阿里云 VPN网关

用户指南

文档版本: 20190906

为了无法计算的价值 | [] 阿里云

<u>法律声明</u>

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。

- 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。
- 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。
A	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。
Ê	用于补充说明、最佳实践、窍门等,不 是用户必须了解的内容。	道 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 listinstanceid 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。	<pre>swich {stand slave}</pre>

目录

法律声明	I
通用约定	I
1 VPN网关介绍	1
- ····································	2
- ロノエマエコマクノン 21 创建VDN図半	······ <u>-</u> 2
2.1 的足VIII的人	2
2.3 配置VPN网关路由	
2.3.1 网关路由概述	
2.3.2 添加策略路由	
2.3.3 添加目的路由	5
2.4 续费	6
2.5 临时升配	6
2.6 续费降配	7
2.7 开启IPsec-VPN和SSL-VPN	7
3 管理用户网关	
3.1 创建用户网关	9
3.2 修改用户网关	9
3.3 删除用户网关	10
4 配置SSL-VPN	11
4.1 �� ℃ 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	11
4.1 配直概觅 4.2 管理SSL服务端	11 12
4.1 配直概觉 4.2 管理SSL服务端 4.2.1 创建SSL服务端	11 12 12
 4.1 配直概題 4.2 管理SSL服务端 4.2.1 创建SSL服务端 4.2.2 修改SSL服务端 	11 12 12 13
 4.1 配直概览 4.2 管理SSL服务端 4.2.1 创建SSL服务端 4.2.2 修改SSL服务端 4.2.3 删除SSL服务端 	11 12 12 12 13 13
 4.1 配直概題 4.2 管理SSL服务端 4.2.1 创建SSL服务端	11 12 12 13 13 13 14
 4.1 配直概览	11 12 12 12 13 13 14 14
 4.1 配直概见. 4.2 管理SSL服务端. 4.2.1 创建SSL服务端. 4.2.2 修改SSL服务端. 4.2.3 删除SSL服务端. 4.3 管理SSL客户端. 4.3.1 创建SSL客户端证书. 4.3.2 下载SSL客户端证书. 	11 12 12 12 13 13 14 14 14
 4.1 配直概觉	11 12 12 13 13 13 14 14 14 14 14 15
 4.1 配直概觉	11 12 12 12 13 13 13 14 14 15 15
 4.1 配直概见. 4.2 管理SSL服务端. 4.2.1 创建SSL服务端. 4.2.2 修改SSL服务端. 4.2.3 删除SSL服务端. 4.3 管理SSL客户端. 4.3 管理SSL客户端证书. 4.3.2 下载SSL客户端证书. 4.3.3 删除SSL客户端证书. 4.4 修改SSL并发连接数. 5 配置IPsec-VPN.	11 12 12 13 13 13 14 14 14 14 15 15 16
 4.1 配直機寬. 4.2 管理SSL服务端. 4.2.1 创建SSL服务端. 4.2.2 修改SSL服务端. 4.2.3 删除SSL服务端. 4.3 管理SSL客户端. 4.3.1 创建SSL客户端证书. 4.3.2 下载SSL客户端证书. 4.3.3 删除SSL客户端证书. 4.3.3 删除SSL客户端证书. 5 配置IPsec-VPN. 5.1 配置概览. 	11 12 12 13 13 13 14 14 14 14 15 15 16
 4.1 配直概題	11 12 12 12 12 13 13 13 14 14 14 15 15 15 16 16 17
 4.1 配置概见. 4.2 管理SSL服务端. 4.2.1 创建SSL服务端. 4.2.2 修改SSL服务端. 4.2.3 删除SSL服务端. 4.3 管理SSL客户端证书. 4.3.1 创建SSL客户端证书. 4.3.2 下载SSL客户端证书. 4.3.3 删除SSL客户端证书. 4.4 修改SSL并发连接数. 5 配置IPsec-VPN. 5.1 配置概览. 5.2 管理IPsec连接. 5.2.1 创建IPsec连接.	11 12 12 13 13 13 14 14 14 14 15 15 16 16 17 17
 4.1 配直概觉. 4.2 管理SSL服务端	11 12 12 12 12 13 13 13 14 14 14 14 15 15 16 16 17 17 17
 4.1 配置概題. 4.2 管理SSL服务端. 4.2.1 创建SSL服务端. 4.2.2 修改SSL服务端. 4.2.3 删除SSL服务端. 4.3 管理SSL客户端证书. 4.3.1 创建SSL客户端证书. 4.3.2 下载SSL客户端证书. 4.3.3 删除SSL客户端证书. 4.4 修改SSL并发连接数. 5 配置IPsec-VPN. 5.1 配置概览. 5.2 管理IPsec连接. 5.2.2 修改IPsec连接. 5.2.3 下载IPsec连接配置. 5.2.4 本美Dece 达按照置.	11 12 12 13 13 13 14 14 14 14 15 15 15 16 17 17 19 19
 4.1 配直概觉. 4.2 管理SSL服务端	11 12 12 13 13 13 14 14 14 14 14 15 15 16 16 17 17 19 19 20 20
 4.1 配直橄宽. 4.2 管理SSL服务端. 4.2.1 创建SSL服务端. 4.2.2 修改SSL服务端. 4.2.3 删除SSL服务端. 4.3 管理SSL客户端证书. 4.3.1 创建SSL客户端证书. 4.3.3 删除SSL客户端证书. 4.3.3 删除SSL客户端证书. 4.4 修改SSL并发连接数. 5 配置IPsec-VPN. 5.1 配置概宽. 5.2 管理IPsec连接. 5.2.1 创建IPsec连接. 5.2.2 修改IPsec连接. 5.2.3 下载IPsec连接配置. 5.2.4 查看IPsec连接 5.2.5 删除IPsec连接. 	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
 4.1 配置機见. 4.2 管理SSL服务端	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$

5.3.2 华三防火墙配置	29
5.3.3 山石网科防火墙配置	
5.3.4 strongSwan配置	
5.3.5 深信服防火墙配置	46
5.3.6 Juniper防火墙配置	
5.3.7 思科防火墙配置	53
5.4 建立VPC到VPC的连接	
6 MTU注意事项	
7 管理配额	64

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。

- 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。
	前明: 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。

- 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。 ・ 不・不労在新添加的路由到VPC路由表。
	送明: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。

- 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。

- 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。

- 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		2		3	4		- 5>
创建	VPN网关	创建	SSL服务端	岩 创建	書客户端证书	3 配置客所	1 二派	配置安全组
•	地域 VPC 带宽规则 功能配置 计费周期	•	名称 VPN网关 本端网段 客户端网 高级配置	。 段	名称 SSL服务崩	L.	•	入方向规则 出方向规则

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。

- 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。					
	道 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。

- 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。

- 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。

- 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		2		3	4		5	6→
创建	≹VPN网关	创建	即户网关	创建	劃Psec连接	配置本地网	关配	置VPN网关路由	测试访问
•	地域 VPC 带宽规则 功能配置 计费周期	•	名称 IP地址	•	名称 VPN网关 用户网关 高级配置 健康检查		•	目的路由 策略路由	

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。

- 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。
	道 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。 道 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。

- 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。

- 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:

 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。

●新建 💢 勝餘		(2) 号(新)	項口名称	V][请输2	、接口名称		Q, 3	间 📬 清	除置
接口名称	安全区域	IP地址	连接类型	VLAN/VXLAN	模式	物理	秋恋 IPv4	IPv6	启用	编
10GE0/0/0(GE0/MGMT)	trust(2 public)	192.120.1.201	静态IP (IPv4) 静态IP (IPv6)		路由	+	+	+		
10GE1/0/0	untrust(III public)	124.90.34.215	静态IP (IPv4) 静态IP (IPv6)		路由	+	+	+		G
10GE1/0/1	trust(public)	10.10.10.1	静态IP (IPv4) 静态IP (IPv6)		踏由			+		G
Virtual-if0	NONE (public)					+	+			G

输入更宽阔的内容		新建安全等略				7	×			
19 20	1615	· · · · · · · · · · · · · · · · · · ·	后来快速定义尔莱斯的编辑。 (人名英格兰姓氏)			23.560000	Ξ	8422	启用	į,
default	This is	名称	to_阿里亚_IPSec_SecPolicy_1		•		L	99 3859	8	ŝ
		腦迷								
		WARKE	- NONE	1						
		相望	课选探察输入标题							
		源安全区域	trust	V	19-31					
		目的完全区域	untrust	V	19-31					
		源地址地区(例	请选择规制入地址							
		用的地址地区(例	课选探察输入地址							
		用户()	调选探索输入用户		19-381					
		服用()	调选择约输入服务							
		应用	请选择统输入应用		19-33					
		URL分类	谱选择统输入URL分离		19-33					
		时间段	通达描印/印印							
		动作	 九许 「禁止」 							
		内容安全								
		反消毒	- NONE -	>	「原語」					
		入985304	- NONE -	Y	(四)田(
		URL过渡	- NONE -	Y	(四)田(
		云接入安全感知	- NONE -	~	(四)(四)					
		APTINO	- NONE -	~	(四)王(
		DNRIdit	- NONE -	Y	(四)田(
		记录屏藏由中日志	_ AR							
		记录会话日本	_ <u>A</u> 9							
		会适考化时间	<1-65535>B				Ц,			
		自定义长连接(例	白月				Ľ.			
			168 *=0-24000=>	141			Ц,			
							Υ.			

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。

新建IPSec策略	
场景	
	 ◎ 透用于对读为单台网关的情况。 ● 本读为隧道两读的任意一台网关,或星型组网中的分支网关。 ◎ 面面 ● 对读网关一般有固定的IP地址或域名。
场最选项	□ IPSec 智能选路
1 出现系统配置	
虚拟系统	public 🗸
2 基本配置	
領略名称	to_阿里云_IPSec •
本調擾口(家)	10GE1/0/0 🔽 * (65)
本調地址(例	124. 215
对端地址	47. 1.10 »>
认证方式(3)	 揭示:为保证协商报文互通,需要开启双向安全策略。(新建安全策略) 预共享密钥 RSA签名 RSA数字信封
预共享密钥	· ·
本端ID②	IP地址 V
对如HD	接受任意对编D

- 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。

3 待加密的数据流 🕐						
地址类型	 IPv4 		IPv6			
💠 新建 🐹 勝勝 💽 抗入		 4) Rist 	请输入要查询的	内容	🔍 童道	📴 清除宣词
	目的地址/地址组	协议	源端口	目的端口	动作	编辑
10.10.10.0/255.255 1	92.168.10.0/255.2	any	any	any	加密	1
10.10.10.0/255.255 1	92.168.11.0/255.2	any	any	any	加密	1 🛛
						共2条
□ 反向路由注入 🕑						

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。

高级				
KE参数 🕑				
IKE版本	✓ v1	v2 使用v	1发起和接受协商	i.
协商模式(?)	() 自动	 主模式 	○ 野窩模式	
加密算法(?)	SM4	AES-256	AES-192	AES-128
	3DES	DES		
认证算法()	SM3	SHA2-512	2 SHA2-384	SHA2-256
	SHA1	MD5		
DH组(?)	21	20	19	16
	15	14	5	₹2
	1			
SA超时时间?	86400		<60-604	800>秒

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。

日装模式()		○ 特新規式	2.税管理 〇	
安全协议(1)	 ESP 	O AH	O AH-ESP	
ESP加密算法(P	SM4	AES-256	AES-192	
	✓ AES-128	3DES	DES	
ESP认证算法(P	SM3	SHA2-512	SHA2-384	SHA2-256
	SHA1	MD5		
PFS()	 NONE 	0 21	0 20	19
	0 16	0 15	0 14	0 5
SASET (?)		0.		
基于时间	86400		<30-604	800>₺⁄
基于流量(?)	20000000		<0,256	200000000>KB

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。

 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。

接口列表										
💠 新建 🐹 粉除		(4) 制新	接口名称	~] 请输	∖ 撫口名称		9,3	间 🏫 🏦	除查询
接口名称	安全区域	IP地址	连接类型	VLAN/VXLAN	根式	物理	状态 IPv4	IPv6	启用	编辑
10GE0/0/0(GE0/MGMT)	trust(I public)	192.120.1.201	静态IP (IPv4) 静态IP (IPv6)		踏由	+	+	+		
10GE1/0/0	untrust(III public)	124.90.34.215	静态IP (IPv4) 静态IP (IPv6)		路由	+	+	+		
10GE1/0/1	trust(III public)	10.10.10.1	静态IP (IPv4) 静态IP (IPv6)		踏由	+	+	+		
Virtual-if0	NONE(I public)					+	+			
	> > 每页显示条数	50 🗸						5	际1-4,	共4条

输入更宽阔的内容		新建安全等略				7	×			
19 20	1615	· · · · · · · · · · · · · · · · · · ·	后来快速定义尔莱斯的编辑。 (人名英格兰姓氏)			23.560000	Ξ	8422	启用	į,
default	This is	名称	to_阿里亚_IPSec_SecPolicy_1		•		L	99 3859	8	ŝ
		腦迷								
		WARKE	- NONE	1						
		相望	课选探察输入标题							
		源安全区域	trust	V	19-31					
		目的完全区域	untrust	V	19-31					
		源地址地区(例	请选择规制入地址							
		用的地址地区(例	课选探察输入地址							
		用户()	调选探索输入用户		19-381					
		服用()	调选择约输入服务							
		应用	请选择统输入应用		19-33					
		URL分类	谱选择统输入URL分离		19-33					
		时间段	通达描印/印印							
		动作	 九许 「禁止」 							
		内容安全								
		反消毒	- NONE -	>	「原語」					
		入985304	- NONE -	×	(四)田(
		URL过渡	- NONE -	Y	(四)田(
		云接入安全感知	- NONE -	~	(四)(四)					
		APTINO	- NONE -	~	(四)王(
		DNRIdit	- NONE -	Y	(四)田)					
		记录屏藏由中日志	_ AR							
		记录会话日本	_ <u>A</u> 9							
		会适考化时间	<1-65535>B				Ц,			
		自定义长连接(例	白月				Ľ.			
			168 *=0-24000=>	141			Ц,			
							Υ.			

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。

新建IPSec策略		
场展	 فالف) خالف) 	
	 ▲ 通用于对請为单台网关的情况。 ▲ 本請为隧道两端的任意一台网关,或星型组网中的分支网关。 ● 对猜网关一般有固定的IP地址或域名。 	
场最远项	 IPSec智範远路 	
1 出现系统配置		
虚拟系统	public 💌	
2 基本配置		
領略名称	to_阿里云_IPSec •	
本調授口(?)	10GE1/0/0 🔽 • (ACIR)	
本調地址()	124 215 🗸	
对请地址	47 .10	»
	揭示:为保证协商报文互通,需要开启双向安全策略。[新建安全策略]	
以让方式(?)	 ● 換共享密朝 ○ RSA發名 ○ RSA数字情封 	
70444699		
本週ID(?)	IP地址 V	
对beiD	接受任意R/J編D 🛛	

- 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。

3 待加密的数据流 🕐						
地址类型	 IPv4 		IPv6			
💠 新建 🐹 勝勝 💽 抗入		 4) Rist 	请输入要查询的	内容	🔍 童道	📴 清除宣词
	目的地址/地址组	协议	源端口	目的端口	动作	编辑
10.10.10.0/255.255 1	92.168.10.0/255.2	any	any	any	加密	1
10.10.10.0/255.255 1	92.168.11.0/255.2	any	any	any	加密	1 🛛
						共2条
□ 反向路由注入 🕑						

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。

高级				
KE參数 🕐				
IKE版本	□ v1	✓ v2 使用v2	发起和接受协调	Γ.
加密算法()	AES-256	AES-192	AES-128	3DE
	DES			
完整性算法()	SHA2-512	2 SHA2-384	SHA2-256	SHA1
	MD5	AES		
PRF算法()	SHA2-512	2 SHA2-384	SHA2-256	SHA1
	MD5	AES-128		
DH组(?)	21	20	19	16
	15	14	5	√ 2
	1			
SA题时时间?	86400		<60-604	800>10

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。

安全协议 ● ESP AH AH-ESP ESP加密算法 ● SM4 AES-256 AES-192 ● AES-128 3DES DES ESP认证算法 ● SM3 SHA2-512 SHA2-384 SHA2-256 ● SHA1 MD5	H AH-ESP 8-256 AES-192 ES DES A2-512 SHA2-384 SHA2-256
ESP加密算法() SM4 AES-256 AES-192 《AES-128 3DES DES ESP认证算法() SM3 SHA2-512 SHA2-384 SHA2-256 《SHA1 MD5	S-256 AES-192 ES DES A2-512 SHA2-384 SHA2-256
✓ AES-128 3DES DES ESP认证期法④ SM3 SHA2-512 SHA2-384 SHA2-256 ✓ SHA1 MD5	ES DES A2-512 SHA2-384 SHA2-256
ESP以证期法 ③ SM3 SHA2-512 SHA2-384 SHA2-256	A2-512 SHA2-384 SHA2-256
SHA1 MD5	NE .
	10
	I 🔿 20 🔿 19
	5 🔿 14 🔿 5
器子时间 86400 <30-604800>秒	
	<30-604800>₺

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。

建IPsec策略								
基本配置								
接口	Reth1				~	*		
IP地址类型	IPv4		O IP	v6				
优先级	1					* (1-65535)		
模式	◉ 对等/分支节	点	◎ 中	心节点				
对端IP地址/主机名	101.132.122	127				*(1-253字符)	
协商模式	 主模式 		◎ 野	蛮模式				
认证方式	预共享密钥				~			
预共享密钥	•••					*(1-128字符)	
再次输入预共享密钥	•••							
IKE提议③	优先级(认证	E算法	;加密算法;	DH)	~			
对端ID	IPv4 地址	~	101.132.122.1	27		*		
本端ID	IPv4 地址	~	122.225.207.2	48				
描述	· · · · · · · · · · · · · · · · · · ·					(1-80字符)		
保护的数据流								
🕣 添加 💼 删除 🚺 插入								
📄 源IP地址	目的IP地址		协议	源端口	目的	端口	动作	
192.168.66.0/255.255	192.168.10.0/255.2	55	any	any	any		保护	

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。

编辑IKE提议				? X
优先级	19		* (1-65535)	
认证方式	预共享密钥			
认证算法	SHA1	~		
加密算法	AES-CBC-128	~		
DH	DH group 2	*		
IKE SA 生存周期	86400		秒(60-604800)	
	确定 取消			

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。

					共1条
- IP	高级配置				
ARP	IPsec参数				
IPv6	封装模式	 隧道模式 	◎ 传输模式		
VPN	安全协议	ESP	O AH	AH-ESP	
GRE	ESP认证算法	SHA1		~	
IPsec	ESP加密算法	AES-CBC-128		~	
- 策略	PFS	Group_2		~	
- IKE提议	IPsec SA生存时间 🕐				
- 监控	基于时间	86400		秒(180-604800)	
高级设置	基于流量			千字节(2560-4294967295)	
SSL VPN	IPsec SA 空闲超时时间 🕐			秒(60-86400)	
🚬 路由	DPD检测 🕐	── 开启			
路由夷	本端IP地址	122.225.207.248			
- 結太敗山	QoS预分类 🕐	□ 开启			
		确定	E 取消		

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

名称	aliyun_to_h3c	
源安全域	Untrust	~
目的安全域	Trust	~
类型	IPv4 IPv6	
描述信息		
动作	◎ 允许 ◎ 拒绝	
源IP地址	192.168.10.0/24	~
目的IP地址	192.168.66.0/24	~
服务	请选择服务	~
应用	请选择应用	~
应用组	请选择应用组	~
用户	请选择或输入用户	~
时间段	请选择时间段	~
VRF	公网	~
内容安全		
IPS策略	-NONE	~
数据过滤策略	NONE	~
文件过滤策略	NONE	~
防病毒策略	NONE	~
URL过滤策略	-NONE	~
记录日志	◎ 开启 ● 关闭	
开启策略匹配统计	◎ 开启 ● 关闭	
会话表化时间	□ 启用	

从本地IDC到阿里云VPC的安全策略配置如下图所示。

名称	h3c_to_aliyun	*(1-127字符)
源安全域	Trust	▼ [多选]
目的安全域	Untrust	▼ [多选]
类型		
描述信息		(1-127字符)
动作	● 允许 ◎ 拒绝	
源IP地址	192.168.66.0/24	▼ [多选]
目的IP地址	192.168.10.0/24	✔ [多选]
服务	请选择服务	▼ [多选]
应用	请选择应用	▼ [多选]
应用组	请选择应用组	▼ [多选]
用户	请选择或输入用户	▼ [多选]
时间段	请选择时间段	~
VRF	公网	~
内容安全 ————————————————————————————————————		
IPS策略	NONE	~
数据过滤策略	-NONE-	•
文件过滤策略	-NONE-	•
防病毒策略	-NONE-	•
URL过滤策略	-NONE-	•
记录日志	◎ 开启 ● 关闭	
开启策略匹配统计	◎ 开启 ● 关闭	
会话表化时间	■ 启用	-
	佣在	

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。

新建IPv4静态路由		? >
VRF	公网	*
目的IP地址	0.0.0.0	*
掩码长度	0	* (0-32)
下一跳 🕐	 ▼ 下一跳所属的VRF 公网 □ 出接口 下一跳IP地址 122.225.207.1 	*
路由优先级 🕐	60	(1-255, 缺省为60)
路由标记 🕐	0	(0-4294967295,缺省为0)
描述		(1-60字符)
	确定取消	

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
/PC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。

阶段1提议配置		×
提议名称:	ike	
认证:	Pre-share ORSA-Signature ODSA-Signature	
验证算法:	MD5 SHA SHA-256 SHA-384 SHA-512	
加密算法:	③ 3DES ● DES ● AES ● AES-192 ● AES-256	
DH 组:	 Group1 Group2 Group5 Group14 Group15 	
生存时间:	86400 (300-86400)秒,缺省值:86400	
	确定	取消

2. 单击P2提议 > 新建。

阶段2提议配置		×
提议名称: 协议: 验证算法: 加密算法: 压缩:	ipsec ● ESP ● AH ● MD5 ● SHA ● SHA-256 ● SHA-384 ● SHA-512 ● NULL (最多选择3个) ● 3DES ● DES ● AES ● AES-192 ● AES-256 ● NULL (最多选择4个) ● None ● Deflate	
PFS 组:	Group1 Group2 Group5 Group14 Group15 Group16 No PFS	
生存时间: 启用生存大小:	86400 (180-86400)秒,缺省值:28800	
	确定耳	又消

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。

VPN 对端配置		×
基本配置	高级配置	
名称: 接口:	to_aliyun Vlan100 ∽	
认证模式: 类型:	 ● 主模式 ● 野蛮模式 ● 静态 IP ● 动态 IP ● 用户组 	
对端PP地址: 本地 ID: 对端 ID:	● 无 ● FQDN ● U-FQDN ● ASN1-DN ● KEY_ID ● IPV4 ● 无 ● FQDN ● U-FQDN ● ASN1-DN ● KEY_ID ● IPV4	
提议 1: 提议 2:	ike ~	
提议 3: 提议 4:	~	
预共享密钥:	(5-127) 字符	
		确定取消

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。

IKE VPN 配置						×
基础设置	场设置					
对端						
对端选项:	to_aliyun		编辑			
信息展示:	名称	模式	类型	本地 ID	对端 ID	
	to_aliyun	主模式	静态 IP			
隧道						
名称:	to_aliyun_vp	n				
模式:	tunnel	transport				
P2提议:	ipsec v					
代理 ID:	◎ 自动 ◎ 手工					
代理ID列表		<u> </u>				
本地IP/ 掩码:		1				
远程 IP/ 掩码:		1				
服务:	any	~				
本地IP/ 掩码		远程 IP/ 掩码	服务		添加	
10.90.5.0/24		192.168.10.0/24	Any		删除	
						确定 取迷
						HUAL 4K/H

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。

安全域配置					×
基本配置 威胁防持	Þ				
基本配置 安全域名称:	aliyun	(1-31) 字符			
描述:		(0-63) 字符			
类型:	◎ 二层安全域	◎ 三层安全域	© TAP		
虚拟路由器:	trust-vr	~			
绑定接口:		~			
	从域中移除接口将删	l除接口的IP配置。			
高级					
应用识别:	🔲 启用				
WAN安全域:	□ 启用				
NBT缓存:	□ 启用				
终端接入识别:	🔲 启用				
				确定	取消

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			
***	夏於 支払 D	D	
叁 平 郎 直	腐吐 向级 RI	P	
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	\sim	
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	月代理	
□ 启用DNS遗信	ŧ		
高级选项 DI	HCP		
管理方式			
Telnet	SSH V Ping	HTTP HTTPS SNMP	1
路由			
逆向路由:	同 启用 〇 关月	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)bp	5
下行带宽:	1,000,000,000	(512,000 ~ 1000,000,000,000)bp	5
			确定 取消

7. 单击策略 > 安全策略 > 新建。

策略配置						0	×
基	本配置	防护状态	选项				
源信息							
	安全域:	trust				\sim	
	地址:	any				\sim	
	用户:					\sim	
目的	安全域:	aliyun	٦			~	
	地址:	any				~	
	服务:	any				~	
	应用-	_				Ŷ	
	操作:	◉ 允许	◎ 拒绝	◎ 安全连接			
		□ 启用Web重	龍定向 ①				
					确定	取消	
						-94112	-
策略配置						0	×
基	本配置	防护状态	选项				
源信息							
	安全域:	aliyun				\sim	
	地址:	any				~	
	用户:		ļ			\sim	
目的	安全域:	trust				~	
	地址:	any				~	
	80.4 7 .						
	服劳: 应用·	any				×	
	ELPH) -					×	
	操作:	◉ 允许	◎ 拒绝	◎ 安全连接			
		启用Web1	重定向				
							I

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。

目的路由配置			×
所属虚拟路由器: 目的地:	trust-vr 192.168.10.0		
子网掩码:	24		
下一跳:	 网关 接口 	 当前系统虚拟路由器 其他系统虚拟路由器 	
接口:	tunnel5 V		
网关:			
时间表:	v		
优先权:	1	(1-255), 缺省值: 1	
路由权值:	1	(1-255), 缺省值: 1	
描述:		(0-63)字符	
		确定 取消	

・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。

	C 3.5				当前用户:
>家田気FOR AG >家时状态 > >家时状态 > >用戶与策略管理 > >逐星管理 > >安全階护 > >防火喘 > >阿格配置 > >多初路洗箔策略 > >本地子四川表 > >隧道间路由设置 >	 第一阶段 第一阶段 十 新博 (統協出口: 他認 状态 设备名称 ◆ 注册列票公里 - Google Chrome ▲ 不安全 https://主 1000 ※ 注册列票公里 - Google Chrome ▲ 不安全 https://主 1000 ※ 注册列票公里 - Google Chrome ● 公司列票公里 - Google Chrome ● 公司公司公司 ● 公司公司 ● 公司 <!--</th--><th>61 ♥ 快备地址 □ © © ■/html/dlan/device_operate.html a_usn ま ms は ● 0 建築数理 ・ の 単 の の の の の の の の の の の の の</th><th> 以证类型 2 高级技巧 内 2 高级技巧 内 2 高级技巧 内 2 新ty/Gus/device 1 玉山次数: 支持模式: D-域:: 支持模式: D-域:: 予約失型: 我方身份:D: 対方身份:D: 戸 局用SATT字通 </th><th>连接模式 《对话程 28800 10 野蛮模式 MOOP 1024群(2) IF始计 (IPV4 ADDR) handmaann 同時時, men</th><th>当前用户: ISAMP存活时间(例) Note: htsl</th>	61 ♥ 快备地址 □ © © ■/html/dlan/device_operate.html a_usn ま ms は ● 0 建築数理 ・ の 単 の の の の の の の の の の の の の	 以证类型 2 高级技巧 内 2 高级技巧 内 2 高级技巧 内 2 新ty/Gus/device 1 玉山次数: 支持模式: D-域:: 支持模式: D-域:: 予約失型: 我方身份:D: 対方身份:D: 戸 局用SATT字通 	连接模式 《对话程 28800 10 野蛮模式 MOOP 1024群(2) IF始计 (IPV4 ADDR) handmaann 同時時, men	当前用户: ISAMP存活时间(例) Note: htsl
 第三方对报 第一阶段 第二阶段 	 □ 作为最份设备 ① ■ 点明设备 ■ 点明设备 	加利主动信赖	ISAXBP算法列表 以証算法: MD5 加密算法: 3DES		
· 安全选项 ▲通用设置	<u><u>a</u><u></u></u>	装 取消		建定	取納

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
	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。

~		e)	策略设置	一 两页对话框			
导航菜单	《 第二阶段	0	https:/po	licy_s/policy_operates	.c/policy_operate.ht	al	
) 实时状态		₹	启用该案	u de la companya de la		^	
> 对象定文	入站策略 出站策略			uthan		-	
用户与策略管理	+ 勤増	R	-e-o-m - [upran			
、這個管理	状态 策略名称	22	a#:		2		操作
, @AB10	紀用 ruzhan	255	- I		-		编辑量阶
* 35.1.10 ¥		12	11英型: [子同+掩码			
▶ 肋火墙		子	网: 1	192.168.1.0			
> 网络配置		14	14): Z	55.255.255.0			
▼ VPN配置		34	(建设本: []		-		
> 多线路设置		1 m	北照点:	aliyun_vpn			
> 多线路选路策略			Mattill - D	0.T		1	
> 本地子同列表		T	Tratilities 1	<u>まへ</u>	-		
> MX101022.dr10.00		e	• 在时间生效范围内允许 C 在时间生效范围内抗通				
- 第二の利用 第二の利用		Г	启用过期	पान			
1 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10			过期时间	: 0-00-00	: 0 : : 0		
中全法道							
JALEAPA							
▲通用设置	×						
▶ 承统配置							
> 系统诊断					确定	取消 🗸	

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。

SANGFOR TAC			2 策略设置	門页对话框		2	3
异脑菜单 《	第二阶段		2 https://p	slicy_sperate_htsl/dlan	/pelicy_oper	ate htal	
dimb db db			▶ 倉用涼瀬町	6			^
) 头时状态	入站策略 出站策略		AM 00 (7 (1))	churthan			
> 对象定义	-		, 東略古称:	chuanan			
用户与策略管理	计大 新能力的	illing			0		4.12
> 流量管理	启用 chuzhan	192.16.	* (3KBR		×		
 安全防护 	and the second	255.25.	渡IP类型:	子冏+掩码			
▶ 防火墙			子阿:	192.168.18.0			
> 网络配置			推码:	255.255.255.0			
▼ VPN配置			对端设备:	D915W	•	1	
> 多线路设置 🔨			SA生存时间:	28800		8	
> 多线路选路策略			出站服务:	所有服务	•		
> 本地子阿狗表			安全选项:	默认安全选项	•		
> 機道间路由设置			生效时间:	全天	•		
▲第三方对接			• 在时间生活	改范围内允许			
》第一阶段			(在时间生物	改范围内拒绝			
> 第二阶段			E emiliar				
安全选项							
			TEAHUSIM		1:6		
▲通用設置 ●			Commen	P M darde /D de			
- or ound at			一周用型明天	0天門前孫密			

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。

导航菜单 《 安全选项	🖉 安全选项设置 网页对话框 🛛 🔀
, 实时状态 + 新增	https:htal/dlan/securityital/dlan/security_op-
> 対象定义 名称	名称: 默认安全选项 密算法
用户与策略管理 默认安全进	
) 流量管理	H221 - [500
9 安全防护	BAK. JESP
> 防火墙	认证算法
9 网络配置	C Bull
▼ VPN配置	(* mD5
> 多线路设置	C SHA-1
> 多线路选路策略	加密算法
> 本地子阿列表	@ DES
> 隧道间路由设置	C 3DES
▲ 第三方对接	CAES
》第一阶段 第一阶段	C SINFOR_DES
→ 第二B(校) 安全連貫	
XIGX	确定取消
▲通用设置 系统配置	
系统论断	

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 netcfgr_192-168-18-0--24 192.168.18.0/24 set security zones security-zone vpn address-book address netcfgr_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-policycfgr 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-vpncfgr match source-address net-cfgr_192-168-18-0--24 set security policies from-zone trust to-zone vpn policy trust-vpncfgr match destination-address net-cfgr_192-168-1-0--24 set security policies from-zone trust to-zone vpn policy trust-vpncfgr match application any set security policies from-zone trust to-zone vpn policy trust-vpncfgr then permit

8. 配置入站策略。

set security policies from-zone vpn to-zone trust policy vpn-trustcfgr match source-address net-cfgr_192-168-1-0--24 set security policies from-zone vpn to-zone trust policy vpn-trustcfgr match destination-address net-cfgr_192-168-18-0--24 set security policies from-zone vpn to-zone trust policy vpn-trustcfgr match application any set security policies from-zone vpn to-zone trust policy vpn-trustcfgr 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。

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

VPC和本地IDC的网络配置如下:

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。



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.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.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.xx.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。



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	10.0.0/8	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。



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。

E	说明:
	シレッシュ・

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。

1 说明:

VPN网关的创建一般需要1-5分钟。

VPN网关										切换到旧版>>
华北1 华北2 华北3 欧洲中部1(法兰克福)	华北5 华东1	华东 2	华南1 香港 亚太东北1(5	_天 京) 亚太东南 1	l (新加坡)	亚太东南 2 (悉尼) 3	『太东南3 (吉隆坡)	美国东部 1 (弗吉尼亚)	美國西部 1 (建谷) 中东东部 1 (迪拜	i)
创建VPN网关 刷新	自定义									
ID/名称	IP地址	监控	VPC	状态	带宽	计费方式	开启IPSec	开启SSL	SSL并发连接数规格	操作
vpn-bp1ffgb0cxvxrcibr1fwj VPN网关1 III	118. 149	ĸ	vpc-bp15k6sx6fhdz2jw4daz 0 VPC1	 正常 	5M 变配	预付费 2018/2/9 00:00:00 到 期	日开启	开启		编辑 续费
vpn-bp18in10ga65vrrw55r5z VPN网关2 旨	121 .143	k	vpc-bp1hlv5hmp6em9ikpxtut VPC2	• 正常	5M 变配	预付魏 2018/2/9 00:00:00 到 期	已开启	已开启	5 变配	编辑 续费

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	vpn-xxxxqwj	118.xxx.xx.149
ID: vpc-xxxxz0		
网段: 172.16.0.0/12		
名称: VPC2	vpn-xxxx15z	121.xxx.xx.143
ID: vpc-xxxxut		
网段: 10.0.0.0/8		

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	vpn-xxxxqwj	121.xxx.xx.143	user_VPC1
ID: vpc-xxxz0			
网段: 172.16.0.0/12			
名称: VPC2	vpn-xxxxxl5z	118.xxx.xx.149	user_VPC
ID: vpc-xxxxut			
网段: 10.0.0.0/8			

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-xxxxqwj。
- ·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10.0.0/8。
- · 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。

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。