1. 新用户的注册：

   说明：这个问题单独列出来是因为新用户的增加影响着第一层 VPN 服务的增加和扩展。

   当一个新用户完成注册后，服务器随即创建一个以用户名命名的 VPN 服务，并且立即生成一定数量的 VPN 证书文件备用。

2. 盒子端和客户端的登录（上线）：

   说明：每个盒子有唯一识别标识（ID），同时对应一个密码（PWD）。

   客户端和盒子端连接到广域网之后，向指定的服务器（域名）发送 HTTP 请求，分别通过用户名/密码和唯一识别标识（ID）/密码（PWD）来与服务器建立连接，即完成登录（上线）。

   补充：当客户端完成登录后，即可自动向服务器请求 VPN1 服务的证书文件，服务器将相应的 ovpn 文件传输给客户端；当多个客户端使用同一个账号登录时，以相同的方式自动向服务器请求 VPN1 服务的证书文件，这里发放的证书文件不能冲突，需要对证书文件使用情况进行管理。

3. 用户账号与盒子的绑定：

   说明：一个用户账号可以同时与多个盒子绑定，每个盒子只能被一个用户账号绑定；在进行绑定操作时，盒子必须是在线状态。

   绑定操作由已经成功登录的客户端发起，客户端通过录入 X-Box 的 ID 和 SVT 请求绑定该盒子，盒子完成首次登录后服务器就会记录盒子 ID 和 SVT 信息，当用户请求绑定时，服务器就会进行查询比对，如果信息符合，就可完成绑定操作；当盒子已经被一个用户绑定成功并且暂未被该用户解绑之前，其他用户无法对其进行绑定。

   补充：当盒子和用户的账号绑定完成后，服务器立即根据用户对应的 VPN1 服务将相应的 ovpn 文件传输给盒子端。

4. 建立指定的 VPN2 服务（传输建立 VPN2 所需要的文件）：

   说明：在用户账号和盒子端绑定完成之后，VPN1 服务已经启动，并且此时客户端和盒子端已经在同一局域网下，这时服务器需要告知（客户端请求）客户端，其欲连接的盒子的 VPN1 的地址。

   VPN2 的建立的操作也是由客户端发起，客户端首先设置 VPN2 虚拟局

域网的网段，然后通过向服务器请求相应的 VPN2 证书文件。这里 VPN2 的证书是在盒子端预先生成，然后等用户账号与盒子完成绑定之后就将 VPN2 的客户端证书文件存储到服务器的指定路径下。这样当客户端请求 VPN2 网络透传时，就可以直接从服务器拿到 VPN2 客户端证书文件。

5. 客户端对盒子的简单设置和控制：

   说明：目前主要考虑的对盒子端 VPN2 服务的参数的设置。

   为了实现这个目标，需要在盒子端启动一个 TCP Server 进程来等待客户端的 TCP 连接。这里的 TCP 连接是通过 VPN1 构建的虚拟局域网来完成的。

   补充：这里对盒子的 VPN2 参数的设置主要目的是修改 VPN2 服务启动的虚拟局域网的网段，使其能够与盒子后面连接的设备处在同一个 IP 地址段内，进而保证客户端可以通过 VPN2 构建的网络直接访问到这些设备。

6. 对服务器的后台管理（后台管理系统）：

   说明：主要目的是方便管理员（我们自己）对用户的一些误操作或者其他意外情况导致的故障进行越权处理；同时也可以方便我们自己对系统整体的运行情况进行监控和维护。

   暂无具体实施方案。