1.虚拟专用网VPN

\*定义：指通过一个公用网络（通常是因特网）建立一个临时的、安全的连接。使用的是一条穿过公用网络的安全、稳定的隧道，是对企业内部网的扩展。

\*基本功能：

1. 加密数据
2. 信息认证和身份认证

（3）提供访问控制

\*特点：

（1）费用低

（2）安全保障

（3）服务质量保证（QoS）

（4）可扩充性和灵活性

（5）可管理性

\*分类：

（1）远程访问VPN

（2）网关-网关VPN

\*主要技术依靠：

（1）隧道技术

（2）加/解密技术

（3）密钥管理技术

（4）身份认证技术

（5）访问控制

2.隧道协议（PPTP、IPsec、TLS）

\*IPsec:

（1）AH

（2）ESP

（3）IKE（密钥交换协议）

\*TLS:

（1）概述：TLS协议主要用于HTTPS协议中，也可以作为构造VPN的技术。最大优点是用户不需要安装和配置客户端软件，只需要在客户端安装一个IE浏览器即可。由于TLS协议允许使用数字签名和证书，故它能提供强大的认证功能。

（2）实现方式：在企业的防火墙后面放置一个TLS代理服务器。

（3）应用：

a.电子邮件

b.内部网页浏览

c.其他基于Web的查询工作

\*IPsec与TLS的比较：

（1）TLS VPN有很多优点（灵活高效，价格低廉），但并不能取代IPSec VPN。

（2）在为企业高级用户提供远程访问及为企业提供LAN-to-LAN隧道连接方面，IPSec具有无可比拟的优势。

（3）目前，IPSec VPN的厂商也开始研究如何让IPSec VPN兼容TLS VPN，以增强可用性。如果成功，IPSec VPN的扩展性将大大加强，生命力也将更长久。