考虑网络安全，应从网络分层模型上入手。ISO/OSI 模型中关于安全的设计是标准 7498-2，刻画了几种安全服务和机制。

实践中，有两个层更适合上安全机制，一是传输层，另一个是网络层。

传输层代表了通信子网提供给资源子网的服务和接口，代表就是 SSL/TLS，提供了基本的认证、加密和完整性保护特性，可以和各种上层应用协议结合，典型就是 HTTP+SSL=HTTPS。缺点是需要重写代码，把 send/recv 换成 ssl_send/ssl_recv。

相比之下，网络层的安全机制 VPN，更方便使用。拨号之后获得一个新的 IP 地址，通过路由规则，可以让该机器上所有应用的通信传输都使用新 IP，即 VPN 对上层应用是透明的。

VPN 的核心技术，网络和系统方面是隧道（tunnel）概念和虚拟网卡技术（tun/tap）；安全方面，可以使用共享秘密口令或公钥体系，比如直接使用 SSL 的 OpenVPN。

桥（network bridge）工作在更下一层，可以把两个 LAN 或多个 LAN 拼成一个 LAN。配合使用 OpenVPN 可以实现远程桥接的效果。

不需重写代码的安全方法，还有“外挂”方法，比如使用 SSH -R、-L 命令选项，即可充分利用已有的 SSH 安全功能。SSH 是为了代替不安全已经不用的 TELNET，同时其设计也方便被借用。

SSH 除了使用口令登录，用户应该更喜欢使用公钥登录（关注~/.ssh/*这几个文件）。SSH 的口令登录方法，虽然基于/etc/{passwd，shadow}的登录方法（参见 crypt()函数），但是显然引入了重大变化。RFC 2617 中的使用 MD5 的挑战应答方法代表了正统的使用口令的网络登录认证方法。实践中 HTTPS+FORM 的方法更多见。

上网第一步，突破 NAS 的访问控制。

NAS：Network Access Server。

注，另一种 NAS（Network Attached Storage）是一块或很多块硬盘堆一起有 IP 地址的存储设备。

NAS 把控一个内部网络，比如家庭 LAN、校园网有线/无线 LAN，在用户尝试访问互联网时，强制用户登录。NAS 主要是个执行机构，因此 NAS 需要使用 RADIUS 协议连接到一个决策机构即 AAA 服务。

如果使用 Linux 实现一个 NAS 原型是简单而直接的，可以使用 iptables、apache2 等命令行和软件。

虽然一般都是 NAS 检查用户身份，但是用户也要谨防假冒的 WiFi。

可以使用 Linux，配合使用 apache2、DNS 服务器、route、iptables 等工具和命令，实现一个假的 WiFi，等待用户主动连接（登录或不需要登录），诱骗访问一个假的百度或假的银行网站、假的游戏网站等，从而骗取用户口令等信息。

企业环境的网络安全，首先得部署便于落实安全机制的网络结构。常见做法之一是使用两层路由器（亦可理解为防火墙）把网络隔离为不同的部分（屏蔽子网），部署不同的服务。Web、邮件、代理等服务通常放在中间（就是所谓的非军事区 DMZ），并被不同的安全规则保护，比如邮件服务器可以主动连接外网，而其他服务器默认不行等。核心业务逻辑以及数据库放在最里面的子网中，通常这里仅限和 Web 服务器等通信，并不能直接和外网通信，因此最安全。

代理服务器是落实网络安全策略，实现安全目标的重要机制。代理服务器除了具有 NAS 的访问控制能力，可以查病毒（sqiud 可以配合 calamav），也可以审查密文流量（比如 squid 通过 sslbump 和 icap）。既然有了 icap，就可以对上传流量进行防泄漏检查，这样不管是入侵成功正在偷文件数据的黑客，还是有意无意作恶的员工，只要有敏感数据外传，都可以被察觉。