



H3C SecPath F1000-S 防火墙

安装手册

杭州华三通信技术有限公司

<http://www.h3c.com.cn>

资料版本: T1-08044S-20070622-C-1.04

声明

Copyright ©2006-2007 杭州华三通信技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

H3C、**H3C**、Aolynk、、H³Care、、TOP G、、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V²G、VⁿG、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。如需要获取最新手册，请登录 <http://www.h3c.com.cn>。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：800-810-0504（固话拨打）

400-810-0504（手机、固话均可拨打）

网址：<http://www.h3c.com.cn>

前言

相关手册

手册名称	用途
《H3C SecPath 系列安全产品 操作手册》	介绍 H3C SecPath 系列安全网关/防火墙的功能特性、工作原理和配置及操作指导。
《H3C SecPath 系列安全产品 命令手册》	详细介绍 H3C SecPath 系列安全网关/防火墙所涉及的配置和操作命令。包括命令名、完整命令行、参数、操作视图、使用指导和操作举例。
《H3C SecPath 系列安全产品 Web 配置手册》	指导用户通过 Web 方式对 H3C SecPath 系列防火墙进行配置操作。

本书简介

本手册各章节内容如下：

- **第 1 章 产品介绍。**介绍 H3C SecPath F1000-S 防火墙的特点及其应用。提供 H3C SecPath F1000-S 防火墙的外观图及系统特性描述。
- **第 2 章 安装前的准备工作。**介绍 H3C SecPath F1000-S 防火墙对安装环境的要求，以及安装前和安装过程中需要注意的事项，安装所需工具也是本章介绍内容。
- **第 3 章 防火墙的安装。**介绍 H3C SecPath F1000-S 防火墙的机械安装方法、电源连接方法，配置口电缆、以太网电缆连接方法。
- **第 4 章 防火墙的启动与配置。**介绍 H3C SecPath F1000-S 防火墙的启动与配置基础知识，包括：防火墙的启动、上电、系统文件初始化等内容。
- **第 5 章 防火墙的软件维护。**介绍 H3C SecPath F1000-S 防火墙的软件维护，包括：软件升级、配置文件的加载等内容。
- **第 6 章 防火墙的硬件维护。**介绍 H3C SecPath F1000-S 防火墙的硬件维护，包括：更换 DDR SDRAM 等内容。
- **第 7 章 安装故障处理。**介绍 H3C SecPath F1000-S 防火墙安装启动过程中可能出现的问题及检查方法。

- **第8章 MIM 多功能接口模块。**介绍 H3C SecPath F1000-S 防火墙各功能模块的外观、面板及指示灯的含义，并介绍功能模块的安装及接口电缆的连接方法等。

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从两个或多个选项选取一个。
[x y ...]	表示从两个或多个选项选取一个或者不选。
{ x y ... } *	表示从两个或多个选项选取多个，最少选取一个，最多选取所有选项。
[x y ...] *	表示从两个或多个选项选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入 1~n 次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 **小心、注意：**提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。



警告：该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。



说明、提示、窍门、思考：对操作内容的描述进行必要的补充和说明。

环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

目 录

第 1 章 产品介绍	1-1
1.1 简介	1-1
1.2 硬件特性	1-2
1.2.1 外观	1-2
1.2.2 系统说明	1-2
1.2.3 指示灯含义	1-3
1.2.4 固定接口属性	1-3
1.2.5 MIM 多功能接口模块	1-5
第 2 章 安装前的准备工作	2-1
2.1 安装场所要求	2-1
2.1.1 温度/湿度要求	2-1
2.1.2 洁净度要求	2-1
2.1.3 防静电要求	2-2
2.1.4 电磁环境要求	2-2
2.1.5 防雷击要求	2-3
2.1.6 检查安装台	2-3
2.2 安全注意事项	2-3
2.3 检查防火墙及其附件	2-4
2.4 安装工具、仪表和设备	2-4
第 3 章 防火墙的安装	3-1
3.1 安装流程	3-1
3.2 安装到指定位置	3-2
3.2.1 安装到工作台上	3-2
3.2.2 安装到机柜中	3-2
3.3 安装通用接口模块	3-3
3.4 连接保护地线	3-3
3.5 连接到配置终端	3-4
3.6 连接到以太网口	3-5
3.7 连接电源线	3-7
3.8 安装后的检查	3-9
第 4 章 防火墙的启动与配置	4-1
4.1 启动	4-1
4.1.1 搭建配置环境	4-1
4.1.2 上电	4-4

4.1.3 启动过程	4-4
4.2 配置基础.....	4-5
4.2.1 基本配置步骤.....	4-5
4.2.2 命令行接口的特点.....	4-6
第 5 章 防火墙的软件维护	5-1
5.1 简介	5-1
5.1.1 Boot菜单	5-1
5.1.2 利用XModem协议完成应用程序和Boot ROM程序升级.....	5-3
5.1.3 Boot ROM程序扩展段的备份及恢复.....	5-5
5.1.4 通过TFTP完成应用程序的升级.....	5-6
5.1.5 利用FTP完成程序/文件的上传下载.....	5-8
5.1.6 修改Boot ROM口令	5-11
5.1.7 口令丢失的处理	5-13
第 6 章 防火墙的硬件维护	6-1
6.1 准备工具.....	6-1
6.2 打开防火墙机箱盖	6-1
6.3 更换DDR SDRAM	6-2
6.3.1 内存条在主板上的位置	6-4
6.3.2 拆卸内存条	6-4
6.3.3 安装内存条	6-5
6.4 合上防火墙机箱盖	6-5
6.5 MIM多功能接口模块的更换.....	6-6
第 7 章 安装故障处理	7-1
7.1 电源系统问题故障处理.....	7-1
7.2 配置系统故障处理	7-1
7.3 应用软件升级故障处理.....	7-2
第 8 章 MIM多功能接口模块	8-1
8.1 MIM多功能接口模块的种类.....	8-1
8.2 MIM多功能接口模块的安装与拆卸	8-1
8.3 MIM接口模块的故障处理	8-3
8.4 1FE/2FE/4FE接口模块.....	8-3
8.4.1 简介	8-3
8.4.2 接口模块外观.....	8-4
8.4.3 接口属性	8-5
8.4.4 面板及接口指示灯.....	8-5
8.4.5 接口连接电缆.....	8-6
8.4.6 接口电缆的连接	8-8
8.5 1GBE/2GBE模块.....	8-8

8.5.1 模块简介	8-8
8.5.2 模块外观	8-9
8.5.3 模块接口属性	8-9
8.5.4 模块接口指示灯	8-10
8.5.5 模块接口连接电缆	8-10
8.5.6 模块接口电缆的连接	8-11
8.6 1GEF/2GEF模块	8-11
8.6.1 模块简介	8-11
8.6.2 模块外观	8-12
8.6.3 模块接口属性	8-12
8.6.4 模块接口指示灯	8-13
8.6.5 模块接口连接光纤	8-14
8.6.6 模块接口光缆的连接	8-14
8.7 SSL模块	8-15
8.7.1 模块简介	8-15
8.7.2 模块外观	8-15
8.7.3 模块属性	8-15
8.7.4 模块运行指示灯	8-15
8.7.5 模块故障排除	8-16

插图目录

图 1-1 H3C SecPath F1000-S防火墙前面板示意图	1-2
图 1-2 H3C SecPath F1000-S防火墙后面板示意图	1-2
图 3-1 防火墙的安装流程	3-1
图 3-2 H3C SecPath系列防火墙机柜安装示意图	3-3
图 3-3 防火墙保护地接地端子	3-4
图 3-4 配置口电缆示意图	3-5
图 3-5 以太网电缆示意图	3-5
图 3-6 交流电源防火墙电源插座部分的外观.....	3-8
图 4-1 通过CONSOLE口进行本地配置示意图	4-1
图 4-2 新建连接	4-2
图 4-3 本地配置连接端口设置	4-2
图 4-4 串口参数设置	4-3
图 4-5 终端类型设置	4-3
图 5-1 [发送文件]对话框.....	5-4
图 5-2 正在发送文件界面	5-4
图 5-3 搭建FTP本地上传/下载环境	5-8
图 5-4 搭建FTP远程上传/下载环境	5-9
图 6-1 打开机箱盖示意图	6-2
图 6-2 内存条维护流程.....	6-3
图 6-3 内存条在主板上的位置示意图	6-4
图 6-4 内存条拆装示意图	6-5
图 6-5 合上机箱盖示意图	6-6
图 8-1 MIM多功能接口模块安装示意图 1	8-2
图 8-2 MIM多功能接口模块安装示意图 2	8-2
图 8-3 1FE接口模块外观.....	8-4
图 8-4 2FE接口模块外观.....	8-4
图 8-5 4FE接口模块外观.....	8-5
图 8-6 1FE接口模块面板.....	8-5
图 8-7 2FE接口模块面板.....	8-6

图 8-8 4FE接口模块面板	8-6
图 8-9 以太网电缆	8-6
图 8-10 5 类双绞线示例图	8-7
图 8-11 1GBE模块外观	8-9
图 8-12 2GBE模块外观	8-9
图 8-13 1GBE模块面板	8-10
图 8-14 2GBE模块面板	8-10
图 8-15 以太网电缆	8-10
图 8-16 5 类双绞线示例图	8-11
图 8-17 1GEF模块外观	8-12
图 8-18 2GEF模块外观	8-12
图 8-19 1GEF模块面板	8-13
图 8-20 2GEF模块面板	8-13
图 8-21 SSL模块外观	8-15
图 8-22 SSL模块面板	8-16

表格目录

表 1-1 H3C SecPath F1000-S防火墙的系统说明表	1-2
表 1-2 防火墙前面板指示灯含义	1-3
表 1-3 配置口属性	1-3
表 1-4 备份口属性	1-4
表 1-5 千兆以太网电接口属性	1-4
表 1-6 千兆以太网光接口属性	1-5
表 2-1 机房温度/湿度要求	2-1
表 2-2 机房灰尘含量限值	2-1
表 2-3 机房有害气体限值	2-2
表 3-1 H3C SecPath F1000-S防火墙外形尺寸	3-2
表 6-1 防火墙内存配置说明表	6-4
表 8-1 1FE/2FE/4FE模块接口属性.....	8-5
表 8-2 1FE/2FE/4FE接口模块指示灯含义	8-6
表 8-3 标准（直通）网线连接关系表	8-7
表 8-4 交叉网线连接关系表.....	8-7
表 8-5 1GBE模块接口属性	8-9
表 8-6 1GBE模块指示灯含义	8-10
表 8-7 1GEF/2GEF模块接口属性.....	8-12
表 8-8 1GEF模块指示灯含义	8-14
表 8-9 SSL模块属性.....	8-15
表 8-10 SSL模块指示灯含义	8-16

第1章 产品介绍

1.1 简介

H3C SecPath F1000-S 系列防火墙设备（以下简称防火墙）是面向企业用户开发的新一代专业防火墙设备，既可以作为中小型企业的出口防火墙设备，也可以作为大中型企业的内部防火墙设备。

H3C SecPath F1000-S 防火墙提供四个固定的 10/100/1000Mbps 自适应以太网口，其中两个千兆以太网口可支持光接口和电接口两种形式，两个支持电接口形式；提供两个 MIM 扩展槽位，目前可选的接口模块有 1FE/2FE/4FE/1GBE/2GBE/1GEF/2GEF/SSL 等；提供双电源冗余备份解决方案（AC+AC）；提供机箱内部环境温度检测功能，并支持网管，可满足电信级产品的高可靠性要求。

防火墙支持多种攻击防范手段、TCP Proxy、内网安全、流量监控、网址过滤、网页过滤、邮件过滤等功能，能够有效的保证网络的安全。

防火墙采用 ASPF 状态检测技术，可对连接过程和有害命令进行监测，并协同 ACL 完成动态包过滤。

防火墙提供多种智能分析和管理手段，支持邮件告警，支持多种日志，提供网络管理监控，协助网络管理员完成网络的安全管理。

防火墙支持 AAA、NAT、混合模式、面向对象管理等技术，可以确保在开放的 Internet 上实现安全的、满足可靠质量要求的网络。

防火墙支持多种 VPN 业务，如 L2TP VPN、IPsec VPN、GRE VPN、动态 VPN 等，并且支持硬件加密，可以针对客户需求通过 ADSL 拨号、VLAN 或隧道等方式接入远端用户，构建 Internet、Intranet、Access 等多种形式的 VPN。

防火墙提供基本的路由能力，支持 RIP/OSPF/BGP/路由策略及策略路由；支持丰富的 QoS 特性，提供流量监管、流量整形及多种队列调度策略。

防火墙支持 DAR（深度应用识别），通过对报文进行深度的识别和分类，大大加强了用户对数据流的控制力度。

防火墙支持双机热备，可以保护当前业务不会中断，很好地解决传统组网方案（例如 VRRP 等）的缺陷。

防火墙软件可以根据需求实现应用程序、Boot ROM 程序的在线升级，增加新特性、扩充新功能。

SecPath 系列防火墙支持通过 BIMS 功能自动更新设备的配置文件及应用程序，支持通过 VPN Manager 功能来完成 VPN 的部署和配置。

SecPath 系列防火墙支持 SNMP V3 网管，为用户提供强大的设备管理功能，并且按照中国、北美、欧洲、澳洲、日本等国家和地区的国际标准和国家标准设计，满足这些国家和地区 EMC、安规等认证及入网需求。

1.2 硬件特性

1.2.1 外观

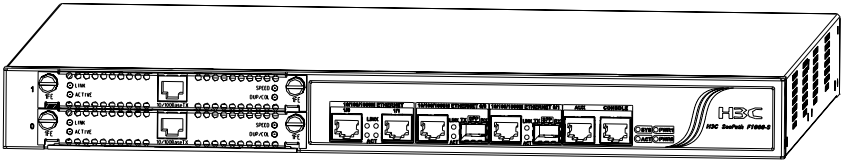


图1-1 H3C SecPath F1000-S 防火墙前面板示意图

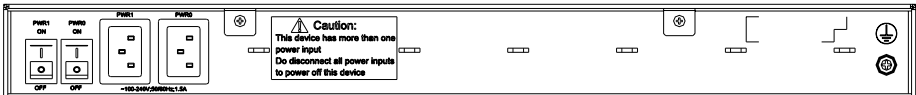


图1-2 H3C SecPath F1000-S 防火墙后面板示意图

1.2.2 系统说明

表1-1 H3C SecPath F1000-S 防火墙的系统说明表

项目		防火墙描述
MIM 插槽		2
固定接口		2 个 10/100/1000Mbps 以太网口(可支持光口和电口) 2 个 10/100/1000Mbps 以太网口(可支持电口) 1 个 AUX 口(备份口) 1 个 CON 口(配置口)
Boot ROM		512KB
DDR SDRAM		缺省：512MB 最大：1GB
Flash		缺省：16MB 最大：32MB
外型尺寸（W×D×H）		436 mm×430 mm×44 mm（不含脚垫）
电输入源	AC+AC	额定电压范围：100～240V AC；50/60Hz 最大电压范围：90～264V AC；50/60Hz 额定电流：1.5A
额定功率		100W

项目	防火墙描述
工作环境温度	0~40℃
环境相对湿度	10%~90%（非凝露）

 说明：

DDR SDRAM（双倍数据速率同步动态随机存取存储器）是常说的内存，存储系统运行时的程序和与 CPU 的通信数据；

FLASH 作为主文件存储介质，存放应用程序文件、异常信息、配置文件等；

Boot ROM（引导只读存储器）存放启动时的引导程序文件。

1.2.3 指示灯含义

H3C SecPath F1000-S 防火墙前面板指示灯含义见下表。

表1-2 防火墙前面板指示灯含义

指示灯	含义
PWR0	系统电源指示灯，灯灭表示 PWR0 电源没有接通，灯亮表示 PWR0 电源已接通。
PWR1	系统电源指示灯，灯灭表示 PWR1 电源没有接通，灯亮表示 PWR1 电源已接通。
SYS	硬件系统运行指示灯，灯常亮表示系统正常运行，灯灭表示系统工作不正常。
ACT	软件系统运行指示灯，灯闪烁表示软件系统正常运行，灯灭表示软件系统工作不正常。
LINK	GE 接口指示灯，灯灭表示链路没有连通，灯亮表示链路已经连通。
ACTIVE	GE 接口指示灯，灯灭表示没有数据收发，灯闪烁表示有数据收发。

1.2.4 固定接口属性

1. 配置口(CON)

表1-3 配置口属性

属性	描述
连接器类型	RJ45
接口标准	RS232
波特率	1200bps~115200bps 缺省 9600bps

属性	描述
支持服务	与字符终端相连 与本地 PC 的串口相连，并在 PC 上运行终端仿真程序 命令行接口

2. 备份口(AUX)

表1-4 备份口属性

属性	描述
连接器类型	RJ45
接口标准	RS232
波特率	1200bps~115200bps
支持服务	Modem 拨号 备份

3. 千兆以太网口

H3C SecPath F1000-S 防火墙提供了四个固定的 10/100/1000Mbps 以太网接口，其中两个千兆以太网口可支持光接口/电接口，两个千兆以太网口只支持电接口。电接口采用 RJ45 连接器，光接口采用 SFP（Small Form-Factor Pluggable，小封装可插拔）模块，用户可以根据需要选用。

H3C SecPath F1000-S 防火墙可提供 5 种类型的 1000Base-FX SFP 可插拔光接口模块，用户可根据自己的需要选购短距多模（850nm）光模块、中距单模（1310nm）光模块、长距单模（1310nm）光模块、长距单模（1550nm）光模块、超长距离单模（1550nm）光模块，光模块提供 LC 接口，所有光模块均可支持热插拔。

H3C SecPath F1000-S 防火墙以太网接口特性如下：

表1-5 千兆以太网电接口属性

属性	描述
连接器类型	RJ45
接口类型	MDI/MDIX 自适应
支持帧格式	Ethernet_II Ethernet_SNAP
工作方式	10/100/1000Mbps 自适应 全双工/半双工 (1000Mbps 与半双工不能同时配置)

表1-6 千兆以太网光接口属性

属性		描述				
		短距多模 (850nm) 光模块	中距单模 (1310nm) 光模块	长距 (1310nm) 光模块	长距 (1550nm) 光模块	超长距离 (1550nm) 光模块
连接器类型		SFP/LC				
光纤		62.5/125 μ m 多模光纤	9/125 μ m 单模光纤	9/125 μ m 单模光纤	9/125 μ m 单模光纤	9/125 μ m 单模光纤
最大传输距离		0.55km	10km	40km	40km	70km
中心波长		850nm	1310nm	1310nm	1550nm	1550nm
发送光功率	最小	-9.5dBm	-9dBm	-2dBm	-4dBm	-4dBm
	最大	0dBm	-3dBm	5dBm	1dBm	2dBm
接收灵敏度		-17dBm	-20dBm	-23dBm -	-21dBm	-22dBm
工作方式		1000Mbps 全双工模式				
支持帧格式		Ethernet_II Ethernet_SNAP				

说明：

- 当使用光模块时，请选用经过我司认证的光模块。
- 当进行电/光口切换时，应先在当前工作模式下（电或光）清除速率、双工等配置后再进行切换，待切换完成后再重新配置。

1.2.5 MIM 多功能接口模块

H3C SecPath F1000-S 防火墙提供了两个 MIM 扩展槽位，可以支持多功能接口模块：

- 1 端口 10Base-T/100Base-TX 快速以太网接口模块（1FE）
- 2 端口 10Base-T/100Base-TX 快速以太网接口模块（2FE）
- 4 端口 10Base-T/100Base-TX 快速以太网接口模块（4FE）
- 1 端口 10Base-T/100Base-TX/1000Base-T 以太网接口模块（1GBE）
- 2 端口 10Base-T/100Base-TX/1000Base-T 以太网接口模块（2GBE）
- 1 端口 1000Base-LX/1000Base-SX 以太网光接口模块（1GEF）
- 2 端口 1000Base-LX/1000Base-SX 以太网光接口模块（2GEF）
- SSL（Security Socket Layer，安全套接层）是安全套接层加密模块

对MIM多功能接口模块的详细介绍请参见《第 8 章 MIM多功能接口模块》。

第2章 安装前的准备工作

2.1 安装场所要求

H3C SecPath 系列防火墙必须在室内使用，为保证防火墙正常工作和延长使用寿命，安装场所应该满足下列要求。

2.1.1 温度/湿度要求

为保证防火墙正常工作，并延长使用寿命，机房内需维持一定的温度和湿度。若机房内长期湿度过高，易造成绝缘材料绝缘不良甚至漏电，还会发生材料机械性能变化、金属部件锈蚀等现象；若相对湿度过低，绝缘垫片会干缩而引起紧固螺丝松动，在干燥的气候环境下，还容易产生静电，危害防火墙上的 CMOS 电路；温度过高危害更大，因为高温会加速绝缘材料的老化过程，使防火墙的可靠性大大降低，严重影响其使用寿命。

H3C SecPath 系列防火墙对温度、湿度的要求见下表。

表2-1 机房温度/湿度要求

温度	相对湿度
0℃～40℃	10%～90%（非凝露）

2.1.2 洁净度要求

灰尘对防火墙的运行安全也是一大危害，因为室内灰尘落在机体上会造成静电吸附，使金属接插件或金属接点接触不良，不但会影响设备寿命，而且容易造成通信故障。当室内相对湿度偏低时，更易产生这种静电吸附。

防火墙对机房的要求为机房无爆炸性、导电性、导磁性及腐蚀性尘埃，灰尘浓度符合下表的要求：

表2-2 机房灰尘含量限值

机械活性物质	单位	含量
灰尘粒子	粒/m ³	≤3×10 ⁴ (3天内桌面无可见灰尘)
注：灰尘粒子：直径≥5 μm		

除灰尘外，H3C SecPath系列防火墙的机房对空气中所含的盐、酸、硫化物也有严格的要求，因为这些有害气体会加速金属的腐蚀和某些部件的老化过程。机房内对SO₂、H₂S、NH₃、Cl₂等有害气体的具体限制值见下表：

表2-3 机房有害气体限值

气体	最大（mg/m ³ ）
二氧化硫SO ₂	0.2
硫化氢H ₂ S	0.006
氨NH ₃	0.05
氯气Cl ₂	0.01

2.1.3 防静电要求

尽管 H3C SecPath 系列防火墙在防静电方面作了大量的考虑，采取了多种措施，但当静电超过一定限度时，仍会对单板电路乃至防火墙整机产生巨大的破坏作用。在与防火墙连接的通信网中，静电感应主要来自两个方面：一是室外高压输电线、雷电等外界电场；二是室内环境、地板材料、整机结构等内部系统。因此为防止静电损伤，应做到：

- 设备良好接地。
- 室内防尘。
- 保持适当的温度、湿度条件。
- 接触电路板时，应戴防静电手腕，穿防静电工作服。
- 将拆卸下的电路板面朝上放置在抗静电的工作台上或放入防静电袋中。
- 当观察或转移拆卸了的电路板时，请用手接触电路板的外边缘，避免用手直接接触摸电路板上的元器件。

2.1.4 电磁环境要求

防火墙使用中可能的干扰源，无论是来自设备或应用系统外部，还是来自内部，都是以电容耦合、电感耦合、电磁波辐射、公共阻抗（包括接地系统）耦合的传导方式对设备产生影响，因此为达到抗干扰的要求，应做到：

- 对供电系统采取有效的防电网干扰措施。
- 防火墙工作地最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些。
- 远离强功率无线电发射台、雷达发射台、高频大电流设备。
- 必要时采取电磁屏蔽的方法。

2.1.5 防雷击要求

尽管 H3C SecPath 系列防火墙在防雷击方面作了大量的考虑,也采取了必要措施,但是在雷击强度超过一定范围时,仍然有可能对防火墙造成损害。为达到更好的防雷效果,建议用户:

- 保证机箱的保护地用保护地线与大地保持良好接触。
- 保证电源插座的接地点与大地良好接触。
- 为增强电源的防雷击效果,可以考虑在电源的输入前端加入电源避雷器,这样可大大增强电源的抗雷击能力。

2.1.6 检查安装台

对 H3C SecPath 系列防火墙进行安装前要保证以下条件:

- 确认防火墙的入风口及通风口处留有空间,以利于防火墙机箱的散热。
- 确认机柜自身有良好的通风散热系统。
- 确认机柜足够牢固,能够支撑防火墙及其安装附件的重量。
- 确认机柜良好接地。

2.2 安全注意事项

基于防火墙的广泛应用及其在数据通信网络中担当的重要作用,再次强调手册中的如下标志,阅读过程中请注意:



警告: 表明该项操作不正确,可能给防火墙或防火墙操作者的人身安全带来极大危险,操作者必须严格遵守正确的操作规程。



注意: 表示在安装、使用防火墙中需要注意的操作。该操作不正确,可能影响防火墙的正常使用。

在防火墙的安装和使用过程中,特提出如下安全建议:

- 请将防火墙放置在远离潮湿或远离热源的地方。
- 请确认防火墙已经正确接地。
- 请在安装维护过程中佩戴防静电手腕,并确保防静电手腕与皮肤良好接触。
- 请不要带电插拔配置口(Console)、备份口(AUX)的电缆。
- 注意激光使用安全。不要用眼睛直视激光器的光发射口或与其相连的光纤连接器。
- 建议用户使用 UPS (Uninterrupted Power Supply, 不间断电源)。

2.3 检查防火墙及其附件

在确认安装环境符合要求后，请打开防火墙包装箱，并对照定货合同及装箱单仔细核对防火墙及附件是否齐全。如有疑问或差错，请与代理商联系。

2.4 安装工具、仪表和设备

1. 工具

- 十字螺丝刀
- 一字螺丝刀
- 防静电手腕
- 防静电袋

2. 电缆

- 地线及电源线
- 配置口（Console）电缆
- 可选电缆

3. 设备及仪表

- HUB 或 LAN Switch
- 配置终端（可以是普通的 PC 机）
- 与选配接口模块相关的设备
- 万用表

说明：

防火墙不附带安装工具、仪表及相关设备。

第3章 防火墙的安装

3.1 安装流程

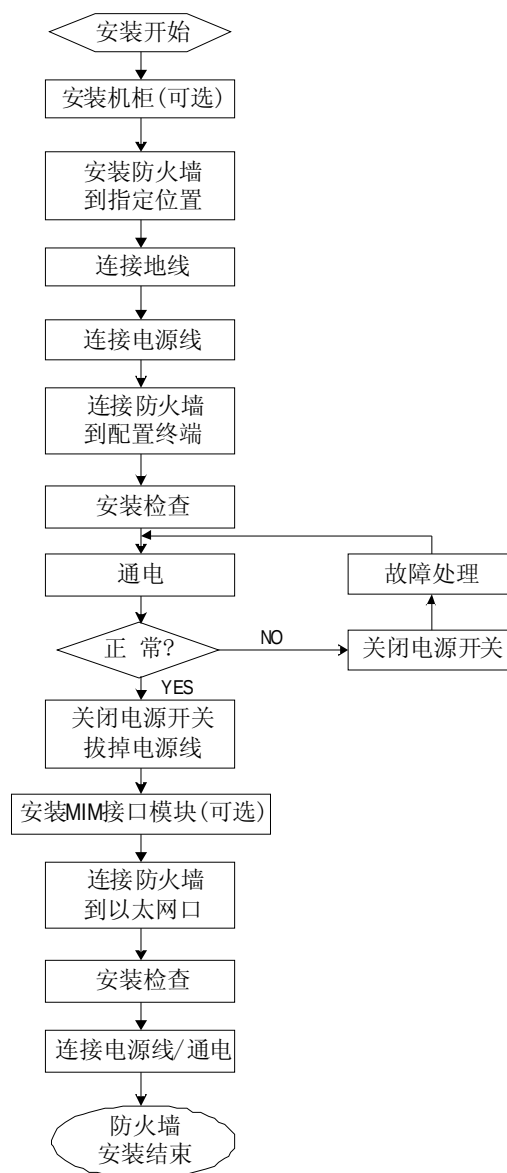


图3-1 防火墙的安装流程



注意：

开始安装 H3C SecPath 系列防火墙前，请确认：

- 已经仔细阅读第二章内容。
- 第二章中所述要求已经满足。

3.2 安装到指定位置

H3C SecPath 系列防火墙有两种安装方式：

- 直接安放在平台上
- 安装到机柜上

3.2.1 安装到工作台上

多数情况下，用户并不具备 19 英寸标准机柜，人们更常用到的方法就是将防火墙放置在干净的工作台上。此种操作比较简单，操作中需要注意如下事项：

- 保证工作台的平稳性与良好接地。
- 防火墙四周留出 10cm 的散热空间。
- 不要在防火墙上放置重物。

3.2.2 安装到机柜中

H3C SecPath 系列防火墙是按照 19 英寸标准机柜的尺寸进行设计的，尺寸如下表：

表3-1 H3C SecPath F1000-S 防火墙外形尺寸

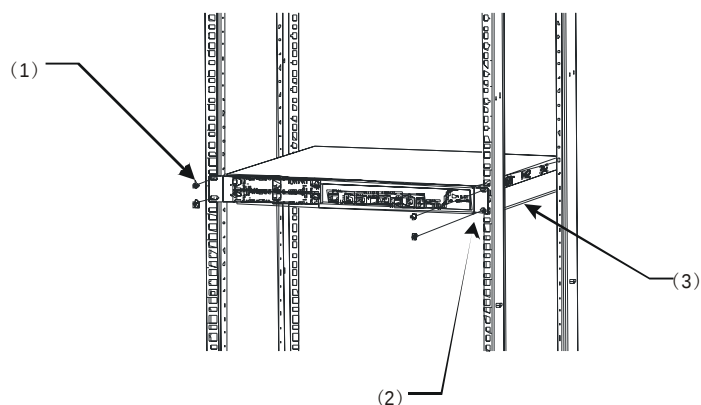
防火墙型号	外形尺寸（单位：mm）
H3C SecPathF1000-S 防火墙（W×D×H）	436×430×44（不含脚垫）

H3C SecPath F1000-S 防火墙安装过程如下：

第一步：检查机柜的接地与稳定性。用螺钉将固定挂耳固定在防火墙前面板两侧；

第二步：将防火墙放置在机柜的一个托盘上，根据实际情况，沿机柜导轨移动防火墙至合适位置，注意保证防火墙与导轨间的合适距离；

第三步：用满足机柜安装尺寸要求的盘头螺钉（螺钉型号最大不得超过国标 M6，表面经过防锈处理）将防火墙通过固定挂耳固定在机柜上，保证防火墙在机柜上位置水平并牢固。



(1) 固定螺钉（4个）

(2) 固定挂耳

(3) 导轨

图3-2 H3C SecPath 系列防火墙机柜安装示意图

3.3 安装通用接口模块

MIM多功能接口模块的安装请参见《第8章 MIM多功能接口模块》。

3.4 连接保护地线

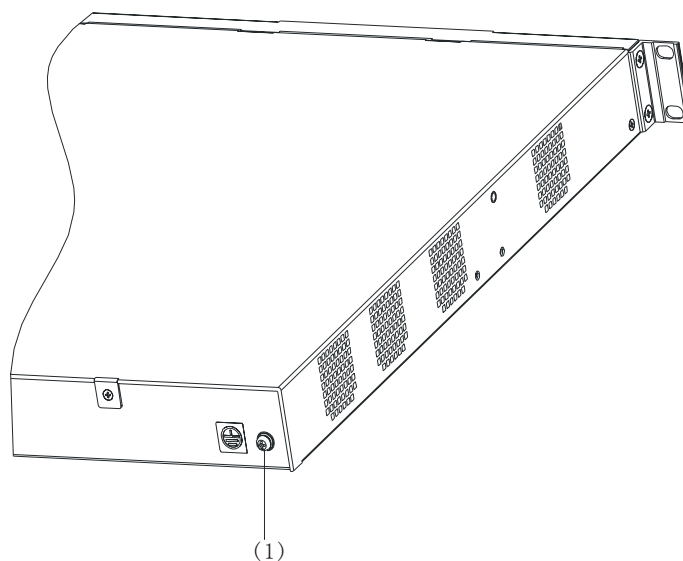


警告：

防火墙保护地线的正常连接是防火墙防雷、抗干扰的重要保障，所以用户在安装、使用防火墙时必须首先正确接好保护地线。

H3C SecPath 系列防火墙提供单独的保护地端子，保护地必须良好接地，以使感应电、泄漏电能够安全流入大地，并提高整机的抗电磁干扰的能力。

H3C SecPath F1000-S 防火墙的保护地端子位于机箱后面板的右下侧，有接地标识，见下图：



(1) 接地端子

图3-3 防火墙保护地接地端子

请用一根保护地电缆（PGND Cable）将该点与大地连接起来，要求接地电阻不大于 5Ω 。如果防火墙是安装在 19 英寸标准机柜上，则同样要求 19 英寸标准机柜接地。

**警告：**

防火墙正常工作时必须良好接地（保护地），否则防火墙无法可靠防雷，从而有可能造成防火墙及对端设备的损坏！

3.5 连接到配置终端

1. 配置口介绍

H3C SecPath系列防火墙提供了一个RS232 异步串行配置口（CON），通过这个接口用户可完成对防火墙的配置。配置口的属性请参见1.2.4 固定接口属性一节。

2. 配置口电缆

配置口电缆是一根 8 芯屏蔽电缆，一端压接 RJ45 插头，插入防火墙的 CON 口；另一端则带有一个 DB9（母）连接器，可插入配置终端的串口。

配置口电缆如图 3-4 所示：

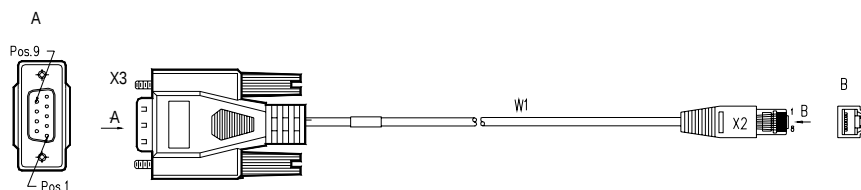


图3-4 配置口电缆示意图

3. 连接配置口电缆

通过终端配置防火墙时，配置口电缆的连接步骤如下：

第一步：选定配置终端。配置终端可以是标准的具有 RS232 串口的字符终端，也可以是一台普通的 PC 机，更常用的是后者。

第二步：连接电缆。关闭防火墙、配置终端的电源，通过配置电缆将配置终端的 RS232 串口与主控板上的配置口相连。

经安装检查后加电，正常情况下将在配置终端上显示防火墙启动信息，详细内容请参见《第 4 章 防火墙的启动与配置》。

3.6 连接到以太网口

1. 以太网接口介绍

H3C SecPath F1000-S 防火墙提供了四个固定的千兆以太网口，可进行 10/100/1000Mbps 自适应，其中两个千兆以太网口可支持光接口/电接口，两个千兆以太网口只支持电接口。光接口采用 SFP 模块，用户可根据需要选用表 1-6 所示的光模块类型（可分别支持多模光纤/单模光纤/单模长距离光纤传输）。

2. 以太网线缆

根据用户选用以太网口的不同，H3C SecPath 系列防火墙以太网线缆一般分为两种。

(1) 连接以太网电接口的线缆

采用 5 类双绞线连接以太网，标准以太网线或交叉以太网线均可，电缆外观如图 3-5 所示：

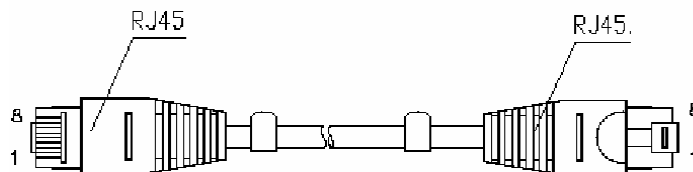


图3-5 以太网电缆示意图

 说明:

用户制作网线时，请优先采用屏蔽电缆，以保证电磁兼容的需要。

(2) 连接以太网光接口的线缆

采用单模或多模光纤连接以太网，用户可根据所选用的 1000Base-FX SFP可插拔光接口模块的类型来选择相应的光纤（光纤类型可参见表 1-6千兆以太网光接口属性）。这几种光模块的光接口均为LC型光纤连接器，故要求用户使用带有LC型光纤连接器的光纤。所有光模块均支持热插拔。

 说明:

光纤连接器（俗称活接头）：国际电信联盟（ITU）建议将其定义为“用以稳定地，但并不是永久地连接两根或多根光纤的无源组件”。光纤连接器是光纤通信系统中不可缺少的无源器件，它的使用使得光通道间的可拆式连接成为可能。

光纤连接器的种类很多，比如：

- FC：圆形带螺纹光纤连接器
 - ST：卡接式圆形光纤连接器
 - SC：方型光纤连接器
 - MT-RJ：收发一体的方型光纤连接器
 - LC：朗讯公司开发的一种小型光纤连接器，采用推拔按钮式安装
-

 说明:

以上几种光纤均为选配，用户在购买防火墙时必须预先指明选配的 SFP 模块，否则不予提供相应的光纤。

3. 连接以太网线缆

以连接 H3C SecPath F1000-S 防火墙正面板上的固定 10/100/1000M Ethernet 0/1 接口为例，请按照下述步骤连接：



注意:

对于每个固定以太网接口（例如 H3C SecPath F1000-S 防火墙的 10/100/1000M Ethernet 0/1 接口），当用双绞线连接电接口的同时，又用光纤连接光接口，此时系统默认工作接口为电接口。

(1) 以太网电接口线缆的连接



注意：

连接时请认准接口上的标识，以免误插入其它接口。

第一步：将以太网电缆一端连接到防火墙，另一端连接到对端设备；

第二步：请检查 10/100/1000M Ethernet 0/1 接口 LINK 指示灯的状态，LINK 灯亮表示链路已经连通，LINK 灯灭表示链路没有连通，请检查线路。

(2) 以太网光接口线缆的连接



注意：

连接光纤时，应注意如下事项：

- 不允许过度弯折光纤，其曲率半径应不小于 10cm；
 - 保证接口的 Tx 与 Rx 端连接正确；
 - 保证光纤端面处的清洁度。
-



警告：

激光危险！不要直接用眼睛直接观察与激光器相连的光纤连接器，否则可能对眼睛造成伤害。

第一步：确认防火墙正面板上的固定 10/100/1000M Ethernet 0/1 接口上的 Rx 和 Tx 光接口，并将光纤一端插入 Rx 口，另一端连至对端设备的 Tx 口；将另一根光纤的一端插入 Tx 口，另一端连至对端设备的 Rx 口。

第二步：上电后请检查 10/100/1000M Ethernet 0/1 接口 LINK 指示灯的状态。LINK 灯亮表示 Rx 链路已经连通，LINK 灯灭表示 Rx 链路没有连通，请检查线路。

3.7 连接电源线

H3C SecPath F1000-S 防火墙提供双交流供电机型。



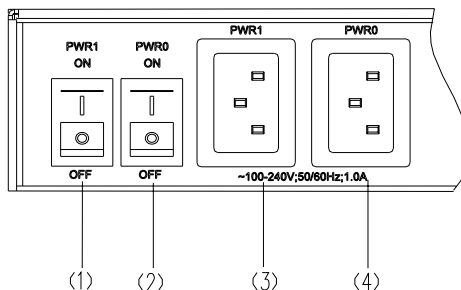
说明：

两路电源同时连接的状态下，若其中一路运行过程中出现故障，可互为备份。

1. 交流电源

交流电源输入范围：100～240V AC；50/60Hz。

双交流供电防火墙的电源插座部分外观如下图所示：



(1) PWR1 电源开关

(2) PWR0 电源开关

(3) 交流输入 PWR1

(4) 交流输入 PWR0

图3-6 交流电源防火墙电源插座部分的外观

2. 建议使用的交流电源插座

建议使用有接地点接头的单相三线电源插座。电源的接地点在建筑物中要可靠接地，一般楼房在施工布线时，已将本楼供电系统的电源接地点埋地。连接防火墙交流电源线前，用户需要确认本楼电源是否已经接地。

3. 交流电源线的连接

以下连接步骤以 H3C SecPath F1000-S 防火墙交流电源线的连接为例：

第一步：确认保护地已经正确连接至大地。

第二步：确认防火墙电源开关置于 OFF 位置后，将防火墙随机所带的电源线一端插到防火墙机箱后面板左侧的 PWR0 电源插座上，另一端插到交流电源插座上。

第三步：将防火墙随机所带的电源线一端插到防火墙机箱后面板左侧的 PWR1 电源插座上，另一端插到交流电源插座上。（也可只连接一个交流电源，则跳过此步）

第四步：把防火墙 PWR0 电源开关拨到 ON 位置。

第五步：把防火墙 PWR1 电源开关拨到 ON 位置（如只连接一个交流电源，则跳过此步）。

第六步：检查防火墙前面板电源灯 PWR0、PWR1 是否变亮，灯亮则表示电源连接正确。

第七步：检查防火墙前面板硬件系统指示灯 SYS 是否变亮，灯亮表明硬件系统正常。

3.8 安装后的检查

在 H3C SecPath 系列防火墙安装过程中，两次加电前均要进行安装检查，检查事项如下：

- 请检查防火墙周围是否留有足够的散热空间，机柜是否稳固。
- 检查电源线所接电源与防火墙要求的电源是否一致。
- 检查防火墙的保护地线是否连接正确。
- 检查防火墙与配置终端等其它设备的连接关系是否正确。

说明：

防火墙安装完毕后的检查非常重要，因为防火墙安装的牢固与否、接地良好与否、电源匹配与否，将直接关系到防火墙的正常使用。

第4章 防火墙的启动与配置

4.1 启动

第一次安装使用 H3C SecPath 系列防火墙时，只能通过配置口（Console）进行配置。

4.1.1 搭建配置环境

1. 连接防火墙到配置终端

如图 4-1 所示，将配置口电缆的 RJ45 一端与防火墙的配置口相连，DB9 一端与微机的串口相连。

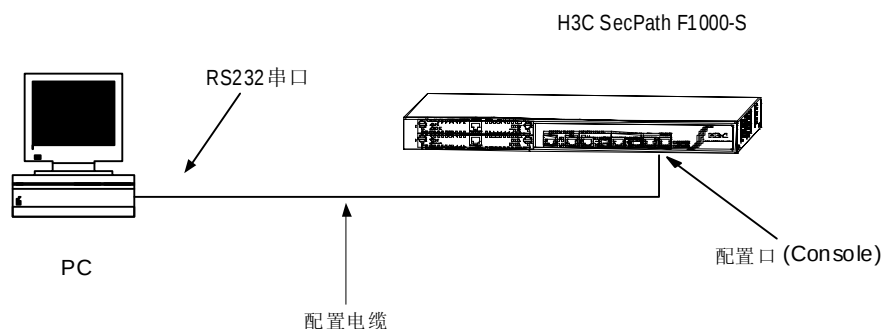


图4-1 通过 CONSOLE 口进行本地配置示意图

2. 设置配置终端的参数

第一步：打开配置终端，建立新的连接。

如果使用微机进行配置，需要在微机上运行终端仿真程序（如 Windows3.1 的 Terminal，Windows95/Windows98/Windows NT 的超级终端），建立新的连接。如图 4-2 所示，键入新连接的名称，按 [确定] 按钮。



图4-2 新建连接

第二步：设置终端参数。

Windows98 超级终端参数设置方法如下：

(1) 选择连接端口

在进行本地配置时，如图 4-3 所示，[连接时使用] 一栏选择连接的串口（注意选择的串口应该与配置电缆实际连接的串口一致）。

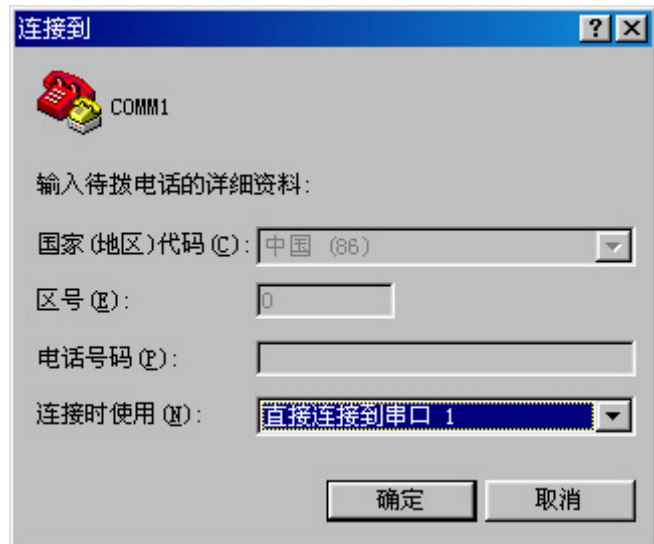


图4-3 本地配置连接端口设置

(2) 设置串口参数

如图 4-4 所示，在串口的属性对话框中设置波特率为 9600，数据位为 8，奇偶校验为无，停止位为 1，流量控制为无，按 [确定] 按钮，返回超级终端窗口。

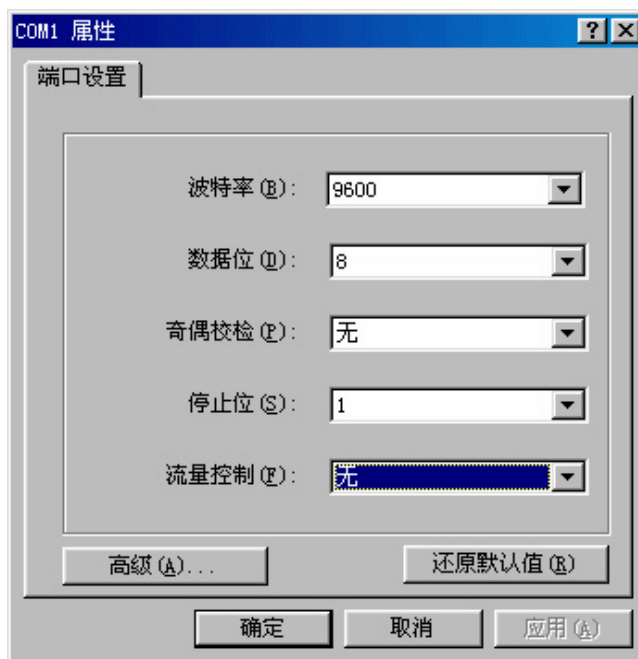


图4-4 串口参数设置

(3) 配置超级终端属性

在超级终端中选择 [属性/设置] 一项，进入图 4-5 所示的属性设置窗口。选择终端仿真类型为 VT100 或自动检测，按 [确定] 按钮，返回超级终端窗口。



图4-5 终端类型设置

4.1.2 上电

1. 上电前检查

防火墙上电之前应进行如下检查：

- 电源线和地线连接是否正确。
- 供电电压与防火墙的要求是否一致。
- 配置电缆连接是否正确，配置用微机或终端是否已经打开，并设置完毕。



警告：

上电之前，要确认设备供电电源开关的位置，以便在发生事故时，能够及时切断供电电源。

2. 上电

- 打开防火墙供电电源开关。
- 打开防火墙电源开关（将防火墙电源开关置于 ON 位置）。

3. 上电后检查/操作

防火墙上电后，要进行如下检查：

- 通风系统是否正常工作。

检查方法：防火墙上电后，应该可以听到风扇旋转的声音，把手放在防火墙的通风孔附近，可以感觉到空气的流动。

- 防火墙前面板上的指示灯显示是否正常。

检查方法：防火墙上电后，正常运行过程中各指示灯状态请参见1.2.3 中关于指示灯含义的描述。

- 配置终端是否显示正常。

检查方法：防火墙上电后，可在配置终端上直接看到启动界面（参见4.1.3 ）。启动结束后将提示用户键入回车，当出现命令行提示符“<H3C>”时即可进行配置了。

4.1.3 启动过程

防火墙上电开机后，将首先运行 Boot ROM 程序，终端屏幕上显示如下系统信息：

说明：

对于不同版本的 Boot ROM，终端上显示的界面可能会略有差别。

```
*
*   H3C SecPath Series Gateway Boot ROM V1.17   *
*
*****
```

Copyright(C) 2004-2007 by Hangzhou H3C Technologies Co.,Ltd.
Compiled at Wed Apr 12 17:39:36 CST 2006

Testing memory...OK!
512M bytes DDR SDRAM Memory
16M bytes Flash Memory
Hardware Version is 2.0
CPLD Version is 1.0

Press Ctrl-B to enter Boot Menu

若此时按下<Ctrl+B>键，系统将进入 Boot 菜单；否则，系统将进入程序解压过程。

说明：

必须在出现“Press Ctrl-B to Enter Boot Menu...”的 3 秒钟之内，按下<Ctrl+B>键，才能进入 Boot 菜单。

系统解压缩、初始化屏幕显示如下：

```
System is self-decompressing.....
System is starting...
User interface Con 0 is available.
```

Press ENTER to get started

键入<Enter>屏幕出现（若没有设置登录验证）：

<H3C>

该提示符表明防火墙已经进入用户视图，可以对防火墙进行配置了。

4.2 配置基础

4.2.1 基本配置步骤

一般情况下配置防火墙的基本思路如下：

第一步：在配置防火墙之前，需要将组网需求具体化、详细化，包括：组网目的、防火墙在网络互连中的角色、传输介质的选择、网络的安全策略和网络可靠性需求等；

第二步：然后根据以上要素绘出一个清晰完整的组网图；

第三步：配置防火墙各接口的 IP 地址；

第四步：配置路由，如果需要启动动态路由协议，还需配置相关动态路由协议的工作参数；

第五步：如果有特殊的安全需求，则需进行防火墙的安全性配置；

第六步：如果有特殊的可靠性需求，则需进行防火墙的可靠性配置。

关于防火墙各协议或功能配置的详细介绍，请参见《H3C SecPath 系列安全产品 操作手册》。

4.2.2 命令行接口的特点

1. 命令行接口的特点

防火墙向用户提供的命令行接口包括一系列的配置命令，用户可以通过这些命令来配置和管理防火墙，命令行接口有如下的特点：

- 通过 CON 口进行本地配置
- 通过 Telnet 进行本地或远程配置，可以用 Telnet 命令直接登录并管理其它防火墙；
- 用户可以随时键入“？”而获得在线帮助；
- 提供全中文的提示和帮助信息，方便国内广大用户；
- 提供网络测试工具，如 Tracert、Ping 等，迅速诊断网络可达性；
- 提供种类丰富、内容详尽的调试信息，帮助诊断网络故障；
- 命令行解释器对关键字采取不完全匹配的搜索方法，用户只需键入无冲突关键字即可被解释，如命令 **display**，键入 **dis** 即可。

2. 命令行接口

防火墙的命令行接口提供了丰富的配置命令，在系统视图下全部命令被分组，每组对应一个视图（详见《H3C SecPath 系列安全产品 操作手册》），可以用命令在不同的视图之间切换。一般情况下，在某个视图下只能执行限定的命令，但对一些常用命令（如 **ping**、**display current-configuration**、**interface** 等）在各种视图下均可执行。

第5章 防火墙的软件维护

5.1 简介

防火墙管理的文件包括三类：

- Boot ROM 程序文件
- 应用程序文件
- 配置文件

防火墙的软件维护主要是针对上面三类文件，包括：Boot ROM 程序文件、应用程序文件的升级下载及配置文件的上传下载等。

5.1.1 Boot 菜单

在防火墙的软件维护过程中需要使用 Boot 菜单，因此本节对 Boot 菜单进行介绍。

按照图 4-1所示搭建配置环境，然后启动防火墙，当配置终端上出现“Press Ctrl-B to enter Boot Menu”提示信息时，按下<Ctrl+B>键，系统将提示：

Please input Boot ROM password :



注意：

- 必须在出现“Press Ctrl-B to Enter Boot Menu...”的 3 秒钟之内，按下<Ctrl+B>键，才能进入 Boot 菜单，否则将进入程序解压过程。
- 若您在进入程序解压过程后希望进入 Boot 菜单，需要重新启动防火墙。

输入正确的口令后，键入<Enter>（如没有设置 Boot ROM 口令，直接键入<Enter>即可）系统将进入 Boot 菜单，显示如下：

1. H3C SecPath F1000-S 的 Boot 菜单

Boot Menu:

- 1: Download application program with XMODEM
- 2: Download application program with NET
- 3: Display file in flash
- 4: Delete file from flash
- 5: Start up and ignore configuration
- 6: Enter debugging environment
- 7: Boot Rom Operation Menu
- 8: Do not check the version of the software

9: Exit and reboot

Enter your choice(1-9):

Boot 菜单各选项含义如下:

- 1: 通过XModem下载应用程序, 具体升级步骤请参见5.1.2 ;
- 2: 通过以太网下载应用程序, H3C SecPath F1000-S仅提供通过TFTP升级应用程序的方法, 具体升级步骤请参见5.1.4 ;
- 3: 显示 flash 中的文件;
- 4: 从 flash 中删除文件;
- 5: 忽略配置文件并以初始配置启动;
- 6: 进入调试环境;
- 7: 进入 Boot ROM 操作子菜单;
- 8: 不检查 Boot ROM 程序扩展段、Boot ROM 程序和应用程序的软件版本, 此项用于版本升级时的后向兼容。当升级软件时, 如采用的软件版本完全正确, 仍无法升级成功, 系统提示软件为 “invalid version”, 此时可选中此项, 以便在软件升级时取消版本检查。此项被选中时只起作用一次, 重新启动防火墙后即恢复版本检查。
- 9: 退出 Boot 菜单并重新启动防火墙。

2. H3C SecPath F1000-S 的 Boot ROM 子菜单

如前所述, 进入 Boot 菜单后选择第七项即可进入 Boot ROM 子菜单, 其内容如下:

Boot ROM Operation Menu:

- 1: Download Boot ROM with XModem
- 2: Download Extended Segment of Boot ROM with XModem
- 3: Restore Extended Segment of Boot ROM from FLASH
- 4: Backup Extended Segment of Boot ROM to FLASH
- 5: Exit to Main Menu

Enter your choice(1-5):

各项含义如下:

- 1: 通过 XModem 升级 Boot ROM 程序;
- 2: 通过 XModem 升级 Boot ROM 程序扩展段;
- 3: 从 FLASH 中恢复 Boot ROM 程序扩展段;
- 4: 备份 Boot ROM 程序扩展段到 FLASH 中;
- 5: 退回到主菜单。

该菜单中提供了Boot ROM程序升级、备份、恢复等方法, 具体操作请参见5.1.2 、5.1.3 。

**注意：**

请勿轻易进行防火墙的软件升级，最好在技术支持人员的指导下进行。另外在进行防火墙升级时，请注意 Boot ROM 软件和应用程序的版本匹配。

5.1.2 利用 XModem 协议完成应用程序和 Boot ROM 程序升级

利用 XModem 协议完成软件升级时直接使用配置口，不必另外搭建配置环境。

1. 应用程序的升级

第一步：进入 Boot 菜单（参见 5.1.1 小节），键入 <1>，选择通过 XModem 协议下载应用程序。防火墙将提供如下可供选择的下载速率：

```
Downloading application program from serial ...
```

```
Please choose your download speed:
```

```
1: 9600 bps
```

```
2: 19200 bps
```

```
3: 38400 bps
```

```
4: 57600 bps
```

```
5: 115200 bps
```

```
6: Exit to Main Menu
```

```
Enter your choice(1-6):
```

第二步：选择合适的下载速率，如键入 <5>，选择 115200 bps 的下载速率，防火墙将提示如下信息：

```
Download speed is 115200 bps. Change the terminal's speed to 115200 bps, and  
select XModem protocol. Press ENTER key when ready.
```

第三步：根据上面提示，改变配置终端设置的波特率（参考图 4-4），使其与所选的软件下载波特率一致。设置完终端波特率后，应做一次终端的断开（即[拨入/断开]）和拨号（即[拨入/拨号]）操作，然后按 <Enter> 键即可开始下载，系统提示如下：

```
Downloading ... CCCCC
```

说明：

设置完配置终端的波特率后，只有做一次终端仿真程序的断开和连接操作，新的设置才会有效。

第四步：从终端窗口选择[传送/发送文件]，弹出如下图所示的对话框：

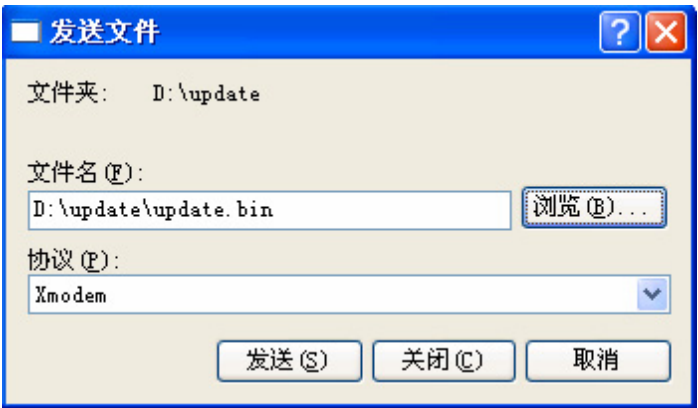


图5-1 [发送文件]对话框

第五步：点击[浏览]按钮，选择需要下载的应用程序文件，并将协议设置为 XModem，然后点击[发送]按钮，系统弹出如下界面：

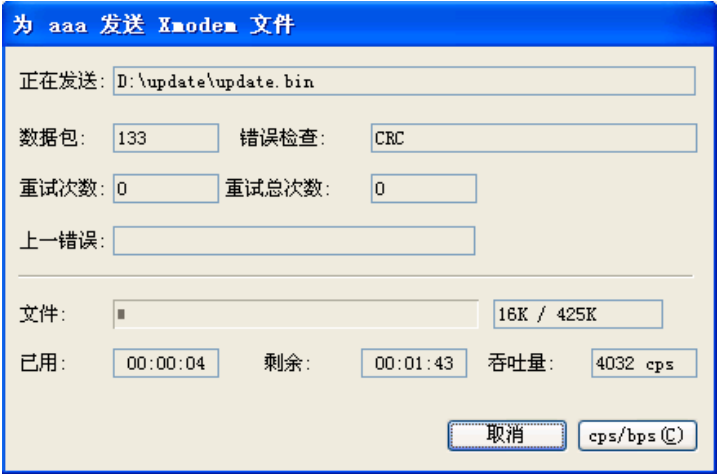


图5-2 正在发送文件界面

第六步：下载完成后，系统开始写 Flash（闪速存储器）操作，当这一操作完成后，终端界面出现如下信息，表明下载完成：

```
XModem download completed, Packet length 8790321 bytes.
System file length 7868992 bytes, http.zip file length 921329 bytes.

Writing file flash:/system to FLASH...
Please wait, it may take a long time
#####
Writing into Flash Succeeds.

Writing file flash:/http.zip to FLASH...
Please wait, it may take a long time
#####
#####
```

```
#####
```

```
Writing into Flash Succeeds.
```

```
Please use 9600 bps.Press <ENTER> key to reboot the system.
```

此时按提示将配置终端速率恢复为 9600bps（并进行一次断开和拨号操作），然后系统正常启动。

2. Boot ROM 程序的升级

第一步：进入Boot菜单（参见5.1.1 小节），选择<7>，进入Boot ROM操作子菜单。

第二步：在Boot ROM操作子菜单中选择<1>，通过XModem升级Boot ROM程序，防火墙将提供多种可选择的速率，随后操作与5.1.2 中的“1. 应用程序的升级”中的描述相同。



注意：

如果整个 Boot ROM 程序升级失败，将无法现场恢复，故只有在必要且有技术支持人员协助的情况下方可升级整个 Boot ROM 程序。

3. Boot ROM 程序扩展段的升级

第一步：进入Boot菜单（参见5.1.1 小节），选择<7>，进入Boot ROM操作子菜单；

第二步：在Boot ROM操作子菜单中选择<2>，通过XModem升级Boot ROM程序扩展段，防火墙将提供多种可选择的速率，随后操作与5.1.2 中的“1. 应用程序的升级”中的描述相同。



注意：

采用这种方法升级 Boot ROM 程序只是升级了程序的一部分，一旦出现错误可以重新升级。

5.1.3 Boot ROM 程序扩展段的备份及恢复

1. 在 FLASH 中备份 Boot ROM 程序的扩展段

如果防火墙需要备份 Boot ROM 程序的扩展段，可以采用如下方法：

第一步：进入Boot菜单（操作方法见5.1.1 ），选择<7>，进入Boot ROM操作子菜单；

第二步：在 Boot ROM 操作子菜单中选择<4>，这样当前的 Boot ROM 程序扩展段将被复制到 FLASH 中。

Backup Extended Segment, are you sure?[Y/N]

键入<Y>，则开始备份；

如果备份成功，则提示信息如下：

```
Writing to FLASH.Please wait...####
```

```
Backuping Boot ROM program to FLASH succeeded!
```

第三步：当再次出现 **Boot** 子菜单时，选择<5>，退出并重启防火墙即可。

2. 从 FLASH 中恢复 Boot ROM 程序扩展段

在 **Boot ROM** 程序扩展段出现问题或被误升级的情况下，可以将以前在 **FLASH** 中备份的 **Boot ROM** 程序扩展段重新恢复到 **Boot ROM** 中，方法如下：

第一步：进入 **Boot** 菜单，选择<7>，进入 **Boot ROM** 操作子菜单（菜单内容如上所示）；

第二步：在 **Boot ROM** 操作子菜单中选择<3>，从 **FLASH** 中恢复 **Boot ROM** 程序扩展段，会出现如下提示：

```
Restore Extended Segment, are you sure?[Y/N]
```

键入<Y>，则开始恢复；

如果成功恢复，则出现如下提示：

```
Writing to Boot ROM.Please wait...#####
```

```
Restoring Boot ROM program succeeded!
```

第三步：当再次出现 **Boot** 子菜单时，选择<5>，退出并重启防火墙即可。

5.1.4 通过 TFTP 完成应用程序的升级

通过网络下载应用程序是指通过以太网口下载应用程序，此时防火墙作为 **Client**，需要在防火墙的固定以太网口上连接 **TFTP Server**。具体的升级方法如下：



注意：

TFTP Server 程序由用户自己购买、安装，H3C SecPath 系列防火墙不提供此软件。

H3C SecPath F1000-S 仅提供 **TFTP client** 的功能，故仅提供通过 **TFTP** 升级应用程序的方法，升级步骤如下：

(1) 启动 TFTP Server

在防火墙的以太网口所连接的 **PC** 上启动 **TFTP Server**，并设置好欲加载文件的所在路径。

(2) 配置防火墙

第一步：进入 **TFTP** 配置状态；

启动防火墙，进入 **Boot** 菜单（操作方法见 5.1.1），选择<2>，进入 **Net Port Download Menu**（网络下载菜单）；

显示如下：

```
Net Port Download Menu:
  1: Change Net Parameter
  2: Download From Net
  3: Exit to Main Menu
Enter your choice(1-3): 1
```

第二步：配置 TFTP 参数；

选择<1>，可配置防火墙的网络接口参数，包括防火墙使用的接口、接口 IP 地址、子网掩码等；以及 TFTP Server 参数，包括 TFTP Server 的以太网口 IP 地址、应用程序的文件名等。

Change Download parameter		
Download device	:ETH0/1	下载所使用的设备名
Download file(Max 60 char)	:system	服务器上的应用程序文件名
IP address of ETH0/1	:192.168.1.15	防火墙接口的 IP 地址
Subnet mask for ETH0/1	:255.255.255.0	防火墙接口的子网掩码
IP address of the server	:192.168.1.10	TFTP 服务器的 IP 地址
IP address of the gateway	:10.110.95.117	网关的 IP 地址



注意：

- 必须使用防火墙的 ETH0/1 接口进行升级。
- “IP address of the server : [192.168.1.10]” 一项必须设为防火墙以太网口所连的 TFTP Server 的 IP 地址。
- 建议将 TFTP Server 的网口 IP 地址与防火墙 ETH0/1 接口的 IP 地址设置为同一网段。

第三步：确认配置参数；

键入最后一项值后，将会出现如下提示并返回 Net Port Download Menu 菜单：

```
Saving config, please wait...OK!
Net Port Download Menu:
  1: Change Net Parameter
  2: Download From Net
  3: Exit to Main Menu
Enter your choice(1-3): 2
```

(3) 通过 TFTP 下载应用程序

按下<2>键，进入 TFTP 下载状态，提示如下：

```
Starting the TFTP download...
.....
.....
TFTP download completed, Packet length 8790321 bytes.
```

```

System file length 7868992 bytes, http.zip file length 921329 bytes.

Writing file flash:/system to FLASH...
Please wait, it may take a long time
#####
Writing into Flash Succeeds.

Writing file flash:/http.zip to FLASH...
Please wait, it may take a long time
#####
#####
#####
Writing into Flash Succeeds.
    
```

5.1.5 利用 FTP 完成程序/文件的上传下载

H3C SecPath 系列防火墙提供 FTP Server 功能，为用户提供了另外一种更新配置文件、升级应用程序及 Boot ROM 程序的途径。任何 FTP Client（包括本地用户和远端用户）只要与防火墙连通即可。当通过用户验证后，即可进行配置文件或应用程序的上传下载。利用 FTP 上传/下载应用程序、配置文件及上传 Boot ROM 程序操作步骤如下：

说明：

- 上传：从 FTP 客户端的微机向防火墙传送文件，即 put 操作。
- 下载：从防火墙向 FTP 客户端的微机传送文件，即 get 操作。

1. 搭建上传/下载环境

- 搭建 FTP 本地上传/下载环境

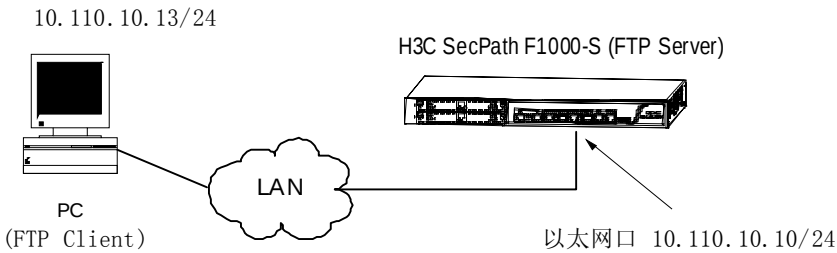


图5-3 搭建 FTP 本地上传/下载环境

- 第一步：通过防火墙以太网口连接微机；
- 第二步：配置防火墙以太网口 IP 地址，假设为 10.110.10.10；
- 第三步：配置微机以太网口 IP 地址，假设为 10.110.10.13；

第四步：将应用程序/Boot ROM 程序/配置文件等拷贝到某一路径下，假设路径为 C:\version;



注意：

微机网口 IP 地址与防火墙以太网口 IP 地址应位于同一网段。

- 搭建 FTP 远程上传/下载环境

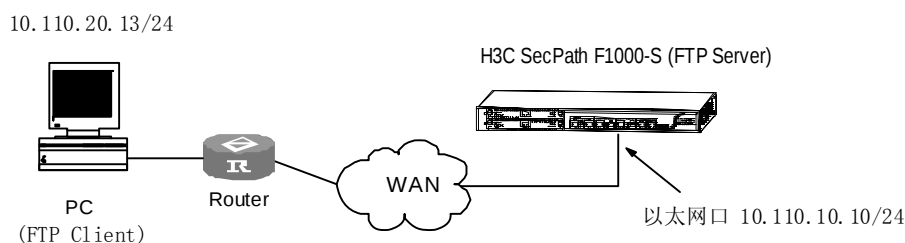


图5-4 搭建 FTP 远程上传/下载环境

第一步：将微机通过 WAN 连接至防火墙任意接口。这种方法不要求微机与防火墙在同一网段，用于防火墙远程升级；

第二步：将应用程序、Boot ROM 程序或配置文件拷贝到某一路径下，假设路径为 C:\version。

2. 启动 FTP 服务器

请防火墙侧维护人员进行配合，作如下配置：

第一步：设置验证方式；

📖 说明：

AAA 验证的具体配置您可以根据自己的实际情况进行选择，命令的详细介绍请参见《H3C SecPath 系列安全产品 操作手册》的 AAA 和 RADIUS 配置。

第二步：添加用户名；

```
[VPNGateway] local-user VPNGateway
```

VPNGateway 表示用户名。

第三步：添加口令；

```
[VPNGateway-luser-vpngateway] password simple 123
```

第四步：添加服务类型，指定 FTP 目录；

```
[VPNGateway-luser-vpngateway] service-type ftp ftp-directory flash:
```

第五步：添加权限等级；

```
[VPNGateway-luser-vpngateway] level 3
```

第六步：启动 FTP 服务器。

```
[VPNGateway] ftp server enable
```

经过以上操作，在防火墙上已经启动了 FTP 服务器，并设置了用户，这样任何一个 FTP 客户端程序均可使用该用户名、口令登录 FTP 服务器。

3. 上传/下载应用程序、配置文件及上传 Boot ROM 程序

第一步：在 DOS 下进入应用程序、Boot ROM 程序或配置文件所在路径，然后执行 FTP 命令，与防火墙建立 FTP 连接，如：

```
C:\version>ftp 10.110.10.10
```

若连接成功，则显示（以 Windows98 为例）：

```
Connected to 10.110.10.10
220 FTP server ready on VPNGateway at
User(10.110.10.10:(none)):
```

第二步：使用已经在防火墙上设置好的用户名、口令登录 FTP 服务器；

```
User(10.110.10.10:(none)): VPNGateway          键入用户名
331 Password required for ftp
Password:          键入口令（屏幕上不显示用户输入的口令）
230 User ftp logged in
ftp>
```

当出现提示符 ftp> 时，表示可以进行上传下载操作了。

第三步：上传/下载应用程序、配置文件或上传 Boot ROM 程序；

说明：

防火墙端应用程序缺省名称为 system，配置文件缺省名称为 config.cfg，Boot ROM 扩展段文件缺省名称为 bootrom，整个 Boot ROM 文件缺省名称为 bootromfull。

- 上传应用程序/Boot ROM 程序/配置文件

ftp> put	键入<put>，表示进行上传操作。
local file	键入要上传的应用程序/Boot ROM 程序/配置文件的名称。
remote file	键入防火墙端上传后所要保存的应用程序/Boot ROM 程序/配置文件名称。

上传文件结束后，重新显示“ftp>”提示符，可键入<dir>显示防火墙上的文件名称和大小，上传成功则配置文件大小与主机上的文件大小一致。



注意：

- 当使用 FTP 对应用程序进行升级时，请确保防火墙的 Flash 中有足够的空间。若剩余空间不足，需使用 **delete /unreserved** 命令将旧版本或其他文件永久删除，否则无法上传新文件。
- 当使用 **put** 命令完成 Boot ROM 程序的上传后，还应接着使用 **upgrade bootrom [full]** 命令将 **bootrom/bootromfull** 程序从 Flash 的根目录中解出，写到 Boot ROM 中，才能完成 Boot ROM 的升级。
- 将应用程序文件上传到 Flash 中后，若要使应用程序在下次启动时生效，需将文件重命名为 **system**。
- 将配置文件上传到 Flash 中后，若要使配置文件在下次启动时生效，需将文件重命名为 **config.cfg**，或使用 **startup saved-configuration** 命令设置系统下次启动时使用的配置文件。

• 下载应用程序/配置文件

```
ftp> get          键入<get>，表示进行下载操作。
remote file      键入防火墙端应用程序/配置文件名称。
local file       键入要保存的应用程序/配置文件的名称。
```

第四步：上传/下载成功后，退出 FTP 客户端程序。

```
ftp> quit        键入<quit>，表示退出 ftp 连接。
```

4. 使用 detach 命令将 Web 文件解包分离出来。

FTP 方式下载完成应用程序/配置文件后。当应用程序中包含 Web 文件时，还需使用 **detach** 命令将其解包分离出来才能使用。

```
<VPNGateway> detach system
      System file length 7856557 bytes, http file length 834724 bytes.
<VPNGateway> dir
Directory of flash:/

  0  -rw-   8691281  Jun 16 2009 06:46:36  system
  1  -rw-    1830   Jun 17 2009 07:47:16  config.cfg
  2  -rw-   834724  Jun 18 2009 02:22:39  http.zip
```

如果要解包的文件没有捆绑 Web 文件，则提示文件中没有捆绑 Web 文件；如果没有指定解包出的 Web 文件名，则 Web 文件名缺省为 **http.zip**。

5.1.6 修改 Boot ROM 口令

可以使用防火墙的 Boot 菜单更改 Boot ROM 的口令。

启动防火墙，当配置终端上出现“System starts booting”提示信息时，按下<Ctrl+D>键，系统将提示：

Please input Boot ROM password :



注意:

- 必须在出现 “System starts booting” 的 3 秒钟之内，按下<Ctrl+D>键，才能进入 Boot 菜单，否则将进入程序解压过程。
- 若您在进入 Boot ROM 扩展段后希望进入 Loader 段菜单，需要重新启动防火墙。

输入正确的口令后，键入<Enter>（如果没有设置 Boot ROM 口令，直接键入<Enter>即可）系统将进入 Boot 菜单，显示信息如下：

Boot Menu:

- 1: Download Boot ROM with XModem
 - 2: Download Extended Segment of Boot ROM with XModem
 - 3: Modify Boot ROM password
 - 4: System booting from Flash
 - 5: Do not check the version of Extended Segment of Boot ROM
 - 6: Exit and reboot
- Enter your choice(1-6):

Boot 菜单各选项含义如下：

- 1: 通过 XModem 下载 Boot ROM 程序；
- 2: 通过 XModem 升级 Boot ROM 程序扩展段；
- 3: 修改 Boot ROM 密码；
- 4: 从flash中引导Boot ROM扩展段；（此项功能需要flash中存在Boot ROM扩展段的备份，请参见5.1.3 。）
- 5: 不检查 Boot ROM 程序扩展段、Boot ROM 程序的软件版本；（此项功能用于版本升级时的后向兼容。当升级软件时，如采用的软件版本完全正确，仍无法升级成功，系统提示软件为 “invalid version”，此时可选中此项，以便在软件升级时取消版本检查。此项被选中时只起作用一次，重新启动防火墙后即恢复版本检查）
- 6: 退出 Loader 段菜单并重新启动防火墙。

在 Boot 菜单中选择<3>，修改 Boot ROM 密码，提示信息如下：

Modify Boot ROM password, are you sure?[Y/N]y

Please input new password(Max 32 char) :

Retype the new password(Max 32 char) :

Saving the password... Success!

 说明:

密码的最大长度是 32 个字符。

5.1.7 口令丢失的处理

如果防火墙 **Boot ROM** 的口令或用户口令丢失，请与技术支持人员联系，技术支持人员会帮助您进入防火墙，并重新设置口令。

第6章 防火墙的硬件维护

6.1 准备工具

- 十字螺丝刀
- 一字螺丝刀
- 防静电手腕
- 防静电袋

 说明：

防火墙并不附带安装工具，工具需要用户自己准备。

6.2 打开防火墙机箱盖

第一步：关掉防火墙电源并拔掉电源线。

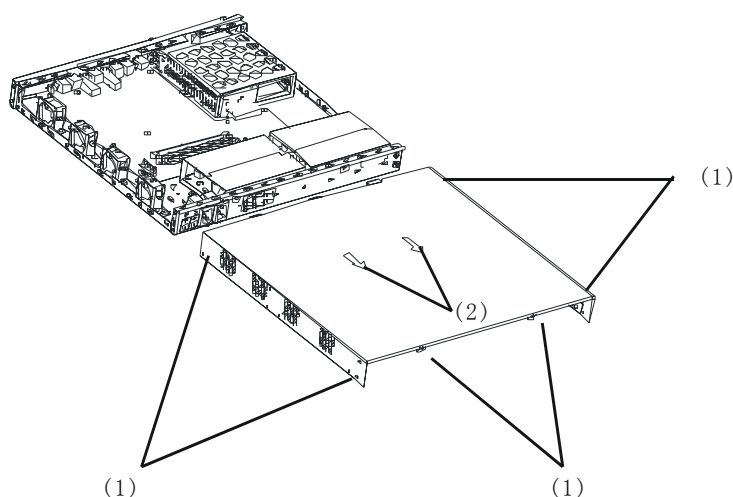
第二步：拔掉防火墙前面板上所有接口模块的接口电缆（注意保留地线的连接）。

第三步：将防火墙放置于平台上，防火墙后面板正对操作者。用十字螺丝刀取下防火墙机箱盖后面板上的两颗固定螺钉。

第四步：用十字螺丝刀分别取下防火墙机箱盖侧面的两颗固定螺钉。

第五步：将机箱盖的前边抬起，直到抬起的高度足以使机箱盖的前边缘脱离防火墙的底座。

第六步：将抬起的机箱盖，向操作者的身前方向拖动，直到机箱盖前边缘上与防火墙前面板咬合的小突起从前面板中分离出来。之后将拆开的机箱盖放到不影响操作的地方。



(1) 从此处拆卸螺钉（6 个）

(2) 沿安装口拔出

图6-1 打开机箱盖示意图



警告：

- 请勿轻易进行防火墙的硬件更换，如有必要，最好在技术支持人员的指导下操作。
- 在防火墙机箱盖的一个安装螺钉上封有 H3C 公司的防拆标签，当代理商对防火墙进行维护时，要求所维护防火墙的防拆标签完好，所以，用户在打开防火墙机箱盖前，请先与本地代理商联系，获得允许；否则，由于擅自操作带来的防火墙无法维护，将由用户本人负责。
- 进行防火墙硬件维护时，请一定要确认已经关闭与防火墙相连的所有电源，否则可能导致操作人员触电或设备的损坏。
- 进行防火墙硬件维护时，必须佩带防静电手腕，确保防静电手腕与操作者的皮肤良好接触。
- 如需更换内存条，必须使用 H3C 公司提供的内存条，否则可能造成设备无法正常使用。

6.3 更换 DDR SDRAM

防火墙存储介质的种类及用途描述如下：

- **DDR SDRAM：** 防火墙程序在 DDR SDRAM 中运行。
- **Flash Memory：** 用于保存防火墙程序、配置文件等。
- **Boot ROM：** 用于保存防火墙的启动、初始化程序。

防火墙存储介质的硬件维护主要指的是内存条（DDR SDRAM）的更换。

内存条的更换方法，遵循如下流程：

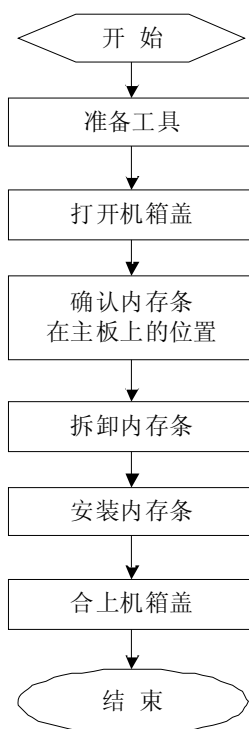


图6-2 内存条维护流程

内存条是防火墙中可由用户根据需要升级或替换的主板部件。用户在以下两种情况下可能需要升级内存：

- 用户升级主机程序时可能需要增加内存。
- 防火墙维护的路由表容量过大，或者由于其它需要耗费大量内存的工作导致需要增加内存。

当用户启动防火墙的时候，可以看到下面的提示信息：

```

*****
*                                     *
*   H3C SecPath Series Gateway Boot ROM V1.17   *
*                                     *
*****
  
```

Copyright(C) 2004-2007 by Hangzhou H3C Technologies Co.,Ltd.
Compiled at Wed Apr 12 17:39:36 CST 2006

```

Testing memory...OK!
512M bytes DDR SDRAM Memory
16M bytes Flash Memory
Hardware Version is 2.0
CPLD Version is 1.0
  
```

Press Ctrl-B to enter Boot Menu

其中“512M bytes DDR SDRAM”，表示用户使用的防火墙中安装了 512M DDR SDRAM。

 说明：
内存条插槽的插装次数是有寿命限制的，使用中请注意。

6.3.1 内存条在主板上的位置

进行拆装内存条时，请先确认所选防火墙的主板类型及其内存条的确切位置。防火墙使用的内存条类型及配置方法请参考下表。

表6-1 防火墙内存配置说明表

项目	防火墙
内存条类型	DDR SDRAM
可识别单条内存最大容量（MB）	512
扩展限制	扩展内存时，最大可扩展到 1GB。

防火墙内存条插槽在主板上的具体位置如下：

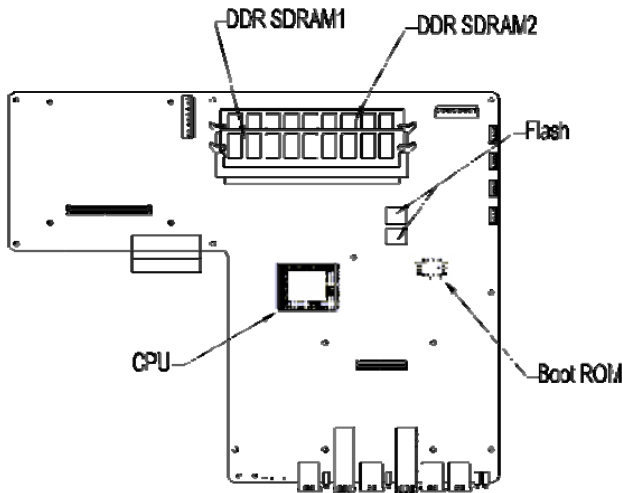


图6-3 内存条在主板上的位置示意图

为了保证内存条的插入方向正确，设计者在内存条的底部设计了一个定位凹槽，主板上的内存条插槽在相应的位置上有一个与之配合的凸起。

6.3.2 拆卸内存条

第一步：按照上图确定内存条在主板上的位置。

第二步：向外摺内存条插槽两端的锁紧弹簧夹。当施加的力度合适时，内存条从插槽中弹出。

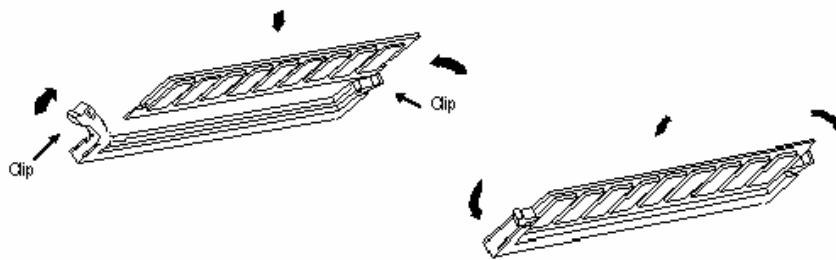


图6-4 内存条拆装示意图

第三步：捏住内存条的非导电边缘，将内存条从插槽中拿出。将取出的内存条放到防静电袋中，以免遭受静电引起的损坏。



注意：

- 只能在内存条的非导电边缘上拿捏内存条。因为内存条容易受静电影响，有可能由于操作者的不当操作导致其损坏。
- 拆卸内存条时，感觉比较费力是正常现象，请不要在操作中用力过猛。
- 不要用手直接接触内存条表面元件。
- 图 6-3 中DDR SDRAM1/DDR SDRAM2 无基本内存条、扩展内存条之分，图中标识仅为说明主板上插有两片内存条。

6.3.3 安装内存条

第一步：参照图 6-3，确定内存条在主板上的位置。

第二步：捏住内存条顶部的非导电边缘，将内存条放置在内存条插槽中。

第三步：在内存条的顶部施加适度压力将内存条压入插槽中，同时向内摺插槽两端的锁紧弹簧夹。当力度合适时，锁紧弹簧夹向中间合拢，两端弹簧夹上的凸起与内存条两侧半圆形定位凹陷相吻合。

请按照上面的方法安装好所有的内存条。

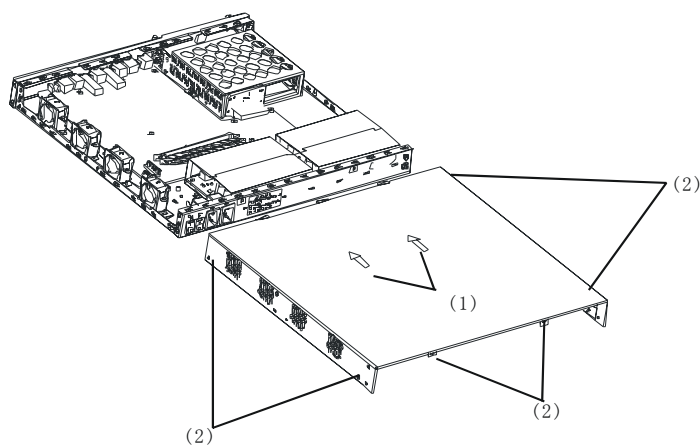
6.4 合上防火墙机箱盖

第一步：将防火墙放置于平台上，使得防火墙的后面板面对操作者。

第二步：端住防火墙的机箱盖，使机箱盖上的小凸起与防火墙底座边缘平齐。

第三步：将机箱盖向后推，使机箱盖上的凸起与防火墙底座前面板咬合，同时防火墙前面板上的凸起与机箱盖咬合。

第四步：将机箱盖放低到防火墙底座上，使得机箱盖侧面上的凸起与防火墙底座侧面板咬合，同时防火墙侧面板上的凸起与机箱盖咬合。



(1) 沿安装口插入

(2) 从此处安装螺钉（6 个）

图6-5 合上机箱盖示意图

第五步：用在6.2 小节“打开防火墙机箱盖”第三步、第四步中卸下的六颗螺钉将机箱盖固定在防火墙底座上。

6.5 MIM 多功能接口模块的更换

参见《第 8 章 MIM多功能接口模块》。

第7章 安装故障处理

7.1 电源系统问题故障处理

(1) 故障现象

电源指示灯 PWR0/PWR1 不亮。

(2) 故障处理

请进行如下检查：

- 防火墙电源开关是否打开。
- 防火墙供电电源开关是否打开。
- 防火墙电源线是否连接正确。
- 防火墙供电电源与防火墙所要求的电源是否匹配。



注意：

请不要带电插拔电源线。如完成上述的检查工作后，电源指示灯 PWR0/PWR1 仍未变亮，请与代理商联系。

7.2 配置系统故障处理

防火墙上电后，如果系统正常，将在配置终端上显示启动信息；如果配置系统出现故障，配置终端可能无显示或者显示乱码。

1. 终端无显示故障处理

(1) 故障现象

防火墙上电后，配置终端无显示信息。

(2) 故障处理

第一步：首先要做以下检查：

- 电源系统是否正常。
- 配置口（Console）电缆是否正确连接。

第二步：如果以上检查未发现问题，很可能是配置电缆的问题或者终端（如超级终端）参数的设置错误，请进行相应的检查。

2. 终端显示乱码故障处理

(1) 故障现象

防火墙上电启动后，配置终端上显示乱码。

(2) 故障处理

请确认终端（如超级终端）的参数设置：波特率为 9600，数据位为 8，奇偶校验为无，停止位为 1，流量控制为无，终端仿真为 VT100。如参数设置与上不符，请重新配置。

7.3 应用软件升级故障处理

1. 故障 1

(1) 故障现象

启动防火墙，用 TFTP 方式升级 Comware 软件，结果显示如下：

```
Net Port Download Menu:
```

```
1: Change Net Parameter
2: Download From Net
3: Exit to Main Menu
Enter your choice(1-3): 2
```

```
Starting the TFTP download...
```

```
Failed to connect the tftp server!!
Please check the network setting!!
```

(2) 故障处理

以上故障的产生是由于 TFTP Server 程序没打开或以太网连接出现故障(包括 IP 地址设置不正确、网线没插好等)，从而造成无法连接 TFTP Server。请打开 TFTP Server 程序并确定 IP 地址等参数设置正确且网线已经插好。

2. 故障 2

(1) 故障现象

启动防火墙，用 TFTP 方式升级 Comware 软件，结果显示如下：

```
Net Port Download Menu:
```

```
1: Change Net Parameter
2: Download From Net
3: Exit to Main Menu
Enter your choice(1-3): 2
```

```
Starting the TFTP download...
```

```
Failed to find the updated file  
Please check the network setting!!
```

(2) 故障处理

以上故障的产生是由于所下载的文件不存在或文件路径设置不正确，请确定所需要下载的文件位于 **TFTP Server** 所指定的目录。

3. 故障 3

(1) 故障现象

启动防火墙，用 TFTP 方式升级 Comware 软件，结果显示如下：

```
Net Port Download Menu:
```

```
1: Change Net Parameter  
2: Download From Net  
3: Exit to Main Menu  
Enter your choice(1-3): 2
```

```
Starting the TFTP download...
```

```
The downloaded software is not a valid version.  
Please download the correct version.
```

(2) 故障处理

以上故障的产生是由于下载的程序版本有误，无法通过版本检测。请确定应用程序版本正确无误。

说明：

防火墙主机及智能接口卡上均贴有包含相关生产维修信息的条形码，如用户需要返修设备，请将故障设备的条形码反馈给代理商。

第8章 MIM 多功能接口模块

8.1 MIM 多功能接口模块的种类

H3C SecPath 系列防火墙支持多种多功能接口模块（MIM），目前 H3C SecPath F1000-S 防火墙可支持的类型如下：

- 1 端口 10Base-T/100Base-TX 快速以太网接口模块（1FE）
- 2 端口 10Base-T/100Base-TX 快速以太网接口模块（2FE）
- 4 端口 10Base-T/100Base-TX 快速以太网接口模块（4FE）
- 1 端口 10Base-T/100Base-TX/1000Base-T 以太网接口模块(1GBE)
- 2 端口 10Base-T/100Base-TX/1000Base-T 以太网接口模块(2GBE)
- 1 端口 1000Base-LX/1000Base-SX 以太网光接口模块（1GEF）
- 2 端口 1000Base-LX/1000Base-SX 以太网光接口模块（2GEF）
- SSL（Security Socket Layer，安全套接层）是安全套接层加密模块

8.2 MIM 多功能接口模块的安装与拆卸



注意：

MIM 多功能接口模块拉手条上的簧片对防火墙整机的电磁屏蔽有特殊的效果，用户在拆换接口模块的过程中，请保证簧片的完整，切不可将簧片去掉。

进行接口模块安装时，请仔细阅读《第 2 章 安装前的准备工作》。

1. 安装工具

- 防静电手腕

2. MIM 接口模块的安装



警告：

进行以下任何操作之前，请一定要确认已经关闭与防火墙相连的所有电源，否则可能导致操作人员触电或设备的损坏。

第一步：将防火墙的前面板面对操作者。

第二步：关掉电源并拔掉电源线。

第三步：选择标记有 **SLOT** 的插槽并将接口模块向防火墙内部推进，直到与防火墙前面板紧密接触为止。

第四步：拧紧松不脱螺钉，将接口模块固定在防火墙上。

第五步：打开防火墙电源开关，并检查防火墙上的 **ACT** 指示灯是否正常闪烁，灯闪烁表示接口模块已经正确安装。

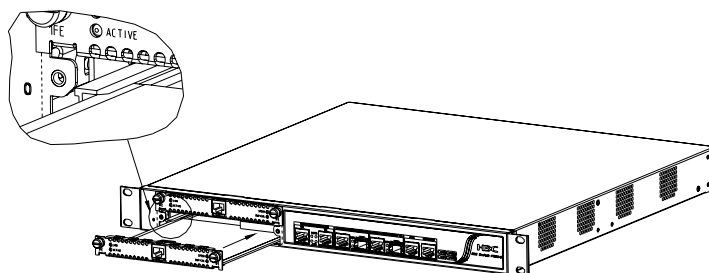


图8-1 MIM 多功能接口模块安装示意图 1

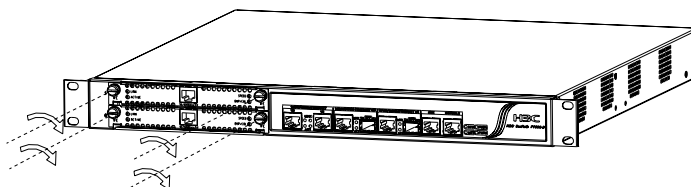


图8-2 MIM 多功能接口模块安装示意图 2

3. MIM 接口模块的拆卸

第一步：将防火墙的前面板面对操作者。

第二步：关掉电源并拔掉电源线。

第三步：拔掉防火墙前面板上所有接口模块的接口电缆。

第四步：松开接口模块两侧的松不脱螺钉。

第五步：将接口模块向操作者身前方向拖动，直到完全脱离防火墙底座为止。



注意：

拆卸 MIM 接口模块时，应注意如下事项：

- 若 MIM 接口模块拆卸完成后无须安装新的接口模块，请及时安装空挡板，以防止灰尘进入，并保证防火墙的正常通风；
- 拆卸 MIM 接口模块时，请与工作间的过道保持一定距离，防止过往人员碰掉拆卸的模块或在拆卸过程中由于碰撞导致事故。

8.3 MIM 接口模块的故障处理

H3C SecPath 系列防火墙的 MIM 接口模块面板为用户提供有指示灯，用户可以根据指示灯的状态来判断接口模块安装是否正确。

若防火墙的接口模块出现工作异常，可按照如下方法来检查：

- 检查接口电缆，判断电缆是否选配正确。
- 观察各接口模块指示灯，判断接口模块工作是否正常。
- 根据配置中的 **display** 命令显示，判断接口是否接受配置，正常工作。

8.4 1FE/2FE/4FE 接口模块

8.4.1 简介

1FE/2FE/4FE 是 1/2/4 端口 10Base-T/100Base-TX 快速以太网接口模块的简称，其中 FE（Fast Ethernet）是快速以太网的英文缩写。FE 接口模块主要用于完成防火墙与局域网的通信。

防火墙包含三种型号的 FE 接口模块：1FE、2FE、4FE。

1FE 模块、2FE 模块、4FE 模块的区别在于：

- 1FE 接口模块提供 1 个 10/100Mbps 以太网 RJ45 接口。
- 2FE 接口模块提供 2 个 10/100Mbps 以太网 RJ45 接口。
- 4FE 接口模块提供 4 个 10/100Mbps 以太网 RJ45 接口。

FE 接口模块支持功能如下：

- 当用户采用 5 类双绞线时，可支持 100 米的传输距离。
- 接口可以工作在 100Mbps、10Mbps 两种速率下，且能实现自适应。
- 接口有全双工和半双工两种工作方式，且全双工是比较常用的工作方式。

8.4.2 接口模块外观

1. 1FE 接口模块外观

1FE 接口模块外观如下图所示：

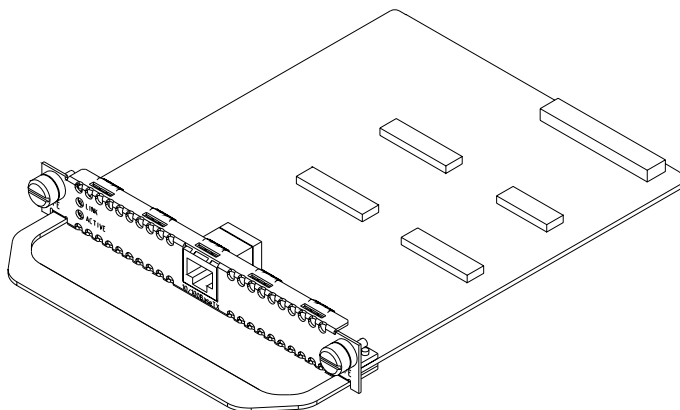


图8-3 1FE 接口模块外观

2. 2FE 接口模块外观

2FE 接口模块外观如下图所示：

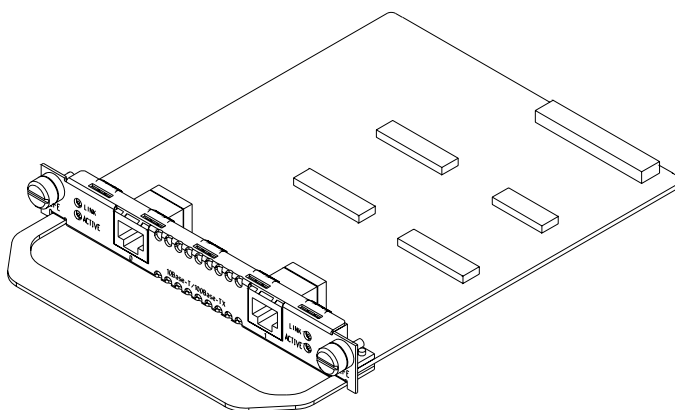


图8-4 2FE 接口模块外观

3. 4FE 接口模块外观

4FE 接口模块外观如下图所示：

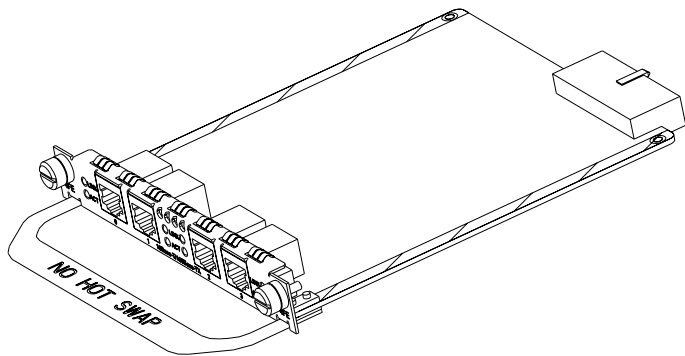


图8-5 4FE 接口模块外观

8.4.3 接口属性

1FE、2FE、4FE 接口属性如下表所示：

表8-1 1FE/2FE/4FE 模块接口属性

属性	描述		
	1FE 模块	2FE 模块	4FE 模块
连接器类型	RJ45		
连接器数量	1	2	4
电缆类型	标准以太网线		
工作方式	全双工/半双工 10M/100Mbps 自适应		
支持帧格式	Ethernet_II Ethernet_SNAP		

8.4.4 面板及接口指示灯

1FE 接口模块的面板如下图所示：

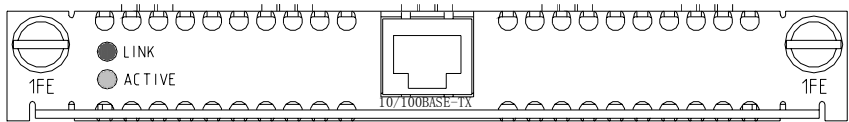


图8-6 1FE 接口模块面板

2FE 接口模块的面板如下图所示：

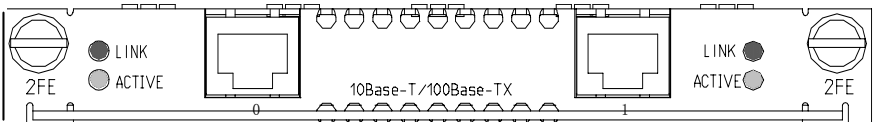


图8-7 2FE 接口模块面板

4FE 接口模块的面板如下图所示：

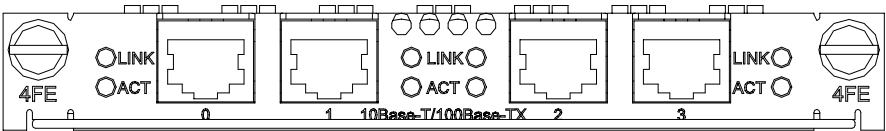


图8-8 4FE 接口模块面板

1FE/2FE/4FE 接口模块面板上的指示灯含义如下：

表8-2 1FE/2FE/4FE 接口模块指示灯含义

指示灯	含义
LINK	灯灭表示链路没有连通，灯亮表示链路已经连通。
ACTIVE	灯灭表示没有数据收发，灯闪烁表示有数据收发。

8.4.5 接口连接电缆

1. 以太网电缆外观

FE 接口电缆为带 RJ45 接头（参见下图）的 5 类双绞线电缆，其接口的 1、2 管脚为发送端，3、6 管脚为接收端。

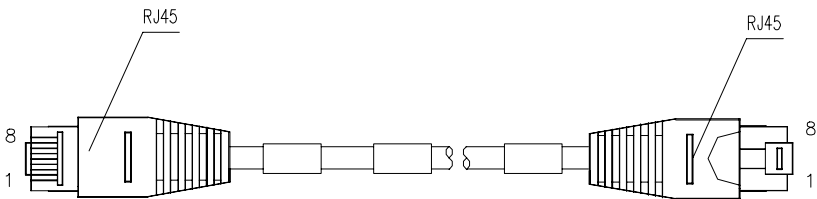


图8-9 以太网电缆

2. 以太网电缆的制作

下图为采用 5 类双绞线制作 RJ45 接头的以太网线缆示例，供用户使用时参考。5 类双绞线有 8 芯细线组成，利用细线外绝缘层上的颜色进行分组标识。通常利用单色和单色加上白色作为成对标识，也有利用色点成对进行标识的，本示例采用前者。

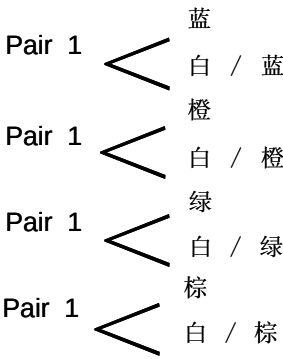


图8-10 5类双绞线示例图

表8-3 标准（直通）网线连接关系表

RJ45	信号	5类双绞线	信号方向	RJ45
1	TX+	白（橙）	→	1
2	TX-	橙	→	2
3	RX+	白（绿）	←	3
4	-	蓝	-	4
5	-	白（蓝）	-	5
6	RX-	绿	←	6
7	-	白（棕）	-	7
8	-	棕	-	8

表8-4 交叉网线连接关系表

RJ45	信号方向	5类双绞线	信号方向	RJ45
1	TX+	白（橙）	→	3
2	TX-	橙	→	6
3	RX+	白（绿）	←	1
4	-	蓝	-	4
5	-	白（蓝）	-	5
6	RX-	绿	←	2
7	-	白（棕）	-	7
8	-	棕	-	8

因使用情况不同又可将以太网线分为标准网线（即直通网线）和交叉网线两种，分别介绍如下：

- 标准网线：又称直通网线，两端 RJ45 接头压接的双绞线的线序完全相同，用于终端设备（如 PC、路由器等）到 HUB 或 LAN Switch 的连接。
- 交叉网线：两端 RJ45 接头压接的双绞线的线序不相同，用于终端设备（如 PC、路由器等）到终端设备（如 PC、路由器等）的连接。用户需要可以自行制作。

 说明：

用户制作网线时，请优先采用屏蔽电缆，以保证电磁兼容的需要。

8.4.6 接口电缆的连接

第一步：如果需要连接防火墙到 PC 或路由器，请使用交叉网线，连接网线的一端到防火墙 FE 接口模块的以太网口，连接另一端到 PC 或路由器；如果需要连接防火墙到 HUB 或 LAN Switch，请使用标准网线，连接网线的一端到防火墙 FE 接口模块的以太网口，连接另一端到 HUB 或 LAN Switch。

第二步：上电后请检查 FE 接口模块面板上 LINK 指示灯的状态。LINK 灯亮表示链路已经连通，LINK 灯灭表示链路没有连通，请检查线路。



注意：

连接时请认准接口上的标识，以免误插入其它接口，导致接口模块或防火墙主机的损坏。

8.5 1GBE/2GBE 模块

8.5.1 模块简介

1GBE/2GBE 是 1/2 端口 10Base-T/100Base-TX/1000Base-T 以太网接口模块的简称，其中 GBE（Gigabit Ethernet）是千兆以太网的英文缩写。GBE 模块主要用于完成防火墙与局域网的通信。

GBE 模块支持功能如下：

- 当用户采用 5 类双绞线时，可支持 100 米的传输距离。
- 接口可以工作在 1000Mbps、100Mbps 和 10Mbps 三种速度下，且能实现自适应。
- 支持全双工工作方式。

8.5.2 模块外观

1. 1GBE 接口模块外观

1GBE 模块外观如下图所示：

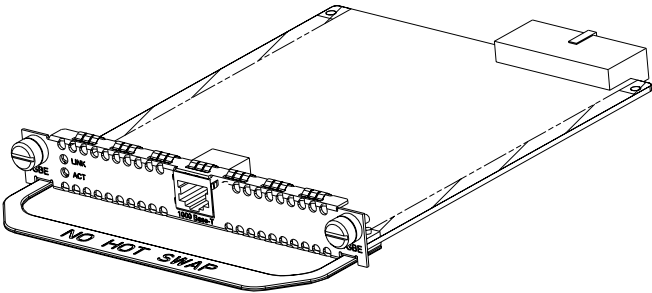


图8-11 1GBE 模块外观

2. 2GBE 接口模块外观

2GBE 模块外观如下图所示：

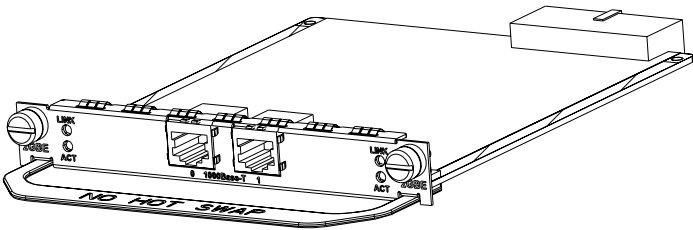


图8-12 2GBE 模块外观

8.5.3 模块接口属性

1GBE/2GBE 模块接口属性如下表所示：

表8-5 1GBE 模块接口属性

属性	1GBE 描述	2GBE 描述
连接器类型	RJ45	
连接器数量	1	2
接口类型	MDI/MDIX	
接口标准	802.3, 802.3u 和 802.3ab	
电缆类型	以太网线	
工作方式	10/100/1000Mbps 自适应 半双工/全双工自动协商	

8.5.4 模块接口指示灯

1GBE/2GBE 模块的面板如下图所示：

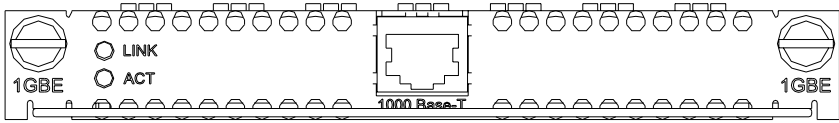


图8-13 1GBE 模块面板

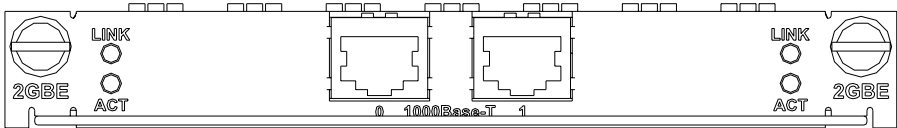


图8-14 2GBE 模块面板

1GBE/2GBE 模块面板上的指示灯含义如下：

表8-6 1GBE 模块指示灯含义

指示灯	含义
LINK	灯灭表示链路没有连通，灯亮表示链路已经连通。
ACT	灯灭表示没有数据收发，灯闪烁表示有数据收发。

8.5.5 模块接口连接电缆

1. 以太网电缆外观

1GBE 模块接口电缆为带 RJ45 接头（参见下图）的 5 类双绞线电缆，其接口的 1、2 管脚为发送端，3、6 管脚为接收端。

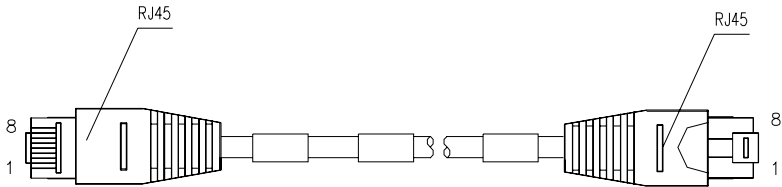


图8-15 以太网电缆

2. 以太网电缆的制作

下图为采用 5 类双绞线制作 RJ45 接头的以太网线缆示例，供用户使用时参考。5 类双绞线有 8 芯细线组成，利用细线外绝缘层上的颜色进行分组标识。通常利用单色和单色加上白色作为成对标识，也有利用色点成对进行标识的，本示例采用前者。

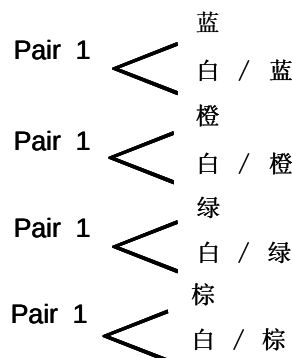


图8-16 5类双绞线示例图

因使用情况不同又可将以太网线分为标准网线（即直通网线）和交叉网线两种，分别介绍如下：

- 标准网线：又称直通网线，两端 RJ45 接头压接的双绞线的线序完全相同，用于终端设备（如 PC、路由器等）到 HUB 或 LAN Switch 的连接。
- 交叉网线：两端 RJ45 接头压接的双绞线的线序不相同，用于终端设备（如 PC、路由器等）到终端设备（如 PC、路由器等）的连接。

以太网电缆的管脚连接关系请参见《中低端系列路由器 电缆手册》。

8.5.6 模块接口电缆的连接

第一步：如果需要连接防火墙到 PC 或路由器，请使用交叉网线，连接网线的一端到防火墙的以太网口，连接另一端到 PC 或路由器；如果需要连接防火墙到 HUB 或 LAN Switch，请使用标准网线，连接网线的一端到防火墙的以太网口，连接另一端到 HUB 或 LAN Switch。

第二步：上电后请检查防火墙前面板上对应槽位的指示灯，灯亮表示模块自检完成，可以正常工作；灯灭表示插上模块后自检不通过，请与代理商联系。

第三步：上电后请检查 GBE 模块面板 LINK 指示灯状态。LINK 灯亮表示链路已经连通，LINK 灯灭表示链路没有连通，请检查线路。

8.6 1GEF/2GEF 模块

8.6.1 模块简介

1GEF/2GEF 是 1/2 端口 1000Base-LX/1000Base-SX 以太网光接口模块的简称，其中 GE (Gigabit Ethernet) 是千兆以太网的英文缩写，F 为 Fiber，表示光接口。GEF 模块主要用于完成防火墙与局域网的通信。

GEF 模块支持功能如下：

- 提供 5 种类型的 1000Base-LX/SX SFP 可插拔光接口模块，包括短距多模（850nm）光模块、中距单模（1310nm）光模块、长距单模（1310nm）光模块、长距单模（1550nm）光模块、超长距离单模（1550nm）光模块，用户可根据自己的需要选购。
- 接口工作在 1000Mbps 速率下。
- 支持全双工工作方式。

8.6.2 模块外观

1. 1GEF 接口模块外观

1GEF 模块外观如下图所示：

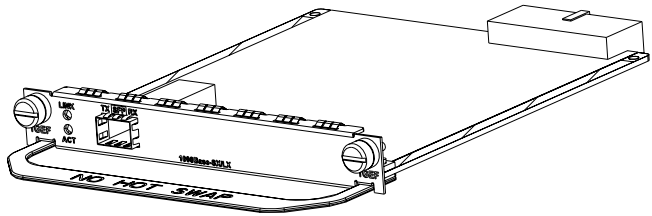


图8-17 1GEF 模块外观

2. 2GEF 接口模块外观

2GEF 模块外观如下图所示：

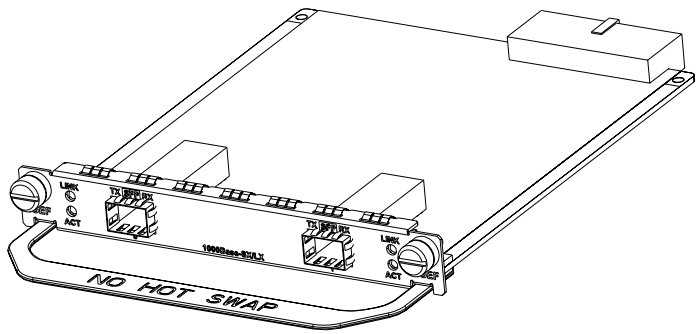


图8-18 2GEF 模块外观

8.6.3 模块接口属性

1GEF/2GEF 模块接口属性如下表所示：

表8-7 1GEF/2GEF 模块接口属性

属性	1GEF 描述	2GEF 描述
连接器类型	SFP/LC	
接口数量	1	2

属性		1GEF 描述		2GEF 描述		
接口标准		802.3, 802.3u 和 802.3ab				
发送光功率	类型	短距多模 (850nm) 光接口模块	中距单模 (1310nm) 光接口模块	长距 (1310nm) 光接口模块	长距 (1550nm) 光接口模块	超长距离 (1550nm) 光接口模块
	最小	-9.5dBm	-9dBm	-2dBm	-4dBm	-4dBm
	最大	0dBm	-3dBm	5dBm	1dBm	2dBm
接收灵敏度		-17dBm	-20dBm	-23dBm -	-21dBm	-22dBm
中心波长		850nm	1310nm	1310nm	1550nm	1550nm
光纤类型		62.5/125 μ m 多模光纤	9/125 μ m 单模光纤	9/125 μ m 单模光纤	9/125 μ m 单模光纤	9/125 μ m 单模光纤
最大传输距离		0.55km	10km	40km	40km	70km
工作方式		1000Mbps 全双工模式				

说明：
当使用光模块时，请选用经过我司认证的光模块。

8.6.4 模块接口指示灯

1GEF 模块的面板如下图所示：

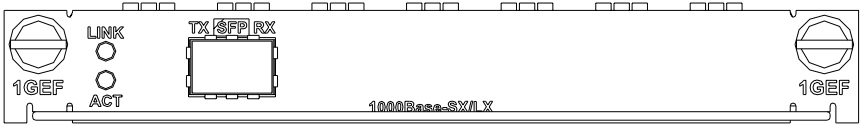


图8-19 1GEF 模块面板

2GEF 模块的面板如下图所示：

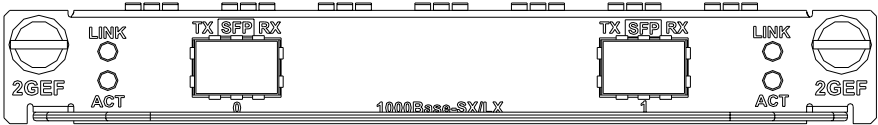


图8-20 2GEF 模块面板

1GEF/2GEF 模块面板上的指示灯含义如下：

表8-8 1GEF 模块指示灯含义

指示灯	含义
LINK	灯灭表示链路没有连通，灯亮表示链路已经连通。
ACT	灯灭表示没有数据收发，灯闪烁表示有数据收发。

8.6.5 模块接口连接光纤

对于 1GEF/2GEF 模块，用户可根据所选用的 1000Base-SX/1000Base-LX SFP 可插拔光接口模块的类型来选择相应的光纤。这几种光模块的光接口均为 LC 型光纤连接器，故要求用户使用带有 LC 型光纤连接器的光纤。

说明：

LC 型光纤连接器为朗讯公司开发的一种小型光纤连接器，采用推拔按钮式安装。光纤为选配，用户在购买接口模块时必须预先指明选配的 SFP 模块，否则不予提供相应的光纤。

8.6.6 模块接口光缆的连接



注意：

连接光纤时，应注意如下事项：

- 不允许过度弯折光纤，其曲率半径应不小于 10cm；
- 保证接口的 Tx 与 Rx 端连接正确；
- 保证光纤端面处的清洁度。



警告：

激光危险！不要用眼睛直接观察与激光器相连的光纤连接器，否则可能对眼睛造成伤害。

第一步：将 SFP 模块插入相应的 SFP 模块插槽。

第二步：确认 GEF 接口上的 Rx 和 Tx 光接口，并将光纤一端插入 Rx 口，另一端连至对端设备的 Tx 口；将另一根光纤的一端插入 Tx 口，另一端连至对端设备的 Rx 口。

第三步：上电后请检查防火墙前面板上对应槽位的指示灯，灯亮表示模块自检完成，可以正常工作，灯灭表示插上模块后自检不通过，请与代理商联系。

第四步：检查 GEF 接口 LINK 指示灯的状态。LINK 灯亮表示 Rx 链路已经连通，LINK 灯灭表示 Rx 链路没有连通，请检查线路。

8.7 SSL 模块

8.7.1 模块简介

SSL（Security Socket Layer，安全套接层）是安全套接层加密模块的简称。SSL 加密模块支持 SSL 协议，通过硬件加速 SSL 协议的处理，支持多种硬件加/解密和散列运算，提供了高性能、高可靠性的加密特性。

SSL 加密模块可安装于部分 SecPath 系列安全产品的 MIM 插槽上，当插入 SSL 模块时，设备主板完成报文收发和 SSL 的协议处理，由加密卡完成 SSL 报文的加/解密工作。

8.7.2 模块外观

SSL 模块外观如下图所示：

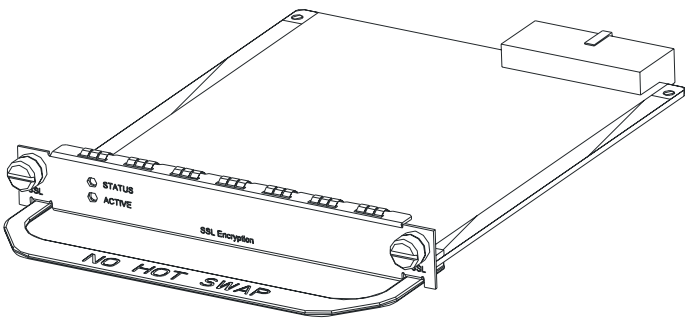


图8-21 SSL 模块外观

8.7.3 模块属性

表8-9 SSL 模块属性

属性	描述
支持的协议	SSL
硬件实现算法	密钥算法（DES、3DES、AES、RC4） 验证算法（HMAC-MD5，HMAC-SHA-1）

8.7.4 模块运行指示灯

安全套接层加密模块前面板如图所示：

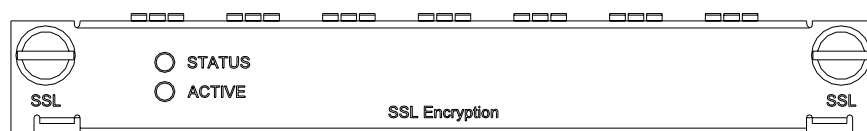


图8-22 SSL 模块面板

表8-10 SSL 模块指示灯含义

指示灯	含义
STATUS	常亮（绿色）：表示模块上电正常 灭：表示模块没有加电，模块电源不工作或严重硬件故障
ACTIVE	闪烁（黄色）2 秒钟后灯灭：表示模块初始化完成 连续闪烁：表示模块正常运行，且与主机之间有数据收发 灭：表示模块正常运行，与主机之间无数据收发

8.7.5 模块故障排除

(1) 故障 1：开机后 STATUS 灯常灭。

排除：开机后 STATUS 灯应保持常亮。一直没有亮，说明模块或模块上的某些硬件没有正常加电。请您检查整机电源是否连接正确。

如果整机电源已经工作，可能模块的电源损坏，也可能 CPLD（Complex Programmable Logic Device）工作不正常，请与 H3C 公司代理商联系。

(2) 故障 2：开机过程中 ACTIVE 灯常灭。

排除：开机过程中，ACTIVE 灯应该闪烁 2 秒钟，然后熄灭，这表明模块的加密处理器已经配置完成，准备工作。如果在开机过程中 ACTIVE 灯保持常灭，即模块处理器初始化配置失败，说明可能是系统总线没有正常工作。请您检查模块是否和主机插接完好，如果插接完好，则可能是主机或模块存在问题，请与 H3C 公司代理商联系。

(3) 故障 3：模块运行中 ACTIVE 灯常亮或常灭。

排除：模块在运行加密业务时 ACTIVE 灯应闪烁，常亮或常灭说明可能是系统总线没有正常工作。请您检查模块是否和主机插接完好，如果插接完好，说明是主机或模块存在问题，请与 H3C 公司代理商联系。