虚拟专用网络

管理员指南

文档版本	01
发布日期	2025-02-05

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

1 站点入云 VPN 企业版

1.1 对接华为 AR 路由器（双活连接）

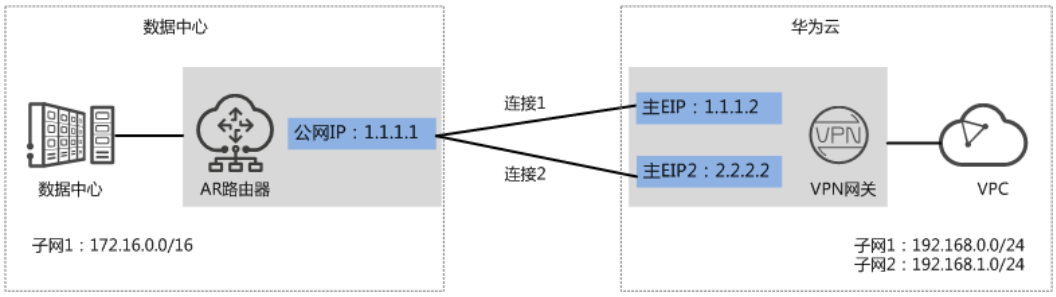
1.1.1 静态路由模式

1.1.1.1 操作指引

场景描述

VPN网关通过静态路由模式对接华为AR路由器的典型组网如**图 典型组网**所示。

图 1-1 典型组网



本场景下以AR路由器单IP地址方案为例，VPN网关采用双活模式，主EIP、主EIP2分别和该IP地址创建一条VPN连接。

约束与限制

VPN和AR路由器支持的认证算法、加密算法存在差异，请确保创建连接时两端策略配置保持一致。

数据规划

表 1-1 数据规划

部件	参数项	AR路由器规划示例	华为云规划示例
VPC	子网	172.16.0.0/16	• 192.168.0.0/24 • 192.168.1.0/24
VPN网关	网关IP	1.1.1.1（AR路由器上行公网网口GE0/0/8的接口IP）	• 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
	互联子网	-	192.168.2.0/24
VPN连接	隧道接口地址	• tunnel1：169.254.70.1/30 • tunnel2：169.254.71.1/30	• tunnel1：169.254.70.2/30 • tunnel2：169.254.71.2/30
	IKE策略	• 版本：v2 • 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group 14 • 生命周期（秒）：86400 • 本端标识：IP Address • 对端标识：IP Address	
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH group 14 • 传输协议：ESP • 生命周期（秒）：3600	

操作流程

通过VPN实现数据中心和VPC互通的操作流程如**图1-2**所示。

图 1-2 操作流程

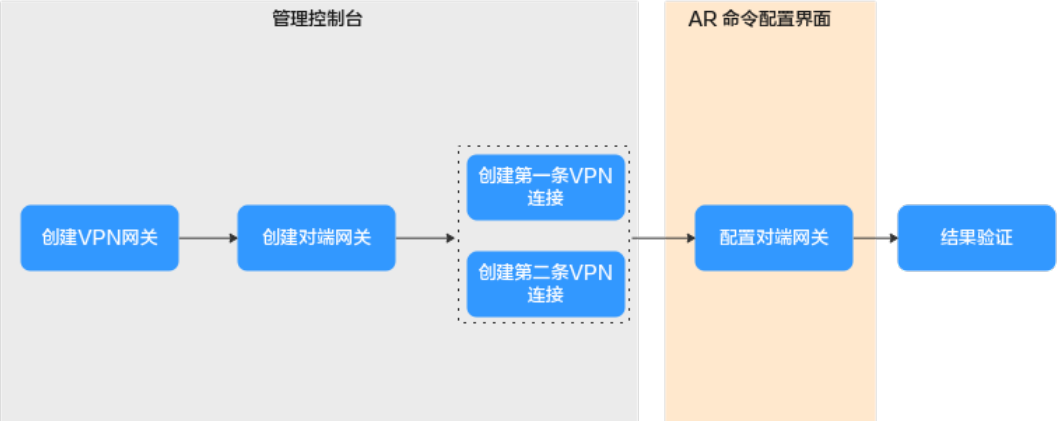


表 1-2 操作流程说明

序号	在哪里操作	步骤	说明
1	管理控制台	**创建VPN网关**	VPN网关需要绑定两个EIP作为出口公网IP。 如果您已经购买EIP，则此处可以直接绑定使用。
2		**创建对端网关**	添加AR路由器作为对端网关。
3		**创建第一条VPN连接**	VPN网关的主EIP和对端网关组建第一条VPN连接。
4		**创建第二条VPN连接**	VPN网关的主EIP2和对端网关组建第二条VPN连接。 第二条VPN连接的连接模式、预共享密钥、IKE/IPsec策略建议和第一条VPN连接配置保持一致。
5	AR命令配置界面	**AR路由器侧操作步骤**	• AR路由器配置的本端隧道接口地址/对端隧道接口地址需要和VPN网关互为镜像配置。 • AR路由器配置的连接模式、预共享密钥、IKE/IPsec策略需要和VPN连接配置保持一致。
6	-	**结果验证**	执行**ping**命令，验证网络互通情况。

1.1.1.2 云侧控制台操作步骤

前提条件

云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“站点入云VPN网关”的页签后，再单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如表1-3所示。

表 1-3 VPN 网关参数说明

参数	说明	参数取值
名称	VPN网关的名称。	vpngw-001
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和用户数据中心的VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	华为云VPC需要与用户数据中心VPC互通的子网。	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP自治系统号码。	64512
HA模式	选择VPN网关的工作模式。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

   对端网关参数说明如表1-4所示。

表 1-4 对端网关参数说明

参数	说明	参数取值
名称	对端网关的名称。	cgw-ar
标识	选择“IP Address”，并输入AR路由器的公网IP地址。	IP Address 1.1.1.1

参数	说明	参数取值
BGP ASN	请输入用户数据中心或私有网络的ASN。 用户数据中心的BGP ASN与VPN网关的BGP ASN不能相同。	65000

步骤5 配置VPN连接。

本场景下，AR路由器与VPN网关主EIP、主EIP2分别创建一条VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
1. 创建第一条VPN连接。
   VPN连接参数说明如**表 第一条VPN连接参数说明**所示。

表 1-5 第一条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-ar
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	172.16.0.0/16
接口分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.70.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.1/30

参数	说明	取值参数
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。 VPN网关会自动对对端接口地址进行NQA探测，要求对端接口地址在对端网关上已配置。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关连接的预共享密钥需要保持一致。	*请根据实际设置*
策略配置	和防火墙的策略配置需要保持一致。	– IKE策略 ■ 版本：v2 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ DH算法：Group 14 ■ 生命周期（秒）：86400 ■ 本端标识：IP Address ■ 对端标识：IP Address – IPsec策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ PFS：DH group 14 ■ 传输协议：ESP ■ 生命周期（秒）：3600

2. 创建第二条VPN连接参数。

说明

此处仅对和第一条VPN连接配置不同的参数进行说明，未提及参数建议和第一条VPN连接保持一致。

表 1-6 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.1/30

----结束

1.1.1.3 AR 路由器侧操作步骤

操作步骤

步骤1 登录AR路由器配置界面。

步骤2 进入系统视图。

<AR651>system-view

步骤3 配置公网接口的IP地址。

[AR651]interface GigabitEthernet 0/0/8

[AR651-GigabitEthernet0/0/8]ip address 1.1.1.1 255.255.255.0

[AR651-GigabitEthernet0/0/8]quit

步骤4 配置默认路由。

[AR651]ip route-static 0.0.0.0 0.0.0.0 1.1.1.254

其中，1.1.1.254为AR路由器公网IP的网关地址，请根据实际替换。

步骤5 配置VPN网关主EIP/主EIP2到AR路由器的路由信息。

[AR651]ip route-static 1.1.1.2 255.255.255.255 1.1.1.254

[AR651]ip route-static 2.2.2.2 255.255.255.255 1.1.1.254

- 1.1.1.2/2.2.2.2为VPN网关的主EIP、主EIP2。
- 1.1.1.254为AR路由器公网IP的网关地址。

步骤6 开启SHA-2算法兼容RFC标准算法功能。

[AR651]IPsec authentication sha2 compatible enable

步骤7 配置IPsec安全提议。

```
[AR651]IPsec proposal hwproposal1
[AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256
[AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128
[AR651-IPsec-proposal-hwproposal1]quit
```

步骤8 配置IKE安全提议。

```
[AR651]ike proposal 2
[AR651-ike-proposal-2]encryption-algorithm aes-128
[AR651-ike-proposal-2]dh Group14
[AR651-ike-proposal-2]authentication-algorithm sha2-256
[AR651-ike-proposal-2]authentication-method pre-share
[AR651-ike-proposal-2]integrity-algorithm hmac-sha2-256
[AR651-ike-proposal-2]prf hmac-sha2-256
[AR651-ike-proposal-2]quit
```

步骤9 配置IKE对等体。

```
[AR651]ike peer hwpeer1
[AR651-ike-peer-hwpeer1]undo version 1
[AR651-ike-peer-hwpeer1]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer1]ike-proposal 2
[AR651-ike-peer-hwpeer1]local-address 1.1.1.1
[AR651-ike-peer-hwpeer1]remote-address 1.1.1.2
[AR651-ike-peer-hwpeer1]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer1]rsa signature-padding pss
[AR651-ike-peer-hwpeer1]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer1]quit
#
[AR651]ike peer hwpeer2
[AR651-ike-peer-hwpeer2]undo version 1
[AR651-ike-peer-hwpeer2]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer2]ike-proposal 2
[AR651-ike-peer-hwpeer2]local-address 1.1.1.1
[AR651-ike-peer-hwpeer2]remote-address 2.2.2.2
[AR651-ike-peer-hwpeer2]rsa encryption-padding oaep
```


[AR651-ike-peer-hwpeer2]rsa signature-padding pss

[AR651-ike-peer-hwpeer2]ikev2 authentication sign-hash sha2-256

[AR651-ike-peer-hwpeer2]quit

相关命令说明如下：

- ike peer hwpeer1、ike peer hwpeer2：对应两条VPN连接。
- pre-shared-key cipher：预共享密钥。
- local-address：AR路由器的公网地址。
- remote-address：VPN网关的主EIP、主EIP2。

步骤10 配置IPsec安全框架。

[AR651]IPsec profile hwpro1

[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1

[AR651-IPsec-profile-hwpro1]proposal hwproposal1

[AR651-IPsec-profile-hwpro1]pfs dh-Group14

[AR651-IPsec-profile-hwpro1]quit

#

[AR651]IPsec profile hwpro2

[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2

[AR651-IPsec-profile-hwpro2]proposal hwproposal1

[AR651-IPsec-profile-hwpro2]pfs dh-Group14

[AR651-IPsec-profile-hwpro2]quit

步骤11 配置虚拟隧道接口。

[AR651]interface Tunnel0/0/1

[AR651-Tunnel0/0/1]mtu 1400

[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252

[AR651-Tunnel0/0/1]tunnel-protocol IPsec

[AR651-Tunnel0/0/1]source 1.1.1.1

[AR651-Tunnel0/0/1]destination 1.1.1.2

[AR651-Tunnel0/0/1]IPsec profile hwpro1

[AR651-Tunnel0/0/1]quit

#

[AR651]interface Tunnel0/0/2

[AR651-Tunnel0/0/2]mtu 1400

[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252


```
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 1.1.1.1
[AR651-Tunnel0/0/2]destination 2.2.2.2
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

相关命令说明如下：

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

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

步骤12 配置NQA。

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

相关命令说明如下：

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

本示例中，IPsec_nqa1对应VPN网关主EIP所在的VPN连接；IPsec_nqa2对应VPN网关主EIP2所在的VPN连接。

- destination-address：VPN网关的Tunnel接口地址。
- source-address：AR路由器的Tunnel接口地址。

步骤13 配置静态路由联动NQA功能。

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

[AR651]ip route-static 192.168.1.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1 IPsec_nqa1

[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/2 preference 100 track nqa IPsec_nqa2 IPsec_nqa2

[AR651]ip route-static 192.168.1.0 255.255.255.0 Tunnel0/0/2 preference 100 track nqa IPsec_nqa2 IPsec_nqa2

相关参数说明如下：

- 192.168.0.0/192.168.1.0：VPC本端子网。
  - 每个子网需要分别独立配置路由track nqa。
  - 同一条命令中，Tunnel*x*和IPsec_nqa*x*需要同属于一条VPN连接。
- preference 100：路由优先级，不配置默认为60。

  本示例中，流量优先走VPN网关主EIP所在的VPN连接；两条VPN连接为双活模式。

  如果希望流量从两条流量各走一半，即负载分担模式，则需要删除preference 100。

----结束

1.1.1.4 结果验证

- 大约5分钟后，查看VPN连接状态。
  - 华为云

    选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
  - AR路由器

    选择“高级 > VPN > IPSec > IPSec策略管理”，两条VPN连接状态显示为“READY|STAYLIVE”。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

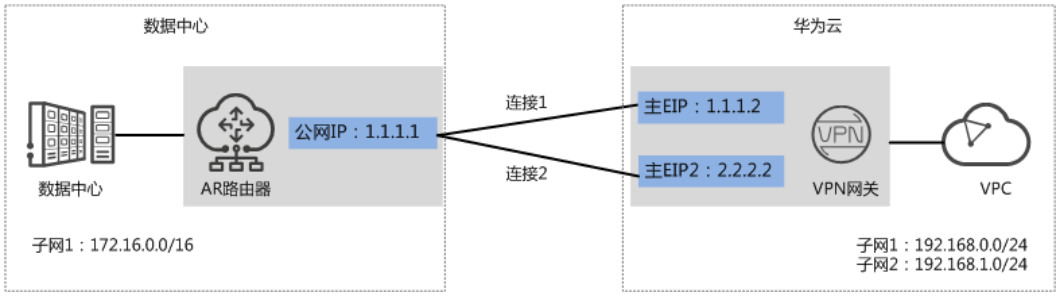
1.1.2 BGP 路由模式

1.1.2.1 操作指引

场景描述

VPN网关通过BGP路由模式对接华为AR路由器的典型组网如**图 典型组网**所示。

图 1-3 典型组网



本场景下以AR路由器单IP地址方案为例，VPN网关采用双活模式，主EIP、主EIP2分别和该IP地址创建一条VPN连接。

约束与限制

VPN和AR路由器支持的认证算法、加密算法存在差异，请确保创建连接时两端策略配置保持一致。

数据规划

表 1-7 数据规划

部件	参数项	AR路由器规划示例	华为云规划示例
VPC	子网	172.16.0.0/16	192.168.0.0/24 192.168.1.0/24
VPN网关	网关IP	1.1.1.1（AR路由器上行公网网口GE0/0/8的接口IP）	主EIP：1.1.1.2 主EIP2：2.2.2.2
	互联子网	-	192.168.2.0/24
	BGP ASN	64515	64512
VPN连接	隧道接口地址	• tunnel1：169.254.70.1/30 • tunnel2：169.254.71.1/30	• tunnel1：169.254.70.2/30 • tunnel2：169.254.71.2/30
	IKE策略	• 版本：v2 • 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group 14 • 生命周期（秒）：86400 • 本端标识：IP Address • 对端标识：IP Address	

部件	参数项	AR路由器规划示例	华为云规划示例
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH group 14 • 传输协议：ESP • 生命周期（秒）：3600	

操作流程

通过VPN实现数据中心和VPC互通的操作流程如图 操作流程所示。

图 1-4 操作流程

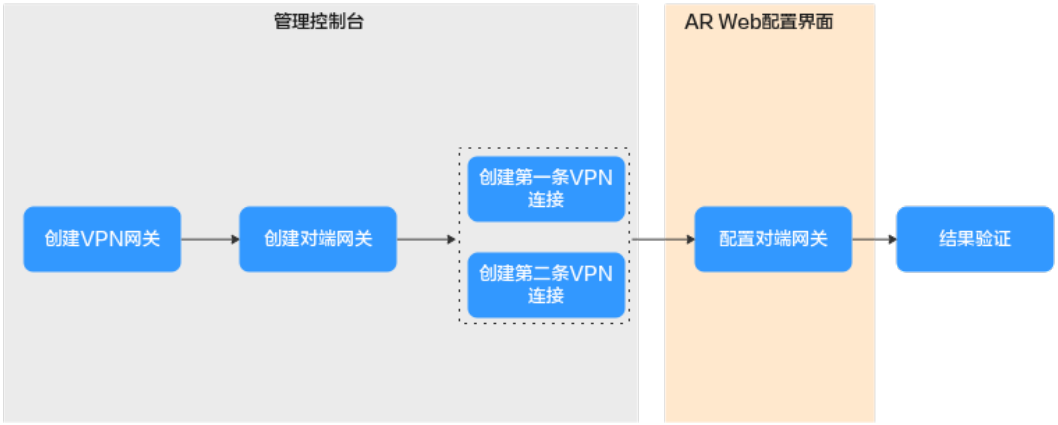


表 1-8 操作流程说明

序号	在哪里操作	步骤	说明
1	管理控制台	创建VPN网关	VPN网关需要绑定两个EIP作为出口公网IP。 如果您已经购买EIP，则此处可以直接绑定使用。
2		创建对端网关	添加AR路由器作为对端网关。
3		创建第一条VPN连接	VPN网关的主EIP和对端网关组建第一条VPN连接。
4		创建第二条VPN连接	VPN网关的主EIP2和对端网关组建第二条VPN连接。 第二条VPN连接的连接模式、预共享密钥、IKE/IPsec策略建议和第一条VPN连接配置保持一致。

序号	在哪里操作	步骤	说明
5	AR命令配置界面	AR路由器侧操作步骤	• AR路由器的本端隧道接口地址/对端隧道接口地址需要和VPN网关互为镜像配置。 • AR路由器的连接模式、预共享密钥、IKE/IPsec策略需要和VPN连接配置保持一致。
6	-	结果验证	执行**ping**命令，验证网络互通情况。

1.1.2.2 云侧控制台操作步骤

前提条件

云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“站点入云VPN网关”的页签后，再单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”。

   VPN网关关键参数说明如**表 VPN网关关键参数说明**所示。此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-9 VPN 网关关键参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和用户数据中心的VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	华为云VPC需要与用户数据中心VPC互通的子网。	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP自治系统号码。	64512

参数	说明	取值参数
HA模式	选择VPN网关的工作模式。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。
   对端网关参数说明如**表 对端网关参数说明**所示。

表 1-10 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-ar
标识	选择“IP Address”，并输入AR路由器的公网IP地址。	IP Address 1.1.1.1
BGP ASN	AR路由器的BGP自治系统号码。	65000

步骤5 配置VPN连接。

本场景下，AR路由器与VPN网关主EIP、主EIP2分别创建一条VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
1. 创建第一条VPN连接。
   VPN连接参数说明如**表 第一条VPN连接参数说明**所示。

表 1-11 第一条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-ar
连接模式	选择“BGP路由模式”。	BGP路由模式

参数	说明	取值参数
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	172.16.0.0/16
接口分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.70.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.1/30
预共享密钥、确认密钥	和防火墙连接的预共享密钥需要保持一致。	*请根据实际设置*

参数	说明	取值参数
策略配置	和防火墙的策略配置需要保持一致。	– IKE策略 ■ 版本：v2 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ DH算法：Group 14 ■ 生命周期（秒）：86400 ■ 本端标识：IP Address ■ 对端标识：IP Address – IPsec策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ PFS：DH Group 14 ■ 传输协议：ESP ■ 生命周期（秒）：3600

2. 创建第二条VPN连接。

说明

此处仅对和第一条VPN连接配置不同的参数进行说明，未提及参数建议和第一条VPN连接保持一致。

表 1-12 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2

参数	说明	取值参数
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.1/30

----结束

1.1.2.3 AR 路由器侧操作步骤

前提条件

- 已配置AR路由器上行公网网口：GE0/0/8，公网IP假设为1.1.1.1。
- 已配置AR路由器下行私网网口：GE0/0/1，私网IP假设为172.16.0.1。

操作步骤

步骤1 登录AR路由器Web管理界面。

此处以AR651 V300R019C13SPC200为例，不同设备型号、系统版本的Web管理界面可能存在差异，配置时请以对应设备型号、系统版本的产品文档为准。

步骤2 配置基础设置。

选择“高级 > IP业务 > 路由 > 静态路由配置 > IPv4 静态路由”，分别填写到主EIP、主EIP2的静态路由信息后，单击“添加”，关键参数配置如**图 静态路由配置**所示。

图 1-5 静态路由配置

步骤3 配置tunnel接口。

1. 选择“高级 > 接口管理 > 逻辑接口”。
2. 配置两个tunnel接口，信息填写完毕后单击“添加”。
   关键参数配置如**图 tunnel接口配置**所示。

图 1-6 tunnel 接口配置

步骤4 配置VPN连接。

1. 选择“高级 > VPN > IPSec > IPSec策略管理”。
2. 配置两个tunnel的IKE策略、IPSec策略，关键参数配置如**图 第一条VPN连接配置**、**图 第二条VPN连接配置**所示。

说明

- 采用IKEv1进行IPSec协商时，如果隧道有一端的流量超时配置为0，则隧道两端都关闭流量超时功能。
- 采用IKEv2进行IPSec协商时，隧道流量超时值配置为0，则关闭本端流量超时功能。

图 1-7 第一条 VPN 连接配置

图 1-8 第二条 VPN 连接配置

步骤5 配置BGP。

1. 选择“高级 > IP业务 > 路由 > 动态路由配置 > BGP”。
2. 将“启动BGP”按钮置为开启状态，“AS号”配置为AR路由器的BGP自治系统号码，“路由器ID”配置为AR路由器下行私网网口的网关地址，单击“应用”。
3. 配置BGP邻居，关键参数配置如图 BGP邻居配置所示。

图 1-9 BGP 邻居配置

4. 配置路由引入，在“路由引入设置”区域将“协议类型”配置为“Direct”。

----结束

1.1.2.4 结果验证

- 大约5分钟后，查看VPN连接状态。
  - 华为云
    选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
  - AR路由器
    选择“高级 > VPN > IPSec > IPSec策略管理”，两条VPN连接状态显示为“READY|STAYLIVE”。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

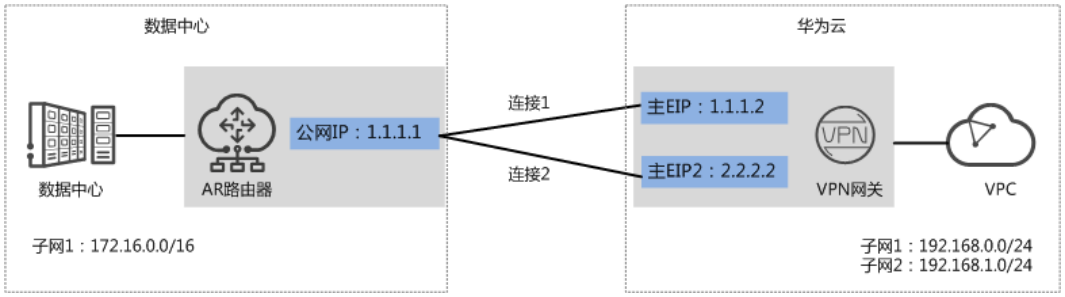
1.1.3 策略模式

1.1.3.1 操作指引

场景描述

VPN网关通过策略模式对接华为AR路由器的典型组网如图 典型组网所示。

图 1-10 典型组网



本场景下以AR路由器单IP地址方案为例，VPN网关采用双活模式，主EIP、主EIP2分别和该IP地址创建一条VPN连接。

约束与限制

VPN和AR路由器支持的认证算法、加密算法存在差异，请确保创建连接时两端策略配置保持一致。

数据规划

表 1-13 数据规划

部件	参数项	AR路由器规划示例	华为云规划示例
VPC	子网	172.16.0.0/16	• 192.168.0.0/24 • 192.168.1.0/24
VPN网关	网关IP	1.1.1.1（AR路由器上行公网网口GE0/0/8的接口IP）	• 主EIP：1.1.1.2 • 主EIP2：2.2.2.2

部件	参数项	AR路由器规划示例	华为云规划示例
	互联子网	-	192.168.2.0/24
VPN连接	IKE策略	• 版本：v2 • 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group 14 • 生命周期（秒）：86400 • 本端标识：IP Address • 对端标识：IP Address	
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH group 14 • 传输协议：ESP • 生命周期（秒）：3600	

操作流程

通过VPN实现数据中心和VPC互通的操作流程如图 操作流程所示。

图 1-11 操作流程

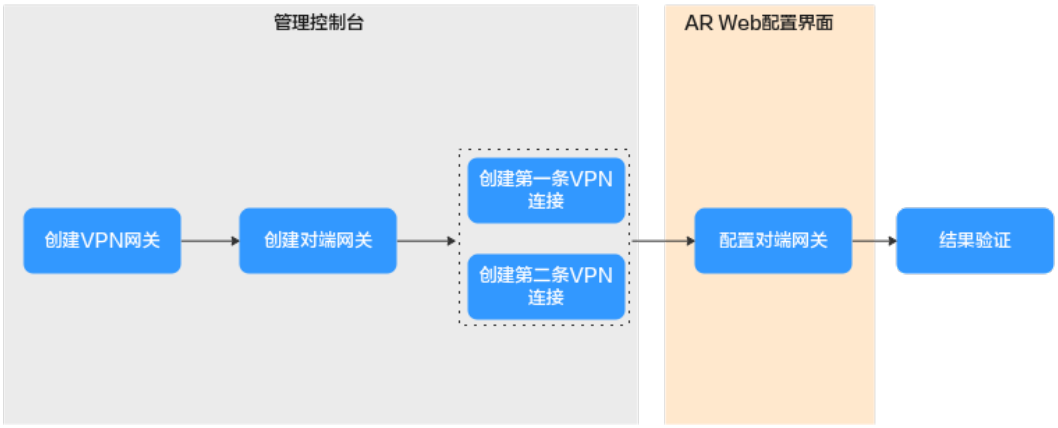


表 1-14 操作流程说明

序号	在哪里操作	步骤	说明
1	管理控制台	**创建VPN网关**	VPN网关需要绑定两个EIP作为出口公网IP。 如果您已经购买EIP，则此处可以直接绑定使用。
2		**创建对端网关**	添加AR路由器作为对端网关。
3		**创建第一条VPN连接**	VPN网关的主EIP和对端网关组建第一条VPN连接。
4		**创建第二条VPN连接**	VPN网关的主EIP2和对端网关组建第二条VPN连接。 第二条VPN连接的连接模式、预共享密钥、IKE/IPsec策略建议和第一条VPN连接配置保持一致。
5	AR命令配置界面	**AR路由器侧操作步骤**	• AR路由器的本端隧道接口地址/对端隧道接口地址需要和VPN网关互为镜像配置。 • AR路由器的连接模式、预共享密钥、IKE/IPsec策略需要和VPN连接配置保持一致。
6	-	**结果验证**	执行**ping**命令，验证网络互通情况。

1.1.3.2 云侧控制台操作步骤

前提条件

云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“站点入云VPN网关”的页签后，再单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”。

   VPN网关关键参数说明如**表 VPN网关关键参数说明**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-15 VPN 网关关键参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和用户数据中心的VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	华为云VPC需要与用户数据中心VPC互通的子网。	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP自治系统号码。	64512
HA模式	选择VPN网关的工作模式。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
备EIP	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。
   对端网关参数说明如**表 对端网关参数说明**所示。

表 1-16 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-ar
标识	选择“IP Address”，并输入AR路由器的公网IP地址。	IP Address 1.1.1.1
BGP ASN	AR路由器的BGP自治系统号码。	65000

步骤5 配置VPN连接。

本场景下，AR路由器与VPN网关主EIP、主EIP2分别创建一条VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 创建第一条VPN连接。
   VPN连接参数说明如**表 第一条VPN连接参数说明**所示。

表 1-17 第一条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-ar
连接模式	选择“策略模式”。	策略模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	172.16.0.0/16
预共享密钥、确认密钥	和对端网关连接的预共享密钥需要保持一致。	*请根据实际设置*
策略规则	用于定义本端子网到对端子网之间具体进入VPN连接加密隧道的数据流信息，由源网段与目的网段来定义。 – 源网段 源网段必须包含部分本端子网。其中，0.0.0.0/0表示任意地址。 – 目的网段 目的网段必须完全包含对端子网。	– 源网段1：192.168.0.0/24 – 目的网段1：172.16.0.0/16 – 源网段2：192.168.1.0/24 – 目的网段2：172.16.0.0/16

参数	说明	取值参数
策略配置	和防火墙的策略配置需要保持一致。	– IKE策略 ■ 版本：v2 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ DH算法：Group 14 ■ 生命周期（秒）：86400 ■ 本端标识：IP Address ■ 对端标识：IP Address – IPsec策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ PFS：DH Group 14 ■ 传输协议：ESP ■ 生命周期（秒）：3600

3. 配置第二条VPN连接参数。

   说明

   此处仅对和第一条VPN连接配置不同的参数进行说明，未提及参数建议和第一条VPN连接保持一致。

   表 1-18 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2

----结束

1.1.3.3 AR 路由器侧操作步骤

前提条件

- 已配置AR路由器WAN口IP地址：GE0/0/8，公网IP地址假设为1.1.1.1。
- 已配置AR路由器LAN口IP地址：GE0/0/1，私网IP地址假设为172.16.0.1。

操作步骤

步骤1 登录AR路由器Web管理界面。

此处以AR651 V300R019C13SPC200为例，不同设备型号、系统版本的Web管理界面可能存在差异，配置时请以对应设备型号、系统版本的产品文档为准。

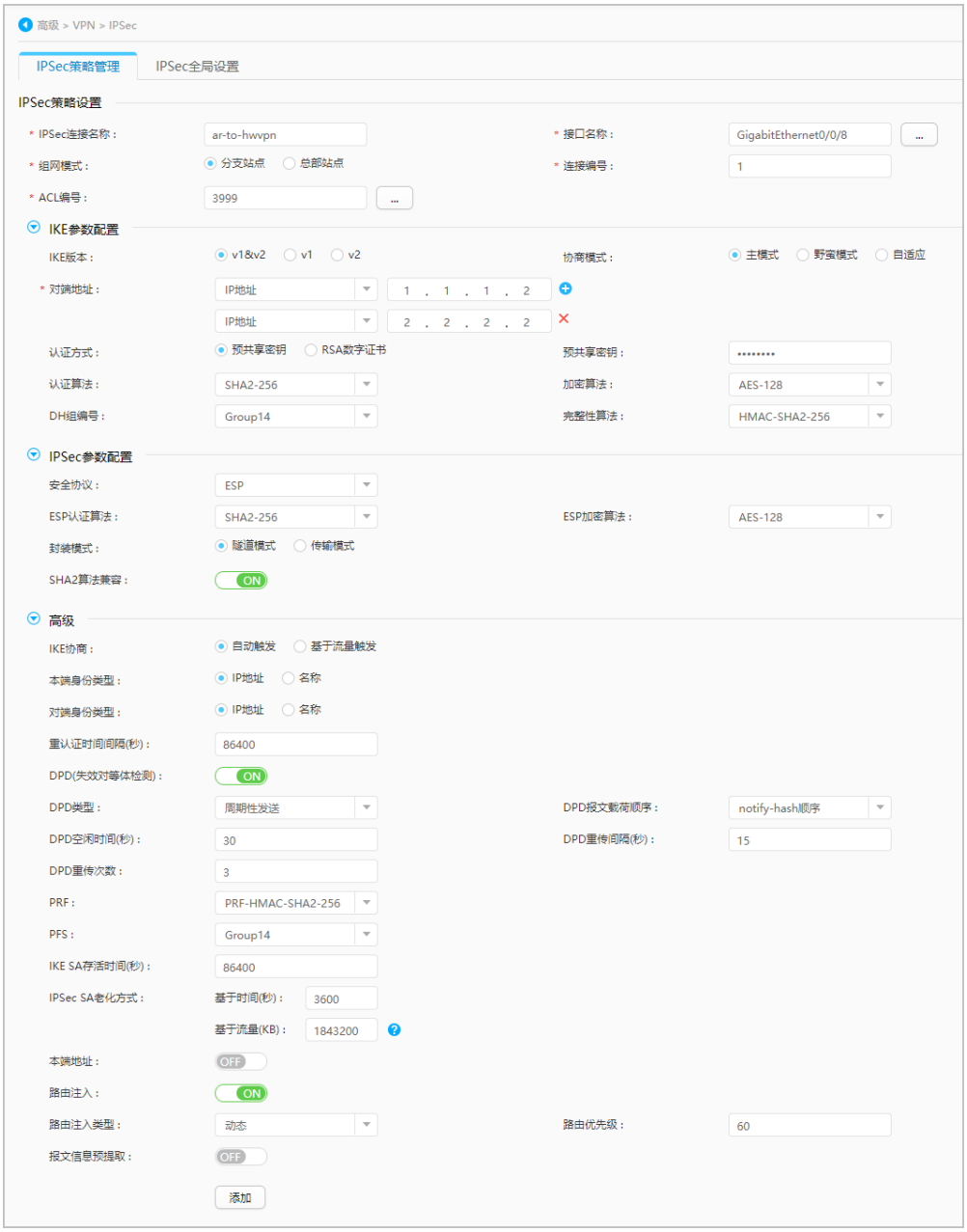
步骤2 配置VPN连接。

1. 选择“高级 > VPN > IPSec > IPSec策略管理”。
2. 配置IKE策略、IPSec策略，关键参数配置如**图 VPN连接配置**所示。

说明

- 采用IKEv1进行IPSec协商时，如果隧道有一端的流量超时配置为0，则隧道两端都关闭流量超时功能。
- 采用IKEv2进行IPSec协商时，如果隧道流量超时值配置为0，则关闭本端流量超时功能。
- 若AR路由器使用非固定IP接入云上VPN网关，**图 VPN连接配置**中“高级>本端身份类型”需设置为“名称”，其值与云上对端网关标识保持一致。

图 1-12 VPN 连接配置



步骤3 配置VPN安全策略。

选择“配置 > 攻击防范 > ACL > 高级ACL”，高级ACL填写完毕后单击“添加”，关键参数配置如**图 高级ACL规则配置**所示。

图 1-13 高级 ACL 规则配置

步骤4 配置业务路由。

选择“高级 > IP业务 > 路由 > 静态路由配置 > IPv4 静态路由”，分别填写到VPN网关主EIP、主EIP2及云上VPC的静态路由信息后，单击“添加”，关键参数配置如**图 业务路由配置**所示。

图 1-14 业务路由配置

----结束

1.1.3.4 结果验证

说明

策略模式下，AR路由器使用1个接口创建2个VPN连接，由于AR路由器功能规格限制，同一时间只能有1个VPN连接是协商正常的。

- 大约5分钟后，查看VPN连接状态。
  - 云侧管理控制台

    选择“虚拟专用网络 > 企业版-VPN连接”，只有1条VPN连接状态显示为“正常”。
  - AR路由器

    选择“高级 > VPN > IPSec > IPSec策略管理”，只有一条VPN连接状态显示为“READY|STAYLIVE”。
- 用户数据中心内服务器和VPC子网内服务器可以相互Ping通。

1.2 对接阿里云

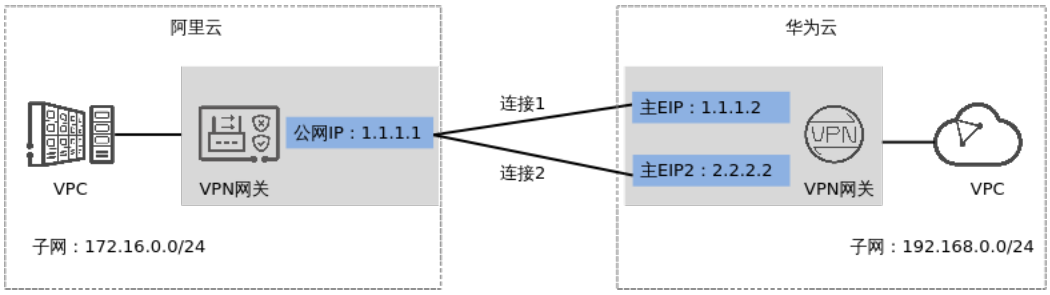
1.2.1 静态路由模式

1.2.1.1 操作指引

场景介绍

华为云VPN网关通过静态路由模式对接阿里云的典型组网如图 典型组网所示。

图 1-15 典型组网



本场景下，阿里云VPN网关采用单IP地址方案，华为云VPN网关采用双活模式，主EIP、主EIP2分别和该IP地址创建一条VPN连接。

数据规划

表 1-19 数据规划

部件	参数项	阿里云规划示例	华为云规划示例
VPC	子网	172.16.0.0/24	192.168.0.0/24
VPN网关	网关IP	1.1.1.1	• 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
	互联子网	-	192.168.2.0/24
VPN连接	隧道接口地址	• tunnel1：169.254.70.1/30 • tunnel2：169.254.71.1/30	• tunnel1：169.254.70.2/30 • tunnel2：169.254.71.2/30

部件	参数项	阿里云规划示例	华为云规划示例
	IKE策略	● 版本：v2 ● 认证算法：SHA2-256 ● 加密算法：AES-128 ● DH算法：Group14 ● 本端标识：IP Address ● 对端标识：IP Address	
	IPsec策略	● 认证算法：SHA2-256 ● 加密算法：AES-128 ● PFS：DH Group14	

1.2.1.2 华为云控制台操作步骤

前提条件

云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“站点入云VPN网关”的页签后，再单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”。

   VPN网关参数说明如下所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-20 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和用户数据中心的VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24

参数	说明	取值参数
本端子网	华为云VPC需要与用户数据中心VPC互通的子网。	192.168.0.0/24
BGP ASN	BGP自治系统号码。	64512
HA模式	选择VPN网关的工作模式。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

   对端网关参数说明如**表 对端网关参数说明**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-21 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-ali
标识	– IP Address：使用对端网关的网关IP作为IP Address。 – FQDN：全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 如果对端网关无固定IP，请选择FQDN类型标识。 **说明** 请确认对端网关的ACL规则已经放通UDP端口4500。	IP Address 1.1.1.1

步骤5 配置VPN连接。

本场景下，对端网关仅支持单IP地址方案，华为云VPN网关推荐使用双活模式，主EIP、主EIP2分别和该IP地址创建一条VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 根据界面提示配置参数。

   VPN连接参数说明如**表 VPN连接参数说明**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-22 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-ali
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	172.16.0.0/24
接口分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.70.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.1/30
检测机制	阿里云不支持NQA功能。	不勾选“使能NQA”
预共享密钥、确认密钥	和对端网关连接的预共享密钥需要保持一致。	*请根据实际设置*

参数	说明	取值参数
策略配置	和防火墙的策略配置需要保持一致。 整体支持情况见**表 数据规划**。	– IKE策略 ▪ 版本：v2 ▪ 认证算法：SHA2-256 ▪ 加密算法：AES-128 ▪ DH算法：Group 14 ▪ 生命周期（秒）：86400 ▪ 本端标识：IP Address ▪ 对端标识：IP Address – IPsec策略 ▪ 认证算法：SHA2-256 ▪ 加密算法：AES-128 ▪ PFS：DH Group 14 ▪ 传输协议：ESP ▪ 生命周期（秒）：3600

a. 创建第二条VPN连接参数。

说明

此处仅对和第一条VPN连接配置不同的参数进行说明，未提及参数建议和第一条VPN连接保持一致。

表 1-23 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2

参数	说明	取值参数
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.1/30

----结束

1.2.1.3 阿里云控制台操作步骤

前提条件

阿里云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录阿里云控制台。

步骤2 选择“产品与服务 > 网络和CDN > 混合云网络 > VPN网关”。

步骤3 配置VPN网关。

1. 单击“创建VPN网关”
2. 根据界面提示配置参数。

   VPN网关参数说明如**表 VPN网关参数说明**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

   表 1-24 VPN 网关参数说明

参数	说明	取值参数
实例名称	VPN网关的名称。	vpngw-ali
VPC	选择VPC信息。	vpc-ali
带宽规格	VPN转发带宽规格。	5Mbps
IPsec-VPN	-	开启
SSL-VPN	-	关闭
计费周期	VPN网关的购买时长。	1个月

步骤4 配置用户网关。

1. 选择“VPN > 用户网关”，单击“创建用户网关”。
2. 根据界面提示配置参数。

   对端网关参数说明如**表 对端网关参数说明**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-25 对端网关参数说明

参数	说明	取值参数
名称	华为VPN网关的名称。	cgw-hw01
IP地址	华为云VPN网关的主EIP。	1.1.1.2

3. 参见上述步骤，配置华为云VPN网关主EIP2对应的用户网关。

步骤5 配置VPN连接。

1. 选择“VPN > IPsec连接”，单击“创建IPsec连接”。
2. 根据界面提示配置参数。

   VPN连接参数说明如**表 VPN连接参数说明**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-26 VPN 连接参数说明

模块	参数	说明	取值参数
-	名称	VPN连接的名称。	vpn-ali
	绑定资源	选择VPN网关	VPN网关
	VPN网关	选择阿里云VPN网关。	vpngw-ali
	用户网关	选择华为云VPN网关。	cgw-hw01
	路由模式	选择目的路由模式	目的路由模式
	立即生效	-	是
	预共享密钥	需要和**表 VPN连接参数说明**设置的预共享密钥保持一致。	*请根据实际设置*
	高级配置	-	开启
IKE策略	版本	需要和**表 VPN连接参数说明**配置的IKE策略保持一致。	– 版本：ikev2 – 协商模式：Main – 加密算法：AES-128 – 认证算法：SHA2-256 – DH分组：Group 14 – SA生存周期：86400 – LocalId：1.1.1.1 – RomoteId：1.1.1.2
	协商模式		
	加密算法		
	认证算法		
	DH分组		

模块	参数	说明	取值参数
	SA生存周期		
	LocalId		
	Romote Id		
IPsec策略	加密算法	需要和**表 VPN连接参数说明**配置的IPsec策略保持一致。 **说明** NAT穿越功能必须配置为开启。	– 加密算法：AES-128 – 认证算法：SHA2-256 – DH分组：Group 14 – SA生存周期：3600 – DPD：开启 – NAT穿越：开启
	认证算法		
	DH分组		
	SA生存周期		
	DPD		
	NAT穿越		
健康检查	健康检查	-	– 健康检查：打开 – 目标IP：192.168.0.10 – 源IP：172.16.0.10 – 重试间隔：3 – 重试次数：3
	目标IP	华为云VPC子网内服务器的私网地址。 此处取值仅作示例，请以实际为准。	
	源IP	阿里云VPC子网内服务器的私网地址。 此处取值仅作示例，请以实际为准。	
	重试间隔	-	
	重试次数	-	

3. 参见上述步骤，配置华为云VPN网关主EIP2对应用户网关（cgw-hw02）的VPN连接。

步骤6 配置路由信息。

需要在阿里云上增加到华为云VPC子网的路由信息。

1. 选择“VPN > VPN网关”。
2. 单击VPN网关名称，在“目的路由表”页签下，单击“添加路由条目”。
3. 根据界面提示配置参数。

- 配置到主EIP的路由信息，如表1-27所示。

  表 1-27 到主 EIP 的路由表参数说明

参数	说明	取值参数
目标网段	华为云VPN网关的本端子网。 如果存在多个本端子网，则创建多条路由。	192.168.0.0/24
下一跳类型	选择“IPsec连接”。	IPsec连接
下一跳	选择阿里云VPN网关。	vpn-ali/xxxxxxxxx
发布到VPC	-	是
权重	-	100

- 配置到主EIP2的路由信息，如表1-28所示。

  表 1-28 到主 EIP2 的路由表参数说明

参数	说明	取值参数
目标网段	华为云VPN网关的本端子网。 如果存在多个本端子网，则创建多条路由。	192.168.0.0/24
下一跳类型	选择“IPsec连接”。	IPsec连接
下一跳	选择阿里云VPN网关。	vpn-ali/xxxxxxxxx
发布到VPC	-	是
权重	-	0

----结束

1.2.1.4 结果验证

- 大约5分钟后，查看VPN连接状态。
  - 华为云

    选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
  - 阿里云

    选择“VPN > IPsec连接”，两条VPN连接状态显示为第二阶段协商成功；由于阿里云VPN连接使用主备模式方案，故健康检查状态显示为主连接正常，备连接异常。
- 阿里云VPC子网内服务器和华为云VPC子网内服务器可以相互Ping通。

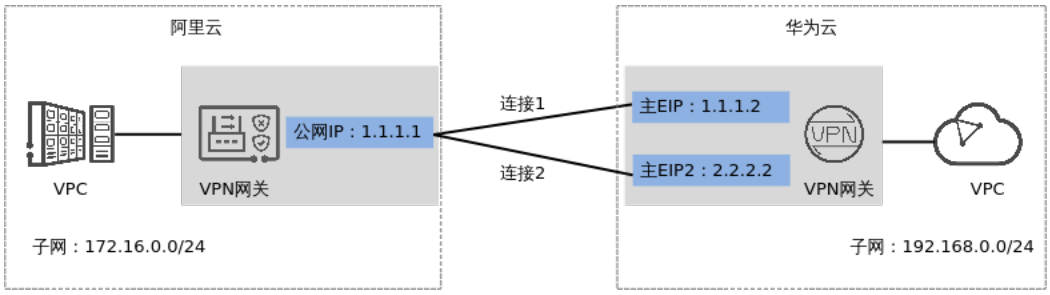
1.2.2 BGP 路由模式

1.2.2.1 操作指引

场景介绍

华为云VPN网关通过BGP路由模式对接阿里云的典型组网如图 典型组网所示。

图 1-16 典型组网



本场景下，阿里云VPN网关仅支持单IP地址方案，华为云VPN网关的主EIP、主EIP2分别和该IP地址创建一条VPN连接。

数据规划

表 1-29 数据规划

部件	参数项	阿里云规划示例	华为云规划示例
VPC	子网	172.16.0.0/24	192.168.0.0/24
VPN网关	网关IP	1.1.1.1	• 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
	互联子网	-	192.168.2.0/24
	BGP ASN	65515	64512
VPN连接	隧道接口地址	• tunnel1：169.254.70.1/30 • tunnel2：169.254.71.1/30	• tunnel1：169.254.70.2/30 • tunnel2：169.254.71.2/30
	IKE策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group14 • 版本：v2 • 本端标识：IP Address • 对端标识：IP Address	

部件	参数项	阿里云规划示例	华为云规划示例
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH Group14	

1.2.2.2 华为云控制台操作步骤

前提条件

云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“站点入云VPN网关”的页签后，再单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”。

   VPN网关参数说明如表1-30所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-30 VPN 网关关键参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和用户数据中心的VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	华为云VPC需要与用户数据中心VPC互通的子网。	192.168.0.0/24
BGP ASN	BGP自治系统号码。	64512
HA模式	选择VPN网关的工作模式。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

   对端网关参数说明如表1-31所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-31 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-ali
标识	– IP Address：使用对端网关的网关IP作为IP Address。 – FQDN：全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 如果对端网关无固定IP，请选择FQDN类型标识。 **说明** 请确认对端网关的ACL规则已经放通UDP端口4500。	IP Address 1.1.1.1
BGP ASN	请输入用户数据中心或私有网络的ASN。 用户数据中心的BGP ASN与VPN网关的BGP ASN不能相同。	65515

步骤5 配置VPN连接。

本场景下，阿里云VPN网关仅支持单IP地址方案，华为云VPN网关的主备EIP分别和该IP地址创建一条VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 根据界面提示配置参数。

   VPN连接参数说明如表1-32所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-32 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-ali

参数	说明	取值参数
连接模式	选择“BGP路由模式”。	BGP路由模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	172.16.0.0/24
接口分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.70.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.1/30
预共享密钥、确认密钥	和防火墙连接的预共享密钥需要保持一致。	*请根据实际设置*

参数	说明	取值参数
策略配置	和防火墙的策略配置需要保持一致。	– IKE策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ DH算法：Group 14 ■ 版本：v2 ■ 生命周期（秒）：86400 ■ 本端标识：IP Address ■ 对端标识：IP Address – IPsec策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ PFS：DH Group 14 ■ 传输协议：ESP ■ 生命周期（秒）：3600

3. 创建第二条VPN连接。

   说明

   此处仅对和第一条VPN连接配置不同的参数进行说明，未提及参数建议和第一条VPN连接保持一致。

表 1-33 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2

参数	说明	取值参数
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.1/30

----结束

1.2.2.3 阿里云控制台操作步骤

前提条件

阿里云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录阿里云控制台。

步骤2 选择“产品与服务 > 网络和CDN > 混合云网络 > VPN网关”。

步骤3 配置VPN网关。

1. 选择“VPN > VPN网关”，单击“创建VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如**表1-34**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-34 VPN 网关关键参数说明

参数	说明	取值参数
实例名称	VPN网关的名称。	vpngw-ali
地域	不同区域的资源之间网络不互通。 选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。	华北2（北京）
VPC	选择VPC信息。	vpc-ali
带宽规格	VPN转发带宽规格。	5Mbps
IPsec-VPN	-	开启
SSL-VPN	-	关闭
计费周期	VPN网关的购买时长。	1个月

步骤4 配置用户网关。

1. 选择“VPN > 用户网关”，单击“创建用户网关”。
2. 根据界面提示配置参数。

   对端网关参数说明如表1-35所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

   表 1-35 对端网关参数说明

参数	说明	取值参数
名称	华为VPN网关的名称。	cgw-hw01
IP地址	华为云VPN网关和阿里云VPN网关主EIP通信的IP地址。	1.1.1.2
自治系统号	BGP自治系统号码。 需要和表1-34配置的BGP ASN保持一致。	64512

3. 参见步骤2，配置华为云VPN网关备EIP对应的用户网关。

步骤5 配置VPN连接。

1. 选择“VPN > IPsec连接”，单击“创建IPsec连接”。
2. 根据界面提示配置参数。

   VPN连接参数说明如表1-36所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

   表 1-36 VPN 连接参数说明

模块	参数	说明	取值参数
-	名称	VPN连接的名称。	vpn-ali
	绑定资源	选择VPN网关	VPN网关
	VPN网关	选择阿里云VPN网关。	vpngw-ali
	用户网关	选择华为云VPN网关。	cgw-hw01
	路由模式	选择目的路由模式	目的路由模式
	立即生效	-	是
	预共享密钥	需要和华为云VPN连接设置的预共享密钥保持一致。	*请根据实际设置*
	高级配置	-	开启

模块	参数	说明	取值参数
IKE配置	版本	IKE配置需要和华为云VPN连接**IKE策略**配置保持一致。	- 版本：ikev2 - 协商模式：main - 加密算法：AES-128 - 认证算法：SHA2-256 - DH分组：Group 14 - SA生存周期：86400 - LocalId：1.1.1.1 - RomoteId：1.1.1.2
	协商模式		
	加密算法		
	认证算法		
	DH分组		
	SA生存周期		
	LocalId		
	RomoteId		
IPsec配置	加密算法	IPsec配置需要和华为云VPN连接**IPsec策略**配置保持一致。 **说明** NAT穿越功能必须配置为开启。	- 加密算法：AES-128 - 认证算法：SHA2-256 - DH分组：Group 14 - SA生存周期：3600 - DPD：开启 - NAT穿越：开启
	认证算法		
	DH分组		
	SA生存周期		
	DPD		
	NAT穿越		
BGP配置	BGP配置	-	开启
	隧道网段	需要和**表1-32**配置的Tunnel接口网段保持一致。	169.254.70.0/30
	本端BGP地址	需要和**表1-32**配置的对端接口地址保持一致。	169.254.70.1
	本端自治系统号	需要和**表1-31**配置的BGP ASN保持一致。	65515

模块	参数	说明	取值参数
健康检查	健康检查	-	– 健康检查：打开 – 目标IP：192.168.0.10 – 源IP：172.16.0.10 – 重试间隔：3 – 重试次数：3
	目标IP	华为云VPC子网内服务器的私网地址。 此处取值仅作示例，请以实际为准。	
	源IP	阿里云VPC子网内服务器的私网地址。 此处取值仅作示例，请以实际为准。	
	重试间隔	-	
	重试次数	-	

3. 参见上述步骤，配置华为云VPN网关备EIP对应用户网关（cgw-hw02）的VPN连接。

步骤6 配置路由信息。

BGP路由无法自动发布到VPC，需要配置一条到VPN网关的静态路由。

1. 选择“路由表”。
2. 单击路由表名称，在“路由条目列表 > 自定义路由条目”页签下，单击“添加路由条目”。
3. 根据界面提示配置参数。

表 1-37 路由表参数说明

参数	说明	取值参数
目标网段	华为云VPN网关的本端子网。 如果存在多个本端子网，则创建多条路由。	192.168.0.0/24
下一跳类型	选择“VPN网关”。	VPN网关
下一跳	选择阿里云VPN网关。	vpn-ali/xxxxxxxxx
发布到VPC	-	是

----结束

1.2.2.4 结果验证

- 大约5分钟后，查看VPN连接状态。

  - 华为云

    选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
  - 阿里云

    选择“VPN > IPsec连接”，两条VPN连接状态显示为第二阶段协商成功；由于阿里云VPN连接使用主备模式方案，故健康检查状态显示为主连接正常，备连接异常。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

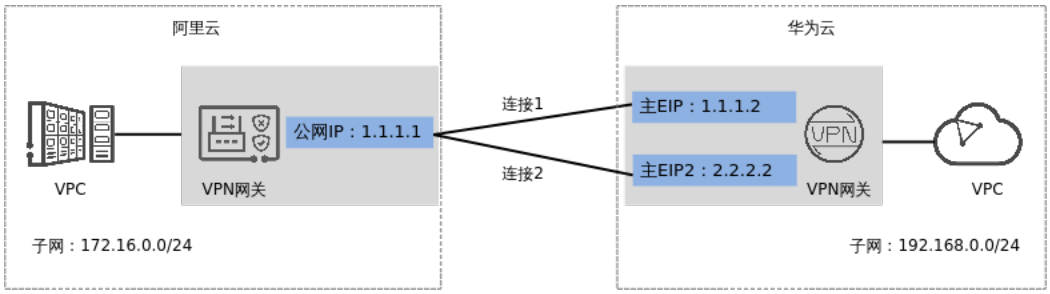
1.2.3 策略模式

1.2.3.1 操作指引

场景介绍

华为云VPN网关通过策略模式对接阿里云的典型组网如图 典型组网所示。

图 1-17 典型组网



本场景下，阿里云VPN网关仅支持单IP地址方案，华为云VPN网关的主EIP、主EIP2分别和该IP地址创建一条VPN连接。

数据规划

表 1-38 数据规划

部件	参数项	阿里云规划示例	华为云规划示例
VPC	子网	172.16.0.0/24	192.168.0.0/24
VPN网关	网关IP	1.1.1.1	• 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
	互联子网	-	192.168.2.0/24

部件	参数项	阿里云规划示例	华为云规划示例
VPN连接	IKE策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group14 • 版本：v2 • 本端标识：IP Address • 对端标识：IP Address	
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH Group14	

1.2.3.2 华为云控制台操作步骤

前提条件

云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“站点入云VPN网关”的页签后，再单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”。

   VPN网关参数说明如**表1-39**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-39 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和用户数据中心的VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24

参数	说明	取值参数
本端子网	华为云VPC需要与用户数据中心VPC互通的子网。	192.168.0.0/24
BGP ASN	BGP自治系统号码。	64512
HA模式	选择VPN网关的工作模式。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

   对端网关参数说明如**表1-40**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-40 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-ali
标识	– IP Address：使用对端网关的网关IP作为IP Address。 – FQDN：全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 如果对端网关无固定IP，请选择FQDN类型标识。 **说明** 请确认对端网关的ACL规则已经放通UDP端口4500。	IP Address 1.1.1.1

步骤5 配置VPN连接。

本场景下，阿里云VPN网关仅支持单IP地址方案，华为云VPN网关的主备EIP分别和该IP地址创建一条VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 根据界面提示配置参数。

   VPN连接参数说明如**表1-41**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-41 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-ali
连接模式	选择“策略模式”。	策略模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	172.16.0.0/24
预共享密钥、确认密钥	和对端网关连接的预共享密钥需要保持一致。	*请根据实际设置*
策略规则	用于定义本端子网到对端子网之间具体进入VPN连接加密隧道的数据流信息，由源网段与目的网段来定义。 – 源网段 源网段必须包含部分本端子网。其中，0.0.0.0/0表示任意地址。 – 目的网段 目的网段必须完全包含对端子网。	– 源网段：192.168.0.0/24 – 目的网段：172.16.0.0/24

参数	说明	取值参数
策略配置	和防火墙的策略配置需要保持一致。	– IKE策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ DH算法：Group 14 ■ 版本：v2 ■ 生命周期（秒）：86400 ■ 本端标识：IP Address ■ 对端标识：IP Address – IPsec策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ PFS：DH Group 14 ■ 传输协议：ESP ■ 生命周期（秒）：3600

3. 配置第二条VPN连接参数。

   说明

   此处仅对和第一条VPN连接配置不同的参数进行说明，未提及参数建议和第一条VPN连接保持一致。

   表 1-42 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2

----结束

1.2.3.3 阿里云控制台操作步骤

前提条件

阿里云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录阿里云控制台。

步骤2 选择“产品与服务 > 网络和CDN > 混合云网络 > VPN网关”。

步骤3 配置VPN网关。

1. 选择“VPN > VPN网关”，单击“创建VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如表1-43所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

   表 1-43 VPN 网关参数说明

参数	说明	取值参数
实例名称	VPN网关的名称。	vpngw-ali
VPC	选择VPC信息。	vpc-ali
带宽规格	VPN转发带宽规格。	5Mbps
IPsec-VPN	-	开启
SSL-VPN	-	关闭
计费周期	VPN网关的购买时长。	1个月

步骤4 配置用户网关。

1. 选择“VPN > 用户网关”，单击“创建用户网关”。
2. 根据界面提示配置参数。

   对端网关参数说明如表1-44所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

   表 1-44 对端网关参数说明

参数	说明	取值参数
名称	华为VPN网关的名称。	cgw-hw01
IP地址	华为云VPN网关的主EIP。	1.1.1.2

3. 参见步骤2，配置华为云VPN网关备EIP对应的用户网关。

步骤5 配置VPN连接。

1. 选择“VPN > IPsec连接”，单击“创建IPsec连接”。
2. 根据界面提示配置参数。

   VPN连接参数说明如表1-45所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-45 VPN 连接参数说明

模块	参数	说明	取值参数
-	名称	VPN连接的名称。	vpn-ali
	VPN网关	选择阿里云VPN网关。	vpngw-ali
	用户网关	选择华为云VPN网关。	cgw-hw01
	本端网段	阿里云VPC的子网。	172.16.0.0/24
	对端网段	华为云VPC的子网。 **说明** 本端网段或对端网段存在多个网段场景下，需要基于每一个本端网段到每一个对端网段创建一条VPN连接，共需要创建VPN连接数为（本端网段数量 * 对端网段数量）。 例如，本端网段存在2个网段，对端网段存在3个网段，则需要在阿里云上创建2*3个VPN连接。	192.168.0.0/24
	立即生效	-	是
	预共享密钥	需要和表1-41设置的预共享密钥保持一致。	*请根据实际设置*
	高级配置	-	打开
IKE配置	版本	需要和表1-41配置的IKE策略保持一致。	– 版本：ikev2 – 协商模式：main – 加密算法：AES-128 – 认证算法：SHA2-256 – DH分组：Group 14 – SA生存周期：86400 – LocalId：1.1.1.1 – RomoteId：1.1.1.2
	协商模式		
	加密算法		
	认证算法		
	DH分组		
	SA生存周期		
	LocalId		

模块	参数	说明	取值参数
	Romote Id		
IPsec配置	加密算法	需要和表1-41配置的IPsec策略保持一致。	– 加密算法：AES-128 – 认证算法：SHA2-256 – DH分组：Group 14 – SA生存周期：3600
	认证算法		
	DH分组		
	SA生存周期		
健康检查	健康检查	-	– 健康检查：打开 – 目标IP：192.168.0.10 – 源IP：172.16.0.10 – 重试间隔：3 – 重试次数：3
	目标IP	华为云VPC子网内服务器的私网地址。 此处取值仅作示例，请以实际为准。	
	源IP	阿里云VPC子网内服务器的私网地址。 此处取值仅作示例，请以实际为准。	
	重试间隔	-	
	重试次数	-	

3. 参见上述步骤，配置华为云VPN网关备EIP对应用户网关（cgw-hw02）的VPN连接。

步骤6 配置路由信息。

需要在阿里云上增加到华为云VPC子网的路由信息。

1. 选择“VPN > VPN网关”。
2. 单击VPN网关名称，在“目的路由表”页签下，单击“添加路由条目”。
3. 根据界面提示配置参数。
   – 配置到主EIP的路由信息，如表1-46所示。

表 1-46 到主 EIP 的路由表参数说明

参数	说明	取值参数
目标网段	华为云VPN网关的本端子网。 如果存在多个本端子网，则创建多条路由。	192.168.0.0/24

参数	说明	取值参数
下一跳类型	选择“IPsec连接”。	IPsec连接
下一跳	选择阿里云VPN网关。	vpn-ali/xxxxxxxxx
发布到VPC	-	是
权重	-	100

- 配置到备EIP的路由信息，如表1-47所示。

  表 1-47 到备 EIP 的路由表参数说明

参数	说明	取值参数
目标网段	华为云VPN网关的本端子网。 如果存在多个本端子网，则创建多条路由。	192.168.0.0/24
下一跳类型	选择“IPsec连接”。	IPsec连接
下一跳	选择阿里云VPN网关。	vpn-ali/xxxxxxxxx
发布到VPC	-	是
权重	-	0

----结束

1.2.3.4 结果验证

- 大约5分钟后，查看VPN连接状态。
  - 华为云

    选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
  - 阿里云

    选择“VPN > IPsec连接”，两条VPN连接状态显示为第二阶段协商成功；由于阿里云VPN连接使用主备模式方案，故健康检查状态显示为主连接正常，备连接异常。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

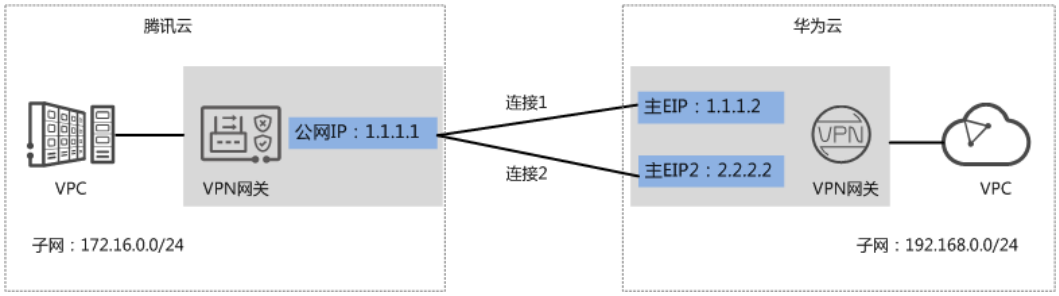
1.3 对接腾讯云

1.3.1 静态路由模式

1.3.1.1 场景介绍

华为云VPN网关通过静态路由模式对接腾讯云的典型组网如图1-18所示。

图 1-18 典型组网



本场景下，腾讯云VPN网关仅支持单IP地址方案，华为云VPN网关推荐采用双活模式，主EIP、主EIP2分别和该IP地址创建一条VPN连接。

1.3.1.2 数据规划

表 1-48 数据规划

部件	参数项	腾讯云规划示例	华为云规划示例
VPC	子网	172.16.0.0/24	192.168.0.0/24
VPN网关	网关IP	1.1.1.1	• 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
	互联子网	-	192.168.2.0/24
VPN连接	隧道接口地址	• tunnel1：169.254.70.1/30 • tunnel2：169.254.71.1/30	• tunnel1：169.254.70.2/30 • tunnel2：169.254.71.2/30
	IKE策略	• 版本：v2 • 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group14 • 本端标识：IP Address • 对端标识：IP Address	
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH group14 • DPD：45秒 华为云DPD默认为45秒，不支持配置。	

1.3.1.3 华为云控制台操作步骤

前提条件

云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“站点入云VPN网关”的页签后，再单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”。

   VPN网关参数说明如表1-49所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-49 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和用户数据中心的VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	华为云VPC需要与用户数据中心VPC互通的子网。	192.168.0.0/24
BGP ASN	BGP自治系统号码。	64512
HA模式	选择VPN网关的工作模式。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

   对端网关参数说明如表1-50所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-50 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-tx
标识	– IP Address：使用对端网关的网关IP作为IP Address。 – FQDN：全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 如果对端网关无固定IP，请选择FQDN类型标识。 **说明** 请确认对端网关的ACL规则已经放通UDP端口4500。	IP Address 1.1.1.1

步骤5 配置VPN连接。

本场景下，对端网关仅支持单IP地址方案，华为云VPN网关推荐使用双活模式，主EIP、主EIP2分别和该IP地址创建一条VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 根据界面提示配置参数。

   VPN连接参数说明如表1-51所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-51 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-tx
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	172.16.0.0/24

参数	说明	取值参数
接口分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.70.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.1/30
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关连接的预共享密钥需要保持一致。	*请根据实际设置*
策略配置	和防火墙的策略配置需要保持一致。	– IKE策略 ■ 版本：v2 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ DH算法：Group 14 ■ 生命周期（秒）：86400 ■ 本端标识：IP Address ■ 对端标识：IP Address – IPsec策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ PFS：DH Group 14 ■ 传输协议：ESP ■ 生命周期（秒）：3600

a. 创建第二条VPN连接参数。

说明

此处仅对和第一条VPN连接配置不同的参数进行说明，未提及参数建议和第一条VPN连接保持一致。

表 1-52 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.1/30

----结束

1.3.1.4 腾讯云控制台操作步骤

前提条件

腾讯云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录腾讯云控制台。

步骤2 选择“云产品 > 混合云网络 > VPN连接”。

步骤3 配置VPN网关。

1. 选择“VPN连接 > VPN网关”，单击“新建”。
2. 根据界面提示配置参数，单击“创建”。

   VPN网关参数说明如表1-53所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-53 VPN 网关参数说明

参数	说明	取值参数
网关名称	VPN网关的名称。	vpngw-tx
协议类型	选择“IPsec”。	IPsec
网络类型	选择“私有网络”。	私有网络

参数	说明	取值参数
所属网络	选择腾讯云需要和华为云VPC通信的VPC。	vpc-tx(172.16.0.0/16)

步骤4 配置对端网关。即华为云VPN网关信息。

1. 选择“VPN连接 > 对端网关”，单击“新建”。
2. 根据界面提示配置参数，单击“确定”。

   对端网关参数说明如**表1-54**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-54 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	hwvpn-01
网关IP	华为云VPN网关的主EIP。	1.1.1.2

3. 参见上述步骤，创建华为云VPN网关主EIP2（2.2.2.2）对应的网关信息（hwvpn-02）。

步骤5 配置VPN连接。

1. 选择“VPN连接 > VPN通道”，单击“新建”。
2. 根据界面提示配置参数，单击“创建”。

   VPN连接参数说明如**表1-55**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-55 VPN 连接参数说明

模块	参数	说明	取值参数
基本配置	VPN通道名称	VPN连接的名称。	vpn-tx
	VPN网关类型	选择“私有网络”。	私有网络
	私有网络	选择需要和华为云VPC通信的VPC。	vpc-tx(172.16.0.0/16)
	VPN网关	选择**步骤3**中创建的VPN网关。	vpngw-tx
	对端网关	选择“选择已有”，然后选择**步骤4**中创建的对端网关。	hwvpn-01
	预共享密钥	需要和华为云VPN连接设置的预共享密钥保持一致。	*请根据实际设置*
	协商类型	选择“主动协商”。	主动协商

模块	参数	说明	取值参数
通信模式	-	选择“目的路由”。	目的路由
高级配置	DPD	华为云DPD默认为45秒，不支持配置。	45
	健康检测	本地地址和对端地址与华为云连接的Tunnel地址对应。 **说明** 健康检查必须配置，否则腾讯云连接故障后流量无法切换。	健康
IKE配置（选填）	版本	IKE配置需要和**表1-51**配置的IKE策略保持一致。	- 版本：IKEV2 - 加密算法：AES-128 - 认证算法：SHA2-256 - 本端标识：IP Address - 对端标识：IP Address（1.1.1.2） - DH group：DH14 - IKE SA Lifetime：86400
	加密算法		
	认证算法		
	本端标识		
	远端标识		
	DH group		
	IKE SA Lifetime		
IPsec配置（选填）	加密算法	IPsec配置需要和**表1-51**配置的IPsec策略保持一致。	- 加密算法：AES-128 - 认证算法：SHA2-256 - 报文封装模式：Tunnel - 安全协议：ESP - PFS：DH-GROUP14 - IPsec sa Lifetime：3600 s - IPsec sa Lifetime：1843200 KB
	认证算法		
	PFS		
	IPsec sa Lifetime		

3. 参见上述步骤，创建腾讯云VPN网关与华为云VPN网关主EIP2（hwvpn-002）的VPN连接。

步骤6 在VPC路由表中增加路由信息。

1. 选择“云产品 > 云上网络 > 私有网络 > 路由表 > 路由表”，单击“新建”。
2. 根据界面提示配置参数，单击“创建”。

路由表参数说明如表1-56所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-56 路由表参数说明

参数	说明	取值参数
名称	路由表名称。	route-hw
所属网络	选择需要和华为云VPC通信的VPC。	vpc-tx(172.16.0.0/16)
目的端	华为云VPC的子网信息。 如果华为云VPC子网信息存在多条，则需要添加多条路由策略。	192.168.0.0/24
下一跳类型	选择“VPN网关”。	VPN网关
下一跳	选择VPN网关。	vpngw-tx

步骤7 在VPN网关路由表中增加路由信息。

1. 选择“云产品 > 混合云网络 > VPN连接 > VPN网关 > 详情 > 路由表”，单击“新增路由策略”。
2. 根据界面提示配置参数，单击“创建”。

   路由表参数说明如表1-57所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

   表 1-57 路由表参数说明

参数	说明	取值参数
目的端	华为云VPC的子网信息。 如果华为云VPC子网信息存在多条，则需要添加多条路由策略。	192.168.0.0/24
下一跳	选择第一条VPN连接。	vpn-tx
路由类型	选择“静态路由”。	静态路由
权重	多条VPN连接的优先级关系。值越小，优先级越高。	0

3. 参考上述步骤，配置第二条VPN连接对应的路由信息。

   说明

   建议两条VPN连接对应的路由信息权重值设置相同。

----结束

1.3.1.5 结果验证

- 大约5分钟后，查看VPN连接状态。

- 华为云

  选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
- 腾讯云

  选择“VPN连接 > VPN通道”，两条VPN连接状态显示为已联通，检查健康状态显示为“健康”。

- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

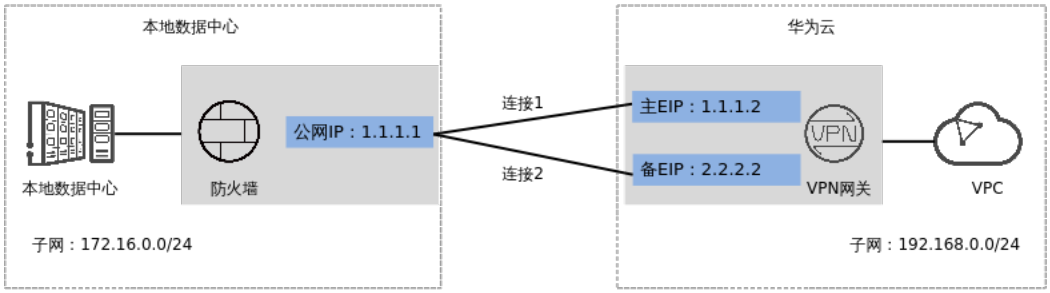
1.4 对接华为 USG 防火墙

1.4.1 静态路由模式

1.4.1.1 场景介绍

华为云VPN网关通过静态路由模式对接华为防火墙的典型组网如图1-19所示。

图 1-19 典型组网



本场景下以防火墙单IP地址方案为例，华为云VPN网关的主EIP、备EIP分别和该IP地址创建一条VPN连接。

1.4.1.2 数据规划

表 1-58 数据规划

部件	参数项	华为USG防火墙规划示例	华为云规划示例
VPC	子网	172.16.0.0/24	192.168.0.0/24
VPN网关	网关IP	1.1.1.1	• 主EIP：1.1.1.2 • 备EIP：2.2.2.2
	互联子网	-	192.168.2.0/24
VPN连接	隧道接口地址	• tunnel1：169.254.70.1/30 • tunnel2：169.254.71.1/30	• tunnel1：169.254.70.2/30 • tunnel2：169.254.71.2/30

部件	参数项	华为USG防火墙规划示例	华为云规划示例
	IKE策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group 15 • 版本：v2 • 生命周期（秒）：86400 • 本端标识：IP Address • 对端标识：IP Address	
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH Group 15 • DPD：45秒 华为云DPD默认为45秒，不支持配置。 • 生命周期（秒）：3600	

1.4.1.3 华为云控制台操作步骤

前提条件

云上VPC及其子网已经创建完成。

操作步骤

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“站点入云VPN网关”的页签后，再单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”。

   VPN网关参数说明如**表 VPN网关参数说明**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-59 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)

参数	说明	取值参数
互联子网	用于VPN网关和用户数据中心的VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	华为云VPC需要与用户数据中心VPC互通的子网。	192.168.0.0/24
BGP ASN	BGP自治系统号码。	64512
HA模式	选择VPN网关的工作模式。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
备EIP	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

   对端网关参数说明如**表 对端网关参数说明**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-60 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw
标识	– IP Address：使用对端网关的网关IP作为IP Address。 – FQDN：全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 如果对端网关无固定IP，请选择FQDN类型标识。 **说明** 请确认对端网关的ACL规则已经放通UDP端口4500。	IP Address 1.1.1.1

步骤5 配置VPN连接。

本场景下以防火墙单IP地址方案为例，华为云VPN网关的主EIP、备EIP分别和该IP地址创建一条VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 根据界面提示配置参数。

   VPN连接参数说明如**表 VPN连接参数说明**所示。 此处仅对关键参数进行说明，非关键参数请保持默认。

表 1-61 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-fw
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	172.16.0.0/24
接口分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.70.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.1/30
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。 VPN网关会自动对对端接口地址进行NQA探测，要求对端接口地址在对端网关上已配置。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关连接的预共享密钥需要保持一致。	*请根据实际设置*

参数	说明	取值参数
策略配置	和防火墙的策略配置需要保持一致。	– IKE策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ DH算法：Group 15 ■ 版本：v2 ■ 生命周期（秒）：86400 ■ 本端标识：IP Address ■ 对端标识：IP Address – IPsec策略 ■ 认证算法：SHA2-256 ■ 加密算法：AES-128 ■ PFS：DH Group 15 ■ 传输协议：ESP ■ 生命周期（秒）：3600

3. 创建第二条VPN连接参数。

   说明

   此处仅对和第一条VPN连接配置不同的参数进行说明，未提及参数建议和第一条VPN连接保持一致。

   表 1-62 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的备EIP。	2.2.2.2

参数	说明	取值参数
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.1/30

----结束

1.4.1.4 防火墙侧操作步骤

操作步骤

1. 登录防火墙设备的命令行配置界面。

   不同防火墙型号及版本命令可能存在差异，配置时请以对应版本的产品文档为准。

2. 配置基本信息。

   a. 配置防火墙接口的IP地址。

   ```
   interface GigabitEthernet1/0/1                //配置防火墙的公网IP地址。
   ip address 1.1.1.1 255.255.255.0
   interface GigabitEthernet1/0/2                //配置防火墙的私网IP地址。
   ip address 172.16.0.233 255.255.255.0
   ```

   b. 将接口划入对应zone。

   ```
   firewall zone untrust
   add interface GigabitEthernet1/0/1
   firewall zone trust
   add interface GigabitEthernet1/0/2
   ```

   c. 配置TCP MSS大小。

   ```
   firewall tcp-mss 1300
   ```

3. 配置协商策略。

   ```
   ike proposal /100/                    //配置防火墙公网IP地址和VPN网关主EIP的IKE策略相关配置
   authentication-algorithm SHA2-256          //请和表1-61配置的IKE策略认证算法保持一致
   encryption-algorithm AES-128               //请和表1-61配置的IKE策略加密算法保持一致
   authentication-method pre-share
   integrity-algorithm HMAC-SHA2-256
   prf HMAC-SHA2-256
   dh group15                             //请和表1-61配置的IKE策略DH算法保持一致
   sa duration 86400                        //请和表1-61配置的IKE策略生命周期保持一致

   ike peer /hwcloud_peer33/
   undo version 1                         //请和表1-61配置的IKE策略IKE版本保持一致
   pre-shared-key XXXXXXX                       //请和表1-61配置的预共享密钥保持一致
   ike-proposal /100/
   remote-address 1.1.1.2                   //请和VPN网关的主EIP保持一致

   IPsec proposal /IPsec-pro100/              //配置防火墙公网IP地址和VPN网关主EIP的IPsec策略相关配置
   transform esp
   encapsulation-mode tunnel
   esp authentication-algorithm SHA2-256     //请和表1-61配置的IPsec策略认证算法保持一致
   esp encryption-algorithm aes-128          //请和表1-61配置的IPsec策略加密算法保持一致

   ike proposal /200/                     //配置防火墙公网IP地址和VPN网关备EIP的相关配置，配置规则同上
   authentication-algorithm SHA2-256
   encryption-algorithm AES-128
   authentication-method pre-share
   integrity-algorithm HMAC-SHA2-256
   prf HMAC-SHA2-256
   ```



```
dh group15
sa duration 86400

ike peer /hwcloud_peer44/
undo version 1
pre-shared-key XXXXXXX
ike-proposal /200/
remote-address 2.2.2.2                    //请和VPN网关的备EIP保持一致

IPsec proposal /IPsec-pro200/
transform esp
encapsulation-mode tunnel
esp authentication-algorithm SHA2-256
esp encryption-algorithm aes-128
```

4. 配置隧道连接。

```
IPsec profile /HW-IPsec100/               //配置防火墙公网IP地址对应的路由策略
ike-peer hwcloud_peer33/
proposal /IPsec-pro100/                     //配置防火墙公网IP地址的路由模式隧道接口
pfs dh-group15                             //请和表1-61配置的IPsec策略PFS保持一致
sa duration time-based 3600                  //请和表1-61配置的IPsec策略生命周期保持一致

interface /Tunnel100/
ip address 169.254.70.1 255.255.255.252       //配置为防火墙的隧道接口1 IP地址
tunnel-protocol IPsec
source 1.1.1.1                            //配置为防火墙的公网IP地址
destination 1.1.1.2                         //配置为VPN网关的主EIP
service-manage ping permit
IPsec profile /HW-IPsec100/
firewall zone untrust
add interface /Tunnel100/

interface /Tunnel200/
ip address 169.254.71.1 255.255.255.252     //配置为防火墙的隧道接口2 IP地址
tunnel-protocol IPsec
source 1.1.1.1                           //配置为防火墙的公网IP地址
destination 2.2.2.2                        //配置为VPN网关的备EIP
service-manage ping permit
IPsec profile /HW-IPsec200/
firewall zone untrust
add interface /Tunnel200/
```

5. 配置路由信息。

   a. 配置华为云公网IP的静态路由。

```
ip route-static 1.1.1.2 255.255.255.255 1.1.1.1    //VPN网关主EIP+空格+255.255.255.255+空格+防火墙公网IP的网关地址
ip route-static 2.2.2.2 255.255.255.255 1.1.1.1    //VPN网关备EIP+空格+255.255.255.255+空格+防火墙公网IP的网关地址
```

   b. 配置私网静态路由。

```
ip route-static 192.168.0.0 255.255.255.0 /Tunnel100/ 1.1.1.2

ip route-static 192.168.0.0 255.255.255.0 /Tunnel200/ 2.2.2.2
```

   说明

   - 格式为ip route-static VPC子网1+空格+子网掩码+空格+/Tunnel100/+VPN主EIP。

     其中，Tunnel100需要和**配置隧道连接**配置的编号保持一致，且对应隧道编号中destination的值需要和配置的EIP保持一致。
   - 如果存在多个VPC子网，则每个EIP均需要配置多条路由。

6. 配置安全策略。

```
ip address-set /localsubnet172/ type object       //定义地址对象
address 0 172.16.0.0 mask 24                    //配置用户数据中心的子网信息
ip address-set /HWCsubnet192/ type object
address 0 192.168.0.0 mask 24                    //配置华为云VPC的子网信息
```



```
security-policy
rule name IPsec_permit1
source-zone untrust
source-zone internet
source-zone local
destination-zone untrust
destination-zone internet
destination-zone local
service ah esp
service protocol udp destination-port 500 4500
action permit
rule name /IPsec_permit2/
source-zone untrust
source-zone internet
source-zone trust
destination-zone untrust
destination-zone internet
destination-zone trust
source-address address-set /localsubnet172/
source-address address-set /HWCsubnet192/
destination-address address-set /localsubnet172/
destination-address address-set /HWCsubnet192/
action permit

nat-policy
rule name IPsec_subnet_bypass
source-zone trust
destination-zone untrust
destination-zone internet
source-address address-set /localsubnet172/
destination-address address-set /HWCsubnet192/
action no-nat
```

1.4.1.5 结果验证

- 大约5分钟后，查看VPN连接状态。
  - 华为云

    选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
  - USG防火墙

    选择“网络 > IPSec > IPSec”，单击策略名称，在IPSec策略监控列表中两条VPN连接状态显示为“IKE协商成功”、“IPSec协商成功”。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

2 站点入云 VPN 经典版

2.1 简介

欢迎使用虚拟专用网络（VPN）管理员指南，该指南可以帮助您配置本地的VPN设备，实现您本地网络与华为云VPC子网的互联互通。

VPN连接将您的数据中心或（或网络）连接到您的VPC，对端网关指用户端使用的定位标记，它可以是物理或软件设备。详细配置示例请参见：

- **示例：HUAWEI USG6600配置**
- **示例：Fortinet飞塔防火墙VPN配置**
- **示例：深信服防火墙配置**
- **示例：使用TheGreenBow IPsec VPN Client配置云上云下互通**
- **示例：使用OpenSwan配置云上云下互通**
- **示例：使用StrongSwan配置云上云下互通**
- **示例：Web配置华为USG防火墙**

2.2 示例：HUAWEI USG6600 配置

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

假设数据中心的子网为192.168.3.0/24和192.168.4.0/24，VPC下的子网为192.168.1.0/24和192.168.2.0/24，VPC上IPsec隧道的出口公网IP为1.1.1.1（从VPC上IPsec VPN的本端网关参数上获取）。

配置步骤

1. 登录防火墙设备的命令行配置界面。
2. 查看防火墙版本信息。

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


3. 创建ACL并绑定到对应的vpn-instance。
```
acl number 3065 vpn-instance vpn64
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
q
```
4. 创建ike proposal。
```
ike proposal 64
dh group5
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```
5. 创建ike peer，并引用之前创建的ike proposal，其中对端IP地址是1.1.1.1。
```
ike peer vpnikepeer_64
pre-shared-key ******** （ ********为您输入的预共享密码 ）
ike-proposal 64
undo version 2
remote-address vpn-instance vpn64 1.1.1.1
sa binding vpn-instance vpn64
q
```
6. 创建IPsec协议。
```
IPsec proposal IPsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```
7. 创建IPsec策略，并引用ike policy和IPsec proposal。
```
IPsec policy vpnIPsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal IPsecpro64
local-address xx.xx.xx.xx
q
```
8. 将IPsec策略应用到相应的子接口上去。
```
interface GigabitEthernet0/0/2.64
IPsec policy vpnIPsec64
q
```
9. 测试连通性。

   在上述配置完成后，我们可以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，如下图所示：


```
root@i-psiybqhh:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:7c:ba:bf:cc
          inet addr:192.168.3.2  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:7cff:feba:bfcc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2304 (2.3 KB)  TX bytes:3404 (3.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1296 (1.2 KB)  TX bytes:1296 (1.2 KB)

root@i-psiybqhh:/home/ubuntu# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=62 time=4.55 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=62 time=1.27 ms
64 bytes from 192.168.1.2: icmp_req=3 ttl=62 time=1.25 ms
64 bytes from 192.168.1.2: icmp_req=4 ttl=62 time=0.871 ms
64 bytes from 192.168.1.2: icmp_req=5 ttl=62 time=0.886 ms
64 bytes from 192.168.1.2: icmp_req=6 ttl=62 time=0.676 ms
64 bytes from 192.168.1.2: icmp_req=7 ttl=62 time=1.06 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.676/1.510/4.554/1.258 ms
```

2.3 示例：Fortinet 飞塔防火墙 VPN 配置

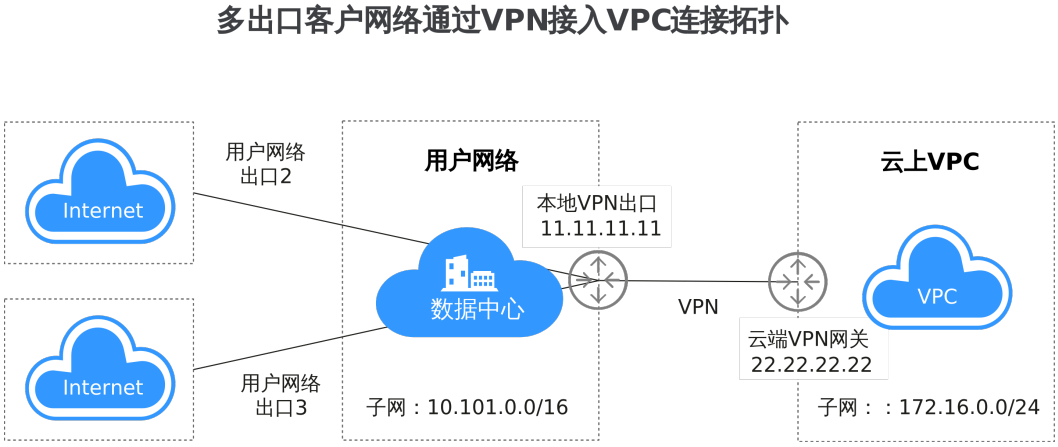
操作场景

用户数据中心的出口防火墙选用飞塔设备，用户数据中心存在多个互联网出口，用户在华为云购买VPN网关，需要创建VPN连接连通本地网络到VPC子网。

拓扑连接

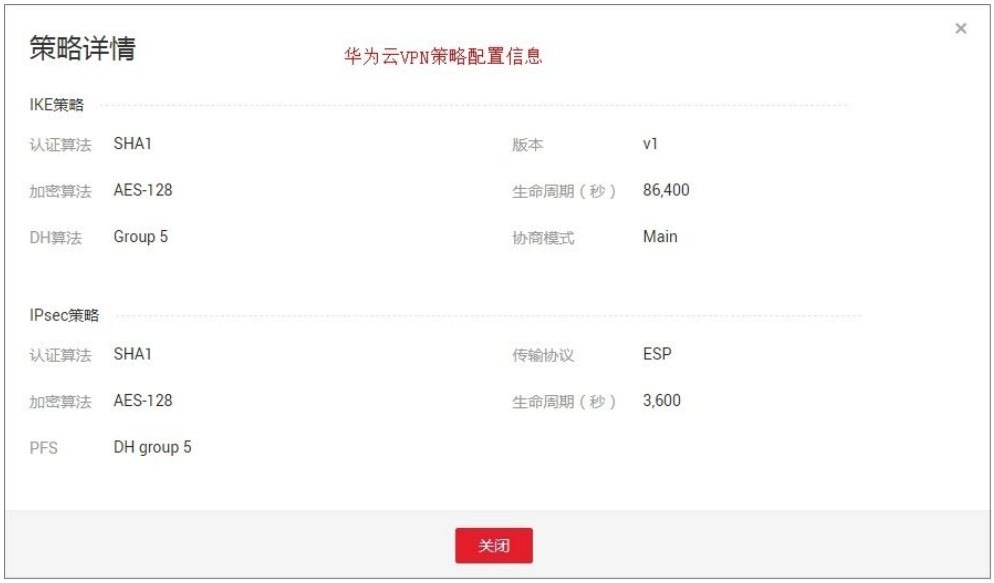
如图 多出口客户网络通过VPN接入VPC连接拓扑所示，用户数据中心存在多个互联网出口，当前指定11.11.11.11的物理接口和华为云的VPC建立VPN连接，本地子网网段为10.10.0.0/16，华为云VPC子网为172.16.0.0/24。假设您在华为云购买的VPN网关IP为22.22.22.22，现通过创建VPN连接方式来连通本地网络到VPC子网。

图 2-1 多出口客户网络通过 VPN 接入 VPC 连接拓扑



华为云端的VPN连接资源策略配置按照缺省信息配置，详见图2-2。

图 2-2 策略配置



配置步骤

本示例以华为云端VPN配置信息为基础，详细介绍用户侧飞塔防火墙设备的VPN配置。

步骤1 配置IPsec VPN

1. 创建隧道。

   选择“虚拟专网 > 隧道 ”，为隧道命名，如IPsec，选择自定义VPN隧道进行创建。

   图 2-3 创建隧道

2. 配置隧道基本信息。

   按照云端网关IP配置网关IP地址为22.22.22.22，选择接口为连接VPN的数据流出接口，即本端为11.11.11.11接口，版本选择1，mode选择主模式。

图 2-4 配置隧道基本信息

3. 配置IKE一阶段。

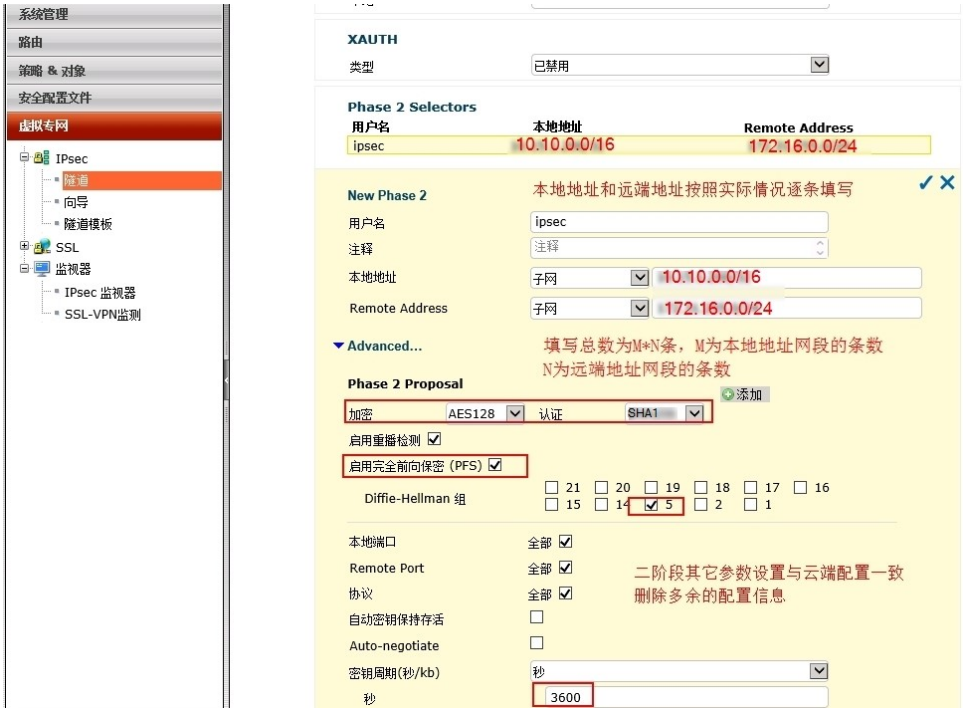
   选择一阶段的加密和认证算法与云端相同，删除多余配置信息，“Diffe-Hellman组”选择5，“XAUTH”选择禁用。

图 2-5 配置 IKE 一阶段

4. 配置IPsec二阶段

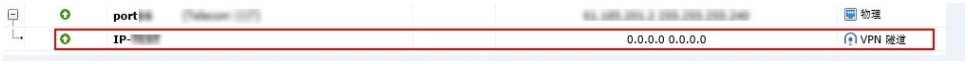
   按照实际情况配置选择本地地址（本端子网：10.10.0.0/16）和remote-address（远端子网：172.16.0.0/24），选择“√”确认，二阶段策略配置信息同样须与云端信息一致。

图 2-6 配置 IPsec 二阶段



VPN隧道创建完成后会在物理接口port下自动生成一个VPN隧道接口。

图 2-7 VPN 隧道接口



5. 完成IPsec隧道配置。

图 2-8 完成 IPsec 隧道配置

步骤2 配置路由

1. 添加静态路由。

   添加去往云端VPC子网172.16.0.0/24的子网路由，出接口为VPN隧道接口。

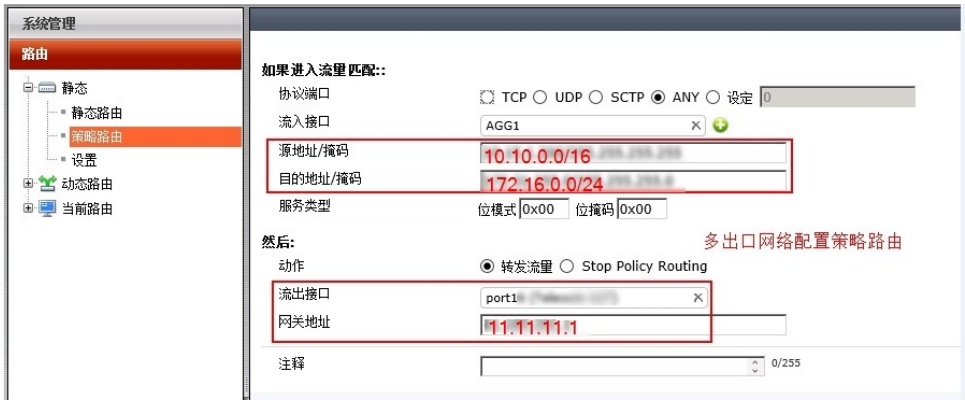
   图 2-9 添加静态路由

2. 配置多出口策略路由。

   配置源地址为本地子网，目标地址为云端VPC的子网的策略路由，请调整策略路由的配置顺序，确保该策略路由优先调用。

   图 2-10 配置多出口策略路由

步骤3 配置策略及NAT

1. 本地访问云端策略。

“流入接口”选择“trust”，“流出接口”选择创建隧道生成的接口，源地址：10.10.0.0/16，目的地址：172.16.0.0/24，“动作”选择“允许访问”，“服务”选择“all”，不启用NAT。

图 2-11 本地访问云端策略配置

2. 云端访问本地策略。

   “流入接口”选择创建隧道生成的接口，“流出接口”选择trust，源地址：172.16.0.0/24，目的地址：10.10.0.0/16，“动作”选择“允许访问”，“服务”选择“all”，不启用NAT。

图 2-12 云端访问本地策略配置

----结束

配置验证

1. 本地VPN状态正常。

   选择“虚拟专网 > 监视器 > IPsec监视器”，查看当前VPN配置状态正常。

图 2-13 查看本地 VPN 状态

2. 云端VPN状态正常。

图 2-14 查看云端 VPN 状态

命令行配置

1. 物理接口配置

```
config system interface
  edit "port1"
      set vdom "root"
      set ip 11.11.11.11 255.255.255.0
      set type physical
next
   edit "IPsec"                          //隧道接口配置信息
      set vdom "root"
      set type tunnel
      set interface "port1"              //隧道绑定的物理接口
           next
       end
```

2. 接口划分区域配置

```
config system zone
   edit "trust"
      set intrazone allow
      set interface "A1"
   next
   edit "untrust"
      set intrazone allow
      set interface "port1 "
   next
end
```

3. 地址对象配置

```
config firewall address
       edit "hw-172.16.0.0/24"
```



```
    set uuid f612b4bc-5487-51e9-e755-08456712a7a0
    set subnet 172.16.0.0 255.255.255.0          //云端地址网段
     next
  edit "local-10.10.0.0/16"
    set uuid 9f268868-5489-45e9-d409-5abc9a946c0c
    set subnet 10.10.0.0 255.255.0.0             //本地地址网段
  next
```

4. IPsec配置

```
config vpn IPsec phase1-interface                          //一阶段配置
  edit "IPsec"
    set interface "port1"
    set nattraversal disable
    set proposal aes128-sha1
    set comments "IPsec"
    set dhgrp 5
    set remote-gw 22.22.22.22
    set psksecret ENC dmFyLzF4tRrIjV3T
+lSzhQeU2nGEoYKC31NaYRWFJl8krlwNmZX5SfwUi5W5RLJqFu82VYKYsXp5+HZJ13VYY8O2Sn/
vruzdLxqu84zbHEIQkTlf5n/
63KEru1rRoNiHDTWfh3A3ep3fKJmxf43pQ7OD64t151ol06FMjUBLHgJ1ep9d32Q0F3f3oUxfDQs21Bi9RA
==
  next
end
config vpn IPsec phase2-interface                          //二阶段配置
  edit "IP-TEST"
    set phase1name "IPsec "
    set proposal aes128-sha1
    set dhgrp 5
    set keylifeseconds 3600
    set src-subnet 10.10.0.0 255.255.0.0
    set dst-subnet 172.16.0.0 255.255.255.0
  next
end
```

5. 访问策略配置

```
config firewall policy
 edit 15                                          //策略编号15，流入至内网策略，未启用NAT
    set uuid 4f452870-ddb2-51e5-35c9-38a987ebdb6c
    set srcintf "IPsec"
    set dstintf "trust"
    set srcaddr "hw-172.16.0.0/24"
    set dstaddr "local-10.10.0.0/16"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
  next
  edit 29                                        //策略编号29，流出至云端策略，未启用NAT
    set uuid c2d0ec77-5254-51e9-80dc-2813ccf51463
    set srcintf "trust"
    set dstintf "IPsec"
    set srcaddr "local-10.10.0.0/16"
    set dstaddr "hw-172.16.0.0/24"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
  next
```

6. 路由配置

```
config router static
  edit 24                            //路由编号24，访问云端静态路由
    set dst 172.16.0.0 255.255.255.0
    set gateway 11.11.11.1
    set distance 10
    set device "port1"
config router policy
edit 2                       //策略路由编号2，云下访问云端策略路由
    set input-device "A1"
    set src "10.10.00/255.255.0.0"
```



```
set dst "172.16.0.0/255.255.255.0"
set gateway 11.11.11.1
set output-device "port1"
```

2.4 示例：深信服防火墙配置

操作场景

用户数据中心的出口防火墙选用深信服设备，同时在DMZ区域旁路接入了一台IPsec VPN设备，需要通过VPN接入华为云网络。

拓扑连接

拓扑连接方式：

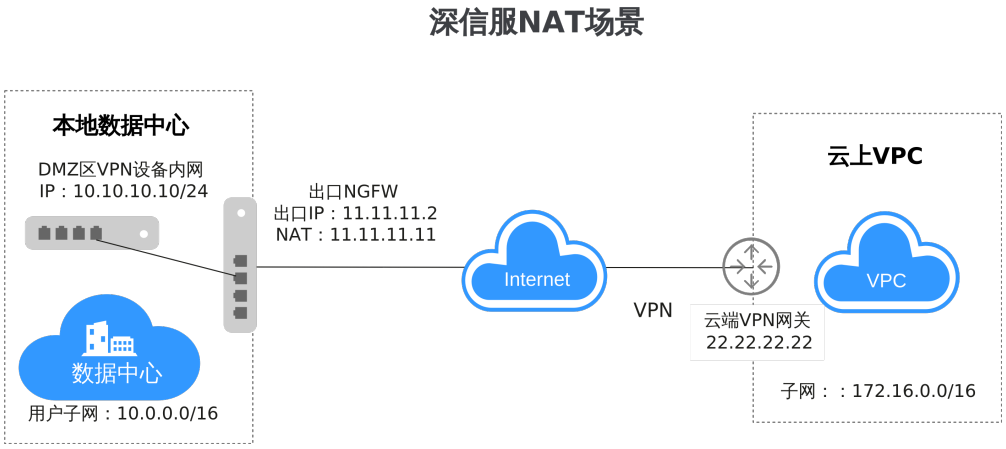
- 使用防火墙设备直接和云端建立VPN连接。
- 使用DMZ区域的专用VPN设备结合NAT穿越与云端建立VPN连接。

VPN接入方式的配置指导，相关信息说明如下：

- 用户数据中心VPN设备私网IP：10.10.10.10/24
- 用户数据中心用户子网：10.0.0.0/16
- 防火墙出口IP：11.11.11.2/24，公网网关：11.11.11.1，VPN设备的NAT IP：11.11.11.11
- 云端VPN网关IP：22.22.22.22，云端子网：172.16.0.0/16

现通过创建VPN连接方式来连通本地网络到VPC子网。

图 2-15 深信服 NAT 场景



华为云端的VPN连接资源策略配置按照图2-16所示信息配置，使用DMZ区域专用的VPN设备进行NAT穿越连接时，协商模式修改为野蛮模式；使用防火墙进行连接协商模式选择缺省。

图 2-16 华为云 VPN 策略配置

配置步骤

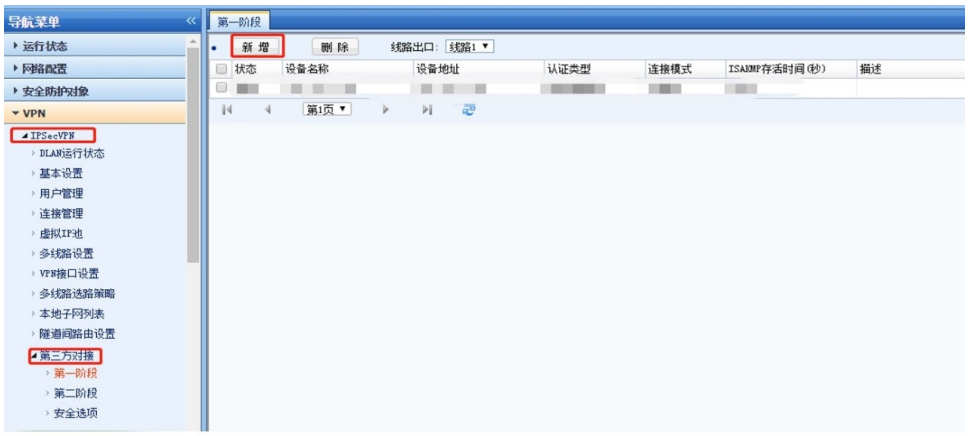
本示例以华为云端VPN配置信息为基础，详细介绍用户侧深信服设备的VPN配置。

步骤1 配置IPsec VPN

1. **IKE一阶段配置**

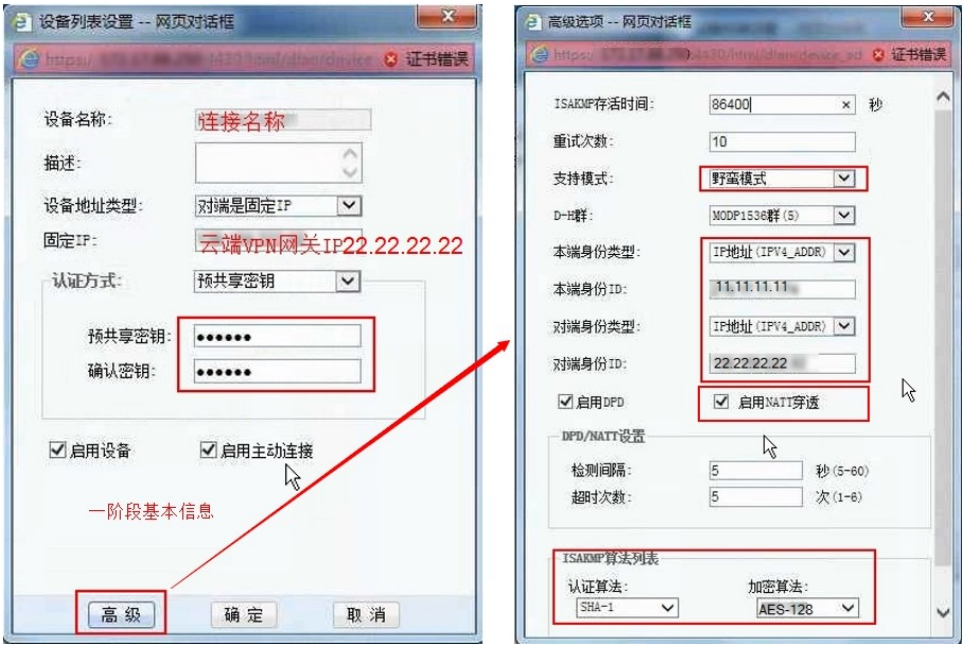
选择“VPN > IPsec VPN > 第三方对接 > 第一阶段 ”，确认线路出口（深信服设备会针对该接口自动下发VPN路由信息），单击“新增”。

图 2-17 IKE 一阶段配置



在弹窗界面配置一阶段基本信息和高级配置项，配置界面如图2-18所示。

图 2-18 参数配置



说明

基本信息：

- 设备名称：自主命名一阶段连接名称，二阶段会调用此设备名称下的相关配置。
- 设备地址类型：选择“对端是固定IP”。
- 固定IP：云端VPN网关IP，本示例IP：22.22.22.22
- 认证方式：预共享密钥，即PSK，与云端密钥相同。
- 启用设备/启用主动连接：可选。

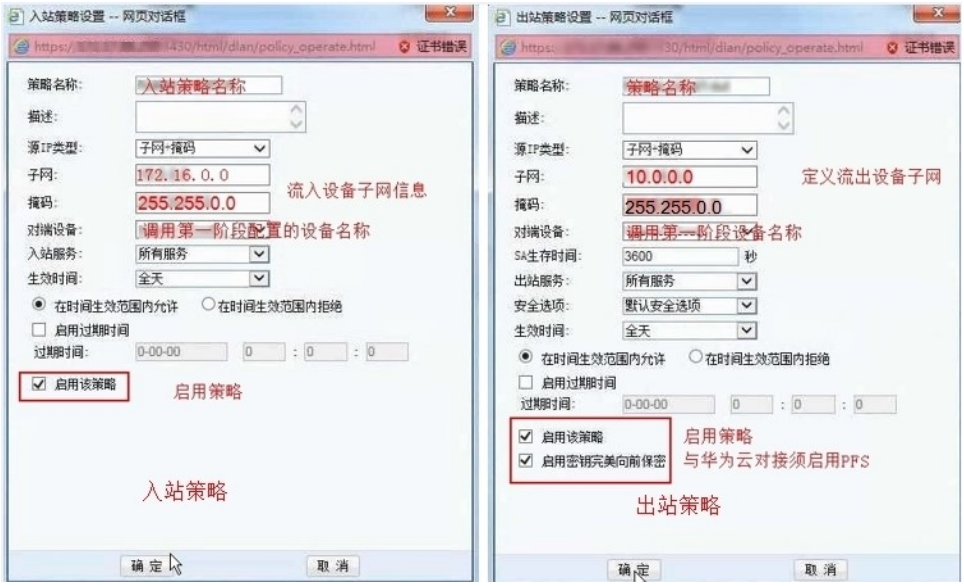
高级配置：

- ISAKMP存活时间：与云端相同86400s。
- 支持模式：深信服设备存在NAT穿越场景时请选择“野蛮模式”。
- D-H群：与云端一致，选择“MODP1536群（5）”。
- 本端/远端身份类型：IP地址，身份ID选择网关IP，NAT场景选择NAT后的IP。
- 使用DMZ专用VPN设备选择开启NAT穿越，选择防火墙不开启NAT穿越。
- DPD为可选配置（推荐不选），加密和认证算法与云端一致。

2. IPsec二阶段配置

选择“ VPN > IPsec VPN > 第三方对接 > 第二阶段 ”，分别新增“入站策略”和“出站策略”，详细配置如图2-19所示。

图 2-19 IPsec 二阶段配置



说明

入站策略：

- 策略名称：自主命名。
- 源IP类型：选择“子网和掩码”。
- 子网及掩码：填入流入本地设备的子网信息，多个子网逐条创建。
- 对端设备：调用IKE一阶段配置的对端IP，此处选择一阶段【设备名称】。
- 入站服务选择所有，生效时间选择全天，并启用该策略。

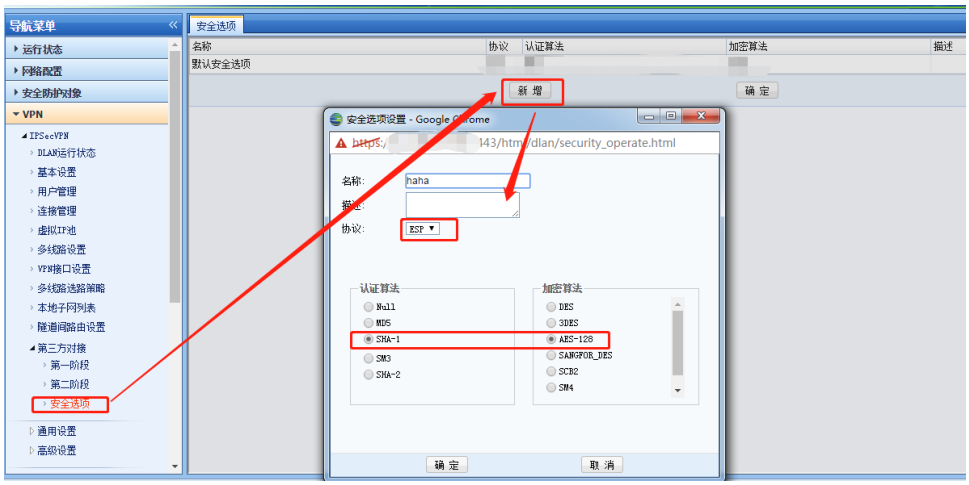
出站策略：

- 策略名称：自主命名策略。
- 源IP类型：选择“子网和掩码”。
- 子网及掩码：填入流出本地设备的子网信息，多个子网逐条创建。
- 对端设备：调用IKE一阶段配置的对端IP，此处选择一阶段【设备名称】。
- SA生存时间：选择和云端一致的3600s
- 出站服务选择所有，生效时间选择全天，并启用该策略。
- 密钥完美向前保密：启用，即开启PFS，DH group选择与IKE相同。

3. **安全选项配置**

   选择“ VPN > IPsec VPN > 第三方对接 > 安全选项 ”，单击“新增”，在弹出页面配置自定义名称，协议选择与云端相同的“ESP”，认证和加密算法也与云端配置相同，详细配置如图2-20所示。

图 2-20 安全选项配置



步骤2 配置路由

选择“ 网络 > 路由 > 静态路由 ”，单击“新增”。不同类别设备的操作页面存在差异。

1. 使用DMZ区域专用VPN设备配置连接。

- VPN设备使用原有缺省路由即可，对应VPN路由在IPsec配置时会自动生成；
- 防火墙添加目标地址为云端子网，下一跳为VPN设备建立VPN连接的私网IP；

2. 使用防火墙配置VPN连接（该场景下不涉及专用VPN设备配置）。

- 防火墙添加目标地址为云端子网，下一跳为出接口的公网IP。

步骤3 配置策略及NAT

1. 选择“ 网络 > 地址转换 ”单击“新增”，配置NAT信息。
2. 选择“ 访问控制 > 应用控制策略 ”单击“新增”，配置访问策略。

   在本示例拓扑中，选择防火墙或DMZ区域专用的VPN设备，在策略及NAT配置同样存在不同之处。
3. 使用DMZ区域专用VPN设备配置连接。
   - 先配置网关地址两个方向的NAT信息

     WAN→DMZ（VPN设备所在区域）源地址ANY，目标地址：11.11.11.11，源端口ANY，目标端口选择AH、ESP、ICMP及UDP的500、4500，转换后IP:10.10.10.10。

     DMZ→ WAN 源地址：10.10.10.10，目标地址：22.22.22.22，源端口ANY，目标端口选择AH、ESP、ICMP及UDP的500、4500，转换后IP：11.11.11.11。
   - 配置云端子网和本地子网互访的两个方向放行策略

     WAN→LAN 源地址：172.16.0.0/16，目标地址：10.0.0.0/16，服务为ANY，策略为放行（不配置该网段访问的NAT）。

     LAN→ WAN 源地址：10.0.0.0/16，目标地址：172.16.0.0/16，服务为ANY，策略为放行（不配置该网段访问的NAT）。
4. 使用防火墙配置VPN连接

   不需要配置NAT信息，需要配置子网间的放行策略，并添加VPN连接建立的放行策略。

WAN→ DMZ（VPN设备所在区域）源地址为ANY，目标地址：11.11.11.2（防火墙出接口地址），服务为AH、ESP、ICMP及UDP的500、4500，策略为放行。

DMZ→ WAN 源地址：11.11.11.2，目标地址为ANY，服务为AH、ESP、ICMP及UDP的500、4500，策略为放行。

----结束

配置验证

本地子网与云上子网互访正常。

2.5 示例：使用 TheGreenBow IPsec VPN Client 配置云上云下互通

操作场景

本文档详细的描述了“VPC+云桌面”和“VPC+VPC”场景下，使用TheGreenBow IPsec VPN Clinet软件与华为云端建立VPN连接的配置指导。

本任务指导您使用The GreenBow IPsec VPN Client测试VPN云连接配置，通过两个应用场景分别说明了IPsec VPN Client的配置信息，场景配置信息说明如下。

- **场景一：桌面云安装客户端与VPC上的VPN网关互联。**
  a. 受客户端限制，桌面云需为Windows操作系统。
  b. 桌面云可Ping通云端VPC的VPN网关IP（Ping不通无法建立VPN连接）。
- **场景二：VPC1上的ECS安装客户端与VPC2上的VPN网关互联。**
  a. VPC1上的Windows虚拟机需要购买EIP。
  b. VPC1的虚拟机可Ping通VPC2上的VPN网关IP（Ping不通无法建立VPN连接）。

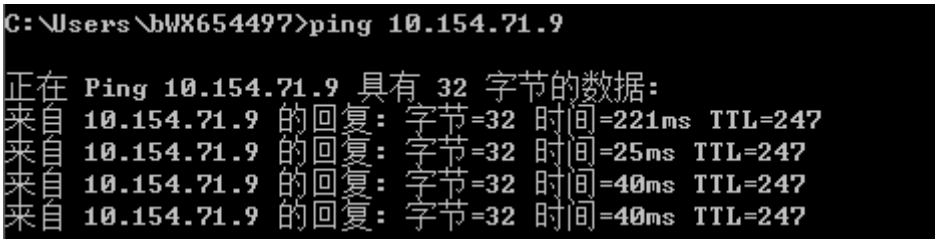
前提条件

- **场景一：桌面云+VPC**
  - 云端完成VPC、子网和ECS配置。
  - 云端完成VPN网关和连接配置。

图 2-21 策略详情

- 云桌面完成TheGreenBow IPsec VPN Client 客户端安装。
- 桌面云可Ping VPN网关IP地址。

图 2-22 桌面云 Ping VPN 连接

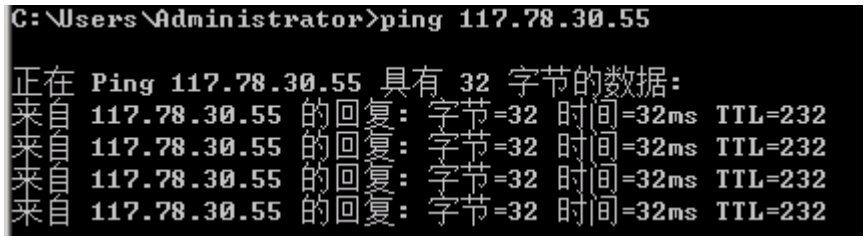


- **场景二：VPC+VPC**
  - 完成两个区域的VPC、子网和ECS配置，其中一个区域的ECS必须为Windows（VPC2）。
  - 在VPC1完成VPN网关和VPN连接配置。

图 2-23 策略详情 2

- VPC2中的Windows虚拟机安装TheGreenBow IPsec VPN Client 客户端。
- VPC2虚拟机可Ping VPC1上的VPN网关IP地址。

图 2-24 VPC 虚拟机 Ping VPN 网关



说明

华为云端的VPN配置信息采用默认配置。

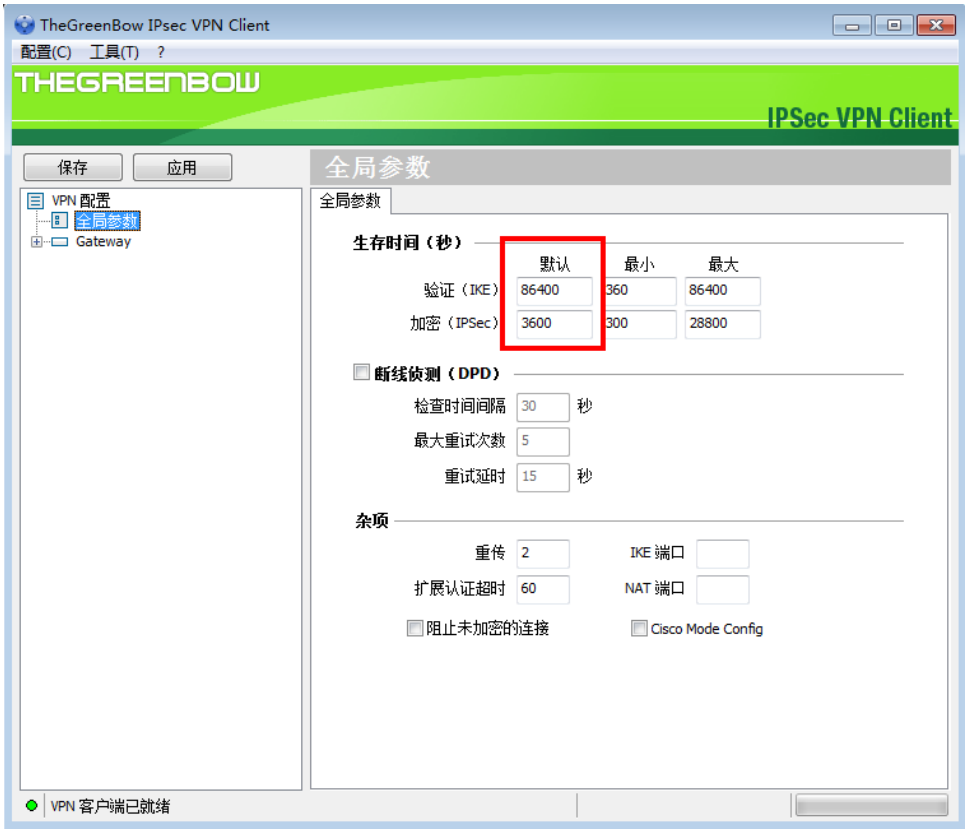
配置步骤

场景一：桌面云+VPC场景的客户端配置

1. 全局参数配置

   修改IKE和IPsec的默认生存时间（非关键配置步骤，选配），建议不勾选断线侦测。

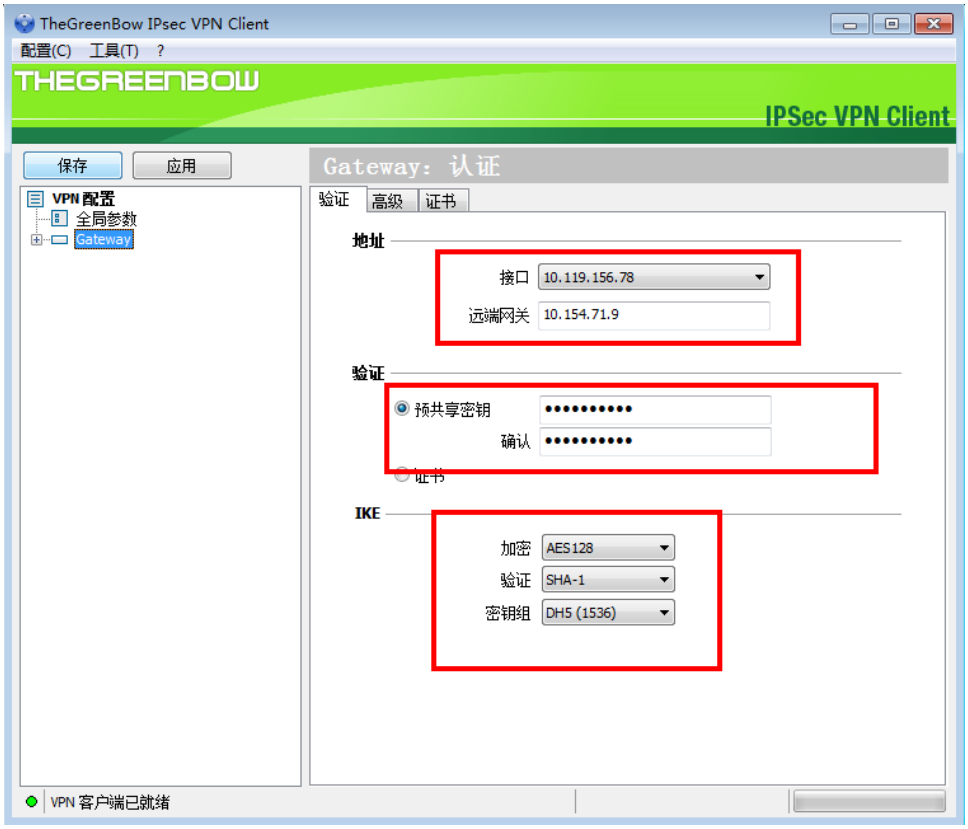
图 2-25 全局参数配置



2. IKE第一阶段配置

   右键单击“VPN配置”，选择“新建第一阶段”，本示例中使用客户端软件已有的第一阶段进行配置，配置信息请参见图2-26。

图 2-26 IKE 第一阶段配置



说明

- 接口：选择本地用于VPN连接的网卡接口。
- 远端网关：VPC云端购买的VPN网关。
- 预共享密钥：与华为云端配置一致【huawei@123】。
- IKE：与华为云端一致。加密【AES128】、验证【SHA-1】、密钥组【DH5(1536)】。
- 第一阶段高级信息按缺省配置，证书无需配置。
- 若高级信息中配置本端和远端ID，推荐选择IP。
  - 可选配置【本端ID】：IP地址10.119.156.78 //选择本端建立VPN的连接地址
  - 可选配置【远端ID】：IP地址10.154.71.9 //选择远端建立VPN的网关IP

IKE阶段高级配置信息请参见图2-27。

图 2-27 高级配置信息

3. IPsec第二阶段配置

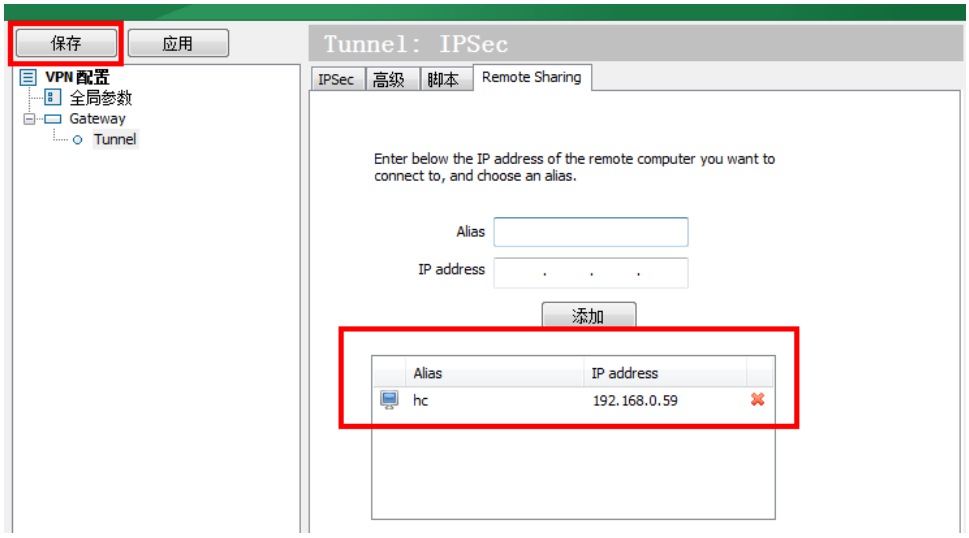
   右键单击“第一阶段”，选择“新建第二阶段”，本示例中使用客户端软件已有的第二阶段进行配置，配置信息请参见图2-28。

图 2-28 IPsec 第二阶段配置

说明

- VPN客户端地址：10.119.156.78 //**选择安装客户端桌面云的真实IP**
- 地址类型：子网地址
- 远端LAN地址：192.168.11.0 //VPC侧的子网
- 子网掩码：255.255.255.0 //VPC侧的子网掩码
- ESP：与华为云端配置一致。加密【AES128】、验证【SHA-1】、模式【隧道】。
- PSF：与华为云端配置一致。勾选PFS、群组【DH5(1536)】。
- 高级和脚本保持默认配置即可。
- Remote Sharing配置需要将VPC云端的ECS主机IP进行添加。

图 2-29 Remote Sharing 配置



须知

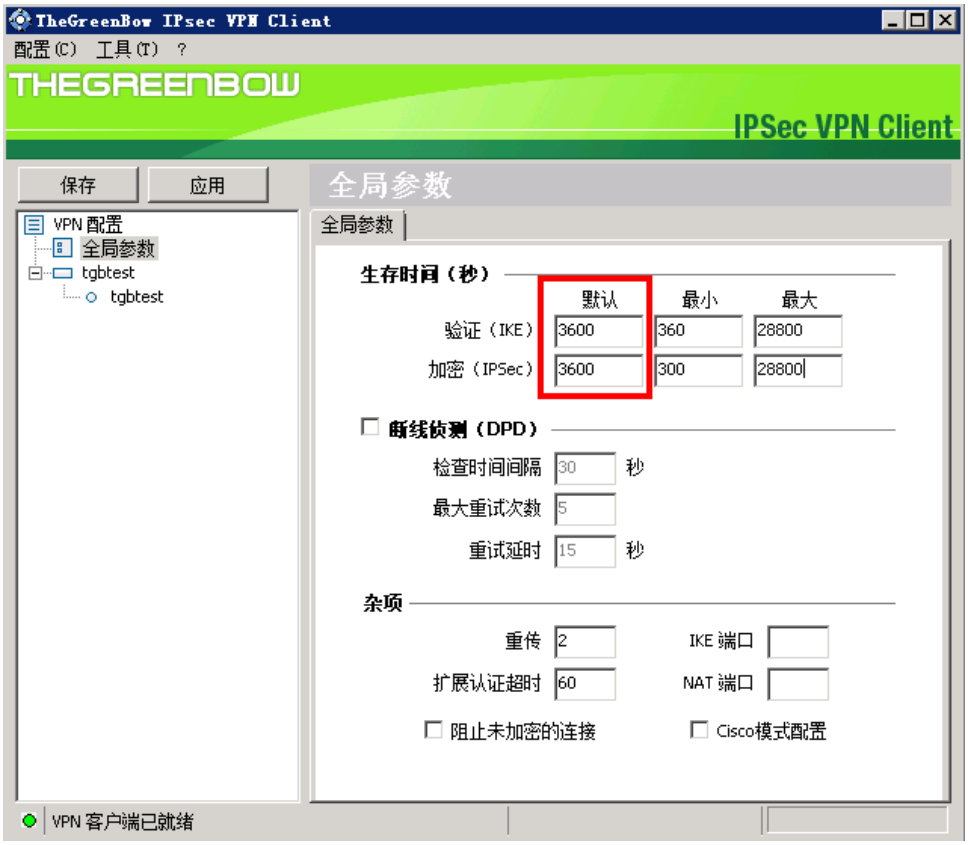
所有配置完成后请单击“保存”，后续修改配置信息请先保存再发起连接，否则更改配置信息不生效，建立连接在第二阶段页签点击右键，选择“开启隧道”，在调试过程中若修改过配置参数，请在保存后选择“工具 > 重置IKE”，待IKE重置后再重新开启隧道。

场景二：VPC+VPC场景的客户端配置

1. 全局参数配置

   修改IKE和IPsec的默认生存时间（非关键配置步骤，选配），建议不勾选断线侦测。

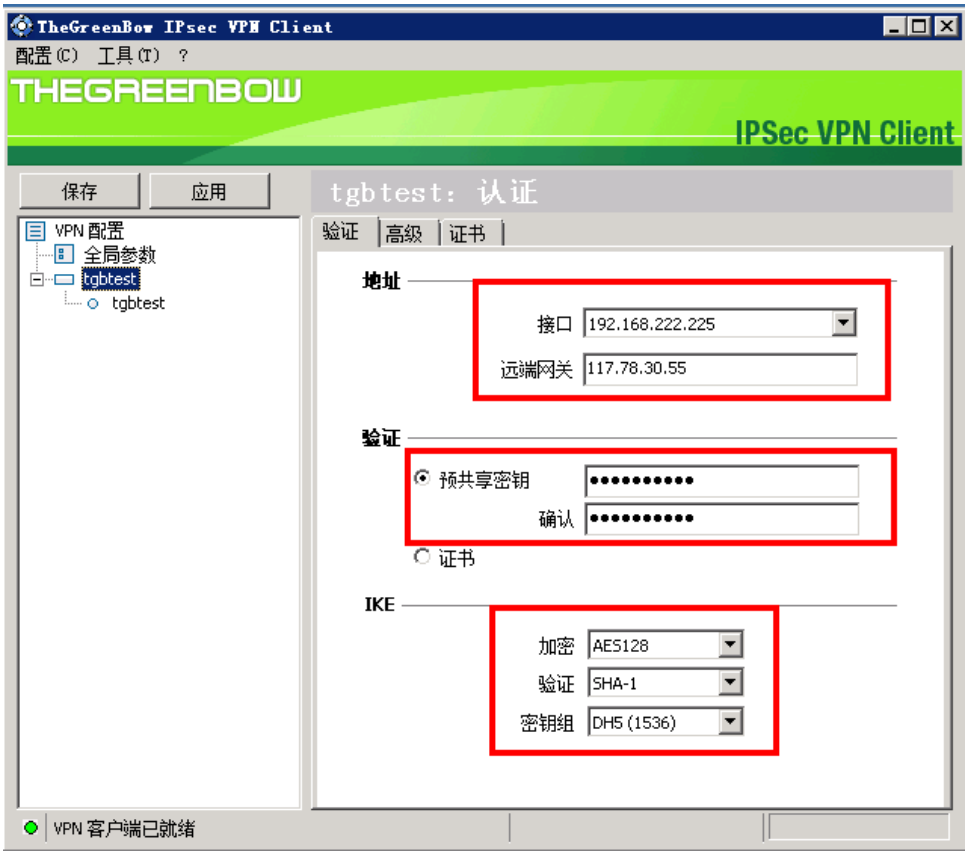
图 2-30 全局参数配置 2



2. IKE第一阶段配置

   右键单击“VPN配置”，选择“新建第一阶段”，本示例中使用客户端软件已有的第一阶段进行配置，配置信息请参见图2-31。

图 2-31 IKE 第一阶段配置 2

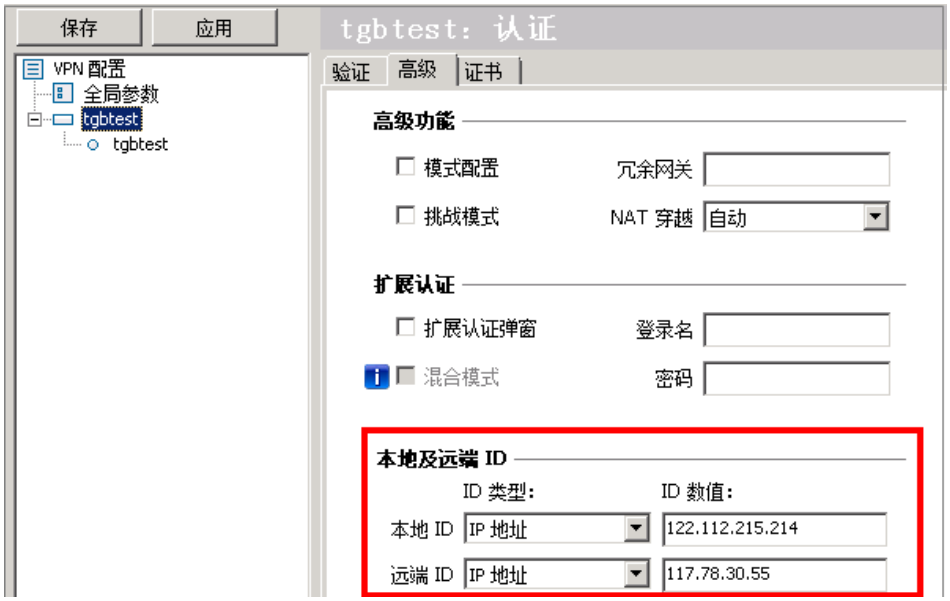


说明

- 接口：选择本地用于VPN连接的网卡接口。
- 远端网关：VPC云端购买的VPN网关。
- 预共享密钥：与华为云端配置一致【huawei@123】。
- IKE：与华为云端一致。加密【AES128】、验证【SHA-1】、密钥组【DH5(1536)】。
- 第一阶段高级信息按缺省配置，证书无需配置。
- 在高级信息中配置本端和远端ID，推荐选择IP； //此配置区别于桌面云
  - 必选配置【本端ID】：IP地址122.112.215.214 //选择本端建立VPN连接EIP
  - 必选配置【远端ID】：IP地址117.78.30.55 //选择远端建立VPN的网关IP

IKE阶段高级配置信息请参见图2-32。

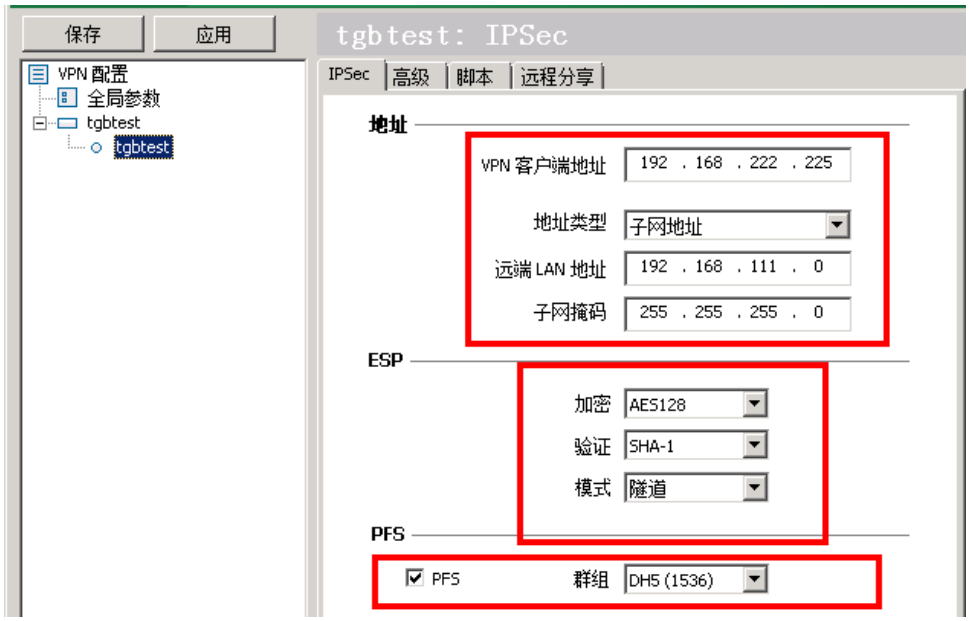
图 2-32 IKE 阶段高级配置信息 2



3. IPsec第二阶段配置

   右键单击“第一阶段”，选择“新建第二阶段”，本示例中使用客户端软件已有的第二阶段进行配置，配置信息请参见图2-33。

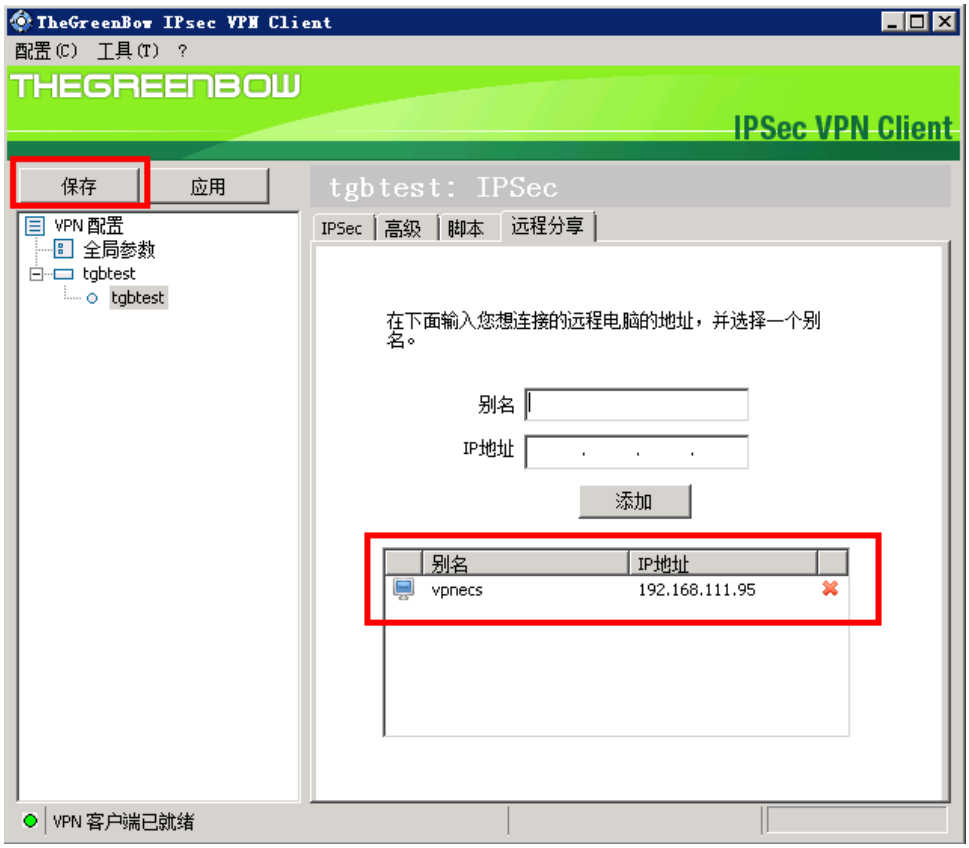
图 2-33 IPsec 第二阶段配置



说明

- VPN客户端地址：192.168.222.225 //**选择安装客户端虚拟机的真实IP**
- 地址类型：子网地址
- 远端LAN地址：192.168.111.0 //VPC侧的子网
- 子网掩码：255.255.255.0 //VPC侧的子网掩码
- ESP：与华为云端配置一致。加密【AES128】、验证【SHA-1】、模式【隧道】。
- PSF：与华为云端配置一致。勾选PFS、群组【DH5(1536)】。
- 高级和脚本保持默认配置即可。
- 远程分享配置需要将VPC云端的ECS主机IP进行添加。

图 2-34 远程分享配置



须知

所有配置完成后请单击“保存”，后续修改配置信息请先保存再发起连接，否则更改配置信息不生效，建立连接在第二阶段页签点击右键，选择“开启隧道”，在调试过程中若修改过配置参数，请在保存后选择“工具 > 重置IKE”，IKE重置后再重新开启隧道。

配置验证

- **场景一验证**

  在桌面云与VPC连接的场景中，桌面云最终可访问VPC远端虚拟机。

a. 桌面云VPN连接在开启隧道后，若配置正确，第一阶段创建的图示会很快切换为第二阶段，第二阶段和隧道建立成功。如下图所示。

图 2-35 发送第二阶段

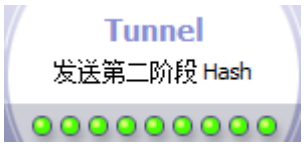


图 2-36 隧道开启

b. VPN连接建立成功如下图所示。

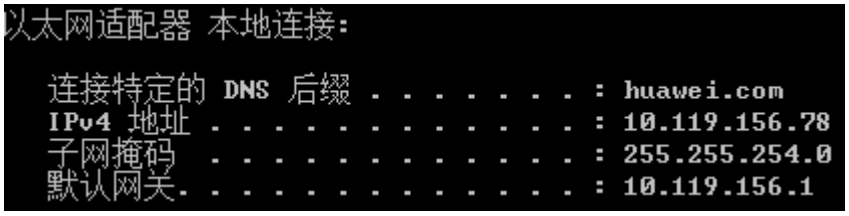
图 2-37 VPN 连接建立成功

c. 查看云端VPC中VPN连接状态。连接状态由“未连接”变为“正常”。

图 2-38 VPN 连接状态

d. 查看桌面云网络配置信息，如下图所示。

图 2-39 桌面云网络配置信息

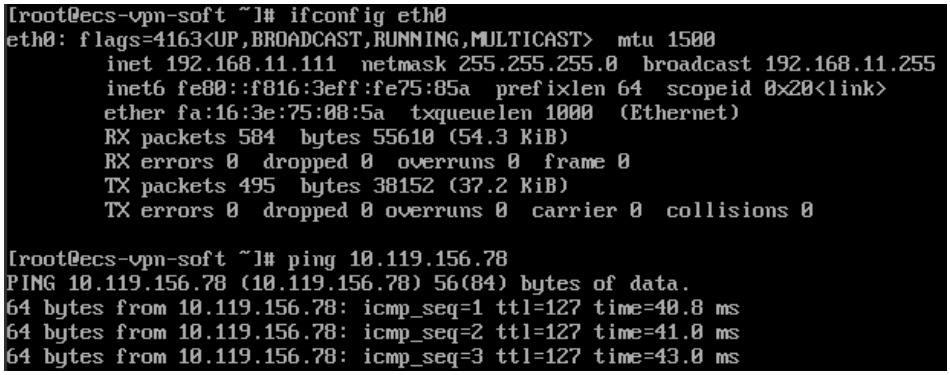


e. 桌面云 Ping 云端VPC虚拟机

图 2-40 桌面云 Ping 云端 VPC 虚拟机

f. 云端VPC虚拟机 Ping 桌面云

图 2-41 云端虚拟机 Ping 桌面云



场景一验证成功。

- **场景二验证**

  在VPC+VPC连接的场景中，VPC1的虚拟机和VPC安装客户端的虚拟机应该可以互通。

  a. VPN连接过程，开启隧道后，若配置正确，第一阶段创建的图示会很快切换为第二阶段，第二阶段和隧道建立成功。如下图所示。

  图 2-42 发送第二阶段 2

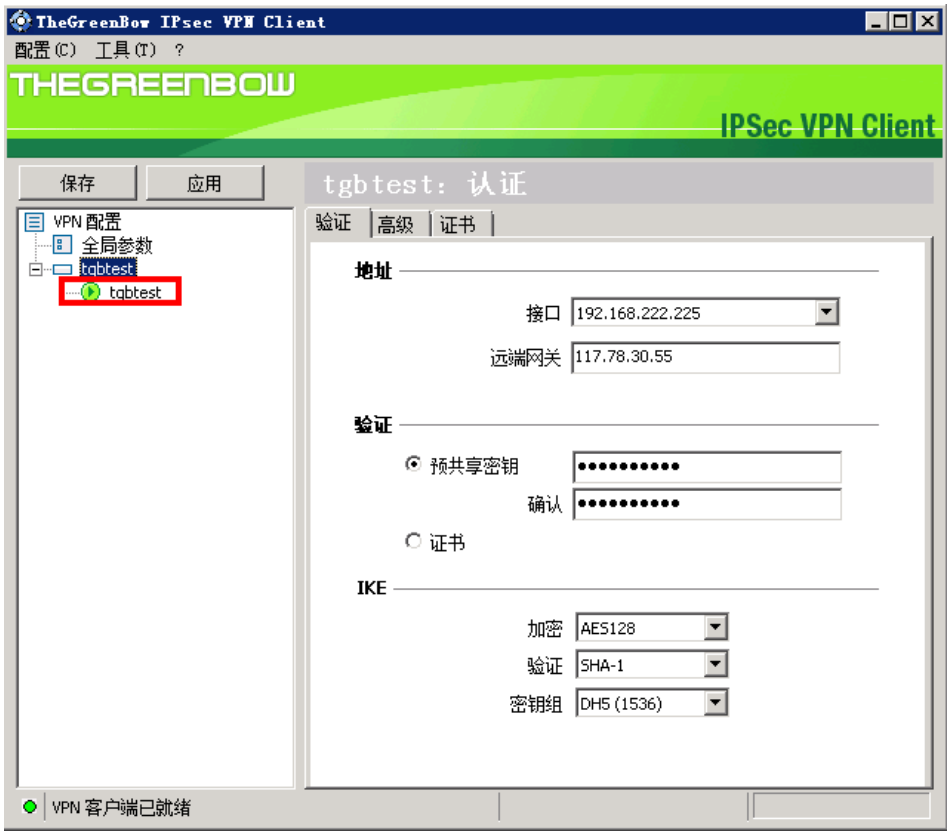
  

  图 2-43 隧道已开启 2

  b. VPN连接建立成功。如下图所示。

图 2-44 VPN 连接建立成功 2

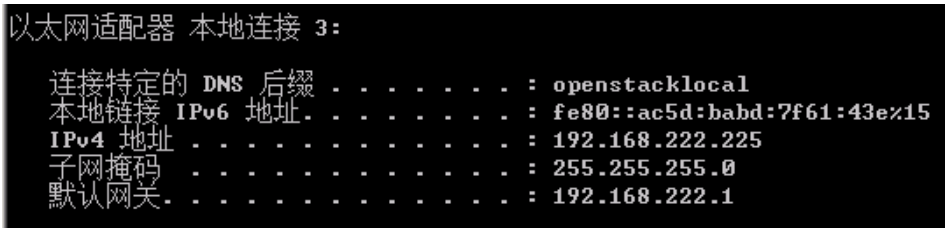


c. 查看云端VPC中VPN连接状态。连接状态由“未连接”变为“正常”。

图 2-45 VPN 连接状态 2

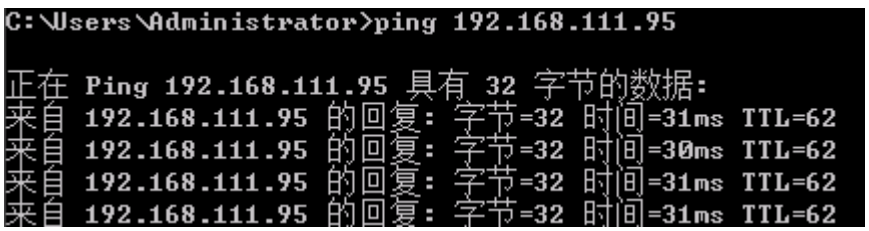
d. 查看VPC网络配置信息。如下图所示。

图 2-46 VPC 网络配置信息



e. VPC内的虚拟机 Ping 云端VPC虚拟机

图 2-47 VPC 内的虚拟机 Ping 云端 VPC 虚拟机



f. 云端VPC虚拟机 Ping VPC内的虚拟机

图 2-48 云端 VPC 虚拟机 Ping VPC 内的虚拟机

```
[root@ecs-vpn-eip ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.111.95  netmask 255.255.255.0  broadcast 192.168.111.255
        inet6 fe80::f816:3eff:feb8:eaab  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:b8:ea:ab  txqueuelen 1000  (Ethernet)
        RX packets 791  bytes 100807 (98.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 416  bytes 33932 (33.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpn-eip ~]# ping 192.168.222.225
PING 192.168.222.225 (192.168.222.225) 56(84) bytes of data.
64 bytes from 192.168.222.225: icmp_seq=5 ttl=127 time=31.2 ms
64 bytes from 192.168.222.225: icmp_seq=6 ttl=127 time=30.9 ms
64 bytes from 192.168.222.225: icmp_seq=7 ttl=127 time=30.7 ms
```

场景二验证成功。

2.6 示例：使用 OpenSwan 配置云上云下互通

操作场景

云端在VPC中购买了VPN网关和连接，云下客户使用主机安装IPsec软件与云端对接，客户主机在出口网络进行了一对一的NAT映射。

拓扑连接

本场景拓扑连接及策略协商配置信息如**图 拓扑连接及策略协商配置信息**所示。

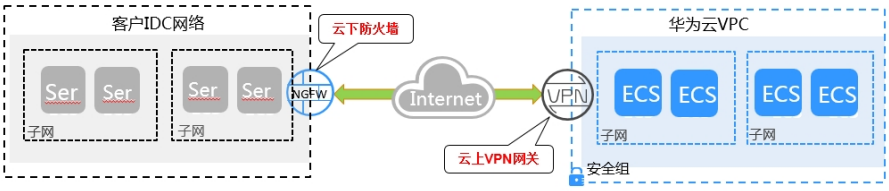
云上VPC的VPN网关IP：11.11.11.11，本地子网：192.168.200.0/24。

客户主机NAT映射IP：22.22.22.22，本地子网：192.168.222.0/24。

云端ECS与客户主机的本地IP地址分别为192.168.200.200和192.168.222.222。

VPN连接的协商参数使用华为云缺省配置。

图 2-49 拓扑连接及策略协商配置信息



用户侧网络			华为云侧网络	
IKE策略	认证SHA1、加密AES128、DH组group5、版本V1、协商模式Main、生命周期86400s	对接模式说明： 1、客户通过主机对接，安装Linux IPsec软件 2、客户主机出用户网络在防火墙进行一对一映射	IKE策略	认证SHA1、加密AES128、DH组group5、版本V1、协商模式Main、生命周期86400s
IPsec策略	认证SHA1、加密AES128、PFS DH-group5、生命周期3600s		IPsec策略	认证SHA1、加密AES128、PFS DH-group5、生命周期3600s
认证模式	预共享密钥		认证模式	预共享密钥
用户侧网关	22.22.22.22		华为云端网关	11.11.11.11
用户侧子网	192.168.222.0/24		华为云端子网	192.168.200.0/24

配置步骤

本示例以在CentOs6.8中配置Openswan IPsec客户端为例进行介绍。

步骤1 安装Openswan客户端。

yum install -y openswan

步骤2 开启IPv4转发。

vim /etc/sysctl.conf

1. 在配置文件中增加如下内容：
   ```
   net.ipv4.ip_forward = 1
   ```
2. 执行**/sbin/sysctl -p**命令，使转发配置参数生效。

步骤3 iptables配置。

确认关闭firewall或允许数据流转发，查询命令：**iptables -L**

```
iptables -L
  Chain INPUT (policy ACCEPT)
  target     prot opt source               destination
  Chain FORWARD (policy ACCEPT)
  target     prot opt source               destination
  Chain OUTPUT (policy ACCEPT)
  target     prot opt source               destination
```

步骤4 预共享密钥配置。

vim /etc/ipsec.d/open_IPsec.secrets

在配置文件中增加如下内容：

```
22.22.22.22 11.11.11.11 : psk "IPsec-key"
```

格式：本地用于连接的IP+空格+远端网关IP+空格+英文冒号+空格+PSK+预共享密钥，冒号的两边都有空格，PSK大小写均可，密钥用英文双引号。

步骤5 IPsec连接配置。

vim /etc/ipsec.d/open_IPsec.conf

在配置文件中增加如下内容：

```
conn openswan_IPsec                # 定义连接名称为openswan_IPsec
 type=tunnel                     # 开启隧道模式
 auto=start                      # 可选择add、route和start

 left=192.168.222.222              # 本地IP，nat场景选择真实的主机地址
 leftid=22.22.22.22                # 本地标识ID
 leftsourceip=22.22.22.22          # 如果存在nat，源地址选择nat后的IP
 leftsubnet=192.168.222.0/24       # 本地子网
 leftnexthop=22.22.22.1            # nat场景下一跳选择nat后的网关IP
 right=11.11.11.11                 # 远端VPN网关IP
 rightid=11.11.11.11               # 远端标识ID
 rightsourceip=11.11.11.11         # 远端源地址选择VPN网关IP
 rightsubnet=192.168.200.0/24      # 远端子网
 rightnexthop=%defaultroute        # 远端路由按缺省配置

 authby=secret                   # 定义认证方式为PSK
 keyexchange=ike                   # ike密钥交换方式
 ike=aes128-sha1;modp1536          # 按照对端配置定义ike阶段算法和group
 ikev2=never                     # 关闭IKEv2版本
 ikelifetime=86400s                # ike阶段生命周期

 phase2=esp                      # 二阶段传输格式
 phase2alg=aes128-sha1;modp1536    # 按照对端配置定义IPsec阶段算法和group，modp1536=DH group 5
 pfs=yes                         # 开启PFS
```



```
compress=no                 # 关闭压缩
salifetime=3600s            # 二阶段生命周期
```

说明

- 在NAT穿越场景中可按需配置forceencaps=yes。
- 华为云VPN使用的DH-group对应的比特位详细请参见**华为云VPN使用的DH-group对应的比特位是多少?** 。

配置完成后通过命令**ipsec verify**进行配置项校验。如果回显信息全部为OK时，表示配置成功。

```
ipsec verify
Verifying installed system and configuration files
Version check and IPsec on-path                                 [OK]
Libreswan 3.25 (netkey) on 3.10.0-957.5.1.el7.x86_64
Checking for IPsec support in kernel                                    [OK]
 NETKEY: Testing XFRM related proc values
        ICMP default/send_redirects             [OK]
        ICMP default/accept_redirects           [OK]
        XFRM larval drop                        [OK]
Pluto IPsec.conf syntax                         [OK]
Two or more interfaces found, checking IP forwarding[OK]
Checking rp_filter                              [OK]
Checking that pluto is running                  [OK]
 Pluto listening for IKE on udp 500             [OK]
 Pluto listening for IKE/NAT-T on udp 4500      [OK]
 Pluto IPsec.secret syntax                      [OK]
Checking 'ip' command                           [OK]
Checking 'iptables' command                     [OK]
Checking 'prelink' command does not interfere with FIPS[OK]
Checking for obsolete IPsec.conf options        [OK]
```

若回显信息出现如下报错：

```
Checking rp_filter                              [ENABLED]
 /proc/sys/net/ipv4/conf/default/rp_filter      [ENABLED]
 /proc/sys/net/ipv4/conf/lo/rp_filter           [ENABLED]
 /proc/sys/net/ipv4/conf/eth0/rp_filter         [ENABLED]
 /proc/sys/net/ipv4/conf/eth1/rp_filter         [ENABLED]
 /proc/sys/net/ipv4/conf/ip_vti01/rp_filter     [ENABLED]
```

通过如下命令解决：

```
echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/default/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth1/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/lo/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/ip_vti01/rp_filter
```

步骤6 启动服务。

service ipsec stop # 关闭服务

service ipsec start # 启动服务

service ipsec restart # 重启服务

ipsec auto --down openswan_IPsec # 关闭连接

ipsec auto --up openswan_IPsec # 开启连接

说明

每次修改配置都需要重启服务，并重新开启连接。

----结束

配置验证

通过查询IPsec的状态，结果显示如下信息（摘录），查询状态命令：**ipsec --status**。

```
Connection list:
000
000 "openswan_IPsec":
192.168.222.0/24===192.168.222.222<192.168.222.222>[22.22.22.22]---22.22.22.1...11.11.11.11<11.11.11.11>
===192.168.200.0/24; erouted; eroute owner: #30
000 "openswan_IPsec":     oriented; my_ip=22.22.22.22; their_ip=11.11.11.11; my_updown=IPsec _updown;
000 "openswan_IPsec":   xauth us:none, xauth them:none,  my_username=[any]; their_username=[any]
000 "openswan_IPsec":   our auth:secret, their auth:secret
000 "openswan_IPsec":   modecfg info: us:none, them:none, modecfg policy:push, dns:unset, domains:unset,
banner:unset, cat:unset;
000 "openswan_IPsec":   labeled_IPsec:no;
000 "openswan_IPsec":   policy_label:unset;
000 "openswan_IPsec":   ike_life: 86400s; IPsec_life: 3600s; replay_window: 32; rekey_margin: 540s;
rekey_fuzz: 100%; keyingtries: 0;
000 "openswan_IPsec":   retransmit-interval: 500ms; retransmit-timeout: 60s;
000 "openswan_IPsec":   initial-contact:no; cisco-unity:no; fake-strongswan:no; send-vendorid:no; send-no-
esp-tfc:no;
000 "openswan_IPsec":   policy: PSK+ENCRYPT+TUNNEL+PFS+UP+IKEV1_ALLOW+SAREF_TRACK
+IKE_FRAG_ALLOW+ESN_NO;
000 "openswan_IPsec":   conn_prio: 24,24; interface: eth0; metric: 0; mtu: unset; sa_prio:auto; sa_tfc:none;
000 "openswan_IPsec":   nflog-group: unset; mark: unset; vti-iface:unset; vti-routing:no; vti-shared:no; nic-
offload:auto;
000 "openswan_IPsec":   our idtype: ID_IPV4_ADDR; our id=1.1.1.1; their idtype: ID_IPV4_ADDR; their
id=2.2.2.2
000 "openswan_IPsec":   dpd: action:hold; delay:0; timeout:0; nat-t: encaps:auto; nat_keepalive:yes;
ikev1_natt:both
000 "openswan_IPsec":   newest ISAKMP SA: #3; newest IPsec SA: #30;
000 "openswan_IPsec":   IKE algorithms: AES_CBC_128-HMAC_SHA1-MODP1536
000 "openswan_IPsec":   IKE algorithm newest: AES_CBC_128-HMAC_SHA1-MODP1536
000 "openswan_IPsec":   ESP algorithms: AES_CBC_128-HMAC_SHA1_96-MODP1536
000 "openswan_IPsec":   ESP algorithm newest: AES_CBC_128-HMAC_SHA1_96; pfsgroup=MODP1536
000
000 Total IPsec connections: loaded 1, active 1
000
000 State Information: DDoS cookies not required, Accepting new IKE connections
000 IKE SAs: total(1), half-open(0), open(0), authenticated(1), anonymous(0)
000 IPsec SAs: total(1), authenticated(1), anonymous(0)
000
000 #3: "openswan_IPsec":4500 STATE_MAIN_R3 (sent MR3, ISAKMP SA established); EVENT_SA_REPLACE
in 15087s; newest ISAKMP; lastdpd=-1s(seq in:0 out:0); idle; import:admin initiate
000 #30: "openswan_IPsec":4500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in
1744s; newest IPsec; eroute owner; isakmp#3; idle; import:admin initiate
000 #30: "openswan_IPsec" esp.b810a24@11.11.11.11 esp.aab7b496@192.168.222.222 tun.0@11.11.11.11
tun.0@192.168.222.222 ref=0 refhim=0 Traffic: ESPin=106KB ESPout=106KB! ESPmax
=4194303B
```

2.7 示例：使用 StrongSwan 配置云上云下互通

操作场景

云端在VPC中购买了VPN网关和连接，云下客户使用主机安装IPsec软件与云端对接，客户主机在出口网络进行了一对一的NAT映射。

拓扑连接

本场景拓扑连接及策略协商配置信息如图2-50所示，

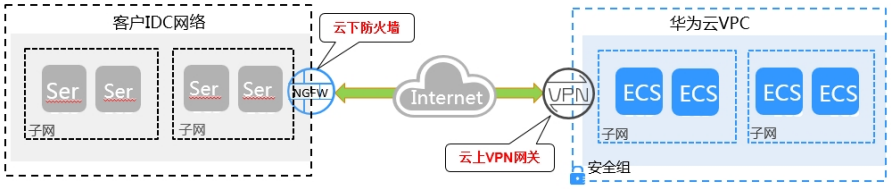
云上VPC的VPN网关IP：11.11.11.11，本地子网：192.168.200.0/24。

客户主机NAT映射IP：22.22.22.22，本地子网：192.168.222.0/24。

云端ECS与客户主机的本地IP地址分别为192.168.200.200和192.168.222.222。

VPN连接的协商参数使用华为云缺省配置。

图 2-50 拓扑连接及策略协商配置信息



用户侧网络		对接模式说明： 1、客户通过主机对接，安装Linux IPsec软件 2、客户主机出用户网络在防火墙进行一对一映射	华为云侧网络	
IKE策略	认证SHA1、加密AES128、DH组group5、版本V1、协商模式Main、生命周期86400s		IKE策略	认证SHA1、加密AES128、DH组group5、版本V1、协商模式Main、生命周期86400s
IPsec策略	认证SHA1、加密AES128、PFS DH-group5、生命周期3600s		IPsec策略	认证SHA1、加密AES128、PFS DH-group5、生命周期3600s
认证模式	预共享密钥		认证模式	预共享密钥
用户侧网关	22.22.22.22		华为云端网关	11.11.11.11
用户侧子网	192.168.222.0/24		华为云端子网	192.168.200.0/24

配置步骤

根据strongswan版本不同，相关配置可能存在差异。本示例以strongswan 5.7.2版本为例，详细介绍strongswan在Linux环境下的VPN配置。

步骤1 安装IPsec VPN客户端。

yum install strongswan

安装交互过程选择“Y”，出现“Complete!”提示即完成安装，strongswan的配置文件集中放置在/etc/strongswan目录中，配置过程只需编辑ipsec.conf和ipsec.secrets文件即可。

步骤2 开启IPv4转发。

vim /etc/sysctl.conf

1. 在配置文件中增加如下内容：
   ```
   net.ipv4.ip_forward = 1
   ```
2. 执行**/sbin/sysctl -p**命令，使转发配置参数生效。

步骤3 iptables配置。

确认关闭firewall或允许数据流转发，查询命令：**iptables -L**

```
iptables -L
  Chain INPUT (policy ACCEPT)
  target     prot opt source               destination
  Chain FORWARD (policy ACCEPT)
  target     prot opt source               destination
  Chain OUTPUT (policy ACCEPT)
  target     prot opt source               destination
```

步骤4 预共享密钥配置。

```
vim /etc/strongswan/ipsec.secrets        # 编辑ipsec.secrets文件
22.22.22.22 11.11.11.11 : PSK "ipsec-key"
```

格式与openswan相同，冒号的两边都有空格，PSK只能为大写，密钥用英文双引号。

步骤5 IPsec连接配置。

vim /etc/strongswan/ipsec.conf

在配置文件中增加如下内容：

```
config setup
conn strong_ipsec                    # 定义连接名称为strong_ipsec
  auto=route                        # 可选择add、route和start
  type=tunnel                       # 开启隧道模式
  compress=no                        # 关闭压缩
  leftauth=psk                      # 定义本地认证方式为PSK
  rightauth=psk                      # 定义远端认证方式为PSK
  ikelifetime=86400s                  # ike阶段生命周期
  lifetime=3600s                     # 二阶段生命周期
  keyexchange=ikev1                    # ike密钥交换方式为版本1
  ike=aes128-sha1-modp1536!              # 按照对端配置定义ike阶段算法和group，modp1536=DH group
5
  esp=aes128-sha1-modp1536!              # 按照对端配置定义ipsec阶段算法和group，modp1536=DH
group 5
  leftid=22.22.22.22                  # 本端标识ID
  left=192.168.222.222                  # 本地IP，nat场景选择真实的主机地址
  leftsubnet=192.168.222.0/24             # 本地子网
  rightid=11.11.11.11                  # 远端标识ID
  right=11.11.11.11                   # 远端VPN网关IP
  rightsubnet=192.168.200.0/24           # 远端子网
```

说明

华为云VPN使用的DH-group对应的比特位详细请参见**华为云VPN使用的DH-group对应的比特位是多少？**。

步骤6 启动服务。

service strongswan stop # 关闭服务

service strongswan start # 启动服务

service strongswan restart # 重启服务

strongswan stop # 关闭连接

strongswan start # 开启连接

说明

每次修改配置都需要重启服务，并重新开启连接。

----结束

配置验证

通过**strongswan statusall**查询，可见连接启动时间。

```
Status of IKE charon daemon (strongSwan 5.7.2, Linux 3.10.0-957.5.1.el7.x86_64, x86_64):
  uptime: 5 minutes, since Apr 24 19:25:29 2019
  malloc: sbrk 1720320, mmap 0, used 593088, free 1127232
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 1
  loaded plugins: charon pkcs11 tpm aesni aes des rc2 sha2 sha1 md4 md5 mgf1 random nonce x509
revocation constra
ints acert pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt fips-prf gmp curve25519
chapoly x
cbc cmac hmac ctr ccm gcm curl attr kernel-netlink resolve socket-default farp stroke vici updown eap-
identity ea
p-sim eap-aka eap-aka-3gpp eap-aka-3gpp2 eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-
tls eap-ttls eap
-peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp led duplicheck unity counters
```

```
Listening IP addresses:192.168.222.222
Connections:
strong_ipsec:  192.168.222.222...11.11.11.11  IKEv1
strong_ipsec:   local:  [22.22.22.22] uses pre-shared key authentication
strong_ipsec:   remote: [11.11.11.11] uses pre-shared key authentication
strong_ipsec:   child:  192.168.222.0/24 === 192.168.200.0/24 TUNNEL
Routed Connections:
strong_ipsec{1}:  ROUTED, TUNNEL, reqid 1
strong_ipsec{1}:   192.168.222.0/24 === 192.168.200.0/24
Security Associations (0 up, 1 connecting):
strong_ipsec[1]: CONNECTING, 192.168.222.222[%any]...11.11.11.11[%any]
strong_ipsec[1]: IKEv1 SPIs: c3090f6512ec6b7d_i* 0000000000000000_r
strong_ipsec[1]: Tasks queued: QUICK_MODE QUICK_MODE
strong_ipsec[1]: Tasks active: ISAKMP_VENDOR ISAKMP_CERT_PRE MAIN_MODE ISAKMP_CERT_POST
ISAKMP_NATD
```

通过**VPC1 ping**安装有IPsec客户端的VPC2的主机：

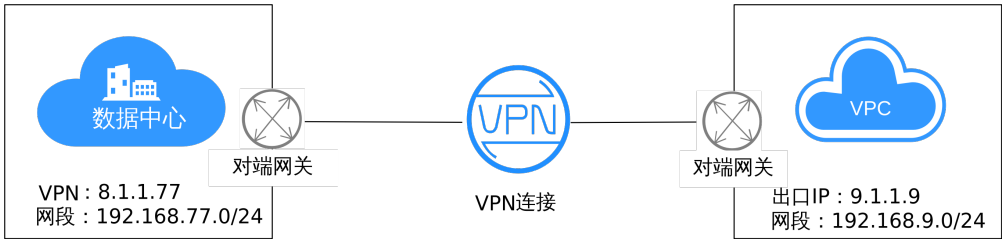
```
ping 192.168.222.222
PING 192.168.222.222 (192.168.222.222) 56(84) bytes of data.
64 bytes from 192.168.222.222: icmp_seq=1 ttl=62 time=3.07 ms
64 bytes from 192.168.222.222: icmp_seq=2 ttl=62 time=3.06 ms
64 bytes from 192.168.222.222: icmp_seq=3 ttl=62 time=3.98 ms
64 bytes from 192.168.222.222: icmp_seq=4 ttl=62 time=3.04 ms
64 bytes from 192.168.222.222: icmp_seq=5 ttl=62 time=3.11 ms
64 bytes from 192.168.222.222: icmp_seq=6 ttl=62 time=3.71 ms
```

2.8 示例：Web 配置华为 USG 防火墙

组网拓扑

云下华为USG为用户的出口防火墙，通过该设备配置VPN与华为云VPC连通，两端的子网信息和连接方式如图 拓扑连接所示。

图 2-51 拓扑连接



用户侧信息：

- 网关：1.1.1.1。
- 子网：192.168.1.0/24。

华为云侧信息：

- 网关：1.1.1.2。
- 子网：192.168.2.0/24。

华为云端的VPN连接资源策略配置按照缺省信息配置，详见图2-52。

图 2-52 策略配置

IKE策略		IPsec策略	
认证算法	SHA1	认证算法	SHA1
加密算法	AES-128	加密算法	AES-128
DH算法	Group 5	PFS	Group 5
版本	v1	传输协议	ESP
协商模式	Main	生命周期（秒）	3600
生命周期（秒）	86400		

配置步骤

步骤1 IPsec基础配置

登录防火墙管理页面，选择“网络 > IPsec”，新建IPsec连接，详情如图2-54所示。

图 2-53 新建 IPsec 连接 1

图 2-54 新建 IPsec 连接 2

表 2-1 新建 IPsec 参数设置

参数名称	说明
虚拟系统	选择默认即可。
策略名称	客户自行指定。
本端接口	配置对接本端公网IP的接口。
本端地址	本端公网IP。
对端地址	对端公网IP。
认证方式	预共享密钥。
本端ID与对端ID	IP地址，并填入对应的公网IP。
待加密数据流	源地址为云下子网，目标地址为云上子网，请勿使用地址组名称配置。
安全提议	按照华为云策略配置，要求两端配置信息一致。

参数名称	说明
DPD	勾选DPD，选择按需发送，配置信息默认即可。

步骤2 路由配置

选择“网络 > 路由 > 静态路由”，新建一条目的为华为云子网的静态路由，下一跳指向本地出接口网关IP。

图 2-55 新建静态路由

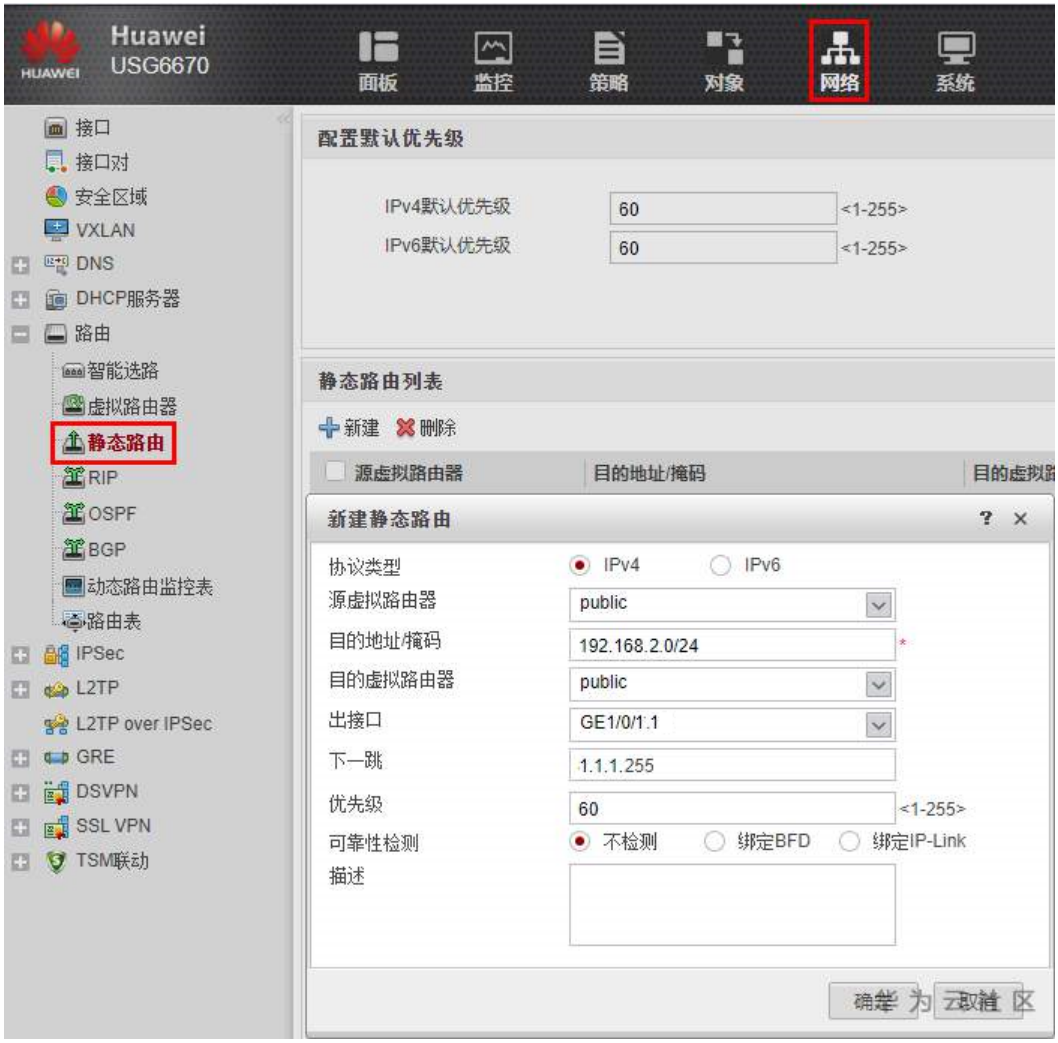


表 2-2 新建静态路由参数设置

参数名称	说明
协议类型	IPv4。
源虚拟路由器	选择默认的“public”。
目的地址/掩码	云端子网地址。

参数名称	说明
目的虚拟路由器	选择默认的“public”。
出接口	本端公网IP配置的接口。
下一跳	本端公网地址下一跳。

说明

其余配置默认即可，存在多出口时，需额外添加访问云端公网IP从此出接口流出的路由。

步骤3 NAT配置

选择“策略 > NAT策略 > 源NAT”，新建一条本地子网访问华为云不做NAT转换的策略。

图 2-56 新建源 NAT 策略

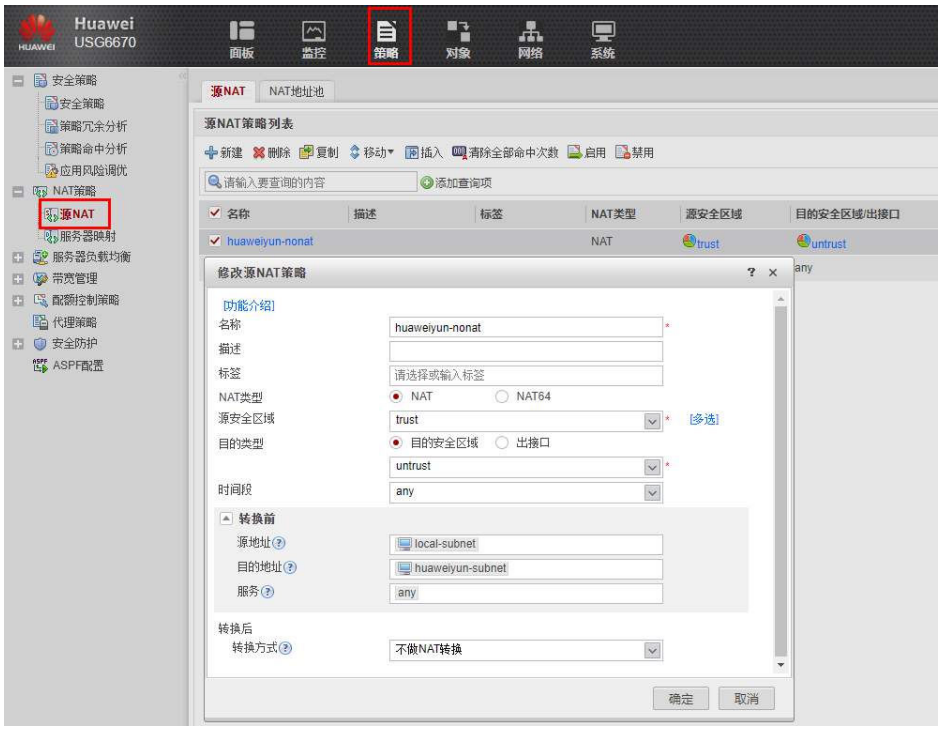


表 2-3 新建源 NAT 策略参数设置

参数名称	说明
源安全区域	本端子网所在安全区域。
目的区域	华为云子网所在安全区域，一般为untrust。
源地址	本端子网。
目的地址	华为云对端子网。

参数名称	说明
服务	any
转换方式	不做NAT转换

说明

- 为确保该策略优先匹配，请将该策略置顶。
- 请注意接口地址出外网不做NAT转换。

  例如已配置缺省策略：源区域为any，访问目标区域any，出口转换为接口地址。请额外添加一条NAT策略：源区域为local，目标区域为any，转换方式为不做NAT转换，并将该策略置于缺省策略之上。

步骤4 安全策略配置

选择“策略 > 安全策略 > 安全策略”，新建一条本地子网访问华为云的放行策略。

图 2-57 安全策略

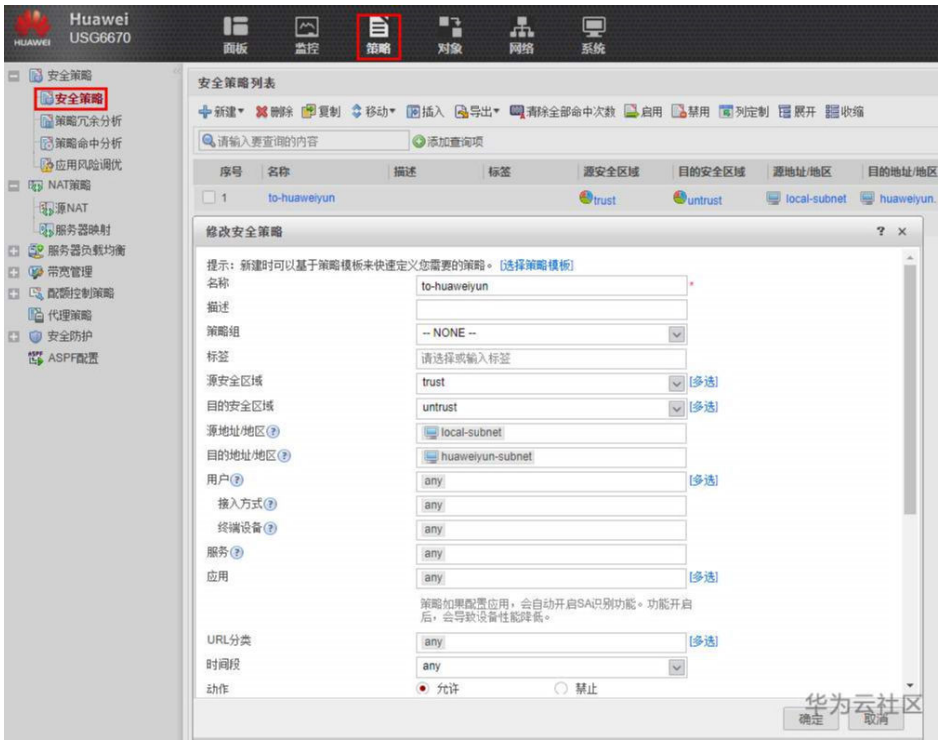


表 2-4 新建策略参数设置

参数名称	说明
源安全区域	本端子网所在区域。
源安全区域	本端子网所在安全区域。

参数名称	说明
目的区域	华为云子网所在安全区域，一般为untrust。
源地址	本端子网。
目的地址	华为云对端子网。
服务	any。
动作	允许

说明

为确保该策略优先匹配，请将该策略置顶。

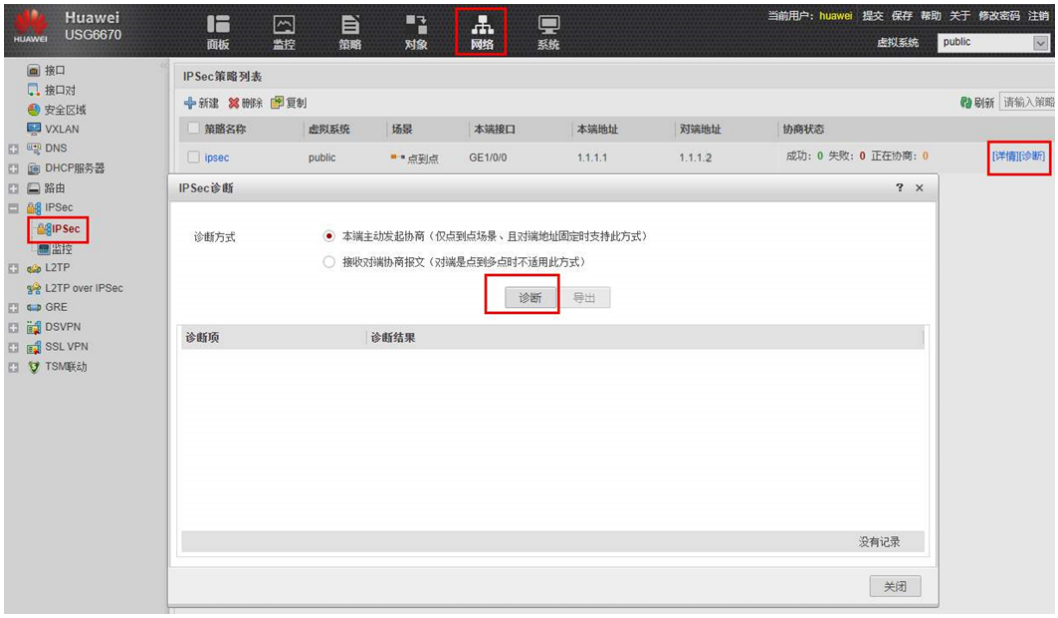
----结束

配置验证

完成配置后，请选择“网络 > IPsec > IPsec”，单击对应策略列的“诊断”，发起连接协商。

连接状态详细在“IPsec-监控”中查看，诊断示意如图2-58所示。

图 2-58 IPsec 诊断



2.9 附录

2.9.1 H3C-SecPath 防火墙(V7)对接华为云配置指引

华为云配置信息说明

VPN网关IP：11.11.11.11

VPC子网：192.168.10.0/24，192.168.20.0/24

客户侧网关IP：22.22.22.22

客户侧子网：172.16.10.0/24，172.16.20.0/24，172.16.30.0/24

协商策略详情：

一阶段策略（IKE Policy）

认证算法（Authentication Algorithm）: sha2-256

加密算法（Encryption Algorithm）: aes-128

版本（Version）: v2

DH算法（DH Algorithm ）: group14

生命周期（Life Cycle）: 86400

二阶段策略（IPsec Policy）

传输协议（Transfer Protocol）: esp

认证算法（Authentication Algorithm）: sha2-256

加密算法（Encryption Algorithm）: aes-128

完美前向安全（PFS）： DH-group14

生命周期（Life Cycle）: 86400

客户侧设备组网与基础配置假设

1. 假定客户侧基础网络配置如下：
   - 内网接口：GigabitEthernet1/0/0 所属zone为Trust，接口IP为10.0.0.1/30。
   - 预进行加密传输的子网为172.16.10.0/24，172.16.20.0/24，172.16.30.0/24，所属zone为Trust。
   - 外网接口：GigabitEthernet1/0/1 所属zone为Untrust，接口IP为22.22.22.22/24。
   - 缺省路由：目标网段0.0.0.0/0 出接口GE1/0/1，下一跳为GE1/0/1的网关IP为22.22.22.1。
   - 安全策略：Trust访问Untrust，源地址、目标地址及服务均为any，动作放行。
   - NAT策略：源地址为内网网段，目标地址为ANY，动作为EasyIP，即转换为接口IP。
2. 基础配置命令行示意如下：

```
interface GigabitEthernet1/0/0
ip address 10.0.0.1 255.255.255.252
#
interface GigabitEthernet1/0/1
```



```
ip address 22.22.22.22 255.255.255.0
#
ip route-static 0.0.0.0 0 GigabitEthernet1/0/1 22.22.22.1
ip route-static 172.16.10.0 255.255.255.0 0 GigabitEthernet1/0/0 10.0.0.2
ip route-static 172.16.20.0 255.255.255.0 0 GigabitEthernet1/0/0 10.0.0.2
ip route-static 172.16.30.0 255.255.255.0 0 GigabitEthernet1/0/0 10.0.0.2
#
security-zone name Trust
import interface GigabitEthernet1/0/0
#
security-zone name Untrust
import interface GigabitEthernet1/0/1
#
security-policy ip
rule 0 name Policy-Internet
  action pass
  logging enable
  counting enable
  source-zone Trust
  destination-zone Untrust
#
object-group ip address Customer-subnet172.16.10.0/24
0 network subnet 172.16.10.0 255.255.255.0
#
object-group ip address Customer-subnet172.16.20.0/24
0 network subnet 172.16.20.0 255.255.255.0
#
object-group ip address Customer-subnet172.16.30.0/24
0 network subnet 172.16.30.0 255.255.255.0
#
nat policy
rule name Snat_Internet
  source-ip Customer-subnet172.16.10.0/24
  source-ip Customer-subnet172.16.20.0/24
  source-ip Customer-subnet172.16.30.0/24
  outbound-interface GigabitEthernet1/0/1
  action easy-ip port-preserved
```

IPsec 配置指引

1. WEB页面的VPN配置过程说明：

   登录设备WEB管理界面，在导航栏中选择“VPN > IPsec”。

   a. 配置IKE提议：选择新建IKE提议，指定认证方式、认证算法、加密算法、DH、生命周期与华为云参数相同。

   b. 配置IPsec策略：

      基本配置中选择设备角色为对等/分支节点，IP地址类型选择IPv4,接口选择外网接口，本地IP填写对接公网地址，对端IP地址填写华为云网关IP。

      IKE策略中，协商模式与预共享秘密选择与华为相同配置，ike提议调用已创建提议，本端ID与对端ID均选择IPv4地址类型，值键入对应的公网IP。

      保护数据流的源IP为本地私网网段，目的地址为华为云侧私网网段。

      高级配置IPsec参数中封装模式、安全协议、认证算法、加密算法、PFS、生存时间均需要与华为云配置一致，建议开通DPD按时检测。

   c. 配置安全策略：添加客户侧私网网段与华为云私网网段互访的安全策略，服务为ANY，动作pass，推荐置顶这两条安全策略规则。

   d. NAT策略：添加源地址为客户侧私网网段，目标为华为云私网网段动作为不做转换的nat规则，并将该规则置顶。

⚠ 注意

- 安全策略中需要添加本地公网IP与华为云网关IP的互访规则，协议为UDP的500、4500和IP协议ESP与AH，确保协商流和加密流数据正常传输。
- 不可以将公网IP的协商流进行NAT转发，需要确保本地公网IP访问华为云的流量不被NAT。
- 确保访问目标子网的路由指向公网出接口下一跳。
- 待加密数据流的网段请填写真实IP和掩码，请勿调用地址对象。
- 若客户侧网络存在多出口时，请确保客户侧访问华为云VPN网关IP及私网网段从建立连接的公网出口流出，推荐使用静态路由配置选择出口网络。

2. 命令行配置说明：

#增加地址对象

```
object-group ip address HWCloud_subnet192.168.10.0/24
0 network subnet 192.168.10.0 255.255.255.0
#
object-group ip address HWCloud_subnet192.168.20.0/24
0 network subnet 192.168.20.0 255.255.255.0
```

#配置一阶段提议，算法详情与华为云相同

```
ikev2 proposal 100
  encryption aes-cbc-128
  integrity sha256
  dh group14
  prf sha256
```

配置两端协商PSK，PSK两端相同

```
ikev2 keychain IPsec-KEY
  peer keypeername
    address 11.11.11.11 255.255.255.255
    pre-shared-key local plaintext ******
    pre-shared-key remote plaintext ******
```

#配置IKEV2的Profile，调用PSK，匹配两端公网IP

```
ikev2 profile IKE-PROFILE
  authentication-method local pre-share
  authentication-method remote pre-share
  keychain IPsec-KEY
  identity local address 22.22.22.22
  match local address 22.22.22.22
  match remote identity address 11.11.11.11 255.255.255.255
  sa duration 86400
```

配置ike policy，类同ike对等体配置，调用ike阶段提议并与接口IP进行关联

```
ikev2 policy IKE-PEER
  proposal 100
  match local address 22.22.22.22
```

配置感兴趣流

```
acl advanced 3999
  rule 0 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
  rule 1 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
  rule 2 permit ip source 172.16.30.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
  rule 4 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
  rule 5 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
  rule 6 permit ip source 172.16.30.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
```

#配置二阶段提议

```
IPsec transform-set IPsec-PH2
  encapsulation-mode tunnel
  esp authentication-algorithm sha256
```



```
  esp encryption-algorithm aes-cbc-128
  pfs dh-group14
```

#配置IPsec policy，调用感兴趣流和二阶段提议

```
IPsec policy IPsec-HW 1 isakmp
  transform-set IPsec-PH2
  security acl 3999
  local-address 22.22.22.22
  remote-address 11.11.11.11
  ikev2-profile IKE-PROFILE
  sa duration time-based 3600
```

#将IPsec policy绑定在协商接口下

```
interface GigabitEthernet1/0/1
  ip address 22.22.22.22 255.255.255.0
  tcp mss 1300
  IPsec apply policy IPsec-HW
```

#配置安全策略，放行两端私网的数据互访，放行公网IP间互访流量

```
security-policy ip
rule 1 name IPsec-OUT
 action pass
 logging enable
 counting enable
 source-zone Trust
 destination-zone Untrust
 source-ip Customer-subnet172.16.10.0/24
 source-ip Customer-subnet172.16.20.0/24
 source-ip Customer-subnet172.16.30.0/24
 destination-ip HWCloud_subnet192.168.10.0/24
 destination-ip HWCloud_subnet192.168.20.0/24
rule 2 name IPsec-IN
 action pass
 logging enable
 counting enable
 source-zone Untrust
 destination-zone Trust
 source-ip HWCloud_subnet192.168.10.0/24
 source-ip HWCloud_subnet192.168.20.0/24
 destination-ip Customer-subnet172.16.10.0/24
 destination-ip Customer-subnet172.16.20.0/24
 destination-ip Customer-subnet172.16.30.0/24
rule 3 name IPsec-NEG-pass
 action pass
 logging enable
 counting enable
 source-ip 11.11.11.11 255.255.255.255
 source-ip 22.22.22.22 255.255.255.255
 destination-ip 11.11.11.11 255.255.255.255
 destination-ip 22.22.22.22 255.255.255.255
rule 0 name Policy-Internet
……
```

#配置NAT策略，确保本地子网访问华为云子网no-nat

```
nat policy
rule name IPsec_NONAT
 source-ip Customer-subnet172.16.10.0/24
 source-ip Customer-subnet172.16.20.0/24
 source-ip Customer-subnet172.16.30.0/24
 destination-ip HWCloud_subnet192.168.10.0/24
 destination-ip HWCloud_subnet192.168.20.0/24
 outbound-interface GigabitEthernet1/0/1
 action no-nat
rule name Snat_Internet
……
```

#路由配置，访问华为云子网路由由公网接口流出

```
ip route-static 0.0.0.0 0 GigabitEthernet1/0/1 B.B.B.1
……
```


3. 使用ikev1协商差异化配置说明：

#无V2标识，算法有差异

```
ike proposal 100
  authentication-algorithm sha256
  encryption-algorithm aes-cbc-128
  authentication-method pre-share
  dh group14
  sa duration 86400
```

#无V2标识，一条命令完成协商PSK配置

```
ike keychain IPsec-KEY
  pre-shared-key address 11.11.11.11 255.255.255.255 key simple *******
```

#无V2标识，配置增加exchange-mode，直接调用一阶段提议，不用单独配置ike policy

```
ike profile IKE-PROFILE
  keychain IPsec-KEY
  local-identity address 22.22.22.22
  exchange-mode main     //aggressive
  dpd interval 3 periodic
  match remote identity address 11.11.11.11 255.255.255.255
  match local address 22.22.22.22
  proposal 100
```

功能验证

VPN连接配置完成后，云上不会主动触发隧道建立，需要数据流触发协商。

触发方式：私网间数据流，例如用192.168.10.0/24网段的主机去ping 172.16.10.0/24网段主机，反过来ping也可以。

⚠ 注意

用私网地址ping对端公网网关IP不触发隧道协商，例如172.16.10.0/24网段主机ping 11.11.11.11是不会触发隧道建立的。

2.9.2 HW-USG 防火墙(V5)对接华为云配置指引

华为云配置信息说明

VPN网关IP：11.11.11.11

VPC子网：192.168.10.0/24，192.168.20.0/24

客户侧网关IP：22.22.22.22

客户侧子网：172.16.10.0/24，172.16.20.0/24，172.16.30.0/24

协商策略详情：

一阶段策略（IKE Policy）

认证算法（Authentication Algorithm）: sha2-256

加密算法（Encryption Algorithm）: aes-128

版本（Version）: v2

DH算法（DH Algorithm ）: group14

生命周期（Life Cycle）: 86400

二阶段策略（IPsec Policy）

传输协议（Transfer Protocol）: esp

认证算法（Authentication Algorithm）: sha2-256

加密算法（Encryption Algorithm）: aes-128

完美前向安全（PFS）: DH-group14

生命周期（Life Cycle）: 86400

客户侧设备组网与基础配置假设

1. 假定客户侧基础网络配置如下：

内网接口：GigabitEthernet1/0/0 所属zone为Trust，接口IP为10.0.0.1/30。

预进行加密传输的子网为172.16.10.0/24，172.16.20.0/24，172.16.30.0/24，所属zone为Trust。

外网接口：GigabitEthernet1/0/1 所属zone为Untrust，接口IP为22.22.22.22/24。

缺省路由：目标网段0.0.0.0/0 出接口GE1/0/1，下一跳为GE1/0/1的网关IP为22.22.22.1。

安全策略：Trust访问Untrust，源地址、目标地址及服务均为any，动作放行。

NAT策略：源地址为内网网段，目标地址为ANY，动作为EasyIP，即转换为接口IP。

2. 基础配置命令行示意如下：

```
interface GigabitEthernet1/0/0
ip address 10.0.0.1 255.255.255.252
#
interface GigabitEthernet1/0/1
ip address 22.22.22.22 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 22.22.22.1
ip route-static 172.16.10.0 255.255.255.0 10.0.0.2
ip route-static 172.16.20.0 255.255.255.0 10.0.0.2
ip route-static 172.16.30.0 255.255.255.0 10.0.0.2
#
firewall zone trust
set priority 85
import interface GigabitEthernet1/0/0
#
firewall zone untrust
set priority 5
import interface GigabitEthernet1/0/1
#
ip address-set Customer-subnet172.16.10.0/24 type object
address 0 172.16.10.0 mask 24
#
ip address-set Customer-subnet172.16.20.0/24 type object
address 0 172.16.20.0 mask 24
#
ip address-set Customer-subnet172.16.30.0/24 type object
address 0 172.16.30.0 mask 24
#
security-policy
rule name Policy-Internet
 policy logging
 session logging
 source-zone trust
```



```
 destination-zone untrust
 action permit
#
nat-policy
rule name Snat_Internet
 source-zone trust
 egress-interface GigabitEthernet1/0/1
 action nat easy-ip
```

IPsec 配置指引

1. WEB页面VPN配置过程说明：

   登录设备WEB管理界面，在导航栏中选择“网络 > IPsec”，选择新建IPsec策略。

   a. 基本配置：命名策略，选择出接口为本端接口，本端地址为出接口公网IP，对端地址为华为云VPN网关IP，认证方式选择预共享密钥，密钥信息与华为云配置一致，本端ID及对端ID均选择IP地址。

   b. 待加密数据流：新建配置，源地址为客户侧子网网段，目标地址为华为云子网网段，多条子网请分开填写，填写的条目数为两端子网数量的乘积，协议选择any，动作允许。

   c. 安全提议：IKE参数与IPsec参数与华为云配置一致，注意IKE版本只勾选与华为云匹配的选项，推荐开启周期性DPD检测。

   d. 安全策略：添加客户侧私网网段与华为云私网网段互访的安全策略，服务为ANY，动作允许，推荐置顶这两条安全策略规则。

   e. NAT策略：添加源地址为客户侧私网网段，目标为华为云私网网段动作为不做转换的nat规则，并将该规则置顶。

   ⚠ 注意

   - 安全策略中需要添加本地公网IP与华为云网关IP的互访规则，协议为UDP的500、4500和IP协议ESP与AH，确保协商流和加密流数据正常传输。
   - 不可以将公网IP的协商流进行NAT转发，必须确保本地公网IP访问华为云的流量不被NAT。
   - 确保访问目标子网的路由指向公网出接口下一跳。
   - 待加密数据流的网段请填写真实IP和掩码，请勿调用地址对象。
   - 若客户侧网络存在多出口时，请确保客户侧访问华为云VPN网关IP及私网网段从建立连接的公网出口流出，推荐使用静态路由配置选择出口网络。

2. 命令行配置说明：

   #增加地址对象

```
ip address-set HWCloud_subnet192.168.10.0/24 type object
address 0 192.168.10.0 mask 24
#
ip address-set HWCloud_subnet192.168.20.0/24 type object
address 0 192.168.20.0 mask 24
```

   #配置一阶段提议，ike v1与ike v2的配置方式相同，ikev1使用认证、加密，ikev2使用加密、完整性、prf

```
ike proposal 100
authentication-algorithm sha2-256
encryption-algorithm aes-128
authentication-method pre-share
integrity-algorithm hmac-sha2-256
```



```
prf hmac-sha2-256
dh group14
sa duration 86400
```

#配置对等体，指定版本，调用一阶段提议（undo version 2时需要配置exchange-mode参数）

```
ike peer IKE-PEER
undo version 1
pre-shared-key ******
ike-proposal 100
remote-address 11.11.11.11
dpd type periodic
```

#配置感兴趣流

```
acl number 3999
rule 0 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
rule 1 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
rule 2 permit ip source 172.16.30.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
rule 4 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
rule 5 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
rule 6 permit ip source 172.16.30.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
```

#配置二阶段提议

```
IPsec proposal IPsec-PH2
transform esp
encapsulation-mode tunnel
esp authentication-algorithm sha2-256
esp encryption-algorithm aes-128
```

#配置IPsec policy，调用ike peer、二阶段提议、ACL，注意PFS配置

```
IPsec policy IPsec-HW 1 isakmp
proposal IPsec-PH2
security acl 3999
ike-peer IKE-PEER
tunnel local 22.22.22.22
pfs dh-group14
sa duration time-based 3600
```

#全局配置，设定TCP分片大小

```
firewall tcp-mss 1300
#IPsec policy 绑定接口
interface GigabitEthernet1/0/1
ip address B.B.B.Y 255.255.255.0
IPsec apply policy IPsec-HW
#
security-policy
rule name IPsec-OUT
policy logging
session logging
source-zone trust
destination-zone untrust
source-address address-set Customer-subnet172.16.10.0/24
source-address address-set Customer-subnet172.16.20.0/24
source-address address-set Customer-subnet172.16.30.0/24
destination-address address-set HWCloud_subnet192.168.10.0/24
destination-address address-set HWCloud_subnet192.168.20.0/24
action permit
rule name IPsec-IN
policy logging
session logging
source-zone untrust
destination-zone trust
source-address address-set HWCloud_subnet192.168.10.0/24
source-address address-set HWCloud_subnet192.168.20.0/24
destination-address address-set Customer-subnet172.16.10.0/24
destination-address address-set Customer-subnet172.16.20.0/24
destination-address address-set Customer-subnet172.16.30.0/24
action permit
rule name IPsec-NEG-pass
```



```
logging enable
counting enable
source-ip 11.11.11.11 255.255.255.255
source-ip 22.22.22.22 255.255.255.255
destination-ip 11.11.11.11 255.255.255.255
destination-ip 22.22.22.22 255.255.255.255
action permit
rule name Policy-Internet
......
#
nat policy
rule name IPsec_NONAT
description IPsec_NONAT
source-zone trust
destination-zone untrust
source-address address-set Customer-subnet172.16.10.0/24
source-address address-set Customer-subnet172.16.20.0/24
source-address address-set Customer-subnet172.16.30.0/24
destination-address address-set HWCloud_subnet192.168.10.0/24
destination-address address-set HWCloud_subnet192.168.20.0/24
action no-nat
rule name Snat_Internet
......
```

#路由配置，访问华为云子网路由由公网接口流出

```
ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet1/0/1 22.22.22.1
```

功能验证

VPN连接配置完成后，云上不会主动触发隧道建立，需要数据流触发协商。

触发方式：私网间数据流，例如用192.168.10.0/24网段的主机去ping 172.16.10.0/24网段主机，反过来ping也可以。

⚠ 注意

用私网地址ping对端公网网关IP不触发隧道协商，例如172.16.10.0/24网段主机ping 11.11.11.11是不会触发隧道建立的。

2.9.3 山石-G 防火墙(V5.5)对接华为云配置指引

华为云配置信息说明

VPN网关IP：11.11.11.11

VPC子网：192.168.10.0/24，192.168.20.0/24

客户侧网关IP：22.22.22.22

客户侧子网：172.16.10.0/24，172.16.20.0/24，172.16.30.0/24

协商策略详情：

一阶段策略（IKE Policy）

认证算法（Authentication Algorithm）: sha2-256

加密算法（Encryption Algorithm）: aes-128

版本（Version）: v1

DH算法（DH Algorithm ）: group14

生命周期（Life Cycle）: 86400

协商模式（Exchange-mode ）: main

二阶段策略（IPsec Policy）

传输协议（Transfer Protocol）: esp

认证算法（Authentication Algorithm）: sha2-256

加密算法（Encryption Algorithm）: aes-128

完美前向安全（PFS）： DH-group14

生命周期（Life Cycle）: 86400

客户侧设备组网与基础配置假设

内网接口：ethnet0/0 所属zone为Trust，接口IP为b.b.b.1/24。

外网接口：ethnet0/1 所属zone为Untrust，接口IP为B.B.B.Y/24。

缺省路由：目标网段0.0.0.0/0 出接口ethnet0/1，下一跳为ethnet0/1的网关IP,如B.B.B.1。

安全策略：Trust访问Untrust，源地址、目标地址及服务均为any，动作放行。

NAT策略：源地址为内网网段，目标地址为ANY，转换为出接口IP。

VPN 配置过程

登录设备WEB管理界面，在导航栏中选择“VPN > IPsec VPN”。

1. 配置P1提议：输入提议名称，选择认证方式为Pre-share，认证算法、加密算法和DH组等参数，详细参数参见**华为云配置信息说明**。
2. 配置P2提议：输入提议名称，协议选择、认证算法、加密算法和PFS等参数，详细参数参见**华为云配置信息说明**，不启用压缩和生存大小。
3. 配置VPN 对端列表：
   a. 基本配置：输入名称，选择公网接口ethnet0/1，选择协议标准（只支持V1版本）和认证模式，类型选择静态IP，对端IP地址键入华为云VPN网关IP地址11.11.11.11，本地ID选择IPv4 22.22.22.22，调用已配置好的P1提议并输入与华为云侧相同的预共享密钥。
   b. 高级配置：建议配置如下，连接类型选择双向，启用NAT穿越，开启对端存活检测，DPD间隔与重试时间默认即可，不启用XAUTH服务器。
4. 配置IKE VPN列表
   a. 基本配置：

      对端：调用对端列表已有配置；

      隧道：输入名称，模式选择tunnel，调用P2提议，代理ID选择手工，即配置感兴趣流，使用IP+掩码的格式进行配置配置的条目数等于本端子网与远端子网数量的乘积。
   b. 高级配置：选择默认配置即可，可以开启VPN隧道检测，源地址为本地私网IP和目标地址为华为云私网的IP（推荐选择真实可用地址）。

5. 接口配置：
   a. 在导航栏安全域下新建一个VPN的安全域，进行命名为VPN，类型选择三层安全域。
   b. 在导航栏接口下新建一隧道接口，完成名称编号，所属安全域（划入新建的VPN安全域）；IP配置选择静态IP，不填写IP信息；隧道类型为IPsec VPN，隧道绑定配置选择已创建的IKE VPN列表名称。
6. 安全策略，新建以下安全策略，并将该策略置顶。
   a. 新建源区域为trust，目标区域为VPN区域，服务为any，动作为允许。
   b. 新建源区域为VPN区域，目标区域为trust，服务为any，动作为允许。
7. 配置路由 目标网段为华为云私网（192.168.10.0/24，192.168.20.0/24），下一跳选择为接口，接口选择为VPN使用的tunnel口。

⚠ 注意

- 安全策略中需要添加本地公网IP与华为云网关IP的互访规则，协议为UDP的500、4500和IP协议ESP与AH，确保协商流和加密流数据正常传输。
- 代理ID（待加密数据流的网段）请填写真实IP和掩码，请勿调用地址对象。
- 若客户侧网络存在多出口时，请确保客户侧访问华为云VPN网关IP及私网网段从建立连接的公网出口流出，推荐使用静态路由配置选择出口网络。

功能验证

VPN连接配置完成后，深信服设备勾选主动连接后会主动发起协商，云上不会主动触发隧道建立。

华为云触发方式：私网间数据流触发，例如用192.168.10.0/24网段的主机去ping 172.16.10.0/24网段主机。

⚠ 注意

用私网地址ping对端公网网关IP不触发隧道协商，例如172.16.10.0/24网段主机ping 11.11.11.11是不会触发隧道建立的。

2.9.4 深信服-SSL-M7.6 对接华为云配置指引

华为云配置信息说明

VPN网关IP：11.11.11.11

VPC子网：192.168.10.0/24，192.168.20.0/24

客户侧网关IP：22.22.22.22

客户侧子网：172.16.10.0/24，172.16.20.0/24，172.16.30.0/24

协商策略详情：

一阶段策略（IKE Policy）

认证算法（Authentication Algorithm）: sha2-256

加密算法（Encryption Algorithm）: aes-128

版本（Version）: v1

DH算法（DH Algorithm ）: group14

生命周期（Life Cycle）: 86400

协商模式（Exchange-mode ）: main

二阶段策略（IPsec Policy）

传输协议（Transfer Protocol）: esp

认证算法（Authentication Algorithm）: sha2-256

加密算法（Encryption Algorithm）: aes-128

完美前向安全（PFS）： DH-group14

生命周期（Life Cycle）: 86400

客户侧设备组网与基础配置假设

部署模式：网关模式。

内网接口：LAN 接口IP为192.168.10.1/24。

外网接口：线路1 即WAN1 接口IP为22.22.22.22/24。

缺省路由：线路1的网关IP,如22.22.22.1。

防火墙规则：LAN访问WAN，源地址、目标地址及服务均为any，动作通过。

代理上网网段配置：源接口LAN，源地址为内网网段，目的接口WAN1目标地址为All IP，转换为目的接口地址。

VPN 配置过程

登录设备WEB管理界面，在控制台中选择“IPsec VPN配置 > 第三方对接配置”。

1. 安全提议：即配置二阶段提议，选择新增，弹出页签输入名称，协议、认证算法和加密算法与华为云保持一致（参见**华为云配置信息说明**）。
2. 第一阶段：
   a. 基本配置：右侧选择新增，弹出页签键入名称，选择线路为出公网线路1，设备地址类型为对端固定IP，固定IP填写11.11.11.11，认证方式选择预共享密钥，并键入预共享密钥，勾选启用设备和启用主动连接。
   b. 高级配置：在基本页面左下角选择高级，在新弹出页签中配置存活时间、支持模式、D-H群、认证算法、加密算法等参数与华为云一致，推荐勾选启用DPD，间隔与次数保持默认即可。
   c. 特殊配置：深信服存在NAT穿越时，只能使用野蛮模式进行对接，且深信服设备不支持IKEv2，在选择野蛮模式时请设置深信服的身份ID为IPv4公网IP，即NAT之后的公网IP。
3. 第二阶段：

a. 入站策略：选择新增，弹出页签键入名称，源IP类型选择子网+掩码，一次输入一个华为云私网网段（192.168.10.0/24，192.168.20.0/24），服务选择所有服务，生效时间选择全天，勾选启用该策略。

b. 出站策略：选择新增，弹出页签键入名称，源IP类型选择子网+掩码，一次输入一个本地私网网段（172.16.10.0/24，172.16.20.0/24，172.16.30.0/24），对端设备调用已配置的第一阶段提议，生命周期与华为云相同，服务选择所有服务，生效时间选择全天，勾选启用该策略，安全选项调用已配置的安全提议，勾选启用该策略和密钥完美向前保密（PFS）。

c. 特殊配置：勾选PFS后二阶段D-H组与第一阶段相同，云下存在多个子网网段时，每一个出站策略均需要配置对端设备、安全选项和PFS。

4. 防火墙规则设置：增加VPN-LAN，LAN-VPN的互访放行策略，服务分别为all-tcp，all-udp，ping。

⚠ 注意

- 安全策略中需要添加本地公网IP与华为云网关IP的互访规则，协议为UDP的500、4500和IP协议ESP与AH，确保协商流和加密流数据正常传输。
- 待加密数据流的网段请填写真实IP和掩码，请勿调用地址对象。
- 若客户侧网络存在多出口时，请确保客户侧访问华为云VPN网关IP及私网网段从建立连接的公网出口流出，推荐使用静态路由配置选择出口网络。

功能验证

VPN连接配置完成后，深信服设备勾选主动连接后会主动发起协商，云上不会主动触发隧道建立。

华为云触发方式：私网间数据流触发，例如用192.168.10.0/24网段的主机去ping 172.16.10.0/24网段主机。

⚠ 注意

用私网地址ping对端公网网关IP不触发隧道协商，例如172.16.10.0/24网段主机ping 11.11.11.11是不会触发隧道建立的。

3 终端入云 VPN

3.1 通过云证书管理服务 CCM 托管服务端证书

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”进入“终端入云VPN网关”页面，单击目标VPN网关操作列的“配置服务端”。

步骤6 在“服务端”界面，选择“服务端证书”，在下拉选项中单击“上传证书”进入“云证书管理服务”页面。

步骤7 在“SSL证书管理”页面，选择“上传证书 > 上传证书”，根据界面提示填写相关信息。

上传证书参数请参见**表 上传国际标准证书参数说明**。

表 3-1 上传国际标准证书参数说明

参数	说明
证书标准	选择国际标准证书。
证书名称	用户自定义。
企业项目	将上传的SSL证书分配至对应的企业项目中。

参数	说明
证书文件	以文本编辑器（如Notepad++）打开待上传证书里的CER或CRT格式的文件，将证书内容复制到此处。 按照“服务端证书--CA证书”的顺序依次排列上传。 **说明** 用户如果没有现成的证书，可以采用自签发的方式生成证书，然后上传。证书文件请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。 上传证书文件格式如**图 证书上传格式**。
证书私钥	以文本编辑器（如Notepad++）打开待上传证书里的KEY格式的文件，将私钥内容复制到此处。 仅上传服务端证书私钥。 上传证书私钥格式如**图 证书上传格式**。

图 3-1 证书上传格式

说明

服务端证书的CN必须是域名格式。

步骤8 单击“确定”，完成上传证书。

步骤9 查看证书列表，确认证书状态为“托管中”。

----结束

3.2 通过 Easy-RSA 自签发证书（服务端和客户端共用 CA 证书）

场景描述

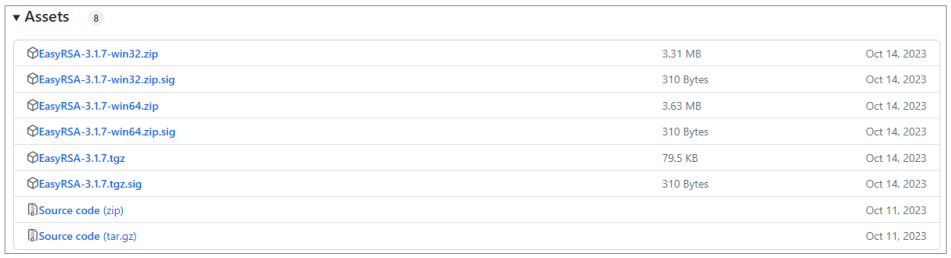
Easy-RSA是一个开源的证书管理工具，用于帮助用户生成和管理数字证书。

本示例介绍在Windows操作系统中，通过Easy-RSA自签发证书，服务端和客户端共用CA证书。本示例使用的软件版本为Easy-RSA 3.1.7，不同软件版本之间可能存在差异，具体请参考官方指导说明。

操作步骤

1. 根据Windows操作系统下载Easy-RSA安装包至“D:\”目录下。
   - Windows 32位操作系统，可以下载**EasyRSA-3.1.7-win32.zip**。
   - Windows 64位操作系统，可以下载**EasyRSA-3.1.7-win64.zip**。

   此处以安装EasyRSA-3.1.7-win64为示例。

2. 解压缩“EasyRSA-3.1.7-win64.zip”至指定目录，如“D:\EasyRSA-3.1.7”。
3. 进入“D:\EasyRSA-3.1.7”目录。
4. 在地址栏中输入**cmd**并按回车键，打开命令行窗口。
5. 执行“**.\EasyRSA-Start.bat**”命令，运行Easy-RSA。

   系统显示如下类似信息：

   ```
   Welcome to the EasyRSA 3 Shell for Windows.
   Easy-RSA 3 is available under a GNU GPLv2 license.

   Invoke './easyrsa' to call the program. Without commands, help is displayed.

   EasyRSA Shell
   #
   ```

6. 执行“**./easyrsa init-pki**”命令，初始化PKI环境。

   系统显示如下类似信息：

   ```
   Notice
   ------
   'init-pki' complete; you may now create a CA or requests.

   Your newly created PKI dir is:
   * D:/EasyRSA-3.1.7/pki

   Using Easy-RSA configuration:
   * undefined


   EasyRSA Shell
   #
   ```

   执行命令后，在“D:\EasyRSA-3.1.7”的目录下自动生成了“pki”的文件夹。

7. 配置变量参数。
   a. 将“D:\EasyRSA-3.1.7”目录下的“vars.example”文件复制到“D:\EasyRSA-3.1.7\pki”目录下。
   b. 将“D:\EasyRSA-3.1.7\pki”目录下的“vars.example”重命名为“vars”。

说明

默认按“vars.example”中描述的参数值进行配置。如需自定义参数值，按需设置“vars”文件的参数值。

8. 执行“**./easyrsa build-ca nopass**”命令，生成CA证书。

   系统显示如下类似信息：

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
.....+..+.............+......+........+...+...+....++++++++++++++++++++++++++++++++++++++++++++
+*.+.+.....+..........+...........+...++++++++++++++++++++++++++++++++++++++++
+*.............+.....+......+...+....+..+.........+.....+....+..............+..+........+.............+......+..+..+...+....+..+.+.....+.....+.....+....+.....
.....+...+...+.....+........................+...+.+.....+....+...+.........+...+...+...+.....+......+........................++++++
.++++++++++++++++++++++++++++++++++++++++*.........+..........++++++++++++++++++++++++++++++++
+++++++*.+......++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:p2cvpn.com    //设置CA证书名称

Notice
------
CA creation complete. Your new CA certificate is at:
* D:/EasyRSA-3.1.7/pki/ca.crt


EasyRSA Shell
#
```

9. 查看CA证书及其私钥。
   - 生成的CA证书默认存放在“D:\EasyRSA-3.1.7\pki”目录下。

     本示例中生成的证书为“ca.crt”。
   - 生成的CA私钥默认存放在“D:\EasyRSA-3.1.7\pki\private”目录下。

     本示例中生成的私钥为“ca.key”。
10. 执行“**./easyrsa build-server-full** *p2cserver.com* **nopass**”命令，生成服务端证书及其私钥。

    此命令中，*“p2cserver.com”*为服务端证书的CN，必须是域名格式，如“p2c-server.com”。否则无法正常托管到云证书管理服务,请根据实际填写。

    系统显示如下类似信息：

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
.+.............+........+.............+.............+.+................+.....+....+.....................+.............+.+..+......+.............+....+.........+..+.........+.+.....
....+..............+.........++++++++++++++++++++++++++++++++++++++++++++*...+......+.....+......+...+++++++++++++++
++++++++++++++++++++++++
+*..+...+..........+......+...........+....+......+.....+....+.....+....+.........+...+.......+...+..+.......+..+.....+..............+..+....+.....+...+.....+.....
..........+......+..+..............+..+................+.....+......+....+...........+....+.....+.........+.+..+.............+...........+..........+......+.........+.....
...+...+....+..+.....+.....................+.....+.....+.+...+..+...+.+.....+.........+...+....+.....+.....+....+...+..+.................+..+...+.......+..+....
..+..........+.........+...+..+.........+......+......++++++
.........+.+......+...+.....+.....+...+.+.....+.+.........+......++++++++++++++++++++++++++++++++++++++++++++
+*...+.....+...+.+.........+.......+.........++++++++++++++++++++++++++++++++++++++++++++
+*.....+.........+.+...+.....+.+..............+.+.....+.+...+...+.....+.......+..................+.+.............+..+......+...+....+...+..+.+.....+.....................
```



```
...+.+..+.+.....+....+.....+.....+.....+....+.....+...+.....+.....+.+.....+...+.....+.....+....+.....+.....+.
.....+..+.....+.....+.+.....+...+.....+.....+.....+.....+.....+.....+.....+.....+.....+...+.+...+
..+...+.+.....+.+.....+.....+.....+..+....+..+....+.....+.....+.....+...+...+.+...+...+..+.....+...+.....+..+.
.....+.....+.....+.....+.....+.....+...+.....+.....+.....+...+.....+.+.....+.+...+.....+.+...+...+...+.....+..+.....+..
.....+.....+...+...+.....+.....+...+....+.....+.....+...+.....+.....+.....+.+.....+....+.....+.+..+.....+.....
..+...+.....+.+...+.....+.+.....+...++++++
-----

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: D:/EasyRSA-3.1.7/pki/reqs/p2cserver.com.req
* key: D:/EasyRSA-3.1.7/pki/private/p2cserver.com.key

You are about to sign the following certificate:
Request subject, to be signed as a server certificate
for '825' days:

subject=
    commonName                = p2cserver.com

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes    //输入“yes”以继续

Using configuration from D:/EasyRSA-3.1.7/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'p2cserver.com'
Certificate is to be certified until Sep 22 09:56:54 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* D:/EasyRSA-3.1.7/pki/issued/p2cserver.com.crt

Notice
------
Inline file created:
* D:/EasyRSA-3.1.7/pki/inline/p2cserver.com.inline


EasyRSA Shell
#
```

11. 查看服务端证书及其私钥。
    - 生成的服务端证书默认存放在“D:\EasyRSA-3.1.7\pki\issued”目录下。
      本示例中生成的服务端证书为“p2cserver.com.crt”。
    - 生成的服务端私钥默认存放在“D:\EasyRSA-3.1.7\pki\private”目录下。
      本示例中生成的服务端私钥为“p2cserver.com.key”。
12. 执行“**./easyrsa build-client-full** *p2cclient.com* **nopass**”命令，生成客户端证书及其私钥。

    此命令中，客户端证书的命名（如*“p2cclient.com”*）应与服务端证书的命名（如*“p2cserver.com”*）不一致。

    系统显示如下类似信息：

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
```



```
.....++++++++++++++++++++++++++++++++++++++++*...+...+...+.....+...+....+......+......+........+.+.....+............++++
++++++++++++++++++++++++++++++++
+*.+.....+.+.....+.........+.......+..+...+.......+...+..+......+.+......+........+....+...+..+...+..+.+.......+.....+.....+.....+
.........+......+.+..+...+.........+........+......+....+.....+.....+...........+.......+.....+.....+.....+..+.+...........+.....+.+.....
+.........+.+..............+..+.........+...+...........+...+.....+.+..........+....+.....+.........+....+.....+....+.....+.....+...+.
............+.....+.............+.+........+.......+.....+....+.........+..+............+..........+..+.............+...+...+..++++++
..+.....+.......+.....+.........+....++++++++++++++++++++++++++++++++++++++++++++*.....+......+..+++++++++++++++++
++++++++++++++++++++++
+*.......+.+.....+....+.........+...+.....+.........+...+................+...+....+.....+.+...+......+......+...+.........+..+...+...+....+.........+..+...+.....
.............+......+.....+.+...+...+.........+.....+...................+...+...+......+.+..+......+.+......+.....+...+...........+..+............+.......+.........+.....
+.....+.+..+.............+.................+..+...+....+......+.....+...+....+..+......+.........+.........++++++
-----

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: D:/EasyRSA-3.1.7/pki/reqs/p2cclient.com.req
* key: D:/EasyRSA-3.1.7/pki/private/p2cclient.com.key

You are about to sign the following certificate:
Request subject, to be signed as a client certificate
for '825' days:

subject=
    commonName                = p2cclient.com

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes    //输入“yes”以继续

Using configuration from D:/EasyRSA-3.1.7/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'p2cclient.com'
Certificate is to be certified until Sep 22 09:58:26 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* D:/EasyRSA-3.1.7/pki/issued/p2cclient.com.crt

Notice
------
Inline file created:
* D:/EasyRSA-3.1.7/pki/inline/p2cclient.com.inline


EasyRSA Shell
#
```

13. 查看客户端证书及其私钥。
    - 生成的客户端证书默认存放在“D:\EasyRSA-3.1.7\pki\issued”目录下。本示例中生成的客户端证书为“p2cclient.com.crt”。
    - 生成的客户端私钥默认存放在“D:\EasyRSA-3.1.7\pki\private”目录下。本示例中生成的客户端私钥为“p2cclient.com.key”。

3.3 通过 Easy-RSA 自签发证书（服务端和客户端使用不同 CA 证书）

场景描述

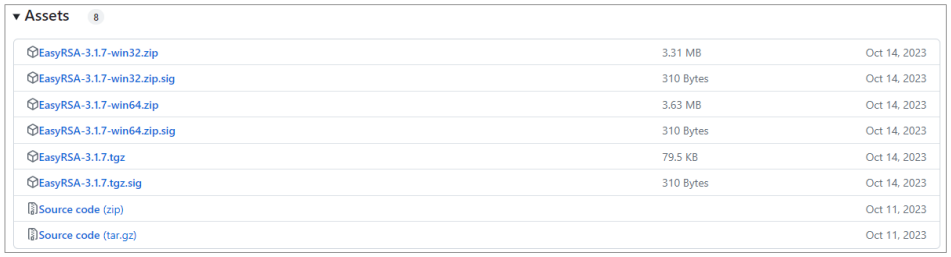
Easy-RSA是一个开源的证书管理工具，用于帮助用户生成和管理数字证书。

本示例介绍在Windows操作系统中，通过Easy-RSA自签发证书，服务端和客户端使用不同CA证书。本示例使用的软件版本为Easy-RSA 3.1.7，不同软件版本之间可能存在差异，具体请参考官方指导说明。

操作步骤

1. 根据Windows操作系统下载Easy-RSA安装包至“D:\”目录下。
   - Windows 32位操作系统，可以下载**EasyRSA-3.1.7-win32.zip**。
   - Windows 64位操作系统，可以下载**EasyRSA-3.1.7-win64.zip**。

   此处以安装EasyRSA-3.1.7-win64为示例。

2. 解压缩“EasyRSA-3.1.7-win64.zip”至指定目录，如“D:\EasyRSA-3.1.7”。
3. 进入“D:\EasyRSA-3.1.7”目录。
4. 在地址栏中输入**cmd**并按回车键，打开命令行窗口。
5. 执行“**.\EasyRSA-Start.bat**”命令，运行Easy-RSA。

   系统显示如下类似信息：

   ```
   Welcome to the EasyRSA 3 Shell for Windows.
   Easy-RSA 3 is available under a GNU GPLv2 license.

   Invoke './easyrsa' to call the program. Without commands, help is displayed.

   EasyRSA Shell
   #
   ```

6. 执行“**./easyrsa init-pki**”命令，初始化PKI环境。

   系统显示如下类似信息：

   ```
   Notice
   ------
   'init-pki' complete; you may now create a CA or requests.

   Your newly created PKI dir is:
   * D:/EasyRSA-3.1.7/pki

   Using Easy-RSA configuration:
   * undefined


   EasyRSA Shell
   #
   ```

执行命令后，在“D:\EasyRSA-3.1.7”的目录下自动生成了“pki”的文件夹。

7. 配置变量参数。
   a. 将“D:\EasyRSA-3.1.7”目录下的“vars.example”文件复制到“D:\EasyRSA-3.1.7\pki”目录下。
   b. 将“D:\EasyRSA-3.1.7\pki”目录下的“vars.example”重命名为“vars”。

      说明

      默认按“vars.example”中描述的参数值进行配置。如需自定义参数值，按需设置“vars”文件的参数值。

8. 生成服务端CA证书认证及其私钥。
   a. 复制解压缩后的“EasyRSA-3.1.7”文件夹至“D:\”目录下，并重命名，如“EasyRSA-3.1.7 - server”。
   b. 进入“D:\EasyRSA-3.1.7 - server”目录。
   c. 在“D:\EasyRSA-3.1.7 - server”的文件夹中，地址栏中输入**cmd**并按回车键，打开命令行窗口。
   d. 执行“**.\EasyRSA-Start.bat**”命令，运行Easy-RSA。

      系统显示如下类似信息：

      ```
      Welcome to the EasyRSA 3 Shell for Windows.
      Easy-RSA 3 is available under a GNU GPLv2 license.

      Invoke './easyrsa' to call the program. Without commands, help is displayed.

      EasyRSA Shell
      #
      ```

   e. 执行“**./easyrsa build-ca nopass**”命令，生成服务端CA证书。

      此命令生成中，**[Easy-RSA CA]**需要设置服务端CA证书名称，例如：**p2cvpn_server.com**。

      系统显示如下类似信息：

      ```
      Using Easy-RSA 'vars' configuration:
      * D:/EasyRSA-3.1.7 - server/pki/vars

      Using SSL:
      * openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
      ..+.....+...+..........+..+.......+..+.........+...+...+..+.....+.......+...++++++++++++++++++++++++++++++++++++++++
      ++*.++++++++++++++++++++++++++++++++++++++++*.........+..........+...+......++++++
      .......+.......+...+......+...+.....+...+...++++++++++++++++++++++++++++++++++++++
      +*......+.....+....+..+....+......+...+......+...+......+.....+.++++++++++++++++++++++++++++++++++++
      +*.......+......+.......+..............+.+...+.....+....+........+.........+....+..+.....+.....+....+.
      ..+.................+.......+..+.......+.....+..........+......+..+.+.....+.+.....+....+.....+.....+...+.....+...+.....+...+.....+...
      ...+......+..........+....+.....+...+..+...+.....+...+.+.....+.......+..+.......+...+...+..+..............+........+.........+.+.........+........+....+
      .........+.....+.........+..............+.....+.+........+.......+.....+.+........+....+..+...+..........+..+......+...+.........+..............+......+....
      .+....+......+......+............+..+......+...+.......+.................+.+......+......+..+.+...........+.........+.........+.+......++++++
      -----
      You are about to be asked to enter information that will be incorporated
      into your certificate request.
      What you are about to enter is what is called a Distinguished Name or a DN.
      There are quite a few fields but you can leave some blank
      For some fields there will be a default value,
      If you enter '.', the field will be left blank.
      -----
      Common Name (eg: your user, host, or server name) [Easy-RSA CA]:p2cvpn_server.com    //设置服务端CA证书名称

      Notice
      ------
      CA creation complete. Your new CA certificate is at:
      * D:/EasyRSA-3.1.7 - server/pki/ca.crt
      ```



```
EasyRSA Shell
#
```

9. 查看服务端CA证书及其私钥。
   - 生成的服务端CA证书默认存放在“D:\EasyRSA-3.1.7 - server\pki”目录下。
     本示例中生成的服务端证书为“ca.crt”。
   - 生成的服务端CA私钥默认存放在“D:\EasyRSA-3.1.7 - server\pki\private”目录下。
     本示例中生成的服务端私钥为“ca.key”。
10. 执行“**./easyrsa build-server-full** *p2cserver.com* **nopass**”命令，生成服务端证书及其私钥。

    此命令中，*“p2cserver.com”*为服务端证书的CN，必须是域名格式，否则无法正常托管到云证书管理服务。请根据实际填写。

    系统显示如下类似信息：

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7 - server/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
.+.+.....+...+.....+.....+...+.....+.....+.+...+..+...+....+.....+.....++++++++++++++++++++++++++++++++++++++++++++
+*....+..+....++++++++++++++++++++++++++++++++++++++++
+*.................+.......+..+.+..+...+.....+.............+...+...+.........+........+.........+...+......+.+...+...+.....+...+.
...+...........+....+..+......+.............+.........+........+...+.+......+.....+.....+.....+.....+.+.....+....+.....+...+.....+...+..+.....+.+........+.........
+.+..+.........+.....+...+....+.....+.....+....+.....+.....+.....+.....+.....+.....+...+........+.+.....+.+.....................+.......+.....+.+..+.......+...+++
+++
......+.....+...+.+.........+..+.+..+...+++++++++++++++++++++++++++++++++++++++++++++*.......+...+........+....+...+..+...+++
++++++++++++++++++++++++++++++++++++
+*..+.........+...+.......+......+..................+...+...+............+...+....+........+.........+..........+......+...+...........+.+..+.............+.+........+....
+...........+....+...........+......+.............+......+.....++++++
-----

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: D:/EasyRSA-3.1.7 - server/pki/reqs/p2cserver.com.req
* key: D:/EasyRSA-3.1.7 - server/pki/private/p2cserver.com.key

You are about to sign the following certificate:
Request subject, to be signed as a server certificate
for '825' days:

subject=
    commonName                = p2cserver.com

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes    //输入“yes”以继续

Using configuration from D:/EasyRSA-3.1.7 - server/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'p2cserver.com'
Certificate is to be certified until Oct  6 03:28:14 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* D:/EasyRSA-3.1.7 - server/pki/issued/p2cserver.com.crt
```



```
Notice
------
Inline file created:
* D:/EasyRSA-3.1.7 - server/pki/inline/p2cserver.com.inline


EasyRSA Shell
#
```

11. 查看服务端证书及其私钥。
    - 生成的服务端证书默认存放在“D:\EasyRSA-3.1.7 - server\pki\issued”目录下的“issued”文件夹中。

      本示例中生成的服务端证书为“p2cserver.com.crt”。
    - 生成的服务端私钥默认存放在“D:\EasyRSA-3.1.7 - server\pki\private”目录下的“private”文件夹中。

      本示例中生成的服务端私钥为“p2cserver.com.key”。
12. 生成客户端CA证书认证及其私钥。
    a. 复制解压缩后的“EasyRSA-3.1.7”文件夹至“D:\”目录下，并重命名，如“EasyRSA-3.1.7 - client”
    b. 进入“EasyRSA-3.1.7 - client”目录。
    c. 在“EasyRSA-3.1.7 - client”的文件夹中，地址栏中输入**cmd**并按回车键，打开命令行窗口。
    d. 执行“**.\EasyRSA-Start.bat**”命令，运行Easy-RSA。

       系统显示如下类似信息：

       ```
       Welcome to the EasyRSA 3 Shell for Windows.
       Easy-RSA 3 is available under a GNU GPLv2 license.

       Invoke './easyrsa' to call the program. Without commands, help is displayed.

       EasyRSA Shell
       #
       ```
    e. 执行“ **./easyrsa build-ca nopass**”命令，生成客户端CA证书。

       系统显示如下类似信息：

       ```
       Using Easy-RSA 'vars' configuration:
       * D:/EasyRSA-3.1.7 - client/pki/vars

       Using SSL:
       * openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
       .++++++++++++++++++++++++++++++++++++++++
       +*.....+.+..+...+....+.....................+..+...+....+.........+.....+......+.+.....+....+++++++++++++++++++++++++++++++++++++++++*....+...+...+...+.............+.........++++++
       .+.........+.........+.+......+...........+....+.....+.........+....+..+...+.+.........+......+......+...+.....+......+.....+..........++++++++++
       ++++++++++++++++++++++++++++++*.+.........+......+.++++++++++++++++++++++++++++++++++++++++++++
       ++*...........+.................+..............+.........+.+...+.....................+..+....+.....+...........+...+...+..+.++++++
       -----
       You are about to be asked to enter information that will be incorporated
       into your certificate request.
       What you are about to enter is what is called a Distinguished Name or a DN.
       There are quite a few fields but you can leave some blank
       For some fields there will be a default value,
       If you enter '.', the field will be left blank.
       -----
       Common Name (eg: your user, host, or server name) [Easy-RSA CA]:p2cvpn_client.com    //设置客户端CA证书名称

       Notice
       ------
       CA creation complete. Your new CA certificate is at:
       ```



```
* D:/EasyRSA-3.1.7 - client/pki/ca.crt


EasyRSA Shell
#
```

13. 查看客户端CA证书及其私钥。
    - 生成的客户端CA证书默认存放在“D:\EasyRSA-3.1.7 - client\pki”目录下。

      本示例中生成的客户端证书为“ca.crt”。
    - 生成的客户端CA私钥默认存放在“D:\EasyRSA-3.1.7 - client\pki\private”目录下。

      本示例中生成的客户端私钥为“ca.key”。
14. 执行“**./easyrsa build-client-full** *p2cclient.com* **nopass**”命令，生成客户端证书及其私钥。

    此命令中，客户端证书的命名（如*“p2cclient.com”*）应与服务端证书的命名（如*“p2cserver.com”*）不一致。

    系统显示如下类似信息：

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7 - client/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
.+++++++++++++++++++++++++++++++++++++++*.........+.....+...+.+........+.+.....+..........+.+......+.....+++++++++++
++++++++++++++++++++++++++++
+*.........+...+...+..+.......+...+..+.+.........+.....+.+..+.+.....................+......+..............+.............+......+..+....+...+......+..+....+.....+..
.......+................+...+...+.....+....+.........++++++
.+..+..........+.........++++++++++++++++++++++++++++++++++++++++*...+..++++++++++++++++++++++++++++
++++++++++++*.......+................+......+.........+..............+....+.....+...+...................+....+...+........+....+.....+.+.....+...............++
++++
-----

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: D:/EasyRSA-3.1.7 - client/pki/reqs/p2cclient.com.req
* key: D:/EasyRSA-3.1.7 - client/pki/private/p2cclient.com.key

You are about to sign the following certificate:
Request subject, to be signed as a client certificate
for '825' days:

subject=
    commonName                = p2cclient.com

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes

Using configuration from D:/EasyRSA-3.1.7 - client/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'p2cclient.com'
Certificate is to be certified until Oct  7 11:19:52 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* D:/EasyRSA-3.1.7 - client/pki/issued/p2cclient.com.crt

Notice
```



```
------
Inline file created:
* D:/EasyRSA-3.1.7 - client/pki/inline/p2cclient.com.inline


EasyRSA Shell
#
```

15. 查看客户端证书和私钥。
    - 生成的客户端证书默认存放在“D:\EasyRSA-3.1.7 - client\pki\issued”目录下。

      本示例中生成的客户端证书为“p2cclient.com.crt”。
    - 生成的客户端私钥默认存放在“D:\EasyRSA-3.1.7 - client\pki\private”目录下。

      本示例中生成的客户端私钥为“p2cclient.com.key”。

3.4 通过云证书管理服务 CCM 购买证书

背景信息

用户除向CA机构申购证书、自签发证书渠道外，也可以通过云证书管理服务购买证书。支持同时购买服务端和客户端证书，也支持单独购买服务端或客户端证书。

约束条件

通过云证书管理服务购买服务端证书，需要在客户端配置文件中增加服务端根证书内容。

操作步骤

- 购买服务端证书
  a. 登录CCM控制台。
  b. **购买SSL证书**。
  c. **申请SSL证书**。

     从云证书管理服务购买的证书会自动托管，无需手动操作。
  d. **下载根证书**。
  e. 安装根证书。

     将根证书以文本编辑器（如Notepad++）打开，复制证书内容到客户端配置文件中已有CA证书后面，在客户端配置文件中增加服务端根证书的方式请参考**如何解决SSL证书链不完整?** 。

     安装服务端根证书如下所示：

     ```
     ....
     <ca>
     -----BEGIN CERTIFICATE-----
     客户端默认自带服务端二级CA证书
     -----END CERTIFICATE-----
     -----BEGIN CERTIFICATE-----
     服务端根证书
     -----END CERTIFICATE-----
     </ca>
     ...
     ```
- 购买客户端证书

a. 登录CCM控制台。
b. **购买SSL证书**。
c. **申请SSL证书**。
d. **下载SSL证书**。

