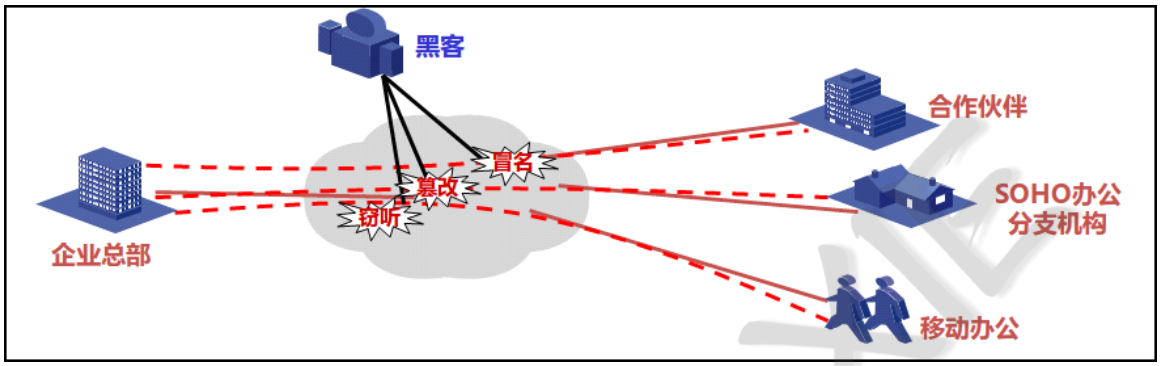
VPN基础

VPN产生背景：

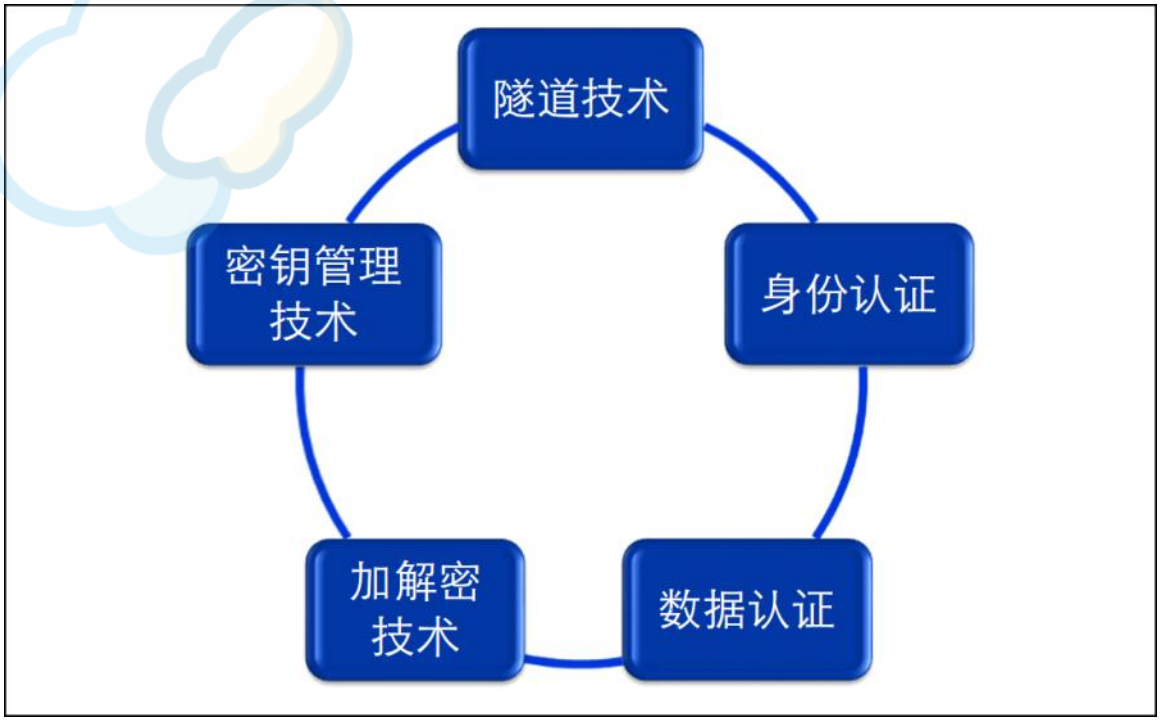
- 在Internet的传输中，绝大部分数据的内容都是明文传输的，存在很多安全隐患（如：窃听、篡改、冒充）
- 总部、分公司、办事处、出差人员、合作单位需要访问总部网络资源的问题
- 

VPN：Virtual Private Network，虚拟专用网络

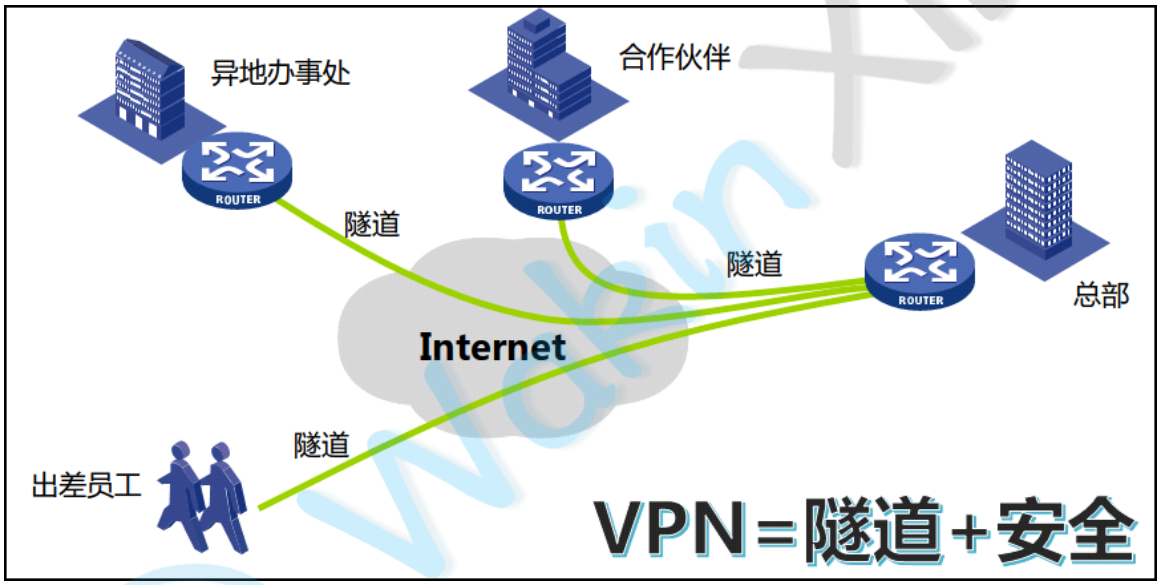
-

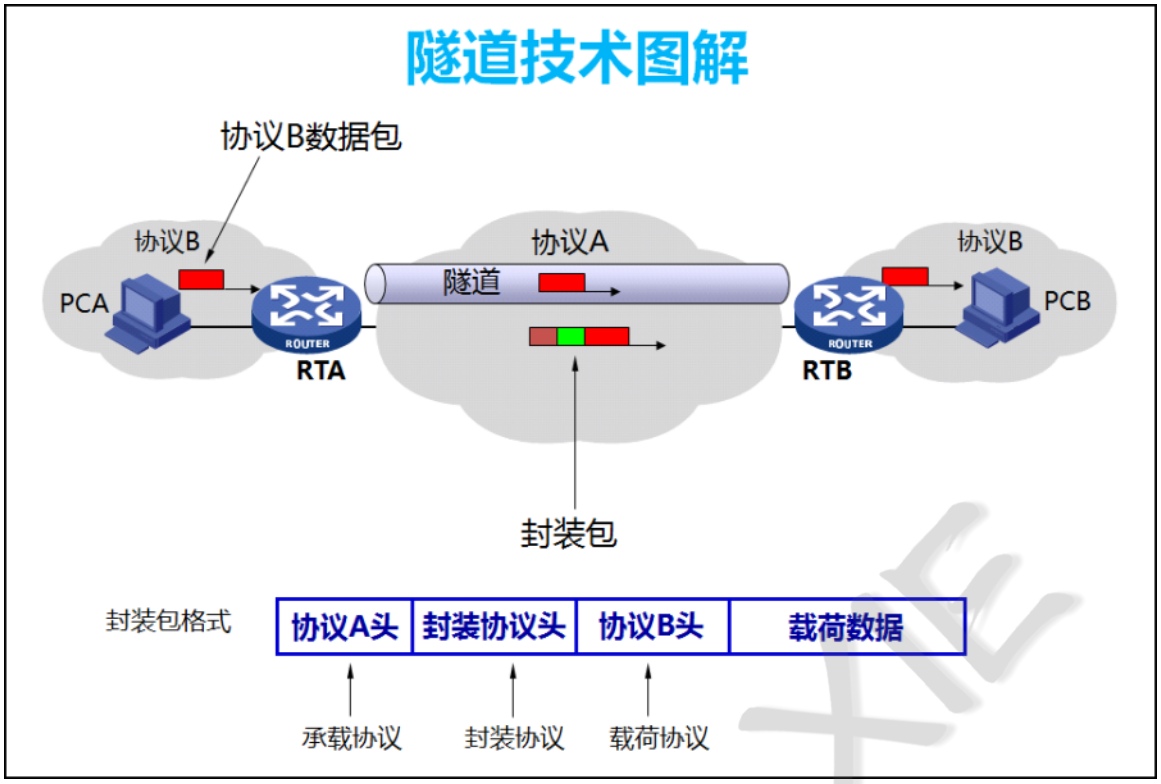
术语	备注
VPN	通过公共网络建立私有网络，并提供一定的安全性和服务质量保证。 IETF草案对基于IP的VPN的定义：使用IP机制仿真出一个私有的广域网
虚拟	用户不再需要拥有实际的专线，而是利用Internet建立自己的私有网络 。
专用	用户可以为自己制定一个最符合自己需求的网络 。

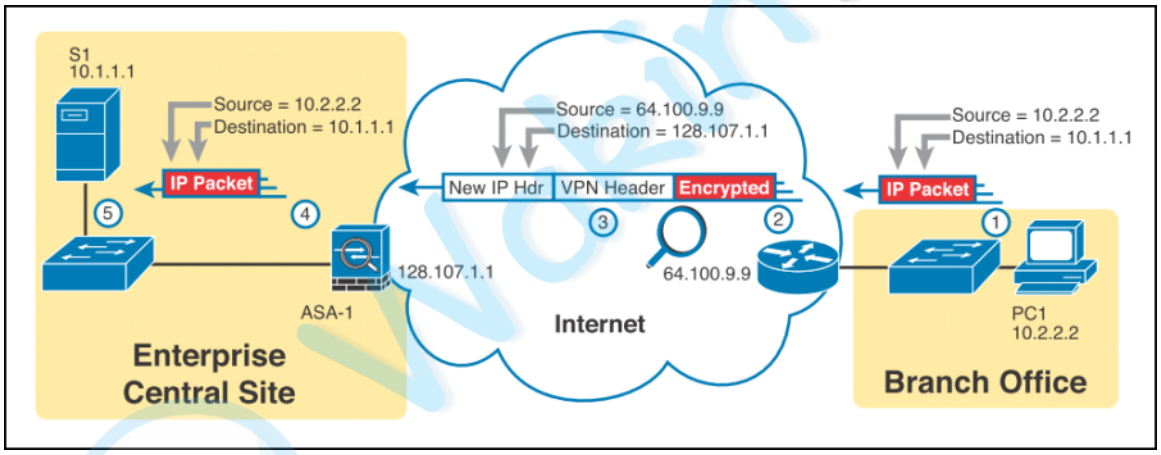
VPN核心技术：

- 

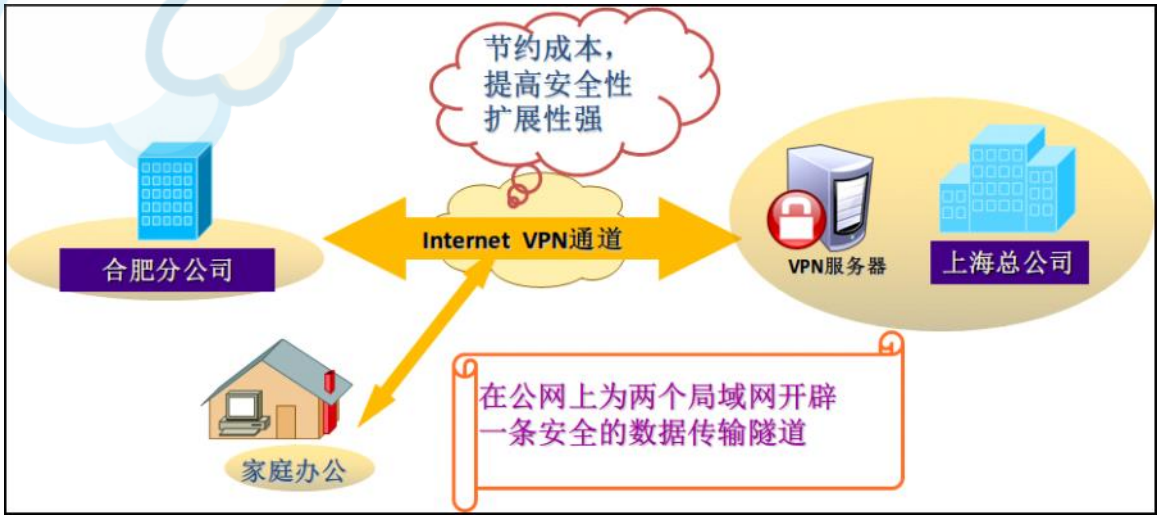
- 

- 

- 

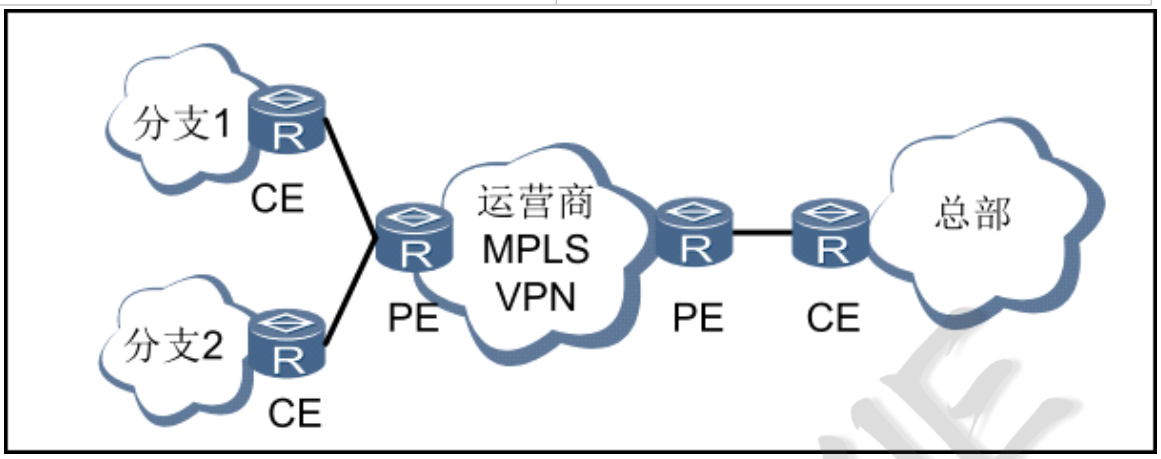
- 

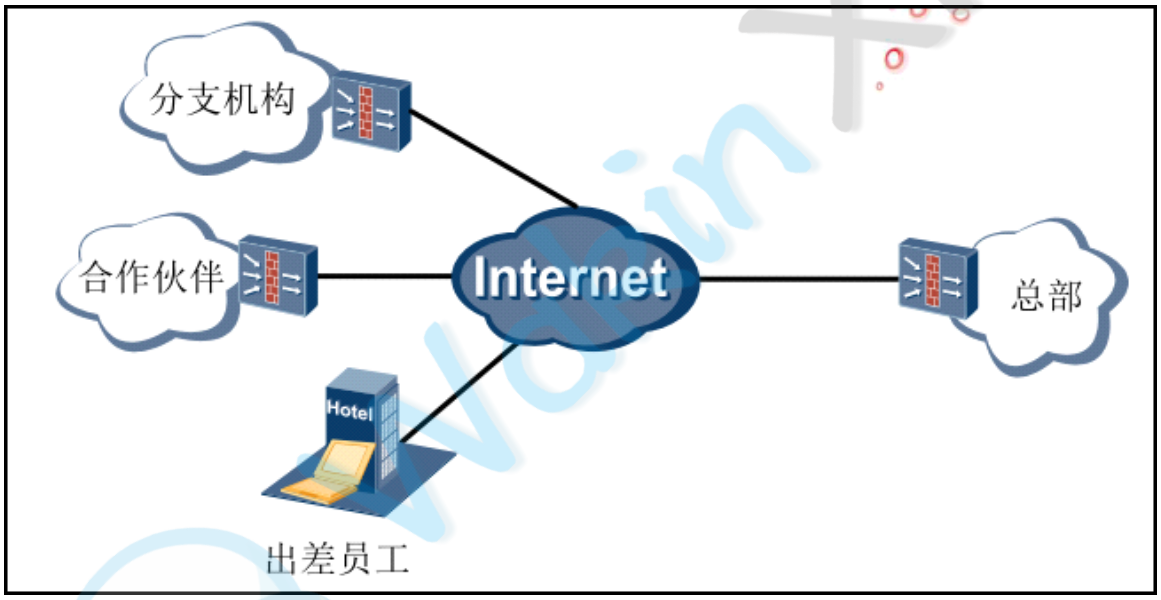
VPN优点：

- 

VPN类型（根据建设单位划分）：

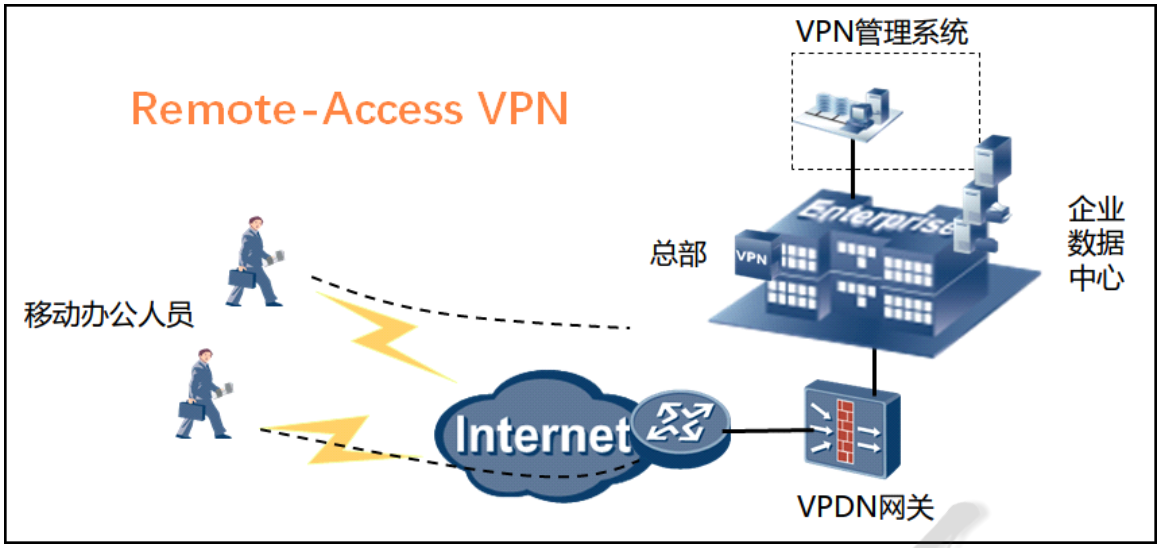
类型	备注
租用运营商专线搭建VPN网络	MPLS VPN
用户自建企业VPN网络	GRE、PPTP、L2TP、IPSec、SSL VPN

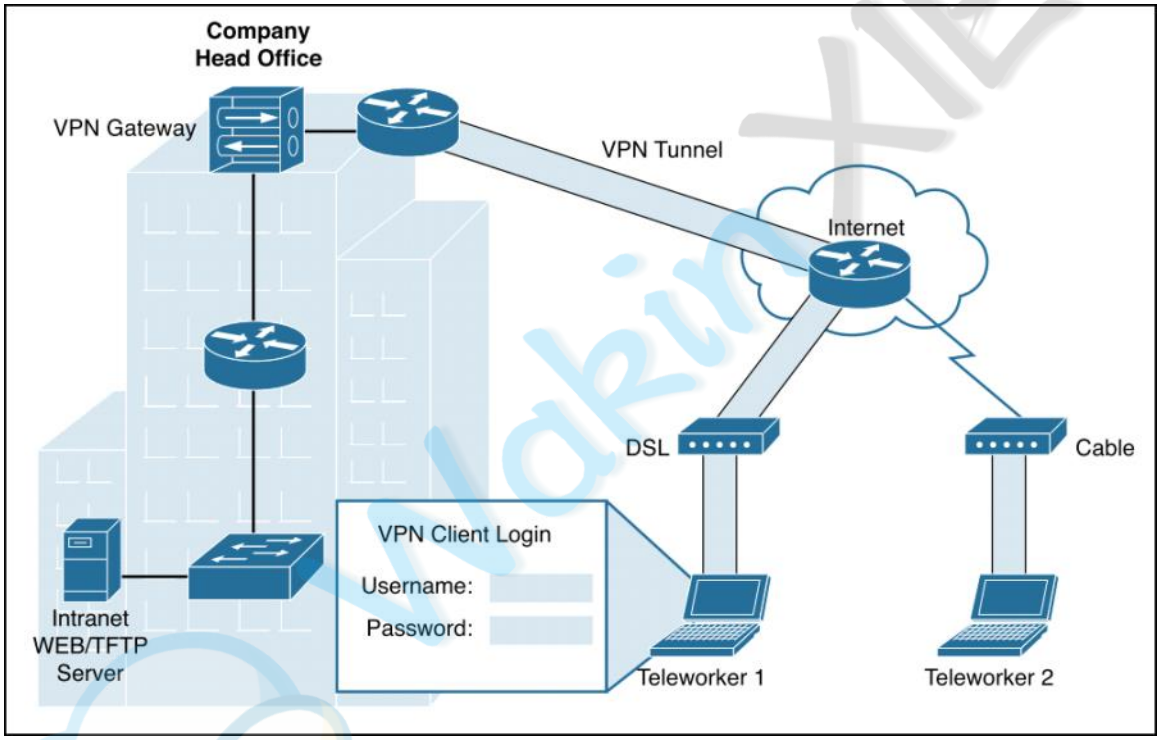


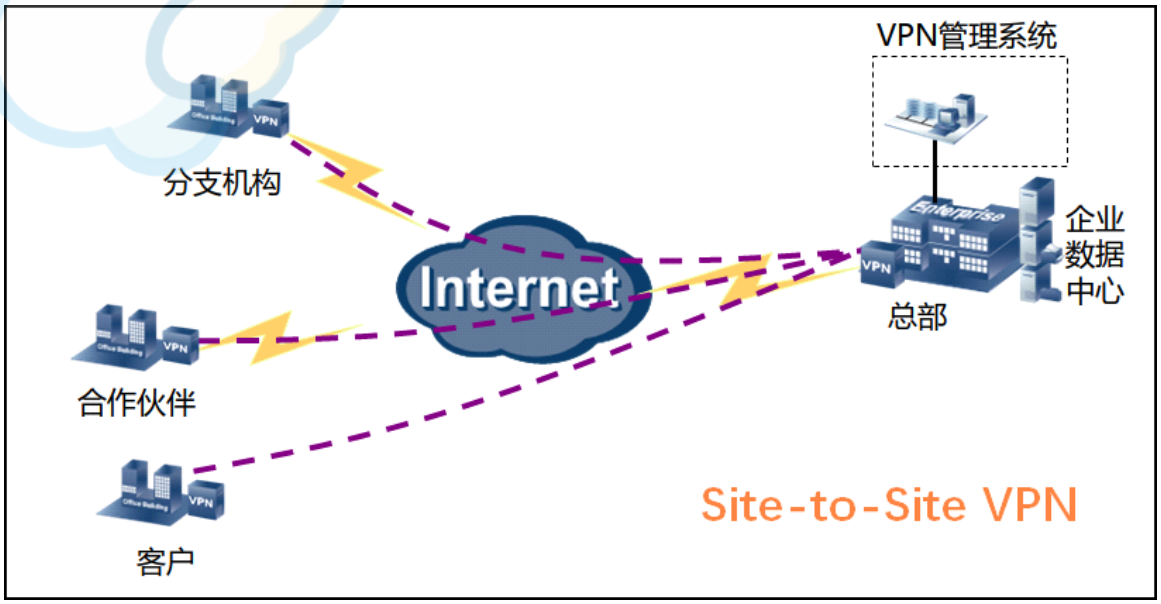


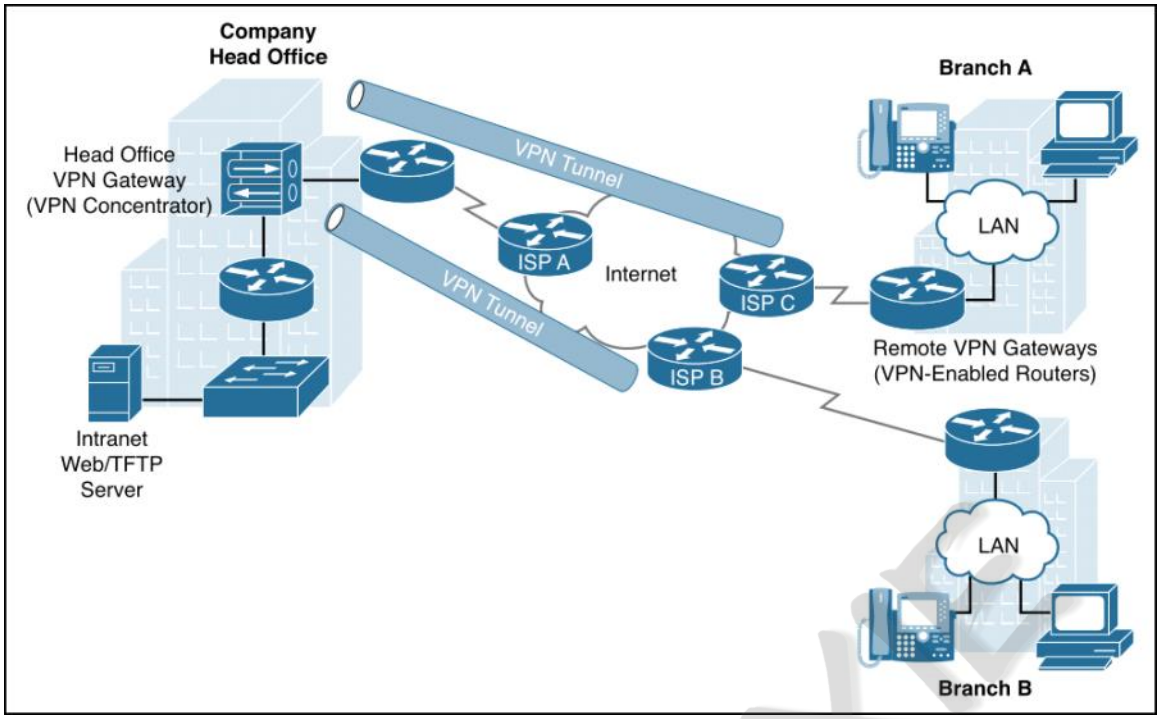
VPN类型（根据组网方式划分）：

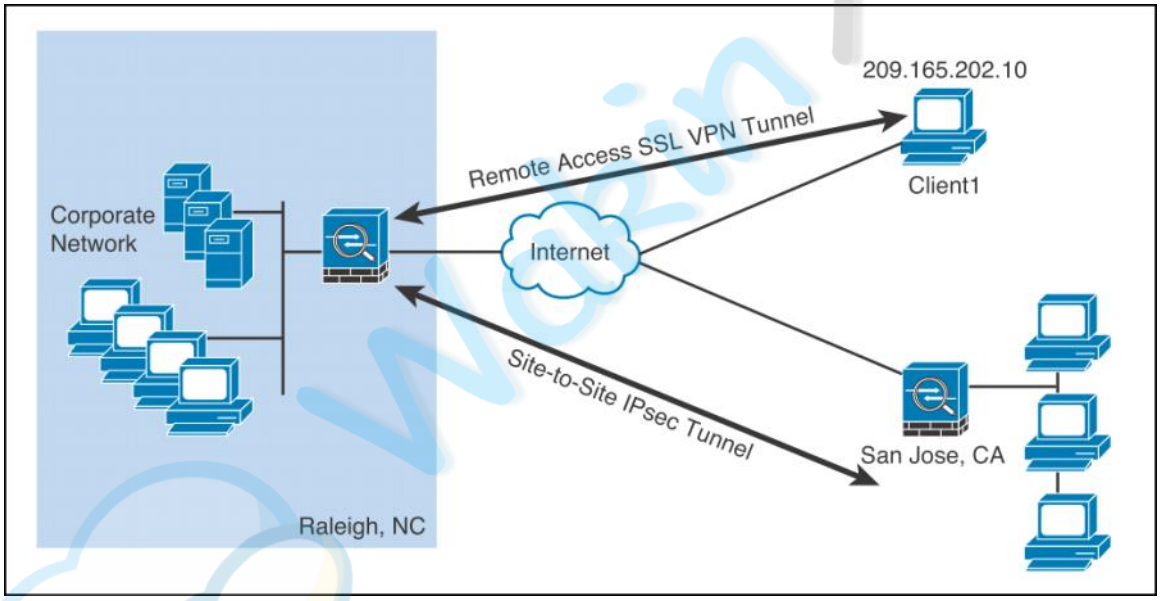
类型	备注
Remote-Access VPN **远程访问VPN**	适合出差员工，移动办公等VPN拨号接入的场景。 员工可以在任何能够接入公网的地方，通过远程拨号接入企业内网，从而访问内网资源。 通常拨号方IP地址不固定。
Site-to-Site VPN **站点到站点VPN**	适合各分支机构、合作伙伴、客户、供应商间的互联。 双方都有固定的IP地址。

- 

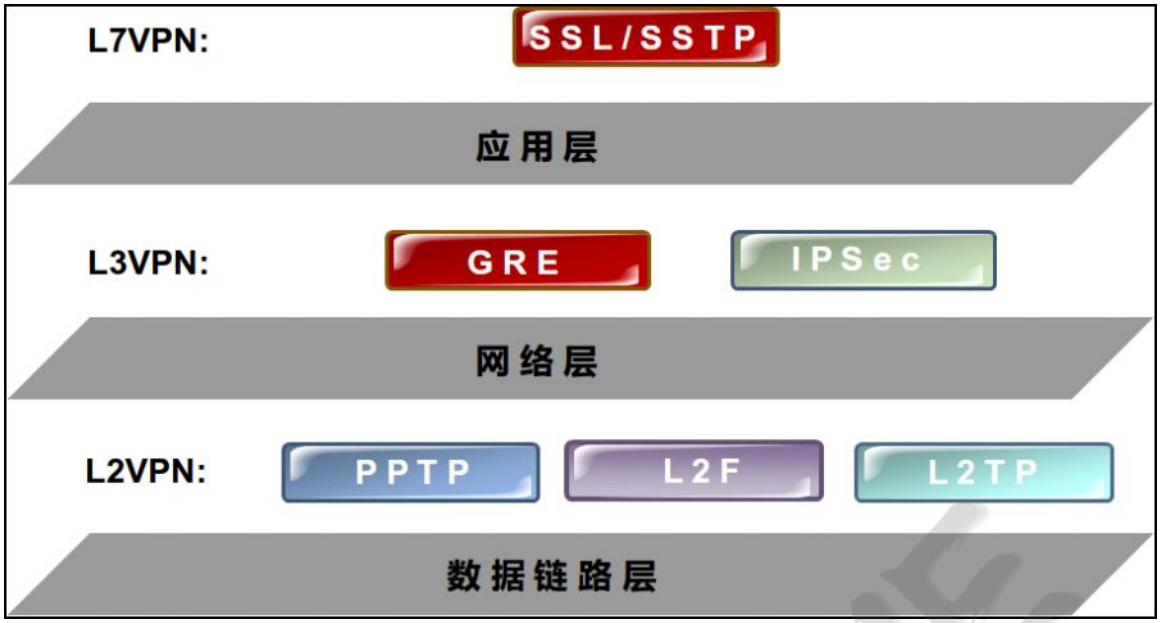
- 

- 

- 

- 

VPN类型（根据实现层、协议划分）：

- 

	GRE	L2TP	IPSec	SSL VPN
保护范围	IP层及以上数据	IP层及以上数据	IP层及以上数据	应用层特定数据
适合场景	Intranet VPN	Access VPN，Extranet VPN	Intranet VPN，Access VPN	Access VPN
身份认证	不支持	支持，基于PPP的Chap、PAP、EAP认证	支持，采用IP或ID+口令或证书进行数据源认证；IKEv2拨号方式采用EAP认证进行用户身份认证	支持，用户名+口令+证书对服务器进行认证。也可以进行双向认证
加密技术	不支持	不支持	支持	支持
数据验证	支持（校验和方式验证、关键字验证）	不支持	支持	支持
如何使用	GRE over IPSec	L2TP over IPSec	单独使用IPSec，或通过IPSec保护GRE、L2TP	SSL VPN

- L2TP端口号：UDP 1701
- PPTP端口号：TCP 1723