

西门子工业安全 SCALANCE S 用户指导手册

SIEMENS Industrial security SCALANCE S User Guide

User Guide

Edition (2008-2)

SIEMENS A&D CS

摘要 随着 PROFINET 和 SCALANCE 在中国市场的不断深入，越来越多的用户选择和使用 PROFINET 和 SCALANCE。使用 PROFINET 和 SCALANCE X/W 构成工厂局域网，根据需要可以与办公室级别的网络连接在一起，甚至连接 Internet。而这时无论对于局域网还是广域网，工厂自动化的信息安全尤显重要。这就要求使用某些方式在工业生产中保护数据的完整性，操作的正确性，防止数据丢失或伪造，以保证工业生产的顺利进行。西门子工业安全 SCALANCE S 是西门子全新推出的高性能安全模块，支持 DHCP，Syslog，防火墙，虚拟专用网络，NAT/NAPT，路由等功能，满足工业网络现场的信息安全要求。本手册全面讲述了 SCALANCE S 的各种功能，用户可以根据本手册了解和掌握 SCALANCE S 的组态，并应用到工业网络控制的信息安全中。

关键词 SCALANCE S，DHCP，Syslog，防火墙，虚拟专用网络，网络地址解析/网络地址端口解析，路由

Key words SCALANCE S，DHCP，Syslog，Firewall，VPN，NAT/NAPT，Route

目 录

第一章SCALANCE S简介	4
第二章DHCP服务器	5
2.1 DHCP概述	5
2.2 DHCP组态	5
第三章Syslog	11
3.1 Syslog概述	11
3.2 Syslog组态	11
第四章 防火墙	13
4.1 防火墙概述	13
4.2 防火墙组态	13
第五章 虚拟专用网络	18
5.1 VPN概述	18
5.2 VPN组态	20
第六章 路由	26
6.1 路由概述	26
6.2 路由组态	26
第七章 NAT/NAPT	33
7.1 NAT/NAPT概述	33
7.2 NAT/NPAT组态	33

第一章 SCALANCE S 简介

通过不同的安全措施的组合，例如防火墙，NAT/NAPT，路由以及VPN等，SCALANCE S612/613实现对自动化网络Cell的保护。这样对于自动化网络的数据探测、随意操作、非法访问是不可能的。

SCALANCE S612/613满足自动化工程应用环境的特殊要求，特别用于保证可用性和无故障操作的场合，保护工厂和产品生产。与Softnet Security Client客户端软件一起，可以实现可伸缩性的保护性能。通过使用Security Configuration Tool工具可以简单的使用SCALANCE S，并且组态安全策略的方法简单，不需要专业IT安全知识。

SCALANCE S提供了以下的安全功能：

防火墙。支持状态包检测功能（Stateful Packet Inspection），可以过滤非IP报以及带宽限制。所有内部网络设备被SCALANCE S保护。

安全的IPSec通讯。SCALANCE S可以通过组态配置成组。IPSec隧道在组内的SCALANCE S之间建立，通过隧道，内部网络节点之间的通讯是安全的。

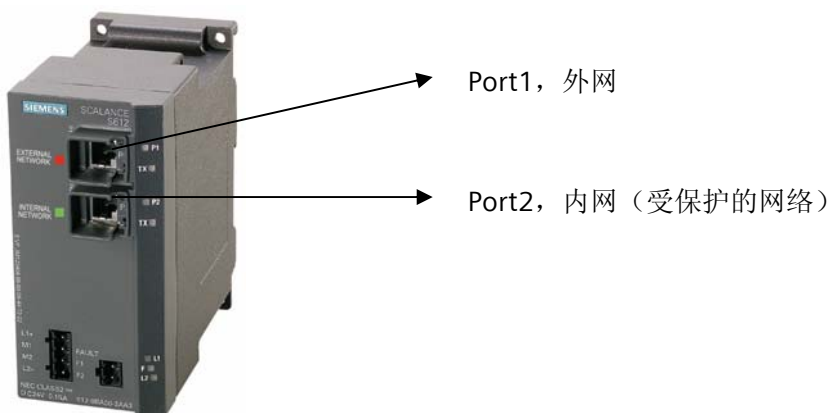
协议无关性。隧道可以允许所有种类的帧通过。IP和非IP帧可以在IPSec隧道中传输。

路由模式。SCALANCE S可以作为路由器。可以通过该路由器，连通内网和外网。于是连接SCALANCE S的内网就成为独立的子网。

保护设备和网段。防火墙和VPN功能可以应用在单独的设备，几个设备或整个网络中

在扁平网络中不需要响应。SCALANCE S不需要组态就可以发现内部网络的节点。这意味着当SCALANCE S安装在已存的网络中，网络节点不需要重新组态。SCALANCE S发现这些内部节点，而不能被发现的内网节点需要组态。

SCALANCE S上有2个RJ45端口，其中Port1红色标记的用于连接外部网络，而Port2绿色标记的用于连接内部网络。内部网络的节点是受保护的。



第二章 DHCP 服务器

2.1 DHCP 概述

DHCP 是 Dynamic Host Configuration Protocol 之缩写，它的前身是 BOOTP，即“动态主机配置协议”。

BOOTP 原本是用于无盘主机连接的网路上的，网路主机使用 BOOTROM 而不是磁碟启动并连接上网路，BOOTP 则可以自动地为那些主机设定 TCP/IP 环境。但 BOOTP 有一个缺点：您在设定前须事先获得客户端的硬件地址，而且，与 IP 的对应是静态的。换言之，BOOTP 非常缺乏“动态性”，若在有限的 IP 资源环境中，BOOTP 的一对一对应会造成非常可观的浪费。

DHCP 可以说是 BOOTP 的增强版本，它分为两个部份：一个是服务器端，而另一个是客户端。所有的 IP 网路设定资料都由 DHCP 伺服器集中管理，并负责处理客户端的 DHCP 要求；而客户端则会使用从伺服器分配下来的 IP 环境资料。比较起 BOOTP，DHCP 透过“租约”的概念，有效且动态的分配客户端的 TCP/IP 设定，而且，作为兼容考量，DHCP 也完全照顾了 BOOTP Client 的需求。

SCALANCE S 可以作为内部网络的 DHCP 服务器，这样 IP 地址自动分配给内部网络的设备。IP 地址的分配可以来自于组态的地址池中，也可以给某一设备分配一个固定的 IP 地址。默认的租约为 2 天。

2.2 DHCP 组态

DHCP 网络组态图：



网络组态由两台主机 Host1 和 Host2 分别与 SCALANCE S 的端口 1（External）和端口 2（Internal）相连。其中 Host1 用于配置 SCALANCE S。而 SCALANCE S 给 Host2 动态分配 IP 地址。在配置 SCALANCE S 之前需要配置 Security Configuration Tool(简称 SCT)软件 V2.1 版本。

序号	组态步骤
1	打开 SCT，点击新建项目图标  ，此时弹出新建项目的用户信息，根据需要建立用户名和密码。这里用户名和密码均为 s。点击 OK 按钮结束。

	New administrator User Name \$ Password * Password confirmation * OK Cancel																		
2	对于 Type，点击下拉菜单，选择要操作的 SCALANCE S，这里使用 SCALACNE S612 V2 版本。在 IP Address ext 和 Subnet Mask ext 中给 SCALANCE S612 的外网 IP 地址和子网掩码为 192.168.0.1 和 255.255.255.0。最后把 SCALANCE S612 上的 MAC 地址输入到 MAC Address 中。 Security Configuration Tool [Configuration1 -- C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Project Edit Insert Transfer View Options Help Offline View All Modules Module1 VPN Groups <table><thead><tr><th>Number</th><th>Name</th><th>Type</th><th>IP Address ext.</th><th>Subnet Mask ext.</th><th>IP Address int.</th><th>Subnet Mask int.</th><th>Default Router</th><th>MAC Address</th></tr></thead><tbody><tr><td>1</td><td>Module1</td><td>S612 V</td><td>192.168.0.1</td><td>255.255.255.0</td><td></td><td></td><td></td><td>08-00-06-9A-E7</td></tr></tbody></table> Ready Current User: s Role: Admin Standard Mode Offline	Number	Name	Type	IP Address ext.	Subnet Mask ext.	IP Address int.	Subnet Mask int.	Default Router	MAC Address	1	Module1	S612 V	192.168.0.1	255.255.255.0				08-00-06-9A-E7
Number	Name	Type	IP Address ext.	Subnet Mask ext.	IP Address int.	Subnet Mask int.	Default Router	MAC Address											
1	Module1	S612 V	192.168.0.1	255.255.255.0				08-00-06-9A-E7											
3	点击 View 菜单，选择高级模式 Advanced Mode。 Security Configuration Tool [Configuration1 -- C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Project Edit Insert Transfer View Options Help Advanced Mode Ctrl+E Offline Ctrl+Shift+D Online Ctrl+D <table><thead><tr><th>IP Address ext.</th><th>Subnet Mask ext.</th><th>IP Address int.</th><th>Subnet Mask int.</th><th>Default Router</th><th>MAC Address</th></tr></thead><tbody><tr><td>192.168.0.1</td><td>255.255.255.0</td><td></td><td></td><td></td><td>08-00-06-9A-E7</td></tr></tbody></table> Ready Current User: s Role: Admin Standard Mode Offline 这时会弹出一个警告对话框，提示一旦选择高级模式，将不会切换回标准模式。 Security Module Engineering Do you want to change to advanced mode? Warning: If you make changes in advanced mode, you cannot return to standard mode! Yes No 这里点击 Yes 按钮。	IP Address ext.	Subnet Mask ext.	IP Address int.	Subnet Mask int.	Default Router	MAC Address	192.168.0.1	255.255.255.0				08-00-06-9A-E7						
IP Address ext.	Subnet Mask ext.	IP Address int.	Subnet Mask int.	Default Router	MAC Address														
192.168.0.1	255.255.255.0				08-00-06-9A-E7														
4	双击模块图标或者在菜单 Edit 中选择属性 Property 选项。弹出模块属性对话框。该模式是 SCALACNE S 的高级模式。																		

Module Properties - Module 1

Network | Firewall Settings | SSL Certificate | Time Synchronization | Logging | Nodes

VPN | Routing Modus | **DHCP-Server**

☐ activate DHCP

static IP Addresses:

MAC Address	ClientID	IP Address

Add Remove

dynamic IP Addresses:

Start End

OK Cancel Help

- 5 在模块属性对话框中，使能 DHCP 属性。在动态 IP 分配栏中分配 192.168.0.10 的起始地址以及 192.168.0.99 的结束地址，这个地址段需要与 SCALANCE S 的 IP 地址处于同一网段。这里也可以给设备根据 MAC 地址来设置固定的 IP 地址，这里保持默认。租约默认为 2 天。点击 OK 按钮结束。

Module Properties - Module 1

Network | Firewall Settings | SSL Certificate | Time Synchronization | Logging | Nodes

VPN | Routing Modus | DHCP-Server

☒ activate DHCP

static IP Addresses:

MAC Address	ClientID	IP Address

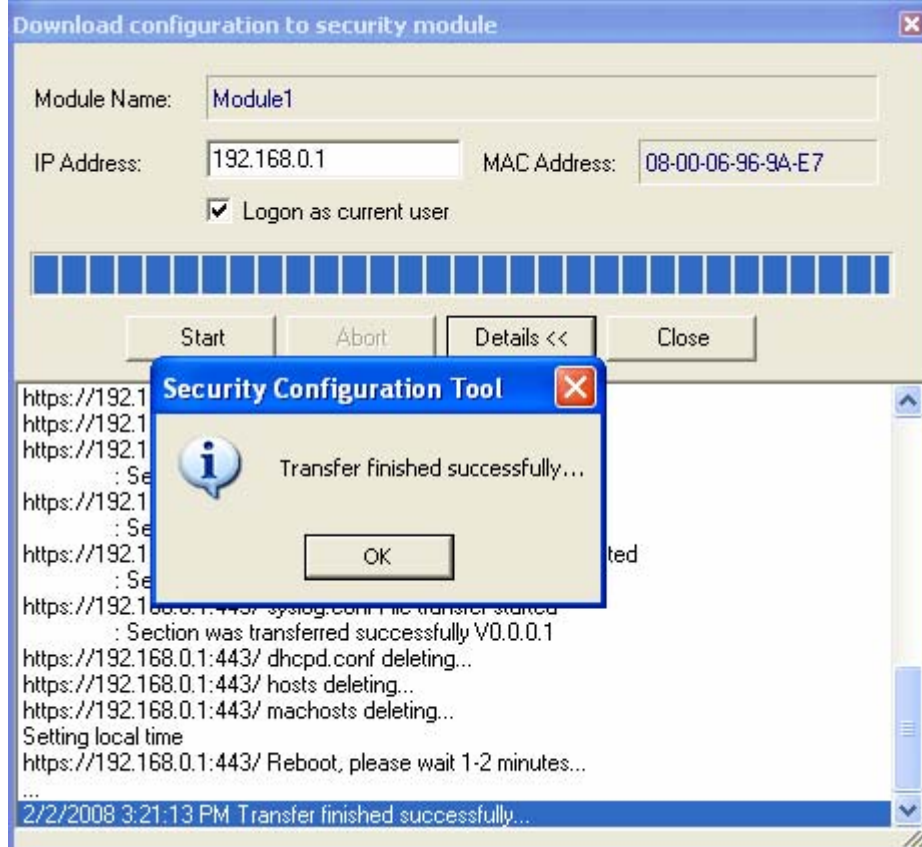
Add Remove

dynamic IP Addresses:

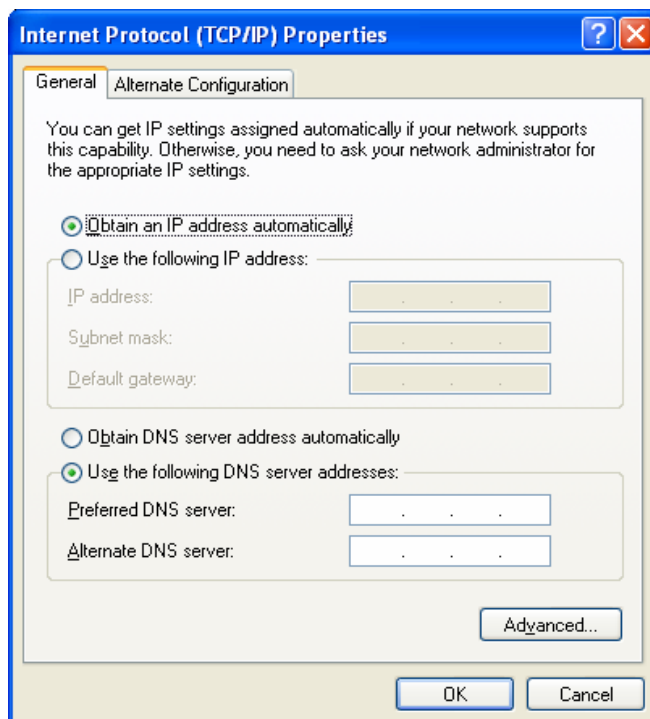
Start 192.168.0.10 End 192.168.0.99

OK Cancel Help

- 6 点击工具栏上的保存图标 ，保存该项目。设置 Host1 的 IP 地址 192.168.0.3。点击工具栏上的下载图标  载项目到 SCALANCE S612 中，直到提示下载成功。可以点击 Detail<< 按钮察看下载详细状态。如果在 SCALANCE S 中有先前的项目，需要通过背板按钮复位该模块。



- 7 设置主机 Host2 的 IP 为自动获取。



然后观察是否获得由 DHCP 服务器分配的动态 IP 地址。在 CMD 中输入 IPconfig -all 命令察看结果。

```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig -all

Windows IP Configuration

    Host Name . . . . . : SIMATIC
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Description . . . . . : VIA Rhine II Fast Ethernet Adapter
    Physical Address. . . . . : 08-00-06-90-BA-AD
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . : Yes
    IP Address. . . . . : 192.168.0.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
    DHCP Server . . . . . : 192.168.0.1
    Lease Obtained. . . . . : 2008年2月2日 16:37:13
    Lease Expires . . . . . : 2008年2月4日 16:37:13

C:\Documents and Settings\Administrator>
```

第三章 Syslog

3.1 Syslog 概述

Syslog 是 IP 网络中转发日志消息的标准协议。这个术语 Syslog 常常看作实际的 Syslog 协议，以及应用或者发送 Syslog 信息的库。

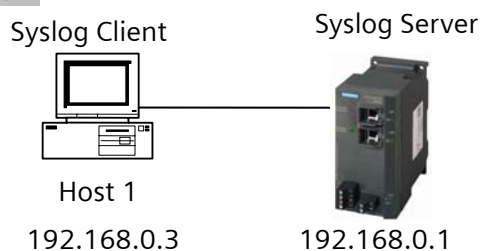
Syslog 协议是一个 Client/Server 的结构：Syslog 发送者发送少于 1024 个字节给 Syslog 接收者。接收者常常被称为 Syslogd，Syslog daemon 或者 Syslog server。Syslog 消息可以通过 UDP 或者 TCP 来发送。数据发送以纯文本结构，可以通过 SSL 进行数据加密。

Syslog 典型的用于网络系统的管理和安全审查。大多数设备和跨平台的接收者都支持 Syslog，这样 Syslog 就可以从不同类型的系统读取日志文件到中央存储。

SCALANCE S 的日志文件可以通过组态发送到 Syslogd 上，这样可以方便的管理和诊断 SCALANCE S。

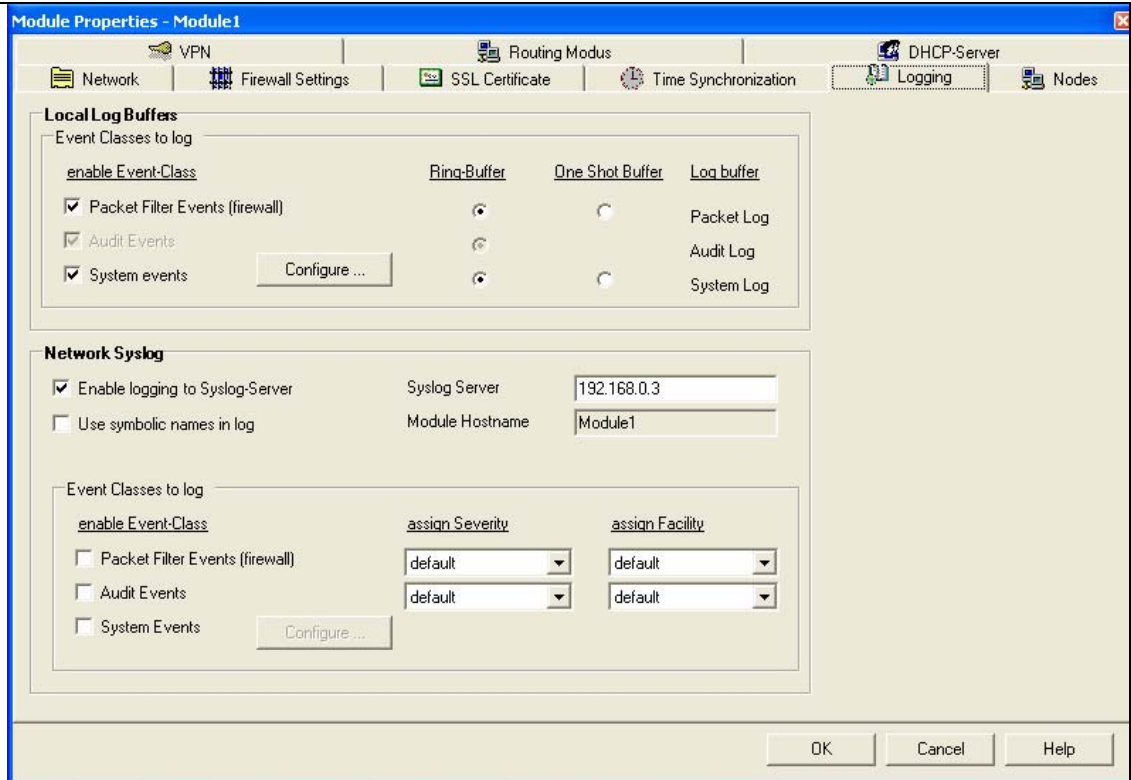
3.2 Syslog 组态

Syslog 网络组态图：

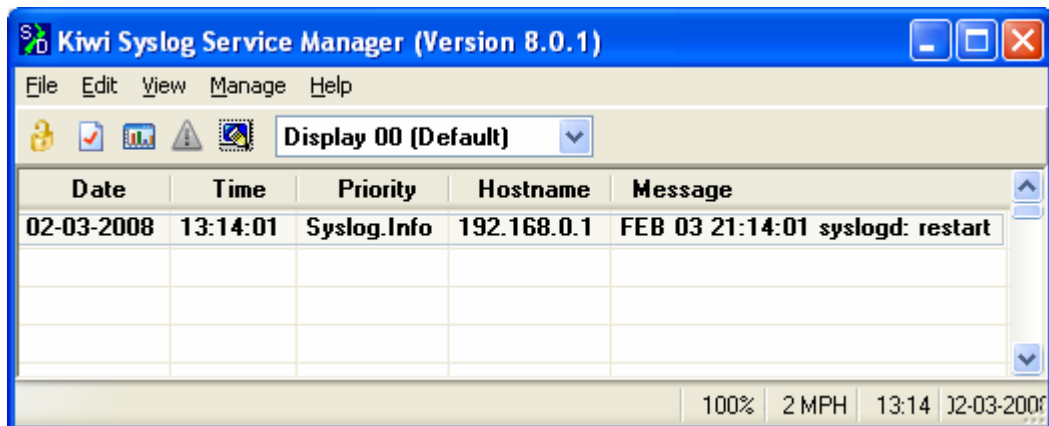


Host1 与 SCALANCE S 的端口 1 相连，IP 地址如图所示。在配置 SCALANCE S 之前需要配置 Security Configuration Tool(简称 SCT)软件 V2.1 版本。在 Syslog client 中需要安装 Syslogd，这里安装了免费的 Kiwi syslog daemon。

序号	组态步骤
1	参考 DHCP 服务器的组态步骤到 4。双击模块图标或者在菜单 Edit 中选择属性 Property 选项。弹出模块属性对话框。使能 Enable logging to Syslog Server 选项，设置 192.168.0.3 的 Syslog Server 的 IP 地址。点击 OK 按钮结束。



- 2 保存和下载项目参考 DHCP 项目的步骤 6。打开 Kiwi syslog daemon，可以看见 SCALANCE S 的日志文件。



第四章 防火墙

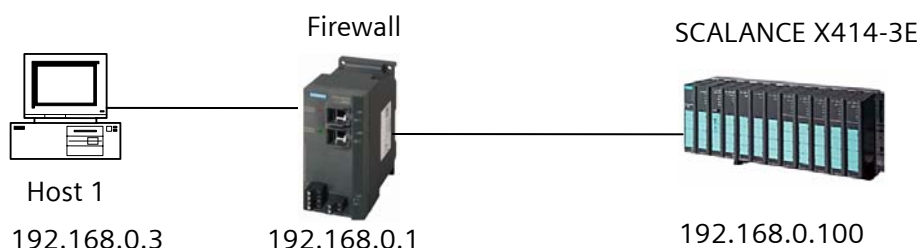
4.1 防火墙概述

防火墙的基本任务就是控制不同信任级别的计算机网络中的数据流。所有来自于外部网络的防护是绝对必须的。防火墙不但可以应用在Internet，也可以应用在Intranet中，特别是在重要的工业现场局域网中。通过防火墙可以防止外部网络的非法访问和错误操作，保护PLC等现场设备正常的运行。防火墙可以通过过滤数据包例如IP地址或端口号，监视应用层的内容以及监视外部访问的授权等，来实现某一特定的安全策略。

SCALANCE S作为防火墙的主要作用就是防止外网非法入侵以保护内网的安全。这就意味着通过某些组态，某些外部网络到内部网络的数据流才允许通过。所有处于内网的节点受SCALANCE S防火墙的保护。SCALANCE S支持状态包检测，非IP包的过滤（2层数据帧），带宽限制等等实现防火墙的功能。

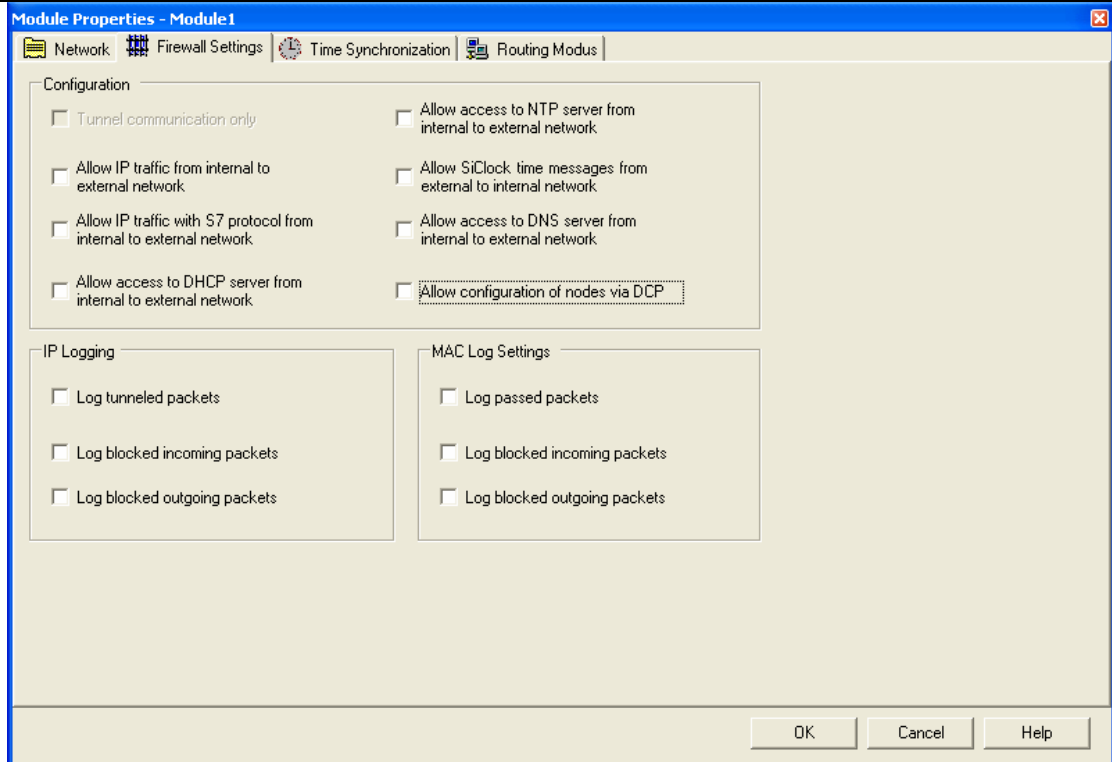
4.2 防火墙组态

防火墙网络组态图：



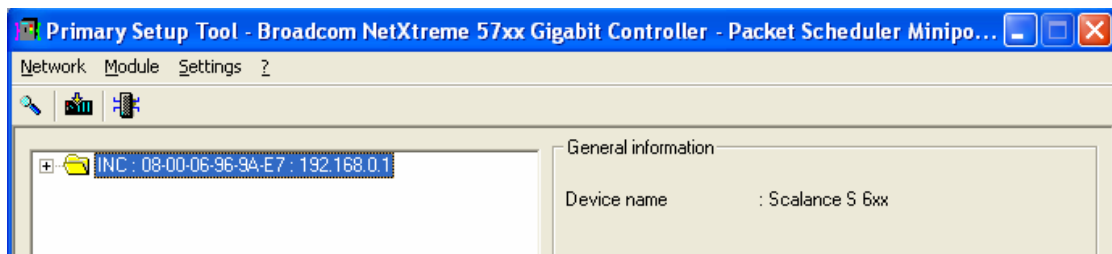
主机 Host1 与 SCALANCE S 的端口 1 相连，西门子交换机 SCALANCE X414-3E 与 SCALANCE S 的端口 2 相连。这时 Host1 处于外网，而 SCALANCE X414-3E 处于内部网络。默认 SCALANCE S 是一个防火墙，阻止任何外部数据访问内部网络，只能通过一系列的组态允许某些外部数据访问内部网络。通过设置，Host1 可以使用 PST 工具扫描到 SCALANCE X414-3E，在 Host1 中可以通过 IE 浏览器浏览 SCALANCE X414-3E 的 Web。

序号	组态步骤
1	参考 DHCP 服务器的组态步骤到 2。双击模块图标或者在菜单 Edit 中选择属性 Property 选项。弹出模块属性对话框。该模式是 SCALACNE S 的标准模式。



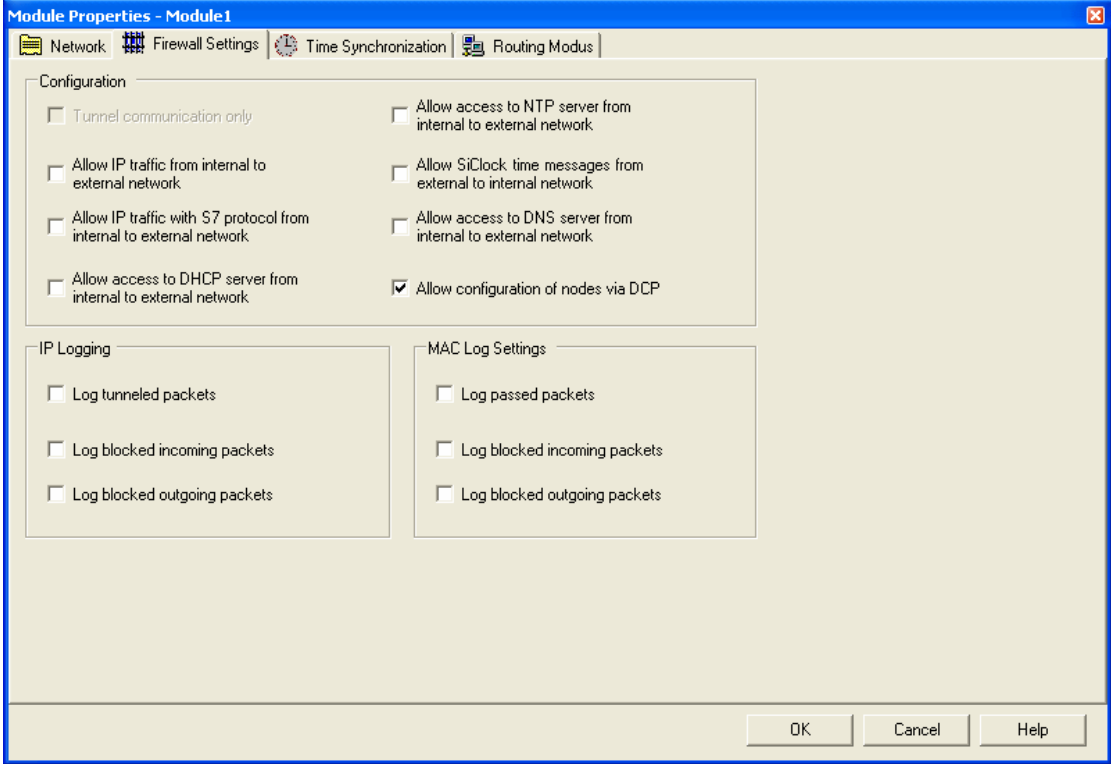
保存和下载默认项目参考 DHCP 项目的步骤 6。

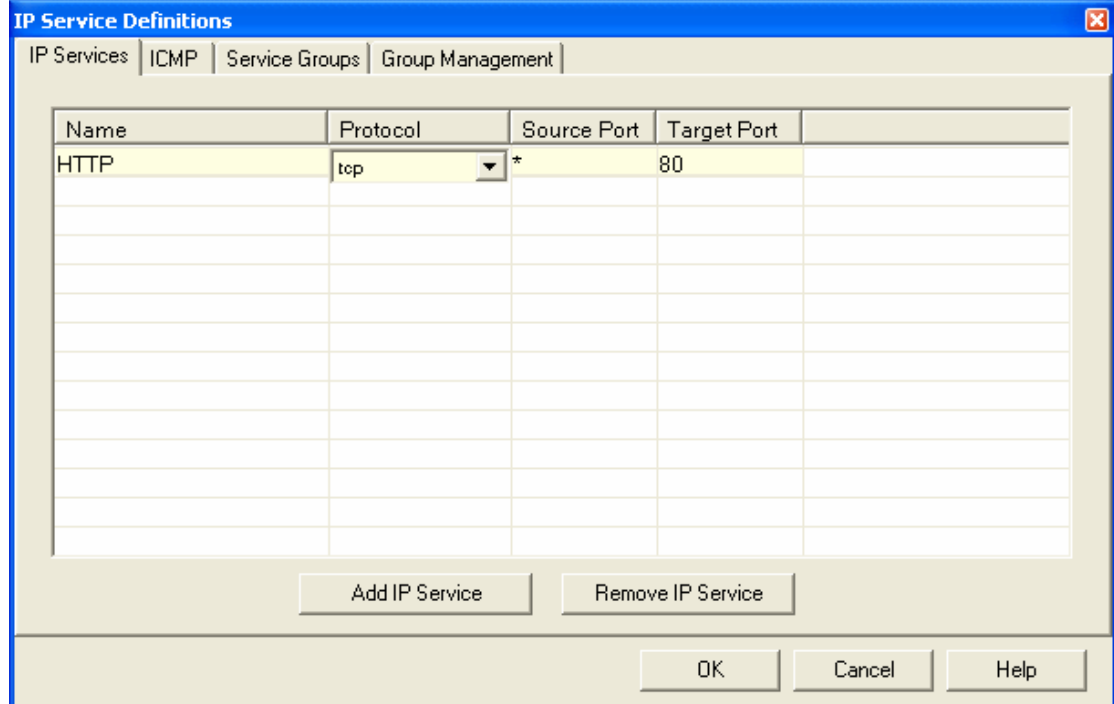
- 2 按照网络连接，在 Host1 中打开 PST 工具，扫描网络中的设备。结果可以发现仅有 SCALANCE S。



通过 IE 浏览器不能打开 192.168.0.100 的 Web 页面。



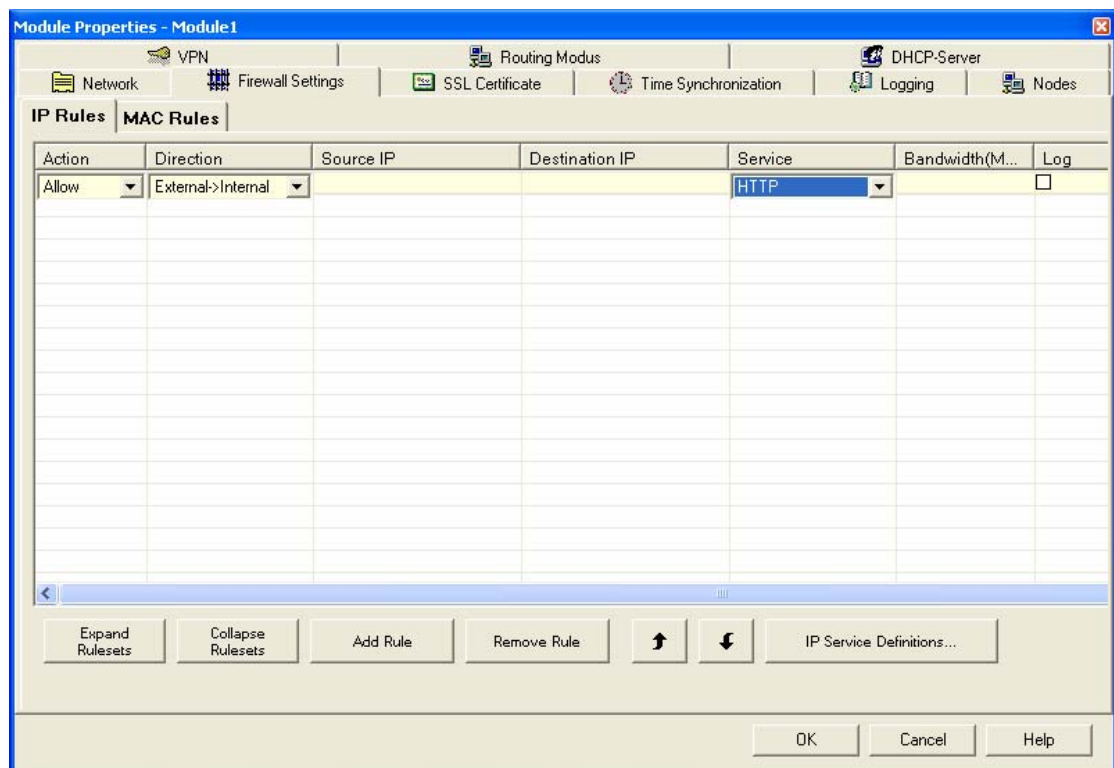
3	打开 SCALANCE S 标准属性的对话框选择 Firewall setting 栏，使能 Allow configuration of nodes via DCP。点击 OK 按钮结束。 
4	选择高级模式，具体方式参考 DHCP 项目的 3 和 4。点选 Firewall settings 栏。点击 IP Service Definitions...按钮。在 TCP 服务中，点击按钮 Add IP Service 增加一个 IP 服务 Service0，修改名字为 HTTP，目的端口号设置为 80。该端口号是 HTTP 服务的端口号。然后点击 OK 结束。



The dialog box titled "IP Service Definitions" has tabs for "IP Services", "ICMP", "Service Groups", and "Group Management". The "IP Services" tab is active, showing a table with columns: Name, Protocol, Source Port, and Target Port. The first row is highlighted in yellow and contains "HTTP", "tcp", "*", and "80". Below the table are buttons for "Add IP Service" and "Remove IP Service". At the bottom are "OK", "Cancel", and "Help" buttons.

Name	Protocol	Source Port	Target Port
HTTP	tcp	*	80

- 5 在 Firewall settings 高级属性对话框中，点击 Add Rule 按钮，增加一个安全规则，动作为允许 Allow，方向为外部到内部 External->Internal，服务为 HTTP。也可以根据需要设置源 IP 和目的 IP，这里为默认。点击 OK 按钮结束。

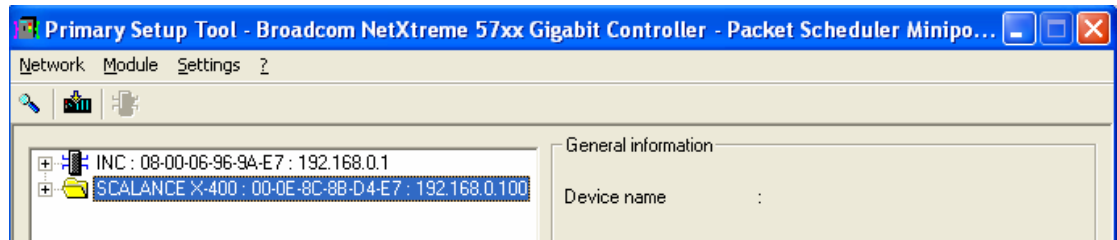


The dialog box titled "Module Properties - Module1" has tabs for "VPN", "Firewall Settings", "Routing Modus", "SSL Certificate", "Time Synchronization", "DHCP-Server", "Logging", and "Nodes". The "Firewall Settings" tab is active, showing "IP Rules" and "MAC Rules" sub-tabs. The "IP Rules" sub-tab is active, showing a table with columns: Action, Direction, Source IP, Destination IP, Service, Bandwidth(M...), and Log. The first row is highlighted in yellow and contains "Allow", "External->Internal", empty fields, "HTTP", empty fields, and an unchecked "Log" checkbox. Below the table are buttons for "Expand Rulesets", "Collapse Rulesets", "Add Rule", "Remove Rule", up/down arrows, and "IP Service Definitions...". At the bottom are "OK", "Cancel", and "Help" buttons.

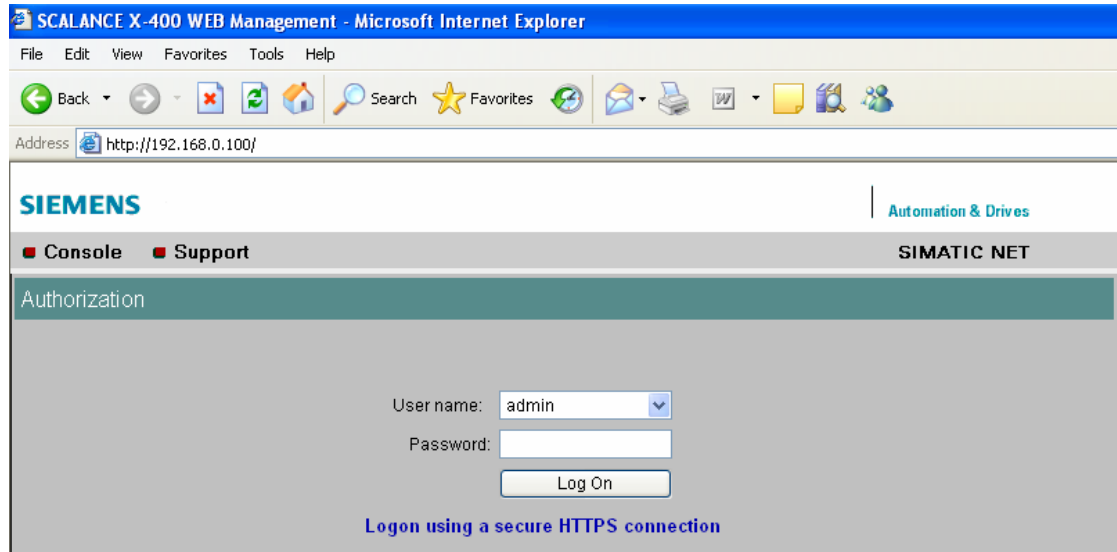
Action	Direction	Source IP	Destination IP	Service	Bandwidth(M...)	Log
Allow	External->Internal			HTTP		☐

- 6 保存和下载默认项目，参考 DHCP 项目的步骤 6。在 Host1 中打开 PST 工具浏览网络。可

以看见 SCALANCE X414-3E。



通过 IE 浏览器可以打开 192.168.0.100 的 Web 页面。



第五章 虚拟专用网络

5.1 VPN 概述

VPN即虚拟专用网 (Virtual Private Network)，是一条穿过混乱的公用网络（非安全的网络）的安全、受保护的、稳定的隧道。通过对网络数据的封包和加密传输，在一个公用网络（通常是因特网）建立一个临时的、安全的连接，从而实现在公网上传输私有数据、达到私有网络的安全级别。通常，VPN是对企业内部网的扩展，通过它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。而对于工业网络，VPN可以用安全机制来保障设备之间数据交换的机密型

（Confidentiality），真实可靠行（Authentication），完整性（Integrity）严格的访问控制。这样就建立了一个逻辑上虚拟的私有网络。VPN提供了一个经济有效的手段来解决通过公用网络安全的交换私有信息。

在建立VPN时，需要VPN Server和VPN Client，并且以成对的方式出现。例如，可以通过两个SCALANCE S建立VPN通道，也可以利用Softnet Security Client软件实现PC与SCALANCE S之间建立VPN通道。这样SCALANCE S的内网以及PC都是安全的网络。

VPN的隧道技术本质上是封装技术，所谓封装技术就是原始数据包通过某一层时，额外增加了包头，这样完成从一种协议的完整报文没有变化的生成另外一种协议的报文。

SCALANCE S使用IPSec协议的隧道模式实现VPN的隧道。IPSec是在发展IPv6时创建的，是IPv6的一部分。其工作在ISO/OSI的网络层，即第3层。IPSec协议把多种安全技术集合到一起，可以建立一个安全、可靠的隧道。IPSec是一种基于点到点的连接，实现安全联盟（SA Security Association）的连接。IPSec是在IP网络上保证安全通信的开放标准框架，IPSec实际上是一套协议包而不是单个的协议，它在IP层提供数据源验证、数据完整性和数据保密性。其中比较重要的有RFC2409 IKE（Internet Key Exchange）互连网密钥交换、RFC2402 AH（Authentication Header）验证包头、RFC2406 ESP (Encapsulating Security Payload 封装安全载荷) 加密数据等协议。

IPSec通过AH和ESP这两个安全协议来实现数据源验证、数据完整性和数据保密性的目标，并且还可以通过IKE为IPSec提供了自动协商交换密钥、建立和维护安全联盟SA的服务，以简化IPSec的使用和管理。AH是包头验证协议，主要提供的功能有数据源验证、数据完整性校验和防报文重放功能；然而，AH并不加密所保护的数据报。ESP是封装安全载荷协议，它除提供AH协议的所有功能之外（但其数据完整性校验不包括IP头），还可提供对IP报文的加密功能。AH和ESP可以单独使用，也可以同时使用。对于AH和ESP，都有两种操作模式：传输模式和隧道模式。SCALANCE S应用VPN安全策略时仅使用ESP安全协议。

IKE使用了两个阶段为IPSec进行密钥协商并建立安全联盟：第一阶段，通信各方彼此间建立了一个已通过身份验证和安全保护的通道，此阶段的交换建立了一个安全联盟，称为IKE

SA；第二阶段，用第一阶段所建立的安全通道为IPSec协商安全服务，即为IPsec协商具体的安全联盟，建立IPSec SA，而IPSec SA用于最终的IP数据安全传送。

IPSec SA可以通过手工配置的方式建立，但是当网络中节点增多时，手工配置将非常困难，而且难以保证安全性。这时就要使用IKE自动地进行安全联盟建立与密钥交换的过程。IKE协议为IPSec提供了自动协商交换密钥、建立安全联盟的服务，以简化IPSec的使用和管理。IKE具有一套自保护机制，可以在不安全的网络上安全地分发密钥、验证身份、建立IKE安全联盟。

DH（Diffie-Hellman）交换及密钥分发。Diffie-Hellman算法是一种公共密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。完善的前向安全性（Perfect Forward Secrecy, PFS）。PFS是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。PFS是由DH算法保障的。

身份验证。身份验证确认通信双方的身份。对于pre-shared key验证方法，验证字用来作为一个输入产生密钥，验证字不同是不可能在双方产生相同的密钥的。验证字是验证双方身份的关键。

身份保护。身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

在RFC2409中规定，IKE第一阶段的协商可以采用两种模式：主模式（main mode）和野蛮模式（aggressive mode）。两者的主要区别在于野蛮模式不提供身份保护。SCALANCE S可以使用IKE自动协商建立IKE SA。并可以根据需要的网络环境选择主模式或野蛮模式。

安全联盟是IPSec的基础，也是IPSec的本质。SA是通信对方对某些要素的约定，例如，使用哪种协议（AH、ESP还是两者结合使用）、协议的操作模式（传输模式和隧道模式）、加密算法（DES和3DES）、特定流中保护数据的共享密钥以及密钥的生存周期等。

IPSec SA安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。安全联盟具有生存周期。生存周期的计算包括两种方式：以时间为限制，每隔指定长度的时间就进行更新；以流量为限制，每传输指定的数据量（字节）就进行更新。SCALANCE S使用时间或者流量来更新IPSec SA。

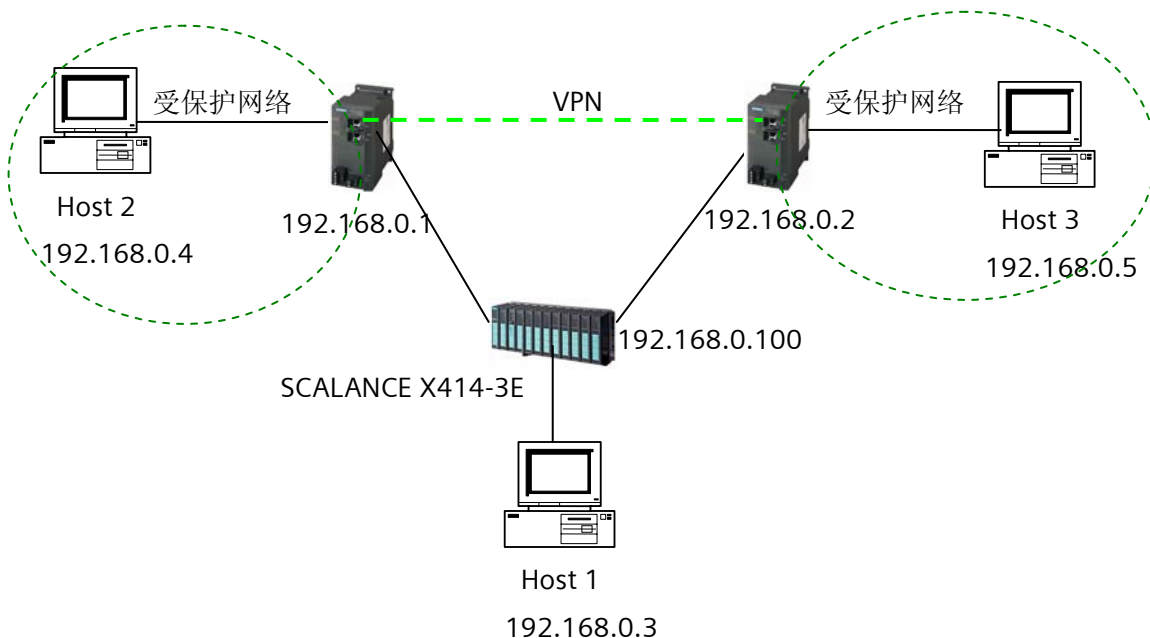
AH和ESP都能够对IP报文的完整性进行验证，以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过杂凑函数，杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec 对方计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。一般来说IPSec使用两种验证算法：MD5（Message Digest Version 5）通过输入任意长度的消息，产生128bit的消息摘要。SHA-1通过输入长度小于2的

64次方比特的消息，产生160bit的消息摘要。SHA-1（Secure Hash Algorithm 1）的摘要长于MD5，因而是更安全的。在IPSec SA阶段，SCALANCE S可以设置MD5或者SHA-1。

ESP能够对IP报文内容进行加密保护，防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。一般来说IPSec使用两种加密算法：DES（Data encryption standard）使用56bit的密钥对一个64bit的明文块进行加密。3DES（Special triple DES）使用三个56bit的DES密钥（共168bit密钥）对明文进行加密。3DES具有更高的安全性，但其加密数据的速度要比DES慢得多。在IPSec SA阶段，SCALANCE S除了可以使用DES或3DES进行数据加密，还可使用AES（Advanced Encrypting Standard）的方法进行加密。

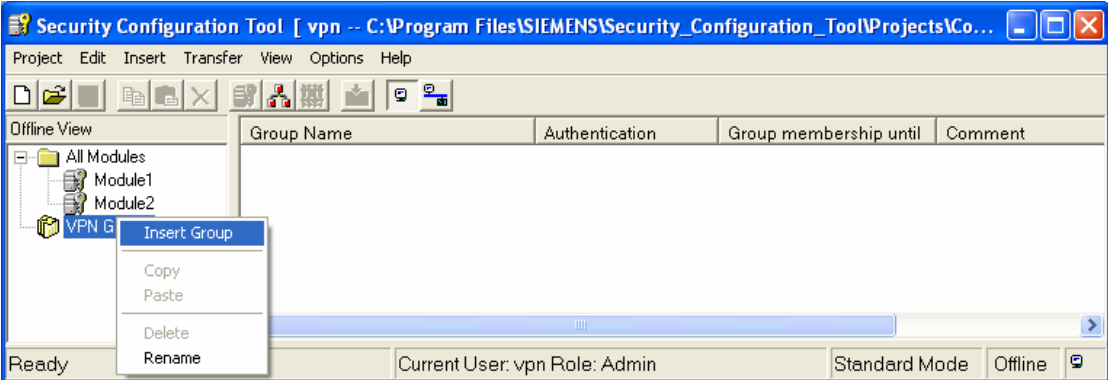
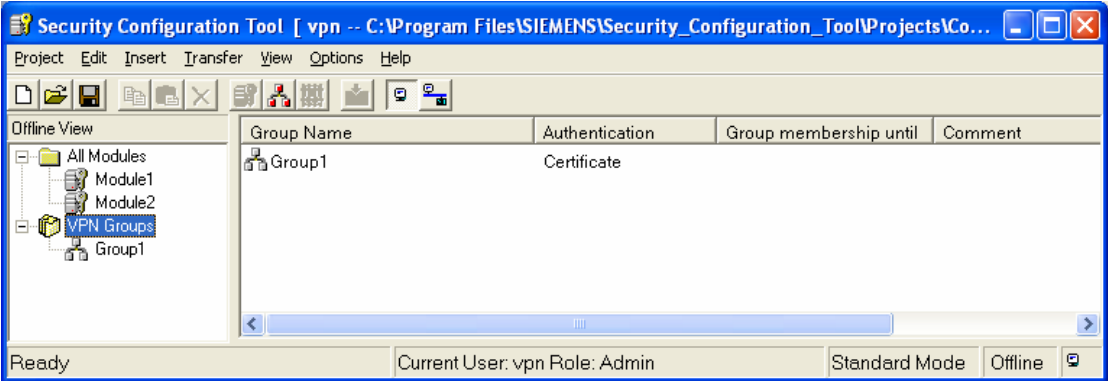
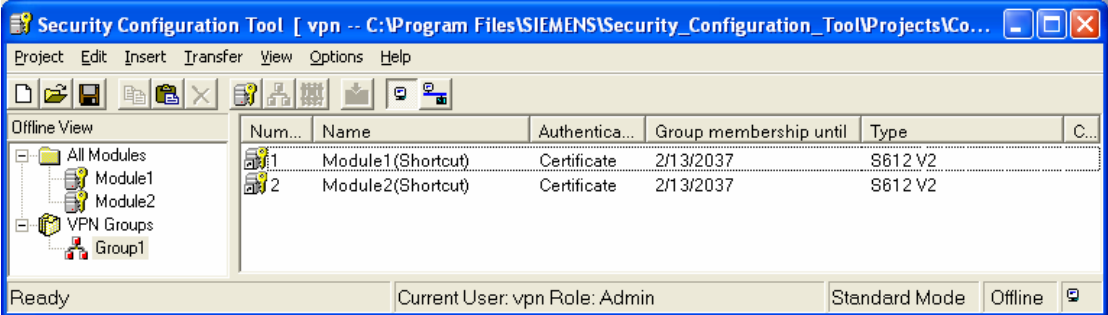
5.2 VPN 组态

VPN 网络组态图：

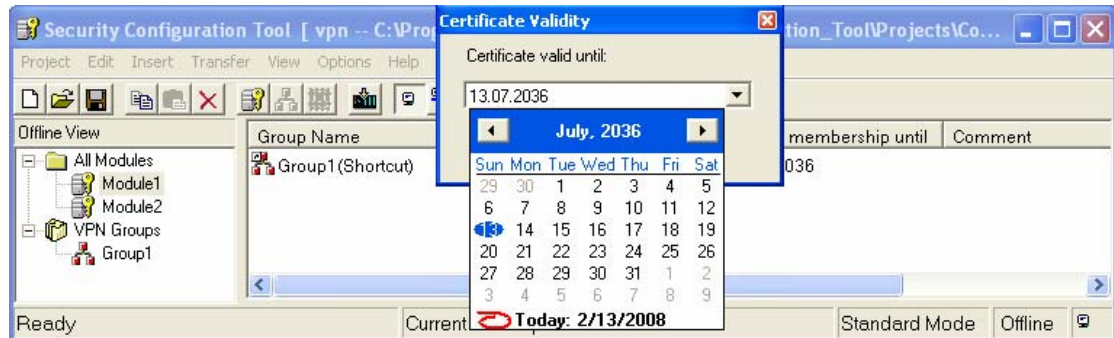


Host1 与交换机 SCALANCE X414-3E 相连，2 个 SCALANCE S 的外部网络端口 1 分别与 SCALANCE X414-3E 相连。2 个 SCALANCE S 的内部网络端口分别与主机 Host2 和 Host3 相连。

序号	组态步骤
1	新建项目用户名和密码均为 vpn，具体组态参考 DHCP 组态步骤。在项目中加入两个安全模块 S612 V2。根据网络组态图设置 IP 地址，子网掩码并相应添加 SCALANCE S 的 MAC 地址。

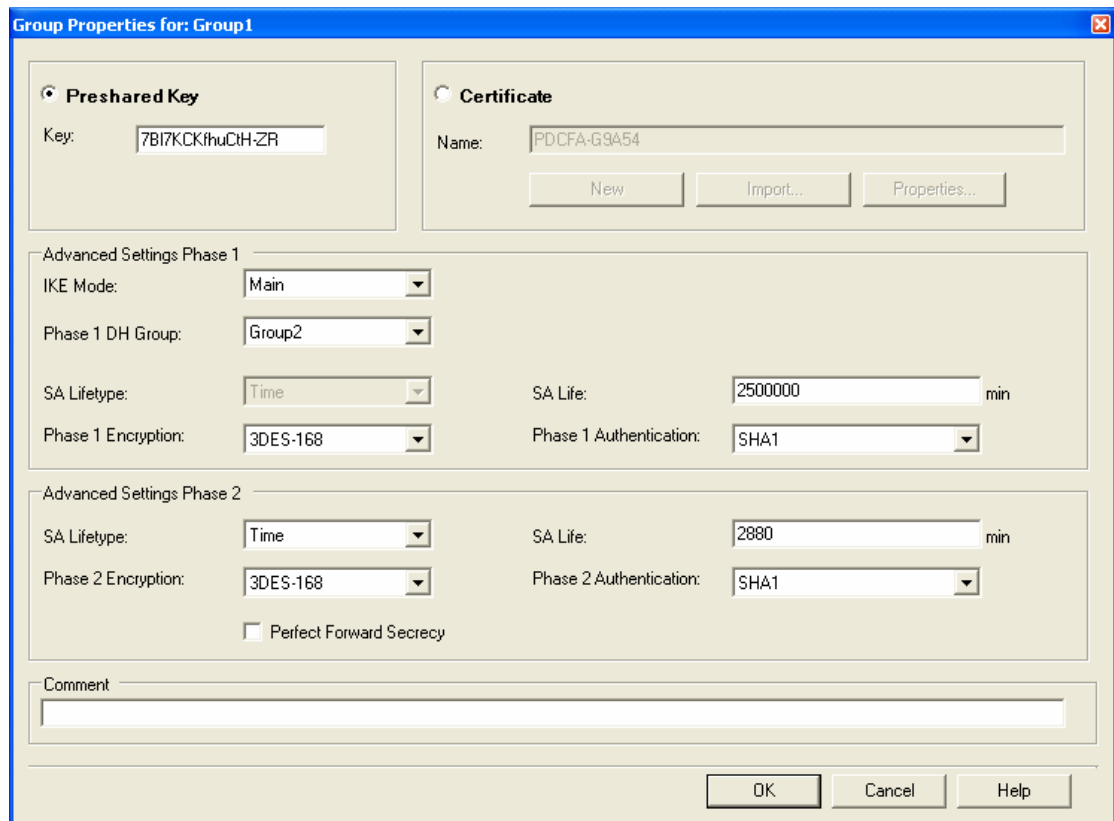
- 2
- 在左侧栏内，右键点击 VPN Groups，插入一个新组。或点击工具栏按钮 。
- 
- 默认为 Group1。
- 
- 3
- 然后在左侧栏内，用鼠标托拽 Module1 和 Module2 到新建的 VPN Group1 中。这时安全模块的图标钥匙的颜色变为黄色和 Group1 的图标颜色变为红色。在标准模式下，可以看到默认的身份验证方式使用的是证书验证方式，有效期至 2037 年的 2 月 13 日。
- 
- 也可以根据需要修改其中的安全模块的有效期时间。例如，双击 Module1 的右侧栏内

Group1 图标。下拉菜单中修改有效期时间。

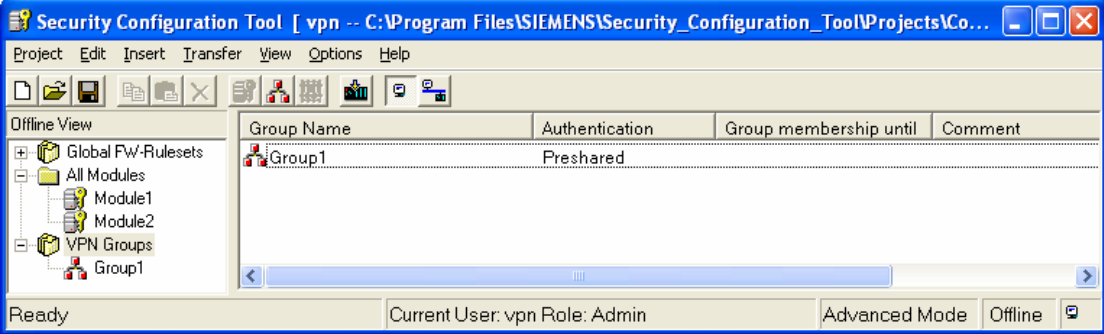
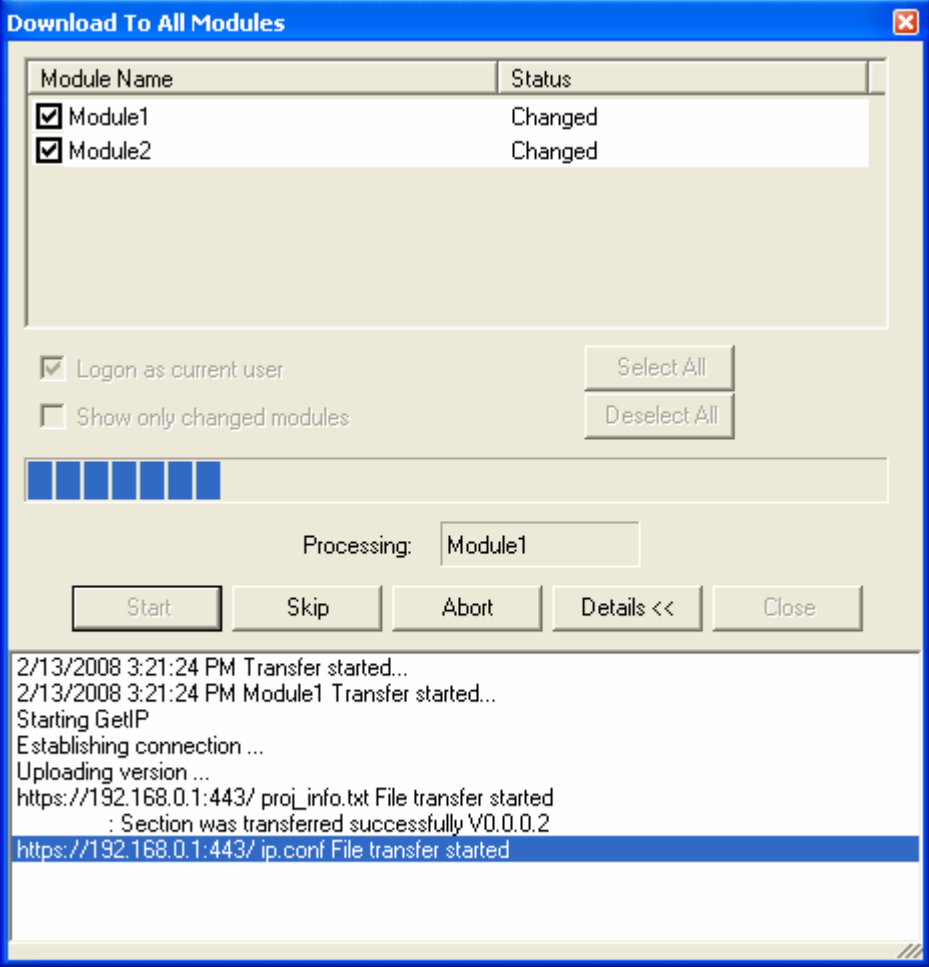
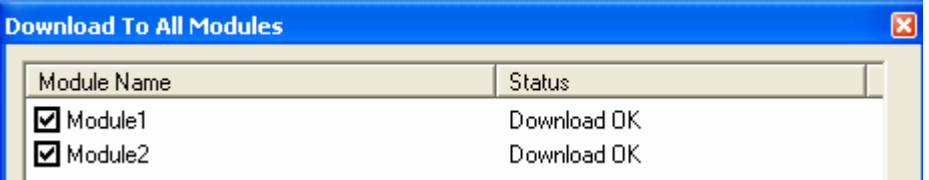


4

电子证书的验证方式非常安全，也可以使用预制共享密钥验证。选择 View 菜单下的 Advanced Mode。双击 VPN Groups 下的右侧栏的 Goup1 图标，弹出 Group 属性。选择预制共享密钥验证。对于 IKE SA 和 IPSec SA 可以根据需要进行修改，这里使用默认的设置。

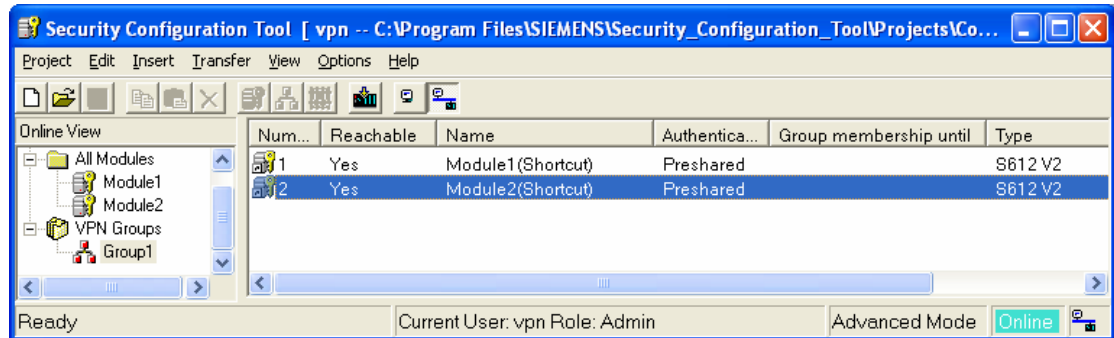


这时，项目 VPN 的安全联盟的验证方式通过 Preshared Key 的方式。

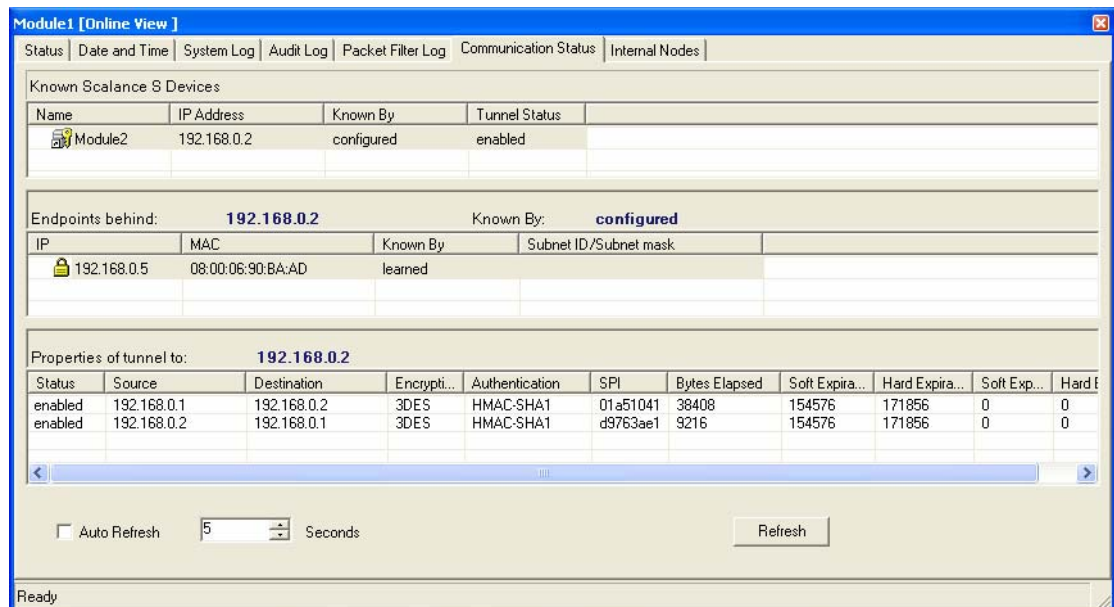
	
5	在 Transfer 菜单中，选择 to All modules 选项。下载项目。  注意下载状态。 
6	使用 Ping 测试，利用 Host1 去 Ping 其它主机 host2 或 3，结果 Ping 不通。 而主机 host2 和 3 之间可以相互 Ping 通。

7

点击工具栏按钮 ，在线观察模块 Module1 和 Module2。注意组态的状态栏的信息。



双击右侧栏的 Module1 图标。可以查看 module1 的状态信息、时间日期、系统日志、追述日志、包过滤日志、通讯状态、内部节点。Module1 的通讯状态信息。



Module2 的通讯状态信息。

Module2 [Online View]

Status | Date and Time | System Log | Audit Log | Packet Filter Log | Communication Status | Internal Nodes |

Known Scalance S Devices

Name	IP Address	Known By	Tunnel Status
Module1	192.168.0.1	configured	enabled

Endpoints behind: **192.168.0.1** Known By: **configured**

IP	MAC	Known By	Subnet ID/Subnet mask
192.168.0.4	00:11:25:85:AA:40	learned	

Properties of tunnel to: **192.168.0.1**

Status	Source	Destination	Encryption	Authenti...	SPI	Bytes Elapsed	Soft Expira...	Hard Expira...	Soft Exp...	Hard f
enabled	192.168.0.1	192.168.0.2	3DES	HMAC...	01a51041	43712	154162	171442	0	0
enabled	192.168.0.2	192.168.0.1	3DES	HMAC...	d9763ae1	10022	154162	171442	0	0

☐ Auto Refresh 5 Seconds Refresh

Ready

第六章 路由

6.1 路由概述

路由器的主要作用是连通不同网段的 IP 网络，另外可以选择信息传送的线路。选择通畅快捷的近路，能大大提高通信速度，减轻网络系统通信负荷，节约网络系统资源，提高网络系统畅通率，从而让网络系统发挥出更大的效益来。

从过滤网络流量的角度来看，路由器的作用与交换机非常相似。但是与工作在网络第二层的交换机不同，路由器使用专门的软件协议从逻辑上对整个网络进行划分。例如，一台支持 IP 协议的路由器可以把网络划分成多个子网段，只有指向特殊 IP 地址的网络流量才可以通过路由器。对于每一个接收到的数据包，路由器都会重新计算其校验值，并写入新的物理地址。因此，使用路由器转发和过滤数据的速度往往要比只查看数据包物理地址的交换机慢。但是，对于那些结构复杂的网络，使用路由器可以提高网络的整体效率。另外，网络中会存在广播数据，而大量的广播会消耗网络带宽，无谓的占用了网络资源，使网络的传输效率降低。路由器可以自动过滤网络广播，是路由器的另外一个优点。

从总体上说，在网络中添加路由器的整个安装过程要比即插即用的交换机复杂很多。一般说来，异构网络互联与多个子网互联都应采用路由器来完成。路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表（Route Table），供路由选择时使用。

路由表可以是由系统管理员固定设置好的，也可以由系统动态修改。由系统管理员事先设置好固定的路由表称之为静态（static）路由表，一般是在系统安装时就根据网络的配置情况预先设定的，它不会随未来网络结构的改变而改变。动态（Dynamic）路由表是路由器根据网络系统的运行情况而自动调整的路由表。路由器根据路由选择协议（Routing Protocol）提供的功能，自动学习和记忆网络运行情况，在需要时自动计算数据传输的最佳路径。

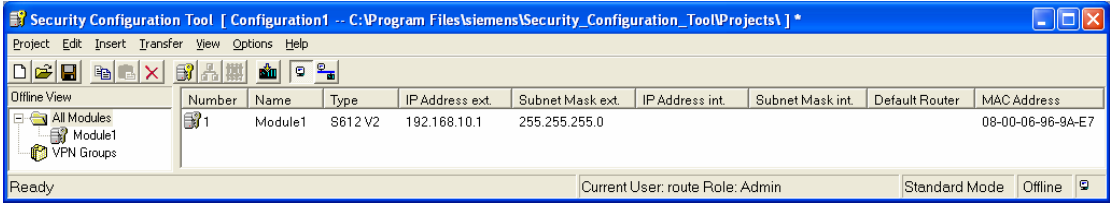
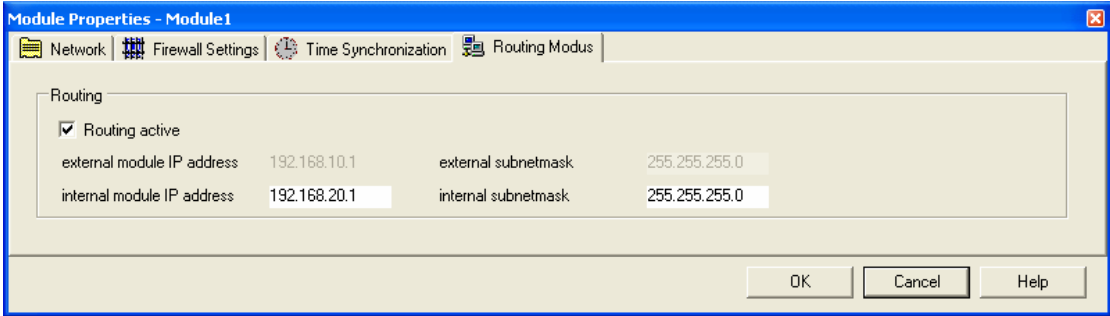
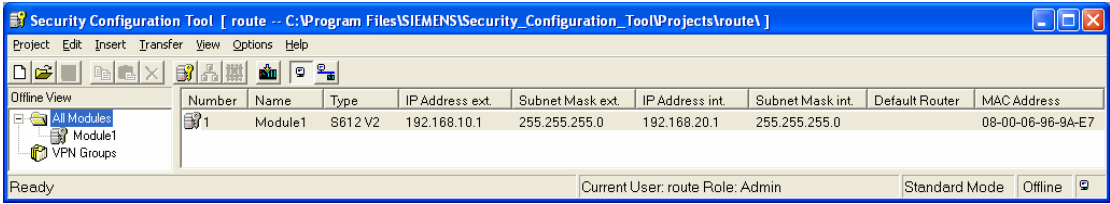
SCALANCE S 提供基本的路由功能，需要人为的手动添加来完成。SCALANCE S 由于具有防火墙功能，需要在路由组态是组态过滤策略，这样才能实现设备之间的相互通讯。

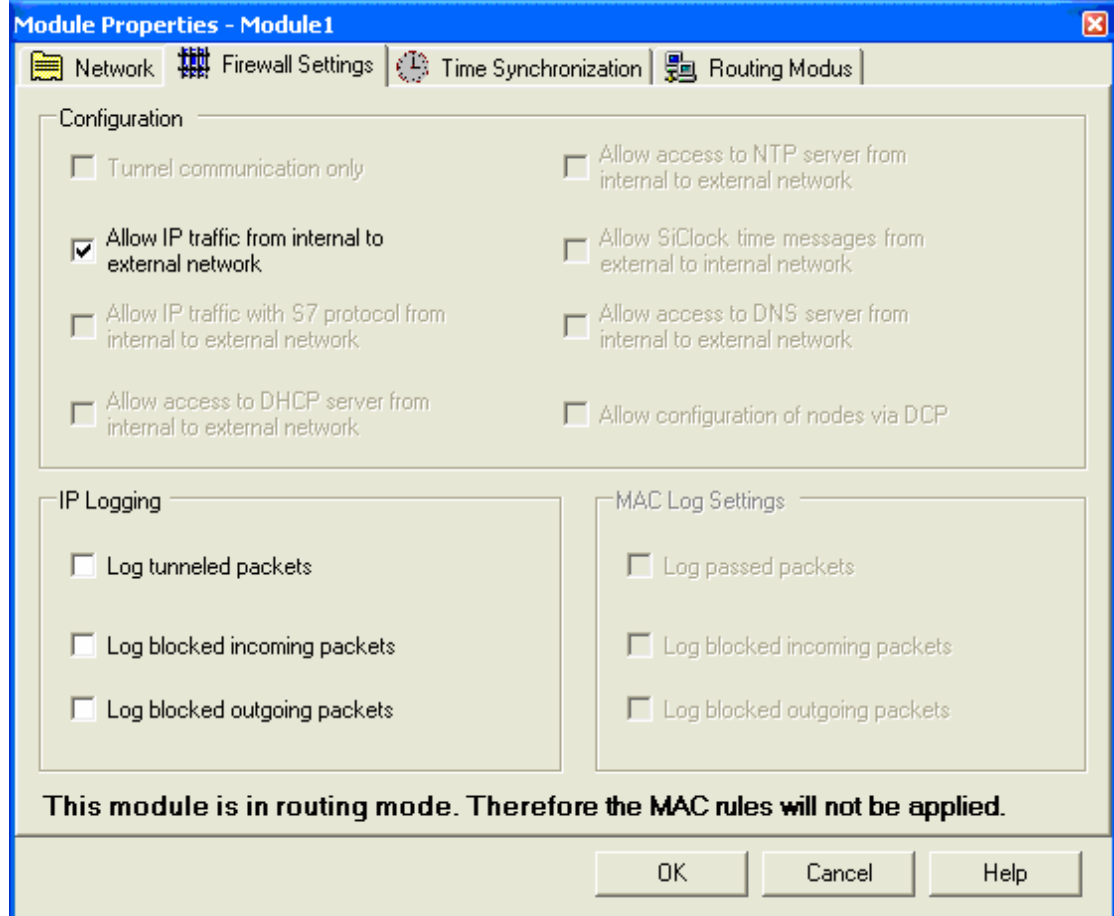
6.2 路由组态

路由网络组态图：

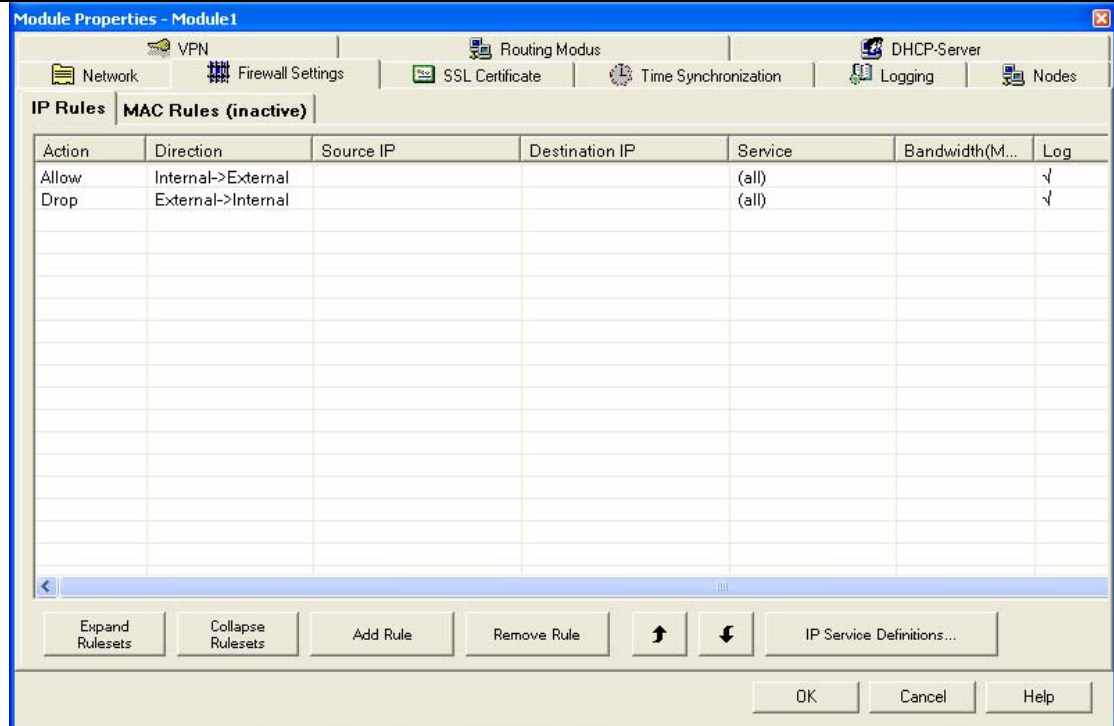


主机 Host2 与 SCALANCE S 端口 1 相连，主机 Host3 与 SCALANCE S 端口 2 相连。Host2 位于子网 2 中，该网段的 IP 网关为 192.168.10.1/24，Host3 位于子网 3 中，该网段 IP 网关为 192.168.20.1/24。具体 IP 地址参考网络组态图。

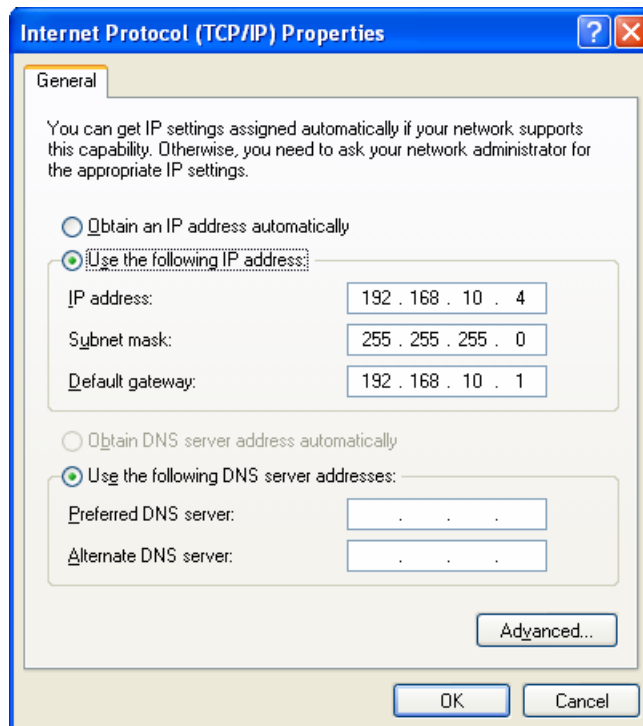
序号	组态步骤
1	新建项目用户名和密码均为 Route，具体组态参考 DHCP 组态步骤。在项目中加入 1 个安全模块 S612 V2。根据网络组态图设置 IP 地址，子网掩码并相应添加 SCALANCE S 的 MAC 地址。 
2	双击右侧栏 Module1 的图标，弹出标准模式的模块属性对话框。选择 Routing Modus，使能 Routing active，增加内部网络的 IP 网关为 192.168.20.1/24。  点击 OK 按钮结束，并保存项目。 
3	在路由模式下，需要开启防火墙规则。双击右侧栏 Module1 的图标，弹出标准模式的模块属性对话框。选择 Firewall settings，使能 Allow IP traffic from internal to external network。这样允许内部网络访问外部网络，以保护内网。点击 OK 按钮结束设置。保存项目并下载。



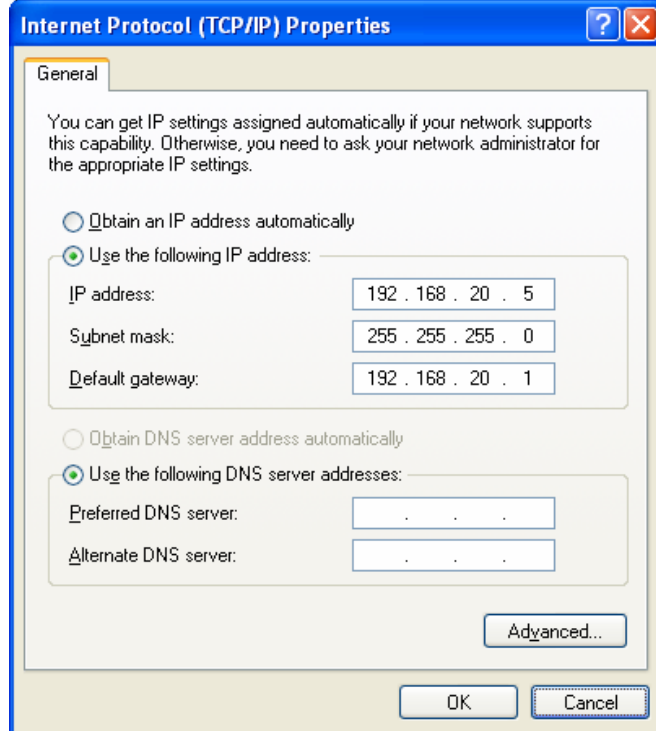
另外也可以根据特殊需要，比如需要观察包过滤机制。这时可以设置防火墙规则的高级模式。在高级模式中使能 Log 日志功能。



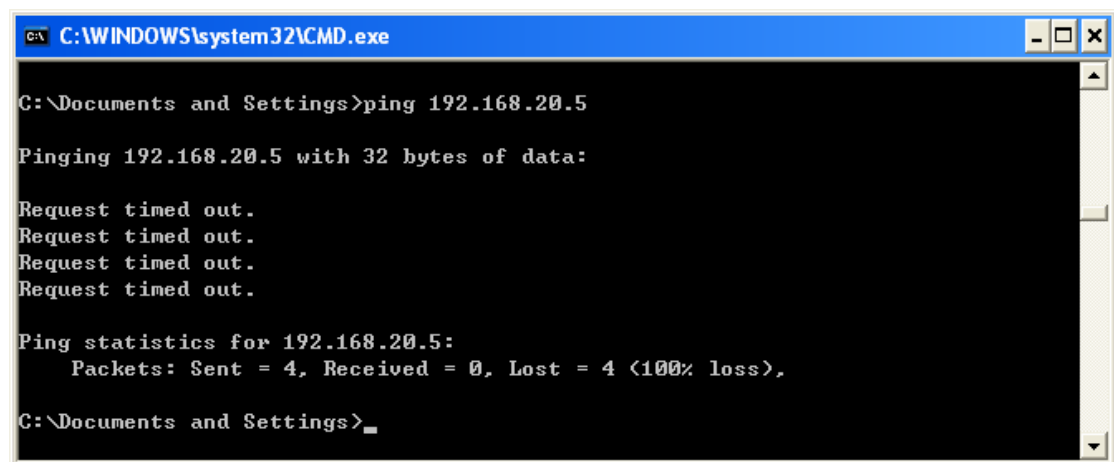
4 给 PC 主机 Host2 设置 IP 和网关。



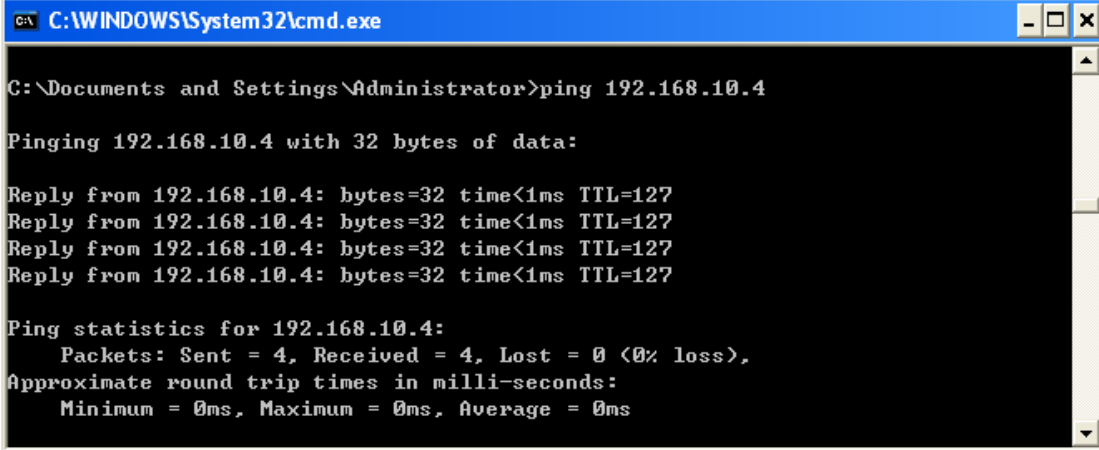
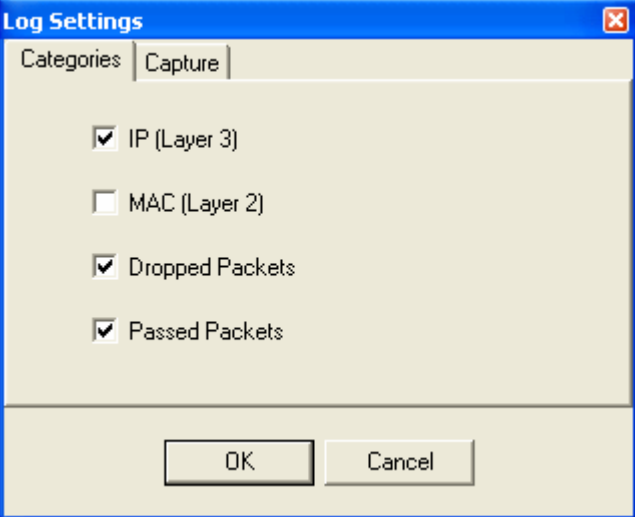
给 PC 主机 Host3 设置 IP 和网关。



- 5 使用 Ping 功能测试路由功能。Host2 使用 Ping 到 Host3。测试结果不通。



Host3 使用 Ping 到 Host2。测试结果通。实现内网到外网的路由功能。

	 <pre> C:\WINDOWS\System32\cmd.exe C:\Documents and Settings\Administrator>ping 192.168.10.4 Pinging 192.168.10.4 with 32 bytes of data: Reply from 192.168.10.4: bytes=32 time<1ms TTL=127 Reply from 192.168.10.4: bytes=32 time<1ms TTL=127 Reply from 192.168.10.4: bytes=32 time<1ms TTL=127 Reply from 192.168.10.4: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.10.4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
6	点击工具栏按钮 ，双击右侧栏的 Module1 图标。可以查看 module1 的包过滤日志信息。点击 Start reading 按钮，弹出 Log Settings 对话框，点选 IP、Dropped Packets 和 Passed Packets 3 个选项。  观察包的过滤信息。

Module1 [Online View]

Status | Date and Time | System Log | Audit Log | Packet Filter Log | Communication Status | Internal Nodes

PacketFilter

No.	Date	Time	Source	Destination	Protocol	Interface	Action	Direction	Notes
✖ 176	2/14/2008	1:24:58 PM.84	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: Typ
✖ 177	2/14/2008	1:24:58 PM.84	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: Typ
✖ 178	2/14/2008	1:24:59 PM.84	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: Typ
✖ 179	2/14/2008	1:24:59 PM.84	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: Typ
✖ 180	2/14/2008	1:25:00 PM.77	192.168.10.04	192.168.20.06	Icmp	Ext	Dropped	In	ICMP: Typ
✖ 181	2/14/2008	1:25:00 PM.84	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: Typ
✖ 182	2/14/2008	1:25:00 PM.84	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: Typ
✖ 183	2/14/2008	1:25:01 PM.85	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: Typ
✖ 184	2/14/2008	1:25:01 PM.85	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: Typ
✖ 185	2/14/2008	1:25:02 PM.85	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: Typ
✖ 186	2/14/2008	1:25:02 PM.85	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: Typ
✖ 187	2/14/2008	1:25:03 PM.85	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: Typ
✖ 188	2/14/2008	1:25:03 PM.85	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: Typ
✖ 189	2/14/2008	1:25:04 PM.85	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: Typ
✖ 190	2/14/2008	1:25:04 PM.85	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: Typ
✖ 191	2/14/2008	1:25:05 PM.85	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: Typ
✖ 192	2/14/2008	1:25:05 PM.85	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: Typ
✖ 193	2/14/2008	1:25:06 PM.85	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: Typ
✖ 194	2/14/2008	1:25:06 PM.85	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: Typ

Clear

Buffer Settings: Ring Buffer

Open...

Stop Reading

Stop Logging

Ready

第七章 NAT/NAPT

7.1 NAT/NAPT 概述

随着 Internet 的迅速发展, IP 地址短缺已成为一个十分突出的问题。已经有很多方法来减轻 IP 地址扩展问题的方案。比如,使用私有地址(在 RFC1918 中定义),变长子网掩码(VLSM, Variable-length subnet mask),无类域间路由(CIDR, Classless inter-domain routing),地址转换(NAT 和 PAT),动态地址池(如 DHCP)及 IPv6。但最根本的解决 IP 地址不足的问题的方法还是尽快实现 IPv6。

为了减少公有 IP 地址的浪费,一种解决方法是在广域网链路上使用私有地址。但是,在广域网链路上使用私有地址的一个条件就是在这些链路上使用的私有地址不能是去往因特网的通信的起始源,或是来自因特网的通信的最终目的。为满足这一条件 NAT 技术应运而生。

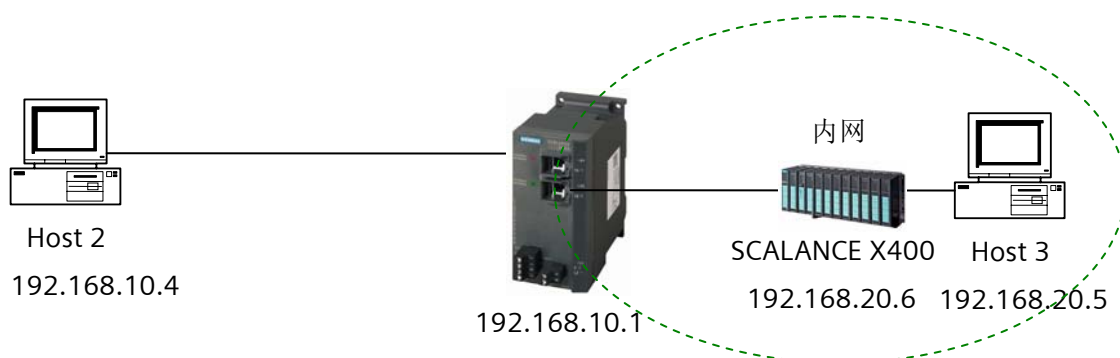
NAT (Network Address Translation) 的功能,就是指在一个网络内部,根据需要可以随意自定义 IP 地址,而不需要经过申请。在网络内部,各计算机间通过内部的 IP 地址进行通讯,而当内部的计算机要与外部 Internet 网络进行通讯时,具有 NAT 功能的设备(比如路由器)负责将其内部的 IP 地址替换(Translation)为合法的 IP 地址(即经过申请的 IP 地址)进行通信。

NAPT (Network Address Port Transition) 的功能是与 NAT 的概念是相当接近的,也就是端口地址解析。与 NAT 技术的不同,数据是内部网络主机的 IP 地址和端口号在通过路由器时被替换修改为(Translation)外部网络的 IP 地址和端口号。

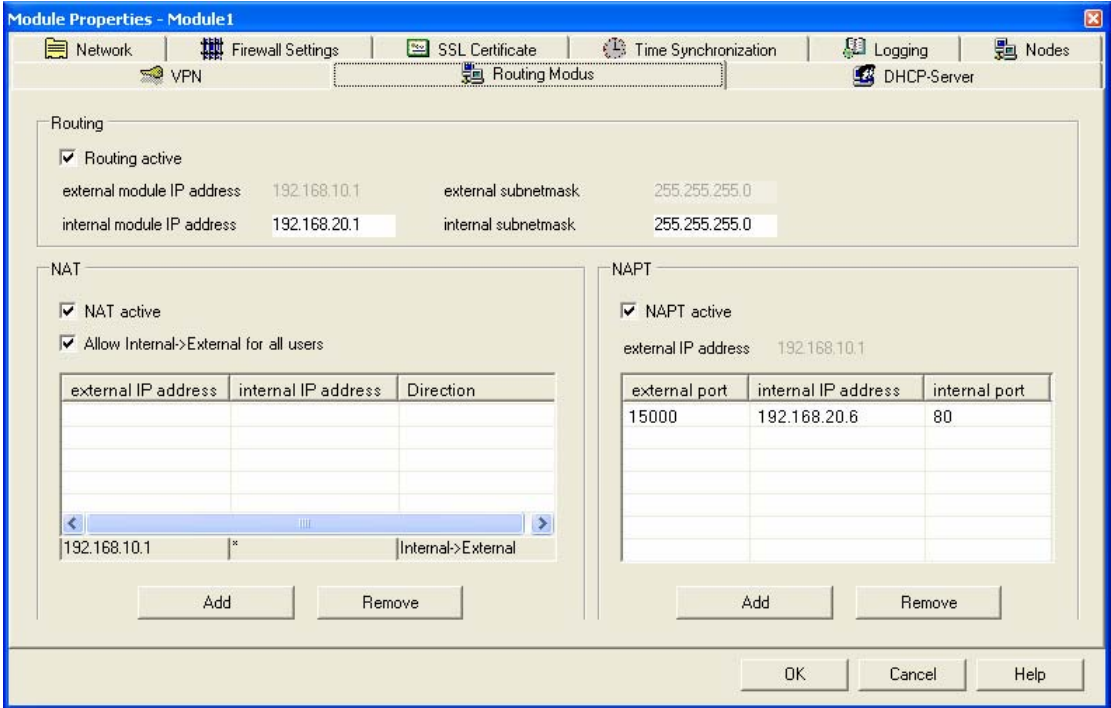
SCALANCE S 支持 NAT 和 NAPT 功能,这样可以对于 SCALANCE S 所连接的内网设备进行保护(内部网络)。另外,对于很多重复的网络且其内部带有相同 IP 的设备,使用 NAT 的方法进行访问是非常有效的。另外,由于 SCALANCE S 同时又具有防火墙功能,这样在实现了 NAT/NAPT 后,数据才会经过防火墙,所以需要在路由组态后,组态正确的过滤策略,这样才能实现设备之间的相互通讯。

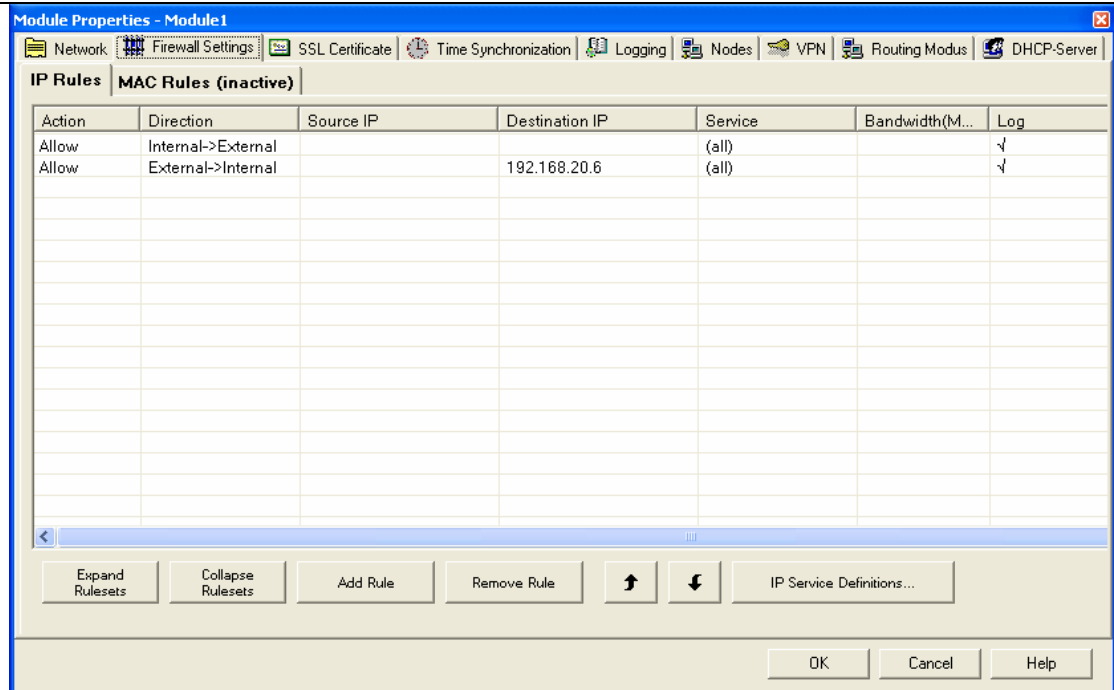
7.2 NAT/NAPT 组态

NAT/NAPT 网络组态:

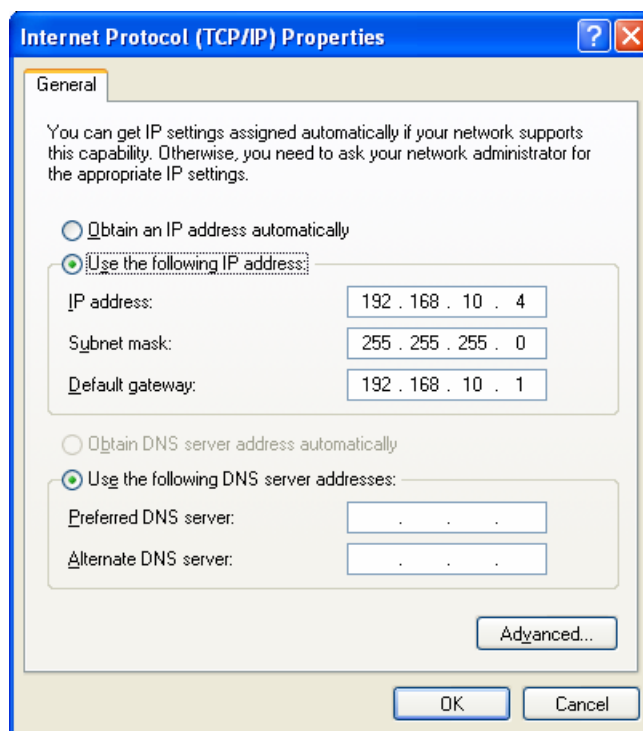


主机 Host2 与 SCALANCE S 端口 1 相连，主机 Host3 与交换机 SCALANCE X400 相连，交换机 SCALANCE X400 与 SCALANCE S 的端口 2 相连。Host2 位于外网 2 中，该网段的 IP 网关为 192.168.10.1/24，SCALANCE X-400 和 Host3 位于内网中，该网段 IP 网关为 192.168.20.1/24。具体 IP 地址参考网络组态图。

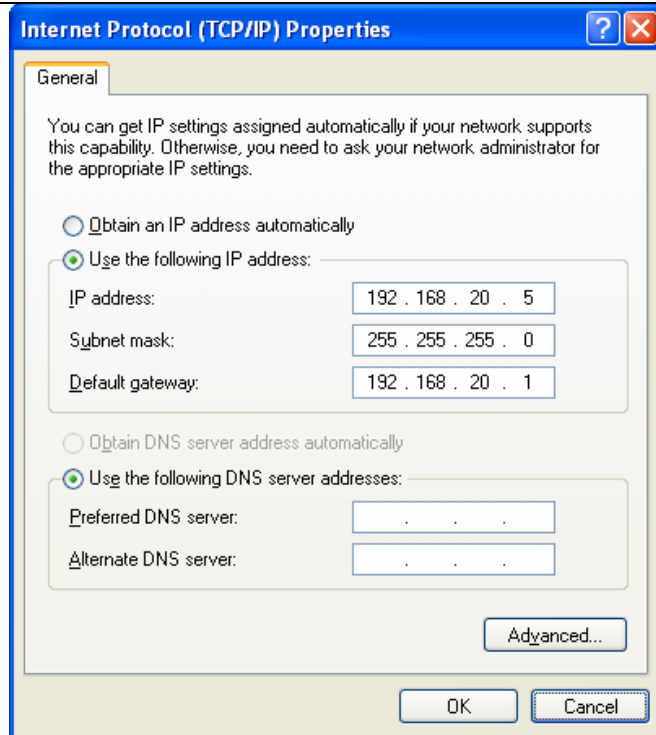
序号	组态步骤
1	新建项目用户名和密码均为 NAT，具体参考路由组态到步骤 3。点击 View 菜单，选择 Advanced mode。双击右侧栏 Module1 的图标，弹出高级模式的模块属性对话框。选择 Routing Modus 栏。使能 NAT active 和 Allow Internal->External for all users。这样所有内部设备可以给外部网络设备发送通讯请求。使能 NAPT active，给内网的设备 SCALANCE X-400 设置外部端口号 15000。注意需要配置在 8000 和 65535 之间的端口号。 
2	点击 Firewall Settings 栏，组态防火墙规则。这里可以指定该内网设备 SCALANCE X400 的 IP。并在 Log 栏激活日志功能。保存项目并下载。



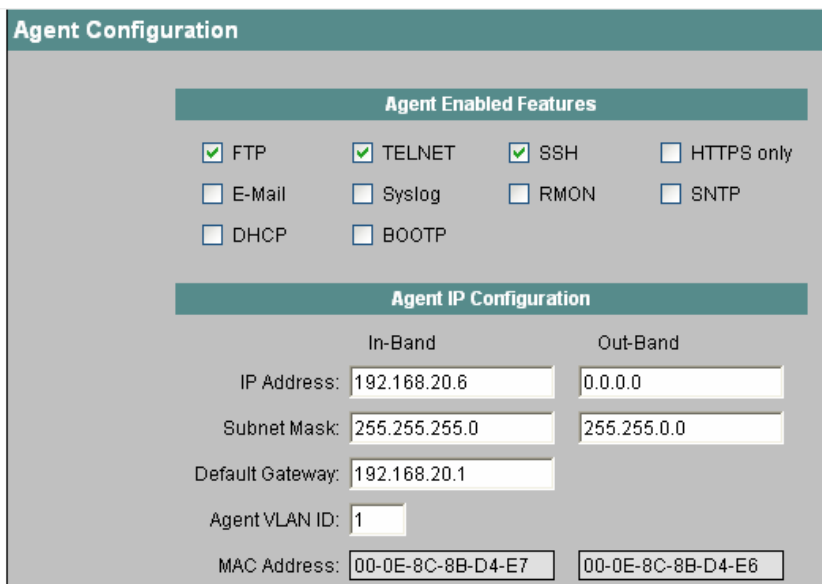
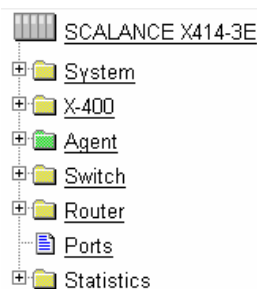
3 给 PC 主机 Host2 设置 IP 和网关。



给 PC 主机 Host3 设置 IP 和网关。



设置 SCALANCE X400 的 IP 地址和网关如下：



4 使用 Ping 功能测试 NAT 功能。Host2 使用 Ping 到 Host3。测试结果不通。

```
C:\WINDOWS\system32\CMD.exe

C:\Documents and Settings>ping 192.168.20.5

Pinging 192.168.20.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings>
```

Host3 使用 Ping 到 Host2。测试结果通。实现内网到外网的路由功能。

```
C:\WINDOWS\System32\cmd.exe

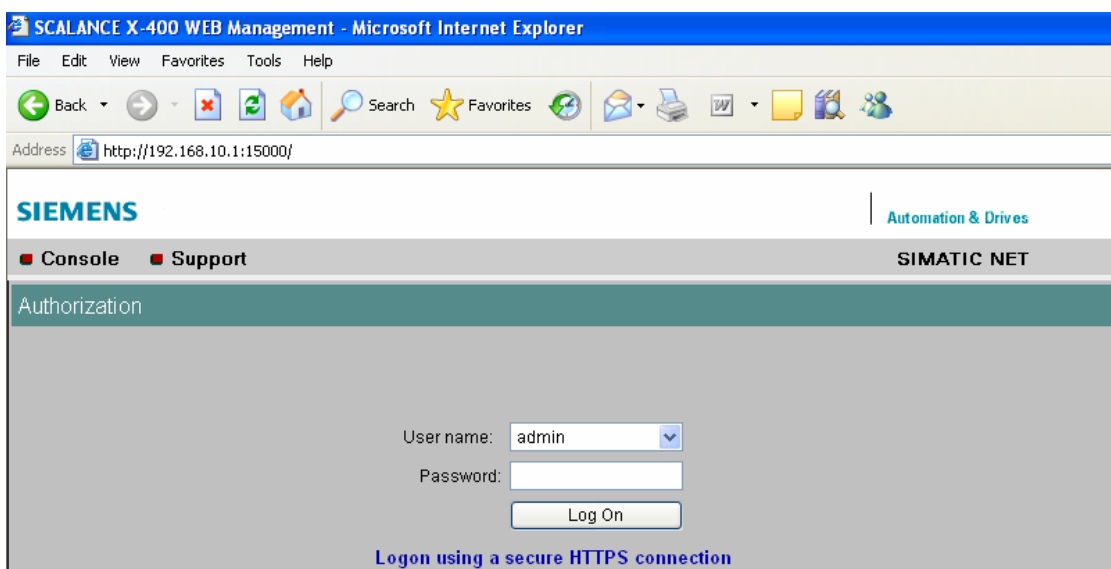
C:\Documents and Settings\Administrator>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

Reply from 192.168.10.4: bytes=32 time<1ms TTL=127
Reply from 192.168.10.4: bytes=32 time<1ms TTL=127
Reply from 192.168.10.4: bytes=32 time<1ms TTL=127
Reply from 192.168.10.4: bytes=32 time<1ms TTL=127

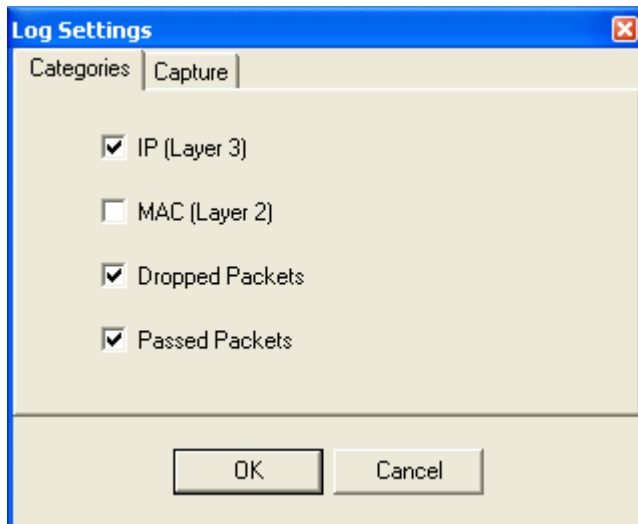
Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

5 测试NAPT功能，打开IE浏览器，在地址栏内输入//192.168.10.1:15000。回车。

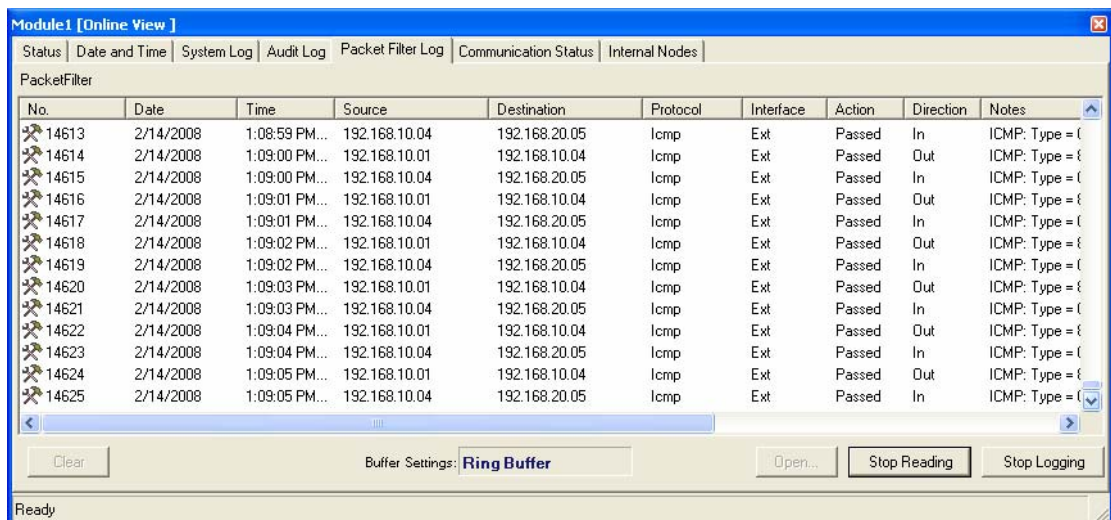


6

点击工具栏按钮 , 双击右侧栏的 Module1 图标。可以查看 module1 的包过滤日志信息。点击 Start reading 按钮, 弹出 Log Settings 对话框, 点选 IP、Dropped Packets 和 Passed Packets 3 个选项。



观察包的过滤信息。



附录一 推荐网址

NET

西门子（中国）有限公司

自动化与驱动集团 客户服务与支持中心

网站首页: <http://www.ad.siemens.com.cn/Service/>

专家推荐精品文档: <http://www.ad.siemens.com.cn/Service/recommend.asp>

Net常问问题: <http://support.automation.siemens.com/CN/view/zh/10805868/133000>

Net更新信息: <http://support.automation.siemens.com/CN/view/zh/10805868/133400>

“找答案”NET 版区:

<http://www.ad.siemens.com.cn/service/answer/category.asp?cid=1031>