虚拟私有云

最佳实践

文档版本	01
发布日期	2024-08-22

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

目 录

1 节约公网成本

在您购买带宽产品之前一定要分析您业务系统的流量模型，以便选择适合的产品及计费模式。

独享带宽

如您需要保证单个弹性公网IP的带宽大小，建议您购买独享带宽。独享带宽只针对单个弹性公网IP进行限速，不受其他业务影响。

支持两种计费模式：

- 按带宽计费：针对流量使用较大且比较稳定的业务。
- 按流量计费：针对流量使用相对较小的业务，搭配共享流量包使用价格更优惠。

对于流量比较稳定，没有突发流量的系统可以考虑选择预付费的按带宽计费模式，可以比正常后付费按带宽计费享受更多价格优惠。

共享带宽

当您有大量业务在云上时，如果每个ECS单独使用一条独享带宽，则需要较多的带宽实例，并且总的带宽费用会较高，如果所有实例共用一条带宽，就可以节省企业的网络运营成本，同时方便运维统计。共享带宽是独立的带宽产品，支持将多个按需计费的弹性公网IP添加到共享带宽，对多个弹性公网IP进行集中限速。您可以将EIP绑定到ECS、NAT网关、ELB等产品，从而使这些产品使用共享带宽。

共享流量包

共享流量包是公网流量的预付费套餐，价格比后付费流量更低，大大降低了公网流量成本。共享流量包购买后立即生效，自动抵扣按需计费（按流量计费）的EIP带宽产生的流量资费，使用简单，无需额外操作。

- 共享流量包适用哪些场景?

  对于按流量计费的带宽，启用共享流量包后，该带宽所产生的流量费用优先从共享流量包中进行抵扣。共享流量包全部使用完后，再按后付费流量进行结算。从节约成本的角度看，流量越大，节省的成本越多。

- 共享流量包使用说明
  - 只能抵扣同一区域产生的带宽流量，不支持跨区域抵扣。

- 共享流量包包括动态和静态两种类型，分别抵扣全动态BGP和静态BGP产生的流量。
- 共享流量包具有使用有效期（从购买开始计算1个自然月或1个自然年）。超过有效期后，没有使用完的流量无法继续使用。建议根据业务系统历史情况仔细评估需要多少共享流量包。
- 共享流量包支持自动续费功能。如果您开通了自动续费功能，那么共享流量包到期前7天内，系统会尝试自动续费扣款，续费成功后，共享流量包中剩余的流量可以在新的有效期内继续使用。
- 共享流量包全部使用完后，系统会自动按后付费流量进行结算，不会导致业务系统无法使用。

2 VPC 网络安全

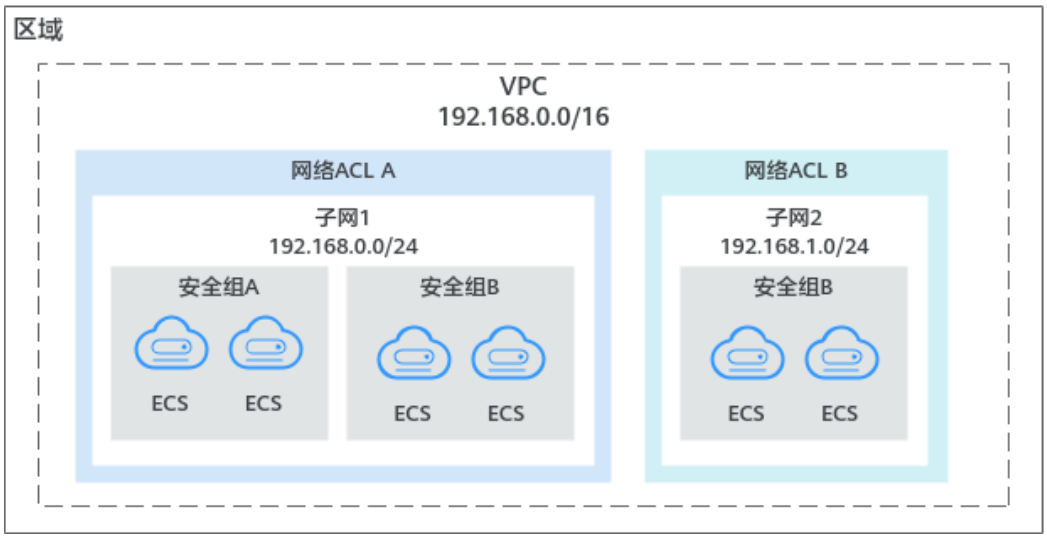
2.1 通过安全组和网络 ACL 实现 VPC 的访问控制

虚拟私有云VPC是您在云上的私有网络，通过配置安全组和网络ACL策略，可以保障VPC内部署的实例安全运行，比如弹性云服务器、数据库、云容器等。

- 安全组对实例进行防护，将实例加入安全组内后，该实例将会受到安全组的保护。
- 网络ACL对整个子网进行防护，将子网关联至网络ACL，则子网内的所有实例都会受到网络ACL保护。相比安全组，网络ACL的防护范围更大。

如图2-1所示，安全组A和安全组B可以保护其中ECS的网络安全，通过网络ACL A和网络ACL B，可以分别保护整个子网1和子网2的安全，双层防护提升安全保障。

图 2-1 安全组与网络 ACL



以下为您介绍一些常用的安全组和网络ACL的配置示例：

- 安全组：**控制外部指定IP地址或安全组对实例的访问**
- 安全组：**控制虚拟IP访问安全组内实例**

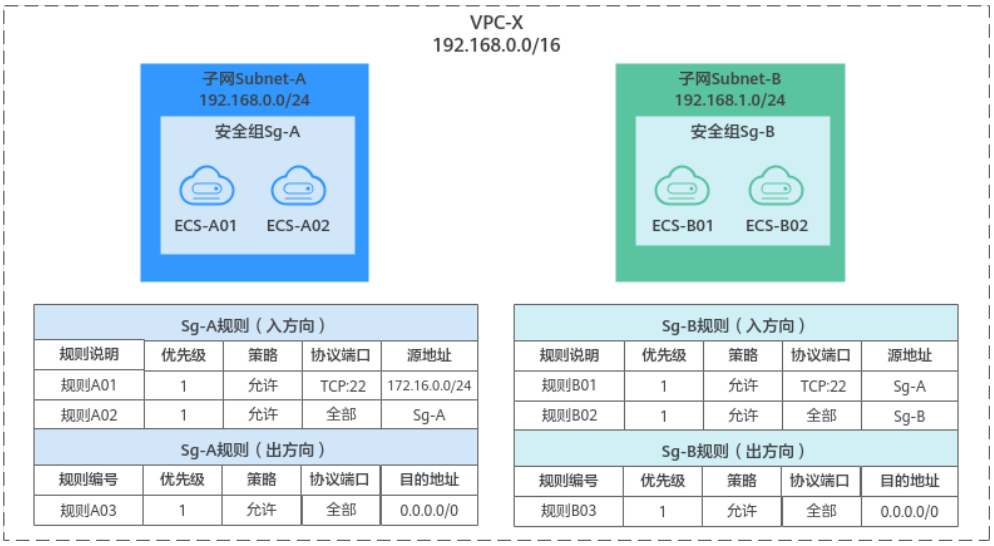
- 安全组：**控制对等连接两端VPC内的实例互访**
- 网络ACL：**控制外部对子网内实例的访问**
- 网络ACL：**控制不同子网内实例的互通和隔离**

控制外部指定 IP 地址或安全组对实例的访问

本示例安全组配置如**图2-2**所示，您可以通过设置安全组入方向规则，允许特定IP地址，或者其他安全组内的实例访问您的实例。

- 在安全组Sg-A的入方向中，添加规则A01，允许指定IP (172.16.0.0/24)访问安全组内实例的SSH(22)端口，用于远程登录安全组内的Linux云服务器。
- 在安全组Sg-B的入方向中，添加规则B01，允许其他安全组内的实例访问本安全组内实例的SSH(22)端口，即通过子网Subnet-A的ECS可远程登录Subnet-B内的ECS。

图 2-2 控制外部指定 IP 地址或安全组对实例的访问



Sg-A规则（入方向）

规则说明	优先级	策略	协议端口	源地址
规则A01	1	允许	TCP:22	172.16.0.0/24
规则A02	1	允许	全部	Sg-A

Sg-A规则（出方向）

规则编号	优先级	策略	协议端口	目的地址
规则A03	1	允许	全部	0.0.0.0/0

Sg-B规则（入方向）

规则说明	优先级	策略	协议端口	源地址
规则B01	1	允许	TCP:22	Sg-A
规则B02	1	允许	全部	Sg-B

Sg-B规则（出方向）

规则编号	优先级	策略	协议端口	目的地址
规则B03	1	允许	全部	0.0.0.0/0

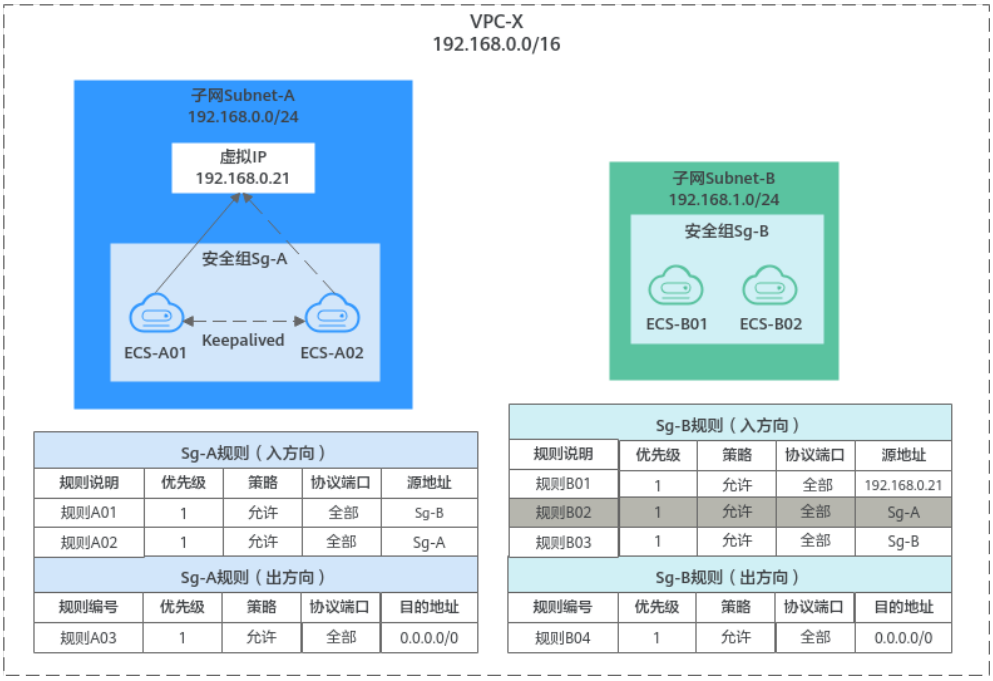
控制虚拟 IP 访问安全组内实例

本示例安全组配置如**图2-3**所示，您可以通过设置安全组入方向规则，允许虚拟IP，或者其他安全组内的实例访问您的实例。

- 在安全组Sg-A的入方向中，添加规则A01，允许Sg-B内的实例使用任何协议和端口，通过私有IP地址访问Sg-A内的实例。
- 在安全组Sg-B的入方向中，添加规则B01，允许虚拟IP(192.168.0.21)使用任何协议和端口访问Sg-B内的实例。当前组网中，您还可以将源地址设置成子网Subnet-A的网段192.168.0.0/24。

  规则B02仅能允许Sg-A内实例通过私有IP访问Sg-B内的实例，无法放通虚拟IP访问。

图 2-3 控制虚拟 IP 访问安全组内实例

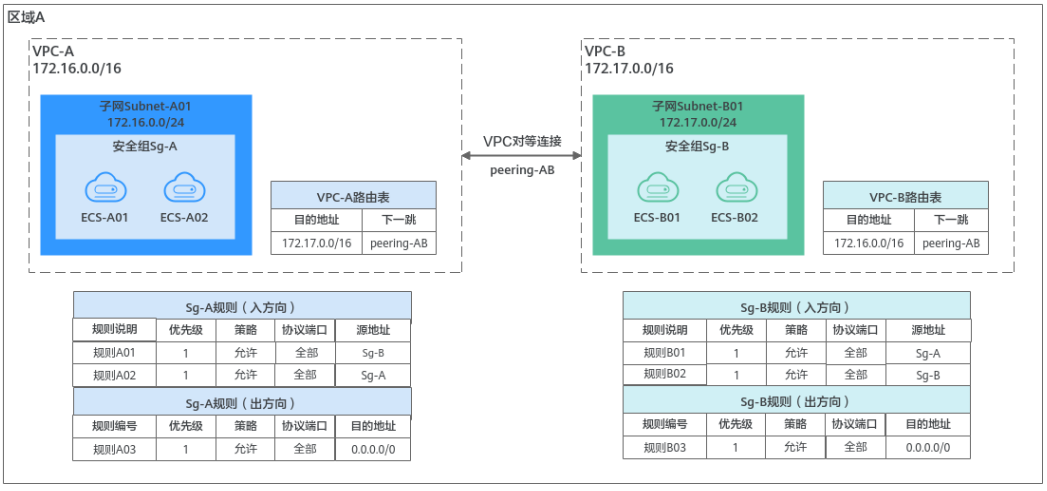


控制对等连接两端 VPC 内的实例互访

本示例安全组配置如图2-4所示。您可以通过设置安全组入方向规则，实现对等连接两端的ECS网络互通。

- 在安全组Sg-A中，添加规则A01，允许来自Sg-B内实例的流量访问Sg-A内的实例，源地址为安全组Sg-B。
- 在安全组Sg-B中，添加规则B01，允许来自Sg-A内实例的流量访问Sg-B内的实例，源地址为安全组Sg-A。

图 2-4 控制对等连接两端 VPC 内的实例互访



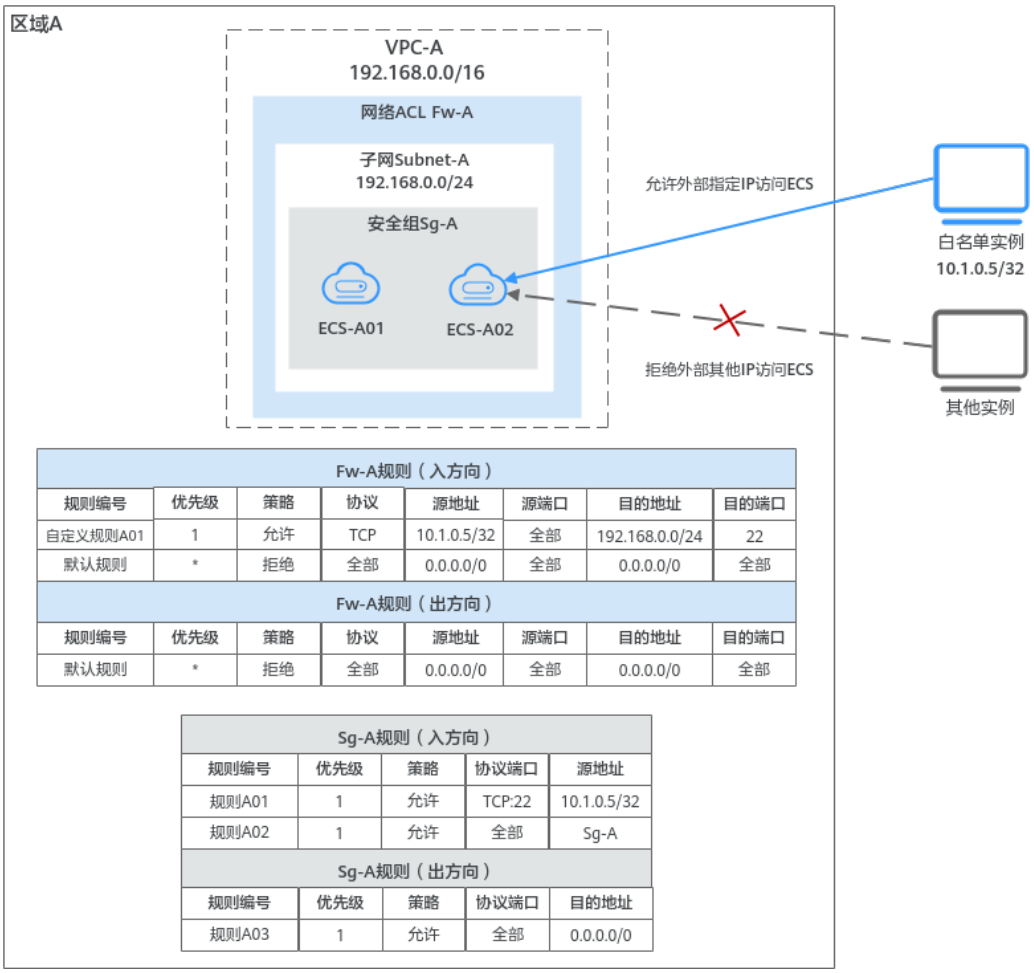
控制外部对子网内实例的访问

网络ACL可以控制流入/流出子网的流量，流量优先匹配网络ACL的规则，然后匹配安全组规则。

本示例如图2-5所示，子网Subnet-A内的两个业务实例ECS-A01和ECS-A02网络互通，并允许白名单实例远程登录业务实例，白名单实例的IP地址为10.1.0.5/32。白名单实例可能是VPC-A的其他子网或者其他VPC内的实例，也可以是本地计算机，可远程连接业务实例执行运维操作。因此，网络ACL和安全组规则需要放通白名单实例的流量，拦截来自其他网络的流量，规则配置如下：

- 网络ACL规则：
  - 入方向：自定义规则A01允许白名单实例，通过SSH远程登录子网Subnet-A内的实例。默认规则拒绝其他网络流量流入子网。
  - 出方向：网络ACL是有状态的，允许入站请求的响应流量流出，因此不用额外添加规则放通白名单实例的响应流量。默认规则拒绝其他网络流量流出子网。
- 安全组规则：
  - 入方向：规则A01允许白名单实例，通过SSH远程登录子网Subnet-A内的实例。规则A02允许安全组内实例互通。其他流量无法流入安全组内实例。
  - 出方向：规则A03允许所有流量从安全组内实例流出。

图 2-5 控制外部对子网内实例的访问



Fw-A规则（入方向）							
规则编号	优先级	策略	协议	源地址	源端口	目的地址	目的端口
自定义规则A01	1	允许	TCP	10.1.0.5/32	全部	192.168.0.0/24	22
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

Fw-A规则（出方向）							
规则编号	优先级	策略	协议	源地址	源端口	目的地址	目的端口
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

Sg-A规则（入方向）				
规则编号	优先级	策略	协议端口	源地址
规则A01	1	允许	TCP:22	10.1.0.5/32
规则A02	1	允许	全部	Sg-A

Sg-A规则（出方向）				
规则编号	优先级	策略	协议端口	目的地址
规则A03	1	允许	全部	0.0.0.0/0

控制不同子网内实例的互通和隔离

本示例中，VPC-X内有两个子网Subnet-X01和Subnet-X02，ECS-01和ECS-02属于Subnet-X01，ECS-03属于Subnet-X02。三台ECS的网络通信需求如下：

- ECS-02和ECS-03网络互通
- ECS-01和ECS-03网络隔离

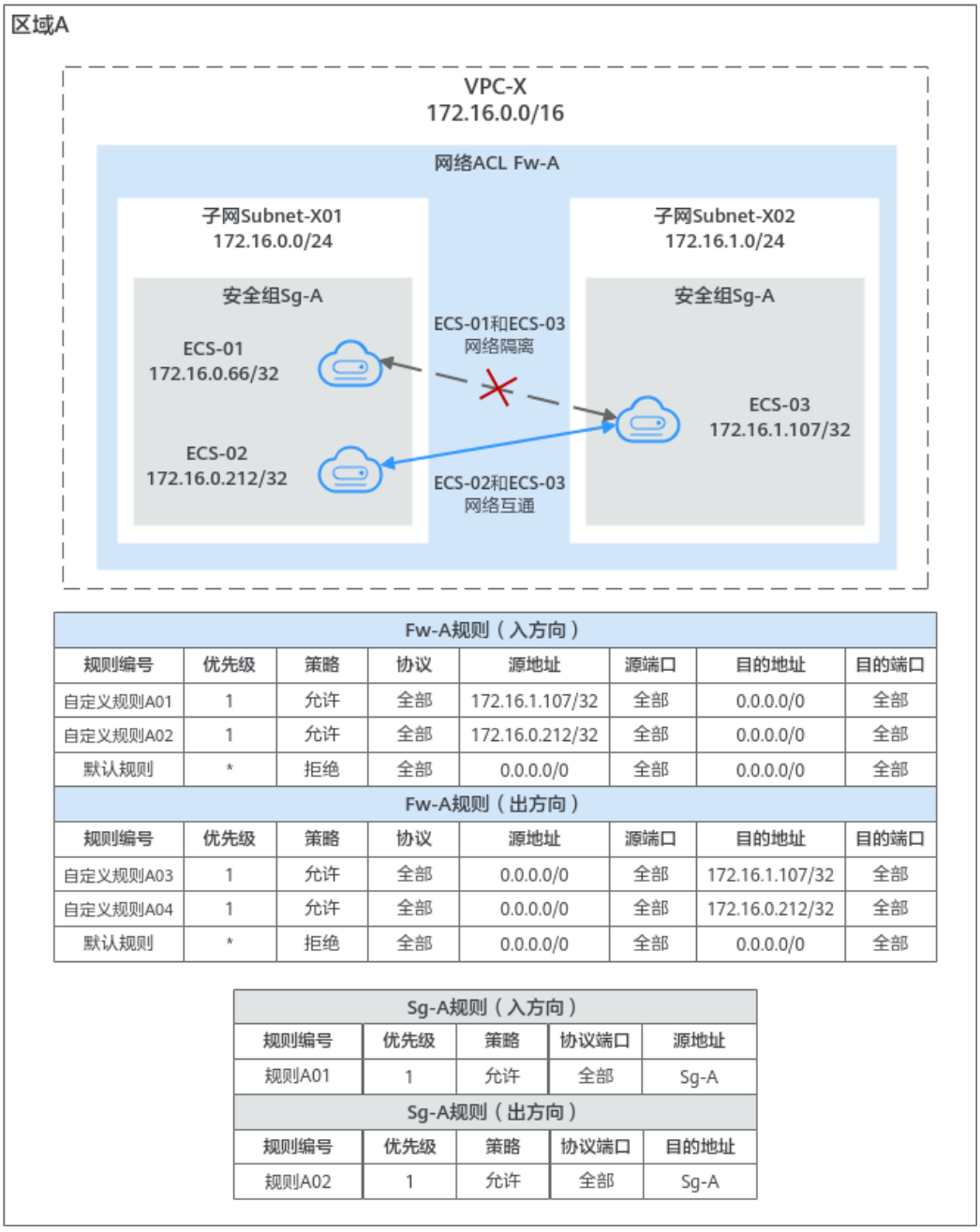
为了实现以上网络通信需求，本示例的安全组和网络ACL配置如下：

1. 三台ECS属于同一个安全组Sg-A，在Sg-A中添加入方向和出方向规则，确保安全组内实例网络互通。

   此时子网还未关联网络ACL，安全组规则配置完成后，ECS-01、ECS-02均可以和ECS-03进行通信。
2. 将两个子网均关联至网络ACL Fw-A。

   当Fw-A中只有默认规则时，同一个子网内实例网络互通，不同子网内实例网络隔离。此时ECS-01和ECS-02网络互通，ECS-01和ECS-03网络隔离、ECS-02和ECS-03网络隔离。
3. 在网络ACL Fw-A中添加自定义规则，放通ECS-02和ECS-03之间的网络。
   - 自定义规则A01：允许来自ECS-03的流量流入子网。
   - 自定义规则A02：允许来自ECS-02的流量流入子网。
   - 自定义规则A03：允许访问ECS-03的流量流出子网。
   - 自定义规则A04：允许访问ECS-02的流量流出子网。

图 2-6 控制不同子网内实例的互通和隔离



Fw-A规则（入方向）							
规则编号	优先级	策略	协议	源地址	源端口	目的地址	目的端口
自定义规则A01	1	允许	全部	172.16.1.107/32	全部	0.0.0.0/0	全部
自定义规则A02	1	允许	全部	172.16.0.212/32	全部	0.0.0.0/0	全部
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部
Fw-A规则（出方向）							
规则编号	优先级	策略	协议	源地址	源端口	目的地址	目的端口
自定义规则A03	1	允许	全部	0.0.0.0/0	全部	172.16.1.107/32	全部
自定义规则A04	1	允许	全部	0.0.0.0/0	全部	172.16.0.212/32	全部
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

Sg-A规则（入方向）				
规则编号	优先级	策略	协议端口	源地址
规则A01	1	允许	全部	Sg-A
Sg-A规则（出方向）				
规则编号	优先级	策略	协议端口	目的地址
规则A02	1	允许	全部	Sg-A

2.2 通过对等连接和第三方防火墙实现多 VPC 互访流量清洗

应用场景

虚拟私有云支持用户自主配置和管理虚拟网络环境，您可以在VPC中使用安全组及网络ACL来进行网络访问控制，也可以使用第三方防火墙软件，对云上的业务进行灵活的安全控制。

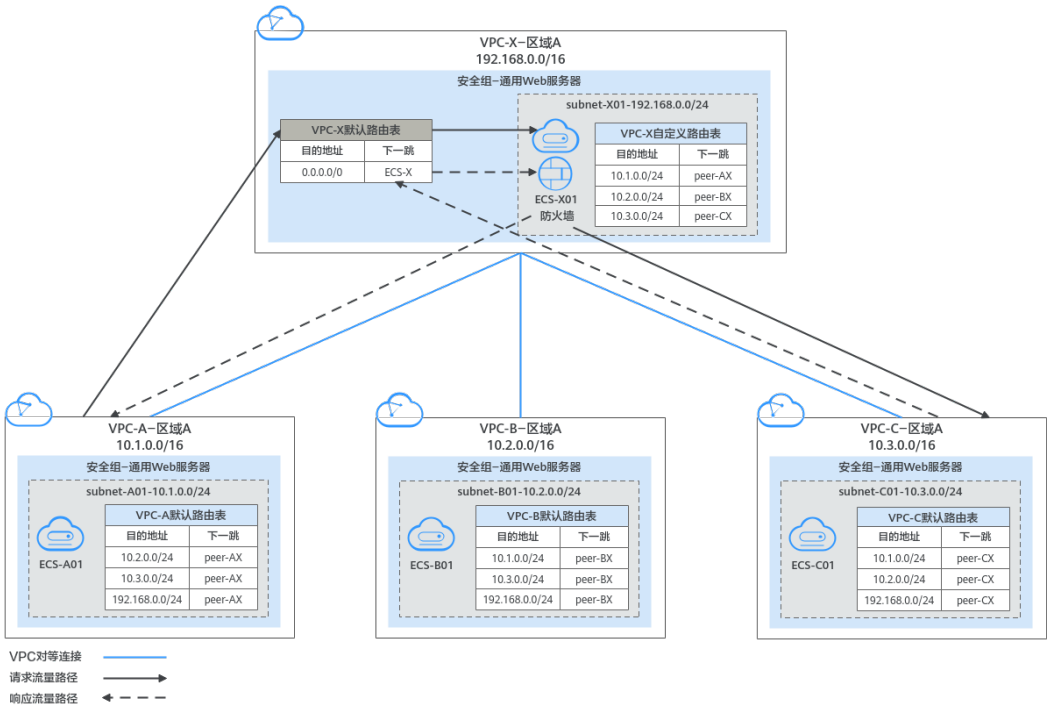
本文为您介绍通过防火墙软件实现VPC内流量安全管控的需求，首先基于VPC对等连接实现多个VPC网络互通，然后VPC之间互访流量通过防火墙软件过滤清洗。

方案架构

本示例中vpc-A、vpc-B、vpc-C为业务所在的VPC，vpc-X为防火墙所在的VPC，这些VPC通过对等连接实现网络互通。vpc-A、vpc-B、vpc-C之间互通的流量均需要经过vpc-X上的防火墙。根据默认路由表配置，所有vpc-X的入方向流量均引入防火墙，通过防火墙清洗后的流量根据自定义路由表的目的地址送往指定业务VPC。

在图2-7中，以ecs-A01访问ecs-C01为例，您可以清晰的看到流量的请求路径和响应路径。

图 2-7 云上 VPC 互访使用第三方防火墙组网规划



资源规划说明

本示例中需要创建虚拟私有云VPC、弹性云服务器ECS以及VPC对等连接，资源规划总体说明请参见表2-1。

说明

以下资源规划详情仅为示例，供您参考，您需要根据实际业务情况规划资源。

表 2-1 云上 VPC 互访使用第三方防火墙资源规划总体说明

资源	说明
虚拟私有云 VPC	VPC的资源规划详情如表2-2所示。 本示例中共有4个VPC，包括业务所在VPC和防火墙所在的VPC。这些VPC位于同一个区域内，且这些VPC的子网网段不重叠。 • vpc-A、vpc-B、vpc-C为业务VPC，vpc-X为防火墙VPC，这些VPC通过对等连接实现网络互通。 • vpc-A、vpc-B、vpc-C、vpc-X各有一个子网。 • vpc-A、vpc-B、vpc-C各有一个默认路由表，子网关联VPC默认路由表。 • vpc-X有两个路由表，一个系统自带的默认路由表，一个用户创建的自定义路由表，vpc-X的子网关联自定义路由表。 默认路由表控制vpc-X的入方向流量，自定义路由表控制vpc-X的出方向流量。 **须知** 需要通过对等连接通信的VPC的子网网段不能重叠，否则对等连接不会生效，更多详情请参见无效的VPC对等连接配置。
弹性云服务器 ECS	ECS的资源规划详情如表2-3所示。 本示例中共有4个ECS，这些ECS分别位于不同的VPC内，这些ECS如果位于不同的安全组，需要在安全组中添加规则放通对端安全组的网络。
VPC对等连接	VPC对等连接的资源规划详情如表2-4所示。 本示例中共3个对等连接，网络连通需求如下： • peer-AX：连通vpc-A和vpc-X的网络。 • peer-BX：连通vpc-B和vpc-X的网络。 • peer-CX：连通vpc-C和vpc-X的网络。 由于VPC对等连接具有传递性，通过路由配置，vpc-A、vpc-B以及vpc-C之间可以通过vpc-X进行网络通信。

表 2-2 VPC 资源规划详情

VPC名称	VPC网段	子网名称	子网网段	关联路由表	子网作用
vpc-A	10.1.0.0/16	subnet-A01	10.1.0.0/24	默认路由表	部署业务的子网
vpc-B	10.2.0.0/16	subnet-B01	10.2.0.0/24	默认路由表	部署业务的子网
vpc-C	10.3.0.0/16	subnet-C01	10.3.0.0/24	默认路由表	部署业务的子网
vpc-X	192.168.0.0/16	subnet-X01	192.168.0.0/24	自定义路由表	部署防火墙的子网

表 2-3 ECS 资源规划详情

ECS名称	VPC名称	子网名称	私有IP地址	镜像	安全组	ECS作用
ecs-A01	vpc-A	subnet-A01	10.1.0.139	公共镜像：CentOS 8.2 64bit	sg-demo：通用Web服务器	部署业务的云服务器
ecs-B01	vpc-B	subnet-B01	10.2.0.93			部署业务的云服务器
ecs-C01	vpc-C	subnet-C01	10.3.0.220			部署业务的云服务器
ecs-X01	vpc-X	subnet-X01	192.168.0.5			部署防火墙的云服务器

表 2-4 VPC 对等连接资源规划详情

VPC对等连接名称	本端VPC	对端VPC
peer-AX	vpc-A	vpc-X
peer-BX	vpc-B	vpc-X
peer-CX	vpc-C	vpc-X

组网规划说明

本示例中需要在VPC路由表中配置路由，实现VPC之间的互通以及通过防火墙的流量清洗、组网规划总体说明请参见**表2-5**。

说明

以下路由规划详情仅为示例，供您参考，您需要根据实际业务情况规划路由。

表 2-5 云上 VPC 互访使用第三方防火墙组网规划总体说明

路由表	说明
业务所在VPC	vpc-A、vpc-B、vpc-C为业务VPC，路由表的规划详情如**表2-6**所示。 在vpc-A、vpc-B、vpc-C的默认路由表中，分别添加指向其他VPC子网，下一跳为对等连接的路由，实现不同VPC之间的网络互通。

路由表	说明
防火墙所在VPC	vpc-X为防火墙VPC，路由表的规划详情如表2-7所示。 1. 在vpc-X的默认路由表中，根据您防火墙部署方案分为以下情况： • 防火墙部署在一台ECS上，则添加目的地址为默认网段（0.0.0.0/0），下一跳为ecs-X01的路由，将流量引入防火墙所在的云服务器。 • 防火墙部署在两台ECS上，对外通过同一个虚拟IP通信，当主ECS发生故障无法对外提供服务时，动态将虚拟IP切换到备ECS，继续对外提供服务。此场景下，则添加目的地址为默认网段（0.0.0.0/0），下一跳为虚拟IP的路由，将流量进入虚拟IP，由虚拟IP将流量引入防火墙所在的云服务器。 本文以防火墙部署在一台ECS上为例，vpc-A、vpc-B、vpc-C互访的流量，都需要经过vpc-X，然后通过该条路由，将流量引入防火墙中进行清洗过滤。 2. 在vpc-X的自定义路由表中，添加目的地址为业务VPC子网网段（vpc-A、vpc-B、vpc-C子网），下一跳为对等连接的路由，将清洗后的流量引入业务VPC。

表 2-6 业务 VPC 路由表规划

VPC名称	VPC路由表	目的地址	下一跳类型	下一跳	路由类型	路由作用
vpc-A	默认路由表：rtb-vpc-A	10.2.0.0/24	对等连接	peer-AX	自定义	• 目的地址指向vpc-B的子网subnet-B01 • 连通子网subnet-A01和subnet-B01
		10.3.0.0/24	对等连接	peer-AX	自定义	• 目的地址指向vpc-C的子网subnet-C01 • 连通子网subnet-A01和subnet-C01
		192.168.0.0/24	对等连接	peer-AX	自定义	• 目的地址指向vpc-X的子网subnet-X01 • 连通子网subnet-A01和subnet-X01

VPC名称	VPC路由表	目的地址	下一跳类型	下一跳	路由类型	路由作用
vpc-B	默认路由表：rtb-vpc-B	10.1.0.0/24	对等连接	peer-BX	自定义	• 目的地址指向vpc-A的子网subnet-A01 • 连通子网subnet-A01和subnet-B01
		10.3.0.0/24	对等连接	peer-BX	自定义	• 目的地址指向vpc-C的子网subnet-C01 • 连通子网subnet-B01和subnet-C01
		192.168.0.0/24	对等连接	peer-BX	自定义	• 目的地址指向vpc-X的子网subnet-X01 • 连通子网subnet-B01和subnet-X01
vpc-C	默认路由表：rtb-vpc-C	10.1.0.0/24	对等连接	peer-CX	自定义	• 目的地址指向vpc-A的子网subnet-A01 • 连通子网subnet-A01和subnet-C01
		10.2.0.0/24	对等连接	peer-CX	自定义	• 目的地址指向vpc-B的子网subnet-B01 • 连通子网subnet-B01和subnet-C01
		192.168.0.0/24	对等连接	peer-CX	自定义	• 目的地址指向vpc-X的子网subnet-X01 • 连通子网subnet-C01和subnet-X01

表 2-7 防火墙 VPC 路由表规划

VPC名称	VPC路由表	目的地址	下一跳类型	下一跳	路由类型	路由作用
vpc-X	默认路由表：rtb-vpc-X	0.0.0.0/0	服务器实例	ECS-X	自定义	• 目的地址指向部署防火墙的ecs-X • 将vpc-X入方向的流量引入防火墙 本文以防火墙部署在一台ECS上为例，如果您的防火墙同时部署在多台ECS上，对外通过虚拟IP通信，则路由下一跳选择虚拟IP。
	自定义路由表：rtb-vpc-custom-X	10.1.0.0/24	对等连接	peer-AX	自定义	• 目的地址指向vpc-A的子网subnet-A01 • 连通子网subnet-A01和subnet-X01
		10.2.0.0/24	对等连接	peer-BX	自定义	• 目的地址指向vpc-B的子网subnet-B01 • 连通子网subnet-B01和subnet-X01
		10.3.0.0/24	对等连接	peer-CX	自定义	• 目的地址指向vpc-C的子网subnet-C01 • 连通子网subnet-C01和subnet-X01

约束与限制

- VPC对等连接只能实现同区域VPC的网络互通，因此请确保您的VPC位于同一个区域内。
- 需要通过VPC对等连接通信的VPC的子网网段不能重叠，否则对等连接不会生效，更多详情请参见**无效的VPC对等连接配置**。
- 第三方防火墙部署的ECS所在的子网需要关联自定义路由表 ，请确保您资源所在的区域支持自定义路由表功能。

  如果在网络控制台的左侧子栏目看到独立的“路由表”选项，表示支持自定义路由表功能。

图 2-8 支持定义路路由

操作步骤

步骤1 在区域A内，创建4个VPC及其子网。

具体方法请参见**创建虚拟私有云和子网**。

本示例中的VPC和子网资源规划详情请参见**表2-2**。

步骤2 创建vpc-X内的自定义路由表，并将subnet-X01关联至自定义路由表。

1. 在vpc-X内，创建自定义路由表。
   具体方法请参见**创建自定义路由表**。
2. 将子网subnet-X01的关联至**步骤2.1**创建的自定义路由表。
   子网创建完成后，自动关联VPC默认路由表，因此当前子网subnet-X01关联的是vpc-X的默认路由表，需要更换为**步骤2.1**创建的自定义路由表。
   具体方法请参见**更换子网关联的路由表**。

步骤3 创建四个ECS，分别属于不同的VPC内。

创建ECS，具体方法请参见**创建弹性云服务器**。

步骤4 配置ecs-X的网卡，并安装第三方防火墙软件。

1. 关闭ecs-X的网卡“源/目的检查”。
   a. 在ECS列表中，单击目标ECS的名称。
      进入ECS详情页。
   b. 选择“弹性网卡”页签，并单击 展开ECS的网卡详情区域，可以查看“源/目的检查”功能。
      如**图2-9**所示，表示“源/目的检查”功能已关闭。

图 2-9 关闭网卡的“源/目的检查”功能

2. 在ecs-X中安装第三方防火墙。

步骤5 （可选）为云服务器配置虚拟IP。

此步骤为可选：您可以在vpc-X中创建主备服务器，并绑定同一虚拟IP，当主服务器发生故障无法对外提供服务时，动态将虚拟IP切换到备服务器，继续对外提供服务。如果部署第三方防火墙的弹性云服务器不需要主备，此步骤不需要执行。

1. 在vpc-X的子网内，创建虚拟IP。

   具体方法请参见**申请虚拟IP地址**。

2. 将虚拟IP绑定到部署防火墙的主备ECS上。

   具体方法请参见**虚拟IP绑定云服务器**。

步骤6 创建3个VPC对等连接，并配置路由。

1. 创建3个VPC对等连接。
   - 如果您的VPC在同一个账号内，具体方法请参见**创建同一账户下的对等连接**，您只需要执行该章节的“创建VPC对等连接”小节。
   - 如果您的VPC在不同一个账号内，具体方法请参见**创建不同账户下的对等连接**，您需要执行该章节的“创建VPC对等连接”小节和“接受对等连接”小节。

   本示例中的VPC对等连接资源规划详情请参见**表2-4**。

2. 在3个业务VPC的默认路由表中，添加指向其他3个VPC，下一跳为对等连接的路由。

   具体方法请参见**添加自定义路由**。

   本示例中，分别在vpc-A、vpc-B、vpc-C的路由表中，添加**表2-6**中规划的路由。

3. 在防火墙VPC的默认路由表和自定义路由表中，分别配置路由。

   具体方法请参见**添加自定义路由**。

   本示例中，分别在vpc-X的默认路由表和自定义路由表中，添加**表2-7**中规划的路由。

步骤7 登录ECS，验证防火墙是否生效。

弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

本示例是通过管理控制台远程登录（VNC方式）。

1. 登录ecs-A01，验证vpc-A与vpc-B网络互通情况。

   ping *ecs-B01的私有IP地址*

   命令示例：

   ping 10.2.0.93

   回显类似如下信息，表示网络互通配置成功。

   ```
   [root@ecs-A01 ~]# ping 10.2.0.93
   PING 10.2.0.93 (10.2.0.93) 56(84) bytes of data.
   64 bytes from 10.2.0.93: icmp_seq=1 ttl=64 time=0.849 ms
   64 bytes from 10.2.0.93: icmp_seq=2 ttl=64 time=0.455 ms
   64 bytes from 10.2.0.93: icmp_seq=3 ttl=64 time=0.385 ms
   64 bytes from 10.2.0.93: icmp_seq=4 ttl=64 time=0.372 ms
   ...
   --- 10.2.0.93 ping statistics ---
   ```

2. 不要中断**步骤7.1**，登录ecs-X01，验证vpc-A到vpc-B的流量是否通过ecs-X01。
3. 在ecs-X01上，执行以下命令，检查eth0网卡的流量变化。

   至少连续执行两次命令，检查RX packets和TX packets是否变化。

   ifconfig eth0

   流量变化说明，表示流量通过ecs-X01，流量被防火墙过滤。

   ```
   [root@ecs-X01 ~]# ifconfig eth0
   eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
         inet 192.168.0.5  netmask 255.255.255.0  broadcast 192.168.0.255
         inet6 fe80::f816:3eff:feb6:a632  prefixlen 64  scopeid 0x20<link>
         ether fa:16:3e:b6:a6:32  txqueuelen 1000  (Ethernet)
         RX packets 726222  bytes 252738526 (241.0 MiB)
         RX errors 0  dropped 0  overruns 0  frame 0
         TX packets 672597  bytes 305616882 (291.4 MiB)
         TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

   [root@ecs-X01 ~]# ifconfig eth0
   eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
         inet 192.168.0.5  netmask 255.255.255.0  broadcast 192.168.0.255
         inet6 fe80::f816:3eff:feb6:a632  prefixlen 64  scopeid 0x20<link>
         ether fa:16:3e:b6:a6:32  txqueuelen 1000  (Ethernet)
         RX packets 726260  bytes 252748508 (241.0 MiB)
         RX errors 0  dropped 0  overruns 0  frame 0
         TX packets 672633  bytes 305631756 (291.4 MiB)
         TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
   ```

4. 参考**步骤7.1**~**步骤7.3**，检查其他VPC之间的通信情况。

----结束

2.3 通过第三方防火墙实现 VPC 和云下数据中心互访流量清洗

操作场景

用户IDC数据中心和华为云通过云专线（DC）或虚拟专用网络（VPN）通信成功，在华为云的内网上使用第三方虚拟化防火墙，使得云上云下的业务流量经过自定义的第三方防火墙，对云上的业务进行灵活的安全控制。

本文以用户同区域的多VPC与本地IDC连通为例，介绍混合云使用第三方防火墙的应用场景。

方案优势

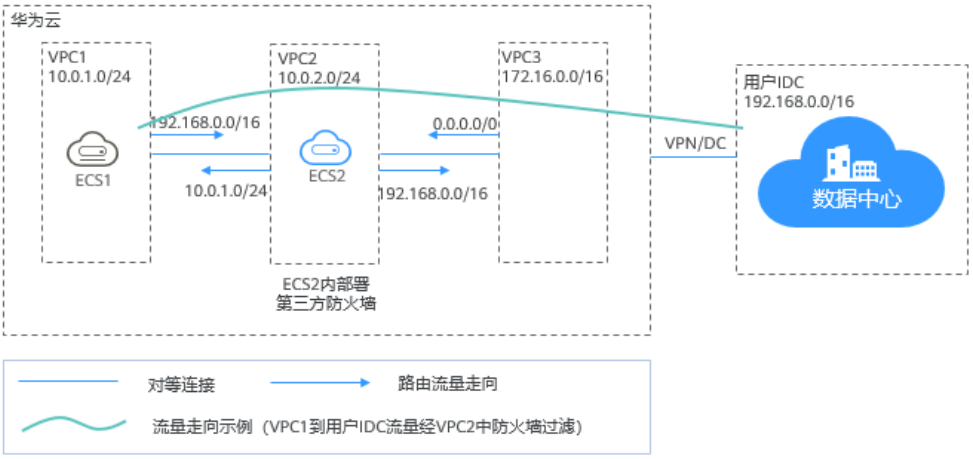
- 支持用户的第三方防火墙。
- 用户云上云下流量经过第三方防火墙。
- 支持用户自定义的更加灵活的安全策略。

典型拓扑

假设用户业务部署在VPC1、VPC2、VPC3及本地IDC中，并且需要在云上使用第三方虚拟化防火墙。用户可以将第三方虚拟化防火墙配置在VPC2的弹性云服务器中，使用对等连接及路由规则将VPC间进行连通。同时，在VPC3中创建云专线，使云上VPC与云下IDC实现连通。

实现方式如下：

图 2-10 场景示意



前提条件

VPC1与VPC2，VPC3子网网段不能重叠，否则对等连接无法通信成功。

配置步骤

步骤1 创建VPC

创建VPC1，VPC2，VPC3。

具体操作请参见**创建虚拟私有云和子网**。

说明

创建的VPC1，VPC2，VPC3网段不能重叠。例如VPC1：10.0.1.0/24；VPC2：10.0.2.0/24；VPC3：172.16.0.0/16

步骤2 创建弹性云服务器

1. 创建ECS1，ECS2，分别属于VPC1的子网，VPC2的子网。

具体操作请参见章节**创建弹性云服务器**。

说明

ECS2的网卡要关闭源/目的检查。

2. 在弹性云服务器ECS2中部署第三方防火墙。

步骤3 创建对等连接

VPC1和VPC2，VPC2和VPC3，分别创建对等连接，实现VPC间的连通。

创建对等连接时，先不配置本端和对端的路由规则，具体配置路由规则参见**配置路由规则**。

具体操作请参见**创建对等连接**。

步骤4 创建子网路由表

创建自定义路由表，关联VPC2的子网，控制VPC2的子网的出流量走向。

具体操作请参见**创建自定义路由表**。

步骤5 创建虚拟IP并绑定弹性云服务器（可选）

您可以在VPC2中创建主备服务器，并绑定同一虚拟IP，当主服务器发生故障无法对外提供服务时，动态将虚拟IP切换到备服务器，继续对外提供服务。如果不需要备用服务器，此步骤可以省略。

1. 在VPC2的子网下创建虚拟IP。

   具体操作请参见**申请虚拟IP地址**。

2. 将创建的虚拟IP绑定到弹性云服务器ECS2上。

   具体操作请参考**虚拟IP绑定云服务器**。

步骤6 创建云专线

使用VPC3创建专线，使云上VPC与云下IDC实现连通。具体操作参见**创建云专线**。

步骤7 配置路由规则

通过配置路由规则将指向目的地址的流量转发到指定的下一跳地址。

1. 修改VPC1的默认路由表，增加一条路由规则：

   VPC1 > 用户IDC，目的地址：用户IDC的CIDR，下一跳：VPC1与VPC2的对等连接。

2. 修改VPC2的默认路由表，增加一条路由规则：

   目的地址：0.0.0.0/0，下一跳：ECS2。

   如果涉及主备部署，创建了虚拟IP的情况下，此处下一跳是虚拟IP的地址。

3. 修改VPC2的子网路由表，增加两条规则：

   a. VPC2 > VPC1，目的地址：VPC1的CIDR，下一跳：VPC1与VPC2的对等连接。

   b. VPC2 > 用户IDC，目的地址：用户IDC的CIDR，下一跳：VPC2与VPC3的对等连接。

4. 修改VPC3的默认路由表，增加一条路由规则：

   目的地址：0.0.0.0/0，下一跳：VPC2和VPC3的对等连接。

由于上述的**创建云专线**创建了专线，此处有一条系统自动下发的到专线的路由

----结束

配置验证

登录弹性云服务器ECS1访问用户IDC，在ECS2中可以收到ECS1发给用户IDC的报文，报文经过ECS2中的防火墙，被防火墙规则过滤。

3 基于华为云弹性云服务器自建容器并实现通信

操作场景

在不使用华为云容器产品的情况下，支持用户在华为云弹性云服务器中部署容器，并实现同一个子网中不同弹性云服务器内的容器相互通信。

方案优势

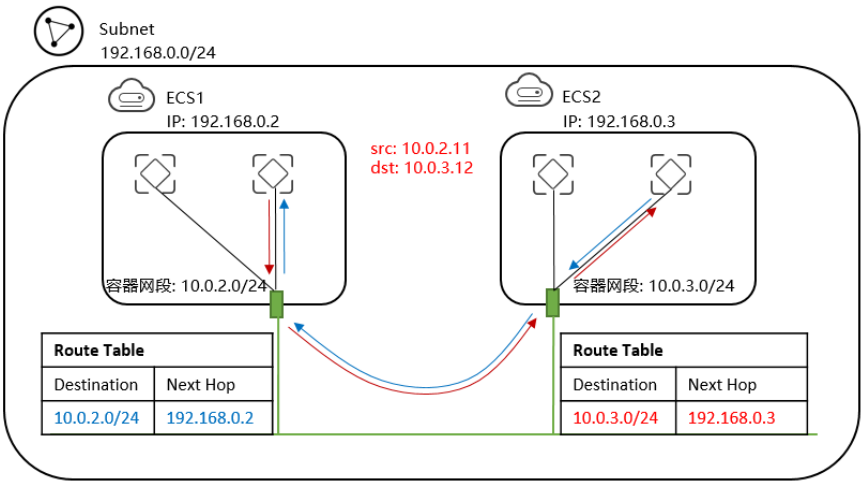
- 云服务器内部署容器，容器地址非VPC网络地址，通过VPC路由方式转发。
- 只需简单配置路由表，就可实现容器网络的互通，灵活方便。

典型拓扑

此场景下对网络拓扑有如下要求：

- 弹性云服务器在同一子网内。如图中VPC子网网段为192.168.0.0/24，弹性云服务器的IP地址为192.168.0.2和192.168.0.3。
- 容器网段与VPC子网不在一个网段，同一台弹性云服务器内的容器在同一个网段，不同弹性云服务器内容器的网段不同。如图中ECS1中容器网段为10.0.2.0/24，ECS2中容器网段为10.0.3.0/24。
- 发送给容器的数据包下一跳为容器所在弹性云服务器。如图中发送给10.0.2.0/24网段的数据包下一跳为192.168.0.2，发送给10.0.3.0/24网段的数据包下一跳为192.168.0.3。

图 3-1 网络拓扑



配置步骤

步骤1 创建VPC及VPC网段。

具体操作请参见**创建虚拟私有云和子网**。

步骤2 创建弹性云服务器。

具体操作请参见**创建弹性云服务器**。

创建完成后在弹性云服务器网卡上取消源地址校验，如**图3-2**所示。

图 3-2 取消源地址校验

步骤3 在弹性云服务器上部署容器。

您可以使用Docker CE完成容器的部署，详细操作步骤，请参考第三方软件的帮助文档，本文不做详细说明。

说明

同一台ECS内的容器需要在同一个网段，且不同ECS内容器网段不能重叠。

步骤4 添加VPC路由表信息。

在VPC路由表中添加路由信息。让发送给10.0.2.0/24网段的数据包下一跳为192.168.0.2，发送给10.0.3.0/24网段的数据包下一跳为192.168.0.3，也就是让发送给容器的数据包下一跳都为容器所在ECS。

说明

- 单个VPC中内默认支持50个不同网段的容器部署，如须扩大需要申请扩大VPC路由表数目。
- 容器迁移到其他弹性云服务器后，需要在VPC路由表中添加新的路由信息。

步骤5 添加安全组规则。

为了能够通过traceroute命令和ping命令测试容器网络是否连通，为弹性云服务器的安全组添加如**表3-1**所示规则，开放ICMP和UDP规则。

具体操作请参见**添加安全组规则**。

表 3-1 安全组规则

方向	协议/应用	端口	源地址
入方向	ICMP	全部	0.0.0.0/0
入方向	UDP	全部	0.0.0.0/0

----结束

配置验证

分别在两台弹性云服务器上部署容器，通过ping来测试容器网络是否能连通。

以使用Docker部署容器为例，在ECS1上先创建一个网络连接my-net并指定容器网段为10.0.2.0/24，然后创建容器并指定使用my-net。

```
$ docker network create  --subnet 10.0.2.0/24 my-net
$ docker run -d --name nginx --net my-net -p 8080:80  nginx:alpine
```

在ECS2上同样创建网络连接和容器，容器网段为10.0.3.0/24。

```
$ docker network create  --subnet 10.0.3.0/24 my-net
$ docker run -d --name nginx --net my-net -p 8080:80  nginx:alpine
```

将弹性云服务器上iptables里面filter表的FORWARD链的默认策略设置为ACCEPT。

说明

此处设置是因为Docker为安全性将iptables里面filter表的FORWARD链默认策略设置成了drop，因此需要修改。

```
$ iptables -P FORWARD ACCEPT
```

进入10.0.2.2这个容器，尝试ping和traceroute 10.0.3.2，可以看到能够ping通，且traceroute路由路径为10.0.2.2 -> 10.0.2.1 -> 192.168.0.3 -> 10.0.3.2，与前面设置的路由转发规则一致。

```
[root@ecs1 ~]# docker exec -it nginx /bin/sh
/ # traceroute -d 10.0.3.2
traceroute to 10.0.3.2 (10.0.3.2), 30 hops max, 46 byte packets
 1  10.0.2.1 (10.0.2.1)  0.007 ms  0.004 ms  0.007 ms
 2  192.168.0.3 (192.168.0.3)  0.232 ms  0.165 ms  0.248 ms
 3  10.0.3.2 (10.0.3.2)  0.366 ms  0.308 ms  0.158 ms
/ # ping 10.0.3.2
PING 10.0.3.2 (10.0.3.2): 56 data bytes
64 bytes from 10.0.3.2: seq=0 ttl=62 time=0.570 ms
64 bytes from 10.0.3.2: seq=1 ttl=62 time=0.343 ms
```



```
64 bytes from 10.0.3.2: seq=2 ttl=62 time=0.304 ms
64 bytes from 10.0.3.2: seq=3 ttl=62 time=0.319 ms
```

