虚拟专用网络

管理员指南

文档版本	01
发布日期	2025-11-13

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。

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）

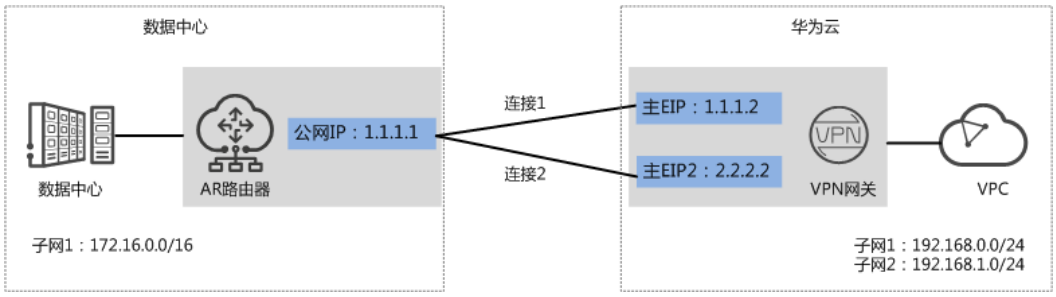
1.1.1 静态路由模式

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和该IP地址创建一组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	“连接1配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30	
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：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

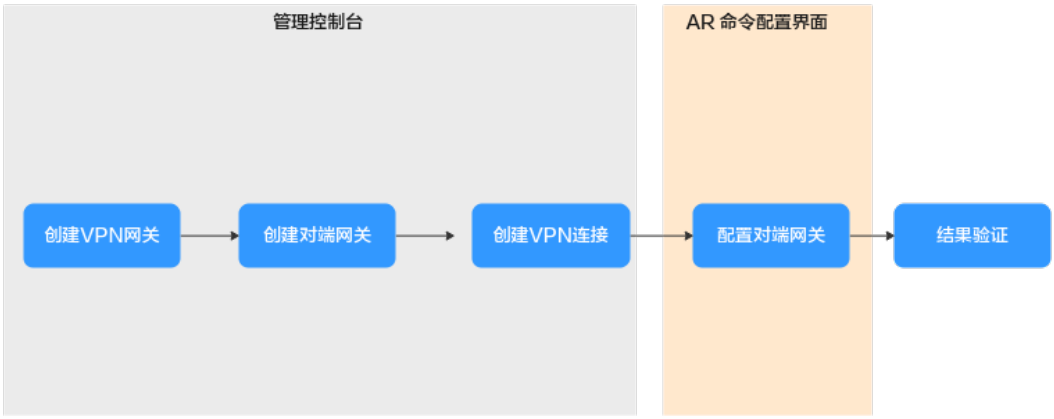


表 1-2 操作流程说明

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VPN连接**	• VPN网关的主EIP、主EIP2和连接1对端网关、连接2对端网关创建一组VPN连接。 • 预共享密钥、IKE/IPsec策略需要和AR路由器连接配置保持一致。
4	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。
5	-	**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“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创建一组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VPN连接。
   VPN连接参数说明如**表1-5**所示。

表 1-5 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
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
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、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*

参数	说明	取值参数
接口地址分配方式	– 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。	169.254.70.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.2/30
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 ▪ 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
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

----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 169.254.70.2 255.255.255.252
[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 169.254.71.2 255.255.255.252
[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 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.2
[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 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.2
[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。

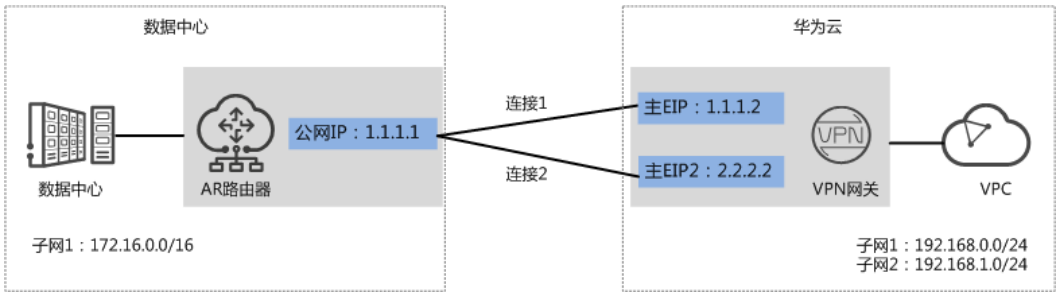
1.1.2 BGP 路由模式

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和该IP地址创建一组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 1-6 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	“连接1配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30	
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：169.254.71.2/30	

部件	参数项	AR路由器规划示例	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：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 1-4 操作流程

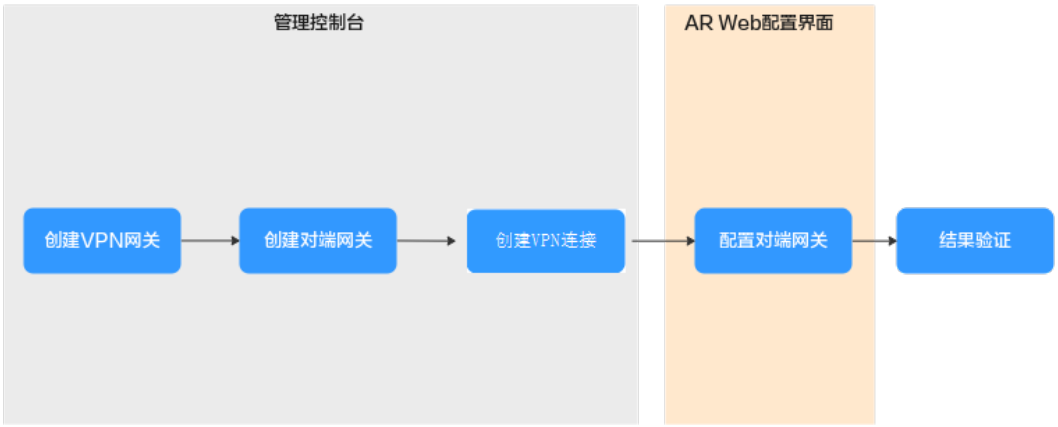


表 1-7 操作流程说明

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。

序号	在哪里操作	步骤	说明
3		创建VPN连接	• VPN网关的主EIP、主EIP2和连接1对端网关、连接2对端网关创建一组VPN连接。 • 连接2配置的连接模式、预共享密钥、IKE/IPsec策略建议和连接1配置保持一致。
4	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。
5	-	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“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 1-8 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)

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。	192.168.0.0/24 192.168.1.0/24
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 对端网关参数说明**所示。

表 1-9 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创建一组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VPN连接。
   VPN连接参数说明如**表1-10**所示。

表 1-10 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
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1

参数	说明	取值参数
连接2网关IP	选择VPN网关的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
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、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 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。	169.254.70.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.2/30
预共享密钥、确认密钥	和AR路由器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AR路由器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
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

----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。

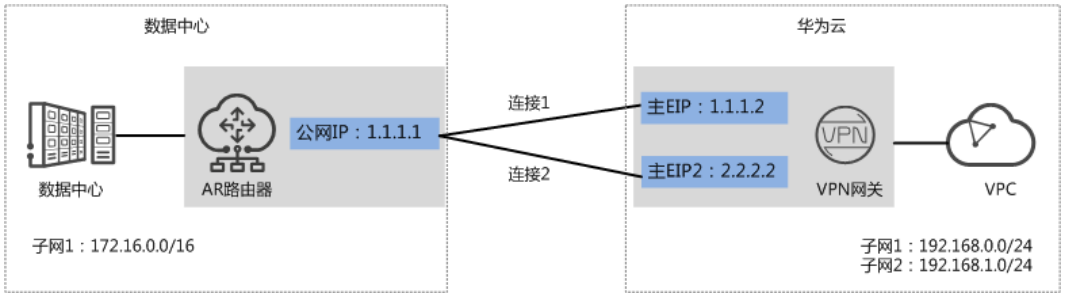
1.1.3 策略模式

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和该IP地址创建一组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 1-11 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

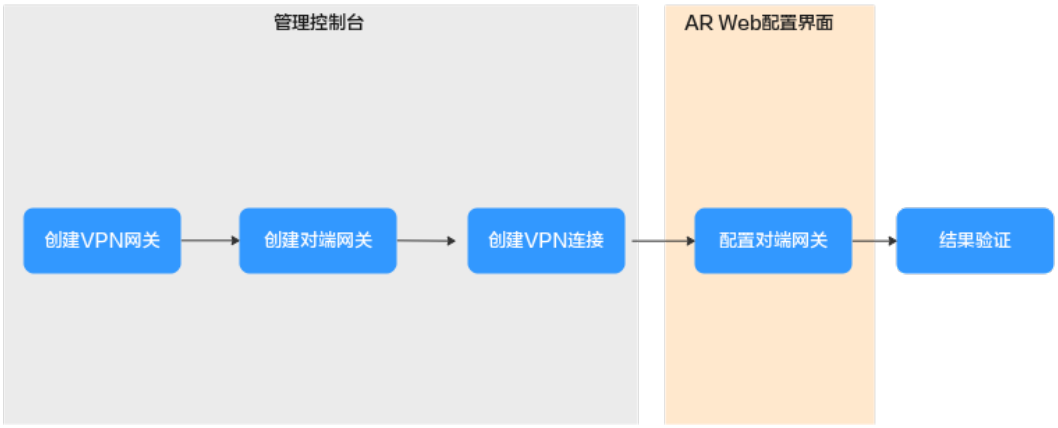


表 1-12 操作流程说明

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VPN连接**	• VPN网关的主EIP、主EIP2和连接1对端网关、连接2对端网关创建一组VPN连接。 • 连接2配置的连接模式、预共享密钥、IKE/IPsec策略建议和连接1配置保持一致。
4	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。
5	-	**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“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 1-13 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 1-14 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创建一组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 1-15 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
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
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、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的预共享密钥、确认密钥和策略配置。	*请根据实际设置*
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
连接2配置	选择是否“与连接1保持一致”。 **说明** 建议连接2配置和连接1配置保持一致。	开启

----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。

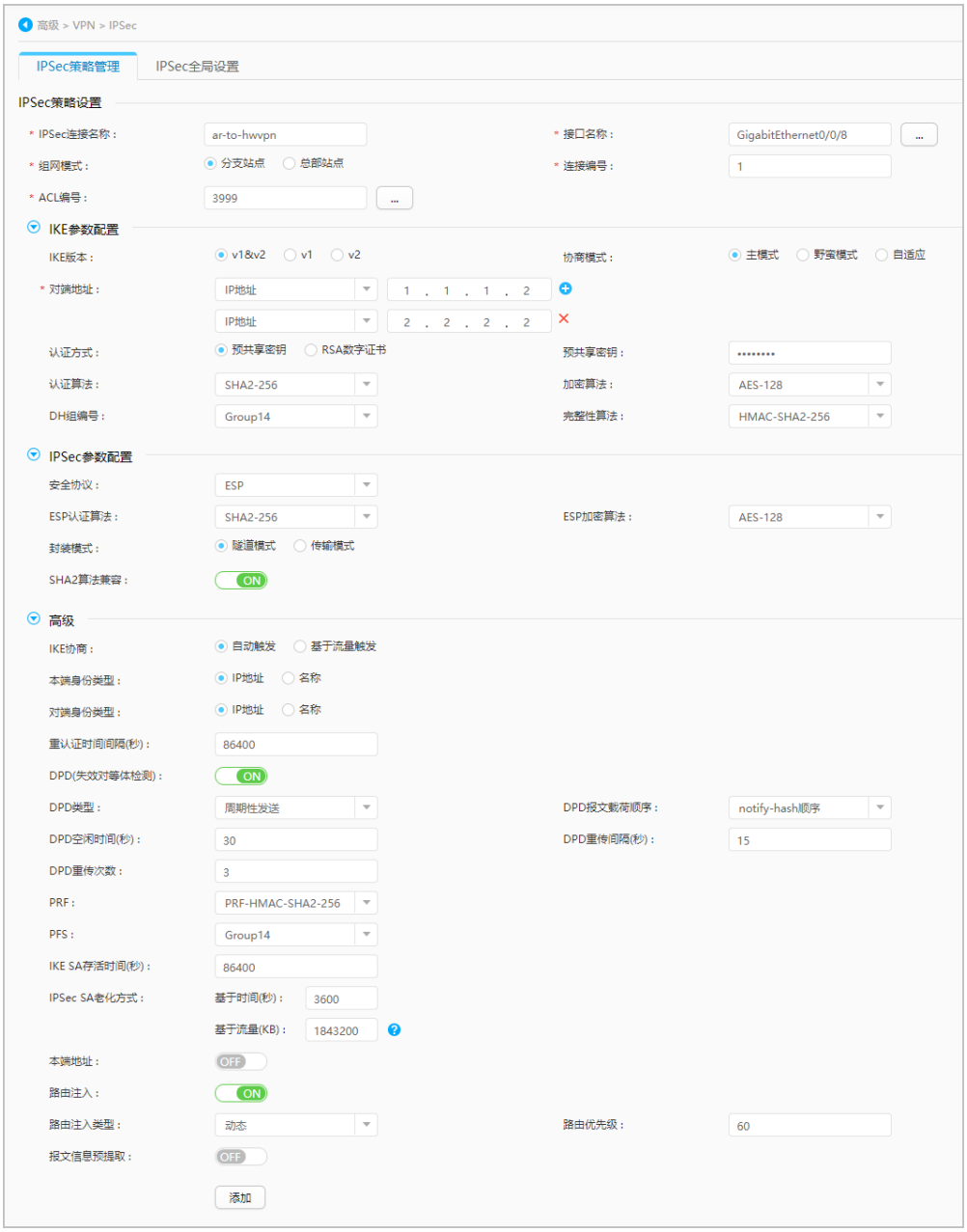
步骤2 配置VPN连接。

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 对接华为 AR 路由器（双 Internet 线路双活连接）

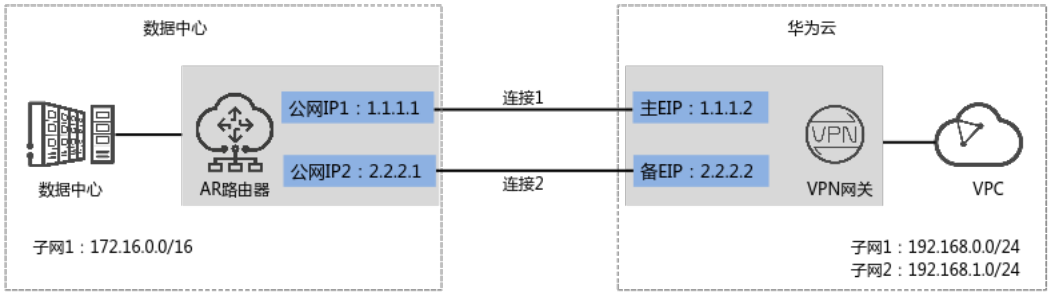
1.2.1 静态路由模式

1.2.1.1 操作指引

场景描述

华为云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1-15所示。

图 1-15 典型组网



本场景下以AR路由器双IP地址方案为例，华为云VPN网关采用主备模式，主EIP和备EIP和AR路由器的两个IP地址各建立一条VPN连接。

约束与限制

华为云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 1-16 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	• 公网IP1：1.1.1.1 • 公网IP2：2.2.2.1	• 主EIP：1.1.1.2 • 备EIP：2.2.2.2
	互联子网	-	192.168.2.0/24
VPN连接	“连接1配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30	
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：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1-16所示。

图 1-16 操作流程

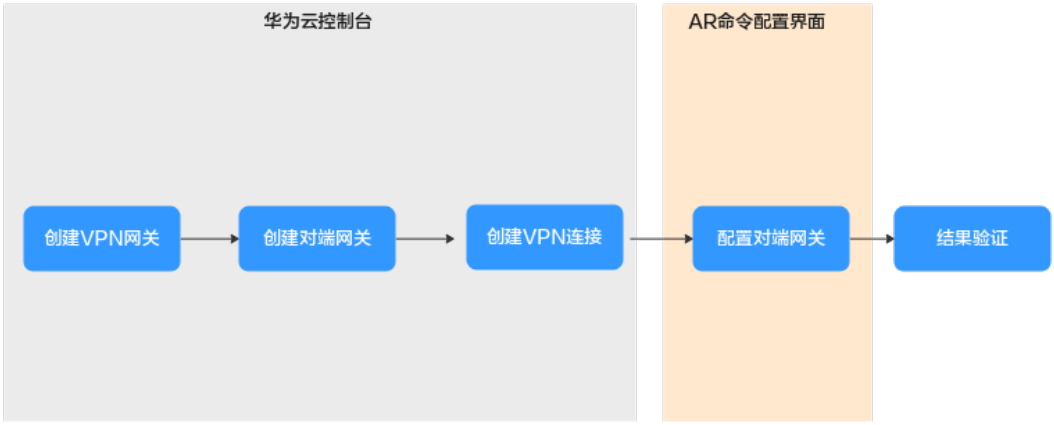


表 1-17 操作流程说明

序号	在哪里操作	步骤	说明
1	华为云控制台	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	分别添加AR路由器的两个公网IP地址作为对端网关，共计两个对端网关。
3		创建VPN连接	• VPN网关的主EIP、备EIP和对端网关创建一组VPN连接。 • 连接1配置的路由模式、预共享密钥、IKE/IPsec策略建议和连接2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路由器配置的本端接口地址/对端接口地址需要和VPN网关互为镜像配置。 • AR路由器配置的路由模式、预共享密钥、IKE/IPsec策略需要和VPN连接配置保持一致。
6	-	结果验证	执行**ping**命令，验证网络互通情况。

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“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。

表 1-18 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。	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP自治系统号码。	64512
HA模式	选择“主备”。	主备

参数	说明	取值参数
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，配置第一个对端网关参数。
   对端网关参数说明如**表 第一个对端网关参数说明**所示。

表 1-19 第一个对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-ar01
标识	AR路由器的第一个公网IP地址。	1.1.1.1

3. 配置第二个对端网关参数。
   对端网关参数说明如**表 第二个对端网关参数说明**所示。

表 1-20 第二个对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-ar02
标识	AR路由器的第二个公网IP地址。	2.2.2.1

步骤5 配置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. 配置VPN连接参数。
   VPN连接参数说明如**VPN连接参数说明**所示。

表 1-21 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
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的备EIP。	2.2.2.2
连接2对端网关	选择连接2对端网关。	2.2.2.1

参数	说明	取值参数
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、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 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。	169.254.70.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.2/30
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。 **说明** 功能开启前，请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则可能导致VPN流量不通。	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。	Test@123

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
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

----结束

1.2.1.3 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
[AR651]interface GigabitEthernet 0/0/9
[AR651-GigabitEthernet0/0/9]ip address 2.2.2.1 255.255.255.0
[AR651-GigabitEthernet0/0/9]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
[AR651]ip route-static 0.0.0.0 0.0.0.0 2.2.2.254 preference 100
```

其中，1.1.1.254/2.2.2.254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/备EIP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 2.2.2.254
```

- 1.1.1.2/2.2.2.2为VPN网关的主/备EIP。
- 1.1.1.254/2.2.2.254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 2.2.2.1
[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/备EIP。

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]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.2 255.255.255.252
[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]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.2 255.255.255.252
[AR651-Tunnel0/0/2]source 2.2.2.1
[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网关备EIP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/备EIP。

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 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.2
[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 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.2
[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网关备EIP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连接为主备模式。

  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

1.2.1.4 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。
  - 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。

1.3 对接华为 USG 防火墙

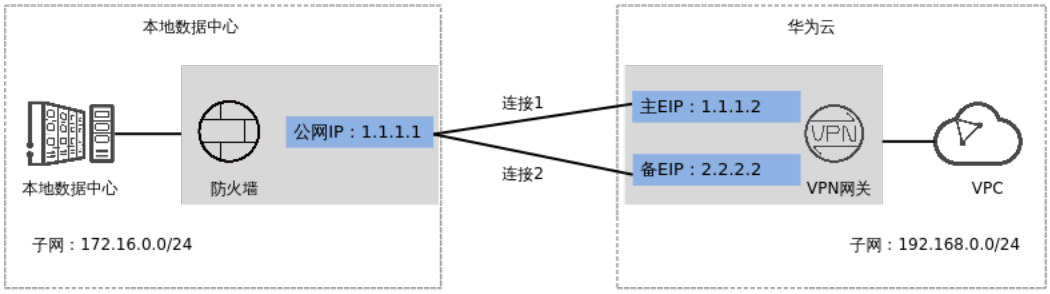
1.3.1 静态路由模式

1.3.1.1 操作指引

场景描述

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 典型组网所示。

图 1-17 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和该IP地址创建一组VPN连接。

数据规划

表 1-22 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	“连接1配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30	
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：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	

1.3.1.2 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“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 1-23 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 1-24 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和该IP地址创建一组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 1-25 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
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的备EIP。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
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、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/24
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 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。	169.254.70.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.2/30
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”

参数	说明	取值参数
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 ■ 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
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

----结束

1.3.1.3 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     # 和表1-25配置的IKE策略认证算法保持一致
   encryption-algorithm AES-128          # 和表1-25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                        # 和表1-25配置的IKE策略DH算法保持一致
   sa duration 86400                   # 和表1-25配置的IKE策略生命周期保持一致

   ike peer hwcloud_peer33
   undo version 1                    # 和表1-25配置的IKE策略IKE版本保持一致
   pre-shared-key XXXXXXX              # 和表1-25配置的预共享密钥保持一致
   ike-proposal 100
   remote-address 1.1.1.2              # 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 # 和表1-25配置的IPsec策略认证算法保持一致
   esp encryption-algorithm aes-128    # 和表1-25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                # 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IPsec隧道。

```
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
pfs dh-group15                  # 和表1-25配置的IPsec策略PFS保持一致
sa duration time-based 3600       # 和表1-25配置的IPsec策略生命周期保持一致

interface Tunnel100
ip address 169.254.70.2 255.255.255.252       # 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

IPsec profile HW-IPsec200
ike-peer hwcloud_peer44
proposal IPsec-pro200
pfs dh-group15                  # 和表1-25配置的IPsec策略PFS保持一致
sa duration time-based 3600       # 和表1-25配置的IPsec策略生命周期保持一致

interface Tunnel200
ip address 169.254.71.2 255.255.255.252     # 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. 配置华为云私网IP的静态路由。

   ```
   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+Tunnel口编号+VPN主EIP/备EIP。
   - 如果存在多个VPC子网，则需要为每个VPC子网配置两条路由。

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
```

1.3.1.4 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。
  - USG防火墙
    选择“网络 > IPSec > IPSec”，两条VPN连接状态显示为“Succeeded”。
- 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。

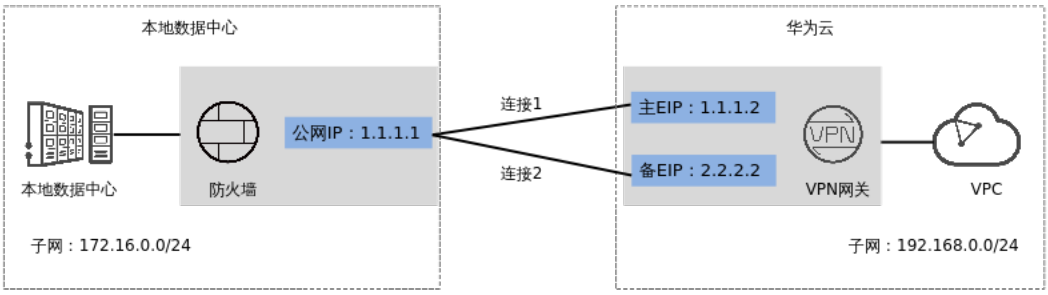
1.3.2 BGP 路由模式

1.3.2.1 操作指引

场景描述

华为云VPN网关通过BGP路由模式对接华为防火墙的典型组网如图 典型组网所示。

图 1-18 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和备EIP和该IP地址创建一组VPN连接。

数据规划

表 1-26 数据规划

部件	参数项	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
	BGP ASN	64515	64512
VPN连接	“连接1配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30	
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：169.254.71.2/30	
	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	

1.3.2.2 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“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 1-27 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
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 1-28 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
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。	64515

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和备EIP和该IP地址创建一组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 1-29 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
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的备EIP。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
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、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/24
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 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。	169.254.70.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.70.2/30
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 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
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

----结束

1.3.2.3 防火墙侧操作步骤

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 172.16.0.233 255.255.0.0
   ```

   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     # 和表1-25配置的IKE策略认证算法保持一致
   encryption-algorithm AES-128          # 和表1-25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                        # 和表1-25配置的IKE策略DH算法保持一致
   sa duration 86400                   # 和表1-25配置的IKE策略生命周期保持一致

   ike peer hwcloud_peer33
   undo version 1                      # 和表1-25配置的IKE策略IKE版本保持一致
   pre-shared-key Test@123               # 和表1-25配置的预共享密钥保持一致
   ike-proposal 100
   remote-address 1.1.1.2              # 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    # 和表1-25配置的IPsec策略认证算法保持一致
   esp encryption-algorithm aes-128    # 和表1-25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 Test@123
   ike-proposal 200
   remote-address 2.2.2.2                          # 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IPsec隧道。

   ```
   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
   ```



```
pfs dh-group15                    # 和表1-25配置的IPsec策略PFS保持一致
sa duration time-based 3600       # 和表1-25配置的IPsec策略生命周期保持一致

interface Tunnel100
ip address 169.254.70.2 255.255.255.252      # 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

IPsec profile HW-IPsec200
ike-peer hwcloud_peer44
proposal IPsec-pro200
pfs dh-group15                    # 和表1-25配置的IPsec策略PFS保持一致
sa duration time-based 3600       # 和表1-25配置的IPsec策略生命周期保持一致

interface Tunnel200
ip address 169.254.71.2 255.255.255.252      # 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BGP邻居和BGP路由。

   ```
   bgp 64515
    router-id 1.1.1.1
    private-4-byte-as enable
    peer 169.254.70.1 as-number 64512
    peer 169.254.70.1 connect-interface Tunnel100
    peer 169.254.71.1 as-number 64512
    peer 169.254.71.1 connect-interface Tunnel200
    #
    ipv4-family unicast
     network 172.16.0.0 255.255.255.0
     peer 169.254.70.1 enable
     peer 169.254.71.1 enable
   ```

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 16                       # 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
address 0 192.168.1.0 mask 24

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
```

1.3.2.4 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。
- 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。

- **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**

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

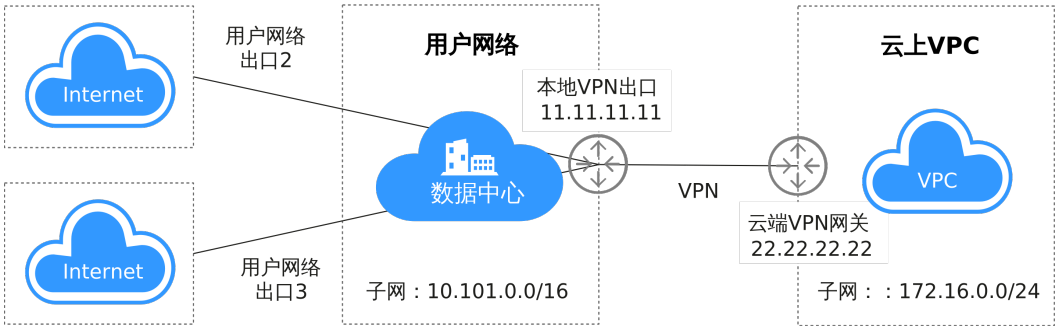
用户数据中心的出口防火墙选用飞塔设备，用户数据中心存在多个互联网出口，用户在华为云购买VPN网关，需要创建VPN连接连通本地网络到VPC子网。

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。

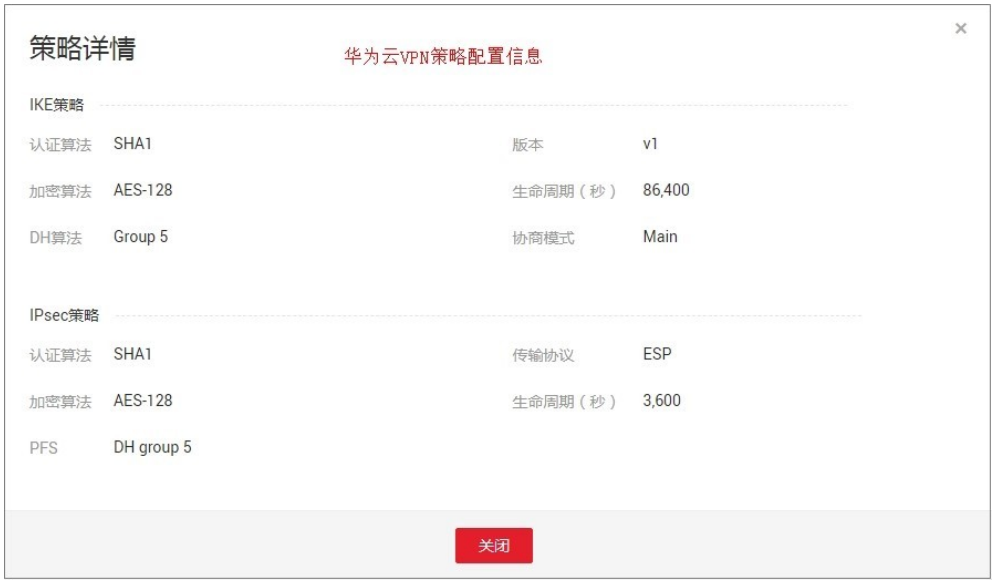
图 2-1 多出口客户网络通过 VPN 接入 VPC 连接拓扑

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。
2. 配置隧道基本信息。
3. 配置IKE一阶段。
4. 配置IPsec二阶段
5. 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。
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。

步骤3 配置策略及NAT

1. 本地访问云端策略。
2. 云端访问本地策略。

----结束

配置验证

1. 本地VPN状态正常。

2. 云端VPN状态正常。

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：

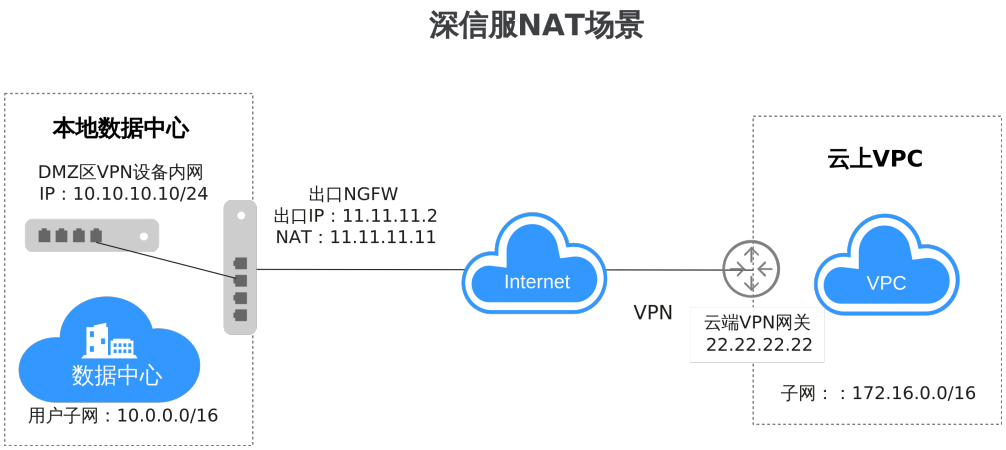
- 使用防火墙设备直接和云端建立VPN连接。
- 使用DMZ区域的专用VPN设备结合NAT穿越与云端建立VPN连接。

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 2-3 深信服 NAT 场景



华为云端的VPN连接资源策略配置按照图2-4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 2-4 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**
2. **IPsec二阶段配置**
3. **安全选项配置**

步骤2 配置路由

步骤3 配置策略及NAT

----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

本文档详细地描述了“VPC+云桌面”和“VPC+VPC”场景下，使用TheGreenBow IPsec VPN Client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 2-5 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。

- **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 2-6 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。

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
2. IKE第一阶段配置
3. IPsec第二阶段配置

场景二：VPC+VPC场景的客户端配置

1. 全局参数配置
2. IKE第一阶段配置
3. IPsec第二阶段配置

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. VPN连接建立成功如下图所示。
  b. 查看云端VPC中VPN连接状态。连接状态由“未连接”变为“正常”。
  c. 查看桌面云网络配置信息，如下图所示。
  d. 桌面云 Ping 云端VPC虚拟机
  e. 云端VPC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。

  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。

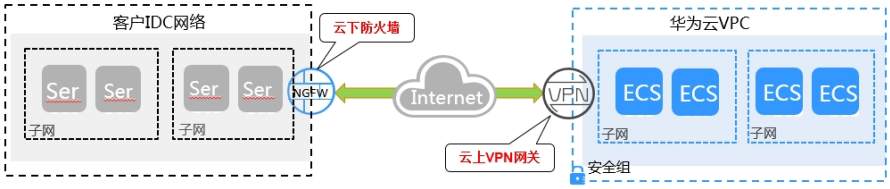
云上VPC的VPN网关IP：11.11.11.11，本地子网：192.168.200.0/24。

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 2-7 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

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

步骤1 执行以下命令，安装Openswan客户端。

yum install -y openswan

步骤2 执行以下命令，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. 执行以下命令，使转发配置参数生效。
   /sbin/sysctl -p

步骤3 执行以下命令，查询iptables配置，确认关闭firewall或允许数据流转发。

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 执行以下命令，配置预共享密钥。

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 执行以下命令，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？**。

执行以下命令，进行配置项校验。

ipsec verify

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 执行以下命令，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

执行以下命令，查询IPsec的状态。

ipsec --status

结果显示如下信息（摘录）。

```
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2-8所示，

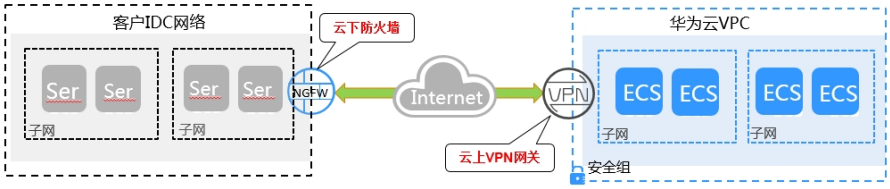
云上VPC的VPN网关IP：11.11.11.11，本地子网：192.168.200.0/24。

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 2-8 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 执行以下命令，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 执行以下命令，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. 执行以下命令，使转发配置参数生效。

   /sbin/sysctl -p

步骤3 执行以下命令，查询iptables配置，确认关闭firewall或允许数据流转发。

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 执行以下命令，配置预共享密钥。

vim /etc/strongswan/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 执行以下命令，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 执行以下命令，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

执行以下命令，查询可见连接启动时间。

strongswan statusall

```
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
```

执行以下命令，安装有IPsec客户端的VPC2的主机。

VPC1 ping

```
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
```


3 终端入云 VPN

3.1 通过云证书与管理服务 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，将服务端证书配置为“已有证书”，在下拉选项中单击“上传证书”进入“云证书与管理服务”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

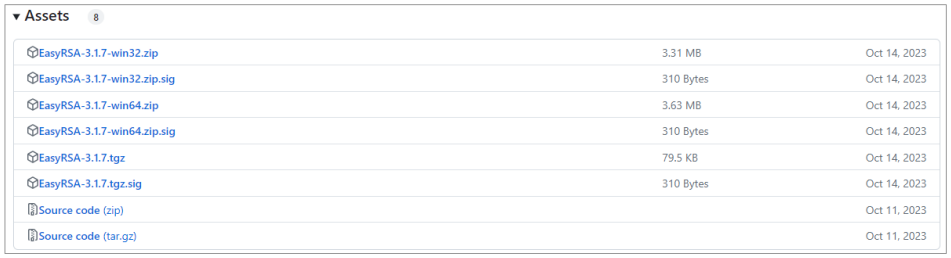
Easy-RSA是一个开源的证书管理工具，用于帮助用户生成和管理数字证书。

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. 执行以下命令，运行Easy-RSA。

   .\EasyRSA-Start.bat

   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. 执行以下命令，初始化PKI环境。

   ./easyrsa init-pki

   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. 执行以下命令，生成CA证书。

   ./easyrsa build-ca nopass

   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. 执行以下命令，生成服务端证书及其私钥。

    ./easyrsa build-server-full *p2cserver.com* **nopass**

    说明

    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与管理服务，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. 执行以下命令，生成客户端证书及其私钥。

    ./easyrsa build-client-full *p2cclient.com* **nopass**

    说明

    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

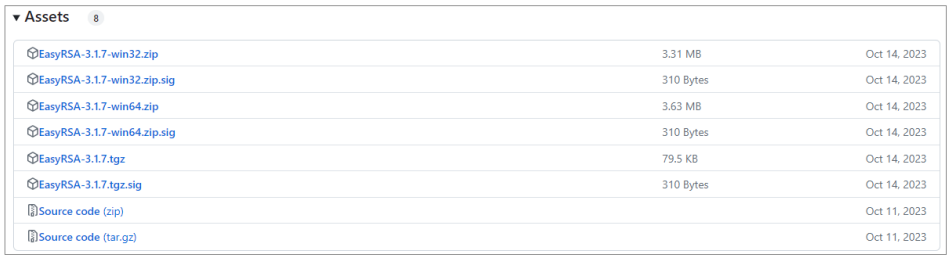
Easy-RSA是一个开源的证书管理工具，用于帮助用户生成和管理数字证书。

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. 执行以下命令，运行Easy-RSA。

   .\EasyRSA-Start.bat

   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. 执行以下命令，初始化PKI环境。

   ./easyrsa init-pki

   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. 执行以下命令，运行Easy-RSA。

      .\EasyRSA-Start.bat

      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. 执行以下命令，生成服务端CA证书。

      ./easyrsa build-ca nopass

      说明

      在此命令生成中，**[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. 执行以下命令，生成服务端证书及其私钥。

    ./easyrsa build-server-full *p2cserver.com* **nopass**

    说明

    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与管理服务，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. 执行以下命令，运行Easy-RSA。

       .\EasyRSA-Start.bat

       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. 执行以下命令，生成客户端CA证书。

       ./easyrsa build-ca nopass

       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. 执行以下命令，生成客户端证书及其私钥。

    ./easyrsa build-client-full *p2cclient.com* **nopass**

    说明

    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 通过云证书与管理服务 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，也可以通过云证书与管理服务购买证书。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

通过云证书与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**。

     从云证书与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**。

