网络卫士防火墙
系统安装手册

北京天融信公司

Beijing Topsec Co., Ltd.

版权声明:

商标声明:

防火墙版本号：V2.4.80

发布日期：2004 年 9 月

文档版本号：V1.6

发布日期：2004 年 9 月

TopSEC®天融信

天融信技术支持信息

技术支持	电话	传真	E-mail
北京总部	010-82611122 800-810-5119	010-62304552	support@topsec.com.cn
上海天融信	021-58395230	021-38890477	shanghai@topsec.com.cn
成都天融信	028-85183688	028-85138161	xiaobo_zou@163.net
武汉天融信	027-87522653	027-87522653-2698	whtit_m@mail.hust.edu.cn
深圳天融信	0755-83692433	0755-83692229	jingquan@guo.com.cn
山东天融信	0531-8111395／96／97／98	0531-8111395	sdtrx@263.net
长沙天融信	0731-5214069	0731-5234975	libin0731@vip.sina.com
广州天融信	020-38732900／01／02	020-38732900-200	guangzhou@topsec.com.cn
西北办事处	029-85365686	029-85365686	xibei@topsec.com.cn
江西办事处	0791-6284762	0791-6284762	keke2008@vip.sina.com
安徽办事处	0551-3636778	0551-3636778	ahtrx@263.net
浙江办事处	0571-85021571	0571-85021400	zhejiang@topsec.com.cn
江苏办事处	025-3201127	025-3201127	jstalentit@163.net
福建办事处	0591-3330955／56	0591-3338039	lbp823@163.com
重庆办事处	023-68698713	023-68698713	cdxiechao@263.com
兰州办事处	0931-4611097	0931-4611097	hexg@topsec.com.cn
宁夏办事处	0951-6020875	0951-6020875-801	Qiao_jun@topsec.com.cn

甘肃办事处	0931-4611097		shichaohui@topsec.com.cn
新疆办事处	0991-5877365	0991-5877177	lovelsg@sina.com
云南办事处	0871-3197265	0871-3197265	jordanwang99@163.com
贵州办事处	0851-5213245	0851-5213245	lyl@topsec.com.cn
辽宁办事处	024-62124208	024-62124209	kz@topsec.com.cn
吉林办事处	0431-5674800	0431-5643077	wyuangui@sohu.com
广西办事处	0771-2203096	0771-2203095	kuangfong25@163.com
内蒙天大天财	0471-4914996	0471-4914995	jwk2000@163.com
郑州办事处	0371-5333434/5/6	0371-5333435	Li_guochang@topsec.com.cn
山西友信	0351-6197997-98	0351-6820100	sxyouxin@sina.com
太原办事处	0351-4695661	0351-4695662	lx@topsec.com.cn
北京原创鑫	010-82863981	010-82863981-22	dqliangmail@yahoo.com.cn
天津原创鑫	022-23364859	022-23364859	dqliangmail@yahoo.com
河北原创鑫	0311-3993182	0311-3993182	dqliangmail@yahoo.com

目 录

2.4.80 版

一.TOPSEC 防火墙安装指南

1 概 要

系统安装说明提供如下主要内容:

- 防火墙系统的构成
- 系统的主要使用方案
- 系统安装工程人员快速将防火墙系统安装到目标网络的基本方法和步骤
- 系统管理员对防火墙的基本管理方法和过程
- 提供一在典型的防火墙应用方案中的防火墙安装案例

2 系统组成与规格

2.1 产品型号说明

2.1.1 型号定义

NGFW4000-UF/E/S/T-VPN(E/S)
NGFWARES-S/M-VPN(E/S)

2.1.2 型号说明

NGFW：是网络卫士防火墙的英文简称;
4000：表示该设备是 4000 防火墙;
ARES：表示该设备是 ARES 防火墙;
UF：表示防火墙为千兆防火墙;
E：表示防火墙是百兆企业版类型的;
S：表示防火墙是百兆小型版类型的；（此处无参数则表示防火墙是百兆标准版类型的）
T：表示防火墙为电口型防火墙;
M：表示防火墙为桌面型防火墙;
VPN：表示该防火墙包含 VPN 模块；（此处无参数则表示防火墙没有 VPN 模块）
（E）：表示 VPN 模块使用硬件加密卡;
（S）：表示 VPN 模块使用软加密;
如：NGFW4000-E-VPN(E)
该型号为：网络卫士防火墙 4000 百兆企业版，包含 VPN 模块，使用硬件加密卡进行加密通信。
各型号机箱宽度尺寸均为 19 吋（NGFWARES-S 型号除外）。

2.2 通用型号防火墙

2.2.1 型号标识

NGFW4000

2.2.2 装箱单

防火墙设备:1 台;
安装光盘:1 张;
电源线：1 条;
直通网络线:1 条;
交叉网络线:1 条;
串口控制线:1 条;
上架支架:1 套;
《客户回执信封》：1 个;
《产品保修卡》：1 份;
《装箱单》：1 份;
《产品安装调试验收单》：1 份;
《用户意见反馈表》：1 份

2.2.3 系统组成

2.2.3.1 防火墙设备（硬件）

包括 1U 设备机箱和标准数量的 3 个百兆以太网络接口,防火墙软件包括标准配置的软件模块;

2.2.3.2 管理器（软件）

一个集中式防火墙专用管理软件，运行于中文 Windows98、WindowsNT4.0、Windows2000、WindowsXP 环境下;

2.2.3.3 认证客户端（软件）

一个防火墙客户认证专用软件，运行于中文 Windows98、WindowsNT4.0、Windows2000、WindowsXP 环境下；目前支持的认证数据库有：Radius、TACACS+、VieCA、RSA SecuID。

2.2.4 硬件配置

2.2.4.1 接口数量

标配：三个百兆接口，最大可以扩展到七个百兆口
一个 Console 口
一个 AUX 口

2.2.4.2 接口规范

百兆网络接口：10/100Base-TX
Console 口：RS232C，DTE，9600-8-N-1

2.2.5 电气特性

2.2.5.1 电源

技术参数：AC90~260V ,47~63HZ，2.0A（最大），100W（最大）

安规标准：

美国：FCC CFR 47 Part 15 (B 级)
欧洲/CE 标志：EN55022&EN55024

2.2.5.2 环境规范

运行温度：0 ～ 45 摄氏度
非运行温度：-20 ～ 65 摄氏度
相对湿度：10 ～ 90%@40 摄氏度，非冷凝

2.2.6 几何规格

2.2.6.1 适用机架

标准 19 吋机架

2.2.6.2 几何尺寸

百兆：430(长)X290（深）X44.45（高）（mm）

千兆：430(长)X390（深）X88.90（高）（mm）

- 注：
- 其中高度为未安装脚垫时尺寸；
- 长度尺寸为未安装上架支架情况，上架支架安装后，其长度尺寸为标准 19 吋机柜尺寸；

2.3 执行标准

GB/T 18019-1999
GB/T 18020-1999
TCP/IP 相关 RFC

2.4 安全规范及标准

GJB151A-97：
CS101
CS114
RS103
RE102
CE102

2.5 系统性能说明

产品型号：FW4000　　版本号：2.4.80

最大吞吐率：100M

平均延时：35us

NAT 时对内部 IP 地址的数目没有限制

NAT 连接数量：32,000 连接/1 个 NAT 地址

访问控制规则数量最大：10240 记录（包括对象记录）

各型号防火墙的详细性能指标请见《天融信网络卫士防火墙技术白皮书》。

3 基本使用方案

3.1 当前运行网络中添加防火墙

3.1.1 应用环境描述

防火墙的应用目标网络为一已经建立并正在运行的网络，此类网络的防火墙应用往往要求尽可能少改动或不许可改动网络接点的任何属性，并要求防火墙的接入对网络通信的中断时间最小，基本做到系统应用不敏感；
此类型网络是在保障正常网络业务应用基础上，逐步严格强化网络通信行为和提高网络应用安全性；
此类网络应用的安全要求必须经过由宽松到严格的渐进过程，防火墙策略的制定要求有准确的应用分析调查；

3.1.2 防火墙工作模式

满足此类应用目标的最理想的防火墙工作方式为透明模式，应用系统往往对透明方式还有如下具体要求：
设备必须做到以太层透明，即防火墙设备不改变通信包的以太头，这可以避免防火墙各个防火区中应用设备的物理地址重新刷新；

3.1.3 防火墙的安装位置

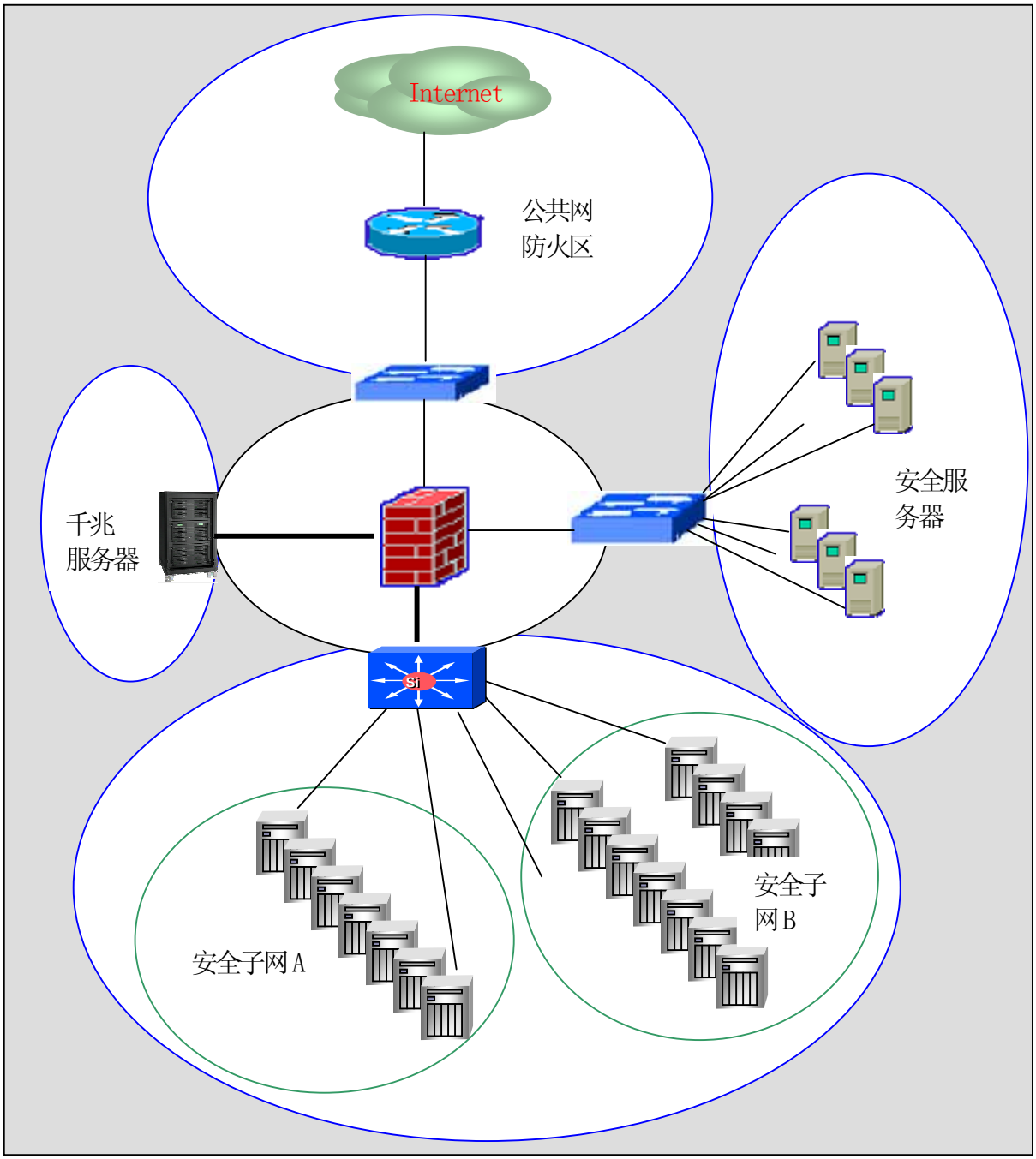
防火墙的安装位置是各个安全区的交点处，可以通过交换机或 HUB 将安全区的边界收缩为一个接点，将此接点连接于防火墙的网络接口；
防火墙的网络接口逻辑上为对等设计，接口区域属性由管理员选择设定；

- 防火墙的防火区属性直接与安全策略逻辑相关，请注意防火区与防火墙网络接口的对应关系

3.1.4 使用方案图

此方案中，防火墙的临接区在同一网段中，通过此网段，防火墙将网络空间分成 4 部分：
内部防火区；
公共防火区；
千兆服务器防火区；
安全服务器组防火区；

其中内部防火区和千兆服务器防火区使用防火墙的千兆接口。



3.2 工程网络中安装防火墙

3.2.1 应用环境描述

防火墙的安全功能和通信功能在网络初始设计中已经融入网络方案中，此类防火墙应用往往还启用了防火墙的通信功能，如路由，地址转换等。

3.2.2 防火墙工作模式

此类网络较好的防火墙工作模式为综合模式，可以同时使用防火墙的透明功能和路由功能，透明功能可以使同一网段的网络区域分布在不同的防火区中，这主要适应了基于业务的 IP 分配方案，其将同一应用业务的服务器和客户机通过同一网段连接起来，以提高整体网络的通信性能；透明模式还可以将路由信息转发到其它防火区，减少了应安全设备带来的网络管理的工作量；

防火墙的路由模式提供完整的静态路由功能，对于中小规模的内部网络，其完全可以代替内部路由器的路由功能；
该工作模式对于网络的扩展还提供了极大的支持，如原有网段主机的增加或网段增加，可以不改变网络配置或很少改变网络配置情况下完成管理；

3.2.3 防火墙的安装位置

安装位置首先考虑防火区的划分外，还需要考虑目标网络的 IP 分配和路由功能分布情况，防火墙所处的防火区边界为安全区域边界同时也是网段边界，网络间的路由在防火墙上实现；

3.2.4 使用方案图

防火墙的防火区定义及网络拓扑图同上方案
内部防火区；
公共防火区；
千兆服务器防火区；
安全服务器组防火区；

其中内部防火区和千兆服务器防火区使用防火墙的千兆接口。

防火墙的邻接网络中，公共防火区和安全服务器组防火区属于同一网段，其透明通过防火墙；
其他防火区路由方式通过防火墙；

4 系统安装

4.1 设备安装

4.1.1 支架安装

百兆防火墙外形几何尺寸为标准19吋1U机箱，可以安装固定在标准机柜中，随机附件中有一对上架支架，将其固定在防火墙设备上；

4.1.2 机柜设备托架

防火墙设备要求放在机柜的托架上，请适当调节机柜托架与防火墙的相对位置，使防火墙的固定支架在垂直方向上受力较小；

4.1.3 线缆连接

防火区可以通过随机附件中的线缆与防火墙连接，本地管理主机通过CONSOLE线缆与防火墙的CONSOLE口连接；

- 注意：
- 请确认防火墙的防火区与防火墙接口名称的对应关系；
- 请注意双绞线中直通线和交叉线的使用方法：交叉线用于通信主机间的直接连接，如防火墙与路由器间的直接连接；

4.2 管理器安装

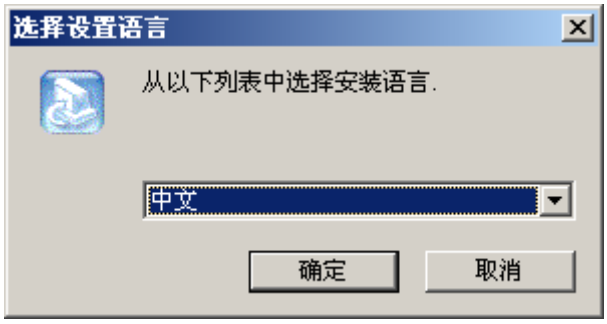
4.2.1 安全管理主机

防火墙安全管理直接关系安全系统的有效性，安全管理主机直接制定防火墙的安全策略，网络规划中必须设计管理主机的合理的物理位置：既确保管理的方便性，又有助于管理安全性的提高，通常，管理主机位于管理中心网络的网管主机上，管理中心为内部防火区的子集，同时，管理主机或管理中心与其它安全区域相比有更严格的访问安全策略；

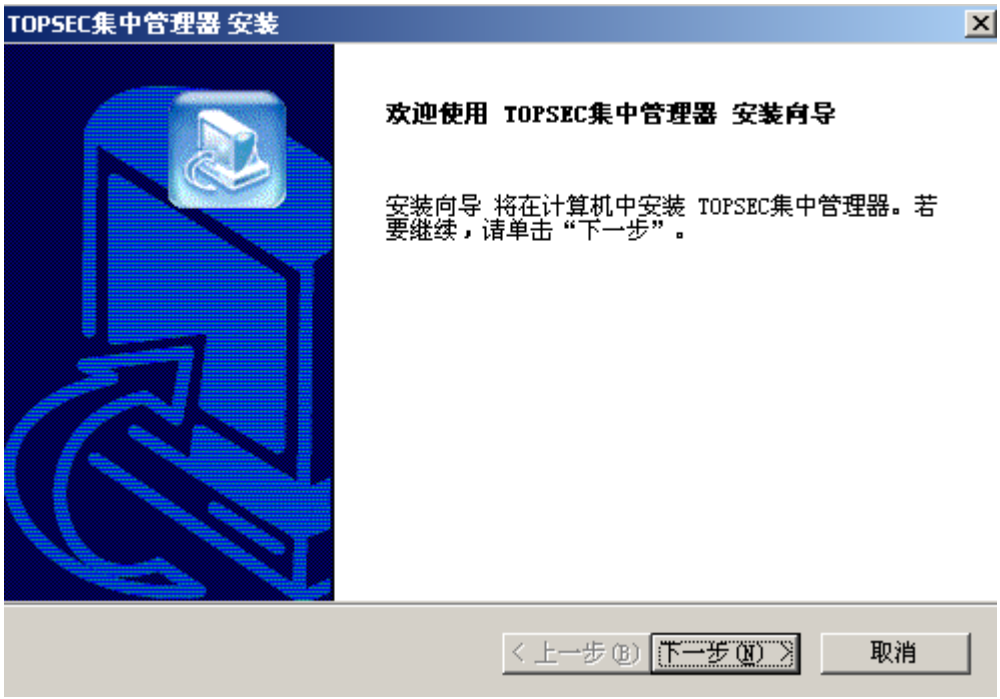
防火墙的管理主机分本地管理主机和远程管理主机；

4.2.2 管理器安装

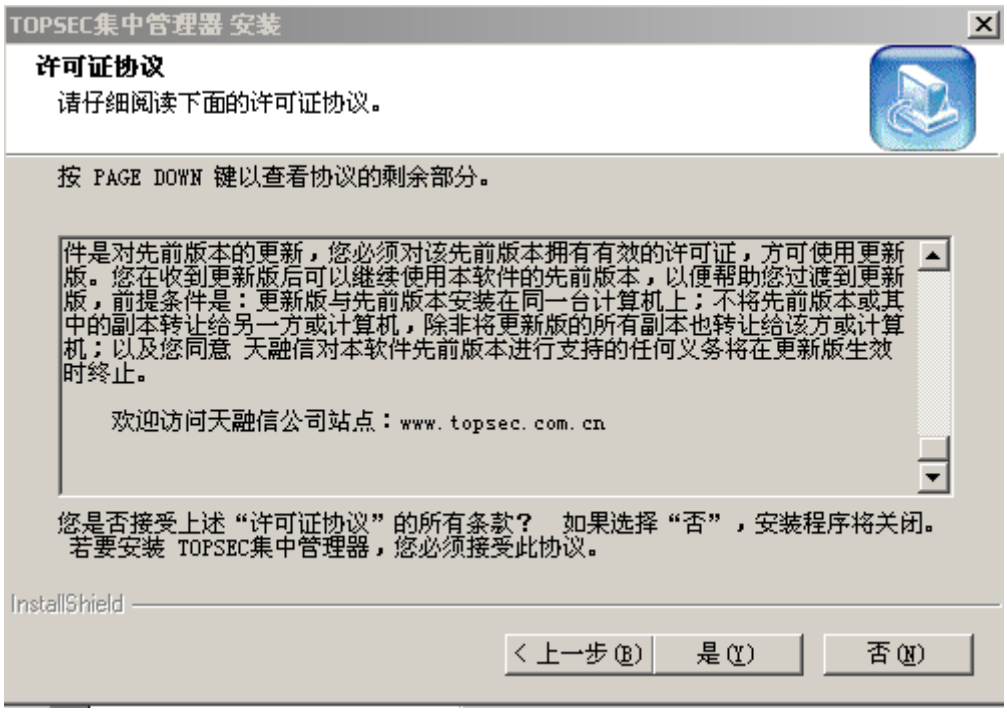
防火墙的本地管理器可以使用任何类型的终端，如WINDOWS的hyperterminal（hypertrm.exe），终端仿真类型至少支持VT100或ANSI等常用类型；
远程管理器为一防火墙专用集中管理器软件，安装过程如下：
运行随机光盘上的集中管理器安装程序，进入‘选择设置语言’窗口：可选择的语言有英文、中文和中文（台湾）三种；



按‘确定’按钮，进入欢迎窗口；

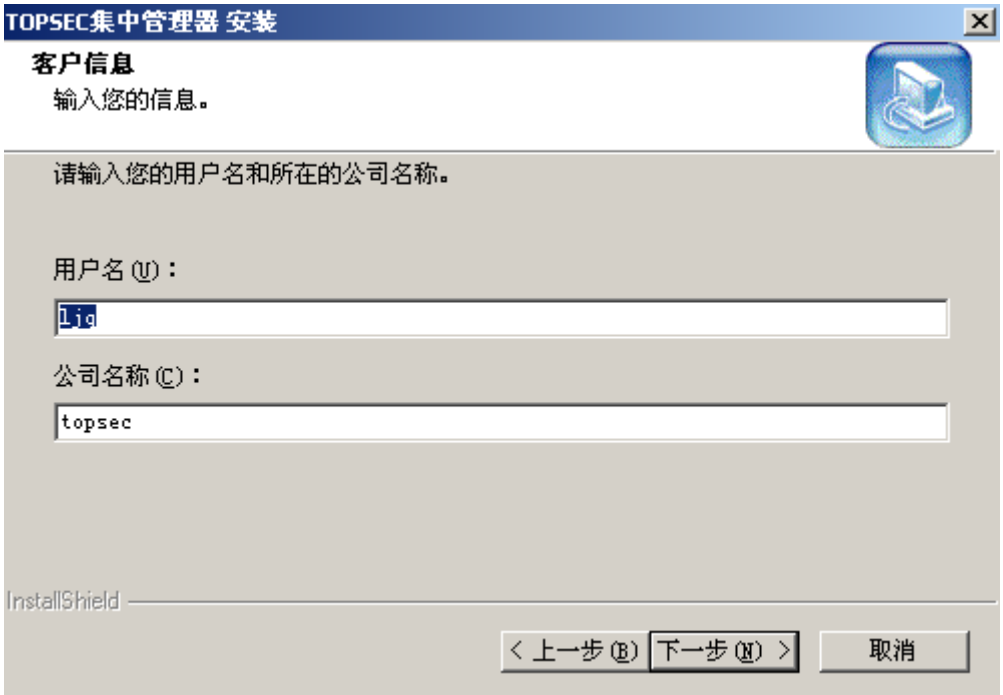


按‘下一步’按钮，进入许可证协议窗口；

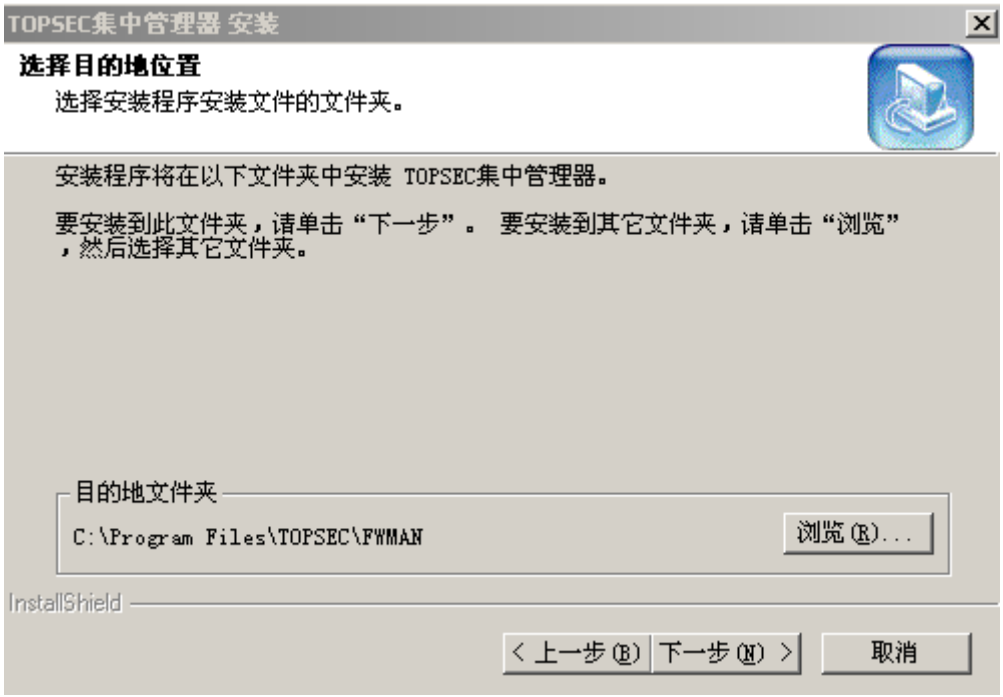


按‘是’按钮，进入信息窗口，显示关于此集中管理器的相关信息；

按‘下一步’按钮，进入客户信息窗口。可在此窗口输入用户相关的信息；



按‘下一步’按钮，进入选择安装路径窗口。系统默认的安装路径是当前操作系统盘符下的\Program Files\TOPSEC\FWMAN 目录下，用户可自行更改；

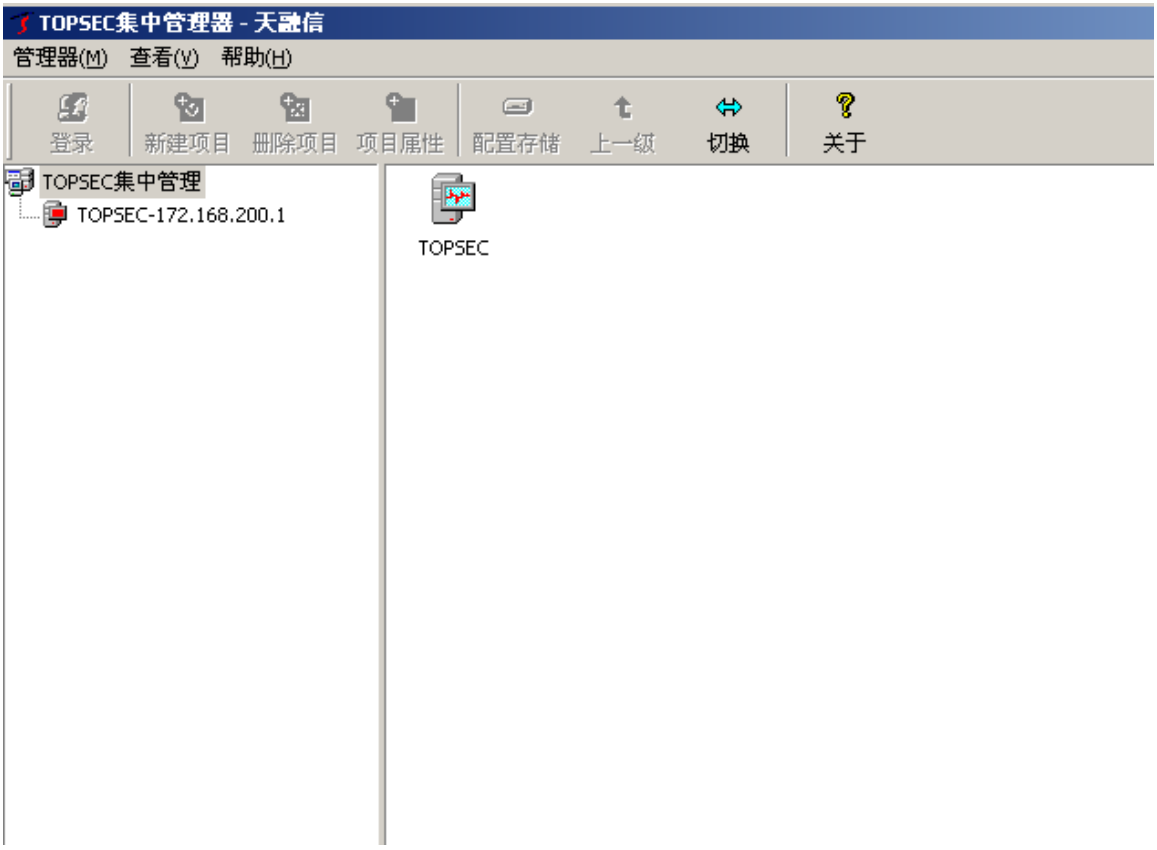


按‘下一步’按钮后，系统开始安装集中管理器软件。

4.2.3 管理器运行

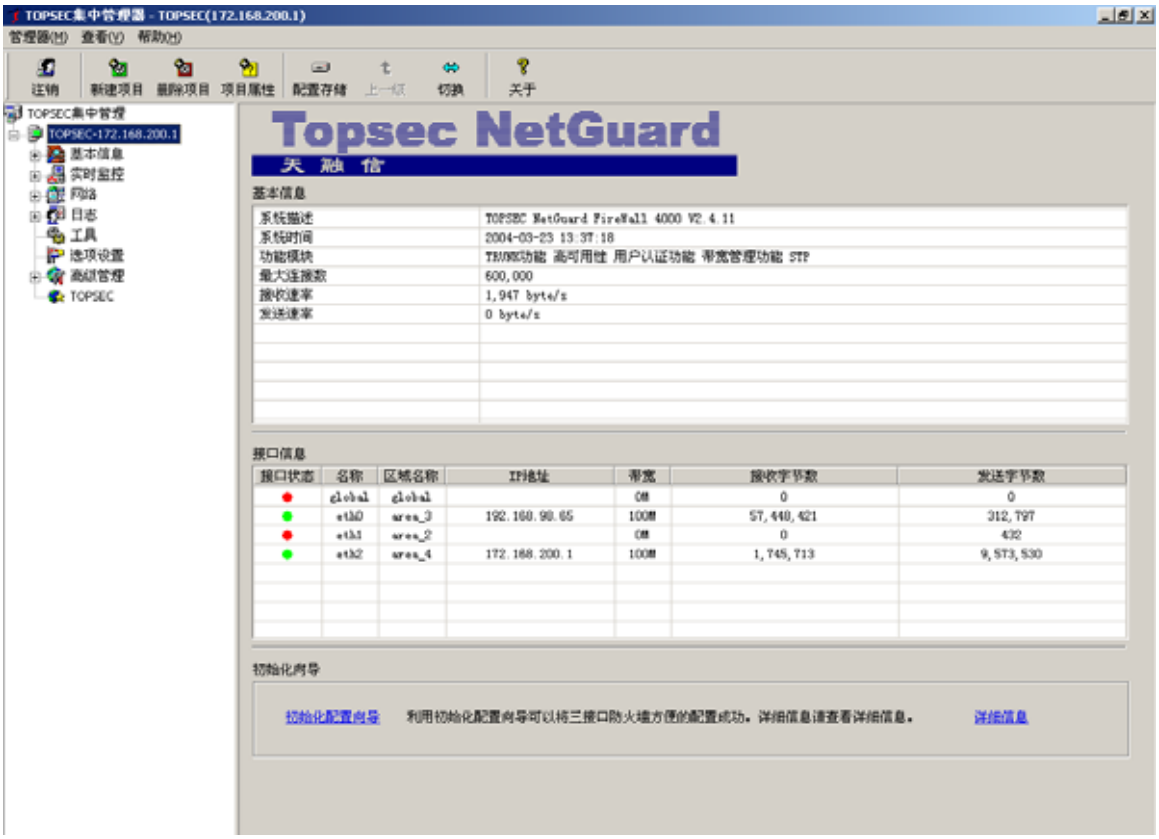
4.2.3.1 快捷菜单：

管理器安装完成后，在系统启动菜单中建立了快捷菜单，可以直接从此处运行，以下为一运行示例：



4.2.3.2 防火墙：

管理器远程连接防火墙，需要先在防火墙上配置管理地址，使用超级终端登录防火墙，配置一防火区，防火区的接口地址及客户登录权限即可作为管理地址；
如下是集中管理器登录上其中一台防火墙后的界面：



4.2.3.3 配置脚本说明

防火墙管理器的配置脚本在 WINDOWS 的系统目录下，文件名为：FWMANAGER.INI，管理员可以将管理中心将要管理的防火墙列表预先添加在此脚本中，如下为一示例：

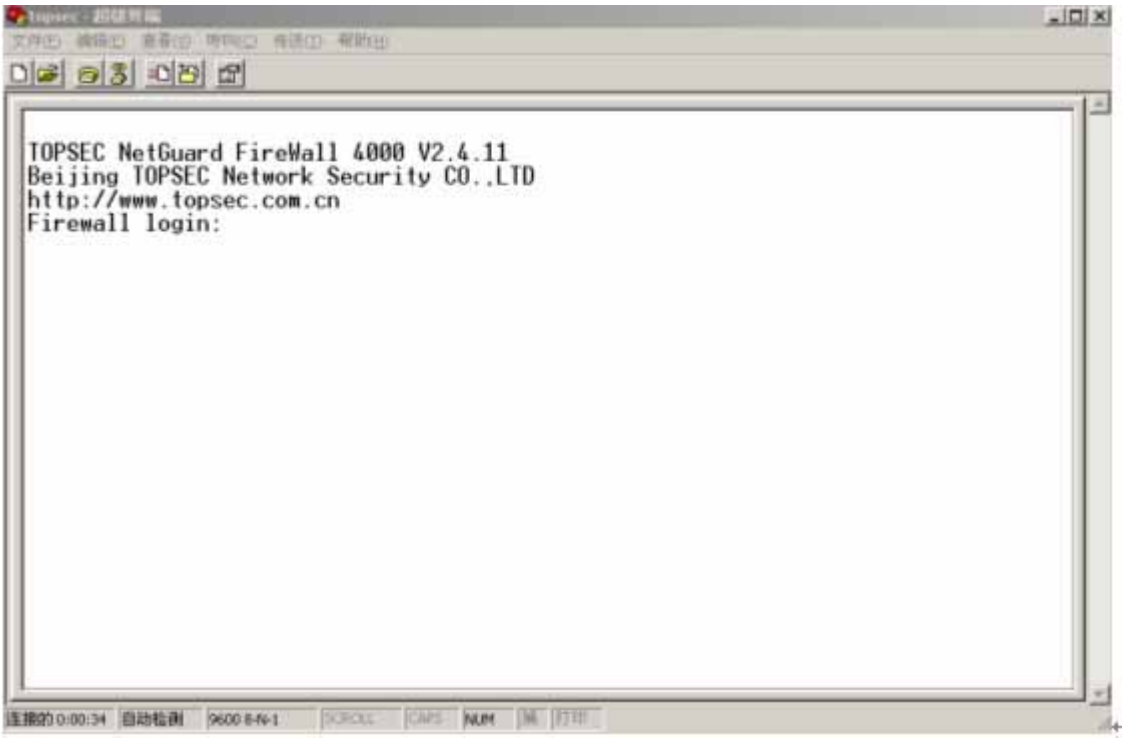
共 7 台防火墙预定义在管理器中，管理器在启动过程中会自动读入防火墙信息；

4.3 系统基本管理方案

4.3.1 本地管理

通过防火墙的 CONSOLE 接口进行命令行本地管理方式可以完成防火墙的全功能配置，本地管理在独立的环境中完成，具有最高的安全属性，系统的初始化要求通过本地管理完成；

本地管理使用超级终端登录防火墙：



防火墙的本地管理用户帐号为 superman，管理员直接可以输入口令：

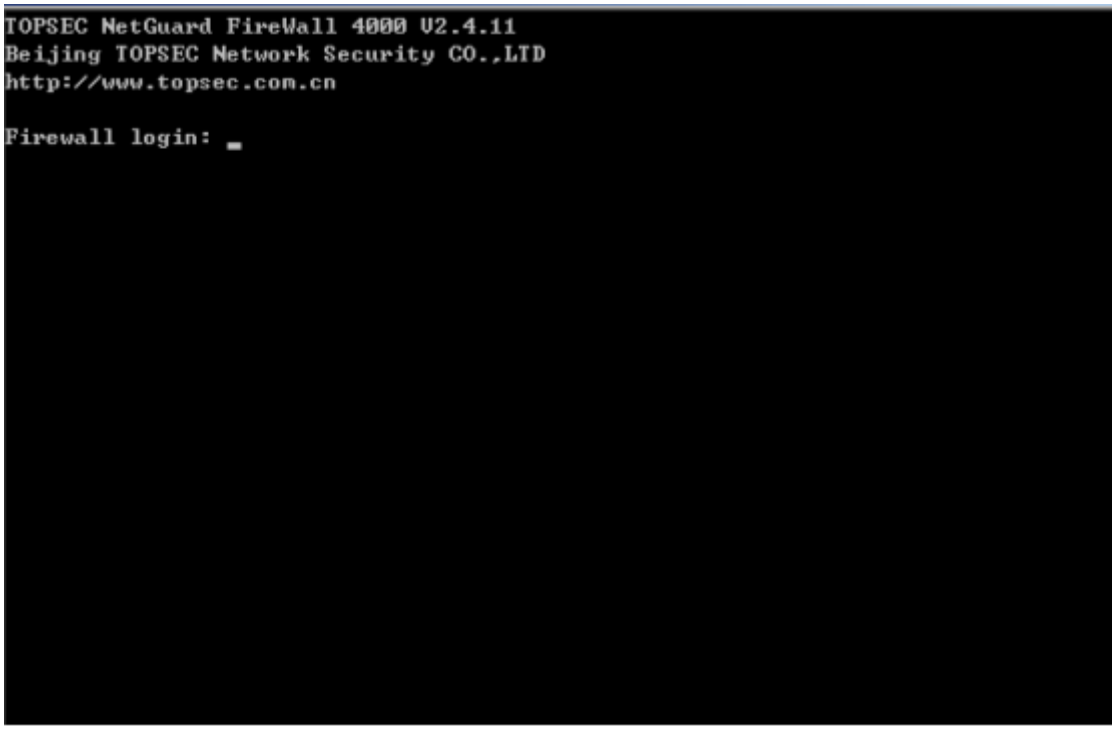
初始口令为：talent；

本地管理员具有防火墙所有管理权限，为超级管理员；

4.3.2 远程管理

远程管理两种方式：

① Telnet 方式：通过网络直接登录防火墙的管理接口，其管理员帐号同CONSOLE 方式的帐号；

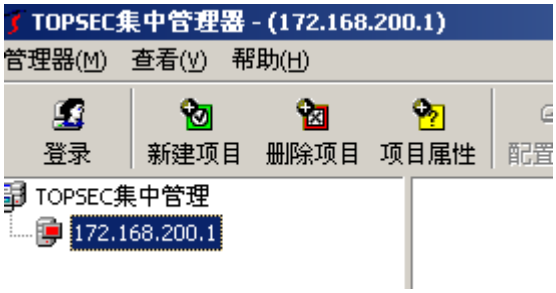


② 集中管理器方式：

从管理主机启动菜单运行集中管理器，管理软件启动后可以读入预定义项目。要添加一个管理项目，可以在管理器窗口中点击‘新建项目’图标。

打开管理配置窗口：添加防火墙到管理配置中：

选中新添加的防火墙，双击它或点击‘登录’图标或使用右键菜单



打开登录窗口，使用超级管理员身份登录防火墙，初始默认口令是 talent

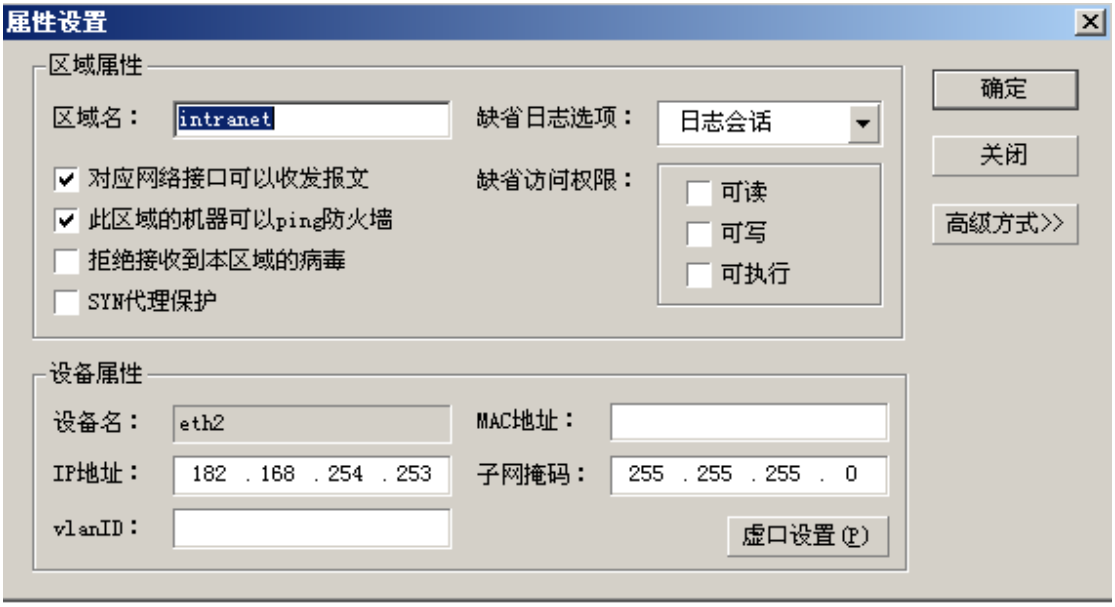
激活防火墙管理连接:

正常连接后防火墙状态指示绿灯亮，此时可以对防火墙进行各项管理;

4.3.3 管理安全选项

防火墙的防火区的管理属性可以由管理员定义，在系统基本管理建立后，应及时调整防火墙的安全管理属性。

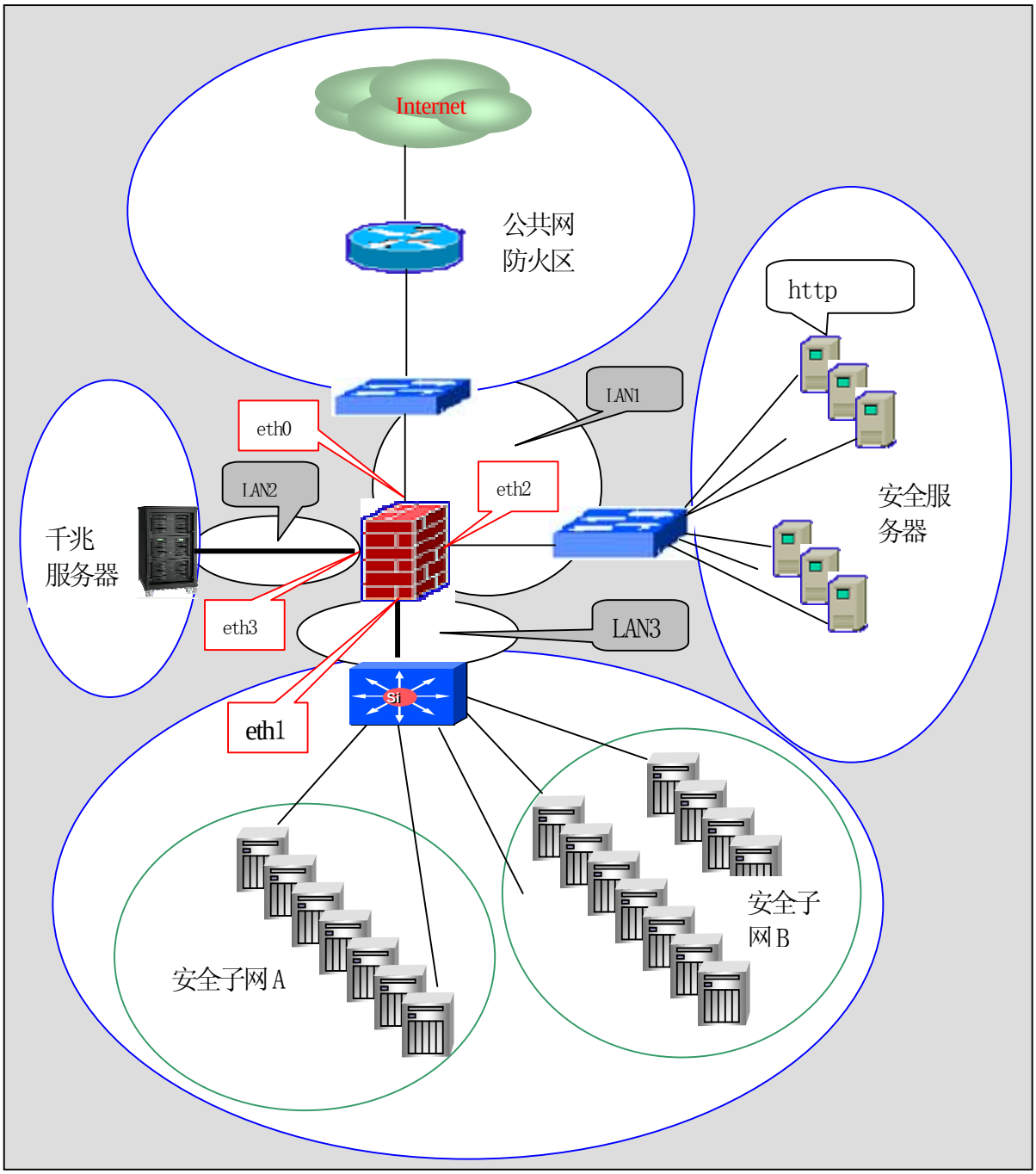
双击要配置的防火墙的网络接口，出现防火区域设置窗口，在此可设置相应的安全管理。



5 简单应用示例

5.1 应用环境与方案

以上述方案二为例，网络分布和防火区分布如下图示意：



5.1.1 网络结构说明：

公共网络防火区和安全服务防火区：LAN-1：202.100.100.0/24

千兆服务网络防火区：LAN-2：202.100.101.0/24
内部网络防火区：LAN-3：192.168.1.0/24;192.168.2.0/24

内部网防火区包括两个网络;
LAN-1 跨两个防火区;

5.1.2 防火墙接口与防火区对应关系：

eth0：公共网络防火区
eth1：内部网络防火区
eth2：安全服务网络防火区
eth3：千兆服务网络防火区

5.2 配置过程

5.2.1 防火区配置

```
area ‘internet’ -d ‘eth0’ -a any enable ping
area ‘intranet’ -d ‘eth1’ -a any enable ping
area ‘ssn’ -d ‘eth2’ -a any -l session enable ping
area ‘GBNETS’ -d ‘eth3’ -a any -l command enable ping
```

5.2.2 管理接口配置

```
ifconfig ‘eth0’ 202.100.100.253 255.255.255.0
ifconfig ‘eth1’ 192.168.1.254 255.255.255.0
ifconfig ‘eth1:0’ 192.168.2.254 255.255.255.0
ifconfig ‘eth3’ 202.100.101.254 255.255.255.0
```

防火墙的接口地址为防火墙的逻辑接口属性，防火墙可以智能判定网段归属，故接口地址逻辑上可以在任意物理接口上配置，但为方便管理理解，最好与对应的接口名一致;

5.2.3 登录客户权限配置

```
system client add ‘test’ -t gui -a ‘intranet’ -i
0.0.0.0-255.255.255.255
system client add ‘test’ -t gui -a ‘ssn’ -i
0.0.0.0-255.255.255.255
```

- 以下可以通过集中管理器方式管理，本例以命令行方式介绍为主

5.2.4 工作模式配置

5.2.4.1 路由接口：

Intranet 与其它防火区间的通信为路由模式，添加一缺省到 Internet 的路由为：

```
route ad -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 -g 202.100.100.254
```

5.2.4.2 透明接口组定义：

防火区 Internet 和 SSN 间为透明接口组：

```
vlan add 'Internet-SSN' -a 'Internet' 'SSN'|
```

上述命令定义了一名为：Internet-SSN 的透明接口组，其包括 Internet 和 SSN 两个防火区；

5.2.5 安全策略配置

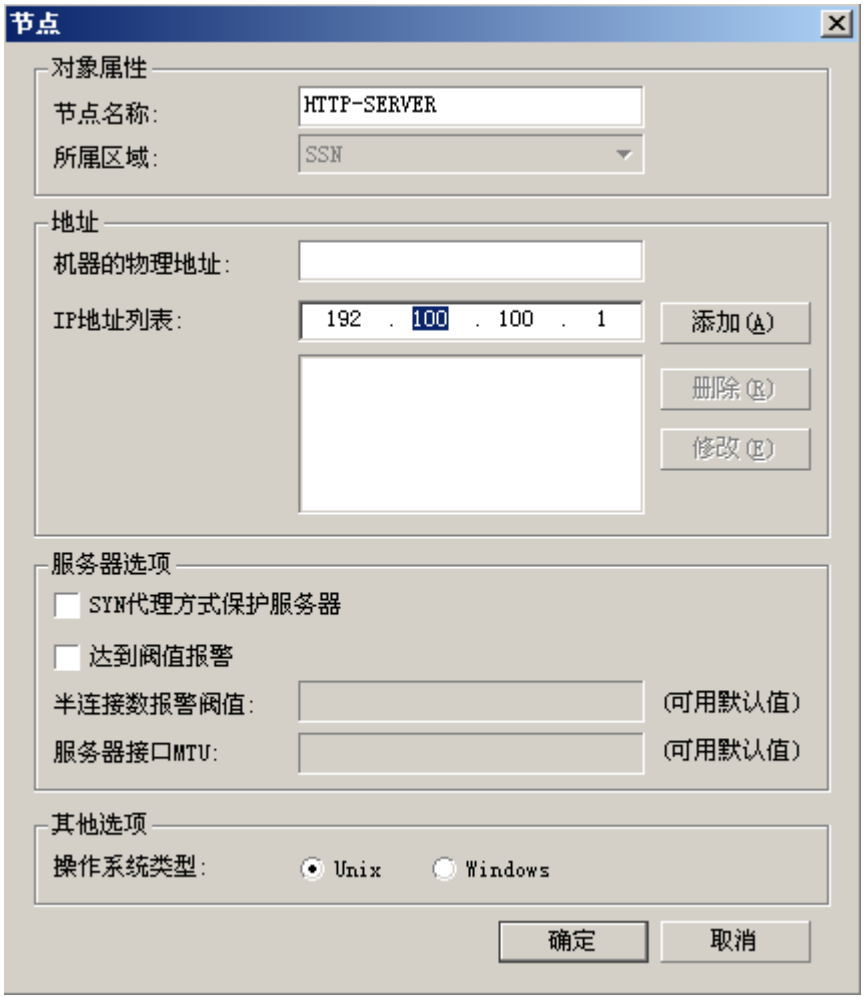
定义一条 Internet 访问 SSN 的 HTTP 服务器的安全策略：

5.2.5.1 定义 INTERNET 和 SSN 防火区中的网络对象：

首先进入防火墙集中管理器，在‘高级管理’→‘网络对象’下，选择相应的防火区域，在右边框中使用右键菜单：

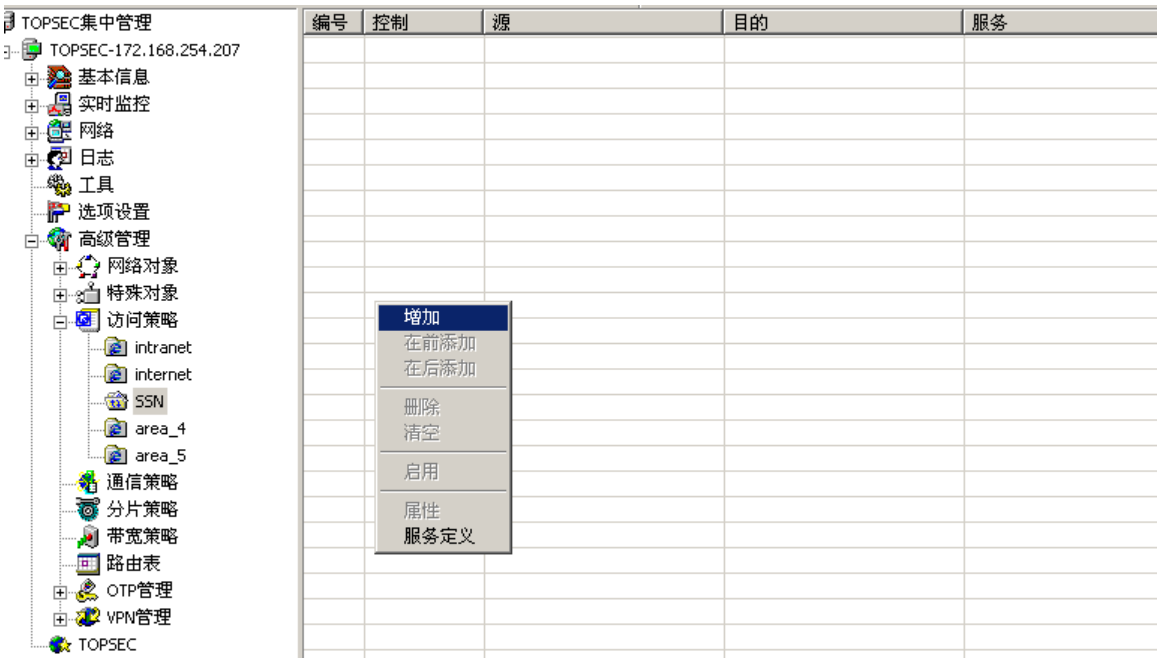
点击‘定义新对象’-‘子网’，建立一个属于 Intranet 区的子网对象‘Out-Net’：

点击‘定义新对象’-‘节点’，建立一个属于SSN区的节点对象‘HTTP-SERVER’：

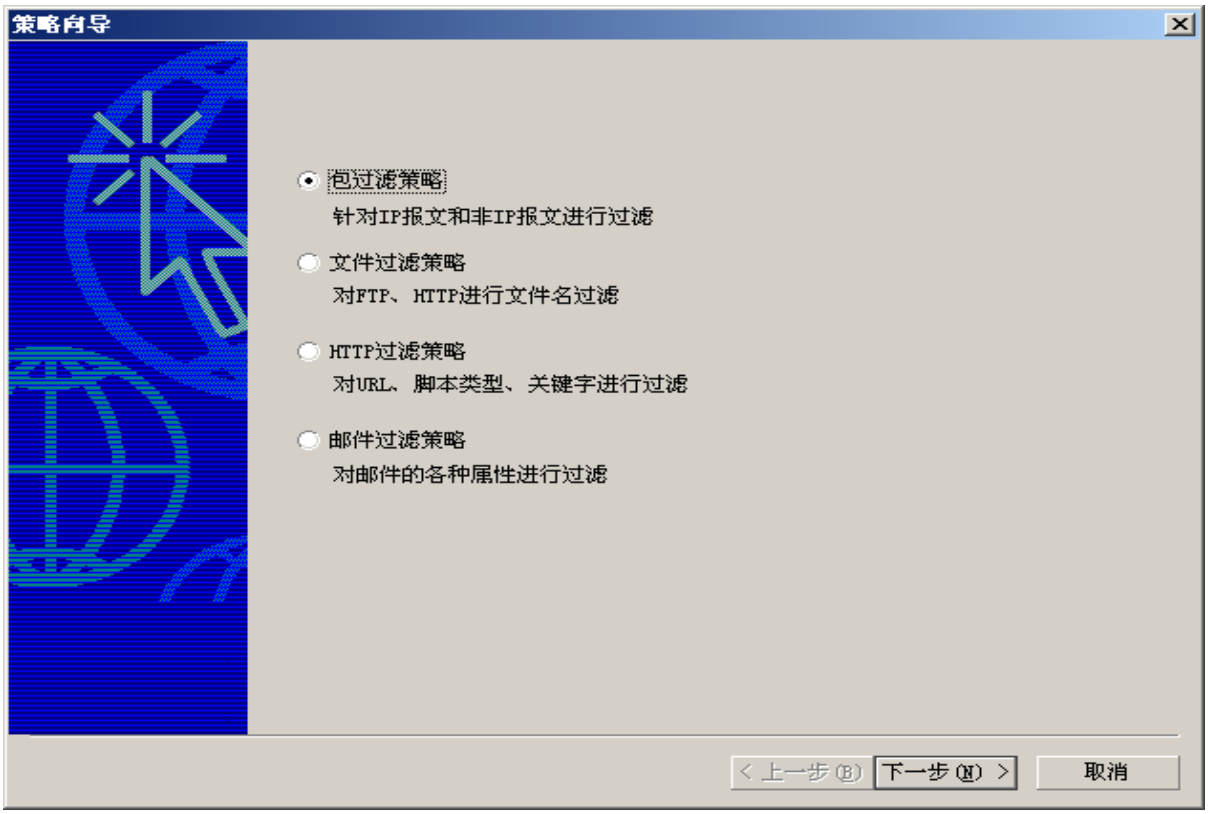


5.2.5.2 添加访问规则：

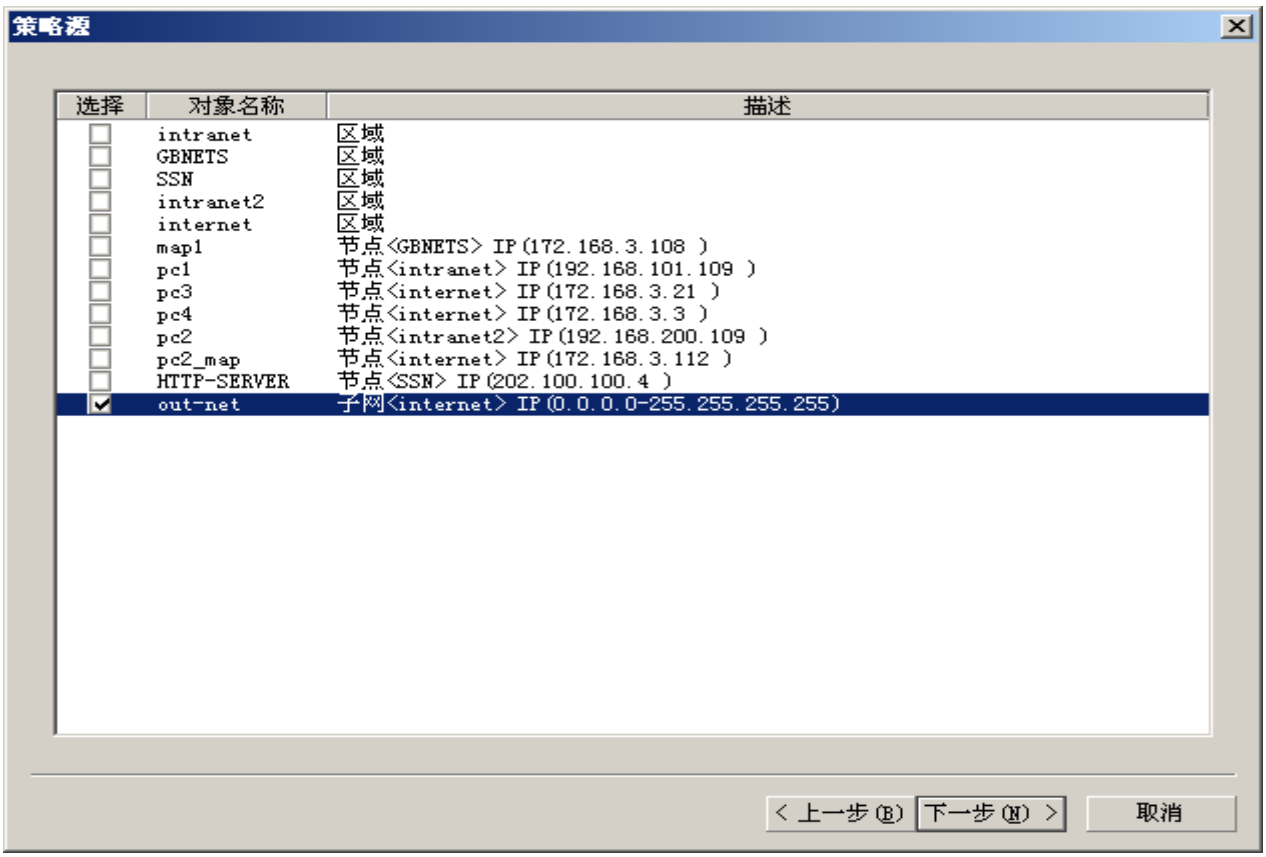
首先进入防火墙集中管理器，在‘高级管理’→‘访问策略’下，选择SSN防火区域，在右边框中使用右键菜单



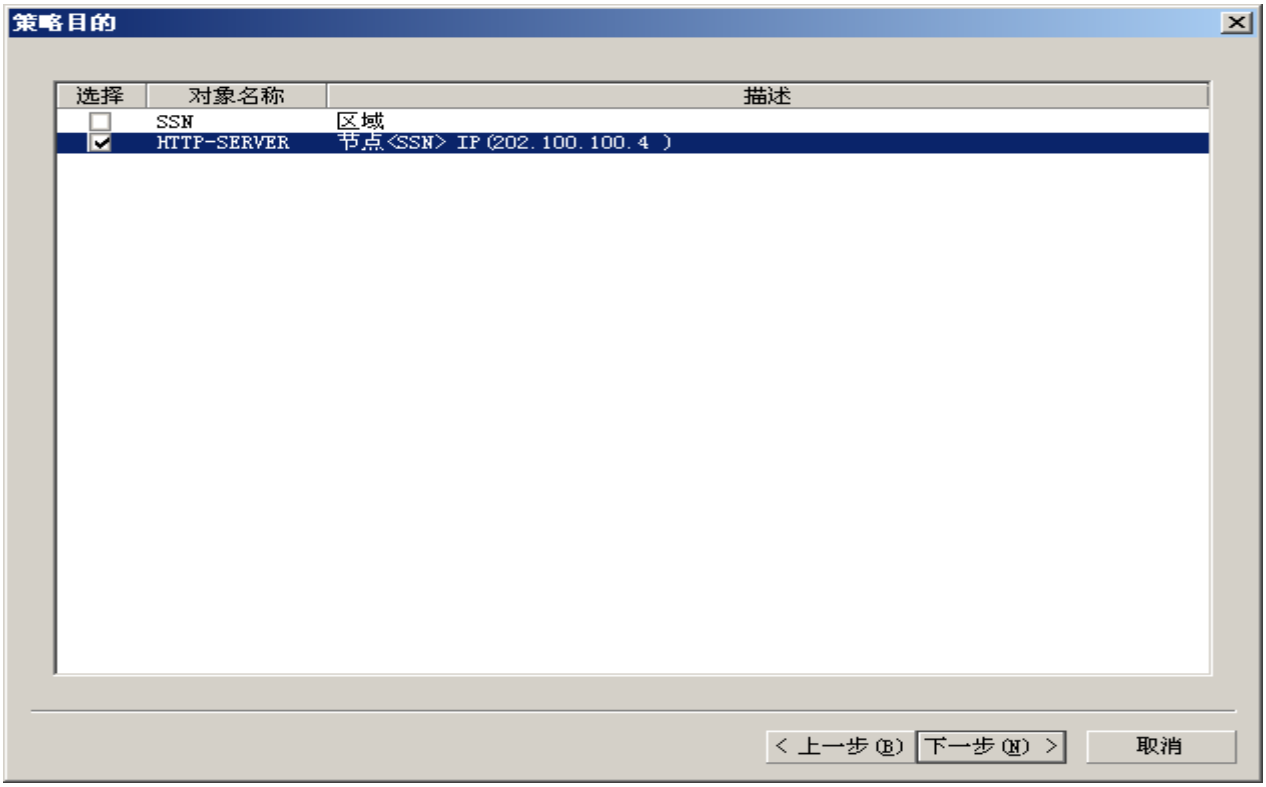
选择‘增加’，弹出‘策略向导’窗口：



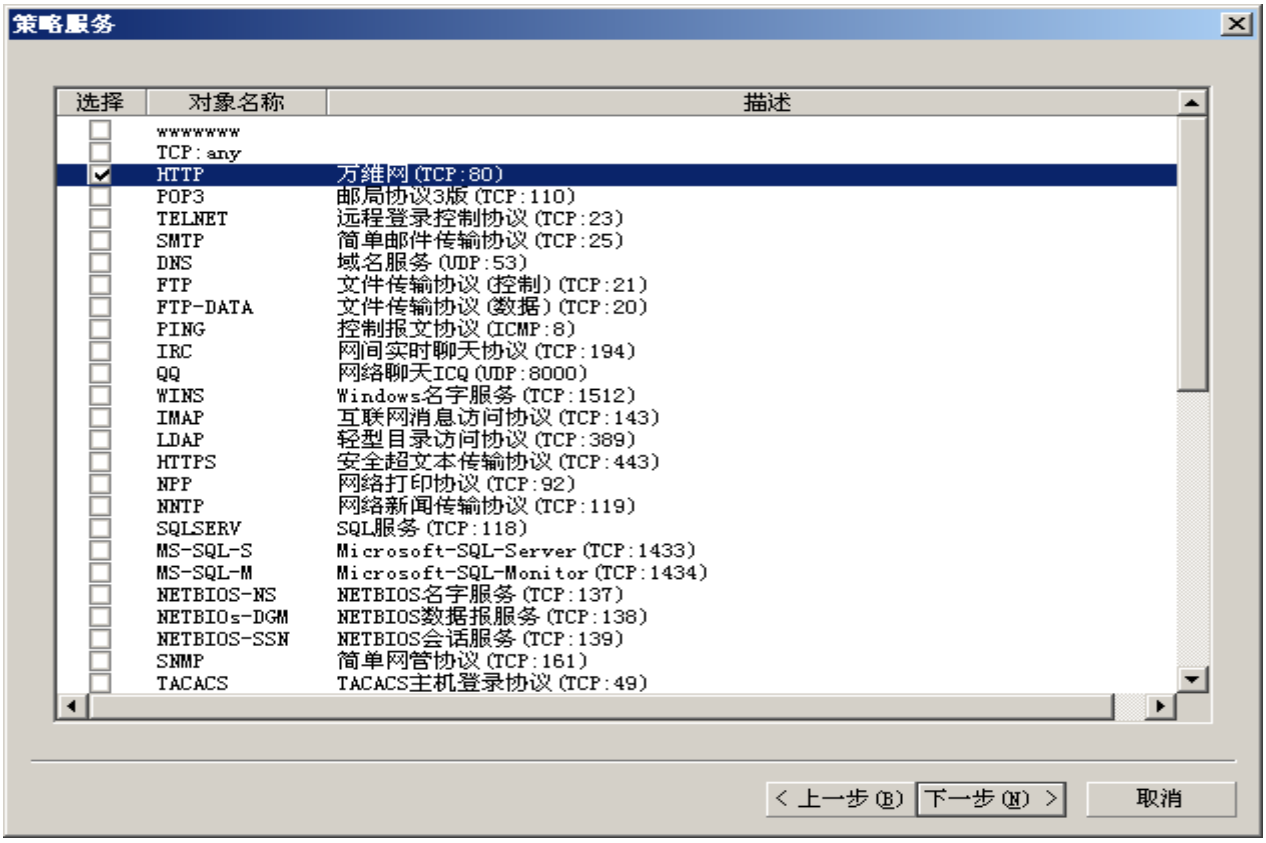
选择‘包过滤策略’项，进入下一步，定义策略的源为‘out-net’对象：



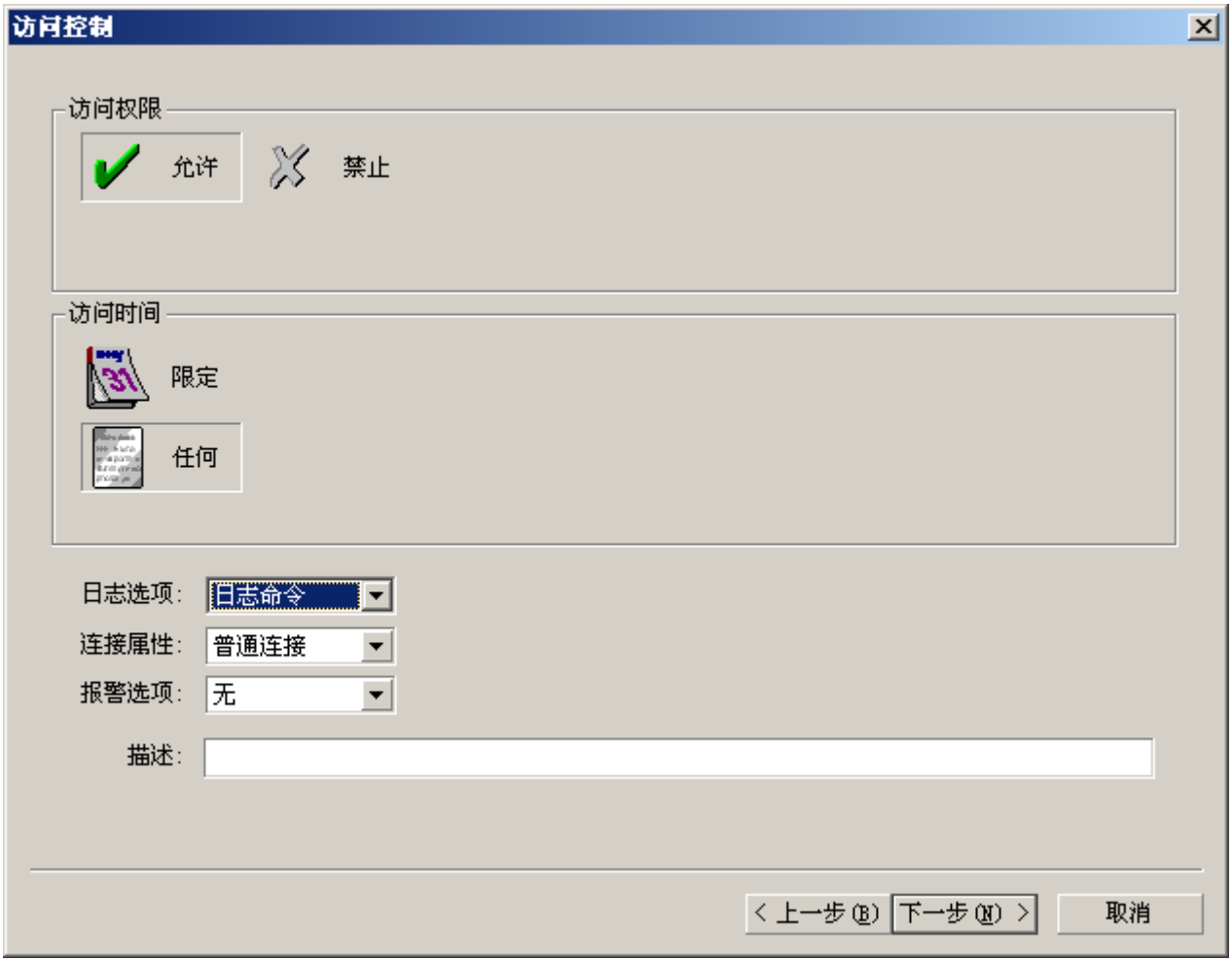
点击下一步，定义策略的目的为‘HTTP-SERVER’对象：



点击下一步，定义策略的服务为 TCP：80 HTTP 服务；



点击下一步，进入访问控制窗口：



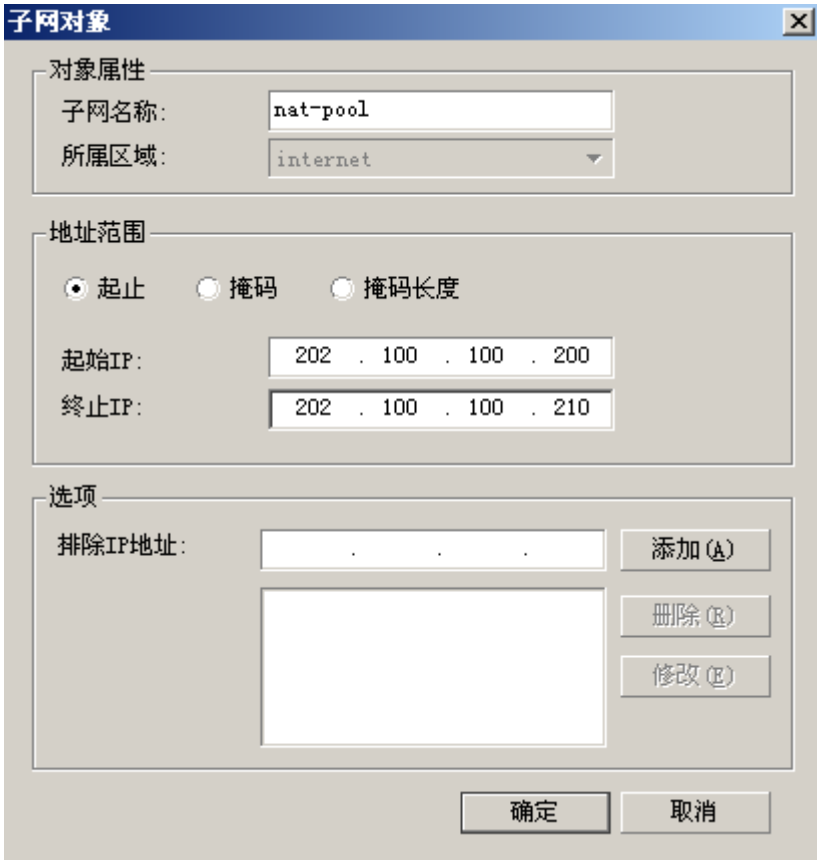
点击下一步，提示确认后完成该策略的制订，完成后该策略显示如下：

编号	控制	源	目的	服务	资源	时间	日志
1	允许访问	out-net	HTTP-SERVER	HTTP			命令

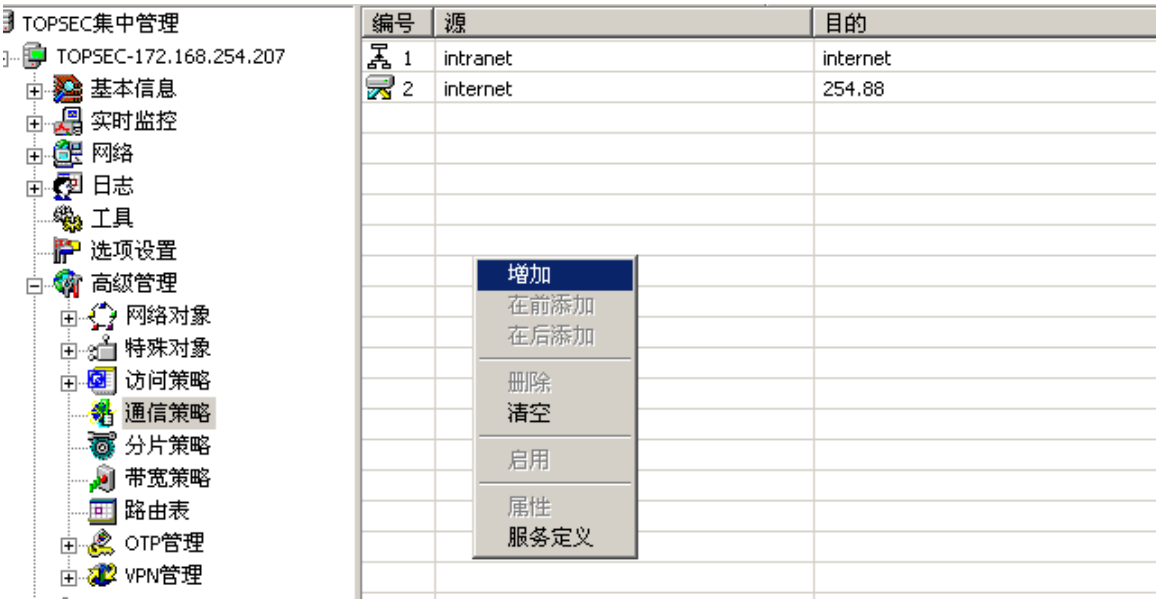
至此完成了一条访问策略的制订。

5.2.6 通信策略配置

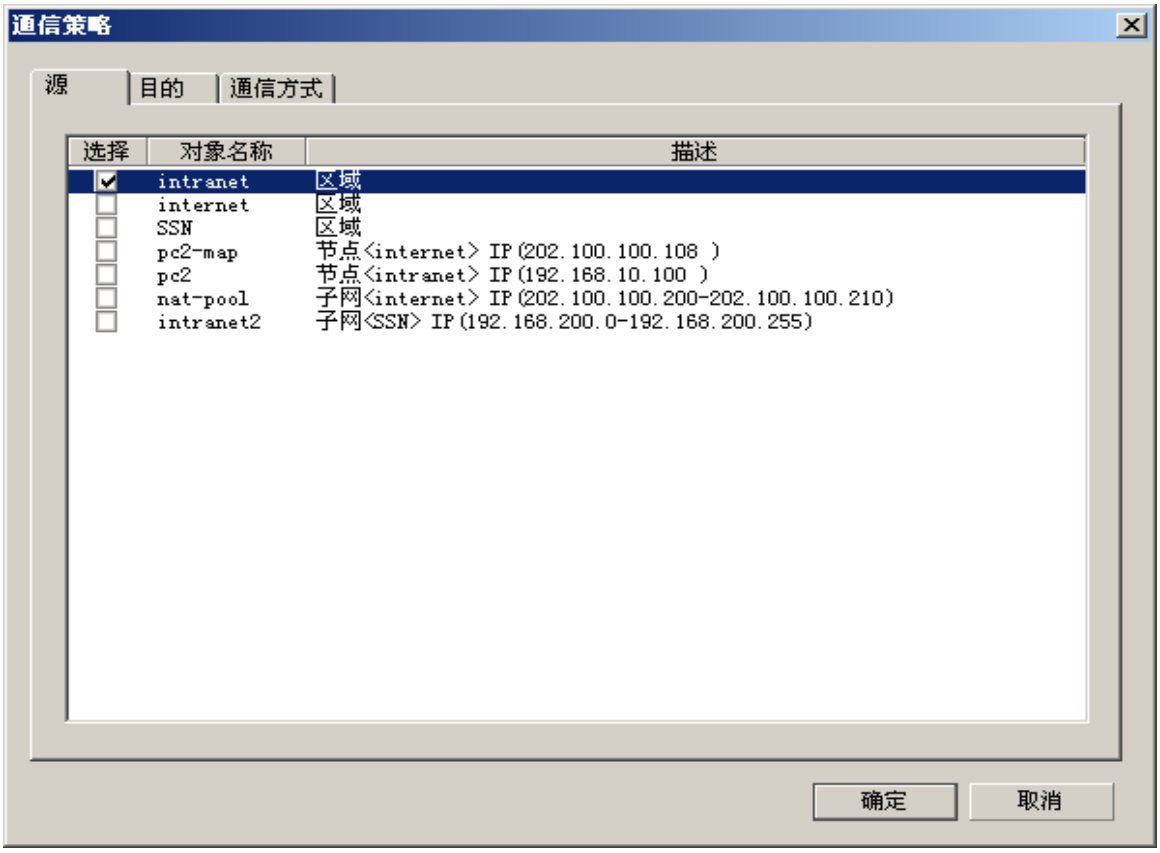
Intranet 防火区访问 Internet 防火区为 NAT 方式；其它访问为 transfer 方式；
增加一子网对象作为 NAT 地址池：



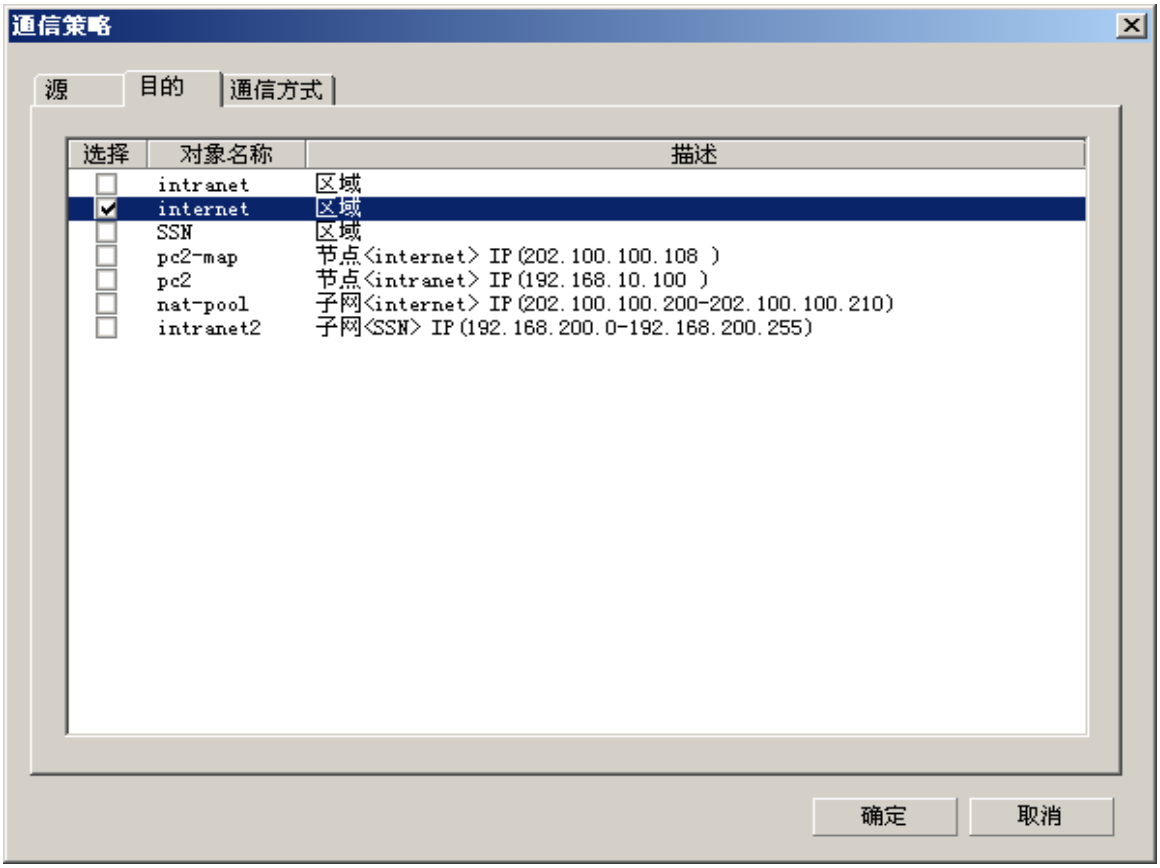
在‘高级管理’→‘通信策略’下，在右边框中使用右键菜单：



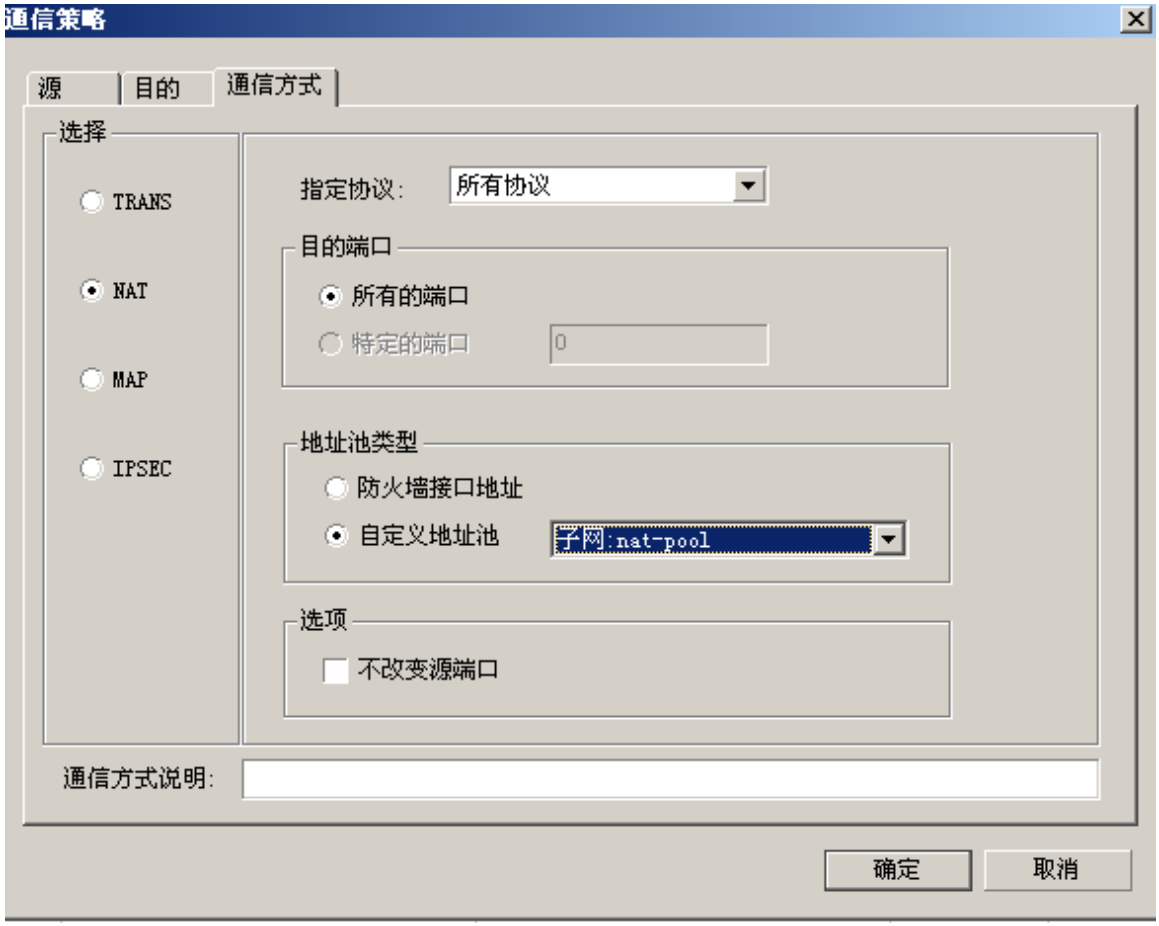
选择通信策略的源：


通信策略
源
目的
通信方式
选择
对象名称
描述
intranet 区域
internet 区域
SSN 区域
pc2-map 节点<internet> IP(202.100.100.108)
pc2 节点<intranet> IP(192.168.10.100)
nat-pool 子网<internet> IP(202.100.100.200-202.100.100.210)
intranet2 子网<SSN> IP(192.168.200.0-192.168.200.255)
确定
取消

选择通信策略的目的:


通信策略
源
目的
通信方式
选择
对象名称
描述
intranet 区域
internet 区域
SSN 区域
pc2-map 节点<internet> IP(202.100.100.108)
pc2 节点<intranet> IP(192.168.10.100)
nat-pool 子网<internet> IP(202.100.100.200-202.100.100.210)
intranet2 子网<SSN> IP(192.168.200.0-192.168.200.255)
确定
取消

定义通信方式：NAT，

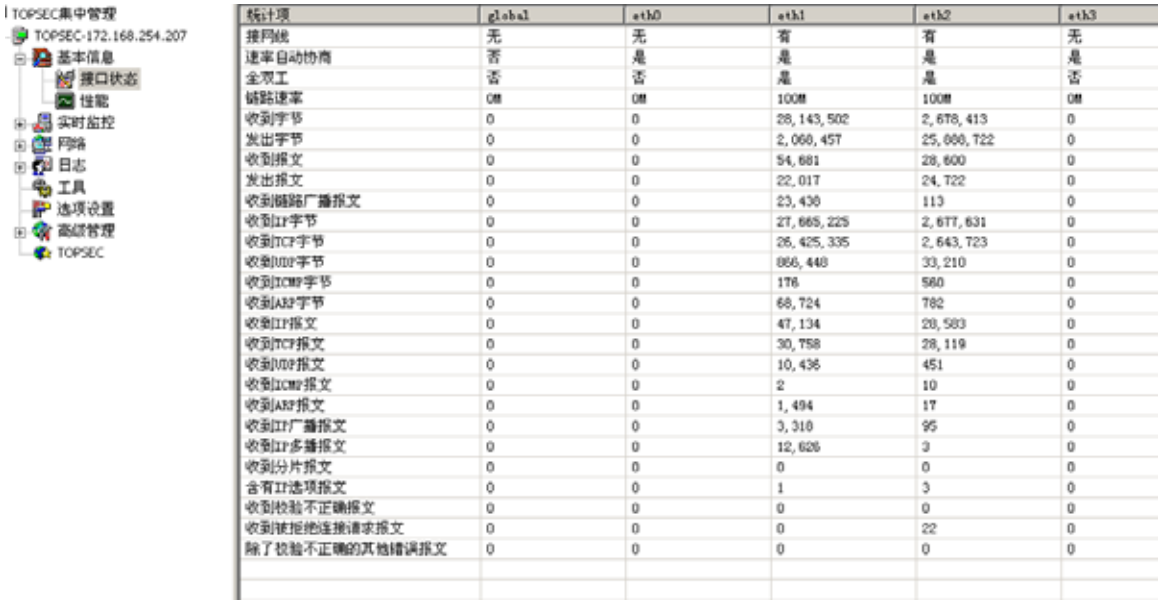


点击确定，完成通信策略的配置：

编号	源	目的	通信方式	详细
1	intranet, intranet2	internet	nat	使用防火墙接口
2	internet	intranet	transfer	
3	internet	pc2-map	map	=>pc2
4	intranet	internet	nat	使用自定义地址池(nat-pool)

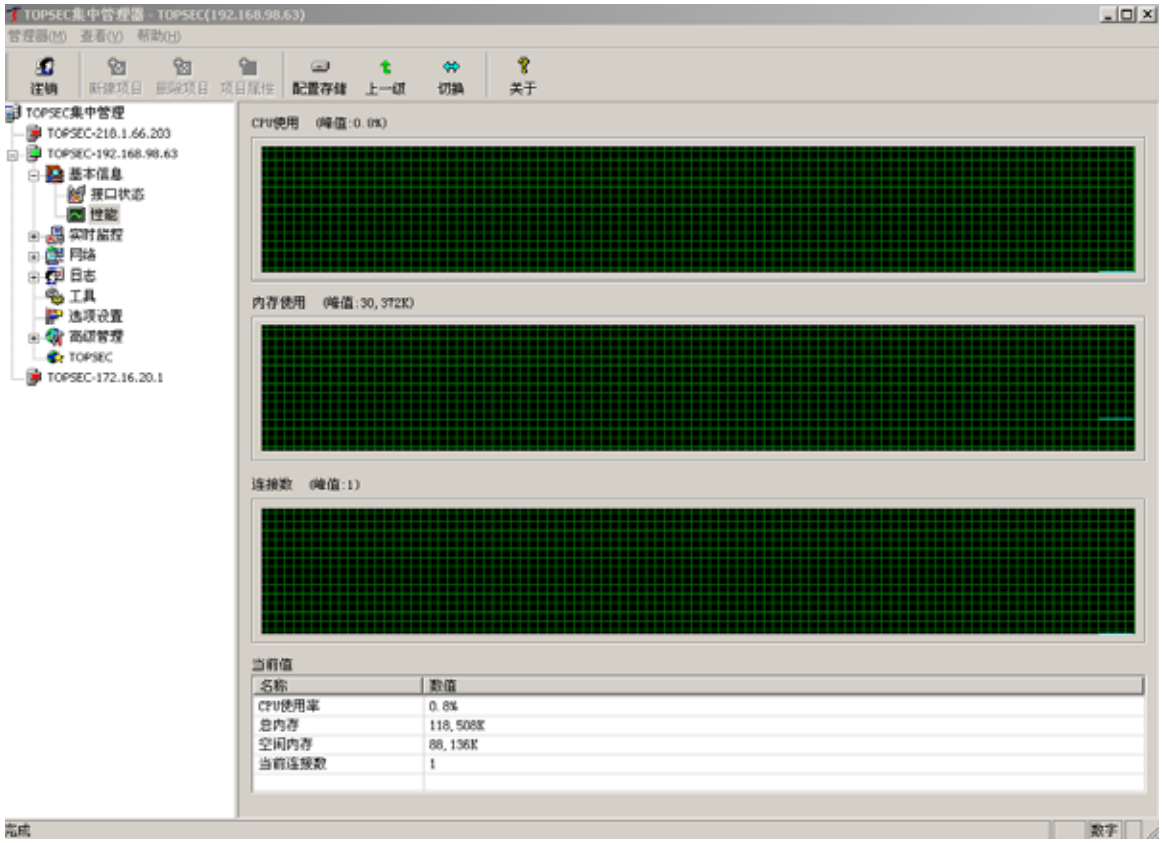
5.3 通信状态监控

防火墙的状态可以通过集中管理软件的基本信息来显示。
在‘基本信息’→‘接口状态’下，显示当前防火墙接口的通信情况：



统计项	global	eth0	eth1	eth2	eth3
接网线	无	无	有	有	无
速率自动协商	否	是	是	是	是
全双工	否	否	是	是	否
链路速率	0M	0M	100M	100M	0M
收到字节	0	0	28, 143, 502	2, 678, 413	0
发出字节	0	0	2, 060, 457	25, 860, 722	0
收到报文	0	0	54, 681	28, 600	0
发出报文	0	0	22, 017	24, 722	0
收到链路广播报文	0	0	23, 430	113	0
收到IP字节	0	0	27, 665, 225	2, 677, 631	0
收到TCP字节	0	0	26, 425, 335	2, 643, 723	0
收到UDP字节	0	0	866, 448	33, 210	0
收到ICMP字节	0	0	176	560	0
收到ARP字节	0	0	68, 724	782	0
收到IP报文	0	0	47, 134	28, 583	0
收到TCP报文	0	0	30, 758	28, 119	0
收到UDP报文	0	0	10, 436	451	0
收到ICMP报文	0	0	2	10	0
收到ARP报文	0	0	1, 494	17	0
收到IP广播报文	0	0	3, 310	95	0
收到IP多播报文	0	0	12, 626	3	0
收到分片报文	0	0	0	0	0
含有IP选项报文	0	0	1	3	0
收到校验不正确报文	0	0	0	0	0
收到被拒绝连接请求报文	0	0	0	22	0
除了校验不正确的其他错误报文	0	0	0	0	0

在‘基本信息’→‘性能’下，显示当前防火墙各种资源的使用情况：



1.4 版

二 .TOPSEC 认证客户端安装指南

1 概 要

系统安装说明提供如下主要内容:
软件概述
TOPSEC 认证客户端的安装
TOPSEC 认证客户端的卸载

2 软件概述

TOPSEC 认证客户端，是网络卫士防火墙对第三方认证服务器的支持软件。

3TOPSEC 认证客户端安装

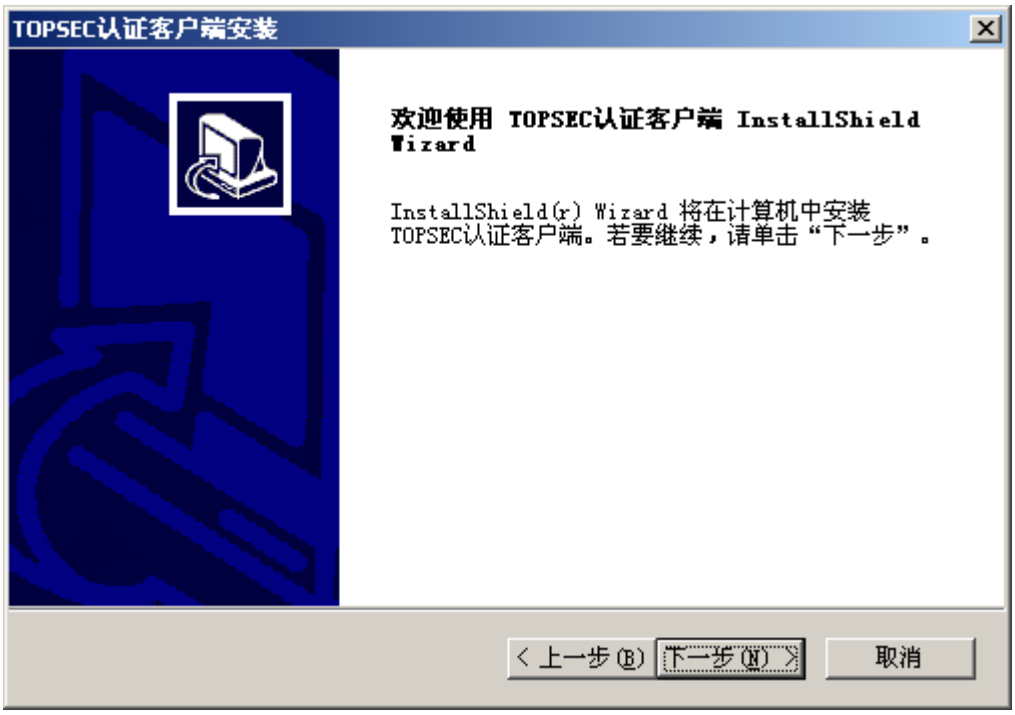
3.1 安装系统需求

软件要求：操作系统版本为 Windows98/NT/2000 以上，并正确设置 TCP/IP 协议。
硬件要求：
a 最低配置：
CPU：奔腾III500
内存：64MB
显示卡：标准 VGA
硬盘：剩余空间 100MB 以上
网卡：一块 10M 局域网卡
b 建议配置：
CPU：奔腾 IV 或更高
内存：256MB 或更高
显示卡：SVGA，16 位真彩以上显示模式
硬盘：剩余空间 400MB 以上
网卡：一块 100M 局域网卡

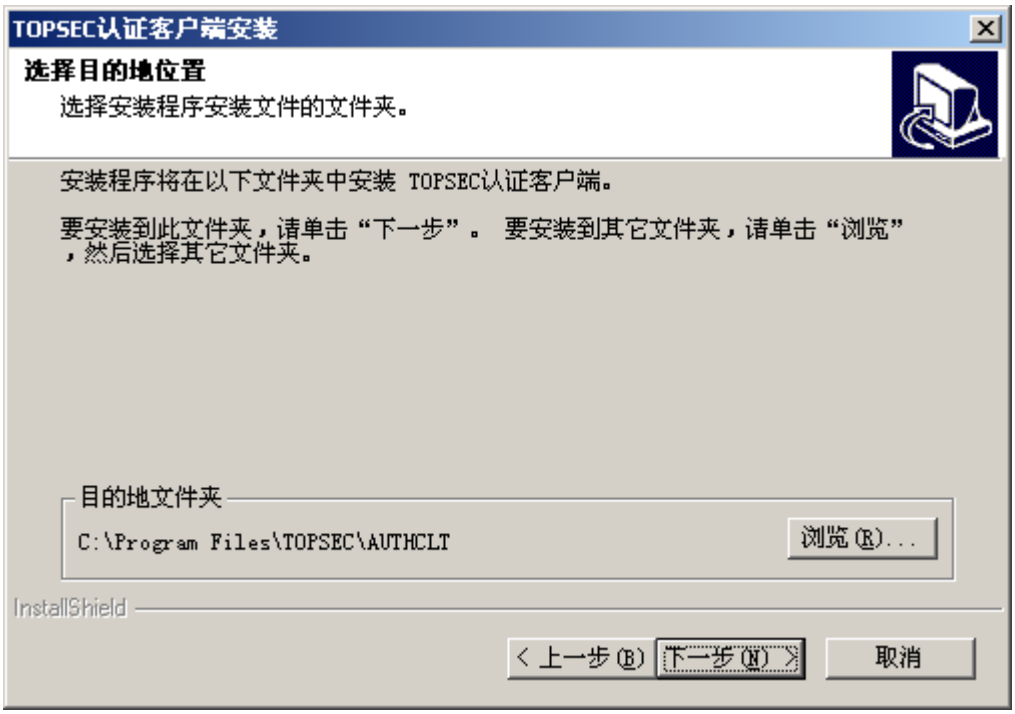
3.2 安装步骤

运行随机光盘上的安装包 TOPSEC 认证客户端的 TOPSEC_AUTH_C_1.4.04.EXE 可执行文件。

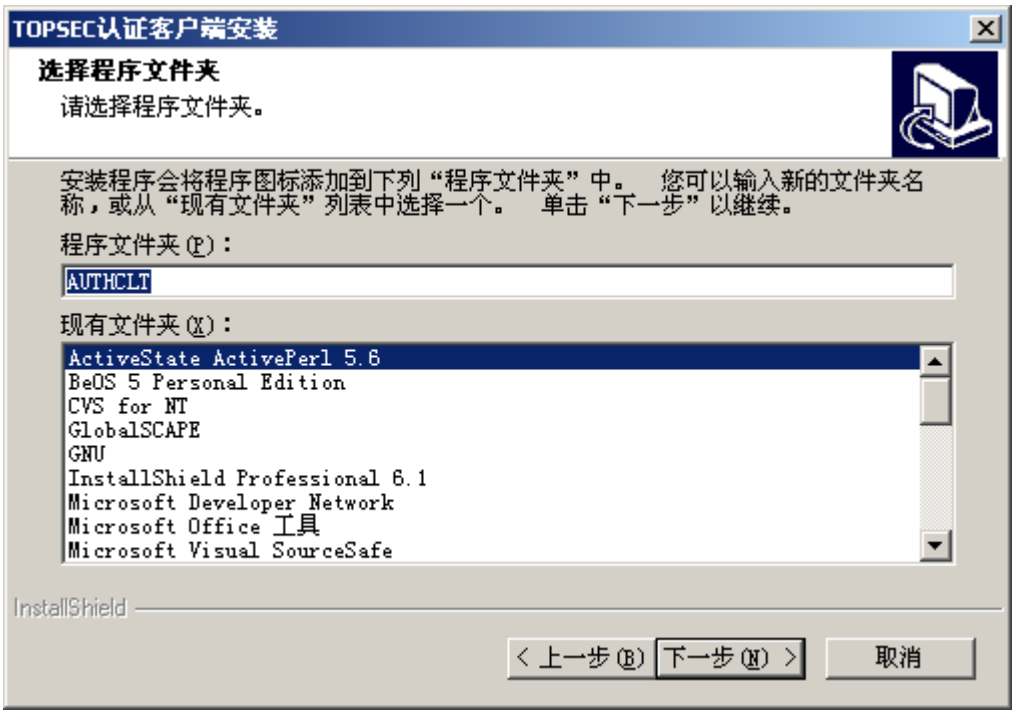
安装界面：



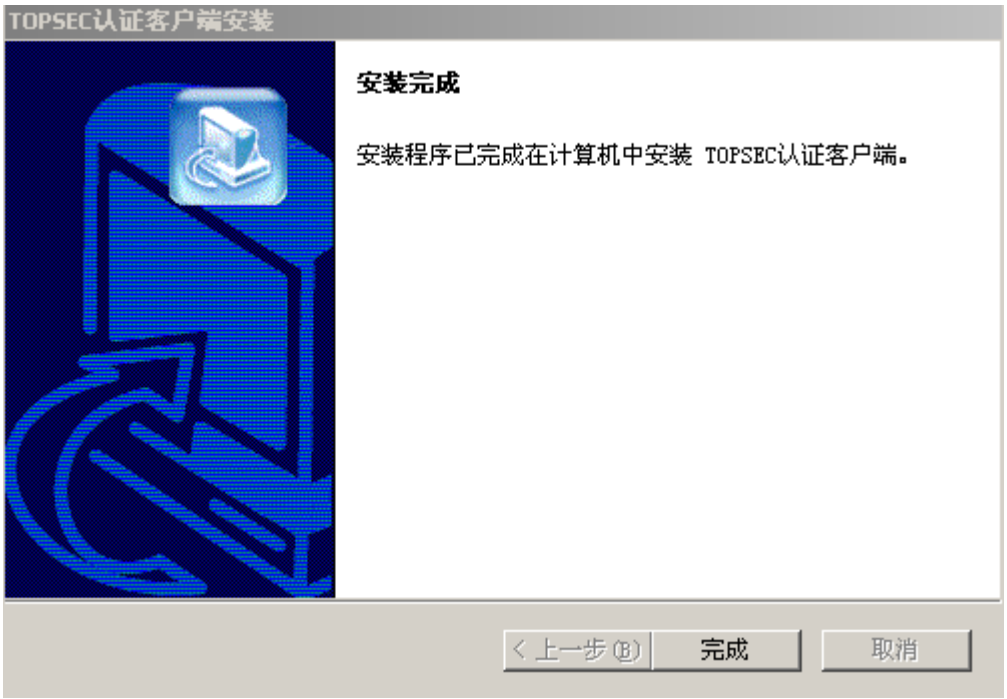
选择安装路径，缺省为：C：\Program Files\TOPSEC\AUTHCLT



选择程序文件夹：



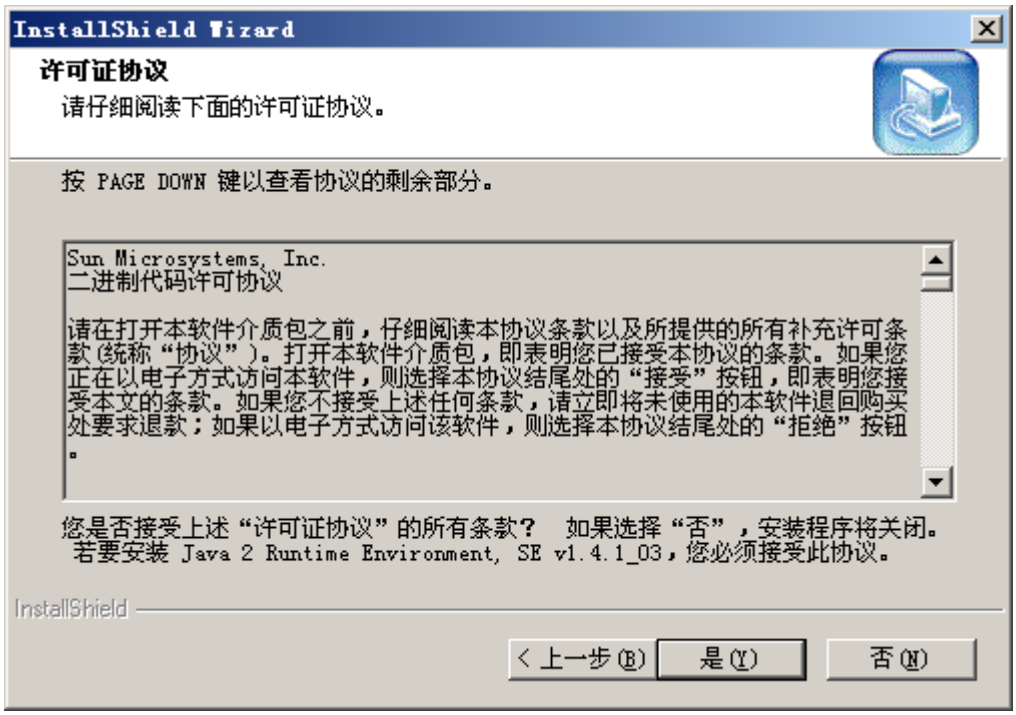
完成安装:



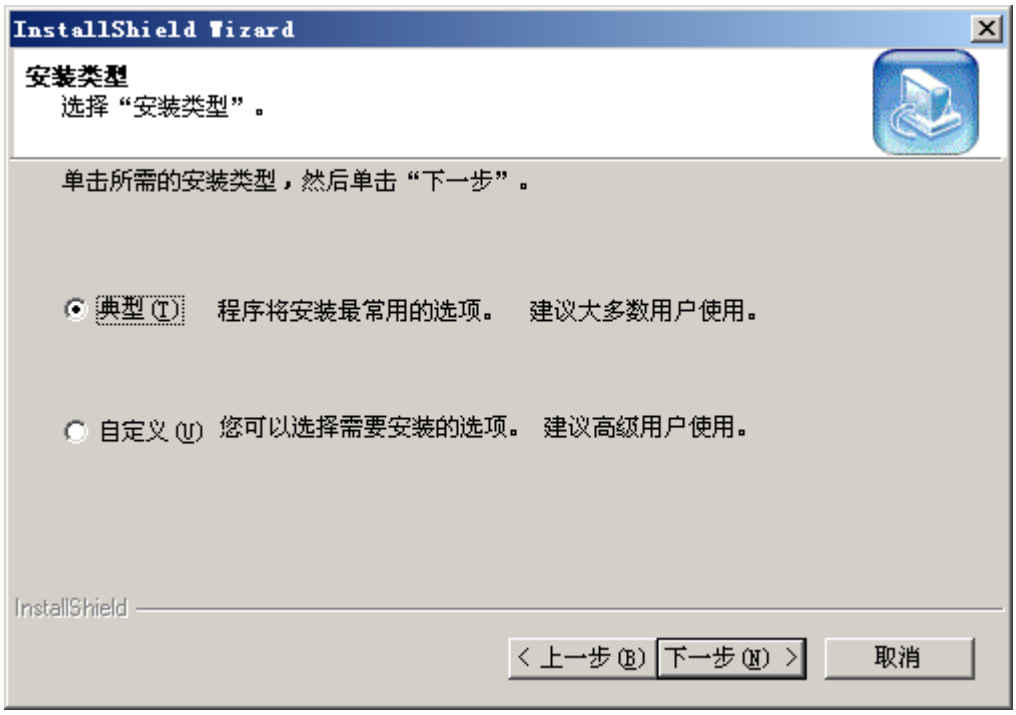
4Java 虚拟机的安装和使用

2.4.80 版本的 FW4000 除了支持原有的 TOPSEC 认证客户端外，还新增加了 OTP 的认证方式。OTP 认证必须要求在客户端上安装有 Java 虚拟机，安装软件在随机光盘的/Tools 目录下可以找到。下面就简单介绍一下在 windows 平台下的安装过程:

运行随机光盘/Tools 目录下的 j2re-1_4_1_03-windows-i586-i.exe 可执行文件，在经过初始化后，首先弹出‘许可证协议’窗口：



选择‘是（Y）’后，进入下一步：



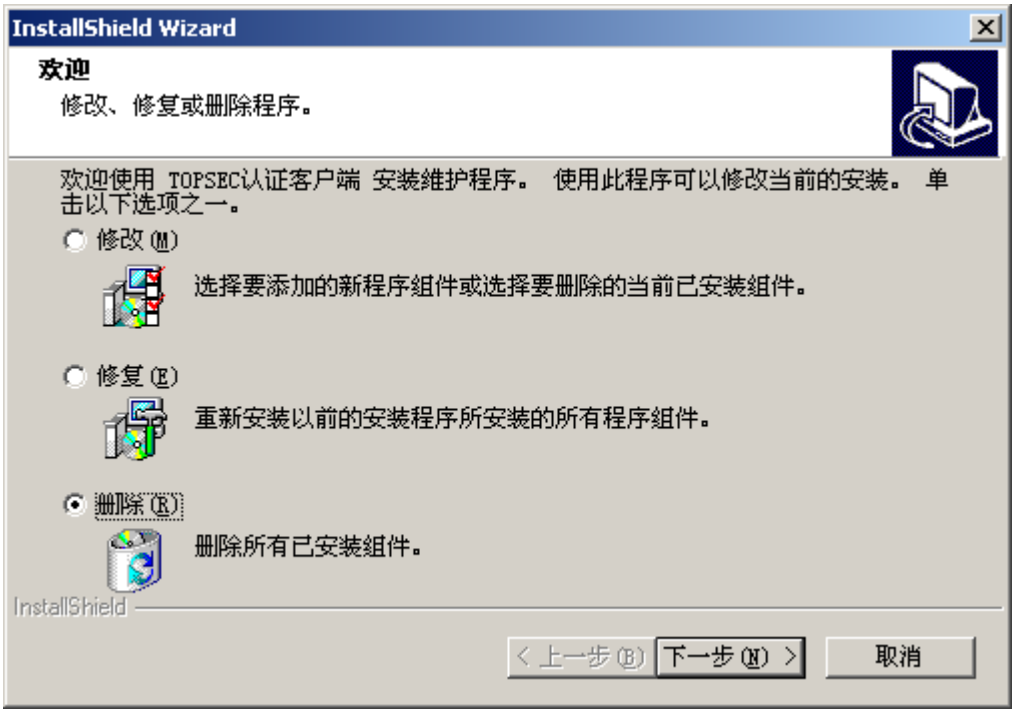
在这里推荐用户选择典型安装即可。继续下一步，就开始自动安装过程。一会后系统就会提示您安装成功。

这时，就可以使用 OTP 来进行认证了。打开 IE，在地址栏中输入防火墙的 IP 地址，认证端口为 4000，如：192.168.4.25:4000 即可（在此之前，必须先在防火墙上进行相应的设置，具体

请参见防火墙的用户手册）。回车后，就弹出认证窗口，认证类型选择‘one time password’。当然可以使用这种方式来进行 radius 和 tacacs＋的认证。

5 卸载 TOPSEC 认证客户端

运行安装盘中的安装程序：TOPSEC_AUTH_C_1.4.04.EXE，安装程序出现提示指导用户完成卸载：



用户也可以使用计算机系统中的添加/删除程序来完成 TOPSEC 认证客户端的卸载：在开始菜单中选择“设置->控制面板”，在控制面板中，选择“添加/删除程序”，打开“添加/删除程序”窗口后，选择“TOPSEC 认证客户端”，点击“更改/删除”按钮，系统指导用户完成卸载（图同上）。

1.6 版

三.接口扩展模块安装指南


接口扩展模块　　安装指南

适用型号	TopSEC-FE-1	TopSEC-FE-2
	TopSEC-FEE-1	TopSEC-FEE-2

警告:

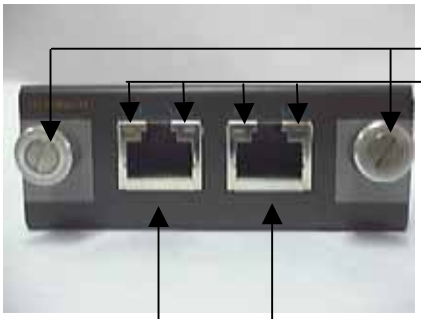
☆ 插拔接口扩展模块前，请先关闭防火墙系统的电源;

☆ 请检查防火墙电源开关处于关闭状态:

☆ 错误使用会损坏防火墙系统和模块本身;

1 产品介绍

接口扩展模块用于防火墙快速以太网接口扩展，扩展的网络接口与防火墙系统配置的网络接口具有相同的性能指标和参数。



2 规范

网络接口：10/100BASE-TX
网络接口类型：RJ45 连接器；
重量：215 克（TopSEC-FE-2/ TopSEC-FEE-2）,208 克（TopSEC-FE-1/ TopSEC-FEE-1）
几何尺寸：75 x 30 x96 mm(长 x 高 x 深)
工作温度：0 ℃~60 ℃
存储温度：-20 ℃~70 ℃

3 安装过程

拆下扩展位扩展条：扩展条的紧固螺钉在机箱底面，如下图：

取下扩展条：

注意：拆装紧固螺钉时请使用合适规格的螺丝刀，以防损坏螺钉的工具槽。

插入接口扩展模块：

接插到位后（扩展模块的端面与机箱前面板同平面），紧固锁紧螺母：

4 接口顺序

防火墙的以太网接口名称及顺序号与防火墙的安全策略定义密切相关，接口扩展模块所接插的目标系统的接口顺序遵循从右到左（正对防火墙前面板）原则，防火墙的第一个接口的名称为“eth0”，顺序号依次增加；扩展模块上的第一个网络接口为“快速以太接口 1”，顺序为从右到左（正视图）；

对于有两个扩展位的防火墙产品，接口扩展模块可以插入任意一个扩展位；

5 模块与产品型号对应表

模块型号	适用产品型号
TopSEC-FE-1 TopSEC-FE-2	NG FW4000 系列 NG FW4000-S 系列 NG FW4000-T 系列 SJW11-A 系列 SJW11-A-L 系列 SJW11-A-S 系列
TopSEC-FEE-1 TopSEC-FEE-2	NG FW4000-E 系列 SJW11-A-E 系列

说明：模块型号与产品型号严格按照以上的对应表配合使用，错误的插拔模块会损坏产品和扩展模块本身。。

版本号：1.6
发布日期：2004-9

*产品型号规格如有变化，恕不另行通知，产品图片请以实物为准

1.1 版

四.千兆接口转换器模块安装指南

适用型号：
TopSEC-GBIC-SX　　TopSEC-SFP-T
TopSEC-GBIC-LX　　TopSEC-SFP-SX
TopSEC-GBIC-ZX　　TopSEC-SFP-LX
TopSEC-GBIC-T　　TopSEC-SFP-ZX
TopSEC-GBIC-AUTO

1 GBIC 描述

千兆接口转换器模块(GigaBit Interface Converters，简称：GBIC)分为标准GBIC模块和专用GBIC模块，标准GBIC模块遵循GBIC规范5.5版本；专用GBIC模块为天融信公司产品专用，必须配合天融信的千兆产品使用；

1.1 专用GBIC

型号:TopSEC-GBIC-AUTO
接口标准：10/100Base-tx　1000Base-T
接口形式：RJ45
自适应千兆接口转换器为天融信公司产品专用模块，其必须配合天融信的千兆安全产品使用，详细说明请参见天融信千兆安全产品的规格说明；

警告：此模块产品不能用于其它厂商的产品；

1.2 标准GBIC

型号与接口标准
TopSEC-GBIC-SX：1000Base-SX
TopSEC-GBIC-LX：1000Base-LX
TopSEC-GBIC-ZX：1000Base-ZX
TopSEC-GBIC-T：1000Base-T

2 SFP 描述

小型GBIC模块（Small Form Pluggable,简称：SFP），一种小型的千兆接口转换器；适用于光纤接头为LC的线路应用。
型号与接口标准：
TopSEC-SFP-SX：1000Base-SX
TopSEC-SFP-LX：1000Base-LX
TopSEC-SFP-ZX：1000Base-ZX
TopSEC-SFP-T：1000Base-T

3 产品规格

几何尺寸（最大HxWxD）	GBIC: 10x30x65mm SFP: 13X14X66mm
连接器	GBIC: 多模光纤：SC连接器 单模光纤：SC连接器 SFP: 多模光纤：LC连接器 单模光纤：LC连接器 1000Base-T: RJ45连接器
波长	-SX: 850nm -LX: 1310nm -ZX: 1550nm
线缆距离(最大)	-T: 100m -SX: 550m -LX: 10km -ZX: 70km -AUTO: 100m
工作温度	0 ℃~60 ℃
存储温度	-20 ℃~70 ℃
重量(每个最大)	215克

4 接口线缆规格

产品型号	波长	光纤类型	芯径	带宽（MHz/km)	线缆距离
TopSEC-GBIC-SX TopSEC-SFP-SX	850	MMF	62.5	160	220m
			62.5	200	275m
			50	400	500m
			50	500	550m
TopSEC-GBIC-LX TopSEC-SFP-LX	1310	MMF	62.5	500	550m
			50.0	400	550m
			50.0	500	550m
			9/10		10km
TopSEC-GBIC-ZX TopSEC-SFP-ZX	1550	SMF			70km

5 GBIC/SFP 保护

光接口的GBIC或SFP,在未接入光纤线缆时，请将保护橡胶塞安装;

6 安装/撤卸过程

6.1 专用GBIC的安装/撤卸过程

任何情况下，需要安装或撤卸专用GBIC 时候，请首先关闭主设备的电源;

警告：未关闭电源就执行后续的安装或撤卸操作，可能导致系统无法正确识别模块类型而不能正常工作甚至损害。
检查GBIC 的型号为你需要的类型，请查看GBIC 正面的标签;
标签面朝下，将GBIC插入到设备上的GBIC 插槽
听到“咔哒”一声后，表示GBIC正确插入到GBIC槽位中
拔卸过程时，请按下GBIC 两侧的卡口，直接拔出即可;

注意事项:
通用接口与专用接口不能混插，即0和1，2和3，4和5端口必须插入相同类型的GBIC模块，不能在0口插入专用模块而1口插入通用模块。同理对2和3，4和5端口也是一样。

6.2 通用GBIC的安装/撤卸过程

标准GBIC 支持热插拔，需要安装前:

请先确认主设备的插槽已经工作在标准GBIC 状态下，GBIC 的状态切换请参看主设备的安装手册；
注意：天融信公司的主设备上的GBIC 插座可以工作在标准GBIC 模式和专用GBIC 模式，实现模式切换，设备需要重新启动；不匹配的工作模式会导致对应GBIC 接口工作错误；
确认GBIC 的型号正确，对于光接口GBIC,请确认为你希望的波长；
将GBIC 标签面朝下，插入主设备的GBIC 插槽；
听到“咔哒”一声后，表示GBIC 已经正确插入到GBIC 槽位中；

撤卸过程按下GBIC 两侧卡口直接拔下；

注：在标准模块与专用模块混插的情况下，端口号的识别会发生变化，防火墙会先识别标准模块，然后识别专用模块，
例如：在eth2 插入了专用模块，其它口均插标准模块，那么防火墙在识别端口号时，会认为
eth0=0,eth1=1,eth4=2,eth5=3,eth2=4,eth3=5
也就是说，在标准模块全部排完后，再排专用模块，因此，在给客户安装模块时，最好从eth5 开始安装，然后依次向前。

6.3 SFP 安装过程

SFP 模块支持热插拔；
安装前请确认模块为你需要的型号；
请将SFP 模块的标签面朝上，松开卡紧环，插入SFP 插座；
插到位后请向上拉紧卡环；
撤卸SFP:
将SFP 模块上的线缆拔下；
松开卡环，直接拔下即可；

7 Class 1 Laser Compliance

本产品测试标准：Class 1 laser EN 60825-1
AND FDA 21 CFR 1040.10 AND 1040.11

8 适用产品型号

NGFW4000-UF
NGFW4000-UF-VPN(S)
NGFW4000-UF-VPN(E)

文档版本号：V1.1
发布日期：2004年9月
TopSEC®天融信公司

*产品型号规格如有变化，恕不另行通知。

五.专用 GBIC：GBIC-AUTO 模块安装指南

注：只有产品型号代码为“6GN”、“6GF”、“4MN”、“5MN”的千兆产品支持 TopSEC-GBIC-AUTO 类型的千兆转换器
产品型号代码贴在防火墙硬件的后面标签中。

1 GBIC-AUTO 模块简介

由于普通的电口 GBIC 都只能工作在千兆状态，无法自适应到百兆状态，为使此电口自适应地工作在百兆或千兆状态，我司特设计具有自适应 GBIC 模块：TOPSEC-GBIC-AUTO，简称 GBIC-AUTO 模块。当使用标准的 GBIC 模块时，相应的端口按照标准的 GBIC 方式工作；当使用特殊 GBIC－AUTO 模块时，相应端口工作在 10/100/1000Base-T 状态。

2 GBIC-AUTO 的安装/撤卸过程

任何情况下，需要安装或撤卸专用 GBIC 时候，请首先关闭主设备的电源；

警告：未关闭电源就执行后续的安装或撤卸操作，可能导致系统无法正确识别模块类型而不能正常工作甚至损害。
检查 GBIC 的型号为你需要的类型，请查看 GBIC 正面的标签；
标签面朝下，将 GBIC 插入到设备上的 GBIC 插槽
听到“咔哒”一声后，表示 GBIC 正确插入到 GBIC 槽位中
拔卸过程时，请按下 GBIC 两侧的卡口，直接拔出即可；

注意事项：
通用接口与专用接口不能混插，即 0 和 1，2 和 3，4 和 5 端口必须插入相同类型的 GBIC 模块，不能在 0 口插入专用模块而 1 口插入通用模块。同理对 2 和 3，4 和 5 端口也是一样。

3 GBIC-AUTO 模块使用说明

此模块与公司的主板 TOPSEC-SBC04C 配套工作，安装使用时需要注意以下事项：

3.1 重新启动

当要插入 GBIC-AUTO 模块时，如果系统处于运行状态，需要将系统关闭，然后将所需要使用的 GBIC 槽位中的原有 GBIC 模块取出，再放入 TOPSEC-GBIC-AUTO 模块，重新开机后方能使用。

3.2 端口限定

互限端口：只能工作在相同模式下的两个端口，这两个端口属于同一个控制组。
相同控制组：产品型号代码为“6GN” 、“6GF”、“4MN”、“5MN”的千兆产品中 ETH0 和 ETH1 为一控制组，ETH2 和 ETH3 为一控制组，ETH4 和 ETH5 为一控制组，
如果一个端口工作在 GBIC-AUTO 模式下，其相同控制组的另一个互限端口也只能工作在该模式下；类似的，如果一个端口工作在普通模式下并使用标准的 GBIC 模块，其相应的另一个互限端口也只能工作在普通模式下。

3.3 更换 GBIC-AUTO 模块

检查系统是否处于运行状态，如果是，请将系统关闭；
将需要使用的 GBIC 槽位 A 及其互限槽位 B 清空；
在 A 槽位中放入 TOPSEC-GBIC-AUTO 模块；
B 槽位只能使用 TOPSEC-GBIC-AUTO 模块，否则将其空置；

3.4 更换标准 GBIC 模块

检查系统是否处于运行状态，如果是，请将系统关闭；
将需要使用的 GBIC 槽位 A 及其互限槽位 B 清空；
在 A 槽位中放入标准 GBIC 模块；
B 槽位只能使用标准 GBIC 模块，否则将其空置；

技术支持
电话：86-10-82611122，　800-810-5119
传真：86-10-62304552
www.topsec.com.cn
邮件：support@topsec.com.cn
北京市海淀区希格玛大厦 4 层

更多的信息请参阅防火墙产品说明书或查阅天融信的技术支持网站：
www.topsec.com.cn

备注：

若实际操作中的图形与手册的图形有出入的地方，均以实图为准，但此处变化不影响功能的描述。