AWS EC2 Network Configuration

AWS EC2 实例的内外网连接涉及几个关键的网络组件和配置。以下是一个详细的解释，描述了如何使公有 IP（Public IP）和私有 IP（Local IP）之间的通信正常工作：  
  
1. 公有 IP 和私有 IP  
- 私有 IP（Private IP）：这是实例内部的 IP 地址，只在你的 VPC（虚拟私有云）内部有效，用于内部通信。  
- 公有 IP（Public IP）：这是实例的外部 IP 地址，可以从互联网访问。  
  
2. 关键网络组件  
- VPC（Virtual Private Cloud）：这是一个虚拟网络，类似于你自己的数据中心。在 VPC 内部，你可以定义子网、路由表、网络ACL等。  
- 子网（Subnet）：这是一个VPC内的子网络，可以是公有子网（有互联网访问权限）或私有子网（没有直接互联网访问权限）。  
- Internet Gateway：这是一个连接 VPC 和互联网的网关，使得公有子网中的实例可以访问互联网。  
- 路由表（Route Table）：定义了流量的去向规则。通常，公有子网的路由表会有一条指向 Internet Gateway 的路由。  
- NAT Gateway/Instance：用于让私有子网中的实例能够访问互联网（出站流量），但不允许外部互联网直接访问这些实例（入站流量）。  
  
3. 公有子网和私有子网的配置  
- 公有子网：通常包含直接连接到 Internet Gateway 的实例，这些实例会有公有 IP 地址。  
- 私有子网：通常包含不直接连接到 Internet Gateway 的实例，这些实例没有公有 IP 地址，但可以通过 NAT 网关访问互联网。  
  
4. 实例的网络配置  
- 分配私有 IP：当你启动 EC2 实例时，它会自动分配一个私有 IP 地址。  
- 分配公有 IP：你可以选择自动分配一个公有 IP 地址，或者在实例启动后手动分配一个弹性 IP（Elastic IP）。  
  
5. 路由配置  
- 公有子网的路由表：  
 - 有一条指向 Internet Gateway 的默认路由（0.0.0.0/0）。  
- 私有子网的路由表：  
 - 通常有一条指向 NAT Gateway 的默认路由（0.0.0.0/0）。  
  
6. 安全组和网络ACL  
- 安全组（Security Group）：作用于实例级别，定义了入站和出站流量的允许规则。  
- 网络ACL（Network ACL）：作用于子网级别，提供了一个更细粒度的流量控制机制，通常作为安全组的补充。  
  
7. 连接流程  
- 从外部访问实例：  
 - 当一个外部请求到达实例的公有 IP 时，流量首先经过 Internet Gateway，然后通过路由表指向公有子网的实例。  
 - 实例的安全组会检查入站规则，决定是否允许该流量通过。  
  
- 从实例访问外部：  
 - 当一个实例尝试访问互联网（出站流量），如果实例在公有子网，流量会通过路由表指向 Internet Gateway，然后到达互联网。  
 - 如果实例在私有子网，流量会通过 NAT Gateway，然后到达互联网。  
  
图解：  
+-------------------------+ +---------------------+  
| Internet | | VPC |  
| | | |  
| | | +----------------+ |  
| | | | Subnet (Public)| |  
| | | | | |  
| | | | +----------+ | |  
| | | | | EC2 Inst | | |  
| | | | +----------+ | |  
| | | | | | |  
| | | +-------|--------+ |  
| | | | |  
| | | +-------|--------+ |  
| | | | Subnet (Private)| |  
| | | | | |  
| +----------+ | +----------+ | |  
| | | EC2 Inst | | |  
| | +----------+ | |  
| +----------------+ |  
+--------------------------------------+------------------+  
Notes:  
- Public subnet has a route to the Internet Gateway.  
- Private subnet uses a NAT Gateway for outbound internet traffic.  
- Security Groups and Network ACLs control traffic at the instance and subnet levels respectively.