ALIBABA CLOUD

阿里云

VPN网关

用户指南

文档版本：20220704

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.VPN网关介绍 07
2.管理VPN网关 08
2.1. 创建和管理VPN网关实例 08
2.2. 配置VPN网关路由 10
2.2.1. 网关路由概述 10
2.2.2. 使用策略路由 11
2.2.3. 使用目的路由 14
2.3. 管理国密证书 15
2.4. 开启IPsec-VPN和SSL-VPN 16
2.5. 开启一键诊断 17
2.6. 升级VPN网关 20
2.7. 服务关联角色 21
2.7.1. AliyunServiceRoleForVpn 21
2.7.2. AliyunServiceRoleForVPNCertificate 23
3.管理用户网关 25
3.1. 创建用户网关 25
3.2. 修改用户网关 25
3.3. 删除用户网关 26
4.SSL-VPN 27
4.1. 配置概览 27
4.2. 管理SSL服务端 27
4.2.1. 创建SSL服务端 27
4.2.2. 修改SSL服务端 30
4.2.3. 删除SSL服务端 31
4.3. 管理SSL客户端 31
4.3.1. 创建SSL客户端证书 31

4.3.2. 下载SSL客户端证书 31
4.3.3. 删除SSL客户端证书 32
4.4. 修改SSL并发连接数 32
4.5. 查看SSL-VPN连接日志 32
5.IPsec-VPN 34
5.1. 配置概览 34
5.2. 管理IPsec连接 34
5.2.1. 创建IPsec连接 34
5.2.2. 修改IPsec连接 41
5.2.3. 下载IPsec连接配置 41
5.2.4. 查看IPsec连接日志 42
5.2.5. 删除IPsec连接 42
5.3. 本地网关配置 42
5.3.1. 华三防火墙配置 42
5.3.2. 华为防火墙配置 48
5.3.3. 山石网科防火墙配置 54
5.3.4. strongSwan配置 60
5.3.5. 深信服防火墙配置 62
5.3.6. Juniper防火墙配置 68
5.3.7. 思科防火墙配置 70
6.IPsec服务端 75
6.1. IPsec服务端配置简介 75
6.2. 创建和管理IPsec服务端 76
6.3. 客户端配置 79
6.4. 查看IPsec服务端日志 80
7.标签管理 81
7.1. 标签概述 81
7.2. 添加标签 82

7.2.1. 为单个实例添加标签 82
7.2.2. 为多个实例批量添加标签 82
7.3. 使用标签搜索实例 83
7.4. 删除标签 84
7.4.1. 为单个实例删除标签 84
7.4.2. 为多个实例批量删除标签 85
8.MTU配置说明 86
9.管理配额 88

1.VPN网关介绍

VPN网关是一款网络连接服务，通过建立加密通道的方式实现企业本地数据中心、企业办公网络、互联网客户端与阿里云专有网络VPC（Virtual Private Cloud）之间安全可靠的私网互联。

功能特性

VPN网关提供IPsec-VPN连接和SSL-VPN连接：

- IPsec-VPN
  IPsec-VPN是一种基于路由的网络连接技术，不仅可以让您更方便地配置和维护VPN策略，而且还为您提供了灵活的流量路由方式。
  您可以使用IPsec-VPN功能在本地数据中心与VPC之间或者在VPC与VPC之间建立安全连接。IPsec-VPN支持IKEv1和IKEv2协议，只要支持这两种协议的设备均可以和阿里云VPN网关互连。
  IPsec-VPN可满足不同的应用场景。更多信息，请参见IPsec-VPN入门概述。
- SSL-VPN
  您可以使用SSL-VPN功能从客户端远程接入VPC中部署的应用和服务。部署完成后，您仅需要在客户端中加载证书发起连接，即可实现远程接入。
  SSL-VPN可满足不同的应用场景。更多信息，请参见SSL-VPN入门概述。

2.管理VPN网关

2.1. 创建和管理VPN网关实例

在创建VPN连接前，您必须先创建一个VPN网关实例。本文为您介绍如何创建、修改和删除VPN网关实例。

背景信息

VPN网关类型说明

依据加密算法和网络类型的不同，VPN网关划分为以下三种类型，不同类型的VPN网关建立加密隧道的方式也不相同，满足不同场景的网络连接需求。

VPN网关类型	支持的加密算法	支持的网络类型	支持的网络连接方式	建立加密隧道的方式	适用的应用场景	相关文档
普通型VPN网关	普通算法	公网	• IPsec-VPN • SSL-VPN	通过互联网建立加密隧道，加密时使用普通算法。	适用于在企业本地数据中心、企业办公网络、互联网客户端与阿里云VPC之间建立网络连接。	应用场景
		私网	IPsec-VPN	通过基于物理专线的私网连接建立加密隧道，加密时使用普通算法。	适用于在企业本地数据中心、企业办公网络通过物理专线已与阿里云VPC建立私网连接的基础上实现私网流量的加密传输。	
国密型VPN网关	国密算法	公网	IPsec-VPN	通过互联网建立加密隧道，加密时使用国密算法。	适用于在仅支持国密算法的企业本地数据中心、企业办公网络与阿里云VPC之间建立网络连接。	

> **说明** 私网VPN网关正在邀测中，您可以向商务经理申请体验或者提交工单申请体验。

VPN网关加密算法说明

下表为您介绍普通型VPN网关和国密型VPN网关在IPsec-VPN连接不同加密阶段支持的加密算法：

VPN网关类型	不同加密阶段支持的算法			
	IKE加密	IKE认证	IPsec加密	IPsec认证
普通型	aes、aes192、aes256、des、3des	sha1、md5、sha256、sha384、sha512	aes、aes192、aes256、des、3des	sha1、md5、sha256、sha384、sha512
国密型	sm4	sm3	sm4	sm3

使用限制

- 国密型VPN网关功能默认不开放。如需使用，请提交工单申请。
- 目前仅华北2（北京）、华北3（张家口）、华东1（杭州）、华东2（上海）、华南1（深圳）地域支持国

密型VPN网关。

> **说明** 关于支持国密型VPN网关的地域的最新信息，请参见支持的地域，其中仅密码机检测类型为**国密局商用密码检测认证**的地域支持国密型VPN网关。

- 普通型VPN网关不支持变更为国密型VPN网关。
  如果您需要使用国密型VPN网关，需重新创建VPN网关实例，其中**网关类型**选择**国密型**。

创建VPN网关实例

1. 登录VPN网关管理控制台。
2. 在**VPN网关**页面，单击**创建VPN网关**。
3. 在购买页面，根据以下信息进行配置，然后单击**立即购买**并完成支付。

配置项	说明
实例名称	VPN网关实例的名称。
地域和可用区	选择VPN网关实例的地域。 需确保VPN网关实例的地域和待关联的专有网络VPC（Virtual Private Cloud）实例的地域相同。
网关类型	选择VPN网关实例的类型。 ○ **普通型** ○ **国密型** **说明** 使用国密型VPN网关时，国密型VPN网关需要关联国密证书进行数据加密和身份认证。更多信息，请参见管理国密证书。
网络类型	选择VPN网关实例的网络类型。 ○ **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。
VPC	选择VPN网关实例关联的VPC实例。
指定交换机	是否为VPN网关实例指定交换机。 ○ **否**：不为VPN网关实例指定交换机。创建VPN网关后，VPN网关自动关联至VPC内的任意一个交换机下。 ○ **是**：为VPN网关实例指定交换机。创建VPN网关后，VPN网关会被关联至指定的交换机下。
带宽规格	选择VPN网关实例的带宽规格。单位：Mbps。
IPsec-VPN	选择开启或关闭IPsec-VPN功能。 默认值：**开启**。 IPsec-VPN可以在本地数据中心和VPC之间或在VPC和VPC之间建立安全连接。

配置项	说明
SSL-VPN	选择开启或关闭SSL-VPN功能。默认值：**关闭**。 SSL-VPN可以在点和站点之间建立安全连接，无需配置用户网关。例如，SSL-VPN可以在Linux客户端和VPC之间建立安全连接。
SSL连接数	选择需要同时连接的客户端的规格。 **说明** 开启SSL-VPN功能后才支持配置本参数。
计费周期	选择购买时长。 您可以选择是否自动续费： ○ 按月购买：自动续费周期为1个月。 ○ 按年购买：自动续费周期为1年。
服务关联角色	单击**创建关联角色**，系统自动创建服务关联角色AliyunServiceRoleForVpn。 VPN网关使用此角色来访问其他云产品中的资源，更多信息，请参见AliyunServiceRoleForVpn。 若本配置项显示为**已创建**，则表示您当前账号下已创建了该角色，无需重复创建。

修改VPN网关实例的名称和描述信息

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，找到目标VPN网关实例，单击实例ID。
4. 在VPN网关实例详情页面的**基本信息**区域，修改VPN网关实例的名称和描述信息。
   - 在**名称**后面单击**编辑**，在弹出的对话框中修改实例的名称，然后单击**确定**。
   - 在**描述**后面单击**编辑**，在弹出的对话框中修改实例的描述信息，然后单击**确定**。

删除VPN网关实例

VPN网关实例不支持删除，到期后将进入自动释放流程。VPN网关实例到期状态说明，请参见到期资源状态说明。

相关文档

- CreateVpnGateway：创建VPN网关实例。
- ModifyVpnGatewayAttribute：修改VPN网关实例的名称和描述信息。
- DescribeVpnGateway：查询指定VPN网关实例的信息。
- DescribeVpnGateways：查询指定地域下VPN网关实例的信息。

2.2. 配置VPN网关路由

2.2.1. 网关路由概述

创建IPsec连接后，您需要手动添加VPN网关路由。
基于路由的IPsec-VPN，不仅可以更方便的配置和维护VPN策略，而且还提供了灵活的流量路由方式。

您可以为VPN网关添加如下两种路由：

- 策略路由。
- 目的路由。

策略路由

策略路由基于源IP和目的IP进行更精确的路由转发。

添加策略路由的详细信息，请参见使用策略路由。

> **说明** 策略路由比目的路由的优先级高。

目的路由

目的路由仅基于目的IP进行路由转发。

添加目的路由的详细信息，请参见使用目的路由。

2.2.2. 使用策略路由

创建IPsec连接后，您可以为IPsec连接添加策略路由。策略路由会基于流量的源IP和目的IP进行更精确的路由转发。本文为您介绍如何添加、发布、修改、删除策略路由。

前提条件

您已经创建了IPsec连接。具体操作，请参见创建IPsec连接。

使用限制

- 不支持添加目标网段为0.0.0.0/0的策略路由。
- 请勿添加目标网段为100.64.0.0/10（包含该网段下的子网段），下一跳指向IPsec连接的策略路由，该类策略路由会导致控制台无法显示IPsec连接的状态或者导致IPsec连接协商失败。

策略路由匹配规则

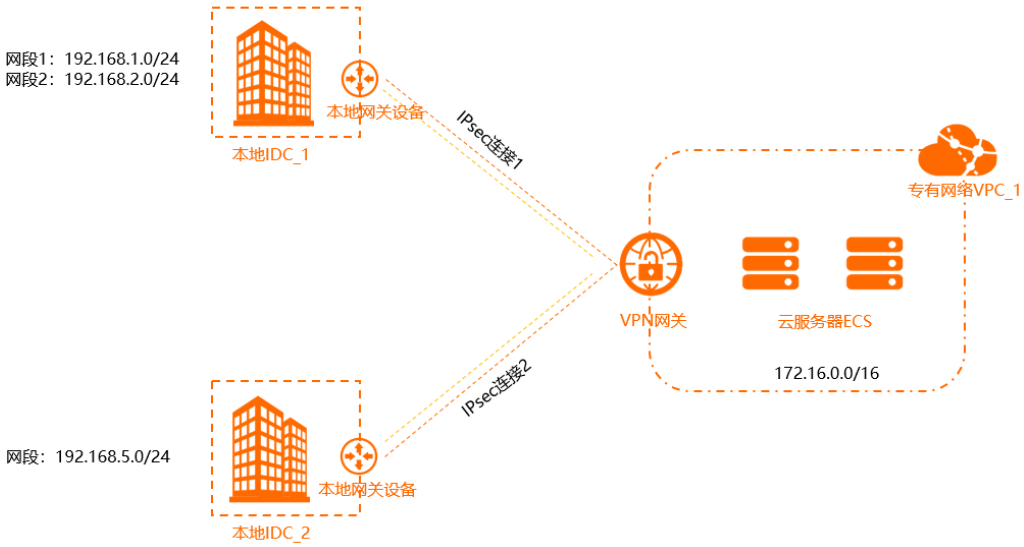
在VPN网关转发流量时，不按照最长掩码匹配原则匹配策略路由，VPN网关会按照策略路由的顺序逐条匹配路由，一旦能够匹配到策略路由，立即按照当前策略路由转发流量。

策略路由的顺序由策略路由被下发至系统的时间决定。通常是先配置的策略路由被优先下发至系统，但当前情况无法完全保证，因此有可能存在后配置的策略路由被优先下发至系统，造成后配置的策略路由的优先级高于先配置的策略路由的优先级。

策略路由配置建议

为确保流量按照您期望的路径进行转发，在您配置策略路由时，请尽量添加精确的策略路由以保证流量仅可匹配到一条策略路由。

策略路由匹配规则示例



如上图所示，本地IDC_1通过IPsec连接1和VPC_1互通，本地IDC_2通过IPsec连接2和VPC_1互通。本地IDC_1待互通网段为192.168.1.0/24和192.168.2.0/24，本地IDC_2待互通网段为192.168.5.0/24，VPC_1待互通网段为172.16.0.0/16。

在配置策略路由时，您首先配置了VPC_1去往本地IDC_2的路由，然后将VPC_1去往本地IDC_1的路由的目标网段聚合为192.168.0.0/21进行配置，配置完成后，策略路由并未按照您的配置顺序被下发至系统，导致策略路由表各策略路由条目的顺序发生了变化，如下表所示。

策略路由顺序	目标网段	源网段	下一跳
1	192.168.0.0/21	172.16.0.0/16	IPsec连接1
2	192.168.5.0/24	172.16.0.0/16	IPsec连接2

VPN网关在转发VPC_1去往本地IDC_2的流量时，会按照策略路由的顺序逐条匹配路由，经系统分析VPC_1去往本地IDC_2的流量可以匹配上顺序为1的策略路由，则VPC_1去往本地IDC_2的流量会通过IPsec连接1被转发至本地IDC_1中。

在上述场景中由于策略路由被下发至系统的时间不可控，导致策略路由未按照期望的顺序进行排列，进而导致流量未按照期望的路径进行转发。为了避免上述现象，在配置策略路由时，建议您尽量配置精确的策略路由，以确保流量仅可匹配到一条策略路由，不受策略路由顺序的影响。

在本示例中，建议您配置如下表所示的策略路由，VPN网关在转发VPC_1去往本地IDC_2的流量时，流量仅会匹配到顺序为2的策略路由，流量会按照期望的路径被转发至本地IDC_2。

策略路由顺序	目标网段	源网段	下一跳
1	192.168.1.0/24	172.16.0.0/16	IPsec连接1
2	192.168.5.0/24	172.16.0.0/16	IPsec连接2
3	192.168.2.0/24	172.16.0.0/16	IPsec连接1

添加策略路由

1. 登录VPN网关管理控制台。

2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，单击目标VPN网关实例ID。
4. 单击**策略路由表**页签，然后单击**添加路由条目**。
5. 在**添加路由条目**面板，根据以下信息配置策略路由，然后单击**确定**。

配置	说明
目标网段	输入要访问的私网网段。
源网段	输入VPC侧的私网网段。
下一跳类型	选择IPsec连接。
下一跳	选择需要建立VPN连接的IPsec连接实例。
发布到VPC	选择是否将新添加的路由发布到VPC路由表。 ○ （推荐）**是**：将新添加的路由发布到VPC路由表。 ○ **否**：不发布新添加的路由到VPC路由表。 **说明** 如果您选择否，添加策略路由后，您还需在策略路由表中发布路由。
权重	选择权重值： ○ **100**（默认值）：高优先级。 ○ **0**：低优先级。 **说明** 如果策略路由表中存在多条源网段、目标网段、权重值均相同的路由条目，则系统将随机选择一条路由条目转发流量。

发布策略路由

在您创建IPsec连接时，您可以选择**路由模式**。如果您选择了**感兴趣流模式**，在IPsec连接创建完成后，系统会自动为您的VPN网关创建策略路由，路由是**未发布**状态。您可以执行本操作，将路由发布到VPC路由表中。

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，单击目标VPN网关实例ID。
4. 单击**策略路由表**页签，找到目标路由条目，在**操作**列单击**发布**。
5. 在**发布路由**对话框，单击**确定**。

   目标路由发布后，您可以单击**撤销发布**，撤销已经发布的路由。

编辑策略路由

添加策略路由后，您可以修改策略路由的权重值。

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。

3. 在**VPN网关**页面，单击目标VPN网关实例ID。
4. 单击**策略路由表**页签，找到目标路由条目，在**操作**列单击**编辑**。
5. 在编辑面板，修改策略路由的权重值，然后单击**确定**。

删除策略路由

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，单击目标VPN网关实例ID。
4. 单击**策略路由表**页签，找到目标路由条目，在**操作**列单击**删除**。
5. 在**删除路由条目**对话框，单击**确定**。

2.2.3. 使用目的路由

创建IPsec连接后，您可以为IPsec连接添加目的路由。目的路由基于流量的目的IP进行路由转发。本文为您介绍如何添加、发布、修改以及删除目的路由。

前提条件

您已经创建了IPsec连接。具体操作，请参见创建IPsec连接。

使用限制

- 不支持添加目标网段为0.0.0.0/0的目的路由。
- 请勿添加目标网段为100.64.0.0/10（包含该网段下的子网段），下一跳指向IPsec连接的目的路由，该类路由条目会导致控制台无法显示IPsec连接的状态或者导致IPsec连接协商失败。

添加目的路由

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，单击目标VPN网关实例ID。
4. 在**目的路由表**页签，单击**添加路由条目**。
5. 在**添加路由条目**面板，根据以下信息配置目的路由，然后单击**确定**。

配置	说明
目标网段	输入要访问的私网网段。
下一跳类型	选择IPsec连接。
下一跳	选择需要建立VPN连接的IPsec连接实例。
发布到VPC	选择是否将新添加的路由发布到VPC路由表。 ○ （推荐）**是**：将新添加的路由发布到VPC路由表。 ○ **否**：不发布新添加的路由到VPC路由表。 **说明** 如果您选择**否**，添加目的路由后，您还需在目的路由表中发布路由。

配置	说明
权重	选择权重值： ○ 100：优先级高。 ○ 0：优先级低。 说明 如果目的路由表中存在多条目标网段、权重值均相同的路由条目，则系统将随机选择一条路由条目转发流量。

发布目的路由

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，单击目标VPN网关实例ID。
4. 在**目的路由表**页签，找到目标路由条目，在**操作**列单击**发布**。
5. 在**发布路由**对话框，单击**确定**。

   目标路由发布后，您可以单击**撤销发布**，撤销已经发布的路由。

编辑目的路由

添加目的路由后，您可以修改目的路由的权重值。

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，单击目标VPN网关实例ID。
4. 在**目的路由表**页签，找到目标路由条目，在**操作**列单击**编辑**。
5. 在编辑面板，修改目的路由的权重值，然后单击**确定**。

删除目的路由

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，单击目标VPN网关实例ID。
4. 在**目的路由表**页签，找到目标路由条目，在**操作**列单击**删除**。
5. 在**删除路由条目**对话框，单击**确定**。

2.3. 管理国密证书

在您创建国密型VPN网关后，您需要为国密型VPN网关绑定国密证书，用于数据加密和身份认证。

前提条件

- 您已经创建了国密型VPN网关。具体操作，请参见创建和管理VPN网关实例。
- 您已经在密钥管理服务KMS（Key Management Service）控制台创建了国密证书。

背景信息

国密型VPN网关通过绑定KMS平台的证书，进行数据加密和身份认证。每一个国密型VPN网关，需要绑定以下两种类型的国密证书：

- 加密证书：用于对传送数据进行加密，以保证传送数据的保密性和完整性。
- 签名证书：用于对传送的数据进行签名认证，以保证传送数据的有效性和不可否认性。

绑定国密证书

1. 登录VPN网关管理控制台。
2. 在**VPN网关**页面，找到目标VPN网关，然后在其**操作**列，选择 **> 查看/关联证书**。
3. 在VPN实例详情页面，单击**绑定KMS证书**。
4. 在**绑定KMS证书**对话框，选择证书类型和证书实例，然后单击**确定**。

配置项	说明
证书类型	选择证书类型。 ○ **加密证书**：用于对传送数据进行加密，以保证传送数据的保密性和完整性。 ○ **签名证书**：用于对传送的数据进行签名认证，以保证传送数据的有效性和不可否认性。
证书实例	选择证书实例。

解除国密证书

1. 登录VPN网关管理控制台。
2. 在**VPN网关**页面，找到目标VPN网关，然后在其**操作**列，选择 **> 查看/关联证书**。
3. 在VPN实例详情页面的**关联证书**页签下，找到目标证书，在**操作**列单击**解绑**。
4. 在**解绑KMS证书**对话框，确认证书信息，然后单击**确定**。

2.4. 开启IPsec-VPN和SSL-VPN

您可以在创建VPN网关时直接开启IPsec-VPN和SSL-VPN功能，也可以在创建VPN网关后根据需要再开启IPsec-VPN和SSL-VPN功能。

开启IPsec-VPN

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，找到目标VPN网关实例，在**功能配置**列单击**IPsec连接**后的**开启**。
4. 在配置页面，选择**开启**IPsec-VPN功能，查阅并选中服务协议，单击**立即购买**并完成支付。

开启SSL-VPN

- 如果您的VPN网关是在2018年01月20日前创建的，在开启VPN网关的SSL-VPN功能前，请先将VPN网关升级至最新版本。具体操作，请参见升级VPN网关。
- 如果您的VPN网关是在2018年01月20日后创建的，您可以在控制台直接开启VPN网关的SSL-VPN功能。

1. 登录VPN网关管理控制台。

2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，找到目标VPN网关实例，在**功能配置**列单击**SSL**后的**开启**。
4. 在配置页面，选择**开启**SSL-VPN、选择SSL连接数、查阅并选中服务协议，单击**立即购买**并完成支付。

2.5. 开启一键诊断

VPN网关支持一键诊断功能，一键诊断可以检测VPN连接的配置、配额、路由冲突以及网络连通性问题，帮助您快速定位VPN连接建立失败的原因，然后您可以根据原因自助排查VPN连接的故障。

前提条件

- 开启一键诊断功能前，请确保您已经创建了VPN网关，并在该VPN网关中创建了IPsec连接。具体操作，请参见创建和管理VPN网关实例和创建IPsec连接。

  > **说明** 目前，仅以下地域支持一键诊断功能：华北1（青岛）、华北6（乌兰察布）、日本（东京）、新加坡、澳大利亚（悉尼）、马来西亚（吉隆坡）、印度尼西亚（雅加达）、印度（孟买）、菲律宾（马尼拉）、美国（硅谷）、德国（法兰克福）、英国（伦敦）、阿联酋（迪拜）。

- 请确保您的VPN网关是最新版本。如果您的VPN网关不是最新版本，默认您无法使用一键诊断功能。您可以在**升级**按钮处查看VPN网关是否是最新版本，如果不是最新版本，您可以通过**升级**按钮进行升级。具体操作，请参见升级VPN网关。

背景信息

目前，VPN网关仅支持一键诊断IPsec连接，不支持一键诊断SSL-VPN连接。一键诊断功能支持以下诊断项：

诊断项	说明
VPN网关IPsec连接配额	系统会检测所选VPN网关下已经创建的IPsec连接的数量和您账号下单个VPN网关支持创建的IPsec连接的配额数量，并计算所选VPN网关下已经创建的IPsec连接数量占您账号下单个VPN网关支持创建的IPsec连接配额数量的比例。 • 如果所占比例未超过80%，则诊断结果为**normal**。 • 如果所占比例超过80%，则诊断结果为**warning**。 例如，您的VPN网关支持创建的IPsec连接的配额数量为10： • 如果您已经在该VPN网关下创建了8条IPsec连接，则该VPN网关IPsec连接配额的诊断结果为**normal**。 • 如果您已经在该VPN网关下创建了9条IPsec连接，则该VPN网关IPsec连接配额的诊断结果为**warning**。 **说明** 默认情况下，单个VPN网关支持创建的IPsec连接的数量为10个。您可以通过以下任意方式自助提升配额： • 前往配额管理页面提升配额。具体操作，请参见管理配额。 • 前往配额中心提升配额。具体操作，请参见创建配额提升申请。

诊断项	说明
VPN网关策略路由配额	系统会检测所选VPN网关下已经创建的策略路由的数量和您账号下单个VPN网关支持创建的策略路由的配额数量，并计算所选VPN网关下已经创建的策略路由的数量占您账号下单个VPN网关支持创建的策略路由配额数量的比例。 • 如果所占比例未超过80%，则诊断结果为**normal**。 • 如果所占比例超过80%，则诊断结果为**warning**。 例如，您的VPN网关支持创建的策略路由的配额数量为20： • 如果您已经在该VPN网关下创建了16条策略路由，则该VPN网关策略路由配额的诊断结果为**normal**。 • 如果您已经在该VPN网关下创建了17条策略路由，则该VPN网关策略路由配额的诊断结果为**warning**。 **说明** 默认情况下，单个VPN网关支持创建的策略路由的数量为20个。 您可以通过以下任意方式自助提升配额： • 前往配额管理页面提升配额。具体操作，请参见管理配额。 • 前往配额中心提升配额。具体操作，请参见创建配额提升申请。
VPN网关目的路由配额	系统会检测所选VPN网关下已经创建的目的路由的数量和您账号下单个VPN网关支持创建的目的路由的配额数量，并计算所选VPN网关下已经创建的目的路由数量占您账号下单个VPN网关支持创建的目的路由配额数量的比例。 • 如果所占比例未超过80%，则诊断结果为**normal**。 • 如果所占比例超过80%，则诊断结果为**warning**。 例如，您的VPN网关支持创建的目的路由的配额数量为20： • 如果您已经在该VPN网关下创建了16条目的路由，则该VPN网关目的路由配额的诊断结果为**normal**。 • 如果您已经在该VPN网关下创建了17条目的路由，则该VPN网关目的路由配额的诊断结果为**warning**。 **说明** 默认情况下，单个VPN网关支持创建的目的路由的数量为20个。 您可以通过以下任意方式自助提升配额： • 前往配额管理页面提升配额。具体操作，请参见管理配额。 • 前往配额中心提升配额。具体操作，请参见创建配额提升申请。

诊断项	说明
路由冲突	系统会检测指定的IPsec连接的路由（路由的下一跳为指定的IPsec连接），并判断其与所选VPN网关路由表中的路由是否冲突： • 如果VPN网关路由表中的路由，不存在与指定的IPsec连接的路由的目的地址相同的路由，且不存在与指定的IPsec连接路由的目的地址有包含和被包含关系的路由，则诊断结果为**normal**。 • 如果VPN网关路由表中的路由，存在与指定的IPsec连接的路由的目的地址相同的路由，或存在包含了指定的IPsec连接路由的目的地址的路由，则诊断结果为**error**。 • 如果指定的IPsec连接路由的目的地址，包含了所选VPN网关路由表中任一路由的目的地址，则诊断结果为**warning**。 例如，您的IPsec连接路由的目的地址为172.23.0.0/16，下一跳为vco-1： • 如果您的VPN网关路由表中还存在一条目的地址为192.168.0.0/16的路由，无其他路由，则诊断结果为**normal**。 • 如果您的VPN网关路由表中还存在目的地址为172.23.0.0/16、下一跳为vco-2的路由，则诊断结果为**error**。 • 如果您的VPN网关路由表中还存在目的地址为172.23.1.0/24、下一跳为vco-3的路由，则诊断结果为**warning**。
IPsec配置一致性	系统会检测所选VPN网关的IPsec连接配置和本地网关设备的IPsec连接配置是否一致： • 如果一致，则诊断结果为**normal**。 • 如果不一致，则诊断结果为**error**。 **说明** 一键诊断功能如果检测不到本地网关设备的IPsec连接配置时，诊断结果也为**normal**。
用户网关公网连通性	系统会发送公网连通性的探测包。 • 如果探测包丢包率为0，则诊断结果为**normal**。 • 如果探测包丢包率为0~100%（不含0和100%），则诊断结果为**warning**。 • 如果探测包丢包率为100%，则诊断结果为**error**。
私网连通性	系统会发送私网连通性的探测包。 • 如果探测包丢包率为0，则诊断结果为**normal**。 • 如果探测包丢包率为0~100%（不含0和100%），则诊断结果为**warning**。 • 如果探测包丢包率为100%，则诊断结果为**error**。 **说明** 诊断私网连通性需要您配置源地址和目的地址，如果未配置，则不会进行私网连通性诊断。

操作步骤

1.
2. 在顶部菜单栏处，选择VPN网关的地域。
3. 在**VPN网关**页面，找到目标VPN网关，在其**操作**列下，选择 > **一键诊断**。
4. 在**一键诊断**对话框，根据以下信息配置一键诊断，然后单击**下一步**。

配置	说明
IPsec连接	选择要进行一键诊断的IPsec连接。
私网连通性检查	
源地址	输入VPC侧的IP地址，该IP地址为私网连通性检查的源地址。
目的地址	输入本地数据中心侧的IP地址，该IP地址为私网连通性检查的目的地址。

5. 在**诊断结果**区域，查看IPsec连接的诊断结果。

2.6. 升级VPN网关

VPN网关支持自助升级，升级完成后VPN网关会变为最新版，您可以体验VPN网关的更多功能特性。例如：BGP动态路由、对等体存活检测DPD（Dead Peer Detection）功能等。

升级说明

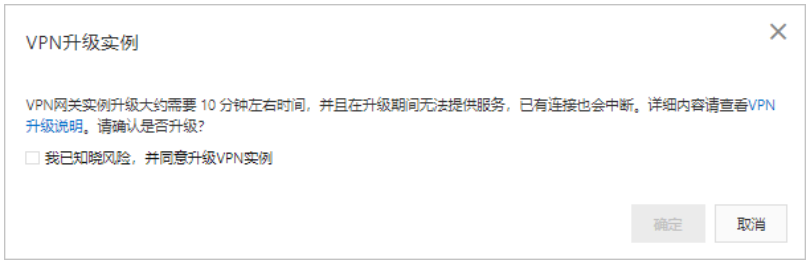
- VPN网关升级约需要10分钟时间，在升级期间VPN网关无法提供服务，已有连接也会中断。建议您在网络维护窗口期间进行升级，以免影响业务运行。
- 如果您的IPsec-VPN连接配置了多个网段且IKE版本为IKE V1，那么您需要将IKE版本修改为IKE V2，或者将多个网段拆分为多个IPsec-VPN连接才能进行升级，否则会升级失败。
- 您可以根据**升级**按钮的状态来判定您的VPN网关是否可以升级。
  - 如果您的VPN网关为最新版，**升级**按钮会显示为灰色，升级功能不可用。在您将鼠标移动至**升级**按钮上时，控制台会通过气泡给您相应提示，您无需进行升级。
    对于新建的VPN网关，其版本默认为最新版，无需进行升级。
  - 如果**升级**按钮显示不是灰色，则表示您当前的VPN网关不是最新版，升级功能可用。关于如何升级，请参见升级操作。
    如果您的VPN网关是在2019年03月21日之前创建的，则在进行升级时，该VPN网关的路由无法被转化为最新版本的策略路由，升级完成后，您需要为VPN网关重新配置路由以确保网络连通。具体操作，请参见网关路由概述。
    2019年03月21日之后创建的VPN网关，升级前后配置不变。

升级操作

1.
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，找到目标VPN网关实例，单击实例ID。
4. 在VPN网关实例详情页面，单击**升级**。

5. 在**VPN升级实例**对话框，仔细阅读升级提示，了解升级风险并同意升级后，单击**确定**。
   - 对于2019年03月21日之前创建的VPN网关，在您进行升级时，系统将弹出以下对话框，提示您完成升级后进行路由配置。

- 对于2019年03月21日之后创建的VPN网关，在您进行升级时，系统将弹出以下对话框，您在知晓升级风险后直接进行升级即可。



单击**确定**后，系统将直接开始升级，请耐心等待升级完成。

2.7. 服务关联角色

2.7.1. AliyunServiceRoleForVpn

本文为您介绍VPN网关的服务关联角色AliyunServiceRoleForVpn。

背景信息

服务关联角色是指与某个云服务关联的RAM角色。在某些场景下，为了完成云服务的某个功能，需要获取其他云服务的访问权限。通过服务关联角色，您可以更好地管理云服务正常操作所需的权限，避免误操作带来的风险。更多信息，请参见服务关联角色。

创建服务关联角色AliyunServiceRoleForVpn

创建VPN网关时，系统会自动创建服务关联角色AliyunServiceRoleForVpn，该角色下包含名称为AliyunServiceRolePolicyForVpn的权限策略，此权限策略允许VPN网关访问其他云资源，策略内容如下。

> **说明** 如果您的账号下已存在该服务关联角色，系统则不会重复创建。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVSwitchAttributes"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:CreateNetworkInterface",
```

```
        "ecs:CreateSecurityGroup",
        "ecs:AuthorizeSecurityGroup",
        "ecs:RevokeSecurityGroup",
        "ecs:DeleteSecurityGroup",
        "ecs:JoinSecurityGroup",
        "ecs:LeaveSecurityGroup",
        "ecs:DescribeSecurityGroups",
        "ecs:AttachNetworkInterface",
        "ecs:DetachNetworkInterface",
        "ecs:DeleteNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:CreateNetworkInterfacePermission",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs:DeleteNetworkInterfacePermission",
        "ecs:CreateSecurityGroupPermission",
        "ecs:AuthorizeSecurityGroupPermission",
        "ecs:RevokeSecurityGroupPermission",
        "ecs:JoinSecurityGroupPermission",
        "ecs:DeleteSecurityGroupPermission",
        "ecs:LeaveSecurityGroupPermission",
        "ecs:DescribeSecurityGroupPermissions",
        "ecs:AttachNetworkInterfacePermissions",
        "ecs:DetachNetworkInterfacePermissions",
        "ecs:AssignPrivateIpAddresses",
        "ecs:UnassignPrivateIpAddresses",
        "ecs:DescribeNetworkInterfaceAttribute"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "vpn.aliyuncs.com"
        }
      }
    }
  ]
}
```

删除服务关联角色AliyunServiceRoleForVpn

VPN网关实例不支持手动删除，到期后自动释放。请在所有VPN网关实例均释放后，再删除服务关联角色。具体操作，请参见删除服务关联角色。

常见问题

阿里云账号（主账号）默认拥有创建服务关联角色AliyunServiceRoleForVpn的权限，RAM用户（子账号）必须拥有相应权限，才可以创建服务关联角色AliyunServiceRoleForVpn。

您需要创建如下自定义权限策略，为RAM用户（子账号）授予创建服务关联角色AliyunServiceRoleForVpn的权限。具体操作，请参见创建自定义权限策略和为RAM角色授权。

```
{
    "Statement": [
        {
            "Action": "ram:CreateServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "vpn.aliyuncs.com"
                }
            }
        }
    ],
    "Version": "1"
}
```

为什么我的RAM用户（子账号）无法创建服务关联角色AliyunServiceRoleForVpn?

相关文档

创建和管理VPN网关实例

2.7.2. AliyunServiceRoleForVPNCertificate

本文为您介绍VPN网关的服务关联角色AliyunServiceRoleForVPNCertificate以及如何删除VPN网关服务关联角色。

背景信息

服务关联角色SLR（Service Linked Role）是指与某个云服务关联的RAM角色。在某些场景下，为了完成云服务的某个功能，需要获取其他云服务的访问权限。通过服务关联角色，您可以更好的创建云服务正常操作所需的权限，避免误操作带来的风险。关于服务关联角色的更多信息，请参见服务关联角色。

创建服务关联角色AliyunServiceRoleForVPNCertificate

您在首次绑定国密型VPN网关和国密证书时，系统将会为您自动创建一个名称为AliyunServiceRoleForVPNCertificate的服务关联角色，并且为该角色添加名称为AliyunServiceRolePolicyForVPNCertificate的权限策略，该权限会允许VPN网关访问其他云资源。权限策略内容如下：

> **说明** 如果服务关联角色AliyunServiceRoleForVPNCertificate已存在，系统则不会重复创建。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeCertificate",
        "kms:GetCertificate",
        "kms:CertificatePublicKeyEncrypt",
        "kms:CertificatePrivateKeyDecrypt",
        "kms:CertificatePublicKeyVerify",
        "kms:CertificatePrivateKeySign"
      ],
      "Resource": "*"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "certificate.vpn.aliyuncs.com"
        }
      }
    }
  ],
  "Version": "1"
}
```

删除服务关联角色AliyunServiceRoleForVPNCertificate

系统不会自动删除VPN网关的服务关联角色AliyunServiceRoleForVPNCertificate。如果您要删除VPN网关的服务关联角色AliyunServiceRoleForVPNCertificate，请确保当前阿里云账号下的国密型VPN网关与国密证书没有绑定关系。具体操作，请参见：

- 解除国密证书
- 删除服务关联角色

相关文档

绑定国密证书

3.管理用户网关

3.1. 创建用户网关

当使用IPsec-VPN在本地数据中心与VPC或不同的VPC之间建立连接时，需要创建用户网关。通过创建用户网关，您可以将本地网关的信息注册到云上，然后将用户网关和VPN网关连接起来。一个用户网关可以连接多个VPN网关。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > 用户网关**。
3. 在顶部菜单栏，选择用户网关的地域。

   > **说明** 用户网关的地域必须和要连接的VPN网关的地域相同。

4. 在**用户网关**页面，单击**创建用户网关**。
5. 在**创建用户网关**面板，根据以下信息配置用户网关，然后单击**确定**。

配置	说明
名称	用户网关的名称。 名称长度为2~128个字符，以大小写字母或中文开始，可包含数字、下划线（_）和短划线（-）。
IP地址	本地数据中心网关设备的静态公网IP地址。
自治系统号	本地数据中心网关设备的自治系统号ASN（Autonomous System Number）。自治系统号取值范围：1~4294967295。 支持按照两段位的格式进行输入，即：前16位比特.后16位比特。每个段位使用十进制输入。 例如输入123.456，则表示自治系统号：123*65536+456=8061384。 **说明** ◦ 当您的VPN网关启用BGP动态路由协议时需要配置该参数。 ◦ 建议您使用自治系统号的私有号码与阿里云建立BGP连接。自治系统号的私有号码范围请自行查阅文档。
描述	用户网关的描述信息。 描述信息长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（_）和短划线（-）。 您可以在**描述**输入框下面单击+图标，一次创建多个用户网关。

相关文档

- CreateCustomerGateway

3.2. 修改用户网关

创建用户网关实例后，您可以修改用户网关实例的名称和描述信息。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > 用户网关**。
3. 在顶部菜单栏，选择用户网关实例的地域。
4. 在**用户网关**页面，找到目标用户网关实例，在**实例ID/名称**列单击图标，在弹出的对话框中修改实例名称，然后单击**确定**。

   名称长度为2~128个字符，以大小写字母或中文开始，可包含数字、下划线（_）和短划线（-）。
5. 在**描述**列单击图标，在弹出的对话框中修改用户网关实例的描述信息，然后单击**确定**。

   描述信息长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（_）和短划线（-）。

相关文档

- ModifyCustomerGatewayAttribute

3.3. 删除用户网关

您可以删除一个不需要的用户网关实例。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > 用户网关**。
3. 在顶部菜单栏，选择用户网关实例的地域。
4. 在**用户网关**页面，找到目标用户网关实例，在**操作**列单击**删除**。
5. 在**删除用户网关**对话框中，单击**确定**。

4.SSL-VPN

4.1. 配置概览

本文为您介绍如何通过SSL-VPN功能远程接入VPC。

配置流程说明

通过SSL-VPN功能远程接入VPC的流程如下：

1. 创建VPN网关
   创建VPN网关并开启SSL-VPN功能。
2. 创建SSL服务端
   在SSL服务端中指定要连接的IP地址段和客户端连接时使用的IP地址段。
3. 创建客户端证书
   根据服务端配置，创建客户端证书，下载客户端证书和配置。
4. 配置客户端
   在客户端中下载安装客户端VPN软件，加载客户端证书和配置，发起连接即可。
5. 配置安全组
   确保ECS的安全组规则允许客户端访问。

4.2. 管理SSL服务端

4.2.1. 创建SSL服务端

开启SSL-VPN功能建立点到站点连接时，您必须先创建SSL服务端。

前提条件

您已经创建了VPN网关并开启了SSL-VPN。具体操作，请参见创建和管理VPN网关实例。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
3. 在顶部菜单栏，选择SSL服务端的地域。
4. 在**SSL服务端**页面，单击**创建SSL服务端**。
5. 在**创建SSL服务端**面板，根据以下信息配置SSL服务端，然后单击**确定**。

配置	说明
名称	SSL服务端的名称。 名称在2~128个字符之间，以大小写字母或中文开始，可包含数字、短划线（-）和下划线（_）。
VPN网关	选择要关联的VPN网关。 确保该VPN网关已经开启了SSL-VPN功能。

配置	说明
本端网段	本端网段是客户端通过SSL-VPN连接要访问的地址段。 本端网段可以是专有网络VPC（Virtual Private Cloud）的网段、交换机的网段、通过物理专线和VPC互连的本地数据中心的网段、云服务（例如对象存储、云数据库）等的网段。 单击**+添加本端网段**添加多个本端网段。 **说明** 本端网段的子网掩码位数在8至32位之间。

<table>
<tr><th>配置</th><th>说明</th></tr>
<tr><td>客户端网段</td><td>
客户端网段是给客户端虚拟网卡分配访问地址的网段，不是指客户端已有的内网网段。当客户端通过SSL-VPN连接访问本端时，VPN网关会从指定的客户端网段中分配一个IP地址给客户端使用。
在您指定客户端网段时需保证客户端网段所包含的IP地址个数是当前VPN网关SSL连接数的4倍及以上。

单击查看原因。例如您指定的客户端网段为192.168.0.0/24，系统在为客户端分配IP地址时，会先从192.168.0.0/24网段中划分出一个子网掩码为30的子网段，例如192.168.0.4/30，然后从192.168.0.4/30中分配一个IP地址供客户端使用，剩余三个IP地址会被系统占用以保证网络通信，此时一个客户端会耗费4个IP地址。因此，为保证您的客户端均能分配到IP地址，请确保您指定的客户端网段所包含的IP地址个数是VPN网关SSL连接数的4倍及以上。
单击查看每个SSL连接数建议的客户端网段。
<table>
<tr><th>SSL连接数</th><th>建议的客户端网段</th></tr>
<tr><td>5</td><td>子网掩码位数小于或等于27的网段。
例如：10.0.0.0/27、10.0.0.0/26。</td></tr>
<tr><td>10</td><td>子网掩码位数小于或等于26的网段。
例如：10.0.0.0/26、10.0.0.0/25。</td></tr>
<tr><td>20</td><td>子网掩码位数小于或等于25的网段。
例如：10.0.0.0/25、10.0.0.0/24。</td></tr>
<tr><td>50</td><td>子网掩码位数小于或等于24的网段。
例如：10.0.0.0/24、10.0.0.0/23。</td></tr>
<tr><td>100</td><td>子网掩码位数小于或等于23的网段。
例如：10.0.0.0/23、10.0.0.0/22。</td></tr>
<tr><td>200</td><td>子网掩码位数小于或等于22的网段。
例如：10.0.0.0/22、10.0.0.0/21。</td></tr>
<tr><td>500</td><td>子网掩码位数小于或等于21的网段。
例如：10.0.0.0/21、10.0.0.0/20。</td></tr>
<tr><td>1000</td><td>子网掩码位数小于或等于20的网段。
例如：10.0.0.0/20、10.0.0.0/19。</td></tr>
</table>

注意

客户端网段的子网掩码位数在16至29位之间。
请确保客户端网段和本端网段不冲突。
在指定客户端网段时，建议您使用10.0.0.0/8、172.16.0.0/12和192.168.0.0/16网段及其子网网段。如果您的客户端网段需要指定为公网网段，您需要将公网网段设置为VPC的用户网段，以确保VPC可以访问到该公网网段。关于用户网段的更多信息，请参见什么是用户网段？和如何配置用户网段？。

</td></tr>
</table>

配置	说明
协议	SSL-VPN连接使用的协议。取值： ○ UDP（默认值） ○ TCP
端口	SSL-VPN连接使用的端口。默认端口：1194。
加密算法	SSL-VPN连接使用的加密算法。取值： ○ AES-128-CBC（默认值） ○ AES-192-CBC ○ AES-256-CBC ○ none 本参数表示不使用加密算法。
是否压缩	是否对传输数据进行压缩处理。取值： ○ 是 ○ 否（默认值）
双因子认证	选择是否开启VPN网关的双因子认证功能。系统默认关闭VPN网关的双因子认证功能。 如果您选择开启VPN网关的双因子认证功能，您还需要选择IDaaS实例。双因子认证支持使用IDaaS实例中的用户名和密码对SSL客户端进行二次认证。更多信息，请参见助力SSL VPN二次认证校验和SSL-VPN双因子认证。 **说明** ○ 仅2020年03月05日00时00分00秒之后创建的VPN网关支持开启双因子认证。 如果您的VPN网关是2020年03月05日之前创建的，您可以通过自助升级方式将VPN网关升级至最新版，体验双因子认证功能。具体操作，请参见升级VPN网关。 ○ 如果您是首次使用双因子认证功能，请先完成授权后再创建SSL服务端。

相关文档

- CreateSslVpnServer

4.2.2. 修改SSL服务端

创建SSL服务端后，您可以修改SSL服务端的配置。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。

3. 在顶部菜单栏，选择SSL服务端的地域。
4. 在**SSL服务端**页面，找到目标SSL服务端，在**操作**列单击**编辑**。
5. 在**编辑SSL服务端**面板，修改SSL服务端的名称、本端网段、客户端网段、高级配置等信息，然后单击**确定**。

   关于参数的详细说明，请参见创建SSL服务端。

4.2.3. 删除SSL服务端

您可以删除一个不需要的SSL服务端。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
3. 在顶部菜单栏，选择SSL服务端的地域。
4. 在**SSL服务端**页面，找到目标SSL服务端，在**操作**列单击**删除**。
5. 在**删除服务端配置**对话框中，单击**确定**。

4.3. 管理SSL客户端

4.3.1. 创建SSL客户端证书

创建SSL服务端后，您还需根据SSL服务端创建SSL客户端证书。

前提条件

您已经创建了SSL服务端。具体操作，请参见创建SSL服务端。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL客户端**。
3. 在顶部菜单栏，选择SSL客户端的地域。
4. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
5. 在**创建SSL客户端证书**面板，根据以下信息配置客户端证书，然后单击**确定**。

配置	说明
名称	SSL客户端证书的名称。 名称在2~128个字符之间，以英文字母或中文开始，可包含数字、短划线（-）和下划线（_）。
SSL服务端	选择要关联的SSL服务端。

4.3.2. 下载SSL客户端证书

SSL客户端连接SSL-VPN，需要加载SSL客户端证书。您可以在VPN网关管理控制台下载SSL客户端证书。

前提条件

您已经创建了SSL客户端证书。具体操作，请参见创建SSL客户端证书。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL客户端**。
3. 在顶部菜单栏，选择SSL客户端的地域。
4. 在**SSL客户端**页面，找到目标SSL客户端证书，在**操作**列单击**下载**。

4.3.3. 删除SSL客户端证书

您可以删除一个不需要的SSL客户端证书。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL客户端**。
3. 在顶部菜单栏，选择SSL客户端的地域。
4. 在**SSL客户端**页面，找到目标SSL客户端证书，在**操作**列单击**删除**。
5. 在**删除SSL客户端证书**的对话框中，单击**确定**。

4.4. 修改SSL并发连接数

您可以根据业务需要修改SSL并发连接数。

操作步骤

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关的地域。
3. 在**VPN网关**页面，找到目标VPN网关：
   - 如果您想增加SSL并发连接数，在**SSL并发连接数规格**列单击**升配**。
   - 如果您想降低SSL并发连接数，在**SSL并发连接数规格**列单击**降配**。
4. 在**SSL连接数**区域，选择新的SSL连接数并完成支付。

4.5. 查看SSL-VPN连接日志

您可以分别查看SSL服务端和SSL客户端的日志信息，通过日志信息排查SSL-VPN连接过程中的故障。

背景信息

系统支持您查看一个月内的SSL服务端和SSL客户端的日志信息，您一次可查看的日志周期最长为10分钟。

查看SSL服务端日志

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
3. 在顶部菜单栏，选择SSL服务端的地域。
4. 在**SSL服务端**页面，找到目标SSL服务端，在**操作**列选择 ⋮ **> 查看日志**。
5. 在**SSL VPN 连接日志**对话框，设置要查看的日志周期，查看日志。

查看SSL客户端日志

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL客户端**。
3. 在顶部菜单栏，选择SSL客户端的地域。
4. 在**SSL客户端**页面，找到目标SSL客户端证书，在**操作**列单击**查看日志**。
5. 在**SSL-VPN 客户端日志**对话框，设置要查看的日志周期，查看日志。

5.IPsec-VPN

5.1. 配置概览

本文为您介绍如何通过IPsec-VPN，建立VPC到本地数据中心的VPN连接。

环境要求

使用IPsec-VPN功能建立VPC与本地数据中心的VPN连接前，请确保您的环境满足以下条件：

- 本地数据中心的网关设备必须支持IKEv1和IKEv2协议。
  IPsec-VPN支持IKEv1和IKEv2协议，只要支持这两种协议的设备均可以和阿里云VPN网关互连。
- 本地数据中心的网关设备必须配置静态公网IP地址。
- 本地数据中心和VPC间互通的网段没有重叠。
- 您已了解VPC中所应用的安全组规则，并确保安全组规则允许本地数据中心的网关设备访问云上资源。具体操作，请参见查询安全组规则。

使用流程

1. 创建VPN网关
   VPN网关开启IPsec-VPN功能，一个VPN网关可以建立多条IPsec连接。
2. 创建用户网关
   通过创建用户网关，您可以将本地数据中心网关设备的信息注册到阿里云上。
3. 创建IPsec连接
   IPsec连接是指VPN网关和本地数据中心网关设备建立连接后的VPN通道。只有建立IPsec连接后，本地数据中心才能使用VPN网关进行加密通信。
4. 配置本地网关
   您需要在本地数据中心的网关设备中加载阿里云上VPN网关的配置。具体操作，请参见本地网关配置。
5. 配置VPN网关路由
   您需要在VPN网关中配置路由，并发布路由到VPC路由表以实现本地数据中心和VPC的通信。更多信息，请参见网关路由概述。
6. 测试连通性
   登录到阿里云VPC内一台无公网IP的ECS实例，通过ping命令，ping本地数据中心内一台服务器的私网IP地址，验证通信是否正常。

5.2. 管理IPsec连接

5.2.1. 创建IPsec连接

创建VPN网关和用户网关后，您可以创建IPsec连接建立加密通信通道。

前提条件

- 您已创建VPN网关。具体操作，请参见创建和管理VPN网关实例。

- 您已创建用户网关。具体操作，请参见创建用户网关。
- 如果要为国密型VPN网关创建IPsec连接，请确保您已经满足以下条件：
  - 您的国密型VPN网关已经绑定了国密证书。具体操作，请参见管理国密证书。
  - 您已知国密型VPN网关对端的CA（Certification Authority）证书和CA证书主体名称。

背景信息

创建IPsec连接时，您可以选择为IPsec连接开启或关闭以下功能：

- **DPD**：对等体存活检测DPD（Dead Peer Detection）功能。
  开启DPD功能后，IPsec发起端会发送DPD报文用来检测对端的设备是否存活，如果在设定时间内未收到正确回应则认为对端已经断线，IPsec将删除ISAKMP SA和相应的IPsec SA，安全隧道同样也会被删除。系统默认开启该功能。
- **NAT穿越**：NAT（Network Address Translation）穿越功能。
  开启NAT穿越功能后，IKE协商过程会删除对UDP端口号的验证过程，同时能帮您发现VPN隧道中NAT网关设备。系统默认开启该功能。
- **BGP**：BGP（Border Gateway Protocol）动态路由功能。
  开启BGP功能后，VPN网关通过BGP动态路由协议自动学习路由实现资源互通，帮您降低网络维护成本和网络配置风险。系统默认关闭该功能。
- **健康检查**：IPsec连接的健康检查功能。
  通过配置健康检查，可以帮您检测IPsec连接状态，方便您及时发现问题。系统默认关闭该功能。

> **说明**
>
> - 如果您的VPN网关是最新版本，您可以直接使用DPD功能、NAT穿越功能、BGP动态路由功能和健康检查功能；如果您的VPN网关不是最新版，默认您无法使用DPD功能、NAT穿越功能、BGP动态路由功能和健康检查功能。
>   您可以在**升级**按钮处查看VPN网关是否是最新版本，如果不是最新版本，您可以通过**升级**按钮进行升级。具体操作，请参见升级VPN网关。
> - VPN网关开启BGP动态路由功能后，不支持关闭。

操作步骤

1.
2. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
3. 在顶部菜单栏，选择IPsec连接的地域。
4. 在**IPsec连接**页面，单击**创建IPsec连接**。
5. 在**创建IPsec连接**页面，根据以下信息配置IPsec连接，然后单击**确定**。

为普通型VPN网关创建IPsec连接

配置	说明
名称	IPsec连接的名称。 名称在2~128个字符之间，以大小写字母或中文开始，可包含数字、短划线（-）和下划线（_）。
VPN网关	选择待连接的普通型VPN网关。
用户网关	选择待连接的用户网关。

配置	说明
路由模式	选择路由模式。默认为**目的路由模式**。 ○ **目的路由模式**：基于目的IP进行路由转发。 您在创建IPsec连接后，需要在VPN网关目的路由表中添加目的路由。具体操作，请参见添加目的路由。 ○ **感兴趣流模式**：基于源IP和目的IP进行精确的路由转发。 您在创建IPsec连接时，如果您选择了**感兴趣流模式**，您需要配置**本端网段**和**对端网段**。配置完成后，系统自动在VPN网关策略路由表中添加策略路由。 系统在VPN网关策略路由表中添加策略路由后，路由默认是未发布状态，您需要在策略路由表中手动将路由发布至VPC中。 **说明** ○ 如果您当前的VPN版本为旧版，您无需选择路由模式。在您创建IPsec连接后，请您手动为VPN网关配置目的路由或策略路由。更多信息，请参见网关路由概述。 ○ 请勿添加目标网段为100.64.0.0/10（包含该网段下的子网段），下一跳指向IPsec连接的路由，该类路由会导致控制台无法显示IPsec连接的状态或者导致IPsec连接协商失败。
本端网段	输入需要和本地数据中心互连的VPC侧的网段，用于第二阶段协商。 单击文本框后面的 + 图标，可添加多个需要和本地数据中心互连的VPC侧的网段。 **说明** 只有IKE V2版本下才可以配置多网段。
对端网段	输入需要和VPC互连的本地数据中心侧的网段，用于第二阶段协商。 单击文本框后面的 + 图标，可添加多个需要和VPC互连的本地数据中心侧的网段。 **说明** 只有IKE V2版本下才可以配置多网段。
立即生效	选择是否立即生效。 ○ **是**：配置完成后立即进行协商。 ○ **否**：当有流量进入时进行协商。
预共享密钥	输入IPsec-VPN连接的认证密钥，用于VPN网关与本地数据中心之间的身份认证。密钥长度为1~100个字符。 若您未指定预共享密钥，系统会随机生成一个16位的字符串作为预共享密钥。创建IPsec连接后，您可以通过**编辑**按钮查看系统生成的预共享密钥。具体操作，请参见修改IPsec连接。 **注意** IPsec连接侧的预共享密钥需和本地数据中心侧的认证密钥一致，否则本地数据中心和VPN网关之间无法建立连接。

配置	说明
高级配置：IKE配置	
版本	选择IKE协议的版本。 ○ **ikev1** ○ **ikev2** 目前系统支持IKE V1和IKE V2，相对于IKE V1版本，IKE V2版本简化了SA的协商过程并且对于多网段的场景提供了更好的支持，所以建议选择IKE V2版本。
协商模式	选择协商模式。 ○ **main**：主模式，协商过程安全性高。 ○ **aggressive**：野蛮模式，协商快速且协商成功率高。 协商成功后两种模式的信息传输安全性相同。
加密算法	选择第一阶段协商使用的加密算法。普通型VPN网关支持**aes**、**aes192**、**aes256**、**des**和**3des**。
认证算法	第一阶段协商使用的认证算法。普通型VPN网关支持**sha1**、**md5**、**sha256**、**sha384**和**sha512**。
DH分组	选择第一阶段协商的Diffie-Hellman密钥交换算法。普通型VPN网关支持以下DH组： ○ **group1**：表示DH分组中的DH1。 ○ **group2**：表示DH分组中的DH2。 ○ **group5**：表示DH分组中的DH5。 ○ **group14**：表示DH分组中的DH14。
SA生存周期（秒）	设置第一阶段协商出的SA的生存周期。单位：秒。默认值：**86400**。取值范围：**0~86400**。
LocalId	作为IPsec VPN网关的标识，用于第一阶段的协商。默认值为VPN网关的公网IP地址。如果手动设置LocalId为FQDN格式，建议将协商模式改为野蛮模式（**aggressive**）。
RemoteId	作为用户网关的标识，用于第一阶段的协商。默认值为用户网关的公网IP地址。如果手动设置RemoteId为FQDN格式，建议将协商模式改为野蛮模式（**aggressive**）。
高级配置：IPSec配置	
加密算法	选择第二阶段协商的加密算法。支持**aes**、**aes192**、**aes256**、**des**和**3des**。
认证算法	选择第二阶段协商的认证算法。支持**sha1**、**md5**、**sha256**、**sha384**和**sha512**。

配置	说明
DH分组	选择第二阶段协商的Diffie-Hellman密钥交换算法。普通型VPN网关以下DH组： ○ **disabled**：表示不使用DH密钥交换算法。 ■ 对于不支持PFS的客户端请选择**disabled**。 ■ 如果选择为非**disabled**的任何一个组，会默认开启PFS功能（完美向前加密），使得每次重协商都要更新密钥，因此，相应的客户端也要开启PFS功能。 ○ **group1**：表示DH分组中的DH1。 ○ **group2**：表示DH分组中的DH2。 ○ **group5**：表示DH分组中的DH5。 ○ **group14**：表示DH分组中的DH14。
SA生存周期（秒）	设置第二阶段协商出的SA的生存周期。单位：秒。默认值：**86400**。取值范围：**0~86400**。
DPD	选择开启或关闭对等体存活检测功能。DPD功能默认开启。
NAT穿越	选择开启或关闭NAT穿越功能。NAT穿越功能默认开启。
BGP配置	
隧道网段	输入IPsec隧道的网段。 该网段应是一个在169.254.0.0/16内的掩码长度为30的网段。
本端BGP地址	输入本端BGP地址。 该地址为隧道网段内的一个IP地址。 **说明** 请确保IPsec隧道两端的BGP地址不冲突。
本端自治系统号	输入VPC侧的自治系统号。取值范围：**1~4294967295**。默认值：**45104**。 **说明** 建议您使用自治系统号的私有号码与阿里云建立BGP连接。自治系统号的私有号码范围请自行查阅文档。
健康检查	
目标IP	VPC侧通过IPSec连接可以访问的本地数据中心的IP地址。
源IP	本地数据中心通过IPSec连接可以访问的VPC侧的IP地址。
重试间隔	健康检查的重试间隔时间，单位：秒。
重试次数	健康检查的重试发包次数。

为国密型VPN网关创建IPsec连接

配置	说明
名称	IPsec连接的名称。 名称在2~128个字符之间，以大小写字母或中文开始，可包含数字、短划线（-）和下划线（_）。
VPN网关	选择待连接的国密型VPN网关。
用户网关	选择待连接的用户网关。
路由模式	选择路由模式。默认为**目的路由模式**。 ○ **目的路由模式**：基于目的IP进行路由转发。 您在创建IPsec连接后，需要在VPN网关目的路由表中添加目的路由。具体操作，请参见添加目的路由。 ○ **感兴趣流模式**：基于源IP和目的IP进行精确的路由转发。 您在创建IPsec连接时，如果您选择了**感兴趣流模式**，您需要配置**本端网段**和**对端网段**。配置完成后，系统自动在VPN网关策略路由表中添加策略路由。 系统在VPN网关策略路由表中添加策略路由后，路由默认是未发布状态，您需要在策略路由表中手动将路由发布至VPC中。 **说明** ○ 如果您当前的VPN版本为旧版，您无需选择路由模式。在您创建IPsec连接后，请您手动为VPN网关配置目的路由或策略路由。更多信息，请参见网关路由概述。 ○ 请勿添加目标网段为100.64.0.0/10（包含该网段下的子网段），下一跳指向IPsec连接的路由，该类路由可能会导致IPsec连接协商失败。
本端网段	输入需要和本地数据中心互连的VPC侧的网段，用于第二阶段协商。 单击文本框后面的 ＋，可添加多个需要和本地数据中心互连的VPC侧的网段。 **说明** 只有IKE V2版本下才可以配置多网段。
对端网段	输入需要和VPC互连的本地数据中心侧的网段，用于第二阶段协商。 单击文本框后面的 ＋，可添加多个需要和VPC互连的本地数据中心侧的网段。 **说明** 只有IKE V2版本下才可以配置多网段。
立即生效	选择是否立即生效。 ○ **是**：配置完成后立即进行协商。 ○ **否**：当有流量进入时进行协商。
RemoteId	输入对端CA证书的主体名称。

配置	说明
对端CA证书	输入对端CA证书。 通过输入对端CA证书，VPN网关可以在建立IPsec连接时校验对端证书的合法性。 您还可以通过以下两种方式选择对端CA证书： ○ 单击**上传证书**，选择本地已经保存的证书。 ○ 单击**选择证书**，选择您在KMS平台创建的证书实例。
高级配置：IKE配置	
版本	选择IKE协议的版本。 ○ **ikev1** ○ **ikev2** 目前系统支持IKE V1和IKE V2，相对于IKE V1版本，IKE V2版本简化了SA的协商过程并且对于多网段的场景提供了更好的支持，所以建议选择IKE V2版本。
协商模式	选择协商模式。 ○ **main**：主模式，协商过程安全性高。 ○ **aggressive**：野蛮模式，协商快速且协商成功率高。 协商成功后两种模式的信息传输安全性相同。
加密算法	选择第一阶段协商使用的加密算法。国密型VPN网关支持**sm4**。
认证算法	选择第一阶段协商使用的认证算法。国密型VPN网关支持**sm3**。
SA生存周期（秒）	设置第一阶段协商出的SA的生存周期。单位：秒。默认值：**86400**。取值范围：**0~86400**。
高级配置：IPSec配置	
加密算法	选择第二阶段协商的加密算法。国密型VPN网关支持**sm4**。
认证算法	选择第二阶段协商的认证算法。国密型VPN网关支持**sm3**。
SA生存周期（秒）	设置第二阶段协商出的SA的生存周期。单位：秒。默认值：**86400**。取值范围：**0~86400**。
DPD	选择开启或关闭对等体存活检测功能。DPD功能默认开启。
NAT穿越	选择开启或关闭NAT穿越功能。NAT穿越功能默认开启。
BGP配置	
隧道网段	输入IPsec隧道的网段。 该网段应是一个在169.254.0.0/16内的掩码长度为30的网段。

配置	说明
本端BGP地址	输入VPN网关侧的BGP IP地址。 该地址为隧道网段内的一个IP地址。 **说明** 请确保IPsec隧道两端的BGP IP地址不冲突。
本端自治系统号	输入VPN网关侧的自治系统号。自治系统号取值范围：**1~4294967295**。默认值：**45104**。 自治系统号支持按照两段位的格式进行输入，即：前16位比特.后16位比特。每个段位使用十进制输入。 例如输入123.456，则表示自治系统号：123*65536+456=8061384。 **说明** 建议您使用自治系统号的私有号码与阿里云建立BGP连接。自治系统号的私有号码范围请自行查阅文档。
健康检查	
目标IP	VPC侧通过IPSec连接可以访问的本地数据中心的IP地址。
源IP	本地数据中心通过IPSec连接可以访问的VPC侧的IP地址。
重试间隔	健康检查的重试间隔时间，单位是秒。
重试次数	健康检查的重试发包次数。

5.2.2. 修改IPsec连接

创建IPsec连接后，您可以修改IPsec连接的配置。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
3. 在顶部菜单栏，选择IPsec连接的地域。
4. 在**IPsec连接**页面，找到目标IPsec连接，在**操作**列单击**编辑**。
5. 在**编辑IPsec连接**页面，修改IPsec连接的名称、高级配置、互通网段等配置，然后单击**确定**。

   关于参数的详细说明，请参见创建IPsec连接。

5.2.3. 下载IPsec连接配置

创建IPsec连接后，您可以下载IPsec连接的配置。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
3. 在顶部菜单栏，选择IPsec连接的地域。

4. 在**IPsec连接**页面，找到目标IPsec连接，在**操作**列选择 ⋮ > **下载对端配置**。

后续步骤

在您下载IPsec连接配置后，您可以将IPsec连接的配置加载本地网关设备中。具体操作，请参见本地网关配置。

5.2.4. 查看IPsec连接日志

您可以查看一个月内的IPsec连接日志，通过日志信息排查IPsec连接过程中的故障。日志查询的时间周期为10分钟。

操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
3. 在顶部菜单栏，选择IPsec连接的地域。
4. 在**IPsec连接**页面，找到目标IPsec连接，在**操作**列选择 ⋮ > **查看日志**。
5. 在**IPsec连接日志**对话框，设置要查看的日志周期，然后查看日志。

5.2.5. 删除IPsec连接

您可以删除一个不需要的IPsec连接。

操作步骤

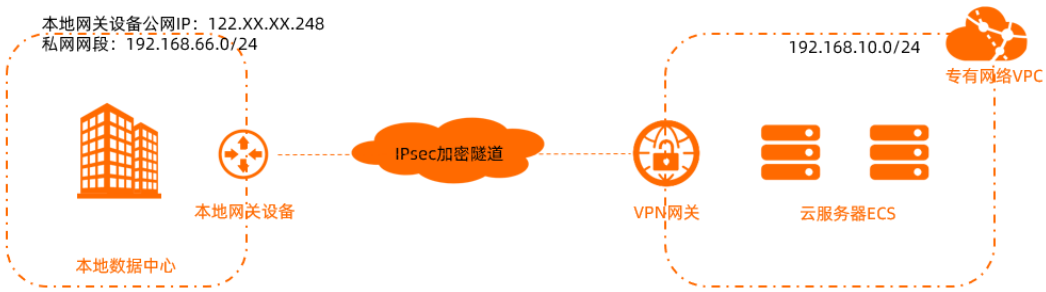
1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
3. 在顶部菜单栏，选择IPsec连接的地域。
4. 在**IPsec连接**页面，找到目标IPsec连接，在**操作**列单击**删除**。
5. 在**请确认是否删除以下资源？**对话框中，单击**确定**。

5.3. 本地网关配置

5.3.1. 华三防火墙配置

使用IPsec-VPN建立站点到站点的连接时，在阿里云侧完成VPN网关的配置后，您还需在本地站点的网关设备中添加VPN配置。本文以华三防火墙为例介绍如何在本地站点的网关设备中添加VPN配置。

场景示例



本文以上图场景为例。某公司在阿里云拥有一个专有网络VPC（Virtual Private Cloud），VPC网段为192.168.10.0/24，VPC中使用云服务器ECS（Elastic Compute Service）部署了应用服务。同时该公司在本地拥有一个数据中心IDC（Internet Data Center），本地IDC网段为192.168.66.0/24。公司因业务发展，需要本地IDC与云上VPC互通，实现资源互访。该公司计划使用VPN网关产品，在本地IDC与云上VPC之间建立IPsec-VPN连接，实现云上和云下的互通。
本示例涉及的网络配置详情请参见下表。

配置项		示例值
VPC	待和本地IDC互通的私网网段	192.168.10.0/24
VPN网关	VPN网关公网IP地址	101.XX.XX.127
本地IDC	待和VPC互通的私网网段	192.168.66.0/24
	本地网关设备的公网IP地址	122.XX.XX.248
	本地网关设备连接公网的接口	Reth1
	本地网关设备连接本地IDC的接口	G2/0/10

前提条件

- 您已在阿里云侧完成创建VPN网关、创建用户网关、创建IPsec连接、配置VPN网关路由的操作。具体操作，请参见建立VPC到本地数据中心的连接。
- 您已下载IPsec连接的配置。具体操作，请参见下载IPsec连接配置。
  本示例IPsec连接的配置如下表所示。

配置项		示例值
预共享密钥		ff123TT****
IKE配置	IKE版本	ikev1
	协商模式	main
	加密算法	aes 说明 如果IPsec连接的加密算法为aes，则华三防火墙设备的加密算法需配置为AES-CBC-128。
	认证算法	sha1
	DH分组	group2
	SA生存周期（秒）	86400

配置项		示例值
IPsec配置	加密算法	aes 说明 如果IPsec连接的加密算法为aes，则华三防火墙设备的加密算法需为AES-CBC-128。
	认证算法	sha1
	DH分组	group2
	SA生存周期（秒）	86400

开始配置

说明 以下内容仅供参考，实际操作请以对应的厂商设备手册为准。

1. 登录华三防火墙Web管理页面。
2. 在左侧导航栏，选择**网络 > VPN > IPsec > 策略**。在**新建IPsec策略**页面，根据已下载的IPsec连接的信息配置IPsec策略的基本信息。

   本示例IPsec策略的基本配置如下图所示。在配置过程中，您需要在**保护的数据流**区域，添加需要加密传输的数据流。
   数据流的源IP地址为本地IDC的私网网段192.168.66.0/24，数据流的目的IP地址为VPC的私网网段192.168.10.0/24。

3. 在左侧导航栏，选择**网络 > VPN > IPsec > IKE提议**，单击**新建**，添加IKE配置。

   本示例IKE配置如下图所示。

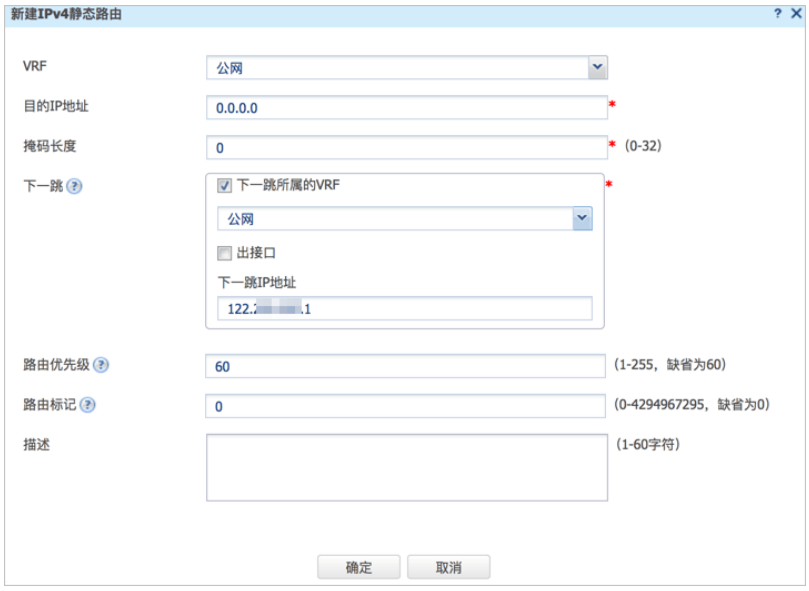
4. 在左侧导航栏，选择**网络 > VPN > IPsec > 策略**，找到新建的IPsec策略，单击**高级配置**，添加IPsec配置。

   本示例IPsec配置如下图所示。

5. 在左侧导航栏，选择**网络 > VPN > IPsec > 策略 > 安全策略 > 新建**，分别创建上行安全策略和下行安全策略。
   - 上行安全策略指流量从本地IDC去往阿里云VPC方向的安全策略。本示例上行安全策略配置如下图所示。

- 下行安全策略指流量从阿里云VPC去往本地IDC方向的安全策略。本示例下行安全策略配置如下图所示。

6. 在左侧导航栏，选择**网络 > 路由 > 静态路由**。在**新建IPv4静态路由**页面，添加静态路由。
   - 为本地IDC去往阿里云VPC方向的流量添加静态路由。本示例配置如下图所示。



   - 为阿里云VPC去往本地IDC方向的流量添加静态路由。

> **说明** 本示例中为直连路由，无需配置该项。请依据您网络的实际情况添加相应的静态路由。

5.3.2. 华为防火墙配置

使用IPsec-VPN建立站点到站点的连接时，在配置完阿里云VPN网关后，您还需在本地站点的网关设备中进行VPN配置。
阿里云VPN网关支持标准的IKEv1和IKEv2协议。因此，只要支持这两种协议的设备都可以和云上VPN网关互连，例如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和 Ixia等。

本文以华为防火墙为例介绍如何在本地站点中加载VPN配置：

配置		示例值
VPC网络配置	vSwitch网段	192.168.10.0/24、 192.168.11.0/24
	VPN网关公网IP	47.xx.xx.10
本地IDC网络配置	私网网段	10.10.10.0/24
	防火墙公网IP	124.xx.xx.215/26
	上行公网网口	10GE1/0/0
	下行私网网口	10GE1/0/1

说明 如果本地IDC侧有多个网段要与VPC互通，建议您在阿里云侧创建多个IPsec连接，并添加VPN网关路由。

配置IKEv1 VPN

前提条件

- 已经在阿里云VPC内创建了IPsec连接，详情参见创建IPsec连接。
- 已经在阿里云VPC管理控制台下载的IPsec连接的配置，本操作中以下表中的配置为例。

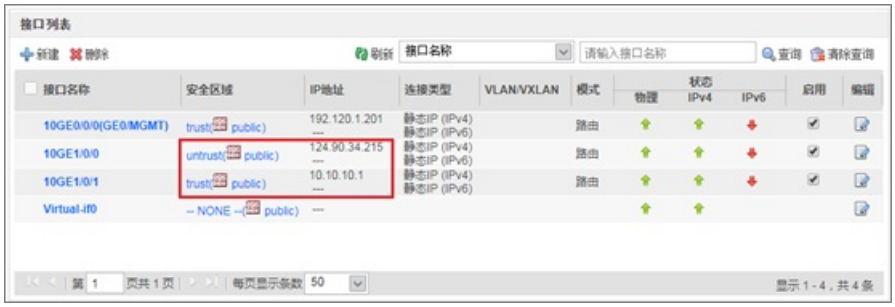
协议	配置	示例值
IKE	认证算法	SHA-1
	加密算法	AES-128
	DH 分组	group 2
	IKE 版本	IKE v1
	生命周期	86400
	协商模式	main
	PSK	123456
	认证算法	SHA-1
	加密算法	AES-128

协议	配置	示例值
IPsec	DH 分组	group 2
	IKE 版本	IKE v1
	生命周期	86400
	协商模式	esp

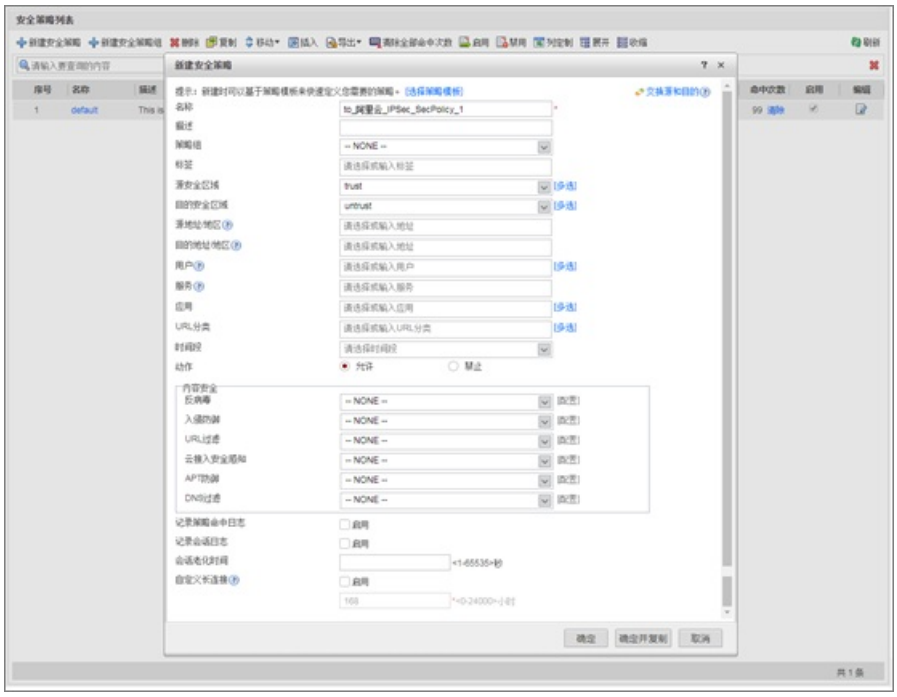
操作步骤

完成以下操作，在华为防火墙中加载用户网关的配置：

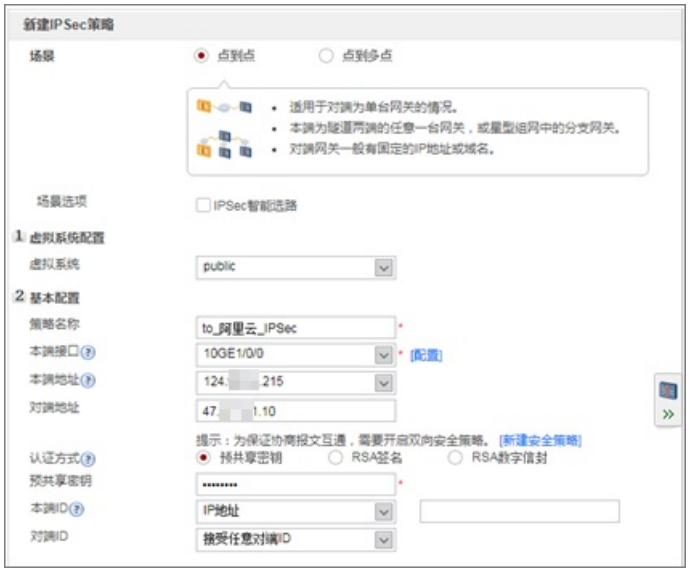
1. 登录防火墙管理页面，选择**网络 > 接口 > 接口列表**。将上行公网网口10GE1/0/0加入untrust安全区域，并配置公网IP；将下行公网网口10GE1/0/1加入trust安全区域，并置私网IP，如下图所示。



2. 选择**策略 > 安全策略 > 新建**，创建安全策略。



3. 选择**网络 > IPsec > IPsec 策略列表 > 新建**，参考以下信息配置VPN对端：
   - **本端接口**：选择防火墙上行公网网口，本操作中选择10GE1/0/0。
   - **对端地址**： 填写阿里云VPN网关的公网IP地址，本操作中输入47.xx.xx.10。
   - 预共享密钥和阿里云侧的PSK一致，本操作中输入123456。



4. 在**待加密的数据流**页面，单击**新建**。参考以下信息，为VPC中所有交换机网段添加待加密数据流：
   - **源地址/地址组**：输入本地IDC的私网网段，本操作中输入10.10.10.0/24。
   - **目的地址/地址组**： 输入VPC的交换机网段，本操作中分别输入192.168.10.0/24和192.168.11.0/24。

5. 在**安全提议**页面，单击**高级**。根据您下载的IPsec连接的配置，配置IKE协议参数。

6. 在**IPsec参数**页面，根据您下载的IPsec连接的配置，配置IPsec协议参数。

7. 选择**网络 > 路由 > 静态路由 > 静态路由列表 > 新建**，为防火墙配置静态路由。其中，添加默认路由时，下一跳为防火墙的公网IP；添加指向VPC的路由时，下一跳为VPN网关的公网IP。

配置IKEv2 VPN

前提条件

- 已经在阿里云VPC内创建了IPsec连接。
- 已经在阿里云VPC管理控制台下载的IPsec连接的配置，本操作中以下表中的配置为例。

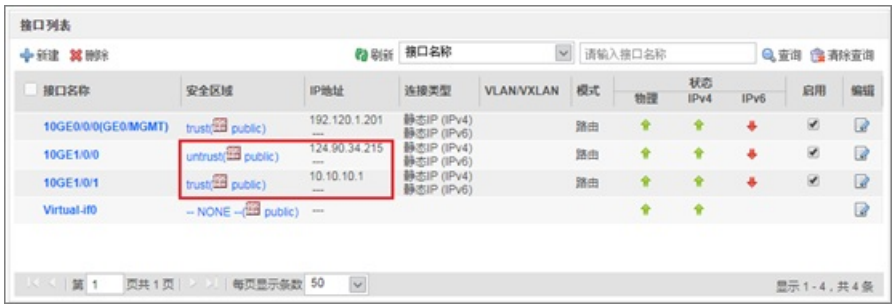
协议	配置	示例值
IKE	认证算法	SHA-1
	加密算法	AES-128
	DH 分组	group 2
	IKE 版本	IKE v2
	生命周期	86400
	PRF算法	SHA-1
	PSK	123456
IPsec	认证算法	SHA-1
	加密算法	AES-128
	DH 分组	group 2
	IKE 版本	IKE v2
	生命周期	86400
	协商模式	esp

操作步骤

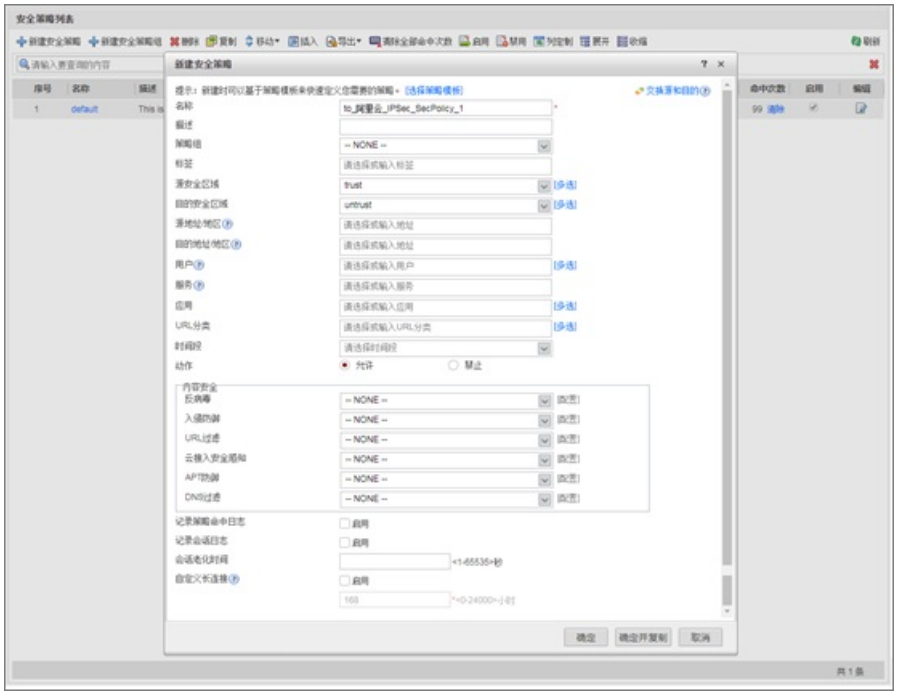
完成以下操作，在华为防火墙中加载用户网关的配置。

1. 登录防火墙管理页面，选择**网络 > 接口 > 接口列表**。将上行公网网口10GE1/0/0加入untrust安全区

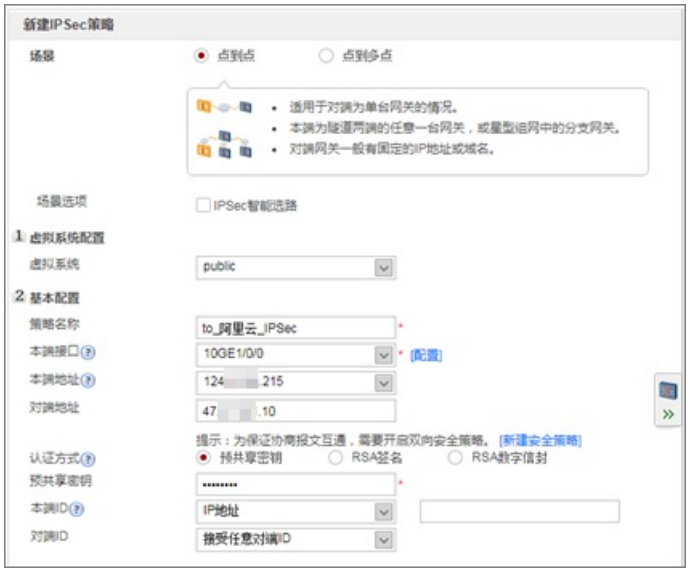
域，并配置公网IP；将下行公网网口10GE1/0/1加入trust安全区域，并置私网IP，如下图所示。



2. 选择**策略 > 安全策略 > 新建**，创建安全策略。



3. 选择**网络 > IPsec > IPsec 策略列表 > 新建**，参考以下信息配置VPN对端。
   - **本端接口**：选择防火墙上行公网网口，本操作中选择10GE1/0/0。
   - **对端地址**： 填写阿里云VPN网关的公网IP地址，本操作中输入47.xx.xx.10。
   - 预共享密钥和阿里云侧的PSK一致，本操作中输入123456。



4. 在**待加密的数据流**页面，单击**新建**。参考以下信息，为VPC中所有交换机网段添加待加密数据流：
   - **源地址/地址组**：输入本地IDC的私网网段，本操作中输入10.10.10.0/24。
   - **目的地址/地址组**： 输入VPC的交换机网段，本操作中分别输入192.168.10.0/24和192.168.11.0/24。

5. 在**安全提议**页面，单击**高级**。根据您下载的IPsec连接的配置，配置IKE协议参数。

6. 在**IPsec参数**页面，根据您下载的IPsec连接的配置，配置IPsec协议参数。

7. 选择**网络 > 路由 > 静态路由 > 静态路由列表 > 新建**，为防火墙配置静态路由。其中，添加默认路由时，下一跳为防火墙的公网IP；添加指向VPC的路由时，下一跳为VPN网关的公网IP。

5.3.3. 山石网科防火墙配置

使用IPsec-VPN建立站点到站点的连接时，在配置完阿里云VPN网关后，您还需在本地站点的网关设备中进行VPN配置。本文以山石防火墙为例介绍如何在本地站点中加载VPN配置。

前提条件

- 确保您已经在阿里云VPC内创建了IPsec连接，详情参见配置站点到站点连接。
- 创建IPsec连接后，获取的IPsec配置信息，详情参见IPsec连接管理。
  本操作的IPsec连接配置如下表所示。
  - IPsec协议信息

配置		示例值
IKE	认证算法	sha1
	加密算法	aes
	DH分组	group2
	IKE版本	ikev1
	生命周期	86400
	协商模式	main
	PSK	hillstone
IPSec	认证算法	sha1
	加密算法	aes
	DH分组	group2
	IKE版本	ikev1
	生命周期	86400

配置		示例值
	安全协议	esp

- 网络配置信息

配置		示例值
VPC信息	私网CIDR	192.168.10.0/24
	网关公网IP	118.31.79.25
IDC信息	私网CIDR	10.90.5.0/24
	网关公网IP	222.92.194.18
	上行公网网口	vlan100
	下行私网网口	E 0/3

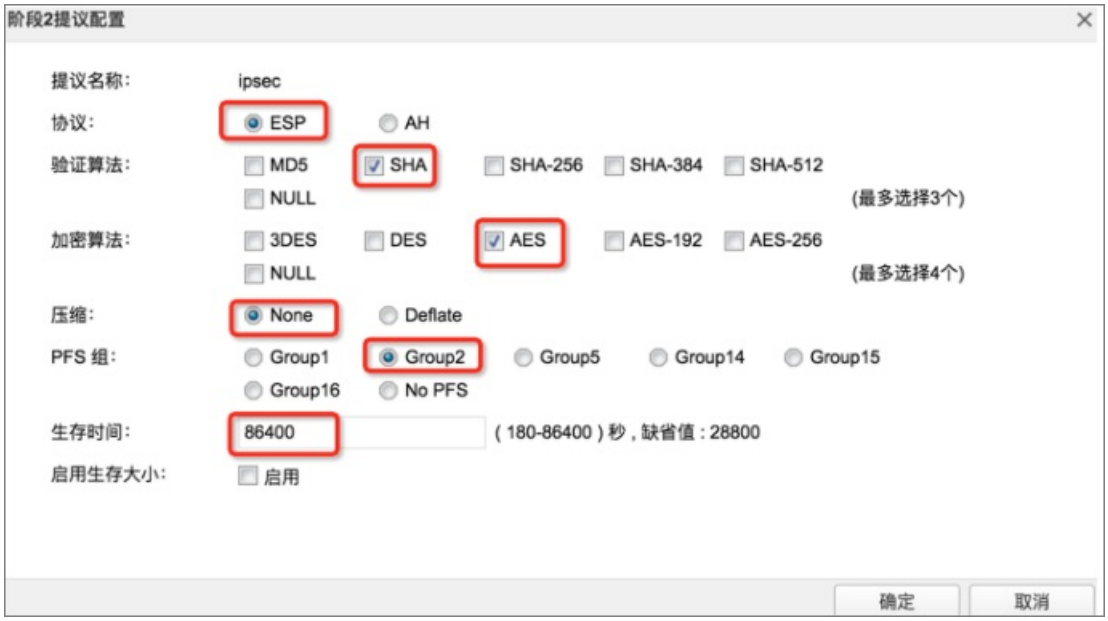
操作步骤

1. 登录防火墙Web页面，选择**网络 > VPN > IPsecVPN > P1提议 - P1提议 > 新建**。

   根据阿里云VPN连接的IKE协议信息配置IDC的IKE协议。

2. 选择**P2提议 > 新建**。

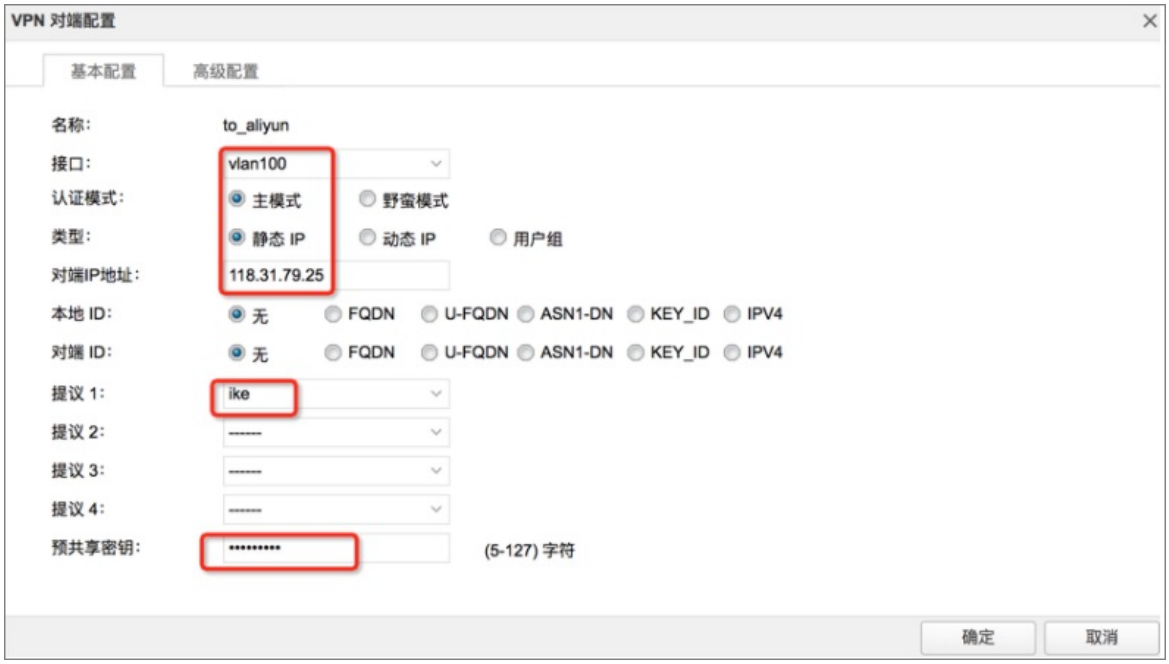
   根据阿里云VPN连接的IPsec协议信息配置IDC的IPsec协议。



3. 选择**VPN对端列表 > 新建**。

   根据以下信息配置VPN对端：

   - **接口**选择防火墙上出方向公网口。
   - **对端IP地址**填写阿里云VPN网关的公网IP地址。
   - **提议**为步骤一创建的p1提议。
   - **预共享密钥**和阿里云侧的PSK一致。如果要打开NAT穿越，可以在高级配置中单击**启用**。



4. 选择**IKE VPN列表 > 新建**。

   根据以下信息配置IKE VPN：

   - **对端选项**选择步骤三创建的VPN对端。
   - **P2提议**为步骤二创建的P2提议。

- **代理ID**选择**手工**，并在**代理ID列表**中输入**本地IP/掩码**即本地IDC的私网网段10.90.5.0/24；在**远程IP/掩码**中输入为阿里云VPC的网段192.168.10.0/24，然后单击**添加**。

5. 选择**网络 > 安全域 > 新建**。

   在**安全域名称**页面，输入安全域的名称，并在**类型**中选择**三层安全域**。

6. 选择**网络 > 接口 > 新建**。

   根据以下信息，配置隧道接口：

   - 在**接口名称**中输入”tunnelX”，x的取值范围为1-512，例如 `tunnel5` 。
   - **安全域**选择之前创建的安全域。
   - **隧道类型**选择**IPSec VPN**。
   - **VPN 名称**选择之前创建的VPN。

7. 选择**策略 > 安全策略 > 新建**。

8. 选择**网络 > 路由 > 新建**。

   分别添加上行和下行路由：

   - 上行路由：目的地址为阿里云VPC的网段，下一跳为新建的隧道接口。

- 下行路由：由于本例中防火墙下行口地址10.90.5.1/24，属于本地IDC的私网网段10.90.5.0/24，所以已经存在本地直连路由。

5.3.4. strongSwan配置

使用IPsec-VPN建立站点到站点的连接时，在配置完VPN网关后，您还需在本地IDC的网关设备中进行VPN配置。本文以strongSwan为例介绍如何在本地IDC的网关设备中加载VPN配置。

前提条件

- 您已经创建了IPsec连接。具体操作，请参见建立VPC到本地数据中心的连接。
- 您已经获得IPsec连接的配置信息。具体操作，请参见下载IPsec连接配置。
  本文示例中，VPN网关使用的IPsec连接配置信息如下所示：

协议	配置	示例值
IKE	认证算法	sha1
	加密算法	aes
	DH分组	group2
	IKE 版本	ikev1
	生命周期	86400
	协商模式	main
	预共享密钥（PSK）	123456

协议	配置	示例值
IPsec	认证算法	sha1
	加密算法	aes
	DH分组	group2
	生命周期	86400

场景说明

本文以下图场景为例。本地IDC和阿里云VPC之间通过IPsec VPN互通，其中：

- 阿里云VPC的网段是192.168.10.0/24。
- 本地IDC的网段是172.16.2.0/24。
- strongSwan的公网IP地址是59.XX.XX.70。

步骤一：安装strongSwan软件

1. 运行以下命令安装strongSwan软件。

```
yum install strongswan
```

2. 运行以下命令查看安装的软件版本。

```
strongswan version
```

步骤二：配置strongSwan

1. 运行以下命令打开*ipsec.conf*配置文件。

```
vi /etc/strongswan/ipsec.conf
```

2. 参考以下配置，更改*ipsec.conf*的配置。

```
ipsec.conf - strongSwan IPsec configuration file
basic configuration
 config setup
     uniqueids=never
 conn %default
     authby=psk                    #使用预共享密钥认证方式
     type=tunnel
 conn tomyidc
     keyexchange=ikev1             #IPsec连接使用的IKE协议的版本
     left=59.XX.XX.70
     leftsubnet=172.16.2.0/24      #本地IDC的网段
     leftid=59.XX.XX.70            #本地IDC网关设备的公网IP地址
     right=119.XX.XX.125
     rightsubnet=192.168.10.0/24 #VPC的网段
     rightid=119.XX.XX.125         #VPN网关的公网IP地址
     auto=route
     ike=aes-sha1-modp1024         #IPsec连接中IKE协议的加密算法-认证算法-DH分组
     ikelifetime=86400s            #IKE协议的SA生命周期
     esp=aes-sha1-modp1024         #IPsec连接中IPsec协议的加密算法-认证算法-DH分组
     lifetime=86400s               #IPsec协议的SA生命周期
     type=tunnel
```

3. 配置*ipsec.secrets*文件。
   i. 运行以下命令打开配置文件。

   ```
   vi /etc/strongswan/ipsec.secrets
   ```

   ii. 添加如下配置。

   ```
   59.XX.XX.70 119.XX.XX.125 : PSK 123456   #123456为IPsec连接的预共享密钥，本地IDC侧和VPN网关侧的预共享密钥需一致
   ```

4. 打开系统转发配置。

   ```
   echo 1 > /proc/sys/net/ipv4/ip_forward
   ```

   更多场景配置示例，参见场景配置示例。

5. 执行以下命令启动strongSwan服务。

   ```
   systemctl enable strongswan
   systemctl start strongswan
   ```

6. 在您本地IDC侧，设置IDC客户端到strongSwan网关及strongSwan网关到IDC客户端的路由。

> **说明** 如果您使用strongSwan建立了3条（不包含3条）以上的IPsec连接，您需要修改*/etc/strongswan/strongswan.d/charon.conf*中的配置：您需要删除 `max_ikev1_exchanges = 3` 命令前的注释符号，启用此命令，并修改命令中参数的值大于您建立的IPsec连接数。
> 例如：您使用strongSwan建立了4条IPsec连接，您可以修改该命令为 `max_ikev1_exchanges = 5` 。

5.3.5. 深信服防火墙配置

使用IPsec-VPN建立站点到站点的连接时，在配置完阿里云VPN网关后，您还需在本地站点的网关设备中进行VPN配置。本文以深信服防火墙为例介绍如何在本地站点中加载VPN配置。

前提条件

- 已经在阿里云VPC内创建了IPsec连接。详细说明，请参见创建IPsec连接。
- 已经下载了IPsec连接的配置。详细说明，请参见下载IPsec连接配置。
  本操作的IPsec连接配置如下表所示。
  IPsec协议信息

配置		示例值
IKE	认证算法	md5
	加密算法	3des
	DH分组	group2
	IKE版本	IKE v1
	生命周期	28800
	协商模式	aggressive
	PSK	123456
IPsec	认证算法	md5
	加密算法	des
	DH分组	group2
	IKE版本	IKE v1
	生命周期	28800

网络配置信息

配置		示例值
VPC配置	私网CIDR	192.168.1.0/24
	网关公网IP	47.xxx.xxx.56
IDC网络配置	私网CIDR	192.168.18.0/24
	网关公网IP	122.xxx.xxx.248

操作步骤

1. 登录深信服防火墙的Web页面，单击**VPN配置 > 第三方对接 > 第一阶段**，然后单击**新增**。
   根据阿里云VPN连接的IKE协议信息配置IDC的第一阶段。

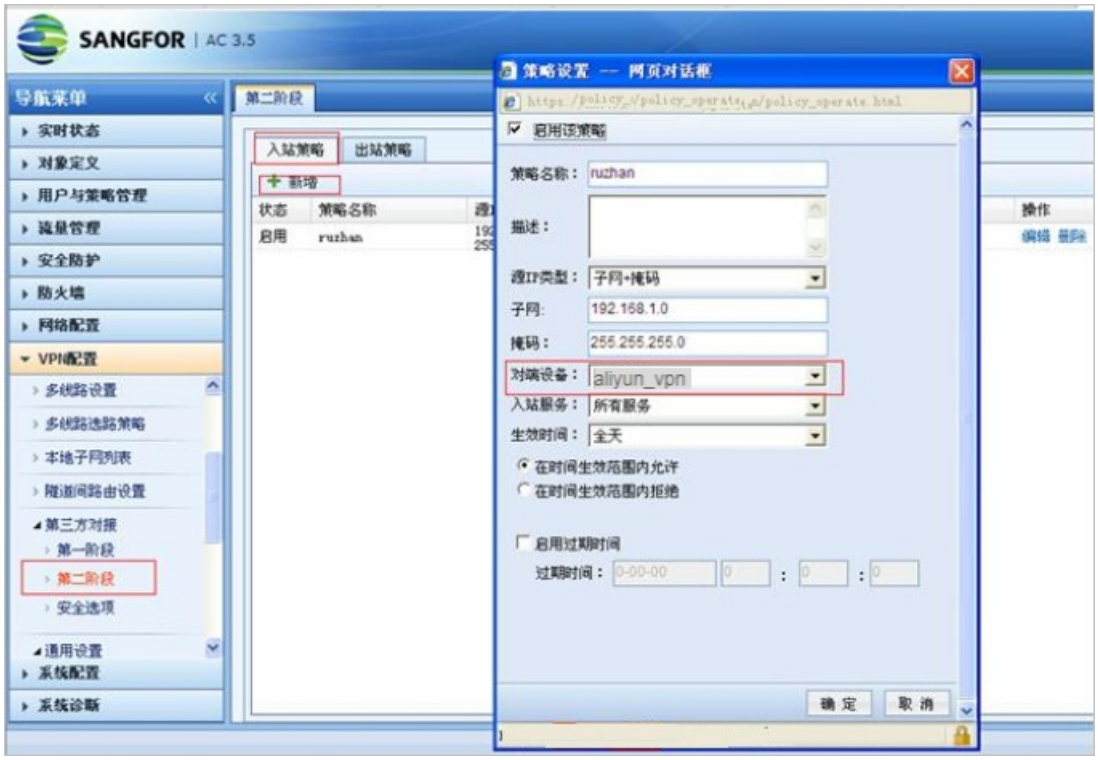
配置	说明
设备名称	自定义设备名称。

配置	说明
描述	输入描述信息。
线路出口	选择IPsec隧道出口。
设备地址类型	选择对端是固定IP。
固定IP	输入VPC侧公网IP，本示例为47.xxx.xxx.56。
认证方式	选择预共享密钥。
预共享密钥	输入预共享密钥，本示例为123456。
确认密钥	再次输入预共享密钥。
高级	
ISAKMP存活时间（秒）	输入ISAKMP存活时间，本示例为28800。
重试次数	输入重新发起IPsec连接的次数。
支持模式	选择野蛮模式。
D-H群	本示例选择MOOP 1024群（2）。
身份类型	选择验证身份的类型，本示例选择IPv4地址（IPv4 ADDR）。
我方身份ID	输入本端公网IP地址，本示例为122.xxx.xxx.248。
对方身份ID	输入VPC端公网IP地址，本示例47.xxx.xxx.56。
启用NAT穿透	本示例选择启用NAT穿透。
认证算法	选择认证算法，本示例为MD5。
加密算法	选择加密算法，本示例为3DES。

2. 单击**VPN配置 > 第三方对接 > 第二阶段**，然后单击**入站策略**。

   根据网络配置信息，配置IDC的入站策略。

配置	说明
策略名称	自定义策略名称。
描述	输入描述信息。
源IP类型	选择源IP的类型，本示例为子网+掩码。
子网	输入VPC侧的子网，本示例为192.168.1.0。
掩码	输入VPC侧的掩码，本示例为255.255.255.0。
对端设备	选择第一阶段配置设备名称。
入站服务	选择允许开放的服务。
生效时间	选择策略生效的时间。



3. 单击**VPN配置 > 第三方对接 > 第二阶段**，然后单击**出站策略**。

   根据网络配置信息，配置IDC的出站策略。

配置	说明
策略名称	自定义策略名称。
描述	输入描述信息。
源IP类型	选择源IP的类型，本示例为子网+掩码。
子网	输入本端子网，本示例为192.168.18.0。
掩码	输入本端的掩码，本示例为255.255.255.0。
对端设备	选择第一阶段配置设备名称。
出站服务	选择允许开放的服务。
安全选项	选择安全选项，本示例为默认安全选项。
生效时间	选择策略生效的时间。

4. 单击**VPN配置 > 第三方对接 > 安全选项**。

   根据阿里云VPN连接的IPsec协议信息配置IDC的安全选项。

配置	说明
名称	自定义名称。
描述	输入描述信息。
协议	选择第二阶段认证协议，本示例为ESP。
认证算法	选择第二阶段认证算法，本示例为MD5。
加密算法	选择第二阶段加密算法，本示例为DES。

5.3.6. Juniper防火墙配置

使用IPsec-VPN建立站点到站点的连接时，在配置完阿里云VPN网关后，您还需在本地站点的网关设备中进行VPN配置。本文以Juniper防火墙为例介绍如何在本地站点中加载VPN配置。

前提条件

- 已经在阿里云VPC内创建了IPsec连接。详细说明，请参见创建IPsec连接。
- 已经下载了IPsec连接的配置。详细说明，请参见下载IPsec连接配置。
  本操作的IPsec连接配置如下表所示。

- IPsec协议信息

配置		示例值
IKE	认证算法	md5
	加密算法	3des
	DH分组	group2
	IKE版本	IKE v1
	生命周期	86400
	协商模式	main
	PSK	123456
IPsec	认证算法	md5
	加密算法	des
	DH分组	group2
	IKE版本	IKE v1
	生命周期	28800

- 网络配置信息

配置		示例值
VPC配置	私网CIDR	192.168.1.0/24
	网关公网IP	47.xxx.xxx.56
IDC网络配置	私网CIDR	192.168.18.0/24
	网关公网IP	122.xxx.xxx.248

操作步骤

完成以下操作，在Juniper防火墙中加载用户网关的配置：

1. 登录防火墙设备的命令行配置界面。
2. 配置基本网络、安全域和地址簿信息。

```
set security zones security-zone trust address-book address net-cfgr_192-168-18-0--24 1
92.168.18.0/24
set security zones security-zone vpn address-book address net-cfgr_192-168-1-0--24 192.
168.1.0/24
```

3. 配置IKE策略。

```
set security ike policy ike-policy-cfgr mode main
set security ike policy ike-policy-cfgr pre-shared-key ascii-text "123456"
```

4. 配置IKE网关、出接口和协议版本。

```
set security ike gateway ike-gate-cfgr ike-policy ike-policy-cfgr
set security ike gateway ike-gate-cfgr address 47.xxx.xxx.56
set security ike gateway ike-gate-cfgr external-interface ge-0/0/3
set security ike gateway ike-gate-cfgr version v1-only
```

5. 配置IPsec策略。

```
set security ipsec policy ipsec-policy-cfgr proposal-set standard
```

6. 应用IPsec策略。

```
set security ipsec vpn ipsec-vpn-cfgr ike gateway ike-gate-cfgr
set security ipsec vpn ipsec-vpn-cfgr ike ipsec-policy ipsec-policy-cfgr
set security ipsec vpn ipsec-vpn-cfgr bind-interface st0.0
set security ipsec vpn ipsec-vpn-cfgr establish-tunnels immediately
set security ipsec policy ipsec-policy-cfgr perfect-forward-secrecy keys group2
```

7. 配置出站策略。

```
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr match source-ad
dress net-cfgr_192-168-18-0--24
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr match destinati
on-address net-cfgr_192-168-1-0--24
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr match applicati
on any
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr then permit
```

8. 配置入站策略。

```
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr match source-ad
dress net-cfgr_192-168-1-0--24
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr match destinati
on-address net-cfgr_192-168-18-0--24
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr match applicati
on any
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr then permit
```

5.3.7. 思科防火墙配置

使用IPsec-VPN建立站点到站点的连接时，在配置完阿里云VPN网关后，您还需在本地站点的网关设备中进行VPN配置。本文以思科防火墙为例介绍如何在本地站点中加载VPN配置。

背景信息

VPC和本地IDC的网络配置如下：

配置		示例值
VPC网络配置	vSwitch网段	192.168.10.0/24、 192.168.11.0/24

配置		示例值
	VPN网关公网IP	47.XX.XX.161
本地IDC网络配置	私网网段	10.10.10.0/24
	防火墙公网IP	124.XX.XX.171

说明 如果本地IDC侧有多个网段要与VPC互通，建议您在阿里云侧创建多个IPsec连接，并添加VPN网关路由。

配置IKEv1 VPN

前提条件：

- 您已经在阿里云VPC内创建了IPsec连接。具体操作，请参见创建IPsec连接。
- 您已经下载了IPsec连接的配置。具体操作，请参见下载IPsec连接配置。本操作中以下表中的配置为例。

协议	配置	示例值
IKE	认证算法	SHA-1
	加密算法	AES-128
	DH 分组	group 2
	IKE 版本	IKE v1
	生命周期	86400
	协商模式	main
	PSK	123456
IPsec	认证算法	SHA-1
	加密算法	AES-128
	DH 分组	group 2
	IKE 版本	IKE v1
	生命周期	86400
	协商模式	esp

1. 登录防火墙设备的命令行配置界面。
2. 配置isakmp策略。

```
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group  2
lifetime 86400
```

3. 配置预共享密钥。

```
crypto isakmp key 123456 address 47.XX.XX.161
```

4. 配置IPsec安全协议。

```
crypto ipsec transform-set ipsecpro64 esp-aes esp-sha-hmac
mode tunnel
```

5. 配置ACL（访问控制列表），定义需要保护的数据流。

> **说明** 如果本地网关设备配置了多网段，则需要分别针对多个网段添加ACL策略。

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.11.0 0.0.0.255
```

6. 配置IPsec策略。

```
crypto map ipsecpro64 10 ipsec-isakmp
set peer 47.XX.XX.161
set transform-set ipsecpro64
set pfs group2
match address 100
```

7. 应用IPsec策略。

```
interface g0/0
crypto map ipsecpro64
```

8. 配置静态路由。

```
ip route 192.168.10.0 255.255.255.0 47.XX.XX.161
ip route 192.168.11.0 255.255.255.0 47.XX.XX.161
```

9. 测试连通性。

   您可以利用您在云中的主机和您数据中心的主机进行连通性测试。

配置IKEv2 VPN

前提条件：

- 已经在阿里云VPC内创建了IPsec连接。具体操作，请参见创建IPsec连接。
- 已经下载了IPsec连接的配置。具体操作，请参见下载IPsec连接配置。本操作中以下表中的配置为例。

协议	配置	示例值
	认证算法	SHA-1

协议	配置	示例值
IKE	加密算法	AES-128
	DH 分组	group 2
	IKE 版本	IKE v2
	生命周期	86400
	PRF算法	SHA-1
	PSK	123456
IPsec	认证算法	SHA-1
	加密算法	AES-128
	DH 分组	group 2
	IKE 版本	IKE v2
	生命周期	86400
	协商模式	esp

1. 登录防火墙设备的命令行配置界面。
2. 配置IKE第一阶段算法。

```
crypto ikev2 proposal daemon
encryption aes-cbc-128
integrity sha1
group 2
```

3. 配置IKE v2策略，并应用proposal。

```
crypto ikev2 policy ipsecpro64_v2
proposal daemon
```

4. 配置预共享密钥。

```
crypto ikev2 keyring ipsecpro64_v2
peer vpngw
address 47.XX.XX.161
pre-shared-key 0 123456
```

5. 配置身份认证。

```
crypto ikev2 profile ipsecpro64_v2
match identity remote address 47.XX.XX.161 255.255.255.255
identity local address 10.10.10.1
authentication remote pre-share
authentication local pre-share
keyring local ipsecpro64_v2
```

6. 配置IPsec安全协议。

```
crypto ipsec transform-set ipsecpro64_v2 esp-aes esp-sha-hmac
mode tunnel
```

7. 配置ACL（访问控制列表），定义需要保护的数据流。

> **说明** 如果本地网关设备配置了多网段，则需要分别针对多个网段添加ACL策略。

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.11.0 0.0.0.255
```

8. 配置IPsec策略。

```
crypto map ipsecpro64_v2 10 ipsec-isakmp
set peer 47.XX.XX.161
set transform-set ipsecpro64_v2
set pfs group2
set ikev2-profile ipsecpro64_v2
match address 100
```

9. 应用IPsec策略。

```
interface g0/1
crypto map ipsecpro64_v2
```

10. 配置静态路由。

```
ip route 192.168.10.0 255.255.255.0 47.XX.XX.161
ip route 192.168.11.0 255.255.255.0 47.XX.XX.161
```

11. 测试连通性。

    您可以利用您在云中的主机和您数据中心的主机进行连通性测试。

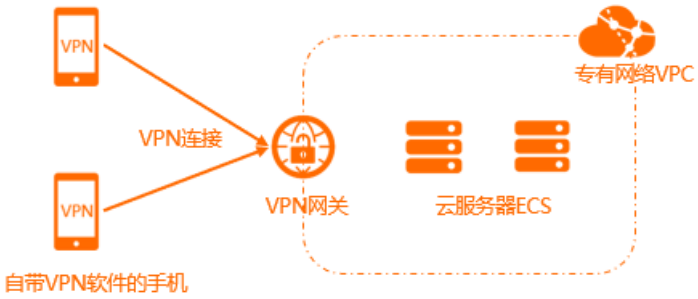
6.IPsec服务端

6.1. IPsec服务端配置简介

VPN网关的IPsec服务端功能，能让您通过手机端自带的VPN应用和阿里云建立VPN连接，实现手机端和云上资源的互通。

使用场景

IPsec服务端通过IPsec协议实现端到站点的连接，让您能通过手机端自带的VPN应用连接到阿里云的VPN网关，和阿里云建立安全可靠的VPN连接，实现和云上资源的互通。



使用限制

- 目前，仅以下地域支持IPsec服务端功能：华东1（杭州）、华东2（上海）、华东5（南京-本地地域）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华北6（乌兰察布）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）、日本（东京）、韩国（首尔）、新加坡、澳大利亚（悉尼）、马来西亚（吉隆坡）、印度尼西亚（雅加达）、菲律宾（马尼拉）、泰国（曼谷）、印度（孟买）、德国（法兰克福）、英国（伦敦）、美国（弗吉尼亚）、美国（硅谷）、阿联酋（迪拜）。
- IPsec服务端仅支持连接iOS系统的手机。
- 一个VPN网关实例，仅支持创建一个IPsec服务端。
- 对于一个VPN网关实例，如果同时创建了SSL服务端和IPsec服务端，则SSL服务端和IPsec服务端共同使用该VPN网关的SSL连接数。
  例如：您的一个VPN网关实例购买了20个SSL连接数，其中SSL服务端已经连接了5个客户端，则IPsec服务端最多还能连接15个客户端。

环境要求

在您使用IPsec服务端功能前，请确保您的环境满足以下条件：

- 您已经在目标地域创建了专有网络。具体操作，请参见搭建IPv4专有网络。
- 您的手机端能访问互联网。
- 您的手机端的系统为iOS。
- 请确保您ECS实例的安全组规则允许手机端访问。具体操作，请参见查询安全组规则和添加安全组规则。

使用流程

1. 创建VPN网关
   创建VPN网关并开启SSL-VPN功能。
2. 创建IPsec服务端
   在IPsec服务端中指定客户端（即手机端）要访问的IP地址段和客户端要使用的IP地址段。
3. 在手机端配置VPN连接信息
   在手机端配置VPN网关的信息，建立VPN连接。
4. 测试连通性
   手机端和VPN网关建立VPN连接后，您可以在手机端尝试访问云端资源，验证网络的连通性。

关于IPsec服务端的使用示例，请参见使用手机（iOS系统）自带的VPN软件建立远程连接。

相关文档

- 在您创建IPsec服务端后，您可以通过查看IPsec服务端的日志，进行故障排查。具体操作，请参见查看IPsec服务端日志。
- 关于IPsec服务端的相关操作文档，请参见：
  - 创建和管理VPN网关实例
  - 创建和管理IPsec服务端
  - 客户端配置

IPsec服务端和SSL服务端的区别是什么？

对比项	IPsec服务端	SSL服务端
使用场景	提供端到站点的连接。	提供端到站点的连接。
客户端模式	支持手机端建立和阿里云的VPN连接。	支持电脑等终端建立和阿里云的VPN连接。
客户端连接模式	手机端通过自带的VPN应用和阿里云建立VPN连接。	电脑等终端通过OpenVPN软件和阿里云建立VPN连接。
加密方式	IPsec协议	SSL证书

6.2. 创建和管理IPsec服务端

您可以通过IPsec服务端，使用手机端（iOS系统）自带的VPN应用和阿里云建立IPsec-VPN连接。本文为您介绍如何创建、修改和删除IPsec服务端。

前提条件

- 您已经了解IPsec服务端的使用限制和环境要求。更多信息，请参见使用限制和环境要求。
- 您已经创建VPN网关实例且VPN网关实例已开启SSL-VPN功能。具体操作，请参见创建和管理VPN网关实例。

创建IPsec服务端

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > IPsec服务端**。
3. 在顶部菜单栏，选择IPsec服务端的地域。

   单击查看IPsec服务端支持的地域
   华东1（杭州）、华东2（上海）、华东5（南京-本地地域）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华北6（乌兰察布）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）、日本（东京）、韩国（首尔）、新加坡、澳大利亚（悉尼）、马来西亚（吉隆坡）、印度尼西亚（雅加达）、菲律宾（马尼拉）、泰国（曼谷）、印度（孟买）、德国（法兰克福）、英国（伦敦）、美国（弗吉尼亚）、美国（硅谷）、阿联酋（迪拜）
4. 在**IPsec服务端**页面，单击**创建IPsec服务端**。
5. 在**创建IPsec服务端**页面，根据以下信息进行配置，然后单击**确定**。

配置项	说明
名称	输入IPsec服务端的名称。 名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）和短划线（-）。
VPN网关	输入IPsec服务端所关联的VPN网关实例。 **说明** IPsec服务端创建完成后，不支持修改关联的VPN网关实例。
本端网段	输入客户端通过IPsec服务端要访问的地址段。 本端网段可以是专有网络VPC（Virtual Private Cloud）的网段、交换机的网段、通过物理专线和VPC互连的本地数据中心的网段等。 单击**添加本端网段**添加多个本端网段。
客户端网段	客户端网段是给客户端虚拟网卡分配IP地址的网段，不是指客户端已有的内网网段。当客户端通过IPsec服务端连接访问本端时，VPN网关会从指定的客户端网段中分配一个IP地址给客户端使用。 **注意** ○ 请确保客户端网段与本端网段以及VPC中的网段不冲突。 ○ 请确保您指定的客户端网段所包含的IP地址个数是VPN网关中SSL连接数的4倍及以上。 例如：您指定的客户端网段为192.168.0.0/24，系统在为客户端分配IP地址时，会先从192.168.0.0/24网段中划分出一个子网掩码为30的子网段，例如192.168.0.4/30，然后从192.168.0.4/30中分配一个IP地址供客户端使用，剩余三个IP地址会被系统占用以保证网络通信，此时一个客户端会耗费4个IP地址。因此，请确保您指定的客户端网段所包含的IP地址个数是VPN网关中SSL连接数的4倍及以上。

配置项	说明
预共享密钥	输入IPsec服务端的认证密钥，用于IPsec服务端与客户端之间的身份认证。密钥长度为1~100个字符。 若您未指定预共享密钥，系统会随机生成一个16位的字符串作为预共享密钥。创建IPsec服务端后，您可以通过**编辑**按钮查看系统生成的预共享密钥。具体操作，请参见修改IPsec服务端。 **注意** 客户端的认证密钥需和IPsec服务端侧的预共享密钥一致，否则客户端和IPsec服务端之间无法建立连接。
立即生效	选择是否立即生效。 ○ **是**：配置完成后立即进行协商。 ○ **否**：当有流量进入时进行协商。
高级配置：IKE配置	
版本	IKE协议的版本。 ○ **ikev1** ○ **ikev2** 目前系统支持IKE V1和IKE V2，相对于IKE V1版本，IKE V2版本简化了协商过程并且对于多网段的场景提供了更好的支持，建议您选择IKE V2版本。
LocalId	IPsec服务端的标识，支持FQDN格式和IP地址格式。默认值为VPN网关的公网IP地址。
RemoteId	客户端的标识，支持FQDN格式和IP地址格式。默认值为空。

修改IPsec服务端

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
3. 在顶部菜单栏，选择IPsec服务端的地域。
4. 在**IPsec服务端**页面，找到目标IPsec服务端实例，在**操作**列单击**编辑**。
5. 在**编辑IPsec服务端**页面，更改IPsec服务端的配置，然后单击**确定**。

   关于参数的说明，请参见创建IPsec服务端。

删除IPsec服务端

删除IPsec服务端时，系统会自动断开当前IPsec服务端已连接的客户端。

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
3. 在顶部菜单栏，选择IPsec服务端的地域。
4. 在**IPsec服务端**页面，找到目标IPsec服务端实例，在**操作**列单击**删除**。
5. 在**删除Ipsec服务端配置**对话框，确认删除信息，然后单击**确定**。

相关文档

- CreateIpsecServer：创建IPsec服务端。
- ListIpsecServers：查询已创建的IPsec服务端的信息。
- UpdateIpsecServer：修改IPsec服务端的配置。
- DeleteIpsecServer：删除IPsec服务端。

6.3. 客户端配置

在您创建IPsec服务端后，您还需要完成客户端（即手机端）的配置，才能建立手机端和阿里云的VPN连接。

前提条件

在您开始以下操作前，请确保您已经满足以下条件：

- 您已经创建了IPsec服务端。具体操作，请参见创建和管理IPsec服务端。
- 您已经在VPN网关管理控制台获取到以下信息：
  - 您的IPsec服务端所关联的VPN网关的公网IP地址。
  - 您的IPsec服务端使用的IKE的版本。
  - 您的IPsec服务端使用的预共享密钥。

iOS手机端配置

目前，IPsec服务端仅支持连接iOS系统的手机。本操作以iOS 14系统为例，为您介绍如何在手机端配置VPN连接信息。

1. 打开手机端的**设置**。
2. 选择**通用 > VPN > 添加VPN配置**。
3. 在**添加配置**页面，根据以下信息配置VPN。
   - **类型**：选择手机端的VPN的类型。
     本项的配置需要和IPsec服务端使用的IKE版本一致。
   - **描述**：输入手机端的VPN的描述信息。
   - **服务器**：输入手机端要连接的云上VPN网关的公网IP地址。
   - **远程ID**：输入手机端要连接的云上VPN网关的公网IP地址。
   - **本地ID**：输入手机端的标识，可以为空。
   - **用户鉴定**：选择**无**。
   - **使用证书**：选择**关闭**。
   - **密钥**：用于IPsec服务端与手机端之间的身份认证，建立IPsec连接时要求两端密钥必须一致。
     本项输入IPsec服务端使用的预共享密钥。
   - **代理**：不使用代理。保持默认值**关闭**。
4. 单击**完成**。
5. 在**VPN**页面，选中目标VPN配置，打开**状态**开关。

待VPN状态显示**已连接**表示VPN连接成功。

6.4. 查看IPsec服务端日志

您可以查看IPsec服务端的日志信息，通过日志信息排查客户端连接IPsec服务端过程中的问题。

背景信息

系统自动为您保留最近一个月内的IPsec服务端的日志信息，您可以分批次进行查看，一次可查看的日志周期最长为10分钟。

操作步骤

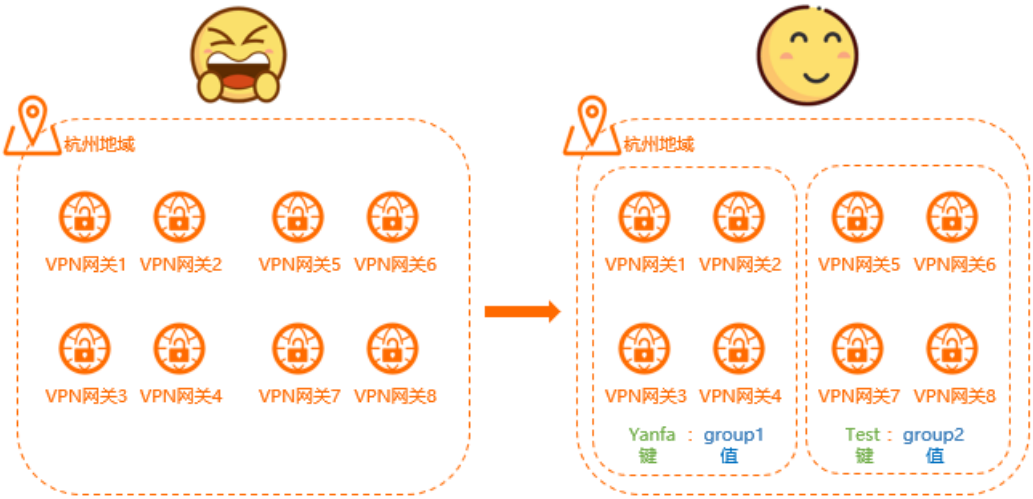
1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > IPsec服务端**。
3. 在顶部菜单栏，选择IPsec服务端的地域。
4. 在**IPsec服务端**页面，找到目标IPsec服务端实例，在**操作**列单击**查看日志**。
5. 在**IPsec服务端日志**页面，设置要查看的日志周期，查看日志。

7.标签管理

7.1. 标签概述

VPN网关支持标签管理功能，您可以通过标签对VPN网关实例进行标记和分类，便于资源的搜索和聚合。

功能简介



如上图，随着VPN网关实例数量的增多，会加大对实例的管理难度。通过标签将实例进行分组管理，有助于您搜索和筛选实例。

标签是您为实例分配的标记，每个标签都由一对键值对（Key-Value）组成。标签的使用说明如下：

- 一个实例上的每条标签的标签键（Key）必须唯一。
- 不支持未绑定实例的空标签存在，标签必须绑定在实例上。
- 不同地域中的标签信息不互通。
  例如，在华东1（杭州）地域创建的标签在华东2（上海）地域不可见。
- 您可以修改标签的键和值，也可以随时删除实例的标签。如果删除实例，绑定实例的所有标签也会被删除。

使用限制

一个VPN网关实例最多可以绑定20条标签，暂不支持提升配额。

相关操作

标签管理相关的操作如下表所示。

操作描述	控制台	API
添加标签	为单个实例添加标签	TagResources
	为多个实例批量添加标签	
使用标签搜索实例	使用标签搜索实例	ListTagResources
	为单个实例删除标签	

删除标签 操作描述	控制台	UnTagResources API
	为多个实例批量删除标签	

7.2. 添加标签

7.2.1. 为单个实例添加标签

标签是您为实例分配的标记，您可以根据添加的标签搜索和筛选实例。本文介绍如何为单个实例添加标签。

背景信息

您可以为每个实例最多添加20条标签，标签的使用说明如下：

- 一个实例上的每条标签的标签键（Key）必须唯一。
- 不支持未绑定实例的空标签存在，标签必须绑定在实例上。
- 不同地域中的标签信息不互通。
  例如，在华东1（杭州）地域创建的标签在华东2（上海）地域不可见。
- 您可以修改标签的键和值，也可以随时删除实例的标签。如果删除实例，绑定实例的所有标签也会被删除。

操作步骤

1.
2. 在顶部菜单栏处，选择VPN网关的地域。
3. 在**VPN网关**页面，找到目标VPN网关实例，将鼠标悬停在**标签**列下的 图标上，然后单击气泡框中的**添加**。
4. 在**编辑标签**对话框中，根据以下信息配置标签，然后单击**确定**。

配置	说明
标签键	标签的标签键，支持选择已有标签键或输入新的标签键。 标签键最多支持64个字符，不能以 `aliyun` 或 `acs:` 开头，不能包含 `http://` 和 `https://` 。
标签值	标签的标签值，支持选择已有标签值或输入新的标签值。 标签值最多支持128个字符，不能以 `aliyun` 或 `acs:` 开头，不能包含 `http://` 和 `https://` 。

相关文档

- TagResources

7.2.2. 为多个实例批量添加标签

标签是您为实例分配的标记，您可以根据添加的标签搜索和筛选实例。本文介绍如何为多个实例批量添加标签。

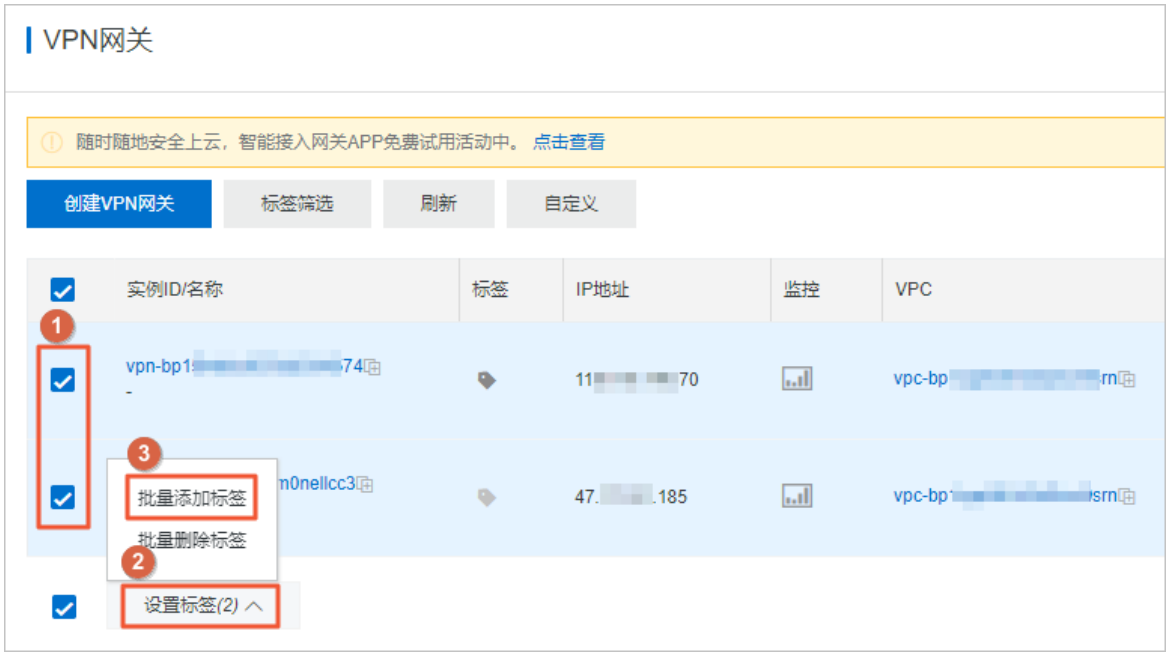
背景信息

您可以为每个实例最多添加20条标签，标签的使用说明如下：

- 一个实例上的每条标签的标签键（Key）必须唯一。
- 不支持未绑定实例的空标签存在，标签必须绑定在实例上。
- 不同地域中的标签信息不互通。
  例如，在华东1（杭州）地域创建的标签在华东2（上海）地域不可见。
- 您可以修改标签的键和值，也可以随时删除实例的标签。如果删除实例，绑定实例的所有标签也会被删除。

操作步骤

1.
2. 在顶部菜单栏处，选择VPN网关的地域。
3. 在**VPN网关**页面，选中需要批量添加标签的实例，单击**设置标签 > 批量添加标签**。



4. 在**批量编辑标签**对话框中，根据以下信息配置标签，然后单击**确定**。

配置	说明
标签键	标签的标签键，支持选择已有标签键或输入新的标签键。 标签键最多支持64个字符，不能以 `aliyun` 或 `acs:` 开头，不能包含 `http://` 和 `https://` 。
标签值	标签的标签值，支持选择已有标签值或输入新的标签值。 标签值最多支持128个字符，不能以 `aliyun` 或 `acs:` 开头，不能包含 `http://` 和 `https://` 。

相关文档

- TagResources

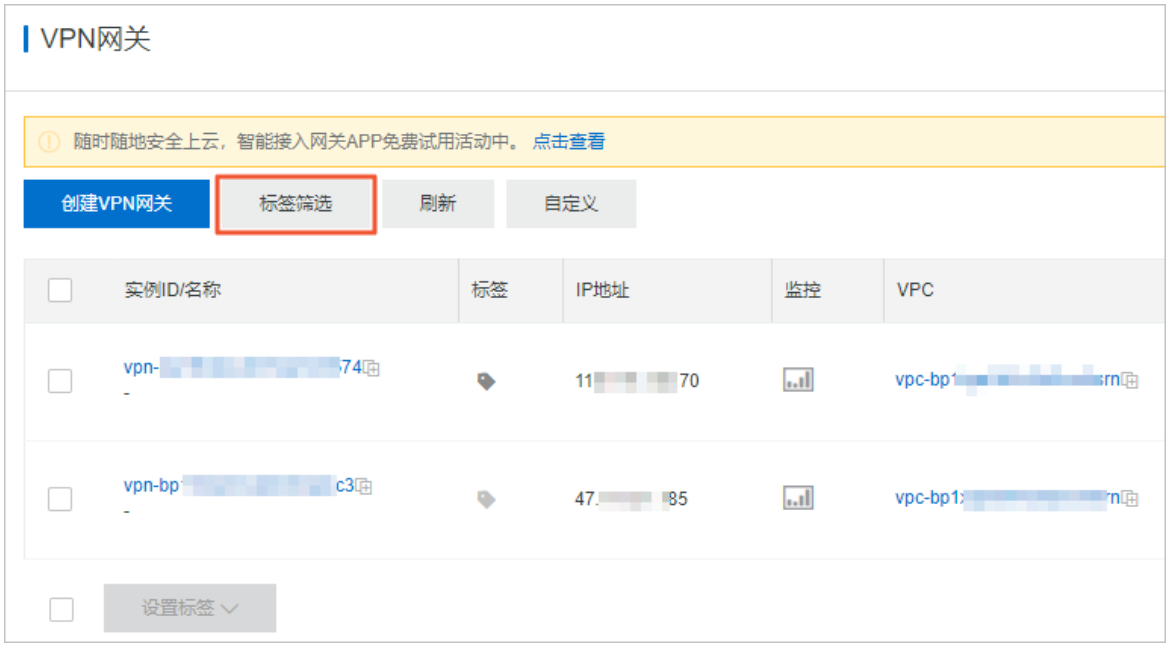
7.3. 使用标签搜索实例

为实例添加标签后，您可以使用标签搜索实例。

操作步骤

操作步骤

1.
2. 在顶部菜单栏处，选择VPN网关的地域。
3. 在**VPN网关**页面，单击**标签筛选**。



4. 在弹出的对话框中，选择或输入完整的标签键和值，然后单击**搜索**。

   此操作中，您可以选择或输入一对完整的标签键值对，也可以只选择或输入标签键，最多可以使用20条标签搜索实例。

相关文档

- ListTagResources

7.4. 删除标签

7.4.1. 为单个实例删除标签

如果实例不再需要某个标签，您可以删除该标签。本文介绍如何为单个实例删除标签。

背景信息

删除标签前，请了解以下注意事项：

- 单次最多可以删除20条标签。
- 如果您将一个标签添加到多个实例上，删除其中一个实例上的标签不会影响其它添加了该标签的实例。

操作步骤

1.
2. 在顶部菜单栏处，选择VPN网关的地域。
3. 在**VPN网关**页面，找到目标VPN网关实例，将鼠标悬停在**标签**列下的 图标上，然后单击气泡框中的**编辑**。
4. 在**编辑标签**对话框中，找到需要解绑的标签键值对，然后单击其右侧的 图标。

在该对话框中，您不仅可以删除标签，还可以为实例添加标签。

5. 单击**确定**。

相关文档

- UnTagResources

7.4.2. 为多个实例批量删除标签

如果实例不再需要某个标签，您可以删除该标签。本文介绍如何为多个实例批量删除标签。

背景信息

删除标签前，请了解以下注意事项：

- 单次最多可以删除20条标签。
- 如果您将一个标签添加到多个实例上，删除其中一个实例上的标签不会影响其它添加了该标签的实例。

操作步骤

1.
2. 在顶部菜单栏处，选择VPN网关的地域。
3. 在**VPN网关**页面，选中需要批量删除标签的实例，单击**设置标签 > 批量删除标签**。

4. 在**批量删除标签**对话框中，找到需要删除的标签键值对，然后单击其右侧的图标。
5. 单击**确定**。

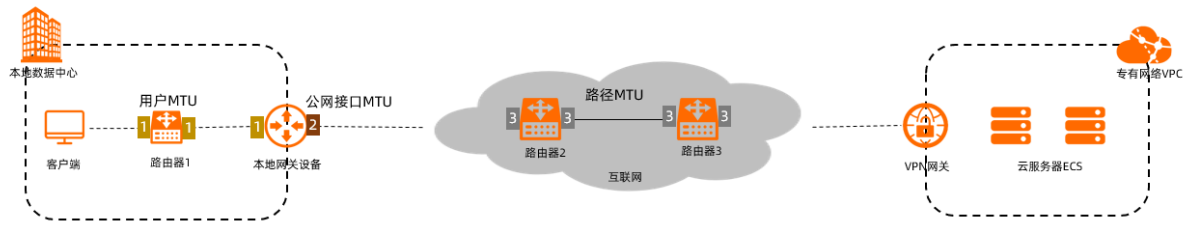
相关文档

- UnTagResources

8.MTU配置说明

VPN网关只支持传输已经分片的数据包，不支持对数据包分片及数据包分片重组。在您使用IPsec-VPN时，IPsec协议会对数据包进行加密，加密过程会扩大数据包长度，扩大后的数据包长度可能会超过网络中设置的最大数据传输单元MTU（Maximum Transmission Unit），影响数据包的正常传输。本文介绍如何设置MTU以确保数据包的正常传输。

MTU配置原则



本文以上图场景为例说明MTU配置原则。本地数据中心已与专有网络VPC（Virtual Private Cloud）建立了IPsec-VPN连接。在客户端访问VPC资源时，数据包将在本地网关设备中加密后被传输至互联网，经过互联网中的网络设备（图例中为路由器2和路由器3）被传输至VPN网关。

在数据包从客户端传输至VPN网关的过程中，数据包的大小将会受到以下三种MTU的限制：

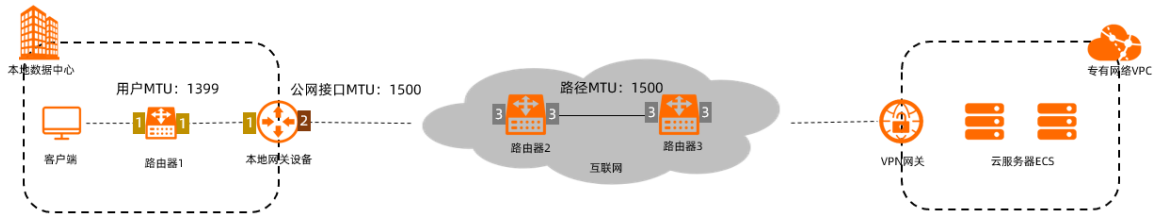
- 用户MTU
  用户MTU即客户端和本地网关设备之间所有网络设备接口MTU的最小值。该MTU会限制客户端发送的数据包的大小。
  本示例用户MTU取标记为1的接口中MTU的最小值。
- 公网接口MTU
  公网接口MTU即本地网关设备连接VPN网关的公网接口上的MTU。该MTU会限制被加密后的数据包的大小。
  本示例公网接口MTU取标记为2的接口的MTU。
- 路径MTU
  路径MTU即互联网中所有网络设备接口MTU的最小值。该MTU会限制被加密后的数据包的大小。
  您可以向相关互联网厂商咨询路径MTU。通常以太网的路径MTU默认为1500字节。
  本示例中路径MTU取标记为3的接口中MTU的最小值。

为确保数据包被正常传输，您需要在本地数据中心配置用户MTU和公网接口MTU，使上述三种MTU满足以下关系：

```
用户MTU的最大值=min{公网接口MTU,路径MTU}-101
```

> **说明** 101是IPsec协议为数据包加密后占用的最大字节数。

MTU配置示例



如上图所示，假设路径MTU为1500字节，您设置的本地网关设备公网接口的MTU也为1500字节，则：

```
用户MTU的最大值=min{1500,1500}-101=1500-101=1399字节
```

即客户端发送数据包时，数据包的大小建议不超过1399字节，否则可能会导致数据包无法正常传输。

MSS配置建议

在通过IPsec-VPN连接传输TCP流量的场景下，如果需要确保数据包不被分段传输，则最大分段大小MSS（Maximum Segment Size）和用户MTU需保证以下关系：

```
MSS=用户MTU-IP数据包头部占用字节数（20字节）-TCP数据包头部占用字节数（20字节）
```

例如，在公网接口MTU和路径MTU均为1500字节的情况下，用户MTU最大为1399字节，为确保数据包不被分段传输，MSS的最大值为1359字节。

9.管理配额

您可以通过VPN网关管理控制台查询当前资源配额使用情况。如果某个资源的剩余配额不满足业务需求，您可以直接申请增加配额。

操作步骤

1.
2. 在左侧导航栏，选择**运维与监控 > 配额管理**。
3. 在**配额管理**页面，选择**VPN网关**页签，查看当前账号下VPN网关的资源使用情况。
4. 如果需要提升配额，在**操作**列单击**申请**，提交提升配额申请。
   - **申请数量**：需要的资源配额数量，申请数量必须为数字且大于当前配额。VPN网关的资源默认使用限制，请参见使用限制。
   - **申请原因**：请详细描述申请配额的详细原因、业务场景和必要性。
   - **手机/固话**：申请配额的用户电话号码。
   - **电子邮箱**：申请配额的用户电子邮箱。
5. 单击**确定**。

   系统会自动审批配额申请是否合理，如果不合理，申请状态为**拒绝**，如果合理，申请状态为**通过**，配额立即自动提升为申请的数量。
   在**操作**列单击**申请历史**，可以查看配额申请历史。