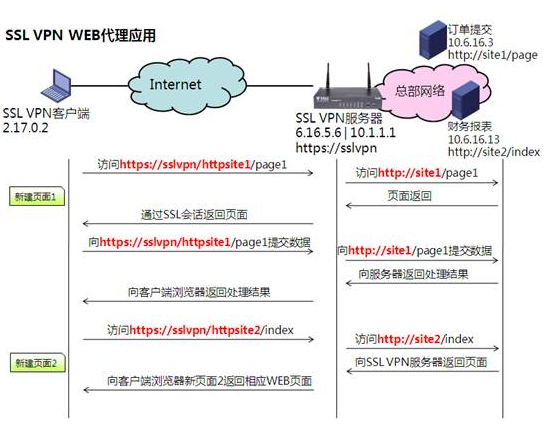
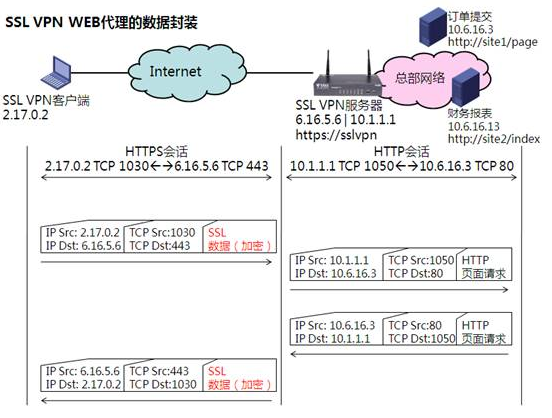
当前获得的情报：

1. 锐捷NBR-6120E经咨询客服，确认该机型已经删去了Web接入访问资源的功能。如果不开启客户端、而是直接使用Web登录，即使管理员给用户分配了相关资源，也无法看到或点击。要想访问资源，只能通过客户端登陆后使用隧道方式进行访问。从其配置了虚拟网卡和抓包结果分析，其实现思路应当与OpenVPN一致。

2. Web代理的大致原理推测





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。

3. 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；

4. 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。

当模拟外网的电脑点击相应的url时，从模拟内网的电脑上抓取到了源IP为内网网关、目的IP为Web服务器地址的http请求（明文）；从模拟外网的电脑上抓取到的数据包全为外网主机与外网网关的通信。因此其内部实现确实是代理方式而非隧道方式。

5. 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192.168.137.100:8080被映射为192.168.137.1:4000（192.168.137.1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。

将同样的url设置端口映射方式、映射端口为192.168.137.1:4000，当外网访问内网url时，于外网主机抓取到的相关报文均是外网主机与192.168.137.1:4000之间的通信，而在内网主机上却未侦听到由192.168.137.1:4000与192.168.137.100（Web资源所在）的通信，只能侦听到192.168.137.100与网关上的另一端口：36370的通信。因此推断其流程应当为：

1. 外网主机向映射端口（192.168.90.1:4000）发送http请求

2. 映射端口将http请求转发到Web服务器所在子网的网关

3. Web服务器所在的子网网关将该http请求转发到Web服务器（代理方式）

4. Web服务器收到网关发起的http请求。之后响应，目的地址为网关地址。

6. 由于在Web接入和访问资源的过程中都没有出现虚拟网卡或类似的概念，且OpenVPN相关资料中也提到无法使用浏览器等非客户端的方式配置OpenVPN，初步推断Web代理功能的实现应该与OpenVPN没有太大关联。

遇到的问题：

1. 外网主机与外网网关之间的通信过程由于SSL加密，看不到具体的通信内容（指http请求与应答），且尝试网上方法：设置环境变量存储SSL预主密钥用来给wireshark解密没有效果。

2. 当url资源设置为域名映射时（比如将内网url：<http://192.168.137.100:8080>映射为a.com），外网主机点击内网url后，将先向自己的DNS服务器请求解析a.com，不是很清楚这样有什么意义。