基于SSL协议的VPN方案和产品可以分为两类：

一类是代理型SSL VPN。这一类VPN通过代理技术来增强SSL协议记录层的隧道功能。这类VPN的特点是基于代理技术实现和“无客户端”的运行模式，即其运行只需要WEB浏览器即可，无需专门安装客户端。但这类VPN所支持的应用通常有限，这与采用的代理技术和厂商的实现有关。代理型SSL VPN通过不同的代理技术来支持不同的应用。

另一类是隧道型SSL VPN，这类VPN基于虚拟网卡技术实现，其运行需要通信双方安装VPN软件，通过虚拟网卡建立的隧道进行安全数据传输。这类VPN可以支持物理网络中的所有网络应用。这种VPN的典型代表是OpenVPN。

所谓的代理型SSL VPN，是一种基于HTTPS和代理技术实现的VPN。其突出特点是实现了应用级访问控制，且用户只需通过WEB浏览器就可实现对VPN内部资源的安全访问，而无需安装客户端和进行配置。代理型SSL VPN的核心功能是代理和转发外部网络终端用户的访问请求，使之能够进入内部网络。同时，代理型SSL VPN对应用的访问控制功能也是建立在代理技术基础之上的。

基本的代理型SSL VPN访问过程如下：

1. 用户在支持HTTPS协议的浏览器中输入VPN服务器的URL。
2. 浏览器与VPN服务器完成SSL握手，建立SSL安全通道。
3. VPN服务器会给客户端浏览器返回一个网页，要求用户输入用户名称和密码。
4. VPN服务器认证通过用户名/密码之后，从访问控制策略中取得该用户有权限访问的内部应用资源列表，并发送到客户端浏览器。
5. 用户从资源列表中选择要访问的资源。
6. VPN服务器接受用户的访问请求，并转发给相应的内部应用服务器。
7. 内部应用服务器将访问结果返回给VPN服务器。
8. VPN服务器将访问结果转发给用户端浏览器。

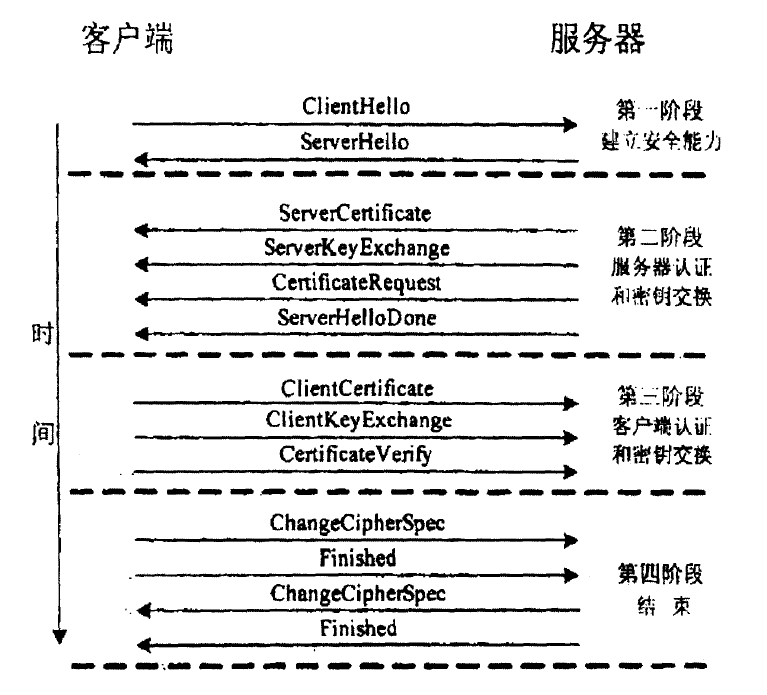
（1）-（2）为SSL安全通道建立过程，（3）-（4）为身份认证过程，（5）-（8）为web代理/转发过程。

### 1. SSL安全通道的建立

安全通道的建立依赖于SSL中的握手协议，握手协议主要内容是协商客户端与服务器之间建立会话所依赖的一些参数、相互认证以及在双方之间生成共享秘钥。

握手过程描述如下：

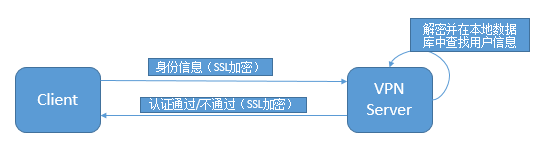
1. 客户端将它所支持的算法列表连同一个随机数（该随机数在之后的秘钥的产生过程中作为输入使用）。
2. 服务器根据列表的内容从中选择一种加密算法，并将其连同一份包含服务器公用秘钥的证书发回给客户端。该证书还包含了用于认证目的的服务器标志，服务器同时还提供了一个作为秘钥产生过程部分输入的随机数。
3. 客户端对服务器的证书进行验证，并抽取服务器的公用秘钥。然后再产生一个称为pre-master\_secret的随机密码串，并使用服务器的公共秘钥对其进行加密。最后，客户端将加密后的信息发送给服务器。
4. 客户端与服务器根据pre-master\_secret以及客户端与服务器的随机数独立计算出主密钥和MAC秘钥。
5. 客户端将所有握手消息的MAC值发送给服务器。
6. 服务器将所有握手消息的MAC值发送给客户端。

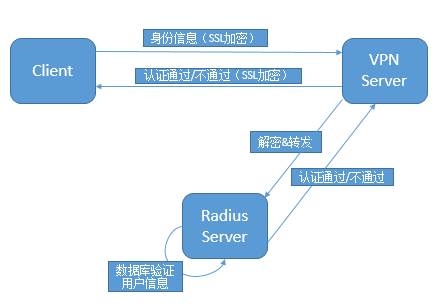


之后，客户端与服务器的通信将使用第（4）步中得到的主密钥（对称密钥）对两者之间的通信数据进行加密。至此，客户端与VPN Server之间便建立起了一条安全的通信通道，后续的数据交换都是基于这条安全通道进行的。

### 2. 身份认证

RG-6120-E支持本地认证（VPN Server直接验证用户发送过来的身份信息）和RADIUS认证（VPN Server将用户传来的用户名和密码解密后转发给RADIUS服务器，由RADIUS服务器对其进行认证）。





该方面技术已经很成熟，且更偏顶层、数据包转发流程比较常规

Web业务：即Web接入方式。在该业务下需要以URL表项和列表的形式创建Web接入资源。缺省情况下SSL VPN网关会对URL进行常规改写。常规改写可能会造成URL改写遗漏和改写错误等问题，从而导致SSL VPN客户端不能访问内网资源。因此可以通过配置域名映射或端口映射的方式尽可能的解决此问题。

以SSL VPN网关名gw（域名为https://www.gateway.com:4430，对应的IP地址为1.1.1.1），内网资源服务器URL=http://www.server.com:8080为例：

¡ 当不配置URL映射方式时（默认为常规改写），客户端访问内网资源服务器的URL显示为：https://www.gateway.com:4430/\_proxy2/http/8080/www.server.com

¡ 当配置域名映射，映射的域名为www.domain.com时，www.domain.com与内网资源http://www.server.com:8080为一一映射关系。客户端访问内网资源服务器的URL显示为：https://www.domain.com:4430

¡ 当配置端口映射，又分为配置虚拟主机名和不配置虚拟主机名两种情况：

- 不配置虚拟主机名，引用SSL VPN网关gw2时，客户端访问内网资源服务器的URL显示为：https://2.2.2.2:4430（网关gw2的IP地址为2.2.2.2，端口号是4430）

- 配置虚拟主机名，虚拟主机名为vhosta，vhosta与内网资源http://www.server.com:8080为一一映射关系。引用SSL VPN网关gw时，客户端访问内网资源服务器的URL显示为：https://vhosta:4430

当内网资源为HTTPS服务器时，需要为Web业务指定SSL客户端策略，以便SSL VPN网关使用指定的SSL客户端策略与HTTPS服务器建立连接。如果没有指定SSL客户端策略，则SSL VPN网关使用缺省的SSL客户端策略，该策略支持的加密套件为rsa\_rc4\_128\_md5

<http://www.h3c.com/cn/d_201008/686807_97665_0.htm>

由于SSL是封装在TCP上的，穿越NAT不是问题，所以在示例中客户端使用公网地址进行介绍：

1.   假设SSL VPN的WEB站点的互联网域名是https://sslvpn，该WEB站点对应的主机则是SSL VPN服务器；

2.   使用者登陆SSL VPN的WEB页面后，WEB代理一栏会有许多链接，如内部财务报表、订单提交等内部网站；

3.   假设“订单提交”网站在单位内部私有URL是http://site1/page，那么在SSL VPN服务器上的订单提交链接URL则会进行相应的修改，变成https://sslvpn/httpsite1/pate，相当于SSL VPN站点的内部链接；

4.   使用者点击“订单提交”链接后，会新建一个浏览器窗口，打开链接https://sslvpn/httpsite1/page，也就是说对于使用者而言，订单提交像是SSL VPN站点的一个链接，而非另外一个站点，所有的访问都终结在SSL VPN站点；

5.   SSL VPN站点的所有者SSL VPN服务器在接收到使用者对https://sslvpn/httpsite1/page的页面请求后，SSL VPN服务器会做WEB代理的工作，即以内部地址10.1.1.1向真正的“订单提交”站点10.6.16.3访问页面http://site1/page；

6.   可以发现整个页面访问是由使用者与服务器之间的HTTPS会话、服务器与“订单提交”站点的HTTP会话连接而成的，服务器在这个访问中起的是WEB代理作用，因为在“订单提交”站点看来，访问者IP是服务器，而不是最终用户IP；

7.   而使用者访问另外一个站点“财务报表”，也是类似过程。

WEB代理因为原理简单，实现起来较为容易，因为传统的WEB Proxy代理是两段HTTP会话的衔接，而SSL VPN的WEB代理则把用户与服务器的连接把HTTP换成了HTTPS、并对网站的URL进行了替换而已，从图中我们可以看到红色部分即为URL的替换。