AWS 中最最基础的网络概念

StrokMitream 举报

2020-06-28 21:50

AWS 中最最基础的网络概念

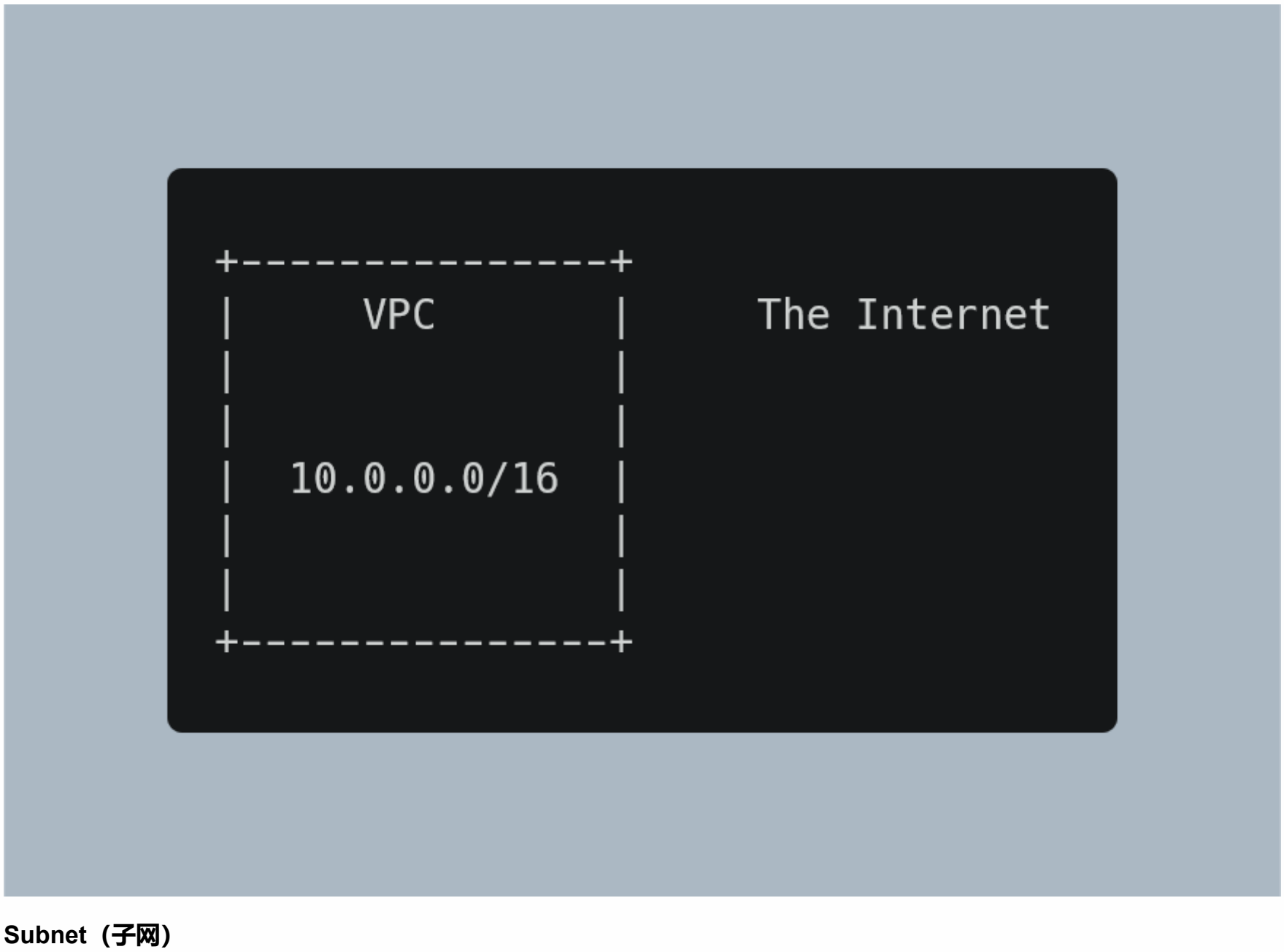
原文：https://grahamlyons.com/article/everything-you-need-to-know-about-networking-on-aws

如果你有在 AWS 有基础设施服务或应用程序，那么下面所有这些概念你都将会碰到。
这些不仅仅是网络设施的一部分，根据我的经验来看，更是其中最重要的部分之一。

VPC

VPC （Virtual Private Cloud ），虚拟私有云，是你的基础设施所运行在的一个私有网络空间。你可以自己选择 VPC 的地址空间（CIDR 范围），例如10.0.0.0/16 。这将决定 VPC 内有多少可分配 IP 。因为 VPC 内的每一台服务器都需要一个 IP 地址，所以 VPC 地址空间的大小，将决定该私有网络可容纳的资源上限。 10.0.0.0/16 地址空间的可用地址从10.0.0.0 到10.0.255.255 , 一共 2^16， 65,536 个 IP 地址。

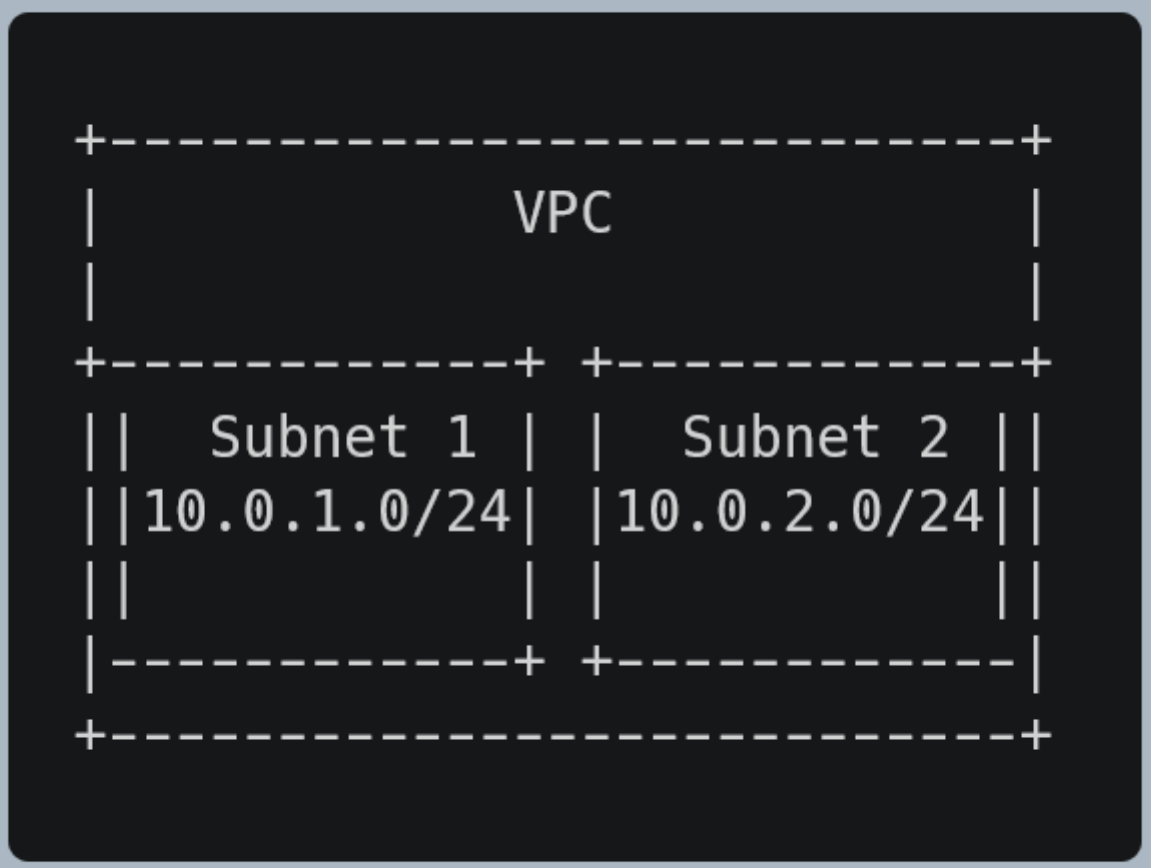
VPC 是 AWS 中最基础的基础，每一个新创建的账户，在每个AZ （Available Zone，可用区），都包含一个带子网 的默认 VPC 。



Subnet（子网）

subnet（子网）是 VPC 的一部分，有其单独的 CIDR 范围和流量转发规则。其 CIDR 范围是 VPC 的一个子集。举个栗子，10.0.0.0 的一个子网 10.0.1.0/24，地址范围从 10.0.10.0 到 10.0.1.255 ，一共 256 个 IP 地址。

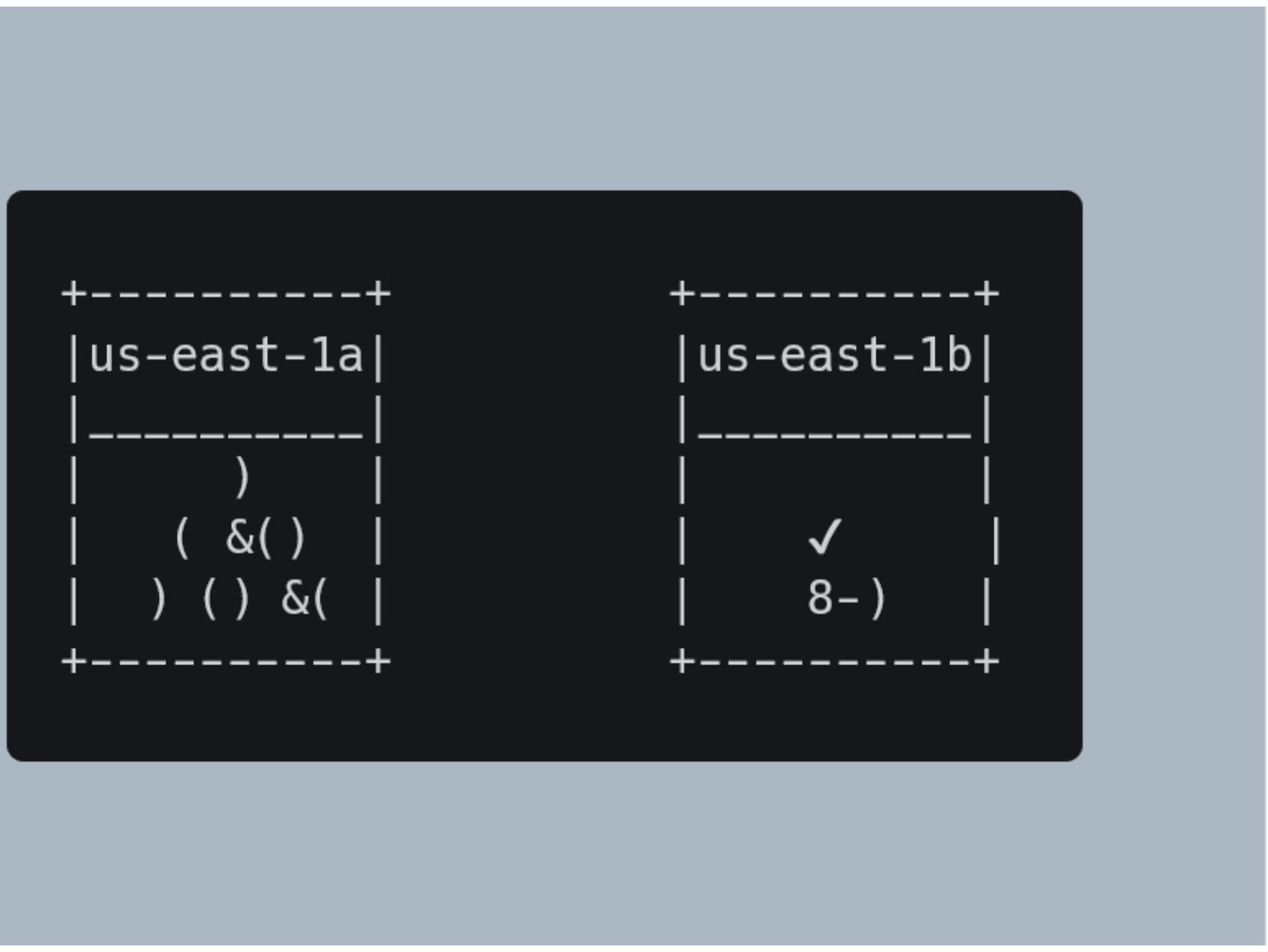
根据是否可以从外部（公网）访问进来，子网也经常被称为“公有”或“私有”子络。这种可见度是由网络路由规则控制的，每个子网都有其自己的规则。
子网必须位于某个区域具体的 AZ 中，因此，在每个区域划分子网是很好的做法。如果你要划分公有子网和私有子网，那么，在每个 AZ 都要有一套。



Availability Zones （可用区）

前面我们说到，每个 Availability Zone 必须有子网，可是，这到底是什么意思呢？

在 AWS 中，为了保证每个地区资源的极高的可用性。每个区域（zone）的资源都被划分为 2 个或更多不同可用区（AZ）。对每个区域（zone）来说，基本上即使其他所有 AZ 都中断了，也要确保至少有一个 AZ 还能正常运行。



Routing Tables（路由表）

路由表，是一系列规定子网 IP 数据包如何传输到其他不同 IP 地址的规则。

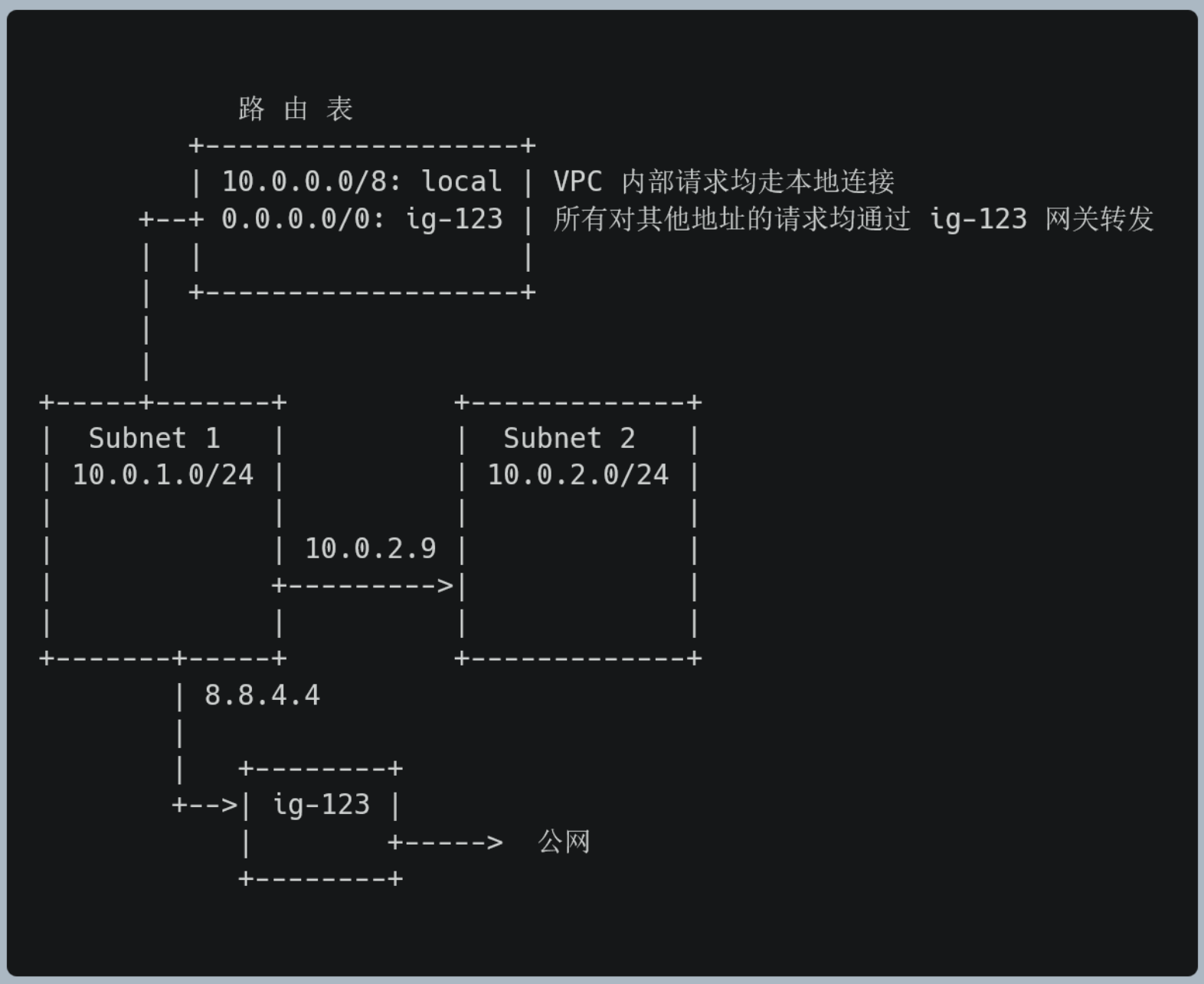
每个 VPC 内，都有一个默认的路由表，只允许流量在本地（VPC 内部）转发。如果某个子网没有关联路由表，则使用该默认路由，也就是一个“私有”子网。

如果你想要能从外部访问子网，那么你就需要创建一个路由表，显式地指定该规则。这样，关联该路由表的子网就是“公有”子网。

Internet Gateways（互联网网关）

将子网配置为可从外部访问的路由表，需要借助互联网网关来控制外部数据包出入 VPC 。

例如，创建一个网关，配置规则为所有去往 0.0.0.0/0 的数据包均需通过网关 。

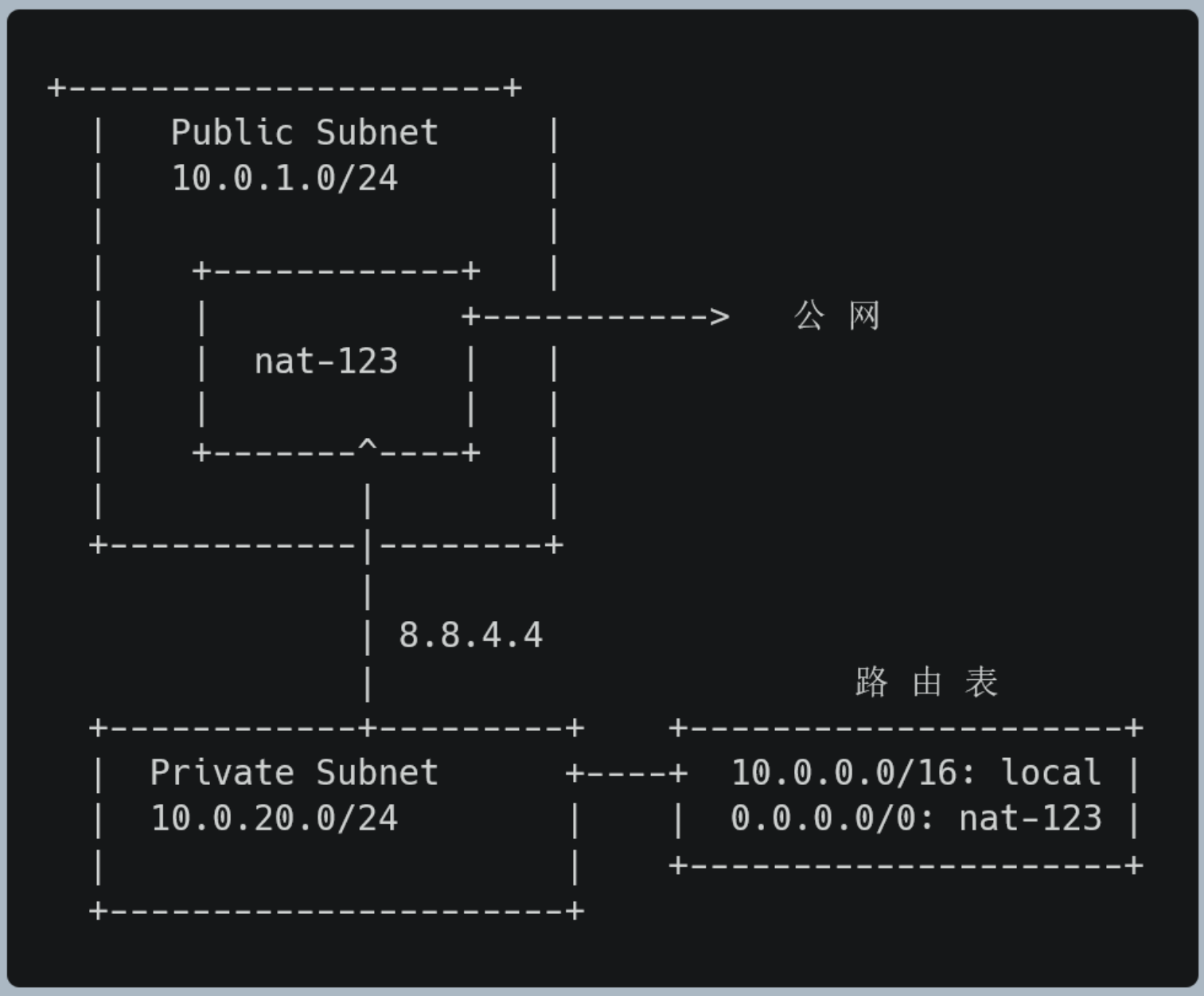


NAT Gateways（NAT 网关）

如果你有一台在 AWS 私有子网内，不允许公网访问的 EC2 实例，那么该实例的数据也没办法发送到公网。我们需要一种机制，将数据包发出去，并且正确地接收到对端的响应包。这便是 NAT ——网络地址转换，跟家里的 wifi 路由器很类似。

NAT 网关是位于公有子网的一个设备，负责接收从私有子网发往公网的数据包，转发至其目的地址；同时转发返回的数据包到源地址。

如果你 VPC 中私有子网中的实例不需要公网访问的话，那么 NAT 并不是必需的。只有你的实例需要访问诸如外部 API，SaaS 数据库等时，你才需要配置 NAT 网关。或者是使用 AWS 提供的 NAT 网关资源（由 AWS 配置，更易于用户管理）。



•NAT 网关位于公有子网中•从私有子网发出对某个公网地址的请求•根据路由表规则，请求数据包被转发到 NAT 网关•NAT 网关将数据包转发出去

Security Groups（安全组）

VPC 网络安全组标志 VPC 中的哪些流量可以发往 EC2 实例或从 EC2 发出。安全组指定具体的入向和出向流量规则，并精确到源地址（入向）和目的地址（出向）。这些安全组是与 EC2 实例而非子网关联的。

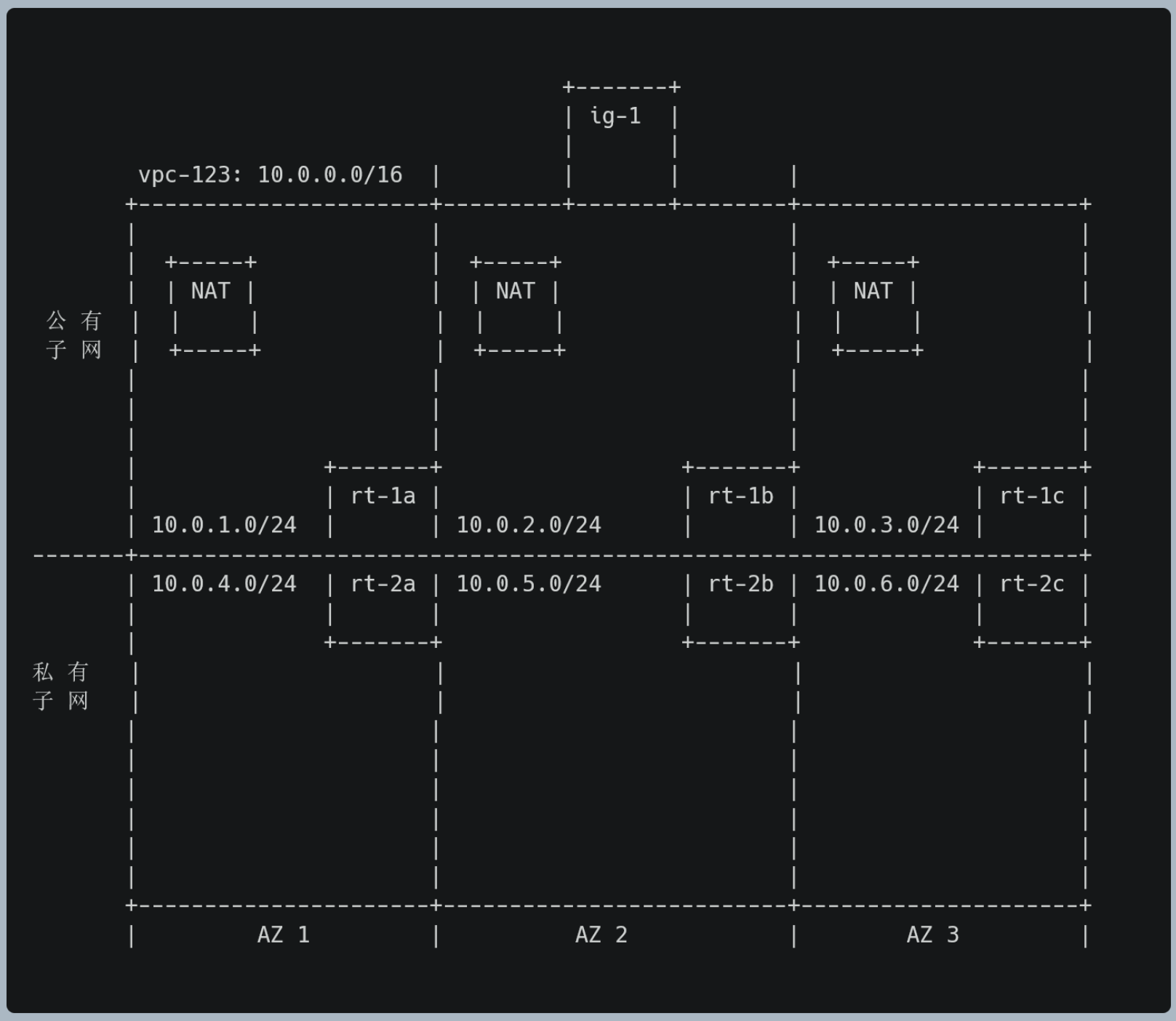
默认情况下，流量只允许出，不允许入。

入向规则可具体指定源地址——CIDR 段或者另一个安全组亦或是端口范围。当指定的源地址为另一个安全组时，该安全组必需位于同一个 VPC 。例如，VPC 默认的安全组允许任意来自同一安全组的访问流量。如果将该安全组应用于 VPC 内创建的所有资源，那么该 VPC 中的资源之间将可以互通。

•实例 (i-67890) 的安全组 (sg-abcde) 允许来自 443 端口的 TCP 流量•来自 IP 10.0.1.123 22 端口的请求不被允许通过•来自 443 端口的请求被允许通过

所有这些组装起来

整个虚拟网络完整的架构如下图所示：公有子网/私有子网跨越 AZ 将整个网络划分为两部分。NAT 位于公有子网，用路由表指定数据包的路由规则。 EC2 实例将运行于任意子网，附加安全组。



Reference

•1.Amazon Virtual Private Cloud 用户指南 https://docs.amazonaws.cn/vpc/latest/userguide/what-is-amazon-vpc.html

【AWS】VPC 系列（一）一文搞懂「可用区」「子网」「Internet 网关」「NAT 网关」

麻薯
香港科技大学 理学硕士

前言

VPC 是 AWS 中最基础也是应用最广泛的一个服务，然而大多数人对 VPC 却不甚了解，以至于经常遇到一些奇怪的网络问题。
计算机网络是一门既复杂又晦涩难懂的学科，就连 VPC 的官方文档也是写得云里雾里，这让很多没有网络背景的人根本无从下手。

本系列文章旨在从实战的角度出发介绍 VPC 的基本概念，让没有网络背景的人也可以轻松玩转 VPC。
本文会介绍 VPC 最基础的几个概念：可用区、子网、Internet 网关和 NAT 网关。尤其是子网，在创建很多资源的时候都要指定。

VPC

> 通过 Amazon Virtual Private Cloud（Amazon VPC），您可以将 AWS 资源启动到您定义的虚拟网络中。这个虚拟网络与您在数据中心中运行的传统网络极其相似，并会为您提供可扩展的基础设施。

-摘自 AWS 官方文档

换句话说，VPC 是 AWS 为你开辟的一块专属空间，这个 VPC 就是你的专属领地，其他人无法入侵。

可用区（Available Zone、AZ）

> 一个可用区（AZ）是指一个 AWS 区域中的一个或多个离散的数据中心，具有冗余电源、联网和连接。可用区让客户能够运行在可用性、容错能力和可扩展性方面比单个数据中心更强的生产应用程序和数据库。一个 AWS 区域中的所有可用区都通过高带宽、低延迟网络与完全冗余的专用城域光纤互连，为可用区之间提供高吞吐量和低延迟的联网。可用区之间的所有流量都进行了加密。网络性能足以确保可用区之间的同步复制。可用区使分区应用程序更容易获得高可用性。如果应用程序在可用区之间进行分区，则可以更好地隔离公司并防止断电、雷击、龙卷风、地震等问题的影响。可用区与任何其他可用区都间隔一定距离，不过彼此都在 100 公里（60 英里）以内。

-摘自 AWS 官方文档

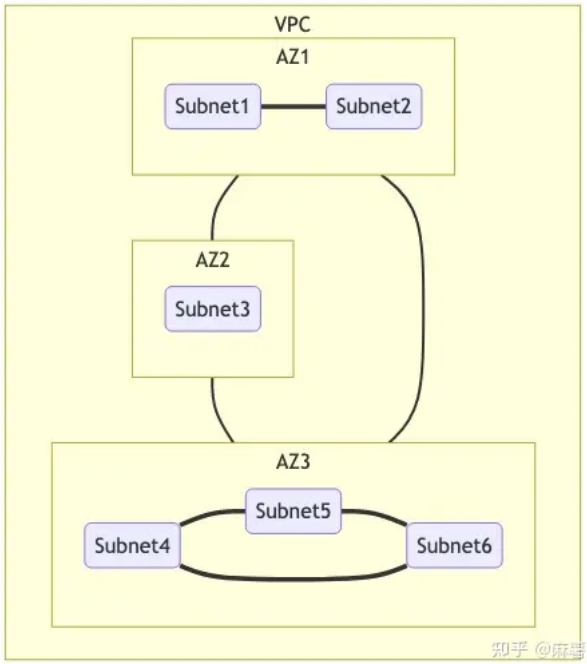
可用区的作用是增强可用性。如果一个可用区出现了故障（例如断网、断电），其他可用区可以继续提供服务，用户完全无感知。可用区之间的网络延迟极低，就像大学校园里的局域网一样。因此不同的可用区就像在同一个大的局域网中，可以通过**内网 IP** 直接访问。

子网（Subnet）

> 子网是您的 VPC 内的 IP 地址范围。您可以将AWS资源（例如 EC2 实例）在特定子网中启动。在创建子网时，指定子网的 IPv4 CIDR 块，它是 VPC CIDR 块的子集。每个子网都必须完全位于一个可用区之内，**不能跨越多个可用区**。通过在独立的可用区内启动实例，您可以保护您的应用程序不受单一可用区故障的影响。

-摘自 AWS 官方文档

简单来说，子网就是在可用区内基于 IP 地址再划分出的专属区域，每个子网的 IP 地址段**互不重叠**。下图展示了 VPC、可用区和子网的关系。该示例中的 VPC 总共包含三个可用区，每个可用区划分出了若干个子网。



子网

子网类型

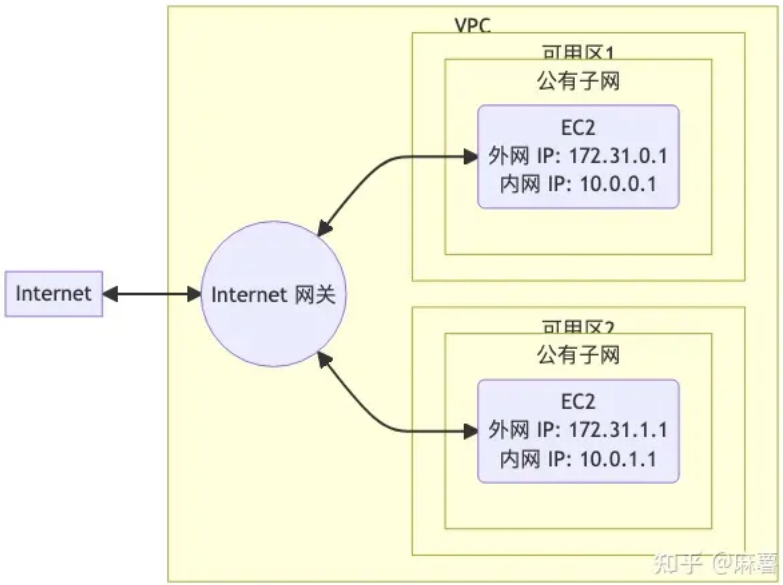
子网存在的意义是什么？为什么要在可用区里创建子网？要回答这个问题，首先要知道有哪几种类型的子网。
VPC 总共有三种类型的子网：

- **公有**子网
- 带有 NAT 网关的**私有**子网
- 被隔离的**私有**子网

有的子网可以访问外网，有的则不能；有的子网可以被外网访问，而有的则不能。听着有些拗口，像绕口令一样，下面具体看看这 3 种子网都有什么特性。

公有子网

公有子网具有**最大**的连通性，既可以访问 Internet 也可以被 Internet 访问。公有子网中的资源有两个 IP 地址：**外网 IP** 和**内网 IP**，Internet 网关作为桥梁，连接了 Internet 和公有子网。



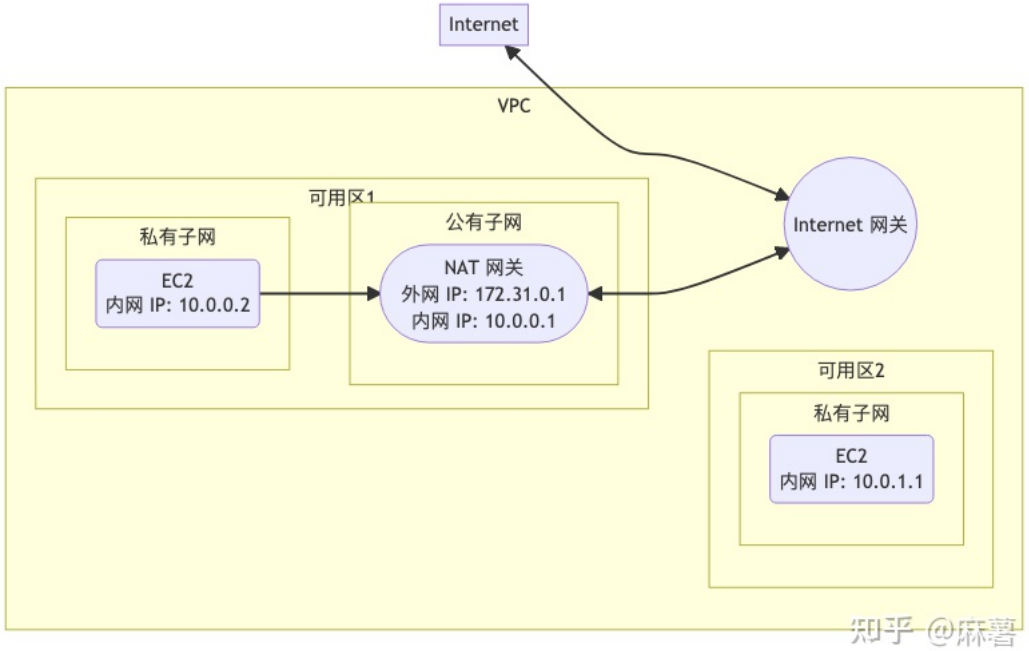
公有子网

需要注意的是每个 VPC 只有**一个** Internet 网关，而且 Internet 网关只是 VPC 和 Internet 之间的一个**逻辑连接**，不是一个物理设备。因此 Internet 网关的带宽并不由 Internet 网关本身决定，而是由 EC2 的带宽决定。

如果没有 Internet 网关，VPC 将失去和 Internet 的连接。
最后再总结一下 Internet 网关的作用：让公有子网内的资源连接 Internet，同时也让 Internet 连接公有子网内的资源。

带有 NAT 网关的私有子网

NAT 网关介于私有子网和 Internet 网关之间，能够将私有子网内的多个**私有 IP** 映射到一个**公有 IP**，从而让私有子网内的资源可以访问 Internet。下图展示了一个 NAT 网关的使用案例。



私有子网

NAT 网关是和 EC2 平级的位于公有子网内的计算资源，负责**私有 IP** 和**公有 IP** 的转换及流量转发。
可用区 1 中的 EC2 通过 NAT 网关访问 Internet。而可用区 2 没有 NAT 网关，因此该可用区内的 EC2 **无法**访问 Internet。

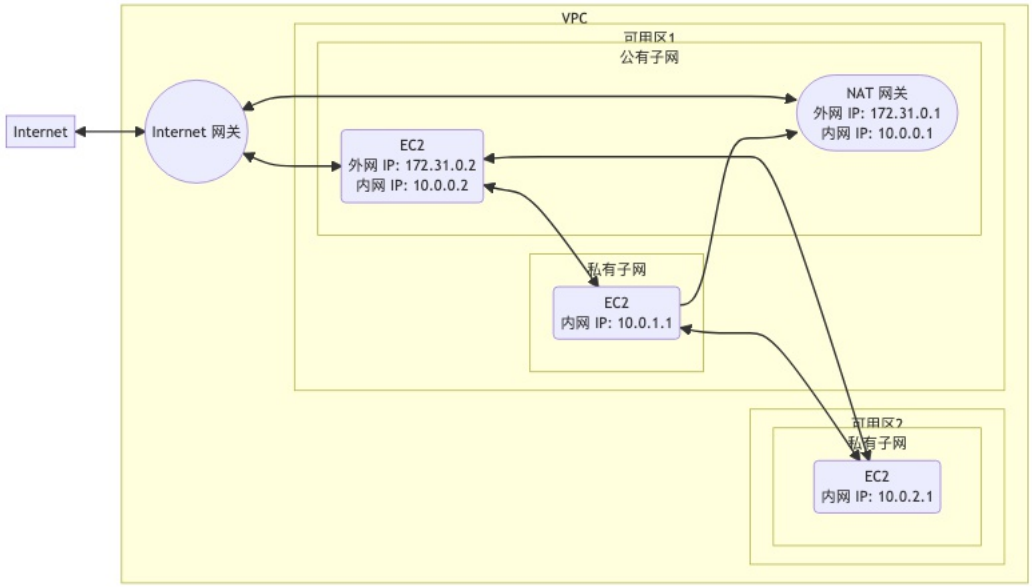
NAT 网关和 Internet 网关有以下几个区别：

1. NAT 网关负责让**私有**子网访问 Internet；Internet 网关负责让**公有**子网访问 Internet。
2. NAT 网关的连接是**单向**的，私有子网可以访问 Internet，但是 Internet **无法**访问私有子网（除非显示地允许该访问，但不在本文的讨论范围之内）；Internet 网关的连接是**双向**的。
3. NAT 网关工作在**可用区**，Internet 网关工作在 **VPC**。
4. NAT 网关运行于具体的**物理设备**，带宽从 5Gbps 至 45Gbps 不等，因此使用 NAT 网关会产生额外费用；Internet 网关只是个**逻辑连接**，没有带宽限制，也不会产生费用。

隔离的私有子网

隔离的私有子网就是**没有** NAT 网关的私有子网，上图中可用区 2 的私有子网就是一个隔离的私有子网。隔离的私有子网无法访问或被 Internet 访问，只能和 VPC 内的资源相互连接。

下图是融合了公有子网、带有 NAT 的私有子网以及隔离的私有子网的使用案例。



融合案例

上图涉及到 5 类参与方，分别是：

1. 公有子网的**外网 IP**
2. 公有子网的**内网 IP**
3. 带有 NAT 网关的私有子网的**内网 IP**
4. 隔离的私有子网的**内网 IP**
5. Internet

下边的表格总结了这 5 方的连通性（**Y** 表示可联通，**N** 表示不可联通）。
该表格的**行**为连接的发起方，**列**为连接的接收方。例如从 Internet 发起向公有子网外网 IP 的连接，对应表格的最后一行第一列，该格的值是 **Y**，表示可连通。

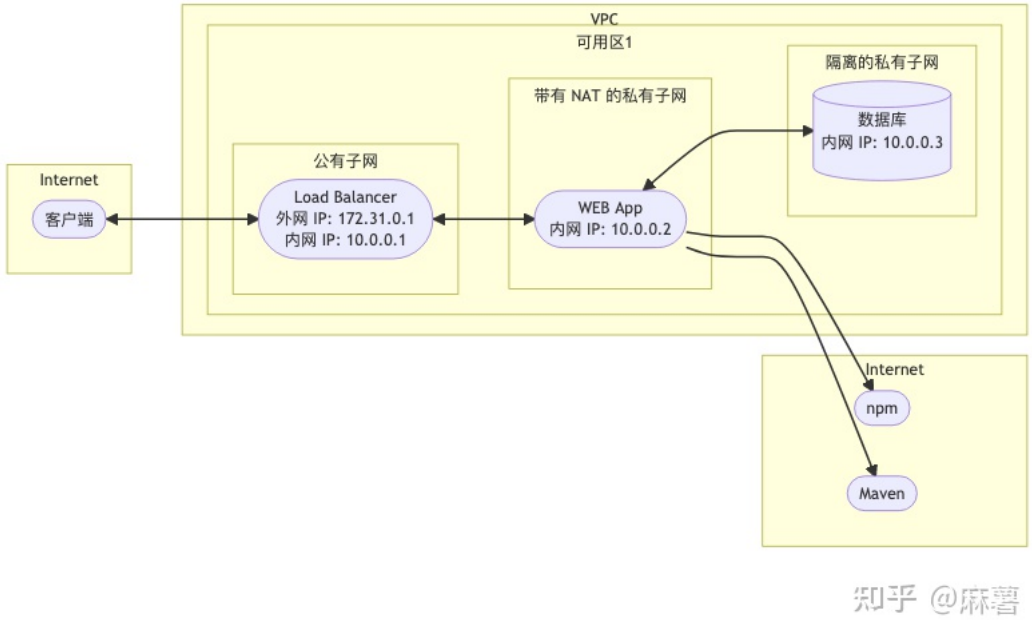
通信方	公有子网外网 IP	公有子网内网 IP	带有 NAT 网关的私有子网内网 IP	隔离的私有子网内网 IP	Internet
公有子网	Y	Y	Y	Y	Y
带有 NAT 网关的私有子网	Y	Y	Y	Y	Y
隔离的私有子网	N	Y	Y	Y	N

Internet	Y	N	N	N	Y

子网实战案例

回到最开始的问题，子网存在的意义是什么？答案是为了**安全**。诚然，将所有资源都放置在公有子网中完全不影响功能性。但是这样一来，VPC 内的所有资源就都暴露在了互联网之上，随时有遭到攻击的可能。因此将敏感的资源（例如数据库）放置在私有子网内，和外界彻底隔离，从而提升系统的安全性。

通过一个典型的 API 案例来说明如何正确地使用这 3 种子网类型。为了清晰起见，略去 Internet 网关和 NAT 网关。



API 实战案例

公有子网中的 Load Balancer 作为 Internet 的唯一入口，接收来自客户端的请求并转发给私有子网内的 WEB App。WEB App 接到 Load Balancer 转发过来的请求后查询数据库生成响应结果，并通过 Load Balancer 返回给客户端。

总结

以上就是关于可用区、子网、Internet 网关和 NAT 网关的基本介绍，希望这篇文章能帮助你了解 VPC 最基础的概念。更详尽的介绍请参阅 AWS 的官方文档。

发布于 2022-04-06 22:43