service & SUPPORT

通过互联网在PC 站和 SCALANCE S61x 间配置VPN通道

SIEMENS

FAQ

ID: 32447942

目录

本条目由 Siemens AG, Automation and Drives, Service & Support 提供。
点击如下连接可以直接到达下载页面。

http://support.automation.siemens.com/WW/view/zh/32447942

问题

如何通过互联网在 PC station 和 SCALANCE S61x 间用 SOFTNET Security Client 2008 建立 VPN 通道？

解答

本文档提供了对该问题的详细解答。

ID: 32447942

1 导言

使用 SOFTNET Security Client Edition 2008， 可以在 Internet 上为 SCALANCE S61x 通过 Security Configuration Tool 建立 VPN 通道, SCALANCE S61x 运行于路由模式。

下面说明对 VPN 通道的组态。

图 1-1 配置说明了该配置的结构。

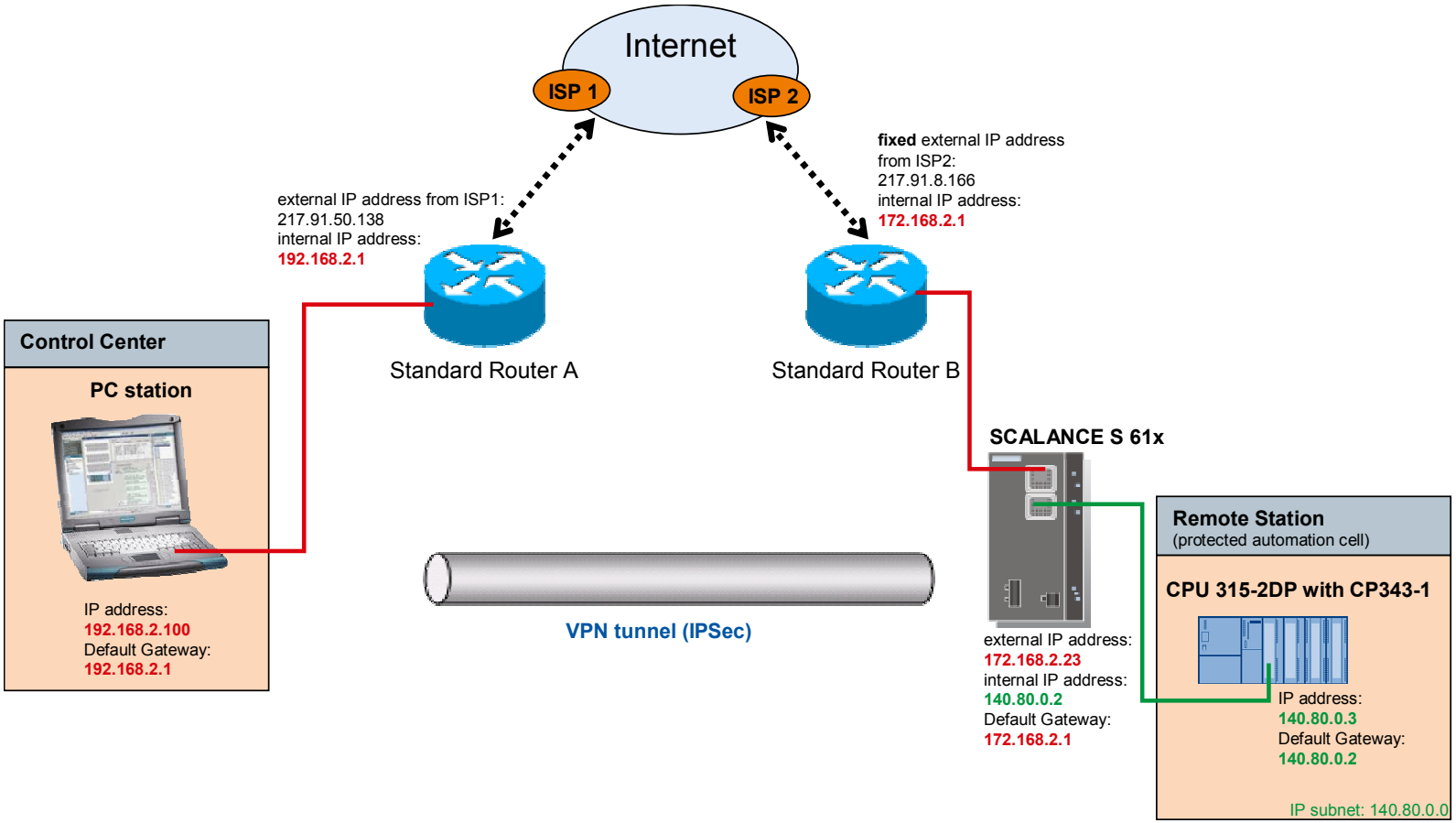
配置要求：

- 要支持建立通过路由模式的互联网 VPN 通道，SCALANCE S 61x 至少要固件版本 V2.1， SCALANCE S 61x 当前固件版本 V2.3 可通过如下链接下载:

  http://support.automation.siemens.com/WW/view/en/37352999

- 需要下列软件：
  - SOFTNET Security Client V2.0 (Edition 2008) 或更高版本
  - Security Configuration Tool V2.3 或更高版本
- 标准路由器 B 需要指定一个固定的外部 IP 地址。主动模块 (SOFTNET Security Client) 通过固定的外部 IP 地址，发起建立 VPN 通道。 被动模块 (SCALANCE S 61x) 等待来自远端 VPN 网关的连接。

图 1-1 配置



配置描述

S7-300 站包括一个 CPU 315-2DP 和一个 CP343-1。 该 CP 连接到 SCALANCE S61x 的内网。SCALANCE S 61x 保护 S7-300 站不受来自非信任的外部访问。

SCALANCE S 61x 是 S7-300 站的路由或者网关。

IP 地址 192.168.2.100 的 PC 站位于 SCALANCE S 61x 的外网。

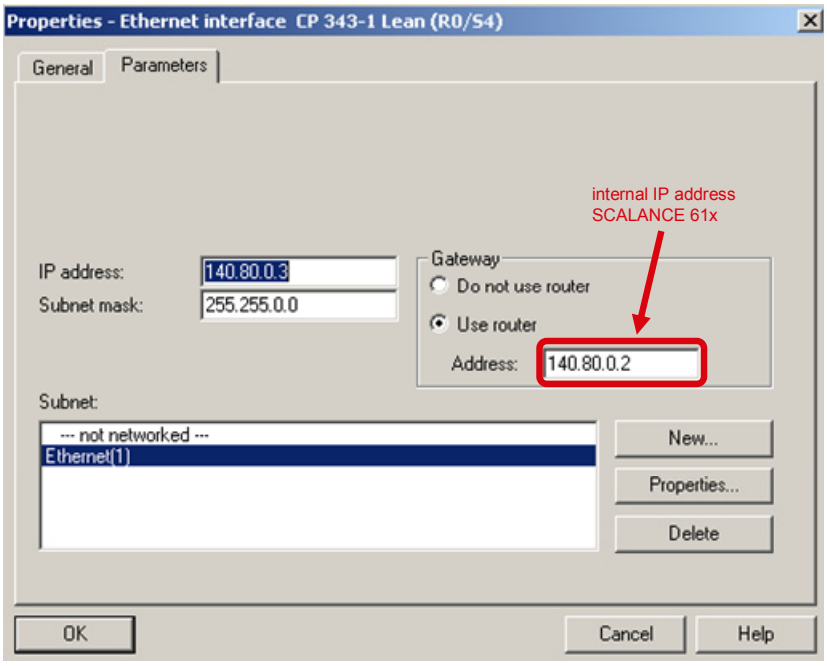
标准路由器 A 是 PC 站的网关或路由器和 DNS 服务器。

标准路由器 B 是 SCALANCE S 61x 的网关或路由器。

在 S7-300 站中定义路由或网关

- 在 S7-300 站硬件组态中打开 CP343-1 的接口属性。
- 激活 “Use router” （使用路由）功能，输入 SCALANCE S 61x 的内部 IP 地址 140.80.0.2。

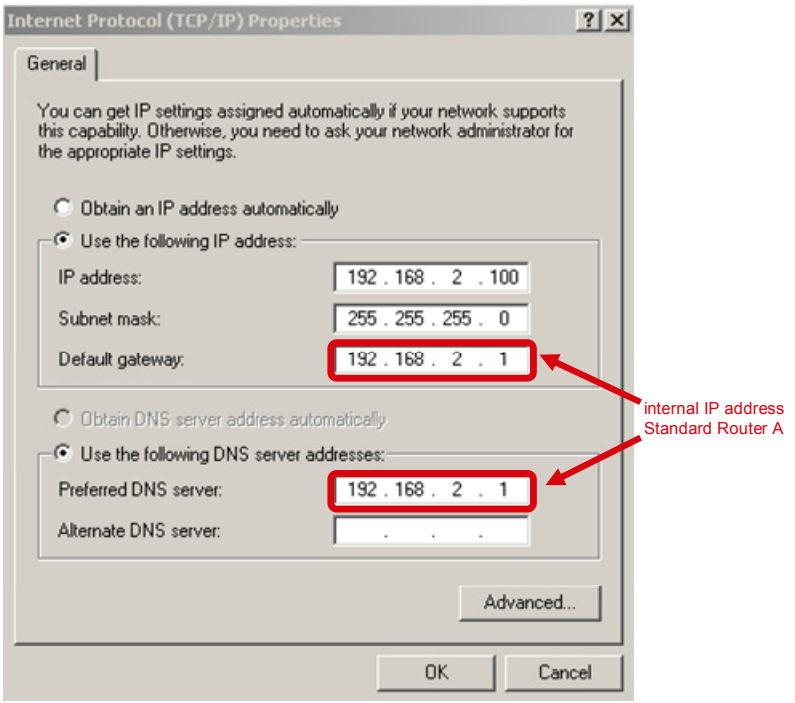
图 1-2 CP343-1 接口属性



在 PC 站中定义路由或网关

- 在 Windows 中，网络连接下打开本地网络(LAN).连接的属性
- 输入标准路由器 A 的内部 IP 地址，作为缺省网关和 DNS 服务器

图 1-3 LAN 属性对话框



说明

如果标准路由器 A 具有 DHCP 功能，那么 PC 可以从路由器 A 自动获取 IP 地址和 DNS 服务器地址。

下面是标准路由器 A 和 B 的配置。

2 配置标准路由器

标准路由器 A 连接到安装有 SOFTNET Security Client 的 PC 站。作为主动端的 SOFTNET Security Client 通过标准路由器 B 的固定外部 IP 地址发起建立 VPN 通道。

标准路由器 B 连接到被动模块 SCALANCE S 61x 的外部网络。SCALANCE S 61x 是被动参与到建立 VPN 通道中，它等待来自远端 VPN 网关的连接。

配置标准路由器 B 的端口转发规则

按照下面图表配置与被动端连接的标准路由器（路由器 B）的端口转发规则：

- 标准路由器 B 的端口 500 和 4500 的互联网 UDP 包， 转发到 SCALANCE S 61x 外部 IP 地址 172.168.2.23。

图 2-1 标准路由器 B 的端口转发

Custom Services Table

	#	Name	Type	Start Port	Finish Port
☐	60	IPSEC	UDP	4500	4500
☐	61	IKE_S	UDP	500	500

external IP address
SCALANCE S61x

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Bandwidth Profile	Log
☐	●	IKE_S	Allow Always	172.168.2.23		ANY	WAN1	NONE	Never
☐	●	IPSEC	Allow Always	172.168.2.23		ANY	WAN1	NONE	Never

根据如下说明配置 SCALANCE S 61x 和 SOFTNET Security Client.

3 配置 SCALANCE S 61x 和 SOFTNET Security Client

启动 Security Configuration Tool

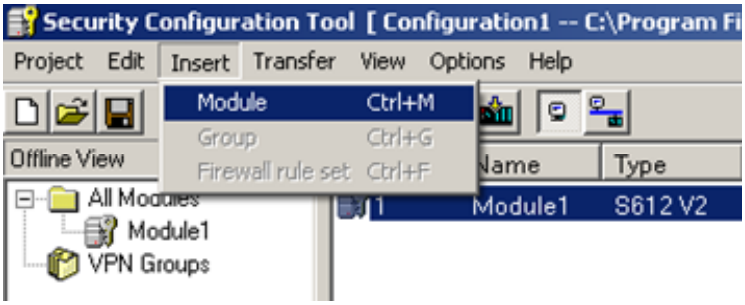
启动 Security Configuration Tool ： Start → SIMATIC → SCALANCE → Security → Security Configuration Tool 并创建一个新的项目。

3.1 配置 SCALANCE S 61x

插入模块

通过菜单 "Insert → Module"，插入一类型为 “S612 V2”的模块。

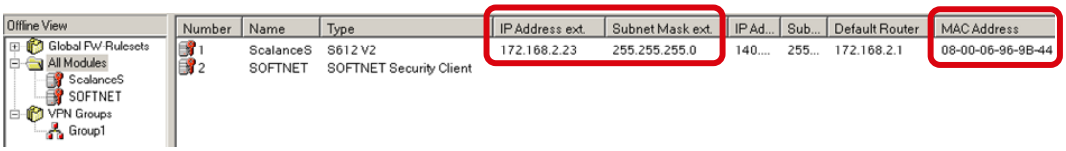
图 3-1 插入 “S612 V2”模块



分配外部 IP 地址和 MAC 地址

- 为 “S612 V2” 模块分配外部 IP 地址 172.168.2.23 和子网掩码 255.255.255.0。
- 输入 SCALANCE S 61x 的 MAC 地址。

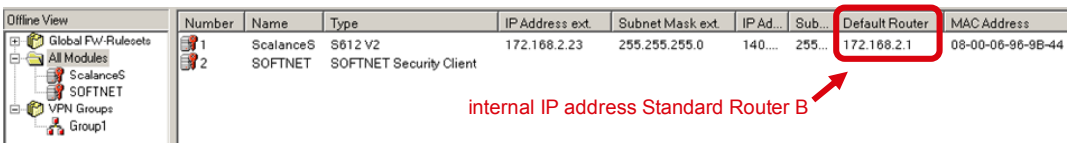
图 3-2 分配外部 IP 地址和 MAC 地址



输入缺省路由器

输入标准路由器 B 的内部 IP 地址 172.168.2.1，作为缺省路由器。

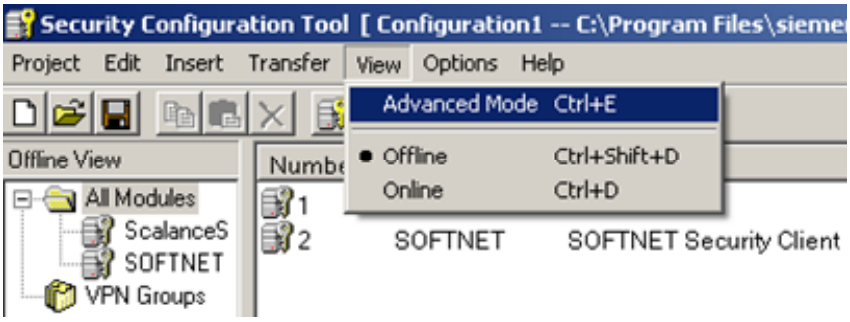
图 3-3 输入缺省路由器



使能 “Advanced Mode（高级模式）”，分配内部 IP 地址

通过"View"菜单，使能 "Advanced Mode 高级模式"

图 3-4 使能 “Advanced Mode（高级模式）”



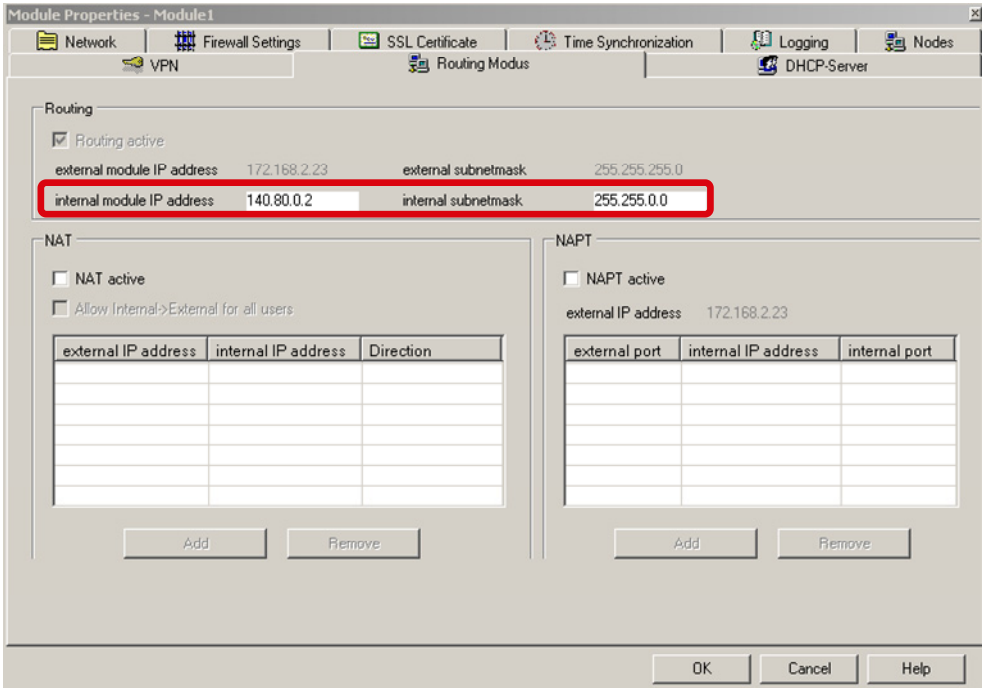
在“All Modules”下双击 “S612 V2”模块，打开模块属性。

切换到 “Routing Modus” 标签。

使能 “Routing active”功能。

输入内部 IP 地址 140.80.0.2 和子网掩码 255.255.0.0.

图 3-5 模块属性 “S612 V2” → 标签 “Routing Modus”

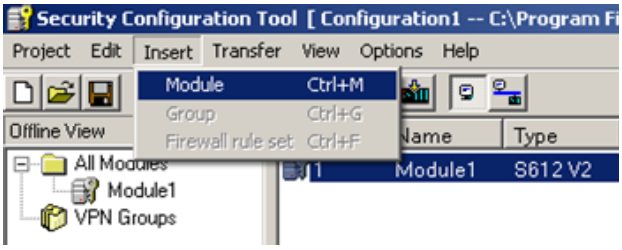


3.2 配置 SOFTNET Security Client

插入模块

通过菜单"Insert → Module"，插入 “SOFTNET Security Client”模块

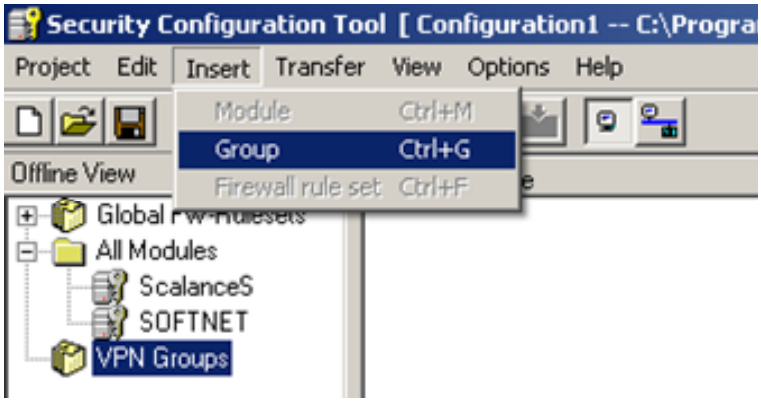
图 3-6 插入 “SOFTNET Security Client”模块



创建组

通过菜单“Insert → Group”创建一新组。

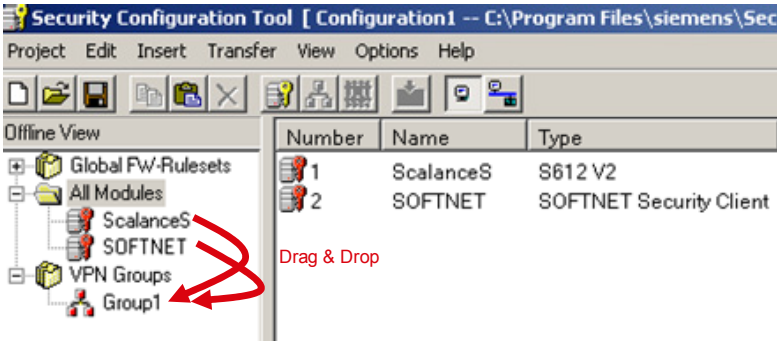
图 3-7 创建组



分配模块到组

通过拖放操作，将“S612 V2”模块和 “SOFTNET Security Client”模块分配到创建的组。

图 3-8 分配模块到组



3.3 配置虚拟专用网络 (VPN)

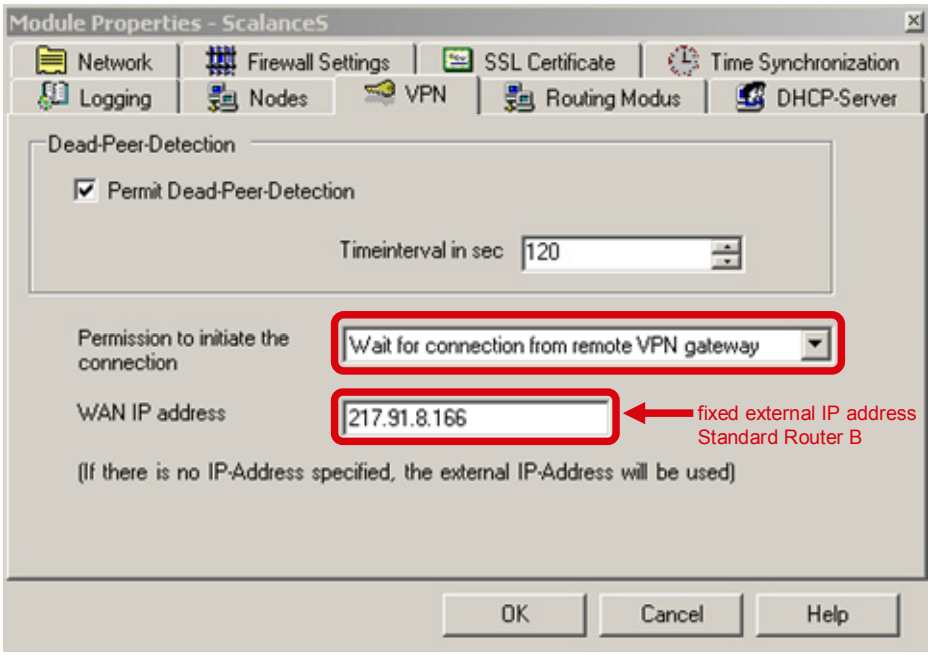
在“All Modules”下，双击 “S612 V2”打开模块属性

在模块属性里切换到标签 “VPN”

选择功能 “Wait for connection from remote gateway（等待来自远端网关的连接）”

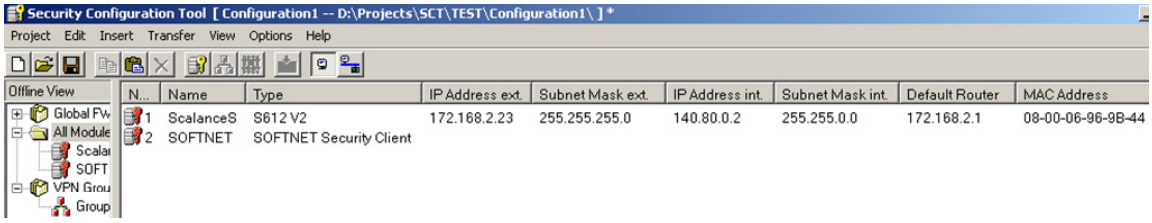
在“WAN IP address”里输入标准路由器 B 的固定外部 IP 地址 217.91.8.166

图 3-9 模块属性 “S612 V2” → 标签 “VPN”



现在完成了 SCALANCE S 61x 和 SOFTNET Security Client 的配置。

图 3-90 完成配置

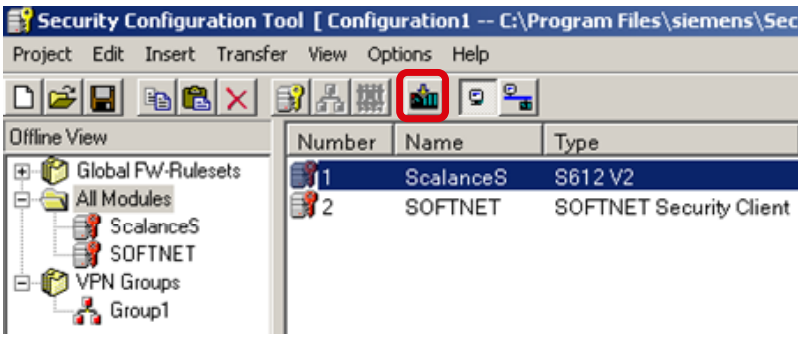


3.4 下载和保存配置

下载配置到 SCALANCE S61x

在“All Modules”中选择 “S612 V2”模块，点击按钮“download”， 将配置分配到 SCALANCE S 61x.

图 3-11 分配配置到 SCALANCE S61x

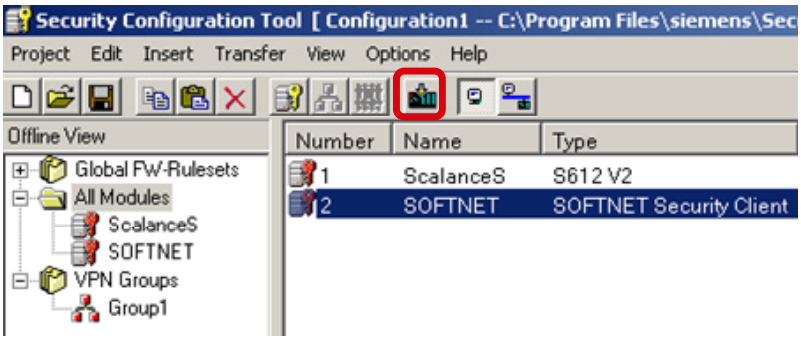


说明： 当 SCALANCE S61x 处于工厂设置时，对 SCALANCE S61x 的第一次下载不能通过 internet 完成。第一次下载必定发生在工厂设置时。

保存 SOFTNET Security Client 配置

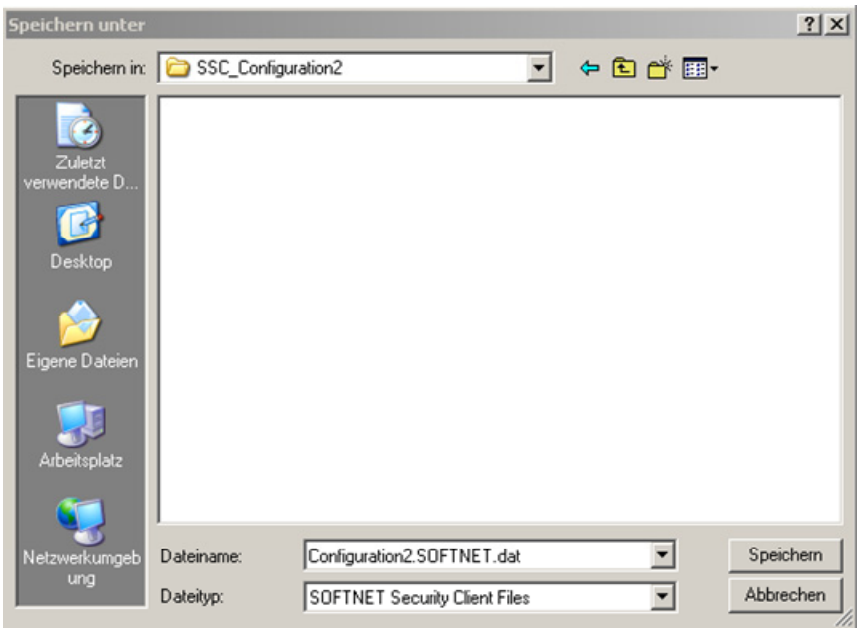
在 “All Modules” 中选择 “SOFTNET Security Client”，点击按钮“download”，保存 SOFTNET Security Client 的配置数据。

图 3-102 保存 SOFTNET Security Client 配置



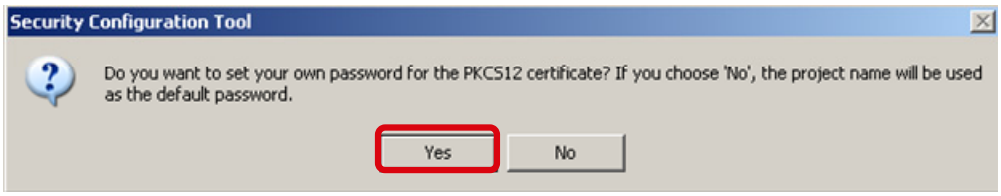
SSC 的配置数据保存到一个 "*.dat" 格式的文件，在本例中，该文件命名为 "Configuration2.SOFTNET.dat".

图 3-13 创建配置数据



可以为 PKCS12 认证定义一个独立的密码。点击 “Yes”确认如下信息，如果点击 “No”， 项目名将作为 PKCS12 认证密码。

图 3-14 定义 PKCS12 认证密码



在下面的对话框中输入并确认 PKCS12 认证密码。点击 “OK” 关闭对话框。

图 3-115 PKCS12 认证密码

4 用 SOFTNET Security Client 建立 VPN 通道

SOFTNET Security Client 通过 Internet 在 PC 站和 SCALANCE S61x 之间建立 VPN 通道

启动 SOFTNET Security Client

启动 SOFTNET Security Client ： Start → SIMATIC → SCALANCE → Security → SOFTNET Security Client.

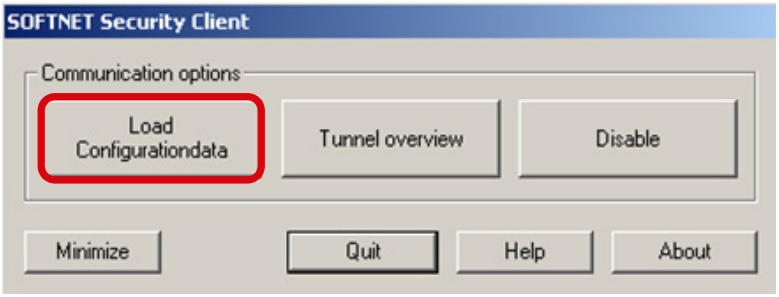
如果 PC 站上安装有多个访问 internet 的接口 (如. WLAN, UMTS 卡...), 打开 SOFTNET Security Client 时，将会出现选择接口的对话框，在该对话框中选中期望用于 internet 访问的接口。

可以在对话框 “Tunnel overview” 中打开选择接口的对话框，右击建立 VPN 通道的模块，选择菜单“Select Network Device”。

加载配置数据

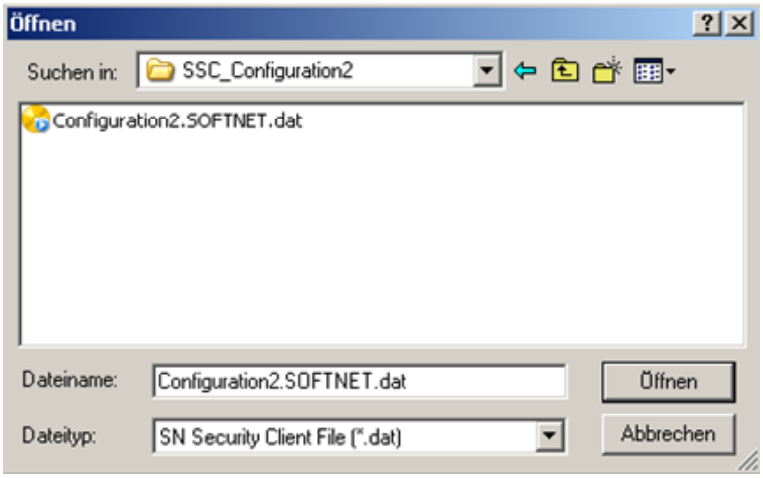
单击按钮 “Load Configurationdata”， 在 SOFTNET Security Client 中加载配置数据。

图 4-1 加载配置数据



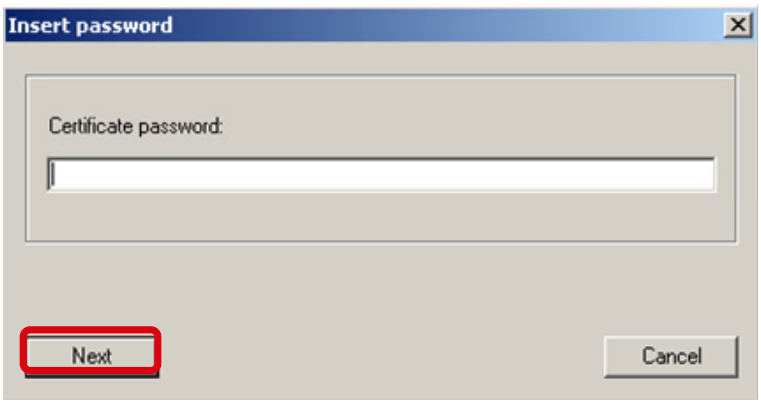
打开配置文件 “Configuration2.SOFTNET.dat”.

图 4-2 打开配置文件



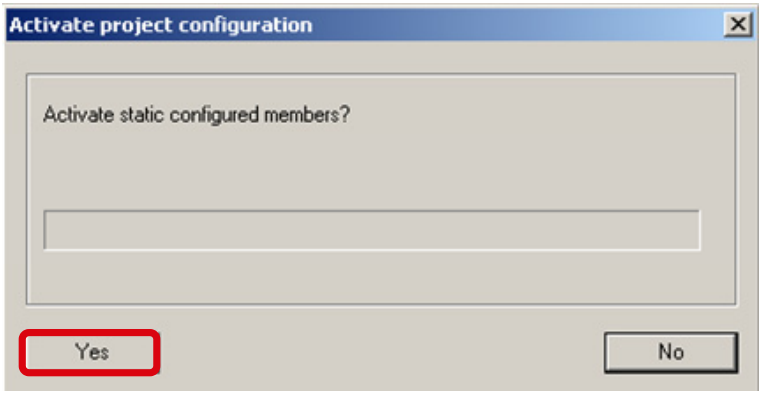
在下面的对话框中，输入在保存配置数据文件时为 PKCS12 认证所定义的密码。如果没有为 PKCS12 认证定义独立的密码，输入由 Security Configuration Tool 创建并保存有 SCALANCE S61x 和 SOFTNET Security Client 配置信息的项目的名称作为密码。

图 4-3 输入 PKCS12 认证密码



点击“Yes”认如下信息：

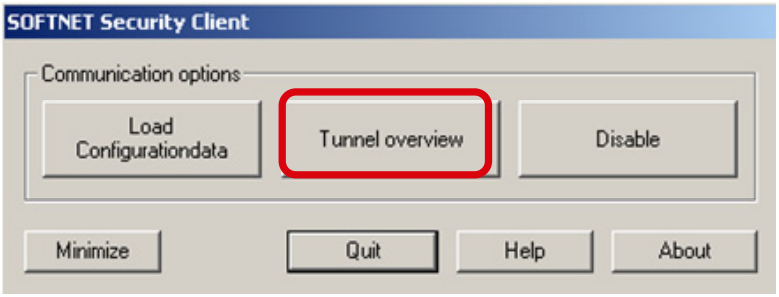
图 4-4 对话框 “激活项目组态”



检查 VPN 通道

在下面的对话框中，点击按钮 “Tunnel overview”，打开“Tunnel overview” 对话框。

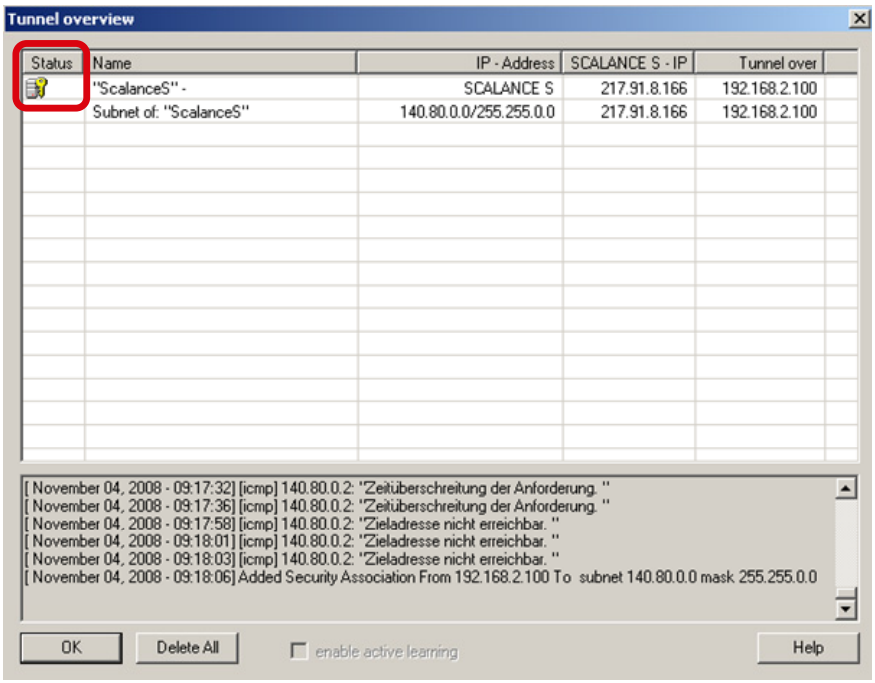
图 4-5 打开 “Tunnel overview”对话框



在 “Tunnel overview” 对话框中，列出了通过 VPN 通道能够连接到的模块和子网。

如果成功建立的 VPN 通道，SCALANCE S61x 可以被 PC 站访问到，那在 “Status（状态）”栏中将出现一个带黄色钥匙的图标。

图 4-6 对话框 “Tunnel overview”



5 诊断

如果 PC 和 SCALANCE S61x 之间的 VPN 通道是建立在 Internet 上，则可以从 PC 站访问到受保护的自动化单元 (S7-300 站) 。

- 可以在 PC 站 ping 通 S7-300 站的工业以太网通讯模块。
- 在 STEP 7 里，可以通过 PG/OP 在线访问到 S7-300 控制器，这样可以把 STEP 7 项目或组态下载到 S7-300 CPU 或者读取 CPU 的诊断信息。

说明

VPN 通道不支持二层协议，如 STEP 7 中的"accessible nodes 功能。
如果在 PC 站里安装了额外的防火墙，可能导致出现问题。

6 历史

表 6-1 历史

版本	日期	修改内容
V1.0	03.12.08	第一版
V1.1	15.12.08	修改了文档结构和内容
V1.2	11.08.09	• 改正了部分拼写错误 • 如果保存证书时没有定义单独的密码,那么项目名将用作密码. • 章节1: 增加了下载SCALANCE S61x 当前固件版本 V2.3 的链接. • 章节 3.1: 删除了 “增加防火墙规则”的段落. • 章节 4: 增加了如何打开选择网络正确适配器对话框的说明.