阿里云
VPN网关

用户指南

文档版本：20190906

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

1 VPN网关介绍

VPN网关是一款基于Internet的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或Internet终端与阿里云专有网络（VPC）安全可靠的连接。VPN网关提供IPsec-VPN连接和SSL-VPN连接。

IPsec-VPN功能介绍

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。

您可以使用IPsec-VPN功能将本地数据中心与VPC或不同的VPC之间进行连接。IPsec-VPN支持IKEv1和IKEv2协议。只要支持这两种协议的设备都可以和阿里云VPN网关互连，比如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和 Ixia等。

IPsec-VPN可满足不同的应用场景。详细信息，请参见IPsec-VPN使用场景。

SSL-VPN功能介绍

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。详细说明，请参见SSL-VPN使用场景。

2 管理VPN网关

2.1 创建VPN网关

在使用IPsec-VPN和SSL-VPN功能前，您必须创建一个VPN网关。成功创建VPN网关后，系统会为VPN网关分配一个公网IP地址。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 在VPN网关页面，单击创建VPN网关。
4. 在购买页面，根据以下信息配置VPN网关，然后单击立即购买完成支付。

配置	说明
实例名称	（可选）VPN网关的实例名称。 长度为2-128个字符，以大小写字母或中文开头，可包含数字，点（.），下划线（_）和短横线（-）。
地域	选择VPN网关的地域。 如果使用VPN网关的IPsec-VPN功能建立VPC到本地数据中心和VPC到VPC的VPN连接，必须确保VPN网关的地域和VPC的地域相同。
VPC	选择VPN网关关联的VPC。
带宽规格	选择VPN网关的带宽规格。带宽规格是VPN网关所具备的公网带宽。
IPsec-VPN	选择是否开启IPsec-VPN功能。 您可以通过创建IPsec隧道，建立本地数据中心到VPC、VPC到VPC的安全连接。
SSL-VPN	选择是否开启SSL-VPN功能。 提供点到站点的VPN连接，不需要配置客户网关，终端直接接入。
SSL连接数	选择您需要同时连接的客户端最大规格。 **说明:** 本选项只有在选择开启了SSL-VPN功能后才可配置。

配置	说明
计费周期	选择购买时长。
自动续费	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：则自动续费周期为1年。

2.2 修改VPN网关

创建VPN网关后，您可以修改VPN网关的名称和描述信息。

前提条件

您已经创建了VPN网关。详细信息，请参见#unique_8。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 选择VPN网关的地域。
4. 在VPN网关页面，找到目标VPN网关，单击实例ID/名称列下的 图标修改实例名称。

   名称长度为2-100个字符，以英文字母或中文开头，可包含数字，下划线（_）或短横线（-）。
5. 单击描述列下的 图标修改描述信息。

   描述信息长度为2-256个字符，不能以http://和https://开头。

2.3 配置VPN网关路由

2.3.1 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，请参见添加策略路由。

> 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，请参见添加目的路由。

2.3.2 添加策略路由

创建IPsec连接后，您可以手动添加策略路由。策略路由基于源IP和目的IP进行更精确的路由转发。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 选择VPN网关的地域。
4. 在VPN网关页面，找到目标VPN网关，单击实例ID/名称列下的实例ID。
5. 在策略路由表页签，单击添加路由条目。
6. 在添加路由条目页面，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。

配置	说明
权重	选择权重值： · 100 · 0 权重值越大，路由优先级越高。

2.3.3 添加目的路由

创建IPsec连接后，您可以手动添加目的路由。目的路由仅基于目的IP进行路由转发。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 选择VPN网关的地域。
4. 在VPN网关页面，找到目标VPN网关，单击实例ID/名称列下的实例ID。
5. 在目的路由表页签，单击添加路由条目。
6. 在添加路由条目页面，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。
权重	选择权重值： · 100：优先级高。 · 0：优先级低。 说明: 相同目的网段的目的路由，不支持同时设置权重值为100。

2.4 续费

为避免VPN网关欠费对您的业务造成影响，请您及时为VPN网关续费。

前提条件

您已经创建了VPN网关。详细信息，请参见创建VPN网关。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 选择VPN网关的地域。
4. 在VPN网关页面，找到目标VPN网关，单击操作列下的续费。
5. 在续费页面，选择续费时长并完成支付。

2.5 临时升配

您可以临时提升VPN网关的配置，并在到达还原时间后自动恢复升级前的配置。

前提条件

您已经创建了VPN网关。详细信息，请参见创建VPN网关。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 选择VPN网关的地域。
4. 在VPN网关页面，找到目标VPN网关，单击操作列下的临时升配。
5. 在配置变更区域，根据以下信息变更配置，然后单击去支付完成支付。

配置	说明
带宽规格	选择新的带宽规格。
还原时间	设置临时升配的还原时间。 说明: 临时升配到达还原时间后，配置将降为升配前的配置。还原过程不中断业务，但带宽从高变低可能会出现闪断，建议后端应用具备重连机制。临时升配支持最短升配间隔为2小时，按小时单价计费，支付完成后带宽即刻升配成功，升配过程不中断业务。

配置	说明
IPsec-VPN	选择开启或关闭IPsec-VPN。
SSL-VPN	选择开启或关闭SSL-VPN。

2.6 续费降配

您可以为VPN网关续费，且续费时可以降低VPN网关的带宽。

前提条件

您已经创建了VPN网关。详细信息，请参见创建VPN网关。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 选择VPN网关的地域。
4. 在VPN网关页面，找到目标VPN网关，单击操作列下的续费降配。
5. 在配置变更区域，根据以下信息变更配置，然后单击去支付完成支付。

配置	说明
带宽规格	选择新的带宽规格。
IPsec-VPN	选择开启或关闭IPsec-VPN。
SSL-VPN	选择开启或关闭SSL-VPN。
续费时长	选择续费的时长。

2.7 开启IPsec-VPN和SSL-VPN

您可以在创建VPN网关时开启IPsec-VPN和SSL-VPN功能，也可以在创建后根据需要再开启IPsec-VPN和SSL-VPN功能。

> 说明:
> 2018年1月20日前创建的VPN网关要开启SSL-VPN功能，需要提交工单。新创建的实例，可以在控制台上直接开启。

开启IPsec-VPN

完成以下操作，开启IPsec-VPN功能。

1. 登录专有网络管理控制台。

2. 在左侧导航栏，单击VPN > VPN网关。
3. 选择VPN网关的地域。
4. 在VPN网关页面，找到目标VPN网关，在功能配置列下，单击IPsec连接后的开启。
5. 在购买页面，完成支付。

开启SSL-VPN

完成以下操作，开启SSL-VPN功能。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 选择VPN网关的地域。
4. 在VPN网关页面，找到目标VPN网关，在功能配置列下，单击SSL后的开启。
5. 在购买页面，完成支付。

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. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > 用户网关。
3. 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. 在创建用户网关页面，根据以下信息，配置用户网关。

配置	说明
名称	用户网关的名称。 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，连字符（-）和下划线（_）。
IP地址	本地数据中心网关设备的静态公网IP地址。
描述	用户网关的描述。 描述在2-256个字符之间，不能以http:// 和 https:// 开始。

6. （可选）单击+添加添加另一个用户网关。
7. 单击确定。

3.2 修改用户网关

创建用户网关后，您可以修改用户网关的名称和描述信息。

前提条件

您已经创建了一个用户网关。详细信息，请参见#unique_23。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > 用户网关。
3. 选择用户网关的地域。
4. 在用户网关页面，找到目标用户网关，单击实例ID/名称列下的 图标修改用户网关的名称。

   名称长度为2-100个字符，以英文字母或中文开头，可包含数字，下划线（_）或短横线（-）。
5. 单击描述列下的 图标修改用户网关的描述信息。

   描述信息长度为2-256个字符，不能以http://和https://开头。

3.3 删除用户网关

您可以删除一个不需要的用户网关。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > 用户网关。
3. 选择用户网关的地域。
4. 在用户网关页面，找到目标用户网关，单击操作列下的删除。
5. 在弹出的对话框中，单击确认。

4 配置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。

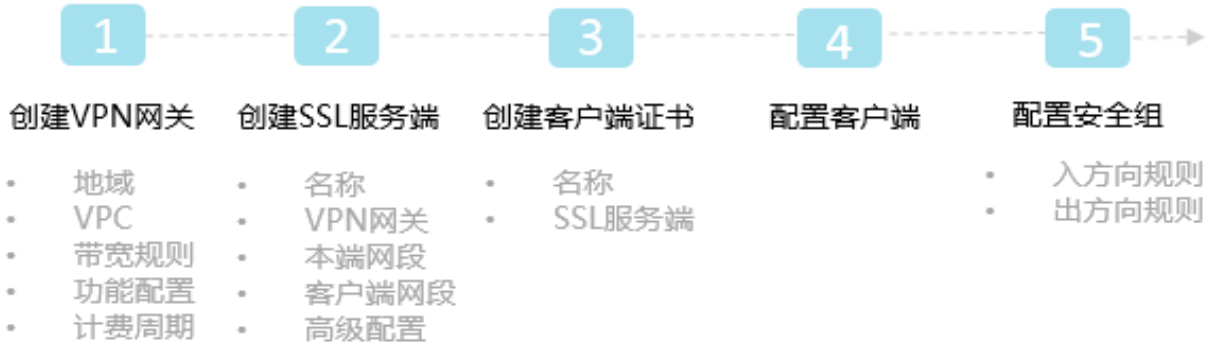
前提条件

在部署VPN网关前，确保您的环境满足以下条件：

- 本地设备和VPC的私网IP地址段不能相同，否则无法通信。
- 客户端必须能访问Internet。

配置流程说明

通过SSL-VPN功能远程接入VPC的流程图如下：



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

您必须已经创建了VPN网关并开启了SSL-VPN。详细信息，请参见创建VPN网关。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > SSL服务端。
3. 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服务端页面，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，以英文字母或中文开始，可包含数字，连字符（-）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。
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VPC的网段、交换机的网段、通过专线和VPC互连的IDC的网段、云服务如RDS/OSS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在16到29位。
客户端网段	客户端网段是给客户端虚拟网卡分配访问地址的的地址段，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。 说明: 确保客户端网段和本端网段不冲突。

配置	说明
高级配置	
协议	SSL连接使用的协议，可选UDP或TCP。建议使用UDP协议。
端口	SSL连接使用的端口，默认为1194。
加密算法	SSL连接使用的加密算法，支持AES-128-CBC、AES-192-CBC、AES-256-CBC。
是否压缩	是否对传输数据进行压缩处理。

4.2.2 修改SSL服务端

创建SSL服务端后，您可以修改SSL服务端的名称、本端网段、客户端网段和高级配置。

前提条件

您已经创建了SSL服务端。详细信息，请参见创建SSL服务端。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > SSL服务端。
3. 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，单击操作列下的编辑。
5. 在编辑SSL服务端页面，修改SSL服务端的名称、本端网段、客户端网段和高级配置，然后单击确定。

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. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > SSL服务端。
3. 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，单击操作列下的删除。
5. 在弹出的对话框中，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。详细信息，请参见#unique_34。

背景信息

每个用户可保有的SSL客户端证书的数量为50个，如需提升配额，请提交工单。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > SSL客户端 。
3. 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客户端证书页面，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，连字符（-）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。创建SSL客户端证书后，您可以下载SSL客户端证书。

前提条件

您已经创建了SSL客户端证书。详细信息，请参见#unique_36。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > SSL客户端 。
3. 选择SSL客户端的地域。
4. 在SSL客户端页面，找到目标客户端证书，单击操作列下的下载。

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. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > SSL客户端 。
3. 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，单击操作列下的删除。
5. 在弹出的对话框中，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. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 选择VPN网关的地域。
4. 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，单击SSL并发连接数列下的升配。
   - 如果您想降低SSL并发连接数，单击SSL并发连接数列下的降配。
5. 在配置变更区域，选择新的SSL连接数并完成支付。

5 配置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。

前提条件

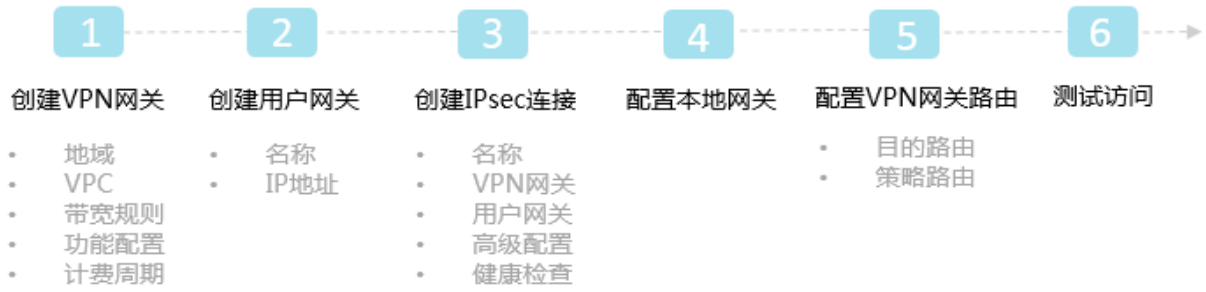
使用IPsec-VPN功能建立VPC到本地数据中心的VPN连接，确保满足以下条件：

- 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都可以和阿里云VPN网关互连，比如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和Ixia等。
- 本地数据中心的网关必须配置静态公网IP。
- 本地数据中心的网段和专有网络的网段不能重叠。

配置流程说明

建立VPC到本地数据中心的VPN连接的流程图如下：



1. 创建VPN网关

   VPN网关开启IPsec-VPN功能，一个VPN网关最多可以建立10个IPsec连接。
2. 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。
3. 创建IPsec连接

   IPsec连接是指VPN网关和用户网关建立连接后的VPN通道。只有IPsec连接建立后，用户侧企业数据中心才能使用VPN网关进行加密通信。

4. 配置本地网关

   您需要在本地VPN网关设备中加载阿里云VPN网关的配置。详细信息，请参见本地CPE配置。

5. 配置VPN网关路由

   您需要在VPN网关中配置路由，并发布到VPC路由表中。详细信息，请参见#unique_42。

6. 测试访问

   登录到阿里云VPC内一台无公网IP的ECS实例，通过ping本地IDC内一台服务器的私网IP地址，验证通信是否正常。

详细配置信息，请参见#unique_43。

5.2 管理IPsec连接

5.2.1 创建IPsec连接

创建IPsec 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。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > IPsec连接。
3. 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。

配置	说明
名称	IPsec连接的名称。 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，连字符（-）和下划线（_）。
VPN网关	选择待连接的VPN网关。
用户网关	选择待连接的用户网关。
本端网段	输入需要和本地IDC互连的VPC侧的网段，用于第二阶段协商。
+添加 本端网段	添加多个需要和本地IDC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。

配置	说明
对端网段	输入需要和VPC互连的本地IDC侧的网段，用于第二阶段协商。
+添加 对端网段	添加多个需要和VPC互连的本地IDC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。
高级配置：IKE配置	
预共享密钥	用于IPsec VPN网关与用户网关之间的身份认证。默认情况下会随机生成，也可以手动指定密钥。
版本	选择IKE协议的版本。目前支持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IKE V1版本的协商模式。 · 主模式（main）：协商过程安全性高。 · 野蛮模式（aggressive）：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的加密算法。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。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。
SA生存周期（秒）	设置第一阶段协商出的SA的生存周期。默认值为86400秒。
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。

配置	说明
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。
DH分组	选择第二阶段协商的Diffie-Hellman密钥交换算法： · 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，相应的客户端也要配置为PFS开启。 · 对于不支持PFS的客户端请选择disabled。
SA生存周期（秒）	设置第二阶段协商出的SA的生存周期。默认值为86400秒。
健康检查	
目标IP	VPC侧通过IPSec连接可以访问的线下IDC的IP地址。
源IP	线下IDC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连接的名称、高级配置和健康检查。

前提条件

您已经创建了IPsec连接。详细信息，请参见创建IPsec连接。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > IPsec连接。
3. 选择IPsec连接的地域。
4. 在IPsec连接页面，找到目标IPsec连接，单击操作列下的编辑。
5. 在编辑IPsec连接页面，修改IPsec连接的名称、高级配置和健康检查，然后单击确定。

5.2.3 下载IPsec连接配置

配置IPsec连接并协商成功后，您可以下载IPsec连接配置，将该配置加载到本地网关设备中。

前提条件

您已经创建了IPsec连接。详细信息，请参见#unique_49。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > IPsec连接。

3. 选择IPsec连接的地域。
4. 在IPsec连接页面，找到目标IPsec连接，单击操作列下的下载对端配置。

> 说明:
> 下载配置中的RemotSubnet和LocalSubnet与创建IPsec连接时的本端网段和对端网段正好是相反的。因为从阿里云VPN网关的角度看，对端是本地IDC的网段，本端是阿里云侧的VPC网段；而从本地IDC的网关设备角度看，LocalSubnet就是指本地IDC的网段，RemotSubnet则是指阿里云VPC的网段。

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. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > IPsec连接。
3. 选择IPsec连接的地域。
4. 在IPsec连接页面，找到目标IPsec连接，单击操作列下的查看日志。
5. 在IPsec连接日志页面，设置要查看的日志周期，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. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > IPsec连接。
3. 选择IPsec连接的地域。
4. 在IPsec连接页面，找到目标IPsec连接，单击操作列下的删除。
5. 在弹出的对话框中，单击确定。

5.3 本地网关配置

5.3.1 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，比如华为、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#unique_54。
- 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。

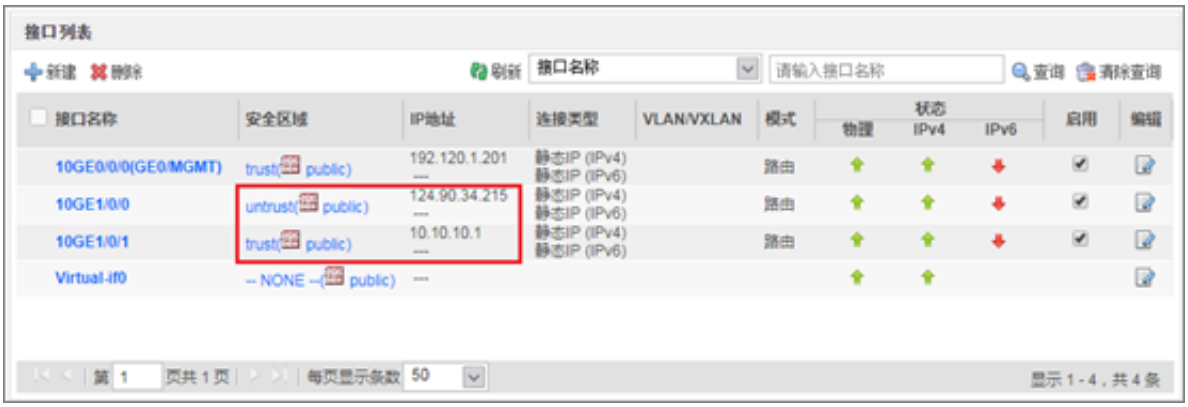
协议	配置	示例值
IKE	认证算法	SHA-1
	加密算法	AES-128
	DH 分组	group 2
	IKE 版本	IKE v1
	生命周期	86400

协议	配置	示例值
	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

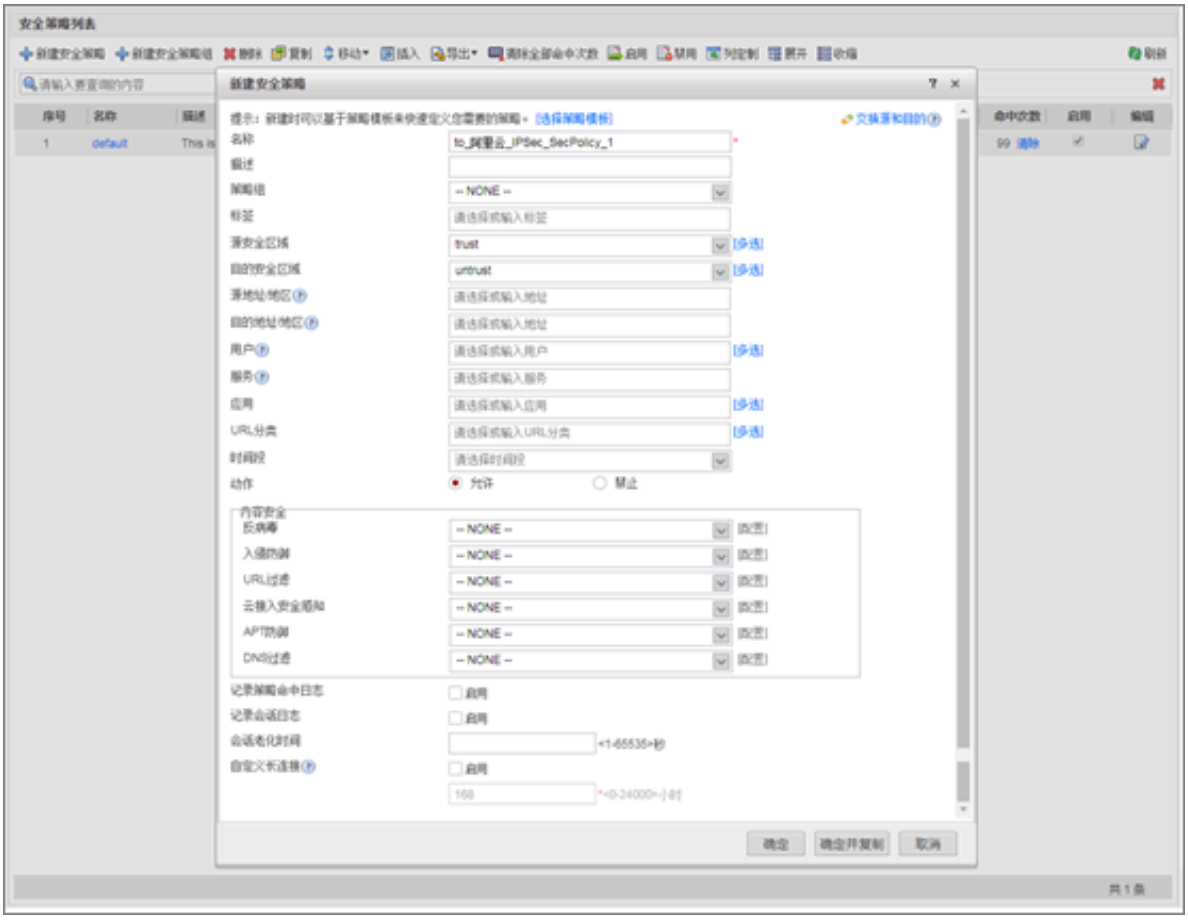
操作步骤

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，单击网络 > 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。**

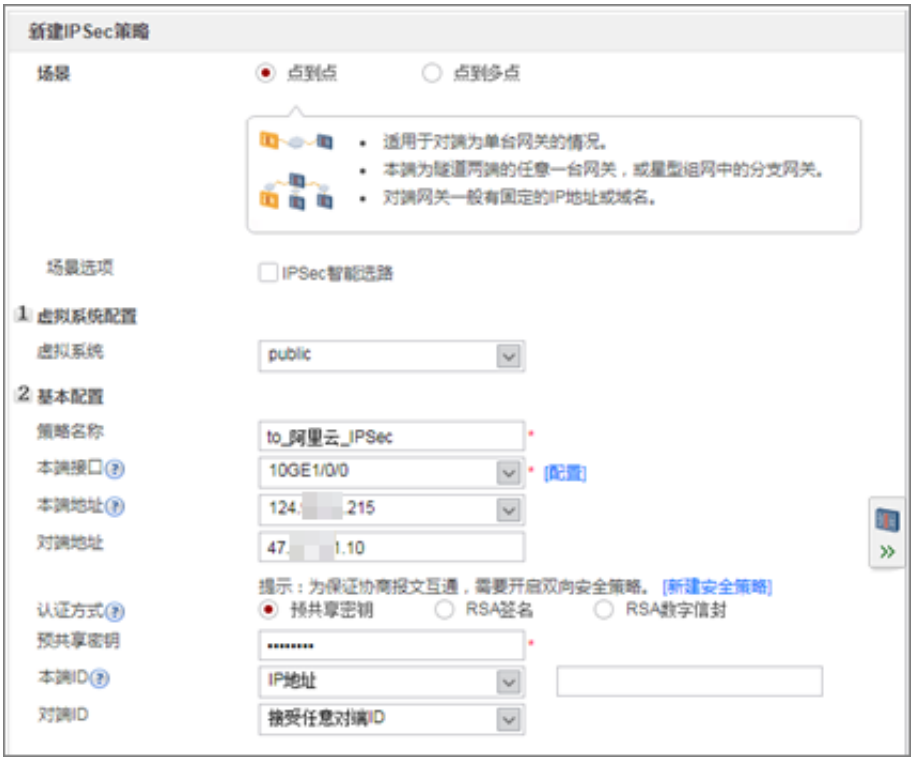


2. 单击策略 > 安全策略 > 新建，创建安全策略。



3. 单击网络 > 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. 单击网络 > 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，下一条为防火墙的公网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。

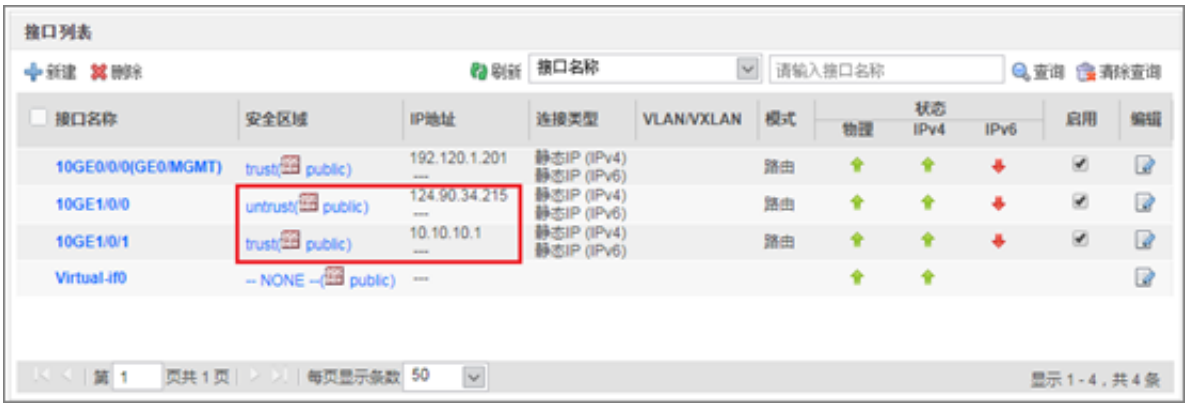
协议	配置	示例值
IKE	认证算法	SHA-1
	加密算法	AES-128

协议	配置	示例值
	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

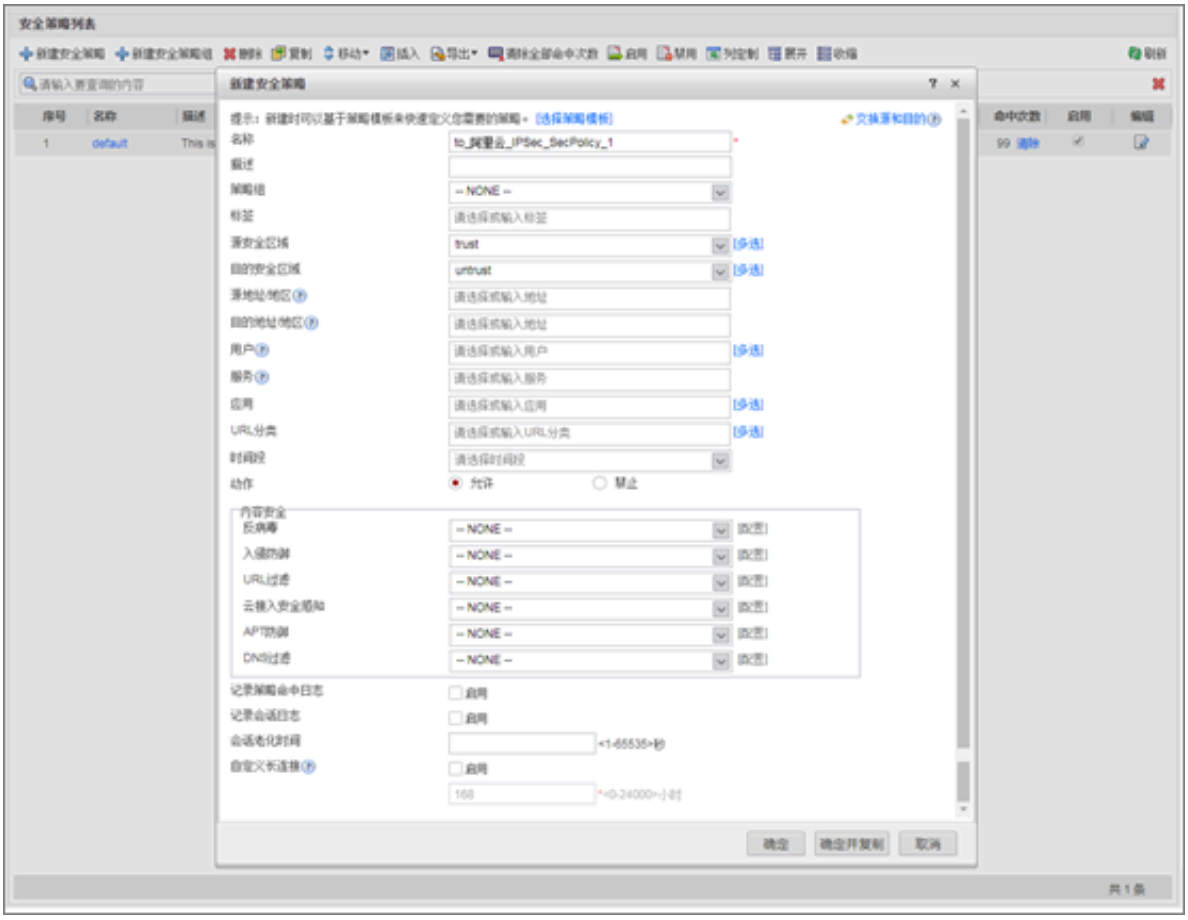
操作步骤

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，单击网络 > 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。

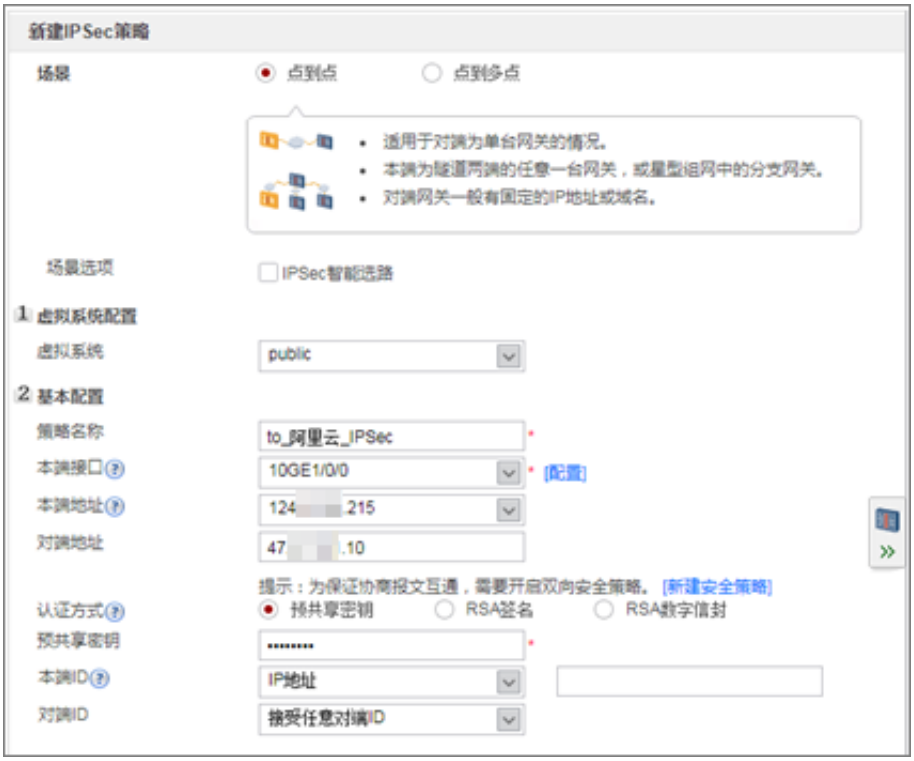


2. 单击策略 > 安全策略 > 新建，创建安全策略。



3. 单击网络 > 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. 单击网络 > 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，下一条为防火墙的公网IP；添加指向VPC的路由时，一下跳为VPN网关的公网IP。

5.3.2 华三防火墙配置

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。本文以华三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#unique_56。

- 创建IPsec连接后，获取的IPsec配置信息，详情参见#unique_47。

  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	h3c
IPsec	认证算法	sha1
	加密算法	aes
	DH分组	group2
	IKE版本	ikev1
	生命周期	86400

  - 网络配置信息

配置		示例值
VPC配置	私网CIDR	192.168.10.0/24
	网关公网IP	101.xxx.xxx.127
IDC网络配置	私网CIDR	192.168.66.0/24
	网关公网IP	122.xxx.xxx.248
	上行公网网口	Reth 1
	下行私网网口	G 2/0/10

操作步骤

1. 登录防火墙Web页面，单击网络 > VPN > IPsec > 策略 。

2. 根据阿里云VPN连接的IPsec协议信息配置IDC的H3C防火墙IPsec策略。并在保护的数据流列表中单击添加加入保护的兴趣流，兴趣流源IP和目的IP分别为IDC和阿里云VPC的网段。

3. 单击IKE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。

4. 单击网络 > VPN > IPsec > 策略。

5. 选择刚刚新建的IPsec策略，单击高级配置配置IPsec协议。

   根据阿里云VPN连接的IPsec协议信息配置IPsec协议。

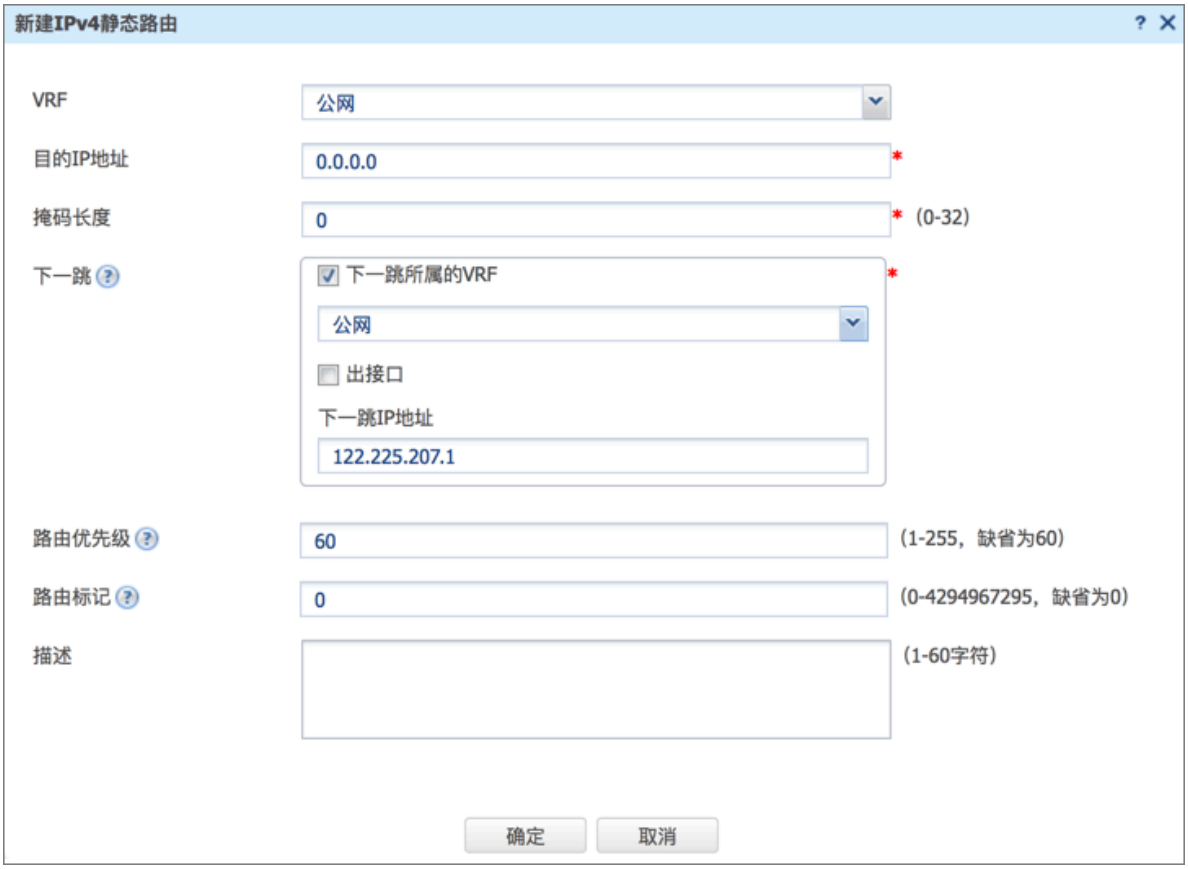
6. 单击策略 > 安全策略 > 新建，分别创建上行安全策略和下行安全策略。

从阿里云VPC到本地IDC的安全策略配置如下图所示。

从本地IDC到阿里云VPC的安全策略配置如下图所示。

7. 单击网络 > 路由 > 静态路由。

8. 添加缺省路由，使出方向流量走上行接口，本例中下行接口为直连路由，无需配置。



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

配置		示例值
	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
	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

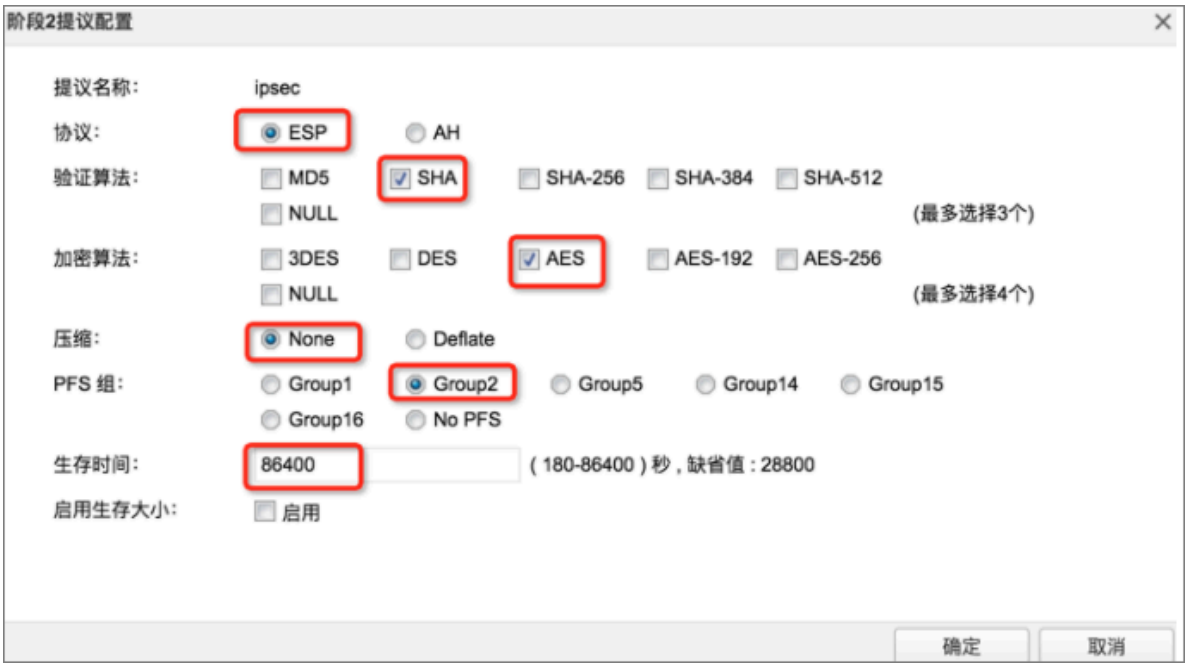
操作步骤

1. 登录防火墙Web页面，单击网络 > 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. 单击P2提议 > 新建 。

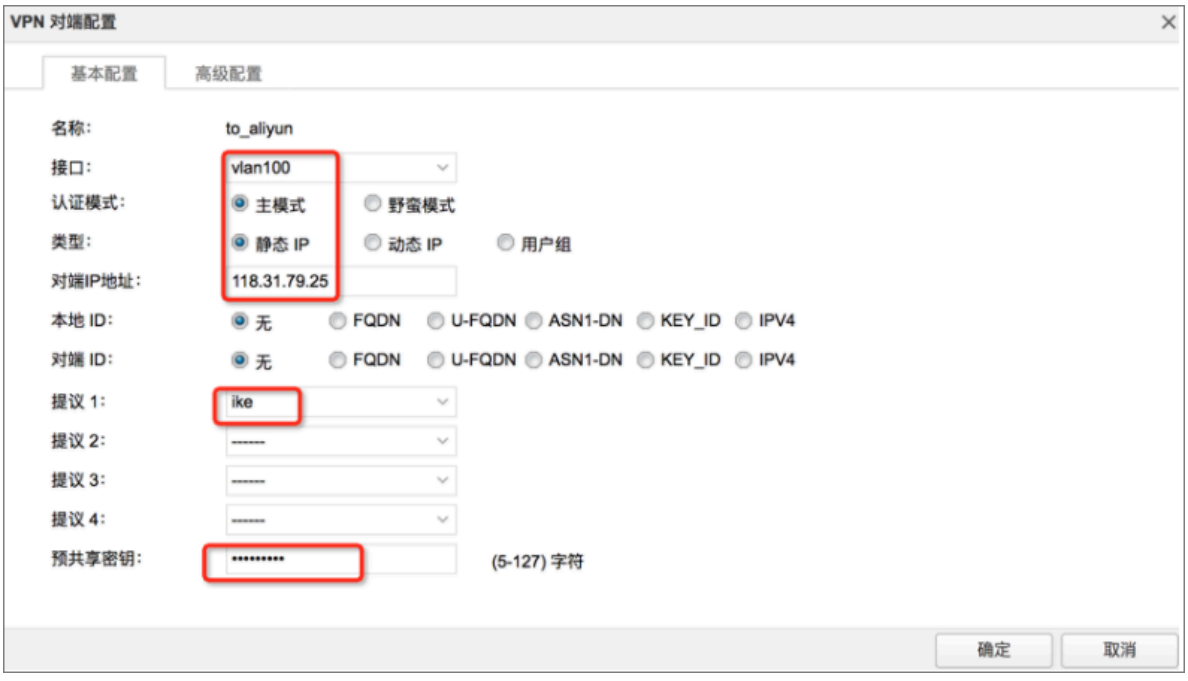
   根据阿里云VPN连接的IPsec协议信息配置IDC的IPsec协议。



3. 单击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. 单击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. 单击网络 > 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. 单击网络 > 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。


隧道接口
基本配置
属性
高级
RIP
基本配置
接口名称:
tunnel5
描述:
vpn_tunnel
(0-63) 字符
绑定安全域:
二层安全域
三层安全域
TAP
无绑定
安全域:
aliyun
HA同步:
启用
IP配置
类型:
静态IP
自动获取
PPPoE
IP地址:
网络掩码:
配置为Local IP
启用DNS代理
代理
透明代理
启用DNS透传
高级选项
DHCP...
管理方式
Telnet
SSH
Ping
HTTP
HTTPS
SNMP
路由
逆向路由:
启用
关闭
自动
隧道绑定配置
隧道类型:
IPSec VPN
SSL VPN
VPN 名称:
to_aliyun_vpn
网关:
VPN 名称
类型
网关
添加
to_aliyun_vpn
IPSec VPN
删除
带宽
上行带宽:
1,000,000,000
(512,000 ~ 1000,000,000,000)bps
下行带宽:
1,000,000,000
(512,000 ~ 1000,000,000,000)bps
确定
取消

7. 单击策略 > 安全策略 > 新建。

8. 单击网络 > 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strongSwan为例介绍如何在本地站点中加载VPN配置。

本文以strongSwan为例介绍如何在本地站点中加载VPN配置。本操作中作为示例的配置信息如下：

- 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59.110.165.70

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#unique_56。
- 创建IPsec连接后，获取的IPsec配置信息，详情参见#unique_47。

安装strongSwan

1. 运行以下命令安装strongSwan。

```
# yum install strongswan
```

2. 运行以下命查看安装的软件版本。

```
# strongswan version
```

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
     type=tunnel
 conn tomyidc
     keyexchange=ikev1
     left=59.110.165.70
     leftsubnet=172.16.2.0/24
     leftid=59.110.165.70 (IDC网关设备的公网IP)
     right=119.23.227.125
     rightsubnet=192.168.10.0/24
     rightid=119.23.227.125 (VPN网关的公网IP)
     auto=route
     ike=aes-sha1-modp1024
     ikelifetime=86400s
     esp=aes-sha1-modp1024
```

```
    lifetime=86400s
    type=tunnel
```

3. 配置*ipsec.secrets*文件。

   a. 运行以下命令打开配置文件。

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

   b. 添加如下配置。

   ```
   59.110.165.70 119.23.227.125 : PSK yourpassword
   ```

4. 打开系统转发配置。

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

   更多场景配置样例，参见场景配置样例。

5. 执行以下命令启动strongSwan服务。

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

6. 设置IDC客户端到strongSwan网关及网关下行到客户端路由。

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	main
	PSK	123456

配置		示例值
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. 登录防火墙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。
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）。

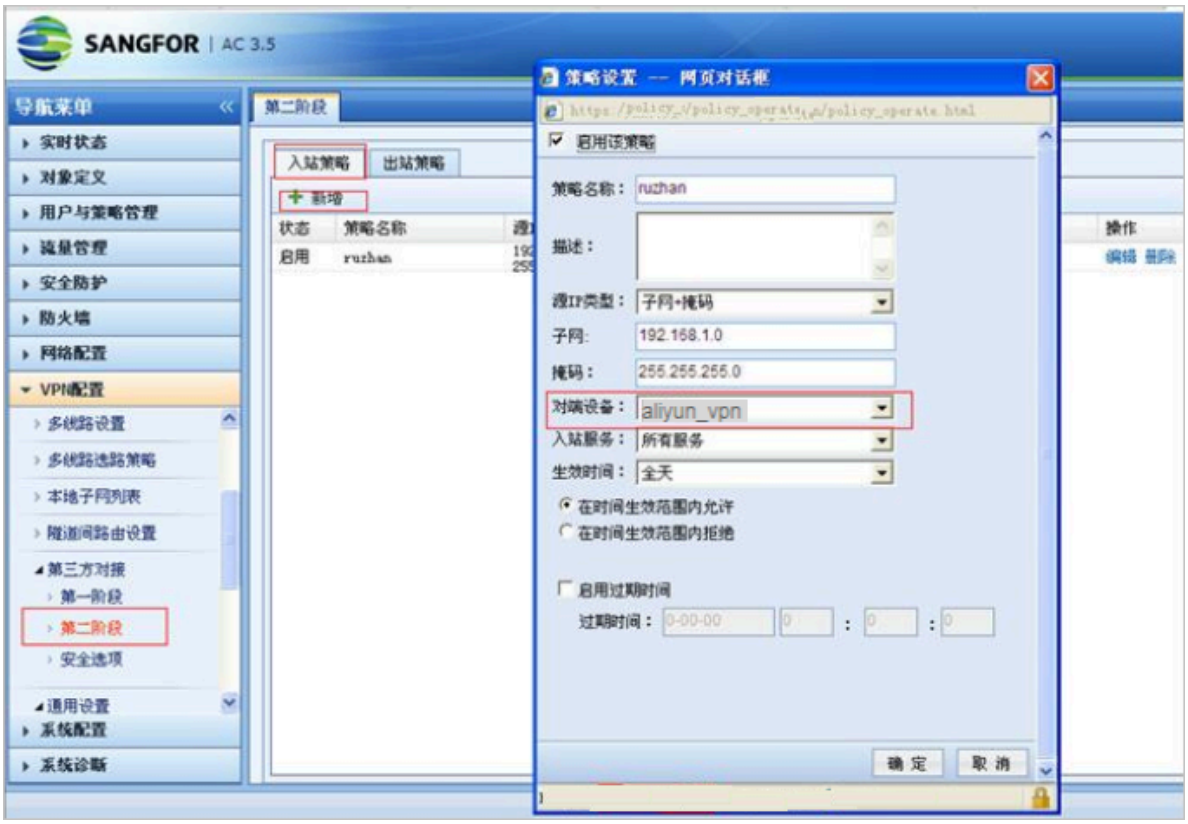
配置	说明
身份类型	选择验证身份的类型，本示例选择IPv4地址（IPv4 ADDR）。
我方身份ID	输入本端公网IP地址，本示例为122.xxx.xxx.248。
对方身份ID	输入VPC端公网IP地址，本示例47.xxx.xxx.56。
启用NAT穿透	本示例选择启用NAT穿透。
认证算法	选择认证算法，本示例为MD5。
加密算法	选择加密算法，本示例为3DES。

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。

配置	说明
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。

配置	说明
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。

配置	说明
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#unique_49。
- 已经下载了IPsec连接的配置。详细说明，请参见#unique_63。

  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

配置		示例值
	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--24 192.168.18.0/24
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-address net-cfgr_192-168-18-0--24
set security policies from-zone trust to-zone vpn policy trust-vpn-
cfgr match destination-address net-cfgr_192-168-1-0--24
set security policies from-zone trust to-zone vpn policy trust-vpn-
cfgr match application 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-address net-cfgr_192-168-1-0--24
set security policies from-zone vpn to-zone trust policy vpn-trust-
cfgr match destination-address net-cfgr_192-168-18-0--24
set security policies from-zone vpn to-zone trust policy vpn-trust-
cfgr match application 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。

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

- 已经在阿里云VPC内创建了IPsec连接。详细说明，请参见#unique_49。
- 已经下载了IPsec连接的配置。详细说明，请参见#unique_63。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

操作步骤

完成以下操作，在思科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.xxx.xxx.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 0.0.0.255 192.168.20.0 0.0.0.
255
```

6. 配置IPsec策略。

```
crypto map ipsecpro64 10 ipsec-isakmp
set peer 47.xxx.xxx.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.xxx.xxx.161
ip route 192.168.20.0 255.255.255.0 47.xxx.xxx.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。详细说明，请参见#unique_49。

- 已经下载了IPsec连接的配置。详细说明，请参见#unique_63。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，在思科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.xxx.xxx.161
```

```
pre-shared-key 0 123456
```

5. 配置身份认证。

```
crypto ikev2 profile ipsecpro64_v2
match identity remote address 47.xxx.xxx.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 0.0.0.255 192.168.20.0 0.0.0.
255
```

8. 配置IPsec策略。

```
crypto map ipsecpro64_v2 10 ipsec-isakmp
set peer 47.xxx.xxx.161
set transform-set ipsecpro64_v2
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。

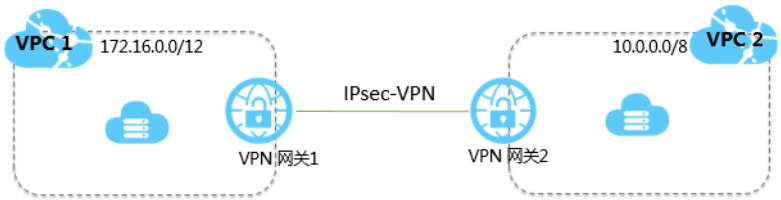
```
ip route 192.168.10.0 255.255.255.0 47.xxx.xxx.161
ip route 192.168.20.0 255.255.255.0 47.xxx.xxx.161
```

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。

5.4 建立VPC到VPC的连接

本文介绍如何使用VPN网关建立VPC到VPC的VPN连接，从而实现两个VPC内的资源互访。



本操作以同一个账号下的两个VPC为例。如果是跨账号VPC互通，操作步骤和同账号VPC互通一样。只是在创建用户网关前，需要获取对方账号的VPN网关的公网IP地址，然后使用获取的对方账号的公网IP地址创建用户网关。

VPC名称	VPC网段	VPC ID	ECS名称
VPC1	172.16.0.0/12	vpc-xxxxz0	ECS1
VPC2	10.0.0.0/8	vpc-xxxxut	ECS2

说明:

VPN 网关是基于Internet建立加密隧道进行通信，通信质量依赖Internet。如果对通信质量要求高，可以使用高速通道。详细信息，请参见#unique_66和#unique_67。

开始之前

确保两个VPC的私网IP地址不重叠。

步骤一 创建VPN网关

完成以下操作，创建VPN网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
3. 在VPN网关页面，单击创建VPN网关。
4. 在购买页面，根据以下信息配置VPN网关，然后单击立即购买完成支付。
   - 实例名称：输入VPN网关的实例名称。
   - 地域：选择VPN网关的地域。

说明:

确保VPC的地域和VPN网关的地域相同。

- VPC： 选择要连接的VPC。
- 带宽规格：选择一个带宽规格。带宽规格是VPN网关所具备的公网带宽。
- IPsec-VPN： 选择开启IPsec-VPN功能。
- SSL-VPN： 选择是否开启SSL-VPN功能。SSL-VPN功能允许您从任何位置的单台计算机连接到专有网络。
- SSL连接数： 选择您需要同时连接的客户端最大规格。

说明:
本选项只有在选择开启了SSL-VPN功能后才可配置。

- 计费周期：选择购买时长。

5. 重复上述步骤，为另外一个VPC创建一个VPN网关。

刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态就表明VPN网关完成了初始化，可以正常使用了。VPN 网关创建后，系统会自动分配两个公网IP。

说明:
VPN网关的创建一般需要1-5分钟。

本例中分配的公网IP地址为121.xxx.xx.143和118.xxx.xx.149，如下表所示。

VPC	VPN网关	IP地址
名称：VPC1 ID：vpc-xxxxz0 网段：172.16.0.0/12	vpn-xxxxxqwj	118.xxx.xx.149
名称：VPC2 ID：vpc-xxxxut 网段：10.0.0.0/8	vpn-xxxxxl5z	121.xxx.xx.143

步骤二 创建用户网关

完成以下操作，创建用户网关。

1. 在左侧导航栏，单击VPN > 用户网关。
2. 选择用户网关的地域。
3. 在用户网关页面，单击创建用户网关。
4. 在创建用户网关页面，根据以下信息配置用户网关，然后单击确定。
   - 名称：输入用户网关的名称。
   - IP地址：输入VPC要连接的本地数据中心网关设备的公网IP。
   - 描述：输入用户网关的描述信息。
5. 重复上述步骤，使用另外一个IP地址再创建一个用户网关。

   本操作后，VPC与VPN网关、用户网关之间的对应关系如下表所示。

VPC	VPN网关	IP地址	用户网关
名称：VPC1 ID：vpc-xxxxz0 网段：172.16.0.0/12	vpn-xxxxxqwj	121.xxx.xx.143	user_VPC1
名称：VPC2 ID：vpc-xxxxut 网段：10.0.0.0/8	vpn-xxxxxl5z	118.xxx.xx.149	user_VPC

步骤三 创建IPsec连接

创建好VPN网关和用户网关后，您需要分别创建两个IPsec连接建立VPN加密通道。

1. 在左侧导航栏，单击VPN > IPsec连接。
2. 选择创建IPsec连接的地域。
3. 在IPsec连接页面，单击创建IPsec连接。

4. 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。
   - 名称：输入IPsec连接的名称。
   - VPN网关： 选择已创建的VPN网关。本例先选择VPC1的VPN网关vpn-xxxxxqwj。
   - 用户网关：选择要连接的用户网关。本例选择VPC2的用户网关user_VPC2。
   - 本端网段：输入已选VPN网关所属VPC的网段，本例输入VPC1的网段172.16.0.0/12。
   - 对端网段：输入对端VPC的网段，本例输入VPC2的网段10.0.0.0/8。
   - 是否立即生效：选择是否立即协商。
     - 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：输入共享密钥，本例输入1234567。两个IPsec连接的共享密钥必须相同。
   - 健康检查：开启健康检查并输入目的IP、源IP、重试间隔和重试次数。

   其他选项使用默认配置。
5. 重复上述步骤，为另外一个VPC创建IPsec连接。

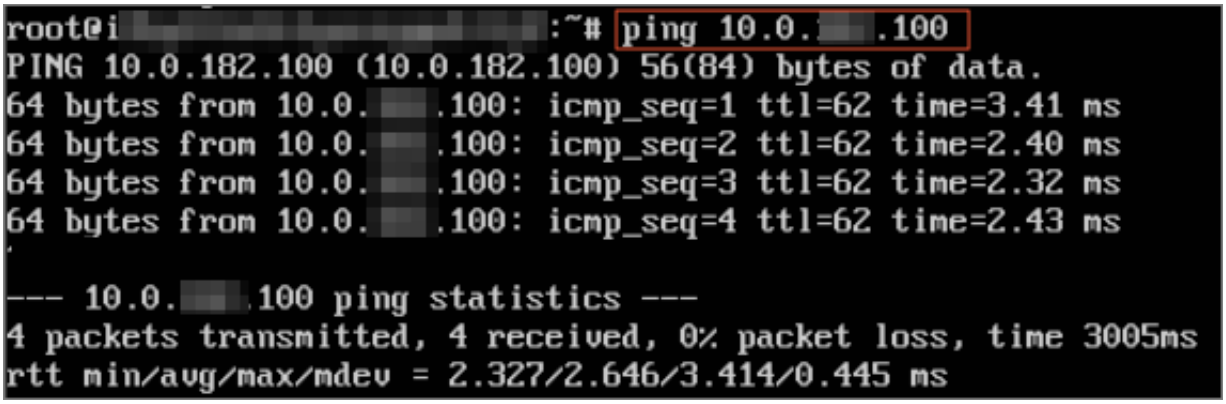
步骤四 配置VPN网关路由

完成以下操作，配置IPsec-VPN网关路由。

1. 在左侧导航栏，单击VPN > VPN网关。
2. 选择VPN网关的地域。
3. 在VPN网关页面，找到目标VPN网关，单击实例ID/名称列下的实例ID。
4. 在目的路由表页签，单击添加路由条目。
5. 在添加路由条目页面，根据以下信息配置目的路由，然后单击确定。
   - 目标网段：输入VPC2的私网网段。
   - 下一跳：选择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。本例选择是。
   - 权重：选择权重值。本例选择100。
6. 重复上述步骤，为另一个VPN网关配置路由。

步骤五 测试私网通信

在专有网络VPC1内的ECS1实例上ping ECS2 实例的私网IP，测试两个VPC的私网通信。


root@i:~# ping 10.0.[redacted].100
PING 10.0.182.100 (10.0.182.100) 56(84) bytes of data.
64 bytes from 10.0.[redacted].100: icmp_seq=1 ttl=62 time=3.41 ms
64 bytes from 10.0.[redacted].100: icmp_seq=2 ttl=62 time=2.40 ms
64 bytes from 10.0.[redacted].100: icmp_seq=3 ttl=62 time=2.32 ms
64 bytes from 10.0.[redacted].100: icmp_seq=4 ttl=62 time=2.43 ms
--- 10.0.[redacted].100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.327/2.646/3.414/0.445 ms

6 MTU注意事项

最大传输单元 (MTU) 是网络层协议（如 TCP）支持的最大数据包的大小（以字节为单位），标头和数据均包括在内。

通过IPsec隧道发送的网络数据包经过加密，然后封装在外部数据包中，以便进行路由。因为封装的内部数据包本身必须适合外部数据包的MTU，所以其MTU必须更小。

网关MTU与系统MTU

您必须配置本地VPN网关，将其使用的MTU限制在1400字节之内，建议MTU设置为1400字节。

如果是TCP流量，可基于最大分段大小（MSS），在TCP收发双方通信时，协商每一个报文段所能承载的最大数据长度。

7 管理配额

您可以通过专有网络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. 登录专有网络管理控制台。
2. 在左侧导航栏，单击配额管理。
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，可以单击操作列的申请，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#unique_70。
   - 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。

   在申请历史列单击申请历史，可以查看配额申请历史。