第3章 VPN专用设备Site-to-Site的安全

3.1 构建站点到站点IPSec VPN(预共享密钥)

【实验名称】

构建站点到站点 IPSec VPN(预共享密钥)。

【实验目的】

学习配置站点到站点(Site-to-Site)的 IPSec VPN 隧道,加深对 IPSec 的理解。

【背景描述】

北京的某公司在上海设立分公司,分公司要远程访问总公司内网中的各种网络资源,例如,CRM 系统、FTP 服务器等。由于在 Internet 上传输数据本身存在安全隐患,公司希望通过 IPSec VPN 技术实现数据的安全传输。

【需求分析】

需求:解决上海分公司和北京总公司之间通过 Internet 进行数据传输的安全问题。

分析:IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等有效地保证了数据在 Internet 传输的安全性,是目前最安全、使用最广泛的 VPN 技术。通过建立 IPSec VPN 的加密隧道,实现分公司和总公司之间的安全的数据传输。

【实验拓扑】

如图 3-1 所示网络拓扑,是某公司为解决上海分公司和北京总公司之间通过 Internet 进行数据传输的安全问题。分公司要远程访问总公司内网中的各种网络资源,需要在 Internet 上传输数据,公司希望通过配置站点到站点(Site-to-Site)的 IPSec VPN 隧道技术,实现数据在 Internet 上的安全传输。

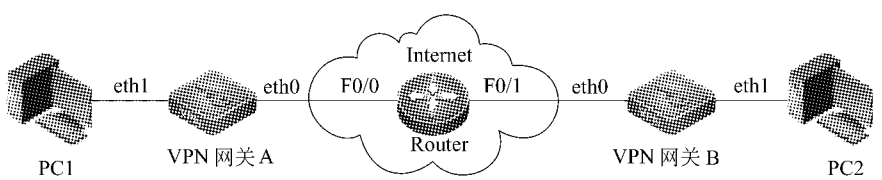

图 3-1 构建站点到站点 IPSec VPN

【实验设备】

RG-WALL VPN 网关：2 台；PC：2 台；路由器：1 台。

【预备知识】

IKE 工作原理

IPSec 协议是基于 IP 网络(包括 Intranet、Extranet 和 Internet)，由 IETF 正式定制的开放的 IP 安全标准，IPSec 提供三种不同的形式保护通过公有或私有 IP 网络传送数据的安全性。

- 认证：作用是确定所接收的数据与所发送数据的一致性，同时确定申请发送者在实际发送中的真实身份。
- 数据完整：作用是保证数据从源发地到目的地的传送过程中，没有任何不可检测的数据丢失与改变。
- 机密性：作用是使相应的接收者能获取发送的真正内容，无意获取数据的接收者无法获知数据的真正内容。

IPSec 协议由三个基本要素来提供以上三种保护形式：认证协议头(AH)、安全加载封装(ESP)和互联网密匙管理协议(IKMP)。认证协议头和安全加载封装可以通过分开或组合使用来达到所希望的保护等级。认证协议头(AH)是在所有数据包头加入一个密码。安全加载封装(ESP)通过对数据包的全部数据和加载内容进行全加密来严格保证传输信息的机密性，这样可以避免其他用户通过监听来打开信息内容，保证只有受信任的用户拥有密匙才能打开内容。

IPSec 协议提供的安全服务，需要使用共享密钥来保证数据验证以及数据的机密性。如果采用人工增加密钥的方法，也可实现基本 IPSec 协议间的互通性，但其在使用上难以扩展。因此需要定义一种标准的方法，用以动态地验证 IPSec 参与各方的身份、协商安全服务以及生成共享密钥等，这种密钥管理协议称为“Internet 密钥交换”(Internet Key Exchange，IKE)。Internet 密钥交换协议是用于交换和管理在 VPN 中使用的加密密钥，协商 AH 和 ESP 协议所使用的密码算法，使用了 UPD 协议来交换密钥和其他安全信息，并将算法所需的密钥放在合适的位置。

IPSec 提供的安全服务，当应用环境规模较小时，可以用手工配置；当应用环境规模较大、参与的节点位置不固定时，IKE 可自动地为参与通信的实体协商，并对安全关联库维护，保障通信安全。

IKE 协议属于一种混合型协议，由 Internet 安全关联、密钥管理协议(ISAKMP)和两种密钥交换协议(OAKLEY 与 SKEME)组成。IKE 创建在由 ISAKMP 定义的框架上，沿用了 OAKLEY 的密钥交换模式以及 SKEME 的共享和密钥更新技术，定义了自己的两种密钥交换方式。

为确保通过 Internet 网使用 IPSec 协议安全通信，Internet 密钥交换 IKE 协议将执行双阶段协商工作。IKE 使用了两个阶段的 ISAKMP 密钥管理协议：第一阶段，协商创建一个通信信道(IKE SA)，并对该信道进行验证，为双方进一步的 IKE 通信提供机密性、消息完整性以及消息源验证服务；第二阶段，使用已建立的 IKE SA 建立 IPSec SA。

IKE 共定义两种交换。第一阶段有两种模式交换：对身份进行保护“主模式”交换以及根据基本 ISAKMP 文档制订“野蛮模式”交换。第二阶段交换使用“快速模式”交换。IKE 定义了两种信息交换：①为通信各方间协商一个 Diffie Hellman 组类型“新组模式”交换；②在 IKE 通信双方间传送错误及状态消息的 ISAKMP 信息交换。

Internet 密钥交换 IKE 解决了在不安全的网络环境(如 Internet)中安全地建立或更新共享密钥的问题。IKE 是非常通用的协议，不仅可为 IPSec 协议协商安全关联，而且可以为 SNMPv3、RIPv2、OSPFv2 等任何要求保密的协议协商安全参数。

【实验原理】

IPSec 协议的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议，它是一套完整的体系框架，包括 AH、ESP 和 IKE 三个协议。IPSec 使用了多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全保障，提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务。

IKE 为 IPSec 协议提供安全协商，可以使用两种对等体认证方式：预共享密钥和数字签名(或称数字证书)，本实验使用预共享密钥认证方式。

【实验步骤】

第一步：准备好 PC。

准备好 PC1 和 PC2 后，先在 PC1 和 PC2 上安装 VPN 管理软件。具体的安装步骤不在这里详述，查看 VPN 产品的随机说明书和产品光盘。

第二步：搭建拓扑，配置 IP 地址。

按照如图 3-1 所示拓扑图，搭建实验拓扑，并根据如表 3-1 所示编址方案，配置各设备的 IP 地址。

表 3-1　设备 IP 地址

设　备	接　口	地　址
VPN 网关 A	eth1 接口地址	192.168.1.1
	eth0 接口地址	10.1.1.1
PC1	PC1 的 IP 地址	192.168.1.2
	PC1 网关地址	192.168.1.1
VPN 网关 B	eth1 口地址	192.168.2.1
	eth0 口地址	10.1.2.1
PC2	PC2 的 IP 地址	192.168.2.2
	PC2 网关地址	192.168.2.1
Router	F0/0 地址	10.1.1.2
	F0/1 地址	10.1.2.2

说明：PC 及 Router 地址的配置方式不再详述。

(1) 如图 3-2 所示,在模拟客户机 PC1 的超级终端,转入命令行状态,在命令行下配置 VPN 网关 A 的 eth1 口地址。

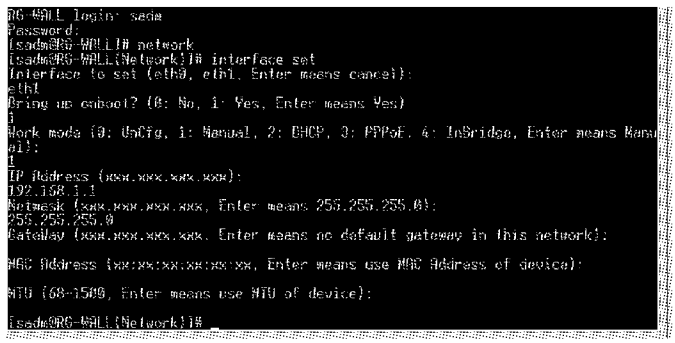

图 3-2 命令行模式配置 VPN 网关 eth1 口地址

(2) 如图 3-3 所示,在模拟客户机 PC1 上,打开 VPN 管理软件,登录 VPN 网关 A,然后配置 eth0 口地址。设置如图 3-4 所示 eth0 口地址。

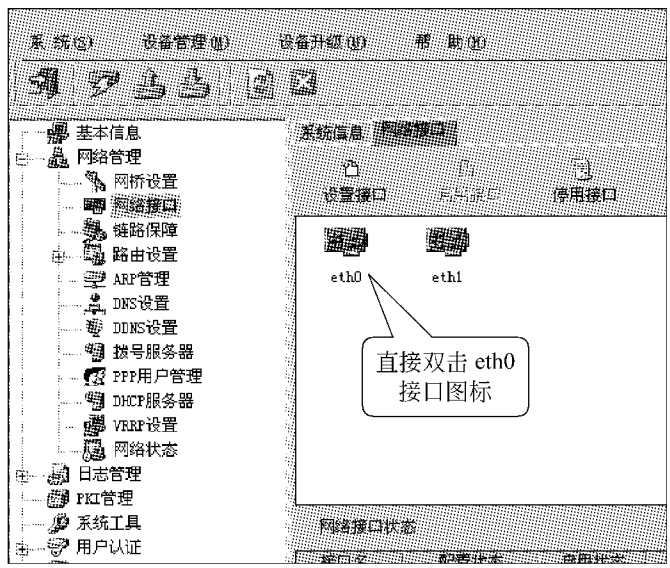

图 3-3 配置 eth0 口地址(1)

(3) 如上过程通过 PC2 的超级终端,在命令行下配置 VPN 网关 B 的 eth1 口地址,如图 3-5 所示。

(4) 通过 PC2 上的 VPN 管理软件登录 VPN 网关 B,然后配置 eth0 口地址,如图 3-6 所示。

设置如图 3-7 所示 eth0 口地址。

图 3-4　配置 eth0 口地址(2)

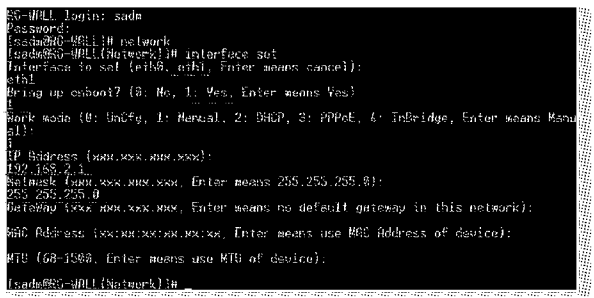

图 3-5　命令行模式配置 VPN 网关 eth1 口地址

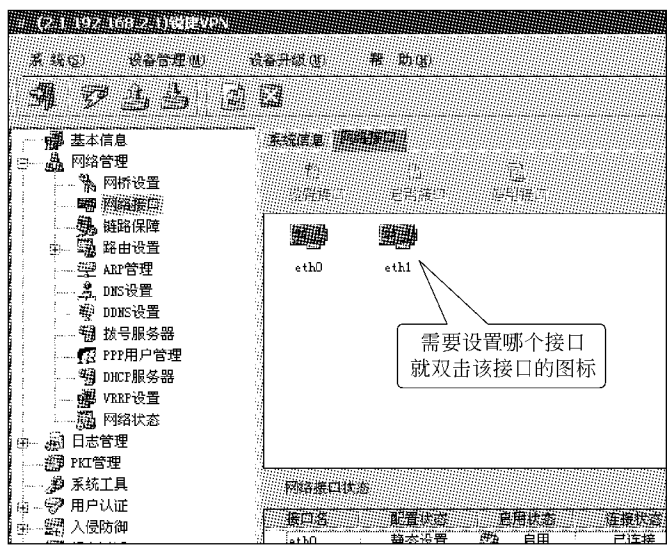

图 3-6　配置 eth0 口地址(1)

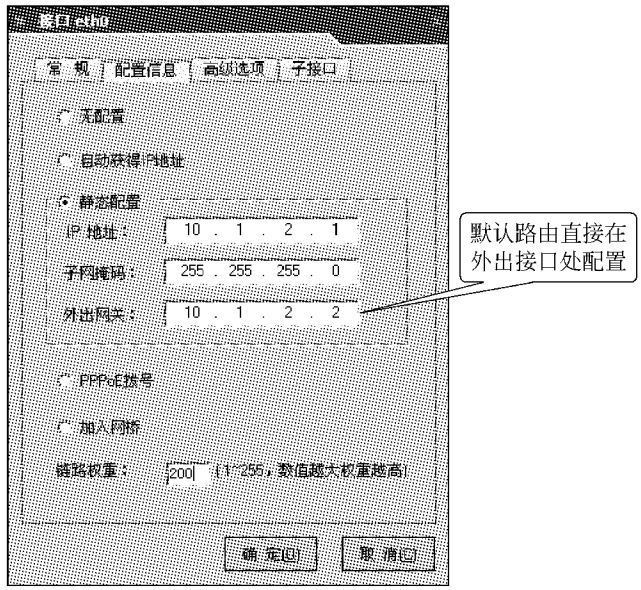

图 3-7 配置 eth0 口地址(2)

第三步：配置 VPN 网关 A 的 IPSec VPN 隧道。

(1) 进行设备配置，打开“虚拟专用网”中“隧道配置”项，单击“添加设备”按钮，添加设备，如图 3-8 所示。

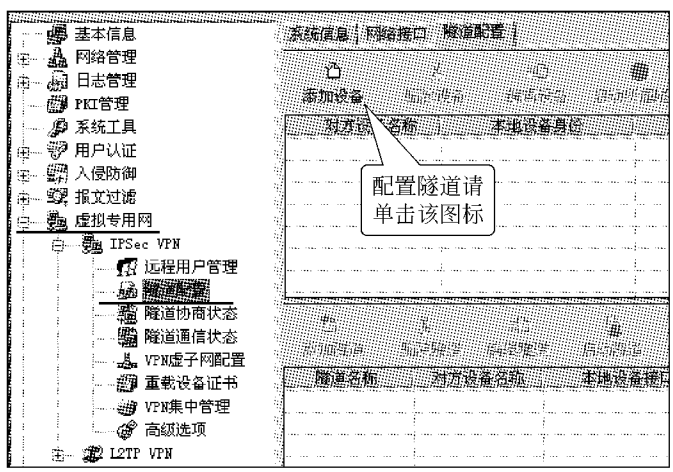

图 3-8 添加 IPSec VPN 隧道设备

在打开的 IPSec VPN 隧道设备配置信息中，选择设备名称和共享密钥，如图 3-9 所示。

如图 3-10 所示，在隧道设备信息的“高级选项”中配置图中设置相关信息。

图 3-9　配置 IPSec VPN 隧道设备信息

图 3-10　配置 IPSec VPN 隧道设备高级选项信息

(2) 在“隧道配置”选项中，进行隧道配置，如图 3-11 所示，选择添加的设备，单击“添加隧道”按钮。

如图 3-12 所示，在添加的新隧道中，为添加隧道配置隧道信息。

为添加的信息隧道配置“通信策略”信息，如图 3-13 所示。

添加完隧道后的信息如图 3-14 所示。

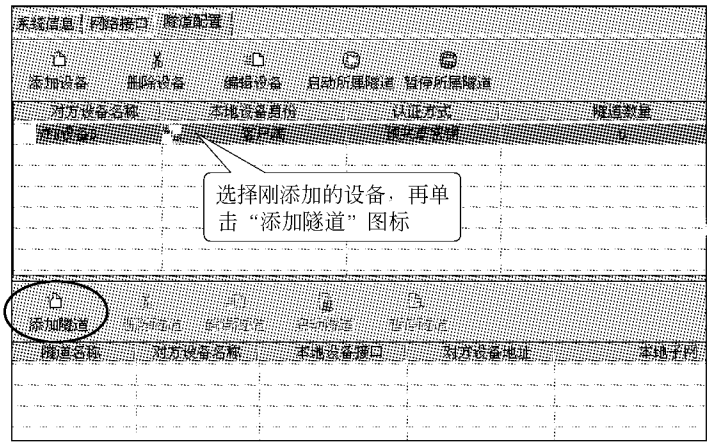

图 3-11 添加新隧道

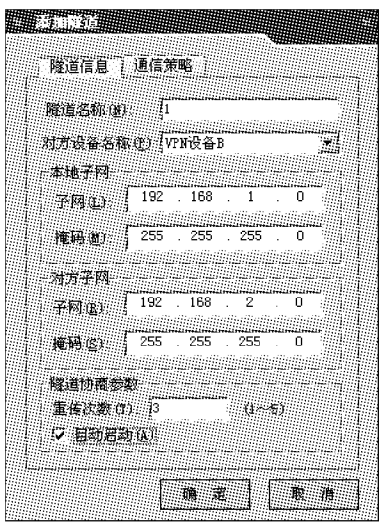

图 3-12 配置隧道信息

图 3-13 配置“通信策略”信息

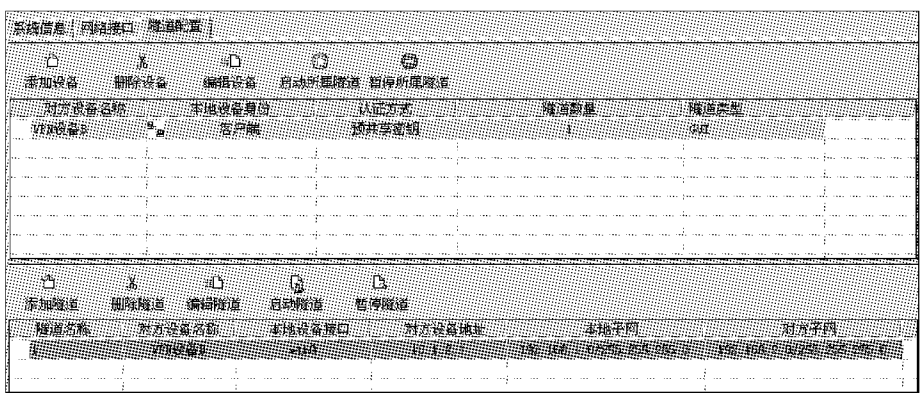

图 3-14 完成隧道配置信息

第四步：配置 VPN 网关 B 的 IPSec VPN 隧道。

(1) 进行设备配置。打开“虚拟专用网”中“隧道配置”项，单击“添加设备”按钮，添加设备，如图 3-15 所示。

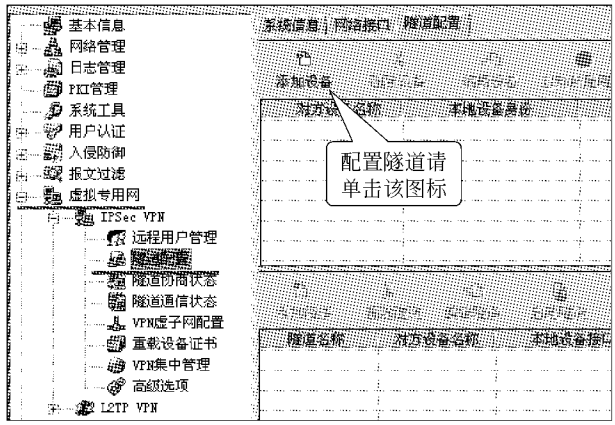

图 3-15　添加 IPSec VPN 隧道设备

在 IPSec VPN 隧道设备信息中，选择设备名称和共享密钥，如图 3-16 所示。

图 3-16　配置 IPSec VPN 隧道设备信息

如图 3-17 所示，在隧道设备信息的“高级选项”中配置相关信息。

(2) 进行隧道配置。

在“隧道配置”选项中进行隧道配置，如图 3-18 所示，选择添加的设备，单击“添加隧道”按钮。

图 3-17 配置 IPSec VPN 隧道设备高级选项信息

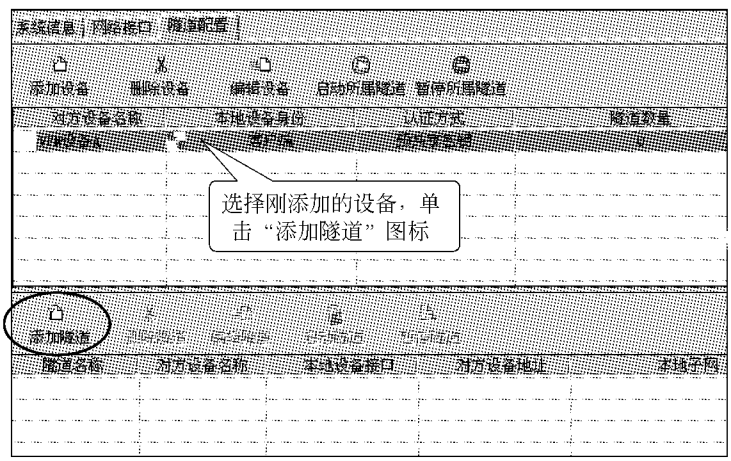

图 3-18 添加隧道

如图 3-19 所示，在添加的新隧道中，为添加隧道配置隧道信息。

为添加的信息隧道配置“通信策略”信息，如图 3-20 所示。

如图 3-21 所示，为添加完隧道后的界面截图。

第五步：启动隧道。

如图 3-22 所示，选择添加好隧道，单击“启动隧道”按钮，启动配置完成的隧道。

第六步：验证测试。

隧道启动后可以在“隧道协商状态”栏下看到隧道的协商状态。