9.11——9.13工作内容：

1. 安装并学习使用H3C的防火墙，配置其相关功能。

2. 用两台电脑模拟内外网，在内网中搭建Web服务器，在外网中使用SSL VPN Web登入访问。

3. 使用Wireshark在两台电脑上进行抓包。

目前获得的情报：

1. 当采用Web接入方式时，管理员可以通过三种方式配置Web资源：常规改写、端口映射和域名映射。

采用常规改写方式时，倘若Web资源的真实域名是a.com，SSL VPN Server将为其添加固定的前缀（比如https://sslvpn/proxy/）。这样在用户视角看来，会认为自己访问的URL是域名为https://sslvpn/proxy/a.com，即SSL VPN Sever上的一个站点，以此来实现Web反向代理。

采用端口映射方式时，会将内网Web资源的IP + 端口号映射为SSL VPN网关的IP + 端口号（管理员指定）。如真实的Web资源[192.168.90.2:8080](http://192.168.90.2:8080)被映射为192.168.90.1:4000（192.168.90.1是SSL VPN中的某个网关）。这样，在用户视角看来，自己访问的是SSL VPN Server某个网关上的端口、而非内网Web资源，以此来实现反向代理。

域名映射的相关功能可能需要DNS服务器的相关支持，目前还未搞清楚其具体功能。

2. H3C的SSL VPN配置灵活性较高，可以配置服务器的SSL/TLS可选加密算法，但即使设置为NONE，仍会在会话时进行加密。

3. 通过抓取外网访问内网Web资源的过程中、两台电脑上的数据包，可以看到从SSL VPN网关 🡪 内网，存在正常的http请求和应答报文；而从外网 🡪 SSL VPN网关，只能看到一堆TCP包，通过解码为SSL可以看到client hello、server hello之类的握手过程和加密的Application data，但还是看不到http请求。需要对加密的Application data进行解密。后才能看到。

9.14——9.15工作计划：

1. 查找资料并进行实际操作，探究域名映射功能的正确用法和原理。

2. 寻找解密SSL数据的方法，以期在外网 🡪 SSL VPN网关的抓包结果中看到http请求。