SSL VPN Web反向代理调研结果

1. 样机功能介绍

1.1. 锐捷样机功能介绍

锐捷样机的SSL VPN只能配置隧道资源，所有对内网资源的访问以隧道的方式进行。

经咨询锐捷客服，锐捷样机的SSL VPN功能并不支持通过Web直接登录、访问管理员授权的资源。倘若只使用Web登录，将看不到任何资源；必须使用客户端拨号登录、建立隧道后再打开网页，才能看到相关资源。在这种情况下，所有访问内网资源的请求都被封装入隧道，分别通过虚拟网卡和实际网卡两次进出协议栈进行传送。

1.2. H3C样机功能介绍

H3C样机的SSL VPN功能支持配置三种资源：Web资源、TCP资源和IP资源，分别对应Web接入方式、TCP接入方式和IP接入方式。其中，Web接入不需要客户端的参与，只需网页登陆即可访问授权的Web资源；TCP资源和IP资源则需要使用客户端拨号后才能访问。

H3C样机的SSL VPN功能以“访问实例”的形式存在。一个访问实例对应一个WAN口IP+端口，作为外网用户登录SSL VPN的入口。其基本配置如下图所示。



图1.1 SSL VPN访问实例配置

SSL VPN Web资源以“表项”和“列表”形式组织，单个URL资源对应一个表项，多个表项组成一个列表。



图1.2 SSL VPN Web资源配置界面

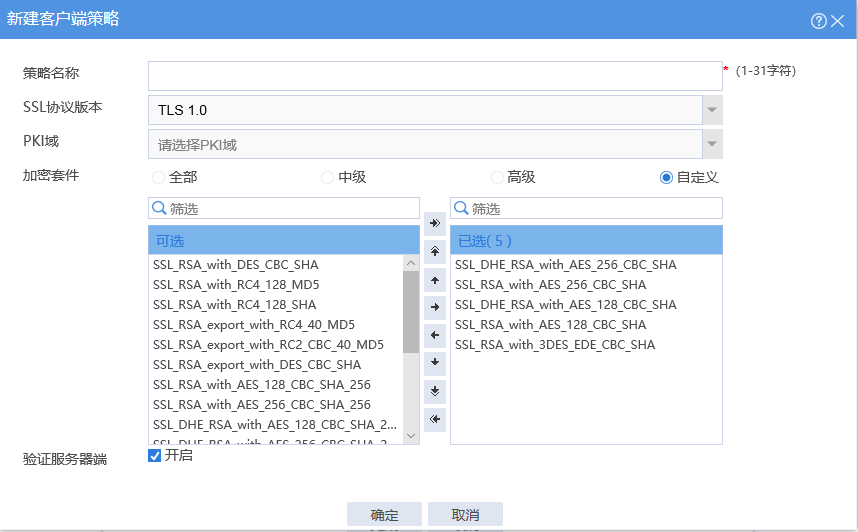


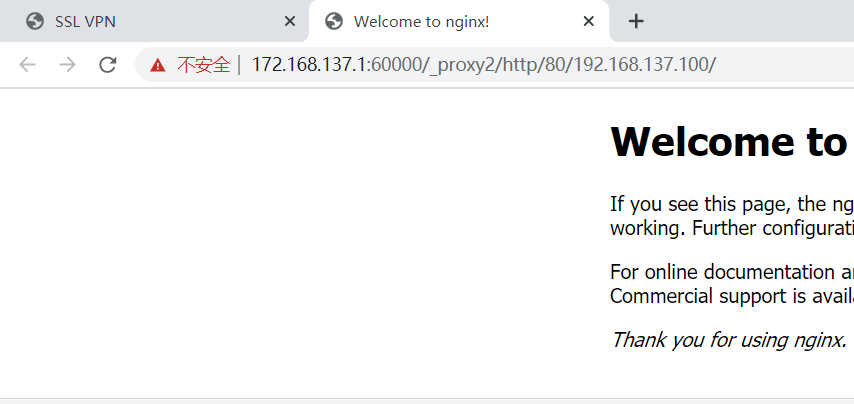
图1.3 SSL VPN客户端策略配置

H3C的Web资源配置支持三种模式，分别是：常规改写、域名映射和端口映射。

图1.4 SSL VPN URL表项配置



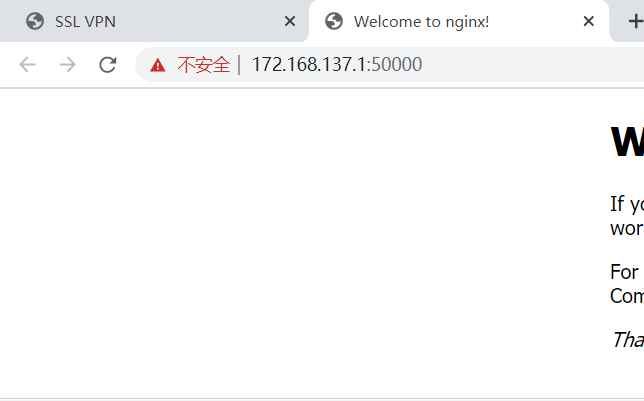
采用常规改写方式时，倘若Web资源的真实域名是a.com，SSL VPN Server将为其添加固定的前缀（比如 https://sslvpn/proxy/ ），并对URL做修改。这样在用户视角看来，会认为自己访问的URL是SSL VPN Sever上的一个站点，以此来实现Web反向代理。



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192.168.137.100:8080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。



图1.5 SSL VPN Web资源端口映射配置



采用域名映射方式时，需要相关DNS服务器的支持。用户按照映射后的域名访问内网资源时，首先会进行DNS查询，之后根据查询到的IP访问资源。

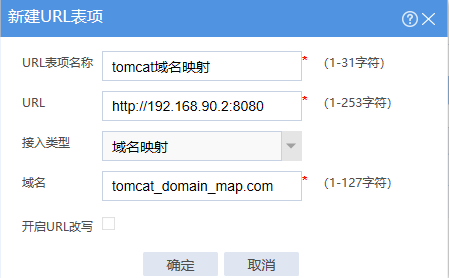
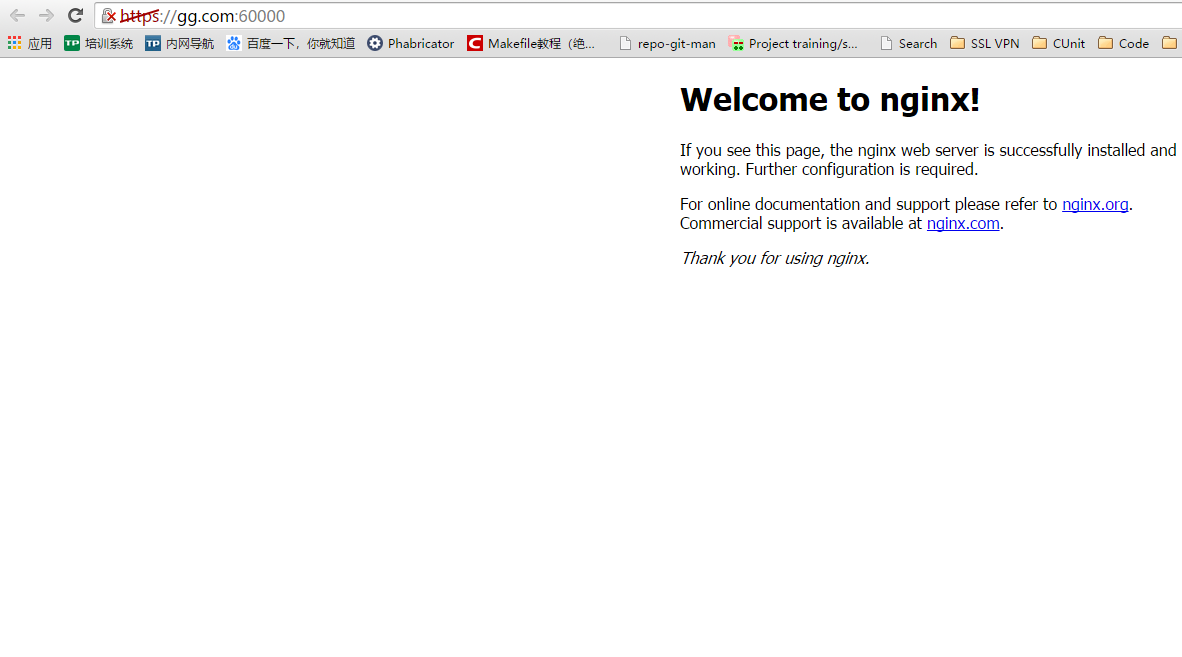
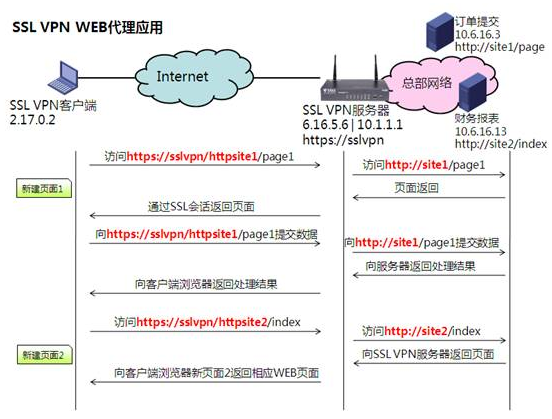
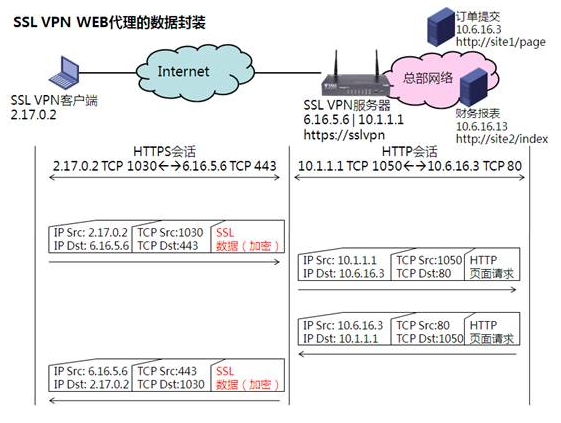


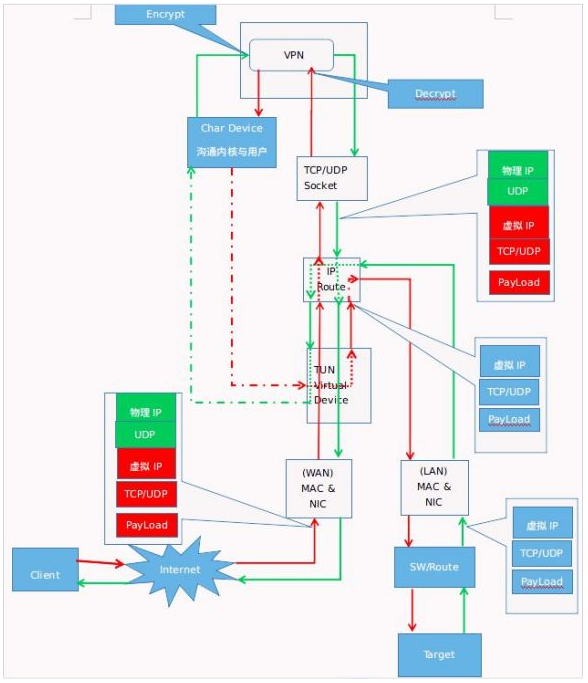
图1.6 SSL VPN Web资源域名映射配置



2. 实现原理分析





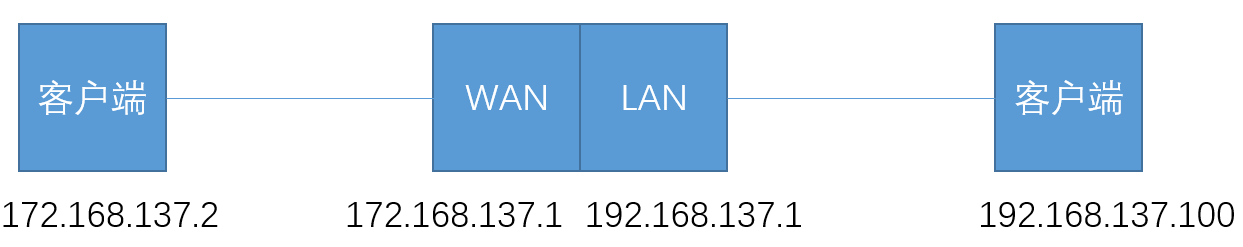


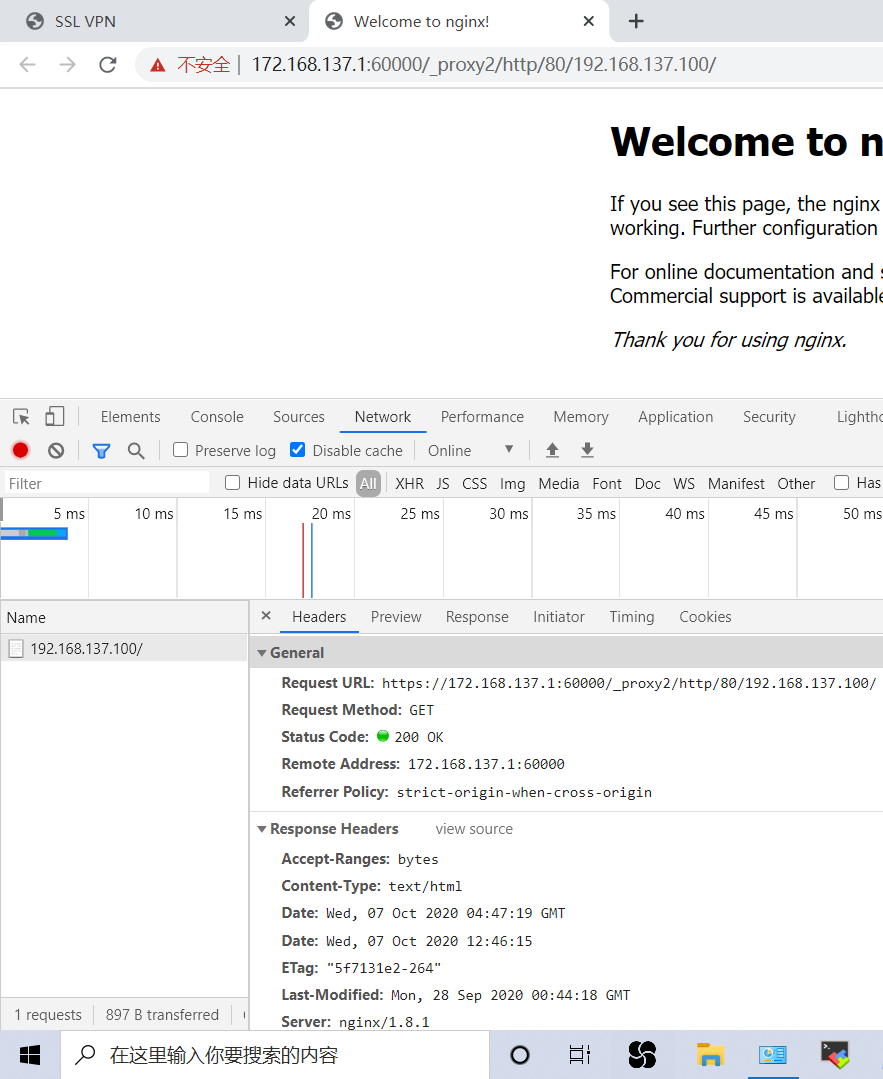
现象：

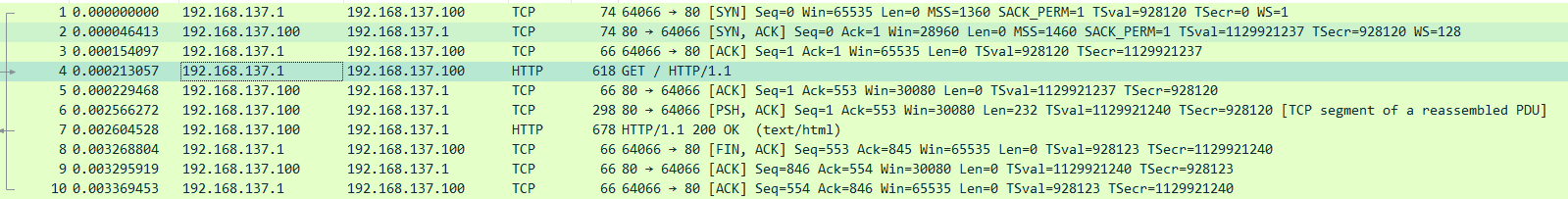
1.H3C使用Web接入方式访问Web资源时路由表无变化，也没有安装虚拟网卡。

2. Open VPN不支持用浏览器作为客户端

3. 在Chrome的开发者模式中看到了客户机向SSL VPN Server外网网关发送的https请求；在内网Web服务器端抓包，看到了SSL VPN Server内网网关向内网Web服务器发出的http请求。







结论：

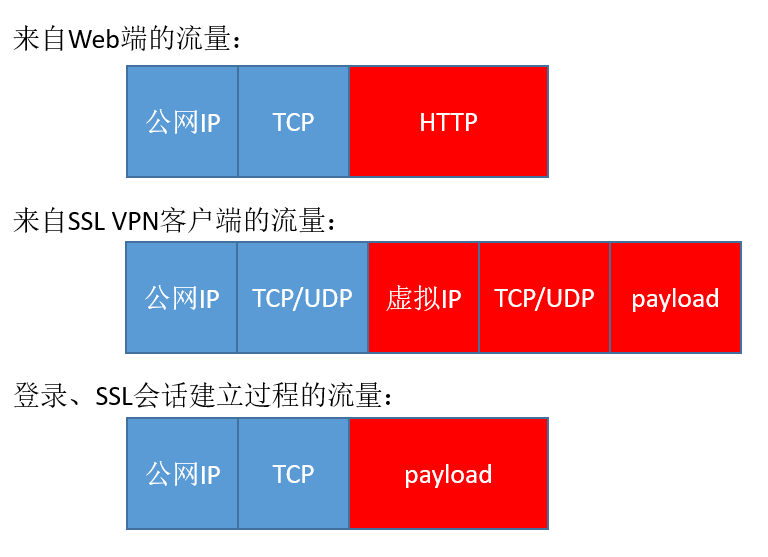
1. 网页接入SSL VPN访问Web资源是通过Web代理的方式实现的，而不是类似Open VPN的隧道方式。

现象：

1. Web资源访问（代理方式）和IP资源访问（隧道方式）均与同一个端口进行通信（即配置好的外网网关：172.168.137.1：60000）。

推测：

1. SSL VPN Server上监控外网网关的程序应当可以判断出来的流量是从客户端用户而来，还是由网页用户而来。



Nginx反向代理配置：

