Alibaba Cloud Virtual Private Cloud

產品簡介

檔案版本：20180807

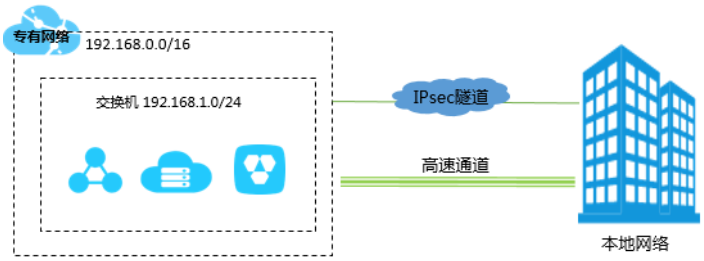
目錄

1 什麼是專有網路

Virtual Private Cloud（Virtual Private Cloud）是基於阿里雲構建的一個隔離的網路環境，專有網路之間邏輯上徹底隔離。

專有網路是您自己獨有的雲上私有網路。您可以完全掌控自己的專有網路，例如選擇IP位址範圍、配置路由表和網關等，您可以在自己定義的專有網路中使用阿里雲資源如ECS、RDS、SLB等。

您可以將專有網路連接到其他專有網路或本網，形成一個按需定製的網路環境，實現應用的平滑遷移上雲和對資料中心的擴充。



組成部分

每個VPC都由一個私網網段、一個路由器和至少一個交換器組成。

- 私網網段

  在建立專有網路和交換器時，您需要以CIDR地址塊的形式指定專有網路使用的私網網段。關於CIDR的相關資訊，參見維基百科上的*Classless Inter-Domain Routing*條目說明。

  您可以使用下表中標準的私網網段及其子網作為VPC的私網地址，更多資訊參見####。

  > 说明：
  > 要使用標準網段的子網，您需要通過*CreateVpc*介面建立VPC。

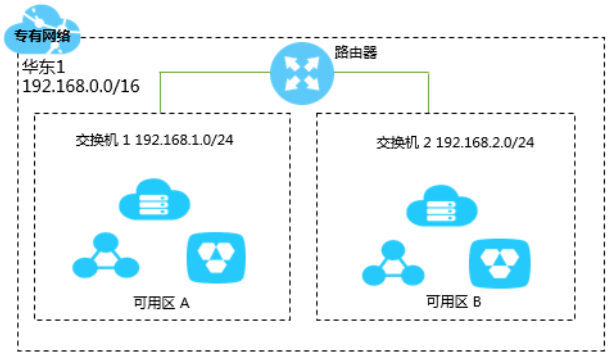
網段	可用私網IP數量（不包括系統保留地址）
192.168.0.0/16	65,532
172.16.0.0/12	1,048,572
10.0.0.0/8	16,777,212

- 路由器

  路由器（VRouter）是專有網路的樞紐。作為專有網路中重要的功能組件，它可以串連VPC內的各個交換器，同時也是串連VPC和其他網路的網關裝置。每個專有網路建立成功後，系統會自動建立一個路由器。每個路由器關聯一張路由表。更多資訊參見##。

- 交換器

  交換器（VSwitch）是組成專有網路的基礎網路裝置，用來串連不同的雲產品實例。建立專有網路之後，您可以通過建立交換器為專有網路劃分一個或多個子網。同一專有網路內的不同交換器之間內網互通。您可以將應用部署在不同可用區的交換器內，提高應用的可用性，更多資訊參見#####。



2 基礎架構

基於目前主流的隧道技術，專有網路（Virtual Private Cloud，簡稱VPC）隔離了虛擬網路。每個VPC都有一個獨立的隧道號，一個隧道號對應著一個虛擬化網路。

背景資訊

隨著雲端運算的不斷髮展，對虛擬化網路的要求越來越高，比如彈性（scalability）、安全性（security）、可靠性（reliability）和私密性（privacy），並且還有極高的互聯性能（performance）需求，因此催生了多種多樣的網路虛擬化技術。

比較早的解決方案，是將虛擬機器的網路和物理網路融合在一起，形成一個扁平的網路架構，例如大二層網路。隨著虛擬化網路規模的擴大，這種方案中的ARP欺騙、廣播風暴、主機掃描等問題會越來越嚴重。為了解決這些問題，出現了各種網路隔離技術，把物理網路和虛擬網路徹底隔開。其中一種技術是用戶之間用VLAN進行隔離，但是VLAN的數量最大隻能支援到4096個，無法支撐公共雲的巨大用戶量。

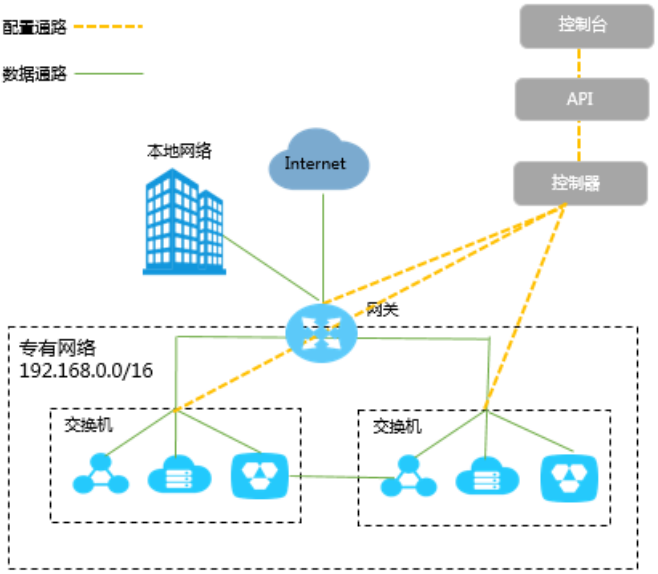
原理描述

基於目前主流的隧道技術，專有網路（Virtual Private Cloud，簡稱VPC）隔離了虛擬網路。每個VPC都有一個獨立的隧道號，一個隧道號對應著一個虛擬化網路。一個VPC內的ECS（Elastic Compute Service）實例之間的傳輸數據包都會加上隧道封裝，帶有唯一的隧道ID標識，然後送到物理網路上進行傳輸。不同VPC內的ECS實例因為所在的隧道ID不同，本身處於兩個不同的路由平面，所以不同VPC內的ECS實例無法進行通訊，天然地進行了隔離。

基於隧道技術和軟體定義程式網路（Software Defined Network，簡稱SDN）技術，阿里雲的研發在硬體網關和自研交換器裝置的基礎上實現了VPC產品。

邏輯架構

如下圖所示，VPC包含交換器、網關和控制器三個重要的組件。交換器和網關組成了數據通路的關鍵路徑，控制器使用自研的協議下發轉寄表到網關和交換器，完成了配置通路的關鍵路徑。整體架構裡面，配置通路和數據通路互相分離。交換器是分布式的結點，網關和控制器都是叢集部署並且是多機房互備的，並且所有鏈路上都有冗餘容災，提升了VPC產品的整體可用性。


配置通路
数据通路
控制台
API
控制器
本地网络
Internet
网关
专有网络
192.168.0.0/16
交换机
交换机

3 產品優勢

專有網路安全性高、配置靈活、支援多種串連方式。

安全隔離

- 不同用戶的雲端服務器部署在不同的專有網路。
- 不同專有網路之間通過隧道ID進行隔離。專有網路內部由於交換器和路由器的存在，所以可以像傳統網路環境一樣劃分子網，每一個子網內部的不同雲端服務器使用同一個交換器互聯，不同子網間使用路由器互聯。
- 不同專有網路之間內部網路完全隔離，只能通過對外映射的IP（Elastic IP Address和NAT IP）互聯。
- 由於使用隧道封裝技術對雲端服務器的IP報文進行封裝，所以雲端服務器的資料連結層（二層MAC地址）資訊不會進入物理網路，實現了不同雲端服務器間二層網路隔離，因此也實現了不同專有網路間二層網路隔離。
- 專有網路內的ECS使用安全性群組防火牆進行三層網路存取控制。

存取控制

- 靈活的存取控制規則。
- 滿足政務，金融的安全隔離規範。

軟體定義程式網路

- 按需配置網路設定，軟體定義程式網路。
- 管理操作即時生效。

豐富的網路連接方式

- 支援軟體VPN。
- 支援專線串連。

4 應用場景

專有網路（VPC）是完全隔離的網路環境，配置靈活，可滿足不同的應用場景。

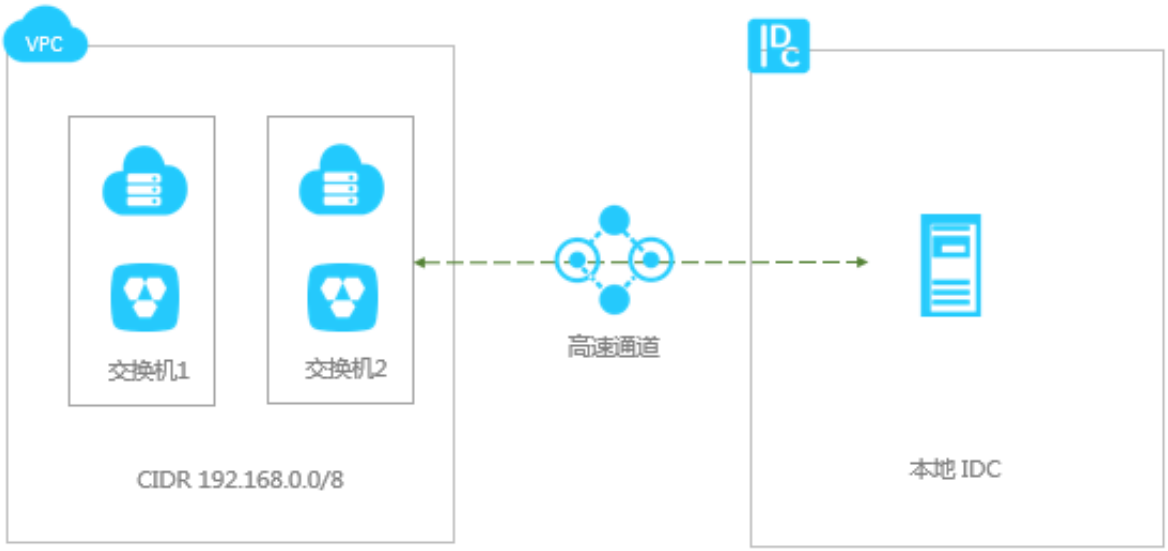
場景一：本機資料中心+雲上業務的混合雲模式

如果您有以下業務需求，建議您使用VPC+*Express Connect*+*ECS*+*RDS*的配置架構。

- 將內部核心系統與核心數據放置在自建資料中心以確保核心數據的安全；
- 雲上部署對外客戶的應用系統，即時應對業務訪問量激增。

架構解讀：

使用VPC、RDS、ECS搭建雲上業務系統，核心數據部署在雲下自建資料中心，使用Express Connect專線接入保證雲上數據快速同步，實現雲上雲下數據互通，搭建一個混合雲使用環境。



場景二：多租戶的安全隔離

如果您有以下業務需求，建議使用VPC+*ECS*+*RDS*+*SLB*的配置架構。

- 希望在雲上構建一個完全隔離的業務環境，因為傳統雲架構的多租戶共用機制不能保證數據安全；
- 自主定義私有網路設定。

架構解讀：

您可以在阿里雲上建立一個專有網路，和其他租戶的網路完全隔離。您可以完全掌控自己的虛擬網路，例如選擇自己的IP位址範圍、劃分網段、配置路由表和網關等，從而實現安全而輕鬆的資源訪問和應用程式訪問。此外，您也可以通過專線或VPN等串連方式將您的專有網路與傳統資料中心相連，形成一個按需定製的網路環境，實現應用的平滑遷移上雲和對資料中心的擴充。

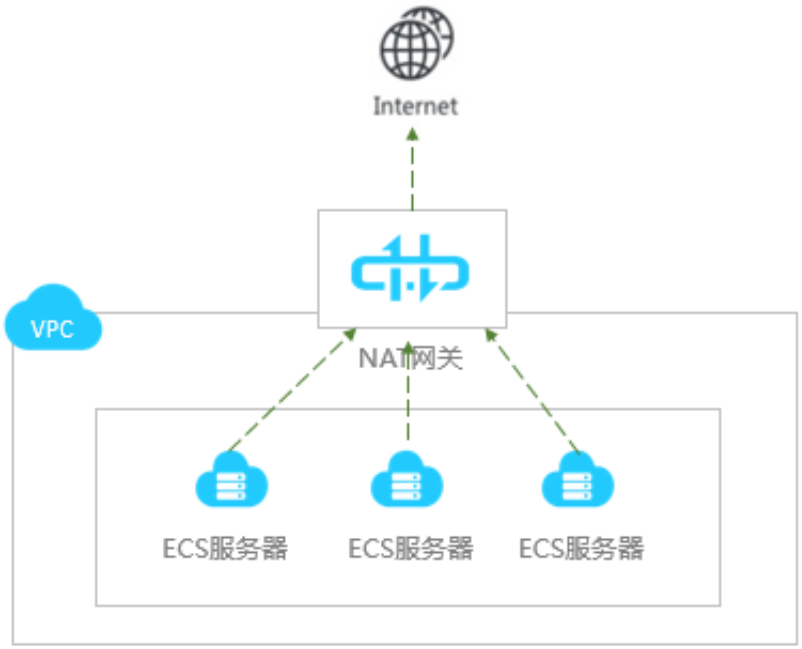
場景三：主動訪問公網的抓取類業務

如果您有以下業務需求，建議使用VPC+*ECS*+*NAT Gateway*的配置架構。

- 專有網路中的多個伺服器可以主動訪問互連網；
- 避免這些伺服器的公網IP暴露在公網上。

架構解讀：

您可以對專有網路中的同一虛擬交換器下的所有ECS做SNAT配置，多台ECS通過同一公網IP訪問互連網，並可隨時進行公網IP替換，避免被外界攻擊。



5 VPC串連

阿里雲提供了豐富的解決方案以滿足VPC內的雲產品實例與Internet、其他VPC、或本機資料中心（IDC）互連的需求。

串連公網（**Internet**）

當專有網路中的雲產品需要和Internet通訊時，您可以使用NAT Gateway、Elastic IP Address（EIP）或負載平衡等產品如下表所示。

产品	功能
弹性公网IP（EIP）	能够动态和VPC ECS绑定和解绑，支持VPC ECS访问公网（SNAT）和用户从公网访问VPC ECS（DNAT）。
VPC ECS固定公网IP	在专有网络内创建ECS时自动分配的公网IP，支持VPC ECS访问公网（SNAT）和用户从公网访问VPC ECS（DNAT）。
NAT网关	NAT网关支持多台VPC ECS访问公网（SNAT）和用户从公网访问VPC ECS（DNAT）。 NAT网关有自有的带宽包，本身就支持共享带宽。
负载均衡	基于端口的公网负载均衡，支持从公网通过负载均衡访问ECS。

串連**VPC**或本地**IDC**

當您的VPC需要和其他VPC或本地IDC互連時，您可以使用VPN網關、Express Connect、雲企業網等產品，或組合使用構建混合雲環境。

表 **5-1:** 私网连接

产品	功能	优势
高速通道	• VPC与VPC互通 支持位于相同地域或不同地域，同一账号或不同账号的VPC之间进行内网互通。 • 与本地IDC互通 通过物理专线接入使VPC与本地数据中心网络互通。	• 基于骨干网络，延迟低。 • 专线连接更加安全、可靠、速度更快、延迟更低。

产品	功能	优势
VPN网关	• VPC与VPC互通 提供IPsec-VPN功能，通过在两个VPC之间创建IPsec连接，建立加密通信通道。 • 与本地IDC互通 提供IPsec-VPN功能，通过IPsec连接，可以将本地数据中心网络和云上VPC连接起来。 • 多本地IDC连接 VPN网关默认开始VPN-Hub功能，支持多站点连接。各连接的站点不仅可以和VPC互通，并且各站点之间也可以通过VPN-Hub通信。 • 客户端远程接入 通过建立SSL-VPN连接，客户端可以远程接入VPC。	• 成本低、安全、配置简单，即开即用，但网络质量依赖公网（Internet）。 • IPsec-VPN支持IKEv1和IKEv2协议。只要支持这两种协议的设备都可以和阿里云VPN网关互连，比如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和 Ixia等。 • SSL-VPN连接支持Windows、Linux、Mac、IOS和Android等操作系统多终端接入。
云企业网	• VPC与VPC互通 支持将多个不同地域、不同账号的VPC连接起来，构建互联网络。 • 与本地IDC互通 支持将要互通的本地IDC关联的边界路由器（VBR）加载到已创建的云企业网实例，构建互联网络。 • 多VPC与IDC互通 支持将要互通的多个网络实例（VPC和VBR）加载到已创建的云企业网实例，构建企业级互联网络。	• 配置简单，自动学习分发路由。 • 低时延高速率。 • 加载到同一个云企业网实例的网络实例（VPC/VBR）全互通。 • 同地域网络实例互通免费。

产品	功能	优势
智能接入网关	• 可实现线下机构（IDC/分支机构/门店等）接入阿里云数据中心，轻松构建混合云。 • 支持线下机构互通	• 配置高度自动化，即插即用，网络拓扑变化自适应快速收敛。 • 城域内Internet就近接入，可通过设备及链路级主备方式实现线下多机构可靠上云。 • 混合云私网加密互连，Internet传输过程中加密认证。

6 基本概念

術語	說明
專有網路（VPC）	專有網路是您基於阿里雲建立的自訂私有網路，不同的專有網路之間徹底邏輯隔離。您可以在自己建立的專有網路內建立和管理雲產品實例，例如ECS，SLB，RDS等。
交換器（VSwitch）	交換器是組成專有網路的基礎網路裝置。它可以串連不同的雲產品實例。在專有網路內建立雲產品實例時，必須指定雲產品實例所串連的交換器。
路由器（VRouter）	路由器是專有網路的樞紐。它可以串連專有網路的各個交換器，同時也是串連專有網路與其它網路的網關裝置。路由器根據具體的路由條目的設定來轉寄網路流量。
路由表（Route Table）	路由表是指路由器上管理路由條目的列表。
路由條目（Route Entry）	路由表中的每一項是一條路由條目。路由條目定義了通向指定目標網段的網路流量的下一跳地址。路由條目包括系統路由和自訂路由兩種類型。

7 使用限制

資源	預設限制	提升配額
每個地域可建立的專有網路數量	10	提交工單
專有網路可選的網段範圍	192.168.0.0/16，172.16.0.0/12，10.0.0.0/8以及它們的子網	提交工單
單個專有網路的路由器數量	1	無法調整
單個專有網路的交換器數量	24	提交工單
單個專有網路的路由表數量	1	無法調整
單個路由表的自訂路由條目數量	48	提交工單
單個專有網路容納雲產品數量	15,000	無法調整