1.VPN技术有哪些类型，这些技术各自有些什么特点，分别适用于什么场景

1. PPTP（Point-to-Point Tunneling Protocol）：是一种基于TCP/IP协议的VPN技术。它具有易于设置和使用的优点，但安全性不如其他技术，因此适用于非敏感数据传输和低风险的场合。
2. L2TP（Layer 2 Tunneling Protocol）：是一种基于点对点协议（PPP）和IPsec协议的VPN技术。它具有较高的安全性和可靠性，但设置和使用较为复杂，因此适用于需要高安全性和可靠性的场合。
3. IPsec（Internet Protocol Security）：是一种基于IP协议的VPN技术。它具有高度的安全性和可靠性，但需要专门的设备和软件支持，因此适用于需要高安全性和可靠性的企业级应用场合。
4. SSL（Secure Socket Layer）：是一种基于浏览器的VPN技术。它具有易于设置和使用、无需专门客户端的优点，但速度较慢，因此适用于需要远程访问企业内部资源的场合。
5. TLS（Transport Layer Security）：是一种基于传输层的VPN技术，可以提供端到端的加密和认证。它具有高度的安全性和可靠性，但需要专门的设备和软件支持，因此适用于需要高安全性和可靠性的企业级应用场合。
6. OpenVPN：是一种开源的VPN技术，具有高度的安全性和可靠性，易于设置和使用，同时支持多种平台，因此适用于需要高安全性和可靠性的场合。

2.分析基于SSL/TLS的VPN，是如何实现对两端流量的正确路由的？TUN/TAP接口在当中起什么作用

在SSL/TLS VPN中，客户端通过SSL/TLS协议与VPN服务器建立安全的连接。客户端发送的数据经过SSL/TLS协议加密后传输到服务器，服务器解密后进行正确的路由，并将响应数据加密后发送回客户端。这一过程中，客户端和服务器端之间的通信是通过加密的隧道进行的，第三方无法获取数据内容。

在实现正确路由的过程中，VPN服务器需要了解VPN客户端的IP地址和路由表信息。通常，客户端连接VPN服务器后会自动获取VPN服务器分配的IP地址，同时VPN服务器会将客户端需要访问的网络路由表信息发送给客户端，使其能够正确地将数据发送到目标网络。此外，在路由过程中，VPN服务器还需要防止IP地址冲突等问题，保证数据的正确传输。

基于SSL/TLS的VPN通过在应用层实现加密和身份验证，确保了数据的安全性和可靠性，同时在路由方面，通过客户端和服务器端之间的通信协议和路由表信息的交换，实现对两端流量的正确路由。

TUN/TAP 是操作系统内核中的虚拟网络设备，由软件进行实现，向操作系统和应用程序提供与硬件网络设备完全相同的功能。其中 TAP 是以太网设备(二层设备)，操作和封装以太网数据帧，TUN 则是网络层设备(三层设备)，操作和封装网络层数据帧。当应用程序发出报文后，报文将通过操作系统协议栈处理，到达网络设备，硬件网络设备将收到的报文转化为电信号发出，而虚拟网络设备(TUN/TAP)不具备实际的物理功能，报文需要上层应用进行处理。

在基于SSL/TLS的VPN中，TUN/TAP接口通常被用作虚拟隧道的一个端点。当客户端和服务器之间建立VPN连接后，VPN客户端会创建一个虚拟的TUN/TAP接口，并将该接口的IP地址设置为VPN的虚拟IP地址。当客户端向VPN虚拟IP地址发送数据包时，该数据包将被拦截并加密，并通过SSL/TLS协议发送到服务器端。服务器端收到数据包后，会将其解密并通过TUN/TAP接口发送到目标主机。

因此，TUN/TAP接口在基于SSL/TLS的VPN中起到了非常重要的作用，它可以将流量从内核协议栈中拦截出来，并将其传递到VPN应用程序中进行处理，从而实现了对两端流量的正确路由。同时，TUN/TAP接口也可以在不同操作系统之间提供通用的接口，使得基于SSL/TLS的VPN可以在各种不同的平台上运行。