基于IpSec和SSL的VPN网络简单设置

适用范围：

1、由于每家VPN网管的设置参数和设置方法均有所区别，本文档基于深信服的VPN硬件基础上而写，不一定适用于其他厂家的VPN设备。

2、 本文档主要提供在VPN网络中适用TwinCAT进行远程操作时，无法添加目标控制器时对VPN设置的重点参数设置，如果需要更详细的VPN设置，请查阅深信服的官网中的帮助文档。

IPSec网络原理：

IPSec 主要实现跨局域网的网络互连问题，适用于企业之间在不同地域时的局域网内计算机之间的互连和通信，条件是两端需要专门的 VNP 设备；如果远程为个人用户时也可以使用厂家提供的客户端工具（深信服 DLAN 工具）。具体原理如下：

具体通讯方式为：

其通信过程为：若有两个使用 PPTP（Point-to-Point Tunneling Protocol）的 RAS（Remote Access Service）服务器连接的 IP 网络，一个局域网的网络地址是 10.1.1，另一个是 10.1.2。每个网络上的 RAS 服务器都提供到 Internet 的连接。一个 RAS 服务器有一个局域网的 IP 地址 10.1.1.1 和一个 ISP 分配的因特网地址 250.121.13.12，而另一个 RAS 服务器的局域网地址是 10.1.2.1，ISP 分配的因特网地址是 110.121.112.34。这时若 10.1.1 网络中的一个计算机，假设为 10.1.1.23，需向 10.1.2 网络中的一个计算机，假设为 10.1.2.99，发送一个 IP 包。

1) 发送方的计算机首先注意到，目标地址 10.1.2.99 的网络部分与它自己的网络地址不匹配。

2) 发送方不将包直接发送给目标地址，而是将包发送给自己子网缺省的网关地址

10.1.1.1。

3) 这个 10.1.1 网络上的 RAS 服务器读这个包。

4) 网络 10.1.1 上的 RAS 服务器判断出这个包应被放到 10.1.2 网络的子网上。

5) RAS 服务器加密这个包，并用另一个包将它封装起来。

6)路由器从它的网络接口上发送这个封装的包（这个接口连接到因特网上，假设地址为 24.121.13.12）到 10.1.2 网络子网的 RAS 服务器的因特网地址 110.121.112.34 上。

7)10.1.2 网络子网的 RAS 服务器从它的因特网接口读这个封装和加密的包。

8)10.1.2 网络子网的 RAS 服务器解密这个封装的 IP 包，验证它是一个有效的 IP 包，也就是它没有被改动过并且来自可靠的地方。

9)10.1.2 网络子网的 RAS 服务器从它的适配器上将这个包发送到网络子网的目标地址 10.1.2.99。

10)目标计算机读这个包。

IPSec网络设置：

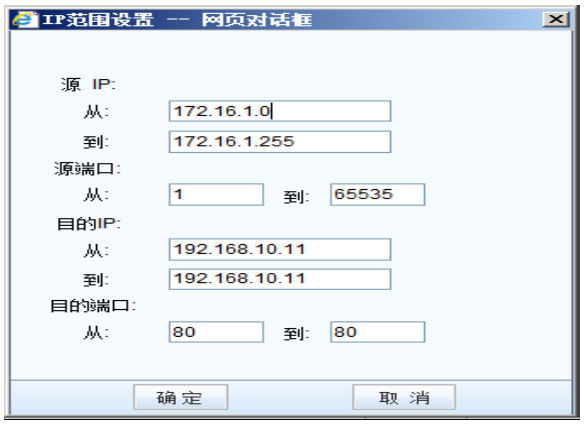
1、打开IE浏览器，输入(举例：http://10.254.254.254:1000)，即可到登录界面，输入设备出厂默认的账号密码Admin/Admin，界面如下：

2、登陆账户后会出现如下界面，其中左边列表中为当前 VNP 硬件的系统设置、IpSec、SSL、防火墙等设置的引导功能。需要在用户管理中添加 IPSec 和 SSL 客户端登陆的用户管理

信息，包括用户名、密码、和相应权限等。

3、下图为设置 VPN 网络需要实现的服务，如 TCP、UDP 和 ICMP 等，其中要保证 ADS 通讯的化，最好是启动所有服务。

服务所对应的的网络 IP 和端口的设置界面。

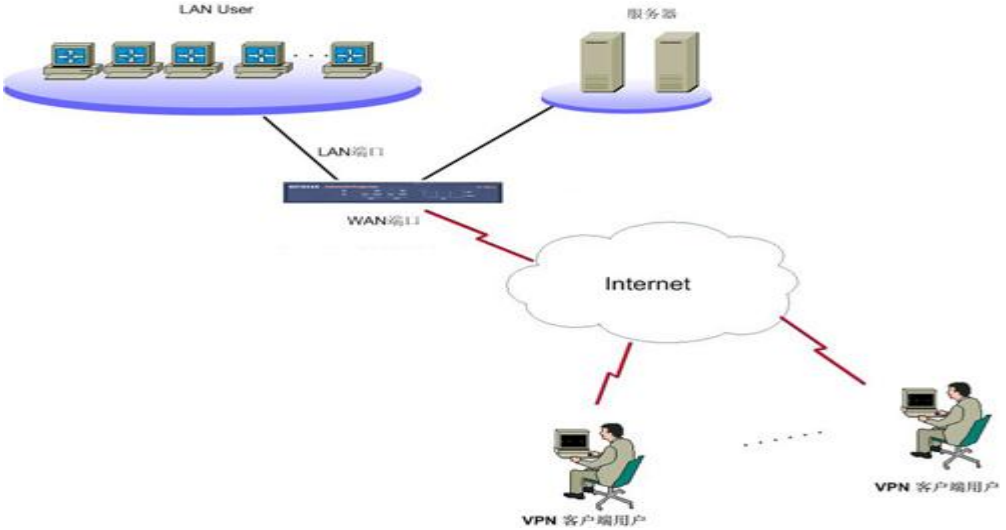


4、下面这张图片中的设置是保证 TwinCAT 添加路由的前提，要选择启用虚拟 IP 功能。虚拟 IP 需要为自动获取，也就是 0.0.0.0。

设置完成。

SSL网络原理:

SSL网络原理在VPN服务器端与IPSec网络相同，需要专门的硬件设置，但在客户端不需要专业的硬件设备，仅需要通过IP浏览器即可连接远程服务器。

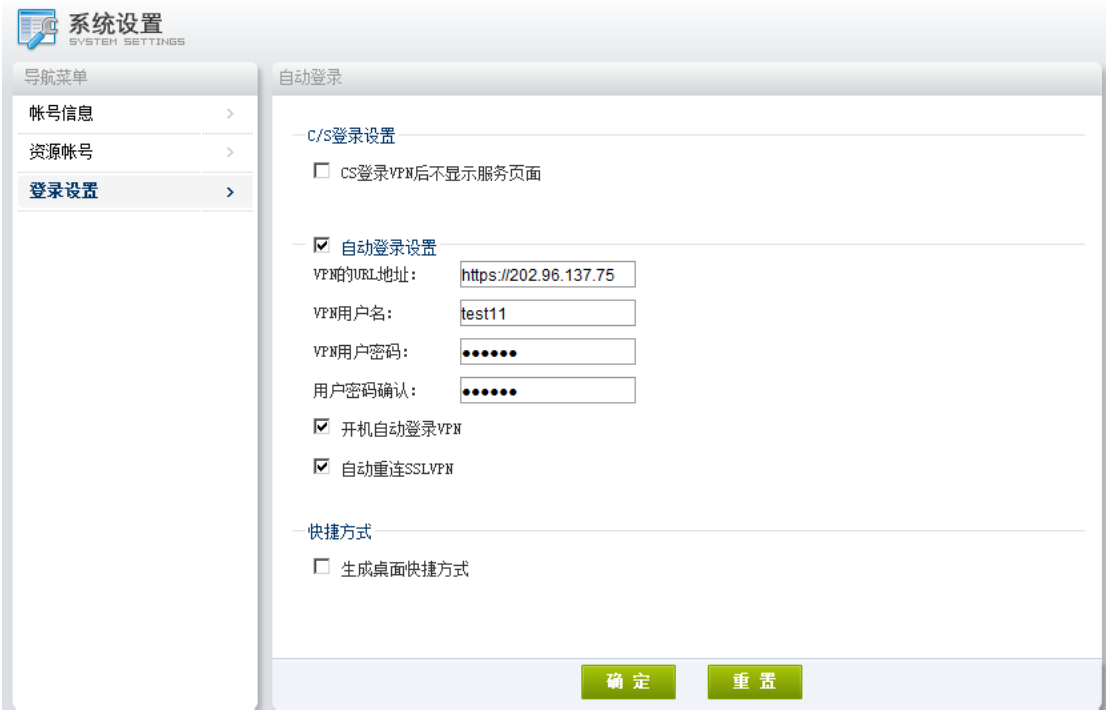


基于 B/S 架构，网络结构简单灵活、配置方便容易、立即安装、立即生效，适用于但客户端连接。

SSL网络设置：

1、首先按照本文档的 IPSec 网络的设置的前 3 步骤完成 SSL 网络设置，其中添加用的界面如下：

2、设置用户登录相关参数的界面如下：



3、客户端需求和配置：

客户端计算机已经接入因特网，并且网络通信正常。

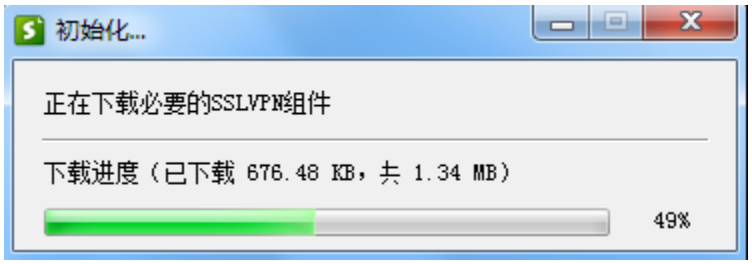
计算机必须安装浏览器（XP可以，win7的32位和64位不行）。

电脑安装3721、上网助手等工具，可能会影响正常使用SSL VPN，可以先卸载。

客户端登陆界面如下：

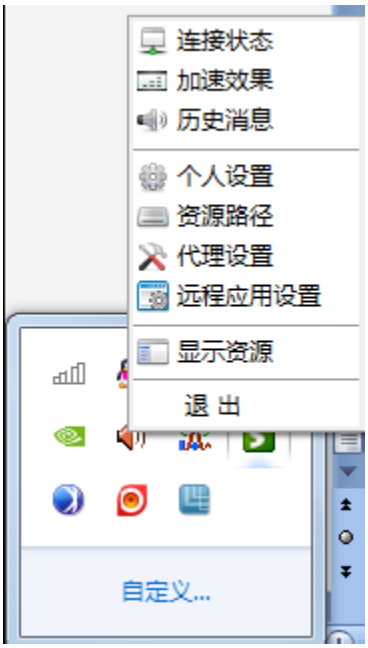
登录中依照向导完成插件安装，在安装 SSL VPN 组件的过程中，请先关闭本机的防火墙及杀

毒软件，否则可能会安装不成功。



若在设备里设置了客户端启用系统托盘，则登录后在电脑桌面的右下角显示SSL VPN客户端图标，将鼠标移上去，显示SSL VPN的流速信息，如下图：

右击该图标，可查看SSL VPN状态及对SSL VPN进行相关设置，如下图：



登陆成功后 web 页面如下：

设置完成。