接入。当 VPN 网关需要从指定子网接入时设置。	选择“与互联子网一致”

步骤 5 （可选）对于国密型网关，创建后需要上传 VPN 网关证书，否则 VPN 连接将无法建立。

----结束

4.1.2 查看已创建的 VPN 网关

场景描述

用户创建 VPN 网关后，可以查看已创建的 VPN 网关。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。
3. 在“VPN 网关”页面，查看 VPN 网关列表信息。
4. 单击 VPN 网关的名称，查看 VPN 网关详情。
   - 公网类型网关：可查看基本信息和弹性公网 IP。
   - 私网类型网关：可查看基本信息和高级配置。
   - 国密型网关：可查看基本信息和证书信息。

说明

在 VPN 网关列表中，选择目标 VPN 网关所在行，单击网关 IP 列的 ，查看该 VPN 网关带宽和流量的监控信息。

4.1.3 修改已创建的 VPN 网关

场景描述

您可以对 VPN 网关基本信息进行修改，包括名称、本端子网。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。

2. 在左侧导航栏，单击“虚拟专用网络 > 企业版-VPN 网关”。
3. 在“VPN 网关”界面，选择目标 VPN 网关所在行，单击操作列的“修改基本信息”。

   若仅需修改 VPN 网关的名称，您也可以直接单击 VPN 网关名称右侧的  按钮进行修改。
4. 根据界面提示，修改 VPN 网关的名称、本端子网。
5. 单击“确定”完成修改。

4.1.4 修改 VPN 网关策略模板

场景描述

若 VPN 网关规格为“专业型 1-非固定 IP”或“专业型 2-非固定 IP”，您可以在 VPN 网关页面修改策略模板。

操作步骤

1. 登录管理控制台，单击“网络 >VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 > 企业版-VPN 网关”。
3. 在“VPN 网关”界面，选择目标 VPN 网关所在行，单击操作列“查看/修改策略模板”，在“策略模板”页签下单击“修改策略模板”进行修改。

说明

修改策略模板后，以非固定 IP 接入的对端网关需要更新对应配置重新接入，否则会导致连接中断。

表4-3 策略模板参数说明

参数		说明	是否支持修改
IKE 策略	版本	IKE 密钥交换协议版本，支持的版本：v2。	×
	认证算法	认证哈希算法，支持的算法： • SHA2-256 • SHA2-384 • SHA2-512 默认配置为：SHA2-256。	√

参数		说明	是否支持修改
	加密算法	加密算法，支持的算法： • AES-256-GCM-16 • AES-128（此算法安全性较低，请慎用） • AES-192（此算法安全性较低，请慎用） • AES-256（此算法安全性较低，请慎用） 默认配置为：AES-128	√
	DH 算法	支持的算法 ： • Group 14（此算法安全性较低，请慎用） • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 默认配置为：Group 15。	√
	生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 • 单位：秒。 • 取值范围：60~604800 默认配置为：86400。	√
	本端标识	IPsec 连接协商时，VPN 网关的鉴权标识。在对端网关配置的 VPN 网关标识需要和此处配置的本端标识保持一致，否则协商失败。 默认配置为：VPN 网关的 EIP。	×
IPsec 策略	认证算法	认证哈希算法，支持的算法： • SHA2-256 • SHA2-384 • SHA2-512 默认配置为：SHA2-256。	√

参数		说明	是否支持修改
	加密算法	加密算法，支持的算法： • AES-256-GCM-16 • AES-128（此算法安全性较低，请慎用） • AES-192（此算法安全性较低，请慎用） • AES-256（此算法安全性较低，请慎用） 默认配置为：AES-128	√
	PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，配置 IPsec 隧道协商时使用。 PFS 组支持的算法： • DH group 14（此算法安全性较低，请慎用） • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 • Disable 默认配置为：DH group 15。	√
	传输协议	IPsec 传输和封装用户数据时使用的安全协议。 目前支持的协议：ESP。	×
	生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 • 单位：秒。 • 取值范围：30~604800 默认配置：3600。	√

4. 单击“确定”完成修改。

4.1.5 绑定弹性公网 IP

场景描述

用户根据需要为已创建的 VPN 网关绑定 EIP。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。
3. 选择目标 VPN 网关所在行，单击操作列的“绑定 EIP”。
   - 如果 VPN 网关是双活模式，VPN 网关支持绑定主 EIP/主 EIP2。
   - 如果 VPN 网关是主备模式，VPN 网关支持绑定主/备 EIP。
4. 根据界面提示，选择需要绑定的 EIP，单击“确定”。

4.1.6 解绑弹性公网 IP

场景描述

用户创建 VPN 网关后，可以解绑已关联的弹性公网 IP。

约束与限制

已创建 VPN 连接的 EIP 不支持解绑操作。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。
3. 在“VPN 网关”列表页面，选择目标 VPN 所在行，单击操作列的“解绑 EIP”。
   - 如果 VPN 网关是双活模式，VPN 网关支持解绑主 EIP/主 EIP2，请根据实际需要进行解绑配置。
   - 如果 VPN 网关是主备模式，VPN 网关支持解绑主/备 EIP，请根据实际需要进行解绑配置。
4. 单击“是”，完成解绑。

说明

未绑定 VPN 网关的弹性 IP 会继续计费（弹性 IP 保有费），如果不再使用建议释放该弹性 IP。

4.1.7 删除 VPN 网关

场景描述

当无需使用 VPN 网关时，可以删除 VPN 网关。

约束与限制

- 在 VPN 网关状态处于“创建中”、“更新中”、“删除中”三种状态时，不能进行 VPN 网关删除操作。
- 如果 VPN 网关下存在 VPN 连接，则无法直接删除 VPN 网关。您需要先删除 VPN 网关下的所有 VPN 连接，然后再删除 VPN 网关。

  如何删除 VPN 连接，请参见删除 VPN 连接。
- 如果 VPN 网关绑定的 EIP 计费模式为包周期，删除 VPN 网关时会同步解绑 EIP。解绑后弹性公网 IP 继续保留，若不再使用可在网关删除后释放。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。
3. 在“VPN 网关”界面需要删除的 VPN 网关所在行，选择“更多 ＞ 删除”。
4. 单击“是”，完成删除。

4.1.8 上传 VPN 网关证书

场景描述

国密型 VPN 网关，需要上传证书，用于和对端网关建立 VPN 连接；首次使用国密型网关，用户需要在云监控页面配置云监控告警，详细步骤请参见《云监控服务用户指南》。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。
3. 在“VPN 网关”界面需要上传证书的国密型 VPN 网关所在行，选择“更多 ＞ 查看/上传证书”。
4. 单击“上传证书”，根据界面提示填写相关信息。

   VPN 网关证书参数请参见表 4-4。

表4-4 VPN 网关证书参数说明

参数	说明	取值样例
证书名称	用户自定义。	certificate-001

参数	说明	取值样例
签名证书	签名证书用于对数据进行签名认证，以保证数据的有效性和不可否认性。 以文本方式打开签名证书 PEM 格式的文件（后缀名为“.pem”），将证书内容复制到此处。 签名证书需要同时上传签发此签名证书的 CA 证书。	-----BEGIN CERTIFICATE----- *签名证书* -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- *CA 证书* -----END CERTIFICATE-----
签名私钥	签名私钥用于对签名证书加密过的数据进行解密，签名私钥是非公开的，由用户自行保管。 以文本方式打开签名私钥 KEY 格式的文件（后缀名为“.key”），将私钥复制到此处。	-----BEGIN EC PRIVATE KEY----- *签名私钥* -----END EC PRIVATE KEY-----
加密证书	加密证书用于对 VPN 连接的传输数据进行加密，以保证数据的保密性和完整性。签发该加密证书的 CA 机构需和签发签名证书的 CA 机构保持一致。 以文本方式打开加密证书 PEM 格式的文件（后缀名为“.pem”），将证书内容复制到此处。	-----BEGIN CERTIFICATE----- *加密证书* -----END CERTIFICATE-----
加密私钥	加密私钥用于对加密证书加密过的数据进行解密，加密私钥是非公开的，由用户自行保管。 以文本方式打开加密私钥 KEY 格式的文件（后缀名为“.key”），将私钥内容复制到此处。	-----BEGIN EC PRIVATE KEY----- *加密私钥* -----END EC PRIVATE KEY-----

4.1.9 更换 VPN 网关证书

场景描述

国密型 VPN 网关证书到期或失效后，需要更换 VPN 网关证书。

更换 VPN 网关证书，对端网关需要使用新的配套 CA 证书与 VPN 网关进行重协商，否则连接中断。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。
3. 在“VPN 网关”界面需要上传证书的国密型 VPN 网关所在行，选择“更多 ＞ 查看/上传证书”。
4. 单击“更换”，根据界面提示填写相关信息。

   VPN 网关证书参数请参见表 4-5。

表4-5 VPN 网关证书参数说明

参数	说明	取值样例
证书名称	不支持修改。	与原证书名称保持一致。
新签名证书	签名证书用于对数据进行签名认证，以保证数据的有效性和不可否认性。 以文本方式打开签名证书 PEM 格式的文件（后缀名为“.pem”），将证书内容复制到此处。 签名证书需要同时上传签发此签名证书的 CA 证书。	-----BEGIN CERTIFICATE----- *签名证书* -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- *CA 证书* -----END CERTIFICATE-----
新签名私钥	签名私钥用于对签名证书加密过的数据进行解密，签名私钥是非公开的，由用户自行保管。 以文本方式打开签名私钥 KEY 格式的文件（后缀名为“.key”），将私钥复制到此处。	-----BEGIN EC PRIVATE KEY----- *签名私钥* -----END EC PRIVATE KEY-----
新加密证书	加密证书用于对 VPN 连接的传输数据进行加密，以保证数据的保密性和完整性。签发该加密证书的 CA 机构需和签发签名证书的 CA 机构保持一致。 以文本方式打开加密证书 PEM 格式的文件（后缀名为“.pem”），将证书内容复制到此处。	-----BEGIN CERTIFICATE----- *加密证书* -----END CERTIFICATE-----

参数	说明	取值样例
新加密私钥	加密私钥用于对加密证书加密过的数据进行解密，加密私钥是非公开的，由用户自行保管。 以文本方式打开加密私钥 KEY 格式的文件（后缀名为“.key”），将私钥内容复制到此处。	-----BEGIN EC PRIVATE KEY----- *加密私钥* -----END EC PRIVATE KEY-----

5. 勾选“我已知晓上述内容，确认更换证书”，单击“确定”。

4.1.10 按标签搜索 VPN 网关

场景描述

用户在使用 VPN 服务时，根据使用场景不同，可以将 VPN 资源按照特定规则进行分类，便于资源管理与费用计算。

VPN 支持对接标签管理服务（Tag Management Service，简称 TMS），通过给账号下 VPN 资源添加标签，可以对 VPN 资源进行自定义标记，实现资源的分类。已添加标签的 VPN 资源，用户可以在控制台对应位置，按照标签进行搜索。

前提条件

已为 VPN 资源添加标签。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。
3. 单击右上角“标签搜索”，选择对应标签键值，然后单击“搜索”。
   - 此查询功能仅支持选择下拉列表中已存在的键和值。
   - 支持最多 20 个不同标签的组合搜索。

4.2 企业版对端网关管理

4.2.1 创建对端网关

场景描述

如果您需要将 VPC 中的弹性云主机和您的数据中心或私有网络连通，创建 VPN 连接之前，需要创建对端网关。

约束与限制

- 国密型对端网关标识仅支持网关 IP，且该网关 IP 地址值必须是静态地址。
- FQDN 类型标识的对端网关只支持策略模板模式对接。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-对端网关”。
3. 在“对端网关”界面，单击“创建对端网关”。
4. 根据界面提示配置参数，单击“立即创建”。

   对端网关参数请参见表 4-6。

表4-6 对端网关参数说明

参数	说明	取值样例
名称	对端网关的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	cgw-001
BGP ASN	请输入用户数据中心或私有网络的 ASN。 对端网关的 BGP ASN 与 VPN 网关的 BGP ASN 不能相同。	65000
CA 证书（可选）	使用国密型网关时，需要上传对端网关的 CA 证书，用于和 VPN 网关建立 VPN 连接。 • 上传证书：手动输入，以“-----BEGIN CERTIFICATE-----”作为开头，以“-----END CERTIFICATE-----”作为结尾。 • 使用已上传证书：查看并勾选已上传证书，请注意证书到期时间。	-----BEGIN CERTIFICATE----- *CA 证书* -----END CERTIFICATE-----
标签	VPN 服务的标识，包括键和值，最大可以创建 20 对标签。 标签设置时，可以选择预定义标签，也可以自定义创建。 预定义标签可以通过单击“查看预定义标签”进行查看。	-

5. （可选）如果存在两个对端网关，请参见上述步骤添加另一个网关标识对应的对端网关。

相关操作

因为隧道的对称性，还需要在您数据中心的路由器或者防火墙上进行 IPsec VPN 隧道配置。

4.2.2 查看已创建的对端网关

场景描述

用户创建对端网关后，可以查看已创建的对端网关。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-对端网关”。
3. 在“对端网关”界面，查看对端网关列表信息。
4. 单击对端网关名称，查看对端网关详情页面。
   - 基础信息：可查看对端网关的名称、ID、BGP ASN、VPN 连接。
   - CA 证书：可查看证书序列号、签名算法、到期时间、颁发者、使用者，可添加或更换 CA 证书（对端网关为国密型时，需要添加 CA 证书）。

4.2.3 修改已创建的对端网关

场景描述

用户创建对端网关后，可以修改已创建的对端网关名称，国密型对端网关同时支持添加或更换 CA 证书。

添加或更换 CA 证书相关操作请参见上传对端网关证书和更换对端网关证书。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-对端网关”。
3. 在“对端网关”界面，选择目标对端网关所在行，单击 。
4. 修改对端网关名称，单击“确定”。

4.2.4 删除对端网关

场景描述

用户根据实际需要删除已创建的对端网关。

约束与限制

若对端网关已被 VPN 连接关联，则无法直接删除该对端网关，需要先将该对端网关在 VPN 连接中移除。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-对端网关”。

3. 在“对端网关”界面，选择目标对端网关所在行，单击操作列的“删除”。
4. 确定要删除的对端网关信息，单击“是”。

4.2.5 上传对端网关证书

场景描述

国密型对端网关，需要上传对端网关的 CA 证书，用于和 VPN 网关建立 VPN 连接。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-对端网关”。
3. 在“对端网关”界面，单击目标对端网关名称进入详情页面。
4. 在“CA 证书”区域，单击“添加”。
5. 根据界面提示填写相关信息，单击“确定”。
   对端网关 CA 证书参数请参见表 4-7。

表4-7 对端网关 CA 证书参数说明

参数	说明	取值样例
上传证书	对端网关的 CA 证书。	-----BEGIN CERTIFICATE----- *CA 证书* -----END CERTIFICATE-----
使用已上传证书	查看并勾选已上传证书，请注意证书到期时间。	-

4.2.6 更换对端网关证书

场景描述

国密型网关 CA 证书到期或失效后，需要更换 CA 证书。

更换 CA 证书后，该对端网关需要使用新 CA 签发的国密证书与 VPN 网关重协商，否则连接断开。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-对端网关”。
3. 在“对端网关”界面，单击目标对端网关名称进入详情页面。
4. 在“CA 证书”区域，单击“更换”。

5. 根据界面提示填写相关信息。
   对端网关 CA 证书参数请参见表 4-8。

表4-8 对端网关 CA 证书参数说明

参数	说明	取值样例
上传证书	对端网关的 CA 证书。	-----BEGIN CERTIFICATE----- *CA 证书* -----END CERTIFICATE-----
使用已上传证书	查看并勾选已上传证书，请注意证书到期时间。	-

6. 勾选“我已知晓上述内容，确认更换 CA 证书”，单击“确定”。

4.2.7 按标签搜索对端网关

场景描述

用户在使用 VPN 服务时，根据使用场景不同，可以将 VPN 资源按照特定规则进行分类，便于资源管理与费用计算。

VPN 支持对接标签管理服务（Tag Management Service，简称 TMS），通过给账号下 VPN 资源添加标签，可以对 VPN 资源进行自定义标记，实现资源的分类。已添加标签的 VPN 资源，用户可以在控制台对应位置，按照标签进行搜索。

前提条件

已为 VPN 资源添加标签。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-对端网关”。
3. 单击右上角“标签搜索”，选择对应标签键值，然后单击“搜索”。
   - 此查询功能仅支持选择下拉列表中已存在的键和值。
   - 支持最多 20 个不同标签的组合搜索。

4.3 企业版 VPN 连接管理

4.3.1 创建 VPN 连接

场景描述

如果您需要将 VPC 中的弹性云主机和数据中心或私有网络连通，创建 VPN 网关、对端网关之后，需要继续创建 VPN 连接。

约束与限制

- 使用静态路由模式创建 VPN 连接时，使能 NQA 前请确认对端网关支持 ICMP 功能，且对端接口地址已在对端网关上正确配置，否则可能导致流量不通。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 连接”。
3. 在“VPN 连接”页面，单击“创建 VPN 连接”。

说明

VPN 网关的两个 EIP 支持分别和对端网关创建一条 VPN 连接。VPN 双连接可以很大程度提升云上云下连接的可靠性，强烈建议配置。

4. 根据界面提示配置参数，单击“立即购买”。

   VPN 连接参数请参见表 4-9。

表4-9 VPN 连接参数说明

参数	说明	取值样例
名称	VPN 连接的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	vpn-001
VPN 网关	选择待关联的 VPN 网关名称。 您也可以单击“创建 VPN 网关”进行新建，相关参数解释请参见表 4-2。 如果您使用国密型 VPN 网关，且 VPN 网关没有绑定相关证书，请先单击右侧“上传证书”完成上传证书操作，否则 VPN 连接将无法建立。	vpngw-001
网关 IP	选择 VPN 网关 IP。 VPN 网关对接同一对端网关时，不能选择已使用过的 EIP 地址。	可选的网关 IP

参数	说明	取值样例
对端网关	选择对端网关信息。 您也可以单击“创建对端网关”进行新建，相关参数解释请参见表 4-6。 如果您使用国密型网关，且对端网关没有绑定 CA 证书，请先参见上传对端网关证书上传 CA 证书，否则 VPN 连接将无法建立。 说明 如果一个对端网关同时对接多个 VPN 网关，则 VPN 网关的 BGP ASN 和连接模式需要相同。	cgw-001
连接模式	IPsec 连接的模式，支持路由模式和策略模式。 • 静态路由模式。 根据路由配置（本端子网与对端子网）确定哪些数据进入 IPsec VPN 隧道。 **适用场景：对端网关之间要求互通。** • BGP 路由模式。 根据 BGP 动态路由确定哪些数据进入 IPsec VPN 隧道。 **适用场景：对端网关之间要求互通，互通子网数量多或变化频繁、与专线互备等组网场景。** • 策略模式。 根据策略规则（用户侧到 VPC 之间通信的数据流信息）确定哪些数据进入 IPsec VPN 隧道，支持以源网段和目的网段定义策略规则。 **适用场景：对端网关之间要求隔离。**	静态路由模式

参数	说明	取值样例
对端子网	指需要通过 VPN 连接访问云上 VPC 的用户侧子网。 若存在多个对端子网，请用半角逗号（,）隔开。 说明 • 对端子网可以和本端子网重叠，但不能重合。 • 对端子网不能被 VPN 网关关联的 VPC 内已有子网所包含；不能作为被 VPN 网关关联的 VPC 自定义路由表的目的地址。 • 对端子网不能是 VPC 的预留网段，例如 100.64.0.0/10、214.0.0.0/8。	172.16.1.0/24,172.16.2.0/24
接口分配方式	仅“连接模式”采用“静态路由模式”和“BGP 路由模式”时需要配置。 说明 • 接口地址为 VPN 网关和对端网关通信的 tunnel 隧道 IP 地址。 • 如果对端网关的 tunnel 接口地址固定不可更改，请使用“手动分配”模式，并根据对端网关的 tunnel 接口地址设置 VPN 网关的 tunnel 接口地址。 • 手动分配。 仅支持在 169.254.x.x/30 网段（除 169.254.195.x/30）范围内，配置 VPN 网关本端接口地址的 tunnel 接口地址；对端网关对端接口地址的 tunnel 接口地址会根据本端接口地址随机生成。 例如：本端接口地址配置为 169.254.1.6/30，则对端接口地址自动配置为 169.254.1.5/30。 • 自动分配。 VPN 网关默认使用 169.254.x.x/30 网段对 tunnel 接口分配地址。 自动分配的本端接口地址/对端接口地址，可以在 VPN 连接页面，单击“修改连接信息”进行查看。	自动分配
本端隧道接口地址	仅“接口分配方式”采用“手动分配”时需要配置。 配置在 VPN 网关上的 tunnel 接口地址。	-

参数	说明	取值样例
对端隧道接口地址	仅“接口分配方式”采用“手动分配”时需要配置。 配置在对端网关上的 tunnel 接口地址，该接口地址需要和对端网关实际配置的 tunnel 接口地址保持一致。	-
检测机制	仅“连接模式”采用“静态路由模式”时需要配置。 **说明** **功能开启前，请确认对端网关支持 ICMP 功能，且对端接口地址已在对端网关上正确配置，否则可能导致流量不通。** 功能开启后，VPN 网关会自动对对端接口地址进行 NQA 探测。	勾选
预共享密钥	VPN 网关和对端网关的预共享密钥需要保持一致。 取值范围： • 取值长度：8~128 个字符。 • 只能包括以下几种字符，且必须包含三种及以上类型： – 数字。 – 大写字母。 – 小写字母。 – 特殊符号：包括“~”、“!”、“@”、“#”、“$”、“%”、“^”、“(”、“)”、“-”、“_”、“+”、“=”、“{”、“}”、","、"."、"/"、“:”和“;”。 **说明** **国密型 VPN 连接无此参数。**	Test@123
确认密钥	再次输入预共享密钥。 **说明** **国密型 VPN 连接无此参数。**	Test@123

参数	说明	取值样例
策略规则	仅“连接模式”采用“策略模式”时需要配置。 用于定义本端子网到对端子网之间具体进入 VPN 连接加密隧道的数据流信息，由源网段与目的网段来定义。系统默认支持配置 5 条策略规则。 • 源网段。 源网段必须包含部分本端子网。其中，0.0.0.0/0 表示任意地址。 • 目的网段。 目的网段必须完全包含对端子网。一个策略规则最大支持 5 个目的网段，目的网段之间使用英文逗号（,）进行分隔。	• 源网段 1：192.168.1.0/24 • 目的网段 1：172.16.1.0/24,172.16.2.0/24 • 源网段 2：192.168.2.0/24 • 目的网段 2：172.16.1.0/24,172.16.2.0/24
策略配置	• 默认配置。 • 自定义配置：自定义配置 IKE 策略和 IPsec 策略。相关配置说明请参见表 4-10 和表 4-11。	自定义配置

表4-10 IKE 策略

参数	说明	取值样例
版本	IKE 密钥交换协议版本，支持的版本： • v1（v1 版本安全性较低，如果用户设备支持 v2 版本，建议选择 v2） 建立国密型 VPN 连接，IKE 密钥交换协议版本只能为“v1”。 • v2。 国密型 VPN 连接默认配置为：v1。 非国密型 VPN 连接默认配置为：v2。	v2
协商模式	仅“版本”采用“v1”时需要配置。 • Main。 当使用国密型 VPN 网关创建 VPN 连接时，“协商模式”仅支持“Main”。 • Aggressive。	Main

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： • SHA1（此算法安全性较低，请慎用）。 • MD5（此算法安全性较低，请慎用）。 • SHA2-256。 • SHA2-384。 • SHA2-512。 • SM3。 仅国密型 VPN 连接选择该认证算法，此时 IKE 密钥交换协议版本只能为“v1”。 国密型 VPN 连接默认配置为：SM3。 非国密型 VPN 连接默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： • 3DES（此算法安全性较低，请慎用）。 • AES-128（此算法安全性较低，请慎用）。 • AES-192（此算法安全性较低，请慎用）。 • AES-256（此算法安全性较低，请慎用）。 • AES-256-GCM-16。 选择该加密算法时，IKE 密钥交换协议版本只能为“v2”。 • SM4。 仅国密型 VPN 连接选择该加密算法，此时 IKE 密钥交换协议版本只能为“v1”。 国密型 VPN 连接默认配置为：SM4。 非国密型 VPN 连接默认配置为：AES-128。	AES-128

参数	说明	取值样例
DH 算法	支持的算法 ： • Group 1（此算法安全性较低，请慎用）。 • Group 2（此算法安全性较低，请慎用）。 • Group 5（此算法安全性较低，请慎用）。 • Group 14（此算法安全性较低，请慎用）。 • Group 15。 • Group 16。 • Group 19。 • Group 20。 • Group 21。 默认配置为：Group 15。 **说明** 国密型 VPN 连接无此参数。	Group 14
生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 • 单位：秒。 • 取值范围：60~604800。 • 默认配置为：86400。	86400
本端标识	IPsec 连接协商时，VPN 网关的鉴权标识。在对端网关配置的 VPN 网关标识需要和此处配置的本端标识保持一致，否则协商失败。 • IP Address（默认）。 系统自动读取 VPN 网关的 EIP 作为 IP Address，无需用户手动配置。 • FQDN。 全地址域名，支持自定义设置。长度范围是 1~128 个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 **说明** 国密型 VPN 连接无此参数。	IP Address

参数	说明	取值样例
对端标识	IPsec 连接协商时，对端网关的鉴权标识。在对端网关配置的对端网关标识需要和此处配置的对端标识保持一致，否则协商失败。 • IP Address（默认）。 系统自动读取对端网关的网关 IP 作为 IP Address，无需用户手动配置。 • FQDN。 全地址域名，支持自定义设置。长度范围是 1~128 个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 说明 国密型 VPN 连接无此参数。	IP Address

表4-11 IPsec 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： • SHA1（此算法安全性较低，请慎用）。 • MD5（此算法安全性较低，请慎用）。 • SHA2-256。 • SHA2-384。 • SHA2-512。 • SM3。 仅国密型 VPN 连接选择该认证算法。 国密型 VPN 连接默认配置为：SM3。 非国密型 VPN 连接默认配置为：SHA2-256。	SHA2-256

参数	说明	取值样例
加密算法	加密算法，支持的算法： • 3DES（此算法安全性较低，请慎用）。 • AES-128（此算法安全性较低，请慎用）。 • AES-192（此算法安全性较低，请慎用）。 • AES-256（此算法安全性较低，请慎用）。 • AES-128-GCM-16。 • AES-256-GCM-16。 • SM4。 仅国密型 VPN 连接选择该加密算法。 国密型 VPN 连接默认配置为：SM4。 非国密型 VPN 连接默认配置为：AES-128。	AES-128

参数	说明	取值样例
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，配置 IPsec 隧道协商时使用。 PFS 组支持的算法： • Disable（此算法安全性较低，请慎用）。 • DH group 1（此算法安全性较低，请慎用）。 • DH group 2（此算法安全性较低，请慎用）。 • DH group 5（此算法安全性较低，请慎用）。 • DH group 14（此算法安全性较低，请慎用）。 • DH group 15。 • DH group 16。 • DH group 19。 • DH group 20。 • DH group 21。 默认配置为：DH group 15。 说明 • 国密型 VPN 连接无此参数。 • 国密型 VPN 网关和国密型对端网关创建 VPN 连接时，需要保证国密型对端网关关闭 PFS 功能，否则会导致 VPN 连接无法建立。	DH group 15
传输协议	IPsec 传输和封装用户数据时使用的安全协议。目前支持的协议： • ESP。 默认配置为：ESP。	ESP
生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 • 单位：秒。 • 取值范围：30~604800。 • 默认配置：3600。	3600
报文封装模式	默认设置为隧道（TUNNEL）模式。	TUNNEL

说明

IKE 策略指定了 IPsec 隧道在协商阶段的加密和认证算法，IPsec 策略指定了 IPsec 隧道在数据传输阶段所使用的协议、加密以及认证算法。VPC 和数据中心的 VPN 连接在策略配置上需要保持一致，否则会导致 VPN 协商失败，进而导致 VPN 连接建立失败。

以下算法安全性较低，请慎用：

- **认证算法**：SHA1、MD5。
- **加密算法**：3DES、AES-128、AES-192、AES-256。

  出于部分对端设备不支持安全加密算法的考虑，VPN 连接的默认加密算法仍为 AES-128。在对端设备功能支持的情况下，建议使用更安全的加密算法。
- **DH 算法**：Group 1、Group 2、Group 5、Group 14。

5. 确认 VPN 连接规格，单击“提交”。
6. 参见上述步骤，创建第二条 VPN 连接。

   VPN 连接的 IP 对应关系，请参见背景信息。

4.3.2 创建健康检查

场景描述

VPN 连接创建完成后，添加健康检查可以配置 VPN 网关向对端网关发送监测报文，统计链路往返时延和丢包率，用于检测连接的质量。云监控服务提供对 VPN 连接链路往返时延和丢包率的监控指标，详情请参见支持的监控指标（企业版 VPN）。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 连接”。
3. 在“VPN 连接”界面，单击目标 VPN 连接名称，在“基本信息 ＞ 健康检查”区域单击“添加”。
4. 在“添加健康检查”界面，单击“确定”。

4.3.3 查看已创建的 VPN 连接

场景描述

用户创建 VPN 连接后，可以查看已创建的 VPN 连接。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 连接”。
3. 在“VPN 连接”界面，查看 VPN 连接列表信息。
4. 单击 VPN 连接的名称，查看 VPN 连接基本信息和策略配置。

说明

- 在 VPN 连接列表中，选择目标 VPN 连接所在行，单击“修改策略配置”，查看该 VPN 连接对应的 IKE 策略和 IPsec 策略详情。
- 在 VPN 连接列表中，选择目标 VPN 连接所在行，单击“查看监控”，查看该 VPN 连接的监控信息。

  在监控视图中，“VPN 连接状态”显示为“0”，表示 VPN 连接未连接；“VPN 连接状态”显示为“1”，表示 VPN 连接已连接；“VPN 连接状态”显示为“2”，表示 VPN 连接在最近 180 秒内未上报状态。

4.3.4 修改已创建的 VPN 连接

场景描述

VPN 连接是建立 VPN 网关和外部数据中心对端网关之间的加密通道。当 VPN 连接的网络参数变化时，可以修改 VPN 连接。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 连接”。
3. 在“VPN 连接”界面，选择目标 VPN 连接所在行，单击“修改连接信息”或“修改策略配置”。
4. 根据界面提示修改 VPN 连接的配置参数。
5. 单击“确定”。

注意

修改预共享密钥和 IKE/IPsec 策略场景下，请确保 VPN 连接和对端网关配置的信息一致，否则会导致 VPN 连接中断。

不同参数修改后的生效机制不同，如表 4-12 所示。

表4-12 生效机制

场景	参数	生效机制	操作方法
-	预共享密钥	• IKE 策略为 v1 时：修改后下个协商周期生效。 • IKE 策略为 v2 时：重建 VPN 连接后生效。 说明 国密型 VPN 连接无“预共享密钥”参数。	• IKE 策略为 v1 时 在需要修改的 VPN 连接所在行，选择“更多 > 重置密钥”，修改 VPN 连接的预共享密钥。 • IKE 策略为 v2 时 1. 删除当前 VPN 连接。 2. 重新创建 VPN 连接。
IKE 策略（版本为 v1）	加密算法 认证算法 DH 算法 协商模式 本端标识 对端标识 生命周期	修改后下个协商周期生效。 说明 • 国密型 VPN 连接不支持修改以下参数：“加密算法”、“认证算法”、“协商模式”。 • 国密型 VPN 连接无以下参数：“DH 算法”、“本端标识”、“对端标识”。	在需要修改的 VPN 连接所在行，单击“修改策略配置”。
	版本	修改后立即生效。 说明 国密型 VPN 连接不支持修改“版本”参数。	
IKE 策略（版本为 v2）	加密算法 认证算法 DH 算法 生命周期	修改后下个协商周期生效。	在需要修改的 VPN 连接所在行，单击“修改策略配置”。
	版本	修改后立即生效。	
	本端标识 对端标识	重建 VPN 连接后生效。	1. 删除当前 VPN 连接。 2. 重新创建 VPN 连接。
IPsec 策略	加密算法 认证算法 PFS 生命周期	修改后下个协商周期生效。 说明 • 国密型 VPN 连接不支持修改以下参数：加密算法、认证算法。 • 国密型 VPN 连接不包含以下参数：PFS。	在需要修改的 VPN 连接所在行，单击“修改策略配置”。
	传输协议	暂不支持控制台修改。	

4.3.5 删除 VPN 连接

场景描述

当无需使用 VPN 网络、需要释放网络资源时，可删除 VPN 连接。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 网关”。
3. 在“VPN 连接”界面所需删除的 VPN 连接所在行的操作列，选择“更多 ＞ 删除”。
4. 单击“是”，完成 VPN 连接删除。

4.3.6 按标签搜索 VPN 连接

场景描述

用户在使用 VPN 服务时，根据使用场景不同，可以将 VPN 资源按照特定规则进行分类，便于资源管理与费用计算。

VPN 支持对接标签管理服务（Tag Management Service，简称 TMS），通过给账号下 VPN 资源添加标签，可以对 VPN 资源进行自定义标记，实现资源的分类。已添加标签的 VPN 资源，用户可以在控制台对应位置，按照标签进行搜索。

前提条件

已为 VPN 资源添加标签。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏，单击“虚拟专用网络 ＞ 企业版-VPN 连接”。
3. 单击右上角“标签搜索”，选择对应标签键值，然后单击“搜索”。
   - 此查询功能仅支持选择下拉列表中已存在的键和值。
   - 支持最多 20 个不同标签的组合搜索。

4.4 经典版 VPN 网关管理

4.4.1 创建 VPN 网关

操作场景

您需要将 VPC 中的弹性云主机和您的数据中心或私有网络连通，需要先创建 VPN 网关。购买 VPN 网关后，可以同时购买一条与其关联的 VPN 连接。

前置条件

- 请确认虚拟私有云 VPC 已经创建完成。
- 请确认虚拟私有云 VPC 的安全组规则已经配置，ECS 通信正常。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 网关”。
   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”。
3. 在“经典版-VPN 网关”界面，单击“创建 VPN 网关”。
4. 根据界面提示配置参数，并单击“立即购买”。VPN 网关参数请参见表 4-13

表4-13 经典版 VPN 网关参数说明

参数	说明	取值样例
计费模式	VPN 网关支持按需计费模式。	按需
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	-
名称	VPN 网关名称。	vpngw-001
虚拟私有云	VPN 接入的 VPC 名称。	vpc-001
类型	VPN 类型。默认为选择“IPsec”。	IPsec
带宽计费方式	带宽按需计费支持两种计费方式：按带宽计费/按流量计费。 • 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 • 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。	按流量计费
带宽大小	本地 VPN 网关的带宽大小（单位 Mbit/s），为所有基于该网关创建的 VPN 连接共享的带宽，VPN 连接带宽总和不超过 VPN 网关的带宽。	10

参数	说明	取值样例
描述	VPN 网关的描述信息。	-

5. 确认创建的 VPN 网关规格，单击“确认申请”。

   VPN 网关创建成功后，系统会分配一个公网出口 IP，即 VPN 网关列表中“网关 IP”对应显示的 IP 地址。该网关 IP 也是用户侧 VPN 网络配置对应的远端网关 IP。

4.4.2 查看已创建的 VPN 网关

操作场景

用户创建 VPN 网关后，可以查看已创建的 VPN 网关。

操作步骤

6. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
7. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 网关”。

   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”。
8. 在“经典版-VPN 网关”页面的 VPN 网关列表中可以查看 VPN 网关。

4.4.3 修改已创建的 VPN 网关

修改 VPN 网关基本信息

操作场景：

用户根据需要修改 VPN 网关名称和描述信息。

操作步骤：

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 网关”。

   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”。
3. 在“经典版-VPN 网关”界面目标 VPN 网关所在行，选择“更多 ＞ 修改基本信息”。
4. 根据界面参数，修改 VPN 网关的名称和描述信息。

   说明

   VPN 网关名称只能由中文、英文字母、数字、下划线、中划线、点组成。
5. 单击“确定”。

修改 VPN 网关带宽

操作场景：

当 VPN 网关带宽不能满足需求时，可修改 VPN 网关带宽。

操作步骤：

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 网关”。
   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”。
3. 在“VPN 网关”界面目标 VPN 网关所在行，单击“修改带宽”。
4. 根据界面参数，重新选择合适的带宽。
5. 单击“提交”。

说明

- 按需计费的网关支持增加或减小网关带宽值。

4.4.4 删除 VPN 网关

操作场景

当无需使用 VPN 网关时，可删除 VPN 网关。

已被 VPN 连接使用的 VPN 网关不可删除，请先删除相关的 VPN 连接，再删除 VPN 网关。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 网关”。
   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”。
3. 在“经典版-VPN 网关”界面所需删除的 VPN 网关所在行，选择“更多 ＞ 删除”。
4. 单击“是”，完成 VPN 网关删除。

4.5 经典版 VPN 连接管理

4.5.1 创建 VPN 连接

操作场景

您需要将 VPC 中的弹性云主机和您的数据中心或私有网络连通，创建 VPN 网关后需要创建 VPN 连接。

前置条件

- 请确认 VPN 网关已经创建完成。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 网关”。
   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”。
3. 在“经典版-VPN 连接”界面，单击“创建 VPN 连接”。
4. 根据界面提示配置参数，并单击“立即创建”。VPN 连接参数请参见表 4-14。

表4-14 经典版 VPN 连接参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	-
计费模式	VPN 连接支持按需计费。	按需计费
名称	VPN 连接名称。	vpn-001
VPN 网关	VPN 连接挂载的 VPN 网关名称。	vpcgw-001
本端子网	本端子网指需要通过 VPN 访问用户本地网络的 VPC 子网。支持以下方式设置本端子网： • 选择子网，表示用户数据中心或者私有网络与您选择的子网进行互通。 • 手动输入网段，表示用户数据中心或者私有网络与您配置的网段之间进行互通。	192.168.1.0/24， 192.168.2.0/24
远端网关	您的数据中心或私有网络中 VPN 的公网 IP 地址，用于与 VPC 内的 VPN 互通。	-
远端子网	远端子网指需要通过 VPN 访问 VPC 的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端 VPC 已有的对等连接网段、云专线的远端子网网段重复。	192.168.3.0/24， 192.168.4.0/24

参数	说明	取值样例
预共享密钥	配置在云上 VPN 连接的密钥，需要与本地网络 VPN 设备配置的密钥一致。此密钥用于 VPN 连接协商。 取值范围： • 取值长度：6~128 个字符。 • 只能包括以下几种字符： – 数字 – 大小写字母 – 特殊符号：包括“~”、“`”、“!”、“@”、“#”、“$”、“%”、“^”、“(”、“)”、“-”、“_”、“+”、“=”、“[”、“]”、“{”、“}”、“|”、"\"、","、"."、"/"、“:”和“;”	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	• 默认配置。 • 已有配置。 • 自定义配置：包含 IKE 策略和 IPsec 策略，用于指定 VPN 隧道加密算法。相关配置说明请参见表 4-15 和表 4-16。	自定义配置

表4-15 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： • MD5（此算法安全性较低，请慎用） • SHA1（此算法安全性较低，请慎用） • SHA2-256 • SHA2-384 • SHA2-512 默认配置为：SHA1。	SHA1

参数	说明	取值样例
加密算法	加密算法，支持的算法： • AES-128 • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
DH 算法	• Group 1（此算法安全性较低，请慎用） • Group 2（此算法安全性较低，请慎用） • Group 5（此算法安全性较低，请慎用） • Group 14 • Group 15 • Group 16 • Group 19 • Group 20 • Group 21	Group 5
版本	IKE 密钥交换协议版本，支持的版本： • v1（有安全风险不推荐） • v2	v1
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400
协商模式	默认配置为：Main。	Main

表4-16 IPsec 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： • SHA1（此算法安全性较低，请慎用） • MD5（此算法安全性较低，请慎用） • SHA2-256 • SHA2-384 • SHA2-512	SHA1
加密算法	加密算法，支持的算法： • AES-128 • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置 IPsec 隧道协商时使用。 • DH group 1（此算法安全性较低，请慎用） • DH group 2（此算法安全性较低，请慎用） • DH group 5（此算法安全性较低，请慎用） • DH group 14 • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21	DH group 5
传输协议	IPsec 传输和封装用户数据时使用的安全协议，目前支持的协议： • AH • ESP • AH-ESP 默认配置为：ESP。	ESP

参数	说明	取值样例
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：3600。	3600

说明

IKE 策略指定了 IPsec 隧道在协商阶段的加密和认证算法，IPsec 策略指定了 IPsec 在数据传输阶段所使用的协议，加密以及认证算法；这些参数在 VPC 上的 VPN 连接和您数据中心的 VPN 中需要进行相同的配置，否则会导致 VPN 无法建立连接。

以下算法安全性较低，请慎用：

- **认证算法**：SHA1、MD5。
- **加密算法**：3DES。
- **DH 算法**：Group 1、Group 2、Group 5。

5. 因为隧道的对称性，还需要在您自己数据中心的路由器或者防火墙上进行 IPsec VPN 隧道配置。

4.5.1 查看已创建的 VPN 连接

操作场景

用户创建 VPN 连接后，可以查看已创建的 VPN 连接。

操作步骤

6. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
7. 在左侧导航栏选择“虚拟专用网络> 经典版-VPN 连接”。

   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”，然后单击“VPN 连接”页签。
8. 在“经典版-VPN 连接”页面的 VPN 列表中，查看 VPN 连接信息，也可以在 VPN 连接所在行，单击“操作”列的“策略详情”，查看该 VPN 连接对应的 IKE 策略和 IPsec 策略详情。

4.5.2 修改已创建的 VPN 连接

操作场景

VPN 连接是建立 VPN 网关和外部数据中心 VPN 网关之间的加密通道。当 VPN 连接的网络参数变化时，可以修改 VPN 连接。

⚠ 注意

修改 VPN 连接高级配置时，有流量中断风险，请谨慎操作。

修改预共享密钥不会删除当前连接，新的预共享密钥在 IKE 生命周期到期后重协商时生效。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 连接”。
   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”，然后单击“VPN 连接”页签。
3. 在“经典版-VPN 连接”界面所需修改的 VPN 连接所在行，单击“修改”。
4. 根据界面提示配置参数。

说明

VPN 网关名称只能由中文、英文字母、数字、下划线、中划线、点组成。

5. 单击“确定”。

4.5.3 删除 VPN 连接

操作场景

当无需使用 VPN 网络、需要释放网络资源时，可删除 VPN 连接。

操作步骤

1. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
2. 在左侧导航栏选择“虚拟专用网络 ＞ 经典版-VPN 连接”。
   如果所在 region 已同步上线企业版 VPN，请选择“虚拟专用网络 ＞ 经典版”，然后单击“VPN 连接”页签。
3. 在“经典版-VPN 连接”界面所需删除的 VPN 连接所在行，选择“更多 ＞ 删除”。
4. 单击“是”，完成 VPN 连接删除。

4.6 监控

4.6.1 监控 VPN

监控是保持 VPN 可靠性、可用性和性能的重要部分，通过监控，用户可以观察 VPN 资源。为使用户更好地掌握自己的 VPN 运行状态，云平台提供了云监控服务。您可以

使用该服务监控您的 VPN，执行自动实时监控、告警和通知操作，帮助您更好地了解 VPN 的各项性能指标。

4.6.2 支持的监控指标（企业版 VPN）

功能说明

本节定义了虚拟专用网络服务上报云监控服务的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控服务提供的管理控制台检索 VPN 服务产生的监控指标和告警信息。

命名空间

SYS.VPN

监控指标

表4-17 企业版 VPN 网关支持的监控指标

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
gateway_send_pkt_rate	出云包速率	该指标用于统计测量对象平均每秒出云的数据包数量。	≥ 0 pps	网关	1 分钟
gateway_recv_pkt_rate	入云包速率	该指标用于统计测量对象平均每秒入云的数据包数量。	≥ 0 pps	网关	1 分钟
gateway_send_rate	出云带宽	该指标用于统计测量对象平均每秒出云流量。	0-1Gbit/s	网关	1 分钟
gateway_recv_rate	入云带宽	该指标用于统计测量对象平均每秒入云流量。	0-1Gbit/s	网关	1 分钟
gateway_send_rate_usage	出云带宽使用率	该指标用于统计测量对象出云带宽使用率。	0-100%	网关	1 分钟
gateway_recv_rate_usage	入云带宽使用率	该指标用于统计测量对象入云带宽使用率。	0-100%	网关	1 分钟
gateway_connection_num	连接数	该指标用于统计测量对象关联 VPN 连接数。	≥ 0	网关	1 分钟

表4-18 企业版 VPN 连接支持的监控指标

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
tunnel_average_latency	隧道往返平均时延	VPN 网关与对端网关之间隧道的往返平均时延。	0~5000 ms	VPN 连接	1 分钟
tunnel_max_latency	隧道往返最大时延	VPN 网关与对端网关之间隧道的往返最大时延。	0~5000 ms	VPN 连接	1 分钟
tunnel_packet_loss_rate	隧道丢包率	VPN 网关与对端网关之间隧道的丢包率。	0~100 %	VPN 连接	1 分钟
link_average_latency	链路往返平均时延	VPN 网关与对端网关之间链路的往返平均时延。	0~5000 ms	VPN 连接	1 分钟
link_max_latency	链路往返最大时延	VPN 网关与对端网关之间链路的往返最大时延。	0~5000 ms	VPN 连接	1 分钟
link_packet_loss_rate	链路丢包率	VPN 网关与对端网关之间链路的丢包率。	0~100 %	VPN 连接	1 分钟
connection_status	VPN 连接状态	展示 VPN 连接的通断状态。 0：未连接状态 1：连接状态 2：未知状态	0，1，2	VPN 连接	1 分钟
recv_pkt_rate	接收包速率	平均每秒接收的数据包数量。	≥ 0 pps	VPN 连接	1 分钟
send_pkt_rate	发送包速率	平均每秒发送的数据包数量。	≥ 0 pps	VPN 连接	1 分钟
recv_rate	接收速率	平均每秒接收流量。	0~1Gbit/s	VPN 连接	1 分钟
send_rate	发送速率	平均每秒发送流量。	0~1Gbit/s	VPN 连接	1 分钟
sa_send_pkt_rate	SA 发送包速率	平均每秒发送的数据包数量	≥ 0 pps	VPN 连接 SA	1 分钟
sa_recv_pkt_rate	SA 接收包速率	平均每秒接收的数据包数量	≥ 0 pps	VPN 连接 SA	1 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
sa_recv_rate	SA 接收速率	平均每秒接收流量	0~1Gbit/s	VPN 连接 SA	1 分钟
sa_send_rate	SA 发送速率	平均每秒发送流量	0~1Gbit/s	VPN 连接 SA	1 分钟

维度

key	Value
evpn_connection_id	企业版站点入云 VPN 连接
evpn_sa_id	企业版站点入云 VPN 连接 sa
evpn_gateway_id	企业版站点入云 VPN 网关

4.6.3 支持的监控指标（经典版 VPN）

功能说明

本节定义了虚拟专用网络服务上报云监控服务的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控服务提供的管理控制台检索 VPN 服务产生的监控指标和告警信息。

命名空间

SYS.VPN

监控指标

表4-19 经典版 VPN 网关支持的监控指标

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
upstream_bandwidth	出网带宽	该指标用于统计测试对象出云平台的网络速度（原指标为上行带宽）。 单位：比特/秒	≥ 0 bit/s	带宽或弹性公网 IP	1 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
downstream_bandwidth	入网带宽	该指标用于统计测试对象入云平台的网络速度（原指标为下行带宽）。 单位：比特/秒	≥ 0 bit/s	带宽或弹性公网 IP	1 分钟
upstream_bandwidth_usage	出网带宽使用率	该指标用于统计测量对象出云平台的带宽使用率，以百分比为单位。 出网带宽使用率=出网带宽指标/购买的带宽大小	0-100%	带宽或弹性公网 IP	1 分钟
downstream_bandwidth_usage	入网带宽使用率	该指标用于统计测量对象入云平台的带宽使用率，以百分比为单位。 入网带宽使用率=入网带宽指标/购买的带宽大小 说明 • 由于在部分站点对 10Mbps 以下的配置带宽提供 10Mbps 的入网带宽上限，此时监控的入网带宽使用率会存在大于 100%的情况。 • EIP 使用时修改带宽大小，带宽使用率的指标同步生效会有 5~10min 的延时。	0-100%	带宽或弹性公网 IP	1 分钟
up_stream	出网流量	该指标用于统计测试对象出云平台的网络流量（原指标为上行流量）。 单位：字节	≥ 0 bytes	带宽或弹性公网 IP	1 分钟
down_stream	入网流量	该指标用于统计测试对象入云平台的网络流量（原指标为下行流量）。 单位：字节	≥ 0 bytes	带宽或弹性公网 IP	1 分钟

表4-20 经典版 VPN 连接支持的监控指标

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
connection_status	VPN 连接状态	展示 VPN 连接的通断状态。 0：未连接状态 1：连接状态	0，1	VPN 连接	5 分钟

维度

key	Value
vpn_connection_id	VPN 连接

4.6.4 查看监控指标

操作场景

查看 VPN 连接状态、带宽、弹性公网 IP 的使用情况。

背景信息

表4-21 背景信息

监控指标名称	VPN 支持情况	是否默认开启
VPN 连接状态	企业版 VPN、经典版 VPN 均支持。	是
• 链路往返平均时延 • 链路往返最大时延 • 链路丢包率 • 接收包速率 • 发送包速率 • 接收速率 • 发送速率 • SA 接收包速率 • SA 发送包速率 • SA 接收速率 • SA 发送速率	仅企业版 VPN 支持。	否 单击 VPN 连接名称，在“基本信息”页签添加健康检查项。

监控指标名称	VPN 支持情况	是否默认开启
• 隧道往返平均时延 • 隧道往返最大时延 • 隧道丢包率	仅企业版 VPN 支持。	是 仅 VPN 连接使用静态路由模式，且开启 NQA 检测机制场景时支持私网相关监控指标。

查看 VPN 连接监控指标

- 通过 VPN 服务入口
  a. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
  b. 选择“虚拟专用网络 ＞ 企业版-VPN 连接”。
  c. 单击，查看 VPN 连接相关信息。
     仅支持查看 VPN 连接状态，如需查看更多监控指标，请通过云监控服务入口查看。
     支持查看“近 1 小时”、“近 3 小时”、“近 12 小时”、“近 24 小时”和“近 7 天”的数据。
- 通过云监控服务入口
  a. 登录管理控制台，单击“管理与部署 ＞ 云监控服务”。
  b. 选择“云服务监控 ＞ 虚拟专用网络”。
  c. 在“企业版站点入云 VPN 连接”页签下，单击“操作”列的“查看监控指标”，查看 VPN 连接状态。
     支持查看“近 1 小时”、“近 3 小时”、“近 12 小时”、“近 24 小时”和“近 7 天”的数据。

查看 VPN 网关监控指标

- 通过 VPN 服务入口（推荐）
  a. 登录管理控制台，单击“网络 ＞VPN”进入 VPN 控制台。
  b. 选择“虚拟专用网络 ＞ 企业版-VPN 网关”。
  c. 在“网关 IP”列下单击网关 IP 后的，查看 VPN 网关 IP 状态。
     支持查看“近 1 小时”、“近 3 小时”、“近 12 小时”、“近 24 小时”和自定义时间段的数据。
- 通过云监控服务入口
  a. 登录管理控制台，单击“管理与监管 ＞ 云监控服务”。
  b. 选择“云服务监控 ＞ 虚拟专用网络”。
  c. 在“企业版站点入云 VPN 网关”页签下，找到对应的 VPN 网关，单击“操作”列的“查看监控指标”，查看对应的 VPN 网关状态。
     支持查看“近 1 小时”、“近 3 小时”、“近 12 小时”、“近 24 小时”和“近 7 天”的数据。

4.6.5 创建告警规则

操作场景

通过设置告警规则，用户可自定义监控目标与通知策略，及时了解虚拟专用网络的状况，从而起到预警作用。

操作步骤

1. 登录管理控制台，单击“管理与监管 > 云监控服务”。
2. 选择“云服务监控 > 虚拟专用网络”，单击“创建告警规则”。

   VPN 告警规则请在“独享型 VPN 连接”页签配置。

   - VPN 默认不提供告警模板，请先创建自定义告警模板，然后重新在“云服务监控 > 虚拟专用网络”，单击“创建告警规则”进行告警规则配置。
3. 规则参数设置完成后，单击“立即创建”。

   虚拟专用网络告警规则设置完成后，当符合规则的告警产生时，系统会自动进行通知。

说明

更多关于虚拟专用网络监控规则的信息，请参见《云监控用户指南》。

4.7 审计

4.7.1 云审计服务支持的 VPN 操作列表

表4-22 企业版 VPN 操作列表

操作名称	资源类型	事件名称
创建用户对端网关	customer-gateway	createCgw
更新用户对端网关	customer-gateway	updateCgw
删除用户对端网关	customer-gateway	deleteCgw
创建虚拟专用网络网关	vpn-gateway	createVgw
更新虚拟专用网络网关	vpn-gateway	updateVgw
删除虚拟专用网络网关	vpn-gateway	deleteVgw
包周期创建 VPN 网关	vpn-gateway	CreatePrePaidVgw

操作名称	资源类型	事件名称
更新 VPN 网关状态	vpn-gateway	UpdateResourceState
创建虚拟专用网络连接	vpn-connection	createVpnConnection
更新虚拟专用网络连接	vpn-connection	updateVpnConnection
删除虚拟专用网络连接	vpn-connection	deleteVpnConnection
上传网关证书	vgw-certificate	createVgwCertificate
更换网关证书	vgw-certificate	updateVgwCertificate
创建资源标签	instance	createResourceTag
删除资源标签	instance	deleteResourceTag

4.7.2 查看云审计日志

用户进入贵州资源池云审计服务创建管理类追踪器后，系统开始记录 VPN 资源的操作。云审计服务管理控制台会保存最近 7 天的操作记录。

如何查看审计日志，请参考云审计服务用户指南。

----结束

5 故障排除

5.1 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。
- 安全组和客户设备侧 ACL 配置不正确。

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 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。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。

- 检查安全组和客户设备侧 ACL 配置
  - 确认 default 安全组已经放通客户设备侧公网 IP 的 UDP 协议端口 500 和 4500。

    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 UDP 协议端口 500 和 4500。

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

可能原因

- 安全组配置不正确
- 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

- 检查安全组配置
  - 确认 default 安全组已经放通去往对端子网数据流。

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 default 安全组已经放通来自对端子网数据流。
- 确认 default 安全组已经放通去往本端子网数据流。
- 确认 default 安全组已经放通来自本端子网数据流。
- 确认 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 > 弹性云主机”，单击“更多 > 安全组规则配置”查看。
- 确认 ECS 所在的安全组已经放通来自对端子网数据流。

- 检查客户设备侧放通策略
  - 确认客户设备侧已经放通去往 VPN 本端子网的数据流。
  - 确认客户设备侧已经放通来自 VPN 本端子网的数据流。

  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 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 VPN 本端子网，下一跳为设备出口地址。

    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。

5.3 流量丢包

故障现象

- 云下数据中心服务器对 VPC 上的 ECS 服务器执行 Ping 操作时，存在流量丢包。
- 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云侧。
  - 使用客户侧 VPN 网关地址 Ping 云侧 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。

- 检查云侧组网和带宽情况
  - 检查 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。

5.4 适用于经典版 VPN

5.4.1 常规检查项

用户在 VPN 产品使用过程中，通常会出现由于配置错误（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。

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 VPC 子网的数据流。
- 确认放行来自 VPC 子网的数据流。

检查防火墙路由表

确认存在目标地址为 VPC 子网的路由信息：

- 确认配置去往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 VPC 网段不一致，导致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。

5.4.2 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。

6 常见问题

6.1 热点问题

6.1.1 哪些设备可以与云进行 VPN 对接？

VPN 支持标准 IPsec 协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与云进行对接：

1. 设备是否具备 IPsec 功能和授权：请查询设备的特性列表获取是否支持 IPsec VPN。
2. 关于组网结构，要求用户侧数据中心有固定的公网 IP 或者经过 NAT 映射后的固定公网 IP（即 NAT 穿越，VPN 设备在 NAT 网关后部署）也可以。

说明

- 普通家庭宽带路由器、个人的移动终端设备、Windows 主机自带的 VPN 服务（如 L2TP）无法与云的 VPN 进行对接。
- 与云 VPN 服务做过对接测试厂商包括：
- 设备厂商：华为（防火墙/AR）、山石（防火墙），CheckPoint（防火墙）。
- 云服务厂商包括：阿里云，腾讯云，亚马逊（aws），微软（Microsoft Azure）。
- 软件厂商包括：strongSwan。
- IPsec 协议属于 IETF 标准协议，宣称支持该协议的厂商均可与云进行对接，用户不需要关注具体的设备型号。

  目前绝大多数企业级路由器和防火墙都支持该协议。
- 部分硬件厂商在特性规格列表中是宣称支持 IPsec VPN 的，但是需要专门购买软件 License 才能激活相关功能。

  请用户侧数据中心管理员根据设备具体型号与厂商进行确认。

6.1.2 VPN 协商参数有哪些？默认值是什么？

表6-1 VPN 协商参数

协议	配置项	值
IKE	认证算法	• MD5（此算法安全性较低，请慎用） • SHA1（此算法安全性较低，请慎用） • SHA2-256（默认） • SHA2-384 • SHA2-512
	加密算法	• 3DES（此算法安全性较低，请慎用） • AES-128（默认） • AES-192 • AES-256 • AES-256-GCM-16
	DH 算法	• Group 1（此算法安全性较低，请慎用） • Group 2（此算法安全性较低，请慎用） • Group 5（此算法安全性较低，请慎用） • Group 14（此算法安全性较低，请慎用） • Group 15（默认） • Group 16 • Group 19 • Group 20 • Group 21
	版本	• v1（有安全风险不推荐） • v2（默认）
	生命周期	86400（默认） 单位：秒。 取值范围：60-604800。
	本端标识	• IP Address 本端 IP 地址由系统自动关联显示，无需用户手动配置。 • FQDN 默认的本端标识类型是 IP Address，ID 值是 VPN 网关的公网 IP。

协议	配置项	值
	对端标识	• IP Address • FQDN 默认的对端标识类型是 IP Address，ID 值是对端网关的公网 IP。
IPsec	认证算法	• SHA1（此算法安全性较低，请慎用） • MD5（此算法安全性较低，请慎用） • SHA2-256（默认） • SHA2-384 • SHA2-512
	加密算法	• AES-128（默认） • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用） • AES-256-GCM-16
	PFS	• Disable（此算法安全性较低，请慎用） • DH group 1（此算法安全性较低，请慎用） • DH group 2（此算法安全性较低，请慎用） • DH group 5（此算法安全性较低，请慎用） • DH group 14（此算法安全性较低，请慎用） • DH group 15（默认） • DH group 16 • DH group 19 • DH group 20 • DH group 21
	传输协议	• ESP（默认）
	生命周期	3600（默认） 单位：秒。 取值范围：30-604800。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。

IKE 协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致 IPsec VPN 受到侵犯。为提升密钥管理的安全性，IKE 提供了 PFS（完美向前保密）功能。启用 PFS 后，在进行 IPsec SA 协商时会进行一次附加的 DH 交换，重新生成新的 IPsec SA 密钥，提高了 IPsec SA 的安全性。

- 为了增强安全性，默认开启 PFS，请确认用户侧数据中心网关设备也开启了该功能，且两端配置保持一致，否则会导致协商失败。
- IPsec SA 字节生命周期，不是 VPN 服务可配置参数，云侧采用的是默认配置 1843200KB。该参数不是协商参数，不影响双方建立 IPsec SA。

6.1.3 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联？

可以。

VPN 连通的是两个子网，即云上 VPC 网络与用户数据中心网络。

VPN 成功建立后，两个子网间可以运行任何类型的业务流量，此时应用服务器访问数据库业务在逻辑上和访问同一局域网的其它主机是相同的，因此该方案可行的。

这种场景是 IPsec VPN 的典型场景，请用户放心使用。

同时 VPN 连通以后，并不限定业务的发起方是云上还是用户侧数据中心，即用户可以从云上向用户侧数据中心发起业务，也可以反向。

须知

- 用户在打通 VPN 以后，需要关注网络延迟和丢包情况，避免影响业务正常运行。
- 建议用户先运行 ping，获取网络的丢包和时延情况。

6.1.4 是否可以通过 VPN 实现跨境访问网站？

不可以。

VPN 实现的是将云上的 VPC 子网和用户侧数据中心的 IDC 网络打通的场景，即站点与站点互通（site to site）。

6.1.5 VPN 连接是什么？用户在购买 VPN 网关时如何选择 VPN 连接数？

VPN 连接，指一个 VPN 网关与用户侧一个独立的公网 IP 之间建立的 IPsec 连接，一个连接中可以配置多个本端子网（vpc 中的子网）和对端子网（用户侧子网）， 无需配置多个连接。

拟创建 VPN 连接的数量通常与用户数据中心数量有关，每条 VPN 连接可打通当前 VPC 与云下的一个数据中心网络。

说明

当云侧的网段 a1、a2 与用户侧网段 b1、b2 分别通信时，仅需创建一条 VPN 连接并指定云侧多个源网段和多个地址网段即可。

6.1.6 VPN 连接中断后会通知我吗？

VPN 连接的状态监控功能已上线，VPN 连接创建后即会向云监控服务 CES 上报状态信息，但是并不会自动向用户发送告警通知，需要在服务列表中选择“管理与监管 > 云监控”创建告警规则。

VPN 连接状态请在 VPN 连接“监控”列中单击 进行查看。

6.1.7 建立 IPsec VPN 连接需要账户名和密码吗？

常见的使用账户名和密码进行认证的 VPN 有 SSL VPN、PPTP 或 L2TP，云的 IPsec VPN 使用预共享密钥方式进行认证，密钥配置在 VPN 网关上，在 VPN 协商完成后即建立通道，VPN 网关所保护的主机在进行通信时无需输入账户名和密码。

说明

IPsec XAUTH 技术是 IPsec VPN 的扩展技术，它在 VPN 协商过程中可以强制接入用户输入账户名和密码。

目前 VPN 不支持该扩展技术。

6.1.8 IPsec VPN 是否会自动建立连接？

支持自动建立连接。

6.1.9 VPN 网关删除后公网地址是否可以保留？

按需 VPN 网关如果绑定了按需 EIP，则 VPN 网关删除后会同步删除绑定的按需 EIP。

如果需要保留 EIP，请在删除 VPN 网关前对 EIP 进行解绑操作。

6.1.10 VPN 监控可以监控哪些内容？

VPN 网关

可以监控网关 IP 的带宽信息，包含入网流量、入网带宽、出网流量、出网带宽及出网带宽使用率。

查询 VPN 网关监控状态，请在 VPN 网关“网关 IP”列中单击 EIP 后面的 进行查看。

VPN 连接

可以监控连接的状态信息，包括 VPN 连接状态、链路往返平均时延、链路往返最大时延、链路丢包率、隧道往返平均时延、隧道往返最大时延、隧道丢包率。

其中，链路往返平均时延、链路往返最大时延、链路丢包率、隧道往返平均时延、隧道往返最大时延、隧道丢包率需要单击 VPN 连接，在“基本信息”页签通过添加健康检查项进行添加；私网相关指标仅 VPN 连接使用静态路由模式，且开启 NQA 检测机制场景下支持配置。

查询 VPN 连接监控状态，请在 VPN 连接“监控”列中单击 进行查看。

6.1.11 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？

云上用户购买的 VPN 网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下：

- 如果所购买的带宽<=10Mbit，则入云方向统一限定为 10Mbit。
- 如果所购买的带宽>10Mbit，则入云方向与购买的带宽一致。

按带宽计费度量采用国际统一的带宽单位 Mbit，按流量计费的度量单位为 GByte。

6.1.12 如何测试 VPN 速率情况？

假设测试环境 VPN 连接已经创建，在 VPN 连接两端 VPC 的本端子网下分别创建 ECS，并使两个 VPC 之间的 ECS 相互能够 ping 通的情况下，测试 VPN 的速率情况。

当用户购买的 VPN 网关的带宽为 200Mbit/s 时，测试情况如下。

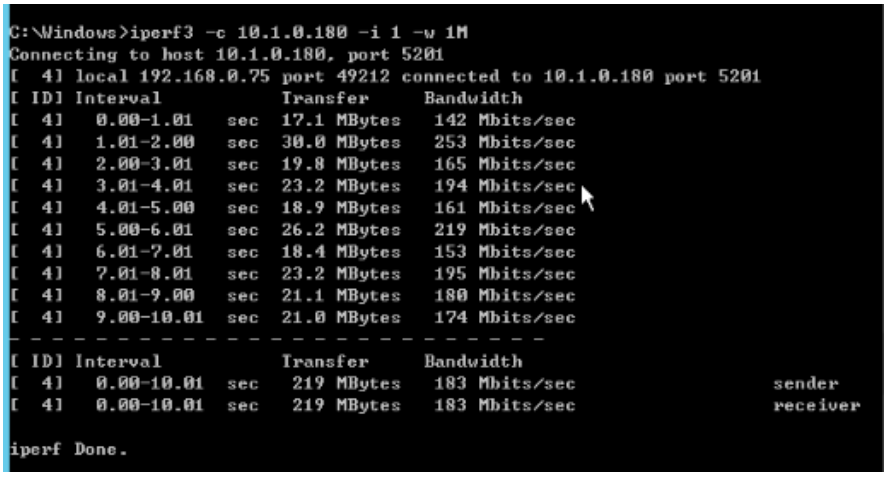
1. 互为对端的 ECS 都使用 Windows 系统，测试速率可达 180Mbit/s，使用 iperf3 和 filezilla（是一款支持 ftp 的文件传输工具）测试均满足带宽要求。

   说明

   基于 TCP 的 FTP 协议有拥塞控制机制，180Mbit/s 为平均速率，且 IPsec 协议会增加新的 IP 头，因此 10%左右的速率误差在网络领域是正常现象。

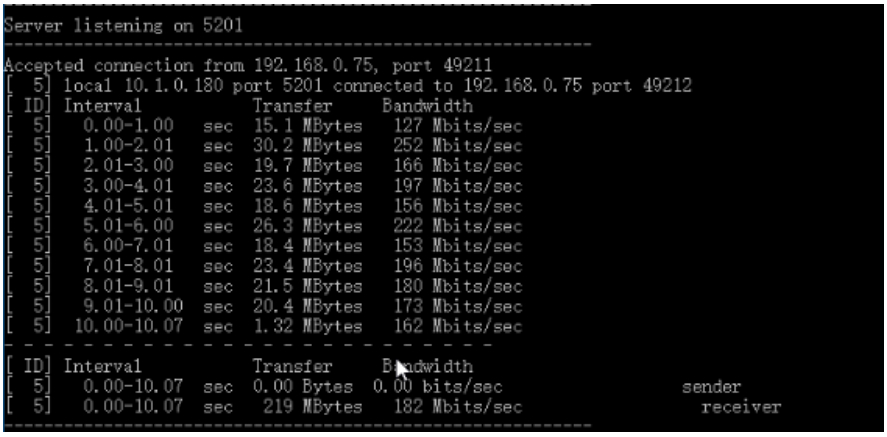
   使用 iperf3 客户端测试结果截图如图 6-1 所示。

图6-1 200M 带宽客户端 iperf3 测试结果



使用 iperf3 服务器端测试结果截图如图 6-2 所示。

图6-2 200M 带宽服务端 iperf3 测试结果

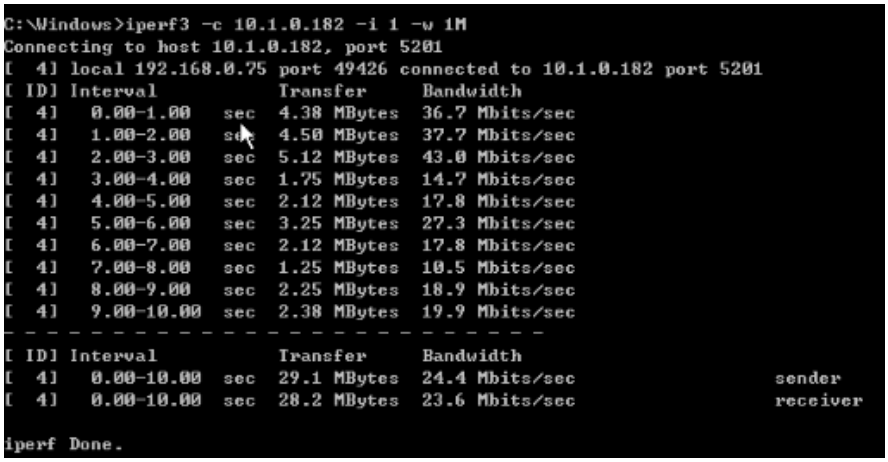


2. 互为对端的 ECS 都使用 Centos7 系统，测试速率可达 180M，使用 iperf3 测试满足带宽要求。
3. 服务器端 ECS 使用 Centos7 系统，客户端使用 Windows 系统，测试速率只有 20M 左右，使用 iperf3 和 filezilla 测试均不能满足带宽要求。

   原因在于 Windows 和 Linux 对 TCP 的实现不一致，导致速率慢。所以对端 ECS 使用不同的系统时，无法满足带宽要求。

   使用 iperf3 测试结果截图如图 6-3 所示。

图6-3 互为对端的 ECS 系统不同时 iperf3 测试结果



用户购买的 VPN 网关为网关的整体吞吐能力，即该 VPN 网关下所有 VPN 连接的带宽之和。在大带宽场景下，由于主机的转发性能限制，需要使用多台主机构建多条流量才能充分利用网关的带宽。这种场景下对 ECS 的配置要求也很高，建议 ECS 的网卡支持 2G 以上的带宽。

测试总结：综上测试结果，云网关能够满足带宽速率要求，但是建议两端主机使用相同的操作系统，并且网卡要达到配置要求。

6.1.13 VPC、VPN 网关、VPN 连接之间有什么关系？

- VPC，即云上私有专用网络，同一 Region 中可以创建多个 VPC，且 VPC 之间相互隔离。一个 VPC 内可以划分多个子网网段。
- VPN 网关，基于 VPC 创建，是 VPN 连接的接入点。一个 VPC 下支持购买多个 VPN 网关，每个网关可以创建多个 VPN 连接。
- VPN 连接，基于 VPN 网关创建，用于连通 VPC 子网和用户数据中心（或其它 Region 的 VPC）子网，即每个 VPN 连接连通了一个用户侧数据中心的网关。

说明

VPN 连接的数量与 VPN 连接的本端子网和远端子网的数量无关，仅与用户 VPC 需要连通的用户数据中心（或其它 Region 的 VPC）的数量有关，已创建的 VPN 连接的数量即 VPN 连接列表中展示的数量（一个条目即一个 VPN 连接），也可以在 VPN 网关中查看当前网关已创建的 VPN 连接数量。

6.1.14 如何理解 VPN 连接中的对端网关和对端子网？

对端网关和对端子网是个相对的概念，在建立 VPN 连接时，从云的角度出发，VPC 网络就是本地子网，创建的 VPN 网关就是本地网关，与之对接的用户侧网络就是对端子网， 用户侧的网关就是对端网关。

对端网关 IP 就是用户侧网关的公网 IP，对端子网指需要和 VPC 子网互联的子网。

6.1.15 连接云下的多台服务器需要购买几个连接？

云的 VPN 属于 IPsec VPN，它是用于打通云上 VPC 和用户侧数据中心子网的 VPN，所以购买 VPN 连接的个数与服务器的数量无关，而与这些服务器所在的数据中心数量有关。

一个 VPN 网关支持绑定两个 EIP 和用户侧网关进行通信：

- 如果用户侧数据中心只有一个公网出口网关，所有服务器（或用户主机）都通过该网关连接至 Internet：这种情况需要配置一个 VPN 连接组，即 VPN 网关的两个 EIP 分别配置一条 VPN 连接和用户侧出口网关通信。
- 如果用户侧数据中心只有两个公网出口网关，所有服务器（或用户主机）通过两个网关连接至 Internet：这种情况需要配置两个 VPN 连接组，即 VPN 网关的两个 EIP 分别配置一条 VPN 连接和两个用户侧出口网关通信。

6.1.16 VPN 支持将两个 VPC 互连吗？

- 如果两个 VPC 位于同一区域内，不支持 VPN 互连，推荐使用 VPC 对等连接互连。
- 如果两个 VPC 位于不同区域，支持 VPN 互连，具体操作如下：
  a. 为这两个 VPC 分别创建 VPN 网关，并为两个 VPN 网关创建 VPN 连接。
  b. 将两个 VPN 连接的对端网关设置为对方 VPN 网关的网关 EIP。
  c. 将两个 VPN 连接的远端子网设置为对方 VPC 的网段。
  d. 两个 VPN 连接的预共享密钥和算法参数需保持一致。

6.1.17 使用 VPN 会对本地网络造成哪些影响，访问云端主机在路由上会有哪些变化？

配置 VPN 时，用户需要在用户侧数据中心的网关上增加以下 VPN 配置信息：

- IKE/IPsec 策略配置。
- 配置 VPN 连接模式为路由模式或策略模式。
- 用户需要审视用户侧数据中心网关的路由配置，确保发往 VPC 的流量被路由到正确的出接口（即绑定 IPsec 策略的接口）。

6.1.18 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置？

可以。

6.1.19 如何防止 VPN 连接出现中断情况？

VPN 连接在正常的使用过程中会存在重协商情况，触发重协商的条件有 IPsec SA 的生命周期即将到期和 VPN 传输的流量超过 20GB，重协商一般不造成连接中断。

大多数的连接中断都是因为两端的配置信息错误造成的，或公网异常导致重协商失败造成的。

常见的连接中断原因有：

- 两端的 ACL 不匹配；
- SA 生命周期不匹配；
- 用户侧数据中心未配置 DPD；
- VPN 使用过程中修改了配置信息；
- 运营商网络抖动。

因此请在配置 VPN 时确保操作和配置，以进行连接状态保活：

- 两端的子网配置互为镜像；
- SA 生命周期信息一致；
- 用户侧数据中心网关开启 DPD 配置，探测次数不少于 3 次；
- 连接过程中修改参数两侧同步修改；
- 设置用户侧数据中心设备 TCP MAX-MSS 为 1300；
- 确保用户侧数据中心出口有足够的带宽可被 VPN 使用；
- 确认 VPN 连接可被两端触发协商，开启用户侧数据中心设备的主动协商配置；

6.1.20 如何解决 VPN 连接无法建立连接问题？

1. 登录控制台，进入“虚拟专用网络 > 企业版-VPN 连接”页面。
2. 在 VPN 连接列表中，单击目标 VPN 连接“操作”列的“修改策略配置”，查看该 VPN 连接对应的 IKE 策略和 IPsec 策略详情。
3. 检查云上 VPN 连接中的 IKE 策略和 IPsec 策略中的协商模式和加密算法是否与远端配置一致。

   如果第一阶段 IKE SA 已经建立，第二阶段 IPsec SA 未建立，常见情况为 IPsec 策略与数据中心远端的配置不一致。
4. 检查 ACL 是否配置正确。

   假设您的数据中心的子网为 192.168.3.0/24 和 192.168.4.0/24，VPC 下的子网为 192.168.1.0/24 和 192.168.2.0/24，则你在数据中心或局域网中的 ACL 应对你的每一个数据中心子网配置允许 VPC 下的子网通信的规则，如下例：

   ```
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   ```
5. 配置完成后检查 VPN 是否连接，从两侧测试 ping 是否正常。

6.1.21 EIP 能作为 VPN 的网关 IP 吗？

企业版 VPN 可以。

用户可以在创建 VPN 网关时绑定 EIP 作为网关 IP。

6.1.22 VPN 配置完成了，为什么连接一直处于未连接状态？

可能存在信息配置错误，请从以下方面进行排查：

1. 确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/对端子网、本端网关/对端网关互为镜像。
2. 确认用户侧数据中心设备的路由、NAT 和安全策略配置无误。

6.1.23 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置？

VPN 连接的“连接模式”选择“策略模式”时，才需要在控制台上配置策略规则 ACL。

6.2 组网与使用场景

6.2.1 是否可以通过 VPN 实现跨境访问网站？

不可以。

VPN 实现的是将云上的 VPC 子网和用户侧数据中心的 IDC 网络打通的场景，即站点与站点互通（site to site）。

6.2.2 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联？

可以。

VPN 连通的是两个子网，即云上 VPC 网络与用户数据中心网络。

VPN 成功建立后，两个子网间可以运行任何类型的业务流量，此时应用服务器访问数据库业务在逻辑上和访问同一局域网的其它主机是相同的，因此该方案可行的。

这种场景是 IPsec VPN 的典型场景，请用户放心使用。

同时 VPN 连通以后，并不限定业务的发起方是云上还是用户侧数据中心，即用户可以从云上向用户侧数据中心发起业务，也可以反向。

须知

- 用户在打通 VPN 以后，需要关注网络延迟和丢包情况，避免影响业务正常运行。
- 建议用户先运行 ping，获取网络的丢包和时延情况。

6.2.3 连接云下的多台服务器需要购买几个连接？

VPN 属于 IPsec VPN，它是用于打通云上 VPC 和用户侧数据中心子网的 VPN，所以购买 VPN 连接的个数与服务器的数量无关，而与这些服务器所在的数据中心数量有关。

一个 VPN 网关支持绑定两个 EIP 和用户侧网关进行通信：

- 如果用户侧数据中心只有一个公网出口网关，所有服务器（或用户主机）都通过该网关连接至 Internet：这种情况需要配置一个 VPN 连接组，即 VPN 网关的两个 EIP 分别配置一条 VPN 连接和用户侧出口网关通信。
- 如果用户侧数据中心只有两个公网出口网关，所有服务器（或用户主机）通过两个网关连接至 Internet：这种情况需要配置两个 VPN 连接组，即 VPN 网关的两个 EIP 分别配置一条 VPN 连接和两个用户侧出口网关通信。

6.2.4 VPN 支持将两个 VPC 互连吗？

- 如果两个 VPC 位于同一区域内，不支持 VPN 互连，推荐使用 VPC 对等连接互连。
- 如果两个 VPC 位于不同区域，支持 VPN 互连，具体操作如下：
  a. 为这两个 VPC 分别创建 VPN 网关，并为两个 VPN 网关创建 VPN 连接。
  b. 将两个 VPN 连接的对端网关设置为对方 VPN 网关的网关 EIP。
  c. 将两个 VPN 连接的远端子网设置为对方 VPC 的网段。

6.2.5 使用 VPN 会对本地网络造成哪些影响，访问云端主机在路由上会有哪些变化？

配置 VPN 时，用户需要在用户侧数据中心的网关上增加以下 VPN 配置信息：

- IKE/IPsec 策略配置。
- 配置 VPN 连接模式为路由模式或策略模式。
- 用户需要审视用户侧数据中心网关的路由配置，确保发往 VPC 的流量被路由到正确的出接口（即绑定 IPsec 策略的接口）。

6.2.6 通过 VPN 来实现云下 IDC 与云端 VPC 的互通，两端分别需要做哪些配置？

VPN 对接的工作分为两个部分：云上创建 VPN 和用户侧数据中心配置 VPN 设备。

- 云上创建 VPN
  - 购买 VPN 网关，配置计费模式、带宽大小和对接的 VPC 等信息。
  - 配置对端网关，配置路由模式等信息。
  - 配置 VPN 连接，配置两端网关 IP，两端子网和协商策略等信息。
- 用户侧数据中心配置 VPN 设备
  a. 配置用户侧数据中心公网 IP，在支持 IPsec VPN 的设备上完成 IPsec 协商的一、二阶段配置。
  b. 进行网络路由、NAT 和安全策略配置。

6.2.7 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置？

可以。

6.2.8 同一个 Region 的两个 VPC 可以通过 VPN 连通吗？

不可以。

对于同 Region 的两个 VPC，您可以通过对等连接（VPC peering）打通两个 VPC。

6.2.9 可以通过哪些方式连通同一个 Region 的两个 VPC？

可通过创建对等连接的方式打通同 Region 的两个 VPC，对等连接可连通同 Region 的 VPC。

6.2.10 云端创建了两个 VPC，如何与云下的 IDC 网络互通？

配置步骤

1. 确认云上的两个 VPC 是否在同一 Region。如果在同一 Region 可通过对等连接将两个 VPC 连接起来（对等连接免费）。
2. 用户侧数据中心 IDC 与其中一个 VPC 建立 VPN 连接。

   修改用户侧数据中心设备的远端子网为云上两个 VPC 子网，VPN 对接的 VPC1 本端子网需要包含通过对等连接的子网，对等连接的子网路由包含用户侧数据中心 IDC 子网。

6.2.11 云端两个 Region，每 Region 有两个子网，是否可以创建两个 VPN 连接，分别连通不同子网？

不可以。

两个 Region 间只需创建一个 VPN 连接即可，在 VPN 连接中将两个子网都加入到 VPN 中。

针对这种场景，如果用户试图去创建第二条 VPN 连接，由于两个连接的对端网关地址一样，因此管理控制台界面会提示冲突。

6.2.12 VPN 和 OBS 可以直接通信吗？

可以。

1. 用户站点通过 VPN 访问 OBS 服务，需要使用 VPC 终端节点服务。需要为内网 DNS 和 OBS 分别申请两个终端节点。
2. 在用户侧配置云的内网 DNS 和路由

6.2.13 用户本地电脑如何连接云上 VPN？

普通家庭宽带路由器、个人的移动终端设备、Windows 主机自带的 VPN 服务（如 L2TP）无法与云的 VPN 进行对接。

与云下对接需要对端有支持标准 IPsec 协议的设备。

6.2.14 公司网络已通过 VPN 连通了云，我如何在家访问云 ECS？

VPN 为 IPsec VPN，是连接云上 VPC 和云下局域网的；家庭网络非公司局域网络的组成部分，无法直接和云上 VPC 实现互联。

居家办公主机需要访问云上 VPC 资源可以考虑直接访问服务对应的 EIP，或通过 SSL VPN（需公司支持 SSL 接入）先连接至公司局域网，然后通过公司局域网访问云上 VPC 资源。

6.2.15 购买 VPN 网关和连接后，发现云下没有支持 IPsec 的设备，如何临时建立 VPN 连接？

与云进行 VPN 连通时，需要云下有支持标准的 IPsec 设备和固定公网 IP，二者缺一不可。

如果需要临时与云对接，可通过在主机上安装第三方软件完成与云的对接。

6.2.16 如何选择在云上的哪个区域创建 VPN 网关？

在云上创建 VPN 网关，您可用选择任一区域的 VPC 进行创建。

推荐您选择与 IDC 同城的区域创建 VPN 网关，这样可以更大程度降低因公网质量对 VPN 的影响。

同区域的多个 VPC，可以通过 VPN+DC 的方式进行打通。

6.3 产品与使用

6.3.1 VPC、VPN 网关、VPN 连接之间有什么关系？

- VPC，即云上私有专用网络，同一 Region 中可以创建多个 VPC，且 VPC 之间相互隔离。一个 VPC 内可以划分多个子网网段。
- VPN 网关，基于 VPC 创建，是 VPN 连接的接入点。一个 VPC 下支持购买多个 VPN 网关，每个网关可以创建多个 VPN 连接。
- VPN 连接，基于 VPN 网关创建，用于连通 VPC 子网和用户数据中心（或其它 Region 的 VPC）子网，即每个 VPN 连接连通了一个用户侧数据中心的网关。

说明

VPN 连接的数量与 VPN 连接的本端子网和远端子网的数量无关，仅与用户 VPC 需要连通的用户数据中心（或其它 Region 的 VPC）的数量有关，已创建的 VPN 连接的数量即 VPN 连接列表中展示的数量（一个条目即一个 VPN 连接），也可以在 VPN 网关中查看当前网关已创建的 VPN 连接数量。

6.3.2 VPN 配置下发后，多久能够生效？

用户在管理控制台完成 VPN 资源创建后，配置 1-5 分钟下发完成，下发后立即生效。

说明

VPN 配置下发成功后，并不表示 VPN 连接已经建立成功，用户还需要对用户侧网关设备进行配置，完成与 VPN 网关的隧道协商。

6.3.3 VPN 配置完成了，为什么连接一直处于未连接状态？

可能存在信息配置错误，请从以下方面进行排查：

1. 确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/对端子网、本端网关/对端网关互为镜像。
2. 确认用户侧数据中心设备的路由、NAT 和安全策略配置无误。

6.3.4 VPN 网关删除后公网地址是否可以保留？

按需 VPN 网关如果绑定了按需 EIP，则 VPN 网关删除后会同步删除绑定的按需 EIP。

如果需要保留 EIP，请在删除 VPN 网关前对 EIP 进行解绑操作。

6.3.5 已经创建的 VPN 哪些信息可以修改，哪些信息不可以修改？

- VPN 网关
  - 可以修改的信息
    - ✓ 名称
    - ✓ 本端子网
    - ✓ 主备 EIP
      - 可以通过先解绑 EIP，然后绑定 EIP 的方式对主备 EIP 进行修改。

        如果 EIP 已经创建了 VPN 连接，则无法解绑。
      - EIP 的名称、公网 IP 类型、带宽大小等属性修改。
  - 不可以修改的信息
    - ✓ 区域
    - ✓ 关联模式
    - ✓ 虚拟私有云
    - ✓ 互联子网
    - ✓ BGP ASN
    - ✓ 计费模式，包括包年/包月和按需计费
    - ✓ 规格
    - ✓ 可用区
    - ✓ VPN 连接组数（仅“计费模式”为“包年/包月”时需要设置）
- 对端网关

- 可以修改的信息
  - ✓ 名称
- 不可以修改的信息
  - ✓ 路由模式
  - ✓ BGP ASN（仅“路由模式”选择“动态 BGP”时需要设置）
  - ✓ 公网 IP

⑩ VPN 连接

- 可以修改的信息
  - ✓ 名称
  - ✓ 本端接口地址
  - ✓ 对端网关
  - ✓ 对端子网
  - ✓ 策略配置，包括 IKE 策略和 IPsec 策略
  - ✓ 预共享密钥
- 不可以修改的信息
  - ✓ VPN 网关
  - ✓ 公网 IP
  - ✓ 连接模式，包括路由模式和策略模式
  - ✓ 路由模式，包括静态路由和 BGP（仅“连接模式”选择“路由模式”时需要设置）
  - ✓ 检测机制（仅“连接模式”选择“路由模式”时需要设置）
  - ✓ 策略规则，包括源网段和目的网段（仅“连接模式”选择“策略模式”时需要设置）

6.3.6 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置？

VPN 连接的“连接模式”选择“策略模式”时，才需要在控制台上配置策略规则 ACL。

6.3.7 创建 VPN 连接时添加对端子网，提示系统异常，如何处理？

检查 VPC 内是否存在对等连接、云专线的子网路由使用了该子网，导致 VPN 下发子网路由冲突，确认后将其配置的子网路由删除后重新创建即可。

6.3.8 Console 界面在哪添加 VPN 远端路由？

云端在 VPN 连接创建时会自动下发远端子网路由，无需手动配置。

6.3.9 如何理解 VPN 连接中的对端网关和对端子网？

对端网关和对端子网是两个相对的概念，在建立 VPN 连接时，从云的角度出发，VPC 网络就是本地子网，创建的 VPN 网关就是本地网关，与之对接的用户侧网络就是对端子网，用户侧的网关就是对端网关。

对端网关 IP 就是用户侧网关的公网 IP，对端子网指需要和 VPC 子网互联的子网。

6.3.10 创建 VPN 连接时如何关闭 PFS？

- 云

  请在 VPN 连接配置参数中，将 IPsec 策略中 PFS 的选项选择为 Disable。云默认开启 PFS。
- 用户数据中心对端网关

  部分设备厂商默认关闭了 PFS 功能，请查询设备对应用户手册进行操作。

说明

配置过程中，请确认云和对端网关侧 PFS 配置一致，否则会导致协商失败。

为了增强安全性，建议云和对端网关侧均开启 PFS。

6.3.11 VPN 本端子网和对端子网的数量有限制吗？

- 每 VPN 网关配置的本地子网数量：50
- 每 VPN 连接支持配置的对端子网个数：50

6.3.12 配置 VPN 连接的本端子网和对端子网时需要注意什么？

- 子网数量满足规格限制，数量超出规格限制请进行聚合汇总。
  - 每 VPN 网关配置的本地子网数量：50
  - 每 VPN 连接支持配置的对端子网个数：50
- 本端子网不可以包含远端子网，远端子网可以包含本端子网。
- 推荐配置的本端子网在 VPC 内有路由可达。
- 同一个 VPN 网关创建两条连接：若这两条连接的远端子网存在包含关系，在访问的目的网络处于交集网段部分时，按照创建连接的先后顺序匹配 VPN 连接，且与连接状态无关（策略模式不能按照掩码长度进行匹配）。

6.3.13 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接？

VPN 连接状态刷新存在一定的延迟，业务已通但是网页上 VPN 连接状态还是未连接是正常现象。

如果数据面已正常（即业务访问已正常）， 连接就已经完成建立了，短暂等待后 VPN 连接状态就会更新为“已连接”。

6.3.14 修改协商策略后，页面显示资源不存在，如何处理？

此问题为页面刷新周期问题。

在修改连接高级策略时，系统会先删除，再重建 VPN 连接，如果在页面创建过程中出现短暂的删除中或创建中属于正常现象，切勿重复创建同一连接（本端子网、对端子网、对端网关相同的连接）；

如果页面长时间停留在删除或创建中，请提交工单解决。

6.3.15 VPN 网关最大支持多大带宽？

VPN 网关规格最大支持 1Gbit/s。

6.3.16 创建 VPN 连接时如何选择 IKE 的版本？

推荐您选择 IKEv2 进行协商，其原因是 IKEv1 的版本存在一定的安全风险，且 IKEv2 在连接的协商建立过程，认证方法支持，DPD 超时处理，SA 超时处理上都优于 IKEv1。

云将大力推进 IKEv2 的使用，逐步停用 IKEv1 协商策略。

IKEv1 与 IKEv2 的协议介绍

- IKEv1 协议是一个混合型协议，其自身的复杂性不可避免地带来一些安全及性能上的缺陷，已经成为目前实现的 IPsec 系统的瓶颈。
- IKEv2 协议保留了 IKEv1 的基本功能，并针对 IKEv1 研究过程中发现的问题进行修正，同时兼顾简洁性、高效性、安全性和健壮性的需要，整合了 IKEv1 的相关文档，由 RFC4306 单个文档替代。通过核心功能和默认密码算法的最小化规定，新协议极大地提高了不同 IPsec VPN 系统的互操作性。

IKEv1 存在的安全风险

- IKEv1 支持的密码算法已超过 10 年未做更新，并不支持诸如 AES-GCM、ChaCha20-Poly1305 等推荐的强密码算法。IKEv1 使用 ISALMP 头的 E 比特位来指定该头后跟随的是加密载荷，但是这些加密载荷的数据完整性校验值放在单独的 hash 载荷中。这种加密和完整性校验的分离阻碍了 v1 使用认证加密（AES-GCM），从而限制了只能使用初期定义的 AES 算法。
- 协议本身也无法防止报文放大攻击（属于 DOS 攻击）初始报文交换，IKEv1 容易被半连接攻击，响应方响应初始化报文后维护发起-响应的关系，维护了大量的关系会消耗大量的系统资源。

  针对连接的 DOS 攻击，IKEv2 协议上有针对性的解决方案。
- IKEv1 野蛮模式安全性低：野蛮模式开始信息报文不加密，存在用户配置信息泄漏的风险，当前也存在针对野蛮攻击，如：中间人攻击。

IKEv1 和 IKEv2 的区别

- **协商过程不同。**
  - IKEv1 协商安全联盟主要分为两个阶段，其协议相对复杂、带宽占用较多。IKEv1 阶段 1 的目的是建立 IKE SA，它支持两种协商模式：主模式和野蛮模式。主模式用 6 条 ISAKMP 消息完成协商。野蛮模式用 3 条 ISAKMP 消息完成协商。野蛮模式的优点是建立 IKE SA 的速度较快。但是由于野蛮模式密钥交换与身份认证一起进行无法提供身份保护。IKEv1 阶段 2 的目的就是建立用来传输数据的 IPsec SA，通过快速交换模式（3 条 ISAKMP 消息）完成协商。
  - IKEv2 简化了安全联盟的协商过程。IKEv2 正常情况使用 2 次交换共 4 条消息就可以完成一个 IKE SA 和一对 IPsec SA，如果要求建立的 IPsec SA 大于一对时，每一对 SA 只需额外增加 1 次交换，也就是 2 条消息就可以完成。

  说明

  IKEv1 协商，主模式需要 6+3，共 9 个报文；野蛮模式需要 3+3，共 6 个报文。IKEv2 协商，只需要 2+2，共 4 个报文。

- **认证方法不同。**
  - 数字信封认证（hss-de）仅 IKEv1 支持（需要安装加密卡），IKEv2 不支持。
  - IKEv2 支持 EAP 身份认证。IKEv2 可以借助 AAA 服务器对远程接入的 PC、手机等进行身份认证、分配私网 IP 地址。IKEv1 无法提供此功能，必须借助 L2TP 来分配私网地址。
  - IKE SA 的完整性算法支持情况不同。IKE SA 的完整性算法仅 IKEv2 支持，IKEv1 不支持。
- **DPD 中超时重传实现不同。**
  - retry-interval 参数仅 IKEv1 支持。表示发送 DPD 报文后，如果超过此时间间隔未收到正确的应答报文，DPD 记录失败事件 1 次。当失败事件达到 5 次时，删除 IKE SA 和相应的 IPsec SA。直到隧道中有流量时，两端重新协商建立 IKE SA。
  - 对于 IKEv2 方式的 IPsec SA，超时重传时间间隔从 1 到 64 以指数增长的方式增加。在 8 次尝试后还未收到对端发过来的报文，则认为对端已经下线，删除 IKE SA 和相应的 IPsec SA。
- **IKE SA 与 IPsec SA 超时时间手工调整功能支持不同。**

  IKEv2 的 IKE SA 软超时为硬超时的 9/10±一个随机数，所以 IKEv2 一般不存在两端同时发起重协商的情况，故 IKEv2 不需要配置软超时时间。

IKEv2 相比 IKEv1 的优点

- 简化了安全联盟的协商过程，提高了协商效率。
- 修复了多处公认的密码学方面的安全漏洞，提高了安全性能。
- 加入对 EAP（Extensible Authentication Protocol）身份认证方式的支持，提高了认证方式的灵活性和可扩展性。
- EAP 是一种支持多种认证方法的认证协议，可扩展性是其最大的优点，即如果想加入新的认证方式，可以像组件一样加入，而不用变动原来的认证体系。当前 EAP 认证已经广泛应用于拨号接入网络中。

- IKEv2 使用基于 ESP 设计的加密载荷，v2 加密载荷将加密和数据完整性保护关联起来，即加密和完整性校验放在相同的载荷中。AES-GCM 同时具备保密性、完整性和可认证性的加密形式与 v2 的配合比较好。

6.3.17 建立 IPsec VPN 连接需要账户名和密码吗？

常见的使用账户名和密码进行认证的 VPN 有 SSL VPN、PPTP 或 L2TP，云的 IPsec VPN 使用预共享密钥方式进行认证，密钥配置在 VPN 网关上，在 VPN 协商完成后即建立通道，VPN 网关所保护的主机在进行通信时无需输入账户名和密码。

说明

IPsec XAUTH 技术是 IPsec VPN 的扩展技术，它在 VPN 协商过程中可以强制接入用户输入账户名和密码。

目前 VPN 不支持该扩展技术。

6.3.18 VPN 监控可以监控哪些内容？

VPN 网关

可以监控网关 IP 的带宽信息，包含入网流量、入网带宽、出网流量、出网带宽及出网带宽使用率。

查询 VPN 网关监控状态，请在 VPN 网关“网关 IP”列中单击 EIP 后面的 进行查看。

VPN 连接

可以监控连接的状态信息，包括 VPN 连接状态、链路往返平均时延、链路往返最大时延、链路丢包率、隧道往返平均时延、隧道往返最大时延、隧道丢包率。

其中，链路往返平均时延、链路往返最大时延、链路丢包率、隧道往返平均时延、隧道往返最大时延、隧道丢包率需要单击 VPN 连接，在“基本信息”页签通过添加健康检查项进行添加；私网相关指标仅 VPN 连接使用静态路由模式，且开启 NQA 检测机制场景下支持配置。

查询 VPN 连接监控状态，请在 VPN 连接“监控”列中单击 进行查看。

6.3.19 VPN 连接中断后会通知我吗？

VPN 连接的状态监控功能已上线，VPN 连接创建后即会向云监控服务 CES 上报状态信息，但是并不会自动向用户发送告警通知，需要在服务列表中选择“管理与监管 > 云监控”创建告警规则。

VPN 连接状态请在 VPN 连接“监控”列中单击 进行查看。

6.4 VPN 协商与对接

6.4.1 哪些设备可以与云进行 VPN 对接？

云的 VPN 支持标准 IPsec 协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与云进行对接：

1. 设备是否具备 IPsec 功能和授权：请查询设备的特性列表获取是否支持 IPsec VPN。
2. 关于组网结构，要求用户侧数据中心有固定的公网 IP 或者经过 NAT 映射后的固定公网 IP（即 NAT 穿越，VPN 设备在 NAT 网关后部署）也可以。

设备型号多为路由器、防火墙等，对接配置请参见 VPN 管理员指南。

说明

- 普通家庭宽带路由器、个人的移动终端设备、Windows 主机自带的 VPN 服务（如 L2TP）无法与云的 VPN 进行对接。
- 与 VPN 服务做过对接测试厂商包括：
- 设备厂商：华为（防火墙/AR）、山石（防火墙），CheckPoint（防火墙）。
- 云服务厂商包括：阿里云，腾讯云，亚马逊（aws），微软（Microsoft Azure）。
- 软件厂商包括：strongSwan。
- IPsec 协议属于 IETF 标准协议，宣称支持该协议的厂商均可与云进行对接，用户不需要关注具体的设备型号。

  目前绝大多数企业级路由器和防火墙都支持该协议。
- 部分硬件厂商在特性规格列表中是宣称支持 IPsec VPN 的，但是需要专门购买软件 License 才能激活相关功能。

  请用户侧数据中心管理员根据设备具体型号与厂商进行确认。

6.4.2 VPN 协商参数有哪些？默认值是什么？

表6-2 VPN 协商参数

协议	配置项	值
IKE	认证算法	• MD5（此算法安全性较低，请慎用） • SHA1（此算法安全性较低，请慎用） • SHA2-256（默认） • SHA2-384 • SHA2-512
	加密算法	• 3DES（此算法安全性较低，请慎用） • AES-128（默认） • AES-192

协议	配置项	值
		• AES-256 • AES-256-GCM-16
	DH 算法	• Group 1（此算法安全性较低，请慎用） • Group 2（此算法安全性较低，请慎用） • Group 5（此算法安全性较低，请慎用） • Group 14（默认） • Group 16 • Group 19 • Group 20 • Group 21
	版本	• v1（有安全风险不推荐） • v2（默认）
	生命周期	86400（默认） 单位：秒。 取值范围：60-604800。
	本端标识	• IP Address 本端 IP 地址由系统自动关联显示，无需用户手动配置。 • FQDN 默认的本端标识类型是 IP Address，ID 值是 VPN 网关的公网 IP。
	对端标识	• IP Address • FQDN 默认的对端标识类型是 IP Address，ID 值是对端网关的公网 IP。
IPsec	认证算法	• SHA1（此算法安全性较低，请慎用） • MD5（此算法安全性较低，请慎用） • SHA2-256（默认） • SHA2-384 • SHA2-512
	加密算法	• AES-128（默认） • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用）

协议	配置项	值
		• AES-256-GCM-16
	PFS	• DH group 1（此算法安全性较低，请慎用） • DH group 2（此算法安全性较低，请慎用） • DH group 5（此算法安全性较低，请慎用） • DH group 14（默认） • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 • Disable
	传输协议	• ESP（默认）
	生命周期	3600（默认） 单位：秒。 取值范围：30-604800。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。

  IKE 协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致 IPsec VPN 受到侵犯。为提升密钥管理的安全性，IKE 提供了 PFS（完美向前保密）功能。启用 PFS 后，在进行 IPsec SA 协商时会进行一次附加的 DH 交换，重新生成新的 IPsec SA 密钥，提高了 IPsec SA 的安全性。
- 为了增强安全性，默认开启 PFS，请确认用户侧数据中心网关设备也开启了该功能，且两端配置保持一致，否则会导致协商失败。
- IPsec SA 字节生命周期，不是 VPN 服务可配置参数，云侧采用的是默认配置 1843200KB。该参数不是协商参数，不影响双方建立 IPsec SA。

6.4.3 IPsec VPN 是否会自动建立连接？

支持自动建立连接。

6.4.4 如何配置 VPN 对端设备？（HUAWEI USG6600 配置示例）

因为隧道的对称性，在云上的 VPN 参数和您的 VPN 中需要进行相同的配置，否则会导致 VPN 无法建立连接。

在您自己数据中心的路由器或者防火墙上需要进行 IPsec VPN 隧道配置，具体配置方法取决于您使用的网络设备，请查询对应设备厂商的指导书。

本文以 Huawei USG6600 系列 V100R001C30SPC300 版本的防火墙的配置过程为例进行说明。

假设数据中心的子网为 192.168.3.0/24 和 192.168.4.0/24，数据中心 IPsec 隧道的出口公网 IP 为 1.1.1.2；VPC 下的子网为 192.168.1.0/24 和 192.168.2.0/24 ，VPC 上 IPsec 隧道的出口公网 IP 为 1.1.1.1。

操作步骤

1. 登录防火墙设备的命令行配置界面。
2. 查看防火墙版本信息。

```
display version
17:20:502017/03/09
Huawei Versatile Security Platform Software
Software Version: USG6600 V100R001C30SPC300(VRP (R) Software，Version 5.30)
```

3. 创建 ACL。

```
acl number 3065 vpn-instance vpn64
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
q
```

4. 创建 ike proposal。

```
ike proposal 64
dh group5
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```

5. 创建 ike peer，并引用之前创建的 ike proposal，其中对端 IP 地址是 1.1.1.1。

```
ike peer vpnikepeer_64
pre-shared-key ******** （********为您输入的预共享密码）
ike-proposal 64
undo version 2
remote-address vpn-instance vpn64 1.1.1.1
sa binding vpn-instance vpn64
q
```

6. 配置 IPsec proposal。

```
IPsec proposal IPsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```

7. 配置 IPsec 策略，并引用之前创建的 IPsec proposal。

```
IPsec policy vpnIPsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
```

```
proposal IPsecpro64
local-address 1.1.1.2
q
```

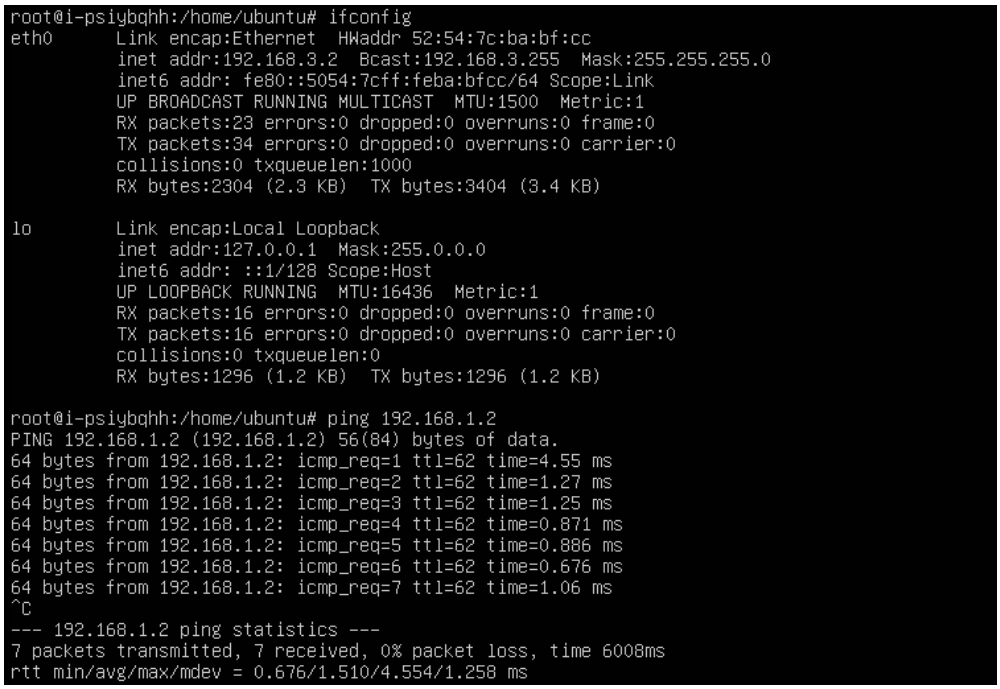
8. 将 IPsec 策略应用到相应的子接口上去。

```
interface GigabitEthernet0/0/2.64
IPsec policy vpnIPsec64
q
```

9. 测试连通性。

   在上述配置完成后，我们可以通过云上主机和数据中心的主机进行连通性测试，如下图图 6-4 所示。

图6-4 连通性测试



6.4.5 VPN 支持对端网关域名对接吗？

对端 VPN 连接需要明确对端的公网 IP 地址，暂不支持通过域名方式与对端设备进行对接。

6.4.6 我创建的 VPN 连接有几个隧道？

VPN 连接下的隧道和本端子网/对端子网的数量有关，隧道总数等于本端子网数和远端子网数的乘积。

- 当两个子网间存在数据流时，连接这两个子网的 IPsec 隧道状态就会变成 Active。
- 只要有一个 IPsec 隧道的状态为 Active，对应 VPN 连接的状态就会显示已连接。

6.4.7 如何在已创建的 VPN 连接中，限定特定的主机访问云上子网？

云下限制：

- VPN 设备按照策略限制访问
- 路由器或交换机上设置 ACL 限制

云上限制：

- 安全组限制源 IP
- ACL 限制

说明

不建议通过修改本端子网和对端子网的方式来限定访问。

6.4.8 VPN 是否启动了 DPD 检测机制？

是的。

VPN 服务默认开启了 DPD 探测机制，用于探测用户侧数据中心 IKE 进程的存活状态。

3 次探测失败后即认为用户侧数据中心 IKE 异常，此时云会删除本端隧道，以保持双方的隧道同步。

DPD 协议本身并不要求对端也同步进行配置（但是要求对端可以应答 DPD 探测），为了保证协商双方隧道状态一致，避免出现单边隧道（一端存在隧道，而另一端已不存在），建议用户同时启动用户侧网关的 DPD 探测机制，用于探测云侧 VPN 服务的 IKE 状态。

说明

DPD 探测失败后会删除隧道，不会导致业务不稳定。

6.4.9 如何通过安全组控制使 VPN 不能访问 VPC 上的部分虚拟机，实现安全隔离？

如果用户需要控制 VPN 站点只能访问 VPC 的部分网段或者部分主机，可以通过安全组进行控制。

配置示例：不允许客户侧的子网 192.168.1.0/24 访问 VPC 内子网 10.1.0.0/24 下的 ECS。

配置方法：

1. 创建两个安全组：安全组 1 和安全组 2。
2. 安全组 1 的入方向规则配置 deny 网段 192.168.1.0/24。
3. 安全组 2 允许 192.168.1.0/24 访问。
4. 网段 10.1.0.0/24 的 ECS 选择安全组 1，其他的主机选择安全组 2。

6.4.10 修改 VPN 连接的配置会造成连接重建吗？

VPN 连接包含本端子网、对端子网、对端网关、预共享密钥、IKE 协商策略、IPsec 协商策略。修改 VPN 连接具体包括以下几种情况：

- 修改本端子网和对端子网，连接 ID 不发生变化，只是更新了连接两端的子网信息，如果更新的是部分子网信息，已经建立的子网间隧道不会重建。
- 修改对端网关 IP，连接 ID 不发生变化，但连接的对端已改变，连接需要重建。
- 仅修改连接的预共享密钥，连接的 ID 不发生变化，连接状态当时并不发生改变，重协商会重新校验密钥匹配情况，如果密钥不匹配重协商会失败。
- 修改协商策略（需验证预共享密钥），连接 ID 发生改变，相当于连接删除重建过程，连接需要重建。

6.4.11 云对接 AWS 后，为何不可以从 AWS 向云发起协商？

VPN 建立连接完成后，AWS 为 Response 模式，并不主动发起协商，当从 AWS 的 EC2 向云 ECS 发起数据流时，也不触发该 VPN 建立 SA。

请按照 AWS 的知识文档，只能从客户侧（即对接 AWS 的云）发起协商。

6.4.12 对接云时，如何配置 DPD 信息？

云默认开启 DPD 配置，且不可关闭该配置。

DPD 配置信息如下：

- DPD-type：按需
- DPD idle-time：30s
- DPD retransmit-interval：15s
- DPD retry-limit：3 次
- DPD msg：seq-hash-notify。

两端 DPD 的 type、空闲时间、重传间隔、重传次数无需一致，只要能接收和回应云的 DPD 探测报文即可，DPD msg 格式必须一致。

6.4.13 本地防火墙无法收到 VPN 网关的 IKE 第一阶段的回复包怎么解决？

1. 检查两端公网 IP 是否可以互访，推荐使用 ping 命令，VPN 网关 EIP 缺省可以 ping 通。
2. 云下网关与 VPN 网关可以互访 UDP 500、4500 报文。
3. 云下公网 IP 访问 VPN 网关 IP 时，没有发生源端口 NAT 转换，如果存在 NAT 穿越，端口号在 nat 穿越后不得发生改变。
4. 两端的 IKE 协商参数配置一致。

   NAT 穿越场景中，云下 ID 标识类型选择 IP，IP 值为 NAT 转换后的公网 IP。

6.4.14 本地防火墙无法收到 VPN 子网的回复包怎么解决？

1. 如果二阶段协商中需要检查云下的路由、安全策略、NAT 和感兴趣流、协商策略信息。

- 路由设置：将访问云上子网的数据送入隧道。
- 安全策略：放行云下子网访问云上子网的流量。
- NAT 策略：云下子网访问云上子网不做源 nat。
- 感兴趣流：两端感兴趣流配置互为镜像，使用 IKE v2 配置感兴趣流不可使用地址对象名称。
- 协商信息：协商策略信息云上云下一致，特别注意 PFS 的配置。

2. 确认一、二阶段协商均已正常后，请检查云上安全组策略，放行入方向的云下子网访问云上子网的 ICMP 协议。

6.4.15 VPN 使用的 DH group 对应的比特位是多少？

Diffie-Hellman(DH)组确定密钥交换过程中使用的密钥的强度。较高的组号更安全，但需要额外的时间来计算密钥。

VPN 使用的 DH group 对应的比特位如表 6-3 所示。

表6-3 DH group 对应比特位

DH group	Modulus
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	ecp256 bits
20	ecp384 bits
21	ecp521 bits

说明

以下 DH 算法有安全风险，不推荐使用：DH group 1、DH group 2、DH group 5。

6.5 连接故障或无法 PING 通

6.5.1 VPN 配置完成了，为什么连接一直处于未连接状态？

可能存在信息配置错误，请从以下方面进行排查：

1. 确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/对端子网、本端网关/对端网关互为镜像。
2. 确认用户侧数据中心设备的路由、NAT 和安全策略配置无误。

6.5.2 如何防止 VPN 连接出现中断情况？

VPN 连接在正常的使用过程中会存在重协商情况，触发重协商的条件有 IPsec SA 的生命周期即将到期和 VPN 传输的流量超过 20GB，重协商一般不造成连接中断。

大多数的连接中断都是因为两端的配置信息错误造成的，或公网异常导致重协商失败造成的。

常见的连接中断原因有：

- 两端的 ACL 不匹配；
- SA 生命周期不匹配；
- 用户侧数据中心未配置 DPD；
- VPN 使用过程中修改了配置信息；
- 运营商网络抖动。

因此请在配置 VPN 时确保操作和配置，以进行连接状态保活：

- 两端的子网配置互为镜像；
- SA 生命周期信息一致；
- 用户侧数据中心网关开启 DPD 配置，探测次数不少于 3 次；
- 连接过程中修改参数两侧同步修改；
- 设置用户侧数据中心设备 TCP MAX-MSS 为 1300；
- 确保用户侧数据中心出口有足够的带宽可被 VPN 使用；
- 确认 VPN 连接可被两端触发协商，开启用户侧数据中心设备的主动协商配置；

6.5.3 使用中 IPsec VPN 连接中断后如何快速恢复？

1. 如果无法正常触发协商，请检查 IPsec 两侧公网 IP 的连通性，比如两个公网 IP 互 Ping 验证。VPN 网关 IP 默认回应 ICMP 报文。
2. 如果公网链路正常，需排查是否存在多出口的链路切换，即当前访问云网关 IP 流量未从协商端口流出。
3. 如果无多出口或出口路径正常，可尝试 IPsec 隧道两端同时修改一次 PSK，重新触发协商。
4. 如果重新触发协商失败，请确认两端配置的协商策略是否一致、感兴趣流是否互为镜像（条目数、子网均相同）。

5. 如果协商策略和感兴趣流配置无误，请关停云下设备的 VPN 连接，等待云端连接显示为“未连接”后，重启云下设备 VPN 连接，并进行数据流触发。
6. 如果依然无法触发协商时，请执行以下操作：
   a. 记录 VPN 连接的协商策略、PSK、本端子网、对端网关、对端子网。
   b. 使用现有网关新建一条连接，协商策略、PSK、本端子网均与原连接相同，对端网关和对端子网先任意填写。
   c. 待新创建连接成功后，删除原连接，之后再修改新建连接的对端网关和对端子网与记录数据一致。
   d. 修改完成后重新触发协商。

6.5.4 VPN 网关带宽到达限额时有什么影响？

VPN 带宽限速限制的出 VPC 方向的带宽，如果您 VPN 的带宽超过限额使用时，会出现网络卡顿、部分子网间无法访问、甚至出现 VPN 连接中断现象（无法收到 VPN 的探测报文）。

因此在出现 VPN 带宽已达到上限时，建议您对 VPN 网关带宽进行扩容。

说明

VPN 的带宽最大为 1Gbit/s。

6.5.5 IPsec VPN 是否会自动建立连接？

支持自动建立连接。

6.5.6 两个 Region 创建的 VPN 连接状态正常，为什么不能 ping 通对端 ECS？

安全组默认放行了出方向的所有端口，入方向需要按照实际需要添加放行规则，确认接收 ping 报文的 ECS 安全组放行了入方向的 ICMP。

6.5.7 IDC 与云端对接，VPN 连接正常，子网间业务无法互相访问？

连接状态正常，说明两端的协商参数没有问题，排查项如下：

- 用户侧数据中心设备子网路由是否从网关开始逐跳指向 VPN 出口设备。
- VPN 设备有安全设置放行了子网间的数据互访。
- IDC 子网访问云端数据不做 NAT。
- 确保两侧公网 IP（网关 IP）间访问不被阻拦。

6.5.8 正在使用 VPN 出现了连接中断，提示数据流不匹配，如何排查？

这通常是由于云上与用户侧数据中心设备配置的 ACL 不匹配造成的。

1. 首先确认两端 VPN 连接的子网信息是否配置一致，确保云端生成的 ACL 与用户侧数据中心 ACL 配置互为镜像

2. 用户侧数据中心感兴趣流配置推荐使用“子网/掩码”的格式，避免使用网络地址对象模式，即 address object 模式，address object 为非标模式，容易引起不兼容问题。

6.5.9 正在使用 VPN 出现了连接中断，提示 DPD 超时，如何排查？

出现 DPD 超时的连接中断是因为两端网络访问无数据，在 SA 老化后发送 DPD 未得到对端响应而删除连接。

解决方法：

1. 开启用户侧数据中心设备的 DPD 配置，测试两端的数据流均可触发连接建立；
2. 在两端的主机中部署 Ping shell 脚本，也可在用户侧数据中心的子网的网关设备上配置保活数据，如 NQA。

6.5.10 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接？

管理控制台界面中 VPN 连接状态刷新存在一定的延迟，是正常现象。

如果数据面已正常（即业务访问已正常）， 则 VPN 连接已完成建立。

6.5.11 VPN 连接中断后会通知我吗？

VPN 连接的状态监控功能已上线，VPN 连接创建后即会向云监控服务 CES 上报状态信息，但是并不会自动向用户发送告警通知，需要在服务列表中选择“管理与监管 > 云监控”创建告警规则。

VPN 连接状态请在 VPN 连接“监控”列中单击 进行查看。

6.5.12 如何解决 VPN 连接无法建立连接问题？

1. 登录控制台，进入“VPN 连接 > 企业版-VPN 连接”页面。
2. 在 VPN 连接列表中，单击目标 VPN 连接“操作”列的“修改策略配置”，查看该 VPN 连接对应的 IKE 策略和 IPsec 策略详情。
3. 检查云上 VPN 连接中的 IKE 策略和 IPsec 策略中的协商模式和加密算法是否与远端配置一致。

   如果第一阶段 IKE SA 已经建立，第二阶段 IPsec SA 未建立，常见情况为 IPsec 策略与数据中心远端的配置不一致。
4. 检查 ACL 是否配置正确。

   假设您的数据中心的子网为 192.168.3.0/24 和 192.168.4.0/24，VPC 下的子网为 192.168.1.0/24 和 192.168.2.0/24，则你在数据中心或局域网中的 ACL 应对你的每一个数据中心子网配置允许 VPC 下的子网通信的规则，如下例：

   ```
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   ```
5. 配置完成后检查 VPN 是否连接，从两侧测试 ping 是否正常。

6.5.13 VPN 建立后您的数据中心或局域网无法访问弹性云主机？

我们提供的安全组默认不允许任何源访问，请确认您的安全组是否配置允许远端的子网地址访问。

6.5.14 为什么 VPN 创建成功后状态显示未连接？

VPN 连接状态存在一定延迟，请等待大约 2 分钟后重新刷新 VPN 连接状态。

6.5.15 VPN 是否启动了 DPD 检测机制？

是的。

VPN 服务默认开启了 DPD 探测机制，用于探测用户侧数据中心 IKE 进程的存活状态。

3 次探测失败后即认为用户侧数据中心 IKE 异常，此时云会删除本端隧道，以保持双方的隧道同步。

DPD 协议本身并不要求对端也同步进行配置（但是要求对端可以应答 DPD 探测），为了保证协商双方隧道状态一致，避免出现单边隧道（一端存在隧道，而另一端已不存在），建议用户同时启动用户侧网关的 DPD 探测机制，用于探测云侧 VPN 服务的 IKE 状态。

说明

DPD 探测失败后会删除隧道，不会导致业务不稳定。

DPD 可以及时发现对方 IKE 进程异常，并通过重置隧道的方法来保持双方隧道同步。在删除隧道后，当有用户流量时，可以重新触发协商并建立隧道。

6.6 公网地址

6.6.1 VPN 网关删除后公网地址是否可以保留？

按需 VPN 网关如果绑定了按需 EIP，则 VPN 网关删除后会同步删除绑定的按需 EIP。

如果需要保留 EIP，请在删除 VPN 网关前对 EIP 进行解绑操作。

6.6.2 EIP 能作为 VPN 的网关 IP 吗？

可以。

用户可以在创建 VPN 网关时绑定 EIP 作为网关 IP。

6.6.3 通过 VPN 互访的主机需要购买 EIP 吗？

如果用户本地的主机通过 VPN 访问云上的 ECS，此时 ECS 不需要购买 EIP。

如果 ECS 要向公网用户提供服务，需要购买 EIP。

6.6.4 为什么我开通 VPN 后，云端 ECS 会有公网 IP 的访问信息？

可能原因：在 VPN 对接之前，ECS 已经绑定了 EIP。该场景下，用户除了通过 VPN，也可通过公网地址直接访问该 ECS。

如果 ECS 主机只允许 VPN 内的主机访问，可在完成 VPN 对接后将 ECS 的 EIP 解绑。

6.6.5 用户侧数据中心的网关设备没有固定的公网 IP 可以吗？

可以。

用户数据中心与云进行 VPN 对接时，如果用户购买的 VPN 网关规格支持非固定 IP 接入能力，对端网关设备就可以使用非固定 IP 接入。

说明

VPN 网关是否支持非固定 IP 接入能力，以管理控制台实际显示区域为准。

6.7 路由设置

6.7.1 如何理解 VPN 连接中的对端网关和对端子网？

对端网关和对端子网是两个相对的概念，在建立 VPN 连接时，从云的角度出发，VPC 网络就是本地子网，创建的 VPN 网关就是本地网关，与之对接的用户侧网络就是对端子网，用户侧的网关就是对端网关。

对端网关 IP 就是用户侧网关的公网 IP，对端子网指需要和 VPC 子网互联的子网。

6.7.2 Console 界面在哪添加 VPN 远端路由？

云端在 VPN 连接创建时会自动下发到达远端子网的路由，无需手动配置。

6.7.3 ECS 主机多网卡是否需要添加去往线下网络的路由？

- 如果客户使用主网卡与线下网络建立了 VPN，不需要添加路由。
- 如果客户使用非主网卡与线下网络建立了 VPN，需要添加去往线下网段的路由指向非主网卡的网关。

6.7.4 什么是 NQA

什么是 NQA

网络质量分析（Network Quality Analysis，NQA）是一种实时的网络性能探测和统计技术，可以对响应时间、网络抖动、丢包率等网络指标进行统计。NQA 能够实时监视网络服务质量，在网络发生故障时进行有效的故障诊断和定位。

为什么需要 NQA

随着运营商增值业务的开展，用户和运营商对 QoS（Quality of Service）的相关要求越来越高，特别是在传统的 IP 网络承载语音和视频业务后，运营商与客户之间签订 SLA（Service Level Agreement）成为普遍现象。

为了让用户看到承诺的带宽是否达到需求，运营商需要提供相关的时延、抖动、丢包率等相关的统计参数，以及时了解网络的性能状况。传统的网络性能分析方法（如 Ping、Tracert 等）已经不能满足用户对业务多样性和监测实时性的要求。NQA 可以实现对网络运行状况的准确测试，输出统计信息。NQA 可以监测网络上运行的多种协议的性能，使网络运营商能够实时采集到各种网络运行指标，例如：HTTP 的总时延、TCP 连接时延、DNS 解析时延、文件传输速率、FTP 连接时延、DNS 解析错误率等。通过对这些指标进行控制，网络运营商可以为用户提供不同等级的网络服务。同时，NQA 也是网络故障诊断和定位的有效工具。

静态路由与 NQA 联动

静态路由本身并没有检测机制，如果非本机直连链路发生了故障，静态路由不会自动从 IP 路由表中自动删除，需要网络管理员介入，这就无法保证及时进行链路切换，可能造成较长时间的业务中断。

使用静态路由模式创建 VPN 连接时，为了避免出现以上问题，需要使用 NQA 来检测静态路由所在的链路，确保 VPN 连接稳定性。使能 NQA 时需要确保对端网关设备支持 ICMP 功能，且对端接口地址已在对端网关上正确配置，否则可能导致流量不通。

6.8 VPN 子网设置

6.8.1 配置 VPN 连接的本端子网和对端子网时需要注意什么？

- 子网数量满足规格限制，数量超出规格限制请进行聚合汇总。
  - 每 VPN 网关配置的本地子网数量：50。
  - 每 VPN 连接支持配置的对端子网个数：50。
- 本端子网不可以包含远端子网，远端子网可以包含本端子网。
- 推荐配置的本端子网在 VPC 内有路由可达。
- 同一个 VPN 网关创建两条连接：若这两条连接的远端子网存在包含关系，在访问的目的网络处于交集网段部分时，按照创建连接的先后顺序匹配 VPN 连接，且与连接状态无关（策略模式不能按照掩码长度进行匹配）。

6.8.2 VPN 本端子网和对端子网的数量有限制吗？

- 每 VPN 网关配置的本地子网数量：50
- 每 VPN 连接支持配置的对端子网个数：50

6.8.3 创建 VPN 连接时添加对端子网，提示系统异常，如何处理？

检查 VPC 内是否存在对等连接、云专线的子网路由使用了该子网，导致 VPN 下发子网路由冲突，确认后将其配置的子网路由删除后重新创建即可。

6.8.4 VPN 网关删除后公网地址是否可以保留？

按需 VPN 网关如果绑定了按需 EIP，则 VPN 网关删除后会同步删除绑定的按需 EIP。

如果需要保留 EIP，请在删除 VPN 网关前对 EIP 进行解绑操作。

6.8.5 VPN 接入 VPC 的网络地址如何规划？

- 云上 VPC 地址段和客户云下的地址段不能冲突，且不允许存在包含关系。
- 为避免和云服务地址冲突，用户侧网络应尽量避免使用 127.0.0.0/8、169.254.0.0/16、224.0.0.0/3、100.64.0.0/10 的网段。

6.8.6 创建 VPN 网关时 IP 是如何分配的？

云的 VPN 网关 IP 是一组提前规划好的地址组，提前预置了 VPN 的相关配置。

在用户创建 VPN 网关时，系统会随机分配一个 IP 地址和 VPC 进行绑定，且这个 IP 地址也只能绑定 1 个 VPC。

因为 VPN 的网关 IP 存在预置数据，在创建 VPN 网关时也不能指定 IP 地址。删除 VPN 网关时会释放 IP 地址与 VPC 的绑定关系；重新创建 VPN 网关时系统会重新随机分配网关 IP 地址。

6.9 VPN 感兴趣流

6.9.1 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置？

VPN 连接的“连接模式”选择“策略模式”时，才需要在控制台上配置策略规则 ACL。

6.9.2 如何配置和修改云上 VPN 的感兴趣流？

感兴趣流由本端子网与远端子网 full-mesh 生成，例如本端子网有 2 个，分别为 A 与 B，远端子网有 3 个，分别为 C、D 和 E，生成感兴趣流 ACL 的 rule 如下：

```
rule 1 permit ip source A destination C
rule 2 permit ip source A destination D
rule 3 permit ip source A destination E
rule 4 permit ip source B destination C
rule 5 permit ip source B destination D
rule 6 permit ip source B destination E
```

在管理控制台界面修改本端子网和对端子网会自动更新感兴趣流信息，即修改了云上的 ACL 配置。

6.10 VPN 连接保活

6.10.1 如何防止 VPN 连接出现中断情况？

VPN 连接在正常的使用过程中会存在重协商情况，触发重协商的条件有 IPsec SA 的生命周期即将到期和 VPN 传输的流量超过 20GB，重协商一般不造成连接中断。

大多数的连接中断都是因为两端的配置信息错误造成的，或公网异常导致重协商失败造成的。

常见的连接中断原因有：

- 两端的 ACL 不匹配。
- SA 生命周期不匹配。
- 用户侧数据中心未配置 DPD。
- VPN 使用过程中修改了配置信息。
- 运营商网络抖动。

因此请在配置 VPN 时确保操作和配置，以进行连接状态保活：

- 两端的子网配置互为镜像。
- SA 生命周期信息一致。
- 用户侧数据中心网关开启 DPD 配置，探测次数不少于 3 次。
- 连接过程中修改参数两侧同步修改。
- 设置用户侧数据中心设备 TCP MAX-MSS 为 1300。
- 确保用户侧数据中心出口有足够的带宽可被 VPN 使用。
- 确认 VPN 连接可被两端触发协商，开启用户侧数据中心设备的主动协商配置。

6.11 监控

6.11.1 VPN 监控可以监控哪些内容？

VPN 网关

可以监控网关 IP 的带宽信息，包含入网流量、入网带宽、出网流量、出网带宽及出网带宽使用率。

查询 VPN 网关监控状态，请在 VPN 网关“网关 IP”列中单击 EIP 后面的 进行查看。

VPN 连接

可以监控连接的状态信息，包括 VPN 连接状态、链路往返平均时延、链路往返最大时延、链路丢包率、隧道往返平均时延、隧道往返最大时延、隧道丢包率。

其中，链路往返平均时延、链路往返最大时延、链路丢包率、隧道往返平均时延、隧道往返最大时延、隧道丢包率需要单击 VPN 连接，在“基本信息”页签通过添加健康

检查项进行添加；私网相关指标仅 VPN 连接使用静态路由模式，且开启 NQA 检测机制场景下支持配置。

查询 VPN 连接监控状态，请在 VPN 连接“监控”列中单击 进行查看。

6.11.2 VPN 连接中断后会通知我吗？

VPN 连接的状态监控功能已上线，VPN 连接创建后即会向云监控服务 CES 上报状态信息，但是并不会自动向用户发送告警通知，需要在服务列表中选择“管理与监管 > 云监控”创建告警规则。

VPN 连接状态请在 VPN 连接“监控”列中单击 进行查看。

6.11.3 VPN 监控能不能查看每条连接的流量？

VPN 的流量监控是基于 VPN 网关的，可查看该 VPN 网关的出入方向的流量、带宽等信息，无法查看单独的某一条连接的流量使用情况。

6.11.4 当 VPN 监控结果异常时，可以发送提醒信息吗？

可以。

用户可以在“云监控服务”通过配置告警规则，实现 VPN 监控结果异常提醒。

6.12 带宽与网速

6.12.1 如何测试 VPN 速率情况？

假设测试环境 VPN 连接已经创建，在 VPN 连接两端 VPC 的本端子网下分别创建 ECS，并使两个 VPC 之间的 ECS 相互能够 ping 通的情况下，测试 VPN 的速率情况。

当用户购买的 VPN 网关的带宽为 200Mbit/s 时，测试情况如下。

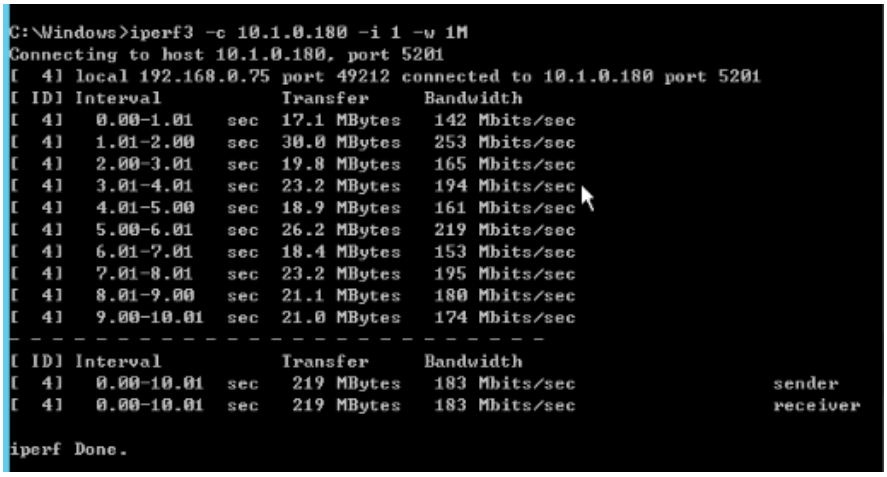
1. 互为对端的 ECS 都使用 Windows 系统，测试速率可达 180Mbit/s，使用 iperf3 和 filezilla（是一款支持 ftp 的文件传输工具）测试均满足带宽要求。

说明

基于 TCP 的 FTP 协议有拥塞控制机制，180Mbit/s 为平均速率，且 IPsec 协议会增加新的 IP 头，因此 10%左右的速率误差在网络领域是正常现象。

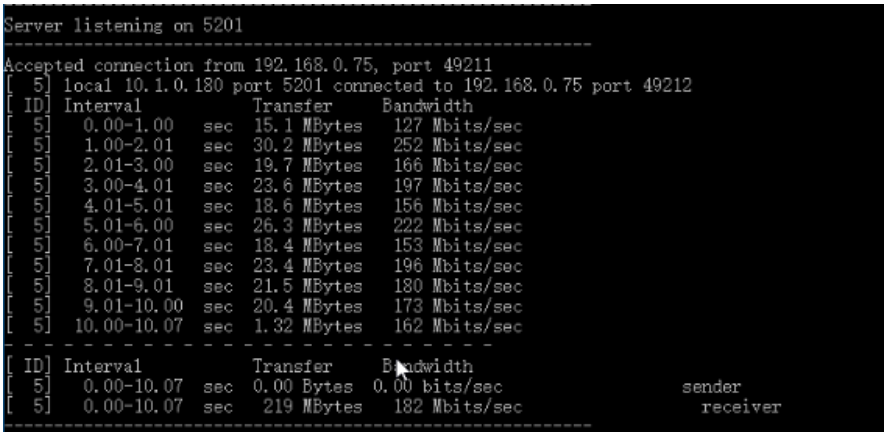
使用 iperf3 客户端测试结果截图如图 6-5 所示。

图6-5 200M 带宽客户端 iperf3 测试结果



使用 iperf3 服务器端测试结果截图如图 6-6 所示。

图6-6 200M 带宽服务端 iperf3 测试结果

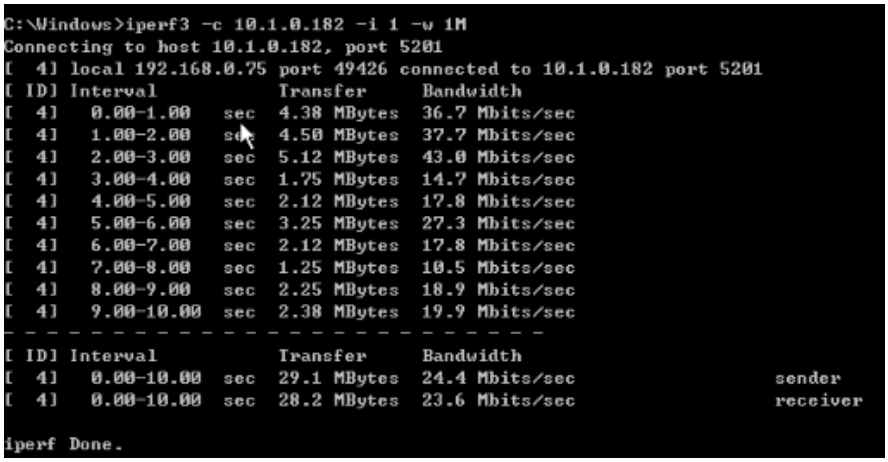


2. 互为对端的 ECS 都使用 Centos7 系统，测试速率可达 180M，使用 iperf3 测试满足带宽要求。
3. 服务器端 ECS 使用 Centos7 系统，客户端使用 Windows 系统，测试速率只有 20M 左右，使用 iperf3 和 filezilla 测试均不能满足带宽要求。

   原因在于 Windows 和 Linux 对 TCP 的实现不一致，导致速率慢。所以对端 ECS 使用不同的系统时，无法满足带宽要求。

   使用 iperf3 测试结果截图如图 6-7 所示。

图6-7 互为对端的 ECS 系统不同时 iperf3 测试结果



用户购买的 VPN 网关为网关的整体吞吐能力，即该 VPN 网关下所有 VPN 连接的带宽之和。在大带宽场景下，由于主机的转发性能限制，需要使用多台主机构建多条流量才能充分利用网关的带宽。这种场景下对 ECS 的配置要求也很高，建议 ECS 的网卡支持 2G 以上的带宽。

测试总结：综上测试结果，云网关能够满足带宽速率要求，但是建议两端主机使用相同的操作系统，并且网卡要达到配置要求。

6.12.2 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？

云上用户购买的 VPN 网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下两种情况：

- 如果所购买的带宽<=10Mbit，则入云方向统一限定为 10Mbit。
- 如果所购买的带宽>10Mbit，则入云方向与购买的带宽一致。

按带宽计费度量采用国际统一的带宽单位 Mbit，按流量计费的度量单位为 GByte。

6.12.3 VPN 网关带宽到达限额时有什么影响？

VPN 带宽限速限制的出 VPC 方向的带宽，如果您 VPN 的带宽超过限额使用时，会出现网络卡顿、部分子网间无法访问、甚至出现 VPN 连接中断现象（无法收到 VPN 的探测报文）。

因此在出现 VPN 带宽已达到上限时，建议您对 VPN 网关带宽进行扩容。

说明

VPN 的带宽最大为 1000(Mbit/s)。

6.12.4 修改了 VPN 带宽大小，为什么测试没有生效？

VPN 带宽修改到生效会有一定的延迟，是正常现象。

请在修改带宽 5 分钟后再进行带宽测试。

说明

修改 VPN 带宽大小，不会导致用户业务和网络中断。

6.12.5 如何选择购买 VPN 带宽的大小？

购买 VPN 时，选择带宽大小需要考虑以下两个因素：

- VPN 隧道中单位时间的数据传输量（需要冗余一定带宽，防止链路拥塞）。
- 考虑两端的出口带宽，云上带宽要小于云下出口带宽。

6.13 配额

6.13.1 虚拟专用网络的配额是什么？

什么是配额？

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少台弹性云主机、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

资源类型

VPN 的资源类型包括 VPN 网关、VPN 连接和对端网关，对应资源类型的总配额根据部署 Region 存在差异，请以实际部署环境为准。

怎样查看我的配额？

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击页面右上角的“我的配额”图标 。
   系统进入“服务配额”页面。
4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请提交工单，申请扩大配额。

6.13.2 创建 VPN 网关和连接的缺省配额是多少？

每个用户缺省可创建 50 个 VPN 网关和 100 个对端网关；每个 VPN 网关缺省可创建 100 个连接组。其中，VPN 网关不同 EIP 对接到对端网关的同一个公网 IP 占用 1 个 VPN 连接组配额；VPN 网关不同 EIP 对接到对端网关的不同公网 IP 或多个对端网关的公网 IP 占用 2 个 VPN 连接组配额。

6.14 账号权限

6.14.1 建立 IPsec VPN 连接需要账户名和密码吗？

常见的使用账户名和密码进行认证的 VPN 有 SSL VPN、PPTP 或 L2TP，云的 IPsec VPN 使用预共享密钥方式进行认证，密钥配置在 VPN 网关上，在 VPN 协商完成后即建立通道，VPN 网关所保护的主机在进行通信时无需输入账户名和密码。

说明

IPsec XAUTH 技术是 IPsec VPN 的扩展技术，它在 VPN 协商过程中可以强制接入用户输入账户名和密码。

目前 VPN 不支持该扩展技术。

6.14.2 创建 VPN 时系统提示权限不足，如何处理？

- 确认您的账号为子账号。
- 确保子账号具有“VPC Administrator”、“Tenant Guest”、“VPN Administrator”这三个【系统角色】权限。

  如果未开通 VPC 操作权限，请使用主账号在统一身份认证服务（IAM）中对您的账号进行授权。

6.14.3 如何确定我的账号是因为权限不足而无法创建 VPN 的？

- 主账号创建的 VPN 网关和连接，子账号不可见。
- 创建 VPN 网关或连接时提示系统繁忙。

账号创建 VPN 连接所需权限详见 VPN 连接用户指南 > 权限管理。

6.15 经典版 VPN

6.15.1 产品咨询

6.15.1.1 IPsec VPN 适用连接典型组网结构有哪些？

VPN 是打通的点到点的网络，实现两点之间的私网互访，不能打通点到端的网络。

- 适用典型场景：
  - 不同 region 之间创建 VPN，实现跨 region 的 VPC 间网络互访
  - 云与友商云创建 VPN，如与阿里云的 VPC 间网络互访
  - 云与客户 IDC 机房打通 VPN，实现线上 VPC 与线下的 IDC 网络互访
  - 结合 SNAT 实现跨云访问特定 IP
- 不适用的典型场景：
  - 相同 region 的两个 VPC 不可以使用 VPN，推荐使用对等连接打通
  - 不可与家庭 PPPoE 拨号网络建立 VPN 连接

- 不可与 4G/5G 路由器建立 VPN 连接
- 不可与个人终端建立 VPN 连接

6.15.1.2 什么是 VPC、VPN 网关、VPN 连接？

VPC：虚拟私有云是指云上隔离的、私密的虚拟网络环境，用户可通过虚拟专用网络（VPN）服务，安全访问云上虚拟网络内的主机（ECS）。

VPN 网关：虚拟私有云中建立的出口网关设备，通过 VPN 网关可建立虚拟私有云和企业数据中心或其它区域 VPC 之间的安全可靠的加密通信。

VPN 连接：是一种基于 Internet 的 IPsec 加密技术，帮助用户快速构建 VPN 网关和用户数据中心的远端网关之间的安全、可靠的加密通道。

云上建立 VPN 网络分为以下两个步骤：

1. 创建 VPN 网关：创建 VPN 网关指明了 VPN 互联的本地 VPC，同时创建连接带宽和网关 IP。
2. VPN 连接：创建 VPN 连接指明了与客户侧对接的网关 IP、子网和协商策略信息。

6.15.1.3 VPC、VPN 网关、VPN 连接之间有什么关系？

- VPC，即云上私有专用网络，同一 Region 中可以创建多个 VPC，且 VPC 之间相互隔离。一个 VPC 内可以划分多个子网网段。
- VPN 网关，基于 VPC 创建，是 VPN 连接的接入点。云中一个 VPC 仅能购买一个 VPN 网关，每个网关可以创建多个 VPN 连接。
- VPN 连接，基于 VPN 网关创建，用于连通 VPC 子网和用户数据中心（或其它 Region 的 VPC）子网，即每个 VPN 连接连通了一个用户侧数据中心的网关。

说明

VPN 连接的数量与 VPN 连接的本端子网和远端子网的数量无关，仅与用户 VPC 需要连通的用户数据中心（或其它 Region 的 VPC）的数量有关，已创建的 VPN 连接的数量即 VPN 连接列表中展示的数量（一个条目即一个 VPN 连接），也可以在 VPN 网关中查看当前网关已创建的 VPN 连接数量。

6.15.1.4 如何理解 VPN 连接中的远端网关和远端子网？

远端网关和远端子网是个相对的概念，在建立 VPN 连接时，从云的角度出发，VPC 网络就是本地子网，创建的 VPN 网关就是本地网关，与之对接的用户侧网络就是远端子网， 用户侧的网关就是远端网关。

远端网关 IP 就是用户侧网关的公网 IP，远端子网指需要和 VPC 子网互联的子网。

6.15.1.5 VPN 接入 VPC 的网络地址如何规划？

- 云上 VPC 地址段和客户云下的地址段不能冲突，且不允许存在包含关系。
- 为避免和云服务地址冲突，用户侧网络应尽量避免使用 127.0.0.0/8、169.254.0.0/16、224.0.0.0/3、100.64.0.0/10 的网段。

6.15.1.6 IPsec VPN 是否会自动进行协商？

IPsec VPN 的协商流程为流量触发的，用户在完成配置后，如果云上与用户侧数据中心间没有交互流量，则不会建立起 VPN 隧道。

因此在完成 VPN 配置后，VPN 连接会处于 down 状态，此时，用户可以使用 ping 触发协商流程。

说明

ping 包的源目地址需要处于 VPN 保护的范围内。

6.15.1.7 VPN 协商参数有哪些？默认值是什么？

表6-4 VPN 协商参数

协议	配置项	值
IKE	认证算法	• MD5（此算法安全性较低，请慎用） • SHA1（此算法安全性较低，请慎用） • SHA2-256（默认） • SHA2-384 • SHA2-512
	加密算法	• 3DES（此算法安全性较低，请慎用） • AES-256 • AES-192 • AES-128（默认）
	DH 算法	• Group 5（此算法安全性较低，请慎用） • Group 2（此算法安全性较低，请慎用） • Group 14（默认） • Group 1（此算法安全性较低，请慎用） • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 说明 部分区域仅支持 Group 14、Group 2、Group 5。
	版本	• v1（有安全风险不推荐） • v2（默认）

协议	配置项	值
	生命周期	86400（默认） 单位：秒。 取值范围：60-604800。
IPsec	认证算法	• SHA1（此算法安全性较低，请慎用） • MD5（此算法安全性较低，请慎用） • SHA2-256（默认） • SHA2-384 • SHA2-512
	加密算法	• AES-128（默认） • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用）
	PFS	• DH group 5（此算法安全性较低，请慎用） • DH group 2（此算法安全性较低，请慎用） • DH group 14（默认） • DH group 1（此算法安全性较低，请慎用） • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 • Disable **说明** 部分区域仅支持 DH group 14、DH group 2、DH group 5。
	传输协议	• ESP（默认） • AH • AH-ESP
	生命周期	3600（默认） 单位：秒。 取值范围：480-604800。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。

  IKE 协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致 IPsec VPN 受到侵犯。为提升密钥管理的安全性，IKE 提供了 PFS（完美向前保密）功能。启用 PFS 后，在进行 IPsec SA 协商时会进行一次附加的 DH 交换，重新生成新的 IPsec SA 密钥，提高了 IPsec SA 的安全性。
- 为了增强安全性，云默认开启 PFS，请用户在配置用户侧数据中心网关设备时确认也开启了该功能，否则会导致协商失败。
- 用户开启此功能的同时，需要保证两端配置一致。
- IPsec SA 字节生命周期，不是 VPN 服务可配置参数，云侧采用的是默认配置 1843200KB。该参数不是协商参数，不影响双方建立 IPsec SA。

6.15.1.8 哪些设备可以与云进行 VPN 对接？

VPN 支持标准 IPsec 协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与云进行对接：

1. 设备是否具备 IPsec 功能和授权：请查询设备的特性列表获取是否支持 IPsec VPN。
2. 关于组网结构，要求用户侧数据中心有固定的公网 IP 或者经过 NAT 映射后的固定公网 IP（即 NAT 穿越，VPN 设备在 NAT 网关后部署）也可以。

说明

- 普通家庭宽带路由器、个人的移动终端设备、Windows 主机自带的 VPN 服务（如 L2TP）无法与云的 VPN 进行对接。
- 与 VPN 服务做过对接测试厂商包括：
- 设备厂商：华为（防火墙/AR）、山石（防火墙），CheckPoint（防火墙）。
- 云服务厂商包括：阿里云，腾讯云，亚马逊（aws），微软（Microsoft Azure）。
- 软件厂商包括：strongSwan。
- IPsec 协议属于 IETF 标准协议，宣称支持该协议的厂商均可与云进行对接，用户不需要关注具体的设备型号。

  目前绝大多数企业级路由器和防火墙都支持该协议。
- 部分硬件厂商在特性规格列表中是宣称支持 IPsec VPN 的，但是需要专门购买软件 License 才能激活相关功能。

  请用户侧数据中心管理员根据设备具体型号与厂商进行确认。

6.15.1.9 建立 IPsec VPN 连接需要账户名和密码吗？

常见的使用账户名和密码进行认证的 VPN 有 SSL VPN、PPTP 或 L2TP，云的 IPsec VPN 使用预共享密钥方式进行认证，密钥配置在 VPN 网关上，在 VPN 协商完成后即建立通道，VPN 网关所保护的主机在进行通信时无需输入账户名和密码。

说明

IPsec XAUTH 技术是 IPsec VPN 的扩展技术，它在 VPN 协商过程中可以强制接入用户输入账户名和密码。

目前 VPN 不支持该扩展技术。

6.15.1.10 如何在已创建的 VPN 连接中，限定特定的主机访问云上子网？

云下限制：

- VPN 设备的按照策略中限制访问
- 路由器或交换机上设置 ACL 限制

云上限制：

- 安全组限制源 IP
- ACL 限制

说明

所有的限定规则需要添加在建立 VPN 隧道之前的设备上。不建议通过修改本端子网和远端子网的方式来限定访问。

6.15.1.11 VPN 监控可以监控哪些内容？

VPN 网关

可监控带宽信息包含入网流量、入网带宽、出网流量、出网带宽及出网带宽使用率；查询网关监控状态请在 VPN 网关列表中选择“操作 > 查看监控”即可。

VPN 连接

可监控连接的状态，1 为正常、0 为未连接；查询 VPN 连接监控请在 VPN 连接列表中选择“操作 > 更多 > 查看监控”。

6.15.1.12 EIP 能作为 VPN 的网关 IP 吗？

不可以。

VPN 网关 IP 是在创建 VPN 网关时分配的，需要和系统内的相关配置信息结合使用，EIP 不具备 VPN 对接服务的功能。

6.15.1.13 通过 VPN 互访的主机需要购买 EIP 吗？

如果用户本地的主机通过 VPN 访问云上的 ECS，此时 ECS 不需要购买 EIP。

如果 ECS 要向公网用户提供服务，需要购买 EIP。

6.15.1.14 如何选择购买 VPN 带宽的大小？

购买 VPN 时，选择带宽大小需要考虑以下两个因素：

- VPN 隧道中单位时间的数据传输量（需要冗余一定带宽，防止链路拥塞）。
- 考虑两端的出口带宽，云上带宽要小于云下出口带宽。

6.15.1.15 创建 VPN 连接时如何选择 IKE 的版本？

推荐您选择 IKEv2 进行协商，其原因是 IKEv1 的版本存在一定的安全风险，且 IKEv2 在连接的协商建立过程，认证方法支持，DPD 超时处理，SA 超时处理上都优于 IKEv1。

云将大力推进 IKEv2 的使用，逐步停用 IKEv1 协商策略。

IKEv1 与 IKEv2 的协议介绍

- IKEv1 协议是一个混合型协议，其自身的复杂性不可避免地带来一些安全及性能上的缺陷，已经成为目前实现的 IPsec 系统的瓶颈。
- IKEv2 协议保留了 IKEv1 的基本功能，并针对 IKEv1 研究过程中发现的问题进行修正，同时兼顾简洁性、高效性、安全性和健壮性的需要，整合了 IKEv1 的相关文档，由 RFC4306 单个文档替代。通过核心功能和默认密码算法的最小化规定，新协议极大地提高了不同 IPsec VPN 系统的互操作性。

IKEv1 存在的安全风险

- IKEv1 支持的密码算法已超过 10 年未做更新，并不支持诸如 AES-GCM、ChaCha20-Poly1305 等推荐的强密码算法。IKEv1 使用 ISALMP 头的 E 比特位来指定该头后跟随的是加密载荷，但是这些加密载荷的数据完整性校验值放在单独的 hash 载荷中。这种加密和完整性校验的分离阻碍了 v1 使用认证加密（AES-GCM），从而限制了只能使用初期定义的 AES 算法。
- 协议本身也无法防止报文放大攻击（属于 DOS 攻击）初始报文交换，IKEv1 容易被半连接攻击，响应方响应初始化报文后维护发起-响应的关系，维护了大量的关系会消耗大量的系统资源。

  针对连接的 DOS 攻击，IKEv2 协议上有针对性的解决方案。
- IKEv1 野蛮模式安全性低：野蛮模式开始信息报文不加密，存在用户配置信息泄漏的风险，当前也存在针对野蛮攻击，如：中间人攻击。

IKEv1 和 IKEv2 的区别

- **协商过程不同。**

  - IKEv1 协商安全联盟主要分为两个阶段，其协议相对复杂、带宽占用较多。IKEv1 阶段 1 的目的是建立 IKE SA，它支持两种协商模式：主模式和野蛮模式。主模式用 6 条 ISAKMP 消息完成协商。野蛮模式用 3 条 ISAKMP 消息完成协商。野蛮模式的优点是建立 IKE SA 的速度较快。但是由于野蛮模式密钥交换与身份认证一起进行无法提供身份保护。IKEv1 阶段 2 的目的就是建立用来传输数据的 IPsec SA，通过快速交换模式（3 条 ISAKMP 消息）完成协商。
  - IKEv2 简化了安全联盟的协商过程。IKEv2 正常情况使用 2 次交换共 4 条消息就可以完成一个 IKE SA 和一对 IPsec SA，如果要求建立的 IPsec SA 大于一对时，每一对 SA 只需额外增加 1 次交换，也就是 2 条消息就可以完成。

  说明

  IKEv1 协商，主模式需要 6+3，共 9 个报文；野蛮模式需要 3+3，共 6 个报文。IKEv2 协商，只需要 2+2，共 4 个报文。

- **认证方法不同。**

- 数字信封认证（hss-de）仅 IKEv1 支持（需要安装加密卡），IKEv2 不支持。
- IKEv2 支持 EAP 身份认证。IKEv2 可以借助 AAA 服务器对远程接入的 PC、手机等进行身份认证、分配私网 IP 地址。IKEv1 无法提供此功能，必须借助 L2TP 来分配私网地址。
- IKE SA 的完整性算法支持情况不同。IKE SA 的完整性算法仅 IKEv2 支持，IKEv1 不支持。

- **DPD 中超时重传实现不同。**

- retry-interval 参数仅 IKEv1 支持。表示发送 DPD 报文后，如果超过此时间间隔未收到正确的应答报文，DPD 记录失败事件 1 次。当失败事件达到 5 次时，删除 IKE SA 和相应的 IPsec SA。直到隧道中有流量时，两端重新协商建立 IKE SA。
- 对于 IKEv2 方式的 IPsec SA，超时重传时间间隔从 1 到 64 以指数增长的方式增加。在 8 次尝试后还未收到对端发过来的报文，则认为对端已经下线，删除 IKE SA 和相应的 IPsec SA。

- **IKE SA 与 IPsec SA 超时时间手工调整功能支持不同。**

  IKEv2 的 IKE SA 软超时为硬超时的 9/10±一个随机数，所以 IKEv2 一般不存在两端同时发起重协商的情况，故 IKEv2 不需要配置软超时时间。

IKEv2 相比 IKEv1 的优点

- 简化了安全联盟的协商过程，提高了协商效率。
- 修复了多处公认的密码学方面的安全漏洞，提高了安全性能。
- 加入对 EAP（Extensible Authentication Protocol）身份认证方式的支持，提高了认证方式的灵活性和可扩展性。
- EAP 是一种支持多种认证方法的认证协议，可扩展性是其最大的优点，即如果想加入新的认证方式，可以像组件一样加入，而不用变动原来的认证体系。当前 EAP 认证已经广泛应用于拨号接入网络中。
- IKEv2 使用基于 ESP 设计的加密载荷，v2 加密载荷将加密和数据完整性保护关联起来，即加密和完整性校验放在相同的载荷中。AES-GCM 同时具备保密性、完整性和可认证性的加密形式与 v2 的配合比较好。

6.15.1.16 VPN 使用的 DH group 对应的比特位是多少？

Diffie-Hellman(DH)组确定密钥交换过程中使用的密钥的强度。较高的组号更安全，但需要额外的时间来计算密钥。

VPN 使用的 DH group 对应的比特位如表 6-5 所示。

表6-5 DH group 对应比特位

DH group	Modulus
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits

DH group	Modulus
15	3072 bits
16	4096 bits
19	ecp256 bits
20	ecp384 bits
21	ecp521 bits

说明

以下 DH 算法有安全风险，不推荐使用：DH group 1、DH group 2、DH group 5。

6.15.1.17 是否可以通过 VPN 实现跨境访问网站？

不支持。

VPN 实现的是将云上的 VPC 子网和用户侧数据中心的 IDC 网络打通的场景，即站点与站点互通（site to site）。

6.15.1.18 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联？

VPN 连通的是两个子网，即云上 VPC 网络与用户数据中心网络。

VPN 成功建立后，两个子网间可以运行任何类型的业务流量，此时应用服务器访问数据库业务在逻辑上和访问同一局域网的其它主机是相同的，因此该方案可行的。

这种场景是 IPsec VPN 的典型场景，请用户放心使用。

同时 VPN 连通以后，并不限定业务的发起方是云上还是用户侧数据中心，即用户可以从云上向用户侧数据中心发起业务，也可以反向。

须知

- 用户在打通 VPN 以后，需要关注网络延迟和丢包情况，避免影响业务正常运行。
- 建议用户先运行 ping，获取网络的丢包和时延情况。

6.15.1.19 IPsec VPN 和 SSL VPN 在使用场景和连接方式上有什么区别？

使用场景

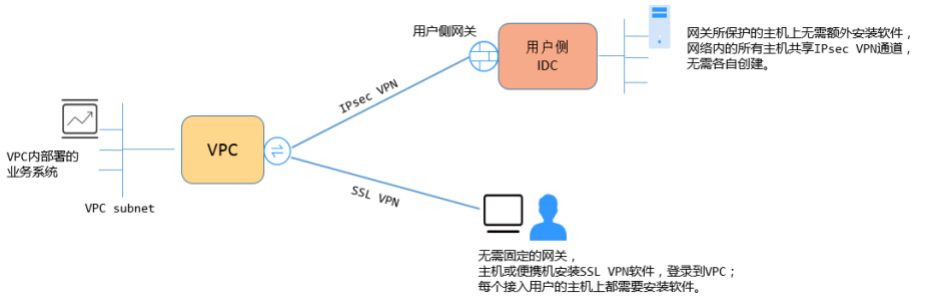
IPsec VPN：连通的是两个局域网，如分支机构与总部（或 VPC）之间、本地 IDC 与云端 VPC 的子网；即 IPsec VPN 是网对网的连接。

SSL VPN：连通的是一个客户端到一个局域网络，如出差员工的便携机访问公司内网。

连接方式

IPsec VPN：要求两端有固定的网关设备，如防火墙或路由器； 管理员需要分别配置两端网关完成 IPsec VPN 协商。

SSL VPN：需要在主机上安装指定的 Client 软件，通过用户名/密码拨号连接至 SSL 设备。



说明

VPN 目前仅支持 IPsec VPN，不支持 SSL VPN。

6.15.1.20 通过 VPN 互访的主机需要购买 EIP 吗？

如果用户本地的主机通过 VPN 访问云上的 ECS，此时 ECS 不需要购买 EIP。

如果 ECS 要向公网用户提供服务，需要购买 EIP。

6.15.1.21 Console 界面在哪添加 VPN 远端路由？

云端在 VPN 连接创建时会自动下发远端子网路由，无需手动配置。

6.15.1.22 VPN 连接中断后会通知我吗？

VPN 连接的状态监控功能已上线，VPN 连接创建后即会向 CES 上报状态信息，但是并不会自动向用户发送告警通知，需要在服务列表中选择“管理与监管 ＞ 云监控”创建告警规则。

创建 VPN 连接后，在 VPN 连接列表页面选择“操作 ＞ 更多 ＞ 查看监控”，可以跳转到 VPN 连接监控页面。

6.15.1.23 如何解决 VPN 无法建立连接问题？

1. 检查云上 VPN 连接中的 IKE 策略和 IPsec 策略中的协商模式和加密算法是否与远端配置一致。
   a. 如果第一阶段 IKE 策略已经建立，第二阶段的 IPsec 策略未开启，常见情况为 IPsec 策略与数据中心远端的配置不一致。
   b. 如果客户本地侧使用的是 CISCO 的物理设备，建议客户使用 MD5 算法。同时将云上 VPN 连接端 IPsec 策略中的认证算法设置为 MD5。
2. 检查 ACL 是否配置正确。

假设您的数据中心的子网为 192.168.3.0/24 和 192.168.4.0/24，VPC 下的子网为 192.168.1.0/24 和 192.168.2.0/24，则你在数据中心或局域网中的 ACL 应对你的每一个数据中心子网配置允许 VPC 下的子网通信的规则，如下例：

```
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
```

3. 配置完成后检查 VPN 是否连接，ping 测试两端内网是否正常。

6.15.1.24 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？

云上用户购买的 VPN 网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下两种情况：

- 如果所购买的带宽<=10Mbit，则入云方向统一限定为 10Mbit。
- 如果所购买的带宽>10Mbit，则入云方向与购买的带宽一致。

按带宽计费度量采用国际统一的带宽单位 Mbit，按流量计费的度量单位为 GByte。

6.15.2 组网与使用场景

6.15.2.1 连接云下的多台服务器需要购买几个连接？

VPN 属于 IPsec VPN，它是用于打通云上 VPC 和用户侧数据中心子网的 VPN，所以购买 VPN 连接的个数与服务器的数量无关，而与这些服务器所在的数据中心数量有关。

大部分情况下一个用户侧数据中心会有一个公网出口网关，所有服务器（或用户主机）都通过该网关连接至 Internet，因此对于这种情况配置一个 VPN 连接即可，通过该连接即可打通 VPC 与用户网络之间的流量。

6.15.2.2 多人访问 ECS，是否可以给每个客户机安装一套 IPsec 软件和云端建立 VPN 连接？

不可以。

VPN 打通的是两个局域网的网络，用户侧数据中心局域网内多台主机都安装 IPsec 软件，实际情况是用户侧数据中心多个主机使用同一个公网 IP 与云端对接，云端的 VPN 网关会收到来自用户侧数据中心不同主机的协商报文，系统会收到大量的重复协商信息，导致连接异常，甚至出现连接不可用的现象。

建议您使用出口的防火墙设备配置 VPN 与云端进行对接。建立 VPN 时可以选择多个网段，结合云上安全组或用户侧数据中心安全策略，限定属于开发人员主机才能访问云端 ECS。

6.15.2.3 VPN 支持将两个 VPC 互连吗？

- 如果两个 VPC 位于同一区域内，不支持 VPN 互连，推荐使用 VPC 对等连接互连。
- 如果两个 VPC 位于不同区域，支持 VPN 互连，具体操作如下：
  a. 为这两个 VPC 分别创建 VPN 网关，并为两个 VPN 网关创建 VPN 连接。
  b. 将两个 VPN 连接的远端网关设置为对方 VPN 网关的网关 IP。

c. 将两个 VPN 连接的远端子网设置为对方 VPC 的网段。

d. 两个 VPN 连接的预共享密钥和算法参数需保持一致。

6.15.2.4 使用 VPN 会对本地网络造成哪些影响，访问云端主机在路由上会有哪些变化？

配置 VPN 时，用户需要在用户侧数据中心的网关上增加以下 VPN 配置信息：

1. IKE/IPsec 策略配置。
2. 指定感兴趣流（ACL）。
3. 用户需要审视用户侧数据中心网关的路由配置，确保发往 VPC 的流量被路由到正确的出接口（即绑定 IPsec 策略的接口）。

在完成 VPN 配置后，只有命中感兴趣流的流量会进入 VPN 隧道，其它网络的访问都不受影响。

例如，云端的 ECS 绑定的 EIP，在未创建 VPN 前，本地用户访问云端主机都通过 EIP 访问，创建 VPN 后，数据流匹配了 ACL 后会通过 VPN 隧道访问云端 ECS 的私网 IP。

6.15.2.5 通过 VPN 来实现云下 IDC 与云端 VPC 的互通，两端分别需要做哪些配置？

VPN 对接的工作分为两个部分：云上创建 VPN 和用户侧数据中心配置 VPN 设备。

- 云上创建 VPN：购买 VPN 网关，选定计费模式、带宽大小、指定对接的 VPC；购买 VPN 连接，指定两端网关 IP，两端子网和协商策略。
- 用户侧数据中心配置 VPN 设备：选定用户侧数据中心公网 IP，在支持 IPsec VPN 的设备上完成 IPsec 协商的一、二阶段配置，然后进行网络路由、NAT 和安全策略配置。

6.15.2.6 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置？

不可以。

云端创建 VPN 时，本端子网为 VPC 内部子网，远端子网为客户用户侧数据中心子网，两条连接使用相同的本端子网和远端子网是无法进行创建的。

6.15.2.7 同一个 Region 的两个 VPC 可以通过 VPN 连通吗？

不可以。

对于同 Region 的两个 VPC，您可以通过对等连接（VPC peering）打通两个 VPC。

6.15.2.8 使用 VPN 替换专线该如何配置？

1. 首先需要确认用户侧数据中心设备支持 IPsec VPN。
2. 然后在云上创建一个 VPN 网关（请注意选择原专线所属的 VPC）和 VPN 连接。

须知

配置 VPN 连接时需要注意，因为远端子网与专线远端子网一样，不能直接配置，否则会产生路由冲突。 可采用以下方案:

- 先删除专线 VIF，再配置 VPN 连接。
- 将远端子网分拆为两个细分子网再配置 VPN 连接，等专线删除之后，再改为正常的子网配置。

6.15.2.9 云端创建了两个 VPC，如何与云下的 IDC 网络互通？

组网拓扑

IDC-VPC1-VPC2。

说明

其中 IDC 表示用户数据中心，VPC1 与 IDC 建立 VPN 连接。

配置步骤

1. 确认云上的两个 VPC 是否在同一 Region。
   - 如果在同一 Region 可通过对等连接将两个 VPC 连接起来（免费）。
2. 用户侧数据中心 IDC 与其中一个 VPC 建立 VPN 连接，修改用户侧数据中心设备的远端子网为云上两个 VPC 子网，VPN 对接的 VPC1 本端子网需要包含通过对等连接的子网，对等连接的子网路由包含用户侧数据中心 IDC 子网。

6.15.2.10 组网拓扑如（IDC1-VPC1-VPC2-IDC2），如何实现四个子网互联？

组网拓扑

IDC1-VPC1-VPC2-IDC2。

说明

其中 IDC1、IDC2 表示用户数据中心，VPC1、VPC2 分别与 IDC1、IDC2 建立 VPN 连接。

配置步骤

1. IDC1 可通过 VPN 与 VPC1 互联。
2. 同 Region 的两个 VPC 之间使用 VPC 对等连接互连。
3. IDC2 可通过 VPN 与 VPC2 互联。
4. 同时完成 VPN 子网更新、VPC 对等连接子网路由更新即可实现四个子网相互访问。

6.15.2.11 云端两个 Region，每 Region 有两个子网，是否可以创建两个 VPN 连接，分别连通不同子网？

不可以。

两个 Region 间只需创建一个 VPN 连接即可，在 VPN 连接中将两个子网都加入到 VPN 中。

针对这种场景，如果用户试图去创建第二条 VPN 连接，由于两个连接的远端网关地址一样，因此管理控制台界面会提示冲突。

6.15.2.12 VPN 和 OBS 可以直接通信吗？

可以。

用户站点通过 VPN 访问 OBS 服务，需要使用 VPC 终端节点服务。需要为内网 DNS 和 OBS 分别申请两个终端节点。

然后在用户侧配置云的内网 DNS 和路由

6.15.2.13 用户本地电脑如何连接云上 VPN？

普通家庭宽带路由器、个人的移动终端设备、Windows 主机自带的 VPN 服务（如 L2TP）无法与云的 VPN 进行对接。

与云下对接需要对端有支持标准 IPsec 协议的设备。

6.15.2.14 公司网络已通过 VPN 连通了云，我如何在家访问 ECS？

VPN 为 IPsec VPN，是连接云上 VPC 和云下局域网的。

家庭网络非公司局域网络的组成部分，无法直接和云上 VPC 实现互联。

居家办公主机需要访问云上 VPC 资源可以考虑直接访问云服务的 EIP，或通过 SSL VPN（需公司支持 SSL 接入）先连接至公司局域网，然后通过公司局域网访问云上 VPC 资源。

6.15.2.15 购买 VPN 网关和连接后，发现云下没有支持 IPsec 的设备，如何临时建立 VPN 连接？

与云进行 VPN 连通时，需要云下有支持标准的 IPsec 设备和固定公网 IP，二者缺一不可。

如果需要临时与云对接，可通过在主机上安装第三方软件完成与云的对接。

第三方 IPsec 软件推荐：strongSwan、Openswan、The GreenBow 等。

6.15.2.16 如何选择在云上的哪个区域创建 VPN 网关？

在云上创建 VPN 网关，您可用选择任一区域的 VPC 进行创建。

推荐您选择与 IDC 同城的区域创建 VPN 网关，这样可以更大程度降低因公网质量对 VPN 的影响。

- 同区域的多个 VPC，只需创建一个 VPN 网关，其它 VPC 可以通过对等连接（免费）打通。

6.15.3 Console 与页面使用

6.15.3.1 VPN 配置下发后，多久能够生效？

用户在管理控制台完成 VPN 资源创建后，配置 1-5 分钟下发完成，下发后立即生效。

说明

VPN 配置下发成功后，并不表示 VPN 连接已经建立成功，用户还需要对用户侧网关设备进行配置，完成与 VPN 网关的隧道协商。

6.15.3.2 VPN 配置完成了，为什么连接一直处于未连接状态？

首先需要确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/远端子网、本端网关/远端网关互为镜像。

其次确认用户侧数据中心设备的路由、NAT 和安全策略配置无误，最后通过两端的子网互 PING 对端子网主机。

说明

因为 VPN 是基于数据流触发的，在配置完成后需要从任一端子网主机 ping 对端子网主机，ping 之前请关闭主机防火墙，云上安全组开启入方向 ICMP。

ping 网关 IP 无法触发 VPN 协商，需要 ping 网关保护的子网中的主机。

6.15.3.3 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置？

用户侧数据中心配置 VPN 设备时，是需要独立创建 ACL，且该 ACL 会被 IPsec 的策略引用。

云上配置 VPN 服务时，会根据管理控制台界面填入的本端子网和远端子网自动生成 ACL，然后下发给 VPN 网关。其中 ACL 中的 rule 数量是两端子网数量的乘积。

6.15.3.4 Console 界面在哪添加 VPN 远端路由？

云端在 VPN 连接创建时会自动下发远端子网路由，无需手动配置。

6.15.3.5 创建 VPN 连接时如何关闭 PFS 的 Group 配置？

云在部分区域开启了 PFS 的 Disable 选项，推荐用户侧数据中心也开启 PFS 的 Group 配置。

PFS 功能可以增强 IKE 二阶段协商的安全性，建议用户开启功能。

部分设备厂商默认关闭了 PFS 功能，请用户查询设备配置手册确保 PFS 功能打开。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。

IKE 协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致 IPsec VPN 受到侵犯。为提升密钥管理的安全性，IKE 提供了 PFS（完美向前保密）功能。启用 PFS 后，在进行 IPsec SA 协商时会进行一次附加的 DH 交换，重新生成新的 IPsec SA 密钥，提高了 IPsec SA 的安全性。

- 为了增强安全性，云默认开启 PFS，请用户在配置用户侧数据中心网关设备时确认也开启了该功能，否则会导致协商失败。

6.15.3.6 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接？

VPN 连接状态刷新存在一定的延迟，业务已通但是网页上 VPN 连接状态还是未连接是正常现象。

如果数据面已正常（即业务访问已正常）， 连接就已经完成建立了，短暂等待后 VPN 连接状态就会更新为“已连接”。

6.15.3.7 修改协商策略后，页面显示资源不存在，如何处理？

此问题为页面刷新周期问题。

在修改连接高级策略时，系统会先删除，再重建 VPN 连接，如果在页面创建过程中出现短暂的删除中或创建中属于正常现象，切勿重复创建同一连接（本端子网、远端子网、远端网关相同的连接）；

6.15.3.8 如何重置已经建立的 VPN 连接？

- 在线下设备上关闭 VPN 连接，待云上 VPN 连接状态变为未连接后重新启动线下设备上的 VPN 连接；
- 更改线上 VPN 连接的远端网关 IP 为其它任意 IP，待云下连接状态变为 inactive 后，重新将云上的远端网关 IP 修改为之前的 IP。

6.15.4 VPN 协商与对接

6.15.4.1 使用 VPN 连通云端 VPC 网络，云下设备如何配置？

首先按照网络的连接规划，明确用户侧数据中心子网、云上子网以及两端的网关公网 IP 信息。

其次按照云端 VPN 的协商策略信息完成用户侧数据中心设备的 IPsec 配置，并开启云上 VPC 主机关联的安全组的出入方向的 ICMP 报文。

- 路由设置：用户侧数据中心设备从子网的网关设备开始至 VPN 对接设备，逐跳添加去往云端子网的路由，下一跳指向连接 VPN 设备出方向的路由，在 VPN 设备上的路由指向出接口下一跳公网网关 IP。
- NAT 设置：在 VPN 设备上关闭本地子网访问云端子网的 NAT，即本端子网访问云端子网不做 NAT。最后在安全策略中双向放行本地子网和云端子网互访，双向放行云端 VPN 网关 IP 与本地 VPN 设备对接使用的公网 IP 的 UDP500、UDP4500、ESP(IP protocol 50)、AH(IP protocol 51)报文。

6.15.4.2 VPN 支持远端网关域名对接吗？

云端 VPN 连接需要明确对端的公网 IP 地址，暂不支持通过域名方式与对端设备进行对接。

6.15.4.3 我创建的 VPN 连接有几个隧道？

VPN 连接下的隧道和本端子网和远端子网的数量有关，隧道总数等于本端子网数和远端子网数的乘积。但在实际建立隧道时，只要有一个隧道的状态 Active，连接的状态就会显示正常，如果需要每个隧道都处于 Active 状态，需要每两个子网间都进行数据流触发。

6.15.4.4 如何通过安全组控制使 VPN 不能访问 VPC 上的部分虚拟机，实现安全隔离？

如果用户需要控制 VPN 站点只能访问 VPC 的部分网段或者部分主机，可以通过安全组进行控制。

配置示例：VPC 内子网 10.1.0.0/24 下的 ECS 不允许访问客户侧的子网 192.168.1.0/24，

配置方法：

1. 创建两个安全组：安全组 1 和安全组 2。
2. 安全组 1 的入方向规则配置 deny 网段 192.168.1.0/24。
3. 安全组 2 允许 192.168.1.0/24 访问。
4. 网段 10.1.0.0/24 的 ECS 选择安全组 1，其他的主机选择安全组 2。

6.15.4.5 修改 VPN 连接的配置会造成连接重建吗？

VPN 连接包含本端子网、远端子网、远端网关、预共享密钥、IKE 协商策略、IPsec 协商策略。修改 VPN 连接具体包括以下几种情况：

- 修改本端子网和远端子网，连接 ID 不发生变化，只是更新了连接两端的子网信息，如果更新的是部分子网信息，已经建立的子网间隧道不会重建。
- 修改远端网关 IP，连接 ID 不发生变化，但连接的对端已改变，连接需要重建。
- 仅修改连接的预共享密钥，连接的 ID 不发生变化，连接状态当时并不发生改变，重协商会重新校验密码匹配情况，如果密码不匹配重协商会失败。
- 修改协商策略（需验证预共享密钥），连接 ID 发生改变，相当于连接删除重建过程，连接需要重建。

6.15.4.6 云对接 AWS 后，为何不可以从 AWS 向云发起协商？

VPN 建立连接完成后，AWS 为 Response 模式，并不主动发起协商，当从 AWS 的 EC2 向云 ECS 发起数据流时，也不触发该 VPN 建立 SA。

请按照 AWS 的知识文档，只能从客户侧（即对接 AWS 的云）发起协商。

6.15.4.7 对接云时，如何配置 DPD 信息？

云默认开启 DPD 配置，且不可关闭该配置。

DPD 配置信息如下：

- DPD-type：按需
- DPD idle-time：30s
- DPD retransmit-interval：15s
- DPD retry-limit：3 次
- DPD msg：seq-hash-notify。

两端 DPD 的 type、空闲时间、重传间隔、重传次数无需一致，只要能接收和回应云的 DPD 探测报文即可，DPD msg 格式必须一致。

6.15.4.8 本地防火墙无法收到 VPN 网关的 IKE 第一阶段的回复包怎么解决？

1. 检查两端公网 IP 是否可以互访，推荐使用 ping 命令，云端网关 IP 缺省可以 ping 通。
2. 云下网关与云网关可以互访 UDP 500、4500 报文。
3. 云下公网 IP 访问网关 IP 时，没有发生源端口 NAT 转换，如果存在 nat 穿越，端口号在 nat 穿越后不得发生改变。
4. 两端的 ike 协商参数配置一致，nat 穿越场景中云下 ID 标识类型选择 IP，本地的标识选择 NAT 转换后的公网 IP。

6.15.4.9 本地防火墙无法收到 VPN 子网的回复包怎么解决？

1. 如果二阶段协商中需要检查云下的路由、安全策略、NAT 和感兴趣流、协商策略信息。
   - 路由设置：将访问云上子网的数据送入隧道。
   - 安全策略：放行云下子网访问云上子网的流量。
   - NAT 策略：云下子网访问云上子网不做源 nat。
   - 感兴趣流：两端感兴趣流配置互为镜像，使用 IKE v2 配置刚兴趣流不可使用地址对象名称。
   - 协商信息：协商策略信息云上云下一致，特别注意 PFS 的配置。
2. 确认一、二阶段协商均已正常后，请检查云上安全组策略，放行入方向的云下子网访问云上子网的 ICMP 协议。

6.15.5 连接故障或无法 PING 通

6.15.5.1 如何防止 VPN 连接出现中断情况？

VPN 连接在正常的使用过程中会存在重协商情况，触发重协商的条件有 IPsec SA 的生命周期即将到期和 VPN 传输的流量超过 20GB，重协商一般不造成连接中断。

大多数的连接中断都是因为两端的配置信息错误造成的，或公网异常导致重协商失败造成的。

常见的连接中断原因有：

- 两端的 ACL 不匹配；
- SA 生命周期不匹配；

- 用户侧数据中心未配置 DPD；
- VPN 使用过程中修改了配置信息；
- 数据超过 MTU 后导致报文分片；
- 运营商网络抖动。

因此请在配置 VPN 时确保操作和配置，以进行连接状态保活：

- 两端的子网配置互为镜像；
- SA 生命周期信息一致；
- 用户侧数据中心网关开启 DPD 配置，探测次数不少于 5 次；
- 连接过程中修改参数两侧同步修改；
- 设置用户侧数据中心设备 TCP MAX-MSS 为 1300；
- 确保用户侧数据中心出口有足够的带宽可被 VPN 使用；
- 确认 VPN 连接可被两端触发协商，开启用户侧数据中心设备的主动协商配置；
- 两端子网进行长 Ping 操作（脚本内容如下）。

```
#!/bin/sh
host=$1
if [ -z $host ]; then
   echo "Usage: `basename $0` [HOST]"
   exit 1
fi
log_name=$host".log"

while :; do
   result=`ping -W 1 -c 1 $host | grep 'bytes from '`
   if [ $? -gt 0 ]; then
      echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is down"| tee -a
$log_name
   else
      echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is ok -`echo $result |
cut -d ':' -f 2`"| tee -a $log_name
   fi
sleep 5 # avoid ping rain
done
#./ping.sh x.x.x.x >>/dev/null &
```

说明

1. 通过 VI 编辑器将以上脚本粘贴在 ping.sh 文本中。
2. 给文件授权 chmod 777 ping.sh。
3. 使用文件执行 ping 命令：

   ./ping.sh x.x.x.x >>/dev/null &

   x.x.x.x 是您需要 ping 的远端目标 IP。
4. 执行 ping 命令后，后台运行并生成 x.x.x.x.log 文件，执行命令：

   tail -f x.x.x.x.log

   可以实时查看长 ping 结果。

6.15.5.2 使用中 IPsec VPN 连接中断后如何快速恢复？

1. 通过私网数据流重新触发 IPsec 协商。比如两端私网间进行互 Ping，如果流量触发可正常建立请考虑部署长 Ping 保活脚本。详细请参见6.15.10.1 如何防止 VPN 连接出现中断情况？。
2. 如果无法正常触发协商，请检查 IPsec 两侧公网 IP 的连通性，比如两个公网 IP 互 Ping 验证。VPN 网关 IP 默认回应 ICMP 报文。
3. 如果公网链路正常，需排查是否存在多出口的链路切换，即当前访问云网关 IP 流量未从协商端口流出。
4. 如果无多出口或出口路径正常，可尝试隧道两端同时修改一次 PSK，重新触发协商。
5. 如果重新触发协商失败，请确认两端配置的协商策略是否一致、感兴趣流是否互为镜像（条目数、掩码均相同）。
6. 如果协商策略和感兴趣流配置无误，请关停云下设备的 VPN 连接，等待云端连接显示为“未连接”后，重启云下设备 VPN 连接，并进行数据流触发。
7. 如果依然无法触发协商时，请执行以下操作：
   a. 记录 VPN 连接的协商策略、PSK、本端子网、远端网关、远端子网。
   b. 使用现有网关新建一条连接，协商策略、PSK、本端子网均与原连接相同，远端网关和远端子网先任意填写。
   c. 待新创建连接成功后，删除原连接，之后再修改新建连接的远端网关和远端子网与记录数据一致。
   d. 修改完成后重新触发协商。

6.15.5.3 VPN 网关带宽到达限额时有什么影响？

VPN 带宽限速限制的出 VPC 方向的带宽，如果您 VPN 的带宽超过限额使用时，会出现网络卡顿、部分子网间无法访问、甚至出现 VPN 连接中断现象（无法收到 VPN 的探测报文）。

因此在出现 VPN 带宽已达到上限时，建议您对 VPN 网关带宽进行扩容。

说明

VPN 的带宽最大为 300(Mbit/s)。

6.15.5.4 两个 Region 创建的 VPN 连接状态正常，为什么不能 ping 通对端 ECS？

安全组默认放行了出方向的所有端口，入方向需要按照实际需要添加放行规则，确认接收 ping 报文的 ECS 安全组放行了入方向的 ICMP。

6.15.5.5 IDC 与云端对接，VPN 连接正常，子网间业务无法互相访问？

连接状态正常，说明两端的协商参数没有问题，排查项如下：

- 用户侧数据中心设备子网路由是否从网关开始逐跳指向 VPN 出口设备。
- VPN 设备有安全设置放行了子网间的数据互访。
- IDC 子网访问云端数据不做 NAT。

- 确保两侧公网 IP（网关 IP）间访问不被阻拦。

6.15.5.6 正在使用 VPN 出现了连接中断，提示数据流不匹配，如何排查？

这通常是由于云上与用户侧数据中心设备配置的 acl 不匹配造成的。

1. 首先确认两端 VPN 连接的子网信息是否配置一致，确保云端生成的 ACL 与用户侧数据中心 ACL 配置互为镜像
2. 用户侧数据中心感兴趣流配置推荐使用“子网/掩码”的格式，避免使用网络地址对象模式，即 address object 模式，address object 为非标模式，容易引起不兼容问题。

6.15.5.7 正在使用 VPN 出现了连接中断，提示 DPD 超时，如何排查？

出现 DPD 超时的连接中断时因为两端网络访问无数据，在 SA 老化后发送 DPD 未得到对端响应而删除连接。

解决方法：

1. 开启用户侧数据中心设备的 DPD 配置，测试两端的数据流均可触发连接建立；
2. 在两端的主机中部署 Ping shell 脚本，也可在用户侧数据中心的子网的网关设备上配置保活数据，如 NQA，或 cisco 的 ip sla。

6.15.5.8 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接？

管理控制台界面中 VPN 连接状态刷新存在一定的延迟，是正常现象。

如果数据面已正常（即业务访问已正常）， 则 VPN 连接已完成建立。

6.15.5.9 VPN 建立后您的数据中心或局域网无法访问弹性云主机？

我们提供的安全组默认不允许任何源访问，请确认您的安全组是否配置允许远端的子网地址访问。

6.15.5.10 为什么 VPN 创建成功后状态显示未连接？

VPN 对接成功后两端的服务器或者虚拟机之间需要进行通信，VPN 的状态才会刷新为正常。

- IKE v1 版本：

  如果 VPN 连接经历了一段无流量的空闲时间，则需要重新协商。协商时间取决于 IPsec Policy 策略中的“生命周期（秒）”取值。“生命周期（秒）”取值一般为 3600（1 小时），会在第 54 分钟时重新发起协商。如果协商成功，则保持连接状态至下一轮协商。如果协商失败，则在 1 小时内将状态设置为未连接，需要 VPN 两端重新进行通信才能恢复为连接状态。可以使用网络监控工具（例如 IP SLA）生成保持连接的 Ping 信号来避免这种情况发生。
- IKE v2 版本：如果 VPN 连接经历了一段无流量的空闲时间，VPN 保持连接状态。

6.15.5.11 VPN 是否启动了 DPD 检测机制？

是的。

VPN 服务默认开启了 DPD 探测机制，用于探测用户侧数据中心 IKE 进程的存活状态。

3 次探测失败后即认为用户侧数据中心 IKE 异常，此时云会删除本端隧道，以保持双方的隧道同步。

DPD 协议本身并不要求对端也同步进行配置（但是要求对端可以应答 DPD 探测），为了保证协商双方隧道状态一致，避免出现单边隧道（一端存在隧道，而另一端已不存在），建议用户同时启动用户侧网关的 DPD 探测机制，用于探测云侧 VPN 服务的 IKE 状态。

说明

DPD 探测失败后会删除隧道，不会导致业务不稳定。

DPD 可以及时发现对方 IKE 进程异常，并通过重置隧道的方法来保持双方隧道同步。在删除隧道后，当有用户流量时，可以重新触发协商并建立隧道。

6.15.6 公网地址

6.15.6.1 VPN 网关删除后公网地址是否可以保留？

VPN 网关删除后不保留网关 IP。

通过管理控制台界面删除 VPN 网关后， VPN 网关相关联的资源，如公网 IP，配置信息即被释放，不会保留。

须知

在按需计费模式下，删除最后一个连接会同步删除网关，用户如果需要保留公网 IP，请确保不要删除最后一个 VPN 连接。

6.15.6.2 EIP 能作为 VPN 的网关 IP 吗？

不可以。

VPN 网关 IP 是在创建 VPN 网关时分配的，需要和系统内的相关配置信息结合使用，EIP 不具备 VPN 对接服务的功能。

6.15.6.3 通过 VPN 互访的主机需要购买 EIP 吗？

如果用户本地的主机通过 VPN 访问云上的 ECS，此时 ECS 不需要购买 EIP。

如果 ECS 要向公网用户提供服务，需要购买 EIP。

6.15.6.4 为什么我开通 VPN 后，云端 ECS 会有公网 IP 的访问信息？

此现象多因您在 VPN 对接之前，ECS 绑定了 EIP。即用户除了通过 VPN，也可通过公网地址直接访问该 ECS。

VPN 打通后，在感兴趣流内的主机访问云端 ECS 时会封装在隧道中。

- 如果 ECS 绑定了 EIP，则非 VPN 网络中的设备仍可通过 EIP 直接访问该 ECS。
- 如果 ECS 主机只允许 VPN 内的主机访问，可在完成 VPN 对接后将 ECS 的 EIP 解绑。当 ECS 需要绑定 EIP 时，可通过 ACL 来限定哪些流量可以通过 EIP 访问该 ECS。

说明

用户是否要保留 EIP，与业务类型相关。如用户 ECS 可以通过 VPN 获取用户侧数据中心的数据，同时该 ECS 还向互联网用户提供服务（如 web server），此时就需要保留 EIP。

6.15.6.5 用户侧数据中心的网关设备没有固定的公网 IP 可以吗？

不可以。

用户数据中心与云进行 VPN 对接时，要求用户侧数据中心有固定的公网 IP 或者经过 NAT 映射后的固定公网 IP（即 NAT 穿越，VPN 设备在 NAT 网关后部署）。

说明

普通家庭宽带路由器、个人的移动终端设备、Windows 主机自带的 VPN 服务（如 L2TP）无法与云的 VPN 进行对接。

6.15.7 路由设置

6.15.7.1 如何理解 VPN 连接中的远端网关和远端子网？

远端网关和远端子网是两个相对的概念，在建立 VPN 连接时，从云的角度出发，VPC 网络就是本地子网，创建的 VPN 网关就是本地网关，与之对接的用户侧网络就是远端子网， 用户侧的网关就是远端网关。

远端网关 IP 就是用户侧网关的公网 IP，远端子网指需要和 VPC 子网互联的子网。

6.15.7.2 Console 界面在哪添加 VPN 远端路由？

云端在 VPN 连接创建时会自动下发到达远端子网的路由，无需手动配置。

6.15.7.3 ECS 主机多网卡是否需要添加去往线下网络的路由？

- 如果客户使用主网卡与线下网络建立了 VPN，不需要添加路由。
- 如果客户使用非主网卡与线下网络建立了 VPN，需要添加去往线下网段的路由指向非主网卡的网关。

6.15.8 VPN 子网设置

6.15.8.1 配置 VPN 连接的本端子网和远端子网时需要注意什么？

- 子网数量满足规格限制，数量超出规格限制请进行聚合汇总。
- 本端子网不可以包含远端子网，远端子网可以包含本端子网。
- 推荐配置的本端子网在 VPC 内有路由可达。
- 同一个 VPN 网关创建两条连接：若这两条连接的远端子网存在包含关系，在访问的目的网络处于交集网段部分时，按照创建连接的先后顺序匹配 VPN 连接，且与连接状态无关（策略模式不能按照掩码长度进行匹配）。

6.15.8.2 VPN 本端子网和远端子网的数量有限制吗，为什么我选择网段更新本地子网提示报错？

- 本端子网限制数量为 5 个，VPN 本端子网和远端子网数量乘积最大支持到 225。
- VPC 会根据 VPN 连接的远端子网、云专线的远端子网、VPC 对等连接子网下发 VPC 子网路由，每个子网网段对应一条子网路由。
- VPC 子网路由条目数不得大于 200，即同一个 VPC 中所有 VPN 连接的远端子网数、专线的远端子网数、VPC 对等连接子网数以及自定义路由条目数的总和不得大于 200。

6.15.8.3 创建 VPN 连接时添加远端子网，提示系统异常，如何处理？

检查 VPC 内是否存在对等连接、云专线的子网路由使用了该子网，导致 VPN 下发子网路由冲突，确认后将其配置的子网路由删除后重新创建即可。

6.15.8.4 VPN 接入 VPC 的网络地址如何规划？

- 云上 VPC 地址段和客户云下的地址段不能冲突，且不允许存在包含关系。
- 为避免和云服务地址冲突，用户侧网络应尽量避免使用 127.0.0.0/8、169.254.0.0/16、224.0.0.0/3、100.64.0.0/10 的网段。

6.15.8.5 创建 VPN 网关时 IP 是如何分配的？

VPN 网关 IP 是一组提前规划好的地址组，提前预制了 VPN 的相关配置。

在用户创建 VPN 网关时，系统会随机分配一个 IP 地址和 VPC 进行绑定，且这个 IP 地址也只能绑定 1 个 VPC。

因为 VPN 的网关 IP 存在预置数据，所以 VPN 网关 IP 和 EIP 不能转换，在创建 VPN 网关时也不能指定 IP 地址。删除 VPN 网关时会释放 IP 地址与 VPC 的绑定关系；重新创建 VPN 网关时系统会重新随机分配网关 IP 地址。

6.15.9 VPN 感兴趣流

6.15.9.1 本地设备配置 VPN 时需要设置 ACL，为何在 Console 上找不到对应的配置？

用户侧数据中心配置 VPN 设备时，是需要独立创建 ACL，且该 ACL 会被 IPsec 的策略引用。

云上配置 VPN 服务时，会根据管理控制台界面填入的本端子网和远端子网自动生成 ACL，然后下发给 VPN 网关，其中 ACL 中的 rule 数量是两端子网数量的乘积。

6.15.9.2 如何配置和修改云上 VPN 的感兴趣流？

感兴趣流由本端子网与远端子网 full-mesh 生成，例如本端子网有 2 个，分别为 A 与 B，远端子网有 3 个，分别为 C、D 和 E，生成感兴趣流 ACL 的 rule 如下：

```
rule 1 permit ip source A destination C
rule 2 permit ip source A destination D
rule 3 permit ip source A destination E
rule 4 permit ip source B destination C
```

```
rule 5 permit ip source B destination D
rule 6 permit ip source B destination E
```

在管理控制台界面修改本端子网和远端子网会自动更新 VPN 设备的感兴趣流信息，即修改了云上的 ACL 配置。

6.15.10 VPN 连接保活

6.15.10.1 如何防止 VPN 连接出现中断情况？

VPN 连接在正常的使用过程中会存在重协商情况，触发重协商的条件有 IPsec SA 的生命周期即将到期和 VPN 传输的流量超过 20GB，重协商一般不造成连接中断。

大多数的连接中断都是因为两端的配置信息错误造成的，或公网异常导致重协商失败造成的。

常见的连接中断原因有：

- 两端的 ACL 不匹配；
- SA 生命周期不匹配；
- 用户侧数据中心未配置 DPD；
- VPN 使用过程中修改了配置信息；
- 数据超过 MTU 后导致报文分片；
- 运营商网络抖动。

因此请在配置 VPN 时确保操作和配置，以进行连接状态保活：

- 两端的子网配置互为镜像；
- SA 生命周期信息一致；
- 用户侧数据中心设备开启 DPD 配置，探测次数不少于 5 次；
- 连接过程中修改参数两侧同步修改；
- 设置用户侧数据中心设备 TCP MAX-MSS 为 1300；
- 确保用户侧数据中心出口有足够的带宽可被 VPN 使用；
- 确认 VPN 连接可被两端触发协商，开启用户侧数据中心设备的主动协商配置；
- 两端子网进行长 Ping 操作（脚本内容如下）。

```
#!/bin/sh
host=$1
if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi
log_name=$host".log"

while :; do
    result=`ping -W 1 -c 1 $host | grep 'bytes from '`
    if [ $? -gt 0 ]; then
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is down"| tee -a
$log_name
    else
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is ok -`echo $result |
```

```
cut -d ':' -f 2`"| tee -a $log_name
   fi
sleep 5 # avoid ping rain
done
#./ping.sh x.x.x.x >>/dev/null &
```

说明

1. 通过 VI 编辑器将以上脚本粘贴在 ping.sh 文本中。
2. 给文件授权 chmod 777 ping.sh。
3. 使用文件执行 ping 命令：

   ./ping.sh x.x.x.x >>/dev/null &

   x.x.x.x 是您需要 ping 的远端目标 IP。
4. 执行 ping 命令后，后台运行并生成 x.x.x.x.log 文件，执行命令：

   tail -f x.x.x.x.log

   可以实时查看长 ping 结果。

6.15.11 监控类

6.15.11.1 VPN 监控可以监控哪些内容？

VPN 网关

可监控带宽信息包含入网流量、入网带宽、出网流量、出网带宽及出网带宽使用率；查询网关监控状态请在 VPN 网关列表中选择“操作 > 查看监控”即可。

VPN 连接

可监控连接的状态，1 为正常、0 为未连接；查询 VPN 连接监控请在 VPN 连接列表中选择“操作 > 更多 > 查看监控”。

6.15.11.2 VPN 连接中断后会通知我吗？

VPN 连接的状态监控功能已上线，VPN 连接创建后即会向 ces 上报状态信息，但是并不会自动向用户发送告警通知，需要在服务列表中选择“管理与监管 > 云监控”创建告警规则。

创建 VPN 连接后，在 VPN 连接列表页面选择“操作 > 更多 > 查看监控”，可以跳转到 VPN 连接监控页面。

6.15.11.3 VPN 监控能不能查看每条连接的流量？

VPN 的流量监控是基于 VPN 网关的，可查看该 VPN 网关的出入方向的流量、带宽等信息，无法查看单独的某一条连接的流量使用情况。

6.15.12 带宽与网速

6.15.12.1 如何测试 VPN 速率情况？

当测试环境为已创建 VPN 连接，并在 VPN 连接的本端子网下创建 ECS，并使其相互能够 ping 通的情况下，测试 VPN 的速率情况。

当用户购买的 VPN 网关的带宽为 200Mbit/s 时，测试情况如下。

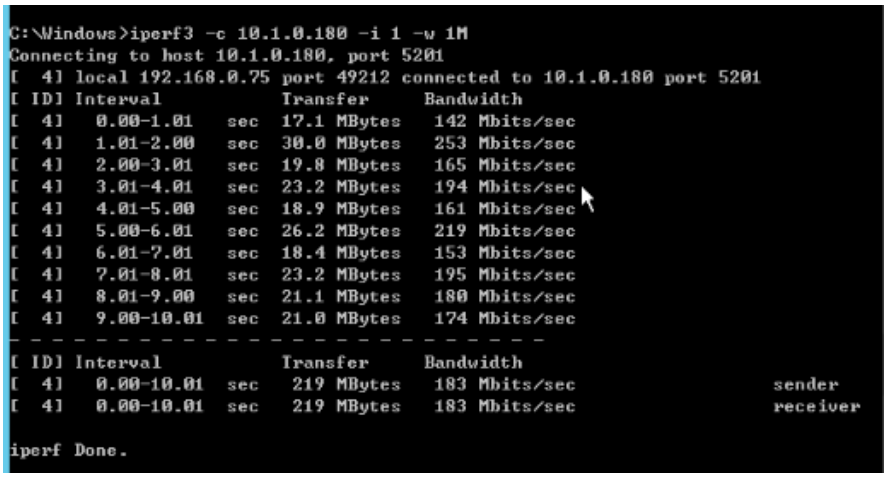
1. 互为对端的 ECS 都使用 Windows 系统，测试速率可达 180Mbit/s，使用 iperf3 和 filezilla（是一款支持 ftp 的文件传输工具）测试均满足带宽要求。

说明

基于 TCP 的 FTP 协议有拥塞控制机制，180Mbit/s 为平均速率，且 IPsec 协议会增加新的 IP 头，因此 10%左右的速率误差在网络领域是正常现象。

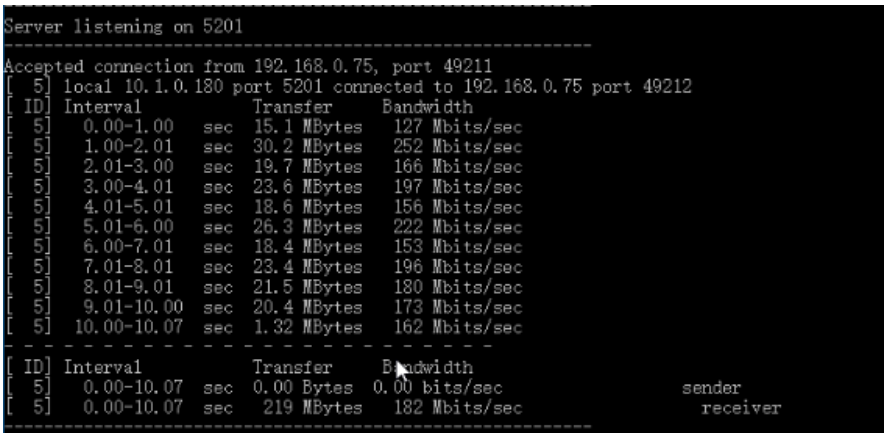
使用 iperf3 客户端测试结果截图如图 6-8 所示。

图6-8 200M 带宽客户端 iperf3 测试结果



使用 iperf3 服务器端测试结果截图如图 6-9 所示。

图6-9 200M 带宽服务端 iperf3 测试结果

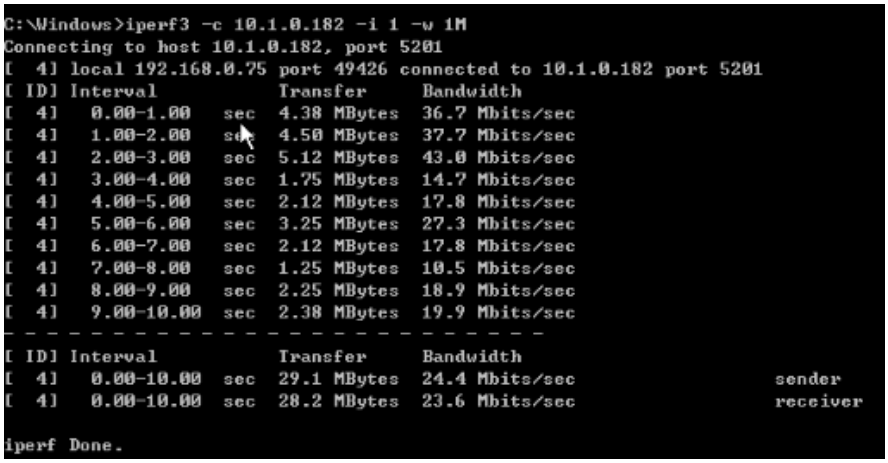


2. 互为对端的 ECS 都使用 Centos7 系统，测试速率可达 180M，使用 iperf3 测试满足带宽要求。
3. 服务器端 ECS 使用 Centos7 系统，客户端使用 Windows 系统，测试速率只有 20M 左右，使用 iperf3 和 filezilla 测试均不能满足带宽要求。

原因在于 Windows 和 Linux 对 TCP 的实现不一致，导致速率慢。所以对端 ECS 使用不同的系统时，无法满足带宽要求。

使用 iperf3 测试结果截图如图 6-10 所示。

图6-10 互为对端的 ECS 系统不同时 iperf3 测试结果



测试总结：综上测试结果，云网关能够满足带宽速率要求，但是建议两端主机使用相同的操作系统，并且网卡要达到配置要求。

6.15.12.2 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？

云上用户购买的 VPN 网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下两种情况：

- 如果所购买的带宽<=10Mbit，则入云方向统一限定为 10Mbit。
- 如果所购买的带宽>10Mbit，则入云方向与购买的带宽一致。

按带宽计费度量采用国际统一的带宽单位 Mbit，按流量计费的度量单位为 GByte。

6.15.12.3 如何修改 VPN 的带宽大小？

1. 在 VPN 网关列表页目标 VPN 网关所在行，选择“更多 > 修改带宽”。
2. 在修改带宽页面选择带宽大小。
3. 单击“提交”，完成修改。

6.15.12.4 VPN 网关带宽到达限额时有什么影响？

VPN 带宽限速限制的出 VPC 方向的带宽，如果您 VPN 的带宽超过限额使用时，会出现网络卡顿、部分子网间无法访问、甚至出现 VPN 连接中断现象（无法收到 VPN 的探测报文）。

因此在出现 VPN 带宽已达到上限时，建议您对 VPN 网关带宽进行扩容。

说明

VPN 的带宽最大为 300(Mbit/s)。

6.15.12.5 修改了 VPN 带宽大小，为什么测试没有生效？

VPN 带宽修改到生效会有一定的延迟，是正常现象。

请在修改带宽 5 分钟后再进行带宽测试。

说明

修改 VPN 带宽大小，不会导致用户业务和网络中断。

6.15.12.6 VPN 能否共用 EIP 的带宽？

不可以。

目前 VPN 的公网地址与 EIP 是各自独立的，用户在创建 VPN 网关时会自动生成公网地址并设置带宽，无法与 EIP 共享带宽。

6.15.12.7 VPN 产品中的带宽和云专线的带宽有什么区别？

概念

- 云专线的带宽指用户创建的物理连接的带宽大小。
- VPN 的带宽指的是出云方向的带宽。

带宽大小

- 云专线默认最大带宽 1000(Mbit/s)，用户在管理控制台创建物理连接界面，“端口类型”参数选择“10GE 单模光口”，支持最大带宽 10Gbit/s
- VPN 的带宽最大为 300(Mbit/s)。

网络质量

- 云专线用户独占一条网络资源，网络质量高。
- VPN 是基于 VPN 网关创建的 VPN 连接共享的带宽，VPN 连接带宽总和不超过 VPN 网关的带宽。网络质量依赖公网质量。

6.15.12.8 如何选择购买 VPN 带宽的大小？

购买 VPN 时，选择带宽大小需要考虑以下两个因素：

- VPN 隧道中单位时间的数据传输量（需要冗余一定带宽，防止链路拥塞）。
- 考虑两端的出口带宽，云上带宽要小于云下出口带宽。

6.15.13 配额类

6.15.13.1 虚拟专用网络的配额是什么？

什么是配额？

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少台弹性云主机、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额？

1. 登录管理控制台。
2. 单击页面右上角的“My Quota”图标  。
   系统进入“服务配额”页面。
3. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。

如果当前配额不能满足业务要求，请提交工单申请扩大配额。

6.15.13.2 创建 VPN 网关和连接的缺省配额是多少？

- 经典版 VPN：每个用户缺省可创建 2 个 VPN 网关和 12 个 VPN 连接。请在购买 VPN 网关前确认您可用的配额，如果选购信息超出可用配额可申请扩容。

6.15.13.3 一个用户下支持多少个 IPsec VPN？

默认情况下，每个用户可以创建 2 个 VPN 网关，12 条 VPN 连接。

如果用户实际使用网关或连接超出缺省配额，可提交工单申请扩容配额。

配额中 VPN 网关数量不得大于 VPC 数量。

6.15.14 账号权限

6.15.14.1 建立 IPsec VPN 连接需要账户名和密码吗？

常见的使用账户名和密码进行认证的 VPN 有 SSL VPN，PPTP 或 L2TP，云的 IPsec VPN 使用预共享密钥方式进行认证，密钥是配置在 VPN 网关上的，在 VPN 协商完成后即建立通道，VPN 网关所保护的主机在进行通信时无需输入账户名和密码。

说明

IPsec XAUTH 技术是 IPsec VPN 的扩展技术，它在 VPN 协商过程中可以强制接入用户输入账户名和密码。

目前 VPN 不支持该扩展技术。

6.15.14.2 创建 VPN 时系统提示权限不足，如何处理？

请确认您的账号是否为子账号，如果未开通 VPC 操作权限，请使用主账号在统一身份认证服务（IAM）中对您的账号进行授权。确保具有“VPC Administrator”、“Tenant Guest”、“VPN Administrator”这三个【系统角色】权限。

6.15.14.3 如何确定我的账号是因为权限不足而无法创建 VPN 的？

- 主账号创建的 VPN 网关和连接，子账号不可见。
- 创建 VPN 网关或连接时提示系统繁忙。

账号创建 VPN 连接所需权限详见 VPN 连接用户指南 > 权限管理。